シトリックス バーチャル アプリ アンド デスクトップ™ 7 2603

> **重要:**
>
> 現在のリリース (CR) および長期サービスリリース (LTSR) の製品ライフサイクル戦略については、Lifecycle Milestonesに記載されています。

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

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

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

以前のリリース

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

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

Citrix Cloud™環境でのCitrix Virtual Apps and Desktopsの利用について

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

役立つリンク

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

新機能

リリースについて

Citrix Virtual Apps and Desktops™ 2603 リリースには、Windows Virtual Delivery Agent (VDA) の新しいバージョンと、いくつかのコアコンポーネントの新しいバージョンが含まれています。次のことができます。

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

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

インストールとアップグレードの手順：

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

サポート対象バージョンおよびレガシーバージョンのドキュメント

サポートされているバージョンのドキュメントは、Citrix Virtual Apps and Desktops で入手できます。

End of Life (EOL) バージョンのドキュメント PDF は、レガシードキュメントにアーカイブされています。

リリース情報

- 新機能

- 修正された問題
- 既知の問題
- 非推奨および削除

新機能

この記事では、Citrix Virtual Apps and Desktops™ 7 2603 の新機能と強化された機能について説明します。更新はコンポーネントごとに整理されています。

デリバリーコントローラー

SQL Server 2025 のサポート

Citrix Virtual Apps and Desktops は SQL Server 2025 をサポートするようになりました。その他のサポートされている SQL Server のバージョンについては、「データベース」を参照してください。

HDX

HDX 接続

Microsoft Entra シングルサインオン (プレビュー)

Microsoft Entra ハイブリッド参加セッションホストで仮想アプリケーションおよびデスクトップにアクセスする際に、Microsoft Entra ID 資格情報を使用してシングルサインオン (SSO) を利用できるようになりました。詳細については、「Microsoft Entra シングルサインオン」を参照してください。

HDX ダイレクト

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

仮想チャネル許可リスト

VDI 用の Microsoft Teams および Zoom Meetings 仮想チャネルは、仮想チャネル許可リストに明示的に追加する必要がなくなりました。詳細については、「サードパーティ製仮想チャネルに関する考慮事項」を参照してください。

デバイス

タッチキーボードの動作とジェスチャ処理の強化

この機能強化により、アプリケーションのハングを防ぎ、応答しないタッチ入力を修正し、意図的なシングルタップ操作でのみタッチキーボードが表示されるようにすることで、タッチ対応 CVAD セッションの信頼性が大幅に向上します。Microsoft Teams、Slack、ファイルエクスプローラー、Visual Studio Code などの一般的なアプリで、**高遅延**環境でも互換性と**タッチドラッグ**の応答性が向上しています。

マルチメディア

HDX Teams Redirection Service の明示的なサービス依存関係

Citrix HDX Teams Redirection Service (HDX Optimized Microsoft Teams および UCSDK Optimized アプリケーションで使用) は、**Citrix HDX HTML5 Video Redirection Service (WebSocketService)** への依存関係を明示的に宣言するようになりました。

この更新により、Teams サービスが起動する際に HTML5 サービスが自動的に検証および開始され、サービスが厳密に管理されている環境での Microsoft Teams および UCSDK 統合アプリケーションの最適化の失敗が防止されます。詳細については、「Microsoft Teams 最適化の明示的なサービス依存関係」を参照してください。

UCSDKとHDX Microsoft Teams最適化の分離

Citrix Unified Communications SDK (UCSDK) を使用するアプリケーションの最適化は、**Microsoft Teams リダイレクト**ポリシーに依存しなくなりました。管理者は、他の UCSDK 統合アプリケーションの最適化を中断または無効にすることなく、Microsoft Teams の最適化を無効にできるようになりました。詳細については、「Unified Communications SDK ドキュメント」を参照してください。

Web カメラリダイレクトによる Microsoft 仮想カメラのサポート

2603以降、Windows VDA (Windows 11およびWindows Server 2025) は、Microsoftの組み込み仮想カメラ機能を使用して、Webカメラのリダイレクトとカメラエクスペリエンスをアップグレードします。これにより、より多くのアプリケーションとの互換性の拡張、セキュリティとプライバシーの向上、ローカルおよびネイティブのカメラエクスペリエンスに近い提供といったメリットがあります。この機能はデフォルトで有効になっています。

> **注:**

この機能には、システム設定で**カメラへのアクセス**が有効になっている必要があります。この設定は、Windows Server 2025ではデフォルトで無効になっています。

グラフィック

CTX Snippingツール

VDAには、BCRや最適化されたTeamsなどのオーバーレイコンテンツのスクリーンショットをユーザーが撮影できる新しいCTXSnippingツールが含まれるようになりました。

視覚品質の向上

デフォルトの視覚品質設定により視覚品質が向上し、ネットワークの変化により効果的に調整されるようになりました。

インテリジェントサーフェスエンコーディング

インテリジェントサーフェスエンコーディングは、複数のモニターを使用する際の混合ワークロードや高負荷ワークロードのパフォーマンスを向上させます。

HDXグラフィック超解像度 GA

HDXグラフィック超解像度が一般提供開始されました。HDXグラフィック超解像度は、帯域幅の状態が最適でないと検出され、互換性のあるクライアントが利用可能な場合に、デフォルトで自動的に有効になります。

視覚的にロスレスなサポートの拡張

YUV 4:4:4による視覚的にロスレスな圧縮が、選択的エンコーディング、Build to Lossless、Intelligent Build to Losslessを含むすべてのビデオエンコーディングモードで利用可能になりました。

クリップボード

クリップボードの事前定義された形式グループ

Citrixクリップボードポリシーには、最も一般的な種類のクリップボードデータに対応する事前定義された形式グループが含まれるようになりました。

シームレスアプリケーション

シームレスアプリケーションのアイコンバッジサポート

アプリケーションのステータスや更新を示すために、シームレスアプリケーションへのアイコンバッジのサポートが追加されました。

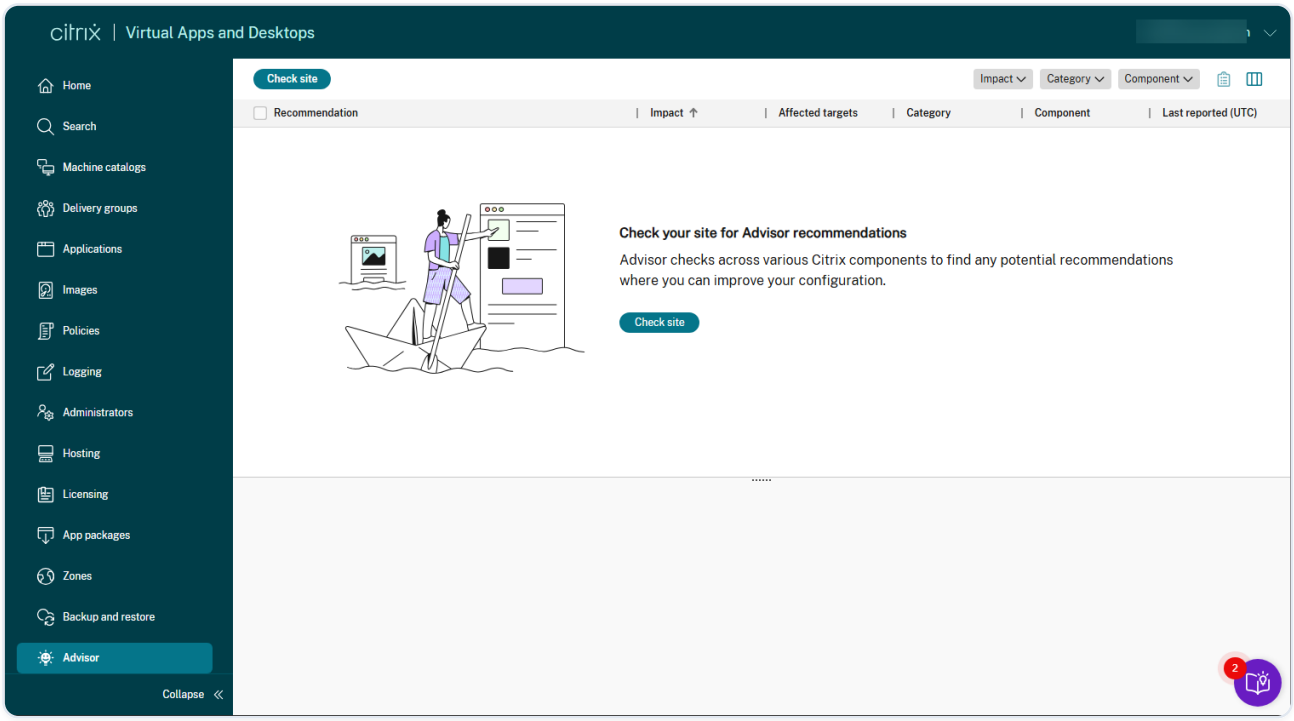
ウェブスタジオ

Web Studio との Citrix Aidrien 統合

Web Studio では、右上隅から Citrix Aidrien を開いて、Citrix ナレッジベースから AI を活用した回答を得られるようになりました。クリックすると、新しいブラウザタブが開き、資格情報を使用して Citrix Cloud にサインインし、チャットを開始できます。

Citrix Advisor: 展開のためのプロアクティブなインサイトと最適化

Citrix Advisor は、展開を最適化し、その全体的な健全性と準備状況を向上させるのに役立つコンポーネントです。環境チェックを自動化し、実用的な推奨事項を提供することで、構成の問題、非効率性、リソースの無駄、ベストプラクティスからの逸脱などをプロアクティブに特定できるようになります。



Advisorを使用すると、次のことができます。

- **問題をプロアクティブに特定し、解決する:** ユーザーに影響を与えたり、ビジネス運用を妨げたり、セキュリティを侵害したりする前に、潜在的な問題、構成のずれ、ベストプラクティスからの逸脱を検出します。
- **環境のパフォーマンスと安定性を最適化する:** 構成を微調整し、リソース割り当てを最適化し、ベストプラクティスを実装して、Citrix展開の安定性、セキュリティ、およびパフォーマンスを向上させます。
- **運用を合理化し、オーバーヘッドを削減する:** 定期的なチェックを自動化し、複雑な修復タスクを簡素化し、ガイド付き支援を受けることで、運用オーバーヘッドを削減し、管理リソースを解放します。

- **コストとリソース利用を最適化する:** 過剰支出の領域を特定し、リソース最適化の機会を発見し、Citrixテクノロジーの効率的な利用を確保して、総所有コストを最小限に抑えます。
- **コンプライアンスとベストプラクティスへの準拠を維持する:** Citrix展開がCitrixのベストプラクティス、セキュリティ標準、および業界規制に準拠していることを確認し、リスクを軽減し、全体的なガバナンスを向上させます。
- **複雑なタスクを簡素化する:** 健全で最適化された環境をサポートするために、管理タスクを簡素化します。

詳細については、「Citrix Advisor」を参照してください。

Web Studio での Microsoft Entra シングルサインオン構成

Web Studio > 設定で、Microsoft Entra シングルサインオン (SSO) を直接構成できるようになりました。この機能を有効にすると、デリバリーグループの作成時にユーザーログオンのIDタイプを選択する際に、**Microsoft Entra ハイブリッドID**オプションが利用可能になります。

詳細については、「Web Studio で Microsoft Entra シングルサインオン (SSO) を構成する」および「デリバリーグループ内のリソースにユーザーがアクセスする方法を構成する」を参照してください。

リソースフィルタリング

リソースフィルタリング機能を使用すると、デリバリーグループ全体のリソースへのユーザーアクセスを制御するルールを構成できます。リソースタイプ (アプリケーション、デスクトップ、またはその両方) を定義し、タグ制限を適用し、ネットワークの場所やストア接続コンテキストなどの要因に基づいてルール適用の条件を設定できます。この機能にアクセスするには、**デリバリーグループ > 設定 > リソースフィルター**に移動します。詳細については、「すべてのデリバリーグループのリソースへのユーザーアクセスを制限する」を参照してください。

デフォルトポリシーセットのスコープ制御の改善

ポリシーセットにはスコープ制御が利用可能でした。互換性を維持するため、**デフォルトポリシーセット**は現在、*任意*のスコープに割り当てられており、**スコープ制御のバイパス**がデフォルトで有効になっています。スコープに基づいてアクセスを制限したい場合は、**デフォルトポリシーセット**の割り当てを確認し、調整してください。

スコープの割り当ては、次の2つの方法で更新できます。

- ポリシーから：**デフォルトポリシーセット**を編集し、関連するスコープを変更します。
- スコープから：**管理者 > スコープ**でスコープに移動し、そこから**デフォルトポリシーセット**を割り当てるか削除します。

詳細については、「スコープの作成と管理」および「ポリシーセットの作成と管理」を参照してください。

拡張されたアイコンサポート

デスクトップやアプリケーションのアイコンをカスタマイズする際、以前サポートされていた `.icon` 形式に加えて、`.exe` ファイルからアイコンを抽出して使用できるようになりました。

これらのアイコンは、ローカルマシンまたはVDAマシンから参照して選択できます。サポートされるアイコンファイルの最大サイズは500 KBです。詳細については、「デリバリーグループの作成」を参照してください。

Task Center が利用可能になりました

Task Center は、Studio でスケジュールされたタスクと定期的なタスクを一元的に表示し、これらのタスクのステータス (スケジュール済み、完了、失敗、実行間近) を追跡するのに役立ちます。Task Center には、Studio コンソールの右上隅にあるカレンダーアイコンを選択してアクセスできます。

このリリースでは、Task Center は ハードウェア更新 および OS ディスクのリセット タスクをサポートします。追加のタスクタイプのサポートは、今後のリリースで追加される予定です。詳細については、「Task Center でタスクを監視および管理する」を参照してください。

タスクセンター(/en-us/citrix-virtual-apps-desktops/current-release/media/whatsnew-task-center.png)

ネットワーク共有から Numecent Cloudpaging アプリケーションを検出する

Web Studio の ノードを使用して、ネットワーク共有から Numecent Cloudpaging アプリケーションを検出できるようになりました。以前は、Cloudpaging の検出は Cloudpager コンソールからのみサポートされていました。この機能には、VDA バージョン 2603 以降のデリバリーグループが必要です。詳細については、「アプリパッケージの展開と配信」を参照してください。

検索メインビューの列レイアウトをカスタマイズする

Web Studio で列の順序を変更して、関連情報をより適切に整理およびグループ化できるようになりました。Web Studio は列の順序と幅の設定を保持するため、カスタマイズされたレイアウトはセッション間で維持されます。現在、この機能は検索のメインビューでサポートされています。

検索ノードでの複数選択の改善

検索ノードをより直感的なテーブルレイアウトに更新しました。この変更により、次のことが可能になります。

- 各行のチェックボックスを使用して複数の項目を選択できるため、より直感的な操作が可能になります。
- 列ヘッダーのチェックボックスを使用して、現在のページのすべての項目を選択します。

複数選択とページレベルの選択は新しい機能ではありませんが（以前はキーボードショートカットを使用して行われていました）、この機能強化により、アフォーダンスとユーザビリティが大幅に向上し、将来の複数ページにわたる複数選択のサポートの基礎が築かれます。

PowerShell SDK を使用したデータベースとサイトの自動アップグレード

Site Manager を介したアップグレードに加えて、新しい PowerShell SDK コマンドレット `Update-XDSite` を使用して、データベースとサイトを自動的にアップグレードできるようになりました。このコマンドレットは、バージョンに依存しないアップグレードプロセスの長期的な自動化を可能にし、Site Manager を使用する代替手段を提供します。スクリプト化された、または繰り返し可能なアップグレードワークフローを必要とする環境で特に役立ちます。

詳細については、「データベースとサイトを自動的にアップグレードする」および「Citrix Virtual Apps and Desktops SDK ガイド」を参照してください。

Red Hat OpenShift: MCS を使用した Citrix Provisioning カタログ

Web Studio を使用すると、Red Hat OpenShift 仮想化環境で Citrix Provisioning カタログを作成できるようになりました。以前は、これらのカタログをプロビジョニングおよび管理するために、異なるコンソールを切り替える必要がありました。この機能によりプロセスが簡素化され、プロビジョニングと電源管理タスクをすべて Studio 内で実行できます。詳細については、「Citrix Studio で Citrix Provisioning™ カタログを作成する」を参照してください。

自動アンシェアによるイメージバージョンの削除の簡素化

以前は、共有イメージバージョンを削除するには、まず「イメージ共有の管理」を介してすべてのリソースロケーションから手動でアンシェアし、その後削除する必要がありました。

現在、展開にイメージバージョンを積極的に使用しているマシンカタログがない限り、1つのステップで削除できます。Web Studioは、削除の一部として、すべてのリソースロケーションにわたるイメージ共有構成を自動的に削除します。手動でのアンシェアは不要です。

XenServerの同じリソースプール内のホスト間で準備済みイメージバージョンを共有する

XenServerの同じリソースプール内のホスト間でイメージバージョンを共有するために、**イメージ**ノードを使用できるようになりました。この実装により、異なるホスト間でのイメージの一貫性と均一性が確保され、展開の柔軟性と運用効率が向上します。この目的を達成するために

PowerShellコマンドを使用することもできます。詳細については、イメージ管理を参照してください。

Azure Localの準備済みイメージを管理する

イメージ管理機能がAzure Local環境で一般提供されるようになりました。**イメージ**ノードを使用して、イメージ定義、バージョン、およびMCSマシンカタログを作成できます。この実装により、ストレージと時間のコストが大幅に削減され、VMの展開とイメージの更新プロセスが簡素化されます。この目的を達成するためにPowerShellコマンドを使用することもできます。詳細については、Azure Localで準備済みイメージマシンカタログを作成するを参照してください。

既存のIDプールを使用してMCSプロビジョニング済みマシンのIDを作成する

Studioを使用してAD参加カタログを作成したり、マシンを追加したりする際に、既存のIDプールを使用してマシンIDを割り当てることができるようになりました。この機能により、複数のカタログ間で一貫したマシンアカウント命名スキームを適用できます。詳細については、マシンIDを参照してください。

エフェメラルOSディスク用のAzure SSDストレージタイプ

Studioでは、AzureエフェメラルOSディスクを使用するAzureマシンカタログで、カタログ作成時およびその後のカタログ/スキーム更新時に、ベースOSマネージドディスクストレージタイプ（Premium SSD、Standard SSD、またはStandard HDD）を選択できるようになりました。UI検証と事前チェックにより、サポートされていない構成が防止されます。

詳細については、AzureエフェメラルOSディスクを使用するを参照してください。

Citrix Director (シトリックス ディレクター)

シトリックス エイドリアンとシトリックス ディレクターの統合

Citrix Directorは、2603リリースでCitrixおよびNetScalerソリューションの製品内サポートと支援のために、Citrix CloudのCitrix Aidrienとの統合を含むようになりました。ワンクリックで、管理者はCitrix CloudでCitrix Aidrienを起動し、Citrix Cloudの資格情報を使用してサインインし、Citrix Aidrienの機能にアクセスできます。

Citrix AidrienおよびCitrix Directorでサポートされているユースケースの詳細については、Director向けCitrix Aidrien統合を参照してください。

Citrix Directorでのアプリ保護レポート

保護ポリシーのアクティベーションとセキュリティリスク検出のリアルタイムレポートは、Citrix DirectorおよびMonitorで利用できます。このレポートにより、リスクを迅速に評価し、より安全な

環境を確保するために保護ポリシーを設定できます。プロアクティブなリスク管理とポリシーの再構成により、環境のエンドポイントセキュリティを強化し、新たな脅威への露出を減らすことができます。詳細については、「Directorでのエンドポイントセキュリティポリシーのアクティベーションと脅威検出レポート」を参照してください。

uberAgent統合 - セッション、マシン、アプリケーションのパフォーマンスメトリックの強化

uberAgentからのセッション、マシン、およびアプリケーションのパフォーマンスデータが、Director/Monitorで利用可能になります。DirectorおよびMonitorの統合された可観測性により、パフォーマンスデータがCitrix環境の単一の一貫したビューにまとめられます。これにより、セッションスコアなどのユーザーエクスペリエンス指標が、基盤となるセッション動作、マシンリソース使用率、およびアプリケーションパフォーマンスと相関付けられ、配信スタック全体にわたるエンドツーエンドの可視性が提供されます。この統合されたアプローチは、管理者が全体的なエクスペリエンスの健全性を評価し、パフォーマンスの傾向を分析し、切断されたビューやツールを切り替えることなくパフォーマンス問題の根本原因を特定するのに役立ちます。

Citrix DaaS MCP Server Local がプレビュー版として利用可能に

Citrix Virtual Apps and Desktops には、MCP 対応 AI エージェントを Citrix Delivery Controller に接続する Model Context Protocol (MCP) サーバーが含まれるようになりました。管理者は AI エージェントを使用して、デリバリーグループ、マシンのステータスと正常性、セッションパフォーマンス、セッションログオンなどの詳細の取得を含む、Citrix Virtual Apps and Desktops サイトのクエリとトラブルシューティングを行うことができます。詳細については、Citrix DaaS MCP Server Localを参照してください。

マシンクリエーションサービス™ (MCS)

サービスウィンドウ

サービスウィンドウ機能は、MCSプロビジョニングされたVMに対する操作をスケジュールおよび自動化する機能を提供します。この機能は現在、Web StudioおよびPowerShellを使用して、OSディスクのリセットやハードウェア構成の変更など、さまざまな操作をサポートしています。詳細については、以下を参照してください。

- サービスウィンドウ
- Azureでのサービスウィンドウ操作

既存のMCSプロビジョニング済みカタログのActive Directoryアカウントを修復する

サービスウィンドウを使用して、既存のオンプレミスAD参加済みおよびMicrosoft Entra Hybrid参加済みMCSマシンカタログのActive Directory (AD) コンピュータアカウントを修復できるようになりました。これは、VMがドメイン信頼を失った場合に役立ちます。この機能は、永続的および非永続的MCSマシンカタログの両方に適用されます。詳細については、「既存のカタログのADアカウントを修復する」を参照してください。

オンプレミスイメージレプリケーションの管理

この機能強化により、オンプレミスハイパーバイザー向けの明示的なイメージレプリケーションワークフローが導入されます。以前は、新しく追加されたストレージの場所や置き換えられたストレージの場所にイメージバージョンインスタンスをレプリケートすることができず、必要なすべてのストレージでイメージの可用性を管理することが困難でした。この機能強化により、PowerShellコマンドを実行して、イメージバージョンインスタンスをストレージの場所にレプリケートできます。この機能は、VMware、XenServer、Nutanix AHV Prism Central環境を含むオンプレミスハイパーバイザーに適用されます。

詳細については、「サポートされているオンプレミスハイパーバイザーの追加ストレージのイメージレプリケーション」を参照してください。

既存のMCSプロビジョニング済みカタログでEntraハイブリッド参加を有効にする

サービスウィンドウを使用して、既存のオンプレミスActive Directory参加済みMCSマシンカタログをMicrosoft Entra Hybrid参加済みカタログに変換できるようになりました。この機能は、永続的および非永続的MCSマシンカタログの両方に適用されます。詳細については、「既存のカタログのEntra Hybrid参加を有効にする」を参照してください。

非永続的VMのSCCM GUIDを保持する

この機能強化により、MCSはSCCMクライアントがインストールされたMCSプロビジョニング済み非永続的VMのSMS一意識別子 (`GUID`) を保持します。以前は、これらのマシンは再起動またはイメージ更新時に新しい `GUID` を生成し、SCCMコンソールに重複エントリが発生していました。

これにより、次のことが可能になります。

- プロビジョニングされた各マシンに一意のSCCMクライアント `ID` があることを確認します。
- SCCMコンソールで同じマシンに対する重複エントリを防止します。
- 再起動およびイメージ更新後も永続的なSCCM `GUIDs` を維持します。

MCSでのEntra ID拡張属性のサポート

Entra ID拡張属性をMCS環境に統合できるようになりました。これらの属性を使用すると、Entra IDデバイスオブジェクトに一意のカスタムデータを直接保存できます。これにより、拡張属性を持つデバイスをフィルタリングすることで、正確な条件付きアクセスポリシーを適用できます。デバイス属性に基づいてさらにフィルタを作成するには、「Supported operators and device properties for filters」を参照してください。この機能は、Microsoft Entraハイブリッド参加済みIDタイプでサポートされています。

Entra ID拡張属性（ExtensionAttribute1-15）を使用してMCSマシンカタログを管理できます。このためには、「Device.ReadWrite.All」権限を持つサービスプリンシパルを準備します。StudioとPowerShellコマンドの両方を使用して、Extra ID拡張機能でMCSマシンカタログを作成および更新できます。

拡張属性は、デバイス（永続VMと非永続VMの両方）が登録されるときに割り当てられます。「Identity pool of Microsoft Entra hybrid joined machine identity」を参照してください。

アジュール

準備済みイメージ用のAzure ZRSディスクタイプ

AzureのMCSでは、MCSイメージ管理を使用して準備済みイメージにゾーン冗長ストレージ（`ZRS`）ディスクタイプを選択できるようになりました。この機能強化により、ディスクタイプの選択の柔軟性が向上し、準備済みイメージディスクの可用性が高まることで、AzureのMCSマシンカタログの回復性が向上します。

これにより、次のことが可能になります。

- より高い可用性を持つ準備済みイメージディスクを使用できます。
- ゾーンの停止による準備済みイメージの損失リスクを回避します。
- ストレージ側のディスク障害の影響を受けることなく、継続的な運用を維持します。

詳細については、「準備済みイメージの作成」を参照してください。

Azure VMの可用性ゾーンを変更する

この機能強化により、Azureの既存のMCSプロビジョニング済みVMの可用性ゾーンプロパティを変更できます。以前は、VMの再作成が必要でした。この機能は、特に永続仮想マシンにとって、より高い柔軟性を提供します。

これにより、次のことが可能になります。

- 既存のAzure VMをアベイラビリティゾーンのアフィニティを持たないように調整します。

- 現在アベイラビリティゾーンが割り当てられていないAzure VMに、特定のアベイラビリティゾーンを割り当てます。
- 既存のAzure VMをあるアベイラビリティゾーンから別のアベイラビリティゾーンに移動します。

詳細については、「プロビジョニングされたマシンを現在のプロビジョニングスキームの状態に更新する」を参照してください。

Azureバックアップ SKUミックスの強化

この機能強化により、Azureの`BackupVmConfiguration`機能における以前の制限が解消されます。以前は、休止状態をサポートするVM SKUとサポートしないVM SKUを同じバックアップリスト内で混在させることはできませんでした。この更新により、休止状態対応と非休止状態対応の両方のSKUをバックアップ構成に含めることができます。

これにより、次のことが可能になります。

- バックアップ構成でより広範なVM SKUを使用できます。
- AzureでのVMプロビジョニングと起動の成功率を向上させます。
- デプロイの回復性を高めます。

詳細については、「バックアップVMサイズの構成」を参照してください。

エフェメラルOSディスク用のAzure SSDストレージ

この機能により、より高ティアのSSDストレージタイプを選択できるようになり、Azureでのエフェメラル OSディスクのパフォーマンスが向上します。以前は、`Standard_LRS`のみがサポートされていました。現在では、MCSカタログを作成する際に`StorageType`カスタムプロパティを設定することで、`StandardSSD_LRS`または`Premium_LRS`を使用できます。

これにより、次のことが可能になります。

- 信頼性が向上し、より高いSLAを達成できます。
- `Standard_LRS`と比較して、大幅に高いIOPSを体験できます。

詳細については、「エフェメラルディスクで使用されるストレージタイプの構成」を参照してください。

Azure拡張ゾーンのサポート

MCSプロビジョニングを使用して、Azure Extended Zonesでワークロードをプロビジョニングできるようになりました。Azure Extended Zonesは、主要なAzureリージョンのフットプリントの小

さい拡張機能です。これらは、メインリージョンの場所から離れた顧客に対して、低遅延とデータレジデンシーを提供します。詳細については、「Azure Extended Zones」を参照してください。

AWS

Amazon Workspaces Coreマネージドインスタンス: PowerShellを使用したクロスアカウントプロビジョニング

Cloud Connectorを別のAWSアカウント（共有サービスアカウントまたはサイトコンポーネントアカウント）に配置し、クロスアカウントアクセス（クロスアカウントIAMロール）を持つIAMロールを使用し、MCSプロビジョニング済みマシンカタログを別のセカンダリAWSアカウント（ワークロードアカウント）に配置するユースケースがあります。この場合、別のAWSアカウントに追加のCloud Connectorは必要ありません。このようなシナリオをサポートするために、この機能はVPCピアリングとIAMロールを使用したクロスアカウントアクセスを利用して、複数のAWSアカウントを管理する企業向けに異なるAWSアカウント間でのプロビジョニングを可能にします。

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

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

詳細については、「クロスアカウントプロビジョニング」を参照してください。

Amazon WorkSpaces Core マネージドインスタンスの柔軟な課金

Citrix MCS を使用して Amazon WorkSpaces Core マネージドインスタンスをプロビジョニングする際に、月額 (定額) と時間単位 (従量課金) の課金モデルを選択できるようになりました。

この柔軟性により、特定のワークロード要件と使用パターンに基づいてコンピューティングコストを最適化できます。

永続デスクトップには月額課金モードを使用して予測可能な定額料金のメリットを享受するか、オンデマンドまたは断続的なワークロードには時間単位課金を使用してください。

この機能を使用するには、AWSアカウントがAmazon WorkSpaces課金サービス用に構成されている必要があります。

詳細については、「Fexible billing」を参照してください。

Amazon WorkSpaces CoreマネージドインスタンスのMCSIO対応MCSマシンカタログ作成のサポート

MCSIO対応MCSカタログを作成して、Amazon WorkSpaces CoreマネージドインスタンスのMCSIO対応MCSマシンカタログを作成できるようになりました。これにより、書き込み操作をライトバックキャッシュに転送することで書き込みIOPSを向上させ、OSディスクの永続化が有効になっている場合の起動時間を短縮できます。詳細については、「MCSIO対応カタログ」を参照してください。

AWS EC2のマシンプロファイルを使用した、VMへのネットワークインターフェースごとのセキュリティグループ割り当てのサポート

AWS EC2仮想化環境では、プロビジョニングされたVMにENI（ネットワークインターフェース）ごとのセキュリティグループが割り当てられるMCSマシンカタログを作成できるようになりました。これを行うには、異なるセキュリティグループが異なるENIにマッピングされているマシンプロファイル入力（EC2インスタンスまたは起動テンプレート）を使用します。たとえば、マシンプロファイル入力にENI AにSG 1、ENI BにSG 2が設定されている場合、プロビジョニングされたVMもENI AにSG 1、ENI BにSG 2が設定されます。

この機能は以下に適用されます。

- 永続カタログと非永続カタログ
- 新しいマシンカタログ
- 既存のカタログにプロビジョニングされた新しいVM

詳細については、「PowerShell を使用してマシンプロファイルベースのマシンカタログを作成する」を参照してください。

ニュータニックス AHV プリズムセントラル

Nutanix AHV Prism Central接続でMCS PowerShellコマンドを使用したCitrix Provisioningカタログ作成のサポート

Nutanix AHV Prism Centralホスト接続でMCS PowerShellコマンドを使用して、Citrix Provisioningカタログを作成できるようになりました。

この実装により、次の利点が得られます。

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

詳細については、「PowerShellを使用してNutanix AHV Prism Centralでカタログを作成する」を参照してください。

マシンカタログをCitrix管理のNutanix AHV Prism Centralホスト接続に移行する

この機能により、既存のNutanix AHV (Prism Element用) およびNutanix AHV PC (NC2 on Azure用) ホスト接続から、Citrix管理のNutanix AHV Prism Centralホスト接続に、Citrixマシンカタログとその関連VMを移行できます。移行にはPowerShellコマンドを使用します。これには、問題発生時の高速ロールバックオプションや、移行後にソースリソースをクリーンアップするコマンドも含まれます。詳細については、「マシンカタログをCitrix管理のNutanix AHV Prism Centralホスト接続に移行する」を参照してください。

Nutanix AHV Prism Central環境でのイメージ管理のサポート

Nutanix AHV Prism Central仮想化環境向けのイメージ管理機能が一般提供されるようになりました。この実装により、ストレージと時間のコストが大幅に削減され、VMの展開とイメージ更新プロセスが簡素化されます。現在、この目標を達成するにはPowerShellコマンドのみを使用できます。詳細については、「Nutanix AHV Prism Centralで準備済みイメージを使用してカタログを作成する」を参照してください。

永続VMのOSディスクをリセットする

この機能により、Nutanix AHV Prism Central環境で`Reset-ProvVMDisk` PowerShellコマンドを使用して、永続VMのOSディスクをリセットできるようになりました。詳細については、永続VMのOSディスクをリセットするを参照してください。

ヴイエムウェア

VMwareでのデータディスクのプロビジョニングのサポート

データディスクを使用すると、イベントログ、セキュリティトレース、アプリケーションデータなどの永続データを保存できます。この機能により、VMwareのMCSマシンカタログのMCSによって作成された永続VMまたは非永続VMに、永続および非永続データディスクを作成して割り当てることができるようになりました。

データディスクはマスターイメージからプロビジョニングする必要があります。プロビジョニングされたVMのデータディスクは、ストレージポリシー、サイズなどのプロパティをマスターイメージから継承します。マシンプロファイルベースのカタログの場合、オプションでVMテンプレートのデータディスクを使用してプロパティを派生させることができます。VMテンプレートにデータディスクがない場合は、ストレージのデフォルトポリシーが使用されます。詳細については、MCSで作成されたVMにデータディスクをプロビジョニングするを参照してください。

レッドハット オープンシフト

vCPUの計算とCPUトポロジの制約

OpenShift仮想マシンのCPU構成を更新すると、プラグインは要求されたvCPU数とマシンプロファイルからの既存のCPUトポロジ（コアとスレッド）に基づいてソケット数を計算します。

使用される式は次のとおりです。

```
sockets = requestedVCpuCount / (cores × threads)
```

詳細については、vCPUの計算とCPUトポロジの制約を参照してください。

OpenShift MCSでのvGPUサポート

OpenShift MCSは現在、パススルー動作を介したvGPU構成をサポートしています。マスターVMまたはマシンプロファイルで定義されたvGPU設定は、MCSカタログを介してプロビジョニングされたVMに読み取られ、適用されます。現在、カタログ作成中にvGPUパラメーターを変更することはできません。vGPU構成はソース構成から直接継承され、構成されたとおりにプロビジョニングされたVMに適用されます。

Citrix Virtual Desktop Assistantアプリケーションの機能強化

Citrix Virtual Desktop Assistantアプリケーションは、以下の新機能が追加され、機能強化されました。

- **ホーム**ページ:
  - セッションを記録する: アクティブな仮想デスクトップセッションをMP4ビデオクリップとして記録し、トラブルシューティング、コラボレーション、セッションレビューに役立てます。
  - スクリーンショットを撮る: Windows Snipping Toolが見逃したり、黒く表示されたりする可能性のある領域を含め、セッション全体をキャプチャします。
- **アプリ**ページ: アプリケーションが最適化リストにある場合、アプリケーション名の横に**最適化済み**タグが表示されます。
- **ツール**ページ: Snipping Tool やセッションレコーディングなどのツールが表示されます。
- サウンドページ: Citrix Virtual Desktop Assistant がマイクを使用できない場合、警告メッセージが表示されます。
- **AOTログ**: セッションのログをエクスポートし、管理者とログを共有します。

- **バージョン情報**ページ: サポートファイルをダウンロードし、Citrix Virtual Desktop Assistant のログとともにフィードバックを送信するオプション。

プレビュー機能

Oracle C3 プラグインによる Oracle Compute Cloud@Customer (C3) インスタンスの電源管理 (プレビュー)

Oracle Compute Cloud@Customer (C3) は、Oracle Cloud Infrastructure (OCI) サービスをオンプレミス環境に拡張します。このハイブリッド展開は、データをローカルに保持しつつ、OCI の ID およびガバナンスサービスを利用してアクセス管理を合理化することで、データ主権と規制要件を満たすように設計されています。

Oracle C3 プラグインを使用すると、Oracle C3 環境へのホスティング接続を作成し、カタログを作成し、Web Studio を使用してカタログ内のインスタンスの電源を管理できます。または、PowerShell コマンドを使用することもできます。詳細については、以下を参照してください。

- オラクル コンピュート クラウド・アット・カスタマー (C3) 環境
- オラクル コンピュート クラウド・アット・カスタマー (C3) への接続
- Compute Cloud@Customer (C3) カタログの作成
- Compute Cloud@Customer (C3) VM の電源管理

Amulet Hotkey CoreStation プラグインのサポート (プレビュー)

この機能により、Citrix は Amulet Hotkey CoreStation プラグインを介して Amulet Hotkey CoreStation ワークロードを管理します。このプラグインを使用すると、Amulet Hotkey CoreStation エンクロージャへのホスティング接続を作成し、カタログを作成し、PowerShell コマンドを使用してカタログ内のマシンの電源を管理できます。

詳細については、以下を参照してください。

- Amulet Hotkey CoreStation 仮想化環境
- アミュレット ホットキー コアステーションへの接続
- Amulet Hotkey CoreStation VMの電源管理
- Amulet Hotkey CoreStation マシンカタログの作成

プロファイル管理

新機能については、別のドキュメントの「新機能」を参照してください。

リナックス VDA

新機能については、別のドキュメントの「新機能」を参照してください。

セッション録画

新機能については、別のドキュメントの「新機能」を参照してください。

シトリックス プロビジョニング™

新機能については、別のドキュメントの 新機能 の記事を参照してください。

macOS 用 Citrix バーチャル デリバリー エージェント

新機能については、別のドキュメントの 新機能 の記事を参照してください。

ワークスペース環境管理™

新機能については、別のドキュメントの「新機能」を参照してください。

フェデレーション認証サービス

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

修正された問題

Citrix Virtual Apps and Desktops™ 7 2603 には、以下の修正された問題が含まれています。

> **注:**
>
> Citrix Virtual Apps and Desktops™ の以前のバージョンにおける問題の修正は、本リリースおよびそれ以降のリリースに含まれています。

全般

HDX

マルチメディア

- ブラウザコンテンツリダイレクトのオーバーレイがアクティブな場合、それが誤って最上位のウィンドウとして残り、Windowsタスクバーで他のアプリケーションのプレビューにカーソルを合わせても、それらが前面に表示されないことがあります。

ウェブスタジオ

- Web Studioを2511より*前の*バージョンから2511にアップグレードした後、以前のバージョンがデフォルトのディレクトリではなく*非デフォルト*のディレクトリにインストールされていた場合、Web Studioが開かなくなります。`C:\Program Files\Citrix`.

  回避策として、`StudioConfig.exe` を使用して、Web Studioマニフェストファイルで Delivery Controllerのアドレスを手動で構成します。

- Web StudioからVDAのヘルスチェックを実行すると、ログオン期間チェックのレポートに次の警告が表示されます。



マシン作成サービス

- Red Hat OpenShift環境で、マスターイメージがドメインに参加している場合、カタログ作成に使用された後、ドメイン信頼を失う可能性があります。
- Nutanix AHV Prism Central ホスト接続を使用して MCS カタログに大量の VM を追加すると、`OutOfMemory` エラーで失敗する場合があります。これを回避するには、一度に作成する VM の数を減らしてください。一度に追加する VM は最大 10 台にすることをお勧めします。

- 既存のVDAをバージョン2511にアップグレードした後、`MachineGuid` はマシン固有のユニークな値に変更されます。ライセンスのために `MachineGuid` に依存するソフトウェアは、再登録が必要になる場合があります。
- 環境がマスターイメージから継承されたワイルドカード証明書に依存している場合、VDAバージョン2511のTLS暗号化が機能しなくなります。

  シングルセッションマシンの回避策として、マシンごとの証明書を使用できます。詳細については、Enable TLS / DTLS on VDAs を参照してください。

プロファイル管理

- Profile Management 2603 documentation には、本リリースでの更新に関する具体的な情報が記載されています。

リナックス ブイディーエー

- Linux VDA 2603 documentation には、本リリースでの更新に関する具体的な情報が記載されています。

セッション録画

- Session Recording 2603 documentation には、本リリースでの更新に関する具体的な情報が記載されています。

ワークスペース環境管理™

- (/ja-jp/workspace-environment-management/current-release/fixed-issues.html)は、このリリースでの更新に関する具体的な情報を提供します。

シトリックス プロビジョニング™

- (/ja-jp/provisioning/current-release/whats-new/fixed-issues.html)は、このリリースでの更新に関する具体的な情報を提供します。

フェデレーション認証サービス

- (/ja-jp/federated-authentication-service/current-release/whats-new/fixed-issues)は、このリリースでの更新に関する具体的な情報を提供します。

既知の問題

Citrix Virtual Apps and Desktops™ 7 2603 には、以下の既知の問題が含まれています。

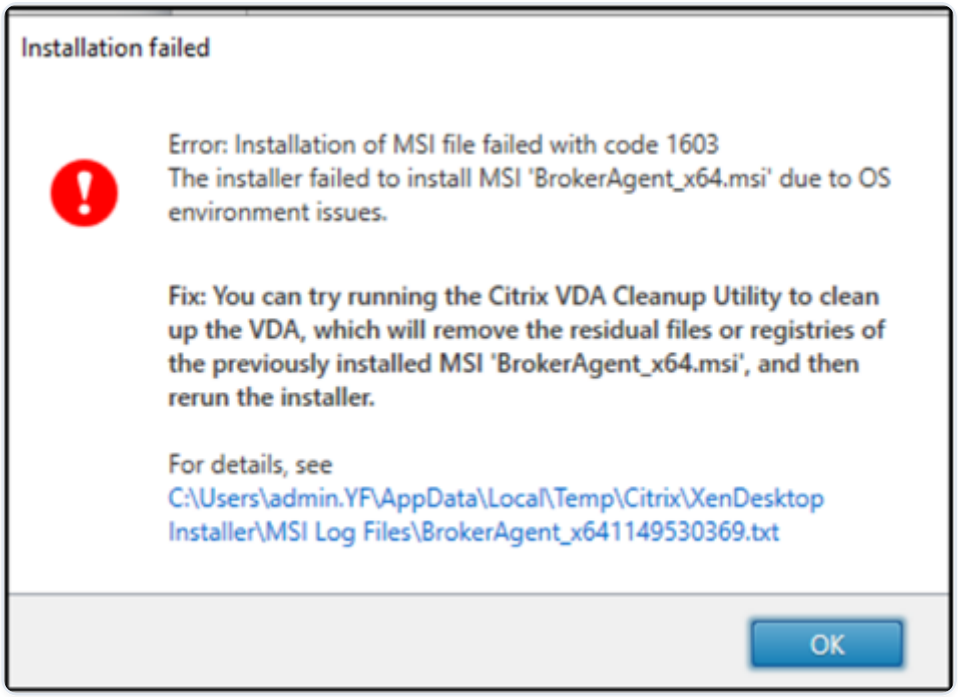
注

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

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

全般

- Windows 10 (22H2) および Windows Server 2022 プラットフォームでの Citrix VDA インストール中に、次のエラーが発生する可能性があります。



また、ブローカーエージェントの msi ログに、次のエラーメッセージが表示される場合があります。

```
MSI (s) (04:D8) [09:46:08:426]: Note: 1: 1722 2: CA_RunInstallAgent 3:
C:\Program Files\Citrix\Virtual Desktop Agent\BrokerAgent.exe 4:
-install
```

```
CustomAction CA_RunInstallAgent returned actual error code 1701 (note
this may not be 100% accurate if translation happened inside sandbox)

MSI (s) (04:D8) [09:46:08:427]: Product: Citrix Virtual Desktop Agent -
x64 -- Error 1722. There is a problem with this Windows Installer
package. A program run as part of the setup did not finish as expected.
Contact your support personnel or package vendor. Action
CA_RunInstallAgent, location: C:\Program Files\Citrix\Virtual Desktop
Agent\BrokerAgent.exe, command: -install
```

この問題を解決するには、インストーラーを閉じ、Windows パフォーマンスカウンターを再構築し、マシンを再起動して、再度インストールを実行します。詳細については、Microsoft ドキュメント「Manually rebuild performance counters for Windows Server 2008 64 bit or Windows Server 2008 R2 systems」を参照してください。

- アプリバーを起動してから、Windows 向け Citrix Workspace™ アプリで接続センターメニューを開くと、アプリバーがホストサーバーの下に表示されません。
- Windows Server 2022、Windows 10 Enterprise multi-session、および Windows 11 Enterprise multi-session を実行しているセッションホストでは、マルチセッション VDA の **セッション制限** 設定が拒否されます。
- Microsoft は、モダン印刷ダイアログを使用する際に印刷ジョブ間で印刷設定が保持されない問題があることを確認しており、現在その解決に取り組んでいます。現在の予測では、2025 年上半期に解決される見込みです。モダン印刷ダイアログは、Windows 11 や Windows Server 2025 などの新しい OS バージョンでデフォルトで有効になっています。OS をレガシー印刷ダイアログを使用するように構成するには、次の操作を行います。

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

- RDP 経由でシングルセッション VDA に再接続しても、クライアントプリンターはクリーンアップされません。

シングルセッションマシンでは、ユーザーが RDP を使用して同じマシンに再接続しても、以前の ICA セッションからリダイレクトされたクライアントプリンターは削除されません。その結果、古いクライアントプリンターはセッション内に表示されたままになりますが、機能しなくなります。これはマルチセッション VDA には影響しません。

- Citrix Virtual Apps and Desktopsセッション中に、オーディオ再生をサポートするクライアントモニターの電源が入れ直された場合（オフにしてからオンにした場合）、VDAのサウンドコントロールパネル（mmsys.cpl）内のモニターのオーディオ再生デバイスの名前が、正しい特定の名前から「Citrix HDX Audio」に変更されます。これは断続的な問題です。回避策として、VDAのサウンドコントロールパネル（mmsys.cpl）ウィンドウを閉じてから再起動します。
- Windows Server 2019 Virtual Delivery Agent (VDA) で公開されている特定のアプリケーション内から新しいプリンターを追加しようとすると、プリンターが一覧表示または追加されないエラーが発生します。具体的には、`rundll32.exe` にアクセスできないことを示すエラーメッセージが表示されます。

  回避策として、アプリケーションにすでに表示されているプリンターを使用するか、現在のセッションで利用できるようにプリンターを追加します。
- セッションがアクティブなときにクライアントマシンでデバイス名が変更されても、新しい名前はセッション設定にすぐに反映されません。この動作は、再生デバイスと録音デバイスの両方に影響します。

  回避策として、更新されたデバイス名を表示するには、セッションから切断してから再接続する必要があります。または、セッションからログアウトして再度ログインすることでも、この問題は解決されます。
- Browser Content Redirection (BCR) 用に構成されたタブを含む複数のChromeブラウザタブが、あるChromeウィンドウから別のChromeウィンドウに同時にドラッグアンドドロップされると、リダイレクトされたコンテンツが予期しない動作を示す可能性があります。
- ビデオコンテンツを含むタブを新しいウィンドウに移動すると、再生が停止したり、ビデオが表示されなくなったりする場合があります。
- Browser Profile SharingでBrowser Content redirectionを使用する場合、複数のプロファイルでのSSO永続性はサポートされていません。
- Windows 11 には、デスクトップ上でウィンドウをスナップする新しい UI 機能があります。ユーザーがウィンドウをドラッグしている間、デスクトップの上部に特別なツールバーが表示されます。そのため、マルチメディアオーバーレイのクリッピングロジックが上部/中央領域を切り取ってしまいますが、これはおそらくこの機能のための新しい非表示/透明なウィンドウが原因です。

  回避策については、以下を参照してください。

  - ウィンドウのスナップセクション。
  - 「ウィンドウのスナップ」機能を無効にする方法

- **Citrix VDA が既にインストールされているマシンでインプレース Windows アップグレード後に印刷が失敗する可能性がある** インプレース Windows アップグレード後、Citrix 印刷プロバイダーが呼び出されなくなり、印刷の失敗につながる可能性があります。この問題は、Windows アップグレードプロセスが印刷プロバイダーの実行順序をリセットし、Citrix 登録済みプロバイダーを保持しないために発生します。Microsoft は、これが Windows の動作であり、アップグレード中に実行順序のプロバイダー登録を現在保持しないことを確認しています。

回避策は、適切なレジストリの場所にプリントプロバイダーを再度追加することです。

```
1.  Open the Registry Editor.

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

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

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

1.  Reboot the VDA.
```

- ストレージ最適化のために MCSIO ライトキャッシュを使用するカタログでは、VDA のインストールおよびアップグレードの一部として Citrix MCS I/O ドライバーを必ずインストールしてください。詳細については、「ハイパーバイザーで共有されるストレージ」および「一時データのキャッシュの構成」を参照してください。VDA に MCS I/O ドライバーがない場合、カタログの更新時に問題が発生する可能性があります。
- Citrix ツールバーを使用してロックされた Windows セッションからサインアウトしようとすると、操作が失敗します。この問題は、Linux 用 Citrix Workspace アプリ (CWA) と Windows 用 CWA の両方で発生します。

回避策として、切断またはサインアウトを試みる前に、Windows セッションがロック解除されていることを確認してください。セッションがロック解除されていれば、切断機能とサインアウト機能は正しく動作します。

オーディオ

- ヘッドセットなどのオーディオデバイスが USB リダイレクトを使用して Windows Server Virtual Delivery Agent (VDA) (例: Windows Server 2019 または 2022) に汎用的にリダイレクトされ、同じ VDA で複数のユーザーセッションが同時にアクティブになっている場合、タスクバーの右下隅にある音量アイコンをクリックして設定を調整すると、Windows `ShellExperienceHost.exe` プロセスが予期せずクラッシュする可能性があります。この問題は主に、オーディオデバイスがアクティブにリダイレクトされていないセッションで発生しますが、同じ VDA 上の別のセッションが汎用 USB オーディオリダイレクトを使用している場合に発生します。

  回避策として、タスクマネージャーを介して、影響を受けるセッションで Windows Explorer プロセス (explorer.exe) を再起動します。これにより、ボリュームアイコンがクラッシュせずに機能するようになる可能性があります。

Citrix Always On トレース

Citrix GatewayがStoreFront 2603とともに使用される場合、Citrix Workspaceアプリ (CWA) のログはAOTログサーバーに転送されません。その結果、この構成を使用する展開では、トラブルシューティングのためにCWAログを利用できません。

この問題は、StoreFront 2603とともにCitrix Gatewayを使用する展開のみに影響します。Virtual Delivery Agent (VDA) などの他のAOTログソースは、引き続きログを正常にアップロードします。回避策として、以下のいずれかのStoreFrontバージョンを使用してください。

- StoreFront 2507 CU1
- StoreFront 2511

これらのバージョンは、Citrix Gatewayとともに展開された場合、CWAログをAOTログサーバーに正しく転送することをサポートします。

> **注:**
>
> この問題は、ユーザーがCitrix GatewayなしでStoreFrontに直接接続する展開には影響しません。

マシン作成サービス™

- Nutanix AHV Prism Central接続を介して、MCS非永続マシンカタログ用のvTPM対応マスターイメージを更新すると、VMの再作成がトリガーされ、DNS予約が無効になる可能性があり、ライセンスにMACアドレスを利用するソフトウェアの再登録が必要になる場合があります。
- Accelerated Networkingが有効になっている複数のネットワークインターフェイス (NIC) を持つマシンプロファイルを使用する場合、選択したVMサイズがすべてのNICでAccelerated Networkingをサポートしていることを確認してください。一部のAzure VMサイズ (例: Standard_D2ads_v5) は、Accelerated Networkingを単一のNICに制限します。マシンプロファイルがVMサイズで許可されているよりも多くのNICでAccelerated Networkingを有効にしている場合、マシンはエラー `VmSizeRestrictedToSingleNicWithAcceleratedNetworkingEnable` で起動に失敗します。これを解決するには、複数のNICでAccelerated Networkingをサポートするサイズを選択するか、マシンプロファイルを更新して1つのNICでのみAccelerated Networkingを有効にしてください。
- Azure Connected Machineエージェントバージョン1.61以降がインストールされ、オンボードされたAzure Local VMを使用してマスターイメージを準備すると、エージェント構成ファイルの削除時にアクセス拒否が発生するため、イメージ準備プロセスでMCSのカタログ作成が失敗します。回避策として、マスターイメージの作成中に次の手順を実行します。`C:\ProgramData\AzureConnectedMachineAgent\Config\agentconfig.json` に移動し、ファイルを右クリックして **プロパティ** を選択し、**読み取り専用** 属性のチェックボックスをオフにします。
- Nutanix AHV Prism Central ホスト接続を使用して MCS カタログに大量の VM を追加すると、`OutOfMemory` エラーで失敗する場合があります。これを回避するには、一度に作成する VM の数を減らしてください。一度に追加する VM は最大 10 台にすることをお勧めします。
- 既存のVDAをバージョン2511にアップグレードした後、`MachineGuid` はマシン固有のユニークな値に変更されます。ライセンスのために `MachineGuid` に依存するソフトウェアは、再登録が必要になる場合があります。
- 環境がマスターイメージから継承されたワイルドカード証明書に依存している場合、VDAバージョン2511のTLS暗号化が機能しなくなります。

  シングルセッションマシンに対する回避策として、代わりにマシンごとの証明書を使用できます。詳細については、VDAでのTLS/DTLSの有効化 を参照してください。
- `InstanceType` を使用して作成された VM は、Red Hat OpenShift 環境ではマスターイメージとしてサポートされていません。

- Red Hat OpenShift 仮想化環境で MCS マシンカタログを作成する場合、異なるオペレーティングシステムタイプを持つマスターイメージとマシンプロファイルを使用することはできません。これは、Red Hat OpenShift が各 OS タイプを管理する方法によるものです。したがって、Windows VM をマスターイメージとして使用し、非 Windows (例: Linux) VM をマシンプロファイルとして使用すること、またはその逆はサポートされていません。
- AWSでホストされているVMware環境では、マスターイメージでvTPMが有効になっている場合、MCSマシンカタログの作成が失敗します。この問題は、すべてのCitrix Virtual Apps and Desktopsバージョンに影響し、VMware環境の問題が原因です。サポートについては、VMwareサポートにお問い合わせください。

プロファイル管理

- Profile Management 2603のドキュメント には、このリリースでの更新に関する具体的な情報が記載されています。

macOS 用 Citrix バーチャル デリバリー エージェント

- macOS用Citrix Virtual Delivery Agent 2603のドキュメント

リナックス ブイディーエー

- Linux VDA 2603のドキュメント には、このリリースでの更新に関する具体的な情報が記載されています。

セッション録画

- Session Recording 2603のドキュメント には、このリリースでの更新に関する具体的な情報が記載されています。

ワークスペース環境管理™

- Workspace Environment Management 2603 documentation は、このリリースにおける更新に関する詳細情報を提供します。

シトリックス プロビジョニング™

- Citrix Provisioning 2603 documentation は、このリリースにおける更新に関する詳細情報を提供します。

フェデレーション認証サービス

- Federated Authentication Service 2603 documentation は、このリリースにおける更新に関する詳細情報を提供します。

廃止予定と削除

この記事のお知らせは、段階的に廃止されるプラットフォーム、Citrix®製品、および機能について事前にお知らせし、お客様が適切なビジネス上の意思決定を行えるようにすることを目的としています。Citrixは、お客様の使用状況とフィードバックを監視して、それらがいつ廃止されるかを決定します。お知らせは、その後のリリースで変更される可能性があり、すべての非推奨の機能や機能性を含まない場合があります。

製品ライフサイクルサポートの詳細については、製品ライフサイクルサポートポリシーの記事を参照してください。Long Term Service Release (LTSR) サービスオプションについては、`<https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX205549>`を参照してください。

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

非推奨

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

項目	非推奨が発表されたバージョン	代替
セキュア プライベート アクセスとウェブ スタジオの統合	2603	
セキュア プライベート アクセスとディレクターの統合	2603	

項目	非推奨が発表されたバージョン	代替
デリバリーグループごとのライセンス上書き（複数タイプライセンス）	2603	Citrix Virtual Apps and Desktopsは、サイトレベルのライセンス設定のみを使用します。デリバリーグループの上書きは無視され、デリバリーグループの作成および編集ウィザードのライセンス割り当てステップは削除されます。詳細については、複数タイプライセンスを参照してください。
App-Vフルインフラストラクチャ用のStudio UIオプション	2603	(/ja-jp/citrix-virtual-apps-desktops/current-release/manage-deployment/applications-manage/app-packages.html#migrate-from-app-v-full-infrastructure-to-single-admin-workflow)
ゼロレイテンシーテキスト（ローカルテキストエコーとも呼ばれる）	2603	
Audio over UDP のサポート (https://docs.citrix.com/ja-jp/citrix-virtual-apps-desktops/multimedia/audio#audio-over-udp-real-time-	2511	アダプティブオーディオ(https://docs.citrix.com/ja-jp/citrix-virtual-apps-desktops/multimedia/

項目	非推奨が発表されたバージョン	代替
transport-and-audio-udp-port-range)		audio#adaptive-audio)を EDT ロス許容モード (オーディオ用)(https://docs.citrix.com/ja-jp/citrix-virtual-apps-desktops/multimedia/audio#loss-tolerant-mode-for-audio)と併用します。以下の最小バージョンが必要です。 仮想デリバリーエージェント • ウィンドウズ 2308 • リナックス 2411 • Mac 2411 Citrix Workspace アプリ • ウィンドウズ 2309 • リナックス 2402 • Mac 2402
オーディオ品質 (https://docs.citrix.com/ja-jp/citrix-virtual-apps-	2511	アダプティブオーディオ(https://docs.citrix.com/ja-

項目	非推奨が発表されたバージョン	代替
desktops/multimedia/audio#audio-quality) 設定 (およびレガシーオーディオコーデックのサポート)		jp/citrix-virtual-apps-desktops/multimedia/audio#adaptive-audio)を使用します。以下の最小バージョンが必要です。 仮想デリバリーエージェント • ウィンドウズ 2109 • リナックス 2112 • Mac 2411 Citrix Workspace アプリ • ウィンドウズ 2109 • リナックス 2109 • Mac 2109
ローカルアプリアクセス (LAA)	2511	LAAに直接的な代替手段はありません。代わりに、エンドポイントからVDAにローカルにインストールされたアプリケーションをインストールすることをお勧めします。LAAは、2402 LTSRまたは2507 LTSRのメン

項目	非推奨が発表されたバージョン	代替
		テナンスが終了するまでサポートされます。この非推奨化に伴い、Microsoft Internet ExplorerおよびFirefox用のローカルアプリアクセス拡張機能も非推奨となります。
HTML5マルチメディアリダイレクト	2511	ブラウザコンテンツリダイレクト
ファイルベースのライセンス	2507	License Activation Service (LAS)は、Citrix製品スイート全体での製品アクティベーションのための次世代テクノロジーです。ファイルベースのライセンスを使用しているお客様は、April 15, 2026までに互換性のあるリリースにアップグレードし、このテクノロジー移行を実行する必要があります。April 15, 2026以降、LASがCitrixオンプレミスコンポーネントをアクティベートおよびライセンス供与する唯一の方法となります。
`Get-BrokerMachine`のサポート	2507	`Get-BrokerMachineV2`を使用してください。

項目	非推奨が発表されたバージョン	代替
ユニバーサル印刷最適化のデフォルトポリシー設定の「画像圧縮」セクションにある**高負荷圧縮を有効にする**オプションのサポート	2507	
「`Repair-AcctADAccount` PowerShellコマンド」のサポート	2503	次のコマンドを使用します • `Repair-AcctIdentity`: IDアカウントの現在の状態を変更せずに修復するため。これにより、既存のプロビジョニング済みVMの既存の使用中IDアカウントを修復できます。例えば、Microsoft Entraハイブリッド参加済みIDアカウントの `repair userCertificate` 属性。AD参加済みIDアカウントの `Repair identity info`（マシンパス

項目	非推奨が発表されたバージョン	代替	
		ワード/信頼キーペアを含む）。 • `Reset-AcctIdentity`：IDアカウントを初期状態にリセットするため（例えば、破損状態から利用可能状態へ）。これにより、破損したIDアカウントをプールに戻し、利用可能なIDアカウントとして使用できます。	
3D HDXグラフィックポリシーの最適化	2411	圧縮にビデオコーデックを使用し、「画面全体」に設定します。`<https://docs.citrix.com/ja-jp/citrix-virtual-apps-desktops/policies/reference/ica-policy-settings/graphics-policy-settings.html#use-video-codec-for-compression>`を参照してください。	

項目	非推奨が発表されたバージョン	代替
NVIDIA GPUハードウェアエンコーディング (NVENC) (vGPU 15以前、およびドライバーバージョン529.19以前の場合)。	2411	現在サポートされているNVIDIAドライバーを使用してください: vGPU 16以降、およびドライバーバージョン536.22以降。詳細については、NVIDIAがサポートするvGPUおよびドライバーバージョンに関する `<https://docs.nvidia.com/vgpu/index.html#driver-versions>` を参照してください。
以下の `-AcctADAccount` PowerShellコマンドのサポート • New-AcctADAccount • Add-AcctADAccount • Update-AcctADAccount コマンドレット • Remove-AcctADAccount コマンド	2411	-AcctIdentity PowerShellコマンドを使用 • New-AcctIdentity • Add-AcctIdentity • Update-AcctIdentity コマンドレット • Remove-AcctIdentity コマンド • Unlock-AcctIdentity (IDのロック解除) • Get-AcctIdentity

項目	非推奨が発表されたバージョン	代替
• Unlock-AcctADAccount (ADアカウントのロック解除) • Get-AcctADAccount		
「`-ResetIdentityInfo` PowerShellコマンド」のサポート	2411	IDディスクを再作成するには、`-Recreate`を使用します。詳細については、「アクティブなコンピューターアカウントのID情報を修復する」を参照してください。
MMCベースのStudio	2411	MMC ベースの Studio は 2511 で削除されました。代わりに Web Studio を使用してください。
複数モニターフック	2407	-
ドメインパススルー認証	2407	シングルサインオン用の拡張ドメインパススルーを使用してください。
ランデブー V1	2402	Rendezvous V2を使用してください。
セキュア ICA®	2402	Secure HDXを使用してください。
Windows Server 2016でのVDAサポート	2402	最新のWindows Serverバージョンに

項目	非推奨が発表されたバージョン	代替
		アップグレードしてください。
Windows Server 2016でのDelivery Controller™、Web Studio、Citrix Director、Citrix License Server、Citrix StoreFront、シングルセッションOS用Server VDI、マルチセッションOS用VDA、Active Directoryフォレストおよびドメイン、Universal Print Serverのサポート	2402	Windows Server の最新バージョンにアップグレードしてください。
サイト構成、構成ログ、および監視データベースに対するMicrosoft SQL Server バージョン 2016 および 2017 のサポート	2402	Microsoft SQL Server の最新バージョンにアップグレードしてください。
オンデマンドプロビジョニング機能より前に作成されたAzureカタログ（「レガシー」カタログ）のサポート	2402	Azure レガシーカタログVMを再作成します。カタログはオンデマンドでプロビジョニングされるため、ストレージコストを節約できます。
ターゲット最小フレームレートポリシー	2311	**グラフィックステータスインジケーター**を使用して、ターゲット最小フレーム

項目	非推奨が発表されたバージョン	代替
		レートを変更します。
カタログが作成されたリージョンとは異なるリージョンでのマスターイメージの使用のサポート	2311	Azure Compute Gallery を使用して、マスターイメージを目的のリージョンにレプリケートします。
HDX™ グラフィック表示メモリ制限設定	2311	クライアントの表示レイアウトが完全に収まるように、必要な最小メモリ量が割り当てられます。
HDX Graphicsでのプログレッシブモードのサポート	2311	Thinwireを使用してください。プログレッシブモードを参照してください。
Internet Explorer 11でのブラウザーコンテンツリダイレクトのサポート	2311	Google Chromeベースのブラウザーコンテンツリダイレクトを使用してください。
BrokerでのSQL Server 2016のサポート	2308	最新バージョンを使用してください。詳しくは、システム要件を参照してください。
DirectorでのXenApp 5.xのサポート	2308	---
DirectorでのXenApp 6.xのサポート	2308	---

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

項目	非推奨が発表されたバージョン	代替
		`indow` を使用します。
`Cancel-ProvVMUpdate` PowerShellコマンド	2305	`Clear-ProvVMUpdateTimeWindow` を使用します。
`New-ProvScheme` コマンドで使用される `DedicatedTenancy` パラメーター	2303	`TenancyType` パラメーターを使用します。
ライセンスサーバーVPX	2206	---
ホストからクライアントへの (URL) リダイレクト	2203	双方向コンテンツリダイレクト。
クラウドおよびオンプレミス環境で使用される4つのAWS固有のコマンド（`Revoke-HypSecurityGroupIngress`、`Revoke-HypSecurityGroupEgress`、`Grant-Hypsecuritygroupegress`、および `Grant-HypSecurityGroupIngress`）のサポート。	2203	---

項目	非推奨が発表されたバージョン	代替
VDAメタインストーラーからのCitrix Files for WindowsおよびCitrix Files for Outlook。	2203	スタンドアロンインストーラーを使用します。
VDAメタインストーラーからのWEMエージェントコンポーネント。	2203	---
XenAppおよびXenDesktop、Provisioning Services、StoreFront用のCitrix SCOM管理パック。監視できる製品バージョンについては、「Citrix SCOM管理パックのドキュメント」を参照してください。	1912	展開の監視と管理にはDirectorを使用してください。SCOMのEOLと代替策の詳細については、https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX266943を参照してください。
モビリティ SDK / モバイル SDK (旧シトリックスラボ製)	7.16	モバイルエクスペリエンスポリシー設定、およびホスト型デスクトップ/アプリのネイティブエクスペリエンスに置き換えられました。

削除された機能

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

項目	廃止が発表されたバージョン	削除されたバージョン	代替
サーバーVDAでのCitrix Backup and Restoreのサポートを削除	2603	2603	サーバーVDAをインストールまたはアップグレードする前に手動でバックアップしてください
Remote PC Access 用のSCCM統合Wake on LANオプション。	2012	2511	スタンドアロンのWake on LAN機能を使用します。
System Center Configuration Manager に対応する Citrix Connector 3.1 のサポート	2311	2507	イメージまたはアプリケーションの更新を手動で行います。
AWS ボリュームワーカーのサポートを削除しました	2311	2503	ディスクの直接アップロードとダウンロードを使用します。ディスクの直接アップロードとダウンロードを参照してください。
SQL Server 2016 および 2017 のサポート	2402 および 2308	2411	SQL Server 2019 および 2022 を使用
MCS I/Oライトバックキャッシュを、ディスクキャッシュの	2402	2411	ライトバックキャッシュが有効なマシンを作成するときは、

項目	廃止が発表されたバージョン	削除されたバージョン	代替
みを含み、メモリキャッシュを含まないように構成するサポート			**メモリキャッシュサイズ (MB)** オプションを選択し、ゼロ以外のサイズを指定します。
Citrix Studio での PVS インポートウィザードのサポート	1912 LTSR	2311	以下のいずれかの方法で Citrix Provisioning™ マシンをプロビジョニングします • Citrix Provisioning Console を使用してマシンをプロビジョニングし、Citrix Provisioningデバイスエクスポートウィザードを使用してCitrix Virtual Apps and Desktopsにエクスポートします。詳細については、「デ

項目	廃止が発表されたバージョン	削除されたバージョン	代替	
			バイスエクスポートウィザード」を参照してください。 • Web Studioを使用してCitrix Provisioningカタログを作成します。詳細については、「Citrix StudioでCitrix Provisioningカタログを作成する」を参照してください。	
Windows 1912用 Citrix Workspace アプリ	---	2402	最新バージョンを使用してください。	
HDX Graphics FullScreen + テキスト最適化	2311	2311		
HDX 3D ProでのNVIDIA Frame Buffer	2308	2311	Desktop Duplication API	

項目	廃止が発表されたバージョン	削除されたバージョン	代替
Capture (NVFBC) のサポート			(DDAPI) を使用してください。
ポリシー設定「インボックスプリンタードライバーの自動インストール」に対する VDA サポート。	7.16	2311	なし。このポリシー設定は、以前の OS (Windows 7、Windows Server 2012 R2 以前) 上の VDA でのみサポートされます。
NVIDIA GPU ハードウェアエンコード (NVENC) (vGPU 11以前、およびドライバーバージョン466.77以前)。	2305	2305	現在サポートされているNVIDIAドライバーを使用してください: vGPU 13以降、バージョン471.41以降。
VDAメタインストーラーからのCitrix Supportability Tools (SupportabilityTool_x64 .msi)。	---	2212	---
Citrix License Administration Console (Windows License Server 11.16.3 build 30000に最後に含まれ、Windows	2003	2006	Citrix Licensing Managerを使用してください。

項目	廃止が発表されたバージョン	削除されたバージョン	代替
License Server v11.16.6 build 31000で削除されました)。			
Windows 10 バージョン 1709以前での Citrix Indirect Display Driver (IDD) グラフィックアダプターのサポート。	2003	2003	Citrix Virtual Apps and Desktops™ 7 1912 LTSR VDA を使用します。
GRID 9 以前のディスプレイドライバーを使用した NVIDIA GPU (NVENC) によるハードウェアエンコード。	2003	2003	Citrix Virtual Apps and Desktops 7 2003以降のVDAでGRID 10ディスプレイドライバーを使用するか、Citrix Virtual Apps and Desktops 7 1912 LTSR VDAを使用します。
セルフサービスパスワードリセット (SSPR) 機能。	2003	2006	---
VDA およびコアサーバーコンポーネントにおける Microsoft .NET Framework バージョン 4.8	1912	2003	.NET Frameworkバージョン4.8にアップグレードします。

項目	廃止が発表されたバージョン	削除されたバージョン	代替
より前のバージョンへのサポート。Delivery Controller、Studio、Director を含む。			
Windows Server 2012 R2 で動作する VDA。	1912	2003	サポートされているオペレーティングシステムにVDAをインストールします。
Citrix Virtual Apps and Desktops Premium edition の AppDNA® アプリケーション移行コンポーネント。	1909	2003	---
32ビット (x86) マシンへの Studioのインストール。	1909	2003	サポートされているx64オペレーティングシステムにインストールします。
シームレスアプリケーションでのExcelフックのサポート。これは、Microsoft Excel 2010の各ワークブックに個別のタスクバーアイコンを	1909	1909	---

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

項目	廃止が発表されたバージョン	削除されたバージョン	代替
			き続きサポートされています。
Citrix Virtual Apps and DesktopsインストールメディアからのCitrix Smart Tools Agentの削除。	1903	1906	---
Red Hat Enterprise Linux/CentOS 7.5でのLinux VDAのサポート。	1903	1903	Red Hat Enterprise Linux の以降のバージョンに Linux VDA をインストールします。
Citrix Virtual Apps and Desktops（旧XenAppおよびXenDesktop）とCitrix Receiver、およびWorkspace Hub間のTLS 1.0およびTLS 1.1プロトコルに対するStoreFrontのサポート。	7.17	2203	Citrix Receiver を TLS 1.2 プロトコルをサポートする Citrix Workspace アプリにアップグレードしてください。Citrix Workspace アプリの詳細については、https://docs.citrix.com/ja-jp/citrix-workspace-app を参照してください。
ポリシー設定「インボックスプリンタードライバーの自動インストール」に	7.16	2311	なし。このポリシー設定は、以前の OS (Windows 7、Windows

項目	廃止が発表されたバージョン	削除されたバージョン	代替
対する VDA サポート。			Server 2012 R2 以前) 上の VDA でのみサポートされます。
Framehawk ディスプレイリモートテクノロジーのサポート	1811	1903	adaptive transport を有効にして Thinwire を使用してください。
すべての Citrix Virtual Apps and Desktops (および XenApp and XenDesktop) バージョンにおける Citrix Smart Scale のサポート。この機能は、31 May 2019 にサポート終了となります。	1808	1906	電源管理機能の向上のため、Citrix Cloud 上の Virtual Apps and Desktops Service の使用を検討してください。
Citrix StoreFront、Citrix VDA、Citrix Studio、Citrix Director、および Citrix Delivery Controller による Microsoft .NET Framework バージョン 4.5.1、4.5.2、4.6、4.6.1、	7.18	1808	.NET Framework バージョン 4.7.1 以降にアップグレードします。(インストーラーは、.NET Framework 4.7.1 がまだインストールされていない場合、自動的にインス

項目	廃止が発表されたバージョン	削除されたバージョン	代替
4.6.2、および 4.7 のサポート。			トールします。)
Red Hat Enterprise Linux 7.3 上の Linux VDA のサポート。	7.18	1808	Red Hat Enterprise Linux の以降のバージョンに Linux VDA をインストールします。
SUSE Linux Enterprise Server 11 Service Pack 4 上での Linux VDA のサポート。	7.16	7.16	サポートされている SUSE バージョンに Linux VDA をインストールします。
VDA での Citrix WDDM ドライバーのサポート	7.16	7.16	Citrix WDDMドライバーは、VDAとともにインストールされなくなりました。
Windows 10 バージョン1511（Threshold 2）およびそれ以前のWindows シングルセッションOSリリース（Windows 8.xおよびWindows 7を含む）上の VDA（`<https://`	7.15 LTSR（および7.12）	7.16	Windows 10の最小バージョン1607（Redstone 1）以降の半期チャネルにシングルセッションOS VDAをインストールします。1607 LTSBを使用している場合は、7.15 VDAをお勧めします。

項目	廃止が発表されたバージョン	削除されたバージョン	代替
`www.citrix.com/blogs/2018/01/08/the-citrix-strategy-for-windows-7-virtual-desktop-users/>`を参照）。			CTX224843を参照してください。
Windows Server 2008 R2 およびWindows Server 2012（Service Packを含む）上のVDA	7.15 LTSR（および7.12）	7.16	サポートされているオペレーティングシステムにVDAをインストールします。
デスクトップコンポジションリダイレクト (以前は DirectX Command Remoting と呼ばれていました) (DCR)	7.15 LTSR	7.16	Thinwireを使用します。
Windows Server 2012 および Windows Server 2008 R2 (Service Packを含む) 上のコアコンポーネント。含まれるもの: Delivery Controller、Studio、Director、	7.15 LTSR	7.18	サポートされているオペレーティングシステムにコンポーネントをインストールします。

項目	廃止が発表されたバージョン	削除されたバージョン	代替
StoreFront、License Server、Universal Print Server。			
Windows Server 2012 および Windows Server 2008 R2 (Service Pack を含む) 上のセルフサービスパスワードリセット (SSPR) 機能	7.15 LTSR	7.18	より新しいサポート対象のオペレーティングシステムにインストールしてください。
Windows 7、Windows 8、および Windows 8.1 (Service Pack を含む) 上の Studio	7.15 LTSR	7.18	サポートされているオペレーティングシステムに Studio をインストールします。
Flashリダイレクト	7.15 LTSR	1912	HTML5ビデオとしてビデオコンテンツを作成します。管理対象コンテンツにはHTML5ビデオリダイレクトを、公開Webサイトにはブラウザコンテンツリダイレクトを使用します。詳細については、Flashリダイレクトのサポート終了の注記を参

項目	廃止が発表されたバージョン	削除されたバージョン	代替
			照してください。
StoreFrontとのCitrix Online統合 (Goto製品)	7.14 (およびStoreFront 3.11)	StoreFront 3.12	---
VDAのインストール中に作成され、VDAマシンのローカル管理者グループに追加されたユーザーアカウントCtxAppVCOMAdminは、作成されなくなりました。基盤となる「COM」メカニズムも削除されました。	7.14	7.14	WindowsサービスCtxAppVServiceは同じ機能を実行します。これは自動的にインストールおよび構成され、ユーザーによる操作は不要です。
Windows Server 2008 32ビット版でのUniversal Print Server UpsServerコンポーネントのサポート	7.14	7.14	より新しいサポート対象のオペレーティングシステムにインストールしてください。
インターネットエクスプローラー 8 での ストアフロントおよび レシーバー・フォー・ウェブ	7.13	7.13	---

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

項目	廃止が発表されたバージョン	削除されたバージョン	代替
			Server 2012 R2またはWindows Server 2016に移行し、Thinwireを使用してください。
StoreFront 2.0、2.1、2.5、および2.5.2からのインプレースアップグレード	7.13	7.16	これらのバージョンのいずれかから、サポートされている新しいバージョンにアップグレードし、その後XenAppおよびXenDesktop 7.16にアップグレードします。
XenDesktop 5.6または5.6 FP1からのインプレースアップグレード	7.12	7.16	XenDesktop 5.6または5.6 FP1の展開を現在のXenDesktopバージョンに移行します。これを行うには、まずXenDesktop 7.6 LTSR（最新のCUを含む）にアップグレードし、その後、最新のCitrix Virtual Desktops（旧XenDesktop）リリースまたはLTSRバージョンにアップグレードします。

項目	廃止が発表されたバージョン	削除されたバージョン	代替
32ビット（x86）マシンへのDelivery Controller、Director、StoreFront、またはLicense Serverのインストール。	7.12	7.16	サポートされているx64オペレーティングシステムにインストールします。
接続リース	7.12	7.16	ローカルホストキャッシュを使用します。
Windows XPで使用されるXenDesktop 5.6。Windows XPへのVDAインストールはサポートされていません。	7.12	7.16	サポートされているオペレーティングシステムにVDAをインストールします。
CloudPlatform接続のサポート	7.12	2003	別のサポートされているハイパーバイザーまたはクラウドサービスを使用します。
Azure Classic（別名Azure Service Management）接続のサポート	7.12	2003	Citrix Cloud の Virtual Apps and Desktops Service の使用を検討してください。
AppDisks 機能 (およびそれをサポートする	7.13	2003	Citrix App Layering を使用してください。

項目	廃止が発表されたバージョン	削除されたバージョン	代替
Studio への AppDNA 統合)			
Personal vDisk 機能	7.15	2006†	Citrix App Layering ユーザーレイヤー または ユーザーパーソナライゼーションレイヤー テクノロジーを使用してください。

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

システム要件

はじめに

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

インストールを開始する前に、インストールの準備を確認してください。

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

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

グローバリゼーションについては、Knowledge Centerの記事CTX119253を参照してください。

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

ハードウェア要件

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

次の表に、コアコンポーネントの最小要件を示します。

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

デスクトップとアプリケーションを提供するVMのサイジング

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

詳細については、以下を参照してください。

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

マイクロソフト ビジュアル C++

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

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

デリバリーコントローラー

> **注:**

> **ライセンスサーバーのバージョン互換性:** ライセンスサーバーがバージョン11.17.2ビルド53100以降で実行されていることを確認してください。この前提条件を満たさない場合、Citrix Virtual Apps and Desktops (CVAD) サイトのアップグレードおよびサイト作成がブロックされます。

> サポートされているオペレーティングシステム:

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

要件:

- Microsoft .NET Framework 4.8（またはそれ以降のバージョン）がまだインストールされていない場合、自動的にインストールされます。
- Windows PowerShell 3.0、4.0、または5.0。
- Microsoft Visual C++ 2015–2022 再頒布可能パッケージ。
- Citrix Virtual Apps and Desktopsバージョン2407から2411以降にアップグレードする場合、またはバージョン2411以降を新規インストールする場合は、最初のステップとしてライセンスサーバーを最新バージョン（バージョン11.2.17ビルド53100以降）に更新してください。その後、Delivery Controllerをアップグレードします。これを怠ると、UIに警告メッセージが表示され、コマンドラインインストールが失敗します。

> **注:**

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

データベース

> **注:**

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

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

- SQL Server 2022、Express、Standard、およびEnterprise エディション。
  - 新規インストールの場合：既存のサポートされているSQL Serverインストールが検出されない場合、Controllerのインストール時に、累積更新プログラム14が適用されたSQL Server Express 2022がデフォルトでインストールされます。
- SQL Server 2019、Express、Standard、およびEnterprise エディション。
- SQL Server 2025、Express、Standard、および Enterprise エディション。

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

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

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

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

- コントローラーをインストールする際、ローカルホストキャッシュ機能で使用するために、累積更新プログラム15適用済みのMicrosoft SQL Server Express LocalDB 2022がインストールさ

れます。(このインストールは、サイトデータベース用のデフォルトのSQL Server Expressインストールとは別です。)

- コントローラーをアップグレードする際、既存のMicrosoft SQL Server Express LocalDBのバージョンは自動的にアップグレードされません。交換要件と手順については、「SQL Server Express LocalDBの交換」を参照してください。

その他のデータベース情報:

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

ウェブスタジオ

> **注:**
>
> - Web Studioは、オンプレミスのCitrix Virtual Apps and Desktops展開を構成および管理できるWebベースの管理コンソールです。ユーザーエクスペリエンスの向上を目的として設計されており、Citrix Studioよりも一般的に応答が高速です。インストール手順については、「Web Studioのインストール」を参照してください。
> - バージョン2511以降、Web Studio（Webベース）はCitrix Virtual Apps and Desktopsの唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。

> Web Studioのインストールと使用に関するサポート対象のオペレーティングシステム、ブラウザー、表示設定、およびハードウェア要件については、Web Studioの記事のシステム要件を参照してください。

シトリックス ディレクター

サポートされているオペレーティングシステム:

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

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

要件:

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

シトリックス プロファイル マネージメント:

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

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

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

Directorの表示でサポートされているブラウザー:

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

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

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

サポートされているオペレーティングシステム:

- ウィンドウズ 11
- Windows 10 (x64のみ)、現在メインストリームサポート中のすべてのバージョン。

- エディションのサポートについては、Knowledge Centerの記事CTX224843を参照してください。

要件:

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

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

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

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

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

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

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

サポートされているオペレーティングシステム:

- ウィンドウズ サーバー 2025
- Windows 11 (Citrix DaaS™でのみサポート)

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

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

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

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

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

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

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

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

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

Amazon WorkSpaces Coreマネージドインスタンスの VDA

サポートされているオペレーティングシステム:

- Windows 11シングルセッション

- Windows 10シングルセッション
- ウィンドウズ サーバー 2025
- ウィンドウズ サーバー 2022
- ウィンドウズ サーバー 2019
- ウィンドウズ サーバー 2016
- ウブントゥ サーバー 24.04 LTS
- デビアン 12

ホスト / 仮想化リソース

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

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

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

サポートされているハイパーバイザー:

- **Azure ローカル**

  詳細については、Azure Local環境を参照してください。
- **ゼノサーバー (旧称 シトリックス ハイパーバイザー™)**

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

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

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

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

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

- **Nutanix アクロポリス**

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

  詳細については、Nutanix仮想化環境を参照してください。

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

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

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

  詳細については、VMware仮想化環境を参照してください。

サポートされているパブリッククラウドホスト:

- **アマゾン ウェブ サービス (AWS)**

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

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

- **マイクロソフト アジュール リソース マネージャー**

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

- **レッドハット OpenShift**

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

- **Nutanix クラウドおよびパートナーソリューション**

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

- **VMware クラウドおよびパートナーソリューション**

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

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

- ハイブリッド権限ライセンスが必要です。ハイブリッド権限ライセンスについては、「ハイブリッド権限による移行とアップグレード (TTU)」を参照してください。ライセンスの追加については、「サイトの作成」を参照してください。
- 情報源は Citrix DaaS のドキュメントを参照しています。Citrix DaaS 製品のパブリッククラウドホストに精通している場合でも、オンプレミスバージョンとはいくつかの違いがあります。
    - Citrix DaaS への更新は、約4週間ごとに展開されます。そのため、Citrix DaaS で利用できる特定の機能がオンプレミスバージョンでは利用できない場合があります。

Active Directoryの機能レベル

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

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

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

HDX

オーディオ

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

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

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

HDX Windows Media の配信

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

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

HDX 3D Pro 機能

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

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

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

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

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

グラフィック処理ユニット (GPU):

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

ユーザーデバイス:

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

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

ユニバーサル プリント サーバー

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

UpsServerコンポーネントは以下でサポートされています。

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

要件:

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

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

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

詳細については、Citrix Universal Print Serverを参照してください。

その他

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

バージョン互換性の詳細については、製品マトリックスを参照してください。

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

Workspace Environment Management (WEM) のシステム要件については、WEMドキュメントのシステム要件を参照してください。

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

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

複数のNICがサポートされています。

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

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

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

この製品はPowerShellバージョン3から5をサポートしています。

技術概要

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

Citrix Virtual Apps and Desktops™ では、以下が可能です。

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

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

主要コンポーネント

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

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

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

デリバリーコントローラー™

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

- アプリケーションとデスクトップを配信する

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

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

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

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

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

データベース

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

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

仮想配信エージェント (VDA)

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

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

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

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

シトリックス ストアフロント™

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

シトリックス ワークスペース™ アプリ

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

スタジオ

Web Studio は、オンプレミスの Citrix Virtual Apps and Desktops 展開を構成および管理できる Web ベースの管理コンソールです。

Studio のコンポーネント(/en-us/citrix-virtual-apps-desktops/current-release/media/new-stud-dashboard-breakdown.png)

コールアウト	エリア	説明
A	ナビゲーションメニュー	仮想アプリとデスクトップを配信するための DaaS 展開を構成および管理できます。例としては、検索、マシンカタログ、デリバリーグループな

コールアウト	エリア	説明
		どがあります。詳細については、「展開の計画と構築」および「展開の管理」を参照してください。
B	パンくずリスト	コンテキストを提供し、上位ページへの迅速なナビゲーションを可能にします。
C	共通アクション	フィードバックの送信、ホームページのカスタマイズ、通知センターへのアクセスなどの一般的なアクションが表示されます。
		• 通知センターは、リアルタイムの更新と、長時間実行される操作の 48 時間の履歴を提供します。操作の実行中は、その進行状況を示すステータス通知が共通アクション領域の下に表示されます。
		• タスクセンターには、カテゴリ別に整理されたすべてのタスクの包括的なリストが表示されます。UI には、メインビューと一貫性のあるフィルター、検索、その他のコントロールが用意されています。**削除**や**詳細表示**などの一般的なアクション、およびタスクの再実行やサブタスクステータ

コールアウト	エリア	説明
		スのエクスポートなどのタスク固有のアクションを含む、リストされた任意のタスクに対してアクションを実行できます。現在、タスクセンターはハードウェア更新およびOS ディスクリセットタスクをサポートしています。
F	作業ペイン	ナビゲーションメニューで選択されたノードのアクションと詳細が表示されます。

詳細については、「Web Studio のインストール」を参照してください。

セキュアプライベートアクセス

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

シトリックス ディレクター

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

Directorは以下を表示します。

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

- コントローラー内のモニターサービスからの履歴サイトデータ。

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

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

Citrix ライセンスサーバー

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

ハイパーバイザーまたはその他のサービス

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

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

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

追加コンポーネント

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

シトリックス プロビジョニング™

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

理マシンをホストするために使用できます。PVSはControllerと通信して、ユーザーにリソースを提供します。

シトリックス ゲートウェイ

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

シトリックス SD-WAN™

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

一般的な展開の仕組み

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

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

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

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

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

ユーザー接続の処理方法

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

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

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

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

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

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

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

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

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

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

データアクセスが機能する仕組み

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

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

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

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

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

デスクトップとアプリケーションの配信

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

マシンカタログ

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

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

有効なマシンタイプは次のとおりです。

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

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

デリバリーグループ

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

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

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

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

詳細については、「デリバリーグループの作成」を参照してください。

アプリケーショングループ

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

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

詳細情報

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

データベース

> **注:**

> バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

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

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

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

Citrixは、データベースに関して以下を推奨します。

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

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

高可用性

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

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

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

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

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

データベースソフトウェアのインストール

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

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

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

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

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

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

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

サイト作成ウィザードからデータベースをセットアップする

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

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

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

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

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

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

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

自動セットアップ

必要なデータベース権限がある場合は、次の手順でデータベースをセットアップします。

1. サイト作成ウィザードの**データベース**ページで、**Studioからデータベースを作成およびセットアップ**を選択します。
2. プリンシパルデータベースの名前とアドレスを指定します。
3. データベース接続設定のセキュリティと柔軟性を向上させるために、次のSQL Server接続オプションを構成します。

- **暗号化**: 接続の暗号化レベルを指定します。
- **サーバー証明書を信頼する**: サーバー証明書の検証をバイパスするには、これを選択します。
- **証明書のホスト名**: サーバーの証明書が一致する必要があるホスト名を入力します。この設定により、より厳格な証明書検証が保証されます。

詳細については、このMicrosoftの記事を参照してください。

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

スクリプトによるセットアップ

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

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

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

   スクリプトの保存場所を指定できます。

> **注:**
>
> エンタープライズ環境では、データベースのセットアップには、異なる役割（権限）を持つ異なるチームによって処理される可能性のあるスクリプトが含まれます。`securityadmin` または `db_owner`。該当する場合、まず `securityadmin` ロールを持つ管理者によって「SysAdmin」スクリプトが実行され、次に `db_owner` 権限を持つ

> 管理者によって「DbOwner」スクリプトが実行されます。これらのスクリプトを生成するには、PowerShellを使用することもできます。詳細については、「推奨されるデータベース権限スクリプト」を参照してください。

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

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

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

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

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

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

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

Web Studio はサイト作成を続行するように求めます。**データベース**ページに戻り、次の手順を完了します。

1. アドレスを入力します。
2. データベース接続設定のセキュリティと柔軟性を向上させるために、次の SQL Server 接続オプションを構成します。

- **暗号化**: 接続の暗号化レベルを指定します。
- **サーバー証明書を信頼する**: サーバー証明書の検証をバイパスするには、これを選択します。
- **証明書のホスト名**: サーバーの証明書が一致する必要があるホスト名を入力します。この設定により、より厳密な証明書検証が保証されます。

詳細については、このMicrosoft の記事を参照してください。

データベースをホストしているサーバーのいずれかに接続できない場合、エラーメッセージが表示されます。

データベースのセットアップに必要な権限

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

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

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

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

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

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

優先データベース権限スクリプト

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

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

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

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

詳細については、コマンドレットのヘルプを参照してください。

データベースアドレスの形式

データベースアドレスは、次のいずれかの形式で指定できます。

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

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

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

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

データベースの場所を変更する

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

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

データベースの場所を変更するには：

1. Microsoft SQL Serverを使用している場合は、データベースを配置するサーバーにサポートされているバージョンがインストールされていることを確認してください。必要に応じて高可用性機能をセットアップしてください。
2. Web Studioにサインインし、左ペインで**設定**を選択します。
3. **データベース**タイルを見つけ、**編集**を選択します。

4. **データベースの管理**ページで、新しい場所を指定したいデータベースを選択し、アクションバーで**データベースの変更**を選択します。
5. 新しい場所とデータベース名を指定します。データベースがAzure SQLでホストされている場合は、データベースを管理する権限を持つサービスプリンシパルの資格情報を入力します。
6. Web Studioにデータベースを作成させたい場合で、適切な権限を持っている場合は、**完了**をクリックします。プロンプトが表示されたら**完了**をクリックすると、Web Studioが自動的にデータベースを作成します。Web Studioは、あなたの資格情報を使用してデータベースへのアクセスを試みます。それが失敗した場合は、データベースユーザーの資格情報を求められます。その後、Web Studioはデータベーススキーマをデータベースにアップロードします。資格情報は、データベース作成期間中のみ保持されます。
7. Web Studioにデータベースを作成させたくない場合、または十分な権限がない場合は、**データベーススクリプトの生成**をクリックします。生成されたスクリプトには、必要に応じてデータベースとミラーデータベースを手動で作成するための手順が含まれています。スキーマをアップロードする前に、データベースが空であり、少なくとも1人のユーザーがデータベースにアクセスして変更する権限を持っていることを確認してください。

詳細情報

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

配信方法

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

はじめに

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

- **インストール済みアプリ:** アプリケーションはベースデスクトップイメージの一部です。インストールプロセスには、レジストリの変更に加えて、イメージドライブにコピーされるdll、exe、その他のファイルが含まれます。詳細については、「マシンカタログの作成」を参照してください。
- **ストリーミングアプリ (Microsoft App-V):** アプリケーションはプロファイルされ、ネットワーク経由でオンデマンドでデスクトップに配信されます。アプリケーションファイルとレジ

ストリ設定は、仮想デスクトップ上のコンテナに配置され、ベースオペレーティングシステムおよび相互から分離されます。この分離により、互換性の問題に対処できます。詳細については、「App-Vアプリケーションの展開と配信」を参照してください。

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

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

Citrix Virtual Apps™公開アプリとデスクトップ

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

ユースケース:

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

利点と考慮事項:

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

ユーザーエクスペリエンス:

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

アプリケーションの処理、ホスト、および配信:

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

セッション管理と割り当て:

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

  例えば、ユーザーがログオンしてアプリケーションを要求します。そのマシン上の1つのセッションは、他のユーザーには利用できなくなります。2人目のユーザーがログオンし、そのマシンがホストするアプリケーションを要求します。同じマシン上の2つ目のセッションも利用できなくなります。両方のユーザーがさらにアプリケーションを要求しても、ユーザーは同じセッションを使用して複数のアプリケーションを実行できるため、追加のセッションは必要あ

りません。さらに2人のユーザーがログオンしてデスクトップを要求し、同じマシンで2つのセッションが利用可能な場合、その単一のマシンは4つの異なるユーザーをホストするために4つのセッションを使用していることになります。

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

VMホスト型アプリ

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

ユースケース:

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

利点と考慮事項:

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

- この方法では、アプリケーション処理のためのサーバーリソースの量が増加し、ユーザーのデータのためのストレージの量が増加する可能性があります。

ユーザーエクスペリエンス：

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

アプリケーションの処理、ホスト、および配信：

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

セッション管理と割り当て：

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

VDIデスクトップ

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

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

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

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

- **ランダム非永続デスクトップ（プールされたVDIデスクトップとも呼ばれる）：** ユーザーがこれらのデスクトップのいずれかにログオンするたびに、デスクトップのプールから選択された

デスクトップに接続します。このプールは単一のマスターイメージに基づいています。デスクトップへのすべての変更は、マシンの再起動時に失われます。

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

リモートPCアクセス

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

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

詳細については、リモートPCアクセス。

ネットワークポート

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

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

ポート情報が必要になる場合があります。

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

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

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

HDX™

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

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

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

HDXは、次の3つの技術原則に基づいて設計されています。

- インテリジェントリダイレクト
- 適応型圧縮
- データ重複排除

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

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

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

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

デバイス上での動作

HDXは、ユーザーデバイスのコンピューティング能力を利用して、ユーザーエクスペリエンスを強化および最適化します。HDXテクノロジーにより、ユーザーは仮想デスクトップまたはアプリケーションでマルチメディアコンテンツをスムーズかつシームレスに体験できます。ワークスペー

スコントロールにより、ユーザーは仮想デスクトップとアプリケーションを一時停止し、作業を中断した時点から別のデバイスで作業を再開できます。

ネットワーク上

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

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

データセンター内

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

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

HDX インサイト

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

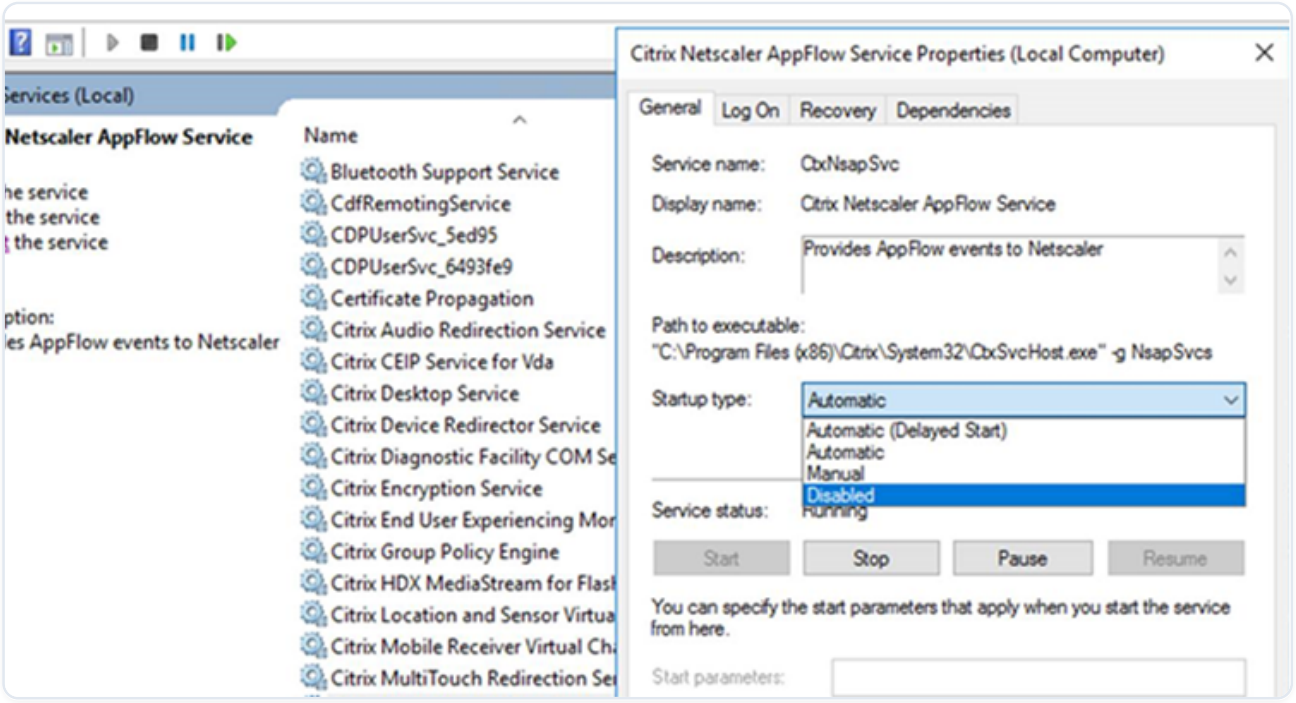
NetScalerでHDX Insight仮想チャネルを使用して、必要なすべてのデータポイントを非圧縮形式で移動させることができます。この機能を無効にすると、NetScalerデバイスは、さまざまな仮想チャネルに分散されたICA®トラフィックを復号化および解凍します。単一の仮想チャネルを使用することで、複雑さが軽減され、スケーラビリティが向上し、費用対効果が高まります。

最小要件:

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

HDX Insight仮想チャネルの有効化または無効化

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



仮想デスクトップからHDX機能を利用する

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

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

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

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

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

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

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

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

知っておくと良いこと:

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

自動クライアント再接続とセッションの信頼性

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

自動クライアント再接続:

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

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

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

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

自動クライアント再接続のデフォルト設定：

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

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

セッションの信頼性:

セッションの信頼性は、ネットワークの中断を越えて、ICAセッションをシームレスに再接続します。セッションの信頼性は、設定で指定された時間の経過後にユーザーセッションを閉じます（または切断します）。セッションの信頼性のタイムアウト後、自動クライアント再接続設定が有効になり、切断されたセッションにユーザーを再接続しようとします。セッションの信頼性が

進行中の場合、アプリケーションおよびデスクトップのネットワーク中断通知は次のようにユーザーに送信されます。

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

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

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

デフォルトのセッションの信頼性設定

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

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

NetScalerと自動クライアント再接続およびセッションの信頼性:

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

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

HDX アダプティブスループット

HDX アダプティブスループットは、出力バッファーを調整することで、ICA セッションのピークスループットをインテリジェントに微調整します。出力バッファーの数は、初期値として高い値に設定されます。この高い値により、特に高遅延ネットワークにおいて、データがより迅速かつ効率

的にクライアントに送信されます。インタラクティブ性の向上、ファイル転送の高速化、ビデオ再生のスムーズ化、フレームレートと解像度の向上により、ユーザーエクスペリエンスが強化されます。

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

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

この機能には、以下の要件があります。

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

ユーザーデバイスに送信される画質の向上

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

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

> **注:**

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

ビデオ会議のパフォーマンスを向上させる

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

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

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

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

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

ネットワークトラフィックの優先順位

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

- TCPストリーム - リアルタイム、インタラクティブ、バックグラウンド、バルク

- UDPストリーム - 音声とFramehawkディスプレイリモート

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

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

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

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

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

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

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

ターまたはレガシーNetScaler SD-WANを使用する場合は、このポリシー設定を構成してください。

- マルチストリームユーザー設定 - この設定はデフォルトで無効になっています。

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

リモート言語バーの表示/非表示

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

VDAから言語バー機能のクライアント制御を無効にするには：

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

Unicodeキーボードマッピング

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

Unicode キーボードレイアウトマッピングを有効または無効にする

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

KEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

名前: EnableKlMap

種類: DWORD

値: 1

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

Unicode キーボードレイアウトマッピング互換モードを有効にする

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

HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

名前: DisableWindowHook

種類: DWORD

値: 1

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

Citrix ICA® 仮想チャネル

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

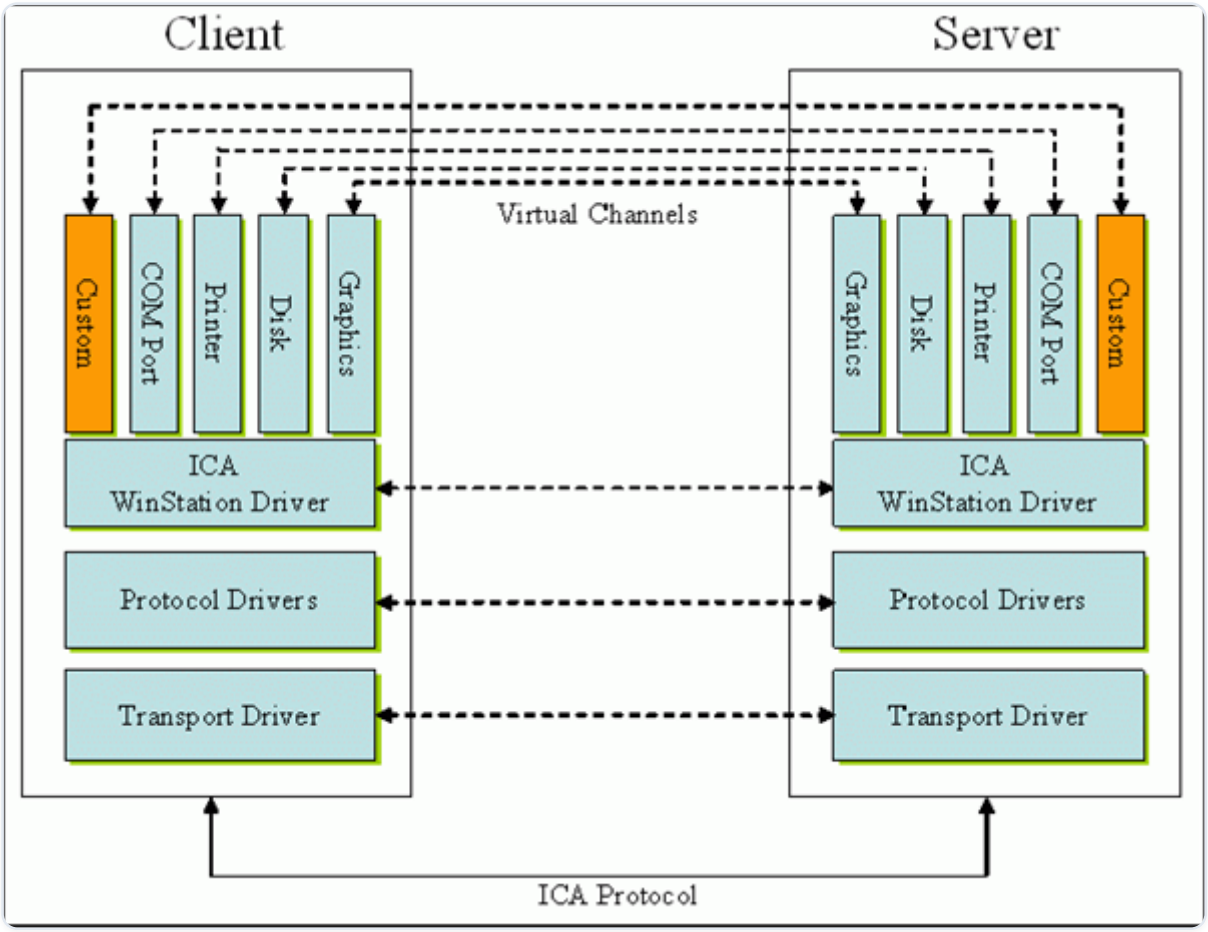
ICA仮想チャネルとは?

Citrix Workspace™アプリとCitrix Virtual Apps and Desktops™サーバー間の機能と通信の大部分は、仮想チャネルを介して行われます。仮想チャネルは、Citrix Virtual Apps and Desktopsサー

バーでのリモートコンピューティングエクスペリエンスに不可欠な部分です。仮想チャネルは次の目的で使用されます。

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

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



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

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

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

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

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

または

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

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

- TwainRdr
- ユーザーエクスペリエンス
- Vd3d

注:

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

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

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

- vdspl30n.dll – クライアントUPD
- vdsspin.dll – ケルベロス
- vdtuin.dll – 透明UI
- vdtw30n.dll – クライアント Thinwire
- vdtwin.dll – シームレス
- vdtwn.dll – ツイン

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

64ビット互換性

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

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

汎用USB仮想チャネル

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

- ctxusbm.sys
- ctxusbr.sys

ICA仮想チャネルの仕組み

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

シェルによってロードされる仮想チャネルモジュール（例）：

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

一部はカーネルモードとしてロードされます。例:

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

サーバー側のグラフィック仮想チャネル

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

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

Windowsサービスでの特殊チャネルのホスティング

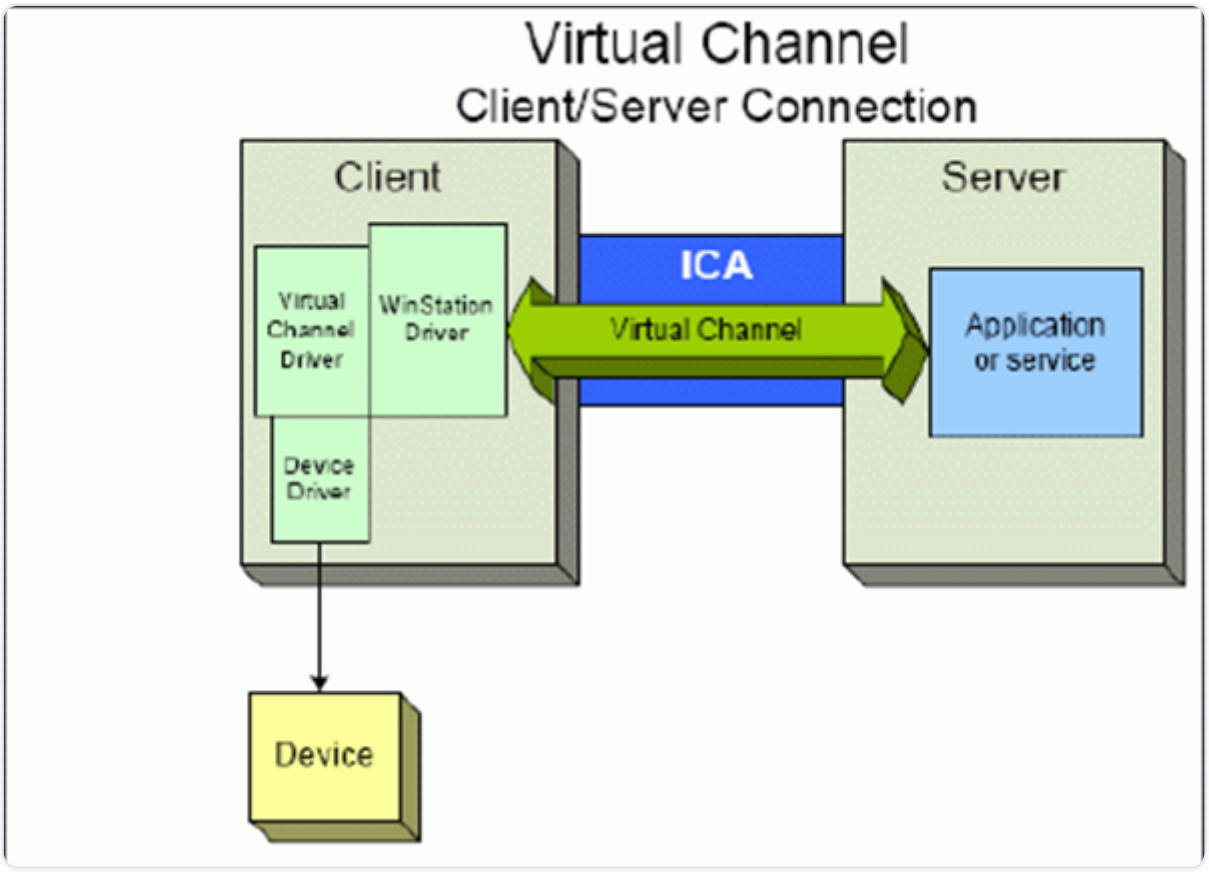
Citrix Virtual Apps and Desktopsサーバーでは、さまざまなチャネルがWindowsサービスとしてホストされます。このようなホスティングは、セッション内の複数のアプリケーションとサーバー上

の複数のセッションに対して、1対多のセマンティクスを提供します。このようなサービスの例を次に示します。

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

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

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



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

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

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

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

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

注:

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

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

注:

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

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

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

重要:

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

仮想チャネルのパススルー機能

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

次の機能は、シングルホップまたはマルチホップで同じように動作します。

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

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

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

> **重要:**

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

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

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

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

以下の従来の仮想チャネルとその機能をサポートしています。

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

セキュリティとICA仮想チャネル

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

ベストプラクティス

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

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

仮想チャネルの命名:

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

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

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

ダブルホップサポート:

仮想チャネル	ダブルホップはサポートされていますか？
オーディオ	いいえ
ブラウザコンテンツリダイレクション	いいえ
CDM	はい
CEIP	いいえ
クリップボード	はい
コンティニュアム (MRVC)	いいえ
コントロールVC	はい
HTML5 ビデオリダイレクト (v1)	はい
キーボード、マウス	はい
マルチタッチ	いいえ
NSAPVC	いいえ
印刷	はい
SensVC	いいえ
スマートカード	はい

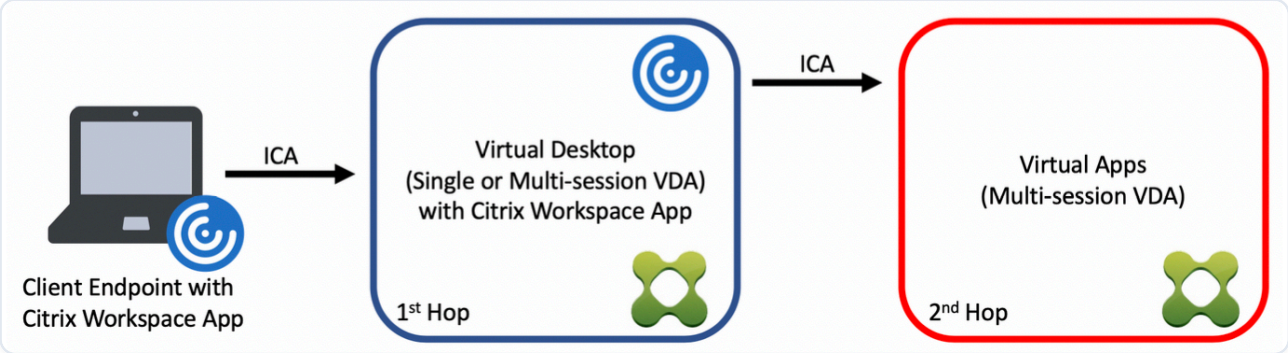
仮想チャネル	ダブルホップはサポートされていますか？
ツイン	はい
USB VC	はい
WAYCOM デバイス - K2M (USB VC を使用)	はい
Webカメラビデオ圧縮	はい
Windows Mediaリダイレクト	はい

参照

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

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

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



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

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

システム要件

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

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

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

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

ダブルホップにおけるHDX™の展開に関する考慮事項

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

グラフィック

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

遅延

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

マルチメディア

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

USBデバイスリダイレクト

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

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

注:

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

FIDO2リダイレクト

FIDO2リダイレクトは、中間ホップVDAにインストールされているCitrix Workspace App for Windowsがバージョン2503以降である限り、ダブルホップシナリオでサポートされます。さらに、これは2番目のホップ接続がICA経由の場合にのみサポートされます。

サポートの例外

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

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

インストールと構成

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

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

準備

インストール準備 を確認し、必要なタスクをすべて完了します。

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

コアコンポーネントのインストール

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

サイトの作成

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

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

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

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

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

オプションコンポーネントのインストール

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

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

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

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

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

マシンカタログを作成する

Studioでサイトを作成した後、マシンカタログの作成に誘導されます。

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

デリバリーグループを作成する

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

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

アプリケーショングループの作成（オプション）

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

既知の制限事項

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

マシンID

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

マシンIDの種類

以下のマシンIDの種類がサポートされています。

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

マシンIDの種類	説明
Microsoft Entraハイブリッド参加済み	IDはオンプレミスのActive Directoryで作成され、Microsoft Entra Connectを介してMicrosoft Entra IDと同期されます。プロビジョニングされたマシンはオンプレミスのActive Directoryに参加します。その後、マシンはMicrosoft Entraハイブリッド参加済みになります。Microsoft Entraハイブリッド参加済みVMをインポートする場合、そのVMはCitrix Virtual Apps and DesktopsによってActive Directory参加済みVMとして扱われます。
ドメイン非参加	IDはマシン内でローカルに作成および管理されます。Citrix Virtual Apps and DesktopsへのVMのインポートはサポートされていません。

サポートされる構成

以下は、各シナリオでサポートされる構成の詳細です。

サポートされるインフラストラクチャ

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

サポートされているワークスペース認証IDプロバイダー

マシンID	マイクロソフトエントラID	アクティブディレクトリ	ACTIVE DIRECTORYとトークン	オクタ	SAML	シトリックス ゲートウェイ	アダプティブ認証
AD参加済み	はい	はい	はい	はい	はい	はい	はい
Microsoft Entra ハイブリッド参加済み	はい	はい	はい	はい	はい	はい	はい
ドメイン非参加	はい	はい	はい	はい	はい	はい	はい

Active Directory 参加済み

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

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

この製品は以下をサポートします。

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

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

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

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

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

複数のActive Directoryフォレスト環境での展開

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

外部信頼が設定されている場合、VDAで次の変更を行います:

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

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

次の表に、サポートされている信頼の種類を示します。

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

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

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

次のステップ

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

Microsoft Entraハイブリッド参加済み

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

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

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

Microsoft Entra ハイブリッド参加の要件

- VDAの種類: シングルセッション（デスクトップのみ）またはマルチセッション（アプリとデスクトップ）
- VDAバージョン: 2212以降
- プロビジョニングの種類: Machine Creation Services™ (MCS)、永続的および非永続的
- 割り当ての種類: 専用およびプール

- ホスティングプラットフォーム: 任意のハイパーバイザーまたはクラウドサービス

Microsoft Entra ハイブリッド参加の制限事項

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

Microsoft Entra ハイブリッド参加に関する考慮事項

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

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

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

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

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

$MaxCount = 60



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

{

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

  {

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

    if ($provider -eq 'Citrix')

    {

        break;

    }



    if ($provider -eq 1)

    {

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

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

        Start-Sleep 5

        dsregcmd /join
```

```
        break

    }

  }


  Start-Sleep 1

}
```

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

Microsoft Intune に登録されている Microsoft Entra ハイブリッド参加済みカタログ

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

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

Microsoft Intuneに登録されているMicrosoft Entraハイブリッド参加カタログの前提条件

この機能を有効にする前に、以下を確認してください。

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

Microsoft Intuneに登録されているMicrosoft Entraハイブリッド参加カタログの要件

- VDAタイプ: シングルセッションまたはマルチセッション
- VDAバージョン: 2407以降
- プロビジョニングタイプ: Machine Creation Service (MCS)、永続的。非永続的なシングルセッションおよびマルチセッションVM向けのMicrosoft Intuneに登録されたMicrosoft Entraハイブリッド参加カタログは現在プレビュー中です。ハイブリッドEntra ID参加の非永続VMのMicrosoft Intuneへの登録を参照してください。

- 割り当ての種類: 専用およびプール
- ホスティングプラットフォーム: 任意のハイパーバイザーまたはクラウドサービス

Microsoft Intuneに登録されているMicrosoft Entraハイブリッド参加カタログの制限事項

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

Microsoft Intune に登録された Microsoft Entra ハイブリッド参加カタログに関する考慮事項

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

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

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

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

- Configuration Manager の Cloud Attach を構成します。詳細については、Microsoft ドキュメントを参照してください。
- マスター VM に Configuration Manager クライアントを手動でインストールし、`.\CCMSetup.exe /mp:SCCMServer /logon FSP=SCCMServer` でサイトコードを割り当てないでください。SCCMServer は、お使いの環境の SCCM サーバー名です。詳細については、Microsoft ドキュメントを参照してください。
- MCS で作成されたマシンは、Active Directory Domain Services に公開されているサイト境界グループを見つけるために、自動サイト割り当てメカニズムを使用します。お使いの環境で **Configuration Manager** の境界と境界グループが構成されていることを確認してください。自動サイト割り当てが利用できない場合は、次のレジストリ設定を通じてマスター VM に静的な Configuration Manager サイトコードを構成できます。

  キー:

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

値の名前: `MdmSccmSiteCode`

値の型: **String**

値のデータ: `the site code to be assigned`

- Microsoft Intune を構成して、古いデバイスを削除します。これにより、デバイスレコードが最新の状態に保たれます。古いデバイスの削除については、クリーンアップルールでデバイスを自動的に削除するを参照してください。

次のステップ

Microsoft Entra ハイブリッド参加カタログの ID プールの作成の詳細については、Microsoft Entra ハイブリッド参加マシン ID の ID プールを参照してください。

ドメインに参加していない

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

要件

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

制限事項

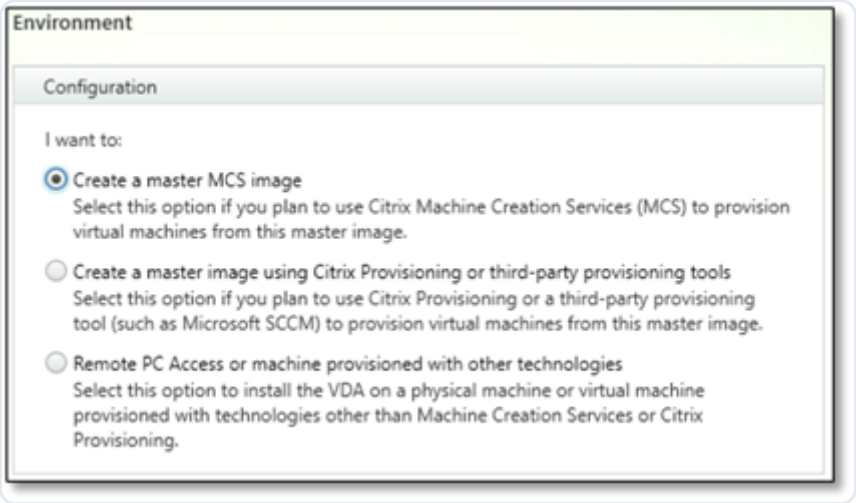
- サービス継続性はサポートされていません。
- マルチセッションのドメインに参加していないVDAを使用する場合、ローカルユーザーのプロファイルデータは保持されず、ログオフ時に削除されます。

VDAのインストールと構成

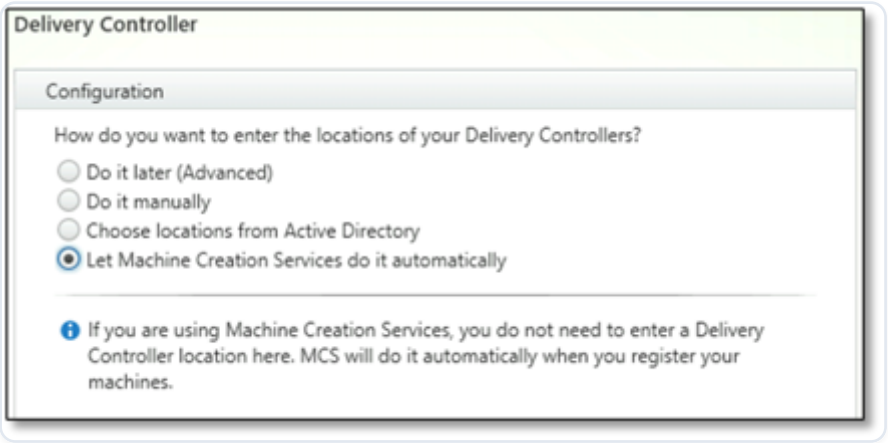
VDAをインストールする手順に従います。

1. インストールウィザードで以下のオプションを選択していることを確認してください。

   - 「環境」ページで、**「マスターMCSイメージを作成」**を選択します。



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



次のステップ

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

セッション認証

Microsoft Entra シングルサインオン (プレビュー)

Microsoft Entra ID の資格情報を使用して Microsoft Entra ハイブリッド参加セッションホスト上の仮想アプリケーションとデスクトップにアクセスする際に、シングルサインオン (SSO) を活用できます。

DaaS については、Microsoft Entra single sign-on を参照してください。

重要:

Citrix Virtual Apps and Desktops 向け Microsoft Entra シングルサインオンは現在プレビュー中です。この機能はサポートなしで提供されており、本番環境での使用はまだ推奨されていません。

サポートされるインフラストラクチャ

以下は、Microsoft Entraシングルサインオンでサポートされるインフラストラクチャコンポーネントの概要です。

マシンID	シトリックス DAAS	CVAD オンプレミス	シトリックス ワークスペース	シトリックス ストアフロント	シトリックス ゲートウェイ サービス	NETSCALER ゲートウェイ
Microsoft Entra 参加済み	はい	いいえ	はい	いいえ	はい	はい
Microsoft Entraハイブリッド参加済み	はい	はい	はい	はい	はい	はい

注:

StoreFront では、Microsoft Entra シングルサインオンは Modern UI エクスペリエンスでのみサポートされており、Classic UI エクスペリエンスではサポートされていません。

サポートされているアクセス方法

Citrix環境で利用できるアクセス方法は次のとおりです:

- **ネイティブアクセス**: ネイティブの Citrix Workspace アプリクライアントを使用して Citrix Storefront にアクセスし、セッション接続を確立します。
- **ブラウザアクセス**: ブラウザを介して Citrix Storefront にアクセスし、Citrix Workspace アプリ for HTML5 クライアントを使用して仮想アプリまたはデスクトップセッションに接続します。
- **ハイブリッドアクセス**: ブラウザを介して Citrix Storefront にアクセスし、ネイティブの Workspace アプリクライアントを使用して仮想アプリまたはデスクトップセッションに接続します。

以下は、Microsoft Entraシングルサインオンでサポートされているアクセス方法の概要です。

アクセス方法	ウィンドウズ	リナックス	MAC	クロームOS	アンドロイド	IOS
ネイティブ	はい	はい	はい	はい	はい	はい
ブラウザー	はい	はい	はい	はい	はい	はい
ハイブリッド	はい	はい	はい	いいえ	いいえ	いいえ

> **注:**
>
> ブラウザアクセスおよびハイブリッドアクセスでシングルサインオンが機能するように、ポップアップを許可する必要があります。

システム要件

Microsoft Entraシングルサインオンを使用するためのシステム要件は次のとおりです。

- コントロールプレーン: Citrix Virtual Apps and Desktops 2603 以降
- アクセスティア: StoreFront 2603 以降
- 仮想配信エージェント (VDA)
  - Windows: バージョン 2507 以降

- Citrix Workspaceアプリ
  - Windows: バージョン 2508 以降
  - Linux: バージョン2511以降
  - Mac: バージョン 2511 以降
  - HTML5: バージョン 2603 以降
  - Chrome OS: 2603 以降
  - Android: 2511 以降
  - iOS: バージョン 2511 以降
- Citrix ウェブ拡張機能
  - マイクロソフト エッジ と シトリックス ウェブ エクステンション
  - グーグル クローム と シトリックス ウェブ エクステンション
- セッションホストOS:
  - Windows 11 バージョン 24H2、2025年9月 Windows 11 用累積更新プログラム (KB5065789) 以降がインストールされていること (ビルド 26100.6725)
  - Windows Server 2025、2026年1月 Windows Server 2025 用累積更新プログラム (KB5073379) 以降がインストールされていること (ビルド 26100.32230)

注:

Citrix Web Extension は、ユーザーが **Windows**、**Linux**、または **Mac** デバイスでハイブリッドアクセスを利用する場合にのみ必要です。ユーザーがネイティブアクセスまたはブラウザアクセスを利用する場合は、Citrix Web Extension は必要ありません。

考慮事項

- ユーザーがハイブリッドアクセスを利用する場合は、Microsoft Edge または Google Chrome のいずれかを使用し、Citrix Web Extension をインストールする必要があります。ハイブリッドアクセスでの Microsoft Entra シングルサインオンは、他のブラウザではサポートされていません。
- Microsoft Entra シングルサインオンを使用してセッションにログオンする場合、自動クライアント再接続はサポートされていません。このログオン方法が使用されると、この機能は自動的

に無効になります。ネットワーク障害が発生した場合でも、セッションの信頼性は自動再接続に利用できます。

- 仮想デスクトップがロックされると、デフォルトの動作としてWindowsロック画面が表示されます。認証要件によっては、セッションロックの動作を変更する必要がある場合があります。詳細については、セッションロックの動作を参照してください。
- Microsoft Entra ハイブリッド参加セッションホストでは、Domain Admins などの特権グループのメンバーに対しては、デフォルトでシングルサインオンが機能しません。これを有効にするには、Microsoft Entra Kerberos アクセス用の読み取り専用ドメインコントローラー (RODC) 許可リストにグループまたはユーザーを追加します。詳細については、Microsoft Entra Kerberos TGT と Active Directory アクセス制御 を参照してください。
- Microsoft Entraシングルサインオンでは、Windows設定「**カスタムSSPとAPのLSASSへの読み込みを許可する**」を有効にする必要があります（デフォルト）。Microsoft Intune経由で「**Windows 10 以降のセキュリティベースライン**」テンプレートを展開すると、この設定は自動的に無効になり、SSOがブロックされるため、Intuneデバイス構成ポリシーを更新して有効な状態を維持する必要があります。

Microsoft Entraシングルサインオンの構成方法

概要

Microsoft Entraシングルサインオンの構成は、次の手順で構成されます。

1. Azure および Microsoft Entra ID の構成。
    a. Citrixリソースおよびクライアントアプリケーションを登録する。
    b. Citrixリソースアプリケーションに対してMicrosoft Entra ID Remote Desktop Services認証プロトコルを有効にする。
    c. ユーザーの同意プロンプトを非表示にする。
    d. クライアントアプリケーションを承認する。
    e. Kerberosサーバーオブジェクトを作成する (Microsoft Entraハイブリッド参加環境のみ)。
    f. Microsoft Entra条件付きアクセスポリシーを確認する。
2. Citrix の構成。
    a. 必要なOSバージョン、IDタイプ、VDAバージョンでセッションホストをプロビジョニングします。
    b. StoreFront を構成します。
    c. サイトで Microsoft Entra シングルサインオンを有効にします。

d. デリバリーグループで Microsoft Entra シングルサインオンを有効にします。

AzureとMicrosoft Entra IDの構成

Microsoft Entraシングルサインオンを利用するには、まずMicrosoft Entra IDテナントでWindows向けMicrosoft Entra認証を許可する必要があります。これにより、Microsoft Entra参加済みおよびMicrosoft Entraハイブリッド参加済みセッションホストにユーザーがサインインするために必要な認証トークンが発行されます。

Azure構成を行う担当者は、最低限、以下のMicrosoft Entra組み込みロールのいずれか、または同等のロールを割り当てられている必要があります。

- アプリケーション管理者
- クラウドアプリケーション管理者

構成は、Azure Portal、Microsoft Graph PowerShell SDK、またはMicrosoft Graph APIを使用して完了できます。以下のセクションでは、Azure Portalを介して構成を完了するための詳細を説明します。Microsoft Graph PowerShell SDKまたはMicrosoft Graph APIの使用を希望する場合は、Microsoft Entra single sign-on Azure configurationを参照してください。

CITRIXアプリケーションの登録

AzureテナントにマルチテナントのCitrix Resourceアプリケーションを登録し、シングルテナントのClientアプリケーションを作成する必要があります。

まず、Citrix Resourceアプリケーションを登録する必要があります。そのためには、以下の同意URLのいずれかを使用します。

- 米国、EU、APS: `https://login.microsoftonline.com/common/adminconsent?client_id=3a510bb1-e334-4298-831e-3eac97f8b26c`
- 日本: `https://login.microsoftonline.com/common/adminconsent?client_id=0027603f-364b-40f2-98be-8ca4bb79bf8b`

Resourceアプリケーションが登録されたら、シングルテナントのClientアプリケーションを作成する必要があります。
シングルテナントのClientアプリケーションを作成する

1. Azure Portalに移動します。
2. **Microsoft Entra ID > エンタープライズ アプリケーション** に移動します。
3. **New application**を選択します。
4. **Create your own application**を選択します。

5. アプリケーションの名前を入力し、**Register an application to integrate with Microsoft Entra ID**を選択し、**Create**をクリックします。
6. **Supported account types**で、**Single tenant only**を選択し、**Register**をクリックします。
7. **Microsoft Entra ID > App registrations**に移動し、**All applications**を選択します。
8. 作成したばかりのアプリケーションを検索してクリックします。
9. **リダイレクト URI の追加**をクリックします。
10. 3つのリダイレクトURIを追加する必要があります: **Web**、**シングルページアプリケーション**、**モバイルおよびデスクトップアプリケーション**。

    a. 各URIについて、**リダイレクト URI の追加**を選択します。

    b. リダイレクトURIを入力します。追加する内容の詳細については、以下の表を参照してください。

プラットフォームの種類	リダイレクトURI	注
Web	NetScaler ログイン URI (`https://<URL>/oauth/login`)	NetScaler 認証 URL を入力します。例: `https://nsg.mycitrix.com/oauth/login`。
モバイルおよびデスクトップアプリケーション	`ctxaadsso://citrix.aad.redirect`	このURIをそのまま入力します。
SPAアプリ（シングルページアプリケーション）	NetScaler Gateway URL に続く StoreFront ストア Web パス	NetScaler Gateway URL と StoreFront ストアのパスを入力します。たとえば、ストアへのアクセスに使用する URL が `https://access.mycitrix.com/Citrix/MyStoreWeb` で、NetScaler Gateway URL が `https://nsg.mycitrix.com` の場合、SPA リダイレクト URI は `https://nsg.mycitrix.com/Citrix/MyStoreWeb` である必要があります。環境内に複数のストアがある場合

プラットフォームの種類	リダイレクトURI	注
		は、すべてのストアに対して SPA リダイレクト URI エントリを追加する必要があります。

c. を選択します。

11. すべてのリダイレクトURIが追加されたら、クライアントアプリケーションにAPIアクセス許可を追加する必要があります。

    a. 左側のペインの の下にある を選択します。

    b. を選択します。

    c. を選択します。

    d. Citrixリソースアプリケーション (**Citrix-Workspace-Resource**) を選択します。

    e. アクセス許可のリストで、**user_impersonation** をオンにします。

    f. を選択します。

12. 左側のペインで を選択し、割り当てられたアプリケーションIDをメモします。

クライアントアプリケーションを登録する
アプリケーションが作成および構成されたら、アプリケーションのアクセス許可に同意する必要があります。

Azure portal内でアプリケーションのアクセス許可に同意できます。

1. **Microsoft Entra ID > エンタープライズ アプリケーション** に移動します。
2. クライアントアプリケーションを検索して選択します。
3. 「セキュリティ」の下にある左側のペインで「**アクセス許可**」を選択します。
4. 「**\<tenantName\> の管理者の同意を付与**」をクリックします。
5. アクセス許可に同意します。

または、管理者同意URLを使用することもできます: `https://login.microsoftonline.com/<EntraTenantID>/adminconsent?client_id=<clientAppID>`

> **注：**

> `<EntraTenantID>` を Entra テナントの ID に、`<clientAppID>` をクライアントアプリケーションのアプリケーション ID に置き換える必要があります。

Citrix Resource アプリケーションのアクセス許可
アプリケーションのアクセス許可は次のとおりです。

API名	クレーム値	アクセス許可	タイプ
マイクロソフト グラフ	User.Read	サインインおよびユーザープロファイルの読み取り	委任

米国、EU、およびAPSの場合、アプリケーションは **Citrix-Workspace-Resource** (アプリケーションID 3a510bb1-e334-4298-831e-3eac97f8b26c) と呼ばれます。

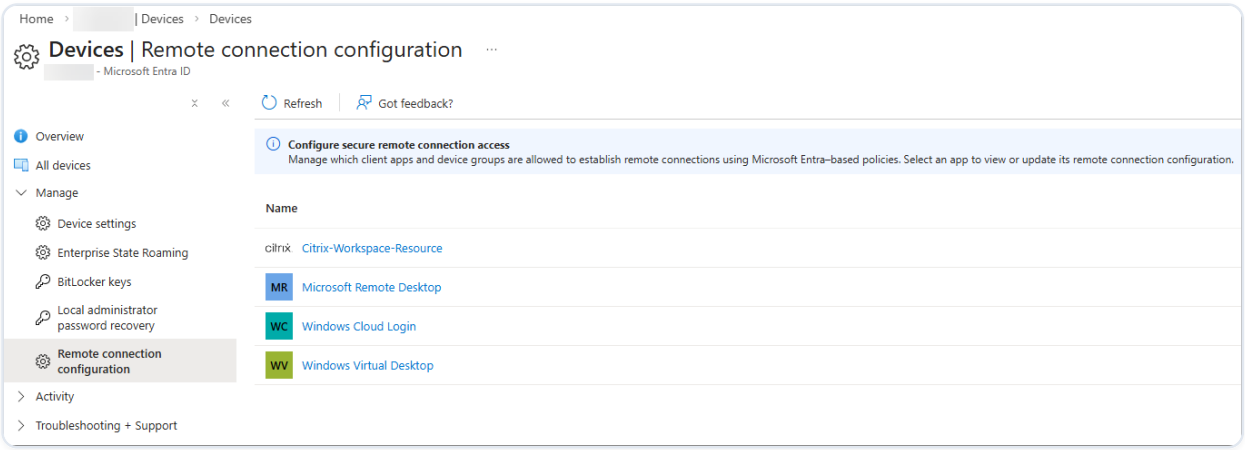
日本の場合、アプリケーションは **Citrix-Workspace-Resource-JP** (アプリケーションID 0027603f-364b-40f2-98be-8ca4bb79bf8b) と呼ばれます。
Citrix Client アプリケーションのアクセス許可
アプリケーションのアクセス許可は次のとおりです。

API名	クレーム値	アクセス許可	タイプ
シトリックス-ワークスペース-リソース シトリックス-ワークスペース-リソース-JP	user_impersonation	シトリックス Entra ID SSO	委任
マイクロソフト グラフ	User.Read	サインインおよびユーザープロファイルの読み取り	委任

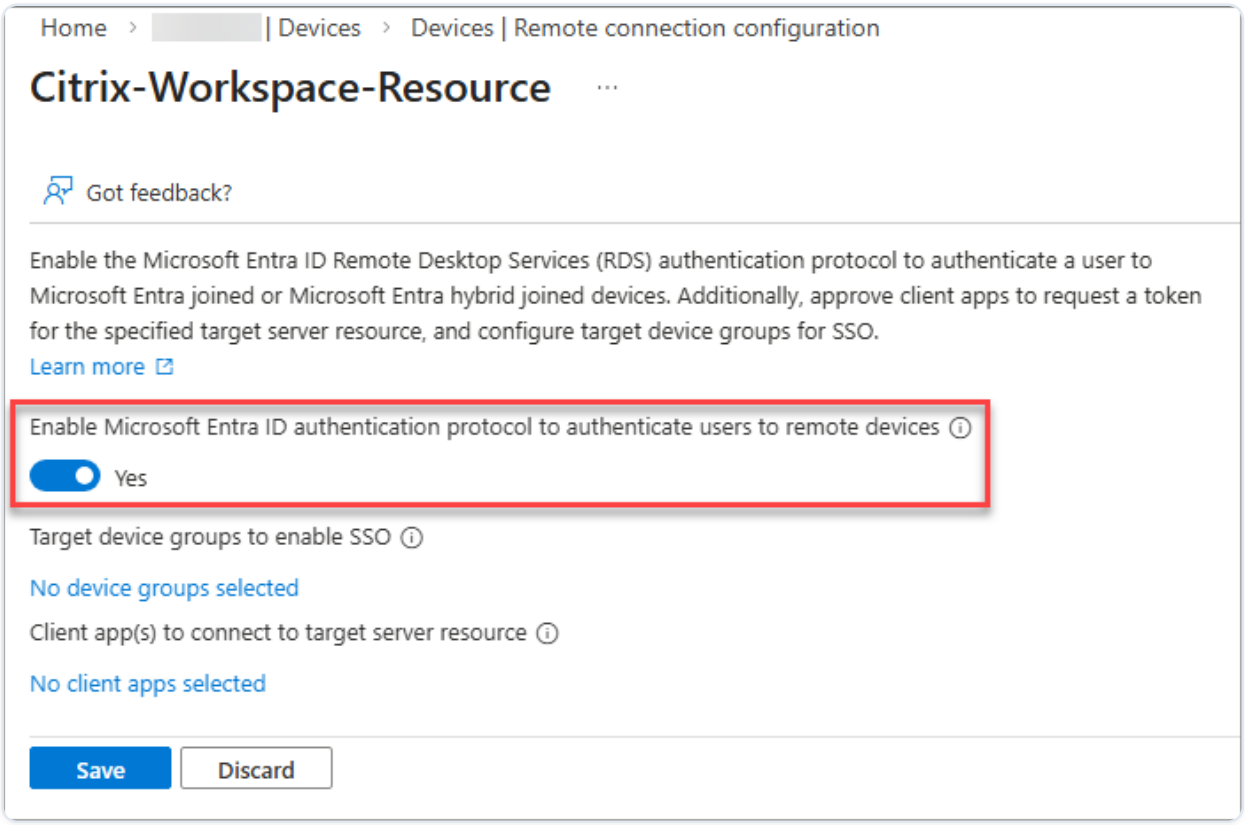
MICROSOFT ENTRA ID REMOTE DESKTOP SERVICES認証プロトコルを有効にする

Citrix ResourceアプリケーションでMicrosoft Entra ID Remote Desktop Services認証プロトコルを有効にする必要があります。手順は次のとおりです。

1. Azure Portalで、`Microsoft Entra ID` > `Devices` > `Manage` > `Remote connection configuration` に移動します。



2. **Citrix-Workspace-Resource**を選択します。
3. **Microsoft Entra ID Remote Desktop Services認証プロトコル**を有効にします。



4. ユーザー同意プロンプトを非表示にするに進みます。

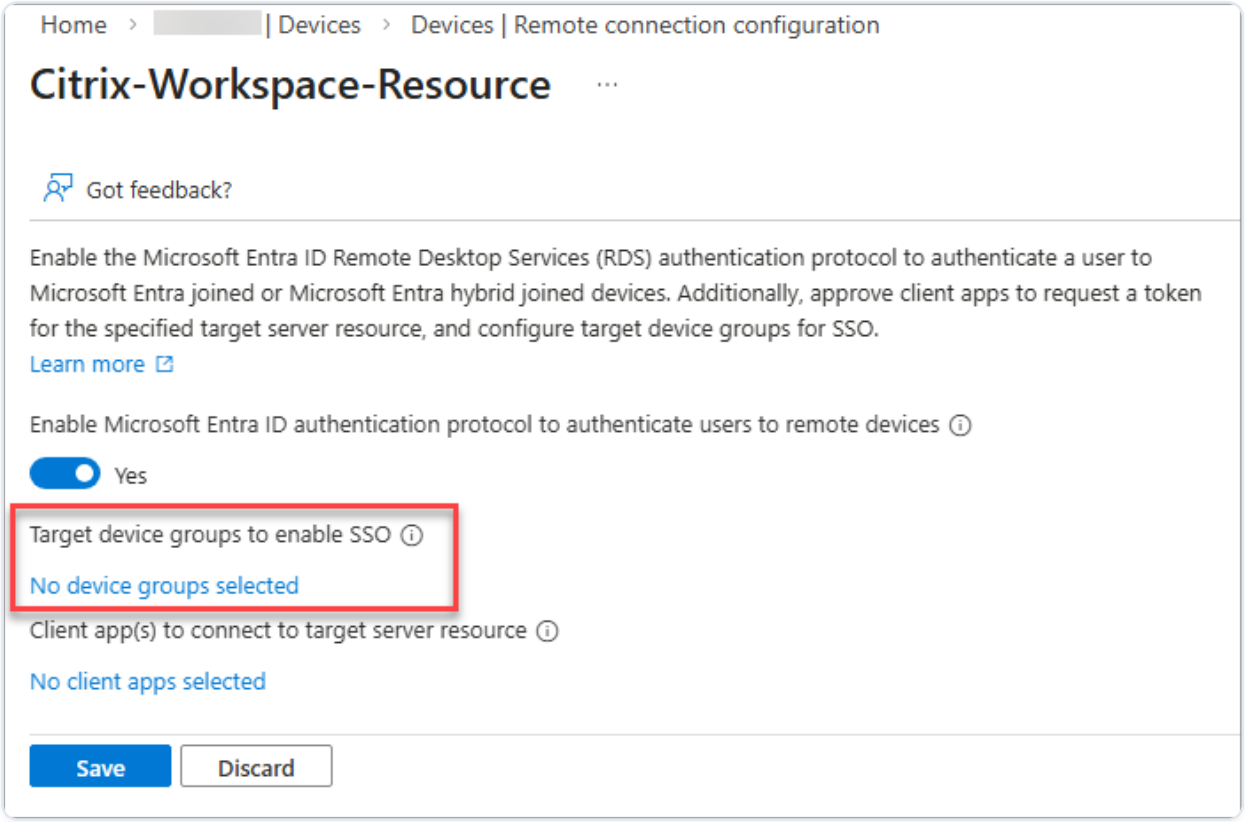
ユーザー同意プロンプトダイアログを非表示にする

デフォルトでは、Microsoft Entraシングルサインオンが有効なMicrosoft Entra参加済みまたはMicrosoft Entraハイブリッド参加済みセッションホストに接続する際、ユーザーはリモートデスクトップ接続を許可するよう求められ、シングルサインオンを許可するために**はい**を選択する必要があります。Microsoft Entraは、再度プロンプトを表示するまで、最大15個の一意のセッションホストを30日間記憶します。

ターゲットデバイスのリストを構成することで、このダイアログを非表示にできます。デバイスのリストを構成するには、Microsoft Entra参加済みおよび/またはMicrosoft Entraハイブリッド参加済みのセッションホストを含む1つ以上のグループをMicrosoft Entra IDで作成し、その後、リソースアプリケーションでそれらのグループを承認する必要があります（最大10グループまで）。

Microsoft Entra ID Remote Desktop Services 認証プロトコルを有効にし、グループが作成されたら:

1. ターゲットデバイスグループを追加するためのリンクをクリックし、適切なグループを選択します。



注

グループのメンバーシップ管理を簡素化するために、動的グループを作成することを強くお勧めします。動的グループは通常5〜10分以内に更新されますが、大規模なテナントでは最大24時間かかる場合があります。

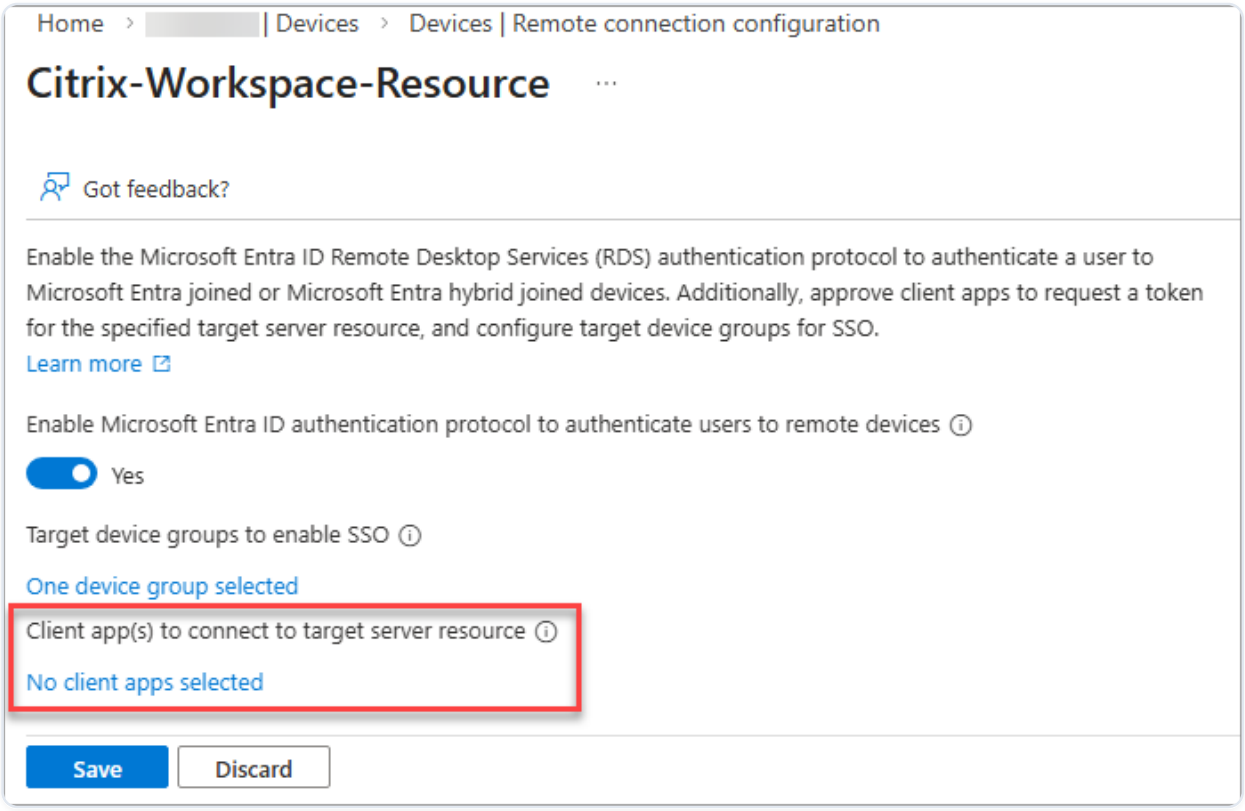
動的グループには、Microsoft Entra ID P1ライセンスまたはIntune for Educationライセンスが必要です。詳細については、グループの動的メンバーシップ規則を参照してください。

1. クライアントアプリケーションの承認に進みます。

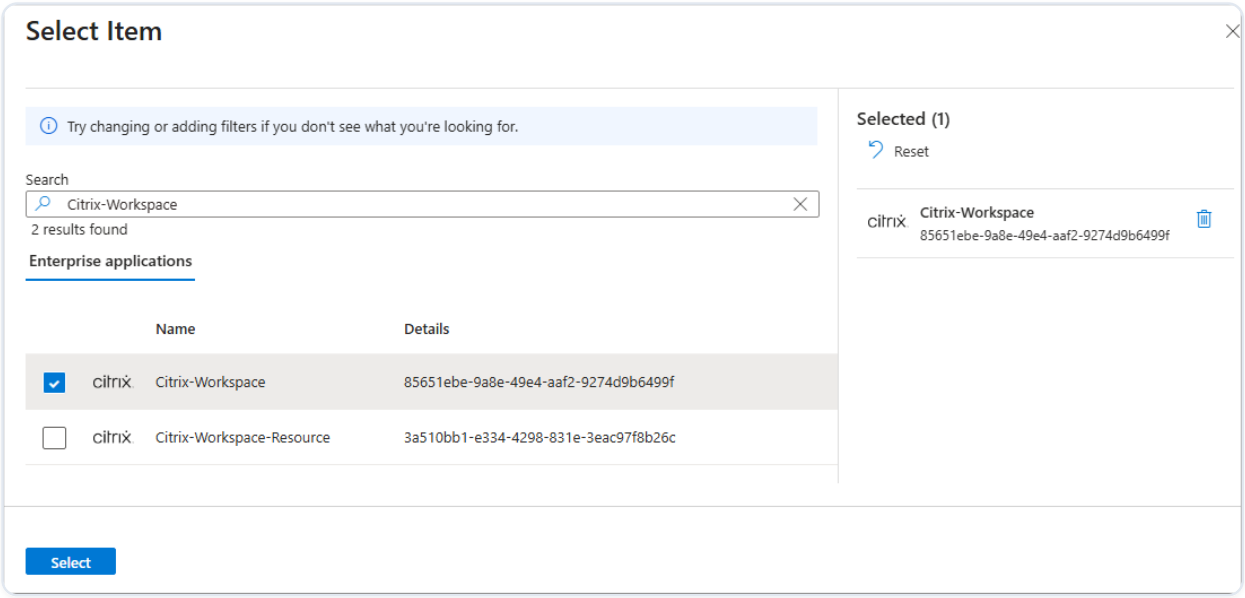
クライアントアプリケーションを承認する

Citrix Resource アプリケーションで、Citrix Client アプリケーションを承認済みクライアントとして明示的に追加する必要があります。

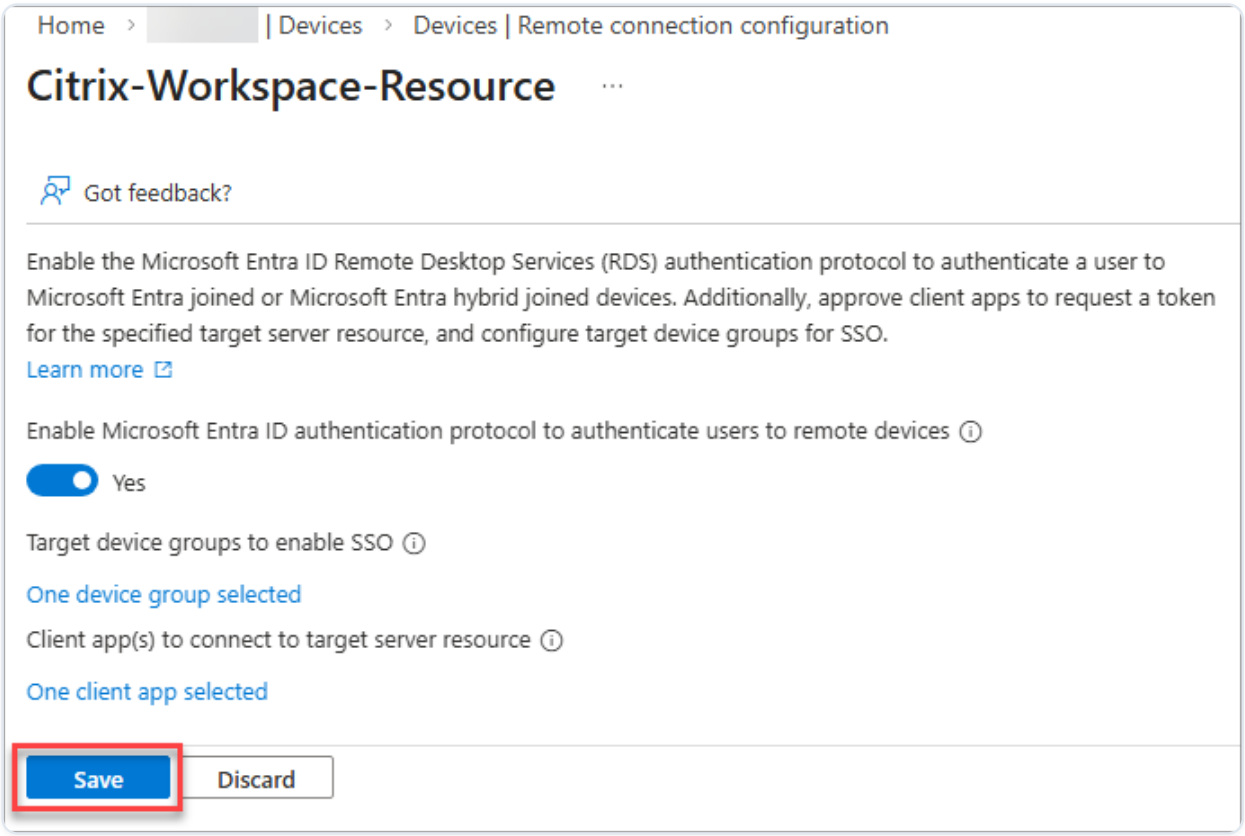
1. 信頼済みクライアントアプリケーションを追加するためのリンクをクリックします。



2. Citrix Client アプリケーションを選択します。



3. **保存**を選択して、Citrix Resource アプリケーションに構成変更を適用します。



4. Kerberos サーバーオブジェクトの作成に進みます。

KERBEROSサーバーオブジェクトを作成する

セッションホストがMicrosoft Entraハイブリッド参加している場合、ユーザーアカウントとコンピューターアカウントが存在するActive DirectoryドメインにKerberosサーバーオブジェクトを構成する必要があります。詳細については、Kerberosサーバーオブジェクトを作成するを参照してください。

MICROSOFT ENTRA 条件付きアクセス ポリシーの確認

Microsoft Entra 条件付きアクセス ポリシーを使用している、または使用する予定がある場合は、ユーザーが意図したサインインエクスペリエンスを得られるように、Citrix Resource application に適用されている構成を確認してください。

DaaS 用 Microsoft Entra シングルサインオンを使用する際の条件付きアクセス構成の詳細については、Microsoft ドキュメント を参照してください。必要な条件付きアクセス設定は、Microsoft アプリケーションではなく、**Citrix Resource アプリケーション**に適用する必要があることに注意してください。

Citrixの構成

CITRIXセッションホスト

セッションホストのシステム要件が満たされていることを確認してください。

1. セッションホストがMicrosoft Entraハイブリッド参加済みであることを確認します。
2. システム要件で指定されている必要なオペレーティングシステムのバージョンとビルドをインストールします。
3. システム要件で指定されている必要なVDAバージョンをインストールします。

Microsoft Entraハイブリッド参加済みセッションホスト
Citrix Machines Creation Services、Citrix Provisioning、またはWindows 365を使用してMicrosoft Entraハイブリッド参加済みセッションホストを展開する場合は、次のセクションに進んでください。他のツールまたは方法を使用してMicrosoft Entraハイブリッド参加済みホストをプロビジョニングする場合は、セッションホストに次のレジストリ値を追加する必要があります。

- キー: `HKLM\SYSTEM\CurrentControlSet\Control\Citrix`
- 値の型: **DWORD**
- 値の名前: `AzureADJoinType`
- データ: `1`

セッションロックの動作
仮想デスクトップがロックされている場合、デフォルトの動作はWindowsのロック画面を表示することです。この時点では、デスクトップのロック解除にサポートされている認証方法は、**ユーザー名とパスワード**または**スマートカード**です。

ユーザーがパスワードを知らないパスワードレス展開を使用している場合は、ロック画面を表示する代わりにセッションを切断するようにセッションロックの動作を構成することをお勧めします。

この動作は、Intuneまたはグループポリシーを通じて「**Microsoft IDプラットフォーム認証のロック時にリモートセッションを切断する**」設定を有効にすることで構成できます。詳細な手順については、Azure Virtual Desktopのセッションロック動作を構成するを参照してください。

CITRIXアクセスおよびコントロールプレーン

StoreFrontの構成
StoreFrontでMicrosoft Entraシングルサインオンを有効にするには、StoreFrontドキュメントのEntra ID single-onを参照してください。
Web StudioでMicrosoft Entraシングルサインオンを有効にする
サイトでMicrosoft Entraシングルサインオンを有効にするには、クライアントおよびリソースアプリケーションの詳細とリダイレクトURIを追加する必要があります。詳細については、Settingsドキュメントを参照してください。
デリバリーグループのMicrosoft Entraシングルサインオンを有効にする
Web Studioの使用

1. Web Studioでデリバリーグループに移動し、**［デリバリーグループの作成］**をクリックします。
2. **［ユーザー］ページで、IDの種類として**［Microsoft Entraハイブリッド参加済み］**を選択します。
3. 次のページで構成を完了します。参照については、「デリバリーグループの作成」を参照してください。

PowerShellの使用

1. 新しいデリバリーグループを作成し、VDAをデリバリーグループに追加します。ユーザー（ADアカウント）をVDAに割り当てます。
2. デリバリーグループ`MachineLogonType`を`HybridAzureAd`に設定します。例：

```
Get-BrokerDesktopGroup -Name <dgName> | Set-BrokerDesktopGroup
-MachineLogOnType "HybridAzureAd"
```

3. Xml Serviceを信頼します。

```
Add-PSSnapin Citrix.Broker.Admin.V2

Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true
```

4. SSOパラメーターを設定します（ガイダンスについては以下の表を参照）。

```
Set-BrokerSite -AzureGlobalCloudId "B16898C6-
A148-4967-9171-64D755DA8520" -AzureSSOnAuthorizeUrl "<URL>"
-AzureSSOnClientId "<clientAppID>" -AzureSSOnRedirectUrl "<URL>"
-AzureSSOnResourceAppId "<resourceAppID>"
```

以下の表に、パラメーターとその既定値の詳細を示します。

パラメーター	デフォルト値	説明
AzureGlobalCloudId	B16898C6-A148-4967-9171-64D755DA8520	Entra認証に使用されるWindows Webアカウントマネージャーのデフォルト GUID。

パラメーター	デフォルト値	説明
AzureSSOnAuthorizeUrl	`https://login.microsoftonline.com/common/`	初期ログイン URL。これは、Entra テナントが存在する Azure クラウド (例: Azure Commercial と Azure Gov) によって決定されます。
AzureSSOnClientId	既定値なし	クライアントアプリケーションのアプリケーション ID。
AzureSSOnRedirectUrl	既定値なし	認証後のリダイレクト URI。クライアントアプリケーションでリダイレクト URI として構成されている URL である必要があります。
AzureSSOnResourceAppId	`citrix.cloud.com/<resourceApplicationID>`	Citrix リソースアプリケーションのアプリケーション ID。
		- 米国、EU、APS: citrix.cloud.com/3a510bb1-e334-4298-831e-3eac97f8b26c
		- 日本: citrix.cloud.com/0027603f-364b-40f2-98be-8ca4bb79bf8b

クライアントデバイス

クライアントデバイスのシステム要件が満たされていることを確認してください。

1. システム要件に記載されている必要なCitrix Workspaceアプリのバージョンをインストールします。
2. ユーザーがハイブリッドアクセスを利用する場合は、Citrix Web Extensionがインストールされていることを確認してください。ユーザーがネイティブアクセスまたはブラウザアクセスを使用する場合は、Citrix Web Extensionは不要です。

トラブルシューティング

- StoreFrontの問題のトラブルシューティングについては、「診断ログ」を参照してください。
- StoreFrontから次のエラーが表示される場合: `There was a failure with the mapped account` : それはおそらく、同期された/バックアップのADアカウントを持たない純粋なEntraユーザーです。
- 起動時にICAファイルを取得する前に即座にエラーが発生する場合: XMLサービスを信頼するように設定したことを確認してください。
- 登録中にVDAが「Initializing」で停止する場合: VDAが実際にEntraと同期されているOUに移動されていることを確認してください。

シングルサインオンが失敗する場合

仮想デスクトップまたはアプリケーションへのアクセス時にシングルサインオンが失敗した場合は、次のように進めます。

1. StoreFrontでMicrosoft Entraシングルサインオンが有効になっていることを確認してください。
2. サイトでMicrosoft Entraシングルサインオンが有効になっていることを確認してください。
3. デリバリーグループでMicrosoft Entraシングルサインオンが有効になっていることを確認してください。
4. ユーザーが利用しているアクセス方法がサポートされていることを確認してください。
5. ユーザーがハイブリッドアクセスを利用している場合は、Citrix Web Extensionがインストールされていることを確認してください。
6. クライアントデバイスで必要なCitrix Workspaceアプリのバージョンが実行されていることを確認してください。
7. セッションホストで必要なWindowsビルドが実行されていることを確認してください。
8. セッションホストで必要なVDAバージョンが実行されていることを確認してください。
9. セッションホストでWindows設定 `Always prompt for password upon connection` が有効になっていないことを確認してください。この設定はデフォルトで無効になっており、`Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security` の下にあるグループポリシーまたはIntuneを通じて構成できます。レジストリで設定が有効になっているかどうかは、`HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services` の下にある値 `fPromptForPassword` を探すことで確認できます。値が `1` に設定されている場合、設定は有効になっており、シングルサインオンは利用できません。値がないか、`0` に設定されている場合、設定は無効になっています。

10. セッションホストでWindows設定`Allow Custom SSPs and APs to be loaded into LSASS`が有効になっていることを確認します。この設定はデフォルトで有効になっており、グループポリシーまたはIntuneの`Computer Configuration\System\Local Security Authority`で構成できます。
11. セッションホストで`AzureADJoinType`設定が正しく構成されていることを確認します。
    - キー: `HKLM\SYSTEM\CurrentControlSet\Control\Citrix`
    - 値の型: **DWORD**
    - 値の名前: `AzureADJoinType`
    - 値のデータ: `1` (Microsoft Entraハイブリッド参加済み)
12. Citrix Studioで、仮想デスクトップまたはアプリケーションがEntra ID IDではなくActive Directory IDに割り当てられていることを確認してください。
13. 次のPowerShellコマンドを実行して、デリバリーグループのログオンタイプが正しく構成されていることを確認してください。

    ```
    Get-BrokerDesktopGroup -Name <deliveryGroupName>
    ```

    Microsoft Entra ハイブリッド参加済みセッションホストの場合、`MachineLogOnType` は `HybridAzureAd` に設定されている必要があります。
14. Citrix リソースアプリケーションとシングルテナントクライアントアプリケーションが Microsoft Entra テナントに登録されていることを確認します。
15. Microsoft Entra ID RDS 認証プロトコルが Citrix リソースアプリケーションで有効になっていることを確認します。
16. クライアントアプリケーションが、Citrix リソースアプリケーションで承認済みクライアントアプリケーションとして追加されていることを確認します。
17. セッションホストが Microsoft Entra ハイブリッド参加済みである場合、ユーザーアカウントとコンピューターアカウントが存在する Active Directory ドメインに Kerberos サーバーオブジェクトが作成されていることを確認します。
18. Microsoft Entra条件付きアクセス ポリシーを確認します。Citrixリソースおよびクライアントアプリケーション、またはセッションホストに、シングルサインオンエクスペリエンスに影響を与えるポリシーが適用されていないことを確認してください。

フェデレーション認証サービス

Citrix Federated Authentication Service (FAS) は、SAML や OpenID Connect (OIDC) などの最新のIDプロバイダーを介してユーザーが認証し、Windowsパスワードを提供しない環境において、Citrix仮想デスクトップおよびアプリケーションへのシングルサインオン (SSO) を可能にし、Active Directoryドメインに参加しているセッションホストへのシームレスなアクセスを保証します。

詳細については、Federated Authentication Serviceのドキュメントを参照してください。

スマートカード

Citrix Virtual Apps and Desktops および Citrix DaaS は、仮想デスクトップやアプリケーションへのログオン、およびアクティブセッション内での使用の両方でスマートカードをサポートしています。スマートカードは、物理カードとPINの両方を要求することでセキュリティを強化する、証明書ベースの二要素認証を提供します。これにより、組織はコンプライアンス要件を満たし、機密データを保護し、Windowsログオンやセキュアなアプリケーションにすでにスマートカードを利用しているユーザーのアクセスを合理化できます。認証後、ユーザーはセッション内でスマートカードを使用して、ドキュメントにデジタル署名したり、メールを暗号化したり、その他のスマートカード対応アプリケーションにアクセスしたりすることもでき、ローカル環境と仮想環境の両方で一貫性のある安全なエクスペリエンスを保証します。

詳細については、スマートカードのドキュメントを参照してください。

インストール準備

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

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

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

> **注:**

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

> - Microsoft **ボリュームシャドウコピー** サービスと **Microsoft Software Shadow Copy Provider** サービスが実行されていること。詳しくは、「ボリュームシャドウコピーサービス」を参照してください。
> - **MS-Defender** のバージョンが4.18.2105.5より高いこと。詳しくは、「Microsoft Defender Antivirusのセキュリティインテリジェンスと製品の更新」を参照してください。

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

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

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

インストール前に確認する情報

- 技術概要: 製品とそのコンポーネントについて理解を深めるため。
- セキュリティ: 展開環境を計画する際。
- 既知の問題: このバージョンで発生する可能性のある問題。

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

コンポーネントのインストール場所

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

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

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

  他のサーバーに他のコンポーネントをインストールする前に、Citrix License Serverとライセンスをインストールします。

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

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

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

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

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

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

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

> **ヒント:**
>
> デフォルト値は`HostTime="UTC"`です。この値をUTC以外のもの（例: `Local`）に変更します。この変更により、ホストとの時刻同期が実質的に無効になります。

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

コンポーネントをインストールしない場所:

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

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

権限とActive Directoryの要件

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

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

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

- (/ja-jp/citrix-virtual-apps-desktops/current-release/system-requirements.html) には、サポートされている Active Directory の機能レベルが記載されています。(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/machine-identities/active-directory.html) に詳細情報があります。
- Active Directory ドメインサービスを実行しているドメインコントローラーが少なくとも1つ必要です。
- ドメインコントローラーに Citrix Virtual Apps and Desktops™ コンポーネントをインストールしないでください。
- Studio で組織単位名を指定する際に、スラッシュ (/) を使用しないでください。

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

詳細については、以下を参照してください。

- (/ja-jp/citrix-virtual-apps-desktops/current-release/secure/best-practices.html)
- (/ja-jp/citrix-virtual-apps-desktops/current-release/manage-deployment/delegated-administration.html)
- Active Directory 構成に関する Microsoft ドキュメント

インストールのガイダンス、考慮事項、およびベストプラクティス

いずれかのコンポーネントのインストール中

- フルプロダクトメディアから Delivery Controller、Studio、License Server、または Director をインストールまたはアップグレードする際に、Citrix インストーラーがマシン上の以前の

Windows インストールからの再起動が保留中であることを検出すると、インストーラーは終了/リターンコード 9 で停止します。マシンの再起動を促されます。

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

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

- 通常、コンポーネントに前提条件がある場合、インストーラーはそれらが存在しない場合に展開します。一部の前提条件では、マシンの再起動が必要になる場合があります。
- インストール前、インストール中、インストール後にオブジェクトを作成するときは、各オブジェクトに一意の名前を指定してください。たとえば、ネットワーク、グループ、カタログ、リソースには一意の名前を付けてください。
- コンポーネントのインストールが正常に完了しなかった場合、インストールはエラーメッセージを表示して停止します。正常にインストールされたコンポーネントは保持されます。それらを再インストールする必要はありません。
- コンポーネントをインストール（またはアップグレード）すると、Citrix Analytics が自動的に収集されます。デフォルトでは、インストールが完了するとそのデータは自動的にCitrixにアップロードされます。また、コンポーネントをインストールすると、匿名データをアップロードするCitrixカスタマーエクスペリエンス向上プログラム（CEIP）に自動的に登録されます。

  インストール中に、メンテナンスとトラブルシューティングのための診断情報を収集する他のCitrixテクノロジーに参加することも選択できます。これらのプログラムの詳細については、「Citrix Insight Services」を参照してください。
- VDAのインストールが失敗した場合、MSIアナライザーは失敗したMSIログを解析し、正確なエラーコードを表示します。既知の問題である場合、アナライザーはCTX記事を提案します。アナライザーは、失敗エラーコードに関する匿名化されたデータも収集します。このデータは、CEIPによって収集された他のデータに含まれます。CEIPへの登録を終了すると、収集されたMSIアナライザーデータはCitrixに送信されなくなります。

VDAのインストール中

- Windows向けCitrix Workspace™アプリは利用可能ですが、VDAをインストールする際にはデフォルトではインストールされません。ユーザーまたは管理者は、Citrix Webサイトから Windows向けCitrix Workspaceアプリやその他のCitrix Workspaceアプリをダウンロードしてインストール（およびアップグレード）できます。または、それらのCitrix Workspaceアプリを

StoreFrontサーバーから利用可能にすることもできます。StoreFrontのドキュメントを参照してください。

- Microsoft Print Spoolerサービスは有効にする必要があります。このサービスが無効になっている場合、VDAを正常にインストールすることはできません。
- ほとんどのサポートされているWindowsエディションには、Microsoft Media Foundationがすでにインストールされています。マシンにMedia Foundationがない場合（Nエディションなど）、いくつかのマルチメディア機能はインストールされず、動作しません。
  - Windows Mediaリダイレクト
  - HTML5ビデオのリダイレクト
  - HDX™ RealTimeウェブカメラのリダイレクト

  制限を承諾するか、VDAのインストールを終了して、Media Foundationのインストール後に再開することができます。グラフィカルインターフェイスでは、この選択肢はメッセージで表示されます。コマンドラインでは、`/no_mediafoundation_ack`オプションを使用して制限を承諾できます。
- VDAをインストールすると、**Direct Access Users**という新しいローカルユーザーグループが自動的に作成されます。シングルセッションOS用VDAでは、このグループはRDP接続にのみ適用されます。マルチセッションOS用VDAでは、このグループはICA®およびRDP接続に適用されます。
- VDAは、通信するための有効なControllerアドレスを持っている必要があります。そうでない場合、セッションを確立できません。Controllerアドレスは、VDAのインストール時または後で指定できます。必ず実行してください。詳細については、「VDA登録」を参照してください。

VDAインストール後およびインストール中の再起動

VDAインストールの最後に再起動が必要です。その再起動は、デフォルトで自動的に行われます。

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

VDAインストール中に必要な再起動の回数を最小限に抑えるには：

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

VDAをインストールする前にこれらの前提条件をインストールしない場合：

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

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

インストールまたはアップグレードの失敗時の復元

> **注:**
>
> この機能はワークステーションVDAでのみ利用可能です。「障害発生時の復元」機能は、より信頼性が高く合理化されたインストールエクスペリエンスを確保するため、サーバーVDAではサポートされなくなりました。Citrixは、サーバーVDAをインストールまたはアップグレードする前に、手動でバックアップを作成することをお勧めします。

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

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

デフォルトでは、この機能は無効になっています。

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

ワークステーションVDAをインストールまたはアップグレードする際にこの機能を有効にするには：

- VDAインストーラーのグラフィカルインターフェイス（**Autostart**または復元オプションやサイレントオプションなしで`XenDesktopVDASetup.exe`コマンドを使用する場合など）を使用する場合は、**追加コンポーネント**ページで**Citrix Backup and Restore Service**チェックボックスを選択します。

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

- コマンドラインを使用してVDAインストーラーを実行し、次のいずれかのオプションを追加します：`/enablerestorecleanup`、`/enablerestore`、または`/includeadditional` "Citrix Backup and Restore"。

  - `/enablerestorecleanup`オプションを使用し、インストール/アップグレードが正常に完了した場合、復元ポイントは自動的に削除されます。
  - /enablerestore または /includeadditional 「シトリックス バックアップ アンド リストア」オプションを使用し、インストール/アップグレードが正常に完了した場合、復元ポイントは使用されませんが、保持されます。

> **注:**
>
> サーバーVDAで`/enablerestorecleanup`、`/enablerestore`、または`/includeadditional` "Citrix Backup and Restore"オプションを使用しようとすると、インストーラーはこれらのオプションを無視し、バックアップを作成せずに続行します。

インストーラー

フルプロダクトインストーラー

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

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

- Session Recording をインストールします。
- Workspace Environment Management をインストールします。

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

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

スタンドアロン VDA インストーラー

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

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

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

4つのスタンドアロンVDAインストーラーをダウンロードできます。

マルチセッションOS Virtual Delivery Agent (VDAServerSetup.exe):

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

シングルセッションOS Virtual Delivery Agent (VDAWorkstationSetup.exe):

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

シングルセッションOSコアサービス Virtual Delivery Agent (VDAWorkstationCoreSetup.exe):

Remote PC Access展開またはコアVDIインストール用に最適化されたシングルセッションOS用VDAをインストールします。Remote PC Accessは物理マシンを使用します。コアVDIインストールは、イメージとして使用されていないVMです。このような展開のVDA接続に必要なコアサービスのみをインストールします。そのため、フルプロダクトインストーラーまたは `VDAWorkstationSetup.exe` インストーラーで有効なオプションのサブセットのみをサポートします。

このインストーラーは、以下の目的で使用されるコンポーネントをインストールまたは含みません。

- アップブイ。
- Profile Management。Citrix Profile Managementをインストールから除外すると、Citrix Directorの表示に影響します。詳細については、「VDAのインストール」を参照してください。
- マシンIDサービス。
- シトリックス MCS IOドライバー
- シトリックス バックアップとリストア
- deviceTRUST
- uberAgent
- WEM

`VDAWorkstationCoreSetup.exe` インストーラーは、以下のコンポーネントをインストールまたは含んでいません: Citrix Workspace app for Windows (CWA)、Citrix Secure Access Client (CSA)、Citrix User Personalization Layer (UPL)、Session Recording Agent (SRAGENT)、およびCitrix Assistant App (ASSISTANTAPP)。

`VDAWorkstationCoreSetup.exe` を使用することは、フルプロダクトインストーラーまたは `VDAWorkstationSetup` インストーラーを使用してシングルセッションOS VDAをインストールし、以下のいずれかを実行することと同じです。

- グラフィカルインターフェイスで、 ページでRemote PC Accessオプションを選択します。
- コマンドラインインターフェイスで: `/remotepc` オプションを指定する。
- コマンドラインインターフェイスで: `/components vda` と、有効な追加コンポーネント名をすべてリストする `/exclude` オプションを指定する。

省略されたコンポーネント/機能は、後でフルプロダクトインストーラーを実行してインストールできます。この操作により、不足しているすべてのコンポーネントをインストールできます。

`VDAWorkstationCoreSetup.exe` インストーラーは、Browser Content Redirection MSI を自動的にインストールします。この自動インストールは、VDA リリース 2003 以降のサポート対象リリースに適用されます。

シングルセッションコアサービスVirtual Delivery Agent (VDASingleSessionCoreSetup.exe):

Windows 365 Cloud PCおよびRemote PC展開で利用可能な、新しい軽量のシングルセッションVDAメタインストーラーです。このインストーラーは、既存のVDAWorkstationCoreSetup.exeインストーラーをベースにしており、Profile Management、deviceTRUST、uberAgent、WEM、Backup and Restore、およびVDA Upgrade Agentとともに、必須のVDAコンポーネントを提供します。Backup and Restore機能は、コマンドラインオプション/enablerestoreまたは/enablerestorecleanupを使用して有効にできます。

これにより、パッケージサイズが大幅に削減され、クラウドベースのワークロードのインストール信頼性が向上します。最新の Remote PC シナリオ向けに設計されたこのインストーラーは、Windows 365 および Remote PC に Citrix ワークロードを展開するための、シンプルで高性能なオプションを提供します。

シングルセッション VDA インストーラーを使用するためのベストプラクティス

シングルセッションオペレーティングシステムには、4種類のインストーラーが用意されています。フルプロダクト VDA インストーラーと VDAWorkstationSetup.exe インストーラーはすべてのコンポーネントのインストールを提供しますが、VDAWorkstationCoreSetup.exe および VDASingleSessionCoreSetup.exe インストーラーには一部のデフォルトおよび追加コンポーネントは含まれていません。

環境の安定性、一貫したパフォーマンス、および継続的なサポート性を維持するため、Citrix は、インストール、アップグレード、アンインストールを含む Citrix VDA のライフサイクル全体で、一貫したインストーラータイプを使用することを推奨します。インストーラータイプを混在させると、特定のリスクが生じる可能性があります。

インストーラータイプの混在に伴うリスク:

シナリオ1: シングルセッションVDAがVDAWorkstationCoreSetup.exeまたはVDASingleSessionCoreSetup.exeインストーラーを使用して最初にインストールされ、その後フルプロダクトVDAインストーラーまたはVDAWorkstationSetup.exeインストーラーでアップグレードされた場合、以前に除外されたコンポーネントは、明示的に除外されない限り、アップグレード中にインストールされる可能性があります。

シナリオ2： シングルセッションVDAが、フルプロダクトVDAインストーラーまたはVDAWorkstationSetup.exeを使用して最初にインストールされ、その後VDAWorkstationCoreSetup.exeまたはVDASingleSessionCoreSetup.exeを使用してアップグレードされた場合、コアサービスVDAインストーラーによってインストールされなかったコンポーネントはアップグレードから除外されます。これらのコンポーネントは、アップグレードプロセス中にアップグレードされることも、アンインストール中に削除されることもありません。

シナリオ3： シングルセッションVDAが、VDAWorkstationCoreSetup.exeインストーラーを使用して最初にインストールされ、その後VDASingleSessionCoreSetup.exeでアップグレードされた場合、新しい機能が利用可能になります。次回VDAWorkstationCoreSetup.exeでアップグレードした場合、VDASingleSessionCoreSetup.exeによって新しく追加されたコンポーネントは、アップグレードプロセス中にアップグレードされることも、アンインストール中に削除されることもありません。

混在するインストーラータイプへの対処に関するガイダンス：

インストーラータイプを混在させる必要が生じた場合は、アップグレードプロセス中に同じコンポーネントが含まれるようにすることが不可欠です。

インストーラータイプが意図せず混在し、追加のコンポーネントがインストールされたり、特定のコンポーネントが管理対象外になったりした場合で、以前の環境を復元する必要がある場合は、次のように進めてください。

- **シナリオ1の場合：** プログラムのアンインストールまたは変更のためのWindows機能からVDAをアンインストールし、その後、最初に利用したインストーラー（VDAWorkstationCoreSetup.exeまたはVDASingleSessionCoreSetup.exe）を使用してVDAを再インストールします。
- **シナリオ2の場合：** フルプロダクトVDAインストーラーまたはVDAWorkstationSetup.exeインストーラーを利用して、不足しているコンポーネントをアップグレードします。
- **シナリオ3の場合：** 新しい機能を引き続き活用する予定がある場合は、VDASingleSessionCoreSetup.exeインストーラーを使用して不足しているコンポーネントをアップグレードします。あるいは、VDASingleSessionCoreSetup.exeでアップグレードした後に新しい機能を使用しない場合は、まずプログラムのアンインストールまたは変更のためのWindows機能からVDAをアンインストールし、その後VDAWorkstationCoreSetup.exeを使用してVDAを再インストールします。

Citrixインストールのリターンコード

インストールログには、コンポーネントインストールの結果が Microsoft の値ではなく、Citrix のリターンコードとして含まれています。

- 0 = 成功
- 1 = 失敗
- 2 = 部分的な成功
- 3 = 部分的な成功と再起動が必要
- 4 = 失敗と再起動が必要
- 5 = ユーザーによってキャンセルされました
- 6 = 不正なコマンドライン引数
- 7 = 新しいバージョンが見つかりました
- 8 = 成功と再起動が必要
- 9 = ファイルロック再起動
- 10 = 中止
- 11 = メディア失敗
- 12 = ライセンス失敗
- 13 = 事前チェック失敗
- 14 = 再起動保留チェック中止
- 15 = 事前チェック合格 - これは、新しい /precheckonly コマンドラインオプションを使用した後に事前チェックが合格した場合に返されます。
- 16 = 事前チェック失敗 - これは、新しい /precheckonly コマンドラインオプションを使用した後に事前チェックが失敗した場合に返されます。
- 17 = オプションソフトウェアの失敗 - これは、新しいオプションソフトウェアコンポーネントのいずれかのインストールが失敗し、「他の選択されたコンポーネントのインストールが失敗した場合でも、VDAのインストールまたはアップグレードを続行する」が選択されている場合に返されます。

例えば、Microsoft System Center Configuration Managerなどのツールを使用する場合、インストールログにリターンコード3が含まれていると、スクリプトによるVDAインストールが失敗したように見えることがあります。これは、VDAインストーラーがユーザーが開始する必要のある再起動を待機している場合に発生する可能性があります (例えば、サーバーへのRDSロールの前提条件のインストール後など)。VDAインストールは、すべての前提条件と選択されたコンポーネントがインストールされ、インストール後にマシンが再起動されて初めて成功と見なされます。

あるいは、インストールをCMDスクリプト (Microsoftの終了コードを返します) でラップするか、Configuration Managerパッケージの成功コードを変更できます。

Windows Serverワークロード向けにMicrosoft RDSライセンスサーバーを構成する

この製品は、Windows 2016などのWindows Serverワークロードを提供する場合に、Windows Serverリモートセッション機能にアクセスします。これには通常、リモートデスクトップサービスクライアントアクセスライセンス (RDS CAL) が必要です。VDAは、RDS CALを要求するためにRDSライセンスサーバーに接続できる必要があります。ライセンスサーバーをインストールしてアクティブ化します。詳細については、Microsoftドキュメント「リモートデスクトップサービスライセンスサーバーをアクティブ化する」を参照してください。概念実証環境では、Microsoftが提供する猶予期間を使用できます。

この方法を使用すると、このサービスにライセンスサーバー設定を適用させることができます。イメージ上のRDSコンソールで、ライセンスサーバーとユーザーごとのモードを構成できます。Microsoftグループポリシー設定を使用してライセンスサーバーを構成することもできます。詳細については、Microsoftドキュメント「クライアントアクセスライセンス (CAL) を使用してRDS展開をライセンスする」を参照してください。

グループポリシー設定を使用してRDSライセンスサーバーを構成するには:

1. 利用可能なマシンにリモートデスクトップサービスライセンスサーバーをインストールします。そのマシンは常に利用可能である必要があります。Citrix製品のワークロードは、このライセンスサーバーに到達できる必要があります。
2. Microsoftグループポリシーを使用して、ライセンスサーバーのアドレスとユーザーごとのライセンスモードを指定します。詳細については、Microsoftドキュメント「RDセッションホストサーバーのリモートデスクトップライセンスモードを指定する」を参照してください。

Windows 10ワークロードには、適切なWindows 10ライセンスのアクティベーションが必要です。Windows 10ワークロードをアクティベートするには、Microsoftのドキュメントに従うことをお勧めします。

詳細情報

特定のホストタイプのリソースの場所を設定する場合:

- AWSクラウド環境
- XenServer仮想化環境
- Google Cloud環境
- Microsoft Azure Resource Managerクラウド環境
- マイクロソフト システム センター コンフィギュレーション マネージャー 環境

- マイクロソフト System Center Virtual Machine Manager 仮想化環境
- Nutanix仮想化環境
- Nutanixクラウドおよびパートナーソリューション
- VMware 仮想化環境
- VMware クラウドおよびパートナーソリューション

Amulet Hotkey CoreStation 仮想化環境 (プレビュー)

Citrix Virtual Apps and Desktops™ は、Citrix が管理する Amulet Hotkey CoreStation プラグインを介して、Amulet Hotkey CoreStation ワークロードを管理します。このプラグインを使用すると、Amulet Hotkey CoreStation エンクロージャーへの接続を作成し、カタログを作成し、カタログ内のマシンの電源管理を行うことができます。

主な手順

1. Amulet Hotkey CoreStation 環境をセットアップします。
2. Amulet Hotkey CoreStation エンクロージャーへの接続を作成します。
3. Amulet Hotkey CoreStation マシンカタログを作成します。

> **注:**
>
> カタログを作成する前に、1つ以上の Amulet Hotkey CoreStation ノードを用意し、それらのノードに VDA をインストールしてください。Amulet Hotkey CoreStation エンクロージャーをハイパーバイザーとして、ノードを VM として考えることができます。

4. デリバリーグループを作成します。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- 接続の作成と管理については、「Connection to Amulet Hotkey CoreStation」を参照してください。

詳細情報

- 接続とリソースの作成および管理

- マシンカタログの作成

AWSクラウド環境

この記事では、Citrix Virtual Apps and Desktopsで使用できるリソースの場所としてAWSアカウントを設定する手順について説明します。このリソースの場所は、AWS EC2およびAmazon WorkSpaces Coreマネージドインスタンスでワークロードをプロビジョニングするために使用されます。Amazon WorkSpaces Coreマネージドインスタンスでサポートされているの種類については、「Amazon WorkSpaces CoreマネージドインスタンスのVDA」を参照してください。

構成可能なさまざまなリソースの場所の比較: AWS EC2 用 MCS、Amazon WorkSpaces Core マネージドインスタンス用 MCS、および Amazon WorkSpaces Core バンドル用クイック展開。

AWS EC2 用 MCS	AMAZON WORKSPACES CORE マネージドインスタンス用 MCS	AMAZON WORKSPACES CORE バンドル用クイック展開
Citrix® が AWS アカウントでの VM のプロビジョニングを処理します	Citrix が AWS アカウントでの VM のプロビジョニングを処理します	Amazon が AWS マネージド WorkSpaces アカウントでの VM のプロビジョニングを処理します
VM ライフサイクル管理のための高度な MCS ワークフロー	VM ライフサイクル管理のための高度な MCS ワークフロー	5ステップの迅速で簡単なワークフロー
EC2 インスタンス	WorkSpaces Core マネージドインスタンス (AWS アカウントに直接起動されるオンデマンド EC2 インスタンスを利用)	WorkSpaces バンドル、完全に AWS マネージドのキャパシティ (より高レベルの抽象化)
Microsoft 365ライセンスのサポートなし	BYOL Microsoft 365のサポート	BYOL Microsoft 365のサポート
ウィンドウズ サーバー、ウィンドウズ デスクトップ、およびLinux	ウィンドウズ サーバー、ウィンドウズ デスクトップ、およびLinux	ウィンドウズ サーバー、ウィンドウズ デスクトップ
永続的および非永続的VM	永続的および非永続的VM	永続的VMのみ
従量課金制のみ	従量課金制	月額固定料金のみ

AWS EC2 用 MCS	AMAZON WORKSPACES CORE マネージドインスタンス用 MCS	AMAZON WORKSPACES CORE バンドル用クイック展開
シトリックス DaaSおよびシトリックス Virtual Apps and Desktops™	シトリックス DaaSおよびシトリックス Virtual Apps and Desktops™	Citrix DaaSのみ

この記事のタスクを完了すると、リソースロケーションには次のコンポーネントが含まれます。

- 単一のアベイラビリティゾーン内にパブリックサブネットとプライベートサブネットを持つ仮想プライベートクラウド (VPC)。
- VPCのプライベートサブネットに配置され、Active Directoryドメインコントローラーと DNS サーバーの両方として実行されるインスタンス。
- VPCのパブリックサブネットで踏み台ホストとして機能するインスタンス。このインスタンスは、管理目的でプライベートサブネット内のインスタンスへのRDP接続を開始するために使用されます。リソースの場所の設定が完了したら、このインスタンスをシャットダウンして、容易にアクセスできないようにすることができます。VDAインスタンスなど、プライベートサブネット内の他のインスタンスを管理する必要がある場合は、踏み台ホストインスタンスを再起動できます。

タスクの概要

パブリックサブネットとプライベートサブネットを持つ仮想プライベートクラウド（VPC）を設定します。このタスクを完了すると、AWSはパブリックサブネットにElastic IPアドレスを持つNATゲートウェイを展開します。このアクションにより、プライベートサブネット内のインスタンスがインターネットにアクセスできるようになります。パブリックサブネット内のインスタンスはインバウンドのパブリックトラフィックにアクセスできますが、プライベートサブネット内のインスタンスはアクセスできません。

セキュリティグループを構成します。 セキュリティグループは、VPC内のインスタンスのトラフィックを制御する仮想ファイアウォールとして機能します。パブリックサブネット内のインスタンスがプライベートサブネット内のインスタンスと通信できるようにするルールをセキュリティグループに追加します。また、これらのセキュリティグループをVPC内の各インスタンスに関連付けます。

DHCPオプションセットを作成します。Amazon VPCでは、DHCPおよびDNSサービスがデフォルトで提供されており、Active Directoryドメインコントローラーでの DNSの構成方法に影響します。AmazonのDHCPは無効にできず、AmazonのDNSはパブリックDNS解決にのみ使用でき、Active Directory名解決には使用できません。DHCPを介してインスタンスに渡されるドメインと

ネームサーバーを指定するには、DHCPオプションセットを作成します。このセットは、Active Directoryドメインサフィックスを割り当て、VPC内のすべてのインスタンスのDNSサーバーを指定します。インスタンスがドメインに参加したときにホスト（A）および逆引き（PTR）レコードが自動的に登録されるようにするには、プライベートサブネットに追加する各インスタンスのネットワークアダプタープロパティを構成します。

踏み台ホストとドメインコントローラーをVPCに追加します。踏み台ホストを介して、プライベートサブネット内のインスタンスにログオンし、ドメインを設定してインスタンスをドメインに参加させることができます。

タスク1：VPCをセットアップする

1. AWSマネジメントコンソールから、**VPC**を選択します。
2. VPCダッシュボードから、**Create VPC**を選択します。
3. 「**VPC and more**」を選択します。
4. NAT ゲートウェイ ($) の下で、「**In 1 AZ**」または「**1 per AZ**」を選択します。
5. DNS オプションの下で、「**Enable DNS hostnames**」が選択されたままにします。
6. 「**Create VPC**」を選択します。AWS は、パブリックサブネットとプライベートサブネット、インターネットゲートウェイ、ルートテーブル、およびデフォルトのセキュリティグループを作成します。

タスク 2: セキュリティグループの構成

このタスクでは、VPC 用に次のセキュリティグループを作成および構成します:

- パブリックサブネット内のインスタンスに関連付けるためのパブリックセキュリティグループ。
- プライベートサブネット内のインスタンスに関連付けるためのプライベートセキュリティグループ。

セキュリティグループを作成するには:

1. VPC ダッシュボードで、「**Security Groups**」を選択します。
2. パブリックセキュリティグループ用のセキュリティグループを作成します。「**Create Security Group**」を選択し、グループの名前タグと説明を入力します。VPC で、以前に作成した VPC を選択します。「**Yes, Create**」を選択します。

パブリックセキュリティグループの構成

1. セキュリティグループのリストから、パブリックセキュリティグループを選択します。

2. **［Inbound Rules］タブを選択し、［Edit］**を選択して、次のルールを作成します。

タイプ	送信元
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	パブリックセキュリティグループを選択します。
ICMP	0.0.0.0/0
22 (SSH)	0.0.0.0/0
80 (HTTP)	0.0.0.0/0
443 (HTTPS)	0.0.0.0/0
1494 (ICA/HDX)	0.0.0.0/0
2598 (セッションの信頼性)	0.0.0.0/0
3389 (RDP)	0.0.0.0/0

3. 完了したら、**保存**を選択します。
4. **［Outbound Rules］タブを選択し、［Edit］**を選択して、次のルールを作成します。

タイプ	宛先
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	0.0.0.0/0
ICMP	0.0.0.0/0

5. 完了したら、**保存**を選択します。

プライベートセキュリティグループを構成する

1. セキュリティグループリストから、プライベートセキュリティグループを選択します。

2. パブリックセキュリティグループからのトラフィックを設定していない場合は、TCPポートを設定する必要があります。**［Inbound Rules］**タブを選択し、**［Edit］**を選択して、次のルールを作成します。

タイプ	送信元
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	パブリックセキュリティグループを選択します。
ICMP	パブリックセキュリティグループを選択します。
TCP 53 (DNS)	パブリックセキュリティグループを選択します。
UDP 53 (DNS)	パブリックセキュリティグループを選択します。
80 (HTTP)	パブリックセキュリティグループを選択します。
TCP 135	パブリックセキュリティグループを選択します。
TCP 389	パブリックセキュリティグループを選択します。
UDP 389	パブリックセキュリティグループを選択します。
443 (HTTPS)	パブリックセキュリティグループを選択します。
TCP 1494 (ICA/HDX)	パブリックセキュリティグループを選択します。
TCP 2598 (セッションの信頼性)	パブリックセキュリティグループを選択します。

タイプ	送信元
3389 (RDP)	パブリックセキュリティグループを選択します。
TCP 49152–65535	パブリックセキュリティグループを選択します。

3. 完了したら、**保存**を選択します。
4. **［Outbound Rules］**タブを選択し、**［Edit］**を選択して、次のルールを作成します。

タイプ	宛先
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	0.0.0.0/0
ICMP	0.0.0.0/0
UDP 53 (DNS)	0.0.0.0/0

5. 完了したら、**保存**を選択します。

タスク3：インスタンスの起動

次の手順を実行して、2つのEC2インスタンスを作成し、Amazonが生成するデフォルトの管理者パスワードを復号します。

1. AWS管理コンソールから、**EC2**を選択します。
2. EC2ダッシュボードから、**インスタンスの起動**を選択します。
3. Windows Serverマシンイメージとインスタンスタイプを選択します。
4. **［Configure Instance Details］**ページで、インスタンスの名前を入力し、以前に設定したVPCを選択します。
5. **サブネット**で、各インスタンスについて次の選択を行います。
   - Bastionホスト：パブリックサブネットを選択します
   - ドメインコントローラー：プライベートサブネットを選択します

6. 「**パブリック IP アドレスの自動割り当て**」で、各インスタンスについて次の選択を行います。
   - 踏み台ホスト：**［Enable］**を選択します。
   - ドメインコントローラー：**［Use default setting］**または**［Disable］**を選択します。
7. 「**ネットワークインターフェース**」で、ドメインコントローラーのプライベートサブネットのIP範囲内のプライマリIPアドレスを入力します。
8. 必要に応じて、「**ストレージの追加**」ページでディスクサイズを変更します。
9. 「**インスタンスのタグ付け**」ページで、各インスタンスにわかりやすい名前を入力します。
10. 「**セキュリティグループの設定**」ページで、「**既存のセキュリティグループを選択**」を選択し、各インスタンスについて次の選択を行います。
    - バスティオンホスト: パブリックセキュリティグループを選択します。
    - ドメインコントローラー: プライベートセキュリティグループを選択します。
11. 選択内容を確認し、「**起動**」を選択します。
12. 新しいキーペアを作成するか、既存のキーペアを選択します。新しいキーペアを作成する場合は、秘密鍵（.pem）ファイルをダウンロードして安全な場所に保管してください。インスタンスのデフォルトの管理者パスワードを取得する際に、秘密鍵を提供する必要があります。
13. 「**インスタンスの起動**」を選択します。「**インスタンスの表示**」を選択して、インスタンスのリストを表示します。新しく起動したインスタンスがすべてのステータスチェックに合格するまで待ってからアクセスしてください。
14. 各インスタンスのデフォルトの管理者パスワードを取得します。
    a. インスタンスリストから、インスタンスを選択し、「**接続**」を選択します。
    b. 「**RDP クライアント**」タブに移動し、「**パスワードの取得**」を選択し、プロンプトが表示されたら秘密鍵 (`.pem`) ファイルをアップロードします。
    c. 「**パスワードの復号**」を選択して、人間が読めるパスワードを取得します。AWSはデフォルトのパスワードを表示します。
15. 手順2から繰り返して、2つのインスタンスを作成します。
    - パブリックサブネットに1つの踏み台ホストインスタンス
    - ドメインコントローラーとして使用するプライベートサブネット内のインスタンスを1つ。

タスク4：DHCPオプションセットを作成する

1. VPCダッシュボードから、「**DHCPオプションセット**」を選択します。
2. 次の情報を入力します。
   - 名前タグ：セットのわかりやすい名前を入力します。
   - ドメイン名：ドメインコントローラーインスタンスを設定するときに使用する完全修飾ドメイン名を入力します。
   - ドメインネームサーバー：ドメインコントローラーインスタンスに割り当てたプライベートIPアドレスと、カンマで区切られた文字列「**AmazonProvidedDNS**」を入力します。
   - NTPサーバー：このフィールドは空白のままにします。
   - NetBIOSネームサーバー：ドメインコントローラーインスタンスのプライベートIPアドレスを入力します。
   - NetBIOSノードタイプ：「**2**」と入力します。
3. **はい、作成**を選択します。
4. 新しいセットをVPCに関連付けます。
   a. VPCダッシュボードから、**Your VPCs**を選択し、以前に設定したVPCを選択します。
   b. **アクション > DHCPオプションセットの編集**を選択します。
   c. プロンプトが表示されたら、作成した新しいセットを選択し、「**保存**」を選択します。

タスク5：インスタンスを構成する

1. RDPクライアントを使用して、踏み台ホストインスタンスのパブリックIPアドレスに接続します。プロンプトが表示されたら、管理者アカウントの資格情報を入力します。
2. 踏み台ホストインスタンスから、リモートデスクトップ接続を起動し、構成するインスタンスのプライベートIPアドレスに接続します。プロンプトが表示されたら、インスタンスの管理者資格情報を入力します。
3. プライベートサブネット内のすべてのインスタンスについて、DNS設定を構成します。
   a. **スタート > コントロールパネル > ネットワークとインターネット > ネットワークと共有センター > アダプターの設定の変更**を選択します。表示されているネットワーク接続をダブルクリックします。
   b. **プロパティ > インターネットプロトコルバージョン4 (TCP/IPv4) > プロパティ**を選択します。

c. 「**詳細設定 > DNS**」を選択します。次の設定が有効になっていることを確認し、「**OK**」を選択します。

- この接続のアドレスをDNSに登録する
- この接続のDNSサフィックスをDNS登録で使用する

4. ドメインコントローラーを構成するには:

a. Server Manager を使用して、Active Directory ドメインサービス の役割をすべてのデフォルト機能とともに追加します。

b. インスタンスをドメインコントローラーに昇格させます。昇格中にDNSを有効にし、DHCPオプションセットを作成したときに指定したドメイン名を使用します。プロンプトが表示されたらインスタンスを再起動します。

AWSの権限については、「Required AWS permissions-Amazon EC2」および「Required AWS permissions-Amazon WorkSpaces Core Managed Instances」を参照してください。

次のステップ

- コアコンポーネントをインストールする
- VDAのインストール
- サイトを作成する
- 接続の作成と管理については、以下を参照してください。
  - AWS EC2への接続
  - Amazon WorkSpaces Coreマネージドインスタンスへの接続

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

Azure Local 環境

Azure Local (Azure Arc ベース) は、オンプレミスシステムを Azure に接続し、クラウドベースのサービス、監視、管理を可能にするハイパーコンバージドインフラストラクチャ (HCI) ソリューションです。

前提条件

- Azure Local クラスター: 2503 以降

    - ストレージパスが作成されていること
    - DHCP が有効な論理ネットワークが作成されていること

- Azure Local クラスターを展開するには、Microsoft ドキュメントのAzure Local の展開についてを参照してください。

考慮事項

- Windows 10 および 11 のマルチセッションワークロードはサポートされていません。

主な手順

Azure Local クラスターで MCS カタログを作成するための主要な手順は次のとおりです。

1. ホスト接続を作成します。
2. カタログを作成します。

次のステップ

- Azure Local への接続を作成するには、Azure Local への接続を参照してください。

詳細情報

- 接続とリソースの作成および管理

XenServer® 仮想化環境

XenServer は運用管理を簡素化し、負荷の高いワークロード向けに高精細なユーザーエクスペリエンスを保証します。

XenServer をセットアップするには、「(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/install-prepare.html)インストール準備」を参照してください。

次に行うこと

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- XenServer で接続を作成および管理するには、「(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/connections/connection-citrix-hypervisor.html)XenServer への接続」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

Google Cloud環境

Citrix Virtual Apps and Desktops™ を使用すると、Google Cloud 上でマシンをプロビジョニングおよび管理できます。

要件

- Citrix Cloud™アカウント。この記事で説明されている機能は、Citrix Cloudでのみ利用可能です。
- Google Cloudプロジェクト。このプロジェクトには、マシンカタログに関連付けられているすべてのコンピューティングリソースが保存されます。既存のプロジェクトでも新規のプロジェクトでもかまいません。
- Google Cloudプロジェクトで4つのAPIを有効にします。詳細については、「Enable Google Cloud APIs」を参照してください。
- Google Cloud サービスアカウント。サービスアカウントは、プロジェクトへのアクセスを有効にするために Google Cloud に対して認証を行います。詳細については、「サービスアカウントの構成と更新」を参照してください。
- Googleプライベートアクセスを有効にします。詳細については、「Enable-private-google-access」を参照してください。

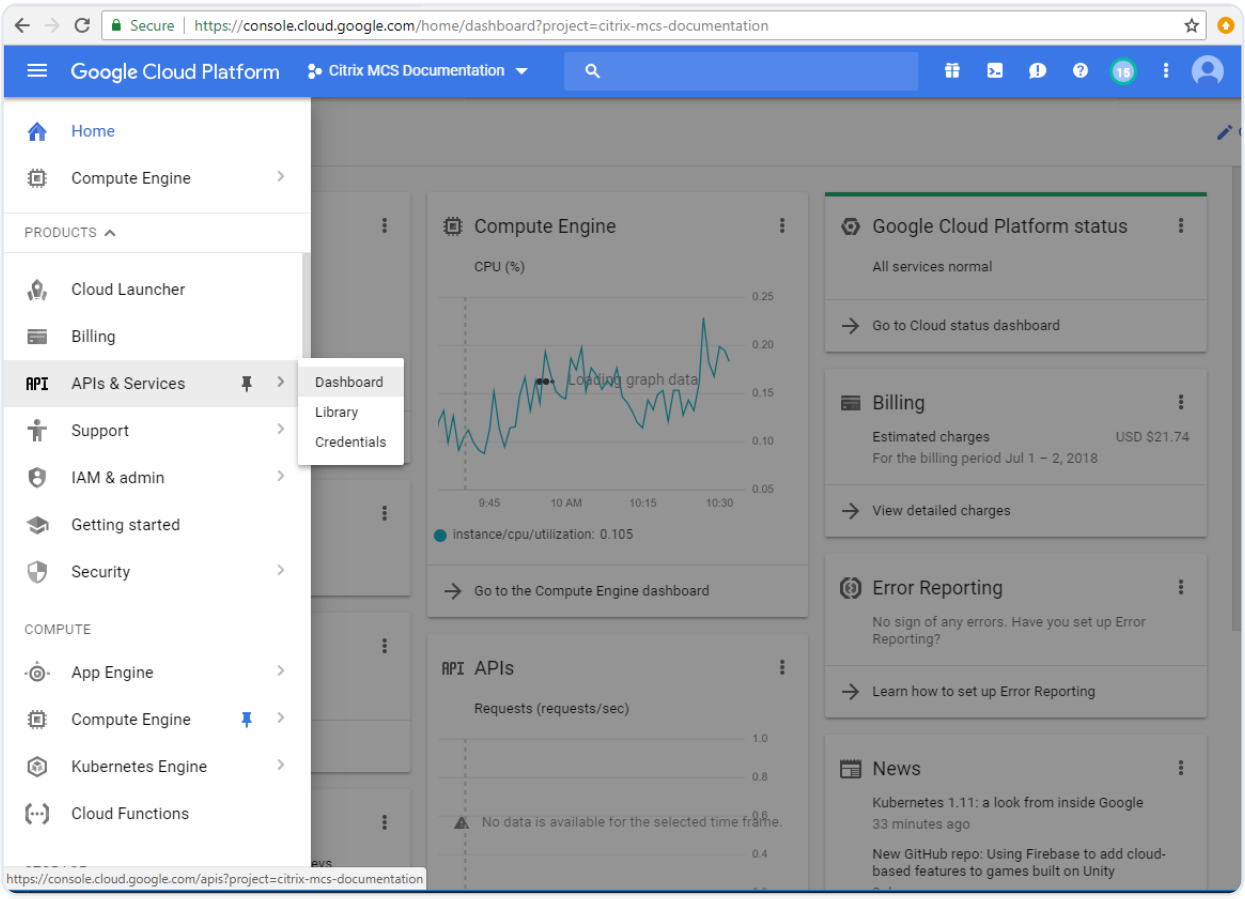
Google Cloud APIを有効にする

Web Studioを介してGoogle Cloudの機能を使用するには、Google Cloudプロジェクトで次のAPIを有効にします。

- コンピュート エンジン API
- クラウド リソース マネージャー API
- ID およびアクセス管理 (IAM) API
- クラウド ビルド API
- クラウド キー マネジメント サービス (KMS)

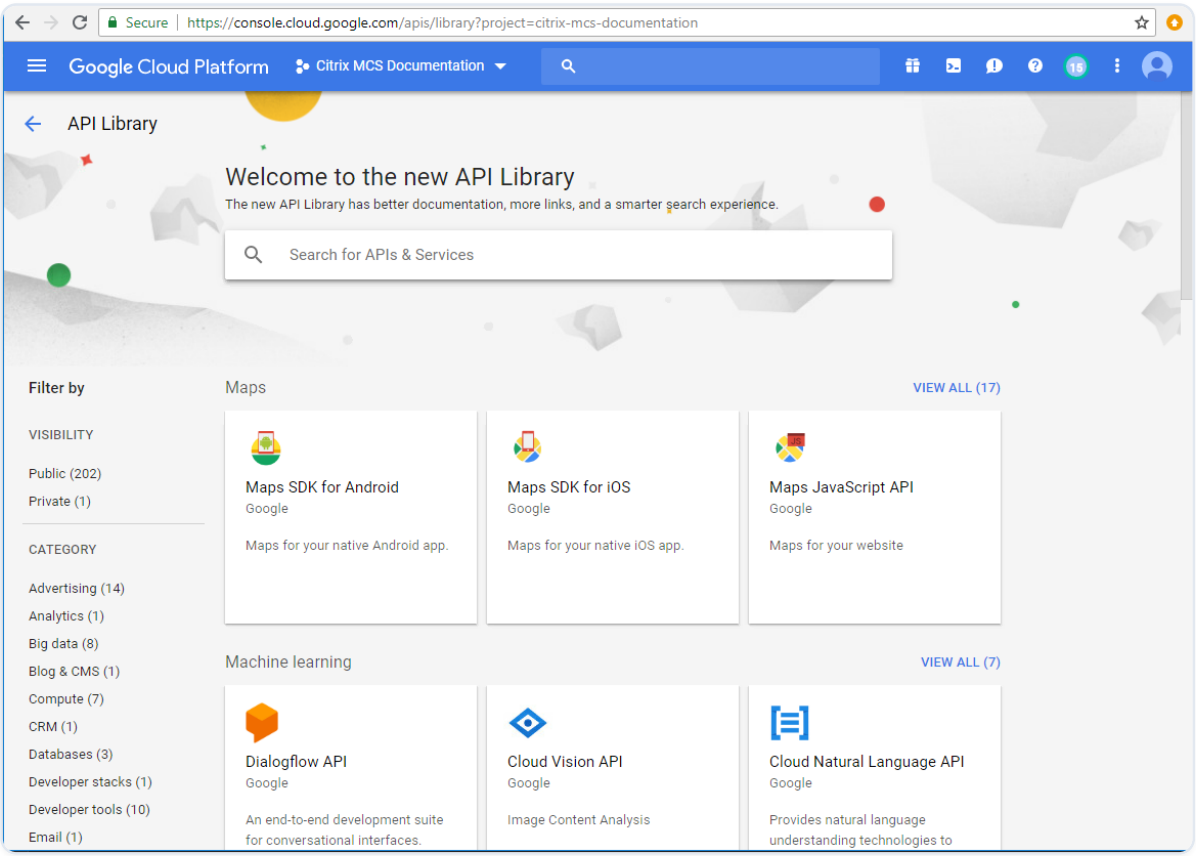
Google Cloudコンソールから、次の手順を実行します。

1. 左上のメニューで、**「APIとサービス」>「ダッシュボード」**を選択します。



2. **ダッシュボード**画面で、Compute Engine APIが有効になっていることを確認します。 有効になっていない場合は、次の手順に従ってください。

   a. 「**APIとサービス > ライブラリ**」に移動します。



b. 検索ボックスに「*Compute Engine*」と入力します。

c. 検索結果から「**Compute Engine API**」を選択します。

d. 「**Compute Engine API**」ページで、「**有効にする**」を選択します。

3. Cloud Resource Manager APIを有効にします。

a. 「**APIとサービス > ライブラリ**」に移動します。

b. 検索ボックスに「*Cloud Resource Manager*」と入力します。

c. 検索結果から「**Cloud Resource Manager API**」を選択します。

d. 「**Cloud Resource Manager API**」ページで、「**有効にする**」を選択します。APIのステータスが表示されます。

4. 同様に、**Identity and Access Management (IAM) API**と**Cloud Build API**を有効にします。

Google Cloud Shellを使用してAPIを有効にすることもできます。これを行うには：

1. Googleコンソールを開き、Cloud Shellをロードします。
2. Cloud Shellで次の4つのコマンドを実行します。

- gcloud services enable compute.googleapis.com を有効にします。
- gcloud services enable cloudresourcemanager.googleapis.com を有効にします。

- gcloud services enable iam.googleapis.com を有効にします。
- gcloud services enable cloudbuild.googleapis.com を有効にします。

3. Cloud Shellがプロンプトを表示した場合、「**承認**」をクリックします。

サービスアカウントの構成と更新

> **注:**
>
> GCPは、Cloud Build Serviceのデフォルトの動作とサービスアカウントの使用に関して、April 29, 2024以降に変更を導入します。詳細については、Cloud Build Service Account Changeを参照してください。April 29, 2024より前にCloud Build APIが有効になっている既存のGoogleプロジェクトは、この変更の影響を受けません。ただし、April 29以降も既存のCloud Build Serviceの動作を維持したい場合は、Cloud Build APIを有効にする前に、組織のポリシーを作成または適用して制約の適用を無効にすることができます。その結果、以下のコンテンツは2つに分かれています。April 29, 2024より前とApril 29, 2024以降です。新しい組織ポリシーを設定した場合は、April 29, 2024より前のセクションに従ってください。

April 29, 2024より前

Citrix Cloudは、Google Cloudプロジェクト内で3つの個別のサービスアカウントを使用します。

- *Citrix Cloudサービスアカウント*: このサービスアカウントにより、Citrix CloudはGoogleプロジェクトにアクセスし、マシンをプロビジョニングおよび管理できます。このサービスアカウントは、Google Cloudによって生成されたキーを使用してGoogle Cloudに認証します。

  ここに概説されているように、このサービスアカウントを手動で作成する必要があります。詳細については、Citrix Cloudサービスアカウントの作成を参照してください。

  このサービスアカウントは、メールアドレスで識別できます。例: `<my-service-account>@<project-id>.iam.gserviceaccount.com`。
- *Cloud Buildサービスアカウント*: このサービスアカウントは、Google Cloud APIの有効化で言及されているすべてのAPIを有効にすると自動的にプロビジョニングされます。自動的に作成されたすべてのサービスアカウントを表示するには、**Google Cloud**コンソールで**IAMと管理 > IAM**に移動し、**Googleが提供するロールの付与を含める**チェックボックスをオンにします。

  このサービスアカウントは、**プロジェクトID**と**cloudbuild**という単語で始まるメールアドレスで識別できます。例: `<project-id>@cloudbuild.gserviceaccount.com`

サービスアカウントに以下のロールが付与されていることを確認します。ロールを追加する必要がある場合は、Cloud Build サービスアカウントにロールを追加するに記載されている手順に従ってください。

  - Cloud Build サービスアカウント
  - Compute Instance 管理者
  - サービスアカウントユーザー

- *Cloud Compute サービスアカウント*: このサービスアカウントは、Compute API がアクティブ化されると、Google Cloud によって Google Cloud で作成されたインスタンスに追加されます。このアカウントには、操作を実行するための IAM 基本編集者ロールがあります。ただし、よりきめ細かな制御を行うためにデフォルトの権限を削除した場合は、次の権限を必要とする **Storage Admin** ロールを追加する必要があります。

  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

このサービスアカウントは、**プロジェクト ID** と **compute** という単語で始まるメールアドレスで識別できます。例: `<project-id>-compute@developer.gserviceaccount.com`。

CITRIX CLOUD サービスアカウントを作成する

Citrix Cloud サービスアカウントを作成するには、次の手順に従います。

1. Google Cloud コンソールで、**IAM と管理 > サービスアカウント**に移動します。
2. **サービスアカウント**ページで、**サービスアカウントを作成**を選択します。
3. **サービスアカウントの作成**ページで、必要な情報を入力し、**作成して続行**を選択します。
4. 「**このサービスアカウントにプロジェクトへのアクセスを許可する**」ページで、「**ロールを選択**」ドロップダウンメニューをクリックし、必要なロールを選択します。さらにロールを追加する場合は、「**+別のロールを追加**」をクリックします。

   各アカウント（個人またはサービス）には、プロジェクトの管理を定義するさまざまなロールがあります。このサービスアカウントには、以下のロールを付与してください。

   - Compute 管理者
   - Storage管理者
   - Cloud Build編集者

- サービスアカウントユーザー
- クラウド データストア ユーザー
- Cloud KMS 暗号オペレーター

Cloud KMS 暗号オペレーターには、以下の権限が必要です。

- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.get
- cloudkms.keyRings.list
- cloudkms.cryptoKeyVersions.useToDecrypt
- cloudkms.cryptoKeyVersions.useToEncrypt

> **注:**
>
> 新しいサービスアカウントを作成する際に利用可能なロールの完全なリストを取得するには、すべてのAPIを有効にしてください。

5. **CONTINUE**をクリックします。
6. **このサービスアカウントへのユーザーアクセスを許可**ページで、このサービスアカウントでアクションを実行するアクセス権を付与するために、ユーザーまたはグループを追加します。
7. **DONE**をクリックします。
8. IAMメインコンソールに移動します。
9. 作成されたサービスアカウントを特定します。
10. ロールが正常に割り当てられていることを検証します。

考慮事項:

サービスアカウントを作成する際は、以下を考慮してください。

- **このサービスアカウントにプロジェクトへのアクセスを許可**および**このサービスアカウントへのユーザーアクセスを許可**の手順はオプションです。これらのオプションの構成手順をスキップすることを選択した場合、新しく作成されたサービスアカウントは、**IAMと管理 > IAM**ページに表示されません。

- サービスアカウントに関連付けられたロールを表示するには、オプションの手順をスキップせずにロールを追加します。このプロセスにより、構成されたサービスアカウントにロールが表示されるようになります。

CITRIX CLOUDサービスアカウントキー

Citrix DaaS で接続を作成するには、Citrix Cloud Service Account キーが必要です。キーは資格情報ファイル (.json) に含まれています。キーを作成すると、ファイルは自動的にダウンロードされ、**ダウンロード**フォルダーに保存されます。キーを作成するときは、キータイプを JSON に設定してください。そうしないと、Web Studio はそれを解析できません。

サービスアカウントキーを作成するには、**IAMと管理 > サービスアカウント**に移動し、Citrix Cloudサービスアカウントのメールアドレスをクリックします。**キー**タブに切り替え、**キーを追加 > 新しいキーを作成**を選択します。キータイプとして**JSON**を選択していることを確認してください。

> **ヒント:**
>
> Google Cloud コンソールの ページを使用してキーを作成します。セキュリティ上の理由から、キーを定期的に変更することをお勧めします。既存の Google Cloud 接続を編集することで、新しいキーを Citrix Virtual Apps and Desktops™ アプリケーションに提供できます。

CITRIX CLOUD サービスアカウントにロールを追加する

Citrix Cloud サービスアカウントにロールを追加するには、次の手順を実行します。

1. Google Cloud コンソールで、**IAM と管理 > IAM** に移動します。
2. **IAM > 権限**ページで、作成したサービスアカウントを電子メールアドレスで特定し、見つけます。

   例: `<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. 鉛筆アイコンを選択して、サービスアカウントのプリンシパルへのアクセスを編集します。
4. 選択したプリンシパルオプションの**「project-id」へのアクセスを編集**ページで、**別のロールを追加**を選択して、必要なロールをサービスアカウントに1つずつ追加し、**保存**を選択します。

CLOUD BUILD サービスアカウントにロールを追加する

Cloud Build サービスアカウントにロールを追加するには、次の手順を実行します。

1. Google Cloud コンソールで、**IAM と管理 > IAM** に移動します。

2. **IAM**ページで、**プロジェクト ID**と**cloudbuild**という単語で始まる電子メールアドレスで識別できる Cloud Build サービスアカウントを見つけます。

   例: `<project-id>@cloudbuild.gserviceaccount.com`

3. 鉛筆アイコンを選択して、Cloud Build アカウントのロールを編集します。
4. 選択したプリンシパルオプションの**「"project-id"へのアクセスを編集」ページ**で、「別のロールを追加」**を選択して、必要なロールをCloud Buildサービスアカウントに1つずつ追加し、**「保存」**を選択します。

> **注:**
>
> すべてのAPIを有効にして、ロールの完全なリストを取得します。

April 29, 2024 以降

Citrix Cloudは、Google Cloudプロジェクト内で2つの異なるサービスアカウントを使用します。

- *Citrix Cloudサービスアカウント*: このサービスアカウントにより、Citrix CloudはGoogleプロジェクトにアクセスし、マシンをプロビジョニングおよび管理できます。このサービスアカウントは、Google Cloudによって生成されたキーを使用してGoogle Cloudに認証します。

  このサービスアカウントは手動で作成する必要があります。

  このサービスアカウントは、メールアドレスで識別できます。例: `<my-service-account>@<project-id>.iam.gserviceaccount.com`。
- *Cloud Computeサービスアカウント*：このサービスアカウントは、Google Cloud APIを有効にするで言及されているすべてのAPIを有効にした後に自動的にプロビジョニングされます。自動的に作成されたすべてのサービスアカウントを表示するには、**Google Cloud**コンソールで**「IAMと管理」>「IAM」**に移動し、**「Google提供のロール付与を含める」**チェックボックスを選択します。このアカウントには、操作を実行するためのIAM基本編集者ロールがあります。ただし、より詳細な制御を行うためにデフォルトの権限を削除した場合、次の権限を必要とする**Storage Admin**ロールを追加する必要があります。
  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

このサービスアカウントは、**プロジェクトID**と**compute**という単語で始まるメールアドレスで識別できます。例：`<project-id>-compute@developer.gserviceaccount.com.`.

サービスアカウントに次のロールが付与されていることを確認します。

- Cloud Build サービスアカウント
- Compute Instance 管理者
- サービスアカウントユーザー

CITRIX CLOUD サービスアカウントを作成する

Citrix Cloud サービスアカウントを作成するには、次の手順に従います。

1. Google Cloud コンソールで、**IAM と管理 > サービスアカウント**に移動します。
2. **サービスアカウント**ページで、**サービスアカウントを作成**を選択します。
3. **サービスアカウントの作成**ページで、必要な情報を入力し、**作成して続行**を選択します。
4. 「**このサービスアカウントにプロジェクトへのアクセスを許可する**」ページで、「**ロールを選択**」ドロップダウンメニューをクリックし、必要なロールを選択します。さらにロールを追加する場合は、「**+別のロールを追加**」をクリックします。

   各アカウント（個人またはサービス）には、プロジェクトの管理を定義するさまざまなロールがあります。このサービスアカウントには、以下のロールを付与してください。

   - Compute 管理者
   - Storage管理者
   - Cloud Build編集者
   - サービスアカウントユーザー
   - クラウド データストア ユーザー
   - Cloud KMS 暗号オペレーター

   Cloud KMS 暗号オペレーターには、以下の権限が必要です。

   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.get
   - cloudkms.keyRings.list

> **注:**

> 新しいサービスアカウントを作成する際に利用可能なロールの完全なリストを取得するには、すべてのAPIを有効にしてください。

5. **CONTINUE**をクリックします。
6. **このサービスアカウントへのユーザーアクセスを許可**ページで、このサービスアカウントでアクションを実行するアクセス権を付与するために、ユーザーまたはグループを追加します。
7. **DONE**をクリックします。
8. IAMメインコンソールに移動します。
9. 作成されたサービスアカウントを特定します。
10. ロールが正常に割り当てられていることを検証します。

考慮事項:

サービスアカウントを作成する際は、以下を考慮してください。

- **このサービスアカウントにプロジェクトへのアクセスを許可**および**このサービスアカウントへのユーザーアクセスを許可**の手順はオプションです。これらのオプションの構成手順をスキップすることを選択した場合、新しく作成されたサービスアカウントは、**IAMと管理 > IAM**ページに表示されません。
- サービスアカウントに関連付けられたロールを表示するには、オプションの手順をスキップせずにロールを追加します。このプロセスにより、構成されたサービスアカウントにロールが表示されるようになります。

CITRIX CLOUDサービスアカウントキー

Citrix DaaSで接続を作成するには、Citrix Cloudサービスアカウントキーが必要です。キーは資格情報ファイル（.json）に含まれています。キーを作成すると、ファイルは自動的にダウンロードされ、**ダウンロード**フォルダーに保存されます。キーを作成するときは、キーの種類をJSONに設定してください。そうしないと、Web Studioはそれを解析できません。

サービスアカウントキーを作成するには、**IAMと管理 > サービスアカウント**に移動し、Citrix Cloudサービスアカウントのメールアドレスをクリックします。**キー**タブに切り替え、**キーを追加 > 新しいキーを作成**を選択します。キータイプとして**JSON**を選択していることを確認してください。

> **ヒント:**

Google Cloud コンソールで、**サービスアカウント**ページを使用してキーを作成します。セキュリティ上の理由から、キーを定期的に変更することをお勧めします。既存の Google Cloud 接続を編集することで、Citrix Virtual Apps and Desktops アプリケーションに新しいキーを提供できます。

CITRIX CLOUD サービスアカウントにロールを追加する

Citrix Cloud サービスアカウントにロールを追加するには、次の手順を実行します。

1. Google Cloud コンソールで、**IAM と管理 > IAM** に移動します。
2. **IAM > 権限**ページで、作成したサービスアカウントを電子メールアドレスで特定し、見つけます。

   例: `<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. 鉛筆アイコンを選択して、サービスアカウントのプリンシパルへのアクセスを編集します。
4. 選択したプリンシパルオプションの**「project-id」へのアクセスを編集**ページで、**別のロールを追加**を選択して、必要なロールをサービスアカウントに1つずつ追加し、**保存**を選択します。

CLOUD COMPUTE SERVICE ACCOUNT にロールを追加する

Cloud Compute Service Account にロールを追加するには、次の手順を実行します。

1. Google Cloud コンソールで、**IAM と管理 > IAM** に移動します。
2. **IAM** ページで、**プロジェクト ID** と **compute** という単語で始まるメールアドレスで識別できる Cloud Compute Service Account を見つけます。

   例: `<project-id>-compute@developer.gserviceaccount.com`
3. 鉛筆アイコンを選択して、Cloud Build アカウントのロールを編集します。
4. 選択したプリンシパルオプションの**「"project-id"へのアクセスを編集」ページで、「別のロールを追加」を選択して、必要なロールをCloud Buildサービスアカウントに1つずつ追加し、「保存」**を選択します。

注:

すべてのAPIを有効にして、ロールの完全なリストを取得します。

ストレージの権限とバケット管理

Citrix Virtual Apps and Desktops は、Google Cloud サービス のクラウドビルド失敗のレポートプロセスを改善します。このサービスは Google Cloud 上でビルドを実行します。Citrix Virtual Apps and Desktops は、Google Cloud サービスがビルドログ情報をキャプチャする `citrix-mcs-cloud-build-logs-{region}-{5 random characters}` という名前のストレージバケットを作成します。このバケットには、30日後にコンテンツを削除するオプションが設定されています。このプロセスでは、接続に使用されるサービスアカウントに `storage.buckets.update` に設定された Google Cloud 権限が必要です。サービスアカウントにこの権限がない場合、Citrix Virtual Apps and Desktops はエラーを無視し、カタログ作成プロセスを続行します。この権限がないと、ビルドログのサイズが増加し、手動でのクリーンアップが必要になります。

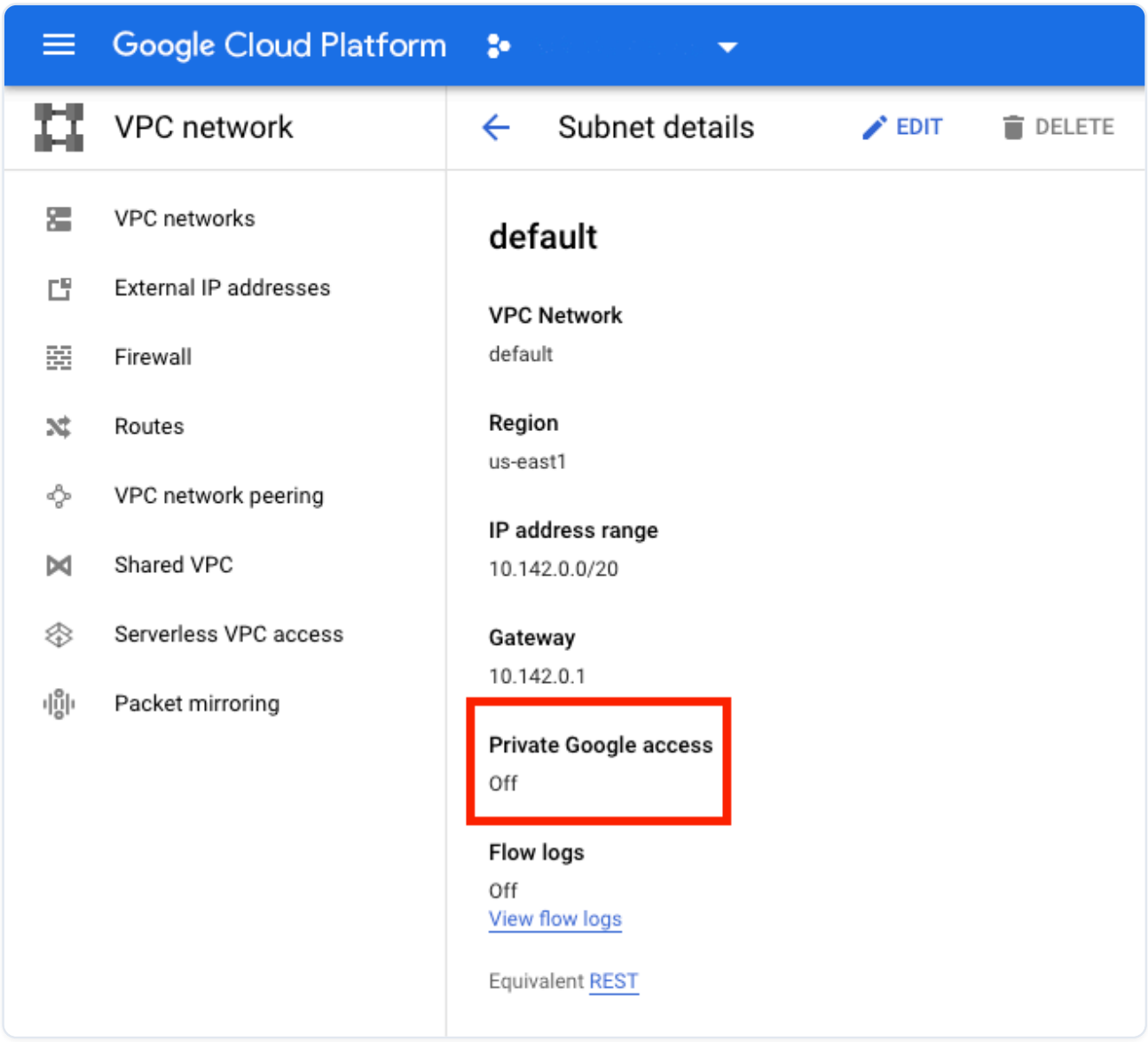
プライベート Google アクセスを有効にする

VM のネットワークインターフェイスに外部 IP アドレスが割り当てられていない場合、パケットは他の内部 IP アドレスの宛先にのみ送信されます。プライベートアクセスを有効にすると、VM は Google API および関連サービスで使用される外部 IP アドレスのセットに接続します。

> **注:**
>
> プライベート Google アクセスが有効になっているかどうかにかかわらず、パブリック IP アドレスを持つ VM と持たない VM の両方が、特にサードパーティのネットワークアプライアンスが環境にインストールされている場合、Google Public API にアクセスできる必要があります。

> MCSプロビジョニングのために、サブネット内のVMがパブリックIPアドレスなしでGoogle APIにアクセスできるようにするには、次の手順を実行します。

1. Google Cloudで、**VPC network configuration**にアクセスします。
2. サブネットの詳細画面で、「**Private Googleアクセス**」をオンにします。



詳細については、「Configuring Private Google Access」を参照してください。

重要:

ネットワークがVMのインターネットアクセスを防止するように構成されている場合、VMが接続されているサブネットに対してPrivate Googleアクセスを有効にすることに関連するリスクを組織が負うことを確認してください。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成

- Google Cloud 環境での接続の作成と管理については、「Google Cloud 環境への接続」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

HPE Moonshot 仮想化環境

Citrix Virtual Apps and Desktops™ は、Citrix が管理する HPE Moonshot プラグインを介して HPE Moonshot ワークロードを管理します。Citrix が管理する HPE Moonshot プラグインは、Citrix Virtual Apps and Desktops バージョン 2503 のアップグレードまたはインストール時に自動的にインストールされます。このプラグインを使用すると、HPE Moonshot シャーシへの接続の作成、カタログの作成、およびカタログ内のマシンの電源管理を行うことができます。

主な手順

1. HPE 環境をセットアップします。
2. HPE Moonshot シャーシへの接続を作成します。
3. マシンカタログを作成します。

> **注:**
>
> カタログを作成する前に、1 つ以上の HPE Moonshot カートリッジノードがあることを確認し、それらのノードに VDA をインストールしてください。HPE Moonshot シャーシをハイパーバイザー、カートリッジノードを VM と考えることができます。

4. デリバリーグループを作成します。
5. 管理されていない残りの HPE Moonshot ノードを、管理対象のカタログまたはデリバリーグループに移行します。

> **注:**
>
> MMC ベースの Studio の代わりに Web Studio を使用してください。

トラブルシューティング

Citrix 管理と HPE 管理の両方の HPE Moonshot プラグインがインストールされており、

- **HPE 管理の Moonshot プラグイン**を使用する場合は、Citrix 管理の HPE Moonshot プラグインをアンインストールし、`RegisterPlugin` キャッシュを更新する必要があります。これを行うには、次の手順を実行します。

  a. 管理者として PowerShell を開き、次のコマンドを実行して Citrix 管理の HPE Moonshot プラグインをアンインストールします。

  ```
  $CtxMnsht = Get-WmiObject -Class Win32_Product | Where-
  Object{$_.Name -Contains "Citrix HPE Moonshot Plugin"}

  $CtxMnsht.Uninstall()
  ```

  b. 次のコマンドを実行して、HPE 管理の Moonshot プラグインを登録します。

  ```
  cd "C:\Program Files\Common Files\Citrix\HCLPlugins\"

  .\RegisterPlugins.exe -PluginsRoot "C:\Program Files\Common
  Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0\"
  ```

  c. プラグインの登録が成功したら、**タスクマネージャー**から次のサービスを再起動します。

  a. CitrixBrokerService

  b. CitrixHostService

  c. CitrixMachineCreationService

  d. `Get-HypHypervisorPlugins` を実行して、プラグインが Delivery Controller にインストールされているかを確認します。出力の `DisplayName` フィールドには、HPE Moonshot Machine Manager と表示されている必要があります。

- Citrix管理のHPE Moonshotプラグインを再度インストールする場合は、次の手順を実行します。

  a. `E:\x64\Citrix Desktop Delivery Controller\MoonshotPlugin.msi`をインストールします。`E:\`はISOです。

  b. PowerShellを管理者として開き、次のコマンドを実行してCitrix管理のHPE Moonshotプラグインを登録します。

```
C:\Program Files\Common Files\Citrix\HCLPlugins> .
\RegisterPlugins.exe -pluginsroot .\CitrixMachineCreation\v1.0.0.0\
```

c. プラグインの登録が成功したら、タスクマネージャーから次のサービスを再起動します。

   a. CitrixBrokerService

   b. CitrixHostService

   c. CitrixMachineCreationService

1. `Get-HypHypervisorPlugins`を実行して、プラグインがDelivery Controllerにインストールされているかを確認します。出力のDisplayNameフィールドにはHPE Moonshotと表示されている必要があります。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- HPE Moonshotで接続を作成および管理する方法については、「HPE Moonshotへの接続」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

Microsoft Azure Resource Manager クラウド環境

Citrix Virtual Apps and Desktops™ 展開で Microsoft Azure Resource Manager を使用して仮想マシンをプロビジョニングする場合、以下について理解しておいてください。

- マイクロソフト Entra ID：`<https://docs.microsoft.com/en-in/azure/active-directory/fundamentals/active-directory-whatis/>`
- 同意フレームワーク: `<https://docs.microsoft.com/ja-jp/azure/active-directory/manage-apps/plan-an-application-integration>`
- サービスプリンシパル: `<https://docs.microsoft.com/ja-jp/azure/active-directory/develop/app-objects-and-service-principals/>`

Microsoft Azure Resource Manager をセットアップするには、インストール準備 を参照してください。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- Azure 環境で接続を作成および管理するには、Microsoft Azure への接続 を参照してください

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成
- CTX219211: Microsoft Entra アカウントを設定する
- CTX219243: Azure サブスクリプションへの XenApp および XenDesktop アクセスを許可する
- CTX219271: サイト間 VPN を使用してハイブリッドクラウドを展開する

マイクロソフト システムセンター コンフィギュレーションマネージャー 環境

アプリケーションとデスクトップへのアクセスを管理するために Microsoft System Center Configuration Manager (Configuration Manager) を使用しているサイトは、以下のオプションを使用してその利用を Citrix Virtual Apps and Desktops™ に拡張できます。

- SCCM を使用した VDA のインストール。
- **Configuration Manager Wake Proxy 機能:** Remote PC Access の Wake on LAN 機能は Configuration Manager でサポートされています。詳細については、「Wake on LAN - SCCM 統合」を参照してください。
- **Citrix Virtual Apps and Desktops のプロパティ:** プロパティ を使用すると、Configuration Manager を介して管理する Citrix Virtual Desktops™ を識別できます。（一部のバージョンでは、Configuration Manager は Citrix Virtual Apps and Desktops の旧名である XenApp および XenDesktop を使用します。）

プロパティ

仮想デスクトップを管理するために、Microsoft System Center Configuration Manager でプロパティを利用できます。

Configuration Manager に表示されるブール型プロパティは、true または false ではなく、`1` または `0` として表示されます。

これらのプロパティは、`Root\Citrix\DesktopInformation` 名前空間の `Citrix_virtualDesktopInfo` クラスで利用できます。プロパティ名は Windows Management Instrumentation (WMI) プロバイダーから取得されます。

プロパティ	説明
`AssignmentType`	IsAssigned の値を設定します。有効な値は、`ClientIP`、`ClientName`、`None`、および `User` です (`IsAssigned` を `True` に設定します)。
`BrokerSiteName`	`HostIdentifier` と同じ値を返します。
`DesktopCatalogName`	デスクトップに関連付けられているマシンカタログ。
`DesktopGroupName`	デスクトップに関連付けられているデリバリーグループ。
`HostIdentifier`	`BrokerSiteName` と同じ値を返します。
`IsAssigned`	デスクトップをユーザーに割り当てるには `True`、ランダムなデスクトップの場合は `False` に設定します。
`IsMasterImage`	環境に関する決定を可能にします。たとえば、プロビジョニングされたマシンではなく、イメージにアプリケーションをインストールします。有効な値は次のとおりです。イメージとして使用されるVMでは `True`。この値は、インストール時に選択に基づいて設定されるか、そのイメージからプロビジョニングされたVMではクリアされます。
`IsVirtualMachine`	仮想マシンの場合は `True`、物理マシンの場合は `false`。
`OSChangesPersist`	デスクトップオペレーティングシステムイメージが再起動のたびにクリーンな状態にリ

プロパティ	説明
	セットされる場合は `False`。それ以外の場合は `true`。
`PersistentDataLocation`	Configuration Manager が永続データを保存する場所。これはユーザーにはアクセスできません。
`BrokerSiteName`、`DesktopCatalogName`、`DesktopGroupName`、`HostIdentifier`	デスクトップがControllerに登録されるときに決定されます。完全に登録されていないデスクトップの場合はnullです。

プロパティを収集するには、Configuration Manager でハードウェアインベントリを実行します。プロパティを表示するには、Configuration Manager Resource Explorer を使用します。これらの場合、名前にはスペースが含まれるか、プロパティ名とわずかに異なります。たとえば、`BrokerSiteName` は `Broker Site Name` として表示されます。

- Citrix VDA から Citrix WMI プロパティを収集するように Configuration Manager を構成する
- Citrix WMI プロパティを使用してクエリベースのデバイスコレクションを作成する
- Citrix WMI プロパティに基づいてグローバル条件を作成する
- グローバル条件を使用してアプリケーション展開タイプの要件を定義する

`Root\ccm_vdi` 名前空間の Microsoft クラス `CCM_DesktopMachine` で Microsoft プロパティを使用することもできます。詳細については、Microsoft のドキュメントを参照してください。

Microsoft System Center 仮想マシンマネージャー仮想化環境

Hyper-V と Microsoft System Center Virtual Machine Manager (VMM) を使用して仮想マシンを提供する場合は、このガイダンスに従ってください。

このリリースでは、システム要件に記載されているVMMバージョンがサポートされています。

> **注:**
>
> 混在するHyper-Vクラスター（異なるHyper-Vバージョンを実行しているサーバーを含む）はサポートされていません。

> Citrix Provisioning（旧Provisioning Services）およびMachine Creation Services™を使用して、以下をプロビジョニングできます。

- 第1世代でサポートされているデスクトップまたはサーバーOSのVM。
- セキュアブートのサポートを含む、第2世代でサポートされているデスクトップまたはサーバーOSのVM。

ハイパーバイザーのインストールと構成

> **重要:**
>
> すべてのDelivery Controllerは、VMMサーバーと同じフォレスト内にある必要があります。

1. サーバーにMicrosoft Hyper-VサーバーとVMMをインストールします。
2. すべてのControllerにSystem Center Virtual Machine Managerコンソールをインストールします。コンソールのバージョンは管理サーバーのバージョンと一致している必要があります。以前のコンソールでも管理サーバーに接続できますが、バージョンが異なる場合、VDAのプロビジョニングは失敗します。
3. 次のアカウント情報を確認してください。

   Studioでホストを指定するために使用するアカウントは、関連するHyper-Vマシンに対するVMM管理者またはVMM委任管理者である必要があります。このアカウントがVMMで委任管理者ロールのみを持っている場合、ホスト作成プロセス中にStudioにストレージデータが表示されません。

   Studio統合に使用されるユーザーアカウントは、各Hyper-Vサーバーのadministratorsローカルセキュリティグループのメンバーである必要もあります。この構成は、VMの作成、更新、削除などのVMライフサイクル管理をサポートします。

   Hyper-Vを実行しているサーバーにControllerをインストールすることはサポートされていません。

単一のSCVMMが異なるデータセンター内の複数のクラスターを管理する大規模な展開では、委任管理者のホストグループのスコープを制限できます。

ホストグループのスコープを制限するには、Microsoft System Center Virtual Machine Manager (VMM) コンソールで委任管理者ロールを使用します。

1. **ユーザーロールの作成ウィザード**で、ユーザーロールとしてFabric Administrator (Delegated Administrator) を選択します。
2. **メンバー**で、委任管理者として使用する Active Directory のユーザーアカウントを追加します。
3. 「**スコープ**」で、委任された管理者がアクセスできるようにするホストグループを選択します。
4. 委任された管理者ユーザーの資格情報を使用して、新しい**実行アカウント**を作成します。これらの資格情報を使用して、後でハイパーバイザー接続を作成します。メインの管理者ロールアカウントは使用しないでください。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- SCVMM での接続の作成と管理については、Microsoft System Center Virtual Machine Manager への接続を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

Nutanix仮想化環境

Citrix Virtual Apps and Desktops を Nutanix AHV クラスターに接続するには、Nutanix AHV Prism Central ホスト接続を使用して Nutanix Prism Central 経由で接続します。このホスト接続は次のとおりです。

- 電源管理されたVDAとMCSプロビジョニングされたVDAの両方を含むマシンカタログをサポートします。
- テンプレートバージョンを使用して、AHVクラスター間でMCSマスターイメージの共有を可能にします。
- ホスト接続での証明書信頼を簡素化します。
- Cloud ConnectorへのNutanixプラグインのインストールが不要になります。

「Nutanix Prism Central on AHV」を参照してください。

Citrix Virtual Apps and Desktops の展開で VM を提供するために、Nutanix Acropolis をホスト接続として使用して、AHV 上の Nutanix Prism Element を使用することもできます。ただし、このセットアッププロセスでは、Citrix Virtual Apps and Desktops 環境に Nutanix プラグインをインストールして登録する必要があります。AHV 上の Nutanix Prism Element を参照してください。

Nutanix Acropolis MCS プラグインのインストールガイドの詳細については、「Nutanix Support Portal」を参照してください。

AHV環境でのNutanix Prism Central

Citrix は、Citrix Virtual Apps and Desktops を AHV 上の Nutanix Prism Central と統合するプラグインを開発し、保守しています。このプラグインは Citrix Delivery Controllers と統合されており、個別のプラグインをインストールする必要がありません。

Nutanix AHV Prism Central プラグインは、Citrix が管理する Delivery Controller にプリインストールされているため、Delivery Controller に個別にインストールする必要がありません。Citrix が管理するコンポーネントとサービスについては、技術概要 を参照してください。

前提条件

Nutanix AHV Prism Centralには、以下が必要です。

- Prism Centralバージョンpc.2025.2以降。サポートされているPrism Centralバージョンの詳細については、「Supported Hypervisors for Citrix Virtual Apps and Desktops (MCS) and Citrix Provisioning (PVS)」を参照してください。
- Nutanix AHV クラスター向けの AOS バージョン 7.3 以降。
- Nutanix AHV クラスターは Prism Central に登録する必要があります。
- Citrix 管理者アカウントには、ホスト接続、マシンカタログ、およびデリバリーグループを作成するための十分な権限が必要です。詳細については、「委任管理の構成」を参照してください。
- Citrix Cloud™ は Cloud Connector を介して Nutanix Prism Central と通信します。したがって、Nutanix Prism Central インスタンスは Cloud Connector からアクセスできる必要があります。

機能の制限事項

Nutanix Prism および API の制限により、Windows VM でゲストの再起動やゲストのシャットダウンなどの電源操作が失敗する可能性があります。この問題を解決するには、ドキュメント「Prism または API から開始された電源操作が Windows VM で失敗する可能性がある」に記載されている Nutanix の指示に従って、VDA に設定を適用することをお勧めします。

主要な手順

1. Nutanix 仮想化環境をセットアップします。詳細については、インストールの準備 または 未使用のドメインのアクティブ化 を参照してください。
2. Nutanix AHV Prism Central への接続を作成する
3. Nutanix マシンテンプレートバージョンを使用してマシンカタログを作成する。

AHV 上の ニュタニックス プリズム エレメント

AHV 上の Nutanix Prism Element では、Citrix Virtual Apps and Desktops が Nutanix ハイパーバイザーを持つリソースの場所にホスト接続を作成する必要があるすべての Delivery Controller に Nutanix プラグインをインストールする必要があります。

主要な手順

1. Nutanix プラグインをインストールして登録します。
2. Nutanix 仮想化環境をセットアップします。詳細については、「リソースの種類を追加する」または「未使用のドメインをアクティブ化する」を参照してください。
3. 接続を作成します。
4. マシンカタログを作成します。

Nutanixプラグインのインストールと登録

すべてのCloud ConnectorにNutanixプラグインをインストールして登録する手順を完了します。Nutanixプラグインのインストールについては、Nutanixドキュメントサイトを参照してください。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- Nutanix 環境での接続の作成と管理については、Nutanix への接続 を参照してください。

詳細情報

- 接続とリソースの作成と管理
- マシンカタログの作成

Nutanix クラウドおよびパートナーソリューション

ニュータニックス AHV プリズムセントラル

Citrix Virtual Apps and Desktops は、Citrix管理のNutanix AHV Prism Centralプラグイン向けに、以下のクラウドハイパーバイザーで Nutanix Cloud Clusters (NC2) をサポートします。

- アマゾン ウェブ サービス (AWS)
- マイクロソフト アジュール

Nutanix クラウド クラスター

Citrix Virtual Apps and Desktopsは、AWSおよびAzure上のNutanix Cloud Clustersをサポートしています。Nutanixクラスターは、プライベートクラウドまたは複数のパブリッククラウドでアプリケーションを実行する方法を簡素化します。

NC2のセットアップの詳細については、以下を参照してください。

- AWS上でのNutanix Cloud Clustersの展開およびユーザーガイド
- Azure上でのNutanix Cloud Clustersの展開およびユーザーガイド。

要件

NC2を使用するには、次のアカウントが必要です。

- Nutanixアカウント
- AWSの場合：次の権限を持つAWSアカウント。
  - IAMFullAccess
  - AWSConfigRole
  - AWSCloudFormationFullAccess
- Azureの場合:
  - 有効な「NC2 on Azure」ライセンス
  - 次のいずれかのロールを含むAzureアカウント：
    - グローバル管理者
    - クラウドアプリケーション管理者
    - アプリケーション管理者
    - すべての権限

NC2 on Azureの権限

```
Microsoft.Compute/register/action

Microsoft.Compute/availabilitySets/write

Microsoft.Compute/availabilitySets/delete

Microsoft.Compute/disks/read

Microsoft.Compute/disks/write

Microsoft.Compute/disks/delete

Microsoft.Compute/locations/usages/read

Microsoft.Compute/availabilitySets/read

Microsoft.Compute/virtualMachines/*

Microsoft.Compute/snapshots/*

Microsoft.Compute/images/*

Microsoft.Network/register/action

Microsoft.Network/natGateways/*

Microsoft.Network/networkInterfaces/*

Microsoft.Network/networkSecurityGroups/*

Microsoft.Network/publicIPAddresses/*

Microsoft.Network/virtualNetworks/*

Microsoft.Network/locations/usages/read

Microsoft.Storage/register/action

Microsoft.Storage/checknameavailability/read Microsoft.Storage/locations/
checknameavailability/read Microsoft.Storage/locations/usages/read

Microsoft.Storage/storageAccounts/write
```

```
Microsoft.Storage/storageAccounts/read

Microsoft.Storage/storageAccounts/delete Microsoft.Storage/
storageAccounts/blobServices/containers/clearLegalHold/action
Microsoft.Storage/storageAccounts/blobServices/containers/delete
Microsoft.Storage/storageAccounts/blobServices/containers/lease/action

Microsoft.Storage/storageAccounts/blobServices/containers/ read
Microsoft.Storage/storageAccounts/blobServices/containers/ write
Microsoft.Storage/storageAccounts/blobServices/read Microsoft.Storage/
storageAccounts/blobServices/write Microsoft.Storage/storageAccounts/
listAccountSas/action Microsoft.Storage/storageAccounts/listkeys/action
Microsoft.Storage/storageAccounts/listServiceSas/action Microsoft.Storage/
storageAccounts/regeneratekey/action Microsoft.Storage/storageAccounts/
revokeUserDelegationKeys/action Microsoft.ResourceHealth/
AvailabilityStatuses/read Microsoft.ResourceHealth/events/read

Microsoft.ResourceHealth/AvailabilityStatuses/current/read

Microsoft.ManagedIdentity/userAssignedIdentities/* Microsoft.Resources/
subscriptions/locations/read Microsoft.Resources/subscriptions/
resourceGroups/read Microsoft.Resources/subscriptions/resourceGroups/write
Microsoft.Resources/subscriptions/resourceGroups/delete
Microsoft.Resources/subscriptions/resourcegroups/deployments/read

Microsoft.Resources/subscriptions/resourcegroups/deployments/write
Microsoft.Resources/subscriptions/resourcegroups/resources/read
Microsoft.Resources/subscriptions/tagNames/read Microsoft.Resources/
subscriptions/tagNames/write Microsoft.Resources/subscriptions/tagNames/
delete Microsoft.Resources/subscriptions/tagNames/tagValues/write
Microsoft.Resources/subscriptions/tagNames/tagValues/read
Microsoft.Resources/subscriptions/tagNames/tagValues/delete
Microsoft.Resources/tags/read

Microsoft.Resources/tags/write

Microsoft.Resources/tags/delete

Microsoft.Resources/providers/read

Microsoft.Compute/sshPublicKeys/read

Microsoft.Compute/sshPublicKeys/write
```

```
Microsoft.Compute/sshPublicKeys/delete Microsoft.Compute/sshPublicKeys/
generateKeyPair/action Microsoft.Nutanix/Interfaces/read

Microsoft.Nutanix/Interfaces/write

Microsoft.Nutanix/Interfaces/delete

Microsoft.Nutanix/Nodes/read

Microsoft.Nutanix/Nodes/write

Microsoft.Nutanix/Nodes/delete

Microsoft.Nutanix/register/action

Microsoft.Network/virtualHubs/*

Microsoft.Network/routeTables/read

Microsoft.Network/routeTables/write

Microsoft.Network/routeTables/delete

Microsoft.Network/routeTables/join/action

Microsoft.Network/routeTables/routes/read Microsoft.Network/routeTables/
routes/write Microsoft.Network/routeTables/routes/delete
Microsoft.CostManagement/query/read

Microsoft.CostManagement/views/read Microsoft.CostManagement/
externalSubscriptions/query/read Microsoft.CostManagement/
externalSubscriptions/dimensions/read Microsoft.CostManagement/
externalSubscriptions/read Microsoft.CostManagement/
externalBillingAccounts/forecast/read

Microsoft.CostManagement/externalBillingAccounts/read

Microsoft.CostManagement/externalBillingAccounts/query/read
Microsoft.CostManagement/externalBillingAccounts/ externalSubscriptions/
read Microsoft.CostManagement/externalSubscriptions/forecast/read
Microsoft.CostManagement/operations/read Microsoft.CostManagement/
forecast/read
```

```
Microsoft.Network/virtualWans/write

Microsoft.Network/virtualWans/read

Microsoft.Network/virtualWans/delete Microsoft.Network/virtualWans/
virtualHubs/read Microsoft.Network/virtualWans/join/action
Microsoft.Network/virtualHubs/hubVirtualNetworkConnections/ read
Microsoft.Network/virtualHubs/hubVirtualNetworkConnections/ write
Microsoft.Network/virtualHubs/hubVirtualNetworkConnections/ delete
Microsoft.Network/privateEndpoints/pushPropertiesToResource/ action
Microsoft.Network/privateEndpoints/read

Microsoft.Network/privateEndpoints/write Microsoft.Network/
privateEndpoints/delete Microsoft.Network/privateDnsZones/read
Microsoft.Network/privateDnsZones/delete Microsoft.Network/
privateDnsZones/join/action Microsoft.Network/privateDnsZones/write
Microsoft.Network/privateEndpoints/privateDnsZoneGroups/ write

Microsoft.Network/privateEndpoints/privateDnsZoneGroups/read
Microsoft.Network/privateEndpoints/privateDnsZoneGroups/delete

Microsoft.Storage/storageAccounts/blobServices/containers/blobs/add/action
Microsoft.Storage/storageAccounts/blobServices/containers/blobs/delete

Microsoft.Storage/storageAccounts/blobServices/containers/blobs/
deleteBlobVersion/action

Microsoft.Storage/storageAccounts/blobServices/containers/blobs/filter/
action Microsoft.Storage/storageAccounts/blobServices/containers/ blobs/
read Microsoft.Storage/storageAccounts/blobServices/containers/blobs/tags/
read

Microsoft.Storage/storageAccounts/blobServices/containers/blobs/tags/write
Microsoft.Storage/storageAccounts/blobServices/containers/ blobs/write
Microsoft.Storage/storageAccounts/blobServices/containers/blobs/filter/
action Microsoft.Storage/storageAccounts/blobServices/containers/blobs/
modifyPermissions/action
```

Nutanix クラスターを作成する

1. Nutanix アカウントにログインします。

2. Nutanix クラスターオプションに移動し、**Launch** をクリックします。**Nutanix Console** が開きます。詳細については、以下を参照してください。
    - AWS で Nutanix クラスターを開始する
    - Microsoft Azure 上の ニュータニックス クラウド クラスターズ
3. 新しい VPC を作成するオプションを選択します。

クラスターが作成されたら、Nutanix Prism のアドレスを取得します。

トラブルシューティング

クラスター作成プロセスは、以下のエラーで失敗する可能性があります。

- **指定された時間内にクラスターを作成できませんでした。クラスターを削除しています**
- **ホスト Nutanix クラスター - ノード XXXXXXXXXXX: インスタンス i-xxxxxxxxxxxxx: ネットワークインターフェースのソース/宛先チェックを無効にするエラー.**
- **ホスト Nutanix クラスター - ノード XXXXXXXXXXX: インスタンス i-xxxxxxxxxxxxxx のネットワークインターフェース情報を取得できません**

クラスターの作成に失敗した場合は、別のリージョンで再作成してみてください。再試行する前に、Nutanix CloudFormation Stack (CFS) を必ず削除してください。

> **注:**

> 他のリソースに加えて、Nutanix CFS は以下を作成します。

> - Nutanix Cluster xxxxxxxxxxxx 10.0.0.0/16 という名前の VPC を 1 つ
> - 2 つのサブネット 10.0.128.0/24 と 10.0.129.0/24
> - 1つのインターネットゲートウェイ
> - 1つのNATゲートウェイ

Prismサーバーアドレスの取得

1. NC2クラスターをPrism Centralサーバーに登録します。「Registering a Cluster with Prism Central」を参照してください。
2. Prism Centralサーバーのホスト名またはIPアドレスをアドレスとして使用します。

ニュータニックス プリズム エレメント 用 NC2

Citrix Virtual Apps and Desktops は、Nutanix Prism Element プラグイン向けに、以下のクラウドハイパーバイザーで Nutanix Cloud Clusters (NC2) をサポートします。

- アマゾン ウェブ サービス (AWS)

AWS 上のニュータニックス クラウドクラスター

AWS 上の Nutanix Cloud Clusters の詳細については、「Nutanix Cloud Clusters on AWS Deployment and User Guide」を参照してください。

> **ヒント:**
>
> このサポートは、Nutanix オンプレミス クラスターと同じ機能を提供します。サポートされるクラスターは、*Prism Element* のみです。詳細については、こちらを参照してください。

> AWS で NC2 を使用するには、次のアカウントが必要です。

- Nutanix アカウント
- 次の権限を持つ AWS アカウント:
  - IAMFullAccess
  - AWSConfigRole
  - AWSCloudFormationFullAccess

Nutanix クラスターの作成、およびクラスター作成が失敗した場合のトラブルシューティングについては、「Create a Nutanix Cluster」と「Troubleshooting」を参照してください。

クラスターが作成されたら、**Nutanix Prism**のアドレスを取得します。

Prismサーバーのアドレスを取得する

1. **Nutanix Console**に移動します。
2. コンソールの右上隅で、**Launch Prism Element**リンクにカーソルを合わせ、URLをコピーします。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール

- サイトの作成
- Nutanixクラウドおよびパートナーソリューションの接続を作成および管理するには、「Nutanixクラウドおよびパートナーソリューションへの接続」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

Oracle C3 仮想化環境 (プレビュー)

Citrix Virtual Apps and Desktops は、Citrix Virtual Apps and Desktops コントロールプレーン内の Citrix 管理の Oracle C3 プラグインを介して、Oracle Compute Cloud@Customer (Oracle C3) ワークロードを管理します。このプラグインを使用すると、Oracle C3 への接続を作成し、カタログを作成し、カタログ内のマシンの電源管理を行うことができます。

> **注:**
>
> - Citrix Virtual Apps and Desktops 2603 用の Oracle C3 は、ハイブリッド権限またはユニバーサルライセンスを持つお客様のみが利用できます。
> - 分離された Oracle C3 環境は現在サポートされていません。

前提条件

開始する前に:

- Oracle C3 REST API が環境で利用可能であることを確認してください。API 接続には Oracle C3 の `<system_name>.<domain name>` が必要です。Using the API to Manage Compute Cloud@Customer Resources を参照してください。
- Oracle C3 認証に使用される IAM 構成 `.ini` ファイルと秘密鍵を準備します。リージョンが `<system_name>.<domain_name>` に設定されていることを確認してください。
- Oracle C3 がプライベート CA 証明書によって保護されている場合は、接続設定時に信頼性検証用の証明書サムプリントを取得してください。

主な手順

1. Oracle C3 環境をセットアップします。
2. Oracle C3 エンドポイントへの接続を作成します。

3. マシンカタログを作成します。

> **注:**
>
> カタログを作成する前に、1 つ以上の Oracle C3 マシンが利用可能であり、それらのマシンに VDA がインストールされていることを確認してください。

4. デリバリーグループを作成します。
5. 残っている管理されていない Oracle C3 マシンを、管理対象カタログまたはデリバリーグループに移行します。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- 接続の作成と管理については、Connection to Oracle C3 を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

Red Hat OpenShift 仮想化環境

Citrix® は、Citrix が管理する OpenShift プラグインを介して、Red Hat OpenShift ワークロードを管理します。このプラグインを使用すると、OpenShift クラスターへのホスティング接続とホスティングユニットの作成、カタログの作成、およびカタログ内のマシンの電源管理を行うことができます。

以下の構成がサポートされています。

- **ネットワークオプション:**
  - Linux Bridge および OVS Bridge: クラスターネットワークで利用可能です。
- **ストレージオプション:**
  - ローカルストレージ: ノード上の永続ストレージでサポートされています。

- Red Hat OpenShift Data Foundation (ODF) ブロックストレージ: クラスター全体の分散ブロックストレージでサポートされています。「ODF ブロックストレージの構成」を参照してください。

> **ODF ブロックストレージの構成**
>
> Citrix は、マシンカタログに ODF ブロックストレージ `(ocs-storagecluster-ceph-rbd)` をサポートしています。 OpenShift プラグインは、Containerized Data Importer (CDI) を介して VM ディスクをプロビジョニングします。CDI は、ストレージクラスごとに StorageProfile を公開します。ホスティングユニットを作成する前に、以下を構成してください。
>
> - CDI を含む OpenShift Virtualization (CNV) をインストールします。ODF ブロックストレージクラスと同じ名前の StorageProfile が存在することを確認します。
> - その StorageProfile で、`accessModes` と `volumeMode` が設定されていることを確認します。
> - `dataImportCronSourceFormat`が設定されていることを確認します。`snapshot` に設定されている場合は、`snapshotClass`も設定されており、スナップショットクラスがストレージクラスと同じCSIドライバーを使用していることを確認します。— ODFブロックストレージの場合は、*openshift-storage.rbd.csi.ceph.com*。

- **NetApp ストレージ:** エンタープライズグレードの外部ストレージ統合でサポートされています。

主な手順

- Red Hat OpenShift 環境をセットアップします。
- OpenShift クラスターへの接続とリソースを作成します。
- マシンカタログを作成します。
- デリバリーグループを作成します。

Red Hat OpenShift 環境をセットアップする

1. *OpenShift クラスターを作成し、クラスター API アドレスを取得する*: OpenShift コンソールで、クラスターをセットアップした後、**Home > Overview > Details** に移動し、クラスター API アドレスを取得します。

2. 「*サービスアカウントを作成し、OpenShiftコマンドラインインターフェイス (CLI) (ocコマンド) を使用してサービスアカウントトークンを取得します*」: サービスアカウントトークンは、サービスアカウントに関連付けられた認証資格情報です。サービスアカウントは、OpenShiftプラグインをOpenShiftで認証するために使用されます。各サービスアカウントは、1つの名前空間に関連付けられています。
3. 「*サービスアカウントの権限を構成します*」: サービスアカウントには複数のロールを設定でき、各ロールはOpenShiftプラグインがどのリソースに対してどのようなアクションを実行できるかを定義する権限で構成されます。ロールは**ロールバインディング**を介してバインドされ、**ロールバインディング**には次の2種類があります。

    a. **クラスター全体のロールバインディング**: OpenShiftからイベントを受信するために使用されます。 名前空間にバインドされたロールバインディング: 特定の名前空間でVMを管理するために使用されます。

    b. **名前空間にバインドされたロールバインディング**: 特定の名前空間でVMを管理するために使用されます。

4. 「*名前空間 (プロジェクト) を作成します*」: OpenShiftの名前空間は、VMやネットワークなどのリソースをグループ化する分離された環境であり、より良い整理とアクセス制御を可能にします。**名前空間**はKubernetesの用語であり、**プロジェクト**はOpenShiftの用語です。OpenShiftプラグインの観点からは、これらは同じです。VMを展開するには名前空間が必要です。OpenShiftコンソールまたはOpenShift Container Platform CLIを使用して名前空間を作成します。
5. 「*ターゲットの名前空間の下にネットワークアタッチメント定義を1つ作成します*」: ネットワークアタッチメント定義は、OpenShiftで実行されているVMのネットワーク構成を指定します。**Networking > NetworkAttachmentDefinitions**の下で、各名前空間のネットワークアタッチメント定義を確認できます。
6. 「*ストレージクラスを構成します*」: ストレージクラスは、VMストレージがどのように割り当てられるかを定義します。**Storage > StorageClass**の下で、ストレージプロバイダーのリストを構成および確認できます。

サービスアカウントを作成する

1. ocコマンドラインツールをダウンロードして解凍します。
2. ログインIDを使用してOpenShiftコンソールにアクセスします。
3. ユーザープロファイルをクリックし、**ログインコマンドをコピー**をクリックします。
4. **トークンを表示**をクリックし、トークンをコピーします。
5. ocコマンドラインを使用してログインコマンドを実行します。例:

```
.\oc.exe login --token=<token> --server=<server address>
```

6. サービスアカウントを作成します。

   - デフォルトの名前空間の下にサービスアカウントを作成する場合は、次を実行します。

     ```
     .\oc.exe create sa <service account name>
     ```

   - 独自のネームスペースでサービスアカウントを作成する場合は、次を実行します。

     ```
     .\oc.exe create sa <service account name> -n mynamespace
     ```

7. シークレット用の `YAML` ファイルを作成します。例:

   - デフォルトのネームスペースでサービスアカウントを作成する場合:

     ```
     apiVersion: v1

     kind: Secret

     metadata:

     name: service account name

     annotations:

     kubernetes.io/service-account.name: service account name

     type: kubernetes.io/service-account-token
     ```

   - 独自のネームスペースでサービスアカウントを作成する場合:

     ```
     apiVersion: v1

     kind: Secret

     metadata:

     name: service account name
     ```

```
namespace: mynamespace

annotations:

kubernetes.io/service-account.name: service account name

 type: kubernetes.io/service-account-token
```

8. YAMLを適用します。

```
.\oc.exe apply -f <yamlFile.yaml>
```

注:

`oc` はトークンを取得するためのシークレットを記述します。トークンはパスワードとして使用されます。

サービスアカウントのロールとロールバインディングを作成する

クラスター全体のロールバインディングにより、サービスアカウントはクラスター全体のすべてのVMイベントを読み取る権限を持ち、OpenShiftプラグインがすべてのVM関連イベントに対して単一のイベントウォッチャーを維持できるようになります。 ネームスペースロールバインディングにより、サービスアカウントはターゲットネームスペース内のVMを管理する権限を持ちます。 スクリプトを使用してロールを作成し、それらをサービスアカウントにバインドできます。 `<https://github.com/citrix/citrix-mcs-sdk-samples/tree/main/OpenShift/Hosting%20Connection/Role/>` を参照してください。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- 接続の作成と管理については、Red Hat OpenShiftへの接続 を参照してください。

詳細情報

- 接続とリソースの作成および管理

- マシンカタログの作成

VMware 仮想化環境

仮想マシンを提供するのにVMwareを使用する場合は、このガイダンスに従ってください。

vCenter Serverと適切な管理ツールをインストールします。(vSphere vCenter Linked Mode操作はサポートされていません。)

MCSを使用する予定がある場合は、vCenter ServerのDatastore Browser機能（`<https://kb.vmware.com/s/article/2101567>`で説明）を無効にしないでください。この機能を無効にすると、MCSは正しく動作しません。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- VMware環境での接続の作成と管理については、「Connection to VMware」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

VMware クラウドおよびパートナーソリューション

Citrix Virtual Apps and Desktops™ は、以下の VMware クラウドおよびパートナーソリューションをサポートしています。

- Azure VMware ソリューション (AVS)(#azure-vmware-solution-avs-integration)
- Google Cloud VMware エンジン(#google-cloud-vmware-engine)
- VMware クラウド オン Amazon Web Services (AWS)(#vmware-cloud-on-amazon-web-services-aws)

Azure VMware ソリューション (AVS) の統合

Citrix Virtual Apps and Desktop サービスは AVS をサポートしています。AVS は、Azure インフラストラクチャによって作成された vSphere クラスターを含むクラウドインフラストラクチャを提

供します。Citrix Virtual Apps and Desktop サービスを活用して、オンプレミス環境で vSphere を使用する場合と同じ方法で、AVS を使用して VDA ワークロードをプロビジョニングします。

AVS クラスターのセットアップ

Citrix Virtual Apps™ and Desktop サービスで AVS を使用できるようにするには、Azure で次の手順を実行します。

- ホストクォータを要求する
- Microsoft.AVS リソース プロバイダーを登録する
- ネットワークチェックリスト
- Azure VMware Solution プライベートクラウドを作成する
- Azure VMware Solution プライベートクラウドにアクセスする
- AzureでVMwareプライベートクラウドのネットワークを構成する
- Azure VMware Solution の DHCP を構成する
- Azure VMware Solution にネットワークセグメントを追加する
- Azure VMware Solution 環境を確認する

AZURE ENTERPRISE AGREEMENTのお客様のホストクォータを要求する

Azureポータルの**ヘルプとサポート**ページで、**新しいサポートリクエスト**を選択し、次の情報を含めます。

- 問題の種類: 技術
- サブスクリプション: サブスクリプションを選択してください
- サービス: すべてのサービス > Azure VMware Solution
- リソース: 一般的な質問
- 概要: 容量が必要
- 問題の種類: 容量管理の問題
- 問題のサブタイプ: 追加のホストクォータ/容量に関する顧客からの要求

サポートチケットの に、 タブで次の情報を含めます。

- POC または本番環境
- リージョン名
- ホスト数
- その他の詳細

注:

AVS には最低 3 つのホストが必要であり、N+1 ホストの冗長性を使用することをお勧めします。

サポート チケットの詳細を指定したら、 を選択して Azure にリクエストを送信します。

MICROSOFT.AVS リソース プロバイダーを登録する

ホスト クォータを要求した後、リソース プロバイダーを登録します。

1. Azure portal にサインインします。
2. Azure portal メニューで、 を選択します。
3. メニューで、サブスクリプションを入力し、 を選択します。
4. サブスクリプション リストからサブスクリプションを選択します。
5. を選択し、検索バーに **Microsoft.AVS** と入力します。
6. リソース プロバイダーが登録されていない場合は、 を選択します。

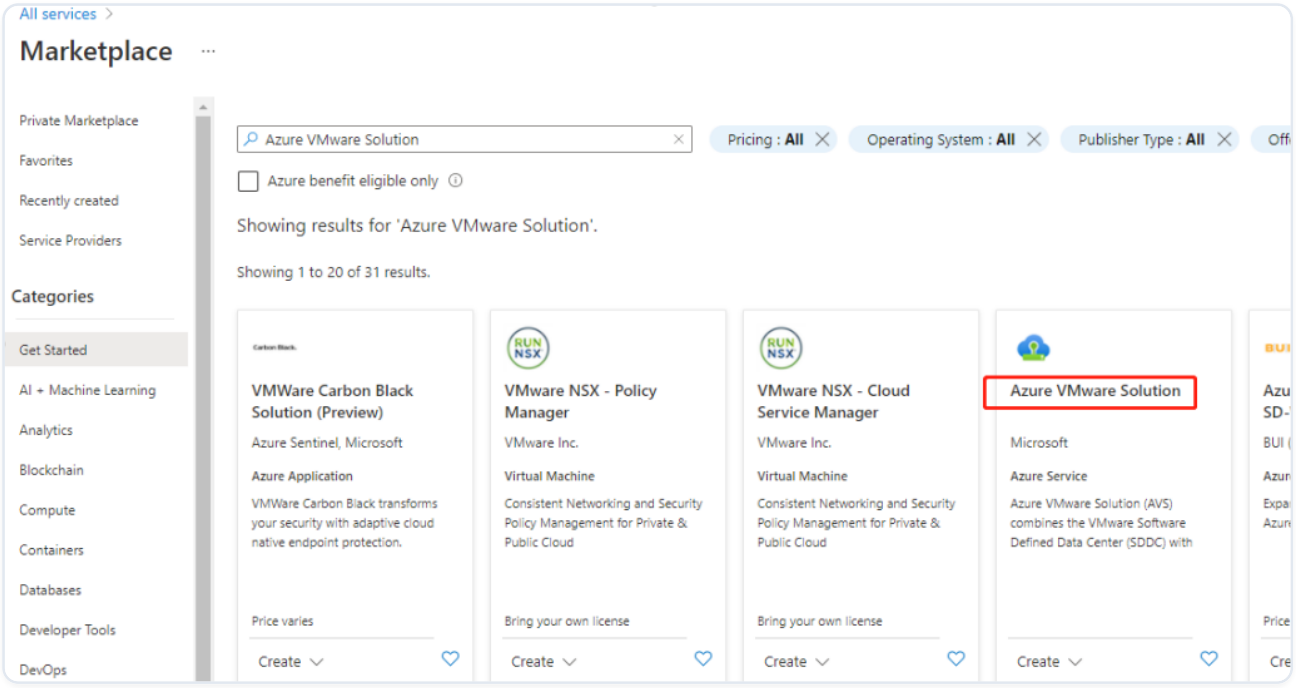
ネットワークに関する考慮事項

AVSは、特定のネットワークアドレス範囲とファイアウォールポートを必要とするネットワークサービスを提供します。詳細については、Azure VMware Solution のネットワーク計画チェックリストを参照してください。

AZURE VMWARE SOLUTION プライベートクラウドを作成する

環境のネットワーク要件を考慮した後、AVS プライベートクラウドを作成します。

1. Azureポータルにサインインします。
2. **新しいリソースの作成**を選択します。
3. **Marketplace の検索**テキストボックスに、*Azure VMware Solution*と入力し、リストから**Azure VMware Solution**を選択します。



image

Azure VMware Solutionウィンドウで、:

1. **作成**を選択します。
2. タブをクリックします。
3. 以下の表の情報を使用して、フィールドに値を入力します。

フィールド	値
サブスクリプション	展開に使用するサブスクリプションを選択します。Azure サブスクリプション内のすべてのリソースはまとめて請求されます。
リソースグループ	プライベートクラウドのリソースグループを選択します。Azure リソースグループは、Azure リソースがデプロイおよび管理される論理コンテナです。または、プライベートクラウド用に新しいリソースグループを作成することもできます。
場所	east us などの場所を選択します。これは、計画フェーズで定義したリージョンです。
リソース名	Azure VMware Solution プライベートクラウドの名前を指定します。

フィールド	値
SKU	AV36 を選択します。
ホスト	プライベートクラウドクラスターに割り当てられたホストの数を示します。デフォルト値は3で、デプロイ後に増減できます。
アドレスブロック	プライベートクラウドの IP アドレスブロックを指定します。CIDR はプライベートクラウド管理ネットワークを表し、vCenter Server や NSX-T Manager などのクラスター管理サービスに使用されます。/22 アドレス空間を使用します（例: 10.175.0.0/22）。アドレスは一意であり、他の Azure 仮想ネットワークやオンプレミスネットワークと重複しないようにしてください。
仮想ネットワーク	Azure VMware Solution ExpressRoute 回線は展開後の手順で確立されるため、ここは空白のままにします。

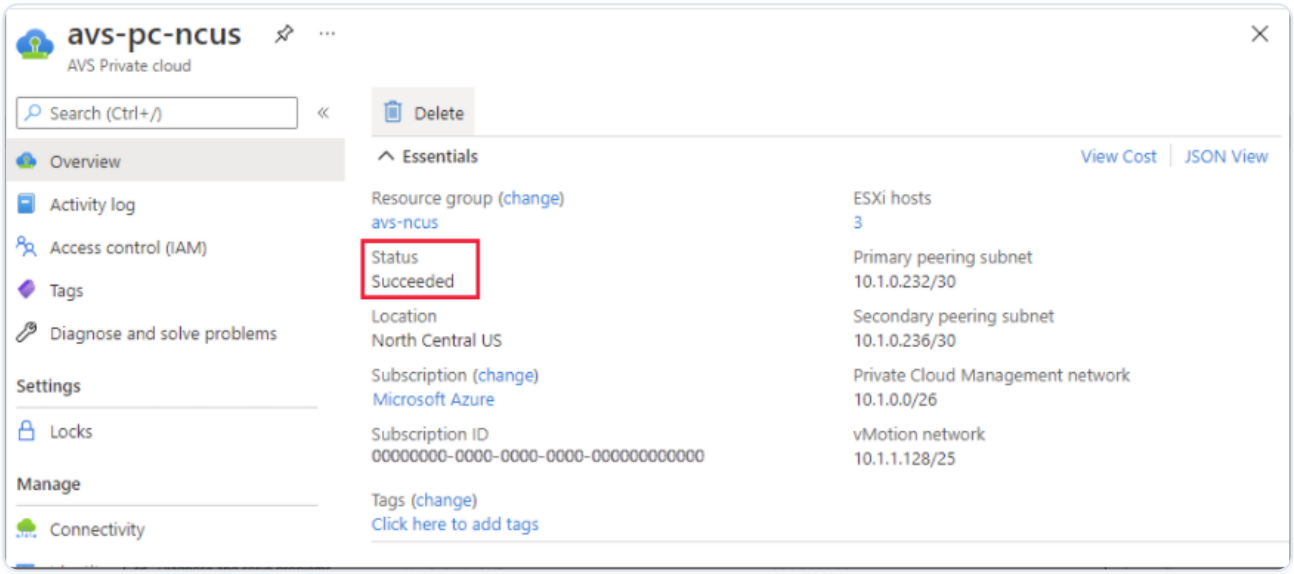
プライベートクラウドの作成画面で：

1. フィールドで、AVS が存在するリージョンを選択します。リソースグループのリージョンは AVS リージョンと同じです。
2. フィールドで、 を選択します。
3. 「**アドレスブロック**」フィールドにIPアドレスを指定します。例: 10.15.0.0/22。
4. 「**確認 + 作成**」を選択します。
5. 情報を確認したら、「**作成**」をクリックします。

Azure ASV プライベートクラウドの作成(/en-us/citrix-virtual-apps-desktops/current-release/media/azure-avs-create-private-cloud.png)

> **ヒント:**
>
> プライベートクラウドの作成には3〜4時間かかる場合があります。クラスターに単一のホストを追加するには30〜45分かかる場合があります。

> 展開が成功したことを確認します。作成したリソースグループに移動し、プライベートクラウドを選択します。**ステータス**が**成功**になったら、展開は完了です。



AZURE VMWARE SOLUTION プライベートクラウドへのアクセス

プライベートクラウドを作成したら、Windows VMを作成し、プライベートクラウドのローカルvCenterに接続します。
新しいWindows仮想マシンの作成

1. リソースグループで、**+ 追加**を選択し、**Microsoft Windows 10/2016/2019**を検索して選択します。
2. **作成**をクリックします。
3. 必要な情報を入力し、「**確認 + 作成**」を選択します。
4. 検証が完了したら、「**作成**」を選択して仮想マシンの作成プロセスを開始します。

プライベートクラウドのローカルvCenterに接続する

1. クラウド管理者として **vSphere Client with VMware vCenter SSO** にサインインします。

   Azure ASV vSphere ログイン(/en-us/citrix-virtual-apps-desktops/current-release/media/azure-avs-vsphere-login.png)

2. Azure portal でプライベートクラウドを選択し、 **>** を選択します。

プライベートクラウドのvCenterおよびNSX-T ManagerのURLとユーザー資格情報が表示されます。

Azure ASV セットアップ vCenter(/en-us/citrix-virtual-apps-desktops/current-release/media/azure-avs-setup-vcenter.png)

URLとユーザー資格情報を確認した後:

1. 前の手順で作成したVMに移動し、仮想マシンに接続します。
2. Windows VMでブラウザを開き、vCenterとNSX-T ManagerのURLを2つのブラウザタブで開きます。vCenterタブで、前の手順で取得した*cloudadmin@vmcp.local*ユーザーの資格情報を入力します。

AZUREでVMWAREプライベートクラウドのネットワークを構成する

ASVプライベートクラウドにアクセスした後、仮想ネットワークとゲートウェイを作成してネットワークを構成します。
仮想ネットワークを作成する

1. Azure portal にサインインします。
2. 以前に作成したリソースグループに移動します。
3. 新しいリソースを定義するには、 を選択します。
4. テキストボックスに「*仮想ネットワーク*」と入力します。仮想ネットワークリソースを見つけて選択します。
5. 「**仮想ネットワーク**」ページで、「**作成**」を選択してプライベートクラウドの仮想ネットワークを設定します。
6. 「**仮想ネットワークの作成**」ページで、仮想ネットワークの詳細を入力します。
7. 「**基本**」タブで、仮想ネットワークの名前を入力し、適切なリージョンを選択して、「**次へ：IPアドレス**」をクリックします。
8. 「**IPアドレス**」タブのIPv4アドレス空間で、以前に作成したアドレスを入力します。

> **重要:**
>
> プライベートクラウドを作成したときに使用したアドレス空間と重複しないアドレスを使用してください。

> アドレス空間を入力した後:

1. 「**+ サブネットの追加**」を選択します。
2. 「**サブネットの追加**」ページで、サブネットに名前と適切なアドレス範囲を割り当てます。
3. 「**追加**」をクリックします。
4. 「**確認 + 作成**」を選択します。

5. 情報を確認し、「**作成**」をクリックします。デプロイが完了すると、仮想ネットワークがリソースグループに表示されます。

仮想ネットワークゲートウェイを作成する
仮想ネットワークを作成した後、仮想ネットワークゲートウェイを作成します。

1. リソースグループで、「**+ 追加**」を選択して新しいリソースを追加します。
2. 「**Search the Marketplace**」テキストボックスに「*virtual network gateway*」と入力します。仮想ネットワークリソースを見つけて選択します。
3. 「**Virtual Network gateway**」ページで、「**Create**」をクリックします。
4. 「**Create virtual network gateway**」ページの「**Basics**」タブで、フィールドに値を入力します。
5. 「**Review + create**」をクリックします。

Azure ASV セットアップ vCenter(/en-us/citrix-virtual-apps-desktops/current-release/media/azure-avs-create-virtual-gateway.png)

仮想ネットワークゲートウェイの構成を確認したら、**作成**をクリックして仮想ネットワークゲートウェイを展開します。 展開が完了したら、**ExpressRoute**接続をAzure AVSプライベートクラウドを含む仮想ネットワークゲートウェイに接続します。

EXPRESSROUTEを仮想ネットワークゲートウェイに接続する

仮想ネットワークゲートウェイを展開した後、それとAzure AVSプライベートクラウドの間に接続を追加します。

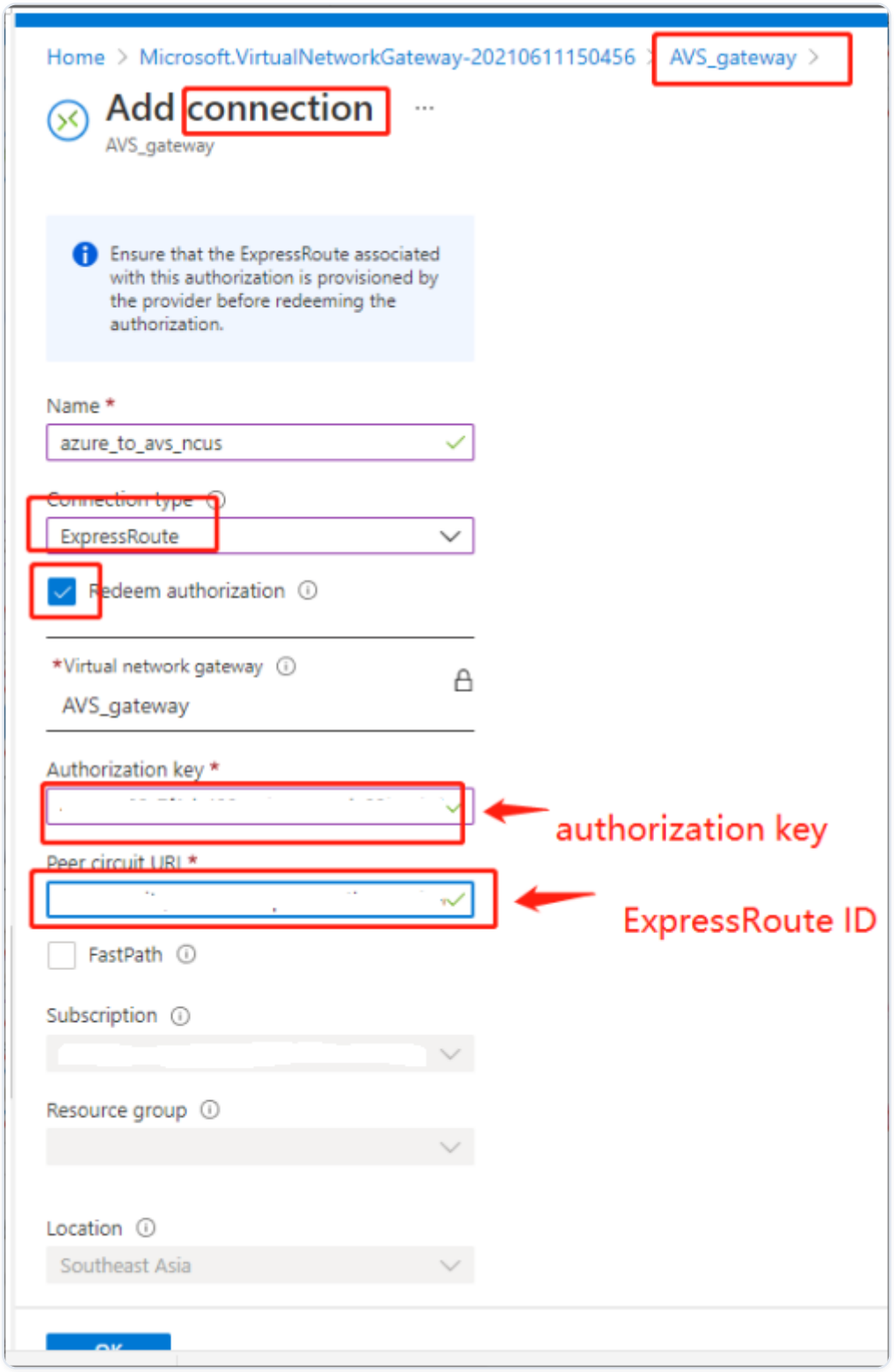
1. ExpressRoute承認キーを要求します。
2. Azureポータルで、**Azure VMware Solution private cloud**に移動します。「**Manage> Connectivity > ExpressRoute**」を選択し、次に「**+ Request an authorization key**」を選択します。

Azure ASV 承認キーの要求(/en-us/citrix-virtual-apps-desktops/current-release/media/azure-avs-expressroute.png)

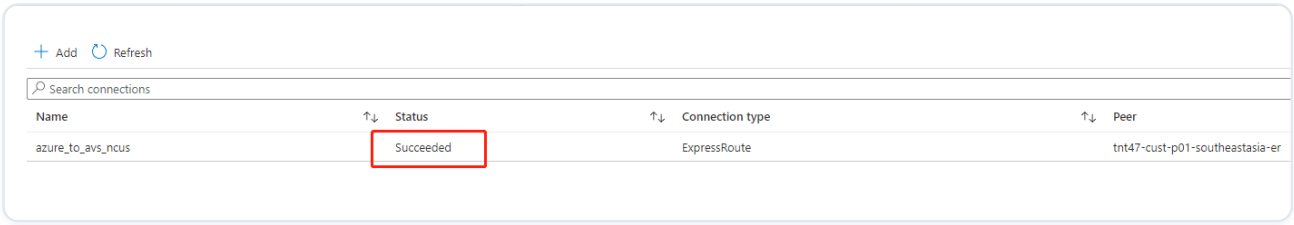
承認キーを要求した後：

1. キーの名前を入力し、「**Create**」をクリックします。キーの作成には約30秒かかる場合があります。作成されると、新しいキーはプライベートクラウドの承認キーのリストに表示されます。
2. **承認キー**と**ExpressRoute ID**をコピーします。これらはピアリングプロセスを完了するために必要です。承認キーはしばらくすると消えるため、表示されたらすぐにコピーしてください。

3. 使用する**仮想ネットワークゲートウェイ**に移動し、「**Connections> + Add**」を選択します。
4. 「**接続の追加**」ページで、フィールドの値を入力し、「**OK**」を選択します。



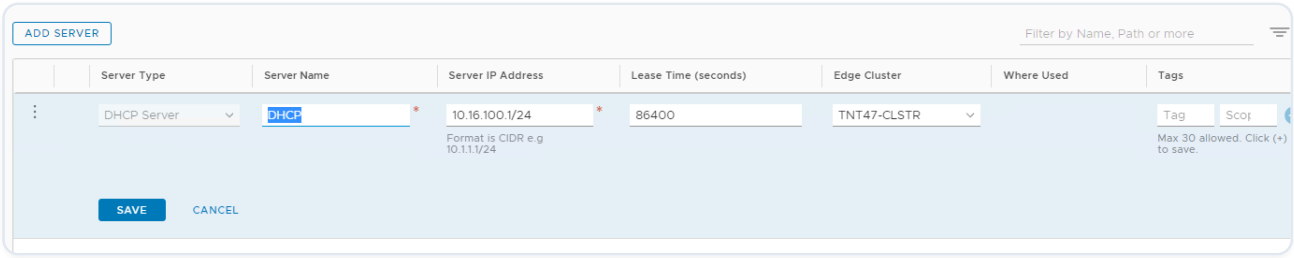
ExpressRoute回線と仮想ネットワーク間の接続が確立されます。



AZURE VMWARE SOLUTION の DHCP を構成する

ExpressRouteを仮想ゲートウェイに接続した後、DHCPを構成します。
NSX-T を使用して DHCP サーバーをホストする
NSX-T Manager で、次の手順を実行します。

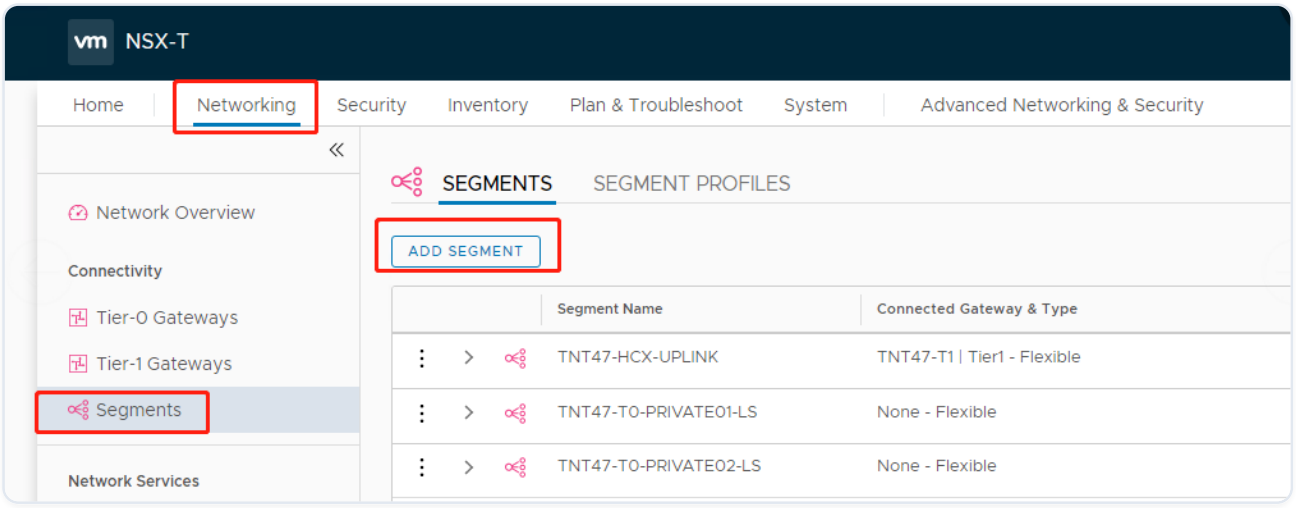
1. **「ネットワーク」>「DHCP」**の順に選択し、**「サーバーの追加」**を選択します。
2. **「サーバーの種類」で「DHCP」**を選択し、サーバー名とIPアドレスを入力します。
3. 「**保存**」をクリックします。
4. **「Tier 1 ゲートウェイ」を選択し、Tier-1 ゲートウェイの縦の省略記号を選択して、「編集」**を選択します。
5. サブネットを追加するには、**「IP割り当てなし」**を選択します。
6. **「種類」で「DHCPローカルサーバー」**を選択します。
7. **「DHCPサーバー」で「Default DHCP」を選択し、「保存」**をクリックします。
8. もう一度**Save**をクリックし、**Close Editing**を選択します。



AZURE VMWARE SOLUTIONでネットワークセグメントを追加する

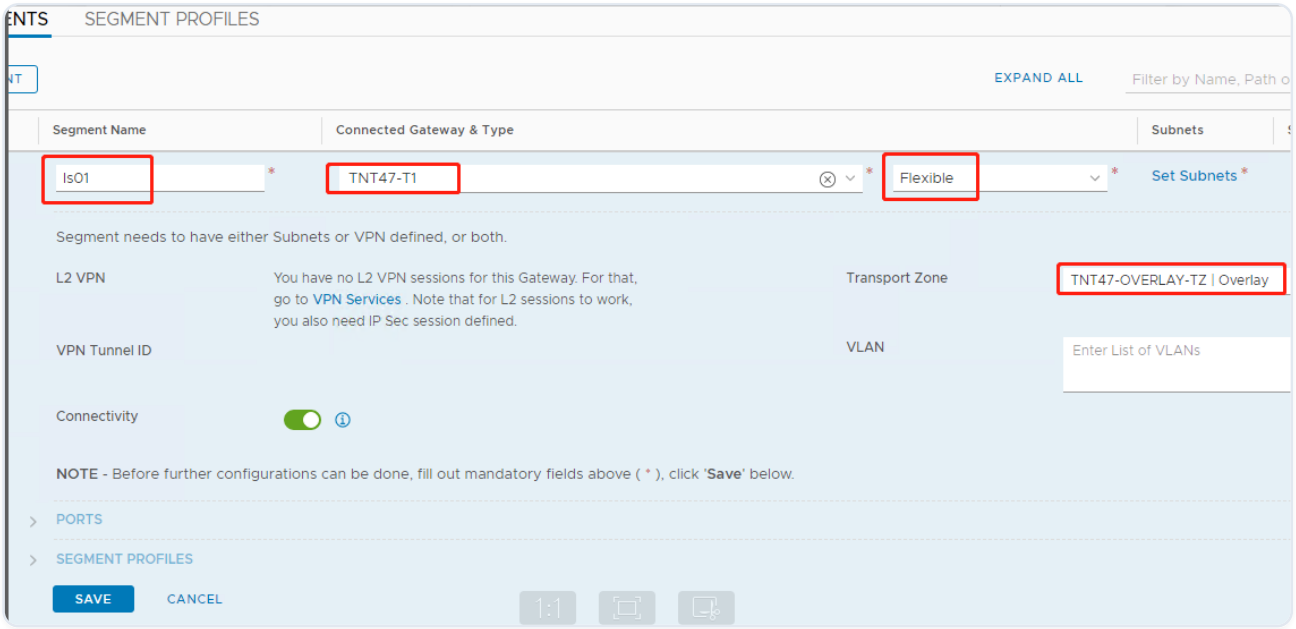
DHCPを設定した後、ネットワークセグメントを追加します。

ネットワークセグメントを追加するには、NSX-T Managerで**Networking> Segments**を選択し、**Add Segment**をクリックします。



Segments profile画面で：

1. セグメントの**name**を入力します。
2. **Tier-1 Gateway (TNTxx-T1)**を**Connected Gateway**として選択し、**Type**は**Flexible**のままにします。
3. 事前設定されたオーバーレイ**Transport Zone(TNTxx-OVERLAY-TZ)**を選択します。
4. **Set Subnets**をクリックします。



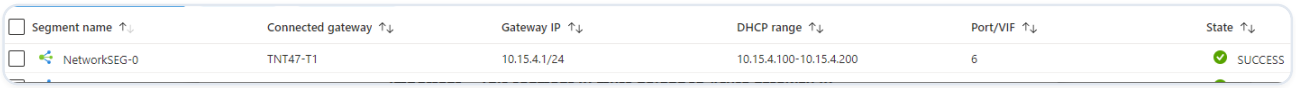
Subnetsセクションで：

1. ゲートウェイIPアドレスを入力します。
2. **Add**を選択します。

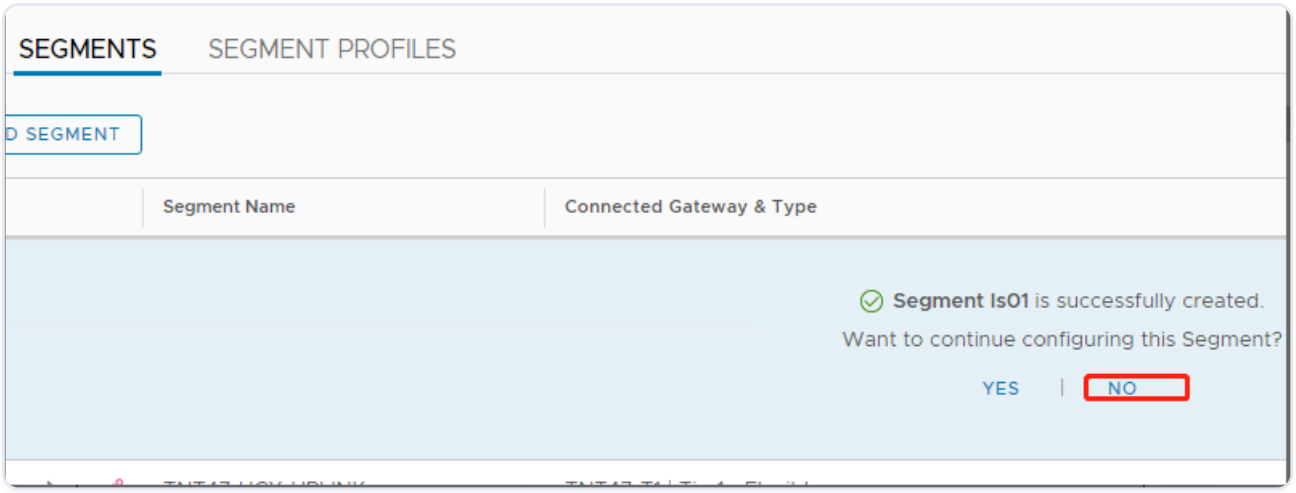
> **重要:**

> このセグメントのIPアドレスは、Azureゲートウェイの IPアドレス (10.15.0.0/22) に属している必要があります。

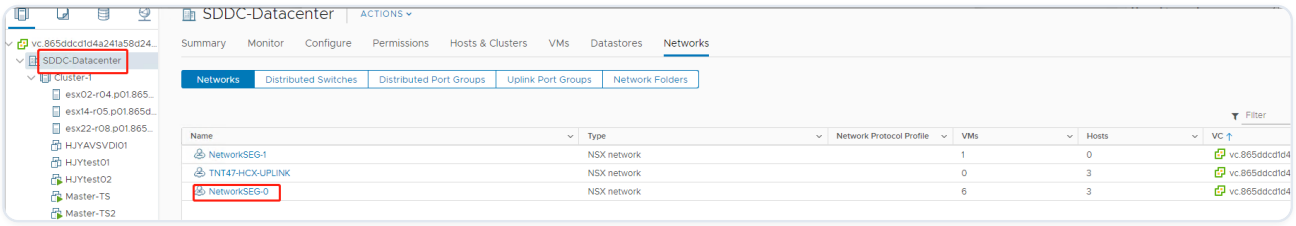
> DHCP範囲はセグメントIPアドレスに属している必要があります。



セグメントの構成を続行するオプションを拒否するには、 を選択します:

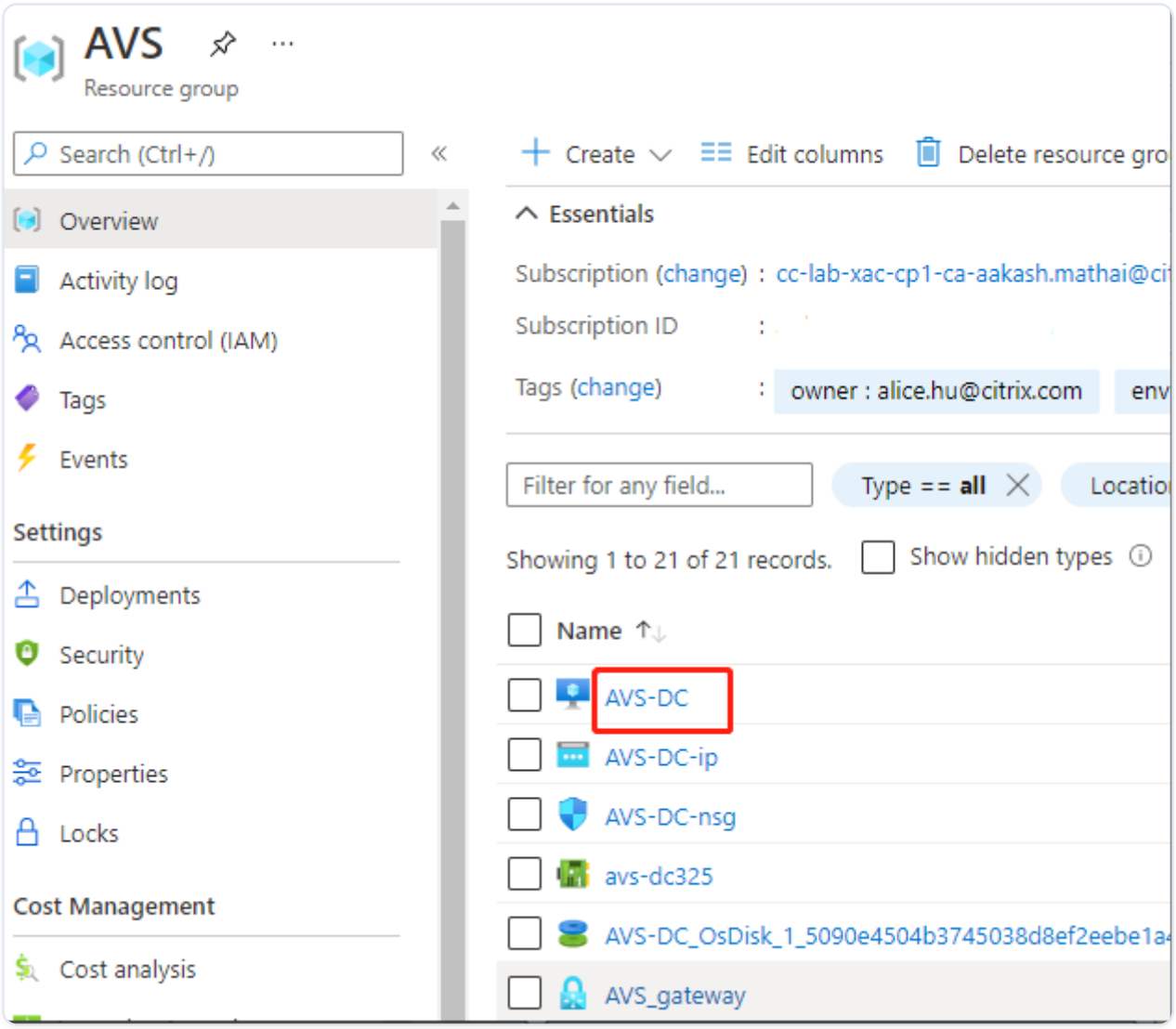


vCenterで、 > を選択します:

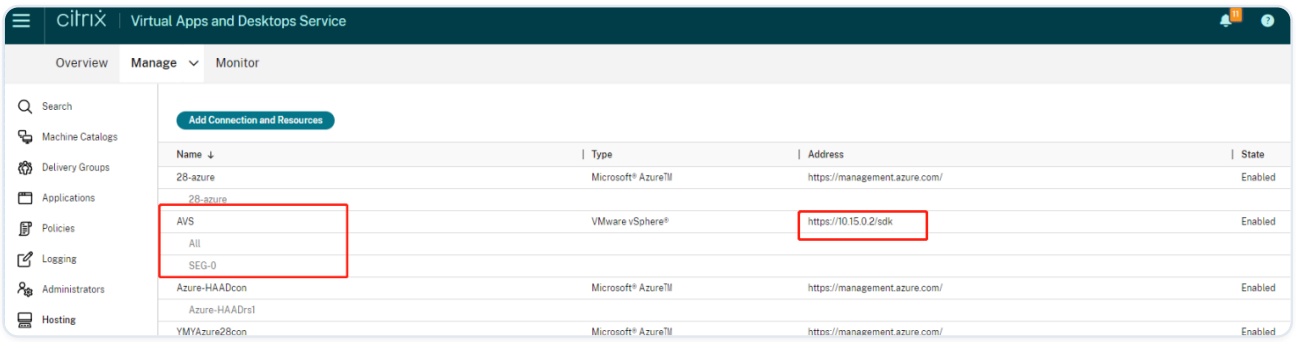


AZURE AVS環境の検証

Azureリソースグループで直接接続とコネクタを設定します。



vCenterの資格情報で接続を確認します。



グーグル クラウド ヴイエムウェア エンジン

Citrix Virtual Apps and Desktopsを使用すると、VMwareベースのオンプレミスCitrixワークロードをGoogle Cloud VMware Engineに移行できます。

Google Cloud VMware Engineを構成する

以下の手順では、Google Cloud VMware Engineでクラスターを取得してセットアップする方法について説明します。

VMWARE ENGINEポータルにアクセスする

1. **Google Cloud Console**で、ナビゲーションメニューをクリックします。
2. **Compute**セクションで、**VMware Engine**をクリックして、新しいブラウザータブでVMware Engineを開きます。

最初のプライベートクラウドを作成するための要件

Google Cloud VMware Engineへのアクセス、利用可能なVMware Engineノードクォータ、および適切なIAMロールが必要です。プライベートクラウドの作成を続行する前に、以下の要件を準備してください。

1. APIアクセスとノードクォータをリクエストします。詳細については、「APIアクセスとクォータのリクエスト」を参照してください。
2. VMware管理アプライアンスおよびHCX展開ネットワークに使用するアドレス範囲をメモします。詳細については、「ネットワーク要件」を参照してください。
3. VMware Engine Service Admin IAMロールを取得します。

最初のプライベートクラウドを作成する

1. VMware Engineポータルにアクセスします。
2. VMware Engineのホーム画面で、 をクリックします。ホスティング場所とハードウェアノードの種類が一覧表示されます。
3. プライベートクラウドのノード数を選択します。少なくとも3つのノードが必要です。
4. VMware管理ネットワークのクラスレスドメイン間ルーティング（CIDR）範囲を入力します。
5. HCX展開ネットワークのCIDR範囲を入力します。

> **重要:**
>
> CIDR範囲は、オンプレミスまたはクラウドのサブネットと重複してはなりません。
> CIDR範囲は/27以上である必要があります。

6. を選択します。
7. 設定を確認します。設定を変更するには、 をクリックします。
8. プライベートクラウドの作成を開始するには、 をクリックします。

VMware Engineが新しいプライベートクラウドを作成すると、いくつかのVMwareコンポーネントが展開され、プライベートクラウド内のクラスターの初期Autoscale™ポリシーが設定されます。

プライベートクラウドの作成には30分から2時間かかる場合があります。プロビジョニングが完了すると、メールが届きます。

GOOGLE CLOUD VMWARE ENGINE VPNゲートウェイをセットアップする

Google Cloud VMware Engineへの初期接続を確立するには、VPNゲートウェイを使用できます。これはOpenVPNベースのクライアントVPNであり、これを使用してVMware Software Defined Data Center (SDDC) vCenterに接続し、必要な初期構成を行うことができます。

VPNゲートウェイを展開する前に、SDDCが展開されているリージョンの**Edge Services**範囲を構成します。これを行うには：

1. **Google Cloud VMware Engine**ポータルにログオンし、 **>** に移動します。 をクリックします。
2. SDDCが展開されているリージョンを選択し、 と を有効にします。
3. 計画中にメモしたEdge Servicesの範囲を入力し、 をクリックします。これらのサービスを有効にするには10〜15分かかります。

   完了すると、リージョン設定ページでEdge Servicesが**** と表示されます。これらの設定を有効にすると、SDDCにパブリックIPを割り当てることができ、これはVPNゲートウェイを展開するための要件です。

VPNゲートウェイを展開するには：

1. **Google Cloud VMware Engine**ポータルで、 **>** に移動します。 をクリックします。
2. VPNゲートウェイの名前と、計画中に予約したクライアントサブネットを指定します。**次へ**をクリックします。
3. VPNアクセスを許可するユーザーを選択します。「**次へ**」をクリックします。
4. VPN経由でアクセス可能にする必要があるネットワークを指定します。「**次へ**」をクリックします。
5. 概要画面が表示されます。選択内容を確認し、「**送信**」をクリックしてVPNゲートウェイを作成します。VPNゲートウェイページに、新しいVPNゲートウェイのステータスが「**作成中**」と表示されます。
6. ステータスが「**稼働中**」に変わったら、新しいVPNゲートウェイをクリックします。
7. 「**VPN構成をダウンロード**」をクリックして、VPNゲートウェイ用に事前設定されたOpenVPNプロファイルを含むZIPファイルをダウンロードします。UDP/1194およびTCP/443経由で接続するためのプロファイルが利用可能です。好みのプロファイルを選択してOpenVPNにインポートし、接続します。
8. 「**リソース**」に移動し、SDDCを選択します。

VPNを接続する

1. VPNゲートウェイの設定を通じて、オンプレミスネットワークとプライベートクラウド間のポイントツーサイト接続を確立します。Google Cloud VMware Engine VPNゲートウェイのセットアップを参照してください。
2. Google Cloud VMware Engine VPNゲートウェイのセットアップでダウンロードしたVPN構成をアップロードします。
3. VPNクライアント（例: OpenVPN Connect）にインポートします。

詳細については、VPNを使用した接続を参照してください。

最初のサブネットを作成する

VMware EngineポータルからNSX-T Managerにアクセスする
サブネットの作成プロセスはNSX-Tで行われ、VMware Engineを介してアクセスします。NSX-T Managerにアクセスするには、次の手順を実行します。

1. **Google Cloud VMware Engine**ポータルにログオンします。
2. メインナビゲーションから、**リソース**に移動します。
3. サブネットを作成するプライベートクラウドに対応する**プライベートクラウド名**をクリックします。
4. プライベートクラウドの詳細ページで、**vSphere Management Network**タブをクリックします。
5. NSX-T Managerに対応する**FQDN**をクリックします。
6. プロンプトが表示されたら、サインイン資格情報を入力します。vIDMを設定し、Active DirectoryなどのIDソースに接続している場合は、代わりにIDソースの資格情報を使用します。

> **注意:**
>
> 生成された資格情報は、プライベートクラウドの詳細ページから取得できます。

サブネットのDHCPサービスを設定する
サブネットを作成する前に、DHCPサービスを設定します。

NSX-T マネージャーで：

1. **ネットワーキング > DHCP**に移動します。ネットワーキングダッシュボードには、DHCPサービスが1つのTier-0と1つのTier-1ゲートウェイを作成することが示されます。

2. DHCPサーバーのプロビジョニングを開始するには、**サーバーの追加**をクリックします。
3. **サーバータイプ**で**DHCP**を選択し、サーバー名とIPアドレスを指定します。
4. **保存**をクリックしてDHCPサービスを作成します。

このDHCPサービスを関連するTier-1ゲートウェイにアタッチするには、次の手順を実行します。デフォルトのTier-1ゲートウェイは、DHCPサービスによってすでにプロビジョニングされています。

1. 「**Tier 1 Gateways**」を選択し、Tier-1 ゲートウェイの縦の省略記号を選択し、「**Edit**」を選択します。
2. 「**IP Address Management**」フィールドで、「**No IP Allocation Set**」を選択します。
3. 「**Type**」に「**DHCP Local Server**」を選択します。
4. 「**DHCP Server**」には、作成した DHCP サーバーを選択します。
5. 「**保存**」をクリックします。
6. 「**Close Editing**」をクリックします。

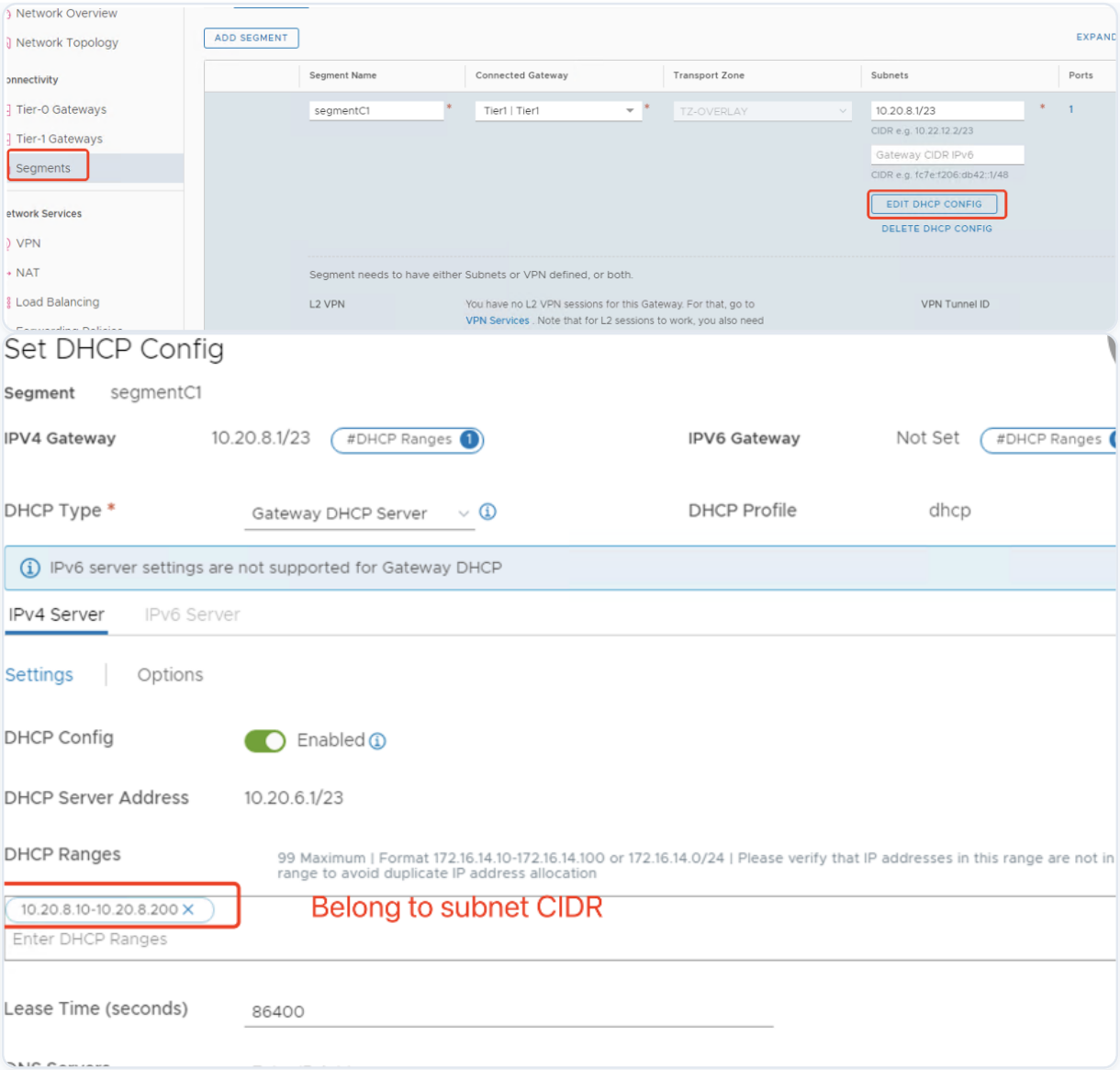
これで、NSX-T でネットワークセグメントを作成できます。NSX-T の DHCP の詳細については、DHCP に関する VMware ドキュメントを参照してください。
NSX-T でネットワークセグメントを作成する
ワークロード VM の場合、プライベートクラウドの NSX-T ネットワークセグメントとしてサブネットを作成します。

1. NSX-T Manager で、「**Networking > Segments**」に移動します。
2. 「**Add Segment**」をクリックします。
3. セグメントの名前を入力します。
4. 「**Connected Gateway**」として「**Tier-1**」を選択し、「Type」は「**Flexible**」のままにします。
5. 「**Set Subnets**」をクリックします。
6. 「**Add Subnets**」をクリックします。
7. 「**Gateway IP/Prefix Length**」にサブネット範囲を入力します。最後のオクテットが「**.1**」となるようにサブネット範囲を指定します。例: **10.12.2.1/24**。
8. DHCP範囲を指定し、**ADD**をクリックします。
9. 「**Transport Zone**」で、ドロップダウンリストから「**TZ-OVERLAY**」を選択します。
10. **Save**をクリックします。これで、VMの作成時にvCenterでこのネットワークセグメントを選択できるようになります。

特定のリージョンでは、VMware EngineからVPC networkへのプライベートサービスアクセスを使用して、最大100個の一意のルートを設定できます。これには、たとえば、プライベートクラウド管理IPアドレス範囲、NSX-Tワークロードネットワークセグメント、HCXネットワークIPアドレス範囲が含まれます。この制限には、リージョン内のすべてのプライベートクラウドが含まれます。

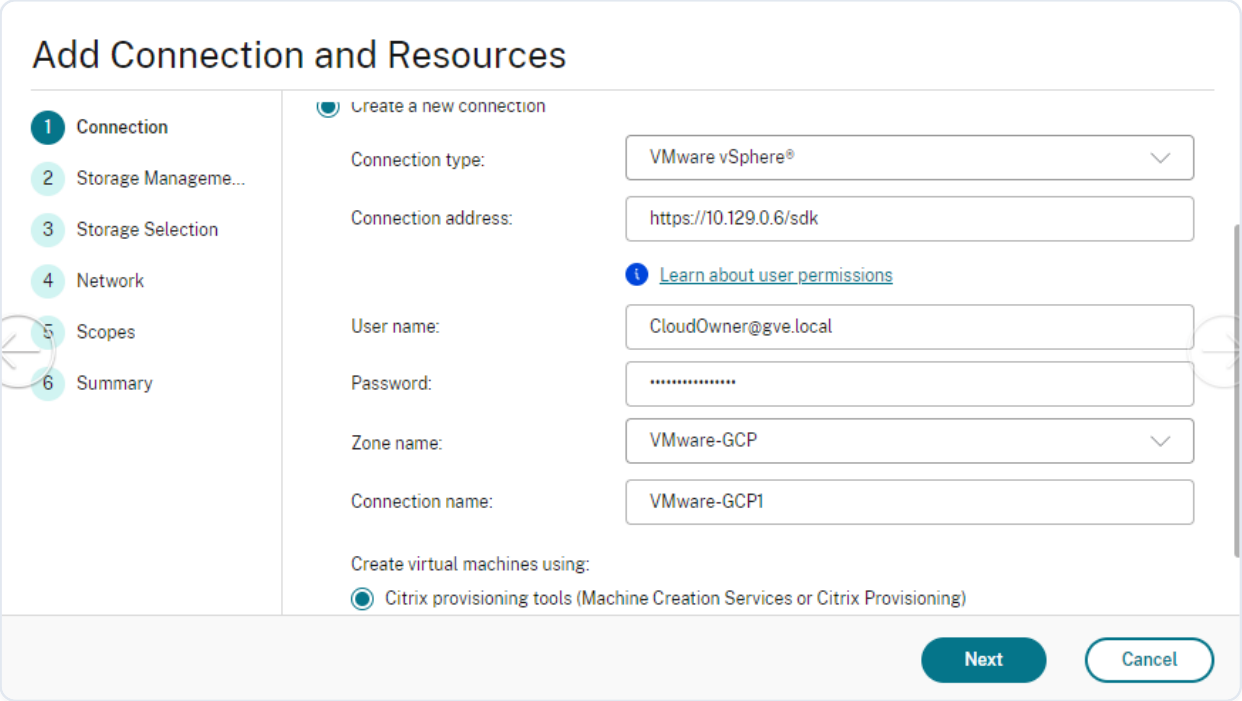
注:

Google Cloudの構成の問題により、DHCP範囲設定を複数回構成する必要があります。したがって、Google Cloudの構成後にDHCP範囲設定を構成するようにしてください。DHCP範囲を構成するには、**EDIT DHCP CONFIG**をクリックします。



CITRIX STUDIOでGOOGLE CLOUD VMWARE接続を作成する

1. vCenterでマシンを作成します。
2. Citrix Studioを起動します。
3. ホスティングノードを選択し、**Add Connection and Resources**をクリックします。
4. 「**Connection**」画面で、「**Create a new Connection**」を選択し、以下の詳細を入力します。



   a. 「**Connection type**」として「**VMware vSphere**」を選択します。
   b. 「**接続アドレス**」にvCenterのプライベートIPアドレスを入力します。
   c. vCenterの資格情報を入力します。
   d. 接続名を入力します。
   e. 仮想マシンを作成するツールを選択します。

5. **ネットワーク**画面で、NSX-Tサーバーで作成されたサブネットを選択します。
6. ウィザードを完了します。

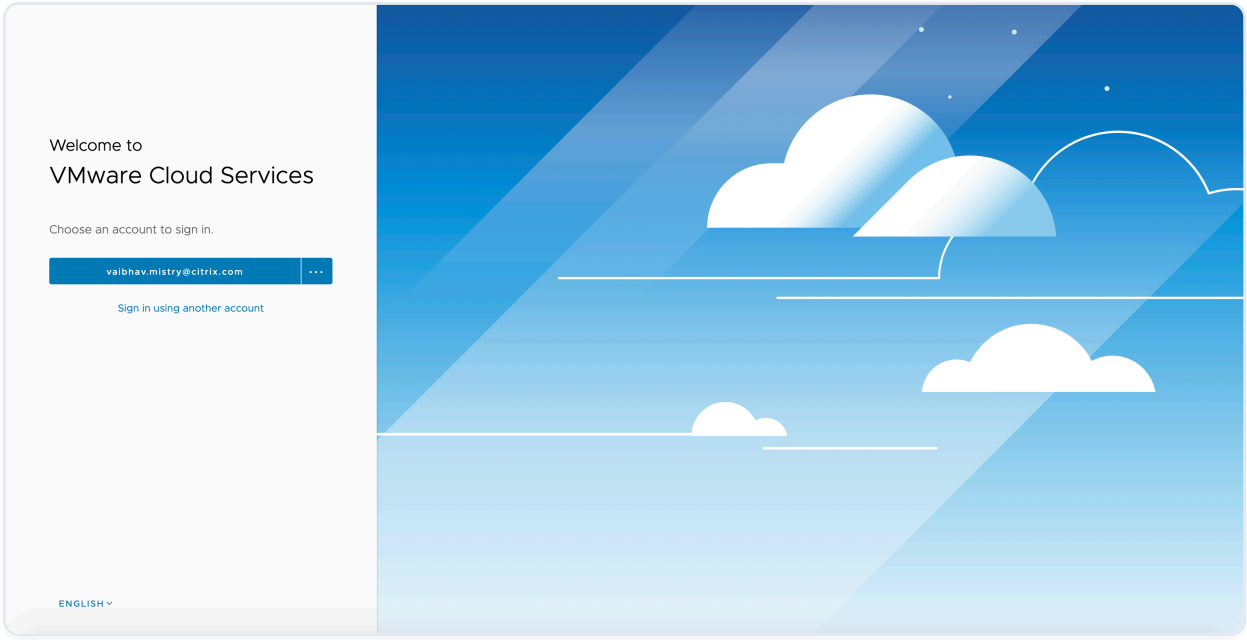
アマゾン ウェブ サービス (AWS) 上の ヴイエムウェア クラウド

Amazon Web Services (AWS) 上のVMware Cloudを使用すると、VMwareベースのオンプレミスCitrixワークロードをAWS Cloudに移行できます。

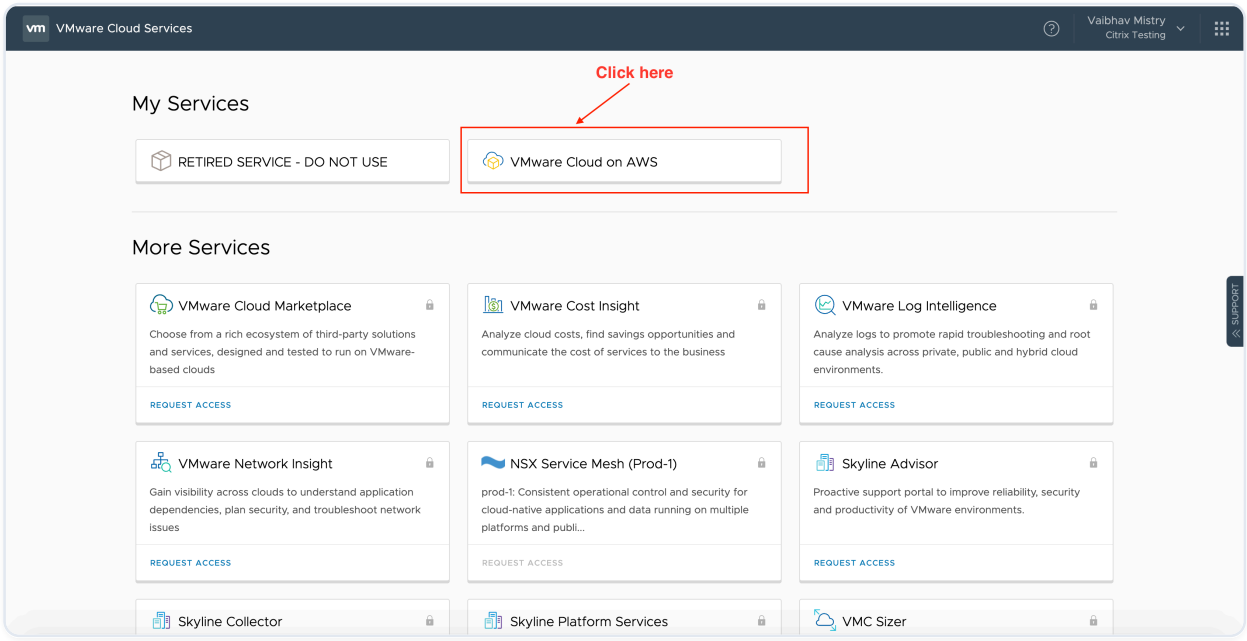
この記事では、AWS上にVMware Cloudをセットアップする手順について説明します。

VMware Cloud環境にアクセスする

1. URL `<https://console.cloud.vmware.com/>` を使用してVMware Cloudサービスにログインします。



2. 「**VMware Cloud on AWS**」をクリックします。「Software-Defined Data Centers (SDDC)」ページが表示されます。



3. 「**OPEN VCENTER**」をクリックし、次に「**SHOW CREDENTIALS**」をクリックします。後で使用するために資格情報を控えておきます。

「vCenterを開く」(/en-us/citrix-virtual-apps-desktops/current-release/media/vmc-sddc.png)

「資格情報を表示」(/en-us/citrix-virtual-apps-desktops/current-release/media/show-credentials-vmc.png)

4. Webブラウザを開き、vSphere Web ClientのURLを入力します。
5. 記載されている資格情報を入力し、**ログイン**をクリックします。vSphereクライアントのWebページは、オンプレミス環境のものと似ています。

「vSphereクライアントのWebページ」(/en-us/citrix-virtual-apps-desktops/current-release/media/vcenter-page.png)

VMwareクラウド環境について

vSphereクライアントのWebページには4つのビューがあります。

- ホストおよびクラスタービュー: 新しいクラスターを作成することはできませんが、クラウド管理者は複数のリソースプールを作成できます。

  「ホストおよびクラスタービュー」(/en-us/citrix-virtual-apps-desktops/current-release/media/host-cluster-view.png)
- VMおよびテンプレートビュー: クラウド管理者は多くのフォルダーを作成できます。

  「VMおよびテンプレートビュー」(/en-us/citrix-virtual-apps-desktops/current-release/media/vm-template-view.png)
- ストレージビュー: Citrix Studioでホスティングユニットを追加する際は、**WorkloadDatastore**ストレージを選択してください。Workload Datastoreにのみアクセスできるためです。

  「ストレージビュー」(/en-us/citrix-virtual-apps-desktops/current-release/media/storage-view.png)
- ネットワークビュー: VMwareクラウドネットワークと不透明なネットワークでは、アイコンが異なります。

  「ネットワークビュー」(/en-us/citrix-virtual-apps-desktops/current-release/media/network-view.png)

クラスターを設定した後、接続とリソースを追加するには、VMware virtualization environmentsを参照してください。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成

- 接続の作成と管理については、「VMware Cloudおよびパートナーソリューションへの接続」を参照してください。

詳細情報

- 接続とリソースを作成および管理する
- マシンカタログを作成する

コアコンポーネントをインストールする

重要:

- Citrix は、ライセンスコンプライアンスを含む正当な利益のために、必要に応じて基本的なライセンスデータを収集します。詳細については、「Citrix ライセンスデータ」を参照してください。
- ライセンスサーバーがバージョン 11.17.2 ビルド 53100 以降で実行されていることを確認してください。この前提条件を満たさない場合、Citrix Virtual Apps and Desktops サイトのアップグレードとサイト作成がブロックされます。

コアコンポーネントは、Citrix Delivery Controller™、Citrix Studio、Web Studio、Citrix Director、および Citrix License Server です。

注:

Citrix Studio は、オンプレミスの Citrix Virtual Apps and Desktops 展開を構成および管理できる Windows ベースの管理コンソールです。Web Studio は、Citrix Studio の次世代版であり、Citrix Studio と同等の機能を備えた Web ベースの管理コンソールです。Web Studio の詳細については、「Web Studio のインストール」を参照してください。

(2003 より前のバージョンでは、コアコンポーネントに Citrix StoreFront が含まれていました。**Citrix StoreFront** タイルをクリックするか、インストールメディアで利用可能なコマンドを実行することで、StoreFront をインストールできます。)

インストールを開始する前に、この記事と「インストールの準備」を確認してください。

この記事では、コアコンポーネントのインストール時のインストールウィザードのシーケンスについて説明します。コマンドラインの同等機能も提供されています。詳細については、「コマンドラインを使用したインストール」を参照してください。

ステップ 1. 製品ソフトウェアをダウンロードしてウィザードを起動する

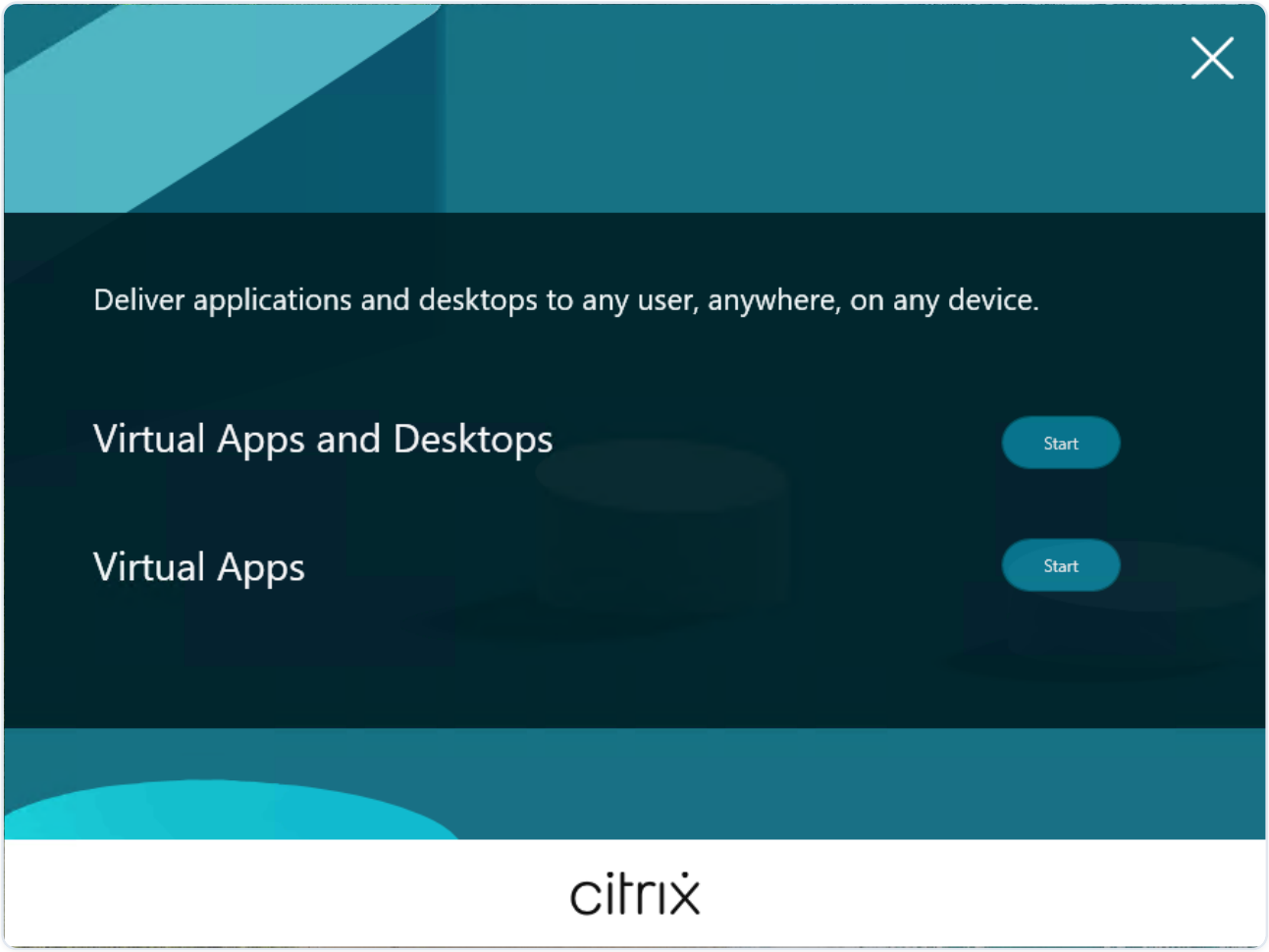
Citrix アカウントの資格情報を使用して、Citrix Virtual Apps and Desktops™ のダウンロードページにアクセスします。製品の ISO ファイルをダウンロードします。

ファイルを解凍します。必要に応じて、ISO ファイルを DVD に書き込みます。

コアコンポーネントをインストールするマシンに、ローカル管理者アカウントを使用してログオンします。

DVD をドライブに挿入するか、ISO ファイルをマウントします。インストーラーが自動的に起動しない場合は、**AutoSelect** アプリケーションまたはマウントされたドライブをダブルクリックします。

ステップ 2. インストールする製品を選択する



インストールする製品 (Virtual Apps または Virtual Apps and Desktops) の横にある **Start** をクリックします。

（マシンにCitrix Virtual Apps and Desktops™コンポーネントがすでにインストールされている場合、このページは表示されません。）

コマンドラインオプション: Citrix Virtual Apps をインストールするには `/xenapp` を使用します。このオプションを省略すると、Citrix Virtual Apps and Desktops がインストールされます。

ステップ 3. インストールするものを選択する

コンポーネントインストーラーのコンポーネント選択ページ(/en-us/citrix-virtual-apps-desktops/current-release/media/what-to-install-2.png)

初めて使用する場合は、**Delivery Controller** を選択します。(後のページで、このマシンにインストールする特定のコンポーネントを選択します。)

コントローラーをすでにインストールしている場合 (このマシンまたは別のマシンに)、別のコンポーネントをインストールするには、**展開の拡張**セクションからコンポーネントを選択します。

コマンドラインオプション: `/components`

ステップ 4. ライセンス契約を読んで同意する

コンポーネントインストーラーのライセンス契約ページ(/en-us/citrix-virtual-apps-desktops/current-release/media/core-license-75.png)

ライセンス契約ページで、ライセンス契約を読んだ後、内容を読んで同意したことを示します。次に、**次へ**をクリックします。

ステップ 5. インストールするコンポーネントとインストール場所を選択する

コンポーネントインストーラーのコアコンポーネントページ(/en-us/citrix-virtual-apps-desktops/current-release/media/core-components-75.png)

コアコンポーネントページで:

- **場所:** デフォルトでは、コンポーネントは `C:\Program Files\Citrix` にインストールされます。ほとんどの展開では、デフォルトで問題ありません。別の場所を指定する場合は、ネットワークサービスに対する実行権限が必要です。

- **コンポーネント:** デフォルトでは、すべてのコアコンポーネントのチェックボックスが選択されています。すべてのコアコンポーネントを1台のサーバーにインストールすることは、概念実証、テスト、または小規模な本番環境の展開には問題ありません。大規模な本番環境では、Citrix は Director、StoreFront、Secure Private Access、およびライセンスサーバーを別々のサーバーにインストールすることを推奨します。

  > **注:**
  >
  > 複数のサーバーにコンポーネントをインストールする場合は、他のサーバーに他のコンポーネントをインストールする前に、Citrix License Server とライセンスを最初にインストールしてください。ガイダンスについては、Citrix Virtual Apps and Desktops のライセンスガイド の「自動インストール」セクションを参照してください。

  > このマシンに必須のコアコンポーネントをインストールしないことを選択すると、アイコンで警告が表示されます。この警告は、そのコンポーネントをインストールする必要があることを通知しますが、必ずしもこのマシンにインストールする必要があるわけではありません。

Nextをクリックします。

コマンドラインオプション: `/installdir`、`/components`、`/exclude`

ハードウェアチェック

Delivery Controller をインストールまたはアップグレードすると、ハードウェアがチェックされます。マシンに推奨される RAM 容量 (5 GB) より少ない場合、インストーラーは警告を表示します。これはサイトの安定性に影響を与える可能性があります。詳細については、「ハードウェア要件」を参照してください。

グラフィカルインターフェイス: ダイアログボックスが表示されます。

- 推奨: **キャンセル** をクリックしてインストールを停止します。マシンに RAM を追加してから、再度インストールを開始します。
- または、**次へ** をクリックしてインストールを続行します。サイトで安定性の問題が発生する可能性があります。

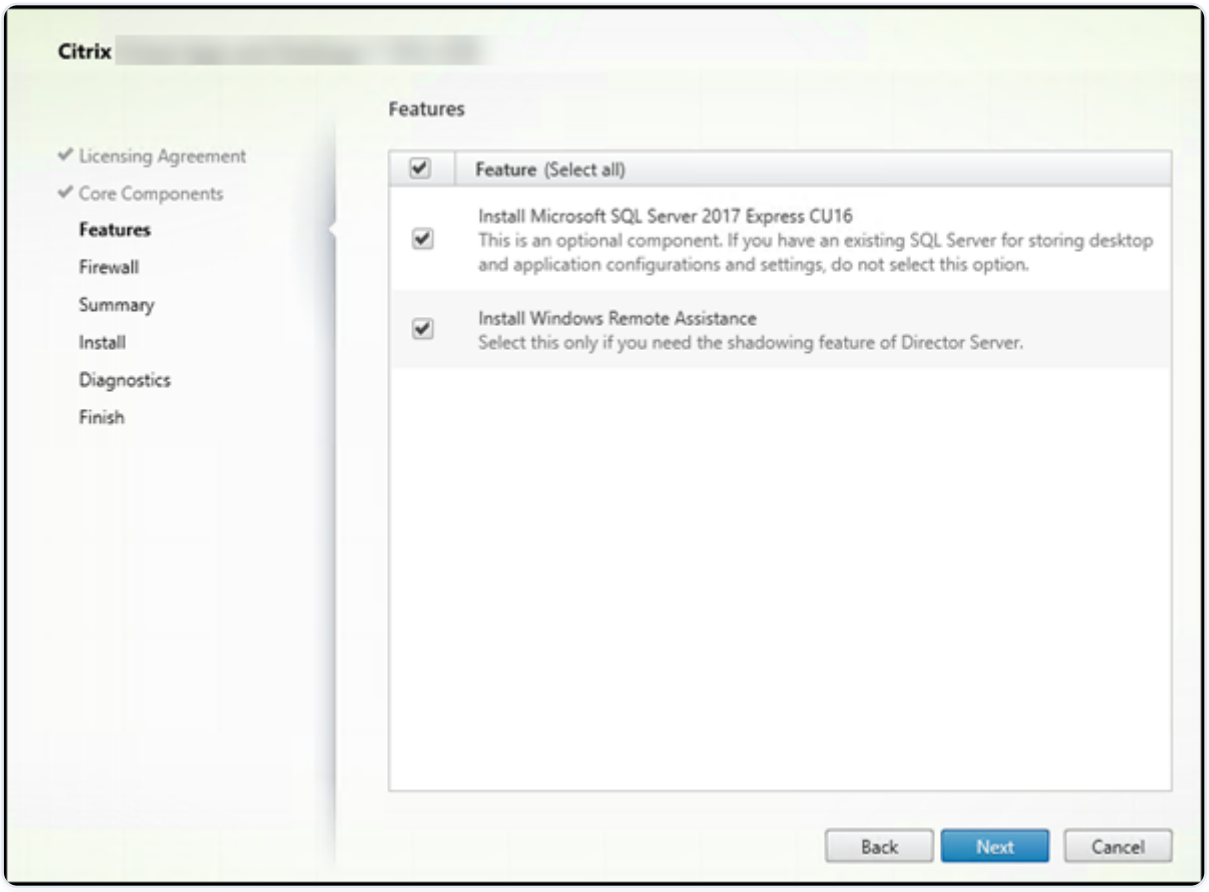
コマンドラインインターフェイス: インストール/アップグレードが終了します。インストールログには、検出された内容と利用可能なオプションを説明するメッセージが含まれています。

- 推奨: マシンに RAM を追加してから、再度コマンドを実行します。

- または、`/ignore_hw_check_failure` オプションを指定してコマンドを再度実行し、警告を上書きします。サイトで安定性の問題が発生する可能性があります。

アップグレード時には、OS または SQL Server のバージョンがサポートされなくなった場合にも通知されます。詳細については、「展開のアップグレード」を参照してください。

手順 6. 機能の有効化または無効化



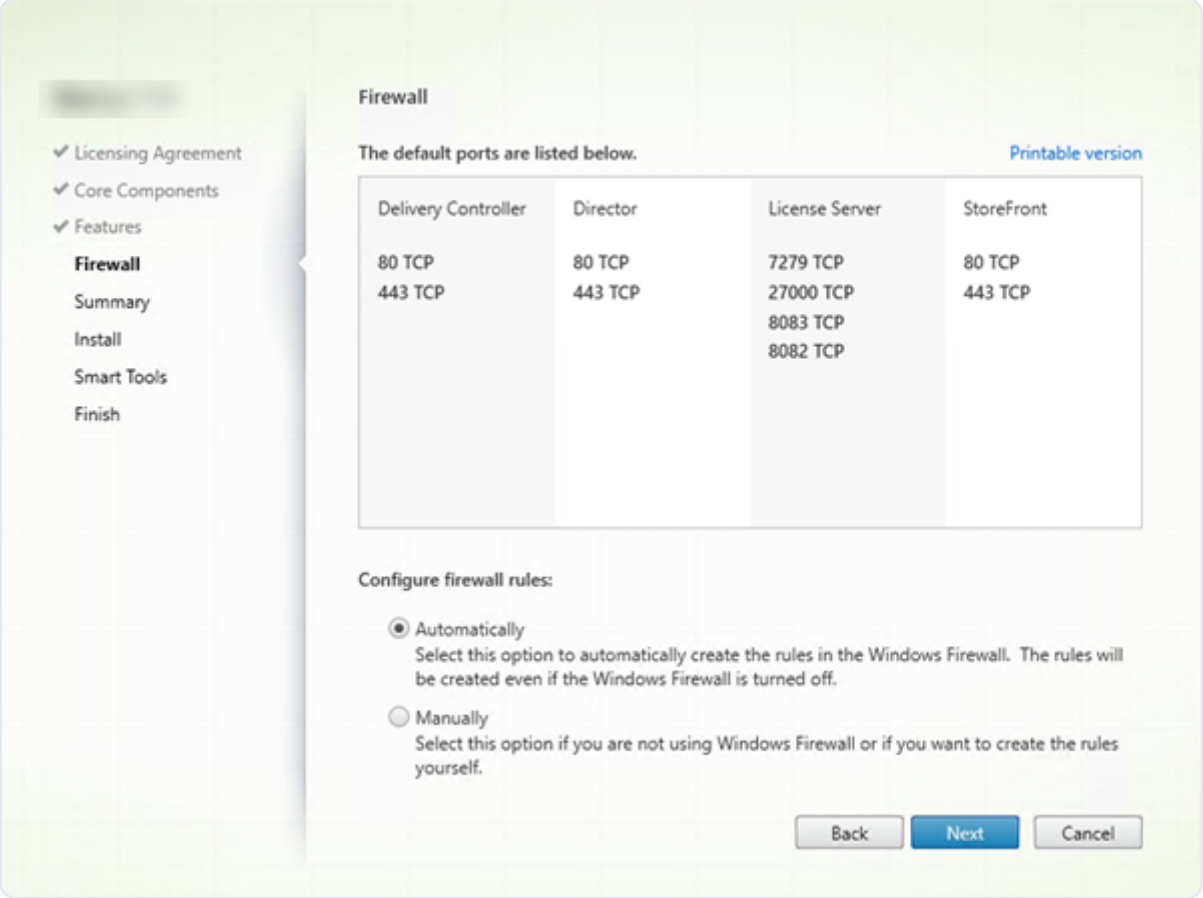
機能ページで:

- サイトデータベースとして使用するMicrosoft SQL Server Expressをインストールするかどうかを選択します。デフォルトでは、この選択は有効になっています。Citrix Virtual Apps and Desktopsデータベースに慣れていない場合は、データベースを確認してください。
- Directorをインストールすると、Windowsリモートアシスタンスが自動的にインストールされます。Directorのユーザーシャドウイングで使用するために、Windowsリモートアシストでシャドウイングを有効にするかどうかを選択します。シャドウイングを有効にすると、TCPポート3389が開きます。デフォルトでは、この機能は有効になっています。ほとんどの展開では、デフォルト設定で問題ありません。この機能は、Directorをインストールしている場合にのみ表示されます。

Nextをクリックします。

コマンドラインオプション: `/nosql` (インストールを防止するため)、`/no_remote_assistance` (有効化を防止するため)

手順7. Windowsファイアウォールポートを開く



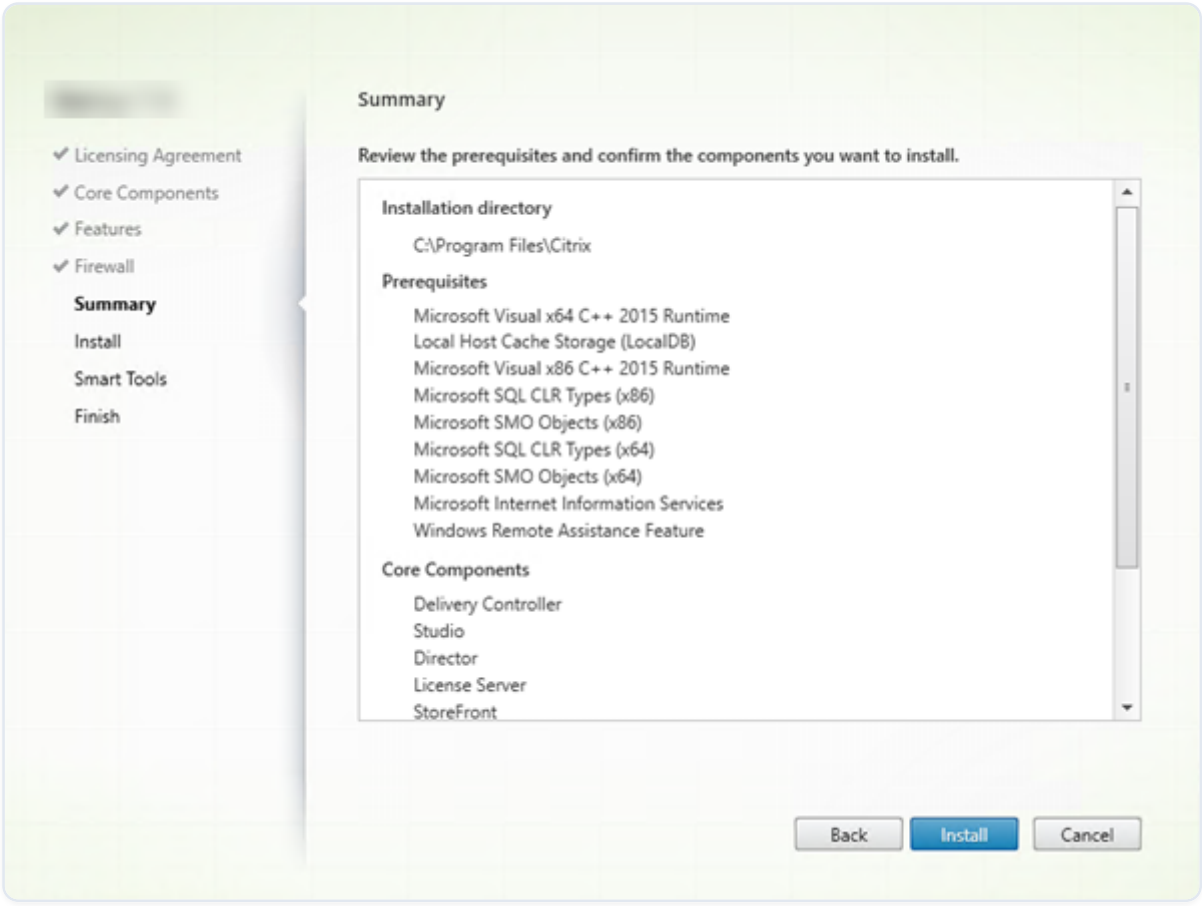
デフォルトでは、Windowsファイアウォールサービスが実行されている場合、ファイアウォールが有効になっていなくても、**ファイアウォール**ページ上のポートは自動的に開かれます。ほとんどの展開では、デフォルト設定で問題ありません。ポート情報については、ネットワークポートを参照してください。

Nextをクリックします。

(このグラフィックは、このマシンにすべてのコアコンポーネントをインストールしたときのポートリストを示しています。この種のインストールは、通常、テスト展開のみを対象としています。)

コマンドラインオプション: `/configure_firewall`

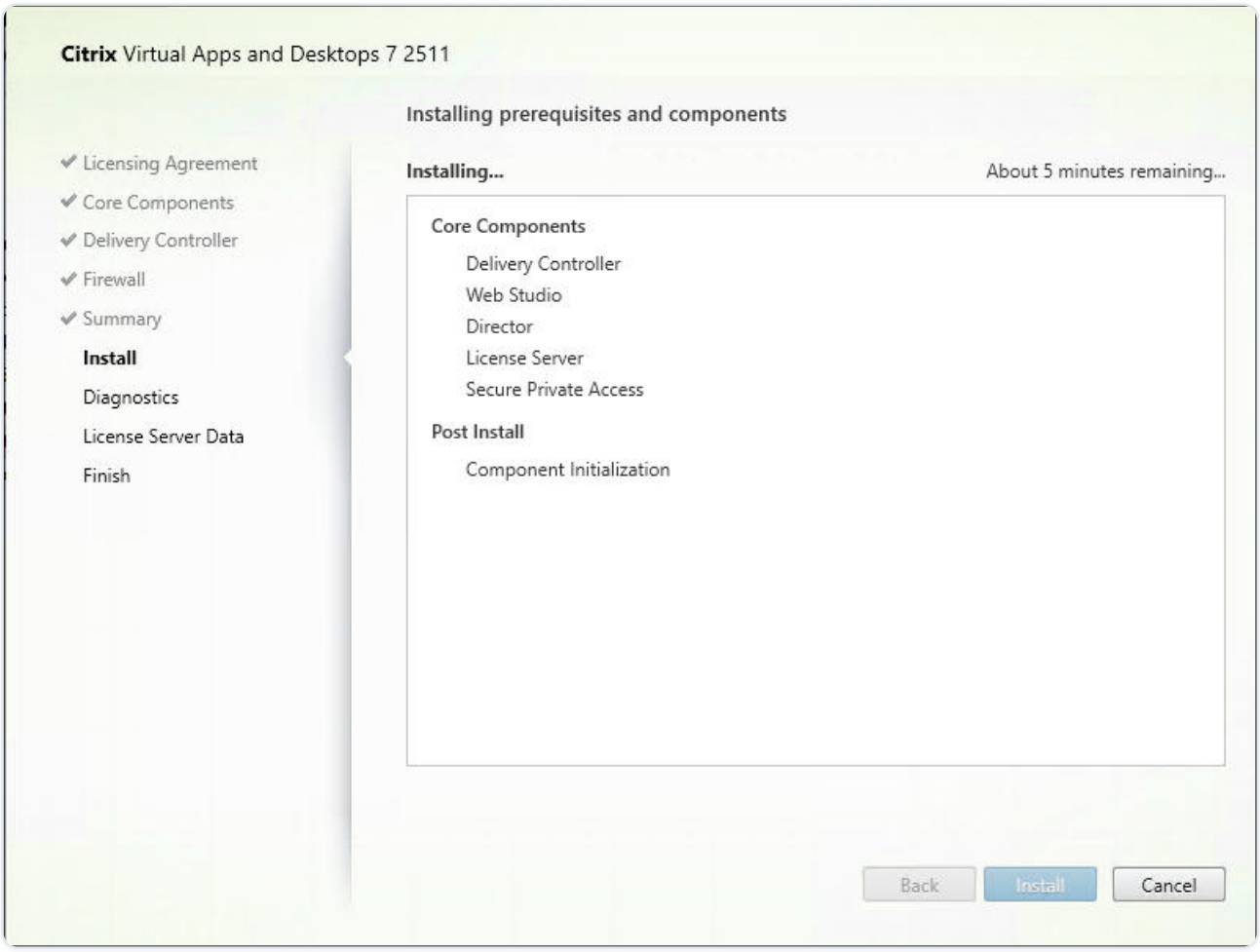
手順8. 前提条件を確認し、インストールを確定する



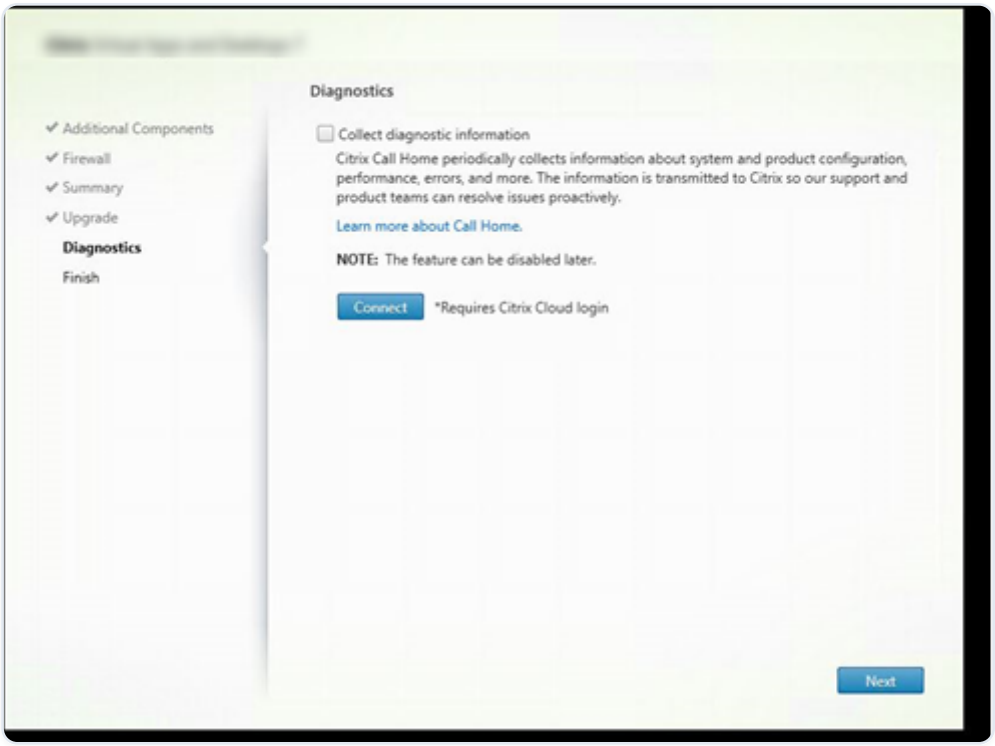
概要ページには、インストールされるものが一覧表示されます。必要に応じて、**戻る**ボタンを使用して以前のウィザードページに戻り、選択を変更します。

準備ができたら、**インストール**をクリックします。

ディスプレイにはインストールの進行状況が表示されます。



ステップ9. Cloud Software Groupとの診断情報の共有



診断ページで、Citrix Call Homeに参加するかどうかを選択します。

このページは、グラフィカルインターフェイスを使用してDelivery Controllerをインストールするときに表示されます。StoreFrontをインストールする場合（ただしControllerではない場合）、ウィザードはこのページを表示します。その他のコアコンポーネントをインストールする場合（ただしControllerまたはStoreFrontではない場合）、ウィザードはこのページを表示しません。

アップグレード中に、Call Homeがすでに有効になっている場合、またはインストーラーがCitrix Telemetry Serviceに関連するエラーを検出した場合、このページは表示されません。

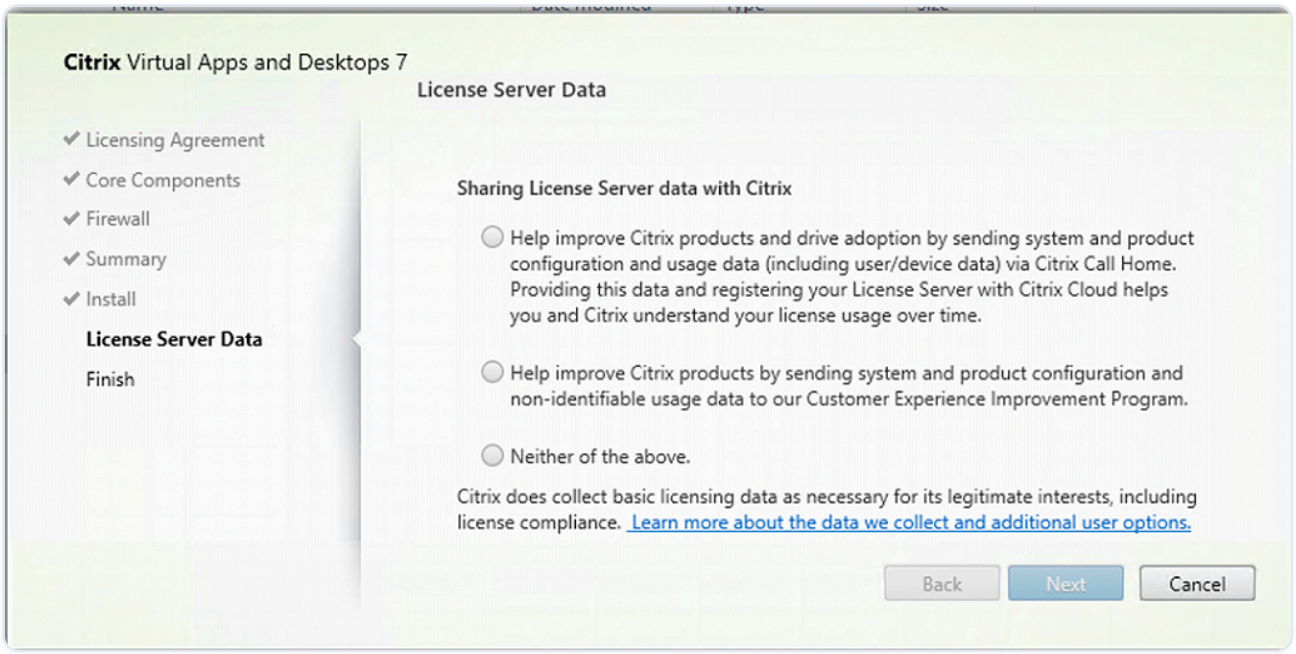
参加することを選択した場合（デフォルト）、**接続**をクリックします。プロンプトが表示されたら、Citrixアカウントの資格情報を入力します。登録の選択は、インストール後に変更できます。

資格情報が検証された後（または参加しないことを選択した場合）、**次へ**をクリックします。

診断ページで、最初に**診断情報の収集**を選択せずに**接続**をクリックした場合、**Citrix Insight Servicesに接続**ダイアログを閉じると**次へ**ボタンが無効になります。次のページに進むことはできません。**次へ**ボタンを再度有効にするには、**診断情報の収集**を選択してすぐに選択を解除します。

詳細については、Call Homeを参照してください。

ステップ10. Cloud Software Groupとのライセンスサーバーデータの共有



ライセンスサーバーデータページでは、お客様を支援するために、Call Homeデータまたはカスタマーエクスペリエンス向上プログラム（CEIP）データのいずれかを共有していただくようお願いしています。さらに、Cloud Software Groupは、正当な利益のために必要に応じて、ライセンスコンプライアンスを含む基本的なライセンスデータの収集も要求します。

ライセンスサーバーデータページは、ライセンスサーバーをインストールしたときに表示されます。

- スタンドアロンとして。
- Delivery Controllerのインストール中に、コアコンポーネントとして。

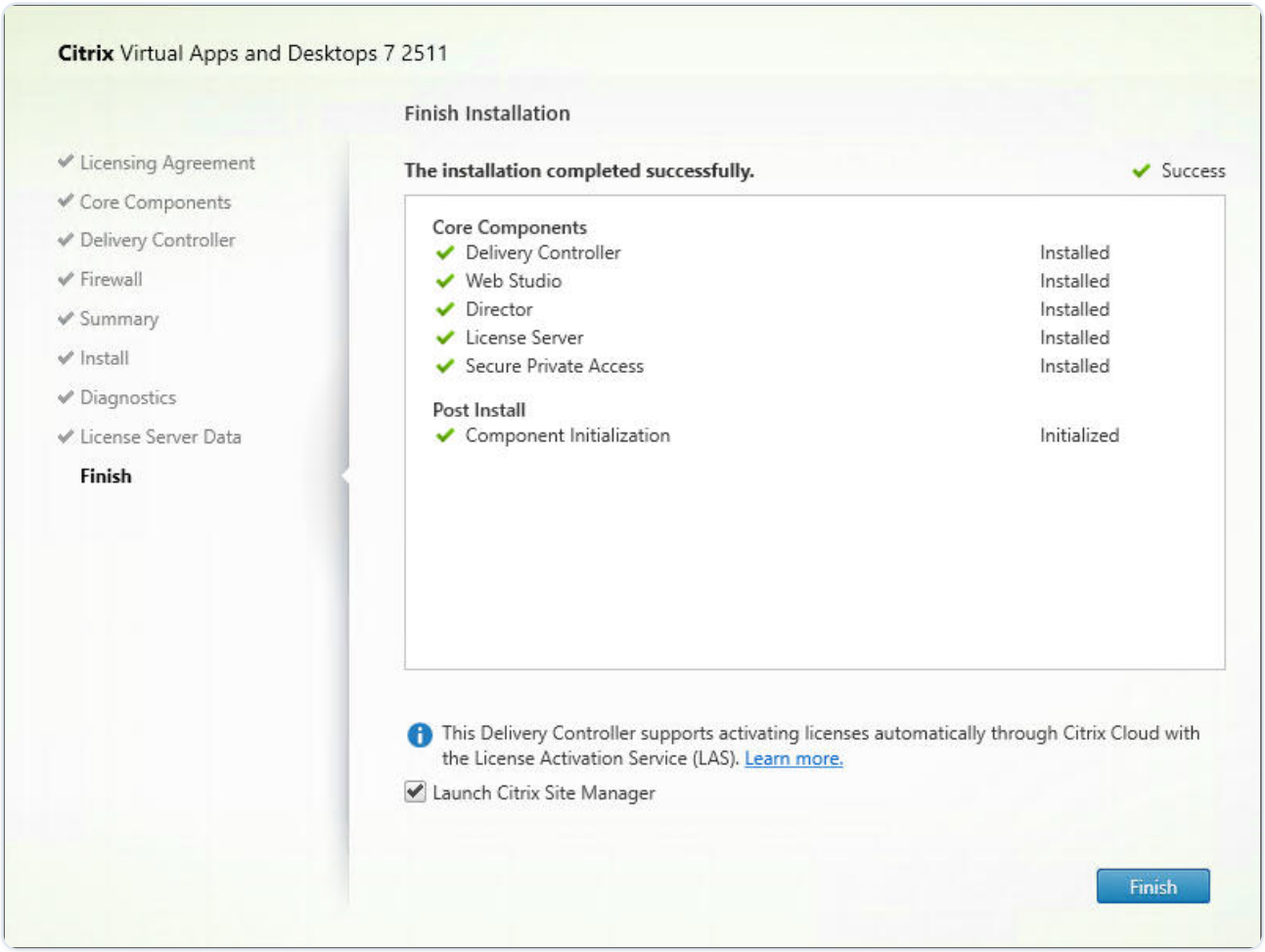
アップグレード中に、`/CITRIX.opt:` ファイルで構成がすでに設定されている場合、このページは表示されません。

ライセンスサーバーは、ライセンスデータ、Call Homeデータ、CEIPデータなど、いくつかの種類のユーザーデータを監視します。Call HomeデータとCEIPデータの収集を有効にするには、参加（オプトイン）を選択する必要があります。

コマンドラインを使用してインストールする際にCall HomeおよびCEIPデータ収集を有効にする方法の詳細については、「コアコンポーネントをインストールするためのコマンドラインオプション」を参照してください。

Cloud Software Groupのライセンスデータ収集の詳細については、「Citrixライセンスデータ収集プログラム」を参照してください。

ステップ11. このインストールを完了する



完了ページには、正常にインストールおよび初期化されたすべての前提条件とコンポーネントに緑色のチェックマークが表示されます。

完了をクリックします。

> **注:**
>
> バージョン2511にアップグレードすると、インストーラーはCitrix Studio（MMCベース）を自動的にアンインストールします。構成データはデータベースに保存され、自動アンインストールによる影響は受けません。

ステップ12. 残りのコアコンポーネントを他のマシンにインストールする

すべてのコアコンポーネントを1台のマシンにインストールした場合は、「次のステップ」に進みます。そうでない場合は、他のマシンでインストーラーを実行して他のコンポーネントをインストールします。他のサーバーにControllerを追加でインストールすることもできます。

次のステップ

必要なすべてのコンポーネントをインストールしたら、Web Studioを使用して「サイトを作成」します。

サイトを作成したら、VDAをインストールします。

いつでも、フルプロダクトインストーラーを使用して、以下のコンポーネントで展開を拡張できます。

- **Universal Print Serverサーバーコンポーネント:** プリントサーバーでインストーラーを起動します。

  a. **展開の拡張**セクションで**Universal Print Server**を選択します。

  b. ライセンス契約に同意します。

  c. 「**ファイアウォール**」ページでは、Windowsファイアウォールサービスが実行されている場合、ファイアウォールが有効になっていない場合でも、デフォルトでTCPポート7229および8080がファイアウォールで開かれます。ポートを手動で開きたい場合は、このデフォルトのアクションを無効にできます。

  このコンポーネントをコマンドラインからインストールするには、「Universal Print Serverをインストールするためのコマンドラインオプション」を参照してください。
- 「フェデレーション認証サービス」。
- 「セッション録画」。
- 「ワークスペース環境管理」。
- uberAgent のインストール
- deviceTRUST Agent のインストール
- WEM クイックスタートガイド

Web Studio のインストール

> **注:**
>
> Citrix Studio (MMC Studio) はバージョン 2511 以降削除され、サポートされなくなりました。この記事では、Web Studio が唯一使用される管理コンソールであると仮定しています。

はじめに

Web Studio は、Citrix Studio と完全に同等の機能を備えた Web ベースの管理コンソールです。(/ja-jp/citrix-daas/overview#studio) と同じルックアンドフィールで、Web Studio はネイティブの Web エクスペリエンスを提供することで、管理エクスペリエンスを最新化します。

Web Studio は、Internet Information Service (IIS) がインストールされている任意の Windows サーバーに展開できます。展開オプションは次の 2 つです。

- 専用サーバーにインストールする:

  パフォーマンスと拡張性が重要な大規模環境では、Web Studio を専用サーバーにインストールすることをお勧めします。このサーバーは、オプションで Director もホストできます。

- Delivery Controller™ と統合する:

  迅速な展開とシンプルな環境では、Web Studio を Delivery Controller に直接インストールします。このアプローチは、管理オーバーヘッドを最小限に抑えることが優先される小規模な展開に最適です。

次の図は、Web Studio のアーキテクチャを示しています。

「Web Studio のアーキテクチャ」(/en-us/citrix-virtual-apps-desktops/current-release/media/web-studio-architecture.png)

Web Studio を稼働させるための一般的なワークフローは次のとおりです。

1. (#install-web-studio-1)。
2. (#set-up-a-site)。
3. (#add-delivery-controllers-to-web-studio-for-management)。
4. (オプション) Delivery Controller のプロキシとして Web Studio を構成する(#optional-configure-web-studio-as-a-proxy-for-delivery-controllers)
5. 「(オプション) Pendoを無効にする」(#optional-enable-or-disable-pendo)。
6. Web Studioのセキュアなサーバー構成(#secure-server-configuration-for-web-studio)
7. 「Web Studioにサインインする」(#sign-in-to-web-studio)。

負荷分散されたWeb Studio展開をセットアップするには、(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/install-core/install-web-studio/load-balance-studio.html)を参照してください。

Web Studioで利用可能な新機能

(/ja-jp/citrix-virtual-apps-desktops/current-release/whats-new.html#web-studio)の記事を参照してください。

システム要件

以下の表に、Studio のインストールと使用に関するサポートされているオペレーティングシステム、ブラウザー、表示設定、およびハードウェア要件を示します。

サポートされているオペレーティングシステム

オペレーティングシステム	エディション	SERVER CORE のサポート
ウィンドウズ サーバー 2025	スタンダード、データセンター	はい
ウィンドウズ サーバー 2022	スタンダード、データセンター	はい
ウィンドウズ サーバー 2019	スタンダード、データセンター	はい
ウィンドウズ サーバー 2016	スタンダード、データセンター	はい

サポートされているブラウザー

ブラウザー	サポートされる最小バージョン
マイクロソフト エッジ	92
Firefox ESR (延長サポート版)	90
グーグル クローム	92
サファリ	14

表示要件

要件	値
推奨画面解像度	1440 × 1024

ハードウェア要件

リソース	最小要件
メモリ	1 GB RAM
ディスク容量	100 MB

Web Studio のインストール

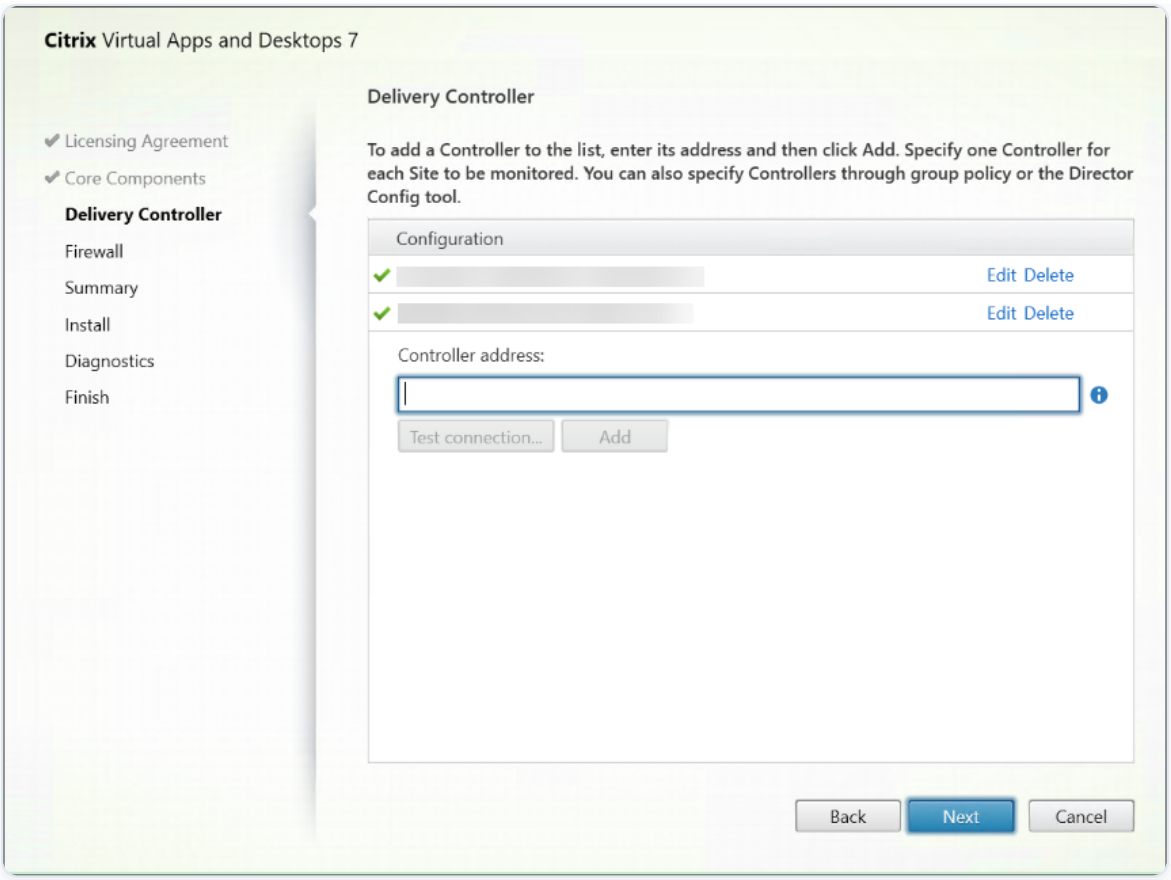
次の情報は、コアコンポーネントのインストールのガイダンスを補足するものです。Web Studio をインストールするには：

- Citrix Virtual Apps and Desktops™ のフル製品 ISO インストーラーを使用して Web Studio をインストールします。ISO インストーラーは、前提条件を確認し、不足しているコンポーネントをインストールし、Web Studio Web サイトをセットアップし（Delivery Controller のインストールに含まれている場合は Delivery Controller 上に）、基本的な構成を実行します。
- インストール時にWeb Studioが含まれていなかった場合は、インストーラーを使用してWeb Studioを追加します。
- Web Studioのインストール時に、Delivery ControllerのFQDNを入力するよう求められます。

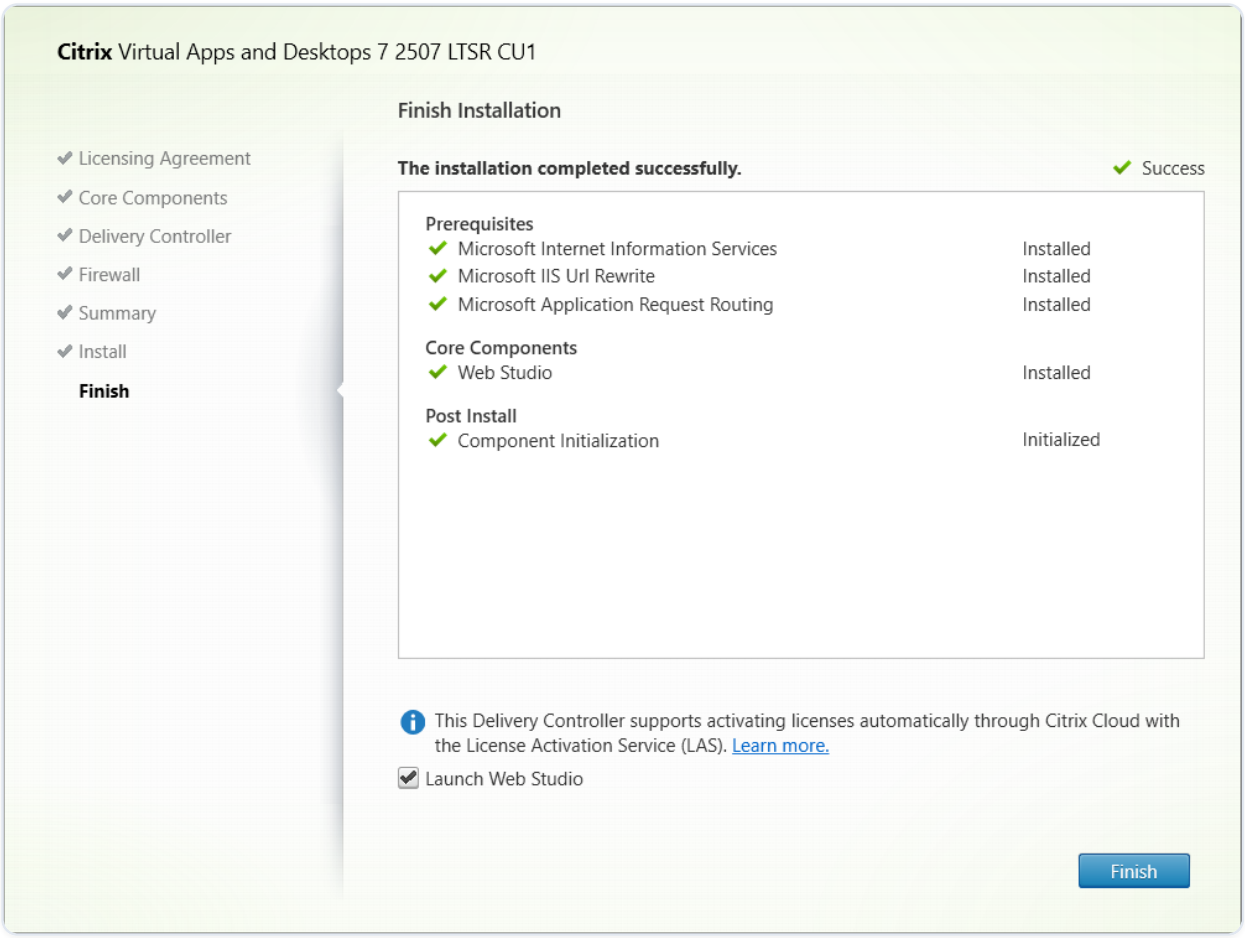
注:

- 完全な機能性を確保するために、Web StudioとDelivery Controllerは同じバージョンで実行することをお勧めします。
- 複数のDelivery Controllerを追加できます。Web Studioはランダムな順序でそれらに接続を試みます。Web Studioが接続しようとしているDelivery Controllerに到達できない場合、Web Studioは自動的に他のDelivery Controllerにフォールバックします。
- **コアコンポーネント**でDirectorが選択され、インストールされている場合、ここで追加するDelivery ControllerはWeb StudioとDirectorの両方で使用されます。
- Delivery ControllerがTLS用に構成されている（推奨）場合、入力されたFQDNは、Delivery Controllerにインストールされている証明書の共通名またはサブジェクトの別名と一致する必要があります。
- Web Studioは、サイト名に関係なく、**Site ID = 1**の任意のIIS Webサイトにインストールできます。この機能により、**Default Web Site**の代わりにカスタムIISサイトでWeb Studioをホストできます。

- ISOインストーラーを実行する前にIISがインストールされていない場合、インストーラーはIISを自動的に構成し、**Default Web Site**（サイトID = 1）の下にWeb Studioを展開します。インストール後、必要に応じてサイト名を変更できます。
- IISがすでにインストールされている場合、**Site ID**が**1**である限り、任意の名前と物理パスでIISサイトを事前に作成できます。Web Studioは、追加の構成なしでそのサイトの直下にインストールされます。



- **完了**ページで、インストールされたコンポーネントを確認し、**完了**をクリックします。



> **注:**
>
> コマンドラインを使用してWeb Studioをインストールすることもできます。例：`.\XenDesktopServerSetup.exe /components webstudio /controllers "ddc1.studio.local" /configure_firewall /quiet`。詳細については、コマンドラインを使用したインストールを参照してください。

TLS 用の証明書を構成する

デフォルトでは、IISがHTTPS用に構成されていない場合、インストーラーはサーバーのFQDNを証明書の共通名として使用して自己署名証明書を作成し、それをポート443にバインドします。この動作により、ユーザーはローカルマシンからWeb Studioにアクセスできますが、証明書が信頼されていないため、他のマシンから接続するユーザーにはセキュリティ警告が表示されます。この証明書を、エンタープライズまたはパブリック認証局（CA）によって署名された証明書に置き換えることをお勧めします。詳しくは、Web StudioおよびDirectorでTLSを有効にするを参照してください。IISでTLS証明書がすでに構成されている場合、インストーラーは変更を行いません。

> **注:**

> Web Studioの展開を保護する方法について詳しくは、Web Studioの展開を保護するを参照してください。

サイトをセットアップする

Citrix Virtual Apps and Desktops 展開（サイトとも呼ばれます）をセットアップするには、Citrix Site Manager ツールを使用します。このツールは、Delivery Controller とともに自動的にインストールされます。

サイトをセットアップするには、次の手順に従います。

1. Delivery Controller で、デスクトップのスタートメニューを開き、**Citrix > Citrix Site Manager** を選択します。
2. Citrix Site Manager で、**Create a site** を選択します。サイトセットアップウィザードが表示されます。
3. サイトを作成し、その設定を次のように構成します。
   - **Introduction** ページで、サイトの名前を入力します。
   - **Databases** ページには、サイト、監視、および構成ログデータベースをセットアップするための選択肢が含まれています。詳細については、「手順 3. データベース」を参照してください。
   - **Licensing** ページで、ライセンスサーバーのアドレスを指定し、使用（インストール）するライセンスを示します。詳細については、「手順 4. ライセンス」を参照してください。
4. **Summary** ページで、すべての設定を確認し、**Submit** をクリックします。

   このコントローラーの IP アドレスは、サイトに自動的に追加されます。

> **注:**
>
> サイトを作成したユーザーは、そのサイトのフル管理者になります。詳細については、「委任管理」を参照してください。

サイトの作成後に新しいコントローラーをインストールする場合は、そのコントローラーをサイトに追加する必要があります。詳細な手順は次のとおりです。

1. この新しいControllerでCitrix Site Managerを実行します。

2. **既存のサイトに参加**を選択します。
3. 既にサイトに追加されているControllerのアドレスを入力します。
4. **Submit**をクリックします。

管理のためにDelivery ControllerをWeb Studioに追加する

Studio構成ツールを使用して、管理のためにDelivery ControllerをWeb Studioに追加します。このツールはWeb Studioのインストールフォルダーにあります。

デフォルトでは、このツールは次のデフォルトフォルダーにインストールされます。

- `C:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe`

Web Studioで管理したいサイトに対して、次の2つのDelivery Controller (`ddc1.studio.local` と `ddc2.studio.local`) を構成するとします。次のPowerShellコマンドを実行します。

- `.\StudioConfig.exe --server "ddc1.studio.local,ddc2.studio.local"`

注:

- このツールにはコンピューターの管理者権限が必要です。
- IISサーバーのキャッシュ設定により、Delivery Controllerの構成変更がすぐに反映されない場合があります。すぐに反映させるには、Web Studioサーバーに移動し、インターネットインフォメーションサービス（IIS）マネージャーを開き、*Server_name* > **サイト** > *Web Studioがインストールされ ているIISサイト名（サイトID = 1）* に移動して、ペインで「**再起動**」を選択します。
- 新しいFQDNでDelivery Controllerを再展開する場合、`StudioConfig.exe` を使用してWeb Studioで、および `C:\Program Files\Citrix\Web Studio\Site\assets\json\manifest.json` ファイルでFQDNを更新します。`manifest.json` ファイルを更新しないと、古いFQDNがWeb Studioのサインインウィンドウに表示されたままになります。その結果、サインイン時に代替として新しいFQDNを入力する必要があります。
- サポートされているすべてのパラメーターを表示するには、`StudioConfig.exe --help` を実行します。

(オプション) Web StudioをDelivery Controllerのプロキシとして構成する

デフォルトでは、Web Studioコンソールを使用して展開を管理する場合、Webブラウザーを介してWeb StudioサーバーとDelivery Controllerの両方に接続します。Web StudioサーバーをDelivery Controllerのプロキシとして構成するオプションが提供されています。その結果、展開を管理する際にはWeb Studioサーバーにのみ接続することになります。

このセクションでは、Web StudioサーバーをDelivery Controllerのプロキシとして構成する方法を説明します。Web StudioとDelivery Controllerは異なるサーバーにインストールされていることを前提としています。

開始する前に、必要なすべてのコアコンポーネントが展開環境にインストールされていることを確認してください。詳細については、「コアコンポーネントのインストール」を参照してください。

Web Studio のプロキシモードを有効にするには、次の手順に従います。

1. Web Studio サーバーで、Windows PowerShell を管理者として実行します。
2. 次のコマンドを実行します。`fqdn_of_webstudio_machine` は Web Studio サーバーの FQDN に置き換えてください。

   ```
   & "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --enableproxy --proxyserver "fqdn_of_webstudio_machine"
   ```

   > **注:**
   >
   > ロードバランスされた Web Studio 展開環境がある場合は、`fqdn_of_webstudio_machine` をロードバランサーサーバー (仮想サーバーとも呼ばれます) の FQDN に置き換えてください。詳細については、「ロードバランスされた Web Studio 展開環境のセットアップ」を参照してください。

Web Studio のプロキシモードを無効にするには、この PowerShell コマンドを実行します。

```
& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --disableproxy
```

(オプション) Pendo を有効または無効にする

バージョン 2411 以降、Web Studio は Pendo を統合しており、これはデフォルトで有効になっています。Pendo は、Citrix プライバシーポリシー に従って使用状況データを収集します。また、Web Studio の右下隅にアイコンを追加し、コンテキストに応じた機能情報とフィードバックオプ

ションを提供します。使用状況データを共有したくない場合は、Studio 構成ツールを使用して Pendo を無効にできます。

このツールは Web Studio のインストールフォルダーにあります。デフォルトでは、ツールは次のフォルダーにインストールされます: `C:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe`。

Pendo を無効にするには、次の手順に従います。

1. Web Studio にサインインします。右下隅にアイコンが表示されている場合、Pendo は有効になっています。
2. Web Studio サーバーで、Windows PowerShell を管理者として実行します。 この PowerShell コマンドを実行します。

```
& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --
disablependo
```

Pendo を有効にするには、このコマンドを実行します。

```
& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --enablependo
```

Web Studioのセキュアなサーバー構成

セキュリティを強化するために、Web Studio をホストするサーバーに次のセキュリティ構成を適用します。これらの設定は、Web Studio 自体ではなく、サーバーレベルで適用されます。

中強度のSSL暗号（SWEET32）を無効にする

Web Studioサーバーは、SWEET32攻撃に対して脆弱な中強度の暗号 `TLS_RSA_WITH_3DES_EDE_CBC_SHA` を使用する可能性があります。 この暗号を無効にするには、Web Studioサーバーで次のPowerShellコマンドを実行します。 `Disable-TlsCipherSuite -Name TLS_RSA_WITH_3DES_EDE_CBC_SHA`

非推奨のTLS 1.0および1.1プロトコルを無効にする

TLS 1.0およびTLS 1.1は非推奨であり、Web Studioサーバーで有効にすべきではありません。 これらを無効にするには：

1. レジストリエディター (`regedit.exe`) を開きます。
2. `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocol` に移動します。

3. 次のサブキーが存在しない場合は作成します。
   - `TLS 1.0\Client`
   - `TLS 1.0\Server`
   - `TLS 1.1\Client`
   - `TLS 1.1\Server`
4. 各`Client`および`Server`キーに、次の`DWORD (32-bit)`値を作成します。
   - `Enabled` = `0`
   - `DisabledByDefault` = `1` (オプションですが推奨)
5. 変更を適用するには、サーバーを再起動します。

Web Studioにサインインする

1. デフォルトのポート番号 443 が使用されている場合は、`https://<address of the server hosting Web Studio>/Citrix/Studio` で Web Studio にアクセスします。別のポートが構成されている 場合は、`https://<address of the server hosting Web Studio>:<port number>/Citrix/Studio` を使用します。

   Web StudioにDelivery Controllerを(#add-delivery-controllers-to-web-studio-for-management)追加しており、それらに到達可能な場合、サインインページが表示されます。

   > **注:**
   >
   > 以下の場合は、**サインインできません**ページが表示されます。
   >
   > - サイトにDelivery Controllerが指定されていません。接続するためにDelivery Controllerを追加するよう求められます。
   > - 指定されたDelivery Controllerに到達できません。接続を確認するには、**テスト**をクリックします。または、代替のDelivery Controllerを入力して**接続**をクリックします。

2. **ユーザー名**、**パスワード**、**ドメイン**を入力します。
3. **サインイン**をクリックします。

次のステップ

1. VDAのインストール
2. Web Studioを使用して、次の方法で仮想アプリとデスクトップをユーザーに配信します。
    a. マシンカタログを作成する(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/machine-catalogs-create.html)
    b. デリバリーグループを作成する(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/delivery-groups-create.html)
    c. アプリケーショングループを作成する（オプション）(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/application-groups-create.html)

Web Studio展開のセキュリティ保護

この記事では、Web Studioを展開する際にシステムセキュリティに影響を与える可能性のある構成領域について説明します。

> **注:**

> ユーザーのWebブラウザとWeb Studio間の通信を保護するには、Web StudioおよびDirectorでTLSを有効にするを参照してください。

IIS設定の構成

セキュリティのベストプラクティスとして、Web Studioを制限されたIIS構成で構成します。

1. 要求フィルタリングを制限する:
    - Web StudioをDirectorとともにインストールする場合、IISは以下のフィルタリングルールで自動的に構成されます。
    - Web Studioをスタンドアロンコンポーネントとしてインストールする場合は、IISを手動で次のように構成します。
        - 以下のファイル名拡張子のみを許可する:

          `.`, `.aspx`, `.css`, `.eot`, `.html`, `.ico`, `.js`, `.png`, `.svc`, `.svg`, `.jpg`, `.gif`, `.j`

          詳細については、このMicrosoftの記事を参照してください。
        - 以下のHTTP動詞のみを許可する:

          `GET`, `POST`, `HEAD`

詳細については、このMicrosoftの記事を参照してください。

2. 不要なハンドラーマッピングを削除します。

   Web Studioには`StaticFile`ハンドラーマッピングのみが必要です。他のものはすべて削除してください。詳細については、このMicrosoft記事を参照してください。

3. 未使用のISAPIフィルターを削除します。

   Web StudioはISAPIフィルターを必要としません。すべて削除できます。詳細については、このMicrosoft記事を参照してください。

   > **注:**
   >
   > ASP.NETにはISAPI Windows機能が必要です。

4. `C:\inetpub\wwwroot`から以下のデフォルトIISランディングページファイルを削除します。

   - `iisstart.htm`
   - `welcome.png`

5. **.NET信頼レベル**が**完全信頼**に設定されたままであることを確認してください。この設定はインストール中に自動的に構成され、Web Studioが正しく機能するために必要です。変更しないでください。

未使用のアプリケーションプール権限を削除する

インストール中、Web Studioアプリケーションプールには以下のユーザー権限が付与されます。

- **サービスとしてログオン**
- **プロセスのメモリクォータを調整**
- **セキュリティ監査を生成**
- **プロセスレベルトークンを置き換える**

これらの権限はIISアプリケーションプールの標準です。Web Studioはこれらを使用しないため、削除できます。

Web Studioの展開を分離する

Web Studioと同じWebドメイン（ドメイン名とポート）に任意のWebアプリケーションを展開できます。ただし、それらのWebアプリケーションにおけるセキュリティリスクは、Web Studio展開のセキュリティを低下させる可能性があります。より高度なセキュリティ分離が必要な場合は、

Web Studioを他のサードパーティアプリケーションとは別のWebドメインに展開することをお勧めします。

Web Studio のスマートカード認証を設定する

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

ステップ 1: スマートカードドライバーをインストールする

ステップ 2: スマートカードユーザーに証明書を発行する

ステップ 3: スマートカードユーザーの証明書を登録する

ステップ 4: Web Studio IIS サーバーを構成する

ステップ 5 (オプション): Web Studio の認証委任を構成する

ステップ 6: Web Studio のスマートカード認証を有効にする

> **注:**

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

ステップ 1: スマートカードドライバーをインストールする

以下のマシンにスマートカードドライバーをインストールします。

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

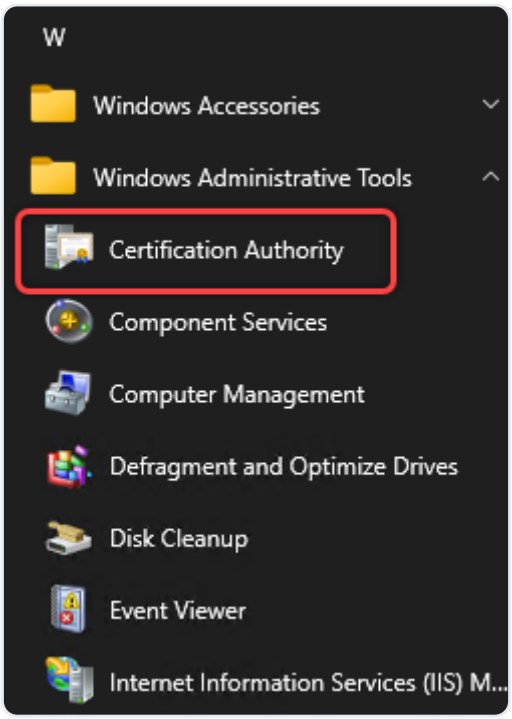
スマートカードドライバーはベンダーによって異なります。たとえば、ITS が提供するスマートカードハードウェアを使用している場合は、`<https://support.globalsign.com/ssl/ssl-certificates-installation/safenet-drivers>` から SaftNet ドライバーをダウンロードしてください。

ステップ2：スマートカードユーザーの証明書を発行する

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

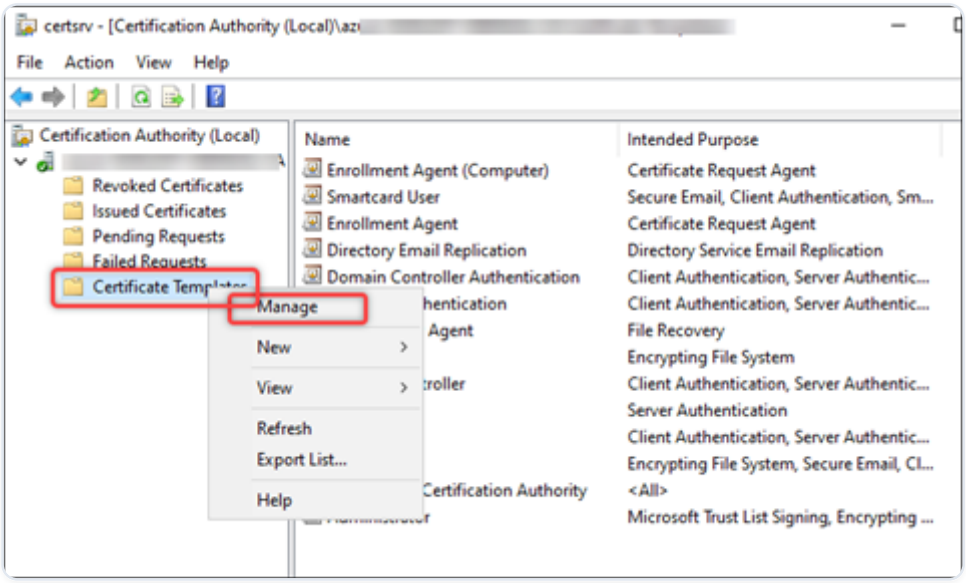
ドメインコントローラーで、以下の手順に従ってタスクを完了します。

1. ドメインコントローラーにアクセスし、**証明機関**を開きます。



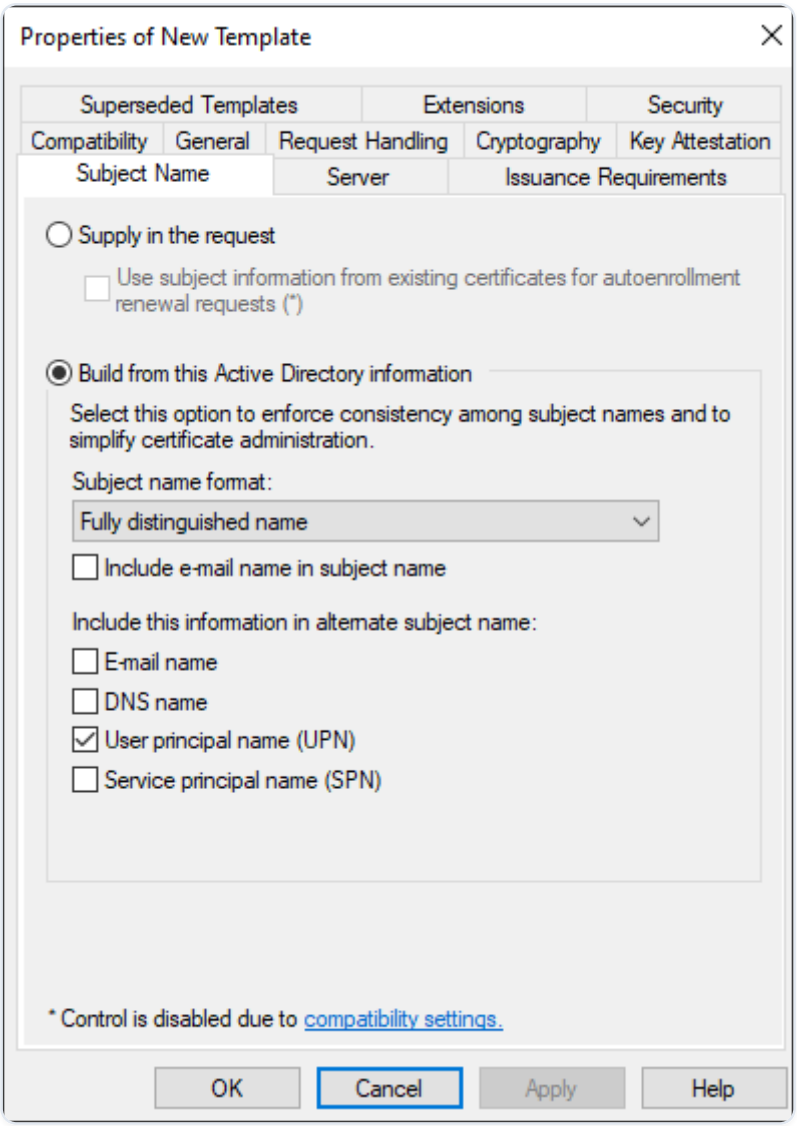
2. **登録エージェント**テンプレートを複製します。詳細な手順は次のとおりです。

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

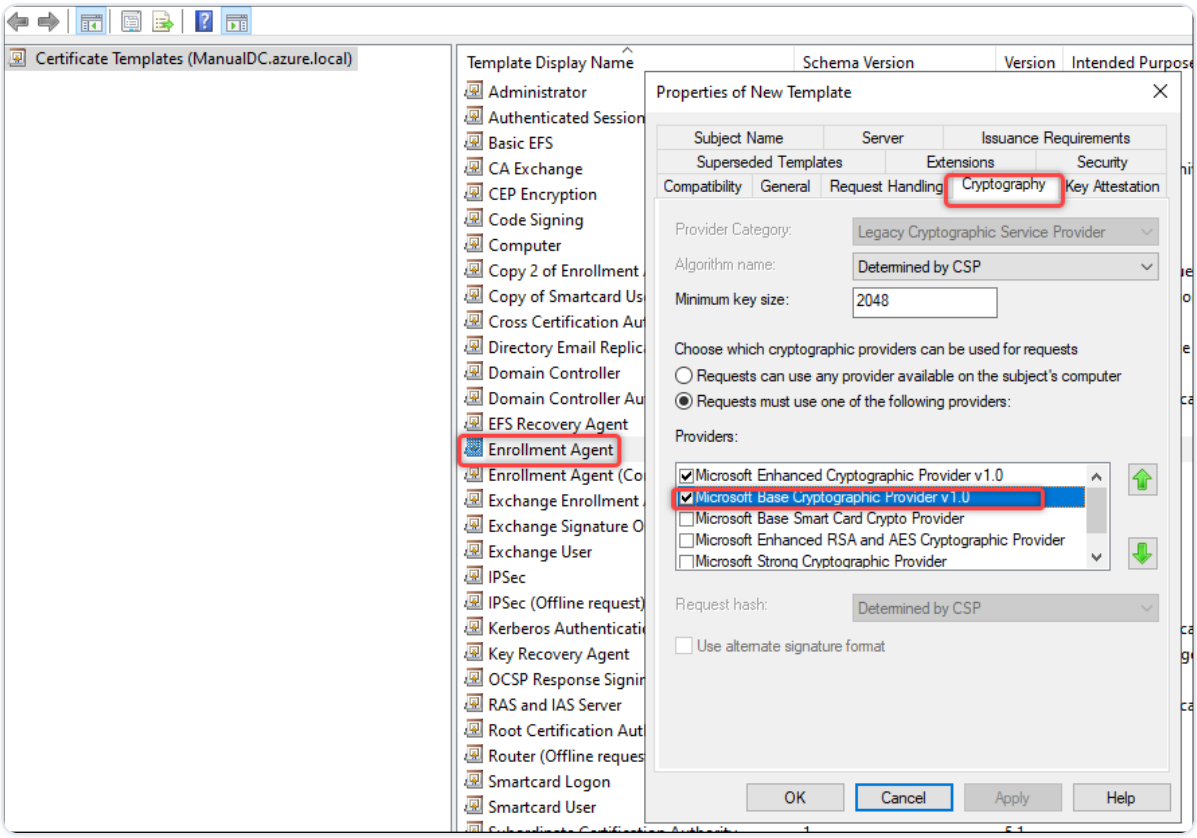


b. **登録エージェント**を右クリックし、**テンプレートの複製**を選択します。

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



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



3. スマートカードの証明書を発行します。詳細な手順は次のとおりです。

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

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

   c. **OK**をクリックします。

ステップ3：スマートカードユーザーの証明書を登録する

> **注:**

> 以下の手順は、プロセスをガイドするための例として提供されています。

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

1. 登録用にドメインに参加している物理Windowsマシンを準備します。

   a. スマートカードドライバーがインストールされていることを確認します。

   b. スマートカードをマシンに挿入します。

c. スマートカードに割り当てるユーザーアカウントを使用してマシンにログオンします。

2. ステップ1で準備したマシンに**証明書**スナップインを追加します。詳細な手順は次のとおりです。

   a. 「**mmc**」を開きます。

   b. 「**ファイル**」をクリックし、次に「**スナップインの追加と削除**」をクリックします。

   c. 表示される「**スナップインの追加と削除**」ウィンドウで、「**証明書**」を選択し、「**追加 >**」をクリックします。

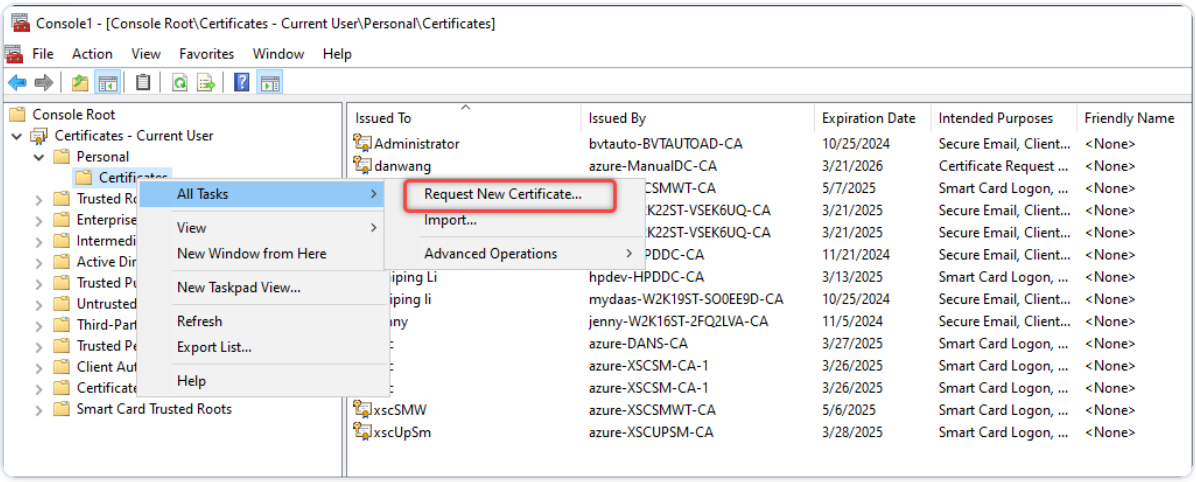
   d. 表示されるダイアログボックスで、「**マイユーザーアカウント**」を選択し、「**完了**」をクリックします。

   e. **OK**をクリックします。

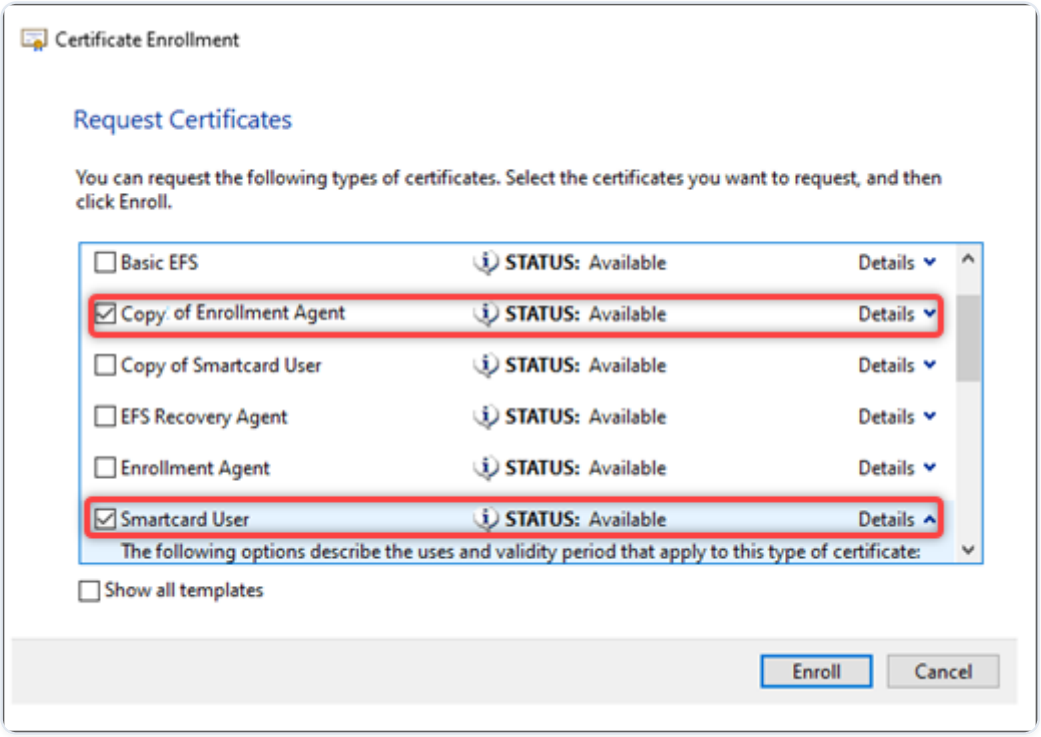
      証明書の追加(/en-us/citrix-virtual-apps-desktops/current-release/media/add-certificate-1.png)

3. 「**証明書**」スナップインの新しい証明書を要求します。詳細な手順は次のとおりです。

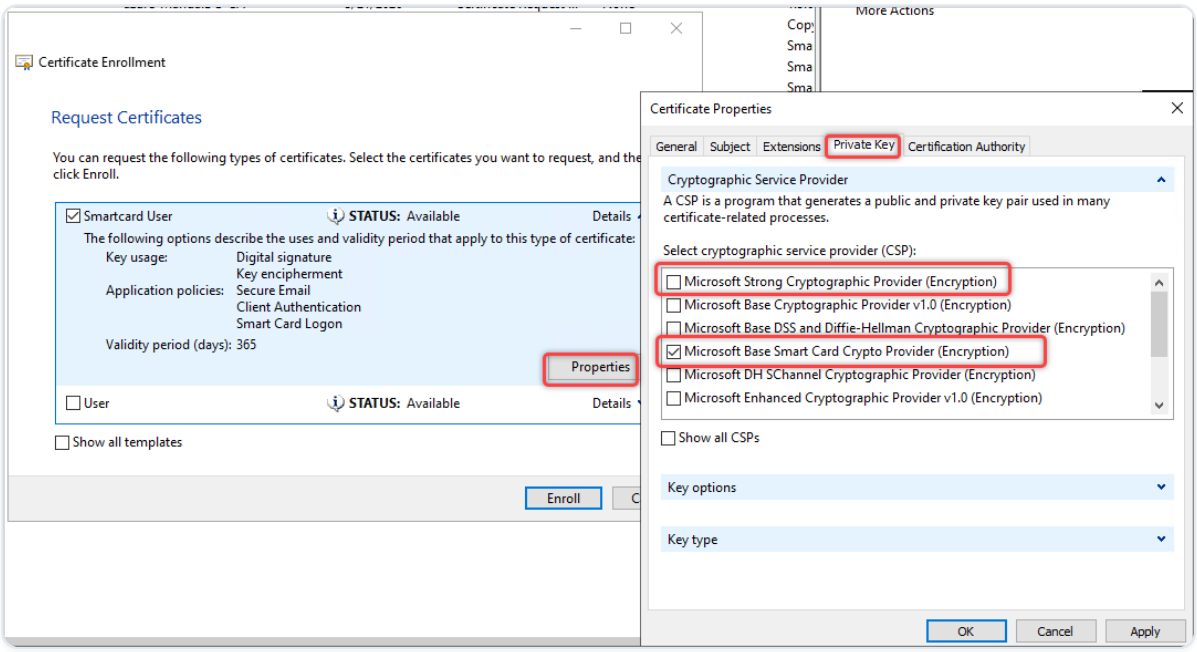
   a. **証明書 - 現在のユーザー > 個人**に移動し、**証明書**を右クリックして、**すべてのタスク > 新しい証明書の要求**を選択します。



   b. 表示される**証明書の要求**ダイアログボックスで、**登録エージェントのコピー**と**スマートカードユーザー**を選択します。



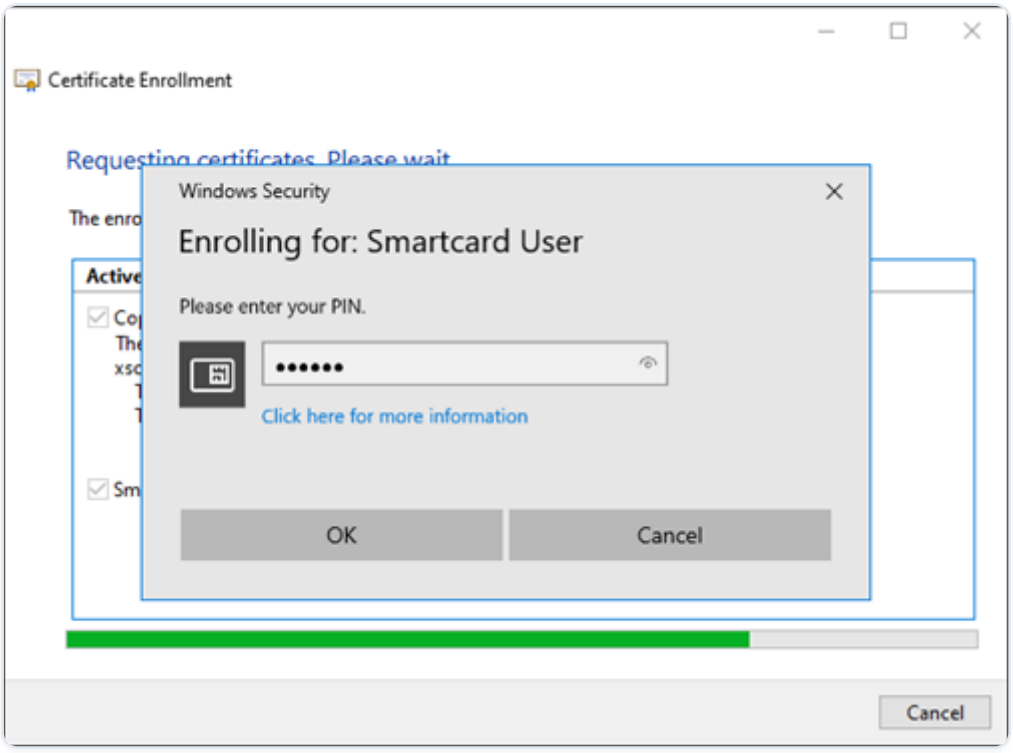
c. 上記のダイアログボックスで、**Smartcard User** の **詳細** をクリックし、次に **プロパティ** をクリックします。**証明書のプロパティ** ダイアログボックスが表示されます。



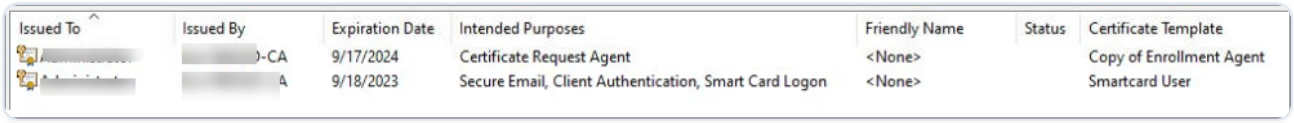
d. **秘密キー**タブで、**暗号化サービスプロバイダー**を展開し、**Microsoft Strong Cryptographic Provider (Encrption)** のチェックを外し、**Microsoft Base Smart Card Crypto Provider (Encryption)** のみを選択して、**OK**をクリックします。

e. **登録**をクリックします。

f. 表示される **Windows セキュリティ** ダイアログボックスで、スマートカードの PIN コードを入力し、**OK** をクリックします。登録が完了したら、**完了** をクリックします。



登録が成功すると、次のスクリーンショットに示すように、**証明書 - 現在のユーザー -> 個人 -> 証明書**の下に2つの証明書が表示されます。



Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Template
	-CA	9/17/2024	Certificate Request Agent	<None>		Copy of Enrollment Agent
		9/18/2023	Secure Email, Client Authentication, Smart Card Logon	<None>		Smartcard User

手順4：Web Studio IISサーバーを構成する

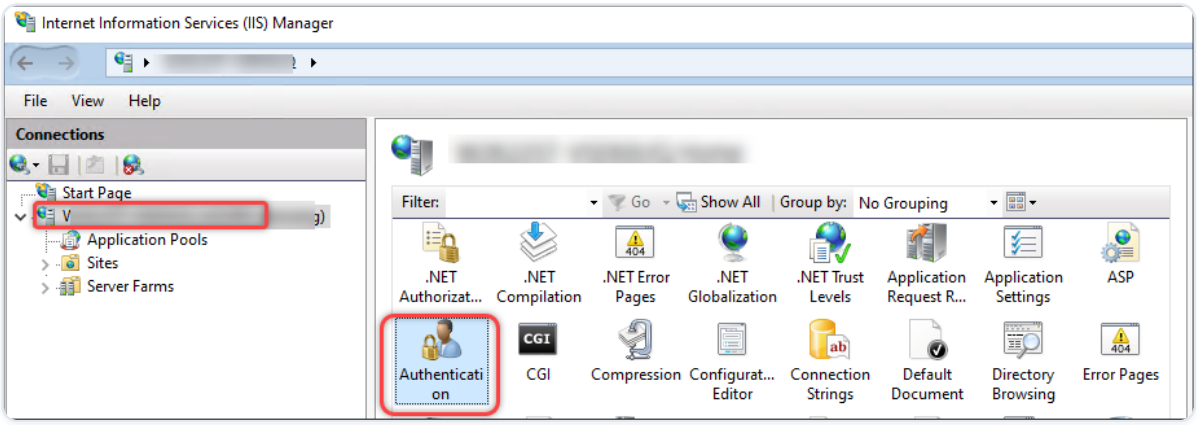
各Web Studioサーバーで、スマートカード認証用にIISを構成するには、次の手順に従います。

1. Web Studio マシンで **クライアント証明書マッピング認証** を有効にします。

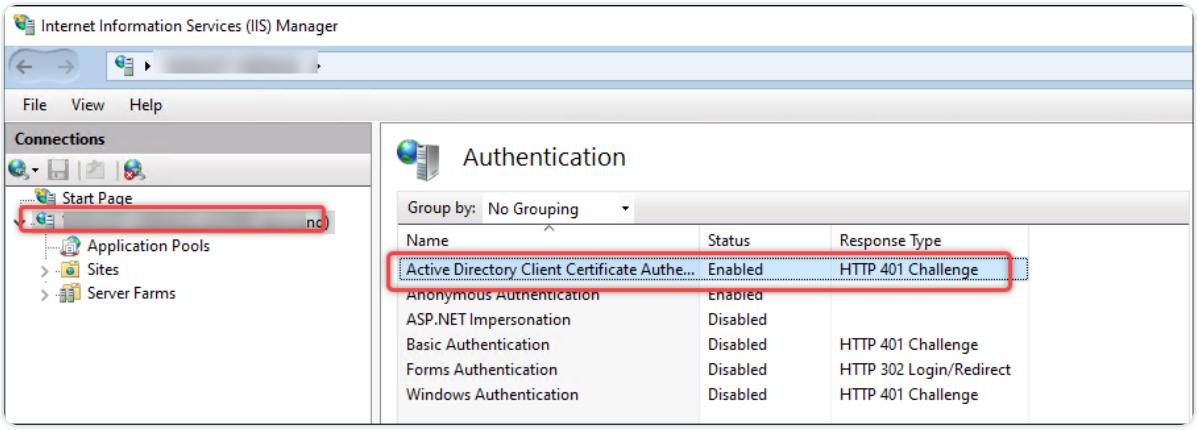
   `<clientCertificateMappingAuthentication>` 要素は、IIS 7以降のデフォルトインストールでは利用できません。インストールと有効化の詳細については、このMicrosoftの記事を参照してください。

2. Web StudioマシンでIIS マネージャーを起動します。
3. 「**Active Directory クライアント証明書認証**」をマシンで有効にします。詳細な手順は次のとおりです。

   a. 左ペインでマシンを選択し、「**認証**」をダブルクリックします。

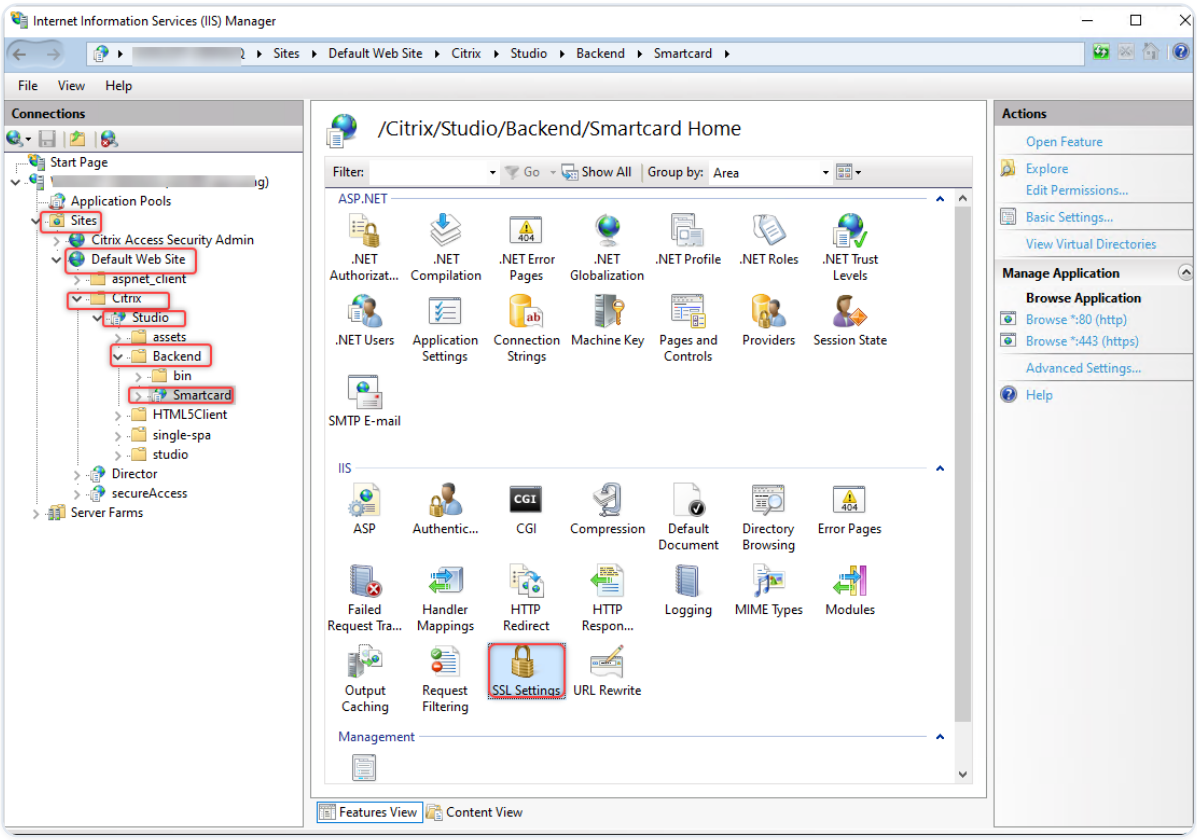


b. 「**Active Directory クライアント証明書認証**」を有効にします。

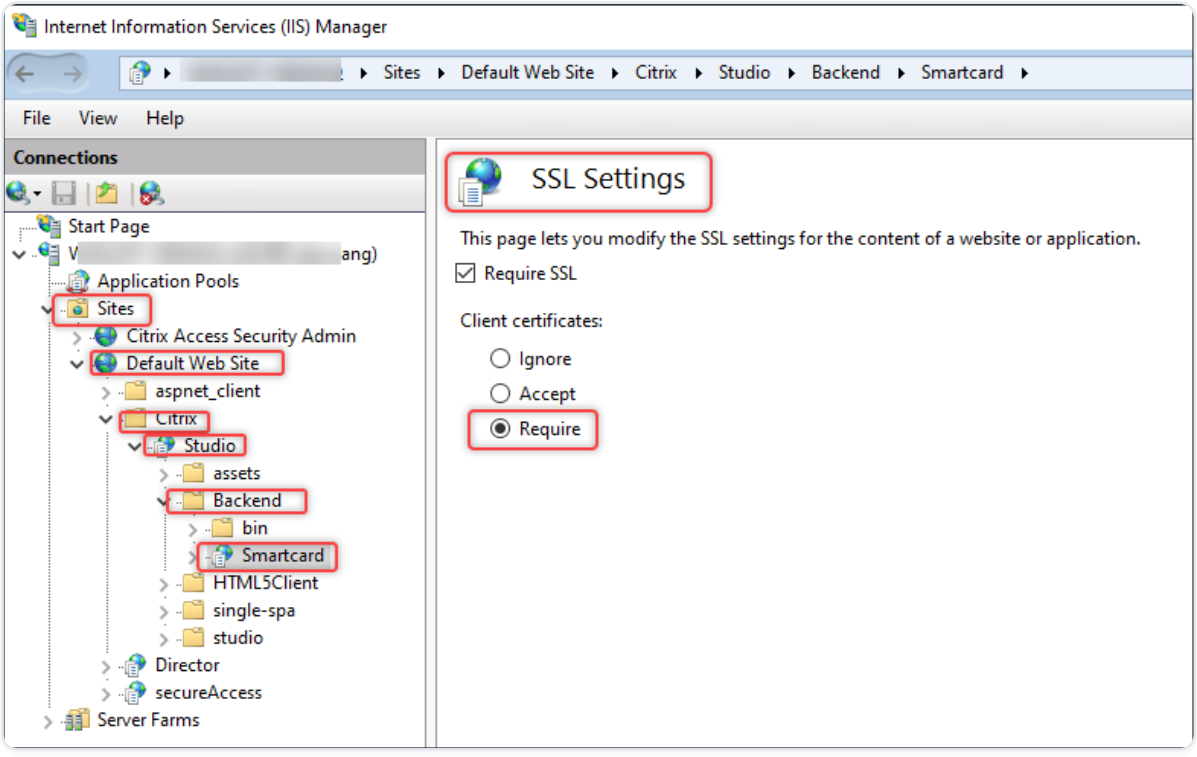


4. クライアント証明書認証を使用して、より安全なHTTPSプロトコルのWeb Studioバックエンドモジュールを構成します。

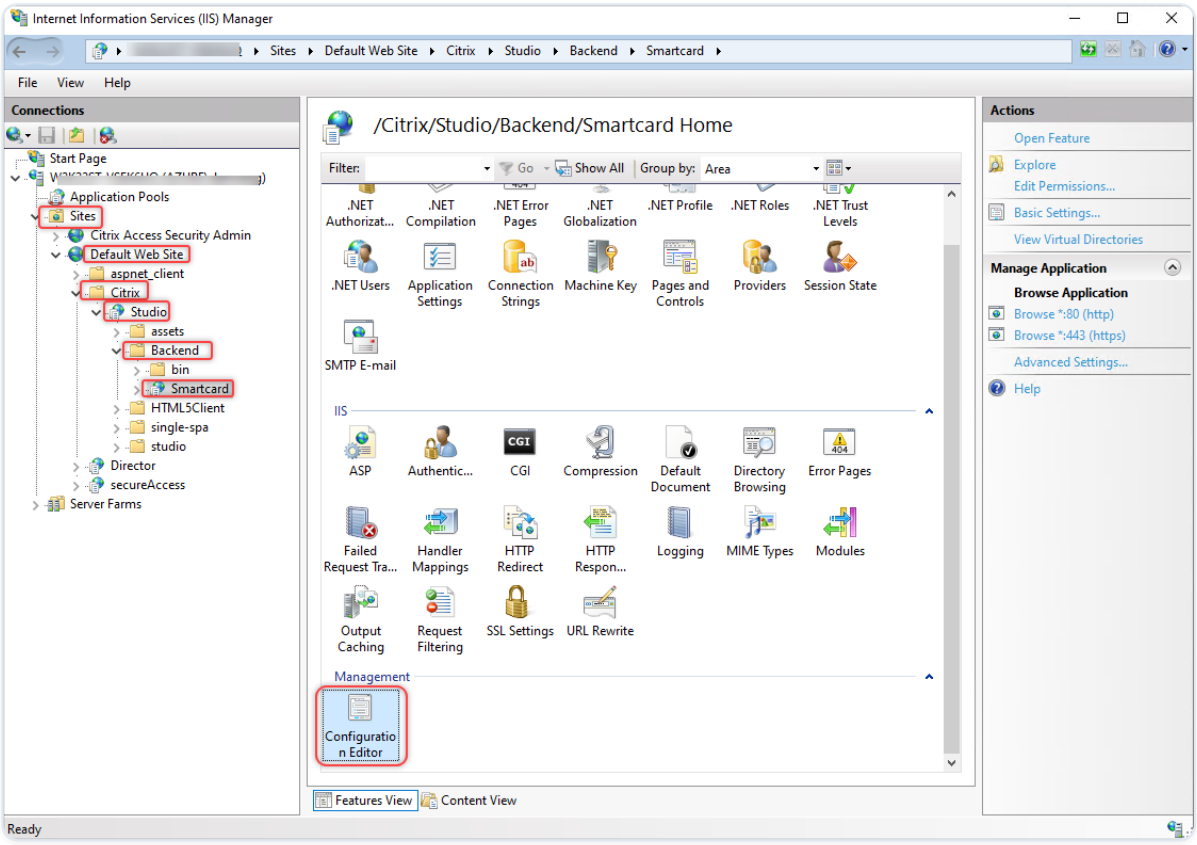
   a. **サイト >** `the IIS site name where Web Studio is installed (site ID = 1, by default, Default Web Site)` **> Studio > Backend > Smartcard** に移動し、次に、**IIS** セクションで **SSL 設定** をダブルクリックします。



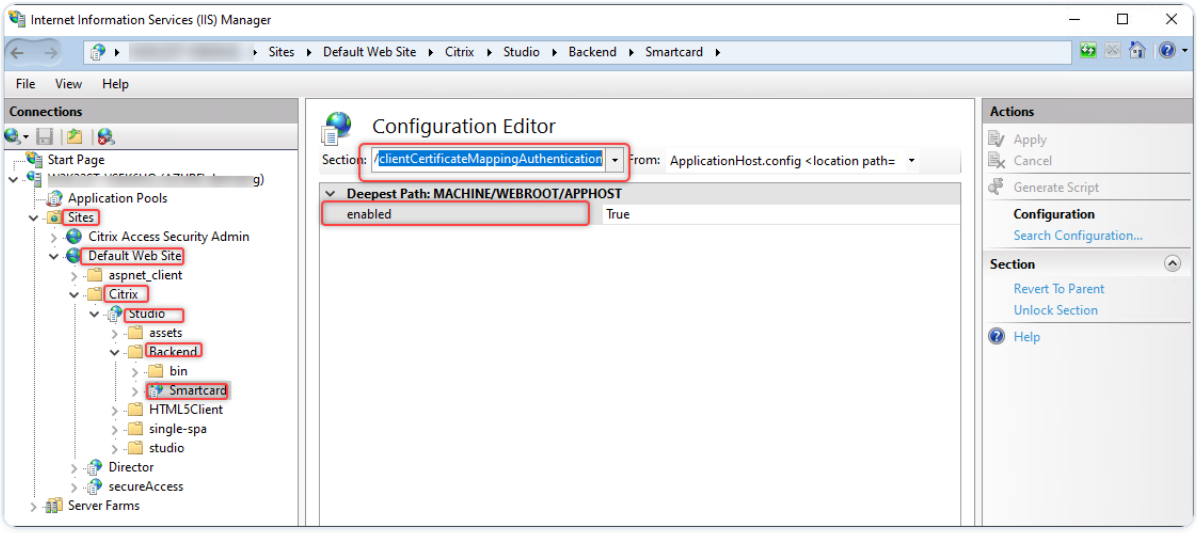
b. 「**クライアント証明書**」で「**要求**」を選択します。



c. **サイト >** `the IIS site name where Web Studio is installed (site ID = 1, by default, Default Web Site)` **> Studio > Backend > Smartcard** に戻り、次に、**IIS** セクションで **構成エディター** をダブルクリックします。



d. **/clientCertificateMappingAuthentication**が**有効**になっていることを確認します。



5. (Windows 2022のみ) TCP経由のTLS 1.3を無効にします。詳細な手順は次のとおりです。

   a. **サイト >** `the IIS site name where Web Studio is installed (site ID = 1, by default, Default Web Site)` に移動します。

   b. 「**サイトの編集 > バインド**」をクリックします。

   c. 表示される「**サイトバインド**」ダイアログボックスで、「**https**」レコードを選択し、「**編集**」をクリックします。

Windows 2022 のみ https 編集(/en-us/citrix-virtual-apps-desktops/current-release/media/iis-server-default-site-https-edit.png)

d. 表示される「**サイトバインドの編集**」ダイアログボックスで、「**TCP 経由の TLS 1.3 を無効にする**」を選択し、「**OK**」をクリックします。

Windows 2022 のみ https 編集無効(/en-us/citrix-virtual-apps-desktops/current-release/media/iis-server-default-site-https-edit-disable.png)

知っておくと良いこと:

Web Studio バックエンドは、Web Studio のモジュールであり、次の機能を提供します。

- スマートカード認証。
- 統合 Windows 認証を使用したオーケストレーションサービスからの FMA ベアラートークンの取得。

手順 5 (オプション) Web Studio の認証委任を構成する

Web Studio と Delivery Controller が異なるサーバーにインストールされている場合、各 Web Studio サーバーから Delivery Controller への HOST および HTTPS サービスに対する委任を構成する必要があります。

各 Web Studio サーバーでタスクを完了するには、次の手順に従います。

1. Delivery Controller™ オーケストレーション HTTPS 証明書をインポートする
2. Web Studio サーバーの委任を構成する
3. （オプション）Web Studio IIS サーバーのサービスアカウントの委任を構成する

DELIVERY CONTROLLER ORCHESTRATION HTTPS証明書のインポート

Web Studioサーバーで、**Delivery Controller Orchestration HTTPS**証明書を**信頼されたルート証明機関**にインポートします。詳細な手順は次のとおりです。

1. **設定 > コンピューター証明書の管理**を開始します。
2. **信頼されたルート証明機関 > 証明書**を右クリックし、**すべてのタスク > インポート**を選択します。

   DDC証明書のインポート(/en-us/citrix-virtual-apps-desktops/current-release/media/web-server-ddc-cert-import.png)
3. 画面の指示に従って、**Delivery Controller Orchestration HTTPS**証明書をインポートします。

WEB STUDIOサーバーの委任を構成する

ドメインコントローラーで、Web StudioサーバーからDelivery ControllerへのHOSTおよびHTTPサービスの委任を構成します。タスクを完了するには、次の手順に従います。

1. ドメインコントローラーで、**Active Directory管理センター**を開始します。
2. 委任を構成する Web Studio サーバーの **コンピューター** アカウントを見つけます（*例: Dan002*）。
3. アカウントを右クリックし、**プロパティ** を選択し、次の手順を実行します。

   Studioサーバーの委任を構成する(/en-us/citrix-virtual-apps-desktops/current-release/media/kerbero-delegation-1.png)

   a. **委任**タブに移動します。

      委任設定を入力する(/en-us/citrix-virtual-apps-desktops/current-release/media/kerbero-delegation-2.png)

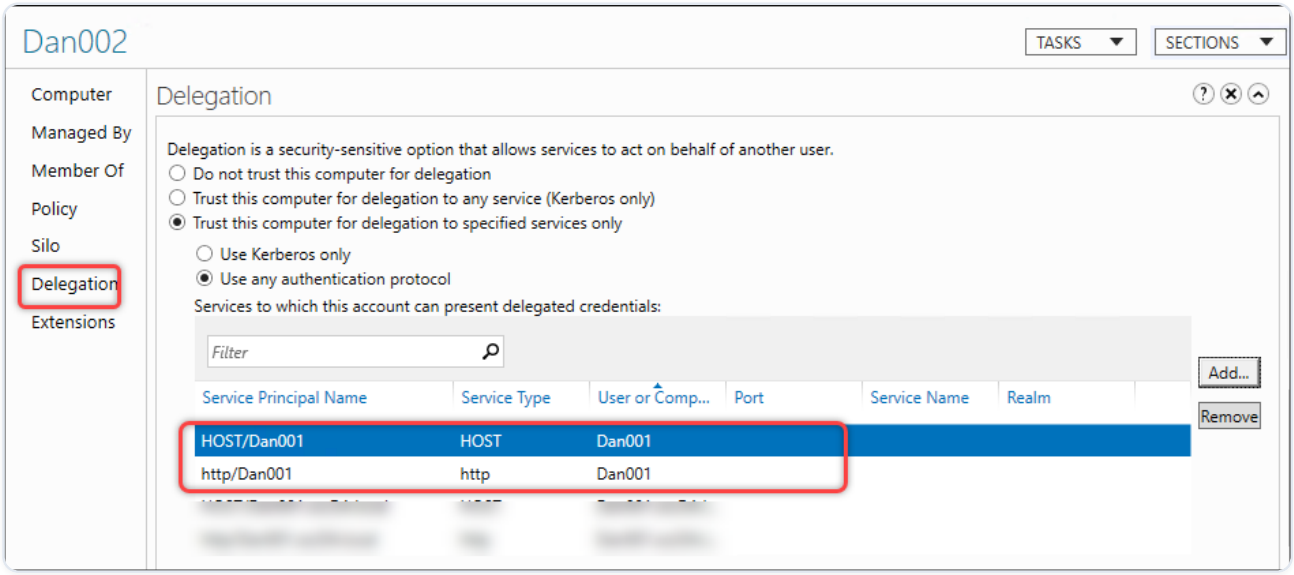
   b. **>** を選択します。

   c. このコンピューターアカウントを委任できるサービスを指定するには、 をクリックします。

   d. 表示される ダイアログボックスで、 をクリックして、Delivery Controller のコンピューター名（*例: Dan001*）を見つけます。

   e. **HOST** サービスと **HTTP** サービスを選択し、 をクリックします。

構成結果を次のスクリーンショットに示します。

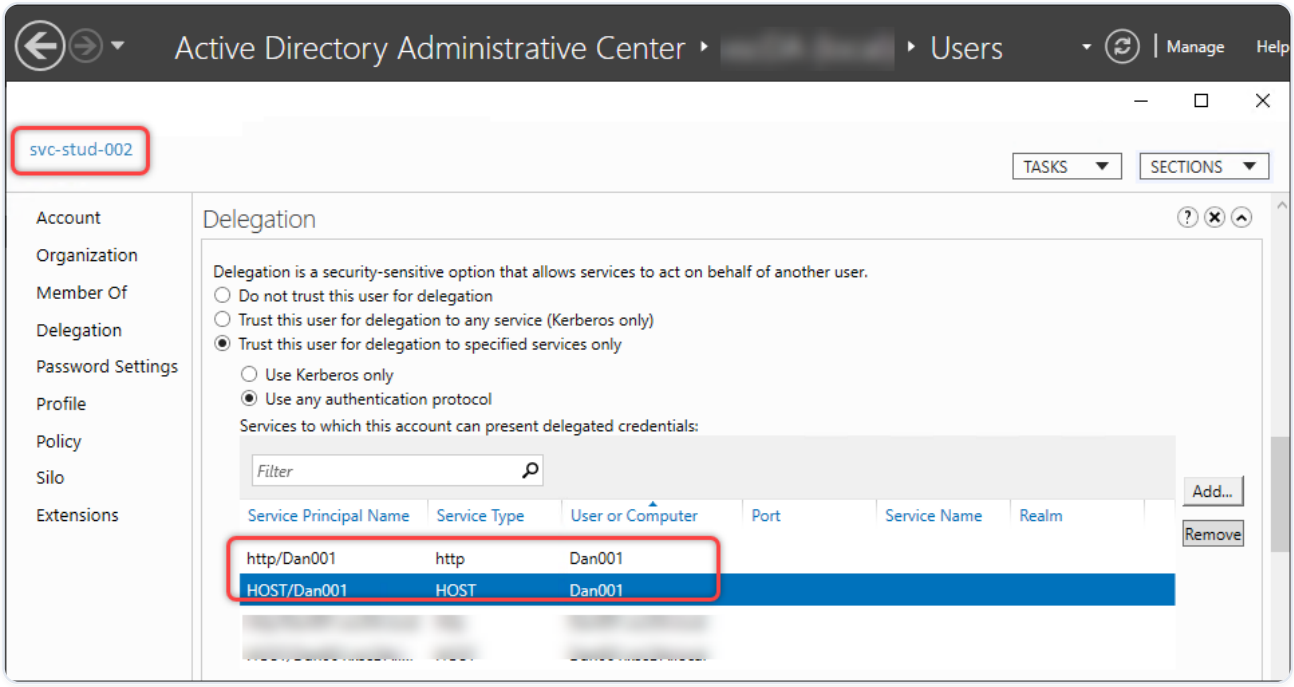


（オプション）WEB STUDIO IIS サーバーのサービスアカウントの委任を構成する

Web Studio IIS サーバーにサービスアカウントを構成している場合は、このサービスアカウントの委任を、HOST および HTTP サービス用の Delivery Controller に対して構成する必要もあります。この委任が確立されると、Web Studio サーバーはサービスアカウントを使用して、現在のスマートカードユーザーになりすまし、HOST および HTTP サービス用の Delivery Controller にアクセスできます。構成を完了するには、次の手順に従います。

1. ドメインコントローラーで、**Active Directory管理センター**を開始します。
2. 委任を構成する Web Studio IIS サーバーの **ユーザー** アカウント（サービスアカウント）を見つけます（*例: svr-stud-002*）。
3. アカウントを右クリックし、**プロパティ**を選択します。
4. 「Web Studioサーバーの委任を構成する」(#configure-delegation-for-the-web-studio-server)のステップ3で説明されている手順に従い、Web Studio IISサーバーのサービスアカウントを、HOSTサービスおよびHTTPサービスのためにDelivery Controllerに委任します。

構成結果を次のスクリーンショットに示します。



手順 6：Web Studio のスマートカード認証を有効にする

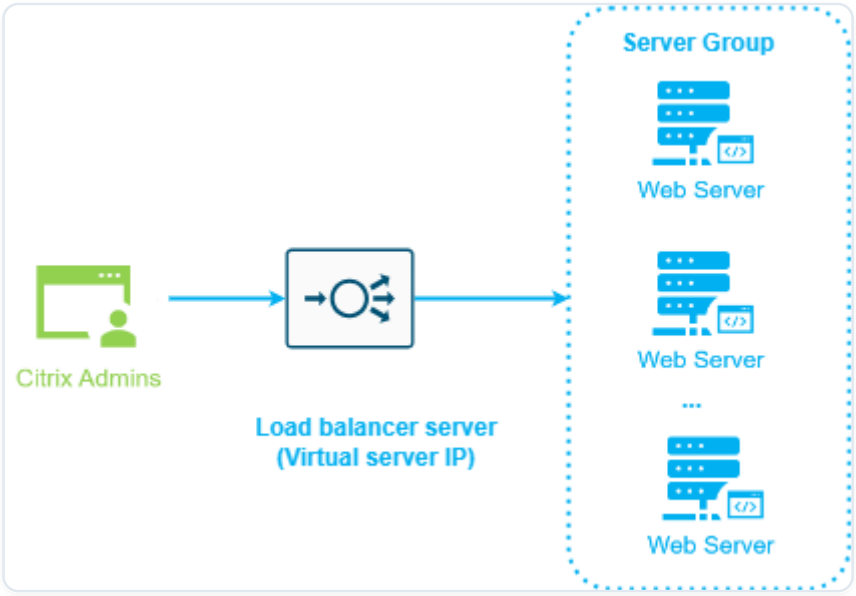
Web Studio のスマートカード認証を有効にするには、次の手順に従います。

1. **Web Studio**にサインインし、左側のペインで**設定**を選択します。
2. 必要に応じて、**スマートカード認証**または**ドメイン資格情報またはスマートカード認証**を選択します。
3. **適用**をクリックします。

証明書テンプレートの管理(/en-us/citrix-virtual-apps-desktops/current-release/media/enable-stud-settings.png)

負荷分散されたWeb Studio展開をセットアップする

高可用性Web Studio展開をセットアップするには、NetScaler® ADC や Windows ネットワーク負荷分散などのツールを選択できます。この記事では、NetScaler ADCアプライアンスを使用して負荷分散されたWeb Studio展開をセットアップする方法について、ステップバイステップのガイドを提供します。



証明書の要件

商用証明機関から証明書を購入する前、またはエンタープライズ証明機関から証明書を発行する前に、ニーズに基づいて以下のオプションを検討してください。

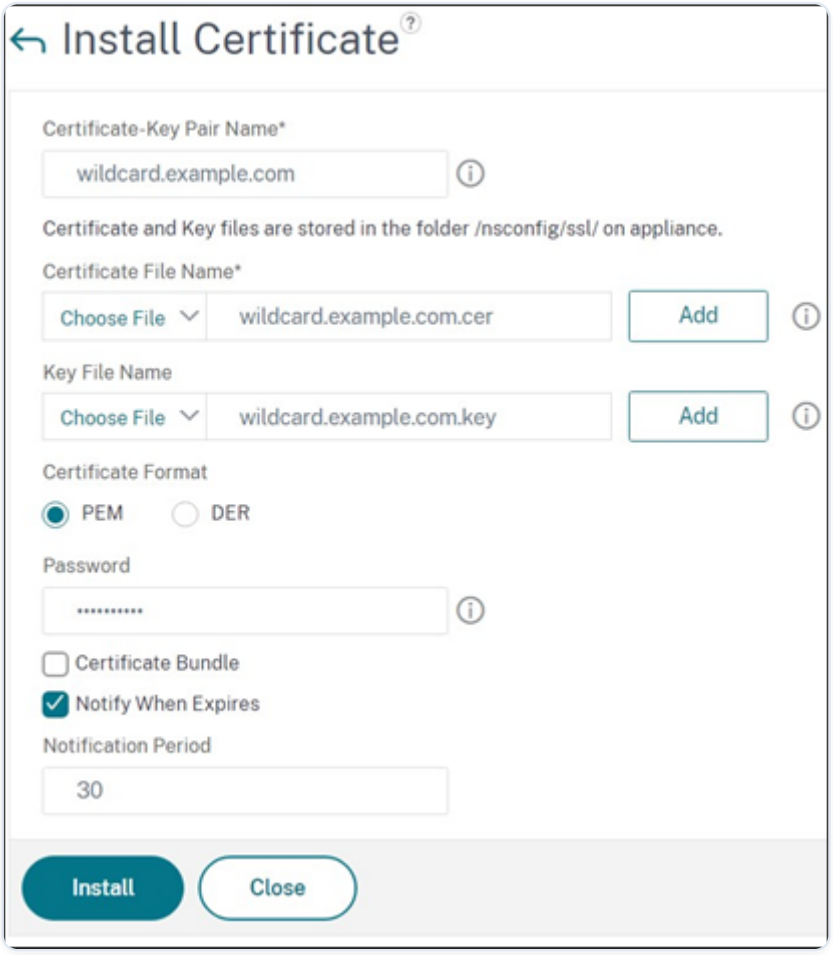
オプション	長所	短所
オプション1：NetScaler ADCアプライアンスのロードバランサーサーバーとWeb Studioサーバーの両方で、*.example.com ワイルドカード証明書を使用する。	• 構成を簡素化する • 管理が容易（単一の証明書） • 証明書を更新せずに新しいサブドメインを追加できる	• ワイルドカード証明書が侵害された場合、すべてのサブドメインが危険にさらされる • すべてのアプリケーションがワイルドカード証明書をサポート

オプション	長所	短所	
		しているわけではない • 個別の証明書よりも高価になる可能性がある	
オプション2：NetScaler ADCアプライアンスのロードバランサーサーバーとWeb Studioサーバーの両方で、サブジェクト代替名 (SAN) を持つ証明書を使用する。	• 柔軟性があり、複数の特定のドメインとサブドメインを含めることができる • 複数のドメインの管理を一元化します • 複数の異なる名前をサポートし、ワイルドカードよりも柔軟性を提供します	• SANエントリの管理は、ドメイン数が増えるにつれて複雑になる可能性があります • 新しいドメインを追加するには、証明書の再発行が必要です • CAがサポートするSANエントリの数によって制限されます	
オプション3：各Web StudioサーバーとNetScaler ADCアプライアンスロードバランサーサーバーに証明書を使用する	• 各サーバーは個別に保護されます • 1つの証明書が侵害されても、他の証明書には影響しません • 各サーバーのニーズに合わせて調整された特	• 各証明書を個別に管理する必要があるため、管理オーバーヘッドが高くなります • 更新する証明書が増え、コストが高くなる可能性があります	

オプション	長所	短所
	定の証明書を使用できます	• すべての証明書が一貫して構成されていることを確認する必要があります

ロードバランサーでサーバー証明書を構成する

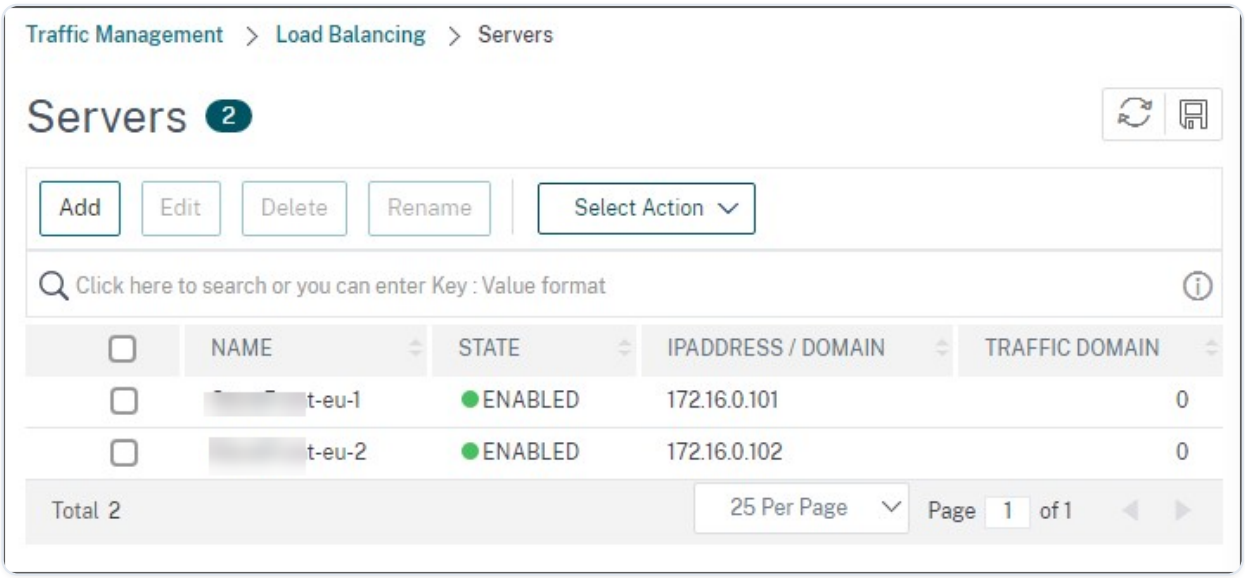
1. NetScaler ADCアプライアンス管理GUIにログオンします。
2. **トラフィック管理 > SSL > 証明書 > サーバー証明書** を選択します
3. 「**インストール**」をクリックします。
4. 「**Install Server Certificate**」ページで、証明書とキーペアの名前を入力し、「**Choose File**」をクリックして、証明書ファイルを参照します。証明書ファイルに秘密キーが含まれていない場合は、「**Key File**」を選択します。



ステップ1: Web Studioサーバーノードを追加する

すべてのWeb Studioサーバーノード (例: `Studio-eu-1` および `Studio-eu-2`) をロードバランサーに追加します。

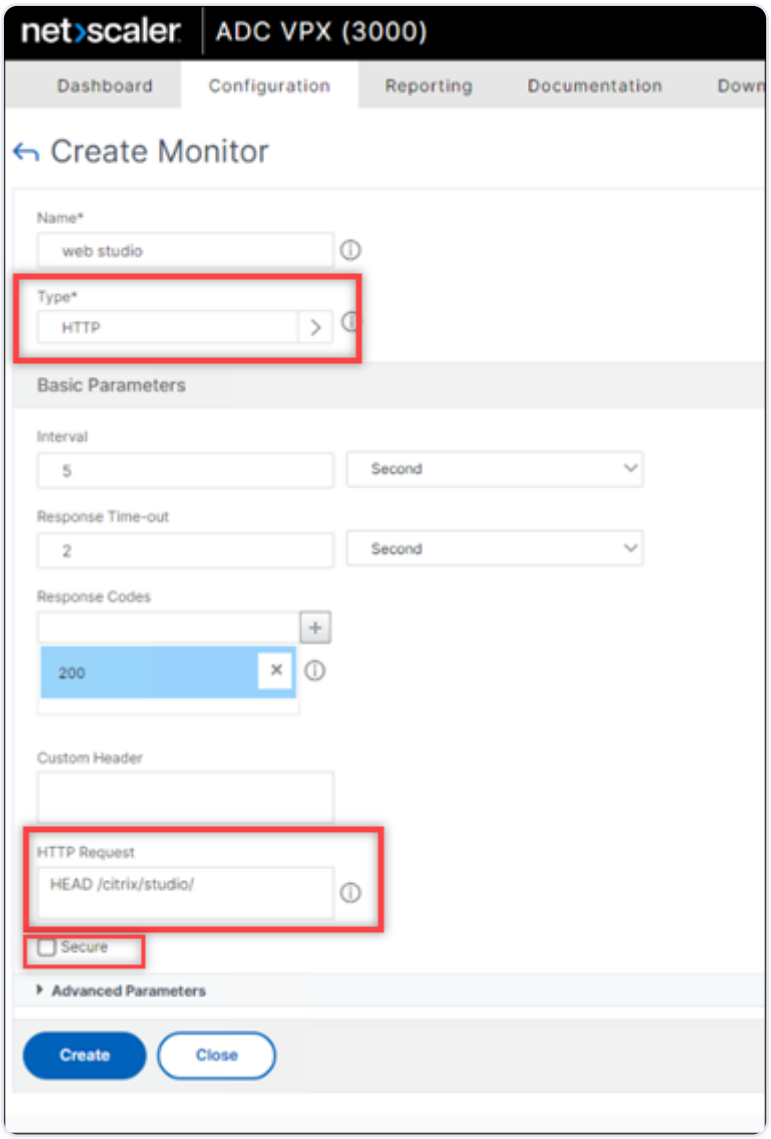
1. NetScaler ADC管理GUIにログオンします。
2. **Traffic Management > Load Balancing > Servers**に移動します。**追加**をクリックします。
3. Web Studioサーバーノードのサーバー**IP**アドレスを入力します。
4. 他のWeb Studioサーバーを追加するには、ステップ2〜3を繰り返します。



ステップ2: Web Studioサーバーノード用のモニターを追加する

すべてのWeb Studioサーバーノードのステータスを確認するために、ロードバランサーでモニターを設定します。

1. **トラフィック管理 > 負荷分散 > モニター > 追加** を選択します。
2. **構成**タブで、次の設定を完了し、その他のデフォルトはそのままにします。
   - **名前**に**Web Studio**と入力します。
   - **タイプ**に**HTTP**または**SSL**を選択します。
   - **Secure**オプションを選択します。
   - **HTTP要求**に**HEAD/citrix/studio/**と入力します。



ステップ3: Web Studioサーバーノード用のサービスグループを作成する

1. **Traffic Management > Load Balancing > Service Groups > Add**を選択します。HTTPS経由でWeb Studioサーバーに接続するには、プロトコルとしてSSLを選択し、その他の設定はデフォルトのままにして、**OK**をクリックします。
2. サービスグループ内で、**Service Group Members**の下にある**No Service Group Member**をクリックし、次の手順に従ってメンバーを追加します。

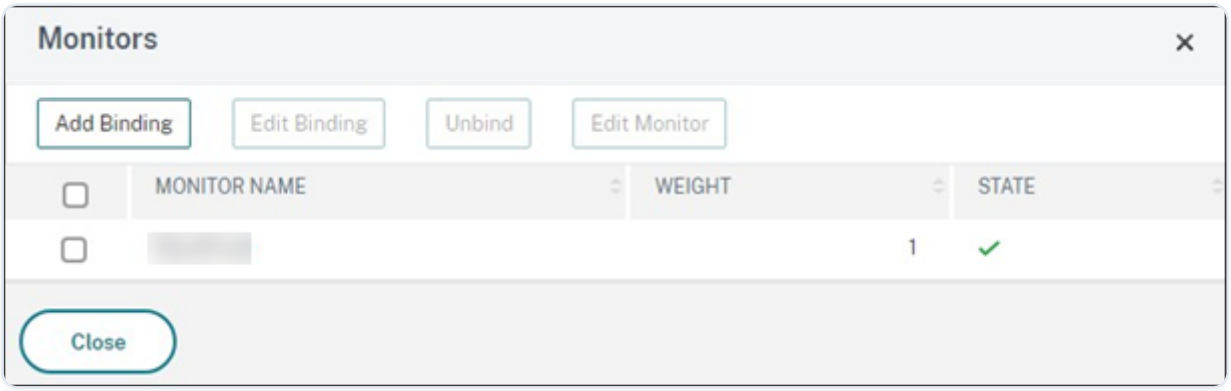
   a. **サービスベース**をクリックします。

   b. 以前に追加したすべてのサーバーを選択します。

   c. ポートに**443**を入力します。

   「サービスグループメンバーの作成」ページのスクリーンショット(/en-us/citrix-virtual-apps-desktops/current-release/media/netscaler-create-service-group-member.png)

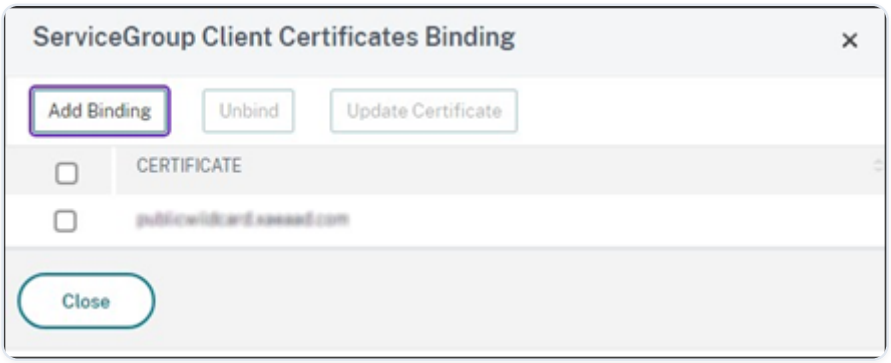
3. **Monitors**セクションを追加し、以前に作成したWeb Studioモニターを選択します。



4. **Certificates**セクションを追加し、次の設定を完了します。

   a. クライアント証明書をバインドします。

   b. 以前にインポートしたサーバー証明書の署名に使用したCA証明書、およびPKI信頼チェーンの一部である可能性のあるその他のCAをバインドします。



5. **Settings**セクションを追加し、**Insert Client IP Header**を選択して、ヘッダー名に**X-Forwarded-For**を入力します。この設定により、クライアントIPアドレスをPoliciesで使用できるようになります。

ステップ4：仮想サーバーを作成する

ユーザーがWeb Studioサーバーグループにアクセスするためのロードバランサー仮想サーバーを作成します。

1. **Traffic Management > Load Balancing > Virtual Servers**に移動し、**Add**をクリックします。
2. 名前を入力し、**Protocol**に**SSL**を選択し、**Port**に**443**を入力して、**OK**をクリックします。

   NetScaler負荷分散仮想サーバー画面のスクリーンショット(/en-us/citrix-virtual-apps-desktops/current-release/media/netscaler-lb-virtual-server.png)

3. 以前に作成した**Service Group**をロードバランシング仮想サーバーにバインドします。
4. ステップ3：Web Studioサーバーノードのサービスグループを作成するでサービスグループにバインドしたCA証明書をバインドします。

5. **Method**セクションを追加し、ロードバランシング方法を選択します。Web Studioのロードバランシングで一般的な選択肢は、**ROUNDROBIN**または**LEASTCONNECTION**です。

   負荷分散メソッドセクションのスクリーンショット(/en-us/citrix-virtual-apps-desktops/current-release/media/leastconnection.png)

6. 「**Persistence**」セクションを追加し、以下の設定を完了します。

   a. 永続化メソッドを「**COOKIEINSERT**」に設定します。

   b. タイムアウトをWeb Studio内のセッションタイムアウトと同じに設定します (デフォルトでは20分)。

   c. 今後のデバッグを容易にするために、Cookieに名前を付けます。例: **NSC_SFPersistence**。

   d. バックアップ永続性を **NONE** に設定します。

   永続性セクションのスクリーンショット(/en-us/citrix-virtual-apps-desktops/current-release/media/persistence.png)

> **注:**
>
> クライアントがHTTP Cookieの保存を許可されていない場合、後続のリクエストにはHTTP Cookieが含まれず、永続化は使用されません。

ステップ5: 仮想サーバーのDNSレコードを作成する

ドメインコントローラーで、仮想サーバーのIPアドレスをFQDNにマッピングするDNSおよびPTRレコードを作成します。ネットワーク内のWeb Studioユーザーは、このFQDNを使用してWeb Studioサーバーグループにアクセスします。たとえば、webstudio.example.comはロードバランサー仮想サーバーのIPアドレス (VIP) に解決されます。

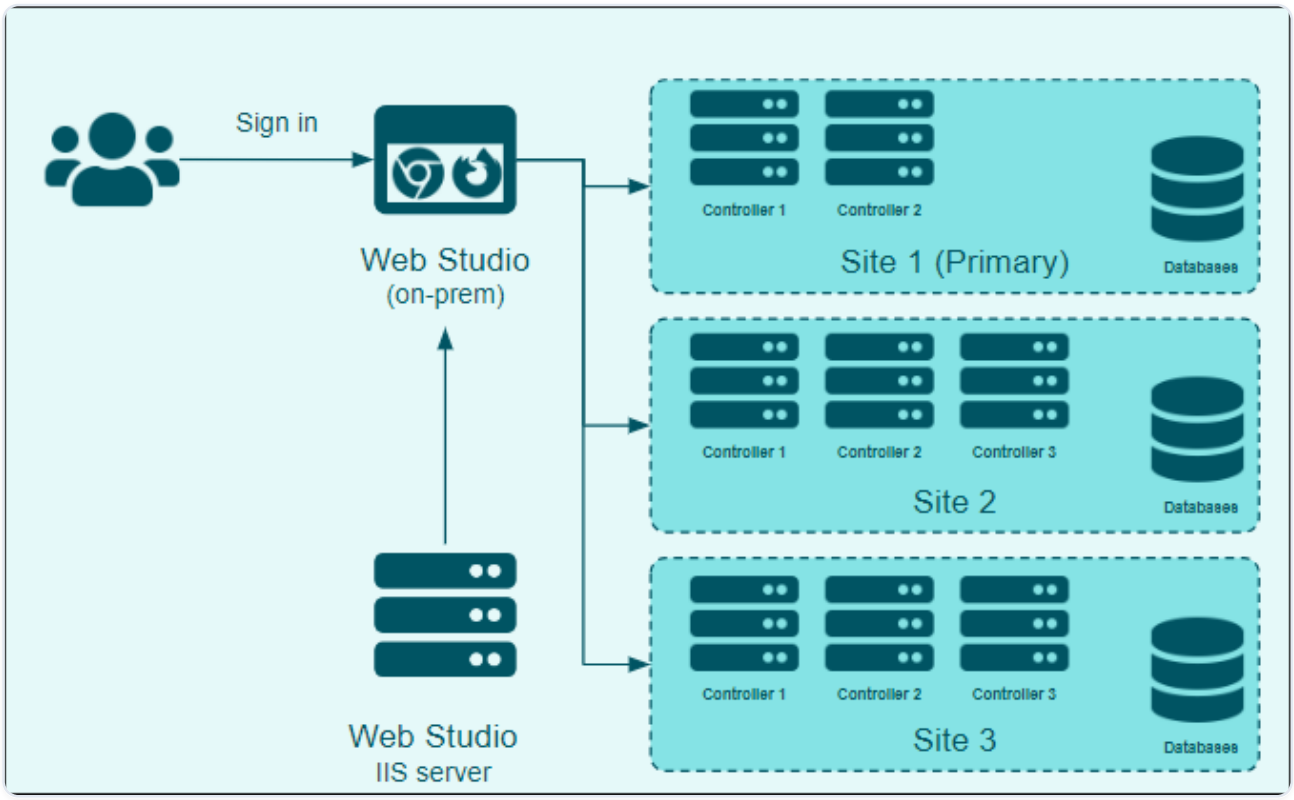
永続性セクションのスクリーンショット(/en-us/citrix-virtual-apps-desktops/current-release/media/new-dns.png)

ユーザーがWeb Studioサーバーにアクセスするためのurlを提供します: `https://<FQDN of the virtual server>/<text you entered in the HTTP Request field when creating a monitor>`。例: `https://webstudio.example.com/citrix/studio`

複数サイト管理を有効にする

デフォルトでは、1つのWeb Studioコンソールは単一のCitrix Virtual Apps and Desktops™サイトにマッピングされますが、必要に応じて、Web Studioコンソールを複数のサイトを管理するように構成できます。これにより、1つのWeb Studioをインストールするだけで、すべてのサイトを構成および管理できます。

次の図は、単一のWeb Studio展開が複数の独立したCitrix Virtual Apps and Desktops™サイトを管理する複数サイトアーキテクチャを示しています。



注:

マルチサイト展開では、Web Studioが1つ前のバージョンのDelivery Controllerに接続することをサポートしています。この下位互換性により、段階的なアップグレードが可能です。ただし、完全な機能を確保するには、すべてのコンポーネントを同じバージョンで実行することをお勧めします。

利点

- 統合されたシングルサインオンエクスペリエンスで複数のサイトを管理する際の効率が向上します。

- すべての構成が1つのコンソールからアクセスできるため、トラブルシューティングが容易になります。

考慮事項

サイトを構成および展開する際は、次の点に留意してください。

- 必須バージョン:
  - Citrix Virtual Apps and Desktops 2311 およびそれ以降のバージョン。
  - Delivery Controller™のバージョンは、Web Studioのバージョンと一致するか、それ以前のバージョンである必要があります。最小要件は2311以降です。
  - この機能はWeb Studio（Webベース）専用であり、Citrix Studio（Windowsベース）では利用できません。
- シングルサインオンをサポートするには、すべてのサイトを信頼されたドメインに展開します。
- 統合されたWeb Studioコンソールを使用して、最大10個のCitrix Virtual Apps and Desktopsサイトを管理できます。

ワークフロー

始める前に

- プライマリサイトを決定し、Web Studioコンソールがプライマリサイト管理にアクセス可能であることを確認します。

  注:

  - プライマリサイトを設計する際は、追加されたサイトのアクセシビリティがプライマリサイトの可用性に依存することに注意してください。プライマリサイトのパフォーマンスの問題は、追加されたサイトへのアクセスに影響を与える可能性があります。
  - Web Studioがインストールされていない場合は、「Web Studioのインストール」を参照してください。

- Web Studioで管理する予定のサイトがすでに設定されていることを確認してください。
  - 新しいサイトを作成するには、「サイトの作成」を参照してください。

- (推奨) コンソールでサイトを切り替える際にシングルサインオンを有効にするには、すべてのサイトで統合Windows認証 (IWA) を有効にします。IWAが有効になっていないサイトでは、ログイン資格情報を使用してサインインすることもできます。

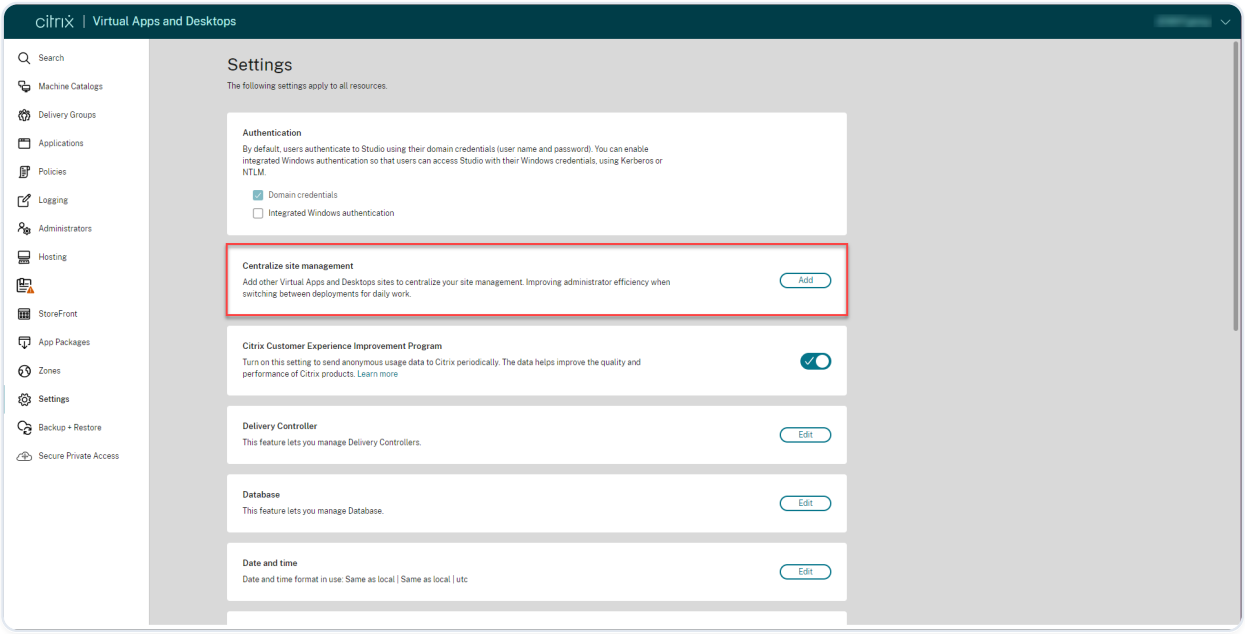
ステップ1：WEB STUDIOコンソールにサインインする

1. Webブラウザを開きます。`https://<address of the server hosting Web Studio>/Citrix/Studio`を入力します。
2. Web Studioにサインインして、プライマリサイトを管理します。

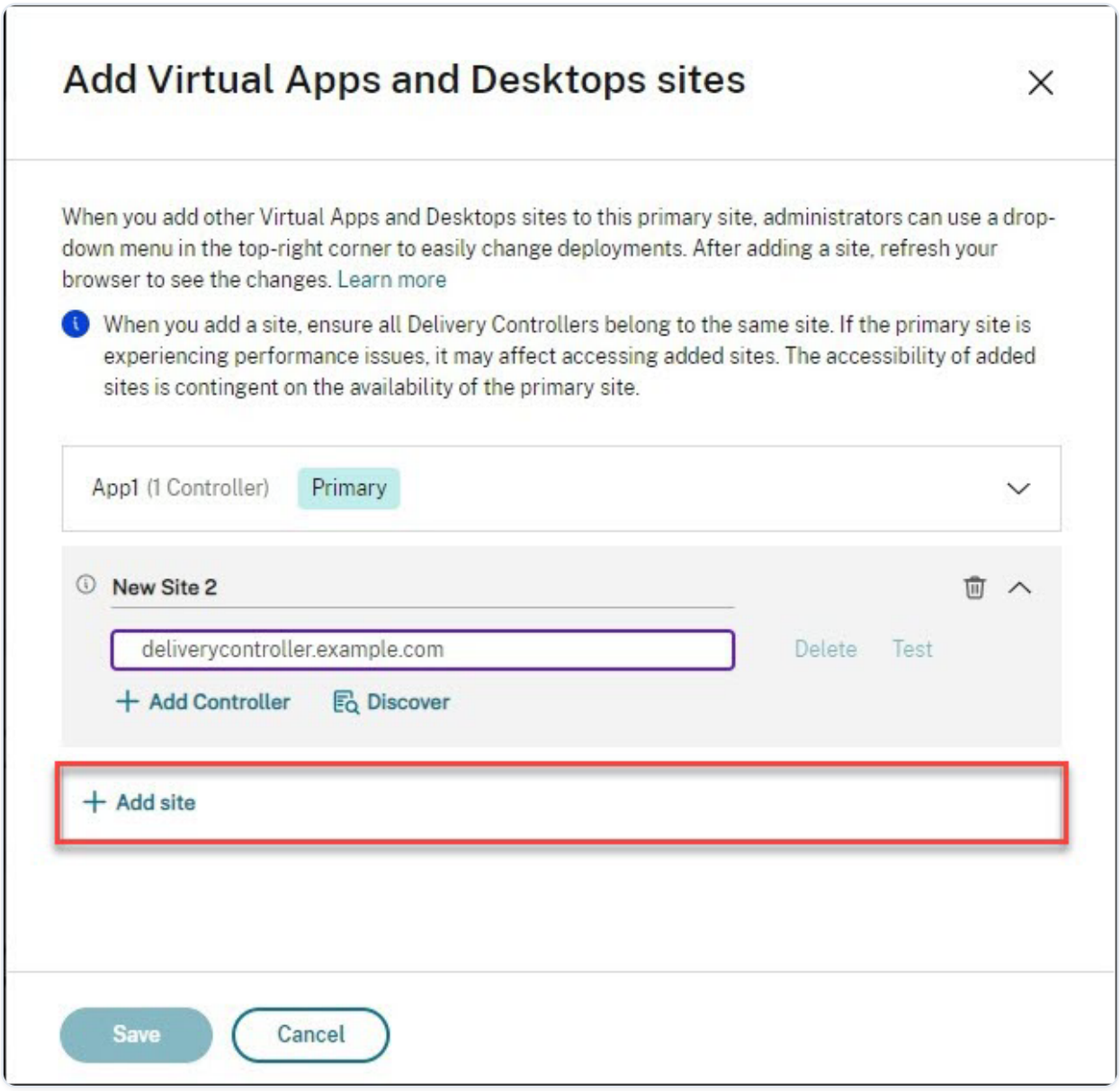
> **注:**
>
> インストール時に使用するDelivery Controllerのアドレスによってサイトが識別されます。Delivery Controllerがプライマリサイトのものである場合、そのサイトにサインインします。

ステップ2：WEB STUDIOを使用してサイトを追加する

1. **設定** > **サイト管理の集中化**に移動し、**追加**をクリックします。



2. **Virtual Apps and Desktopsサイトの追加**ページで、**サイトの追加**をクリックします。



3. Delivery Controllerを追加するには、次のいずれかの操作を実行します。

   - 「**コントローラーの追加**」をクリックし、FQDNを入力します。「**テスト**」をクリックして接続をテストします。
   - 「**検出**」をクリックします。

     a. 「**サイト検出**」ページで、サイト内にあるコントローラーのアドレスを選択または入力します。

     b. コントローラーへの完全なアクセス許可を持つ管理者の資格情報を、「**ユーザー名**」と「**パスワード**」フィールドに入力します。

     c. 「**完了**」をクリックします。

   サイト検出(/en-us/citrix-virtual-apps-desktops/current-release/media/site-discovery.png)

> **注:**
>
> 検出機能は、入力したデリバリーコントローラーのアドレスに基づいて、サイト内で到達可能なデリバリーコントローラーを自動的に追加します。

4. 「**保存**」をクリックします。

   サイト構成を管理または編集するには、「**設定**」>「**サイト管理の集中化**」に移動し、「**管理**」をクリックします。 「**管理**」オプションはプライマリサイトでのみ有効です。

   集中サイトの管理(/en-us/citrix-virtual-apps-desktops/current-release/media/centralize-site-mgmt-manage.png)

ステップ3：サイト設定の管理

サイト構成の変更を反映させるには、ブラウザーを更新してください。サイト選択ボックスは、コンソールの右上隅に表示されます。

「**設定**」ページで、「**更新**」アイコンの横にある右隅のドロップダウンメニューからサイトを選択します。 コンソールには、選択したサイトの構成が表示されます。

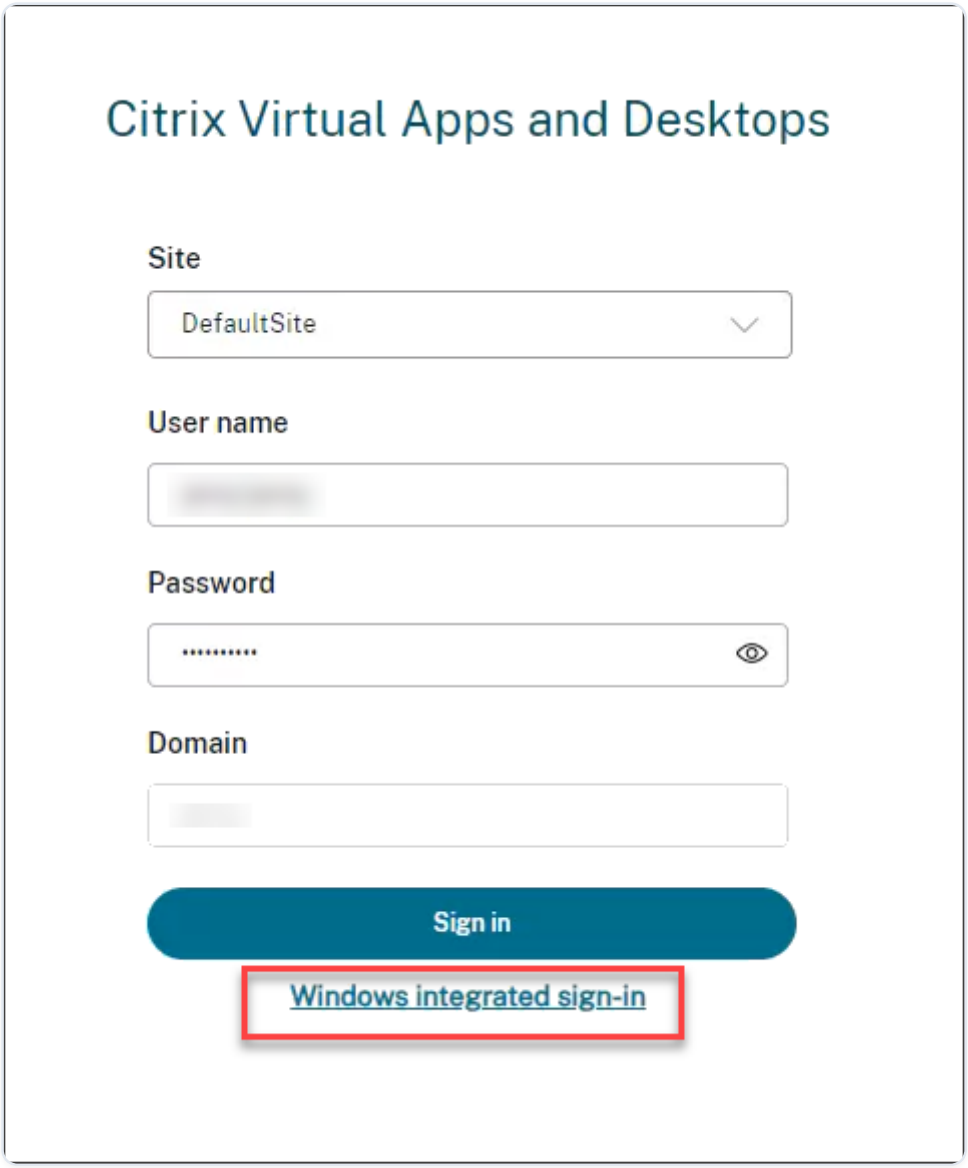
> **注:**
>
> - プライマリサイトに到達できない場合、それに関連付けられている他のサイトにアクセスすることはできません。
> - 別のサイトに切り替える際は、サインインに必要なアクセス許可またはアクセス資格情報があることを確認してください。

サイト構成後のサインインエクスペリエンス

1. Webブラウザーを開きます。`https://<address of the server hosting Web Studio>/Citrix/Studio`を入力します。
2. **サイト**フィールドからサイトを選択します。
3. **Windows統合サインイン**を選択するか、**ユーザー名**と**パスワード**を入力してサインインします。

   > **注:**

> Windows統合サインインは、選択したサイトで有効になっている場合にのみ利用できます。統合Windows認証の詳細については、「認証の管理」を参照してください。



REST API を使用して管理を自動化する

Citrix Virtual Apps and Desktops™ REST API を使用すると、Citrix Virtual Apps and Desktops 展開内のリソースの管理を自動化できます。

Citrix Virtual Apps and Desktops REST API は `<https://developer.cloud.com/citrixworkspace/citrix-daas/citrix-daas-rest-apis/docs/overview>` で利用できます。Citrix Virtual Apps and Desktops に適用されない API は、そのようにマークされています。そこにあるガイダンスに従って、API サービスへのアクセスを設定し、API を使用してリソースを管理および最適化してください。

コマンドラインを使用したインストール

重要:

- アップグレード中で、現在のバージョンでPersonal vDiskまたはAppDisksソフトウェアが使用されているかインストールされている場合は、「PvD、AppDisks、およびサポートされていないホストの削除」を参照してください。
- Citrixは、ライセンスコンプライアンスを含む正当な利益のために、必要に応じて基本的なライセンスデータを収集します。詳細については、「Citrixライセンスデータ」を参照してください。

はじめに

この記事は、Windowsオペレーティングシステムを搭載したマシンにコンポーネントをインストールする場合に適用されます。Linuxオペレーティングシステム用VDAについては、「Linux Virtual Delivery Agent」を参照してください。

この記事では、製品のインストールコマンドを発行する方法について説明します。インストールを開始する前に、「インストールの準備」を確認してください。この記事には、利用可能なインストーラーの説明が含まれています。

コマンドの実行の進行状況と戻り値を確認するには、元の管理者であるか、「**管理者として実行**」を使用する必要があります。詳しくは、Microsoftのコマンドに関するドキュメントを参照してください。

インストールコマンドを直接使用することに加えて、Active Directory内のマシンにVDAをインストール、アップグレード、または削除するサンプルスクリプトが製品ISOに用意されています。詳しくは、「スクリプトを使用したVDAのインストール」を参照してください。

このCitrix Virtual Apps and Desktopsのバージョンでサポートされていないバージョンにインストールまたはアップグレードしようとすると、オプションに関する情報を示すメッセージが表示されます。「以前のオペレーティングシステム」を参照してください。

Citrixがコンポーネントインストールの結果を報告する方法については、「Citrixインストールのリターンコード」を参照してください。

フル製品インストーラーを使用する

フル製品インストーラーのコマンドラインインターフェイスにアクセスするには：

1. Citrixから製品パッケージをダウンロードします。ダウンロードサイトにアクセスするには、Citrixアカウントの資格情報が必要です。
2. ファイルを解凍します。必要に応じて、ISOファイルをDVDに書き込みます。
3. コンポーネントをインストールするサーバーに、ローカル管理者アカウントを使用してログオンします。
4. DVDをドライブに挿入するか、ISOファイルをマウントします。
5. メディアの `\x64\XenDesktop Setup` ディレクトリから、適切なコマンドを実行します。

   コアコンポーネントをインストールするには: `XenDesktopServerSetup.exe` を実行します。オプションについては、コアコンポーネントのインストール用コマンドラインオプション を参照してください。

   VDAをインストールするには: `XenDesktopVDASetup.exe` を実行します。オプションについては、VDAのインストール用コマンドラインオプション を参照してください。

   StoreFrontをインストールするには: インストールメディアの `x64 > StoreFront` フォルダーで `CitrixStoreFront-x64.exe` を実行します。

   Universal Print Serverをインストールするには: Universal Print Serverのインストール用コマンドラインオプション のガイダンスに従ってください。

   Federated Authentication Serviceをインストールするには: Citrixでは、グラフィカルインターフェイスを使用することをお勧めします。

   Session Recordingをインストールするには: Session Recording のガイダンスに従ってください。

   Workspace Environment Managementをインストールするには： Workspace Environment Managementのガイダンスに従ってください。

   Secure Private Accessをインストールするには： インストールメディアの `x64 > XenDesktop` Setupフォルダーで `XenDesktopSPASetup.exe` を実行します。Secure Private Accessのインストールに関するコマンドラインオプションのガイダンスに従ってください。

コアコンポーネントのインストール用コマンドラインオプション

`XenDesktopServerSetup.exe` コマンドでコアコンポーネントをインストールする場合、以下のパラメーターオプションが有効です。オプションの詳細については、コアコンポーネントのインストールを参照してください。

注:

- コアコンポーネントのインストール用コマンドラインオプションを使用している間は、`/exclude` を使用しないでください。
- `/components` を使用して1つのコンポーネントをアップグレードすると、他のコンポーネントもアップグレードされる場合があります。これは、異なるコンポーネント間の互換性の問題を回避するためです。
- 1つのコンポーネントのみをアップグレードする場合は、そのコンポーネントの個別のインストーラーを使用してください。展開のアップグレード を参照してください。

- **/ceipoptin** *ceipoptin* など.

  Call Home データとカスタマーエクスペリエンス向上プログラム (CEIP) データの収集を有効にします。有効な値は次のとおりです。

  - `DIAGNOSTIC`: Citrix Licensing が Call Home データを収集できるようにするには、この値を選択します。
  - `ANONYMOUS`: Citrix Licensing が未識別の CEIP データ (ユーザーを特定しないデータ) を収集できるようにするには、この値を選択します。
  - `NONE`: Citrix Licensing による CEIP データの収集を無効にするには、この値を選択します。

  Call Home データ収集の詳細については、「Citrix Licensing Call Home」を参照してください。

  CEIP データ収集の詳細については、「Citrix Licensing Customer Experience Improvement Program」を参照してください。

  CEIP データの詳細については、「Citrix Licensing CEIP data elements」を参照してください。

  ライセンスサーバーのライセンスデータの詳細については、「Citrix Licensing Data」を参照してください。

- **/components** *コンポーネント* ...

  インストールまたは削除するコンポーネントのコンマ区切りリスト。有効な値は次のとおりです。

- `CONTROLLER`: コントローラー
- `WEBSTUDIO`: スタジオ
- `DESKTOPDIRECTOR`: ディレクター
- `LICENSESERVER`: Citrix ライセンスサーバー
- `SECUREPRIVATEACCESS`: セキュアプライベートアクセス

VDAのみをインストールし、他のCitrixコンポーネントのインストールを除外するには、/components vda を指定します。

このオプションは、VDAWorkstationCoreSetup_xxxx.exe インストーラーを使用する場合は無効です。このインストーラーでは、Citrix Workspaceアプリやその他のCitrixコンポーネントをインストールできません。

このオプションを省略すると、すべてのコンポーネントがインストールされます（`/remove` オプションも指定されている場合は削除されます）。

（2003より前のリリースでは、有効な値には `STOREFRONT™` が含まれていました。バージョン2003以降では、Use the full-product installer で説明されている専用のStoreFrontインストールコマンドを使用してください）。

- **前提条件のみ**

  選択したコンポーネントの前提条件のみがインストールされます。Citrix製品コンポーネントはインストールされません。

- **/configure_firewall**

  Windows ファイアウォールサービスが実行されている場合、ファイアウォールが有効になっていなくても、インストールされるコンポーネントが使用するWindows ファイアウォールのすべてのポートを開きます。サードパーティのファイアウォールを使用している場合、またはファイアウォールを使用していない場合は、手動でポートを開く必要があります。

- **/ディスエーブルエクスペリエンスメトリクス**

  インストール、アップグレード、または削除中に収集された分析データがCitrixに自動的にアップロードされるのを防ぎます。

- **/help** または **/h**

  コマンドのヘルプを表示します。

- **/ignore_hw_check_failure**

ハードウェアチェックが失敗した場合（たとえば、RAM不足のため）でも、Delivery Controllerのインストールまたはアップグレードを続行できるようにします。詳細については、Hardware check を参照してください。

- **/ignore_site_test_failure**

  Controllerのアップグレード中にのみ有効です。通常、サイトテストの失敗は無視され、アップグレードは続行されます。省略された場合（またはfalseに設定された場合）、サイトテストの失敗があると、アップグレードを実行せずにインストーラーが失敗します。デフォルト = false

  アップグレード中に、サポートされていないSQL Serverバージョンが検出された場合、このオプションは無視されます。詳細については、SQL Server version check を参照してください。

- **/installdir *ディレクトリ***

  コンポーネントがインストールされる既存の空のディレクトリ。デフォルト = `c:\Program Files\Citrix`。

- **/logpath *パス***

  ログファイルの場所。指定されたフォルダーは存在している必要があります。インストーラーは作成しません。デフォルト = `TEMP%\Citrix\XenDesktop Installer`

- **/no_remote_assistance**

  Director のインストール時にのみ有効です。Windows リモートアシスタンスを使用するユーザーシャドウイング機能を無効にします。

- **再起動なし**

  インストール後の再起動を防止します。（ほとんどのコアコンポーネントでは、再起動はデフォルトで有効になっていません。）

- **再開しない**

  デフォルトでは、インストール中にマシンの再起動が必要な場合、再起動が完了するとインストーラーは自動的に再開します。デフォルトを上書きするには、`/noresume`を指定します。これは、メディアを再マウントする必要がある場合や、自動インストール中に情報を取得したい場合に役立ちます。

- **ノースキューエル**

  Controller をインストールするサーバーへの Microsoft SQL Server Express のインストールを防止します。このオプションを省略すると、サイトデータベースとして使用するために SQL Server Express がインストールされます。

このオプションは、ローカルホストキャッシュに使用される SQL Server Express LocalDB のインストールには影響しません。

- **サイレント** または **パッシブ**

  インストール中にユーザーインターフェイスは表示されません。インストールプロセスの唯一の証拠はWindowsタスクマネージャーにあります。このオプションを省略すると、グラフィカルインターフェイスが起動します。

- **/削除**

  `/components`オプションで指定されたコアコンポーネントを削除します。

- **/すべて削除**

  インストールされているすべてのコアコンポーネントを削除します。

- **/エクスペリエンスメトリックを送信**

  インストール、アップグレード、または削除中に収集された分析データをCitrixに自動的に送信します。このオプションを省略した場合（または`/disableexperiencemetrics`が指定された場合）、分析データはローカルで収集されますが、自動的には送信されません。

- **一時ディレクトリ** *directory*

  インストール中に一時ファイルを保持するディレクトリ。デフォルト = `c:\Windows\Temp`。

- **/minutestowaitmsimutexfree minutes**

  MSIMutexがタイムアウトするまでに解放されるのを待つ分数（デフォルトは3分）。有効な範囲は0～60分の整数（例：15、30、45）。

コアコンポーネントのインストール例

次のコマンドは、サーバーにDelivery Controller™、Studio、Citrix Licensing、およびSQL Server Expressをインストールします。コンポーネント通信に必要なファイアウォールポートは自動的に開かれます。

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components controller,webstudio,licenseserver /configure_firewall
```

次のコマンドは、サーバーにCitrix Virtual Apps™ Controller、Studio、およびSQL Server Expressをインストールします。コンポーネント通信に必要なファイアウォールポートは自動的に開かれます。

`\x64\XenDesktop Setup\XenDesktopServerSetup.exe /xenapp /components controller,webstudio /configure_firewall`

次のコマンドは、サーバーにDelivery Controller、Secure Private Access、およびSQL Server Expressをインストールします。コンポーネント通信に必要なファイアウォールポートは自動的に開かれます。

`\x64\XenDesktop Setup\XenDesktopServerSetup.exe /xenapp /components controller,secureprivateaccess /configure_firewall`

Citrix Virtual Apps and Desktopsバージョン2407から2411以降にアップグレードする場合、またはバージョン2411以降の新規インストールを実行する場合は、最初のステップとしてLicense Serverを最新バージョン（バージョン11.2.17ビルド51000）に更新してください。その後、Delivery Controllerをアップグレードします。これを怠ると、コマンドラインによるインストールとアップグレードが失敗します。License ServerおよびDelivery Controller、Studio、Citrix Directorなどのコンポーネントをアップグレードするには、次のコマンドを実行します（マウントされたISOの\x64フォルダー内にいることを前提とします）。

1. 次を実行します。

   ```
   \x64\Licensing\CitrixLicensing.exe /quiet
   ```

   ライセンスバイナリをローカルドライブのいずれかにコピーした場合は、次のコマンドを実行します。

   ```
   \x64\Licensing\CitrixLicensing.exe /quiet /l install.log
   ```

2. 次を実行します。

   ```
   \x64\XenDesktop Setup\XenDesktopServerSetup.exe /components
   "CONTROLLER,WEBSTUDIO,DESKTOPDIRECTOR" /CONFIGURE_FIREWALL
   ```

スタンドアロンVDAインストーラーを使用する

ダウンロードサイトにアクセスするには、Citrixアカウントの資格情報が必要です。インストールを開始する前に、管理者特権を昇格させるか、**管理者として実行**を使用する必要があります。

1. Citrixから適切なパッケージをダウンロードします。

   - マルチセッションOS Virtual Delivery Agent: `VDAServerSetup_xxxx.exe`

- シングルセッションOS Virtual Delivery Agent: `VDAWorkstationSetup_xxxx.exe`
- シングルセッションOS Core Services Virtual Delivery Agent: `VDAWorkstationCoreSetup_xxxx.exe`
- 新しいシングルセッションOSコアサービスVirtual Delivery Agent: `VDASingleSessionCoreSetup_xxxx.exe`

2. まず、パッケージから既存のディレクトリにファイルを抽出し、インストールコマンドを実行するか、単にパッケージを実行します。

   ファイルをインストールする前に抽出するには、絶対パスを指定して`/extract`を使用します（例: `C:\YourExtractFolder\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia`）。ディレクトリが存在している必要があります。存在しない場合、抽出は失敗します。その後、別のコマンドで、この記事に記載されている有効なオプションを使用して、適切なコマンドを実行します。

   - `VDAServerSetup_XXXX.exe` の場合は、`<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe` を実行します
   - `VDAWorkstationCoreSetup_XXXX.exe` の場合は、`<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopRemotePCSetup.exe` を実行します
   - `VDASingleSessionCoreSetup_XXXX.exe` の場合は、`<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopSingleSessionCoreSetup.exe` を実行します
   - `VDAWorkstationSetup_XXXX.exe` の場合は、`<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe` を実行します

   ダウンロードしたパッケージを実行するには、その名前を実行します: `VDAServerSetup.exe`、`VDAWorkstationSetup.exe`、`VDAWorkstationCoreSetup.exe`または`VDASingleSessionCoreSetup`。この記事に記載されている有効なオプションを使用してください。

フル製品インストーラーに慣れている場合：

- スタンドアロンの`VDAServerSetup.exe`または`VDAWorkstationSetup.exe`インストーラーを、名前以外はすべて`XenDesktopVdaSetup.exe`コマンドであるかのように実行します。
- `VDAWorkstationCoreSetup.exe`または`VDASingleSessionCoreSetup.exe`インストーラーは、他のインストーラーで利用可能なオプションのサブセットをサポートしているため、異なります。

VDA をインストールするためのコマンドラインオプション

次のオプションは、次のコマンド（インストーラー）の1つ以上で有効です: `VDAServerSetup_xxxx.exe`、`VDAWorkstationSetup_xxxx.exe`、`VDAWorkstationCoreSetup_xxxx.exe`、および`VDASingleSessionCoreSetup_xxxx.exe`。

オプションの詳細については、「VDA のインストール」を参照してください。

- **/コンポーネント** *コンポーネント*\[,*コンポーネント*\]

  インストールまたは削除するコンポーネントのコンマ区切りリスト。有効な値は次のとおりです。

  - `VDA`: バーチャル デリバリー エージェント
  - `PLUGINS`: Windows 用 Citrix Workspace アプリ
  - `CSA`: Citrix セキュア アクセス クライアント
  - `UPL`: Citrixユーザーパーソナライゼーションレイヤー (WS VDAのみ)
  - `SRAGENT`: セッション レコーディング エージェント
  - `ASSISTANTAPP`: Citrix Virtual Desktop アシスタント
  - `CEAL`: Citrixエラスティックアプリレイヤリング (TS VDAのみ)

2507 LTSR以降、Citrix Device Trust、Citrix uberAgent、およびCitrix Workspace Environment Management™ (WEM) Agentは、デフォルトのVDAインストールに統合されています。これらのコンポーネントはVDAセットアップの一部としてサイレントインストールされ、個別のコンポーネントとして管理されることはなくなりました。

> **注:**
>
> 環境内で既存のスタンドアロン版のCitrix uberAgent®が検出された場合、インストーラーによってインストール、アップグレード、またはアンインストールされることはありません。

> 一般的なコンポーネント選択の例:

- WS VDAインストーラーですべてのサポート対象コンポーネントをインストールするには、`/components VDA,PLUGINS,CSA,UPL,SRAGENT,ASSISTANTAPP`を指定します。これは、WS VDAインストーラーのコンポーネントページで利用可能なすべてのコンポーネントを選択することと同じです。

- TS VDAインストーラーですべてのサポート対象コンポーネントをインストールするには、`/components VDA,PLUGINS,CSA,CEAL,SRAGENT,ASSISTANTAPP`を指定します。これは、TS VDAインストーラーのコンポーネントページで利用可能なすべてのコンポーネントを選択することと同じです。
- `/components`が省略された場合、インストーラーはデフォルトでVDA、SRAGENT、およびASSISTANTAPPをインストールします。インストーラーのユーザーインターフェイスでは、これはVirtual Delivery Agent、Session Recording Agent、およびCitrix Virtual Desktop Assistantを選択することと同じです。
- VDAとCitrix Workspace app for Windowsをインストールするには、/components VDA,PLUGINSを指定します。
- VDAのみをインストールするには、/components VDAを指定します。これにより、Citrix Workspace app for Windowsおよびその他のコンポーネントは除外されます。

このオプションは、VDAWorkstationCoreSetup_xxxx.exeおよびVDASingleSessionCoreSetup_xxxx.exeインストーラーでは無効です。これらのインストーラーは、Citrix Workspace app for Windowsやその他のオプションコンポーネントをサポートしていません。

- **/オンリープレレックス**

  選択したコンポーネントの前提条件のみがインストールされます。Citrix 製品コンポーネントはインストールされません。

- **/controllers** "*コントローラー*\[*コントローラー*\]"

  VDA が通信できるコントローラーのスペース区切りの FQDN を、引用符で囲んで指定します。`/site_guid` オプションと `/controllers` オプションの両方を指定しないでください。

- **/ディスエーブルエクスペリエンスメトリクス**

  インストール、アップグレード、または削除中に収集された分析がCitrixに自動的にアップロードされるのを防ぎます。

- **/enable_hdx_ports**

  Windows ファイアウォールサービスが検出された場合、ファイアウォールが有効になっていなくても、VDAおよび有効な機能（Windows リモートアシスタンスを除く）に必要なポートをWindows ファイアウォールで開きます。別のファイアウォールを使用している場合、またはファイアウォールを使用していない場合は、ファイアウォールを手動で構成する必要があります。ポート情報については、ネットワークポートを参照してください。

HDX アダプティブトランスポートが使用する UDP ポートを開くには、この `/enable_hdx_ports` オプションに加えて、`/enable_hdx_udp_ports` オプションを指定します。

- **/enable_hdx_udp_ports**

  Windows ファイアウォールサービスが検出された場合、ファイアウォールが有効になっていなくても、HDX アダプティブトランスポートが使用する Windows ファイアウォールの UDP ポートを開きます。別のファイアウォールを使用している場合、またはファイアウォールを使用していない場合は、ファイアウォールを手動で構成する必要があります。ポート情報については、「ネットワークポート」を参照してください。

  VDAが使用する追加ポートを開くには、この`/enable_hdx_udp_ports`オプションに加えて、`/enable_hdx_ports`オプションを指定します。

- **/enable_hdx_tls_dtls**

  HDX™ Direct V1用にTCPおよびUDPポート443を開きます。

- **/enable_real_time_transport**

  オーディオパケットにUDPを使用するかどうかを有効または無効にします（オーディオ用のRealTime Audio Transport）。この機能を有効にすると、オーディオパフォーマンスが向上する可能性があります。Windowsファイアウォールサービスが検出されたときにUDPポートを自動的に開く場合は、`/enable_hdx_ports`オプションを含めます。

- **/enable_remote_assistance**

  Directorで使用するために、Windowsリモートアシスタンスのシャドウイング機能を有効にします。このオプションを指定すると、Windowsリモートアシスタンスはファイアウォールで動的ポートを開きます。

- **/enablerestore** または **/enablerestorecleanup**

  （シングルセッションVDAにのみ有効）VDAのインストールまたはアップグレードが失敗した場合に、復元ポイントへの自動復帰を有効にします。

  インストール/アップグレードが正常に完了した場合：

  - `/enablerestorecleanup`は、インストーラーに復元ポイントを削除するよう指示します。
  - `/enablerestore`は、使用されなかった場合でも、インストーラーに復元ポイントを保持するように指示します。

  詳細については、インストールまたはアップグレードの失敗時の復元を参照してください。

- **/ENABLE_SECURE_DEFAULTS**

  より安全な初期設定のために、さまざまな機能のデフォルト設定を有効から無効に変更します。関連する機能は、クライアントドライブリダイレクト、特殊フォルダーリダイレクト、ドラッグアンドドロップ、クライアントTWAINデバイスリダイレクト、クライアントUSBプラグアンドプレイデバイスリダイレクト、クライアントプリンターリダイレクト、クライアントクリップボードリダイレクト、およびクライアントマイクリダイレクトです。

- **/enable_ss_ports**

  Windows ファイアウォールサービスが検出された場合、ファイアウォールが有効になっていなくても、画面共有に必要なポートをWindows ファイアウォールで開きます。別のファイアウォールを使用している場合、またはファイアウォールを使用していない場合は、手動でファイアウォールを構成する必要があります。

- **/SKIPHDXDRIVERCHECK**

  HDX™ドライバーのVDAメタインストーラーへのチェックをスキップします。

- **/exclude** "*コンポーネント*"\[,"*コンポーネント*"\]

  1つ以上のコンマ区切りのオプションコンポーネントのインストールを防止します。各コンポーネントは、ストレート引用符で囲まれています。たとえば、MCSによって管理されていないイメージにVDAをインストールまたはアップグレードする場合、Machine Identity Serviceコンポーネントは必要ありません。有効な値は次のとおりです。

マルチセッションOS	シングルセッションOS	シングルセッションOSコアサービス	新しいシングルセッションOSコアサービス
`Citrix Authentication Identity Assertion VDA Plug-in`	`Citrix Authentication Identity Assertion VDA Plug-in`	`Citrix Authentication Identity Assertion VDA Plug-in`	`Citrix Authentication Identity Assertion VDA Plug-in`
`Citrix Backup and Restore`	`Citrix Backup and Restore`		
`Citrix deviceTRUST®`	`Citrix deviceTRUST`	`Citrix deviceTRUST`	`Citrix deviceTRUST`
`Citrix Secure Access Client`	`Citrix Secure Access Client`		

マルチセッションOS	シングルセッションOS	シングルセッションOSコアサービス	新しいシングルセッションOSコアサービス
Citrix Workspace Environment Management™ Agent	Citrix Workspace Environment Management Agent		Citrix Workspace Environment Management Agent
Citrix Browser Content Redirection	Citrix Browser Content Redirection	Citrix Browser Content Redirection	Citrix Browser Content Redirection
Citrix MCS IODriver	Citrix MCS IODriver		
Citrix Personalization for App-V - VDA	Citrix Personalization for App-V - VDA		
Citrix Profile Management	Citrix Profile Management		Citrix Profile Management
Citrix Profile Management WMI Plug-in	Citrix Profile Management WMI Plug-in		Citrix Profile Management WMI Plug-in
Citrix Rendezvous V2	Citrix Rendezvous V2	Citrix Rendezvous V2	Citrix Rendezvous V2
Citrix Telemetry Service	Citrix Telemetry Service	Citrix Telemetry Service	Citrix Telemetry Service
Citrix Universal Print Client	Citrix Universal Print Client	Citrix Universal™ Print Client	Citrix Universal Print Client
Citrix VDA Upgrade Agent	Citrix VDA Upgrade Agent		Citrix VDA Upgrade Agent
CSE Component	CSE Component	CSE Component	CSE Component

マルチセッションOS	シングルセッションOS	シングルセッションOSコアサービス	新しいシングルセッションOSコアサービス
Director VDA Plug-in	Director VDA Plug-in	Director VDA Plug-in	Director VDA Plug-in
Machine Identity Service	Machine Identity Service		
Machine Management Provider	Machine Management Provider	Machine Management Provider	Machine Management Provider
Elastic App Layering	User Personalization Layer		
VDA Monitor Plug-in	VDA Monitor Plug-in	VDA Monitor Plug-in	VDA Monitor Plug-in
VDA WMI Proxy Plug-in	VDA WMI Proxy Plug-in	VDA WMI Proxy Plug-in	VDA WMI Proxy Plug-in
Citrix App Protection Component	Citrix App Protection Component	Citrix App Protection Component	Citrix App Protection Component
Citrix HyperV Filter Driver	Citrix HyperV Filter Driver	Citrix Web Socket Vda Registration Tool	Citrix Web Socket Vda Registration Tool
App Packages Delivery Component	App Packages Delivery Component	App Packages Delivery Component	App Packages Delivery Component
Session Recording Agent	Session Recording Agent		
Citrix Virtual Desktop Assistant	Citrix Virtual Desktop Assistant		

Citrix Profile Managementをインストールから除外する（`/exclude "Citrix Profile Management"`）と、Citrix DirectorでのVDAの監視とトラブルシューティングに影響します。**ユーザーの詳細**ページと**エンドポイント**ページでは、パーソナライゼーションパネルとログオン期間パネルが機能しません。**ダッシュボード**ページと**トレンド**ページでは、平均ログオン期間パネルはProfile Managementがインストールされているマシンのみのデータを表示します。

サードパーティのユーザープロファイル管理ソリューションを使用している場合でも、Citrixは Citrix Profile Management Serviceをインストールして実行することを推奨します。Citrix Profile Management Serviceを有効にする必要はありません。

Citrix Personalization for App-V – VDA は App Packages Delivery Component に名称変更され、また Citrix Assistant App は Citrix Virtual Desktop Assistant に名称変更されました。

`/components` を使用してインストールできるコンポーネントは、そのコンポーネントを省略することで除外することもできます。たとえば、Citrix Secure Access Client、Session Recording Agent、および Citrix Virtual Desktop Assistant を除外するには、`/components VDA` を指定します。`/components` を指定しない場合は、`/exclude` を使用してこれらのコンポーネントを除外します。

同じコンポーネント名で`/exclude`と`/includeadditional`の両方を指定した場合、そのコンポーネントはインストールされません。

- **/h** または **/help**

  コマンドのヘルプを表示します。

- **/includeadditional** "*コンポーネント*"\[,"*コンポーネント*"\]

  コンマで区切られた1つ以上のオプションコンポーネントのインストールを含めます。各コンポーネントはストレート引用符で囲まれています。このオプションは、リモートPCアクセス展開を作成していて、デフォルトで含まれていない他のコンポーネントをインストールしたい場合に役立ちます。有効な値は次のとおりです。

マルチセッションOS	シングルセッションOS
`Citrix Backup and Restore`	`Citrix Backup and Restore`
`Citrix MCS IODriver`	`Citrix MCS IODriver`
`App Packages Delivery Component`	`App Packages Delivery Component`
`Citrix Profile Management`	`Citrix Profile Management`

マルチセッションOS	シングルセッションOS
`Citrix Profile Management WMI Plug-in`	`Citrix Profile Management WMI Plug-in`
`Citrix Rendezvous V2`	`Citrix Rendezvous V2`
`Citrix VDA Upgrade Agent`	`Citrix VDA Upgrade Agent`
`Citrix Web Socket Vda Registration Tool`	`Citrix Web Socket Vda Registration Tool`
`VDA Token Enrollment`	`VDA Token Enrollment`

同じコンポーネント名で`/exclude`と`/includeadditional`の両方を指定した場合、そのコンポーネントはインストールされません。

- **/installdir** *ディレクトリ*

  コンポーネントがインストールされる既存の空のディレクトリ。デフォルト = `c:\Program Files\Citrix`。

- **/install_mcsio_driver**

  使用しないでください。代わりに`/includeadditional "Citrix MCS IODriver"`または`/exclude "Citrix MCS IODriver"`を使用してください。

- **/logpath** *パス*

  ログファイルの場所。指定されたフォルダーは存在している必要があります。インストーラーは作成しません。デフォルト = 「`%TEMP%\Citrix\XenDesktop Installer`」

  このオプションはグラフィカルインターフェイスでは利用できません。

- **/マスターイメージ**

  VMにVDAをインストールする場合にのみ有効です。VDAを他のマシンを作成するために使用するイメージとして設定します。このオプションは`/mastermcsimage`と同等です。

  このオプションは、`VDAWorkstationCoreSetup_xxxx.exe`インストーラーを使用している場合は無効です。

- **/マスターMCSイメージ**

このマシンがMachine Creation Servicesでイメージとして使用されることを指定します。このオプションは`/masterimage`と同等です。

- **/マスターPVSイメージ**

  このマシンが、Citrix Provisioning™ またはサードパーティのプロビジョニングツール (Microsoft System Center Configuration Manager など) を使用して、VM をプロビジョニングするためのイメージとして使用されることを指定します。

- **/websockettoken** *WebSocketトークン*

  Web Socket VDAを作成します。WebSocketTokenは、必要なトークン用です。

- **/websockettokenfile** *WebSockトークンを含むファイル*

  Web Socket VDAを作成します。*FileContainingWebSockToken* は、必要なトークンを含むファイル用です。

- **ウェブソケットトークン標準入力** *<ウェブソケットトークン>*

  Web Socket VDAを作成します。*<WebSocketToken* は、STDINによって渡される必要なトークン用です。

- **/no_mediafoundation_ack**

  Microsoft Media Foundationがインストールされていないことを確認し、いくつかのHDXマルチメディア機能がインストールされず、動作しないことを承認します。このオプションが省略され、Media Foundationがインストールされていない場合、前提条件が満たされていないため、VDAのインストールは終了します。ほとんどのサポートされているWindowsエディションには、Nエディションを除いて、Media Foundationがすでにインストールされています。Windowsの機能 > メディア機能 を *手動* で 有効にした場合、Citrix Meta Installerが探すレジストリキーに値が設定されていない可能性があります。インストールプロセスを開始する前に、`SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\Windows-Features\WindowsMediaVersion` レジストリキーをチェックして、値が存在し、空ではないことを確認してください。

- **デスクトップエクスペリエンスなし**

  拡張デスクトップエクスペリエンス機能は利用できなくなりました。このオプション（およびポリシー設定）は、指定されても無視されます。

  マルチセッションOS用VDAをインストールする場合にのみ有効です。拡張デスクトップエクスペリエンス機能の有効化を防止します。この機能は、拡張デスクトップエクスペリエンスCitrixポリシー設定でも制御されます。

- **再起動なし**

  インストール後の再起動を防止します。VDAは再起動するまで使用できません。

- **再開しない**

  デフォルトでは、インストール中にマシンの再起動が必要な場合、再起動が完了するとインストーラーは自動的に再開します。デフォルトを上書きするには、`/noresume`を指定します。これは、メディアを再マウントする必要がある場合や、自動インストール中に情報を取得したい場合に役立ちます。

- **物理マシン**

  RemotePCインストールの場合、この引数を`/remotepc`とともに使用してください。そうしないと、特定のユーザーシナリオでVDAが期待どおりに動作しない可能性があります。

- **ポート番号** *port*

  `/reconfig`オプションが指定されている場合にのみ有効です。VDAとController間の通信を有効にするポート番号。以前に構成されたポートは、ポート80でない限り無効になります。

- **/proxyconfig** "*アドレスまたはPACファイルのパス*"

  環境内でGateway Serviceなどのサービスとともに Rendezvous V2プロトコルを使用する予定があり、アウトバウンド接続のためにネットワークに非透過プロキシがある場合は、ここでプロキシを指定します。HTTPプロキシのみがサポートされています。Rendezvousプロトコルで使用するプロキシのアドレスまたはPACファイルパス。このコマンドラインは、/includeadditional "Citrix Rendezvous V2"が使用されたかのように、Citrix Rendezvous V2を自動的にインストールします。機能の詳細については、Rendezvous protocolを参照してください。

  - プロキシアドレスの形式: `http://<url-or-ip>:<port>`
  - PACファイルの形式: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

- **サイレント** または **パッシブ**

  インストール中にユーザーインターフェイスは表示されません。インストールと構成プロセスの唯一の証拠は、Windowsタスクマネージャーにあります。このオプションを省略すると、グラフィカルインターフェイスが起動します。

- **/再構成**

  `/portnumber`、`/controllers`、または`/enable_hdx_ports`オプションと組み合わせて使用すると、以前に構成されたVDA設定をカスタマイズします。このオプションを`/quiet`オ

プションも指定せずに指定すると、VDAをカスタマイズするためのグラフィカルインターフェイスが起動します。

- **/リモートPC**

  リモートPCアクセス展開（シングルセッションOS）またはブローカー接続（マルチセッションOS）の場合にのみ有効です。追加コンポーネントのインストールを除外します（`/exclude` および `/includeadditional` オプションのコンポーネントリストを参照）。

  このオプションは、`VDAWorkstationCoreSetup.exe` インストーラーを使用する場合は無効です。そのインストーラーは、これらのコンポーネントのインストールを自動的に除外します。

  `/remotepc` は `/servervdi` オプションと互換性がありません。

- **/削除**

  `/components` オプションで指定されたコンポーネントを削除します。

- **/remove_appdisk_ack**

  AppDisks™ VDAプラグインがインストールされている場合、VDAインストーラーがそれをアンインストールすることを承認します。

- **/remove_pvd_ack**

  Personal vDiskがインストールされている場合、VDAインストーラーがそれをアンインストールすることを承認します。

- **/すべて削除**

  VDAを削除します。Citrix Workspaceアプリ（インストールされている場合）は削除しません。

- **/REMOVEALLWITHCWA**

  VDA とともに CWA を削除します。

- **/エクスペリエンスメトリックを送信**

  インストール、アップグレード、または削除中に収集された分析データをCitrixに自動的に送信します。このオプションが省略された場合（または `/disableexperiencemetrics` オプションが指定された場合）、分析データはローカルで収集されますが、自動的には送信されません。

- **サーバーVDI**

サポートされているWindowsマルチセッションマシンにシングルセッションOS用VDAをインストールします。Windowsマルチセッションマシンにマルチセッションos用VDAをインストールする場合は、このオプションを省略してください。

このオプションを使用する前に、サーバーVDI を参照してください。

このオプションは、フルプロダクトVDAインストーラーでのみ使用してください。

- **サイトGUID** *guid*

  サイトのActive Directory組織単位（OU）のグローバル一意識別子。これは、検出にActive Directoryを使用している場合に、仮想デスクトップをサイトに関連付けます（自動更新が推奨されるデフォルトの検出方法です）。サイトGUIDは、Studioに表示されるサイトプロパティです。`/site_guid`と`/controllers`の両方のオプションを指定しないでください。

- **一時ディレクトリ** *directory*

  インストール中に一時ファイルを保持するディレクトリ。デフォルト = `c:\Windows\Temp`。

  このオプションはグラフィカルインターフェイスでは利用できません。

- **仮想マシン**

  VDAをVMにインストールする場合にのみ有効です。BIOS情報がVMに渡されることで物理マシンとして表示される、インストーラーによる物理マシンの検出を上書きします。

  このオプションはグラフィカルインターフェイスでは利用できません。

- **/minutestowaitmsimutexfree minutes**

  MSIMutex が解放されるまで待機する分数（タイムアウトするまで）。（デフォルトは3分）。有効な範囲は0〜60分の整数です（例: 15、30、45）。

VDAのインストール例

フルプロダクトインストーラーでVDAをインストールする:

次のコマンドは、シングルセッションOSおよびCitrix Workspaceアプリ用のVDAを、VMのデフォルトの場所にインストールします。このVDAはイメージとして使用され、MCSを使用してVMをプロビジョニングします。VDAは、`mydomain`ドメイン内の`Contr-Main`という名前のサーバー上のControllerに最初に登録されます。VDAはユーザーパーソナライゼーションレイヤーとWindowsリモートアシスタンスを使用します。

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda,plugins /
controllers "Contr-Main.mydomain.local" /enable_hdx_ports /includeadditional
"user personalization layer" /mastermcsimage /enable_remote_assistance
```

VDAWorkstationCoreSetupスタンドアロンインストーラーでシングルセッションOS VDAをインストールする:

次のコマンドは、リモートPCアクセスまたはVDI展開で使用するために、シングルセッションOSにコアサービスVDAをインストールします。Citrix Workspaceアプリおよびその他の非コアサービスはインストールされません。Controllerのアドレスが指定され、Windowsファイアウォールサービス内のポートは自動的に開かれます。管理者が再起動を処理します。

```
VDAWorkstationCoreSetup .exe /quiet /controllers "Contr-East.domain.com" /
enable_hdx_ports /noreboot
```

VDAをカスタマイズする

VDAをインストールした後、いくつかの設定をカスタマイズできます。製品メディアの `\x64\XenDesktop Setup` ディレクトリから、VDAのインストール用コマンドラインオプションで説明されている以下のオプションを1つ以上使用して、`XenDesktopVdaSetup.exe` を実行します。

- `/reconfigure` (VDAをカスタマイズする際に必須)
- `/h` または `/help`
- `/quiet`
- `/noreboot`
- `/controllers`
- `/portnumber port`
- `/enable_hdx_ports`

VDAのトラブルシューティング

- デリバリーグループのStudio表示で、**詳細**ペインの**インストール済みVDAバージョン**エントリが、マシンにインストールされているバージョンと異なる場合があります。マシンのWindowsのプログラムと機能の表示には、実際のVDAバージョンが表示されます。
- VDAがインストールされても、Delivery Controllerに登録されるまでは、ユーザーにアプリやデスクトップを配信できません。

VDAの登録方法と登録の問題のトラブルシューティングについては、VDAの登録を参照してください。

Universal Print Serverをインストールするためのコマンドラインオプション

次のオプションは、`XenDesktopPrintServerSetup.exe`コマンドで有効です。

- **/enable_upsserver_port**

このオプションが指定されていない場合、インストーラーはグラフィカルインターフェイスから**ファイアウォール**ページを表示します。インストーラーにWindowsファイアウォール規則を自動的に追加させるには**自動**を選択し、管理者が手動でファイアウォールを構成する場合は**手動**を選択します。

印刷サーバーにソフトウェアをインストールした後、Citrix Universal Print Server (UPS) のガイダンスを使用して Universal Print Server を構成します。

Secure Private Accessをインストールするためのコマンドラインオプション

以下のオプションは、両方で有効です。

1. CVADインストーラー: `XenDesktopSPASetup.exe`
2. SPAオンプレミスインストーラー: `SecurePrivateAccessSetup_XXXX.exe`

- **/enable_spa_ports**

  Windowsファイアウォールサービスが検出された場合、ファイアウォールが有効になっていなくても、Secure Private Accessに必要なWindowsファイアウォールのポートを開きます。別のファイアウォールを使用している場合、またはファイアウォールを使用していない場合は、ファイアウォールを手動で構成する必要があります。ポート情報については、「ネットワークポート」を参照してください。

- **ノーSQL**

  Secure Private Accessをインストールするサーバーへの Microsoft SQL Server Expressのインストールを防止します。このオプションを省略すると、サイトデータベースとして使用するためにSQL Server Expressがインストールされます。

- **/help または /h または /?**

  コマンドのヘルプを表示します

- **再起動なし**

インストール後の再起動を防止します。再起動するまでSecure Private Accessは使用できません。

- **/quiet または /passive**

  インストール中にユーザーインターフェイスは表示されません。インストールと構成プロセスの唯一の証拠は、Windowsタスクマネージャーにあります。このオプションを省略すると、グラフィカルインターフェイスが起動します。

- **/削除**

  Secure Private Accessを削除します。

オプションの詳細については、Secure Private Accessインストーラーを参照してください。

詳細情報

Citrixがコンポーネントのインストール結果を報告する方法については、(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/install-prepare.html#citrix-installation-return-codes)を参照してください。

VDAのインストール

> **重要:**
>
> - アップグレード中で、現在のバージョンにPersonal vDiskまたはAppDisksソフトウェアがインストールされている場合は、PvD、AppDisks、およびサポートされていないホストの削除を参照してください。
> - Citrix®によって配布されるバイナリは署名されています。署名されたバイナリは、Citrixが生成した証明書または信頼できるサードパーティの証明書によって検証されていることを示します。

> Windowsマシン用のVDAには、マルチセッションOS用VDAとシングルセッションOS用VDAの2種類があります。(Linuxマシン用VDAについては、Linux Virtual Delivery Agentドキュメントを参照してください。)

インストールを開始する前に、インストールの準備を確認し、すべての準備タスクを完了してください。

VDAをインストールする前に、コアコンポーネントをインストールします。VDAをインストールする前にサイトを作成することもできます。

この記事では、VDAをインストールする際のインストールウィザードのシーケンスについて説明します。コマンドラインでの同等の操作も提供されています。詳細については、コマンドラインを使用したインストールを参照してください。

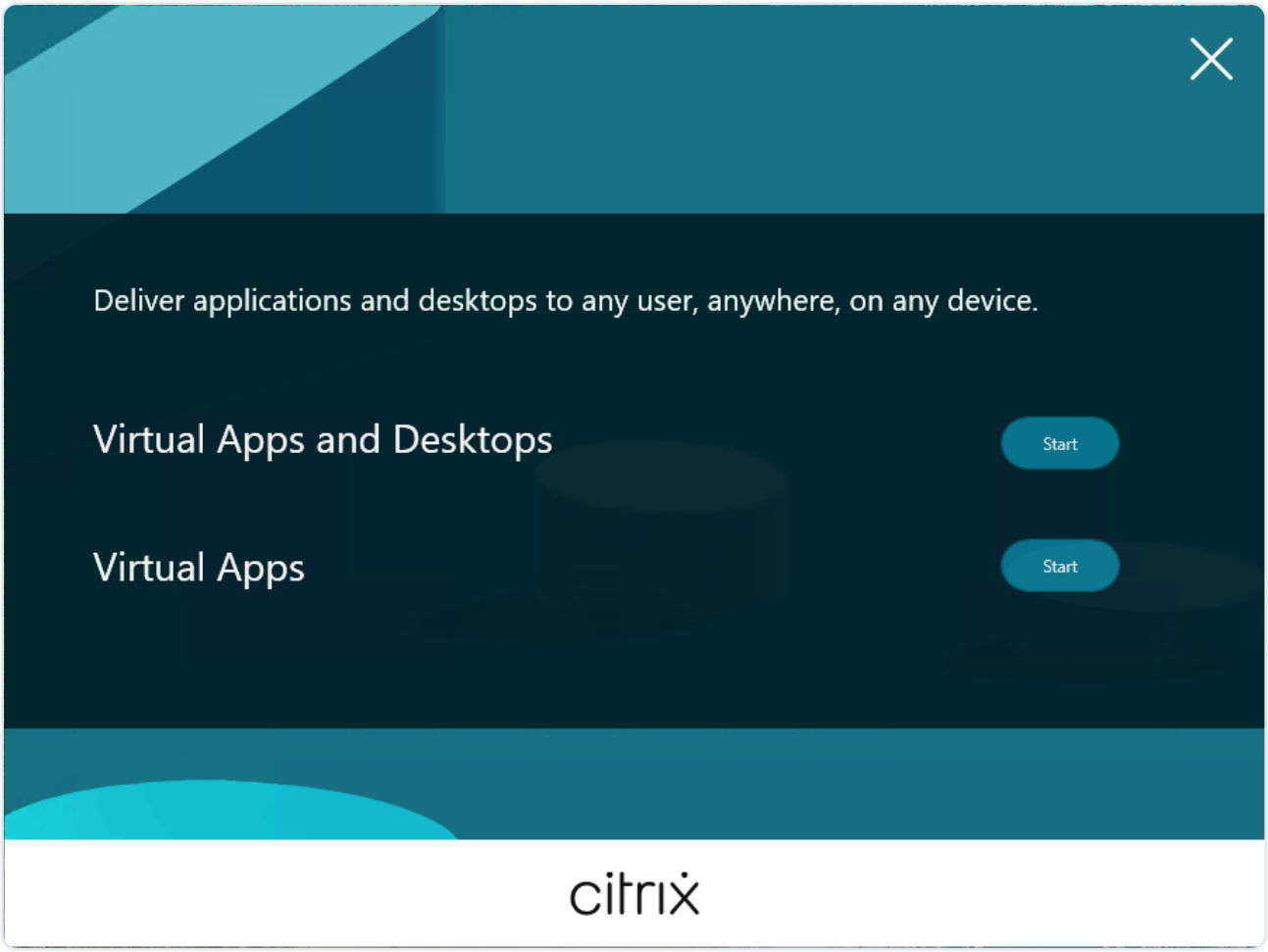
ステップ1. 製品ソフトウェアをダウンロードしてウィザードを起動する

フル製品インストーラーを使用している場合:

1. 製品ISOをまだダウンロードしていない場合:
    - Citrixアカウントの資格情報を使用して、Citrix Virtual Apps and Desktops™ダウンロードページにアクセスします。製品ISOファイルをダウンロードします。
    - ファイルを解凍します。必要に応じて、ISOファイルをDVDに書き込みます。
2. VDAをインストールするイメージまたはマシンでローカル管理者アカウントを使用します。DVDをドライブに挿入するか、ISOファイルをマウントします。インストーラーが自動的に起動しない場合は、マウントされたドライブ上の**AutoSelect**アプリケーションをダブルクリックします。

    インストールウィザードが起動します。

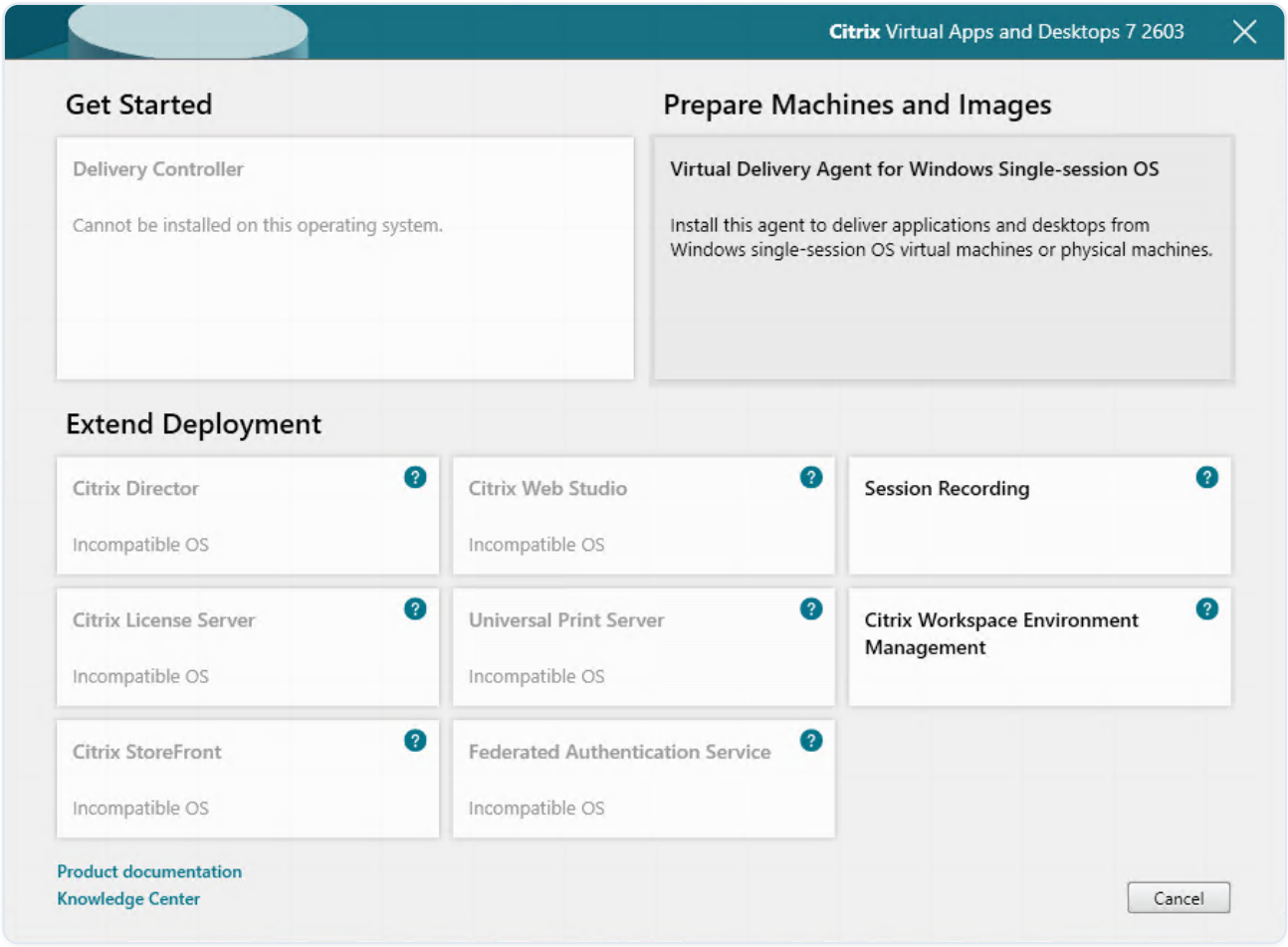
ステップ2. インストールする製品を選択する



インストールする製品（Citrix Virtual AppsまたはCitrix Virtual Desktops）の横にある**開始**をクリックします。（マシンにCitrix Virtual AppsまたはCitrix Virtual Desktopsコンポーネントがすでにインストールされている場合、このページは表示されません。）

コマンドラインオプション: Citrix Virtual Appsをインストールするための`/xenapp`。このオプションが省略された場合、Citrix Virtual Desktopsがインストールされます。

ステップ3. VDAを選択する



Virtual Delivery Agentエントリを選択します。インストーラーは、シングルセッションOSまたはマルチセッションOSのどちらで実行されているかを認識しているため、適切なVDAタイプのみを提供します。

例えば、Windows Server 2019マシンでインストーラーを実行すると、マルチセッションOS用VDAオプションが利用可能です。シングルセッションOS用VDAオプションは提供されません。

このCitrix Virtual Apps and Desktops™バージョンでサポートされていないOSにWindows VDAをインストール（またはアップグレード）しようとすると、オプションに関する情報に誘導するメッセージが表示されます。

スタンドアロンパッケージを使用している場合:

1. Citrixアカウントの資格情報を使用して、Citrix Virtual Apps and Desktops™ダウンロードページにアクセスします。適切なパッケージをダウンロードします。
    - `VDAServerSetup_2603.exe`: マルチセッションOS VDA バージョン
    - `VDAWorkstationSetup_2603.exe`: シングルセッションOS VDA バージョン

- `VDAWorkstationCoreSetup_2603.exe`: シングルセッションOSコアサービスVDA バージョン
- `VDASingleSessionCoreSetup_2603.exe`: 新しいシングルセッションOSコアサービスVDAバージョン

2. パッケージを右クリックし、「**管理者として実行**」を選択します。

   インストールウィザードが起動します。

ステップ4. VDAの使用方法を指定する

VDAインストーラーの環境ページ(/en-us/citrix-virtual-apps-desktops/current-release/media/vda-ss-environment.png)

環境ページで、VDAをどのように使用するかを指定します。このマシンをイメージとして使用して、さらに多くのマシンをプロビジョニングするかどうかを示します。

選択したオプションは、Citrix Provisioning™ツールが自動的にインストールされるかどうか（もしあれば）、およびVDAインストーラーの追加コンポーネントページのデフォルト値に影響します。

VDAをインストールすると、複数のMSI（プロビジョニング用およびその他）が自動的にインストールされます。これらのインストールを防止する唯一の方法は、コマンドラインインストールで`/exclude`オプションを使用することです。

次のいずれかを選択してください。

- **マスターMCSイメージを作成する:** Machine Creation Services™を使用してVMをプロビジョニングする予定がある場合は、このオプションを選択してVDAをVMイメージにインストールします。このオプションは、Machine Identity Serviceをインストールします。これがデフォルトのオプションです。

  コマンドラインオプション: `/mastermcsimage` または `/masterimage`

> **重要:**

> インストールメディアまたはISOイメージはローカルにマウントする必要があります。ソフトウェアのインストールを目的として、ネットワークドライブからISOイメージをマウントすることはサポートされていません。

- **Citrix Provisioningまたはサードパーティのプロビジョニングツールを使用してマスターイメージを作成する:** Citrix Provisioningまたはサードパーティのプロビジョニングツール（Microsoft System Center Configuration Managerなど）を使用してVMをプロビジョニングする予定がある場合は、このオプションを選択してVDAをVMイメージにインストールします。

  コマンドラインオプション: `/masterpvsimage`

- （マルチセッションOSマシンでのみ表示）**サーバーへの仲介接続を有効にする:** 他のマシンをプロビジョニングするためのイメージとして使用されない物理マシンまたは仮想マシンにVDAをインストールするには、このオプションを選択します。

  コマンドラインオプション: `/remotepc`

- （シングルセッションOSマシンでのみ表示）**Remote PC Accessを有効にする:** Remote PC Accessで使用する物理マシンにVDAをインストールするには、このオプションを選択します。

  コマンドラインオプション: `/remotepc`

Nextをクリックします。

このページは表示されません。

- VDAをアップグレードする場合
- `VDAWorkstationCoreSetup_xxxx.exe`、`VDASingleSessionCoreSetup_xxxx.exe`、`VDAServerSetup_xxxx.exe`、または`VDAWorkstationSetup_xxxx.exe`インストーラーを使用している場合

ステップ5. インストールするコンポーネントとインストール場所を選択します

VDAインストーラーのコンポーネントページ(/en-us/citrix-virtual-apps-desktops/current-release/media/vda-ss-components.png)

> **注:**

> バージョン2603以降、以前は「Optional Software」ページに表示されていたコンポーネントが「Components」ページに移動されました。

> **コンポーネント**ページで:

- **場所:** デフォルトでは、VDAは`C:\Program Files\Citrix`にインストールされます。このデフォルトはほとんどの展開で問題ありません。別の場所を指定する場合、その場所にはネットワークサービスに対して`execute`権限が必要です。
- **コンポーネント:** デフォルトでは、Session Recording AgentとCitrix Virtual Desktop AssistantはVDAとともにインストールされます。`VDAWorkstationCoreSetup.exe`インストーラーまたは`VDASingleSessionCoreSetup.exe`インストーラーを使用している場合、VDAのみがインストールされ、他のコンポーネントは表示されません。

Nextをクリックします。

コマンドラインオプション: 指定されたディレクトリにVirtual Delivery Agent、Citrix Workspace Environment Management™エージェント、Citrix deviceTRUST、Citrix uberAgent、Citrix Secure Access Client、およびCitrix Workspaceアプリをインストールするには`/installdir "C:\Program Files\VDA" /components "VDA","CSA","PLUGINS"`を使用します。

注:

以下のシナリオで、VDAのインストール、アップグレード、またはアンインストール中に、Citrix Workspaceアプリおよびその他のコンポーネントをインストール、アップグレード、またはアンインストールすることを選択できます。

- VDAのインストールおよび2603へのアップグレード中に、コンポーネントとCWAプラグインを含めるか除外するかを選択できます。
  - デフォルトでは、**Citrix Workspace app (CWA)**、**Citrix Secure Access Client (CSA)**、**Citrix User Personalization Layer (UPL) (WS VDAのみ)**、および**Citrix Elastic App Layering (CEAL) (TS VDAのみ)**はインストール対象として選択されていませんが、必要に応じてインストール時に選択できます。 **Session Recording Agent (SRAGENT)**および**Citrix Virtual Desktop Assistant (ASSISTANTAPP) (現在、TS VDAとWS VDAの両方で利用可能)**はデフォルトでインストール対象として選択されていますが、必要に応じてインストール時に選択を解除できます。
  - **Citrix Device Trust**、**Citrix uberAgent**、および**Citrix Workspace Environment Management™ agent**はVDAに統合され、常にインストールされます。これらのインストールを防止するには、管理者はサポートされている`/exclude`コマンドラインオプションを使用する必要があります。**uberAgent**もデフォルトでインストールさ

れ、VDA 2511以降および2603では、GUIまたはコマンドライン（CLI）のいずれを使用してもインストールから除外することはできません。

- デフォルトでは、**Citrix Workspace Environment Management™ agent**は**Basic deployment**で実行されます。これは、WEMインフラストラクチャに接続しない機能が制限された単一マシンモードです。エージェントをCitrix CloudのWEMサービスまたはオンプレミス展開に接続して完全なWEM機能を有効にするには、グループポリシーを通じて設定を構成します。詳細については、このWEM記事を参照してください。
- **Citrix User Personalization Layer:** ユーザーパーソナライゼーションレイヤーのMSIをインストールします。詳しくは、「ユーザーパーソナライゼーションレイヤー」を参照してください。
- **コマンドラインの変更**

  `/components VDA,CSA`: このコマンドは、**VDA**と**CSA**（選択済み）をインストールし、さらに**Citrix Device Trust**、**Citrix uberAgent**、および**Citrix Workspace Environment Management agent**（デフォルトで統合済み）もインストールします。

  `/components VDA`: このコマンドは**VDA**をインストールし、**Citrix Device Trust**、**Citrix uberAgent**、および**Citrix Workspace Environment Management agent**もVDA自体に統合されているためインストールします。Citrix Device Trust、Citrix uberAgent、およびCitrix Workspace Environment Management agentを`/components`オプションとともに引数として指定した場合、VDAメタインストーラーは、これらの引数が`/components`オプションから削除されたことを示す通知をログに記録します。その後、VDAメタインストーラーはVDAのインストールまたはアップグレードに進みます。

  `/components`: このコマンドは無効なコマンドであり、常にVDAを含める必要があります。必要に応じて、追加コンポーネントをインストールに追加できます。

  デフォルトで統合されているコンポーネントに`/exclude`コマンドを使用する: `/exclude`オプションは常に優先されます。これは、デフォルトで統合されているコンポーネントのインストールを防止するために使用できます。例: `/exclude "Citrix Device Trust","Citrix Universal Print Client"`。このコマンドは、Citrix Workspace Environment Management agentとともにVDAをインストールしますが、Citrix Device TrustとCitrix Universal Print Clientはインストールしません。

- VDAのアップグレード中に、Citrix Workspace app、Citrix Secure Access Client、Citrix User Personalization Layer（WS VDAのみ）、Session Recording Agent、Citrix Virtual Desktop Assistant、およびElastic App Layering（TS VDAのみ）がVDAにまだインストールされていない場合、それらをインストールすることを選択できます。
- VDAのアップグレード中に、User Personalization LayerまたはElastic App Layeringがすでにインストールされている場合、それらは**Required**として選択され、コンポーネントがアップグレードされます。
- VDAのアップグレード中に、Citrix Workspace appおよびその他のインストールされているプラグインのバージョンをアップグレードできる場合、それらをアップグレードするオプションが表示されます。
- VDAのアンインストール中に、Citrix Workspace app（CWA）およびその他のインストールされているコンポーネントをアンインストールするかどうかを選択できます。デフォルトでは、CWAを除くすべてのコンポーネントが自動的にアンインストールされます。CWAは異なる扱いを受け、明示的に選択されない限り削除されません。

ステップ6. 追加コンポーネントをインストールします

VDAインストーラーの追加コンポーネントページ(/en-us/citrix-virtual-apps-desktops/current-release/media/vda-ss-addtnl-components.png)

追加コンポーネントページには、VDAとともに他の機能やテクノロジーのインストールを有効または無効にするためのチェックボックスが含まれています。コマンドラインインストールでは、`/exclude`または`/includeadditional`オプションを使用して、利用可能なコンポーネントを明示的に除外または含めることができます:

- **/includeadditional** "*コンポーネント*"\[,"*コンポーネント*"\] ...
- **/除外** "*コンポーネント*"\[,"*コンポーネント*"\] ...

次の表は、このページの項目のデフォルト設定を示しています。デフォルト設定は、「**環境**」ページで選択したオプションによって異なります。

追加コンポーネントページ	環境ページ：「MCS を使用したマスターイメージ」または「CITRIX PROVISIONING を使用したマスターイメージ」が選択されている場合	環境ページ：「サーバーへの仲介接続を有効にする」（マルチセッションOSの場合）または「リモートPCアクセス」（シングルセッションOSの場合）が選択されている場合
アプリパッケージ配信コンポーネント	選択されていません	選択されていません
Citrix VDA アップグレードエージェント	選択されていません	選択されていません
Citrix バックアップおよび復元	選択されていません	選択されていません
シトリックス MCS IOドライバー	選択されていません	選択されていません
シトリックス ランデブー V2	選択されていません	選択されていません

このページは、次の場合には表示されません。

- `VDAWorkstationCoreSetup.exe` インストーラーまたは `VDASingleSessionCoreSetup.exe` を使用している場合。また、追加コンポーネントのコマンドラインオプションはそのインストーラーでは無効です。
- VDA をアップグレードしていて、すべての追加コンポーネントがすでにインストールされている場合。一部の追加コンポーネントがすでにインストールされている場合、そのページにはインストールされていないコンポーネントのみが表示されます。

次のチェックボックスをオンまたはオフにします。（コンポーネントはインストーラーで異なる順序で表示される場合があります。）

- **App Packages Delivery Component:** Microsoft App-Vパッケージのアプリケーションを使用する場合は、このコンポーネントをインストールします。詳しくは、「App-Vアプリケーションの展開と配信」を参照してください。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "App Packages Delivery Component"`、コンポーネントのインストールを防止するには `/exclude "App Packages Delivery Component"`。

- **Citrix Profile Management:** このコンポーネントは、ユーザープロファイル内のユーザーパーソナライゼーション設定を管理します。詳細については、「Profile Management」を参照してください。

  Citrix Profile Managementをインストールから除外すると、Citrix DirectorによるVDAの監視とトラブルシューティングに影響します。**ユーザーの詳細**ページと**エンドポイント**ページでは、**パーソナライゼーション**パネルと**ログオン期間**パネルが機能しません。**ダッシュボード**ページと**傾向**ページでは、**平均ログオン期間**パネルはProfile Managementがインストールされているマシンのみのデータを表示します。

  サードパーティのユーザープロファイル管理ソリューションを使用している場合でも、Citrixは Citrix Profile Management Serviceをインストールして実行することをお勧めします。Citrix Profile Management Serviceを有効にする必要はありません。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Profile Management"`、コンポーネントのインストールを防止するには `/exclude "Citrix Profile Management"`。

- **Citrix Profile Management WMIプラグイン:** このプラグインは、WMI（Windows Management Instrumentation）オブジェクト（プロファイルプロバイダー、プロファイルタイプ、サイズ、ディスク使用量など）でProfile Managementのランタイム情報を提供します。WMIオブジェクトは、Directorにセッション情報を提供します。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Profile Management WMI Plug-in"`、コンポーネントのインストールを防止するには `/exclude "Citrix Profile Management WMI Plug-in"`。

注:

2507 LTSR以降、**Citrix Profile Management**と**Citrix Profile Management WMI Plug-in**はVDAの一部となり、**マスターイメージ/MCS/PVS**のユースケースでは自動的にインストールされます。これらのコンポーネントは、**Remote PC**のユースケースでは**デフォルトではインストールされません**。すべての場合において、インストール済みのコンポーネントは自動的にアップグレードされます。コマンドラインの動作は以前のリリースから変更されていません。

- **VDAアップグレードエージェント:** Citrix DaaS（旧Citrix Virtual Apps and Desktopsサービス）の展開にのみ適用されます。VDAがVDAアップグレード機能に参加できるようにします。この機能を使用して、管理コンソールからカタログのVDAを即座に、またはスケジュールされた時

間にアップグレードできます。このエージェントがインストールされていない場合、マシン上でVDAインストーラーを実行することでVDAをアップグレードできます。

コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix VDA Upgrade Agent"`、コンポーネントのインストールを防止するには `/exclude "Citrix VDA Upgrade Agent"`。

- **ストレージ最適化のためのMCSIOライトキャッシュ:** Citrix MCS I/Oドライバーをインストールします。詳細については、「ハイパーバイザーによって共有されるストレージ」および「一時データ用のキャッシュの構成」を参照してください。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix MCS IODriver"`、コンポーネントのインストールを防止するには `/exclude "Citrix MCS IODriver"`。

- **プロキシ構成:** 環境でGateway Service、VDA Upgrade ServiceなどでRendezvousプロトコルを使用する予定があり、ネットワークにアウトバウンド接続用の非透過型プロキシがある場合は、このコンポーネントをインストールし、ここでプロキシを指定します。HTTPプロキシのみがサポートされています。

  このコンポーネントをインストールする場合は、**Rendezvousプロキシ構成**ページでプロキシのアドレスまたはPACファイルのパスを指定します。機能の詳細については、「Rendezvousプロトコル」を参照してください。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Rendezvous V2"`、コンポーネントのインストールを防止するには `/exclude "Citrix Rendezvous V2"`。

- **Citrix Backup and Restore:** VDAのインストールまたはアップグレードが失敗した場合、このコンポーネントはマシンをインストールまたはアップグレード前のバックアップ状態に戻すことができます。

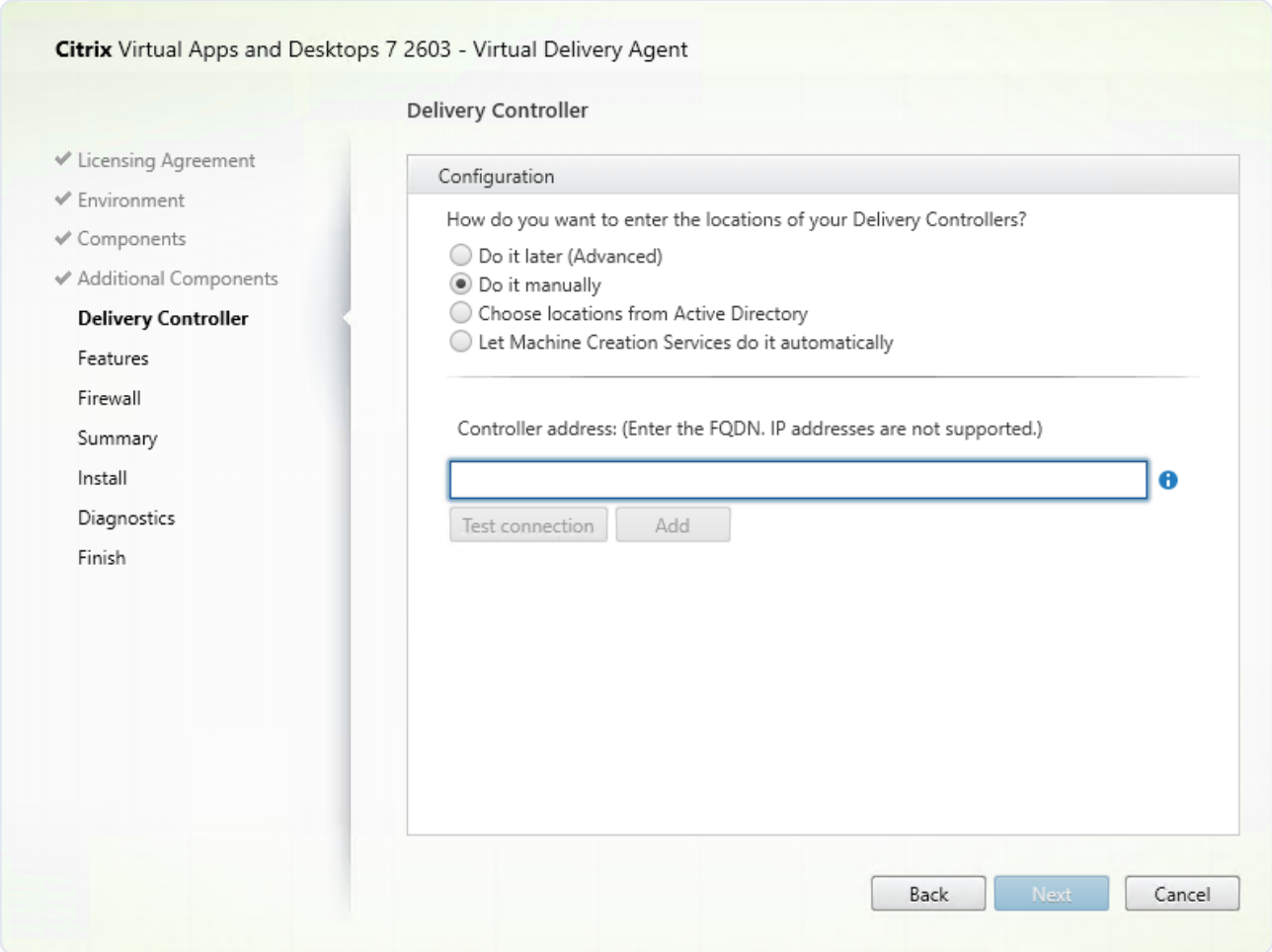
  インストール準備に記載されているMicrosoftの前提条件が満たされていることを確認してください。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Backup and Restore"`、コンポーネントのインストールを防止するには `/exclude "Citrix Backup and Restore"`。

> **注:**

> バージョン2603以降、Citrix Backup and Restoreコンポーネントはワークステーション VDAでのみ利用可能です。MCSストレージ最適化が有効になっている場合、デスクトップオペレーティングシステムのバックアップまたは復元が失敗する可能性があります。これを解決するには、メタインストーラーでMCSストレージ最適化オプションを無効にしてください。

手順7. Delivery Controller™アドレス



Delivery Controllerページで、インストールされているControllerのアドレスを入力する方法を選択します。Citrixでは、VDAのインストール中にアドレスを指定することをお勧めします（**手動で実行**）。VDAは、この情報がないとControllerに登録できません。VDAが登録できない場合、ユーザーはそのVDA上のアプリケーションやデスクトップにアクセスできません。

- **手動で実行:** (デフォルト) インストールされているControllerのFQDNを入力し、**追加**をクリックします。複数のControllerをインストールしている場合は、それらのアドレスも追加します。
- **後で実行 (詳細設定):** このオプションを選択すると、ウィザードは続行する前にその操作を実行するかどうかを確認します。後でアドレスを指定するには、インストーラーを再実行するか、Citrixグループポリシーを使用できます。ウィザードは**概要**ページでも通知します。

- **Active Directoryから場所を選択:** マシンがドメインに参加しており、ユーザーがドメインユーザーである場合にのみ有効です。
- **WebSocketトークンを使用:** WebSocket VDAを作成します。WebSocketTokenは、必要なトークン用です。
- **Machine Creation Servicesに自動的に実行させる:** MCSを使用してマシンをプロビジョニングする場合にのみ有効です。

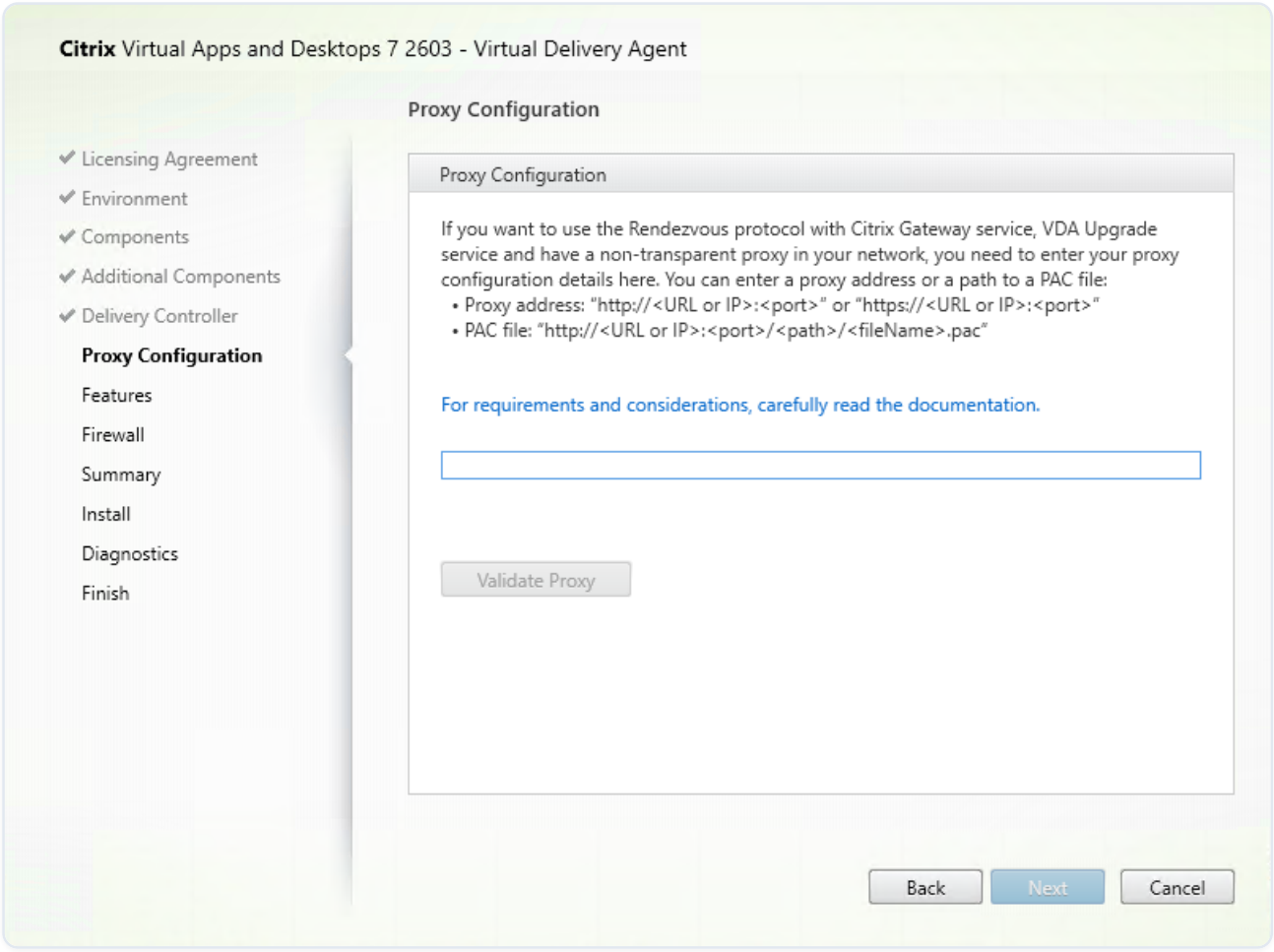
次へをクリックします。**後で実行 (詳細設定)**を選択した場合、Controllerアドレスを後で指定することを確認するよう求められます。

その他の考慮事項:

- アドレスには英数字以外の文字を含めることはできません。
- VDAのインストール時とグループポリシーでアドレスを指定した場合、ポリシー設定がインストール時に指定された設定を上書きします。
- VDAの登録を成功させるには、Controllerとの通信に使用されるファイアウォールポートが開いている必要があります。このアクションは、ウィザードの**ファイアウォール**ページでデフォルトで有効になっています。
- Controllerの場所を指定した後（VDAのインストール中またはインストール後）、Controllerが追加または削除されたときにVDAを更新するために、自動更新機能を使用できます。VDAがControllerを検出して登録する方法の詳細については、「VDA登録」を参照してください。

コマンドラインオプション: `/controllers`

ステップ8. プロキシ構成



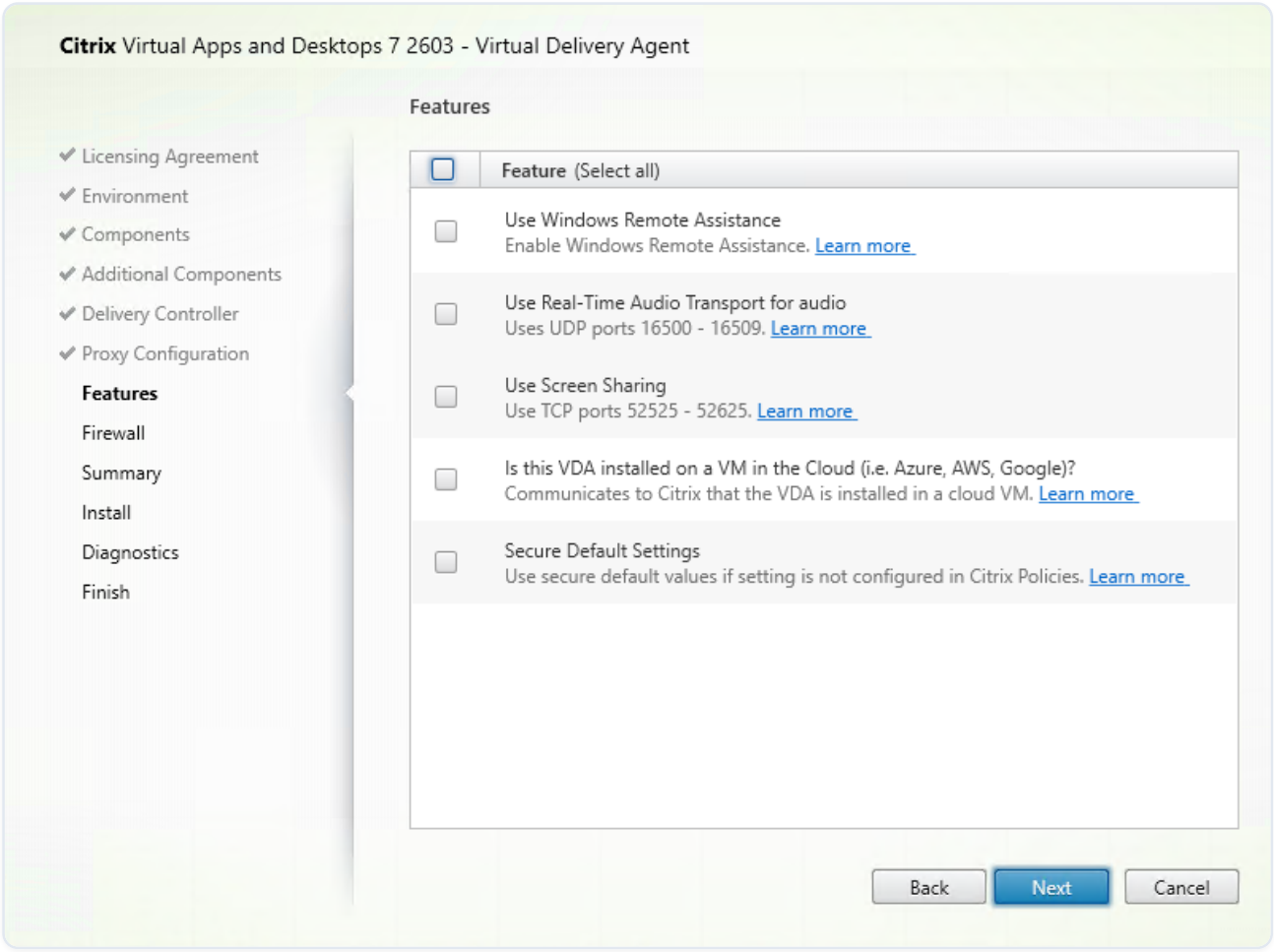
プロキシ構成ページは、**追加コンポーネント**ページで**プロキシ構成**チェックボックスを有効にした場合にのみ表示されます。

1. プロキシソースをプロキシアドレスで指定するか、PACファイルパスで指定するかを選択します。
2. プロキシアドレスまたはPACファイルパスを指定します。
   - プロキシアドレスの形式: `http://<url-or-ip>:<port>`
   - PACファイルの形式: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

接続テストを成功させるには、プロキシポートのファイアウォールが開いている必要があります。プロキシへの接続ができない場合でも、VDAのインストールを続行するかどうかを選択できます。

コマンドラインオプション: `/proxyconfig`

ステップ9. 機能の有効化または無効化



機能ページで、チェックボックスを使用して、使用する機能を有効または無効にします。

- **Windows リモートアシスタンスを使用する:** この機能が有効な場合、Windows リモートアシスタンスはDirectorのユーザーシャドウ機能とともに使用されます。Windows リモートアシスタンスは、ファイアウォールで動的ポートを開きます。(デフォルト = 無効)

  コマンドラインオプション: `/enable_remote_assistance`

- **オーディオにリアルタイムオーディオトランスポートを使用する:** ネットワークでVoice-over-IPが広く使用されている場合は、この機能を有効にします。この機能は、遅延を減らし、損失の多いネットワークでのオーディオの回復力を向上させます。RTP over UDPトランスポートを使用してオーディオデータを送信できます。(デフォルト = 無効)

  コマンドラインオプション: `/enable_real_time_transport`

- **画面共有を使用する:** 有効にすると、画面共有で使用されるポートがWindowsファイアウォールで開かれます。(デフォルト = 無効)

  コマンドラインオプション: `/enable_ss_ports`

- **このVDAはクラウド内のVMにインストールされていますか:** この設定は、Citrixがテレメトリ目的でオンプレミスおよびサービス (Citrix Cloud™) VDA展開のリソースの場所を正しく識別するのに役立ちます。この機能は、顧客側の利用には影響しません。展開でCitrix DaaSを使用している場合は、この設定を有効にします。(デフォルト = 無効).

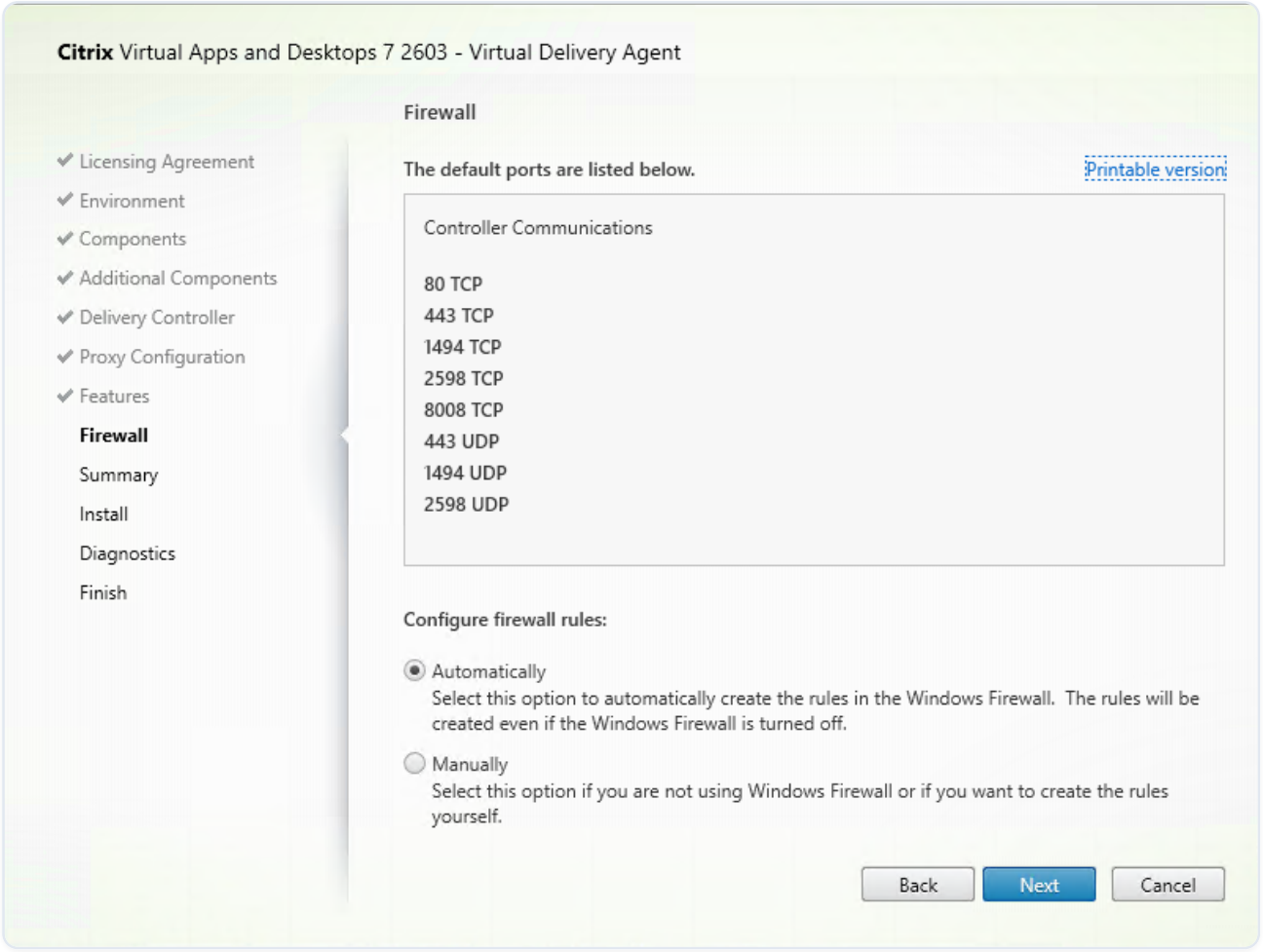
  コマンドラインオプション: `/xendesktopcloud`

- **セキュアなデフォルト設定:** このオプションは、より安全な初期設定のために、さまざまな機能のデフォルト設定を有効から無効に変更します。関連する機能は、クライアントドライブリダイレクト、特殊フォルダーリダイレクト、ドラッグアンドドロップ、クライアントTWAINデバイスリダイレクト、クライアントUSBプラグアンドプレイデバイスリダイレクト、クライアントプリンターリダイレクト、クライアントクリップボードリダイレクト、およびクライアントマイクのリダイレクトです。

コマンドラインオプション: `/ENABLE_SECURE_DEFAULTS`

Nextをクリックします。

手順 10. ファイアウォールポート

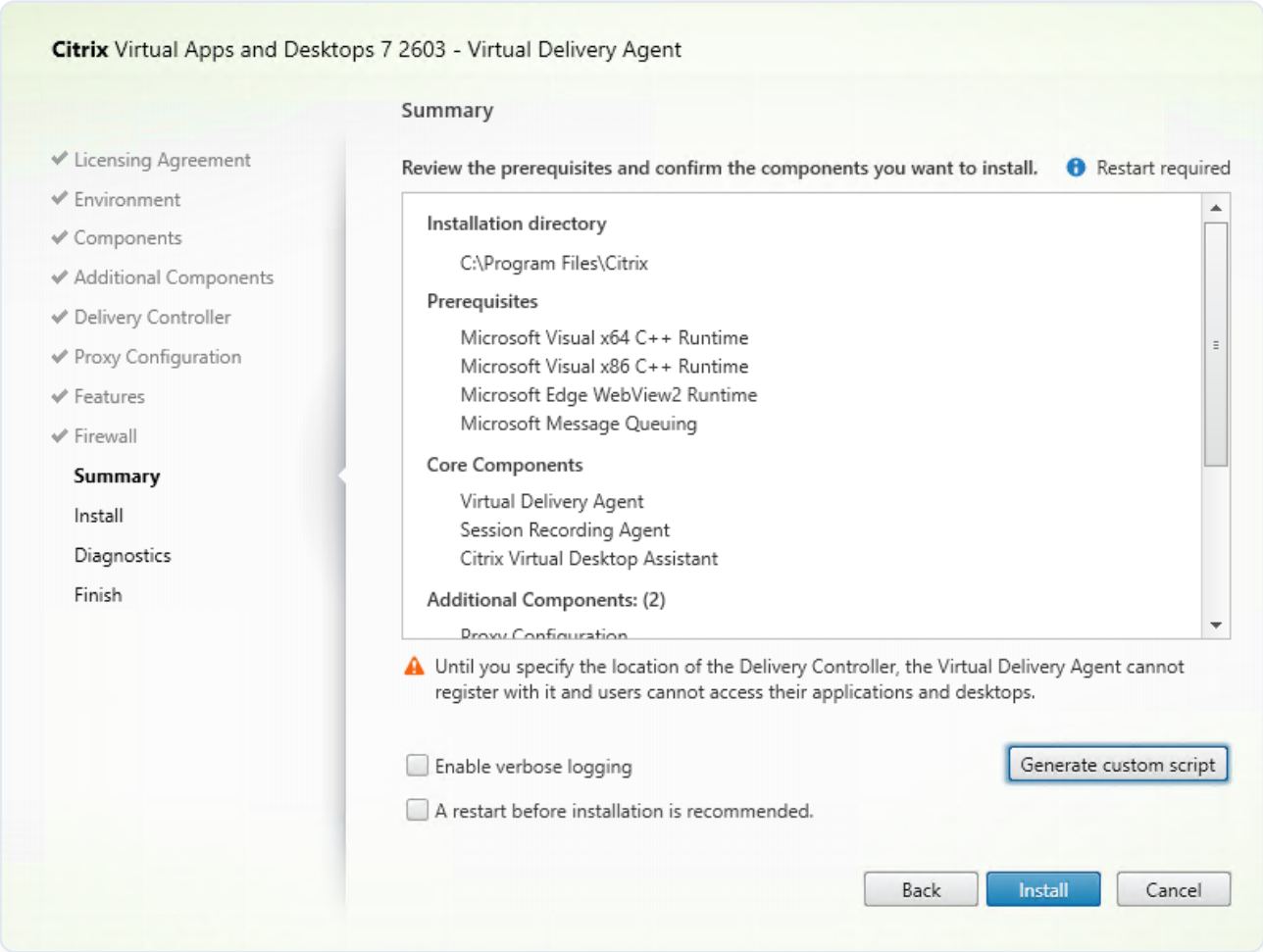


ファイアウォールページでは、デフォルトで、Windowsファイアウォールサービスが実行されている場合、ファイアウォールが有効になっていなくてもポートは自動的に開かれます。このデフォルト設定は、ほとんどの展開で問題ありません。ポート情報については、「ネットワークポート」を参照してください。

Nextをクリックします。

コマンドラインオプション: `/enable_hdx_ports`

手順 11. 前提条件を確認し、インストールを確定する



概要ページには、インストールされるものが一覧表示されます。**戻る**ボタンを使用して、以前のウィザードページに戻り、選択を変更します。

準備ができたら、**インストール**をクリックします。

前提条件がまだインストールまたは有効になっていない場合、マシンは1回以上再起動する可能性があります。インストールの準備を参照してください。

> **注:**

> この時点で、「**概要**」ページの「**カスタムスクリプトの生成**」ボタンをクリックして、現在のインストール選択に基づいてコマンドラインスクリプトを作成することもできます。このスクリプトは、無人モードでVDAをインストールまたはアップグレードするために再利用できます。

ステップ12. 診断

VDAインストーラーの診断ページ(/en-us/citrix-virtual-apps-desktops/current-release/media/vda-ss-diagnostics.png)

診断ページで、Citrix Call Homeに参加するかどうかを選択します。参加することを選択した場合（デフォルト）、**接続**をクリックします。プロンプトが表示されたら、Citrixアカウントの資格情報を入力します。

資格情報が検証された後（または参加しないことを選択した場合）、**次へ**をクリックします。

フル製品インストーラーを使用している場合、**診断**ページで最初に**診断情報の収集**を選択せずに**接続**をクリックすると、**Citrix Insight Servicesへの接続**ダイアログを閉じた後、**次へ**ボタンが無効になります。次のページに進むことはできません。**次へ**ボタンを再度有効にするには、**診断情報の収集**を選択し、すぐに選択を解除します。

詳細については、Call Homeを参照してください。

ステップ13. このインストールを完了する

VDAインストーラーのインストール完了ページ(/en-us/citrix-virtual-apps-desktops/current-release/media/vda-ss-finish.png)

完了ページには、正常にインストールおよび初期化されたすべての前提条件とコンポーネントの緑色のチェックマークが表示されます。

完了をクリックします。デフォルトでは、マシンは自動的に再起動します。この自動再起動を無効にすることはできますが、マシンが再起動するまでVDAは使用できません。

次のステップ

必要に応じて、上記のプロシージャを繰り返して、他のマシンまたはイメージにVDAをインストールします。

すべてのVDAをインストールしたら、Studioを起動します。まだサイトを作成していない場合、Studioはそのタスクに自動的に誘導します。それが完了すると、Studioはマシンカタログとデリバリーグループの作成に誘導します。参照：

- サイトの作成
- マシンカタログの作成
- 「デリバリーグループの作成」(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/delivery-groups-create.html)

シトリックス オプティマイザー

Citrix Optimizerは、Citrix管理者がさまざまなコンポーネントを削除および最適化することでVDAを最適化するのに役立つWindows OS用のツールです。

VDAをインストールし、最終的な再起動を完了した後、Citrix Optimizerをダウンロードしてインストールします。「CTX224676」を参照してください。CTXの記事には、ダウンロードパッケージと、Citrix Optimizerのインストールおよび使用方法に関する手順が含まれています。

VDAをカスタマイズする

インストール済みのVDAをカスタマイズするには：

1. Windowsのプログラムの削除または変更機能から、「**Citrix Virtual Delivery Agent**」または「**Citrix Remote PC Access/VDI Core Services VDA**」を選択します。その後、右クリックして「**変更**」を選択します。
2. 「**Virtual Delivery Agent Settingsのカスタマイズ**」を選択します。インストーラーが起動したら、以下を変更できます。
    - Controllerアドレス
    - Controllerに登録するTCP/IPポート（デフォルト = 80）
    - Windowsファイアウォールポートを自動的に開くかどうか

トラブルシューティング

- コンポーネントインストールの結果をCitrixが報告する方法については、「Citrixインストールリターンコード」(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/install-prepare.html#citrix-installation-return-codes)を参照してください。
- デリバリーグループのStudio表示では、**詳細**ペインの**インストール済みVDAバージョン**エントリが、マシンにインストールされているバージョンと異なる場合があります。マシンのWindowsのプログラムと機能の表示には、実際のVDAバージョンが表示されます。
- VDAがインストールされても、Delivery Controllerに登録されるまでは、ユーザーにアプリやデスクトップを配信できません。

VDA登録方法と登録問題のトラブルシューティング方法については、「VDA登録」(/ja-jp/citrix-virtual-apps-desktops/current-release/manage-deployment/vda-registration.html)を参照してください。

既知の制限事項

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

VDAインストールに関連するWindows Defenderアクセス制御の構成

お客様は、署名されていないバイナリの読み込みを禁止するために、Windows Defenderアクセス制御 (WDAC) 設定を構成します。VDAインストーラーを通じて配布される署名されていないバイナリは、VDAのインストールを制限するため、禁止されます。

Citrix® は現在、すべてのCitrix生成バイナリをCitrixコード署名証明書で署名しています。さらに、Citrixは、当社の製品とともに配布されるサードパーティ製バイナリも、それらのサードパーティ製バイナリを信頼できるバイナリとして認証する証明書で署名しています。

重要:

署名されていないサードパーティ製バイナリを含む古いVDAから、署名されたバイナリを含む新しいVDAバージョンにアップグレードしても、常にアップグレードされたマシンに署名されたバイナリが配置されるとは限りません。 これは、OS内のメカニズムにより、システムのアップグレードで同じバージョンのバイナリが置き換えられないためです。 サードパーティ製バイナリは署名されていますが、サードパーティによって制御されているそのバージョンはCitrixによって更新できないため、これらのバイナリは更新されません。この制限を回避するには：

1. バイナリを許可リストに含めます。これにより、バイナリに署名する必要がなくなります。
2. 古いVDAをアンインストールし、新しいVDAをインストールします。これはVDAの新規インストールに似ており、署名されたバージョンがインストールされます。

ウィザードを使用して新しいベースポリシーを作成する

WDACを使用すると、信頼できるバイナリをシステムで実行できるように追加できます。WDACのインストール後、**Windows Defender Application Control Policy Wizard** が自動的に開きます。

バイナリを追加するには、新しいベースWDACポリシーを作成する必要があります。ベースポリシーを作成するためのCitrix推奨ガイドラインは、このセクションで提供されています。

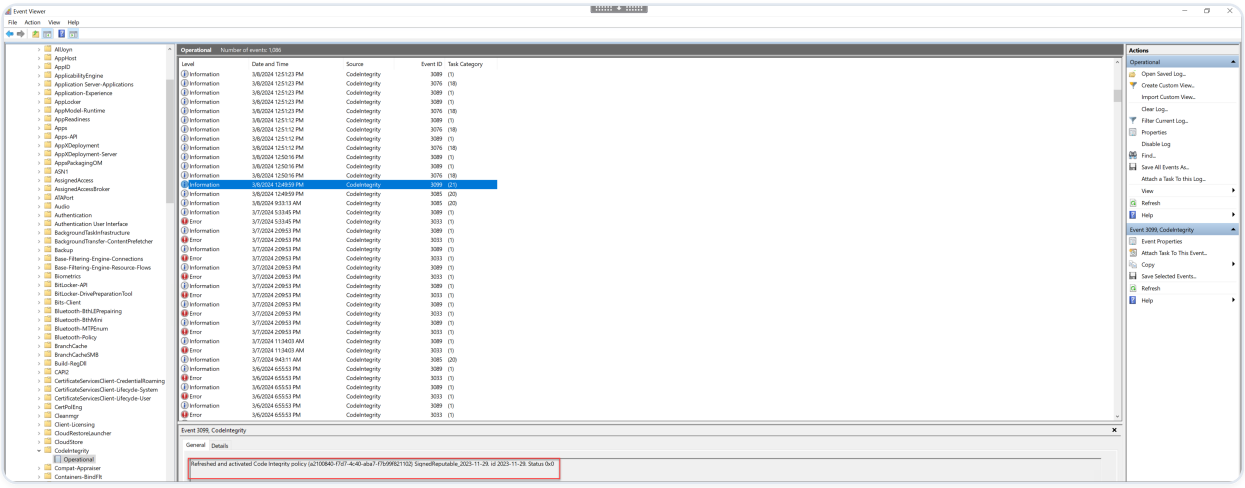
- Windowsオペレーティングコンポーネント、Microsoft Storeからインストールされたアプリ、すべてのMicrosoft署名済みソフトウェア、およびサードパーティのWindowsハードウェア互換ドライバーを承認するため、ベーステンプレートとして を選択します。
- 新しいWindows Defender Application Controlポリシーを適用する前にテストできるため、 を選択します。
- アプリケーションが識別され信頼されるレベルを指定し、参照ファイルを提供するために、に を追加します。ルールタイプとして「発行元」を選択すると、Citrix証明書のいずれかで署名された参照ファイルを選択できます。
- ルールを追加したら、`.XML` および `.CIP` ファイルが保存されているフォルダーに移動します。`.XML` ファイルには、ポリシーで定義されているすべてのルールが含まれています。任意のルールを変更、追加、または削除するように構成できます。
- WDACポリシーを展開する前に、`.XML` ファイルをバイナリ形式に変換する必要があります。WDACファイルは、`.XML` ファイルを `.CIP` ファイルに変換します。
- `.CIP` ファイルを C:\WINDOWS\System32\CodeIntegrity\CiPolicies\Active にコピーして貼り付け、マシンを再起動します。生成されたポリシーは監査モードで適用されます。
- ベースポリシーを作成する手順については、ウィザードで新しいベースポリシーを作成するを参照してください。

このポリシーが適用されると、WDACは、指定された発行元/CA機関によって署名されているCitrixファイルについて警告を発しません。

同様に、サードパーティによって署名されたファイルに対して、発行元レベルのルールを作成できます。

適用されたポリシーを確認する

1. マシンが再起動された後、**イベントビューアー**を開き、**アプリケーションとサービスログ > Microsoft > Windows > CodeIntegrity > Operational**に移動します。
2. 適用されたポリシーがアクティブになっていることを確認します。



3. ポリシーに違反したログを探し、そのファイルのプロパティを確認します。まず、署名されていることを確認します。署名されていない場合で、このマシンがVDAアップグレードを経ている場合、これは上記の制限で説明されているケースである可能性が高いです。署名されている場合、このファイルは、前述のとおり、代替証明書で署名されている可能性があります。

Citrix証明書で署名されたCitrix生成ファイルの例は`C:\Windows\System32\drivers\picadm.sys`です。 Citrixサードパーティ証明書で署名されたサードパーティバイナリの例は`C:\Program Files\Citrix\IcaConfigTool\Microsoft.Practices.Unity.dll`です。

VDAのインストールとアップグレードの事前チェック

VDAのインストールとアップグレードのための独立した事前確認を導入することで、お客様は作業を進める前に潜在的な問題を事前に特定できるようになります。このチェックは、すべての依存関係と前提条件を検証し、各条件の明確な合否ステータスを提供します。不合格が発生した場合は、具体的な推奨事項を含む詳細な修復ガイダンスが提供されます。実際のインストールまたはアップグレードプロセスは分離されており、事前チェックが完了した後に手動で開始する必要があります。

この記事では、VDAのインストールとアップグレードの事前チェックを実行する手順について説明します。

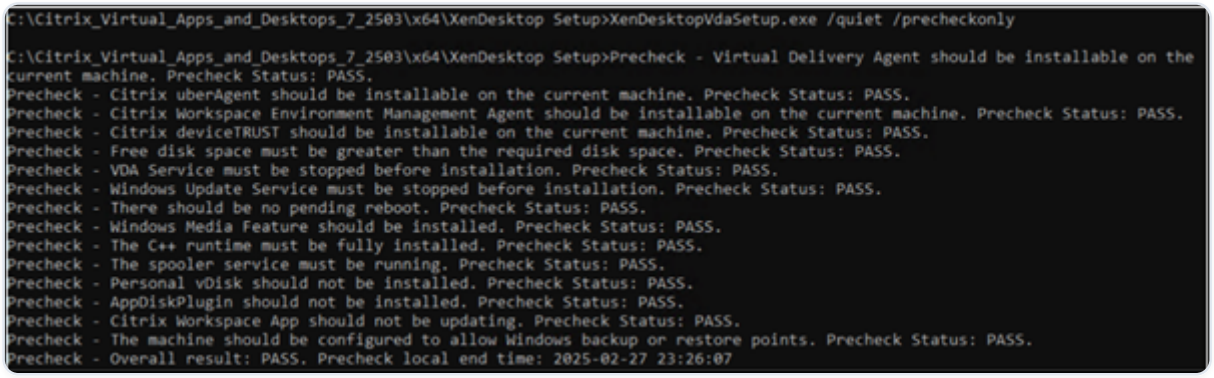
ステップ1. コマンドラインを実行する

> **注:**
>
> - 事前チェックはコマンドラインモードでのみサポートされています。
> - このコマンドを実行しても、インストールまたはアップグレードは開始されません。

> 事前チェックを実行するには、インストールまたはアップグレードによく使用するコマンドに `/precheckonly` オプションを追加します。VDAのインストールまたはアップグレードのすべての事前チェック条件が確認されます。

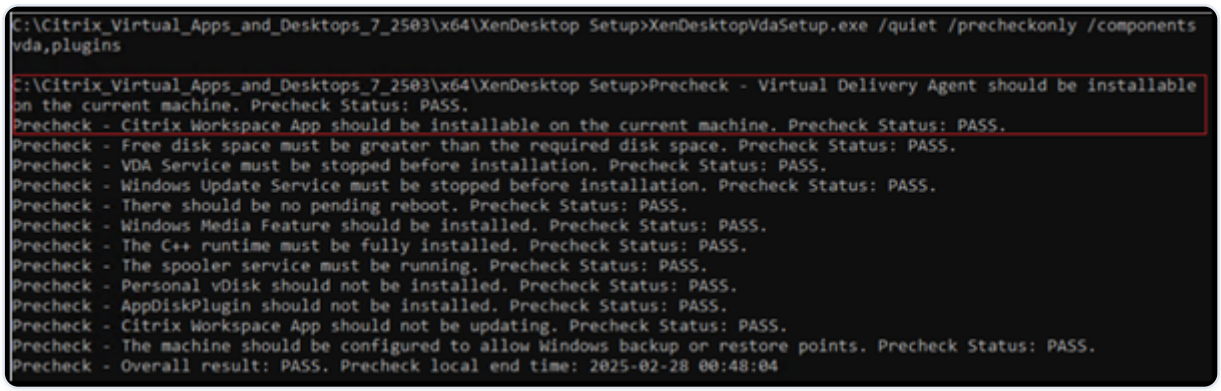
デフォルトのインストールとアップグレードの事前チェックを実行する

事前チェックを実行し、マシンの状態が許容できる状態であることを確認するには、次のコマンドを実行します。 `\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly`



指定されたコンポーネントのインストールとアップグレードの事前チェックを実行する

インストールまたはアップグレードの前に特定のコンポーネントの前提条件を確認するには、コマンドに `/precheckonly` を追加します。 `\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly /components vda,plugins`



追加コンポーネント - Citrix Backup and Restore のインストールとアップグレードの事前チェックを実行する

コマンド `\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly` は、Citrix Backup and Restoreコンポーネントの前提条件をオプションチェックとして確認します。オプションチェックを除くすべての事前チェックが合格した場合、全体の結果はPASSとなります。

追加コンポーネントの事前チェック(/en-us/citrix-virtual-apps-desktops/current-release/media/precheck-for-additional-components.png)

以下のコマンドは、必須チェックの一部としてCitrix Backup and Restoreコンポーネントの前提条件をチェックします。

- `\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly /includeadditional "Citrix Backup and Restore"`
- `\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly /enablerestore`
- `\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly /enablerestorecleanup`

Citrix Backup and Restoreの事前チェック(/en-us/citrix-virtual-apps-desktops/current-release/media/precheck-for-citrix-backup-and-restore.png)

ステップ2. 事前チェック結果の表示

事前チェックの結果はコマンドラインに表示され、`%temp%/Citrix/XenDesktop Installer/XenDesktop Installation.log`にログ記録され、`%temp%/Citrix/XenDesktop Installer/PrecheckResult_{yyyyMMddHHmmss}.json`に保存されます。事前チェックが失敗した場合、全体の結果は`FAIL`となり、各問題に対する修正案が提示されます。

コマンドライン出力

コマンドラインの事前チェック結果には以下が含まれます。

- 事前チェック基準
- 事前チェックステータス
- 失敗に対する修正案
- 全体の結果
- 終了時刻。

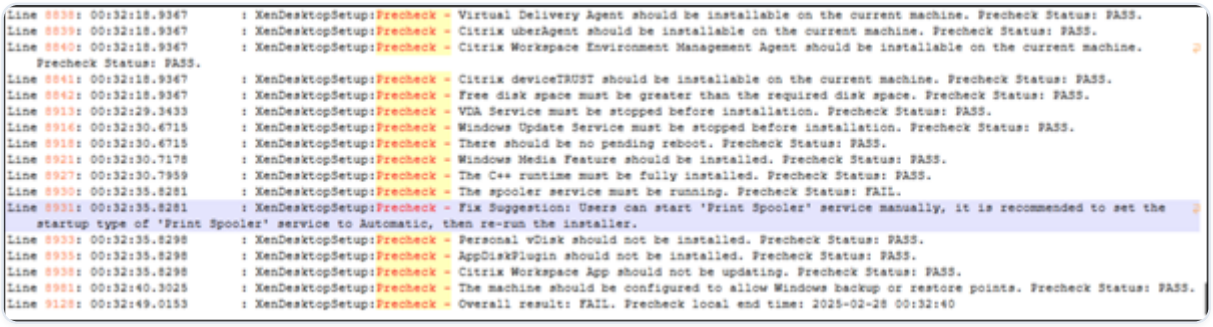
結果が`FAIL`の場合、修正案は「**Precheck - Fix Suggestion:**」で始まる行に記載されています。

ログ出力(/en-us/citrix-virtual-apps-desktops/current-release/media/log-output.png)

ログ出力

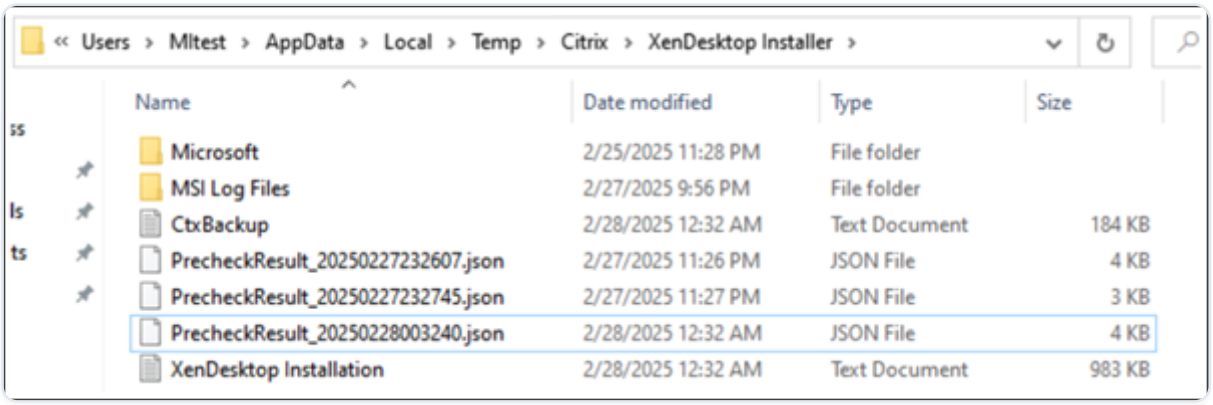
`XenDesktop Installation.log`の事前チェック結果は、コマンドラインに表示されるものと同じです。それらを見つけるには、ログファイルで`Precheck -`を検索してください。 全体的な

結果が `FAIL` の場合、修正の提案は `Precheck - Fix Suggestion:` を含む行で利用できます。



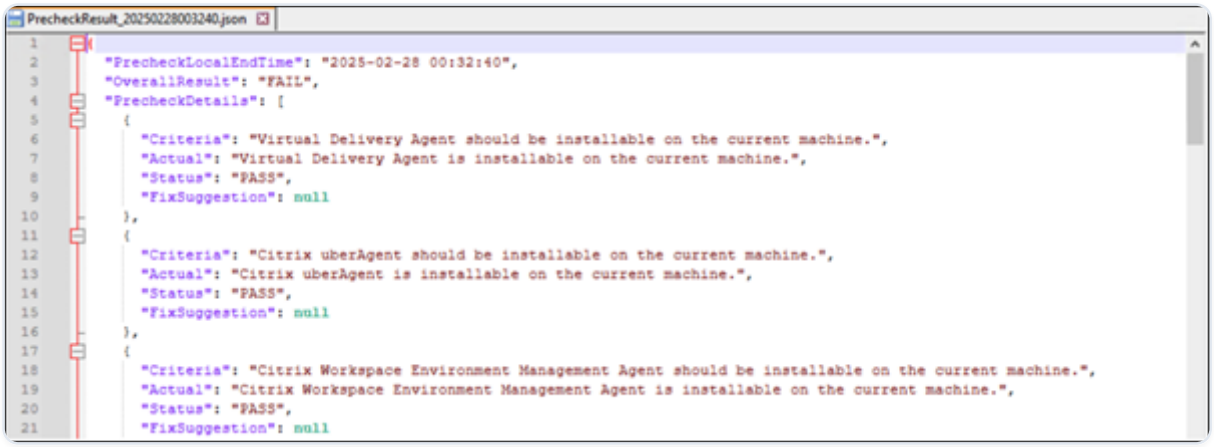
JSON 出力

`/quiet /precheckonly` を含むコマンドが実行されるたびに、`.json` ファイルが生成されます。ファイル名は `PrecheckResult_{yyyyMMddHHmmss}.json` で、タイムスタンプのサフィックスが付いています。

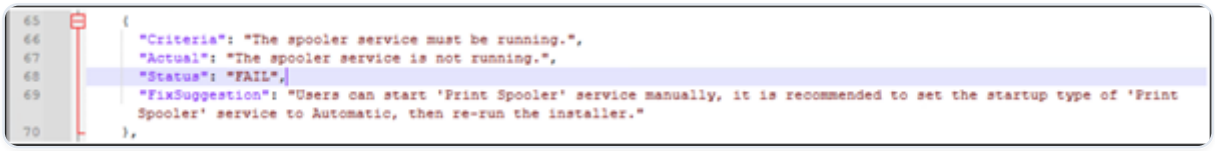


`.json` ファイルには以下が含まれます。

- 事前チェックのローカル終了時刻
- 全体的な結果
- 事前チェックの詳細
  - 基準
  - 実際の値
  - ステータス
  - 修正提案



`FAIL` のステータスを持つ各事前チェック項目に対する修正提案は、`.json` ファイルの事前チェック詳細セクションで見つけることができます。



VDA メタインストーラー ヘルパーツール

1. はじめに

VDA メタインストーラーヘルパーツールには、SCCM タスクシーケンスによる VDA インストールを支援する一連のツールと、インストールログを分析して潜在的な問題を特定するためのユーティリティが含まれています。

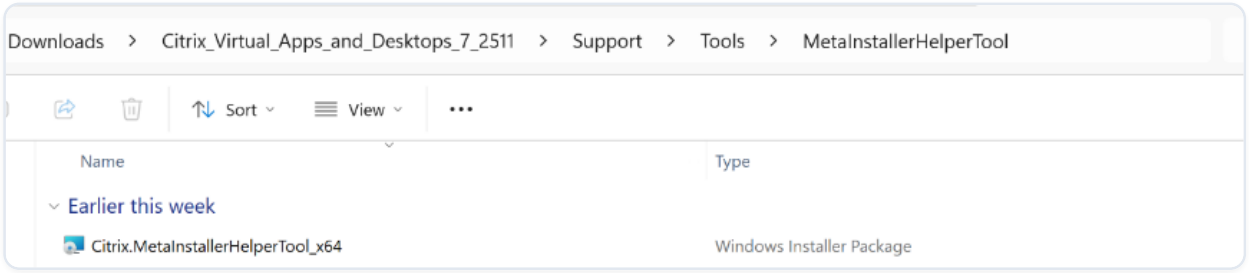
シンプルな MSI インストールと直感的なユーザーインターフェイスを備えたメタインストーラーヘルパーツールは、いくつかの重要な機能を提供します。

- **SCCM タスクシーケンスの確認:** このツールは、既存の SCCM タスクシーケンスをレビューおよび検証し、VDA インストール要件との互換性を確保するのに役立ちます。
- **タスクシーケンスリファレンスの生成:** このツールは、VDA インストールを SCCM 展開ワークフローに最小限の手動設定で統合するのに役立つリファレンスタスクシーケンスを自動的に作成します。
- **VDA インストールログアナライザー:** このツールは、インストールログをレビューして、エラー、警告、または失敗を特定するのに役立ちます。このツールは、根本原因、考えられる解決策、および展開を成功させるための推奨事項を強調したレポートを生成します。

2. インストール

1. Citrix Virtual Apps and Desktops ダウンロードページ から Citrix Virtual Apps and Desktops 製品 ISO をダウンロードします。

2. `\Support\Tools\MetaInstallerHelperTool` フォルダーから Citrix.MetaInstallerHelperTool_x64.msi を見つけます。



3. Citrix.MetaInstallerHelperTool_x64.msi をダブルクリックしてツールをインストールします。

> **注:**
>
> このツールは VDA の一部ではありません。VDA または任意のローカルデバイスにインストールできます。

4. インストール後、スタートメニューで「MetaInstallerHelperTool」を検索して、管理者としてアプリケーションを起動します。

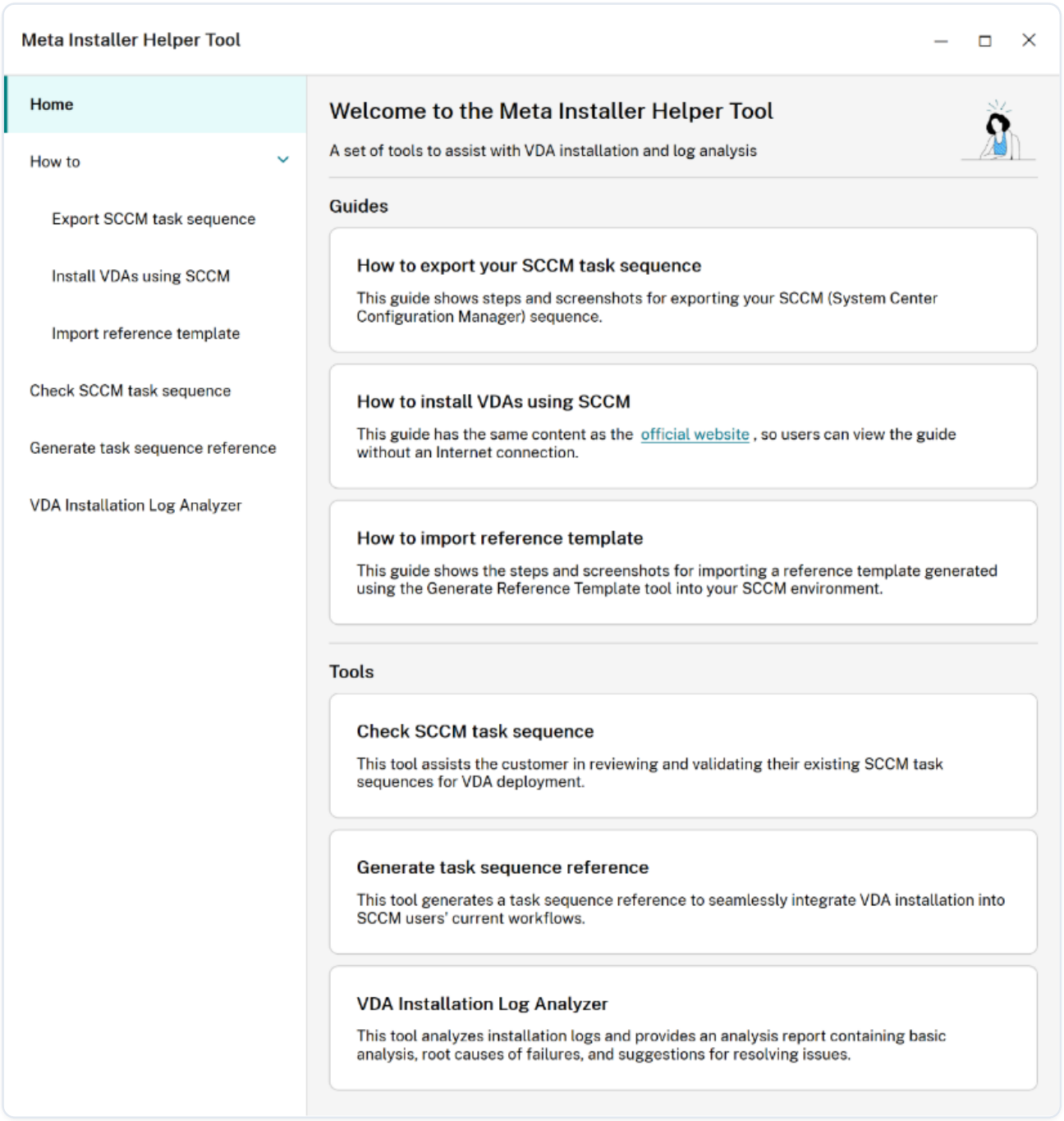


3. ユーザーインターフェイス (UI) の概要

アプリケーション「MetaInstallerHelperTool」を起動すると、直感的なナビゲーションと使いやすさを考慮して設計されたメインユーザーインターフェイスが表示されます。

「**ホーム**」セクションには、「ハウツー」セクションのガイドの説明と、SCCMシーケンスの確認、タスクシーケンステンプレートの生成、VDAインストールログの分析を行うツールの機能説明が記載されています。

これらのガイドとツールには、左側のナビゲーションパネルから対応するタブを選択することでアクセスできます。



「**ハウツー**」セクションには、タスクシーケンスのエクスポート、SCCMを使用したVDAのインストール、スクリーンショットと手順を含む参照テンプレートのインポートに関するガイドが記載されています。

- 「タスクシーケンスのエクスポート方法」を参照して、「SCCMタスクシーケンスの確認」ツールで使用するSCCMタスクシーケンスを取得します。
- VDAをインストールするには、「SCCMを使用してVDAをインストールする方法」を参照してください。「SCCMタスクシーケンスの確認」ツールと「タスクシーケンステンプレートの生成」ツールもこのガイドを参照します。

- 「参照テンプレートのインポート方法」を参照して、「タスクシーケンステンプレートの生成」ツールで生成されたテンプレートを、参照テンプレートとしてSCCM環境にインポートします。

SCCMタスクシーケンスの確認、タスクシーケンステンプレートの生成、VDAインストールログアナライザーの各セクションでは、Meta Installer Helper Toolの主要なタスクを実行できます。

4. ツール

1. SCCMタスクシーケンスの確認

   SCCM環境からエクスポートされたタスクシーケンスをアップロードして、レビューと検証を行います。

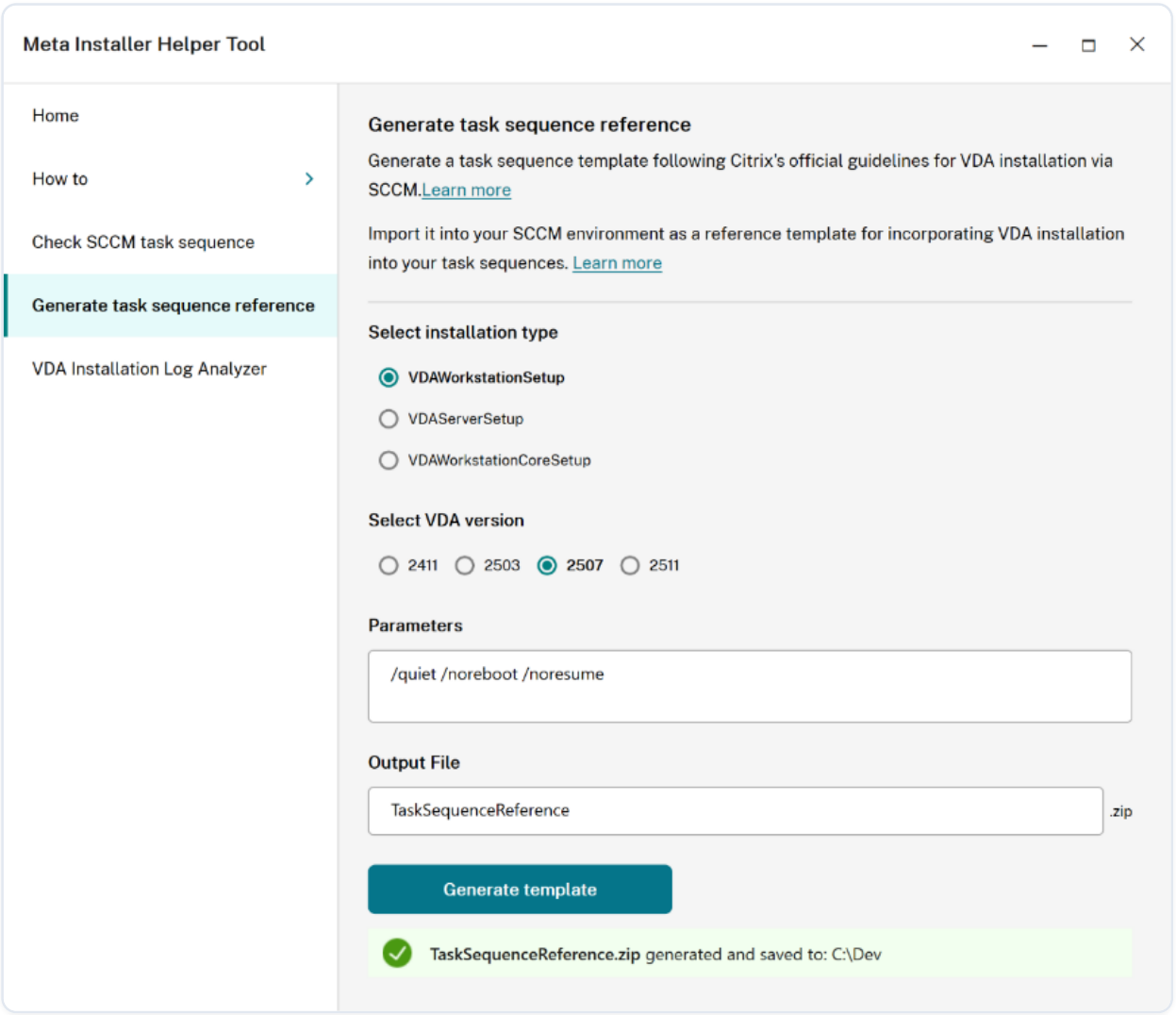
   このツールは、アップロードされたファイルがzipファイルであり、必要なSCCMタスクシーケンスフォルダー構造、必要なオブジェクト.xmlファイル、および有効なタスクシーケンス定義が含まれているかどうかを確認します。また、タスクシーケンスに基づいてコマンドラインパラメーター分析とインストール条件分析も行います。

   Meta Installer SCCMの確認(/en-us/citrix-virtual-apps-desktops/current-release/media/metainstaller-check-sccm.png)

2. タスクシーケンス参照の生成

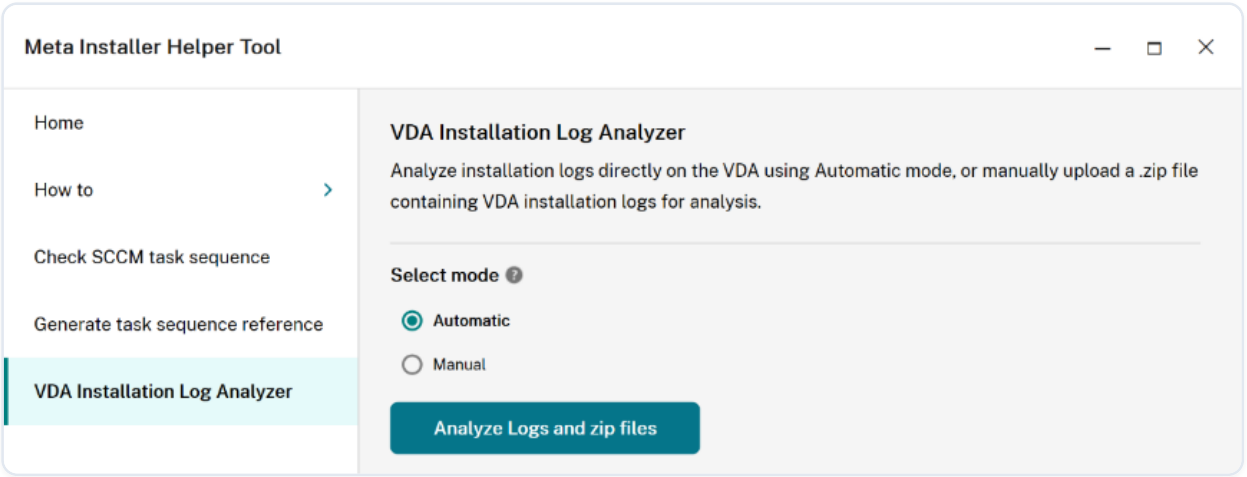
   このツールは、SCCM を介した VDA インストールに関するCitrix の公式ガイドラインに従って、タスクシーケンステンプレートを生成します。

   これを SCCM 環境にインポートして、VDA インストールをタスクシーケンスに組み込むための参照テンプレートとして使用できます。

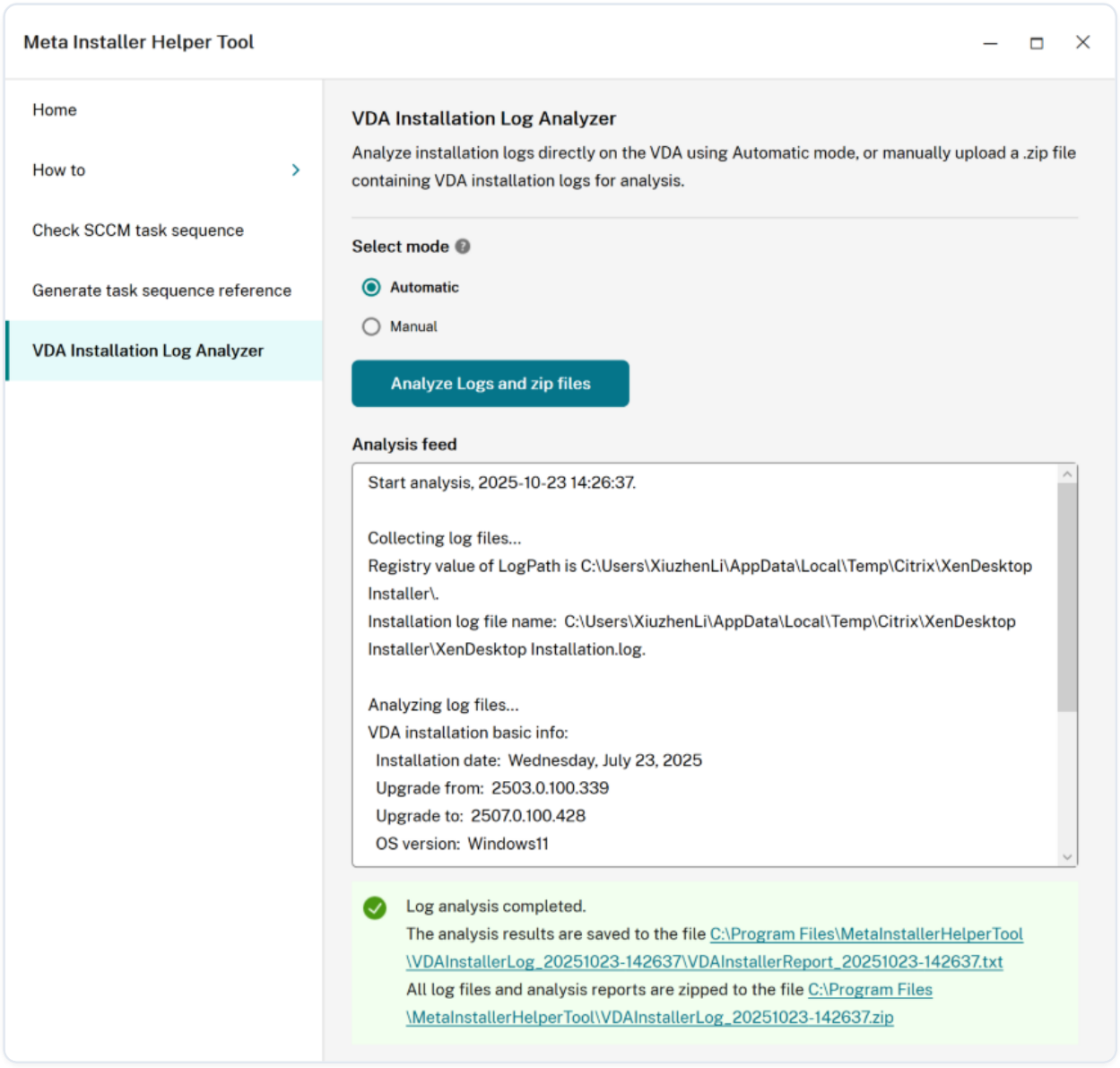


3. VDA インストールログアナライザー

   自動モードを使用して VDA 上で直接インストールログを分析するか、VDA インストールログを含む .zip ファイルを手動でアップロードして分析します。



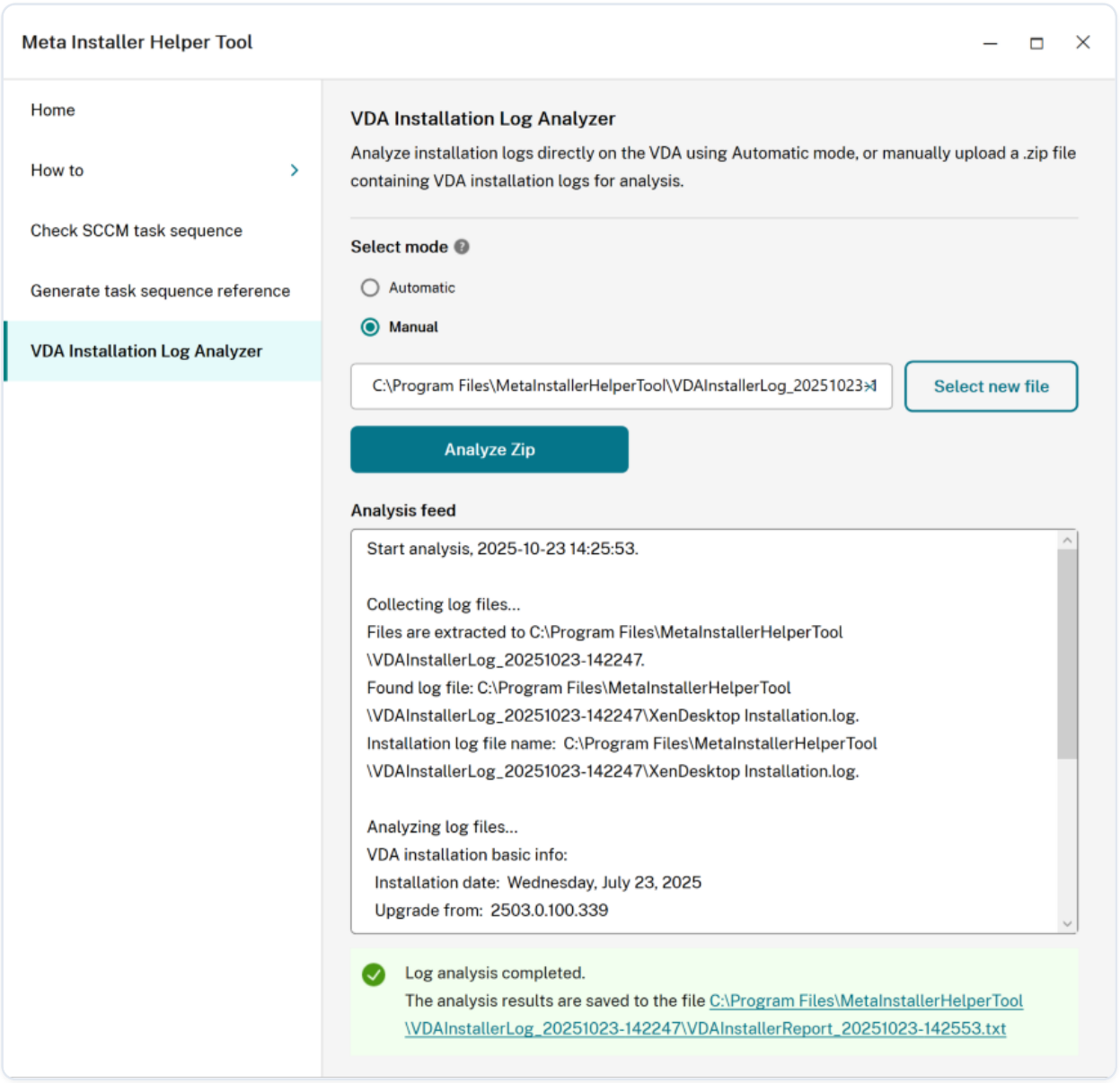
   VDA 上で **自動モード** で実行すると、ツールはログ保存パスを自動的に検出し、インストールログをローカルで分析します。分析結果は保存され、すべてのログファイルとレポートは単一の ZIP ファイルにパッケージ化されます。



手動モード では、分析のために VDA インストールログを含む .zip ファイルをアップロードする必要があります。デフォルトでは、ログファイルは次の場所に保存されます。 `%TEMP%\Citrix\XenDesktop Installer`

デフォルトのログパスが変更されている場合は、Windows レジストリの次の場所で現在の場所を確認できます。 `Computer\HKLM\Software\Citrix\MetaInstall\LogPath`

ツールはアップロードされた .zip ファイルを抽出し、その内容を分析し、分析結果を保存して確認できるようにします。



スクリプトを使用してVDAをインストールする

注:

Citrixは、お客様の運用環境に合わせて調整されたスクリプトによって引き起こされる問題について責任を負いません。インストール関連のCitrixの問題については、Citrixサポートポータルを使用して、関連するインストールログとともにテクニカルサポートケースをオープンしてください。

この記事は、Windowsオペレーティングシステムを搭載したマシンへのVDAのインストールに適用されます。Linuxオペレーティングシステム用VDAの詳細については、Linux Virtual Delivery Agentのドキュメントを参照してください。

インストールメディアには、Active Directory内のマシンにVirtual Delivery Agent（VDA）をインストール、アップグレード、または削除するサンプルスクリプトが含まれています。これらのスクリプトは、Machine Creation Services™およびCitrix Provisioning（旧Provisioning Services）で使用されるマスターイメージの保守にも使用できます。

必要なアクセス権:

- スクリプトには、VDAインストールコマンドが配置されているネットワーク共有へのEveryone読み取りアクセス権が必要です。インストールコマンドは、製品版ISOでは `XenDesktopVdaSetup.exe`、スタンドアロンインストーラーでは `VDAWorkstationSetup.exe` または `VDAServerSetup.exe` です。
- ログの詳細は各ローカルマシンに保存されます。レビューと分析のために結果を集中してログに記録するには、スクリプトに適切なネットワーク共有へのEveryone読み取り/書き込みアクセス権が必要です。

スクリプトの実行結果を確認するには、中央ログ共有を調べます。キャプチャされたログには、スクリプトログ、インストーラーログ、MSIインストールログが含まれます。各インストールまたは削除の試行は、タイムスタンプ付きのフォルダーに記録されます。フォルダーのタイトルは、PASSまたはFAILのプレフィックスで操作結果を示します。標準のディレクトリ検索ツールを使用して、中央ログ共有で失敗したインストールまたは削除を見つけることができます。これらのツールは、ターゲットマシンでローカルに検索する代替手段を提供します。

インストールを開始する前に、インストールの準備のタスクを読み、完了してください。

スクリプトを使用してVDAをインストールまたはアップグレードする

1. インストールメディアの `\\Support\AdDeploy\` からサンプルスクリプト **InstallVDA.bat** を入手します。Citrixは、元のスクリプトをカスタマイズする前にバックアップを作成することをお勧めします。
2. スクリプトを編集します:
    - インストールするVDAのバージョンを指定します: `SET DESIREDVERSION`。完全な値は、インストールメディアのProductVersion.txtファイルに記載されています。ただし、完全に一致している必要はありません。
    - インストーラーが呼び出されるネットワーク共有を指定します。レイアウトのルート（ツリーの最上位）を指します。スクリプトの実行時に、適切なバージョンのインストーラー（32ビットまたは64ビット）が自動的に呼び出されます。例: `SET DEPLOYSHARE=\\fileserver1\share1`。

- オプションで、集中ログを保存するためのネットワーク共有の場所を指定します。例: `SET LOGSHARE=\\fileserver1\log1)`。
- コマンドラインを使用したインストールで説明されているように、VDA構成オプションを指定します。`/quiet`および`/noreboot`オプションは、スクリプトにデフォルトで含まれており、必須です: `SET COMMANDLINEOPTIONS=/QUIET /NOREBOOT /NORESUME`。

3. グループポリシーのスタートアップスクリプトを使用して、スクリプトをマシンを含むOUに割り当てます。このOUには、VDAをインストールするマシンのみを含める必要があります。そのOU内のマシンが再起動されると、スクリプトはすべてのマシンで実行されます。サポートされているオペレーティングシステムを持つ各マシンにVDAがインストールされます。

スクリプトを使用してVDAを削除する

1. インストールメディアの`\\Support\AdDeploy\`からサンプルスクリプトUninstallVDA.batを入手します。Citrixでは、スクリプトをカスタマイズする前に元のスクリプトのバックアップを作成することをお勧めします。
2. スクリプトを編集します。
   - 削除するVDAのバージョンを指定します: `SET CHECK\_VDA\_VERSION`。完全な値は、インストールメディアのProductVersion.txtファイル（例: 7.0.0.3018）で確認できます。ただし、完全一致は必須ではありません。
   - オプションで、集中ログを保存するためのネットワーク共有の場所を指定します。
3. グループポリシーのスタートアップスクリプトを使用して、スクリプトをマシンを含むOUに割り当てます。このOUには、VDAを削除するマシンのみを含める必要があります。OU内のマシンが再起動されると、スクリプトはすべてのマシンで実行されます。各マシンからVDAが削除されます。

トラブルシューティング

- スクリプトは、スクリプトの実行の進行状況を記述する内部ログファイルを生成します。スクリプトは、展開の開始から数秒以内に`Kickoff_VDA_Startup_Script`ログを中央ログ共有にコピーします。全体的なプロセスが機能していることを確認できます。このログが期待どおりに中央ログ共有にコピーされない場合は、ローカルマシンを検査してさらにトラブルシューティングを行ってください。スクリプトは、各マシンの`%temp%`フォルダーに2つのデバッグログファイルを配置します。
  - `Kickoff_VDA_Startup_Script_<DateTimeStamp>.log`
  - `VDA_Install_ProcessLog_<DateTimeStamp>.log`

スクリプトが次の状態であることを確認するために、これらのログを確認します。

- 期待どおりに実行されている。
- ターゲットオペレーティングシステムを適切に検出している。
- `DEPLOYSHARE`共有の`ROOT`を指すように正しく構成されている（`AutoSelect.exe`という名前のファイルが含まれている）。
- `DEPLOYSHARE`と`LOG`の両方の共有に対して認証できる。

- Citrixがコンポーネントインストールの結果を報告する方法については、Citrixインストールのリターンコードを参照してください。
- デリバリーグループのStudio表示では、**詳細**ペインの**インストール済みVDAバージョン**エントリが、マシンにインストールされているバージョンと異なる場合があります。マシンのプログラムと機能の表示には、実際のVDAバージョンが表示されます。
- VDAがインストールされた後、Delivery Controllerに登録されるまで、ユーザーにアプリやデスクトップを配信できません。

  VDA登録方法と登録の問題のトラブルシューティング方法については、「VDA登録」を参照してください。

コマンドライン経由でVDAをインストールまたはアップグレードするためのカスタムスクリプトを生成する

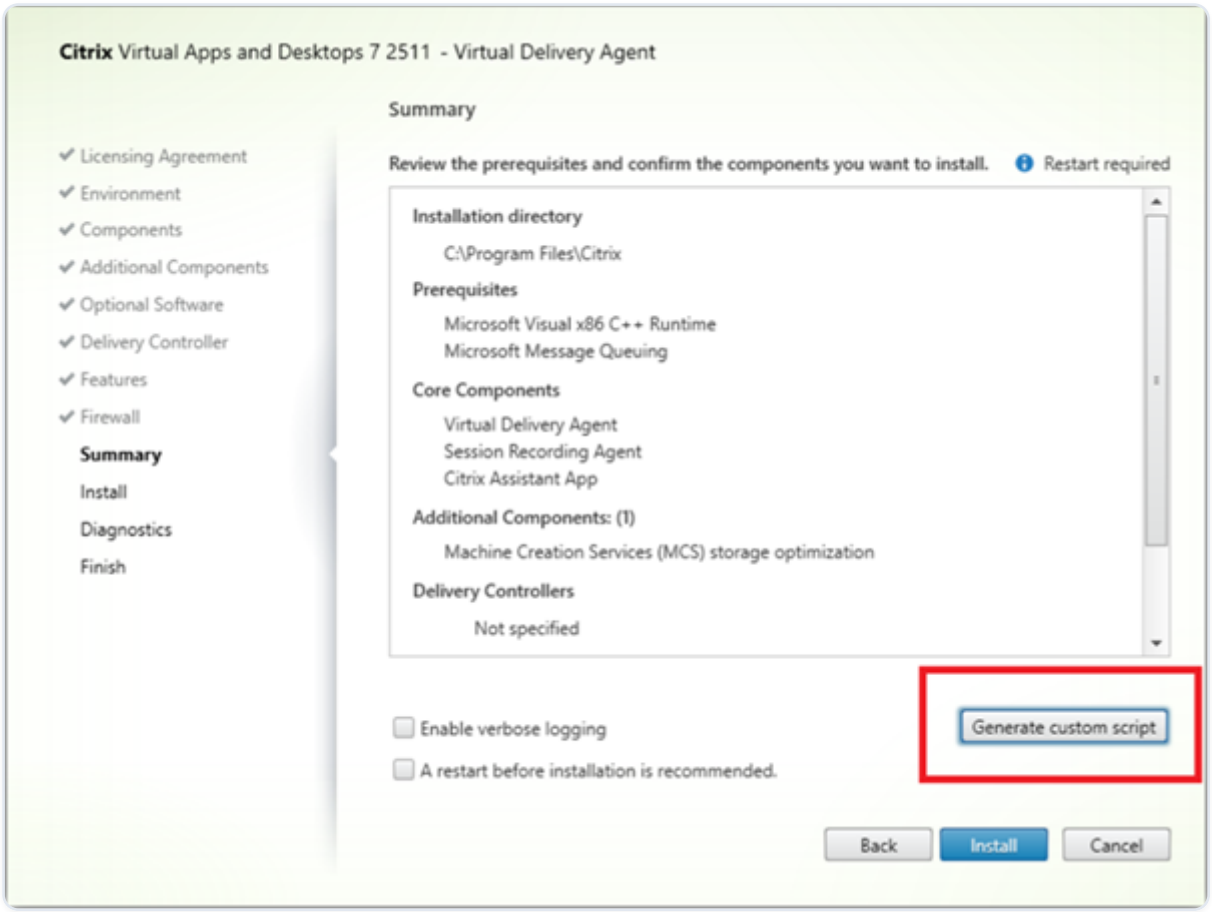
「**カスタムスクリプトの生成**」ボタンを使用すると、VDAインストールUIで行われた構成選択に基づいてバッチまたはスクリプトを作成できます。生成されたスクリプトはエクスポートして、コマンドラインから無人インストールまたはアップグレードを実行するために使用できます。この機能は、展開の自動化、構成の正確性の確保、手動スクリプトエラーの削減に役立ちます。

VDAインストールUIからコマンドラインスクリプトを生成するには、以下の手順を使用します。

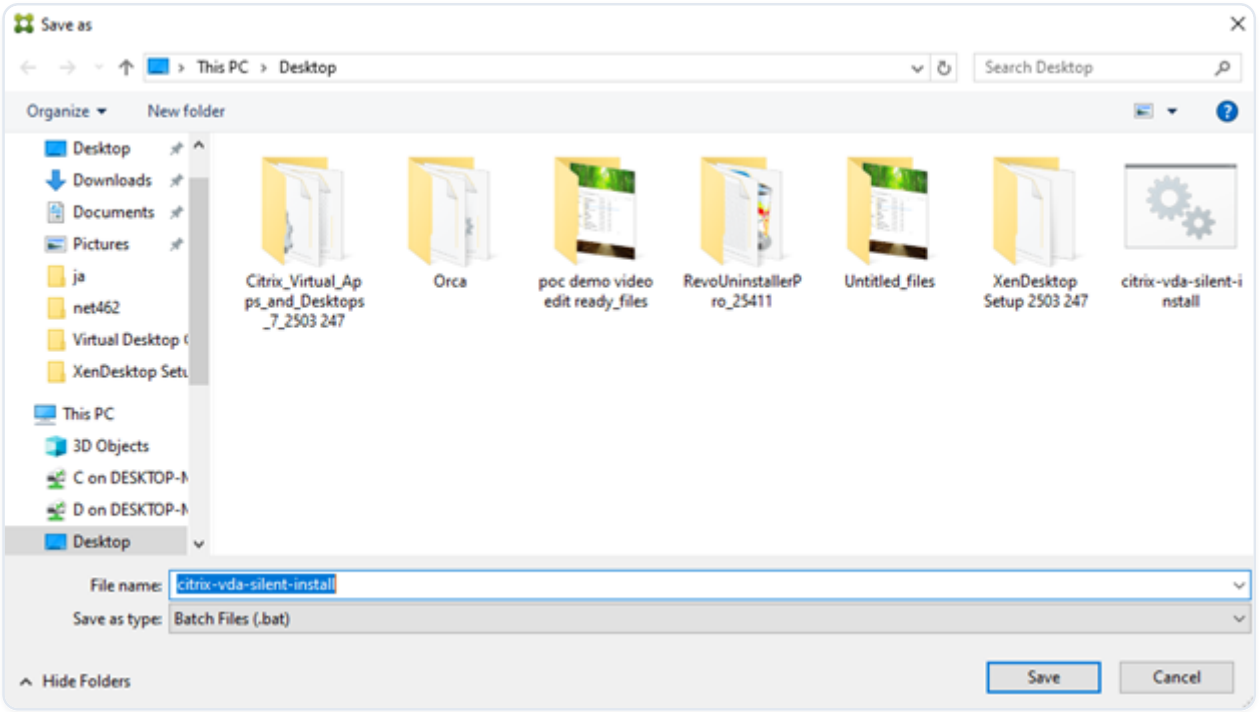
ステップ1：インストーラーUIからカスタムスクリプトを生成する

> **注:**
>
> この機能はUIモードでのみサポートされています。

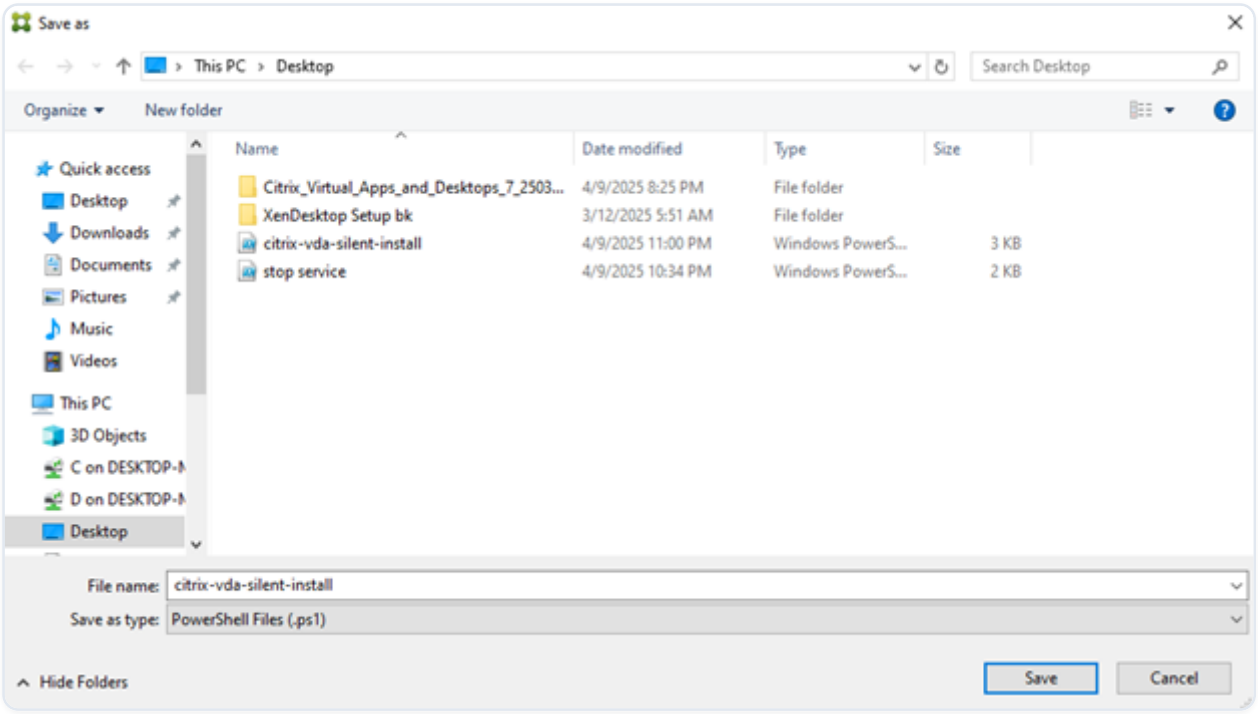
通常どおりUIでVDAインストールオプションを構成します。「**概要**」ページで、「**カスタムスクリプトの生成**」を選択して、以下のスクリーンショットに示すように、構成に基づいてコマンドラインスクリプトを作成します。



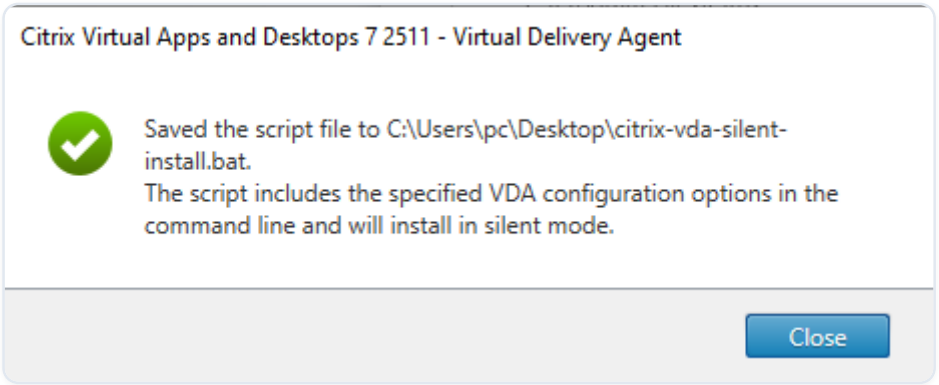
生成されたスクリプトを保存する場所を選択するよう促すダイアログボックスが表示されます。保存する前に、別のディレクトリを選択してスクリプトの名前を変更することもできます。



デフォルトでは、スクリプトはバッチ (.bat) ファイルとして保存されます。PowerShell (.ps1) スクリプトとして保存することもできます。

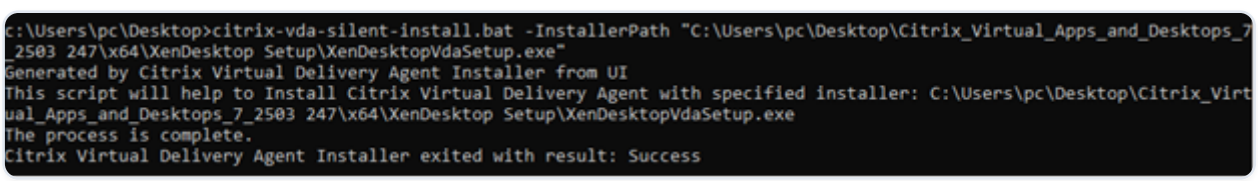


スクリプトが生成されて保存されると、ファイルの場所とスクリプトの目的を説明する確認ダイアログが表示されます。生成されたスクリプトは、メモ帳などの任意のテキストエディターを使用して編集できます。スクリプトを実行する前に、インストーラーUIを終了してください。VDAのインストールまたはアップグレードプロセスは一度に1つしか実行できません。

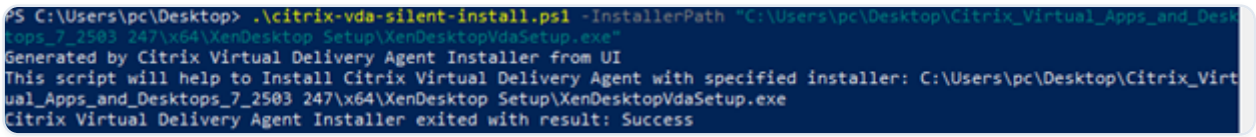


ステップ2. 生成されたスクリプトを使用してVDAをインストールまたはアップグレードする

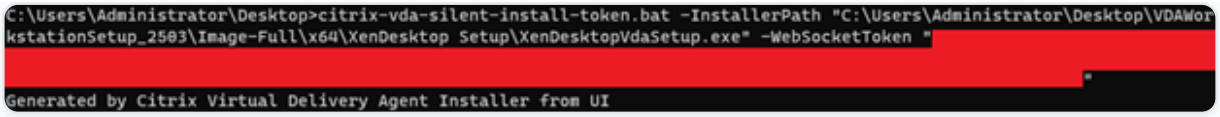
次のスクリーンショットは、生成されたバッチファイルを使用してVDAをインストールまたはアップグレードする方法を示しています。唯一の必須パラメーターは、VDAインストーラーへのパスです。インストーラーパスが有効な場合、スクリプトはインストールまたはアップグレードを実行し、VDAインストーラーと同じ終了コードで終了します。プロセスの結果を示す読みやすい結果メッセージが表示されます。



次のスクリーンショットは、生成されたPowerShellスクリプトを使用してVDAをインストールまたはアップグレードする方法を示しています。唯一の必須パラメーターは、VDAインストーラーへのパスです。インストーラーのパスが有効な場合、スクリプトはインストールまたはアップグレードを実行し、VDAインストーラーと同じ終了コードで終了します。プロセスの結果を示す読み取り可能なステータスメッセージが表示されます。



> **注:**
>
> Delivery Controllerが登録トークンで構成されている場合、次のスクリーンショットに示すようにスクリプトを実行します。



スクリプトには次のパラメーターが必要です: `<Path-to-generated-script>`, `<Path-to-vda-installer>`, `<Websocket-token-value>`。

サードパーティ製VDAの展開方法

Microsoft System Center Configuration Manager (SCCM) や、Ansible、Microsoft Intune などの類似のソフトウェア配布ツールを使用して Virtual Delivery Agent (VDA) を正常に展開するには、Citrix® はVDAインストーラーを段階的に使用することをお勧めします。

> **注:**
>
> 以下の記事では、Citrix が環境をテストした方法に基づいた推奨事項のみを説明しています。これらの手順は、お客様のニーズに合わせてカスタマイズできます。Citrix は、お客様のニーズに合わせてこれに必要な更新や調整について責任を負いません。

- SCCM を使用した VDA のインストール
- Ansible を使用した VDA のインストール
- Microsoft Intune を使用した VDA のインストール

SCCM を使用した VDA のインストール

概要

Microsoft Endpoint Configuration Manager (旧称 System Center Configuration Manager (SCCM)) は、企業全体のデバイスとアプリケーションの管理、展開、およびセキュリティを可能にする Windows 製品です。

> **注:**
>
> 以下の記事では、Citrix® が環境をテストした方法に基づいた推奨事項のみを説明しています。これらの手順は、必要に応じてカスタマイズできます。Citrix は、顧客のニーズに合わせてこれに必要な更新や調整について責任を負いません。

推奨事項

- SCCM または類似のソフトウェア配布ツールを使用して Virtual Delivery Agent (VDA) を正常に展開するには、Citrix は、一連の手順で VDA インストーラーを使用することを推奨します。
- Citrix は、VDA のインストールまたはアップグレードの一部として VDA Cleanup Utility を使用することを推奨しません。VDA インストーラーが以前に失敗した場合にのみ、VDA Cleanup Utility を使用してください。

始める前に

VDA のインストール中に必要な再起動の回数は、環境によって異なります。例:

- 保留中の更新や以前のソフトウェアインストールからの再起動のために、再起動が必要になる場合があります。
- 他のプロセスによって以前にロックされていたファイルは更新が必要になる場合があり、追加の再起動を強制します。
- VDA インストーラーの一部のオプションコンポーネント (Citrix Profile Management や Citrix Files など) は、再起動が必要になる場合があります。
- VDA をアップグレードする場合、インストールされているマシンは、セッションがない状態でメンテナンスモードになっている必要があります。
- マシンで VDA のインストールが初めて実行されると、使用されている VDA インストーラーはそのマシンにコピーされます。 VDA のインストールに関する詳細については、インストーラーを参照してください。

SCCM タスクシーケンサーは、必要なすべての再起動を管理します。

SCCM を使用して VDA を展開するための主要な手順

以下の手順では、仮想マシンに SCCM を使用して VDA を展開する方法について説明します。

1. VDA をインストールする。
2. 組織単位 (OU) を作成する。
3. マシンを検証する。
4. VDA を使用してコンテンツを配布する。

ステップ 1: VDA をインストールする

すべての前提条件を特定した後、**SCCM タスク シーケンサー**を使用して次のタスクを完了します。

1. インストールメディアのアクセス可能なコピーから、またはVDAスタンドアロンインストーラーのいずれかからVDAをインストールします。

   - `VDAWorkstationSetup_XXXX.exe`
   - `VDAServerSetup_XXXX.exe`
   - `VDAWorkstationCoreSetup_XXXX.exe`

   VDAインストーラーの詳細については、「インストーラー」を参照してください。

   > **注:**
   >
   > VDAをアップグレードする場合、VDAがインストールされているマシンは、セッションがないメンテナンスモードである必要があります。

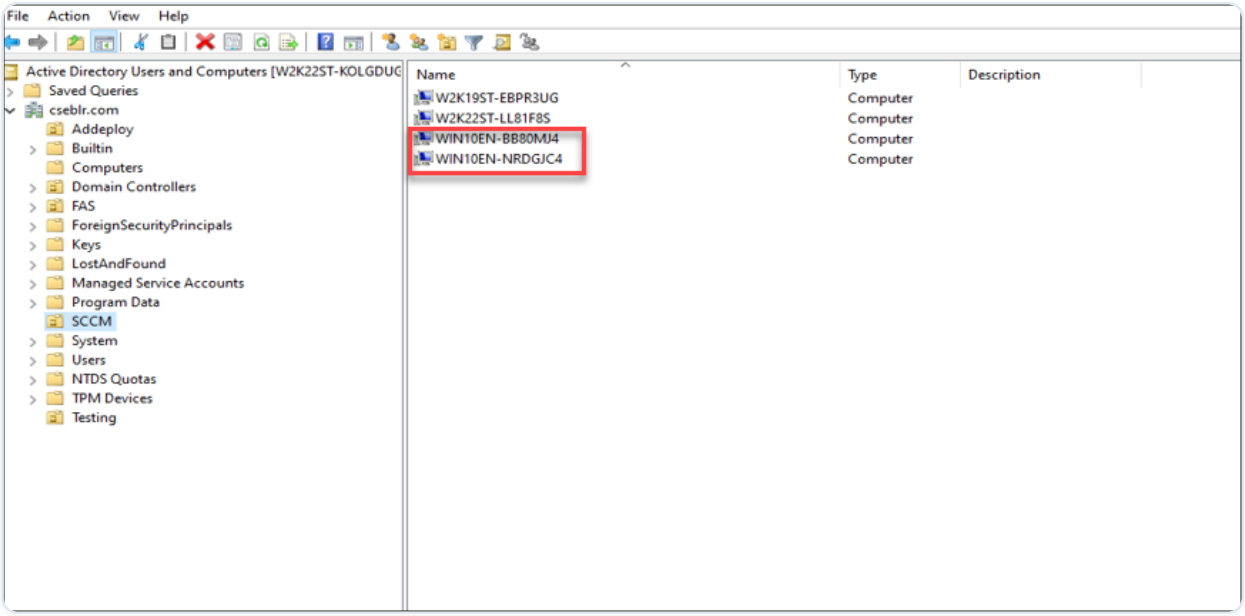
2. マシンでVDAのインストールが初めて実行されると、使用されているVDAインストーラーがそのマシンにコピーされます。

   - `VDAWorkstationCoreSetup_XXXX.exe`以外のVDAインストーラーを使用すると、VDAインストーラーは`%ProgramData%\Citrix\XenDesktopSetup\XenDesktopVdaSetup.exe`にコピーされます。
   - `VDAWorkstationCoreSetup_XXXX.exe`を使用すると、VDAインストーラーは`%ProgramData%\Citrix\XenDesktopSetup\XenDesktopRemotePCSetup.exe.`にコピーされます。

3. VDAインストーラーのディレクトリの場所は、レジストリ `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaInstall"` `"MetaInstallerInstallLocation"` にも保存されます。
4. コマンドラインオプションに `/NOREBOOT`、`/NORESUME`、および `/QUIET` を追加します。
   - `/QUIET`: インストール中にユーザーインターフェイスを表示しないようにします。これにより、SCCMがインストールプロセスを制御できます。
   - `/NOREBOOT`: VDAインストーラーが自動的に再起動するのを抑制します。SCCMは必要に応じて再起動をトリガーします。
   - `/NORESUME`: 通常、インストール中に再起動が必要な場合、VDAインストーラーはrunonceレジストリキー（`\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce`）を設定します。Windowsは、マシンが再起動したときにこのキーを使用してVDAインストーラーを開きます。SCCMはインストールを監視して終了コードをキャプチャできないため、これはSCCMにとって問題となります。

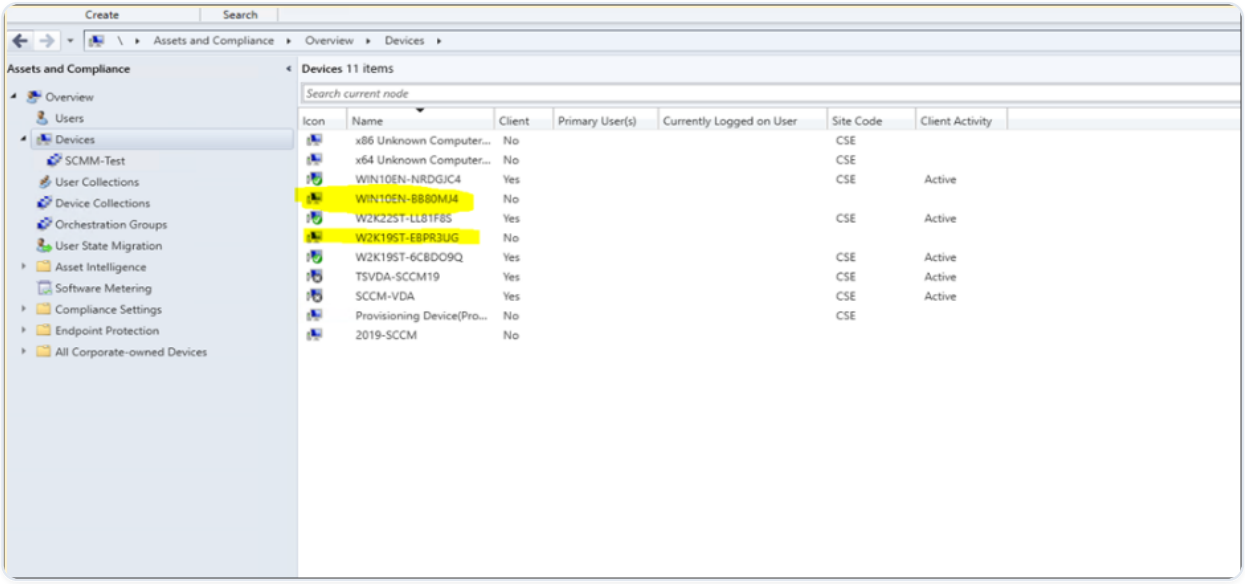
ステップ2: 組織単位 (OU) を作成する

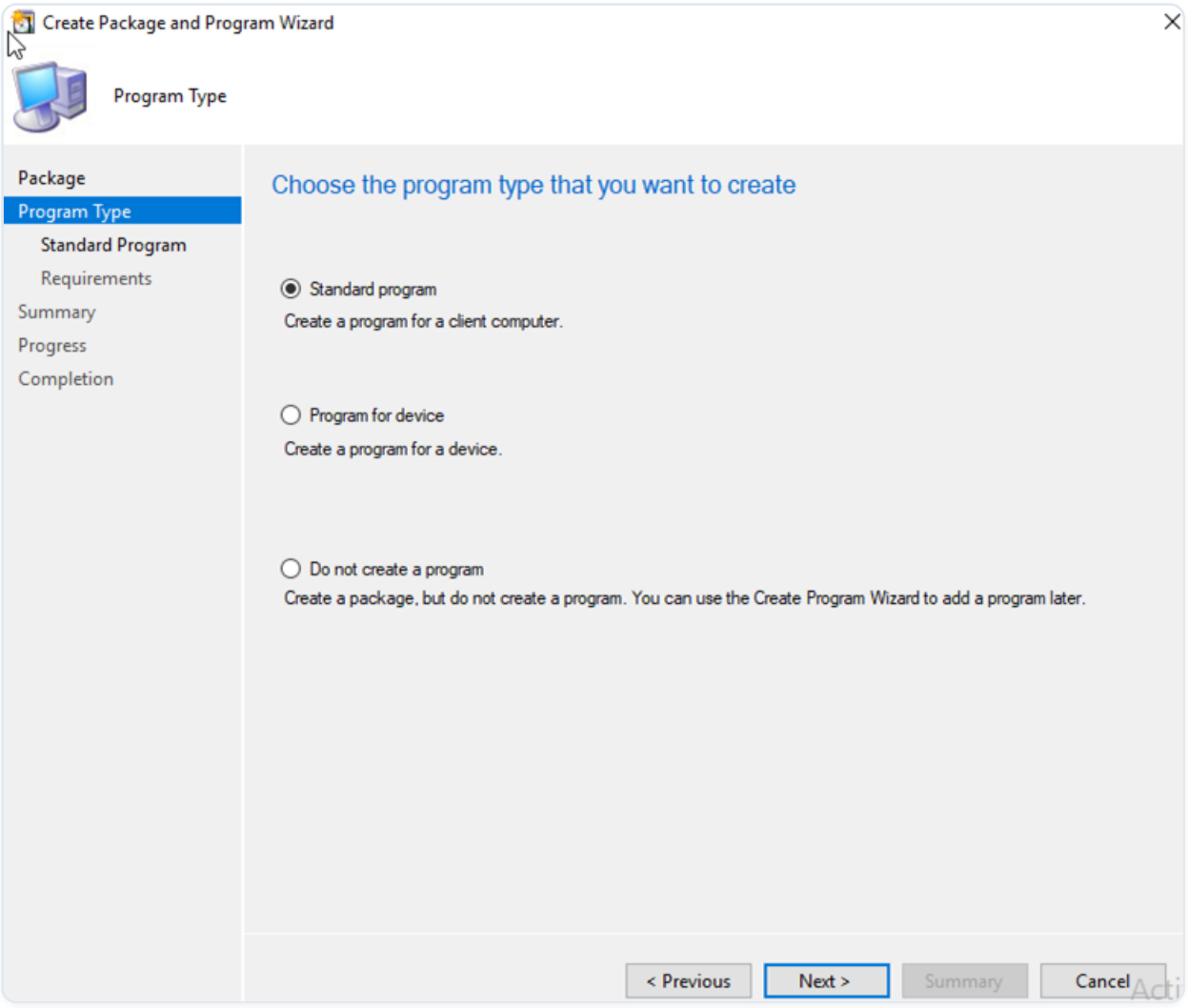
1. OU に追加するドメイン参加済み仮想マシンを 2 台作成します。仮想マシンが最初に作成されると、**Computers** フォルダーにあります。仮想マシンを **SCCM** フォルダーに移動します。
   例: WIN10EN-BB80MJ4.cseblr.com W2K19ST-EBPR3UG.cseblr.com



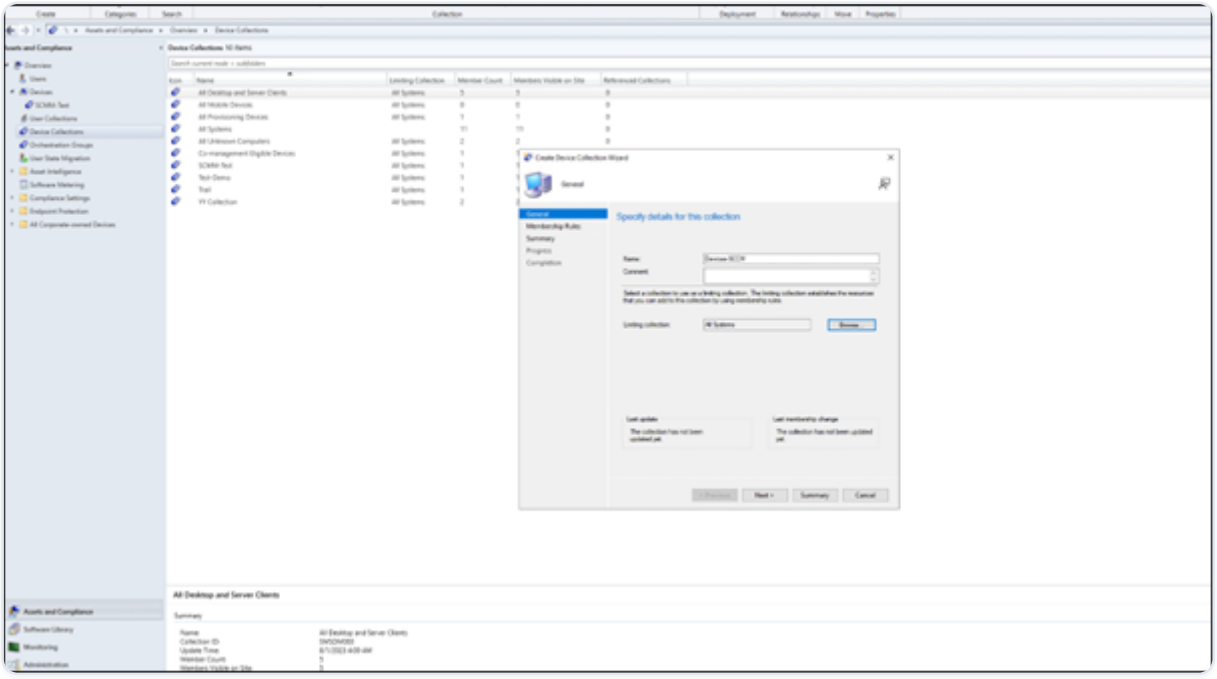
2. Microsoft Configuration Manager で、`\Administration\Overview\Hierarchy Configuration\Discovery Methods\` に移動します。
3. **Active Directory システム検出**をクリックし、**Active Directory システム検出を有効にする**チェックボックスを選択して、新しく作成された仮想マシンの自動検出を有効にします。

4.  アイコンをクリックして、新しいコンテナーを選択します。
5. **場所**セクションで、SCCM 仮想マシンが配置されている**パス**を追加します。
6. `\Administration\Overview\Site Configuration\Sites` に移動し、SCCM VDA を右クリックします。
7. **クライアントインストール設定 > クライアントプッシュインストール**を選択します。**クライアントプッシュインストールのプロパティ**ウィンドウが開きます。
8. VM が `Enabled` に設定されると、以下の画像に示すように VM のリストが表示されます。





9. OU を作成するために**デバイスコレクション**を作成します。コレクション名の**名前**を入力します。



10. ウィザードの指示に従います。

メンバーシップルール(/en-us/citrix-virtual-apps-desktops/current-release/media/sccm-membership-rules.png)

OUが作成されます。

OUの作成(/en-us/citrix-virtual-apps-desktops/current-release/media/sccm-create-device-collection-wizard.png)

11. 作成したVMを、新しく作成したデバイスコレクションに追加します。

    a. VMを右クリックします。「**選択した項目を追加 > 既存のデバイスコレクションに選択した項目を追加**」を選択します。

       項目の追加(/en-us/citrix-virtual-apps-desktops/current-release/media/sccm-add-item-to-device-collection.png)

    b. 「**コレクションの選択**」ウィンドウで、必要なデバイス名を選択します。この例では、`Devices-SCCM`です。

       デバイスリスト(/en-us/citrix-virtual-apps-desktops/current-release/media/sccm-list.png)

    `Devices-SCCM`は、「**資産とコンプライアンス > 概要 > デバイスコレクション**」に表示されます。

    デバイスがリスト表示されました(/en-us/citrix-virtual-apps-desktops/current-release/media/devices-sccm.png)

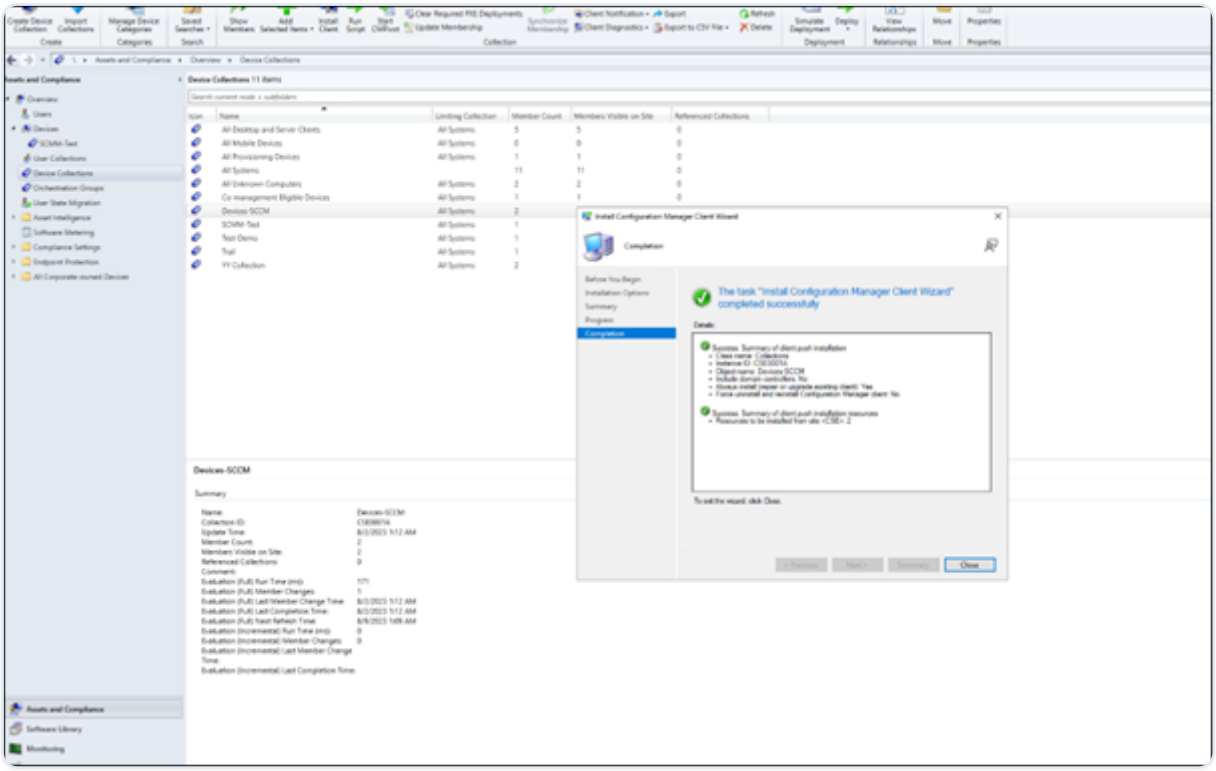
12. デバイスコレクターで「**クライアントのインストール**」を選択します。

    クライアントのインストール(/en-us/citrix-virtual-apps-desktops/current-release/media/sccm-install-client.png)

13. 必要なインストール「**サイト**」を選択します。

    サイトのインストール(/en-us/citrix-virtual-apps-desktops/current-release/media/sccm-install-client-1.png)

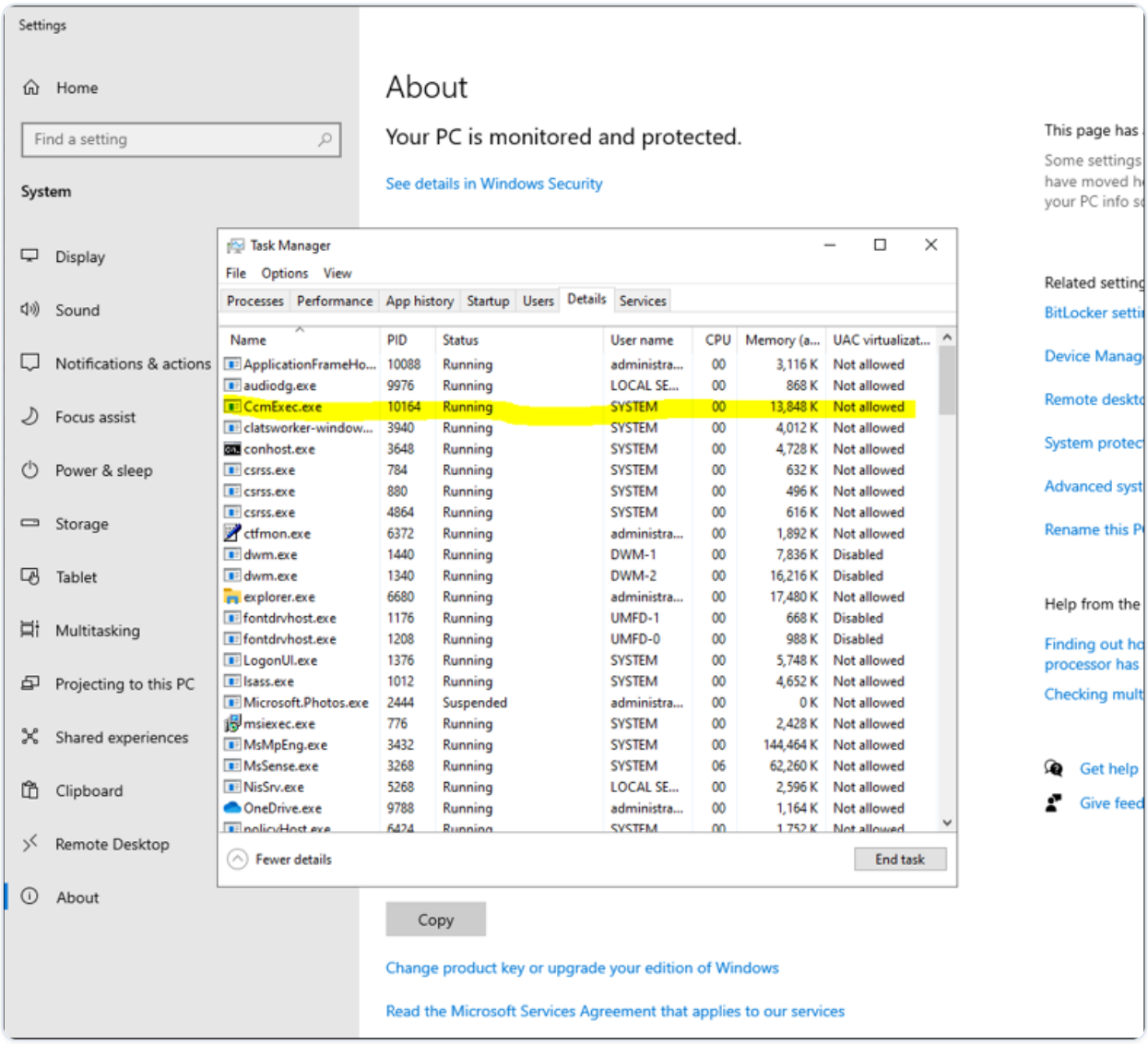
14. ウィザードの指示に従います。**Install Configuration Manager Client Wizard** が正常に完了しました。



詳細については、Microsoft ドキュメントの コレクションの管理 を参照してください。

ステップ 3: マシンの検証

1. クライアントマシンで、`CCMExec` プロセスが実行されていることを確認して、クライアントがインストールされていることを検証します。



2. SCCM 上の VM でクライアントが実行されていることを確認します。

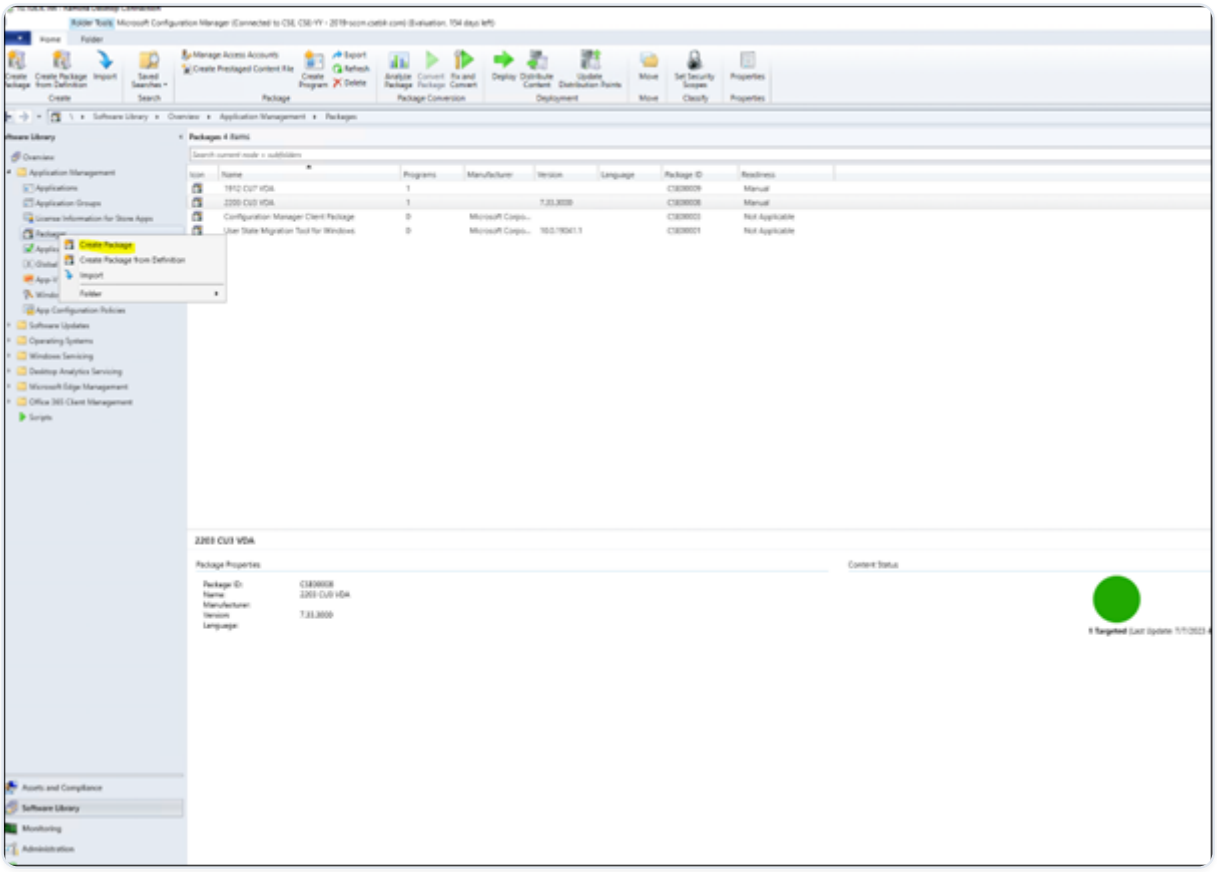
ステップ 4: VDA を使用してコンテンツを配布する

次の手順では、展開された VDA を使用して、関連付けられた仮想マシンにコンテンツを配布する方法について説明します。

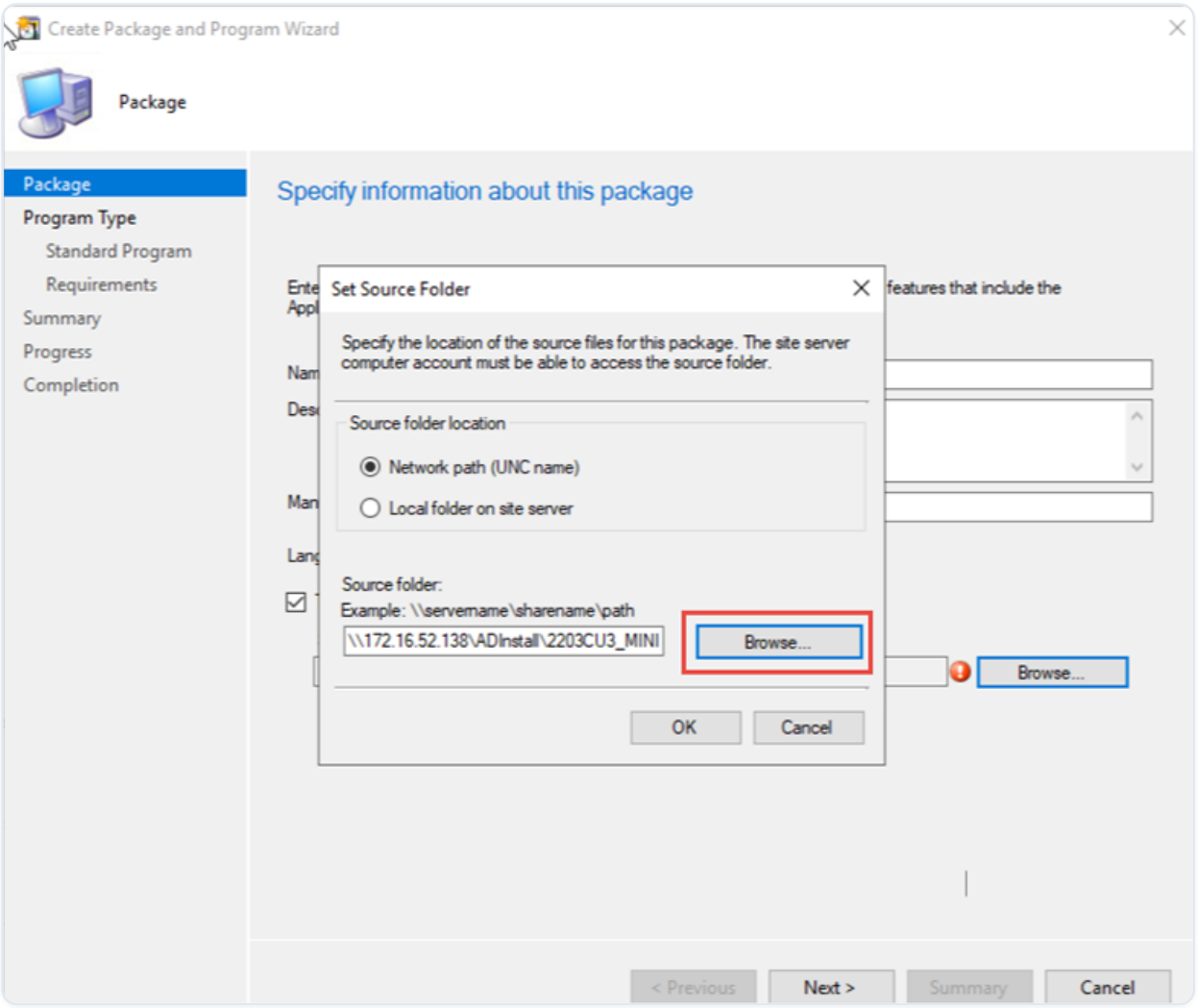
1. パッケージの作成
2. コンテンツの配布

パッケージの作成

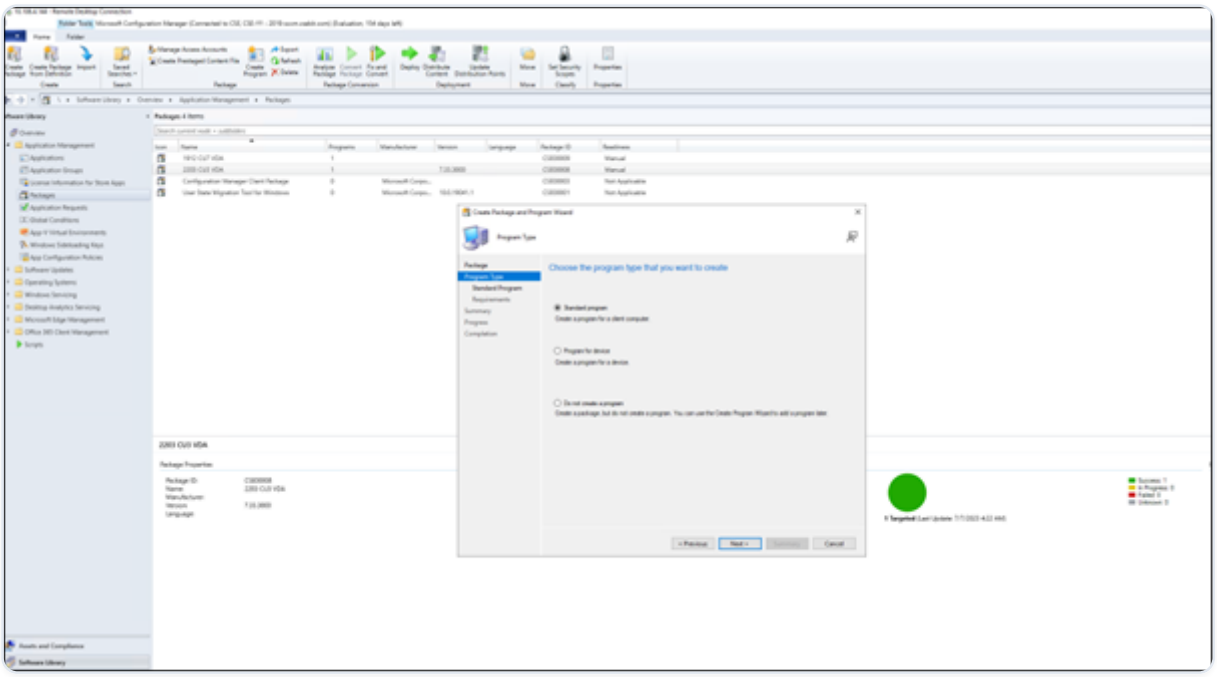
1. パッケージを作成するには、目的の VDA を右クリックし、 をクリックします。



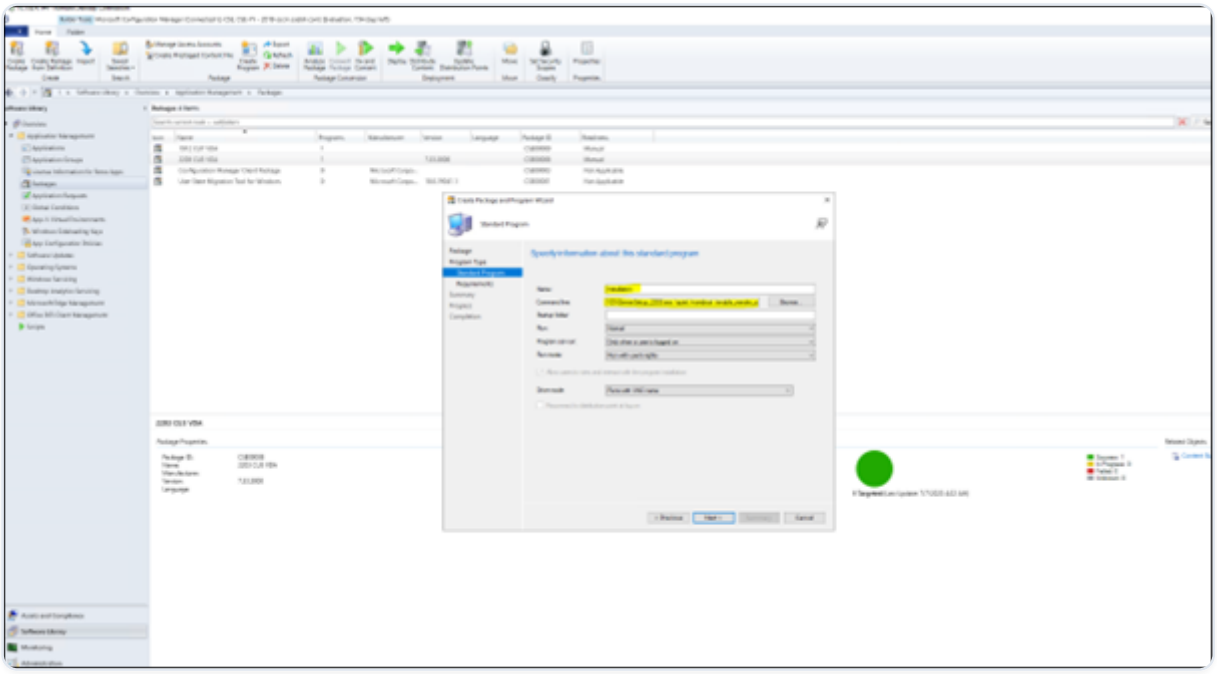
2. をクリックして、このパッケージのソースファイルの場所を指定します。



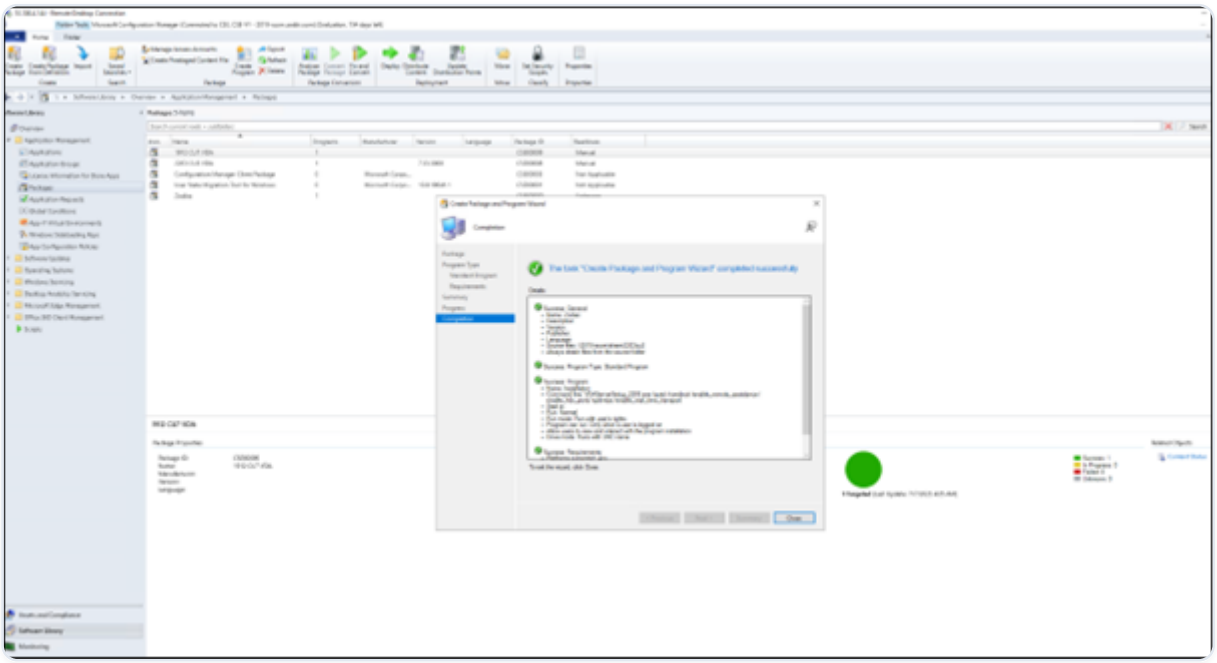
3. 必要なパッケージの種類を選択します。



4. パッケージの**名前**と**コマンドライン**を入力します。



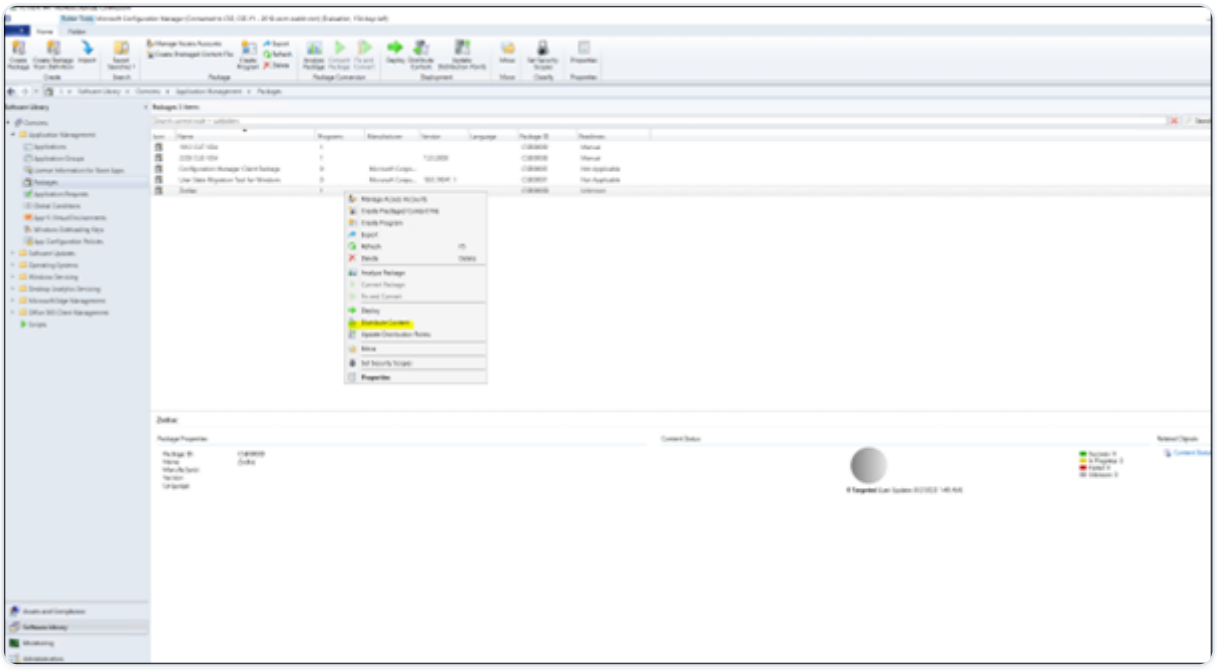
5. **Next**をクリックします。



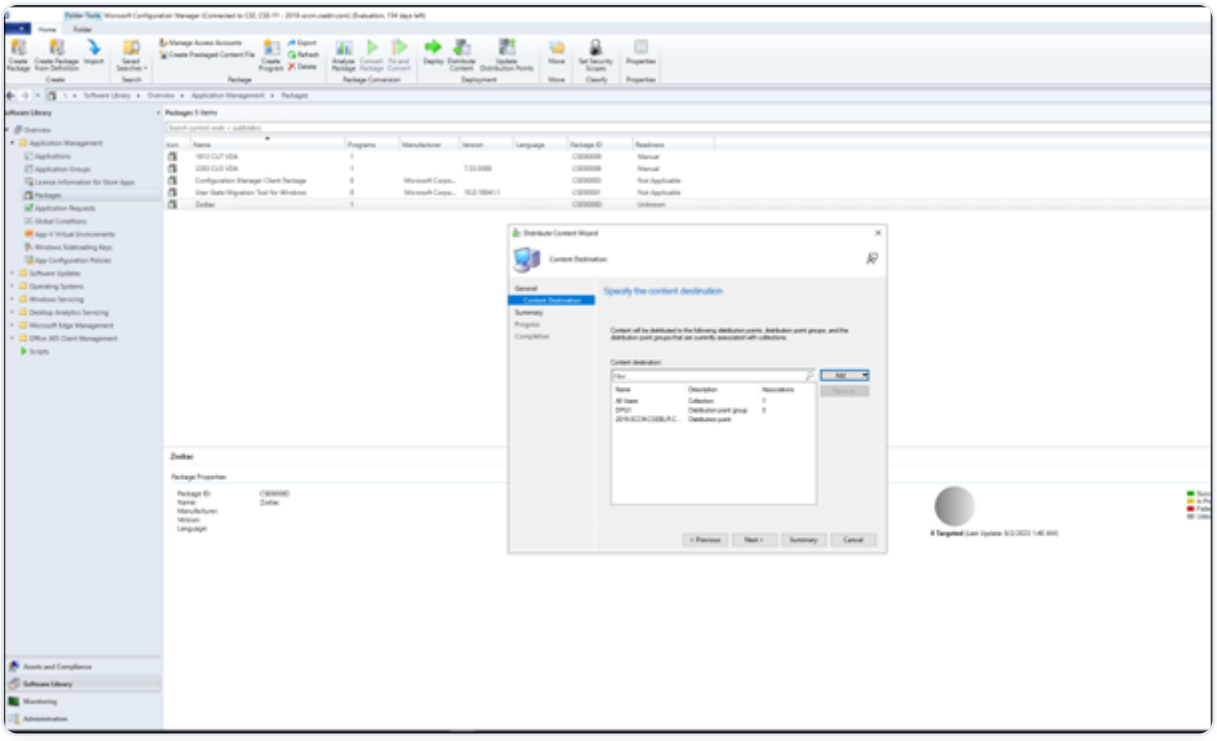
詳細については、Microsoft ドキュメントのConfiguration Manager のパッケージとプログラムを参照してください。

コンテンツの配布

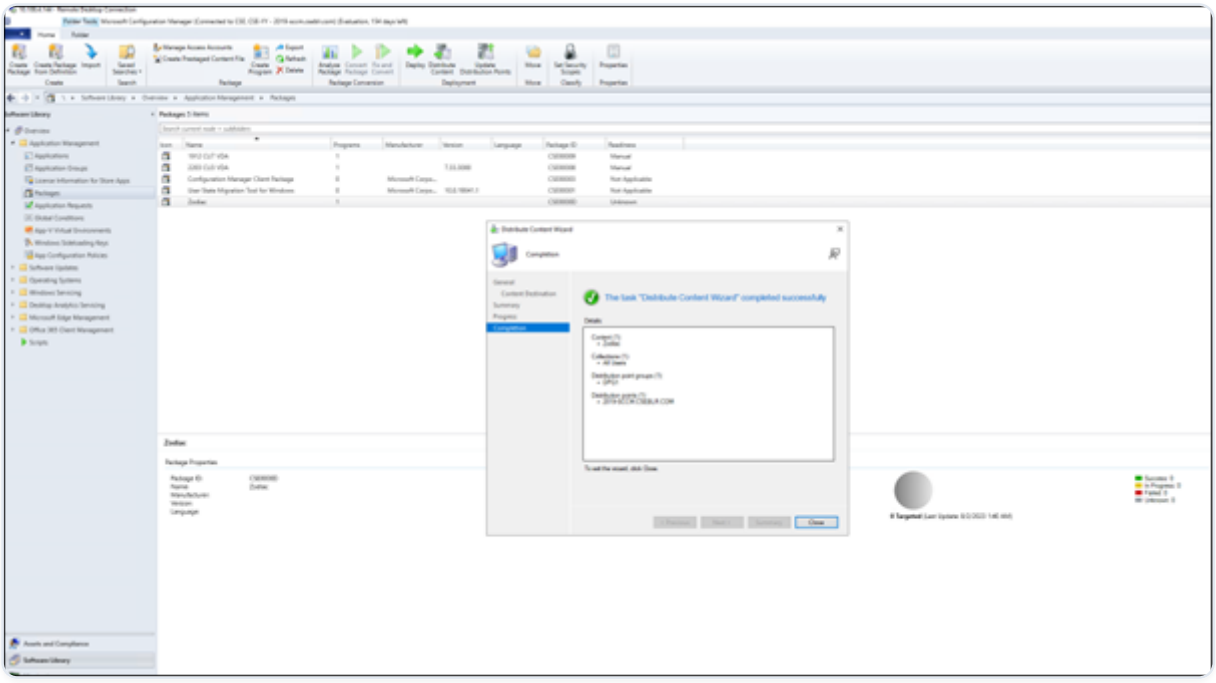
1. 作成したパッケージ名を右クリックします。
2. **コンテンツの配布**を選択します。



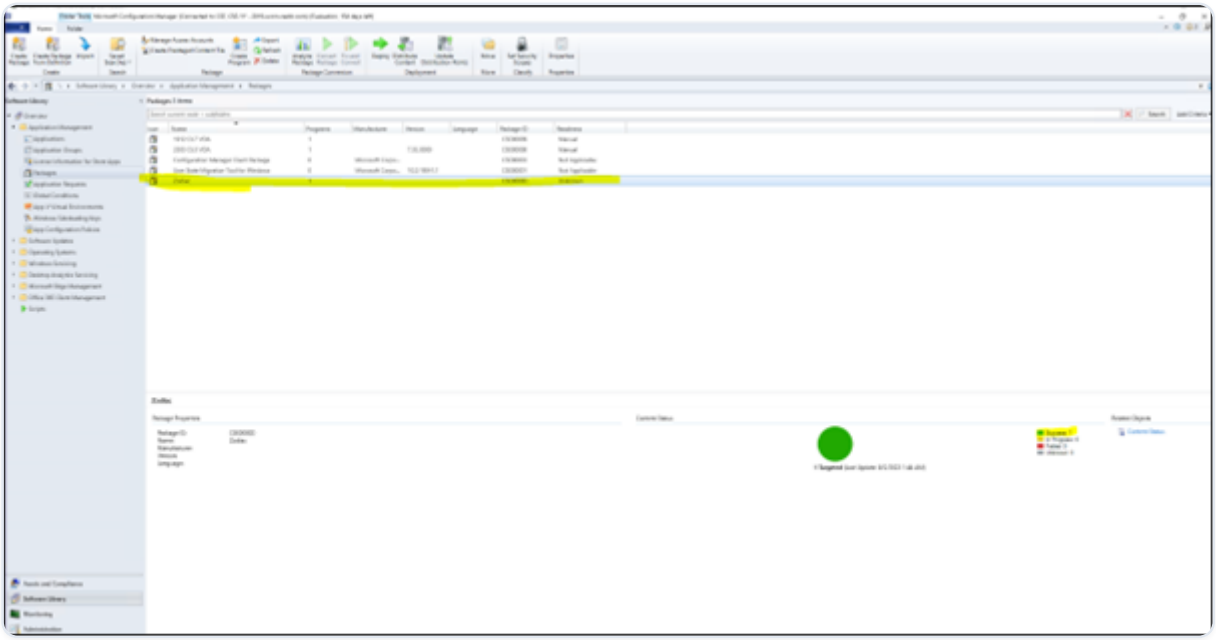
3. **コンテンツの配布ウィザード**ウィンドウで、作成したパッケージのソースファイルの場所を選択します。この例では、`2019-SCCM`です。**次へ**をクリックします。



4. パッケージ (この例では、`Zodiac`) が展開可能であることを確認します。



以下の画像は、パッケージが展開可能であることを示しています。

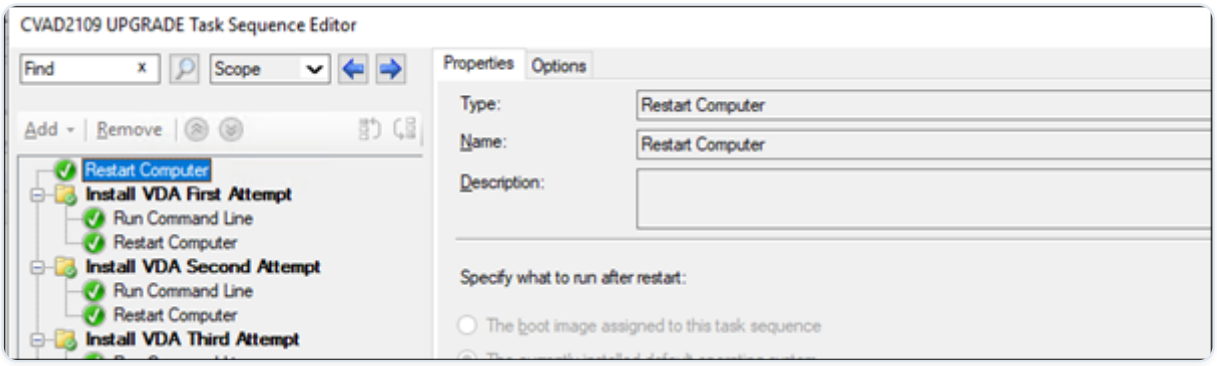


詳細については、Microsoft ドキュメントの「Configuration Manager のコンテンツの展開と管理」を参照してください。

SCCM を使用したインストールシーケンスの例

次の例は、インストールシーケンスを示しています。

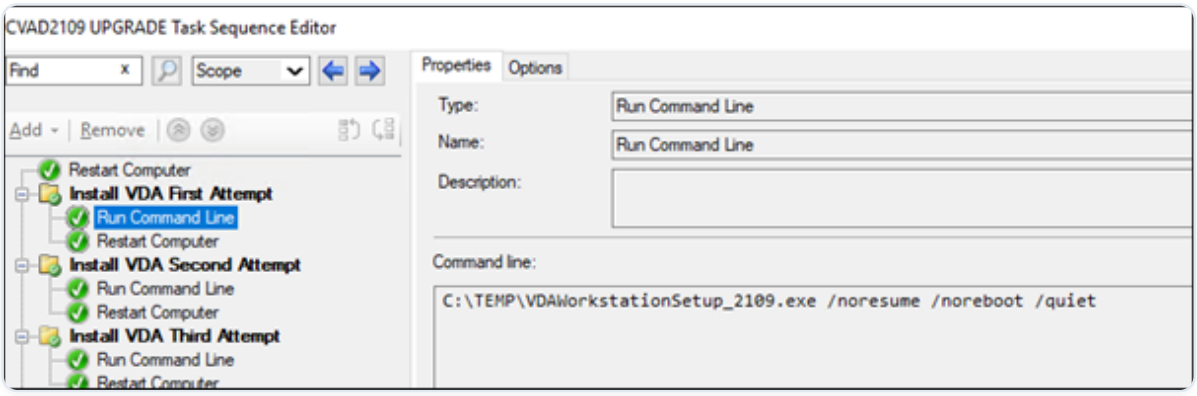
1. **コンピューターの再起動:** マシンを再起動して準備します。



2. **VDA のインストール (初回試行):** VDA のインストールを開始します。

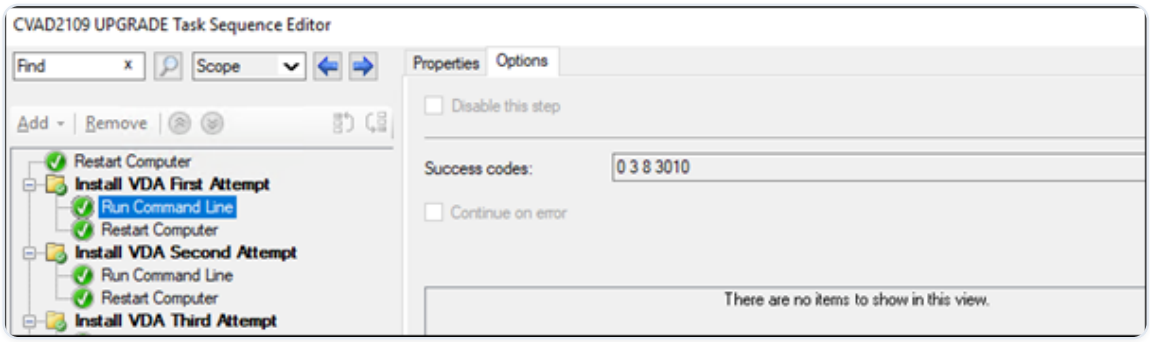
   a. コマンドラインオプションに `/quiet`、`/noreboot`、および `/noresume` オプションを追加します。

   b. 選択した VDA インストーラー (ローカルイメージまたは最小インストーラーのいずれか) を実行します。

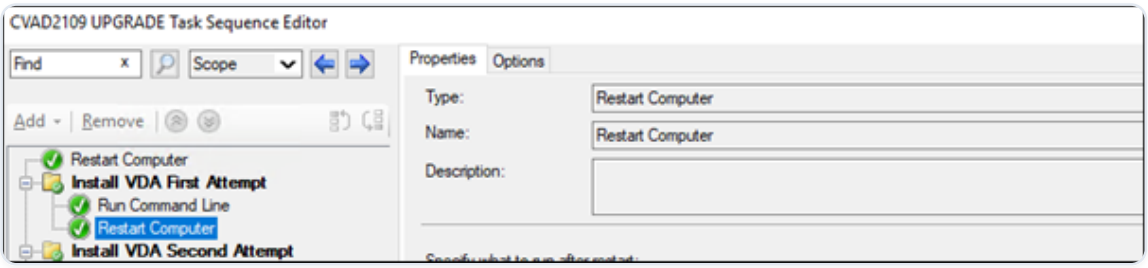


   c. SCCM はリターンコードをキャプチャする必要があります。

   - リターンコードが 0 または 8 の場合、インストールは完了しており、再起動が必要です。



   - リターンコードが 3 の場合は、マシンを再起動してから、**VDA のインストール (2 回目の試行)** に制御を渡します。



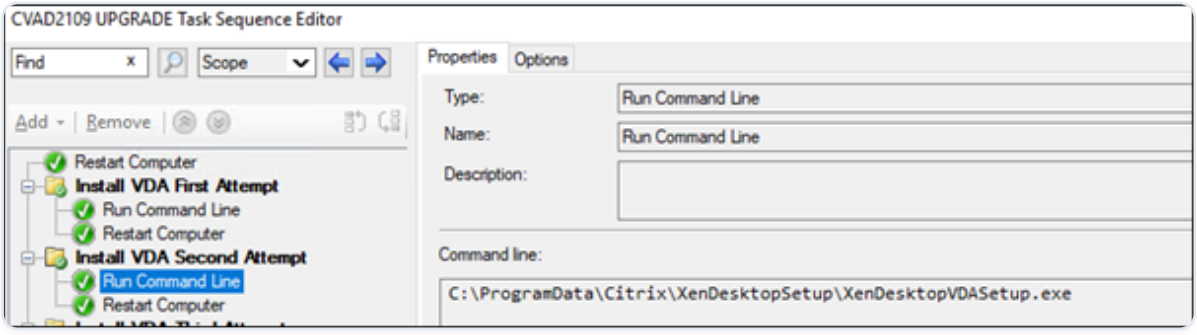
3. **VDAの2回目のインストール:** VDAのインストールを続行します。

   a. **VDAの1回目のインストール**の後、ファイル `%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml` が存在する場合、インストールは完了しておらず、再起動が完了した後に続行する必要があります。



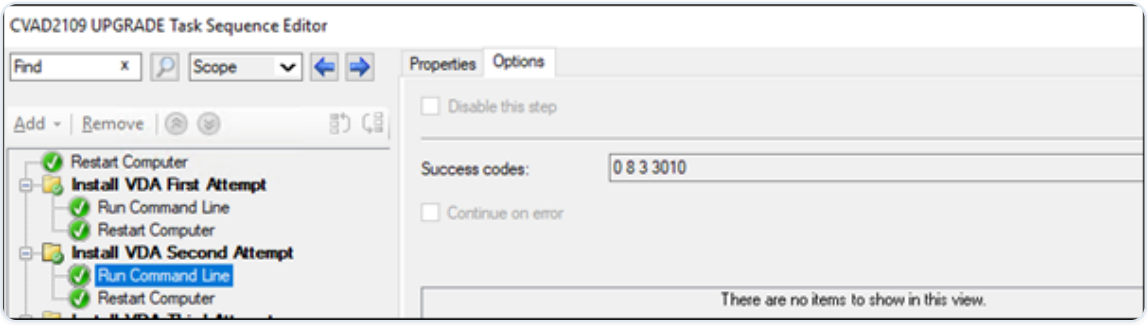
   b. **VDAの2回目のインストール**は、ファイル `%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml` が存在しなくなるか、0または8以外のリターンコードが返されるまで繰り返されます。その他のリターンコードはエラーとして扱い、VDAの2回目のインストールはエラーを報告して停止する必要があります。

   c. 適切なVDAインストーラー（ほとんどの場合 `XenDesktopVdaSetup.exe`、または `VDAWorkstationCoreSetup_XXXX.exe` が使用された場合は `XenDesktopRemotePCSetup.exe`）を、コマンドラインパラメーターなしでファイル `%programdata%\ Citrix\XenDesktopSetup\` ディレクトリから実行して、VDAのインストールを再開します。（VDAインストーラーは、インストーラーの初回実行時に保存されたパラメーターを使用します。）



d. VDAインストーラーからのリターンコードを確認します。

- 0または8：成功、インストール完了、再起動が必要です。



- 3：インストールは完了していません。マシンを再起動し、ファイル `%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml` が存在しなくなるか、0または8が返されるまでVDAの2回目のインストールを繰り返します。その他のリターンコードはエラーとして扱い、VDAの2回目のインストールはエラーを報告して終了する必要があります。

リターンコードの詳細については、Citrixインストールリターンコードを参照してください。

VDAインストールコマンドの例

利用可能なインストールオプションは、使用するインストーラーによって異なります。コマンドラインオプションの詳細については、以下の記事を参照してください。

- VDAのインストール
- コマンドラインを使用したインストール

REMOTE PC ACCESS のインストールコマンド

- 次のコマンドは、シングルセッションコア VDA インストーラー（`VDAWorkstationCoreSetup.exe`）を使用します。

  ```
  VDAWorkstationCoreSetup.exe /quiet /controllers “control.domain.com” /enable_hdx_ports /noresume /noreboot
  ```

- 次のコマンドは、シングルセッションフル VDA インストーラー（`VDAWorkstationSetup.exe`）を使用します。

  ```
  VDAWorkstationSetup.exe /quiet /remotepc /physicalmachine /controllers “control.domain.com” /enable_hdx_ports /noresume /noreboot
  ```

専用 VDI のインストールコマンド

- 次のコマンドは、シングルセッションフル VDA インストーラー（`VDAWorkstationSetup.exe`）を使用します。

  ```
  VDAWorkstationSetup.exe /quiet /components vda /controllers “control.domain.com” /enable_hdx_ports /enable_remote_assistance /noresume /noreboot
  ```

Ansible を使用した VDA のインストール

概要

この記事では、Ansible を使用して VDA を展開する方法について説明します。詳細については、Ansible ドキュメントを参照してください。

> **注:**
>
> この記事は、Citrix® が環境をテストした方法に基づいた推奨事項のみを説明しています。これらの手順は、お客様のニーズに合わせてカスタマイズできます。Citrix は、お客様のニーズに合わせて必要な更新や調整について責任を負いません。

Ansible を使用して VDA を展開するための主要な手順

1. 仮想マシン環境の構成。
2. Ansible のインストール
3. Kerberos の構成
   a. Kerberos のインストール
   b. Kerberos の構成
4. Ansible の構成

ステップ 1: 仮想マシン環境を構成する

Windows サーバーで次のコマンドを実行します。

1. PS RemoteSigned を設定します。 `Set-ExecutionPolicy RemoteSigned`
2. WinRM を暗号化なしで使用するように設定します。 `winrm set winrm/config/service '@{AllowUnencrypted="true"}'`

> **注:**
>
> このステップでエラーが発生した場合は、次のコマンドを使用します。 `Enable-PSRemoting -Force`

3. ファイアウォールポート5985を開きます。 `New-NetFirewallRule -DisplayName "Allow WinRm port 5985" -Direction Inbound -Profile Any -Action Allow -LocalPort 5985 -Protocol tcp`

ステップ2：ANSIBLEのインストール

Ubuntu 20.4以降でAnsibleをインストールするには、次のコマンドを実行します。

- `sudo apt update`
- `sudo apt install software-properties-common`
- `sudo add-apt-repository --yes --update ppa:ansible/ansible`
- `sudo apt install ansible`
- `sudo apt install python3-pip`

ステップ2I：KERBEROSのインストール

Kerberosをインストールするには、次のコマンドを実行します。

`sudo apt install python3-dev libkrb5-dev krb5-user`

ステップ2II：KERBEROSの構成

Kerberosを構成するには、次のコマンドを実行します。

`Edit /etc/krb5.conf`

```
[libdefaults]
        default_realm = [redacted]

# The following krb5.conf variables are only for MIT Kerberos.
        kdc_timesync = 1
        ccache_type = 4
        forwardable = true
        proxiable = true

# The following encryption type specification will be used by MIT Kerberos
# if uncommented.  In general, the defaults in the MIT Kerberos code are
# correct and overriding these specifications only serves to disable new
# encryption types as they are added, creating interoperability problems.
#
# The only time when you might need to uncomment these lines and change
# the enctypes is if you have local software that will break on ticket
# caches containing ticket encryption types it doesn't know about (such as
# old versions of Sun Java).

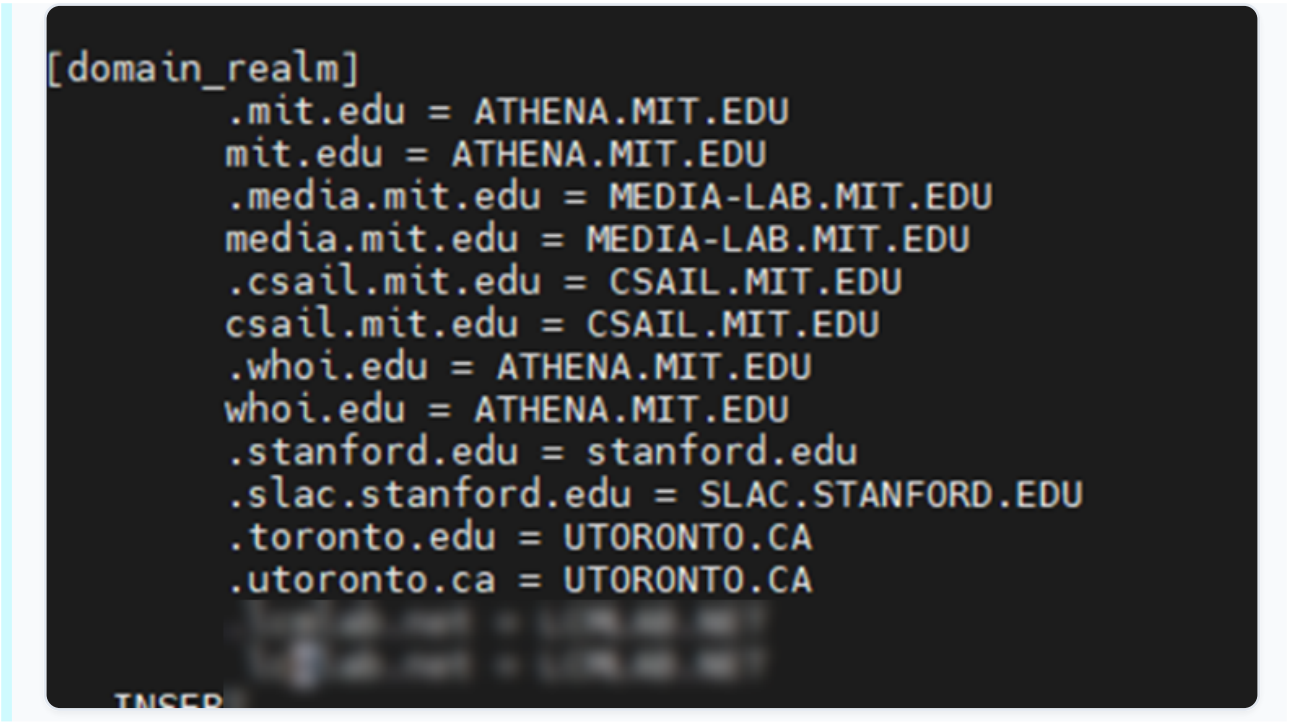
#       default_tgs_enctypes = des3-hmac-sha1
#       default_tkt_enctypes = des3-hmac-sha1
#       permitted_enctypes = des3-hmac-sha1

# The following libdefaults parameters are only for Heimdal Kerberos.
        fcc-mit-ticketflags = true

[realms]
        LTSRLAB.NET = {
                kdc = [redacted]
                admin_server = [redacted]
        }
        ATHENA.MIT.EDU = {
                kdc = [redacted]
```

注:

Kerberosレルム名には大文字を使用します。



ステップ3：ANSIBLEの構成

Ansibleホストを構成するには、次の手順を実行します。

1. 次のコマンドを実行します。

   `Edit /etc/ansible/hosts`

2. Delivery Controller `Install.yaml` ファイルを構成します

   `/QUIET /NOREBOOT /NORESUME /OPTIMIZE /VERBOSELOG /COMPONENTS VDA /CONTROLLERS 'MyDDC.xd.local' /ENABLE_HDX_PORTS /ENABLE_REAL_TIME_TRANSPORT`

   「デリバリーコントローラー」(/en-us/citrix-virtual-apps-desktops/current-release/media/delivery-controller-yaml-1.png)

   「デリバリーコントローラー」(/en-us/citrix-virtual-apps-desktops/current-release/media/delivery-controller-yaml-2.png)

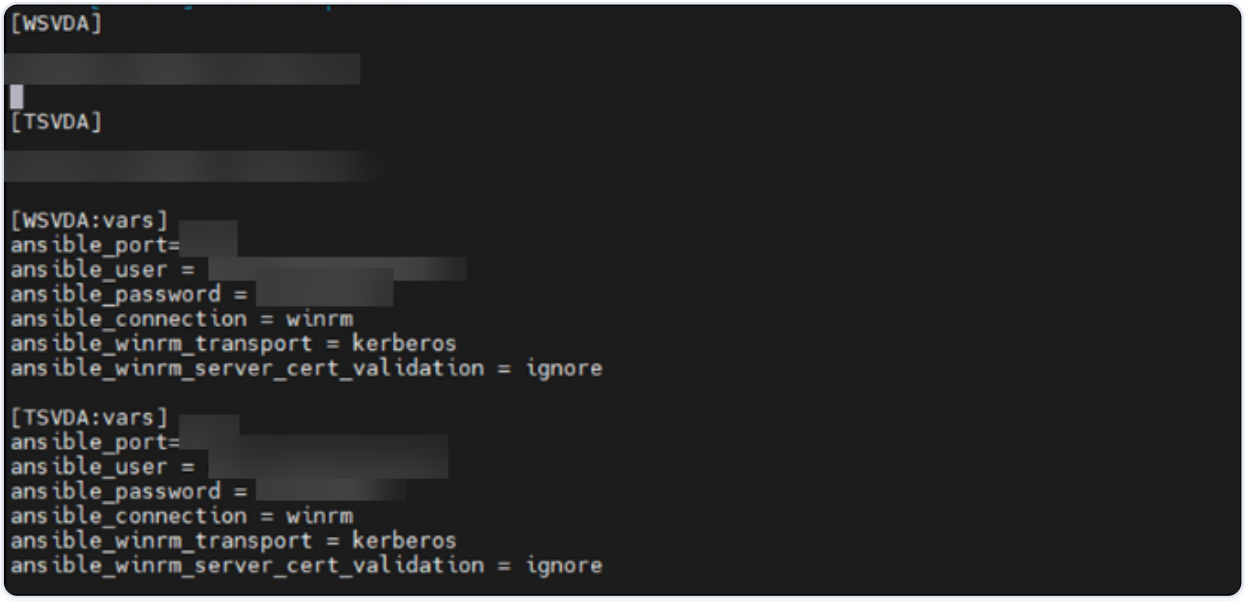
   「デリバリーコントローラー」(/en-us/citrix-virtual-apps-desktops/current-release/media/delivery-controller-yaml-3.png)

   「デリバリーコントローラー」(/en-us/citrix-virtual-apps-desktops/current-release/media/delivery-controller-yaml-4.png)

3. 以下のコマンドでyamlファイルを実行します。 `sudo ansible-playbook install.yml -vvv` (詳細モード)

4. 設定ファイルで、他の追加設定とともに複数のホストを構成できます。

`Edit /etc/ansible/hosts`



Microsoft Intune を使用した VDA のインストール

概要

この記事では、Microsoft Intune を使用して VDA を展開する方法について説明します。詳細については、Microsoft のドキュメントを参照してください。

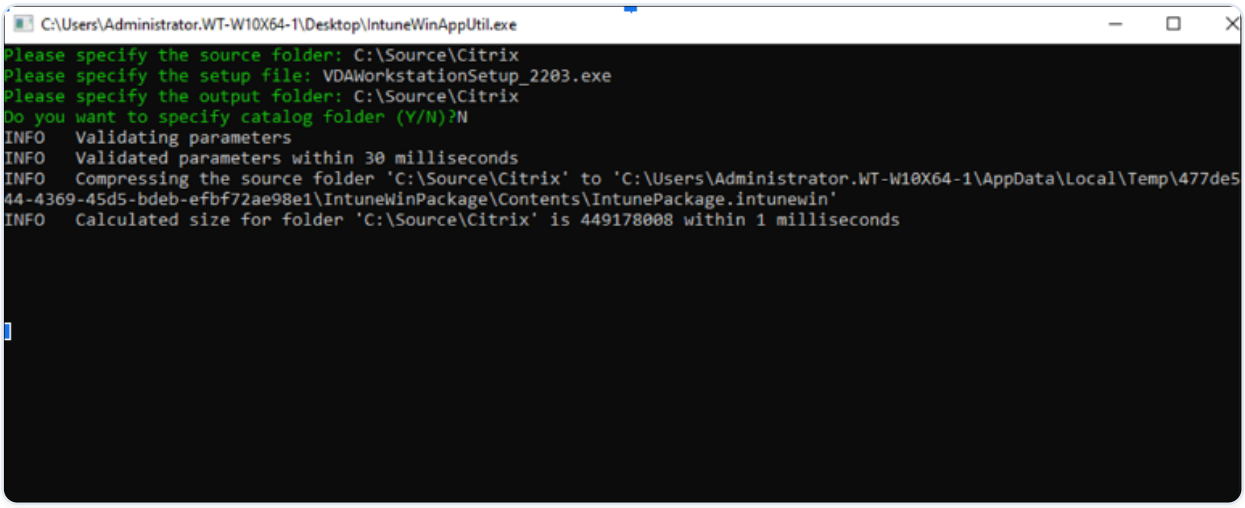
> **注:**
>
> 以下の記事は、Citrix® が環境をテストした方法に基づいた推奨事項のみを説明しています。これらの手順は、お客様のニーズに合わせてカスタマイズできます。Citrix は、お客様のニーズに合わせてこれに必要な更新や調整について責任を負いません。

Microsoft Intune を使用して VDA を展開するための主要な手順

1. Citrix VDA のインストールを準備する。
2. Microsoft 365 Developer Program サブスクライバーを設定する。
3. アプリを追加して割り当てる。
4. 登録済みデバイスにアプリをインストールする。

ステップ 1: CITRIX VDA のインストールを準備する

1. 更新された IntuneWinAppUtil.exe を GitHub からダウンロードします。
2. **管理者として実行**を使用して `IntuneWinAppUtil.exe` ファイルを実行します。
3. 次のデータを入力します。



a. **ソースフォルダーを指定してください**: アプリケーションのセットアップファイルが含まれているフォルダーを入力します。例: C:\source\Citrix。

b. **セットアップファイルを指定してください**: セットアップファイル名 (setup.exe や setup.msi など) を入力します。例: VDAWorkstationSetup_2203.exe。

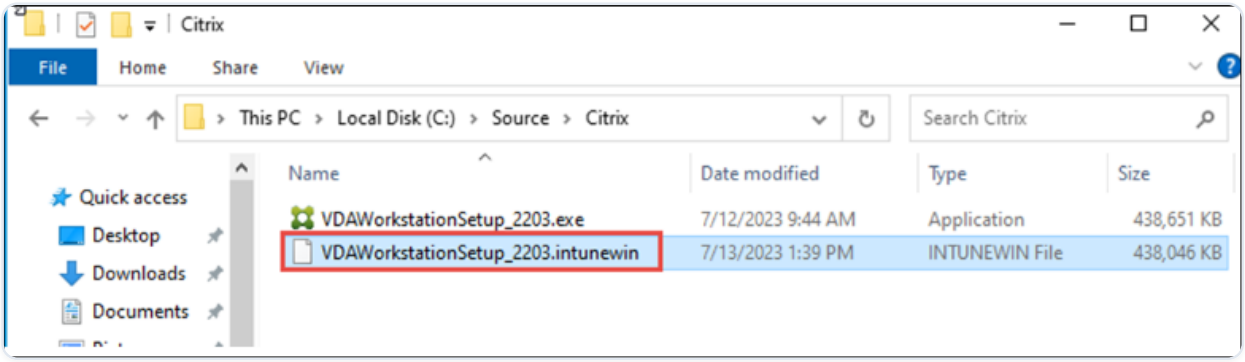
c. **出力フォルダーを指定してください**: .intunewin ファイルを生成する出力フォルダーのパスを入力します。例: C:\source\Citrix。

d. **カタログフォルダーを指定しますか (Y/N)**: N と入力します。

> **注:**
>
> **Win32 Content Prep Tool** の実行中は数分間お待ちください。`.intunewin` ファイルが生成されると、コマンドプロンプトの下部にステータスが 100% と表示されます。

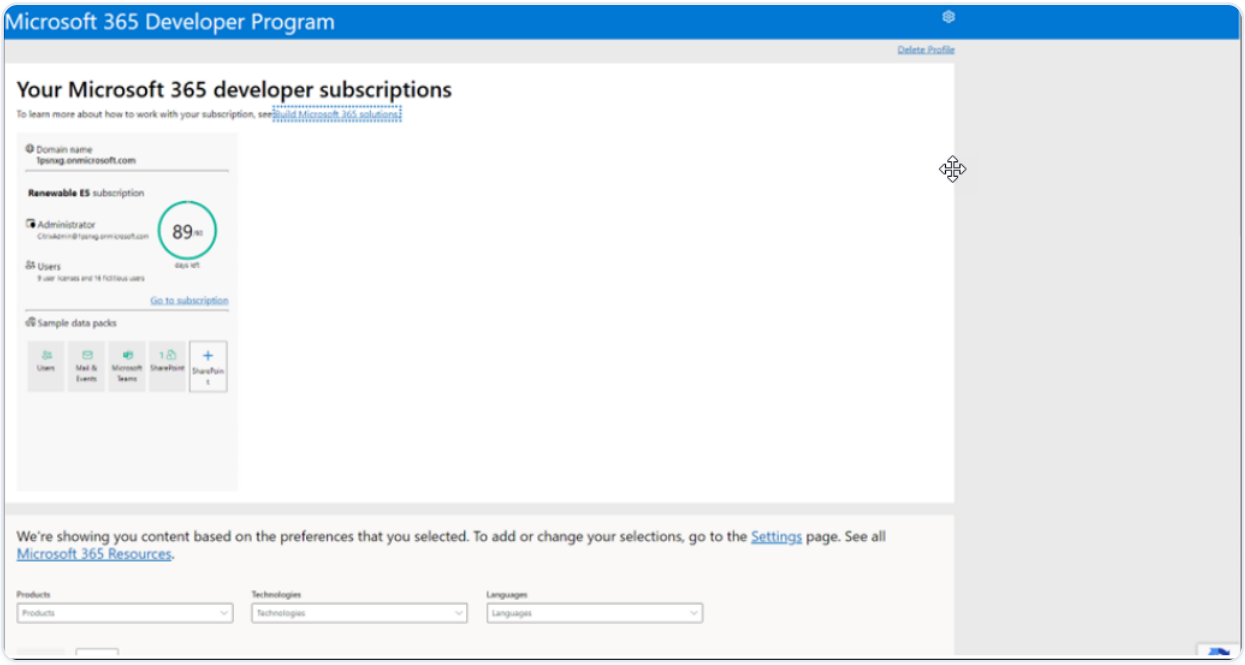
4. プロセスが完了したら、出力フォルダー (この例では `C:\source\Citrix`) に移動して、Microsoft Intune 展開ファイルを取得します。

5. Microsoft Intune の無料試用版にサインアップします。

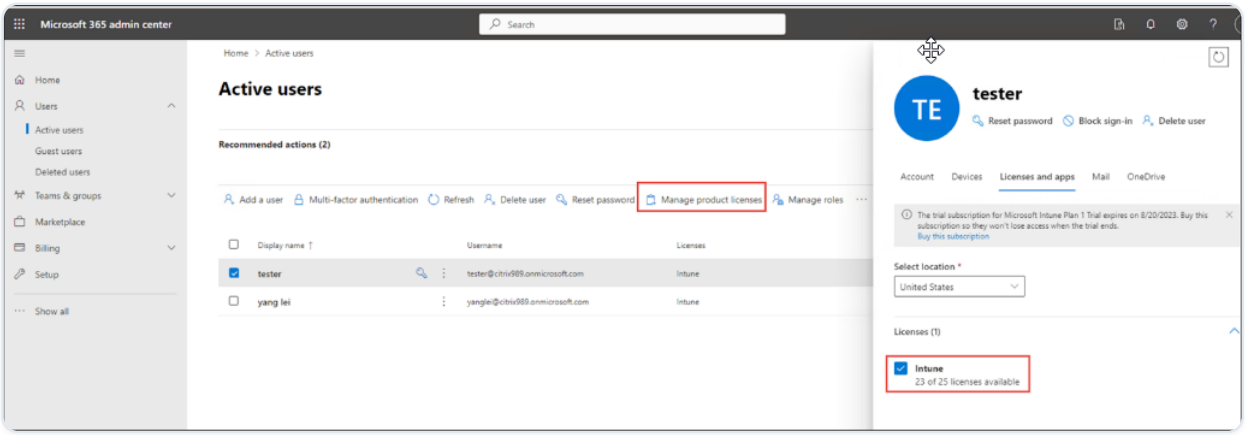


ステップ 2: MICROSOFT 365 DEVELOPER PROGRAM サブスクライバーを設定する

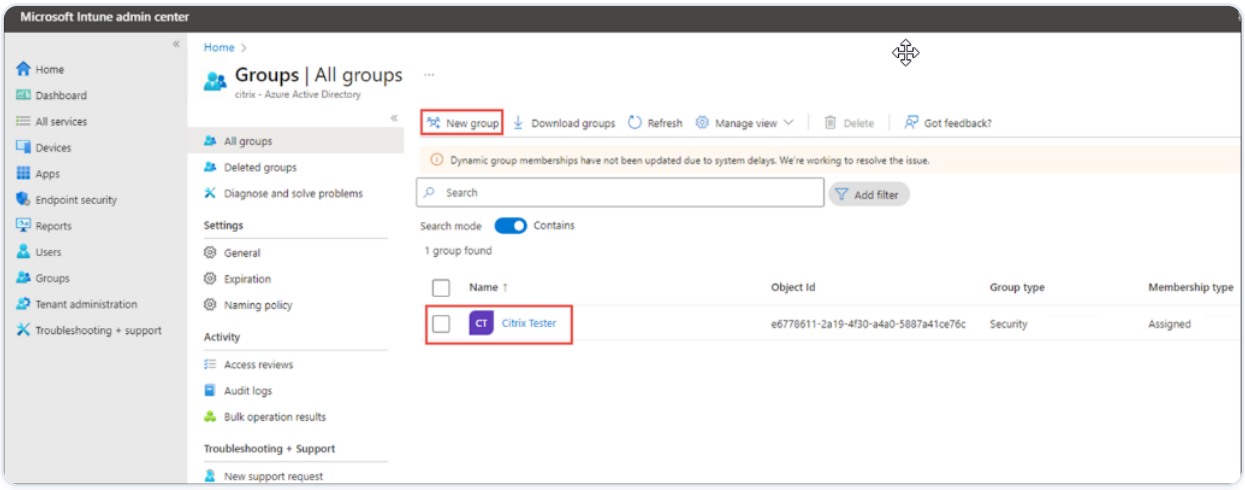
1. サブスクリプションをアクティブ化するために、インスタントサンドボックスを作成します。開発者サンドボックスを取得するには、Microsoft 365 Developer Program ダッシュボード に移動し、**新しいサブスクリプションの追加**を選択します。



2. Microsoft 365 管理センターでユーザーを作成し、そのユーザーにライセンスを割り当てます。



3. グループを作成します。



4. グループが作成されたら、そのグループに MDM 機関を提供する必要があります。自動登録を設定します。アクティブ化には 1 分ほどかかる場合があります。 または、次の手順を実行して、MDM 機関をグループに手動で追加することもできます。

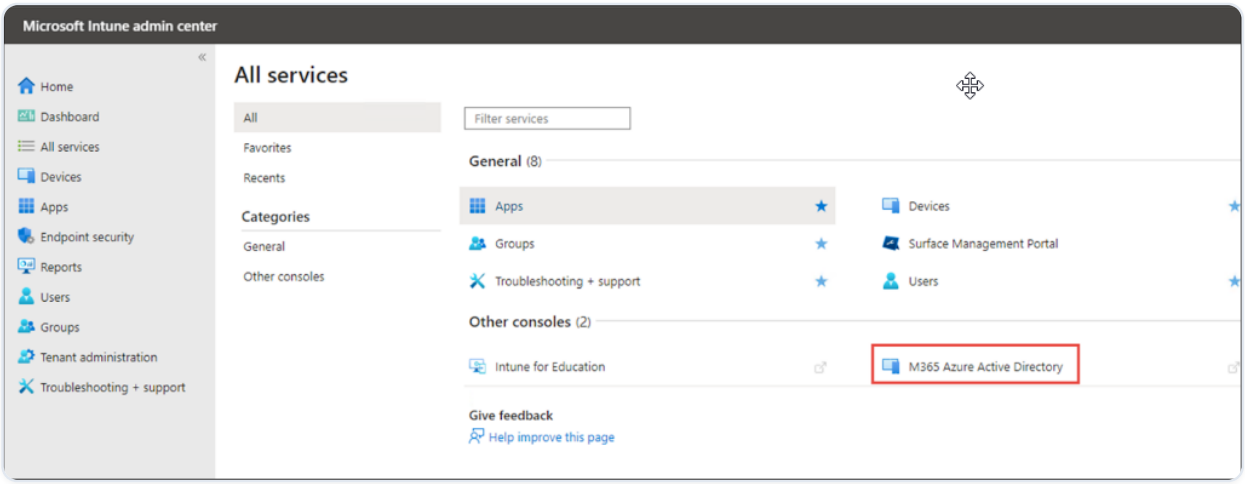
   a. **すべてのサービス > Microsoft Entra** に移動します。

   b. 「**設定 > モビリティ**」に移動し、「**Microsoft Intune**」を選択します。

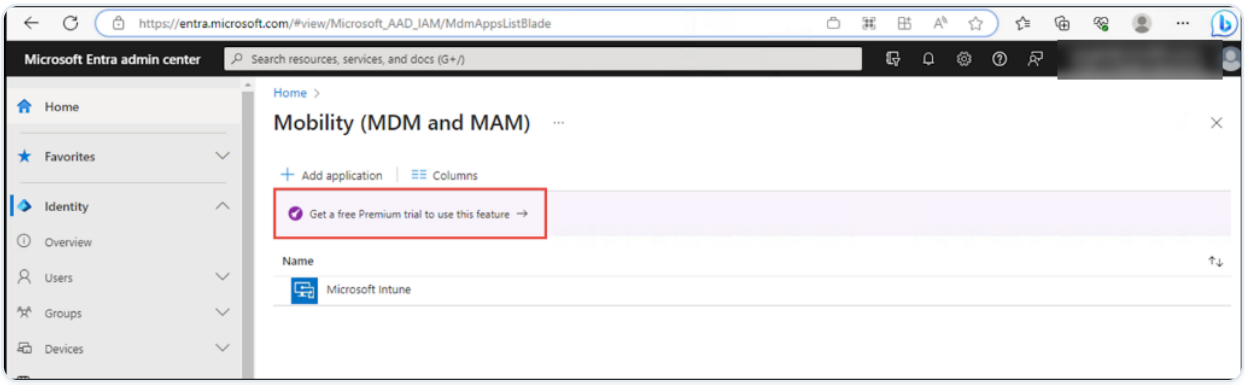
   c. 作成したばかりのグループを選択します。これにより、MDMユーザー範囲のページが開きます。

   d. 「**保存**」をクリックします。

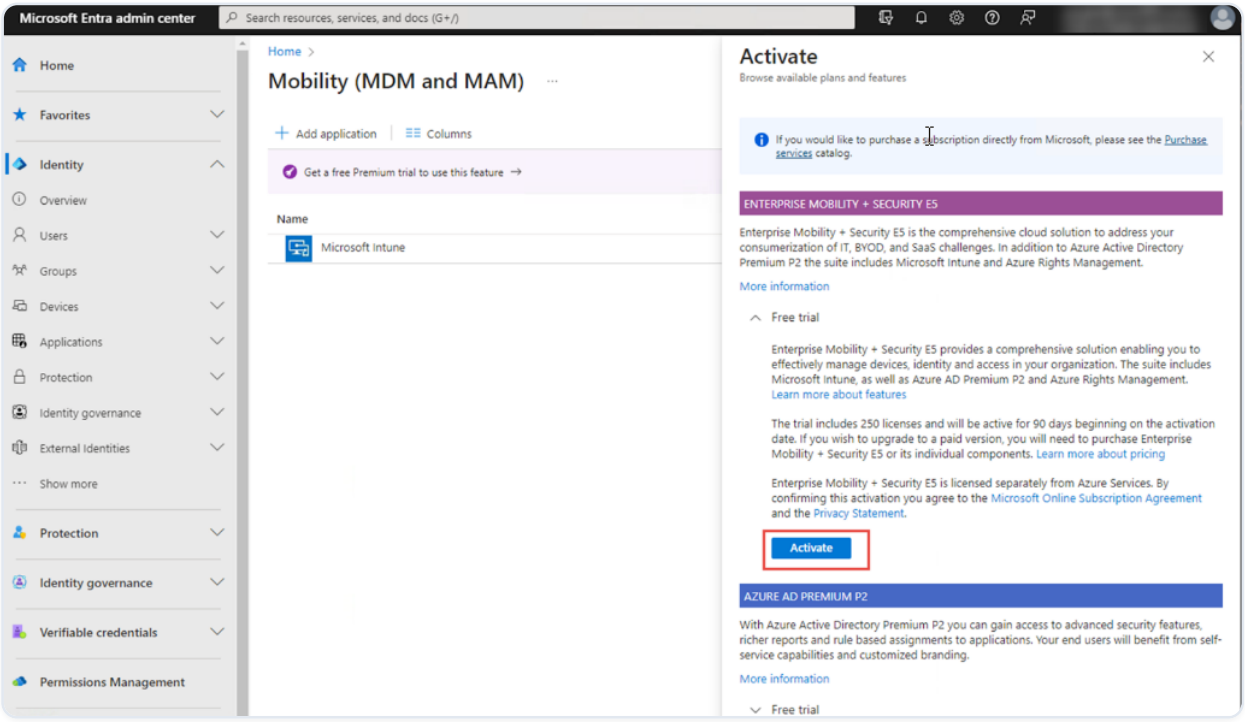
5. 「**すべてのサービス**」タブで、「**M365 Microsoft Entra ID**」をクリックします。



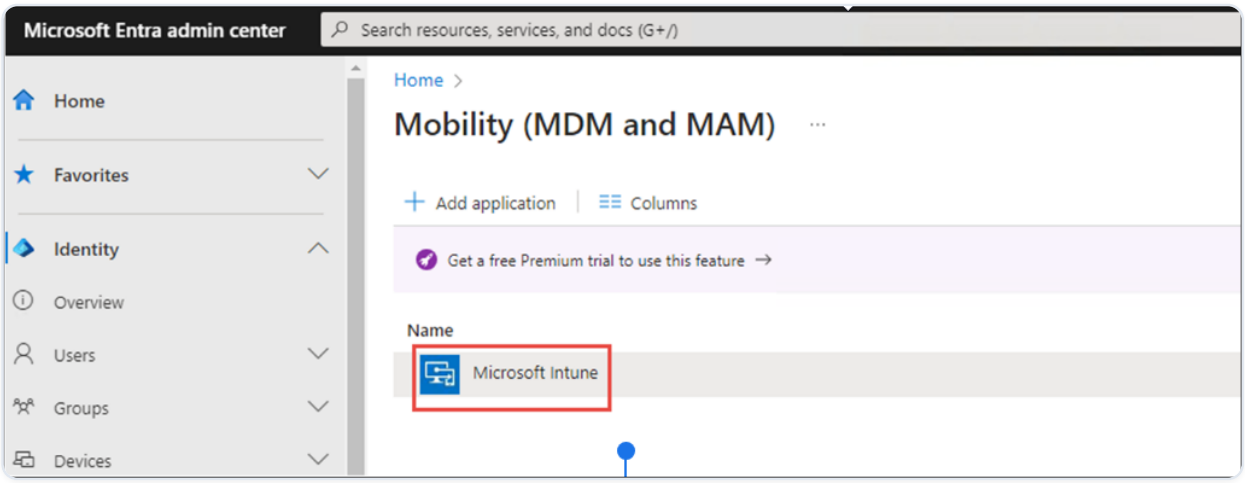
6. 「**この機能を使用するために無料のPremium試用版を入手**」をクリックします。



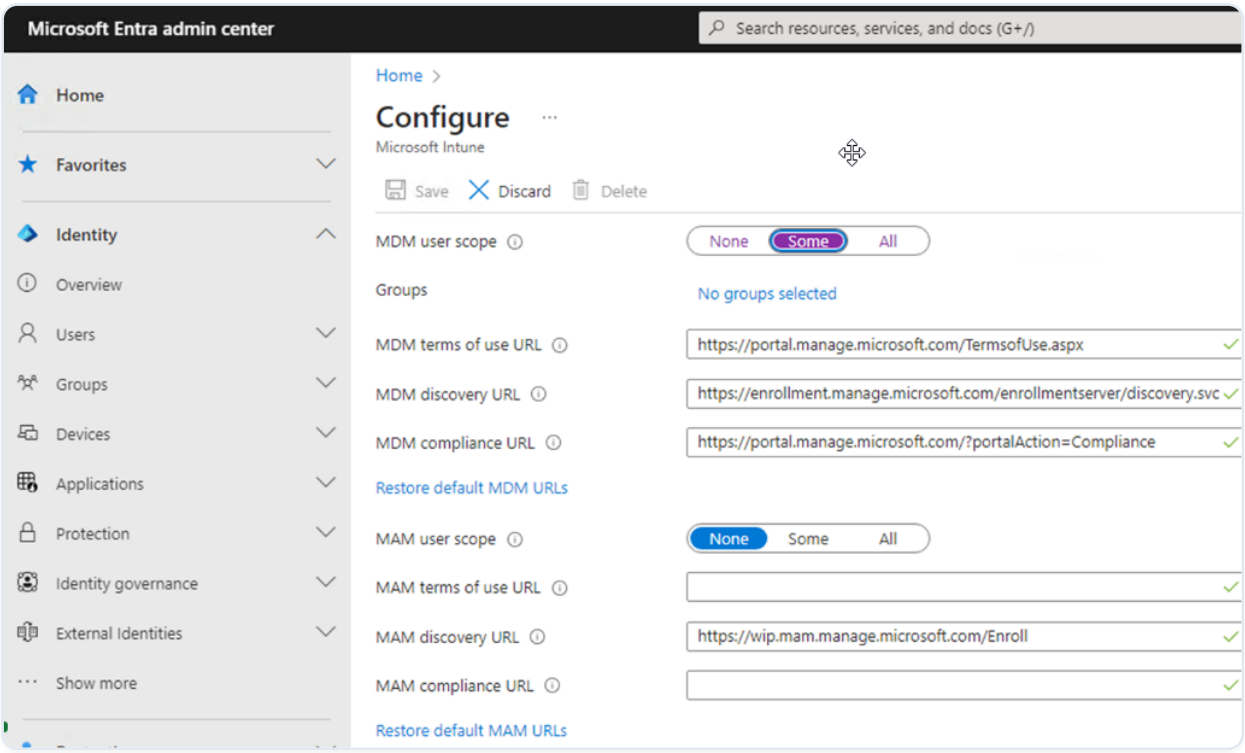
7. 「**アクティブ化**」をクリックします。



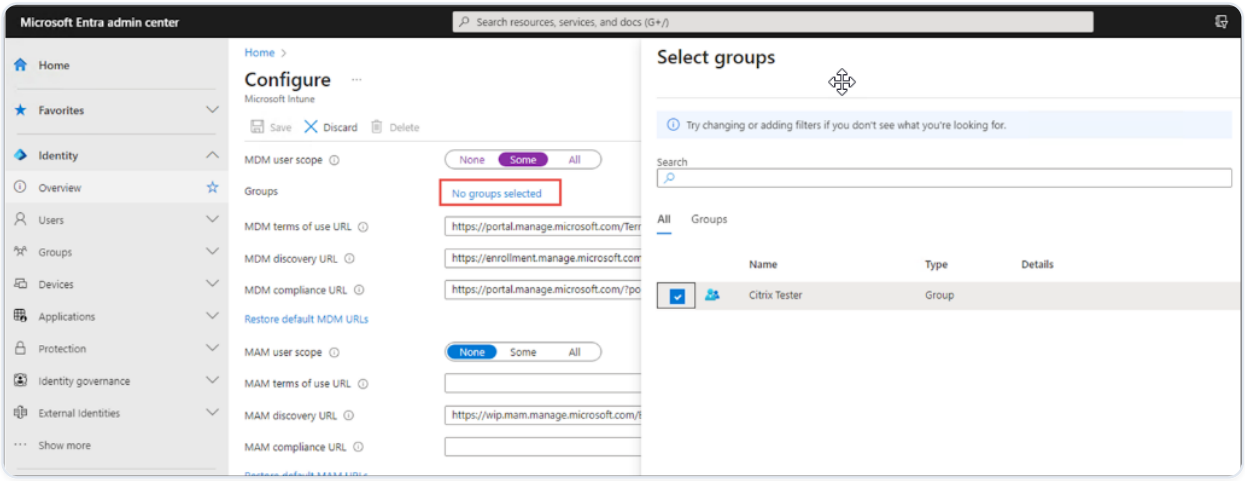
8. 次に、「**Microsoft Intune**」をクリックします。



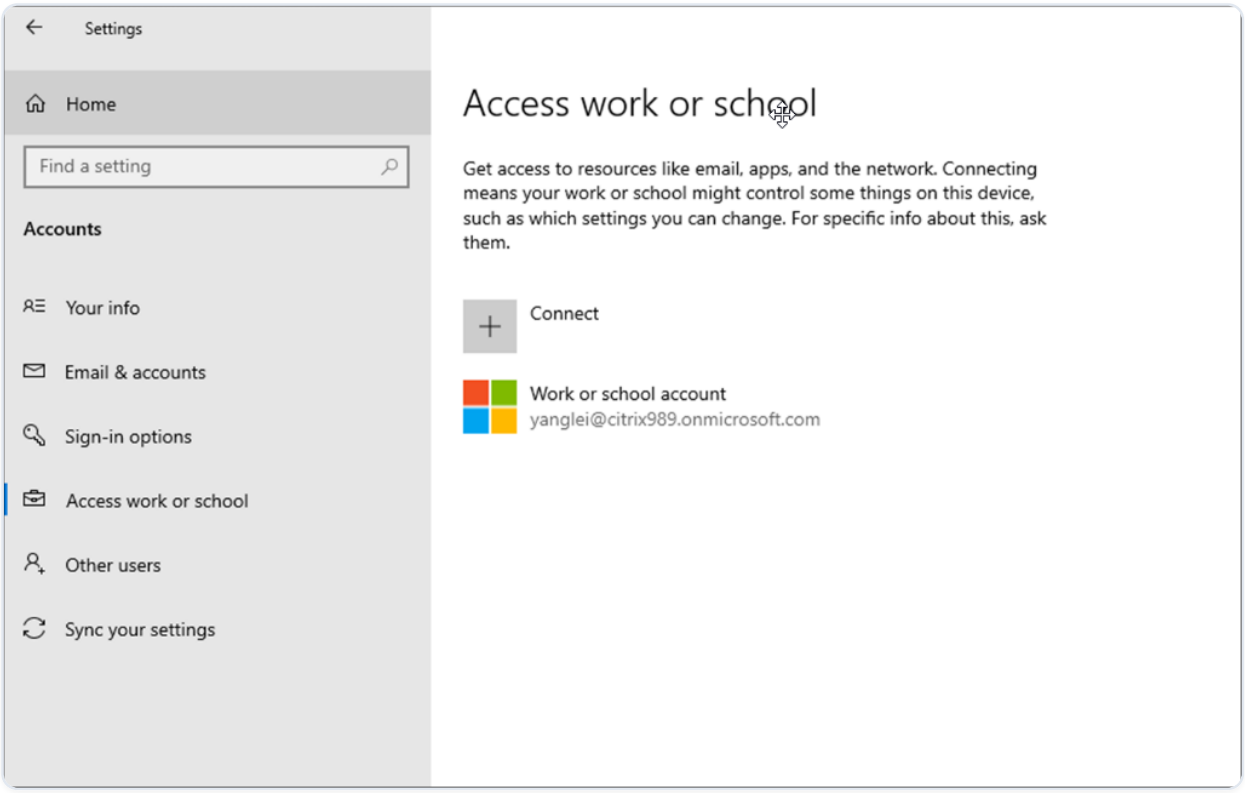
9. 「**構成**」タブで、必要な構成を入力します。



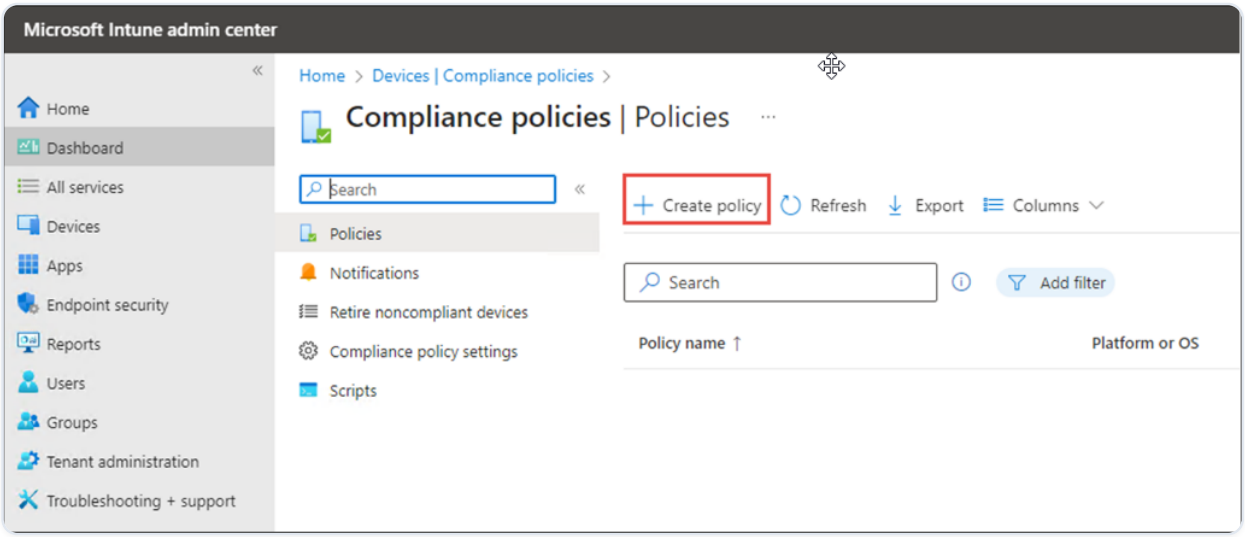
10. グループを追加するには、「**グループが選択されていません**」をクリックします。



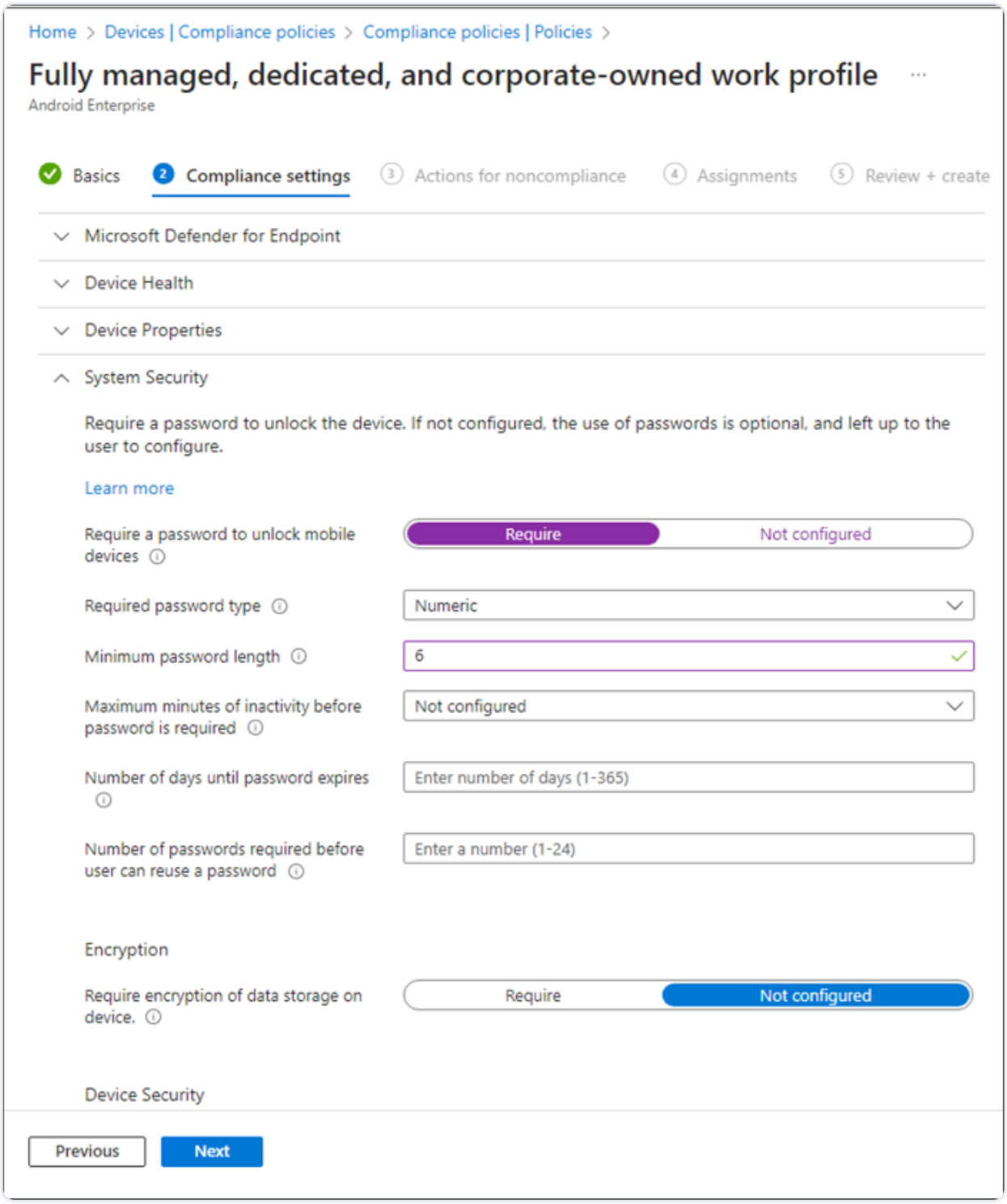
11. デバイスを登録します。



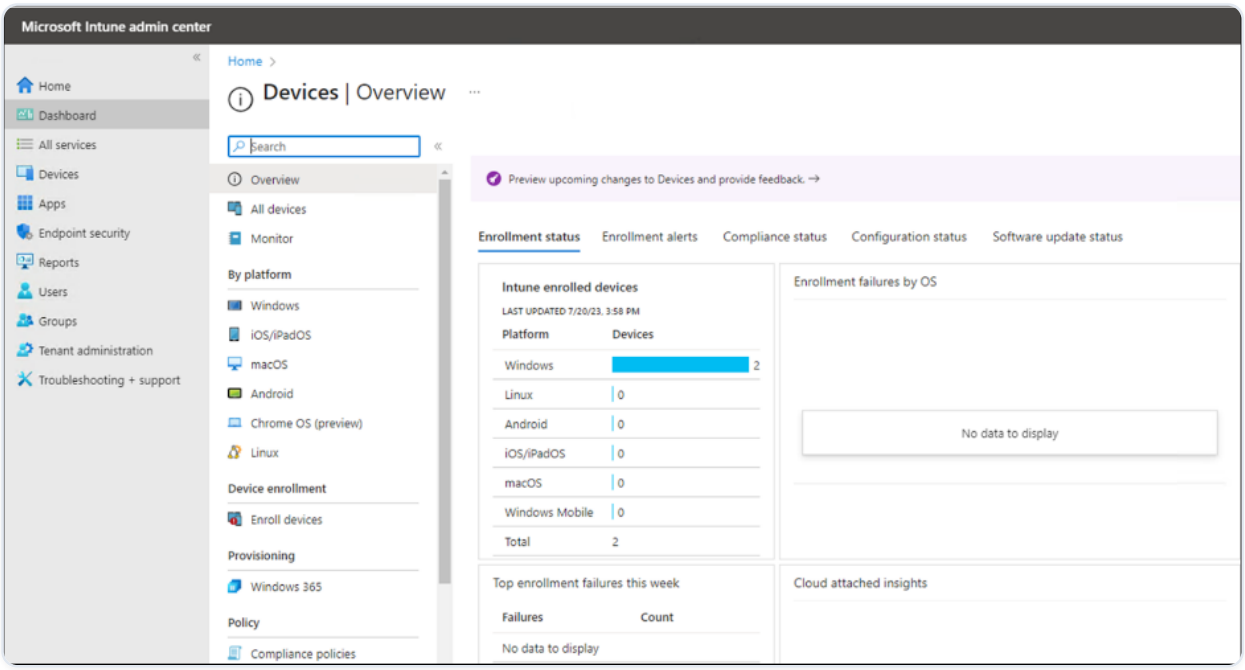
12. 新しく作成したデバイスのコンプライアンスを`Compliant`に変更するためのデバイスコンプライアンスポリシーを作成します。



13. 新しく作成したグループを追加するには、 タブに移動します。



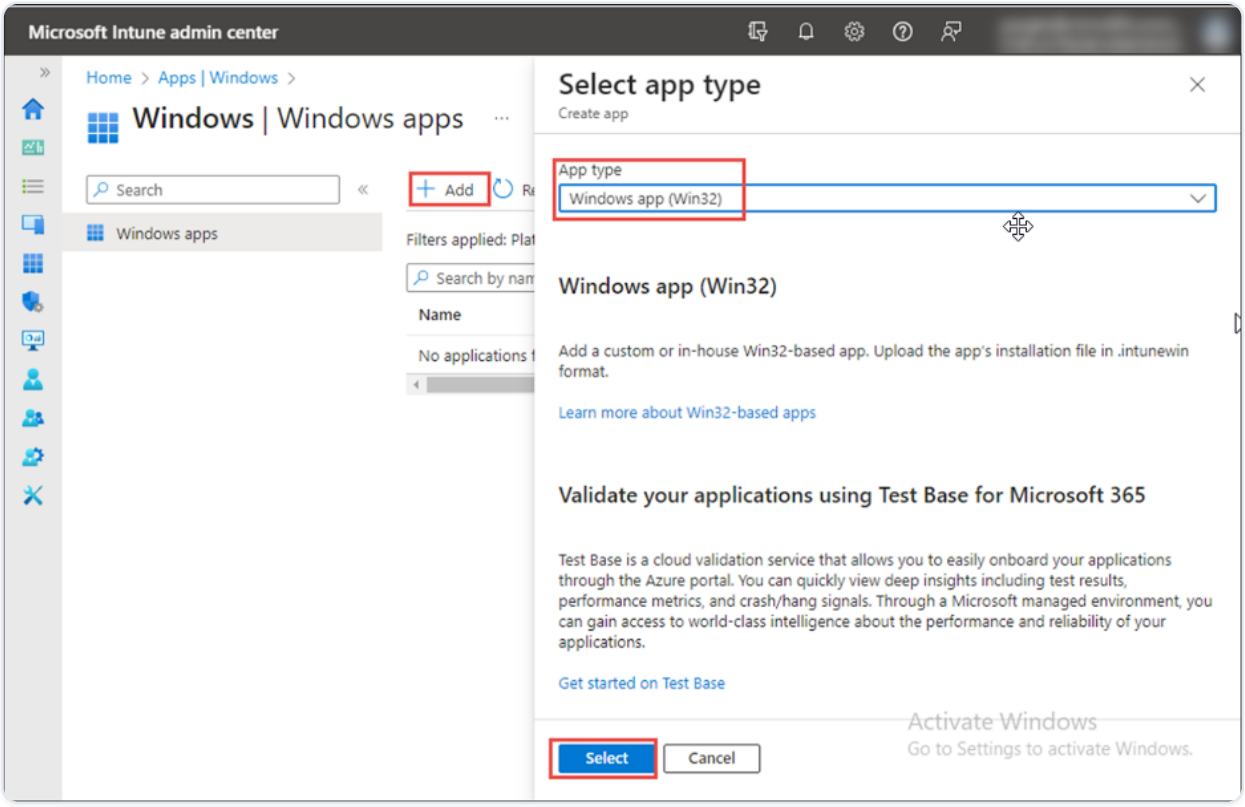
14. デバイスの登録を確認します。



詳細については、Microsoft 365 developer programを参照してください。

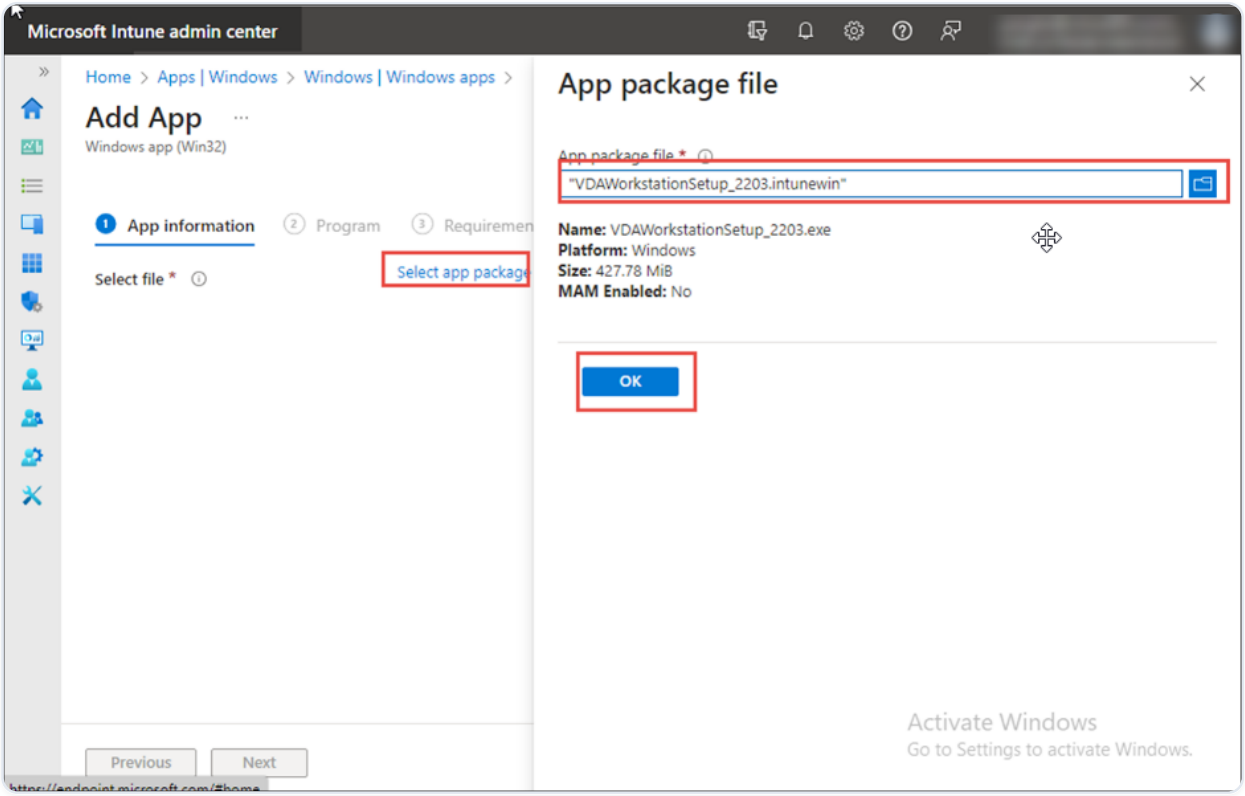
ステップ3：アプリの追加と割り当て

1. Microsoft Intune admin centerにサインインします。
2. **>** **>** を選択するか、 **>** **>** に移動します。



3. ペインで、 **>** を選択し、 をクリックします。
4. ペインで、 をクリックします。 をクリックします。

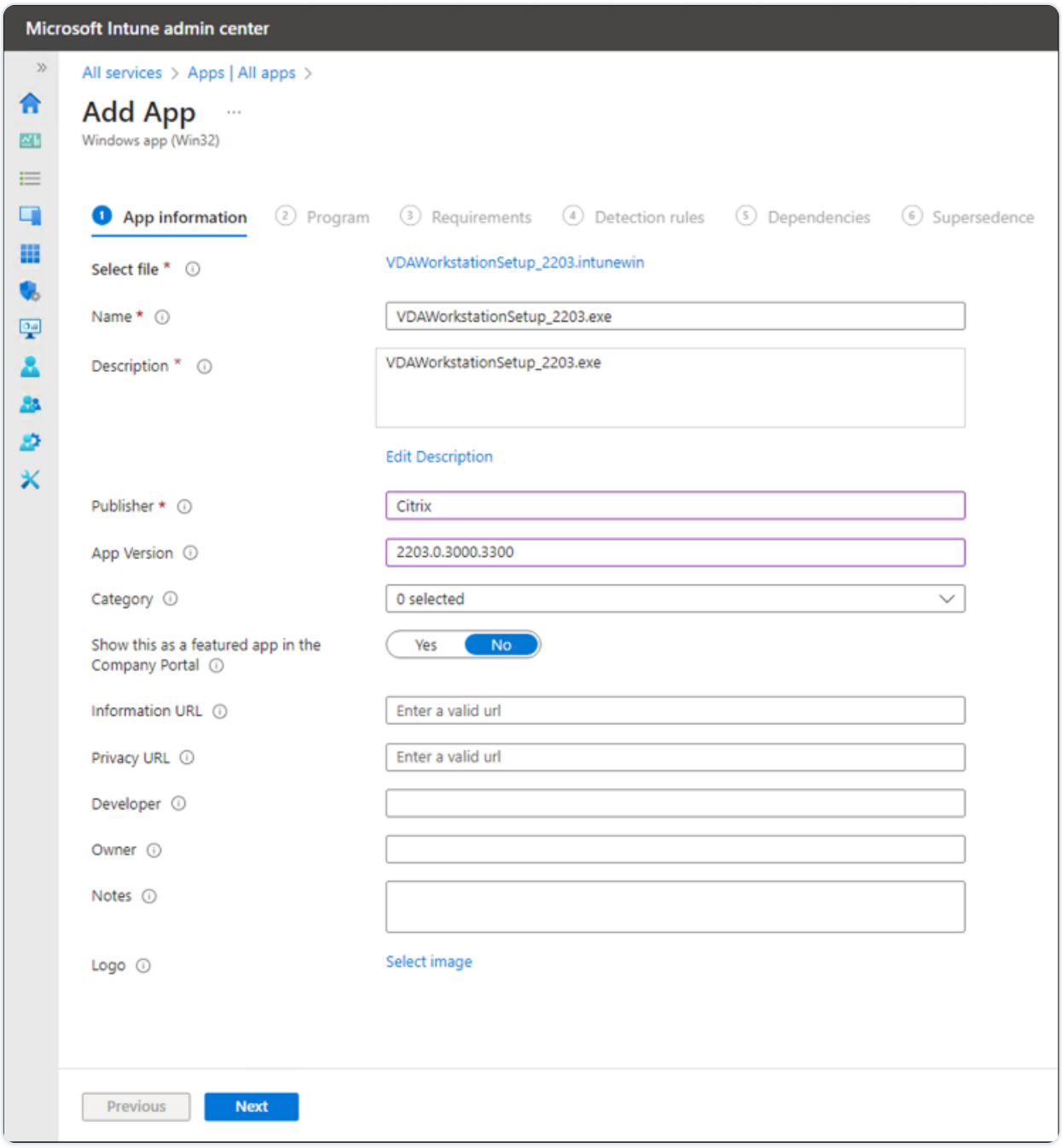
5. 拡張子`.intunewin`の準備済みファイルを選択します。準備済みファイルは、Citrix VDAのインストール準備のステップで作成されます。アプリに関する詳細情報を含むページが表示されます。



注:

- サーバーコアマシンを使用している場合は、VDAワークステーションコアを使用する必要があります。
- Windows 10デスクトップOSを使用している場合は、VDAワークステーションを使用する必要があります。
- サーバーOS（例：Windows 2022）を使用している場合は、VDAサーバーセットアップを使用する必要があります。
- この例ではバージョン2203を使用していますが、これはすべてのバージョンに適用できます。

6. **App package file**ペインで**OK**をクリックします。
7. 次の画面で、**App Information**タブの下にあるアプリの**Name**を入力し、Windowsアプリの**Description**を入力します。**Publisher**名として`Citrix`を入力し、ここで追加のアプリ情報を指定できます。**Next**をクリックします。

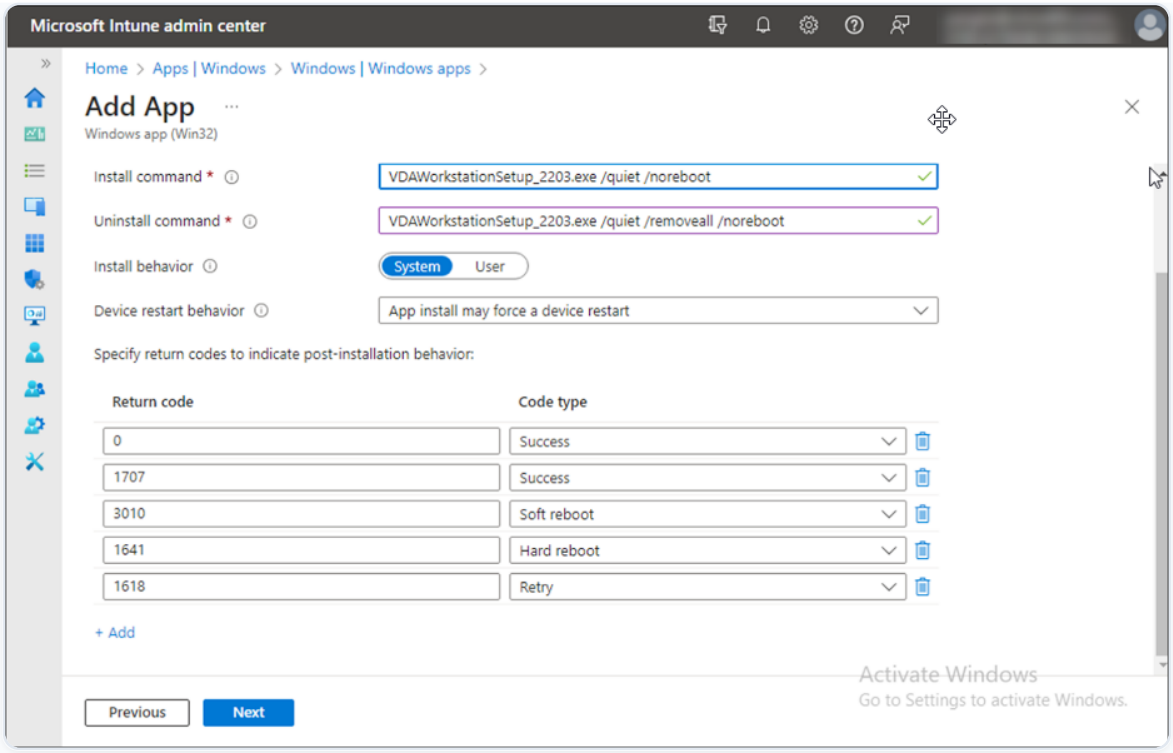


8. 次の画面で、次の値を入力します。

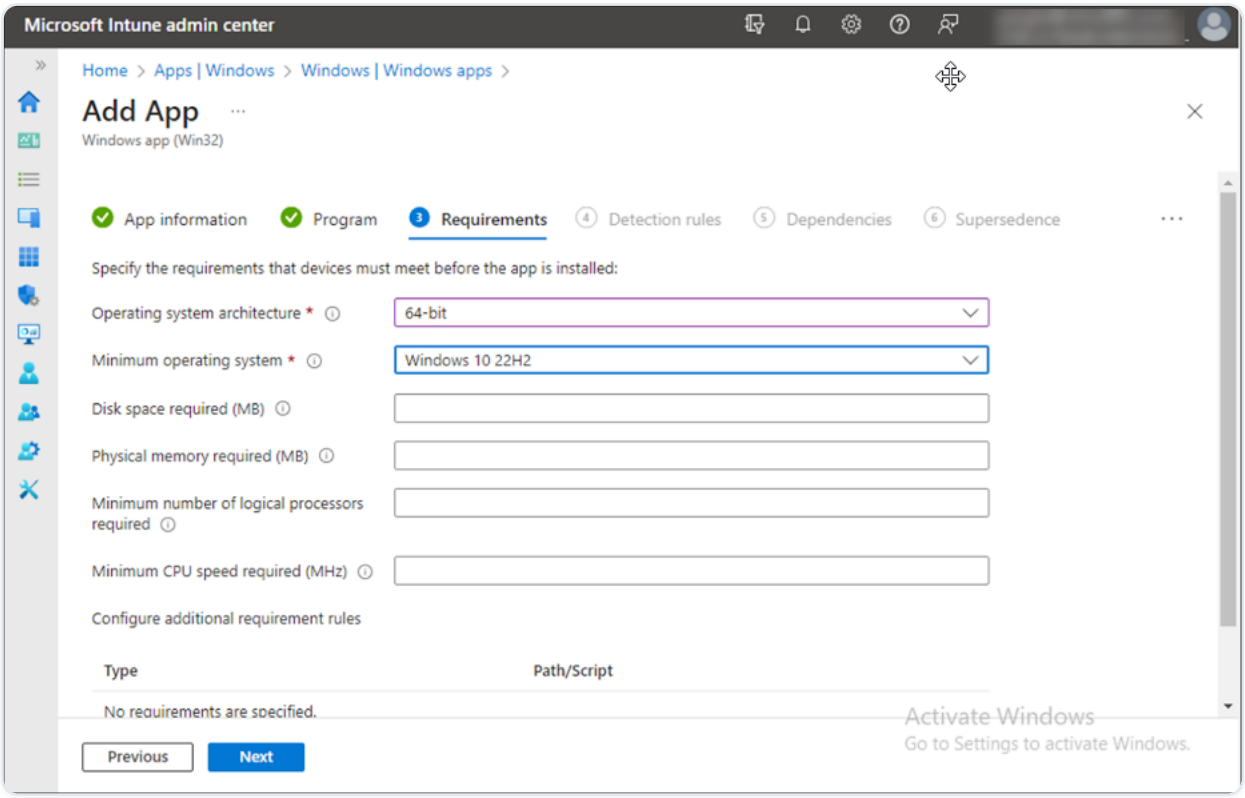
   - **インストールコマンド**: `VDAWorkstationSetup_2203.exe /quiet /noreboot`
   - **アンインストールコマンド**: `VDAWorkstationSetup_2203.exe /quiet /removeall /noreboot`
   - **インストール動作**:
     - **システム**: このオプションを選択すると、グループ内のすべてのデバイスにアプリがインストールされます。
     - **ユーザー**: このオプションを選択すると、グループ内の特定のユーザーデバイスにのみアプリがインストールされます。

9. **Next**をクリックします。

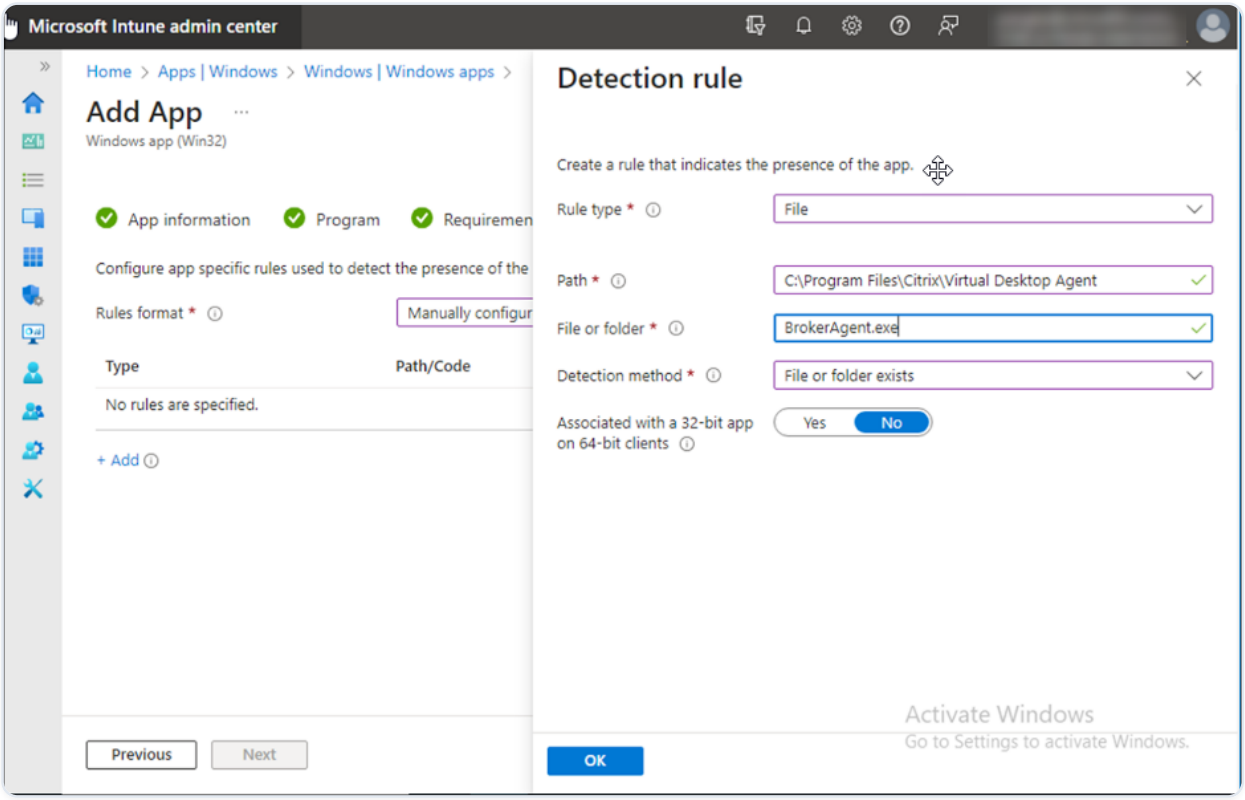
> **注:**
>
> - この例ではバージョン2203を使用していますが、どのバージョンでも使用できます。
> - コマンドに`/noreboot`を追加しても、インストールまたは展開中に再起動が発生しないという意味ではなく、強制的な再起動が適用されるだけです。 スクリプトの詳細については、「VDAをインストールするためのコマンドラインオプション」を参照してください。
> - **デバイスの再起動動作**については、**Intune will force a mandatory device restart**を選択します。
> - 「**リターンコード**」テキストボックスに、インストール後の成功のために`0`、`3`、`8`を入力します。 その他のリターンコードについては、「Citrix インストールリターンコード」を参照してください。



10. 次の画面で、「**要件**」タブの下に、必要な値を入力します。「**次へ**」をクリックします。



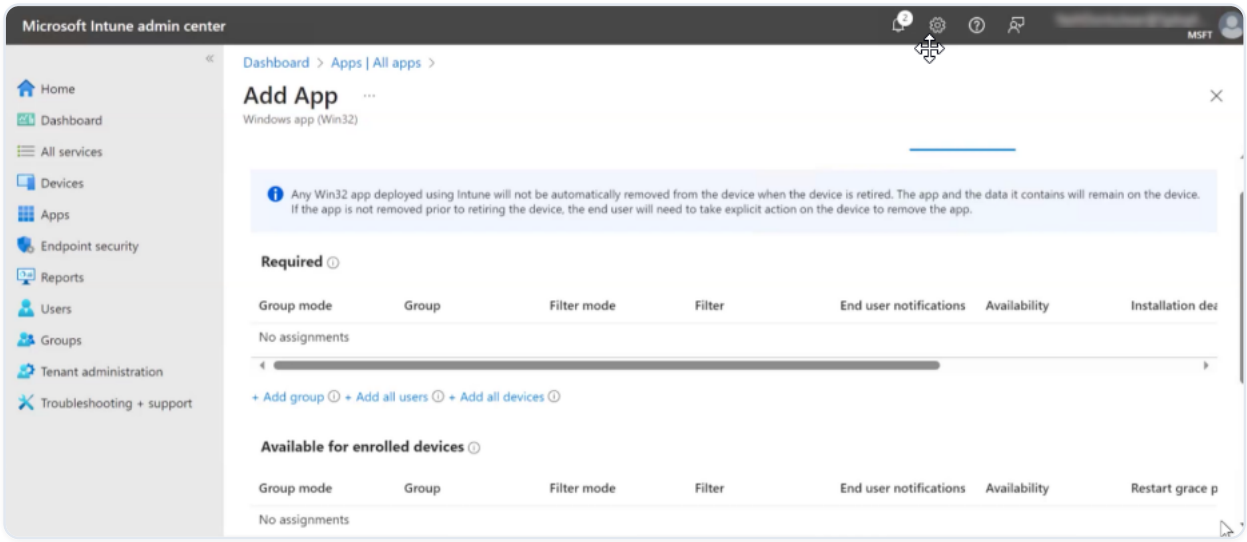
11. 次の画面で、「**検出ルール**」タブの下に、Broker エージェントを追加するための「**検出ルール**」を追加します。「**OK**」をクリックします。



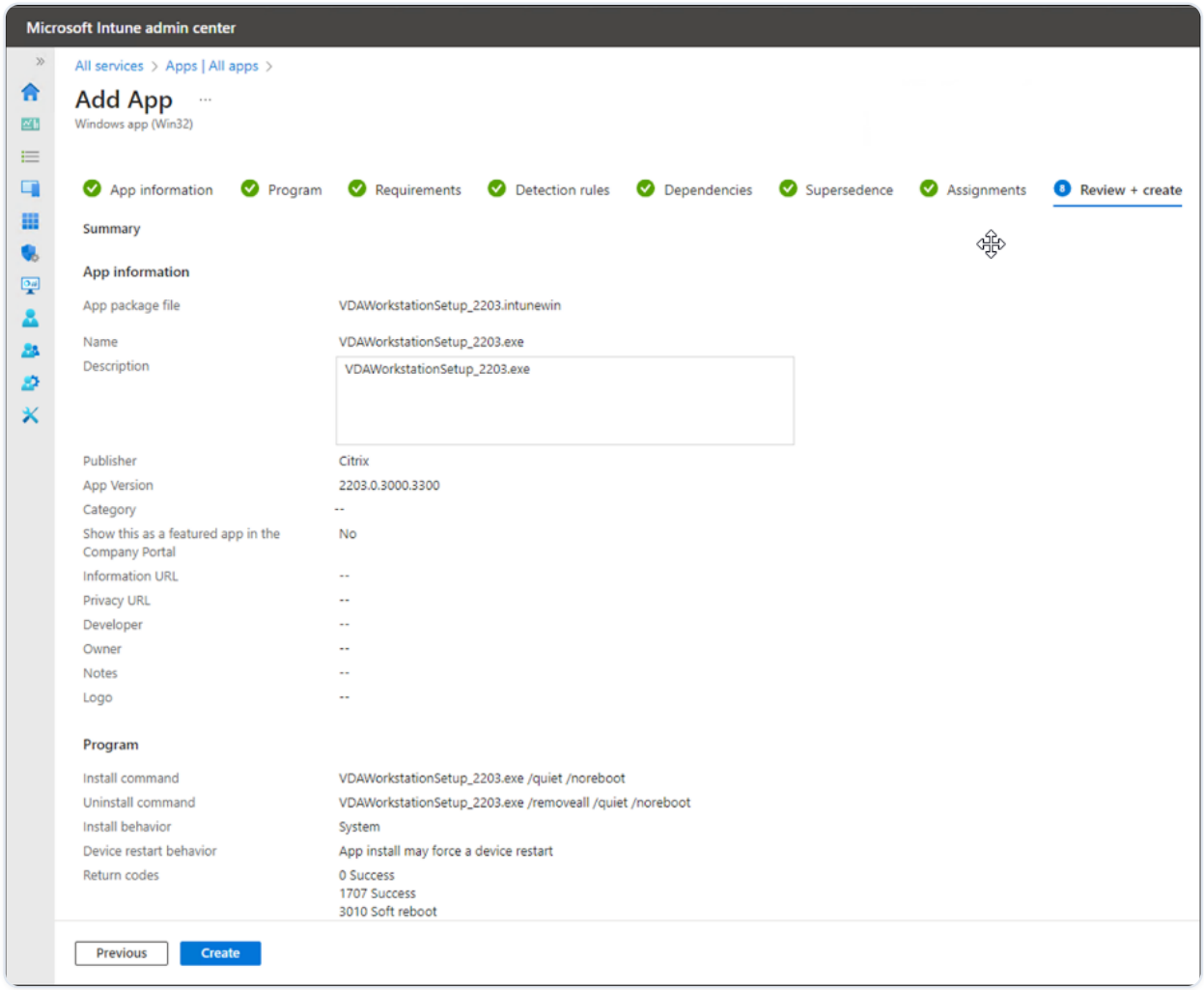
12. 「**割り当て**」タブで、デバイスを次のように追加できます。

- **必須**: 更新が自動的に行われるデバイス。

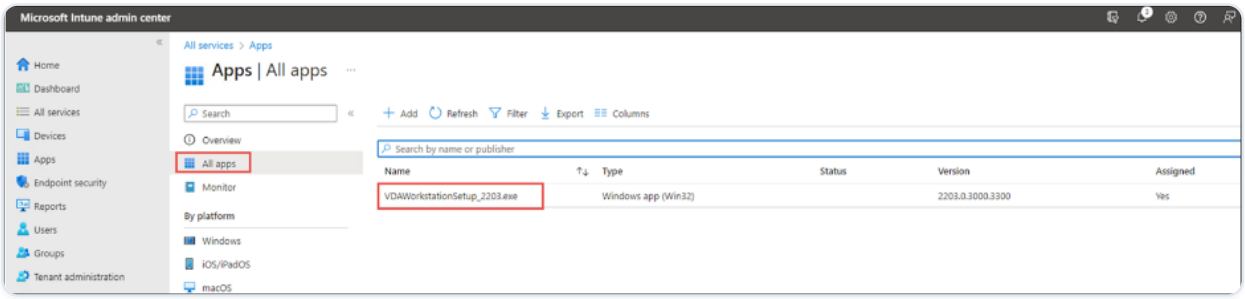
- **登録済みデバイスで利用可能**: 更新が手動で行われるデバイス。



13. 詳細を確認し、「**作成**」をクリックします。



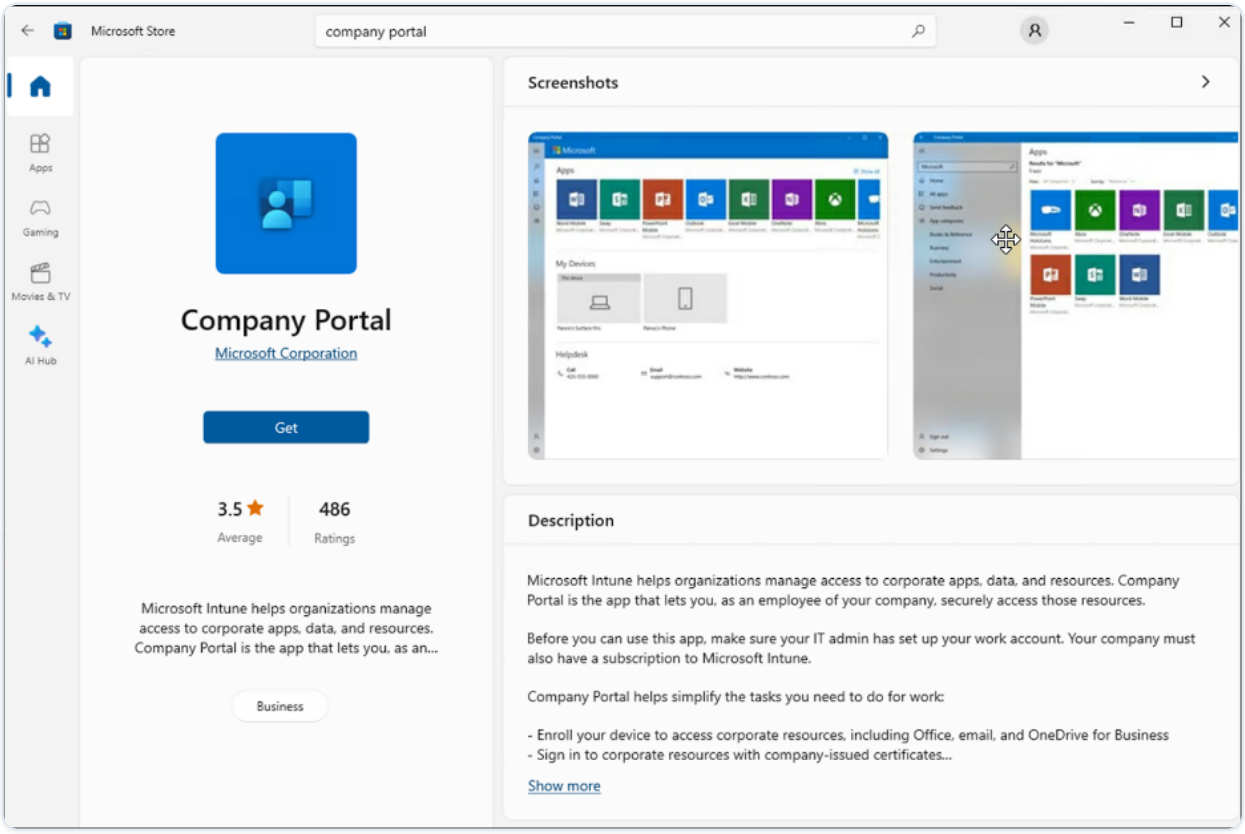
アプリが正常に割り当てられました。



詳細については、「アプリの追加と割り当て」を参照してください。

ステップ 4: 登録済みデバイスにアプリをインストールする

1. 登録済みのWindows 10デスクトップデバイスにサインインします。 デバイスはMicrosoft Intuneに登録されている必要があります。また、アプリに割り当てたグループに含まれるアカウントを使用してデバイスにサインインする必要があります。詳細については、Microsoftのドキュメントを参照してください。
2. 「**スタート**」メニューから「**Microsoft Store**」を開きます。
3. 「**Company Portal**」アプリを検索してインストールします。



4. 「**Company Portal**」アプリを実行します。
5. Microsoft Intuneを使用して追加したアプリをクリックします。 Intuneユーザーにアプリを正常に割り当てなかった場合、次のメッセージが表示されます。 `Your IT administrator did not make any apps available to you.`

6. 「**インストール**」をクリックします。

サイトを作成する

> **注:**
>
> - サイト作成中、ハイブリッド権限ライセンスを有効にするライセンスを追加した後、サイト作成が完了するまで、パブリッククラウドホスト（Microsoft Azure、Google Cloud Platform、Amazon Web Servicesなど）は接続タイプリストに表示されません。
> - ライセンスアクティベーションサービスを有効にしている間、または有効にした後に、製品エディションやライセンスモデルを手動で変更しないでください。

> サイトとは、Citrix Virtual Apps and Desktops™展開に付ける名前です。これには、Delivery Controllerとその他のコアコンポーネント、Virtual Delivery Agent (VDA)、ホストへの接続、マシンカタログ、およびデリバリーグループが含まれます。サイトは、コアコンポーネントをインストールした後、最初のマシンカタログとデリバリーグループを作成する前に作成します。

ControllerがServer Coreにインストールされている場合は、Citrix Virtual Apps and Desktops SDKのPowerShellコマンドレットを使用してサイトを作成します。

サイトを作成すると、Citrixカスタマーエクスペリエンス向上プログラム（CEIP）に自動的に登録されます。CEIPは匿名の統計情報と使用状況情報を収集し、Citrixに送信します。最初のデータパッケージは、サイト作成後約7日後にCitrixに送信されます。サイト作成後いつでも登録を変更できます。Web Studioの左ペインで**設定**を選択し、**Citrixカスタマーエクスペリエンス向上プログラム**の設定を見つけます。詳細については、`<http://more.citrix.com/XD-CEIP>`を参照してください。

サイトを作成したユーザーは、フル管理者になります。詳細については、委任管理を参照してください。

サイトを作成する前にこの記事を確認して、何が期待できるかを知っておいてください。

ステップ1. サイト作成ウィザードを開く - Citrix Site Manager

Citrix Site Manager ツールを使用して、Citrix Virtual Apps and Desktops™ 展開（サイトとも呼ばれます）をセットアップします。このツールは、Delivery Controller をインストールすると自動的にインストールされます。

このツールを実行するには、Delivery Controllerでデスクトップのスタートメニューを開き、**Citrix > Citrix Site Manager**を選択します。Web Studioのインストールを参照してください。

ステップ2. サイト名

はじめにページで、サイトの名前を入力します。

ステップ3. データベース

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

> **データベース**ページには、サイト、監視、および構成ログデータベースの設定に関する選択肢が含まれています。データベースの設定の選択肢と要件の詳細については、データベースを参照してください。

> **注:**
>
> SQL Server Always On ListenerがTLS暗号化用に構成されている場合、データベース作成権限を持つ資格情報の入力を求められることがあります。有効な管理者資格情報を入力しても、データベースの作成は失敗します。SQL Server証明書に、Subject Alternative Names (SAN) にリスナーのDNS名が含まれていることを確認してください。詳細については、`<https://docs.microsoft.com/ja-jp/sql/database-engine/availability-groups/windows/listeners-client-connectivity-application-failover#SSLcertificates>`を参照してください。

> サイトデータベースとして使用するためにSQL Server Expressをインストールすることを選択した場合（デフォルト）、そのソフトウェアのインストール後に再起動が発生します。サイトデータベースとして使用するためにSQL Server Expressソフトウェアをインストールしないことを選択した場合、その再起動は発生しません。

デフォルトのSQL Server Expressを使用しない場合は、サイトを作成する前に、SQL Serverソフトウェアがマシンにインストールされていることを確認してください。システム要件にサポートされているバージョンが記載されています。

サイトにDelivery Controllerを追加したい場合で、すでに他のサーバーにControllerソフトウェアをインストールしている場合は、このページからそれらのControllerを追加できます。データベースを設定するスクリプトを生成する予定がある場合は、スクリプトを生成する前にControllerを追加してください。

ステップ4. ライセンス

ライセンスページで、ライセンスサーバーのアドレスを指定し、使用する（インストールする）ライセンスを示します。

> **注:**
>
> - ライセンスサーバーがバージョン11.17.2ビルド53100以降で動作していることを確認してください。この前提条件を満たさない場合、Citrix Virtual Apps and Desktopsサイトのアップグレードとサイト作成がブロックされます。
> - License Activation Service (LAS) は、従来のCitrixレガシーライセンスに代わるクラウドベースのライセンスソリューションです。詳細については、以下を参照してください。
>   - Citrix Virtual Apps and Desktops ドキュメント: ライセンスアクティベーションサービス
>   - ライセンスドキュメント: License Activation Service
> - License Activation Serviceを有効にしている間、または有効にした後に、製品エディションやライセンスモデルを手動で変更しないでください。

- ライセンスサーバーのアドレスを`name:[port]`の形式で指定します。*名前*はFQDN、NetBIOS、またはIPアドレスである必要があります。FQDNを推奨します。ポート番号を省略した場合、デフォルトは27000です。**接続**をクリックします。ライセンスサーバーへの接続が成功するまで、次のページに進むことはできません。
- 接続が確立されると、デフォルトで**既存のライセンスを使用**が選択されます。表示には、現在インストールされているライセンスに基づいて、この製品が構成できる互換性のある製品が一覧表示されます。
  - ライセンスサーバーがLicense Activation Service (LAS) を使用するように構成されている場合、メタインストーラーはエンタイトルメントを表示します。エンタイトルメントは、対応するライセンスの有効期限とともに提供されます。これらのライセンスのいずれかを

使用して、この製品をリストされている製品の1つとして構成する場合は、そのエントリを選択します。

- この製品で使用するためにライセンスを割り当ててダウンロード済み（Citrix Manage Licenses Toolを使用）だが、まだライセンスをインストールしていない場合：
  - **ライセンスファイルを参照**をクリックします。
  - ファイルエクスプローラーで、ダウンロードしたライセンスを見つけて選択します。関連する製品がサイト作成ウィザードの**ライセンス**ページに表示されます。使用したいエントリを選択します。
- 目的の製品が表示されない場合、または割り当て済みでダウンロード済みのライセンスがない場合は、ライセンスを割り当て、ダウンロードしてインストールできます。これを行うには、ライセンスサーバーがインターネットにアクセスできる必要があります。目的の製品のライセンスアクセスコードが必要です。Citrixからそのコードがメールで送信されます。
  - **割り当ててダウンロード**をクリックします。
  - **ライセンスの割り当て**ダイアログで、Citrixから送信されたライセンスアクセスコードを入力します。**ライセンスを割り当てる**をクリックします。
  - 新しいライセンスに関連付けられている製品が、サイト作成ウィザードの**ライセンス**ページに表示されます。使用するエントリを選択します。

- または、**30日間の無料試用版を使用**を選択し、後でライセンスをインストールします。詳細については、ライセンスドキュメントを参照してください。

ステップ5. 概要

概要ページには、指定した情報が一覧表示されます。変更する場合は、**戻る**ボタンを使用します。完了したら、**完了**をクリックします。

詳細情報

ホスト接続、ネットワーク、およびストレージ

ハイパーバイザーまたはその他のサービス上のVMを使用してアプリケーションとデスクトップを配信している場合、オプションでそのホストへの最初の接続を作成できます。その接続のストレージおよびネットワークリソースを指定することもできます。サイト作成後、この接続とリソースを変更したり、さらに接続を作成したりできます。詳細については、接続とリソースを参照してください。

- **接続**ページで指定する情報については、接続とリソースを参照してください。
  - ハイパーバイザーまたはその他のサービス上のVMを使用しない場合（またはWeb Studioを使用して専用ブレードPC上のデスクトップを管理する場合）は、接続の種類として**なし**を選択します。
  - Remote PC Accessサイトを構成していて、Wake on LAN機能を使用する予定がある場合は、**Microsoft System Center Virtual Machine Manager**または**Remote PC Wake on LAN**の種類を選択します。詳細については、Wake on LANを参照してください。

  接続の種類に加えて、Citrixツール（Machine Creation Services™など）またはその他のツールを使用してVMを作成するかどうかを指定します。
- **ストレージ**ページと**ネットワーク**ページで指定する情報については、ホストストレージ、ストレージ管理、およびストレージの選択を参照してください。
- ハイブリッド権限ライセンスを所有しており、パブリッククラウドホスト接続（AWSなど）を追加している場合、それらの接続がここに一覧表示されます。これらのパブリッククラウドホスト接続を表示するには、追加後数分経ってからWeb Studioを更新してください。

リモートPCアクセス

Remote PC Accessの展開については、Remote PC Accessを参照してください。

Wake on LAN機能を使用する場合は、サイトを作成する前にMicrosoft System Center Configuration Managerで構成手順を完了してください。詳細については、Configuration ManagerとRemote PC Access Wake on LANを参照してください。

接続とリソースの作成および管理

> **重要:**
>
> Citrix Virtual Apps and Desktops™ 7 2006以降、現在の展開で以下のいずれかのテクノロジーを使用している場合、それらのテクノロジーを使用するサポート終了（EOL）項目を削除した後にのみ、現在のリリースに展開をアップグレードできます。
>
> - パーソナル vDisk (PvD)
> - AppDisks™
> - パブリッククラウドホストの種類：Citrix CloudPlatform、Microsoft Azure Classic

詳細については、「PVD、AppDisks、およびサポートされていないホストの削除」を参照してください。

注:

バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

展開にパブリッククラウドホスト接続を使用する場合は、新規インストールまたは現在のリリースへのアップグレードを完了するためにHybrid Rights Licenseが必要です。

インストーラーがサポートされていないテクノロジーの1つ以上、またはHybrid Rights Licenseなしのホスト接続を検出すると、アップグレードが一時停止または停止し、説明メッセージが表示されます。インストーラーのログに詳細が含まれています。詳しくは、「展開のアップグレード」を参照してください。

Hybrid Rights Licenseがホスト接続に与える影響

Hybrid Rights Licenseの資格に基づいて、パブリッククラウドホストへのホスト接続が影響を受ける3つのシナリオがあります。

- パブリッククラウドホストへの新しいホスト接続を作成するには、Hybrid Rights Licenseが必要です。
- Hybrid Rights Licenseを所有しているがライセンスの有効期限が切れている場合、パブリッククラウドホストへの既存の接続は資格なしとマークされ、メンテナンスモードに入ります。既存のホスト接続がメンテナンスモードの場合、次の操作はできません。
  - ホスト接続の追加または変更
  - カタログの作成とイメージの更新
  - 電源操作を実行する
- 権限のないホスト接続が権限ありに変更されると、既存のホスティング接続が再度有効になります。

はじめに

サイトを作成するときに、ホスティングリソースへの最初の接続をオプションで作成できます。後で、その接続を変更したり、他の接続を作成したりできます。接続の構成には、サポートされているハイパーバイザーの中から接続タイプを選択すること、およびその接続のリソースから選択するストレージとネットワークが含まれます。

読み取り専用管理者は、接続とリソースの詳細を表示できます。接続とリソースの管理タスクを実行するには、完全な管理者である必要があります。詳細については、「委任管理」を参照してください。

接続タイプに関する情報の場所

サポートされている仮想化プラットフォームを使用して、Citrix Virtual AppsまたはCitrix Virtual Desktops環境でマシンをホストおよび管理できます。「システム要件」の記事に、サポートされている種類が記載されています。

詳細については、以下の情報源を参照してください。

- **XenServer (旧シトリックス ハイパーバイザー™):**
  - XenServer仮想化環境。
  - XenServer®ドキュメント。
- **ニュータニックス アクロポリス:**
  - Nutanix仮想化環境。
  - Nutanixドキュメント。
- **ヴイエムウェア:**
  - VMware仮想化環境。
  - VMware製品ドキュメント。
- **Microsoft ハイパーV:**
  - Microsoft System Center Virtual Machine Manager 仮想化環境の記事。
  - Microsoft ドキュメント。
- **パブリッククラウドホスト接続（AWS、Google Cloud、Microsoft Azure、Nutanix Cloudおよびパートナーソリューション、VMware Cloudおよびパートナーソリューション）：** パブ

リッククラウドホストに関する情報については、「リソースタイプのセットアップ」を参照してください。

> **注:**
>
> 情報源はCitrix DaaS™のドキュメントを参照するよう指示しています。Citrix DaaS製品のパブリッククラウドホストに慣れている場合、オンプレミスバージョンにはいくつかの違いがあります。オンプレミスのVirtual Apps and Desktopsでは、管理インターフェイスはWeb Studioとして知られています。更新はサービスに約4週間ごとに展開されます。そのため、サービスで利用可能な特定の機能がオンプレミスバージョンでは利用できない場合があります。

ホストストレージ

サポートされているハイパーバイザーによって管理されている場合、ストレージ製品はサポートされます。Citrix Supportは、これらのストレージ製品ベンダーが問題のトラブルシューティングと解決を支援し、必要に応じてナレッジセンターにそれらの問題を文書化します。

マシンをプロビジョニングする際、データはタイプ別に分類されます。

- マスターイメージを含むオペレーティングシステム（OS）データ。
- 一時データ。このデータには、MCSプロビジョニングマシンに書き込まれるすべての非永続データ、Windowsページファイル、ユーザープロファイルデータ、およびShareFileと同期されるすべてのデータが含まれます。このデータは、マシンが再起動するたびに破棄されます。

各データタイプに個別のストレージを提供することで、各ストレージデバイスの負荷を軽減し、パフォーマンスを向上させ、ホストの利用可能なリソースを最大限に活用できます。また、異なるデータタイプに適切なストレージを使用できるようになります。一部のデータでは、永続性と回復性が他のデータよりも重要です。

ストレージは共有（中央に配置され、どのホストからも独立しており、すべてのホストで使用される）することも、ハイパーバイザーにローカルに配置することもできます。たとえば、中央共有ストレージは、1つ以上のWindows Server 2012クラスター化ストレージボリューム（接続ストレージの有無にかかわらず）、またはストレージベンダーのアプライアンスである場合があります。中央ストレージは、ハイパーバイザーストレージ制御パスやパートナープラグインを介した直接アクセスなど、独自の最適化を提供する可能性もあります。

一時データをローカルに保存することで、共有ストレージにアクセスするためにネットワークを介する必要がなくなります。また、共有ストレージデバイスの負荷も軽減されます。共有ストレージはより高価になる可能性があるため、データをローカルに保存することで費用を削減できます。これらの利点は、ハイパーバイザーサーバー上の十分なストレージの可用性と比較検討する必要があります。

接続を作成する際、ハイパーバイザー間で共有されるストレージ、またはハイパーバイザーにローカルなストレージの2つのストレージ管理方法のいずれかを選択します。

1つ以上のXenServerホストで一時データストレージにローカルストレージを使用する場合、プール内の各ストレージの場所に一意の名前があることを確認してください。（XenCenter®で名前を変更するには、ストレージを右クリックして名前プロパティを編集します。）

ハイパーバイザーで共有されるストレージ

ハイパーバイザー間で共有されるストレージ方式は、長期的な永続性が必要なデータを中央に保存し、一元的なバックアップと管理を提供します。このストレージにはOSディスクが格納されます。

この方法を選択すると、一時的なマシンデータにローカルストレージ（同じハイパーバイザープール内のサーバー上）を使用するかどうかを選択できます。この方法は、共有ストレージ内のデータほど永続性や回復性を必要としません。これは*一時データキャッシュ*と呼ばれます。ローカルディスクは、メインOSストレージへのトラフィックを削減するのに役立ちます。このディスクは、マシンが再起動するたびにクリアされます。ディスクはライトスルーメモリキャッシュを介してアクセスされます。一時データにローカルストレージを使用する場合、プロビジョニングされたVDAは特定のハイパーバイザーホストに紐付けられます。そのホストが故障すると、VMは起動できません。

例外: Microsoft System Center Virtual Machine Managerは、クラスター共有ボリューム（CSV）を使用する場合、ローカルストレージ上の一時データキャッシュディスクを許可しません。

一時データをローカルに保存するための接続を作成し、各VMのキャッシュディスクサイズとメモリサイズの非デフォルト値を有効にして構成します。デフォルト値は接続タイプに合わせて調整されており、ほとんどのケースで十分です。詳細については、「マシンカタログの作成」を参照してください。

ハイパーバイザーは、ディスクイメージをローカルで読み取りキャッシュすることにより、最適化テクノロジーを提供することもできます。たとえば、XenServerはIntelliCache™を提供し、中央ストレージへのネットワークトラフィックを削減します。

ハイパーバイザーのローカルストレージ

ハイパーバイザーにローカルなストレージ方式では、データをハイパーバイザーにローカルに保存します。この方式では、マスターイメージやその他のOSデータがサイト内のハイパーバイザーに転送されます。このプロセスは、最初のマシン作成時と将来のイメージ更新時に発生します。このプロセスにより、管理ネットワークでかなりのトラフィックが発生します。イメージ転送には時間がかかり、イメージは各ホストで異なるタイミングで利用可能になります。

接続とリソースを作成する

サイトの作成時に、最初の接続をオプションで作成できます。サイト作成ウィザードには、以下のセクションで説明する接続関連のページが含まれています。

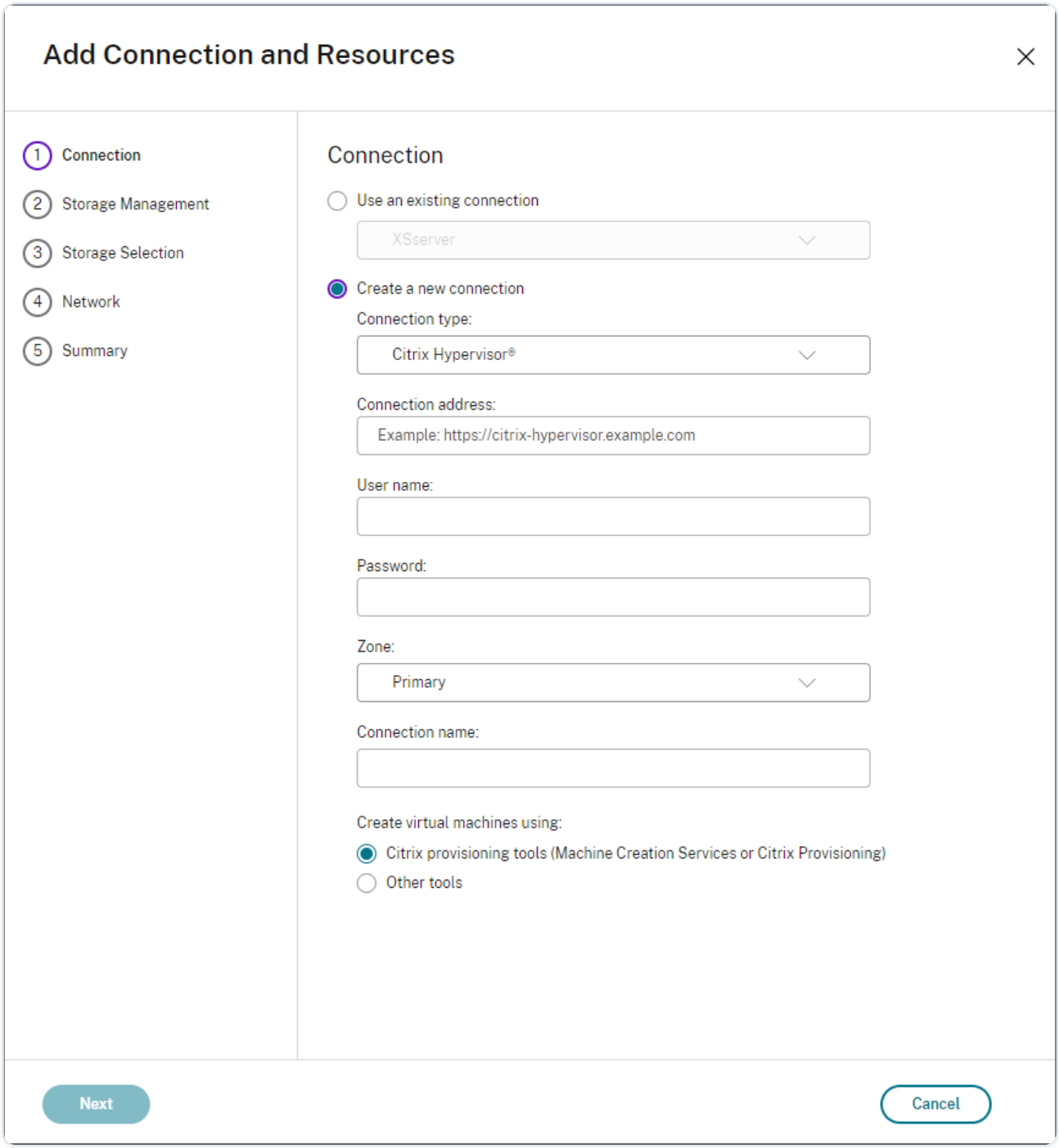
サイトの作成後に接続を作成する場合は、手順1から開始します。

> **重要:**

> 接続を作成する前に、ホストリソース（ストレージとネットワーク）が利用可能である必要があります。

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. アクションバーで を選択します。
4. ウィザードは、以下のページ（特定のページの内容は選択した接続タイプによって異なります）を案内します。各ページを完了したら、 をクリックして ページに進みます。

接続



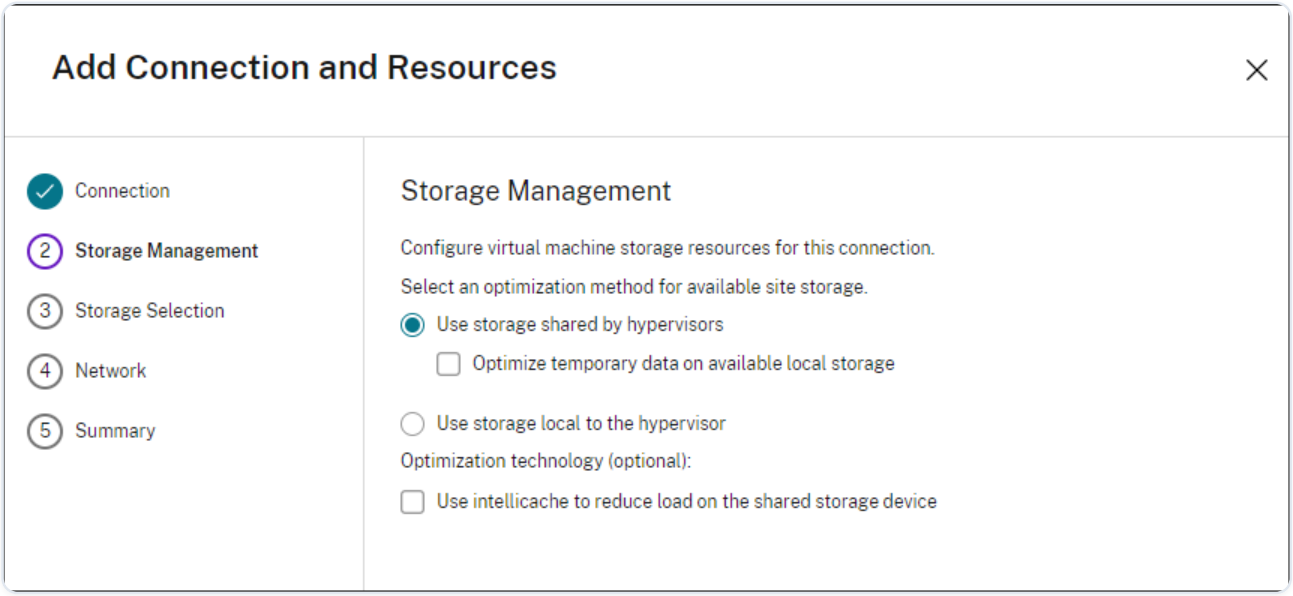
「**接続**」ページで：

- 接続を作成するには、 を選択します。既存の接続と同じホスト構成に基づいて接続を作成するには、 を選択し、関連する接続を選択します。
- フィールドで、使用しているハイパーバイザーを選択します。パブリッククラウドホスト接続は、Hybrid Rights Licenseを使用している場合にのみドロップダウンリストに表示されます。または、PowerShellコマンド `Get-HypHypervisorPlugin [-ZoneUid] $rluid [-IncludeUnavailable]` false/true を使用して、以下を取得できます。

  - サードパーティ製プラグインを含む、Citrixがサポートするすべてのハイパーバイザープラグインのリスト。
  - ハイパーバイザープラグインの可用性。可用性ステータスが**false**の場合、ハイパーバイザープラグインが正しくインストールされていないか、ハイブリッド権限ライセンスが付与されていない可能性があります。

- 接続アドレスと資格情報フィールドは、選択した接続タイプによって異なります。要求された情報を入力します。
- 接続名を入力します。この名前はWeb Studioに表示されます。
- 仮想マシンの作成に使用するツールを選択します: Web Studioツール (Machine Creation Services™ や Citrix Provisioning など) またはその他のツール。

ストレージ管理



ストレージ管理の種類と方法については、「ホストストレージ」を参照してください。

Hyper-V または VMware ホストへの接続を構成している場合は、クラスター名を参照して選択します。その他の接続タイプでは、クラスター名は要求されません。

ストレージ管理方法を選択します。ハイパーバイザーによって共有されるストレージ、またはハイパーバイザーにローカルなストレージ。

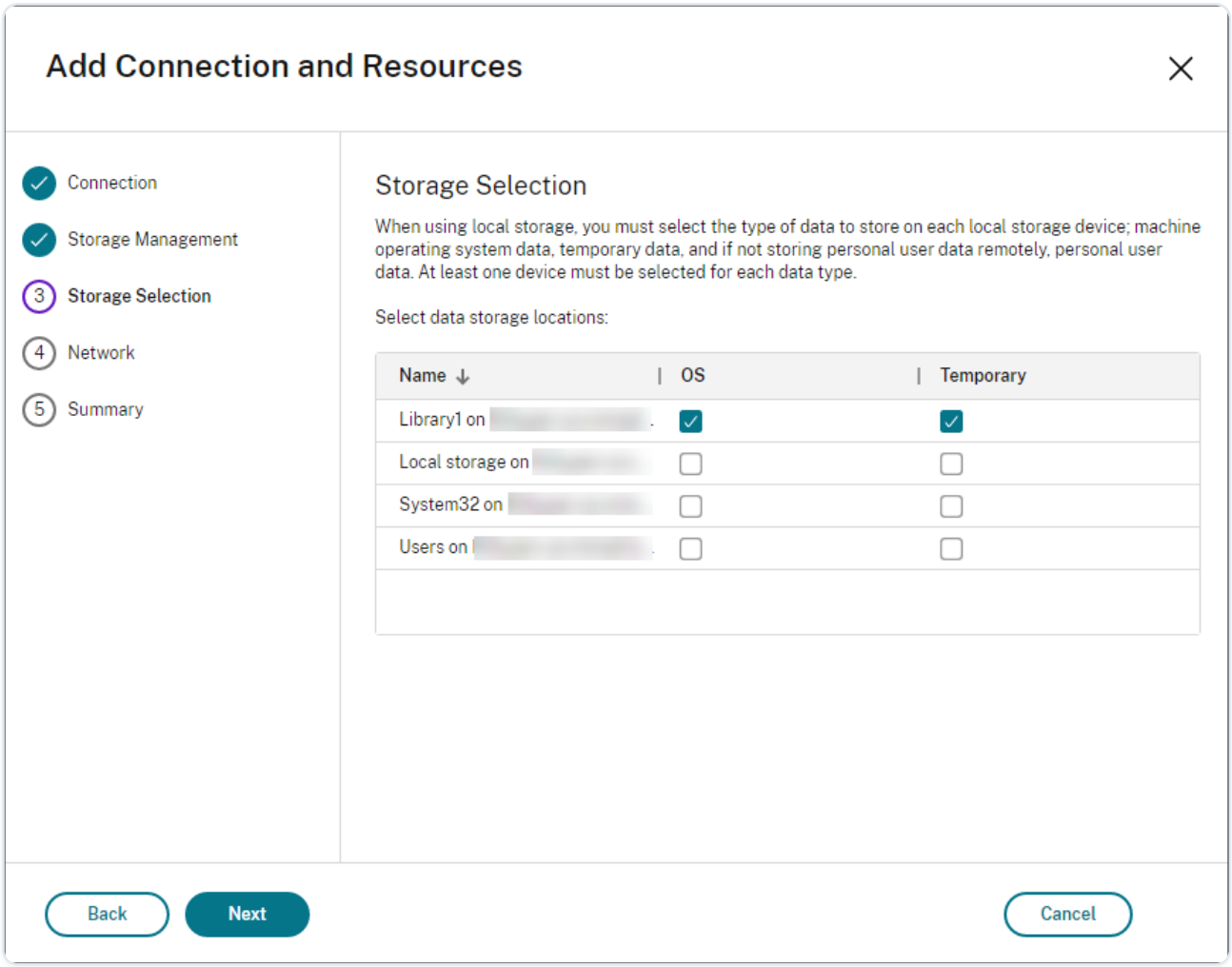
- ハイパーバイザーで共有されるストレージを選択した場合、利用可能なローカルストレージに一時データを保持するかどうかを指定します。（この接続を使用するマシンカタログで、デフォルト以外のサイズの一時ストレージを指定できます。）**例外：** クラスター共有ボリューム（CSV）を使用する場合、Microsoft System Center Virtual Machine Managerはローカルストレージ上の一時データキャッシュディスクを許可しません。Web Studioでそのストレージ管理設定を構成すると失敗します。

XenServer プールで共有ストレージを使用する場合、共有ストレージデバイスの負荷を軽減するために IntelliCache を使用するかどうかを指定します。「XenServer 接続で IntelliCache を使用する」を参照してください。

注:

XenServer、VMware、およびSCVMM仮想化環境では、OSディスクと同じストレージ場所にライトバックキャッシュ（WBC）ディスクを配置できます。この場合、**利用可能なローカルストレージで一時データを最適化する**を選択しないでください。

ストレージの選択



ストレージの選択の詳細については、「ホストストレージ」を参照してください。

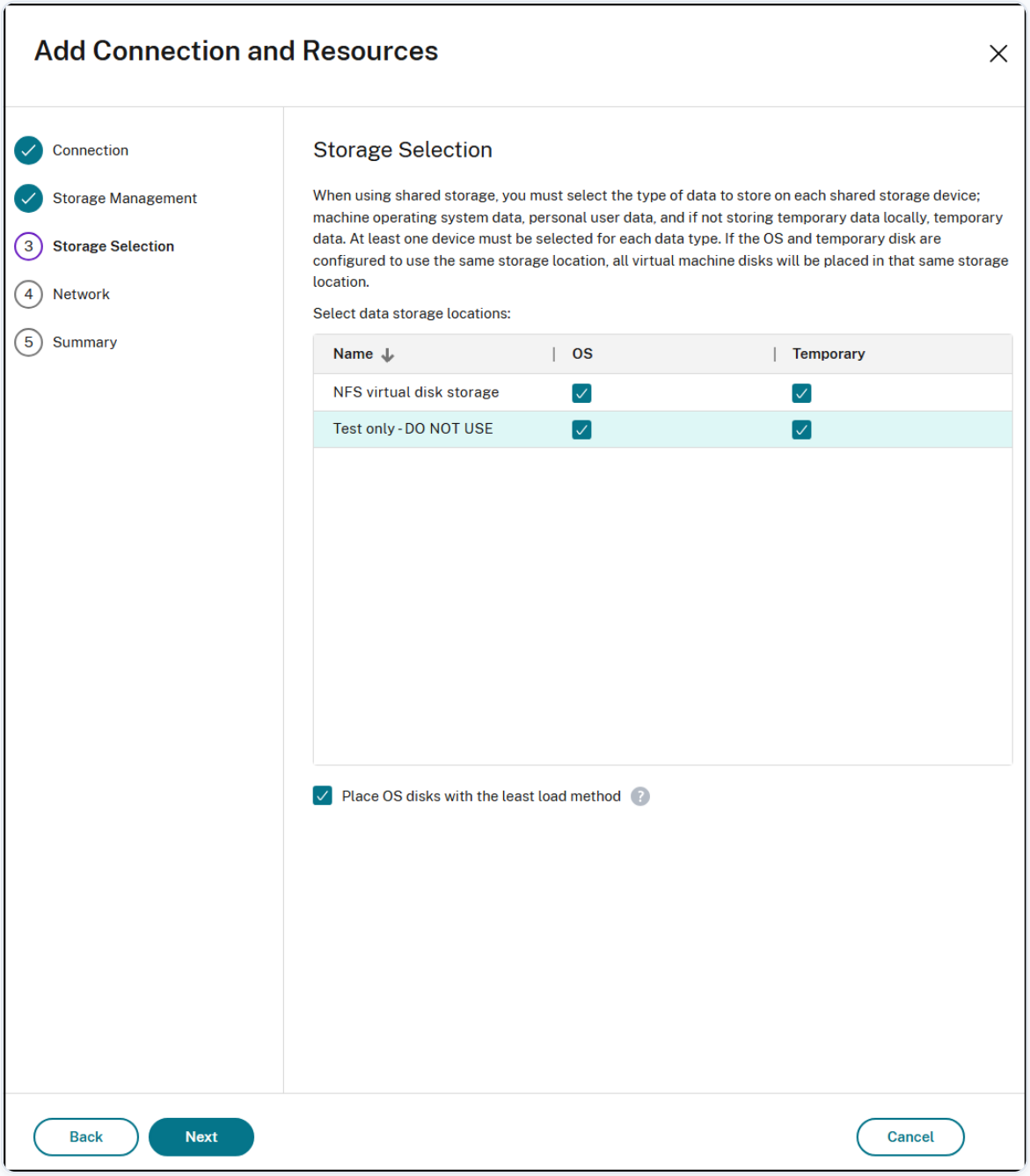
利用可能なデータタイプごとに、少なくとも1つのホストストレージデバイスを選択します。前のページで選択したストレージ管理方法によって、このページで選択できるデータタイプが決まりま

す。ウィザードの次のページに進む前に、サポートされているデータタイプごとに少なくとも1つのストレージデバイスを選択してください。

注:

- XenServer、VMware、SCVMMの仮想化環境では、利用可能なOSストレージリストと利用可能な一時ストレージリストを同じに構成した場合、MCSはライトバックキャッシュ（WBC）ディスクをOSディスクと同じストレージ場所に配置します。
- 少なくとも2つ以上のOSデータストレージの場所を選択すると、**最小負荷方式でストレージの負荷分散を最適化する**オプションが表示されます。このオプションを使用する

と、ディスク割り当てのために最も負荷の低いストレージリポジトリを選択できます。



- **概要**ページには、選択に応じてオプションが**有効**か**無効**かが表示されます。**詳細**パネルには、ストレージ割り当て方法の変更が表示されます。**OSストレージ**ページの**ストレージの編集**オプションを使用して調整できます。または、PowerShellを使用して同じ目標を達成することもできます。VMの柔軟なストレージ場所オプションを参照してください。

ストレージ管理ページで**「ハイパーバイザーで共有されるストレージを使用」を選択し、「利用可能なローカルストレージで一時データを最適化」**を選択すると、**ストレージ選択**

> ページでより多くの構成オプションを利用できます。たとえば、一時データに使用するローカルストレージデバイス（同じハイパーバイザープール内）を選択できます。

現在選択されているストレージデバイスの数が表示されます (上記のグラフィックでは「1 storage device selected」)。そのエントリにカーソルを合わせると、選択されているデバイス名が表示されます。

1. 使用するストレージデバイスを変更するには、**選択**をクリックします。
2. **ストレージの選択**ダイアログボックスで、ストレージデバイスのチェックボックスをオンまたはオフにして、**OK**をクリックします。

ネットワーク

ネットワークページで、リソースの名前を入力します。この名前は、接続に関連付けられたストレージとネットワークの組み合わせを識別するためにWeb Studioに表示されます。

VMが使用するネットワークを1つ以上選択します。

概要

概要ページで、選択内容を確認します。完了したら、**完了**をクリックします。

注意: 一時データをローカルに保存すると、この接続を使用するマシンを含むマシンカタログを作成する際に、一時データストレージの非デフォルト値を構成できます。「マシンカタログの作成」を参照してください。

接続設定の編集

この手順を使用して接続の名前を変更したり、接続を作成したりしないでください。それらの接続は異なる操作です。現在ホストしているマシンに新しいアドレスがある場合にのみ、アドレスを変更してください。別のアドレスを別のマシンに入力すると、接続のマシンカタログが破損します。

このリソースにアクセスするマシンカタログは、適切なGPU固有のマスターイメージを使用する必要があるため、接続の**GPU**設定を変更することはできません。接続を作成してください。

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. 接続を選択し、アクションバーで**接続の編集**を選択します。
4. 接続を編集する際に利用できる設定のガイダンスに従ってください。

5. 完了したら、**適用**をクリックして行った変更を適用し、ウィンドウを開いたままにするか、**保存**をクリックして変更を適用し、ウィンドウを閉じます。

接続プロパティページ:

- 接続アドレスと資格情報を変更するには、**設定の編集...**を選択し、新しい情報を入力します。
- XenServer接続の高可用性サーバーを指定するには、**サーバーの編集...**を選択し、サーバーを選択します。Citrixでは、プールマスターに障害が発生した場合にXenServerとの通信を可能にするため、プール内のすべてのサーバーを選択することをお勧めします。

> **注:**
>
> HTTPSを使用しており、高可用性サーバーを構成したい場合は、プール内のすべてのサーバーにワイルドカード証明書をインストールしないでください。各サーバーには個別の証明書が必要です。

詳細設定ページ:

- Remote PC Accessで使用されるMicrosoft System Center Configuration Manager (ConfMgr) Wake on LAN接続タイプの場合、**ConfMgr Wake Proxy**、マジックパケット、およびパケット送信情報を入力します。
- スロットリングしきい値設定を使用すると、接続で許可される最大電源アクション数を指定できます。これらの設定は、電源管理設定が同時に起動するマシンが多すぎたり少なすぎたりする場合に役立ちます。各接続タイプには、ほとんどのケースに適した特定のデフォルト値があり、変更してはなりません。
- **同時アクション (すべてのタイプ)** 設定では、この接続で同時に発生できる最大絶対数と、この接続を使用するすべてのマシンの最大割合という2つの値を指定します。絶対値とパーセンテージ値の両方を指定する必要があります。実際に適用される制限は、これらの値のうち小さい方です。

  たとえば、34台のマシンがある展開で、**Simultaneous actions (all types)**が絶対値10、パーセンテージ値10に設定されている場合、適用される実際の制限は3です（つまり、34の10パーセントを最も近い整数に丸めたもので、絶対値10台のマシンよりも小さい）。
- **Maximum new actions per minute**は絶対数です。パーセンテージ値はありません。
- 「**接続オプション**」フィールドには、Citrixサポート担当者の指示または明示的なドキュメントの指示がある場合にのみ情報を入力してください。

共有テナントページ:

この接続のサブスクリプションとAzure Compute Galleryを共有するテナントとサブスクリプションを追加します。これにより、カタログを作成または更新する際に、それらのテナントとサブスクリプションから共有イメージを選択できます。

- この接続に関連付けられているアプリケーションの**アプリケーションID**と**アプリケーションシークレット**を入力します。この情報を使用して、Azureに認証できます。セキュリティを確保するために、定期的にキーを変更することをお勧めします。
- 共有テナントとサブスクリプションを指定します。最大8つの共有テナントを追加できます。各テナントにつき、最大8つのサブスクリプションを追加できます。
- 完了したら、**保存**と**適用**をクリックします。

「**接続オプション**」フィールドには、Citrixサポート担当者の指示がある場合にのみ情報を入力してください。

ネットワークの編集

接続のネットワークを変更できます。次の手順を実行します。

1. に移動します。
2. 接続の下にあるターゲットリソースを選択し、アクションバーで を選択します。
3. 仮想マシンが使用するネットワークを1つ以上選択します。
4. 変更を保存して終了するには、**保存**をクリックします。

接続のメンテナンスモードをオンまたはオフにする

接続のメンテナンスモードをオンにすると、新しい電源操作が接続に保存されているマシンに影響を与えるのを防ぎます。ユーザーは、マシンがメンテナンスモードの場合、マシンに接続できません。ユーザーがすでに接続している場合、メンテナンスモードはログオフ時に有効になります。

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. 接続を選択します。メンテナンスモードをオンにするには、アクションバーで**Turn On Maintenance Mode**を選択します。メンテナンスモードをオフにするには、**Turn Off Maintenance Mode**を選択します。

個々のマシンに対してメンテナンスモードをオンまたはオフにすることもできます。また、マシンカタログまたはデリバリーグループ内のマシンに対してメンテナンスモードをオンまたはオフにすることもできます。

接続を削除する

接続を削除すると、多数のマシンが削除され、データが失われる可能性があります。影響を受けるマシン上のユーザーデータがバックアップされているか、不要であることを確認してください。

接続を削除する前に、以下を確認してください。

- すべてのユーザーが接続に保存されているマシンからログオフしていること。
- 切断されたユーザーセッションが実行されていないこと。
- プールされたマシンと専用マシンのメンテナンスモードがオンになっていること。
- 接続で使用されているマシンカタログ内のすべてのマシンは電源がオフになります。

カタログによって参照されている接続を削除すると、マシンカタログは使用できなくなります。この接続がカタログによって参照されている場合、カタログを削除するオプションがあります。カタログを削除する前に、他の接続で使用されていないことを確認してください。

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. 接続を選択し、アクションバーで**接続の削除**を選択します。
4. この接続にマシンが格納されている場合、マシンを削除する必要があるかどうかが尋ねられます。削除する場合は、関連付けられている Active Directory コンピューターアカウントをどうするかを指定します。

接続の名前を変更またはテストする

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. 接続を選択し、アクションバーで または を選択します。

TLS証明書の信頼をテストする

信頼されていない証明書が原因でホスト接続の停止が発生した場合、Web Studio で証明書を再信頼できます。再信頼するには：

1. 左ペインで**ホスティング**を選択します。

2. 証明書を再信頼する接続を右クリックし、 を選択します。
3. 次のウィンドウでパスワードを入力し、**保存**をクリックします。
    - 証明書を再信頼する必要がある場合、証明書を信頼するオプションを含む警告ダイアログボックスが表示されます。
    - 証明書がすでに信頼されている場合、証明書が信頼されていることを示す成功ダイアログボックスが表示されます。

接続上のマシンの詳細を表示する

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. 接続を選択し、アクションバーで**マシンの表示**を選択します。

上部のペインには、接続を介してアクセスされるマシンが一覧表示されます。マシンを選択すると、下部のペインにその詳細が表示されます。開いているセッションのセッション詳細も提供されます。

検索機能を使用して、マシンをすばやく見つけます。ウィンドウ上部のリストから保存された検索を選択するか、新しい検索を作成します。マシン名の全部または一部を入力して検索するか、高度な検索に使用する式を作成できます。式を作成するには、 をクリックし、プロパティと演算子のリストから選択します。

接続上のマシンを管理する

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. 接続を選択し、 ペインで を選択します。
4. アクションバーで次のいずれかを選択します。一部のアクションは、マシンの状態と接続ホストの種類によっては利用できません。

アクション	説明
起動	マシンが電源オフまたは一時停止状態の場合に起動します。
一時停止	マシンをシャットダウンせずに一時停止し、マシンリストを更新します。

アクション	説明
シャットダウン	オペレーティングシステムにシャットダウンを要求します。
強制シャットダウン	マシンを強制的に電源オフにし、マシンリストを更新します。
再起動	オペレーティングシステムにシャットダウンを要求し、その後マシンを再起動します。オペレーティングシステムがこれに応じられない場合、デスクトップは現在の状態のままになります。
メンテナンスモードを有効にする	マシンへの接続を一時的に停止します。この状態のマシンにはユーザーは接続できません。ユーザーが接続している場合、メンテナンスモードはログオフ時に有効になります。（上記のように、接続を介してアクセスされるすべてのマシンに対してメンテナンスモードをオンまたはオフにすることもできます。）
デリバリーグループから削除	Delivery GroupからマシンをDelivery Groupが使用するMachine Catalogからは削除されません。マシンは、ユーザーが接続していない場合にのみ削除できます。マシンを削除している間、ユーザーが一時的に接続できないようにするには、メンテナンスモードをオンにします。
削除	マシンを削除すると、ユーザーはそのマシンにアクセスできなくなり、マシンはMachine Catalogから削除されます。マシンを削除する前に、すべてのユーザーデータがバックアップされているか、不要になっていることを確認してください。マシンは、ユーザーが接続していない場合にのみ削除できます。マシンを削除している間、ユーザーが一時的に接続できないようにするには、メンテナンスモードをオンにします。

マシンのシャットダウンを伴う操作の場合、マシンが10分以内にシャットダウンしないと、電源がオフになります。シャットダウン中にWindowsが更新プログラムのインストールを試みると、更新が完了する前にマシンの電源がオフになるリスクがあります。

ストレージの編集

接続を使用するVMのオペレーティングシステムデータと一時データを保存するために使用されるサーバーのステータスを表示できます。また、各データタイプのストレージにどのサーバーを使用するかを指定することもできます。

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. 接続を選択し、アクションバーで**ストレージの編集**を選択します。
4. 左側のペインで、データタイプ（オペレーティングシステムまたは一時）を選択します。
5. 選択したデータタイプに対して、1つ以上のストレージデバイスのチェックボックスをオンまたはオフにします。
6. **OK**をクリックします。

リスト内の各ストレージデバイスには、その名前とストレージステータスが含まれています。有効なストレージステータスの値は次のとおりです。

- **使用中:** ストレージはマシンの作成に使用されています。
- **廃止済み:** ストレージは既存のマシンにのみ使用されています。このストレージには新しいマシンは追加されません。
- **未使用:** ストレージはマシンの作成に使用されていません。

現在**使用中**のデバイスのチェックボックスをオフにすると、そのステータスは**廃止済み**に変わります。既存のマシンはそのストレージデバイスを引き続き使用し（データを書き込むこともできます）、そのため、マシンの作成に使用されなくなった後でも、その場所がいっぱいになる可能性があります。

リソースの削除、名前の変更、またはテスト

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. リソースを選択し、アクションバーで適切なエントリ（**リソースの削除**、**リソースの名前変更**、または**リソースのテスト**）を選択します。

VMの柔軟なストレージ場所オプション

マシンカタログ内のVMには、さまざまなストレージサービス（SR）が割り当てられます。異なるストレージでのVM割り当てのバランスを取るには、2つのオプションがあります。

- **強化された現在のラウンドロビン割り当て方法**: MCS は、常に同じ固定 SR から開始するのではなく、最後に使用された SR の直後の SR から割り当てを開始します。
- **最小負荷ベースの割り当て方法**: 同じマシンカタログ内の各 SR の VM の総数を比較して決定される、現在の負荷が最も低い SR に VM を配置します。たとえば、マシンカタログに 100 台の VM が次のように分散されている場合（SR1 に 20 台、SR2 に 30 台、SR3 に 50 台）、新しい VM はまず SR1 に割り当てられます。この方法により、SR1、SR2、SR3 全体で負荷が分散されます。

この機能は次のとおりです。

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

負荷ベースの割り当てオプションを実装するには、ホスト接続の作成または更新時にカスタムプロパティ `Name="StorageBalanceType"` `Value="VMCountBasedLeastLoad` を追加します。このカスタムプロパティと値を使用しない場合、デフォルトで強化されたラウンドロビン方式が適用されます。

例:

- ホスト接続の作成時:

```
New-Item -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"><Property
xsi:type=`"StringProperty`" Name=`"StorageBalanceType`"
Value=`"VMCountBasedLeastLoad`" /></CustomProperties>"
-HypervisorConnectionName "Xen-Connection" -NetworkPath @("XDHyp:
\Connections\Xen-Connection\Network 0.network") -Path @("XDHyp:
\HostingUnits\XS-Network") -PersonalvDiskStoragePath @() -RootPath
"XDHyp:\Connections\Xen-Connection\" -StoragePath @("XDHyp:
\Connections\Xen-Connection\NFS virtual disk storage.storage")
```

- ホスト接続の更新時:

```
Set-Item  -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"><Property
xsi:type=`"StringProperty`" Name=`"StorageBalanceType`"
Value=`"VMCountBasedLeastLoad`" /></CustomProperties>" -Path @("XDHyp:
\HostingUnits\XS-Network")
```

孤立したAzureリソースの検出

孤立したリソースは、システム内に存在する使用されていないリソースであり、不要な費用につながる可能性があります。

クラウド管理者以外に、「**ホスト**」の下にある「**ハイパーバイザーでホスト接続を使用して孤立したリソースを検出する**」権限を持つ新しく作成された役割は、孤立したリソースを検出できます。

この機能を使用すると、Citrix Virtual Apps and Desktopsサイトのホストにある孤立したAzureリソースを検出できます。

Web Studioで次の手順を実行します。

1. 「**管理**」から、左ペインで「**ホスティング**」を選択します。
2. 接続を選択し、アクションバーで「**孤立したリソースの検出**」を選択します。「**孤立したリソースの検出**」ダイアログボックスには、孤立したリソースのレポートが表示されます。
3. 孤立したリソースのレポートを表示するには、「**レポートの表示**」を選択します。

または、PowerShellを使用して孤立したAzureリソースを検出できます。詳細については、「孤立したリソースのリストを取得する」を参照してください。

孤立したリソースの原因を理解し、その後の対処方法については、「Citrixで孤立したAzureリソースを効率的に管理する」を参照してください。

接続タイマー

ポリシー設定を使用して、3つの接続タイマーを構成できます。

- 「**最大接続タイマー**」：ユーザーデバイスと仮想デスクトップ間の途切れない接続の最大期間を決定します。「**セッション接続タイマー**」および「**セッション接続タイマー間隔**」ポリシー設定を使用します。

- 「**接続アイドルタイマー**」：ユーザーからの入力がない場合に、仮想デスクトップへの途切れないユーザーデバイス接続が維持される期間を決定します。「**セッションアイドルタイマー**」および「**セッションアイドルタイマー間隔**」ポリシー設定を使用します。
- **接続解除タイマー:** 接続が解除され、ロックされた仮想デスクトップが、セッションがログオフされるまでロックされたままになる時間を決定します。「**接続解除セッションタイマー**」および「**接続解除セッションタイマー間隔**」ポリシー設定を使用します。

これらの設定のいずれかを更新する場合は、展開全体で一貫性があることを確認してください。

詳細については、ポリシー設定のドキュメントを参照してください。

孤立したリソースのリストを取得する

MCS によって作成されたものの、MCS によって追跡されなくなった孤立したリソースのリストを取得できます。これは現在、Azure 環境に適用されます。リストを取得するには、PowerShell コマンドを使用できます。接続を使用してフィルタリングできます。

デフォルトでは、**フル管理者**および**クラウド管理者**の役割にこの権限が割り当てられています。他の役割にこのアクションを実行させるには、**ホスト**の下にある**ハイパーバイザーで孤立したリソースを検出するためにホスト接続を使用する**権限を割り当てます。詳しくは、「役割の作成と管理」を参照してください。

> **注:**
>
> - プロビジョニングまたはイメージの更新が進行中の場合、PowerShell コマンドは拒否されます。
> - すべてのCitrixタグが付けられた顧客管理リソースは、孤立リソースとして検出されます。ただし、そのリソースに値がtrueのCitrixDetectIgnoreという別のタグを追加すると、孤立リソースの検出中にそのリソースは無視されます。

制限事項

- 組み込みのフル管理者またはクラウド管理者ロールの管理者ユーザーのみが、PowerShellコマンドを実行して孤立リソースのリストを取得できます。
- 孤立したリソースの誤認識を避けるため、孤立したリソースをフィルタリングしている間はVMの電源を入れないでください。
- 負荷が高い可能性がある場合、約2,000件のレコードが孤立として表示されます。

孤立リソースのリストを表示するには：

1. **PowerShell**ウィンドウを開きます。
2. 次のコマンドを実行します。
    a. 接続UIDを取得します。接続UIDは、HypervisorConnectionUid属性の値です。

    ```
    Get-ChildItem xdhyp:\connections | where { $_.PluginId -like
    'Azure*' }"
    ```

    b. 孤立したリソースのリストを取得します。

    ```
    get-provorphanedresource -HypervisorConnectionUid <connection uid>
    ```

サブスクリプションIDから孤立リソースのリストを表示するには：

1. **PowerShell**ウィンドウを開きます。
2. 次のコマンドを実行します。
    a. サブスクリプションIDを使用して接続UIDを見つけます。接続UIDはHypervisorConnectionUid属性の値です。

    ```
    Get-ChildItem xdhyp:\connections | where { $_.CustomProperties
    -match '<subscriptionId>' }
    ```

    b. 孤立リソースのリストを取得します。

    ```
    get-provorphanedresource -HypervisorConnectionUid <connection uid>
    ```

注:

削除する前にリソースを慎重に確認してください。

ホスティング接続にWinHttp (netsh) プロキシサーバー設定を使用する

この機能強化により、ホスティング接続でWinHttp (netsh) プロキシサーバー設定をホスティング接続で使用できるようになります。これにより、プロキシ設定が簡素化され、他のCitrixサービスで使用されるプロキシ設定構成とも整合性が取れます。

この機能は、以下の仮想化環境に適用されます。

- XenServer
- グーグル クラウド
- マイクロソフト アジュール
- ニュータニックス
- レッドハット オープンシフト
- ヴイエムウェア

ホスティング接続にDelivery Controllerで構成されたWinHttp (netsh) プロキシサーバーを使用するには、このカスタムプロパティをホスティング接続に含めることができます。

```
<Property xsi:type="StringProperty"
Name="UseWinHttpProxyForHypervisorTraffic" Value="True" />
```

- このカスタムプロパティが`True`に設定されている場合、ハイパーバイザーへのAPI呼び出しは、`netsh winhttp set proxy`コマンドを介してマシンに設定されているWinHttpプロキシサーバーを経由してルーティングされます。
- このカスタムプロパティが`False`に設定されている場合、API呼び出しはDDCに構成されているすべてのプロキシサーバー（WinINetプロキシおよび.netプロキシを含む）を無視します。
- このカスタムプロパティがホスティング接続に存在しない場合、マシンの`WinINet`または`.net`プロキシサーバー構成が使用されます。これは既存の動作です。

ユースケース

- 例1：ホスティング接続にカスタムプロパティが設定されていない場合

  ホスティング接続は、WinINetプロキシ構成、続いて.netプロキシ構成を読み取り、構成されている場合はプロキシ設定を使用します。何も構成されていない場合は、直接接続が作成されます。これは既存の動作であり、引き続きそのまま機能します。

- 例2：ホスティング接続にカスタムプロパティが「True」に設定されている場合

  ホスティング接続はWinHttpプロキシ設定のみを読み取り、存在する場合はプロキシ設定を使用します。存在しない場合、ホスティング接続にはプロキシ設定は使用されません。

- 例3：カスタムプロパティがホスティング接続に値 = False で設定されている

  ホスティング接続は、マシン上のプロキシ構成設定を読み取らず、プロキシなしでハイパーバイザーへの接続を試行します。

前提条件

PowerShellを使用してホスト接続を作成する際にカスタムプロパティを設定する前に、すべてのDesktop Delivery ControllerでWinHTTPプロキシを構成していることを確認してください。

構成手順

CLIを介してWinHttpプロキシ設定を使用する新しいホスティング接続を作成するには：

```
$CustomProperties = "<CustomProperties  xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">

<!-- Include any other hypervisor specific custom properties here -->

<Property xsi:type=`"StringProperty`"
Name=`"UseWinHttpProxyForHypervisorTraffic`" Value=`"True`" />

</CustomProperties>"



New-Item -ConnectionType $ConnectionType -HypervisorAddress @('https://
hypervisorhost1.example.com') -Path @('XDHyp:\Connections\
$ConnectionName') -Password $Password -UserName $User -CustomProperties
$CustomProperties
```

既存のホスティング接続にカスタムプロパティを設定するには：

1. 既存のカスタムプロパティがホスティング接続に存在する場合は、それをコピーします。

   ```
   dir XDHyp:\Connections
   ```

2. ホスティング接続のカスタムプロパティをコピーし、以下を追加して変数に保存します。

   ```
   $CustomProperties

   <Property xsi:type=`"StringProperty`"
   Name=`"UseWinHttpProxyForHypervisorTraffic`" Value=`"True`" />
   ```

   例:

```
Example:

$CustomProperties = "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`"
Value=`"123`" />

<Property xsi:type=`"StringProperty`" Name=`"ManagementEndpoint`"
Value=`"https://management.azure.com/`" />

<Property xsi:type=`"StringProperty`" Name=`"AuthenticationAuthority`"
Value=`"https://login.microsoftonline.com/`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageSuffix`"
Value=`"core.windows.net`" />

<Property xsi:type=`"StringProperty`" Name=`"TenantId`"
Value=`"123abc`" />

<Property xsi:type=`"StringProperty`" Name=`"SharedTenants`"
Value=`"`[ { 'Tenant':'123abc', 'Subscriptions':['345', '567'] } ]`"` /
><Property xsi:type=`"StringProperty`"
Name=`"UseWinHttpProxyForHypervisorTraffic`" Value=`"True`" />

</CustomProperties>"
```

既存のカスタムプロパティが空だった場合は、カスタムプロパティを設定します。

```
$CustomProperties = "<CustomProperties  xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`"
Name=`"UseWinHttpProxyForHypervisorTraffic`" Value=`"True`" />

</CustomProperties>"
```

3. 既存のホスティング接続を更新するには、`Set-Item` コマンドを実行します。

```
Set-Item -CustomProperties $CustomProperties -LiteralPath @("XDHyp:
\Connections\$ConnectionName") -PassThru -UserName $User
-SecurePassword $Password
```

次のステップ

特定のホストタイプへの接続については、以下を参照してください。

- AWSへの接続
- XenServerへの接続
- Google Cloud環境への接続
- Microsoft Azureへの接続
- マイクロソフト システムセンター バーチャルマシンマネージャー への接続
- Nutanixへの接続
- Nutanixクラウドおよびパートナーソリューションへの接続
- VMwareへの接続
- VMwareクラウドおよびパートナーソリューションへの接続

初期展開プロセス中の場合は、マシンカタログを作成します。

Amulet Hotkey CoreStation への接続 (プレビュー)

(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/connections.html)では、接続を作成するための一般的なウィザードについて説明しています。以下の情報は、Amulet Hotkey CoreStationに固有の詳細を扱っています。現在、PowerShellコマンドを使用してAmulet Hotkey CoreStationへの接続を作成できます。

> **注:**
>
> Amulet Hotkey CoreStationへの接続を作成する前に、まずAmulet Hotkey CoreStationアカウントの設定を完了する必要があります。

接続を作成する

PowerShell コマンドを使用して、Amulet Hotkey CoreStation への接続を作成できます。

PowerShellコマンドを使用して接続を作成する場合、次の情報を提供します。

- IP: Amulet Hotkey CoreStation IPアドレス
- ユーザー名: Amulet Hotkey CoreStation ユーザー名
- パスワード: Amulet Hotkey CoreStation パスワード

例:

```
Get-ConfigZone

Get-HypHypervisorPlugin

New-Item `

    -ConnectionType "Custom" `

    -HypervisorAddress $IP `

    -Metadata
@{"Citrix_Orchestration_Hypervisor_Secret_Allow_Edit"="false"} `

    -Path @("XDHyp:\Connections\$connectionName") `

    -Persist `

    -PluginId "AmuletHotkeyCoreStationFactory" `

    -Scope @() `

    -SecurePassword $Password `

    -UserName $UserName `

    -ZoneUid $ZoneUid `

    -SslThumbprint $SslThumbprint

New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$HypervisorConnectionID
```

注:

> `-SslThumbprint` パラメーターは、プライベートCA署名証明書にのみ必要です。

証明書とサムプリントの検証

Amulet Hotkey CoreStationへの接続を正常に作成するには、証明書にエラーがなく、サムプリントが正しい値である必要があります。証明書とサムプリントの検証に関連するユースケースは次のとおりです。

- 公開CA署名証明書にエラーがあります。接続は正常に作成されません。エラーの詳細を確認し、問題を解決してください。
- エラーのないパブリックCA署名証明書。接続は正常に作成され、`SslThumbprints`の値は`Null`です。
- エラーがなく、`sslthumbprint`値を持つプライベートCA署名証明書。正しい`SslThumbprints`値で接続が正常に作成されます。
- サムプリント値が正しくないプライベートCA署名証明書。接続は正常に作成されません。
- エラーのないプライベートCA署名証明書。接続は正常に作成されました。接続の作成時に`SSlThumbprints`は`Null`です。`SSlThumbprints`の値はサイトサービスによって値に更新されます。

接続の管理

証明書の問題を修正する

証明書の問題が発生した場合、Citrix Virtual Apps and DesktopsはAmulet Hotkey CoreStation接続をブロックし、関連するAmulet Hotkey CoreStationノードでのワークロードの配信と管理を妨げます。ホスト接続リストの接続の横にエラーアイコンが表示されます。

特定の問題と解決策については、次の表を参照してください。

問題	解決策
パブリックCA署名証明書に証明書エラーが発生します。	接続をクリックし、**トラブルシューティング**タブを選択します。エラーの詳細を表示し、問題を解決します。
受信した証明書はプライベートCA署名済みであるか、期限切れです。	証明書のサムプリントを更新するには、ホスト接続を編集します。詳細な手順：

問題	解決策	
	1. 接続を選択し、**接続の編集**をクリックします。 2. **接続プロパティ**ページで、**設定の編集**をクリックします。 3. Amulet Hotkey CoreStationエンクロージャに接続するためのパスワードを入力し、**保存**をクリックします。 4. 表示される**警告**ページで、受信したサムプリントをサーバーのものと比較して、証明書の有効性を確認します。 5. 同じである場合は、**証明書を信頼する**を選択し、**OK**をクリックします。	

サムプリント値の更新

接続を作成した後、`Set-Item` PowerShellコマンドを使用して接続のサムプリント値を更新できます。サムプリント値を更新するには、次の手順に従います。

1. 接続の接続詳細を取得します。例：

```
Get-Item -LiteralPath xdhyp:\connections\AmuletCon-101
```

2. サムプリント値を更新します。例:

```
Set-Item -LiteralPath xdhyp:\connections\AmuletCon-101 -Username
Administrator -SslThumbprint xxxxxxxxxxx12AD048480631BB7AB10D69xxxxx
```

3. 更新されたサムプリント値を確認します。例:

```
Get-Item -LiteralPath xdhyp:\connections\AmuletCon-101
```

注:

`Set-Item` コマンドで誤ったサムプリント値を指定すると、更新は失敗します。

次のステップ

- 初期展開プロセス中の場合は、マシンカタログの作成を参照してください。
- Amulet Hotkey CoreStationの詳細については、「Amulet Hotkey CoreStationマシンカタログの作成」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- Amulet Hotkey CoreStation 仮想化環境

AWS EC2への接続

(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/connections.html)では、接続を作成するウィザードについて説明します。以下の情報では、AWSクラウド環境に固有の詳細について説明します。

前提条件

AWS EC2への接続を作成する前に、以下を実行してください。

- AWSをリソースの場所として設定を完了します。(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/install-prepare/aws.html)を参照してください。
- Citrixがお客様に代わってAWSリソースを管理するためのIAMユーザーまたはロールの(#define-iam-permissions)ポリシー。

IAM権限を定義する

ホスト接続を作成する前に、Citrixがお客様のAWSアカウントでリソースをプロビジョニングおよび管理するための適切なアクセス許可を付与するIAMアクセス許可ポリシーを、IAMユーザーまたはロールに対して適切に定義する必要があります。このセクションの情報を使用して、AWS上のCitrix Virtual Apps and DesktopsのIAMアクセス許可を定義します。AmazonのIAMサービスでは、複数のユーザーを持つアカウントが許可されており、それらのユーザーはさらにグループに編成で

きます。これらのユーザーは、アカウントに関連付けられた操作を実行する能力を制御するために、異なるアクセス許可を持つことができます。IAMアクセス許可の詳細については、「IAM JSONポリシーリファレンス」を参照してください。

新しいユーザーグループにIAM権限ポリシーを適用するには：

1. AWSマネジメントコンソールにログインし、ドロップダウンリストから**IAMサービス**を選択します。
2. **新しいユーザーグループの作成**を選択します。
3. 新しいユーザーグループの名前を入力し、**続行**を選択します。
4. **権限**ページで、**カスタムポリシー**を選択し、次に**選択**を選択します。
5. **権限ポリシー**の名前を入力します。
6. **ポリシー ドキュメント**セクションで、関連する権限を入力します。

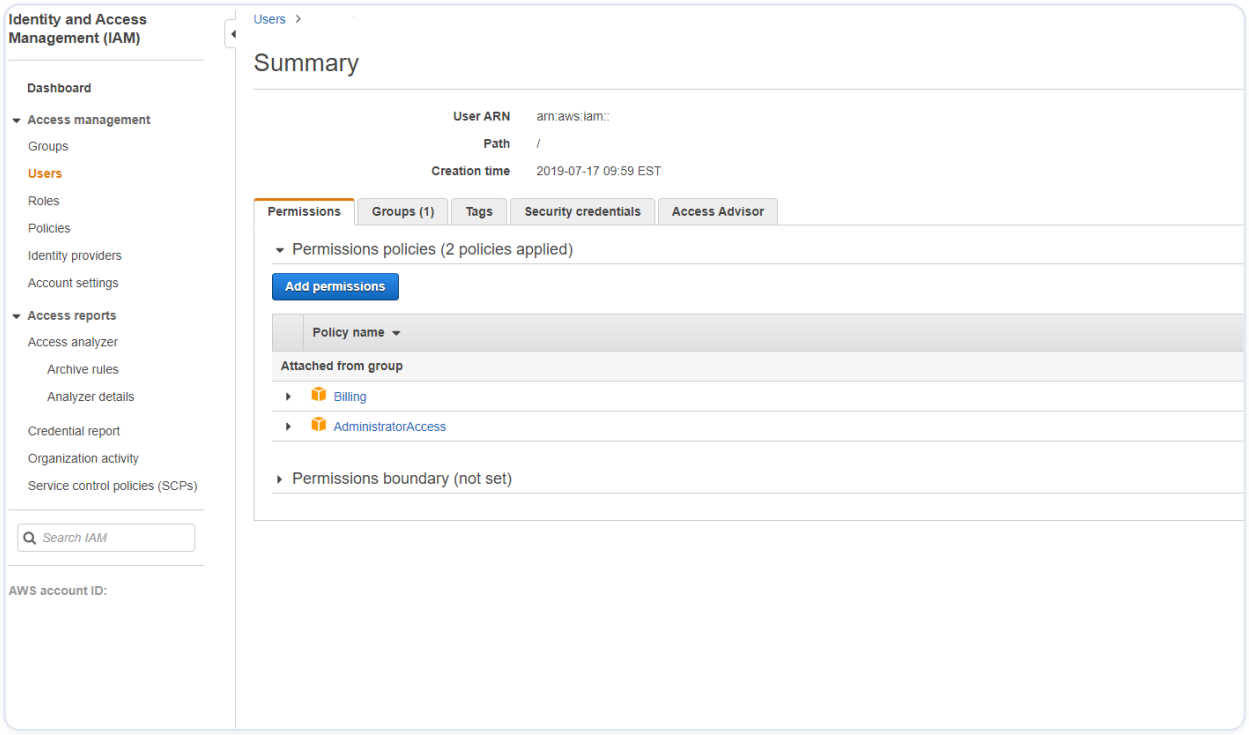
ポリシー情報を入力したら、**続行**を選択して、IAMアクセス許可ポリシーをユーザーグループに適用するプロセスを完了します。グループ内のユーザーには、Citrix Virtual Apps and Desktopsに必要なアクションのみを実行するアクセス許可が付与されます。

> **重要:**
>
> この記事の例で提供されているポリシーテキストを使用して、Citrix Virtual Apps and DesktopsがAWSアカウント内でアクションを実行するために使用するアクションを、それらのアクションを特定のリソースに制限することなくリストします。Citrixは、テスト目的でこの例を使用することをお勧めします。実稼働環境では、リソースにさらなる制限を追加することを選択できます。

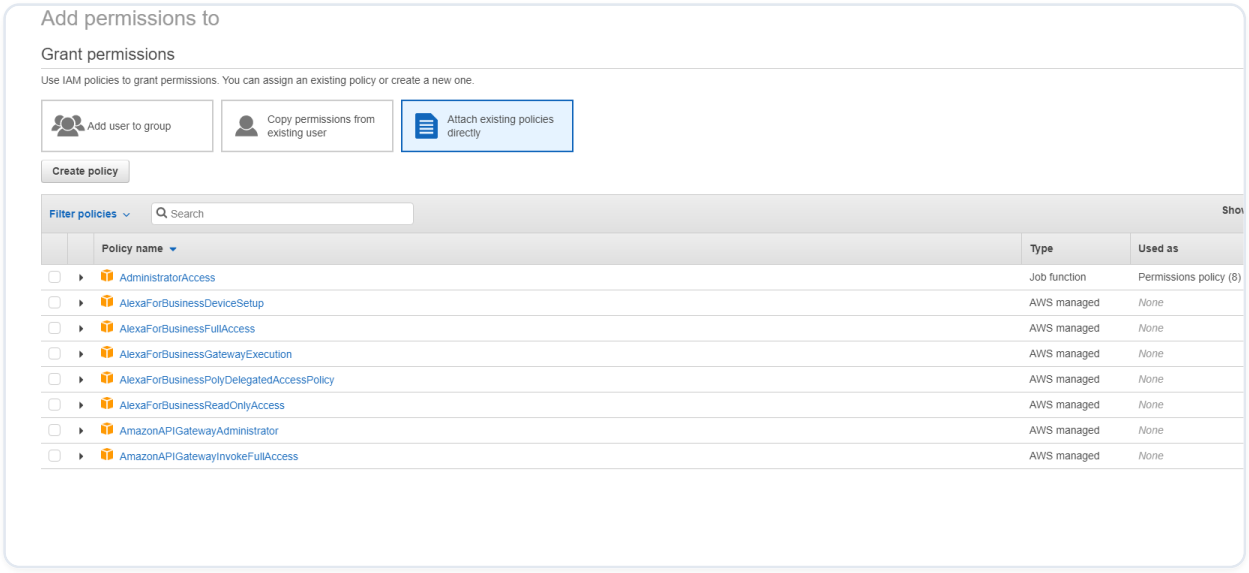
IAMアクセス許可を追加する

AWSマネジメントコンソールの**IAM**セクションでアクセス許可を追加します。

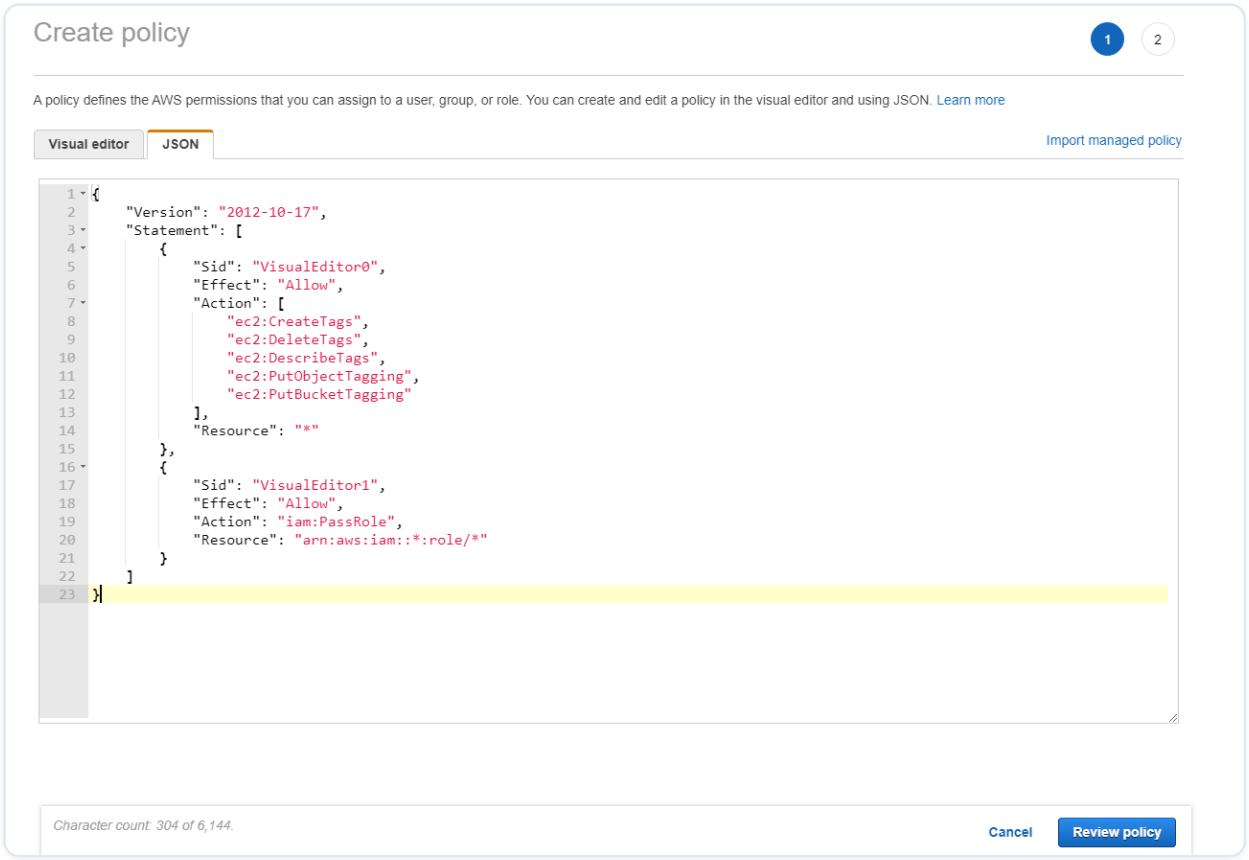
1. **概要**パネルで、**アクセス許可**タブを選択します。
2. **アクセス許可の追加**を選択します。



3. **アクセス許可の追加先**画面で、アクセス許可を付与します。



4. JSONセクションで、お使いの環境の必要なAWSアクセス許可を含めます。



接続を作成する

Amazon EC2への接続は、以下を使用して作成できます。

- ウェブスタジオ
- 「PowerShell コマンド」(#create-a-connection-using-powershell)

> **注:**
>
> プロキシサーバーまたはファイアウォールの制限を確認し、次のアドレスに接続できることを確認してください: `https://*.amazonaws.com`。また、Citrix Gateway service connectivity に記載されているすべてのアドレスに接続できることを確認してください。

> これらのアドレスに接続できない場合、ホスト接続の作成または更新中に障害が発生する可能性があります。

Web Studioを使用した接続の作成

1. **Hosting > Add Connection and Resources** ページに移動します。
2. **接続**ページで、以下の手順に従って接続を構成します。

a. **新しい接続を作成**を選択します。

b. **ゾーン**で、AWS 環境用に設定したリソースの場所を選択します。

c. 接続タイプとして **Amazon EC2** を選択します。

d. リソースをプロビジョニングする方法のいずれかを選択します。

- 「**このAWSアカウントを使用してリソースをプロビジョニングする**」を選択した場合は、「**IAMユーザーアクセスキーを使用する**」または「**IAMロールを使用する**」を選択します。IAMユーザーアクセスキーの場合は、CitrixがAWSアカウントのリソースを管理するための適切なIAMアクセス許可ポリシーを持つIAMユーザーの**APIキー**と**シークレットキー**を入力します。IAMロールの場合は、CitrixがAWSアカウントのリソースを管理するための適切なIAMアクセス許可ポリシーを持つIAMロールをDelivery Controllerインスタンスに割り当てていることを確認してください。詳細については、「ロールベース認証ガイド」を参照してください。
- 「**クロスアカウントアクセスを使用してリソースをプロビジョニングする**」を選択した場合は、Account AのDelivery Controllerが引き受けてプロビジョニング操作を実行する必要があるAccount BのIAMロールの**ARN**を入力します。

e. 接続名を入力し、**次へ**をクリックします。

3. **仮想マシンの場所**ページで、VMをプロビジョニングする必要がある場所を指定します。新しいVMを作成するためのクラウドリージョン、VPC、およびアベイラビリティゾーンを選択します。
4. 「**ネットワーク**」ページで:

a. 以前にアベイラビリティゾーンまたはローカルゾーンで選択したリソースの名前を入力します。

b. 前のメニューで構成したVPC内のサブネットを1つ以上選択します。

5. 残りのページを**概要**ページまでクリックして進みます。
6. **完了**をクリックして、Amazon EC2へのホスト接続を作成します。

重要な考慮事項

Studioを使用して接続を作成する場合:

- CitrixがAWSリソースを管理するための適切なIAM権限を定義します。
- CitrixがAWSリソースを管理するためにIAMユーザーアクセスキーを使用する場合、APIキーとシークレットキーの値を指定する必要があります。これらの値を含むキーファイルをAWSからエクスポートし、インポートできます。また、リージョン、アベイラビリティゾーン、VPC

名、サブネットアドレス、ドメイン名、セキュリティグループ名、および資格情報も指定する必要があります。

- CitrixがAWSリソースを管理するためにIAMロールを使用する場合、すべてのDelivery Controllerに適切なIAMアクセス許可を持つロールを割り当てる必要があります。詳細については、「ロールベース認証ガイド」を参照してください。
- ルートAWSアカウントの資格情報ファイル（AWSコンソールから取得）は、標準のAWSユーザー用にダウンロードされた資格情報ファイルと同じ形式ではありません。そのため、Citrix Virtual Apps and Desktopsは、このファイルを使用してAPIキーとシークレットキーのフィールドに入力することはできません。AWS Identity Access Management (IAM) 資格情報ファイルを使用していることを確認してください。
- ゾーンはアベイラビリティゾーンまたはローカルゾーンのいずれかです。

PowerShellを使用して接続を作成する

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*`を実行します。
3. 次のコマンドを実行します。以下に例を示します。

```
$connectionName = "demo-hostingconnection"

$cloudRegion = "us-east-1"

$apiKey = "aaaaaaaaaaaaaaaaaaaa"

$apiSecret = “bbbbb”

$secureKey = ConvertTo-SecureString -String $apiSecret

$zoneUid = "00000000-0000-0000-0000-000000000000"

$connectionPath = "XDHyp:\Connections\" + $connectionName



$connection = New-Item -Path $connectionPath -ConnectionType "<name of
the connection>" -HypervisorAddress " "@("https://ec2.cn-
north-1.amazonaws.com.cn") -Persist -Scope @() -UserName $apiKey
-SecurePassword $secureKey -ZoneUid $zoneUid
```

```
New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$connection.HypervisorConnectionUid



$hostingUnitName = "demo-hostingunit"

$availabilityzone = "us-east-1a"

$vpcName = "Default VPC"

$jobGroup = [Guid]::NewGuid()

$hostingUnitPath = "XDHyp:\HostingUnits\" + $HostingUnitName

$rootPath = $connectionPath + "\" + $vpcName + ".virtualprivatecloud\"

$availabilityZonePath = @($rootPath + $availabilityzone +
".availabilityzone")

$networkPaths = (Get-ChildItem $availabilityZonePath[0] | Where
ObjectType -eq "Network") | Select-Object -ExpandProperty FullPath #
will select all the networks in the availability zone



New-Item -Path $hostingUnitPath -AvailabilityZonePath
$availabilityZonePath -HypervisorConnectionName $connectionName
-JobGroup $jobGroup -PersonalvDiskStoragePath @() -RootPath $rootPath
-NetworkPath $networkPaths
```

注:

ロールベース認証を使用して接続を作成するには、apiKey と apiSecret を `role_based_auth` として指定します。

制限事項

AWS コンソールで AWS Virtual Private Cloud (VPC) の名前を変更すると、Citrix Cloud™ の既存のホスティングユニットが破損します。ホスティングユニットが破損すると、カタログを作成した

り、既存のカタログにマシンを追加したりできなくなります。この問題を解決するには、AWS VPC の名前を元の名前に戻します。

クロスアカウントプロビジョニング

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

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

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

Delivery Controllerがセカンダリアカウントのリソースにアクセスできるようにするには、セカンダリアカウントからIAMロールを引き受けた後、ホスト接続を作成します。

前提条件

クロスアカウントプロビジョニング用のホスト接続を作成する前に、以下を設定してください。

- VPCピアリングを設定し、両方のリージョンまたはアカウントでセキュリティグループを構成します。(#set-up-vpc-peering)を参照してください。
- IAMロールを使用してクロスアカウントアクセスを委任します。(#delegate-cross-account-access-using-iam-roles)を参照してください。

VPCピアリングを設定する

VPC Aがプライマリアカウント（アカウントA）にあり、Delivery ControllerとActive Directoryがあると仮定します。VPC Bは、VMをプロビジョニングするセカンダリアカウント（アカウントB）にあります。

アカウントAとアカウントBの間でVPCピアリング接続を設定するには、次の手順を実行します。

1. VPCピアリング接続を作成します。参照：
    - 異なるアカウント、同じリージョン

- 異なるアカウント、異なるリージョン

2. VPC Aに移動し、パブリックサブネットに関連付けられているルートテーブルに移動します。
3. **>** をクリックします。 列にVPC BのCIDRブロックを追加し、 列に作成したVPCピアリングを追加します。
4. 手順2と3を繰り返しますが、VPC AとVPC Bのプライベートサブネットを使用します（VPC AのCIDRブロックを追加します）。VPCピアリング接続のルートテーブルを更新するを参照してください。
5. VPC Aに関連付けられているプライベートセキュリティグループに移動します。
6. を選択し、 を選択します。
7. を選択します。タイプには を選択し、 列に以下を追加します。
   - 異なるリージョンの場合は、VPC B の CIDR ブロックを追加します。
   - 異なるアカウントだが同じリージョンの場合は、VPC B のアカウント ID とプライベートセキュリティグループ ID をスラッシュで区切って追加します (例: 123456789012/sg-1a2b3c4d)。
8. ステップ 5 から 7 を繰り返しますが、VPC B のプライベートセキュリティグループを使用します (ただし、VPC A の CIDR ブロック、または同じリージョンだが異なるアカウントの VPC A のアカウント ID とプライベートセキュリティグループ ID を追加します)。ピアセキュリティグループを参照するようにセキュリティグループを更新するを参照してください。

> **注:**
>
> VPC ピアリング接続の作成に料金はかかりません。ただし、アベイラビリティーゾーン内の VPC ピアリングは無料ですが、VPC ピアリング接続を介したデータ転送が複数のアベイラビリティーゾーンやリージョンをまたいで行われる場合、料金が発生します。VPC ピアリング接続の料金を参照してください。

IAM ロールを使用してクロスアカウントアクセスを委任する

アカウント間で VPC ピアリングを設定した後、IAM ロールを使用してクロスアカウントアクセスを委任します。

IAMロールを使用したクロスアカウントアクセスにより、プライマリアカウント（デリバリーコントローラーアカウント）がIAMロールを引き受けて、セカンダリアカウント（マシンカタログVM）内のAWSリソースにアクセスできるようになります。

クロスアカウントリソースにアクセスするには、次の手順を実行します。

> **注意:**
>
> 仮に、VPC Aはプライマリアカウント（アカウントA）にあり、デリバリーコントローラーとActive Directoryがあります。VPC Bは、VMをプロビジョニングしたいセカンダリアカウント（アカウントB）にあります。

1. 前述の手順で、アカウント間で VPC ピアリングを設定します。
2. 最小限の Citrix IAM 権限を持つ IAM ロールとポリシーをアカウント B に作成します。IAM チュートリアル: IAM ロールを使用して AWS アカウント間でアクセスを委任するを参照してください。このロールの ARN は「arn:aws:iam::5678:role/citrix-role」であるとします。
3. ロール「arn:aws:iam::5678:role/citrix-role」に信頼ポリシーを追加し、アカウント A のロール「arn:aws:iam::1234:role/primary-account-citrix-role」からアクセスできるようにします。これは、IAM でのクロスアカウントリソースアクセスに従います。
4. アカウント A に、前述の名前「primary-account-citrix role」で IAM ロールとポリシーを作成します。これは、IAM ロールを引き受け、アカウント B からの IAM ロール (arn:aws:iam::5678:role/citrix-role) を渡すことができます。
5. アカウントAのすべてのDelivery Controllersに、ロール「arn:aws:iam::1234:role/primary-account-citrix-role」を割り当てます。

デリバリーコントローラーは、アカウントBからロール（"arn:aws:iam::5678:role/citrix-role"）を引き受けることができるようになりました。

クロスアカウントプロビジョニング用のホスト接続を作成する

VMをプロビジョニングしたいセカンダリアカウント（アカウントB）にホスト接続を作成します。これにより、アカウントAのデリバリーコントローラーは、アカウントBからロールを引き受けた後、アカウントBのリソースにアクセスできるようになります。

PowerShell コマンドを使用してホスト接続を作成し、次の2つのカスタムプロパティを追加します。

- `CrossAccountRoleArn`: `CrossAccountRoleArn` プロパティを指定しない場合、通常のホスト接続が作成されます。この場合、`MaximumAssumeRoleDurationInSeconds` が指定されていても無視されます。

- `MaximumAssumeRoleDurationInSeconds`: `DurationInSeconds` は900秒から3600秒の間である必要があります。デフォルトは900秒です。3600を超える値を指定した場合、`DurationInSeconds` は3600に設定されます。

例:

```
$connectionName = "cross-account-conn"

$cloudRegion = "us-east-1"

$apiKey = "role_based_auth"

$secretKey = "role_based_auth"

$zoneUid = "xxxxxx"

$secureKey = (ConvertTo-SecureString -String $secretKey -AsPlainText
-Force)

$connectionPath = "XDHyp:\Connections\" + $connectionName

$customProperties = '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="CrossAccountRoleArn"
Value="arn:aws:iam::5678:role/citrix-role" /><Property
xsi:type="StringProperty" Name="MaximumAssumeRoleDurationInSeconds"
Value="3600" />

"</CustomProperties>'



$connection = New-Item -Path $connectionPath -ConnectionType "AWS"
-HypervisorAddress "https://ec2.$($cloudRegion).amazonaws.com" -Persist
-Scope @() -UserName $apiKey -SecurePassword $secureKey -ZoneUid $zoneUid
-CustomProperties $customProperties
```

```
New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$connection.HypervisorConnectionUid
```

ホスト接続が作成されたら、Studio または PowerShell を使用してホスティングユニットを作成します。ただし、VPC とネットワークを選択してください。

接続を編集する

既存のホスト接続を編集して、次のことができます。

- Citrix がリソースを管理するための IAM 権限を提供するオプションを変更する
- ホスティング接続あたりの同時アクション (または同時マシン) の最大数を変更する
- スコープを変更する。
- PowerShell コマンドを使用して、エラスティックネットワークインターフェイス (ENI) ごとに許可されるセキュリティグループの最大数を構成する

IAM権限を付与するためのオプションを編集する

1. 既存のAmazon EC2接続を右クリックします。
2. **接続プロパティ**ページで、**設定の編集**をクリックします。
3. Citrixがリソースを管理するためのIAM権限を付与するオプションのいずれかを選択します。必要な詳細を入力し、**保存**をクリックします。

同時実行アクションの最大数を変更する

StudioでAmazon EC2のホスト接続を作成すると、次のデフォルト値が表示されます。

オプション	絶対値	パーセンテージ
同時実行アクション（すべての種類）	125	100
1分あたりの新規アクションの最大数	150	n/a
最大同時プロビジョニング操作	100	n/a

MCS は、デフォルトで最大 100 の同時プロビジョニング操作をサポートしています。

これらの値は、Citrix Studio の 画面にある セクションにアクセスして構成します。

または、Remote PowerShell SDK を使用して、環境に応じた最適な設定のために同時操作の最大数を設定できます。

PowerShell のカスタムプロパティ `MaximumConcurrentProvisioningOperations` を使用して、AWS の同時プロビジョニング操作の最大数を指定します。

構成する前に:

- Cloud 用 PowerShell SDK がインストールされていることを確認してください。
- `MaximumConcurrentProvisioningOperations` のデフォルト値が 100 であることを理解してください。

`MaximumConcurrentProvisioningOperations` の値をカスタマイズするには、次の手順を実行します。

1. **PowerShell** ウィンドウを開きます。
2. Citrix 固有の PowerShell モジュールをロードするには、`asnp citrix*` を実行します。
3. `cd xdhyp:\Connections\`を入力します。
4. 接続を一覧表示するには、`dir`を入力します。
5. カスタムプロパティ文字列を変更または初期化します:
   - カスタムプロパティ文字列に値がある場合は、カスタムプロパティをメモ帳にコピーします。次に、`MaximumConcurrentProvisioningOperations`プロパティを希望の値に変更します。1〜1000の範囲の値を入力できます。 例: `<Property xsi:type="IntProperty" Name="MaximumConcurrentProvisioningOperations" Value="xyz"/>`。
   - カスタムプロパティ文字列が空またはnullの場合、スキーマと`MaximumConcurrentProvisioningOperations`プロパティの両方に適切な構文を入力して文字列を初期化する必要があります。
6. **PowerShell**ウィンドウで、メモ帳から変更したカスタムプロパティを貼り付け、変更したカスタムプロパティに変数を割り当てます。カスタムプロパティを初期化した場合は、構文の後に次の行を追加します:

   `$customProperties = '<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><Property xsi:type="IntProperty" Name="MaximumConcurrentProvisioningOperations" Value="100"/></CustomProperties>'`。

この文字列は、`MaximumConcurrentProvisioningOperations`プロパティを100に設定します。カスタムプロパティ文字列では、`MaximumConcurrentProvisioningOperations`プロパティをニーズに合った値に設定する必要があります。

7. `Get-XDAuthentication`を入力すると、資格情報の入力を求められます。
8. `$cred = Get-Credential`を実行します。これにより、パスワードのみ（または名前とパスワード）の入力を求められる場合があります。アプリケーションIDと関連するシークレットの入力を求められる場合もあります。ロールベース認証を使用する接続の場合、**role_based_auth**は名前とパスワードの両方です。それ以外の場合は、AWS API IDとシークレットを入力します。
9. `set-item -PSPath 'XDHyp:\Connections<connection-name>' -CustomProperties $customProperties -username $cred.username -Securepassword $cred.password`を実行します。*<connection-name>*を接続の名前に設定する必要があります。
10. 更新されたCustomProperties文字列を確認するには、`dir`を入力します。

ネットワークインターフェースごとのセキュリティグループを構成する

ホスト接続を編集する際、PowerShellコマンドを使用して、エラスティックネットワークインターフェース (ENI) ごとに許可されるセキュリティグループの最大数を構成できるようになりました。AWSセキュリティグループのクォータ値については、セキュリティグループを参照してください。

ネットワークインターフェースごとにセキュリティグループを構成するには:

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. `cd xdhyp:\Connections\`を実行します。
4. 接続を一覧表示するために`dir`を実行します。
5. ネットワークインターフェースごとにセキュリティグループを構成するには、次のPowerShellコマンドを実行します。

```
Set-HypHypervisorConnectionMetadata -HypervisorConnectionName aws -Name
"Citrix_MachineManagement_Options" -Value "
AwsMaxENISecurityGroupLimit=<number>"
```

> **注:**

> `AwsMaxENISecurityGroupLimit`に値を設定しない場合、デフォルト値の5が使用されます。

サービスエンドポイントURL

標準ゾーンサービスエンドポイントURL

MCSを使用すると、APIキーとAPIシークレットを持つ新しいAWS接続が追加されます。この情報と認証済みアカウントを使用して、MCSはAWS DescribeRegions EC2 API呼び出しを使用して、サポートされているゾーンをAWSに照会します。クエリは、汎用EC2サービスエンドポイントURL `https://ec2.amazonaws.com/`を使用して行われます。MCSを使用して、サポートされているゾーンのリストから接続のゾーンを選択します。優先されるAWSサービスエンドポイントURLは、そのゾーンに対して自動的に選択されます。ただし、サービスエンドポイントURLを作成した後、そのURLを設定または変更することはできません。

必要なAWS権限

このセクションには、AWS権限の完全なリストが含まれています。機能が正しく動作するように、このセクションに記載されている権限の完全なセットを使用してください。

> **注:**
>
> `iam:PassRole` 権限は **role_based_auth** にのみ必要です。

ホスト接続の作成

AWSから取得した情報を使用して、新しいホスト接続が追加されます。

```
{

    "Version": "2012-10-17",

    "Statement": [

        {

            "Action": [

                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeSubnets",
```

```
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

VMの電源管理

VMの電源がオンまたはオフになります。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:RebootInstances",
                "ec2:DescribeInstanceStatus"
            ],
```

```
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

VMの作成、更新、または削除

AWSインスタンスとしてプロビジョニングされたVMを使用して、マシンカタログが作成、更新、または削除されます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
```

```
                "ec2:CreateVolume",

                "ec2:DeleteVolume",

                "ec2:DescribeAccountAttributes",

                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeIamInstanceProfileAssociations",

                "ec2:DescribeImages",

                "ec2:DescribeInstances",

                "ec2:DescribeInstanceStatus",

                "ec2:DescribeInstanceTypes",

                "ec2:DescribeLaunchTemplates",

                "ec2:DescribeLaunchTemplateVersions",

                "ec2:DescribeNetworkInterfaces",

                "ec2:DescribeRegions",

                "ec2:DescribeSecurityGroups",

                "ec2:DescribeSnapshots",

                "ec2:DescribeSubnets",

                "ec2:DescribeTags",

                "ec2:DescribeSpotInstanceRequests",

                "ec2:CancelSpotInstanceRequests",

                "ec2:DescribeInstanceCreditSpecifications",

                "ec2:DescribeInstanceAttribute",
```

```
                "ec2:GetLaunchTemplateData",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
```

```
            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

注:

- SecurityGroupsに関連するEC2セクションは、カタログ作成中に準備VM用に分離セキュリティグループを作成する必要がある場合にのみ必要です。これが完了すると、これらの権限は不要になります。

VMのインポート

VMをインポートしてマシンカタログを作成します。

```
{

    "Version": "2012-10-17",

    "Statement": [

        {

            "Action": [

                "ec2:DescribeInstances",

                "ec2:DescribeSecurityGroups",

                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeSubnets",

                "ec2:DescribeVolumes",

                "ec2:DescribeSpotInstanceRequests"

            ],

            "Effect": "Allow",

            "Resource": "*"

        }

    ]

}
```

注:

VMをインポートするAWSリージョンにスポットインスタンスがある場合にのみ、`ec2:DescribeSpotInstanceRequests` が必要です。

ディスクの直接アップロードとダウンロード

直接ディスクアップロードは、マシンカタログプロビジョニングにおけるボリュームワーカーの要件を排除し、代わりにAWSが提供するパブリックAPIを使用します。この機能により、追加のストレージアカウントに関連するコストと、ボリュームワーカー操作を維持する複雑さが軽減されます。

注:

ボリュームワーカーのサポートは削除されました。マシンカタログプロビジョニングには、直接ディスクのアップロードおよびダウンロードの権限が必要です。

以下の権限をポリシーに追加する必要があります。

- `ebs:StartSnapshot`
- `ebs:GetSnapshotBlock`
- `ebs:PutSnapshotBlock`
- `ebs:CompleteSnapshot`
- `ebs:ListSnapshotBlocks`
- `ebs:ListChangedBlocks`
- `ec2:CreateSnapshot`
- `ec2:DeleteSnapshot`
- `ec2:DescribeLaunchTemplates`

重要:

- ボリュームワーカーAMIやボリュームワーカーVMなどのボリュームワーカーリソースなしで、既存のマシンカタログに新しいVMを追加できます。
- 以前にボリュームワーカーを使用していた既存のカタログを削除すると、ボリュームワーカーに関連するすべてのアーティファクトが削除されます。

作成されたボリュームのEBS暗号化

AMIが暗号化されている場合、またはEBSがすべての新しいボリュームを暗号化するように構成されている場合、EBSは新しく作成されたボリュームを自動的に暗号化できます。ただし、この機能を実装するには、IAMポリシーに次の権限を含める必要があります。

```
{
     "Version": "2012-10-17",
     "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:GenerateDataKey",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": "*"
        }
    ]
}
```

注:

ユーザーの判断により、リソースと条件ブロックを含めることで、権限を特定のキーに限定できます。例：**条件付きKMS権限**：

```
{

     "Version": "2012-10-17",

     "Statement": [

        {

            "Effect": "Allow",

            "Action": [

                 "kms:CreateGrant",

                 "kms:Decrypt",

                 "kms:DescribeKey",

                 "kms:GenerateDataKeyWithoutPlainText",

                 "kms:GenerateDataKey",

                 "kms:ReEncryptTo",

                 "kms:ReEncryptFrom"

            ],

            "Resource": [

                "arn:aws:kms:us-east-2:123456789012:key/abcd1234-
a123-456d-a12b-a123b4cd56ef"

            ],

            "Condition": {
```

```
                "Bool": {

                    "kms:GrantIsForAWSResource": true

                }

            }

        }

    ]

}
```

次のキーポリシーステートメントは、アカウントがIAMポリシーを使用してKMSキーに対するすべてのアクション (kms:*) の権限を委任できるようにするために必要な、KMSキーのデフォルトのキーポリシー全体です。

```
{

"Sid": "Enable IAM policies",

"Effect": "Allow",

"Principal": {

"AWS": "arn:aws:iam::111122223333:root"

},

"Action": "kms:",

"Resource": ""

}
```

詳細については、AWS Key Management Serviceの公式ドキュメントを参照してください。

IAMロールベース認証

ロールベース認証をサポートするために、次の権限が追加されます。

```
{

     "Version": "2012-10-17",

     "Statement": [

        {

            "Effect": "Allow",

            "Action": "iam:PassRole",

            "Resource": "arn:aws:iam::*:role/*"

        }

    ]

}
```

最小限のIAM権限ポリシー

次のJSONは、現在サポートされているすべての機能に使用できます。このポリシーを使用すると、ホスト接続の作成、VMの作成、更新、削除、および電源管理を行うことができます。 このポリシーは、IAM権限の定義セクションで説明されているようにユーザーに適用することも、**role_based_auth**セキュリティキーとシークレットキーを使用してロールベース認証を使用することもできます。

> **重要:**
>
> **role_based_auth**を使用するには、まずDelivery Controllersのセットアップ時に、Delivery Controller EC2インスタンスで目的のIAMロールを設定します。Web Studioを使用してホスティング接続を追加し、認証キーとシークレットにrole_based_authを指定します。これらの設定を持つホスティング接続は、ロールベース認証を使用します。

```
{

    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateNetworkInterface",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteLaunchTemplate",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DeregisterImage",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAvailabilityZones",
```

```
                "ec2:DescribeIamInstanceProfileAssociations",

                "ec2:DescribeImages",

                "ec2:DescribeInstances",

                "ec2:DescribeInstanceTypes",

                "ec2:DescribeInstanceStatus",

                "ec2:DescribeLaunchTemplates",

                "ec2:DescribeLaunchTemplateVersions",

                "ec2:DescribeNetworkInterfaces",

                "ec2:DescribeRegions",

                "ec2:DescribeSecurityGroups",

                "ec2:DescribeSnapshots",

                "ec2:DescribeSubnets",

                "ec2:DescribeTags",

                "ec2:DescribeSpotInstanceRequests",

                "ec2:CancelSpotInstanceRequests",

                "ec2:DescribeInstanceCreditSpecifications",

                "ec2:DescribeInstanceAttribute",

                "ec2:GetLaunchTemplateData",

                "ec2:DescribeVolumes",

                "ec2:DescribeVpcs",

                "ec2:DetachVolume",

                "ec2:DisassociateIamInstanceProfile",
```

```
                "ec2:RebootInstances",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
```

```
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:GenerateDataKey",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": "*"
        },
        {
```

```
            "Effect": "Allow",

            "Action": "iam:PassRole",

            "Resource": "arn:aws:iam::*:role/*"

        }

    ]

}
```

注:

- SecurityGroupsに関連するEC2セクションは、カタログ作成時に準備VM用の分離セキュリティグループを作成する必要がある場合にのみ必要です。これが完了すると、これらの権限は不要になります。
- KMSセクションは、EBSボリューム暗号化を使用する場合にのみ必要です。
- `iam:PassRole` 権限セクションは、**role_based_auth** の場合にのみ必要です。
- 要件と環境に基づいて、フルアクセスではなく特定のリソースレベルの権限を追加できます。詳細については、AWSドキュメントのDemystifying EC2 Resource-Level Permissions および Access management for AWS resources を参照してください。
- ボリュームワーカー方式を使用している場合にのみ、`ec2:CreateNetworkInterface` および `ec2:DeleteNetworkInterface` の権限を使用してください。

ホスト接続の権限を検証する

ホスト接続の権限を検証して、MCSマシンカタログの作成と管理に関連するタスクを実行できます。この実装により、VMの作成、削除、更新、VMの電源管理、EBS暗号化など、さまざまなシナリオで必要な不足している権限を事前に特定できるため、重要な時期にブロックされるのを回避できます。

PowerShellコマンド `Test-HypHypervisorConnection` を使用して、ホスト接続の権限を検証できます。コマンドの結果はリストとしてキャプチャされ、リスト内の各項目は3つのセクションに分かれています。

- カテゴリ: ユーザーがMCSマシンカタログを作成および管理するために実行できるアクションまたはタスク。
- 修正措置: 管理者がユーザーの不足している権限の不一致を解決するために実行する必要がある手順。
- 不足している権限: カテゴリの不足している権限のリスト。

権限を検証するには、次の手順を実行します。

1. AWSへのホスト接続を作成します。
2. Delivery Controller™ ホストからPowerShellウィンドウを開きます。
3. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*` を実行します。
4. 権限を検索するために必要な権限があるかどうかを確認するには、次のコマンドを実行します。

   ```
   Test-HypHypervisorConnection -LiteralPath "XDHyp:\Connections\AWSCon"
   ```

5. 権限の検索に必要な不足している権限を追加した後、次のコマンドを実行して、以下のカテゴリの権限があることを確認します。

   - 作成、更新、削除
   - 電源管理
   - EBS暗号化

   ```
   Test-HypHypervisorConnection -LiteralPath "XDHyp:
   \Connections\AWSCon" [-SecurePassword -Password] "password" -UserName
   "" -CustomProperties ""
   ```

権限の追加について詳しくは、「IAM権限の追加」を参照してください。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- AWS固有の情報については、「AWS EC2カタログの作成」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- AWS仮想化環境

アマゾン ワークスペース コア マネージドインスタンスへの接続

(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/connections.html)は、接続を作成するウィザードについて説明しています。以下の情報は、Amazon WorkSpaces Core Managed Instancesに固有の詳細を扱っています。

前提条件

Amazon WorkSpaces Core Managed Instancesへの接続を作成する前に、以下を実行してください。

- AWSをリソースロケーションとして設定を完了します。「AWS仮想化環境」(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/install-prepare/aws.html)を参照してください。
- Citrix®がお客様に代わってAWSリソースを管理するためのIAMユーザーまたはロールのポリシーを(#define-iam-permissions)定義します。
- (#create-a-service-linked-role)を作成します。

IAM権限を定義する

ホスト接続を作成する前に、CitrixがAWSアカウントのリソースをプロビジョニングおよび管理するための適切な権限を付与するIAM権限ポリシーを、IAMユーザーまたはロールに対して適切に定義する必要があります。このセクションの情報を使用して、Amazon WorkSpaces Coreマネージドインスタンス上のCitrix Virtual Apps and DesktopsのIAM権限を定義してください。AmazonのIAMサービスでは、複数のユーザーを持つアカウントを許可しており、それらのユーザーはさらにグループに編成できます。これらのユーザーは、アカウントに関連する操作を実行する能力を制御するために、異なる権限を持つことができます。IAM権限の詳細については、IAM JSONポリシーリファレンスを参照してください。

> **注:**
>
> Citrixがお客様に代わってAWSアカウント内のリソースと自動化をプロビジョニングおよび管理するため、特定のタグまたはリソース命名規則に基づいたIAM権限ポリシーの構成はサポートされていません。

> 新しいユーザーグループにIAM権限ポリシーを適用するには：

1. AWSマネジメントコンソールにログインし、ドロップダウンリストから**IAMサービス**を選択します。

2. **新しいユーザーグループを作成**を選択します。
3. 新しいユーザーグループの名前を入力し、**続行**を選択します。
4. 「**Permissions**」ページで、「**Custom Policy**」を選択します。
5. 「**Permissions policy**」の名前を入力します。
6. 「**Policy Document**」セクションで、関連する権限を入力します。

ポリシー情報を入力したら、**「続行」**を選択して、IAM権限ポリシーのユーザーグループへの適用を完了します。グループ内のユーザーには、Citrix Virtual Apps and Desktopsに必要なアクションのみを実行する権限が付与されます。

> **重要:**
>
> この記事で提供されている例のポリシーテキストを使用して、Citrix Virtual Apps and DesktopsがAWSアカウント内でアクションを実行するために使用するアクションを、特定のリソースに制限することなくリストアップしてください。Citrixは、テスト目的でこの例を使用することを推奨します。本番環境では、リソースに対するさらなる制限を追加することを選択できます。

IAM権限を追加する

AWS Management Consoleの「**IAM**」セクションで権限を追加します。

1. 「**Summary**」パネルで、「**Permissions**」タブを選択します。
2. 「**Add permissions**」を選択します。
3. 「**Add Permissions to**」画面で、権限を付与します。
4. JSONセクションで、環境に必要なRequired AWS permissionsを含めます。

サービスにリンクされたロールを作成する

CitrixがCore V2 APIを呼び出す各AWSアカウントに対して、サービスにリンクされたロール (SLR) を作成します。

ロールを作成する手順：

- AWS マネジメントコンソールでコマンドラインインターフェイス (CLI) を開きます。
- CLI で次のコマンドを実行します。

```
aws iam create-service-linked-role --aws-service-name workspaces-
instances.amazonaws.com
```

Amazon WorkSpaces Core 管理コンソールを使用して、サービスにリンクされたロールを構成することもできます。サービスにリンクされたロールの作成 (コンソール)を参照してください。

接続を作成する

Amazon WorkSpaces Core マネージドインスタンスへの接続は、次の方法で作成できます。

- ウェブスタジオ
- PowerShell コマンド

注:

プロキシサーバーまたはファイアウォールの制限を確認し、次のアドレスに接続できることを確認してください: `https://*.amazonaws.com` および `https://*.api.aws`。また、(/ja-jp/citrix-cloud/overview/requirements/internet-connectivity-requirements#citrix-gateway-service-connectivity)に記載されているすべてのアドレスに接続できることを確認してください。

これらに接続できない場合、ホスト接続の作成または更新中に失敗する可能性があります。

Web Studioを使用して接続を作成する

1. **Hosting > Add Connection and Resources** ページに移動します。
2. **接続**ページで、以下の手順に従って接続を構成します。
    a. **新しい接続を作成**を選択します。
    b. **ゾーン**で、AWS 環境用に設定したリソースの場所を選択します。
    c. 接続タイプとして「**Amazon WorkSpaces Core**」を選択します。
    d. 「**IAMユーザーアクセスキーを使用**」または「**IAMロールを使用**」を選択します。

    IAMユーザーアクセスキーの場合は、CitrixがAWSアカウントのリソースを管理するための適切なIAM権限ポリシーを持つIAMユーザーの**APIキー**と**シークレットキー**を入力します。

IAMロールについては、CitrixがAWSアカウントのリソースを管理するための適切なIAM権限ポリシーを持つIAMロールをDelivery Controllerインスタンスに割り当てたことを確認してください。詳細については、ロールベース認証ガイドを参照してください。

e. 接続名を入力し、**次へ**をクリックします。

3. **仮想マシンの場所**ページで、VMをプロビジョニングする場所を指定します。新しいVMを作成するためのクラウドリージョン、VPC、およびアベイラビリティゾーンを選択します。
4. 「**ネットワーク**」ページで:

   a. 以前にアベイラビリティゾーンまたはローカルゾーンで選択したリソースの名前を入力します。

   b. 前のメニューで構成したVPC内のサブネットを1つ以上選択します。

5. 残りのページを**概要**ページまでクリックして進みます。
6. 「**完了**」をクリックして、Amazon WorkSpaces Core Managed Instancesへのホスト接続を作成します。

重要な考慮事項

Web Studioを使用して接続を作成する場合：

- CitrixがAWSリソースを管理するための適切なIAM権限を定義します。
- CitrixがAWSリソースを管理するためにIAMユーザーアクセスキーを使用する場合、APIキーとシークレットキーの値を指定する必要があります。これらの値を含むキーファイルをAWSからエクスポートし、インポートできます。また、リージョン、アベイラビリティゾーン、VPC名、サブネットアドレス、ドメイン名、セキュリティグループ名、および資格情報も指定する必要があります。
- CitrixがAWSリソースを管理するためにIAMロールを使用する場合、すべてのDelivery Controllerに適切なIAM権限を持つロールを割り当てる必要があります。詳細については、ロールベース認証ガイドを参照してください。
- ルートAWSアカウントの資格情報ファイル（AWSコンソールから取得）は、標準のAWSユーザー用にダウンロードされた資格情報ファイルと同じ形式ではありません。そのため、Citrix Virtual Apps and Desktopsは、このファイルを使用してAPIキーとシークレットキーのフィールドに入力することはできません。AWS Identity Access Management (IAM) 資格情報ファイルを使用していることを確認してください。
- ゾーンはアベイラビリティゾーンまたはローカルゾーンのいずれかです。

PowerShellを使用して接続を作成する

1. PowerShellウィンドウを開きます。

2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*`を実行します。
3. 次のコマンドを実行します。以下に例を示します。

```
$connectionName = "demo-hostingconnection"

$cloudRegion = "us-east-1"

$apiKey = "aaaaaaaaaaaaaaaaaaaa"

$apiSecret = “bbbbb”

$secureKey = ConvertTo-SecureString -String $apiSecret

$zoneUid = "00000000-0000-0000-0000-000000000000"

$connectionPath = "XDHyp:\Connections\" + $connectionName



$connection = New-Item -Path $connectionPath -ConnectionType
"AmazonWorkSpacesCoreMachineManagerFactory" -HypervisorAddress "
"https://workspaces-instances.$($cloudRegion).api.aws"" -Persist -Scope
@() -UserName $apiKey -SecurePassword $secureKey -ZoneUid $zoneUid



New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$connection.HypervisorConnectionUid



$hostingUnitName = "demo-hostingunit"

$availabilityzone = "us-east-1a"

$vpcName = "Default VPC"

$jobGroup = [Guid]::NewGuid()

$hostingUnitPath = "XDHyp:\HostingUnits\" + $HostingUnitName

$rootPath = $connectionPath + "\" + $vpcName + ".virtualprivatecloud\"
```

```
$availabilityZonePath = @($rootPath + $availabilityzone +
".availabilityzone")

$networkPaths = (Get-ChildItem $availabilityZonePath[0] | Where
ObjectType -eq "Network") | Select-Object -ExpandProperty FullPath #
will select all the networks in the availability zone



New-Item -Path $hostingUnitPath -AvailabilityZonePath
$availabilityZonePath -HypervisorConnectionName $connectionName
-JobGroup $jobGroup -PersonalvDiskStoragePath @() -RootPath $rootPath
-NetworkPath $networkPaths
```

注:

ロールベース認証を使用して接続を作成するには、apiKeyとapiSecretを `role_based_auth` として指定します。

制限事項

AWSコンソールでAWS Virtual Private Cloud (VPC) の名前を変更すると、Citrix Cloud™内の既存のホスティングユニットが破損します。ホスティングユニットが破損すると、カタログを作成したり、既存のカタログにマシンを追加したりできなくなります。この問題を解決するには、AWS VPCの名前を元の名前に戻してください。

クロスアカウントプロビジョニング

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

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

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

Cloud Connector がセカンダリアカウントのリソースにアクセスできるようにするには、セカンダリアカウントから IAM ロールを引き受けた後にホスト接続を作成します。

前提条件

クロスアカウントプロビジョニング用のホスト接続を作成する前に、以下を設定してください。

- VPCピアリングを設定し、両方のリージョンまたはアカウントでセキュリティグループを構成します。詳細については、「VPCピアリングの設定」(#set-up-vpc-peering)を参照してください。
- IAMロールを使用してクロスアカウントアクセスを委任します。詳細については、「IAMロールを使用したクロスアカウントアクセスの委任」(#delegate-cross-account-access-using-iam-roles)を参照してください。

VPCピアリングの設定

VPC Aがプライマリアカウント（アカウントA）にあり、Cloud ConnectorとActive Directoryを持っていると仮定します。VPC Bは、VMをプロビジョニングしたいセカンダリアカウント（アカウントB）にあります。

アカウントAとアカウントBの間でVPCピアリング接続を設定するには、次の手順を実行します。

1. VPCピアリング接続を作成します。参照：
    - 異なるアカウント、同じリージョン
    - 異なるアカウント、異なるリージョン
2. VPC Aに移動し、パブリックサブネットに関連付けられているルートテーブルに移動します。
3. **>** をクリックします。 列にVPC BのCIDRブロックを追加し、 列に作成したVPCピアリングを追加します。
4. ステップ2と3を繰り返しますが、VPC AとVPC Bのプライベートサブネットを使用します（VPC AのCIDRブロックを追加します）。詳細については、VPCピアリング接続のルートテーブルを更新するを参照してください。
5. VPC Aに関連付けられているプライベートセキュリティグループに移動します。
6. を選択し、 を選択します。
7. を選択します。タイプには を選択し、 列に以下を追加します。

- 異なるリージョンの場合は、VPC BのCIDRブロックを追加します。
- 異なるアカウントだが同じリージョンの場合は、アカウントIDとVPC Bのプライベートセキュリティグループを追加します（例: 123456789012/sg-1a2b3c4d）。

8. 手順5から7を繰り返しますが、VPC Bのプライベートセキュリティグループを使用します（ただし、VPC AのCIDRブロック、またはVPC Aのアカウントと、同じリージョンだが異なるアカウントのプライベートセキュリティグループIDを追加します）。ピアセキュリティグループを参照するようにセキュリティグループを更新するを参照してください。

> **注:**
>
> VPCピアリング接続の作成に料金はかかりません。ただし、アベイラビリティゾーン内のVPCピアリングは無料ですが、複数のアベイラビリティゾーンやリージョンをまたいでVPCピアリング接続を介したデータ転送が発生した場合は料金がかかります。VPCピアリング接続の料金を参照してください。

IAMロールを使用してクロスアカウントアクセスを委任する

アカウント間でVPCピアリングを設定した後、IAMロールを使用してクロスアカウントアクセスを委任します。

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

クロスアカウントリソースにアクセスするには、次の手順を実行します。

> **注意：**
>
> VPC Aはプライマリアカウント（アカウントA）にあり、Cloud ConnectorとActive Directoryが設定されていると仮定します。VPC Bは、VMをプロビジョニングするセカンダリアカウント（アカウントB）にあります。

1. 前述の手順でアカウント間のVPCピアリングを設定します。

2. 最小限のCitrix IAM権限を持つIAMロールとポリシーをアカウントBに作成します。IAMチュートリアル: IAMロールを使用してAWSアカウント間でアクセスを委任するを参照してください。このロールのARNが「arn:aws:iam::5678:role/citrix-role」であるとします。
3. ロール「arn:aws:iam::5678:role/citrix-role」に信頼ポリシーを追加し、アカウントAのロール「arn:aws:iam::1234:role/primary-account-citrix-role」によってアクセスが許可されるようにします。詳細については、IAMでのクロスアカウントリソースアクセスを参照してください。
4. アカウントAに、前述の「primary-account-citrix role」という名前でIAMロールとポリシーを作成します。これにより、アカウントBのIAMロール（arn:aws:iam::5678:role/citrix-role）を引き受け、そのIAMロールを渡すことができます。
5. アカウントAのすべてのCloud Connectorにロール「arn:aws:iam::1234:role/primary-account-citrix-role」を割り当てます。

Cloud Connectors は、アカウント B のロール ("arn:aws:iam::5678:role/citrix-role") を引き受けることができるようになりました。

クロスアカウントプロビジョニング用のホスト接続を作成する

VM をプロビジョニングするセカンダリアカウント (アカウント B) にホスト接続を作成します。これにより、アカウント A の Cloud Connectors は、アカウント B からロールを引き受けた後、アカウント B のリソースにアクセスできるようになります。

PowerShell コマンドを使用してホスト接続を作成し、次の 2 つのカスタムプロパティを追加します。

- `CrossAccountRoleArn`: `CrossAccountRoleArn` プロパティを指定しない場合、通常のホスト接続が作成されます。この場合、`MaximumAssumeRoleDurationInSeconds` は指定されていても無視されます。
- `MaximumAssumeRoleDurationInSeconds`: `DurationInSeconds` は 900 秒から 3600 秒の間である必要があります。デフォルトは 900 秒です。3600 を超える値を指定した場合、`DurationInSeconds` は 3600 に設定されます。

例:

```
$connectionName = "cross-account-conn"

$cloudRegion = "us-east-1"

$apiKey = "role_based_auth"

$secretKey = "role_based_auth"
```

```
$zoneUid = "xxxxxx"

$secureKey = (ConvertTo-SecureString -String $secretKey -AsPlainText
-Force)

$connectionPath = "XDHyp:\Connections\" + $connectionName

$customProperties = '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="CrossAccountRoleArn"
Value="arn:aws:iam::5678:role/citrix-role" /><Property
xsi:type="StringProperty" Name="MaximumAssumeRoleDurationInSeconds"
Value="3600" />

"</CustomProperties>'



$connection = New-Item -Path $connectionPath -ConnectionType
"AmazonWorkSpacesCoreMachineManagerFactory" -HypervisorAddress "https://
workspaces-instances.$($cloudRegion).api.aws" -Persist -Scope @()
-UserName $apiKey -SecurePassword $secureKey -ZoneUid $zoneUid
-CustomProperties $customProperties



New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$connection.HypervisorConnectionUid
```

ホスト接続が作成されたら、Web StudioまたはPowerShellを使用してホスティングユニットを作成します。ただし、VPCとネットワークを選択してください。

接続の編集

既存のホスト接続を編集して、次のことができます。

- Citrix がリソースを管理するための IAM 権限を提供するオプションを変更する
- ホスティング接続あたりの同時アクション (または同時マシン) の最大数を変更する
- スコープを変更する。

- PowerShell コマンドを使用して、エラスティックネットワークインターフェース (ENI) あたりのセキュリティグループの最大数を構成する

IAM権限を付与するためのオプションを編集する

1. 既存のAmazon WorkSpaces Core接続を右クリックします。
2. **Connection Properties**ページで、**Edit settings**をクリックします。
3. Citrixがリソースを管理するためのIAM権限を付与するオプションのいずれかを選択します。必要な詳細を入力し、**Save**をクリックします。

同時実行アクションの最大数を変更する

Amazon WorkSpaces Coreマネージドインスタンスのホスト接続を作成すると、以下のデフォルト値が表示されます。

オプション	絶対値	パーセンテージ
同時実行アクション（すべての種類）	125	100
1分あたりの新規アクションの最大数	150	N/A
最大同時プロビジョニング操作数	150	N/A

MCS は、デフォルトで最大 150 の同時プロビジョニング操作をサポートします。

これらの値は、**接続の編集**画面の Citrix Studio の**詳細設定**セクションにアクセスして構成できます。

または、Remote PowerShell SDK を使用して、環境に応じた最適な設定のために同時操作の最大数を設定することもできます。

PowerShell カスタムプロパティ `MaximumConcurrentProvisioningOperations` を使用して、AWS の同時プロビジョニング操作の最大数を指定します。

構成前:

- Cloud 用 PowerShell SDK がインストールされていることを確認してください。
- `MaximumConcurrentProvisioningOperations` のデフォルト値は 150 であることを理解してください。

`MaximumConcurrentProvisioningOperations` の値をカスタマイズするには、次の手順を実行します。

1. **PowerShell** ウィンドウを開きます。
2. Citrix 固有の PowerShell モジュールをロードするには、`asnp citrix*` を実行します。
3. `cd xdhyp:\Connections\` を入力します。
4. 接続を一覧表示するには、`dir` を入力します。
5. カスタムプロパティ文字列を変更または初期化します。
   - カスタムプロパティ文字列に値がある場合は、カスタムプロパティをメモ帳にコピーします。次に、`MaximumConcurrentProvisioningOperations` プロパティを希望の値に変更します。1〜1000の範囲の値を入力できます。 例: `<Property xsi:type="IntProperty" Name="MaximumConcurrentProvisioningOperations" Value="xyz"/>`。
   - カスタムプロパティ文字列が空またはnullの場合、スキーマと `MaximumConcurrentProvisioningOperations` プロパティの両方に適切な構文を入力して文字列を初期化する必要があります。
6. **PowerShell** ウィンドウで、メモ帳から変更したカスタムプロパティを貼り付け、変更したカスタムプロパティに変数を割り当てます。カスタムプロパティを初期化した場合は、構文の後に次の行を追加します。

   ```
   $customProperties = '<CustomProperties xmlns="http://
   schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
   www.w3.org/2001/XMLSchema-instance"><Property xsi:type="IntProperty"
   Name="MaximumConcurrentProvisioningOperations" Value="100"/></
   CustomProperties>'
   ```

   この文字列は、`MaximumConcurrentProvisioningOperations` プロパティを100に設定します。カスタムプロパティ文字列では、`MaximumConcurrentProvisioningOperations` プロパティをニーズに合った値に設定する必要があります。
7. 資格情報の入力を求める`Get-XDAuthentication` を入力します。
8. `$cred = Get-Credential` を実行します。これにより、パスワードのみ（または名前とパスワード）の入力を求められる場合があります。アプリケーションIDと関連するシークレットの入力を求められる場合もあります。ロールベース認証を使用する接続の場合、**role_based_auth** は名前とパスワードの両方です。それ以外の場合は、AWS API IDとシークレットを入力します。

9. `set-item -PSPath 'XDHyp:\Connections<connection-name>' -CustomProperties $customProperties -username $cred.username -Securepassword $cred.password` を実行します。*<connection-name>* を接続の名前に設定する必要があります。
10. 更新されたCustomProperties文字列を確認するには、`dir` を入力します。

ネットワークインターフェイスごとのセキュリティグループを構成する

ホスト接続を編集する際、PowerShellコマンドを使用して、エラスティックネットワークインターフェイス（ENI）ごとに許可されるセキュリティグループの最大数を構成できるようになりました。AWSセキュリティグループのクォータ値については、「セキュリティグループ」を参照してください。

ネットワークインターフェイスごとにセキュリティグループを構成するには:

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*` を実行します。
3. `cd xdhyp:\Connections\`を実行します。
4. 接続を一覧表示するには、`dir`を実行します。
5. ネットワークインターフェイスごとにセキュリティグループを構成するには、次のPowerShellコマンドを実行します。

```
Set-HypHypervisorConnectionMetadata -HypervisorConnectionName aws -Name
"Citrix_MachineManagement_Options" -Value "
AwsMaxENISecurityGroupLimit=<number>"
```

注:

`AwsMaxENISecurityGroupLimit`に値を設定しない場合、デフォルト値の5が使用されます。

サービスエンドポイントURL

標準ゾーンサービスエンドポイントURL

MCSを使用すると、APIキーとAPIシークレットを持つ新しいAmazon WorkSpaces Core Managed Instances接続が追加されます。この情報と認証済みアカウントを使用して、MCSはAWS EC2およびAmazon WorkSpaces Core Managed Instances API呼び出しを使用して、サポートされているリージョンとゾーンをAWSに照会します。このクエリは、Workspace Instances

Service Endpoint URL `<https://workspaces-instances.us-east-1.api.aws/>` とEC2 Service Endpoint https:/ec2.us-east-1.api.aws/ を使用して行われます。

> **注:**
>
> `<https://workspaces-instances.us-east-1.api.aws/>` に接続できることを確認してください。

必要なAWS権限

このセクションには、AWS権限の完全なリストが含まれています。機能が正しく動作するように、このセクションに記載されている権限の完全なセットを使用してください。

> **注:**
>
> `iam:PassRole` 権限は、Citrixがリソースを管理するためにIAMロールを使用する場合にのみ必要です。

ホスト接続の作成

AWSから取得した情報を使用して、新しいホスト接続が追加されます。

```
{

    "Version": "2012-10-17",

    "Statement": [

        {

            "Action": [

                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeSubnets",

                "ec2:DescribeVpcs",

                "ec2:DescribeRegions",
```

```
                "workspaces-instances:*"

            ],

            "Effect": "Allow",

            "Resource": "*"

        }

    ]

}
```

VMの電源管理

VMの電源がオンまたはオフになります。

```
{

    "Version": "2012-10-17",

    "Statement": [

        {

            "Action": [

                "ec2:DescribeInstances",,

                "ec2:StartInstances",

                "ec2:StopInstances",

                "ec2:RebootInstances",

                "ec2:DescribeInstanceStatus"

            ],

            "Effect": "Allow",
```

```
            "Resource": "*"
        },
        {
           "Action": [
               "workspaces-instances:*"
           ],
           "Effect": "Allow",
            "Resource": "*"
       }

    ]

}
```

VMの作成、更新、または削除

AWSインスタンスとしてプロビジョニングされたVMを使用して、マシンカタログが作成、更新、または削除されます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
```

```
                "ec2:AssociateIamInstanceProfile",

                "ec2:AuthorizeSecurityGroupEgress",

                "ec2:RevokeSecurityGroupEgress",

                "ec2:AuthorizeSecurityGroupIngress",

                "ec2:CreateImage",

                "ec2:CreateLaunchTemplate",

                "ec2:CreateSecurityGroup",

                "ec2:CreateTags",

                "ec2:CreateVolume",

                "ec2:DeleteVolume",

                "ec2:DescribeAccountAttributes",

                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeIamInstanceProfileAssociations",

                "ec2:DescribeImages",

                "ec2:DescribeInstances",

                "ec2:DescribeInstanceStatus",

                "ec2:DescribeInstanceTypes",

                "ec2:DescribeLaunchTemplates",

                "ec2:DescribeLaunchTemplateVersions",

                "ec2:DescribeNetworkInterfaces",

                "ec2:DescribeRegions",

                "ec2:DescribeSecurityGroups",
```

```
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeSpotInstanceRequests",
                "ec2:DescribeInstanceCreditSpecifications",
                "ec2:DescribeInstanceAttribute",
                "ec2:GetLaunchTemplateData",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:CreateSecurityGroup",
```

```
            "ec2:DeleteSecurityGroup"
        ],
        "Effect": "Allow",
        "Resource": "*"
    },
    {
        "Action": [
            "ebs:StartSnapshot",
            "ebs:GetSnapshotBlock",
            "ebs:PutSnapshotBlock",
            "ebs:CompleteSnapshot",
            "ebs:ListSnapshotBlocks",
            "ebs:ListChangedBlocks",
            "ec2:CreateSnapshot"
        ],
        "Effect": "Allow",
        "Resource": "*"
    },
    {
        "Action": [
            "workspaces-instances:*"
        ],
```

```
            "Effect": "Allow",

            "Resource": "*"

        }



    ]

}
```

注:

- SecurityGroupsに関連するEC2セクションは、カタログ作成時に準備VM用に分離セキュリティグループを作成する必要がある場合にのみ必要です。これが完了すると、これらの権限は不要になります。

ディスクの直接アップロードとダウンロード

次の権限をポリシーに追加する必要があります。

- `ebs:StartSnapshot`
- `ebs:GetSnapshotBlock`
- `ebs:PutSnapshotBlock`
- `ebs:CompleteSnapshot`
- `ebs:ListSnapshotBlocks`
- `ebs:ListChangedBlocks`
- `ec2:CreateSnapshot`
- `ec2:DeleteSnapshot`
- `ec2:DescribeLaunchTemplates`

作成されたボリュームのEBS暗号化

AMIが暗号化されている場合、またはEBSがすべての新しいボリュームを暗号化するように構成されている場合、EBSは新しく作成されたボリュームを自動的に暗号化できます。ただし、この機能を実装するには、IAMポリシーに次の権限を含める必要があります。

```
{
     "Version": "2012-10-17",
     "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:GenerateDataKey",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": "*"
        }
    ]
}
```

注:

権限は、ユーザーの判断でリソースと条件ブロックを含めることにより、特定のキーに制限できます。例：**条件付きKMS権限**：

```
{

     "Version": "2012-10-17",

     "Statement": [

        {

            "Effect": "Allow",

            "Action": [

                 "kms:CreateGrant",

                 "kms:Decrypt",

                 "kms:DescribeKey",

                 "kms:GenerateDataKeyWithoutPlainText",

                 "kms:GenerateDataKey",

                 "kms:ReEncryptTo",

                 "kms:ReEncryptFrom"

            ],

            "Resource": [

                "arn:aws:kms:us-east-2:123456789012:key/abcd1234-
a123-456d-a12b-a123b4cd56ef"

            ],

            "Condition": {
```

```
                "Bool": {

                    "kms:GrantIsForAWSResource": true

                }

            }

        }

    ]

}
```

次のキーポリシーステートメントは、アカウントがIAMポリシーを使用してKMSキーに対するすべてのアクション (kms:*) の権限を委任できるようにするために必要な、KMSキーのデフォルトキーポリシー全体です。

```
{

"Sid": "Enable IAM policies",

"Effect": "Allow",

"Principal": {

"AWS": "arn:aws:iam::111122223333:root"

},

"Action": "kms:",

"Resource": ""

}
```

詳細については、AWS Key Management Serviceの公式ドキュメントを参照してください。

IAMロールベース認証

ロールベース認証をサポートするために、次の権限が追加されます。

```
{

     "Version": "2012-10-17",

     "Statement": [

        {

            "Effect": "Allow",

            "Action": "iam:PassRole",

            "Resource": "arn:aws:iam::*:role/*"

        }

    ]

}
```

最小限のIAM権限ポリシー

次のJSONは、現在サポートされているすべての機能に使用できます。このポリシーを使用して、ホスト接続の作成、VMの作成、更新、削除、および電源管理を行うことができます。 このポリシーは、IAM権限の定義セクションで説明されているようにユーザーに適用することも、ホスト接続を構成するときに**IAMロールを使用**を選択してロールベース認証を使用することもできます。

重要:

CitrixがリソースをIAMロールを使用するには、まずDelivery Controllerのセットアップ時に、Delivery Controller ec2インスタンスで目的のIAMロールを構成します。Citrix Studioを使用して、ホスティング接続を追加し、**IAMロールを使用**オプションを選択します。これらの設定を持つホスティング接続は、ロールベース認証を使用します。

```
{

    "Version": "2012-10-17",

    "Statement": [
```

```
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateNetworkInterface",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteLaunchTemplate",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DeregisterImage",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeIamInstanceProfileAssociations",
```

```
                "ec2:DescribeImages",

                "ec2:DescribeInstances",

                "ec2:DescribeInstanceTypes",

                "ec2:DescribeInstanceStatus",

                "ec2:DescribeLaunchTemplates",

                "ec2:DescribeLaunchTemplateVersions",

                "ec2:DescribeNetworkInterfaces",

                "ec2:DescribeRegions",

                "ec2:DescribeSecurityGroups",

                "ec2:DescribeSnapshots",

                "ec2:DescribeSubnets",

                "ec2:DescribeTags",

                "ec2:DescribeSpotInstanceRequests",

                "ec2:DescribeInstanceCreditSpecifications",

                "ec2:DescribeInstanceAttribute",

                "ec2:GetLaunchTemplateData",

                "ec2:DescribeVolumes",

                "ec2:DescribeVpcs",

                "ec2:DetachVolume",

                "ec2:DisassociateIamInstanceProfile",

                "ec2:RebootInstances",

                "ec2:RunInstances",
```

```
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
```

```
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:GenerateDataKey",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
```

```
            "Resource": "arn:aws:iam::*:role/*"

        },

        {

            "Effect": "Allow",

            "Action": [

                "workspaces-instances:*"

            ],

            "Resource": "*"

        }



    ]

}
```

注:

- SecurityGroupsに関連するEC2セクションは、カタログ作成時に準備VM用に分離セキュリティグループを作成する必要がある場合にのみ必要です。これが完了すると、これらの権限は不要になります。
- KMSセクションは、EBSボリューム暗号化を使用する場合にのみ必要です。
- `iam:PassRole`権限セクションは、Citrixがリソースを管理するためのIAMロールを使用する場合にのみ必要です。
- 要件と環境に基づいて、フルアクセスではなく、特定のリソースレベルの権限を追加できます。詳細については、AWSドキュメントのDemystifying EC2 Resource-Level PermissionsおよびAccess management for AWS resourcesを参照してください。
- ボリュームワーカー方式を使用している場合にのみ、`ec2:CreateNetworkInterface`および`ec2:DeleteNetworkInterface`権限を使用してください。

次のステップ

- 準備済みイメージの作成については、Amazon WorkSpaces Coreマネージドインスタンス用の準備済みイメージを作成するを参照してください。

詳細情報

- 接続とリソースの作成および管理
- AWS仮想化環境
- Amazon WorkSpaces Core GitHub PowerShellの例については、citrix-mcs-sdk-samples-Amazon WorkSpaces Coreを参照してください。

Azure Local への接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明します。以下の情報は、Azure Local 環境に固有の詳細を扱います。

ホスティング接続を作成する

ホスト接続は、以下を使用して作成できます。

- ウェブスタジオ
- PowerShell

Web Studio を使用する

1. ウェブスタジオで、**Hosting > Add Connection and Resources** を開きます。
2. **接続**ページで、以下の手順に従って接続を構成します。
    a. **新しい接続を作成**を選択します。
    b. 接続の種類として **Microsoft® Azure™ Arc** を選択します。
    c. Azure 環境を選択します。
    d. ゾーンを選択します。オプションは、構成したすべてのリソースの場所です。
    e. 仮想マシンを作成するには、「**その他のツール**」を選択します。

> **注:**

> 「**その他のツール**」を選択すると、ホスティングユニットなしでホスティング接続のみが作成されます。

f. **Next**をクリックします。

3. **Connection Details** ページで、ウィザードのガイダンスに従って接続の詳細を入力します。既存の SPN を使用する場合は、SPN にサブスクリプションの共同作成者ロールが付与されていることを確認してください。詳細については、必要な Azure Local 権限 を確認してください。
4. **Scopes** ページで、この接続のスコープを 1 つ以上選択します。
5. 「**概要**」ページで、構成を確認し、「**完了**」をクリックします。

PowerShell を使用する

スクリプトのヘッダー

スクリプトのヘッダーで定義されている正しいパラメーター値を指定していることを確認してください。

```
$azureSubscription = "" # Azure Subscription ID



$azureTenantId = "" # Microsoft Entra Tenant ID



$appClientId = "" # Client ID of an Microsoft Entra application which is
grant with sufficient permissions



$appClientSecret = "" # Client secret of above client ID



$appClientSecretExpirationDateTimestamp = "" # Client secret expiration
date in epoch timestamp format



$region = "" # Azure region of your Azure Local cluster
```

```
$resourceGroupName = "" # Azure resource group of your Azure Local cluster


$zoneUid = "" # Zone UID of your resource location


$hostingConnectionName = "" # Name of the created hosting connection
```

ホスティング接続を作成する

```
asnp citrix*


[SecureString]$appClientSecretSecureString = $appClientSecret | ConvertTo-
SecureString -AsPlainText -Force


$conn = New-Item -ConnectionType "Custom" -CustomProperties
"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`"
Value=`"$azureSubscription`" /><Property xsi:type=`"StringProperty`"
Name=`"ManagementEndpoint`" Value=`"https://management.azure.com/`" /
><Property xsi:type=`"StringProperty`" Name=`"AuthenticationAuthority`"
Value=`"https://login.microsoftonline.com/`" /><Property
xsi:type=`"StringProperty`" Name=`"TenantId`" Value=`"$azureTenantId`" /
></CustomProperties>" -HypervisorAddress @("https://
management.azure.com/") -Path @("XDHyp:\Connections\
$hostingConnectionName") -Persist -PluginId "AzureArcFactory" -Scope @()
-SecurePassword $appClientSecretSecureString -UserName $appClientId
-ZoneUid $zoneUid


New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$conn.HypervisorConnectionUid
```

```
Set-HypHypervisorConnectionMetadata -HypervisorConnectionUid
$conn.HypervisorConnectionUid -Name
Citrix_Orchestration_Hypervisor_Secret_Allow_Edit -Value true



Set-HypHypervisorConnectionMetadata -HypervisorConnectionUid
$conn.HypervisorConnectionUid -Name
Citrix_Orchestration_Hypervisor_Secret_Expiration_Date -Value
$appClientSecretExpirationDateTimestamp
```

ホスティングユニットを作成する

ホスティングユニットは、次の方法で作成できます。

- ウェブスタジオ
- PowerShell

ホスティングユニットを作成する Web Studioを使用する

1. Web Studioで、 **>** を開きます。
2. 「**接続**」ページで：
   - ホスティングユニットとともに新しいホスティング接続を作成するには、 を選択し、次の操作を行います。
     a. **新しい接続を作成**を選択します。
     b. 接続の種類として **Microsoft® Azure™ Arc** を選択します。
     c. Azure環境を選択します。
     d. ゾーンを選択します。オプションは、構成したすべてのリソースの場所です。
     e. 仮想マシンを作成するには、**Citrixプロビジョニングツール (Machine Creation Services™またはCitrix Provisioning)** を選択します。
     f. **Next**をクリックします。
   - 既存のホスト接続からホスティングユニットを作成するには、 を選択し、関連する接続を選択します。

3. ページで、ウィザードのガイダンスに従って接続の詳細を入力します。既存のSPNを使用する場合は、SPNにサブスクリプションの共同作成者ロールが付与されていることを確認してください。
4. ページで、リソースグループを参照し、ターゲットのAzure Localクラスターを選択します。
5. ページで、ウィザードの次のページに進む前に、サポートされているデータタイプごとに少なくとも1つのストレージデバイスを選択します。ストレージの選択について詳しくは、「ホストストレージ」を参照してください。
6. ページで、リソースの名前を入力します。この名前は、接続に関連付けられているストレージとネットワークの組み合わせを識別するためにStudioに表示されます。VMが使用するネットワークを1つ以上選択します。
7. ページで、詳細を確認し、 をクリックします。

PowerShellを使用してホスティングユニットを作成する

スクリプトのヘッダー

スクリプトのヘッダーで定義されている正しいパラメーター値を指定していることを確認してください。

```
$resourceGroupName = "" # Azure resource group of your Azure Local cluster



$clusterName = "" # Name of your Azure Local cluster



$storagePathName = "" # Storage path in your Azure Local cluster that
wants to be used in this hosting unit



$logicalNetworkName = "" # Logical network in your Azure Local cluster
that wants to be used in this hosting unit



$zoneUid = "" # Zone UID of your resource location
```

```
$hostingConnectionName = "" # Name of the created hosting connection



$hostingUnitName = "" # Name of the created hosting unit
```

ホスティングユニットを作成する

```
asnp citrix*



$guid = (New-Guid).Guid



New-HypStorage -StoragePath @("XDHyp:\Connections\$hostingConnectionName\
$region.region\$resourceGroupName.resourcegroup\cluster.folder\
$clusterName.cluster\storage.folder\$storagePathName.storage")
-StorageType "TemporaryStorage" -JobGroup $guid



New-Item -Path XDHyp:\HostingUnits -Name $hostingUnitName
-HypervisorConnectionName $hostingConnectionName -RootPath "XDHyp:
\Connections\$hostingConnectionName\$region.region\
$resourceGroupName.resourcegroup\cluster.folder\$clusterName.cluster"
-NetworkPath "XDHyp:\Connections\$hostingConnectionName\$region.region\
$resourceGroupName.resourcegroup\cluster.folder\
$clusterName.cluster\network.folder\$logicalNetworkName.network"
-StoragePath "XDHyp:\Connections\$hostingConnectionName\$region.region\
$resourceGroupName.resourcegroup\cluster.folder\
$clusterName.cluster\storage.folder\$storagePathName.storage" -JobGroup
$guid
```

必要なAzure Localのアクセス許可

共同作成者ロールは、すべてのリソースを管理するためのフルアクセス権を持ち、現在の機能セットで必要とされる以上のアクセス許可が含まれていますが、今後も最高の互換性を提供します。このセクションでは、Azure Localに必要な最小限のアクセス許可について詳しく説明します。

最小限の権限

VMの電源管理

```
"Microsoft.Resources/tenants/read",

"Microsoft.Resources/subscriptions/read",

"Microsoft.Resources/subscriptions/locations/read",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.AzureStackHCI/VirtualMachines/Read",

"Microsoft.AzureStackHCI/virtualMachineInstances/Read",

"Microsoft.AzureStackHCI/LogicalNetworks/Read",

"Microsoft.AzureStackHCI/StorageContainers/Read",

"Microsoft.AzureStackHCI/Clusters/Read",

"Microsoft.AzureStackHCI/VirtualMachineInstances/start/action",
```

```
"Microsoft.AzureStackHCI/VirtualMachineInstances/stop/action",

"Microsoft.AzureStackHCI/VirtualMachineInstances/restart/action"

"Microsoft.ExtendedLocation/CustomLocations/Read",

"Microsoft.KubernetesConfiguration/extensions/read",

"Microsoft.HybridCompute/machines/read"
```

仮想マシンの作成、更新、または削除

```
"Microsoft.Resources/tenants/read",

"Microsoft.Resources/subscriptions/read",

"Microsoft.Resources/subscriptions/locations/read",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourceGroups/write",

"Microsoft.Resources/subscriptions/resourceGroups/delete",
```

```
"Microsoft.HybridCompute/machines/read",

"Microsoft.HybridCompute/machines/write",

"Microsoft.HybridCompute/machines/delete",

"Microsoft.AzureStackHCI/Clusters/Read",

"Microsoft.AzureStackHCI/VirtualMachines/Read",

"Microsoft.AzureStackHCI/VirtualMachines/Write",

"Microsoft.AzureStackHCI/VirtualMachines/Delete",

"Microsoft.AzureStackHCI/virtualMachineInstances/Read",

"Microsoft.AzureStackHCI/virtualMachineInstances/Write",

"Microsoft.AzureStackHCI/virtualMachineInstances/Delete",

"Microsoft.AzureStackHCI/VirtualMachineInstances/start/action",
```

```
"Microsoft.AzureStackHCI/VirtualMachineInstances/stop/action",

"Microsoft.AzureStackHCI/VirtualMachineInstances/restart/action",

"Microsoft.AzureStackHCI/LogicalNetworks/Read",

"Microsoft.AzureStackHCI/LogicalNetworks/join/action",

"Microsoft.AzureStackHCI/StorageContainers/Read",

"Microsoft.AzureStackHCI/StorageContainers/deploy/action",

"Microsoft.AzureStackHCI/GalleryImages/Read",

"Microsoft.AzureStackHCI/GalleryImages/Write",

"Microsoft.AzureStackHCI/GalleryImages/Delete",

"Microsoft.AzureStackHCI/GalleryImages/deploy/action",

"Microsoft.AzureStackHCI/NetworkInterfaces/Read",
```

```
"Microsoft.AzureStackHCI/NetworkInterfaces/Write",

"Microsoft.AzureStackHCI/NetworkInterfaces/Delete",

"Microsoft.AzureStackHCI/networkInterfaces/join/action",

"Microsoft.AzureStackHCI/VirtualHardDisks/Read",

"Microsoft.AzureStackHCI/VirtualHardDisks/Write",

"Microsoft.AzureStackHCI/VirtualHardDisks/Delete",

"Microsoft.AzureStackHCI/VirtualHardDisks/upload/action",

"Microsoft.AzureStackHCI/VirtualHardDisks/join/action",

"Microsoft.AzureStackHCI/marketplaceGalleryImages/deploy/action",

"Microsoft.ExtendedLocation/CustomLocations/Read",

"Microsoft.ExtendedLocation/customLocations/deploy/action",
```

```
"Microsoft.KubernetesConfiguration/extensions/read",

"Microsoft.Compute/disks/read",

"Microsoft.Compute/disks/write",

"Microsoft.Compute/disks/delete",

"Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.Compute/disks/endGetAccess/action",

"Microsoft.Compute/snapshots/read",

"Microsoft.Compute/snapshots/write",

"Microsoft.Compute/snapshots/delete",

"Microsoft.Compute/snapshots/beginGetAccess/action",
```

```
"Microsoft.Compute/snapshots/endGetAccess/action"
```

次のステップ

- Azure Local マシンカタログの作成については、Azure Local マシンカタログの作成を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

XenServer®への接続

「接続とリソースの作成および管理」(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/connections.html)では、接続を作成するウィザードについて説明します。以下の情報は、XenServer仮想化環境に固有の詳細を扱っています。

> **注:**
>
> XenServerへの接続を作成する前に、まずXenServerアカウントをリソースの場所として設定を完了する必要があります。「XenServer仮想化環境」(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/install-prepare/xenserver.html)を参照してください。

XenServerへの接続を作成する

XenServer（旧Citrix Hypervisor™）への接続を作成する際は、VM Power Admin以上の権限を持つユーザーの資格情報を指定する必要があります。

Citrixでは、XenServerとの通信を保護するためにHTTPSを使用することを推奨しています。HTTPSを使用するには、XenServerにインストールされているデフォルトの SSL証明書を置き換える必要があります。

XenServerサーバーで高可用性が有効になっている場合、高可用性を構成できます。Citrix Virtual Apps and Desktopsバージョン2507 LTSR以降では、HTTPSを使用しており、高可用性サーバーを構成したい場合、プール内のすべてのサーバーにワイルドカード証明書をインストールできます。ただし、2507 LTSRより前のバージョンでは、各サーバーに個別の証明書が必要です。

XenServerがvGPUをサポートしている場合、GPUの種類とグループを選択するか、パススルーすることができます。表示は、選択に専用GPUリソースがあるかどうかを示します。

1つ以上のXenServerホストで一時データストレージにローカルストレージを使用する場合、プール内の各ストレージの場所に一意の名前があることを確認してください。（XenCenter®で名前を変更するには、ストレージを右クリックして名前プロパティを編集します。）

Citrix Provisioning（旧Provisioning Services）およびMachine Creation Services™（MCS）を使用して、以下をプロビジョニングできます。

- サポートされているデスクトップまたはサーバーOS VM用のレガシーBIOS。
- セキュアブートを含む、サポートされているデスクトップまたはサーバーOS VM用のUEFI。

> **注:**
>
> MCSを構成する際には、プールオペレーター以上の権限が必要です。

XenServer接続にIntelliCache™を使用する

IntelliCacheを使用すると、共有ストレージとローカルストレージの組み合わせを使用できるため、ホスト型VDI展開の費用対効果が高まります。これにより、パフォーマンスが向上し、ネットワークトラフィックが削減されます。ローカルストレージは共有ストレージからマスターイメージをキャッシュするため、共有ストレージへの読み取り回数が減少します。共有デスクトップの場合、差分ディスクへの書き込みは、共有ストレージではなくホスト上のローカルストレージに書き込まれます。

- IntelliCacheを使用する場合、共有ストレージはNFSである必要があります。
- Citrixでは、可能な限り最速のデータ転送を確保するために、高性能なローカルストレージデバイスを使用することを推奨しています。

IntelliCacheを使用するには、この製品とXenServerの両方で有効にする必要があります。

- XenServerをインストールする際に、**Enable thin provisioning (Optimized storage for Virtual Desktops)** を選択します。Citrixは、IntelliCacheが有効なサーバーと有効でないサーバーが混在するプールをサポートしていません。詳細については、XenServerのドキュメントを参照してください。
- Citrix Virtual Apps and Desktops™では、IntelliCacheはデフォルトで無効になっています。この設定はXenServer接続を作成するときにのみ変更でき、後でIntelliCacheを無効にすることはできません。XenServer接続を追加する際：

- ストレージの種類として**「Shared」**を選択します。
- 「**IntelliCache を使用**」チェックボックスをオンにします。

必要なXenServer権限

XenServerの権限はロールベース（RBAC）です。XenServerのロールベースアクセス制御（RBAC）機能を使用すると、ユーザー、ロール、および権限を割り当てて、XenServerへのアクセス権を持つユーザーと、それらのユーザーが実行できるアクションを制御できます。XenServer RBACシステムは、ユーザー（またはユーザーグループ）を定義されたロール（名前付きの権限セット）にマッピングします。ロールには、特定の操作を実行するための関連するXenServer権限があります。

詳細については、「Role-based access control」を参照してください。

権限が増加する順序でのロール階層は、次のとおりです。Read-Only → VM Operator → VM Admin → VM Power Admin → Pool Operator → Pool Admin。

次のセクションでは、各プロビジョニングタスクに必要な最小ロールをまとめます。

ホスト接続の作成

タスク	必要な最小ロール
XenServerから取得した情報を使用してホスト接続を追加する	読み取り専用
ユーザーとその割り当てられた役割を表示する	読み取り専用

VMの電源管理

タスク	必要な最小限の役割
VMの電源をオンまたはオフにする	VMオペレーター

VMの作成、更新、または削除

タスク	必要な最小限の役割
既存のスナップショットスケジュールにVMを追加または削除する	VM電源管理者

タスク	必要な最小限の役割
スナップショットスケジュールの追加、変更、削除	プールオペレーター
マスターイメージの公開	プールオペレーター（スイッチポートロックが必要）
マシンカタログの作成	プールオペレーター: スイッチポートロックが必要
VMの追加または削除（GPU対応VMではない）	VM管理者
VMの追加または削除（GPU対応VM）	プールオペレーター
仮想ディスクまたはCDデバイスの追加、削除、または構成	VM管理者
タグの管理	VMオペレーター

RBACの役割と権限の詳細については、「RBACの役割と権限」を参照してください。

スイッチポートロックの詳細については、「スイッチポートロックの使用」を参照してください。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- XenServer 固有の情報については、XenServer カタログの作成を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

Google Cloud環境への接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明します。以下の情報は、Google Cloud環境に固有の詳細を扱っています。

> **注:**

> Google Cloud環境への接続を作成する前に、まずリソースロケーションとしてGoogle Cloudアカウントの設定を完了する必要があります。Google Cloud環境を参照してください。

接続の追加

接続とリソースの作成のガイダンスに従ってください。以下の説明は、ホスティング接続の設定について案内します。

1. **管理 > 構成**から、左側のペインで**ホスティング**を選択します。
2. アクションバーで**「接続とリソースの追加」**を選択します。
3. **「接続」ページで、「新しい接続の作成」と「Citrix provisioning™ tools」を選択し、「次へ」**を選択します。
   - **接続の種類**。メニューから**Google Cloud**を選択します。
   - **接続名**。接続の名前を入力します。
4. **「リージョン」**ページで、メニューからプロジェクト名を選択し、使用するリソースを含むリージョンを選択してから、**「次へ」**を選択します。
5. **「ネットワーク」**ページで、リソースの名前を入力し、メニューから仮想ネットワークを選択し、サブセットを選択してから、**「次へ」**を選択します。リソース名は、リージョンとネットワークの組み合わせを識別するのに役立ちます。名前に*「(Shared)」*サフィックスが付いている仮想ネットワークは、共有VPCを表します。共有VPCのサブネットレベルのIAMロールを構成した場合、共有VPCの特定のサブネットのみがサブネットリストに表示されます。

   > **注:**
   >
   > - リソース名には1～64文字を含めることができ、空白のみ、または文字`\ / ; : # . * ? = < > | [ ] { } " ' ( ) ' )`を含めることはできません。

6. **「概要」**ページで情報を確認し、**「完了」**を選択して**「接続とリソースの追加」**ウィンドウを終了します。

接続とリソースを作成すると、作成した接続とリソースが一覧表示されます。接続を構成するには、接続を選択し、アクションバーで該当するオプションを選択します。

同様に、接続の下に作成されたリソースを削除、名前変更、またはテストできます。これを行うには、接続の下のリソースを選択し、アクションバーで該当するオプションを選択します。

サービスエンドポイントURL

次のURLにアクセスできる必要があります。

- `https://oauth2.googleapis.com`
- `https://cloudresourcemanager.googleapis.com`
- `https://compute.googleapis.com`
- `https://storage.googleapis.com`
- `https://cloudbuild.googleapis.com`

Google Cloudプロジェクト

Google Cloudプロジェクトには基本的に2つのタイプがあります。

- プロビジョニングプロジェクト：この場合、現在の管理者アカウントがプロジェクト内のプロビジョニングされたマシンを所有します。このプロジェクトはローカルプロジェクトとも呼ばれます。
- 共有VPCプロジェクト: プロビジョニングプロジェクトで作成されたマシンが、共有VPCプロジェクトのVPCを使用するプロジェクト。プロビジョニングプロジェクトに使用される管理者アカウントは、このプロジェクトで限られた権限、具体的にはVPCを使用する権限のみを持ちます。

GCP管理トラフィックのセキュアな環境を作成する

Google Cloudプロジェクトへのプライベートアクセスを許可できます。この実装により、機密データを処理するためのセキュリティが強化されます。これを実現するには、次のいずれかを実行できます。

- Cloud BuildサービスアカウントのVPCサービスコントロールの以下のイングレスルールを含めます。この手順を実行する場合は、GCP管理トラフィックのセキュアな環境を作成するための以下の手順に従わないでください。

```
Ingress Rule 1

From:

Identities:

<ProjectID>@cloudbuild.gserviceaccount.com

Source > All sources allowed
```

```
To:

Projects =

All projects

Services =

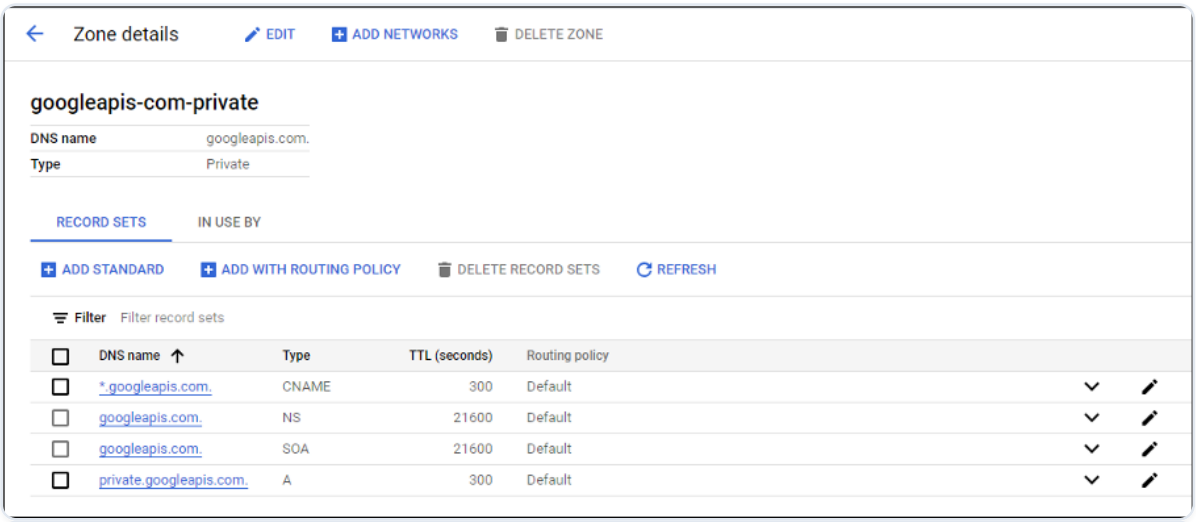
Service name: All services
```

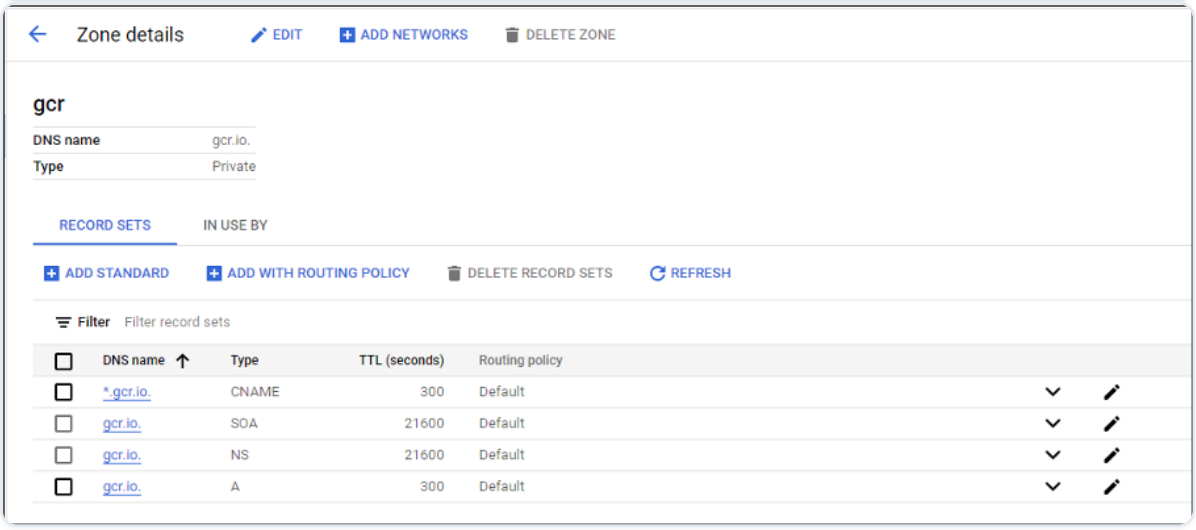
- プライベートワーカープールを使用している場合は、`CustomProperties`に`UsePrivateWorkerPool`を追加します。プライベートワーカープールの詳細については、プライベートプール概要を参照してください。

GCP管理トラフィックのセキュアな環境を作成するための要件

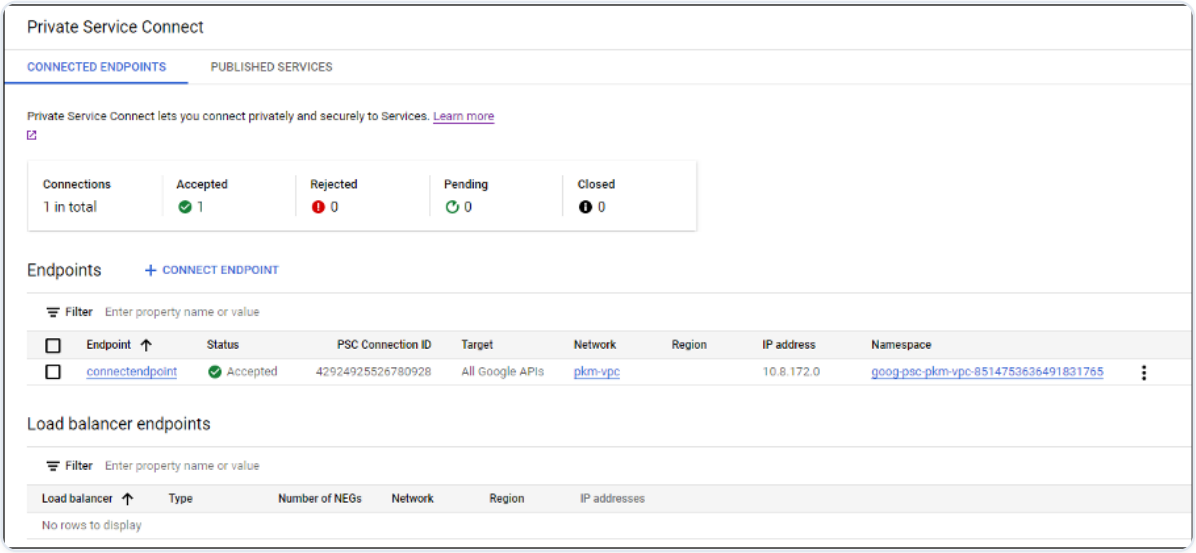
GCP管理トラフィックのセキュアな環境を作成するための要件は次のとおりです。

- カスタムプロパティを更新する際は、ホスティング接続がメンテナンスモードであることを確認してください。
- プライベートワーカープールを使用するには、次の変更が必要です。
  - Citrix Cloud™サービスアカウントには、以下のIAMロールを追加します。
    - Cloud Build サービスアカウント
    - Compute Instance 管理者
    - サービスアカウントユーザー
    - サービスアカウントトークン作成者
    - Cloud Build WorkerPool オーナー
  - ホスティング接続の作成に使用するのと同じプロジェクトにCitrix Cloudサービスアカウントを作成します。
  - DNS構成で説明されているように、`private.googleapis.com`および`gcr.io`のDNSゾーンを設定します。

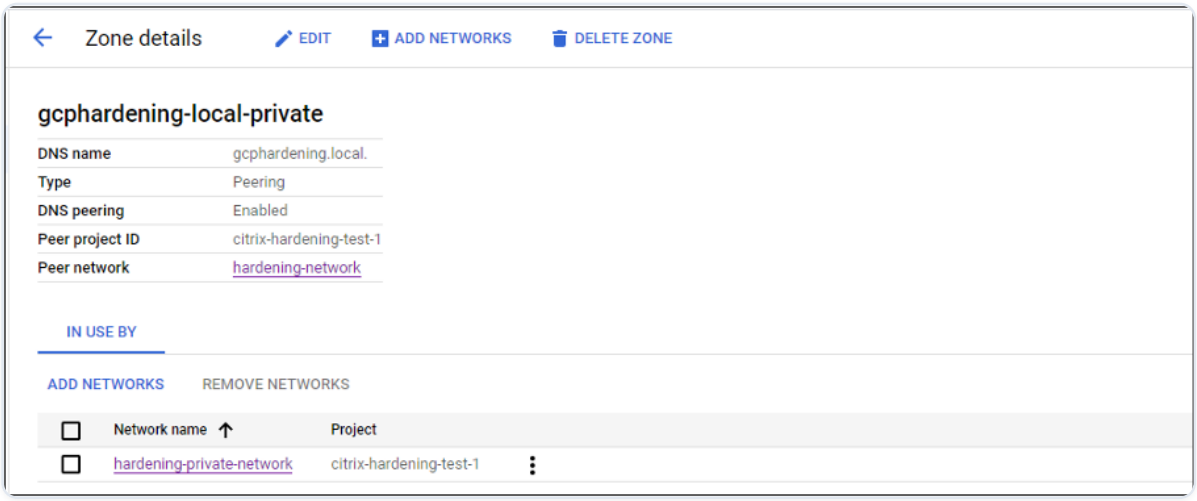




- プライベートネットワークアドレス変換 (NAT) を設定するか、プライベートサービス接続を使用します。詳細については、「エンドポイントを介したGoogle APIへのアクセス」を参照してください。



- ピアリングされたVPCを使用している場合は、ピアリングされたVPCへのCloud DNSゾーンピアリングを作成します。詳細については、「ピアリングゾーンの作成」を参照してください。



- VPCサービスコントロールで、APIとVMがインターネットと通信できるようにエグレスルールを設定します。イングレスルールはオプションです。例：

```
Egress Rule 1

From:

Identities:ANY_IDENTITY

To:

Projects =

All projects

Service =

Service name: All services
```

プライベートワーカープールを有効にする

プライベートワーカープールを有効にするには、ホスト接続でカスタムプロパティを次のように設定します。

1. Delivery ControllerホストからPowerShellウィンドウを開くか、Remote PowerShell SDKを使用します。Remote PowerShell SDKの詳細については、「SDKとAPI」を参照してください。
2. 次のコマンドを実行します。

a. `Add-PSSnapin citrix®*`

b. `cd XDHyp:\Connections\`

c. `dir`

3. 接続から`CustomProperties`をメモ帳にコピーします。
4. プロパティ設定`<Property xsi:type="StringProperty" Name="UsePrivateWorkerPool" Value="True"/>`を追加します。例：

```
```

<CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://schemas.citrix.com/2014/xd/machinecreation">

<Property xsi:type="StringProperty" Name="UsePrivateWorkerPool"
Value="True"/>

</CustomProperties>

```
```

5. PowerShellウィンドウで、変更されたカスタムプロパティに変数を割り当てます。例：`$customProperty = '<CustomProperties…</CustomProperties>'`。
6. `$gcpServiceAccount = "<ENTER YOUR SERVICE ACCOUNT EMAIL HERE>"`を実行します。
7. `$gcpPrivateKey = "<ENTER YOUR SERVICE ACCOUNT PRIVATE KEY HERE AFTER REMOVING ALL INSTANCES OF \n >"`を実行します。
8. `$securePassword = ConvertTo-SecureString $gcpPrivateKey -AsPlainText -Force`を実行します。
9. 既存のホスト接続を更新するには、以下を実行します。

```
Set-Item -PassThru -Path @('XDHyp:\\Connections\\<ENTER YOUR CONNECTION
NAME HERE>') -SecurePassword $securePassword -UserName
$gcpServiceAccount -CustomProperties $customProperty
```

CMEK のグローバルキーとリージョンキーを指定する

注:

> GCP での CMEK のサポートは現在プレビュー中です。

> GCP には、顧客管理の暗号化キー (CMEK) には次の2種類があります。

- リージョン：同じリージョン内のリソースのみが使用できる暗号化キー。
- グローバル：複数のリージョンのリソースが使用できる暗号化キー。

サービスアカウントがアクセスできるすべてのプロジェクトから、グローバルまたはリージョンの顧客管理暗号化キー (CMEK) を参照して使用できます。その後、そのキーを使用して CMEK 対応の MCS マシンカタログを作成し、`Set-ProvScheme` コマンドを使用して既存の CMEK 対応 MCS マシンカタログを更新できます。PowerShell を使用して CMEK 対応カタログを作成する方法については、「カスタムプロパティを使用して CMEK でカタログを作成する」を参照してください。

この機能には、次の2つのサービスアカウントに対する追加の権限が必要です。

- ホスティング接続が作成される現在のプロジェクトのサービスアカウント。
- 現在のプロジェクトの Compute Engine Service Agent (メールアドレス: `service-PROJECT_NUMBER@compute-system.iam.gserviceaccount.com`)。詳細については、「Compute Engine Service Agent」を参照してください。

サービスアカウントでは、使用したい暗号キーがあるプロジェクト (共有プロジェクトなど) で、次の役割を割り当てる必要があります。

- Cloud KMS 閲覧者
- Cloud KMS 暗号鍵 暗号化担当者/復号化担当者

役割を割り当てない場合は、以下の権限があることを確認してください。

- resourcemanager.projects.get
- cloudkms.keyRings.list
- cloudkms.keyRings.get
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.cryptoKeyVersions.useToDecrypt
- cloudkms.cryptoKeyVersions.useToEncrypt

暗号化キーを一覧表示する

PowerShellコマンドを使用して、同じプロジェクト内およびアクセス可能な他のすべてのプロジェクト内のグローバルおよびリージョンの暗号化キーを一覧表示できます。これを行うには、:

1. Delivery Controller™ホストまたはリモートPowerShellからPowerShellウィンドウを開きます。
2. コマンド `asnp citrix*` を実行して、Citrix固有のPowerShellモジュールをロードします。
3. 次のコマンドを実行して、暗号化キーを一覧表示します。例:

   - `encryptionKeys` フォルダーの内容を一覧表示するには:

     ```
     Get-ChildItem XDHyp:\HostingUnits\my-
     hostingunit\encryptionKeys.folder
     ```

   - 同じプロジェクト内でグローバル暗号化キーを取得するには：

     ```
     Get-Item XDHyp:\HostingUnits\my-
     hostingunit\encryptionKeys.folder\myglobalkeyring.globalkeyring\mygl
     obalkey.cryptokey
     ```

   - 同じプロジェクト内でリージョン暗号化キーを取得するには：

     ```
     Get-Item XDHyp:\HostingUnits\my-
     hostingunit\encryptionKeys.folder\regional-ring.keyring\shared-
     key.cryptokey
     ```

   - アクセス可能な別のプロジェクト（例：myanotherproject）からグローバル暗号化キーを取得するには：

     ```
     Get-Item XDHyp:\HostingUnits\my-
     hostingunit\encryptionKeys.folder\myanotherproject.project\shared-
     global-ring.globalkeyring\shared-key.cryptokey
     ```

   - アクセス可能な別のプロジェクト（例：myanotherproject）からリージョン暗号化キーを取得するには：

```
Get-Item XDHyp:\HostingUnits\my-
hostingunit\encryptionKeys.folder\myanotherproject .project.project\
shared-uscentral.keyring\shared-uscentral-key.cryptokey
```

注:

- グローバルキーリングのキーリングインベントリアイテムの拡張子は`.globalkeyring`です。
- グローバルキーリングのIDには、`global`という単語が含まれています。

必要なGCP権限

このセクションには、GCP権限の完全なリストが含まれています。機能が正しく動作するように、このセクションに記載されている権限の完全なセットを使用してください。

注:

GCPは、Cloud Build Servicesのデフォルトの動作とサービスアカウントの使用に関して、April 29, 2024以降に変更を導入します。詳細については、Cloud Build Service Account Changeを参照してください。April 29, 2024より前にCloud Build APIが有効になっている既存のGoogleプロジェクトは、この変更の影響を受けません。ただし、April 29以降も既存のCloud Build Serviceの動作を維持したい場合は、APIを有効にする前に、制約の適用を無効にする組織ポリシーを作成または適用できます。新しい組織ポリシーを設定した場合、このセクションの既存の権限と、**Cloud Build Service Account Change前**とマークされている項目を引き続き使用できます。そうでない場合は、既存の権限と、**Cloud Build Service Account Change後**とマークされている項目に従ってください。

ホスト接続の作成

- プロビジョニングプロジェクトのCitrix Cloudサービスアカウントに必要な最小限の権限：

```
compute.instanceTemplates.list

compute.instances.list

compute.networks.list
```

```
compute.projects.get

compute.regions.list

compute.subnetworks.list

compute.zones.list

resourcemanager.projects.get
```

次の Google 定義ロールには、上記にリストされている権限があります:

- Compute 管理者
- クラウド データストア ユーザー

- 共有 VPC プロジェクト内の Citrix Cloud サービスアカウントの共有 VPC に必要な追加の権限:

```
compute.networks.list

compute.subnetworks.list

resourcemanager.projects.get
```

次の Google 定義ロールには、上記にリストされている権限があります:

- コンピュート ネットワーク ユーザー

- サービスアカウントでは、使用する暗号鍵があるプロジェクト (共有プロジェクトなど) に次のロールを割り当てる必要があります:
  - Cloud KMS 閲覧者
  - Cloud KMS クリプトキー 暗号化/復号化担当者

  ロールを割り当てない場合は、次の権限があることを確認してください:
  - resourcemanager.projects.get
  - cloudkms.keyRings.list
  - cloudkms.keyRings.get
  - cloudkms.cryptoKeys.get

- cloudkms.cryptoKeys.list
- cloudkms.cryptoKeyVersions.useToDecrypt
- cloudkms.cryptoKeyVersions.useToEncrypt

仮想マシンの電源管理

電源管理のみのカタログの場合に、プロビジョニングプロジェクト内のCitrix Cloudサービスアカウントに必要な最小限の権限:

```
compute.instanceTemplates.list

compute.instances.list

compute.instances.get

compute.instances.reset

compute.instances.resume

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.networks.list

compute.projects.get

compute.regions.list

compute.subnetworks.list

compute.zones.list

resourcemanager.projects.get

compute.zoneOperations.get
```

次のGoogle定義のロールは、上記の権限を持っています:

- Compute管理者

- クラウド データストア ユーザー

仮想マシンの作成、更新、または削除

- プロビジョニングプロジェクト内のCitrix Cloudサービスアカウントに必要な最小限の権限:

```
cloudbuild.builds.create

cloudbuild.builds.get

cloudbuild.builds.list

compute.acceleratorTypes.list

compute.diskTypes.get

compute.diskTypes.list

compute.disks.create

compute.disks.createSnapshot

compute.disks.delete

compute.disks.get

compute.disks.list

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.firewalls.create

compute.firewalls.delete

compute.firewalls.list

compute.globalOperations.get

compute.images.create
```

```
compute.images.delete

compute.images.get

compute.images.list

compute.images.setLabels

compute.images.useReadOnly

compute.instanceTemplates.create

compute.instanceTemplates.delete

compute.instanceTemplates.get

compute.instanceTemplates.list

compute.instanceTemplates.useReadOnly

compute.instances.attachDisk

compute.instances.create

compute.instances.delete

compute.instances.detachDisk

compute.instances.get

compute.instances.getSerialPortOutput

compute.instances.list

compute.instances.reset

compute.instances.resume

compute.instances.setDeletionProtection

compute.instances.setLabels

compute.instances.setMetadata
```

```
compute.instances.setServiceAccount

compute.instances.setTags

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.machineTypes.get

compute.machineTypes.list

compute.networks.list

compute.networks.updatePolicy

compute.nodeGroups.list

compute.nodeTemplates.get

compute.projects.get

compute.regions.list

compute.snapshots.create

compute.snapshots.delete

compute.snapshots.list

compute.snapshots.get

compute.snapshots.setLabels

compute.snapshots.useReadOnly

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use
```

```
compute.zoneOperations.get

compute.zoneOperations.list

compute.zones.get

compute.zones.list

iam.serviceAccounts.actAs

resourcemanager.projects.get

storage.buckets.create

storage.buckets.delete

storage.buckets.get

storage.buckets.list

storage.buckets.update

storage.objects.create

storage.objects.delete

storage.objects.get

storage.objects.list

compute.networks.get

compute.resourcePolicies.use
```

以下のGoogle定義ロールには、上記にリストされている権限があります:

- Compute管理者
- Storage管理者
- Cloud Build編集者
- サービスアカウントユーザー

  - クラウド データストア ユーザー

- 共有VPCプロジェクトのVPCとサブネットワークを使用してホスティングユニットを作成するために、共有VPCプロジェクト内のCitrix Cloudサービスアカウントの共有VPCに追加で必要な権限:

```
compute.firewalls.list

compute.networks.list

compute.projects.get

compute.regions.list

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.zones.list

resourcemanager.projects.get
```

以下のGoogle定義ロールには、上記にリストされている権限があります:

  - コンピュートネットワークユーザー
  - クラウド データストア ユーザー

MCSに準備指示ディスクをダウンロードする際に必要な最小限の権限:

  - (Cloud Buildサービスアカウント変更前): プロビジョニングプロジェクトのCloud Buildサービスアカウントにこれらの権限を割り当てます。
  - (Cloud Buildサービスアカウント変更後): プロビジョニングプロジェクトのCloud Computeサービスアカウントにこれらの権限を割り当てます。

```
compute.disks.create

compute.disks.delete

compute.disks.get
```

```
compute.disks.list

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.images.get

compute.images.list

compute.images.useReadOnly

compute.instances.create

compute.instances.delete

compute.instances.get

compute.instances.getSerialPortOutput

compute.instances.list

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setServiceAccount

compute.machineTypes.list

compute.networks.get

compute.networks.list

compute.projects.get

compute.subnetworks.list

compute.subnetworks.use

compute.subnetworks.useExternalIp
```

```
compute.zoneOperations.get

compute.zones.list

iam.serviceAccounts.actAs

logging.logEntries.create

pubsub.topics.publish

resourcemanager.projects.get

source.repos.get

source.repos.list

storage.buckets.create

storage.buckets.get

storage.buckets.list

storage.objects.create

storage.objects.delete

storage.objects.get

storage.objects.list
```

以下のGoogle定義ロールには、上記にリストされている権限があります:

- Cloud Build サービスアカウント (Cloud Build サービスアカウント変更後はCloud Compute サービスアカウント)
- コンピュートインスタンス管理者
- サービスアカウントユーザー

- MCSに準備指示ディスクをダウンロードする際に、Google Cloud Buildサービスによってプロビジョニングプロジェクトの Cloud Compute サービスアカウントに必要とされる最小限の権限:

```
resourcemanager.projects.get

storage.objects.create

storage.objects.get

storage.objects.list
```

以下のGoogle定義ロールには、上記にリストされている権限があります:

- コンピュートネットワークユーザー
- ストレージアカウントユーザー
- クラウド データストア ユーザー

MCSに準備指示ディスクをダウンロードする際に、共有VPCに必要とされる追加の権限:

- (Cloud Buildサービスアカウント変更前): プロビジョニングプロジェクトのCloud Buildサービスアカウントにこれらの権限を割り当てます。
- (Cloud Buildサービスアカウント変更後): プロビジョニングプロジェクトのCloud Computeサービスアカウントにこれらの権限を割り当てます。

```
compute.firewalls.list

compute.networks.list

compute.subnetworks.list

compute.subnetworks.use

resourcemanager.projects.get
```

以下のGoogle定義ロールには、上記にリストされている権限があります:

- コンピュートネットワークユーザー
- ストレージアカウントユーザー
- クラウド データストア ユーザー

- プロビジョニングプロジェクトのCitrix CloudサービスアカウントのCloud Key Management Service (KMS) に必要な追加権限:

```
cloudkms.cryptoKeys.get

cloudkms.cryptoKeys.list

cloudkms.keyRings.get

cloudkms.keyRings.list
```

以下のGoogle定義ロールには、上記にリストされている権限があります:

- Compute KMS 閲覧者

一般的な権限

以下は、MCSでサポートされているすべての機能について、プロビジョニングプロジェクトのCitrix Cloudサービスアカウントの権限です。これらの権限は、今後最高の互換性を提供します:

```
resourcemanager.projects.get

cloudbuild.builds.create

cloudbuild.builds.get

cloudbuild.builds.list

compute.acceleratorTypes.list

compute.diskTypes.get

compute.diskTypes.list

compute.disks.create

compute.disks.createSnapshot

compute.disks.delete

compute.disks.get

compute.disks.setLabels

compute.disks.use
```

```
compute.disks.useReadOnly

compute.firewalls.create

compute.firewalls.delete

compute.firewalls.list

compute.globalOperations.get

compute.images.create

compute.images.delete

compute.images.get

compute.images.list

compute.images.setLabels

compute.images.useReadOnly

compute.instanceTemplates.create

compute.instanceTemplates.delete

compute.instanceTemplates.get

compute.instanceTemplates.list

compute.instanceTemplates.useReadOnly

compute.instances.attachDisk

compute.instances.create

compute.instances.delete

compute.instances.detachDisk

compute.instances.get

compute.instances.getSerialPortOutput
```

```
compute.instances.list

compute.instances.reset

compute.instances.resume

compute.instances.setDeletionProtection

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setTags

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.instances.update

compute.instances.updateAccessConfig

compute.instances.updateDisplayDevice

compute.instances.updateSecurity

compute.instances.updateShieldedInstanceConfig

compute.instances.updateShieldedVmConfig

compute.machineTypes.get

compute.machineTypes.list

compute.networks.list

compute.networks.updatePolicy

compute.nodeGroups.list

compute.nodeTemplates.get
```

```
compute.projects.get

compute.regions.list

compute.snapshots.create

compute.snapshots.delete

compute.snapshots.list

compute.snapshots.get

compute.snapshots.setLabels

compute.snapshots.useReadOnly

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.subnetworks.useExternalIp

compute.zoneOperations.get

compute.zoneOperations.list

compute.zones.get

compute.zones.list

resourcemanager.projects.get

storage.buckets.create

storage.buckets.delete

storage.buckets.get

storage.buckets.list

storage.buckets.update
```

```
storage.objects.create

storage.objects.delete

storage.objects.get

storage.objects.list

cloudkms.cryptoKeys.get

cloudkms.cryptoKeys.list

cloudkms.keyRings.get

cloudkms.keyRings.list

compute.disks.list

compute.instances.setServiceAccount

compute.networks.get

compute.networks.use

compute.networks.useExternalIp

iam.serviceAccounts.actAs

compute.resourcePolicies.use

cloudkms.cryptoKeyVersions.useToDecrypt

cloudkms.cryptoKeyVersions.useToEncrypt
```

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- Google Cloud Platform (GCP)固有の情報については、Google Cloud Platformカタログの作成を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

HPE Moonshotへの接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明します。以下の情報は、HPE Moonshotに固有の詳細を扱います。

> **注:**
>
> HPE Moonshotへの接続を作成する前に、まずHPEアカウントの設定を完了する必要があります。HPE Moonshot仮想化環境を参照してください。

接続を作成する

HPE Moonshotへの接続は、以下を使用して作成できます。

- ウェブスタジオ
- PowerShellコマンド

Web Studioを使用して接続を作成する

1. **接続とリソースの追加**ページで、接続の種類として**HPE Moonshot**を選択します。
2. Moonshot iLO Chassis Managerの接続アドレスを入力します。アドレスには、IPアドレス、ホスト名、またはFQDNを使用できます。
3. シャーシの管理資格情報と、わかりやすい接続名を入力します。

接続設定は、次のいずれかの状況で停止します。

- Citrix Virtual Apps and Desktops™がエラーのある公開CA署名付き証明書を受信した場合：エラーメッセージが表示されます。画面の指示に従って問題を修正してください。修正しないと、接続の作成に進むことはできません。
- Citrix Virtual Apps and Desktops™がプライベートCA署名付き証明書を受信した場合。警告ページが表示されます。受信したサムプリントをサーバーの証明書の有効性と比較します。有効な場合は、**証明書を信頼する**を選択し、**OK**をクリックして接続の作成に進みます。Citrix Virtual Apps and Desktopsはその後、証明書を信頼し、将来の検証のためにサムプリントを保存します。

PowerShellコマンドを使用して接続を作成する

PowerShellコマンドを使用して接続を作成する場合、次の情報を提供します。

- IP: HPEサーバーのIPアドレス
- ユーザー名: HPEユーザー名
- パスワード: HPEパスワード

例:

```
New-Item -ConnectionType "Custom" -HypervisorAddress $IP -Metadata
@{"Citrix_Orchestration_Hypervisor_Secret_Allow_Edit"="false"} -Path
@("XDHyp:\Connections\$connectionName") -Persist -PluginId
"HPMoonshotFactory" -Scope @() -SecurePassword $Password -UserName
$UserName -sslthumbprint $SslThumbprint New-BrokerHypervisorConnection
-HypHypervisorConnectionUid $HypervisorConnectionID
```

注:

`sslthumbprint` パラメーターは、プライベートCA署名付き証明書の場合にのみ必要です。

証明書とサムプリントの検証

HPE Moonshot への接続を正常に作成するには、証明書にエラーがなく、サムプリントが正しい値である必要があります。証明書とサムプリントの検証に関連するユースケースは次のとおりです。

- 公開CA署名証明書にエラーがあります。接続は正常に作成されません。エラーの詳細を確認し、問題を解決してください。
- エラーのない公開CA署名証明書。接続は正常に作成され、`SslThumbprints` の値は**Null**です。
- エラーがなく、`sslthumbprint` 値を持つプライベートCA署名証明書。正しい `SslThumbprints` 値で接続が正常に作成されます。
- サムプリント値が正しくないプライベートCA署名証明書。接続は正常に作成されません。
- エラーのないプライベートCA署名証明書。接続は正常に作成されます。接続作成時、`SSlThumbprints` は**Null**です。`SSlThumbprints` 値はサイトサービスによって値に更新されます。

> **注:**
>
> Citrix Database と Moonshot サーバー間の証明書サムプリントの不一致は、Web Studio で警告をトリガーします。ただし、この警告はMMCベースのStudioには表示されません。

接続の管理

このセクションでは、接続を管理する方法について詳しく説明します。

- Web Studioを使用して証明書の問題を修正する
- PowerShellコマンドを使用してサムプリント値を更新する

証明書の問題を修正する

証明書の問題が発生すると、Citrix Virtual Apps and DesktopsはHPE Moonshot接続をブロックし、関連するHPE Moonshotノードでのワークロードの配信と管理を妨げます。**ホスト接続**リストの接続の横にエラーアイコンが表示されます。特定の問題と解決策については、次の表を参照してください。

問題	解決策
公開CA署名証明書に証明書エラーが発生する	接続をクリックし、**トラブルシューティング**タブを選択します。エラーの詳細を表示し、問題を解決します。
受信した証明書はプライベートCA署名済みであるか、期限切れです。	証明書のサムプリントを更新するには、ホスト接続を編集します。詳細な手順： 1. 接続を選択し、**接続の編集**をクリックします。 2. **接続プロパティ**ページで、**設定の編集**をクリックします。 3. HPE Moonshotシャーシに接続するためのパス

問題	解決策	
	ワードを入力し、**保存**をクリックします。 4. 表示される**警告**ページで、受信したサムプリントをサーバーのものと比較して、証明書の有効性を確認します。 5. 同じである場合は、**証明書を信頼する**を選択し、**OK**をクリックします。	

サムプリント値を更新する

接続を作成した後、`Set-Item` PowerShellコマンドを使用して接続のサムプリント値を更新できます。たとえば、次のコマンドを実行します。

1. 接続の接続詳細を取得します。例：

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
```

2. サムプリント値を更新します。例:

```
Set-Item -LiteralPath xdhyp:\connections\SinMoonshot-101 -Username
Administrator -SslThumbprint xxxxxxxxxxx12AD048480631BB7AB10D69xxxxx
```

3. 更新されたサムプリント値を確認します。例:

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
```

注:

`Set-Item` コマンドで誤ったサムプリント値を指定すると、更新は失敗します。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- AWS固有の情報については、「HPE Moonshotマシンカタログの作成」を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

Microsoft Azure への接続

(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/connections.html)では、接続を作成するウィザードについて説明します。以下の情報は、Azure Resource Managerクラウド環境に固有の詳細を扱います。

> **注:**
>
> Microsoft Azure への接続を作成する前に、リソースの場所として Azure アカウントの設定を完了する必要があります。「Microsoft Azure Resource Manager クラウド環境」を参照してください。

サービスプリンシパルと接続の作成

接続を作成する前に、接続がAzureリソースにアクセスするために使用するサービスプリンシパルを設定する必要があります。接続は2つの方法で作成できます。

- Web Studio を使用してサービスプリンシパルと接続を同時に作成する
- 以前に作成したサービスプリンシパルを使用して接続を作成する

このセクションでは、次のタスクを完了する方法を示します。

- Web Studio を使用してサービスプリンシパルと接続を作成する
- (/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/connections/connection-azure-resource-manager.html#create-a-service-principal-using-powershell)
- (/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/connections/connection-azure-resource-manager.html#get-the-application-secret-in-azure)

- 既存のサービスプリンシパルを使用して接続を作成する](/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/connections/connection-azure-resource-manager.html#create-a-connection-using-an-existing-service-principal)

考慮事項

- Citrix® は、共同作成者ロールを持つサービスプリンシパルの使用を推奨しています。ただし、最小限の権限のリストについては、「最小限の権限」セクションを参照してください。
- 最初の接続を作成するとき、Azure は必要な権限を付与するよう求めます。今後の接続では、引き続き認証が必要ですが、Azure は以前の同意を記憶しており、プロンプトを再度表示することはありません。
- 認証に使用されるアカウントは、Azure RBAC を使用してサブスクリプション内でロールを割り当てる権限を持っている必要があります。例として、サブスクリプションの所有者、ロールベースのアクセス制御管理者、またはユーザーアクセス管理者などです。
- 認証に使用されるアカウントは、サブスクリプションのディレクトリのメンバーである必要があります。注意すべきアカウントの種類は、「職場または学校」と「個人用 Microsoft アカウント」の2種類です。詳細については、CTX219211 を参照してください。
- 既存の Microsoft アカウントをサブスクリプションのディレクトリのメンバーとして追加して使用することはできますが、ユーザーが以前にディレクトリのリソースのいずれかへのゲストアクセスを許可されていた場合、問題が発生する可能性があります。この場合、ディレクトリ内に必要な権限を付与しないプレースホルダーエントリが存在し、エラーが返される可能性があります。

  ディレクトリからリソースを削除し、明示的に追加し直すことで、これを修正します。ただし、このオプションは、アカウントがアクセスできる他のリソースに意図しない影響を与える可能性があるため、慎重に実行してください。
- 特定のアカウントが実際にはメンバーであるにもかかわらず、ディレクトリゲストとして検出される既知の問題があります。このような構成は、通常、古くから確立されたディレクトリアカウントで発生します。回避策: ディレクトリにアカウントを追加し、適切なメンバーシップ値を取得します。
- リソースグループは単にリソースのコンテナであり、自身のリージョン以外のリージョンからのリソースを含むことができます。これは、リソースグループのリージョンに表示されるリソースが利用可能であると期待している場合、混乱を招く可能性があります。
- 必要な数のマシンをホストするのに十分な大きさのネットワークとサブネットがあることを確認してください。これにはある程度の先見性が必要ですが、Microsoft はアドレス空間の容量に関するガイダンスを提供し、適切な値を指定するのに役立ちます。

Web Studio を使用してサービスプリンシパルと接続を作成する

> **重要:**
>
> この機能は、Azure China サブスクリプションではまだ利用できません。

> Web Studio を使用すると、単一のワークフローでサービスプリンシパルと接続の両方を作成できます。サービスプリンシパルは、接続に Azure リソースへのアクセスを許可します。サービスプリンシパルを作成するために Azure に認証すると、アプリケーションが Azure に登録されます。登録されたアプリケーションには、秘密鍵（クライアントシークレットまたはアプリケーションシークレットと呼ばれます）が作成されます。登録されたアプリケーション（この場合は接続）は、クライアントシークレットを使用して Microsoft Entra ID に認証します。

開始する前に、以下の前提条件を満たしていることを確認してください。

- サブスクリプションのMicrosoft Entraテナントにユーザーアカウントがあること。
- 認証に使用されるアカウントは、Azure RBAC を使用してサブスクリプション内でロールを割り当てる権限を持っている必要があります。例として、サブスクリプションの所有者、ロールベースのアクセス制御管理者、またはユーザーアクセス管理者などです。
- 認証には、グローバル管理者、アプリケーション管理者、またはアプリケーション開発者の権限が必要です。これらの権限は、ホスト接続の作成後に取り消すことができます。ロールの詳細については、Microsoft Entra の組み込みロールを参照してください。

接続とリソースの追加ウィザードを使用して、サービスプリンシパルと接続を一緒に作成します。

1. **接続**ページで、**新しい接続の作成**、**Microsoft Azure**接続タイプ、およびAzure環境を選択します。
2. 仮想マシンを作成するために使用するツールを選択し、**次へ**を選択します。
3. ページで、Azure サブスクリプション ID と接続の名前を入力します。サブスクリプション ID を入力すると、 ボタンが有効になります。

   > **注:**
   >
   > 接続名には 1～64 文字を含めることができ、空白のみ、または文字 `\/;:#.*?=<>|[]{}"'()'` を含めることはできません。

4. **新規作成**を選択し、Microsoft Entraアカウントのユーザー名とパスワードを入力します。
5. **サインイン**を選択します。
6. 「**Accept**」を選択して、Citrix Virtual Apps and Desktops™ に一覧表示された権限を付与します。Citrix Virtual Apps and Desktops は、指定されたユーザーに代わって Azure リソースを管理できるようにするサービスプリンシパルを作成します。
7. 「**Accept**」を選択すると、ウィザードの「**Connection**」ページに戻ります。

> **注:**
>
> Azure への認証が正常に完了すると、「**Create new**」ボタンと「**Use existing**」ボタンが消えます。「**Connection successful**」というテキストが緑色のチェックマークとともに表示され、Azure サブスクリプションへの接続が成功したことを示します。

8. 「**Connection Details**」ページで、「**Next**」を選択します。

> **注:**
>
> Azure への認証が正常に完了し、必要な権限の付与に同意するまで、次のページに進むことはできません。

9. 接続のリソースを構成します。リソースには、リージョンとネットワークが含まれます。
   - 「**地域**」ページで、地域を選択します。
   - 「**ネットワーク**」ページで、次の操作を行います。
     - リージョンとネットワークの組み合わせを識別しやすくするために、1〜64文字のリソース名を入力します。リソース名には、空白のみを含めることや、文字 `\/;:#.*?=<>|[]{}"'()'` を含めることはできません。
     - 仮想ネットワーク/リソースグループのペアを選択します。（同じ名前の仮想ネットワークが複数ある場合、ネットワーク名とリソースグループをペアにすることで、一意の組み合わせが提供されます。）前のページで選択した地域に仮想ネットワークがない場合は、そのページに戻り、仮想ネットワークがある地域を選択してください。
10. 「**概要**」ページで、設定の概要を確認し、「**完了**」を選択してセットアップを完了します。

アプリケーションIDを表示する

接続を作成した後、その接続がAzureリソースへのアクセスに使用するアプリケーションIDを表示できます。

「**Add Connection and Resources**」リストで、接続を選択して詳細を表示します。「**Details**」タブにはアプリケーションIDが表示されます。

PowerShellを使用してサービスプリンシパルを作成する

PowerShellを使用してサービスプリンシパルを作成するには、Azure Resource Managerサブスクリプションに接続し、以下のセクションで提供されているPowerShellコマンドレットを使用します。

次の項目を準備してください。

- **SubscriptionId:** VDAをプロビジョニングするサブスクリプションのAzure Resource Manager `SubscriptionID`。
- **ActiveDirectoryID**: Microsoft Entra IDに登録したアプリケーションのテナントID。
- **ApplicationName:** Microsoft Entra IDで作成するアプリケーションの名前。

詳細な手順は次のとおりです。

Azure Resource Manager サブスクリプションに接続します。

```
`Connect-AzAccount`
```

1. サービスプリンシパルを作成する Azure Resource Manager サブスクリプションを選択します。

   ```
   Get-AzSubscription -SubscriptionId $subscriptionId | Select-AzSubscription
   ```

2. AD テナントにアプリケーションを作成します。

   ```
   $AzureADApplication = New-AzADApplication -DisplayName $ApplicationName
   ```

3. サービスプリンシパルを作成します。

   ```
   New-AzADServicePrincipal -ApplicationId $AzureADApplication.AppId
   ```

4. サービスプリンシパルにロールを割り当てます。

   ```
   New-AzRoleAssignment -RoleDefinitionName Contributor -ServicePrincipalName $AzureADApplication.AppId –scope /subscriptions/$SubscriptionId
   ```

5. PowerShell コンソールの出力ウィンドウから ApplicationId をメモします。ホスト接続を作成する際に、その ID を指定します。

Azure でアプリケーションシークレットを取得する

既存のサービスプリンシパルを使用して接続を作成するには、まず Azure portal でサービスプリンシパルのアプリケーションIDとシークレットを取得する必要があります。

詳細な手順は次のとおりです。

1. Web Studio から、または PowerShell を使用して「**Application ID**」を取得します。
2. Azureポータルにサインインします。
3. Azureで、**Microsoft Entra ID**を選択します。
4. Microsoft Entra IDの**アプリの登録**から、アプリケーションを選択します。
5. **証明書とシークレット**に移動します。
6. **クライアントシークレット**をクリックします。

既存のサービスプリンシパルを使用して接続を作成する

サービスプリンシパルが既にある場合は、それを使用して Web Studio で接続を作成できます。

次の項目を準備してください。

- SubscriptionId
- ActiveDirectoryID (テナントID)
- アプリケーションID
- アプリケーションシークレット

  詳細については、「アプリケーションシークレットの取得」を参照してください。
- シークレットの有効期限

詳細な手順は次のとおりです。

接続とリソースの追加ウィザードで、次の手順を実行します。

1. **接続**ページで、**新しい接続の作成**、**Microsoft Azure**接続タイプ、およびAzure環境を選択します。
2. 仮想マシンを作成するために使用するツールを選択し、**次へ**を選択します。
3. 「**接続の詳細**」ページで、Azure サブスクリプション ID と接続の名前を入力します。

> **注:**
>
> 接続名には 1～64 文字を含めることができ、空白のみ、または文字 `\/;:#.*?=<>|[]{}"'()'` を含めることはできません。

4. **既存を使用**を選択します。**既存のサービスプリンシパルの詳細**ウィンドウで、既存のサービスプリンシパルに対して次の設定を入力します。詳細を入力すると、**保存**ボタンが有効になります。**保存**を選択します。有効な詳細情報を提供するまで、このページから先に進むことはできません。

   - **サブスクリプションID**。AzureサブスクリプションIDを入力します。サブスクリプションIDを取得するには、Azureポータルにサインインし、**サブスクリプション > 概要**に移動します。
   - **Active Directory ID** (テナント ID)。Azure AD に登録したアプリケーションのディレクトリ (テナント) ID を入力します。
   - **アプリケーション ID**。Azure AD に登録したアプリケーションのアプリケーション (クライアント) ID を入力します。
   - **アプリケーションシークレット**。シークレットキー (クライアントシークレット) を作成します。登録済みアプリケーションは、このキーを使用して Azure AD に対して認証を行います。セキュリティ上の理由から、キーを定期的に変更することをお勧めします。キーは後で取得できないため、必ず保存してください。
   - **シークレットの有効期限**。アプリケーションシークレットの有効期限が切れる日付を入力します。シークレットキーの有効期限が切れる 14 日前から、「**ホスティング**」ノードの特定のホスト接続に警告アイコンが表示されます。ただし、シークレットキーの有効期限が切れると、エラーが発生します。

     > **注:**
     >
     > セキュリティ上の理由から、有効期限は現在から2年を超えることはできません。

   - **認証 URL**。このフィールドは自動的に入力され、編集できません。
   - **管理 URL**。このフィールドは自動的に入力され、編集できません。
   - **ストレージサフィックス**。このフィールドは自動的に入力され、編集できません。

- **ディスクまたはスナップショットをアップロードまたはダウンロードするためのAzure BLOBストレージエンドポイント**。このフィールドは自動的に入力され、編集できません。
- **Key Vaultサービス**。このフィールドは自動的に入力され、編集できません。
- **サービスバスサフィックス**。このフィールドは自動的に入力され、編集できません。

  AzureでMCSカタログを作成するには、以下のエンドポイントへのアクセスが必要です。これらのエンドポイントへのアクセスにより、ネットワークとAzureポータルおよびそのサービス間の接続が最適化されます。

  - 認証URL: `https://login.microsoftonline.com`
  - 管理URL: `https://management.azure.com`。これはAzure Resource Managerプロバイダー APIのリクエストURLです。管理のエンドポイントは環境によって異なります。たとえば、Azure Globalの場合は `https://management.azure.com`、Azure US Governmentの場合は `https://management.usgovcloudapi.net` です。
  - ストレージサフィックス: `https://*.core.windows.net`。これはストレージサフィックスのワイルドカード文字(*)です。例: `https://demo.table.core.windows.net`。
  - ディスクまたはスナップショットをアップロードまたはダウンロードするためのAzure BLOBストレージエンドポイント: `https://*.storage.azure.net`。これはBLOBストレージのインポートおよびエクスポート操作のワイルドカード文字(*)です。例: `https://md-impexp-xxxxx.z[00-50].blob.storage.azure.net`。
  - Key Vaultサービス: `https://*.vault.azure.net`。これはキーコンテナー名のワイルドカード文字(*)です。例: `https://<your-key-vault-name>.vault.azure.net`。
  - サービスバスサフィックス: `https://*.servicebus.windows.net`。これはグローバルAzureクラウドで作成された名前空間のワイルドカード文字(*)です。例: `https://{serviceNamespace}.servicebus.windows.net/{path}`。

5. **保存**を選択すると、「**接続の詳細**」ページに戻ります。「**次へ**」を選択して次のページに進みます。
6. 接続のリソースを構成します。リソースは、リージョンとネットワークで構成されます。

   - 「**地域**」ページで、地域を選択します。
   - 「**ネットワーク**」ページで、次の操作を行います。

- リージョンとネットワークの組み合わせを識別しやすくするために、1〜64 文字のリソース名を入力します。リソース名には空白のみ、または文字 `\/;:#.*?=<>|[]{}"'()'` を含めることはできません。
- 仮想ネットワーク/リソースグループのペアを選択します。（同じ名前の仮想ネットワークが複数ある場合、ネットワーク名とリソースグループをペアにすることで、一意の組み合わせが提供されます。）前のページで選択した地域に仮想ネットワークがない場合は、そのページに戻り、仮想ネットワークがある地域を選択してください。

7. 「**概要**」ページで、設定の概要を確認し、「**完了**」を選択してセットアップを完了します。

サービスプリンシパルと接続を管理する

このセクションでは、サービスプリンシパルと接続を管理する方法について詳しく説明します。

- Azureスロットル設定を構成する
- Azureでイメージ共有を有効にする
- Web Studio を使用して共有テナントを接続に追加する
- PowerShellを使用してイメージ共有を実装する
- アプリケーションシークレットとシークレットの有効期限を管理する

Azure スロットリング設定の構成

Azure Resource Manager は、サブスクリプションとテナントに対する要求を調整し、プロバイダーの特定のニーズに合わせて定義された制限に基づいてトラフィックをルーティングします。詳細については、Microsoft サイトのResource Manager 要求のスロットリングを参照してください。サブスクリプションとテナントには制限があり、多数のマシンを管理すると問題が発生する可能性があります。たとえば、多数のマシンを含むサブスクリプションでは、電源操作に関連するパフォーマンスの問題が発生する可能性があります。

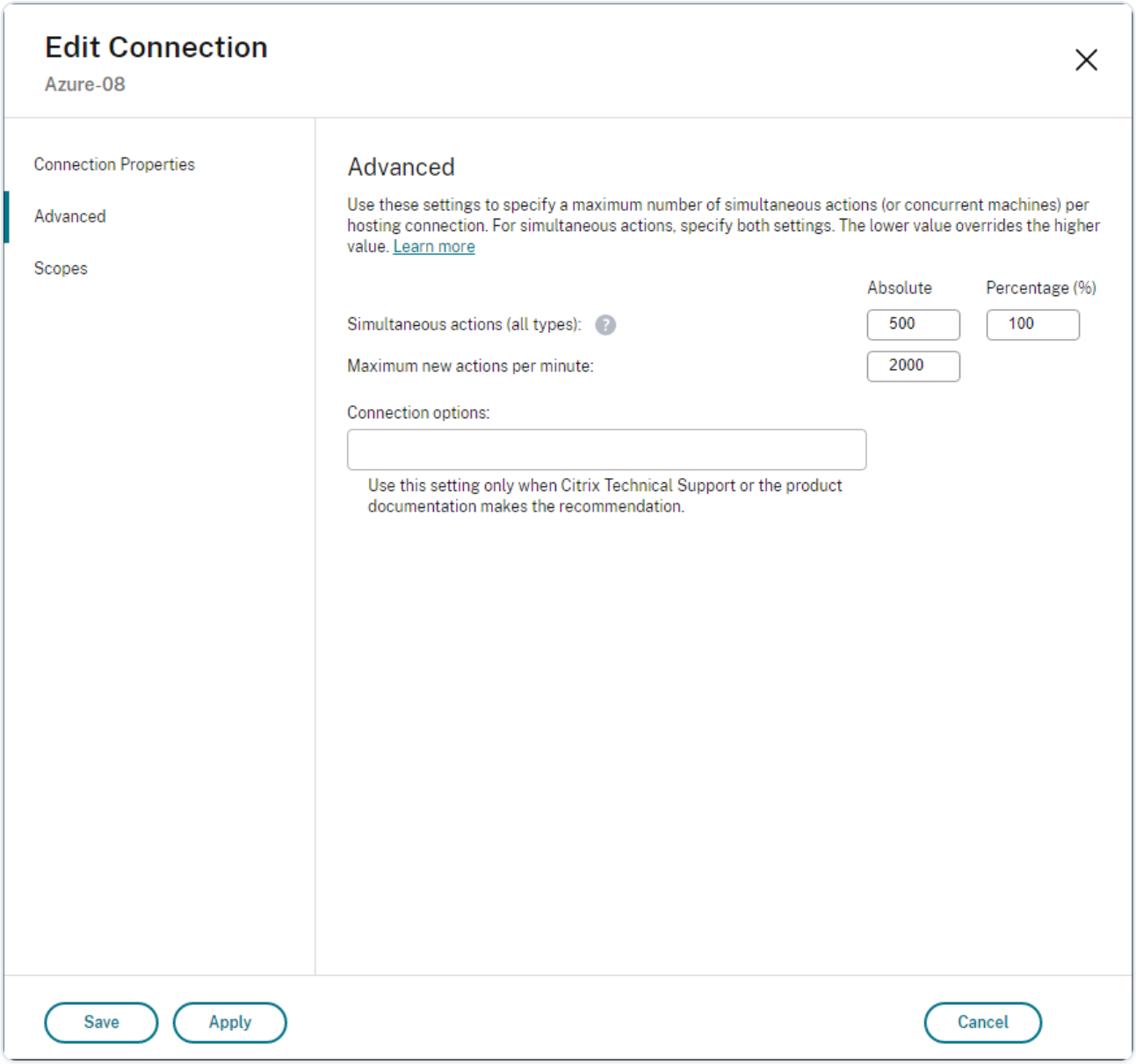
> **ヒント:**
>
> 詳細については、「Machine Creation Services を使用した Azure パフォーマンスの向上」を参照してください。
>
> これらの問題を軽減するために、MCS の内部スロットリングを削除して、Azure から利用可能な要求クォータをより多く使用できます。

たとえば、1,000 台の VM を含む大規模なサブスクリプションで VM の電源をオンまたはオフにする場合は、次の最適な設定をお勧めします。

- 絶対同時操作数: 500
- 1 分あたりの最大新規操作数: 2000
- 操作の最大同時実行数: 500

Web Studio を使用して、特定の Azure 接続の Azure 操作を構成します。

1. Web Studio で、左側のペインの を選択します。
2. 接続を選択します。
3. ウィザードで、 を選択します。
4. ページで、構成オプションを使用して、同時アクションの数、1 分あたりの最大新規アクション数、および追加の接続オプションを指定します。



MCS はデフォルトで最大 500 の同時操作をサポートします。または、Remote PowerShell SDK を使用して、同時操作の最大数を設定することもできます。

PowerShell プロパティ `MaximumConcurrentProvisioningOperations` を使用して、Azure プロビジョニングの同時操作の最大数を指定します。このプロパティを使用する際は、以下を考慮してください。

- `MaximumConcurrentProvisioningOperations` のデフォルト値は 500 です。
- PowerShell コマンド `Set-item` を使用して、`MaximumConcurrentProvisioningOperations` パラメーターを構成します。

Azure でのイメージ共有を有効にする

マシンカタログを作成または更新する際、異なるAzureテナントおよびサブスクリプション（Azure Compute Galleryを介して共有）から共有イメージを選択できます。テナント内またはテナント間でイメージ共有を有効にするには、Azureで必要な設定を行う必要があります。

- テナント内でのイメージ共有（サブスクリプション間）
- テナント間でのイメージ共有

テナント内でのイメージ共有（サブスクリプション間）

別のサブスクリプションに属するAzure Compute Galleryのイメージを選択するには、そのサブスクリプションのサービスプリンシパル (SPN) とイメージを共有する必要があります。

たとえば、Studioで次のように構成されているサービスプリンシパル (SPN 1) がある場合：

サービスプリンシパル: SPN 1

サブスクリプション: subscription 1

テナント: tenant 1

イメージは別のサブスクリプションにあり、Studio では次のように構成されています。

サブスクリプション: subscription 2

テナント: tenant 1

subscription 2のイメージをsubscription 1 (SPN 1) と共有したい場合は、subscription 2に移動し、リソースグループをSPN1と共有します。

イメージは、Azure ロールベースのアクセス制御 (RBAC) を使用して別の SPN と共有する必要があります。Azure RBAC は、Azure リソースへのアクセスを管理するために使用される承認システムです。Azure RBAC の詳細については、Microsoft ドキュメント Azure ロールベースのアクセス制御 (Azure RBAC) とは を参照してください。アクセスを許可するには、リソースグループスコープでサービスプリンシパルに共同作成者ロールを割り当てます。Azure ロールを割り当てるには、ユーザーアクセス管理者や所有者などの `Microsoft.Authorization/roleAssignments/write` 権限が必要です。別の SPN とイメージを共有する方法の詳細については、Microsoft ドキュメント Azure portal を使用して Azure ロールを割り当てる を参照してください。

PowerShell コマンドを使用して別のサブスクリプションからイメージを選択する方法については、「」(#select-an-image-from-a-different-subscription) を参照してください。

テナント間で画像を共有する

Azure Compute Gallery を使用してテナント間でイメージを共有するには、アプリケーション登録を作成します。

たとえば、2つのテナント (テナント1とテナント2) があり、テナント1とイメージギャラリーを共有したい場合は、次の手順を実行します。

1. テナント1のアプリケーション登録を作成します。詳細については、「アプリ登録の作成」を参照してください。
2. ブラウザを使用してサインインを要求することで、テナント2にアプリケーションへのアクセスを許可します。`Tenant2 ID` をテナント1のテナントIDに置き換えます。`Application (client) ID` を作成したアプリケーション登録のアプリケーションIDに置き換えます。置換が完了したら、URLをブラウザに貼り付け、サインインプロンプトに従ってテナント2にサインインします。例:

   ```
   https://login.microsoftonline.com/<Tenant 2 ID>/oauth2/authorize?
   client_id=<Application (client)
   ID>&response_type=code&redirect_uri=https%3A%2F%2Fwww.microsoft.com%2F
   ```

   詳細については、「テナント2へのアクセス許可」を参照してください。
3. アプリケーションに Tenant 2 リソースグループへのアクセス権を付与します。Tenant 2 としてサインインし、ギャラリーイメージを持つリソースグループにアプリケーション登録アクセス権を付与します。詳細については、テナント間の要求を認証する を参照してください。

PowerShell コマンドを使用して別のテナントのイメージからカタログを作成するには:

1. 「」(#update-hosting-connection-custom-properties-with-shared-tenant-ids)。
2. 「」(#select-an-image-from-a-different-tenant)。

Web Studio を使用して共有テナントを接続に追加する

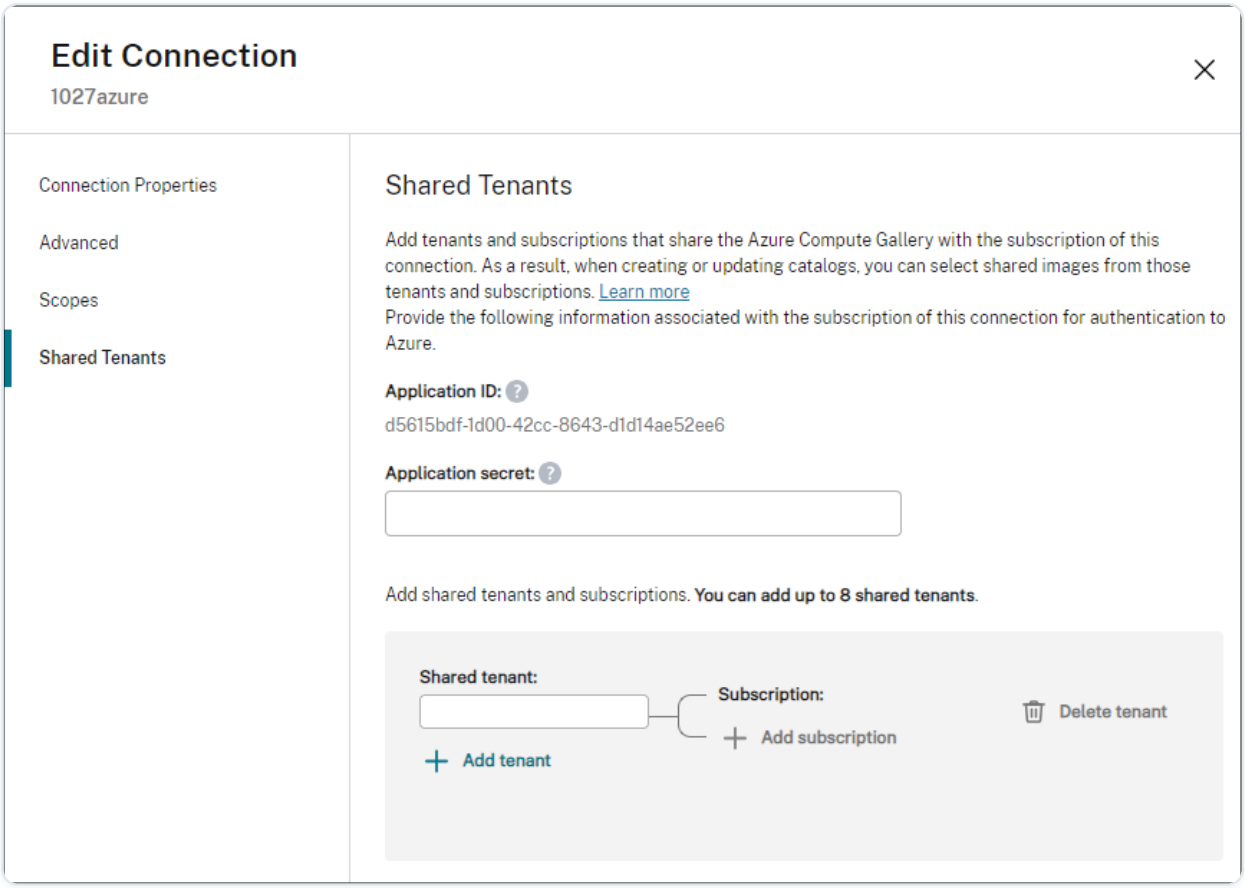
Web Studio でマシンカタログを作成または更新する際、異なる Azure テナントおよびサブスクリプション (Azure Compute Gallery を介して共有) から共有イメージを選択できます。この機能では、関連するホスト接続の共有テナントおよびサブスクリプション情報を提供する必要があります。

> **注:**
>
> テナント間でイメージ共有を有効にするために、Azure で必要な設定が構成されていることを確認してください。詳細については、「テナント間で画像を共有する」を参照してください。

接続に対して次の手順を実行します。

1. Web Studio で、左側のペインの を選択します。

2. 接続を選択し、アクションバーで**接続の編集**を選択します。



3. 「**共有テナント**」で、以下を実行します。

   - 接続のサブスクリプションに関連付けられているアプリケーション ID とアプリケーションシークレットを指定します。Citrix Virtual Apps and Desktops™ は、この情報を使用して Microsoft Entra ID に対して認証を行います。
   - 接続のサブスクリプションと Azure Compute Gallery を共有するテナントとサブスクリプションを追加します。テナントごとに最大8つの共有テナントと8つのサブスクリプションを追加できます。

4. 完了したら、**適用**を選択して行った変更を適用し、ウィンドウを開いたままにするか、**OK**を選択して変更を適用し、ウィンドウを閉じます。

PowerShellを使用したイメージ共有の実装

このセクションでは、PowerShellを使用してイメージを共有するプロセスについて説明します。

- 別のサブスクリプションからイメージを選択する
- 共有テナントIDでホスティング接続のカスタムプロパティを更新する
- 別のテナントからイメージを選択する

別のサブスクリプションからイメージを選択する

同じAzureテナント内の別の共有サブスクリプションに属するAzure Compute Galleryのイメージを選択して、PowerShellコマンドを使用してMCSカタログを作成および更新できます。

1. ホスティングユニットのルートフォルダーに、Citrixは`sharedsubscription`という新しい共有サブスクリプションフォルダーを作成します。
2. テナント内のすべての共有サブスクリプションを一覧表示します。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\sharedsubscription.folder"
```

3. 1つの共有サブスクリプションを選択し、その共有サブスクリプションのすべての共有リソースグループを一覧表示します。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription"
```

4. リソースグループを選択し、そのリソースグループのすべてのギャラリーを一覧表示します。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\
xyz.resourcegroup"
```

5. ギャラリーを選択し、そのギャラリーのすべてのイメージ定義を一覧表示します。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\testgallery.gallery"
```

6. 1つのイメージ定義を選択し、そのイメージ定義のすべてのイメージバージョンを一覧表示します。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\sigtestdef.imagedefinition"
```

7. 次の要素を使用してMCSカタログを作成および更新します。

   - リソースグループ

- ギャラリー
- ギャラリーイメージ定義
- ギャラリーイメージバージョン

Remote PowerShell SDK を使用したカタログの作成方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>` を参照してください。

共有テナントIDでホスティング接続のカスタムプロパティを更新する

`Set-Item` を使用して、共有テナントIDとサブスクリプションIDでホスティング接続のカスタムプロパティを更新します。`CustomProperties` にプロパティ `SharedTenants` を追加します。`Shared Tenants` の形式は次のとおりです。

```
[{"Tenant":"94367291-119e-457c-bc10-25337231f7bd","Subscriptions":
["7bb42f40-8d7f-4230-a920-be2781f6d5d9"]},{"Tenant":"50e83564-c4e5-4209-
b43d-815c45659564","Subscriptions":["06ab8944-6a88-47ee-
a975-43dd491a37d0"]}]
```

例:

```
Set-Item -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`"
Value=`"123`" />

<Property xsi:type=`"StringProperty`" Name=`"ManagementEndpoint`"
Value=`"https://management.azure.com/`" />

<Property xsi:type=`"StringProperty`" Name=`"AuthenticationAuthority`"
Value=`"https://login.microsoftonline.com/`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageSuffix`"
Value=`"core.windows.net`" />

<Property xsi:type=`"StringProperty`" Name=`"TenantId`" Value=`"123abc`" /
>

<Property xsi:type=`"StringProperty`" Name=`"SharedTenants`"
Value=`"`[ { 'Tenant':'123abc', 'Subscriptions':['345', '567'] } ]`"` />
```

```
</CustomProperties>"

-LiteralPath @("XDHyp:\Connections\aazure") -PassThru -UserName "advc345"
-SecurePassword

$psd
```

注:

複数のテナントを追加できます。各テナントは複数のサブスクリプションを持つことができます。

別のテナントからイメージを選択する

PowerShellコマンドを使用してMCSカタログを作成および更新するために、別のAzureテナントに属するAzure Compute Galleryのイメージを選択できます。

1. ホスティングユニットのルートフォルダーに、Citrixは`sharedsubscription`という新しい共有サブスクリプションフォルダーを作成します。
2. すべての共有サブスクリプションを一覧表示します。

   ```
   Get-ChildItem XDHyp:\HostingUnits\azres\sharedsubscription.folder
   ```

3. 1つの共有サブスクリプションを選択し、その共有サブスクリプションのすべての共有リソースグループを一覧表示します。

   ```
   Get-ChildItem XDHyp:
   \HostingUnits\azres\image.folder\abc123.sharedsubscription
   ```

4. リソースグループを選択し、そのリソースグループのすべてのギャラリーを一覧表示します。

   ```
   Get-ChildItem XDHyp:
   \HostingUnits\azres\image.folder\abc123.sharedsubscription\
   xyz.resourcegroup
   ```

5. ギャラリーを選択し、そのギャラリーのすべてのイメージ定義を一覧表示します。

```
Get-ChildItem XDHyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\efg.gallery
```

6. 1つのイメージ定義を選択し、そのイメージ定義のすべてのイメージバージョンを一覧表示します。

```
Get-ChildItem XDHyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\efg.gallery\hij.imagedefinition
```

7. 次の要素を使用してMCSカタログを作成および更新します。

   - リソースグループ
   - ギャラリー
   - ギャラリーイメージ定義
   - ギャラリーイメージバージョン

   Remote PowerShell SDK を使用したカタログの作成方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`を参照してください。

アプリケーションシークレットとシークレットの有効期限を管理する

シークレットの有効期限が切れる前に、接続のアプリケーションシークレットを必ず変更してください。シークレットキーの有効期限が切れる14日前から、**Hosting** ノードの特定のホスト接続に警告アイコンが表示されます。ただし、シークレットキーの有効期限が切れると、エラーが発生します。

AZURE でアプリケーションシークレットを作成する

Azure portal を介して、接続のアプリケーションシークレットを作成できます。

1. **Microsoft Entra ID** を選択します。
2. Microsoft Entra IDの**アプリの登録**から、アプリケーションを選択します。
3. **証明書とシークレット**に移動します。
4. **>** をクリックします。
5. シークレットの説明を入力し、期間を指定します。完了したら、**Add** を選択します。

> **注:**
>
> クライアントシークレットは後で取得できないため、必ず保存してください。

6. クライアントシークレットの値と有効期限をコピーします。
7. Web Studio で、対応する接続を編集し、**Application secret** および **Secret expiration date** フィールドの内容をコピーした値に置き換えます。

シークレットの有効期限を変更する

Web Studio を使用して、使用中のアプリケーションシークレットの有効期限を追加または変更できます。

> **注:**
>
> シークレットキーの有効期限が切れる14日前から、**Hosting** ノードの特定のホスト接続に警告アイコンが表示されます。

1. **接続とリソースの追加**ウィザードで、接続を右クリックし、**接続の編集**をクリックします。
2. **接続プロパティ**ページで、**シークレットの有効期限**をクリックして、使用中のアプリケーションシークレットの有効期限を追加または変更します。

Azure 拡張ゾーン

Azure 拡張ゾーンは、既存の Azure リージョンのフットプリントの小さい拡張機能であり、組織がワークロードをユーザーの近くで実行できるようにすることで、パフォーマンスとコンプライアンスを向上させます。Azure 上の MCS は、拡張ゾーン内の VM のプロビジョニングと電源管理をサポートするようになりました。

Azure 拡張ゾーンの詳細については、Microsoft ドキュメントの Azure Extended Zones documentation を参照してください。

ユースケース

この機能は、永続カタログと非永続カタログに適用できます。

- 電源管理のみのVM: 既存の拡張ゾーンVMを電源管理のみのカタログにインポートし、Citrix MCSで電源管理できます。

- MCSプロビジョニング済みVM: 新しいVMを拡張ゾーンにプロビジョニングし、MCSで管理できます。この機能には、イメージ管理ワークフローのサポートも含まれています。

制限事項

現在、Azure 拡張ゾーンの使用にはいくつかの制限があります。これらの制限の多くは、現在の Azure の制約によるものです。

- 専用ホストはサポートされていません。
- 容量予約はサポートされていません。
- 近接配置グループはサポートされていません。
- スポットVMはサポートされていません。
- 拡張ゾーンではアベイラビリティゾーンはサポートされていません。
- サポートされているストレージタイプは、**StandardSSD_LRS** および **Premium_LRS** のみです。
- 現在、**UseSharedImageGallery** 機能を使用して、マスターイメージを拡張ゾーンのAzure Compute Gallery（またはShared Image Gallery）に保存することはできません。その結果、エフェメラルOSディスクもサポートされていません。
- Azure Compute Galleryのイメージバージョンをマスターイメージとして使用している場合は、使用する前に拡張ゾーンでのレプリケーションが完全に完了していることを確認してください。レプリケーションが完了する前にイメージバージョンを使用しようとすると、展開が失敗する可能性があります。

前提条件

拡張ゾーンを使用する前に、以下の前提条件となる手順を完了していることを確認してください。

1. Azureへの登録:
    a. 拡張ゾーンはデフォルトでは有効になっていません。
    b. Azureサブスクリプションで`Microsoft.EdgeZones`リソースプロバイダーを登録します: リソースプロバイダーMicrosoft.EdgeZonesのサブスクリプションを登録する。
    c. 必要な各拡張ゾーンを個別に登録します（例: LosAngeles、Perth）: Azure拡張ゾーンに登録する。
2. Citrixリソースの準備:
    a. 拡張ゾーンに仮想ネットワークを作成します。
    b. 必要に応じてマスターイメージとスナップショットを作成します。

必要な権限

拡張ゾーンにカタログを作成するには、サービスプリンシパルに次の権限が必要です: `Microsoft.EdgeZones/extendedZones/read`。

必要な最小限の権限の詳細については、「最小権限」を参照してください。

構成手順

1. 拡張ゾーンでホスティングユニットを作成する

   `.extendedzone`タイプを使用する拡張ゾーンは、Citrix MCSインベントリのリージョンと並んで表示されます。拡張ゾーンにプロビジョニングするには、その拡張ゾーンに紐付けられた新しいホスティングユニットを作成する必要があります。

   例: ロサンゼルス拡張ゾーンにホスティングユニットを作成する

   ```
   $RootPath = "XDHyp:\Connections\MyConnectionName\Los
   Angeles.extendedzone"



   $NetworkPath = "XDHyp:\Connections\MyConnectionName\Los
   Angeles.extendedzone\virtualprivatecloud.folder\MyResourceGroup.resourc
   egroup\MyExtendedZoneNetwork.virtualprivatecloud\MyExtendedZoneSubnet.n
   etwork"



   $HostingUnitPath = "XDHyp:\HostingUnits\MyHostingUnitName"



   New-Item -HypervisorConnectionName MyConnectionName -NetworkPath
   @($NetworkPath) -Path @($HostingUnitPath) -RootPath $RootPath
   -StoragePath @()
   ```

2. 拡張ゾーンでMCSカタログを作成する

   ホスティングユニットを作成したら、StudioまたはPowerShellを使用してカタログ作成に進みます。カタログが拡張ゾーンホスティングユニットを参照していることを確認してください。

トラブルシューティング

問題が発生した場合は、以下を確認してください。

1. サブスクリプションが拡張ゾーンに登録されていることを確認します。
    a. サブスクリプションがMicrosoft.EdgeZonesリソースプロバイダーに登録されていることを確認します。
    b. 各拡張ゾーンが個別に登録されていることを確認します。
2. サービスプリンシパルに新しい権限があることを確認します。
    a. サービスプリンシパルには`Microsoft.EdgeZones/extendedZones/read`権限が必要です。

登録または権限が不足している場合、拡張ゾーンのインベントリアイテムは「不明な拡張ゾーン」として表示されることがあります。

> **注:**
>
> 拡張ゾーンのマスターイメージを使用して親リージョンにカタログを作成する場合でも、拡張ゾーンの登録と権限が必要です。

事前作成されたネットワークセキュリティグループを使用する

CitrixにNSGの作成と変更を要求する代わりに、イメージ準備用のDeny-Allネットワークセキュリティグループを作成します。ホスティングユニットのカスタムプロパティをPowerShellコマンド`Set-Item`を使用して編集し、Deny-Allネットワークセキュリティグループを提供するためのパラメーター`NsgForPreparation`を含めます。

前提条件

サービスプリンシパルに必要な以下の権限を構成します。

- `Microsoft.Network/networkSecurityGroups/join/action`: ネットワークセキュリティグループをサブネットまたはネットワークインターフェイスに関連付ける
- `Microsoft.Network/networkSecurityGroups/read`: ネットワークセキュリティグループを取得する
- `Microsoft.Network/networkSecurityGroups/securityRules/read`: ルールを取得する

事前作成されたDeny-Allネットワークセキュリティグループを追加する

事前作成されたDeny-Allネットワークセキュリティグループを追加するには、ホスティングユニットでカスタムプロパティを次のように設定します。

1. Remote PowerShell SDKを使用してPowerShellウィンドウを開きます。
2. 次のコマンドを実行します。

```
Add-PSSnapin citrix*.

cd XDHyp:\HostingUnits\

Dir
```

3. 詳細を取得するホスティングユニットを選択します。

```
Get-Item "XDHyp:\HostingUnits\<hostingunitname>"
```

4. CustomPropertiesをメモ帳にコピーし、プロパティ設定`<Property xsi:type="StringProperty`" Name=`"NsgForPreparation`" Value=`"{ResourceGroupName}/{NetworkSecurityGroupName}"/>`を追加します。例：

```
<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`"
Name=`"NsgForPreparation`" Value=`{ResourceGroupName}/
{NetworkSecurityGroupName}`"/></CustomProperties>
```

5. PowerShell ウィンドウで、変更されたカスタムプロパティに変数を割り当てます。例:

```
$customProperty = "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`"
Name=`"NsgForPreparation`" Value=`"{ResourceGroupName}/
{NetworkSecurityGroupName}`"/></CustomProperties>"
```

6. `$cred = Get-Credential`を実行します。プロンプトが表示されたら、接続資格情報を入力します。資格情報は Azure アプリケーション ID とシークレットです。
7. 次のコマンドを実行します。

```
Set-Item -PSPath XDHyp:\HostingUnits\<hostingunitname>
-CustomProperties $customProperty -username $cred.username
-Securepassword $cred.password
```

> **重要:**
>
> SubscriptionIdがありませんというメッセージが表示された場合は、カスタムプロパティ内のすべての二重引用符（“）をバッククォートの後に二重引用符（`”）に置き換えてください。

8. 更新された `CustomProperties` 設定を確認するには、`dir` を実行します。

> **注:**
>
> 更新が反映されるまでに1分以上かかります。

ネットワークセキュリティグループの詳細を取得する

ネットワークセキュリティグループの詳細を取得するには、まずネットワークセキュリティグループを含むリソースグループを取得し、次にリソースグループ名に基づいてネットワークセキュリティグループを取得します。

1. ネットワークセキュリティグループを含むリソースグループを取得します。例：

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes":
["networksecuritygroup"]}'
```

2. リソースグループ名に基づいてネットワークセキュリティグループを取得します。例：

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType securitygroup -MaxRecords
5 -AdditionalDataFilter '{"location": ["eastus", "westus"],
"resourcegroup":["resourcegroupname"]}'
```

空のリソースグループをフィルターする

マシンカタログ作成時にマスターイメージ、マシンプロファイル、または準備済みイメージを選択する際に、PowerShellコマンド `Get-HypInventoryItem` を使用して空のリソースグループをフィルターします。

例:

- ページ内の最大レコード数を取得する:

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5
```

- ページ内の最大レコード数を取得し、特定のリソースを持つリソースコンテナを見つけるためにフィルタリングする。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["vm",
"manageddisk", "snapshot", "imageversion", "storageaccount"]}'
```

- スキップを使用してページを直接指定して取得し、特定のリソースを持つリソースコンテナを見つけるためにフィルタリングする。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -skip 20 -AdditionalDataFilter '{"containedresourcetypes": ["vm",
"manageddisk", "snapshot", "imageversion", "storageaccount"]}'
```

- トークンを使用して次のページを取得し、特定のリソースを持つリソースコンテナを見つけるためにフィルタリングする。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["vm",
"manageddisk", "snapshot", "imageversion", "storageaccount"]}'
-ContinuationToken
'ew0KICAiJGlkIjogIjEiLA0KICAiTWF4Um93cyI6IDUsDQogICJSb3dzVG9Ta2lwIjogMj
UsDQogICJLdXN0b0NsdXN0ZXJVcmwiOiAiaHR0cHM6Ly9hcmctbmV1LTEzLXNmLmFyZy5jb
3JlLndpbmRvd3MubmV0Ig0KfQ=='
```

- タグ「Citrix internal tag」を持つすべてのリソースグループを取得し、`MaxRecords`で最大レコード数を制限する。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5
```

- タグ「Citrix internal tag」を持つマシンプロファイル（マスターイメージ）をフィルタリングし、`MaxRecords`で最大レコード数を制限する。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["vm",
"templatespecversion"]}'
```

- タグ「Citrix internal tag」を持つ準備済みイメージをフィルタリングし、`MaxRecords`で最大レコード数を制限する。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["manageddisk",
"snapshot", "imageversion"]}'
```

- タグ「Citrix internal tag」を持つマシンプロファイル（準備済みイメージ）をフィルタリングし、`MaxRecords`で最大レコード数を制限する。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["vm",
"templatespecversion"]}'
```

- タグ「Citrix internal tag」を持つイメージをフィルタリングし、`MaxRecords`と場所で最大レコード数を制限する。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["manageddisk",
"snapshot", "imageversion", "storageaccount"], "location": ["eastus",
"westus"]}'
```

- タグを考慮せずにすべてのリソースグループを取得する`CitrixResource`。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
50 -AdditionalDataFilter '{"containedresourcetypes": ["manageddisk",
"snapshot", "imageversion", "storageaccount"]}' -Force $true
```

Azure Sovereign Airgapクラウド環境に接続する

Azure Sovereign Airgapクラウド環境は、分離されたネットワークドメイン上にある必要がある最高機密のワークロードに適しています。ホスト接続の作成時に、カスタムプロパティ `DisableInstanceDiscovery` を使用してAzure Sovereign Airgapクラウド環境に接続できます。

```
<Property xsi:type="StringProperty" Name="DisableInstanceDiscovery"
Value="true" />
```

Azureホスト接続の作成の詳細については、Create-HostingConnection.ps1を参照してください。

必要なAzure権限

このセクションには、Azure に必要な最小限の一般的な権限が含まれています。

最小限の権限

最小限の権限は、より優れたセキュリティ制御を提供します。ただし、追加の権限を必要とする新機能は、最小限の権限のみを使用しているため失敗します。

ホスト接続の作成

Azure から取得した情報を使用して、新しいホスト接続を追加します。

```
"Microsoft.Network/virtualNetworks/read",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/disks/read",

"Microsoft.Resources/providers/read",

"Microsoft.Resources/subscriptions/locations/read",

"Microsoft.Resources/tenants/read",

"Microsoft.Network/networkSecurityGroups/join/action",
```

```
"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/securityRules/read"
```

VM の電源管理

マシンインスタンスの電源をオンまたはオフにします。

```
"Microsoft.Compute/virtualMachines/read",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/virtualMachines/start/action",

"Microsoft.Compute/virtualMachines/restart/action",

"Microsoft.Insights/diagnosticsettings/delete",

"Microsoft.Insights/diagnosticsettings/read",

"Microsoft.Insights/diagnosticsettings/write",
```

仮想マシンの作成、更新、または削除

マシンカタログを作成し、マシンを追加、削除、更新し、マシンカタログを削除します。

以下は、マスターイメージがマネージドディスクである場合、またはスナップショットがホスティング接続と同じリージョンにある場合に必要となる最小限の権限のリストです。

```
"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/deployments/validate/action",

"Microsoft.Resources/tags/read",

"Microsoft.Resources/tags/write",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/virtualMachines/write",
```

```
"Microsoft.Compute/virtualMachines/delete",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/snapshots/read",

"Microsoft.Compute/snapshots/write",

"Microsoft.Compute/snapshots/delete",

"Microsoft.Compute/snapshots/beginGetAccess/action",

"Microsoft.Compute/snapshots/endGetAccess/action",

"Microsoft.Compute/disks/read",

"Microsoft.Compute/disks/write",

"Microsoft.Compute/disks/delete",

"Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.Compute/disks/endGetAccess/action",

"Microsoft.Compute/locations/publishers/artifacttypes/types/versions/
read",

"Microsoft.Compute/skus/read",

"Microsoft.Compute/virtualMachines/extensions/read",

"Microsoft.Compute/virtualMachines/extensions/write",

"Microsoft.Features/providers/features/read",

"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",

"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/networkSecurityGroups/read",
```

```
"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/networkSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkInterfaces/read",

"Microsoft.Network/networkInterfaces/write",

"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkInterfaces/join/action",

"Microsoft.Network/locations/usages/read",

"Microsoft.Compute/capacityReservationGroups/capacityReservations/read"
```

以下の機能については、最小限の権限に加えて、以下の追加権限が必要です。

- マスターイメージがホスティング接続と同じリージョンにあるストレージアカウント内の VHD である場合：

  ```
  "Microsoft.Storage/storageAccounts/read",

  "Microsoft.Storage/storageAccounts/listKeys/action",
  ```

- マスターイメージが共有イメージギャラリーのImageVersionである場合:

  ```
  "Microsoft.Compute/galleries/read",

  "Microsoft.Compute/galleries/images/read",

  "Microsoft.Compute/galleries/images/versions/read",
  ```

- マスターイメージがマネージドディスクである場合、スナップショットまたはVHDがホスティング接続のリージョンとは異なるリージョンにある場合:

```
"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/listKeys/action",

"Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/delete",

"Microsoft.Storage/checknameavailability/read",

"Microsoft.Storage/locations/usages/read",

"Microsoft.Storage/skus/read",
```

- Citrix管理のリソースグループを使用する場合:

```
"Microsoft.Resources/subscriptions/resourceGroups/write",

"Microsoft.Resources/subscriptions/resourceGroups/delete",
```

- マスターイメージを共有テナントまたはサブスクリプションのAzure Compute Gallery（旧Shared Image Gallery）に配置する場合:

```
"Microsoft.Compute/galleries/write",

"Microsoft.Compute/galleries/images/write",

"Microsoft.Compute/galleries/images/versions/write",

"Microsoft.Compute/galleries/read",

"Microsoft.Compute/galleries/images/read",

"Microsoft.Compute/galleries/images/versions/read",

"Microsoft.Compute/galleries/delete",

"Microsoft.Compute/galleries/images/delete",

"Microsoft.Compute/galleries/images/versions/delete",
```

```
"Microsoft.Resources/subscriptions/read",
```

- Azure専用ホストサポートを使用する場合:

```
"Microsoft.Compute/hostGroups/read",

"Microsoft.Compute/hostGroups/write",

"Microsoft.Compute/hostGroups/hosts/read",
```

- カスタマーマネージドキー (CMK) を使用してサーバー側暗号化 (SSE) を使用する場合:

```
"Microsoft.Compute/diskEncryptionSets/read",
```

- ARM テンプレート (マシンプロファイル) を使用して VM を展開する場合:

```
"Microsoft.Resources/deployments/write",

"Microsoft.Resources/deployments/operationstatuses/read",

"Microsoft.Resources/deployments/read",

"Microsoft.Resources/deployments/delete",

"Microsoft.Insights/DataCollectionRuleAssociations/Read",

"Microsoft.Insights/dataCollectionRules/read",
```

- Azure テンプレート仕様をマシンプロファイルとして使用する場合:

```
"Microsoft.Resources/templateSpecs/read",

"Microsoft.Resources/templateSpecs/versions/read",
```

アンマネージドディスクを使用したマシンの作成、更新、削除

マスターイメージが VHD であり、管理者が提供するリソースグループを使用する場合に必要となる最小限の権限のリストは次のとおりです。

```
"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/tags/read",

"Microsoft.Resources/tags/write",

"Microsoft.Storage/storageAccounts/delete",

"Microsoft.Storage/storageAccounts/listKeys/action",

"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/checknameavailability/read",

"Microsoft.Storage/locations/usages/read",

"Microsoft.Storage/skus/read",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/virtualMachines/delete",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/virtualMachines/write",

"Microsoft.Resources/deployments/validate/action",

"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkInterfaces/join/action",

"Microsoft.Network/networkInterfaces/read",

"Microsoft.Network/networkInterfaces/write",

"Microsoft.Network/networkSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkSecurityGroups/read",
```

```
"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",

"Microsoft.Network/locations/usages/read",
```

コスト管理

VM の価格を取得するために必要な最小限の権限は次のとおりです。

```
"Microsoft.Consumption/pricesheets/read"
```

VM のコストを取得するために必要な最小限の権限は次のとおりです。

```
"Microsoft.CostManagement/query/read"
```

注:

Azure マシンカタログの **Cost Insights** タブを表示するには、**Cost Management > Manage > Read cost** 権限 (Cloud Administrators のデフォルト) が必要です。**Cost Insights** タブの詳細については、「カタログの詳細を表示」を参照してください。

一般的な権限

共同作成者ロールは、すべてのリソースを管理するためのフルアクセス権を持っています。この権限セットは、新機能の取得を妨げるものではありません。

以下の権限セットは、現在の機能セットで必要とされる以上の権限が含まれていますが、今後も最高の互換性を提供します。

```
"Microsoft.Compute/diskEncryptionSets/read",

"Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.Compute/disks/delete",
```

```
"Microsoft.Compute/disks/endGetAccess/action",
"Microsoft.Compute/disks/read",
"Microsoft.Compute/disks/write",
"Microsoft.Compute/galleries/delete",
"Microsoft.Compute/galleries/images/delete",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/delete",
"Microsoft.Compute/galleries/images/versions/read",
"Microsoft.Compute/galleries/images/versions/write",
"Microsoft.Compute/galleries/images/write",
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/write",
"Microsoft.Compute/hostGroups/hosts/read",
"Microsoft.Compute/hostGroups/read",
"Microsoft.Compute/hostGroups/write",
"Microsoft.Compute/snapshots/beginGetAccess/action",
"Microsoft.Compute/snapshots/delete",
"Microsoft.Compute/snapshots/endGetAccess/action",
"Microsoft.Compute/snapshots/read",
"Microsoft.Compute/snapshots/write",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/delete",
```

```
"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/virtualMachines/restart/action",

"Microsoft.Compute/virtualMachines/start/action",

"Microsoft.Compute/virtualMachines/write",

"Microsoft.Compute/locations/publishers/artifacttypes/types/versions/
read",

"Microsoft.Compute/skus/read",

"Microsoft.Compute/virtualMachines/extensions/read",

"Microsoft.Compute/virtualMachines/extensions/write",

"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkInterfaces/join/action",

"Microsoft.Network/networkInterfaces/read",

"Microsoft.Network/networkInterfaces/write",

"Microsoft.Network/networkSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",

"Microsoft.Network/locations/usages/read",

"Microsoft.Resources/deployments/operationstatuses/read",
```

```
"Microsoft.Resources/deployments/read",

"Microsoft.Resources/deployments/validate/action",

"Microsoft.Resources/deployments/write",

"Microsoft.Resources/deployments/delete",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourceGroups/write",

"Microsoft.Resources/subscriptions/resourceGroups/delete",

"Microsoft.Resources/providers/read",

"Microsoft.Resources/subscriptions/locations/read",

"Microsoft.Resources/subscriptions/read",

"Microsoft.Resources/tags/read",

"Microsoft.Resources/tags/write",

"Microsoft.Resources/tenants/read",

"Microsoft.Resources/templateSpecs/read",

"Microsoft.Resources/templateSpecs/versions/read",

"Microsoft.Storage/storageAccounts/delete",

"Microsoft.Storage/storageAccounts/listKeys/action",

"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/checknameavailability/read",

"Microsoft.Storage/locations/usages/read",

"Microsoft.Storage/skus/read",
```

```
"Microsoft.Features/providers/features/read",

"Microsoft.Insights/DataCollectionRuleAssociations/Read",

"Microsoft.Insights/dataCollectionRules/read",

"Microsoft.Insights/diagnosticsettings/delete",

"Microsoft.Insights/diagnosticsettings/read",

"Microsoft.Insights/diagnosticsettings/write",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/securityRules/read",

"Microsoft.Compute/capacityReservationGroups/capacityReservations/read"
```

Azureの非シークレット環境でホスト接続を検証する

ホスト接続の権限を検証して、MCSマシンカタログの作成と管理に関連するタスクを実行できます。この実装は、VMの作成、削除、更新、VMの電源管理など、さまざまなシナリオに必要な不足している権限を事前に特定するのに役立ち、重要な時期にブロックされるのを回避できます。

PowerShellコマンド `Test-HypHypervisorConnection` を使用して、ホスト接続の権限を検証できます。コマンドの結果はリストとしてキャプチャされ、リスト内の各項目は3つのセクションに分かれています。

- カテゴリ: ユーザーがMCSマシンカタログを作成および管理するために実行できるアクションまたはタスク。
- 修正措置: 管理者がユーザーの不足している権限の不一致を解決するために実行する必要がある手順。
- 不足している権限: カテゴリの不足している権限のリスト。

権限を検証するには、次の手順を実行します。

1. Azureへのホスト接続を作成します。
2. Delivery Controller™ホストからPowerShellウィンドウを開きます。

3. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
4. 接続をテストするために必要な権限があるかどうかを確認するには、次のコマンドを実行します。

   ```
   Test-HypHypervisorConnection -LiteralPath "XDHyp:\Connections\AzureCon"
   ```

   SPNに必要なロールレベルの権限:

   - Microsoft.Authorization/roleDefinitions/read (サブスクリプションレベル、またはリソースグループが指定されている場合はリソースグループレベル)
   - Microsoft.Authorization/roleAssignments/read (サブスクリプションレベル、またはリソースグループが指定されている場合はリソースグループレベル)

   SPN に必要な API レベルの権限:

   Microsoft.Graph:

   - Application.Read.All
   - Directory.Read.All
   - ServicePrincipalEndpoint.Read.All

5. 権限を検索するために必要な不足している権限を追加した後、次のコマンドを実行して、さまざまなカテゴリで権限があるかどうかを確認します。

   例:

   より高いレベルの承認が必要なサブスクリプションレベルで接続をテストするには:

   ```
   Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\ AzureCon
   -SecurePassword $password -UserName 922e65d5-38ae-4cf5-xxxx-xxxxxxxxx
   ```

   例:

   高レベルの承認なしでリソースグループレベルで接続をテストするには:

   ```
   Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\testles
   -CustomProperties $customProperties | Format-List
   ```

   注:

> CustomPropertiesパラメーターは、リソースグループが接続固有の情報であるため、リソースグループレベルを提供するために使用されます。

> 例:

リソースグループレベルでより高いレベルの承認を使用して接続をテストするには:

```
Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\testles
-SecurePassword $password -UserName
922e65d5-38ae-4cf5-832b-54122196b7dd -CustomProperties
$customProperties
```

アクセス許可については、必要なAzureアクセス許可を参照してください。

Azureシークレット環境でホスト接続を検証する

PowerShellコマンド `Test-HypHypervisorConnection` を使用して、Azureシークレット環境でホスト接続に必要な権限があるかどうかを検証できます。

ただし、検証結果を正常に取得するには、カスタムプロパティ `AuthenticationObjectId` を持つ既存のホスト接続を作成または更新します。このプロパティには、ホスティング接続に関連付けられているサービスプリンシパルのオブジェクトIDが格納されます。

> **注:**

> Azureポータルからサービスプリンシパルのオブジェクトを取得します。アプリケーションのIDは使用しないでください。

AuthenticationObjectId を含めるようにホスト接続を作成または更新する

`New-Item` を使用してホスト接続を作成し、`AuthenticationObjectId` をカスタムプロパティとして追加します。例：

```
New-Item -ConnectionType 'Azure' -HypervisorAddress @('http://
hypervisorhost1.example.com','http://hypervisorhost2.example.com')`

    -LoggingId $loggingId -Path @('XDHyp:\\Connections\\Example') -Persist
-Scope @() `
```

```
    -Password 'Password' -UserName 'root' -CustomProperties <Property
xsi:type="StringProperty" Name="AuthenticationObjectId" Value="Object ID
of the service principal"/>
```

`Set-Item` を使用して既存のホスト接続を更新し、`AuthenticationObjectId` をカスタムプロパティとして追加します。手順は次のとおりです。

1. Remote PowerShell SDKを使用してPowerShellウィンドウを開きます。
2. 次のコマンドを実行します。

```
Add-PSSnapin citrix*.

cd XDHyp:\Connections\

dir
```

3. 接続から `CustomProperties` をメモ帳にコピーし、プロパティ設定 `<Property xsi:type="StringProperty" Name="AuthenticationObjectId" Value="Object ID of the service principal"/>` を `CustomProperties` に追加します。
4. PowerShellウィンドウで、変更されたカスタムプロパティに変数を割り当てます。
5. `$cred = Get-Credential` を実行します。プロンプトが表示されたら、接続資格情報を入力します。資格情報は Azure アプリケーション ID とシークレットです。
6. `Set-Item -PSPath XDHyp:\Connections\<Connection_Name> -CustomProperties $customProperty -username $cred.username -Securepassword $cred.password` を実行します。
7. 更新された `CustomProperties` 設定を確認するには、`dir` を実行します。

```
Set-Item -PSPath XDHyp:\Connections\$connName -CustomProperties
<Property xsi:type="StringProperty" Name="AuthenticationObjectId"
Value="Object ID of the service principal"/> -username $cred.username
-Securepassword $cred.password
```

権限のホスト接続を検証する

必要なロールと権限のホスト接続を検証するには、次のコマンドを実行します。

- サブスクリプションレベルでロールと権限が割り当てられている場合：

```
Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\<Your-
HostingConnection>
```

- リソースグループレベルでロールと権限が割り当てられている場合：

```
Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\<Your-
HostingConnection>  -CustomProperties $CustomProperties



$CustomProperties = '<CustomProperties xmlns:xsi="http://www.w3.org/
2001/XMLSchema-instance" xmlns="http://schemas.citrix.com/2014/xd/
machinecreation">'`

+ '<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="ExampleResourceGroup" />'`

+ '</CustomProperties>'
```

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- Azure固有の情報については、「Microsoft Azureカタログの作成」を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

マイクロソフト システムセンター 仮想マシンマネージャー への接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明しています。以下の情報は、Microsoft System Center Virtual Machine Manager (VMM) に固有の詳細を扱っています。

注:

> VMM への接続を作成する前に、まず VMM アカウントをリソースの場所として設定する必要があります。(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/install-prepare/msscvmm.html)を参照してください。

接続を作成する

MCSを使用してVMをプロビジョニングした場合は、接続作成ウィザードで次の操作を行います。

- ホストサーバーの完全修飾ドメイン名としてアドレスを入力します。
- 以前に設定した管理者アカウントの資格情報を入力します。このアカウントには、新しいVMを作成する権限が必要です。
- 「ホストの詳細」ダイアログボックスで、VMの作成時に使用するクラスターまたはスタンドアロンホストを選択します。

> **重要**
>
> 単一のHyper-Vホスト展開を使用している場合でも、クラスターまたはスタンドアロンホストを参照してください。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- SMB 3 ファイル共有でMCSを使用してマシンカタログを作成する方法については、(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/machine-catalogs-create/create-machine-catalog-mscvmm.html)を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

Nutanixへの接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明しています。以下の情報はNutanixに固有の詳細を扱っています。

> **注:**

> Nutanixへの接続を作成する前に、まず、リソースの場所としてNutanixアカウントの設定を完了する必要があります。Nutanix仮想化環境を参照してください。

Nutanix AHV Prism Centralホスト接続

Nutanix AHV Prism Centralホスト接続を作成する前に、前提条件を参照してください。

以下のいずれかの方法で接続を作成できます。

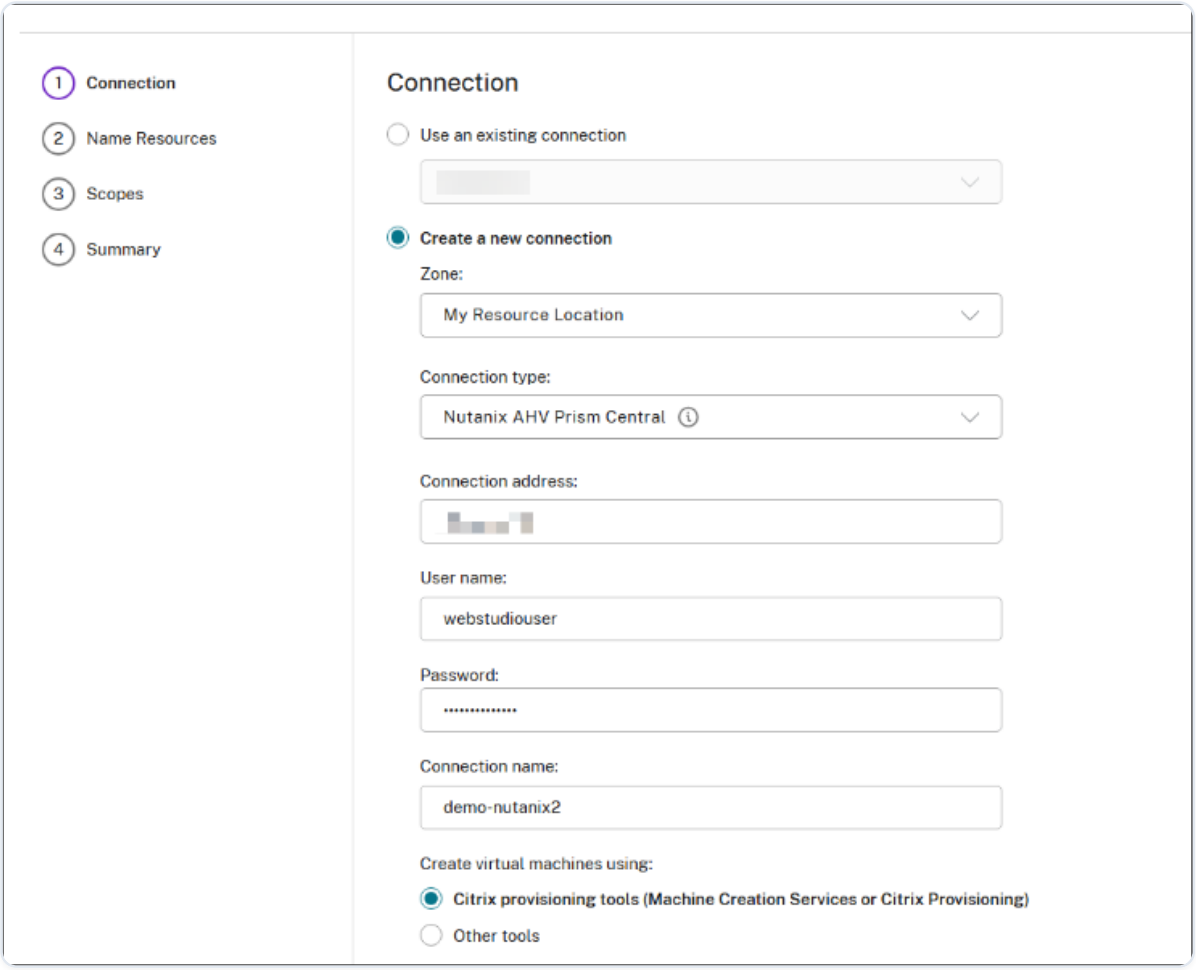
- ウェブスタジオ
- PowerShellコマンド

制限事項

- Nutanix AHV Prism Centralホスト接続は、テンプレートやネットワークなどの項目で重複するオブジェクト名をサポートしていません。カタログ作成のためにそのような項目を選択すると、予期しない動作につながる可能性があります。

Web Studio を使用して接続を作成する

1. Citrix Cloudにサインインします。
2. **管理**をクリックします。
3. 左ペインで**ホスティング**を選択します。
4. アクションバーで**接続とリソースの追加**をクリックします。
5. 「**接続**」ページで：
    a. **新しい接続を作成**を選択します。
    b. 接続の種類として**Nutanix AHV Prism Central**を選択します。
    c. 接続アドレスとして、Nutanix AHV Prism CentralのIPアドレスを入力します。
    d. 管理者資格情報とわかりやすい接続名を入力します。
    e. **Citrixプロビジョニングツール (Machine Creation Services™またはCitrix Provisioning)**を選択します。
    f. **Next**をクリックします。

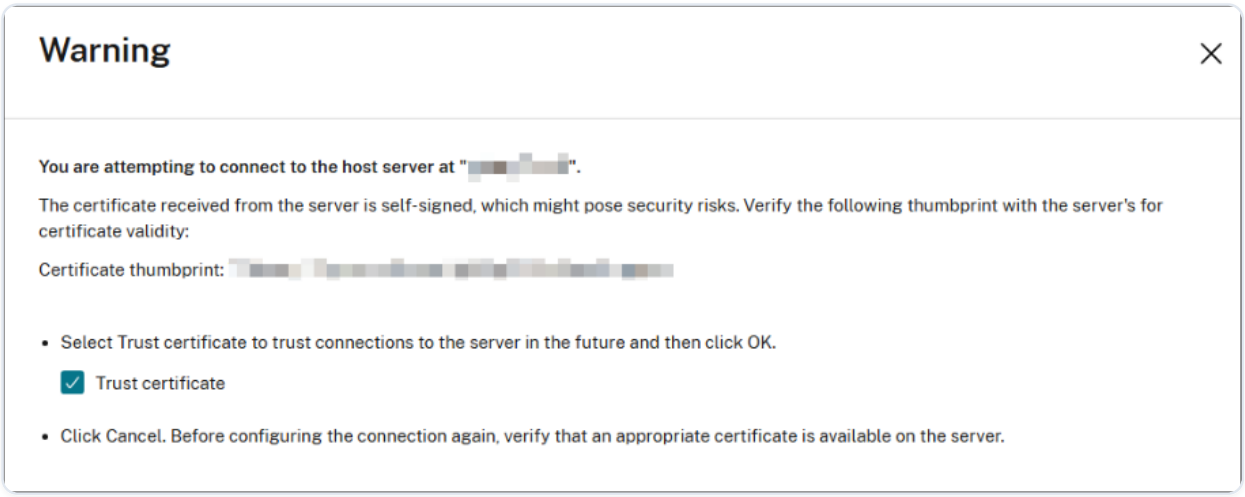


注:

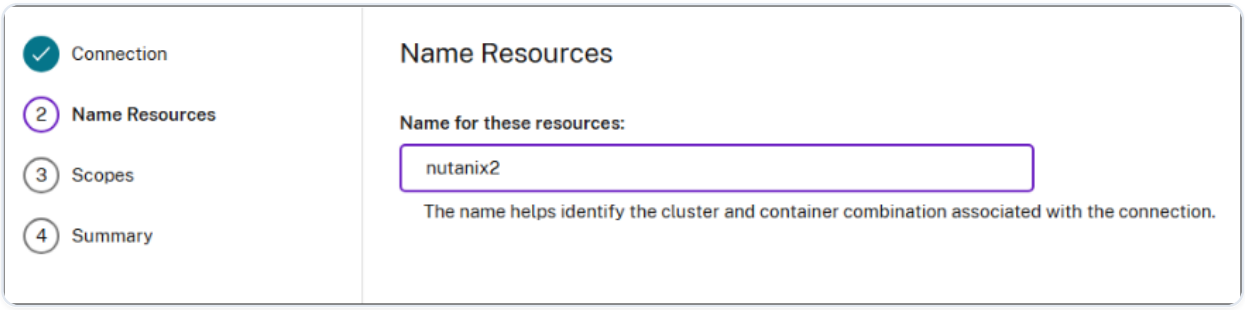
ホスト接続の作成中に、ネットワークまたはクラスターの選択は必要ありません。ホスティングユニット名のみが必要です。マシンカタログの作成中にネットワークとクラスターを選択します。

6. **次へ**をクリックすると、Citrix Virtual Apps and Desktops はプライベート CA 署名証明書を受信し、**警告**ページが表示されます。詳細については、「Nutanix Prism Central へのセキュアな接続」を参照してください。

   受信したサムプリントをサーバーのサムプリントと比較して、証明書の有効性を確認します。有効な場合は、**証明書を信頼する**を選択し、**OK**をクリックして接続の作成を続行します。Citrix Virtual Apps and Desktops は証明書を信頼し、将来の検証のためにサムプリントを保存します。



7. **リソースの命名**ページで、リソースの一意の名前を追加します。**次へ**をクリックします。



8. 「**スコープ**」ページで、このホストのスコープを1つ以上選択します。
9. 「**概要**」ページで、構成を確認し、「**完了**」をクリックします。

> **注:**
>
> Nutanix AHV Prism Central接続は、他の種類のNutanix接続と共存できます。

Nutanix Prism Centralへのセキュアな接続

Nutanix SSLサムプリント機能は、Nutanix Prism Centralハイパーバイザーへのホスト接続を確立する際の証明書の信頼を簡素化します。この機能により、信頼されていない証明書のサムプリントをサイトデータベースに保存できるようになり、Citrix Virtual Apps and Desktopsがハイパーバイザーを常に信頼できるものとして認識するようになります。

Nutanixホスト接続を作成すると、「**警告**」ページが表示され、接続先のマシンの証明書が提示され、それを信頼するかどうかを決定できます。

PowerShellを使用して接続を作成する

1. PowerShellウィンドウを開きます。
2. `asnp citrix*` を実行します。

3. 次のパラメーターを設定します。

```
$ConnectionName = “Name of the connection”

$UserName = “Username of the account on hypervisor”

$ZoneUid =  “UID of the zone where the hosting connection will be
created”

$HypervisorAddress = “The IP address of the hypervisor”

$SSLThumbprint =  “The Nutanix PC SSL thumbprint can be set using
PowerShell SDK”

$connectionPath = "XDHyp:\Connections\" + $ConnectionName

$SecureUserInput = Read-Host "Enter the password for the user $
($UserName)" -AsSecureString

$EncryptedUserInput = $SecureUserInput | ConvertFrom-SecureString

$SecurePass = ConvertTo-SecureString -String $EncryptedUserInput
```

4. 新しいホスティング接続の項目を作成します。例：

```
$connection = New-Item -Path @($connectionPath) -ConnectionType
"Custom" -HypervisorAddress ` @($HypervisorAddress) -Persist -PluginId
"AcropolisHypervisorPCFactory" -Scope @() ` -SecurePassword $SecurePass
-SSLThumbprint @($SSLThumbprint) -UserName $UserName -ZoneUid `
$ZoneUid
```

5. ブローカーハイパーバイザー接続を作成します。例：

```
New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$connection.HypervisorConnectionUid
```

ホスティングユニットを作成する

PowerShellコマンドを使用してホスティングユニットを作成する場合、次の必須パラメーターを指定します。

- `$HostUnitName`: 作成するホスティングユニットの名前

- `ConnectionName`: 以前に作成したハイパーバイザー接続の名前

1. PowerShellウィンドウを開きます。
2. `add-pssnapin citrix*`を実行します。
3. ホスティングユニットを作成するためのPowerShellコマンドを実行します。例：

```
$hostUnitPath = "XDHyp:\HostingUnits\" + $HostUnitName

New-Item -Path @($hostUnitPath) -RootPath $connectionPath
-HypervisorConnectionName $ConnectionName -CustomProperties ""
-NetworkPath @() -StoragePath @()
```

注:

ホスト接続の作成中に、ネットワークまたはクラスターの選択は不要です。ホスティングユニット名のみが必要です。マシンカタログの作成中にネットワークとクラスターを選択します。

ホスト接続の管理

既存のホスト接続は、以下を使用して管理できます。

- ウェブスタジオ
- PowerShell

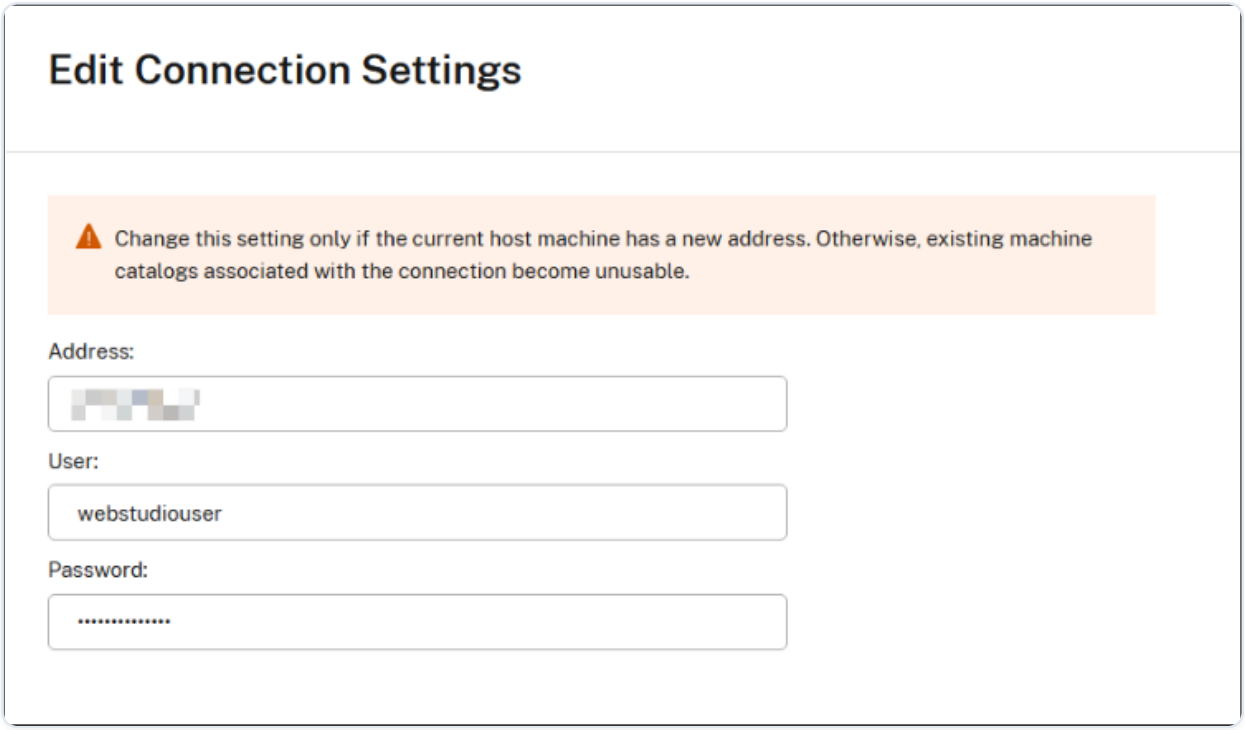
WEB STUDIO を使用してホスト接続を管理する

ホスト接続を作成したら、Web Studio の**ホスティング**ノードに移動し、接続を右クリックして次の操作を実行します。

- **接続の削除**
- **接続の名前を変更**
- **接続の編集**
- **メンテナンスモードをオンにする**
- **マシンを表示**
- **接続のテスト**
- **TLS証明書の信頼をテスト**

WEB STUDIO を使用して接続を編集する

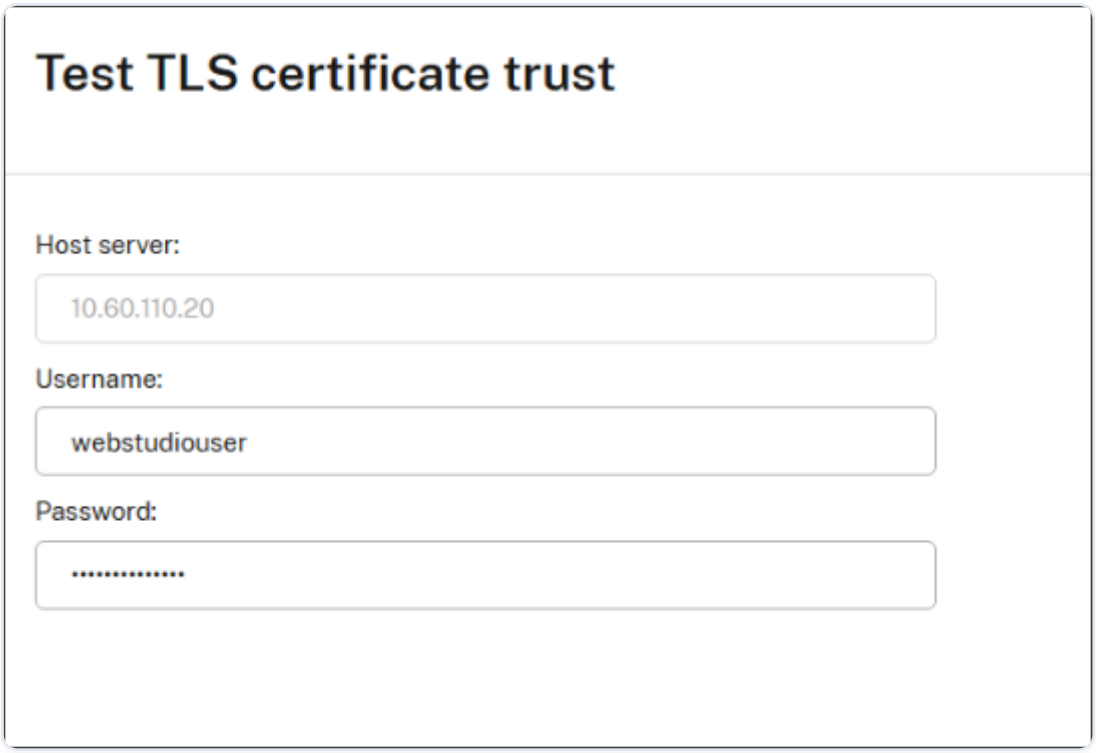
1. 接続を右クリックし、**接続の編集**をクリックします。
2. **接続プロパティ**ページで、**設定の編集**をクリックします。
3. **接続設定の編集**ページで、証明書情報を変更し、**保存**をクリックします。



4. **警告**ページで**証明書を信頼**を選択して、新しい証明書のサムプリントを信頼します。

TLS証明書の信頼をテストする

1. 接続を右クリックし、**TLS証明書の信頼をテスト**をクリックします。
2. **TLS証明書の信頼をテスト**ページで、証明書情報を変更し、**テスト**をクリックします。



テスト結果が成功しなかった場合は、「Web Studio を使用して接続を編集する」を使用して接続の証明書情報を変更します。

POWERSHELL を使用してホスト接続を管理する

PowerShell コマンドを使用して、次のことができます。

- ホスト接続のユーザー資格情報を変更または更新する。例:

```
$UserName = "Username of the account on hypervisor"

$SecureUserInput = Read-Host "Enter the password for the user $
($UserName)" -AsSecureString

$EncryptedUserInput = $SecureUserInput | ConvertFrom-SecureString

$SecurePass = ConvertTo-SecureString -String $EncryptedUserInput

Set-Item  -LiteralPath @("XDHyp:\Connections\<Host connection name>")
 -SecurePassword $SecurePass -UserName $UserName
```

- SSLThumbprint をリセットする。例:

```
$SSLThumbprint =  "The Nutanix PC SSL thumbprint value"

Set-Item  -LiteralPath @("XDHyp:\Connections\<Host connection name>")
```

```
 -SecurePassword $SecurePass -UserName $UserName -SSLThumbprint
$SSLThumbprint
```

必要な権限

Nutanix AHV Prism Central ホスト接続に使用される管理アカウントには、次の権限が必要です。

ホスト接続の作成

クラスター:

- クラスターの表示

VM の電源管理

AHV VM:

- ACPI 仮想マシンのシャットダウン
- ACPI 仮想マシンの再起動
- ゲスト仮想マシンの再起動
- ゲスト仮想マシンのシャットダウン
- 仮想マシンの電源オフ
- 仮想マシンの電源オン
- 仮想マシンのリセット
- 既存の仮想マシンの表示

クラスター:

- クラスターの表示

サブネット:

- サブネットの表示

VMのプロビジョニング

AHV VM:

- ACPI仮想マシンの再起動
- ACPI仮想マシンのシャットダウン
- 仮想マシンカテゴリの関連付け
- 新しい仮想マシンの作成
- 仮想マシンの作成

- 仮想マシンディスクの作成
- 仮想マシンNICの作成
- 既存の仮想マシンの削除
- 仮想マシンの削除
- 仮想マシンディスクの削除
- 仮想マシンGPUの削除
- 仮想マシンNICの削除
- 仮想マシンカテゴリの関連付け解除
- 仮想マシンCD-ROMの取り出し
- ゲスト仮想マシンの再起動
- ゲスト仮想マシンのシャットダウン
- 仮想マシンの電源オフ
- 仮想マシンの電源オン
- 仮想マシンのリセット
- 仮想マシンのスナップショット
- 仮想マシンの基本構成の更新
- 仮想マシンディスクの更新
- 仮想マシンディスクリストの更新
- 仮想マシンNICの更新
- 既存の仮想マシンの表示
- 仮想マシンの表示
- 仮想マシンCD-ROMの表示
- 仮想マシンディスクの表示
- 仮想マシンGPUの表示
- 仮想マシンNICの表示

AHV VMリカバリポイント:

- AHV VMリカバリポイントの表示

カテゴリ:

- カテゴリの表示

クラスター:

- クラスターの表示

ホスト:

- ホストの表示

イメージ:

- イメージの作成
- イメージの削除
- イメージの更新
- イメージの表示

リカバリポイント:

- リカバリポイントの作成
- リカバリポイントの削除
- リカバリポイントのレプリケート
- リカバリポイントの復元
- リカバリポイントの表示
- 仮想マシンリカバリポイントの表示

ストレージコンテナ:

- ストレージコンテナの表示
- ストレージコンテナデータストアの表示
- ストレージコンテナ統計の表示

ストレージポリシー:

- ストレージポリシーの表示

サブネット:

- サブネットの表示
- サブネットvNICの表示

タスク:

- タスクのキャンセル
- タスクの表示

VMリカバリポイント:

- VMリカバリポイントを削除
- VMリカバリポイントを復元
- VMリカバリポイントを表示

VMテンプレート:

- VMテンプレートを表示
- VMテンプレートのバージョンを表示
- VMテンプレートを展開

ボリュームグループ:

- ボリュームグループをAHV VMにアタッチ
- ボリュームグループをAHV VMからデタッチ
- ボリュームグループを表示
- ボリュームグループの詳細を表示

VPC:

- VPCを表示

Nutanix AHV、Nutanix AHV PC、またはNutanix AHV DRaaSホスト接続

1. Citrix Cloudにサインインします。
2. **管理**をクリックします。
3. 左側のペインで を選択します。
4. アクションバーで をクリックします。
5. ページで、次の接続タイプを選択できます。

    - **Nutanix AHV**: Prism Element (PE) クラスターのアドレス、資格情報、および接続の名前を指定します。 ページで、ネットワークを選択し、ホスティングユニットの名前を指定します。

        > **注:**

> Nutanix AHV (Prism Element) をリソースとして使用してマシンを展開する場合は、VM のディスクが格納されているコンテナを選択します。

- **Nutanix AHV PC**: Prism Central (PC) のアドレス、資格情報、および接続の名前を指定します。 ページで、リストからネットワーク、クラスターを選択し、ホスティングユニットの名前を指定します。

> **注:**
>
> 接続タイプ **Nutanix AHV PC** は、Azure 上の Nutanix Cloud Cluster (NC2) への接続を作成する場合にのみ使用されます。また、マシンカタログは、Azure 接続上の NC2 内の単一クラスターでのみホストできます。このタイプの接続には、Cloud Connector に Nutanix プラグインがインストールされている必要があります。

- **Nutanix AHV DRaaS**：アドレスとユーザー名を指定し、Nutanix DRaaS資格情報ファイルに含まれる公開鍵と秘密鍵をインポートします (`.pem`)。(公開鍵と秘密鍵は、Nutanix DRaaS管理者によってNutanix DRaaSクラウドで生成されます。)
  - キーをインポートするには、資格情報ファイルを見つけてメモ帳（または任意のテキストエディター）で開き、内容をコピーします。その後、 ページに戻り、 を選択し、内容を貼り付けて、 を選択します。資格情報の内容や形式を変更しないでください。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- Nutanix固有の情報については、「Nutanixカタログの作成」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- Nutanix仮想化環境
- Nutanixクラウドおよびパートナーソリューション

Nutanix クラウドおよびパートナーソリューションへの接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明します。以下の情報では、Nutanix クラウドおよびパートナーソリューションに固有の詳細について説明します。

ニュータニックス AHV プリズムセントラル

Citrix Virtual Apps and Desktops は、Citrix管理のNutanix AHV Prism Centralプラグイン向けに、以下のクラウドハイパーバイザーで Nutanix Cloud Clusters (NC2) をサポートします。

- AWS
- マイクロソフト アジュール

> **注:**
>
> - AWS および Azure 上の NC2 への接続を作成する前に、クラウドプラットフォームでリソースを準備してください。Nutanix クラウドおよびパートナーソリューションを参照してください。
> - ホスティング接続の作成、VM の電源管理、およびカタログのプロビジョニングに必要な権限については、必要な権限を参照してください。

Azure および AWS 上の NC2 への接続

Azure または AWS 上の Nutanix Cloud Cluster (NC2) に接続するには、展開済みの Prism Central インスタンスへのアクセスと、Prism Admin ロールを持つ資格情報が必要です。

ホスト接続は、以下を使用して作成できます。

- ウェブスタジオ
- PowerShell

接続に関する完全な情報については、Nutanix AHV Prism Central への接続を参照してください。

ニュータニックス プリズム エレメント

Citrix Virtual Apps and Desktops は、Nutanix Prism Element プラグイン向けに、以下のクラウドハイパーバイザーで Nutanix Cloud Clusters (NC2) をサポートします。

- AWS

Nutanix Prismへの接続

Nutanixクラスターを作成したら、Nutanix Prismに接続します。 Nutanix Prismに接続するには：

1. 10.0.129.0/24サブネットに踏み台VMを作成します。

2. 踏み台VMにRDP接続し、前のセクションでコピーした**Prism Element**のURLにアクセスします。
3. デフォルトの資格情報 `admin:nutanix/4u` を使用してログインします。パスワードを変更することを忘れないでください。

Nutanixクラスター上にVMを作成する

Nutanix Prismに接続した後、Nutanixクラスター上にVMを作成します。

VMにインターネットアクセスが必要な場合

1. AWSコンソールに移動します。
2. Nutanix CFS によって作成された VPC と同じ VPC に、新しいサブネット 10.0.130.0/24 を作成します。
3. このサブネットのルートテーブルに、すべての非ローカルトラフィックを上記のNATゲートウェイに転送するルートを追加します。
4. 踏み台VMにRDP接続し、前のセクションでコピーした**Prism Element**のURLにアクセスしてログインします。
5. 新しいネットワークを追加します。**Settings>Network Configuration>Create Subnet** に移動します。AWS で使用したのと同じサブネット 10.0.130.0/24 を使用します。
6. その新しいサブネットにすべての VM (AD、CC、VDA など) を作成します。

VM がインターネットアクセスを必要としない場合

1. 踏み台 VM に RDP 接続し、前のセクションでコピーした **Prism Element** の URL に移動してログインします。
2. 新しいネットワークを追加します。**Settings>Network Configuration>Create Subnet** に移動します。サブネット 10.0.129.0/24 を使用します。
3. そのサブネットにすべての VM (AD、CC、VDA など) を作成します。

> **ヒント:**
>
> VM の時刻とタイムゾーン情報が正しく設定されていることを確認してください。これは特に AD に当てはまります。

ホスト接続を作成する

1. Web Studio から、左側のペインで**ホスティング**を選択します。
2. **Add Connection and Resources** をクリックします。

3. **Connection** 画面で、**Create a new Connection** を選択し、**Connection address** に `https://xxx.xxx.xxx.xxx:9440` を入力します。
4. UI に従ってウィザードを完了します。

> **注:**
>
> すべてのコネクタVMには、Web StudioでNutanixオプションを利用できるようにするため、Nutanixプラグインがインストールされている必要があります。プラグインがNutanixゾーンで使用されていない場合でも同様です。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- Nutanix 固有の情報については、「Nutanix カタログの作成」を参照してください。(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/machine-catalogs-create/create-machine-catalog-nutanix.html)

詳細情報

- 接続とリソース
- Nutanix仮想化環境
- Nutanixクラウドおよびパートナーソリューション

Oracle C3 への接続 (プレビュー)

接続とリソースの作成および管理 の記事では、一般的な接続ワークフローについて説明しています。以下の情報では、Oracle C3 固有の詳細について説明します。

> **注:**
>
> Oracle C3 への接続を作成する前に、Oracle C3 環境のセットアップを完了してください。Oracle C3 仮想化環境 を参照してください。

接続を作成する

Oracle C3 への接続は、次の方法で作成できます。

- ウェブスタジオ

- PowerShellコマンド

Web Studio を使用して接続を作成する

1. で、接続の種類として を選択します。
2. で、 を選択し、Oracle C3 構成ファイル (`.ini`) の内容を貼り付けます。
3. で、 を選択し、資格情報ファイル (`.pem`) から秘密キーの内容を貼り付けます。
4. わかりやすい を入力します。
5. ウィザードを続行し、接続を検証します。

> **注:**
>
> はインポートされた構成から抽出され、Web Studio で直接編集することはできません。Oracle C3 エンドポイントも、インポートされた構成の `region` の値から派生するため、このフローで手動で入力することはできません。Oracle C3 形式で `region` を `<service_name>.<domain_name>` (FQDN 形式の値) として入力します。

> Web Studio で構成をインポートすると、次のキーのみがインポートされます。その他のキーはすべて無視されます。

- `user`
- `fingerprint`
- `tenancy`
- `region`

接続設定は、次の証明書シナリオで停止する可能性があります。

- 証明書の検証またはサムプリントの確認が失敗した場合: 問題が解決されるまで接続の作成はブロックされます。

PowerShellコマンドを使用して接続を作成する

PowerShell を使用して接続を作成する場合、以下を指定します。

- Oracle C3 エンドポイントアドレス（通常は `https://iaas.<service_name>.<domain_name>` ）。
- 構成ファイル (`user`) からの Oracle C3 ユーザー OCID。
- 資格情報ファイル (`.pem`) からの秘密鍵の内容。セキュア文字列として渡されます。

- `TenancyOcid`、`Fingerprint`、および `Region` を含む `CustomProperties` XML。
- 必要に応じて、証明書信頼検証用の SSL サムプリント。

パターン例：

```
$CustomProperties = '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">' +



'<Property xsi:type="StringProperty" Name="TenancyOcid" Value="' +
$TenancyOcid + '" />' +



'<Property xsi:type="StringProperty" Name="Fingerprint" Value="' +
$Fingerprint + '" />' +



'<Property xsi:type="StringProperty" Name="Region" Value="' + $Region +
'" />' +



'</CustomProperties>'



$PrivateKey = ConvertTo-SecureString $PrivateKeyContent -AsPlainText
-Force



New-Item -ConnectionType "Custom" `



-HypervisorAddress $Endpoint `
```

```
-Path @("XDHyp:\Connections\$ConnectionName") `


-Persist `


-PluginId "OracleC3PluginFactory" `


-CustomProperties $CustomProperties `


-SecurePassword $PrivateKey `


-UserName $UserOcid `


-SslThumbprint $SslThumbprint
```

注:

`$Region` を `<service_name>.<domain_name>` 形式の Oracle C3 リージョン値に設定します。証明書信頼ポリシーで必要な場合は `-SslThumbprint` を使用します。

証明書とサムプリントの検証

Oracle C3 接続を成功させるには、証明書の検証が成功し、必要に応じてサムプリント値が正しい必要があります。

接続の管理

このセクションでは、以下について説明します。

- Web Studio を使用して証明書の問題を修正する
- PowerShell を使用してサムプリント値を更新する

証明書の問題を修正する

証明書の問題が発生した場合、Citrix はワークロード操作を保護するために Oracle C3 接続をブロックします。**ホスト接続**リストの接続の横にエラーアイコンが表示されます。

修正するには：

1. **ホスト接続**から接続を開きます。
2. 「**トラブルシューティング**」の詳細を表示し、証明書の問題を特定します。
3. 「**接続の編集 > 設定の編集**」を選択します。
4. Oracle C3 の場合、プロンプトが表示されたら、構成と秘密鍵を再インポートしてください。両方が利用可能な場合は、接続作成時と同様に、変更を保存して新たな証明書検証を開始し、提示された更新された証明書サムプリントを検証または信頼してください。

サムプリント値の更新

作成後に `Set-Item` を使用してサムプリント値を更新できます。

1. 接続の詳細を取得します。

```
Get-Item -LiteralPath xdhyp:\connections\<OracleC3ConnectionName>
```

2. サムプリント値を更新します。

```
Set-Item -LiteralPath xdhyp:\connections\<OracleC3ConnectionName> `



-Username <UserName> `



-SslThumbprint <ThumbprintValue>
```

3. 更新された値を確認します。

```
Get-Item -LiteralPath xdhyp:\connections\<OracleC3ConnectionName>
```

> **注:**
>
> 指定されたサムプリントが正しくないか、サーバー証明書の信頼と一致しない場合、更新は失敗します。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- Oracle C3 固有の情報については、「Oracle C3 マシンカタログの作成」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- Oracle C3 仮想化環境

Red Hat OpenShiftへの接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明しています。以下の情報は、Red Hat OpenShiftに固有の詳細を扱っています。

> **注:**
>
> Red Hat OpenShiftへの接続を作成する前に、まずRed Hat OpenShiftのセットアップを完了する必要があります。「Red Hat OpenShift仮想化環境」(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/install-prepare/red-hat-open-shift.html)を参照してください。

接続を作成する

Red Hat OpenShiftクラスターへの接続は、以下を使用して作成できます。

- ウェブスタジオ
- PowerShell

Web Studioを使用して接続を作成する

1. Web Studioで、 **>** を開きます。
2. **接続**ページで、以下の手順に従って接続を構成します。

a. **新しい接続を作成**を選択します。
b. 接続の種類として**Red Hat OpenShift**を選択します。
c. **接続アドレス**フィールドに、OpenShiftサーバーのIPアドレス、ホスト名、またはFQDNを入力します。
d. サービスアカウントトークンとわかりやすい接続名を入力します。
e. 「**ゾーン名**」フィールドでゾーンを選択します。オプションは、構成したすべてのリソースの場所です。
f. 仮想マシンを作成するには、「**その他のツール**」を選択します。

> **注:**
>
> 「**その他のツール**」を選択すると、ホスティングユニットなしでホスティング接続のみが作成されます。

3. **Next**をクリックします。
4. 自己署名証明書が検出された場合、証明書のサムプリントを含む警告ページが表示されます。続行するには：

   a. サムプリントをサーバーのものと比較して、証明書の有効性を確認します。
   b. 有効な場合は、「**証明書を信頼する**」を選択し、「**OK**」をクリックして接続設定を完了します。

      証明書は信頼済みとしてマークされ、サムプリントは今後の検証のために保存されます。

5. 「**スコープ**」ページで、このホストのスコープを1つ以上選択します。
6. 「**概要**」ページで、構成を確認し、「**完了**」をクリックします。

PowerShellコマンドを使用して接続を作成する

PowerShellコマンドを使用して接続を作成する場合、次の情報を提供します。

- ホスティング接続名
- クラスターAPIアドレス
- ユーザー名
- パスワード（サービスアカウントトークン）

- SSLサムプリント: これはCA証明書のサムプリントであり、APIサーバーのサムプリントではありません。サムプリントを指定せずにホスティング接続を作成しようとすると、サーバーがCA証明書のサムプリントを提供します。
- ゾーンUID

1. PowerShellウィンドウを開きます。
2. `add-pssnapin citrix®*`を実行します。
3. ホスティング接続を作成するには、次のコマンドを実行します。

   サムプリントを指定せずにホスティング接続を作成しようとすると、サーバーがCA証明書のサムプリントを提供します。例:

```
$newItemParameters = @{

ConnectionType= "Custom"

PluginId= "OpenShiftPluginFactory"

HypervisorAddress = "https://
api.myopenshiftclusteraddress.mydomain.local:6443"

Path= "XDHyp:\Connections\OpenShiftConnectionName"

Persist= $true

UserName= "__ServiceAccount__"

Password= "<service account token>"

ErrorVariable= "connectionError"

 }



& New-Item @newItemParameters




$newItemParameters["SSLThumbprint"] =
```

```
$connectionError[0].ErrorData.Thumbprint

$connection = & New-Item @newItemParameters

$brokerConnection = New-BrokerHypervisorConnection
-HypHypervisorConnectionUid $connection.HypervisorConnectionUid
```

ホスティングユニットを作成する

ホスティングユニットは、VMが作成される環境を表します。ホスティングユニットを作成するには、OpenShiftから次の入力が必要です。

- 名前空間
- ストレージクラス
- ネットワークアタッチメント定義

ホスティングユニットは名前空間にバインドされます。これは、1つのホスティングユニットが1つの名前空間のみにアクセスでき、その名前空間下のVMを管理することを意味します。

ホスティングユニットは、次の方法で作成できます。

- ウェブスタジオ
- PowerShell

Web Studioを使用してホスティングユニットを作成する

1. **ホスティング > 接続とリソースの追加**に移動します。
2. 「**接続**」ページで：
    - ホスティングユニットとともに新しいホスティング接続を作成するには、**Create a new connection** を選択し、次の手順を実行します:
        a. 接続の種類として**Red Hat OpenShift**を選択します。
        b. **接続アドレス**フィールドに、OpenShiftサーバーのIPアドレス、ホスト名、またはFQDNを入力します。
        c. サービスアカウントトークンとわかりやすい接続名を入力します。
        d. 「**ゾーン名**」フィールドでゾーンを選択します。オプションは、構成したすべてのリソースの場所です。
        e. 仮想マシンを作成するための **Citrix provisioning tools (Machine Creation Services™ or Citrix Provisioning)** を選択します。

f. **Next**をクリックします。

g. **Warning** ページで、証明書の有効性を確認し、**Trust certificate** を選択します。

- 既存のホスト接続からホスティングユニットを作成するには、**Use an existing Connection** を選択し、その後、関連する接続を選択します。

3. **Namespace Selection** ページで、この接続の名前空間を選択します。
4. **ストレージの選択**ページで、ウィザードの次のページに進む前に、サポートされているデータ型ごとに少なくとも1つのストレージデバイスを選択します。ストレージの選択について詳しくは、「ホストストレージ」を参照してください。
5. **ネットワーク**ページで、リソースの名前を入力します。この名前は、接続に関連付けられているストレージとネットワークの組み合わせを識別するためにStudioに表示されます。VMが使用するネットワークを1つ以上選択します。
6. **概要**ページで詳細を確認し、**完了**をクリックします。

PowerShellを使用してホスティングユニットを作成する

PowerShellコマンドを使用してホスティングユニットを作成する場合は、次の情報を提供します。

- ホスティング接続名
- ホスティングユニット名
- ターゲットの名前空間名
- StorageClasses 名
- NetworkAttachmentDefinition 名

1. PowerShellウィンドウを開きます。
2. `add-pssnapin citrix*` を実行します。
3. PowerShellコマンドを実行して、ホスティングユニットを作成します。例：

```
$HostingConnectionName = "OpenShiftConnectionName"

$HostingUnitName = "HostingUnitName"

$TargetNamespace = "TargetNamespaceName"

$StorageClassToUse = "YourStorageClassesName"

$NetworkAttachmentDefinition = "YourNetworkAttachmentDefinitionName"
```

```
New-HypStorage `

-StoragePath @("XDHyp:\Connections\$HostingConnectionName\
$TargetNamespace.namespace\$StorageClassToUse.storage") `

-StorageType "TemporaryStorage"

New-Item `

-CustomProperties "" `

-HypervisorConnectionName $HostingConnectionName `

-NetworkPath @("XDHyp:\Connections\$HostingConnectionName\
$TargetNamespace.namespace\$NetworkAttachmentDefinition.network") `

-Path @("XDHyp:\HostingUnits\$HostingUnitName") -RootPath "XDHyp:
\Connections\$HostingConnectionName\$TargetNamespace.namespace" `

-StoragePath @("XDHyp:\Connections\$HostingConnectionName\
$TargetNamespace.namespace\$StorageClassToUse.storage")
```

次の手順

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- Red Hat OpenShift固有の情報については、Red Hat OpenShiftカタログの作成を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

VMwareへの接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明しています。以下の情報は、VMware仮想化環境に固有の詳細を扱っています。

> **注:**

> VMwareへの接続を作成する前に、まずVMwareアカウントをリソースの場所として設定を完了する必要があります。「VMware仮想化環境」(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/install-prepare/vmware.html)を参照してください。

接続を作成する

接続作成ウィザードで：

1. VMware接続の種類を選択します。
2. vCenter SDKのアクセスポイントのアドレスを指定します。
3. 以前に設定した、VMを作成する権限を持つVMwareユーザーアカウントの資格情報を指定します。ユーザー名はdomain/usernameの形式で指定します。

VMware SSLサムプリント

VMware SSLサムプリント機能により、VMware vSphereハイパーバイザーへのホスト接続を手動で作成する必要がなくなります。接続を作成する前に、サイト内のDelivery Controllerとハイパーバイザーの証明書との間に信頼関係を手動で作成する必要はなくなりました。

VMware SSLサムプリント機能は、信頼されていない証明書のサムプリントをサイトデータベースに保存します。この構成により、ハイパーバイザーは、Controllerによって信頼されていない場合でも、Citrix Virtual Apps and Desktops™によって継続的に信頼されていると識別されることが保証されます。

StudioでvSphereホスト接続を作成する際、接続先のマシンの証明書を表示できるダイアログボックスが表示されます。その後、それを信頼するかどうかを選択できます。

必要な権限

この記事に記載されている権限の一部またはすべてを持つVMwareユーザーアカウントと1つ以上のVMwareロールを作成します。ロールの作成は、Citrix DaaS™のさまざまな操作をいつでも要求するためにユーザーの権限に必要とされる特定の粒度レベルに基づいて行います。ユーザー固有の権限をいつでも付与するには、**子に伝播**オプションを選択した状態で、少なくともデータセンターレベルでそれぞれのロールに関連付けます。ただし、`StorageProfile`権限と特定の`Tags`権限については、**子に伝播**なしで、ルートvCenter Serverレベルで権限を適用します。各テーブルの注記を参照してください。

次の表は、Citrix Virtual Apps and Desktops™の操作と、必要な最小限のVMware権限とのマッピングを示しています。

注:

権限リストの表示名、特に*ユーザーインターフェイス*は、一部のvSphereバージョンで異なります。たとえば、vSphere 6.7では、*ユーザーインターフェイス*権限は、このページに記載されている必要な権限で説明されている**Settings**および**Memory**ではなく、**Change Memory**および**Change Settings**です。

接続とリソースを追加する

SDK	ユーザーインターフェイス
システム. 匿名、システム. 読み取り、およびシステム. 表示	自動的に追加されます。組み込みの読み取り専用ロールを使用できます。

電源管理

SDK	ユーザーインターフェイス
VirtualMachine.Interact.PowerOff	仮想マシン > インタラクション > 電源オフ
VirtualMachine.Interact.PowerOn	仮想マシン > インタラクション > 電源オン
VirtualMachine.Interact.Reset	仮想マシン > インタラクション > リセット
VirtualMachine.Interact.Suspend	仮想マシン > インタラクション > サスペンド
Datastore.Browse	Datastore > データストアの参照

マシンのプロビジョニング (Machine Creation Services™)

MCS を使用してマシンをプロビジョニングするには、次の権限が必要です。

SDK	ユーザーインターフェイス
Datastore.AllocateSpace	Datastore > スペースの割り当て
Datastore.Browse	Datastore > データストアの参照
Datastore.FileManagement	Datastore > 低レベルファイル操作
Network.Assign	Network > ネットワークの割り当て

SDK	ユーザーインターフェイス
Resource.AssignVMToPool	リソース > 仮想マシンをリソースプールに割り当てる
VirtualMachine.Config.AddExistingDisk	仮想マシン > 構成 > 既存のディスクを追加
VirtualMachine.Config.AddNewDisk	仮想マシン > 構成 > 新しいディスクを追加
仮想マシン.構成.デバイスの追加または削除	仮想マシン > 構成 > デバイスの追加または削除
VirtualMachine.Config.AdvancedConfig	仮想マシン > 構成 > 詳細設定
VirtualMachine.Config.RemoveDisk	仮想マシン > 構成 > ディスクの削除
VirtualMachine.Config.CPUCount	仮想マシン > 構成 > CPU数の変更
VirtualMachine.Config.Memory	仮想マシン > 構成 > メモリの変更
VirtualMachine.Config.Settings	仮想マシン > 構成 > 設定の変更
VirtualMachine.Interact.PowerOff	仮想マシン > 操作 > 電源オフ
VirtualMachine.Interact.PowerOn	仮想マシン > 操作 > 電源オン
VirtualMachine.Interact.Reset	仮想マシン > 操作 > リセット
VirtualMachine.Interact.Suspend	仮想マシン > 操作 > サスペンド
VirtualMachine.Inventory.CreateFromExisting	仮想マシン > インベントリ > 既存から作成
VirtualMachine.Inventory.Create	仮想マシン > インベントリ > 新規作成
VirtualMachine.Inventory.Delete	仮想マシン > インベントリ > 削除
VirtualMachine.Provisioning.Clone	仮想マシン > プロビジョニング > 仮想マシンのクローン作成
VirtualMachine.State.CreateSnapshot	vSphere 5.0、Update 2、vSphere 5.1、Update 1、および vSphere 6.x、Update 1: 仮想マシン > 状態 > スナップショットの作成; vSphere 5.5: 仮想マシン > スナップショット管理 > スナップショットの作成

SDK	ユーザーインターフェイス
VirtualMachine.Config.Rename	仮想マシン > 構成 > 名前変更

イメージの更新とロールバック

SDK	ユーザーインターフェイス
Datastore.AllocateSpace	データストア > スペースの割り当て
Datastore.Browse	データストア > データストアの参照
Datastore.FileManagement	データストア > 低レベルファイル操作
Network.Assign	ネットワーク > ネットワークの割り当て
Resource.AssignVMToPool	リソース > 仮想マシンをリソースプールに割り当てる
VirtualMachine.Config.AddExistingDisk	仮想マシン > 構成 > 既存のディスクを追加
VirtualMachine.Config.AddNewDisk	仮想マシン > 構成 > 新しいディスクを追加
VirtualMachine.Config.AdvancedConfig	仮想マシン > 構成 > 詳細設定
VirtualMachine.Config.RemoveDisk	仮想マシン > 構成 > ディスクの削除
VirtualMachine.Interact.PowerOff	仮想マシン > 操作 > 電源オフ
VirtualMachine.Interact.PowerOn	仮想マシン > 操作 > 電源オン
VirtualMachine.Interact.Reset	仮想マシン > 操作 > リセット
VirtualMachine.Inventory.CreateFromExisting	仮想マシン > インベントリ > 既存から作成
VirtualMachine.Inventory.Create	仮想マシン > インベントリ > 新規作成
VirtualMachine.Inventory.Delete	仮想マシン > インベントリ > 削除
VirtualMachine.Provisioning.Clone	仮想マシン > プロビジョニング > 仮想マシンのクローン作成

準備済みイメージの共有

準備済みイメージを異なるホスティング接続間で共有するには、ターゲットホスティング接続に対して以下の権限が必須です。

SDK	ユーザーインターフェイス
Datastore.AllocateSpace	データストア > スペースの割り当て
Network.Assign	ネットワーク > ネットワークの割り当て
Resource.AssignVMToPool	リソース > 仮想マシンをリソースプールに割り当てる
VirtualMachine.Config.デバイスの追加または削除	仮想マシン > 構成 > デバイスの追加または削除
VirtualMachine.Config.RemoveDisk	仮想マシン > 構成 > ディスクの削除
VirtualMachine.Config.Settings	仮想マシン > 構成 > 設定の変更
VirtualMachine.Inventory.Register	仮想マシン > インベントリ > 登録
VirtualMachine.Inventory.Delete	仮想マシン > インベントリ > 削除

プロビジョニングされたマシンの削除

SDK	ユーザーインターフェイス
Datastore.Browse	データストア > データストアの参照
Datastore.FileManagement	Datastore > 低レベルファイル操作
VirtualMachine.Config.RemoveDisk	仮想マシン > 構成 > ディスクの削除
VirtualMachine.Interact.PowerOff	仮想マシン > 操作 > 電源オフ
VirtualMachine.Inventory.Delete	仮想マシン > インベントリ > 削除

ストレージプロファイル

vSANまたはvVolデータストアでカタログ作成中にストレージポリシーを表示、作成、または削除するには、次の権限が必要です。

SDK	ユーザーインターフェイス
StorageProfile.Update	プロファイル駆動型ストレージ > プロファイル駆動型ストレージの更新。vSphere 8の場合: VMストレージポリシー > VMストレージポリシーの更新
StorageProfile.View	プロファイル駆動型ストレージ > プロファイル駆動型ストレージの表示。vSphere 8の場合: VMストレージポリシー > VMストレージポリシーの表示

注:

ストレージプロファイルの権限は、**子への伝播**なしで、ルートvCenter Serverレベルで適用します。

タグとカスタム属性

タグとカスタム属性を使用すると、vSphereインベントリで作成されたVMにメタデータを添付でき、これらのオブジェクトの検索とフィルタリングが容易になります。タグまたはカテゴリを作成、編集、割り当て、削除するには、次の権限が必須です。

SDK	ユーザーインターフェイス
InventoryService.Tagging.CreateTag	vSphere タグ付け > vSphere タグの作成
InventoryService.Tagging.CreateCategory	vSphere タグ付け > vSphere タグカテゴリの作成
InventoryService.Tagging.EditTag	vSphere タグ付け > vSphere タグの編集
InventoryService.Tagging.EditCategory	vSphere タグ付け > vSphere タグカテゴリの編集
InventoryService.Tagging.DeleteTag	vSphere タグ付け > vSphere タグの削除
InventoryService.Tagging.DeleteCategory	vSphere タグ付け > vSphere タグカテゴリの削除

SDK	ユーザーインターフェイス
InventoryService.Tagging.AttachTag	vSphere タグ付け > vSphere タグの割り当てまたは割り当て解除
InventoryService.Tagging.ObjectAttachable	vSphere タグ付け > オブジェクトへの vSphere タグの割り当てまたは割り当て解除
Global.ManageCustomFields	グローバル > カスタム属性の管理
Global.SetCustomField	グローバル > カスタム属性の設定

注:

- MCS がマシンカタログを作成すると、ターゲット VM に特別な名前タグを付けます。これらのタグは、マスターイメージを MCS によって作成された VM と区別し、MCS によって作成された VM がイメージ準備に使用されるのを防ぎます。vCenter の `XdProvisioned` 属性の値によって違いを識別できます。MCS が VM を作成する場合、この属性は **True** に設定されます。
- ルート vCenter Server レベルで `InventoryService.Tagging.AttachTag` 権限を、**子への伝播**なしで適用します。

暗号化操作

暗号化操作の特権は、誰がどの種類のオブジェクトに対してどの種類の暗号化操作を実行できるかを制御します。vSphere Native Key Provider は `Cryptographer.*` 特権を使用します。暗号化操作には、以下の最小限の権限が必要です。

注:

これらの権限は、vTPM を搭載した VM を使用して MCS マシンカタログを作成するために必要です。

SDK	ユーザーインターフェイス
Cryptographer.Access	特権 > すべての特権 > 暗号化操作 > 直接アクセス
Cryptographer.AddDisk	特権 > すべての特権 > 暗号化操作 > ディスクの追加
Cryptographer.Clone	特権 > すべての特権 > 暗号化操作 > クローン
Cryptographer.Encrypt	特権 > すべての特権 > 暗号化操作 > 暗号化
Cryptographer.EncryptNew	特権 > すべての特権 > 暗号化操作 > 新規暗号化
Cryptographer.Decrypt	特権 > すべての特権 > 暗号化操作 > 復号化
Cryptographer.Migrate	特権 > すべての特権 > 暗号化操作 > 移行
Cryptographer.ReadKeyServersInfo	特権 > すべての特権 > 暗号化操作 > KMS情報の読み取り

マシンのプロビジョニング (Citrix Provisioning™)

Citrix Provisioningコンソールを介してCitrix Virtual Apps and Desktopsセットアップウィザードおよびデバイスのエクスポートウィザードを使用してVMをプロビジョニングするには、テンプレートをクローンおよび展開するためのこれらの権限が必要です。ホスティング接続の作成時に権限を設定します。マシンのプロビジョニング（Machine Creation Services）のすべての権限と、以下の権限が必要です。

SDK	ユーザーインターフェイス
VirtualMachine.Config.AddRemoveDevice	仮想マシン > 構成 > デバイスの追加または削除
VirtualMachine.Config.CPUCount	仮想マシン > 構成 > CPU数の変更
VirtualMachine.Config.Memory	仮想マシン > 構成 > メモリ
VirtualMachine.Config.Settings	仮想マシン > 構成 > 設定

SDK	ユーザーインターフェイス
VirtualMachine.Provisioning.CloneTemplate	仮想マシン > プロビジョニング > テンプレートのクローン作成
VirtualMachine.Provisioning.DeployTemplate	仮想マシン > プロビジョニング > テンプレートの展開
VApp.Export	vApp > エクスポート

注:

マシンプロファイルを使用してMCSマシンカタログを作成するには、`VApp.Export`が必要です。

証明書を取得してインポートする

vSphere通信を保護するため、Citrix®はHTTPではなくHTTPSを使用することを推奨します。

HTTPSにはデジタル証明書が必要です。組織のセキュリティポリシーに準拠した認証局から発行されたデジタル証明書を使用してください。

認証局から発行されたデジタル証明書を使用できない場合は、VMwareがインストールした自己署名証明書を使用できます。この方法は、組織のセキュリティポリシーで許可されている場合にのみ使用してください。VMware vCenter証明書を各Delivery Controllerに追加します。

1. vCenter Serverを実行しているコンピューターの完全修飾ドメイン名（FQDN）を、そのサーバーのhostsファイル（`%SystemRoot%/WINDOWS/system32/Drivers/etc/`）に追加します。この手順は、vCenter Serverを実行しているコンピューターのFQDNがドメインネームシステムにまだ存在しない場合にのみ必要です。
2. 以下の3つの方法のいずれかを使用してvCenter証明書を取得します。

   vCenterサーバーから。

   a. rui.crt ファイルを vCenter サーバーから Delivery Controllers でアクセス可能な場所にコピーします。

   b. Controller で、エクスポートされた証明書の場所に移動し、rui.crt ファイルを開きます。

Web ブラウザーを使用して証明書をダウンロードします。 Internet Explorer を使用している場合は、Internet Explorer を右クリックし、**管理者として実行**を選択して証明書をダウンロードまたはインストールします。

a. Web ブラウザーを開き、vCenter サーバーへの安全な Web 接続を行います (例: `<https://server1.domain1.com)>`)。
b. セキュリティ警告を受け入れます。
c. 証明書エラーが表示されているアドレスバーをクリックします。
d. 証明書を表示し、 タブをクリックします。
e. プロンプトが表示されたら名前を指定して、**ファイルにコピーして .CER 形式でエクスポート**を選択します。
f. エクスポートされた証明書を保存します。
g. エクスポートされた証明書の場所に移動し、.CER ファイルを開きます。

管理者として実行している Internet Explorer から直接インポートします。

- Web ブラウザーを開き、vCenter サーバーへの安全な Web 接続を行います (例: `<https://server1.domain1.com)>`)。
- セキュリティ警告を受け入れます。
- 証明書エラーが表示されているアドレスバーをクリックします。
- 証明書を表示します。

3. 各Controllerの証明書ストアに証明書をインポートします。

a. **証明書のインストール**オプションをクリックし、**ローカルコンピューター**を選択して、**次へ**をクリックします。
b. **証明書をすべて次のストアに配置する**を選択し、**参照**をクリックします。**信頼されたユーザー**を選択し、**OK**をクリックします。**次へ**をクリックし、**完了**をクリックします。

インストール後にvSphereサーバーの名前を変更した場合は、新しい証明書をインポートする前に、そのサーバーで新しい自己署名証明書を生成する必要があります。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- VMware固有の情報については、「VMwareカタログの作成」を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

VMware クラウドおよびパートナーソリューションへの接続

Azure VMware Solution (AVS) クラスター(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/install-prepare/vmware-cloud-partner-solutions.html#azure-vmware-solution-avs-integration)、Google Cloud VMware Engine(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/install-prepare/vmware-cloud-partner-solutions.html#google-cloud-vmware-engine)、およびVMware Cloud on AWS(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/install-prepare/vmware-cloud-partner-solutions.html#vmware-cloud-on-amazon-web-services-aws)をセットアップした後、接続を作成します。接続の作成については、VMwareへの接続を参照してください。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- VMware固有の情報については、VMwareカタログの作成を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

サービスアカウント

サービスアカウントは、保存された資格情報のコンテナであり、ユーザーの操作なしでマシンID関連の操作を実行するように構成および使用されます。マシンID管理の権限を必要とする操作の前に、サービスアカウントを作成してください。

MCSマシンカタログを構成して、サービスアカウントを次の目的で使用できます。

- Active Directoryでコンピューターアカウントを作成または削除する際に、毎回ドメイン資格情報を入力する必要がありません。
- 古くなったMicrosoft Entra参加済みまたはMicrosoft Intune登録済みデバイスを、Microsoft Entra IDまたはIntuneポータルから手動で削除することなく管理できます。

サポートされているサービスアカウントの種類

Citrix®では、IDプロバイダーの種類に基づいて、以下のサービスアカウントを作成できます。

IDプロバイダーの種類	説明	資格情報
オンプレミスActive Directoryサービスアカウント	マシンカタログとコンピューターアカウントを、毎回ドメイン資格情報を入力することなく管理します。	オンプレミスActive Directoryユーザーアカウントのユーザー名とパスワード。

資格情報の保護

Citrixは、サービスアカウントの資格情報を顧客のサイトデータベースに保存します。Citrix Virtual Apps and Desktops展開では、サイトデータベースはテナント（顧客）ごとのデータベースであり、顧客のために実行されているサービスのみがアクセスできます。

保存された資格情報を保護するために、以下の対策も実施されています。

- 資格情報は、データベースに保存される前に **AES 256** 暗号化を使用して暗号化されます。
- 暗号化キーはサイトごとに生成され、Delivery Controller™ にローカルに保存されます。これは、顧客専用のサービスのみがアクセスできます。
- データベースへの接続は、TLS 1.2 プロトコルを使用して暗号化されます。

オンプレミス Active Directory サービスアカウント

オンプレミス Active Directory サービスアカウントは、特権ドメインユーザーアカウントのユーザー名とパスワードを保存するためのコンテナです。このユーザーアカウントは、Active Directory でコンピューターアカウントを管理するのに十分な権限を持っている必要があります。Machine Creation Service は、このサービスアカウントを使用して、毎回ドメイン資格情報を入力することなく、コンピューターアカウント関連の操作を実行できます。

オンプレミス Active Directory サービスアカウントを作成する

Studio または PowerShell を使用して、オンプレミス Active Directory サービスアカウントを作成します。

前提条件

オンプレミス Active Directory サービスアカウントを作成するには、次のタスクを完了していることを確認してください。

- Active Directory または特定の OU でコンピューターオブジェクトを作成、更新、削除するのに十分な権限を持つドメインユーザーアカウントを Active Directory に作成します。

Web Studio を使用する

1. 左側のペインで、「**管理者**」を選択します。
2. 「**サービスアカウント**」タブで、「**サービスアカウントの作成**」をクリックします。
3. **IDの種類** ページで、**オンプレミス Active Directory** を選択します。**次へ** をクリックします。
4. **資格情報** ページで、**資格情報の入力** をクリックして、サービスアカウントとして使用する特権ドメインユーザーアカウントのユーザー名とパスワードを入力します。
5. パスワードの有効期限を設定するか、期限なしのままにします。
6. このサービスアカウントのスコープを1つ以上選択します。
7. サービスアカウントのフレンドリ名と説明（オプション）を入力します。
8. 「**完了**」をクリックして作成を完了します。

PowerShell を使用する

PowerShellコマンドを使用して、オンプレミスのActive Directoryサービスを作成できます。例：

```
$credential = ConvertTo-SecureString -String $password -AsPlainText -Force

New-AcctServiceAccount -IdentityProviderType ActiveDirectory
-IdentityProviderIdentifier test.local -AccountId test\svcacct_mcs
-AccountSecret $credential -SecretExpiryTime 2030/08/15 -DisplayName
'scvacct_mcs' -Description 'Service account for test.local'
```

注:

`$password`は、指定されたドメインユーザーアカウントの一致するパスワードです。

マシンのID関連のアクションを実行する

Active DirectoryまたはMicrosoft Entraハイブリッドベースの IDプールがサービスアカウントに関連付けられると、ドメイン資格情報を入力することなく、さまざまなマシンのID関連のアクションを実行できます。

- サービスアカウントを使用して新しいIDアカウントを作成するには

```
New-AcctADAccount -IdentityPoolName MyPool -Count 2 -UseServiceAccount
```

- サービスアカウントを使用してIDアカウントを修復するには

```
Repair-AcctADAccount -ADAccountName "Domain\account","Domain\account2"
-UseServiceAccount
```

- サービスアカウントを使用してIDアカウントを削除するには

```
Remove-AcctADAccount -IdentityPoolName MyPool -RemovalOption Delete
-ADAccountName "Domain\account","domain\account2" -UserServiceAccount
```

次のステップ

- オンプレミスのActive Directory参加済みカタログを作成するには、オンプレミスのActive Directory参加済みマシンIDのIDプールを参照してください。
- サービスアカウントを管理するには、「サービスアカウントの管理」を参照してください。

サービスアカウントを管理する

サービスアカウントが健全な状態を保ち、その資格情報が最新であることを確認することは、非常に重要な側面です。この記事では、サービスアカウントの表示、名前変更、編集、テスト、および削除の手順について説明します。

サービスアカウントの詳細を表示する

1. 左側のペインで、「**管理者**」を選択します。
2. **サービスアカウント**タブを選択します。
3. サービスアカウントを選択し、下部パネルでその詳細を表示します。下部パネルで、各サービスアカウントのプロパティ、関連するマシンカタログ、およびトラブルシューティングのヒントを確認します。

次の場合、サービスアカウントの横にエラーまたは警告アイコンが表示されます。

- サービスアカウントが異常な状態である。
- サービスアカウントの資格情報の有効期限が近づいている。

トラブルシューティングタブには、問題の診断と修正に関する情報が記載されています。

> **注:**
>
> 問題を修正した後、サービスアカウントテストを実行してステータスを更新します。詳細については、「サービスアカウントをテストする」を参照してください。

サービスの名前を変更する

1. 左側のペインで、「**管理者**」を選択します。
2. **サービスアカウント**タブを選択します。
3. サービスアカウントを選択し、**名前の変更**をクリックします。

サービスアカウントを編集する

1. 左側のペインで、「**管理者**」を選択します。
2. **サービスアカウント**タブを選択します。
3. サービスアカウントを選択し、**編集**をクリックします。

サービスアカウントをテストする

1. 左側のペインで、「**管理者**」を選択します。
2. **サービスアカウント**タブを選択します。
3. サービスアカウントを選択し、**サービスアカウントのテスト**をクリックします。

- オンプレミスのActive Directoryサービスアカウントの場合、テスト中に資格情報が検証されます。
- Microsoft Entraサービスアカウントの場合、アプリケーションIDとシークレット、および必要な権限がテスト中に検証されます。

推奨事項に従って問題を特定し、修正します。**トラブルシューティング**タブには、問題を診断して修正するための情報が提供されます。問題を修正した後、サービスアカウントをテストします。

サービスアカウントを削除する

サービスアカウントを削除する前に、そのサービスアカウントがどのMCSマシンカタログでも使用されていないことを確認してください。

1. 左側のペインで、「**管理者**」を選択します。
2. **サービスアカウント**タブを選択します。
3. サービスアカウントを選択し、**削除**をクリックします。

イメージ管理

はじめに

MCSカタログの作成または更新プロセスには、次の2つのフェーズがあります。

- マスタリング: ソースイメージが公開イメージに変換されます
- クローニング: 公開イメージから新しいVMが作成されます

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

単一のソースイメージからさまざまなMCSイメージバージョン（準備済みイメージ）を準備し、複数の異なるMCSマシンカタログでそれらを使用できます。また、準備済みイメージバージョンをホスティングユニット間で共有することもできます。この実装により、ストレージと時間のコストが大幅に削減され、VMの展開とイメージの更新プロセスが簡素化されます。

このイメージ管理機能を使用する利点は次のとおりです。

- カタログを作成せずに、準備済みイメージを事前に生成します。
- カタログの作成や更新など、複数のシナリオで準備済みイメージを再利用します。
- カタログの作成または更新時間を大幅に短縮します。
- ホスティングユニット間で準備済みイメージバージョンを共有します。
    - AzureおよびVMwareの場合、イメージバージョンは同じ接続タイプのホスト接続間で共有できます。
    - Amazon WorkSpaces Core Managed Instancesの場合、イメージバージョンは、同じAWSリージョン内または異なるリージョン内の、異なるホスティングユニットに紐付けられた異なるアベイラビリティゾーン間で共有できます。
    - AWS EC2の場合、イメージバージョンは、同じAWSリージョン内の、異なるホスティングユニットに紐付けられた異なるアベイラビリティゾーン間で共有できます。
    - XenServerの場合、イメージバージョンは同じホスト接続内のホスティングユニット間でのみ共有できます。

> **注:**

- この機能は現在、Amazon WorkSpaces Core Managed Instances、Azure Local、AWS EC2、Azure、Red Hat OpenShift、VMware virtualization、およびXenServer環境に適用できます。
- 準備済みイメージを使用せずにMCSマシンカタログを作成できます。その場合、この機能のメリットは得られません。ただし、Amazon WorkSpaces Core Managed Instancesの場合、準備済みイメージバージョンのみを使用してMCSカタログを作成します。マスターイメージを直接使用してカタログを作成することはできません。

ユースケース

イメージ管理機能のユースケースの一部を次に示します。

- *バージョン管理*: イメージバージョンを使用すると、次のことができます。
  - 特定のイメージに対する異なるイテレーションや更新を管理する。
  - 異なる目的のためにイメージの複数のバージョンを維持する。
- *論理的なグループ化*: 複数のイメージ定義を作成して、次のことを行えます。
  - プロジェクト、部門、アプリケーション、デスクトップの種類など、さまざまな基準に基づいてイメージのバージョンを論理的にグループ化する。
  - 組織内でイメージをより効率的に管理する。
- *イメージの共有*: 同じ接続タイプのホスト接続内のホスティングユニット間で、準備されたイメージのバージョンを共有して、次のことを行えます。
  - 異なるホスティングユニット間でイメージの一貫性と均一性を確保する。

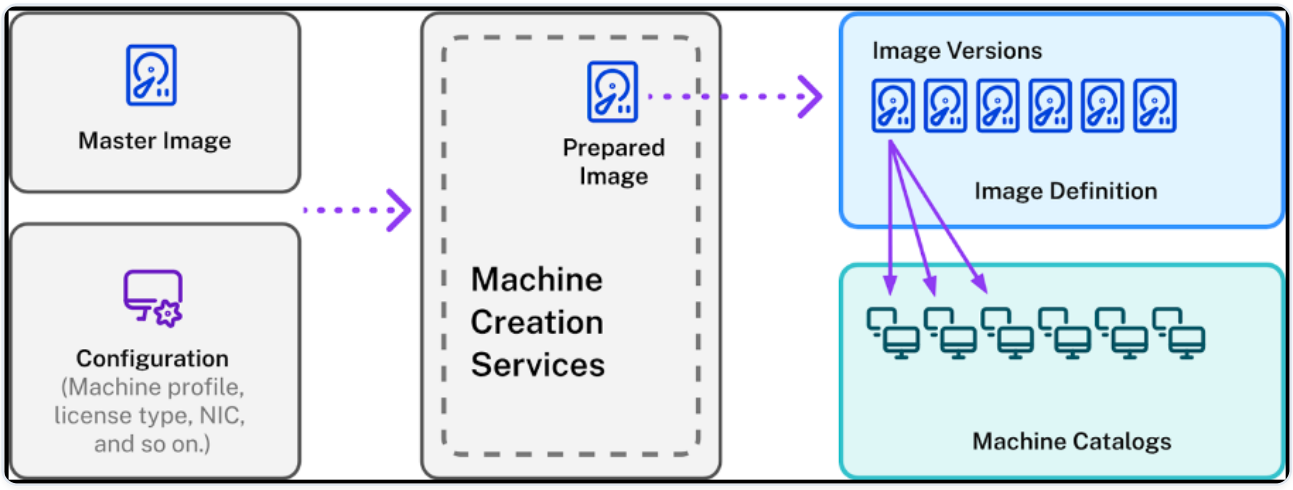
準備されたイメージとは何ですか?

イメージ管理機能により、MCSはマスタリングフェーズをカタログ作成または更新の全体的なワークフローから切り離し、プロセスを2つの段階に分けます。

1. 単一のソースイメージから準備されたイメージを作成する。
2. 準備されたイメージを使用して、MCSマシンカタログを作成または更新する。

準備されたイメージは事前に作成できます。単一の準備されたイメージを使用して、複数のMCSプロビジョニング済みマシンカタログを作成または更新できます。

イメージからWeb Studioを使用する場合に、準備されたイメージが複数のMCSマシンカタログでどのように使用されるかを理解してください。



イメージ定義: イメージ定義は、イメージのバージョンの論理的なグループ化です。イメージ定義には、次の情報が含まれます。

- イメージが作成された理由
- どのOS用であるか
- イメージの使用に関するその他の情報。

カタログはイメージ定義から作成されるのではなく、イメージ定義に基づいて作成されたイメージバージョンから作成されます。

イメージバージョン: イメージバージョンは、イメージ定義のバージョン管理を行います。イメージ定義には複数のイメージバージョンを含めることができます。イメージバージョンを準備済みイメージとして使用して、カタログを作成または更新します。

- AzureおよびVMwareの場合、イメージバージョンは同じ接続タイプのホスト接続間で共有できます。
- Amazon WorkSpaces Core Managed Instancesの場合、イメージバージョンは、同じAWSリージョン内または異なるリージョン内の、異なるホスティングユニットに紐付けられた異なるアベイラビリティゾーン間で共有できます。
- AWS EC2の場合、イメージバージョンは、同じAWSリージョン内の異なるアベイラビリティゾーン間で共有でき、異なるホスティングユニットに紐付けられます。
- XenServerの場合、イメージバージョンは、同じホスト接続内のホスティングユニット間でのみ共有できます。

または、PowerShellコマンドを使用してプロビジョニングスキームを作成し、カタログを作成または更新する場合は、環境の必要に応じて、マスターイメージバージョンスペックに基づいて準備済みイメージバージョンスペックを作成する必要があります。

- AzureおよびVMwareの場合、イメージバージョンは同じ接続タイプのホスト接続間で共有できます。
- Amazon WorkSpaces Core Managed Instancesの場合、イメージバージョンは、同じAWSリージョン内または異なるリージョン内の、異なるホスティングユニットに紐付けられた異なるアベイラビリティゾーン間で共有できます。
- AWS EC2の場合、イメージバージョンは、同じAWSリージョン内の異なるアベイラビリティゾーン間で共有でき、異なるホスティングユニットに紐付けられます。
- XenServerの場合、イメージバージョンは、同じホスト接続内のホスティングユニット間でのみ共有できます。

要件

- Windowsマスターイメージの場合、VDAイメージバージョン2311以降のみがサポートされます。MCS/IOコンポーネントは明示的に選択してインストールする必要があります。MCS I/O構成の有効化または無効化は、デフォルトでは有効になっていないため、マシンカタログの作成または更新時に決定する必要があります。

制限事項

現在、この機能は以下をサポートしていません。

- Azureでの複数のNIC
- 永続データディスク機能
- マルチセッションの休止状態
- イメージタイプの変更
- Azureのホスティングユニット間で準備済みイメージバージョンを共有する場合、以下の共有方法は許可されていません。
  - 直接共有
  - パブリックコミュニティギャラリーへの共有

Web Studioを使用したイメージライフサイクル管理

Web Studioを使用する場合のイメージのライフサイクルは次のとおりです。

1. 準備済みイメージの作成: イメージ定義とその初期イメージバージョンを作成します。
2. 初期イメージバージョンからイメージバージョンを作成します。
3. 必要に応じて、仮想化環境のホスティングユニットとイメージバージョンを共有します。

4. イメージバージョンを準備済みイメージとして使用してカタログを作成します。
5. 別の準備済みイメージでマシンカタログを更新します。
6. イメージ定義とバージョンを管理する: イメージバージョンの名前と説明、およびイメージ定義の説明を編集します。
7. イメージバージョンを削除します。
8. イメージ定義を削除します。

または、PowerShell を使用してイメージを管理することもできます。PowerShell を使用したイメージライフサイクル管理を参照してください。

PowerShell を使用したイメージのライフサイクル管理

PowerShell コマンドを使用してプロビジョニングスキームを作成する場合は、環境の必要に応じて、マスターイメージバージョン仕様に基づいて準備済みイメージバージョン仕様を作成する必要があります。

マスターイメージバージョン仕様: マスターイメージバージョン仕様は、イメージバージョン下に追加または作成された特定のイメージです。ハイパーバイザー内の既存のイメージをマスターイメージバージョン仕様として追加したり、環境の必要に応じてマスターイメージバージョン仕様に基づいて準備済みイメージバージョン仕様を作成したりできます。準備済みイメージバージョン仕様は、複数のプロビジョニングスキームに使用できます。

仮想化環境に応じて、ホスティングユニット間でイメージバージョン仕様を共有できます。

- Azure、VMware、および Amazon WorkSpaces Core Managed Instances 環境では、同じ接続タイプで同じホスト接続または異なるホスト接続にあるかどうかにかかわらず、ホスティングユニット間でイメージバージョン仕様を共有できます。Azure では、Azure Compute Gallery (ACG) のディスク共有機能を使用して共有が実現されます。
- AWS EC2 の場合、イメージバージョンは、同じ AWS リージョン内で、異なるホスティングユニットに紐付けられた異なるアベイラビリティゾーン間で共有できます。
- XenServer では、同じホスト接続内のホスティングユニット間でのみイメージバージョン仕様を共有できます。

PowerShellコマンドを使用する場合のイメージのライフサイクルは次のとおりです。

1. イメージを作成する:
    a. イメージ定義を作成します。
    b. 指定されたホスティング接続にイメージ定義の新しい構成を追加します。

c. イメージバージョンを作成します。

d. マスターイメージバージョンスペックを追加します。

e. 準備済みイメージバージョンスペックを作成します。

2. 必要に応じて、同じホスティング接続内であるかどうかにかかわらず、仮想化環境内の別のホスティングユニットとイメージバージョンスペックを共有します。
3. 準備済みイメージバージョンスペックを使用してMCSマシンカタログを作成する:

a. ブローカーカタログを作成します。

b. ID プールを作成します。

c. `New-ProvScheme` コマンドを使用して、準備済みイメージバージョンスペックUidのパラメーターを持つプロビジョニングスキームを作成します。

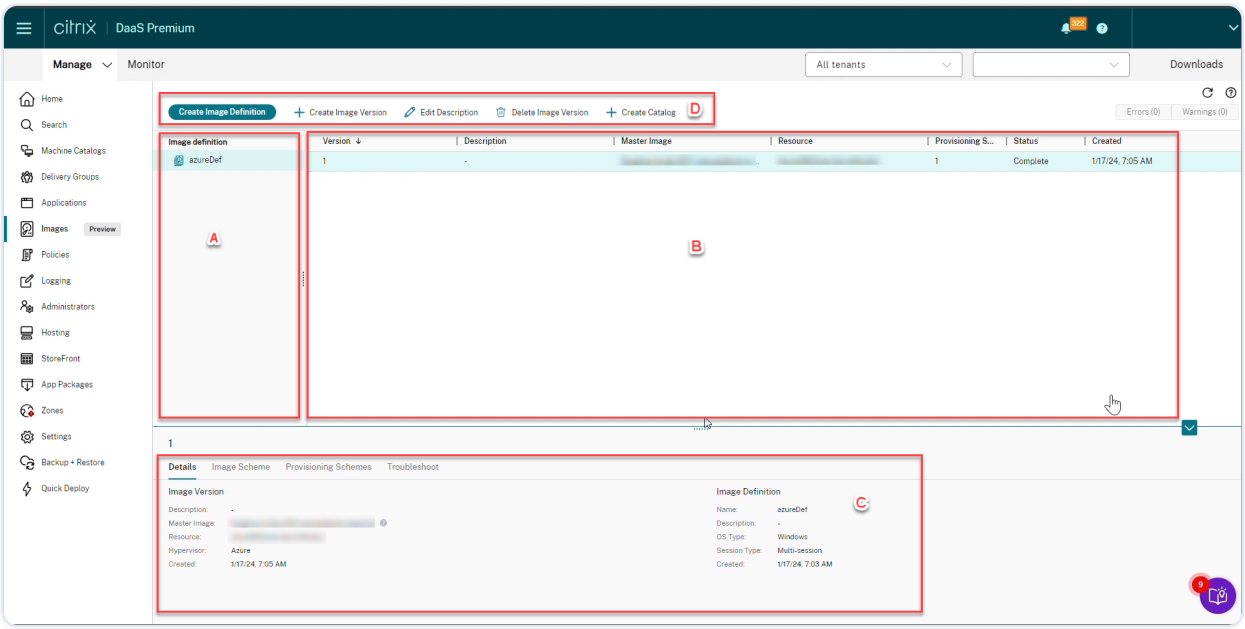
d. ブローカーカタログをプロビジョニングスキームにリンクします。

4. MCSマシンカタログにVMを作成します。
5. `Set-ProvScheme` コマンドを使用して、プロビジョニングスキームの準備済みイメージバージョンスペックを変更します。
6. イメージ定義とバージョンを管理する: イメージバージョンとイメージ定義を編集します。
7. MCSマシンカタログを削除する: 削除順序は、マシンカタログ > 共有準備済みイメージバージョン仕様 (イメージ共有の場合) > 準備済みイメージバージョン仕様 > マスターイメージバージョン仕様 > イメージバージョン > 指定されたホスティング接続内のイメージ定義の構成 > イメージ定義です。イメージバージョン仕様を削除する前に、準備済みイメージバージョン仕様がどのMCSマシンカタログとも関連付けられていないことを確認してください。

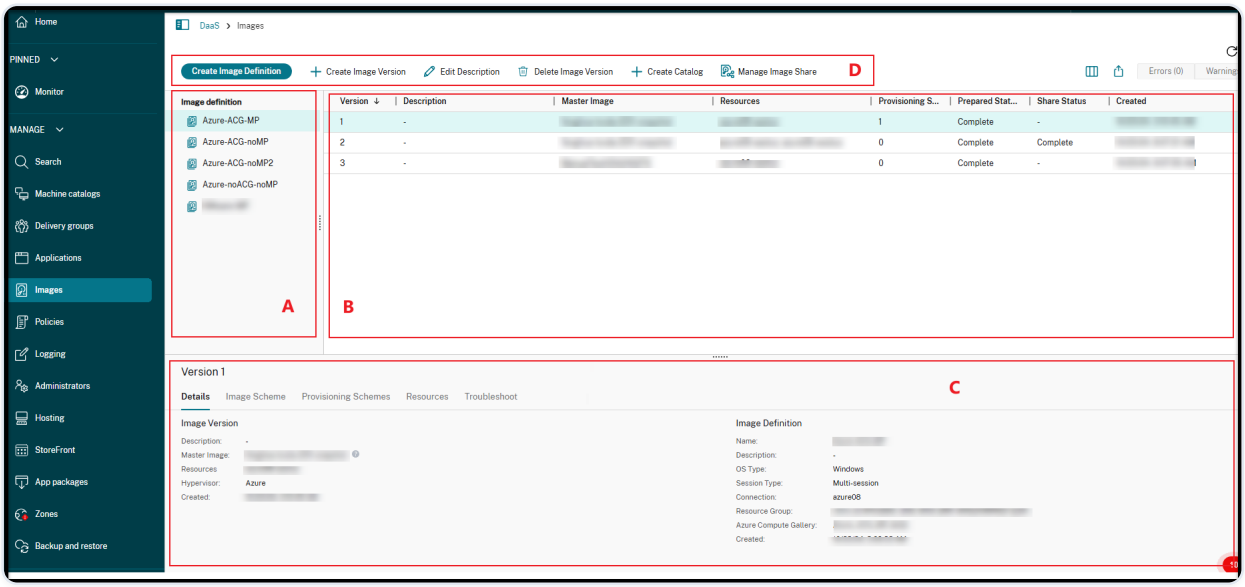
イメージノードについて

イメージノードを使用して、MCSで準備されたイメージを作成および管理します。そのメインビューは4つの部分に分かれています。

- ホストユニット間で準備済みイメージが共有されていない場合



- ホストユニット間で準備済みイメージが共有されている場合:



ラベル	部分	説明
A	イメージ定義	以前に作成されたイメージ定義を一覧表示します。
B	イメージバージョン	選択したイメージ定義のイメージバージョンを表示します。

ラベル	部分	説明
C	詳細	• **詳細**タブには、選択したイメージ定義またはバージョンに関する詳細情報（マスターイメージ、リソース、ハイパーバイザー、イメージ定義の名前、OSタイプ、セッションタイプなど）が表示されます。 • 「**イメージスキーム**」タブには、ハードディスク、マシンサイズ、ライセンスの種類、ディスク暗号化セット、マシンプロファイルなど、イメージの準備に使用されるテンプレートに関する情報が表示されます。 • 「**プロビジョニングスキーム**」タブには、カタログの作成に使用されるプロビジョニングス

ラベル	部分	説明	
		キーム名が表示されます。 • 「**トラブルシューティング**」タブには、選択したイメージバージョンのエラー状態が表示されます。 • イメージ共有の場合：「**リソース**」タブには、イメージバージョンの共有ステータスが表示されます。	
D	アクションバー	**イメージバージョンの作成**、**説明の編集**、**イメージ共有の管理**（準備済みイメージ共有の場合）、**イメージバージョンの削除**、**カタログの作成**など、イメージ定義とバージョンに対して実行できるアクションを一覧表示します。	

Azureサブスクリプションまたはテナント間で準備済みイメージを共有する

Azureプラットフォームでサブスクリプションまたはテナント間で準備済みイメージを共有するには、次の例に従ってください：

- **サービスプリンシパル**：SPN 1

- **サブスクリプション**: Subscription 1
- **テナント**: Tenant 1

このイメージを以下と共有したいとします。

- **サービスプリンシパル**: SPN 2
- **サブスクリプション**: Subscription 2
- **テナント**: Tenant 2 (Tenant 1 と同じでも可)

イメージを正常に共有して使用するには、**Subscription 1** のギャラリー、リソースグループ、またはサブスクリプションのスコープで、SPN 2 に次の権限を付与する必要があります:

- `Microsoft.Resources/subscriptions/read`
- `Microsoft.Compute/galleries/images/read`
- `Microsoft.Compute/galleries/images/versions/read`

> **注:**
>
> サブスクリプションまたはリソースに対して何らかの権限を持つサービスプリンシパルはすべて、`Microsoft.Resources/subscriptions/read` 権限を自動的に継承します。

または、**SPN 2** に組み込みロールの **Compute Gallery Image Reader** を割り当てます。

詳細な手順については、この Microsoft の記事 を参照してください。

次のステップ

- 準備済みイメージのマシンカタログを作成する
  - Amazon WorkSpaces Coreマネージドインスタンス用の準備済みイメージを作成する
  - Amazon WorkSpaces Core マネージドインスタンスのカタログを作成する(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/create-catalog-amazon-wsc.html)
  - Azureで準備済みイメージのマシンカタログを作成する
  - VMwareで準備済みイメージのマシンカタログを作成する
  - Red Hat OpenShiftで準備済みイメージのマシンカタログを作成する

    - XenServerで準備済みイメージマシンカタログを作成する(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/create-prepared-image-machine-catalogs-xenserver.html)

準備済みイメージのマシンカタログを作成する

準備済みイメージを作成し、その準備済みイメージを使用して、次の方法でMCSマシンカタログを作成します。

- ウェブスタジオ
- PowerShellコマンド

現在、Amazon WorkSpaces Core Managed Instances、Azure、Red Hat OpenShift、VMware、およびXenServer®仮想化環境で、準備済みイメージマシンカタログを作成できます。

詳細情報

- イメージ管理

次のステップ

- Amazon WorkSpaces Coreで準備済みイメージを作成するおよびAmazon WorkSpaces Coreカタログを作成する
- Azureで準備済みイメージのマシンカタログを作成する
- VMwareで準備済みイメージのマシンカタログを作成する
- Red Hat OpenShiftで準備済みイメージのマシンカタログを作成する
- XenServerで準備済みイメージマシンカタログを作成する(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/create-prepared-image-machine-catalogs-xenserver.html)
- 準備済みイメージマシンカタログを管理する(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/manage-prepared-image-machine-catalogs.html)

Amazon WorkSpaces Core マネージドインスタンス用の準備済みイメージを作成する

MCS マシンカタログを作成するために、準備済みイメージを作成します。準備済みイメージは、次の方法で作成できます。

- ウェブスタジオ
- (#use-powershell)

主な手順

1. イメージ定義と初期イメージバージョンを作成します。
2. 初期イメージバージョンからイメージバージョンを作成します。

Web Studio を使用する

イメージ定義と初期イメージバージョンを作成する

イメージ定義と初期イメージバージョンを作成するには、次の手順を実行します。

1. Web Studio から、**Images** ノードに移動し、**Create Image Definition** をクリックします。**Introduction** ページで **Next** をクリックします。
2. **イメージ定義**ページで、イメージ定義の**OSタイプ**と**セッションタイプ**を指定します。
3. **イメージ**ページで、**リソース**（設定された接続に適用可能なリソースのみが一覧表示されます）、イメージバージョン作成のテンプレートとして使用するマスターイメージ、およびハードウェアプロパティをキャプチャするためのマシンプロファイルを選択します。VMインスタンスまたは起動テンプレートバージョンからハードウェアプロパティをキャプチャするためのマシンプロファイルを選択します。

   注:

   - イメージを選択する前に、マスターイメージにVDA 2311以降がインストールされており、MCSIOドライバーがVDAにインストールされていることを確認してください。
   - Instance Metadata Service (IMDS) V2 のみがサポートされており、IMDS V1 はサポートされていません。詳細については、「How Instance Metadata Service Version 2 works」を参照してください。

4. 「**Machine Specification**」ページで、マシンサイズを選択します。マシンプロファイル（「**Image**」ページで選択）のマシンサイズがデフォルトで選択されています。
5. 「**NICs**」ページで、準備イメージ用のNICを選択または追加します。各NICについて、関連するVPCサブネットを選択します。
6. 「**Version Description**」ページで、作成された初期イメージバージョンの説明を入力します。
7. 「**概要**」ページで、イメージ定義と作成された初期イメージバージョンの詳細を確認します。イメージ定義の名前と説明を入力します。「**完了**」をクリックします。

イメージバージョンを作成する

イメージバージョンを使用すると、特定のイメージに対するさまざまなイテレーションや更新を管理できます。この機能により、さまざまな目的のためにイメージの複数のバージョンを維持できます。

初期イメージバージョンからイメージバージョンを作成するには、次の手順を実行します。

> **注:**
>
> すべてのイメージバージョンのホスティングユニットは同じである必要があります。

1. 「**Images**」ノードに移動し、イメージバージョンまたはイメージ定義を選択して、「**Create Image Version**」をクリックします。
2. 「**Image definition**」ページで、ホスティングユニットを変更し、そのイメージバージョンのマスターイメージとマシンプロファイルを再選択できます。
3. イメージバージョンの構成を初期構成イメージバージョンと異なるものにする場合は、「**Create Image Version**」ダイアログの「**Machine Specification**」ページと「**NICs**」ページで設定を構成します。
4. イメージバージョンの説明を追加します。「**Finish**」をクリックします。

> **注:**
>
> 何らかの理由でイメージバージョンの作成に失敗した場合、下部にある**トラブルシューティング**タブに**再試行**オプションが表示されます。

PowerShell を使用する

準備済みイメージバージョン仕様を作成するための詳細な PowerShell コマンドは次のとおりです。

1. `Test-ProvImageDefinitionNameAvailable command` を使用して、利用可能なイメージ定義名を確認します。例:

   ```
   Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string[]>
   ```

2. `New-ProvImageDefinition` コマンドを使用してイメージ定義を作成します。例:

```
New-ProvImageDefinition -ImageDefinitionName image1 -OsType Windows
-VdaSessionSupport MultiSession
```

3. `Add-ProvImageDefinitionConnection` コマンドを使用して、指定されたホスティング接続でイメージ定義の新しい構成を作成します。

```
Add-ProvImageDefinitionConnection -ImageDefinitionName image1
-HypervisorConnectionName test-conn
```

4. `New-ProvImageVersion` コマンドを使用してイメージバージョンを作成します。例:

```
New-ProvImageVersion -ImageDefinitionName image1 -Description "version
1"
```

5. `Add-ProvImageVersionSpec` コマンドを使用して、マスターイメージバージョン仕様をイメージバージョンに追加します。例:

```
Add-ProvImageVersionSpec -ImageDefinitionName  image1  -
ImageVersionNumber  1 -HostingUnitName wsc -MasterImagePath "XDHyp:
\HostingUnits\wsc\win10-2411-ami (ami-00123456789abcdef).template”"
```

> **注:**
>
> ホスティングユニットのイメージバージョンには、マスターイメージバージョン仕様を1つだけ追加できます。

6. `New-ProvImageVersionSpec` コマンドを使用して、マスターイメージバージョン仕様から準備済みイメージバージョン仕様を作成します。`SourceImageVersionSpecUid` パラメーターは `Add-ProvImageVersionSpec` コマンドから派生します。例:

```
New-ProvImageVersionSpec

-SourceImageVersionSpecUid  00000000-0000-0000-0000-00000000000

-MachineProfile 'XDHyp:\HostingUnits\wsc\w2022-2411
```

```
(lt-00123456789abcdef).launchtemplate\lt-00123456789abcdef
(1).launchtemplateversion' -RunAsynchronously
```

イメージ定義、イメージバージョン、および準備済みイメージバージョン仕様を作成するための PowerShell コマンドの完全なセットの例:

```
New-ProvImageDefinition -ImageDefinitionName image1 -OsType Windows
-VdaSessionSupport MultiSession




Add-ProvImageDefinitionConnection -ImageDefinitionName image1
-HypervisorConnectionName wsc -CustomProperties $CustomProperties



$imageVersion = New-ProvImageVersion -ImageDefinitionName image1
-Description "version 1"



$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid `

    -HostingUnitUid $hostingunit.HostingUnitUid `

    -MasterImagePath "XDHyp:\HostingUnits\wsc\win10-2411-ami
(ami-00123456789abcdef).template”



New-ProvImageVersionSpec -MachineProfile 'XDHyp:
\HostingUnits\wsc\w2022-2411
(lt-00123456789abcdef).launchtemplate\lt-00123456789abcdef
(1).launchtemplateversion' -SourceImageVersionSpecUid
$SourceImageVersionSpec.ImageVersionSpecUid

Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid
00000000-0000-0000-0000-00000000000-HostingUnitName wsc

$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageVersionUid
```

```
$imageVersion.ImageVersionUid | Where SourceImageVersionSpecUid-eq
$SourceImageVersionSpec.ImageVersionSpecUid
```

注:

- イメージ定義内のすべてのイメージバージョン仕様は、同じホスティングユニットに属している必要があります。
- イメージバージョンには、マスターイメージバージョン仕様を1つ、準備済みイメージバージョン仕様を1つだけ含めることができます。
- すべてのイメージバージョン仕様には、マシンプロファイルが必要です。

準備済みイメージをアベイラビリティゾーンとリージョン間で共有する

Amazon WorkSpaces Core マネージドインスタンスの場合、同じ AWS リージョン内または異なるリージョン内の異なるホスティングユニットに紐付けられた、異なるアベイラビリティゾーン間で単一の準備済みイメージを共有できるようになりました。これにより、1つの準備済みイメージを使用して、さまざまなアベイラビリティゾーンおよびリージョンでMCSマシンカタログを作成および更新できます。異なるリージョン内の異なるAZ間で共有する場合、準備済みイメージのバージョンは元のリージョンから宛先リージョンにコピーされます。

単一の準備済みイメージを維持し、それを使用して、異なるホスティングユニットに紐付けられた複数のアベイラビリティゾーンとリージョン間でマシンカタログを作成および更新できます。これにより、イメージ管理のオーバーヘッドが大幅に削減され、展開全体の一貫性が確保され、プロビジョニングプロセスが合理化されます。また、既存のマシンカタログを、異なるアベイラビリティゾーンまたはリージョンからの準備済みイメージでシームレスに更新することもできます。

ユースケース

- **集中型イメージ管理:** 1つのアベイラビリティゾーン（例: `us-east-1a`）で準備済みイメージを作成します。その後、このイメージを同じ`us-east-1` AWSリージョン内の`us-east-1b`のような他のアベイラビリティゾーン、または異なる`us-west-1`リージョン内の`us-west-1a`に共有できます。これにより、単一のイメージで複数のホスティングユニットに対応でき、メンテナンスが簡素化されます。
- **効率的なカタログの作成と更新:** `AZ 1`で作成された準備済みイメージ（例: `us-east-1a`）を使用して、`AZ 1`に新しいカタログを作成できます。このイメージを`AZ 2`（例: `us-east-1b`）に共有した後、`AZ 2`の共有イメージを使用して、`AZ 2`にカタログを作成および更新できます。

- **クロスホスティングユニットおよびホスティング接続の展開:** 環境に同じまたは異なるAWSリージョンおよびAWSアカウントの下に複数のホスティングユニットがある場合、これらのホスティングユニット間で準備済みイメージを効率的に共有できます。

制限事項

- **同じAWSアカウント内での共有:** 現在の実装では、異なるAWSアカウント間での共有はできません。

重要な考慮事項

- **削除順序:** 元の準備済みイメージバージョン仕様を削除するには、まずその共有イメージバージョン仕様をすべて削除する必要があります。または、元の仕様と共有仕様を同時に削除する必要があります。
- **カタログのバックポート可能性:** この機能が導入される前に展開した既存のマシンカタログを更新できます。カタログを最初に展開した場所とは異なるアベイラビリティゾーンまたはリージョンで作成した準備済みイメージを使用します。
- **完全な削除:** 準備済みイメージを削除すると、共有または最初に作成したどのアベイラビリティゾーンでも使用できなくなります。さらに、準備済みイメージバージョンに紐付けられているすべてのカタログが最初に削除されるまで、準備済みイメージバージョンを削除することはできません。

前提条件

この機能を構成または使用する前に、以下の条件を満たしていることを確認してください。

- お使いの環境は、Amazon WorkSpaces Core Managed Instances環境である必要があります。
- 同じAWSアカウントで、複数のホスティングユニット（それぞれ異なるアベイラビリティゾーンに紐付け可能）とホスト接続（それぞれ異なるリージョンに紐付け可能）を構成する必要があります。

Web Studio UI を使用して構成する

Web Studio UI を使用して、異なるホスティングユニットに紐付けられたアベイラビリティゾーン間で準備済みイメージを共有できます。

準備済みイメージを共有するには

1. Web Studio の **Images** ノードに移動し、他のアベイラビリティゾーンと共有したい準備済みイメージのバージョンを選択します。
2. 上部のナビゲーションバーで**イメージ共有の管理**を選択し、選択したイメージバージョンのイメージ共有を管理します。

3. **Manage Image Share** ページで、イメージバージョンを共有したいリソースを1つ以上選択します。リソースは、元のイメージバージョンとは異なるアベイラビリティゾーンに存在できます。
4. **保存**をクリックして、他のアベイラビリティゾーンのリソースでイメージバージョンを共有します。イメージバージョンは、選択した異なるリソース間で共有されるように更新されます。完了したら、イメージバージョンが共有されているアベイラビリティゾーンでカタログを作成するために、そのイメージバージョンを使用します。

準備済みイメージの共有を削除するには

1. Web Studio の **Images** ノードで、共有を解除したい準備済みイメージのバージョンを選択します。
2. 上部のナビゲーションバーで**イメージ共有の管理**を選択し、選択したイメージバージョンのイメージ共有を管理します。
3. イメージバージョンの共有を停止したい1つ以上のリソース（アベイラビリティゾーン）のチェックボックスをオフにします。

> **注:**
>
> 共有イメージバージョンに関連付けられ、そこから作成されたカタログが、リソースに存在しないようにする必要があります。削除する共有イメージバージョンから作成されたカタログは、まず削除する必要があります。

4. 「**保存**」をクリックして、クリアされたアベイラビリティゾーン全体でのリソースの共有を削除します。イメージバージョンが更新され、それらのアベイラビリティゾーンでは共有されなくなります。

PowerShell を使用して構成する

または、PowerShell コマンドを使用して、異なるホスティングユニットに紐付けられたアベイラビリティゾーン間で準備されたイメージを共有できます。

準備済みイメージを共有するには

1. 共有する準備されたイメージの `ImageVersionSpecUid` を持っていることを確認します。これは、PowerShell で `Get-ProvImageVersionSpec` または同様の `Get-` コマンドを使用して取得できます。

2. 準備されたイメージを利用可能にするアベイラビリティゾーン (同じリージョンでも異なるリージョンでもかまいません) の `HostingUnitName` を特定します。これは、その特定のアベイラビリティゾーン用に構成したホスティングユニットの名前です。
3. 「**`Add-ProvImageVersionSpecHostingUnit` コマンドを実行します:**」次の PowerShell コマンドを使用します。`<ImageVersionSpecUid>` をイメージの Uid に、`<targetHostingUnitName>` を、イメージバージョン仕様を共有するターゲットアベイラビリティゾーンのホスティングユニット名に置き換えます。

```
Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid
<ImageVersionSpecUid> -HostingUnitName <targetHostingUnitName>
```

4. 実行が成功すると、Web Studio UI でイメージのステータスが表示され、指定されたホスティングユニットと共有されたことが示されます。

準備済みイメージの共有を削除するには

1. 共有を削除したい準備されたイメージの `ImageVersionSpecUid` を持っていることを確認します。
2. 共有イメージを削除したいアベイラビリティゾーンの `HostingUnitName` を特定します。
3. 「**`Remove-ProvImageVersionSpecHostingUnit` コマンドを実行します:**」次の PowerShell コマンドを使用します。`<ImageVersionSpecUid>` をイメージの Uid に、`<targetHostingUnitName>` を、イメージバージョン仕様の共有を削除するターゲットアベイラビリティゾーンのホスティングユニット名に置き換えます。

```
Remove-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid
<ImageVersionSpecUid> -HostingUnitName <targetHostingUnitName>
```

次のステップ

- Amazon WorkSpaces Core マネージドインスタンスのカタログを作成するには、Amazon WorkSpaces Core マネージドインスタンスのカタログを作成するを参照してください。

詳細情報

- イメージ管理
- Amazon WorkSpaces Core の GitHub PowerShell の例については、citrix-mcs-sdk-samples-Amazon WorkSpaces Coreを参照してください。

Amazon WorkSpaces Core Managed Instances のカタログを作成する

(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/machine-catalogs-create.html)では、マシンカタログを作成するウィザードについて説明します。以下の情報では、Amazon WorkSpaces Core Managed Instances に固有の詳細について説明します。

> **注:**
>
> 現在、永続VMと非永続VMの両方のカタログ作成（`CleanOnBoot`プロパティが`True`または`False`の場合）がサポートされています。

前提条件

Amazon WorkSpaces Core Managed Instancesのカタログを作成する前に、以下を作成しておく必要があります。

1. Amazon WorkSpaces Core Managed Instancesへの接続。「Amazon WorkSpaces Core Managed Instancesへの接続」を参照してください(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/connections/connection-amazon-wsc.html)。
2. 準備されたイメージ。詳細については、Amazon WorkSpaces Core Managed Instances 用の準備されたイメージを作成するを参照してください。

イメージ準備中のネットワーク設定

イメージ準備中、元のVMに基づいて準備用仮想マシン（VM）が作成されます。この準備用VMはネットワークから切断されます。準備用VMからネットワークを切断するために、すべてのインバウンドおよびアウトバウンドトラフィックを拒否するネットワークセキュリティグループが作成されます。このネットワークセキュリティグループは永続的であり、再利用されます。ネットワークセキュリティグループの名前は`Citrix.XenDesktop.IsolationGroup-GUID`で、GUIDはランダムに生成されます。

マシンプロファイルベースのマシンカタログ

マシンプロファイルを使用して、EC2インスタンス（VM）または起動テンプレートバージョンからハードウェアプロパティをキャプチャし、プロビジョニングされたマシンに適用できます。キャプチャされるプロパティには、たとえば、テナンシータイプ、インスタンスタイプ、セキュリティグループ、ネットワークマッピング、EBSボリュームプロパティ、EBS最適化、CPUオプション、ハイバネーション機能、およびその他のサポートされているAWS構成が含まれます。

マシンプロファイルの入力として、AWS EC2インスタンス（VM）またはAWS起動テンプレートバージョンを使用できます。

注:

- EBSボリュームプロパティは、マシンプロファイルからのみ派生します。
- Instance Metadata Service (IMDS) V2 のみがサポートされており、IMDS V1 はサポートされていません。詳細については、「How Instance Metadata Service Version 2 works」を参照してください。

AWS テナンシー

AWS は、共有テナンシー（デフォルトタイプ）と専用テナンシーの2つのテナンシーオプションを提供しています。共有テナンシーとは、異なる顧客の複数の Amazon WorkSpaces Core インスタンスが同じ物理ハードウェア上に存在する可能性があることを意味します。専用テナンシーとは、Amazon WorkSpaces Core インスタンスが、デプロイした他のインスタンスと同じハードウェア上でのみ実行されることを意味します。

注:

専用インスタンスのみがサポートされています（専用ホストは現在サポートされていません）。他の顧客は同じハードウェアを使用しません。

テナンシータイプはマシンプロファイルから取得されます

MCS を使用して AWS でマシンをプロビジョニングするためのカタログを作成すると、テナンシータイプはマシンプロファイルから取得されます。

- **共有ハードウェア**：この設定は、ほとんどのデプロイに適しています。複数の顧客が互いにやり取りすることなくハードウェアを共有します。共有ハードウェアを使用することは、Amazon EC2 インスタンスを実行するための最も安価なオプションです。
- **専用インスタンス**：この設定は、特定のセキュリティまたはコンプライアンス要件を持つデプロイにより適しています。専用インスタンスを使用すると、他の AWS 顧客とは別のホストを持つという利点を享受できますが、ホスト全体に対して料金を支払う必要はありません。ホストの容量について心配する必要はありませんが、インスタンスの料金は高くなります。さらに、専用インスタンスは、Bring Your Own License (BYOL) のサポートが限定的です。

柔軟な課金

Amazon WorkSpaces Core マネージドインスタンスは、次の2つの課金モードをサポートしています。

課金モード	説明
月額	固定の月額定額課金。永続的なデスクトップや予測可能なワークロードに最適です。
時間単位	従量課金制。これは、課金モードが明示的に指定されていない場合のAWSのデフォルト設定です。

これらのオプションは、ワークロードの永続性と使用パターンに基づいてコンピューティングコストを管理するための柔軟性を提供します。

この機能を使用するには、Amazon WorkSpaces課金サービスを使用する必要があります。デフォルトでは、MCSはこのサービスを使用してインスタンスをプロビジョニングおよび管理し、永続的なワークロードに対してより競争力のある定額料金の恩恵を受けられるようにします。

前提条件と考慮事項

- AWSアカウントの構成: AWSアカウントは、WorkSpaces課金サービスを使用するように構成されている必要があります。AWSアカウントはデフォルトで切り替えられますが、一部のお客様は、WorkSpaces Coreマネージドインスタンスを使用するために、AWSにレガシーEC2課金サービスを維持するよう要求する場合があります。

  > **注:**
  >
  > アカウントがレガシーEC2課金サービスを使用している場合、**月額**課金オプションは利用できません。

- ホスト接続: 柔軟な課金は、Amazon WorkSpaces Coreホスト接続にのみ適用されます。標準のAWS EC2ホスト接続ではサポートされていません。
- スポットインスタンス: スポットインスタンスは、WorkSpaces課金サービスではサポートされていません。

- 混合課金: AWSアカウントは、コアマネージドインスタンスに対してWorkSpaces課金またはEC2課金のいずれかを使用する必要があります。単一アカウント内で両方を混在させることはサポートされていません。
- 互換性: 特定のインスタンスタイプ、プラットフォームタイプ（OS）、およびテナンシータイプのみが特定の課金モードと互換性があります。MCSは、選択内容（サービスオファリング、マシンプロファイル、準備済みイメージ）が選択した課金モードと一致することを確認するために、事前チェックを実行します。

「特定の課金モードでマシンカタログを作成する」を参照してください。

カタログを作成する

Amazon WorkSpaces Coreマネージドインスタンスのカタログを作成するには、準備済みイメージとマシンプロファイルが必要です。マシンプロファイルの入力として、AWS VMインスタンスまたはAWS起動テンプレートバージョンを使用できます。

カタログは以下を使用して作成できます。

- ウェブスタジオ
- PowerShell

Web Studioを使用してカタログを作成する

「イメージ」ノードからマシンカタログを作成する

「**イメージ**」ノードの「**カタログの作成**」オプションを使用して、イメージバージョンでカタログを作成します。

または、「**マシンカタログ**」ノードでカタログを作成する際にバージョンを選択し、カタログ作成ワークフローで準備されたイメージオプションにリンクすることもできます。「マシンカタログ」ノードからマシンカタログを作成する(#create-a-machine-catalog-from-the-machine-catalogs-node)を参照してください。

「**イメージ**」ノードからMCSマシンカタログを作成するには、次の手順を実行します。

1. イメージバージョンを選択し、「**カタログの作成**」をクリックします。「**はじめに**」ページで「**次へ**」をクリックします。
2. **マシン管理**ページと**イメージ**ページでは、選択したイメージバージョンに基づいて設定が事前に選択されています。「イメージ」ページで、選択した準備済みイメージのメモを入力します。
3. 次のページで設定を完了します。

4. **概要**ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。**完了**をクリックします。
5. 作成されたマシンカタログを表示するには、**マシンカタログ**ノードに移動します。

「マシンカタログ」ノードからマシンカタログを作成する

「マシンカタログ」ノードからMCSマシンカタログを作成するには、次の手順を実行します。

1. 左側のナビゲーションペインで**マシンカタログ**をクリックします。
2. **マシンカタログの作成**をクリックします。**マシンカタログのセットアップ**ページが表示されます。
3. **マシンタイプ**ページで、カタログのマシンタイプ（例: **マルチセッションOS**）を選択します。
4. **マシン管理**ページで、次の設定を選択します。

   a. 「**電源管理されているマシン（仮想マシンやブレードPCなど）**」を選択します。

   b. 「**Citrixプロビジョニングテクノロジー**」を選択します。次に、「**Citrix Machine Creation Services™**」を選択します。

   c. **リソース**フィールドで、ホスト接続の作成時に構成したリソース（アベイラビリティゾーンまたはローカルゾーン）を選択し、**次へ**をクリックします。

5. 「**デスクトップエクスペリエンス**」ページで、ユーザーがログオンしたときに使用するランダムまたは静的デスクトップのいずれかを選択します。静的デスクトップを選択した場合は、ユーザーがローカルディスクで行った変更を保存するかどうか（永続的または非永続的）をさらに指定します。
6. 「**イメージ**」ページで、「**イメージの選択**」をクリックして、マシンカタログの準備済みイメージを選択します。作成した準備済みバージョンを選択します。イメージのバージョン名をクリックします。選択したイメージバージョンの詳細を表示するには、下線が引かれているバージョン番号をクリックします。「**完了**」をクリックします。

   準備済みイメージに関連付けられたマシンプロファイルが表示され、そのハードウェアプロパティ（インスタンスタイプ、テナンシータイプ、ネットワークマッピング、セキュリティグループ、ボリュームプロパティなど）がカタログ内のマシンを作成するために使用されます。マシンプロファイルのソースを別のVMまたは起動テンプレートバージョンに変更するには、編集ボタンをクリックします。

7. 「**仮想マシン**」ページで：

   a. カタログのVM数を入力します。

b. マシンプロファイルに基づいて、デフォルトのマシンスペックが表示されます。変更するには、編集アイコンを選択し、マシンスペックを選択します。

8. 「**NIC**」ページで、VMのNIC（またはENI）を選択します。
9. 「**マシンID**」ページで、カタログ内のマシンのマシンIDタイプを構成します。

   a. **ドメイン参加済みマシン（オンプレミスのActive DirectoryまたはMicrosoft Entraハイブリッド参加）**を構成するには、ドメインを選択し、このマシンカタログで作成するVMの新しいADアカウントを作成します。プロビジョニングされたVMは、選択したドメインに参加します。**ドメイン非参加マシン**をプロビジョニングするには、ドメイン非参加オプションを選択します。

   b. VM用に作成する新しいアカウントのアカウント命名スキームを指定します。

10. 「**ドメイン資格情報**」ページで、「**資格情報の入力**」をクリックして、選択したドメインの資格情報を入力します。プロンプトが表示されたら、管理者レベルのユーザー名とパスワードを入力します。以前に当社の製品ドキュメントに従ってドメイン資格情報を保存している場合は、サービスアカウントを使用することもできます。
11. 「**概要**」ページが表示されるまで、残りのページをクリックします。マシンカタログの名前を入力し、「**完了**」を選択してマシンカタログを作成します。

AWSローカルゾーンでのマシンカタログ作成に関する制限事項

- 特定のローカルゾーンは特定のハードウェア構成のみをサポートしています（例：パースのローカルゾーンはGP3ボリュームをサポートせず、GP2のみをサポートします）。
- すべてのローカルゾーンでgp2のみが普遍的にサポートされており、すべてがgp3をサポートしているわけではないため、IDディスクの作成はデフォルトでgp2ボリュームタイプを使用します。
- 目的のローカルゾーンでサポートされているハードウェア仕様を持つマシンプロファイルを選択する必要があります。
- 準備済みイメージAMIスナップショットとIDディスクスナップショットは、デフォルトでローカルゾーンではなくリージョンに配置されます（ローカルゾーンでのEBSスナップショットサポートの可視性に関するAWSの制限のため）。
- 完全なEC2およびEBSサービスをサポートするローカルゾーンのみがサポート対象ゾーンです。

PowerShellを使用してカタログを作成する

準備済みイメージバージョン仕様とマシンプロファイルを使用してカタログを作成する

- `New-ProvScheme`コマンドを使用して、準備済みイメージバージョン仕様からMCS非永続マシンカタログを作成します。例:

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-CleanOnBoot
$true] [-MachineProfile <string>] [-ProvisioningSchemeType “MCS”]
```

- `New-ProvScheme`コマンドを使用して、準備済みイメージバージョン仕様からMCS永続マシンカタログを作成します。例:

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-CleanOnBoot
$false] [-MachineProfile <string>] [-ProvisioningSchemeType “MCS”]
```

カタログを作成するためのPowershellコマンドの完全なセットの例:

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" -Name "wsccatalog" -PersistUserChanges
"Discard" -ProvisioningType "MCS" -Scope @() -SessionSupport
"MultiSession"



$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "domainname"
-IdentityPoolName "wsccatalog" -IdentityType "ActiveDirectory"  -
NamingScheme "aws##" -NamingSchemeType "Numeric" -Scope @()



$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"



$Task = New-ProvScheme -ProvisioningSchemeName wsccatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-HostingUnitName wsc -IdentityPoolName wsccatalog -CleanOnBoot -Scope @()
-SecurityGroup @() -MachineProfile 'XdHyp:\HostingUnits\cvad-test-
```

```
scalestress\us-east-1a.availabilityzone\machine-profile-instance i
(i-0xxxxxxxx).vm' -RunAsynchronously



Get-ProvTask -TaskId $Task.TaskId

$ProvScheme = Get-ProvScheme -ProvisioningSchemeName wsccatalog



Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

マシンプロファイルを更新する

マシンプロファイルで最初にプロビジョニングされたカタログのマシンプロファイルを更新するには、以下を実行します。MCSマシンカタログの編集中に、マシンプロファイルソースのテナンシータイプとハイバネーション機能を変更することもできます。

1. `Set-ProvScheme`コマンドを実行します。例：

```
Set-ProvScheme `

-ProvisioningSchemeUid "<ID" `

-MachineProfile "XDHyp:\HostingUnits\abc\us-
east-1a.availabilityzone\citrix-cvad-machineprofile-instance
(i-0xxxxxxxx).vm"
```

特定の課金モードでマシンカタログを作成する

現在、PowerShellのみを使用してマシンカタログを作成する際に、課金モードを指定できます。

POWERSHELLを使用する

PowerShellで課金モードを指定するには、`New-ProvScheme`コマンドで`CustomProperties`パラメーターを使用します。

```
$custprop = "BillingMode,Monthly"



New-ProvScheme -ProvisioningSchemeName "MyCatalog" `
```

```
-ImageVersionSpecUid $ImageVersionSpecUid `

-HostingUnitName "wsc-unit" `

-IdentityPoolName "MyIdentityPool" `

-MachineProfile "XdHyp:\HostingUnits\wsc-unit\machine-profile
lt-123.launchtemplate\lt-123 (1).launchtemplateversion" `

-CustomProperties $custprop `

-CleanOnBoot
```

注:

`BillingMode`プロパティが省略されている場合、カタログはデフォルトで`Hourly`になります。

既存のカタログの課金モードを変更する

既存のカタログを`Monthly`から`Hourly`に、またはその逆に変換できます。この変更は、カタログ内の新規および既存のVMの両方に適用できます。

更新に関する重要な考慮事項

- サービスウィンドウ：既存のVMは、課金変更を適用するためにサービスウィンドウまたは電源サイクルを経る必要があります。
- 検証：MCSは、変更を適用する前に、既存のインスタンスタイプとプラットフォームが新しい課金モードと互換性があることを検証します。

POWERSHELLを使用した更新

- カタログに追加される新しいVMのみの課金モードを更新するには、プロビジョニングスキームの課金モードカスタムプロパティを更新します。

```
$custprop = "BillingMode,Hourly"
```

```
Set-ProvScheme -ProvisioningSchemeName "MyCatalog" -CustomProperties
$custprop
```

- カタログ内の新規および既存のVMの課金モードを更新するには、更新されたカスタムプロパティを持つ新しいプロビジョニングスキームバージョンを作成し、その新しいバージョンをすべてのVMに適用します。

```
$custprop = "BillingMode,Hourly"



New-ProvSchemeVersion -ProvisioningSchemeName "MyCatalog"
-CustomProperties $custprop



New-ProvSchemeHardwareUpdate -ProvisioningSchemeVersion 2 `

-StartsNow -AllVMs `

-MaxDurationInMinutes 100 `

-ProvisioningSchemeName "MyCatalog"
```

課金情報の監視

カタログおよび個々の仮想マシンの課金モードを確認できます。

アカウントの課金資格を確認するには、次のPowerShellコマンドを実行します。

- CustomPropertiesの一部として`BillingMode`を返します

```
Get-ProvScheme –ProvisioningSchemeName “"MyCatalog" "  | Select
 ProvisioningSchemeName,  CustomProperties
```

- VMInfoの一部として`BillingMode`を返します

```
Get-ProvVMDetails –ProvisioningSchemeName “"MyCatalog" "  | Select-
Object  -ExpandProperty VMInfo
```

トラブルシューティングと検証

MCSには、互換性のない構成を防ぐための事前チェックが含まれています。カタログの作成または編集中に、次のエラーが発生する可能性があります。

- **NoInstanceConfigFoundForBillingMode**: 選択したサービスオファリング（インスタンスタイプ）、テナンシー、およびプラットフォームタイプが、選択された課金モードでサポートされていない場合に発生します。
- **Spot Instance Not Supported**: WorkSpacesホスト接続でスポットインスタンスを使用しようとすると、検証に失敗します。
- **EC2 billing restriction**: AWSアカウントがレガシーEC2課金モデルを使用している場合、月次課金モードを設定しようとすると検証エラーが発生します。

PowerShellを使用して起動テンプレートバージョンでカタログを作成する

起動テンプレートバージョンをマシンプロファイル入力として使用して、MCSマシンカタログを作成できます。また、マシンプロファイルカタログの入力をVMから起動テンプレートバージョンへ、または起動テンプレートバージョンからVMへ更新することもできます。

AWS EC2コンソールで、起動テンプレートのインスタンス構成情報をバージョン番号とともに提供できます。マシンカタログの作成または更新時に、起動テンプレートバージョンをマシンプロファイル入力として指定すると、そのバージョンの起動テンプレートのプロパティがプロビジョニングされたVDA VMにコピーされます。

以下のプロパティは、マシンプロファイル入力として、または`New-ProvScheme`または`Set-ProvScheme`コマンドのパラメータとして明示的に指定できます。`New-ProvScheme`または`Set-ProvScheme`コマンドで指定された場合、これらのプロパティのマシンプロファイル値よりも優先されます。

- サービス提供
- ネットワーク

> **注:**
>
> マシンプロファイルの起動テンプレートでサービス提供が指定されていない場合、または`New-ProvScheme`コマンドのパラメータとして指定されていない場合、適切なエラーが発生します。

起動テンプレートバージョンをマシンプロファイル入力として使用してカタログを作成するには：

1. **PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. 起動テンプレートの起動テンプレートバージョンの一覧を取得します。例：

```
XDHyp:\HostingUnits\test\test-mp-sard (lt-01xxxxx).launchtemplate> ls |
Select FullPath
```

4. 作成されていない場合は、IDプールを作成します。例：

```
New-AcctIdentityPool `

-IdentityPoolName "abc11" `

-NamingScheme "abc1-##" `

-NamingSchemeType Numeric `

-Domain "citrix-xxxxxx.local" `

-ZoneUid "xxxxxxxx" `
```

5. 起動テンプレートバージョンをマシンプロファイル入力として使用してプロビジョニングスキームを作成します。例：

```
New-ProvScheme `

-ProvisioningSchemeName "MPLT1" `

-HostingUnitUid "c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `

-IdentityPoolUid "bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxx" `

-ImageVersionSpecUid ‘24dfb047-e867-527g-896c-25664xxxxx1t’ `

-CleanOnBoot `
```

```
-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-01xxxxx).launchtemplate\lt-01xxxxx (1).launchtemplateversion"
```

6. プロビジョニングスキームをブローカーカタログとして登録します。例：

```
New-BrokerCatalog -Name "MPLT1" `

-AllocationType Random `

-Description "Machine profile catalog" `

-ProvisioningSchemeId fe7df345-244e-4xxxx-xxxxxxxxx `

-ProvisioningType Mcs `

-SessionSupport MultiSession `

-PersistUserChanges Discard
```

7. カタログの作成を完了します。

マシンプロファイルソースを更新する

マシンプロファイルカタログの入力を、VMから起動テンプレートバージョンへ、また起動テンプレートバージョンからVMへ更新することもできます。例：

- VMから起動テンプレートバージョンにマシンプロファイルカタログの入力を更新するには:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-0bxxxxxxxxxxxx).launchtemplate\lt-0bxxxxxxxxxxx
(1).launchtemplateversion"
```

- 起動テンプレートバージョンからVMにマシンプロファイルカタログの入力を更新するには:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\sard-ue1a\us-
```

```
east-1a.availabilityzone\apollo-non-persistent-vda-win2022-2
(i-08xxxxxxxx).vm"
```

MCSIO対応カタログ

MCS Storage Optimization (MCSIO) は、ディスク操作をメモリまたは小型の高速ディスクにキャッシュすることで、VMのパフォーマンスを向上させます。PowerShellコマンドを使用して、MCSIO対応の非永続カタログを作成できます。このようなカタログを作成するには、AMIインスタンスの準備中にVDAをインストールまたはアップグレードする際に、MCSIOドライバーをインストールする必要があります。デフォルトでは、このドライバーはインストールされていません。

MCSIO AMIが準備された後（VDAのインストール時に、MCSIOドライバーをインストールに含めるオプションを選択した場合）、MCSIO対応の非永続カタログを作成できます。

注:

Studioを使用してディスクキャッシュのみ（メモリキャッシュなし）でMCSIOを構成するオプションは、すべてのハイパーバイザーおよびクラウドサービス環境で削除されました。

MCSIO対応カタログを作成する

New-ProvScheme PowerShellコマンドに追加された4つのパラメーターは次のとおりです。

- `UseWriteBackCache`: 指定されたプロビジョニングスキームのキャッシュ（ライトバックキャッシュ）をオンにします
- `WriteBackCacheDiskSize`: キャッシュに使用される一時ディスクのサイズをGB単位で指定します
- `WriteBackCacheMemorySize`: キャッシュに使用するメモリ量をMB単位で指定します。これはオプションのパラメーターです。

注:

- `WriteBackCacheDiskSize`の値は0より大きくする必要があります。これは、少なくとも1 GBのキャッシュディスクストレージが必要なためです。キャッシュディスクサイズはOSディスクサイズより大きくしてはいけません。
- `WriteBackCacheMemorySize`の値はゼロ以外で、マシンカタログのメモリサイズよりも小さくする必要があります。

> MCSIOに影響するカスタムプロパティは次のとおりです。

- `WBCDiskStorageType`: Amazon WorkSpaces Core Managed Instancesの一時ディスクに使用されるボリュームタイプを定義します。このパラメーターは、`volume-type[:iops][:throughput]`の形式で文字列引数を取ります。ボリュームタイプは次のとおりです。
  - gp2: このボリュームタイプには、iopsおよびスループットパラメーターを使用しないでください
  - gp3: このボリュームタイプには、iopsおよびスループットパラメーターを使用してください
  - io1: このボリュームタイプには、iopsパラメーターのみを使用してください
  - io2: このボリュームタイプには、iopsパラメーターのみを使用してください

  デフォルトのボリュームタイプは**gp2**です。
- `PersistWBC`: Amazon WorkSpaces Core Managed Instancesの電源がオフになったときに、キャッシュディスクを保持するか破棄するかを制御します。`true`に設定すると、キャッシュディスクは保持されます。`false`（デフォルト）に設定すると、キャッシュディスクはAMIインスタンスの電源がオンになっている間のみ作成および保持されます。
- `PersistOSDisk`: Amazon WorkSpaces Core Managed Instancesの電源がオフになったときに、OSディスクを保持するか破棄するかを制御します。`true`に設定すると、OSディスクは保持されます。`false`（デフォルト）に設定すると、OSディスクはAMIインスタンスの電源がオンになっている間のみ作成および保持されます。

MCSIOが有効な非永続カタログを作成するには、PowerShellウィンドウで次の手順を実行します。

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*`を実行します。
3. ブローカーカタログとIDプールを作成します。
4. プロビジョニングスキームを作成します。例：

```
$HostingUnitUid = '0xxxx1d9-bbfc-xxxf-bxxb-exxxxxe008b2'

$MasterImageVM = 'XDHyp:\HostingUnits\ctx-test\aws-apollo-non-
persistent-multi-mcsio-vda-win2022 (ami-0bf1810488acbxxxb).template'

$NetworkMap = @{ 'NetworkPath' = 'XDHyp:\HostingUnits\ctx-test\us-
```

```
east-1a.availabilityzone\10.0.128.0`/17
(vpc-0fa6e41d72507fxxx).network' }

$SecurityGroup = $( 'XDHyp:\HostingUnits\ctx-test\us-
east-1a.availabilityzone\private.securitygroup' )

$ServiceOffering = 'XDHyp:\HostingUnits\ctx-test\T3 Medium
Instance.serviceoffering'

$CustomProperties = 'WBCDiskStorageType,gp3:6000:250;PersistWBC,false'



$provScheme = New-ProvScheme -ProvisioningSchemeName $CatalogName
-HostingUnitUid $HostingUnitUid `

-IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `

- MasterImageVM $MasterImageVM `

-NetworkMap $NetworkMap `

-ServiceOffering $ServiceOffering `

-SecurityGroup $SecurityGroup `

-CustomProperties $CustomProperties `

-UseWriteBackCache -WriteBackCacheDiskSize 16 -WriteBackCacheMemorySize
256
```

5. カタログにVMを追加します。

MCSIOで起動パフォーマンスを向上させる

MCSIOを有効にし、`PersistWBC`と`PersistOSDisk`のカスタムプロパティを`true`に設定すると、VMの起動パフォーマンスを向上させることができます。この設定により、VMは新しいキャッシュディスクを初期化したり、テンプレートからルートディスクを再作成したりする必要がないため、より高速に起動できます。

OSディスクとIDディスクを暗号化する

AWS KMSキー（カスタマーマネージドキーおよびAWSマネージドキー）を使用してVMのカタログを作成できます。これらのキーは、OSディスクとIDディスク（ID）の暗号化に使用できます。

- AWSマネージドキーは毎年自動的にローテーションされます。
- カスタマーマネージドキーは自動ローテーションがオプションであり、手動で管理できます。

KMSキーの詳細については、以下のAWSドキュメントを参照してください。

- AWS KMSの概念
- 自動キーローテーションの仕組み

OSディスクとIDディスクの暗号化には、次のいずれかを構成します。

- 暗号化された準備済みイメージを使用します（例：KMSキーで暗号化されたEBSルートボリュームを含むインスタンスまたはスナップショットから作成されたAMI）。
- 暗号化されたEBSルートボリュームを含むマシンプロファイルソース（VMまたは起動テンプレート）を使用します。

制限事項

次の制限事項を考慮してください。

- MCSは現在、準備済みイメージAMI上のディスクを1つのみサポートしています。
- 既存の暗号化されていないEBSボリュームやスナップショットを直接暗号化したり、既存の暗号化されたボリュームのKMSキーを変更したりすることはできません。これを行うには、次の手順を実行する必要があります。

  a. そのボリュームの新しいスナップショットを作成します。

  b. そのスナップショットから新しいボリュームを作成します。

  c. 新しいボリュームを暗号化します。

以下のAWSドキュメントを参照してください。

- 暗号化されていないリソースを暗号化する
- EBSボリュームの自動またはデフォルト暗号化の制限: 既存および新規のAmazon EBSボリュームを自動的に暗号化する。

ディスク暗号化を使用してカタログを作成する

ディスク暗号化を使用してMCSマシンカタログを作成できます。

- 準備済みイメージ（暗号化されたディスクを持つマスターイメージからイメージ管理を使用して作成）
- マシンプロファイル

マシンプロファイル入力を使用する際の考慮事項は次のとおりです。

- マシンプロファイル入力のKMSキーは、準備済みイメージのKMSキーよりも優先されます。
- マシンプロファイル入力が提供されない場合、準備済みイメージAMIのKMSキーがカタログVMのディスクを暗号化するために使用されます。
- マシンプロファイルにブロックデバイスマッピングが存在する場合、準備済みイメージテンプレート（AMI）とマシンプロファイルに存在するブロックデバイスは一致している必要があります。たとえば、AMIに`/dev/sda1`で定義されたデバイスがある場合、マシンプロファイルにも`/dev/sda1`で定義されたデバイスが必要です。
- マシンプロファイルソースにキーがなく、準備されたイメージが暗号化されていない場合、カタログVMのディスクは暗号化されません。
- 準備されたイメージが暗号化されている場合、マシンプロファイルソースVMまたは起動テンプレートには、有効な入力と見なされるために暗号化されたルートボリュームが必要です。

既存のカタログを変更する

`Set-ProvScheme` PowerShellコマンドを使用して、既存のカタログを次のように変更できます。

- 新しいKMSキーを含むボリュームを持つマシンプロファイル入力。
- イメージ管理を使用して、暗号化されたAMIを持つマスターイメージから作成された準備済みイメージ。

重要な考慮事項：

- カタログに追加された新しいVMのボリュームは、新しいKMSキーで暗号化されます。
- 既存のマシンプロファイルがある場合に暗号化設定を更新するには、新しいマシンプロファイルで`Set-ProvScheme`を実行します。
- 既存のカタログを暗号化されたボリュームから暗号化されていないボリュームに変更することはできません。 暗号化された準備済みイメージAMIから暗号化されていない準備済みイメージAMIへのイメージ更新はできません。

VMインスタンスでNitroTPMとUEFIセキュアブートを有効にする

カタログを作成する際、NitroTPMおよび/またはUEFIセキュアブートが有効な準備済みイメージ（AMI）を選択できるようになりました。これにより、カタログ内のプロビジョニングされたVMもNitroTPMおよび/またはUEFIセキュアブートが有効になります。この実装により、VMのセキュリティと信頼性が確保されます。NitroTPMとUEFIセキュアブートの詳細については、Amazonドキュメントを参照してください。

制限事項

- 現在、NitroTPMとセキュアブートは、中国を除くすべてのAWSリージョン（AWS GovCloud (US)リージョンを含む）で利用できます。
- 既存のカタログでNitroTPMとUEFIセキュアブートを有効にすることはできません。NitroTPMとUEFIセキュアブートが有効なカタログが必要な場合は、新しいカタログを作成してください。

主要な手順

1. AWS環境をセットアップします。
2. AWSへの接続を作成します。
3. NitroTPMおよび/またはUEFIセキュアブートが有効なマスターイメージ（AMI）を作成する(#create-an-ami-that-supports-nitrotpm-and-uefi-secure-boot)。
4. マスターイメージから準備済みイメージを作成します。詳細については、「Amazon WorkSpaces Coreマネージドインスタンス用の準備済みイメージを作成する」(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/create-prepared-image-amazon-wsc.html)を参照してください。
5. Web Studioのカタログ作成メニューで、またはPowerShellコマンドを使用してプロビジョニングスキームを作成するときに、NitroTPMとUEFIセキュアブートが有効になっている準備済みのイメージを選択してマシンカタログを作成します。

作成されたカタログに追加されたVMは、NitroTPMおよびUEFIセキュアブートが有効になっています。

NitroTPMおよびUEFIセキュアブートをサポートするAMIを作成する

1. NitroTPMおよび/またはUEFIセキュアブートが有効になっているVMからAMIを作成できます。
   a. AWS Marketplaceイメージを使用してインスタンスを作成します。例：`TPM-Windows_Server-2022-English-Full-Base on the aws-marketplace`を検索します。
   b. シングルセッションまたはマルチセッションVDAをダウンロードします。
   c. そのVMからAMIを作成します。
2. register-imageコマンドを使用します。

```
--boot-mode (string)

--tpm-support (string)
```

詳細については、register-imageを参照してください。

以下のAWSドキュメントを参照してください。

- EC2インスタンスタイプのサポートされているブートモードを決定する
- Amazon EC2インスタンスでNitroTPMを使用するための要件/.

Delivery Controller™ホストからPowerShellウィンドウを開いて、特定の項目を確認できます。

- サービス提供がNitroTPMまたはUEFIセキュアブートをサポートしているか

```
(Get-Item -Path “XDHyp:\HostingUnits\aws\T3 Medium
Instance.serviceoffering”).AdditionalData.BootMode

(Get-Item -Path “XDHyp:\HostingUnits\aws\T3 Medium
Instance.serviceoffering”).AdditionalData.NitroTpmSupportVersions
```

- テンプレートがNitroTPMまたはUEFIセキュアブートをサポートしているか

```
(Get-HypInventoryItem -LiteralPath “XDHyp:\HostingUnits\aws”
-ResourceType “template -Id “ID”).AdditionalData.BootMode



(Get-HypInventoryItem -LiteralPath “XDHyp:\HostingUnits\aws”
-ResourceType “template -Id “ID”).AdditionalData.TpmSupport
```

既存のカタログのサービス提供を更新する

`Set-ProvScheme`を使用して、既存のカタログのサービス提供を変更できます。この変更は、新しく追加されたVMに適用されます。ただし、次のシナリオではエラーが発生します。

AMIのブートモード	AMIはNITRO TPMをサポートしていますか？	サービス提供はNITROTPMとUEFIセキュアブートをサポートしていますか？
UEFI	いいえ	いいえ
レガシーBIOS	はい	いいえ
UEFI	はい	いいえ

AMIのブートモード	AMIはNITRO TPMをサポートしていますか？	サービス提供はNITROTPMとUEFIセキュアブートをサポートしていますか？
UEFI優先	はい	いいえ

VM上のタグをコピーする

マシンプロファイルで指定されたNIC、およびディスク（IDディスク、ライトバックキャッシュディスク、OSディスク）のタグを、MCSマシンカタログで新しく作成されたVMにコピーできます。これらのタグは、マシンプロファイルソース（AWS VMインスタンスまたはAWS起動テンプレートバージョン）のいずれかで指定できます。この機能は、永続および非永続マシンカタログとVMに適用されます。

> **注:**
>
> - AWS EC2コンソールでは、**起動テンプレートバージョンのリソースタグ**の下に**ネットワークインターフェースのタグ**の値が表示されません。ただし、PowerShellコマンド `aws ec2 describe-launch-template-versions --launch-template-id lt-0bb652503d45dcbcd --versions 12` を実行して、タグの仕様を確認できます。
> - マシンプロファイルソース（VMまたは起動テンプレートバージョン）に2つのネットワークインターフェース（eni-1とeni-2）があり、eni-1にタグt1、eni-2にタグt2がある場合、VMは両方のネットワークインターフェースのタグを取得します。

PowerShellを使用してVMインスタンスをフィルタリングする

マシンプロファイルVMとして使用するAWS VMインスタンスは、マシンカタログが正しく作成および機能するために互換性がある必要があります。マシンプロファイルの入力VMとして使用できるAWS VMインスタンスを一覧表示するには、`Get-HypInventoryItem` コマンドを使用できます。このコマンドは、ホスティングユニットで利用可能なVMのインベントリをページングおよびフィルタリングできます。

ページネーション：

「**Get-HypInventoryItem**」は、2つのページネーションモードをサポートします。

- ページングモードでは、`-MaxRecords` と `-Skip` パラメーターを使用してアイテムのセットを返します。

  - `-MaxRecords`: デフォルトは **1** です。これは、返すアイテムの数を制御します。
  - `-Skip`: デフォルトは **0** です。これは、ハイパーバイザー内のリストの絶対的な先頭 (または絶対的な末尾) からスキップするアイテムの数を制御します。

- スクロールモードでは、`-MaxRecords`、`-ForwardDirection`、および `-ContinuationToken` パラメーターを使用してレコードのスクロールを可能にします。
  - `-ForwardDirection`: デフォルトは **True** です。これは `-MaxRecords` とともに使用され、一致するレコードの次のセットまたは前のセットのいずれかを返します。
  - `-ContinuationToken`: 直後のアイテムを返します (または `ForwardDirection` が **false** の場合は直前のアイテムを)。ただし、`ContinuationToken` で指定されたアイテムは含みません。

ページネーションの例:

- 最も低い名前を持つマシンのテンプレートの単一レコードを返すには。`AdditionalData` フィールドには `TotalItemsCount` と `TotalFilteredItemsCount` があります。

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template
```

- 最も低い名前を持つマシンのテンプレートのレコードを10件返すには:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 10 | select Name
```

- 最も高い名前で終わるレコードの配列を返すには:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ForwardDirection $False -MaxRecords 10 | select
Name
```

- 指定された `ContinuationToken` に関連付けられたマシンテンプレートから始まるレコードの配列を返すには:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ContinuationToken "ami-07xxxxxxxxx"
-MaxRecords 10
```

フィルタリング:

フィルタリングには、以下の追加のオプションパラメーターがサポートされています。これらのパラメーターは、ページネーションオプションと組み合わせることができます。

- `-ContainsName "my_name"`: 指定された文字列がAMI名の一部と一致する場合、そのAMIは `Get` の結果に含まれます。例:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -ContainName ‘apollo’ | select
Name
```

- `-Tags '{ "Key0": "Value0", "Key1": "Value1", "Key2": "Value2" }'`: これらのタグのいずれかを少なくとも1つ持つAMIは、 `Get` の結果に含まれます。例:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -Tags '{"opex owner": "Not
tagged"}' | select Name
```

> **注:**
>
> 2つのタグ値がサポートされています。**Not Tagged** タグ値は、タグのリストに指定されたタグがない項目に一致します。**All values** タグ値は、タグの値に関係なく、そのタグを持つ項目に一致します。それ以外の場合、一致は、項目がタグを持ち、その値がフィルターで指定された値と等しい場合にのみ発生します。

- `-Id "ami-0a2d913927e0352f3"`: AMIが指定されたIDに一致する場合、 `Get` の結果に含まれます。例:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -Id ami-xxxxxxxxxxxxx
```

AdditionalDataパラメーターでのフィルタリング:

`AdditionalData` フィルターパラメーターは、テンプレートまたはVMを、その機能、サービス提供、またはAdditionalDataにある任意のプロパティに基づいて一覧表示します。例:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200).AdditionalData
```

互換性のないVMを示すために、`-Warn` パラメーターを追加することもできます。VMは、**Warning** という名前の`AdditionalData` フィールドとともに含まれます。例:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200 -Template "ami-015xxxxxxxx"
-Warn $true).AdditionalData
```

次のステップ

- Amazon WorkSpaces Coreカタログの管理については、Amazon WorkSpaces Coreマネージドインスタンスのカタログを管理するを参照してください。

詳細情報

- AWS仮想化環境
- Amazon WorkSpaces Coreマネージドインスタンスへの接続
- イメージ管理
- Amazon WorkSpaces Coreマネージドインスタンス用の準備済みイメージを作成する
- Amazon WorkSpaces Core GitHub PowerShellの例については、citrix-mcs-sdk-samples-Amazon WorkSpaces Coreを参照してください。

Azure で準備済みイメージのマシンカタログを作成する

準備済みイメージを作成し、その準備済みイメージを使用して、次の方法でMCSマシンカタログを作成します。

- ウェブスタジオ
- (#use-powershell)

準備済みイメージを使用して MCS マシンカタログを作成する主な手順は次のとおりです。

1. イメージ定義と初期イメージバージョンを作成します。
2. イメージバージョンを準備済みイメージとして使用してカタログを作成します。

Web Studio を使用する

イメージ定義と初期イメージバージョンを作成する

イメージ定義と初期イメージバージョンを作成するには、次の手順を実行します。

1. Web Studio から、**イメージ**ノードに移動し、**イメージ定義の作成**をクリックします。**はじめに**ページで**次へ**をクリックします。
2. **イメージ定義**ページで、イメージ定義の**OSタイプ**と**セッションタイプ**を指定します。
3. 既存のリソースグループを選択するか、イメージリソースを保持するための新しいリソースグループを作成します。イメージ共有を有効にするには、Azure Compute Gallery で**イメージバージョンを配置**を選択し、新しいギャラリーを作成するか、既存のギャラリーを使用してイメージバージョンを保持するかを選択します。
4. **［イメージ］ページで、［リソース］**（設定された接続に適用可能なリソースのみが一覧表示されます）と、イメージバージョンを作成するためのテンプレートとして使用するマスターイメージを選択します。**［マシンプロファイルを使用する］**チェックボックスをオンにして、マシンプロファイルを選択できます。

   注:

   - イメージを選択する前に、マスターイメージにVDA 2311以降がインストールされており、MCSIOドライバーがVDAにインストールされていることを確認してください。
   - 機密VMタイプの準備済みイメージを使用してMCSカタログを作成する場合は、機密VMタイプのマスターイメージと機密VMタイプのマシンプロファイルを使用して準備済みイメージを作成します。機密VMタイプのマスターイメージとマシンプロファイルの準備については、Azure機密VMを参照してください。

5. **ストレージとライセンスの種類**ページで、イメージ準備プロセスの一部として使用するストレージとライセンスの種類を選択します。

   注:

   イメージページでマシンプロファイルを選択すると、プロファイル設定に基づいてマシンプロファイルのライセンスタイプが事前に選択されます。

6. **マシン仕様**ページで、マシンサイズを選択します。**イメージ**ページでマシンプロファイルを選択すると、マシンプロファイルのマシンサイズがデフォルトで選択されます。
7. **NIC**ページで、準備イメージのNICを選択または追加します。各NICについて、関連する仮想ネットワークを選択します。
8. **ディスク設定**ページで、顧客管理の暗号化キー（CMEK）を選択します。マシンプロファイルにCMEKがないが、マスターイメージにある場合は、マスターイメージからCMEKが事前に選択されます。
9. 「**Version Description**」ページで、作成された初期イメージバージョンの説明を入力します。
10. 「**概要**」ページで、イメージ定義と作成された初期イメージバージョンの詳細を確認します。イメージ定義の名前と説明を入力します。「**完了**」をクリックします。

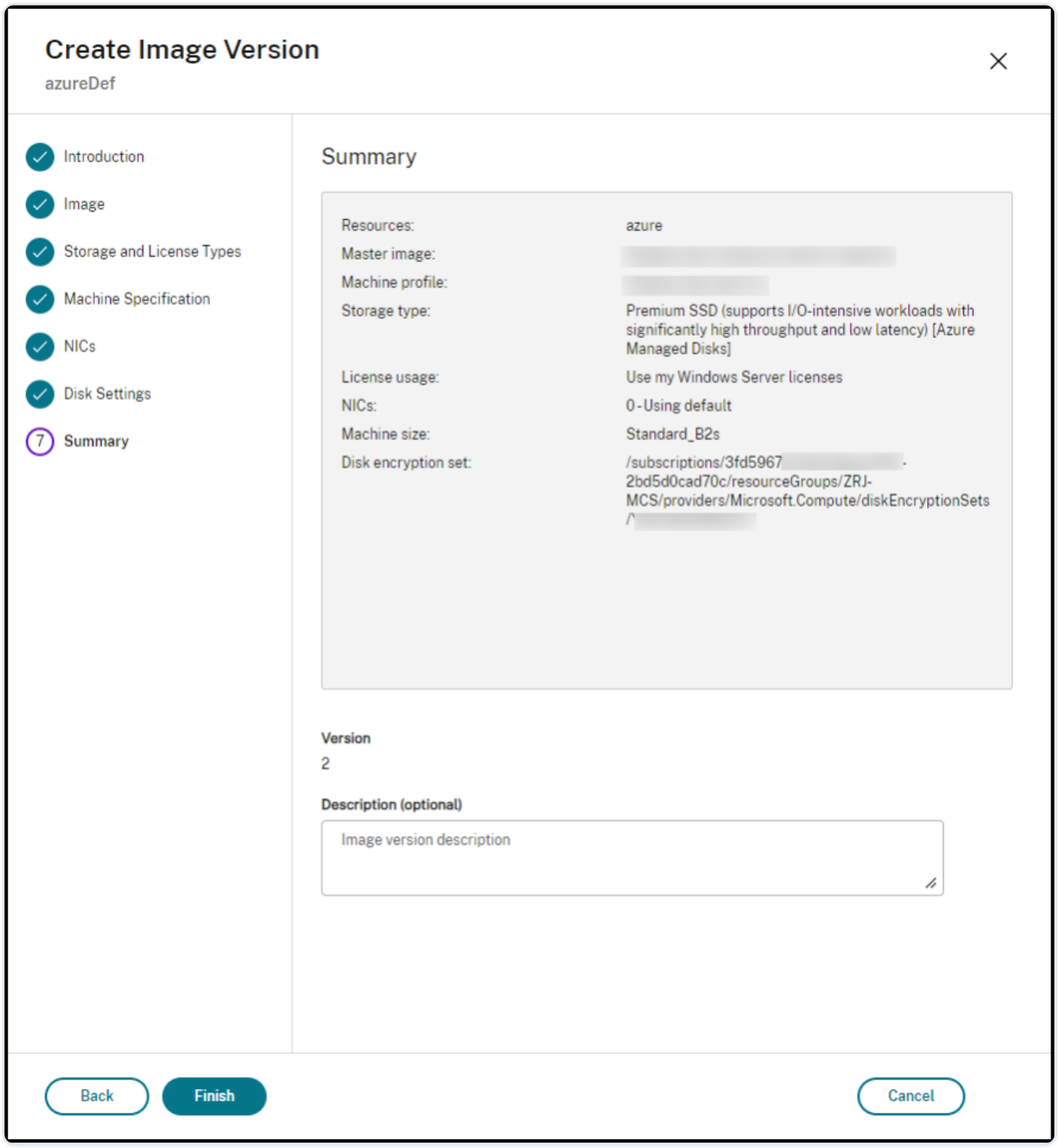
イメージバージョンを作成する

イメージバージョンを使用すると、特定のイメージに対するさまざまなイテレーションや更新を管理できます。この機能により、さまざまな目的のためにイメージの複数のバージョンを維持できます。

初期イメージバージョンからイメージバージョンを作成するには、次の手順を実行します。

> **注:**
>
> すべてのイメージバージョンのホスティングユニットは同じである必要があります。

1. 「**Images**」ノードに移動し、イメージバージョンまたはイメージ定義を選択して、「**Create Image Version**」をクリックします。
2. Image definitionページで、ホスティングユニットを変更し、そのイメージバージョンのマスターイメージとマシンプロファイルを再選択できます。
3. イメージバージョンの構成を、最初に構成されたイメージバージョンと異なるものにしたい場合は、**Create Image Version**ダイアログの**Storage and License Types**、**Machine Specification**、**NICs**、および**Disk Settings**ページで設定を構成します。
4. イメージバージョンの説明を追加します。「**Finish**」をクリックします。



注:

何らかの理由でイメージバージョンの作成に失敗した場合、下部にある**トラブルシューティング**タブに**再試行**オプションが表示されます。

共有準備済みイメージ

Azureの異なるホスティングユニット間で準備済みイメージを共有するには、次の手順に従います。

1. イメージバージョンを右クリックし、**Manage Image Share**を選択します。Azure環境内のすべてのホスティングユニットが表示されます。イメージバージョンが作成されたリソースは、すべてのアクションに対して無効になっています。
2. イメージを共有するホスティングユニットを選択し、**保存**をクリックします。**共有ステータス**列には「進行中」と表示されます。
3. 共有ステータスの詳細については、**Resources**タブをクリックします。

> **注:**
>
> イメージバージョンの共有のステータスが進行中の場合、**イメージバージョンの削除**または**イメージ共有の管理**のオプションは無効になります。

「イメージ」ノードからマシンカタログを作成する

「**イメージ**」ノードの「**カタログの作成**」オプションを使用して、イメージバージョンでカタログを作成します。

または、**マシンカタログ**ノードでカタログを作成する際にバージョンを選択し、カタログ作成ワークフローで準備済みイメージオプションにリンクできます。「マシンカタログノードからマシンカタログを作成する」を参照してください。(#create-a-machine-catalog-from-the-machine-catalogs-node)

「**イメージ**」ノードからMCSマシンカタログを作成するには、次の手順を実行します。

1. イメージバージョンを選択し、「**カタログの作成**」をクリックします。「**はじめに**」ページで「**次へ**」をクリックします。
2. **デスクトップエクスペリエンス**ページで、必要なデスクトップエクスペリエンスを選択します。
3. **イメージ**ページから**ディスク設定**ページまで、設定は選択したイメージバージョンに基づいて事前に選択されています。
4. **リソースグループ**ページで、新しいリソースグループを作成するか、既存のリソースグループを使用してこのカタログのリソースを配置するかを選択できます。
5. 次のページで設定を完了します。
6. **概要**ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。**完了**をクリックします。
7. 作成されたマシンカタログを表示するには、**マシンカタログ**ノードに移動します。

「マシンカタログ」ノードからマシンカタログを作成する

マシンカタログノードからMCSマシンカタログを作成するには、次の手順を実行します。

1. 左側のナビゲーションペインで**マシンカタログ**をクリックします。
2. **マシンカタログの作成**をクリックします。**マシンカタログのセットアップ**ページが表示されます。**はじめに**、**マシンタイプ**、**マシン管理**の各ページで**次へ**をクリックします。
3. **マシン管理**ページで、次の設定を選択します。
    a. 「**電源管理されているマシン（仮想マシンやブレードPCなど）**」を選択します。
    b. 「**Citrixプロビジョニングテクノロジー**」を選択します。次に、「**Citrix Machine Creation Services™**」を選択します。
    c. 「**リソース**」フィールドには、異なるゾーンに属するリソースが一覧表示されます。任意のAzureネットワークリソースを選択し、「**次へ**」をクリックします。
4. **イメージ**ページで、マスターイメージタイプの場合は、次の手順に従います。
    a. マスターイメージを選択します。
    b. マスターイメージの下で、イメージを選択します。ブレードには、リソースと同じリージョンに属するすべてのイメージが一覧表示されます。
    c. 「**完了**」をクリックします。
    d. 準備済みイメージタイプの場合は、**準備済みイメージ**を選択します。
    e. 「**準備済みイメージ**」の下で、イメージ定義のイメージバージョンを選択します。必要に応じて、選択した準備済みイメージバージョンにメモを追加します。
    f. イメージバージョン名をクリックします。選択したイメージバージョンの詳細を表示するには、下線が引かれているバージョン番号をクリックします。
    g. 選択したイメージバージョンがマシンプロファイルで構成されている場合は、マシンプロファイルを選択します。選択したイメージバージョンがマシンプロファイルで構成されていない場合、マシンプロファイルを使用することはできません。
5. 次のページで設定を構成します。
6. 「**ディスク設定**」ページで、選択した準備済みイメージがディスク暗号化セットを使用している場合、その暗号化セットを削除することはできませんが、キーを別の暗号化キーに変更することはできます。
7. **リソースグループ**ページで、新しいリソースグループを作成するか、既存のリソースグループを使用してこのカタログのリソースを配置するかを選択できます。
8. 次のページで設定を完了します。

9. **概要**ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。**完了**をクリックします。

PowerShell を使用する

準備済みイメージを作成する

準備済みイメージバージョン仕様を作成するための詳細な PowerShell コマンドは次のとおりです。

1. `Test-ProvImageDefinitionNameAvailable command` を使用して、利用可能なイメージ定義名を確認します。例:

   ```
   Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string[]>
   ```

2. `New-ProvImageDefinition` コマンドを使用してイメージ定義を作成します。例:

   ```
   New-ProvImageDefinition -ImageDefinitionName image1 -OsType Windows
   -VdaSessionSupport MultiSession
   ```

3. `Add-ProvImageDefinitionConnection` コマンドを使用して、指定されたホスティング接続でイメージ定義の新しい構成を作成します。

   `Add-ProvImageDefinitionConnection` の `CustomProperties` には、次のものが含まれます。これらのパラメーターを使用しない場合、デフォルト値が使用されます。

   - `ResourceGroups`: ベースディスクがあるリソースグループ。
   - `UseSharedImageGallery`: ベースディスクの種類のインジケーター。ACG (イメージ共有) には `true` を、スナップショットには `false` を使用します。
   - `ImageGallery`: ベースディスクがACGイメージバージョンである場合のギャラリー名。

   例:

   - スナップショットおよび顧客が提供するリソースグループの場合:

     ```
     $CustomerOwnRsourceGroupProperties = @"

     <CustomProperties xmlns="http:// schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance">
     ```

```
<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="yangj_image" />

</CustomProperties>

"@
```

- ACG、顧客が提供するリソースグループ、およびイメージギャラリーの場合:

```
$CustomerOwnAllProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="rg" />

<Property xsi:type="StringProperty" Name="ImageGallery"
Value="gallery" />

</CustomProperties>

"@
```

- ACG および顧客が提供するリソースグループのみの場合:

```
$CustomerOwnResourceGroupProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="rg" />
```

```
</CustomProperties>

"@
```

- ACG、Citrix が管理するリソースグループ、およびイメージギャラリーの場合:

```
$CustomerOwnResourceGroupNothingProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

</CustomProperties>

"@
```

```
Add-ProvImageDefinitionConnection -ImageDefinitionName image1
-HypervisorConnectionName Azure28 [-CustomProperties $CustomProperties]
```

4. `New-ProvImageVersion` コマンドを使用してイメージバージョンを作成します。例:

```
New-ProvImageVersion -ImageDefinitionName image1 -Description "version
1"
```

5. `Add-ProvImageVersionSpec` コマンドを使用して、マスターイメージバージョン仕様をイメージバージョンに追加します。例:

```
Add-ProvImageVersionSpec -ImageDefinitionName  image1  -
ImageVersionNumber  1 -HostingUnitName azure -MasterImagePath "XDHyp:
\HostingUnits\azure\image.folder\azureresourcegroup.resourcegroup\win20
22-snapshot.snapshot"
```

注:

> ホスティングユニットのイメージバージョンには、マスターイメージバージョン仕様を1つだけ追加できます。

6. `New-ProvImageVersionSpec` コマンドを使用して、マスターイメージバージョン仕様から準備済みイメージバージョン仕様を作成します。

   `New-ProvImageVersionSpec` の CustomProperties には以下を含めることができます。パラメーターを使用しない場合、デフォルト値が使用されます。

   - `PreparedImageStorageType`: 準備済みイメージに使用するストレージタイプ。デフォルトは `Standard_LRS` ですが、`Premium_LRS` または `Standard_ZRS` にすることもできます。`Standard_ZRS` はイメージのゾーン冗長性を提供します。

```
New-ProvImageVersionSpec

-SourceImageVersionSpecUid  c6e7384c-b2f8-46d6-9519-29a2c57ed3cb

-NetworkMapping @{"0"="XDHyp:
\HostingUnits\azure\virtualprivatecloud.folder\azureresourcegroup.resou
rcegroup\azure-vnet-eastus.virtualprivatecloud\dev.network"}

-ServiceOffering"XDHyp:
\HostingUnits\azure\serviceoffering.folder\Standard_B2ms.serviceofferin
g" -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"></CustomProperties>"
-RunAsynchronously
```

7. `Add-ProvImageVersionSpecHostingUnit` コマンドを使用して、すべてのホスティング接続で準備済みイメージバージョン仕様を別のホスティングユニットと共有することもできます。

   `Add-ProvImageVersionSpecHostingUnit` の CustomProperties には以下を含めることができます。パラメーターを使用しない場合、ソースの準備済みイメージ仕様の値が使用されます。

   - `PreparedImageStorageType`: 準備済みイメージに使用するストレージタイプ。

```
Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx
-HostingUnitName AzureWest
```

> **注:**
>
> 1つのホスティングユニットと準備タイプには、準備済みインスタンスを1つのみ持つことができます。

イメージ定義、イメージバージョン、および準備済みイメージバージョン仕様を作成するための PowerShell コマンドの完全なセットの例:

```
New-ProvImageDefinition -ImageDefinitionName image1 -OsType Windows
-VdaSessionSupport MultiSession



$ImageDefinitionCustomProperties = @" <CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/
2001/XMLSchema-instance"> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="true" /> <Property
xsi:type="StringProperty" Name="ResourceGroups" Value="rg" /> <Property
xsi:type="StringProperty" Name="ImageGallery" Value="gallery" /> </
CustomProperties> "@



Add-ProvImageDefinitionConnection -ImageDefinitionName image1
-HypervisorConnectionName Azure28 -CustomProperties
$ImageDefinitionCustomProperties



$imageVersion = New-ProvImageVersion -ImageDefinitionName image1
-Description "version 1"



$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid ` -HostingUnitUid
$hostingunit.HostingUnitUid ` -MasterImagePath "XDHyp:
\HostingUnits\azure28\image.folder\abc.resourcegroup\def-
snapshot.snapshot"
```

```
$ImageVersionSpecCustomProperties = @'



<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">



<Property xsi:type="StringProperty" Name="PreparedImageStorageType"
Value="Premium_LRS" />



<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />



</CustomProperties>



'@



New-ProvImageVersionSpec -NetworkMapping @{"0" = "XDHyp:
\HostingUnits\azure28\virtualprivatecloud.folder\East
US.region\virtualprivatecloud.folder\studio-mcs-
infrastructure.resourcegroup\studio-mcs-vnet-
eastus.virtualprivatecloud\mcs-dev.network" } -CustomProperties
$ImageVersionSpecCustomProperties -ServiceOffering "XDHyp:
\HostingUnits\azure28\serviceoffering.folder\Standard_B2s.serviceoffering"
-SourceImageVersionSpecUid $SourceImageVersionSpec.ImageVersionSpecUid



$TargetCustomProperties = @'



<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
```

```
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">



<Property xsi:type="StringProperty" Name="PreparedImageStorageType"
Value="Standard_ZRS" />



</CustomProperties>



'@



Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx
-HostingUnitName AzureWest –TargetCustomProperties $TargetCustomProperties



$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid | Where SourceImageVersionSpecUid-eq
$SourceImageVersionSpec.ImageVersionSpecUid
```

注:

- イメージ定義内のすべてのイメージバージョン仕様は、同じホスティングユニットに属している必要があります。
- イメージバージョンには、マスターイメージバージョン仕様を1つ、準備済みイメージバージョン仕様を1つだけ含めることができます。
- すべてのイメージバージョン仕様はマシンプロファイルを持つか、またはどのイメージバージョン仕様もマシンプロファイルを持たないかのいずれかである必要があります。

準備済みイメージバージョン仕様を使用してカタログを作成する

`New-ProvScheme` コマンドを使用して、準備済みイメージバージョン仕様から MCS マシンカタログを作成します。例:

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-VMCpuCount <int>]
[-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping <Hashtable>] [-
CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-ServiceOffering
<string>] [-SecurityGroup <string[]>] [-TenancyType <string>] [-
MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>][-ImageAssignmentNote <string>]
```

または、,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitName <string> -IdentityPoolName <string> [-VMCpuCount
<int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping
<Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-
ServiceOffering <string>] [-SecurityGroup <string[]>] [-TenancyType
<string>] [-MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>][-ImageAssignmentNote <string>]
```

ACGイメージバージョン仕様を使用する場合は、`UseSharedImageGallery` を `true` に設定します。例：

```
$provSchemeCustomProperties= @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

    <Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_LRS" />

</CustomProperties>

"@

New-ProvScheme -ProvisioningSchemeName assignimage -ImageVersionSpecUid
```

```
$PreparedImageVersionSpec.ImageVersionSpecUid `

    -HostingUnitUid $hostingunit.HostingUnitUid `

    -IdentityPoolUid $IdentityPool.IdentityPoolUid `

    -CleanOnBoot -Scope @() -SecurityGroup @() `

    -ServiceOffering "XDHyp:
\HostingUnits\azure28\serviceoffering.folder\Standard_B2s.serviceoffering"
`

    -NetworkMapping @{"0"="XDHyp:
\HostingUnits\azure28\virtualprivatecloud.folder\East
US.region\virtualprivatecloud.folder\studio-mcs-
infrastructure.resourcegroup\studio-mcs-vnet-
eastus.virtualprivatecloud\mcs-dev.network"} `

    -CustomProperties $provSchemeCustomProperties
```

カタログを作成するためのPowershellコマンドの完全なセットの例：

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" -Name "azurecatalog" -PersistUserChanges
"Discard" -ProvisioningType "MCS" -Scope @() -SessionSupport
"MultiSession"



$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "azure.local"
-IdentityPoolName "azurecatalog" -IdentityType "ActiveDirectory"  -
NamingScheme "azure##" -NamingSchemeType "Numeric" -Scope @()



$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"



$Task = New-ProvScheme -ProvisioningSchemeName azurecatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-HostingUnitName azure -IdentityPoolName azurecatalog -CleanOnBoot -Scope
```

```
@() -SecurityGroup @() -ServiceOffering "XDHyp:
\HostingUnits\azure\serviceoffering.folder\Standard_B2s.serviceoffering"
-NetworkMapping @{"0"="XDHyp:
\HostingUnits\azure\virtualprivatecloud.folder\azureresourcegroup.resource
group\azure-vnet-eastus.virtualprivatecloud\dev.network"}
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">    <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="true" /><Property
xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
Value=`"StandardSSD_LRS`" /></CustomProperties>" -RunAsynchronously



Get-ProvTask -TaskId $Task.TaskId

$ProvScheme = Get-ProvScheme -ProvisioningSchemeName azurecatalog



Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

暗号化された準備済みイメージをリージョン、サブスクリプション、テナント間で共有する

Azure Compute Gallery (ACG) イメージは、ディスク暗号化セット (DES) で暗号化できます。ACG 共有機能を使用すると、暗号化された準備済みイメージを Azure のリージョン、サブスクリプション、テナント間で共有できます。ターゲットリソースは、準備済みイメージが属するサブスクリプションから、そのリージョン内の DES を選択する必要があります。その後、暗号化された準備済みイメージが共有されているリソースにマシンカタログを作成できます。

暗号化された準備済みイメージを共有するための主要な手順は次のとおりです。

1. 各リージョンでディスク暗号化セット (DES) を作成します: Microsoft ドキュメント「マネージドディスクのカスタマーマネージドキーによるサーバー側暗号化を有効にするために Azure ポータルを使用する」を参照してください。
2. Azure ホスト接続および Azure Compute Gallery (ACG) のイメージバージョン用のイメージ定義を作成し、準備済みイメージを暗号化するための DES を指定します: 「イメージ定義と初期イメージバージョンを作成する」を参照してください。

3. 暗号化された準備済みイメージをリージョン、サブスクリプション、およびテナント間で共有します。Web Studio または PowerShell コマンドを使用できます。

暗号化された準備済みイメージが共有されているリソースにマシンカタログを作成できるようになりました。カタログの作成について詳しくは、「Azure で準備済みイメージのマシンカタログを作成する」を参照してください。

> **注:**
>
> - プライマリリージョンが暗号化されていない場合、共有リージョンも DES を持つことはできません。
> - 2つのホストユニットが同じリージョンをターゲットとする場合、それらは同じ DES を持ちます。

Web Studio を使用して、暗号化されたイメージをリージョン、サブスクリプション、およびテナント間で共有する

1. イメージバージョンを右クリックし、**Manage Image Share** を選択します。リージョンとディスク暗号化セットを持つリソースが一覧表示されます。
2. イメージバージョンと共有するリソースを選択します。イメージバージョンが作成された元のリソースは、いかなるアクションも無効になっています。リソースに対して DES が構成されていない場合は、ドロップダウンメニューから DES を選択します。

   > **注:**
   >
   > 同じリージョン内のリソースは、同じ暗号化キーを使用する必要があります。

3. 「**保存**」をクリックします。
4. 共有ステータスの詳細については、**Resources**タブをクリックします。

   > **注:**
   >
   > - イメージバージョンの共有のステータスが進行中の場合、**イメージバージョンの削除**または**イメージ共有の管理**のオプションは無効になります。

- リソースが正常に共有されると、DES は編集できません。

PowerShell を使用して、暗号化されたイメージをリージョン、サブスクリプション、およびテナント間で共有する

コマンド `Add-ProvImageVersionSpecHostingUnit` を使用し、パラメーター `CustomProperties` を追加します。`CustomProperties` で、ターゲットリソースの DES を構成します。準備された暗号化イメージを共有する場合、各リソースは、準備されたイメージが属するサブスクリプションから、そのリージョン内の DES を選択します。例:

```
$CustomProperties = "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">"

 "<Property xsi:type=`"StringProperty`" Name=`"DiskEncryptionSetId`"
Value=`"/subscriptions/xxxxxx-7152-46c4-b061-xxxxxx70c/resourceGroups/
resourcegroup1/providers/Microsoft.Compute/diskEncryptionSets/desid1`" /
>"+

 "</CustomProperties>"

Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid <Guid>
-HostingUnitUid <Guid> -CustomProperties $CustomProperties
```

詳細情報

- イメージ管理

次のステップ

- 準備済みイメージマシンカタログを管理する(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/manage-prepared-image-machine-catalogs.html)

Azure Local で準備済みイメージマシンカタログを作成する

準備済みイメージを作成し、その準備済みイメージを使用して、次の方法でMCSマシンカタログを作成します。

- ウェブスタジオ
- (#use-powershell)

準備済みイメージを使用して MCS マシンカタログを作成する主な手順は次のとおりです。

1. イメージ定義と初期イメージバージョンを作成します。
2. イメージバージョンを準備済みイメージとして使用してカタログを作成します。

Web Studio を使用する

イメージ定義と初期イメージバージョンを作成する

イメージ定義と初期イメージバージョンを作成するには、次の手順を実行します。

1. Web Studio から、**Images** ノードに移動し、**Create Image Definition** をクリックします。**Introduction** ページで **Next** をクリックします。
2. **イメージ定義**ページで、イメージ定義の**OSタイプ**と**セッションタイプ**を指定します。
3. 既存のリソースグループを選択するか、イメージリソースを保持するための新しいリソースグループを作成します。
4. **Image** ページで、**Resources** (設定された接続に適用可能なリソースのみが一覧表示されます)と、イメージバージョンを作成するためのテンプレートとして使用するイメージを選択します。

   > **注:**
   >
   > - イメージを選択する前に、マスターイメージにVDA 2311以降がインストールされており、MCSIOドライバーがVDAにインストールされていることを確認してください。
   > - イメージの選択では、Azure Local Gallery Image または仮想マシンを選択できます。

5. **Machine Specification** ページで、準備用VMのCPUとメモリを選択します。
6. **NICs** ページで、準備用イメージのNICを選択します。各NICについて、関連する仮想ネットワークを選択します。
7. 「**Version Description**」ページで、作成された初期イメージバージョンの説明を入力します。
8. 「**概要**」ページで、イメージ定義と作成された初期イメージバージョンの詳細を確認します。イメージ定義の名前と説明を入力します。「**完了**」をクリックします。

イメージバージョンを作成する

イメージバージョンを使用すると、特定のイメージに対するさまざまなイテレーションや更新を管理できます。この機能により、さまざまな目的のためにイメージの複数のバージョンを維持できます。

初期イメージバージョンからイメージバージョンを作成するには、次の手順を実行します。

> **注:**
>
> すべてのイメージバージョンのホスティングユニットは同じである必要があります。

1. 「**Images**」ノードに移動し、イメージバージョンまたはイメージ定義を選択して、「**Create Image Version**」をクリックします。
2. **Image Definition** ページで、ホスティングユニットを変更し、そのイメージバージョンのマスターイメージとマシンプロファイルを再選択できます。
3. イメージバージョンの構成を初期構成イメージバージョンと異なるものにする場合は、「**Create Image Version**」ダイアログの「**Machine Specification**」ページと「**NICs**」ページで設定を構成します。
4. イメージバージョンの説明を追加します。「**Finish**」をクリックします。

> **注：**
>
> 何らかの理由でイメージバージョンの作成に失敗した場合、下部にある**トラブルシューティング**タブに**再試行**オプションが表示されます。

「イメージ」ノードからマシンカタログを作成する

「**イメージ**」ノードの「**カタログの作成**」オプションを使用して、イメージバージョンでカタログを作成します。

または、「**マシンカタログ**」ノードでカタログを作成する際にバージョンを選択し、カタログ作成ワークフローで準備されたイメージオプションにリンクすることもできます。「マシンカタログ」ノードからマシンカタログを作成する(#create-a-machine-catalog-from-the-machine-catalogs-node)を参照してください。

「**イメージ**」ノードからMCSマシンカタログを作成するには、次の手順を実行します。

1. イメージバージョンを選択し、「**カタログの作成**」をクリックします。「**はじめに**」ページで「**次へ**」をクリックします。
2. **デスクトップエクスペリエンス**ページで、必要なデスクトップエクスペリエンスを選択します。

3. **Image** ページから **NICs** ページまで、設定は選択されたイメージバージョンに基づいて事前に選択されています。
4. **リソースグループ**ページで、新しいリソースグループを作成するか、既存のリソースグループを使用してこのカタログのリソースを配置するかを選択できます。
5. 次のページで設定を完了します。
6. **概要**ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。**完了**をクリックします。
7. 作成されたマシンカタログを表示するには、**マシンカタログ**ノードに移動します。

「マシンカタログ」ノードからマシンカタログを作成する

「**マシンカタログ**」ノードからMCSマシンカタログを作成するには、次の手順を実行します。

1. 左側のナビゲーションペインで**マシンカタログ**をクリックします。
2. 「**マシンカタログの作成**」をクリックします。「**マシンカタログのセットアップ**」ページが表示されます。「**はじめに**」ページと「**マシンの種類**」ページで「**次へ**」をクリックします。
3. **マシン管理**ページで:
    a. 「**電源管理されているマシン（仮想マシンやブレードPCなど）**」を選択します。
    b. 「**Citrixプロビジョニングテクノロジー**」を選択します。次に、「**Citrix Machine Creation Services™**」を選択します。
    c. **Resources** フィールドには、異なるゾーンに属するリソースが一覧表示されます。任意のAzureネットワークリソースを選択し、Next をクリックします。
4. **イメージ**ページで：
    - マスターイメージタイプの場合は、次の手順に従います:
        a. マスターイメージを選択します。
        b. マスターイメージの下で、イメージを選択します。ブレードには、リソースと同じリージョンに属するすべてのイメージが一覧表示されます。
        c. 「**完了**」をクリックします。
    - 「準備済みイメージ」タイプの場合、次の手順に従います。
        a. **準備済みイメージ**を選択します。
        b. 「**準備済みイメージ**」の下で、イメージ定義のイメージバージョンを選択します。必要に応じて、選択した準備済みイメージバージョンにメモを追加します。

c. イメージバージョン名をクリックします。選択したイメージバージョンの詳細を表示するには、下線が引かれているバージョン番号をクリックします。

5. 次のページで設定を構成します。
6. **リソースグループ**ページで、新しいリソースグループを作成するか、既存のリソースグループを使用してこのカタログのリソースを配置するかを選択できます。
7. 次のページで設定を完了します。
8. **概要**ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。**完了**をクリックします。

PowerShell を使用する

準備済みイメージを作成する

Azure Local 用の準備済みイメージバージョン仕様を作成するための詳細な PowerShell コマンドは次のとおりです。

1. `Test-ProvImageDefinitionNameAvailable command` を使用して、利用可能なイメージ定義名を確認します。例:

   ```
   Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string[]>
   ```

2. `New-ProvImageDefinition` コマンドを使用してイメージ定義を作成します。例:

   ```
   New-ProvImageDefinition -ImageDefinitionName arc-ACG-image-climber-demo
   -OsType Windows -VDASessionSupport SingleSession -Description "arc ACG
   image for arc"
   ```

3. `Add-ProvImageDefinitionConnection` コマンドを使用して、指定されたホスティング接続でイメージ定義の新しい構成を作成します。

   `Add-ProvImageDefinitionConnection` の `CustomProperties` には、次のものが含まれます。これらのパラメーターを使用しない場合、デフォルト値が使用されます。

   `ResourceGroups`: ベースディスクがあるリソースグループ。

   たとえば、顧客が提供するリソースグループの場合：

```
$CustomerOwnRsourceGroupProperties = @"

<CustomProperties xmlns="http:// schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="sz_res_group" />

</CustomProperties>

"@
```

```
Add-ProvImageDefinitionConnection -HypervisorConnectionName Azurelocal
-ImageDefinitionName arc-ACG-image-climber-demo [-CustomProperties
$CustomProperties]
```

4. `New-ProvImageVersion` コマンドを使用してイメージバージョンを作成します。例:

```
New-ProvImageVersion -ImageDefinitionName arc-ACG-image-climber-demo
```

5. `Add-ProvImageVersionSpec` コマンドを使用して、マスターイメージバージョン仕様をイメージバージョンに追加します。例:

```
Add-ProvImageVersionSpec -ImageVersionNumber 1 -HostingUnitName
network-2 -MasterImagePath XDHyp:
\HostingUnits\network-2\image.folder\MST-W11WS-2507-11-10-no-
sysprep.galleryimage
```

注:

ホスティングユニットのイメージバージョンには、マスターイメージバージョン仕様を1つだけ追加できます。

6. `New-ProvImageVersionSpec`コマンドを使用して、マスターイメージバージョン仕様から準備済みイメージバージョン仕様を作成します。例：

```
New-ProvImageVersionSpec -CustomProperties "<CustomProperties
xmlns=`"http://schemas.citrix.com/2014/xd/machinecreation`"
xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`"><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`" Value=`"citrix-
xd-39d65e7a-f6c0-4772-9e8d-d6eacb36287f-hilxi`" /><Property
xsi:type=`"StringProperty`" Name=`"OsType`" Value=`"Windows`" /></
CustomProperties>" -NetworkMapping @{"0"="XDHyp:
\HostingUnits\network-2\network.folder\VM-Network-2.network"}
-SourceImageVersionSpecUid "86c1a467-f900-4434-990a-c4ae39faca10"
```

イメージ定義、イメージバージョン、および準備済みイメージバージョン仕様を作成するための PowerShell コマンドの完全なセットの例:

```
## create image definition

New-ProvImageDefinition -ImageDefinitionName arc-ACG-image-climber-demo
-OsType Windows -VDASessionSupport SingleSession -Description "arc ACG
image for arc"

## create image definition connection

Add-ProvImageDefinitionConnection -CustomProperties "<CustomProperties
xmlns=`"http://schemas.citrix.com/2014/xd/machinecreation`"
xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`"></
CustomProperties>" -HypervisorConnectionUid "8eac2ad2-
fc81-45d6-9153-9545a779f8d2" -ImageDefinitionUid "39d65e7a-f6c0-4772-9e8d-
d6eacb36287f"

## create new image verison

New-ProvImageVersion -ImageDefinitionName arc-ACG-image-climber-demo

## select azure arc ACG image

Import-Module Citrix.Host.Commands

Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\network-2\image.folder")
| select-object fullpath

## add verison spec through Azure Arc ACG

Add-ProvImageVersionSpec -ImageVersionUid "29da7e07-b7e9-4c8c-
```

```
a5f2-4c03dbcba451" -HostingUnitUid "51305f67-34b3-4b22-a5d2-b6d7deaff9ba"
-MasterImagePath XDHyp:\HostingUnits\network-2\image.folder\MST-
W11WS-2507-11-10-no-sysprep.galleryimage

## create new version spec

New-ProvImageVersionSpec -CustomProperties "<CustomProperties
xmlns=`"http://schemas.citrix.com/2014/xd/machinecreation`"
xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`"><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`" Value=`"citrix-
xd-39d65e7a-f6c0-4772-9e8d-d6eacb36287f-hilxi`" /><Property
xsi:type=`"StringProperty`" Name=`"OsType`" Value=`"Windows`" /></
CustomProperties>" -NetworkMapping @{"0"="XDHyp:
\HostingUnits\network-2\network.folder\VM-Network-2.network"}
-SourceImageVersionSpecUid "86c1a467-f900-4434-990a-c4ae39faca10"
```

注:

- イメージ定義内のすべてのイメージバージョン仕様は、同じホスティングユニットに属している必要があります。
- イメージバージョンには、マスターイメージバージョン仕様を1つ、準備済みイメージバージョン仕様を1つだけ含めることができます。

準備済みイメージバージョン仕様を使用してカタログを作成する

`New-ProvScheme` コマンドを使用して、準備済みイメージバージョン仕様から MCS マシンカタログを作成します。例:

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-VMCpuCount <int>]
[-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping <Hashtable>] [-
CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-ServiceOffering
<string>] [-SecurityGroup <string[]>] [-TenancyType <string>] [-
MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>][-ImageAssignmentNote <string>]
```

または、,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitName <string> -IdentityPoolName <string> [-VMCpuCount
<int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping
<Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-
ServiceOffering <string>] [-SecurityGroup <string[]>] [-TenancyType
<string>] [-MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>][-ImageAssignmentNote <string>]
```

カタログを作成するための PowerShell コマンドの完全なセットの例:

```
New-AcctIdentityPool -IdentityPoolName arc-climbers-local -NamingScheme
"arc-c-vm-###" -NamingSchemeType Numeric -Domain "CLIMBERS.LOCAL"

New-ProvScheme -ProvisioningSchemeName arc-ACG-img-climber-3
-HostingUnitName network-2 -IdentityPoolName arc-climbers-local
-ImageVersionSpecUid 0525360d-6cb5-4f08-bb2c-aaf5678a0d54

New-BrokerCatalog -ProvisioningSchemeId 93fbcebd-3a7a-499e-9d8d-
c09e02021c5a -AllocationType Static -Name arc-ACG-img-climber-3
-PersistUserChanges OnLocal -ProvisioningType MCS -SessionSupport
SingleSession
```

詳細情報

- イメージ管理

次のステップ

- 準備済みイメージマシンカタログを管理する(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/manage-prepared-image-machine-catalogs.html)

Nutanix AHV Prism Central で準備済みイメージマシンカタログを作成する

準備済みイメージを作成し、その準備済みイメージを使用して、次の方法でMCSマシンカタログを作成します。

- (#use-powershell)

準備済みイメージを使用して MCS マシンカタログを作成する主な手順は次のとおりです。

1. イメージ定義と初期イメージバージョンを作成します。
2. イメージバージョンを準備済みイメージとして使用してカタログを作成します。

PowerShell を使用する

Nutanix PC におけるイメージデカップリングワークフローの PowerShell の例。

セットアップ

```
$CustomProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"><StringProperty Name="ClusterId"
Value="00062c63-1fb0-58c9-4fc8-5c2573352378"/></CustomProperties>'

$MasterImagePath="XDHyp:\HostingUnits\${HostingUnitName}
\Templates.folder\hai-vda-novtpm01.template\Initial
Version.templateversion"

$VMNetwork1A="XDHyp:\HostingUnits\${HostingUnitName}\Clusters.folder\mcs-
pvs-ntnx-cluster01.cluster\vmNwCl1-A.network"

$NetworkMapping=@{"0"=$VMNetwork1A}
```

イメージ定義とイメージバージョンを作成する

```
$ImageDefinition = New-ProvImageDefinition -ImageDefinitionName
$ImgDefName -OsType Windows -VdaSessionSupport SingleSession

$ImageVersion = New-ProvImageVersion -ImageDefinitionName
$ImageDefinition.ImageDefinitionName -Description "V1"

Add-ProvImageDefinitionConnection -ImageDefinitionName
$ImageDefinition.ImageDefinitionName -HypervisorConnectionName
$HostingConnection
```

イメージバージョンの仕様を作成する

```
$MasterImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
$ImageVersion.ImageDefinitionName -ImageVersionNumber
$ImageVersion.ImageVersionNumber -HostingUnitName $HostingUnitName
-MasterImagePath $MasterImagePath

$ProvTask = New-ProvImageVersionSpec -SourceImageVersionSpecUid
 $MasterImageVersionSpec.ImageVersionSpecUid -NetworkMapping
```

```
$NetworkMapping -MachineProfile $MachineProfile -CustomProperties
$CustomProperties -AdditionalStorageIds
00062c6d-09a3-134b-446d-58a2e17d0f88 -RunAsynchronously

$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
$ImgDefName -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"
```

プロビジョニングスキームを作成する

```
$ProvTask = New-ProvScheme -ProvisioningSchemeName $ProvSchemeName
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-HostingUnitName $HostingUnitName -IdentityPoolName $IdentityPoolName
-CleanOnBoot -Scope @() -SecurityGroup @() -NetworkMapping $NetworkMapping
-CustomProperties $CustomProperties -MachineProfile $MachineProfile
-RunAsynchronously
```

イメージバージョンの仕様を新しいクラスターにレプリケートする

```
Add-ProvImageVersionSpecInstance -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -StorageID
00062c6d-09a3-134b-446d-58a2e17d0f88
```

同じ準備済みイメージを使用して、新しいクラスターに新しいプロビジョニングスキームを作成する

```
$CustomProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"><StringProperty Name="ClusterId"
Value="00062c6d-09a3-134b-446d-58a2e17d0f88"/></CustomProperties>'

$ProvTask = New-ProvScheme -ProvisioningSchemeName $ProvSchemeName
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-MachineProfile $MachineProfile -HostingUnitName $HostingUnitName
-IdentityPoolName $IdentityPoolName -CleanOnBoot -Scope @() -SecurityGroup
@() -NetworkMapping $NetworkMapping -CustomProperties $CustomProperties
-RunAsynchronously
```

詳細情報

- イメージ管理

次のステップ

- 準備済みイメージを使用して作成されたカタログを管理する

Red Hat OpenShift で準備済みイメージマシンカタログを作成する

準備済みイメージを作成し、その準備済みイメージを使用して、次の方法でMCSマシンカタログを作成します。

- ウェブスタジオ
- (#use-powershell)

準備済みイメージを使用して MCS マシンカタログを作成する主な手順は次のとおりです。

1. イメージ定義と初期イメージバージョンを作成します。
2. イメージバージョンを準備済みイメージとして使用してカタログを作成します。

Web Studio を使用する

イメージ定義と初期イメージバージョンを作成する

イメージ定義と初期イメージバージョンを作成するには、次の手順を実行します。

1. Studioから、**イメージ**ノードに移動し、**イメージ定義の作成**をクリックします。**はじめに**ページで**次へ**をクリックします。
2. **イメージ定義**ページで、イメージ定義の**OSタイプ**と**セッションタイプ**を指定します。
3. **［イメージ］ページで、［リソース］**（設定された接続に適用可能なリソースのみが一覧表示されます）と、イメージバージョンを作成するためのテンプレートとして使用するマスターイメージを選択します。**［マシンプロファイルを使用する］**チェックボックスをオンにして、マシンプロファイルを選択できます。

   > **注:**
   >
   > イメージを選択する前に、マスターイメージにVDA 2311以降がインストールされており、MCSIOドライバーがVDAにインストールされていることを確認してください。

4. 「**マシン仕様**」ページで、マシンサイズを選択します。マシンプロファイルを選択した場合、そのマシンプロファイルから派生した仮想CPUカウントが表示され、変更することはできません。マシンプロファイルを選択しない場合、マスターイメージから派生したメモリサイズのみが表示されます。

5. 「**NIC**」ページで、準備イメージのNICを選択します。各NICについて、関連する仮想ネットワークを選択します。ホスティングユニットに関連付けられたNICは、デフォルトで選択されています。
6. 「**Version Description**」ページで、作成された初期イメージバージョンの説明を入力します。
7. 「**概要**」ページで、イメージ定義と作成された初期イメージバージョンの詳細を確認します。イメージ定義の名前と説明を入力します。「**完了**」をクリックします。

イメージバージョンを作成する

イメージバージョンを使用すると、特定のイメージに対するさまざまなイテレーションや更新を管理できます。この機能により、さまざまな目的のためにイメージの複数のバージョンを維持できます。

初期イメージバージョンからイメージバージョンを作成するには、次の手順を実行します。

1. 「**Images**」ノードに移動し、イメージバージョンまたはイメージ定義を選択して、「**Create Image Version**」をクリックします。
2. 「**イメージ**」ページで、このイメージバージョンのマスターイメージを再選択できます。
3. イメージバージョンの構成を初期構成イメージバージョンと異なるものにする場合は、「**Create Image Version**」ダイアログの「**Machine Specification**」ページと「**NICs**」ページで設定を構成します。
4. イメージバージョンの説明を追加します。「**Finish**」をクリックします。

> **注:**
>
> 何らかの理由でイメージバージョンの作成に失敗した場合、下部にある**トラブルシューティング**タブに**再試行**オプションが表示されます。

「イメージ」ノードからマシンカタログを作成する

「**イメージ**」ノードの「**カタログの作成**」オプションを使用して、イメージバージョンでカタログを作成します。

または、**マシンカタログ**ノードでカタログを作成する際にバージョンを選択し、カタログ作成ワークフローで準備済みイメージオプションにリンクできます。「マシンカタログノードからマシンカタログを作成する」を参照してください。(#create-a-machine-catalog-from-the-machine-catalogs-node)

「**イメージ**」ノードからMCSマシンカタログを作成するには、次の手順を実行します。

1. イメージバージョンを選択し、「**カタログの作成**」をクリックします。「**はじめに**」ページで「**次へ**」をクリックします。
2. **マシン管理**ページで**次へ**をクリックします。
3. **デスクトップエクスペリエンス**ページで、必要なデスクトップエクスペリエンスを選択します。
4. **イメージ**ページから**仮想マシン**ページまで、設定は選択したイメージバージョンに基づいて事前に選択されています。
5. 次のページで設定を完了します。
6. **概要**ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。**完了**をクリックします。
7. 作成されたマシンカタログを表示するには、**マシンカタログ**ノードに移動します。

「マシンカタログ」ノードからマシンカタログを作成する

マシンカタログノードからMCSマシンカタログを作成するには、次の手順を実行します。

1. 左側のナビゲーションペインで**マシンカタログ**をクリックします。
2. **マシンカタログの作成**をクリックします。**マシンカタログのセットアップ**ページが表示されます。**はじめに**、**マシンタイプ**、**マシン管理**の各ページで**次へ**をクリックします。
3. **イメージ**ページで：
   a. **準備済みイメージ**を選択します。
   b. 「**準備済みイメージ**」の下で、イメージ定義のイメージバージョンを選択します。
   c. イメージバージョン名をクリックします。選択したイメージバージョンの詳細を表示するには、下線が引かれているバージョン番号をクリックします。
4. 次のページで設定を構成します。
5. **概要**ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。**完了**をクリックします。

PowerShell を使用する

準備済みイメージを作成する

準備済みイメージバージョン仕様を作成するための詳細な PowerShell コマンドは次のとおりです。

1. `Test-ProvImageDefinitionNameAvailable command` を使用して、利用可能なイメージ定義名を確認します。例:

```
Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string[]>
```

2. `New-ProvImageDefinition` コマンドを使用してイメージ定義を作成します。例:

```
New-ProvImageDefinition -ImageDefinitionName image2 -OsType Windows
-VdaSessionSupport SingleSession
```

3. `Add-ProvImageDefinitionConnection`コマンドを使用して、指定されたホスティング接続でイメージ定義の新しい構成を作成します。例：

```
Add-ProvImageDefinitionConnection -ImageDefinitionUid
$imageDef.ImageDefinitionUid -HypervisorConnectionUid
"00000000-0000-0000-0000-000000000000"
```

4. `New-ProvImageVersion` コマンドを使用してイメージバージョンを作成します。例:

```
New-ProvImageVersion -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -Description "version 1"
```

5. `Add-ProvImageVersionSpec` コマンドを使用して、マスターイメージバージョン仕様をイメージバージョンに追加します。例:

```
Add-ProvImageVersionSpec -MasterImagePath "XDHyp:
\HostingUnits\YourHostingUnitName\YourMasterImage.vm" -HostingUnitUid
"11111111-1111-1111-1111-111111111111" -ImageVersionUid
$imageVersion.ImageVersionUid
```

> **注:**
>
> ホスティングユニットのイメージバージョンには、マスターイメージバージョン仕様を1つだけ追加できます。

6. `New-ProvImageVersionSpec`コマンドを使用して、マスターイメージバージョン仕様から準備済みイメージバージョン仕様を作成します。例：

```
New-ProvImageVersionSpec -SourceImageVersionSpecUid
$masterImageVersionSpec.ImageVersionSpecUid -NetworkMapping @{"1" =
"XDHyp:
\HostingUnits\YourHostingUnitName\YourNamespaceName.namespace\YourNetwo
rkAttachmentDefinition.network" }
```

イメージ定義、イメージバージョン、および準備済みイメージバージョン仕様を作成するための PowerShell コマンドの完全なセットの例:

```
$imageDef = New-ProvImageDefinition -ImageDefinitionName "ImageDefinition"
-OsType "Windows" -VDASessionSupport "MultiSession"




$task = Add-ProvImageDefinitionConnection -ImageDefinitionUid
$imageDef.ImageDefinitionUid -HypervisorConnectionUid
"00000000-0000-0000-0000-000000000000"



$imageVersion = New-ProvImageVersion -ImageDefinitionName
"ImageDefinition"




$masterImageVersionSpec = Add-ProvImageVersionSpec -MasterImagePath
"XDHyp:\HostingUnits\YourHostingUnitName\YourMasterImage.vm"
-HostingUnitUid "11111111-1111-1111-1111-111111111111" -ImageVersionUid
$imageVersion.ImageVersionUid




$newProvImageVersionSpecResult = New-ProvImageVersionSpec
-SourceImageVersionSpecUid $masterImageVersionSpec.ImageVersionSpecUid
-NetworkMapping @{"1" = "XDHyp:
```

```
\HostingUnits\YourHostingUnitName\YourNamespaceName.namespace\YourNetworkA
ttachmentDefinition.network" }
```

注:

- イメージ定義内のすべてのイメージバージョン仕様は、同じホスティングユニットに属している必要があります。
- イメージバージョンには、マスターイメージバージョン仕様を1つ、準備済みイメージバージョン仕様を1つだけ含めることができます。
- すべてのイメージバージョン仕様はマシンプロファイルを持つか、またはどのイメージバージョン仕様もマシンプロファイルを持たないかのいずれかである必要があります。

準備済みイメージバージョン仕様を使用してカタログを作成する

`New-ProvScheme` コマンドを使用して、準備済みイメージバージョン仕様から MCS マシンカタログを作成します。例:

```
$getProvImageVersionSpecResult = Get-ProvImageVersionSpec
-ImageVersionSpecUid $newProvImageVersionSpecResult.ImageVersionSpecUid



New-ProvScheme -ImageVersionSpecUid
$newProvImageVersionSpecResult.ImageVersionSpecUid -ProvisioningSchemeName
"ProvSchemeImageDecoupling" -HostingUnitName "YourHostingUnitName"
-IdentityPoolName "YourIdentityPoolName" -NetworkMapping @{"1" = "XDHyp:
\HostingUnits\YourHostingUnitName\YourNamespaceName.namespace\YourNetworkA
ttachmentDefinition.network"}
```

詳細情報

- イメージ管理

次のステップ

- 準備済みイメージマシンカタログを管理する(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/manage-prepared-image-machine-catalogs.html)

VMware で準備済みイメージのマシンカタログを作成する

準備済みイメージを作成し、その準備済みイメージを使用して、次の方法でMCSマシンカタログを作成します。

- ウェブスタジオ
- (#use-powershell)

準備済みイメージを使用して MCS マシンカタログを作成する主な手順は次のとおりです。

1. イメージ定義と初期イメージバージョンを作成します。
2. イメージバージョンを準備済みイメージとして使用してカタログを作成します。

Web Studio を使用する

イメージ定義と初期イメージバージョンを作成する

イメージ定義と初期イメージバージョンを作成するには、次の手順を実行します。

1. Studioから、**イメージ**ノードに移動し、**イメージ定義の作成**をクリックします。**はじめに**ページで**次へ**をクリックします。
2. **イメージ定義**ページで、イメージ定義の**OSタイプ**と**セッションタイプ**を指定します。
3. **［イメージ］ページで、［リソース］**（設定された接続に適用可能なリソースのみが一覧表示されます）と、イメージバージョンを作成するためのテンプレートとして使用するマスターイメージを選択します。**［マシンプロファイルを使用する］**チェックボックスをオンにして、マシンプロファイルを選択できます。

   > **注:**
   >
   > イメージを選択する前に、マスターイメージにVDA 2311以降がインストールされており、MCSIOドライバーがVDAにインストールされていることを確認してください。

4. 「**マシン仕様**」ページで、マシンサイズを選択します。マシンプロファイルを選択した場合、そのマシンプロファイルから派生した仮想CPUカウントが表示され、変更することはできません。マシンプロファイルを選択しない場合、マスターイメージから派生したメモリサイズのみが表示されます。
5. **NIC** ページで、準備イメージの NIC を選択または追加します。各 NIC について、関連付けられた仮想ネットワークを選択します。マシンプロファイルを選択しない場合、マスターイメー

ジに関連付けられた NIC がデフォルトで選択されます。マシンプロファイルを選択した場合、NIC はマシンプロファイルから派生し、その数は変更できません。

6. 「**Version Description**」ページで、作成された初期イメージバージョンの説明を入力します。
7. 「**概要**」ページで、イメージ定義と作成された初期イメージバージョンの詳細を確認します。イメージ定義の名前と説明を入力します。「**完了**」をクリックします。

イメージバージョンを作成する

イメージバージョンを使用すると、特定のイメージに対するさまざまなイテレーションや更新を管理できます。この機能により、さまざまな目的のためにイメージの複数のバージョンを維持できます。

初期イメージバージョンからイメージバージョンを作成するには、次の手順を実行します。

1. 「**Images**」ノードに移動し、イメージバージョンまたはイメージ定義を選択して、「**Create Image Version**」をクリックします。
2. **イメージ** ページで、同じホスティング接続内のホスティングユニットを変更し、そのイメージバージョン用のマスターイメージとマシンプロファイルを再選択できます。
3. イメージバージョンの構成を初期構成イメージバージョンと異なるものにする場合は、「**Create Image Version**」ダイアログの「**Machine Specification**」ページと「**NICs**」ページで設定を構成します。
4. イメージバージョンの説明を追加します。「**Finish**」をクリックします。

> **注:**
>
> 何らかの理由でイメージバージョンの作成に失敗した場合、下部にある**トラブルシューティング**タブに**再試行**オプションが表示されます。

準備済みイメージを共有する

前提条件

準備済みイメージの共有は、コールドマイグレーションを使用して vCenter Server インスタンス間でイメージを複製します。異なるホスティング接続に属するホスティングユニットには、次の前提条件が適用されます。

- vCenter Server 間でのコールドマイグレーション: コールドマイグレーションには、両方の環境でクロス vCenter マイグレーションのサポートが必要です。

- 両方の vCenter Server は vSphere 7.0 以降 (vSphere 8.0+ を推奨) を実行している必要があります。
- 拡張リンクモードは不要です。

ポート要件: マイグレーションのために次のポートが開いていることを確認してください。

送信元	宛先	ポート	プロトコル	目的
ソース vCenter Server	ターゲット vCenter Server	443	TCP	vCenter 間での API 通信
ソースESXiホスト	ターゲット ESXiホスト	902	TCP	NFC (Network File Copy) データ転送
ソースESXiホスト	ターゲット ESXiホスト	8000	TCP	vMotionトラフィック

> **注:**
>
> ポートは双方向に開いている必要があります。移行では主にデータにNFC (ポート902) を、管理にポート443を使用します。パスによってはポート8000が使用される場合があります。クローン操作中、ソースvCenterはターゲットのSSL証明書サムプリントを検証する必要があります。

> VMkernelアダプターの構成:

ESXIホスト	必要なサービス
ソースESXiホスト	プロビジョニングまたは管理
ターゲットESXiホスト	ソースと同じサービス (プロビジョニングまたは管理)

両側でVMkernelアダプターに同じトラフィックサービス（プロビジョニングまたは管理）を有効にする必要があります。不一致は移行の失敗を引き起こします。

vSphere Client を使用して、**Host > Configure > Networking > VMkernel adapters** の設定を確認します。

既知の制限事項：カスタムストレージポリシーは、vCenter間レプリケーション中に保持されません。ターゲットデータストアのデフォルトストレージポリシーが適用されます。

- vTPM対応マシンプロファイル：キープロバイダーの互換性。vTPMを持つプロファイルの場合、両方のvCenter Serverが互換性のあるキープロバイダーにアクセスできる必要があります。

要件	詳細
同じキープロバイダーへのアクセス	宛先vCenterは、ソースと同じキープロバイダーにアクセスできるか、Native Key Providerをブリッジとして使用する必要があります。
キーマテリアル	外部KMSの場合：両方のvCenterは同じKMSクラスター（またはキーマテリアルを共有するKMSクラスター）に登録されている必要があります。
ネイティブキープロバイダー	両方のvCenter ServerでNative Key Providerを構成します。各vCenterのNative Key Providerは独立していますが、vSphereはvCenter間操作のためにこの組み合わせを受け入れます。ソースと宛先が外部KMSを共有しない場合、Native Key Providerはブリッジとしても機能できます。Native Key Providerは、使用前に両方のvCenterでバックアップする必要があります。

注:

Native Key Providerは最もシンプルなオプションです。両方のサーバーで構成し、バックアップしてください。外部KMSを使用する場合は、両方のvCenterが同じクラスターまたはキーマテリアルを共有していることを確認してください。**vTPM対応カタログのイメージ共有を有効にする前に、vSphere ClientのvCenter > Configure > Security > Key Providersでキープロバイダーの構成を確認してください。**

異なるホストユニット間で準備済みイメージを共有する

異なるホスティングユニット間で準備済みイメージを共有するには、次の手順に従います。

1. イメージバージョンを右クリックし、**Manage Image Share**を選択します。VMware環境内のすべてのホスティングユニットが表示されます。イメージバージョンが作成されたリソースは、いかなる操作も無効になっています。
2. イメージを共有するホスティングユニットを選択し、「**保存**」をクリックします。「**共有ステータス**」列に「**進行中**」と表示されます。
3. 下部にある「**リソース**」タブをクリックして、共有ステータスの詳細を確認します。

注:

イメージバージョンの共有ステータスが進行中の場合、「**イメージバージョンの削除**」または「**イメージ共有の管理**」オプションは無効になります。 別のVMware接続のホスティングユニットとイメージを共有するには、次の要件が満たされていることを確認してください。

- 2つの接続が相互に通信できること。
- ハイパーバイザーのバージョンが一致していること。
- プロビジョニングサービスが、ソースホストとターゲットホストの両方の管理VMkernelアダプターで有効になっていること。VMware vSphere Clientでのナビゲーションパスは「**ホスト > 構成 > ネットワーク > VMkernelアダプター**」です。

「イメージ」ノードからマシンカタログを作成する

「**イメージ**」ノードの「**カタログの作成**」オプションを使用して、イメージバージョンでカタログを作成します。

または、**マシンカタログ**ノードでカタログを作成する際にバージョンを選択し、カタログ作成ワークフローで準備済みイメージオプションにリンクできます。「マシンカタログノードからマシンカタログを作成する」を参照してください。(#create-a-machine-catalog-from-the-machine-catalogs-node)

「**イメージ**」ノードからMCSマシンカタログを作成するには、次の手順を実行します。

1. イメージバージョンを選択し、「**カタログの作成**」をクリックします。「**はじめに**」ページで「**次へ**」をクリックします。
2. **デスクトップエクスペリエンス**ページで、必要なデスクトップエクスペリエンスを選択します。

3. **イメージ**ページから**仮想マシン**ページまで、設定は選択したイメージバージョンに基づいて事前に選択されています。
4. 次のページで設定を完了します。
5. **概要**ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。**完了**をクリックします。
6. 作成されたマシンカタログを表示するには、**マシンカタログ**ノードに移動します。

「マシンカタログ」ノードからマシンカタログを作成する

マシンカタログノードからMCSマシンカタログを作成するには、次の手順を実行します。

1. 左側のナビゲーションペインで**マシンカタログ**をクリックします。
2. **マシンカタログの作成**をクリックします。**マシンカタログのセットアップ**ページが表示されます。**はじめに**、**マシンタイプ**、**マシン管理**の各ページで**次へ**をクリックします。
3. **イメージ**ページで：
    a. **準備済みイメージ**を選択します。
    b. 「**準備済みイメージ**」の下で、イメージ定義のイメージバージョンを選択します。
    c. イメージバージョン名をクリックします。選択したイメージバージョンの詳細を表示するには、下線が引かれているバージョン番号をクリックします。
    d. 選択したイメージバージョンがマシンプロファイルで構成されている場合は、マシンプロファイルを選択します。選択したイメージバージョンがマシンプロファイルで構成されていない場合、マシンプロファイルを使用することはできません。
4. 次のページで設定を構成します。
5. **概要**ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。**完了**をクリックします。

PowerShell を使用する

準備済みイメージを作成する

準備済みイメージバージョン仕様を作成するための詳細な PowerShell コマンドは次のとおりです。

1. `Test-ProvImageDefinitionNameAvailable command` を使用して、利用可能なイメージ定義名を確認します。例:

```
Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string[]>
```

2. `New-ProvImageDefinition` コマンドを使用してイメージ定義を作成します。例:

```
New-ProvImageDefinition -ImageDefinitionName image2 -OsType Windows
-VdaSessionSupport SingleSession
```

3. `Add-ProvImageDefinitionConnection`コマンドを使用して、指定されたホスティング接続でイメージ定義の新しい構成を作成します。例：

```
Add-ProvImageDefinitionConnection -ImageDefinitionName image2
-HypervisorConnectionName VMware
```

4. `New-ProvImageVersion` コマンドを使用してイメージバージョンを作成します。例:

```
New-ProvImageVersion -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -Description "version 1"
```

5. `Add-ProvImageVersionSpec` コマンドを使用して、マスターイメージバージョン仕様をイメージバージョンに追加します。例:

```
$MasterImagePath = "XDHyp:\HostingUnits\vmware\win10-master.vm\win10-
master-snap.snapshot"

$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
$ImageVersion.ImageDefinitionName -ImageVersionNumber
$ImageVersion.ImageVersionNumber -HostingUnitName vmware
-MasterImagePath $MasterImagePath
```

> **注:**
>
> ホスティングユニットのイメージバージョンには、マスターイメージバージョン仕様を1つだけ追加できます。

6. `New-ProvImageVersionSpec`コマンドを使用して、マスターイメージバージョン仕様から準備済みイメージバージョン仕様を作成します。例：

```
New-ProvImageVersionSpec -SourceImageVersionSpecUid
 $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping
@{"0"="XDHyp:\HostingUnits\vmware\\DSwitch-VM Network.network"}
-VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously
```

7. 同じホスティング接続内の別のホスティングユニットと、準備されたイメージバージョンの仕様を`Add-ProvImageVersionSpecHostingUnit`コマンドを使用して共有することもできます。例:

```
Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx
-HostingUnitName VMwareabc
```

イメージ定義、イメージバージョン、および準備済みイメージバージョン仕様を作成するための PowerShell コマンドの完全なセットの例:

```
New-ProvImageDefinition -ImageDefinitionName image2 -OsType Windows
-VdaSessionSupport Single



Add-ProvImageDefinitionConnection -ImageDefinitionName image2
-HypervisorConnectionName VMware



$imageVersion = New-ProvImageVersion -ImageDefinitionName image2



$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid `

    -HostingUnitUid $hostingunit.HostingUnitUid `

    -MasterImagePath "XDHyp:\HostingUnits\vmware\shuaiz-win10-
master.vm\shuaiz-win10-master-snap.snapshot"



New-ProvImageVersionSpec -SourceImageVersionSpecUid
$SourceImageVersionSpec.ImageVersionSpecUid `
```

```
    -NetworkMapping @{"0"="XDHyp:\HostingUnits\vmware\\DSwitch-
VMNetwork.network"} `

    -VMCpuCount 2 -VMMemoryMB 4096




Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx
-HostingUnitName VMwareabc

 $PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid | Where SourceImageVersionSpecUid-eq
$SourceImageVersionSpec.ImageVersionSpecUid
```

注:

- イメージ定義内のすべてのイメージバージョン仕様は、同じホスティングユニットに属している必要があります。
- イメージバージョンには、マスターイメージバージョン仕様を1つ、準備済みイメージバージョン仕様を1つだけ含めることができます。
- すべてのイメージバージョン仕様はマシンプロファイルを持つか、またはどのイメージバージョン仕様もマシンプロファイルを持たないかのいずれかである必要があります。

準備済みイメージバージョン仕様を使用してカタログを作成する

`New-ProvScheme` コマンドを使用して、準備済みイメージバージョン仕様から MCS マシンカタログを作成します。例:

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-VMCpuCount <int>]
[-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping <Hashtable>] [-
CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-ServiceOffering
<string>] [-SecurityGroup <string[]>] [-TenancyType <string>] [-
MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
```

```
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>][-ImageAssignmentNote <string>]
```

または、,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitName <string> -IdentityPoolName <string> [-VMCpuCount
<int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping
<Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-
ServiceOffering <string>] [-SecurityGroup <string[]>] [-TenancyType
<string>] [-MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>][-ImageAssignmentNote <string>]
```

VMwareで準備されたイメージバージョンの仕様を使用してカタログを作成する例:

```
New-ProvScheme -ProvisioningSchemeName assignimage -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid `

    -HostingUnitName $hostingunit.c-IdentityPoolName
$IdentityPool.IdentityPoolName `

    -CleanOnBoot -Scope @() -SecurityGroup @() -VMCpuCount 2 -VMMemoryMB
8192 `

    -NetworkMapping @{"0"="XDHyp:\HostingUnits\vmware\\DSwitch-VM
Network.network"}
```

カタログを作成するためのPowershellコマンドの完全なセットの例：

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" -Name "vmwarecatalog" -PersistUserChanges
"Discard" -ProvisioningType "MCS" -Scope @() -SessionSupport
"MultiSession"

$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain
"vmware.local" -IdentityPoolName "vmwarecatalog" -IdentityType
"ActiveDirectory"  -NamingScheme "vmware##" -NamingSchemeType "Numeric"
-Scope @()
```

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image2 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"

$Task = New-ProvScheme -ProvisioningSchemeName vmwarecatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-HostingUnitName vmware -IdentityPoolName vmwarecatalog -CleanOnBoot
-Scope @() -SecurityGroup @() -NetworkMapping @{"0"="XDHyp:
\HostingUnits\vmware\\DSwitch-VM Network.network"} -VMCpuCount 2
-VMMemoryMB 4096 -RunAsynchronously

Get-ProvTask -TaskId $Task.TaskId

$ProvScheme = Get-ProvScheme -ProvisioningSchemeName vmwarecatalog

Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

詳細情報

- イメージ管理

次のステップ

- 準備済みイメージマシンカタログを管理する(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/manage-prepared-image-machine-catalogs.html)

XenServer® で準備済みイメージのマシンカタログを作成する

準備済みイメージを作成し、その準備済みイメージを使用して、次の方法でMCSマシンカタログを作成します。

- ウェブスタジオ
- (#use-powershell)

準備済みイメージを使用して MCS マシンカタログを作成する主な手順は次のとおりです。

1. イメージ定義と初期イメージバージョンを作成します。
2. イメージバージョンを準備済みイメージとして使用してカタログを作成します。

Web Studio を使用する

イメージ定義と初期イメージバージョンを作成する

イメージ定義と初期イメージバージョンを作成するには、次の手順を実行します。

1. Studioから、**イメージ**ノードに移動し、**イメージ定義の作成**をクリックします。**はじめに**ページで**次へ**をクリックします。
2. **イメージ定義**ページで、イメージ定義の**OSの種類**、**セッションの種類**、および**接続**を指定します。
3. **イメージ**ページで、**リソース**（設定された接続に適用可能なリソースのみが一覧表示されます）と、イメージバージョンを作成するためのテンプレートとして使用するマスターイメージを選択します。

   > **注:**
   >
   > - イメージを選択する前に、マスターイメージにVDA 2311以降がインストールされており、MCSIOドライバーがVDAにインストールされていることを確認してください。

4. **マシン仕様**ページには、マスターイメージから派生したメモリサイズのみが表示され、必要に応じて変更できます。
5. **NIC**ページで、準備イメージのNICを選択します。各NICについて、関連付けられた仮想ネットワークを選択します。マスターイメージに関連付けられたNICがデフォルトで選択されています。
6. 「**Version Description**」ページで、作成された初期イメージバージョンの説明を入力します。
7. 「**概要**」ページで、イメージ定義と作成された初期イメージバージョンの詳細を確認します。イメージ定義の名前と説明を入力します。「**完了**」をクリックします。

イメージバージョンを作成する

イメージバージョンを使用すると、特定のイメージに対するさまざまなイテレーションや更新を管理できます。この機能により、さまざまな目的のためにイメージの複数のバージョンを維持できます。

初期イメージバージョンからイメージバージョンを作成するには、次の手順を実行します。

1. 「**Images**」ノードに移動し、イメージバージョンまたはイメージ定義を選択して、「**Create Image Version**」をクリックします。
2. **イメージ**ページで、ホスティングユニットを変更し、必要に応じてマスターイメージを再選択します。
3. 初期イメージバージョンとは異なる設定を使用するには、**イメージバージョンの作成**ダイアログの**マシン仕様**ページと**NIC**ページで設定を構成します。
4. イメージバージョンの説明を追加します。「**Finish**」をクリックします。

> **注:**
>
> 何らかの理由でイメージバージョンの作成に失敗した場合、下部にある**トラブルシューティング**タブに**再試行**オプションが表示されます。

共有準備済みイメージ

XenServer の異なるホストユニット間で準備済みイメージを共有するには、次の手順に従います。

1. イメージバージョンを右クリックし、**イメージ共有の管理**を選択します。選択した接続下のすべてのホストユニットが一覧表示されます。イメージバージョンが作成されたリソースは、すべてのアクションに対して無効になっています。
2. イメージを共有するホストユニットを選択し、**保存**をクリックします。**共有ステータス**列に**進行中**と表示されます。
3. 共有ステータスの詳細については、**Resources**タブをクリックします。

> **注:**
>
> イメージバージョンの共有ステータスが進行中の場合、イメージバージョンの削除またはイメージ共有の管理オプションは無効になります。

「イメージ」ノードからマシンカタログを作成する

「**イメージ**」ノードの「**カタログの作成**」オプションを使用して、イメージバージョンでカタログを作成します。

または、**マシンカタログ**ノードでカタログを作成する際にバージョンを選択し、カタログ作成ワークフローで準備済みイメージオプションにリンクできます。「マシンカタログノードからマシンカタログを作成する」を参照してください。(#create-a-machine-catalog-from-the-machine-catalogs-node)

「**イメージ**」ノードからMCSマシンカタログを作成するには、次の手順を実行します。

1. イメージバージョンを選択し、「**カタログの作成**」をクリックします。「**はじめに**」ページで「**次へ**」をクリックします。
2. **マシン管理**ページで、ホスティングユニットを選択し、**次へ**をクリックします。
3. **デスクトップエクスペリエンス**ページで、必要なデスクトップエクスペリエンスを選択します。
4. 「**イメージ**」ページから「**仮想マシン**」ページまで、設定は選択されたイメージバージョンに基づいて事前に選択されています。
5. 次のページで設定を完了します。
6. **概要**ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。**完了**をクリックします。
7. 作成されたマシンカタログを表示するには、**マシンカタログ**ノードに移動します。

「マシンカタログ」ノードからマシンカタログを作成する

マシンカタログノードからMCSマシンカタログを作成するには、次の手順を実行します。

1. 左側のナビゲーションペインで**マシンカタログ**をクリックします。
2. **マシンカタログの作成**をクリックします。**マシンカタログのセットアップ**ページが表示されます。**はじめに**、**マシンタイプ**、**マシン管理**の各ページで**次へ**をクリックします。
3. **イメージ**ページで：
    a. **準備済みイメージ**を選択します。
    b. 「**準備済みイメージ**」の下で、イメージ定義のイメージバージョンを選択します。
    c. イメージバージョンを選択します。選択したイメージバージョンの詳細を表示するには、下線が引かれているバージョン番号をクリックします。
4. 次のページで設定を完了します。
5. **概要**ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。**完了**をクリックします。

PowerShell を使用する

準備済みイメージを作成する

準備済みイメージバージョン仕様を作成するための詳細な PowerShell コマンドは次のとおりです。

1. `Test-ProvImageDefinitionNameAvailable command` を使用して、利用可能なイメージ定義名を確認します。例:

```
Test-ProvImageDefinitionNameAvailable -ImageDefinitionName xenimage1
```

2. `New-ProvImageDefinition` コマンドを使用してイメージ定義を作成します。例:

```
$ImageDefintion = New-ProvImageDefinition -ImageDefinitionName
xenimage1 -OsType Windows -VdaSessionSupport SingleSession
```

3. `Add-ProvImageDefinitionConnection` コマンドを使用して、指定されたホスティング接続でイメージ定義の新しい構成を作成します。

```
Add-ProvImageDefinitionConnection -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -HypervisorConnectionName
XenServer1
```

4. `New-ProvImageVersion` コマンドを使用してイメージバージョンを作成します。例:

```
$ImageVersion = New-ProvImageVersion -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -Description "version 1"
```

5. `Add-ProvImageVersionSpec` コマンドを使用して、マスターイメージバージョン仕様をイメージバージョンに追加します。例:

```
$MasterImagePath = "XDHyp:\HostingUnits\xenhu \win10-master.vm\win10-
master-snap.snapshot"

$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -ImageVersionNumber
$ImageVersion.ImageVersionNumber -HostingUnitName xenhu
-MasterImagePath $MasterImagePath
```

> **注:**
>
> ホスティングユニットのイメージバージョンには、マスターイメージバージョン仕様を1つだけ追加できます。

6. `New-ProvImageVersionSpec`コマンドを使用して、マスターイメージバージョン仕様から準備済みイメージバージョン仕様を作成します。例：

```
New-ProvImageVersionSpec -SourceImageVersionSpecUid
 $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping
@{"0"="XDHyp:\HostingUnits\xenhu\VM Network.network"}

-VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously
```

7. 同じホスティング接続内の別のホスティングユニットと、`Add-ProvImageVersionSpecHostingUnit`コマンドを使用して準備済みイメージバージョンの仕様を共有することもできます。例：

```
Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx
-HostingUnitName xenhu2
```

イメージ定義、イメージバージョン、および準備済みイメージバージョン仕様を作成するためのPowerShell コマンドの完全なセットの例:

```
$ImageDefintion = New-ProvImageDefinition -ImageDefinitionName xenimage1
-OsType Windows -VdaSessionSupport SingleSession




Add-ProvImageDefinitionConnection -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -HypervisorConnectionName XenServer1



$ImageVersion = New-ProvImageVersion -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -Description "version 1"
```

```
$MasterImagePath = "XDHyp:\HostingUnits\xenhu \win10-master.vm\win10-
master-snap.snapshot"



$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -ImageVersionNumber
$ImageVersion.ImageVersionNumber -HostingUnitName xenhu -MasterImagePath
$MasterImagePath




New-ProvImageVersionSpec -SourceImageVersionSpecUid
 $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping @{"0"="XDHyp:
\HostingUnits\xenhu\VM Network.network"}

 -VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously



Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx
-HostingUnitName xenhu2
```

注:

- イメージバージョンには、マスターイメージバージョン仕様を1つ、準備済みイメージバージョン仕様を1つだけ含めることができます。
- すべてのイメージバージョン仕様はマシンプロファイルを持つか、またはどのイメージバージョン仕様もマシンプロファイルを持たないかのいずれかである必要があります。

準備済みイメージバージョン仕様を使用してカタログを作成する

`New-ProvScheme` コマンドを使用して、準備済みイメージバージョン仕様から MCS マシンカタログを作成します。例:

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-VMCpuCount <int>]
[-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping <Hashtable>] [-
CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-ServiceOffering
<string>] [-SecurityGroup <string[]>] [-TenancyType <string>] [-
MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>]
```

または、,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitName <string> -IdentityPoolName <string> [-VMCpuCount
<int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping
<Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-
ServiceOffering <string>] [-SecurityGroup <string[]>] [-TenancyType
<string>] [-MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>]
```

XenServer で準備済みイメージバージョンの仕様を使用してカタログを作成する例：

```
New-ProvScheme -ProvisioningSchemeName assignimage -imageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid 1 `

  -HostingUnitName xenhu -IdentityPoolName poo1 `

  -CleanOnBoot -Scope @() -SecurityGroup @() -VMCpuCount 2 -VMMemoryMB
8192 `

  -NetworkMapping @{"0"="XDHyp:\HostingUnits\xenhu\VM Network.network"}
```

カタログを作成するためのPowershellコマンドの完全なセットの例：

```
$CatalogName = "XenCatalog"

$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" `
```

```
  -Name $CatalogName -PersistUserChanges "Discard" -ProvisioningType "MCS"
-Scope @() -SessionSupport "MultiSession"




$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "xen.local"
-IdentityPoolName $CatalogName `

  -IdentityType "ActiveDirectory"  -NamingScheme "xen##" -NamingSchemeType
"Numeric" -Scope @()




$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
xenimage1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"




$Task = New-ProvScheme -ProvisioningSchemeName $CatalogName
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid `

  -HostingUnitName xenhu -IdentityPoolName $CatalogName -CleanOnBoot
-Scope @() -SecurityGroup @() `

  -NetworkMapping @{"0"="XDHyp:\HostingUnits\xenhu\VM Network.network"}
-VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously



Get-ProvTask -TaskId $Task.TaskId

$ProvScheme = Get-ProvScheme -ProvisioningSchemeName $CatalogName
```

```
Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

詳細情報

- イメージ管理

次のステップ

- 準備済みイメージマシンカタログを管理する(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/manage-prepared-image-machine-catalogs.html)

準備済みイメージのマシンカタログを管理する

既存のMCSマシンカタログを別の準備済みイメージで更新し、イメージ定義とバージョンを管理するには、以下を使用します。

- ウェブスタジオ
- PowerShell

Web Studioを使用する

マシンカタログを別の準備済みイメージで更新する

既存のMCSマシンカタログを別の準備済みイメージで更新するには、次の手順を実行します。

1. 左側のナビゲーションペインで をクリックし、更新するマシンカタログを選択します。右クリックして を選択します。
2. **Image** ページで、準備済みイメージを選択します。必要に応じて、選択した準備済みイメージにメモを追加します。

   > **注：**
   >
   > Azureに適用可能：ACGが有効になっていないイメージを選択し、後で チェックボックスをオンにして、イメージをギャラリーに配置することもできます。

3. 以前に割り当てられた準備済みイメージにロールバックするには、ウィザードの下部にある **Use previous image assignment for quick rollback** をクリックします。

新しいウィンドウが開き、利用可能なすべての履歴イメージ割り当てのリストが表示されます。リストからイメージを選択すると、イメージページの準備済みイメージツリーで対応するバージョンが自動的に選択されます。

4. **ロールアウト戦略**ページで、選択した準備済みイメージでこのカタログを更新するタイミングを選択します。
5. ページで詳細を確認します。 をクリックします。

カタログに加えられたイメージ変更の履歴を表示できます。履歴を表示するには、次の手順を実行します。

1. マシンカタログを選択します。
2. タブの フィールドで、 をクリックします。

イメージ定義とバージョンを管理する

イメージ定義とバージョンを編集および削除して、作成されたさまざまなイメージバージョンと定義の使用を管理できます。

イメージ定義を編集する

イメージ定義の名前と説明を編集できます。

イメージ定義を編集するには、次の手順を実行します。

1. **イメージ**ノードに移動し、イメージ定義を選択して、**イメージ定義の編集**を選択します。

イメージバージョンを編集する

イメージバージョンの説明を編集して、そのイメージバージョンの目的を指定できます。

イメージバージョンを編集するには、次の手順を実行します。

1. **イメージ**ノードに移動し、イメージバージョンを選択して、**説明の編集**を選択します。

イメージバージョンを削除する

イメージバージョンを削除するには、次の手順を実行します。

1. **イメージ**ノードに移動し、イメージバージョンを選択して、**イメージバージョンの削除**を選択します。

> 「注：」：

> マシンカタログで使用されているイメージバージョンは削除できません。

イメージ定義を削除する

イメージ定義を削除するには、次の手順を実行します。

1. **イメージ**ノードに移動し、イメージ定義を選択して、**イメージ定義の削除**を選択します。

> 「注：」:

> イメージバージョンが含まれているイメージ定義は削除できません。

PowerShell を使用する

準備済みイメージバージョン仕様を使用してカタログを更新する

`Set-ProvSchemeImage` コマンドを使用してカタログを更新できます。例:

```
Set-ProvSchemeImage -ProvisioningSchemeUid <Guid> -ImageVersionSpecUid
<Guid> [-DoNotStoreOldImage] [-RunAsynchronously] [-PurgeJobOnSuccess][-
ImageAssignmentNote <string>]
```

または、,

```
Set-ProvSchemeImage -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> [-DoNotStoreOldImage] [-RunAsynchronously] [-PurgeJobOnSuccess][-
ImageAssignmentNote <string>]
```

カタログを更新するためのPowershellコマンドの完全なセットの例:

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 2 -Filter "PreparationType -eq 'Mcs'"



Set-ProvSchemeImage -ProvisioningSchemeName azurecatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-RunAsynchronously -ImageAssignmentNote "Update from VST team"
```

プロビジョニングスキームのイメージ変更履歴を取得する

```
Get-ProvSchemeImageVersionSpecHistory -ProvisioningSchemeName azurecatalog
```

イメージ定義、イメージバージョン、および準備済みイメージバージョン仕様を削除する

イメージ定義、イメージバージョン、および準備済みイメージバージョン仕様を削除する前に、以下を考慮してください。

- イメージ定義にイメージバージョンが含まれている場合、そのイメージ定義は削除できません。
- イメージバージョンにイメージバージョン仕様が含まれている場合、そのイメージバージョンは削除できません。
- マスターイメージバージョン仕様が他の準備済みイメージバージョン仕様で使用されている場合、そのマスターイメージバージョン仕様は削除できません。
- 準備済みイメージバージョン仕様がMCSマシンカタログで使用されている場合、その準備済みイメージバージョン仕様は削除できません。
- ホスティングユニットが他の準備済みイメージバージョン仕様で使用されている場合、そのホスティングユニットは削除できません。

詳細な手順は次のとおりです。

1. マシンカタログを削除します。例:

   ```
   Remove-ProvScheme -ProvisioningScheneName decouplingCatalog
   ```

2. 共有準備済みイメージバージョン仕様を削除します。例:

   ```
   Remove-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid <uid>
   -HostingUnitName AzureWest
   ```

3. 準備済みイメージバージョン仕様を削除します。例:

   ```
   $PreparedImageVersionSpec = Get-ProvImageVersionSpec
   -ImageDefinitionName image1 -ImageVersionNumber 1 -Filter
   "PreparationType -eq 'Mcs'"
   ```

```
Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously
```

4. マスターイメージバージョン仕様を削除します。例:

```
$MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"



Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronousl
```

> **注:**
>
> マスターイメージバージョン仕様は、関連付けられた準備済みイメージバージョン仕様がない場合にのみ削除できます。

5. イメージバージョンを削除します。例:

```
Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber
1
```

6. 指定されたホスティング接続でイメージ定義の構成を削除します。例:

```
Remove-ProvImageDefinitionConnection -ImageDefinitionName xx
-HypervisorConnectionName xxx
```

7. イメージ定義を削除します。例:

```
Remove-ProvImageDefinition -ImageDefinitionName image1
```

準備されたイメージがホストユニット間で共有されていない場合のPowerShellコマンドの完全なセットの例:

```
Remove-ProvScheme -ProvisioningSchemeName decouplingCatalog



$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"



Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously



$MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"



Remove-ProvImageVersionSpec -ImageVersionSpecUid
$MasterImageVersionSpec.ImageVersionSpecUid -RunAsynchronously



Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber 1



Remove-ProvImageDefinition -ImageDefinitionName image1
```

準備されたイメージがホストユニット間で共有されている場合のPowerShellコマンドの完全なセットの例:

```
Remove-ProvScheme -ProvisioningSchemeName decouplingCatalog



Remove-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid <uid>

-HostingUnitName AzureWest
```

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"



Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously



$MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"



Remove-ProvImageVersionSpec -ImageVersionSpecUid
$MasterImageVersionSpec.ImageVersionSpecUid -RunAsynchronously



Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber 1



Remove-ProvImageDefinitionConnection -ImageDefinitionName xx
-HypervisorConnectionName xxx



Remove-ProvImageDefinition -ImageDefinitionName image1
```

イメージ定義とイメージバージョンを管理する

イメージ定義の名前変更と編集、およびイメージバージョンの編集が可能です。

- `Rename-ProvImageDefinition`コマンドを使用してイメージ定義の名前を変更します。例:

  ```
  Rename-ProvImageDefinition -ImageDefinitionUid <Guid>
  -NewImageDefinitionName <string>
  ```

  または、,

```
Rename-ProvImageDefinition -ImageDefinitionName <string>
-NewImageDefinitionName <string>
```

- `Set-ProvImageDefinition`コマンドを使用してイメージ定義を編集します。例:

```
Set-ProvImageDefinition -ImageDefinitionUid <Guid> [-Description
<string>]
```

または、,

```
Set-ProvImageDefinition -ImageDefinitionName <string> [-Description
<string>]
```

- `Set-ProvImageVersion`コマンドを使用してイメージバージョンを編集します。例:

```
Set-ProvImageVersion -ImageVersionUid <Guid> [-Description <string>]
```

または、,

```
Set-ProvImageVersion -ImageDefinitionName <string> -ImageVersionNumber
<int> [-Description <string>]
```

イメージ定義、イメージバージョン、準備されたイメージバージョンの仕様、およびプロビジョニングスキームの詳細を取得する

- `Get-ProvImageDefinition`コマンドを使用してイメージ定義の詳細を取得します。例:

```
Get-ProvImageDefinition [-ImageDefinitionName <string>] [-
ImageDefinitionUid <Guid>] [-ReturnTotalRecordCount] [-MaxRecordCount
<int>] [-Skip <int>] [-SortBy <string>] [-Filter <string>]
```

- `Get-ProvImageVersion`コマンドを使用してイメージバージョンの詳細を取得します。例:
  - イメージ定義内のイメージバージョンを一覧表示するには、,

```
Get-ProvImageVersion -ImageDefinitionUid <Guid>
```

または、,

```
Get-ProvImageVersion -ImageDefinitionName <string>
```

  - イメージバージョンの詳細を取得するには、,

```
Get-ProvImageVersion -ImageVersionUid <Guid>
```

    または、,

```
Get-ProvImageVersion -ImageDefinitionName <string>
-ImageVersionNumber <int>
```

- `Get-ProvImageVersionSpec` コマンドを使用して準備済みイメージバージョン仕様を取得します。例:
  - イメージバージョン内のすべての準備済みイメージバージョン仕様を一覧表示するには、,

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid>
```

  - 準備済みイメージバージョン仕様内のマスターイメージバージョン仕様を一覧表示するには、,

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter
'PreparationType -eq "None"'
```

  - マスターイメージに関連付けられているイメージバージョン内の準備済みイメージバージョン仕様を一覧表示するには、,

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter
'PreparationType -eq "MCS" -and SourceImageVersionSpecUid -eq
"xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"'
```

  - イメージバージョン内の成功した準備済みイメージバージョン仕様を取得するには、,

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter
'PreparationType -eq "MCS" -and SourceImageVersionSpecUid -eq
"xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" -and ImageVersionSpecStatus
-eq "Complete"'
```

- 準備済みイメージバージョン仕様の詳細を取得するには、,

```
Get-ProvImageVersionSpec -ImageVersionSpecUid <Guid>
```

- `Get-ProvScheme` コマンドを使用してプロビジョニングスキームの詳細を取得します。例:

```
Get-ProvScheme [[-ProvisioningSchemeName] <String>] [-
ProvisioningSchemeUid <Guid>] [-ScopeId <Guid>] [-ScopeName <String>]
[-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-
SortBy <String>] [-Filter <String>] [-FilterScope <Guid>]
```

- `Get-ProvSchemeImageVersionSpecHistory` コマンドを使用してプロビジョニングスキームの準備済みイメージバージョン仕様の履歴を取得します。例:

```
Get-ProvSchemeImageVersionSpecHistory [-ProvisioningSchemeName
<String>] [-ProvisioningSchemeUid <Guid>] [-ImageVersionSpecUid <Guid>]
[-ImageVersionSpecHistoryUid <Guid>] [-ReturnTotalRecordCount] [-
MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter
<String>] [-FilterScope <Guid>]
```

詳細情報

- イメージ管理

マシンカタログを作成する

重要:

Citrix Virtual Apps and Desktops™ 7 2006以降、現在の展開で以下のいずれかのテクノロジーを使用している場合、それらのテクノロジーを使用するサポート終了（EOL）アイテムを削除した後にのみ、現在のリリースに展開をアップグレードできます。

- パーソナルvDisk (PvDs)
- AppDisks™
- パブリッククラウドホストの種類：Citrix CloudPlatform、Microsoft Azure Classic

詳細については、「PvD、AppDisks、およびサポートされていないホストの削除」を参照してください。

注:

バージョン2511以降、Citrix Web Studio (Webベース) はCitrix Virtual Apps and Desktops™ の唯一の管理コンソールです。Citrix Studio (MMCベース) はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

展開にパブリッククラウドホスト接続を使用する場合は、新規インストールまたは現在のリリースへのアップグレードを完了するためにハイブリッド権限ライセンスが必要です。

インストーラーがサポートされていないテクノロジーの1つ以上、またはHybrid Rights Licenseなしのホスト接続を検出すると、アップグレードは一時停止または停止します。説明メッセージが表示されます。インストーラーログには詳細が含まれています。詳細については、「展開のアップグレード」を参照してください。

はじめに

物理マシンまたは仮想マシンのコレクションは、マシンカタログと呼ばれる単一のエンティティとして管理されます。カタログ内のすべてのマシンは、マルチセッションOSまたはシングルセッションOS、およびWindowsまたはLinuxマシンという同じ種類のオペレーティングシステムを持っています。

Web Studioは、サイトを作成した後、最初のマシンカタログを作成するようにガイドします。最初のカタログを作成した後、Web Studioは最初のデリバリーグループを作成するようにガイドします。後で、作成したカタログを変更したり、さらにカタログを作成したりできます。

ヒント:

既存の展開をアップグレードすると、Machine Creation Services (MCS) ストレージ最適化 (MCS I/O) 機能が有効になり、追加の構成は不要です。Virtual Delivery Agent (VDA) と Delivery Controller のアップグレードが MCS I/O のアップグレードを処理します。

概要

VM のカタログを作成するときは、それらの VM をプロビジョニングする方法を指定します。Machine Creation Services™ (MCS) を使用できます。または、独自のツールを使用してマシンを提供することもできます。

考慮事項:

- MCSは、仮想マシンイメージからの単一のシステムディスクをサポートします。そのイメージに接続されている残りのデータディスクは無視されます。
- MCSを使用してVMをプロビジョニングする場合、カタログに同一のVMを作成するためにマスターイメージ (またはイメージのスナップショット) を提供します。カタログを作成する前に、まずツールを使用してマスターイメージを作成および構成します。このプロセスには、イメージにVirtual Delivery Agent (VDA) をインストールすることが含まれます。次に、Web Studioでマシンカタログを作成します。そのイメージ (またはスナップショット) を選択し、カタログに作成するVMの数を指定し、追加情報を構成します。
- マシンがすでに利用可能な場合でも、それらのマシン用に1つ以上のマシンカタログを作成する必要があります。
- PowerShell SDK を直接使用してカタログを作成する場合、イメージまたはスナップショットではなく、ハイパーバイザーテンプレート (**VMTemplates**) を指定できます。
- テンプレートを使用してカタログをプロビジョニングすることは、実験的な機能と見なされます。この方法を使用すると、仮想マシンの準備が失敗する可能性があります。その結果、テンプレートを使用してカタログを公開することはできません。

MCSまたはCitrix Provisioning™を使用して最初のカタログを作成する場合、サイトを作成したときに構成したホスト接続を使用します。後で（最初のカタログとデリバリーグループを作成した後）、その接続に関する情報を変更したり、さらに接続を作成したりできます。

カタログ作成ウィザードを完了すると、正しく構成されていることを確認するためにテストが自動的に実行されます。テストが完了すると、テストレポートを表示できます。Web Studio からいつでもテストを実行できます。

> **注:**
>
> MCSはWindows 10 IoT CoreおよびWindows 10 IoT Enterpriseをサポートしていません。詳細については、Microsoftサイトを参照してください。

> Citrix Provisioningツールの技術的な詳細については、Citrix Virtual Apps and Desktops Image Managementを参照してください。

RDS ライセンスチェック

Web Studio は現在、Windows マルチセッションOSマシンを含むマシンカタログを作成する際に、有効なMicrosoft RDSライセンスのチェックを実行しません。Windows **マルチセッションOSマシン**のMicrosoft RDSライセンスのステータスを表示するには、Citrix Directorに移動します。**マシン詳細**パネルでMicrosoft RDSライセンスのステータスを表示します。このパネルは、**マシン詳細とユーザー詳細**ページにあります。詳細については、「Microsoft RDS license health」を参照してください。

VDA登録

ブローカーセッションを起動する際、VDAはDelivery Controller™に登録されている必要があります。未登録のVDAは、利用可能なリソースの活用不足につながる可能性があります。VDAが登録されない理由はさまざまあり、その多くは管理者がトラブルシューティングできます。Web Studioは、カタログ作成ウィザードおよびカタログからデリバリーグループにマシンを追加した後に、トラブルシューティング情報を提供します。

ウィザードを使用して既存のマシンを追加すると、コンピューターアカウント名の一覧に、各マシンがカタログへの追加に適しているかどうかが示されます。各マシンの横にあるアイコンにカーソルを合わせると、そのマシンに関する情報メッセージが表示されます。

メッセージで問題のあるマシンが特定された場合は、そのマシンを削除するか、追加します。たとえば、マシンに関する情報が取得できない可能性があることを示すメッセージが表示された場合でも、そのマシンを追加してください。

詳細については、以下を参照してください。

- VDA登録のトラブルシューティングガイダンスについては、CTX136668
- VDAのバージョンと機能レベル
- VDA登録方法

MCSカタログ作成の概要

カタログ作成ウィザードで情報を提供した後の、デフォルトのMCSアクションの概要を以下に示します。

- マスターイメージ（スナップショットではなく）を選択した場合、MCSはスナップショットを作成します。

- MCSはスナップショットの完全なコピーを作成し、そのコピーをホスト接続で定義されている各ストレージの場所に配置します。
- MCSはマシンをActive Directoryに追加し、一意のIDを作成します。
- MCSは、ウィザードで指定された数のVMを作成し、各VMに2つのディスクを定義します。VMごとの2つのディスクに加えて、マスターも同じストレージの場所に保存されます。複数のストレージの場所が定義されている場合、それぞれに次のディスクタイプが割り当てられます。
  - 作成されたばかりのVM間で共有される、読み取り専用のスナップショットの完全なコピー。
  - 各VMに一意のIDを付与する一意の16 MBのIDディスク。各VMはIDディスクを取得します。
  - VMへの書き込みを保存するための固有の差分ディスク。このディスクはシンプロビジョニングされており（ホストストレージでサポートされている場合）、必要に応じてマスターイメージの最大サイズまで増加します。各VMには差分ディスクが割り当てられます。差分ディスクには、セッション中に加えられた変更が保持されます。専用デスクトップの場合は永続的です。プールされたデスクトップの場合、デリバリーコントローラーを介した再起動ごとに削除され、新しいものが作成されます。
  - VDAバージョン2511以降のWindows VMの場合、MCSは各マシンに一意の`MachineGuid`を割り当てます。この`MachineGuid`は、VDAにインストールされている一部のソフトウェアでライセンス目的で使用されます。

あるいは、静的デスクトップを配信するためにVMを作成する際、カタログ作成ウィザードの**マシン**ページで、シック（完全コピー）VMクローンを指定できます。完全クローンは、すべてのデータストアにマスターイメージを保持する必要はありません。各VMは独自のファイルを持っています。

MCSストレージに関する考慮事項

MCSのストレージソリューション、構成、容量を決定する際には、多くの要因があります。以下の情報は、ストレージ容量に関する適切な考慮事項を提供します。

容量に関する考慮事項:

- ディスク

  DeltaまたはDifferencing (Diff) ディスクは、ほとんどのMCS展開において、各VMで最大のスペースを消費します。MCSによって作成される各VMには、作成時に最低2つのディスクが割り当てられます。

  - Disk0 = 差分ディスク：マスターベースイメージからコピーされたOSが含まれます。

- Disk1 = IDディスク: 16 MB - 各VMのActive Directoryデータを格納します。

製品の進化に伴い、特定のユースケースや機能の消費を満たすために、さらにディスクを追加する必要がある場合があります。例:

- MCS Storage Optimizationは、各VMにライトキャッシュスタイルのディスクを作成します。XenServer、VMware、およびSCVMM仮想化環境では、ホスト接続の作成時に利用可能なOSストレージリストと利用可能な一時ストレージリストを同じように構成した場合、MCSはライトバックキャッシュ (WBC) ディスクをOSディスクと同じストレージ場所に配置します。
- MCSは、前のセクションで説明したDeltaディスクのシナリオとは対照的に、フルクローンを使用する機能を追加しました。

ハイパーバイザーの機能も考慮に入れる必要があるかもしれません。例:

- XenServer IntelliCacheは、各XenServerのローカルストレージに読み取りディスクを作成します。このオプションにより、共有ストレージの場所に保持されている可能性のあるマスターイメージに対するIOPSを節約できます。

- ハイパーバイザーのオーバーヘッド

  ハイパーバイザーはそれぞれ、VMのオーバーヘッドとなる特定のファイルを使用します。また、ハイパーバイザーは管理および一般的なログ記録操作にもストレージを使用します。オーバーヘッドを含めるためのスペースを計算します。

  - ログファイル
  - ハイパーバイザー固有のファイル。例：
    - VMwareは、**VMストレージ**フォルダーにファイルを追加します。VMwareのベストプラクティスを参照してください。
    - 仮想マシンの合計サイズ要件を計算します。仮想ディスクに20 GB、スワップファイルに16 GB、ログファイルに100 MBを使用し、合計36.1 GBを消費する仮想マシンを考慮してください。
  - XenServerのスナップショット; VMwareのスナップショット。

- プロセスオーバーヘッド

  カタログの作成、マシンの追加、カタログの更新には、それぞれ固有のストレージへの影響があります。例：

- 初期カタログ作成では、ベースディスクのコピーを各ストレージの場所にコピーする必要があります。
- カタログにマシンを追加する場合、ベースディスクを各ストレージの場所にコピーする必要はありません。カタログの作成は、選択された機能によって異なります。
- カタログを更新すると、各ストレージの場所に余分なベースディスクが作成されます。カタログの更新では、カタログ内の各VMが一定期間2つの差分ディスクを持つため、一時的なストレージのピークも発生します。

その他の考慮事項：

- **RAMサイジング：** I/O最適化ディスク、ライトキャッシュ、スナップショットファイルなど、特定のハイパーバイザーファイルとディスクのサイズに影響します。
- **シンプロビジョニング/シックプロビジョニング:** シンプロビジョニング機能があるため、NFSストレージが推奨されます。

Machine Creation Services (MCS) ストレージ最適化

Machine Creation Services (MCS) ストレージ最適化機能は、MCS I/O とも呼ばれます。この機能は、Azure、GCP、XenServer、VMware、AWS、および SCVMM でのみ利用可能です。

- ライトキャッシュコンテナは*ファイルベース*であり、Citrix Provisioning と同じ機能です。たとえば、Citrix Provisioning のライトキャッシュファイル名は `D:\vdiskdif.vhdx` で、MCS I/O のライトキャッシュファイル名は `D:\mcsdif.vhdx` です。
- ライトキャッシュディスクに書き込まれる Windows クラッシュダンプファイルのサポートを含めることで、診断機能の改善を実現します。
- MCS I/O は、最適な多層書き込みキャッシュソリューションを提供するために、*RAM 内キャッシュとハードディスクへのオーバーフロー*というテクノロジーを保持しています。この機能により、管理者は各層（RAM とディスク）のコストとパフォーマンスのバランスを取り、目的のワークロード要件を満たすことができます。

書き込みキャッシュ方式を*ディスクベース*から*ファイルベース*に更新するには、次の変更が必要です。

1. MCS I/O は、RAMのみのキャッシュをサポートしなくなりました。マシンカタログ作成時にWeb Studioでディスクサイズを指定します。
2. VM の書き込みキャッシュディスクは、VM を初めて起動するときに自動的に作成およびフォーマットされます。VM が起動すると、書き込みキャッシュファイル `mcsdif.vhdx` がフォーマットされたボリューム `MCSWCDisk` に書き込まれます。

3. ページファイルはこのフォーマットされたボリューム `MCSWCDisk` にリダイレクトされます。その結果、このディスクサイズはディスク領域の合計量を考慮します。これには、ディスクサイズと生成されたワークロードの差分に加えて、ページファイルサイズが含まれます。これは通常、VM の RAM サイズに関連付けられます。

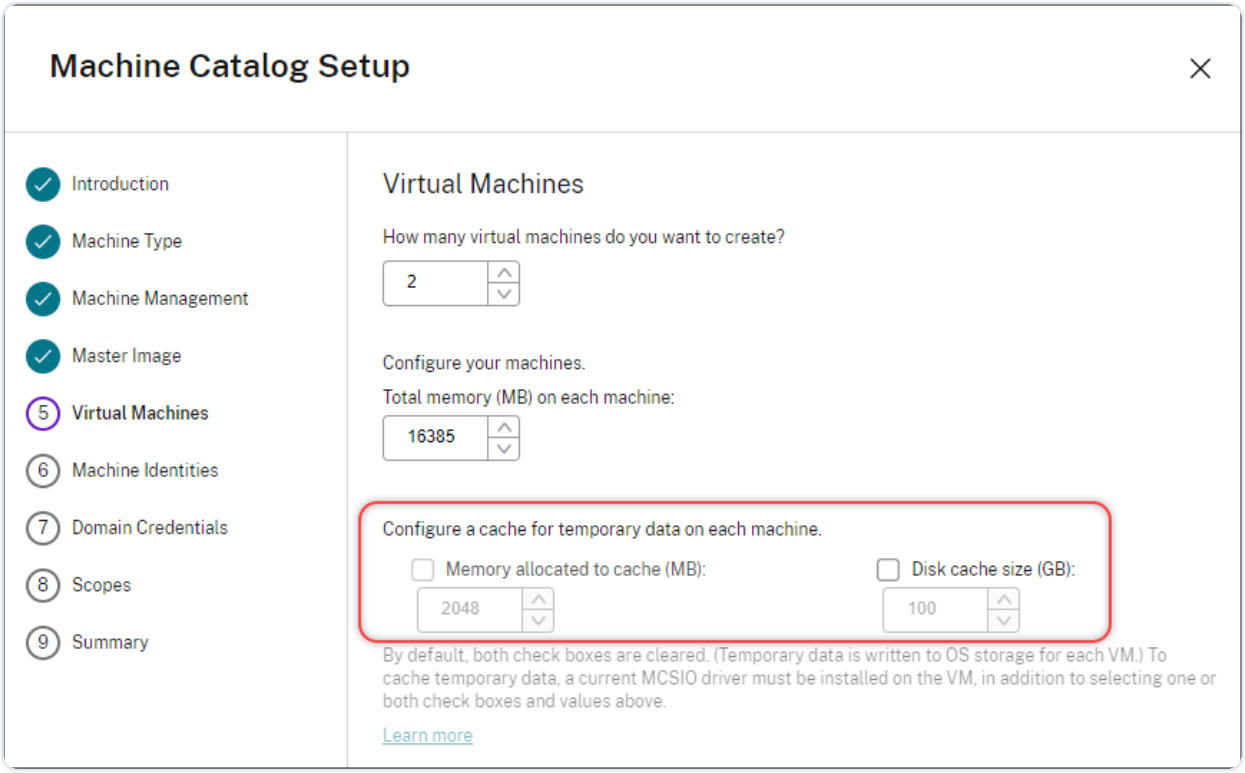
MCS ストレージ最適化の更新の有効化

MCS I/O ストレージ最適化機能を有効にするには、Delivery Controller と VDA を Citrix Virtual Apps and Desktops の最新バージョンにアップグレードしてください。

> **注:**
>
> MCS I/O が有効になっている既存の展開をアップグレードする場合、追加の構成は不要です。VDA と Delivery Controller のアップグレードによって MCS I/O のアップグレードが処理されます。

MCS ストレージ最適化の更新を有効にする際は、次の点を考慮してください。

- マシンカタログを作成する際、管理者は RAM とディスクサイズを構成できます。



- バージョン 1903 用に構成された VDA を含む新しい VM スナップショットに既存のマシンカタログを更新すると、次の動作になります。新しいスナップショットは、既存のカタログの

RAM およびディスクサイズに対する MCS I/O 設定を引き続き使用します。既存の生ディスクはフォーマットされます。

重要:

Citrix Virtual Apps and Desktops バージョン 1903 で MCS ストレージ最適化が変更されました。このリリースでは、ファイルベースのライトキャッシュテクノロジがサポートされ、パフォーマンスと安定性が向上しています。MCS I/O によって提供される新しい機能では、以前の Citrix Virtual Apps and Desktops リリースと比較して、より高いライトキャッシュストレージ要件が必要になる場合があります。Citrix は、割り当てられたワークフローと追加のページファイルサイズに対して十分なディスク容量があることを確認するために、ディスクサイズを再評価することをお勧めします。ページファイルサイズは通常、システム RAM の量に関連しています。既存のカタログディスクサイズが不十分な場合は、マシンカタログを作成し、より大きなライトキャッシュディスクを割り当ててください。

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

MCS I/Oライトバックキャッシュディスクに特定のドライブ文字を割り当てることができます。この実装により、使用するアプリケーションのドライブ文字とMCS I/Oライトバックキャッシュディスクのドライブ文字との間の競合を回避できます。MCS I/Oライトバックキャッシュディスクにドライブ文字を割り当てるには、PowerShellコマンドを使用できます。サポートされているハイパーバイザーは、Azure、GCP、VMware、SCVMM、およびXenServerです。

注:

この機能には、VDAバージョン2305以降が必要です。

制限事項

- Windowsオペレーティングシステムのみに適用
- ライトバックキャッシュディスクに適用可能なドライブ文字：`E`から`Z`
- Azure一時ディスクがライトバックキャッシュディスクとして使用されている場合は適用されません
- 新しいマシンカタログを作成する場合にのみ適用されます

ライトバックキャッシュディスクにドライブ文字を割り当てる

ライトバックキャッシュディスクにドライブ文字を割り当てるには：

1. **PowerShell**ウィンドウを開きます。
2. `asnp citrix*`を実行します。
3. まだ作成されていない場合は、IDプールを作成します。
4. プロパティ`WriteBackCacheDriveLetter`を指定して、`New-ProvScheme`コマンドを使用してプロビジョニングスキームを作成します。例：

```
New-ProvScheme -CleanOnBoot `

-HostingUnitName "<name>" `

-IdentityPoolName $schemeName `

-ProvisioningSchemeName $schemeName `

-InitialBatchSizeHint 1 `

-UseWriteBackCache -WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256 -WriteBackCacheDriveLetter E `

-MasterImageVM "XDHyp:\HostingUnits\<name>\image.folder\abcd-
resources.resourcegroup\MCSIOMasterVm_OsDisk_1_d3e2d6352xxxxxxxxx2130aa
145ec77.manageddisk" `

-NetworkMapping @{"0"="XDHyp:\\HostingUnits\\name\
\virtualprivatecloud.folder\\East US.region\
\virtualprivatecloud.folder\\abcd-resources.resourcegroup\\abcd-
resources-vnet.virtualprivatecloud\\default.network"} `

-ServiceOffering "XDHyp:\\HostingUnits\\<name>\\serviceoffering.folder\
\Standard_D2s_v5.serviceoffering" `

-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />
```

```
<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS"/>

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PersistOsDisk"
Value="false" />

<Property xsi:type="StringProperty" Name="PersistVm" Value="false" />

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="UseTempDiskForWBC"
Value="false" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="abcd-
group1" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

</CustomProperties>'
```

5. カタログの作成を完了します。詳細については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`を参照してください。

マスターイメージを準備する

接続ホストの作成については、「接続とリソース」を参照してください。

マスターイメージには、オペレーティングシステム、仮想化されていないアプリケーション、VDA、およびその他のソフトウェアが含まれています。

知っておくと良いこと:

- マスターイメージは、クローンイメージ、ゴールデンイメージ、ベースVM、またはベースイメージとも呼ばれることがあります。ホストベンダーは異なる用語を使用します。
- ホストに、作成されるマシンの数に対応できる十分なプロセッサ、メモリ、ストレージがあることを確認してください。
- デスクトップとアプリケーションに必要なハードディスク容量を正しく構成してください。この値は後で変更したり、マシンカタログで変更したりすることはできません。
- Remote PC Accessのマシンカタログはマスターイメージを使用しません。

マスターイメージに以下のソフトウェアをインストールして構成します:

- ハイパーバイザー用の統合ツール（Citrix VM Tools、Hyper-V Integration Services、VMware toolsなど）。この手順を省略すると、アプリケーションやデスクトップが正しく機能しない可能性があります。
- VDA。Citrix は、最新機能にアクセスできるように、最新バージョンのインストールを推奨しています。マスターイメージに VDA をインストールしないと、カタログの作成が失敗します。
- 必要に応じて、アンチウイルスソフトウェアや電子ソフトウェア配布エージェントなどのサードパーティツール。ユーザーとマシンタイプに適した設定（更新機能など）でサービスを構成します。
- 仮想化しないサードパーティアプリケーション。Citrixはアプリケーションの仮想化を推奨します。仮想化により、アプリケーションの追加または再構成後にマスターイメージを更新する必要がなくなるため、コストが削減されます。また、インストールされるアプリケーションが少ないほど、マスターイメージのハードディスクサイズが小さくなり、ストレージコストが節約されます。
- App-Vアプリケーションを公開する予定がある場合は、推奨設定のApp-Vクライアント。App-VクライアントはMicrosoftから入手できます。
- MCSを使用する場合、Microsoft Windowsをローカライズする際は、ロケールと言語パックをインストールしてください。プロビジョニング中にスナップショットが作成されると、プロビジョニングされたVMはインストールされているロケールと言語パックを使用します。

> **重要:**

> MCSを使用している場合は、マスターイメージでSysprepを実行しないでください。

> マスターイメージを準備するには：

1. ハイパーバイザーの管理ツールを使用してマスターイメージを作成し、オペレーティングシステムとすべてのサービスパックおよび更新プログラムをインストールします。vCPUの数を指定します。PowerShellを使用してマシンカタログを作成する場合は、vCPU値を指定することもできます。Web Studioを使用してカタログを作成する場合、vCPUの数を指定することはできません。デスクトップとアプリケーションに必要なハードディスク容量を構成します。この値は後で変更したり、カタログ内で変更したりすることはできません。
2. ハードディスクがデバイスロケーション0に接続されていることを確認します。ほとんどの標準マスターイメージテンプレートでは、この場所がデフォルトで構成されていますが、一部のカスタムテンプレートではそうでない場合があります。
3. 上記のソフトウェアをマスターイメージにインストールして構成します。
4. MCSを使用していない場合は、アプリケーションとデスクトップがメンバーであるドメインにマスターイメージを参加させます。マシンが作成されるホストでマスターイメージが利用可能であることを確認します。MCSを使用している場合、マスターイメージをドメインに参加させる必要はありません。プロビジョニングされたマシンは、カタログ作成ウィザードで指定されたドメインに参加します。
5. Citrixは、マスターイメージのスナップショットを作成して名前を付けることを推奨します。カタログ作成時にスナップショットではなくマスターイメージを指定した場合、Web Studioはスナップショットを作成します。そのスナップショットに名前を付けることはできません。

ボリュームライセンス認証

MCSは、WindowsオペレーティングシステムとMicrosoft Officeのアクティベーションを自動化および管理するためのボリュームライセンス認証をサポートしています。MCSがボリュームライセンス認証でサポートする3つのモデルは次のとおりです。

- キー管理サービス (KMS)
- Active Directoryベースのアクティベーション (ADBA)
- 複数ライセンス認証キー (MAK)

マシンカタログを作成した後で、アクティベーション設定を変更できます。

キー管理サービス (KMS)

KMSは、専用のシステムを必要とせず、他のサービスを提供するシステムと簡単に共存できる軽量なサービスです。この機能は、Citrixがサポートするすべてのwindowsバージョンでサポートされています。イメージの準備中に、MCSはMicrosoft WindowsおよびMicrosoft OfficeのKMSリアームを実行します。コマンド `Set-Provserviceconfigurationdata` を実行することで、リアーム

をスキップできます。KMSアクティベーションの詳細については、「Key Management Service を使用してアクティベートする」を参照してください。

> **注:**
>
> コマンド `Set-Provserviceconfigurationdata` の実行後に作成されたすべてのマシンカタログは、コマンドで指定されたものと同じ設定になります。

Active Directoryベースのアクティベーション (ADBA)

ADBAを使用すると、マシンのドメイン接続を介してアクティベートできます。マシンはドメインに参加するとすぐにアクティベートされます。これらのマシンは、ドメインに参加し、ドメインと連絡を取り合っている限り、アクティベートされたままになります。この機能は、Citrixがサポートするすべてのバージョンでサポートされています。Active Directoryベースのアクティベーションの詳細については、「Active Directoryベースのアクティベーション」を参照してください。

マルチプルアクティベーションキー (MAK)

MAKは、Microsoftサーバーの助けを借りて、ボリュームをアクティベートし、Windowsシステムを認証する方法です。MicrosoftからMAKキーを購入する必要があります。このキーには、固定されたアクティベーションカウントが割り当てられています。Windowsシステムがアクティベートされるたびに、アクティベーションカウントが減少します。システムをアクティベートする方法は2つあります。

- オンラインアクティベーション: アクティベートしたいWindowsシステムがインターネットアクセスを持っている場合、製品キーをインストールするとシステムは自動的にWindowsをアクティベートします。このプロセスにより、対応するMAKのアクティベーションカウントが1減少します。
- オフラインアクティベーション: Windowsシステムがオンラインアクティベーションを行うためにインターネットに接続できない場合、MCSはMicrosoftサーバーから確認IDとインストールIDを取得し、Windowsシステムをアクティベートします。このアクティベーション方法は、非永続的なマシンカタログに役立ちます。

> **注:**
>
> - MCSはMAKを使用したMicrosoft Officeのアクティベーションをサポートしていません。

- 必要なVDAの最小バージョンは2303です。

主な要件

- Delivery Controller はインターネットアクセスが必要です。
- 更新する新しいイメージが元のMAKキーと異なる場合は、新しいカタログを作成します。
- マスターイメージにMAKキーをインストールします。WindowsシステムにMAKキーをインストールする手順については、MAKアクティベーションの展開を参照してください。
- イメージ準備を使用しない場合：

  a. `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation`の下にレジストリDWORD値`Manual`を追加します。

  b. 値を`1`に設定します。

アクティベーション数

MAKキーの残りのアクティベーション数を確認したり、VMが2つ以上のアクティベーションを消費しているかどうかを確認したりするには、ボリュームアクティベーション管理ツール (VAMT) を使用します。VAMTのインストールを参照してください。

MAKを使用してWindowsシステムをアクティベートする

MAKを使用してWindowsシステムをアクティベートするには：

1. マスターイメージにプロダクトキーをインストールします。この手順で1つのアクティベーションカウントが消費されます。
2. MCSマシンカタログを作成します。
3. イメージ準備を使用しない場合：

   a. `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation`の下にレジストリDWORD値`Manual`を追加します。

   b. 値を`1`に設定します。

   この方法では、オンラインアクティベーションのオプションが無効になります。
4. マシンカタログにVMを追加します。
5. VM の電源をオンにします。

6. オンラインアクティベーションかオフラインアクティベーションかに応じて、Windows システムがアクティベートされます。

    - オンラインアクティベーションの場合、プロダクトキーのインストール後に Windows システムがアクティベートされます。
    - オフラインアクティベーションの場合、MCS はプロビジョニングされた VM と通信して Windows システムのアクティベーションステータスを取得します。その後、MCS は Microsoft サーバーから確認 ID とインストール ID を取得します。これらの ID は Windows システムのアクティベーションに使用されます。

トラブルシューティング

プロビジョニングされた VM がインストール済みの MAK キーでアクティベートされない場合は、PowerShell ウィンドウで `Get-ProvVM` または `Get-ProvScheme` コマンドを実行します。

- `Get-ProvScheme` コマンド: 最新のマスターイメージから MCS マシンカタログに関連付けられているパラメーター `WindowsActivationType` を参照してください。
- `Get-ProvVM` コマンド。パラメーター `WindowsActivationType`、`WindowsActivationStatus`、`WindowsActivationStatusErrorCode`、および `WindowsActivationStatusError` を参照してください。

エラーを確認し、問題を解決するための手順を検証できます。

Web Studio を使用してマシンカタログを作成する

カタログを作成する前に:

- このセクションを確認して、選択する項目と提供する情報について学習してください。
- マシンをホストするハイパーバイザー、クラウドサービス、およびその他のリソースへの接続が作成されていることを確認してください。
- マシンをプロビジョニングするためのマスターイメージを作成した場合は、そのイメージに VDA がインストールされていることを確認してください。

カタログ作成ウィザードを開始するには：

1. これが最初に作成するカタログである場合、正しい選択肢（「マシンをセットアップし、アプリとデスクトップを実行するためのマシンカタログを作成する」など）に誘導されます。カタログ作成ウィザードが開きます。
2. すでにカタログを作成済みで、別のカタログを作成したい場合は、次の手順に従います。

a. Web Studio にサインインし、左側のペインで **Machine Catalogs** を選択し、アクションバーで **Create Machine Catalog** を選択します。

b. フォルダーを使用してカタログを整理するには、デフォルトの**Machine Catalogs**フォルダーの下にフォルダーを作成します。詳細については、(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/machine-catalogs-manage.html#create-a-catalog-folder)を参照してください。

c. カタログを作成したいフォルダーを選択し、**Create Machine Catalog**をクリックします。カタログ作成ウィザードが開きます。

ウィザードは次の項目について説明します。表示されるウィザードページは、選択内容によって異なります。

オペレーティングシステム

各カタログには、1種類のマシンのみが含まれます。1つ選択してください。

- **マルチセッションOS:** マルチセッションOSカタログは、ホストされた共有デスクトップを提供します。マシンはサポートされているバージョンのWindowsまたはLinuxオペレーティングシステムを実行できますが、カタログに両方を含めることはできません。（そのOSの詳細については、Linux VDAのドキュメントを参照してください。）
- **シングルセッションOS:** シングルセッションOSカタログは、さまざまなユーザーに割り当てることができるVDIデスクトップを提供します。
- **Remote PC Access:** Remote PC Accessカタログは、ユーザーに物理的なオフィスデスクトップマシンへのリモートアクセスを提供します。Remote PC Accessは、セキュリティを提供するためにVPNを必要としません。

マシン管理

このページは、リモートPCアクセスカタログを作成する際には表示されません。

マシン管理ページには、マシンの管理方法と、マシンの展開に使用するツールが示されます。

カタログ内のマシンをWeb Studio経由で電源管理するかどうかを選択します。

- マシンはWeb Studioを介して電源管理されます。たとえば、VMやブレードPCなどです。このオプションは、ホストへの接続をすでに構成している場合にのみ利用可能です。
- マシンはWeb Studioを介して電源管理されません。たとえば、物理マシンなどです。

マシンがWeb Studioを介して電源管理されることを指定した場合は、VMの作成に使用するツールを選択します。

- Citrix Provisioningテクノロジー
  - **Citrix Machine Creation Services (MCS)** MCSを使用してプロビジョニングおよびイメージ化されたVMのカタログを作成します。MCSは、マスターイメージからクローンされたイメージをこれらのVMにコピーします。
  - **Citrix Provisioning Services (PVS)** MCSを使用してプロビジョニングされ、PVSを使用してイメージ化されたVMのカタログを作成します。これらのVMはPVSターゲットデバイスとして機能し、PVSサーバーは単一の共有ディスクイメージをそれらにストリーミングできます。

    > **注:**
    >
    > - このオプションは、Citrix Cloud™に登録されているPVSサイトでのみ利用可能であり、現在、Azureリソースに限定されています。
    > - Citrix Provisioningカタログを作成する際、**ターゲットデバイス**ページで、プロビジョニングするマシンのファームとサイトを選択するためのドロップダウンメニューに、すでに存在しないファームとサイトがリストされている場合があります。回避策として、PowerShellコマンド `Unregister-HypPvsSite` を実行して、データベースからファームとサイトを削除できます。PowerShellコマンドの詳細については、Unregister-HypPvsSiteを参照してください。

- **その他のサービスまたはテクノロジー** データセンターにすでに存在するマシンを管理するツール。Citrixでは、カタログ内のマシンの一貫性を確保するために、Microsoft System Center Configuration Managerまたはその他のサードパーティ製アプリケーションを使用することをお勧めします。

デスクトップの種類（デスクトップエクスペリエンス）

> **注:**
>
> **デスクトップエクスペリエンス**ページで利用できるオプションは、**マシンタイプ**ページで選択したマシンタイプによって異なります。

- **マルチセッションOS**マシンでは、ユーザーはログオンするたびにランダムなデスクトップを割り当てられます。次のいずれかのオプションを選択してください。

- **はい、仮想デスクトップをホストするマシンのローカルディスクに変更を保存します。**（永続的）
- **いいえ、すべての変更を破棄し、ユーザーがログオフするときに仮想デスクトップをクリアします。**（非永続的）

> **注:**
>
> 永続的なマルチセッションマシンでは、ユーザーがデスクトップに行った変更は保存され、すべての承認されたユーザーがアクセスできます。

- **シングルセッションOS**マシンでは、**デスクトップエクスペリエンス**ページで次のオプションが表示されます。
  - **ユーザーがログオンするたびに、新しい（ランダムな）デスクトップに接続するようにします。**
  - **ユーザーがログオンするたびに、同じ（静的な）デスクトップに接続するようにします。**

    静的デスクトップの場合、ユーザーが行った変更をログオフ後に保存するか破棄するかをさらに決定できます。

仮想デスクトップをホストするマシンのローカルディスクに変更を保存する: 永続的を選択した場合、**仮想マシン**ページで仮想マシンコピーモードの高速コピーまたは完全コピーオプションが利用可能になります。

すべての変更を破棄し、ユーザーがログオフするときに仮想デスクトップをクリアする: 非永続的を選択した場合、**仮想マシン**ページで仮想マシンコピーモードを構成することはできません。

イメージとマシンプロファイル

このページは、MCSを使用してVMを作成している場合にのみ表示されます。

1. マシンカタログのイメージの種類を選択し、次にイメージを選択します。2種類のイメージが利用可能です。
   - **マスターイメージ。** イメージ準備プロセスをまだ経ていないイメージです。イメージ準備プロセスは、カタログ作成が開始されると自動的に開始されます。

     > **注:**

> - MCSを使用している場合、マスターイメージでSysprepを実行しないでください。
> - スナップショットではなくマスターイメージを指定した場合、Web Studioはスナップショットを作成しますが、名前を付けることはできません。

- **準備済みイメージ。** イメージ準備プロセスを完了し、VM作成に直接使用できるイメージ。カタログ作成時にマスターイメージではなく準備済みイメージを選択すると、マシンカタログの作成がより高速かつ信頼性の高いものになり、イメージのライフサイクル管理が効率化されます。必要に応じて、選択した準備済みイメージにメモを追加します。

  > **注:**
  >
  > - 準備されたイメージを使用して作成されたVMは、ハイバネーションをサポートしていません。
  > - 現在、準備されたイメージを使用してカタログを作成することは、AzureおよびVMware環境でのみ利用可能です。

  準備されたイメージの作成方法の詳細については、Image management (preview)を参照してください。

  イメージを選択する際、必要に応じて、選択したイメージにメモを追加できます。

  最新の製品機能を使用できるようにするには、マスターイメージに最新のVDAバージョンがインストールされていることを確認してください。デフォルトの最小VDA選択を変更しないでください。ただし、以前のVDAバージョンを使用する必要がある場合は、VDA versions and functional levelsを参照してください。

  ウィザードで以前に選択したマシン管理テクノロジーと互換性のないスナップショットまたはVMを選択すると、エラーメッセージが表示されます。

2. 既存のVMをマシンプロファイルとして使用するには、**Use a machine profile**を選択し、その後、VMを選択します。

   > **注:**

> 現在、マシンプロファイルの使用は、Azure、AWS、GCP、およびVMware VMに限定されています。

> VMware展開の場合、マシンプロファイルを使用してマシンカタログを作成する際、仮想マシンを保持するフォルダーを指定する必要があります。

仮想マシンフォルダーの場所を指定するには、カタログ作成ウィザードで**Virtual Machines**ページに移動し、**Select a folder to place the machines**セクションに移動して仮想マシンフォルダーの場所を選択します。指定されていない場合、システムは選択されたマシンプロファイルのフォルダーをデフォルトの場所と見なします。

3. AWS展開の場合、起動テンプレートをマシンプロファイルとして選択できます。
4. カタログの最小機能レベルを選択します。最新の製品機能を使用できるようにするには、マスターイメージに最新のVDAバージョンがインストールされていることを確認してください。

マシン

リモートPCアクセス カタログを作成している場合、このページは表示されません。

このページのタイトルは、**マシン管理**ページで選択した内容（**マシン**、**仮想マシン**、または**VMとユーザー**）によって異なります。

MCSを使用する場合：

- 作成する仮想マシンの数を指定します。作成しない場合は**0**（ゼロ）を入力します。後で、**Add machines**を実行して、空のカタログにVMを作成できます。
- 各 VM が持つメモリ量 (MB 単位) を選択します。
- 作成された各VMにはハードディスクがあります。そのサイズはマスターイメージで設定されます。カタログでハードディスクのサイズを変更することはできません。
- 展開に複数のゾーンが含まれている場合、カタログのゾーンを選択できます。
- 静的デスクトップVMを作成する場合は、仮想マシンコピーモードを選択します。「仮想マシンコピーモード」を参照してください。
- vDiskを使用しないランダムデスクトップVMを作成する場合は、各マシンの一時データに使用するキャッシュを構成できます。「一時データ用のキャッシュの構成」を参照してください。

その他のツールを使用する場合：

Active Directoryマシンアカウント名を追加（またはリストをインポート）します。VMを追加/インポートした後、そのVMのActive Directoryアカウント名を変更できます。「**デスクトップエクスペ**

リエンス」ページで静的マシンを指定した場合、追加する各VMのActive Directoryユーザー名をオプションで指定できます。

名前を追加またはインポートした後、このページにいる間は「**削除**」ボタンを使用してリストから名前を削除できます。

他のツールを使用する場合（ただしMCSではない場合）：

追加（またはインポート）された各マシンに表示されるアイコンとツールヒントは、カタログに追加できない可能性のあるマシンや、Delivery Controllerに登録できないマシンを特定するのに役立ちます。詳細については、「VDAのバージョンと機能レベル」を参照してください。

仮想マシン作成時にSIDを追加する

新しい仮想マシンを作成する際に、マシンを一意に識別するためにパラメーター`ADAccountSid`を追加できるようになりました。

これを行うには：

1. サポートされているIDタイプでカタログを作成します。
2. `NewProvVM`を使用してカタログにマシンを追加します。例：

```
New-ProvVM  -ProvisioningSchemeName "name"  -ADAccountSid @("SID ")  -
RunAsynchronously
```

ただし、次の条件のいずれかに該当するマシンをプロビジョニングすることはできません。

- カタログIDプールにないADアカウント
- 利用可能な状態ではないADアカウント

仮想マシンのコピーモード

マシンページで指定するコピーモードによって、MCSがマスターイメージからシン（高速コピー）クローンを作成するか、シック（完全コピー）クローンを作成するかが決まります。(デフォルト = シンクローン)

- ストレージをより効率的に使用し、マシンの作成を高速化するには、高速コピーのクローンを使用します。
- マシン作成後のIOPSを削減できる可能性があり、より優れたデータ回復と移行サポートのために、完全コピーのクローンを使用します。

> **注:**
>
> 完全コピーのクローンアプローチは、マルチセッションまたはシングルセッションOS上の永続VMをプロビジョニングする場合にのみ利用できます。

VDAのバージョンと機能レベル

カタログの機能レベルは、カタログ内のマシンで利用できる製品機能を制御します。新しい製品バージョンで導入された機能を使用するには、新しいVDAが必要です。ただし、以前のVDAバージョンを使用しているカタログ内のマシンは登録できません。

「**マシン**」（または「**デバイス**」）ページの下部にあるメニューで、最小VDAレベルを選択できます。これにより、カタログの最小機能レベルが設定されます。デフォルトでは、オンプレミス展開の場合、最新の機能レベルが選択されています。Citrixの推奨に従って、常にVDAとコアコンポーネントを最新バージョンにインストールおよびアップグレードする場合は、この選択を変更する必要はありません。ただし、古いVDAバージョンを使い続ける必要がある場合は、正しい値を選択してください。

Citrix Virtual Apps and Desktopsのリリースには、新しいVDAバージョンが含まれていない場合や、新しいVDAが機能レベルに影響を与えない場合があります。そのような場合、機能レベルは、インストールまたはアップグレードされたコンポーネントよりも古いVDAバージョンを示すことがあります。各リリースの新機能の記事には、デフォルトの機能レベルの変更が示されています。

選択された機能レベルは、その上にあるマシンのリストに影響します。リストでは、各エントリの横にあるツールヒントが、その機能レベルでマシンのVDAがカタログと互換性があるかどうかを示します。

各マシンのVDAが選択された最小機能レベルを満たしていないか、超えていない場合、ページにメッセージが表示されます。ウィザードを続行できます。それらのマシンは、後でControllerに登録できない可能性があります。または、次のことができます。

- 古いVDAを含むマシンをリストから削除し、VDAをアップグレードしてから、カタログに再度追加します。
- 最新の製品機能へのアクセスを妨げる、より低い機能レベルを選択します。

マシンタイプが正しくないためにマシンがカタログに追加されなかった場合も、メッセージが表示されます。例としては、シングルセッションOSカタログにサーバーを追加しようとしたり、ラ

ンダム割り当て用に作成されたシングルセッションOSマシンを静的マシンのカタログに追加したりする場合があります。

> **重要:**
>
> リリース1811で、追加の機能レベル「**1811（またはそれ以降）**」が追加されました。このレベルは、将来のCitrix Virtual Apps and Desktops機能で使用することを目的としています。「**7.9（またはそれ以降）**」の選択はデフォルトのままです。このデフォルトは、現在すべての展開で有効です。

> **1811 (またはそれ以降)** を選択した場合、そのカタログ内の以前のVDAバージョンはControllerに登録できません。ただし、カタログにバージョン1811以降のサポートされているVDAのみが含まれている場合、それらはすべて登録の対象となります。これには、バージョン1903および現在のリリース以前の他の19XXリリースを含む、後のCitrix Virtual Apps and Desktopsリリース用に構成されたVDAを含むカタログが含まれます。

一時データのキャッシュを構成する

MCSを使用してカタログ内のランダムな非永続マシンを管理する場合、I/Oパフォーマンスを向上させるために、マシンに対してライトバックキャッシュを有効にできます。

ライトバックキャッシュはMCSIOと呼ばれます。詳細については、こちらのブログ記事を参照してください。

前提条件

ライトバックキャッシュを有効にするには、カタログが次の要件を満たしている必要があります。

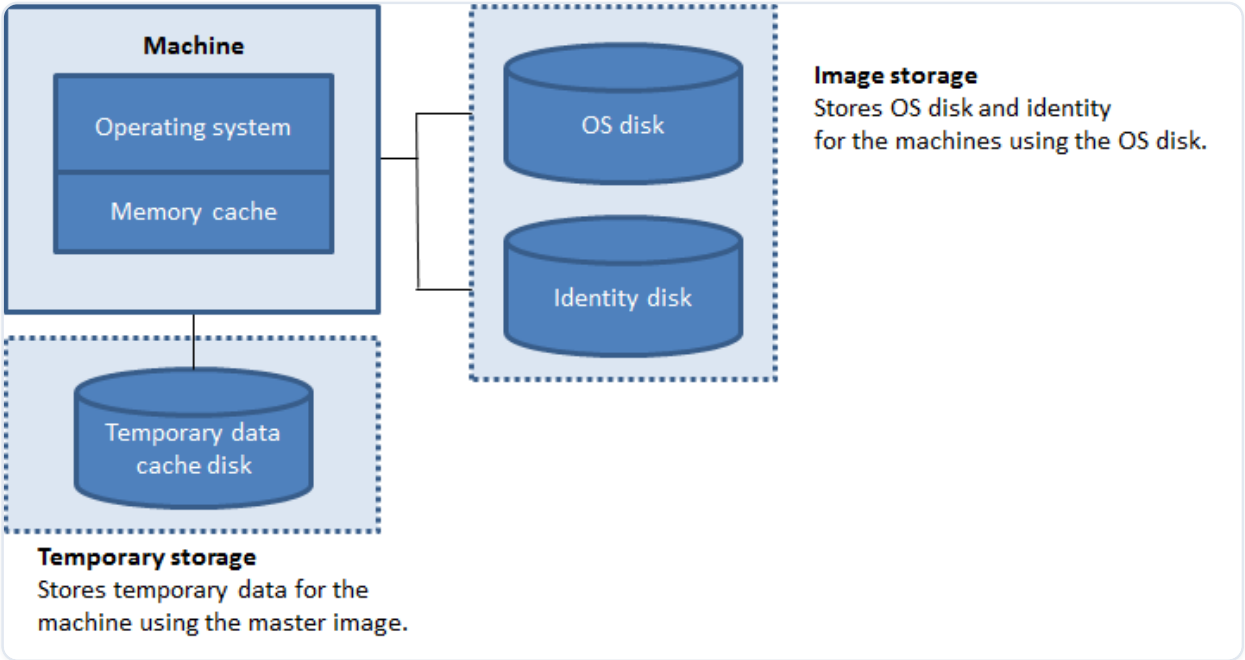
- 一時データのストレージを指定する接続を使用します。詳細については、(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/connections.html)を参照してください。
- VDAはバージョン7.9以降であり、最新のMCSIOドライバーがインストールされている必要があります。

> **注:**
>
> このドライバーのインストールは、VDAをインストールまたはアップグレードする際のオプションです。デフォルトでは、このドライバーはインストールされません。

- ディスクキャッシュのドライブ文字割り当てを有効にするには、VMが次の追加要件を満たしている必要があります。
  - オペレーティングシステム: Windows
  - VDAバージョン: 2305以降

考慮事項

- ライトバックキャッシュには、*メモリキャッシュ*と*ディスクキャッシュ*があります。デフォルトでは、接続タイプによってデフォルト値が異なります。一般的に、ほとんどの場合、デフォルト値で十分ですが、以下のために必要な領域を考慮してください。
  - Windows自体によって作成される一時データファイル（Windowsページファイルを含む）。
  - ユーザープロファイルデータ。
  - ユーザーのセッションに同期されるShareFileデータ。
  - セッションユーザーまたはユーザーがセッション内にインストールする可能性のあるアプリケーションによって作成またはコピーされる可能性のあるデータ。



- ディスクキャッシュとメモリキャッシュなしでライトバックキャッシュを構成する機能は削除されました。一時データのキャッシュを有効にするには、**ディスクキャッシュサイズ (GB)** と **キャッシュに割り当てられるメモリ (MB)** を選択し、メモリキャッシュに0より大きいサイズを指定することをお勧めします。一時データは最初にメモリキャッシュに書き込まれます。メ

モリキャッシュが設定された制限に達すると、最も古いデータが一時データキャッシュディスクに移動します。

- メモリキャッシュは、各マシンの総メモリ量の一部です。したがって、**メモリキャッシュサイズ (MB) (推奨)** チェックボックスを有効にする場合は、各マシンの総メモリ量を増やすことを検討してください。
- **メモリキャッシュサイズ (MB) (推奨)** チェックボックスをオフのままにすると、一時データは最小限のメモリを使用してディスクキャッシュに直接書き込まれます。
- **ディスクキャッシュサイズ (GB)** をデフォルト値から変更すると、パフォーマンスに影響を与える可能性があります。サイズは、ユーザーの要件とマシンにかかる負荷に合わせる必要があります。

> **重要:**
>
> ディスクキャッシュの容量が不足すると、ユーザーセッションは使用できなくなります。

- **ディスクキャッシュサイズ**チェックボックスをオフにすると、キャッシュディスクは作成されません。この場合、すべての一時データを保持するのに十分な大きさの**キャッシュに割り当てられたメモリ**の値を指定します。これは、各VMに割り当てるための大量のRAMが利用可能な場合にのみ可能です。
- 両方のチェックボックスをオフにすると、一時データはキャッシュされません。各VMの差分ディスク（OSストレージにあります）に書き込まれます。（これは、7.9より前のリリースでのプロビジョニングアクションです。）
- このカタログを使用してAppDiskを作成する予定がある場合は、キャッシュを有効にしないでください。
- マシンカタログの作成後に、キャッシュ値を変更することはできません。

セキュリティ

セキュリティページは、AWS仮想化環境でマシンプロファイルを割り当てずにマシンカタログを作成する場合にのみ表示されます。**セキュリティ**ページを使用して、VMのセキュリティグループを構成します。これは、既存のマシンカタログを編集およびクローンする場合にも適用されます。

マシンプロファイルベースのマシンカタログを作成する場合、セキュリティグループの構成はマシンプロファイルから継承され、**セキュリティ**ページは表示されません。

NIC (複数)

このページは、Remote PC Accessカタログを作成しているときには表示されません。

複数のNICを使用する予定がある場合は、各カードに仮想ネットワークを関連付けます。たとえば、一方のカードを特定のセキュアネットワークへのアクセスに割り当て、もう一方のカードをより一般的に使用されるネットワークへのアクセスに割り当てることができます。このページからNICを追加または削除することもできます。

マシンアカウント

このページは、リモートPCアクセス カタログを作成する場合にのみ表示されます。

「**マシンアカウント**」ページで、ユーザーまたはユーザーグループに対応するActive Directoryマシンアカウントまたは組織単位（OU）を指定します。OU名にスラッシュ（/）を使用しないでください。

OUを追加する際、ドメインがリストに表示されない場合は、次のことができます。

- 完全一致で検索します。
- すべてのドメインを参照して見つけます。

以前に構成した電源管理接続を選択するか、電源管理を使用しないことを選択できます。電源管理を使用したいが、適切な接続がまだ構成されていない場合は、後でその接続を作成し、マシンカタログを編集して電源管理設定を更新できます。

マシンID

このページは、MCSを使用してVMを作成する場合にのみ表示されます。

カタログ内の各マシンには一意のIDが必要です。このページでは、カタログ内のマシンのIDを構成できます。マシンはプロビジョニング後にIDに結合されます。カタログ作成後にIDの種類を変更することはできません。

このページで設定を構成するための一般的なワークフローは次のとおりです。

1. リストからIDを選択します。
2. アカウントを作成するか既存のアカウントを使用するか、およびそれらのアカウントの場所（ドメイン）を指定します。

次のいずれかのオプションを選択できます。

- **オンプレミスActive Directory**。組織が所有し、その組織に属するActive Directoryアカウントでサインインするマシン。これらはオンプレミスに存在します。
- **Microsoft Entraハイブリッド参加済み**。組織が所有し、その組織に属するActive Directory Domain Servicesアカウントでサインインするマシン。これらはクラウドとオンプレミスに存在します。要件、制限、考慮事項については、「Microsoft Entraハイブリッド参加済み」を参照してください。

  注:

  - Microsoft Entraハイブリッド参加を使用する前に、Azure環境が前提条件を満たしていることを確認してください。「Microsoft Entraハイブリッド参加の構成」を参照してください。
  - このオプションでは、マスターイメージがオペレーティングシステムの前提条件を満たしている必要があります。詳細については、「Microsoft Entraハイブリッド参加済みデバイス」を参照してください。

- **ドメイン非参加**。どのドメインにも参加していないマシン。要件と制限については、「ドメイン非参加」を参照してください。

重要:

- IDタイプとして**オンプレミス Active Directory**または**Microsoft Entra ハイブリッド参加済み**を選択した場合、カタログ内の各マシンには、対応するActive Directoryコンピューターアカウントが必要です。
- IDタイプが**Non-domain-joined**の場合、カタログの最小機能レベルとしてVDAバージョン2311以降が必要です。利用可能にするには、最小機能レベルを更新してください。

マシンIDを構成する前に、マシンが存在するOUにコンピューターアカウントを作成する権限があることを確認してください。カタログ内の各マシンには一意の名前が必要です。次に、マシンIDを構成する方法を選択します。

- 新しいマシンアカウントを作成する場合は、OUとマシン命名スキームを指定します。詳細については、「マシンアカウント命名スキーム」を参照してください。カタログを作成すると、

このカタログ用に定義したすべてのマシンIDを保持するためのIDプールが自動的に作成されます。

- 既存のマシンアカウントを使用する場合は、環境内の既存のIDプールを選択します。

注:

OU名にスラッシュ（`/`）を使用しないようにしてください。

カタログを作成し、**マシンID**ページで**既存のIDプールを使用**を選択すると、サービスアカウントの動作はIDプールの構成によって異なります。

- 選択したIDプールにサービスアカウントが構成されていない場合、**ドメイン資格情報**ページで保存済みのサービスアカウントを選択しても効果はありません。**マシンの追加**操作は、サービスアカウントが見つからないことを示すエラーで失敗する可能性があります。これを回避するには、**ドメイン資格情報**ページでドメイン資格情報を手動で入力してください。
- 選択したIDプールにサービスアカウントが構成されている場合、**ドメイン資格情報**ページで選択されたサービスアカウントは無視されます。**マシンの追加**操作は常に、IDプールに関連付けられたサービスアカウントを使用します。

既存のアカウントを使用する場合は、アカウントを参照するか、**インポート**をクリックしてアカウント名を含む.csvファイルを指定します。インポートするファイルの内容は、次の形式を使用する必要があります。

- ADcomputeraccountname.domain

追加するすべてのマシンに対して十分なアカウントがあることを確認してください。Web Studioインターフェイスがそれらのアカウントを管理します。したがって、そのインターフェイスですべてのアカウントのパスワードをリセットできるようにするか、すべてのアカウントで同じパスワードを指定してください。

物理マシンまたは既存のマシンを含むカタログの場合、既存のアカウントを選択またはインポートし、各マシンをActive Directoryコンピューターアカウントとユーザーアカウントの両方に割り当てます。

マシンアカウントの命名規則

カタログ内の各マシンには、一意の名前が必要です。カタログを作成する際には、マシンアカウントの命名規則を指定する必要があります。名前に表示される連番または文字のプレースホルダーとして、ワイルドカード（ハッシュマーク）を使用します。

命名スキームを指定する際は、以下の規則に注意してください。

- 命名スキームには少なくとも1つのワイルドカードを含める必要があります。すべてのワイルドカードはまとめて配置する必要があります。
- ワイルドカードを含む名前全体は、2文字以上15文字以下である必要があります。少なくとも1つの非数字文字と1つの#（ワイルドカード）文字を含める必要があります。
- 名前にスペースや次の文字を含めることはできません: `,~!@'$%\^&.(){\/*?"<>|=+[];:_".`。
- 名前をハイフン（-）で終わらせることはできません。

また、命名スキームを指定する際は、将来の拡張のために十分なスペースを確保してください。例を挙げます。「veryverylong#」というスキームで1,000個のマシンアカウントを作成した場合、最後に作成されるアカウント名（veryverylong1000）は16文字になります。したがって、この命名スキームでは、最大15文字を超えるマシン名が1つ以上生成されます。

シーケンシャル値が数字（0-9）か文字（A-Z）かを示すことができます。

- **0-9**。選択した場合、指定されたワイルドカードは連番に解決されます。

  > **注:**
  >
  > ワイルドカードが1つの場合、アカウント名は1から始まります。2つの場合、アカウント名は01から始まります。3つの場合、アカウント名は001から始まります。以降も同様です。

- **A-Z**。選択した場合、指定されたワイルドカードは連続する文字に解決されます。

例えば、PC-Sales-## (**0-9** が選択されている場合) という命名スキームでは、PC-Sales-01、PC-Sales-02、PC-Sales-03 などのアカウントが作成されます。

オプションで、アカウント名の開始文字を指定できます。

- **0-9** を選択すると、アカウントは指定された数字から順に命名されます。前のフィールドで使用するワイルドカードの数に応じて、1桁以上の数字を入力します。たとえば、2つのワイルドカードを使用する場合は、2桁以上の数字を入力します。
- **A-Z** を選択すると、アカウントは指定された文字から順に命名されます。前のフィールドで使用するワイルドカードの数に応じて、1文字以上の文字を入力します。たとえば、2つのワイルドカードを使用する場合は、2文字以上の文字を入力します。

ドメイン資格情報

アカウント操作を実行する権限を持つ管理者の資格情報を入力します。詳細な手順は次のとおりです。

1. **資格情報の入力**をクリックします。Windowsセキュリティページが表示されます。
2. **ユーザー名**フィールドに、管理者のSamName、ユーザー名、またはユーザーSIDを入力します。
   - SamNameを入力すると、**Domain** フィールドが自動的に入力されます。
   - ユーザー名またはSIDを入力した場合、**Domain** フィールドにドメイン名またはSIDを入力することで、ユーザー検索を特定のドメインに限定できます。
3. **Check name** をクリックして、ユーザー名が有効か一意であるかを確認します。
4. **Password** フィールドに、管理者のドメインパスワードを入力します。
5. 「**完了**」をクリックします。

> **注:**
>
> **Machine Identities** で選択したIDタイプが **Microsoft Entra hybrid joined** の場合、入力する資格情報には `Write userCertificate` 権限が付与されている必要があります。

概要、名前、および説明

「**概要**」ページで、指定した設定を確認します。カタログの名前と説明を入力します。この情報はWeb Studioに表示されます。

完了したら、**「完了」をクリックしてカタログの作成を開始します。 完了したら、**「完了」**を選択してカタログの作成を開始します。

マシンカタログに、新しいカタログがインラインの進行状況バーとともに表示されます。

作成の進行状況の詳細を表示するには：

1. マシンカタログにマウスを合わせます。
2. 表示されるツールヒントで、**詳細の表示**をクリックします。

   以下の内容を確認できる段階的な進行状況グラフが表示されます。

   - 手順の履歴
   - 現在のステップの進行状況と実行時間
   - 残りのステップ

MCSの時刻同期

時刻同期は、マスターイメージと、参加しているマシンIDカタログのタイプによって決定されます。マスターイメージとカタログに応じて、次の時刻同期方法が適用されます。

マスターイメージ	カタログ	結果の時刻同期方法
NDJ	AD または Microsoft Entra ハイブリッド	デフォルトではNT5DSです。マスターイメージのレジストリ設定を使用して、MCSが時刻同期設定を変更するのを無効にできます。
NDJ	NDJ または Microsoft Entra ID	元の時刻同期設定と同じ
AD または Microsoft Entra ハイブリッド	AD または Microsoft Entra ハイブリッド	元の時刻同期設定と同じ
マイクロソフト エントラ ID	マイクロソフト エントラ ID	元の時刻同期設定と同じ

注:

元の時刻同期は、以下のレジストリ設定によって制御されており、変更できません。

- Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config

値: MaxAllowedPhaseOffset、MaxNegPhaseCorrection、およびMaxPosPhaseCorrection

- Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters

値: Type

MCSが時刻同期設定を変更しないようにするには、マスターイメージで以下のレジストリ設定の値を設定します。

- `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix`
- 名前: TimeSyncMethodKeep
- 種類: DWORD
- 0 (または、値TimeSyncMethodKeepが構成されていない場合): 元の時刻同期設定を保持しません。
- 1: 元の時刻同期設定とデフォルトのパラメーター値を保持します。

カスタムプロパティの設定に関する重要な考慮事項

GCPおよびAzure環境では、カスタムプロパティを`New-ProvScheme`と`Set-ProvScheme`で正しく設定する必要があります。存在しないカスタムプロパティを指定すると、次のエラーメッセージが表示され、コマンドは実行に失敗します。

- Azureの場合: `Invalid property found: <invalid property>. Ensure that the CustomProperties parameter supports the property.`.
- GCPの場合: `Invalid property found: <invalid property>. Ensure that the value supplied for the property is supported in the Hypervisor.`.

トラブルシューティング

重要:

Web Studio を使用してマシンカタログを作成した後、`Get-ProvTask` PowerShell コマンドを使用して、マシンカタログ作成に関連するタスクを取得することはできません。この制限は、カタログが正常に作成されたかどうかにかかわらず、Web Studio がマシンカタログ作成後にそれらのタスクを削除するためです。

> Citrix では、サポートチームが解決策を提供できるよう、ログを収集することをお勧めします。Citrix Provisioning を使用している場合は、次の手順でログファイルを生成します。

1. マスターイメージで、値 1 (DWORD (32 ビット) 値として) を持つ次のレジストリキーを作成します: `HKLM\Software\Citrix\MachineIdentityServiceAgent\LOGGING`。
2. マスターイメージをシャットダウンし、スナップショットを作成します。
3. Delivery Controller で、次の PowerShell コマンドを実行します: `Set-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown -Value $True`。
4. そのスナップショットに基づいてカタログを作成します。
5. ハイパーバイザー上に準備 VM が作成されたら、ログインして `C:\` のルートから次のファイル (Image-prep.log および PvsVmAgentLog.txt) を抽出します。
6. マシンをシャットダウンすると、その時点で障害が報告されます。
7. イメージ準備マシンの自動シャットダウンを再度有効にするには、次の PowerShell コマンドを実行します: `Remove-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown`。

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

MCS I/Oライトバックキャッシュディスクに特定のドライブ文字を割り当てることができます。この実装により、使用するアプリケーションのドライブ文字とMCS I/Oライトバックキャッシュディスクのドライブ文字との競合を回避できます。これを行うには、PowerShellコマンドを使用します。サポートされているハイパーバイザーは、Azure、GCP、VMware、SCVMM、XenServerです。

> **注:**
>
> この機能には、VDAバージョン2305以降が必要です。

制限事項

- Windowsオペレーティングシステムのみに適用
- ライトバックキャッシュディスクに適用可能なドライブ文字：`E`から`Z`
- Azure一時ディスクがライトバックキャッシュディスクとして使用されている場合は適用されません

- 新しいマシンカタログを作成する場合にのみ適用されます

ライトバックキャッシュディスクにドライブ文字を割り当てる

ライトバックキャッシュディスクにドライブ文字を割り当てるには:

1. **PowerShell**ウィンドウを開きます。
2. `asnp citrix*`を実行します。
3. まだ作成されていない場合は、IDプールを作成します。詳細については、「カタログの作成」を参照してください。
4. プロパティ`WriteBackCacheDriveLetter`を指定して、`New-ProvScheme`コマンドを使用してプロビジョニングスキームを作成します。例：

```
New-ProvScheme -CleanOnBoot `

-HostingUnitName "<name>" `

-IdentityPoolName $schemeName `

-ProvisioningSchemeName $schemeName `

-InitialBatchSizeHint 1 `

-UseWriteBackCache -WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256 -WriteBackCacheDriveLetter E `

-MasterImageVM "XDHyp:\HostingUnits\<name>\image.folder\abcd-
resources.resourcegroup\MCSIOMasterVm_OsDisk_1_d3e2d6352xxxxxxxxx2130aa
145ec77.manageddisk" `

-NetworkMapping @{"0"="XDHyp:\\HostingUnits\\name\
\virtualprivatecloud.folder\\East US.region\
\virtualprivatecloud.folder\\abcd-resources.resourcegroup\\abcd-
resources-vnet.virtualprivatecloud\\default.network"} `

-ServiceOffering "XDHyp:\\HostingUnits\\<name>\\serviceoffering.folder\
\Standard_D2s_v5.serviceoffering" `

-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
```

```
<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS"/>

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PersistOsDisk"
Value="false" />

<Property xsi:type="StringProperty" Name="PersistVm" Value="false" />

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="UseTempDiskForWBC"
Value="false" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="abcd-
group1" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

</CustomProperties>'
```

5. カタログの作成を完了します。

MCSマシンカタログを作成する前に構成を検証する

`New-ProvScheme`コマンドの`-validate`パラメーターを使用して、MCSマシンカタログを作成する前に構成設定を検証できます。このPowerShellコマンドをパラメーター付きで実行すると、誤ったパラメーターが使用されている場合や、パラメーターが別のパラメーターと競合している場合に、適切なエラーメッセージが表示されます。その後、エラーメッセージを使用して問題を解決し、PowerShellを使用してMCSマシンカタログを正常に作成できます。現在、この機能はAWS、Azure、GCP、およびVMwareの仮想化環境に適用できます。

注:

検証中は、実際のMCSマシンカタログを作成してはなりません。コマンドの結果を使用してエラーを修正し、その後で正常なカタログを作成する必要があります。したがって、`New-ProvScheme`コマンドを実行する際は、架空のIDプール名を使用してください。

構成を検証するには、次の手順を実行します。

1. Delivery ControllerホストからPowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*`を実行します。
3. `New-ProvScheme`コマンドを実行し、パラメーター`-validate`を使用します。コマンドが機能するように、架空のIDプール名を提供します。例：

```
$result =New-ProvScheme  -CleanOnBoot -HostingUnitName "vSanRg"
-IdentityPoolName "mptmpcatalogdemo" -InitialBatchSizeHint 1  -
MasterImageVM "XDHyp:
\HostingUnits\vSanRg\Windows19MasterImage.vm\Citrix_XD_NonMachineProfil
eWin19Machines.snapshot" -NetworkMapping @{"0"="XDHyp:
\HostingUnits\vSanRg\\VM Network.network"} -ProvisioningSchemeName
"MachineProfileW10Machines"  -Scope @()

-VMCpuCount 2  -VM

MemoryMB 6143 -MachineProfile "XDHyp:\HostingUnits\vSanRg\TRW-Win11-
tpm-BL-TEMPLATE.template" -TenancyType Shared  -FunctionalLevel "L7_20"
-Validate

$result.TerminatingError | Format-List -Property *
```

エラーメッセージ：

```
ErrorData    : {[[ValidationFailureCount, xxx], [InvalidMemoryValue,
The memory size provided 6143 must be a multiple of 4 MB and must be
greater than or equal to 4 MB.], [InconsistentGuestOsSetting, The
GuestOs setting - windows9_64Guest of the selected machine profile does
not match with the setting - windows2019srv_64Guest of master image.
Please select a machine profile that matches the GuestOs setting of the
master image.], [InconsistentVtpmSetting, The vTPM setting of the
selected machine profile does not match with the selected master image.
```

```
Please select a machine profile that matches the vTPM setting of the
master image.], [InconsistentFirmwareSetting, The firmware setting -
efi of the selected machine profile does not match with the setting -
bios of master image. Please select a machine profile that matches the
firmware setting of the master image ErrorId      : ValidationFailure

ErrorMessage : ValidationFailure

Operation    : ValidatingInputs
```

4. 構成設定を検証した後、実際のIDプール名と正しいパラメーターを使用してMCSマシンカタログを作成できます。

VMをAzure Arcにオンボードする

Azure Arcを使用すると、組織はどこにホストされているVMなどのリソースを、Azureで実行されているかのように管理できます。Azure Arcを使用すると、Azure MonitorなどのAzureサービスを利用して、リソースの包括的な可視性とプロアクティブな管理を実現できます。

VM を Azure Arc にオンボードするには、`New-ProvScheme` コマンドを使用して MCS マシンカタログを作成します。`Set-ProvScheme` コマンドを使用して既存のカタログを更新することもできます。カタログに追加された新しい VM のみが Azure Arc にオンボードされます。

現在、この機能は、Citrix のすべてのオンプレミスハイパーバイザーである VMware、Nutanix、SCVMM に適用されます。

前提条件

MCS カタログで Azure Arc オンボーディングを有効にする前に、以下を考慮してください。

- Azure リソースグループ（以下を含む）：
  - Arc サーバーの読み取り、作成、削除を行うための `Allows` アカウント。
  - VM 拡張機能、ライセンス、プライベートリンクスコープを管理するための `Allows` アカウント。
  - リソースグループスコープでサービスプリンシパルに割り当てられている `Azure Connected Machine Resource Administrator` ロール。

「Azure portal を使用して Azure ロールを割り当てる」を参照してください。

- マスターイメージ（以下を含む）
  - VDA: 2311 以降 (2411 を除く)。

> **注:**
>
> CVAD 2411では、Azure Arcオンボーディングはサポートされていません。

- AzureConnectedMachineAgent エージェントがインストールされていること。MSI は、Microsoft のドキュメントの Windows または Linux セクションからダウンロードできます。

VM を Azure Arc にオンボードする手順

1. `AzureArcResourceManagement`機能を持つサービスアカウントをセットアップします。

   サービスアカウントは、Microsoft Entra IDなどのIDプロバイダーにアクセスするための資格情報を保存することで、認証または承認に使用されます。各サービスアカウントは、単一のIDプロバイダーに紐付けられます。

   `AzureArcResourceManagement capability`を使用してAzureADにアクセスするための新しいサービスアカウントを作成するには、以下を実行します:

   ```
   New-AcctServiceAccount -IdentityProviderType “AzureAD”
   -IdentityProviderIdentifier “tenant-id” -AccountId “application-id”
   -AccountSecret “application-secret” -Capabilities
   “AzureArcResourceManagement”
   ```

   `application-id`は、Azure Connected Machine Resource Administratorロールが割り当てられたサービスプリンシパルと同じである必要があります。

2. サービスアカウントをIDプールに割り当てます。例:

   ```
   Set-AcctIdentityPool -IdentityPoolUid “idn-pool-uid” -ServiceAccountUid
   “service-account-uid”
   ```

3. 以下のArcパラメーターを使用して、MCSカタログを作成または更新します。

   - `EnableAzureArcOnboarding`: カタログでArcオンボーディングを有効にする必要があるかどうかを示します。
   - `AzureArcSubscriptionId`: Arc接続されたVMが作成されるAzureサブスクリプションを示します。
   - `AzureArcRegion`: Arc接続されたVMが作成されるAzureリージョンを示します。

- `AzureArcResourceGroup`: Arc接続されたVMが作成されるAzureリソースグループを示します。Azure Arcリソースグループの詳細については、を参照してください。

例: 新しいカタログでAzure Arcオンボーディングを有効にするには:

```
`New-ProvScheme -ProvisioningSchemeName "demo" -MasterImageVM "XDHyp:
\HostingUnits\hosting-unit\masterVMName.vm\masterSnapshotName.snapshot"
-HostingUnitName “hosting-unit” -IdentityPoolName “identity-pool”`



-EnableAzureArcOnboarding -AzureArcSubscriptionId “azure-sub”
-AzureArcResourceGroup “azure-resourcegroup” - AzureArcRegion “azure-
region”
```

例: 既存のカタログでAzure Arcオンボーディングを有効にするには:

```
Set-ProvScheme -ProvisioningSchemeName "demo" -EnableAzureArcOnboarding
$true -AzureArcSubscriptionId “azure-sub” -AzureArcResourceGroup
“azure-resourcegroup” - AzureArcRegion “azure-region”
```

例: 既存のカタログでAzure Arcオンボーディングを無効にするには:

```
Set-ProvScheme -ProvisioningSchemeName "demo" -EnableAzureArcOnboarding
$false:
```

4. Arcをオンボーディングするために、新しいマシンをカタログに追加します。
5. VMの電源をオンにした後、Azureポータルの**AzureArcResourceGroup**の下に、接続されたマシンとしてVMが表示されるはずです。

考慮事項

- Arc のオンボーディングは現在、新しい VM のみでサポートされています。そのため、`Set-ProvScheme` を使用して既存のカタログを更新した場合、新しく追加された VM のみが最初に電源がオンになったときに Arc にオンボーディングされます。
- Arc カスタムプロパティは、下位互換性のために既存のカタログで引き続きサポートされています。ただし、`EnableAzureArcOnboarding` のような Arc カスタムプロパティを使用して `New-ProvScheme` を実行すると、カタログの作成は失敗します。

- `EnableAzureArcOnboarding` を `true` として構成する場合、`New-ProvScheme` と `Set-ProvScheme` のすべてのパラメーターを追加する必要があります。

トラブルシューティング

`New-ProvScheme` を使用して SCVMM カタログを作成すると、次のエラーが発生する場合があります。

```
Master Image/Machine Profile's VM's device id is different than the
NetworkMapping's device id '0'. Please provide a device id that matches
the master image/machine profile.
```

その場合は、`New-ProvScheme` の `NetworkMapping` パラメーターで `DeviceId` を明示的に指定してください。例:

```
New-ProvScheme -ProvisioningSchemeType "MCS" -InitialBatchSizeHint 1
-HostingUnitName $HostingUnitName `

            -IdentityPoolName $CatalogName -MasterImageVM $MasterImage
-ProvisioningSchemeName $CatalogName `

            -VMCpuCount 2 -VMMemoryMB 4096  -EnableAzureArcOnboarding `

            -AzureArcSubscriptionId $AzureArcSubscription -AzureArcRegion
$AzureArcRegion `

            -AzureArcResourceGroup $AzureArcResourceGroup

            -NetworkMapping @{"FDDxxxxxx-xxxx-4xxx-9EBC-3xxxxxxxx"="XDHyp:
\HostingUnits\<hosting unit name>\abc.network"}
```

サポートされているオンプレミスハイパーバイザーの追加ストレージのイメージレプリケーション

この機能により、オンプレミスハイパーバイザーでサポートされている複数のストレージロケーション間で、イメージバージョン仕様インスタンスの効率的なレプリケーションと管理が可能になります。

ユースケース

- イメージバージョンを新しいストレージの場所または置き換えられたストレージの場所に複製できます。これにより、イメージ準備プロセス中またはその後に、仮想マシンを追加の場所にプロビジョニングできます。
- 新しいイメージバージョンが作成され、追加のストレージの場所が指定されると、準備されたイメージバージョンの仕様は、それらの指定されたストレージの場所に自動的に複製されます。
- 置き換えられたストレージの場所または新しく追加されたストレージの場所で既存のイメージバージョンを使用する必要がある場合は、新しいストレージの場所に複製するためにイメージバージョンインスタンスを追加できます。
- 既存のイメージバージョンにホスティングユニットが追加され、追加のストレージとともに、準備されたイメージバージョンの仕様インスタンスは、ターゲットホスティングユニット内の指定された追加ストレージに複製されます。

PowerShell コマンド

- 準備されたイメージバージョンの仕様を指定されたストレージの場所に複製する新しいイメージインスタンスを追加します。

```
Add-ProvImageVersionSpecInstance -ImageVersionSpecUid <
ImageVersionSpecUid > -StorageIds "<StorageId1,StorageId2>"
-RunAsynchronously
```

- 既存のイメージバージョンの仕様インスタンスレプリカを削除し、既存のVMによって使用されていないもの。

```
Remove-ProvImageVersionSpecInstance -ImageVersionSpecUid <
ImageVersionSpecUid >  -ImageInstanceUid < ImageInstanceUid >
-RunAsynchronously
```

- イメージバージョンの仕様インスタンスのリストを取得します。

```
Get-ProvImageVersionSpecInstance -ImageVersionSpecUid  <
ImageVersionSpecUid >
```

次のステップ

特定のクラウドサービスカタログの作成については、以下を参照してください。

- AWS カタログを作成する
- XenServerカタログを作成する
- Google Cloud Platform カタログを作成する
- Microsoft Azure カタログを作成する
- Microsoft System Center Virtual Machine Manager カタログを作成する
- Nutanix カタログを作成する
- VMwareカタログを作成する

これが最初に作成するカタログである場合、Web Studioはデリバリーグループの作成を案内します。

設定プロセス全体を確認するには、インストールと構成を参照してください。

Web StudioとPowerShellを使用してCitrix Provisioningカタログを作成できます。 この実装には、次の利点があります。

- MCSとCitrix Provisioningカタログの両方を管理するための単一の統合コンソール。
- ID管理ソリューション、オンデマンドプロビジョニングなど、Citrix Provisioningカタログの新機能があります。

現在、この機能はAzureおよびVMwareワークロードでのみ利用可能です。ただし、VMware環境では、現在PowerShellコマンドのみを使用してカタログを作成できます。詳細については、Citrix StudioでCitrix Provisioningカタログを作成するを参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの管理

Amulet Hotkey CoreStation マシンカタログを作成する（プレビュー）

「マシンカタログの作成」(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/machine-catalogs-create.html)では、汎用マシンカタログワークフローについて説明します。以下の情報は、Amulet Hotkey CoreStation固有の詳細を扱います。

> **注:**

> Amulet Hotkey CoreStationカタログを作成する前に、「Amulet Hotkey CoreStationへの接続」(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/connections/connection-amulet-hotkey.html)を完了してください。

> Amulet Hotkey CoreStationマシンカタログは、以下を使用して作成できます。

- ウェブスタジオ
- (#using-powershell-commands)

Web Studioの使用

マシンカタログセットアップウィザードで：

1. **オペレーティングシステム**ページで、**マルチセッションOS**または**シングルセッションOS**を選択します。
2. **マシン管理**ページで、**電源管理されているマシンと別のサービスまたはテクノロジ**を選択します。
3. **仮想マシン**ページで、マシンとそのActive Directoryマシンアカウントを追加します。次のいずれかを実行できます。
   - **マシンの追加**をクリックして、マシンを手動で追加します。**VMの選択**ウィンドウが表示されます。以前に作成したAmulet Hotkey CoreStationエンクロージャ接続を展開し、追加するノードを選択します。その後、関連するマシンアカウント名を追加します。
   - 「**CSVファイルの追加**」をクリックして、マシンを一括追加します。CSVファイルを使用してマシンを追加する方法については、「CSVファイルを使用してマシンをカタログに一括追加する」を参照してください。

「**スコープ**」ページと「**概要**」ページには、Amulet Hotkey CoreStation固有の情報は含まれていません。

PowerShellコマンドの使用

`New-BrokerCatalog`および`New-BrokerMachine` PowerShellコマンドを実行して、ブローカーカタログを作成し、マシンをブローカーカタログにインポートします。

例:

```
New-BrokerCatalog  -AdminAddress "MyDDC.MyDomain.local" -AdminClientIP
"103.14.252.249" -AllocationType "Random" -IsRemotePC $False
-MachinesArePhysical $False -MinimumFunctionalLevel "L7_20" -Name "BurMC"
-PersistUserChanges "OnLocal" -ProvisioningType "Manual" -Scope @()
```

```
-SessionSupport "MultiSession" -ZoneUid "e166e2cb-25dc-4578-bc07-
bcf2a82d1463"

New-BrokerMachine  -AdminAddress "MyDDC.MyDomain.local" -AdminClientIP
"103.14.252.249" -CatalogUid 3 -HostedMachineId "c10n1"
-HypervisorConnectionUid 4 -IsReserved $False -MachineName
"S-1-5-21-2589939477-3963209805-1860259709-1121"
```

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成を案内します。
- 構成プロセス全体を確認するには、「」(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure.html)を参照してください。
- 電源管理については、Amulet Hotkey CoreStation VM の電源管理を参照してください。

詳細情報

- 接続とリソースの作成および管理
- アミュレット ホットキー コアステーションへの接続
- マシンカタログの作成

AWS EC2カタログを作成する

マシンカタログの作成では、マシンカタログを作成するウィザードについて説明します。以下の情報は、AWS EC2仮想化環境に固有の詳細を扱います。

> **注:**

> AWSカタログを作成する前に、AWSへの接続の作成を完了する必要があります。AWS EC2への接続を参照してください。

イメージ準備中のネットワーク設定

イメージ準備中に、元のVMに基づいて準備用仮想マシン（VM）が作成されます。この準備用VMはネットワークから切断されます。準備用VMからネットワークを切断するために、すべてのインバウンドおよびアウトバウンドトラフィックを拒否するネットワークセキュリティグループが作成されます。このネットワークセキュリティグループは永続的であり、再利用されます。ネット

ワークセキュリティグループの名前は`Citrix.XenDesktop.IsolationGroup-GUID`で、GUIDはランダムに生成されます。

AWSテナンシー

AWSは以下のテナンシーオプションを提供します。

- 共有テナンシー（デフォルトタイプ）と専用テナンシー。共有テナンシーとは、異なる顧客の複数のAmazon EC2インスタンスが同じ物理ハードウェア上に存在する可能性があることを意味します。
- 専用テナンシーとは、お客様のEC2インスタンスが、お客様がデプロイした他のインスタンスと同じハードウェア上でのみ実行されることを意味します。他の顧客は同じハードウェアを使用しません。

AWSホストへのプロビジョニングの要件

- インポートされたBYOL（bring your own license）イメージ（AMI）。専用ホストでは、既存のライセンスを使用および管理します。
- プロビジョニング要求を満たすのに十分な利用率を持つ専用ホストの割り当て。
- **自動配置**を有効にする。

AWSテナンシーを設定するオプション

- **共有ハードウェアを使用**。この設定は、ほとんどの展開に適しています。複数の顧客が互いにやり取りすることはありませんが、ハードウェアの一部を共有します。共有ハードウェアを使用することは、Amazon EC2インスタンスを実行するための最も安価なオプションです。
- **専用ホストを使用**。Amazon EC2専用ホストは、EC2インスタンス容量が完全に専用化された物理サーバーであり、既存のソケットごとまたはVMごとのソフトウェアライセンスを使用できます。専用ホストは、インスタンスタイプに基づいて事前に設定された利用率を持っています。たとえば、C4 Largeインスタンスタイプの単一の割り当て済み専用ホストは、16インスタンスの実行に制限されます。詳細については、AWSサイトを参照してください。

  この設定は、ライセンス制限や専用ホストの使用を必要とするセキュリティ要件がある展開に適しています。専用ホストを使用すると、物理ホスト全体を所有し、時間単位で課金されます。そのホストを所有することで、追加料金なしで、そのホストが許可する数のEC2インスタンスを起動できます。
- **専用インスタンスを使用**。この設定は、特定のセキュリティまたはコンプライアンス要件がある展開により適しています。専用インスタンスを使用すると、他のAWS顧客とは別のホストを持つという利点を享受できますが、ホスト全体に対して料金を支払う必要はありません。ホス

トの容量について心配する必要はありませんが、インスタンスに対してはより高い料金が課金されます。

注:

カタログ作成またはイメージ更新タスクが進行中でない場合、利用可能な準備IDディスクを削除できます。

Studio を使用して AWS テナンシーを構成するには、Web Studio を使用してカタログを作成する を参照してください。PowerShell を使用する場合は、PowerShell を使用して AWS 専用ホストのテナンシーを構成する を参照してください。

AWS運用リソースのタグ付け

Amazon マシンイメージ (AMI) は、Amazon Cloud 環境内で仮想マシンを作成するために使用される仮想アプライアンスの一種であり、一般にEC2と呼ばれます。AMIを使用して、EC2環境を使用するサービスを展開します。AWS向けMCSを使用してマシンをプロビジョニングするカタログを作成するときは、そのカタログのゴールデンイメージとして機能する**AMI**を選択します。

重要:

運用リソースのタグ付けを使用するには、マシンプロファイルと起動テンプレートの両方を使用してカタログを作成する必要があります。

AWSカタログを作成するには、まずゴールデンイメージとするインスタンスのAMIを作成する必要があります。MCSはそのインスタンスからタグを読み取り、起動テンプレートに組み込みます。起動テンプレートのタグは、AWS環境で作成されたすべてのCitrix®リソースに適用されます。これには以下が含まれます。

- 仮想マシン
- VMディスク
- VMネットワークインターフェイス
- S3 バケット
- S3 オブジェクト
- 起動テンプレート

- AMI

カタログの作成中に、Studio と PowerShell を使用して運用リソースにタグを付けることができます。Studio の場合は、Web Studio を使用してカタログを作成する（**イメージ**ページ）を参照してください。PowerShell の場合は、PowerShell を使用して運用リソースにタグを付ける を参照してください。

カタログを作成する

次のいずれかを使用してカタログを作成できます。

- ウェブスタジオ
- PowerShell

Web Studio を使用してカタログを作成する

1. 左側のナビゲーションペインで**マシンカタログ**をクリックします。
2. **マシンカタログの作成**をクリックします。**マシンカタログのセットアップ**ページが表示されます。
3. ページで、カタログのマシンの種類（例: マルチセッションOS）を選択します。
4. **マシン管理**ページで、次の設定を選択します。
    a. 電源管理されているマシン（仮想マシンやブレードPCなど）を選択します。
    b. 「**Citrixプロビジョニングテクノロジー**」を選択します。次に、「**Citrix Machine Creation Services™**」を選択します。
    c. **リソース**フィールドで、ホスト接続の作成時に構成したリソース（アベイラビリティゾーンまたはローカルゾーン）を選択し、**次へ**をクリックします。
5. **デスクトップエクスペリエンス**ページで、ユーザーがログインしたときに使用するランダムまたは静的デスクトップを選択します。
6. **イメージ**ページで：
    a. カタログ内のすべてのマシンのマスターイメージとして使用するマシンのテンプレートを選択します。
    b. カタログ内のVMにマシンプロファイルから構成を継承させたい場合は、マシンプロファイルを選択します。デフォルトでは、**マシンプロファイルを使用**チェックボックスが選択されています。マシンプロファイルのソースを別のVMまたは起動テンプレートバージョンに変更するには、編集ボタンをクリックします。

c. **運用リソースにマシンタグを適用**チェックボックスをオンにして、運用リソースにマシンタグを適用します。このオプションは、マシンのプロビジョニングを容易にするためにAWS環境で作成されたすべての項目にマシンタグを適用するかどうかを制御します。運用リソースは、カタログ作成の副産物として作成されます。これには、準備VMインスタンスやAMIなどの一時的および永続的なリソースの両方が含まれます。

> **注:**
>
> **セキュリティ**ページは、マシンプロファイルを割り当てずにマシンカタログを作成している場合にのみ表示されます。

7. 「**仮想マシン**」ページで：

   a. カタログのVM数を入力します。

   b. マシンプロファイルに基づいて、デフォルトのマシンスペックが表示されます。変更するには、編集アイコンを選択し、マシンスペックを選択します。

   c. AWSテナンシーを設定します。(#options-to-configure-aws-tenancy)を参照してください。

   d. プライマリマシンのサイズが最大容量に達した場合、セカンダリVMを設定することもできます。**Secondary size** (オプション) をクリックします。**Secondary machine size**ウィンドウには、スポットVMと通常VMの両方のタイプを持つVMが一覧表示されます。最大10個のセカンダリマシンサイズを選択できます。10個のVMが選択されると、リストされている他のVMはそれ以上選択できなくなります。**Next**をクリックします。**Secondary machine size**ブレードで、複数のマシンサイズを選択し、ドラッグアンドドロップで優先順位を変更できます。**Done**をクリックします。選択したマシンサイズは、Secondary size (オプション) に表示されます。必要に応じて編集するには、編集アイコンをクリックします。

8. **セキュリティ**ページは、マシンプロファイルを割り当てずにマシンカタログを作成する場合にのみ表示されます。**セキュリティ**ページを使用して、VM のセキュリティグループを構成します。これは、既存のマシンカタログを編集およびクローン作成する場合にも適用されます。

   マシンプロファイルベースのマシンカタログを作成する場合、セキュリティグループの構成はマシンプロファイルから継承され、**セキュリティ**ページは表示されません。

9. **NICs**ページで、VMのNIC (またはENI) を選択します。

10. **Disk Settings**ページで、ライトバックキャッシュを有効にするかどうかを選択します。

11. **マシンID**ページで、カタログ内のマシンに対してオンプレミスのActive Directoryまたは Microsoft Entraハイブリッド参加を設定します。これを行うには、ドメインを選択し、このマ

シンカタログで作成されるVM用の新しいADアカウントを作成します。プロビジョニングされたVMは、選択したドメインに参加します。VM用に作成される新しいADアカウントのアカウント命名スキームを指定します。次へをクリックします。

12. **Domain credentials**ページで、**Enter credentials**をクリックして、選択したドメインの資格情報を入力します。プロンプトが表示されたら、管理者レベルのユーザー名とパスワードを入力します。製品ドキュメントに従って以前にドメイン資格情報を保存している場合は、サービスアカウントを使用することもできます。
13. 「**概要**」ページが表示されるまで、残りのページをクリックします。マシンカタログの名前を入力し、「**完了**」を選択してマシンカタログを作成します。

AWSローカルゾーンでのマシンカタログ作成に関する制限事項

- 特定のローカルゾーンは特定のハードウェア構成のみをサポートしています（例：パースのローカルゾーンはGP3ボリュームをサポートせず、GP2のみをサポートします）。
- すべてのローカルゾーンでgp2のみが普遍的にサポートされており、すべてがgp3をサポートしているわけではないため、IDディスクの作成はデフォルトでgp2ボリュームタイプを使用します。
- 目的のローカルゾーンでサポートされているハードウェア仕様を持つマシンプロファイルを選択する必要があります。
- 準備済みイメージAMIスナップショットとIDディスクスナップショットは、デフォルトでローカルゾーンではなくリージョンに配置されます（ローカルゾーンでのEBSスナップショットサポートの可視性に関するAWSの制限のため）。
- 完全なEC2およびEBSサービスをサポートするローカルゾーンのみがサポート対象ゾーンです。

PowerShellを使用してカタログを作成する

PowerShell を使用して AWS 専用ホストのテナンシーを構成する

または、PowerShell を介して AWS 専用ホストをプロビジョニングすることもできます。`New-ProvScheme` コマンドレットを、パラメーター `TenancyType` を `Host` に設定して使用します。

PowerShell を使用して運用リソースにタグを付ける

PowerShell を使用してリソースにタグを付けるには：

1. DDC ホストから PowerShell ウィンドウを開きます。
2. Citrix 固有の PowerShell モジュールをロードするには、コマンド `asnp citrix` を実行します。

プロビジョニングされた VM のリソースにタグを付けるには、カスタムプロパティ `AwsOperationalResourcesTagging` を使用します。例：

```
New-ProvScheme -ProvisioningSchemeName test

-CustomProperties “AwsOperationalResourcesTagging,true”

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-01xxxxx).launchtemplate\lt-01xxxxx (1).launchtemplateversion"

... <Other <standard provscheme parameters>
```

MCSIO が有効なカタログ

MCS Storage Optimization (MCSIO) は、ディスク操作をメモリまたは小型の高速ディスクにキャッシュすることで、VM のパフォーマンスを向上させます。PowerShell コマンドを使用して、MCSIO が有効な非永続カタログを作成できます。このようなカタログを作成するには、AMI インスタンスの準備中に VDA をインストールまたはアップグレードする際に MCSIO ドライバーをインストールする必要があります。デフォルトでは、このドライバーはインストールされていません。

MCSIO AMI の準備が完了したら（VDA のインストール時に MCSIO ドライバーをインストールに含めるオプションを選択した場合）、MCSIO が有効な非永続カタログを作成できます。

> **注:**
>
> Studio を使用してディスクキャッシュのみ（メモリキャッシュなし）で MCSIO を構成するオプションは、すべてのハイパーバイザーおよびクラウドサービス環境で削除されました。

MCSIO が有効なカタログを作成する

New-ProvScheme PowerShell コマンドに追加された 4 つのパラメーターは次のとおりです。

- `UseWriteBackCache`: 指定されたプロビジョニングスキームに対してキャッシュ (ライトバックキャッシュ) を有効にします
- `WriteBackCacheDiskSize`: キャッシュに使用される一時ディスクのサイズをGB単位で指定します
- `WriteBackCacheMemorySize`: キャッシュに使用するメモリ量をMB単位で指定します。これはオプションのパラメーターです。

注:

- `WriteBackCacheDiskSize` の値は、少なくとも1GBのキャッシュディスクストレージが必要なため、ゼロより大きい必要があります。キャッシュディスクのサイズはOSディスクのサイズより大きくしてはいけません。
- `WriteBackCacheMemorySize` の値はゼロ以外で、マシンカタログのメモリサイズよりも小さい必要があります。

MCSIOに影響するカスタムプロパティは次のとおりです。

- `WBCDiskStorageType`: AWSの一時ディスクに使用されるボリュームタイプを定義します。このパラメーターは、`volume-type[:iops][:throughput]` の形式で文字列引数を取ります。ボリュームタイプは次のとおりです。
  - gp2: このボリュームタイプではiopsおよびスループットパラメーターを使用しないでください
  - gp3: このボリュームタイプではiopsおよびスループットパラメーターを使用してください
  - io1: このボリュームタイプではiopsパラメーターのみを使用してください
  - io2: このボリュームタイプではiopsパラメーターのみを使用してください

  デフォルトのボリュームタイプは **gp2** です。
- `PersistWBC`: AWSインスタンスの電源がオフになるたびに、キャッシュディスクを保持するか破棄するかを制御します。`true` に設定すると、キャッシュディスクは保持されます。`false` (デフォルト) に設定すると、キャッシュディスクはAMIインスタンスの電源がオンになっている間のみ作成および保持されます。
- `PersistOSDisk`: AWSインスタンスの電源がオフになるたびに、OSディスクを保持するか破棄するかを制御します。`true` に設定すると、OSディスクは保持されます。`false` (デフォルト) に設定すると、OSディスクはAMIインスタンスの電源がオンになっている間のみ作成および保持されます。

PowerShellウィンドウで、MCSIOが有効な非永続カタログを作成するには、次の手順を実行します。

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*` を実行します。

3. ブローカーカタログとIDプールを作成します。
4. プロビジョニングスキームを作成します。例:

```
$HostingUnitUid = '0xxxx1d9-bbfc-xxxf-bxxb-exxxxxe008b2'

$MasterImageVM = 'XDHyp:\HostingUnits\ctx-test\aws-apollo-non-
persistent-multi-mcsio-vda-win2022 (ami-0bf1810488acbxxxb).template'

$NetworkMap = @{ 'NetworkPath' = 'XDHyp:\HostingUnits\ctx-test\us-
east-1a.availabilityzone\10.0.128.0`/17
(vpc-0fa6e41d72507fxxx).network' }

$SecurityGroup = $( 'XDHyp:\HostingUnits\ctx-test\us-
east-1a.availabilityzone\private.securitygroup' )

$ServiceOffering = 'XDHyp:\HostingUnits\ctx-test\T3 Medium
Instance.serviceoffering'

$CustomProperties = 'WBCDiskStorageType,gp3:6000:250;PersistWBC,false'




$provScheme = New-ProvScheme -ProvisioningSchemeName $CatalogName
-HostingUnitUid $HostingUnitUid `

-IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `

- MasterImageVM $MasterImageVM `

-NetworkMap $NetworkMap `

-ServiceOffering $ServiceOffering `

-SecurityGroup $SecurityGroup `

-CustomProperties $CustomProperties `

-UseWriteBackCache -WriteBackCacheDiskSize 16 -WriteBackCacheMemorySize
256
```

5. カタログにVMを追加します。

MCSIOで起動パフォーマンスを向上させる

MCSIOを有効にし、`PersistWBC`と`PersistOSDisk`のカスタムプロパティを`tru`eとして設定すると、VMの起動パフォーマンスを向上させることができます。このような設定により、VMは新しいキャッシュディスクを初期化したり、テンプレートからルートディスクを再作成したりする必要がないため、より高速に起動できます。

PowerShellを使用してマシンプロファイルベースのマシンカタログを作成する

マシンプロファイルを使用して、EC2インスタンス（VM）または起動テンプレートバージョンからハードウェアプロパティをキャプチャし、プロビジョニングされたマシンに適用できます。キャプチャされるプロパティには、たとえば、EBSボリュームプロパティ、インスタンスタイプ、EBS最適化、CPUオプション、テナンシータイプ、休止状態機能、セキュリティグループ、およびその他のサポートされているAWS構成が含まれます。

AWS EC2インスタンス（VM）またはAWS起動テンプレートバージョンをマシンプロファイルの入力として使用できます。

> **注:**
>
> EBSボリュームプロパティは、マシンプロファイルからのみ派生します。

重要な考慮事項

MCSマシンカタログを作成する際の重要な考慮事項:

- `New-ProvScheme`および`Set-ProvScheme`コマンドでマシンハードウェアプロパティパラメーターを追加すると、パラメーターで指定された値がマシンプロファイルの値を上書きします。
- `AwsCaptureInstanceProperties`を`true`に設定し、`MachineProfile`プロパティを設定しない場合、IAM ロールとタグのみがキャプチャされます。
- `AwsCaptureInstanceProperties`と`MachineProfile`の両方を同時に設定することはできません。

  > **注:**
  >
  > `AwsCaptureInstanceProperties`は非推奨です。

- マシンプロファイルが提供されていない場合は、以下のプロパティの値を明示的に指定する必要があります。
  - セキュリティグループ
  - ENI または仮想ネットワーク
- `AwsOperationalResourcesTagging` は、`AwsCaptureInstanceProperties` を有効にするか、マシンプロファイルを指定した場合にのみ有効にできます。

MCS マシンカタログを作成した後の重要な考慮事項は次のとおりです。

- マシンプロファイルベースのカタログから、非マシンプロファイルベースのカタログに変更することはできません。

マシンプロファイル入力でセキュリティグループを構成する

プロビジョニングされた VM が ENI (ネットワークインターフェース) ごとにセキュリティグループを割り当てられる MCS マシンカタログを作成できます。これを行うには、異なるセキュリティグループが個別の ENI にマッピングされているマシンプロファイル入力 (EC2 インスタンスまたは起動テンプレート) を使用します。たとえば、マシンプロファイル入力に SG 1 を持つ ENI A と SG 2 を持つ ENI B がある場合、プロビジョニングされた VM も SG 1 を持つ ENI A と SG 2 を持つ ENI B を持つ必要があります。

ネットワークインターフェースの詳細を取得する

インターフェースの SubnetId、割り当てられたセキュリティグループ、および割り当てられたネットワークを含む、ネットワークインターフェースデータレコードのリストを取得するには、次のコマンドを実行します。

```
(Get-HypInventoryItem -LiteralPath 'XdHyp:\HostingUnits\cvad-test' –
ResourceType vm). AdditionalData
```

> **注:**
>
> MCSは現在、ネットワークインターフェイスごとに複数のネットワークを許可していません。

マシンプロファイルを使用してマシンカタログを作成する

マシンプロファイルを使用してマシンカタログを作成するには：

1. **PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために、`asnp citrix*`を実行します。
3. まだ作成されていない場合は、IDプールを作成します。例：

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms##
-Domain abcdf -NamingSchemeType Numeric
```

4. New-ProvSchemeコマンドを実行します。例：

```
New-ProvScheme -ProvisioningSchemeName demet-test-1

-HostingUnitUid aa633238-9xxd-4cf6-80e8-232a758a1xx1

-IdentityPoolUid 34d5b088-e312-416f-907d-16573xxxxxc4

-CleanOnBoot

-MasterImageVM 'XDHyp:\HostingUnits\cvad-test-scalestress\citrix-demet-
ami.0 (ami-0ca813xxxxxx061ef).template'

-MachineProfile 'XdHyp:\HostingUnits\cvad-test-scalestress\us-
east-1a.availabilityzone\machine-profile-instance i (i-0xxxxxxxx).vm'
```

5. カタログの作成を完了します。

マシンプロファイルを更新する

マシンプロファイルで最初にプロビジョニングされたカタログのマシンプロファイルを更新するには、以下を実行します。MCSマシンカタログの編集中に、マシンプロファイルソースのテナンシータイプとハイバネーション機能も変更できます。

1. `Set-ProvScheme`コマンドを実行します。例：

```
Set-ProvScheme `

-ProvisioningSchemeUid "<ID" `

-MachineProfile "XDHyp:\HostingUnits\abc\us-
east-1a.availabilityzone\citrix-cvad-machineprofile-instance
(i-0xxxxxxxx).vm"
```

PowerShellを使用して起動テンプレートバージョンでカタログを作成する

起動テンプレートバージョンをマシンプロファイルの入力として使用して、MCSマシンカタログを作成できます。また、マシンプロファイルカタログの入力をVMから起動テンプレートバージョンへ、および起動テンプレートバージョンからVMへ更新することもできます。

AWS EC2コンソールでは、起動テンプレートのインスタンス構成情報をバージョン番号とともに提供できます。マシンカタログの作成または更新中に、起動テンプレートバージョンをマシンプロファイルの入力として指定すると、そのバージョンの起動テンプレートからのプロパティがプロビジョニングされたVDA VMにコピーされます。

以下のプロパティは、マシンプロファイル入力を使用するか、`New-ProvScheme` または `Set-ProvScheme` コマンドのパラメーターとして明示的に指定できます。`New-ProvScheme` または `Set-ProvScheme` コマンドで指定された場合、これらのプロパティのマシンプロファイル値よりも優先されます。

- サービス提供
- ネットワーク
- テナンシータイプ

> **注:**
>
> マシンプロファイルの起動テンプレートでサービス提供が指定されていない場合、または `New-ProvScheme` コマンドのパラメーターとして指定されていない場合、適切なエラーが発生します。

> 起動テンプレートバージョンをマシンプロファイル入力として使用してカタログを作成するには:

1. **PowerShell** ウィンドウを開きます。
2. Citrix 固有の PowerShell モジュールをロードするには、`asnp citrix*` を実行します。
3. 起動テンプレートの起動テンプレートバージョンの一覧を取得します。例:

   ```
   XDHyp:\HostingUnits\test\test-mp-sard (lt-01xxxxx).launchtemplate> ls |
   Select FullPath
   ```

4. 作成されていない場合は、ID プールを作成します。例:

```
New-AcctIdentityPool `

-IdentityPoolName "abc11" `

-NamingScheme "abc1-##" `

-NamingSchemeType Numeric `

-Domain "citrix-xxxxxx.local" `

-ZoneUid "xxxxxxxx" `
```

5. 起動テンプレートバージョンをマシンプロファイル入力として使用してプロビジョニングスキームを作成します。例:

```
New-ProvScheme `

-ProvisioningSchemeName "MPLT1" `

-HostingUnitUid "c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `

-IdentityPoolUid "bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\xxxd-ue1a\apollo-non-persistent-
vda-win2022 (ami-0axxxxxxxxxxx).template" `

-CleanOnBoot `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-01xxxxx).launchtemplate\lt-01xxxxx (1).launchtemplateversion"
```

6. プロビジョニングスキームをブローカーカタログとして登録します。例:

```
New-BrokerCatalog -Name "MPLT1" `

-AllocationType Random `

-Description "Machine profile catalog" `

-ProvisioningSchemeId fe7df345-244e-4xxxx-xxxxxxxxx `
```

```
-ProvisioningType Mcs `

-SessionSupport MultiSession `

-PersistUserChanges Discard
```

7. カタログの作成を完了します。

マシンプロファイルソースを更新する

VMから起動テンプレートバージョンへ、および起動テンプレートバージョンからVMへ、マシンプロファイルカタログの入力を更新することもできます。例:

- VMから起動テンプレートバージョンへマシンプロファイルカタログの入力を更新するには:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-0bxxxxxxxxxxxx).launchtemplate\lt-0bxxxxxxxxxxx
(1).launchtemplateversion"
```

- 起動テンプレートバージョンからVMへマシンプロファイルカタログの入力を更新するには:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\sard-ue1a\us-
east-1a.availabilityzone\apollo-non-persistent-vda-win2022-2
(i-08xxxxxxxx).vm"
```

OS、ID、およびWBCディスクの暗号化

AWS KMSキー (カスタマー管理キーおよびAWS管理キー) を使用して、永続的および非永続的なVMのカタログを作成できます。これらのキーは、OSディスク、IDディスク (ID)、およびライトバックキャッシュディスク (WBC) の暗号化に使用できます。

- AWS管理キーは毎年自動的にローテーションされます。
- カスタマー管理キーは自動ローテーションがオプションであり、手動で管理できます。

KMSキーの詳細については、以下のAWSドキュメントを参照してください:

- AWS KMS の概念

- 自動キーローテーションの仕組み

OS、ID、およびWBCディスクの暗号化には、以下のいずれかを構成します:

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

制限事項

以下の制限事項を考慮してください:

- MCS は現在、マスターイメージ AMI 上のディスクを 1 つのみサポートしています。
- 既存の暗号化されていない EBS ボリュームまたはスナップショットを直接暗号化したり、既存の暗号化されたボリュームの KMS キーを変更したりすることはできません。これを行うには、次の手順を実行する必要があります。

  a. そのボリュームの新しいスナップショットを作成します。

  b. そのスナップショットから新しいボリュームを作成します。

  c. 新しいボリュームを暗号化します。

以下の AWS ドキュメントを参照してください。

- 暗号化されていないリソースを暗号化する
- EBS ボリュームの自動またはデフォルトの暗号化の制限: 既存および新規の Amazon EBS ボリュームを自動的に暗号化する。

ディスク暗号化を使用してカタログを作成する

ディスク暗号化を使用して MCS マシンカタログを作成するには、次のものを使用できます。

- マスターイメージ
- マシンプロファイル

マシンプロファイル入力を使用する際の考慮事項は次のとおりです。

- マシンプロファイル入力の KMS キーは、マスターイメージの KMS キーよりも優先されます。
- マシンプロファイル入力が提供されない場合、マスターイメージ AMI の KMS キーがカタログ VM のディスクを暗号化するために使用されます。

- マシンプロファイルにブロックデバイスマッピングが存在する場合、マスターイメージテンプレート (AMI) とマシンプロファイルに存在するブロックデバイスは一致している必要があります。たとえば、AMI に `/dev/sda1` で定義されたデバイスがある場合、マシンプロファイルにも `/dev/sda1` で定義されたデバイスが必要です。
- マシンプロファイルソースにキーがなく、マスターイメージが暗号化されていない場合、カタログVMのディスクは暗号化されません。
- マスターイメージが暗号化されている場合、マシンプロファイルソースVMまたは起動テンプレートには、有効な入力と見なされるために暗号化されたルートボリュームが必要です。

既存のカタログを変更する

`Set-ProvScheme` PowerShellコマンドを使用して、既存のカタログを次のように変更できます。

- 新しいKMSキーを含むボリュームを持つマシンプロファイル入力。
- 新しいKMSキーで暗号化されたマスターイメージテンプレートAMI。

重要な考慮事項:

- カタログに追加された新しいVMのボリュームは、新しいKMSキーで暗号化されます。
- 既存のマシンプロファイルがある場合に暗号化設定を更新するには、新しいマシンプロファイルで `Set-ProvScheme` を実行します。
- 既存のカタログを、暗号化されたボリュームから暗号化されていないボリュームに変更することはできません。 暗号化されたマスターAMIから暗号化されていないマスターAMIへのイメージ更新はできません。

VMインスタンスのNitroTPMとUEFIセキュアブートを有効にする

カタログを作成する際、NitroTPMおよび/またはUEFIセキュアブートが有効なマスターイメージ (AMI) を選択できるようになりました。これにより、カタログ内のプロビジョニングされたVMもNitroTPMおよび/またはUEFIセキュアブートが有効になります。この実装により、VMが保護され、信頼できるものになります。NitroTPMおよびUEFIセキュアブートの詳細については、Amazonドキュメントを参照してください。

制限事項

- 現在、NitroTPMとセキュアブートの両方を、中国を除くすべてのAWSリージョン (AWS GovCloud (US) リージョンを含む) で使用できます。
- 既存のカタログでNitroTPMとUEFIセキュアブートを有効にすることはできません。NitroTPMとUEFIセキュアブートが有効なカタログが必要な場合は、新しいカタログを作成してください。

主な手順

1. AWS環境をセットアップします。
2. AWSへの接続を作成します。
3. NitroTPMおよび/またはUEFIセキュアブートが有効なマスターイメージ（AMI）を作成します(#create-an-ami-that-supports-nitrotpm-and-uefi-secure-boot)。
4. Web Studioのカタログ作成メニューでNitroTPMとUEFIセキュアブートが有効なマスターイメージを選択するか、PowerShellコマンドを使用してプロビジョニングスキームを作成する際に、マシンカタログを作成します。

作成されたカタログに追加されたVMには、NitoTPMとUEFIセキュアブートが有効になっています。

NitroTPMとUEFIセキュアブートをサポートするAMIを作成する

1. NitroTPMおよび/またはUEFIセキュアブートが有効なVMからAMIを作成できます。
   a. AWS Marketplaceイメージを使用してインスタンスを作成します。例：`TPM-Windows_Server-2022-English-Full-Base on the aws-marketplace`を検索します。
   b. シングルセッションまたはマルチセッションVDAをダウンロードします。
   c. そのVMからAMIを作成します。
2. register-imageコマンドを使用します。

   ```
   --boot-mode (string)

   --tpm-support (string)
   ```

   詳細については、register-imageを参照してください。

以下のAWSドキュメントを参照してください。

- EC2インスタンスタイプのサポートされているブートモードを決定する
- Amazon EC2インスタンスでNitroTPMを使用するための要件/.

Delivery controller™ホストからPowerShellウィンドウを開いて、特定の項目を確認できます。

- サービス提供がNitroTPMまたはUEFIセキュアブートをサポートしているか

```
(Get-Item -Path “XDHyp:\HostingUnits\aws\T3 Medium
Instance.serviceoffering”).AdditionalData.BootMode

(Get-Item -Path “XDHyp:\HostingUnits\aws\T3 Medium
Instance.serviceoffering”).AdditionalData.NitroTpmSupportVersions
```

- テンプレートがNitroTPMまたはUEFIセキュアブートをサポートしているか

```
(Get-HypInventoryItem -LiteralPath “XDHyp:\HostingUnits\aws”
-ResourceType “template -Id “ID”).AdditionalData.BootMode



(Get-HypInventoryItem -LiteralPath “XDHyp:\HostingUnits\aws”
-ResourceType “template -Id “ID”).AdditionalData.TpmSupport
```

既存のカタログのサービス提供を更新する

`Set-ProvScheme`を使用して、既存のカタログのサービス提供を変更できます。この変更は、新しく追加されたVMに適用されます。ただし、次のシナリオではエラーが発生します。

AMIのブートモード	AMIはNITRO TPMをサポートしていますか？	サービス提供はNITROTPMとUEFIセキュアブートをサポートしていますか？
UEFI	いいえ	いいえ
レガシーBIOS	はい	いいえ
UEFI	はい	いいえ
UEFI優先	はい	いいえ

VM上のタグをコピーする

マシンプロファイルで指定されたNICおよびディスク（IDディスク、ライトバックキャッシュディスク、OSディスク）上のタグを、MCSマシンカタログで新しく作成されたVMにコピーできます。これらのタグは、マシンプロファイルソース（AWS VMインスタンスまたはAWS起動テンプレートバージョン）のいずれかで指定できます。この機能は、永続的および非永続的なマシンカタログとVMに適用されます。

注:

- AWS EC2コンソールでは、**起動テンプレートバージョンリソースタグ**の下に**ネットワークインターフェイスのタグ付け**の値は表示されません。ただし、PowerShellコマンド `aws ec2 describe-launch-template-versions --launch-template-id lt-0bb652503d45dcbcd --versions 12` を実行してタグの仕様を確認できます。
- マシンプロファイルソース（VMまたは起動テンプレートバージョン）に2つのネットワークインターフェイス（eni-1とeni-2）があり、eni-1にタグt1、eni-2にタグt2がある場合、VMは両方のネットワークインターフェイスのタグを取得します。

PowerShellを使用してVMインスタンスをフィルタリングする

マシンプロファイルVMとして使用するAWS VMインスタンスは、マシンカタログが正しく作成され機能するために互換性がある必要があります。マシンプロファイル入力VMとして使用できるAWS VMインスタンスを一覧表示するには、`Get-HypInventoryItem` コマンドを使用できます。このコマンドは、ホスティングユニットで利用可能なVMのインベントリをページングおよびフィルタリングできます。

ページネーション：

Get-HypInventoryItemは、2つのページネーションモードをサポートしています。

- ページングモードでは、`-MaxRecords` および `-Skip` パラメーターを使用してアイテムのセットを返します。
  - `-MaxRecords`：デフォルトは**1**です。これは、返すアイテムの数を制御します。
  - `-Skip`：デフォルトは**0**です。これは、ハイパーバイザー内のリストの絶対的な先頭（または絶対的な末尾）からスキップするアイテムの数を制御します。
- スクロールモードでは、`-MaxRecords`、`-ForwardDirection`、および `-ContinuationToken` パラメーターを使用してレコードのスクロールを許可します。
  - `-ForwardDirection`：デフォルトは**True**です。これは `-MaxRecords` と組み合わせて使用され、一致するレコードの次のセットまたは前のセットを返します。
  - `-ContinuationToken`: `ContinuationToken` で指定された項目の直後（または `ForwardDirection` が**false**の場合は直前）の項目を返しますが、その項目自体は含みません。

ページネーションの例:

- 最も名前の小さいマシンテンプレートの単一レコードを返します。`AdditionalData`フィールドには`TotalItemsCount`と`TotalFilteredItemsCount`があります:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template
```

- 最も名前の小さいマシンテンプレートのレコードを10件返します:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 10 | select Name
```

- 最も名前の大きいレコードで終わるレコードの配列を返します:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ForwardDirection $False -MaxRecords 10 | select
Name
```

- 指定された`ContinuationToken`に関連付けられたマシンテンプレートから始まるレコードの配列を返します:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ContinuationToken "ami-07xxxxxxxxx"
-MaxRecords 10
```

フィルタリング:

フィルタリングには、以下の追加のオプションパラメータがサポートされています。これらのパラメータは、ページネーションオプションと組み合わせることができます。

- `-ContainsName "my_name"`: 指定された文字列がAMI名の一部と一致する場合、そのAMIは`Get`結果に含まれます。例:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -ContainName ‘apollo’ | select
Name
```

- `-Tags '{ "Key0": "Value0", "Key1": "Value1", "Key2": "Value2" }'`: AMIがこれらのタグの少なくとも1つを持っている場合、それは`Get`結果に含まれます。例:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -Tags '{"opex owner": "Not
tagged"}' | select Name
```

注:

2つのタグ値がサポートされています。**Not Tagged**タグ値は、タグのリストに指定されたタグがない項目と一致します。**All values**タグ値は、タグの値に関係なくタグを持つ項目と一致します。それ以外の場合、一致は、項目がタグを持ち、その値がフィルターで指定されたものと等しい場合にのみ発生します。

- `-Id "ami-0a2d913927e0352f3"`: AMIが指定されたIDと一致する場合、それは`Get`結果に含まれます。例:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -Id ami-xxxxxxxxxxxxx
```

AdditionalDataパラメータでのフィルタリング:

`AdditionalData`フィルターパラメータは、テンプレートまたはVMを、その機能、サービス提供、またはAdditionalDataにある任意のプロパティに基づいてリストします。例:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200).AdditionalData
```

互換性のないVMを示すために、`-Warn`パラメータを追加することもできます。VMには、**Warning**という名前の`AdditionalData`フィールドが含まれています。例:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200 -Template "ami-015xxxxxxxxx"
-Warn $true).AdditionalData
```

VMのバックアップSKUリスト

パブリッククラウドでは、特定のEC2インスタンスタイプ（「プライマリSKU」）の容量が不足することがあります。プライマリVM構成が利用できない場合、VMは起動できず、時間の損失やビジネスの中断につながります。このようなシナリオに対処するため、容量関連の問題が発生した

場合にMCSがフォールバックできるバックアップEC2インスタンスタイプ（「バックアップSKU」）のリストを提供します。

MCSマシンカタログの作成または更新時に、カスタムプロパティ`BackupVmConfiguration`を使用して、バックアップEC2インスタンスタイプ（「バックアップSKUリスト」）のリストを提供します。

プライマリEC2インスタンスが失敗した場合、MCSは指定された順序でバックアップEC2インスタンスタイプへのフォールバックを試みます。MCSが提供されたバックアップEC2インスタンスタイプのいずれにもフォールバックできない場合、エラーメッセージが表示されます。その後、プライマリEC2インスタンスの電源を再度オンにしてみてください。これが失敗した場合、MCSはバックアップEC2インスタンスタイプを再試行します。

バックアップSKUリストには、オンデマンドインスタンスを含めることができます。

この機能は、永続的および非永続的なMCSマシンカタログの両方に適用できます。

重要な考慮事項

- バックアップSKUリストには、複数のバックアップEC2インスタンスタイプを指定できます。
- バックアップSKUリストは一意である必要があります。
- バックアップEC2インスタンスは、プライマリEC2インスタンスと同じにすることはできません。
- バックアップEC2インスタンスは、有効なAWSインスタンスタイプである必要があります。
- 重複するサービス提供を指定しないでください。例: `BackupVmConfiguration,t2.small|t3.small|t2.small`は無効です。
- リストで指定されたサービス提供は、マシンカタログ構成と互換性がある必要があります。たとえば、カタログがUEFIを使用しており、バックアップリストで指定されたサービス提供がそれをサポートしていない場合、カタログの作成または更新はプレフライト中に失敗します。
- 既存のカタログのバックアップSKUリストは、`Set-ProvScheme` PowerShellコマンドを使用して変更できます。既存のVMは、`Set-ProvVM`および`Set-ProvVMUpdateTimeWindow` PowerShellコマンドを使用して変更できます。

バックアップ EC2 インスタンスを構成する

1. PowerShell ウィンドウを開きます。
2. Citrix 固有の PowerShell モジュールをロードするには、`asnp citrix*` を実行します。
3. ブローカーカタログを作成します。
4. ID プールを作成します。

5. カスタムプロパティ `BackupVmConfiguration` を使用してバックアップ EC2 インスタンスリストを追加し、プロビジョニングスキームを作成します。例:

```
$serviceOffering = "XDHyp:\HostingUnits\$hostingUnitName\T3 Medium
Instance.serviceoffering"

$customProperties =
"AwsCaptureInstanceProperties,false;AwsOperationalResourcesTagging,fals
e;BackupVmConfiguration,t2.small|t2.large|t3.small|t3.large;"

$createdProvScheme = New-ProvScheme -ProvisioningSchemeName
$provisioningSchemeName -HostingUnitName $hostingUnitName
-IdentityPoolName $provisioningSchemeName -NetworkMapping
$networkMapping -SecurityGroup $securityGroupPath -ServiceOffering
$serviceOffering -MasterImageVM $masterImageVm -CustomProperties
$customProperties
```

6. プロビジョニングスキームの一意の ID で BrokerCatalog を更新します。
7. カタログに VM を作成して追加します。

AWS Spot インスタンスを使用したカタログの作成

オンデマンドインスタンスと比較して、Spot インスタンスは最大 90% のコスト削減を実現します。Spot インスタンスは、容量が利用できなくなった場合、Amazon EC2 によって中断される可能性があり、ミッションクリティカルではないアプリケーションやデスクトップにのみ適しています。

Spot インスタンスの詳細については、AWS ドキュメント「Spot インスタンス」を参照してください。

さらに、Spot インスタンスをプライマリ EC2 インスタンスタイプとバックアップ EC2 インスタンスの両方として使用できます。MCS が容量関連の問題でフォールバックできるバックアップ EC2 インスタンスタイプ（オンデマンドおよび Spot インスタンスである「バックアップ SKU」）のリストを PowerShell を使用して提供できます。

重要な考慮事項

- スポットインスタンスのカタログは、マシンプロファイルワークフローでのみ作成する必要があります。
- 永続的なスポットインスタンスリクエストタイプのみがサポートされています。ワンタイムスポットインスタンスリクエストはサポートされていません。

- **停止**および**休止**の中断動作のみがサポートされています。
- 既存のカタログの構成をオンデマンドからスポットインスタンスへ、またはその逆に変更できます。ただし、EC2インスタンスをオンデマンドからスポットに変更するのは複雑です。AWSドキュメントの「オンデマンドからスポット料金にEC2インスタンスを切り替える」を参照してください。
- プロビジョニングされたスポットインスタンスを削除するときは、既存のスポットインスタンスリクエストをキャンセルしてください。そうしないと、AWSが新しいスポットインスタンスを作成します。

AWSスポットインスタンスを使用してカタログを作成する手順

1. スポットインスタンスでマシンプロファイルソースを作成します。スポットインスタンスを作成する手順については、「スポットインスタンスリクエストの作成」を参照してください。
2. `New-ProvScheme` PowerShellコマンドを使用して、マシンプロファイルでマシンカタログを作成します。`Set-ProvScheme`コマンドを使用してカタログを更新できます。

スポットインスタンスをバックアップSKUとして使用する

スポットインスタンスは、プライマリEC2インスタンスタイプとしてもバックアップEC2インスタンスとしても使用できます。PowerShellを使用して、容量関連の問題が発生した場合にMCSがフォールバックできるバックアップEC2インスタンスタイプ（オンデマンドおよびスポットインスタンスである「バックアップSKU」）のリストを提供できます。

> **注:**
>
> バックアップSKUリストに重複するスポットインスタンスを指定できます。例: `BackupVmConfiguration,t2.small:Spot|t2.small|t3.small` は有効です。

必要な権限

スポットインスタンスをプライマリまたはバックアップEC2インスタンスとして使用する場合、次の権限が必要です。

- `ec2:DescribeSpotInstanceRequests`
- `ec2:CancelSpotInstanceRequests`

バックアップスポットインスタンスを構成する

1. PowerShellウィンドウを開きます。
2. `asnp citrix*` を実行して、Citrix固有のPowerShellモジュールをロードします。

3. ブローカーカタログを作成します。
4. IDプールを作成します。
5. カスタムプロパティ `BackupVmConfiguration` を使用してバックアップEC2インスタンスリストを追加し、プロビジョニングスキームを作成します。例:

```
$serviceOffering \= "XDHyp:\\HostingUnits\\$hostingUnitName\\T3 Medium
Instance.serviceoffering"

$customProperties \=
"AwsCaptureInstanceProperties,false;AwsOperationalResourcesTagging,fals
e;BackupVmConfiguration,t2.small|t2.large|t3.small:Spot|t3.large:Spot"



$createdProvScheme \= New-ProvScheme \-ProvisioningSchemeName
$provisioningSchemeName \-HostingUnitName $hostingUnitName \-
IdentityPoolName $provisioningSchemeName \-NetworkMapping
$networkMapping \-SecurityGroup $securityGroupPath \-ServiceOffering
$serviceOffering \-MasterImageVM $masterImageVm \-CustomProperties
$customProperties
```

6. プロビジョニングスキームの一意のIDでBrokerCatalogを更新します。
7. カタログにVMを作成して追加します。

次のステップ

- これが最初に作成されたカタログである場合、デリバリーグループを作成するように案内されます。
- 構成プロセス全体を確認するには、インストールと構成 を参照してください。
- カタログを管理するには、マシンカタログの管理およびAWS EC2カタログの管理を参照してください。

詳細情報

- 接続とリソースの作成および管理
- AWS EC2への接続
- マシンカタログの作成

Azure Localカタログを作成する

マシンカタログを作成するウィザードについては、マシンカタログの作成で説明しています。以下の情報は、Azure Local環境に固有の詳細を扱っています。

> **注:**
>
> Azure Localマシンカタログを作成する前に、Azure Localへの接続の作成を完了する必要があります。Azure Localへの接続を参照してください。

要件

- VDAバージョン: 2507以降
- Windows 10/11 マルチセッションワークロードはサポートされていません

マスターイメージを作成する

マシンカタログを作成するには、マスターイメージが必要です。

MCSはAzure Local VMイメージをマスターイメージとして使用します。Azure Localクラスターでワークロードをプロビジョニングするために MCSを使用する前に、VDAがインストールされたAzure Local VMイメージを準備する必要があります。

1. Azureポータルを使用してAzure Local VMを作成します。
2. 作成したAzure Local VMに接続し、VDAと必要なソフトウェアをインストールします。
3. Windowsタスクスケジューラを使用して、VM起動時にシステムコンテキストで次のスクリプトを実行するスケジュールされたタスクを作成します。マスターイメージでタスクをスケジュールするこのタスクは、VDAバージョン2511以前の場合にのみ必要です。

```
$tagFileName = 'E6DA6616-8EC4-48E0-BE93-58CE6ACE3CFB.tag'



$foundDrive = $null



foreach ($drive in Get-PSDrive -PSProvider FileSystem) {
```

```
$tagPath = Join-Path $drive.Root $tagFileName

if (Test-Path $tagPath) {

    $foundDrive = $drive.Root

    break

}

}

if ([string]::IsNullOrEmpty($foundDrive)) { exit 0 }

$installScript = Join-Path $foundDrive 'install.ps1'

if (Test-Path $installScript) {

powershell.exe -NoProfile -ExecutionPolicy Bypass -File $installScript

} else { exit 1 }
```

```
sc.exe stop mocguestagent 2>$null


sc.exe delete mocguestagent 2>$null


Remove-Item 'HKLM:
\SYSTEM\CurrentControlSet\Services\EventLog\Application\mocguestagent'
-Recurse -Force -ErrorAction SilentlyContinue


$setupComplete = 'C:\Windows\Setup\Scripts\SetupComplete.cmd'


if (Test-Path $setupComplete) { & $setupComplete }
```

4. Azure Local VMを停止します。
5. 準備されたAzure Local VMからAzure Local VMイメージを作成するには、既存のAzure Local VMからVMイメージを作成するを参照してください。

注:

Azure Connected Machineエージェントバージョン1.61以降がインストールされ、オンボードされたAzure Local VMを使用してマスターイメージを準備すると、エージェント構成ファイルの削除時にアクセス拒否が発生するため、MCSでのカタログ作成がイメージ準備プロセスで失敗します。回避策として、マスターイメージの作成中に次の操作を行います: `C:\ProgramData\AzureConnectedMachineAgent\Config\agentconfig.json` に移動し、ファイルを右クリックして、**プロパティ**を選択し、**読み取り専用**属性のチェックボックスをオフにします。

カタログを作成する

Azure Localカタログを作成して、Azure Local環境でマシンを作成、配信、および電源管理できます。

> **注:**
>
> - カタログ名の長さは49文字以内にする必要があります。
> - カタログ名またはマシン命名スキームでMicrosoft Azureの予約語を使用しないでください。詳細については、Microsoft ドキュメントを参照してください。

> カタログは以下を使用して作成できます。

- ウェブスタジオ
- PowerShell

Web Studioを使用してカタログを作成する

Azure Local環境でMCSマシンカタログを作成できます。

マシンカタログセットアップウィザードで：

1. **オペレーティングシステム**ページで、**マルチセッションOS**または**シングルセッションOS**を選択します。
2. **マシン管理**ページで:
   a. 「**電源管理されているマシン（仮想マシンやブレードPCなど）**」を選択します。
   b. 「**Citrixプロビジョニングテクノロジー**」を使用してマシンを展開することを選択します。
   c. Citrix Machine Creation Services (MCS) の下にあるAzure Localホスティングユニットを選択します。
3. 「**デスクトップエクスペリエンス**」ページで、マシンタイプページで選択したマシンタイプに応じてオプションを選択します。
4. **イメージ**ページで：
   a. マスターイメージを選択します。現在、Azure Localは準備済みイメージをサポートしていません。
   b. 選択したイメージにメモを追加できます。

> **注:**
>
> - マスターイメージを選択すると、OSタイプが自動的に入力されます。
> - マシンプロファイルはサポートされていません。

5. 「**NIC**」ページで、1つ以上のNICを選択し、各カードに仮想ネットワークを関連付けます。
6. 「**仮想マシン**」ページで：
   a. 作成する仮想マシンの数を指定します。作成しない場合は0を入力します。後で、マシンを追加することで、空のカタログにVMを作成できます。
   b. 各VMが持つメモリ量（MB単位）と仮想CPU数を指定します。
   c. I/Oパフォーマンスを向上させるために、マシンのライトバックキャッシュを構成します。
7. 画面上の指示に従って、残りの手順を完了してください。これにはAzure Local固有の情報は含まれません。

Web Studioを使用して、Azure Localクラスター内の既存のマシンの能力を提供および管理するためのAzure Localカタログを作成することもできます。

マシンカタログセットアップウィザードで：

1. **オペレーティングシステム**ページで、**マルチセッションOS**または**シングルセッションOS**を選択します。
2. 「**マシン管理**」ページで、「**電源管理されているマシン**」を選択し、マシンの展開方法として「**その他のサービスまたはテクノロジー**」を選択します。
3. 「**仮想マシン**」ページで、マシンとそれらのActive Directoryマシンアカウントを追加します。次のことができます。
   - マシンを手動で追加する: をクリックして、マシンを手動で追加します。 ウィンドウが表示されます。以前に作成したAzure Local接続を展開し、追加するVMを選択します。次に、関連するマシンアカウント名を追加します。
   - CSVファイルを使用してマシンを追加する: をクリックします。CSVファイルを使用してマシンを追加する方法については、「Use CSV files to bulk add machines to a catalog」を参照してください。
4. 画面上の指示に従って、残りの手順を完了してください。これにはAzure Local固有の情報は含まれません。

PowerShellを使用してカタログを作成する

PowerShellコマンドを使用して、Azure Local環境にMCSマシンカタログを作成できます。

スクリプトのヘッダー

スクリプトのヘッダーで定義されている正しいパラメーター値を指定していることを確認してください。

```
$catalogName = "" # Name of the catalog you want to create



$masterImageResourceGroupName = "" # Name of resource group that the
master Azure Local VM image resides in



$catalogResourceGroup = "" # Name of resource group that the created VMs
reside in



$masterImage = "" # Name of the master Azure Local VM image you want to
use



$vNet = "" # Name of the logical network that the created VMs should be
attached to



$masterImagePath = "XDHyp:\HostingUnits\$hostingUnitName\image.folder\
$masterImageResourceGroupName.resourcegroup\$masterImage"



$networkMapping = @{"0"="XDHyp:\HostingUnits\$hostingUnitName\
\network.folder\$vNet.network"}



$customPropertiesXml = "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
```

```
www.w3.org/2001/XMLSchema-instance`"><Property xsi:type=`"StringProperty`"
Name=`"ResourceGroups`" Value=`"$catalogResourceGroup`" /><Property
xsi:type=`"StringProperty`" Name=`"OsType`" Value=`"Windows`" /></
CustomProperties>"
```

1つのVMでMCSカタログを作成する

エーエスエヌピー シトリックス*

マシンカタログを作成する

```
New-BrokerCatalog -AllocationType "Random" -IsRemotePC $false
-MinimumFunctionalLevel "L7_34" -Name $catalogName -PersistUserChanges
"Discard" -ProvisioningType "MCS" -SessionSupport "SingleSession"
```

IDプールを作成する

```
New-AcctIdentityPool -AllowUnicode $true -Domain "test.local"
-IdentityPoolName $catalogName -IdentityType "ActiveDirectory"
-NamingScheme "demoVM#" -NamingSchemeType "Numeric" -OU
"CN=Computers,DC=test,DC=local"
```

プロビジョニングスキームを作成する

```
New-ProvScheme -CleanOnBoot $true -CustomProperties $customPropertiesXml
-HostingUnitName $hostingUnitName -IdentityPoolName $catalogName
-MasterImageVM $masterImagePath -NetworkMapping $networkMapping
-ProvisioningSchemeName $catalogName -ProvisioningSchemeType "MCS"
-VMCpuCount 4 -VMMemoryMB 8192
```

カタログをプロビジョニングスキームにリンクする

```
$schemeUid =(Get-ProvScheme -ProvisioningSchemeName
$catalogName).ProvisioningSchemeUid.Guid



Set-BrokerCatalog -Name $catalogName -ProvisioningSchemeId $schemeUid
```

ADアカウントを作成する

```
New-AcctADAccount -Count 1 -IdentityPoolName $catalogName
```

VMをプロビジョニングする

```
New-ProvVM -ADAccountName "domain\demoVM1" -ProvisioningSchemeName
$catalogName
```

マシンをブローカーカタログに追加する

```
New-BrokerMachine -CatalogName $catalogName -MachineName 'domain\demoVM1'
```

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成を案内します。
- Azure Local VM の電源管理については、Azure Local VM の電源管理を参照してください。

詳細情報

- 接続とリソースの作成および管理
- Azure Local への接続
- マシンカタログの作成

XenServer®カタログを作成する

マシンカタログの作成では、マシンカタログを作成するウィザードについて説明します。以下の情報は、XenServer仮想化環境に固有の詳細を扱っています。

> **注:**
>
> XenServerカタログを作成する前に、XenServerへの接続の作成を完了する必要があります。XenServerへの接続を参照してください。

XenServer接続を使用してマシンカタログを作成する

GPU対応マシンには、専用のマスターイメージが必要です。これらのVMには、GPUをサポートするビデオカードドライバーが必要です。GPU対応マシンを構成して、VMがGPUを操作に使用するソフトウェアで動作できるようにします。

1. XenCenter®で、標準VGA、ネットワーク、およびvCPUを備えたVMを作成します。
2. VM構成を更新して、GPUの使用（パススルーまたはvGPUのいずれか）を有効にします。
3. サポートされているオペレーティングシステムをインストールし、RDPを有効にします。

4. Citrix VM ToolsとNVIDIAドライバーをインストールします。
5. パフォーマンスを最適化するために、Virtual Network Computing (VNC) 管理コンソールをクリアし、VMを再起動します。
6. RDPを使用するように求められます。RDPを使用してVDAをインストールし、VMを再起動します。
7. 必要に応じて、他のGPUマスターイメージのベースラインテンプレートとしてVMのスナップショットを作成します。
8. RDPを使用して、XenCenterで構成され、GPU機能を使用する顧客固有のアプリケーションをインストールします。

制限事項

- Citrix Hypervisor 8.2 Cumulative Update 1でホストされているVMを持つCitrix Virtual Apps and Desktops展開が、単一のMCSカタログで複数のGFS2 SRを使用している場合、カタログ内のVMは展開中にVDIにアクセスできません。「VDI is currently in use」というエラーが報告されます。
- Citrix Hypervisor 8.2 Cumulative Update 1は、GFS2 SRを使用したMCSフルクローンVMをサポートしていません。

詳細については、制約を参照してください。

これらの制約は、XenServer 8 以降には適用されません。

マシンプロファイルを使用してマシンカタログを作成する

MCS を使用してマシンをプロビジョニングするカタログを作成する場合、マシンプロファイルを使用して仮想マシンからハードウェアプロパティをキャプチャし、カタログ内の新しくプロビジョニングされた VM に適用できます。`MachineProfile` パラメーターが使用されていない場合、ハードウェアプロパティはマスターイメージ VM またはスナップショットからキャプチャされます。

> **注:**
>
> 現在、マシンプロファイルの入力として使用できるのは VM のみです。

> MCSIO が有効になっている場合、MCS カタログの作成後にメモリとディスクキャッシュのサイズを更新できます。マシンプロファイル入力のパラメーターの値を上書きするために、次のパラメーターを明示的に構成できます。

- `VMCpuCount`
- `VMMemory`
- `NetworkMapping`

マシンプロファイルを使用してカタログを作成するには：

1. PowerShellウィンドウを開きます。
2. `asnp citrix*`を実行します。
3. ID プールを作成します。ID プールは、作成する VM の Active Directory (AD) アカウントのコンテナです。例：

```
New-AcctIdentityPool -Domain "citrix-xxxxxx.local" -IdentityPoolName
"ExampleIdentityPool" -NamingScheme "abc1-##" -NamingSchemeType
"Numeric" -Scope @() -ZoneUid "xxxxxxxx"
```

4. Active Directoryで必要なADコンピューターアカウントを作成します。

```
$password = "password123" | ConvertTo-SecureString -AsPlainText -Force

New-AcctIdentity -IdentityPoolName "ExampleIdentityPool" -Count 10
-ADUserName "citrix-xxxxxx\admin1" -ADPassword $password

Set-AcctAdAccountUserCert -IdentityPoolName "ExampleIdentityPool"
-ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
```

5. カタログを作成するには、`New-ProvScheme`コマンドを実行します。例:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "ExampleHostingUnit"
-IdentityPoolName "ExampleIdentityPool" -InitialBatchSizeHint 2
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

</CustomProperties>'

-MasterImageVM "XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleVDA.vm\ExampleVDA.snapshot"
```

```
-ProvisioningSchemeName "ExampleCatalog" -Scope @() -SecurityGroup @()

-MachineProfile "XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleMachineProfile.vm"
```

6. プロビジョニングスキームをブローカーカタログとして登録します。例：

```
$ConfigZone = Get-ConfigZone | Where-Object { $_.Name -eq "xxxxxx" }

New-BrokerCatalog -Name "MPLT1" -AllocationType Random -Description
"Machine profile catalog" -ProvisioningSchemeId fe7df345-244e-4xxxx-
xxxxxxxxx -ProvisioningType Mcs -SessionSupport MultiSession
-PersistUserChanges Discard -ZoneUid ($ConfigZone.Uid)
```

7. カタログにVMを追加します。

新しいマシンプロファイルでカタログを更新するには：

1. `Set-ProvScheme`コマンドを実行します。例：

```
Set-ProvScheme -ProvisioningSchemeName "ExampleCatalog" -MachineProfile
"XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleMachineProfileVm.vm\ExampleMach
ineProfileSnapshot.snapshot"
```

   Set-ProvScheme コマンドの詳細については、Set-ProvSchemeを参照してください。

注:

- この場合、`Set-ProvScheme` コマンドはカタログ内の既存の VM のマシンプロファイルを変更しません。カタログに追加された新しく作成された VM のみが新しいマシンプロファイルを持ちます。
- マシンプロファイルベースのマシンカタログを、非マシンプロファイルベースのマシンカタログに変換することはできません。

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成を案内します。

- 構成プロセス全体を確認するには、「」(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure.html)を参照してください。
- カタログを管理するには、マシンカタログの管理およびXenServer カタログの管理を参照してください。

詳細情報

- 接続とリソースの作成および管理
- XenServerへの接続
- マシンカタログの作成

Google Cloud Platformカタログを作成する

(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/machine-catalogs-create.html)は、マシンカタログを作成するウィザードについて説明しています。以下の情報は、Google Cloud環境に固有の詳細を扱っています。

> **注:**
>
> Google Cloud Platform (GCP) カタログを作成する前に、GCPへの接続の作成を完了する必要があります。(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/connections/connection-gcp.html)を参照してください。

マスターVMインスタンスと永続ディスクを準備する

> **ヒント:**
>
> 永続ディスクは、仮想ディスクを指すGoogle Cloudの用語です。

マスターVMインスタンスを準備するには、計画しているマシンカタログ内のクローンVDAインスタンスに必要な構成と一致するプロパティを持つVMインスタンスを作成および構成します。この構成は、インスタンスのサイズとタイプにのみ適用されるわけではありません。メタデータ、タグ、GPU割り当て、ネットワークタグ、サービスアカウントのプロパティなどのインスタンス属性も含まれます。

マスタリングプロセスの一環として、MCSはマスターVMインスタンスを使用してGoogle Cloudのインスタンステンプレートを作成します。このインスタンステンプレートは、マシンカタログを構成するクローンVDAインスタンスの作成に使用されます。クローンインスタンスは、インスタンステンプレートが作成されたマスターVMインスタンスのプロパティ（VPC、サブネット、永続ディスクのプロパティを除く）を継承します。

マスターVMインスタンスのプロパティを要件に合わせて構成したら、インスタンスを起動し、そのインスタンスの永続ディスクを準備します。

ディスクのスナップショットまたはディスクのイメージを手動で作成することをお勧めします。これにより、意味のある命名規則を使用してバージョンを追跡し、マスターイメージの以前のバージョンを管理するためのより多くのオプションが得られ、マシンカタログ作成の時間を節約できます。独自のスナップショットを作成しない場合、MCSは一時的なスナップショットを作成します（これはプロビジョニングプロセスの終了時に削除されます）。OSディスクまたはイメージのマルチリージョンスナップショットを手動で作成すると、異なるGCPリージョンのマシンカタログに同じマスターイメージを使用することもできます。

マシンカタログを作成する

マシンカタログは、次の2つの方法で作成できます。

- Web Studio を使用してマシンカタログを作成する
- PowerShell を使用してマシンカタログを作成する

Web Studio を使用してマシンカタログを作成する

> **注:**
>
> マシンカタログを作成する前に、リソースを作成してください。マシンカタログを構成する際は、Google Cloud が定めた命名規則を使用してください。詳細については、バケットとオブジェクトの命名ガイドラインを参照してください。

> (/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/machine-catalogs-create.html)のガイダンスに従ってください。以下の説明は、Google Cloud カタログに固有のものです。

1. Web Studio にサインインし、左側のペインで を選択します。
2. アクションバーで を選択します。
3. ページで、 を選択し、 を選択します。

- Citrix Virtual Apps and Desktops™ は、シングルセッションOSもサポートしています。

4. ページで、 と オプションを選択し、 を選択します。複数のリソースがある場合は、メニューから1つ選択します。
5. ページで、必要に応じてこれらの手順を完了し、 をクリックします。

   a. マスターイメージを選択します。次のイメージタイプを選択できます。

      - 仮想マシン（リージョンが選択されたホスティングユニットと同じもの）。
      - スナップショット（マルチリージョンスナップショットをサポート）。
      - OSイメージ（マルチリージョンのパブリックイメージおよび非パブリックイメージをサポート）。 単一テナンシー機能を使用する場合は、ノードグループプロパティが正しく構成されているイメージを必ず選択してください。(#enable-zone-selection)を参照してください。

   b. マシンプロファイルからマシンプロパティを継承するには、 を選択し、 タブまたは タブからプロファイルを選択します。

      > **注:**
      >
      > - 現在、このカタログ内のVMは、選択したマシンプロファイルからストレージ、マシンの種類、およびディスク暗号化の設定を継承します。
      > - インスタンステンプレートをマシンプロファイルとして選択した場合、すべてのゾーンがデフォルトで選択されます。必要に応じてゾーンを選択できます。

   c. カタログの最小機能レベルを選択します。

6. ページで、このマシンカタログのオペレーティングシステムを格納するために使用するストレージの種類を選択します。以下の各ストレージオプションには、独自の価格とパフォーマンス特性があります。（IDディスクは常にゾーン標準永続ディスクを使用して作成されます。）

   - 標準永続ディスク
   - バランス永続ディスク
   - SSD永続ディスク

   Google Cloud のストレージオプションの詳細については、`<https://cloud.google.com/compute/docs/disks/>` を参照してください。

7. ページで、作成するVMの数を指定し、VMの詳細な仕様を表示してから、 を選択します。マシンカタログに単一テナントノードグループを使用する場合は、予約済みの単一テナントノードが利用可能なゾーン**のみ**を選択してください。ゾーン選択を有効にするを参照してください。
8. **ディスク設定**ページで、次の設定を構成できます。

   - ライトバックキャッシュを有効にするかどうかを選択します。ライトバックキャッシュを有効にすると、次のことができます。

     - 一時データをキャッシュするために使用するディスクとRAMのサイズを構成します。詳細については、「一時データのキャッシュの構成」を参照してください。
     - ライトバックキャッシュディスクのストレージタイプを選択します。ライトバックキャッシュディスクには、次のストレージオプションを使用できます。

       - 標準永続ディスク
       - バランス永続ディスク
       - SSD永続ディスク

       Google Cloudのストレージオプションの詳細については、「ストレージオプション」を参照してください。
     - ライトバックキャッシュディスクの種類を選択します。

       - **非永続ライトバックキャッシュディスクを使用する**。選択した場合、ライトバックキャッシュディスクはプロビジョニングされたVMに永続しません。ディスクは電源サイクル中に削除され、ディスクにリダイレクトされたデータはすべて失われます。
       - **永続ライトバックキャッシュディスクを使用する**。選択した場合、ライトバックキャッシュディスクはプロビジョニングされたVMに永続します。このオプションを有効にすると、ストレージコストが増加します。

   - MCSストレージ最適化（MCS I/O）が有効になっている場合、次のいずれかを実行できます。

     - 電源サイクル中にVDAのシステムディスクを保持するかどうかを選択します。詳細については、「MCSストレージ最適化の更新を有効にする」を参照してください。
     - メモリとディスクキャッシュのサイズを更新します。

   - ディスクの内容を保護するために独自のキーを使用するかどうかを選択します。この機能を使用するには、まず独自の顧客管理暗号化キー（CMEK）を作成する必要があります。詳細については、「顧客管理暗号化キー（CMEK）を使用する」を参照してください。

> **注:**
>
> Studioインターフェイスでのみ利用可能です。
>
> キーを作成した後、リストからいずれかのキーを選択できます。カタログを作成した後は、キーを変更できません。Google Cloudは、既存の永続ディスクまたはイメージでのキーのローテーションをサポートしていません。したがって、カタログをプロビジョニングした後、カタログは特定のバージョンのキーに紐付けられます。そのキーが無効化または破棄された場合、そのキーで暗号化されたインスタンスとディスクは、キーが再度有効化または復元されるまで使用できなくなります。

9. ページで、Active Directory アカウントを選択し、 を選択します。
   - **新しいActive Directoryアカウントを作成**を選択した場合は、ドメインを選択し、Active Directoryで作成されるプロビジョニングされたVMコンピューターアカウントの命名スキームを表す文字のシーケンスを入力します。アカウントの命名スキームは1〜64文字で、空白スペース、非ASCII文字、または特殊文字を含めることはできません。
   - **既存のActive Directoryアカウントを使用**を選択した場合は、**参照**を選択して、選択したマシン用の既存のActive Directoryコンピューターアカウントに移動します。
10. **ドメイン資格情報**ページで、**資格情報を入力**を選択し、ユーザー名とパスワードを入力して、**保存**を選択し、**次へ**を選択します。
    - 入力する資格情報には、Active Directoryアカウント操作を実行する権限が必要です。
11. **概要**ページで、情報を確認し、カタログの名前を指定して、**完了**を選択します。

> **注:**
>
> バージョン2402以降、GCPカタログ名は以下の規則に準拠する必要があります。
>
> - 小文字で始まること。
> - 小文字 (a-z)、数字、ハイフンのみを含めること。
> - 小文字または数字で終わること。 これらの規則に準拠していない既存のGCPカタログの名前を変更しようとすると、エラーメッセージが表示され、更新された規則に従って名前を変更するように案内されます。

マシンカタログの作成には時間がかかる場合があります。マシンがターゲットノードグループに作成されていることを確認するには、Google Cloudコンソールに移動します。

手動で作成されたGoogle Cloudマシンをインポートする

*Google Cloudへの接続を作成*し、*Google Cloudマシンを含むカタログを作成*できます。その後、Citrix Virtual Apps and Desktops™を介してGoogle Cloudマシンを手動で電源サイクルできます。この機能により、次のことが可能になります。

- 手動で作成したGoogle CloudマルチセッションOSマシンをCitrix Virtual Apps and Desktopsマシンカタログにインポートします。
- 手動で作成したGoogle CloudマルチセッションOSマシンをCitrix Virtual Apps and Desktopsカタログから削除します。
- 既存のCitrix Virtual Apps and Desktopsの電源管理機能を使用して、Google Cloud WindowsマルチセッションOSマシンの電源を管理します。たとえば、それらのマシンの再起動スケジュールを設定します。

この機能は、既存のCitrix Virtual Apps and Desktopsプロビジョニングワークフローの変更や、既存の機能の削除を必要としません。手動で作成したGoogle Cloudマシンをインポートする代わりに、Web StudioでMCSを使用してマシンをプロビジョニングすることをお勧めします。

共有仮想プライベートクラウド

共有仮想プライベートクラウド（VPC）は、共有サブネットが利用可能になるホストプロジェクトと、そのリソースを使用する1つ以上のサービスプロジェクトで構成されます。共有VPCは、共有企業Googleクラウド資産の一元的な制御、使用、管理を提供するため、大規模なインストールに適したオプションです。詳細については、Googleドキュメントサイトを参照してください。

この機能により、Machine Creation Services（MCS）は、共有VPCに展開されたマシンカタログのプロビジョニングと管理をサポートします。このサポートは、現在ローカルVPCで提供されているサポートと機能的に同等ですが、2つの点で異なります。

1. ホスト接続の作成に使用されるサービスアカウントに追加の権限を付与する必要があります。このプロセスにより、MCSは共有VPCリソースにアクセスして使用できるようになります。
2. イングレスとエグレス用にそれぞれ1つずつ、2つのファイアウォールルールを作成する必要があります。これらのファイアウォールルールは、イメージマスタリングプロセス中に使用されます。

必要な新しい権限

ホスト接続を作成する際には、特定の権限を持つGoogle Cloudサービスアカウントが必要です。これらの追加権限は、共有VPCベースのホスト接続の作成に使用されるすべてのサービスアカウントに付与する必要があります。

> **ヒント:**

> これらの追加の権限は、Citrix Virtual Apps and Desktopsにとって新しいものではありません。これらはローカルVPCの実装を容易にするために使用されます。共有VPCでは、これらの追加の権限により、他の共有VPCリソースへのアクセスが可能になります。

> Shared VPCをサポートするために、ホスト接続に関連付けられたサービスアカウントに最大4つの追加権限を付与する必要があります。

1. **compute.firewalls.list** - この権限は必須です。MCSがShared VPCに存在するファイアウォールルールのリストを取得できるようにします。
2. **compute.networks.list** - この権限は必須です。MCSがサービスアカウントで利用可能なShared VPCネットワークを識別できるようにします。
3. **compute.subnetworks.list** – この権限は、VPCの使用方法によってオプションです。MCSが可視Shared VPC内のサブネットを識別できるようにします。この権限はローカルVPCを使用する際にはすでに必要ですが、Shared VPCホストプロジェクトでも割り当てる必要があります。
4. **compute.subnetworks.use** - この権限は、VPCの使用方法によってオプションです。プロビジョニングされたマシンカタログでサブネットリソースを使用するために必要です。この権限はローカルVPCを使用する際にはすでに必要ですが、Shared VPCホストプロジェクトでも割り当てる必要があります。

これらの権限を使用する際には、マシンカタログの作成に使用される権限の種類に基づいて異なるアプローチがあることを考慮してください。

- プロジェクトレベルの権限:
  - ホストプロジェクト内のすべてのShared VPCへのアクセスを許可します。
  - 権限 #3 と #4 をサービスアカウントに割り当てる必要があります。
- サブネットレベルの権限:
  - Shared VPC内の特定のサブネットへのアクセスを許可します。

- 権限 #3 と #4 はサブネットレベルの割り当てに固有のものであるため、サービスアカウントに直接割り当てる必要はありません。

組織のニーズとセキュリティ基準に合ったアプローチを選択してください。

> **ヒント:**
>
> プロジェクトレベルとサブネットレベルの権限の違いの詳細については、Google Cloud のドキュメントを参照してください。

ファイアウォールルール

マシンカタログの準備中に、カタログのマスターイメージシステムディスクとして機能するマシンイメージが準備されます。このプロセスが発生すると、ディスクは一時的に仮想マシンに接続されます。このVMは、すべてのインバウンドおよびアウトバウンドネットワークトラフィックを防止する分離された環境で実行する必要があります。これは、イングレス用とエグレス用の2つのすべて拒否ファイアウォールルールによって実現されます。Google CloudローカルVPCを使用する場合、MCSはこのファイアウォールをローカルネットワークに作成し、マスタリング用のマシンに適用します。マスタリングが完了すると、ファイアウォールルールはイメージから削除されます。

共有VPCを使用するために必要な新しい権限の数を最小限に抑えることをお勧めします。共有VPCはより上位の企業リソースであり、通常、より厳格なセキュリティプロトコルが導入されています。このため、ホストプロジェクトの共有VPCリソースに、イングレス用とエグレス用の2つのファイアウォールルールを作成してください。それらに最高の優先順位を割り当てます。次の値を使用して、これらの各ルールに新しいターゲットタグを適用します。

`citrix-provisioning-quarantine-firewall`

MCSがマシンカタログを作成または更新するとき、このターゲットタグを含むファイアウォールルールを検索します。次に、ルールの正確性を確認し、カタログのマスターイメージを準備するために使用されるマシンに適用します。ファイアウォールルールが見つからない場合、またはルールは見つかったものの、ルールやその優先順位が正しくない場合は、次のようなメッセージが表示されます。

`"Unable to find valid INGRESS and EGRESS quarantine firewall rules for VPC <name> in project <project>. " Please ensure you have created 'deny all' firewall rules with the network tag 'citrix-provisioning-quarantine-firewall' and proper priority." "Refer to Citrix Documentation for details."`

共有 VPC の構成

Web Studio で共有 VPC をホスト接続として追加する前に、プロビジョニングする予定のプロジェクトからサービスアカウントを追加するために、次の手順を完了してください。

1. IAM ロールを作成します。
2. CVAD ホスト接続の作成に使用するサービスアカウントを、共有 VPC ホストプロジェクトの IAM ロールに追加します。
3. プロビジョニングする予定のプロジェクトから Cloud Build サービスアカウントを、共有 VPC ホストプロジェクトの IAM ロールに追加します。
4. ファイアウォールルールを作成します。

IAMロールを作成する

ロールのアクセスレベルを決定します — *プロジェクトレベルアクセス*、またはより制限されたモデルである *サブネットレベルアクセス* を使用します。

IAMロールのプロジェクトレベルアクセス。プロジェクトレベルのIAMロールには、次の権限を含めます。

- compute.firewalls.list
- compute.networks.list
- compute.subnetworks.list
- compute.subnetworks.use

プロジェクトレベルのIAMロールを作成するには：

1. Google Cloudコンソールで、**IAMと管理 > ロール**に移動します。
2. 「**ロール**」ページで、「**ロールを作成**」を選択します。
3. 「**ロールを作成**」ページで、ロール名を指定します。「**権限を追加**」を選択します。
    a. **権限の追加**ページで、ロールに権限を個別に追加します。権限を追加するには、**テーブルをフィルタリング**フィールドに権限の名前を入力します。権限を選択し、**追加**を選択します。
    b. 「**作成**」を選択します。

サブネットレベルのIAMロール。このロールは、**ロールを作成**を選択した後に、権限`compute.subnetworks.list`と`compute.subnetworks.use`の追加を省略します。このIAMアクセスレベルの場合、権限`compute.firewalls.list`と`compute.networks.list`を新しいロールに適用する必要があります。

サブネットレベルのIAMロールを作成するには：

1. Google Cloudコンソールで、**VPCネットワーク** > **共有VPC**に移動します。**共有VPC**ページが表示され、ホストプロジェクトに含まれる共有VPCネットワークのサブネットが表示されます。
2. 「**共有VPC**」ページで、アクセスするサブネットを選択します。
3. 右上隅で「**メンバーを追加**」を選択して、サービスアカウントを追加します。
4. 「**メンバーを追加**」ページで、次の手順を実行します。
    a. 「**新しいメンバー**」フィールドにサービスアカウントの名前を入力し、メニューからサービスアカウントを選択します。
    b. 「**ロールを選択**」フィールドを選択し、次に「**Compute Network User**」を選択します。
    c. 「**保存**」を選択します。
5. Google Cloud コンソールで、「**IAM と管理**」>「**ロール**」に移動します。
6. 「**ロール**」ページで、「**ロールを作成**」を選択します。
7. 「**ロールを作成**」ページで、ロール名を指定します。「**権限を追加**」を選択します。
    a. 「**権限を追加**」ページで、ロールに個別に権限を追加します。権限を追加するには、「**テーブルをフィルタ**」フィールドに権限の名前を入力します。権限を選択し、「**追加**」を選択します。
    b. 「**作成**」を選択します。

ホストプロジェクトのIAMロールにサービスアカウントを追加する

IAMロールを作成したら、ホストプロジェクトのサービスアカウントを追加するために次の手順を実行します。

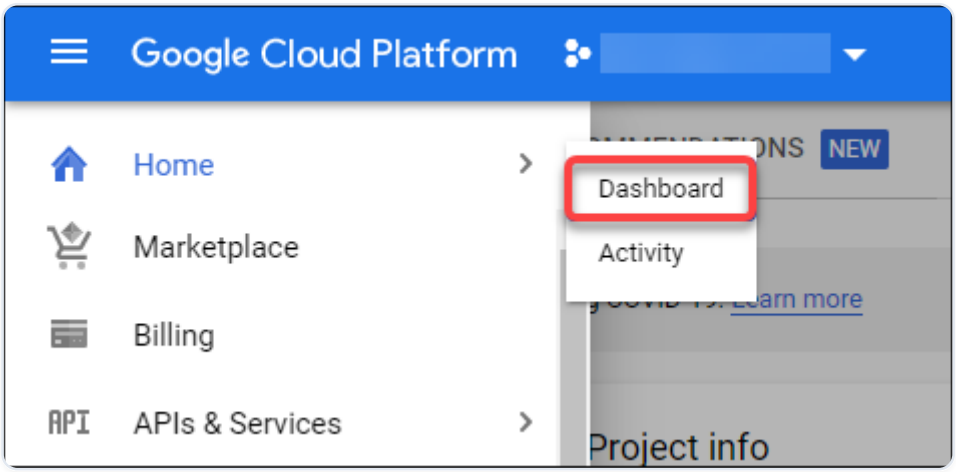
1. Google Cloud コンソールで、ホストプロジェクトに移動し、次に「**IAM と管理 > IAM**」に移動します。
2. 「**IAM**」ページで、「**追加**」を選択してサービスアカウントを追加します。
3. 「**メンバーを追加**」ページで、:
    a. 「**新しいメンバー**」フィールドにサービスアカウントの名前を入力し、メニューからサービスアカウントを選択します。
    b. ロールフィールドを選択し、作成したIAMロールを入力して、メニューからそのロールを選択します。
    c. 「**保存**」を選択します。

これで、サービスアカウントがホストプロジェクト用に構成されました。

クラウドビルドサービスアカウントを共有VPCに追加する

すべてのGoogle Cloudサブスクリプションには、プロジェクトID番号の後に `cloudbuild.gserviceaccount` が続くサービスアカウントがあります。例: `705794712345@cloudbuild.gserviceaccount`。

Google Cloud コンソールで **Home** と **Dashboard** を選択すると、プロジェクトのプロジェクト ID 番号を確認できます。



画面の **Project Info** エリアの下にある **Project Number** を見つけます。

Cloud Buildサービスアカウントを共有VPCに追加するには、次の手順を実行します。

1. Google Cloudコンソールで、ホストプロジェクトに移動し、**IAMと管理** > **IAM**に移動します。
2. 「**権限**」ページで、「**追加**」を選択してアカウントを追加します。
3. 「**メンバーを追加**」ページで、次の手順を実行します。
    a. 「**新しいメンバー**」フィールドにCloud Buildサービスアカウントの名前を入力し、メニューからサービスアカウントを選択します。
    b. 「**ロールを選択**」フィールドを選択し、`Computer Network User` と入力して、メニューからロールを選択します。
    c. 「**保存**」を選択します。

ファイアウォールルールを作成する

マスタリングプロセスの一環として、MCS は選択されたマシンイメージをコピーし、それを使用してカタログ用のマスターイメージシステムディスクを準備します。マスタリング中、MCS はディスクを一時的な仮想マシンに接続し、その仮想マシンが準備スクリプトを実行します。この VM は、すべてのインバウンドおよびアウトバウンドネットワークトラフィックを禁止する分離された環境で実行する必要があります。分離された環境を作成するために、MCS は2つの *すべて拒*

否 ファイアウォールルール（イングレスルールとエグレスルール）を必要とします。したがって、*ホストプロジェクト* に次の2つのファイアウォールルールを作成します。

1. Google Cloud コンソールで、ホストプロジェクトに移動し、次に **VPC ネットワーク > ファイアウォール** に移動します。
2. 「**ファイアウォール**」ページで、「**ファイアウォールルールを作成**」を選択します。
3. 「**ファイアウォールルールを作成**」ページで、以下を完了します。
   - **名前**。ルールの名前を入力します。
   - **ネットワーク**。イングレスファイアウォールルールが適用される共有 VPC ネットワークを選択します。
   - **優先度**。値が小さいほど、ルールの優先度が高くなります。小さい値（例: 10）をお勧めします。
   - **トラフィックの方向**。**イングレス** を選択します。
   - **一致時のアクション**。**拒否** を選択します。
   - **ターゲット**。デフォルトの **指定されたターゲットタグ** を使用します。
   - **ターゲットタグ**。`citrix-provisioning-quarantine-firewall` と入力します。
   - **ソースフィルター**。デフォルトの **IP 範囲** を使用します。
   - **ソース IP 範囲**。すべてのトラフィックに一致する範囲を入力します。`0.0.0.0/0` と入力します。
   - **プロトコルとポート**。「**すべて拒否**」を選択します。
4. 「**作成**」を選択してルールを作成します。
5. 手順 1〜4 を繰り返して別のルールを作成します。**Direction of traffic** には **Egress** を選択します。

接続の追加

Google Cloud 環境への接続を追加します。接続の追加を参照してください。

ゾーン選択を有効にする

Citrix Virtual Apps and Desktops はゾーン選択をサポートしています。ゾーン選択を使用すると、VM を作成するゾーンを指定できます。ゾーン選択を使用すると、管理者は選択したゾーンに単一テナントノードを配置できます。単一テナンシーを構成するには、Google Cloud で以下を完了する必要があります。

- Google Cloud の単一テナントノードを予約する

- VDA マスターイメージを作成する

Google Cloud の単一テナントノードを予約する

単一テナントノードを予約するには、Google Cloud のドキュメントを参照してください。

> **重要:**
>
> ノードテンプレートは、ノードグループに予約されているシステムのパフォーマンス特性を示すために使用されます。これらの特性には、vGPU の数、ノードに割り当てられるメモリ量、およびノード上に作成されるマシンに使用されるマシンタイプが含まれます。詳細については、Google Cloud のドキュメントを参照してください。

VDA マスターイメージの作成

単一テナントノードにマシンを正常に展開するには、マスター VM イメージを作成する際に追加の手順を実行する必要があります。Google Cloud のマシンインスタンスには、*ノードアフィニティラベル*と呼ばれるプロパティがあります。単一テナントノードに展開されるカタログのマスターイメージとして使用されるインスタンスには、**ターゲットノードグループ**の名前と一致する*ノードアフィニティラベル*が必要です。これを実現するには、次の点に留意してください。

- 新しいインスタンスの場合は、インスタンスの作成時に Google Cloud コンソールでラベルを設定します。詳細については、単一テナント VM のプロビジョニングを参照してください。
- 既存のインスタンスの場合は、**gcloud** コマンドラインを使用してラベルを設定します。詳細については、ノードアフィニティラベルの構成を参照してください。

> **注:**
>
> 共有 VPC で単一テナンシーを使用する場合は、共有仮想プライベートクラウドを参照してください。

マシンカタログを作成する

ノードアフィニティラベルを設定したら、マシンカタログを構成します。

顧客管理の暗号化キー (CMEK)

MCS カタログに顧客管理の暗号化キー (CMEK) を使用できます。この機能を使用する場合、Google Cloud Key Management Service `CryptoKey Encrypter/Decrypter` ロールを Compute Engine サービスエージェントに割り当てます。Citrix Virtual Apps and Desktops アカウントは、

キーが保存されているプロジェクトで適切な権限を持っている必要があります。詳細については、「Cloud KMS キーを使用してリソースを保護する」を参照してください。

Compute Engine サービスエージェントは次の形式です: `service-<Project_Number>@compute-system.iam.gserviceaccount.com`。この形式は、デフォルトの Compute Engine サービスアカウントとは異なります。

> **注:**
>
> この Compute Engine サービスアカウントは、Google Console の「**IAM 権限**」表示に表示されない場合があります。そのような場合は、Cloud KMS キーを使用してリソースを保護する で説明されているように、`gcloud` コマンドを使用してください。

Citrix Virtual Apps and Desktops アカウントに権限を割り当てる

Google Cloud KMS の権限はさまざまな方法で構成できます。*プロジェクトレベル*の KMS 権限または*リソースレベル*の KMS 権限のいずれかを付与できます。詳細については、権限とロール を参照してください。

プロジェクトレベルの権限

1つのオプションは、Citrix Virtual Apps and Desktops アカウントに Cloud KMS リソースを参照するためのプロジェクトレベルの権限を付与することです。これを行うには、カスタムロールを作成し、次の権限を追加します。

- `cloudkms.keyRings.list`
- `cloudkms.keyRings.get`
- `cloudkms.cryptokeys.list`
- `cloudkms.cryptokeys.get`

このカスタムロールを Citrix Virtual Apps and Desktops に割り当てます。これにより、インベントリ内の関連プロジェクトでリージョンキーを参照できます。

リソースレベルの権限

もう1つのオプションであるリソースレベルの権限の場合、Google Cloud コンソールで、MCS プロビジョニングに使用する `cryptoKey` を参照します。Citrix Virtual Apps and Desktops アカウントを、カタログプロビジョニングに使用するキーリングまたはキーに追加します。

> **ヒント:**

> このオプションでは、Citrix Virtual Apps and Desktops アカウントが Cloud KMS リソースに対するプロジェクトレベルのリスト権限を持っていないため、インベントリでプロジェクトのリージョンキーを参照できません。ただし、以下で説明するように、`ProvScheme` カスタムプロパティで正しい `cryptoKeyId` を指定することで、CMEK を使用してカタログをプロビジョニングすることは可能です。

カスタムプロパティを使用した CMEK でのプロビジョニング

PowerShellでプロビジョニングスキームを作成する際に、`ProvScheme CustomProperties` で `CryptoKeyId` プロパティを指定します。例:

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="CryptoKeyId"
Value="<yourCryptoKeyId>" />

</CustomProperties>'
```

`cryptoKeyId` は次の形式で指定する必要があります。

`projectId:location:keyRingName:cryptoKeyName`

たとえば、IDが `my-example-project-1` のプロジェクトで、`us-east1` リージョンのキーリング `my-example-key-ring` にあるキー `my-example-key` を使用したい場合、`ProvScheme` カスタム設定は次のようになります。

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-
example-project-1:us-east1:my-example-key-ring:my-example-key" />

</CustomProperties>'
```

このプロビジョニングスキームに関連するすべてのMCSプロビジョニング済みディスクとイメージは、この顧客管理暗号化キーを使用します。

> **ヒント:**

> グローバルキーを使用する場合、顧客プロパティの場所は**リージョン**名ではなく`global`と記述する必要があります。上記の例では**us-east1**です。例: `<Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-example-project-1:global:my-example-key-ring:my-example-key" />`。

顧客管理キーのローテーション

Google Cloudは、既存の永続ディスクまたはイメージでのキーのローテーションをサポートしていません。マシンがプロビジョニングされると、作成時に使用されていたキーのバージョンに紐付けられます。ただし、新しいバージョンのキーを作成でき、その新しいキーは、新しくプロビジョニングされたマシンや、新しいマスターイメージでカタログが更新されたときに作成されるリソースに使用されます。

キーリングに関する重要な考慮事項

キーリングの名前変更や削除はできません。また、キーリングを構成する際に予期せぬ料金が発生する可能性があります。キーリングを削除または削除すると、Google Cloudはエラーメッセージを表示します。

```
Sorry, you can't delete or rename keys or key rings. We were concerned
about the security implications of allowing multiple keys or key versions
over time to have the same resource name, so we decided to make names
immutable. (And you can't delete them, because we wouldn't be able to do a
true deletion--there would still have to be a tombstone tracking that this
name had been used and couldn't be reused).

We're aware that this can make things untidy, but we have no immediate
plans to change this.

If you want to avoid getting billed for a key or otherwise make it
unavailable, you can do so by deleting all the key versions; neither keys
nor key rings are billed for, just the active key versions within the
keys.
```

> **ヒント:**

> 詳細については、「コンソールからキーリングを編集または削除する」を参照してください。

均一なバケットレベルのアクセス互換性

Citrix Virtual Apps and Desktops は、Google Cloud の統一されたバケットレベルのアクセス制御ポリシーと互換性があります。この機能は、ストレージバケットを含むリソースの操作を許可するために、サービスアカウントに権限を付与する IAM ポリシーの使用を強化します。統一されたバケットレベルのアクセス制御により、Citrix Virtual Apps and Desktops は、アクセス制御リスト (ACL) を使用して、ストレージバケットまたはそこに保存されているオブジェクトへのアクセスを制御できます。Google Cloud の統一されたバケットレベルのアクセスに関する概要情報については、「統一されたバケットレベルのアクセス」を参照してください。構成情報については、「統一されたバケットレベルのアクセスを要求する」を参照してください。

PowerShell を使用してマシンカタログを作成する

このセクションでは、PowerShell を使用してカタログを作成する方法について詳しく説明します。

- 永続的なライトバックキャッシュディスクを持つカタログを作成する
- MCSIO で起動パフォーマンスを向上させる
- マシンプロファイルを使用してマシンカタログを作成する
- インスタンステンプレートとしてマシンプロファイルを持つマシンカタログを作成する
- PowerShell を使用してシールドされた VM でカタログを作成する
- 単一テナントノードに Windows 11 VM を作成する

永続的なライトバックキャッシュディスクを持つカタログを作成する

永続的なライトバックキャッシュディスクを持つカタログを構成するには、PowerShell パラメーター `New-ProvScheme` `CustomProperties` を使用します。

> **ヒント:**
>
> ここで PowerShell パラメーターを使用するのは、クラウドベースのホスティング接続の場合のみです。オンプレミスソリューション（XenServer® など）で永続的なライトバックキャッシュディスクを使用してマシンをプロビジョニングする場合、ディスクは自動的に永続化されるため、PowerShell は必要ありません。

> このパラメーターは、MCSプロビジョニングされたマシンに対してライトバックキャッシュディスクがどのように永続化されるかを決定するために使用される追加のプロパティ `PersistWBC` をサポートします。`PersistWBC` プロパティは、`UseWriteBackCache` パ

ラメーターが指定され、かつ `WriteBackCacheDiskSize` パラメーターがディスクが作成されることを示すように設定されている場合にのみ使用されます。

注:

この動作は、AzureとGCPの両方に適用され、電源サイクル時にデフォルトのMCSIOライトバックキャッシュディスクが削除され、再作成されます。ディスクの削除と再作成を避けるために、ディスクを永続化することを選択できます。

`PersistWBC` プロパティを `true` に設定すると、Citrix Virtual Apps and Desktops 管理者が管理インターフェイスからマシンをシャットダウンしても、ライトバックキャッシュディスクは削除されません。

`PersistWBC` プロパティを `false` に設定すると、Citrix Virtual Apps and Desktops 管理者が管理インターフェイスからマシンをシャットダウンしたときに、ライトバックキャッシュディスクが削除されます。

注:

`PersistWBC` プロパティが省略された場合、プロパティはデフォルトで `false` になり、管理インターフェイスからマシンがシャットダウンされるとライトバックキャッシュは削除されます。

たとえば、CustomProperties パラメーターを使用して `PersistWBC` を `true` に設定する場合：

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />
```

```
<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />

</CustomProperties>
```

注:

`PersistWBC`プロパティは、`New-ProvScheme` PowerShellコマンドレットを使用してのみ設定できます。作成後にプロビジョニングスキームの`CustomProperties`を変更しようとしても、マシンカタログや、マシンがシャットダウンされたときのライトバックキャッシュディスクの永続性には影響しません。

たとえば、`New-ProvScheme`を設定してライトバックキャッシュを使用し、同時に`PersistWBC`プロパティを`true`に設定します。

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistWBC`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}
```

```
-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

MCSIOで起動パフォーマンスを向上させる

MCSIOが有効な場合、AzureおよびGCPマネージドディスクの起動パフォーマンスを向上させることができます。この機能を構成するには、`New-ProvScheme`コマンドでPowerShell `PersistOSDisk`カスタムプロパティを使用します。`New-ProvScheme`に関連するオプションは次のとおりです。

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="Resource ``````<!--NeedCopy-->

````````Groups" Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

</CustomProperties>
```

この機能を有効にするには、`PersistOSDisk`カスタムプロパティを`true`に設定します。例：

```
New-ProvScheme

-CleanOnBoot
```
```

```
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

マシンプロファイルを使用してマシンカタログを作成する

Machine Creation Services (MCS) を使用してマシンをプロビジョニングするためのカタログを作成する場合、仮想マシンからハードウェアプロパティをキャプチャし、カタログ内の新しくプロビジョニングされたVMに適用するために、マシンプロファイルを使用できます。

`MachineProfile` パラメーターが使用されていない場合、ハードウェアプロパティはマスターイメージVMまたはスナップショットからキャプチャされます。 明示的に定義する一部のプロパティ

（例: `StorageType`、`CatalogZones`、`CryptoKeyIs`）は、マシンプロファイルから無視されます。

- マシンプロファイルを使用してカタログを作成するには、`New-ProvScheme`コマンドを使用します。例: `New-ProvScheme –MachineProfile "path to VM"`。`MachineProfile`パラメーターを指定しない場合、ハードウェアプロパティはマスターイメージVMからキャプチャされます。
- 新しいマシンプロファイルでカタログを更新するには、`Set-ProvScheme`コマンドを使用します。例: `Set-ProvScheme –MachineProfile "path to new VM"`。このコマンドは、カタログ内の既存のVMのマシンプロファイルを変更しません。カタログに追加された新しく作成されたVMのみが新しいマシンプロファイルを持ちます。
- マスターイメージを更新することもできますが、マスターイメージを更新してもハードウェアプロパティは更新されません。ハードウェアプロパティを更新する場合は、`Set-ProvScheme`コマンドを使用してマシンプロファイルを更新する必要があります。これらの変更は、カタログ内の新しいマシンにのみ適用されます。既存のマシンのハードウェアプロパティを更新するには、`Set-ProvVMUpdateTimeWindow`コマンドを`-StartsNow`および`-DurationInMinutes -1`パラメーターとともに使用できます。

> **注:**
>
> - `StartsNow`は、スケジュールされた開始時刻が現在の時刻であることを示します。
> - 負の数（例: –1）を指定した`DurationInMinutes`は、スケジュールの時間枠に上限がないことを示します。

マシンプロファイルをインスタンステンプレートとして使用してマシンカタログを作成する

マシンプロファイルの入力としてGCPインスタンステンプレートを選択できます。インスタンステンプレートはGCPの軽量リソースであるため、非常に費用対効果が高いです。

マシンプロファイルをインスタンステンプレートとして使用して新しいマシンカタログを作成する

1. PowerShellウィンドウを開きます。
2. `asnp citrix*`を実行して、Citrix固有のPowerShellモジュールをロードします。
3. 次のコマンドを使用して、GCPプロジェクトでインスタンステンプレートを見つけます。

```
cd XDHyp:\HostingUnits\<HostingUnitName>\instanceTemplates.folder
```

4. NewProvSchemeコマンドを使用して、マシンプロファイルをインスタンステンプレートとして新しいマシンカタログを作成します。

```
New-ProvScheme -ProvisioningSchemeName <CatalogName>  -HostingUnitName
<HostingUnitName> -IdentityPoolName <identity pool name> -MasterImageVM

XDHyp:\HostingUnits\<HostingUnitName> \Base.vm\Base.snapshot
-MachineProfile XDHyp:
\HostingUnits\<HostingUnitName>\instanceTemplates.folder\mytemplate.tem
plate
```

   New-ProvSchemeコマンドの詳細については、https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/New-ProvScheme/を参照してください。

5. PowerShell コマンドを使用してマシンカタログの作成を完了します。Remote PowerShell SDK を使用してカタログを作成する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/ を参照してください。

既存のマシンカタログのマシンプロファイルをインスタンステンプレートに変更する

既存のマシンカタログのマシンプロファイルをインスタンステンプレートに変更する詳細な手順は次のとおりです。

1. PowerShell ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. 次のコマンドを実行します。

```
Set-ProvScheme -ProvisioningSchemeName  <CatalogName> -MachineProfile
XDHyp:
\HostingUnits\<HostingUnitName>\instanceTemplates.folder\<TemplateName>
.template
```

   Set-ProvSchemeコマンドの詳細については、https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/Set-ProvScheme/を参照してください。

PowerShell を使用して、シールドされたVMでカタログを作成する

シールドされたVMプロパティを持つMCSマシンカタログを作成できます。シールドされた仮想マシンは、セキュアブート、仮想トラステッドプラットフォームモジュール、UEFIファームウェア、整合性監視などの高度なプラットフォームセキュリティ機能を使用して、Compute Engineインスタンスの検証可能な整合性を提供する一連のセキュリティ制御によって強化されています。

MCSは、マシンプロファイルワークフローを使用してカタログを作成することをサポートしています。マシンプロファイルワークフローを使用する場合、VMインスタンスのシールドされたVMプロパティを有効にする必要があります。その後、このVMインスタンスをマシンプロファイルの入力として使用できます。

マシンプロファイルワークフローを使用して、シールドされたVMでMCSマシンカタログを作成するには。

1. Google Cloud コンソールでVMインスタンスのシールドされたVMオプションを有効にします。クイックスタート: シールドされたVMオプションを有効にするを参照してください。
2. VMインスタンスを使用して、マシンプロファイルワークフローでMCSマシンカタログを作成します。
    a. PowerShell ウィンドウを開きます。
    b. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
    c. まだ作成されていない場合は、IDプールを作成します。
    d. `New-ProvScheme`コマンドを実行します。例：

    ```
    New-ProvScheme -ProvisioningSchemeName <catalog-name>

    -HostingUnitName gcp-hostint-unit

    -MasterImageVM XDHyp:\HostingUnits\gcp-hostint-unit\catalog-vda.vm

    -MachineProfile XDHyp:\HostingUnits\gcp-hostint-unit\catalog-
    machine.vm
    ```

3. マシンカタログの作成を完了します。

新しいマシンプロファイルでマシンカタログを更新するには:

1. `Set-ProvScheme`コマンドを実行します。例：

```
Set-ProvScheme -ProvisioningSchemeName <catalog-name>

-MasterImageVM XDHyp:\HostingUnits\<hostin-unit>\catalog-vda.vm

-MachineProfile "DHyp:\HostingUnits\<hostin-unit>\catalog-machine.vm
```

`Set-ProvScheme` で行った変更を既存のVMに適用するには、`Set-ProvVMUpdateTimeWindow` コマンドを実行します。

1. `Set-ProvVMUpdateTimeWindow` コマンドを実行します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
<List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

2. VMを再起動します。

単一テナントノード上にWindows 11 VMを作成する

GCPでWindows 11 VMを作成できます。ただし、マスターイメージにWindows 11をインストールする場合は、マスターイメージ作成プロセス中にvTPMを有効にする必要があります。また、マシンプロファイルソース（VMまたはインスタンステンプレート）でvTPMを有効にする必要があります。

単一テナントノード上にWindows 11 VMを作成するための主な手順は次のとおりです。

1. Google Cloud仮想化環境をセットアップします。詳細については、「Google Cloud環境」を参照してください。
2. VDAをインストールします。「VDAのインストール」を参照してください。
3. Google Cloud環境への接続を作成します。詳細については、「Google Cloud環境への接続」を参照してください。
4. Windows 11 Bring Your Own License (BYOL) マスターイメージを作成し、そのイメージをGoogle Cloudにインポートします。「Windows 11 BYOLマスターイメージの作成」を参照してください。
5. マシンプロファイルソースを作成します: 単一テナントノード上にVMをプロビジョニングし、ソースマシンプロファイルのvTPMを有効にします。「単一テナントノード上でのVMのプロビジョニング」を参照してください。
6. vTPMが有効なWindows 11マシンプロファイルソースを使用してMCSマシンカタログを作成します。マシンプロファイルソースは、単一テナントノードで説明されているインスタンスタイ

プと同じである必要があります。「Windows 11マシンプロファイルソースを使用したMCSマシンカタログの作成」を参照してください。

Windows 11 BYOLマスターイメージを作成する

Windows 11 BYOLマスターイメージを作成し、そのマスターイメージをGoogle Cloudにインポートするには、2つのオプションがあります。

- Google Cloud Cloud Build Tools を使用する
- 他のハイパーバイザーでマスターイメージを作成する

GOOGLE CLOUD CLOUD BUILD TOOLS を使用する

1. Windows 11 ISO、GCP SDK、.NET Framework、および PowerShell インストーラーファイルを GCP ストレージバケットにアップロードします。
2. クラウドビルド `.yaml` ファイル内のファイルパスをパラメーターとして指定します。
3. コマンドラインから以下の Cloud Build を実行して、最終的な Windows 11 イメージをビルドします。GCP は、GCP の Daisy ワークフローを使用して、選択したプロジェクトでマスターイメージをブートストラップして作成し、マスターイメージは GCP にインポートされます。

```
gcloud compute instances import INSTANCE-NAME--source-uri=gs://BUCKET/
IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE --byol --
machine-type=MACHINE-TYPE --zone=ZONE
```

> **注:**
>
> すべての大文字のテキストを実際の詳細リソースに置き換えます。

詳細については、「カスタム Windows BYOL イメージの作成」を参照してください。

他のハイパーバイザーでマスターイメージを作成する

1. 他のハイパーバイザーを使用して Windows 11 マスターイメージを作成します。
2. マスターイメージを OVF 形式でローカルマシンにエクスポートします。
3. ローカルの gcloud CLI を使用して、OVF ファイルを GCP ストレージバケットにアップロードします。

```
gsutil cp LOCAL_IMAGE_PATH_OVF_FILES gs://BUCKET_NAME/
```

4. コマンドラインから以下の Cloud Build を実行して、最終的な Windows 11 イメージをビルドします。GCP は、GCP の Daisy ワークフローを使用して、選択したプロジェクトでマスターイメージをブートストラップして作成し、マスターイメージは GCP にインポートされます。

```
gcloud compute instances import INSTANCE-NAME --source-uri=gs://BUCKET/
IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE --byol --
machine-type=MACHINE-TYPE --zone=ZONE
```

> **注:**
>
> すべての大文字のテキストを実際のリソースの詳細に置き換えてください。

単一テナントノードでのVMのプロビジョニング

単一テナントノードを使用して、VMを他のプロジェクトのVMから物理的に分離したり、同じホストハードウェア上にVMをグループ化したりできます。単一テナントノードの詳細については、GCPドキュメント「Sole-tenancy overview」を参照してください。

単一テナントノードでのVM（マシンプロファイルソース）のプロビジョニングについては、GCPドキュメント「Provision VMs on sole-tenant nodes」を参照してください。

> **注:**
>
> - ノードグループと同じインスタンスタイプとリージョンを選択します。
> - Shielded VMセクションでvTPMを有効にします。詳細については、「Quickstart: Enable Shielded VM options」を参照してください。
> - ソースVMでBitlockerを無効にします。

Windows 11のマシンプロファイルソースを使用してMCSマシンカタログを作成する

Web StudioまたはPowerShellコマンドを使用して、Windows 11 VMを作成するためのMCSマシンカタログを作成できます。

> **注:**

- マスターイメージには、Windows 11のスナップショットまたはVMを選択します。
- マシンプロファイルソースには、Windows 11 VMをマシンプロファイルとして選択します。マシンプロファイルソースは、単一テナントノードで説明されているものと同じインスタンスタイプである必要があります。

Web Studioの使用方法については、Web Studioを使用してマシンカタログを作成するを参照してください。

PowerShellコマンドについては、マシンプロファイルを使用してマシンカタログを作成するを参照してください。

カタログを作成し、VM の電源をオンにすると、Google Cloud コンソールで単一テナントノード上で実行されている Windows 11 VM を確認できます。

継承されたラベルを持つ VM とディスク

MCS マシンカタログの VM とディスク（ID ディスク、ライトキャッシュバックディスク、OS ディスク）は、マシンプロファイルソース（GCP VM インスタンスまたはインスタンステンプレート）のラベルを継承できます。これらのラベルを使用して、異なるチームが所有するインスタンス（例：team:research や team:analytics）を区別し、さらにコスト計算や予算編成に利用できます。ラベルの詳細については、GCP ドキュメント「Organize resources using labels」を参照してください。

マシンプロファイルソースを使用して、新しいカタログを作成したり、既存のカタログを更新したり、既存の VM を更新してラベルを継承させることができます。

この機能は、永続的および非永続的な MCS マシンカタログに適用されます。

次のことができます。

- 継承されたラベルを持つカタログを作成する
- 継承されたラベルを持つ既存のカタログを更新する
- 継承されたラベルを持つ既存の VM を更新する
- VM およびブートディスクのラベル情報を取得する
- VM を削除する

継承されたラベルを持つカタログを作成する

VM とディスクがマシンプロファイルソースからラベルを継承する MCS マシンカタログを作成するには、次の手順を実行します。

1. ラベルを持つマシンプロファイルソース（VM インスタンスまたはインスタンステンプレート）を作成します。ラベルを持つ VM の作成については、GCP ドキュメント「Create resources with labels」を参照してください。インスタンステンプレートは VM から作成され、VM で定義されたラベルを引き継ぎます。
2. Web StudioまたはPowerShellコマンドを使用してMCSカタログを作成します。
3. Web Studioを使用している場合は、**イメージ**ページで**マシンプロファイルを使用**を選択し、VMまたはテンプレートを選択します。
4. PowerShellコマンドを使用している場合、次の操作を行います。

   a. PowerShellウィンドウを開きます。

   b. asnp citrix* を実行します。

   c. IDプールを作成します。IDプールは、作成されるVMのActive Directory (AD) アカウントのコンテナです。

   d. Active Directoryで必要なADコンピューターアカウントを作成します。

   e. カタログを作成するには、`New-ProvScheme`コマンドを実行します。例:

      マシンプロファイル入力としてテンプレートを使用するNew-ProvScheme (永続カタログ):

      ```
      New-ProvScheme `

      -ProvisioningSchemeName "catalog-name" `

      -HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

      -IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

      -MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

      -MachineProfile "XDHyp:\HostingUnits\hosting-unit-
      name\instanceTemplates.folder\instance-template-name.template" `
      ```

      マシンプロファイル入力としてインスタンステンプレートを使用するNew-ProvScheme (非永続カタログ):

      ```
      New-ProvScheme `

      -ProvisioningSchemeName "catalog-name" `
      ```

```
-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-
name\instanceTemplates.folder\instance-template-name.template" `

-CleanOnBoot
```

マシンプロファイル入力としてVMインスタンスを使用するNew-ProvScheme (永続カタログ):

```
New-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `
```

マシンプロファイル入力としてVMインスタンスを使用するNew-ProvScheme (非永続カタログ):

```
New-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `
```

```
-CleanOnBoot
```

f. プロビジョニングスキームをブローカーカタログとして登録します。

g. カタログにVMを追加します。

継承されたラベルで既存のカタログを更新する

既存のカタログを新しいマシンプロファイルを持つように更新するには、Set-ProvSchemeコマンドを実行します。コマンドを実行すると、カタログに追加されたすべての新しいVMは、新しいマシンプロファイルソースのラベルを持つようになります。非永続カタログは、次回の電源投入時に更新されます。

例:

インスタンステンプレートをマシンプロファイル入力として使用するSet-ProvScheme:

```
Set-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-
name\instanceTemplates.folder\instance-template-name.template" `
```

VMインスタンスをマシンプロファイル入力として使用するSet-ProvScheme:

```
Set-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `
```

継承されたラベルで既存のVMを更新する

更新されたマシンプロファイルソースで既存のVMを更新するには、次のコマンドを実行します。

1. `Set-ProvScheme`
2. `Set-ProvVMUpdateTimeWindow`。例：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
<List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

3. VMを再起動します。

VMおよびブートディスクラベルの情報を取得する

VMを作成した後、`AdditionalData`パラメーターを指定して`Get-Item`コマンドを使用すると、VMおよびブートディスクラベルの情報を取得できます。

VMラベルの情報を取得するには、次のコマンドを実行します。

```
(Get-Item XDHyp:\HostingUnits\hosting-unit-
name\vm_name.vm).AdditionalData.Tags
```

ブートディスクラベルの情報を取得するには、次のコマンドを実行します。

```
(Get-Item XDHyp:\HostingUnits\hosting-unit-name\vm_name.vm\bootdisk-
name.attacheddisk).AdditionalData.Tags
```

注:

さまざまなハイパーバイザー間で一貫性を保つため、GCPラベルを表示するために「タグ」という用語を使用しています。

VMを削除する

カタログからVMを削除するが、GCPからVMを削除しないことを選択できます。この場合、Citrixラベルのみ VMから削除されます。その他の追加されたラベルはすべてVMから削除されません。Web StudioまたはPowerShellコマンドを使用してVMを削除できます。

WEB STUDIOの使用

1. VMを選択して右クリックします。
2. **削除**をクリックします。
3. **仮想マシンをカタログから削除しますが、仮想マシンは削除しません**を選択します。

POWERSHELLコマンドの使用

`ForgetVM`パラメーターを指定して`Remove-ProvVM`を実行します。詳細については、SDKドキュメントのRemove-ProvVMを参照してください。

Google Cloud マーケットプレイス

Citrixが**Google Cloud Marketplace**で提供するイメージを参照して選択し、マシンカタログを作成できます。現在、MCSはこの機能に対してマシンプロファイルワークフローのみをサポートしています。

Google Cloud MarketplaceでCitrix VDA VM製品を検索するには、https://console.cloud.google.com/marketplaceにアクセスしてください。

Google Cloud MarketplaceでカスタムイメージまたはCitrix ready®イメージを使用して、マシンカタログのイメージを更新できます。

> **注:**
>
> マシンプロファイルにストレージタイプ情報が含まれていない場合、値はカスタムプロパティから派生します。

> サポートされているGoogle Cloud Marketplaceイメージは次のとおりです。

- Windows 2019シングルセッション
- Windows 2019 マルチセッション
- ウブントゥ

Citrix対応イメージをマシンカタログ作成のソースとして使用する例:

```
New-ProvScheme -ProvisioningSchemeName GCPCatalog \

-HostingUnitName GcpHu -IdentityPoolName gcpPool -CleanOnBoot \

-MasterImageVM XDHyp:\HostingUnits\GcpHu\images.folder\citrix-daas-
win2019-single-vda-v20220819.publicimage \

-MachineProfile XDHyp:\HostingUnits\GcpHu\Base.vm
```

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループを作成するようにガイドします。
- 構成プロセス全体を確認するには、インストールと構成を参照してください。

- カタログを管理するには、マシンカタログを管理するおよびGoogle Cloud Platformカタログを管理するを参照してください。

詳細情報

- 接続とリソースを作成および管理する
- Google Cloud環境への接続
- マシンカタログを作成する

HPE Moonshot マシンカタログを作成する

(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/machine-catalogs-create.html)は、マシンカタログを作成するウィザードについて説明しています。以下の情報は、HPE Moonshot環境に固有の詳細を扱っています。

> **注:**
>
> - HPE Moonshotへの接続を作成する
> - 1つ以上のHPE Moonshotノードが利用可能であることを確認し、それらのノードにVDAをインストールしてください。
> - 最初のHPE Moonshotカートリッジイメージの作成については、OS Deployment on Moonshot User Guideを参照してください。

HPE Moonshotマシンカタログは、以下を使用して作成できます。

- ウェブスタジオ
- PowerShellコマンド

Web Studioを使用してマシンカタログを作成する

マシンカタログのセットアップウィザードで、:

1. **オペレーティングシステム**ページで、**マルチセッションOS**または**シングルセッションOS**を選択します。
2. **マシン管理**ページで、**電源管理されているマシン**と**別のサービスまたはテクノロジー**を選択します。

3. **仮想マシン**ページで、マシンとそのActive Directoryマシンアカウントを追加します。次のいずれかを実行できます。

   - **マシンの追加**をクリックして、マシンを手動で追加します。**VMの選択**ウィンドウが表示されます。以前に作成したHPE Moonshotシャーシ接続を展開し、追加するノード（VM）を選択します。次に、関連するマシンアカウント名を追加します。
   - 「**CSVファイルの追加**」をクリックして、マシンを一括追加します。CSVファイルを使用してマシンを追加する方法については、「CSVファイルを使用してマシンをカタログに一括追加する」を参照してください。

スコープページと**概要**ページには、HPE Moonshot固有の情報は含まれていません。

PowerShellコマンドを使用してマシンカタログを作成する

ブローカーカタログを作成し、マシンをブローカーカタログにインポートするには、`New-BrokerCatalog`および`New-BrokerMachine` PowerShellコマンドを実行します。

例:

```
New-BrokerCatalog  -AdminAddress "MyDDC.MyDomain.local" -AdminClientIP
"103.14.252.249" -AllocationType "Random" -IsRemotePC $False
-MachinesArePhysical $False -MinimumFunctionalLevel "L7_20" -Name "BurMC"
-PersistUserChanges "OnLocal" -ProvisioningType "Manual" -Scope @()
-SessionSupport "MultiSession" -ZoneUid "e166e2cb-25dc-4578-bc07-
bcf2a82d1463"

New-BrokerMachine  -AdminAddress "MyDDC.MyDomain.local" -AdminClientIP
"103.14.252.249" -CatalogUid 3 -HostedMachineId "c10n1"
-HypervisorConnectionUid 4 -IsReserved $False -MachineName
"S-1-5-21-2589939477-3963209805-1860259709-1121"
```

次のステップ

- これが最初に作成するカタログである場合、Web Studioは(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/delivery-groups-create.html)に誘導します。
- 構成プロセス全体を確認するには、(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure.html)を参照してください。
- カタログを管理するには、(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/machine-catalogs-manage.html)および(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/machine-catalogs-manage/manage-machine-catalog-hpe-moonshot.html)を参照してください。

詳細情報

- 接続とリソースの作成および管理
- HPE Moonshotへの接続
- マシンカタログの作成

Microsoft Azureカタログの作成

(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/machine-catalogs-create.html)では、マシンカタログを作成するウィザードについて説明しています。以下の情報は、Microsoft Azure Resource Managerクラウド環境に固有の詳細を扱っています。

> **注:**
>
> Microsoft Azureカタログを作成する前に、Microsoft Azureへの接続の作成を完了する必要があります。Microsoft Azureへの接続を参照してください。

マシンカタログの作成

マシンカタログは、次の2つの方法で作成できます。

- Web StudioでAzure Resource Managerイメージを使用してマシンカタログを作成する
- PowerShellを使用してマシンカタログを作成する

Web StudioでAzure Resource Managerイメージを使用してマシンカタログを作成する

イメージは、ディスク、スナップショット、またはAzure Compute Gallery内のイメージ定義のイメージバージョンであり、マシンカタログ内のVMを作成するために使用されます。マシンカタログを作成する前に、Azure Resource Managerでイメージを作成します。イメージに関する一般的な情報については、「マシンカタログの作成」を参照してください。

> **注:**
>
> ホスト接続で構成されているリージョンとは異なるリージョンからマスターイメージを使用するサポートは非推奨です。Azure Compute Galleryを使用して、マスターイメージを目的のリージョンにレプリケートしてください。

> MCSマシンカタログを作成する際、DHCPの有効化やライセンスのリアームなどの準備タスクを実行するために、元のVMに基づいて一時的なVMが作成されます。この一時的なVMは準備VMと呼ばれます。この準備VMの名前は**Preparati-84x9n**という形式に従い、最後の5文字は重複を避けるためにランダムに生成されます。この準備VMの命名規則は固定されており、カスタマイズできません。準備タスクが完了すると、準備VMは破棄されます。

準備VMからネットワークを切断するために、すべてのインバウンドおよびアウトバウンドトラフィックを拒否するネットワークセキュリティグループが作成されます。ネットワークセキュリティグループは、カタログごとに1回自動的に作成されます。ネットワークセキュリティグループの名前は`Citrix-Deny-All-a3pgu-GUID`で、GUIDはランダムに生成されます。例: `Citrix-Deny-All-a3pgu-3f161981-28e2-4223-b797-88b04d336dd1`。

マシンカタログ作成ウィザードで:

- 「**マシンタイプ**」および「**マシン管理**」ページには、Azure固有の情報は含まれていません。マシンカタログの作成の記事のガイダンスに従ってください。
- **イメージ**ページで、このカタログにマシンを作成するためのテンプレートとして使用するイメージを選択します。

  使用するイメージの種類として**マスターイメージ**を選択する場合は、**イメージの選択**をクリックし、必要に応じてマスターイメージを選択するために次の手順に従います。

  a. (テナント内またはテナント間で共有イメージが構成されている接続にのみ適用) イメージが存在するサブスクリプションを選択します。
  b. リソースグループを選択します。
  c. Azure VHD、Azure Compute Gallery、またはAzureイメージバージョンに移動します。必要に応じて、選択したイメージにメモを追加します。

  イメージを選択する際は、次の点を考慮してください。

  - イメージにCitrix VDAがインストールされていることを確認します。
  - VMに接続されているVHDを選択する場合は、次の手順に進む前にVMをシャットダウンする必要があります。

> **注:**
>
> - カタログ内のマシンを作成した接続（ホスト）に対応するサブスクリプションは、緑色の点で示されます。その他のサブスクリプションは、Azure Compute Galleryがそ

のサブスクリプションと共有されているものです。これらのサブスクリプションでは、共有ギャラリーのみが表示されます。共有サブスクリプションの構成方法については、テナント内でイメージを共有する（サブスクリプション間）およびテナント間でイメージを共有するを参照してください。

- Trusted Launchが有効になっているイメージまたはスナップショットを選択する場合、**セキュリティの種類**としてTrusted Launchを持つマシンプロファイルを使用することが必須です。その後、マシンプロファイルでSecureBootとvTPMの値を指定することで、それらを有効または無効にできます。Trusted LaunchはShared Image Galleryではサポートされていません。Azure Trusted Launchの詳細については、`<https://docs.microsoft.com/ja-jp/azure/virtual-machines/trusted-launch>`を参照してください。
- Trusted Launchが有効なWindowsでエフェメラルOSディスクを使用してプロビジョニングスキームを作成できます。Trusted Launchが有効なイメージを選択する場合、vTPMが有効なTrusted Launchを持つマシンプロファイルを選択する必要があります。エフェメラルOSディスクを使用してマシンカタログを作成する方法については、(#azure-ephemeral-disks)を参照してください。
- イメージのレプリケーションが進行中でも、イメージをマスターイメージとして選択し、セットアップを完了できます。ただし、イメージのレプリケーション中はカタログ作成に時間がかかる場合があります。MCSでは、カタログ作成開始から1時間以内にレプリケーションが完了する必要があります。レプリケーションがタイムアウトすると、カタログ作成は失敗します。Azureでレプリケーションステータスを確認できます。レプリケーションがまだ保留中の場合、またはレプリケーションが完了した後に再度試してください。
- Azureでマシンカタログのマスターイメージを選択すると、MCSは選択したマスターイメージとマシンプロファイルに基づいてOSタイプを識別します。MCSが識別できない場合は、マスターイメージに一致するOSタイプを選択します。
- Gen2イメージを使用してGen2 VMカタログをプロビジョニングすることで、起動時間のパフォーマンスを向上させることができます。ただし、Gen1イメージを使用してGen2マシンカタログを作成することはサポートされていません。同様に、Gen2イメージを使用してGen1マシンカタログを作成することもサポートされていません。また、世代情報を持たない古いイメージはすべてGen1イメージです。

使用するイメージの種類として**準備済みイメージ**を選択する場合は、**イメージの選択**をクリックし、必要に応じて準備済みイメージを選択します。

VMの作成を成功させるには、イメージにCitrix VDA 2311以降がインストールされており、VDAにMCSIOが存在することを確認してください。

イメージを選択すると、**マシンプロファイルを使用する（Microsoft Entra IDでは必須）** チェックボックスが自動的に選択されます。**マシンプロファイルの選択**をクリックして、リソースグループのリストからVMまたはARMテンプレート仕様を参照します。カタログ内のVMは、選択したマシンプロファイルから構成を継承できます。

ARMテンプレート仕様がマシンカタログを作成するためのマシンプロファイルとして使用できることを確認するために検証します。ARMテンプレート仕様を検証する方法は2つあります。

- リソースグループリストからARMテンプレート仕様を選択した後、**次へ**をクリックします。ARMテンプレート仕様にエラーがある場合、エラーメッセージが表示されます。
- 次のPowerShellコマンドのいずれかを実行します。
  - `Test-ProvInventoryItem -HostingUnitName <string> -InventoryPath <string>`
  - `Test-ProvInventoryItem -HostingUnitUid <Guid> -InventoryPath <string>`

VMがマシンプロファイルから継承できる構成の例は次のとおりです。

- アクセラレーテッドネットワーク
- ブート診断
- ホストディスクキャッシュ (OSおよびMCSIOディスクに関連)
- マシンサイズ (別途指定がない限り)
- VMに配置されたタグ

カタログを作成した後、イメージがマシンプロファイルから継承する構成を表示できます。**マシンカタログ**ノードでカタログを選択し、下部のペインで詳細を表示します。次に、**テンプレートプロパティ**タブをクリックして、マシンプロファイルのプロパティを表示します。**タグ**セクションには最大3つのタグが表示されます。VMに配置されているすべてのタグを表示するには、**すべて表示**をクリックします。

MCSでAzure専用ホストにVMをプロビジョニングする場合は、**専用ホストグループを使用**チェックボックスを有効にしてから、リストからホストグループを選択します。ホストグループは、専用ホストのコレクションを表すリソースです。専用ホストは、1つ以上のVMをホストする物理サーバーを提供するサービスです。サーバーはAzureサブスクリプション専用であり、他のサブスクライバーと共有されることはありません。専用ホストを使用すると、AzureはVMがそのホストで実行されている唯一のマシンであることを保証します。この機能は、規

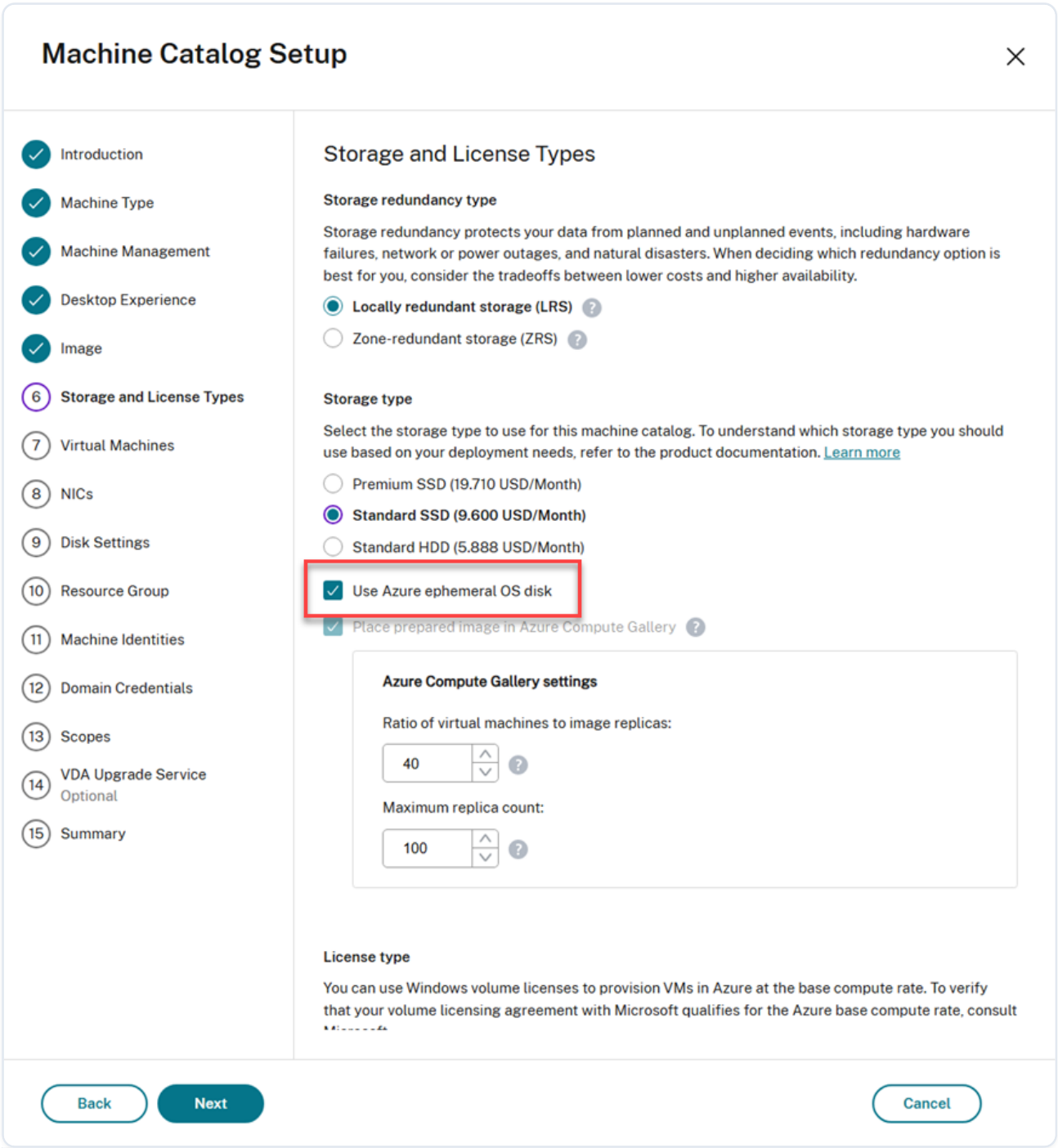
制要件または内部セキュリティ要件を満たす必要があるシナリオに適しています。ホストグループとその使用に関する考慮事項の詳細については、「Azure 専用ホスト」を参照してください。

> **重要:**
>
> - Azure自動配置が有効になっているホストグループのみが表示されます。
> - ホストグループを使用すると、ウィザードの後半で提供される**仮想マシン**ページが変更されます。選択したホストグループに含まれるマシンサイズのみがそのページに表示されます。また、可用性ゾーンは自動的に選択され、選択できません。

- **ストレージとライセンスの種類**ページは、Azure Resource Managerイメージを使用する場合にのみ表示されます。
  - **ストレージ冗長タイプ**を選択します。
    - ローカル冗長ストレージ（LRS）：LRSを使用すると、利用可能なすべてのストレージタイプから選択できます。LRSを使用する場合、Azureは指定された可用性ゾーン内にのみ仮想マシン（VM）をデプロイします。
    - ゾーン冗長ストレージ（ZRS）：ZRSはVM配置の柔軟性を高め、Azureは利用可能な任意のゾーンでVMを起動できます。これはローカル冗長ストレージ（LRS）に対する主要な利点であり、ディスクの元のゾーンにアクセスできなくなった場合でもVMの可用性を保証します。ただし、ZRSはPremium SSDおよびStandard SSDストレージタイプとのみ互換性があります。
  - マシンカタログに使用する**ストレージタイプ**を選択します。ストレージタイプによって、ウィザードの**仮想マシン**ページで提供されるマシンサイズが決まります。
    - I/O負荷の高いワークロードを持つVMに適した、高性能で低遅延のディスクストレージオプションとして、「**Premium SSD**」を提供します。
    - **Standard SSD**。低いIOPSレベルで一貫したパフォーマンスを必要とするワークロードに適した、費用対効果の高いストレージオプションを提供します。
    - **Standard HDD**。待機時間に影響を受けにくいワークロードを実行する VM に適した、信頼性の高い低コストのディスクストレージオプションを提供します。
  - 「**Azureエフェメラルosディスクを使用**」を選択します。AzureエフェメラルOSディスクは、VMのローカルディスクを再利用してオペレーティングシステムディスクをホストす

る、費用対効果の高いストレージオプションを提供します。または、PowerShellを使用してエフェメラルOSディスクを使用するマシンを作成することもできます。詳細については、「Azureエフェメラルディスク」を参照してください。エフェメラルOSディスクを使用する際は、次の点を考慮してください。

- AzureエフェメラルOSディスクとMCS I/Oは同時に有効にできません。
- エフェメラルOSディスクを使用するマシンを更新するには、VMのキャッシュディスクまたは一時ディスクのサイズを超えないイメージを選択する必要があります。
- ウィザードの後半で提供される「**電源サイクル中にVMとシステムディスクを保持**」オプションは使用できません。



> **Note:**
>
> - The identity disk is always created using Standard SSD irrespective of the storage type that you choose.
> - If you select **ZRS** as the **Storage redundancy**, you get the option to only select **Premium SSD** and **Standard SSD**.

```
For details about Azure storage types and storage replication, see the
following:



-  `<https://docs.microsoft.com/en-us/azure/storage/common/storage-
introduction/>`

-  `<https://docs.microsoft.com/en-us/azure/virtual-machines/premium-
storage-performance/>`

-  `<https://docs.microsoft.com/en-us/azure/storage/common/storage-
redundancy/>`
```

既存のWindowsライセンスまたはLinuxライセンスを使用するかどうかを選択します。

```
-  Windows licenses: Using Windows licenses along with Windows images
(Azure platform support images or custom images) lets you run Windows VMs
in Azure at a reduced cost. There are two types of licenses:



    -  **Windows Server license**. Lets you use your Windows Server or
Azure Windows Server licenses, allowing you to use Azure Hybrid Benefits.
For details, see `<https://azure.microsoft.com/en-us/pricing/hybrid-
benefit/>`. Azure Hybrid Benefit reduces the cost of running VMs in Azure
to the base compute rate, waiving the cost of extra Windows Server
licenses from the Azure gallery.



    -  **Windows Client license**. Lets you bring your Windows 10 and
Windows 11 licenses to Azure, allowing you to run Windows 10 and Windows
11 VMs in Azure without the need for extra licenses. For details, see
[Client Access Licenses and Management Licenses](https://
www.microsoft.com/en-us/licensing/product-licensing/client-access-
license).



You can verify that the provisioned VM is using the licensing benefit by
running the following PowerShell command: `Get-AzVM -ResourceGroup
```

MyResourceGroup -Name MyVM`.

- For the Windows Server license type, verify that the license type is **Windows_Server**. More instructions are available at `<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/hybrid-use-benefit-licensing/>`.

- For the Windows Client license type, verify that the license type is **Windows_Client**. More instructions are available at `<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/windows-desktop-multitenant-hosting-deployment/>`.

Alternatively, you can use the `Get-Provscheme` PowerShell SDK to do the verification. For example: `Get-Provscheme -ProvisioningSchemeName "My Azure Catalog"`. For more information about this cmdlet, see `<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Get-ProvScheme/>`.

- Linux licenses: With bring-your-own-subscription (BYOS) Linux licenses, you do not have to pay for the software. The BYOS charge only includes the compute hardware fee. There are two types of licenses:

    - **RHEL_BYOS**: To use RHEL_BYOS type successfully, enable Red Hat Cloud Access on your Azure subscription.

    - **SLES_BYOS**: The BYOS versions of SLES include support from SUSE.

   You can set the LicenseType value to Linux options at `New-ProvScheme` and `Set-ProvScheme`.

Example of setting LicenseType to RHEL_BYOS at `New-ProvScheme`:

```
New-ProvScheme -CleanOnBoot -ProvisioningSchemeName "azureCatalog"
-RunAsynchronously -Scope @() -SecurityGroup @() -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"><Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" /><Property xsi:type="StringProperty"
Name="StorageAccountType" Value="StandardSSD_LRS" /><Property
xsi:type="StringProperty" Name="ResourceGroups" Value="hu-dev-mcs" /
><Property xsi:type="StringProperty" Name="OsType" Value="Linux" /
><Property xsi:type="StringProperty" Name="LicenseType"
Value="RHEL_BYOS" /></CustomProperties>'
```

Example of setting LicenseType to SLES_BYOS at `Set-ProvScheme`:

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog" -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"><Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" /><Property xsi:type="StringProperty"
Name="StorageAccountType" Value="StandardSSD_LRS" /><Property
xsi:type="StringProperty" Name="ResourceGroups" Value="hu-dev-mcs" /
><Property xsi:type="StringProperty" Name="OsType" Value="Linux" /
><Property xsi:type="StringProperty" Name="LicenseType"
Value="SLES_BYOS" /></CustomProperties>'
```

> **Note:**
>
> If `LicenseType` value is empty, then the default values are Azure Windows Server License or Azure Linux License, depending on OsType value.

Example of setting LicenseType to empty:

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog" -CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" /><Property xsi:type="StringProperty" Name="StorageAccountType" Value="StandardSSD_LRS" /><Property xsi:type="StringProperty" Name="ResourceGroups" Value="hu-dev-mcs" /><Property xsi:type="StringProperty" Name="OsType" Value="Linux" /></CustomProperties>'
```

See the following documents to understand License types and their benefits:

- `<https://docs.microsoft.com/en-us/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet>`

- `<https://docs.microsoft.com/en-us/azure/virtual-machines/linux/azure-hybrid-benefit-linux>`

```
Azure Compute Gallery (formerly Azure Shared Image Gallery) is a
repository for managing and sharing images. It lets you make your images
available throughout your organization. We recommend that you store an
image in SIG when creating large non-persistent machine catalogs because
doing that enables faster resets of VDA OS disks. After you select **Place
prepared image in Azure Compute Gallery**, the **Azure Compute Gallery
settings** section appears, letting you specify more Azure Compute Gallery
settings:



-  **Ratio of virtual machines to image replicas**. Lets you specify the
ratio of virtual machines to image replicas that you want Azure to keep.
By default, Azure keeps a single image replica for every 40 non-persistent
machines. For persistent machines, that number defaults to 1,000.



-  **Maximum replica count**. Lets you specify the maximum number of image
replicas that you want Azure to keep. The default is 100.

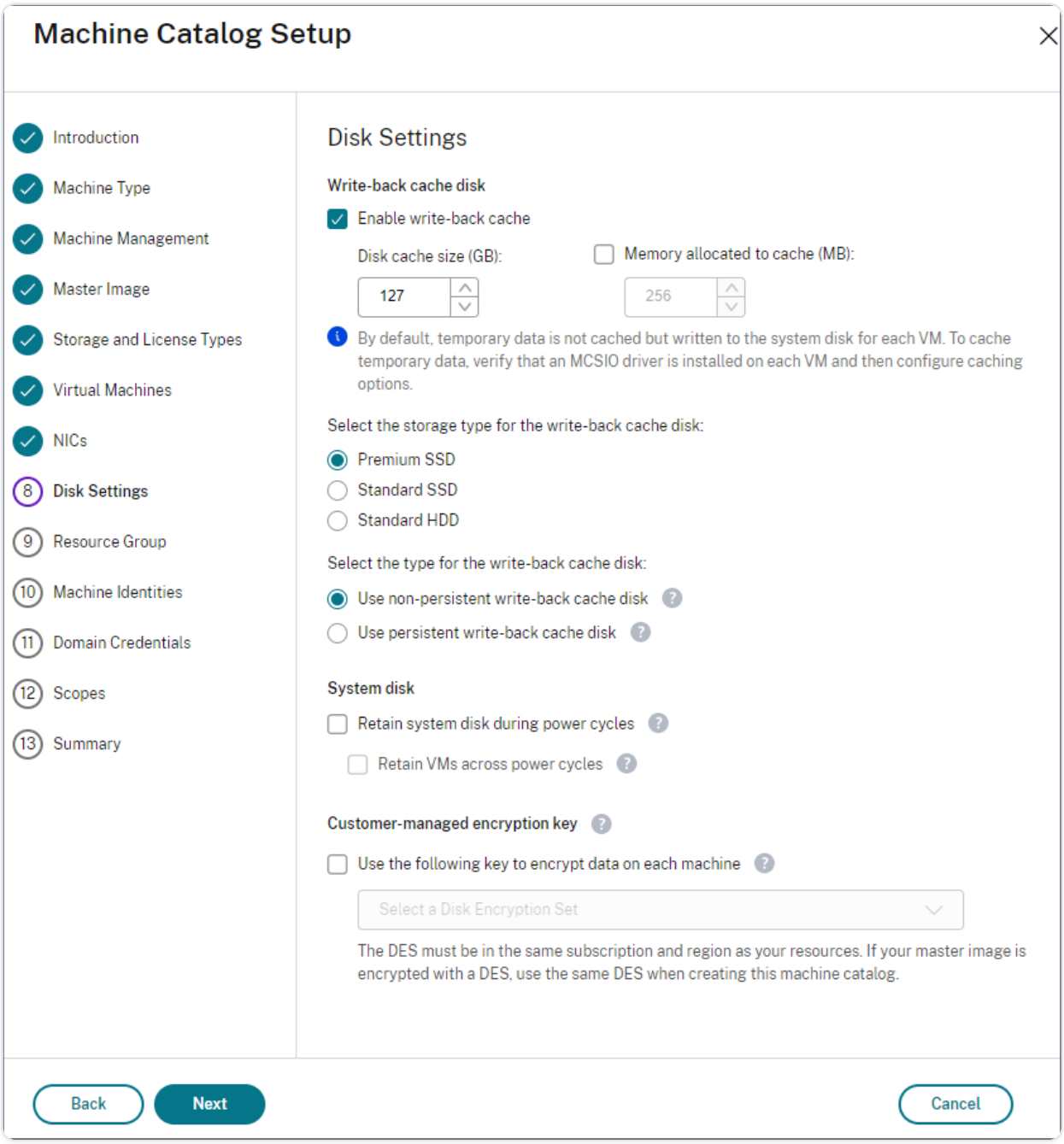


> **Note:**

>

> A gallery is created in ACG to store the image. This gallery is
accessible only to MCS for VM creation and doesn't appear on the **Select
an image** page.
```

- **仮想マシン**ページで、作成する VM の数とマシンのサイズを指定します。カタログ作成後、カタログを編集してマシンのサイズを変更できます。
- **NICs**ページにはAzure固有の情報は含まれていません。マシンカタログの作成の記事のガイダンスに従ってください。
- **ディスク設定**ページで、ライトバックキャッシュを有効にするかどうかを選択します。MCS ストレージ最適化機能が有効になっている場合、カタログ作成時に以下の設定を構成できます。これらの設定は、Azure と GCP の両方の環境に適用されます。



ライトバックキャッシュを有効にした後、以下を実行できます。

- 一時データをキャッシュするために使用するディスクとRAMのサイズを構成します。詳細については、「一時データのキャッシュの構成」を参照してください。
- ライトバックキャッシュディスクのストレージタイプを選択します。ライトバックキャッシュディスクには、次のストレージオプションを使用できます。
  - プレミアム SSD
  - スタンダード SSD
  - スタンダード HDD

> **注:**
>
> **ストレージとライセンスの種類**ページで**ストレージ冗長性**として**ZRS**を選択した場合、ライトバックキャッシュディスクのストレージ冗長性はデフォルトでZRSに設定されます。

- プロビジョニングされたVMに対してライトバックキャッシュディスクを永続化するかどうかを選択します。オプションを有効にするには、**ライトバックキャッシュを有効にする**を選択します。デフォルトでは、**非永続ライトバックキャッシュディスクを使用する**が選択されています。
- ライトバックキャッシュディスクの種類を選択します。
  - **非永続ライトバックキャッシュディスクを使用する**。選択した場合、ライトバックキャッシュディスクは電源サイクル中に削除されます。そこにリダイレクトされたデータはすべて失われます。VMの一時ディスクに十分な空き容量がある場合、コストを削減するためにライトバックキャッシュディスクをホストするために使用されます。カタログ作成後、プロビジョニングされたマシンが一時ディスクを使用しているかどうかを確認できます。これを行うには、カタログをクリックし、**テンプレートプロパティ**タブの情報を確認します。一時ディスクが使用されている場合、**非永続ライトバックキャッシュディスク**が表示され、その値は**はい（VMの一時ディスクを使用）**となります。そうでない場合、**非永続ライトバックキャッシュディスクが表示され、その値は**いいえ（VMの一時ディスクを使用しない）**となります。
  - **永続ライトバックキャッシュディスクを使用する**。選択した場合、ライトバックキャッシュディスクはプロビジョニングされたVMに対して永続的になります。このオプションを有効にすると、ストレージコストが増加します。

> **注:**
>
> 以下のすべての条件が満たされている場合、カタログはWBCディスクにAzure一時ディスクを自動的に使用します。
>
> - MCSIOが有効になっている。
> - WBCディスクが非永続である。
> - VMサイズに、WBCディスクに十分な大きさの一時ディスクが含まれている。

- WBCディスクにドライブ文字が指定されていない。 この機能は、カタログの作成と編集の両方に適用され、ストレージコストの削減に役立ちます。

- 電源サイクル中にVDAのVMとシステムディスクを保持するかどうかを選択します。

  電源サイクル中に VM とシステムディスクを保持する。ライトバックキャッシュを有効にするを選択した場合に利用可能です。デフォルトでは、VM とシステムディスクはシャットダウン時に削除され、起動時に再作成されます。VM の再起動時間を短縮したい場合は、このオプションを選択します。このオプションを有効にすると、ストレージコストも増加することに注意してください。

- **ストレージコストの節約**を有効にするかどうかを選択します。有効にすると、VM シャットダウン時にストレージディスクを Standard HDD にダウングレードすることで、ストレージコストを節約できます。VM は再起動時に元の設定に戻ります。このオプションは、ストレージディスクとライトバックキャッシュディスクの両方に適用されます。または、PowerShell を使用することもできます。VM シャットダウン時にストレージタイプを下位層に変更するを参照してください。

  注:

  Microsoftは、VMシャットダウン中のストレージタイプの変更に制限を課しています。また、Microsoftが将来的にストレージタイプの変更をブロックする可能性もあります。詳細については、このMicrosoft記事を参照してください。

- このカタログ内のマシンのデータを暗号化するかどうか、およびどの暗号化キーを使用するかを選択します。顧客管理キー (CMK) を使用したサーバー側暗号化により、マネージドディスクレベルで暗号化を管理し、カタログ内のマシンのデータを保護できます。デフォルト設定は、マシンプロファイルまたはマスターイメージのいずれかから継承され、プロファイルが優先されます。

  - *CMK* を使用する *マシンプロファイル* を使用している場合、**各マシンのデータを暗号化するために次のキーを使用する** オプションが自動選択され、*マシンプロファイル* のキーがデフォルトになります。
  - プラットフォーム管理キー (PMK) を使用する *マシンプロファイル* を使用しており、*マスターイメージ* が *CMK* で暗号化されている場合、**各マシンのデータを暗号化するために次のキーを使用する** オプションが自動選択され、マスターイメージのキーがデフォルトになります。

- *マシンプロファイル* を使用しておらず、*マスターイメージ* が *CMK* で暗号化されている場合、**各マシンのデータを暗号化するために次のキーを使用する** オプションが自動選択され、*マスターイメージ* のキーがデフォルトになります。

詳細については、Azure サーバー側暗号化を参照してください。

- **リソースグループ** ページで、リソースグループを作成するか、既存のグループを使用するかを選択します。
  - リソースグループを作成することを選択した場合は、**次へ** を選択します。
  - 既存のリソースグループを使用することを選択した場合、**利用可能なプロビジョニングリソースグループ**リストからグループを選択します。**注意**: カタログで作成するマシンを収容するのに十分な数のグループを選択してください。少なすぎるグループを選択すると、メッセージが表示されます。後でカタログに VM を追加する予定がある場合は、必要最小限よりも多く選択することをお勧めします。カタログ作成後、カタログにリソースグループを追加することはできません。

詳細については、Azure リソースグループを参照してください。

- **マシンID** ページで、IDタイプを選択し、このカタログ内のマシンのIDを構成します。VMを **Microsoft Entra joined** として選択した場合、それらをMicrosoft Entraセキュリティグループに追加できます。詳細な手順は次のとおりです。

  a. **IDタイプ**フィールドから、**Microsoft Entra joined**を選択します。**Microsoft Entraセキュリティグループ (オプション)**オプションが表示されます。

  b. **Microsoft Entraセキュリティグループ: 新規作成** をクリックします。

  c. グループ名を入力し、**作成**をクリックします。

  d. 画面の指示に従って Azure にサインインします。 グループ名が Azure に存在しない場合、緑色のアイコンが表示されます。それ以外の場合は、新しい名前を入力するよう求めるエラーメッセージが表示されます。

  e. VM のマシンアカウントの命名スキームを入力します。

  カタログ作成後、Citrix Virtual Apps and Desktopsはユーザーに代わってAzureにアクセスし、セキュリティグループと、そのグループの動的メンバーシップルールを作成します。このルールに基づき、このカタログで指定された命名規則を持つVMは自動的にセキュリティグループに追加されます。

  異なる命名規則を持つVMをこのカタログに追加するには、Azureにサインインする必要があります。その後、Citrix Virtual Apps and Desktops™はAzureにアクセスし、新しい命名規則に基づいて動的メンバーシップルールを作成できます。

このカタログを削除する際、Azure からセキュリティグループを削除するには、Azure へのサインインも必要です。

- **ドメイン資格情報**ページと**概要**ページには、Azure 固有の情報は含まれていません。マシンカタログの作成の記事のガイダンスに従ってください。

> **ヒント:**
>
> **概要**ページでは、Azureの公開価格に基づいて、このマシンカタログ内の仮想マシンの月額推定コストを表示できます。カタログをホストする接続がAzureで `Microsoft.Consumption/pricesheets/read` 権限を持っている場合、見積もりは組織の契約価格を使用して計算されます。
>
> コスト見積もりを選択すると、詳細情報が表示されます。より正確な見積もりを得るには、日ごとの電源オン時間、週あたりの稼働日数、使用状況に基づいた節約オプションなどの設定を調整します。

ウィザードを完了します。

Azure一時ディスクがライトバックキャッシュディスクとして適格であるための条件

Azure一時ディスクをライトバックキャッシュディスクとして使用できるのは、以下のすべての条件が満たされている場合のみです。

- Azure一時ディスクは永続的なデータには適さないため、ライトバックキャッシュディスクは非永続的である必要があります。
- 選択したAzure VMサイズには一時ディスクが含まれている必要があります。
- エフェメラルOSディスクを有効にする必要はありません。
- ライトバックキャッシュファイルをAzure一時ディスクに配置することを受け入れます。
- Azure一時ディスクのサイズは、（ライトバックキャッシュディスクサイズ + ページングファイル用の予約スペース + 1 GBのバッファースペース）の合計サイズよりも大きい必要があります。

非永続的なライトバックキャッシュディスクのシナリオ

次の表は、マシンカタログの作成時に一時ディスクをライトバックキャッシュに使用する場合の3つの異なるシナリオについて説明しています。

シナリオ	結果
ライトバックキャッシュに一時ディスクを使用するためのすべての条件が満たされています。	WBCファイル `mcsdif.vhdx` は一時ディスクに配置されます。
一時ディスクには、ライトバックキャッシュの使用に十分なスペースがありません。	VHDディスク `MCSWCDisk` が作成され、WBCファイル `mcsdif.vhdx` がこのディスクに配置されます。
一時ディスクにはライトバックキャッシュの使用に十分なスペースがありますが、`UseTempDiskForWBC` が **false** に設定されています。	VHDディスク `MCSWCDisk` が作成され、WBCファイル `mcsdif.vhdx` がこのディスクに配置されます。

Azure テンプレート仕様を作成する

Azure ポータルで Azure テンプレート仕様を作成し、Web Studio および PowerShell コマンドで使用して、MCS マシンカタログを作成または更新できます。

既存のVMのAzureテンプレートスペックを作成するには：

1. Azureポータルに移動します。リソースグループを選択し、VMとネットワークインターフェースを選択します。上部にある**...**メニューから、**テンプレートのエクスポート**をクリックします。
2. カタログプロビジョニング用のテンプレートスペックを作成する場合は、**パラメーターを含める**チェックボックスをオフにします。JSONファイルで `parameters` と `variables` のセクションが次のようになっていることを確認します。

   ```
   "parameters": {},

   "variables": {}
   ```

3. **ダウンロード**をクリックして、テンプレートをJSONファイルとして保存します。
4. Azureポータルで、**テンプレートスペック**を選択し、**テンプレートのインポート**をクリックします。
5. コンピューターに保存されているマシンプロファイル（JSON形式）を参照してインポートします。
6. **名前**、**サブスクリプション**、**リソースグループ**、**場所**、**バージョン**を指定します。**次へ: テンプレートの編集**をクリックします。

7. **レビュー+作成**を作成し、テンプレートスペックを作成します。
8. **テンプレート仕様**ページで、作成したばかりのテンプレート仕様を確認します。テンプレート仕様をクリックします。左側のパネルで、**バージョン**をクリックします。
9. 「**新しいバージョンを作成**」をクリックして新しいバージョンを作成できます。新しいバージョン番号を指定し、現在のテンプレート仕様に変更を加え、「**確認 + 作成**」をクリックして、テンプレート仕様の新しいバージョンを作成します。

以下のPowerShellコマンドを使用して、テンプレートスペックとテンプレートバージョンの情報を取得できます。

- テンプレートスペックの情報を取得するには、以下を実行します。

```
get-item XDHyp:
\HostingUnits\East\machineprofile.folder\abc.resourcegroup\bggTemplateS
pec.templatespec
```

- テンプレートスペックバージョンの情報を取得するには、以下を実行します。

```
get-item XDHyp:
\HostingUnits\East\machineprofile.folder\abc.resourcegroup\bggTemplateS
pec.templatespec\bgg1.0.templatespecversion
```

カタログの作成または更新でテンプレート仕様を使用する

MCSマシンカタログは、マシンプロファイル入力としてテンプレート仕様を使用して作成または更新できます。これを行うには、Web StudioまたはPowerShellコマンドを使用できます。

- Web Studioについては、「Web StudioでAzure Resource Managerイメージを使用してマシンカタログを作成する」を参照してください。
- PowerShellについては、「PowerShellを使用してカタログを作成または更新する際にテンプレート仕様を使用する」を参照してください。

Azureサーバー側暗号化

Citrix Virtual Apps and Desktopsは、Azure Key Vaultを介したAzureマネージドディスクの顧客管理暗号化キーをサポートしています。このサポートにより、独自の暗号化キーを使用してマシンカタログのマネージドディスクを暗号化することで、組織およびコンプライアンス要件を管理できます。詳細については、「Azure Disk Storageのサーバー側暗号化」を参照してください。

マネージドディスクでこの機能を使用する場合：

- ディスクの暗号化に使用するキーを変更するには、`DiskEncryptionSet` で現在のキーを変更します。その `DiskEncryptionSet` に関連付けられているすべてのリソースは、新しいキーで暗号化されるように変更されます。
- キーを無効にするか削除すると、そのキーを使用しているディスクを持つVMは自動的にシャットダウンします。シャットダウン後、キーが再度有効になるか、新しいキーを割り当てない限り、VMは使用できません。そのキーを使用しているカタログは電源をオンにできず、VMを追加することもできません。

顧客管理暗号化キーを使用する際の重要な考慮事項

この機能を使用する際は、以下を考慮してください。

- 顧客管理キーに関連するすべてのリソース（Azure Key Vault、ディスク暗号化セット、VM、ディスク、スナップショット）は、同じサブスクリプションとリージョンに存在する必要があります。
- 顧客管理キーで暗号化されたディスク、スナップショット、およびイメージは、別のリソースグループやサブスクリプションに移動できません。
- ディスク暗号化セットのリージョンごとの制限については、Microsoft サイトを参照してください。

> **注:**
>
> Azure サーバー側暗号化の構成については、クイックスタート: Azure portal を使用して Key Vault を作成する を参照してください。

Azureカスタマーマネージド暗号化キー

マシンカタログを作成する際、カタログにプロビジョニングされたマシン上のデータを暗号化するかどうかを選択できます。カスタマーマネージド暗号化キーによるサーバー側暗号化を使用すると、マネージドディスクレベルで暗号化を管理し、カタログ内のマシン上のデータを保護できます。ディスク暗号化セット（DES）は、カスタマーマネージドキーを表します。この機能を使用するには、まずAzureでDESを作成する必要があります。DESは次の形式です。

- `/subscriptions/12345678-1234-1234-1234-123456789012/resourceGroups/Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/SampleEncryptionSet`

リストからDESを選択します。選択するDESは、リソースと同じサブスクリプションおよびリージョンにある必要があります。

「顧客管理キーを使用したマシンカタログの作成」を参照してください。

ホストでのAzureディスク暗号化

ホストでの暗号化機能を備えたMCSマシンカタログを作成できます。現在、MCSはこの機能に対してマシンプロファイルのワークフローのみをサポートしています。VMまたはテンプレート仕様をマシンプロファイルの入力として使用できます。

この暗号化方法は、Azureストレージを介してデータを暗号化しません。VMをホストするサーバーがデータを暗号化し、その後、暗号化されたデータがAzureストレージサーバーを介して流れます。したがって、この暗号化方法はデータをエンドツーエンドで暗号化します。

制限事項：

ホストでのAzureディスク暗号化は次のとおりです。

- すべてのAzureマシンサイズでサポートされているわけではありません
- Azure ディスク暗号化と互換性がありません

ホストでの暗号化機能を持つマシンカタログを作成するには：

1. サブスクリプションでホストでの暗号化機能が有効になっているかどうかを確認します。これを行うには、`<https://learn.microsoft.com/ja-jp/rest/api/resources/features/get?tabs=HTTP/>`を参照してください。有効になっていない場合は、サブスクリプションでこの機能を有効にする必要があります。サブスクリプションで機能を有効にする方法については、`<https://learn.microsoft.com/ja-jp/azure/virtual-machines/disks-enable-host-based-encryption-portal?tabs=azure-powershell#prerequisites/>`を参照してください。
2. 特定のAzure VMサイズがホストでの暗号化をサポートしているかどうかを確認します。これを行うには、PowerShellウィンドウで次のいずれかを実行します。

   ```
   PS XDHyp:\Connections\<your connection>\east
   us.region\serviceoffering.folder>
   ```

   ```
   PS XDHyp:\HostingUnits\<your hosting unit>\serviceoffering.folder>
   ```

3. ホストでの暗号化が有効になっているVMまたはテンプレート仕様を、マシンプロファイルの入力としてAzureポータルで作成します。

- VMを作成する場合は、ホストでの暗号化をサポートするVMサイズを選択します。VMを作成すると、VMプロパティの**ホストでの暗号化**が有効になります。
- テンプレート仕様を使用する場合は、`securityProfile`内でパラメーター`Encryption at Host`を**true**として割り当てます。

4. VMまたはテンプレート仕様のいずれかを選択して、マシンプロファイルワークフローでMCSマシンカタログを作成します。

   - OSディスク/データディスク：顧客管理キーとプラットフォーム管理キーを介して暗号化されます
   - エフェメラルOSディスク：プラットフォーム管理キーのみを介して暗号化されます
   - キャッシュディスク: 顧客管理キーとプラットフォーム管理キーによって暗号化されます

   Web StudioまたはPowerShellコマンドを実行して、マシンカタログを作成できます。

マシンプロファイルからホストでの暗号化情報を取得する

`AdditionalData` パラメーターを指定して PowerShell コマンドを実行すると、マシンプロファイルからホストでの暗号化情報を取得できます。`EncryptionAtHost` パラメーターが **True** の場合、そのマシンプロファイルでホストでの暗号化が有効になっていることを示します。

例: マシンプロファイルの入力が VM の場合、次のコマンドを実行します。

```
(get-item XDHyp:
\HostingUnits\myAzureNetwork\machineprofile.folder\abc.resourcegroup\def.v
m).AdditionalData
```

例: マシンプロファイルの入力がテンプレート仕様の場合、次のコマンドを実行します。

```
(get-item XDHyp:
\HostingUnits\myAzureNetwork\machineprofile.folder\abc.resourcegroup\def_t
emplatespec.templatespec\EncryptionAtHost.templatespecversion).AdditionalD
ata
```

マネージドディスクの二重暗号化

二重暗号化を使用してマシンカタログを作成できます。この機能で作成されたカタログはすべて、プラットフォームキーと顧客管理キーの両方でサーバー側が暗号化されます。Azure Key Vault、暗号化キー、およびディスク暗号化セット (DES) はお客様が所有および管理します。

二重暗号化は、プラットフォーム側暗号化（デフォルト）と顧客管理暗号化（CMEK）です。したがって、暗号化アルゴリズム、実装、または侵害されたキーに関連するリスクを懸念するセキュリティ意識の高いお客様は、この二重暗号化を選択できます。永続的なOSディスクとデータディスク、スナップショット、およびイメージはすべて、二重暗号化によって保存時に暗号化されます。

注:

- Web StudioおよびPowerShellコマンドを使用して、二重暗号化されたマシンカタログを作成および更新できます。PowerShellコマンドについては、「二重暗号化されたマシンカタログを作成する」を参照してください。
- 二重暗号化されたマシンカタログを作成または更新するために、マシンプロファイルに基づかないワークフローまたはマシンプロファイルに基づくワークフローを使用できます。
- マシンプロファイルに基づかないワークフローを使用してマシンカタログを作成する場合、保存されている `DiskEncryptionSetId` を再利用できます。
- マシンプロファイルを使用する場合、VM またはテンプレート仕様をマシンプロファイルの入力として使用できます。

制限事項:

- 二重暗号化は、Ultra Disks または Premium SSD v2 ディスクではサポートされていません。
- 二重暗号化は、アンマネージドディスクではサポートされていません。
- カタログに関連付けられているDiskEncryptionSetキーを無効にすると、そのカタログのVMが無効になります。
- お客様が管理するキーに関連するすべてのリソース（Azure Key Vault、ディスク暗号化セット、VM、ディスク、スナップショット）は、同じサブスクリプションとリージョンにある必要があります。
- サブスクリプションごとに、リージョンあたり最大50個のディスク暗号化セットしか作成できません。

Azureリソースグループ

Azureプロビジョニングリソースグループは、ユーザーにアプリケーションとデスクトップを提供するVMをプロビジョニングする方法を提供します。リソースグループを作成するか、既存のリ

ソースグループを使用して、MCSマシンカタログにVMをプロビジョニングできます。複数のマシンカタログで同じリソースグループを使用できます。Azureリソースグループの詳細については、Microsoftドキュメントを参照してください。

Azureリソースグループの使用法

Azureリソースグループあたりの仮想マシン、マネージドディスク、スナップショット、およびイメージの数に制限はありません。（Azureリソースグループあたり240個のVM、800個のマネージドディスクという制限は削除されました。）

- フルスコープのサービスプリンシパルを使用してマシンカタログを作成する場合、MCSは1つのAzureリソースグループのみを作成し、そのグループをカタログに使用します。
- ナロースコープのサービスプリンシパルを使用してマシンカタログを作成する場合、カタログ用に空の、事前に作成されたAzureリソースグループを提供する必要があります。

Azureエフェメラルディスク

Azureエフェメラルディスクを使用すると、キャッシュディスク、一時ディスク、またはNVMeディスクを再利用して、Azure対応仮想マシンのOSディスクを保存できます。この機能は、標準のHDDディスクよりも高性能なSSDディスクを必要とするAzure環境で役立ちます。Azureエフェメラルディスクを使用してカタログを作成する方法については、「Azureエフェメラルディスクを使用したカタログの作成」を参照してください。

> **注:**
>
> 永続カタログはエフェメラルOSディスクをサポートしていません。

> エフェメラルOSディスクでは、プロビジョニングスキームでマネージドディスクと共有イメージギャラリーを使用する必要があります。

エフェメラルOS一時ディスクを保存する

エフェメラルOSディスクをVMの一時ディスク、リソースディスク、またはNVMeディスクに保存するオプションがあります。この機能により、キャッシュがない、またはキャッシュが不足しているVMでエフェメラルOSディスクを使用できます。このようなVMには、`Ddv4`のようなエフェメラルOSディスクを保存するための一時ディスク、リソースディスク、またはNVMeディスクがあります。

次の点を考慮してください。

- エフェメラルディスクは、VMキャッシュディスク、VMの一時（リソース）ディスク、またはNVMeディスクに保存されます。キャッシュディスクがOSディスクのコンテンツを保持するのに十分な大きさでない限り、一時ディスクよりもキャッシュディスクが優先されます。
- 更新の場合、キャッシュディスクより大きく、一時ディスクより小さい新しいイメージは、エフェメラルOSディスクをVMの一時ディスクに置き換える結果となります。

AzureエフェメラルディスクとMachine Creation Services (MCS) ストレージ最適化 (MCS I/O)

AzureエフェメラルOSディスクとMCS I/Oは同時に有効にできません。

重要な考慮事項は次のとおりです。

- エフェメラルOSディスクとMCS I/Oの両方を同時に有効にしてマシンカタログを作成することはできません。
- PowerShellパラメーター (`UseWriteBackCache` および `UseEphemeralOsDisk`) を `New-ProvScheme` または `Set-ProvScheme` で**true**に設定すると、適切なエラーメッセージが表示されて失敗します。
- 両方の機能が有効になっている既存のマシンカタログについては、引き続き以下を行うことができます。
  - マシンカタログを更新する。
  - VMを追加または削除する。
  - マシンカタログを削除する。

アジュール コンピュート ギャラリー

Azure Compute Gallery (旧称 Azure Shared Image Gallery) を、AzureでMCSプロビジョニングされたマシンの公開イメージリポジトリとして使用します。公開イメージをギャラリーに保存することで、OSディスクの作成とハイドレーションを高速化し、非永続VMの起動時間とアプリケーション起動時間を改善できます。共有イメージギャラリーには、次の3つの要素が含まれています。

- *ギャラリー*: イメージはここに保存されます。MCSは、マシンカタログごとに1つのギャラリーを作成します。
- *ギャラリーイメージ定義*: この定義には、公開イメージに関する情報（オペレーティングシステムの種類と状態、Azureリージョン）が含まれます。MCSは、カタログ用に作成されたイメージごとに1つのイメージ定義を作成します。
- *ギャラリーイメージバージョン*: 共有イメージギャラリー内の各イメージは複数のバージョンを持つことができ、各バージョンは異なるリージョンに複数のレプリカを持つことができます。各レプリカは、公開イメージの完全なコピーです。

注:

共有イメージギャラリー機能は、マネージドディスクとのみ互換性があります。レガシーマシンカタログでは使用できません。

詳細については、Azure Compute Galleryの概要を参照してください。

PowerShell を使用して Azure Compute Gallery イメージでマシンカタログを作成または更新する方法については、「Azure Compute Gallery イメージを使用してマシンカタログを作成または更新する」を参照してください。

Azure 機密 VM

Azure 機密コンピューティング VM は、仮想デスクトップがメモリ内で暗号化され、使用中に保護されることを保証します。

MCSを使用してAzure機密VMを含むカタログを作成できます。このようなカタログを作成するには、マシンプロファイルワークフローを使用する必要があります。VMとARMテンプレート仕様の両方をマシンプロファイル入力として使用できます。

機密VMタイプのAzureマスターイメージと機密VMタイプのAzureマシンプロファイルを使用して準備済みイメージを作成し、その準備済みイメージを使用してMCSカタログを作成することもできます。

機密VMに関する重要な考慮事項

サポートされているVMサイズと機密VMを使用したマシンカタログの作成に関する重要な考慮事項は次のとおりです。

- 機密VMでサポートされているVMサイズを確認するには、サイズを参照してください。
- 機密VMを使用してマシンカタログを作成します。
  - Web Studio および PowerShell コマンドを使用して、Azure 機密VMでマシンカタログを作成できます。
  - Azure機密VMを含むマシンカタログを作成するには、マシンプロファイルベースのワークフローを使用する必要があります。VMまたはテンプレート仕様をマシンプロファイル入力として使用できます。

- マスターイメージとマシンプロファイル入力は、両方とも同じ機密セキュリティタイプで有効にする必要があります。異なるAzureリソースは、機密VMタイプを示すために異なるラベルを使用します。

  Azureスナップショット、マネージドディスク、または仮想マシンの場合、セキュリティタイプは次のとおりです。

  - ConfidentialVM_DiskEncryptedWithCustomerKey.
  - ConfidentialVM_DiskEncryptedWithPlatformKey.
  - ConfidentialVM_VMGuestStateOnlyEncryptedWithPlatformKey

  Azure ARMテンプレート仕様バージョンの場合、セキュリティタイプは次のとおりです。

  - VMGuestStateOnly: VMゲスト状態のみが暗号化された機密VM
  - DiskWithVMGuestState: OSディスクとVMゲスト状態の両方がプラットフォーム管理キーまたは顧客管理キーで暗号化された機密VM。通常ディスクとエフェメラルOSディスクの両方を暗号化できます。

- AdditionalDataパラメーターを使用して、マネージドディスク、スナップショット、Azure Compute Galleryイメージ、VM、ARMテンプレート仕様など、さまざまなリソースタイプの機密VM情報を取得できます。例：

  ```
  PS C:\Users\username> (get-item XDHyp:
  \HostingUnits\mynetwork\image.folder\username-dev-testing-
  rg.resourcegroup\username-dev-tsvda.vm).AdditionalData
  ```

  追加データフィールドは次のとおりです。

- DiskSecurityType
- ConfidentialVMDiskEncryptionSetId
- DiskSecurityProfiles

  マシンサイズの機密コンピューティングプロパティを取得するには、次のコマンドを実行します: `(Get-Item -path "XDHyp:\Connections\my-connection-name\East US.region\serviceoffering.folder\abc.serviceoffering").AdditionalData`

  追加データフィールドは`ConfidentialComputingType`です。

- マスターイメージまたはマシンプロファイルを、機密から非機密セキュリティタイプへ、または非機密から機密セキュリティタイプへ変更することはできません。

- 誤った構成に対しては、適切なエラーメッセージが表示されます。

マスターイメージとマシンプロファイルの準備

機密VMのセットを作成する前に、以下の手順に従ってマスターイメージとマシンプロファイルを準備します。

1. Azureポータルで、次のような特定の構成で機密VMを作成します。
   - **セキュリティの種類**: 機密仮想マシン
   - **機密OSディスク暗号化**: 有効。
   - **キー管理**: プラットフォーム管理キーによる機密ディスク暗号化 機密VMの作成について詳しくは、この Microsoft の記事を参照してください。
2. 作成したVMでマスターイメージを準備します。作成したVMに必要なアプリケーションとVDAをインストールします。

   > **注:**
   >
   > VHDを使用した機密VMの作成はサポートされていません。代わりに、Azure Compute Gallery、マネージドディスク、またはスナップショットを使用してください。

3. 次のいずれかの方法でマシンプロファイルを作成します。
   - 手順1で作成した既存のVMが必要なマシンプロパティを備えている場合は、それを使用します。
   - マシンプロファイルとしてARMテンプレート仕様を選択する場合は、必要に応じてテンプレート仕様を作成します。具体的には、*SecurityEncryptionType* や *diskEncryptionSet* (顧客管理キーの場合) など、機密VMの要件を満たすパラメーターを構成します。詳しくは、(#create-an-azure-template-spec)を参照してください。

     > **注:**
     >
     > - マスターイメージとマシンプロファイルが同じセキュリティキータイプであることを確認してください。

> ◦ 顧客管理キーによる機密OSディスク暗号化を必要とする機密VMを作成するには、マスターイメージとマシンプロファイルの両方でディスク暗号化セットIDが同じであることを確認してください。

機密VMタイプの準備済みイメージを使用してMCSカタログを作成する場合は、機密VMタイプのマスターイメージと機密VMタイプのマシンプロファイルを使用して準備済みイメージを作成します。準備済みイメージの作成については、(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/create-prepared-image-machine-catalogs-azure.html#create-an-image-definition-and-initial-image-version)を参照してください。

Web Studio または PowerShell コマンドを使用して機密VMを作成する

機密VMのセットを作成するには、マスターイメージと、目的の機密VMから派生したマシンプロファイルを使用してマシンカタログを作成します。

Web Studio を使用してカタログを作成するには、「マシンカタログの作成」に記載されている手順に従ってください。以下の考慮事項に留意してください。

- **イメージ**ページで、機密VMの作成用に準備したマスターイメージとマシンプロファイルを選択します。マシンプロファイルの選択は必須であり、選択したマスターイメージと同じセキュリティ暗号化タイプに一致するプロファイルのみが選択可能です。
- 「**仮想マシン**」ページでは、機密VMをサポートするマシンサイズのみが選択肢として表示されます。
- 「**ディスク設定**」ページでは、選択したマシンプロファイルから継承されるため、ディスク暗号化セットを指定することはできません。

起動整合性監視

VM でセキュアブートと仮想トラステッドプラットフォームモジュール (vTPM) が有効になっており、`GuestAttestation` 拡張機能がインストールされている場合、Microsoft Defender for Cloud は VM が正常に起動することをリモートで検証できます。この監視は **ブート整合性監視** と呼ばれます。ブート整合性監視の詳細については、ブート整合性監視の概要 を参照してください。

マシンプロファイル（VMまたはテンプレート仕様）を使用して、MCSマシンカタログVM（永続VMおよび非永続VM）の起動整合性監視を有効にできます。起動整合性監視は、信頼できる起動と機密VMのみでサポートされています。

既存のカタログを更新してブート整合性を使用するには、`Set-ProvScheme` を使用してブート整合性が有効なマシンプロファイルを指定します。カタログに追加された新しい VM は、整合性監視が有効になります。

カタログ内の既存の VM は、`Set-ProvVmUpdateTimeWindow`、`Set-ProvVm`、または `Maintenance Cycles` を使用して更新することもできます。以下を変換できます。

- 整合性監視なしの VM を整合性監視ありに
- 整合性監視ありの VM を整合性監視なしに

整合性監視が有効なマシンカタログを作成する

必要な権限:

次の権限があることを確認してください。

- `Microsoft.Compute/virtualMachines/extensions/read`
- `Microsoft.Compute/virtualMachines/extensions/write`

整合性監視が有効なMCSマシンカタログを作成するには、次の手順を実行します。

1. `GuestAttestation` 拡張機能がインストールされたマシンプロファイル (VM またはテンプレート仕様) を作成します。(以下のコンテンツへのリンク)
2. Web Studio または PowerShell コマンドを使用して、マシンプロファイル入力を利用して MCS マシンカタログを作成します。

   > **注:**
   >
   > `Get-Item` PowerShell コマンドを `AdditionalData` パラメーターとともに使用して、VM またはテンプレート仕様の `GuestAttestationExtensionEnabled` ステータスを確認できます。

3. カタログにVMを追加します。

GUESTATTESTATION 拡張機能がインストールされたマシンプロファイルを作成する

整合性監視が有効な VM またはテンプレート仕様をマシンプロファイル入力として作成します。これは GuestAttestation 拡張機能がインストールされていることを意味します。

整合性監視が有効な VM を作成するには、次の手順を実行します:

1. Azureポータルにサインインします。
2. 新しいVMを作成する場合：

a. **セキュリティの種類**を**信頼された起動仮想マシン**または**機密仮想マシン**として選択します。

b. **セキュリティ機能の構成**をクリックし、**整合性監視**チェックボックスをオンにします。

> **注:**
>
> 整合性監視には、セキュアブートと vTPM を有効にする必要があります。

3. 「**概要**」ページで、「**セキュリティの種類**」セクションに移動し、「**セキュリティの種類**」が「**信頼された起動**」または「**機密性の高い仮想マシン**」であり、「**整合性監視**」が有効になっていることを確認します。
4. 「**拡張機能 + アプリケーションページ**」に移動して、`GuestAttestation` がインストールされていることを確認します。

既存のVMの整合性監視を有効にするには、「整合性監視を有効にする - Azure portal」を参照してください。

`GuestAttestation` *拡張機能がインストールされたテンプレート仕様を作成するには:*

- テンプレート仕様を使用してGuestAttestationをインストールできます。「整合性監視を有効にする - テンプレート仕様」を参照してください。

> **注:**
>
> このテンプレート仕様の「**設定**」で、アテステーションに使用するエンドポイントを構成できます。構成しない場合、Azureが構成するエンドポイントを決定します。

Azure Marketplace (アジュール マーケットプレイス)

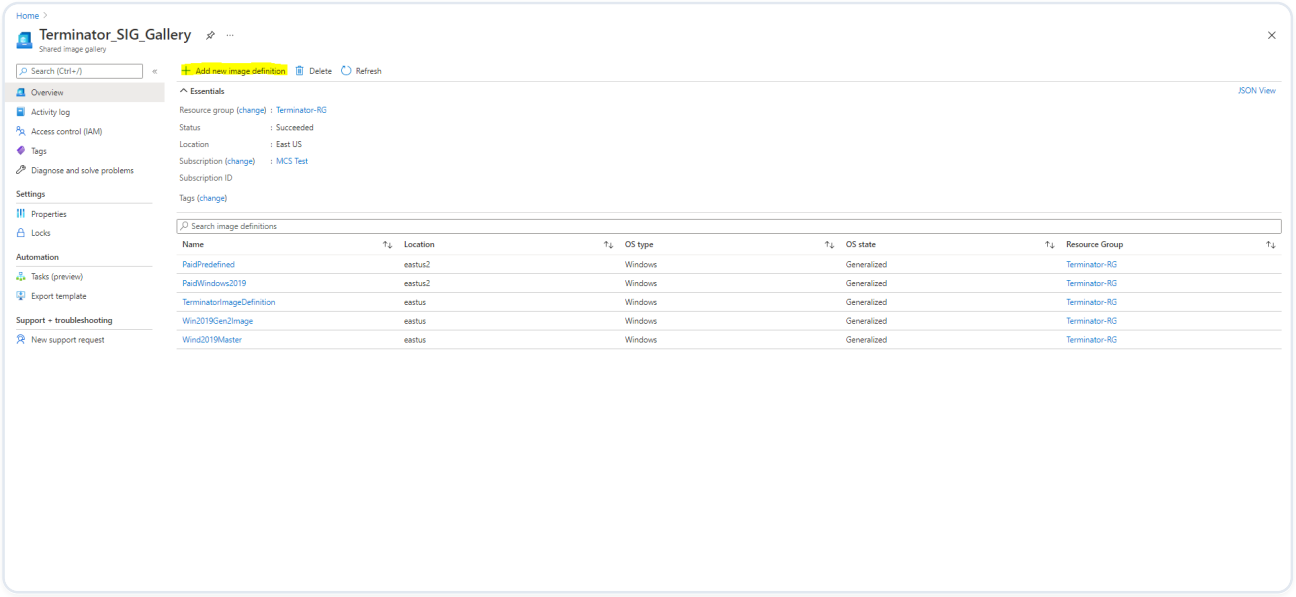
Citrix Virtual Apps and Desktops は、プラン情報を含むAzure上のマスターイメージを使用してマシンカタログを作成することをサポートしています。詳細については、「Microsoft Azure Marketplace」を参照してください。

> **ヒント:**

> 標準のWindows Serverイメージなど、Azure Marketplaceで見つかる一部のイメージには、プラン情報が追加されていません。Citrix Virtual Apps and Desktops の機能は、有料イメージ向けです。

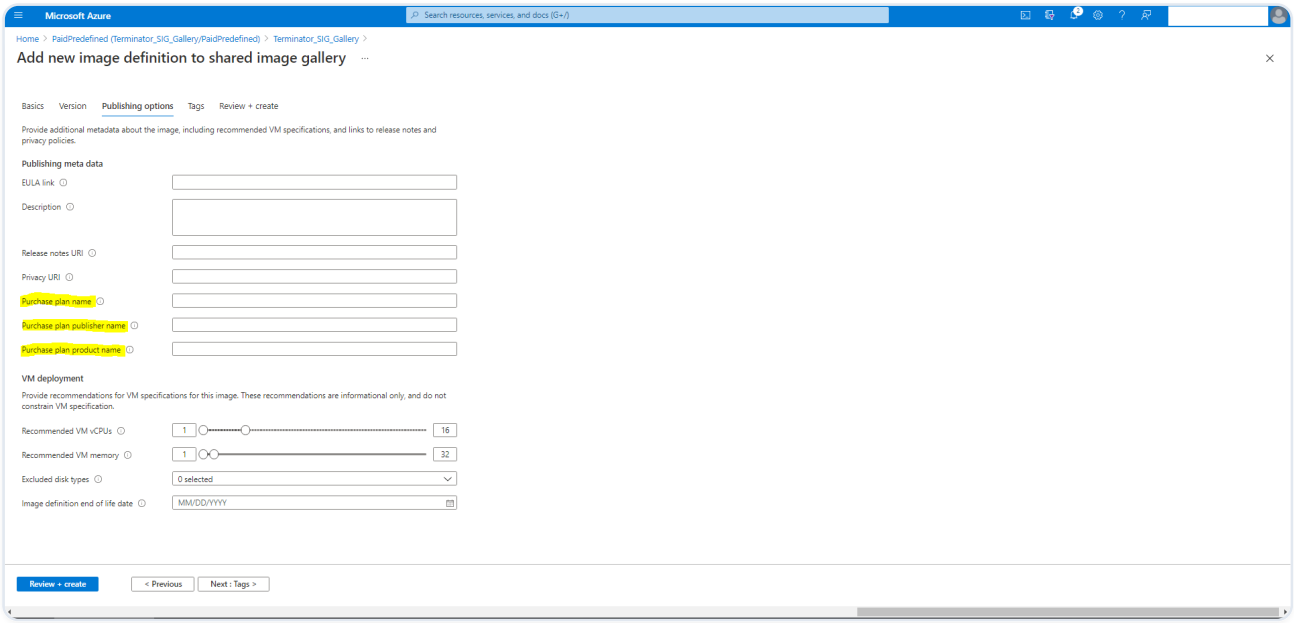
Shared Image Gallery で作成されたイメージに Azure プラン情報が含まれていることを確認します

このセクションの手順を使用して、Web Studio で Shared Image Gallery のイメージを表示します。これらのイメージは、オプションでマスターイメージとして使用できます。イメージを Shared Image Gallery に配置するには、ギャラリーでイメージ定義を作成します。

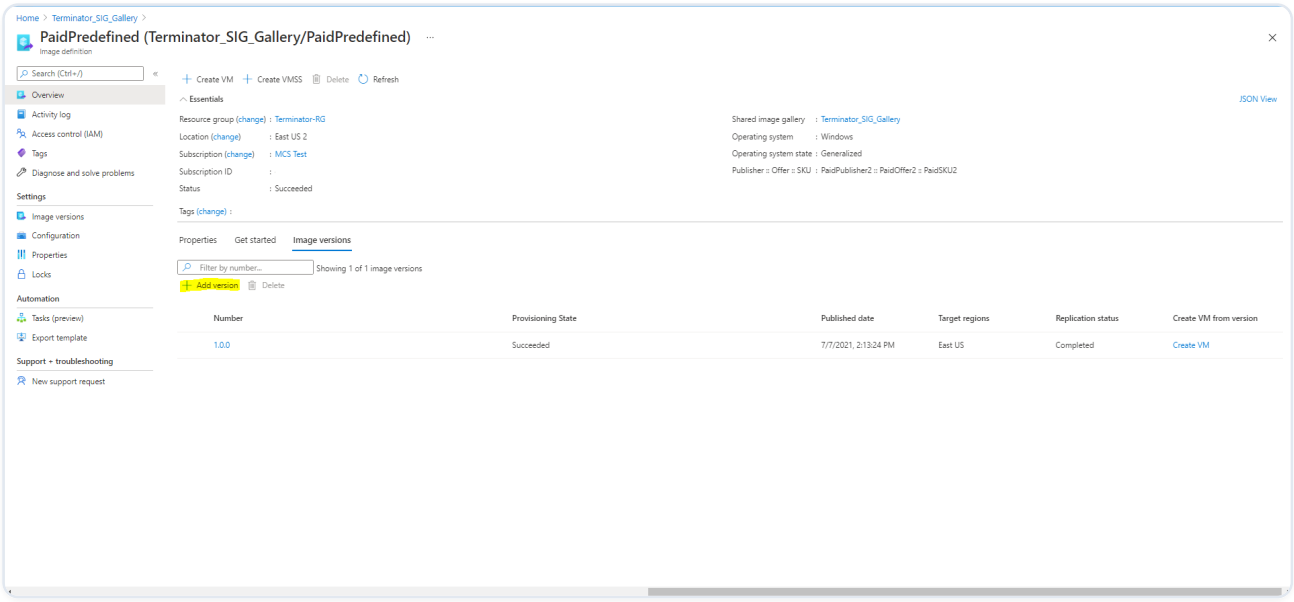


公開オプションページで、購入プラン情報を確認します。

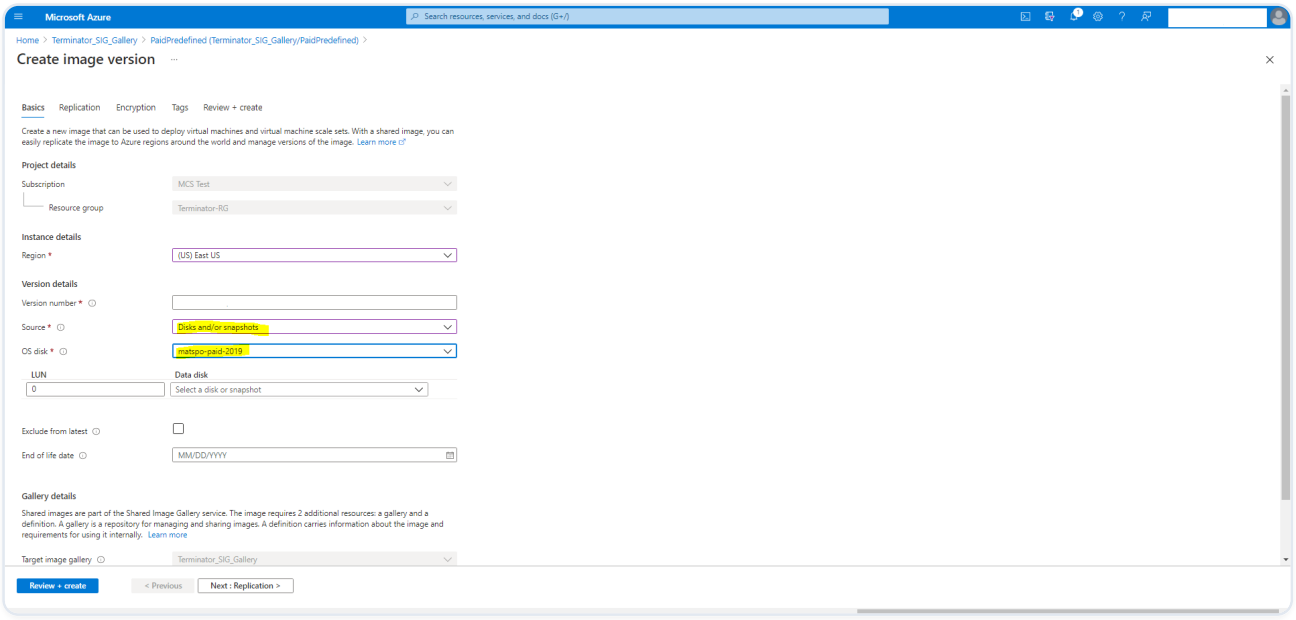
購入プラン情報フィールドは最初は空です。これらのフィールドに、イメージに使用された購入プラン情報を入力します。購入プラン情報を入力しないと、マシンカタログのプロセスが失敗する可能性があります。



購入プラン情報を確認した後、定義内にイメージバージョンを作成します。これはマスターイメージとして使用されます。**バージョンの追加**をクリックします。



バージョン詳細セクションで、イメージスナップショットまたはマネージドディスクをソースとして選択します。



オンデマンド容量予約VMのカタログを作成する

オンデマンド容量予約を使用すると、Azureリージョンまたは可用性ゾーンで任意の期間、コンピューティング容量を予約できます。Azureオンデマンド容量予約の詳細については、Microsoftドキュメント「オンデマンド容量予約」を参照してください。

マシンプロファイル（VMまたはテンプレート仕様）を使用して、オンデマンド容量予約付きのAzure VMのMCSマシンカタログを作成できます。また、既存のマシンカタログと既存のVMを更新して、オンデマンド容量予約を追加または削除することもできます。

この機能は、永続的および非永続的なマシンカタログに適用されます。

制限事項

この機能は以下には適用されません:

- スポットVM
- ホストグループ
- 休止状態が有効なVM

制限の詳細については、Microsoft ドキュメントの「制限事項」を参照してください。

オンデマンド容量予約VMのカタログを作成する手順

1. マシンプロファイルソース（VMまたはARMテンプレート仕様）を作成します。VMまたはARMテンプレート仕様の作成については、「VMを容量予約グループに関連付ける」を参照してください。

2. 次のPowerShellコマンドを実行して、マシンプロファイルでオンデマンド容量予約が有効になっているかどうかを確認します。マシンプロファイルでオンデマンド容量予約が有効になっている場合、`capacityReservationGroup id`が表示されます。

   例：

   マシンプロファイルソースがVMの場合、次のコマンドを実行します。

   ```
   (Get-Item "XDHyp:\HostingUnits\azure-res-
   conn2\machineprofile.folder\fifthcolumn.resourcegroup\demand-
   capacity.vm").AdditionalData
   ```

   マシンプロファイルソースがテンプレート仕様の場合、次のコマンドを実行します。

   ```
   (Get-Item "XDHyp:\HostingUnits\azure-res-
   conn2\machineprofile.folder\fifthcolumn.resourcegroup\fc-aeh-
   templatespec.templatespec\14.0.0-capacity-
   reservation.templatespecversion").AdditionalData
   ```

3. Web StudioまたはPowerShellコマンドを使用して、マシンプロファイルを使用してマシンカタログを作成します。

`Set-ProvScheme`コマンドを使用してカタログを更新できます。PowerShellコマンド`Set-ProvVmUpdateTimeWindow`を使用して既存のVMを更新することもできます。マシンプロファイルは次回の電源投入時に更新されます。

ネストされた仮想化

マスターVMでネストされた仮想化を有効にして構成した場合、そのマスターVMを使用して作成されたMCSマシンカタログ内のすべてのVMで、ネストされた仮想化が有効になります。この機能は、永続VMと非永続VMの両方に適用されます。イメージの更新を通じて、既存のMCSマシンカタログと既存のVMを更新して、ネストされた仮想化を有効にすることができます。

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

ネストされた仮想化の詳細については、Microsoft のブログ Nested Virtualization in Azure を参照してください。

NVMe のみ SKU

通常、汎用、メモリ最適化、コンピューティング最適化 VM の以前の世代 (D/Ev5 または Fv2 以前) は SCSI をサポートします。新しい世代 (Da/Ea/Fav6 以降) は通常、NVMe ストレージインターフェイスのみをサポートします。MCS は、Azure 上の新しい VM SKU をサポートするために、NVMe ストレージコントローラータイプをサポートしています。

NVMe の詳細については、Microsoft ドキュメント General FAQ for NVMe を参照してください。

次のサービスオファリングを使用して MCS カタログを作成できます。

- SCSI と NVMe の両方をサポートする、SCSI と NVMe の両方をサポートするサービスオファリングを使用したカタログの作成 を参照してください
- NVMe のみをサポートする、NVMe のみをサポートするサービスオファリングを使用したカタログの作成 を参照してください

制限事項

- NVMeをサポートするすべてのサービス提供は、同時にTrusted Launchをサポートしません。
- NVMe は Gen 1 VM ではサポートされていません。
- 一部の OS イメージは NVMe をサポートしない場合があります。その場合、Azure UI で NVMe オプションがグレー表示されます。

SCSI と NVMe の両方をサポートするサービスオファリングを使用してカタログを作成する

1. マスターイメージとして使用する VM を作成します。

    a. NVMe をサポートするマーケットプレイスイメージを使用します。NVMe をサポートする Azure Marketplace イメージのリストは、Supported OS images for remote NVMe で確認できます。

    b. VM の OS ディスクのスナップショットを取得して、`New-ProvScheme` コマンドの `MasterImageVM` パラメーターで使用するか、マネージドディスクを直接使用します。

    マスターイメージがNVMeをサポートしているかどうかを、以下のいずれかの方法で確認します。

    - `Get-Item` の `AdditionalData` フィールドにある `SupportedDiskControllerTypes` を確認します。例：

```
(get-item XDHyp:
\HostingUnits\mynetwork\image.folder\abc.resourcegroup\deg-
snapshot).AdditionalData
```

`SupportedDiskControllerTypes`は`SCSI, NVMe`である必要があります。

- Azure CLIとPowerShellを使用する

2. NVMeとSCSIの両方をサポートするサービスオファリングを使用します。
3. NVMeが有効になっているマシンプロファイルとしてVMまたはテンプレート仕様を使用します。`DiskControllerType`がNVMeに設定されている任意のVMを使用します。VMを直接マシンプロファイルとして使用するか、テンプレートをエクスポートしてテンプレート仕様をマシンプロファイルとして使用します。

NVMeのみをサポートするサービスオファリングを使用してカタログを作成する

1. マスターイメージとして使用するVMを作成します。NVMeをサポートするマーケットプレイスイメージを使用します。NVMeをサポートするAzure Marketplaceイメージのリストは、リモートNVMeでサポートされるOSイメージで確認できます。
2. NVMeのみをサポートするサービスオファリングを使用します。

> **注:**
>
> サービスオファリングがNVMeをサポートしているため、カタログでNVMeを有効にするために`NVMe`に設定された`DiskControllerType`を持つマシンプロファイルは必要ありません。ただし、マシンプロファイルを使用する場合は、`DiskControllerType`が`NVMe`に設定されているか、空白であるか、指定されていない必要があります。

既存の永続VMを変更する

NVMe構成は、VMが作成された後に変更することはできません。永続VMのNVMe構成を変更する方法は、VMを再デプロイすることです。これを行うロジックは次のとおりです。

1. VMの現在の状態を保存します。
2. 既存のVMの電源をオンにした後、VMが再デプロイを必要とするかどうかを検出します。
   a. 構成の変更がNVMeからNVMe、またはSCSIからSCSIの場合、VMの再展開は不要です。
   b. 構成の変更がSCSIからNVMe、またはその逆の場合、VMを再展開して再作成します。

PowerShellを使用してマシンカタログを作成する

このセクションでは、PowerShell を使用してカタログを作成する方法について詳しく説明します。

- 非永続的なライトバックキャッシュディスクを持つカタログを作成する
- 永続的なライトバックキャッシュディスクを持つカタログを作成する
- MCSIO で起動パフォーマンスを向上させる
- PowerShellを使用してカタログを作成または更新する際にテンプレート仕様を使用する
- 信頼できる起動を備えたマシンカタログ
- マシンプロファイルのプロパティ値を使用する
- 顧客管理の暗号化キーを使用してマシンカタログを作成する(#create-a-machine-catalog-with-customer-managed-encryption-key)
- 二重暗号化でマシンカタログを作成する
- Azure エフェメラルディスクを持つカタログを作成する
- Azure 専用ホスト
- Azure Compute Gallery イメージを使用してマシンカタログを作成または更新する
- Shared Image Gallery を構成する
- 指定された可用性ゾーンにマシンをプロビジョニングする
- ストレージの種類
- Azure Spot VMを使用してカタログを作成する(#create-a-catalog-using-azure-spot-vms)
- バックアップVMサイズを構成する
- すべてのリソースのタグをコピーする
- Azure Monitor Agentがインストールされたカタログ VMのプロビジョニング(#provision-catalog-vms-with-azure-monitor-agent-installed)

非永続的なライトバックキャッシュディスクを持つカタログの作成

非永続的なライトバックキャッシュディスクを持つカタログを構成するには、PowerShellパラメーター`New-ProvScheme CustomProperties`を使用します。カスタムプロパティ`UseTempDiskForWBC`は、ライトバックキャッシュファイルを保存するためにAzure一時ストレージを使用することを受け入れるかどうかを示します。一時ディスクをライトバックキャッシュディスクとして使用したい場合は、`New-ProvScheme`を実行する際にこれをtrueに構成する必要があ

ります。このプロパティが指定されていない場合、パラメーターはデフォルトで**False**に設定されます。

例えば、`CustomProperties`パラメーターを使用して`UseTempDiskForWBC`を**true**に設定する場合：

```
-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/XMLSchema-
instance"> `

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false"/> `

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false"/> `

<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS"/> `

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="Premium_LRS"/> `

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client"/> `

<Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value="true"/
> `

</CustomProperties>'
```

注:

ライトバックキャッシュファイルにAzureローカル一時ストレージを使用するようにマシンカタログをコミットした後、後でVHDを使用するように変更することはできません。

永続的なライトバックキャッシュディスクを持つカタログを作成する

永続的なライトバックキャッシュディスクを持つカタログを構成するには、PowerShellパラメーター`New-ProvScheme CustomProperties`を使用します。このパラメーターは、MCSプロビジョニングされたマシンに対してライトバックキャッシュディスクがどのように永続化するかを決定

するために使用される追加のプロパティ`PersistWBC`をサポートします。`PersistWBC`プロパティは、`UseWriteBackCache`パラメーターが指定され、`WriteBackCacheDiskSize`パラメーターがディスクが作成されることを示すように設定されている場合にのみ使用されます。

`PersistWBC`をサポートする前の`CustomProperties`パラメーターで見つかったプロパティの例は次のとおりです。

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

</CustomProperties>
```

これらのプロパティを使用する場合、`CustomProperties`パラメーターからプロパティが省略されていると、それらはデフォルト値を含むことに注意してください。`PersistWBC`プロパティには、**true**または**false**の2つの可能な値があります。

`PersistWBC`プロパティを**true**に設定すると、Citrix Virtual Apps and Desktops管理者がWeb Studioを使用してマシンをシャットダウンしても、ライトバックキャッシュディスクは削除されません。

`PersistWBC`プロパティを**false**に設定すると、Citrix Virtual Apps and Desktops管理者がWeb Studioを使用してマシンをシャットダウンしたときに、ライトバックキャッシュディスクが削除されます。

注:

`PersistWBC`プロパティが省略された場合、プロパティはデフォルトで**false**になり、Web Studioを使用してマシンがシャットダウンされるとライトバックキャッシュは削除されます。

例えば、`CustomProperties`パラメーターを使用して`PersistWBC`をtrueに設定する場合：

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />

</CustomProperties>
```

重要:

`PersistWBC`プロパティは、`New-ProvScheme` PowerShellコマンドレットを使用してのみ設定できます。作成後にプロビジョニングスキームの`CustomProperties`を変更しようとしても、マシンカタログや、マシンがシャットダウンされたときのライトバックキャッシュディスクの永続性には影響しません。

例えば、`New-ProvScheme`をライトバックキャッシュを使用するように設定し、同時に`PersistWBC`プロパティをtrueに設定する場合：

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
```

```
Name=`"PersistWBC`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

MCSIOで起動パフォーマンスを向上させる

MCSIOが有効になっている場合、AzureおよびGCPマネージドディスクの起動パフォーマンスを向上させることができます。この機能を構成するには、`New-ProvScheme` コマンドでPowerShell `PersistOSDisk` カスタムプロパティを使用します。`New-ProvScheme` に関連するオプションは次のとおりです。

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="Resource ``````<!--NeedCopy-->
```

```
````````Groups" Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

</CustomProperties>
```

この機能を有効にするには、`PersistOSDisk`カスタムプロパティを`true`に設定します。例：

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127
```
```

```
-WriteBackCacheMemorySize 256
```

PowerShell を使用してカタログを作成または更新する際にテンプレート仕様を使用する

テンプレート仕様をマシンプロファイルの入力として使用して、MCSマシンカタログを作成または更新できます。これを行うには、Web StudioまたはPowerShellコマンドを使用できます。

Web Studioについては、「Web StudioでAzure Resource Managerイメージを使用してマシンカタログを作成する」を参照してください。(#create-a-machine-catalog-using-an-azure-resource-manager-image-in-web-studio)

PowerShell コマンドを使用する手順:

1. **PowerShell** ウィンドウを開きます。
2. `asnp citrix*` を実行します。
3. カタログを作成または更新します。
    - カタログを作成するには:
        a. テンプレート仕様をマシンプロファイルの入力として使用して、`New-ProvScheme` コマンドを使用します。例:

```
New-ProvScheme -MasterImageVM "XDHyp:/HostingUnits/azure/
image.folder/fgthj.resourcegroup/nab-ws-
vda_OsDisk_1_xxxxxxxxxxa.manageddisk"

MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.folder/
fgthj.resourcegroup/test.templatespec/V1.templatespecversion"

-ProvisioningSchemeName <String>

-HostingUnitName <String>

-IdentityPoolName <String>

[-ServiceOffering <String>][-CustomProperties <String>

[-LoggingId <Guid>]

[-BearerToken <String>][-AdminAddress <String>]
```

```
[<CommonParameters>]
```

b. カタログの作成を完了します。

- カタログを更新するには、テンプレート仕様をマシンプロファイルの入力として使用して、`Set-ProvScheme`コマンドを使用します。例:

```
Set-ProvScheme -MasterImageVm 'XDHyp://Connections/Azure/East
Us.region/vm.folder/MasterDisk.vm'

MachineProfile 'XDHyp:/HostingUnits/azure/machineprofile.folder/
fgthj.resourcegroup/testing.templatespec/V1.templatespecversion'

[-ProvisioningSchemeName] <String>

[-CustomProperties <String>][-ServiceOffering <String>] [-PassThru]

[-LoggingId <Guid>] [-BearerToken <String>][-AdminAddress <String>]
[<CommonParameters>]
```

トラステッド起動によるマシンカタログ

トラステッド起動でマシンカタログを正常に作成するには、以下を使用します。

- トラステッド起動が有効なマスターイメージ。マシンプロファイルを使用する必要がありますが、マシンプロファイルがトラステッド起動を有効にする必要はありません。トラステッド起動が有効なマスターイメージと、トラステッド起動が有効でないマシンプロファイルを使用すると、マスターイメージとマシンプロファイル間のトラステッド起動構成の不一致により、警告メッセージが表示されます。
- Trusted Launchをサポートするvmサイズ
- トラステッド起動をサポートするWindows VMバージョン。現在、Windows 10、Windows 11、Windows Server 2016、2019、および2022がトラステッド起動をサポートしています。

Citrix Virtual Apps and Desktopsの提供インベントリアイテムを表示し、VMサイズがTrusted Launchをサポートしているかどうかを判断するには、次のコマンドを実行します。

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、**asnp citrix***を実行します。
3. 次のコマンドを実行します。

```
$s = (ls XDHyp:\HostingUnits\<name of hosting
unit>\serviceoffering.folder\"<VM size>.serviceoffering)
```

4. `$s | select -ExpandProperty Additionaldata` を実行します。
5. `SupportsTrustedLaunch` 属性の値を確認します。
    - `SupportsTrustedLaunch` が **True** の場合、VM サイズは Trusted Launch をサポートしています。
    - `SupportsTrustedLaunch` が **False** の場合、VM サイズは Trusted Launch をサポートしていません。

Azure の PowerShell に従って、Trusted Launch をサポートする VM サイズを判別するには、次のコマンドを使用できます。

```
(Get-AzComputeResourceSku | where {$_.Locations.Contains($region) -and
($_.Name -eq "<VM size>") })[0].Capabilities
```

Azure PowerShellコマンドを実行した後、VMサイズがTrusted Launchをサポートしているかどうかを説明する例を次に示します。

- *例 1*: Azure VM が Generation 1 のみをサポートしている場合、その VM は Trusted Launch をサポートしていません。したがって、Azure PowerShell コマンドを実行しても `TrustedLaunchDisabled` 機能は表示されません。
- *例 2*: Azure VM が Generation 2 のみをサポートし、`TrustedLaunchDisabled` 機能が **True** の場合、Generation 2 VM サイズは Trusted Launch でサポートされていません。
- *例 3*: Azure VM が Generation 2 のみをサポートし、PowerShell コマンドを実行しても `TrustedLaunchDisabled` 機能が表示されない場合、Generation 2 VM サイズは Trusted Launch でサポートされています。

Azure仮想マシンのTrusted Launchの詳細については、Microsoftドキュメント「Azure仮想マシンのTrusted Launch」を参照してください。

Trusted Launch を使用してマシンカタログを作成する

1. Trusted Launchが有効なマスターイメージを作成します。Microsoftドキュメント「Trusted Launch VM Images」を参照してください。

2. セキュリティの種類を **trusted launch virtual machines** として VM またはテンプレート仕様を作成します。VM またはテンプレート仕様の作成の詳細については、Microsoft ドキュメント「Deploy a trusted launch VM」を参照してください。
3. Web StudioまたはPowerShellコマンドを使用してマシンカタログを作成します。

   - Web Studioを使用する場合は、「Web StudioでAzure Resource Managerイメージを使用してマシンカタログを作成する」を参照してください。
   - PowerShellコマンドを使用する場合は、VMまたはテンプレート仕様をマシンプロファイルの入力として`New-ProvScheme`コマンドを使用します。カタログを作成するためのコマンドの完全なリストについては、「カタログの作成」を参照してください。

     VMをマシンプロファイルの入力とする`New-ProvScheme`の例:

     ```
     New-ProvScheme -CleanOnBoot -HostingUnitName "name"
     -IdentityPoolName "name" -InitialBatchSizeHint 1

     -MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/
     fgthj.resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"

     -MachineProfile "XDHyp:
     \HostingUnits\<adnet>\machineprofile.folder\<def.resourcegroup>\<mac
     hine profile vm.vm>"

     -ProvisioningSchemeName <String>

     -HostingUnitName <String>

     -IdentityPoolName <String>

     [-ServiceOffering <String>][-CustomProperties <String>]

     [<CommonParameters>]
     ```

     テンプレート仕様をマシンプロファイルの入力とする`New-ProvScheme`の例:

     ```
     New-ProvScheme -CleanOnBoot -HostingUnitName "name"
     -IdentityPoolName "name" -InitialBatchSizeHint 1

     -MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/
     fgthj.resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
     ```

```
MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.folder/
fgthj.resourcegroup/test.templatespec/V1.templatespecversion"

-ProvisioningSchemeName <String>

-HostingUnitName <String>

-IdentityPoolName <String>

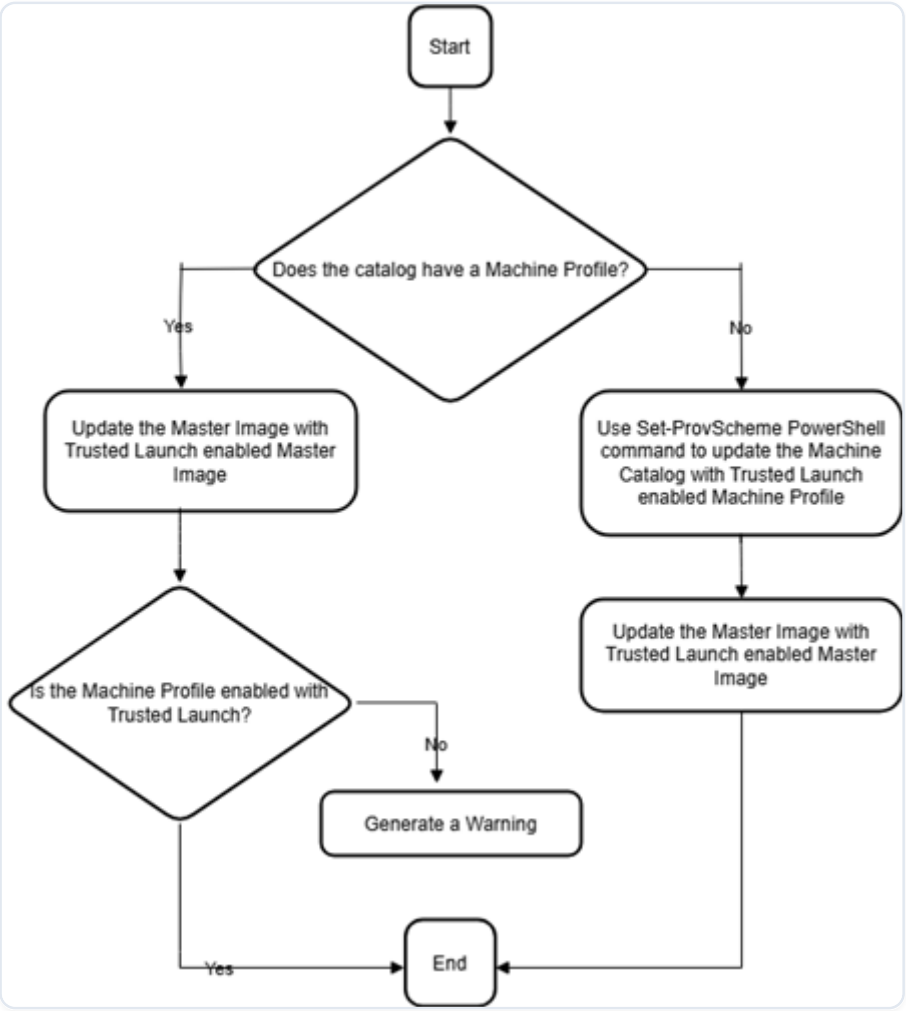
[-ServiceOffering <String>][-CustomProperties <String>]

[<CommonParameters>]
```

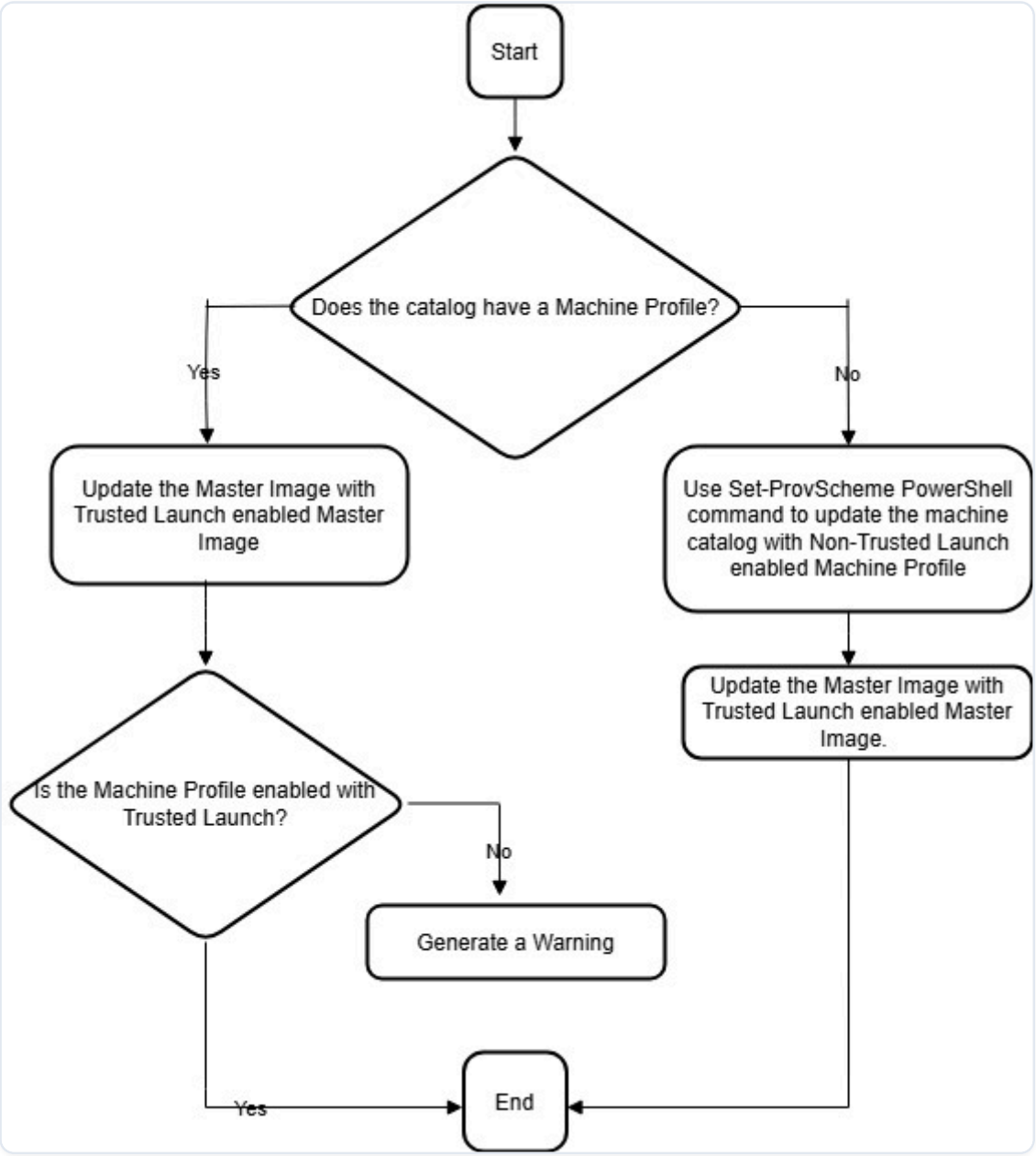
トラステッド起動でマシンカタログを更新する

永続および非永続の両方のマシンカタログを更新できます。

永続マシンカタログの場合:



非永続マシンカタログの場合:



トラステッド起動でマシンカタログを作成する際のエラー

トラステッド起動でマシンカタログを作成する際に、以下のシナリオで適切なエラーが発生します。

シナリオ	エラー
アンマネージドカタログの作成中にマシンプロファイルを選択した場合	`MachineProfileNotSupportedForUnmanagedCatalog`
セキュリティの種類としてTrusted Launchを持つマスターイメージソースを使用して管理カタログを作成する際に、マシンプロファイルを選択しない場合	`MachineProfileNotFoundForTrustedLaunchMasterImage`

シナリオ	エラー
マスターイメージのセキュリティの種類と異なるセキュリティの種類を持つマシンプロファイルを選択した場合	`SecurityTypeConflictBetweenMasterImageAndMachineProfile`
カタログの作成時に、Trusted Launchをサポートしないマシンサイズを選択し、かつTrusted Launchをサポートするマスターイメージを使用した場合	`MachineSizeNotSupportTrustedLaunch`

マシンプロファイルプロパティ値の使用

マシンカタログは、カスタムプロパティで定義されている次のプロパティを使用します。

- アベイラビリティゾーン
- 専用ホストグループID
- ディスク暗号化セットID
- OSの種類
- ライセンスの種類
- ストレージの種類

これらのカスタムプロパティが明示的に定義されていない場合、プロパティ値は、マシンプロファイルとして使用されるARMテンプレート仕様またはVMから設定されます。さらに、`ServiceOffering`が指定されていない場合、マシンプロファイルから設定されます。

> **注:**
>
> マシンプロファイルに一部のプロパティが欠落しており、カスタムプロパティで定義されていない場合、該当する場合、プロパティのデフォルト値が適用されます。

> 次のセクションでは、`New-ProvScheme`と`Set-ProvScheme`におけるいくつかのシナリオについて説明します。この場合、`CustomProperties`はすべてのプロパティを定義しているか、値がMachineProfileから派生しています。

- New-ProvSchemeのシナリオ

- MachineProfileにすべてのプロパティがあり、CustomPropertiesが定義されていない場合。
  例:

  `New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm"`

  カタログのカスタムプロパティとして、次の値が設定されます:

  ```
  Get-ProvScheme | select CustomProperties

  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
  machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
  instance">

  <Property xsi:type="StringProperty" Name="StorageAccountType"
  Value="<mpA-value>"/>

  <Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
  value>"/>

  <Property xsi:type="StringProperty" Name="LicenseType" Value="<mpA-
  value>"/>

  <Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
  Value="<mpA-value>"/>

  <Property xsi:type="StringProperty" Name="DedicatedHostGroupId"
  Value="<mpA-value>"/>

  <Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
  value>"/>

  </CustomProperties>
  ```

- MachineProfileに一部のプロパティがあり、CustomPropertiesが定義されていない場合。
  例: MachineProfileにはLicenseTypeとOsTypeのみがあります。

  `New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm"`

  カタログのカスタムプロパティとして、次の値が設定されます:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mpA-
value>"/>

</CustomProperties>
```

- MachineProfileとCustomPropertiesの両方がすべてのプロパティを定義している場合。例:

  `New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -CustomProperties $CustomPropertiesA`

  カスタムプロパティが優先されます。カタログのカスタムプロパティとして、次の値が設定されます。

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="OSType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="DedicatedHostGroupId"
```

```
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="Zones"
Value="<CustomPropertiesA-value>"/>

</CustomProperties>
```

- MachineProfileで一部のプロパティが定義され、CustomPropertiesで一部のプロパティが定義されている場合。例:
  - CustomProperties は LicenseType と StorageAccountType を定義します
  - MachineProfile は LicenseType、OsType、および Zones を定義します

`New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -CustomProperties $CustomPropertiesA`

カタログのカスタムプロパティとして、次の値が設定されます:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
value>"/>

<Property xsi:type="StringProperty" Name="LicenseType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
value>"/>

</CustomProperties>
```

- 一部のプロパティは MachineProfile で定義され、一部のプロパティは CustomProperties で定義されています。さらに、ServiceOffering は定義されていません。例:

- CustomProperties は StorageType を定義します
- MachineProfile は LicenseType を定義します

```
New-ProvScheme -MachineProfile "XDHyp:
\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mp
.vm"

-ServiceOffering "XDHyp:
\HostingUnits\azureunit\serviceoffering.folder\<explicit-machine-
size>.serviceoffering"
```

カタログのカスタムプロパティとして、次の値が設定されます:

```
Get-ProvScheme | select ServiceOffering

serviceoffering.folder\<explicit-machine-size>.serviceoffering



Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="explicit-storage-type"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="value-
from-machineprofile"/>

</CustomProperties>
```

- OsType が CustomProperties にも MachineProfile にも含まれていない場合、次のようになります:
  - 値はマスターイメージから読み取られます。
  - マスターイメージがアンマネージドディスクの場合、OsType は Windows に設定されます。例:

`New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -MasterImageVM "XDHyp:\HostingUnits\azureunit\image.folder\linux-master-image.manageddisk"`

マスターイメージからの値は、この場合 Linux のカスタムプロパティに書き込まれます。

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="OSType" Value="Linux"/>

</CustomProperties>
```

- Set-ProvScheme シナリオ
  - 既存のカタログ (以下を含む):
    - カスタムプロパティ（`StorageAccountType`およびOsType）
    - ゾーンを定義する MachineProfile `mpA.vm`
  - 更新:
    - StorageAccountType を定義する MachineProfile mpB.vm
    - LicenseType と OsType を定義する新しいカスタムプロパティセット $CustomPropertiesB

`Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpB.vm" -CustomProperties $CustomPropertiesB`

カタログのカスタムプロパティとして、次の値が設定されます:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
```

```
<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<mpB-value>"/>

<Property xsi:type="StringProperty" Name="OSType"
Value="<CustomPropertiesB-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType"
Value="<CustomPropertiesB-value>"/>

    </CustomProperties>
```

- 既存のカタログ (以下を含む):
  - S`torageAccountType` および OsType の CustomProperties
  - StorageAccountType と LicenseType を定義する MachineProfile `mpA.vm`
- 更新:
  - StorageAccountType と OsType を定義する新しいカスタムプロパティセット $CustomPropertiesB。

`Set-ProvScheme -CustomProperties $CustomPropertiesB`

カタログのカスタムプロパティとして、次の値が設定されます:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesB-value>"/>

<Property xsi:type="StringProperty" Name="OSType"
Value="<CustomPropertiesB-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mp-A-
value>"/>

</CustomProperties>
```

- 既存のカタログ (以下を含む):
  - カスタムプロパティ（`StorageAccountType`およびOsType）
  - ゾーンを定義するMachineProfile `mpA.vm`
- 更新:
  - StorageAccountType と LicenseType を定義する MachineProfile mpB.vm
  - `ServiceOffering`は指定されていません

`Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpB.vm"`

カタログのカスタムプロパティとして、次の値が設定されます:

```
Get-ProvScheme | select ServiceOffering

serviceoffering.folder\<value-from-machineprofile>.serviceoffering



Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<mpB-value>"/>

<Property xsi:type="StringProperty" Name="OSType" Value="<prior-
CustomProperties-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mpB-
value>"/>

</CustomProperties>
```

VMごとに複数のNICを持つカタログを作成または更新する

MCSはVMごとに複数のNICをサポートしています。VM上の複数のNICを複数のサブネットに関連付けることができますが、それらのサブネットは同じ仮想ネットワーク（VNet）内にある必要があります。PowerShellコマンドを使用して、次のことができます。

- VM上に複数のNICを持つカタログを作成する(#create-a-catalog-with-multiple-nics-on-a-vm)
- 既存のカタログ構成を更新して、VM上に複数のNICを持たせ、新しく作成されるVMが複数のNICを持つようにする(#update-a-catalog-to-have-multiple-nics-on-a-vm)
- 既存のVMを更新して、複数のNICを持つようにする(#update-an-existing-vm-to-have-multiple-nics-on-a-vm)

マシンプロファイルに基づかないマシンカタログと、マシンプロファイルに基づくマシンカタログを作成または更新して、VM上に複数のNICを持たせることができます。現在、マシンプロファイルに基づくマシンカタログの場合、マシンプロファイルソースで指定されたNICの数と同じ数しか持つことができません。

アクセラレーテッドネットワーキングなどのプロパティは、マシンプロファイルソースから派生します。

> **注:**
>
> VMサイズは、同じ数のNICと対応するアクセラレーテッドネットワーキングをサポートしている必要があります。そうでない場合、エラーが発生します。

> 選択したVMサイズに関連付けられているNICの最大数を取得できます。`AdditionalData` パラメーターを指定してPowerShell `get-item` コマンドを実行すると、`MaxNetworkInterfaces` というPowerShellプロパティにNICの最大数が表示されます。

NICの最大数を取得する

NICの最大数を取得するには：

1. Delivery Controller™ホストから**PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*` を実行します。
3. 利用可能なすべてのVMサイズを一覧表示するには、`Get-ChildItem -Path "XDHyp:\Connections\abc-connection\East US.region\serviceoffering.folder"` を実行します。

4. `get-item -Path "XDHyp:\Connections\abc-connection\East US.region\serviceoffering.folder\Standard_M416ms_v2.serviceoffering").AdditionalData` を実行します。
5. NICの最大数を確認するには、`MaxNetworkInterfaces` をチェックします。

VM上に複数のNICを持つカタログを作成する

VM上に複数のNICを持つカタログを作成するには、次の手順を実行します。

1. Delivery ControllerホストからPowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*` を実行します。
3. まだ作成されていない場合は、IDプールを作成します。
4. プロビジョニングスキームを作成します。

   - マシンプロファイルに基づかないマシンカタログを作成する場合は、`NetworkMappings` パラメーターを指定して `New-ProvScheme` コマンドを実行します。`NetworkMappings` パラメーターに複数のサブネットを追加できます。例：

     ```
     New-Provscheme -NetworkMappings
     @{"0"="subnetpath1";"1"="subnetpath1"}
     ```

   - マシンプロファイルに基づいたマシンカタログを作成する場合：

     a. 複数のNICを持つVMをAzureに作成します。詳細については、「複数のNICを持つWindows仮想マシンの作成と管理」を参照してください。新しいVMを作成し、Azureポータルの「ネットワーク」ページでネットワークインターフェイスをアタッチすることもできます。

     b. VMをマシンプロファイルの入力として、`New-ProvScheme` コマンドを実行します。

     注:

     マシンプロファイルに基づいたマシンカタログを作成する場合、`NetworkMappings` の数はマシンプロファイルの `NetworkInterfaceCount` と同じである必要があります。`NetworkInterfaceCount` は、`Get-item -Path "machine profile path"` の `AdditionalData` から取得できます。

5. カタログの作成を完了します。

VM上に複数のNICを持つようにカタログを更新する

VM上に複数のNICを持つようにカタログを更新するには、次の手順を実行します。

1. Delivery ControllerホストからPowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*`を実行します。
3. プロビジョニングスキームを更新します。

   - マシンプロファイルに基づかないマシンカタログを作成する場合は、`NetworkMappings`パラメーターを指定して`Set-ProvScheme`コマンドを実行します。パラメーター`NetworkMappings`に複数のサブネットを追加できます。例：

     ```
     Set-Provscheme -NetworkMappings
     @{"0"="subnetpath1";"1"="subnetpath1"}
     ```

   - マシンプロファイルに基づいてマシンカタログを作成する場合：

     a. 複数のNICを持つVMをAzureに作成します。詳しくは、「複数のNICを持つWindows仮想マシンの作成と管理」を参照してください。

     b. VMをマシンプロファイルの入力として使用して、`Set-ProvScheme`コマンドを実行します。

既存のVMを更新して、VMに複数のNICを持たせる

`Set-ProvVMUpdateTimeWindow`を使用して既存のVMを更新したり、更新時間枠中に既存のVMでパワーサイクルを実行したりすることもできます。

Azure Monitor Agentがインストールされたカタログ VMをプロビジョニングする

Azure監視は、Azureおよびオンプレミス環境からのテレメトリデータを収集、分析し、それに基づいて行動するために使用できるサービスです。

Azure Monitor Agent (AMA) は、仮想マシンなどのコンピューティングリソースから監視データを収集し、そのデータを Azure Monitor に配信します。現在、イベントログ、Syslog、パフォーマンスメトリックの収集をサポートしており、Azure Monitor Metrics および Azure Monitor Logs データソースに送信します。

監視データ内のVMを一意に識別して監視を有効にするには、AMAを拡張機能としてインストールしたMCSマシンカタログのVMをプロビジョニングできます。

要件

- 権限: 必要な Azure 権限 で指定されている最小限の Azure 権限と、Azure Monitor を使用するための以下の権限があることを確認してください。
  - `Microsoft.Compute/virtualMachines/extensions/read`
  - `Microsoft.Compute/virtualMachines/extensions/write`
  - `Microsoft.Insights/DataCollectionRuleAssociations/Read`
  - `Microsoft.Insights/dataCollectionRuleAssociations/write`
  - `Microsoft.Insights/DataCollectionRules/Read`
- データ収集ルール: Azure portal でデータ収集ルールを設定します。DCR の設定については、データ収集ルールの作成 を参照してください。DCR はプラットフォーム固有 (Windows または Linux) です。必要なプラットフォームに応じて DCR を作成してください。 AMA はデータ収集ルール (DCR) を使用して、VM などのリソースと、Azure Monitor Metrics や Azure Monitor Logs などのデータソース間のマッピングを管理します。
- 既定のワークスペース: Azure portal でワークスペースを作成します。ワークスペースの作成については、Log Analytics ワークスペースの作成 を参照してください。ログとデータを収集すると、その情報はワークスペースに保存されます。ワークスペースには一意のワークスペース ID とリソース ID があります。ワークスペース名は、特定のリソースグループに対して一意である必要があります。ワークスペースを作成したら、データソースとソリューションを設定して、そのデータをワークスペースに保存します。
- 監視拡張機能をホワイトリストに登録: 拡張機能 `AzureMonitorWindowsAgent` および `AzureMonitorLinuxAgent` は、Citrix が定義したホワイトリスト登録済みの拡張機能です。ホワイトリスト登録済みの拡張機能のリストを表示するには、PoSH コマンド `Get-ProvMetadataConfiguration` を使用します。
- マスターイメージ: Microsoft は、既存のマシンから新しいマシンを作成する前に、そのマシンから拡張機能を削除することを推奨しています。拡張機能が削除されていない場合、残存ファイルや予期しない動作につながる可能性があります。詳細については、「既存の VM から VM を再作成する場合」を参照してください。

AMA を有効にしてカタログ VM をプロビジョニングするには:

1. マシンプロファイルテンプレートを設定します。
   - VMをマシンプロファイルテンプレートとして使用する場合：
     a. Azure portal で VM を作成します。

b. VMの電源を入れます。

c. **リソース**の下のデータ収集ルールにVMを追加します。これにより、テンプレートVMにエージェントのインストールが呼び出されます。

> **注:**
>
> Linuxカタログを作成する必要がある場合は、Linuxマシンを設定します。

- テンプレート仕様をマシンプロファイルテンプレートとして使用する場合：

a. テンプレート仕様を設定します。

b. 生成されたテンプレート仕様に、次の拡張機能とデータ収集ルール関連付けを追加します。

```
{

"type": "Microsoft.Compute/virtualMachines/extensions",

"apiVersion": "2022-03-01",

"name": "<vm-name>/AzureMonitorWindowsAgent",

"dependsOn": [

    "Microsoft.Compute/virtualMachines/<vm-name>"

],

"location": "<azure-region>",

"properties": {

    "publisher": "Microsoft.Azure.Monitor",

    "type": "AzureMonitorWindowsAgent",

    "typeHandlerVersion": "1.0",

    "autoUpgradeMinorVersion": true,
```

```
    "enableAutomaticUpgrade": true

}

},

 {

    "type": "Microsoft.Insights/dataCollectionRuleAssociations",

    "apiVersion": "2021-11-01",

    "name": "<associatio-name>",

    "scope": "Microsoft.Compute/virtualMachines/<vm-name>",

    "dependsOn": [

     "Microsoft.Compute/virtualMachines/<vm-name>",

    "Microsoft.Compute/virtualMachines/<vm-name>/extensions/
AzureMonitorWindowsAgent"

    ],

    "properties": {

       "description": "Association of data collection rule.
Deleting this association will break the data collection for this
Arc server.",

     "dataCollectionRuleId": "/subscriptions/<azure-
subscription>/resourcegroups/<azure-resource-group>/providers/
microsoft.insights/datacollectionrules/<azure-data-collection-
rule>"

     }

    }
```

2. 既存のMCSマシンカタログを作成または更新します。

- 新しいMCSカタログを作成するには:

  a. Web Studio で、その VM またはテンプレート仕様をマシンプロファイルとして選択します。

  b. カタログを作成するための次の手順に進みます。

- 既存の MCS カタログを更新するには、次の PoSH コマンドを使用します。

  - 新しい VM に更新されたマシンプロファイルテンプレートを取得させるには、次のコマンドを実行します。

    ```
    Set-ProvScheme -ProvisioningSchemeName "name"

    -MachineProfile "XDHyp:
    \HostingUnits\Unit1\machineprofile.folder\abc.resourcegroup\ab-
    machine-profile.vm"
    ```

  - 既存の VM を更新されたマシンプロファイルテンプレートで更新するには：

    ```
    Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -StartsNow -DurationInMinutes -1
    ```

3. カタログVMの電源を入れます。
4. Azure portal に移動し、モニター拡張機能が VM にインストールされていること、および VM が DCR のリソースの下に表示されていることを確認します。数分後、監視データが Azure Monitor に表示されます。

トラブルシューティング

Azure Monitor Agentのトラブルシューティングガイダンスについては、以下を参照してください。

- https://learn.microsoft.com/ja-jp/azure/azure-monitor/agents/azure-monitor-agent-troubleshoot-windows-vm/
- https://learn.microsoft.com/ja-jp/azure/azure-resource-manager/troubleshooting/create-troubleshooting-template/

顧客管理の暗号化キーでマシンカタログを作成する

顧客管理の暗号化キーを使用してマシンカタログを作成する詳細な手順は次のとおりです。

1. PowerShellウィンドウを開きます。

2. Citrix固有のPowerShellモジュールをロードするために `asnp citrix*` を実行します。
3. `cd xdhyp:/` を入力します。
4. `cd .\HostingUnits\(your hosting unit)` を入力します。
5. `cd diskencryptionset.folder` を入力します。
6. ディスク暗号化セットのリストを取得するには、`dir` を入力します。
7. ディスク暗号化セットのIDをコピーします。
8. ディスク暗号化セットのIDを含めるカスタムプロパティ文字列を作成します。例：

```
$customProperties = "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
Value=`"Standard_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"persistWBC`"
Value=`"False`" />

<Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`"
Value=`"false`" />

<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" />

<Property xsi:type=`"StringProperty`" Name=`"DiskEncryptionSetId`"
Value=`"/subscriptions/0xxx4xxx-xxb-4bxx-xxxx-xxxxxxxx/resourceGroups/
abc/providers/Microsoft.Compute/diskEncryptionSets/abc-des`"/>

</CustomProperties>
```

9. まだ作成されていない場合は、IDプールを作成します。例：

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms##
-Domain def.local -NamingSchemeType Numeric
```

10. New-ProvSchemeコマンドを実行します。例：

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name" -IdentityPoolName
"name" -InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\azure-
res2\image.folder\def.resourcegroup\def.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\azure-res2\
\virtualprivatecloud.folder\def.resourcegroup\def-
vnet.virtualprivatecloud\subnet1.network"}

-ProvisioningSchemeName "name"

-ServiceOffering "XDHyp:\HostingUnits\azure-
res2\serviceoffering.folder\Standard_DS2_v2.serviceoffering"

-MachineProfile "XDHyp:
\HostingUnits\<adnet>\machineprofile.folder\<def.resourcegroup>\<machin
e profile vm.vm>"

-CustomProperties $customProperties
```

11. マシンカタログの作成を完了します。

二重暗号化でマシンカタログを作成する

Web Studio および PowerShell コマンドを使用して、二重暗号化されたマシンカタログを作成および更新できます。

二重暗号化でマシンカタログを作成する詳細な手順は次のとおりです。

1. プラットフォーム管理キーと顧客管理キーを使用して、Azure Key Vault と DES を作成します。Azure Key Vault と DES の作成方法については、「Azure portal を使用してマネージドディスクの保存時の二重暗号化を有効にする」を参照してください。
2. ホスティング接続で利用可能な DiskEncryptionSets を参照するには：
    a. **PowerShell** ウィンドウを開きます。
    b. 次の PowerShell コマンドを実行します。
        i. `asnp citrix*`
        ii. `cd xdhyp:`:
        iii. `cd HostingUnits`

iv. `cd YourHostingUnitName`（例えば、azure-east）

v. `cd diskencryptionset.folder`

vi. `dir`

`DiskEncryptionSet`のIDを使用して、カスタムプロパティでカタログを作成または更新できます。

3. マシンプロファイルワークフローを使用する場合は、VMまたはテンプレート仕様をマシンプロファイルの入力として作成します。

   - VMをマシンプロファイルの入力として使用する場合は、:

     a. Azure PortalでVMを作成します。

     b. **ディスク>キー管理**に移動して、任意の`DiskEncryptionSetID`でVMを直接暗号化します。

   - テンプレート仕様をマシンプロファイルの入力として使用する場合は、:

     a. テンプレートで、`properties>storageProfile>osDisk>managedDisk`の下に`diskEncryptionSet`パラメーターを追加し、二重暗号化DESのIDを追加します。

4. マシンカタログを作成します。

   - Web Studio を使用している場合は、マシンカタログの作成 の手順に加えて、次のいずれかを実行します。

     ◦ マシンプロファイルベースのワークフローを使用しない場合は、 ページで、 を選択します。次に、ドロップダウンメニューから二重暗号化DESを選択します。カタログの作成を続行します。

     ◦ マシンプロファイルワークフローを使用している場合は、 ページでマスターイメージとマシンプロファイルを選択します。マシンプロファイルのプロパティにディスク暗号化セット ID があることを確認します。

     カタログで作成されたすべてのマシンは、選択した DES に関連付けられたキーによって二重に暗号化されます。

   - PowerShellコマンドを使用する場合は、次のいずれかを実行します。

     ◦ マシンプロファイルベースのワークフローを使用しない場合は、`New-ProvScheme`コマンドにカスタムプロパティ`DiskEncryptionSetId`を追加します。例:

```
New-ProvScheme -CleanOnBoot -CustomProperties '<CustomProperties
xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="/subscriptions/12345678-xxxx-1234-1234-123456789012/
resourceGroups/Sample-RG/providers/Microsoft.Compute/
diskEncryptionSets/SampleEncryptionSet" />

</CustomProperties>'

-HostingUnitName "Redacted"

-IdentityPoolName "Redacted"

-InitialBatchSizeHint 1

-MasterImageVM "Redacted"

-NetworkMapping @{"0"="Redacted"}

-ProvisioningSchemeName "Redacted"

-ServiceOffering "Redacted"
```

- マシンプロファイルベースのワークフローを使用する場合は、`New-ProvScheme`コマンドでマシンプロファイル入力を利用します。例:

```
New-ProvScheme -CleanOnBoot

-HostingUnitName azure-east

-IdentityPoolName aio-ip

-InitialBatchSizeHint 1
```

```
-MasterImageVM XDHyp:\HostingUnits\azure-
east\image.folder\abc.resourcegroup\fgb-vda-snapshot.snapshot

-NetworkMapping @{"0"="XDHyp:\HostingUnits\azure-
east\virtualprivatecloud.folder\apa-
resourceGroup.resourcegroup\apa-resourceGroup-
vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName aio-test

-MachineProfile XDHyp:\HostingUnits\azure-
east\machineprofile.folder\abc.resourcegroup\abx-
mp.templatespec\1.0.0.templatespecversion
```

5. リモートPowerShell SDKを使用してカタログの作成を完了します。リモートPowerShell SDKを使用してカタログを作成する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/を参照してください。カタログで作成されたすべてのマシンは、選択したDESに関連付けられたキーによって二重に暗号化されます。

暗号化されていないカタログを二重暗号化を使用するように変換する

マシンカタログの暗号化タイプ（カスタムプロパティまたはマシンプロファイルを使用）を更新できます。

- マシンプロファイルベースのワークフローを使用しない場合は、`Set-ProvScheme`コマンドにカスタムプロパティDiskEncryptionSetIdを追加します。例:

```
Set-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"

-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/12345678-xxxx-1234-1234-123456789012/resourceGroups/
Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/
SampleEncryptionSet" />

</CustomProperties>'
```

- マシンプロファイルベースのワークフローを使用する場合は、`Set-ProvScheme`コマンドでマシンプロファイル入力を利用します。例:

```
Set-ProvScheme -ProvisioningSchemeName mxiao-test -MachineProfile
XDHyp:\HostingUnits\azure-
east\machineprofile.folder\aelx.resourcegroup\elx-
mp.templatespec\1.0.0.templatespecversion
```

成功すると、カタログに追加するすべての新しいVMは、選択したDESに関連付けられたキーによって二重暗号化されます。

カタログが二重暗号化されていることを確認する

- ウェブスタジオで:

  a. **マシンカタログ**に移動します。

  b. 確認するカタログを選択します。画面下部にある**テンプレートプロパティ**タブをクリックします。

  c. **Azureの詳細**の下で、**ディスク暗号化セット**のディスク暗号化セットIDを確認します。カタログのDES IDが空白の場合、カタログは暗号化されていません。

  d. Azure Portal で、DES ID に関連付けられている DES の暗号化の種類がプラットフォーム管理キーと顧客管理キーであることを確認します。

- PowerShellコマンドを使用する:

  a. **PowerShell** ウィンドウを開きます。

  b. `asnp citrix*` を実行して、Citrix 固有の PowerShell モジュールをロードします。

  c. `Get-ProvScheme` を使用して、マシンカタログの情報を取得します。例:

```
Get-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
```

  d. マシンカタログの DES ID カスタムプロパティを取得します。例:

```
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="/subscriptions/12345678-1234-1234-1234-123456789012/
resourceGroups/Sample-RG/providers/Microsoft.Compute/
diskEncryptionSets/SampleEncryptionSet" />
```

e. Azure Portal で、DES ID に関連付けられている DES の暗号化の種類がプラットフォーム管理キーと顧客管理キーであることを確認します。

Azureエフェメラルディスクを使用してカタログを作成する

エフェメラルディスクを使用するには、`New-ProvScheme` の実行時にカスタムプロパティ `UseEphemeralOsDisk` を **true** に設定する必要があります。

> **注:**
>
> カスタムプロパティ `UseEphemeralOsDisk` が **false** に設定されているか、値が指定されていない場合、プロビジョニングされたすべてのVDAはプロビジョニングされたOSディスクを引き続き使用します。

以下は、プロビジョニングスキームで使用するカスタムプロパティのセットの例です。

```
"CustomProperties": [

            {

                "Name": "UseManagedDisks",

                "Value": "true"

            },

            {

                "Name": "StorageType",

                "Value": "Standard_LRS"

            },

            {

                "Name": "UseSharedImageGallery",

                "Value": "true"

            },
```

```
            {
                "Name": "SharedImageGalleryReplicaRatio",
                "Value": "40"
            },
            {
                "Name": "SharedImageGalleryReplicaMaximum",
                "Value": "10"
            },
            {
                "Name": "LicenseType",
                "Value": "Windows_Server"
            },
            {
                "Name": "UseEphemeralOsDisk",
                "Value": "true"
            }
        ],
```

カタログのエフェメラルディスクを構成する

カタログのAzureエフェメラルOSディスクを構成するには、`Set-ProvScheme`で`UseEphemeralOsDisk`パラメーターを使用します。`UseEphemeralOsDisk`パラメーターの値を**true**に設定します。

> **注:**

この機能を使用するには、`UseManagedDisks`と`UseSharedImageGallery`のパラメーターも有効にする必要があります。

例:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

<Property xsi:type="StringProperty" Name="UseEphemeralOsDisk"
Value="true" />

</CustomProperties>'
```

エフェメラルディスクで使用されるストレージタイプを構成する

デフォルトでは、`Standard_LRS`がエフェメラルOSディスク機能で使用されるストレージタイプです。読み取り操作でのディスクIOPSを向上させるために、`StorageType`カスタムプロパティを指定することで、ストレージタイプをSSDを使用するように設定できます。現在サポートされている値は、`Standard_LRS`、`StandardSSD_LRS`、および`Premium_LRS`です。

既存のエフェメラルマシンでは、`Set-ProvScheme`と`Set-ProvVMUpdateTimeWindow`を使用して`StorageType`を更新することもできます。

エフェメラルディスクに関する重要な考慮事項

`New-ProvScheme`を使用してエフェメラルOSディスクをプロビジョニングするには、次の制約を考慮してください。

- カタログに使用されるVMサイズは、エフェメラルOSディスクをサポートしている必要があります。
- VMサイズに関連付けられているキャッシュまたは一時ディスクのサイズは、OSディスクのサイズ以上である必要があります。
- 一時ディスクのサイズは、キャッシュディスクのサイズよりも大きくする必要があります。

以下の際にもこれらの問題を考慮してください:

- プロビジョニングスキームを作成する際。
- プロビジョニングスキームを変更する際。
- イメージを更新する際。

Azure専用ホスト

MCSを使用して、Azure専用ホストにVMをプロビジョニングできます。Azure専用ホストにVMをプロビジョニングする前に:

- ホストグループを作成します。
- そのホストグループにホストを作成します。
- カタログと仮想マシンを作成するために、十分なホスト容量が予約されていることを確認してください。

次のPowerShellスクリプトを使用して、ホストテナンシーが定義されたマシンのカタログを作成できます。

```
New-ProvScheme <otherParameters> -CustomProperties '<CustomProperties
xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <Property xsi:type="StringProperty" Name="HostGroupId"
Value="myResourceGroup/myHostGroup" />

 ...other Custom Properties...

 </CustomProperties>
```

MCSを使用してAzure専用ホストに仮想マシンをプロビジョニングする場合、以下を考慮してください。

- *専用ホスト*はカタログのプロパティであり、カタログ作成後に変更することはできません。専用テナンシーは現在、Azureではサポートされていません。
- ホスティングユニットのリージョンにある、事前に構成されたAzureホストグループが、`HostGroupId` パラメーターを使用する際に必要です。
- Azureの自動配置が必要です。この機能は、ホストグループに関連付けられたサブスクリプションをオンボードするための要求を行います。詳細については、VM Scale Set on Azure Dedicated Hosts - Public Preview を参照してください。自動配置が有効になっていない場合、MCSはカタログ作成中にエラーをスローします。

Azure Compute Galleryイメージを使用してマシンカタログを作成または更新する

マシンカタログの作成に使用するイメージを選択する際、Azure Compute Gallery で作成したイメージを選択できます。

これらのイメージを表示するには、次の操作を行う必要があります。

1. Citrix Virtual Apps and Desktops サイトを構成します。
2. Azure Resource Manager に接続します。
3. Azure portal で、リソースグループを作成します。詳細については、「ポータルを使用して Azure Compute Gallery を作成する」を参照してください。
4. リソースグループで、Azure Compute Gallery を作成します。
5. Azure Compute Gallery で、イメージ定義を作成します。
6. イメージ定義で、イメージバージョンを作成します。

Azure Compute Gallery のイメージを使用してマシンカタログを作成または更新するには、次の PowerShell コマンドを使用します。

1. PowerShell ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. リソースグループを選択し、そのリソースグループのすべてのギャラリーを一覧表示します。

```
Get-ChildItem -LiteralPath @("XDHyp:
\HostingUnits\testresource\image.folder\sharedImageGalleryTest.resource
group")
```

4. ギャラリーを選択し、そのギャラリーのすべてのイメージ定義を一覧表示します。

```
Get-ChildItem -LiteralPath @("XDHyp:
\HostingUnits\testresource\image.folder\sharedImageGalleryTest.resource
group\sharedImageGallery.sharedimagegallery")
```

5. 1つのイメージ定義を選択し、そのイメージ定義のすべてのイメージバージョンを一覧表示します。

```
Get-ChildItem -LiteralPath @("XDHyp:
\HostingUnits\testresource\image.folder\sharedImageGalleryTest.resource
```

```
group\sharedImageGallery.sharedimagegallery\sigtestimage.imagedefinitio
n")
```

6. 次の要素を使用してMCSカタログを作成および更新します。

   - リソースグループ
   - ギャラリー
   - ギャラリーイメージ定義
   - ギャラリーイメージバージョン

   Remote PowerShell SDK を使用してカタログを作成する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/ を参照してください。

共有イメージギャラリーの構成

`New-ProvScheme` コマンドを使用して、Shared Image Gallery をサポートするプロビジョニングスキームを作成します。`Set-ProvScheme` コマンドを使用して、プロビジョニングスキームのこの機能を有効または無効にし、レプリカ比率とレプリカの最大値を変更します。

Shared Image Gallery 機能をサポートするために、プロビジョニングスキームに3つのカスタムプロパティが追加されました。

`UseSharedImageGallery`

- 公開されたイメージの保存に Shared Image Gallery を使用するかどうかを定義します。**True** に設定すると、イメージは Shared Image Gallery イメージとして保存され、それ以外の場合はスナップショットとして保存されます。
- 有効な値は**True**と**False**です。
- プロパティが定義されていない場合、デフォルト値は**False**です。

`SharedImageGalleryReplicaRatio`

- マシンとギャラリーイメージバージョンレプリカの比率を定義します。
- 有効な値は0より大きい整数です。
- プロパティが定義されていない場合、デフォルト値が使用されます。永続OSディスクのデフォルト値は1000、非永続OSディスクのデフォルト値は40です。

`SharedImageGalleryReplicaMaximum`

- 各ギャラリーイメージバージョンに対するレプリカの最大数を定義します。

- プロパティが定義されていない場合、デフォルト値は100です。
- プロパティが定義されていない場合、デフォルト値は100です。

ヒント:

MCS プロビジョニングカタログの公開イメージを保存するために Shared Image Gallery を使用する場合、MCS はカタログ内のマシンの数、レプリカ比率、およびレプリカの最大値に基づいて、ギャラリーイメージバージョンのレプリカ数を設定します。レプリカ数は、カタログ内のマシンの数をレプリカ比率で除算し（最も近い整数に切り上げ）、その値を最大レプリカ数で制限することによって計算されます。たとえば、レプリカ比率が20、最大値が5の場合、0〜20台のマシンには1つのレプリカが作成され、21〜40台には2つのレプリカ、41〜60台には3つのレプリカ、61〜80台には4つのレプリカ、81台以上には5つのレプリカが作成されます。

ユースケース：Shared Image Gallery のレプリカ比率とレプリカの最大値の更新

既存のマシンカタログは Shared Image Gallery を使用しています。`Set-ProvScheme` コマンドを使用して、カタログ内のすべての既存マシンおよび将来のマシンのカスタムプロパティを更新します。

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="True"/> <Property
xsi:type="IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/>
<Property xsi:type="IntProperty" Name="SharedImageGalleryReplicaMaximum"
Value="20"/></CustomProperties>'
```

ユースケース：スナップショットカタログを Shared Image Gallery カタログに変換する

このユースケースの場合：

1. `UseSharedImageGallery` フラグを**True**に設定して `Set-ProvScheme` を実行します。オプションで `SharedImageGalleryReplicaRatio` および `SharedImageGalleryReplicaMaximum` プロパティを含めます。
2. カタログを更新します。

3. マシンをパワーサイクルして、強制的に更新します。

例:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="True"/> <Property
xsi:type="IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/>
<Property xsi:type="IntProperty" Name="SharedImageGalleryReplicaMaximum"
Value="20"/></CustomProperties>'
```

ヒント:

パラメーター `SharedImageGalleryReplicaRatio` と `SharedImageGalleryReplicaMaximum` は必須ではありません。`Set-ProvScheme` コマンドが完了しても、共有イメージギャラリーのイメージはまだ作成されていません。カタログがギャラリーを使用するように構成されると、次回のカタログ更新操作で公開されたイメージがギャラリーに保存されます。カタログ更新コマンドは、ギャラリー、ギャラリーイメージ、およびイメージバージョンを作成します。マシンを再起動すると更新され、必要に応じてレプリカ数が更新されます。その時点から、既存のすべての非永続マシンは共有イメージギャラリーのイメージを使用してリセットされ、新しくプロビジョニングされたすべてのマシンはそのイメージを使用して作成されます。古いスナップショットは数時間以内に自動的にクリーンアップされます。

ユースケース: 共有イメージギャラリーカタログをスナップショットカタログに変換する

このユースケースの場合：

1. `UseSharedImageGallery` フラグを **False** に設定するか、未定義のままにして `Set-ProvScheme` を実行します。
2. カタログを更新します。
3. マシンをパワーサイクルして、強制的に更新します。

例:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="False"/></CustomProperties>'
```

ヒント:

スナップショットから共有イメージギャラリーカタログへの更新とは異なり、各マシンのカスタムデータは新しいカスタムプロパティを反映するようにまだ更新されていません。元の共有イメージギャラリーのカスタムプロパティを表示するには、次のコマンドを実行します: `Get-ProvVm -ProvisioningSchemeName catalog-name`。`Set-ProvScheme` コマンドが完了しても、イメージスナップショットはまだ作成されていません。カタログがギャラリーを使用しないように構成されると、次回のカタログ更新操作で公開されたイメージがスナップショットとして保存されます。その時点から、既存のすべての非永続マシンはスナップショットを使用してリセットされ、新しくプロビジョニングされたすべてのマシンはスナップショットから作成されます。マシンを再起動すると更新され、その時点でカスタムマシンデータが更新され、`UseSharedImageGallery` が **False** に設定されていることが反映されます。古い共有イメージギャラリーのアセット（ギャラリー、イメージ、バージョン）は数時間以内に自動的にクリーンアップされます。

指定された可用性ゾーンにマシンをプロビジョニングする

Azure環境では、特定の可用性ゾーンにマシンをプロビジョニングできます。これはPowerShellを使用して実現できます。

注:

- ゾーンが指定されていない場合、MCSはAzureにそのリージョン内にマシンを配置させます。複数のゾーンが指定されている場合、MCSはそれらのゾーンにマシンをランダムに分散させます。
- **ストレージとライセンスの種類**ページでストレージ冗長性としてZRSを選択すると、ゾーン選択をクリアしてAzureにVM可用性ゾーンを管理させることを推奨する警告が表

> 示されます。この警告は、可用性ゾーンを持つマシンプロファイルまたはホストグループを選択した場合にのみ表示されます。

PowerShellによる可用性ゾーンの構成

PowerShellを使用して、`Get-Item` で提供されるインベントリアイテムを表示できます。たとえば、*米国東部リージョンの* `Standard_B1ls` サービス提供を表示するには:

```
$serviceOffering = Get-Item -path "XDHyp:\Connections\my-connection-name\East US.region\serviceoffering.folder\Standard_B1ls.serviceoffering"
```

ゾーンを表示するには、アイテムの`AdditionalData`パラメーターを使用します:

`$serviceOffering.AdditionalData`

可用性ゾーンが指定されていない場合、マシンのプロビジョニング方法に変更はありません。

PowerShellを介して可用性ゾーンを構成するには、`New-ProvScheme`操作で利用可能な**Zones**カスタムプロパティを使用します。**Zones**プロパティは、マシンをプロビジョニングする可用性ゾーンのリストを定義します。これらのゾーンには、1つ以上の可用性ゾーンを含めることができます。たとえば、ゾーン1および3の`<Property xsi:type="StringProperty" Name="Zones" Value="1, 3"/>`です。

プロビジョニングスキームのゾーンを更新するには、`Set-ProvScheme`コマンドを使用します。

無効なゾーンが提供された場合、プロビジョニングスキームは更新されず、無効なコマンドを修正する方法に関する指示を提供するエラーメッセージが表示されます。

> **ヒント:**
>
> 無効なカスタムプロパティを指定すると、プロビジョニングスキームは更新されず、関連するエラーメッセージが表示されます。

ストレージの種類

MCSを使用するAzure環境の仮想マシンに対して、異なるストレージの種類を選択します。ターゲットVMの場合、MCSは以下をサポートします。

- OSディスク: プレミアムSSD、SSD、またはHDD

- ライトバックキャッシュディスク: プレミアムSSD、SSD、またはHDD

これらのストレージの種類を使用する場合、以下を考慮してください。

- 選択したストレージの種類をVMがサポートしていることを確認してください。
- 構成でAzureエフェメラルディスクを使用している場合、ライトバックキャッシュディスク設定のオプションは表示されません。

ヒント:

`StorageType` はOSタイプとストレージアカウント用に構成されます。`WBCDiskStorageType` はライトバックキャッシュストレージタイプ用に構成されます。通常のカタログの場合、`StorageType` が必要です。`WBCDiskStorageType` が構成されていない場合、`StorageType` が `WBCDiskStorageType` のデフォルトとして使用されます。

WBCDiskStorageType が構成されていない場合、StorageType が WBCDiskStorageType のデフォルトとして使用されます。

ストレージの種類を構成する

VMのストレージタイプを構成するには、`New-ProvScheme` の `StorageType` パラメーターを使用します。`StorageType` パラメーターの値をサポートされているストレージタイプのいずれかに設定します。

以下は、プロビジョニングスキームにおける `CustomProperties` パラメーターの設定例です。

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

</CustomProperties>'
```

ゾーン冗長ストレージを有効にする

カタログ作成時にゾーン冗長ストレージを選択できます。これは、Azure マネージドディスクを複数の可用性ゾーン間で同期的にレプリケートし、あるゾーンでの障害から他のゾーンの冗長性を利用して回復できるようにします。

ストレージタイプのカスタムプロパティで **Premium_ZRS** および **StandardSSD_ZRS** を指定できます。ZRSストレージは、既存のカスタムプロパティを使用するか、**MachineProfile** テンプレートを介して設定できます。ZRSストレージは、`-StartsNow` および `-DurationInMinutes -1` パラメーターを持つ `Set-ProvVMUpdateTimeWindow` コマンドでもサポートされており、既存のマシンをLRSからZRSストレージに変更できます。

制限事項:

- マネージドディスクのみをサポート
- プレミアムおよび標準ソリッドステートドライブ (SSD) のみでサポート
- `StorageTypeAtShutdown` には対応していません
- 一部のリージョンでのみ利用可能です。
- 大規模にZRSディスクを作成すると、Azureのパフォーマンスが低下します。そのため、最初の電源投入時には、マシンをより小さなバッチ（一度に300台未満のマシン）で起動してください。

ゾーン冗長ストレージをディスクストレージタイプとして設定する

初期カタログ作成時にゾーン冗長ストレージを選択することも、既存のカタログでストレージタイプを更新することもできます。

POWERSHELLコマンドを使用してゾーン冗長ストレージを選択する

`New-ProvScheme` PowerShellコマンドを使用してAzureで新しいカタログを作成する場合、`StorageAccountType` の値として `Standard_ZRS` を使用します。 例:

```
<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_ZRS" />
```

この値を設定すると、それが適切に使用できるかどうかを判断する動的APIによって検証されます。ZRSの使用がカタログに対して有効でない場合、以下の例外が発生する可能性があります。

- **StorageTypeAtShutdownNotSupportedForZrsDisks**: StorageTypeAtShutdownカスタムプロパティはZRSストレージでは使用できません。

- **StorageAccountTypeNotSupportedInRegion**: この例外は、ZRSをサポートしていないAzureリージョンでZRSストレージを使用しようとすると発生します。
- **ZrsRequiresManagedDisks**: ゾーン冗長ストレージはマネージドディスクでのみ使用できます。

以下のカスタムプロパティを使用して、ディスクストレージタイプを設定できます。

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`

> **注:**
>
> カタログ作成時、カスタムプロパティが設定されていない場合は、マシンプロファイルのOSディスク`StorageType`が使用されます。

マシンプロファイルからVMとNICの診断設定をキャプチャする

マシンカタログの作成時、既存のマシンカタログの更新時、および既存のVMの更新時に、マシンプロファイルからVMとNICの診断設定をキャプチャできます。

VMまたはテンプレート仕様をマシンプロファイルのソースとして作成できます。

主な手順

1. Azureで必要なIDを設定します。これらのIDはテンプレート仕様で指定する必要があります。
    - ストレージアカウント
    - Log Analyticsワークスペース
    - 標準ティアの価格設定のEvent Hub名前空間
2. マシンプロファイルのソースを作成します。
3. 新しいマシンカタログを作成するか、既存のカタログを更新するか、既存のVMを更新します。

Azureで必要なIDを設定する

Azureで次のいずれかを設定します。

- ストレージアカウント

- ログ分析ワークスペース
- Standardティアの価格設定を持つイベントハブ名前空間

ストレージアカウントを設定する

Azureで標準ストレージアカウントを作成します。テンプレート仕様では、ストレージアカウントの完全なresourceIdを`storageAccountId`として指定します。

VMがストレージアカウントにデータをログ記録するように設定されると、データは`insights-metrics-pt1m`コンテナの下で見つけることができます。

ログ分析ワークスペースを設定する

ログ分析ワークスペースを作成します。テンプレート仕様では、ログ分析ワークスペースの完全なresourceIdをworkspaceIdとして指定します。

VMがワークスペースにデータをログ記録するように設定されると、Azureのログでデータをクエリできます。Azureのログで次のコマンドを実行すると、リソースによってログ記録されたすべてのメトリックの数を表示できます。

```
AzureMetrics | summarize Count=count() by ResourceId
```

イベントハブを設定する

Azureポータルでイベントハブを設定するには、次の手順を実行します。

1. 標準ティアの価格設定でイベントハブ名前空間を作成します。
2. 名前空間の下にイベントハブを作成します。
3. イベントハブの下にある**キャプチャ**に移動します。トグルをONにして、Avro出力タイプでキャプチャします。
4. ログをキャプチャするために、既存のストレージアカウントに新しいコンテナを作成します。
5. テンプレートスペックで、次の形式で`eventHubAuthorizationRuleId`を指定します: `/subscriptions/093f4c12-704b-4b1d-8339-f339e7557f60/resourcegroups/matspo/providers/Microsoft.EventHub/namespaces/matspoeventhub/authorizationrules/RootManageSharedAccessKey`
6. イベントハブの名前を指定します。

VMがイベントハブにデータをログするように設定されると、データは構成されたストレージコンテナにキャプチャされます。

マシンプロファイルソースを作成する

VMまたはテンプレートスペックをマシンプロファイルソースとして作成できます。

診断設定を含むVMベースのマシンプロファイルを作成する

VMをマシンプロファイルとして作成する場合は、まずテンプレートVM自体に診断設定をセットアップします。詳細な手順については、MicrosoftドキュメントのAzure Monitorの診断設定を参照してください。

VMまたはNICに関連付けられた診断設定が現在存在することを確認するには、次のコマンドを実行できます。

```
az monitor diagnostic-settings list --resource-group matspo --resource
matspo-tog-cc2659 --resource-type microsoft.network/networkInterfaces
```

```
az monitor diagnostic-settings list --resource-group matspo --resource
matspo-tog-cc2 --resource-type microsoft.compute/virtualMachines
```

診断設定を含むテンプレートスペックベースのマシンプロファイルを作成する

診断設定がすでに有効になっているVMを使用し、それをARMテンプレートスペックにエクスポートする場合、これらの設定はテンプレートに自動的に含まれません。ARMテンプレート内で診断設定を手動で追加または変更する必要があります。

ただし、VMをマシンプロファイルとして使用する場合、MCSは、重要な診断設定が正確にキャプチャされ、MCSカタログ内のリソースに適用されることを保証します。

1. VMとNICを定義する標準テンプレート仕様を作成します。
2. スペックに従って診断設定をデプロイするための追加リソースを追加します: Microsoft.Insights diagnosticSettings。スコープには、テンプレート内のVMまたはNICを部分的なIDを持つ名前で参照します。たとえば、テンプレートスペック内のtest-VMという名前のVMにアタッチされた診断設定を作成する場合、スコープを次のように指定します。

   ```
   "scope": "microsoft.compute/virtualMachines/test-VM",
   ```

3. テンプレートスペックをマシンプロファイルソースとして使用します。

診断設定を含むカタログを作成または更新する

マシンプロファイルソースを作成した後、`New-ProvScheme` コマンドを使用してマシンカタログを作成し、`Set-ProvScheme` コマンドを使用して既存のマシンカタログを更新し、`Request-ProvVMUpdate` コマンドを使用して既存のVMを更新できます。

ページファイルの場所の決定

ページファイルの場所は、次のシナリオに従って決定されます。

注:

デフォルトのページファイルの場所は OS ディスクです。

シナリオ	場所
ページファイルの設定がカスタムプロパティで指定されている	カスタムプロパティで指定されているとおり
エフェメラルOSディスクまたは休止状態が有効になっている	OSディスク
VMに一時ディスクがある	一時ディスク
MCS I/O が有効になっています	WBCディスク

ページファイル設定のシナリオ

次の表は、イメージ準備中およびプロビジョニングスキームの更新中に考えられるページファイル設定のシナリオの一部を示しています。

期間	シナリオ	結果
イメージの準備	ソースイメージのページファイルを一時ディスクに設定しますが、プロビジョニングスキームで指定するVMサイズには一時ディスクがありません	ページファイルはOS上に配置されます
イメージの準備	OSディスクにソースイメージのページファイルを設定しますが、プロビジョニングスキームで指定するVMサイズには一時ディスクがあります	ページファイルは一時ディスクに配置されます

期間	シナリオ	結果
イメージの準備	一時ディスクにソースイメージのページファイルを設定し、プロビジョニングスキームでエフェメラルOSディスクを有効にします	ページファイルはOSディスクに配置されます
プロビジョニングスキームの更新	VDAバージョンが2311より前のときにプロビジョニングスキームを更新しようとします	警告とともにページファイル設定を変更します
プロビジョニングスキームの更新	VDAバージョンが2311以降のときにプロビジョニングスキームを更新しようとします	ページファイルの場所の決定に従ってページファイルの場所を決定します

ページファイル設定の指定

PowerShellコマンドを使用して、場所やサイズを含むページファイル設定を指定できます。これにより、ページファイルの場所の決定に従ってMCSによって決定されたページファイル設定が上書きされます。これは、マシンカタログ作成中に次の`New-ProvScheme`コマンドを実行することで行えます。

重要な考慮事項

カタログ作成を進める前に、以下を考慮してください。

- すべてのカスタムプロパティ（'PageFileDiskDriveLetterOverride'、'InitialPageFileSizeInMB'、'MaxPageFileSizeInMB'）を`New-ProvScheme`コマンドで指定するか、または何も指定しないでください。
- この機能はCitrix Studioではサポートされていません。
- 初期ページファイルサイズは16 MBから16777216 MBの間である必要があります。
- 最大ページファイルサイズは、初期ページファイルサイズ以上で、かつ16777216 MB未満である必要があります。
- 初期ページファイルサイズと最大ページファイルサイズの両方を同時にゼロに設定できます。

> **注:**
>
> マスターイメージを更新することなく、既存のカタログに新しく追加されたVMのページファイル設定を変更できます。ページファイル設定を変更するには、VDAバージョン2311以

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

```
New-ProvScheme -CleanOnBoot `

-HostingUnitName "zijinnet" `

-IdentityPoolName "PageFileSettingExample" `

-ProvisioningSchemeName "PageFileSettingExample" `

-InitialBatchSizeHint 1 `

-MasterImageVM "XDHyp:\HostingUnits\zijinnet\image.folder\neal-zijincloud-
resources.resourcegroup\CustomWin10VDA_OsDisk_1_9473d7c8a6174b2c8284c7d3ef
eea88f.manageddisk" `

-NetworkMapping @{"0"="XDHyp:\\HostingUnits\\zijinnet\
\virtualprivatecloud.folder\\East US.region\\virtualprivatecloud.folder\
\neal-zijincloud-resources.resourcegroup\\neal-zijincloud-resources-
vnet.virtualprivatecloud\\default.network"} `

-ServiceOffering "XDHyp:\\HostingUnits\\zijinnet\\serviceoffering.folder\
\Standard_B2ms.serviceoffering" `

-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/XMLSchema-
instance"> `

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false"/> `

<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `

<Property xsi:type="StringProperty" Name="PageFileDiskDriveLetterOverride"
Value="d"/> `

<Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
Value="2048"/> `

<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB"
Value="8196"/> `
```

```
<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS"/> `

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client"/> `

</CustomProperties>'
```

ページファイル設定の変更

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

ページファイル設定を変更するには、VDAバージョン2311以降が必要です。PowerShellコマンドを使用してページファイル設定を変更できます。

Azure環境で変更できるページファイル設定は次のとおりです。

- `PageFileDiskDriveLetterOverride`
- `InitialPageFileSizeInMB`
- `MaxPageFileSizeInMB`

既存のカタログのページファイル設定を変更する

既存のマシンカタログのページファイル設定を変更するには、`Set-ProvScheme` コマンドを実行します。この場合、更新はカタログに追加された新しいVMにのみ適用されます。例：

```
Set-ProvScheme -ProvisioningSchemeName $schemeName -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="StandardSSD_LRS" />

<Property xsi:type="StringProperty" Name="PageFileDiskDriveLetterOverride"
Value="D" />

<Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
```

```
Value="2048" />

<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB"
Value="8196" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property  xsi:type="StringProperty" Name="Zones" Value="1" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="neal-
test-group1" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

</CustomProperties>'
```

注:

ライトバックキャッシュを有効にして、PowerShell コマンドを使用して `PageFileDiskDriveLetterOverride` を `C:` に設定しようとすると、MCS IO ドライバーはページファイルを自動的に正しいディスクドライブにリダイレクトし、`C:` にはリダイレクトしません。

Azure Spot VMを使用してカタログを作成する

Azure Spot VMを使用すると、Azureの未使用のコンピューティング能力を大幅なコスト削減で活用できます。ただし、Azure Spot VMを割り当てる能力は、現在の容量と価格設定に依存します。そのため、Azureは強制排除ポリシーに従って、実行中のVMを強制排除したり、VMの作成に失敗したり、VMの電源をオンに失敗したりする可能性があります。したがって、Azure Spot VMは、一部の重要でないアプリケーションやデスクトップに適しています。詳細については、Azure Spot Virtual Machinesの使用を参照してください。

制限事項

- すべてのVMサイズがAzure Spot VMでサポートされているわけではありません。詳細については、制限事項を参照してください。

VMサイズがSpot VMをサポートしているかどうかを確認するには、次のPowerShellコマンドを実行します。VMサイズがSpot VMをサポートしている場合、`SupportsSpotVM`は**True**になります。

```
(Get-Item "XDHyp:\HostingUnits\azure-res-
conn2\serviceoffering.folder\Standard_D2ds_v4.serviceoffering").
AdditionalData
```

- 現在、Azure Spot VMは休止状態をサポートしていません。

要件

Azure Spot VMカタログのマシンプロファイルソース（VMまたはテンプレート仕様）を作成する際、(VMを使用している場合は) Azure Spot Instanceを選択するか、(テンプレート仕様を使用している場合は) `priority`を`Spot`として設定する必要があります。

Azure Spot VMを使用してカタログを作成する手順

1. マシンプロファイルソース（VMまたは起動テンプレート）を作成します。
   - Azureポータルを使用してVMを作成するには、Azureポータルを使用してAzure Spot Virtual Machinesを展開するを参照してください。
   - テンプレート仕様を作成するには、テンプレート仕様の**resources > type: Microsoft.Compute/virtualMachines > properties**の下に次のプロパティを追加します。例：

     ```
     "priority": "Spot",

     "evictionPolicy": "Deallocate",

     "billingProfile": {

     "maxPrice": 0.01

     }
     ```

注:

- 削除ポリシーは**Deallocate**または**Delete**にすることができます。

- 非永続VMの場合、MCSは常に削除ポリシーを**Delete**に設定します。VMが削除された場合、非永続ディスク（例：OSディスク）とともに削除されます。永続ディスク（例：IDディスク）は削除されません。ただし、カタログタイプが永続的であるか、`PersistOsDisk`カスタムプロパティがTrueに設定されている場合、OSディスクは永続的です。同様に、`PersistWbc`カスタムプロパティが**True**に設定されている場合、WBCディスクは永続的です。
- 永続VMの場合、MCSは常に削除ポリシーをDeallocateに設定します。VMが削除された場合、割り当て解除されます。ディスクに変更は加えられません。
- 最大価格は、1時間あたりに支払ってもよい価格です。**容量のみ**を使用している場合、これは**-1**です。最大価格は、null、-1、またはゼロより大きい小数のみです。詳細については、価格を参照してください。

2. マシンプロファイルがAzure Spot VM対応であるかどうかを確認するには、次のPowerShellコマンドを実行します。`SpotEnabled`パラメーターが**True**で、`SpotEvictionPolicy`が**Deallocate**または**Delete**に設定されている場合、マシンプロファイルはAzure Spot VM対応です。例：

   - マシンプロファイルのソースがVMの場合、次のコマンドを実行します。

     ```
     (Get-Item "XDHyp:\HostingUnits\azure-res-
     conn2\machineprofile.folder\fifthcolumn.resourcegroup\kb-spot-
     delete.vm"). AdditionalData
     ```

   - マシンプロファイルのソースがテンプレート仕様の場合、次のコマンドを実行します。

     ```
     (Get-Item "XDHyp:\HostingUnits\azure-res-
     conn2\machineprofile.folder\fifthcolumn.resourcegroup\fc-aeh-
     templatespec.templatespec\14.0.0-spot-
     delete.templatespecversion").AdditionalData
     ```

3. `New-ProvScheme` PowerShellコマンドを使用して、マシンプロファイルでマシンカタログを作成します。

`Set-ProvScheme`コマンドを使用してカタログを更新できます。既存のVMをPowerShellコマンド`Set-ProvVmUpdateTimeWindow`を使用して更新することもできます。マシンプロファイルは次回の電源投入時に更新されます。

実行中のAzure Spot VMでの強制排除

コンピューティング容量が利用できない場合、または時間あたりの価格が設定された最大価格よりも高い場合、Azureは実行中のSpot VMを強制排除します。デフォルトでは、強制排除の通知はされません。VMは単にフリーズし、強制排除されます。Microsoftは、強制排除を監視するためにScheduled Eventsを使用することを推奨しています。強制排除を継続的に監視するを参照してください。VM内からスクリプトを実行して、強制排除前に通知を受け取ることもできます。たとえば、MicrosoftはPythonでポーリングスクリプトScheduledEvents.csを提供しています。

トラブルシューティング

- プロビジョニングされたVMのcustomMachineDataで、`Get-ProvVM`コマンドを使用してSpot VMのプロパティを確認できます。優先度フィールドが**Spot**に設定されている場合、Spotが使用されています。
- Azure PortalでVMがSpotを使用しているかどうかを確認できます。

  a. Azure PortalでVMを見つけます。

  b. **概要**ページに移動します。

  c. 下にスクロールして、**Azure Spot**セクションを見つけます。

    - Spotが使用されていない場合、このフィールドは空です。
    - Spotが使用されている場合、**Azure Spot**および**Azure Spot eviction policy**フィールドが設定されます。

1. 構成ページで、VMの課金プロファイルまたは1時間あたりの最大価格を確認できます。

バックアップVMサイズの構成

パブリッククラウドでは、特定のVMサイズの容量が不足する場合があります。Azureの容量が不足した場合、MCSは事前に構成されたバックアップVMサイズのリストにフォールバックします。この、顧客がワークロード要件に合わせて調整した厳選されたリストにより、VMが以前に休止状態であった場合に、これらのサイズのいずれかがPower OnまたはResumeで起動するのに十分な容量を持つ可能性が高まります。

電源操作が開始されると、MCSは高可用性を確保するために自動フォールバックシーケンスを実装します。ワークフローは次のとおりです。

1. 開始: ユーザーまたは管理者がWeb Studioを介して**PowerOn**または**Resume**コマンドを発行します。
2. 例外監視: MCSはプライマリ構成を使用してVMを起動しようとします。Quota Exceeded、Allocation Failed、Zonal Allocation Failed、SKU Not Availableなどの特定のAzure容量例外を監

視します（これについては一般的に、Azureの容量または割り当ての失敗を監視すると言えます）。

3. シーケンシャルフォールバック: 上記のエラーのいずれかが発生した場合、MCSはVMが正常に起動するまでBackupVmConfigurationリストを順次反復処理します。BackupVmConfiguration内のすべてのサイズが失敗した場合、電源操作は失敗としてマークされます。
4. 更新と再作成のロジック:
    - 直接更新: ほとんどの場合、MCSはバックアップSKUへの単純なVMサイズ更新を実行し、その後VMの電源をオンにします。
    - 削除と再作成: 環境の整合性を維持するため、特定の移行では既存のVMを削除し、その場所に新しいVMを作成する必要があります。これは次の場合に発生します。
        - Spot VMタイプとRegular VMタイプを切り替える場合。
        - リソースディスク（一時ストレージ）をサポートするVMサイズとサポートしないVMサイズを切り替える場合。
5. データの永続性と回復: 「削除と再作成」操作中に、極端なAzure容量不足によりすべてのバックアップサイズも失敗した場合、VMは一時的にAzure Portalから消えることがあります。ただし、データ損失は発生しません。次回のPowerOn試行時に、MCSは元の設定を使用してVMを再作成し、既存のOS、Identity、およびDataディスクを再アタッチします。
6. Spot VMの課金とMaxPriceの動作 プライマリ構成でSpot優先度と特定のBilling Profile (MaxPrice) を持つMachine Profile (VM Template) を使用している場合、フォールバック中に次のロジックが適用されます。
    - プライマリサイズ: Machine Profileで定義されたMaxPriceを使用します。強制排除は価格または容量に基づきます。
    - バックアップスポットサイズ: BackupVmConfigurationプロパティは現在、各SKUに対して一意の `MaxPrice` 入力をサポートしていません。MCSは次のように移行を処理します。
    - MaxPriceのリセット: MCSはMaxPriceを-1に設定します。
    - 削除ポリシーの変更: これにより、Azureの削除動作が価格ベースから容量ベースに変更されます。
    - 料金: そのバックアップSKUの標準的な従量課金制 (PAYG) レートを上限として、現在のスポット価格が課金されます。これにより、VMは価格変動のためではなく、Azureの物理容量が本当に不足した場合にのみ削除されることが保証されます。

7. バックアップ状態の永続性: 一度起動すると、VMはシャットダウンまたは休止状態のリクエストが処理されるまで、セッション中はバックアップサイズで維持されます。
8. プライマリサイズの復元: 次回のPowerOnまたはResume時に、MCSは常にVMをそのプライマリサービスオファリング（カタログまたはマシンプロファイルで定義されている）に戻そうとします。プライマリサイズが利用できない場合、フォールバックシーケンスが繰り返されます。

休止状態に関する課題

一般的な制限事項で説明されているように、Azureは休止状態のVMのサイズ変更を許可していません。VMは停止状態である必要があります。したがって、サイズを変更する前に、MCSは休止状態をクリアするために割り当て解除リクエストを発行し、これによりVMの休止状態が失われます。その後、MCSはバックアップサイズをループし、VMサイズを更新して電源をオンにします。

バックアップVMサイズのサポートされていないシナリオ

次の構成はサポートされていません。

- 永続VMの場合、次のシナリオはサポートされていません。
  - VMがDiskControllerType SCSIを使用しているが、バックアップVMサイズがDiskControllerType NVMeのみをサポートしている場合。
  - VMがDiskControllerType NVMeを使用しているが、バックアップVMサイズがDiskControllerType SCSIのみをサポートしている場合。
- MCSIOが有効な非永続VMの場合、ライトバックキャッシュディスクがリソースディスクの一時ストレージを使用している場合、一時ストレージのないサイズへの切り替えはサポートされていません。

バックアップVMサイズを構成するための前提条件

以下のいずれかが満たされていない場合、エラーがスローされます。

- マシンカタログでマシンプロファイルが使用されている場合にのみサポートされます。
- タイプはオプションで、SpotまたはRegularのいずれかです。指定しない場合、デフォルトはRegularです。
- 繰り返し構成を避けるため、ServiceOfferingの各組み合わせは一意である必要があります。
- リージョンクォータは、ServiceOfferingに十分なコアを持っている必要があります。
- ネットワークインターフェースの数は、ServiceOfferingで許可されている最大値を超えてはなりません。

- このBackupVmConfigurationリスト内のServiceOfferingは、現在のカスタムプロパティ、マスターイメージの機能、およびMachineProfileと互換性がある必要があります。いくつかの失敗シナリオは次のとおりです。
  - Azure Dedicated Hosts: 専用ホストが使用されている場合、ホストグループ内のホストはServiceOfferingをサポートしている必要があります。
  - エフェメラルOSディスク: カスタムプロパティで有効になっている場合、ServiceOfferingはエフェメラルOSディスクをサポートしている必要があります。
  - Premium Storage: カスタムプロパティで指定されている場合、ServiceOfferingはPremiumストレージをサポートしている必要があります。
  - Accelerated Networking: MachineProfileで有効になっている場合、ServiceOfferingはAccelerated Networkingをサポートしている必要があります。
  - DiskEncryptionAtHost: MachineProfileで有効になっている場合、ServiceOfferingはEncryption at Hostをサポートしている必要があります。
  - 一時ストレージ: MCSIOが使用されており、ライトバックキャッシュが一時ディスク上にある場合、一時ストレージを持たないVMサイズの利用は許可されません。
  - HyperVGeneration: ServiceOfferingは、MasterImageVMで指定されたVM世代（1または2）と互換性がある必要があります。
  - TrustedLaunch: MachineProfileで有効になっている場合、ServiceOfferingはTrustedLaunchをサポートしている必要があります。
  - 機密VM: MachineProfile で有効になっている場合、ServiceOffering は機密VMをサポートする必要があります。

バックアップVMサイズでカタログを作成する

> **注:**
>
> Studio UI のフリーズの問題に対処するには、PowerShell コマンドを実行する際に、すべてのシングルクォートを `"` に置き換えてください。

1. PowerShell ウィンドウを開きます。
2. Citrix 固有の PowerShell モジュールをロードするには、`asnp citrix*` を実行します。
3. ブローカーカタログを作成します。このカタログには、作成される予定のマシンが格納されます。

4. ID プールを作成します。これは、作成されるマシン用に作成された AD アカウントのコンテナになります。
5. マシンプロファイルを使用してプロビジョニングスキームを作成します。「バックアップ構成を構成する方法」を参照してください。
6. プロビジョニングスキームの一意の ID で `BrokerCatalog` を更新します。
7. VM を作成してカタログに追加します。

既存のカタログを更新する

`Set-ProvScheme` コマンドを使用してプロビジョニングスキームを更新できます。「バックアップ構成を構成する方法」を参照してください。

既存のVMを更新する

`Set-ProvVMUpdateTimeWindow` PowerShell コマンドを使用して、カタログ内の既存の VM を更新できます。このコマンドは、指定された時間枠内で次回の電源投入時に、カタログに関連付けられたプロビジョニングスキームから作成された VM を更新します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-StartTimeInUTC "3/12/2022 3am" -DurationInMinutes 60`
```

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-StartsNow -DurationInMinutes 60
```

選択した既存のMCS VMのバックアップVMサイズリストを`Set-ProvVM`コマンドを使用して構成できます。ただし、更新を適用するには、`Set-ProvVMUpdateTimeWindow`を使用してVMの更新時間枠を設定し、その時間枠内でVMを起動します。例：

1. 選択した既存のMCS VMのバックアップVMサイズリストを構成するには、`Set-ProvVM`コマンドを実行します。例：

```
Set-ProvVM -ProvisioningSchemeName "name" -VMName "Vm-001"

-CustomProperties

"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`"xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">

<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
```

```
Value=`"true`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"LicenseType`"
Value=`"Windows_Server`"/>

<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`"
Value=`"true`"/>  <Property xsi:type=`"StringProperty`"
Name=`"BackupVmConfiguration`" Value=`"[{&quot;ServiceOffering&quot;:
&quot;Standard_D2as_v4&quot;, &quot;Type&quot;: &quot;Spot&quot;},
{&quot;ServiceOffering&quot;: &quot;Standard_D2s_v3&quot;,
&quot;Type&quot;: &quot;Regular&quot;}, {&quot;ServiceOffering&quot;:
&quot;Standard_D2s_v3&quot;, &quot;Type&quot;: &quot;Spot&quot;}]`"/>
</CustomProperties>"
```

2. 更新を適用するには、`Set-ProvVMUpdateTimeWindow`コマンドを実行します。例：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-StartsNow -DurationInMinutes 60
```

すべてのリソースにタグをコピーする

マシンプロファイルで指定されたタグを、マシンカタログ内の新しい VM または既存の VM の複数の NIC やディスク（OS ディスク、ID ディスク、ライトバックキャッシュディスク）など、すべてのリソースにコピーできます。マシンプロファイルのソースは、VM または ARM テンプレート仕様にすることができます。

注:

リソースにタグを保持するには、タグにポリシーを追加するか（タグコンプライアンスのポリシー定義を割り当てるを参照）、マシンプロファイルソースにタグを追加する必要があります。

前提条件

そのVMのVM、ディスク、NICにタグを付けるには、マシンプロファイルソース（VMまたはARMテンプレート仕様）を作成します。

- VMをマシンプロファイルの入力として使用したい場合は、AzureポータルでVMとすべてのリソースにタグを適用します。Azureポータルでタグを適用するを参照してください。
- ARMテンプレート仕様をマシンプロファイルの入力として使用したい場合は、各リソースの下に次のタグブロックを追加します。

```
 "tags": {

"TagC": "Value3"

},
```

注:

テンプレート仕様には、最大1つのディスクと少なくとも1つのNICを含めることができます。

新しいマシンカタログ内のVMのリソースにタグをコピーする

1. VMまたはARMテンプレート仕様をマシンプロファイルの入力として使用して、非永続または永続カタログを作成します。
2. カタログにVMを追加して電源をオンにします。マシンプロファイルで指定されたタグが、そのVMの対応するリソースにコピーされていることを確認する必要があります。

注:

マシンプロファイルで提供されるNICの数と、VMで使用するNICの数に不一致がある場合、エラーが発生します。

既存のVMのリソース上のタグを変更する

1. すべてのリソースにタグを付けたマシンプロファイルを作成します。
2. 既存のマシンカタログを、更新されたマシンプロファイルで更新します。例：

```
Set-ProvScheme -ProvisioningSchemeName <YourCatalogName>
-MachineProfile <PathToYourMachineProfile>
```

3. 更新を適用したいVMの電源をオフにします。
4. VMのスケジュールされたアップデートを要求します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName <YourCatalogName>  -
VMName machine1 -StartsNow -DurationInMinutes -1
```

5. VMの電源をオンにします。
6. マシンプロファイルで指定されたタグが、対応するリソースにコピーされていることを確認する必要があります。

注:

マシンプロファイルで提供されるNICの数と、`Set-ProvScheme`で提供されるNICの数に不一致がある場合、エラーが発生します。

事前フォーマットされたWBCディスクカタログを作成する

プロビジョニングされたマシンの起動パフォーマンスを向上させるために、事前フォーマットされたWBCディスクカタログを作成できます。この機能を実装するには、WBCが有効なAzureカタログを作成し、追加のカスタムプロパティ`PreformatWriteBackCache`を`True`として含めます。

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

この機能は、MCSがマスタリングフェーズをプロビジョニングワークフロー全体から分離するイメージ管理ワークフローと互換性があります。イメージ管理の詳細については、イメージ管理を参照してください。

WBCを有効にし、`PreformatWriteBackCache`を`True`としてAzureカタログを作成する例:

```
$customProperties = @'

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="PreformatWriteBackCache"
Value="true" />

</CustomProperties>
```

```
'@



New-ProvScheme -CleanOnBoot `

-ProvisioningSchemeName "provisioningschemename" `

-HostingUnitName "hostingunitname" `

-IdentityPoolName "identitypoolnamename" `

-MasterImageVM "XDHyp:
\HostingUnits\AzureHostingUnit\image.folder\rg.resourcegroup\masterImage.m
anageddisk" `

-CustomProperties $customProperties `

-NetworkMapping $networkMapping `

-UseWriteBackCache `

-WriteBackCacheDiskSize 30
```

既存のカタログのWBCディスクキャッシュサイズを更新する例:

```
Set-ProvScheme -ProvisioningSchemeName provisioningschemename
-WriteBackCacheDiskSize 127
```

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

AzureでMCSプロビジョニングされたCitrix Provisioningカタログを作成する際、WBCディスクを非永続的（`PersistWBC`をFalseとして）にプロビジョニングできます。この構成により、AzureでMCSプロビジョニングされたCitrix ProvisioningカタログのVMをシャットダウンした後、ライトバックキャッシュ（WBC）ディスクを削除するのに役立ちます。

条件:

この機能が動作するためには、カスタムプロパティ`PreformatWriteBackCache`を`True`として設定する必要があります。

`PersistWBC`を`False`として、`PreformatWriteBackCache`を`True`としてAzureカタログを作成する例:

```
$customProperties = @'

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PreformatWriteBackCache"
Value="true" />

</CustomProperties>

'@



New-ProvScheme -CleanOnBoot `

-ProvisioningSchemeName "provisioningschemename" `

-HostingUnitName "hostingunitname" `

-IdentityPoolName "identitypoolnamename" `

-MasterImageVM "XDHyp:
\HostingUnits\AzureHostingUnit\image.folder\rg.resourcegroup\masterImage.m
anageddisk" `

-CustomProperties $customProperties `

-NetworkMapping $networkMapping `

-UseWriteBackCache `

-WriteBackCacheDiskSize 30
```

既存のカタログを`Set-ProvScheme`コマンドを使用して更新し、`PersistWBC`カスタムプロパティを更新することもできます。

データディスクのプロビジョニング

AzureのMCSマシンカタログのMCSによって作成された永続的または非永続的なVMに、永続的なデータディスクを作成して割り当てることができます。

データディスクは、イメージソースとしてマネージドディスクからプロビジョニングする必要があります。

データディスクのプロパティ

データディスクは、カスタムプロパティで指定されていない場合、カスタムプロパティまたはOSディスクテンプレートからプロパティを派生させます。

- カスタムプロパティから派生したプロパティ
  - `DiskEncryptionSetId`
  - `Zones`
  - `StorageType`
- カスタムプロパティで指定されていない場合、OSディスクテンプレートから派生するプロパティ
  - `DiskEncryptionSetId`
  - `Zones`
  - `StorageType`

> **注:**
>
> - カスタムプロパティまたはOSディスクテンプレートでゾーン冗長ストレージ（ZRS）が指定されていない場合、データディスクはOSディスクおよびIDディスクと同じゾーンに配置されます。
> - タグはOSディスクテンプレートからのみ派生します。

制限事項

現在、以下の操作はサポートされていません。

- 複数のデータディスクのプロビジョニング。
- 非永続データディスクのプロビジョニング。

- テンプレートを使用したデータディスクの作成。
- 既存のカタログとVMをデータディスクを使用するように変更する。
- データディスクをリセットする。
- データディスクのイメージ更新。
- マネージドディスク以外のソースを使用する。
- データディスクをAzure Compute Gallery (ACG) に保存する。
- データディスクに`StorageTypeAtShutdown`を使用する

データディスクを使用してカタログを作成する

データディスクを使用してMCSマシンカタログをプロビジョニングするには、`New-ProvScheme` PowerShellコマンドに次のパラメーターを含めます。

- `DataDisk`: 有効なManagedDiskタイプのインベントリアイテムへのパス。
- `DataDiskPersistence`: `DataDisk`が永続的か非永続的かを示すため。ただし、現在サポートされているのは永続的なデータディスクのみです。

例:

```
New-ProvScheme  -CleanOnBoot -HostingUnitName "<HostingUnitName >"
-IdentityPoolName "<IdentityPoolName >" -InitialBatchSizeHint 1
-MasterImageVM disk.manageddisk -NetworkMapping <NetworkMapping >
-ProvisioningSchemeName "<ProvisioningSchemeName >" -DataDisk "XDHyp:
\HostingUnits\Azure-Resources-1\image.folder\<resourcegroupname>\xxxx-
datadisk.manageddisk"  -DataDiskPersistence "Persistent"  -Scope @()
-VMCpuCount 4  -VMMemoryMB 6144  -TenancyType Shared  -FunctionalLevel
"L7_20"
```

データディスクが使用中かどうかを判断する

データディスクがVMに割り当てられているかどうかを確認するには、次の手順を実行します。

- `Get-ProvVm`を実行し、VMの`CustomVmData`を確認します。VMがデータディスクを使用している場合、役割が`DiskRole.DataDisk`のディスクレコードがあります。
- AzureポータルでVMの下にデータディスクが存在するかどうかを確認します。

データディスクを削除する

カタログを削除すると、`forgetVM` または `purgeDBOnly` オプションを使用しない限り、データディスクは削除されます。VM を削除すると、`forgetVM` または `purgeDBOnly` オプションを使用しない限り、データディスクは削除されます。

アンマネージドディスクからマネージドディスクへの移行

September 30, 2025 に、Azure はアンマネージドディスク (つまり VHD) を正式に廃止します。アンマネージドディスクを使用している既存の VM は、期限後に停止され、割り当てが解除されます。

ただし、MCS でプロビジョニングされた VM をアンマネージドディスクからマネージドディスクに移行することで、Azure のアンマネージドディスク廃止計画によるサービス停止を回避できます。

VM に接続されているすべてのアンマネージドディスクが変換されます。これには、ID ディスク、OS ディスク、および WBC ディスク (使用されている場合) が含まれます。

Azure のアンマネージドディスク廃止計画の詳細については、September 30, 2025 までに Azure アンマネージドディスクを移行する を参照してください。

ユースケース

この機能は、永続的および非永続的な MCS プロビジョニングカタログに適用されます。

また、オンデマンド VM と非オンデマンド (レガシー) VM の両方の移行をサポートしています。

- オンデマンド VM: 既存のディスクをアンマネージドディスクからマネージドディスクに移行して、Azure の更新されたサポートに合わせます。
- 非オンデマンド (レガシー) VM: レガシーまたは非オンデマンド VM は、アンマネージドディスクのみをサポートしています。この機能を使用して、レガシー VM をオンデマンドに変換すると同時に、マネージドディスクに移行します。

オンデマンドプロビジョニングの詳細については、「Azure オンデマンドプロビジョニング」を参照してください。

制限事項

- マシンカタログまたは VM がマネージドディスクに変換されると、アンマネージドディスクに戻すことはできません。
- 非オンデマンド (レガシー) VMの場合、移行プロセスには、それらをオンデマンドプロビジョニングに変換することが含まれます。ディスクのみを変換して非オンデマンドVMを使い続けることはできません。

重要な考慮事項

- 変換は自動的には行われません。電源オン操作の一部として行われます。

- VMに対して複数の更新が要求された場合、ディスク変換が優先されます。追加の更新は、その後の電源オンまで延期されます。
- VMが正常に変換され、電源がオンになると、コストを節約するために、VMのVHDはクリーンアップされます。ストレージアカウント自体はクリーンアップされません。
    - ベースディスクがストレージアカウントに残っている場合があります。カタログの更新を実行すると、新しいスナップショット（またはACG）ベースディスクが作成されます。
    - カタログ内のすべてのVMが変換され、新しいベースディスクが作成されたら、空のストレージアカウントを削除できます。

必要な権限

アンマネージドディスクからマネージドディスクへの変換を許可するには、Azureサービスプリンシパルで次の権限が必要です。

```
Microsoft.Compute/virtualMachines/convertToManagedDisks/write
```

構成手順

オンデマンドカタログの場合:

1. `UseManagedDisks`を`True`に更新するには、`Set-ProvScheme`（永続VMの場合は`Set-ProvVM`）を実行します。例：

    ```
    Set-ProvScheme -ProvisioningSchemeName "<provscheme-name>"
    -CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
    2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
    instance`"><Property xsi:type=`"StringProperty`"
    Name=`"UseManagedDisks`" Value=`"true`" /></CustomProperties>"
    ```

    ```
    Set-ProvVM -ProvisioningSchemeName "<provscheme-name>" -VMName "<vm-
    name>" -CustomProperties "<CustomProperties xmlns=`"http://
    schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
    www.w3.org/2001/XMLSchema-instance`"><Property
    xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"true`" /
    ></CustomProperties>"
    ```

2. `Set-ProvVMUpdateTimeWindo`w` を実行して更新を適用します。この例では、更新はVMの次回の電源オン時に適用されます。

```
Set-ProvVmUpdateTimeWindow -ProvisioningSchemeName "<provscheme-name>"
-VMName "<vm-name>"
```

3. VMの電源を入れます。

非オンデマンド (レガシー) カタログの場合:

1. 永続VMの場合は`Set-ProvVM`、それ以外の場合は`Set-ProvScheme`を実行して、`Set DeploymentSchema`を`1.1`に構成します。例:

```
Set-ProvScheme -ProvisioningSchemeName "<provscheme-name>"
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`"
Name=`"DeploymentSchema`" Value=`"1.1`" /></CustomProperties>"
```

```
Set-ProvVM -ProvisioningSchemeName "<provscheme-name>" -VMName "<vm-
name>" -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"><Property
xsi:type=`"StringProperty`" Name=`"DeploymentSchema`" Value=`"1.1`" /
></CustomProperties>
```

2. `Set-ProvVMUpdateTimeWindow`を実行して更新を適用します。この例では、更新はVMの次回の電源投入時に適用されます。

```
Set-ProvVmUpdateTimeWindow -ProvisioningSchemeName "<provscheme-name>"
-VMName "<vm-name>"
```

3. VMの電源を入れます。

トラブルシューティング

VMがアンマネージドディスクからマネージドディスクへの変換に失敗した場合:

- `UseManagedDisks`または`DeploymentSchema`のカスタムプロパティが正しく設定されていることを確認します:
  - `Set-ProvScheme`を使用している場合は、`Get-ProvScheme`を実行してProvSchemeカスタムプロパティを確認します。詳細については、Get-ProvSchemeを参照してください。

  - `Set-ProvVM`を使用している場合は、`Get-ProvVMConfiguration`を実行して、VMが更新されたカスタムプロパティを持つ新しい構成になっていることを確認します。詳細については、Set-ProvVMを参照してください。

- Azureサービスプリンシパルに次の権限があることを確認します:
  - `Microsoft.Compute/virtualMachines/convertToManagedDisks/write`
- `Get-ProvOperationEvent`を実行して、プロビジョニングスキームの警告を表示します。詳細については、Get-ProvOperationEventを参照してください。例:

```
Get-ProvOperationEvent -LinkedObjectType ProvisioningScheme
-LinkedObjectUid <your-provscheme-id>
```

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成を案内します。
- 構成プロセス全体を確認するには、「」(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure.html)を参照してください。
- カタログを管理するには、「」(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/machine-catalogs-manage.html)および「」(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/machine-catalogs-manage/manage-machine-catalog-azure.html)を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マイクロソフト Azure リソース マネージャーへの接続
- マシンカタログの作成

Microsoft System Center Virtual Machine Managerカタログを作成する

(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/machine-catalogs-create.html)では、マシンカタログを作成するウィザードについて説明しています。以下の情報は、Microsoft System Center Virtual Machine Manager (VMM) 仮想化環境に固有の詳細を扱っています。

> **注:**

> VMMカタログを作成する前に、VMMへの接続の作成を完了する必要があります。(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/connections/connection-mscvmm.html)を参照してください。

マスターVMを作成する

1. マスターVMにVDAをインストールし、パフォーマンスを向上させるためにデスクトップを最適化するオプションを選択します。
2. バックアップとして使用するために、マスターVMのスナップショットを作成します。
3. 仮想デスクトップを作成します。

SMB 3ファイル共有上のMCS

VMストレージ用のSMB 3ファイル共有でMCSを使用して作成されたマシンカタログの場合、資格情報が次の要件を満たしていることを確認してください。これらの要件により、ControllerのHypervisor Communications Library（HCL）からの呼び出しがSMBストレージに正常に接続されます。

- VMMユーザーの資格情報には、SMBストレージへの完全な読み取り/書き込みアクセス権が含まれている必要があります。
- VMライフサイクルイベント中のストレージ仮想ディスク操作は、VMMユーザー資格情報を使用してHyper-Vサーバー経由で実行されます。

SMBストレージを使用する場合は、Controllerから個々のHyper-Vマシンへの認証資格情報セキュリティサポートプロバイダー（CredSSP）を有効にします。このプロセスは、Windows Server 2012上のHyper-VとVMM 2012 SP1で使用します。詳細については、CTX137465を参照してください。

HCLは`CredSSP`を使用してHyper-Vマシンへの接続を開きます。この機能は、Kerberosで暗号化されたユーザー資格情報をHyper-Vマシンに渡します。リモートHyper-Vマシン上のセッションでの**PowerShell**コマンドは、提供された資格情報で実行されます。この場合、ストレージへの通信コマンドが正しく機能するように、VMMユーザーの資格情報が使用されます。

次のタスクでは、HCLで生成され、SMB 3.0ストレージに対して動作するためにHyper-Vマシンに送信されるPowerShellスクリプトを使用します。

- **マスターイメージの統合**: マスターイメージは、MCSプロビジョニングスキーム（マシンカタログ）を作成します。マスターVMをクローンしてフラット化し、新しく作成されたディスクからVMを作成できるようにします（元のマスターVMへの依存関係を削除します）。

root\\virtualization\\v2名前空間のConvertVirtualHardDisk

例:

```
$ims = Get-WmiObject -class $class -namespace "root\\virtualization\\v2";

$result = $ims.ConvertVirtualHardDisk($diskName, $vhdastext)

$result
```

- **差分ディスクの作成:** マスターイメージを統合して生成されたマスターイメージから差分ディスクを作成します。その後、差分ディスクは新しいVMに接続されます。

  root\\virtualization\\v2名前空間のCreateVirtualHardDisk

  例:

```
$ims = Get-WmiObject -class $class -namespace "root\\virtualization\\v2";

$result = $ims.CreateVirtualHardDisk($vhdastext);

$result
```

- **IDディスクのアップロード:** HCLはIDディスクをSMBストレージに直接アップロードできません。そのため、Hyper-VマシンがIDディスクをストレージにアップロードしてコピーする必要があります。Hyper-VマシンはControllerからディスクを読み取ることができないため、HCLはまず次のようにHyper-Vマシン経由でIDディスクをコピーする必要があります。

  a. HCLは、管理者共有を介してIDをHyper-Vマシンにアップロードします。
  b. Hyper-Vマシンは、PowerShellリモートセッションで実行されているPowerShellスクリプトを介して、ディスクをSMBストレージにコピーします。Hyper-Vマシン上にフォルダーが作成され、そのフォルダーのアクセス許可はVMMユーザーのみにロックされます（リモートPowerShell接続を介して）。
  c. HCLは、管理者共有からファイルを削除します。
  d. HCLがIDディスクのHyper-Vマシンへのアップロードを完了すると、リモートPowerShellセッションはIDディスクをSMBストレージにコピーします。その後、Hyper-Vマシンから削除します。

  IDディスクフォルダーは、削除された場合でも再利用できるように再作成されます。

- **IDディスクのダウンロード:** アップロードと同様に、IDディスクはHyper-Vマシンを経由してHCLに渡されます。次のプロセスでは、Hyper-Vサーバー上にVMMユーザー権限のみを持つフォルダーが存在しない場合に作成します。

  a. Hyper-Vマシンは、PowerShellスクリプトを介してSMBストレージからローカルのHyper-Vストレージにディスクをコピーします。このスクリプトは、PowerShell V3リモートセッションで実行されます。

  b. HCL は、Hyper-V マシンの管理者共有からディスクをメモリに読み込みます。

  c. HCL は、管理者共有からファイルを削除します。

マシンプロファイルを使用してカタログを作成する

System Center Virtual Machine Manager (SCVMM) 環境では、マシンプロファイルを使用して MCS マシンカタログを作成および更新できます。vTPM を有効にできます。また、マシンプロファイル VM のカスタムタグをプロビジョニングされた VM に追加することもできます。

重要な考慮事項

- マスターイメージはスナップショットのみで、VM にすることはできません。
- マシンプロファイルのソースとして使用できるのは VM のみです。
- Hyper-V コンソールから VTPM を構成できますが、SCVMM コンソールからは構成できません。
- マスターイメージで vTPM が有効になっている場合は、マシンプロファイルソースで vTPM を有効にする必要があります。
- vTPM は第2世代のマシンでのみサポートされています。
- 次のパラメーターは、個別に指定された場合、マシンプロファイルでキャプチャされた値を上書きします。
  - VMCpuCount
  - VMMemoryMB
  - ディスクストレージ
- カスタムタグは、マスターイメージからではなく、マシンプロファイルからのみ継承されます。`CitrixProvisioningSchemeId`タグは、デフォルトでVMに追加されます。`CitrixProvisioningSchemeId`タグを含めたくない場合は、ホスティングユニットの作成時に`-NoVmTagging`パラメーターを追加します。例:

```
New-Item -HypervisorConnectionName  $ConnectionName `

    -NetworkPath @($NetworkPath) `

    -Path @($HostingUnitPath) `

    -PersonalvDiskStoragePath @() `

    -RootPath $RootPath `

    -StoragePath @($StoragePath) `

    -NoVmTagging

    ```
```

- 既存のカタログは、`Set-ProvScheme`コマンドを使用して更新できます。
- MCSIO が有効になっている場合、MCS カタログの作成後にメモリとディスクキャッシュのサイズを更新できます。

マシンプロファイルを使用してマシンカタログを作成する

1. マシンプロファイルのソースとなるVMを作成します。詳しくは、「VMMファブリックでの仮想マシンのプロビジョニング」を参照してください。**世代**は一度選択すると変更できません。SCVMMでは、次のことができます。
    - vTPMを有効にするには：
        a. VMを作成したら、Hyper-Vホストにログオンし、**Hyper-Vマネージャー**でVMを見つけます。
        b. VMを右クリックし、**設定**に移動します。
        c. **セキュリティ**で、**トラステッドプラットフォームモジュールを有効にする**チェックボックスをオンにします。
2. **PowerShell**ウィンドウを開きます。
3. Citrix固有のPowerShellモジュールをロードするために`asnp citrix®*`を実行します。
4. Brokerカタログを作成します。このカタログには、これから作成されるマシンが格納されます。
```

5. IDプールを作成します。これは、作成されるマシン用に作成されたADアカウントのコンテナになります。
6. マシンプロファイルを使用してプロビジョニングスキームを作成します。例：

```
New-ProvScheme -HostingUnitName "<hostingunit name>"

-IdentityPoolName "ID1" -MasterImageVM "XDHyp:\HostingUnits\HU1\<path
to the checkpoint/snapshot>"

-ProvisioningSchemeName "<catalogname>"  -MachineProfile "XDHyp:\<path
to the machine profile VM>"
```

7. プロビジョニングスキームの一意のIDでBrokerカタログを更新します。
8. カタログにVMを作成して追加します。

既存のカタログを更新する

Set-ProvSchemeコマンドを使用して、既存のカタログを更新できます。例：

```
Set-ProvScheme -ProvisioningSchemeName "<catalogname>" -MachineProfile
"XDHyp:\<path to the machine profile VM>"
```

VMを削除する

カタログから VM を削除することを選択できますが、SCVMM から VM を削除することはできません。この場合、`CitrixProvisioningSchemeId` タグは VM からのみ削除されます。カスタムタグは VM から削除されません。Web Studio または PowerShell コマンドを使用して VM を削除できます。

WEB STUDIO を使用して VM を削除する

1. VMを選択して右クリックします。
2. **削除**をクリックします。
3. **仮想マシンをカタログから削除しますが、仮想マシンは削除しません**を選択します。

POWERSHELLコマンドの使用

`ForgetVM` パラメーターを指定した `Remove-ProvVM`。詳細については、以下を参照してください。

- タグを削除する
- ハイパーバイザーアクセスなしでマシンを削除する

次のステップ

- これが最初に作成されたカタログである場合、Web Studio は デリバリーグループの作成 に誘導します
- 構成プロセス全体を確認するには、インストールと構成 を参照してください
- カタログを管理するには、マシンカタログの管理 および Microsoft System Center Virtual Machine Manager カタログの管理 を参照してください

詳細情報

- 接続とリソースの作成および管理
- マイクロソフト システムセンター バーチャルマシンマネージャー への接続
- マシンカタログの作成

Nutanixカタログを作成する

「(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/machine-catalogs-create.html)」では、マシンカタログを作成するウィザードについて説明します。以下の情報は、Nutanix仮想化環境に固有の詳細を扱っています。

> **注:**
>
> Nutanixカタログを作成する前に、Nutanixへの接続の作成を完了する必要があります。「(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/connections/connection-nutanix.html)」を参照してください。

Nutanixマシンテンプレートバージョンを使用してマシンカタログを作成する

Citrix管理のNutanix AHV Prism Centralホスト接続を使用してMCSプロビジョニングされたマシンカタログを作成する場合、ベースイメージはNutanix VMテンプレートバージョンから作成されます。主な利点は、Nutanix Prism CentralがVMテンプレートを複数のクラスターで使用できるようにすることです。その結果、Citrix管理者は、それらのカタログが異なるNutanixクラスター上にある場合でも、単一のNutanix VMテンプレートバージョンを複数のMCSマシンカタログのマスターVMとして使用できます。

マシンプロファイルのソースとしてテンプレートバージョンを選択することもできます。マスターイメージのテンプレートバージョンは、新しいカタログのマシンプロファイルとしてデフォルトで設定されます。ただし、マシンプロファイルのテンプレートバージョンを変更できます。以下のハードウェアプロパティは、マシンプロファイルから取得されます：CPU、メモリ、ソケットあ

たりのコア数、GPU、およびカテゴリ。オプションで、CPU、メモリ、ソケットあたりのコア数のプロパティを指定して、選択したマシンプロファイルの設定を上書きすることもできます。

> **注:**
>
> カテゴリは、仮想マシン、クラスター、イメージなどのエンティティをグループ化および管理し、ポリシーと自動化を適用するために使用されるキーと値のペアです。

> カタログを作成する前に、マスターVMを作成し、Nutanix Prism CentralでVMテンプレートバージョンに変換します。手順については、Nutanixのドキュメントを参照してください。

次のような方法でカタログを作成できます。

- Web Studio。既存のVMを使用してカタログを作成することもできます。既存のマシン（電源管理）を使用してマシンカタログを作成するを参照してください。
- 「(#create-a-machine-catalog-using-powershell-commands)」

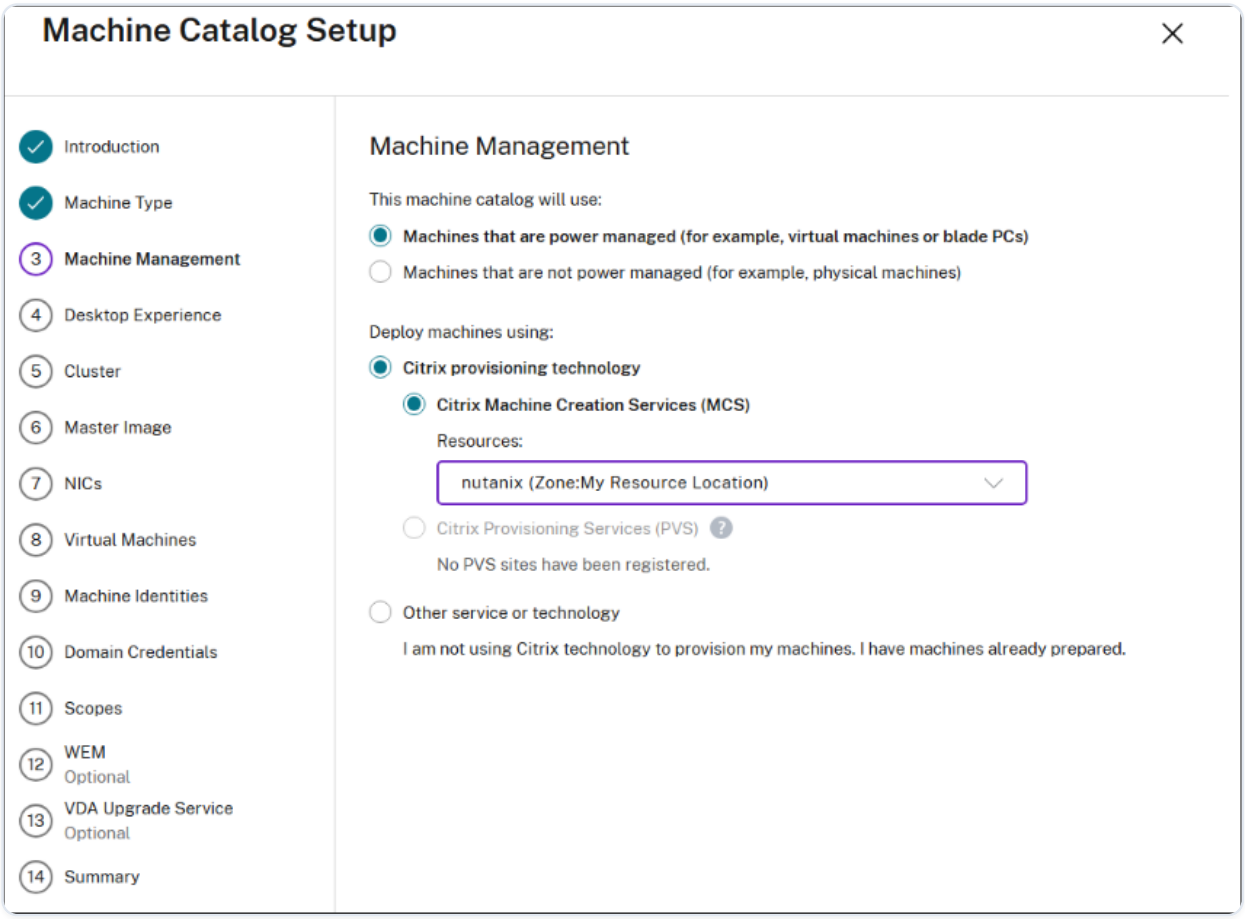
制限事項

- 複数のNICを同じサブネットに接続することはサポートされていません。
- Nutanixの制限により、MCSプロビジョニングされた各マシンカタログには、オーバーレイネットワーク、VLANベーシックサブネット、VLANサブネットの中から単一タイプのネットワークのNICのみを割り当てることができます。
- 特定のシナリオでは、非永続マシンカタログのMCSマスターイメージを更新すると、潜在的な問題が発生する可能性があります。「(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/security-policies/secure-boot.html#secure-boot-and-vtpm-in-nutanix-prism-central)」を参照してください。
- Nutanix VMテンプレートをマスターイメージとして選択する場合、テンプレート名またはテンプレートバージョン名に「#」や「&」などの文字を含めることはできません。

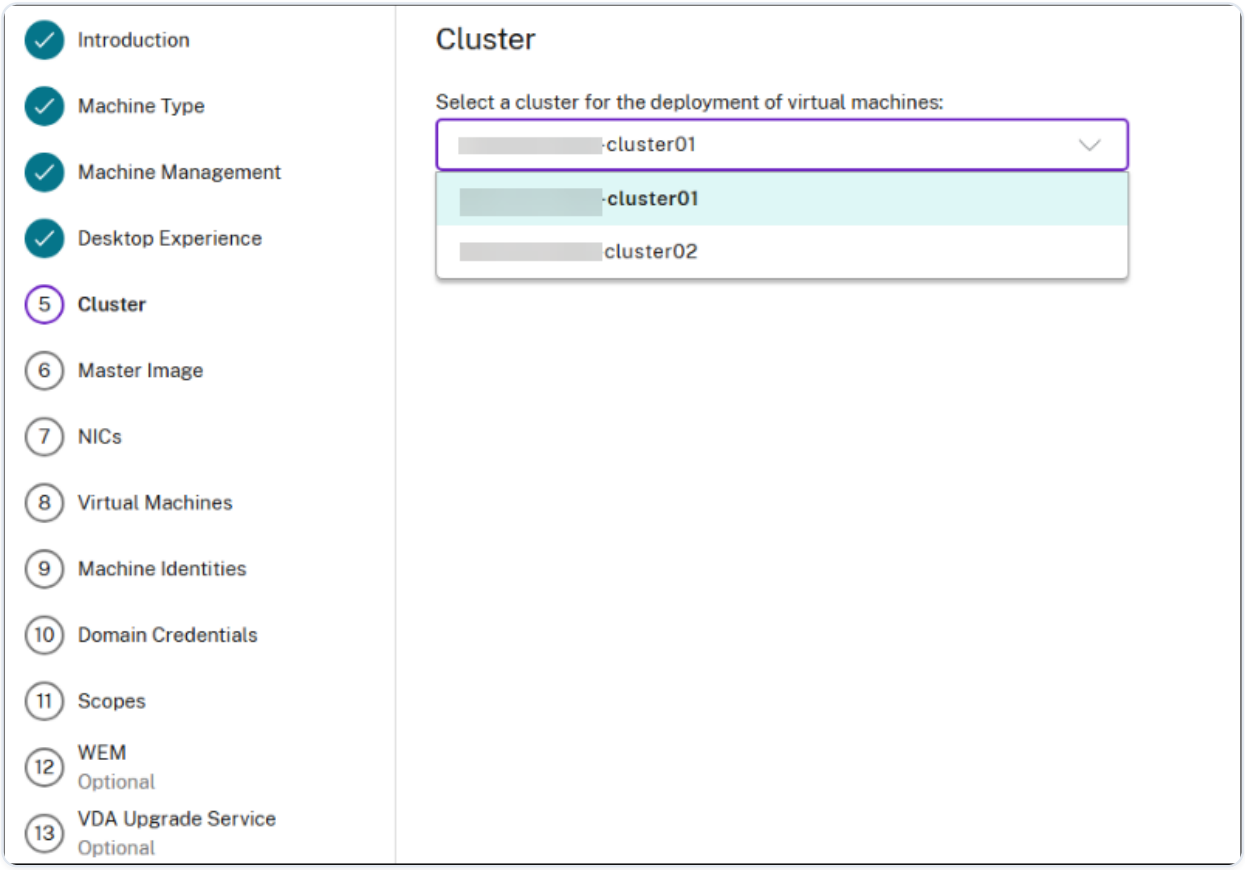
Web Studioを使用してマシンカタログを作成する

マシンカタログセットアップウィザードで：

1. **マシンタイプ**ページで、**マルチセッションOS**、**シングルセッションOS**、または**リモートPCアクセス**を選択します。
2. **マシン管理**ページで、展開方法として**電源管理されているマシン**と**Citrix Machine Creation Services™**を選択します。**リソース**を選択します。

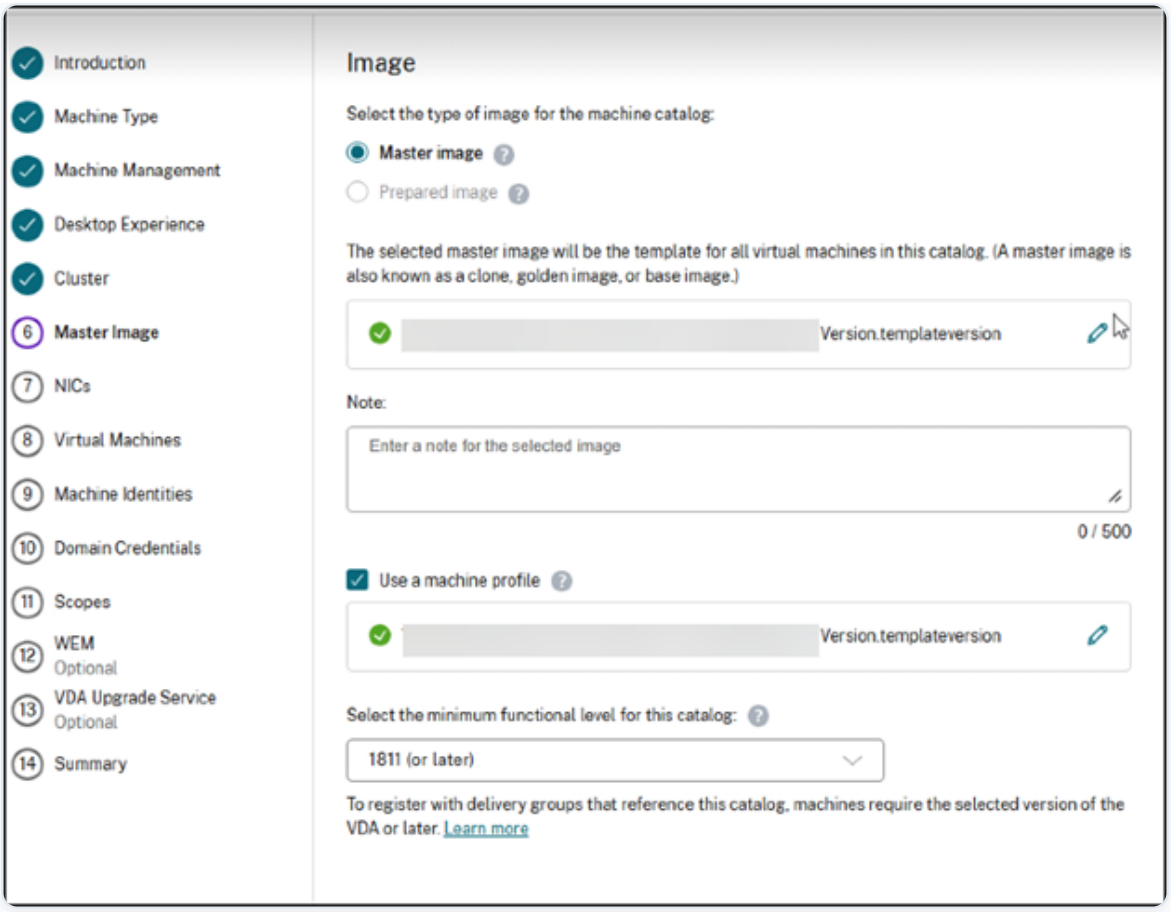


3. **デスクトップエクスペリエンス**ページで、2つのオプションのいずれかを選択します。
4. **クラスター**ページで、VMの展開に使用するクラスターを選択します。

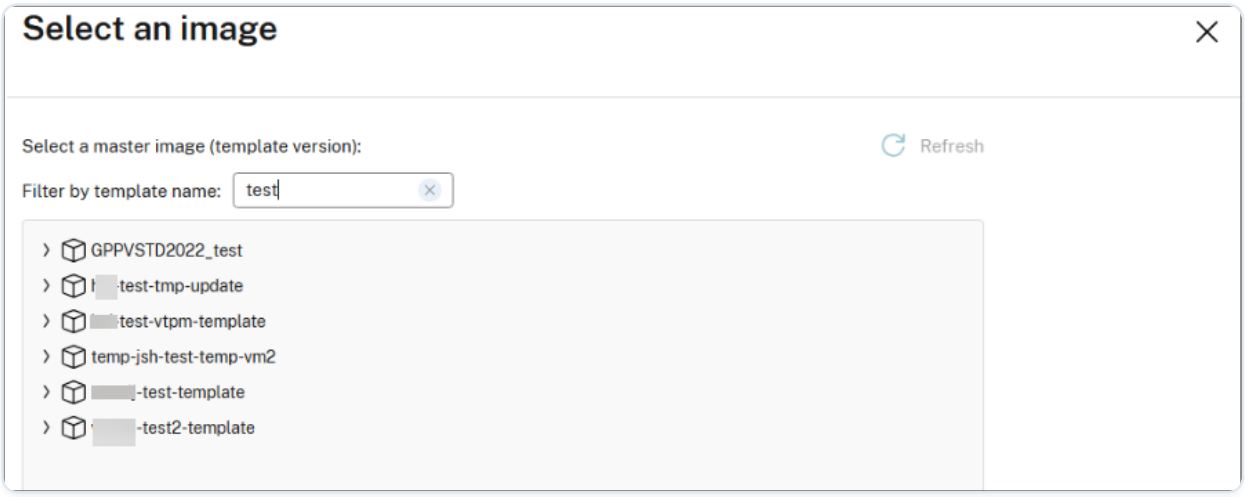


5. **マスターイメージ**ページで、**マスターイメージ**をクリックし、マスターイメージ（テンプレートバージョン）を選択します。マシンテンプレートを名前でフィルタリングできます。マスターイメージのテンプレートバージョンは、新しいカタログのマシンプロファイルとしてデフォルトで設定されます。ただし、マシンプロファイルのテンプレートバージョンを変更できます。

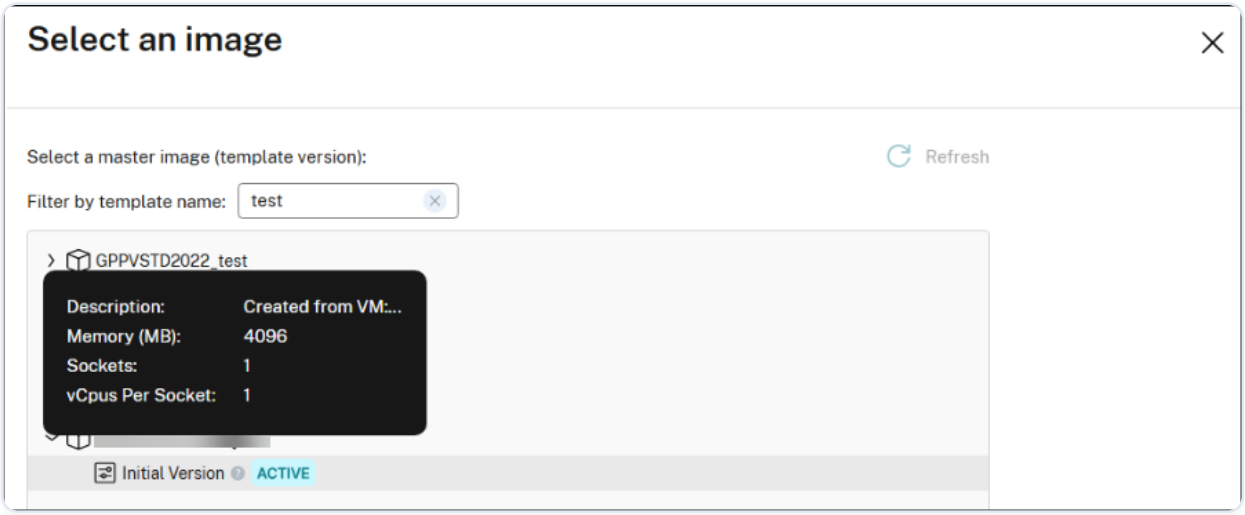
> **注:**
>
> 複数のMCSマシンカタログに対して、たとえそれらのカタログが異なるNutanixクラスター上にある場合でも、単一のNutanix VMテンプレートバージョンをマスターVMとして使用できます。



マシンテンプレートを名前でフィルタリング：

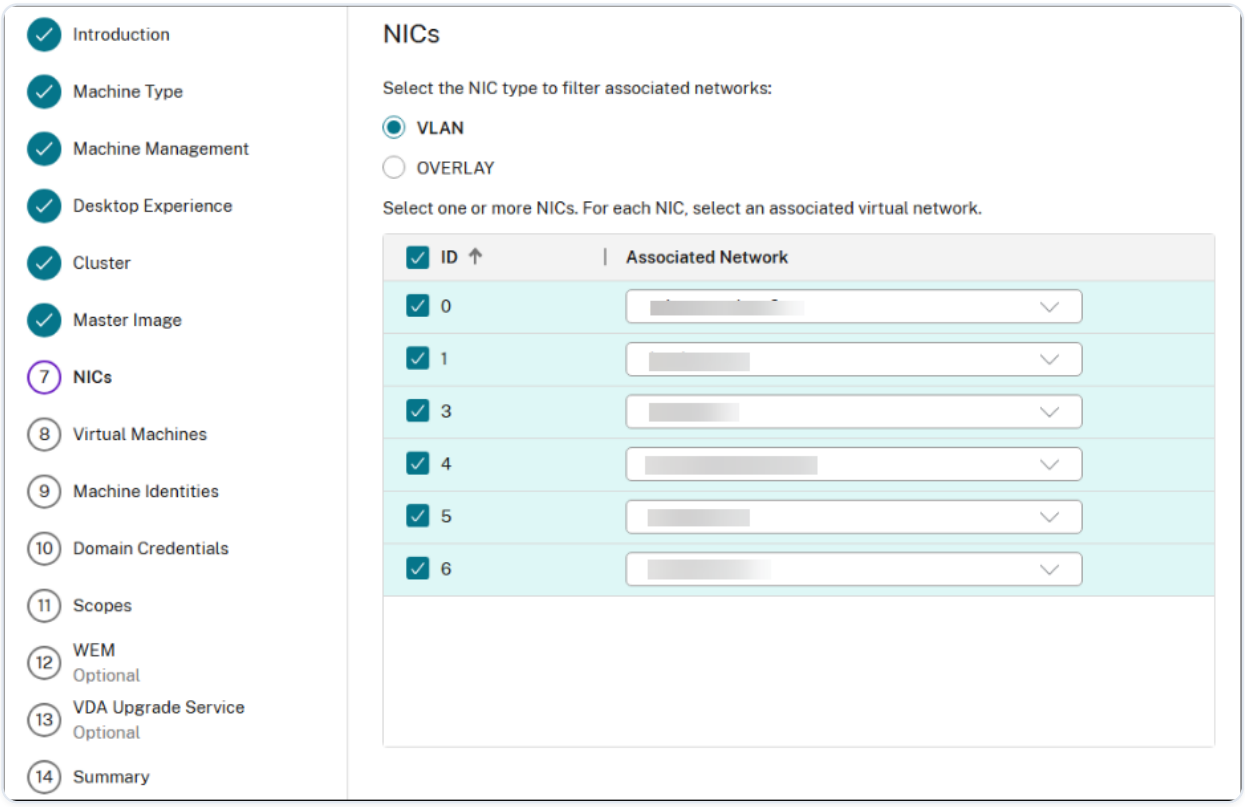


テンプレートの説明を参照してください:



6. **NIC**ページで:

   - 関連するネットワークをフィルタリングするためにNICタイプを選択します。
   - マスターイメージに含まれる1つ以上のNICを選択し、各NICに関連付けられた仮想ネットワークを選択します。



7. **仮想マシン**ページで、作成する仮想マシンの数を示し、各マシンの合計メモリ (MB)、仮想CPU、およびCPUあたりのコア数を構成します。これらの値は、マシンプロファイルから自動的に入力されます。
8. **概要**ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。**完了**をクリックします。

マシンプロファイルのエクスポート

マシンカタログで使用されているマシンプロファイルをJSONファイルにエクスポートできます。

1. マシンカタログを選択し、**テンプレートプロパティ**タブに移動します。
2. **マシンプロファイル**の詳細の下で、**最終バージョン**の横にある**エクスポート**をクリックします。

PowerShellコマンドを使用してマシンカタログを作成する

1. PowerShell ウィンドウを開きます。
2. `asnp citrix*` を実行します。
3. まだ作成されていない場合は、ID プールを作成します。例:

```
New-AcctIdentityPool    -Domain "<string>" -IdentityPoolName "<string>"
-IdentityType "ActiveDirectory"  -NamingScheme "DemoVM-##"
-NamingSchemeType "Numeric" -ZoneUid "GUID" -Scope @()
```

4. プロビジョニングスキームを作成します。

   例: マシンプロファイルなしの場合

```
New-ProvScheme -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"><Property
xsi:type=`"StringProperty`" Name=`"ClusterId`"
Value=`"00062c63-1fb0-58c9-4fc8-5c2573352378`" /><Property
xsi:type=`"StringProperty`" Name=`"CPUCores`" Value=`"1`" /></
CustomProperties>" -HostingUnitName "<Hosting unit name>"
-IdentityPoolName "<string>" -InitialBatchSizeHint 1  -MasterImageVM
"XDHyp:\HostingUnits\<Hosting Unit Name>\Templates.folder\<template
name>.template\<template version name>.templateversion" -NetworkMapping
@{"5"="XDHyp:\HostingUnits\<Hosting unit name>\Clusters.folder\<Cluster
Name>.cluster\<Network name>.network"} -ProvisioningSchemeName
"<Catalog name>" -ProvisioningSchemeType "MCS" -RunAsynchronously
-Scope @() -VMCpuCount 2 -VMMemoryMB 10240
```

   例: マシンプロファイルありの場合

   マシンプロファイルを使用して、テンプレートバージョンからハードウェアプロパティをキャプチャし、プロビジョニングされたVMに適用します。マシンプロファイルを指定しない場合、ハードウェアプロパティはマスターイメージのテンプレートバージョンからキャプチャされます。

   注:

   - OSディスク、vTPM、およびセキュアブートのプロパティは、マシンプロファイルが使用されている場合でも、常にマスターイメージからキャプチャされます。
   - OSディスクはマシンプロファイルから読み取られないため、ディスクレスVMを作成し、それをマシンプロファイルに使用できるテンプレートバージョンに変換できます。
   - マシンプロファイルテンプレートバージョンの完全なJSON仕様が保存されているため、Prism Centralからテンプレートバージョンを削除してもVMを作成できます。

   マシンプロファイルからキャプチャされるプロパティは次のとおりです。

プロパティ	APIでのプロパティ名 (GETTEMPLATEVERSIONBYID)	コメント/参照
CPU	numSockets	
RAM	memorySizeBytes	
コア	numCoresPerSocket	
カテゴリ	カテゴリ	カテゴリ管理
GPU	GPU	GPU概要ビュー
コアあたりのスレッド数	numThreadsPerCore	aCLI-VM
NUMAノード	numNumaNodes	
VCPUハードピンニングを有効にする	isVcpuHardPinningEnabled	
CPUパススルーを有効にする	isCpuPassthroughEnabled	
メモリオーバーコミットを有効にする	isMemoryOvercommitEnabled	Prism Central (AHV) を使用した VM の作成
GPUコンソールアクセスを有効にする	isGpuConsoleEnabled	
CPUホットプラグを有効にする	isCpuHotplugEnabled	
SCSIコントローラーを有効にする	isScsiControllerEnabled	
タイムゾーン	hardwareClockTimezone	Prism Central (AHV) を使用した VM の作成
AHV ブランディングを有効にする	isBrandingEnabled	

プロパティ	APIでのプロパティ名 (GETTEMPLATEVERSIONBYID)	コメント/参照
VGA コンソールを有効にする	isVgaConsoleEnabled	
VM	isAgentVm	Prism Central (AHV) を使用した VM の作成

注:

同じマスターイメージテンプレートバージョンを使用して、さまざまなマシンプロファイルを持つ異なるカタログを作成できます。それぞれが上記の異なるプロパティセットを備えています。たとえば、Nutanix ポリシーにリンクできる異なるカテゴリを割り当てたり、CPU/メモリを調整したり、メモリオーバーコミット設定を変更したり、複数の GPU を追加または削除したりできます。

`CustomProperties` 内の `VMCpuCount`、`VMMemoryMB`、`CPUCores` などのコマンドラインパラメータは、指定することができ、マシンプロファイルテンプレートバージョンからのこれらのパラメータの値よりも優先されます。指定されていない場合、これらは指定されたマシンプロファイルから読み取られます。

```
$customProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <StringProperty Name="ClusterId"
Value="00062c63-1fb0-58c9-4fc8-5c2573352378" />

    <StringProperty Name="CPUCores" Value="2" />

</CustomProperties>

"@
```

```
New-ProvScheme -HostingUnitName "<Hosting unit name>" `

           -IdentityPoolName "<string>" `

           -InitialBatchSizeHint 1 `

           -MasterImageVM "XDHyp:\HostingUnits\<Hosting Unit
Name>\Templates.folder\<template name>.template\<template version
name>.templateversion" `

           -MachineProfile "XDHyp:\HostingUnits\<Hosting Unit
Name>\Templates.folder\<template name for machine
profile>.template\<template version name>.templateversion" `

           -NetworkMapping @{"0"="XDHyp:\HostingUnits\<Hosting unit
name>\Clusters.folder\<Cluster Name>.cluster\<Network name>.network"} `

           -ProvisioningSchemeName "<Catalog name>" `

           -ProvisioningSchemeType "MCS" `

           -CustomProperties $customProperties `

           -RunAsynchronously `

           -VMCpuCount 2 `

           -Scope @()
```

5. プロビジョニングスキームをブローカーカタログとして登録します。例:

```
New-BrokerCatalog -AllocationType "Random" -IsRemotePC $False  -
MinimumFunctionalLevel "L7_20" -Name "<Catalog Name>"
-PersistUserChanges "Discard" -ProvisioningType "MCS"    -
SessionSupport "MultiSession" -ZoneUid "GUID"  -ProvisioningSchemeId
fe7df345-244e-4xxxx-xxxxxxxxx `  -Scope @()
```

既存のマシンを使用してマシンカタログを作成する (電源管理対象)

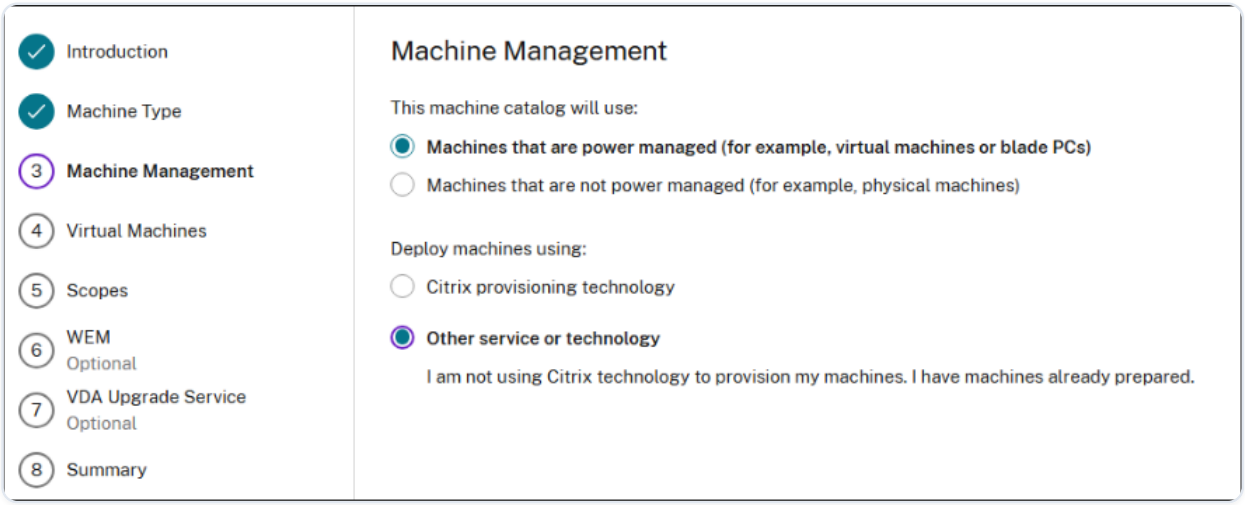
既存のマシン（電源管理対象）を使用してマシンカタログを作成できます。

- ウェブスタジオ
- PowerShell

Web Studioを使用して既存のマシン（電源管理）でマシンカタログを作成する

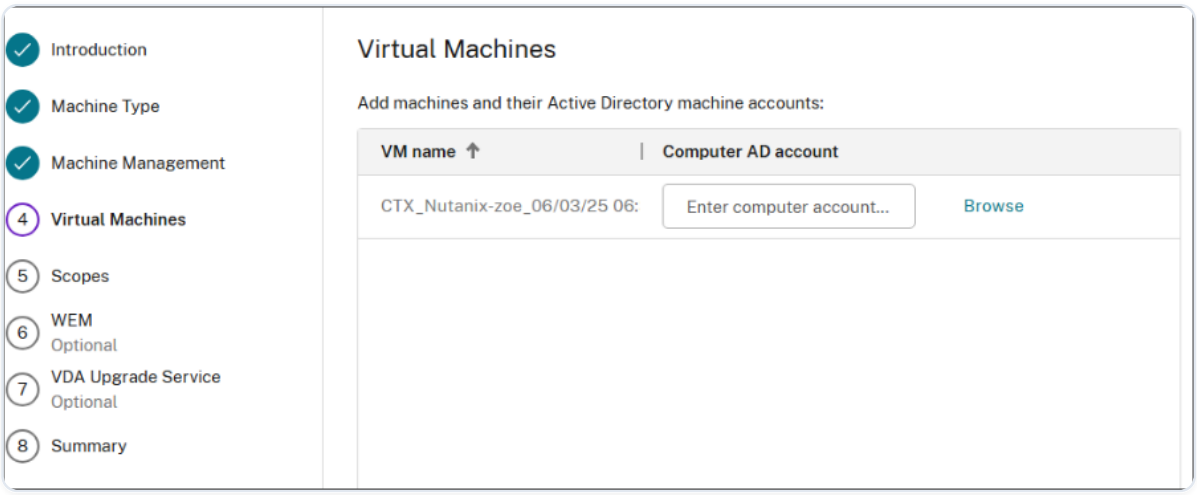
マシンカタログセットアップウィザードで：

1. **オペレーティングシステム**ページで、**マルチセッションOS**または**シングルセッションOS**を選択します。
2. **マシン管理**ページで、**電源管理対象のマシン**と**その他のサービスまたはテクノロジー**を選択します。



3. **仮想マシン**ページで、マシンとそのActive Directoryマシンアカウントを追加します。次のいずれかを実行できます。

   - をクリックして、マシンを一括追加します。
   - **マシンの追加**をクリックして、マシンを手動で追加します。**VMの選択**ウィンドウが表示されます。以前に作成したNutanix AHV Prism Central接続を展開し、追加するVMを選択します。次に、関連するマシンアカウント名を追加します。



4. **スコープ**ページと**概要**ページには、Nutanix AHV Prism Centralに固有の情報は含まれていません。

PowerShell を使用して既存のマシン（電源管理対象）でマシンカタログを作成する

1. PowerShellウィンドウを開きます。
2. `asnp citrix*`を実行します。
3. ユーザーに割り当てられる電源管理されたVMを持つカタログを作成します。例:

```
New-BrokerCatalog -AllocationType "Permanent"  -IsRemotePC $False
-MachinesArePhysical $False  -Name "<Catalog Name>" -PersistUserChanges
"OnLocal" -ProvisioningType "Manual" -Scope @() -SessionSupport
"SingleSession" -ZoneUid "fb202053-8c35-4db2-a299-a8d9538ec6be"
```

4. カタログにVMを追加します。例:

```
New-BrokerMachine  -CatalogUid 6 -HostedMachineId "d859caf3-4bf0-447b-
b012-8af0594c7d88" -HypervisorConnectionUid 1 -IsReserved $False  -
MachineName "S-1-5-21-1334627847-1250330507-3910179295-100245"
```

Nutanixスナップショットを使用してマシンカタログを作成する

このセクションでは、Nutanix Acropolis (Prism Element) ホスト接続を使用してMCSプロビジョニングされたマシンカタログを作成する方法について説明します。カタログを作成する前に、Nutanixでマスターイメージとスナップショットを作成してください。詳細については、Nutanixのドキュメントを参照してください。

マシンカタログセットアップウィザードで:

- **Container**または**Cluster and Container**ページはNutanix固有のものです。
  - Nutanix AHV XIをリソースとして使用してマシンを展開する場合、**Container**ページで、VMのIDディスクが配置されるコンテナを選択します。
  - Nutanix AHV PCをリソースとして使用してマシンを展開する場合、**Cluster and Container**ページが表示されます。VMの展開に使用するクラスターを選択し、次にコンテナを選択します。
- **Image**ページで、イメージスナップショットを選択します。必要に応じて、Acropolisコンソールを使用してスナップショットの名前を変更します。スナップショットの名前を変更した場合は、カタログ作成ウィザードを再起動して、更新されたリストを表示します。

- **Virtual Machines**ページで、仮想CPUの数とvCPUあたりのコア数を指定します。
- **NICs**ページで、関連するネットワークをフィルタリングするNICタイプを選択します。このオプションは、Nutanix AHV PC接続でのみ利用可能です。
- **Machine Identities**、**Domain Credentials**、**Scopes**、および**Summary**ページには、Nutanix固有の情報は含まれていません。

制限事項

Nutanixホスト接続（特にNutanix AHVプラグイン2.7.1およびNutanix AHVプラグイン2.5.1）でMCSカタログを作成すると、プロビジョニングされたVMのハードディスクサイズがWeb Studioに誤って表示されます。

- Nutanix AHV プラグイン 2.7.1: 表示されるサイズは、実際のストレージサイズよりも小さい (1 GB)。
- Nutanix AHV プラグイン 2.5.1: 表示されるサイズは、実際のストレージサイズよりも小さい (32 GB)。

ただし、マスターイメージVMがVM内のスナップショットである場合、これは設計どおりに機能します。

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成を案内します。
- 構成プロセス全体を確認するには、インストールと構成を参照してください。
- カタログを管理するには、マシンカタログの管理とNutanixカタログの管理を参照してください。

詳細情報

- 接続とリソースの作成および管理
- Nutanixへの接続
- Nutanixクラウドおよびパートナーソリューションへの接続
- マシンカタログの作成

Oracle C3 マシンカタログを作成する (プレビュー)

(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/machine-catalogs-create.html)は、一般的なマシンカタログのワークフローについて説明しています。以下の情報は、Oracle C3固有の詳細を扱っています。

> **注:**
>
> Oracle C3カタログを作成する前に、以下の前提条件を完了してください:
>
> - Oracle C3への接続(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/connections/connection-oracle-c3.html)。
> - 1つ以上のOracle C3マシンがオンボーディングに利用可能であることを確認してください。
> - それらのマシンを必要なVDAの準備ができた状態にしてください。

Oracle C3マシンカタログは、以下を使用して作成できます:

- ウェブスタジオ
- PowerShellコマンド

Web Studioを使用してマシンカタログを作成する

マシンカタログセットアップウィザードで：

1. **オペレーティングシステム**ページで、**マルチセッションOS**または**シングルセッションOS**を選択します。
2. **マシン管理**ページで、**電源管理されているマシン**と**別のサービスまたはテクノロジー**を選択します。
3. **仮想マシン**ページで、以下のいずれかの方法でマシンと関連するマシンアカウントを追加します:
   - **マシンの追加**を選択して、Oracle C3接続からOracle C3マシンを手動で追加します。
   - **CSVファイルの追加**を選択して、Oracle C3マシンとマシンアカウントのマッピングを一括で追加します。

スコープおよび**概要**ページには、Oracle C3固有の情報は含まれていません。

PowerShellコマンドを使用してマシンカタログを作成する

カタログを作成し、既存のOracle C3マシンをインポートするには、`New-BrokerCatalog` と `New-BrokerMachine` を使用します。

例:

```
New-BrokerCatalog -AllocationType "Random" -ProvisioningType "Manual" `

-SessionSupport "MultiSession" -Name "OracleC3-Catalog" `

-PersistUserChanges "OnLocal"

New-BrokerMachine -CatalogUid <CatalogUid> `

-HostedMachineId <OracleC3MachineId> `

-HypervisorConnectionUid <OracleC3ConnectionUid> `

-MachineName <Domain\MachineAccount>
```

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループを作成するようにガイドします。
- 構成プロセス全体を確認するには、インストールと構成を参照してください。
- 電源管理については、Oracle C3 VMの電源管理を参照してください。

詳細情報

- 接続とリソースの作成および管理
- Oracle C3への接続
- マシンカタログの作成

Red Hat OpenShiftカタログを作成する

「(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/machine-catalogs-create.html)」では、マシンカタログを作成するウィザードについて説明します。以下の情報は、Red Hat OpenShift仮想化環境に固有の詳細を扱っています。

注:

Red Hat OpenShiftカタログを作成する前に、Red Hat OpenShiftへの接続とホスティングユニットの作成を完了してください。「(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/connections/connection-redhat-openshift.html)」を参照してください。

マスターイメージVMを作成する

マシンカタログを作成するには、マスターイメージVMが必要です。

1. ログインIDを使用してOpenShiftコンソールにアクセスします。
2. **Virtualization > VirtualMachines**に移動して、マスターイメージVMを含むVMのリストを表示します。
3. マスターイメージを作成します。マスターイメージを作成する際は、マスターイメージVMにストレージデバイスが1つだけであることを確認してください。

注:

- クラスター環境に対する顧客の要件に従って、ルーティング可能なNADがマスターイメージVMに追加されていることを確認してください。
- マスターイメージがドメインに参加している場合、カタログ作成に使用された後にドメイン信頼を失う可能性があります。この問題は、OpenShift環境の制限により、Citrix Virtual Apps and Desktops™ 2503に影響します。回避策は、マスターイメージでドメインに参加しないことです。CitrixはRed Hatと協力して、ネットワーク分離機能を強化しています。
- Red Hat OpenShift仮想化環境でMCSマシンカタログを作成する場合、異なるオペレーティングシステムタイプを持つマスターイメージとマシンプロファイルを使用することはできません。これは、Red Hat OpenShiftが各OSタイプを管理する方法によるものです。したがって、Windows VMをマスターイメージとして、非Windows（例：Linux）VMをマシンプロファイルとして使用すること、またはその逆はサポートされていません。

- 現在、`InstanceType`を使用して作成されたVMは、マスターイメージとしてサポートされていません。

カタログを作成する

OpenShift環境でマシンを作成、配信、電源管理するためにOpenShiftカタログを作成できます。

- Web Studio を使用してカタログを作成する(#create-a-catalog-using-web-studio)
- PowerShellコマンドを使用してカタログを作成する(#create-a-catalog-using-powershell-commands)

Web Studioを使用してカタログを作成する

Web Studioを使用して、マシンプロファイルありまたはなしでRed Hat OpenShift環境にMCSマシンカタログを作成できます。VMはマシンプロファイルの入力として使用されます。

マシンカタログセットアップウィザードで：

1. **オペレーティングシステム**ページで、**マルチセッションOS**または**シングルセッションOS**を選択します。
2. マシン管理ページで：
   - **「電源管理されているマシン（仮想マシンやブレードPCなど）」**を選択します。
   - **Citrixプロビジョニングテクノロジー Citrix Machine Creation Services™ (MCS)**を使用してマシンを展開することを選択します。
   - Citrix Machine Creation Services (MCS)の下にあるOpenshiftホスティングユニットを選択します。
3. **デスクトップエクスペリエンス**ページで、**マシンタイプ**ページで選択したマシンタイプに応じてオプションを選択します。
4. **イメージ**ページで：
   a. マスターイメージを選択します。現在、Openshiftは準備済みイメージをサポートしていません。
   b. 選択したイメージにメモを追加できます。
   c. 「マシンプロファイルを使用」チェックボックスを選択し、マシンプロファイルを選択できます。
   d. 最新の製品機能を使用できるように、マスターイメージに最新のVDAバージョンがインストールされていることを確認してください。デフォルトの最小VDA選択を変更しないでく

ださい。ただし、以前のVDAバージョンを使用する必要がある場合は、「VDAバージョンと機能レベル」を参照してください。

5. 「**NIC**」ページで、1つ以上のNICを選択し、各カードに仮想ネットワークを関連付けます。
6. 「**仮想マシン**」ページで：

   a. 作成する仮想マシンの数を指定します。作成しない場合は0（ゼロ）を入力します。後で、マシンを追加して空のカタログのVMを作成できます。

   b. 各 VM が持つメモリ量 (MB 単位) を選択します。

   c. ランダムな非永続カタログを作成している場合、I/Oパフォーマンスを向上させるために、マシンのライトバックキャッシュを有効にできます。「一時データのキャッシュを構成する」を参照してください。

7. 画面の指示に従って、OpenShift固有の情報を含まない残りの手順を完了します。

Studioを使用してOpenShiftカタログを作成し、OpenShift環境内の既存のマシンの能力を提供および管理することもできます。次の手順を実行します。

マシンカタログセットアップウィザードで：

1. **オペレーティングシステム**ページで、**マルチセッションOSまたはシングルセッションOS**を選択します。
2. **マシン管理**ページで、**電源管理されているマシンと別のサービスまたはテクノロジ**を選択します。
3. 「**仮想マシン**」ページで、マシンとそれらのActive Directoryマシンアカウントを追加します。次のことができます。

   - *マシンを手動で追加する*：「**マシンを追加**」をクリックして、マシンを手動で追加します。「**VMの選択**」ウィンドウが表示されます。以前に作成したOpenShift接続を展開し、追加するノード（VM）を選択します。次に、関連するマシンアカウント名を追加します。
   - *CSVファイルを使用してマシンを追加する*：「**CSVファイルを追加**」をクリックして、マシンを一括で追加します。CSVファイルを使用してマシンを追加する方法については、「CSVファイルを使用してマシンをカタログに一括追加する」を参照してください。

4. 画面の指示に従って、OpenShift固有の情報を含まない残りの手順を完了します。

PowerShellコマンドを使用してカタログを作成する

PowerShell コマンドを使用して、Red Hat OpenShift 環境に MCS マシンカタログを作成できます。マシンプロファイルを使用しても使用しなくても、マシンカタログを作成できます。VM はマシンプロファイルの入力として使用されます。

1. PowerShellウィンドウを開きます。
2. `asnp citrix*`を実行します。
3. PowerShellコマンドを実行して、以下を行います。
    a. IDプールを作成する
    b. ADアカウントを作成する
    c. マシンプロファイルを使用しても使用しなくても、永続VMを持つMCSマシンカタログを作成する。
    d. カタログにVMを追加する
    e. ブローカーカタログを作成する
    f. 新しいVMにブローカーマシンを追加する

以下はスクリプトの例です。

IDプールを作成する

```
New-AcctIdentityPool `

    -IdentityPoolName "IdentityPoolName" `

    -ZoneUid "00000000-0000-0000-0000-000000000000" `

    -NamingScheme "vm###" `

    -NamingSchemeType "Numeric" `

    -AllowUnicode `

    -Domain "MyDomain.local" `

    -AdminAddress "MyDDC.MyDomain.Local"
```

ADアカウントを作成する

```
New-AcctADAccount `

    -IdentityPoolUid "11111111-1111-1111-1111-111111111111" `

    -ADUserName "MyDomain\MyUserName" `

    -ADPassword SecurePassword `
```

```
    -Count 1 `

    -AdminAddress "MyDDC.MyDomain.Local"
```

永続マシンを使用したプロビジョニングスキームを作成する (マシンプロファイルなし)

```
New-ProvScheme `

    -ProvisioningSchemeName "ProvisioningSchemeName" `

    -HostingUnitName "HostingUnitName" `

    -IdentityPoolName "IdentityPoolName" `

    -ProvisioningSchemeType "MCS" `

    -MasterImageVM "XDHyp:
\HostingUnits\HostingUnitName\TargetNamespace.namespace\MasterImageVM.vm"
`

    -NetworkMapping @{"0" = "XDHyp:
\HostingUnits\HostingUnitName\TargetNamespace.namespace\MyNetwork.network"
 } `

    -VMCpuCount 1 `

    -VMMemoryMB 4096 `

    -InitialBatchSizeHint 1 `

    -AdminAddress "MyDDC.MyDomain.Local"
```

永続マシンを使用したプロビジョニングスキームを作成する (マシンプロファイルあり)

```
New-ProvScheme `

    -ProvisioningSchemeName "ProvisioningSchemeName" `

    -HostingUnitName "HostingUnitName" `

    -IdentityPoolName "IdentityPoolName" `
```

```
    -ProvisioningSchemeType "MCS" `

    -MasterImageVM "XDHyp:
\HostingUnits\HostingUnitName\TargetNamespace.namespace\MasterImageVM.vm"
`

    -NetworkMapping @{"0" = "XDHyp:
\HostingUnits\HostingUnitName\TargetNamespace.namespace\MyNetwork.network"
 } `

    -VMCpuCount 1 `

    -VMMemoryMB 4096 `

    -InitialBatchSizeHint 1 `

    -AdminAddress "MyDDC.MyDomain.Local" `

    -MachineProfile "XDHyp:
\HostingUnits\HostingUnitName\TargetNamespace.namespace\MachineProfileVM.v
m"
```

新しいPROVVMを作成する

```
New-ProvVM `

    ProvisioningSchemeName "ProvisioningSchemeName" `

    ADAccountName "MyDomain\vm001" `

    AdminAddress "MyDDC.MyDomain.Local"



Lock-ProvVM `

    -ProvisioningSchemeName "ProvisioningSchemeName" `

    -Tag "Brokered" `

    -VMID "TargetNamespace:vm001"
```

新しいブローカーカタログを作成する

```
New-BrokerCatalog `

    -Name "ProvisioningSchemeName" `

    -ProvisioningType "MCS" `

    -SessionSupport "MultiSession" `

    -AllocationType "Random" `

    -PersistUserChanges "OnLocal" `

    -ZoneUid "00000000-0000-0000-0000-000000000000" `

    -AdminAddress "MyDDC.MyDomain.Local"
```

ブローカーカタログのメタデータを設定する

```
Set-BrokerCatalogMetadata `

    -CatalogId "1" `

    -Name "Citrix_DesktopStudio_IdentityPoolUid" `

    -Value "11111111-1111-1111-1111-111111111111"



Set-BrokerCatalog `

    -Name "ProvisioningSchemeName " `

    -ProvisioningSchemeId "22222222-2222-2222-2222-222222222222"
```

新しいPROVVM用のブローカーマシンを作成する

```
New-BrokerMachine `

    -CatalogUid "33333333-3333-3333-3333-333333333333" `

    -AdminAddress "MyDDC.MyDomain.Local" `
```

```
    -MachineName "S-0-0-00-0000000000-0000000000-000000000-000000"
```

vCPU の計算と CPU トポロジの制約

OpenShift 仮想マシンの CPU 構成を更新すると、プラグインは要求された vCPU 数とマシンプロファイルからの既存の CPU トポロジ（コアとスレッド）に基づいてソケット数を計算します。

使用される式は次のとおりです。

```
sockets = requestedVCpuCount / (cores × threads)
```

要件

- マシンプロファイルのコアとスレッドの値は両方ともゼロより大きい必要があります。
- 要求された vCPU 数は、コア × スレッドの正確な倍数である必要があります。均等に割り切れない場合、更新は拒否されます。
- ソケット値のみが調整され、マシンプロファイルからのコアとスレッドの値はそのまま保持されます。

例

マシンプロファイル	要求された VCPU	計算されたソケット	有効ですか？
コア数=2、スレッド数=2	8	8 / (2×2) = 2	はい
コア=2, スレッド=2	6	6 / (2×2) = 1.5	いいえ
コア=4, スレッド=1	12	12 / (4×1) = 3	はい

既知の制限事項

マシンプロファイルで、コア数 × スレッド数が1より大きいCPUトポロジが定義されている場合、その積の正確な倍数であるvCPU数のみがサポートされます。

プロビジョニングスキームを作成または更新する際は、要求されたvCPU数がマシンプロファイルのトポロジと一致していることを確認してください。

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成を案内します。

- 構成プロセス全体を確認するには、「」(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure.html)を参照してください。
- 電源管理については、Red Hat OpenShift VMの電源管理 を参照してください

詳細情報

- 接続とリソースを作成および管理する
- Red Hat OpenShiftへの接続
- マシンカタログを作成する

VMwareカタログを作成する

(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/machine-catalogs-create.html)では、マシンカタログを作成するウィザードについて説明します。以下の情報では、VMware仮想化環境に固有の詳細について説明します。

> **注:**
>
> VMwareカタログを作成する前に、VMwareへの接続の作成を完了する必要があります。(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/connections/connection-vmware-virtualization-environments.html)を参照してください。

マスターVMを作成する

マスターVMを使用して、マシンカタログでユーザーデスクトップとアプリケーションを提供します。ハイパーバイザーで、次の操作を行います。

1. マスターVMにVDAをインストールし、デスクトップを最適化するオプションを選択して、パフォーマンスを向上させます。
2. バックアップとして使用するために、マスターVMのスナップショットを作成します。

> **注:**
>
> MCSを使用して、vSAN 8.0環境でVMをプロビジョニングできます。

マシンプロファイルを使用してマシンカタログを作成する

マシンプロファイルを使用してMCSマシンカタログを作成できます。マシンプロファイルの入力元はVMwareテンプレートです。マシンプロファイルは、VMwareテンプレートからハードウェアプロパティを取得し、カタログ内の新しくプロビジョニングされたVMに適用します。

注:

- マスターイメージ入力（スナップショット）とマシンプロファイル入力（VMwareテンプレート）は、vTPMが有効であるか、vTPMが無効であるかのいずれかでなければなりません。このルールは、`New-ProvScheme`と`Set-ProvScheme`の両方に適用されます。
- マスターイメージでvTPMが有効になっている場合、VMwareテンプレートはマスターイメージと同じVMソースからのみ取得できます。
- 暗号化されたストレージポリシーは、フルクローンのみをサポートします。
- マシンプロファイルベースのカタログは、提供されたVMwareテンプレートを利用してストレージコントローラー情報を収集し、接続されている仮想ディスクに依存します。テンプレートには、仮想マシンの仮想ディスクを構成するために使用されるストレージコントローラー情報を取得するために必要な仮想ディスクを含める必要があります。

マシンプロファイル内のVMwareテンプレートは、カタログへのVMのプロビジョニングを許可するために、カタログのライフサイクル中に存在する必要があります。VMwareテンプレートがないと、新しいVMをプロビジョニングできません。VMwareテンプレートが削除された場合は、`Set-ProvScheme`コマンドを使用して新しいテンプレートを提供する必要があります。

- MCSはVMwareテンプレートのプロパティをキャプチャします。Get-Provschemeコマンドを使用して、VMwareテンプレートの保存されたプロパティを参照する新しいVMwareテンプレートを作成できます。
- あるいは、マシンカタログとプロビジョニングされたVMが存在する場合、MCSでプロビジョニングされたマシンを使用して新しいVMwareテンプレートを作成することもできます。
- MCSIOが有効な場合、MCSカタログ作成後にメモリとディスクキャッシュのサイズを更新できます。

異なるOSに基づいて、異なる構成でマシンカタログを作成できます。

- マスターイメージにWindows 11がインストールされている場合、マスターイメージでvTPMを有効にする必要があります。したがって、マシンプロファイルのソースであるVMwareテンプレートにはvTPMがアタッチされている必要があります。
- マスターイメージにvTPMがアタッチされていないWindows 10がインストールされている場合、非vTPM VMwareテンプレートをマシンプロファイルのソースとして使用してマシンカタログを作成できます。

暗号化されたストレージポリシーが適用されたマシンプロファイルテンプレートを使用して、フルコピーディスクモードでマシンカタログを作成できる別の構成があります。

マシンプロファイルを入力としてPowerShellコマンドを使用してマシンカタログを作成するには：

1. **PowerShell**ウィンドウを開きます。
2. `asnp citrix®*`を実行します。
3. 次のコマンドを実行します。

    - vTPMがアタッチされたVMwareテンプレートをマシンプロファイル入力のソースとして、Windows 11がインストールされたマスターイメージでマシンカタログを作成するには：

```
$identityPool = New-AcctIdentityPool  -IdentityPoolName "<string>"

-NamingScheme "<string>-###"

-NamingSchemeType Numeric

-Domain "<domain name"

-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme  -CleanOnBoot

-HostingUnitName "vSanRg"

-IdentityPoolName "<string>"

-InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
name>.snapshot"
```

```
-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
\<network name>.network"}

-ProvisioningSchemeName "<string>"

-Scope @() -VMCpuCount 4

-VMMemoryMB 6144

-MachineProfile "XDHyp:\HostingUnits\<hosting unit name>\<template
name>.template" -TenancyType Shared

-FunctionalLevel "L7_20"
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"

-PersistUserChanges  "OnLocal"

-Description "<string>"

-IsRemotePC $False

-MinimumFunctionalLevel 'L7_9'

-Name "<catalog name>"

-ProvisioningType 'MCS'

-Scope @()

-SessionSupport "SingleSession" -ZoneUid "<Uid>"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

- 非vTPM VMwareテンプレートをマシンプロファイルのソースとして、Windows 10がインストールされたマスターイメージでマシンカタログを作成するには：

```
$identityPool = New-AcctIdentityPool

-IdentityPoolName "<string>"

-NamingScheme "<string>-###" -NamingSchemeType Numeric

-Domain "<domain name>"

-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme

-CleanOnBoot -HostingUnitName "<string>"

-IdentityPoolName "<string>"

-InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
name>.snapshot

-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
\<string>.network"}

-ProvisioningSchemeName "<string>"  -Scope @() -VMCpuCount 4  -
VMMemoryMB 8192

-MachineProfile "XDHyp:\HostingUnits\<hosting unit name>\<template
name>.template"

-TenancyType Shared  -FunctionalLevel "L7_20"
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"

-PersistUserChanges  "OnLocal"

-Description "<string>"

-IsRemotePC $False
```

```
-MinimumFunctionalLevel 'L7_9' -Name "<string>" -ProvisioningType
'MCS' -Scope @()

-SessionSupport "SingleSession" -ZoneUid "<Uid"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

- 暗号化されたストレージポリシーが適用されたマシンプロファイルテンプレートを使用して、フルコピーディスクモードでマシンカタログを作成するには：

```
$identityPool = New-AcctIdentityPool

-IdentityPoolName "<string>"

-NamingScheme "<string>-###"

-NamingSchemeType Numeric

-Domain "<domain name>"

-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme

-HostingUnitName "<string>"

-IdentityPoolName "<string>"

-InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
name>.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
\<string>.network"}

-ProvisioningSchemeName "<string>"
```

```
-Scope @() -VMCpuCount 4  -VMMemoryMB 8192 -MachineProfile "XDHyp:
\HostingUnits\<hosting unit name>\<template name>.template"

-TenancyType Shared

-FunctionalLevel "L7_20" -UseFullDiskCloneProvisioning
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"

-PersistUserChanges  "OnLocal"

-Description "<string>"  -IsRemotePC $False

-MinimumFunctionalLevel 'L7_9'

-Name "<string>" -ProvisioningType 'MCS' -Scope @()

-SessionSupport "SingleSession" -ZoneUid "<Uid>"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

マシンプロファイルを更新するには、Set-ProvSchemeコマンドを使用します。例：

```
Set-ProvScheme -ProvisioningSchemeName 'name' -IdentityPoolName 'name'
-MachineProfile 'XDHyp:\HostingUnits\<hosting unit name>\<template
name>.template'
```

複数のNICの確認

マシンプロファイルを使用し、`New-ProvScheme`および`Set-ProvScheme`コマンドで`NetworkMapping`パラメーターを使用する場合、複数のNICの事前チェック中にさまざまなエラーメッセージが表示されます。

複数のNICの事前チェックリストは次のとおりです。

- マシンプロファイルテンプレートからのNIC数のみが使用され、検証されます。これらのNICが指すネットワークは、ホスティングユニットネットワークに対して使用または検証されません。
- マシンプロファイルテンプレートのNIC数がホスティングユニットのネットワーク数よりも多い場合、エラーメッセージが表示されます。
- マシンプロファイルテンプレートのNIC数がゼロの場合、エラーメッセージが表示されます。マシンプロファイルテンプレートのNIC数が1の場合：
  - `New-ProvScheme`または`Set-ProvScheme`コマンドでネットワークマッピングが指定されておらず、ホスティングユニットネットワークが1つの場合、そのホスティングユニットネットワークが使用されます。
  - ネットワークマッピングが指定されている場合、それが有効であれば、指定されたネットワークマッピングが使用されます。
- マシンプロファイルテンプレートのNIC数が1より大きい場合、またはホスティングユニットネットワーク数が1より大きい場合：
  - コマンドでは有効なネットワークマッピングが必要であり、各NICのマッピングを提供する必要があります（つまり、NetworkMappingの数はマシンプロファイルのNIC数と同じである必要があります）。
  - ホスティングユニット内で複数のNICを同じネットワークにマッピングすることはできません。
  - `NetworkMapping`数とマシンプロファイルのNIC数は、ホスティングユニットネットワーク数以下である必要があります。
  - `NetworkMapping`は、0からn-1までの各IDに対して提供する必要があります。ここでnは、マシンプロファイルテンプレート内のネットワークアダプターの数です。

MCSで作成されたVMにデータディスクをプロビジョニングする

データディスクを使用すると、イベントログ、セキュリティトレース、アプリケーションデータなどの永続データを保存できます。VMwareのMCSマシンカタログで、MCSによって作成された永続または非永続VMに、永続または非永続のデータディスクを作成して割り当てることができます。

マスターイメージからデータディスクをプロビジョニングします。準備されたマスターイメージのデータディスクは、`<Prov Scheme Name>-dataDisk-<datastoreId>`フォルダーに保存されます。

マシンプロファイルベースと非マシンプロファイルベースの両方のMCSカタログを作成できます。マシンプロファイルベースのMCSカタログの場合、マシンプロファイルのデータディスクソースとして同じマスターイメージVMを使用できます。

プロビジョニングされたVMのデータディスクは、ストレージポリシーやサイズなどのプロパティをマスターイメージから継承します。マシンプロファイルベースのカタログの場合、オプションでVMテンプレートのデータディスクを使用してプロパティを継承できます。VMテンプレートにデータディスクがない場合、ストレージのデフォルトポリシーが使用されます。

プロビジョニングされたVMのデータディスクは、OSディスクおよびIDディスクと同じディレクトリに作成されます。

サポートされているデータディスクのシナリオ

サポートされているOSディスクとデータディスクのシナリオは次のとおりです。

- 永続OSディスクと永続データディスク
- 非永続OSディスクと永続データディスク
- 非永続OSディスクと非永続データディスク

> **注:**
>
> 永続マシンカタログには、非永続データディスクを含めることはできません。

制限事項

現在、以下の操作はサポートされていません。

- 複数のデータディスクのプロビジョニング。
- データディスクのリセット。
- データディスクを持つMCSカタログをデータディスクを持たないMCSカタログに更新する。同様に、データディスクを持たないMCSカタログをデータディスクを持つMCSカタログに更新する。

主な手順

1. VMwareでデータディスクを持つマスターイメージVMを作成する(#create-a-master-image-vm-with-data-disk-in-vmware)。マシンプロファイルベースのMCSカタログの場合、同じマスターイメージVMをマシンプロファイルのデータディスクソースとして使用できます。

2. `New-ProvScheme` PowerShellコマンドを使用して、データディスクがプロビジョニングされたVMを持つMCSマシンカタログを作成します。データディスクがプロビジョニングされたVMを持つカタログを作成するを参照してください。
3. `New-ProvVM` PowerShellコマンドを使用して、VMをカタログに追加します。
4. VMにログインして、データディスクが正しくフォーマットされているか確認します。マスターイメージVMで参照されているデータディスクにコンテンツがある場合、そのコンテンツもデータディスク上にあります。

VMwareでデータディスクを持つマスターイメージVMを作成する

1. 2つのハードディスクを持つVMを作成します。1つはOSディスク、もう1つはデータディスクです。既存のVMに新しいハードディスク（データディスク）を追加するには、このガイドに従ってください。
2. VMにログインして、ディスクを初期化し、目的のドライブ文字を設定し、コンテンツを追加します。

データディスクがプロビジョニングされたVMを含むカタログを作成する

データディスクを持つMCSマシンカタログをプロビジョニングするには、`New-ProvScheme` PowerShellコマンドに次のパラメーターを含めます。

- `DataDisk`: 指定されたデータディスクのパスを指定します。
- `DataDiskPersistence`: DataDiskが永続的か非永続的かを示します。

  `CleanOnBoot`がfalseの場合、データディスクは非永続的であってはなりません。マシンカタログが一度構成されると、`DataDiskPersistence`の値を変更することはできません。

カタログを作成した後、`New-ProvVM`コマンドを使用してVMを追加します。

イメージの更新

OSおよびデータディスクのソースを更新するには、`Publish-ProvMasterVMImage`コマンドを実行します。`Publish-ProvMasterVMImage`コマンドを実行した後:

- 新しいVMは、更新されたOSおよびデータディスクで作成されます。
- 既存のVMの非永続ディスクは、次回の電源サイクルで更新されます。
- 既存のVMの永続ディスクは、次回の電源サイクルでは更新されません。

データディスクの削除

カタログを削除すると、`forgetVM`または`purgeDBOnly`オプションを使用しない限り、データディスクは削除されます。VMを削除すると、`forgetVM`または`purgeDBOnly`オプションを使用

しない限り、データディスクは削除されます。これらの条件は、永続MCSマシンカタログにのみ適用されます。

トラブルシューティング

カタログの作成に失敗した場合は、CTX294978を参照してください。

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成を案内します。
- 構成プロセス全体を確認するには、「」(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure.html)を参照してください。
- カタログを管理するには、マシンカタログの管理およびVMwareカタログの管理を参照してください。

詳細情報

- 接続とリソースの作成および管理
- VMwareへの接続
- マシンカタログの作成

異なるマシンID結合タイプのIDプール

MCSを使用すると、オンプレミスAD参加済み、Microsoft Entraハイブリッド参加済み、またはドメイン非参加のマシンをプロビジョニングできます。

Web StudioでマシンIDを構成する方法については、マシンカタログの作成を参照してください。

異なるマシンID参加タイプのIDプールを作成する方法の詳細については、以下を参照してください。

- オンプレミスActive Directory参加済みマシンIDのIDプール
- Microsoft Entraハイブリッド参加済みマシンIDのIDプール
- ドメインに参加していないマシンIDのIDプール

オンプレミスActive Directoryに参加しているマシンIDのIDプール

この記事では、オンプレミスActive Directoryに参加しているマシンIDのIDプールを作成する方法について説明します。

Web Studioを使用する

以下の情報は、マシンカタログの作成のガイダンスを補足するものです。

1. **マシンID**ページで：
    a. IDの種類として**オンプレミスActive Directory**を選択します。
    b. Active Directory アカウントオプションを選択します。
        - **新しい Active Directory アカウントを作成する：**
            - 「**新しいActive Directoryアカウントを作成**」を選択し、既存のIDプールを使用して新しいアカウントを作成する場合は、それらのアカウントのドメインを選択し、アカウント命名スキームを指定します。
            - 「**新しいActive Directoryアカウントを作成**」を選択し、既存のIDプールを使用して新しいアカウントを作成する場合は、リストからIDプールを選択します。
        - **既存のActive Directoryアカウントを使用する**：CSVファイルから参照またはインポートし、パスワードをリセットするか、すべてのアカウントに同じパスワードを指定できます。
    c. **Next**をクリックします。
2. **ドメイン資格情報**ページで、サービスアカウントを選択するか、資格情報を手動で入力します。サービスアカウントの詳細については、オンプレミスActive Directoryサービスアカウントを参照してください。

サービスアカウントの関連付けを変更する

関連付けられているサービスアカウントを変更したり、既存のMCSマシンカタログに新しい関連付けを追加したりするには、「**マシンカタログの編集**」ページを使用します。

- サービスアカウントを追加するには、「**サービスアカウント**」ページで「**サービスアカウントの選択**」をクリックします。
- サービスアカウントの関連付けを変更するには、「**サービスアカウント**」ページで編集アイコンをクリックします。

PowerShell を使用する

オンプレミスサービスアカウントをIDプールに関連付けることで、オンプレミスサービスアカウントをMCSで作成されたマシンカタログに関連付けることができます。IDプールを作成するか、既存のIDプールを更新して、サービスアカウントに関連付けることができます。

例: 新しいIDプールを作成し、サービスアカウントに関連付けるには、以下を実行します。

```
New-AcctIdentityPool -IdentityType ActiveDirectory -IdentityPoolName
MyPool -NamingScheme Acc#### -Domain MyDomain.com -NamingSchemeType
Numeric -OU "CN=MyOU,DC=MyDomain,DC=com" -ServiceAccountUid
$serviceAccountUid
```

例: 既存のIDプールを更新してサービスアカウントに関連付けるには、以下を実行します。

```
$identityPoolUid = (Get-ProvScheme -ProvisioningSchemeName
"MyProvScheme").IdentityPoolUid

Set-AcctIdentityPool -IdentityPoolUid $identityPoolUid -ServiceAccountUid
$serviceAccountUid
```

注:

`$serviceAccountUid` は、オンプレミスのActive Directoryサービスアカウントの有効なUIDである必要があります。

Microsoft Entra ハイブリッド参加済みマシンIDのIDプール

この記事では、以下のIDプールを作成する方法について説明します。

- Microsoft Entra ハイブリッド参加済みカタログ
- Microsoft Intune に登録されている Microsoft Entra ハイブリッド参加済みカタログ

要件、制限、および考慮事項については、「Microsoft Entra ハイブリッド参加済み」を参照してください。

Microsoft Entra ハイブリッド参加カタログを作成する

Web Studio を使用する

以下の情報は、マシンカタログの作成のガイダンスを補足するものです。

カタログ作成ウィザードの ページで、次のようにします。

- を選択します。作成されたマシンは組織が所有し、その組織に属する Active Directory アカウントでサインインします。

- デバイス管理のために作成されたマシンを Microsoft Intune (Configuration Manager を含む) に登録するには、 を選択します。カタログ作成中のエラーを回避するには、マスターイメージが次の要件を満たしていることを確認してください。
  - VDA バージョン 2405 以降がインストールされていること。
  - サイトコードが割り当てられていない **Configuration Manager クライアント**がインストールされていること。詳細については、この Microsoft の記事を参照してください。

> **注:**
>
> IDの種類として を選択した場合、カタログ内の各マシンには対応するADコンピューターアカウントが必要です。

- 「**拡張属性の追加**」をクリックして、一意のカスタムデータをEntra IDデバイスオブジェクトに直接保存します。「**拡張属性の追加**」ページで、「**拡張属性**」と「**値**」を追加します。

> **注:**
>
> - 最大15個の拡張属性を追加できます。
> - 名前と値は一意である必要があり、空にすることはできません。

拡張属性の追加または変更

既存のMCSマシンカタログに拡張属性を変更または追加したり、サービスアカウントなしでMCSカタログに拡張属性を追加したりするには、「**マシンカタログの編集**」ウィザードを使用します。

- 追加の拡張属性を変更または追加するには、「**Microsoft Entraデバイス拡張属性**」ページに移動します。鉛筆アイコンをクリックし、拡張属性を追加または更新します。
- Microsoft Entraサービスアカウントなしで MCSカタログに拡張属性を追加するには：
  a. 「**サービスアカウント**」ページに移動します。Microsoft Intra IDのMicrosoft Entraサービスアカウントを選択します。
  b. Microsoft Entraデバイス拡張属性ページに移動し、「**拡張属性の追加**」をクリックします。

PowerShell を使用する

以下は、Web Studio での操作に相当する PowerShell の手順です。Remote PowerShell SDK を使用してカタログを作成する方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`を参照してください。

オンプレミスのAD参加済みカタログとMicrosoft Entraハイブリッド参加済みカタログの違いは、IDプールとマシンアカウントの作成にあります。

Microsoft Entra ハイブリッド参加カタログのアカウントとともにIDプールを作成するには：

```
New-AcctIdentityPool -AllowUnicode -IdentityType "HybridAzureAD" -Domain
"corp.local" -IdentityPoolName "HybridAADJoinedCatalog" -NamingScheme
"HybridAAD-VM-##" -NamingSchemeType "Numeric" -OU
"CN=AADComputers,DC=corp,DC=local" -Scope @() -ZoneUid "81291221-
d2f2-49d2-ab12-bae5bbd0df05"

New-AcctIdentity -IdentityPoolName "HybridAADJoinedCatalog" -Count 10
-ADUserName "corp\admin1" -ADPassword $password

Set-AcctAdAccountUserCert -IdentityPoolName "HybridAADJoinedCatalog" -All
-ADUserName "corp\admin1" -ADPassword $password
```

注:

`$password` は、書き込み権限を持つADユーザーアカウントの一致するパスワードです。

Microsoft Entra ハイブリッド参加済みカタログを作成するために使用される他のすべてのコマンドは、従来のオンプレミスAD参加済みカタログの場合と同じです。

指定された拡張属性を持つ新しいIDプールを作成し、それをサービスアカウントに関連付けるには、次を実行します。

```
New-AcctIdentityPool -IdentityPoolName HybridAzureAD -NamingScheme ACC####
-NamingSchemeType Numeric -Domain "abc.local" -IdentityType HybridAzureAD
-ServiceAccountUid $serviceAccountUid -EntraIDExtensionAttributes
@{"extensionAttribute1" = "val1"; "extensionAttribute2" = "val2"}
```

VMがMicrosoft Entra IDに参加した後、初めて電源がオンになると、VMはそのEntra ID deviceIdをMCSに報告します。

例：`EntraIDDeviceID`を確認するには、`Get-AcctADAccount`または`Get-AcctIdentity`を実行します。

```
Get-AcctADAccount -IdentityPoolName MyPool
```

再起動後、永続VMと非永続VMの両方で、`EntraIDDeviceID` は同じままです。

注:

カタログから VM を削除しても Azure から削除しない場合、MCS は関連付けられたデバイス ID と拡張属性を自動的に削除します。

既存のカタログの拡張属性を編集するには、以下を実行します。

注:

- 既存のカタログVMをVDAバージョン2511以降にアップグレードした後、再起動が必要です。この再起動により、VMはそのEntra ID deviceIdをMCSに報告できるようになり、MCSはVMの拡張属性を構成できるようになります。
- 既存のカタログには、「Device.ReadWrite.All」の権限を持つAzureADタイプのサービスアカウントが必要です。

新しい属性を追加するには：

```
Set-AcctIdentityPool -IdentityPoolName MyPool -EntraIDExtensionAttributes
@{"extensionAttribute1" = "val1"; "extensionAttribute2" = "val2"}
```

既存の属性を削除するには

```
Set-AcctIdentityPool -IdentityPoolName MyPool -EntraIDExtensionAttributes
@{}
```

または

```
Set-AcctIdentityPool -IdentityPoolName MyPool -EntraIDExtensionAttributes
@{extensionAttribute1 = ""; extensionAttribute2 = ""}
```

`Set-AcctIdentityPool` は、すでに Entra ID に参加しており、その ID 内に `EntraIDDeviceID` 値を持つ VM の Entra ID デバイスの拡張属性も更新します。

Microsoft Entra ハイブリッド参加プロセスのステータスを表示する

Web Studio では、デリバリーグループ内の Microsoft Entra ハイブリッド参加マシンが電源オン状態の場合に、Microsoft Entra ハイブリッド参加プロセスのステータスが表示されます。ステータスを表示するには、検索を使用してそれらのマシンを特定し、下部ペインの タブで各マシンの を確認します。 には次の情報が表示されます。

- Microsoft Entraハイブリッド参加済み
- Microsoft Entra IDにまだ参加していません

注:

- マシンの初回起動時に、Microsoft Entra ハイブリッド参加が遅延する場合があります。これは、デフォルトのマシンID同期間隔（Microsoft Entra Connectの30分）が原因です。マシンIDがMicrosoft Entra Connectを介してMicrosoft Entra IDに同期された後にのみ、マシンはMicrosoft Entra ハイブリッド参加状態になります。
- マシンがMicrosoft Entraハイブリッド参加状態にならなかった場合、それらはデリバリーコントローラーに登録されません。登録ステータスは**初期化中**と表示されます。

また、Web Studioを使用して、マシンが利用できない理由を知ることができます。そのためには、**検索**ノードでマシンをクリックし、下部ペインの**詳細**タブで**登録**を確認し、ツールチップを読んで追加情報を確認します。

トラブルシューティング

マシンがMicrosoft Entraハイブリッド参加に失敗した場合は、次の操作を行います。

- マシンアカウントがMicrosoft Microsoft Entra IDポータルを介してMicrosoft Entra IDに同期されているか確認します。同期されている場合、**Microsoft Entra IDにまだ参加していません**と表示され、登録保留中のステータスを示します。

マシンアカウントをMicrosoft Entra IDに同期するには、以下を確認してください。

- マシンアカウントが、Microsoft Entra IDと同期するように構成されているOU内にあること。**userCertificate**属性を持たないマシンアカウントは、同期するように構成されているOU内にあってもMicrosoft Entra IDに同期されません。
- **userCertificate**属性がマシンアカウントに設定されていること。属性を表示するには、Active Directory Explorerを使用します。
- マシンアカウントが作成された後、Microsoft Entra Connectが少なくとも1回同期されている必要があります。同期されていない場合は、Microsoft Entra Connectマシンの PowerShellコンソールで`Start-ADSyncSyncCycle -PolicyType Delta`コマンドを手動で実行して、即時同期をトリガーします。

- **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix**の下にある**DeviceKeyPairRestored**の値を照会して、Microsoft Entra ハイブリッド参加用のCitrix管理デバイスキーペアがマシンに正しくプッシュされているか確認します。

  値が1であることを確認します。そうでない場合、考えられる理由は次のとおりです。

  - プロビジョニングスキームに関連付けられたIDプールの`IdentityType`が`HybridAzureAD`に設定されていません。これは`Get-AcctIdentityPool`を実行して確認できます。
  - マシンがマシンカタログと同じプロビジョニングスキームを使用してプロビジョニングされていません。
  - マシンがローカルドメインに参加していません。ローカルドメイン参加は、Microsoft Entra ハイブリッド参加の前提条件です。

- MCSでプロビジョニングされたマシンで`dsregcmd /status /debug`コマンドを実行して、診断メッセージを確認します。

  - Microsoft Entra ハイブリッド参加が成功した場合、コマンドラインの出力で**AzureAdJoined**と**DomainJoined**が**YES**になります。
  - そうでない場合、問題をトラブルシューティングするにはMicrosoftのドキュメントを参照してください: `<https://docs.microsoft.com/ja-jp/azure/active-directory/devices/troubleshoot-hybrid-join-windows-current>`。
  - エラーメッセージ「**Server Message: The user certificate is not found on the device with id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx**」が表示された場合は、ユーザー証明書を修復するために次のPowerShellコマンドを実行します。

```
Repair-AcctIdentity -IdentityAccountName TEST\VM1 -Target
UserCertificate
```

ユーザー証明書の問題の詳細については、CTX566696を参照してください。

Microsoft Intune に登録された Microsoft Entra ハイブリッド参加済みカタログを作成する

永続的なシングルセッションおよびマルチセッションVM向けに、Microsoft Intuneに登録されたMicrosoft Entraハイブリッド参加カタログの共同管理対応カタログを作成できます。共同管理対応カタログは、StudioとPowerShellの両方を使用して作成できます。

Web Studioを使用する

以下の情報は、マシンカタログの作成のガイダンスを補足するものです。

マシンカタログのセットアップウィザードで、:

- **マシンID**ページで、**Microsoft Entraハイブリッド参加**を選択し、次に**Configuration Managerでマイクロソフト Intuneにマシンを登録する**を選択します。このアクションを使用すると、Configuration ManagerとMicrosoft Intune（つまり、共同管理）がVMを管理します。

PowerShell を使用する

以下は、Studio の手順に相当する PowerShell の手順です。

Remote PowerShell SDK を使用して Configuration Manager で Microsoft Intune にマシンを登録するには、`New-AcctIdentityPool` の `DeviceManagementType` パラメーターを使用します。この機能には、カタログが Microsoft Entra ハイブリッド参加済みであり、Microsoft Entra ID が適切な Microsoft Intune ライセンスを所有している必要があります。

Microsoft Entra ハイブリッド参加済みカタログと共同管理が有効なカタログの違いは、ID プールの作成方法にあります。例:

```
New-AcctIdentityPool -AllowUnicode -DeviceManagementType "IntuneWithSCCM"
IdentityType="HybridAzureAD" -IdentityPoolName "CoManagedCatalog"
-NamingScheme "CoManaged-VM-##" -NamingSchemeType "Numeric" -Scope @()
-ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
```

トラブルシューティング

マシンがMicrosoft Intuneに登録できない場合、または共同管理状態に到達できない場合は、次の操作を行います。

- Intuneライセンスを確認する

  Microsoft Entra テナントに適切な Intune ライセンスが割り当てられているか確認します。Microsoft Intune のライセンス要件については、Microsoft Intune licensing を参照してください。

- Microsoft Entra ハイブリッド参加のステータスを確認する

  MCSプロビジョニングされたマシンがMicrosoft Entra ハイブリッド参加済みであるか確認します。Microsoft Entra ハイブリッド参加済みでない場合、マシンは共同管理の対象になりません。Microsoft Entra ハイブリッド参加の問題のトラブルシューティングについては、(#troubleshoot)を参照してください。

- 共同管理の適格性を確認する

  - MCS でプロビジョニングされたマシンに、期待される Configuration Manager サイトが正しく割り当てられているか確認します。割り当てられたサイトを取得するには、影響を受けるマシンで次の PowerShell コマンドを実行します。

    ```
    (New-Object -ComObject "Microsoft.SMS.Client").GetAssignedSite()
    ```

  - VM にサイトが割り当てられていない場合は、次のコマンドを使用して、Configuration Manager サイトが自動的に検出できるか確認します。

    ```
    (New-Object -ComObject "Microsoft.SMS.Client").AutoDiscoverSite()
    ```

  - サイトコードが検出できない場合は、Configuration Manager 環境で境界と境界グループが適切に構成されていることを確認してください。詳細については、Considerations を参照してください。

  - Configuration Manager クライアントのサイト割り当てに関する問題がないか、`C:\Windows\CCM\Logs\ClientLocation.log` を確認してください。

  - マシンの共同管理の状態を確認します。影響を受けるマシンで **Configuration Manager コントロールパネル**を開き、**General** タブに移動します。共同管理プロパティの値は **Enabled** である必要があります。そうでない場合は、`C:\Windows\CCM\Logs\CoManagementHandler.log` の下のログを確認してください。

- Intune 登録を確認する

  すべての前提条件が満たされていても、マシンが Microsoft Intune への登録に失敗する場合があります。Intune 登録の問題については、**Application and Services Logs > Microsoft >**

Windows > DeviceManagement-Enterprise-Diagnostics-Provider の下の Windows イベントログを確認してください。

非ドメイン参加型マシンIDのIDプール

この記事では、Citrix Virtual Apps and Desktopsを使用して、非ドメイン参加型カタログのIDプールを作成する方法について説明します。

要件、制限、考慮事項については、非ドメイン参加型を参照してください。

マシンカタログを作成する前に、次のものが必要です。

1. 新しいリソースの場所
    - Citrix Cloud™ 管理 UI > 左上のハンバーガーメニュー > **リソースの場所** に移動します。
    - **+ リソースの場所** をクリックします。
    - 新しいリソースの場所の名前を入力し、**保存** をクリックします。
2. ホスティング接続を作成します。詳細については、接続の作成と管理セクションを参照してください。

Citrix Virtual Apps and Desktops™ を使用すると、ワークグループまたはドメインに参加していないマシンに基づいてカタログを作成できます。ドメインに参加していないマシンの作成は、アカウントIDプールがどのように作成されるかによって異なります。アカウントIDプールは、カタログプロビジョニング中にMCSがマシン名を作成および追跡するために使用するメカニズムです。

Web Studioを使用する

以下の情報は、マシンカタログの作成のガイダンスを補足するものです。

カタログ作成ウィザードで：

- **マシンID**ページで、**非ドメイン参加型**を選択します。作成されたマシンはどのドメインにも参加していません。

> **注:**
>
> **非ドメイン参加型**IDタイプでは、カタログの最小機能レベルとしてVDAバージョン2311以降が必要です。利用可能にするには、必要に応じて最小機能レベルを更新してください。

PowerShell を使用する

Remote PowerShell SDKを使用して、非ドメイン参加型カタログのIDプールを作成できます。

PowerShellパラメーターの**WorkgroupMachine**と**IdentityType**を使用して、非ドメイン参加型カタログのIDプールを作成します。これらのパラメーターにより、ドメイン管理者資格情報を含むすべてのAD固有のパラメーターを指定する必要がなくなります。

```
New-AcctIdentityPool -AllowUnicode -IdentityType "Workgroup"
-WorkgroupMachine -IdentityPoolName "NonDomainJoinedCatalog" -NamingScheme
"NDJ-VM-##" -NamingSchemeType "Numeric" -Scope @() -ZoneUid "81291221-
d2f2-49d2-ab12-bae5bbd0df05"
```

非ドメイン参加型カタログの作成に使用されるその他のすべてのコマンドは、従来のオンプレミスActive Directory参加型カタログの場合と同じです。

マシンカタログを管理する

注:

バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

はじめに

マシンカタログへのマシンの追加または削除、名前の変更、説明の変更、またはカタログのActive Directoryコンピューターアカウントの管理を行うことができます。

カタログの保守には、各マシンが最新のOSアップデートを適用していることを確認することも含まれます。これには、ウイルス対策の更新、オペレーティングシステムのアップグレード、または構成の変更が含まれます。

- Machine Creation Services™ (MCS) を使用して作成されたプールされたランダムマシンを含むカタログは、カタログで使用されるマスターイメージを更新し、その後マシンを更新することでマシンを保守します。この方法により、多数のユーザーマシンを効率的に更新できます。

- 静的で永続的に割り当てられたマシンを含むカタログ、およびリモートPCアクセス マシンカタログの場合、ユーザーのマシンへの更新はWeb Studioの外部で管理します。このタスクは、個別に、またはサードパーティのソフトウェア配布ツールを使用してまとめて実行します。

ホストハイパーバイザーへの接続の作成と管理については、「接続とリソース」を参照してください。

> **注:**
>
> MCSはWindows 10 IoT CoreおよびWindows 10 IoT Enterpriseをサポートしていません。詳細については、Microsoftサイトを参照してください。

永続インスタンスについて

永続的または専用インスタンスを使用して作成されたMCSカタログを更新する場合、カタログ用に作成された新しいマシンはすべて更新されたイメージを使用します。既存のインスタンスは引き続き元のインスタンスを使用します。イメージの更新プロセスは、他の種類のカタログと同じ方法で行われます。以下を考慮してください。

- 永続ディスクカタログの場合、既存のマシンは新しいイメージに更新されませんが、カタログに追加される新しいマシンは新しいイメージを使用します。
- 非永続ディスクカタログの場合、マシンイメージはマシンがリセットされる次回のタイミングで更新されます。
- 永続マシンカタログの場合、イメージを更新すると、それを使用するカタログインスタンスも更新されます。
- 永続化しないカタログの場合、異なるマシンに異なるイメージを使用したい場合は、イメージは別々のカタログに存在する必要があります。

マシンカタログを管理する

マシンカタログは、次の2つの方法で管理できます。

- Web Studioの使用
- PowerShellを使用する

Web Studioを使用する

このセクションでは、Web Studioを使用してカタログを管理する方法について詳しく説明します。

- マシンカタログの管理
  - はじめに
  - 永続インスタンスについて
- マシンカタログの管理
- Web Studioを使用する
- カタログの詳細を表示する
  - カタログにマシンを追加する
  - カタログからマシンを削除する
- カタログを編集する
- カタログの名前を変更する
- カタログを別のゾーンに移動する
- カタログを削除する
- (Azure のレガシー MCS カタログをマシンプロファイルベースのカタログに変換する)
- カタログ内のActive Directoryコンピューターアカウントを管理する
- カタログを更新する
  - マスターイメージを更新または作成する(#update-or-create-a-master-image)
  - マスターイメージを変更する(#change-the-master-image)
  - マスターイメージをロールバックする(#roll-back-the-master-image)
- 機能レベルを変更する、または変更を元に戻す(#change-the-functional-level-or-undo-the-change)
- カタログをクローンする(#clone-a-catalog)
- フォルダーを使用してカタログを整理する(#organize-catalogs-using-folders)
  - カタログフォルダーを作成する(#create-a-catalog-folder)
  - カタログを移動する(#move-a-catalog)
  - カタログフォルダーを管理する(#manage-catalog-folders)
- VDAをアップグレードする(#upgrade-vdas)
- カタログ作成を再試行する(#retry-catalog-creation)

- トークンを使用して非MCSプロビジョニングVDAを登録する(#enroll-non-mcs-provisioned-vdas-using-tokens)
- PowerShellを使用する(#use-powershell)
- カタログに関連付けられている警告とエラーを取得する(#retrieve-warnings-and-errors-associated-with-a-catalog)
- イメージに説明を追加する
- OSディスクをリセットする
- 既存のプロビジョニングスキームのネットワーク設定を変更する(#change-the-network-setting-for-an-existing-provisioning-scheme)
- マシンカタログのバージョンを管理する(#manage-versions-of-a-machine-catalog)
- マシンプロファイルに基づかないマシンカタログを、マシンプロファイルに基づくマシンカタログに変換する(#convert-a-non-machine-profile-based-machine-catalog-to-machine-profile-based-machine-catalog)
- アクティブなコンピューターアカウントのID情報を修復する
  - 条件(#conditions)
  - IDディスクをリセットする(#reset-identity-disk)
- 既存のマシンカタログのキャッシュ構成を変更する(#change-cache-configuration-on-an-existing-machine-catalog)
  - 要件
  - キャッシュ構成を変更する
- ローカルファイル共有アクセスによるVDA更新のサポート
  - PowerShell コマンドレット
  - 前提条件
  - ファイル共有のアクセス許可を設定する方法
  - ローカルファイル共有からのVDA更新
- トラブルシューティング
- 次のステップ

カタログの詳細を表示

1. 検索機能を使用して特定のマシンカタログを見つけます。手順については、インスタンスの検索を参照してください。
2. 検索結果から、必要に応じてカタログを選択します。
3. カタログ列の説明については、次の表を参照してください。
4. カタログ列の説明については、次の表を参照してください。

列	説明
マシンカタログ	カタログの名前と割り当てタイプ。割り当てタイプには以下が含まれます。
	• ランダム: カタログ内のマシンはユーザーにランダムに割り当てられます。
	• 永続: カタログ内のマシンはユーザーに永続的に割り当てられます。
マシンタイプ	カタログ内のマシンでサポートされているセッションタイプ。可能な値には以下が含まれます。
	• OSタイプ: マルチセッションOS (仮想); ユーザーデータ: 破棄。
	• OSタイプ: マルチセッションOS (仮想); ユーザーデータ: ローカルディスク上
	• OSタイプ: シングルセッションOS (リモートPCアクセス)
	• OSタイプ: シングルセッションOS (仮想); ユーザーデータ: 破棄
	• OSタイプ: シングルセッションOS (仮想); ユーザーデータ: ローカルディスク上
マシン数	カタログ内のマシン数とプロビジョニング方法。可能なプロビジョニング方法には、Machine Creation Services (MCSマシン)、

列	説明
	手動、およびCitrix Provisioning™ Servicesが含まれます。
割り当て済み数	デリバリーグループに割り当てられているカタログ内のマシンの数。
フォルダ	**マシンカタログ**ツリー内のカタログの場所。カタログが存在するフォルダーの名前（末尾のバックスラッシュを含む）が表示されます。カタログがルートレベルにある場合は`-`が表示されます。
VDAアップグレード	VDAアップグレードの状態。可能な値は、未構成、スケジュール済み、利用可能、および最新です。
イメージステータス	カタログのイメージ更新のステータス。非永続マシンカタログにのみ適用されます。可能な値は、完全に更新済み、部分的に更新済み、更新保留中、準備中です。

5. 下部の詳細ペインでタブをクリックすると、選択したカタログに関する詳細情報が表示されます。

タブ	説明
詳細	マシンタイプ、プロビジョニング方法、サービスアカウント、OS、VDAバージョンなど、主要なマシンカタログ設定を要約し、リソースを迅速に表示および管理できるようにします。
テンプレートプロパティ	MCSでプロビジョニングされたカタログでのみ利用可能です。
	選択したカタログの詳細なプロビジョニング情報を表示します。これには以下が含まれます。
	• マシンテンプレートプロパティ

タブ	説明
	• ハイパーバイザー固有の詳細
	• マシンプロファイルプロパティ
マシン	選択したカタログ内のマシン名のページ分割されたリストを表示します。
デリバリーグループ	リモートPCカタログで利用可能です。
	選択したカタログに関連付けられているデリバリーグループを表示します。デリバリーグループ名とカタログの関連付けが表示されます。
タグ	マルチテナント環境では利用できません。
	選択したマシンカタログに割り当てられているタグのタグ名と説明を表示します。
ワークスペース環境管理	WEMサービスがプロビジョニングされ、アクセス可能な場合にのみ表示されます。
	Workspace Environment Management のシステム最適化設定を表示します。
コストインサイト	Azure MCSカタログにのみ適用され、以下が表示されます。
	過去30日間に発生した総コスト。
	現在の30日間の総コストと、以前の30日間の期間との比較。
	タブを表示するにはCitrix **コスト管理 > 管理 > コストの読み取り** 権限 (クラウド管理者向けデフォルト) が必要であり、コストの詳細を表示するには `Microsoft.CostManagement/query/read` Azure権限が必要です。
トラブルシューティング	推奨されるアクションとともに、カタログのエラーまたは警告を表示します。

マシンをカタログに追加する

開始する前に:

- 仮想化ホストに、追加のマシンを収容するのに十分なプロセッサ、メモリ、ストレージがあることを確認してください。
- 未使用のActive Directoryコンピューターアカウントが十分にあることを確認してください。既存のアカウントを使用している場合、追加できるマシンの数は利用可能なアカウントの数によって制限されます。
- Web Studioを使用して追加のマシン用のActive Directoryコンピューターアカウントを作成する場合、適切なドメイン管理者権限が必要です。

カタログにマシンを追加するには:

1. Studioから、左ペインで**マシンカタログ**を選択します。
2. マシンカタログを選択し、アクションバーで**マシンの追加**を選択します。
3. **仮想マシン**ページで、追加する仮想マシンの数を選択します。
4. **マシンID**ページで、設定を次のように構成します。

    - リストからIDを選択します。
    - 該当する場合は、アカウントを作成するか既存のアカウントを使用するか、およびそれらのアカウントの場所（ドメイン）を指定します。

      追加するVMの数に対して既存のActive Directoryアカウントが不足している場合は、アカウントが作成されるドメインと場所を選択します。

      既存のActive Directoryアカウントを使用する場合は、アカウントを参照するか、**インポート**を選択してアカウント名を含む`.csv`ファイルを指定します。追加するすべてのマシンに対して十分なアカウントがあることを確認してください。Studioはこれらのアカウントを管理します。そのインターフェイスですべてのアカウントのパスワードをリセットできるようにするか、すべてのアカウントで同じである必要があるアカウントパスワードを指定します。
    - このIDプールが他のカタログで使用されている場合、Studio を使用して別のプールに変更することはできません。代わりに、**Set-ProvScheme** PowerShell コマンドレットを使用してください。
    - 連続する数字または文字が表示される場所を示すハッシュマークを使用して、アカウントの命名スキームを指定します。たとえば、PC-Sales-##（0-9を選択）という命名スキームは、PC-Sales-01、PC-Sales-02、PC-Sales-03などのコンピューターアカウントになります。

- オプションで、アカウント名の開始文字を指定できます。

  アカウント名の開始文字を指定する際は、次のシナリオに注意してください。開始番号または文字がすでに使用されている場合、最初に作成されるアカウントは、その後に続く最も近い未使用の番号または文字を使用して命名されます。

5. **ドメイン資格情報**ページで、**資格情報の入力**を選択し、マシンアカウントを作成するのに十分な権限を持つユーザー資格情報を入力します。

マシンはバックグラウンドプロセスとして作成され、多数のマシンを作成する場合は時間がかかることがあります。Studioを閉じてもマシンの作成は続行されます。

カタログからマシンを削除する

マシンカタログからマシンを削除すると、ユーザーはそのマシンにアクセスできなくなるため、マシンを削除する前に、以下を確認してください。

- ユーザーデータがバックアップされているか、不要になっていること。
- すべてのユーザーがログオフしていること。メンテナンスモードをオンにすると、マシンへの新しい接続が停止します。
- マシンが電源オフになっていること。

カタログからマシンを削除するには：

1. Web Studioにサインインします。
2. 左側のペインで**Machine Catalogs**を選択します。
3. カタログを選択し、アクションバーで**マシンを表示**を選択します。
4. 1つ以上のマシンを選択し、アクションバーで**削除**を選択します。

削除するマシンを削除するかどうかを選択します。マシンを削除することを選択した場合、それらのマシンのActive Directoryアカウントを保持するか、無効にするか、削除するかを指定します。

カタログを編集する

1. **説明**ページで、カタログの説明を変更します。
2. 左側のペインで**Machine Catalogs**を選択します。
3. カタログを選択し、アクションバーで**マシンカタログの編集**を選択します。
4. **スコープ**ページで、スコープを変更します。
5. **NIC**ページで、次のアクションを実行します。

- NICのサブネットマッピングを変更するには、**関連ネットワーク**フィールドからネットワークを選択します。
- サブネットマッピングを追加するには、**NICの追加**を選択し、**関連ネットワーク**フィールドからネットワークを選択して、**保存**をクリックします。

カタログに関連付けられているホストに存在するサブネットのみが、**関連ネットワーク**フィールドに表示されます。

マシンプロファイルのないAzureマシンカタログにのみNICを追加できます。

> **注:**
>
> - AWSマシンカタログの場合、同じサブネットを複数のNICにマッピングすることはできません。
> - マシンプロファイルを持つマシンカタログの場合、カタログ上のNICの数は、マシンプロファイル上のNICの数と等しくなければなりません。
> - この機能は、IBM Cloudハイパーバイザーではサポートされていません。
> - この機能は、Nutanixハイパーバイザーの場合、Nutanix Prism Elementでのみサポートされています。

6. カタログの種類によっては、他のページが表示される場合があります。

   Azure Resource Managerイメージを使用して作成されたカタログの場合、次のページが表示されます。行った変更は、後でカタログに追加するマシンにのみ適用されることに注意してください。既存のマシンは変更されません。

   - **Virtual Machines**ページで、マシンを作成するマシンサイズと可用性ゾーンを変更します。

     > **注:**
     >
     > - カタログがサポートするマシンサイズのみが表示されます。
     > - 必要に応じて、**Show only machine sizes used in other machine catalogs**を選択して、マシンサイズリストをフィルターします。

    - Azureカタログの場合、「**Storage and License Types**」ページで「**Storage redundancy**」が「**ZRS**」である場合、ゾーン選択をクリアしてAzureにVM可用性ゾーンを管理させることを推奨する警告が表示されます。

- **Machine Profile**ページで、マシンプロファイルを使用するか変更するかを選択します。

  注:

  Azureカタログの場合、可用性ゾーンを含むマシンプロファイルを変更し、ストレージ冗長性にZRSを選択すると、ゾーン選択をクリアするよう促す警告が表示されます。

- （カタログが専用グループホストで構成されている場合にのみ表示）**専用ホストグループ**ページで、ホストグループを変更するかどうかを選択します。
- **ストレージとライセンスの種類**ページで、ストレージ冗長タイプ (Azureカタログの場合)、ストレージタイプ、ライセンスタイプ、およびAzure Computer Gallery設定 (「**準備済みイメージをAzure Galleryに配置**」が使用されている場合にのみ利用可能) を変更するかどうかを選択します。

注:

新しく選択した設定が現在のマシンサイズをサポートしていない場合、設定を変更するとマシンサイズの設定がリセットされることを通知する警告ダイアログボックスが表示されます。続行することを選択すると、**仮想マシン**メニューの横に赤い点が表示され、新しいマシンサイズを選択するように促されます。

- **ライセンスの種類**ページで、WindowsライセンスまたはLinuxライセンスの設定を変更するかどうかを選択します。

Remote PC Accessカタログの場合、以下のページが表示されます。

- **電源管理**ページで、電源管理設定を変更し、電源管理接続を選択します。
- **組織単位**ページで、Active Directory OUを追加または削除します。

7. 行った変更を適用するには**適用**をクリックし、終了するには**保存**をクリックします。

カタログの名前を変更する

1. Web Studioにサインインします。
2. 左側のペインで**Machine Catalogs**を選択します。
3. カタログを選択し、アクションバーで**マシンカタログの名前を変更**を選択します。
4. 新しい名前を入力します。

カタログを別のゾーンに移動する

展開に複数のゾーンがある場合、カタログをあるゾーンから別のゾーンに移動できます。

カタログ内のVMを含むハイパーバイザーとは異なるゾーンにカタログを移動すると、パフォーマンスに影響します。

1. Web Studioにサインインします。
2. 左側のペインで**Machine Catalogs**を選択します。
3. カタログを選択し、アクションバーで**移動**を選択します。
4. カタログを移動するゾーンを選択します。

カタログを削除する

カタログを削除する前に、以下を確認してください。

- すべてのユーザーがログオフしており、切断されたセッションは実行されていません。
- カタログ内のすべてのマシンでメンテナンスモードがオンになっており、新しい接続が確立できないこと。
- カタログ内のすべてのマシンが電源オフになっていること。
- カタログはデリバリーグループに関連付けられていません。つまり、デリバリーグループにはそのカタログのマシンが含まれていません。

カタログを削除するには：

1. Web Studioにサインインします。
2. 左側のペインで**Machine Catalogs**を選択します。
3. カタログを選択し、アクションバーで**マシンカタログの削除**を選択します。
4. カタログ内のマシンを削除するかどうかを指定します。マシンを削除することを選択した場合、それらのマシンのActive Directoryコンピューターアカウントを保持するか、無効にするか、削除するかを指定します。

Azure のレガシー MCS カタログをマシンプロファイルベースのカタログに変換する

マシンプロファイルベースではないマシンカタログをマシンプロファイルベースのマシンカタログに変換するには、次の手順を実行します。

1. **マシンカタログ**ページで、変換する**マシンカタログ**名を右クリックし、**マシンカタログの編集**を選択します。
2. **マシンカタログの編集 > マシンプロファイル**ページで、**マシンプロファイルを使用する（Microsoft Entra IDでは必須）**チェックボックスをオンにします。
3. **マシンプロファイルの選択**をクリックします。
4. **マシンプロファイルの選択**ページで、マシンプロファイルとして使用する仮想マシンまたは起動テンプレートを選択します。
5. 現在の設定の一部が新しいマシンプロファイルの設定と異なる場合は、使用する設定に必要なオプションを選択し、**続行**をクリックします。
6. **適用**をクリックします。

> **注:**
>
> 現在、この機能はAzure、AWS、VMwareでのみサポートされています。

カタログ内のActive Directoryコンピューターアカウントを管理する

マシンカタログ内のActive Directoryアカウントを管理するには、次の操作を実行できます。

- シングルセッションOSおよびマルチセッションOSカタログからActive Directoryコンピューターアカウントを削除して、未使用のマシンアカウントを解放します。これらのアカウントは、他のマシンに使用できます。
- カタログにマシンが追加されたときにコンピューターアカウントがすでに存在するように、アカウントを追加します。OU名にスラッシュ（/）を使用しないでください。

Active Directoryアカウントを管理するには：

1. Web Studioにサインインします。
2. 左側のペインで**Machine Catalogs**を選択します。
3. カタログを選択し、アクションバーで**Manage AD accounts**を選択します。

4. コンピューターアカウントを追加するか削除するかを選択します。アカウントを追加する場合は、アカウントのパスワードをどうするかを指定します。すべてリセットするか、すべてのアカウントに適用されるパスワードを入力します。

   現在のアカウントパスワードが不明な場合は、パスワードをリセットできます。パスワードリセットを実行する権限が必要です。パスワードを入力すると、インポート時にアカウントのパスワードが変更されます。アカウントを削除する際は、Active Directory内のアカウントを保持するか、無効にするか、削除するかを選択します。

カタログからマシンを削除したり、カタログを削除したりする際に、Active Directoryアカウントを保持するか、無効にするか、削除するかを指定します。

カタログを更新する

カタログ内のマシンを更新する前に、マスターイメージのコピーまたはスナップショットを保存することをお勧めします。データベースは、各マシンカタログで使用されたマスターイメージの履歴レコードを保持します。カタログ内のマシンをロールバックまたは元に戻して、マスターイメージの以前のバージョンを使用します。ユーザーがデスクトップに展開した更新プログラムで問題が発生した場合に、このタスクを実行します。これにより、ユーザーのダウンタイムが最小限に抑えられます。マスターイメージを削除、移動、または名前変更しないでください。それらを使用してカタログを元に戻すことはできません。

マシンが更新されると、自動的に再起動します。

マスターイメージを更新または作成する

マシンカタログを更新する前に、既存のマスターイメージを更新するか、ホストハイパーバイザー上に新しいマスターイメージを作成します。

1. ハイパーバイザーで、現在のVMのスナップショットを取得し、そのスナップショットに意味のある名前を付けます。このスナップショットは、必要に応じてカタログ内のマシンを元に戻す（ロールバックする）ために使用できます。
2. 必要に応じて、マスターイメージの電源をオンにし、ログオンします。
3. 更新プログラムをインストールするか、マスターイメージに必要な変更を加えます。
4. VMの電源をオフにします。
5. VMのスナップショットを取得します。Web Studioでカタログが更新されたときに認識されるような、意味のある名前を付けます。Web Studioでスナップショットを作成することもできますが、Citrixではハイパーバイザー管理コンソールを使用して作成することをお勧めします。その後、Web Studioでそのスナップショットを選択します。このプロセスにより、自動生成され

た名前ではなく、意味のある名前と説明を提供できます。GPUマスターイメージの場合、マスターイメージはXenServer®コンソールからのみ変更できます。

マスターイメージを変更する

カタログ内のすべてのマシンに更新プログラムを準備して展開するには：

1. Web Studioにサインインします。
2. 左側のペインで**Machine Catalogs**を選択します。
3. カタログを選択し、アクションバーで **［マスターイメージの変更］** を選択します。
4. **［イメージ］** ページで、展開するホストとイメージを選択します。

> **ヒント:**
>
> MCSで作成されたカタログの場合、イメージにメモを追加して注釈を付けることができます。メモには最大500文字を含めることができます。マスターイメージを変更するたびに、メモを追加したかどうかにかかわらず、メモ関連のエントリが作成されます。メモを追加せずにカタログを更新した場合、エントリはnull (-) として表示されます。イメージのメモ履歴を表示するには、カタログを選択し、下部ペインで **［テンプレートプロパティ］** をクリックし、 **［メモ履歴の表示］** をクリックします。

5. 「**展開戦略**」ページで、マシンカタログ内のマシンを新しいマスターイメージで更新するタイミング（次回のシャットダウン時または即時）を選択します。

> **注:**
>
> **［ロールアウト戦略］** ページは永続VMでは利用できません。ロールアウトは非永続VMにのみ適用されるためです。

6. 「**概要**」ページで情報を確認し、「**完了**」をクリックします。各マシンは更新後に自動的に再起動します。

更新の進行状況を追跡するには、「**マシンカタログ**」でカタログを見つけ、インラインの進行状況バーと段階的な進行状況グラフを表示します。

Web StudioではなくPowerShell SDKを直接使用してカタログを更新する場合は、ハイパーバイザーテンプレート（**VMTemplates**）を指定します。これは、イメージまたはイメージのスナップショットの代替として使用します。

Azureベースのマシンカタログに新しいマスターイメージを展開するには：

1. Web Studioで、左側のペインから**** を選択します。
2. Azure カタログを選択し、アクションバーで「**マスターイメージの変更**」を選択します。
3. 「**マスターイメージの変更**」ページで、マスターイメージの下にあるイメージを選択します。ブレードには、リソースと同じリージョンに属するすべてのイメージが一覧表示されます。

展開戦略：

次回のシャットダウン時にイメージを更新すると、現在使用されていないマシン、つまりアクティブなユーザーセッションがないマシンにすぐに影響します。使用中のシステムは、現在のアクティブセッションが終了したときに更新を受け取ります。以下を考慮してください。

- 該当するマシンでの更新が完了するまで、新しいセッションを起動することはできません。
- シングルセッションOSマシンでは、マシンが使用されていないとき、またはユーザーがログオンしていないときに、マシンはすぐに更新されます。
- 子マシンを持つマルチセッションOSの場合、再起動は自動的に行われません。更新されたマスターイメージを適用するには、Studio、PowerShell、またはWorkspaceを使用してマシンを再起動します。マシンまたはハイパーバイザーからの再起動では、更新は適用されません。

> **ヒント:**
>
> ホスト接続の詳細設定を使用して、再起動されるマシンの数を制限します。これらの設定を使用して、特定のカタログに対して実行されるアクションを変更します。詳細設定はハイパーバイザーによって異なります。

マスターイメージをロールバックする

更新された、または新しいマスターイメージを展開した後、それをロールバックできます。このプロセスは、新しく更新されたマシンで問題が発生した場合に必要になることがあります。ロールバックすると、カタログ内のマシンは最後に正常に動作したイメージにロールバックされます。新しいイメージを必要とする新機能は利用できなくなります。展開と同様に、マシンのロールバックには再起動が含まれます。

1. Web Studioにサインインします。

2. 左側のペインで**Machine Catalogs**を選択します。
3. カタログを選択し、アクションバーで を選択します。
4. 展開操作の前のセクションで説明されているように、以前のマスターイメージをマシンに適用するタイミングを指定します。

ロールバックは、元に戻す必要があるマシンにのみ適用されます。新しいまたは更新されたマスターイメージで更新されていないマシンは、通知メッセージを受信せず、強制的にログオフされることもありません。

ロールバックの進行状況を追跡するには、 でカタログを見つけて、インラインの進行状況バーと段階的な進行状況グラフを表示します。

機能レベルを変更または変更を元に戻す

マシンのVDAを新しいバージョンにアップグレードした後、マシンカタログの機能レベルを変更します。Citrixは、すべての最新機能にアクセスできるように、すべてのVDAを最新バージョンにアップグレードすることを推奨します。

マシンカタログの機能レベルを変更する前に、次の点に注意してください。

- アップグレードされたマシンを起動して、Controllerに登録させます。このプロセスにより、Web Studioはカタログ内のマシンがアップグレードを必要としていることを判断できます。

カタログの機能レベルを変更するには：

1. Web Studioにサインインします。
2. 左側のペインで**Machine Catalogs**を選択します。
3. カタログを選択します。下ペインの**「詳細」**タブにバージョン情報が表示されます。
4. **機能レベルの変更**を選択します。Web Studioがカタログのアップグレードが必要であると検出した場合、メッセージが表示されます。プロンプトに従ってください。1台以上のマシンをアップグレードできない場合、その理由を説明するメッセージが表示されます。すべてのマシンが適切に機能するように、Citrixは**変更**をクリックして続行する前に、マシンの問題を解決することを推奨します。

カタログの変更が完了した後、カタログを選択し、アクションバーで**機能レベルの変更を元に戻す**を選択することで、マシンを以前のVDAバージョンに戻すことができます。

カタログを複製する

カタログを複製する前に、次の考慮事項に注意してください。

- オペレーティングシステムおよびマシン管理に関連する設定は変更できません。複製されたカタログは、元のカタログからこれらの設定を継承します。

> **注:**
>
> 複製するAzureカタログを選択し、マスターイメージを選択した場合、ブレードにはリソースと同じリージョンに属するすべてのイメージが一覧表示されます。

- カタログの複製には時間がかかる場合があります。必要に応じて、**「進行状況を非表示」**を選択して、バックグラウンドで複製を実行します。
- クローンされたカタログは元の名前を継承し、サフィックス `Copy` を持ちます。名前は変更できます。「カタログの名前を変更する」を参照してください。
- クローン作成が完了したら、クローンされたカタログをデリバリーグループに割り当てるようにしてください。

1. Web Studioにサインインし、左側のペインで**マシンカタログ**を選択します。
2. カタログを選択し、アクションバーで を選択します。
3. ウィンドウで、クローンされたカタログの設定を表示し、必要に応じて設定を構成します。 を選択して次のページに進みます。
4. ページで、設定の概要を表示し、 を選択してクローン作成を開始します。
5. 必要に応じて、 を選択して、バックグラウンドでクローン作成を実行します。

フォルダーを使用してカタログを整理する

フォルダーを作成してカタログを整理し、簡単にアクセスできるようにすることができます。たとえば、イメージの種類別または組織構造別にカタログを整理できます。

> **ヒント:**
>
> アクションバーの右上にある**フォルダー**アイコンをクリックすると、マシンカタログノードの優先デフォルトビュー（フォルダービューまたはリストビュー）を設定できます。

カタログフォルダーを作成する

開始する前に、まずカタログの整理方法を計画してください。次の点を考慮してください。

- フォルダーは最大5レベルまでネストできます（デフォルトのルートフォルダーを除く）。
- カタログフォルダーには、カタログとサブフォルダーを含めることができます。
- Web Studioのすべてのノード（**マシンカタログ**、**デリバリーグループ**、**アプリケーション**、**アプリケーショングループ**など）は、バックエンドで同じフォルダーツリーを共有します。フォルダーの名前変更や移動の際に名前の競合を避けるため、異なるノード間で最上位フォルダーには一意の名前を使用してください。

  `New-BrokerAdminFolder` SDKコマンドレットを使用してフォルダーを作成し、それを**マシンカタログ**ノードの下に表示させたい場合は、`Set-BrokerAdminFolderMetadata`コマンドレットを使用して`ContainsMachineCatalogs`メタデータを追加する必要があります。

  例:

  ```
  Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
  ContainsMachineCatalogs -Value true
  ```

カタログフォルダーを作成するには、次の手順に従います。

1. 左側のペインで**Machine Catalogs**を選択します。
2. フォルダー階層でフォルダーを選択し、**アクション**バーで**フォルダーの作成**を選択します。
3. 新しいフォルダーの名前を入力し、**完了**をクリックします。

ヒント:

意図しない場所にフォルダーを作成した場合でも、正しい場所にドラッグして移動できます。

カタログを移動する

カタログはフォルダー間で移動できます。詳細な手順は次のとおりです。

1. 左側のペインで**Machine Catalogs**を選択します。
2. フォルダー別にカタログを表示します。フォルダー階層の上にある**すべて表示**をオンにすると、すべてのカタログを一度に表示することもできます。
3. カタログを右クリックし、**マシンカタログの移動**を選択します。
4. カタログの移動先のフォルダーを選択し、**完了**をクリックします。

> **ヒント:**
>
> カタログをフォルダーにドラッグできます。

カタログフォルダーの管理

カタログフォルダーの削除、名前の変更、移動ができます。

フォルダーとそのサブフォルダーにカタログが含まれていない場合にのみ、フォルダーを削除できます。

フォルダーを管理するには、以下の手順に従います。

1. 左側のペインで**Machine Catalogs**を選択します。
2. フォルダー階層でフォルダーを選択し、必要に応じて**アクション**バーでアクションを選択します。
   - フォルダーの名前を変更するには、**フォルダー名の変更**を選択します。
   - フォルダーを削除するには、**フォルダーの削除**を選択します。
   - フォルダーを移動するには、**フォルダーの移動**を選択します。
3. 画面の指示に従って、残りの手順を完了します。

VDAのアップグレード

Studioインターフェースを使用して、VDAsを簡単にアップグレードできます。詳細および段階的なガイダンスについては、Citrix VDA Upgrade Serviceドキュメントを参照してください。

カタログ作成を再試行する

> **注:**
>
> この機能はMCSカタログにのみ適用されます。

失敗したカタログにはエラーアイコンが表示されます。詳細を確認するには、各カタログの**トラブルシューティング**タブに移動します。カタログの作成を再試行する前に、以下の考慮事項に注意してください。

- まずトラブルシューティング情報を確認し、問題を解決してください。この情報には、検出された問題が記述されており、それらを解決するための推奨事項が提供されています。
- オペレーティングシステムおよびマシン管理に関連する設定は変更できません。カタログは、元の設定を継承します。
- 作成には時間がかかる場合があります。必要に応じて、**進行状況を非表示**を選択して、バックグラウンドで作成を実行します。

カタログの作成を再試行するには、次の手順を実行します。

1. Web Studioから、左側のペインで**マシンカタログ**を選択します。
2. カタログを選択し、その**トラブルシューティング**タブに移動します。
3. 再試行ハイパーリンクをクリックして、カタログの作成を再試行します。
4. 表示されるウィザードで、必要に応じて設定を変更します。変更する必要がない場合は、直接**概要**ページに移動できます。
5. 完了したら、**完了**を選択して作成を開始します。

トークンを使用してMCS以外のプロビジョニング済みVDAを登録する

MCS以外でプロビジョニングされたVDAの登録トークンを生成および管理できるようになりました。この実装により、MCSでVDAをプロビジョニングすることなく、WebSocket経由でVDAを登録できます。この機能は、Linux Virtual Delivery Agent、macOS用Citrix Virtual Delivery Agent、およびCitrix Virtual Apps and Desktops™を使用するドメインに参加していないVDAもサポートします。

始める前に

1. サイトを構成します。詳細については、「サイトの作成」を参照してください。
2. Delivery ControllerにTLS証明書をインストールします。詳細については、「ControllerにTLSサーバー証明書をインストールする」を参照してください。
3. Delivery Controllerを信頼するために、VDAにルートCAと中間CAをインストールします。
4. Delivery ControllerでWebSocket接続を有効にします。サイト上の各Delivery Controllerで次のコマンドを実行します。

```
New-ItemProperty "HKLM:\SOFTWARE\Citrix\DesktopServer\WorkerProxy"
-Name "WebSocket_Enabled" -PropertyType "DWord" -Value 1 -Force
```

注:

> WebSocketを有効にした後、Delivery Controllerを再起動してください。

登録トークンの生成

Citrix以外でプロビジョニングされたマシン向けにトークンベースの登録を有効にすることを決定したら、まずマシンカタログごとにトークンを生成し、その後、VDAインストール管理者と共有する必要があります。

登録トークンの特徴：

- 登録範囲：1〜5000台のVDAマシン
- 有効期間：最大14日間

Web Studioを使用してカタログのトークンを生成するには、次の手順に従います。

1. **Web Studio > マシンカタログ**で、**マシン数**列に**プロビジョニング方法: 手動**と表示されている、MCSでプロビジョニングされていないカタログを見つけます。
2. カタログを右クリックし、**登録トークンの管理**を選択します。
3. 表示される**登録トークンの生成**ページで、次のトークン情報を提供します。
   - トークンの名前を入力します。
   - 有効期間を入力します。期間は14日以内である必要があります。トークンは指定された期間のみ有効です。
   - （オプション）トークンで登録されたVDAの電源管理のためにホスト接続を選択します。オプションには、このカタログのゾーン下のすべてのホスト接続が含まれます。
   - トークンの使用制限（1〜5000）を入力します。
4. **生成**をクリックします。
5. 表示される**トークンが正常に生成されました**ウィンドウで、トークンをコピーして安全な場所に保存するか、**ダウンロード**をクリックして**ダウンロード**フォルダーにダウンロードします。

   トークンリストにトークンレコードが表示されます。

   トークンの生成(/en-us/citrix-virtual-apps-desktops/current-release/media/token-based-enrollment.png)
6. トークンをVDAインストール管理者と共有します。

マシンにVDAとトークンをインストールする方法の詳細については、「VDAsのインストール」を参照してください。

トークンの管理

トークンを取り消してVDA登録に使用できないようにするには、2つのオプションがあります。

- 取り消し：トークンを取り消しますが、ログ記録のためにリストに残します。
- 削除：トークンを取り消し、リストから削除します。

> **注:**
>
> 期限切れのトークンは14日後に自動的に削除されます。

WebSocket VDA登録ツールを使用してマシンをカタログに登録する

WebSocket VDA登録ツールは、VDAマシン向けのトークンベースの登録を容易にします。このツールは、登録トークンを使用してVDAをマシンカタログに追加することで、接続をWebSocket接続に変換するのに役立ちます。

> **注:**
>
> このツールは、どのマシンカタログにも登録されていないVDAマシンを登録するために設計されています。

登録ツールを実行するには、以下の手順に従ってください。

1. VDAにログオンします。
2. `C:\Program Files\Citrix\Virtual Desktop Agent\Web Socket Vda Enrollment Tool` にあるツール `EnrollMachine.exe` を見つけます。
3. 適切な入力パラメータを指定してツールを実行します。例：`EnrollMachine.exe -websocket_token_string:xxxxxxxxx`

次の表は、登録ツールの入力パラメータについて説明しています。

パラメータ名	必須	説明	例
`-websocket_token_stdin`	はい	登録トークンを読み取ります。	`.\EnrollMachine.exe -websocket_token_stdin`
`-websocket_token_string`		コマンドラインパラメータから登録トークンを直接読み取ります。	`.\EnrollMachine.exe -websocket_token_string:<token>`
`-websocket_token_file:[token-file-path]`		指定されたパスから登録トークンを読み取ります。	`.\EnrollMachine.exe -websocket_token_file:C:\token\test2.txt`
`log:[log-file-path]`	いいえ	登録ツールのログを表示します。	`.\EnrollMachine.exe log:[C:\ProgramData\Citrix\EnrollMachine\EnrollMachine.txt]`
`-help`	いいえ	短いヘルプテキストを表示します。	`.\EnrollMachine.exe -help`

登録が成功すると、ツールとログに成功メッセージが表示されます。Web Studioにサインインして、VDAマシンがカタログに追加され、マシンのステータスが登録済みであることを確認してください。

トラブルシューティング

デフォルトでは、登録ツールのログは次の場所にあります。

`C:\ProgramData\Citrix\EnrollMachine\EnrollMachine.txt`

ログに別のパスを指定した場合は、`log:[log-file-path]` を使用してログを取得できます。

次の表に、登録ツールによって返されるコードを示します。

コード	文字列	説明
0	成功	VDAがマシンカタログに正常に追加されました。
-1	InvalidArgument	登録トークン内の入力パラメーターが無効です。
-2	BrokerAgentNotFound	ブローカーエージェントサービスが見つかりません。
-3	TokenInvalid	入力されたトークンが無効です。
-4	TokenMissingRequiredClaims	トークンに必要なクレーム（CustomerIdや登録URIなど）がありません。
-5	InternalError	一般的なエラーが発生しました。
-6	タイムアウト	タスクがタイムアウトしました。
-7	マシンのAD参加ステータスの判別失敗	マシンのAD参加ステータスを返すサービスが失敗しました。
-8	ADマシンSIDの検索失敗	ADマシンSIDを返すサービスが失敗しました。
-9	登録要求の失敗	HTTPエラーにより要求が失敗しました。
-10	登録応答に必須フィールドがありません	登録ツールの応答にパラメーター `VirtualSiteId` がありません。
-11	権限不足	タスクを実行するために必要な権限がありません。

コード	文字列	説明
-12	マシンのAAD参加ステータスを判断できませんでした	マシンのAD参加ステータスを確認するサービスがエラーをスローしました。
-13	AADマシンがデバイスIDを見つけられませんでした	システムによって追加された追加パラメーター `AAD device id` が空です。
-14	AADデバイスIDが無効です	システムによって追加された追加パラメーター `AAD device id` は有効なGUIDではありません。
-15	有効なMACアドレスがありません	無効なMACアドレスです。
-16	FailedToGetComputerHostNameForVdaInstanceName	追加パラメーター `VdaInstanceName` を設定するためのコンピューターホスト名の取得に失敗しました。
-17	VirtualDesktopAgentRegistryKeyFailedToOpen	デリバリーコントローラーのリストを書き込むためのVDAレジストリキーを開くのに失敗しました。
-18	失敗したトークンが最大数に達しました	失敗したトークンが最大数に達しました。

PowerShell を使用する

このセクションでは、PowerShellを使用してカタログを管理する方法について詳しく説明します。

- カタログに関連付けられている警告とエラーを取得する(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/machine-catalogs-manage.html#retrieve-warnings-and-errors-associated-with-a-catalog)
- イメージに説明を追加する
- OSディスクをリセットする

- 既存のプロビジョニングスキームのネットワーク設定を変更する
- マシンカタログのバージョンを管理する(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/machine-catalogs-manage.html#manage-versions-of-a-machine-catalog)
- マシンプロファイルに基づかないマシンカタログを、マシンプロファイルに基づくマシンカタログに変換する(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/machine-catalogs-manage.html#convert-a-non-machine-profile-based-machine-catalog-to-machine-profile-based-machine-catalog)
- アクティブなコンピューターアカウントのID情報を修復する
- 既存のマシンカタログのキャッシュ構成を変更する
- ローカルファイル共有アクセスによるVDA更新のサポート(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/machine-catalogs-manage.html#vda-update-support-via-local-file-share-access)

カタログに関連付けられた警告とエラーを取得する

履歴エラーと警告を取得して、MCSマシンカタログの問題を理解し、それらの問題を修正できます。

PowerShellコマンドを使用して、次のことができます。

- エラーまたは警告のリストを取得する
- 警告の状態を**新規**から**確認済み**に変更する
- エラーまたは警告を削除する

PowerShellコマンドを実行するには:

1. PowerShell ウィンドウを開きます。
2. Citrix 固有の PowerShell モジュールをロードするには、`asnp citrix*` を実行します。

エラーと警告のリストを取得するには：

`Get-ProvOperationEvent` コマンドを実行します。

- パラメーターなしの場合：すべてのエラーと警告を取得します
- `LinkedObjectType` および `LinkedObjectUid` パラメーターを使用する場合：特定のプロビジョニングスキームに関連付けられているすべてのエラーと警告を取得します
- `EventId` パラメーターを使用する場合：このイベント ID に一致する特定のエラーまたは警告を取得します

- `Filter`パラメーターを使用: カスタマイズされたフィルターでエラーまたは警告を取得します

エラーまたは警告の状態を **New** から **Acknowledged** に変更するには：

`Confirm-ProvOperationEvent` コマンドを実行します。

- `EventId` パラメーターを使用する場合：このイベント ID に一致する特定のエラーまたは警告の状態を設定します。特定のイベントのエラーまたは警告の `EventId` は、`Get-ProvOperationEvent` コマンドの出力として取得できます。
- `LinkedObjectType` および `LinkedObjectUid` パラメーターを使用する場合：特定のプロビジョニングスキームに関連付けられているすべてのエラーと警告の状態を設定します
- `All` パラメーターを使用する場合：すべてのエラーと警告の状態を **Acknowledged** に設定します

エラーまたは警告を削除するには：

`Remove-ProvOperationEvent` コマンドを実行します。

- `EventId` パラメーターを使用する場合: このイベントIDに一致する特定のエラーまたは警告を削除します。特定のイベントまたは警告の `EventId` は、`Get-ProvOperationEvent` コマンドの出力として取得できます。
- `LinkedObjectType` および `LinkedObjectUid` パラメーターを使用する場合: 特定のプロビジョニングスキームに関連付けられているすべてのエラーと警告を削除します。
- `All` パラメーターを使用する場合: すべてのエラーと警告を削除します。

詳しくは、Citrix PowerShell SDKを参照してください。

ハイパーバイザーアクセスなしでマシンを削除する

VMまたはプロビジョニングスキームを削除する際、MCSはVMから、場合によってはベースディスクからもタグを削除する必要があります。これにより、削除オプションに含まれるリソースがMCSによって追跡または識別されなくなります。ただし、これらのリソースの一部はハイパーバイザーを介してのみアクセス可能です。ハイパーバイザーアクセスがない場合でも、`Remove-ProvVM` PowerShell の `PurgeDBOnly` オプションを使用して、VM、ベースディスク、ACG内のイメージなどのVMリソースオブジェクトをデータベースから削除します。

このオプションは以下で有効になります。

- サポートされているすべてのハイパーバイザー

- 永続VMおよび非永続VM

制限事項

-PurgeDBOnly コマンドと -ForgetVM コマンドを同時に使用することはできません。

PurgeDBOnly コマンドを使用する

PowerShell コマンド `Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -ForgetVM` を実行すると、以下のシナリオで削除操作が失敗する可能性があります。

- ホスト接続がメンテナンスモードになっている
- 無効な資格情報
- 認証失敗
- 許可されていない操作
- ハイパーバイザーに到達できません

> **注:**
>
> Remove-provVM -ForgetVM は永続的なVMのみを対象とします。リスト内のVMのいずれかが非永続的である場合、操作は失敗します。

> ハイパーバイザーに到達できないために操作が失敗すると、次のプロンプトが表示されます。

`Try to use -PurgeDBOnly option to clean DDC database.`.

MCSデータベースからVMの参照を削除するには、`Remove-ProvVM` PowerShellコマンドで`-PurgeDBOnly`オプションを使用します。例：

```
Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -PurgeDBOnly
```

イメージに説明を追加する

マシンカタログのイメージ更新に関連する変更について、情報提供の記述を追加できます。この機能を使用して、カタログの作成時、またはカタログの既存のマスターイメージを更新する際に説明を追加します。カタログ内の各マスターイメージの情報を表示することもできます。イメージの説明を追加または表示するには、次のコマンドを使用します。

- マスターイメージを使用してマシンカタログを作成する際にメモを追加するには、`NewProvScheme`コマンドで`MasterImageNote`パラメーターを使用します。例：

```
C:\PS>New-ProvScheme -ProvisioningSchemeName <name> -HostingUnitName
<name> -IdentityPoolName <name> -MasterImageVM

XDHyp:\HostingUnits\<hosting unit name>\<vm name>.vm\Base.snapshot
-MasterImageNote "Note"
```

- マシンカタログに関連付けられているマスターイメージを更新するには、`Publish-ProvMasterVMImage`コマンドで`MasterImageNote`パラメーターを使用します。例：

```
C:\PS>Publish-ProvMasterVMImage -ProvisioningSchemeName <name>
-MasterImageVM XDHyp:\HostingUnits\<hosting unit name>\<vm
name>.vm\base.snapshot -MasterImageNote "Note"
```

- 各イメージの情報を表示するには、Get-ProvSchemeMasterVMImageHistoryコマンドを使用します。例：

```
C:\PS>Get-ProvSchemeMasterVMImageHistory -ProvisioningSchemeName
MyScheme -Showall
```

ロールバックの進行状況を追跡するには、 でカタログを見つけて、インラインの進行状況バーと段階的な進行状況グラフを表示します。

次のような特定のシナリオでは、ロールバックできません。（ オプションは表示されません）。

- ロールバックする権限がありません。
- カタログがMCSを使用して作成されていません。
- カタログがOSディスクのイメージを使用して作成されています。
- カタログの作成に使用されたスナップショットが破損しています。
- カタログ内のマシンに対するユーザーの変更が保持されません。
- カタログ内のマシンが実行中です。

OSディスクをリセットする

MCSで作成されたマシンカタログ内の永続VMのOSディスクをリセットするには、PowerShellコマンド`Reset-ProvVMDisk`を使用します。現在、この機能はAWS、Azure、XenServer、Google Cloud、SCVMM、VMwareの仮想化環境に適用できます。

PowerShellコマンドを正常に実行するには、以下を確認してください。

- ターゲットVMが永続MCSカタログ内にあること。
- MCSマシンカタログが正常に機能していること。
- これは、プロビジョニングスキームとホストが存在し、プロビジョニングスキームに正しいエントリがあることを意味します。
- ハイパーバイザーがメンテナンスモードではないこと。
- ターゲットVMの電源がオフになっており、メンテナンスモードになっていること。

OSディスクをリセットするには、次の手順を実行します。

1. PowerShell ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、**asnp citrix***を実行します。
3. 次のいずれかの方法でPowerShellコマンド`Reset-ProvVMDisk`を実行します。
    - VMのリストをコンマ区切りリストとして指定し、各VMでリセットを実行します。

      ```
      Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName ("abc","def")
      -OS
      ```

    - `Get-ProvVM`コマンドからの出力としてVMのリストを指定し、各VMでリセットを実行します。

      ```
      (Get-ProvVM -ProvisioningSchemeName "xxx") | Reset-ProvVMDisk "abc"
      -OS
      ```

    - 名前で単一のVMを指定します。

      ```
      Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
      ```

    - `Get-ProvVM`コマンドによって返されるVMごとに個別のリセットタスクを作成します。各タスクは、ハイパーバイザーの機能チェック、各VMの接続チェックなど、同じ冗長なチェックを実行するため、これは効率的ではありません。

```
Get-ProvVM -ProvisioningSchemeName "xxx" | Reset-ProvVMDisk
-ProvisioningSchemeName "xxx" -OS
```

4. リセットされるVMのリストと、回復不能な操作であるという警告メッセージが表示された確認プロンプトが表示されます。回答を入力せずに**Enter**キーを押すと、それ以上のアクションは実行されません。

   注:

   リセットプロセスが完了するまで、VMをメンテナンスモードから解除したり、電源をオンにしたりしないでください。

   PowerShellコマンド`-WhatIf`を実行して、実行されるアクションを出力し、アクションを実行せずに終了できます。

   次のいずれかの方法を使用して、確認プロンプトをバイパスすることもできます。

   - `-Force`パラメーターを指定します。

     ```
     Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
     -Force
     ```

   - `-Confirm:$false`パラメーターを指定します。

     ```
     Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
     -Confirm:$false
     ```

   - `Reset-ProvVMDisk`を実行する前に、`$ConfirmPreference`を**None**に変更します。

     ```
     PS C:\Windows\system32> $ConfirmPreference='None'

     PS C:\Windows\system32> $ConfirmPreference

     None

     PS C:\Windows\system32> Reset-ProvVMDisk -ProvisioningSchemeName
     "xxx" -VMName "abc" -OS
     ```

5. `Reset-ProvVMDisk`コマンドによって返されるタスクのステータスを取得するには、`Get-ProvTask`を実行します。

既存のプロビジョニングスキームのネットワーク設定を変更する

既存のプロビジョニングスキームのネットワーク設定を変更して、新しいVMが新しいサブネットワーク上に作成されるようにすることができます。ネットワーク設定を変更するには、`Set-ProvScheme`コマンドで`-NetworkMapping`パラメーターを使用します。

> **注:**
>
> この機能は、Citrix Virtual Apps and Desktops 2203 LTSR CU3以降のバージョンでサポートされています。

> 既存のプロビジョニングスキームのネットワーク設定を変更するには、次の手順を実行します。

1. PowerShellウィンドウで、コマンド`asnp citrix*`を実行してPowerShellモジュールをロードします。
2. 変更するネットワークパスに移動するには、`(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps`を実行します。
3. 新しいネットワーク設定に変数を割り当てます。例:

   ```
   $NewNetworkMap = @{"0"= "XDHYP:\HostingUnits\MyNetworks\Network 0.network"}
   ```

4. `Set-ProvScheme -ProvisioningSchemeName "name" -NetworkMapping $NewNetworkMap`を実行します。
5. 既存のプロビジョニングスキームの新しいネットワーク設定を確認するには、`(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps`を実行します。

マシンカタログのバージョンを管理する

MCSマシンカタログが`Set-ProvScheme`コマンドで更新されると、現在の構成がバージョンとして保存されます。その後、PowerShellコマンドを使用して、マシンカタログのさまざまなバージョンを管理できます。次のことができます。

- マシンカタログのバージョンリストを表示する

- 以前のバージョンを使用してマシンカタログを更新する
- そのマシンカタログのVMで使用されていないバージョンは手動で削除する
- マシンカタログで保持される最大バージョン数を変更する（デフォルトは99）

バージョンには、マシンカタログの次の情報が含まれます。

- VMCpuCount
- VMMemoryMB
- CustomProperties
- ServiceOffering
- MachineProfile
- NetworkMapping
- SecurityGroup

マシンカタログのさまざまなバージョンを管理するには、次のコマンド（例として提供）を実行します。

- マシンカタログのさまざまなバージョンの構成詳細を表示するには：

```
Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog
```

- マシンカタログの特定のバージョンの構成詳細を表示するには：

```
Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -Version 2
```

- マシンカタログに関連付けられているバージョンの総数を確認するには：

```
(Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog).Count
```

- 以前のバージョンを使用してマシンカタログを更新するには：

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -Version 2
```

- そのマシンカタログのVMによって使用されていないバージョンを手動で削除するには：

```
Remove-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -Version
3
```

- マシンカタログで保持される最大バージョン数を設定します（デフォルトは99）。この設定は、すべてのカタログに適用されます。たとえば、この場合、すべてのMCSプロビジョニング済みカタログに対して最大15バージョンが保持されます。

```
Set-ProvServiceConfigurationData -Name "MaxProvSchemeVersions" -Value
15
```

バージョン数が最大バージョン数に達した場合、マシンカタログ内のいずれかのVMで古いバージョンが使用されていると、新しいバージョンを作成できません。その場合は、次のいずれかを実行してください。

- マシンカタログによって保持される最大バージョン数の制限を増やします。
- 古いバージョンを使用している一部のVMを更新して、それらの古いバージョンがどのVMからも参照されなくなり、削除できるようにします。

マシンプロファイルベースではないマシンカタログをマシンプロファイルベースのマシンカタログに変換する

VM、テンプレート仕様（Azureの場合）、起動テンプレート（AWSの場合）、またはVMwareテンプレート（VMwareの場合）をマシンプロファイルの入力として使用して、マシンプロファイルに基づかないマシンカタログをマシンプロファイルに基づくマシンカタログに変換できます。カタログに追加された新しいVMは、明示的なカスタムプロパティによって上書きされない限り、マシンプロファイルからプロパティ値を取得します。

注:

既存のマシンプロファイルベースのマシンカタログを、マシンプロファイルベースではないマシンカタログに変更することはできません。

これを行うには：

1. 永続的または非永続的なマシンカタログを、VMを使用して、マシンプロファイルなしで作成します。
2. **PowerShell**ウィンドウを開きます。

3. マシンプロファイルからのプロパティ値を、マシンカタログに追加された新しいVMに適用するには、`Set-ProvScheme`コマンドを実行します。例:

   - Azureの場合:

     ```
     Set-ProvScheme -ProvisioningSchemeName xxxx -MachineProfile XDHyp:
     \HostingUnits\<HostingUnitName>\machineprofile.folder\<ResourceGroup
     Name>\<TemplateSpecName>\<VersionName>
     ```

   - AWSの場合:

     ```
     Set-ProvScheme -ProvisioningSchemeName xxxx -MachineProfile "XDHyp:
     \HostingUnits\<hosting-unit>\<launch-
     template>.launchtemplate\<launch-template-
     version>.launchtemplateversion"
     ```

   - VMwareの場合:

     ```
     Set-ProvScheme -ProvisioningSchemeName "my-prov-scheme"
     -MachineProfile "XDHyp:\HostingUnits\my-hosting-unit\my-
     template.template"
     ```

     注:

     VMwareテンプレートから`FolderID`が派生するのを避けるために、`FolderID`をカスタムプロパティとして設定します。

アクティブなコンピューターアカウントのID情報を修復する

ID関連の問題があるアクティブなコンピューターアカウントのID情報をリセットできます。マシンパスワードと信頼キーのみをリセットするか、IDディスクのすべての構成をリセットするかを選択できます。この実装は、永続的および非永続的な両方のMCSマシンカタログに適用できます。

注:

現在、この機能はAWS、GCP、Azure、SCVMM、XenServer、およびVMwareの仮想化環境でサポートされています。

条件

IDディスクを正常にリセットするには、以下を確認してください。

- VMをシャットダウンし、メンテナンスモードに設定します
- PowerShellコマンドにパラメーター-OSを含めないでください

IDディスクのリセット

IDディスクをリセットするには：

1. **PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. ID情報をリセットします。

    - マシンパスワードと信頼キーのみをリセットするには、次のコマンドを実行します。

    ```
    Repair-AcctIdentity -IdentityAccountName TEST\VM1
    -PrivilegedUserName TEST\admin1 -PrivilegedUserPassword $password
    -Target IdentityInfo
    ```

    コマンドで使用されるパラメーターの説明は次のとおりです。

        - IdentityAccountName：修復する必要があるIDアカウントの名前。
        - PrivilegedUserName：IDプロバイダー（ADまたはAzureAD）に対する書き込み権限を持つユーザーアカウント。
        - PrivilegedUserPassword：PrivilegedUserNameのパスワード。
        - Target: 修復アクションのターゲット。アカウントパスワード/信頼キーを修復するためのIdentityInfo、およびMicrosoft Entraハイブリッド参加済みマシンIDのユーザー証明書属性を修復するためのUserCertificateを指定できます。

    - IDディスクのすべての構成をリセットするには、次のコマンドを次の順序で実行します。

    ```
    Repair-AcctIdentity -IdentityAccountName TEST\VM1
    -PrivilegedUserName TEST\admin1 -PrivilegedUserPassword $password
    -Target IdentityInfo
    ```

```
Reset-ProvVMDisk ProvisioningSchemeName <name> -VMName <name>  -
Identity
```

- IDディスクを完全に再作成するには:

```
Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMname <name>
-Identity -Recreate
```

注:

マシンがVDAバージョン2511以降を使用するWindowsマシンの場合、`-Recreate` の設定に関係なく、以前と同じ `MachineGuid` を引き続き使用します。

4. アクションを確定するには「**y**」と入力します。`-Force` パラメーターを使用して確認プロンプトをスキップすることもできます。例:

```
Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMName <name>
-Identity -Force
```

5. 更新されたIDディスク設定を確認するには、`Get-ProvVM -ProvisioningSchemeName <name> -VMName <name>` を実行します。IDディスクの属性（例: `IdentityDiskId`）は更新されている必要があります。`StorageId` と `IdentityDiskIndex` は変更されていてはなりません。

既存のマシンカタログのキャッシュ構成を変更する

MCSIOを有効にして非永続カタログを作成した後、Set-ProvSchemeコマンドを使用して以下のパラメータを変更できます。

- WriteBackCacheMemorySize
- WriteBackCacheDiskSize

この機能は現在、以下に適用されます。

- GCPおよびMicrosoft Azure環境、および
- MCSIOが有効な非永続カタログ

要件

キャッシュ構成を変更するための要件は次のとおりです。

- VDA を最新バージョン (2308 以降) に更新します。
- 既存のマシンカタログでパラメーター `UseWriteBackCache` を有効にします。`UseWriteBackCache` が有効なマシンカタログを作成するには、`New-ProvScheme` を使用します。例:

```
New-ProvScheme -ProvisioningSchemeName $CatalogName -HostingUnitUid
$HostingUnitUid `

-IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `

-MasterImageVM $MasterImage `

-ServiceOffering $ServiceOffering `

-NetworkMap $NetworkMap `

-SecurityGroup $SecurityGroup `

-UseWriteBackCache -WriteBackCacheDiskSize 8
```

キャッシュ構成を変更する

Set-ProvSchemeコマンドを実行します。例:

```
Set-ProvScheme -ProvisioningSchemeName $provScheme.ProvisioningSchemeName
-WriteBackCacheDisk32 -WriteBackCacheMemorySize 128
```

注:

- 少なくとも 1 GB のキャッシュディスクストレージが必要なため、`WriteBackCacheDiskSize` の値はゼロより大きくする必要があります。
- `WriteBackCacheMemorySize` の値は、マシンカタログのメモリサイズよりも小さくする必要があります。

- これらの変更は、変更後にカタログに追加された新しい VM にのみ影響します。既存の VM はこれらの変更の影響を受けません。

ローカルファイル共有アクセスによるVDAアップデートのサポート

PowerShellコマンドレットを介してVDAインストーラーの場所を指定することで、各VDAがCitrix Managed Azure CDNから新しいVDAインストーラーを取得できるようにするためのネットワークルールを提供する手間を省くことができます。

PowerShellコマンドレット

ローカルファイル共有からインストーラーを使用できるようにする、**New-VusCatalogSchedule** および **New-VusMachineUpgrade** コマンドレットに2つの新しいオプションパラメータが追加されました。

- **VdaWorkstationPackageUri** - ワークステーションOS VDAインストーラーへのUNCパスを指定します。
- **VdaServerPackageUri** - サーバーOS VDAインストーラーへのUNCパスを指定します。

前提条件

- VDA 2311に付属するVUSエージェントインストーラー
- VDAアップグレードエージェントをバージョン7.40.0.35以降にアップグレード（VDAインストーラーバージョン2311以降を使用）
- Virtual Apps and Desktops Remote PowerShell SDK バージョン 7.40 以降 (Jan 10, 2024 以降にリリース)

ファイル共有のアクセス許可を設定する方法

VDAインストーラーパッケージを含むネットワーク共有には、Local System (NT AUTHORITY\SYSTEMプリンシパル) として実行されるVDAアップグレードエージェントサービスに対する読み取りアクセス権が必要です。

- **ドメイン参加済みファイル共有のアクセス許可**

  VDAマシンがドメインに参加している場合、**ローカルシステム**アカウント（VUAはローカルシステムとして実行されます）は、ネットワーク共有にアクセスする際にコンピューターの資格情報を使用します。

  最小特権のアクセス許可は、Domain Computers に **読み取り** アクセスを付与することで設定できます。

a. ファイルを共有するネットワーク上のユーザーを選択します。

b. **詳細な共有設定** をクリックし、**ファイルとプリンターの共有** をオンにします。

- **ドメインに参加していないファイル共有のアクセス許可**

  VDA マシンがドメインに参加していない場合、**ローカルシステム** アカウント (VUA はローカルシステムとして実行されます) は、ネットワーク共有にアクセスするときに **ANONYMOUS LOGON** を使用します。

  a. 共有フォルダーを選択します。

  b. パスワード保護を無効にします。

     a. フォルダーの **プロパティ** に移動します。

     b. **ネットワークと共有センター** を選択します。

     c. **パスワード保護共有** をオフにします。

  c. **詳細な共有** をクリックして、共有アクセス許可を付与します。

     a. **アクセス許可** を選択します。

     b. **ANONYMOUS LOGON** に **読み取り** 共有アクセス許可を付与します。

  d. フォルダーのアクセス許可を付与するには、**セキュリティ** タブを選択します。

     a. 共有フォルダーにアクセス許可を追加するには、**編集** をクリックします。

     b. 共有フォルダーを選択し、**ANONYMOUS LOGON** にフォルダーのアクセス許可を付与します。

  e. **詳細設定**をクリックして、**ファイルとプリンターの共有**をオンにします。

  f. 共有フォルダー名を**ネットワークアクセスセキュリティポリシー**に追加します。

> **注:**
>
> 変更をすぐに有効にするには、マシンを再起動します。

ローカルファイル共有からのVDAアップデート

1. VDAインストーラーをダウンロードし、共有ファイルに配置します。

> **注:**

> Virtual Upgrade Serviceを使用すると、Current ReleaseトラックまたはLTSRトラックのいずれかを選択できます。

> **例：** マシンカタログがCurrent Release（2311）に設定されており、VDAバージョンが2305の場合、VDAをバージョン2311にアップグレードする必要があります。

a. 弊社のWebサイトの**ダウンロード**ページに移動します。
b. 製品として**Citrix Virtual Apps and Desktops**を選択します。
c. **シトリックス バーチャルアプリ＆デスクトップ 7 2311, 全エディション**を選択します。
d. **製品ISOに含まれるが個別にパッケージ化されているコンポーネント**の展開可能な項目からVDAインストーラーを選択します。

2. カタログの種類に基づいて、関連するVDAインストーラーを選択します。

- カタログの種類が**マルチセッション**の場合は、**マルチセッションOS VDAインストーラー**をダウンロードします。
- カタログの種類が**シングルセッション**の場合は、**シングルセッションOS VDAインストーラー**をダウンロードします。
- カタログタイプが**Remote PC Access**の場合は、**Single-session OS Core Services VDA installer**をダウンロードします。

> **注:**
>
> ファイル共有インストーラーのバージョンは、VUSによってクラウドに公開された最新のインストーラーバージョンと**正確に**一致している必要があります。

VMのストレージ移行

VMwareおよびXenServer環境では、既存のVMのディスクストレージを古いストレージから新しいストレージに移動できます。移行中、MCSは電源管理、OSディスクのリセットなどのVM機能を保持します。新しいディスクストレージを使用して、新しいVMをマシンカタログに追加することもできます。これを行うには、PowerShellコマンド `Move-ProvVMDisk` を使用します。

フルクローン永続VMと非永続VMを移行できます。

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

新しいストレージは、次の条件を満たす必要があります。

- 古いストレージと同じクラスター内にある必要があります。
- VMが実行されているホストは、古いデータストアと新しいデータストアの両方にアクセスできる必要があります。

ディスクストレージの移行

ディスクストレージを移行するには：

1. 既存のホスティングユニットに宛先ストレージを追加します。宛先ストレージを追加するには、PowerShellコマンド `Add-Hyphostingunitstorage` を実行します。

   古いストレージに新しいVMを追加したくない場合は、古いストレージを**Superseded**に変更します。これはStudioまたはPowerShellコマンドを使用して実行できます。Studioについては、ストレージの編集 を参照してください。または、`Set-Hyphostingunitstorage` を実行し、`Superseded` を `true` に設定して、古いストレージでの新しいVM作成を無効にします。

   > **注:**
   >
   > 非永続VMの場合：
   >
   > - WBCを使用する場合は、ホスティングユニットでWBC宛先ストレージを構成します。
   > - OS宛先ストレージが構成されている場合、WBC（使用されている場合）はOS宛先ストレージと互換性がある必要があります。
   > - OS宛先ストレージが構成されていない場合、WBC（使用されている場合）は現在のOSストレージと互換性がある必要があります。

2. VMをシャットダウンし、**メンテナンスモード**をオンにします。
3. プロビジョニングスキーム、ホスティングユニット、OSディスクストレージ、およびWBCディスクストレージに関する情報を取得します。

- OSストレージ情報については、`ProvResourceInStorage` を実行します。例：

```
$result=Get-ProvSchemeResourceInStorage -ProvisioningSchemeName
xxxxx

$result

$result.ProvResourceInStorage | Format-List -Property *
```

- WBCストレージ情報については`TemporaryStorageInfo`を実行します。例:

```
$result=Get-ProvSchemeResourceInStorage -ProvisioningSchemeName
xxxxx

$result

$result.TemporaryStorageInfo | Format-List -Property *
```

4. OSディスク、IDディスク、およびWBCディスク (非永続VMに適用) を`Move-ProvVMDisk` PowerShellコマンドを使用して宛先ストレージに移行します。

> **注:**
>
> - 常にOSディスクとIDディスクをDiskTypeおよび`DestinationStorageId`パラメーターで指定します。
> - OSディスクとIDディスクの`DestinationStorageId`は同じである必要があります。

例:

永続VM：

```
(Get-ProvVM -ProvisioningSchemeName xxxxx) | Move-ProvVMDisk
-ProvisioningSchemeName "myFullCloneProvScheme" -VMName "machine01"
-DiskType OS,Identity -DestinationStorageId datastore1,datastore1
```

> **重要:**

永続VMの場合、すべてのディスクが移動されます。移動するディスクを選択することはできません。

非永続VM：

```
(Get-ProvVM -ProvisioningSchemeName xxxxx) | Move-ProvVMDisk
-ProvisioningSchemeName "myCleanOnBootProvScheme" -VMName "machine01"
-DiskType OS,Identity,WBC -DestinationStorageId None,None,datastore1
```

重要:

- 特定のディスクを移行したくない場合は、`DestinationStorageId`パラメーターの値を`None`として設定します。
- VMにWBCディスクがある場合は、WBCディスクを`DiskType`パラメーターに追加し、必要な情報を`DestinationStorageId`パラメーターに追加します。

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

既存のMCSプロビジョニング済みマシンカタログは、PowerShellコマンド`Set-ProvSchemeImage`を使用して準備済みイメージマシンカタログに変換できます。ただし、移行後にレガシーカタログに戻すことはできません。現在、この機能はAzureおよびVMware仮想化環境に適用されます。

制限事項

次の制限事項を考慮してください。

- MCSカタログが永続データディスクを使用している場合、そのカタログを準備済みイメージを使用するように移行することはできません。
- MCSカタログがアンマネージドディスクを使用している場合、そのカタログを準備済みイメージを使用するように移行することはできません。

準備済みイメージマシンカタログへの移行

移行するには、次の手順を実行します。

1. StudioまたはPowerShellコマンドを使用して、イメージ定義とイメージバージョンを作成します。イメージ定義とイメージバージョンを作成する手順については、以下を参照してください。
   - アジュール:
     - ウェブスタジオ
     - PowerShell
   - ヴイエムウェア：
     - ウェブスタジオ
     - PowerShell
2. プロビジョニングスキームのUIDを取得するには、`Get-ProvScheme`コマンドを実行します。例:

```
Get-ProvScheme -ProvisioningSchemeName <name> | select
ProvisioningSchemeName, ProvisioningSchemeUid
```

3. イメージ定義名、イメージバージョン仕様のUIDを取得するには、`Get-ProvImageVersionSpec`コマンドを実行します。例:

```
Get-ProvImageVersionSpec -ImageDifinitionName <name> -Filter
{IsPrepared -eq $true} | select ImageDefinitionName ImageVersionSpecUId
```

4. 既存のMCSプロビジョニング済みマシンカタログを準備済みイメージマシンカタログに移行するには、`Set-ProvSchemeImage`コマンドを実行します。例:

```
Set-ProvSchemeImage -ProvisioningSchemeName [ProvisioningSchemeName]
-ImageVersionSpecUid [ImageVersionSpecUid]
```

5. カタログが移行されたことを確認するには、`Get-ProvScheme`コマンドを実行します。例:

```
Get-ProvScheme -ProvisioningSchemeName <name> | select
ProvisioningSchemeName, ProvisioningSchemeUid, ImageVersionSpecUid
```

トラブルシューティング

- 「Power State Unknown」ステータスのマシンについては、ガイダンスとしてCTX131267を参照してください。
- 不明な電源状態を継続的に表示するVMを修正するには、How to fix VMs that continuously show an unknown power stateを参照してください。

次のステップ

特定のクラウドサービスカタログの管理については、以下を参照してください。

- AWSカタログの管理
- XenServerカタログを管理する(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/machine-catalogs-manage/manage-machine-catalog-citrix-hypervisor.html)
- Google Cloud Platformカタログの管理
- Microsoft Azureカタログを管理する(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/machine-catalogs-manage/manage-machine-catalog-azure.html)
- Microsoft System Center Virtual Machine Managerカタログを管理する(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/machine-catalogs-manage/manage-machine-catalog-mscvmm.html)
- VMwareカタログを管理する(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/machine-catalogs-manage/manage-machine-catalog-vmware.html)

AWS EC2カタログを管理する

マシンカタログの管理は、マシンカタログを管理するウィザードについて説明します。以下の情報は、AWS EC2クラウド環境に固有の詳細を扱っています。

> **注:**
>
> AWSカタログを管理する前に、AWSカタログの作成を完了する必要があります。AWS EC2カタログの作成を参照してください。

タグを削除する

カタログまたはVMを作成すると、MCSによって作成されたタグが以下のリソースに作成されます。

- 仮想マシン

- ルートディスクボリューム
- 識別ディスクボリューム
- NIC
- ルートディスクイメージ (AMI)
- 起動テンプレート
- AMIまたはルートディスクのスナップショット

Citrix®データベースからVMとマシンカタログを削除し、MCSによって作成されたタグを削除できます。以下を使用できます。

- `Remove-ProvVM`を`ForgetVM`パラメーターとともに使用して、マシンカタログから単一のVMまたはVMのリストからVMとMCSによって作成されたタグを削除します。
- `Remove-ProvScheme`を`ForgetVM`パラメーターとともに使用して、Citrixデータベースからマシンカタログを削除し、マシンカタログからリソースを削除します。

この機能は、永続VMにのみ適用されます。

これを行うには：

1. **PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. VMを削除する前にVMをロック解除します。例：

   ```
   Unlock-ProvVM -ProvisioningSchemeName "<name>" -VMID "<id"
   ```

4. 以下のいずれかのコマンドを実行して、リソースからVM、マシンカタログ、およびMCSによって作成されたタグを削除します。

   - `Remove-ProvVM`を`ForgetVM`とともに実行して、CitrixデータベースからVMを、VMからタグを削除します。例：

     ```
     Remove-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name>"
     -ForgetVM
     ```

   - `Remove-ProvScheme`を実行して、Citrixデータベースからマシンカタログを削除し、マシンカタログからリソースを削除します。例：

```
Run Remove-ProvScheme -ProvisioningSchemeName "<name>" -ForgetVM
```

5. VMがDelivery Controller™から削除されていることを確認しますが、ハイパーバイザーからは削除されていません。

   a. `Get-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name>"`を実行します。これは何も返さないはずです。

   b. AWS EC2コンソールに移動します。VMは表示されますが、タグは削除されています。以下のリソースからタグが削除されます。

      - 仮想マシン
      - ルートディスクボリューム
      - 識別ディスクボリューム
      - NIC

6. マシンカタログを削除する場合は、そのカタログがDelivery Controllerから削除されていることを確認します。

   a. `Get-ProvScheme -ProvisioningSchemeName "forgetvmdemo"`を実行します。これはエラーを返すはずです。

   b. AWS EC2コンソールで、以下のリソースが削除されていることを確認します。

      - ルートディスクイメージ (AMI)
      - 起動テンプレート
      - AMIまたはルートディスクのスナップショット

MCSによって作成されたリソースを識別する

以下は、MCS がリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
IDディスク	"名前": "VMName_IdentityDisk"
	"Xd構成": "Xdプロビジョニング済み=true"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

リソース名	タグ
イメージ	"Xd構成": "Xdプロビジョニング済み=true"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
NIC	"説明": "XD NIC"
	"Xd構成": "Xdプロビジョニング済み=true"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
OSディスク	"名前": "VMName_rootDisk"
	"Xd設定": "XdProvisioned=True"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "Citrix リソース": ""
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""
PrepVM	"Name": "準備 - カタログ名 - xxxxxxxxxx"
	"Xd構成": "Xdプロビジョニング済み=true"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "Citrix リソース": ""
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""
公開されたスナップショット	"Xd構成": "Xdプロビジョニング済み=true"

リソース名	タグ
	ボリュームワーカーAMIのスナップショットでない場合、「CitrixProvisioningSchemeId」：「xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx」
テンプレート	[when AwsCaptureInstanceProperties = true] "XdConfig": "XdProvisioned=true"
	[when AwsCaptureInstanceProperties = true] "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] 「CitrixResource」：「」
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] 「CitrixOperationalResource」：「」
カタログ内のVM	"Xd構成": "Xdプロビジョニング済み=true"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] 「CitrixResource」：「」
	[when AwsCaptureInstanceProperties = true] "AWS EC2起動テンプレートID":"lt-xxxx"
	[when AwsCaptureInstanceProperties = true] "AWS EC2起動テンプレートバージョン": "n"
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] 「CitrixOperationalResource」：「」
ボリュームワーカーAMI	"Xd構成": "Xdプロビジョニング済み=true"
ボリュームワーカーブートストラッパー	"名前": "XenDesktop® Temp"
	"Xd構成": "Xdプロビジョニング済み=true"

リソース名	タグ
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] 「CitrixVolumeWorkerBootstrapper」: 「」
ボリュームワーカーインスタンス	"名前": "Citrix.XD.Volumeworker-xxxx-xx-xx-xx-xxxx"
	"Xd構成": "Xdプロビジョニング済み=true"

詳細情報

- 接続とリソースの作成および管理
- AWS EC2への接続
- マシンカタログの作成
- AWS EC2カタログを作成する
- マシンカタログの管理

Amazon WorkSpaces Core マネージドインスタンスのカタログを管理する

マシンカタログの管理では、マシンカタログを管理するウィザードについて説明します。以下の情報は、Amazon WorkSpaces Core マネージドインスタンスに固有の詳細を扱っています。

> **注:**
>
> Amazon WorkSpaces Core マネージドインスタンスのカタログを管理する前に、Amazon WorkSpaces Core マネージドインスタンスのカタログの作成を完了する必要があります。Amazon WorkSpaces Core マネージドインスタンスのカタログを作成するを参照してください。

タグを削除する

カタログまたはVMを作成すると、以下のリソースにタグが作成されます。

- 仮想マシン
- ルートディスクボリューム
- 識別ディスクボリューム
- 弾力性のあるネットワークインターフェース (ENI)
- ルートディスクイメージ (AMI)
- 起動テンプレート
- AMIまたはルートディスクのスナップショット

Citrix®データベースからVMとマシンカタログを削除し、Citrixが作成したタグを削除できます。以下を使用できます。

- マシンカタログから単一のVMまたはVMのリストからVMとCitrixが作成したタグを削除するには、`ForgetVM`パラメーターを指定した`Remove-ProvVM`を使用します。

  > **注:**
  >
  > `ForgetVM`パラメーターを使用すると、Citrixのプロビジョニングスキームデータベースからが削除されますが、VMはハイパーバイザーに残ります。

- `Remove-ProvScheme`を`ForgetVM`パラメーターとともに使用して、Citrixデータベースからマシンカタログを削除し、マシンカタログからリソースを削除します。

これを行うには：

1. **PowerShell**ウィンドウを開きます。
2. `asnp citrix*`を実行して、Citrix固有のPowerShellモジュールをロードします。
3. VMを削除する前にVMをロック解除します。例：

   ```
   Unlock-ProvVM -ProvisioningSchemeName "<name>" -VMID "<id"
   ```

4. 次のいずれかのコマンドを実行して、VM、マシンカタログ、およびリソースからCitrixが作成したタグを削除します。

   - `Remove-ProvVM`を`ForgetVM`とともに実行して、CitrixデータベースからVMを削除し、VMからCitrixが作成したタグを削除します。例：

```
Remove-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name>"
-ForgetVM
```

- `Remove-ProvScheme`を実行して、Citrixデータベースからマシンカタログを削除し、マシンカタログからリソースを削除します。例：

```
Run Remove-ProvScheme -ProvisioningSchemeName "<name>" -ForgetVM
```

5. VMがDelivery Controller™から削除されているが、ハイパーバイザーからは削除されていないことを確認します。

   a. `Get-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name>"`を実行します。これは何も返さないはずです。

   b. AWS EC2コンソールに移動します。VMは表示されますが、Citrixが作成したタグは削除されています。以下のリソースからCitrixが作成したタグが削除されます。

      - 仮想マシン
      - ルートディスクボリューム
      - 識別ディスクボリューム
      - ENI

6. マシンカタログを削除する場合は、そのカタログがDelivery Controllerから削除されていることを確認します。

   a. `Get-ProvScheme -ProvisioningSchemeName "forgetvmdemo"`を実行します。これはエラーを返すはずです。

   b. AWS EC2コンソールで、以下のリソースが削除されていることを確認します。

      - ルートディスクイメージ (AMI)
      - 起動テンプレート
      - AMIまたはルートディスクのスナップショット

MCSによって作成されたリソースを識別する

以下は、MCSがAWSプラットフォーム上のリソースに追加するタグです。表のタグは「"key":"value"」として表されています。

リソース名	タグ
IDディスク	"名前": "VMName_IdentityDisk"
	"Xd構成": "Xdプロビジョニング済み=true"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
イメージ	"Xd構成": "Xdプロビジョニング済み=true"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
ENI	"説明": "XD Nic"
	"Xd構成": "Xdプロビジョニング済み=true"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
OSディスク	"名前": "VMName_rootDisk"
	"Xd設定": "XdProvisioned=True"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
PrepVM	"Name": "準備 - カタログ名 - xxxxxxxxxx"
	"Xd構成": "Xdプロビジョニング済み=true"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
公開されたスナップショット	"Xd構成": "Xdプロビジョニング済み=true"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
テンプレート	"Xd構成": "Xdプロビジョニング済み=true"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

リソース名	タグ
カタログ内のVM	"Xd構成": "Xdプロビジョニング済み=true"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

詳細情報

- AWS仮想化環境
- Amazon WorkSpaces Coreマネージドインスタンスへの接続
- イメージ管理
- Amazon WorkSpaces Coreマネージドインスタンス用の準備済みイメージを作成する
- Amazon WorkSpaces Core マネージドインスタンスのカタログを作成する(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/create-catalog-amazon-wsc.html)
- 準備済みイメージマシンカタログを管理する(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/manage-prepared-image-machine-catalogs.html)

XenServer®カタログを管理する

マシンカタログの管理では、マシンカタログを管理するウィザードについて説明します。以下の情報は、XenServer仮想化環境に固有の詳細を扱います。

> **注:**
>
> XenServerカタログを管理する前に、XenServerカタログの作成を完了する必要があります。「XenServerカタログの作成」を参照してください。

MCSによって作成されたリソースを識別する

以下は、MCS がリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
公開されたベースディスクと、各ネットワークまたはローカルストレージ上のそのコピー	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

リソース名	タグ
IDディスク	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
OSディスク	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
準備用 VM	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
カタログ内のVM	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
WBCディスク	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

詳細情報

- 接続とリソースの作成および管理
- XenServerへの接続
- マシンカタログの作成
- XenServerカタログを作成する
- マシンカタログの管理

Google Cloud Platformカタログを管理する

マシンカタログの管理では、マシンカタログを管理するウィザードについて説明します。以下の情報は、Google Cloud環境に固有の詳細を扱います。

> **注:**
>
> Google Cloud Platformカタログを管理する前に、Google Cloud Platformカタログの作成を完了する必要があります。Google Cloud Platformカタログの作成を参照してください。

マシンカタログの管理

カタログにマシンを追加したり、マシンを更新したり、更新をロールバックしたりするには、「マシンカタログの管理」を参照してください。

電源管理

Citrix DaaS™を使用すると、Google Cloudマシンの電源管理を行うことができます。左ペインの**検索**ノードを使用して、電源管理したいマシンを見つけます。以下の電源操作が利用可能です。

- 削除
- 起動
- 再起動
- 強制再起動
- シャットダウン
- 強制シャットダウン
- デリバリーグループに追加
- タグの管理
- メンテナンスモードをオンにする

Autoscaleを使用してGoogle Cloudマシンを電源管理することもできます。これを行うには、Google Cloudマシンをデリバリーグループに追加し、そのデリバリーグループでAutoscaleを有効にします。Autoscaleの詳細については、「Autoscale」を参照してください。

PowerShellを使用してプロビジョニングされたマシンを更新する

`Set-ProvScheme`コマンドはプロビジョニングスキームを変更しますが、既存のマシンには影響しません。PowerShellコマンド`Set-ProvVMUpdateTimeWindow`を使用すると、現在のプロビジョニングスキームを既存の永続マシンまたは非永続マシン、あるいはマシンセットに適用できるようになります。現在、GCPでは、この機能でサポートされているプロパティ更新はマシンプロファイルです。

更新できるもの:

- 単一のVM
- 特定のVMのリスト、またはプロビジョニングスキームIDに関連付けられている既存のすべてのVM
- プロビジョニングスキーム名に関連付けられた特定のVMのリスト、またはすべての既存のVM

既存のVMを更新するには：

1. 既存のマシンの構成を確認します。例えば、,

```
Get-ProvScheme | select ProvisioningSchemeName,
ProvisioningSchemeVersion
```

2. プロビジョニングスキームを更新します。例えば、,

```
`Set-ProvScheme –ProvisioningSchemeName "my-catalog" –MachineProfile
"XDHyp:\HostingUnits\<hosting-unit>\machineprofileinstance.vm"
```

3. VMの現在のプロパティが現在のプロビジョニングスキームと一致しているか、およびVMに保留中の更新アクションがあるかを確認します。例えば、,

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

   特定のバージョンのマシンを見つけることもできます。例えば、,

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select VMName,
ProvisioningSchemeVersion
```

4. 既存のマシンを更新します。

   - すべての既存のマシンを更新するには：

     ```
     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
     -StartsNow -DurationInMinutes -1
     ```

   - 特定のマシンのリストを更新するには：

     ```
     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
     -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
     ```

   - `Get-ProvVM`の出力に基づいてマシンを更新するには：

     ```
     Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
     ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -StartsNow
     -DurationInMinutes -1
     ```

5. 更新がスケジュールされているマシンを見つける。例：

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName,
ProvisioningSchemeUpdateAfter
```

6. マシンを再起動します。次回の電源投入時に、プロパティの変更が既存のマシンに適用されます。以下のコマンドを使用して更新されたステータスを確認できます。

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

既存のカタログのディスク関連のカスタムプロパティを変更する

既存のカタログおよびカタログの既存のVMの、以下のディスク関連のカスタムプロパティを変更できます。

- `PersistOSDisk`
- `PersistWBC`
- `StorageType`
- `IdentityDiskStorageType`
- `WbcDiskStorageType`

注:

- `StorageType` プロパティは OS ディスク用です
- `PersistOsDisk` プロパティは、ライトバックキャッシュが有効な非永続カタログに対してのみ設定できます

この実装により、カタログ作成後でも異なるディスクに異なるストレージタイプを選択できるようになり、さまざまなストレージタイプに関連する価格のバランスを取ることができます。

これを行うには、PowerShell コマンド `Set-ProvScheme` と `Set-ProvVMUpdateTimeWindow` を使用します。

1. **PowerShell**ウィンドウを開きます。
2. `asnp citrix®*`を実行します。

3. カスタムプロパティを取得するには、`Get-ProvVM -VMName <VM name>` を実行します。
4. カスタムプロパティ文字列を変更します。
   a. カスタムプロパティをメモ帳にコピーし、カスタムプロパティを変更します。
   b. **PowerShell** ウィンドウで、メモ帳から変更されたカスタムプロパティを貼り付け、変更されたカスタムプロパティに変数を割り当てます。例:

```
$cp =  '<CustomProperties xmlns=http://schemas.citrix.com/2014/xd/
machinecreation xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="CatalogZones" Value="" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" /
>

<Property xsi:type="StringProperty" Name="PersistOSDisk"
Value="true" />

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="pd-standard" />

<Property xsi:type="StringProperty" Name="StorageType" Value="pd-
standard" />

</CustomProperties>'
```

5. 既存のカタログを更新します。例:

```
Set-ProvScheme -ProvisioningSchemeName <yourCatalogName>
-CustomProperties $cp
```

6. 既存の VM を更新します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
<List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

7. VM を再起動します。次回の電源投入時に、カスタムプロパティの変更が既存の VM に適用されます。

偶発的なマシン削除からの保護

Citrix DaaSでは、偶発的な削除を防ぐために、Google Cloud上のMCSリソースを保護できます。プロビジョニングされたVMを構成するには、`deletionProtection`フラグをTRUEに設定します。

デフォルトでは、MCSまたはGoogle Cloudプラグインを介してプロビジョニングされたVMは、InstanceProtectionが有効な状態で作成されます。この実装は、永続カタログと非永続カタログの両方に適用されます。非永続カタログは、インスタンスがテンプレートから再作成されるときに更新されます。既存の永続マシンについては、Google Cloudコンソールでフラグを設定できます。フラグの設定の詳細については、「Googleドキュメントサイト」を参照してください。永続カタログに追加される新しいマシンは、`deletionProtection`が有効な状態で作成されます。

`deletionProtection`フラグを設定したVMインスタンスを削除しようとすると、リクエストは失敗します。ただし、`compute.instances.setDeletionProtection`権限が付与されているか、IAMの**Compute Admin**ロールが割り当てられている場合は、フラグをリセットしてリソースを削除できるようにすることができます。

MCSによって作成されたリソースを識別する

以下は、MCS がリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
IDディスク	"CitrixResource": "内部"
	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
イメージ	"CitrixResource": "内部"
	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
OSディスク	"CitrixResource": "内部"
	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
PrepVM	"CitrixResource": "内部"
	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

リソース名	タグ
公開されたスナップショット	"CitrixResource": "内部"
ストレージバケット	"Citrixresource": "内部向け"
テンプレート	"CitrixResource": "内部"
	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
カタログ内のVM	"CitrixResource": "内部"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx". プラグインは、MCSでプロビジョニングされたVMにもこのラベルを追加します: "citrix-provisioning-scheme-id": "provSchemeId"。このラベルを使用して、GCPコンソールでカタログによってフィルタリングできます。
WBCディスク	"CitrixResource": "内部"
	Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

注:

MCSによって作成されたリソースとして識別するために**CitrixResource**タグが追加されている場合、VMはCitrixインベントリに表示されません。タグを削除または名前変更することで、表示させることができます。

詳細情報

- 接続とリソースの作成および管理
- Google Cloud環境への接続
- マシンカタログの作成
- Google Cloud Platform カタログを作成する
- マシンカタログの管理

HPE Moonshot カタログの管理

マシンカタログの管理では、マシンカタログを管理するウィザードについて説明しています。以下の情報は、HPE Moonshot カタログに固有の詳細を扱っています。

> **注:**
>
> HPE Moonshotカタログを管理する前に、HPE Moonshotカタログの作成を完了する必要があります。

電源管理

Citrix Virtual Apps and Desktops™では、HPE Moonshotマシンの電源管理を行うことができます。電源管理を行うマシンを見つけるには、ナビゲーションペインの**検索**ノードを使用します。以下の電源操作が利用可能です。

- 起動
- シャットダウン
- 強制シャットダウン
- 再起動
- リセット

> **注:**
>
> **一時停止**および**再開**の電源操作はサポートされていません。

詳細情報

- 接続とリソースの作成および管理
- HPE Moonshotへの接続
- マシンカタログの作成
- HPE Moonshotマシンカタログの作成
- マシンカタログの管理

Microsoft Azureカタログを管理する

マシンカタログの管理では、マシンカタログを管理するウィザードについて説明します。以下の情報は、Microsoft Azure Resource Managerクラウド環境に固有の詳細を扱います。

> **注:**
>
> Microsoft Azureカタログを管理する前に、Microsoft Azureカタログの作成を完了する必要があります。Microsoft Azureカタログの作成を参照してください。

VMシャットダウン時にストレージタイプを下位層に変更する

VMをシャットダウンするときに、管理ディスクのストレージタイプを下位層に切り替えることで、ストレージコストを節約できます。これを行うには、`StorageTypeAtShutdown`カスタムプロパティを使用します。

VMをシャットダウンすると、ディスクのストレージタイプは下位層（`StorageTypeAtShutdown`カスタムプロパティで指定）に変更されます。VMの電源をオンにすると、ストレージタイプは元の状態（`StorageType`カスタムプロパティまたは`WBCDiskStorageType`カスタムプロパティで指定）に戻ります。

> **重要:**
>
> ディスクはVMが少なくとも一度電源オンになるまで存在しません。したがって、VMを最初に電源オンにしたときにストレージタイプを変更することはできません。

要件

- 管理ディスクに適用されます。これは、カスタムプロパティ`UseManagedDisks`をtrueに設定することを意味します。
- 永続OSディスクを持つ永続および非永続カタログに適用されます。これは、カスタムプロパティ`persistOsDisk`をtrueに設定することを意味します。
- 永続WBCディスクを持つ非永続カタログに適用されます。これは、カスタムプロパティ`persistWBC`をtrueに設定することを意味します。

制限

- Microsoftによると、ディスクの種類は1日2回しか変更できません。Microsoftドキュメントを参照してください。Citrixによると、VMの起動または割り当て解除アクションがあるたびに `StorageType` の更新が行われます。したがって、VMあたりの電源アクションの数を1日2回に制限してください。たとえば、午前中にVMを起動するための電源アクションを1回、夕方にVMを割り当て解除するための電源アクションを1回実行します。

ストレージの種類を下位層に変更する

手順を進める前に、要件と制限を参照してください。

1. カスタムプロパティ `StorageTypeAtShutdown` を追加し、値をStandard_LRS (HDD)に設定して、 `New-ProvScheme` を使用してカタログを作成します。PowerShellを使用してカタログを作成する方法については、 `<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>` を参照してください。

   > **注:**
   >
   > `StorageTypeAtShutdown` が空またはStandard_LRS (HDD)以外の値を持つ場合、操作は失敗します。

   永続カタログの作成中にカスタムプロパティを設定する例：

   ```
   $customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
   2014/xd/machinecreation"

   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

   <Property xsi:type="StringProperty" Name="UseManagedDisks"
   Value="true" />

   <Property xsi:type="StringProperty" Name="StorageType"
   Value="Premium_LRS" />

   <Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

   <Property xsi:type="StringProperty" Name="LicenseType"
   Value="Windows_Client" />

   <Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
   ```

```
<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'
```

非永続カタログの作成中にカスタムプロパティを設定する例：

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="WbcDiskStorageType"
Value="Standard_SSD_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />

<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'
```

> **注:**
>
> マシンプロファイルを使用する場合、カスタムプロパティは`MachineProfile`で定義されたプロパティよりも優先されます。

2. VMをシャットダウンし、AzureポータルでVMのストレージタイプを確認します。ディスクのストレージタイプは、`StorageTypeAtShutdown`カスタムプロパティで指定されたように、下位の層に変更されます。
3. VMをオンにします。ディスクのストレージの種類は、以下に記載されているストレージの種類に戻ります。
   - OSディスクの`StorageType`カスタムプロパティ
   - WBCディスクの`WBCDiskStorageType`カスタムプロパティ（`CustomProperties`で指定した場合のみ）。それ以外の場合は、`StorageType`に記載されているストレージの種類に戻ります。

既存のカタログに`StorageTypeAtShutdown`を適用する

手順を進める前に、要件と制限を参照してください。

既存のカタログにVMを追加するには、`Set-ProvScheme`を使用します。この機能は、`Set-ProvScheme`の実行後に追加された新しいVMに適用されます。既存のマシンには影響しません。

既存のカタログにVMを追加する際にカスタムプロパティを設定する例：

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="WbcDiskStorageType"
Value="Standard_SSD_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

<Property xsi:type="StringProperty" Name="LicenseType"
```

```
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />

<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'



$ProvScheme = Get-Provscheme -ProvisioningSchemeName $CatalogName



Set-ProvScheme -ProvisioningSchemeName $ProvScheme.ProvisioningSchemeName
-CustomProperties $customProperties
```

既存のVMのストレージタイプをシャットダウン時に下位層に変更する

手順を進める前に、要件と制限を参照してください。

VMがシャットダウンされているときに、既存のVMのストレージタイプを下位の層に変更することで、ストレージコストを節約できます。これを行うには、`StorageTypeAtShutdown`カスタムプロパティを使用します。

VMのシャットダウン時に、カタログ内の既存マシンのストレージタイプを下位層に変更するには：

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために、`asnp citrix®*`を実行します。
3. `Get-Provscheme -ProvisioningSchemeName $CatalogName`を実行します。
4. カスタムプロパティ文字列を変更します。

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'
```

5. 既存のカタログのプロビジョニングスキームを更新します。この更新は、`Set-ProvScheme`の実行後に追加された新しいVMに適用されます。

```
Set-ProvScheme -ProvisioningSchemeName $CatalogName -CustomProperties
$customProperties
```

6. 既存のVMを更新して`StorageTypeAtShutdown`を有効にします。

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName $CatalogName
-StartsNow -DurationInMinutes -1
```

7. 次回マシンを起動すると、マシンの`StorageTypeAtShutdown`プロパティが更新されます。ストレージタイプは次回のシャットダウン時に変更されます。
8. カタログ内の各VMの`StorageTypeAtShutdown`値を表示するには、次のコマンドを実行します。

```
Get-ProvVM -ProvisioningSchemeName <catalog-name> | foreach { $vmName =
$_.VMName; $storageTypeAtShutdown = ($_.CustomVmData | ConvertFrom-
Json).StorageTypeAtShutdown.DiskStorageAccountType; return New-Object
psobject -Property @{ "VMName" = $vmName; "StorageTypeAtShutdown" =
$storageTypeAtShutdown } }
```

プロビジョニングされたマシンを現在のプロビジョニングスキームの状態に更新する

`Set-ProvScheme`コマンドはプロビジョニングスキームを変更します。ただし、既存のマシンには影響しません。PowerShellコマンド`Set-ProvVMUpdateTimeWindow`を使用すると、現在のプロビジョニングスキームを既存の永続的または非永続的なマシン、またはマシンのセットに適用できます。また、既存のMCSプロビジョニング済みマシンの構成更新のタイムスロットをスケジュールすることもできます。スケジュールされたタイムスロット中の電源オンまたは再起動は、

スケジュールされたプロビジョニングスキームの更新をマシンに適用します。現在、Azureでは、`ServiceOffering`、`MachineProfile`、および次のカスタムプロパティを更新できます。

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`
- `LicenseType`
- `DedicatedHostGroupId`
- `PersistWBC`
- `PersistOsDisk`
- `PersistVm`
- `Zones`

注:

- Azure環境でマネージドディスクを使用するカタログの場合、`StorageType`、`WBCDiskStorageType`、および`IdentityDiskStorageType`カスタムプロパティのみを更新できます。
- `Set-ProvVMUpdateTimeWindow`を2回実行した場合、最新のコマンドが有効になります。
- VMが`Set-ProvVMUpdateTimeWindow`で更新され、Zonesカスタムプロパティによって提供される現在の可用性ゾーンリストが、VMが現在使用しているゾーンを含まないように変更された場合、VMの永続ディスクは新しいゾーンにコピーされ、元のディスクは削除されます。たとえば、ゾーン3でプロビジョニングされ、Zonesカスタムプロパティが「1,2」に設定されて更新されたVMは、ゾーン1と2の間でマシンをバランスさせるために、どちらのゾーンのマシンが少ないかに応じて、VMとそのディスクをゾーン1または2のいずれかに移動します。
- Zonesカスタムプロパティが完全にクリアされた場合（空の値に設定された場合）、VMのゾーンアフィニティは削除され、Azureは容量に基づいてVMを任意の可用性ゾーンに配置できるようになります。この場合、VMの永続ディスクは元のゾーンに残り、移動されません。

更新できるもの:

- 単一のVM
- 特定のVMのリスト、またはプロビジョニングスキームIDに関連付けられている既存のすべてのVM
- 特定のVMのリスト、またはプロビジョニングスキーム名（マシンカタログ名）に関連付けられている既存のすべてのVM

プロビジョニングスキームに以下の変更を加えると、Azureの永続カタログの場合、VMインスタンスが再作成されます:

- `MachineProfile`を変更する
- 削除 `LicenseType`
- 削除 `DedicatedHostGroupId`

> **注:**
>
> 既存のマシンのOSディスクとそのすべてのデータはそのまま残り、新しいVMがそのディスクに接続されます。

既存のVMを更新する前に:

1. 既存のマシンの構成を確認します。例えば、,

   ```
   Get-ProvScheme | select ProvisioningSchemeName,
   ProvisioningSchemeVersion
   ```

2. プロビジョニングスキームを更新します。例えば、,

   - マシンプロファイルの入力としてVMを使用する場合:

     ```
     Set-ProvScheme -ProvisioningSchemeName "my-catalog" -MachineProfile
     "XDHyp:\HostingUnits\<hosting-unit>\machineprofile.folder\<resource-
     group>.resourcegroup\<virtual-machine>.vm"
     ```

   - マシンプロファイルの入力としてテンプレート仕様を使用する場合:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog"

-MachineProfile "XDHyp:\HostingUnits\<hosting-
unit>\machineprofile.folder\<resource-
group>.resourcegroup\<template-spec>.templatespec\<template-spec-
version>.templatespecversion"

-ServiceOffering "XDHyp:\HostingUnits\<hosting-
unit>\serviceoffering.folder\<service-offering>.serviceoffering"
```

- サービス提供のみの場合:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog" -ServiceOffering
"XDHyp:\HostingUnits\<hosting-unit>\serviceoffering.folder\<service-
offering>.serviceoffering"
```

3. VMの現在のプロパティが現在のプロビジョニングスキームと一致しているか、およびVMに保留中の更新アクションがあるかを確認します。例えば、,

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

特定のバージョンのマシンを見つけることもできます。例えば、,

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select VMName,
ProvisioningSchemeVersion
```

既存のマシンに次回の再起動時に適用される更新を要求するには:

1. 既存のマシンを更新し、次回の再起動時に更新が適用されるようにするには、次のコマンドを実行します。

   - すべての既存のマシンを更新するには。例えば、,

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-StartsNow -DurationInMinutes -1
```

   - 特定の仮想マシンのリストを更新する場合。例：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

- Get-ProvVM の出力に基づいてマシンを更新する場合。例：

```
Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -StartsNow
-DurationInMinutes -1
```

注:

- `StartsNow` は、スケジュールされた開始時刻が現在の時刻であることを示します。
- 負の数（例：–1）の `DurationInMinutes` は、スケジュールの時間枠に上限がないことを示します。

2. 更新がスケジュールされているマシンを見つける。例：

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName,
ProvisioningSchemeUpdateAfter
```

3. マシンを再起動します。次回の電源投入時に、プロパティの変更が既存のマシンに適用されます。以下のコマンドを使用して、更新されたステータスを確認できます。例：

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

スケジュールされた時間枠内で次回起動時に最新のプロビジョニング設定に更新するようにVMをスケジュールするには：

1. 次のコマンドを実行します。

- 開始時刻を現在時刻として更新をスケジュールするには

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-VMName vm1 -StartsNow -DurationInMinutes 120
```

- 週末に更新をスケジュールするには

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName “ my-catalog “
-VMName “vm1” -StartTimeInUTC “10/15/2022 9:00am” -DurationInMinutes
(New –TimeSpan –Days 2).TotalMinutes
```

注:

- `VMName` はオプションです。指定しない場合、更新はカタログ全体に対してスケジュールされます。
- `StartTimeInUTC` の代わりに `StartsNow` を使用して、スケジュール開始時刻が現在時刻であることを示します。
- `DurationInMinutes` はオプションです。デフォルトは120分です。負の数（例：–1）は、スケジュールの時間枠に上限がないことを示します。

2. 更新ステータスを確認します。

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeUpdateUntil, ProvisioningSchemeVersion
```

3. VM の電源を入れます。スケジュールされた時間枠の後にマシンの電源を入れた場合、構成の更新は適用されません。スケジュールされた時間枠内にマシンの電源を入れた場合、,

- マシンがオフになっていて、
  - マシンを起動しない場合、構成の更新は適用されません
  - マシンを起動すると、構成の更新が適用されます
- マシンの電源が入っていて、
  - マシンを再起動しない場合、構成の更新は適用されません
  - マシンを再起動すると、構成の更新が適用されます。

構成の更新をキャンセルするには：

単一のVM、複数のVM、またはカタログ全体の構成更新をキャンセルすることもできます。構成更新をキャンセルするには：

1. `Clear-ProvVMUpdateTimeWindow` を実行します。例：

   - 単一のVMに対してスケジュールされた構成更新をキャンセルするには：

     ```
     Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName “ my-catalog “
     -VMName “vm1”
     ```

   - 複数のVMに対してスケジュールされた構成更新をキャンセルするには：

     ```
     Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-catalog"
     -VMName "vm1","vm2"
     ```

     注:

     VM は同じカタログのものである必要があります。

個々のVMのプロパティを更新する

永続的なMCSマシンカタログ内の個々のVMのプロパティは、PowerShellコマンド `Set-ProvVM` を使用して更新できます。ただし、更新はすぐに適用されません。更新を適用するには、PowerShellコマンド `Set-ProvVMUpdateTimeWindow` を使用して時間枠を設定する必要があります。

この実装により、マシンカタログ全体を更新することなく、個々のVMを効率的に管理できます。現在、この機能はAzure環境にのみ適用されます。

現在、更新できるプロパティは次のとおりです。

- `CustomProperties`
- `ServiceOffering`
- `MachineProfile`

この機能を使用すると、次のことができます。

- VMのプロパティを更新する
- マシンカタログの更新後もVMで更新されたプロパティを保持する
- VMに適用された構成の更新を元に戻す

VMのプロパティを更新する前に：

1. **PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. 既存のマシンカタログの構成を確認します。例：

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
```

4. 更新を適用するVMの構成を確認します。例：

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

VMのプロパティを更新する

VMのプロパティを更新するには、次の手順を実行します。

1. 更新を適用したいVMの電源をオフにします。
2. VMのプロパティを更新します。例えば、VMのストレージタイプ (`StorageType`) カスタムプロパティを更新したい場合は、以下を実行します。

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
-CustomProperties "...<Property Name='StorageType'
Value='Premium_LRS' />..."
```

マシンカタログ内の2つのVMのプロパティを同時に更新できます。例:

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
-CustomProperties "...<Property Name='StorageType'
Value='Premium_LRS' />..."
```

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine2
-CustomProperties "...<Property Name='StorageType'
Value='StandardSSD_LRS' />..."
```

注:

更新はすぐに適用されません。

3. 更新対象として指定されたプロパティのリストと構成バージョンを取得します。例:

```
Get-ProvVMConfiguration -ProvisioningSchemeName AzureCatalog -VMName
machine1
```

`Version` のプロパティ値と、更新対象のプロパティ (この場合は `StorageType`) を確認します。

4. 構成バージョンを確認します。例:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

`ProvVMConfigurationVersion` のプロパティ値を確認します。更新はまだ適用されていません。VMはまだ古い構成のままです。

5. スケジュールされた更新を要求します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog
-StartsNow -DurationInMinutes -1
```

スケジュールされた更新の詳細については、プロビジョニングされたマシンを現在のプロビジョニングスキームの状態に更新する を参照してください。

> **注:**
>
> 保留中のプロビジョニングスキームの更新も適用されます。

6. VMを再起動します。例:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

7. 構成バージョンを確認します。例:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

`ProvVMConfigurationVersion` のプロパティ値を確認します。更新が適用されました。VMは新しい構成になりました。

8. VMにさらに構成アップデートを適用するには、VMをオフにして、手順を繰り返します。

マシンカタログの更新後にVMで更新されたプロパティを保持する

VMで更新されたプロパティを保持するには、以下を実行します。

1. 更新を適用したいVMの電源をオフにします。
2. マシンカタログを更新します。たとえば、VMサイズ (`ServiceOffering`) とストレージタイプ (`StorageType`) を変更したい場合は、以下を実行します。

   ```
   Set-ProvScheme -ProvisioningSchemeName AzureCatalog -ServiceOffering
   Standard_E4_v3 -CustomProperties "...<Property Name='StorageType'
   Value='StandardSSD_LRS' />..."
   ```

3. マシンカタログの構成詳細を取得します。例:

   ```
   Get-ProvScheme -ProvisioningSchemeName AzureCatalog
   ```

   `ProvisioningSchemeVersion` が1つ増えました。VMサイズとストレージタイプも更新されます。

4. VMのプロパティを更新します。たとえば、VMにマシンプロファイルを提供します。

   ```
   Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
   -MachineProfile "XDHyp:\HostingUnits\<hosting-
   unit>\machineprofile.folder\<resource-group>.resourcegroup\<template-
   spec>.templatespec\<template-spec-version>.templatespecversion"
   ```

   注:

   マシンプロファイルの入力には、タグと異なるVMサイズ (`ServiceOffering`) が指定されています。

5. VM上の構成アップデートとマシンカタログのアップデートをマージした後にVMが持つプロパティのリストを取得します。例:

   ```
   Get-ProvVMConfigurationResultantSet -ProvisioningSchemeName
   AzureCatalog -VMName machine1
   ```

> **注:**
>
> VMに対するすべてのアップデートは、マシンカタログで行われたアップデートを上書きします。

6. VMのスケジュールされたアップデートを要求します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -VMName
machine1 -StartsNow -DurationInMinutes -1
```

7. VMを再起動します。例:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

   VMは、マシンプロファイルから派生した更新済みのVMサイズを保持します。マシンプロファイルで指定されたタグ値もVMに適用されます。ただし、ストレージタイプは最新のプロビジョニングスキームから派生します。

8. VMの構成バージョンを取得します。例:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

   `ProvisioningSchemeVersion` と `ProvVMConfigurationVersion` に最新バージョンが表示されます。

VMに適用された構成の更新を元に戻す

1. VMに更新を適用した後、VMをシャットダウンします。
2. 次のコマンドを実行して、VMに適用された更新を削除します。例:

```
Set-ProvVM -RevertToProvSchemeConfiguration -ProvisioningSchemeName
AzureCatalog -VMName machine1
```

3. VMのスケジュールされたアップデートを要求します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -VMName
machine1 -StartsNow -DurationInMinutes -1
```

4. VMを再起動します。例:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

5. VMの構成バージョンを確認します。例:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

`ProvVMConfigurationVersion` の値が、マシンカタログの構成バージョンになります。

ディスク暗号化の変更

Azure仮想化環境でディスク暗号化を変更し、次の操作を実行できます。

- マスターイメージのDESとは異なるディスク暗号化セット（DES）を使用してMCSマシンカタログを作成するには、`New-ProvScheme` コマンドを使用します。例：

```
$customProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="DiskEncryptionSetId" Name="Zones" Value="/
subscriptions/XXXXXXXXXXXXXXXXXXXXXXXXXXXX/resourceGroups/testrsg/
providers/Microsoft.Compute/diskEncryptionSets/test-diskEncryptionSet"/
>

</CustomProperties>

"@

New-ProvScheme -CleanOnBoot `

-ProvisioningSchemeName $provisioningSchemeName `

-HostingUnitName $hostingUnitName `

-IdentityPoolName $identityPoolName `

-InitialBatchSizeHint $numberOfVms `

-masterImagePath $masterImagePath `
```

```
-NetworkMapping $networkMapping `

-CustomProperties $customProperties
```

- 既存のMCSマシンカタログおよび既存のVMのディスク暗号化タイプを、あるDESキーから別のDESキーに変更するには、`Set-ProvScheme`および`Set-ProvVMUpdateTimeWindow`コマンドを使用します。VMを再起動すると、更新されたDESキーが表示されます。例：

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/456c683e2ed7/resourceGroups/testrg/providers/
Microsoft.Compute/diskEncryptionSets/diskEncryptionSet1" />

</CustomProperties>'

Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties

Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01, azu02 -StartsNow -DurationInMinutes -1
```

- 以前CMEKが有効になっていなかったMCSマシンカタログとVMを、顧客管理の暗号化キー（CMEK）暗号化（DES）、ホストでのディスク暗号化、または二重暗号化を持つように更新するには、`Set-ProvScheme`および`Set-ProvVMUpdateTimeWindow`コマンドを使用します。異なる暗号化タイプについては、Azureサーバー側暗号化、ホストでのAzureディスク暗号化、およびマネージドディスクの二重暗号化を参照してください。
- 以前暗号化されていた既存のMCSマシンカタログとVMを非暗号化にするには、`Set-ProvScheme`および`Set-ProvVMUpdateTimeWindow`コマンドを使用します。例：

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="" />
```

```
</CustomProperties>'

Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties

Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01, azu02 -StartsNow -DurationInMinutes -1
```

- プライベートエンドポイントでディスク暗号化を有効にする（`ProxyHypervisorTrafficThroughConnector`で有効化されたホスト接続を使用したMCSマシンカタログ）。プライベートエンドポイントでディスク暗号化を有効にする方法については、「プライベートエンドポイントでディスク暗号化を有効にする」を参照してください。

プライベートエンドポイントでディスク暗号化を有効にする

Azureの制限により、現在、プライベートエンドポイントに対して顧客管理キーによるサーバー側暗号化を使用することはできません。ただし、既存のMCSマシンカタログとプライベートエンドポイントを持つVMをDESキーで暗号化するように更新することは可能です。

プライベートエンドポイントを持つ既存のマシンカタログを更新する

プライベートエンドポイントを持つ既存のマシンカタログを更新する詳細な手順は次のとおりです。

1. `ProxyHypervisorTrafficThroughConnector`を介してディスク暗号化なしでカタログを作成します。
2. `DiskEncryptionSetId`を使用してカタログを更新するには、`Set-ProvScheme`を実行します。

> **注:**
>
> `DiskEcryptionSetId`は、`CustomProperties`または`MachineProfile`を介して構成できます。`CustomProperties`と`MachineProfile`の両方で定義されている場合、`CustomProperties`で定義されているプロパティが適用されます。

`CustomProperties`を使用する場合の例:

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/456c683e2ed7/resourceGroups/testrg/providers/
Microsoft.Compute/diskEncryptionSets/diskEncryptionSet1"/>

</CustomProperties>'

Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties
```

MachineProfile を使用する場合の例: ディスク暗号化が有効な VM、またはディスク暗号化設定を含むテンプレート仕様を使用します:

```
Set-ProvScheme -ProvisioningSchemeName azure-catalog -MachineProfile
"XDHyp:
\HostingUnits\azureunit\machineprofile.folder\testrg.resourcegroup\new-
template.vm"
```

または、Web Studioを使用してマシンプロファイルを更新することもできます。

3. 既存のカタログ VM を更新するには、`Set-ProvVMUpdateTimeWindow` を実行します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01, azu02 -StartsNow -DurationInMinutes -1
```

4. VM を再起動すると、Azure portal の VM のディスクで更新されたディスク暗号化を確認できます。
5. 新しいカタログ VM を追加する前にディスク暗号化を解除するには、`Set-ProvScheme` を実行します。

> **注:**
>
> プライベートエンドポイントカタログを更新しているため、この手順が必要です。この手順を実行しないと、新しいVMをカタログに追加しようとしたときにエラーが発生します。

例:

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="" />

</CustomProperties>'

Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties
```

6. カタログに新しい VM を追加します。

個々のカタログ VM を更新する

個々のカタログ VM を更新する詳細な手順は次のとおりです。

1. `ProxyHypervisorTrafficThroughConnector`を介してディスク暗号化なしでカタログを作成します。
2. `DiskEncryptionSetId` を使用してカタログ VM を更新するには、`Set-ProvVM` を実行します。

注:

The `DiskEcryptionSetId` は、`CustomProperties` または `MachineProfile` のいずれかを使用して構成できます。

`CustomProperties` を使用する場合の例:

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/456c683e2ed7/resourceGroups/testrg/providers/
Microsoft.Compute/diskEncryptionSets/diskEncryptionSet1" />
```

```
</CustomProperties>'

Set-ProvVM -ProvisioningSchemeName azure-catalog  -VMName azu01
-CustomProperties $customProperties
```

MachineProfile を使用する場合の例:

```
Set-ProvVM -ProvisioningSchemeName azure-catalog  -VMName azu01
-MachineProfile "XDHyp:
\HostingUnits\azureunit\machineprofile.folder\testrg.resourcegroup\new-
template.vm"
```

3. 既存のカタログVMを更新するには、`Set-ProvVMUpdateTimeWindow` を実行します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01 -StartsNow -DurationInMinutes -1
```

4. VM を再起動すると、Azure portal の VM ディスクで更新されたディスク暗号化を確認できます。
5. 新しいVMをカタログに追加します。

既存のカタログのWBCディスクとして一時ディスクを使用する

既存のMCSマシンカタログのライトバックキャッシュディスク (WBC) ディスクとして、Azure一時ディスクを使用できます。既存のカタログとVMを更新するには、`Set-ProvScheme` PowerShellコマンドを使用します。

前提条件

既存のカタログは、次の条件を満たしている必要があります。

> **注:**
>
> 既存のカタログが次の要件を満たしていない場合、WBCディスクは一時ディスク内に配置されません。

- MCSIOが有効になっている: カスタムプロパティ `WriteBackCacheMemorySize`、`WriteBackCacheDiskSize`、および `UseWriteBackCache` が有効になっています。

- エフェメラルOSディスクが有効になっていない。
- WBCは非永続的である: `PersistWBC` は `false` です。
- `UseTempDiskForWBC` が null または false です。
- 一時ディスクのサイズは、（ライトバックキャッシュディスクサイズ + ページングファイル用の予約済み領域 + 1 GB のバッファースペース）の合計サイズよりも大きくする必要があります。

> **重要:**
>
> 一時ディスクがあるサービスオファリングから一時ディスクがないサービスオファリングへの変更、またはその逆の変更は許可されていません。

既存のカタログを更新する

既存のカタログを更新するには、次のコマンドを実行します。

1. 既存のカタログで `Set-ProvScheme` を実行して、`UseTempDiskForWBC` を `true` に更新します。例:

```
Set-ProvScheme -ProvisioningSchemeName name -CustomProperties
"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Standard_LRS`"/><Property
xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"True`"/
><Property xsi:type=`"StringProperty`" Name=`"ManagedDisksPreview`"
Value=`"False`"/><Property xsi:type=`"StringProperty`"
Name=`"PersistOsDisk`" Value=`"False`"/><Property
xsi:type=`"StringProperty`" Name=`"UseTempDiskForWBC`" Value=`"True`"/
><Property xsi:type=`"StringProperty`" Name=`"PersistWBC`"
Value=`"False`"/></CustomProperties>"
```

2. カタログに新しいマシンを追加して電源を入れます。新しい VM には、一時ディスク内に WBC ディスクがあります。

Azure VM、スナップショット、OS ディスク、およびギャラリーイメージ定義の情報を取得する

OSディスクと種類、スナップショット、ギャラリーイメージ定義を含むAzure VMの情報を表示できます。この情報は、マシンカタログが割り当てられている場合、マスターイメージ上のリソースに対して表示されます。この機能を使用して、LinuxまたはWindowsイメージを表示および選択します。PowerShellプロパティ `TemplateIsWindowsTemplate` が `AdditionDatafield` パラメーターに追加されました。このフィールドには、VMタイプ、OSディスク、ギャラリーイメージ情報、OSタイプ情報など、Azure固有の情報が含まれています。 `TemplateIsWindowsTemplate` を **True**に設定するとOSタイプがWindowsであることを示し、 `TemplateIsWindowsTemplate` を **False**に設定するとOSタイプがLinuxであることを示します。

> **ヒント:**
>
> `TemplateIsWindowsTemplate` PowerShell プロパティによって表示される情報は、Azure API から派生しています。このフィールドが空の場合があります。たとえば、データディスクからのスナップショットには `TemplateIsWindowsTemplate` フィールドが含まれていません。これは、OS の種類をスナップショットから取得できないためです。

> たとえば、PowerShell を使用して、Windows OS の種類に対して Azure VM `AdditionData` パラメーターを **True** に設定します。

```
PS C:\Users\username> (get-item XDHyp:
\HostingUnits\mynetwork\image.folder\username-dev-testing-
rg.resourcegroup\username-dev-tsvda.vm).AdditionalData

Key Value

ServiceOfferingDescription Standard_B2ms

HardDiskSizeGB 127

ResourceGroupName FENGHUAJ-DEV-TESTING-RG

ServiceOfferingMemory 8192

ServiceOfferingCores 2

TemplateIsWindowsTemplate True
```

```
ServiceOfferingWithTemporaryDiskSizeInMb 16384

SupportedMachineGenerations Gen1,Gen2
```

MCS カタログのクローンを作成する

既存の永続的および非永続的 MCS カタログを複数のカタログに分割します。元のプロビジョニングスキームのクローンを作成することで、特定の VM サブセットに異なるカタログレベルのポリシーと構成を適用できます。この機能は、組織内の異なる機能ロール（財務や役員など）が、標準ユーザーと比較して異なるリソース構成（例えば、バックアップ制限）を必要とする場合に特に役立ちます。

使用例

管理者は大規模な VM カタログを管理しています。役員チームは、標準ポリシーで許可されているよりも多くのバックアップを必要とします。管理者は `Copy-ProvScheme` コマンドを使用して、既存のカタログプロビジョニングスキームを新しいカタログにクローンします。これにより、管理者は新しい役員カタログに専用のバックアップポリシーを適用しつつ、組織の他の部分には元の設定を維持できます。

適用範囲

- Azure 環境
- 永続的および非永続的 MCS カタログ
- MCS プロビジョニングされた Citrix Provisioning カタログ

制限事項

- **プロビジョニングスキーム:** プロビジョニングスキームの最新バージョンのみがコピーされます。
- **バックアップスケジュール**: バックアップスケジュールは新しいカタログにコピーされません。新しいカタログには独自のバックアップスケジュールを設定する必要があります。
- **ID プール**: ID 関連のオブジェクトはクローンされず、同じ `ADAccountIdentityPool` を使用して共有されたままになります。
- **デリバリーグループ**: クローン作成プロセス中に、デリバリーグループの操作とユーザー割り当ては変更または関連付けられません。

重要な考慮事項

- **リソースグループ (ターゲットの場所)**:

  - `TargetLocation` (Azure リソースグループ) を提供しない場合:
    - Citrix管理のリソースグループの場合、新しいCitrix管理のリソースグループが作成されます。
    - BYO (Bring Your Own) リソースグループの場合、新しいプロビジョニングスキームのリソースは同じリソースグループに作成されます。
  - `TargetLocation` を提供する場合:
    - リソースは、指定されたリソースグループに作成されます。
    - 指定されたリソースグループは、Azureにすでに存在している必要があります。

- **ベースディスクスナップショット**: リソースグループの構成に関係なく、ベースディスクスナップショットのコピーは常に作成されます。

前提条件

- 既存のプロビジョニングスキーム (ソースカタログ) が利用可能である必要があります。
- ターゲットの場所を指定する場合、ターゲットのAzureリソースグループが存在している必要があります。

PowerShellを使用した構成

1. PowerShellウィンドウを開きます。
2. 必要なパラメーター: `SourceProvisioningSchemeName` (または `SourceProvisioningSchemeUid`) と `TargetProvisioningSchemeName` を使用して、`Copy-ProvScheme` コマンドを実行します。

   例1: プロビジョニングスキームを名前でコピーする。

   この例では、「Backup」という名前のスキームを「TestCopy」という名前の新しいスキームにコピーします。

   ```
   Copy-ProvScheme -SourceProvisioningSchemeName Backup
   -TargetProvisioningSchemeName TestCopy
   ```

   例 2: Uid でプロビジョニングスキームを特定のリソースグループにコピーする

   この例では、Uid を使用してスキームをコピーし、「TestRg」という名前のターゲットリソースグループを指定します。

```
Copy-ProvScheme -SourceProvisioningSchemeUid 771e205d-1ee5-4ad2-b044-ecf3d7f24ec7 -TargetProvisioningSchemeName TestCopy -TargetLocation TestRg
```

MCS によって作成されたリソースを識別する

以下は、MCSがリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
ID ディスク	"Citrixプロビジョニングスキーム ID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
イメージ	"Citrixプロビジョニングスキーム ID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
NIC	"Citrixプロビジョニングスキーム ID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
OSディスク	"Citrixプロビジョニングスキーム ID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
PrepVM	"Citrixプロビジョニングスキーム ID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
公開スナップショット	"Citrixプロビジョニングスキーム ID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
リソースグループ	"CitrixResource" : "内部"
	CitrixSchemaVersion: 2.0

リソース名	タグ
	"CitrixプロビジョニングスキームID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
ストレージアカウント	"CitrixプロビジョニングスキームID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
カタログ内のVM	"CitrixプロビジョニングスキームID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
WBCディスク	"CitrixプロビジョニングスキームID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"

注:

MCSによって作成されたリソースとして識別するために**CitrixResource**タグが追加されている場合、VMはCitrixインベントリに表示されません。タグを削除または名前変更することで、表示させることができます。

タグを削除する

カタログまたはVMを作成すると、以下のリソースにタグが作成されます。

- リソースグループ
- 仮想マシン
- OSディスク
- 識別ディスク
- ネットワークインターフェイス
- ストレージアカウント

CitrixデータベースからVMとマシンカタログを削除し、タグを削除できます。以下を使用できます。

- マシンカタログから単一のVMまたはVMのリストからVMとタグを削除するには、`ForgetVM`パラメーターを指定した`Remove-ProvVM`を使用します。
- Citrixデータベースからマシンカタログを削除し、マシンカタログ全体からタグを削除するには、`ForgetVM`パラメーターを指定した`Remove-ProvScheme`を使用します。

この機能は、永続VMにのみ適用されます。

これを行うには：

1. **PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、**asnp citrix***を実行します。
3. CitrixデータベースからVMを削除し、VMからタグを削除するには、`Remove-ProvVM`を実行します。 例：

```
Remove-ProvVM -ProvisioningSchemeName “ProvisioningSchemeName” -VMName “vmname” -ForgetVM
```

4. Citrixデータベースからマシンカタログを削除し、マシンカタログからタグを削除するには、`Remove-ProvScheme`を実行します。例：

```
Remove-ProvScheme -ProvisioningSchemeName “ProvisioningSchemeName” -ForgetVM
```

> **注:**
>
> `Remove-ProvScheme`で`ForgetVM`パラメーターを使用すると、プロビジョニングスキームがBYORG（Bring Your Own Resource Group）またはCitrix管理リソースグループのいずれかに存在する場合、MCSはベースディスクスナップショットを含むすべてのスナップショットを削除します。

詳細情報

- 接続とリソースの作成および管理
- Microsoft Azureへの接続
- マシンカタログの作成
- Microsoft Azureカタログの作成

- マシンカタログの管理

Microsoft System Center Virtual Machine Manager カタログを管理する

マシンカタログの管理では、マシンカタログを管理するウィザードについて説明します。以下の情報は、Microsoft System Center Virtual Machine Manager (VMM) 仮想化環境に固有の詳細を扱っています。

> **注:**
>
> VMMカタログを管理する前に、VMMカタログの作成を完了する必要があります。Microsoft System Center Virtual Machine Managerカタログの作成を参照してください。

MCSによって作成されたリソースを識別する

以下は、MCS がリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
準備用 VM	タグ文字列は以下のとおりです: "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	カスタムプロパティエントリ: "XdConfig:"XdProvisioned=True"
カタログ内のVM	タグ文字列は以下のとおりです: "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	カスタムプロパティエントリ: "XdConfig:"XdProvisioned=True"

詳細情報

- 接続とリソースの作成および管理
- マイクロソフト システムセンター バーチャルマシンマネージャー への接続
- マシンカタログの作成
- Microsoft System Center Virtual Machine Manager カタログを作成する
- マシンカタログの管理

Nutanixカタログの管理

マシンカタログの管理では、マシンカタログを管理するウィザードについて説明します。以下の情報は、Nutanix AHV Prism Central環境に固有の詳細を扱っています。

> **注:**
>
> Nutanix AHV Prism Centralでマシンカタログを管理する前に、Nutanix AHV Prism Centralでマシンカタログの作成を完了する必要があります。Nutanixカタログの作成を参照してください。

Nutanix AHV Prism Centralでマシンカタログを管理するには、次の方法を使用できます。

- ウェブスタジオ
- PowerShell

Web Studio の使用

Web Studio を使用して Nutanix AHV Prism Central 上でマシンカタログを管理するためのオプションは次のとおりです。

オプション	説明
マシンの追加	マシンカタログにVMを作成して追加します。
マシンカタログの削除	マシンカタログを削除します。同時にVMを削除するか、永続VMをそのまま残すかを選択できます。
マスターイメージの変更	カタログ内のすべてのVMのテンプレートとして使用されるマスターイメージを変更します。
マシンプロファイルの追加または変更	マシンプロファイルのテンプレートバージョンを変更するか、既存のカタログにマシンプロファイルを追加します。
構成セットの管理	カタログをWorkspace Environment Management™構成セットにバインドするか、別の構成に切り替えます。

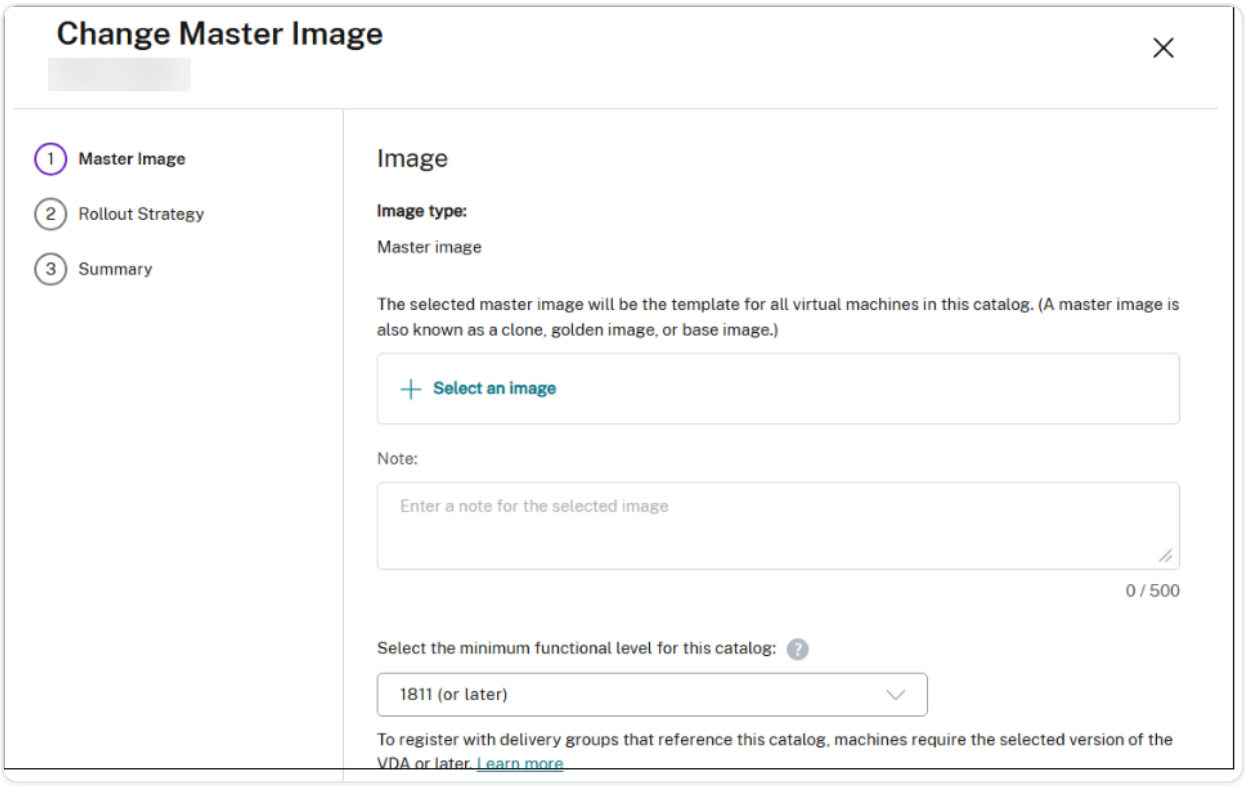
オプション	説明
マシンカタログの編集	NICや仮想マシンなど、カタログの構成を変更します。
マシンの表示	カタログに属するすべてのVMを表示するには、**検索**ノードに移動します。
マシンカタログの名前変更	カタログ名を変更します。
VDAのアップグレード	カタログごとにVDAをアップグレードします。この機能は、静的永続マシンにのみ適用されます。
機能レベルの変更	カタログの最小機能レベルを選択します。機能レベルを設定すると、すべての機能が利用可能になります。
マシンカタログのテスト	カタログにエラーまたは警告があるかどうかをテストします。
タグの管理	タグを作成、編集、削除します。カタログに適用するタグを選択します。
マシンカタログの移動	カタログを別のフォルダーに移動します。

> **注:**
>
> 現在、**クローン**オプションは利用できません。

マスターイメージの変更

カタログのマスターイメージを変更するには、次の手順に従います。

1. **マシンカタログ**ページで、更新するマシンカタログを右クリックし、**マスターイメージの変更**を選択します。
2. **マスターイメージの変更**ページで、**イメージの選択**をクリックします。



3. **イメージの選択**ページで、テンプレートを展開し、マスターイメージとして使用するテンプレートバージョンを選択します。マシンテンプレートは名前でフィルタリングできます。
4. 「**ロールアウト戦略**」ページで、更新を適用するタイミングを選択します。

> **注:**
>
> Nutanix AHV Prism Central ホスト接続プラグインを使用するMCSでプロビジョニングされた非永続カタログの場合、ブート構成をレガシーとUEFIの間で切り替えるためにマスターイメージを更新すると、既存のVMが次回の起動時に開始できなくなります。 マスターイメージを更新すると、OSディスクのみが更新されます。ハードウェアプロパティは変更されません。ハードウェアプロパティを更新するには、マシンプロファイルの追加または変更、NICの変更、およびVM構成の変更を参照してください。

マシンプロファイルの追加または変更

カタログのマシンプロファイルを追加または変更するには、次の手順に従います。

1. 「**マシンカタログ**」ページで、変更するマシンカタログを右クリックし、「**マシンカタログの編集**」を選択します。
2. 「**マシンプロファイル**」ページで、,

- マシンカタログにすでにマシンプロファイルがある場合は、鉛筆アイコンをクリックして別のマシンプロファイルテンプレートバージョンを選択します。テンプレート名でフィルタリングできます。マシンプロファイルの設定を確認します。
- マシンカタログにマシンプロファイルがない場合は、「マシンプロファイルを使用」を選択し、マシンプロファイルを選択します。マシンプロファイルの設定を確認します。

3. 「**仮想マシン**」ページには、選択したマシンプロファイルテンプレートバージョンに従って更新された構成が反映されている必要があります。

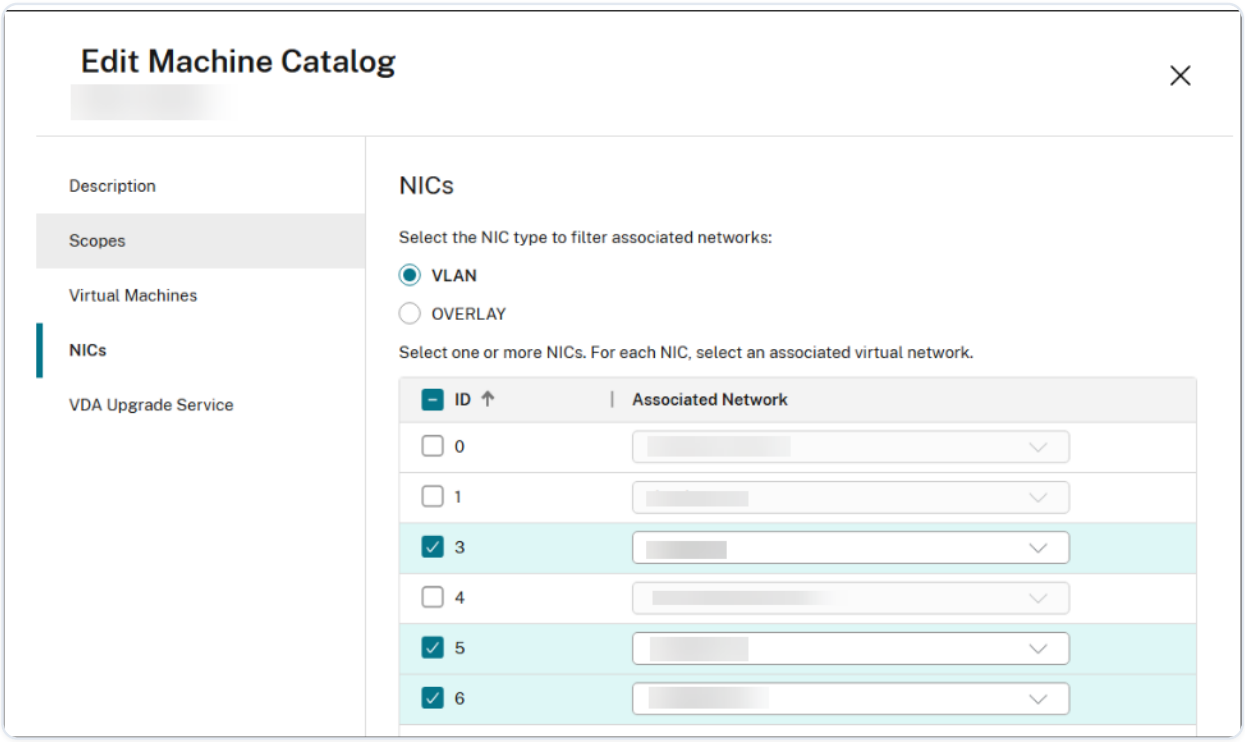
NICの変更

カタログのNICを変更するには、次の手順に従います。

1. 「**マシンカタログ**」ページで、変更するマシンカタログを右クリックし、「**マシンカタログの編集**」を選択します。
2. **NIC**ページで:

   a. NICの種類を選択します

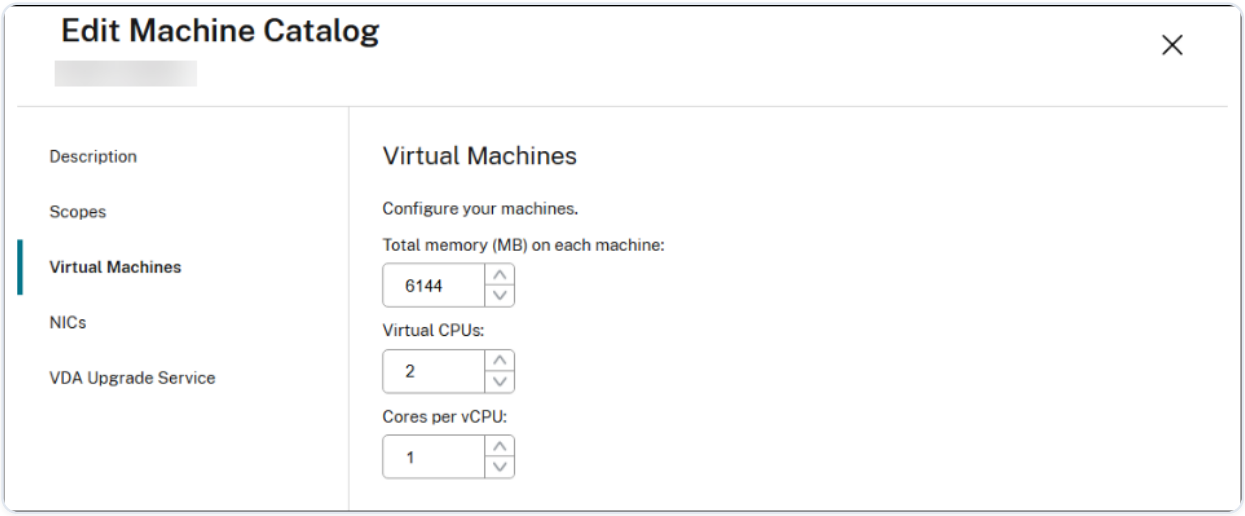
   b. ボックスをオンまたはオフにしてNICを選択し、各NICに関連付けられた仮想ネットワークを選択します。



VMの構成を変更する

メモリ、CPU数、vCPUあたりのコア数など、VMの構成を変更するには、次の手順に従います。

1. 「**マシンカタログ**」ページで、変更するマシンカタログを右クリックし、「**マシンカタログの編集**」を選択します。
2. **仮想マシン**ページで、上矢印または下矢印を使用するか、値を直接入力して、VMのメモリ、CPU数、vCPUあたりのコア数を調整します。



PowerShell を使用する

マスターイメージを変更する

必要なパラメーターは次のとおりです。

- `ProvisioningSchemeName`: 編集するプロビジョニングスキームの名前。
- `MasterImage`: 新しいマスターイメージへのリテラルパス。

次のコマンドを実行します。例:

```
Set-ProvSchemeMetadata  -Name "ImageManagementPrep_DoImagePreparation"
-ProvisioningSchemeName "<ProvisioningSchemeName>" -Value "True"



Publish-ProvMasterVMImage  -MasterImageVM "<Literal path to the new master
image- template version> -ProvisioningSchemeName
"<ProvisioningSchemeName>" -RunAsynchronously
```

> **注:**

> マスターイメージを更新すると、OSディスクのみが更新されます。ハードウェアプロパティは変更されません。ハードウェアプロパティを更新するには、「マシンプロファイルの追加または変更」、「NICの変更」、および「NICとVMの構成の変更」を参照してください。

マシンプロファイルの追加または変更

`Set-ProvScheme`コマンドを使用します。

- 新しいマシンプロファイルでカタログを更新する場合、または
- マシンプロファイルを持たない既存のカタログを、ハードウェア仕様のソースとしてマシンプロファイルを使用するように更新する場合。

> **注:**
>
> これにより、カタログ内の既存のVMのハードウェア仕様は更新されません。カタログに追加された新しいVMのみが、指定されたマシンプロファイルからのハードウェア仕様を持ちます。

> マシンプロファイルを変更するか、既存のカタログをマシンプロファイルを使用するように変換するには：

```
Set-ProvScheme -ProvisioningSchemeName <ProvScheme Name> `

               -MachineProfile "XDHyp:\HostingUnits\<Hosting Unit
Name>\Templates.folder\<Template Name>.template\<Template Version
Name>.templateversion"
```

マシンプロファイルには少なくとも1つのNICが必要であり、マシンプロファイル内のNICの数はNetworkMappingのサブネットマッピングと一致する必要があります。

テンプレートバージョンのNICの総数は、次の方法でそのインベントリアイテムの`AdditionalData`から取得できます。

```
$tv = Get-Item -Path "XDHyp:\HostingUnits\<Hosting Unit
Name>\Templates.folder\<Template Name>.template\<Template Version
Name>.templateversion"
```

```
$tv.AdditionalData.TotalNics
```

オーバーライドされたハードウェア仕様でマシンプロファイルを変更するには：

特定の構成は、特定のコマンドラインパラメーターを使用して構成できます。`CustomProperties`の`VMCpuCount`、`VMMemoryMB`、および`CPUCores`などのこれらのコマンドラインパラメーターは、マシンプロファイルテンプレートバージョンの値よりも優先されます。

```
$customProperties = @"

    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

        <StringProperty Name="ClusterId"
Value="00062c63-1fb0-58c9-4fc8-5c2573352378" />

        <StringProperty Name="CPUCores" Value="2" />

    </CustomProperties>

"@



Set-ProvScheme -ProvisioningSchemeName <ProvScheme Name> `

               -MachineProfile "XDHyp:\HostingUnits\<Hosting Unit
Name>\Templates.folder\<Template Name>.template\<Template Version
Name>.templateversion" `

               -CustomProperties $customProperties `

               -VMCpuCount 4 `

               -VMMemoryMB 4096
```

NICとVMの構成を変更する

必要なパラメーターは次のとおりです。

- `ProvisioningSchemeName`: 編集するプロビジョニングスキームの名前。

- `NetworkMapping`: 更新されたネットワークマッピング。

次のコマンドを実行します。例：

```
Set-ProvScheme  -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"><Property xsi:type=`"StringProperty`"
Name=`"ClusterId`" Value=`"000xxxx-1fb0-xxxxx-4fc8-5c257335xxxx`" /
><Property xsi:type=`"StringProperty`" Name=`"CPUCores`" Value=`"1`" /></
CustomProperties>"  -NetworkMapping @{"6"="XDHyp:\HostingUnits\<Hosting
Unit Name>\Clusters.folder\<Cluster Name>\<Network name>.network"}
-ProvisioningSchemeName "<ProvisioningSchemeName>" -VMCpuCount 4
```

永続VMのOSディスクをリセットする

永続VM、特にvTPMが有効になっているVMでOSディスクをリセットすると、vTPMキーとBitLockerに依存するアプリケーションが破損し、起動できなくなる可能性があります。そのため、この機能では次のことが可能です。

- 永続VMのOSディスクをリセットし、VMハードウェア構成を保持する。
- ディスクスワップ中にvTPMの依存関係が壊れるのを避けるために、vTPMが有効なVMを管理する。

`Reset-ProvVMDisk` PowerShellコマンドを使用して、永続VMのOSディスクをリセットできます。

- vTPMが有効なVMの場合：元のハードウェア情報を使用してリカバリポイントから新しいVMが作成され、vTPMキーが保持されます。
- vTPM以外のVMの場合：OSディスクが交換されます。

例については、「OSディスクのリセット」を参照してください。

マシンカタログをCitrix管理のNutanix AHV Prism Centralホスト接続に移行する

Citrixマシンカタログとそれに関連付けられたVMを、既存のNutanix AHV（Prism Element用）およびNutanix AHV PC（Azure上のNC2用）ホスト接続から、Citrix管理のNutanix AHV Prism Centralホスト接続に移行します。移行にはPowerShellコマンドを使用します。これには、問題が発生した場合の高速ロールバックオプションや、移行後にソースリソースをクリーンアップするコマンドも含まれます。

利点

- **中断の最小化**: Nutanix AHV Prism Centralプラグインへのスムーズな移行が可能です。これにより、既存の展開への影響を最小限に抑えられます。
- **シームレスなアップグレードパス**: インフラストラクチャをアップグレードし、新しい管理インターフェイスを活用するための明確でサポートされたパスを提供します。
- **データの整合性と安全性**: ロールバックオプションにより、予期せぬ問題が発生した場合でも環境を元の状態に戻すことができます。これにより、リスクが軽減されます。
- **リソース効率**: 移行が成功した後、ソースリソースをクリーンアップします。これにより、ストレージと管理のオーバーヘッドが最適化されます。
- **柔軟性**: MCSとサードパーティテクノロジーの両方によってプロビジョニングされたカタログの移行をサポートします。これにより、より幅広い適用性が提供されます。

適用性

この機能は、Nutanix AHV（Prism Element用）およびNutanix AHV PC（Azure上のNC2用）ホスト接続下のマシンカタログに適用されます。

- MCSによって管理されるマシンカタログ（永続タイプと非永続タイプの両方を含む）。
- サードパーティテクノロジーによってプロビジョニングされたVMを含む、電源管理のみのマシンカタログ。

システム要件

- **Nutanix AHV Prism Element (PE) AOSバージョン**: 最小バージョン6.8が必要です。
- **Nutanix Prism Central (PC)バージョン**: 最小バージョン2024.3が必要です。

> **注:**
>
> Nutanixの既知の問題により、Nutanix Prism Central 7.3にはAOS 7.3が必要です。

制限事項

- **PVSカタログはサポートされていません**：この機能は、**Citrix Provisioning Services** (PVS) Xendesktop Setup Wizard を使用して作成されたマシンカタログを**サポートしていません**。
- **ロールバックの制限**：
  - 移行されたカタログのロールバックは、最初の移行後にカタログを**変更していない**場合にのみ許可されます。

    - 「**Cleanup Source Resources**」操作を実行すると、移行状態がクリアされます。これにより、その後のロールバックが防止されます。

- **再移行はできません**：すでに移行したマシンカタログは、再移行がサポートされていません。
- **複数ホスト接続VM**：複数のホスト接続からインポートされたVMを含む、電源管理のみのマシンカタログの移行はサポートされていません。

重要な考慮事項

- **Nutanixクラスター管理**：ホスティングNutanix AHVクラスターは、Nutanix Prism Centralに登録されている必要があります。
- **マスターイメージテンプレートの作成**：MCSマシンカタログの場合、移行コマンドは、マシンカタログマスターイメージの元のスナップショットからPrism Central上にVMテンプレートバージョンを生成するオプションを提供します。このVMテンプレートバージョンは、後でPrism Centralホスト接続下のマシンカタログのMCSマスターイメージとして使用できます。デフォルトでは、このオプションは有効になっていません。
- **ロールバックの前提条件**：

  ロールバックを成功させるには、ホスト接続、ベースディスクを含む元のソース環境が変更されていない必要があります。また、移行が成功したと確認されるまで、移行されたマシンカタログへの構成変更やVMの追加/削除は避ける必要があります。 確認後、最終的なCleanup Source Resources操作を実行できますが、これは元に戻せない手順であり、ロールバックが不可能になることに注意してください。

移行とロールバックに必要な権限

カタログを移行またはロールバックするには、次の権限が必要です。

Prism Element管理者：

- 仮想マシンの作成

Prism Central管理者：

- VMテンプレートを作成
- VMテンプレートを削除
- VMリカバリポイントを削除
- 仮想マシンを削除

Citrix管理のNutanix AHV Prism Centralホスト接続に必要な特定の権限の完全なリストについては、「必要な権限」を参照してください。

移行方法

この機能は、専用のPowerShellコマンドレットを使用して管理します。一般的なワークフローには、移行、ロールバック、ソースリソースのクリーンアップという3つの主要な操作が含まれます。

マシンカタログを移行する

- この操作は、マシンカタログとその関連VMを、ソースのNutanix AHVまたはNutanix AHV PCホスト接続から、ターゲットのCitrix管理Nutanix AHV Prism Centralホスト接続に移動します。
- MCSプロビジョニングされたカタログの場合、このプロセスはターゲット接続に新しいベースディスクを作成します。
- オプションで、元のマスターイメージスナップショットから、ターゲット接続にマスターVM相当（VMテンプレートバージョン）を作成することを選択できます。

1. **新しいNutanix AHV Prism Centralホスト接続を作成する**: 移行する前に、ホスティングNutanix AHVクラスターをNutanix Prism Centralに登録し、ターゲットのNutanix Prism Centralインスタンスを指す新しいNutanix AHV Prism Centralホスト接続を確立します。この接続は、移行されたカタログの宛先として機能します。詳細については、「Nutanix AHV Prism Centralホスト接続」を参照してください。
2. **既存のマシンカタログを移行する**: 既存のマシンカタログの場合、`Switch-ProvCatalog` PowerShellコマンドレットを使用して、Citrix管理のNutanix AHV Prism Centralホスト接続への移行を開始します。

   ```
   c:\PS>Switch-ProvCatalog -BrokerCatalogUid <Catalog_UID>
   -DestinationHypervisorConnectionName "DestinationConnection"
   -DestinationHostingUnitName "DestinationUnit"
   -CreateMasterImageAtDestination
   ```

   - `<Catalog_UID>` を、移行するマシンカタログの一意の識別子に置き換えます。カタログ名 `Get-BrokerCatalog -Name <Catalog Name>` で `BrokerCatalogUid` を検索するには、次のPowerShellコマンドレットを使用します。
   - `DestinationConnection` は、手順1で作成された新しい**Nutanix AHV Prism Centralホスト接続**の名前です。
   - `DestinationUnit` は、マシンカタログが配置される `DestinationConnection` 内のホスティングユニットに与える名前です。
   - The `-CreateMasterImageAtDestination` パラメーターはオプションです。これは、ターゲットのPrism Central上にマスターイメージVMテンプレートバージョンを作成します。

3. **移行の完了を確認する**: 移行コマンドレットを実行した後、PowerShellウィンドウでタスクのステータスを監視し、正常に完了したことを確認します。移行が完了すると、カタログはステップ1で作成されたターゲットホスト接続に移動されます。タスクタイプSwitchProvCatalogで「完了」ステータスが表示されるはずです。移行の完了を確認するための推奨手順は次のとおりです。

    - Studioでカタログのステータスを確認します。
    - カタログ内のVMが、新しい宛先ハイパーバイザー接続に関連付けられていることを確認します。
    - カタログ内のVMが正しい電源状態を表示していることを確認します。
    - マシンを追加または削除したり、電源操作を実行したりして、移行されたマシンカタログの機能をテストし、カタログが正しく機能していることを確認します。

移行されたカタログをロールバックする

この操作により、マシンカタログとそのVMが元のソースホスト接続に復元されます。移行プロセス中に作成したリソースはすべて削除されます。

> **重要:**
>
> ロールバックは、移行後にカタログを変更しておらず、**ソースリソースのクリーンアップ**操作を実行していない場合にのみ実行します。元のソース接続は変更されず、引き続きベースディスクが含まれています。

```
c:\PS>Switch-ProvCatalog -BrokerCatalogUid <Catalog_UID> -Rollback
```

ソースリソースのクリーンアップ

移行が成功した後、この操作により、元のハイパーバイザー接続からソースリソース（ベースディスクなど）が削除されます。

> **重要:**
>
> このコマンドを実行すると、移行状態がクリアされます。これにより、その後のロールバックは不可能になります。

```
c:\PS>Switch-ProvCatalog -BrokerCatalogUid <Catalog_UID>
-CleanupSourceResources
```

続行する前に確認プロンプトが表示されます。この操作は元に戻せないためです。クリーンアップを完了するには、プロンプトを承認してください。

詳細情報

- 接続とリソースの作成および管理(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/connections.html)
- Nutanixへの接続(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/connections/connection-nutanix.html)
- Nutanixクラウドおよびパートナーソリューションへの接続(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/connections/connection-nutanix-cloud-and-partner-solutions.html)
- マシンカタログの作成(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/machine-catalogs-create.html)
- Nutanixカタログの作成(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/machine-catalogs-create/create-machine-catalog-nutanix.html)
- マシンカタログの管理(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/machine-catalogs-manage.html)

VMwareカタログの管理

マシンカタログの管理では、マシンカタログを管理するウィザードについて説明します。以下の情報は、VMware仮想化環境に固有の詳細を扱っています。

> **注:**
>
> VMwareカタログを管理する前に、VMwareカタログの作成を完了する必要があります。「VMwareカタログを作成する」を参照してください。

マシンカタログのフォルダーIDを更新する

MCSマシンカタログのフォルダーIDは、`Set-ProvScheme`コマンドのカスタムプロパティで`FolderId`を指定することで更新できます。フォルダーIDの更新後に作成されたVMは、この新し

いフォルダーIDの下に作成されます。このプロパティが`CustomProperties`で指定されていない場合、VMはマスターイメージが配置されているフォルダーの下に作成されます。

マシンカタログのフォルダーIDを更新するには、次の手順を実行します。

1. Webブラウザーを開き、**vSphere Web Client**のURLを入力します。
2. 資格情報を入力し、**ログイン**をクリックします。
3. **vSphere Web Client**でVM配置フォルダーを作成します。
4. PowerShellウィンドウを開きます。
5. **asnp citrix®***を実行して、Citrix固有のPowerShellモジュールをロードします。
6. `Set-ProvScheme`の`CustomProperties`で`FolderID`を指定します。この例では、フォルダーIDの値は`group-v2406`です。

   ```
   Set-ProvScheme -ProvisioningSchemeUid
   "50bb319c-2e83-4a37-9ea1-94f630687372" -CustomProperties
   "<CustomProperties xmlns=""http://schemas.citrix.com/2014/xd/
   machinecreation"" xmlns:xsi=""http://www.w3.org/2001/XMLSchema-
   instance""><Property xsi:type=""StringProperty"" Name=""FolderId""
   Value=""group-v2406"" /></CustomProperties>"
   ```

7. Studioを使用してマシンカタログにVMを追加します。
8. vSphere Web Clientで新しいVMを確認します。新しいVMは新しいフォルダーの下に作成されます。

vSphereでフォルダーIDを検索する

VMのフォルダーIDを見つけるには、任意のESXiまたはvCenterサーバーシステムでManaged Object Browser (MOB) にアクセスします。

MOBは、すべてのESX/ESXiおよびvCenterサーバーシステムに組み込まれているWebベースのサーバーアプリケーションです。このvSphereユーティリティを使用すると、VM、データストア、リソースプールなどのオブジェクトに関する詳細情報を表示できます。

1. Webブラウザーを開き、`http://x.x.x.x/mob`と入力します。ここで、x.x.x.xはvCenter ServerまたはESX/ESXiホストのIPアドレスです。例：`<https://10.60.4.70/mob>`。
2. MOBの**Home**ページで、プロパティ**content**の値をクリックします。
3. **rootFolder**の値をクリックします。
4. **childEntity**の値をクリックします。

5. **vmFolder**の値をクリックします。
6. フォルダーIDは**childEntity**の値にあります。

MCSによって作成されたリソースを識別する

以下は、MCS がリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
準備用 VM	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"XdConfig:"XdProvisioned=真"
カタログ内のVM	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"XdConfig:"XdProvisioned=真"

詳細情報

- 接続とリソースの作成および管理
- VMwareへの接続
- マシンカタログの作成
- VMwareカタログを作成する
- マシンカタログの管理

電源管理

Citrix Virtual Apps and Desktops™ を使用すると、さまざまなサポート対象のハイパーバイザーとクラウドサービスで、MCSプロビジョニングされたVMの電源管理を行うことができます。電源管理操作により、以下が提供されます。

- 最適なユーザーエクスペリエンス
- コスト管理と電力節約

利用可能な電源操作は次のとおりです。

- 起動
- シャットダウン

- 再起動
- 一時停止
- 再開
- 強制再起動
- 強制シャットダウン

> **注:**
>
> - 非永続VMの場合、電源サイクル（シャットダウン/起動および再起動）によりOSディスクがリセットされます。
> - 電源操作の機能と動作は、ハイパーバイザーまたはクラウドサービスによって異なります。

> この記事では、特定のサポート対象ハイパーバイザーに関連する主要な電源管理機能について説明します。

- AWS VMの電源管理
- Azure VMの電源管理

Amulet Hotkey CoreStation VM の電源管理 (プレビュー)

Citrix Virtual Apps and Desktops™ を使用すると、Amulet Hotkey CoreStation VM の電源管理を行うことができます。電源管理するマシンを見つけるには、ナビゲーションペインの **検索** ノードを使用します。

次の電源操作が利用可能です:

- 起動
- シャットダウン
- 強制シャットダウン
- 強制再起動
- 再起動

> **注：**

- リセット、一時停止、再開の電源操作はサポートされていません。
- シャットダウン/再起動: ノードにオペレーティングシステムをシャットダウンして電源を切るように要求します。これは、物理デスクトップマシンの電源ボタンを短く押すことと同じです。アクティブなユーザーがいる場合や、シャットダウンを中断するプログラムが実行されている場合、またはOSの更新プログラムをインストールする必要がある場合、ワークステーションはシャットダウン要求に応答しないことがあります。

AWS VM の電源管理

必要な権限については、必要なAWS権限を参照してください。

インスタンスの休止

休止プロセスは、インスタンスのインメモリ状態と、プライベート IP アドレスおよび Elastic IP アドレスを保存し、中断したところから正確に再開できるようにします。

インスタンスに休止が指示されると、インメモリ状態をルート EBS ボリューム内のファイルに書き込み、その後シャットダウンします。Amazon EBS ボリュームは、インスタンスにアタッチできる耐久性のあるブロックレベルストレージデバイスです。ボリュームをインスタンスにアタッチすると、物理ハードドライブと同じように使用できます。インスタンスのルート EBS ボリュームを暗号化します。暗号化により、メモリから EBS ボリュームにコピーされる機密データが適切に保護されます。EBS 暗号化の詳細については、「Amazon EBS 暗号化」を参照してください。

サポートされているインスタンス休止の制限事項は次のとおりです。

- 最大 150 GB までのインスタンスメモリ (RAM) のみがサポートされます
- UEFI ブートモードはサポートされていません
- 汎用 SSD とプロビジョンド IOPS SSD のみが EBS ボリュームタイプとしてサポートされます。

休止をサポートする VM の作成

休止をサポートする VM を作成するには：

1. ホスト接続を作成します。「AWS への接続」を参照してください。
2. EBSルートが暗号化され、**Stop-Hibernate**プロパティが有効になっているインスタンスを起動します。インスタンスの起動方法、ルートEBSボリュームの暗号化、および休止状態の有効化の詳細については、`<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/launching-instance.html/>`を参照してください。このインスタンスをマスターイメージとして使用してAMIを作成します。

3. マスターイメージを準備します。

   a. マスターイメージに VDA をインストールします。Citrix では、最新機能にアクセスできるように、最新バージョンをインストールすることをお勧めします。マスターイメージに VDA をインストールしないと、カタログ作成が失敗します。VDA のインストール方法の詳細については、「VDA のインストール」を参照してください。

   b. マスターイメージを、アプリケーションとデスクトップが属するドメインに参加させます。マスターイメージが、マシンが作成されるホストで利用可能であることを確認してください。

4. そのインスタンスから AMI を作成します。インスタンスから AMI を作成する方法については、「Amazon EC2 インスタンスから AMI を作成する」を参照してください。

5. `New-ProvScheme`コマンドを使用してマシンカタログを作成します。`AwsCaptureInstanceProperties`カスタムプロパティを**True**に設定します。Web StudioでAWSインスタンスプロパティを有効にする方法については、「**Web StudioでのAWSインスタンスプロパティの適用と運用リソースのタグ付け**」を参照してください。

   ```
   New-ProvScheme  -AdminAddress "xxx" -CleanOnBoot

   -CustomProperties "AwsCaptureInstanceProperties,true;"

   -HostingUnitName "xxx" -IdentityPoolName $catalog_name
   -InitialBatchSizeHint 1

   -MasterImageVM "xyz.template" -NetworkMapping @{"0"="XDHyp:
   \HostingUnits\MyConn\\us-east-2a.availabilityzone\10.0.0.0``/24
   (vpc-0f1771e45671aedcd).network"}

   -ProvisioningSchemeName $catalog_name

   -RunAsynchronously -Scope @() -SecurityGroup @("xxx") -ServiceOffering
   "xxx"
   ```

   PowerShell コマンドを使用してマシンカタログを作成する方法については、`<https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/>` を参照してください。

ハイバネート可能な VM は、次の場合に作成されます。

- **Stop-Hibernate** プロパティが有効になっているマスターイメージから作成された AMI を選択した場合。
- マスター VM がドメインに参加しており、VDA がインストールされている場合。
- 休止状態を処理できる正しいVMサイズ（サービス提供）を選択します。

次の場合、**New-ProvScheme**コマンドは適切なエラーメッセージを表示して失敗します。

- マスターVMは休止状態が有効になっていますが、サービス提供は休止状態を処理できません。
- マスターVMがドメインに参加しておらず、VDAがインストールされていない場合。

サービス提供とAMIの休止状態

サービス提供とAMI（テンプレート）の休止状態を取得するには、次のコマンドを実行します。

- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\WIN2016-ADDC-2021.09.10.145334-a1968709-10c4-47d5-9642-21e743159a7b(ami-0e6c5b33a52d2a6b6).template'`
- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\R6i Sixteen Extra Large Instance.serviceoffering'`

既存の休止状態対応プロビジョニングスキームのサービス提供を更新する

1. `Set-ProvScheme`コマンドを実行します。例：

```
Set-ProvScheme -ProvisioningSchemeName <String> -ServiceOffering
<String>
```

サービス提供に互換性がない場合、システムは例外メッセージを表示します。

休止状態をサポートするマシンカタログを作成する

マシンカタログを作成する際、休止状態をサポートするマシンプロファイルを使用できます。

1. カタログ作成ウィザードで、マシンプロファイルの選択まで指示に従います。
2. **マシンテンプレート**ページで、**マシンプロファイルの選択**をクリックし、マシンプロファイルを選択します。
3. 「**仮想マシン**」ページで、「**編集**」アイコンをクリックし、VMを選択します。

> **注:**

> マシンプロファイルで休止状態が有効になっている場合、システムは休止状態にできるVMのみを表示します。

4. 画面の指示に従ってすべての設定を完了します。「**概要**」ページにカタログの休止状態が表示されます。

> **注:**
>
> マシンカタログの編集で、マシンプロファイルを休止状態が有効なものに変更すると、それに応じてVMを再構成するように求められます。

休止状態をサポートするマシンカタログを更新する

既存のマシンカタログを休止状態をサポートしないマシンカタログで更新しようとすると、適切なエラーメッセージが表示されて更新が失敗します。

休止状態のVMの電源管理

休止状態のVMに対して、以下の電源管理操作を実行できます。

1. 実行中の状態からVMをサスペンドします。
2. 一時停止状態からVMを再開します。
3. 一時停止状態からVMを再起動します。

AzureローカルVMの電源管理

Citrix Virtual Apps and Desktops™ では、AzureローカルVMの電源管理が可能です。電源管理したいマシンを見つけるには、ナビゲーションペインの**検索**ノードを使用します。

次の電源操作が利用可能です:

- 起動
- シャットダウン
- 強制シャットダウン
- 再起動

> **注:**

> リセット、一時停止、再開の電源操作はサポートされていません。

Azure VM の電源管理

必要な権限については、「必要な Azure 権限」を参照してください。

Azure オンデマンドプロビジョニング

Azureオンデマンドプロビジョニングでは、VMはプロビジョニングが完了した後、Citrix Virtual Apps and Desktops™が電源オンアクションを開始したときにのみ作成されます。

MCS を使用して Azure Resource Manager でマシンカタログを作成する場合、Azure オンデマンドプロビジョニング機能は次のとおりです。

- ストレージコストを削減します
- カタログ作成を高速化します

MCS カタログを作成すると、Azure portal にリソースグループ内のネットワークセキュリティグループ、ネットワークインターフェイス、ベースイメージ、およびIDディスクが表示されます。

Azure portalには、Citrix Virtual Apps and Desktops™がVMの電源オンアクションを開始するまで、VMは表示されません。以下の違いを持つ2種類のマシンがあります。

- プールされたマシンの場合、オペレーティングシステムディスクとライトバックキャッシュはVMが存在する場合にのみ存在します。コンソールでプールされたマシンをシャットダウンすると、VMはAzureポータルに表示されません。定期的にマシンをシャットダウンする場合（たとえば、勤務時間外）、ストレージコストを大幅に節約できます。
- 専用マシンの場合、オペレーティングシステムディスクはVMが最初に電源オンされたときに作成されます。AzureポータルのVMは、マシンIDが削除されるまでストレージに残ります。コンソールで専用マシンをシャットダウンしても、VMはAzureポータルに表示されたままです。

> **注:**
>
> オンデマンドプロビジョニング機能の前に作成されたAzureカタログ（「レガシー」カタログ）のサポートは非推奨です。したがって、Azureレガシーカタログ VMを再作成してください。カタログはオンデマンドとしてプロビジョニングされ、ストレージコストを節約できます。

電源サイクル時にプロビジョニングされた仮想マシンを保持する

電源サイクル時にプロビジョニングされた仮想マシンを保持するかどうかを選択します。PowerShellパラメーター`New-ProvScheme CustomProperties`を使用します。このパラメーターは、電源サイクル時にプロビジョニングされた仮想マシンが保持されるかどうかを決定するために使用される追加のプロパティ`PersistVm`をサポートします。電源オフ時に仮想マシンを保持するには`PersistVm`プロパティを**true**に設定し、電源オフ時に仮想マシンが保持されないようにするにはプロパティを**false**に設定します。

> **注:**
>
> `PersistVm`プロパティは、`CleanOnBoot`および`UseWriteBackCache`プロパティが有効になっているプロビジョニングスキームにのみ適用されます。非永続仮想マシンに対して`PersistVm`プロパティが指定されていない場合、それらは電源オフ時にAzure環境から削除されます。

「次の例では、`New-ProvScheme CustomProperties`パラメーターは`PersistVm`プロパティを **true** に設定します。」:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

<Property xsi:type="StringProperty" Name="PersistVm" Value="true" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="demo-
resourcegroup" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />
```

```
</CustomProperties>
```

「次の例では、`New-ProvScheme CustomProperties` パラメーターは、`PersistVM` を **true** に設定することでライトバックキャッシュを保持します。」:

```
 New-ProvScheme

 -AzureAdJoinType "None"

 -CleanOnBoot

 -CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageType`" Value=`"Standard_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"false`" /
><Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`"
Value=`"true`" /><Property xsi:type=`"StringProperty`" Name=`"PersistVm`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"ResourceGroups`" Value=`"demo-resourcegroup`" /><Property
xsi:type=`"StringProperty`" Name=`"LicenseType`"
Value=`"Windows_Client`" /></CustomProperties>"

 -HostingUnitName "demo"

 -IdentityPoolName "NonPersistent-MCSIO-PersistVM"

 -MasterImageVM "XDHyp:\HostingUnits\demo\image.folder\scale-
test.resourcegroup\demo-snapshot.snapshot"

 -NetworkMapping @ {"0"="XDHyp:\HostingUnits\demo\
\virtualprivatecloud.folder\East US.region\virtualprivatecloud.folder\ji-
test.resourcegroup\jitest-vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName "NonPersistent-MCSIO-PersistVM"

 -ServiceOffering "XDHyp:
\HostingUnits\demo\serviceoffering.folder\Standard_B2ms.serviceoffering"
-UseWriteBackCache

 -WriteBackCacheDiskSize 127
```

```
-WriteBackCacheMemorySize 256
```

ヒント:

`PersistVm`プロパティは、プロビジョニングされた仮想マシンを保持するかどうかを決定します。`PersistOsdisk`プロパティは、OSディスクを永続化するかどうかを決定します。プロビジョニングされた仮想マシンを保持するには、まずOSディスクを保持します。仮想マシンを削除せずにOSディスクを削除しないでください。`PersistVm`パラメーターを指定せずに`PersistOsdisk`プロパティを使用できます。

ストレージタイプの変更失敗時の電源オン動作をカスタマイズする

電源オン時に、Azureでの障害により、管理ディスクのストレージタイプが目的のタイプに変更できない場合があります。このようなシナリオでは、VMはオフのままで、障害メッセージが送信されます。ただし、ストレージが構成されたタイプに復元できない場合でもVMの電源をオンにするか、VMをオフのままにするかを選択できます。

- カスタムプロパティ`FailSafeStorageType`を **true** (デフォルト設定) に構成した場合、または`New-ProvScheme`または`Set-ProvScheme`コマンドで指定しない場合:
  - 電源オン時に、VMは誤ったストレージタイプで電源オンされます。
  - シャットダウン時、VMは誤ったストレージタイプでオフのままになります。
- `New-ProvScheme`または`Set-ProvScheme`コマンドでカスタムプロパティ`FailSafeStorageType`を **false** に構成した場合:
  - 電源オン時に、VMは誤ったストレージタイプでオフのままになります。
  - シャットダウン時、VMは誤ったストレージタイプでオフのままになります。

マシンカタログを作成するには：

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix®*`を実行します。
3. まだ作成されていない場合は、IDプールを作成します。
4. `New-ProvScheme`でカスタムプロパティを追加します。例：

```
New-ProvScheme -HostingUnitName "Azure-Resources-1" -IdentityPoolName
"name" -InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\Azure-
Resources-1\image.folder\abc.resourcegroup\def.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\Azure-
Resources-1\ght.folder\abc.resourcegroup\abc-
vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName "name"

-ServiceOffering "XDHyp:\HostingUnits\Azure-
Resources-1\serviceoffering.folder\Standard_DS2_v2.serviceoffering"

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">

<Property xsi:type=`"StringProperty`" Name=`"StorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageTypeAtShutdown`"
Value=`"Standard_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
Value=`"true`" />

</CustomProperties>"
```

5. マシンカタログを作成します。Remote PowerShell SDKを使用してカタログを作成する方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`を参照してください。

既存のマシンカタログを更新して、`FailSafeStorageType`カスタムプロパティを含めます。この更新は既存のVMには影響しません。

1. `Set-ProvScheme`コマンドでカスタムプロパティを更新します。例：

```
Set-ProvScheme -ProvisioningSchemeName <String> -CustomProperties "

<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
```

```
machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"StorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"IdentityDiskStorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
Value=`"false`" />

</CustomProperties>"
```

Set-ProvSchemeで行われた変更を既存のVMに適用するには、`-StartsNow`および`-DurationInMinutes -1`パラメーターを指定して`Set-ProvVMUpdateTimeWindow`コマンドを実行します。

1. `-StartsNow`と`-DurationInMinutes -1`のパラメータを指定して`Set-ProvVMUpdateTimeWindow`コマンドを実行します。例:

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
   <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
   ```

2. VMを再起動します。

休止状態対応VMを作成する

Azure環境では、休止状態をサポートするMCSマシンカタログを作成できます。この機能を使用すると、VMを中断し、ユーザーが再度サインインしたときにVMの以前の状態に再接続できます。

休止状態機能は以下に適用されます。

- シングルセッションOS
- 永続VMと非永続VM
- 静的およびランダム (プールされた) VDI デスクトップ

VDI デスクトップが静的かランダムかに関わらず、VM を休止状態にした後、同じセッションに再開できます。

このセクションでは、以下を参照してください。

- 前提条件

- 制限事項
- 休止状態対応のマシンカタログを作成および管理する
- 既存の休止状態対応 VM 用のマシンカタログを作成する
- 休止状態プロパティを確認する
- VM の電源管理 (手動および自動)

休止状態を使用するための前提条件

休止状態を使用するには、以下のタスクを完了していることを確認してください。

- Windows と Linux の両方のマスターイメージに Azure VM Agent をインストールします。Windows イメージのページファイルは一時ディスクに配置できます。マシンカタログで休止状態が有効になっている場合、MCS はページファイルの場所をベースディスクの C: ドライブに設定します。
- MCS は、生成されたリソースの休止状態プロパティを自動的に設定します。休止状態をサポートするために、マスターリソースのプロパティを構成する必要はありません。
- 休止状態をサポートするサブスクリプション内の VM サイズを使用してください。
- VM が休止状態機能を継承できるように、休止状態対応のマシンプロファイル (VM またはテンプレート仕様) を作成します。VM の作成については、休止状態の概要 を参照してください。

  > **注:**
  >
  > Microsoftによると、OSディスクから休止状態が有効なVMを展開できます。この機能は現在一部のリージョンでサポートされており、まもなくすべてのリージョンで利用可能になります。詳細については、「OSディスクから休止状態が有効なVMを展開する」を参照してください。
  >
  > テンプレート仕様を作成するには、次の手順を実行します。

  a. Azure Portalを開きます。テンプレートで使用する構成を持つVMを選択します。左ペインで**テンプレートのエクスポート**を選択します。
  b. **パラメーターを含める**チェックボックスをオフにします。コンテキストをコピーし、JSONファイルとして保存します（例: `VMExportTemplate.json`）。
  c. パラメーター`hibernationEnabled`がテンプレート上で`true`であることを確認します。パラメーターが`true`でない場合は、使用したVM構成を確認してください。テンプレート

ファイルでサポートされているVMサイズを指定できます。ただし、カタログ作成時にマシンサイズを指定することもできます。

d. ネットワークインターフェースリソースのテンプレートをJSONファイル `VMExportTemplate.json` に追加します。これにより、2つのリソースを持つARMテンプレートファイルが作成されます。

e. このテンプレートファイルをARMテンプレート仕様としてインポートするには、**Azure Portal > テンプレート仕様 > テンプレートのインポート > ローカルテンプレートファイルの選択**を選択します。

f. ARMテンプレート仕様が作成されたら、それをマシンプロファイルとして使用できます。

> **注:**
>
> Citrix Studioに同期されるまで数分かかる場合があります。

詳細については、Microsoftドキュメント休止状態を使用するための前提条件を参照してください。

制限事項

- シングルセッションOSマシンカタログ（永続的および非永続的）のみがサポートされています。
- エフェメラルOSディスクおよびMCS I/O機能は、Azureの休止状態をサポートしていません。
- 自動Windowsアップデート中に休止状態が失敗する可能性があります。

詳細については、Microsoftドキュメントを参照してください。

休止状態対応のマシンカタログを作成および管理する

休止状態対応のVMを作成するには、以下を使用して休止状態対応のマシンカタログを作成および管理できます。

- Web Studio、または
- PowerShellコマンド

WEB STUDIOを使用してカタログを作成する

1. **マシンカタログの作成**を選択します。カタログ作成ウィザードが開きます。
2. **マシンタイプ**ページで、このカタログの**シングルセッションOS**マシンタイプを選択します。
3. **マシン管理**ページで、次のように設定を選択します。

a. 「**電源管理されているマシン（仮想マシンやブレードPCなど）**」を選択します。

b. 「**Citrix Machine Creation Services™ (MCS)**」を選択します。

4. **デスクトップエクスペリエンス**ページで、必要に応じてランダムまたは静的デスクトップエクスペリエンスを選択します。
5. **イメージ**ページで、マスターイメージを選択します。「**マシンプロファイルを使用する**」チェックボックスをオンにし、ハイバネーションをサポートするマシンプロファイルを選択します。ツールヒントをクリックして、マシンプロファイルがハイバネーションをサポートしているかどうかを確認します。

> **注:**
>
> Azureマネージドマスターイメージを選択すると、ブレードにはリソースと同じリージョンに属するすべてのイメージが一覧表示されます。

6. **ストレージとライセンスの種類**ページで、このカタログに使用するストレージとライセンスを選択します。
7. **仮想マシン**ページで、VMの数、VMサイズ、およびアベイラビリティゾーンを選択します。

> **注:**
>
> ハイバネーションをサポートするマシンサイズのみが選択肢として表示されます。

8. **NIC**ページで、VMが使用するNICを追加します。
9. **ディスク設定**ページで、ライトバックキャッシュディスクのストレージの種類とサイズを選択します。
10. **リソースグループ**ページで、VMをプロビジョニングするリソースグループを選択します。
11. **マシンID**ページで、「**新しいActive Directoryアカウントを作成する**」を選択します。次に、アカウント命名スキームを指定します。
12. **ドメイン資格情報**ページで、「**資格情報を入力**」をクリックします。ターゲットのActive Directoryドメインでアカウント作成を実行するために、ドメイン資格情報を入力します。
13. 「**概要**」ページで、マシンカタログの名前を入力し、「**完了**」をクリックします。

MCSマシンカタログの作成が完了したら、カタログリストでそのカタログを見つけ、「**テンプレートプロパティ**」タブをクリックします。パラメーター「**休止状態**」の値は「**サポート対象**」である必要があります。

マシンカタログを編集する場合は、以下の制限事項を考慮してください。

- 現在のマシンカタログが休止状態をサポートしている場合、次のことはできません。
  - VMサイズを休止状態に対応していないものに変更する。
  - マシンプロファイルを休止状態に対応していないものに変更する。
- 現在のマシンカタログが休止状態をサポートしていない場合、次のことはできません。
  - 現在、Web Studioを使用してマシンプロファイルを休止状態対応のものに変更します。

既存の休止状態対応VMを管理するためのマシンカタログを作成する

既に休止状態対応VMがあり、それらを一時停止および再開したい場合は、それらのVMを電源管理のためにインポートするマシンカタログを作成します。

> **注:**
>
> 休止状態に対応しているVMと対応していないVMの両方を含むマシンカタログを作成できます。ただし、休止状態に関連する機能が必要な場合は、休止状態に対応しているVMのみを含むマシンカタログを作成する必要があります。

> Web Studioを使用して既存の休止状態対応VMのカタログを作成するには、画面の指示に従って手順を完了し、以下の主要な設定に注意してください。

1. 「**マシン管理**」ページで、「**電源管理されているマシン**」を選択し、マシンの展開方法として「**その他のサービスまたはテクノロジー**」を選択します。
2. 「**仮想マシン**」ページで、休止状態に対応しているVMのみを追加またはインポートします。

POWERSHELLコマンドを使用してマシンカタログを作成する

休止状態を使用するためのすべての要件を満たした後、`New-ProvScheme`コマンドを使用して休止状態対応のマシンカタログを作成できます。Remote PowerShell SDKを使用してカタログを作成する方法については、New-ProvSchemeを参照してください。

カタログの作成中に、以下のPowerShellコマンドを使用して、VMサイズとマシンプロファイルが休止状態をサポートしているかどうかを確認できます。

- VMサイズの場合、次のコマンドを実行し、プロパティ`supportsHibernation`が**True**であるかどうかを確認します。例：

```
Get-ChildItem -AdminAddress "MyDDC.MyDomain.local" -LiteralPath
@("XDHyp:\HostingUnits\ <VirtualNetwork> \serviceoffering.folder") |
select Name, AdditionalData | ConvertTo-Json
```

- マシンプロファイルの場合、次のコマンドを実行し、プロパティ`supportsHibernation`が**True**であるかどうかを確認します。例：

```
Get-ChildItem -AdminAddress "MyDDC.MyDomain.local" -LiteralPath
@("XDHyp:\HostingUnits\ <VirtualNetwork>
\machineprofile.folder\abc.resourcegroup")|select Name, AdditionalData|
ConvertTo-Json
```

マシンカタログを編集する場合は、次の制限事項を考慮してください。

- 現在のマシンカタログが休止状態をサポートしている場合、次のことはできません。
  - VMサイズを休止状態非対応のものに変更する
  - マシンプロファイルを休止状態非対応のものに変更する
- 現在のマシンカタログが休止状態をサポートしていない場合、次のことはできません。
  - 現在、Web Studioを使用してマシンプロファイルを休止状態対応のものに変更します。

Remote PowerShell SDKを使用してカタログのVMサイズとマシンプロファイルを変更する方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Set-ProvScheme/>`を参照してください。

休止状態プロパティの確認

PowerShellコマンドを使用して、マシンカタログ、VM、およびブローカーマシンの休止状態プロパティを確認できます。

- プロビジョニングスキームの休止状態プロパティを確認するには、次のPowerShellコマンドを実行します。`HibernationEnabled`パラメーターは`True`である必要があります。

```
(Get-ProvScheme -provisioningSchemeName <YourSchemeName>).VMMetadata
-join "" |  ConvertFrom-Json | Select HibernationEnabled
```

- プロビジョニングVMの休止状態プロパティを確認するには、次のPowerShellコマンドを実行します。`SupportsHibernation`パラメーターは`True`である必要があります。

```
(Get-ProvVM -VMName <YourVMName>).CustomVmData | ConvertFrom-Json |
Select SupportsHibernation
```

- ブローカーマシンの休止状態容量を確認するには、次のPowerShellコマンドを実行します。**Suspend** および **Resume** の電源アクションは、休止状態機能を示します。

```
(Get-BrokerMachine -MachineName
<YourMachineName>).SupportedPowerActions
```

休止状態対応VMの電源管理

休止状態対応VMに対して、以下の電源管理操作を実行できます。

- 実行状態からVMを**一時停止**する
- 一時停止状態からVMを**再開**する
- 一時停止状態からVMを**強制シャットダウン**する
- 一時停止状態からVMを**強制再起動**する

詳細については、以下を参照してください。

- 一時停止
- 再開

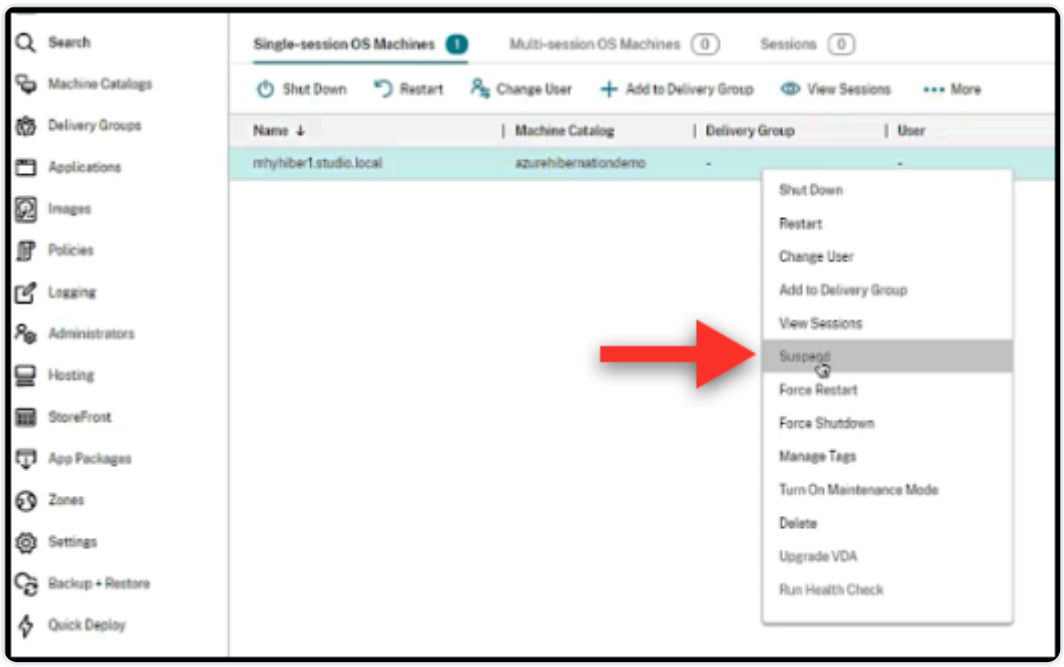
一時停止

VMを一時停止するには、以下のいずれかの方法を使用できます。

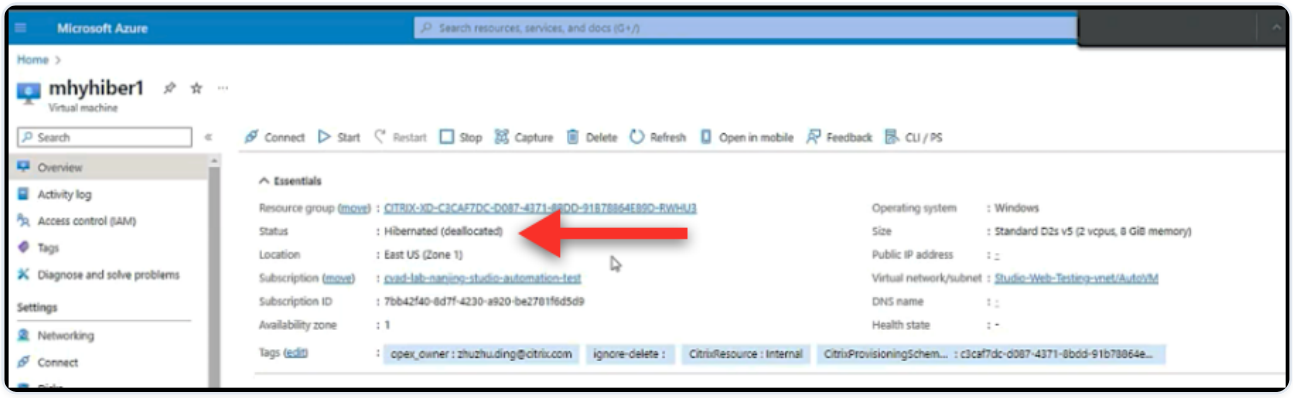
- Web Studioを使用して**手動で**
- タイムアウトポリシーを使用して**自動的に**: 詳細については、その他の設定を参照してください。

VMを手動で一時停止するには：

1. VMを右クリックし、**一時停止**を選択します。アクションを確定するには、**はい**をクリックします。**電源状態**が**一時停止中**から**一時停止済み**に変わります。



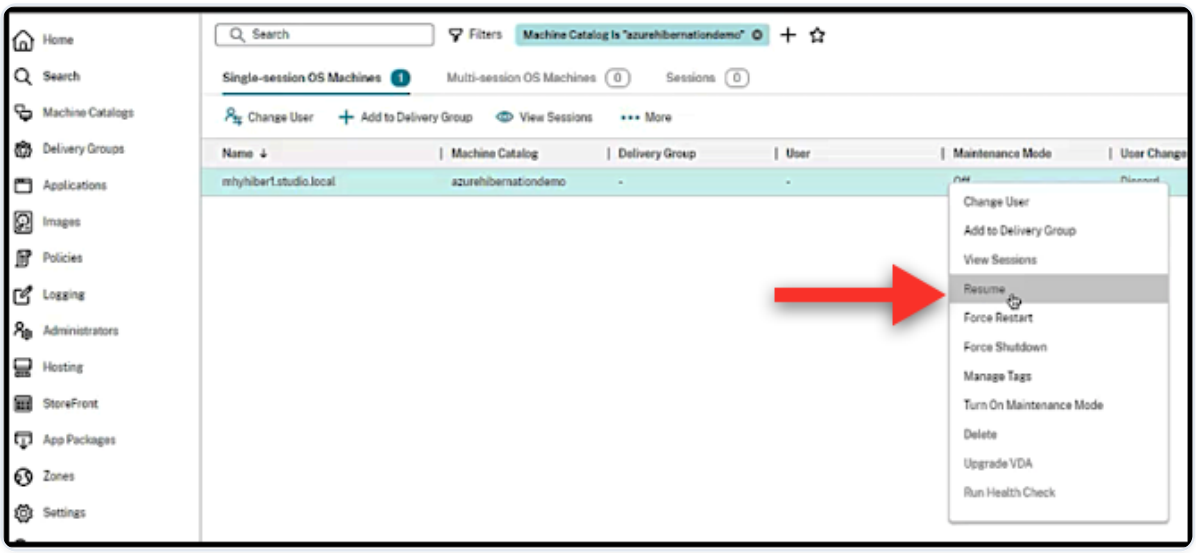
AzureポータルでVMのステータスを確認できます。



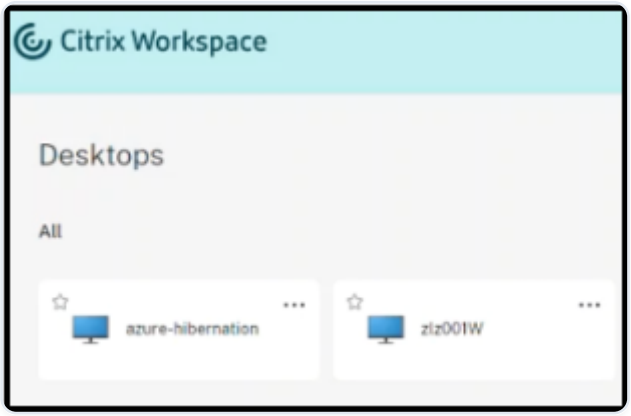
再開

休止状態のVMを再開するには、次のいずれかの方法を使用します。

- **手動で：**
  - 管理者はWeb Studioを使用してVMを再開できます。



- エンドユーザーは、デスクトップアイコンをクリックすると、Citrix Workspace™メニューを使用してVMを起動できます。



- **自動的に：**
  - Autoscale™は、ピーク時間を正しく構成した場合、休止状態のマシンを自動的に電源オンにできます。タイムスケジュールをクリックすることで、ピーク時間を30分間隔で設定できます。各青いフレームは、ピーク時間としてマークされたタイムスロットを表します。ピーク時間には、連続したタイムスロットと非連続のタイムスロットを設定できます。
    - 連続したタイムスロット

      「連続したピーク時間帯」(/en-us/citrix-virtual-apps-desktops/current-release/media/consecutive-peak-time-autoscale.png)
    - 連続しない時間帯

      「連続しないピーク時間帯」(/en-us/citrix-virtual-apps-desktops/current-release/media/non-consecutive-peak-time-autoscale.png)

> **注:**
>
> **Manage Autoscale > Load-based Settings**で、**Action**が**Suspend**に構成されている場合、そのデリバリーグループ内のすべてのVMが休止状態機能を持っていることを確認してください。そうでない場合、休止状態にできないVMは実行され続けます。

> 「オートスケール負荷ベース設定の管理」(/en-us/citrix-virtual-apps-desktops/current-release/media/azure-hibernation-autoscale.png)

休止状態の失敗に関する警告メッセージを取得する

MCSプロビジョニング済みおよび既存の休止状態対応VMの休止状態の失敗の場合に、PowerShellコマンド`Get-ProvOperationEvent`を使用して警告メッセージを取得できます。PowerShellコマンドの詳細については、SDKドキュメントGet-ProvOperationEventを参照してください。

これを行うには：

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. 休止状態の失敗の場合に警告メッセージを取得するために`Get-ProvOperationEvent`を実行します。

   ```
   Get-ProvOperationEvent -filter { OperationName -eq "Suspend" }
   ```

   出力：

   ```
   EventAdditionalData : Error code = OperationNotAllowed and Error
   message = The Hibernate-Deallocate Operation cannot be performed on a
   VM that has extension 'AzureHibernateExtension' in failed state. For
   more information, see https://aka.ms/hibernate-resume/errors. Error
   details from the extension : Enabling

                    hibernate failed. Response from the powercfg command.
   Exit Code: 1. Error message:

                    Hibernation failed with the following error: The
   request is not supported.
   ```

```
                  The following items are preventing hibernation on
this system.

                    The current Device Guard configuration has disabled
hibernation.

                    An internal system component has disabled
hibernation.

                            Hypervisor

                  Status: 409

                  ErrorCode: OperationNotAllowed



                  Content:

                  {

                    "error": {

                      "code": "OperationNotAllowed",

                      "message": "The Hibernate-Deallocate Operation
cannot be performed on a VM that has extension
'AzureHibernateExtension' in failed state. For more information, see
https://aka.ms/hibernate-resume/errors. Error details from the
extension : Enabling hibernate failed. Response from the

                  powercfg command. Exit Code: 1. Error message:
\nHibernation failed with the following error: The request is not
supported.\r\r\n\r\nThe following items are preventing hibernation on
this system.\r\n\tThe current Device Guard configuration has disabled
hibernation.\r\n\tAn internal system

                  component has disabled hibernation.
\r\n\t\tHypervisor"

                    }

                  }
```

```
EventCategory       : Warning

EventDateTime       : 1/11/2024 4:18:31 AM

EventId             : 0

EventMessage        : Failed to suspend machine my-resource-group/my-
vm.

EventSeverity       : Important

EventSource         : AzureRmPlugin

EventState          : New

LinkedObjectType    : ProvisioningScheme

LinkedObjectUid     : 589cb600-6e65-479f-9d47-9715c4732366

OperationName       : Suspend

OperationTargetName : my-resource-group/my-vm

OperationTargetType : VirtualMachine

OperationType       : PowerManagement

Recommendation      :
```

休止状態の問題のトラブルシューティング

休止状態と信頼できる起動VM機能の両方を有効にしようとしたときに、ゲストOSの構成が正しくない場合、次のエラーメッセージが表示されます。

エラーコード	エラーメッセージ
OperationNotAllowed	拡張機能「AzureHibernateExtension」が失敗状態のVMでは、休止状態解除操作を実行できません。詳細については、`<https://aka.ms/hibernate-resume/errors/>`を参照してください。拡張機能からのエラー詳細: 休止状態の有効化に失敗しました。powercfgコマンドからの応答。終了コード: 1。エラー

エラーコード	エラーメッセージ
	メッセージ: 次のエラーにより休止状態に失敗しました: 要求はサポートされていません。以下の項目がこのシステムでの休止状態を妨げています。**現在のDevice Guard構成により休止状態が無効になっています。内部システムコンポーネントにより休止状態が無効になっています。**

この問題を解決するには、ゲストVM内で仮想化が有効になっていることを確認してください。たとえば、Windows環境でHyper-Vが有効になっていることを確認します。Microsoft Windowsの制限によると、休止状態は、VMで信頼できる起動が有効になっている場合にのみ、ネストされた仮想化でサポートされます。

警告メッセージの詳細については、Microsoftドキュメント Troubleshooting VM hibernationを参照してください。

> **注:**
>
> VMの再開の失敗に関連するエラーメッセージは、今後のリリースで提供される予定です。

詳細情報

Citrix Azureの休止状態の詳細については、Citrix Tech Zoneの記事を参照してください。

Oracle C3 VM の電源管理 (プレビュー)

Citrix Virtual Apps and Desktops™ を使用すると、Oracle C3 VM の電源管理を行うことができます。ナビゲーションペインの**検索**ノードを使用して、電源管理するマシンを見つけます。

次の電源操作が利用可能です:

- 起動
- シャットダウン
- 強制シャットダウン
- 再起動
- リセット

> **注:**
>
> サスペンドおよび再開の電源操作はサポートされていません。

Red Hat OpenShift VMの電源管理

Citrix Virtual Apps and Desktops™ を使用すると、Red Hat OpenShift VMの電源管理を行うことができます。ナビゲーションペインの検索ノードを使用して、電源管理したいマシンを見つけてください。

次の電源操作が利用可能です:

- 起動
- シャットダウン
- 強制シャットダウン
- 再起動

> **注:**
>
> リセット、一時停止、再開の電源操作はサポートされていません。

Nutanix AHV VM の電源管理

Citrix DaaS™ を使用すると、Nutanix AHV VM の電源を管理できます。ナビゲーションペインの**検索**ノードを使用して、電源管理したいマシンを見つけます。

次の電源アクションを使用できます。

- 起動
- シャットダウン
- 強制シャットダウン
- 強制再起動
- 再起動

> **注:**

- リセット、一時停止、再開の電源操作はサポートされていません。
- シャットダウンまたは再起動: アクティブなユーザーや実行中のプログラムがシャットダウンを中断したり、OSが更新を必要とする場合、VMはシャットダウン要求に応答しない場合があります。Windows VM でゲストのシャットダウンと再起動が適切に機能するようにするには、スクリーンセーバーやディスプレイの電源設定など、VDA で推奨される電源アクション設定を適用します。詳細については、Nutanix KBを参照してください。

セキュリティポリシー

この記事では、さまざまなサポート対象クラウドサービスにおけるセキュリティ機能について説明します。セキュリティ機能には、次のものが含まれます。

- セキュリティグループ(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/security-policies/security-group.html)
- セキュアブート(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/security-policies/secure-boot.html)
- 暗号化機能(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/security-policies/encryption-capabilities.html)

セキュリティグループ

セキュリティグループは、仮想ネットワーク内のリソース間のネットワークトラフィックをフィルタリングするためのセキュリティルールのグループです。セキュリティルールは、いくつかの種類のリソースに対するインバウンドネットワークトラフィックまたはアウトバウンドネットワークトラフィックを許可または拒否します。各ルールは次のプロパティを指定します。

- 名前: ネットワークセキュリティグループ内の一意の名前
- 優先度: ルールは優先度順に処理され、数値が小さいほど優先度が高いため、数値が小さいものから先に処理されます
- 送信元または宛先: 任意、または個別のIPアドレス、クラスレスドメイン間ルーティング (CIDR) ブロック (例: 10.0.0.0/24)、サービスタグ、またはアプリケーションセキュリティグループ
- プロトコル: 各セキュリティグループのルールを追加する際のベースとなるプロトコル
- 方向: ルールがインバウンドトラフィックまたはアウトバウンドトラフィックに適用されるかどうか

- ポート範囲: 個別のポートまたはポート範囲を指定できます
- アクション: 許可または拒否

サポートされているハイパーバイザーの詳細については、以下を参照してください。

- AWS のセキュリティグループ
- Microsoft Azure のセキュリティグループ
- Google Cloud Platform のセキュリティグループ

AWS のセキュリティグループ

セキュリティグループは、VPC 内のインスタンスのトラフィックを制御する仮想ファイアウォールとして機能します。パブリックサブネット内のインスタンスがプライベートサブネット内のインスタンスと通信できるようにするルールをセキュリティグループに追加します。これらのセキュリティグループをVPC内の各インスタンスに関連付けることもできます。インバウンドルールはインスタンスへの受信トラフィックを制御し、アウトバウンドルールはインスタンスからの送信トラフィックを制御します。

イメージ準備中のネットワーク設定の詳細については、イメージ準備中のネットワーク設定を参照してください。

インスタンスを起動するときに、1つ以上のセキュリティグループを指定できます。セキュリティグループを構成するには、「セキュリティグループの構成」(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/install-prepare/aws.html#task-2-configure-security-groups)を参照してください。

Microsoft Azure のセキュリティグループ

Citrix Virtual Apps and Desktops は、Azure のネットワークセキュリティグループをサポートしています。ネットワークセキュリティグループは、サブネットに関連付けられることが想定されています。詳細については、ネットワークセキュリティグループを参照してください。

イメージの準備中に作成されるネットワークセキュリティグループの詳細については、「Azure Resource Manager イメージを使用してマシンカタログを作成する」(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/machine-catalogs-create/create-machine-catalog-citrix-azure.html#create-a-machine-catalog-using-an-azure-resource-manager-image-in-web-studio)を参照してください。

Google Cloud Platform のセキュリティグループ

マシンカタログの準備中に、カタログのマスターイメージシステムディスクとして機能するマシンイメージが準備されます。このプロセスが発生すると、ディスクは一時的に仮想マシンに接続され

ます。この VM は、すべてのインバウンドおよびアウトバウンドネットワークトラフィックを防止する分離された環境で実行する必要があります。これは、すべてのトラフィックを拒否するファイアウォールルールによって実現されます。詳細については、「ファイアウォールルール」(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/machine-catalogs-create/create-machine-catalog-gcp.html#firewall-rules)を参照してください。

セキュアブートとvTPM

セキュアブートは、システムの起動を担当するUnified Extensible Firmware Interface (UEFI) の機能です。これにより、起動プロセス中に信頼できるソフトウェアのみがロードされることが保証されます。

トラステッドプラットフォームモジュール (TPM) は、暗号化キーやその他の機密データを安全に保存するためのハードウェアチップです。仮想トラステッドプラットフォームモジュール (vTPM) は、TPM と同じ機能を実行しますが、暗号化コプロセッサ機能をソフトウェアで実行します。TPM はセキュリティを強化できますが、セキュアブートの要件ではありません。

サポートされているハイパーバイザーの詳細については、以下を参照してください。

- AWS でのセキュアブートとNitroTPM
- Google Cloud Platform でのセキュアブートとvTPM
- Microsoft Azure でのセキュアブートとvTPM
- Nutanix Prism Central でのセキュアブートとvTPM
- VMware でのvTPM
- XenServer® の Secure Boot と vTPM
- SCVMM でのセキュアブートとvTPM

AWS でのセキュアブートとNitroTPM

AWS 環境では、NitroTPM および/または UEFI Secure Boot が有効なマスターイメージ (AMI) を選択できます。したがって、カタログ内のプロビジョニングされた VM も NitroTPM および/または UEFI Secure Boot が有効になります。この実装により、VM が保護され、信頼できるものになります。NitroTPM および UEFI Secure Boot の詳細については、Amazon ドキュメント を参照してください。NitroTPM および UEFI Secure Boot が有効なカタログを作成するには、VM インスタンスの NitroTPM および UEFI Secure Boot を有効にする を参照してください。

Google Cloud Platform でのセキュアブートとvTPM

Google Cloud Platform (GCP) でシールドされた仮想マシンをプロビジョニングできます。シールドされたVM の検証可能な整合性は、次の機能を使用することで実現されます。

- セキュアブート
- vTPM対応メジャーブート
- 整合性監視

シールドされたVMでカタログを作成するためのPowerShellの使用方法について詳しくは、「Using PowerShell to create a catalog with shielded VM」を参照してください。

> **注:**
>
> マスターイメージにWindows 11をインストールする場合、マスターイメージ作成プロセス中にvTPMを有効にする必要があります。また、カタログ作成にマシンプロファイルを使用する場合、マシンプロファイルソース（VMまたはインスタンステンプレート）でvTPMを有効にする必要があります。単一テナントノードでのWindows 11 VMの作成について詳しくは、「Create Windows 11 VMs on the sole-tenant node」を参照してください。

Microsoft AzureにおけるセキュアブートとvTPM

Azure 環境では、Trusted Launch が有効なマシンカタログを作成できます。Azure は、第 2 世代 VM のセキュリティを向上させるシームレスな方法として Trusted Launch を提供します。Trusted Launch は、高度で永続的な攻撃手法から保護します。Trusted Launch を有効にするには、マシンプロファイルベースのカタログ構成を使用します。Trusted Launch の根幹には、VM の Secure Boot があります。Trusted Launch は、クラウドによるリモートアテステーションを実行するために vTPM も使用します。これは、プラットフォームのヘルスチェックや信頼に基づく決定を行うために使用されます。Secure Boot と vTPM は個別に有効にできます。 Trusted Launch を使用したマシンカタログの作成の詳細については、Trusted Launch を使用したマシンカタログ を参照してください。

Nutanix Prism CentralにおけるセキュアブートとvTPM

MCS は、Nutanix Prism Central を使用して、vTPM、UEFI、および Secure Boot を備えたマシンカタログの作成をサポートしています。vTPM および UEFI Secure Boot が有効なマスターイメージ (テンプレート) を選択できます。

Nutanix Prism Centralでは、UEFIセキュアブートはvTPMを必要としません。ただし、vTPMをVMにリンクするには、セキュアブートが有効かどうかにかかわらず、VMがUEFIで起動されている必要があります。

さらに、vTPM、UEFI、および Secure Boot が有効な VM は、Nutanix Prism Central からインポートでき、Citrix Virtual Apps and Desktops によって電源管理できます。

NutanixはvTPMとUEFIセキュアブートをサポートしています。以下を参照してください。

- AHVでのvTPM (仮想トラステッドプラットフォームモジュール) サポート。
- VMのセキュアブートサポート
- Virtual Trusted Platform Module を使用して AHV VM を保護する

VMware における vTPM

MCS は、vTPM を使用したマシンカタログの作成をサポートしています。マスターイメージに Windows 11 がインストールされている場合、マスターイメージで vTPM を有効にすることが要件となります。マシンプロファイルベースの構成が使用され、vTPM が有効になっている場合、カタログ内の VM は VM テンプレートから同じ vTPM コンテンツを継承します。マシンプロファイルが使用されておらず、マスターイメージで vTPM が有効になっている場合、カタログ内の VM は空の vTPM を持ちます。詳細については、マシンプロファイルを使用してマシンカタログを作成する を参照してください。

XenServer® のセキュアブートと vTPM

XenServer は、サポートされている一部の VM オペレーティングシステムで UEFI セキュアブートを提供します。セキュアブートは、署名されていない、誤って署名された、または変更されたバイナリが起動中に実行されるのを防ぎます。セキュアブートを強制する UEFI 対応 VM では、すべてのドライバーが署名されている必要があります。詳細については、「ゲスト UEFI とセキュアブート」を参照してください。

XenServer 8 では、UEFI セキュアブートに vTPM は必要ありません。ただし、vTPM を VM にリンクするには、その VM が UEFI で起動されている必要があります（セキュアブートが有効かどうかにかかわらず）。Windows 11 VM にはリンクされた vTPM が必要であり、提供されたテンプレートから Windows 11 VM が作成されるときに自動的に作成されます。他のオペレーティングシステムの場合、vTPM はオプションです。詳細については、「vTPM」を参照してください。

SCVMM におけるセキュアブートと vTPM

System Center Virtual Machine Manager (SCVMM) 環境では、vTPM および/またはセキュアブートが有効なマスターイメージとマシンプロファイルを選択できます。その結果、カタログは vTPM および/またはセキュアブートが有効な VM をプロビジョニングします。この実装により、VM は保護され、信頼性が維持されます。vTPM とセキュアブートが有効なカタログを作成するには、「マシンプロファイルを使用してカタログを作成する」を参照してください。

暗号化機能

暗号化機能は、共有仮想マシンホスト上の悪意のあるゲストによる攻撃や、ホスト上のすべての仮想マシンを管理するハイパーバイザー制御ソフトウェアによる攻撃から、仮想マシンのコンテンツを保護します。

サポートされているクラウドサービスの詳細については、以下を参照してください。

- AWS の暗号化機能
- Google Cloud Platform の暗号化機能
- Microsoft Azure の暗号化機能

AWS の暗号化機能

このセクションでは、AWS 仮想化環境における暗号化機能について説明します。

自動暗号化

アカウントで作成された新しい Amazon EBS ボリュームとスナップショットコピーの自動暗号化を有効にできます。詳細については、「自動暗号化」を参照してください。

Google Cloud Platform の暗号化機能

このセクションでは、Google Cloud Platform (GCP) 仮想化環境における暗号化機能について説明します。

Googleマネージド暗号化キーで許可されているよりもキー操作を詳細に制御する必要がある場合は、顧客管理の暗号化キーを使用できます。顧客管理の暗号化キーを使用する場合、オブジェクトがバケットに保存されるときにCloud Storageによってキーで暗号化され、オブジェクトがリクエスターに提供されるとCloud Storageによって自動的に復号化されます。詳細については、「顧客管理の暗号化キー」を参照してください。

MCS カタログに顧客管理の暗号化キー (CMEK) を使用できます。詳細については、「顧客管理の暗号化キー (CMEK) の使用」を参照してください。

Microsoft Azure の暗号化機能

このセクションでは、Azure仮想化環境における暗号化機能について説明します。

Azureサーバー側暗号化

ほとんどのAzureマネージドディスクは、Azure Storage暗号化で暗号化されています。これは、サーバー側暗号化 (SSE) を使用してデータを保護し、セキュリティとコンプライアンスのコミットメントを満たすのに役立ちます。Citrix Virtual Apps and Desktopsは、Azure Key Vaultを介した

Azureマネージドディスクの顧客管理の暗号化キーをサポートしています。詳細については、「Azureサーバー側暗号化」を参照してください。

ホストでのAzureディスク暗号化

ホストでの暗号化機能を備えたMCSマシンカタログを作成できます。

この暗号化方法は、Azureストレージを介してデータを暗号化しません。VMをホストするサーバーがデータを暗号化し、その後、暗号化されたデータがAzureストレージサーバーを介して流れます。したがって、この暗号化方法はデータをエンドツーエンドで暗号化します。

ホストでの暗号化機能を備えたMCSマシンカタログの作成の詳細については、ホストでのAzureディスク暗号化を参照してください。

Azure二重暗号化

二重暗号化は、プラットフォーム側暗号化（デフォルト）と顧客管理暗号化（CMEK）です。したがって、暗号化アルゴリズム、実装、または侵害されたキーに関連するリスクを懸念するセキュリティ意識の高いお客様は、この二重暗号化を選択できます。永続的なOSおよびデータディスク、スナップショット、イメージはすべて、二重暗号化によって保存時に暗号化されます。詳細については、マネージドディスクの二重暗号化を参照してください。

Azure機密VM

Azure機密コンピューティングVMは、仮想デスクトップがメモリ内で暗号化され、使用中に保護されることを保証します。

MCSを使用して、Azure機密VMを含むカタログを作成できます。このようなカタログを作成するには、マシンプロファイルワークフローを使用する必要があります。マシンプロファイルの入力として、VMとARMテンプレート仕様の両方を使用できます。

詳細については、Azure機密VMを参照してください。

サービスウィンドウ

サービスウィンドウ機能は、MCSプロビジョニングされたVMでの操作をスケジュール設定および自動化する機能を提供します。この機能は現在、OSディスクのリセットやハードウェア構成の変更など、さまざまな操作をサポートしています。これらの操作をスケジュール設定し、後で完了を確認できるため、手動で更新を実行する必要がありません。

特定のVMリストまたはマシンカタログ全体に対して操作をスケジュール設定できます。各操作は指定された時間に実行されます。同じVMに対して複数の操作をスケジュール設定できます。ただし、単一のVMに対して複数のハードウェア更新をスケジュール設定することはできません。

また、次のこともできます。

- サービスウィンドウの説明を追加する。
- 操作の実行時にログオンしているユーザーに表示される詳細なメッセージを提供する。
- 完了後、タスクのメタデータを何日間保持するかを指定する。
- 操作が強制的に実行される前に、ログオンしているユーザーが作業を保存するために何分間のバッファ時間が与えられるかを構成する。

利点

ユーザーエクスペリエンスと継続性の向上

- **グレースフルセッション処理**: 突然の切断ではなく、VMの電源がオフになる前に作業を保存するためのプロフェッショナルな通知を定義できます。
- **スケジュールされたダウンタイム**: 大規模な更新タスクをオフピーク時間帯（例: 午前2時）に移動でき、その時間に手動でログインする必要がありません。
- **費用対効果の高いハードウェア更新**: サービスウィンドウを使用してハードウェアを更新すると、大規模な実装で大幅なコストを節約できます。この機能は、VMが設定を適用するために再起動を必要とするかどうかを自動的に分析します。したがって、不要な再起動を回避することで、サービスウィンドウはこれらの費用を最小限に抑えます。

高度なハードウェアの柔軟性

- **ハードウェア構成の更新**: サービスウィンドウを使用してハードウェア更新をスケジュール設定します。システムは更新フローをインテリジェントに管理し、再起動の必要性を確認し、セッションのログオフを処理することで、手動での監視なしに、カタログが新しいリソース要件を満たすように進化することを保証します。
- **柔軟なSKU再構成**: 以前はカタログの手動再作成が必要だったSKUを簡単に更新できます。
- **既存のVMの休止状態のサポート**: 「一時ディスク」の制限を克服します。サービスウィンドウにより、MCSIOドライバーはページファイルをC:ドライブに再配置し、すでに展開されているVMで休止状態のプロパティを有効にできます。

重要な考慮事項

- **ユーザー通知**: ログインしているユーザーは、サービスウィンドウの操作に関する初期アラートを受け取り、作業を保存するのに十分な時間を確保できます。通知期間が終了すると、マシンは自動的にシャットダウンして操作を実行します。

サービスウィンドウの操作

サービスウィンドウは現在、OSディスクのリセット、既存のMCSプロビジョニング済みカタログのActive Directoryアカウントの修復、既存のMCSプロビジョニング済みカタログのEntraハイブリッド参加の有効化、およびハードウェア構成の変更をサポートしています。これらの操作は、Web StudioまたはPowerShellを使用して実行できます。

Web Studio: 現在、Azure環境でのみサポートされています。ガイダンスについては、特定のハイパーバイザーの記事を参照してください。

PowerShellコマンド: 一般的なコマンドはこの記事で概説されており、詳細なハイパーバイザー固有のスクリプトは弊社のGitHubページ `<https://github.com/citrix/citrix-mcs-sdk-samples/>` で確認できます。

OSディスクをリセットする

OSディスクのリセットは、PowerShellコマンド `New-ProvMaintenanceCycle` を使用して実行できます。このコマンドは、カタログ全体または特定のVM用に新しいサービスウィンドウを作成します。サイクルは、 `ScheduledStartTimeInUTC` で指定した時刻に開始されます。また、サービスウィンドウが実行できる最大時間を示す `MaxDurationInMinutes` も指定します。

例: 特定のVMのOSディスクをリセットする

```
New-ProvMaintenanceCycle -Operation ResetOSDisk
-MaintenanceCycleDescription "Resetting Boot Disk" -StartsNow
-MaxDurationInMinutes 100 -ProvisioningSchemeName CVC -PurgeDBAfterInDays
1 -SessionWarningTimeInMinutes 15 -SessionWarningLogOffTitle "Scheduled
Maintenance" -SessionWarningLogOffMessage "There is a scheduled
maintenance coming up and involves turning off the machine, please save
your work and log out, Thank You" -VMName VDA02,VDA03
```

例: カタログ全体のOSディスクをリセットする

```
New-ProvMaintenanceCycle -Operation ResetOSDisk
-MaintenanceCycleDescription "Resetting Boot Disk" -StartsNow
-MaxDurationInMinutes 100 -ProvisioningSchemeName CVC -PurgeDBAfterInDays
1 -SessionWarningTimeInMinutes 15 -SessionWarningLogOffTitle "Scheduled
Maintenance" -SessionWarningLogOffMessage "There is a scheduled
maintenance coming up and involves turning off the machine, please save
your work and log out, Thank You" -AllVMs
```

ハードウェア設定の更新

サービスウィンドウを使用してハードウェア更新をスケジュールすることで、変更がいつ適用されるかを完全に制御できます。必要に応じて、新しく作成されたVMのみ、カタログ全体（新規および既存のVM）、または特定のVMをターゲットに選択できます。

- 新しいVMまたはカタログ全体のハードウェア設定を更新するには、プロビジョニングスキームのバージョンを選択し、PowerShellコマンド `New-ProvSchemeHardwareUpdate` を実行します。以前に作成したプロビジョニングスキームのバージョンをVMに適用できます。一時ディスクを持つVMで休止状態を有効にすることもできます。
- 特定のVMのハードウェア設定を更新するには、VM構成バージョンを選択し、PowerShellコマンド `New-ProvVmHardwareUpdate` を実行します。

重要な考慮事項

- ハードウェア更新のスケジュール後にカタログに追加された新しいマシンは、新しい仕様を適用するための指定されたUTC時刻まで、古い仕様で作成され続けます。
- サービスウィンドウの作成中に単一の検証が失敗すると、サイクルが作成されなくなり、エラーメッセージが返されます。
- 休止状態を有効にするには、以下を考慮してください。
  - VDAのバージョンは2503より大きい必要があります。
  - Machine Creation Services I/O (MCSIO) がインストールされている必要があります。
  - マシンプロファイルが休止状態をサポートしている必要があります。
  - VM SKUとオペレーティングシステムが休止状態をサポートしている必要があります。
  - VBSが有効になっている場合、Hyper-Vも有効にする必要があります。ネストされた仮想化には、VMでTrusted Launchが必要です。
  - 空きOSディスクサイズは、VMのメモリサイズよりも大きい必要があります。

マシンカタログ全体または新しいVMでのハードウェア更新のスケジュール

1. 更新されたハードウェア設定で新しいプロビジョニングスキームバージョンを作成するには、`New-ProvSchemeVersion` を実行します。詳細については、SDKドキュメント を参照してください。
2. プロビジョニングスキームバージョンで指定されたハードウェア更新のサービスウィンドウをスケジュールするには、PowerShellコマンド `New-ProvSchemeHardwareUpdate` を実行します。

例: マシンカタログ内の `AllVMs` (新規および既存) が更新の対象となります:

```
New-ProvSchemeHardwareUpdate -ProvisioningSchemeVersion 4
-MaintenanceCycleDescription "Updating RAM and CPU Count to 8GB and 4"
-StartsNow -MaxDurationInMinutes 100 -ProvisioningSchemeName CVC
-PurgeDBAfterInDays 1 -SessionWarningTimeInMinutes 15
-SessionWarningLogOffTitle "Scheduled Maintenance"
-SessionWarningLogOffMessage "There is a scheduled maintenance coming up
and involves turning off the machine, please save your work and log out,
Thank You" -AllVMs
```

例: マシンカタログ内の `NewVMsOnly` (新規および既存) が更新の対象となります:

```
New-ProvSchemeHardwareUpdate -ProvisioningSchemeVersion 4
-MaintenanceCycleDescription "Updating RAM and CPU Count to 8GB and 4"
-StartsNow -MaxDurationInMinutes 100 -ProvisioningSchemeName CVC
-PurgeDBAfterInDays 1 -SessionWarningTimeInMinutes 15
-SessionWarningLogOffTitle "Scheduled Maintenance"
-SessionWarningLogOffMessage "There is a scheduled maintenance coming up
and involves turning off the machine, please save your work and log out,
Thank You" -NewVMsOnly
```

ハードウェアスキームの更新に関連付けられたサービスウィンドウオブジェクトを取得するには、`Get-ProvSchemeHardwareUpdate` を実行します。例:

```
Get-ProvSchemeHardwareUpdate -MaintenanceCycleId xxxx-xxxx-yyyy-zzzz
```

特定のVMでのハードウェア更新のスケジュール

1. 新しいプロビジョニングVM構成を作成するには、`New-ProvVmConfiguration`を実行します。詳細については、SDKドキュメントを参照してください。
2. VM構成バージョンで指定されているハードウェア更新のサービスウィンドウをスケジュールするには、PowerShellコマンド`New-ProvVmHardwareUpdate`を実行します。

> **注:**
>
> 各VMでは、パーソナライズされた設定（VM構成バージョン）が常にプロビジョニングスキームバージョンで定義された仕様よりも優先されます。特定のVMで設定がパーソナライズされていない場合、その値は関連付けられたプロビジョニングスキームバージョンから継承されます。

例:

```
New-ProvVmHardwareUpdate -ProvVmConfigurationVersion 4 -StartsNow
-MaxDurationInMinutes 100 -ProvisioningSchemeName CVC -VMName AbcTest01
```

ハードウェアVM更新に関連付けられているサービスウィンドウオブジェクトを取得するには、`Get-ProvVmHardwareUpdate`を実行します。例:

```
Get-ProvVmHardwareUpdate -MaintenanceCycleId xxxx-xxxx-yyyy-zzzz
```

プロビジョニングVMバージョンを作成するために使用されたパーソナライゼーションは、`Remove-ProvVmConfiguration`コマンドを使用して削除することもできます。例:

```
Remove-ProvVmConfiguration -Version 2 -VMName AbcTest01
```

既存のカタログのADアカウントを修復する

サービスウィンドウを使用して、既存のオンプレミスAD参加済みおよびMicrosoft Entraハイブリッド参加済みMCSマシンカタログのActive Directory（AD）コンピューターアカウントを修復できます。これは、VMがドメイン信頼を失った場合に役立ちます。この機能は、永続および非永続MCSマシンカタログの両方に適用されます。

既存のMCSマシンカタログのADアカウントを修復するには、PowerShellコマンドを使用して次の手順を実行します。

1. PowerShell ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. 次のいずれかの方法で`New-ProvIdentityUpdate`コマンドを実行します。

    - 「特定のVMのADアカウントを名前で修復するには:」:

        ```
        New-ProvIdentityUpdate -MaintenanceCycleDescription 'repair AD
        account' -Operation RepairADAccount -MaxDurationInMinutes 60
        -ProvisioningSchemeName <catalog-name> -VMName @("vm-1", "vm-2")
        -StartsNow
        ```

    - 操作をすぐに開始するのではなく、将来の時刻にスケジュールするには:

```
New-ProvIdentityUpdate -MaintenanceCycleDescription 'repair AD
account' -Operation RepairADAccount -MaxDurationInMinutes 60
-ProvisioningSchemeName <catalog-name> -AllVMs
-ScheduledStartTimeInUTC "2026-04-01T02:00:00Z"
```

4. 「メンテナンスサイクルのステータスを確認するには、`Get-ProvMaintenanceCycle` を実行します。」.

「詳細については、Citrix PowerShell SDK を参照してください。」

「**注:**」:

- この機能は、オンプレミスのActive Directory参加済みおよびMicrosoft Entraハイブリッド参加済みMCSマシンカタログにのみ適用されます。Entra ID参加済みおよび非ドメイン参加済みマシンはサポートしていません。
- プロビジョニングスキームのIDプールには、ドメイン内のコンピューターアカウントのパスワードをリセットするのに十分な権限を持つオンプレミスのActive Directoryサービスアカウントが必要です。

既存のMCSプロビジョニング済みカタログでEntraハイブリッド参加を有効にする

Service Windowを使用して、既存のオンプレミスActive Directory参加済みMCSマシンカタログをMicrosoft Entraハイブリッド参加済みカタログに変換できるようになりました。この機能は、永続および非永続MCSマシンカタログの両方に適用されます。

既存のMCSマシンカタログでEntraハイブリッド参加を有効にするには、PowerShellコマンドを使用して次の手順を実行します。

1. PowerShell ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. 次のいずれかの方法で`New-ProvIdentityUpdate`コマンドを実行します。
    - カタログ内のすべてのVMでEntraハイブリッド参加をすぐに有効にするには：

```
New-ProvIdentityUpdate -MaintenanceCycleDescription 'enable Entra
hybrid join' -Operation MigrateActiveDirectoryToEntraHybridJoin
-MaxDurationInMinutes 60 -ProvisioningSchemeName <catalog-name>
-AllVMs -StartsNow
```

- 特定のVMを名前で指定してEntraハイブリッド参加を有効にするには：

```
New-ProvIdentityUpdate -MaintenanceCycleDescription 'enable Entra
hybrid join' -Operation MigrateActiveDirectoryToEntraHybridJoin
-MaxDurationInMinutes 60 -ProvisioningSchemeName <catalog-name>
-VMName @("vm-1", "vm-2") -StartsNow
```

- Entraハイブリッド参加を有効にし、新しいVMのターゲットOUを指定するには：

```
New-ProvIdentityUpdate -MaintenanceCycleDescription 'enable Entra
hybrid join' -Operation MigrateActiveDirectoryToEntraHybridJoin
-MaxDurationInMinutes 60 -ProvisioningSchemeName <catalog-name>
-AllVMs -StartsNow -OU "OU=SyncedDevices,DC=example,DC=com"
```

- 操作をすぐに開始するのではなく、将来の時刻にスケジュールするには：

```
New-ProvIdentityUpdate -MaintenanceCycleDescription 'enable Entra
hybrid join' -Operation MigrateActiveDirectoryToEntraHybridJoin
-MaxDurationInMinutes 60 -ProvisioningSchemeName <catalog-name>
-AllVMs -ScheduledStartTimeInUTC "2026-04-01T02:00:00Z"
```

4. メンテナンスサイクルのステータスを確認するには、`Get-ProvMaintenanceCycle`を実行します。

詳細については、Citrix PowerShell SDKを参照してください。

注：

- カタログが正しく機能することを確認するには、カタログ内の既存のすべての仮想マシンをMicrosoft Entraハイブリッド参加に変換する必要があります。

- この機能は、IDプールを共有するMCSプロビジョニング済みカタログをサポートしていません。
- 既存のプロビジョニングスキームのベースイメージには、VDAバージョン2212以降がインストールされている必要があります。「Microsoft Entraハイブリッド参加の要件」を参照してください。
- プロビジョニングスキームのIDプールには、ドメイン内でuserCertificateプロパティを設定する権限を持つオンプレミスのActive Directoryサービスアカウントが必要です。
- コンピューターアカウントを含むOUが、Microsoft Entra Connect を介して Entra ID に同期するように構成されていることを確認します。2つのオプションがあります。
  - Azure AD Connect を構成して、元のOUからEntra IDにデバイスを同期します。
  - 既存のコンピューターアカウントを、Azure AD Connect 同期が構成されたOUに手動で移動します。

サービスウィンドウに関連するその他のPowerShellコマンド

- `Get-ProvMaintenanceCycle`：すべてのサービスウィンドウの情報を取得します。例：

```
Get-ProvMaintenanceCycle -MaintenanceCycleId
10073b8e-7e94-4527-8580-0e448eae0ad1
```

- `Get-ProvMaintenanceCycleVM`: 個々のVMの各サービスウィンドウ操作の情報を、そのステータスとともに取得します。例:

```
Get-ProvMaintenanceCycleVM -MaintenanceOperation HardwareUpdate
-VirtualMachineSid 42263076-44ae-1ff9-f58b-62d57ddf8db5
```

  サービスウィンドウのさまざまなステータスは次のとおりです。
  - 実行中
  - 失敗
  - 完了
  - キャンセル中
  - キャンセル済み
  - 未処理

  - 保留中
  - 不完全
  - 修復済み
  - 回復中

- `Remove-ProvMaintenanceCycle`: サービスウィンドウがアクティブでない場合に、サービスウィンドウを削除します。例:

```
Remove-ProvMaintenanceCycle -MaintenanceCycleId
867af1ba-5b72-402e-9dc3-033298248f8e
```

- `Cancel-ProvMaintenanceCycle`: 仮想マシン上でMCSによって操作がまだ開始されていない場合、このPowerShellコマンドは操作をキャンセルします。MCSは、現在仮想マシンで実行中の操作をキャンセルしません。例:

```
Cancel-ProvMaintenanceCycle -MaintenanceCycleId
867af1ba-5b72-402e-9dc3-033298248f8e
```

- `Restart-ProvMaintenanceCycle`: サービスウィンドウが、ハイパーバイザーの停止や時間不足などの外部要因により失敗したか不完全な場合、このコマンドはサイクルを再開し、失敗したジョブや未処理のジョブを処理するのに役立ちます。例:

```
Restart-ProvMaintenanceCycle -MaintenanceCycleId
4f363b78-458a-403a-82e5-7fcc6caa498b -ScheduledStartTimeInUTC "June
19th 2024, 6AM" -MaxAllocatedDurationInMinutes 400
```

- `Update-ProvMaintenanceCycle`: サービスウィンドウがすでにスケジュールされており、まだ開始されていない場合、このコマンドは特定のパラメーターを変更します。

  例: 最大期間の更新:

```
Update-ProvMaintenanceCycle -MaintenanceCycleId
4f363b78-458a-403a-82e5-7fcc6caa498b -MaxDurationInMinutes 100
```

  例: プロビジョニングスキームのVMを更新:

```
Update-ProvMaintenanceCycle -MaintenanceCycleId
4f363b78-458a-403a-82e5-7fcc6caa498b -ProvisioningSchemeUid
867af1ba-5b72-402e-9dc3-033298248f8e -VMName ncn01,ncn02
```

次のステップ

AzureでWeb Studioを使用してサービスウィンドウ操作を管理するには、Azureでのサービスウィンドウ操作を参照してください。

Azure でのサービスウィンドウ操作

この記事では、Azure 環境で Web Studio を使用してサービスウィンドウ操作を実行する方法について説明します。

サービスウィンドウは現在、OS ディスクのリセットとハードウェア構成の変更をサポートしています。

検索ノードと**マシンカタログ**ノードの両方で**ハードウェアビュー**を使用して、ハードウェア設定を更新し、OS ディスクをリセットします。

検索ノードのハードウェアビュー

検索ノード内のハードウェアビューには、MCS プロビジョニングされた VM と、マシンのセキュリティ設定、ネットワークの詳細、イメージ、マシンプロファイルの詳細などの重要なプロパティが表示されます。

検索ノード > ハードウェアビュー(/en-us/citrix-virtual-apps-desktops/current-release/media/search-hw-view-phase1.png)

コールアウト	エリア	説明
A	検索バー	クイック検索と、複雑な検索条件を定義できるフィルターベースの検索を提供します。詳細については、「マシンの検索」を参照してください。 **ヒント：**フィルターを使用して、特定のプロパティでマシン

コールアウト	エリア	説明
		をすばやく絞り込みます。たとえば、**ID タイプ = Microsoft Entra 参加済み**で、すべての Microsoft Entra 参加済みマシンを表示します。
B	デフォルトビューに切り替える	ハードウェアビューからデフォルトビューに切り替えます。
C	メインビュー	MCSプロビジョニングされたマシンとその重要なプロパティを表示します。「**表示する列**」アイコンを選択して、ビューをカスタマイズできます。利用可能な列の詳細については、マシン列を参照してください。
D	詳細ペイン	選択したマシンの詳細情報を表示します。
E	リストレベルのアクション	表示されているリスト全体に対して実行できるアクションを表示します： • 「**エクスポート**」アイコン: メインビューに表示されているマシンのリストを

コールアウト	エリア	説明
		CSVファイルにエクスポートします。 • 「**表示する列**」アイコン: リストのメインビューをカスタマイズします。

リファレンス: マシン列

この表は、ハードウェアビューのすべての列とその説明を一覧表示します。

列	説明
名前	マシンのDNSホスト名。
プロビジョニングスキーム名	マシンのプロビジョニングに使用されるプロビジョニングスキームの名前。
CPUコア	マシンに割り当てられたCPUコア数。
メモリ (MB)	マシンに割り当てられたメモリ量 (MB)。
永続性	マシンのディスクとデータが再起動後も保持されるかどうかを示します。
IDの種類	マシンのIDの種類。
保留中のイメージ更新	マシンのVMイメージが古くなっており、次回の再起動時に新しいイメージに更新される予定であるかどうかを示します。
最終起動時刻 (UTC)	マシンが最後に起動された日時 (UTC)。
WBCを使用	マシンがWBC (MCSIOとも呼ばれる) で構成されているかどうかを示します。
WBCディスクサイズ (GB)	マシンのMCSIOディスクキャッシュサイズ。

列	説明
WBCメモリサイズ (MB)	マシンのMCSIOメモリキャッシュサイズ。
IDプロバイダー	マシンのIDプロバイダー。
アクティベーションの種類	Windows VDAにのみ有効です。マシンのWindowsライセンス認証の種類。値には、サポートされていないVDA、キー管理サービス、マルチプルアクティベーションキー、および無効が含まれます。

VM のハードウェア設定を更新する

この機能は、サービスウィンドウを使用して、ストレージ、ライセンス、NIC などの VM ハードウェア設定への変更を一元的に管理および適用する方法を提供します。

制限事項

- 現在、Azure MCS 永続 VM のみでサポートされています。
- Quick Deploy カタログ VM ではサポートされていません。
- すべての VM は同じカタログに属している必要があります。
- 潜在的な問題を回避するには、以下を行う場合は VDA をバージョン 2503 以降にアップグレードしてください：
  - 既存の一時ディスクを使用しているVMの休止状態を有効にします。
  - 一時ディスクありのAzure SKUと一時ディスクなしのAzure SKUの間でVMサイズを変更します。

単一VMのハードウェア設定を更新する

1. **検索**ノードに移動します。**ハードウェアビュー**に切り替えます。更新するVMを右クリックし、**ハードウェアの更新**を選択します。
2. **ハードウェアの更新**ページで、**バージョンの作成**をクリックします。変更したい設定のみを構成します。デフォルト設定はありません。
3. **概要**ページに移動し、**完了**をクリックします。
4. 選択したVMに変更を適用するタイミングを確認するために、**スケジュール**または**バージョンのみ保存**のいずれかを選択します。

- **スケジュール**を選択すると、**VMに適用**ページにリダイレクトされます。スケジュール時間と情報を構成し、**保存**をクリックします。スケジュール付きの新しいハードウェアバージョンが作成されます。スケジュールが完了するとVMが更新されます。
- **バージョンのみ保存**を選択すると、システムは選択したVMに変更をすぐに適用せずに、新しいハードウェアバージョンを作成します。

> **注:**
>
> 新しく作成されたハードウェアバージョンは、以前のバージョンからの変更を継承します。
>
> 適用時間をスケジュールせずにハードウェア変更を保存した場合でも、VMに適用できます。

1. **検索**ノードに移動します。**ハードウェアビュー**に切り替えます。VMを右クリックし、**ハードウェアの更新**を選択します。
2. **ハードウェアの更新**ページで、バージョンを選択します。**VMに適用**をクリックしてスケジュールを作成します。スケジュールが完了するとVMが更新されます。

複数のVMのハードウェア設定を更新する

1. **検索**ノードに移動します。**ハードウェアビュー**に切り替えます。複数のVMを選択し、右クリックして**ハードウェアの更新**を選択します。
2. 「**ハードウェアバージョンを作成**」ウィザードには、デフォルト設定はありません。変更したい設定のみを構成してください。
3. 「**スケジュール**」ページでスケジュールを構成します。
4. 「**概要**」ページに移動します。作成ワークフローを完了します。
5. 作成後、各VMを右クリックし、「**ハードウェアの更新**」を選択してバージョン詳細を表示できます。

単一VMのハードウェアバージョンを管理する

単一VMのハードウェアバージョンを削除したり、スケジュールをキャンセルしたり、カスタマイズをクリアしたりできます。

- **ハードウェアバージョンの削除**: 「**ハードウェアの更新**」ページで、1つ以上のバージョンを選択し、「**削除**」をクリックしてバージョンを削除します。

- **スケジュールのキャンセル**: 「**ハードウェアの更新**」ページで、まだ開始されていないスケジュールをキャンセルしたい場合は、「**スケジュール**」ステータス列の「**キャンセル**」をクリックしてキャンセルします。
- **カスタマイズのクリア**: 「**ハードウェアの更新**」ページで、すべてのカスタムハードウェア設定を削除するバージョンを作成または適用したい場合は、「**カスタマイズのクリア**」をクリックします。バージョンを作成して適用するようにスケジュールするには、「**スケジュール**」を選択します。適用せずにバージョンを作成するには、「**バージョンのみ保存**」を選択します。

OSディスクをリセットする

この機能は、サービスウィンドウを使用して1つまたは複数のVMのOSディスクをリセットする方法を提供します。

制限事項

- 現在、Azure MCS永続VMのみがサポートされています。
- クイック展開カタログVMではサポートされていません。
- すべてのVMは同じカタログに属している必要があります。

単一または複数のVMのOSディスクをリセットする

1. 「**検索**」ノードに移動します。「**ハードウェアビュー**」に切り替えます。OSディスクをリセットしたいVMまたは複数のVMを右クリックし、利用可能な場合は「**OSディスクのリセット**」を選択します。
2. すぐにリセットするか、後でスケジュールするかを選択します。

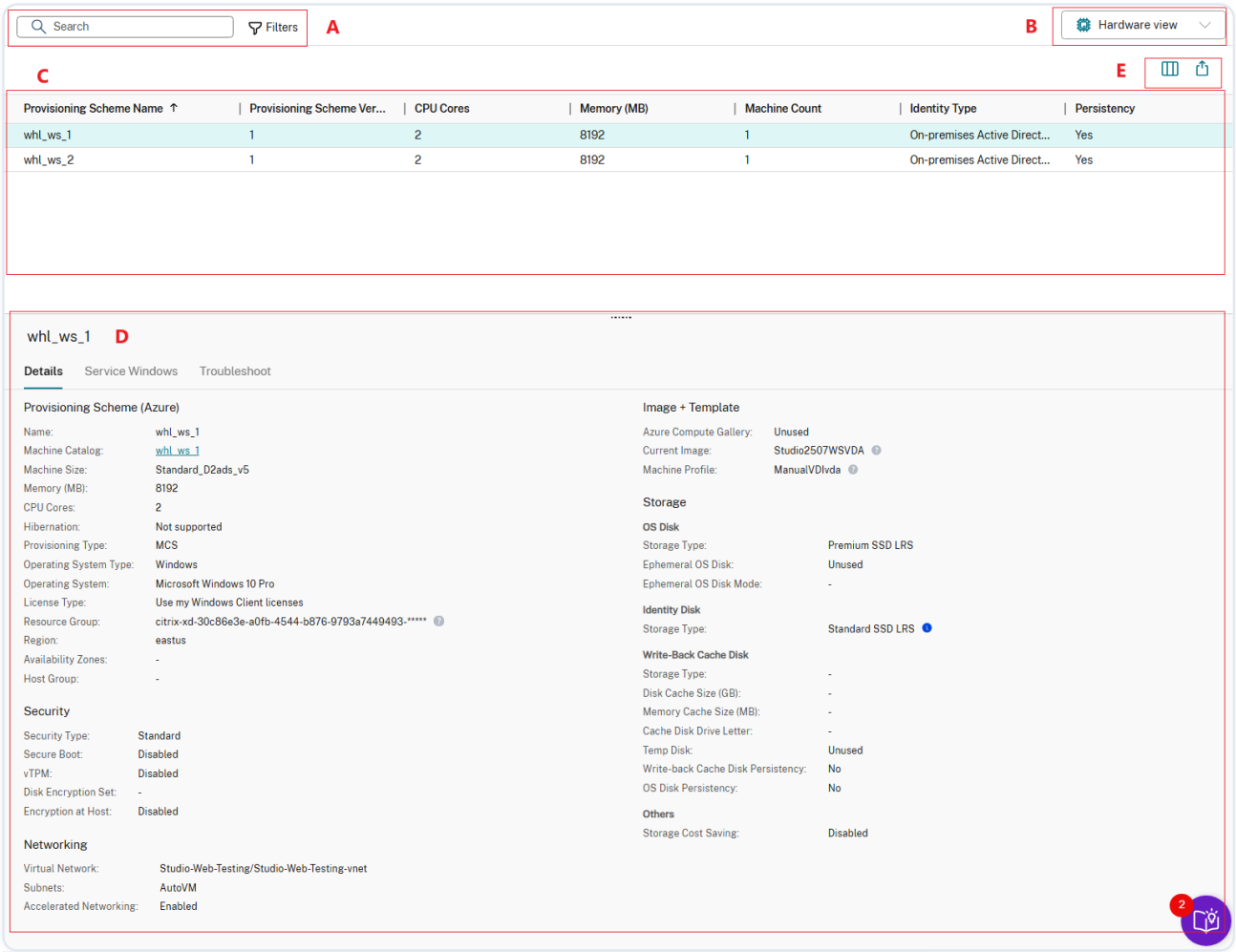
VM のタスクステータスを監視する

OS ディスクのリセットが正常に適用されたかどうかを確認するには、次の手順を実行します。

1. VM を選択します。
2. **詳細 > サービスウィンドウ**タブに移動し、**ステータス**列を確認します。
3. タスク ID をクリックして、**タスクセンター**にアクセスします。このセンターでは、詳細なタスクの進行状況と結果が提供されます。タスクセンターでタスクを監視および管理するを参照してください。

マシンカタログノードのハードウェアビュー

マシンカタログノード内の**ハードウェアビュー**には、プロビジョニングスキームとその重要なプロパティ（セキュリティ設定、ネットワーク詳細、イメージ、マシンプロファイル詳細など）が表示されます。



コールアウト	エリア	説明
A	検索バー	クイック検索と、複雑な検索条件を定義できるフィルターベースの検索を提供します。
B	ハードウェアビューのドロップダウン	**ハードウェアビュー**から**デフォルトビュー**に切り替えるには、これを選択します。
C	メインビュー	プロビジョニングスキームとその重要なプロパティを表示します。表示する列アイコンを選択して、ビューをカスタマイズできます。利用可

コールアウト	エリア	説明
		能な列の詳細については、プロビジョニングスキームの列を参照してください。
D	詳細ペイン	選択したプロビジョニングスキームの詳細情報を表示します。
E	リストレベルのアクション	表示されているリスト全体に対して実行できるアクションを表示します。 • **エクスポート**アイコン: メインビューに表示されているカタログのリストをCSVファイルにエクスポートします。 • **表示する列**アイコン: リストのメインビューをカスタマイズします。

リファレンス: ProvScheme列

この表は、**ハードウェアビュー**のすべての列とその説明を示しています。

列	説明
ProvScheme 名	プロビジョニングスキームの名前。
ProvSchemeバージョン	プロビジョニングスキームのバージョン番号

列	説明
CPUコア	プロビジョニングスキームに割り当てられたCPUコアの数。
メモリ (MB)	プロビジョニングスキームに割り当てられたメモリ量（MB単位）。
マシン数	プロビジョニングスキームによってプロビジョニングされたマシンの数。
永続性	プロビジョニングスキームのディスクとデータが再起動後も保持されるかどうかを示します。
IDの種類	プロビジョニングスキームのIDタイプ。
WBCを使用	プロビジョニングスキームがWBC（MCSIOとも呼ばれる）で構成されているかどうかを示します。
WBCディスクサイズ (GB)	プロビジョニングスキームのMCSIOディスクキャッシュサイズ。
WBCメモリサイズ (MB)	プロビジョニングスキームのMCSIOメモリキャッシュサイズ。
アクティベーションの種類	Windows VDAにのみ有効です。プロビジョニングスキームのWindowsライセンスアクティベーションタイプ。値には、Unsupported VDA、Key Management Service、Multiple Activation Key、Not validが含まれます。

マシンカタログのハードウェア設定を更新する

この機能は、サービスウィンドウを使用して、マシンプロファイル、ストレージ、ライセンス、NICなどのマシンカタログVMのハードウェア設定に対する変更を一元的に管理および適用する方法を提供します。変更は、既存のVMと新しいVMの両方に適用されます。

次のことができます。

- マシンカタログのハードウェア設定を更新する
- ハードウェアバージョンを管理する
- マシンカタログのタスクステータスを監視する

制限事項

- 現在、Azure MCSマシンカタログのみがサポートされています。
- クイック展開カタログではサポートされていません。
- 潜在的な問題を回避するには、次の操作を行う場合にVDAをバージョン2503以降にアップグレードしてください。
  - 一時ディスクを使用している既存のVMで休止状態を有効にする。
  - 一時ディスクありのAzure SKUと一時ディスクなしのAzure SKUの間でVMサイズを変更する。

マシンカタログのハードウェア設定を更新する手順

1. **マシンカタログ**ノードに移動し、**ハードウェア**ビューに切り替え、更新するマシンカタログを右クリックして、**ハードウェアの更新**を選択します。
2. 「**ハードウェアの更新**」ページで、「**バージョンを作成**」をクリックします。変更する設定のみを構成します。デフォルト設定はありません。
3. 「**概要**」ページに移動し、「**完了**」をクリックします。
4. 選択したマシンカタログに変更を適用するタイミングを確認するには、「**スケジュール**」または「**バージョンのみ保存**」のいずれかを選択します。
   - 「**スケジュール**」を選択すると、「**マシンカタログに適用**」ページにリダイレクトされます。スケジュール時間と情報を構成し、「**保存**」をクリックします。スケジュール付きの新しいハードウェアバージョンが作成されます。スケジュールが完了すると、マシンカタログが更新されます。
   - 「**バージョンのみ保存**」を選択すると、システムは選択したマシンカタログに変更をすぐに適用せずに、新しいハードウェアバージョンを作成します。

> **注:**
>
> 新しく作成されたハードウェアバージョンは、以前のバージョンからの変更を継承します。
>
> 適用時間をスケジュールせずにハードウェアの変更を保存した場合でも、マシンカタログにハードウェアの変更を適用できます。

1. マシンカタログを右クリックし、「**ハードウェアの更新**」を選択します。

2. 「**ハードウェアの更新**」ページで、バージョンを選択します。「**マシンカタログに適用**」をクリックしてスケジュールを作成します。スケジュールが完了すると、マシンカタログが更新されます。

マシンカタログのハードウェアバージョンを管理する

マシンカタログのハードウェアバージョンを削除したり、スケジュールをキャンセルしたりできます。

- **ハードウェアバージョンの削除**: 「**ハードウェアの更新**」ページで、1つ以上のバージョンを選択し、「**削除**」をクリックしてバージョンを削除します。
- **スケジュールのキャンセル**: 「**ハードウェアの更新**」ページで、まだ開始されていないスケジュールをキャンセルしたい場合は、「**スケジュール**」ステータス列の「**キャンセル**」をクリックしてキャンセルします。

マシンカタログのタスクステータスを監視する

ハードウェアの更新が正常に適用されたかどうかを確認するには：

1. マシンカタログを選択します。
2. **詳細 > サービスウィンドウ**タブに移動し、**ステータス**列を確認します。
3. タスクIDをクリックして**タスクセンター**にアクセスします。このセンターでは、タスクの進行状況と結果の詳細が提供されます。を参照してください(/ja-jp/citrix-virtual-apps-desktops/current-release/manage-deployment/task-center.html)

マシンの負荷分散

負荷分散は、組織が望むコストバランスを達成し、クラウドが提供するすべての利点を活用するのに役立ちます。負荷分散はデリバリーグループレベルで構成されます。

> **注:**

> 負荷分散は、マルチセッションOSマシンにのみ適用されます。

> 負荷分散には2つのオプションがあります。

- 水平負荷分散
- 垂直負荷分散

デフォルトでは、水平負荷分散が有効になっています。

水平負荷分散: 水平負荷分散モデルでは、受信ユーザーセッションは利用可能な最も負荷の低いマシンに割り当てられます。この例を考えてみましょう。展開環境で2つのVDAがあると仮定します。一方にはアクティブなユーザーセッション（ユーザー1）があり、もう一方のユーザー（ユーザー2）はセッションを待っています。水平負荷分散アルゴリズムは、より有利な負荷インデックスのため、ユーザー2をVDA 2に割り当てます。このように、水平アルゴリズムはすべての利用可能なVDAにセッションを分散するため、負荷が減少したときにマシンがオフになるのを妨げる可能性があります。

垂直負荷分散: 垂直負荷分散モデルでは、セッションは最も負荷インデックスが高いVDAに割り当てられます。これにより、受信ユーザーセッションを他のユーザーがすでに使用しているVDAに統合し、電源をオンにしてユーザーセッションの準備をしておく必要があるVDAの数を減らすことができます。水平負荷分散で述べたものと同じ展開環境を考えてみましょう。ユーザー1はVDA 1に割り当てられ、垂直負荷分散アルゴリズムがユーザー2のセッションに適用されます。負荷インデックスが高いのはVDA 1であるため、ユーザー2はVDA 1に割り当てられます。したがって、すべての受信セッションは、高負荷インデックスのウォーターマークに達するまで、最も負荷の高いVDAに割り当てられます。その後初めて、他のVDAがセッションの受信を開始します。

サイトレベルでの負荷分散設定

すべてのデリバリーグループに対して負荷分散を構成できます（サイト全体の構成）。

Studioからこの機能を構成するには、左ペインで**設定**を選択します。**マシンのセッション負荷分散**の下のオプションを選択します。

または、PowerShellを使用して、サイト全体で垂直負荷分散を有効または無効にできます。`Set-BrokerSite` コマンドレットで `UseVerticalScalingForRdsLaunches` 設定を使用します。`UseVerticalScalingForRdsLaunches` 設定の値を表示するには、`Get-BrokerSite` を使用します。詳細については、コマンドレットのヘルプを参照してください。

> **ヒント:**
>
> マシンがホストできるセッションの最大数を指定するには、最大セッション数 ポリシー設定を使用します。

デリバリーグループレベルでの負荷分散設定

ロードバランシングはデリバリーグループレベルで構成でき、サイトレベルから継承されたロードバランシング設定を上書きできます。

これは、デリバリーグループの作成中または既存のデリバリーグループの編集中に構成できます。「手順2. ロードバランシング」を参照してください。

ロード管理

ロード管理は、サーバーの負荷を測定し、現在の環境条件でどのサーバーを選択するかを決定します。この選択は、以下に基づいています。

- **サーバーメンテナンスモードの状態**: マルチセッションOSマシンは、メンテナンスモードがオフの場合にのみロードバランシングの対象となります。
- **サーバー負荷インデックス**: マルチセッションOSマシンを提供するサーバーが接続を受信する可能性を決定します。このインデックスは、セッション数やCPU、ディスク、メモリ使用量などのパフォーマンスメトリックの設定といった負荷評価子の組み合わせです。負荷評価子は、ロード管理ポリシー設定で指定されます。デフォルトでは、負荷インデックスは計算にセッション数のみを使用し、CPU、ディスク、メモリはロード管理ポリシー設定で構成されるまで使用しません。ポリシー設定の詳細については、「ロード管理ポリシー設定」を参照してください。

  サーバー負荷インデックスが10000の場合、サーバーが完全にロードされていることを示します。他のサーバーが利用できない場合、ユーザーはセッションを起動したときに、デスクトップまたはアプリケーションが現在利用できないというメッセージを受け取る可能性があります。 負荷インデックスは、Director (Monitor)、Studio検索、およびSDKで監視できます。

  コンソール表示で、**サーバー負荷インデックス**列（デフォルトでは非表示）を表示するには、マシンを選択し、列ヘッダーを右クリックして、**列の選択**を選択します。**マシンカテゴリ**で、**負荷インデックス**を選択します。

  SDKでは、`Get-BrokerMachine` コマンドレットを使用します。詳細については、「CTX202150」を参照してください。
- **同時ログオン許容ポリシー設定**: サーバーへの同時ログオン要求の最大数。（この設定は、XenApp 6.xバージョンでのロードスロットリングに相当します。）

  すべてのサーバーが同時ログオン許容設定以上の場合、次のログオン要求は保留中のログオンが最も少ないサーバーに割り当てられます。複数のサーバーがこれらの基準を満たす場合、負荷インデックスが最も低いサーバーが選択されます。「同時ログオン許容」を参照してください。

> **ヒント:**

> ログオン許容設定を適用し、指定された数を超える同時ログオンを失敗させるには、`Set-BrokerServiceConfigurationData Core.LogonToleranceIsHardLimit -SettingValue $true` を実行できます。

デリバリーグループの作成

> **注:**
>
> バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

> デリバリーグループは、1つ以上のマシンカタログから選択されたマシンの集合です。デリバリーグループは、どのユーザーがそれらのマシンにアクセスできるか、および利用可能なアプリケーションとデスクトップを定義します。

デリバリーグループの作成は、サイトとマシンカタログを設定した後の次のステップです。後で初期設定を変更したり、必要に応じて追加のデリバリーグループを作成したりできます。

一部の機能と設定は、既存のデリバリーグループを編集する場合にのみ構成できます。詳細については、「デリバリーグループの管理」を参照してください。

始める前に

デリバリーグループを作成する前に：

- 必要な選択肢と情報を理解するために、この記事を確認してください。
- ハイパーバイザー、クラウドサービス、またはマシンをホストするその他のリソースへの接続が作成されていることを確認してください。
- 仮想マシンまたは物理マシンを含むマシンカタログが利用可能であることを確認してください。

デリバリーグループを作成するには：

1. デリバリーグループなしでサイトとマシンカタログを作成した場合、Web Studioはデリバリーグループを作成するための正しい開始場所に案内します。

ウィザードのページ

サイトとマシンカタログを作成したが、デリバリーグループを作成していない場合、Web Studioはデリバリーグループを作成するための正しい開始点に案内します。

すでにデリバリーグループを作成しており、別のデリバリーグループを作成したい場合は、次の手順に従ってください。

1. を選択します。
2. アクションペインで、 を選択します。
3. デリバリーグループを整理するには、デフォルトの**Delivery Groups**フォルダーの下にフォルダーを作成できます。詳しくは、「フォルダーの作成」を参照してください。
4. グループを作成するフォルダーを選択し、**Create Delivery Group**をクリックします。グループ作成ウィザードが開きます。
5. ウィザードは**Introduction**ページから開始します。このページは、今後起動する際にスキップすることもできます。その後、次の表に示すいくつかのページが表示されます。各ページを完了したら、**Next**をクリックして最終ページに進みます。

	マルチセッションOS	シングルセッションOS静的（割り当て済み）	シングルセッションOS共有（プール済み）	リモートPCアクセス
ページ	マシン	マシン	マシン	マシン
	負荷分散	デリバリーの種類	ユーザー	ユーザー
	ユーザー	ユーザー	アプリケーション	アプリケーション
	アプリケーション	アプリケーション	デスクトップ	デスクトップ割り当てルール
	デスクトップ	デスクトップ割り当てルール	アプリ保護	アプリ保護
	アプリ保護	アプリ保護	スコープ	スコープ
	スコープ	スコープ	ライセンス契約	ライセンス契約
	ライセンス契約	ライセンス契約	ポリシーセット	ポリシーセット

	マルチセッションOS	シングルセッションOS静的（割り当て済み）	シングルセッションOS共有（プール済み）	リモートPCアクセス
	ポリシーセット	ポリシーセット	ローカルホストキャッシュ	概要
	概要	概要	概要	

注:

- 選択したシングルセッションOS静的マシンカタログに利用可能な割り当て済みマシンがある場合、**マシン割り当て**ページ（**マシン**ページの直後）が表示されます。
- ローカルホストキャッシュ設定ページは、電源管理されたシングルセッションのプールされたマシンを含むデリバリーグループでのみ利用可能です。

マシンページ

1. シングルセッションのサスペンド対応VMのみでデリバリーグループを作成するには、**このデリバリーグループにサスペンド機能を必須にする**を選択します。

   注:

   この機能は、シングルセッションのサスペンド対応マシンにのみ適用されます。

2. マシンカタログを選択し、そのカタログから使用するマシンの数を選択します。

重要な考慮事項

- カタログを選択する際、リストには未使用のマシンが少なくとも1台あるカタログのみが表示されます。
- 1つのカタログは複数のデリバリーグループにマシンを提供できます。1つのマシンは1つのデリバリーグループでのみ使用できます。デリバリーグループにマシンを追加すると、Web Studioはデフォルトで同じカタログを提案します。

- 1つのデリバリーグループは複数のカタログのマシンを使用できますが、それらのカタログには同じマシンタイプ（マルチセッションOS、シングルセッションOS、またはリモートPCアクセス）が含まれている必要があります。デリバリーグループ内のすべてのマシンは、同じ割り当てタイプ（プールまたは静的）である必要があります。つまり、デリバリーグループ内でマシンタイプを混在させることはできません。
- Citrixでは、すべてのマシンで最新のVDAバージョンを使用することをお勧めします。
- **リモートPCアクセス**の場合、サイトを作成すると、**Remote PC Access Machines**という名前のカタログと**Remote PC Access Desktops**という名前のデリバリーグループが自動的に作成されます。**Remote PC Access Machines**カタログ内の各マシンは、自動的にデリバリーグループに関連付けられます。
- 以下の互換性チェックが実行されます。
  - MinimumFunctionalLevelは互換性がある必要があります
  - SessionSupportは互換性がある必要があります
  - AllocationTypeはSingleSessionと互換性がある必要があります
  - Remote PC Access は Remote PC Access カタログとのみ互換性があります。

マシンの割り当てページ

「**マシン**」ページで選択されたシングルセッションOS静的マシンカタログに、利用可能な割り当て済みマシンがある場合、「**マシンの割り当て**」ページが表示されます。

このページを使用して、このデリバリーグループ内のマシンについて、ユーザーの割り当てとデスクトップの表示名を管理します。

- 「**表示名**」フィールドを使用して、デスクトップの表示名を管理します。
- 「**参照**」をクリックし、ユーザーまたはグループを選択します。

負荷分散ページ

「**マシン上のセッションの負荷分散**」ページは、マルチセッションOSマシンで利用できます。

このページを使用して、このデリバリーグループで使用する負荷分散設定を構成します。デフォルトでは、デリバリーグループはサイト全体の負荷分散設定を使用します。

1. このデリバリーグループの負荷分散設定を構成するには、「**サイト全体の設定を上書き**」チェックボックスを選択します。
2. 必要に応じて、「**水平負荷分散**」または「**垂直負荷分散**」オプションを選択します。水平負荷分散と垂直負荷分散の方法については、マシンの負荷分散を参照してください。

デリバリーグループ作成時の負荷分散設定(/en-us/citrix-virtual-apps-desktops/current-release/media/load-balancing.png)

「**垂直負荷分散**」を選択した場合、同時ログオン許容数と最大セッション数ポリシーが適切に構成されていることを確認してください。

配信の種類ページ

「**配信の種類**」ページは、シングルセッションOS静的（割り当て済み）マシンにのみ表示されます。

このページを使用して、カタログ内のマシンを構成し、デスクトップまたはアプリケーションをユーザーに配信します。

1. **アプリケーション**または**デスクトップ**のいずれかを選択します。両方を有効にすることはできません。

> **注:**
>
> マルチセッションOSまたはシングルセッションOSのランダム（プールされた）カタログからマシンを選択した場合、配信タイプはアプリケーションとデスクトップであると見なされます。アプリケーション、デスクトップ、またはその両方を配信できます。

ユーザーページ

ユーザーページはすべてのマシンタイプで利用できます。ただし、ページ上のオプションはマシンタイプによって異なります。

このページを使用して、ユーザーがデリバリーグループ内のリソースにアクセスする方法を指定します。

ユーザーアクセス制御の仕組み

デリバリーグループでのユーザーアクセスは、アクセス設定を作成または編集する際に指定されたユーザーリストを通じて制御されます。

- 以下の *すべての*条件を満たすユーザーは、デリバリーグループ内の**アプリケーション**にアクセスできます。
    - このデリバリーグループ内のリソース（アプリとデスクトップ）にアクセスできること。デフォルトでは、アクセスは展開のユーザーアクセスリスト（Active Directoryのユー

ザー）によって決定され、これはStudioでは構成されません。詳細については、「デリバリーグループでのユーザーの追加または削除」を参照してください。

- このグループのアプリケーションにアクセスできます。デフォルトでは、アプリケーションエンタイトルメントポリシー規則には全員が含まれます。詳細については、PowerShell SDK `BrokerAppEntitlementPolicyRule` コマンドレットを参照してください。
- このアプリケーションを含むアプリケーショングループにアクセスできること。

- 以下の*両方*の条件を満たすユーザーは、デリバリーグループ内のデスクトップにアクセスできます。
  - このデリバリーグループ内のリソース（アプリとデスクトップ）にアクセスできること。デフォルトでは、アクセスは展開のユーザーアクセスリスト（Active Directoryのユーザー）によって決定され、これはStudioでは構成されません。デフォルトのユーザースコープからユーザーを追加または削除できます。詳細については、「デリバリーグループでのユーザーの追加または削除」を参照してください。
  - このグループ内のデスクトップにアクセスできること。詳しくは、「デスクトップ（またはデスクトップ割り当て規則ページ）」を参照してください。

構成手順

1. デリバリーグループ内のリソースの使用を許可または制限するオプションのいずれかを選択します：
   - **認証済みユーザーによるリソースの使用を許可する：** アプリケーションとデスクトップにアクセスするには、指定したユーザーとグループメンバーが、スマートカードやユーザー名とパスワードなどの資格情報をStoreFront™またはCitrix Workspace™アプリに提示する必要があります。（シングルセッションOSマシンを含むデリバリーグループの場合、後でデリバリーグループを編集してユーザーデータ（ユーザーリスト）をインポートできます。）
   - **リソースの使用を制限する：** または、ユーザーまたはユーザーグループを**許可リスト**に追加することで、デリバリーグループの使用を制限できます。**許可リスト**のユーザーのみが、デリバリーグループ内のアプリとデスクトップにアクセスできます。また、**ブロックリストの追加**をクリックして、ユーザーとユーザーグループをブロックリストに追加することもできます。これにより、ユーザーは選択したデリバリーグループ内のアプリとデスクトップを使用できなくなります。ブロックリストは、許可リスト内のユーザーをブロックする場合にのみ意味があります。
2. セッションへのユーザーログオンのIDタイプを選択します：

- **Active Directory**: ユーザーがActive Directoryの資格情報を使用してデリバリーグループ内のリソースにログオンできるようにします。
- **Microsoft Entra ハイブリッドID**: ユーザーがActive DirectoryまたはMicrosoft Entra ハイブリッドIDのいずれかを使用してデリバリーグループ内のリソースにログオンできるようにします。

> **注:**
>
> Microsoft Entra シングルサインオン (SSO) が構成されていない場合、**Microsoft Entra ハイブリッドID** オプションは利用できません。

3. マルチセッションOSマシンの場合、ユーザーがStoreFrontまたはCitrix Workspaceアプリに資格情報を提示せずにアプリケーションとデスクトップにアクセスできるようにするには、**認証されていない（匿名）ユーザーへのアクセスを許可する。資格情報は不要**を選択します。たとえば、キオスクではアプリケーションに資格情報が必要な場合がありますが、Citrixアクセスポータルとツールには必要ありません。
   - 認証されていないユーザーアカウントは、セッションが起動されるとオンデマンドで作成され、AnonXYZという名前が付けられます。ここでXYZは一意の3桁の値です。
   - 認証されていないユーザーセッションには、デフォルトで10分間のアイドルタイムアウトがあり、クライアントが切断されると自動的にログオフされます。再接続、クライアント間のローミング、およびWorkspace Controlはサポートされていません。
4. ユーザーのホームゾーンに十分なリソースがある場合に、セッションが他の利用可能なゾーンにデフォルトで設定されるのを防ぐには、**セッションをユーザーのホームゾーンで起動することを要求する（構成されている場合）**を選択します。
5. デバイスや現在のセッションの有無にかかわらず、セッションを追跡させたい場合は、**ユーザーと共にクライアントデバイス間でセッションローミングを許可する**を選択します。(/ja-jp/citrix-virtual-apps-desktops/current-release/manage-deployment/sessions.html#session-roaming)を参照してください。

次の表は、**ユーザー**ページでの選択肢について説明しています。

アクセスを有効にする対象	ユーザーとユーザーグループを追加/割り当てますか？	「認証されていないユーザーにアクセスを許可する」チェックボックスを有効にしますか？
認証済みユーザーのみ	はい	いいえ

アクセスを有効にする対象	ユーザーとユーザーグループを追加/割り当てますか？	「認証されていないユーザーにアクセスを許可する」チェックボックスを有効にしますか？
認証されていないユーザーのみ	いいえ	はい
認証済みユーザーと未認証ユーザーの両方	はい	はい

アプリケーションページ

「**アプリケーション**」ページは、すべてのマシンタイプで利用できます。ただし、追加できるアプリケーションは、マシンタイプによって異なります。

このページを使用して、このグループのデスクトップにパッケージ化されたアプリケーションを追加できます。

重要な考慮事項

- デリバリーグループにパッケージ化されたアプリケーションを追加できます。これらのアプリケーションを含むパッケージは、ユーザーがデスクトップまたはRemote PCにサインインするたびに自動的にマウントされます。
- デフォルトでは、追加する新しいアプリケーションは「Applications」という名前のフォルダーに配置されます。別のフォルダーを指定することもできます。詳細については、アプリケーションの記事を参照してください。
- アプリケーションのプロパティは、デリバリーグループに追加するとき、または後で変更できます。詳細については、アプリケーションの記事を参照してください。
- アプリケーションを追加しようとして、そのフォルダーに同じ名前のアプリケーションが存在する場合、追加しようとしているアプリケーションの名前を変更するよう求められます。拒否した場合、そのアプリケーションは、そのアプリケーションフォルダー内で一意になる接尾辞を付けて追加されます。
- 複数のデリバリーグループにアプリケーションを追加する場合、それらすべてのデリバリーグループでアプリケーションを表示する権限がないと、表示に関する問題が発生する可能性があります。そのような場合は、より高い権限を持つ管理者に相談するか、アプリケーションが追加されたすべてのデリバリーグループを含むようにスコープを拡張してください。
- 同じ名前のアプリケーションを2つ、同じユーザーに公開する場合、アプリケーション名（ユーザー向け）プロパティを変更してください。そうしないと、ユーザーはCitrix Workspaceアプリで重複した名前を目にすることになります。

構成手順

1. アプリケーションソースを表示するには、**追加**メニューを選択します。

   - **スタートメニューから:** アプリケーションは、デリバリーグループに割り当てられている現在登録済みのVDAのいずれかを介して検出されます。このソースを選択すると、検出されたアプリケーションのリストが表示された新しいページが起動します。追加したいアプリケーションを選択し、**OK**を選択します。
   - **手動で：** デリバリーグループ内のVDAまたはネットワーク上の他の場所にあるアプリケーション。このソースを選択すると、新しいページが開き、次の方法で追加するアプリケーションを指定します。

     ◦ 実行可能ファイルへのパス、作業ディレクトリ、オプションのコマンドライン引数、および管理者とユーザーの表示名を入力します。

     ◦ デリバリーグループ内のVDAからアプリケーションを選択します。これを行うには、**［参照］** をクリックし、VDAにアクセスするための資格情報を入力し、VDAへの接続を待ってから、VDAからアプリケーションを選択します。選択したアプリケーションのプロパティが、ページのフィールドに自動的に入力されます。

   - **既存:** 以前に展開に追加されたアプリケーション（おそらく別のデリバリーグループ内）。このソースを選択すると、検出されたアプリケーションのリストが表示された新しいページが起動します。追加したいアプリケーションを選択し、**OK**を選択します。
   - **アプリケーションパッケージ:** App-V、MSIX、MSIX app attach、またはFlexAppアプリケーションパッケージ内のアプリケーション。このソースを選択すると、**パッケージからのアプリケーションの追加**ページが起動します。アプリケーションパッケージソースを選択し、表示された結果から追加したいアプリケーションを選択し、**OK**を選択します。

     > **注:**
     >
     > ◦ サイトにアプリケーションパッケージが構成されていない場合、このオプションは淡色表示されます。
     >
     > \> - MSIXまたはMSIX app attachアプリを公開するには、デリバリーグループの機能レベルが2106以降である必要があります。FlexAppアプリの場合、機能レベルは2206以降である必要があります。機能レベルの要件が満たされない場合、**アプリケーションパッケージソース**ドロップダウンリストの対応するオプションは淡色表示されます。

- **アプリケーショングループ:** 展開内に存在するアプリケーショングループ。

アプリケーションソースまたはアプリケーションが利用できないか無効な場合、それは表示されないか、選択できません。たとえば、展開にアプリケーションが追加されていない場合、**既存**ソースは利用できません。または、アプリケーションが選択されたマシンカタログ内のマシンのサポートされているセッションタイプと互換性がない場合があります。

デスクトップ（またはデスクトップ割り当てルール）ページ

このページのタイトルは、ウィザードで以前に選択したマシンカタログによって異なります。

- マルチセッションまたはプールされたシングルセッションマシンを含むカタログを選択した場合、このページは**デスクトップ**というタイトルになります。
- シングルセッションの静的マシンを含むカタログを選択し、**配信の種類**ページで「デスクトップ」を指定した場合、このページは**デスクトップ割り当てルール**というタイトルになります。

> **注:**
>
> シングルセッションの静的マシンを含むカタログを選択し、**配信の種類**ページで「アプリケーション」を指定した場合、このページは表示されません。

1. (オプション) デフォルトのデスクトップアイコンを更新するには、**変更**を選択します。ローカルマシンまたはVDAマシンから`.ico`または`.exe`ファイルを参照して選択します。サポートされるアイコンファイルの最大サイズは500 KBです。このアイコンは、個々のデスクトップに別のアイコンが設定されていない限り、グループ内のすべてのデスクトップのデフォルトアイコンを上書きします。
2. **追加**を選択します。ダイアログボックスで:
    a. **表示名**および**説明**フィールドに、Citrix Workspaceアプリに表示する情報を入力します。
    b. マルチセッションまたはプールされたシングルセッションOSマシンの場合: デスクトップにタグ制限を追加するには、**このタグを持つマシンへの起動を制限する**を選択し、メニューからタグを選択します。
    c. ラジオボタンを使用して、次のいずれかを実行できます。
        i. **この配信グループへのアクセス権を持つすべてのユーザーがデスクトップを使用できるようにする。** 配信グループ内のすべてのユーザーは、デスクトップを起動できます（プールされたマシンを持つグループの場合）、またはデスクトップを起動したとき

にマシンを割り当てられます（シングルセッションの静的マシンを持つグループの場合）。

ii. **デスクトップの使用を制限する**には、ユーザーとユーザーグループを**許可リスト**に追加します。**許可リスト**のユーザーのみがデスクトップにアクセスできます。**［ブロックリストの追加］** をクリックして、ユーザーとユーザーグループをブロックリストに追加することもできます。これにより、ユーザーは選択したデリバリーグループのデスクトップを使用できなくなります。ブロックリストは、許可リスト内のユーザーをブロックする場合にのみ意味があります。

d. グループにシングルセッションの静的マシンが含まれている場合、ユーザーあたりの最大デスクトップ数を指定します。これは1以上の値である必要があります。この設定は必須ではありません。マシンを手動で割り当てるか、RemotePCを使用してマシンを自動的に割り当てることができます。

e. (オプション) **変更**を選択して、プールされたデスクトップのデスクトップアイコン、またはシングルセッション静的デスクトップのデスクトップ割り当てルールを更新します。ローカルマシンまたはVDAマシンから`.ico`または`.exe`ファイルを参照してアイコンを選択します。サポートされるアイコンファイルの最大サイズは500 KBです。指定されたアイコンは、デリバリーグループレベルで設定されたデフォルトのアイコンを上書きします。

f. デスクトップ（マルチセッションマシン用）またはデスクトップ割り当てルール（シングルセッション静的マシン用）を有効または無効にします。デスクトップを無効にすると、デスクトップの配信が停止します。デスクトップ割り当てルールを無効にすると、ユーザーへのデスクトップの自動割り当てが停止します。

g. ダイアログボックスでの作業が完了したら、**OK**を選択します。

サイト内のデスクトップの最大インスタンス数（PowerShellのみ）

サイト内のデスクトップの最大インスタンス数を構成するには（PowerShellのみ）：

- PowerShellで、適切なBrokerEntitlementPolicyRuleコマンドレットをMaxPerEntitlementInstancesパラメーターとともに使用します。たとえば、次のコマンドレットは、`tsvda-desktop`ルールを変更して、サイトで許可されるデスクトップの同時インスタンスの最大数を2に設定します。2つのデスクトップインスタンスが実行されている場合、3番目のサブスクライバーがデスクトップを起動しようとするとエラーが発生します。

```
Set-BrokerEntitlementPolicyRule -Name tsvda-desktop
-MaxPerEntitlementInstances 2
```

- ガイダンスについては、Get-Help コマンドレットを使用してください。たとえば、`Get-Help Set-BrokerEntitlementPolicyRule-Parameter MaxPerEntitlementInstances`。

アプリ保護ページ

アプリ保護ページは、すべてのマシンタイプで利用できます。

このページを使用して、Citrix公開アプリケーションとデスクトップのセキュリティを強化できます。

次の情報は、`<https://docs.citrix.com/ja-jp/citrix-workspace-app/app-protection.html>` の Citrix Workspace アプリのドキュメントにある App protection の記事を補足するものです。

- 有効な App Protection の資格が必要です。App Protection 機能を購入するには、Citrix の営業担当者にお問い合わせください。
- App protection には XML 信頼が必要です。XML 信頼を有効にするには、**［設定］> ［XML 信頼を有効にする］** に移動します。

保護は以下の条件で適用されます。

- **画面キャプチャ防止**：
  - WindowsおよびmacOSでは、保護されたコンテンツのウィンドウのみが空白になります。保護されたウィンドウが最小化されていない場合、アプリ保護はアクティブになります。
  - Linuxでは、キャプチャ全体が空白になります。保護されたウィンドウが最小化されているかどうかにかかわらず、アプリ保護はアクティブになります。
- **キーロギング防止**：保護されたウィンドウがフォーカスされている場合に有効になります。保護を無効にするには、別のウィンドウにフォーカスを変更します。

スコープページ

スコープページは、すべてのマシンタイプで利用できます。

このページを使用して、組織に関連する方法でオブジェクト（接続、カタログ、デリバリーグループなど）をグループ化します。

ライセンス割り当てページ

ライセンス割り当てページは、すべてのマシンタイプで利用できます。

このページを使用して、デリバリーグループで使用するライセンスを指定します。デフォルトでは、デリバリーグループはサイトライセンスを使用します。詳細については、「マルチタイプライセンス」を参照してください。

ポリシーセットページ

ポリシーセットページは、すべてのマシンタイプで利用できます。

このページを使用して、このデリバリーグループが使用するポリシーセットを指定します。

ローカルホストキャッシュ設定ページ

このページは、電源管理されたシングルセッションのプールされたマシンを含むデリバリーグループでのみ利用できます。

デフォルトでは、電源管理されているプールされたマシンは、データ漏洩のリスクがあるため、ローカルホストキャッシュ (LHC) モードでは使用できません。デフォルトの動作を変更し、LHCモードで新しいユーザー接続に利用できるようにするには、**［リソースを維持する］** を選択します。

または、PowerShellコマンドを使用してデフォルトの動作を変更することもできます。詳しくは、「アプリケーションとデスクトップのサポート」を参照してください。

> **重要:**
>
> 電源管理されたシングルセッションのプールされたマシンへのアクセスを有効にすると、以前のユーザーセッションからのデータと変更が後続のセッションに存在する可能性があります。

ローカルホストキャッシュでの1回限りの使用のプールされたデスクトップ

ローカルホストキャッシュ（LHC）の停止中、プールされたデスクトップは1回限り使用できます。これは、対応するVDAにハイジーンブロブを発行し、再起動を開始することによって実現されます。このプロセスにより、停止からの復旧時にデスクトップのクリーンな状態が保証されます。対応していないマシンやレガシーマシンの場合、再利用が明示的に有効になっている場合にのみ参加します。 この機能は、停止時の可用性をよりシームレスにすることで、顧客満足度を向上させます。

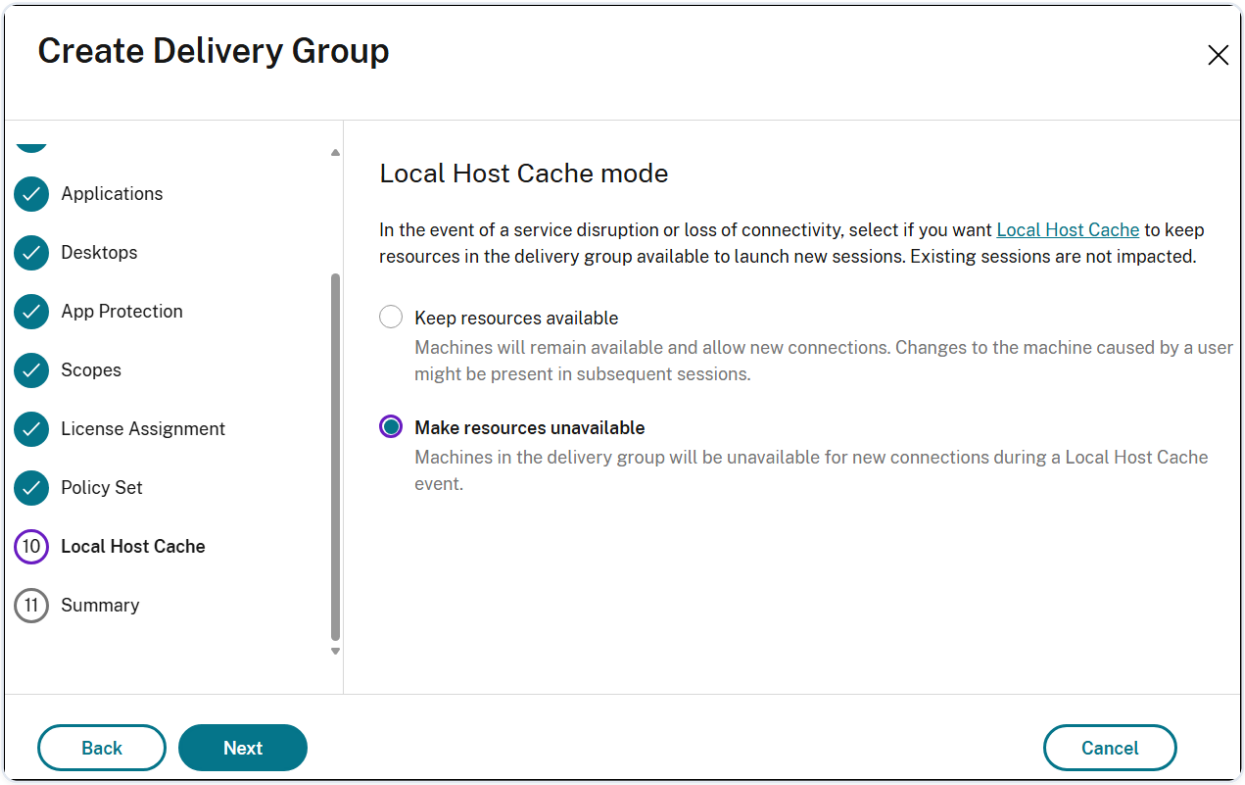
前提条件

- 完全なハイジーン適用にはVDAバージョン2407以降が必要です。レガシーVDA（VDAバージョン2407以前）は、再利用が有効になっている場合にのみ使用できます。これらのVDAは、ハイジーンブロブや強制再起動を受け取りません。
- シングルセッションマシンを含むマシンカタログ。

プールされたデスクトップの1回限りの使用を構成する

1. VDAビルド2407以降を使用して、シングルセッションマシンを含むMCSカタログを作成します。
2. 対応するデリバリーグループを作成します。Remote PowerShell からデリバリーグループの `ReuseMachinesWithoutShutdownInOutage` デスクトップグループ設定を `false` に設定するか、デリバリーグループの作成時に Web Studio の **［ローカルホストキャッシュモード］** ページで **［リソースを使用不可にする］** を選択します。

```
Set-BrokerDesktopGroup -Name "name"
-ReuseMachinesWithoutShutdownInOutage $false
```



3. 構成が完了すると、LHC停止モード中にマシンは1回限りの使用が可能になります。LHC停止モードが解除されると、汚染されたマシンは再起動され、再度使用できるようになります。

> **注:**

> マシンは、最新の電源投入後にユーザーセッションが開始されると、汚染済みとして分類されます。汚染されていないマシンとは、最新の電源投入イベント以降、ユーザーセッションが起動されていないマシンを指します。

概要ページ

デリバリーグループの名前を入力します。オプションで、Citrix WorkspaceアプリとStudioに表示される説明を入力することもできます。

概要情報を確認し、**「完了」**をクリックします。

制限事項

デスクトップをクライアント IP アドレスに割り当てる機能は、非常に限られたクライアントの種類と構成でのみ機能します。クライアント IP アドレスに基づいてアクセスフィルタリングを実行すると、クラウドクライアントにはパブリック IP アドレスが使用されます。

マージグループを使用したカナリアデプロイメントの有効化（プレビュー）

マージグループを使用して、アプリケーションおよびデスクトップリソースのカナリアデプロイメントモデルを実装します。この機能を使用すると、同じリソースの複数のバージョンを公開しながら、エンドユーザーには単一のアイコンとして表示できます。

マージグループを使用すると、特定のユーザーグループを同じリソースの異なる実装バージョンに誘導できます。ユーザーの一部（5%など）を新しいバージョンのテストに指定し、残りのユーザーは安定版を使用させることができます。新しいバージョンで問題が発生した場合でも、ユーザーのエクスペリエンスを中断することなく、簡単に安定版にフェールオーバーできます。この機能は、再列挙や構成変更を必要とせずに、高可用性と災害復旧の両方のシナリオをサポートします。

使用例

アプリケーションの異なるバージョンが利用可能な場合にユーザーエクスペリエンスを合理化するには、マージグループ機能の使用を検討してください。たとえば、Microsoft Word 2016とMicrosoft Word 2019がある場合、2つの別々のアイコンを表示する代わりに、それらを1つのアイコンにグループ化します。マージグループ機能を使用すると、システムは特定のユーザーに対してどのバージョンのアプリケーション（たとえば、Word 2016またはWord 2019）を起動するかを決定できます。

制限事項

マージグループ内のユーザーの優先リソースが一時的に利用できない場合（例：メンテナンスモード）、ブローカーはフォールバックリソースでセッションを起動します。ユーザーが再接続する前に優先リソースが再び利用可能になった場合、ブローカーはフォールバックリソース上の既存のセッションに再接続するのではなく、優先リソース上に新しいセッションを作成します。

影響：ユーザーは各リソースで1つずつ、2つのアクティブなセッションを持つことになりますが、優先リソース上のセッションにのみアクセスできます。フォールバックリソース上の切断されたセッションはアクセスできなくなります。

回避策：管理者はStudioから孤立したセッションをログオフするか、そのセッションをホストしているマシンを再起動できます。

マージグループを構成するコマンド

注:

コマンドの詳細については、SDKドキュメントを参照してください。

アクション	コマンド	説明
マージグループの作成	`New-BrokerMergeGroup`	指定された名前と説明（オプション）でマージグループを作成します。
マージグループの設定	`Set-BrokerMergeGroup`	マージグループの名前、説明、MergeGroupSetUid、およびDefaultResourceUidを設定します。DefaultResourceはマージグループのアイコンリソースです。Citrix Workspaceアプリでは、マージグループはこのリソースのアイコンを継承します。
マージグループの削除	`Remove-BrokerMergeGroup`	指定されたマージグループを削除します。マージグループにマージ済みリソー

アクション	コマンド	説明
		スが含まれている場合、削除は失敗します。そのようなマージグループを削除するには、`Force` パラメーターが必要です。これにより、マージグループとその関連する `MergedResources` の両方がマージグループ内で削除されます。
マージ済みリソースの作成	`New-BrokerMergedResource`	サイトに新しいマージ済みリソースを作成します。applicationUid または EntitlementPolicyRuleUid (共有/ランダムデスクトップグループ) を持つマージ済みリソースを作成します。これは、アプリケーションリソースまたはエンタイトルメントポリシー規則の単なるラッパーでもあります。マージ済みリソースを削除しても、アプリケーションまたはエンタイトルメントポリシー規則は削除されません。
マージ済みリソースの設定	`Set-BrokerMergedResource`	`MergedResource` オブジェクトのプロパティを設定します。Users パラメーターは、マージ済みリソースに関連付けられている以前のユーザーをすべて削除し、新しいリスト (または単一のユーザー) をこのマージ済みリソースのユーザーリストとして設定します。既存のユーザーリストにユーザーを追加したい場

アクション	コマンド	説明
		合は、`AddUsers` パラメーターを使用できます。既存のユーザーリストからユーザーを削除したい場合は、`RemoveUsers` パラメーターを使用できます。
マージ済みリソースの削除	`Remove-BrokerMergedResource`	指定されたマージ済みリソースを削除します。

詳細情報

- デリバリーグループの管理
- アプリケーション

デリバリーグループの管理

注:

バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

はじめに

この記事では、管理コンソールからデリバリーグループを管理する手順について説明します。グループ作成時に指定した設定を変更するだけでなく、デリバリーグループの作成時には利用できないその他の設定も構成できます。

手順のカテゴリには、全般、ユーザー、マシン、セッションがあります。一部のタスクは複数のカテゴリにまたがります。たとえば、「ユーザーがマシンに接続できないようにする」はマシンのカテゴリで説明されていますが、ユーザーにも影響します。あるカテゴリでタスクが見つからない場合は、関連するカテゴリを確認してください。

その他の関連情報については、以下の記事も参照してください。

- 「アプリケーション」(/ja-jp/citrix-virtual-apps-desktops/current-release/manage-deployment/applications-manage.html)には、デリバリーグループ内のアプリケーションの管理に関する情報が含まれています。
- デリバリーグループの管理には、Delivery Group Administratorの組み込みロール権限が必要です。詳細については、「委任管理」(/ja-jp/citrix-virtual-apps-desktops/current-release/manage-deployment/delegated-administration.html)を参照してください。

全般

- グループの詳細を表示(#view-group-details)
- 優先プロパティの変更(#change-preferred-properties)
- 配信タイプの変更(#change-the-delivery-type-of-a-delivery-group)
- StoreFront™アドレスの変更(#change-storefront-addresses)
- 機能レベルの変更(#change-the-functional-level)
- Remote PC Accessデリバリーグループの管理(#manage-remote-pc-access-delivery-groups)
- フォルダーを使用してデリバリーグループを整理する
- アプリ保護の管理
- デリバリーグループのサスペンド機能を変更する

グループの詳細を表示

1. 検索機能を使用して特定のデリバリーグループを見つけます。手順については、インスタンスの検索を参照してください。
2. 検索結果から、必要に応じてグループを選択します。
3. グループの列の説明については、次の表を参照してください。
4. このグループの詳細については、下部の詳細ペインのタブをクリックしてください。

列	説明
デリバリーグループ	グループ名とセッションの種類。セッションの種類には、シングルセッションOSとマルチセッションOSが含まれます。
配信中	このグループから配信されるリソースの種類。可能な値には、アプリケーション、デスクトップ、およびアプリケーションとデスクトップが含まれます。デリバリーグループが専

列	説明
	用マシンで構成されている場合、「静的マシン割り当て」が表示されます。
使用中のセッション	セットアップされているマシンの数と、切断状態にあるマシンの数。
割り当て済み数	デリバリーグループに割り当てられているカタログ内のマシンの数。
フォルダ	**デリバリーグループ**ツリー内でのグループの場所。グループが存在するフォルダーの名前（末尾のバックスラッシュを含む）が表示されます。グループがルートレベルにある場合は `-` が表示されます。

優先プロパティの変更

優先プロパティは、ユーザーがデリバリーグループからリソースにアクセスして起動する方法を制御します。デリバリーグループの優先プロパティを変更するには、次の手順に従います。

1. Studioで、左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**編集**を選択します。
3. **設定**ページで、次の表の設定を変更します。
4. **適用**を選択して変更を適用し、ウィンドウを開いたままにします。または、**OK**を選択して変更を適用し、ウィンドウを閉じます。

設定	説明
説明	Citrix Workspace™（またはStoreFront）が使用し、ユーザーに表示されるテキスト。
デリバリーグループを有効にする	デリバリーグループが有効になっているかどうか。
タイムゾーン	このデリバリーグループのマシンが存在するタイムゾーン。この設定は、新しく作成されたデリバリーグループの場合、**設定 > 日付と時刻**で設

設定	説明	
	定されたタイムゾーンを自動的に表示します。必要に応じて、デリバリーグループのタイムゾーンを変更できます。ドロップダウンメニューには、サイトでサポートされているタイムゾーンが一覧表示されます。 **注：** デリバリーグループのタイムゾーンを変更すると、そのデリバリーグループ内のマシンが再起動する場合があります。これを避けるため、タイムゾーン設定は稼働時間外に変更してください。	
Secure ICA® を有効にする	SecureICA を使用してデリバリーグループ内のマシンとの通信を保護します。SecureICA は ICA プロトコルを暗号化します。デフォルトのレベルは 128 ビットです。このレベルは SDK を使用して変更できます。Citrix® は、パブリックネットワークを通過する際に TLS 暗号化などのより多くの暗号化方法を使用することを推奨しています。また、SecureICA はデータ整合性をチェックしません。	

デリバリーグループのデリバリーの種類を変更する

デリバリーの種類は、グループが提供できるもの（アプリケーション、デスクトップ、またはその両方）を示します。

アプリケーションのみまたは**デスクトップとアプリケーション**のタイプを**デスクトップのみ**のタイプに変更する前に、グループからすべてのアプリケーションを削除してください。

1. 左側のペインで、**［デリバリーグループ］**を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. ページで、目的のデリバリーの種類を選択します。
4. **［適用］をクリックして変更を適用し、ウィンドウを開いたままにします。または、［保存］**をクリックして変更を適用し、ウィンドウを閉じます。

StoreFrontアドレスを変更する

1. 左側のペインで、**［デリバリーグループ］**を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. **［StoreFront］**ページで、StoreFrontのURLを選択または追加します。これらのURLは、デリバリーグループ内の各マシンにインストールされているCitrix Workspace™アプリによって使用されます。
4. **［適用］をクリックして変更を適用し、ウィンドウを開いたままにします。または、［保存］**をクリックして変更を適用し、ウィンドウを閉じます。

左側のペインで**［StoreFront］**を選択して、StoreFrontサーバーアドレスを指定することもできます。

機能レベルを変更する

デリバリーグループ内のマシン上のVDAと、デリバリーグループで使用されるマシンを含むマシンカタログをアップグレードした後、デリバリーグループの機能レベルを変更します。

開始する前に：

- Citrix Provisioning™（旧Provisioning Services）を使用している場合は、Citrix Provisioningコンソールで VDAバージョンをアップグレードします。
- アップグレードされたVDAを含むマシンを起動して、Delivery Controllerに登録できるようにします。このプロセスにより、デリバリーグループで何がアップグレードされる必要があるかがコンソールに通知されます。
- 以前のVDAバージョンを引き続き使用する必要がある場合、新しい製品機能は利用できません。詳しくは、アップグレードのドキュメントを参照してください。

デリバリーグループの機能レベルを変更するには：

1. 左側のペインで、**［デリバリーグループ］**を選択します。
2. グループを選択し、アクションバーの**機能レベルの変更**をクリックします。**機能レベルの変更**アクションは、アップグレードされたVDAが検出された場合にのみ表示されます。

3. **変更**をクリックします。

ディスプレイには、どのマシンが機能レベルに変更できないか、およびその理由が表示されます。その後、変更アクションをキャンセルし、マシンの問題を解決してから、変更アクションを再度実行できます。

変更が完了したら、マシンを以前の状態に戻すことができます。デリバリーグループを選択し、アクションバーで を選択します。

Remote PC Accessデリバリーグループの管理

Remote PC Accessマシンカタログ内のマシンが割り当てられていない場合、そのマシンは一時的にそのカタログに関連付けられたデリバリーグループに割り当てられます。この一時的な割り当てにより、後でマシンをユーザーに割り当てることができます。

デリバリーグループとマシンカタログの関連付けには優先度値があります。優先度は、マシンがシステムに登録されるとき、またはユーザーがマシン割り当てを必要とするときに、マシンに割り当てられるデリバリーグループを決定します。値が小さいほど優先度が高くなります。Remote PC Accessマシンカタログに複数のデリバリーグループ割り当てがある場合、ソフトウェアは最も優先度の高い一致を選択します。この優先度値を設定するには、PowerShell SDKを使用します。

リモートPCアクセス マシンカタログは、最初に作成されたときにデリバリーグループに関連付けられます。後でカタログに追加されたマシンアカウントまたは組織単位は、デリバリーグループに追加できます。この関連付けは、オン/オフを切り替えることができます。

Remote PC Accessマシンカタログとデリバリーグループの関連付けを追加または削除するには：

1. 左側のペインで**デリバリーグループ**を選択します。
2. Remote PC Accessグループを選択します。
3. **詳細**セクションで、**マシンカタログ**タブをクリックし、Remote PC Accessカタログを選択します。
4. 関連付けを追加または復元するには、**デスクトップの追加**をクリックします。関連付けを削除するには、**関連付けの削除**をクリックします。

フォルダーを使用したデリバリーグループの整理

デリバリーグループに簡単にアクセスできるように、フォルダーを作成できます。

> **ヒント:**

> デリバリーグループノードの優先するデフォルトビュー（フォルダービューまたはリストビュー）を設定するには、アクションバーの右上にある**フォルダー**アイコンをクリックします。

必要な役割

デフォルトでは、デリバリーグループフォルダーを作成および管理するには、Cloud Administrator、Full Administrator、またはDelivery Group Administratorの組み込み役割が必要です。必要に応じて、デリバリーグループフォルダーの作成と管理のための役割をカスタマイズできます。詳しくは、「必要な権限」を参照してください。

デリバリーグループフォルダーを作成する

開始する前に、デリバリーグループの整理方法を計画してください。次の点を考慮してください。

- フォルダーは最大5レベルまでネストできます（デフォルトのルートフォルダーを除く）。
- フォルダーには、デリバリーグループとサブフォルダーを含めることができます。
- Web Studioのすべてのノード（**マシンカタログ**、**デリバリーグループ**、**アプリケーション**、**アプリケーショングループ**など）は、バックエンドで同じフォルダーツリーを共有します。フォルダーの名前変更や移動の際に名前の競合を避けるため、異なるノード間で最上位フォルダーに一意の名前を使用してください。

  `New-BrokerAdminFolder` SDKコマンドレットを使用してフォルダーを作成し、それを**デリバリーグループ**ノードの下に表示したい場合は、`Set-BrokerAdminFolderMetadata`コマンドレットを使用して`ContainsDeliveryGroups`メタデータを追加する必要があります。

  例:

  ```
  Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
  ContainsDeliveryGroups -Value true
  ```

デリバリーグループフォルダーを作成するには、次の手順に従います。

1. 左側のペインで**デリバリーグループ**を選択します。
2. フォルダー階層でフォルダーを選択し、**アクション**バーで **Create Folder** を選択します。
3. 新しいフォルダーの名前を入力し、**Done** をクリックします。

> **ヒント:**

> 意図しない場所にフォルダーを作成してしまった場合は、正しい場所にドラッグできます。

デリバリーグループを移動する

デリバリーグループはフォルダー間で移動できます。詳細な手順は次のとおりです。

1. 左側のペインで**デリバリーグループ**を選択します。
2. フォルダーごとにグループを表示します。フォルダー階層の上にある **View all** をオンにすると、すべてのグループを一度に表示することもできます。
3. グループを右クリックし、**Move Delivery Group** を選択します。
4. グループを移動するフォルダーを選択し、**Done** をクリックします。

> **ヒント:**
>
> グループをフォルダーにドラッグできます。

デリバリーグループフォルダーの管理

デリバリーグループフォルダーを削除、名前変更、移動できます。

フォルダーとそのサブフォルダーにデリバリーグループが含まれていない場合にのみ、フォルダーを削除できることに注意してください。

フォルダーを管理するには、次の手順に従います。

1. 左側のペインで**デリバリーグループ**を選択します。
2. フォルダー階層でフォルダーを選択し、必要に応じて**アクション**バーでアクションを選択します。
   - フォルダーの名前を変更するには、**Rename Folder**を選択します。
   - フォルダーを削除するには、**Delete Folder**を選択します。
   - フォルダーを移動するには、**Move Folder**を選択します。
3. 画面の指示に従って、残りの手順を完了してください。

必要な権限

次の表に、デリバリーグループフォルダーに対してアクションを実行するために必要な権限を示します。

アクション	必要な権限
デリバリーグループフォルダーの作成	デリバリーグループフォルダーを作成
デリバリーグループフォルダーを削除	デリバリーグループフォルダーを削除
デリバリーグループフォルダーを移動	デリバリーグループフォルダーを移動
デリバリーグループフォルダーの名前を変更	デリバリーグループフォルダーを編集
デリバリーグループをフォルダーに移動	デリバリーグループフォルダーを編集および デリバリーグループのプロパティを編集

アプリ保護の管理

以下の情報は、`<https://docs.citrix.com/ja-jp/citrix-workspace-app/app-protection.html>` のアプリ保護に関する記事を補足するものです。以下の詳細に注意してください。

- 有効なアプリ保護の資格が必要です。アプリ保護機能を購入するには、Citrix の営業担当者にお問い合わせください。
- アプリ保護には XML 信頼が必要です。XML 信頼を有効にするには、**設定 > XML 信頼を有効にする** に移動します。
- 画面キャプチャ防止について：
  - Windows および macOS では、保護されたコンテンツのウィンドウのみが空白になります。保護されたウィンドウが最小化されていない場合、アプリ保護はアクティブになります。
  - Linux では、キャプチャ全体が空白になります。保護されたウィンドウが最小化されているかどうかにかかわらず、アプリ保護はアクティブになります。

デリバリーグループのアプリ保護方法を選択するには、次の手順に従います。

1. 左側のペインで **デリバリーグループ** を選択します。
2. グループを選択し、アクションバーで**編集**を選択します。
3. ページには、次のオプションが表示されます。

オプション	説明
適用しない	この設定を適用しない場合は、このオプションを選択します。
このデリバリーグループに適用する	**キーロギング対策**および/または**キーキャプチャ対策**オプションを選択します。これらの各設定にカーソルを合わせると、ツールチップに詳細が表示されます。
コンテキストに応じて適用する	この設定を適用するには、**アクセスポリシー設定**ページでアクセスポリシーを構成します。
	1. 左ペインで**アクセスポリシー**をクリックし、**追加**をクリックします。
	1. **ポリシーの追加**ページで、以下を実行します。
	- i. **ポリシー名**を入力し、必要に応じて設定を構成します。
	- ii. **フィルター**フィールドと**値**フィールドに詳細を入力し、**完了**をクリックします。新しいポリシーは**アプリ保護**ページに表示されます。このポリシーに必要な設定を有効にします。
	- iii. 「**保存**」をクリックします。

4. 「**デリバリーグループ**」ページで、「**デリバリーグループ**」を選択し、下部にある「**詳細**」タブをクリックします。適用された新しい「**アプリ保護**」設定が表示されます。

デリバリーグループのサスペンド機能を変更する

デリバリーグループのサスペンド機能を必須またはオプションにする：

- **必須** - デリバリーグループには、サスペンド可能なVMのみを含めることができます。
- **オプション** - デリバリーグループには、サスペンド可能なVMとサスペンド不可能なVMの両方を含めることができます。

始める前に

デリバリーグループ内のすべてのVMがサスペンド可能である場合にのみ、デリバリーグループのサスペンド機能を`Required`に変更できます。

デリバリーグループのサスペンド機能を変更するには：

1. Web Studioから、左ペインの**デリバリーグループ**に移動します。
2. グループを選択し、アクションバーで**中断機能の変更**をクリックします。
3. 「**はい**」をクリックして操作を確定します。

ユーザー

このセクションでは、次のトピックについて説明します。

- ユーザーの追加または削除
- デリバリーグループ内のデスクトップおよびアプリへのユーザーアクセスを制限する
- デリバリーグループ内のリソースへのアクセスを制限する
- すべてのデリバリーグループのリソースへのユーザーアクセスを制限する
- アクセスポリシーのユーザー範囲を構成する

デリバリーグループでのユーザーの追加または削除

ユーザーに関する詳細については、「ユーザー」を参照してください。

1. 左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. **ユーザー**ページで:
    - ユーザーを追加するには、**追加**をクリックし、追加するユーザーを指定します。
    - ユーザーを削除するには、1人以上のユーザーを選択し、**削除**をクリックします。
    - 認証されていないユーザーによるアクセスを許可するには、チェックボックスをオンまたはオフにします。
4. 変更を適用してウィンドウを開いたままにするには、**適用**をクリックします。または、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

ユーザーリストのインポートまたはエクスポート

物理的なシングルセッションOSマシンを含むデリバリーグループの場合、デリバリーグループの作成後に.csvファイルからユーザー情報をインポートできます。ユーザー情報を.csvファイルにエ

クスポートすることもできます。.csvファイルには、以前の製品バージョンのデータを含めることができます。

CSVファイルの最初の行には、コンマで区切られた2つの列ヘッダーが含まれている必要があります。最初のヘッダーが`Machine Account`で、2番目のヘッダーが`User Names`であることを確認してください。（追加のヘッダーを含めることはできますが、サポートされていません。）ファイルの以降の行には、コンマで区切られたデータが含まれます。`Machine Account`エントリは、コンピューターSID、FQDN、またはドメインとコンピューター名のペアにすることができます。

ユーザー情報をインポートまたはエクスポートするには：

1. 左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. **マシン割り当て**ページで、**リストのインポート**または**リストのエクスポート**を選択し、ファイルの場所を参照します。
4. 「**適用**」をクリックして変更を適用し、ウィンドウを開いたままにします。または、「**保存**」をクリックして変更を適用し、ウィンドウを閉じます。

デリバリーグループ内のデスクトップとアプリへのアクセスを制限する

以下のタスクを実行することで、デリバリーグループ内のリソースへのユーザーアクセスを管理できます。

- 特定のユーザーへのデスクトップアクセスを制限する
- 特定のユーザーへのアプリケーションアクセスを制限する

特定のユーザーへのデスクトップアクセスを制限する

以下の*両方*の条件を満たすユーザーは、デリバリーグループ内のデスクトップにアクセスできます。

- このデリバリーグループ内のリソース（アプリとデスクトップ）へのアクセス権を持っている。

  デフォルトでは、アクセスは展開のユーザーアクセスリストによって決定されますが、これはStudioでは構成されません。デフォルトのユーザー範囲からユーザーを追加または削除できます。デリバリーグループでユーザーを追加または削除するを参照してください。
- このグループ内のデスクトップへのアクセス権を持っている。

  詳細については、デスクトップ（またはデスクトップ割り当てルール）を参照してください。

特定のユーザーへのデスクトップへのアクセスを制限するには、「デリバリーグループの作成および編集時のデスクトップ使用の制限」を参照してください。

特定のユーザーへのアプリケーションアクセスを制限する

以下の すべての条件を満たすユーザーは、デリバリーグループ内のアプリケーションにアクセスできます。

- このデリバリーグループ内のリソース（アプリとデスクトップ）へのアクセス権を持っている。

  デフォルトでは、アクセスは展開のユーザーアクセスリストによって決定されますが、これはStudioでは構成されません。デフォルトのユーザー範囲からユーザーを追加または削除できます。デリバリーグループでユーザーを追加または削除するを参照してください。
- このグループ内のアプリケーションにアクセスできます。

  デフォルトでは、アプリケーションエンタイトルメントポリシー規則にはすべてのユーザーが含まれます。詳細については、PowerShell SDK `BrokerAppEntitlementPolicyRule` コマンドレットを参照してください。必要に応じて、このセクションで説明されている手順を使用して、デリバリーグループ内のアプリケーションへのユーザーアクセスを制限できます。
- このアプリケーションを含むアプリケーショングループにアクセスできます。

デリバリーグループレベルで特定のユーザーへのアプリケーションアクセスを制限するには、次の手順に従います。

1. Studioで、左ペインの を選択します。
2. デリバリーグループを選択し、アクションバーの を選択します。
3. アプリケーションアクセスを制限するには、次の手順に従います。

   a. 左ペインで、 をクリックします。

   b. 特定のユーザーがアプリケーションにアクセスできるようにするには、 を選択し、 領域で をクリックして、含めるユーザーまたはユーザーグループを指定します。

   c. 特定のユーザーがアプリケーションにアクセスできないようにするには、 領域で をクリックして、除外するユーザーまたはユーザーグループを指定します。

> **注:**

- を選択し、許可リストとブロックリストの両方を空のままにした場合、このグループのアプリケーションはどのユーザーも使用できません。
- を選択し、許可リストを空のままにした場合、 のユーザーを除くすべてのユーザーがアプリケーションを使用できます。

デリバリーグループ内のリソースへのアクセスを制限する

デリバリーグループ内のリソースへのユーザーアクセスを制限するために行った変更は、使用する方法に関係なく、以前の設定よりも優先されます。次のことができます。

- **委任管理スコープを使用した管理者アクセスの制限：** 管理者がすべてのアプリケーションにアクセスできるスコープと、特定のアプリケーションにのみアクセスできる別のスコープを作成して割り当てることができます。詳しくは、「委任管理」を参照してください。
- **スマートアクセス ポリシー式を使用してユーザーアクセスを制限する：**アクセス ポリシー規則を構成して、特定のデリバリーグループへのユーザーアクセスを制御できます。例を次に示します。
  - ユーザーのサブセットへのアクセスを制限し、許可されたユーザーデバイスを指定します。
  - Workspace（StoreFrontではなく）を介して接続しているユーザーへのアクセスを制限する。
  - 特定のWorkspace URLを介して接続しているユーザーへのアクセスを制限する。

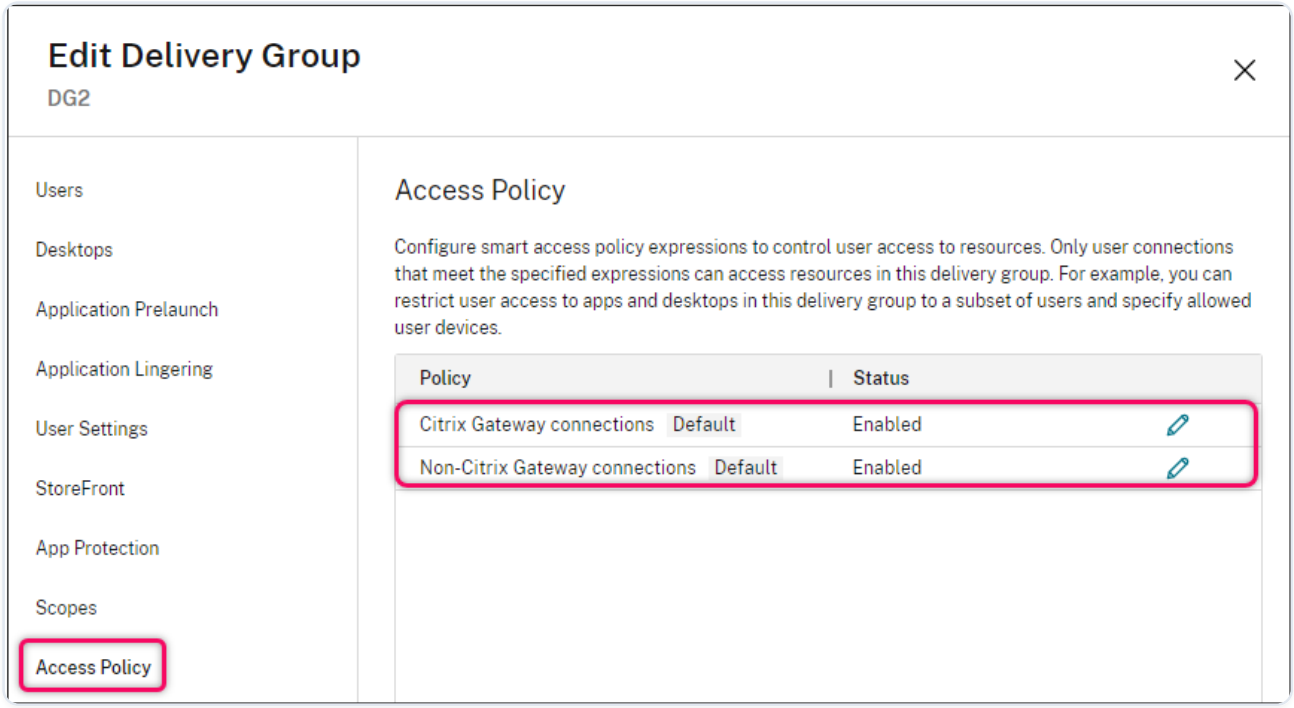
このセクションでは、アクセスポリシー規則を使用してデリバリーグループへのユーザーアクセスを制限する方法について説明します。

- アクセスポリシー規則について
- アクセスポリシー規則の追加
- Web Studioを使用したアクセスポリシー規則の管理
- PowerShellを使用したポリシー規則の追加と調整

アクセスポリシー規則について

デリバリーグループに対して複数のアクセスポリシー規則を構成できます。デリバリーグループ内のアプリとデスクトップは、ユーザーの接続がデリバリーグループに対して定義したアクセスポリシー規則のいずれかに一致する場合、順序に関係なく、ユーザーのStoreFrontまたはWorkspaceに表示されます。

各規則は個別に有効または無効にできます。無効な規則は、アクセスポリシーが評価されるときに無視されます。



Web Studioでは、アクセス ポリシー リストに次のデフォルトのSmartAccessポリシー規則が含まれています。必要に応じて、さらに追加できます。

- **Citrix Gateway接続。** このポリシーでは、Citrix Gatewayを介して行われたユーザー接続のみがデリバリーグループ内のリソースにアクセスできます。デバイスポスチャまたはネットワークロケーション機能が有効になっている場合にWorkspaceを介して行われたユーザー接続も、Citrix Gatewayを介した接続と見なされます。
- **Citrix Gateway以外の接続。** このポリシーでは、Citrix Gateway を介さずに行われたユーザー接続のみがデリバリーグループ内のリソースにアクセスできます。

注:

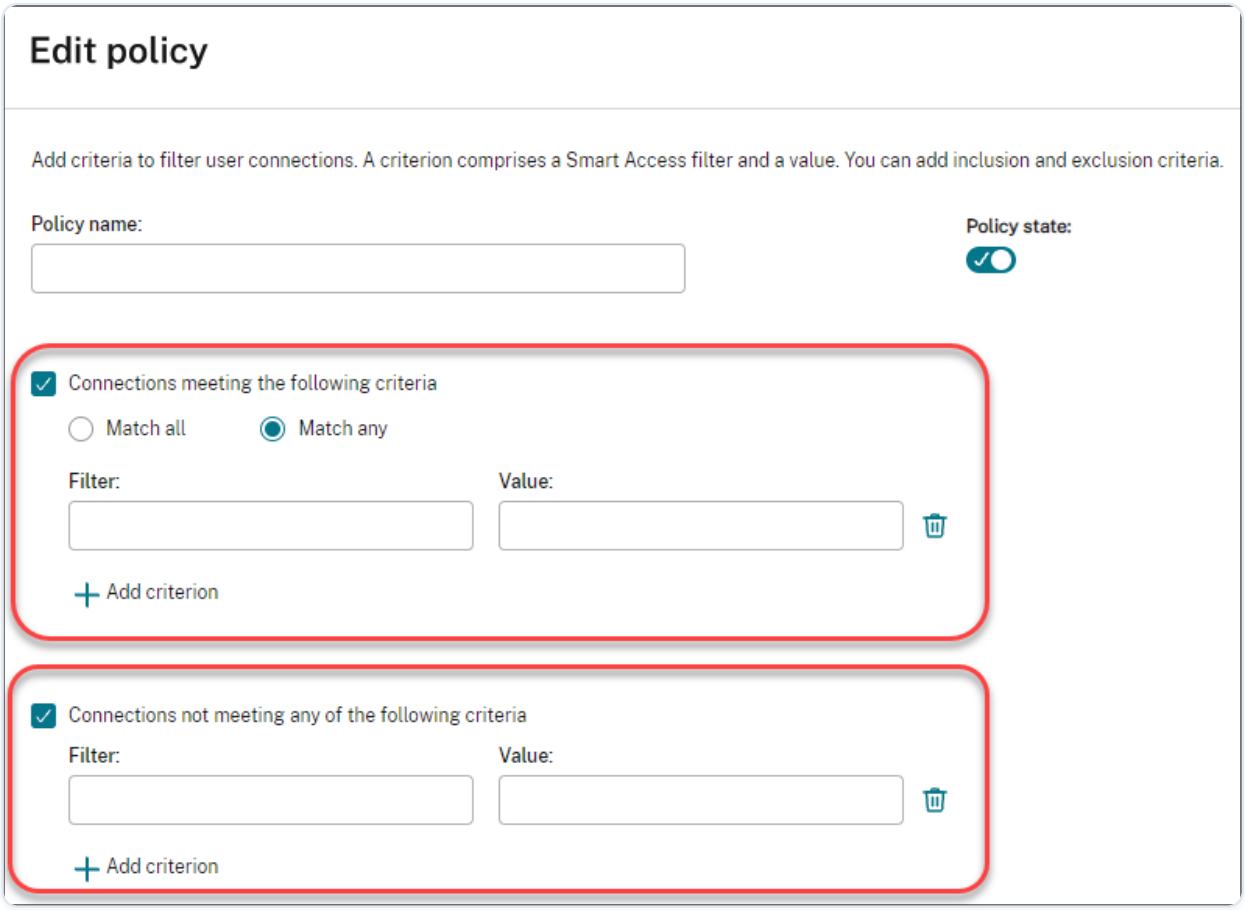
- デフォルトのルールが新しく構成されたルールを上書きしないようにするには、デフォルトのルールを無効にするか、新しいポリシーで使用されているフィルターを除外するようにルールを調整する必要があります。
- デフォルトのポリシーは削除できませんが、無効にすることはできます。ポリシーを無効にするには、**編集**アイコンをクリックし、**ポリシーの状態**を**無効**に変更します。
- ポリシーリストには、PowerShellコマンドを使用して追加された規則も表示されます。これらのポリシーは削除できますが、Web Studioで編集することはできません。

Web Studioを使用したアクセスポリシー規則の追加

アクセスポリシー規則は、一連のフィルターで構成されます。フィルターの詳細については、この記事を参照してください。アクセスポリシー規則を追加するときは、必要に応じて複数の条件フィルターを規則に追加します。

Web Studioを使用してデリバリーグループのポリシーを追加するには、次の手順に従います。

1. コンソールで、左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. **アクセスポリシー**ページで、**追加**をクリックします。**ポリシーの追加**ページが表示されます。



4. **ポリシー名**フィールドに、ポリシーのわかりやすい名前を入力します。名前は展開内で一意である必要があります。
5. 許可されるユーザー接続の基準を定義するには、次の手順に従います。

   a. 「**次の条件を満たす接続**」を選択します。

   b. 「**条件の追加**」をクリックします。

   c. 「**フィルター**」フィールドに、使用するフィルターの名前を入力します。「**値**」フィールドに、フィルターの目的の値を入力します。たとえば、Workspace (StoreFront ではなく) を介して接続されたユーザーのみがこのデリバリーグループのリソースにアクセスできる

ようにするには、「**フィルター**」に `Citrix-Via-Workspace`、「**値**」に `True` と入力します。

d. さらに条件を追加するには、手順 b〜c を繰り返します。

e. 条件間の関係を選択します:

- **いずれかに一致**。受信ユーザー接続が構成されたフィルター条件のいずれかを満たす場合にのみアクセスを許可します。
- **すべてに一致**。受信ユーザー接続が構成されたフィルター条件のすべてを満たす場合にのみアクセスを許可します。

6. 禁止されているユーザー接続の条件を定義するには、次の手順に従います:

a. 「**次の条件のいずれも満たさない接続**」を選択します。

b. 「**条件の追加**」をクリックします。

c. **フィルター**フィールドに、使用するフィルターの名前を入力します。**値**フィールドに、フィルターの目的の値を入力します。たとえば、`example.cloud.com` Workspace URL を介して接続しているユーザーがこのデリバリーグループのリソースにアクセスするのを禁止する場合などです。**フィルター**には`Citrix.Workspace.UsingDomain`を、**値**には`example.cloud.com`を入力します。

d. さらに条件を追加するには、手順 b〜c を繰り返します。

> **注:**
>
> 構成された条件のいずれかを満たすユーザー接続は、このデリバリーグループのリソースへのアクセスを禁止されます。

7. 「**完了**」をクリックします。

新しいポリシーがポリシーリストに表示されます。

8. この新しいポリシーでカバーされる接続との意図しない重複を避けるために、デフォルトのポリシー規則を確認し、調整してください。既存のポリシーを調整するには、以下の方法を使用します。

- デフォルトのポリシー規則を無効にします。
- 新しいポリシーの包含条件に追加したSmartAccessフィルターを除外するように、デフォルトのポリシー規則を構成します。詳しくは、「Web Studio を使用したポリシー規則の管

理」および「PowerShell を使用したアクセスポリシー規則の追加と管理」を参照してください。

> **重要:**
>
> アクセスポリシー規則についてで説明されているように、ユーザーの接続がデリバリーグループ内の1つ以上のポリシー規則に一致すると、ユーザーはそのリソースにアクセスできるようになります。したがって、規則を作成した後、新しい規則でカバーされる接続との意図しない重複を避けるために、既存の規則を慎重に確認し、調整する必要があります。

Web Studio を使用したアクセスポリシー規則の管理

包含条件と除外条件を使用して、デフォルトのポリシーを調整できます。たとえば、それらの接続のサブセットへのアクセスを制限するには、次の手順に従います。

1. デフォルトのポリシーを編集します。
2. **次のいずれかの条件を満たす接続**を選択します。
3. 許可されたユーザーアクセスシナリオのSmartAccessポリシー式を追加、編集、または削除します。

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

PowerShellを使用したアクセスポリシー規則の追加と管理

デリバリーグループのアクセスポリシー規則を追加および管理するには、次のPowerShellコマンドレットを使用できます。

- New-BrokerAccessPolicyRule
- Get-BrokerAccessPolicyRule
- Set-BrokerAccessPolicyRule
- BrokerAccessPolicyRule の名前を変更する
- BrokerAccessPolicyRule を削除する

詳細については、Citrix Developer Documentationの関連記事を参照してください。

すべてのデリバリーグループにわたるリソースへのユーザーアクセスを制限する

すべてのデリバリーグループにわたるアプリケーションおよびデスクトップへのユーザーアクセスを制御するために、リソースフィルタリングルールを構成できます。これらのルールにより、リ

ソースタイプを指定し、タグベースの制限を適用し、ネットワークロケーションやストア接続コンテキストなどの要因に基づいてアクセス条件を強制できます。

必要な権限

このタスクを実行するには、**リソースフィルターの管理**権限を持つ管理者ロールである必要があります。

リソースフィルタリングルールを追加する

リソースフィルタリングルールを追加するには、次の手順を実行します。

1. **デリバリーグループ > 設定**に移動します。
2. **リソースフィルター**タイルで**管理**を選択します。
3. **リソースフィルターの管理ルール**ダイアログボックスで、**追加**をクリックします。
4. ルールに**名前**と**説明**を入力します。
5. ルールが適用されるリソースの種類を選択します:
   - **アプリケーション**
   - **デスクトップ**
   - **両方**
6. ルールが適用されるリソースを識別するタグを選択します。

> **注:**
>
> リソースの種類として**両方**を選択した場合、タグの選択は必須です。

7. リソースがフィルタリングされる条件を定義するために、**Smart Access filter**を構成します。
8. ルールを保存するには、**追加**をクリックします。

アクセス ポリシーのユーザー スコープを構成する

デリバリー グループ内のすべてのアクセス ポリシーは、デフォルトで同じユーザー セットに適用されます。Studio、PowerShell、またはRest APIを使用して、特定のユーザーに適用されるようにアクセス ポリシーを構成できます。

Studioを使用して指定したユーザーにアクセス ポリシーを適用するには、次の手順に従います:

1. Studioで、左側のペインで**デリバリー グループ**を選択します。

2. グループを選択し、アクション バーで**デリバリー グループの編集**を選択します。
3. **ユーザー**ページで、**コンテキスト アクセスを使用**を選択します。
4. 設定したいアクセスポリシーを選択し、**ユーザーアクセススコープ**をクリックします。**ユーザーアクセススコープ**ページが表示されます。
5. このポリシーを適用する認証済みユーザーを定義するには：
   - このポリシーを*任意*の認証済みユーザーに適用するには、**任意の認証済みユーザーがリソースを使用することを許可する**を選択します。
   - このポリシーを特定のユーザーに適用するには、**リソースの使用を制限する**が選択されたままにします。その後、許可リストとブロックリストを使用して、このポリシーのユーザーを追加または削除します。
6. 資格情報を提供しないユーザーにこのアクセスポリシーを適用するには、**認証されていない（匿名）ユーザーへのアクセスを許可する。資格情報は不要**を選択します。

マシン

- マシンのユーザー割り当てを管理する
- マシンからユーザーへの割り当てを変更する
- 電源管理されたシングルセッションのプールされたVDAでローカルホストキャッシュを有効にする
- ユーザーあたりの最大マシン数を変更する
- マシンを更新する
- デスクトップのタグ制限を追加、変更、または削除する
- マシンを削除する
- ユーザーがマシンに接続するのを防ぐ（メンテナンスモード）
- マシンをシャットダウンして再起動する
- マシンの再起動スケジュールを作成および管理する
- 1回限りの再起動スケジュールを有効にする
- マシンの電源管理

マシンに対するユーザー割り当ての管理

デリバリーグループ内のマシンのユーザー割り当てを管理します。デスクトップ割り当て規則がデリバリーグループに構成されている場合、マシンは最初のデスクトップ起動時にユーザーにランダムに割り当てられ、ユーザー割り当てが変更されない限り、ユーザーに割り当てられたままに

なります。割り当てられていないマシンを特定のユーザーに手動で割り当てたり、マシンの既存のユーザー割り当てを変更したりする場合は、このトピックで説明されている手順に従って変更します。これらの手順を使用すると、ユーザーに割り当てられたマシンのCitrix Workspaceアプリに表示される名前を変更することもできます。

詳細な手順は次のとおりです。

1. Studioから、左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**編集**を選択します。
3. 左側のペインで、**マシン割り当て**を選択します。グループ内の各マシンの以下の詳細が表示されます。
   - **マシン名:** マシンの名前が表示されます。
   - **表示名:** Citrix Workspaceアプリでのマシンの表示名が表示されます。
   - **ユーザー:** このマシンに割り当てられているユーザーが表示されます。デスクトップ割り当てルールが構成されている場合、マシンは最初のデスクトップ起動時にユーザーにランダムに割り当てられ、ユーザー割り当てが変更されない限り、ユーザーに割り当てられたままになります。
4. マシンを見つけ、ユーザーを割り当てるか、そのユーザー割り当てを変更します。
   - ユーザーを参照するには、**参照**をクリックします。
   - 「**ユーザー**」列に、セミコロンで区切られたユーザー名のリストを入力します。
   - をクリックして、CSVファイルを使用して設定の詳細をインポートします。
   - **変更**をクリックして、マシンのデスクトップアイコンを更新します。ローカルマシンまたはVDAマシンから`.ico`または`.exe`ファイルを選択して参照します。指定されたアイコンは、マシンレベルでのみデフォルトのアイコンセットを上書きします。
5. (オプション) マシンがユーザーに割り当てられている場合は、必要に応じて表示名を変更します。

> **注:**
>
> 表示名フィールドは、マシンがユーザーに割り当てられている場合にのみ有効になります。

- デスクトップ割り当てルールに基づいてマシンがユーザーに割り当てられている場合、このフィールドにはそのルールで構成された表示名が表示されます。
- マシンがユーザーに手動で割り当てられており、フィールドが空白のままの場合、デリバリーグループの公開名（指定されている場合）がマシンの表示名として使用されます。公開名が指定されていない場合は、デリバリーグループの名前が使用されます。デリバリーグループの公開名はPowerShellでのみ指定できることに注意してください。

6. 変更を適用してウィンドウを開いたままにするには、 を選択します。または、変更を適用してウィンドウを閉じるには、 を選択します。

デリバリーグループ内のマシンからユーザーへの割り当てを変更する

MCSでプロビジョニングされたシングルセッションOSマシンの割り当てを変更できます。マルチセッションOSマシンまたはCitrix Provisioningでプロビジョニングされたマシンの割り当ては変更できません。

1. 左側のペインで「**デリバリーグループ**」を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. **デスクトップ**または**デスクトップ割り当てルール**ページ（ページタイトルはデリバリーグループが使用するマシンカタログの種類によって異なります）で、新しいユーザーを指定します。
4. 「**適用**」をクリックして変更を適用し、ウィンドウを開いたままにします。または、「**保存**」をクリックして変更を適用し、ウィンドウを閉じます。

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

デフォルトでは、電源管理されたシングルセッションのプールされたマシンは、ローカルホストキャッシュモードでは使用できません。デリバリーグループごとにデフォルトの動作を上書きできます。詳細な手順は次のとおりです。

1. Studioで、左側のペインで**デリバリーグループ**を選択します。

   グループリストでは、MCSまたはCitrix Provisioningによってプロビジョニングされたシングルセッションのプールされたマシンを含むグループに警告アイコンが表示されます。
2. 必要に応じてグループを選択し、アクションバーの を選択します。
3. **ローカルホストキャッシュ**ページで、**リソースを常に利用可能にする**を選択します。

4. **適用**を選択して変更を適用し、ウィンドウを開いたままにします。または、**OK**を選択して変更を適用し、ウィンドウを閉じます。

または、PowerShellコマンドを使用してデフォルトの動作を上書きすることもできます。詳しくは、「アプリケーションとデスクトップのサポート」を参照してください。

> **重要:**

> 電源管理されたシングルセッションのプールされたマシンへのアクセスを有効にすると、以前のユーザーセッションからのデータと変更が後続のセッションに存在する可能性があります。

デリバリーグループ内のユーザーあたりの最大マシン数を変更する

1. 左側のペインで「**デリバリーグループ**」を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. **デスクトップ割り当てルール**ページで、ユーザーあたりの最大デスクトップ数を設定します。
4. 変更を適用してウィンドウを開いたままにするには、**適用**をクリックします。または、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

デリバリーグループ内のマシンを更新する

1. 左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**マシンの表示**をクリックします。
3. マシンを選択し、アクションバーで**マシンの更新**をクリックします。

別のイメージを選択するには、**「イメージ」**を選択し、スナップショットを選択します。

変更を適用してマシンユーザーに通知するには、**「エンドユーザーへのロールアウト通知」**を選択します。次に、以下を指定します。

- マスターイメージを更新するタイミング: 今すぐ、または次回の再起動時
- 再起動の配布時間（グループ内のすべてのマシンの更新を開始するまでの合計時間）
- ユーザーに再起動が通知されるかどうか
- ユーザーが受信するメッセージ

デスクトップのタグ制限を追加、変更、または削除する

タグ制限の追加、変更、削除は、起動対象となるデスクトップに予期せぬ影響を与える可能性があります。「タグ」の考慮事項と注意点を確認してください。

1. 左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. **デスクトップ**ページで、デスクトップを選択し、**編集**をクリックします。
4. タグ制限を追加するには、**タグを持つマシンへの起動を制限する**を選択し、タグを選択します。
5. タグ制限を変更または削除するには、次のいずれかを実行します。
   - 別のタグを選択します。
   - **このタグを持つマシンへの起動を制限する**のチェックを外して、タグ制限を削除します。
6. 変更を適用してウィンドウを開いたままにするには、**適用**をクリックします。または、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

デリバリーグループからマシンを削除する

マシンを削除すると、デリバリーグループから削除されます。デリバリーグループが使用するマシンカタログからは削除されません。したがって、そのマシンは別のデリバリーグループに割り当てることができます。

マシンは、削除する前にシャットダウンする必要があります。削除中にユーザーがマシンに接続するのを一時的に停止するには、シャットダウンする前にマシンをメンテナンスモードにします。

マシンには個人データが含まれている可能性があるため、別のユーザーにマシンを割り当てる前に注意してください。マシンの再イメージングを検討してください。

1. 左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**マシンの表示**をクリックします。
3. マシンがシャットダウンされていることを確認します。
4. マシンを選択し、アクションバーで**デリバリーグループから削除**をクリックします。

マシンが使用する接続を介して、デリバリーグループからマシンを削除することもできます。

デリバリーグループ内のマシンへのユーザー接続を防止する（メンテナンスモード）

マシンへの新しい接続を一時的に停止する必要がある場合は、デリバリーグループ内の1台またはすべてのマシンでメンテナンスモードをオンにできます。これは、パッチを適用したり、管理ツールを使用したりする前に行うことがあります。

- マルチセッションOSマシンがメンテナンスモードの場合、ユーザーは既存のセッションに接続できますが、新しいセッションを開始することはできません。
- シングルセッションOSマシン（またはリモートPCアクセスを使用するPC）がメンテナンスモードの場合、ユーザーは接続または再接続できません。現在の接続は、切断またはログオフするまで接続されたままになります。

メンテナンスモードをオンまたはオフにするには：

1. 左ペインで****を選択します。
2. グループを選択します。
3. デリバリーグループ内のすべてのマシンでメンテナンスモードをオンにするには、アクションバーの****をクリックします。

   1台のマシンでメンテナンスモードをオンにするには、アクションバーの**をクリックします。**マシンを選択し、アクションバーの**をクリックします。
4. デリバリーグループ内の1台またはすべてのマシンでメンテナンスモードをオフにするには、上記の手順に従い、アクションバーの****をクリックします。

Windowsリモートデスクトップ接続（RDC）の設定も、マルチセッションOSマシンがメンテナンスモードであるかどうかに影響します。メンテナンスモードは、次のいずれかが発生した場合にオンになります。

- 前述のとおり、メンテナンスモードがオンに設定されています。
- RDCが**このコンピューターへの接続を許可しない**に設定されています。
- RDCが****に設定されていません。設定は、または**のいずれかです。

以下のメンテナンスモードをオンまたはオフにすることもできます。

- 接続。その接続を使用しているマシンに影響します。
- マシンカタログ。そのカタログ内のマシンに影響します。

デリバリーグループ内のマシンをシャットダウンして再起動する

この手順は、Remote PC Accessマシンではサポートされていません。

1. 左ペインで****を選択します。
2. グループを選択し、アクションバーで**マシン表示**をクリックします。
3. マシンを選択し、アクションバーで次のいずれかのエントリをクリックします。

   - **強制シャットダウン：** マシンの電源を強制的にオフにし、マシンリストを更新します。
   - **再起動：** オペレーティングシステムにシャットダウンを要求し、その後マシンを再起動します。オペレーティングシステムがこれに応じられない場合、マシンは現在の状態のままになります。
   - **強制再起動：** オペレーティングシステムを強制的にシャットダウンし、その後マシンを再起動します。
   - **一時停止:** マシンをシャットダウンせずに一時停止し、マシンの一覧を更新します。
   - **シャットダウン:** オペレーティングシステムにシャットダウンを要求します。

強制ではないアクションの場合、マシンが10分以内にシャットダウンしないと、電源がオフになります。シャットダウン中にWindowsが更新プログラムのインストールを試みると、更新が完了する前にマシンの電源がオフになるリスクがあります。

Citrixでは、シングルセッションOSマシンのユーザーがセッション内で**シャットダウン**を選択できないようにすることをお勧めします。詳細については、Microsoftのポリシーに関するドキュメントを参照してください。

接続でマシンをシャットダウンおよび再起動することもできます。

デリバリーグループ内のマシンの再起動スケジュールを作成および管理する

> **注:**
>
> - Autoscale™が有効なデリバリーグループに再起動スケジュールが適用されると、そのマシンは電源がオフになり、Autoscaleが電源をオンにするまでそのままになります。
> - ランダムなシングルセッションマシンに再起動スケジュールが適用されると、コストを節約するために、それらのマシンは再起動されるのではなく電源がオフになります。マシンの電源をオンにするには、Autoscaleを使用することをお勧めします。
> - デリバリーグループのタイムゾーンを変更すると、そのデリバリーグループ内のマシンが再起動される可能性があります。これを避けるには、稼働時間外にタイムゾーン設定を変更するようにしてください。

再起動スケジュールは、デリバリーグループ内のマシンが定期的に再起動されるタイミングを指定します。デリバリーグループに対して1つ以上のスケジュールを作成できます。スケジュールは、次のいずれかに影響します。

- グループ内のすべてのマシン。
- グループ内の1つまたは複数（ただしすべてではない）のマシン。マシンは、マシンに適用するタグによって識別されます。これはタグ制限と呼ばれます。タグがアクションをそのタグを持つアイテムのみに制限するためです。

たとえば、すべてのマシンが1つのデリバリーグループにあるとします。すべてのマシンを週に1回再起動し、経理チームが使用するマシンを毎日再起動したいとします。これを実現するには、すべてのマシンに対して1つのスケジュールを設定し、経理のマシンのみに対して別のスケジュールを設定します。

スケジュールには、再起動が開始される曜日と時刻、および期間が含まれます。

スケジュールを有効または無効にできます。スケジュールを無効にすることは、テスト中、特別な期間中、またはスケジュールが必要になる前に準備する際に役立ちます。

管理コンソールから自動電源オンまたはシャットダウンにスケジュールを使用することはできません。再起動のみに使用できます。

スケジュールの重複

複数のスケジュールが重複する可能性があります。上記の例では、両方のスケジュールが経理部門の仮想マシンに影響を与えます。これらのマシンは日曜日に2回再起動される可能性があります。スケジューリングコードは、意図したよりも頻繁に同じマシンを再起動しないように設計されていますが、保証はできません。

- スケジュールの開始時刻と期間が正確に一致する場合、マシンが再起動されるのは1回だけである可能性が高くなります。
- スケジュールの開始時刻と期間が異なるほど、複数回の再起動が発生する可能性が高くなります。
- スケジュールによって影響を受けるマシンの数も、重複の可能性に影響します。この例では、すべてのマシンに影響する週次スケジュールは、それぞれに指定された期間に応じて、経理部門の仮想マシンに対する日次スケジュールよりも早く再起動を開始する可能性があります。

再起動スケジュールの詳細については、「再起動スケジュールの内部」を参照してください。

再起動スケジュールの表示

1. 左側のペインで**デリバリーグループ**を選択します。

2. グループを選択し、アクションバーで をクリックします。
3. **Restart Schedule**ページを選択します。

Restart Scheduleページには、構成された各スケジュールについて次の情報が含まれています。

- スケジュール名
- 使用されているタグ制限（ある場合）
- マシンの再起動が実行される頻度
- マシンユーザーが通知を受け取るかどうか
- スケジュールが有効になっているかどうか

タグの追加（適用）

タグ制限を使用する再起動スケジュールを構成する場合は、スケジュールが影響するマシンにタグが追加されていることを確認してください。上記の例では、経理チームが使用する各マシンにタグが適用されています。詳細については、「タグ」を参照してください。

1台のマシンに複数のタグを適用できますが、再起動スケジュールで指定できるタグは1つだけです。

1. 左側のペインで**デリバリーグループ**を選択します。
2. スケジュールによって制御されるマシンを含むグループを選択します。
3. 「**マシンの表示**」をクリックし、タグを追加するマシンを選択します。
4. アクションバーで「**タグの管理**」をクリックします。
5. タグが存在する場合は、タグ名の横にあるチェックボックスをオンにします。タグが存在しない場合は、 をクリックし、タグの名前を指定します。タグが作成されたら、新しく作成されたタグ名の横にあるチェックボックスをオンにします。
6. 「**タグの管理**」ダイアログで「**保存**」をクリックします。

再起動スケジュールの作成

> **注:**
>
> 再起動スケジュールは、電源管理されているすべてのマルチセッションマシンと、電源管理されていないマルチセッションマシンに適用できます。

1. 左側のペインで「**デリバリーグループ**」を選択します。

2. グループを選択し、アクションバーで をクリックします。
3. 「**再起動スケジュール**」ページで、「**追加**」をクリックします。
4. 「**再起動スケジュールの追加**」ページで、次のようにします。

   - スケジュールを有効にするには、「**はい**」を選択します。スケジュールを無効にするには、「**いいえ**」を選択します。
   - スケジュール名と説明を入力します。
   - 「**タグに制限**」で、タグの制限を適用します。
   - 「**メンテナンスモードのマシンを含める**」で、メンテナンスモードのマシンをこのスケジュールに含めるかどうかを選択します。代わりにPowerShellを使用するには、「メンテナンスモードのマシンのスケジュールされた再起動」を参照してください。
   - 「**再起動頻度**」で、再起動の発生頻度（毎日、毎週、毎月、または1回）を選択します。「**毎週**」または「**毎月**」を選択した場合は、1つ以上の特定の日を指定できます。
   - 「**繰り返し間隔**」で、スケジュールを実行する頻度を指定します。
   - 「**開始日**」で、スケジュールの初回実行の開始日を指定します。
   - 「**再起動開始時刻**」で、再起動を開始する時刻を24時間形式で指定します。

     - 「**再起動期間**」について：
     - 応答しないセッションを持つマシンを強制的に再起動するには、「**強制再起動**」を選択し、次のいずれかのオプションを選択します。

       - **すべてのマシンを一度に再起動**
       - **すべてのマシンを一定期間内に再起動**し、時間を「**時間**」または「**分**」で指定します。

     - 再起動する前にすべてのセッションがドレインされるのを待つには、「**グレースフル再起動**」を選択します。

       グレースフル再起動を使用するように構成された再起動スケジュールを開始すると:

       - デリバリーグループに属するすべてのアイドル状態のマシンは、すぐに再起動されます。
       - 1つ以上の有効なセッションを持つデリバリーグループに属する各マシンは、すべてのセッションがログオフされたときに再起動されます。

     > **注:**

> グレースフル再起動スケジュールは、電源管理されたマシンのみを再起動できます。

- で、再起動が開始される前に、該当するマシンに通知メッセージを表示するかどうかを決定します。デフォルトでは、メッセージは表示されません。
- 再起動が開始される15分前にメッセージを表示することを選択した場合、最初のメッセージの後に5分ごとにメッセージを繰り返すことができます。デフォルトでは、メッセージは繰り返されません。
- 通知のタイトルとテキストを入力します。デフォルトのテキストはありません。

  メッセージに再起動までのカウントダウンを含める場合は、変数 **%m%** を含めます。すべてのマシンを同時に再起動することを選択しない限り、メッセージは再起動前の適切なタイミングで各マシンに表示されます。

5. をクリックして変更を適用し、 ウィンドウを閉じます。
6. 「**適用**」をクリックして変更を適用し、ウィンドウを開いたままにします。または、「**保存**」をクリックして変更を適用し、ウィンドウを閉じます。

ドレイン後の再起動

PowerShell を使用してマシンの再起動スケジュールを作成または更新する場合 (`New-BrokerRebootSchedulev2` または `Set-BrokerRebootSchedulev2`)、別の再起動期間値を使用できます。

`-UseNaturalReboot <Boolean>` パラメーターでドレイン後の再起動機能を有効にすると、すべてのセッションがドレインされた後にすべてのマシンが再起動されます。再起動時刻になると、マシンはドレイン状態になり、すべてのセッションがログオフされると再起動されます。

この機能は、シングルセッションまたはマルチセッションマシンを含むデリバリーグループでサポートされています。このオプションは、電源管理されているマシンと電源管理されていないマシンの両方で使用できます。

オンプレミス環境では、この機能は PowerShell を使用する場合にのみサポートされます。この機能は Web Studio では利用できません。

再起動スケジュールの編集、削除、有効化、または無効化

1. 左側のペインで を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. 「**再起動スケジュール**」ページで、スケジュールのチェックボックスを選択します。

- スケジュールを編集するには、 をクリックします。再起動スケジュールの作成 のガイダンスに従って、スケジュール構成を更新します。
- スケジュールを有効または無効にするには、**編集**をクリックします。**再起動スケジュールを有効にする**チェックボックスをオンまたはオフにします。
- スケジュールを削除するには、 をクリックします。削除を確認します。スケジュールを削除しても、影響を受けるマシンに適用されているタグには影響しません。

データベース障害により遅延したスケジュールされた再起動

> **注:**
>
> この機能はPowerShellでのみ利用可能です。

> デリバリーグループ内のマシン (VDA) のスケジュールされた再起動が開始される前にサイトデータベースの停止が発生した場合、停止が終了すると再起動が開始されます。これにより、予期しない結果が生じる可能性があります。

たとえば、デリバリーグループの再起動を非稼働時間中 (03:00 から) に発生するようにスケジュールしたとします。スケジュールされた再起動が開始される1時間前 (02:00) にサイトデータベースの停止が発生しました。停止は6時間 (08:00 まで) 続きました。Delivery Controller とサイトデータベース間の接続が復元されると、再起動スケジュールが開始されます。VDA の再起動は元のスケジュールから5時間後に開始され、稼働時間中に VDA が再起動されることになります。

この状況を回避するために、`New-BrokerRebootScheduleV2`および`Set-BrokerRebootScheduleV2`コマンドレットで`MaxOvertimeStartMins`パラメーターを使用できます。この値は、再起動スケジュールが開始できる、スケジュールされた開始時刻を超える最大分数を示します。

- その時間内 (スケジュールされた時間 + `MaxOvertimeStartMins`) にデータベース接続が復元された場合、VDAの再起動が開始されます。
- その時間内にデータベース接続が復元されない場合、VDAの再起動は開始されません。
- このパラメーターが省略されているか、値がゼロの場合、停止期間に関係なく、データベースへの接続が復元されたときにスケジュールされた再起動が開始されます。

詳細については、コマンドレットのヘルプを参照してください。この機能は PowerShell でのみ利用できます。Web Studio で再起動スケジュールを構成する際には、この値を設定できません。

メンテナンスモードのマシンのスケジュールされた再起動

> **注:**
>
> この機能はPowerShellでのみ利用できます。オプション `IgnoreMaintenanceMode` は、Citrix Virtual Apps and Desktops™ 7 2006以降でサポートされています。

> 再起動スケジュールがメンテナンスモードのマシンに影響するかどうかを示すには、`BrokerRebootScheduleV2` コマンドレットで `IgnoreMaintenanceMode` オプションを使用します。

たとえば、次のコマンドレットは、メンテナンスモードのマシン (メンテナンスモードではないマシンに加えて) を再起動するスケジュールを作成します。

```
New-Brokerrebootschedulev2 rebootSchedule1 -DesktopGroupName <myDesktopGroup>
-IgnoreMaintenanceMode $true
```

次のコマンドレットは、既存の再起動スケジュールを変更します。

```
Set-Brokerrebootschedulev2 rebootSchedule1 -IgnoreMaintenanceMode $true
```

詳細については、コマンドレットのヘルプを参照してください。この機能はPowerShellでのみ利用可能です。

1回限りの再起動スケジュールを有効にする

PowerShell を使用して1回限りの再起動スケジュールを有効にする場合は、次の `BrokerCatalogRebootSchedule` PowerShell コマンドを使用して、再起動スケジュールを作成、変更、削除します。

- Get-BrokerCatalogRebootSchedule
- New-BrokerCatalogRebootSchedule
- Set-BrokerCatalogRebootSchedule
- ブローカーカタログの再起動スケジュールを削除
- ブローカーカタログの再起動スケジュール名を変更

制限事項:

- タイムゾーンが構成されていないカタログに関連付けられたカタログ再起動スケジュールは作成されますが、開始されません。

- カタログ再起動スケジュールが作成されると、その再起動スケジュールはデリバリーグループに属するカタログVMでのみ実行されます。

例、,

- **BankTellers** という名前のカタログ内のVMの再起動スケジュールを、Feb 3, 2022 の午前2時から午前4時の間に開始するように作成します。

```
C:\PS> New-BrokerCatalogRebootSchedule -Name BankTellers -CatalogName
BankTellers  -StartDate "2022-02-03" -StartTime "02:00" -Enabled $true
-RebootDuration 120
```

- UID 17を持つカタログ内のVMの再起動スケジュールを、Feb 3, 2022の午前1時から午前5時の間に開始するように作成します。再起動の10分前に、各VMは、すべてのユーザーセッションで、タイトルが「**WARNING: Reboot pending**」、メッセージが「**Save your work**」のメッセージボックスを表示するように設定されます。

```
C:\PS> New-BrokerCatalogRebootSchedule -Name 'Update reboot'
-CatalogUid 17 -StartDate "2022-02-03" -StartTime "01:00" -Enabled
$true -RebootDuration 240 -WarningTitle "WARNING: Reboot pending"
-WarningMessage "Save your work" -WarningDuration 10
```

- **Old Name** という名前のカタログ再起動スケジュールを **New Name** に変更します。

```
C:\PS> Rename-BrokerCatalogRebootSchedule -Name "Old Name" -NewName
"New Name"
```

- UID 1 を持つすべてのカタログ再起動スケジュールを表示し、その後、UID 1 を持つカタログ再起動スケジュールを **New Name** に変更します。

```
C:\PS> Get-BrokerCatalogRebootSchedule -Uid 1 | Rename-
BrokerCatalogRebootSchedule -NewName "New Name" -PassThru
```

- **Accounting**という名前のカタログ再起動スケジュールを、各VMの再起動の10分前に、タイトルが「**WARNING: Reboot pending**」、メッセージが「**Save your work**」のメッセージを表示するように設定します。このメッセージは、そのVM上のすべてのユーザーセッションに表示されます。

```
C:\PS> Set-BrokerCatalogRebootSchedule -Name Accounting -WarningMessage
"Save your work" -WarningDuration 10 -WarningTitle "WARNING: Reboot
pending"
```

- 無効になっているすべての再起動スケジュールを表示し、その後、無効になっているすべての再起動スケジュールを有効にします。

```
C:\PS> Get-BrokerCatalogRebootSchedule -Enabled $false | Set-
BrokerCatalogRebootSchedule -Enabled $true
```

- UID 17を持つカタログ再起動スケジュールを、各VMの再起動の15分前、10分前、5分前に「**Rebooting in %m% minutes**」というメッセージを表示するように設定します。

```
C:\PS> Set-BrokerCatalogRebootSchedule 17 -WarningMessage "Rebooting in
%m% minutes." -WarningDuration 15 -WarningRepeatInterval 5
```

- 「**MyCatalog**」という名前のカタログのタイムゾーンを構成します。

```
C:\PS> Set-BrokerCatalog -Name "MyCatalog" -TimeZone &lt;TimeZone>
```

デリバリーグループ内のマシンの電源管理

仮想シングルセッションOSマシンのみ電源管理が可能で、物理マシン（リモートPCアクセスを含む）はできません。GPU機能を備えたシングルセッションOSマシンは一時停止できないため、電源オフ操作は失敗します。マルチセッションOSマシンについては、再起動スケジュールを作成できます。

プールされたマシンを含むデリバリーグループでは、仮想シングルセッションOSマシンは次のいずれかの状態になります。

- ランダムに割り当てられ、使用中
- 割り当てられていない、未接続

静的マシンを含むデリバリーグループでは、仮想シングルセッションOSマシンは次のようになります。

- 永続的に割り当てられ、使用中
- 永続的に割り当てられ、未接続（ただし準備完了）

- 割り当てられていない、未接続

通常の使用では、静的デリバリーグループには通常、永続的に割り当てられたマシンと割り当てられていないマシンの両方が含まれます。最初は、デリバリーグループの作成時に手動で割り当てられたマシンを除き、すべてのマシンが割り当てられていません。ユーザーが接続すると、マシンは永続的に割り当てられます。これらのデリバリーグループ内の割り当てられていないマシンは完全に電源管理できますが、永続的に割り当てられたマシンは部分的にしか管理できません。

- **プールとバッファー:** プールされたデリバリーグループおよび割り当てられていないマシンを持つ静的デリバリーグループの場合、プール（このインスタンスでは）とは、電源オン状態に保たれ、ユーザーが接続する準備ができている、割り当てられていない、または一時的に割り当てられたマシンのセットです。ユーザーはログオン後すぐにマシンを取得します。プールサイズ（電源オン状態に保たれるマシンの数）は、時間帯によって構成可能です。静的デリバリーグループの場合は、SDKを使用してプールを構成します。

  バッファーとは、プール内のマシンの数がしきい値を下回ったときに電源がオンになる、割り当てられていないマシンの追加のスタンバイセットです。しきい値は、デリバリーグループサイズのパーセンテージです。大規模なデリバリーグループの場合、しきい値を超えるとかなりの数のマシンがオンになる可能性があります。したがって、デリバリーグループのサイズを慎重に計画するか、SDKを使用してデフォルトのバッファーサイズを調整してください。

- **電源状態タイマー:** 電源状態タイマーを使用して、ユーザーが指定された時間切断された後にマシンを中断できます。たとえば、ユーザーが10分以上切断されている場合、営業時間外にマシンは自動的に中断されます。

  タイマーは、平日と週末、およびピーク時と非ピーク時の間隔で構成できます。

- **永続的に割り当てられたマシンの部分的な電源管理:** 永続的に割り当てられたマシンでは、電源状態タイマーを設定できますが、プールやバッファーは設定できません。マシンは各ピーク期間の開始時にオンになり、各オフピーク期間の開始時にオフになります。消費されたマシンを補うために利用可能になるマシンの数について、割り当てられていないマシンで行うようなきめ細かな制御はできません。

仮想シングルセッションOSマシンの電源管理

1. 左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**デリバリーグループの編集**をクリックします。
3. **電源管理**ページで、**マシンの電源管理**で**平日**を選択します。デフォルトでは、平日は月曜日から金曜日です。
4. ランダムなデリバリーグループの場合、**電源をオンにするマシン**で**編集**をクリックし、平日のプールサイズを指定します。次に、電源をオンにするマシンの数を選択します。

5. **ピーク時間**で、各日のピーク時間とオフピーク時間を設定します。
6. 平日のピーク時間と非ピーク時間の電源状態タイマーを設定します。**ピーク時間中 > 切断時**で、デリバリーグループ内の切断されたマシンを中断するまでの遅延時間（分単位）を指定し、**中断**を選択します。**オフピーク時間中 > 切断時**で、デリバリーグループ内のログオフされたマシンをオフにするまでの遅延時間を指定し、**シャットダウン**を選択します。このタイマーは、ランダムなマシンを含むデリバリーグループでは使用できません。
7. **マシンの電源管理**で**週末**を選択し、週末のピーク時間と電源状態タイマーを構成します。
8. 加えた変更を適用してウィンドウを開いたままにするには、 をクリックします。または、変更を適用してウィンドウを閉じるには、 をクリックします。

SDKを使用して、次の操作を実行します。

- 電源状態タイマーに応じてマシンをサスペンドするのではなくシャットダウンする場合、またはタイマーを接続解除ではなくログオフに基づいて設定する場合。
- デフォルトの平日と週末の定義を変更します。
- 電源管理を無効にします。詳しくは、「CTX217289」を参照してください。

切断されたセッションで異なる期間に移行するVDIマシンの電源管理

> **重要:**
>
> この機能強化は、切断されたセッションを持つVDIマシンにのみ適用されます。ログオフされたセッションを持つVDIマシンには適用されません。

> 以前のリリースでは、アクション（切断アクション="**Suspend**"または"**Shutdown**"）が必要な期間に移行するVDIマシンは、電源がオンのままでした。このシナリオは、マシンがアクション（切断アクション="**Nothing**"）が不要な期間（ピーク時またはオフピーク時）に切断された場合に発生しました。

Citrix Virtual Apps and Desktops 7 1909以降、指定された切断時間が経過すると、移行先の期間に設定された切断アクションに応じて、マシンはサスペンドまたは電源オフされます。

たとえば、VDIデリバリーグループに対して次の電源ポリシーを構成します。

- `PeakDisconnectAction`を「Nothing」に設定
- `OffPeakDisconnectAction`を「Shutdown」に設定
- `OffPeakDisconnectTimeout`を「10」に設定

電源ポリシーの切断アクションについて詳しくは、https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policyおよびhttps://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/を参照してください。

以前のリリースでは、ピーク時にセッションが切断されたVDIマシンは、ピークからオフピークに移行しても電源がオンのままでした。Citrix Virtual Apps and Desktops 7 1909以降、期間移行時に`OffPeakDisconnectAction`および`OffPeakDisconnectTimeout`ポリシーアクションがVDIマシンに適用されます。その結果、マシンはオフピークに移行してから10分後に電源オフされます。

以前の動作に戻したい場合（つまり、ピークからオフピーク、またはオフピークからピークに切断されたセッションで移行するマシンに対して何もしない場合）は、次のいずれかを実行します。

- `LegacyPeakTransitionDisconnectedBehaviour` レジストリ値を `1` に設定します。これは以前の動作を有効にする *true* と同等です。デフォルトでは、値は `0` または *false* であり、期間移行時に切断電源ポリシーアクションをトリガーします。
  - パス: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer`
  - 名前: `LegacyPeakTransitionDisconnectedBehaviour`
  - 種類: `REG_DWORD`
  - データ: `0x00000001 (1)`
- `Set-BrokerServiceConfigurationData` PowerShell コマンドを使用して設定を構成します。例:
  - `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

期間移行時に電源ポリシーアクションを適用する前に、マシンは次の基準を満たしている必要があります。

- 切断されたセッションがあること。
- 保留中の電源アクションがないこと。
- 異なる時間帯に移行する VDI (シングルセッション) デリバリーグループに属していること。
- 特定の時間帯（ピーク時またはオフピーク時）に切断され、電源アクションが割り当てられている期間に移行するセッションがあること。

カタログの電源オン状態の VDA の割合を変更する

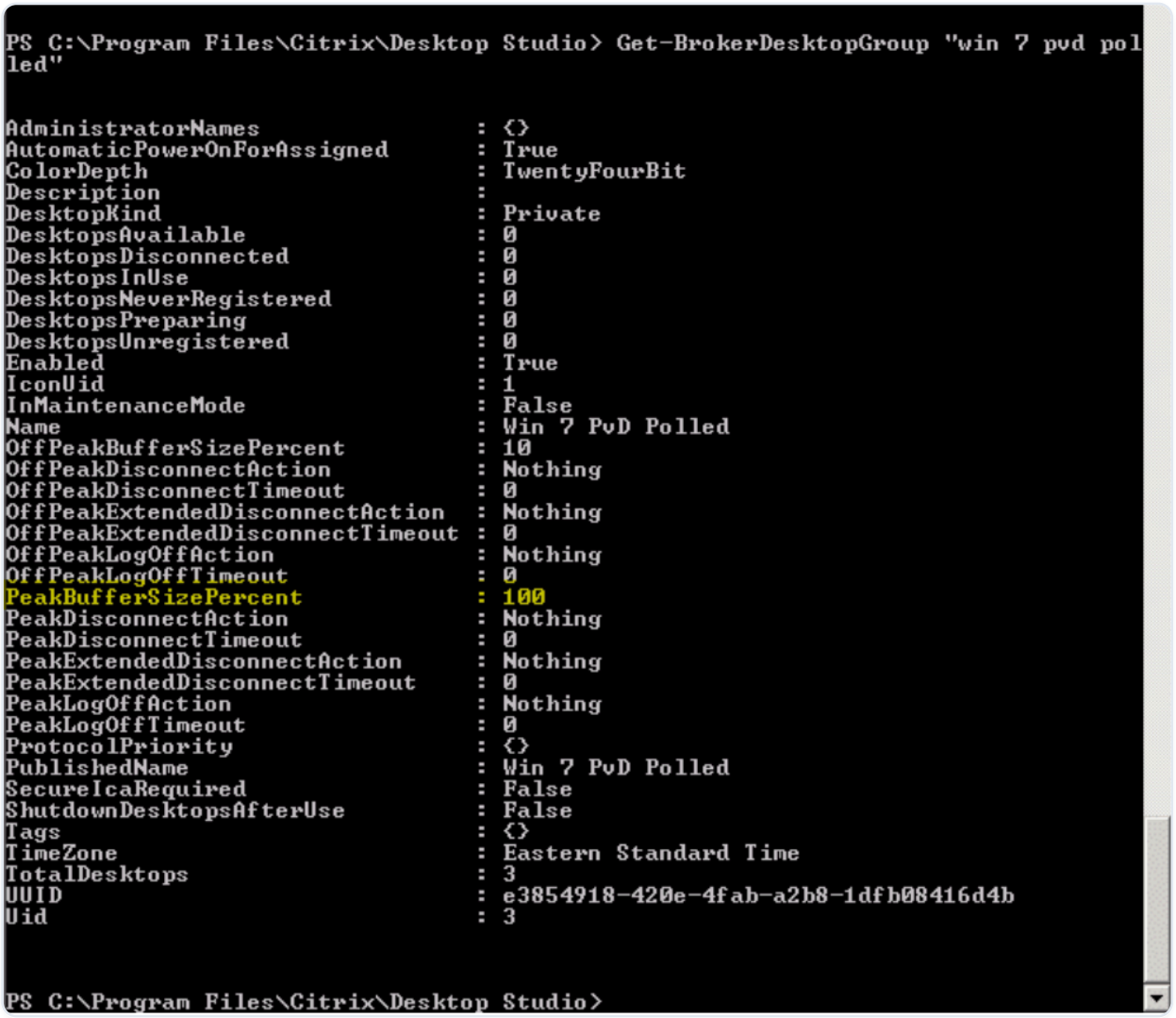
1. デリバリーグループの **電源管理** セクションから、デリバリーグループのピーク時間を調整します。
2. デスクトップグループ名をメモします。
3. 管理者権限で PowerShell を起動し、次のコマンドを実行します。「Desktop Group Name」を、実行中の VDA の割合が変更されたデスクトップグループの名前に置き換えます。

   ```
   asnp Citrix*
   ```

   ```
   # Set-BrokerDesktopGroup "Desktop Group Name" -PeakBufferSizePercent 100
   ```

   値が 100 の場合、VDA の 100% が準備完了状態であることを意味します。
4. 次を実行してソリューションを確認します。

   ```
   #Get-BrokerDesktopGroup "Desktop Group Name"
   ```



変更が有効になるまで、最大1時間かかる場合があります。

ユーザーがログオフした後にVDAをシャットダウンするには、次のように入力します。

```
# Set-BrokerDesktopGroup "Desktop Group Name" -ShutDownDesktopsAfterUse $True
```

ピーク時間中にVDAを再起動して、ユーザーがログオフした後に利用できるようにするには、次のように入力します。

```
# Set-BrokerDesktopGroup "Desktop Group Name"
-AutomaticPowerOnForAssignedDuringPeak $True
```

セッション

- セッションのログオフまたは切断、またはユーザーへのメッセージ送信
- セッションのプレ起動とセッションの維持を構成する
- メンテナンスモードのマシンから切断された場合のセッション再接続を制御する
- セッションローミングを構成する

セッションのログオフまたは切断

1. 左ペインで**Delivery Groups**を選択します。
2. デリバリーグループを選択し、アクションバーで**View Machines**を選択します。
3. 中央ペインでマシンを選択し、アクションバーで**View Sessions**を選択してから、セッションを選択します。
    - または、中央ペインで**Session**タブを選択し、セッションを選択します。
4. セッションからログオフするには、アクションバーで**Log off**を選択します。セッションが閉じられ、ユーザーはログアウトされます。マシンが特定のユーザーに割り当てられていない限り、他のユーザーが利用できるようになります。
5. セッションを切断するには、アクションバーで**Disconnect**を選択します。アプリケーションはセッション内で実行を継続し、マシンはそのユーザーに割り当てられたままになります。ユーザーは同じマシンに再接続できます。

シングルセッションOSマシンでは、未使用のセッションを自動的に処理するように電源状態タイマーを構成できます。詳細については、「電源管理されたマシン」を参照してください。

デリバリーグループにメッセージを送信する

1. 左ペインで**Delivery Groups**を選択します。
2. デリバリーグループを選択し、アクションバーで**View Machines**を選択します。

3. 中央ペインで、メッセージを送信するマシンを選択します。
4. アクションバーで**View Sessions**を選択します。
5. 中央ペインで、すべてのセッションを選択し、アクションバーで**メッセージの送信**を選択します。
6. メッセージを入力し、**OK**をクリックします。必要に応じて、重大度レベルを指定できます。オプションには、**重大**、**質問**、**警告**、**情報**があります。

または、Citrix Directorを使用してメッセージを送信することもできます。詳しくは、「ユーザーへのメッセージの送信」を参照してください。

デリバリーグループでセッションの事前起動とセッションの維持を構成する

これらの機能は、マルチセッションOSマシンでのみサポートされています。

セッションの事前起動とセッションの維持機能は、要求される前にセッションを開始すること（セッションの事前起動）と、ユーザーがすべてのアプリケーションを閉じた後もアプリケーションセッションをアクティブに保つこと（セッションの維持）により、指定されたユーザーがアプリケーションにすばやくアクセスできるようにします。

デフォルトでは、セッションの事前起動とセッションの維持は使用されません。セッションは、ユーザーがアプリケーションを起動したときに開始（起動）され、セッション内の最後に開いたアプリケーションが閉じるまでアクティブなままになります。

考慮事項：

- デリバリーグループはアプリケーションをサポートしている必要があり、マシンはマルチセッションOS用のVDA（最小バージョン7.6）を実行している必要があります。
- これらの機能は、Windows向けCitrix Workspaceアプリを使用している場合にのみサポートされ、追加のCitrix Workspaceアプリ構成も必要です。手順については、お使いのWindows向けCitrix Workspaceアプリバージョンの製品ドキュメントで「session prelaunch」を検索してください。
- Citrix Workspace app for HTML5はサポートされていません。
- セッションの事前起動を使用している場合、ユーザーのマシンがサスペンドまたは休止状態になると、事前起動は機能しません（セッションの事前起動設定にかかわらず）。ユーザーはマシン/セッションをロックできます。ただし、ユーザーがCitrix Workspaceアプリからログオフすると、セッションは終了し、事前起動は適用されなくなります。
- セッションの事前起動を使用している場合、物理クライアントマシンは、サスペンドまたはハイバネートの電源管理機能を使用できません。クライアントマシンのユーザーはセッションをロックできますが、ログオフしてはいけません。

- 事前起動および維持されているセッションは同時接続ライセンスを消費しますが、これは接続されている場合に限ります。ユーザー/デバイスライセンスを使用している場合、ライセンスは90日間有効です。未使用の事前起動および維持されているセッションは、デフォルトで15分後に切断されます。この値はPowerShellで構成できます（`New/Set-BrokerSessionPreLaunch` コマンドレット）。
- これらの機能が互いに補完し合うように調整するには、ユーザーのアクティビティパターンを慎重に計画し、監視することが不可欠です。最適な構成は、ユーザーがより早くアプリケーションを利用できるという利点と、ライセンスの使用とリソースの割り当てにかかるコストとのバランスを取ります。
- Citrix Workspaceアプリで、スケジュールされた時刻にセッションの事前起動を構成することもできます。

未使用の事前起動セッションと残存セッションがアクティブなままになる期間

ユーザーがアプリケーションを起動しない場合に、未使用のセッションがアクティブなままになる期間を指定する方法はいくつかあります。構成されたタイムアウトとサーバー負荷のしきい値です。これらすべてを構成できます。最初に発生したイベントにより、未使用のセッションが終了します。

- **タイムアウト:** 構成されたタイムアウトは、未使用の事前起動セッションまたは残存セッションがアクティブなままになる分、時間、または日数を指定します。タイムアウトを短く設定しすぎると、事前起動セッションは、ユーザーにアプリケーションへのより迅速なアクセスという利点を提供する前に終了します。タイムアウトを長く設定しすぎると、サーバーに十分なリソースがないため、受信ユーザー接続が拒否される可能性があります。

  このタイムアウトは、管理コンソールからではなく、SDKからのみ有効にできます (`New/Set-BrokerSessionPreLaunch` コマンドレット)。タイムアウトを無効にすると、そのデリバリーグループのコンソール表示や**デリバリーグループの編集**ページには表示されません。
- **しきい値:** サーバー負荷に基づいて事前起動セッションと残存セッションを自動的に終了することで、サーバーリソースが利用可能であると仮定して、セッションが可能な限り開いたままになることを保証します。未使用の事前起動セッションと残存セッションは、新しいユーザーセッションにリソースが必要なときに自動的に終了されるため、接続拒否を引き起こしません。

  2つのしきい値を構成できます。デリバリーグループ内のすべてのサーバーの平均負荷率と、グループ内の単一サーバーの最大負荷率です。しきい値を超えると、事前起動または残存状態にあった時間が最も長いセッションが終了されます。負荷がしきい値を下回るまで、セッションは1分間隔で1つずつ終了されます。しきい値を超えている間は、新しい事前起動セッションは開始されません。

Controllerに登録されていないVDAを持つサーバーと、メンテナンスモードのサーバーは、完全にロードされていると見なされます。計画外の停止により、容量を解放するために事前起動セッションと残存セッションが自動的に終了します。

セッションの事前起動を有効にするには

1. グループを選択し、アクションバーで**デリバリーグループの編集**をクリックします。
2. **アプリケーションの事前起動**ページで、セッションを起動するタイミングを選択して、セッションの事前起動を有効にします。

    - ユーザーがアプリケーションを起動したとき。これはデフォルト設定です。セッションの事前起動は無効になっています。
    - デリバリーグループ内の任意のユーザーがCitrix Workspaceアプリ for Windowsにログオンしたとき。
    - ユーザーおよびユーザーグループのリスト内のいずれかのユーザーがCitrix Workspaceアプリ for Windowsにログオンしたとき。このオプションを選択する場合は、ユーザーまたはユーザーグループも指定してください。

    アプリケーションの事前起動セッションページ(/en-us/citrix-virtual-apps-desktops/current-release/media/dws-session-2.png)
3. ユーザーがアプリケーションを起動すると、事前起動されたセッションは通常のセッションに置き換えられます。ユーザーがアプリケーションを起動しない場合（事前起動されたセッションが未使用の場合）、以下の設定がそのセッションがアクティブなままになる期間に影響します。

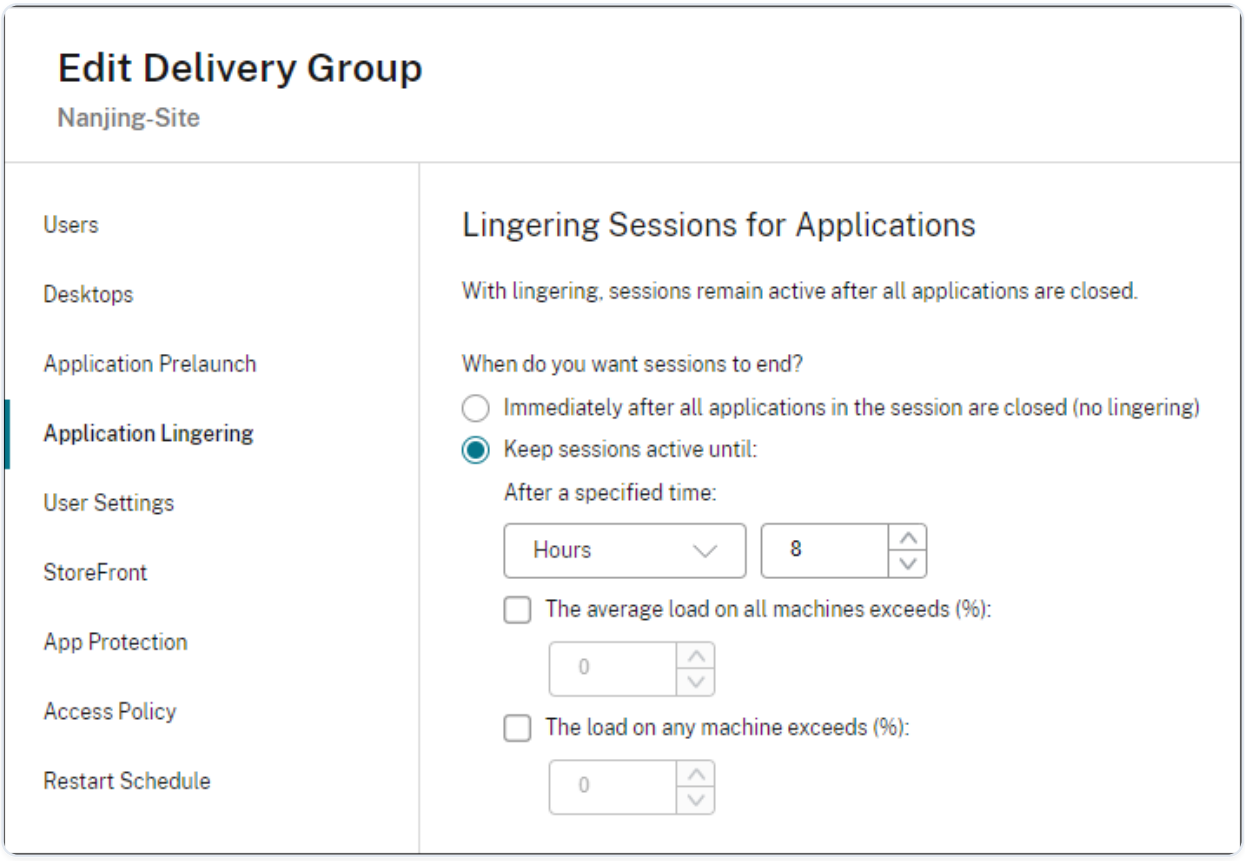
    - 指定された時間間隔が経過したとき。時間間隔は変更できます（1〜99日、1〜2376時間、または1〜142,560分）。
    - デリバリーグループ内のすべてのマシンの平均負荷が指定された割合（1〜99%）を超えたとき。
    - デリバリーグループ内のいずれかのマシンの負荷が指定された割合（1〜99%）を超えたとき。

    まとめ：事前起動されたセッションは、ユーザーがアプリケーションを起動する、指定された時間が経過する、または指定された負荷しきい値を超える、のいずれかのイベントが発生するまでアクティブなままです。

セッションの維持を有効にするには

1. 左側のペインで**デリバリーグループ**を選択します。

2. グループを選択し、アクションバーで**デリバリーグループの編集**をクリックします。
3. **アプリケーションの維持**ページで、**セッションをアクティブなままにする期間**を選択して、セッションの維持を有効にします。



4. ユーザーが別のアプリケーションを起動しない場合、残存セッションがアクティブなままになる期間に影響する設定がいくつかあります。

   - 指定された時間間隔が経過した場合。時間間隔は、1～99日、1～2376時間、または1～142,560分に変更できます。
   - デリバリーグループ内のすべてのマシンの平均負荷が指定された割合（1～99%）を超えた場合。
   - デリバリーグループ内のいずれかのマシンの負荷が指定された割合（1～99%）を超えた場合。

   まとめ：残存セッションは、ユーザーがアプリケーションを起動する、指定された時間が経過する、または指定された負荷しきい値を超える、のいずれかのイベントが発生するまでアクティブなままです。

メンテナンスモードのマシンから切断された場合のセッション再接続を制御する

> **注：**

> この機能はPowerShellでのみ利用可能です。

> メンテナンスモードのマシンで切断されたセッションが、デリバリーグループ内のマシンに再接続できるかどうかを制御できます。

バージョン2106より前は、メンテナンスモードのマシンから切断されたシングルセッションのプールされたデスクトップセッションの再接続は許可されていませんでした。バージョン2106以降では、メンテナンスモードのマシンから切断された後の再接続（セッションの種類に関係なく）を許可または禁止するようにデリバリーグループを構成できます。

デリバリーグループを作成または編集する際（`New-BrokerDesktopGroup`、`Set-BrokerDesktopGroup`）、`-AllowReconnectInMaintenanceMode <boolean>`パラメーターを使用して、メンテナンスモードのマシンから切断されたマシンへの再接続を許可または禁止します。

- trueに設定すると、セッションはグループ内のマシンに再接続できます。
- 「false」に設定されている場合、セッションはグループ内のマシンに再接続できません。

デフォルト値:

- シングルセッション: 無効
- マルチセッション: 有効

セッションローミングの構成

デフォルトでは、デリバリーグループに対してセッションローミングが有効になっています。セッションはユーザーとともにクライアントデバイス間をローミングします。ユーザーがセッションを起動し、別のデバイスに移動すると、同じセッションが使用され、アプリケーションは両方のデバイスで同時に利用可能になります。複数のデバイスでアプリケーションを表示できます。アプリケーションは、デバイスや現在のセッションの有無にかかわらず追従します。多くの場合、アプリケーションに割り当てられたプリンターやその他のリソースも追従します。または、PowerShellを使用することもできます。詳しくは、「セッションローミング」を参照してください。

アプリケーションのセッションローミングの構成

アプリケーションのセッションローミングを構成するには、次の手順に従います。

1. コンソールで、左側のペインの**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**「デリバリーグループの編集」**を選択します。
3. ページで、 チェックボックスをオンにして、セッションローミングを有効にします。

- 有効にすると、ユーザーがアプリケーションセッションを起動して別のデバイスに移動した場合、同じセッションが使用され、両方のデバイスで利用可能になります。無効にすると、セッションはデバイス間をローミングしなくなります。

4. **「OK」**を選択して変更を適用し、ウィンドウを閉じます。

デスクトップのセッションローミングを構成する

デスクトップのセッションローミングを構成するには、次の手順に従います。

1. コンソールで、左側のペインの**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**編集**を選択します。
3. **デスクトップ**ページで、デスクトップを選択し、**編集**を選択します。
4. **セッションローミング**チェックボックスをオンにして、セッションローミングを有効にします。

- 有効にすると、ユーザーがデスクトップを起動してから別のデバイスに移動した場合、同じセッションが使用され、アプリケーションは両方のデバイスで利用可能になります。無効にすると、セッションはデバイス間をローミングしなくなります。

OKを選択して変更を適用し、ウィンドウを閉じます。

アプリケーション

デリバリーグループのアプリケーションを表示および追加します。

1. コンソールで、左ペインの**デリバリーグループ**を選択します。
2. グループを選択します。このグループにアプリケーションが含まれている場合、アクションバーに**アプリケーションの表示**が表示されます。
3. **アプリケーションの表示**を選択します。このグループで利用可能なすべてのアプリケーションが表示される**アプリケーション**ノードに移動します。
4. このグループにアプリケーションを追加するには、**デリバリーグループ**ノードに移動し、グループを選択して、アクションバーで**アプリケーションの追加**を選択します。

VDA上のCitrix Secure Access™クライアントからのシームレスなログオン

VDAに存在するCitrix Secure Access (CSA) クライアントからCitrix Secure Private Accessへのシングルサインオン (SSO) を使用して、Citrix Workspaceにシームレスにログオンできます。この機能は、シングルセッションVDAとマルチセッションVDAの両方に適用されます。

これを実現する手順は次のとおりです。

1. 既存のデリバリーグループを編集してSPA SSOを有効にします。例:

   ```
   Set-BrokerDesktopGroup -Name &lt;String> -SpaSsoEnabled 1
   ```

2. Get -BrokerDesktopGroup PowerShellコマンドを使用して、デリバリーグループのSPA SSOのステータスを確認します。例:

   ```
   Get-BrokerDesktopGroup -Name &lt;String> -property 'SpaSsoEnabled'
   ```

3. SPAで、アプリケーションとポリシーを作成します。「TCP/UDPアプリの構成」および「アプリケーションのアクセスポリシーの構成」を参照してください。
4. シングルセッションまたはマルチセッションVDAにRDP接続し、最新のCSAエージェントをインストールします。
5. Citrix Workspace を開き、シングルセッションまたはマルチセッションVDAにログオンします。

トラブルシューティング

- Delivery Controllerに登録されていないVDAは、ブローカーセッションの起動時に考慮されません。これにより、利用可能なはずのリソースが十分に活用されないことになります。VDAが登録されない理由はさまざまであり、その多くは管理者がトラブルシューティングできます。詳細表示には、カタログ作成ウィザードと、デリバリーグループにカタログを追加した後のトラブルシューティング情報が表示されます。

  デリバリーグループを作成した後、デリバリーグループの詳細ペインには、登録可能だが登録されていないマシンの数が表示されます。たとえば、1台以上のマシンが電源オンでメンテナンスモードではないが、現在Controllerに登録されていない場合などです。「登録されていないが、登録されるべき」マシンを表示するときは、詳細ペインの**トラブルシューティング**タブで考えられる原因と推奨される是正措置を確認してください。

  機能レベルに関するメッセージについては、「VDAのバージョンと機能レベル」を参照してください。

  VDA登録のトラブルシューティングについては、「CTX136668」を参照してください。
- デリバリーグループの表示では、詳細ペインの**インストール済みVDAバージョン**が、マシンに実際にインストールされているバージョンと異なる場合があります。マシンのWindowsのプログラムと機能の表示には、実際のVDAバージョンが表示されます。

- **電源状態不明**のステータスのマシンについては、ガイダンスとしてCTX131267を参照してください。

アプリケーショングループの作成

> **注:**
>
> バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

はじめに

アプリケーショングループを使用すると、アプリケーションのコレクションを管理できます。異なるデリバリーグループ間で共有されるアプリケーション、またはデリバリーグループ内のユーザーのサブセットによって使用されるアプリケーションに対してアプリケーショングループを作成します。アプリケーショングループはオプションであり、同じアプリケーションを複数のデリバリーグループに追加する代替手段を提供します。デリバリーグループを複数のアプリケーショングループに関連付けたり、アプリケーショングループを複数のデリバリーグループに関連付けたりできます。

アプリケーショングループを使用すると、より多くのデリバリーグループを使用する場合と比較して、アプリケーション管理とリソース制御の利点が得られます。

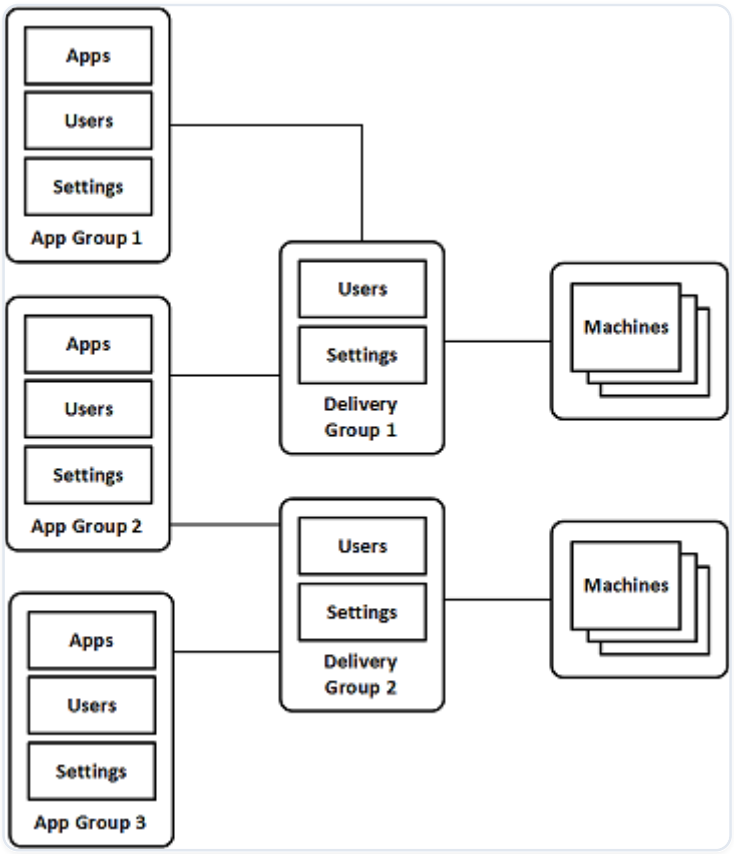
- アプリケーションとその設定を論理的にグループ化することで、それらのアプリケーションを単一の単位として管理できます。たとえば、同じアプリケーションを個々のデリバリーグループに1つずつ追加（公開）する必要はありません。
- アプリケーショングループ間のセッション共有は、リソース消費を節約できます。それ以外の場合、アプリケーショングループ間のセッション共有を無効にすることが有益な場合もあります。
- タグ制限機能を使用すると、選択したデリバリーグループ内のマシンのサブセットのみを考慮して、アプリケーショングループからアプリケーションを公開できます。タグ制限を使用すると、既存のマシンを複数の公開タスクに使用できるため、追加のマシンの展開と管理に関連するコストを節約できます。タグ制限は、デリバリーグループ内のマシンを細分化（またはパーティション分割）するものと考えることができます。タグ制限付きのアプリケーショングルー

プまたはデスクトップを使用すると、デリバリーグループ内のマシンのサブセットを分離してトラブルシューティングする際に役立ちます。

構成例

例 1:

次のグラフィックは、アプリケーショングループを含むCitrix Virtual Apps and Desktops™展開を示しています。



この構成では、アプリケーションはデリバリーグループではなくアプリケーショングループに追加されます。デリバリーグループは、どのマシンが使用されるかを指定します。（図には示されていませんが、マシンはマシンカタログ内にあります。）

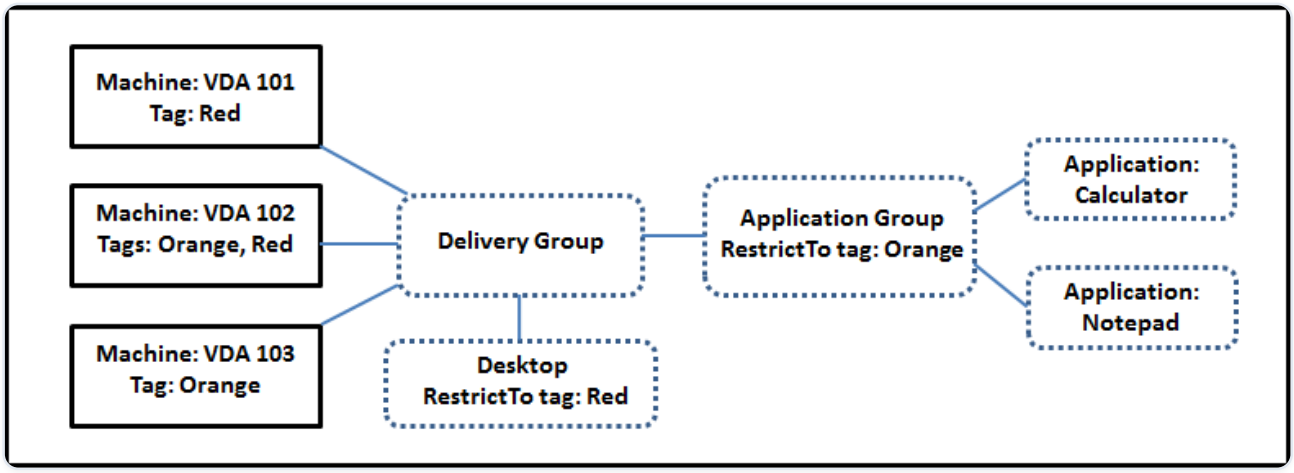
アプリケーショングループ1はデリバリーグループ1に関連付けられています。アプリケーショングループ1で指定されたユーザーがアプリケーショングループ1のアプリケーションにアクセスします。これらのグループは、デリバリーグループ1のユーザーリストにも含まれている場合にのみ表示されます。この構成は、アプリケーショングループのユーザーリストが、関連付けられたデリバリーグループのユーザーリストのサブセット（制限）であるというガイダンスに従います。アプリケーショングループ1の設定（アプリケーショングループ間のアプリケーションセッション共有、関連付けられたデリバリーグループなど）は、そのグループ内のアプリケーションとユーザーに適用されます。デリバリーグループ1の設定は、アプリケーショングループ1と2のユーザーに適用

されます。これは、これらのアプリケーショングループがそのデリバリーグループに関連付けられているためです。

アプリケーショングループ2は、2つのデリバリーグループ（1と2）に関連付けられています。これらの各デリバリーグループには、アプリケーショングループ2で優先度が割り当てられ、アプリケーションが起動されるときにデリバリーグループがチェックされる順序を示します。優先度が等しいデリバリーグループはロードバランスされます。アプリケーショングループ2で指定されたユーザーがアプリケーショングループ2のアプリケーションにアクセスします。ただし、それらのユーザーはデリバリーグループ1とデリバリーグループ2のユーザーリストにも含まれている必要があります。

例 2:

このシンプルなレイアウトでは、タグ制限を使用して、特定のデスクトップおよびアプリケーションの起動に考慮されるマシンを制限します。このサイトには、1つの共有デリバリーグループ、1つの公開デスクトップ、および2つのアプリケーションで構成された1つのアプリケーショングループがあります。



3台のマシン（VDA 101～103）のそれぞれにタグが追加されています。

アプリケーショングループは「Orange」タグ制限付きで作成されました。その各アプリケーションは、そのデリバリーグループ内で「Orange」タグを持つマシン（VDA 102および103）でのみ起動されます。

アプリケーショングループ（およびデスクトップ）でタグ制限を使用するためのより包括的な例とガイダンスについては、「タグ」を参照してください。

ガイダンスと考慮事項

Citrixでは、アプリケーションをアプリケーショングループまたはデリバリーグループのいずれかに追加することをお勧めします。両方に追加することはお勧めしません。そうしないと、2種類の

グループにアプリケーションが存在することで複雑さが増し、管理が難しくなる可能性があります。

デフォルトでは、アプリケーショングループは有効になっています。アプリケーショングループを作成した後、グループを編集してこの設定を変更できます。「アプリケーショングループの管理」を参照してください。

デフォルトでは、アプリケーショングループ間のアプリケーションセッション共有は有効になっています。「アプリケーショングループ間のセッション共有」を参照してください。

Citrixでは、デリバリーグループを現在のバージョンにアップグレードすることをお勧めします。このプロセスには、次のものが必要です。

1. デリバリーグループで使用されているマシン上のVDAをアップグレードする。
2. それらのマシンを含むマシンカタログのアップグレード。
3. デリバリーグループのアップグレード。

詳細については、「デリバリーグループの管理」を参照してください。

アプリケーショングループを使用するには、コアコンポーネントが最小バージョン7.9である必要があります。

アプリケーショングループを作成するには、Delivery Group Administrator の組み込みロールの委任管理権限が必要です。詳細については、「委任管理」(/ja-jp/citrix-virtual-apps-desktops/current-release/manage-deployment/delegated-administration.html) を参照してください。

この記事では、アプリケーションを複数のアプリケーショングループに「関連付ける」ことについて言及しています。これは、利用可能なソースからそのアプリケーションのインスタンスを追加する操作とは区別されます。同様に、デリバリーグループは、互いの追加やコンポーネントではなく、アプリケーショングループに関連付けられます。

アプリケーショングループとのセッション共有

アプリケーションセッション共有が有効になっている場合、すべてのアプリケーションは同じアプリケーションセッションで起動します。これにより、より多くのアプリケーションセッションを起動するコストが削減され、コピー＆ペースト操作など、クリップボードを使用するアプリケーション機能の使用が可能になります。ただし、状況によってはセッション共有をクリアできます。

アプリケーショングループを使用する場合、デリバリーグループのみを使用する場合に利用できる標準のセッション共有動作を拡張する、次の3つの方法でアプリケーションセッション共有を構成できます。

- アプリケーショングループ間でセッション共有が有効。
- 同じアプリケーショングループ内のアプリケーション間でのみセッション共有が有効。
- セッション共有が無効。

アプリケーショングループ間のセッション共有

アプリケーショングループ間でアプリケーションセッション共有を有効にすることも、または、同じアプリケーショングループ内のアプリケーションにのみアプリケーションセッション共有を制限するために無効にすることもできます。

- **アプリケーショングループ間のセッション共有を有効にすることが役立つ例:**

  アプリケーショングループ1にはWordやExcelなどのMicrosoft Officeアプリケーションが含まれています。アプリケーショングループ2にはメモ帳や電卓などの他のアプリケーションが含まれており、両方のアプリケーショングループが同じデリバリーグループに接続されています。両方のアプリケーショングループにアクセスできるユーザーがWordを起動してアプリケーションセッションを開始し、次にメモ帳を起動します。コントローラーが、ユーザーの既存のWordを実行しているセッションがメモ帳の実行に適していると判断した場合、メモ帳は既存のセッション内で起動されます。既存のセッションからメモ帳を実行できない場合（たとえば、タグ制限によってセッションが実行されているマシンが除外される場合など）、セッション共有を使用するのではなく、適切なマシン上に新しいセッションが作成されます。

- **アプリケーショングループ間のセッション共有を無効にすることが役立つ例:**

  同じマシンにインストールされている他のアプリケーションとうまく相互運用できない一連のアプリケーションの構成。たとえば、同じソフトウェアスイートの2つの異なるバージョンや、同じWebブラウザーの2つの異なるバージョンなどです。ユーザーが同じセッションで両方のバージョンを起動することを許可しないようにしたい場合。

  ソフトウェアスイートのバージョンごとにアプリケーショングループを作成し、各バージョンのソフトウェアスイートのアプリケーションを対応するアプリケーショングループに追加します。これらのアプリケーショングループのそれぞれでグループ間のセッション共有が無効になっている場合、それらのグループで指定されたユーザーは、同じバージョンのアプリケーションを同じセッションで実行できます。ユーザーは同時に他のアプリケーションを実行できますが、同じセッションでは実行できません。異なるバージョンのアプリケーション、またはアプリケーショングループに含まれていないアプリケーションを起動すると、そのアプリケーションは新しいセッションで起動されます。

このアプリケーショングループ間のセッション共有機能は、セキュリティサンドボックス機能ではありません。これは完璧ではなく、ユーザーが他の手段（例えば、Windows Explorer経由など）でセッションにアプリケーションを起動するのを防ぐことはできません。

マシンが容量に達している場合、新しいセッションはそのマシンでは開始されません。必要に応じて、セッション共有を使用して、新しいアプリケーションがそのマシンの既存のセッションで開始されます。

アプリケーションセッション共有が許可されているアプリケーショングループに対してのみ、事前起動セッションを利用可能にできます。（セッションリンガー機能を使用するセッションは、すべてのアプリケーショングループで利用可能です。）これらの機能は、アプリケーショングループに関連付けられている各デリバリーグループで有効にして構成する必要があります。アプリケーショングループ内でこれらを構成することはできません。

デフォルトでは、アプリケーショングループを作成する際に、アプリケーショングループ間のアプリケーションセッション共有が有効になります。グループ作成時にこれを変更することはできません。アプリケーショングループを作成した後、グループを編集してこの設定を変更できます。アプリケーショングループの管理を参照してください。

アプリケーショングループ内でのセッション共有を無効にする

同じアプリケーショングループ内のアプリケーション間でのアプリケーションセッション共有を防ぐことができます。

- **アプリケーショングループ内でのセッション共有を無効にすることが役立つ例:**

  ユーザーに、別々のモニターでアプリケーションの複数の同時フルスクリーンセッションにアクセスさせたい場合。

  アプリケーショングループを作成し、そこにアプリケーションを追加します。

デフォルトでは、アプリケーショングループを作成すると、アプリケーションセッション共有が有効になります。グループの作成時にこの設定を変更することはできません。アプリケーショングループを作成した後、グループを編集してこの設定を変更できます。「アプリケーショングループの管理」を参照してください。

アプリケーショングループを作成する

アプリケーショングループを作成するには：

1. Web Studioにサインインします。
2. 左側のペインで［**アプリケーション**］を選択し、［**アプリケーショングループ**］タブを選択します。
3. フォルダーを使用してアプリケーショングループを整理するには、**アプリケーショングループ**ルートフォルダーの下にフォルダーを作成します。詳細については、フォルダーを使用してアプリケーショングループを整理するを参照してください。

4. グループを作成するフォルダーを選択し、**アプリケーション グループの作成**をクリックします。グループ作成ウィザードが**はじめに**ページで起動します。このページは、今後のウィザード起動時に表示しないように設定できます。
5. ウィザードに従って、以下に説明するページで設定を構成します。各ページでの作業が完了したら、**次へ**を選択して**概要**ページに進みます。

手順1. デリバリーグループ

デリバリーグループページには、すべてのデリバリーグループと、各グループに含まれるマシンの数が一覧表示されます。

- 「**互換性のあるデリバリーグループ**」リストには、選択可能なデリバリーグループが含まれています。互換性のあるデリバリーグループには、ランダムな（永続的または静的に割り当てられていない）マルチセッションまたはシングルセッションOSマシンが含まれます。
- 「**互換性のないデリバリーグループ**」リストには、選択できないデリバリーグループが含まれています。各エントリには、静的に割り当てられたマシンが含まれるなど、互換性がない理由が説明されています。

アプリケーショングループは、アプリケーションを配信できる共有（プライベートではない）マシンを含むデリバリーグループに関連付けることができます。

以下の両方の条件が満たされている場合、デスクトップのみを配信する共有マシンを含むデリバリーグループを選択することもできます。

- デリバリーグループに共有マシンが含まれており、XenDesktopバージョン7.9より前のバージョンで作成されていること。
- デリバリーグループの編集権限があること。

アプリケーショングループ作成ウィザードがコミットされると、デリバリーグループの種類は自動的に「デスクトップとアプリケーション」に変換されます。

関連付けられたデリバリーグループがないアプリケーショングループを作成することはできますが（アプリケーションを整理するため、または現在使用されていないアプリケーションのストレージとして機能させるためなど）、少なくとも1つのデリバリーグループが指定されるまで、そのアプリケーショングループをアプリケーションの配信に使用することはできません。また、デリバリーグループが指定されていない場合、「**スタートから**」メニューソースからアプリケーショングループにアプリケーションを追加することはできません。

選択したデリバリーグループは、アプリケーションの配信に使用されるマシンを指定します。アプリケーショングループに関連付けるデリバリーグループの横にあるチェックボックスをオンにします。

タグ制限を追加するには、「**タグを持つマシンへの起動を制限する**」を選択し、ドロップダウンリストからタグを選択します。

手順2. ユーザー

アプリケーショングループでアプリケーションユーザーを指定します。前のページで選択したデリバリーグループ内のすべてのユーザーとユーザーグループを許可するか、それらのデリバリーグループから特定のユーザーとユーザーグループを選択します。指定されたユーザーに利用を制限する場合、デリバリーグループで指定されたユーザーのうち、アプリケーショングループで指定されたユーザーのみが、このグループのアプリケーションにアクセスできます。基本的に、アプリケーショングループのユーザーリストは、デリバリーグループのユーザーリストに対するフィルターとして機能します。

認証されていないユーザーによるアプリケーションの使用の有効化または無効化は、アプリケーショングループではなく、デリバリーグループでのみ利用できます。

展開でユーザーリストが指定される場所については、「ユーザーリストが指定される場所」を参照してください。

ステップ3. アプリケーション

知っておくと良いこと:

- デフォルトでは、追加する新しいアプリケーションは「**Applications**」という名前のフォルダーに配置されます。別のフォルダーを指定できます。アプリケーションを追加しようとしたときに、そのフォルダーに同じ名前のアプリケーションが存在する場合、追加しようとしているアプリケーションの名前を変更するよう求められます。提案された一意の名前に同意すると、その新しい名前でアプリケーションが追加されます。そうでない場合は、追加する前に自分で名前を変更する必要があります。詳細については、「アプリケーションフォルダーの管理」を参照してください。
- アプリケーションのプロパティ（設定）は、追加時または後で変更できます。「アプリケーションプロパティの変更」を参照してください。同じ名前の2つのアプリケーションを同じユーザーに公開する場合、Web Studioで「**アプリケーション名（ユーザー向け）**」プロパティを変更します。そうしないと、ユーザーはCitrix Workspaceアプリで重複する名前を目にします。
- アプリケーションを複数のアプリケーショングループに追加する場合、それらのすべてのグループでアプリケーションを表示するのに十分な権限がないと、表示の問題が発生する可能性があります。そのような場合は、より高い権限を持つ管理者に相談するか、アプリケーションが追加されたすべてのグループを含むようにスコープを拡張してください。

アプリケーションソースを表示するには、ドロップダウンメニューから「**追加**」をクリックします。

- **スタートメニューから**：選択したデリバリーグループ内のマシンで検出されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストが表示された新しいページが起動します。追加するアプリケーションのチェックボックスをオンにして、「**OK**」をクリックします。

  以下のいずれかを選択した場合、このソースは選択できません。

  - 関連付けられたデリバリーグループがないアプリケーショングループ。
  - 関連付けられたデリバリーグループにマシンが含まれていないアプリケーショングループ。
  - マシンが含まれていないデリバリーグループ。

- **手動で定義**：サイト内またはネットワーク内の別の場所にあるアプリケーション。このソースを選択すると、実行可能ファイルへのパス、作業ディレクトリ、オプションのコマンドライン引数、管理者とユーザーの表示名を入力する新しいページが起動します。この情報を入力したら、「**OK**」をクリックします。
- **既存**：以前にサイトに追加されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストが表示された新しいページが起動します。追加するアプリケーションのチェックボックスをオンにして、「**OK**」をクリックします。サイトにアプリケーションがない場合、このソースは選択できません。
- **App-V**：App-Vパッケージ内のアプリケーション。このソースを選択すると、**App-Vサーバー**または**アプリケーションライブラリ**を選択する新しいページが起動します。表示された画面から、追加するアプリケーションのチェックボックスをオンにして、「**OK**」をクリックします。詳細については、「App-Vアプリケーションの展開と配信」を参照してください。サイトでApp-Vが構成されていない場合、このソースは選択できません（または表示されない場合があります）。

記載されているように、「**追加**」ドロップダウンメニューの一部のエントリは、その種類の有効なソースがない場合、選択できません。互換性のないソースはまったく表示されません（たとえば、アプリケーショングループにアプリケーショングループを追加することはできないため、アプリケーショングループを作成するときにそのソースは表示されません）。

ステップ4. スコープ

このページは、以前にカスタムスコープを作成した場合にのみ表示されます。デフォルトでは、**すべて**のスコープが選択されています。詳細については、委任管理を参照してください。

ステップ5. 概要

アプリケーショングループの名前を入力します。説明を（オプションで）入力することもできます。

概要情報を確認し、**「完了」**をクリックします。

アプリケーショングループの管理

> **注:**
>
> バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

はじめに

この記事では、作成したアプリケーショングループを管理する方法について説明します。

アプリケーショングループまたはデリバリーグループ内のアプリケーションの管理方法については、アプリケーションを参照してください。これには、以下の方法が含まれます。

- アプリケーショングループ内のアプリケーションを追加または削除する。
- アプリケーショングループの関連付けを変更する。

アプリケーショングループの管理には、Delivery Group Administratorの組み込みロールの委任管理権限が必要です。詳細については、委任管理を参照してください。

アプリケーショングループを有効または無効にする

アプリケーショングループが有効になっている場合、そのグループに追加されたアプリケーションを配信できます。アプリケーショングループを無効にすると、そのグループ内の各アプリケーションが無効になります。ただし、それらのアプリケーションが他の有効なアプリケーショングループにも関連付けられている場合、それらの他のグループから配信できます。アプリケーションがアプリケーショングループに関連付けられたデリバリーグループに明示的に追加された場合、アプリケーショングループを無効にしても、それらのデリバリーグループ内のアプリケーションには影響しません。

アプリケーショングループは作成時に有効になります。グループ作成時にこの設定を変更することはできません。

1. 左ペインで**アプリケーション**を選択し、**アプリケーショングループ**タブを選択します。
2. アプリケーショングループを選択し、アクションバーで**アプリケーショングループの編集**を選択します。
3. **設定**ページで、**アプリケーショングループを有効にする**チェックボックスをオンまたはオフにします。
4. ウィンドウを開いたままにするには**適用**をクリックし、変更を適用してウィンドウを閉じるには**保存**をクリックします。

アプリケーショングループ間のアプリケーションセッション共有を有効または無効にする

アプリケーションセッション共有は、アプリケーショングループの作成時に有効になります。この構成は、グループの作成時に変更できません。詳細については、「アプリケーショングループとのセッション共有」を参照してください。

1. 左側のペインで を選択し、 タブを選択します。
2. アプリケーショングループを選択し、アクションバーで を選択します。
3. ページで、 チェックボックスをオンまたはオフにします。
4. をクリックしてウィンドウを開いたままにするか、 をクリックして変更を適用し、ウィンドウを閉じます。

アプリケーショングループ内でのアプリケーションセッション共有を無効にする

同じアプリケーショングループ内のアプリケーション間でのセッション共有は、アプリケーショングループの作成時にデフォルトで有効になります。アプリケーショングループ間でのアプリケーションセッション共有を無効にしても、同じアプリケーショングループ内のアプリケーション間でのセッション共有は有効のままです。

PowerShell SDKを使用して、アプリケーションセッション共有を無効にしたアプリケーショングループを構成できます。場合によっては、このオプションが望ましいことがあります。たとえば、ユーザーに非シームレスアプリケーションを別のモニターの全画面表示アプリケーションウィンドウで起動させたい場合があります。

アプリケーショングループ内でアプリケーションセッション共有を無効にすると、そのグループ内の各アプリケーションは新しいアプリケーションセッションで起動します。同じアプリケーションを実行している適切な切断されたセッションが利用可能な場合、そのセッションが再接続されます。たとえば、メモ帳を実行している切断されたセッションがある状態でメモ帳を起動すると、新しいセッションを作成する代わりにそのセッションが再接続されます。複数の適切な切断されたセッションが利用可能な場合、ランダムではあるものの決定論的な方法で、いずれかのセッションが再接続のために選択されます。同じ状況が再発した場合、同じセッションが選択されますが、それ以外の場合にセッションが予測可能であるとは限りません。

PowerShell SDKを使用して、既存のアプリケーショングループ内のすべてのアプリケーションのアプリケーションセッション共有を無効にするか、アプリケーションセッション共有を無効にしたグループを作成します。

PowerShellコマンドレットの例

セッション共有を無効にするには、Broker PowerShellコマンドレット `New-BrokerApplicationGroup` または `Set-BrokerApplicationGroup` を使用し、パラメーター `SessionSharingEnabled` を `False` に、パラメーター `SingleAppPerSession` を `True` に設定します。

- たとえば、グループ内のすべてのアプリケーションでアプリケーションセッション共有を無効にしたアプリケーショングループを作成するには、次のようにします。

  ```
  New-BrokerApplicationGroup AppGr1 -SessionSharingEnabled $False -SingleAppPerSession $True
  ```

- たとえば、既存のアプリケーショングループ内のすべてのアプリケーション間でアプリケーションセッション共有を無効にするには、次のようにします。

  ```
  Set-BrokerApplicationGroup AppGR1 -SessionSharingEnabled $False -SingleAppPerSession $True
  ```

考慮事項

- `SingleAppPerSession` プロパティを有効にするには、`SessionSharingEnabled` プロパティを False に設定する必要があります。両方のプロパティを同時に有効にすることはできません。`SessionSharingEnabled` パラメーターは、アプリケーショングループ間のセッション共有を指します。
- アプリケーションセッション共有は、アプリケーショングループに関連付けられているがデリバリーグループには関連付けられていないアプリケーションでのみ機能します。デリバリーグ

ループに直接関連付けられているすべてのアプリケーションは、デフォルトでセッションを共有します。

- アプリケーションが複数のアプリケーショングループに割り当てられている場合は、グループの設定が競合しないようにしてください。たとえば、一方のグループのオプションが `True` に設定され、もう一方のグループのオプションが `False` に設定されている場合、予期しない動作が発生します。

アプリケーショングループの名前を変更する

1. 左側のペインで を選択し、 タブを選択します。
2. アプリケーショングループを選択し、アクションバーで を選択します。
3. 新しい一意の名前を指定し、 をクリックします。

アプリケーショングループとのデリバリーグループの関連付けを追加、削除、または優先度を変更する

アプリケーショングループは、アプリケーションを配信できる共有（プライベートではない）マシンを含むデリバリーグループに関連付けることができます。

以下の両方の条件が満たされている場合、デスクトップのみを配信する共有マシンを含むデリバリーグループを選択することもできます。

- デリバリーグループには共有マシンが含まれており、バージョン7.9より前のバージョンで作成されました。
- デリバリーグループの編集権限があること。

ダイアログがコミットされると、デリバリーグループの種類は自動的に「デスクトップとアプリケーション」に変換されます。

1. 左側のペインで を選択し、 タブを選択します。
2. アプリケーショングループを選択し、アクションバーで を選択します。
3. ページを選択します。
4. デリバリーグループを追加するには、 をクリックします。利用可能なデリバリーグループのチェックボックスをオンにします。（互換性のないデリバリーグループは選択できません。）選択が完了したら、 をクリックします。
5. デリバリーグループを削除するには、削除するグループのチェックボックスをオンにして、 をクリックします。確認を求められたら削除を確定します。

6. デリバリーグループの優先度を変更するには、デリバリーグループのチェックボックスをオンにして、 をクリックします。優先度（0 = 最高）を入力し、 をクリックします。
7. 変更を適用してウィンドウを開いたままにするには、**適用**をクリックするか、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

アプリケーショングループのタグ制限を追加、変更、または削除する

タグ制限の追加、変更、削除は、アプリケーション起動の対象となるマシンに予期せぬ影響を与える可能性があります。タグの考慮事項と注意事項を確認してください。

1. 左側のペインで**アプリケーション**を選択し、**アプリケーショングループ**タブを選択します。
2. アプリケーショングループを選択し、アクションバーで**アプリケーショングループの編集**を選択します。
3. **デリバリーグループ**ページを選択します。
4. タグ制限を追加するには、**タグを持つマシンへの起動を制限する**を選択し、ドロップダウンリストからタグを選択します。
5. タグ制限を変更または削除するには、別のタグを選択するか、**このタグを持つマシンへの起動を制限する**のチェックを外してタグ制限を完全に削除します。
6. 変更を適用してウィンドウを開いたままにするには、**適用**をクリックするか、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

アプリケーショングループのユーザーを追加または削除する

ユーザーの詳細については、「アプリケーショングループの作成」を参照してください。

1. 左側のペインで**アプリケーション**を選択し、**アプリケーショングループ**タブを選択します。
2. アプリケーショングループを選択し、アクションバーで**アプリケーショングループの編集**を選択します。
3. **ユーザー**ページを選択します。関連付けられたデリバリーグループのすべてのユーザーにアプリケーショングループ内のアプリケーションの使用を許可するか、特定のユーザーとグループのみに許可するかを指定します。ユーザーを追加するには、**追加**をクリックし、追加するユーザーを指定します。ユーザーを削除するには、1人以上のユーザーを選択し、**削除**をクリックします。
4. 変更を適用してウィンドウを開いたままにするには、**適用**をクリックするか、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

アプリケーショングループ内のアプリケーションアイコンを追加、変更、または削除する

アプリケーションアイコンを追加、変更、または削除するには、次の手順を実行します。

1. 左ペインで **Applications** を選択します。
2. **Applications** タブで、アプリケーションを選択し、**Properties** を選択します。

   アプリケーショングループレベルで変更を行うには、**Application Groups** タブに移動し、グループ内のアプリケーションを選択して、**Properties** を選択します。
3. **Delivery** ページを選択し、**Change** を選択します。**Select Icon** ウィンドウが表示されます。
4. **Select Icon** ウィンドウで、次のいずれかを実行します。

   - アイコンを追加するには、**Add** を選択し、アイコンを参照します。
   - アイコンを削除するには、アイコンを選択し、**Remove** を選択します。
   - アイコンを変更するには、アプリケーションのアイコンを選択します。

   > **重要:**
   >
   > - サイズが200 KBを超えるアイコンを追加することはできません。
   > - .iconファイルのみを追加できます。
   > - 組み込みアイコンを削除することはできません。
   > - 使用中のアプリケーションのアイコンを削除することはできません。

5. **Save** を選択して変更を適用し、ウィンドウを閉じます。

アプリケーショングループのスコープを変更する

スコープは、作成した場合にのみ変更できます (すべてのスコープは編集できません)。詳細については、「委任管理」を参照してください。

1. 左側のペインで を選択し、次に タブを選択します。
2. アプリケーショングループを選択し、次にアクションバーで を選択します。
3. ページを選択します。スコープの横にあるチェックボックスをオンまたはオフにします。
4. 加えた変更を適用してウィンドウを開いたままにするには をクリックするか、変更を適用してウィンドウを閉じるには をクリックします。

アプリケーショングループのスコープを変更する

スコープは、作成した場合にのみ変更できます (すべてのスコープは編集できません)。詳細については、「委任管理」を参照してください。

1. 左側のペインで を選択し、次に タブを選択します。
2. アプリケーショングループを選択し、次にアクションバーで を選択します。
3. ページを選択します。変更するスコープの横にあるチェックボックスをオンまたはオフにします。
4. 加えた変更を適用してウィンドウを開いたままにするには を選択するか、変更を適用してウィンドウを閉じるには を選択します。

アプリケーショングループを削除する

アプリケーションは、少なくとも1つのデリバリーグループまたはアプリケーショングループに関連付けられている必要があります。アプリケーショングループを削除した結果、1つ以上のアプリケーションがどのグループにも属さなくなった場合、そのグループを削除するとそれらのアプリケーションも削除されるという警告が表示されます。その後、削除を確定またはキャンセルできます。

アプリケーションを削除しても、元のソースから削除されるわけではありません。ただし、再度利用可能にする場合は、もう一度追加する必要があります。

1. 左ペインで**アプリケーション**を選択し、**アプリケーション グループ**タブを選択します。
2. アプリケーション グループを選択し、アクション バーで**グループの削除**を選択します。
3. プロンプトが表示されたら、削除を確定します。

フォルダーを使用してアプリケーション グループを整理する

フォルダーを作成してアプリケーション グループを整理し、簡単にアクセスできるようにすることができます。

必要な役割

デフォルトでは、次の組み込みロールのいずれかを持っている場合、アプリケーション グループのフォルダーを作成および管理できます。

- クラウド管理者
- フル管理者
- アプリケーション グループ管理者

カスタム ロールを作成することで、管理アクションを他のユーザーに委任できます。次の表に、各アクションに必要な権限を示します。

アクション	必要な権限
アプリケーション グループ フォルダーの作成	アプリケーション グループ フォルダーの作成
アプリケーション グループ フォルダーの削除	アプリケーション グループ フォルダーの削除
アプリケーション グループ フォルダーの移動	アプリケーション グループ フォルダーの移動
アプリケーショングループフォルダーの名前を変更	アプリケーショングループフォルダーの編集
アプリケーショングループをフォルダーに移動	アプリケーショングループフォルダーの編集、アプリケーショングループプロパティの編集

詳しくは、「役割の作成と管理」を参照してください。

フォルダーの作成と管理

アクションバーまたは右クリックメニューを使用して、アプリケーショングループフォルダーを作成および管理できます。さらに、アプリケーショングループまたはフォルダーをフォルダーツリー内の目的の場所にドラッグすることもできます。

知っておくと良いこと:

- フォルダーは最大5レベルまでネストできます（デフォルトのルートフォルダーを除く）。
- フォルダーには、アプリケーショングループとサブフォルダーを含めることができます。フォルダーを削除できるのは、そのフォルダーとサブフォルダーにアプリケーショングループが含まれていない場合のみです。
- Web Studioのすべてのノード（**マシンカタログ**、**デリバリーグループ**、**アプリケーション**、**アプリケーショングループ**など）は、バックエンドで同じフォルダーツリーを共有します。フォルダーの名前変更または移動時に名前の競合を避けるため、異なるノード間で最上位フォルダーに一意の名前を使用してください。

  `New-BrokerAdminFolder` SDKコマンドレットを使用してフォルダーを作成し、それを**アプリケーショングループ**ノードの下に表示させたい場合は、`Set-BrokerAdminFolderMetadata` コマンドレットを使用して `ContainsApplicationGroups` メタデータを追加する必要があります。

例:

```
Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
ContainsApplicationGroups -Value true
```

リモートPCアクセス

注:

バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

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

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

この機能は、**Remote PC Access**タイプのマシンカタログで構成されており、次の機能を提供します。

- OUを指定してマシンを追加する機能。この機能により、PCの一括追加が容易になります。
- オフィスWindows PCにログオンするユーザーに基づいた自動ユーザー割り当て。シングルユーザーおよび複数ユーザーの割り当てをサポートしています。デフォルトでは、次に割り当てられていないマシンに複数のユーザーを自動的に割り当てます。自動割り当てをシングル

ユーザーに制限するには、Web Studioにサインインし、**設定**に移動して、**Remote PC Access の複数ユーザーの自動割り当てを有効にする**設定をオフにします。

Citrix Virtual Apps and Desktopsは、他の種類のマシンカタログを使用することで、物理PCのより多くのユースケースに対応できます。これらのユースケースには、次のものが含まれます。

- 物理Linux PC
- プールされた物理PC（つまり、ランダムに割り当てられ、専用ではないもの）

> **注:**
>
> サポートされているOSバージョンの詳細については、シングルセッションOSおよびLinux VDAのVDAのシステム要件を参照してください。

> オンプレミス展開の場合、Remote PC AccessはCitrix Virtual Apps and Desktops AdvancedまたはPremiumライセンスでのみ有効です。セッションは、他のCitrix Virtual Desktops™ セッションと同じ方法でライセンスを消費します。Citrix Cloudの場合、Remote PC AccessはCitrix DaaS（旧Citrix Virtual Apps and Desktopsサービス）およびWorkspace Premium Plusで有効です。

考慮事項

Citrix Virtual Apps and Desktops全般に適用されるすべての技術要件と考慮事項はRemote PC Accessにも適用されますが、物理PCの使用事例により関連性が高い、または排他的なものもあります。

> **重要:**
>
> Windows 11物理システム（および一部のWindows 10を実行しているシステム）には、仮想化ベースのセキュリティ機能が含まれており、その結果、VDAソフトウェアがそれらを仮想マシンとして誤って検出します。この問題を軽減するには、以下のオプションがあります。

> - VDAコマンドラインインストールの一部として、「/remotepc」オプションとともに「/physicalmachine」オプションを使用する

- 以前に言及したオプションを使用しなかった場合は、VDAのインストール後に次のレジストリ値を追加します `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`
  - 名前: ForceEnableRemotePC
  - 種類: DWORD
  - データ: 1

展開に関する考慮事項

Remote PC Accessの展開を計画する際には、いくつかの一般的な決定を下します。

- 既存のCitrix Virtual Apps and Desktops展開にRemote PC Accessを追加できます。このオプションを選択する前に、次の点を考慮してください。
  - 現在のDelivery ControllerまたはCloud Connectorは、Remote PC Access VDAに関連する追加の負荷をサポートするために適切にサイジングされていますか？
  - オンプレミスサイトのデータベースおよびデータベースサーバーは、Remote PC Access VDAに関連する追加の負荷をサポートするために適切にサイジングされていますか？
  - 既存のVDAと新しいRemote PC Access VDAは、サイトあたりの最大サポートVDA数を超えますか？
- VDAは自動プロセスを通じてオフィスPCに展開する必要があります。利用可能なオプションは次のとおりです。
  - SCCMなどの電子ソフトウェア配布 (ESD) ツール: SCCMを使用してVDAをインストールする。
  - 展開スクリプト: スクリプトを使用してVDAをインストールする。
- Remote PC Accessのセキュリティに関する考慮事項を確認してください。

注:

Remote PC Access を設計する際は、リモート PC の GPU に接続され、現在構成/動作している物理モニターの数を考慮する必要があります。モニターが Citrix セッションで使用されていなくても、GPU によって検出された場合、そのモニターの存在は GPU がサポートする最大モニター数にカウントされます。

マシンカタログに関する考慮事項

必要なマシンカタログの種類は、ユースケースによって異なります。

- Remote PC Accessマシンカタログ
  - Windows専用PC
  - Windows専用マルチユーザーPC。このユースケースは、複数のユーザーが異なるシフトでリモートからアクセスできる物理的なオフィスPCに適用されます。
  - プールされたWindows PC。このユースケースは、コンピューターラボのように、複数のランダムなユーザーがアクセスできる物理PCに適用されます。
- シングルセッションOSマシンカタログ
  - 静的 - 専用Linux PC
  - ランダム - プールされたLinux PC

マシンカタログの種類を特定したら、次の点を考慮してください。

- 1台のマシンは、一度に1つのマシンカタログにのみ割り当てることができます。
- 委任された管理を容易にするために、地理的な場所、部門、または各カタログの管理を適切な管理者に委任しやすくするその他のグループに基づいてマシンカタログを作成することを検討してください。
- マシンアカウントが存在するOUを選択する際は、より詳細な粒度を得るために下位レベルのOUを選択します。そのような粒度が必要ない場合は、上位レベルのOUを選択できます。たとえば、Bank/Officers/Tellersの場合、より詳細な粒度を得るには**Tellers**を選択します。それ以外の場合は、要件に基づいて**Officers**または**Bank**を選択できます。
- Remote PC Accessマシンカタログに割り当てられた後にOUを移動または削除すると、VDAの関連付けに影響を与え、今後の割り当てで問題が発生します。したがって、マシンカタログのOU割り当ての更新がActive Directoryの変更計画で考慮されるように、適切に計画してください。
- OU構造のためにマシンカタログにマシンを追加するOUを選択するのが容易でない場合、OUを選択する必要はありません。後でPowerShellを使用してカタログにマシンを追加できます。デリバリーグループでデスクトップ割り当てが正しく構成されていれば、ユーザーの自動割り当ては引き続き機能します。ユーザー割り当てとともにマシンカタログにマシンを追加するサンプルスクリプトは、GitHubで入手できます。
- 統合されたWake on LANは、**Remote PC Access**タイプのマシンカタログでのみ利用可能です。

Linux VDAに関する考慮事項

以下の考慮事項は、Linux VDAに固有のものです。

- 物理マシンでは、Linux VDAを非3Dモードでのみ使用してください。NVIDIAドライバーの制限により、HDX 3Dモードが有効になっている場合、PCのローカル画面をブラックアウトできず、セッションのアクティビティが表示されます。この画面を表示することはセキュリティリスクです。
- 物理Linuxマシンには、シングルセッションOSタイプのマシンカタログを使用します。
- 自動ユーザー割り当てはLinuxマシンでは利用できません。
- ユーザーがすでにローカルでPCにログオンしている場合、StoreFront™からPCを起動しようとすると失敗します。
- 省電力オプションはLinuxマシンでは利用できません。

技術要件と考慮事項

このセクションでは、物理PCの技術要件と考慮事項について説明します。

- 以下はサポートされていません。
  - KVMスイッチ、またはセッションを切断できるその他のコンポーネント。
  - ハイブリッドPC（オールインワンPC、NVIDIA Optimus搭載ノートPC、PCを含む）。
  - デュアルブートマシン。
- キーボードとマウスはPCに直接接続してください。モニターや、電源を切ったり切断したりできるその他のコンポーネントに接続すると、これらの周辺機器が利用できなくなる可能性があります。入力デバイスをモニターなどのコンポーネントに接続する必要がある場合は、それらのコンポーネントの電源を切らないでください。
- PCはActive Directory Domain Servicesドメインに参加している必要があります。
- セキュアブートはWindows 10およびWindows 11でのみサポートされています。
- PCにはアクティブなネットワーク接続が必要です。信頼性と帯域幅を向上させるには、有線接続が推奨されます。
- Wi-Fiを使用する場合は、次の操作を行います。

  a. 電源設定でワイヤレスアダプターをオンのままにするように設定します。

  b. ユーザーがログオンする前にワイヤレスネットワークに自動的に接続できるように、ワイヤレスアダプターとネットワークプロファイルを構成します。そうしないと、ユーザーが

ログオンするまでVDAは登録されません。ユーザーがログオンするまで、PCはリモートアクセスに利用できません。

c. Delivery ControllerまたはCloud ConnectorがWi-Fiネットワークから到達可能であることを確認します。

- ラップトップコンピューターでRemote PC Accessを使用できます。ラップトップがバッテリーで動作するのではなく、電源に接続されていることを確認してください。ラップトップの電源オプションをデスクトップPCのオプションと一致するように構成します。例：

  a. 休止状態機能を無効にします。

  b. スリープ機能を無効にします。

  c. 蓋を閉じたときの動作を**何もしない**に設定します。

  d. 「電源ボタンを押したときの動作」を**シャットダウン**に設定します。

  e. ビデオカードとNICの省電力機能を無効にします。

- Remote PC Accessは、Windows 10を搭載したSurface Proデバイスでサポートされています。前述のラップトップと同じガイドラインに従ってください。
- ドッキングステーションを使用している場合、ラップトップのドッキング解除と再ドッキングが可能です。ラップトップをドッキング解除すると、VDAはWi-Fi経由でDelivery ControllerまたはCloud Connectorに再登録されます。ただし、ラップトップを再ドッキングしても、ワイヤレスアダプターを切断しない限り、VDAは有線接続に切り替わりません。一部のデバイスには、有線接続が確立されたときにワイヤレスアダプターを切断する組み込み機能が提供されています。その他のデバイスでは、ワイヤレスアダプターを切断するためにカスタムソリューションまたはサードパーティ製ユーティリティが必要です。前述のWi-Fiに関する考慮事項を確認してください。

  Remote PC Accessデバイスのドッキングとドッキング解除を有効にするには、次の操作を行います。

  a. **スタート**メニューで、**設定 > システム > 電源とスリープ**を選択し、**スリープ**を**なし**に設定します。

  b. 「**デバイスマネージャー > ネットワークアダプター > イーサネットアダプター**」で「**電源の管理**」に移動し、「**電力節約のために、コンピューターでこのデバイスの電源をオフにできるようにする**」のチェックを外します。「**このデバイスで、コンピューターのスタンバイ状態を解除できるようにする**」がオンになっていることを確認してください。

- 同じオフィスPCにアクセスする複数のユーザーには、Citrix Workspaceで同じアイコンが表示されます。ユーザーがCitrix Workspaceにログオンすると、そのリソースが他のユーザーによってすでに使用されている場合、利用不可として表示されます。
- オフィスPCにアクセスする各クライアントデバイス（たとえば、自宅のPC）にCitrix Workspaceアプリをインストールします。

構成シーケンス

このセクションでは、**Remote PC Access**タイプのマシンカタログを使用する場合にRemote PC Accessを構成する方法の概要を説明します。その他の種類のマシンカタログの作成方法については、マシンカタログの作成を参照してください。

1. オンプレミスサイトのみ - 統合されたWake on LAN機能を使用するには、Wake on LANに記載されている前提条件を構成してください。
2. Remote PC Access用に新しいCitrix Virtual Apps and Desktopsサイトが作成された場合：

   a. **Remote PC Access**サイトタイプを選択します。

   b. **電源の管理**ページで、デフォルトのRemote PC Accessマシンカタログの電源管理を有効または無効にするかを選択します。この設定は、後でマシンカタログのプロパティを編集して変更できます。Wake on LANの構成の詳細については、Wake on LANを参照してください。

   c. **ユーザー**ページと**マシンアカウント**ページで情報を入力します。

   これらの手順を完了すると、**Remote PC Access Machines**という名前のマシンカタログと、**Remote PC Access Desktops**という名前のデリバリーグループが作成されます。
3. 既存のCitrix Virtual Apps and Desktopsサイトに追加する場合：

   a. **Remote PC Access**タイプのマシンカタログを作成します（ウィザードの「オペレーティングシステム」ページ）。マシンカタログの作成方法の詳細については、マシンカタログの作成を参照してください。ターゲットPCがRemote PC Accessで使用できるよう、適切なOUを割り当ててください。

   b. マシンカタログ内のPCへのユーザーアクセスを提供するために、デリバリーグループを作成します。デリバリーグループの作成方法の詳細については、デリバリーグループの作成を参照してください。デリバリーグループを、PCへのアクセスを必要とするユーザーを含むActive Directoryグループに割り当ててください。
4. オフィスPCにVDAを展開します。

- シングルセッションOSコアVDAインストーラー（VDAWorkstationCoreSetup.exe）を使用することをお勧めします。
- シングルセッションフルVDAインストーラー（VDAWorkstationSetup.exe）を`/remotepc/physicalmachine`オプションとともに使用することもできます。これは、コアVDAインストーラーを使用した場合と同じ結果になります。

  > **注:**
  >
  > RemotePCのインストールでは、特定のユーザーシナリオでVDAが期待どおりに動作するように、`/physicalmachine`引数を`/remotepc`とともに使用します。

- ヘルプデスクチームがCitrix Directorを介してリモートサポートを提供できるように、Windowsリモートアシスタンスを有効にすることを検討してください。これを行うには、`/enable_remote_assistance`オプションを使用します。詳細については、「コマンドラインを使用したインストール」を参照してください。
- Directorでログオン期間情報を表示するには、シングルセッションのフルVDAインストーラーを使用し、**Citrix User Profile Management WMI Plugin** コンポーネントを含める必要があります。このコンポーネントを含めるには、`/includeadditional`オプションを使用します。詳細については、「コマンドラインを使用したインストール」を参照してください。
- SCCMを使用してVDAを展開する方法については、「SCCMを使用したVDAのインストール」を参照してください。
- 展開スクリプトを使用してVDAを展開する方法については、「スクリプトを使用したVDAのインストール」を参照してください。

手順2～4を正常に完了すると、ユーザーがPCにローカルでログオンしたときに、自分のマシンに自動的に割り当てられます。

5. ユーザーに、オフィスPCにリモートでアクセスするために使用する各クライアントデバイスにCitrix Workspaceアプリをダウンロードしてインストールするよう指示します。Citrix Workspaceアプリは、`https://www.citrix.com/downloads/`またはサポートされているモバイルデバイスのアプリケーションストアから入手できます。

レジストリを介して管理される機能

> **注意:**

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

複数ユーザーの自動割り当てを無効にする

各Delivery Controller™で、次のレジストリ設定を追加します。

`HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer`

- 名前: AllowMultipleRemotePCAssignments
- 種類: DWORD
- データ: 0

スリープモード (最小バージョン 7.16)

Remote PC Accessマシンをスリープ状態にするには、VDAにこのレジストリ設定を追加し、マシンを再起動します。再起動後、オペレーティングシステムの省電力設定が適用されます。事前設定されたアイドルタイマーが経過すると、マシンはスリープモードに入ります。マシンがウェイクアップすると、Delivery Controllerに再登録されます。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 名前: DisableRemotePCSleepPreventer
- 種類: DWORD
- データ: 1

セッション管理

デフォルトでは、ローカルユーザーがそのマシンでセッションを開始したとき（CTRL+ATL+DELを押すことによって）、リモートユーザーのセッションは自動的に切断されます。この自動的な動作を防ぐには、オフィスPCに以下のレジストリエントリを追加し、その後、マシンを再起動します。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- 名前: SasNotification
- 種類: DWORD

- データ: 1

デフォルトでは、接続メッセージがタイムアウト期間内に確認されない場合、リモートユーザーがローカルユーザーよりも優先されます。この動作を設定するには、以下の設定を使用します。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- 名前: RpcaMode
- 種類: DWORD
- データ:
  - 1 - 指定されたタイムアウト期間内にメッセージングUIに応答しない場合、リモートユーザーが常に優先されます。この設定が構成されていない場合、この動作がデフォルトです。
  - 2 - ローカルユーザーが優先されます。

Remote PC Accessモードを適用するためのタイムアウトは、デフォルトで30秒です。このタイムアウトは構成できますが、30秒未満に設定しないでください。タイムアウトを構成するには、このレジストリ設定を使用します。

`HKLM\SOFTWARE\Citrix\PortICA\RemotePC`

- 名前: RpcaTimeout
- 種類: DWORD
- データ: タイムアウトの秒数（10進値）

ユーザーが強制的にコンソールアクセスを取得したい場合: ローカルユーザーは、10秒の間にCtrl+Alt+Delを2回押すことで、リモートセッションのローカル制御を取得し、切断イベントを強制できます。

レジストリ変更とマシンの再起動後、リモートユーザーが使用中にローカルユーザーがCtrl+Alt+Delを押してそのPCにログオンしようとすると、リモートユーザーにプロンプトが表示されます。このプロンプトは、ローカルユーザーの接続を許可するか拒否するかを尋ねます。接続を許可すると、リモートユーザーのセッションは切断されます。

セッション管理のログ記録

Remote PC Accessには、アクティブなICA®セッションを持つPCに誰かがアクセスしようとしたときにログを記録する機能が追加されました。これにより、不要なアクティビティや予期しないア

クティビティがないか環境を監視し、インシデントを調査する必要がある場合にそのようなイベントを監査できます。

イベントはWindowsイベントビューアーを使用してログに記録され、**Applications and Services > Citrix > HostCore > ICA Service > Admin**にあります。

Remote PC Accessを使用すると、3つの異なるイベントがログに記録されます。

Ctrl+Alt+Delイベント

このイベントは、アクティブなリモートセッション中にローカルユーザーがコンソールキーボードでCtrl+Alt+Delを押したときに表示されます。

イベントの詳細

- ログ名: アプリケーションとサービス
- イベントID: 43, 44, 45
- ソース: ICA サービス

イベント ID 43

このイベント ID は、SasNotification レジストリ値が存在しない場合、または SasNotification レジストリ値が 0 の場合に表示されます。

- メッセージ:

```
Ctrl+Alt+Del has been pressed on the endpoint.

The session management behavior is set to automatically disconnect the
remote session.
```

イベント ID 44

このイベント ID は、SasNotification レジストリ値が 1 で、RpcaMode レジストリ値が 1 の場合、または RpcaMode レジストリ値が存在しない場合に表示されます。

- メッセージ:

```
Ctrl+Alt+Del has been pressed on the endpoint.

The session management behavior is set to notify the remote user. The
user preference is set to remote user.
```

イベント ID 45

このイベント ID は、SasNotification レジストリ値が 1 で、RpcaMode レジストリ値が 2 の場合に表示されます。

- メッセージ:

```
Ctrl+Alt+Del has been pressed on the endpoint.

The session management behavior is set to notify the remote user.

The user preference is set to local user.
```

リモートセッション切断イベント

このイベントは、さまざまな理由でリモートセッションが切断された場合に表示されます。

イベントの詳細

- ログ名: アプリケーションとサービス
- イベント ID: 46, 47, 48
- ソース: ICA Service

イベントID 46

このイベントIDは、リモートセッションが切断され、SasNotification レジストリ値が存在しないか、SasNotification レジストリ値が0である場合に表示されます。

- メッセージ:

```
The remote session for &lt;remoteUserName> has been disconnected.
```

イベントID 47

このイベントIDは、リモートユーザーがセッションの切断に同意し、SasNotification レジストリ値が1であり、RpcaMode レジストリ値が1であるか、RpcaMode レジストリ値が2であるか、または RpcaMode レジストリ値が存在しない場合に表示されます。

- メッセージ:

```
The remote session for &lt;remoteUserName> has been disconnected
because the user accepted the request to disconnect the session.
```

イベントID 48

このイベントIDは、リモートユーザーが指定されたタイムアウト期間内に切断要求を拒否せず、SasNotification レジストリ値が1であり、RpcaMode レジストリ値が2である場合に表示されます。

- メッセージ:

```
The remote session for &lt;remoteUserName> has been disconnected
because the user did not decline the disconnection request within the
configured timeout period (&lt;timeout period>).
```

Ctrl+Alt+Del 2回押しイベント

このイベントは、10秒以内にCtrl+Alt+Delが2回押された場合に表示されます。

イベントの詳細

- ログ名: アプリケーションとサービス
- イベントID: 49
- ソース: ICA Service

イベントID 49

このイベントIDは、Ctrl+Alt+Delが10秒以内に2回押されたときに表示されます。

- メッセージ:

```
The remote session for &lt;remoteUserName> has been forcibly
disconnected.
```

Wake on LAN (ウェイク・オン・ラン)

Remote PC AccessはWake on LANをサポートしており、ユーザーは物理PCをリモートで起動できます。この機能により、ユーザーは使用していないときにオフィスPCの電源を切ったままにして、エネルギーコストを節約できます。また、誤ってマシンの電源が切れてしまった場合でも、リモートアクセスを可能にします。

Wake on LAN機能を使用すると、デリバリーコントローラーからの指示があった場合、PC上で実行されているVDAから、そのPCが存在するサブネットにマジックパケットが直接送信されます。これにより、追加のインフラストラクチャコンポーネントやマジックパケット配信のためのサードパーティソリューションに依存することなく、この機能が動作します。

制限事項

Wake on LAN機能を使用するRemote PC Accessは、ピーク時の自動電源オンをサポートしていません。

システム要件

Wake on LAN機能を使用するためのシステム要件は次のとおりです。

- コントロールプレーン:
  - シトリックス DaaS™
  - シトリックス バーチャルアプリおよびデスクトップ 2009以降
- 物理PC:
  - VDAバージョン2009以降
  - Windows 10またはWindows 11。サポートの詳細については、VDAシステム要件を参照してください。
  - BIOS/UEFIでWake on LANが有効になっていること
  - Windows構成内のネットワークアダプターのプロパティでWake on LANが有効になっていること

Wake on LANの構成

Studioを使用したWake on LANの構成

Wake on LAN接続を作成するには:

1. 左側のペインで、**「ホスティング」**ノードを選択します。
2. **接続とリソースの追加**を選択します。
3. ウィザードの**「接続」**ページで、以下を指定します。
   a. 接続の種類: Remote PC Wake on LAN
   b. ゾーン名: Remote PC Accessカタログが存在するゾーンを選択します
   c. 接続名: Wake on LAN接続の名前を入力します
4. 接続とリソースの追加ウィザードの残りの手順を完了します。

Wake on LAN接続をRemote PC Accessマシンカタログに追加するには:

1. 新しいRemote PC Accessマシンカタログを作成している場合は、マシンカタログセットアップウィザードの**マシンタイプ**ページでドロップダウンリストを使用して接続を追加できます。
2. 既存のマシンカタログにWake on LAN接続を追加する場合:
    a. 左側の**マシンカタログ**ノードに移動します。
    b. 適切なRemote PC Accessマシンカタログを選択します。
    c. マシンカタログを右クリックするか、上部の**その他**メニューを選択します。
    d. **マシンカタログの編集**を選択します。
    e. **電源管理**ページで、**はい**を選択します。
    f. ドロップダウンリストから適切な接続を選択します。
    g. **保存**を選択します。

> **注:**
>
> Studio を介した Wake on LAN の構成は、現時点では Citrix DaaS でのみ利用可能です。

PowerShell を使用して Wake on LAN を構成する

PowerShell を使用して Wake on LAN を構成するには：

1. まだ Remote PC Access マシンカタログがない場合は、作成します。
2. まだ Wake on LAN ホスト接続がない場合は、作成します。
3. Wake on LAN ホスト接続の一意の識別子を取得します。
4. Wake on LAN ホスト接続をマシンカタログに関連付けます。

Wake on LAN ホスト接続を作成するには：

```
# Load Citrix SnapIns

Add-PSSnapIn -Name "*citrix*"



# Provide the name of the Wake on LAN host connection

[string]$connectionName = "Remote PC Access Wake on LAN"
```

```
# Create the hypervisor connection

$hypHc = New-Item -Path xdhyp:\Connections `

                -Name $connectionName `

                -HypervisorAddress "N/A" `

                -UserName "woluser" `

                -Password "wolpwd" `

                -ConnectionType Custom `

                -PluginId VdaWOLMachineManagerFactory `

                -CustomProperties "<CustomProperties></CustomProperties>"
`

                -Persist



$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid



# Wait for the connection to be ready before trying to use it

while (-not $bhc.IsReady)

{

    Start-Sleep -s 5

    $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid

}
```

ホスト接続の準備ができたら、次のコマンドを実行してホスト接続の一意の識別子を取得します。

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"

$hypUid = $bhc.Uid
```

接続の一意の識別子を取得したら、次のコマンドを実行して、その接続を Remote PC Access マシンカタログに関連付けます。

```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog
-RemotePCHypervisorConnectionUid $hypUid
```

設計上の考慮事項

Remote PC Access で Wake on LAN を使用する予定がある場合は、次の点を考慮してください。

- 複数のマシンカタログで同じ Wake on LAN ホスト接続を使用できます。
- ある PC が別の PC を起動するには、両方の PC が同じサブネット内にあり、同じ Wake on LAN ホスト接続を使用している必要があります。PC が同じマシンカタログ内にあるか、異なるマシンカタログ内にあるかは関係ありません。
- ホスト接続は特定のゾーンに割り当てられます。展開に複数のゾーンが含まれている場合は、各ゾーンに Wake on LAN ホスト接続が必要です。これはマシンカタログにも当てはまります。
- マジックパケットはグローバルブロードキャストアドレス255.255.255.255を使用してブロードキャストされます。このアドレスがブロックされていないことを確認してください。
- そのサブネット内のマシンを起動できるようにするには、Wake on LAN接続ごとに、サブネット内に少なくとも1台のPCが電源オンになっている必要があります。

運用上の考慮事項

Wake on LAN機能を使用する際の考慮事項は次のとおりです。

- 統合されたWake on LAN機能を使用してPCを起動できるようにするには、VDAが少なくとも1回登録されている必要があります。
- Wake on LANはPCを起動するためにのみ使用できます。再起動やシャットダウンなどの他の電源操作はサポートしていません。

- Wake on LAN接続が作成されると、Web Studioに表示されます。ただし、オンプレミスのCitrix Virtual Apps and Desktopsを使用している場合、Web Studio内でのそのプロパティの編集はサポートされていません。
- マジックパケットは次の2つの方法のいずれかで送信されます。

  a. ユーザーが自分のPCへのセッションを起動しようとし、VDAが未登録の場合

  b. 管理者がWeb StudioまたはPowerShellから手動で電源オンコマンドを送信した場合

- デリバリーコントローラーはPCの電源状態を認識していないため、Web Studioでは電源状態の下に**サポートされていません**と表示されます。デリバリーコントローラーは、VDA登録状態を使用してPCがオンかオフかを判断します。

トラブルシューティング

モニターのブランキングが機能しない

アクティブなHDXセッション中にWindows PCのローカルモニターが空白にならない場合（ローカルモニターにセッションで発生していることが表示される場合）、それはGPUベンダーのドライバーの問題である可能性があります。この問題を解決するには、次のレジストリ値を設定して、Citrix Indirect Display driver (IDD) にグラフィックカードのベンダードライバーよりも高い優先順位を与えます。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits`

- 名前: CitrixIDD
- 種類: DWORD
- データ: 3

ディスプレイアダプターの優先順位とモニターの作成の詳細については、Knowledge Centerの記事CTX237608を参照してください。

セッション管理通知が有効になっているマシンでCtrl+Alt+Delを選択すると、セッションが切断されます

SasNotificationレジストリ値によって制御されるセッション管理通知は、VDAでRemote PC Accessモードが有効になっている場合にのみ機能します。物理PCでHyper-Vの役割または仮想化ベースのセキュリティ機能が有効になっている場合、そのPCは仮想マシンとして報告されます。VDAが仮想マシン上で実行されていることを検出すると、Remote PC Accessモードを自動的に無効にします。Remote PC Accessモードを有効にするには、次のレジストリ値を追加します。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 名前: ForceEnableRemotePC
- 種類: DWORD
- データ: 1

設定を有効にするには、PCを再起動します。

診断情報

Remote PC Accessに関する診断情報は、Windowsアプリケーションイベントログに書き込まれます。情報メッセージはスロットリングされません。エラーメッセージは、重複するメッセージを破棄することでスロットリングされます。

- 3300（情報）: マシンがカタログに追加されました
- 3301（情報）: マシンがデリバリーグループに追加されました
- 3302（情報）: マシンがユーザーに割り当てられました
- 3303 (エラー): 例外

電源管理

Remote PC Accessの電源管理が有効になっている場合、サブネット指向ブロードキャストでは、Controllerとは異なるサブネットにあるマシンを起動できないことがあります。サブネット指向ブロードキャストを使用してサブネット間で電源管理が必要で、AMTサポートが利用できない場合は、Wake-upプロキシまたはユニキャスト方式を試してください。これらの設定が電源管理接続の詳細プロパティで有効になっていることを確認してください。

アクティブなリモートセッションはローカルのタッチスクリーン入力を記録します

VDA が Remote PC Access モードを有効にすると、マシンはアクティブなセッション中にローカルのタッチスクリーン入力を無視します。物理 PC で Hyper-V ロールまたは仮想化ベースのセキュリティ機能が有効になっている場合、その PC は仮想マシンとして報告されます。VDA が仮想マシン上で実行されていることを検出すると、Remote PC Access モードを自動的に無効にします。Remote PC Access モードを有効にするには、次のレジストリ設定を追加します。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 名前: ForceEnableRemotePC
- 種類: DWORD
- データ: 1

設定を有効にするには、PC を再起動してください。

その他のリソース

以下は Remote PC Access に関するその他のリソースです。

- ソリューション設計ガイダンス: Remote PC Access Design Decisions。
- Remote PC Access アーキテクチャの例: Citrix Remote PC Access ソリューションのリファレンスアーキテクチャ。

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

If using on-premises Site aggregation with Citrix Workspace™ or using Citrix Gateway Service with StoreFront, Cloud Connectors handle Secure Ticket Authority (STA) traffic for your Citrix Virtual Apps and Desktops™ site. The standalone STA service enables you to have more control over the delivery of STA tickets in your environment.

The standalone Citrix STA service is installed on every Cloud Connector in a Resource Location by default. The standalone STA service shifts STA ticketing from the Citrix Cloud™ ticketing service to the Cloud Connectors and standardizes ticketing operations across both normal and LHC modes. The standalone STA service reduces reliance on cloud services and reduces intermittent LHC events.

システム要件

- オンプレミスStoreFront™を使用している場合: バージョン2311以降
- デリバリーコントローラー™: 2503以降

スタンドアロンSTAサービスを有効にする

オンプレミスのDelivery ControllersでCitrix Gateway Serviceを有効にし、Citrix Workspaceサービスへのオンプレミスサイト集約の回復力を向上させるスタンドアロンSTAサービスを有効にするには、次のレジストリキーを構成します。

1. お使いのCloud Connectorsで、レジストリキー `HKEY_LOCAL_MACHINE\Software\Citrix\XaXdCloudProxyPersist\StandaloneStaServiceForced` を `1` に設定します。

名前: `StandaloneStaServiceForced` 種類: DWORD 値: 1

レジストリキーが構成されたら、変更を有効にするには、Citrix Remote Broker Provider Service を再起動します。

重要な考慮事項

- オンプレミス環境でCitrix WorkspaceとオンプレミスCitrix Gatewayを使用する場合、ワークスペースでのVirtual Apps and Desktopsの集約を参照してください。
- オンプレミスのStoreFrontをCitrix Gateway Serviceで使用する場合、StoreFront用Citrix Gateway Serviceを参照してください。
- オンプレミスのStoreFrontを構成して、Cloud ConnectorsのFQDNをSTAサーバーとして使用します。オンプレミスのNetScaler® Gateway vServerには、StoreFrontで指定されているものと一致する、STAとして構成されたCloud Connectorsの完全なリストを含める必要があります。
- オンプレミスのNetScaler Gateway vServerをICA®プロキシとしてCitrix Workspaceで使用している場合: すべてのCloud ConnectorsをSTAサーバーとして使用するようにNetScaler Gatewaysを構成します。

制限事項

- デュアルSTAチケットの引き換えはCitrix Workspaceではサポートされていません。
- クラウドテナントでDaaSが構成されていない場合、構成同期は実行されず、イベントログに517エラーが記録されます。

コンテンツの公開

> **注:**
>
> バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

Microsoft WordドキュメントやWebリンクなど、リソースへのURLまたはUNCパスであるアプリケーションを公開できます。この機能は「公開コンテンツ」として知られています。コンテンツを公開する機能により、ユーザーへのコンテンツ配信方法に柔軟性が加わります。既存のアクセス制御とアプリケーション管理の恩恵を受けることができます。また、コンテンツを開くためにローカルアプリケーションを使用するか、公開アプリケーションを使用するかを指定することもできます。

公開されたコンテンツは、StoreFront™およびCitrix Workspace™アプリの他のアプリケーションと同様に表示されます。ユーザーはアプリケーションにアクセスするのと同じ方法でアクセスします。クライアントでは、リソースは通常どおり開きます。

- ローカルにインストールされたアプリケーションが適切な場合、そのアプリケーションが起動されてリソースが開かれます。
- ファイルの種類に関連付けが定義されている場合、公開されたアプリケーションが起動されてリソースが開かれます。

コンテンツはPowerShell SDKを使用して公開します。Web Studioを使用してコンテンツを公開することはできません。ただし、公開後にWeb Studioを使用してアプリケーションのプロパティを編集することはできます。

構成の概要と準備

コンテンツの公開には、次の主要なプロパティを持つ `New-BrokerApplication` コマンドレットを使用します。（すべてのコマンドレットプロパティの説明については、コマンドレットのヘルプを参照してください。）

```
New-BrokerApplication –ApplicationType PublishedContent
-CommandLineExecutable location -Name app-name -DesktopGroup delivery-
group-name
```

`ApplicationType` プロパティは `PublishedContent` である必要があります。

`CommandLineExecutable` プロパティは、公開コンテンツの場所を指定します。以下の形式がサポートされており、255文字の制限があります。

- HTMLウェブサイトアドレス（例: `<http://www.citrix.com>`）
- ウェブサーバー上のドキュメントファイル（例: `https://www.citrix.com/press/pressrelease.doc`）
- FTPサーバー上のディレクトリ（例: `ftp://ftp.citrix.com/code`）
- FTPサーバー上のドキュメントファイル（例: `ftp://ftp.citrix.com/code/Readme.txt` >）
- UNC ディレクトリパス (例: `file://myServer/myShare or \\\\myServer\\myShare`)
- UNC ファイルパス (例: `file://myServer/myShare/myFile.asf` または `\\myServer\myShare\myFile.asf`)

正しいSDKがあることを確認してください。

- Citrix DaaS (旧Citrix Virtual Apps and Desktopsサービス) の展開の場合、ダウンロード して、Citrix Virtual Apps and Desktops Remote PowerShell SDKをインストールします。
- オンプレミスのCitrix Virtual Apps and Desktops展開の場合、Delivery Controllerとともにインストールされているの PowerShell SDKを使用します。公開コンテンツアプリケーションを追加するには、最低バージョン7.11のDelivery Controllerが必要です。

以下の手順では例を使用します。例では、次のようになります:

- マシンカタログが作成されています。
- `PublishedContentApps` という名前のデリバリーグループが作成されています。このグループは、カタログからマルチセッションOSマシンを使用します。WordPadアプリケーションがグループに追加されています。
- デリバリーグループ名、`CommandLineExecutable` の場所、およびアプリケーション名が割り当てられます。

はじめに

PowerShell SDKを含むマシンで、PowerShellを開きます。

次のコマンドレットは、適切なPowerShell SDKスナップインを追加し、返されたデリバリーグループレコードを割り当てます。

`Add-PsSnapin Citrix* $dg = Get-BrokerDesktopGroup –Name PublishedContentApps`

Citrix DaaSを使用している場合は、Citrix Cloud™の資格情報を入力して認証します。複数の顧客がいる場合は、1つを選択します。

URLを公開する

場所とアプリケーション名を割り当てた後、次のコマンドレットは、Citrixのホームページをアプリケーションとして公開します。

```
$citrixUrl = "https://www.citrix.com/"

$appName = "Citrix Home Page"
```

```
New-BrokerApplication –ApplicationType PublishedContent –
CommandLineExecutable $citrixURL –Name $appName –DesktopGroup $dg.Uid
```

成功を確認します:

- StoreFrontを開き、PublishedContentAppsデリバリーグループ内のアプリケーションにアクセスできるユーザーとしてログオンします。デフォルトのアイコンを持つ新しく作成されたアプリケーションが表示されます。アイコンのカスタマイズについては、`<https://www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-xd7/>`を参照してください。
- **Citrix Home Page**アプリケーションをクリックします。URLは、ローカルで実行されているデフォルトブラウザの新しいタブで起動します。

UNCパスにあるリソースを公開する

この例では、管理者は`PublishedResources`という名前の共有をすでに作成しています。場所とアプリケーション名を割り当てた後、以下のコマンドレットはその共有内のRTFファイルとDOCXファイルをリソースとして公開します。

```
$rtfUNC = "\\GMSXJ-EDGE0.xd.local\\PublishedResources\\PublishedRTF.rtf"

$rtfAppName = "PublishedRTF"



New-BrokerApplication –ApplicationType PublishedContent

–CommandLineExecutable $rtfUNC -Name $rtfAppName

-DesktopGroup $dg.Uid



$docxUNC = "\\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedDOCX.docx"

$docxAppName = "PublishedDOCX"



New-BrokerApplication –ApplicationType PublishedContent
```

```
–CommandLineExecutable $docxUNC -Name $docxAppName

-DesktopGroup $dg.Uid
```

成功を確認する:

- StoreFrontウィンドウを更新して、新しく公開されたドキュメントを表示します。
- **PublishedRTF**および**PublishedDOCX**アプリケーションをクリックします。各ドキュメントは、ローカルで実行されているWordPadで開きます。

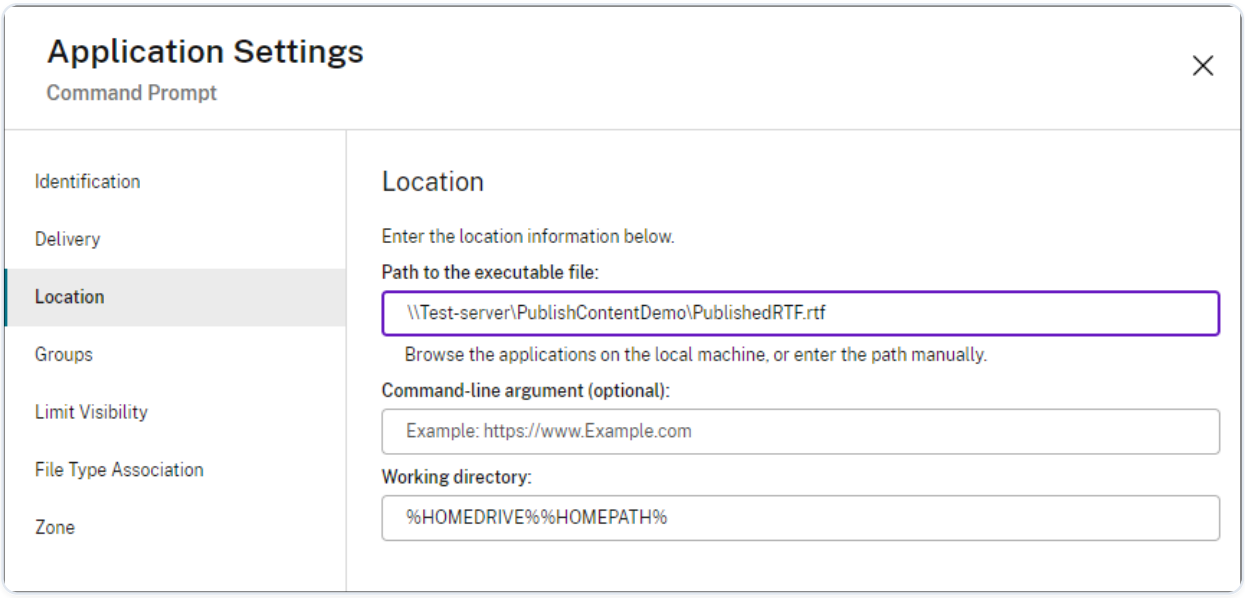
PublishedContentアプリケーションの表示と編集

公開されたコンテンツは、他のアプリケーションタイプに使用するのと同じ方法で管理します。

`PublishedContent`アプリケーションを表示および編集するには、次の手順に従います。

1. Web Studioにサインインし、左ペインで**アプリケーション**を選択します。
2. **アプリケーション**タブで、PublishedContentアプリケーションを選択し、**プロパティ**を選択します。

   アプリケーションのプロパティ（ユーザーの可視性、グループの関連付け、ショートカットなど）は、公開されたコンテンツに適用されます。ただし、**場所**ページでは、コマンドライン引数または作業ディレクトリのプロパティを変更することはできません。
3. リソースを変更するには、そのページの**実行可能ファイルへのパス**フィールドを変更します。



4. 公開アプリケーションを使用して`PublishedContent`アプリケーション（ローカルアプリケーションではなく）を開くには、次の手順に従います。

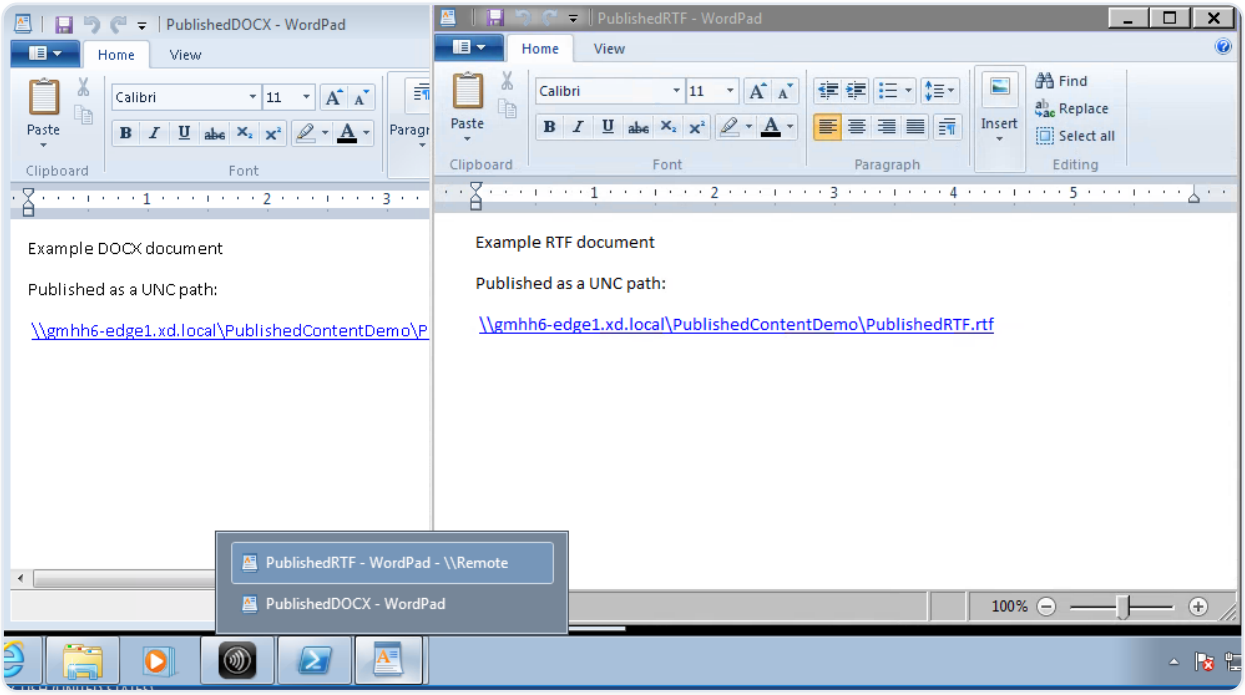
この例では、公開されたWordPadアプリケーションが編集され、.rtfファイル用のファイルタイプ関連付けが作成されます。

a. デリバリーグループのメンテナンスモードをオンにします。

b. **ファイルタイプ関連付け**プロパティを編集します。

c. 完了したら、メンテナンスモードをオフにします。

d. StoreFrontを更新してファイルタイプ関連付けの変更を読み込み、**PublishedRTF**および**PublishedDOCX**アプリケーションをクリックします。違いに注目してください。**PublishedDOCX**は引き続きローカルのWordPadで開きます。しかし、**PublishedRTF**はファイルタイプ関連付けにより、公開されたWordPadで開くようになりました。



詳細情報

- マシンカタログの作成
- デリバリーグループの作成
- アプリケーションプロパティの変更

サーバー VDI

Server VDI (Virtual Desktop Infrastructure) 機能を使用して、単一ユーザー向けにサーバーオペレーティングシステムからデスクトップを配信します。

- エンタープライズ管理者は、サーバーオペレーティングシステムをVDIデスクトップとして配信できます。これは、エンジニアやデザイナーなどのユーザーにとって価値があります。

- サービスプロバイダーは、クラウドからデスクトップを提供できます。これらのデスクトップは、Microsoft Services Provider License Agreement (SPLA) に準拠しています。

サポート:

- Citrix Virtual Apps and Desktops™ および Citrix DaaS (旧 Citrix Virtual Apps and Desktops service) の展開では、Server VDI は Windows Server 2022 および Windows Server 2019 でサポートされています。
- すべてのServer VDI展開は、ユーザーパーソナライゼーションレイヤーテクノロジーをサポートしています。
- Server VDIがスキャナーなどのTWAINデバイスで動作するには、Windows Serverのデスクトップエクスペリエンス機能がインストールされている必要があります。
- 以下の機能はServer VDIでは使用できません:
  - ホスト型アプリケーション
  - ローカルアプリアクセス
  - 直接（ブローカーなし）デスクトップ接続
  - リモートPCアクセス

Server VDIのインストールと構成

1. Windowsサーバーをインストール用に準備します。
   - Windows Server Managerを使用して、リモートデスクトップサービスロールサービスがインストールされていないことを確認します。以前にインストールされていた場合は、削除してください。これらのロールサービスがインストールされていると、VDAのインストールは失敗します。
   - 「**各ユーザーを単一セッションに制限する**」プロパティが有効になっていることを確認します。Windowsサーバーで、ターミナルサーバー設定のレジストリを編集します。

     `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server`

     `DWORD fSingleSessionPerUser = 1`
2. Citrix Virtual Apps and Desktopsインストーラーのコマンドラインインターフェイスを使用して、サポートされているサーバーまたはサーバーマスターイメージにVDAをインストールし、`/servervdi`オプションを指定します。(デフォルトでは、インストーラーのグラフィカルインターフェイスは、サーバーオペレーティングシステム上のWindowsシングルセッションOS

VDAをブロックします。コマンドラインを使用すると、この動作が上書きされます。)次のいずれかのコマンドを使用します。

- Citrix Virtual Apps and Desktops™展開の場合:
  - `XenDesktopVdaSetup.exe /servervdi`
  - `VDAWorkstationSetup.exe /servervdi`
- Citrix DaaS™展開の場合:
  - `VDAWorkstationSetup.exe /servervdi`

その他のオプション:

- Delivery ControllerまたはCloud Connectorを指定するには、`/controllers`を使用します。
- ファイアウォールを手動で構成する場合を除き、ファイアウォールでポートを開くには、`/enable_hdx_ports`を使用します。
- イメージにVDAをインストールし、そのイメージからMCSを使用してサーバーVMを作成する場合は、`/mastermcsimage` (または`/masterimage`) を使用します。
- すべてのオプションの詳細については、「コマンドラインを使用したインストール」を参照してください。

3. Server VDI用のマシンカタログを作成します。カタログ作成ウィザードで:
   - **オペレーティングシステム**ページで、**シングルセッションOS**を選択します。
   - **概要**ページで、Server VDIであることを明確に識別できるマシンカタログ名と管理者向けの記述を指定します。これは、カタログがServer VDIをサポートしていることをStudioで示す唯一のインジケーターです。

   Studioで検索を使用すると、VDAがマルチセッションマシンにインストールされている場合でも、Server VDIカタログは**シングルセッションOSマシン**タブに表示されます。
4. デリバリーグループを作成し、作成したServer VDIカタログを選択します。

VDAのインストール中にDelivery ControllerまたはCloud Connectorを指定しなかった場合は、後で指定することを忘れないでください。詳細については、「VDA登録」を参照してください。

ユーザーパーソナライゼーションレイヤー

> **注:**

バージョン 2511 以降、Citrix Web Studio (Web ベース) は Citrix Virtual Apps and Desktops™ の唯一の管理コンソールです。Citrix Studio (MMC ベース) はインストーラーから削除されました。この記事は Web Studio にのみ適用されます。Citrix Studio の詳細については、Citrix Virtual Apps and Desktops 7 2212 以前の同等の記事を参照してください。Citrix Virtual Apps and Desktops 7 2212 以前の同等の記事を参照してください。

Citrix Virtual Apps and Desktopsのユーザーパーソナライゼーションレイヤー機能は、非永続マシンカタログの機能を拡張し、ユーザーのデータとローカルにインストールされたアプリケーションをセッション間で保持します。基盤となるCitrix App Layeringテクノロジーを搭載したユーザーパーソナライゼーションレイヤー機能は、非永続マシンカタログでCitrix ProvisioningおよびMachine Creation Services™ (MCS) をサポートします。

マスターイメージ内のVirtual Delivery Agentとともに、ユーザーパーソナライゼーションレイヤーコンポーネントをインストールします。VHDファイルには、ユーザーがローカルにインストールしたアプリケーションが保存されます。イメージにマウントされたVHDは、ユーザー自身の仮想ハードドライブとして機能します。

重要:

ユーザーパーソナライゼーションレイヤーは、Citrix Virtual Apps and Desktops™ に展開することも、イメージテンプレートで有効になっている App Layering ユーザーレイヤーに展開することもできますが、両方を同時に展開することはできません。App Layering 内のレイヤーにユーザーパーソナライゼーションレイヤー機能をインストールしないでください。

この機能はPersonal vDisk (PvD) に代わるものであり、非永続（プールされた）デスクトップ環境のユーザーに永続的なワークスペースエクスペリエンスも提供します。

ユーザーパーソナライゼーションレイヤー機能を展開するには、記事に詳述されている手順を使用してインストールおよび構成します。

アプリケーションのサポート

以下の例外を除き、ユーザーがデスクトップにローカルでインストールするすべてのアプリケーションは、ユーザーパーソナライゼーションレイヤーでサポートされます。

例外

以下のアプリケーションは例外であり、ユーザーパーソナライゼーションレイヤーではサポートされません。

- MS OfficeやVisual Studioなどのエンタープライズアプリケーション。
- ネットワークスタックまたはハードウェアを変更するアプリケーション。例: VPNクライアント。
- ブートレベルドライバーを持つアプリケーション。例：ウイルススキャナー。
- ドライバー ストアを使用するドライバーを持つアプリケーション。例: プリンタードライバー。

> **注:**
>
> Windowsグループポリシーオブジェクト (GPO) を使用してプリンターを利用可能にできます。

サポートされていないアプリケーションをローカルにインストールすることをユーザーに許可しないでください。代わりに、これらのアプリケーションはマスターイメージに直接インストールしてください。

ローカルユーザーまたは管理者アカウントを必要とするアプリケーション

ユーザーがアプリケーションをローカルにインストールすると、そのアプリはユーザーレイヤーに格納されます。その後、ユーザーがローカルユーザーまたはグループを追加または編集しても、その変更はセッションを超えて保持されません。

> **重要:**
>
> 必要なローカルユーザーまたはグループは、マスターイメージに追加してください。

要件

ユーザーパーソナライゼーションレイヤー機能には、以下のコンポーネントが必要です。

- シトリックス バーチャル アプリケーションズ アンド デスクトップ 7 1909 以降
- Virtual Delivery Agent (VDA)、バージョン1912以降

- Citrix Provisioning™、バージョン1909以降
- Windowsファイル共有 (SMB)、またはオンプレミスAD認証が有効なAzure Files

ユーザーパーソナライゼーションレイヤー機能は、OSがシングルセッションとして展開されている場合、以下のWindowsバージョンで展開できます。サポートは、シングルセッション上の単一ユーザーに限定されます。

- ウィンドウズ 11 エンタープライズ x64
- Windows 10 Enterprise x64、バージョン1607以降
- Windows Server 2019 (Azure Files がサポートされています)
- Windows Server 2022 (Azure Files がサポートされています)

Citrix Virtual Apps and Desktops 7の場合、User personalization layersでのAzure Filesの使用は、Windows Server 2022、Windows Server 2019、およびWindows 10クライアントでサポートされています。

注:

サーバーOSを使用している場合、Server VDIのみがサポートされます。展開の詳細については、Server VDIの記事を参照してください。

ユーザーパーソナライゼーションレイヤーは、マシンごとに一度に1人のユーザーのみをサポートし、その後、ディスクをリセットするためにマシンを再起動する必要があります。ユーザーパーソナライゼーションレイヤーは、マルチセッションサーバーオペレーティングシステムでは使用できず、シングルセッションサーバーシステムでのみ使用できます。ユーザーパーソナライゼーションレイヤーは、非永続デスクトップでのみサポートされます。

ユーザーパーソナライゼーションレイヤー機能がインストールされている場合は、アンインストールします。最新リリースをインストールする前に、マスターイメージを再起動します。

ファイル共有を設定する

ユーザーパーソナライゼーションレイヤー機能には、Windows Server Message Block (SMB) ストレージが必要です。Windowsファイル共有を作成するには、使用しているWindowsオペレーティングシステムの通常の手順に従ってください。

Azureベースのカタログでは Azure Filesを使用する方法の詳細については、「ユーザーパーソナライゼーションレイヤー用のAzure Filesストレージを設定する」を参照してください。

推奨事項

ユーザーパーソナライゼーションレイヤーの展開を成功させるには、このセクションの推奨事項に従ってください。

マイクロソフト システムセンター コンフィグレーションマネージャー (SCCM)

ユーザーパーソナライゼーションレイヤー機能でSCCMを使用している場合は、VDI環境でイメージを準備するためのMicrosoftのガイドラインに従ってください。詳細については、このMicrosoft TechNet記事を参照してください。

ユーザーレイヤーのサイズ

ユーザーレイヤーは、ディスク上のスペースが使用されるにつれて拡張するシンプロビジョニングディスクです。ユーザーレイヤーに許可されるデフォルトサイズは10 GBで、これは推奨される最小値です。

> **注:**
>
> インストール中に値がゼロ (0) に設定されている場合、デフォルトのユーザーレイヤーサイズは10 GBに設定されます。

> ユーザーレイヤーのサイズを変更したい場合は、**User Layer Size** ポリシーに別の値を入力できます。「**オプション: User Layer Size in GBの横にあるをクリックします。**」の下にある「**ステップ5: デリバリーグループのカスタムポリシーを作成する**」を参照してください。

ユーザーレイヤーのサイズを上書きするためのツール (オプション)

Windowsツールを使用してユーザーレイヤーファイル共有にクォータを定義することで、ユーザーレイヤーのサイズを上書きできます。

以下のMicrosoftクォータツールのいずれかを使用して、**Users**という名前のユーザーレイヤーディレクトリにハードクォータを設定します。

- ファイルサーバーリソースマネージャー (FSRM)
- クォータマネージャー

注:

クォータを増やすと、新しいユーザーレイヤーに影響し、既存のユーザーレイヤーが拡張されます。クォータを減らすと、新しいユーザーレイヤーのみに影響します。既存のユーザーレイヤーのサイズが小さくなることはありません。

ユーザーパーソナライゼーションレイヤーを展開する

ユーザーパーソナライゼーション機能を展開する際は、Web Studio内でポリシーを定義します。その後、その機能が展開されるマシンカタログにバインドされているデリバリーグループにポリシーを割り当てます。

マスターイメージにユーザーパーソナライゼーションレイヤーの設定がない場合、サービスはアイドル状態のままであり、オーサリングアクティビティを妨げません。

マスターイメージでポリシーを設定すると、サービスはマスターイメージ内でユーザーレイヤーを実行およびマウントしようとします。マスターイメージは予期しない動作や不安定性を示します。

ユーザーパーソナライゼーションレイヤー機能を展開するには、以下の手順をこの順序で完了します。

- ステップ1：Citrix Virtual Apps and Desktops環境の可用性を確認します。
- ステップ2：マスターイメージを準備します。
- ステップ3：マシンカタログを作成します。
- ステップ4：デリバリーグループを作成します。
- ステップ5：デリバリーグループのカスタムポリシーを作成します。

注:

イメージ上のWindows 10をアップグレードした後、初めてログインするのに通常よりも時間がかかります。ユーザーレイヤーは新しいバージョンのWindows 10用に更新する必要があり、その結果、ログオン時間が増加します。

ステップ 1: Citrix Virtual Apps and Desktops 環境が利用可能であることを確認する

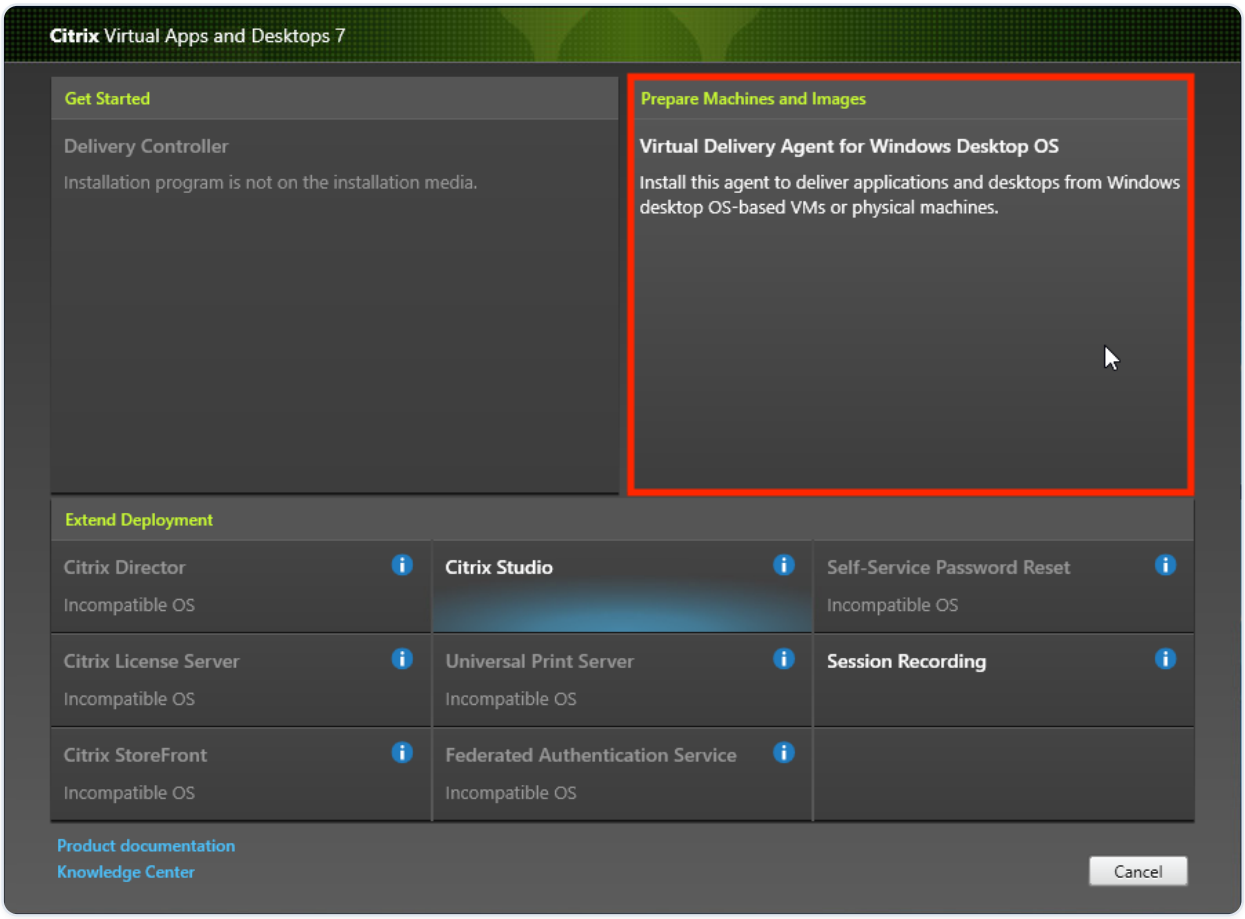
この新機能を使用するために、Citrix Virtual Apps and Desktops 環境が利用可能であることを確認してください。セットアップの詳細については、「Citrix Virtual Apps and Desktops のインストールと構成」を参照してください。

ステップ 2: マスターイメージを準備する

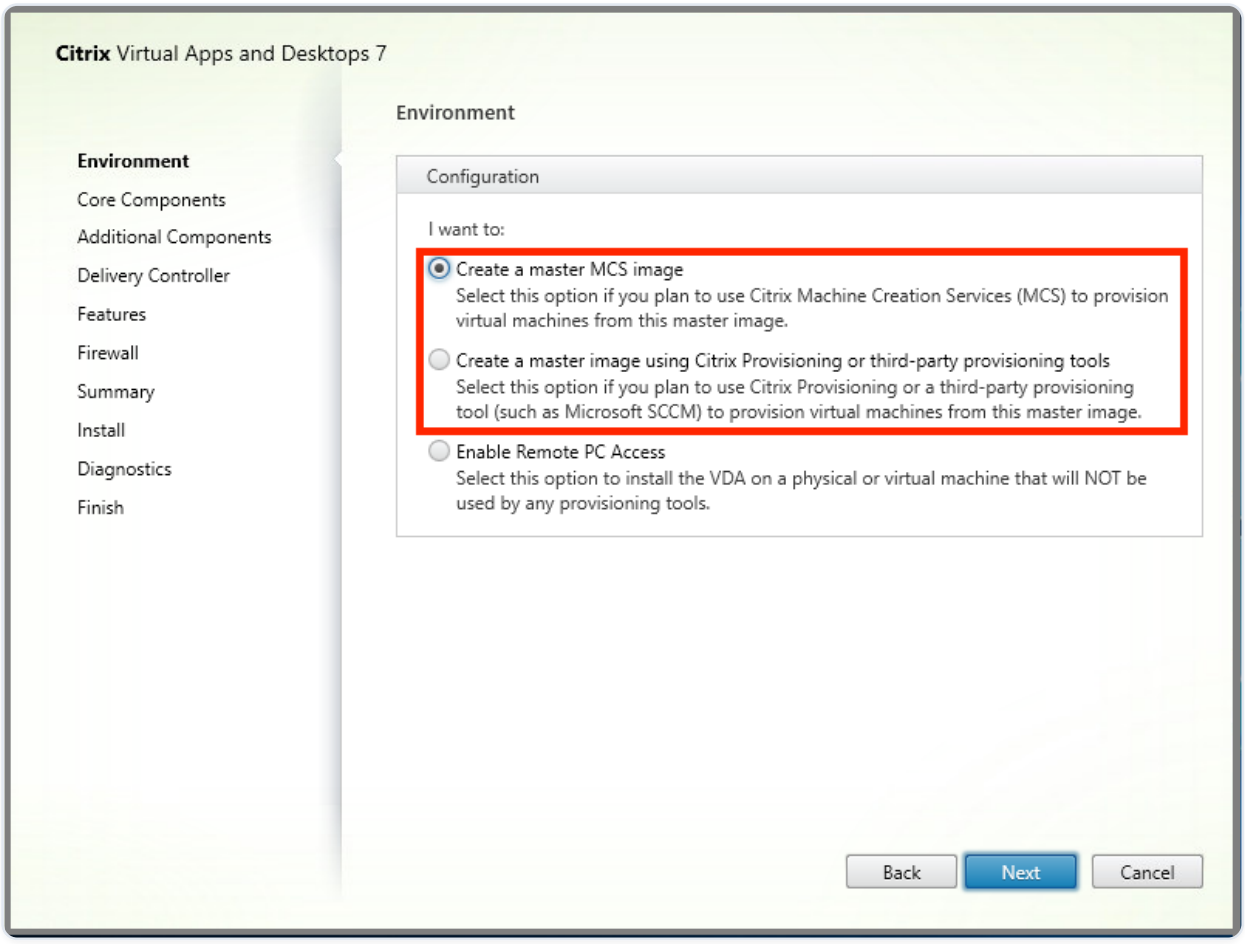
マスターイメージを準備するには:

1. マスターイメージを見つけます。組織のエンタープライズアプリケーションと、ユーザーが一般的に役立つその他のアプリをインストールします。
2. Server VDI を展開する場合は、Server VDI の記事の手順に従ってください。オプションコンポーネントである**ユーザーパーソナライゼーションレイヤー**を必ず含めてください。詳細については、「VDA をインストールするためのコマンドラインオプション」を参照してください。
3. Windows 10 を使用している場合は、Virtual Delivery Agent (VDA) 1912 以降をインストールします。古いバージョンの VDA がすでにインストールされている場合は、まず古いバージョンをアンインストールしてください。新しいバージョンをインストールする際は、オプションコンポーネントである**Citrix User Personalization Layer**を次のように選択してインストールしてください。

    a. **Virtual Delivery Agent for Windows Desktop OS**タイルをクリックします:

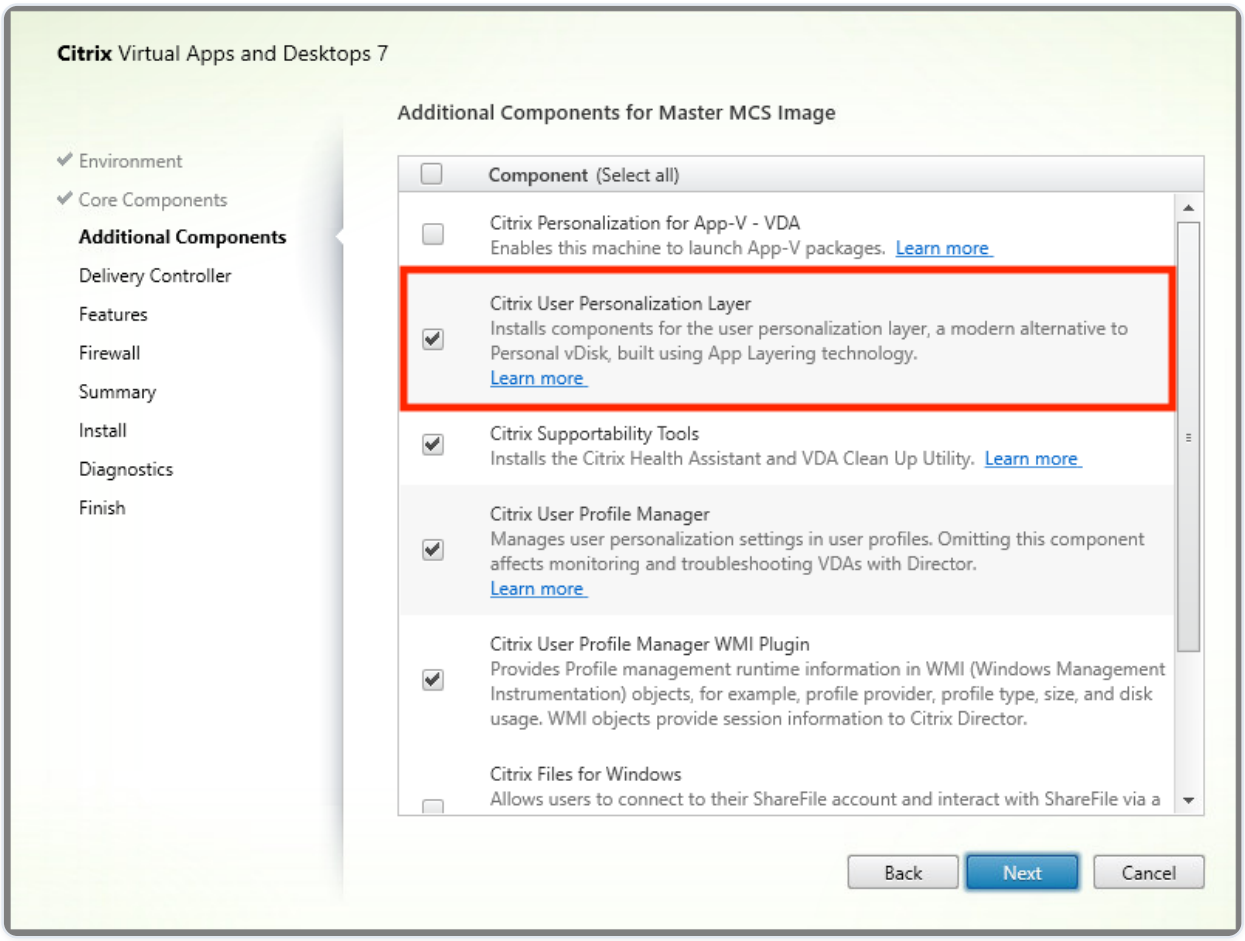


a. **環境:**「マスター MCS イメージを作成する」または「**Citrix Provisioning またはサードパーティのプロビジョニングツールを使用してマスターイメージを作成する**」のいずれかを選択します。



a. **コアコンポーネント:** 「次へ」をクリックします。

b. **追加コンポーネント:** 「**Citrix User Personalization Layer**」をチェックします。



a. 残りのインストール画面を進み、必要に応じて VDA を構成し、「**インストール**」をクリックします。インストール中にイメージが 1 回以上再起動します。

4. **Windows Update**は無効のままにしてください。ユーザーパーソナライゼーションレイヤーインストーラーは、イメージ上のWindows Updateを無効にします。更新は無効のままにしてください。

イメージをWeb Studioにアップロードする準備ができました。

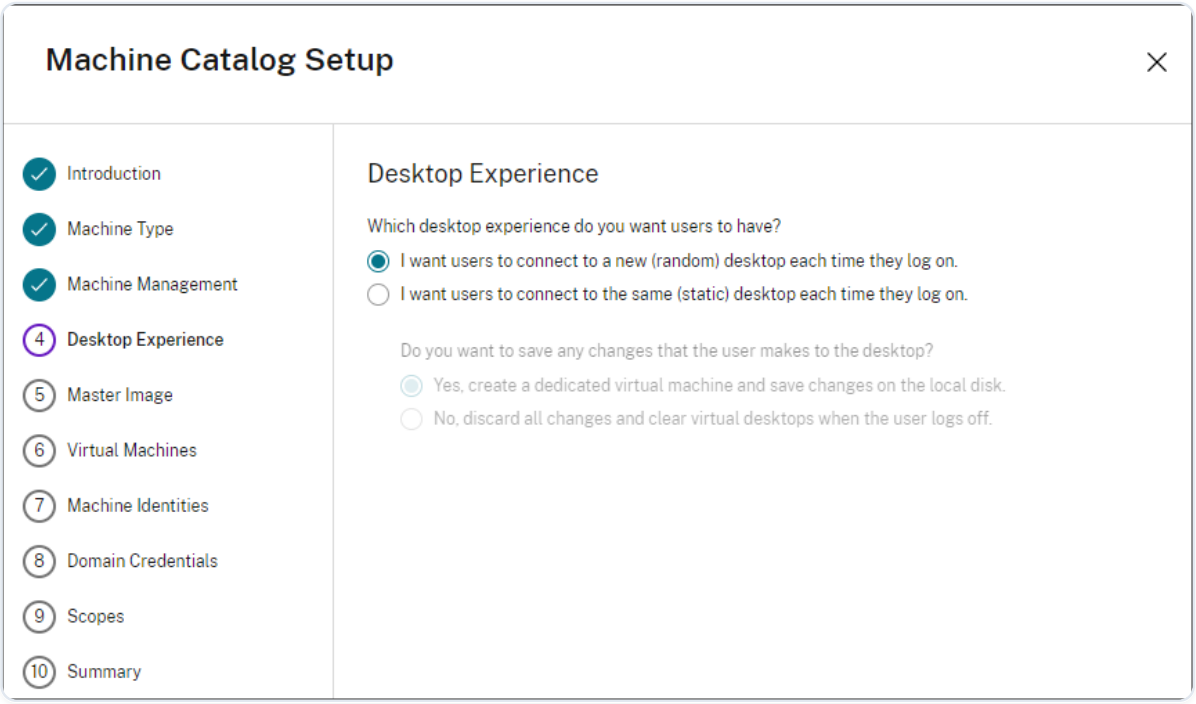
> **注:**
>
> ユーザーパーソナライゼーションレイヤー (UPL) を単にアップグレードしたい場合は、新しいバージョンのUPLとスタンドアロンパッケージを使用してアップグレードできます。VDAをアップグレードする必要はありません。

ステップ3：マシンカタログを作成する

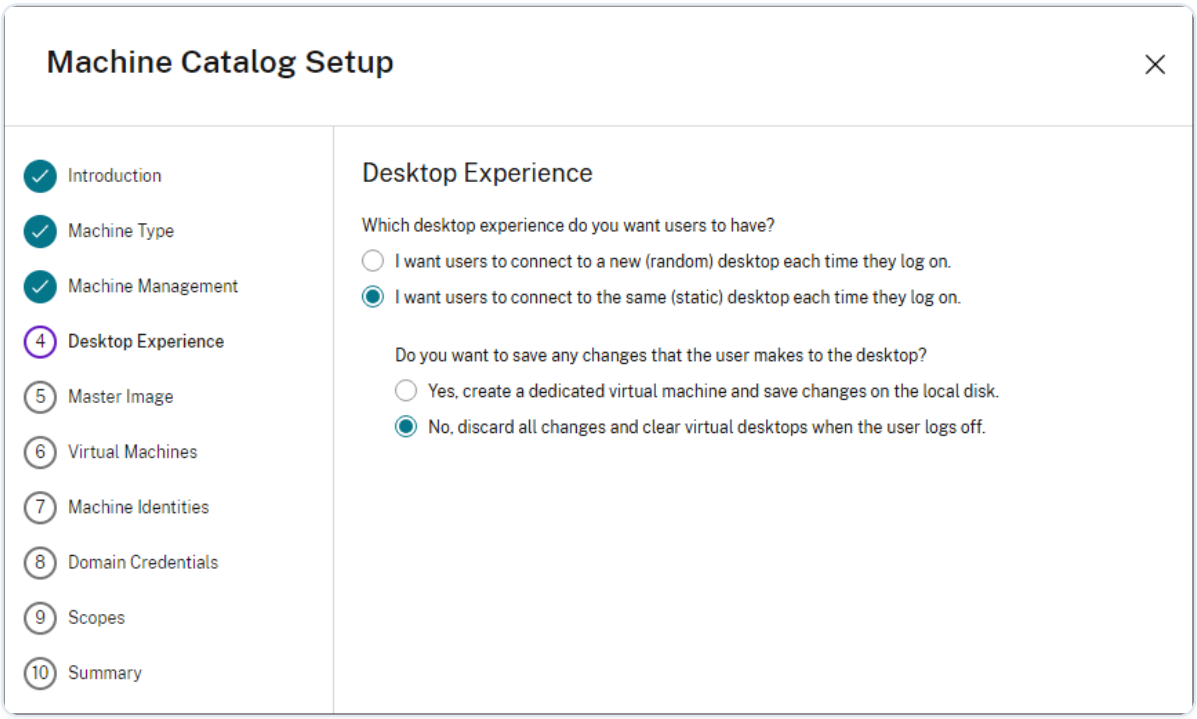
Web Studioで、マシンカタログを作成する手順に従います。カタログ作成時には、以下のオプションを使用します。

1. **オペレーティングシステム**を選択し、**シングルセッションOS**に設定します。
2. **マシン管理**を選択し、**電源管理されているマシン**に設定します。たとえば、仮想マシンやブレードPCなどです。
3. **デスクトップエクスペリエンス**を選択し、以下の例のように、**プールされたランダム**または**プールされた静的**カタログタイプに設定します。

   - **プールされたランダム:**



   - **プールされた静的:** プールされた静的を選択した場合、次のスクリーンショットに示すように、ユーザーがログオフするときにすべての変更を破棄し、仮想デスクトップをクリアするようにデスクトップを構成します。



注:

ユーザーパーソナライゼーションレイヤーは、Citrix Personal vDiskを使用するように構成されている、または専用仮想マシンとして割り当てられているプールされた静的カタログをサポートしていません。

4. MCSを使用している場合は、**イメージ**と、前のセクションで作成したイメージのスナップショットを選択します。
5. 環境の必要に応じて、残りのカタログプロパティを構成します。

ステップ 4: デリバリーグループを作成する

作成したマシンカタログのマシンを含め、**デリバリーグループ**を作成して構成します。詳細については、「デリバリーグループの作成」を参照してください。

ステップ 5: デリバリーグループのカスタムポリシーを作成する

Virtual Delivery Agent 内でユーザーレイヤーのマウントを有効にするには、構成パラメーターを使用して以下を指定します。

- ネットワーク上のどこでユーザーレイヤーにアクセスするか。
- ユーザーレイヤーディスクの最大許容サイズ。

パラメーターを Web Studio でカスタム Citrix ポリシーとして定義し、デリバリーグループに割り当てます。

1. Web Studio にサインインし、左ペインで を選択します。

   Studioでポリシーを選択(/en-us/citrix-virtual-apps-desktops/current-release/media/upl-studio-select-policies.png)

2. アクションバーで を選択します。 ウィンドウが表示されます。
3. 検索フィールドに `user layer` と入力します。利用可能なポリシーのリストに、次の3つのポリシーが表示されます。

   - ユーザーレイヤーの除外
   - ユーザーレイヤーリポジトリパス
   - ユーザーレイヤーサイズ (GB)

   > **注:**
   >
   > サイズを増やすと、新しいユーザーレイヤーに影響し、既存のユーザーレイヤーが拡張されます。サイズを減らすと、新しいユーザーレイヤーにのみ影響します。既存のユーザーレイヤーのサイズが小さくなることはありません。

   ユーザーレイヤーポリシーの選択(/en-us/citrix-virtual-apps-desktops/current-release/media/user-layer-policies.png)

4. **User Layer Repository Path** の横にあるチェックボックスをオンにして、**Edit** をクリックします。**Edit Setting** ウィンドウが表示されます。
5. **Value** フィールドにパスを入力し、**Save** をクリックします。

   - **パス形式:** `\\server-name-or-address\share-name\folder`
   - **パスの例:** `\\Server\Share\UPLUsers`
   - **結果のパスの例: CoolCompanyDomain** の **Alex** という名前のユーザーの場合、パスは次のとおりです。 `\\Server\Share\UPLUsers\Users\CoolCompanyDomain_Alex\A_OK`

   リポジトリパス(/en-us/citrix-virtual-apps-desktops/current-release/media/upl-user-layer-repo-enter-path-no-variables.png)

`%USERNAME%` および `%USERDOMAIN%` 変数、マシン環境変数、および Active Directory (AD) 属性を使用してパスをカスタマイズできます。これらの変数を展開すると、明示的なパスになります。

環境変数の例:

- **パス形式:** `\\Server-name-or-address\share-name\folder-with-environment-variables`
- **パスの例:** `\\Server\Share\UPLUserLayers\%USERNAME%\%USERDOMAIN%`
- **結果のパスの例: CoolCompanyDomain** の **Alex** という名前のユーザーの場合、パスは次のようになります。 `\\Server\Share\UPLUserLayers\Alex\CoolCompanyDomain\A_OK`

環境変数を含むリポジトリパス(/en-us/citrix-virtual-apps-desktops/current-release/media/upl-user-layer-repo-enter-path-variables.png)

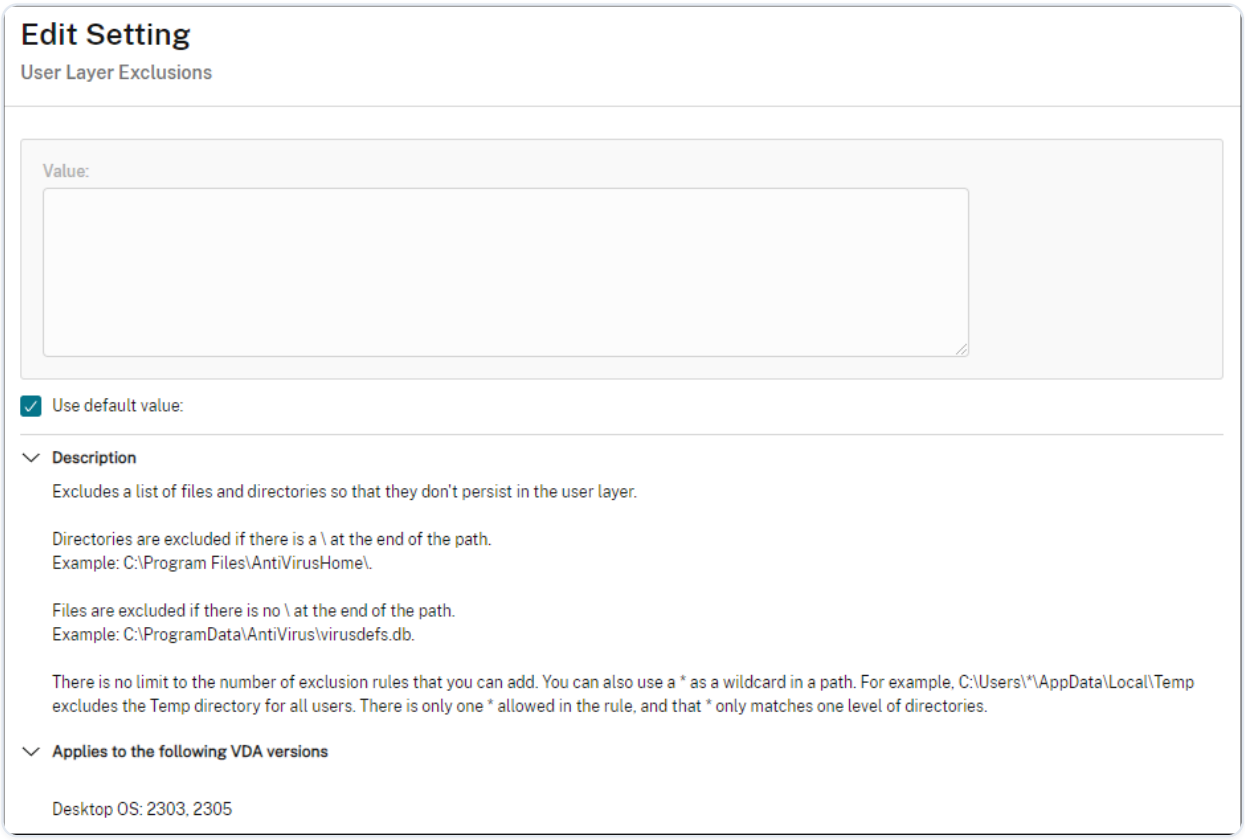
カスタム AD 属性の例:

- パス形式: `\\Server-name-or-address\share-name\AD-attribute`
- パスの例: `\\Server\share#sAMAccountName#`
- 結果のパスの例: `\\Server\share\JohnSmith` (現在のユーザーに対して #sAMAccountName# が JohnSmith に解決される場合)

6. オプション: **User Layer Size in GB** の横にあるチェックボックスをオンにして、**Edit** をクリックします。

   ユーザーレイヤーリポジトリパス(/en-us/citrix-virtual-apps-desktops/current-release/media/upl-select-user-layer-size.png)

   設定の編集ウィンドウが表示されます。
7. オプション: デフォルト値の **10 GB** を、各ユーザーレイヤーが拡張できる最大サイズに変更します。**Save** をクリックします。
8. オプション: **User Layer Exclusions** の横にあるチェックボックスをオンにして、**Edit** をクリックします。



9. オプション: 除外するファイルとフォルダーを指定し、**Save** をクリックします。詳細については、Citrix App Layering のドキュメント を参照してください。
10. 割り当てるユーザーとマシンを設定するには、**Next** をクリックします。この画像で強調表示されている **Delivery Group Assign** リンクをクリックします。

    ユーザーレイヤーリポジトリパス(/en-us/citrix-virtual-apps-desktops/current-release/media/upl-delivery-group-assign.png)
11. **Delivery Group** メニューで、前のセクションで作成したデリバリーグループを選択します。**OK** をクリックします。

    デリバリーグループを選択(/en-us/citrix-virtual-apps-desktops/current-release/media/upl-delivery-group-select.png)
12. ポリシーの名前を入力します。ポリシーを有効にするには、チェックボックスをオンにして、**Finish** をクリックします。

    ユーザーレイヤーポリシー名(/en-us/citrix-virtual-apps-desktops/current-release/media/upl-name-policy.png)

ユーザーレイヤーフォルダーのセキュリティ設定を構成する

ドメイン管理者として、ユーザーレイヤーのストレージ場所を複数指定できます。ストレージ場所ごとに（デフォルトの場所を含め）、`\Users` サブフォルダーを作成します。次の設定を使用して、各場所を保護します。

設定名	値	適用先	
作成者/所有者	変更	サブフォルダーとファイルのみ	
所有者の権限	変更	サブフォルダーとファイルのみ	
ユーザーまたはグループ	フォルダーの作成/データの追加; フォルダーの走査/ファイルの実行; フォルダーの一覧表示/データの読み取り; 属性の読み取り	選択したフォルダーのみ	
システム	フルコントロール	選択したフォルダー、サブフォルダー、およびファイル	
ドメイン管理者、および選択された管理者グループ	フルコントロール	選択したフォルダー、サブフォルダー、およびファイル	

ユーザーレイヤーメッセージ

ユーザーがユーザーレイヤーにアクセスできない場合、次のいずれかの通知メッセージが表示されます。

- **ユーザーレイヤーが使用中です**

  `We were unable to attach your user layer because it is in use. Any changes you make to application settings or data will not be saved. Be sure to save any work to a shared network location.`.

- **ユーザーレイヤーが利用できません**

`We were unable to attach your user layer. Any changes you make to application settings or data will not be saved. Be sure to save any work to a shared network location.`.

- **ユーザーサインアウト後にシステムがリセットされませんでした**

  `This system was not shut down properly. Please log off immediately and contact your system administrator.`.

トラブルシューティング時に使用するログファイル

ログファイル ulayersvc.log には、変更がログに記録されるユーザーパーソナライゼーションレイヤーソフトウェアの出力が含まれています。

```
C:\ProgramData\Unidesk\Logs\ulayersvc.log
```

ユーザーレイヤー/UPL領域の再利用

ユーザーレイヤー/UPL領域の再利用を使用して、ユーザーがログオフするたびにVHDXファイルを自動的に圧縮できます。 詳細については、「ユーザーレイヤー/UPL領域の再利用」を参照してください。

制限事項

ユーザーパーソナライゼーションレイヤー機能をインストールして使用する際は、以下の制限事項に注意してください。

- App Layering内のレイヤーにユーザーパーソナライゼーションレイヤーソフトウェアを展開しようとしないでください。Citrix Virtual Apps and Desktopsでユーザーパーソナライゼーションレイヤーを展開するか、App Layeringイメージテンプレートでユーザーレイヤーを有効にするかのいずれかであり、両方ではありません。どちらのプロセスでも、必要なユーザーレイヤーが生成されます。
- 永続的なマシンカタログでユーザーパーソナライゼーションレイヤー機能を構成しないでください。
- 「セッションホスト」は使用しないでください。
- 新しいOSインストールを実行しているイメージ (Windows 10の同じバージョンであっても) でマシンカタログを更新しないでください。ベストプラクティスは、マシンカタログ作成時に使用した同じマスターイメージ内でOSの更新を適用することです。
- ブート時ドライバーやその他の初期ブートパーソナライゼーションは使用しないでください。

- PvDデータをユーザーパーソナライゼーションレイヤー機能に移行しないでください。
- 既存のユーザーレイヤーを完全なApp Layering製品からユーザーパーソナライゼーションレイヤー機能に移行しないでください。
- 異なるマスターOSイメージを使用して作成されたユーザーレイヤーにアクセスするために、ユーザーレイヤーのSMBパスを変更しないでください。
- ユーザーがセッションからログアウトし、再度ログインすると、新しいセッションはプール内の別のマシンで実行されます。VDI環境では、Microsoft Software Centerは、最初のマシンではアプリケーションを**インストール済み**として表示しますが、2番目のマシンでは**利用不可**として表示します。

  アプリケーションの実際のステータスを確認するには、ユーザーにSoftware Centerでアプリケーションを選択し、**インストール**をクリックするよう指示します。すると、SCCMがステータスを実際の値に更新します。
- ユーザーパーソナライゼーションレイヤー機能が有効になっているVDA内で、Software Centerが起動直後に停止することがあります。この問題を回避するには、XenDesktop VDI環境でのSCCMの実装に関するMicrosoftの推奨事項に従ってください。また、Software Centerを起動する前に、`ccmexec`サービスが実行されていることを確認してください。
- グループポリシー (コンピューター設定) では、ユーザーレイヤー設定は、マスターイメージに適用された設定を上書きします。そのため、GPOを使用してコンピューター設定で行った変更は、次回のセッションログイン時にユーザーに常に適用されるとは限りません。

  この問題を回避するには、次のコマンドを発行するユーザーログオンスクリプトを作成します。

  ```
  gpupdate /force
  ```

  たとえば、あるお客様は、ユーザーがログインするたびに次のコマンドを実行するように設定しました。

  ```
  gpudate /Target:Computer /force
  ```

  最良の結果を得るには、ユーザーがログインした後で、コンピューター設定への変更をユーザーレイヤーに直接適用します。
- ドメインユーザーアカウントは、マスターイメージに最後にログインしたユーザーであってはなりません。そうしないと、そのイメージからプロビジョニングされたマシンで問題が発生する可能性があります。

- 純粋なMicrosoft Entra環境でUPLが有効になっている場合、Azureで実行されているWindowsの根本的な問題により、カスタム証明書は保持されません。Microsoftが将来の機能強化でこの問題を修正した場合、この記事を更新します。

コンポーネントの削除

コンポーネントを削除するには、プログラムの削除または変更を行うWindows機能を使用することをお勧めします。または、コマンドラインまたはインストールメディア上のスクリプトを使用してコンポーネントを削除することもできます。

コンポーネントを削除しても、前提条件は削除されず、ファイアウォール設定も変更されません。たとえば、Delivery Controller™を削除しても、SQL Serverソフトウェアとデータベースは削除されません。

Web Interfaceを含む以前の展開からControllerをアップグレードした場合は、Web Interfaceコンポーネントを個別に削除する必要があります。インストーラーを使用してWeb Interfaceを削除することはできません。

以下に記載されていない機能の削除については、その機能のドキュメントを参照してください。

準備

Controllerを削除する前に、サイトから削除してください。詳しくは、「Controllerを削除する」を参照してください。

StudioとDirectorを削除する前に、それらを閉じます。

Windowsのプログラムの削除または変更機能を使用してコンポーネントを削除する

Windowsのプログラムの削除または変更機能から：

- Controller、Studio、Director、License Server、またはStoreFrontを削除するには、**Citrix Virtual Apps *version*** または **Citrix Virtual Apps and Desktops™ *version*** を右クリックして、**アンインストール**を選択します。インストーラーが起動します。削除するコンポーネントを選択します。

  または、**Citrix StoreFront**を右クリックして**アンインストール**を選択することで、StoreFront™を削除できます。

- VDAを削除するには、**Citrix Virtual Delivery Agent *version*** を右クリックして、**アンインストール**を選択します。インストーラーが起動し、削除するコンポーネントを選択できます。デフォルトでは、削除後にマシンは自動的に再起動します。
- Universal Print Serverを削除するには、**Citrix Universal™ Print Server**を右クリックして、**アンインストール**を選択します。

コマンドラインを使用してコアコンポーネントを削除する

`\x64\XenDesktop Setup`ディレクトリから、`XenDesktopServerSetup.exe`コマンドを実行します。

- 1つ以上のコンポーネントを削除するには、`/remove`および`/components`オプションを指定します。
- すべてのコンポーネントを削除するには、`/removeall`オプションを指定します。

コマンドとパラメーターの詳細については、「コマンドラインを使用したインストール」を参照してください。

例えば、次のコマンドはWeb Studioを削除します。

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components webstudio
```

アップグレード中に、`\x64\Licensing\CitrixLicensing.exe /quiet`または`\x64\Licensing\CitrixLicensing.exe /quiet /l install.log`コマンドを使用して最初にライセンスサーバーをインストールし、その後コアコンポーネントをインストールした場合は、アンインストールも同じ順序で行ってください。

1. コマンドラインを使用してライセンスサーバーをアンインストールします:

   ```
   CitrixLicensing.exe /quiet /uninstall /l uninstall.log
   ```

2. GUIまたはコマンドラインを使用してコンポーネントをアンインストールします。詳細については、「コンポーネントの削除」を参照してください。

コマンドライン`XenDesktopServerSetup.exe`または`removeall`を使用してライセンスサーバーとコンポーネントをアンインストールした場合は、レジストリエントリと残りのファイルをクリーンアップしてください。

レジストリエントリをクリーンアップするには:

1. レジストリキー `Citrix Licensing` を検索し、そのエントリを削除します。ほとんどの場合、エントリは次の場所にあります:

   ```
   "Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\
   ```

2. レジストリキーの **Uninstall String** が指すフォルダーを削除します。

コマンドラインを使用してVDAを削除する

`\x64\XenDesktop Setup` ディレクトリから、`XenDesktopVdaSetup.exe` コマンドを実行します。

- 1つ以上のコンポーネントを削除するには、`/remove` オプションと `/components` オプションを使用します。例えば、VDAとCitrix Workspaceアプリを削除するには、`/remove /components vda,plugin` を使用します。
- `/removeall` オプションはVDAのみを削除します。Citrix Workspaceアプリは削除しません。

コマンドとパラメーターの詳細については、コマンドラインを使用したインストールを参照してください。

デフォルトでは、削除後にマシンは自動的に再起動します。

Active Directoryでスクリプトを使用してVDAを削除するには、スクリプトを使用したVDAのインストールまたは削除を参照してください。

アップグレードと移行

注:

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

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

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

はじめに

アップグレードすると、新しいマシンやサイトをセットアップすることなく、展開がCitrix Virtual Apps and Desktops™ 7 **Current Release (CR)** に変更されます。これはインプレースアップグレードとして知られています。

アップグレードにより、対象となる最新の機能とテクノロジーにアクセスできるようになります。アップグレードには、以前のバージョンからの修正、明確化、および機能強化も含まれる場合があります。

アップグレードの概要

1. アップグレードを開始する前に、展開のアップグレードの記事を確認してください。これは、アップグレードの準備方法と実装方法を学ぶための主要な情報源です。
2. 現在のカスタマーサクセスサービスの日付が有効であり、期限切れになっていないことを確認してください。詳細については、Customer Success Services renewal licensesの記事を参照してください。
3. 準備ガイダンスを完了します。
4. インストーラーを実行してコアコンポーネントをアップグレードします。
5. システムデータベースとサイトをアップグレードします。
6. イメージ上のVDA（またはマシンに直接）をアップグレードします。
7. その他のコンポーネントをアップグレードします。

各準備およびアップグレードの手順については、展開のアップグレードで詳しく説明しています。

アップグレード可能なバージョン

Citrix Virtual Apps and Desktops™ 2507 LTSRには、以下からアップグレードできます。

- Virtual Apps and Desktops 2402 LTSR（CUの有無にかかわらず、CU2までを含む）
- Virtual Apps and Desktops 2203 LTSR（CUの有無にかかわらず、CU6までを含む）
- Citrix Virtual Apps and Desktopsの現在サポートされているCRバージョン

> 注:
>
> - アップグレードプロセスを開始する前に、Citrix®は、管理された環境でアップグレードをテストし、特定の要件を満たしていることを確認することを推奨します。さらに、シームレスな移行を確実にするために、廃止リストや既知の問題を含むすべての関連製品ドキュメントを確認することをお勧めします。このアプローチは、本番システムへの潜在的な中断を軽減し、全体的なアップグレードエクスペリエンスを向上させるのに役立ちます。 サポートされているバージョンのリストの詳細については、製品マトリックスを参照してください。

よくある質問

このセクションでは、Citrix Virtual Apps and Desktopsのアップグレードに関するよくある質問に回答します。

- **Virtual Apps and Desktops環境をアップグレードする正しい順序は何ですか？**

  推奨されるアップグレードシーケンスの図と説明については、アップグレードシーケンスおよびアップグレード手順を参照してください。

- **私のサイトには複数のDelivery Controller（異なるゾーンにあります）があります。一部のみをアップグレードした場合、どうなりますか？同じメンテナンス期間中にサイト内のすべてのControllerをアップグレードする必要がありますか？**

  各 Controller 上のさまざまなサービスが相互に通信するため、すべての Delivery Controller を同じメンテナンス期間中にアップグレードすることがベストプラクティスです。異なるバージョンを維持すると、問題が発生する可能性があります。メンテナンス期間中には、Controller の半分をアップグレードし、サイトをアップグレードしてから、残りの Controller をアップグレードすることをお勧めします。詳細については、アップグレード手順 を参照してください。

- **最新バージョンに直接アップグレードできますか、それとも段階的なアップグレードを行う必要がありますか？**

  アップグレード先のバージョンの **新機能** の記事で明示的に記載されていない限り、ほとんどの場合、中間リリースをスキップして最新バージョンにアップグレードできます。

- **お客様はLong Term Service Release (LTSR) 環境からCurrent Releaseにアップグレードできますか？**

  はい。お客様は長期間にわたってLong Term Service Releaseにとどまる必要はありません。お客様は、ビジネス要件と機能に基づいて、LTSR環境をCurrent Releaseに移行できます。

- **コンポーネントの混在バージョンは許可されていますか？**

  各サイト内で、Citrixはすべてのコンポーネントを同じバージョンにアップグレードすることを推奨しています。一部のコンポーネントで以前のバージョンを使用することはできますが、最新バージョンのすべての機能が利用できない場合があります。詳細については、混在環境に関する考慮事項を参照してください。

- **Current Releaseはどのくらいの頻度でアップグレードする必要がありますか？**

  Current Release は、リリース日から 6 か月後に End of Maintenance (EOM) に達します。Citrix は、お客様が最新の Current Release を採用することを推奨しています。Current Release は、リリース日から 18 か月後に End of Life (EOL) に達します。

- **推奨されるのは、LTSRへのアップグレードですか、それともCRへのアップグレードですか？**

  Current Release (CR) は、最新かつ最も革新的なアプリ、デスクトップ、およびサーバー仮想化の機能を提供します。これにより、最先端のテクノロジーを維持し、競合他社の一歩先を行くことができます。

  Long Term Service Release (LTSR) は、長期間にわたって同じベースバージョンを維持することを好む大規模なエンタープライズ本番環境に最適です。

> For details, see [Servicing Options](https://www.citrix.com/support/citrix-customer-success-services/citrix-virtual-apps-and-desktops-servicing-options.md).

- **ライセンスをアップグレードする必要がありますか？**

  現在のライセンスの有効期限が切れておらず、アップグレード先のリリースで有効であることを確認してください。CTX111618を参照してください。更新については、Customer Success Services renewal licensesを参照してください。

- **アップグレードにはどのくらい時間がかかりますか？**

  展開のアップグレードにかかる時間は、インフラストラクチャとネットワークによって異なります。そのため、正確な時間をお伝えすることはできません。

- **ベストプラクティスは何ですか？**

  準備ガイダンスを理解し、それに従ってください。

- **Citrix Virtual Apps and Desktopsサイトのアップグレードにはsysadmin権限が必要ですか？**

  いいえ。Windows認証（デフォルト）を使用する標準的なサイトアップグレードの場合、既存のデータベース（サイト、ログ、監視）に対するdb_owner権限があれば、サイトマネージャーがスキーマを更新するのに十分です。sysadminは、主に最初のサイト作成時、またはプロセスが新しいデータベースとサーバーレベルのログインを自動的に作成する必要がある場合にのみ必要です。

- **アップグレード中にサイトマネージャーが管理者権限を要求することがあるのはなぜですか？**

  アップグレードにサーバーレベルのアクションが必要な場合、サイトマネージャーは管理者権限を確認することがあります。たとえば、次のとおりです。

  - 新しいDelivery Controllerの追加：これには、Delivery ControllerのマシンID用の新しいSQLログインの作成が必要です。

  - ログインの変更：`securityadmin`または`dbcreator`ロールを必要とするアクションは、sysadminの要求に簡略化されることがよくあります。
  - 自動作成：サイトマネージャーが、事前準備されたスクリプトを使用するのではなく、新しいデータベース構造を自動的に作成したり、ユーザーをマッピングしたりするタスクを負っている場合。

- **Citrix管理者にsysadmin権限を付与せずにデータベースをアップグレードできますか？**

  はい、手動アップグレードを実行することでアップグレードできます。Citrix管理者はSite Managerを使用してアップグレードSQLスクリプトを取得し、そのスクリプトをデータベース所有者に提供してデータベースのアップグレードを実行します。データベースがアップグレードされた後、Citrix管理者はSite Managerに戻り、アップグレードプロセス全体を完了します。

- **Citrixサービスはなぜマシンアカウントで実行されるのですか？**

  Citrixサービスは、デフォルトでNetwork Serviceアカウントで実行されます。これは、サーバーが自身のID（たとえば、DOMAIN\SERVER$などのマシンアカウント）を使用して、手動のパスワード管理なしに他のサーバーやSQLデータベースと安全に通信できるためです。この設定はWindows認証に依存しており、Active Directory内の既存の信頼関係を利用するため、SQLへの接続において最も安全で推奨される方法です。

- **サポートされているオペレーティングシステムは何ですか？**

  アップグレード先のバージョンのシステム要件の記事に、サポートされているOSが記載されています。

  現在の展開でサポートされなくなったオペレーティングシステムを使用している場合は、以前のオペレーティングシステムを参照してください。

- **サポートされているVMware vSphere (vCenter + ESXi) のバージョンは何ですか？**

  CTX131239には、サポートされているホストとバージョン、および既知の問題へのリンクが記載されています。

- **私のバージョンはいつEOLになりますか？**

  製品マトリックスを確認してください。

- **最新リリースにおける既知の問題は何ですか？**

  - シトリックス仮想アプリおよびデスクトップ
  - StoreFront
  - シトリックス プロビジョニング

- シトリックス ライセンス サーバー
- Windows向けCitrix Workspaceアプリ

詳細情報

長期サービスリリース (LTSR) 展開の更新には累積更新プログラム (CU) が使用されます。CUはLTSRのベースラインコンポーネントを更新し、各CUには独自のメタインストーラーが含まれています。

各CUには専用のドキュメントがあります。たとえば、2203 LTSRの場合、最新のCUについては、そのLTSRの**「新機能」**ページにあるリンクを確認してください。各CUページには、サポートされているバージョン情報、手順、およびCUダウンロードパッケージへのリンクが含まれています。

移行

クラウドへの移行

Citrix Virtual Apps and Desktopsの自動構成ツールを使用して、オンプレミス展開をクラウドに移行できます。詳しくは、「クラウドへの移行」を参照してください。

レガシー移行

移行とは、以前の展開から新しいバージョンにデータを移動することです。このプロセスには、新しいコンポーネントのインストールと新しいサイトの作成、古いファームからのデータのエクスポート、そして新しいサイトへのデータのインポートが含まれます。

XenAppおよびXenDesktopのバージョン、または以前のCitrix Virtual Apps and Desktopsのバージョンを移行するためのサポートされているツールやスクリプトはありません。この製品ドキュメントで説明されているCitrix Virtual Apps and Desktopsのバージョンについては、*アップグレード*がサポートされています。

以前のXenApp 6.xの移行コンテンツについては、以下を参照してください。スクリプトはサポートも保守もされていません。

- XenApp 6.xバージョンのオープンソース移行スクリプトは`<https://github.com/citrix/xa65migrationtool>`で入手できます。Citrixはこれらの移行スクリプトをサポートまたは保守していません。
- **7.xでの変更点、XenApp 6.5ワーカーを新しいVDAにアップグレードする**、および**XenApp 6.xを移行する**については、`<https://docs.citrix.com/ja-jp/legacy-archive/citrix-`

`virtual-apps-and-desktops.html>`のCitrix Virtual Apps and Desktopsレガシーアーカイブを参照してください。

デプロイをアップグレードする

> **注:**
>
> 従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されてきたファイルベースのライセンスシステムは、End of Life (EOL) on April 15, 2026となります。License Activation Service (LAS) は、Citrix製品スイート全体で製品アクティベーションを行う次世代テクノロジーです。LASは、April 15, 2026以降、Citrixオンプレミスコンポーネントをアクティベートおよびライセンス供与する唯一の方法となります。サポートを継続するには、Citrix Virtual Apps and Desktopsの展開がLAS互換バージョンである必要があります。LAS互換の最小要件となるCVADバージョンは次のとおりです。
>
> - CVAD 2203 LTSR CU7
> - CVAD 2402 LTSR CU3
> - CVAD 2507 LTSR
> - CVAD 2411
>
> ご質問やご不明な点がございましたら、カスタマーケアにお問い合わせください。Citrixは、これらの要件を遵守しない場合、Citrixが法律または衡平法上持つ可能性のあるその他の救済措置に加えて、責任を負うことなくCitrix Maintenanceを制限または停止する場合があります。これらの要件は、法律または規制によって禁止されている場合には適用されません。

はじめに

> **注:**
>
> この記事では、Web Studioを含む展開のアップグレードについて説明します。Citrix Studioを含むアップグレードについては、Citrix Virtual Apps and Desktops™ 7 2212以前の同等の記事を参照してください。

> 新しいマシンやサイトを最初にセットアップすることなく、特定の展開を新しいバージョンにアップグレードできます。これはインプレースアップグレードと呼ばれます。

アップグレードできるCitrix Virtual Apps and Desktopsのバージョンについては、(/ja-jp/citrix-virtual-apps-desktops/current-release/upgrade-migrate.html#versions-you-can-upgrade)を参照してください。

Citrix Virtual Apps and Desktopsのいずれかのリリースにアップグレードする前に、現在のCustomer Success Servicesの有効期限が切れていないことを確認してください。詳細については、(/ja-jp/licensing/current-release/customer-success-services.html#customer-success-services-renewal-licenses)の記事を参照してください。

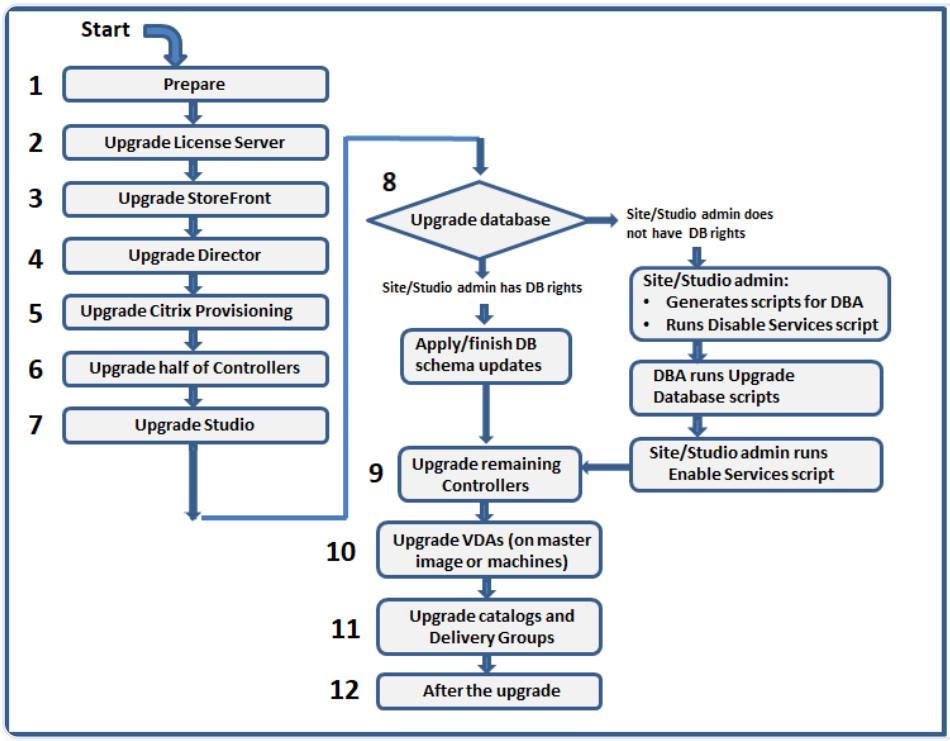
アップグレードを開始するには、新しいバージョンのインストーラーを実行して、以前にインストールされたコアコンポーネント、VDA、および特定のその他のコンポーネントをアップグレードします。次に、データベースとサイトをアップグレードします。

新しいバージョンが提供されている場合、フルプロダクトインストーラー（およびスタンドアロンVDAインストーラー）でインストールできる任意のコンポーネントをアップグレードできます。フルプロダクトインストーラーでインストールされないその他のコンポーネント（Citrix Provisioning™やProfile Managementなど）については、そのコンポーネントのドキュメントを参照してください。ホストのアップグレードについては、適切なドキュメントを参照してください。

アップグレードを開始する前に、この記事のすべての情報を確認してください。

アップグレードシーケンス

次の図は、アップグレードシーケンスのステップを示しています。Upgrade procedure には、図の各ステップの詳細が含まれています。



注:

障害を回避するため、新しいマシンカタログの作成、マシンカタログの削除、デリバリーグループ内のマシンの更新など、プロビジョニングおよびデリバリーグループ関連のタスクを実行する前に、すべてのDelivery Controllerとデータベースをアップグレードする必要があります。

ハイブリッド権限ライセンス

ハイブリッド権限ライセンスは、顧客が永続ライセンスからクラウドサービスサブスクリプションに移行またはアップグレードする際に、クラウドサービスサブスクリプションに加えて提供される期間ベースのサブスクリプションライセンスです。DaaSサブスクリプションでハイブリッド権限アドオンを購入することもできます。

SaaS属性を持つハイブリッドライツライセンスをお持ちの場合、Citrix Virtual Apps and Desktops™ LTSR 2203以降にアップグレードすると、Citrix Virtual Apps and Desktops LTSR 1912では利用できなかった機能にアクセスできるようになります。これらの機能には、Microsoft Azure、AWS EC2、Google Cloudなどのパブリッククラウドでのワークロードのプロビジョニングとホスティングが含まれます。新しいライセンスファイルを展開する前に、ライセンスサーバーを最新バージョンに更新してください。この前提条件を満たさない場合、Citrix Virtual Apps and Desktopsサイトのアップグレードとサイト作成がブロックされます。

SaaS属性のないハイブリッドライツライセンスにアクセスできる場合は、次の手順に従ってSaaS属性を持つ新しいハイブリッドライツライセンスにアクセスしてください。

注:

- 新しいライセンスコードが記載されたメールが届きます。詳しくは、「ライセンスアクセスコードの使用」を参照してください。
- 既存のライセンスは取り消されます。取り消されたライセンスはライセンスサーバーから削除し、その後新しいライセンスをインストールする必要があります。詳しくは、「ライセンスファイルの削除」を参照してください。

1. citrix.comのライセンス管理ポータルにアクセスし、クラウドプロビジョニング権限が有効になっている（SaaS属性を持つ）新しいハイブリッド権限ライセンスファイルをダウンロードします。詳細については、「ライセンスのダウンロード」を参照してください。次の画像は、増分セクションにSaaS属性を持つハイブリッド権限ライセンスファイルを示しています。

```
INCREMENT XDT_PLT_CCS CITRIX 2022.1201 01-dec-2022 5 \
    VENDOR_STRING=;LT=RetailS;GP=720;PSL=10;CL=VDS,VDA,VDE,VDP,SaaS:SA=0;ODP=0;NUDURMIN=2880;NUDURMAX=525600;AP=ADMIN/INT/14
    OVERDRAFT=1 DUP_GROUP=V ISSUED=18-dec-2005 NOTICE="Citrix \
    Systems Inc." SN=RetailSSaaS SIGN="..."
```

2. ライセンスサーバーにハイブリッド権限ライセンスファイルをインストールします。詳しくは、「ライセンスのインストール」を参照してください。
3. ライセンスのエディションまたはモデルに変更がある場合は、ブローカーコマンドを実行してエディションとモデルを設定し、インプレースアップグレードを開始してください。ブローカーコマンドの詳細については、「Broker PowerShell SDK」セクションを参照してください。

Citrix Virtual Apps and DesktopsのCurrent ReleasesおよびLong Term Service Releasesでのパブリッククラウドサポートの詳細については、CTX270373を参照してください。

アップグレード手順

主要な製品コンポーネントのほとんどは、コンポーネントを含むマシンで製品インストーラーを実行することでアップグレードできます。

1台のマシンに複数のコンポーネント（Studioやライセンスサーバーなど）が含まれている場合、製品メディアにそれらのソフトウェアの新しいバージョンが含まれていれば、そのマシン上のすべてのコンポーネントがアップグレードされます。

インストーラーを使用するには：

- フル製品インストーラーのグラフィカルインターフェイスを実行するには、マシンにログオンし、メディアを挿入するか、新しいリリースのISOドライブをマウントします。**AutoSelect** をダブルクリックします。
- コマンドラインインターフェイスを使用するには、適切なコマンドを発行します。「コマンドラインを使用したインストール」を参照してください。

ステップ1：準備

アップグレードを開始する前に、準備が整っていることを確認してください。必要なタスクを読み、完了してください。

- PVD、AppDisks™、およびサポートされていないホストの削除
- PvDまたはAppDiskコンポーネントを持つVDA
- 制限事項
- 混在環境に関する考慮事項
- 以前のオペレーティングシステム
- 準備
- サイトの事前テスト
- SQL Serverのバージョンチェック

ステップ2：ライセンスサーバーのアップグレード

インストールに新しいバージョンのCitrix License Serverソフトウェアが含まれている場合は、他のコンポーネントよりも先にこのコンポーネントをアップグレードしてください。

まだライセンスサーバーが新しいバージョンと互換性があるかどうかを判断していない場合は、他のコアコンポーネントをアップグレードする前に、ライセンスサーバーでインストーラーを実行することが不可欠です。

ステップ3：StoreFront™のアップグレード

インストールメディアに新しいバージョンのStoreFrontソフトウェアが含まれている場合は、StoreFrontサーバーを含むマシンでインストーラーを実行します。

- グラフィカルインターフェイスで、 セクションから を選択します。
- コマンドラインから、Citrix Virtual Apps and Desktopsインストールメディアの`x64`フォルダーにある`CitrixStoreFront-x64.exe`を実行します。

ステップ4：Directorのアップグレード

インストールメディアに新しいバージョンのDirectorソフトウェアが含まれている場合は、Directorを含むマシンでインストーラーを実行します。

ステップ5：Citrix Provisioningのアップグレード

Citrix Provisioningのインストールメディアは、Citrix Virtual Apps and Desktopsのインストールメディアとは別に提供されています。Citrix Provisioningサーバーおよびターゲットデバイスソフトウェアのインストールとアップグレードの方法については、Citrix Provisioning製品ドキュメントを参照してください。

ステップ6：Delivery Controllerの半分をアップグレードする

たとえば、サイトに4つのControllerがある場合、そのうちの2つでインストーラーを実行します。

Controllerの半分をアクティブなままにしておくことで、ユーザーはサイトにアクセスできます。VDAは残りのControllerに登録できます。Controllerの数が少ないため、サイトの容量が低下する場合があります。アップグレードによって、最終的なデータベースアップグレード手順中に新しいクライアント接続の確立が一時的に中断されるだけです。アップグレードされたControllerは、サイト全体がアップグレードされるまで要求を処理できません。

サイトにControllerが1つしかない場合、アップグレード中は動作しません。

実際のアップグレードが開始される前に、最初のControllerでサイトの事前テストが実行されます。詳細については、「サイトの事前テスト」を参照してください。

> **注:**
>
> Site Managerは、Delivery Controllerとともに自動的にアップグレードされます。

ステップ7：Web Studioのアップグレード

Web Studio をまだアップグレードしていない場合（別のコンポーネントと同じマシンにあったため）、Studio が含まれているマシンでインストーラーを実行します。

> **注:**
>
> Web Studio をアップグレードした後、バージョン情報がすぐに更新されない場合があります。Web Studio がすでに最新の状態であっても、アップグレードを促されることがあります。この問題に対処するには、Web Studio サーバーに移動し、インターネットインフォメー

ションサービス（IIS）マネージャーを開き、スタートページ > サイト > 既定の Web サイトに移動して、**再起動**を**Web サイトの管理**ペインで選択します。

ステップ 8: データベースとサイトをアップグレードする

注:

障害を回避するため、新しいマシンカタログの作成、マシンカタログの削除、デリバリーグループ内のマシンの更新など、プロビジョニングおよびデリバリーグループ関連のタスクを実行する前に、すべてのDelivery Controllerとデータベースをアップグレードする必要があります。

SQL Serverデータベースのスキーマを更新するために必要な権限については、準備を確認してください。

- SQL Serverデータベーススキーマを更新する十分な権限がある場合は、自動データベースアップグレードを開始できます。データベースとサイトを自動的にアップグレードするに進みます。
- データベースの十分な権限がない場合は、スクリプトを使用する手動アップグレードを開始し、データベース管理者（必要な権限を持つユーザー）の助けを借りて続行できます。手動アップグレードの場合、Site Managerユーザーがスクリプトを生成し、サービスを有効/無効にするスクリプトを実行します。データベース管理者は、SQLCMDユーティリティまたはSQLCMDモードのSQL Server Management Site Managerを使用して、データベーススキーマを更新する他のスクリプトを実行します。データベースとサイトを手動でアップグレードするに進みます。
- マルチゾーン展開でデータベースとサイトを自動的にアップグレードする場合、Citrix は、dbschema のアップグレードを、サイトの SQL Server データベースをホストするのと同じゾーンで実行することを推奨します。そうしないと、データベースとサイトの自動アップグレードが失敗する可能性があります。

Citrix は、アップグレード前にデータベースをバックアップすることを強く推奨します。CTX135207 を参照してください。データベースのアップグレード中は、製品サービスが無効になります。その間、Controller はサイトの新しい接続を仲介できないため、慎重に計画してください。

Site Managerを使用してデータベースとサイトを自動的にアップグレードする

1. アップグレードされたDelivery ControllerでSite Managerを起動します。
2. サイトのアップグレードを自動的に開始することを示し、準備ができたことを確認します。

PowerShellコマンドレットを使用してデータベースとサイトを自動的にアップグレードする

Site Managerを使用する代わりに、PowerShell SDKコマンドレット `Update-XDSite` を使用して、データベースとサイトを自動的にアップグレードします。詳細については、Citrix Virtual Apps and Desktops SDK Guideを参照してください。

1. 2番目のDelivery Controllerで、PowerShellセッションを開きます。
2. `Update-XDSite` コマンドレットを実行します。

コマンドレットは、アップグレードが必要なすべてのコンポーネントを自動的に検出し、次のアクションを実行します。

- データベース接続を切断し、必要なデータベーステーブルを更新し、サービスを再接続します。データベースが他のスクリプトまたはスタンドアロンツールによってすでにアップグレードされている場合、この手順はスキップされます。
- 環境に必要な追加のアップグレード手順を実行します。すでに完了しているグローバルレベルのアップグレードはスキップされます。

データベースとサイトを手動でアップグレードする

1. アップグレードされたDelivery ControllerでSite Managerを起動します。
2. サイトを手動でアップグレードすることを示します。ウィザードはライセンスサーバーの互換性を確認し、確認を求めます。
3. データベースをバックアップしたことを確認します。

   ウィザードは、スクリプトとアップグレード手順のチェックリストを生成して表示します。アップグレード対象の製品バージョン以降、データベースのスキーマが変更されていない場合、そのスクリプトは生成されません。たとえば、ログデータベースのスキーマが変更されない場合、`UpgradeLoggingDatabase.sql` スクリプトは生成されません。
4. 以下のスクリプトを記載されている順序で実行します。

   - `DisableServices.ps1`: Site Managerユーザーは、製品サービスを無効にするために、このPowerShellスクリプトをControllerで実行します。
   - `UpgradeSiteDatabase.sql`: データベース管理者は、サイトデータベースを含むサーバーでこのSQLスクリプトを実行します。

- `UpgradeMonitorDatabase.sql`: データベース管理者は、監視データベースを含むサーバーでこのSQLスクリプトを実行します。
- `UpgradeLoggingDatabase.sql`: データベース管理者は、構成ログデータベースを含むサーバーでこのSQLスクリプトを実行します。このスクリプトは、このデータベースが変更された場合（たとえば、ホットフィックスを適用した後など）にのみ実行してください。
- `EnableServices.ps1`: Site Managerユーザーは、製品サービスを有効にするために、このPowerShellスクリプトをControllerで実行します。

データベースのアップグレードが完了し、製品サービスが有効になると、Site Managerは環境と構成を自動的にテストし、HTMLレポートを生成します。問題が特定された場合は、データベースのバックアップを復元できます。問題を解決した後、データベースを再度アップグレードできます。

5. チェックリストのタスクを完了したら、**Finish upgrade** をクリックします。

ステップ 9: 残りのDelivery Controllerをアップグレードする

残りのDelivery Controllerをアップグレードします。アップグレードが完了したら、Site Managerを閉じて再度開きます。その後、Site Managerから、Delivery Controllerのサービスをサイトに登録するために追加のサイトアップグレードを実行するよう求められる場合があります。

ステップ 10: VDAをアップグレードする

> **重要:**
>
> VDAをバージョン1912以降にアップグレードする場合は、「VDAを1912以降にアップグレードする」を参照してください。

> VDAを含むマシンで製品インストーラーを実行します。

Machine Creation Services™とマスターイメージを使用してマシンを作成した場合、ホストに移動し、マスターイメージ上のVDAをアップグレードします。利用可能なVDAインストーラーのいずれかを使用できます。

- グラフィックインターフェイスのガイダンスについては、VDAのインストールを参照してください。
- コマンドラインのガイダンスについては、コマンドラインを使用したインストールを参照してください。

Citrix Provisioningを使用してマシンを作成した場合は、アップグレードに関するガイダンスについてCitrix Provisioning製品ドキュメントを参照してください。

手順 11: マシンカタログとデリバリーグループを更新する

- アップグレードされたVDAを持つマシンを使用するカタログを更新する。
- アップグレードされたVDAを持つマシンを使用するカタログをアップグレードする。
- アップグレードされたVDAを持つマシンを使用するデリバリーグループをアップグレードする。

手順 12: アップグレード後

展開内の他のコンポーネントをアップグレードします。ガイダンスについては、以下の製品ドキュメントを参照してください。

- StoreFront
- AppDNA
- Citrix App Layering (Citrixアプリケーションレイヤリング)
- HDX RealTime Optimization Pack (HDX RealTime最適化パック)
- プロファイル管理
- Citrix プロビジョニング
- セッションレコーディング
- ワークスペース環境管理

Microsoft SQL Server Express LocalDBソフトウェアを新しいバージョンに置き換える必要がある場合は、「SQL Server Express LocalDBの置き換え」を参照してください。

Dbschemaのアップグレード

展開を更新すると、複数のデータベーススキーマをアップグレードできます。次の表に、そのプロセスでアップグレードされるデータベーススキーマを示します。

From\To	1912 CU1	1912 CU2	1912 CU3	1912 CU4	1912 CU5	2203
7.15 RTM or 7.15 CU releases	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 RTM	Config	Site, Config	Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU1		Site	Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU2			Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU3				Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU4					Site, Config	Site; Monitor; Config; Logging
1912 CU5						Site; Monitor; Config; Logging
2112						Site; Monitor; Config

用語の定義:

- サイト: サイトデータストア。Dbschemaの更新はサイトデータストアに対して行われます。

- モニター: モニターデータストア。Dbschemaの更新はモニターデータストアに対して行われます。
- 構成: 構成テーブル。構成テーブルでは、Desktop Studioのバージョン、ライセンス情報、またはその両方が更新されます。
- ロギング: ロギングデータストア。Dbschemaの更新はロギングデータストアに対して行われます。

VDAを2203以降にアップグレードする

Personal vDisk (PvD) コンポーネントがVDAにインストールされていた場合、そのVDAはバージョン2203以降にアップグレードできません。新しいVDAを使用するには、現在のVDAをアンインストールしてから、新しいVDAをインストールする必要があります。

この指示は、PvDを一度も使用したことがない場合でも適用されます。

以前のバージョンでPvDコンポーネントがインストールされた可能性のある方法は次のとおりです。

- VDAインストーラーのグラフィカルインターフェイスでは、PvDは**追加コンポーネント**ページでオプションとして提供されていました。
- コマンドラインでは、`/baseimage` オプションによってPvDがインストールされました。このオプションを指定した場合、またはこのオプションを含むスクリプトを使用した場合は、PvDがインストールされました。

VDAにPvDがインストールされているかどうかわからない場合は、マシンまたはイメージで新しいVDA（2203以降）のインストーラーを実行してください。

- PvDがインストールされている場合、互換性のないコンポーネントがあることを示すメッセージが表示されます。
  - グラフィカルインターフェイスから、メッセージが表示されているページで**キャンセル**をクリックし、インストーラーを閉じたいことを確認します。
  - CLIからは、コマンドは表示されたメッセージとともに失敗します。
- PvDがインストールされていない場合、アップグレードが続行されます。

対処法

VDAにPvDがインストールされていない場合は、通常のアップグレード手順に従ってください。

VDAにPvDがインストールされている場合：

1. 現在のVDAをアンインストールします。
2. 新しいVDAをインストールします。

Windows 10 (1607以前、更新なし) マシンでPvDを継続して使用する場合は、VDA 7.15 LTSRが最新のサポート対象バージョンです。

> **注:**
>
> *XenAppおよびXenDesktop 7.15 LTSRでWindows 7デスクトップとPersonal vDiskを使用できますか？*
>
> Citrixは、January 2016に発表されたXenAppおよびXenDesktop 7.6 LTSRからPersonal vDisk (PvD) を除外しました。さらに、CitrixはPvDテクノロジの非推奨を発表し、今後はCitrix App Layeringの使用を開始することを推奨しています。Citrix App Layering (バージョン4.4以降) は、XenAppおよびXenDesktop 7.15 LTSRの互換コンポーネントです。しかし、Windows 7上の既存のPvD展開を持つお客様がCitrix App Layeringテクノロジに移行するのを支援するため、Citrixは、XenAppおよびXenDesktop 7.15 LTSR累積更新プログラム (CU) を通じて、Windows 7デスクトップ用のPvD展開に対する期間限定のサポートをJan 14, 2020まで提供することを決定しました。PvDコンポーネントはLTSR CUから削除され、Jan 14, 2020以降はサポートされません。また、Jan 14, 2020以降にWindows 7でPvDを使用すると、LTSRサイトは非準拠になります。さらに、Windows 10用のPvDは7.15 LTSRから引き続き除外されます。したがって、お客様は7.15 LTSRサイトでこれを使用しないでください。

PvD、AppDisks、およびサポートされていないホストを削除する

Citrix Virtual Apps and Desktops 7 Current Release展開では、以下のテクノロジーとホストタイプはサポートされていません。

- カタログ内のユーザーのVMの隣にデータを保存するための**Personal vDisks (PvD)**。ユーザーパーソナライゼーションレイヤー機能がユーザーの永続性を処理するようになりました。
- デリバリーグループで使用されるアプリケーションを管理するための**AppDisks**。
- **ホストタイプ:** Azure Classic、CloudPlatform (元のCitrix製品)。
    - このリリースでサポートされているホストタイプについては、システム要件を参照してください。

現在の展開でPvDまたはAppDisksを使用している場合、あるいはサポートされていないホストタイプ (例: Microsoft Azure Classic) への接続がある場合、それらのテクノロジーを使用する項目を削除した後にのみ、バージョン2006 (またはそれ以降のサポートされているバージョン) にアップグレードできます。現在の展開でパブリッククラウドホスト接続 (例: AWS) を使用している場合は、アップグレードする前にハイブリッドライツライセンスがあることを確認してください。インストーラーがサポートされていないテクノロジーまたはハイブリッドライツライセンスのないホスト接続を1つ以上検出すると、アップグレードは一時停止または停止し、説明メッセージが表示されます。インストーラーログには詳細が含まれています。

アップグレードを確実に成功させるために、サポートされていない項目を削除するための該当するガイダンスを確認し、それに従ってください。

- PvDを削除
- AppDisk を削除する
- サポートされていないホスト項目を削除する

展開でPvDまたはAppDiskを使用していなかった場合でも、関連するMSIが以前のVDAのインストールまたはアップグレードに含まれていた可能性があります。VDAをバージョン2006（またはそれ以降のサポートされているバージョン）にアップグレードする前に、そのソフトウェアを一度も使用していなかったとしても、削除する必要があります。グラフィカルインターフェイスを使用する場合、その削除は自動的に行われるか、CLIを使用する際に削除オプションを含めることができます。詳細については、「PvDまたはAppDiskコンポーネントを持つVDAのアップグレード」(#vdas-that-have-pvd-or-appdisks-components)を参照してください。

PvDを削除する

PvDを使用するように構成されているすべてのマシンを削除するまで、展開のアップグレードは成功しません。これはカタログとデリバリーグループに影響します。

グループとカタログからPvDを削除するには：

1. Studioで、デリバリーグループにPvDを使用するカタログのマシンが含まれている場合、「それらのマシンをグループから削除」(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/delivery-groups-manage.html#remove-a-machine-from-a-delivery-group)します。
2. Studioで、PvDを使用するマシンを含む「すべてのカタログを削除」(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/machine-catalogs-manage.html#delete-a-catalog)します。

VDAのアップグレード： 展開のアップグレードでは、VDAにAppDiskまたはPvDコンポーネントがインストールされているかどうかは検出されません。ただし、VDAインストーラーは検出しま

す。詳細については、「PvDまたはAppDiskコンポーネントを持つVDA」(#vdas-that-have-pvd-or-appdisks-components)を参照してください。

AppDiskを削除する

AppDiskを使用するすべてのデリバリーグループからAppDiskを削除し、その後AppDisk自体を削除するまで、展開のアップグレードは続行できません。

1. Studioのナビゲーションペインで**［デリバリーグループ］**を選択します。
2. グループを選択し、アクションペインで**［AppDiskの管理］**をクリックします。
3. グループからAppDiskを削除するアクションをクリックします。
4. AppDiskを使用する各デリバリーグループに対して、手順2と3を繰り返します。
5. StudioナビゲーションペインでAppDisksを選択します。
6. AppDiskを選択し、AppDiskを削除するアクションをクリックします。
7. 各AppDiskについて、手順5と6を繰り返します。

VDAのアップグレード: 展開のアップグレードでは、VDAにAppDiskまたはPvDコンポーネントがインストールされているかどうかは検出されません。ただし、VDAインストーラーは検出します。詳細については、「PvDまたはAppDisksコンポーネントがインストールされているVDA」を参照してください。

サポートされていないホストアイテムを削除する

サイトがCitrix CloudPlatformやMicrosoft Azure Classicなどのサポートされていないホストタイプへの接続を持っている場合、バージョン2006（またはそれ以降のサポートされているバージョン）への展開のアップグレードは続行できません。アップグレードを試みる前に、次のタスクを完了してください。

Studioから：

- サポートされていないホストへのすべての接続を削除します。
- デリバリーグループに、サポートされていないホストのマスターイメージで作成されたカタログのマシンが含まれている場合は、それらのマシンをグループから削除します。
- サポートされていないホストのマスターイメージを使用して作成されたすべてのカタログを削除します。

PvDまたはAppDisksコンポーネントがインストールされているVDA

PvDおよびAppDisksテクノロジーを有効にするコンポーネントがVDAにインストールされている場合、それらのコンポーネントが削除されるまで、そのVDAはアップグレードできません。

注:

バージョン1912にアップグレードする場合、現在のVDAをアンインストールしてから新しいVDAをインストールする必要がありました。このバージョンでは、Citrixがコンポーネントを削除してアップグレードを続行するかどうかを尋ねられます。

AppDiskおよびPvDコンポーネントは、それらのテクノロジーを一度も使用していなくても、以前のVDAバージョンでインストールされている可能性があります。

- グラフィカルインターフェイス：VDAインストーラーの**追加コンポーネント**ページには、**Citrix AppDisk / Personal vDisk**オプションが含まれていました。7.15 LTSRおよびそれ以前の7.xリリースでは、このオプションがデフォルトで有効になっていました。したがって、デフォルトを受け入れた場合（または、このオプションが提供されたリリースで明示的に有効にした場合）、そのコンポーネントがインストールされました。
- CLI: `/baseimage`オプションを指定すると、コンポーネントがインストールされました。

対処法

VDAインストーラーが現在インストールされているVDAでAppDisksまたはPvDコンポーネントを検出しない場合、アップグレードは通常どおり続行されます。

インストーラーが現在インストールされているVDAでAppDisksまたはPvDコンポーネントを検出した場合：

- グラフィックインターフェイス：アップグレードが一時停止します。サポートされていないコンポーネントを自動的に削除するかどうかを尋ねるメッセージが表示されます。**OK**をクリックすると、コンポーネントは自動的に削除され、アップグレードが続行されます。
- CLI：コマンドの失敗を避けるには、コマンドに次のオプションを含めます。
  - `/remove_appdisk_ack`
  - `/remove_pvd_ack`

制限事項

アップグレードには次の制限が適用されます。

- **選択的なコンポーネントのインストール：** 新しいバージョンにコンポーネントをインストールまたはアップグレードしても、アップグレードが必要な他のコンポーネント（別のマシン上）をアップグレードしないことを選択した場合、Studioから通知されます。たとえば、アッ

プグレードにControllerとStudioの新しいバージョンが含まれているとします。Controllerはアップグレードしましたが、Studioがインストールされているマシンでインストーラーを実行しませんでした。Studioは、Studioをアップグレードするまでサイトの管理を続行できません。

VDAをアップグレードする必要はありませんが、利用可能なすべての機能を使用できるように、すべてのVDAをアップグレードすることをお勧めします。

- **早期リリースまたはテクノロジプレビューバージョン：** 早期リリース、テクノロジプレビュー、またはプレビューバージョンからアップグレードすることはできません。
- **以前のオペレーティングシステム上のコンポーネント：** MicrosoftまたはCitrixでサポートされなくなったオペレーティングシステムに現在のVDAをインストールすることはできません。詳しくは、「以前のオペレーティングシステム」を参照してください。
- **混在環境/サイト：** 以前のバージョンのサイトと現在のバージョンのサイトを継続して実行する必要がある場合は、「混在環境に関する考慮事項」を参照してください。
- **製品の選択：** 以前のバージョンからアップグレードする場合、インストール時に設定された製品（Citrix Virtual AppsまたはCitrix Virtual Apps and Desktops）を選択または指定することはありません。

混在環境に関する考慮事項

アップグレード時には、エディションとバージョンで利用可能なすべての新機能と強化された機能にアクセスできるように、すべてのコンポーネントとVDAをアップグレードすることをお勧めします。

例えば、以前のControllerバージョンを含む展開で現在のVDAを使用することはできますが、現在のリリースで追加された新機能は利用できない場合があります。最新ではないバージョンを使用している場合、VDA登録の問題も発生する可能性があります。

一部の環境では、すべてのVDAを最新バージョンにアップグレードできない場合があります。その場合、マシンカタログを作成する際に、マシンにインストールされているVDAバージョンを指定できます。(これは機能レベルと呼ばれます。)デフォルトでは、この設定は推奨される最小VDAバージョンを指定します。ほとんどの展開では、デフォルト値で十分です。カタログにデフォルトよりも古いVDAが含まれている場合にのみ、設定を以前のバージョンに変更することを検討してください。マシンカタログ内でVDAバージョンを混在させることは推奨されません。

カタログがデフォルトの最小VDAバージョン設定で作成され、1つ以上のマシンがデフォルトバージョンよりも古いVDAを持っている場合、それらのマシンはControllerに登録できず、機能しません。

詳細については、VDAバージョンと機能レベルを参照してください。

異なるバージョンを持つ複数のサイト

環境に異なる製品バージョンを持つサイト（例えば、XenDesktop 7.18サイトとCitrix Virtual Apps and Desktops 1909サイト）が含まれている場合、CitrixはStoreFrontを使用して異なる製品バージョンからのアプリケーションとデスクトップを集約することを推奨します。詳細については、StoreFrontのドキュメントを参照してください。

混在環境では、各リリースに対応するStudioおよびDirectorのバージョンを引き続き使用しますが、異なるバージョンは別々のマシンにインストールされていることを確認してください。

以前のオペレーティングシステム

サポートされているオペレーティングシステム（OS）バージョンを実行しているマシンに、コンポーネントの以前のバージョンをインストールしたとします。現在、より新しいコンポーネントバージョンを使用したいと考えていますが、そのOSは現在のコンポーネントバージョンではサポートされていません。

たとえば、Windows Server 2016マシンにサーバーVDAをインストールしたとします。現在、そのVDAを現在のリリースにアップグレードしたいが、アップグレード先の現在のリリースではWindows Server 2016がサポートされていません。

許可されていないオペレーティングシステムにコンポーネントをインストールまたはアップグレードしようとすると、「このオペレーティングシステムにはインストールできません」などのエラーメッセージが表示されます。

これらの考慮事項は、Current ReleaseおよびLong Term Service Releaseバージョンのアップグレードに適用されます。（LTSRバージョンにCUを適用することには影響しません。）

サポートされているOSについては、以下のリンクを参照してください。

- Citrix Virtual Apps and Desktops (現在のリリース):
  - デリバリーコントローラー、スタジオ、ディレクター、VDA、ユニバーサルプリントサーバー
  - フェデレーション認証サービス
  - StoreFront、セルフサービスパスワードリセット、およびセッションレコーディングについては、現在のリリースのシステム要件の記事を参照してください。

- LTSRについては、お使いのLTSRバージョンとCUのコンポーネントリストを参照してください。(メインのCitrix Virtual Apps and Desktops製品ドキュメントページからお使いのLTSRバージョンを選択してください。)

無効なオペレーティングシステム

以下の表に、現在のリリースでコンポーネントのインストール/アップグレードに無効な以前のオペレーティングシステムを示します。各OSでサポートされる最新の有効なコンポーネントバージョンと、インストールおよびアップグレードが無効になったコンポーネントバージョンを示します。

表中のオペレーティングシステムにはサービスパックと更新プログラムが含まれます。

オペレーティングシステム	コンポーネント/機能	最新の有効なバージョン	インストール/アップグレードが不可能になったバージョン
Windows 7および Windows 8	VDA	7.15 LTSR	7.16
Windows 7および Windows 8	その他のインストーラーコンポーネント	7.17	7.18
Windows 10 バージョン 1607 より前のもの	VDA	7.15 LTSR	7.16
Windows 10 x86 バージョン	VDA	1906.2.0	1909
Windows サーバー 2008 R2	VDA	7.15 LTSR	7.16
Windows サーバー 2008 R2	その他のインストーラーコンポーネント	7.17	7.18
Windows サーバー 2012	VDA	7.15 LTSR	7.16
Windows サーバー 2012	その他のインストーラーコンポーネント	7.17	7.18

オペレーティングシステム	コンポーネント/機能	最新の有効なバージョン	インストール/アップグレードが不可能になったバージョン
ウィンドウズ サーバー 2012 R2	その他のインストーラーコンポーネント *	1912 LTSR	2003
ウィンドウズ サーバー 2012 R2	サーバーVDI	7.15 LTSR	7.16
ウィンドウズ サーバー 2016	サーバーVDI	7.15 LTSR	7.16

Windows XPおよびWindows Vistaは、7.xのコンポーネントまたはテクノロジーでは無効です。

* Delivery Controller、Studio、Director、およびVDAに適用されます。

実行できること

選択肢があります。次のことができます。

- 現在のOSを継続して使用する(#continue-with-the-current-os)
- マシンの再イメージ化またはアップグレード(#reimage-or-upgrade-the-machine)
- 新しいマシンを追加してから古いマシンを削除する(#add-new-machines-and-then-remove-old-machines)

現在のOSを継続して使用する

これらの方法はVDAで実行可能です。以前のOSを搭載したマシンの使用を継続する場合は、次のいずれかを選択できます。

- インストールされているコンポーネントバージョンを継続して使用する。
- 最新の有効なコンポーネントバージョンをダウンロードし、そのバージョンにコンポーネントをアップグレードする。（これは、最新の有効なコンポーネントバージョンがまだインストールされていないことを前提としています。）

たとえば、Windows 7 SP1マシンに7.14 VDAがインストールされているとします。Windows 7 OSマシンで有効な最新のVDAバージョンは、XenApp and XenDesktop 7.15 LTSRです。7.14を継続して使用するか、7.15 LTSR VDAをダウンロードしてVDAをそのバージョンにアップグレードすることができます。これらの以前のVDAバージョンは、新しいバージョンのDelivery Controllerを

含む展開で動作します。たとえば、7.15 LTSR VDAはCitrix Virtual Apps and Desktops 7 1808 Controllerに接続できます。

マシンの再イメージ化またはアップグレード

これらの方法は、VDAおよびコアコンポーネント（Delivery Controllerなど）がインストールされていないその他のマシンで実行可能です。次のいずれかを選択してください。

- マシンをサービスから外し（メンテナンスモードをオンにしてすべてのセッションを閉じさせてから）、サポートされているWindows OSバージョンに再イメージ化し、コンポーネントの最新バージョンをインストールできます。
- 再イメージ化せずにVDAマシンでOSをアップグレードするには、まずアップグレード先のOSでサポートされているVDAバージョンをインストールするか、OSのアップグレード後にVDAをアップグレードする必要があります。そうしないと、Citrixソフトウェアはサポートされません。VDAをアンインストールせずにインプレースアップグレードを実行する場合、次の最小OSバージョンにアップグレードできます。
  - 2023-07 Cumulative Update for Windows 11 (KB5028185)以降がインストールされているWindows 11（ビルド22621.1992以降）。
  - 2023-07 Dynamic Update for Windows 10 (KB5028311)がインストールされているWindows 10。
- アップグレードを計画しているWindowsのバージョンが上記のガイドラインに合致しない場合は、OSをアップグレードする前にVDAをアンインストールし、OSのアップグレードが完了した後にサポートされているVDAバージョンをインストールする必要があります。

新しいマシンを追加し、古いマシンを削除する

この方法は、Delivery Controller™ またはその他のコアコンポーネントを含むマシンの OS をアップグレードする必要がある場合に実行可能です。

Citrix は、サイト内のすべてのコントローラーが同じ OS を持つことを推奨しています。以下のアップグレードシーケンスは、異なるコントローラーが異なる OS を持つ期間を最小限に抑えます。

1. サイト内のすべての Delivery Controller のスナップショットを取得し、サイトデータベースをバックアップします。
2. サポートされているオペレーティングシステムを搭載したクリーンなサーバーに新しいDelivery Controllerをインストールします。
3. 新しいコントローラーをサイトに追加します。

4. 現在のリリースで無効なオペレーティングシステムで実行されているControllerを削除します。Controllerの削除に関する推奨事項については、「(/ja-jp/citrix-virtual-apps-desktops/current-release/manage-deployment/delivery-controllers.html) 」を参照してください。

準備

アップグレードを開始する前に、以下の情報を確認し、必要なタスクを完了してください。

> **注:**
>
> VDA のアップグレードは アップグレードシーケンス の後半で行われますが、アップグレードを開始する前にインストーラーを選択し、手順を確認して、何が予想されるかを知っておくことをお勧めします。

インストーラーとインターフェイスを選択する

コンポーネントをアップグレードするには、製品ISOのフルプロダクトインストーラーを使用します。VDAは、フルプロダクトインストーラーまたはスタンドアロンVDAインストーラーのいずれかを使用してアップグレードできます。すべてのインストーラーは、グラフィカルインターフェイスとコマンドラインインターフェイスを提供します。

詳細については、インストーラー を参照してください。

インストールの詳細: 準備作業を完了し、インストーラーを起動する準備ができたら、インストール記事には、表示される内容 (グラフィカルインターフェイスを使用している場合) または入力する内容 (コマンドラインインターフェイスを使用している場合) が示されています。

- グラフィカルインターフェイスを使用してコアコンポーネントをインストール/アップグレードする
- コマンドラインを使用してコアコンポーネントをインストール/アップグレードする
- グラフィカルインターフェイスを使用したVDAのインストール/アップグレード
- コマンドラインを使用したVDAのインストール/アップグレード

シングルセッションオペレーティングシステムには、4種類のインストーラーがあります。Citrixでは、Citrix VDAのライフサイクル全体（インストール、アップグレード、アンインストールを含む）で一貫したインストーラータイプを使用することをお勧めします。詳しくは、「シングルセッションVDAインストーラーを使用するためのベストプラクティス」を参照してください。

VDAを現在のリリースにアップグレードする際、アップグレードプロセス中にマシンの再起動が発生します（この要件は7.17リリースから始まりました）。これは回避できません。再起動後、アップグレードは自動的に再開されます（コマンドラインで`/noresume`を指定しない限り）。

データベース操作

サイト、監視、および構成ログデータベースをバックアップします。CTX135207の手順に従ってください。アップグレード後に問題が発見された場合、バックアップを復元できます。

サポートされなくなったSQL Serverバージョンのアップグレードについては、SQL Serverバージョンチェックを参照してください。（これは、サイト、モニター、および構成ログデータベースに使用されるSQL Serverを指します。）

Microsoft SQL Server Express LocalDBは、ローカルホストキャッシュで使用するために自動的にインストールされます。以前のバージョンを置き換える必要がある場合、新しいバージョンはSQL Server Express LocalDB 2019である必要があります。コンポーネントとサイトをアップグレードした後にSQL Server Express LocalDBを新しいバージョンに置き換える方法の詳細については、SQL Server Express LocalDBの置き換えを参照してください。

Citrixライセンスが最新であることを確認する

Citrixライセンスの管理に関する包括的な情報については、Citrixライセンスのアクティブ化、アップグレード、および管理を参照してください。

フルプロダクトインストーラーを使用してライセンスサーバーをアップグレードできます。または、ライセンスコンポーネントを個別にダウンロードしてアップグレードすることもできます。アップグレードを参照してください。

アップグレードする前に、Customer Success Services / Software Maintenance / Subscription Advantageの有効期限が新しい製品バージョンに対応していることを確認してください。日付は2021年11月15日以降である必要があります。

Citrixライセンスサーバーの互換性を確認する

Citrixライセンスサーバーが新しいバージョンと互換性があることを確認してください。これには2つの方法があります。

- 他のCitrixコンポーネントをアップグレードする前に、Delivery Controllerを含むマシンでISOレイアウトから`XenDesktopServerSetup.exe`インストーラーを実行します。互換性の問題がある場合、インストーラーは推奨される解決手順とともにそれを報告します。
- インストールメディアの`XenDesktop Setup`ディレクトリから、コマンド`.\LicServVerify.exe -h <license-server-fqdn> -p 27000 -v`を実行します。表示でライ

センスサーバーが互換性があるかどうかが示されます。ライセンスサーバーに互換性がない場合は、ライセンスサーバーをアップグレードしてください。

StoreFrontの変更をバックアップする

アップグレードを開始する前に、`C:\inetpub\wwwroot\Citrix\<StoreName>\App_Data` 内のファイル（*default.ica* や *usernamepassword.tfrm* など）を変更している場合は、各ストア用にそれらをバックアップしてください。アップグレード後、それらを復元して変更を元に戻すことができます。

アプリケーションとコンソールを閉じる

アップグレードを開始する前に、管理コンソールやPowerShellセッションなど、ファイルロックを引き起こす可能性のあるすべてのプログラムを閉じます。

マシンを再起動すると、ファイルロックがすべて解除され、保留中のWindowsアップデートがないことが保証されます。

アップグレードを開始する前に、サードパーティの監視エージェントサービスをすべて停止して無効にします。

適切な権限があることを確認する

ドメインユーザーであることに加えて、製品コンポーネントをアップグレードするマシンではローカル管理者である必要があります。

サイトデータベースとサイトは、自動または手動でアップグレードできます。データベースの自動アップグレードの場合、Studioユーザーの権限には、SQL Serverデータベーススキーマを更新する機能（たとえば、`db_securityadmin` または `db_owner` データベースロール）が含まれている必要があります。詳細については、「データベース」を参照してください。

Studioユーザーがこれらの権限を持っていない場合、手動データベースアップグレードを開始すると、スクリプトが生成されます。Studioユーザーは、Studioから一部のスクリプトを実行します。データベース管理者は、SQL Server Management Studioなどのツールを使用して、他のスクリプトを実行します。

その他の準備タスク

- 必要に応じて、テンプレートをバックアップし、ハイパーバイザーをアップグレードします
- 事業継続計画で定められているその他の準備タスクを完了します。

サイトの事前テスト

Delivery Controllerとサイトをアップグレードすると、実際のアップグレードが始まる前に予備サイトテストが実行されます。これらのテストでは、以下が検証されます。

- サイトデータベースにアクセスでき、バックアップされていること
- 重要なCitrixサービスへの接続が正しく機能していること
- Citrixライセンスサーバーのアドレスが利用可能であること
- 構成ログデータベースにアクセスできること
- パブリッククラウドホスト接続（例：AWS）を追加する場合は、ハイブリッド権限ライセンスがあることを確認してください。そうしないと、予備サイトテストが一時停止または停止し、説明メッセージが表示されます。

テストの実行後、結果のレポートを表示できます。検出された問題を修正し、テストを再度実行できます。予備サイトテストを実行せず、問題を解決しないと、サイトの動作に影響を与える可能性があります。

テスト結果を含むレポートは、インストールログと同じディレクトリにあるHTMLファイル（`PreliminarySiteTestResult.html`）です。そのファイルが存在しない場合は作成されます。ファイルが存在する場合は、その内容が上書きされます。

テストを実行する

- インストーラーのグラフィカルインターフェイスを使用してアップグレードする場合、ウィザードにはテストを開始してレポートを表示できるページが含まれています。テストが実行され、レポートを確認し、見つかった問題を解決した後、テストを再実行できます。テストが正常に完了したら、 をクリックしてウィザードを続行します。
- コマンドラインインターフェイスを使用してアップグレードする場合、テストは自動的に実行されます。デフォルトでは、テストが失敗した場合、アップグレードは実行されません。レポートを確認し、問題を解決した後、コマンドを再実行してください。

Citrixは、Controllerとサイトのアップグレードを続行する前に、常に予備サイトテストを実行し、問題を解決することを推奨しています。テストを実行するのにかかるわずかな時間で得られる潜在的なメリットは十分にあります。ただし、この推奨されるアクションを上書きすることもできます。

- グラフィカルインターフェイスでアップグレードする場合、テストをスキップしてアップグレードを続行することを選択できます。
- コマンドラインからアップグレードする場合、テストをスキップすることはできません。デフォルトでは、サイトテストが失敗すると、アップグレードを実行せずにインストーラーが失

敗します。通常、`/ignore_site_test_failure` オプションを含めると、テストの失敗は無視され、アップグレードが続行されます。(例外については、SQL Server のバージョンチェック を参照してください。)

複数のControllerをアップグレードする場合

1つのControllerでアップグレードを開始し、その後、同じサイト内の別のControllerでアップグレードを開始した場合（最初のアップグレードが完了する前）：

- 最初のControllerで予備サイトテストが完了している場合、他のControllerのウィザードには予備サイトテストページは表示されません。
- 他のControllerでアップグレードを開始したときに最初のControllerでのテストが進行中の場合、他のControllerのウィザードにサイトテストページが表示されます。ただし、最初のControllerでのテストが完了すると、最初のControllerからのテスト結果のみが保持されます。

サイトの健全性に関連しないテストの失敗

- 予備サイトテストがメモリ不足で失敗した場合は、より多くのメモリを確保してからテストを再実行してください。
- アップグレードの権限はあるがサイトテストを実行する権限がない場合、予備サイトテストは失敗します。これを解決するには、テストを実行する権限を持つユーザーアカウントでインストーラーを再実行してください。

SQL Serverバージョンの確認

Citrix Virtual Apps and Desktopsの展開を成功させるには、サイト、モニター、および構成ログデータベース用にサポートされているバージョンのMicrosoft SQL Serverが必要です。サポートされなくなったSQL ServerバージョンでCitrix展開をアップグレードすると、機能上の問題が発生する可能性があり、サイトはサポート対象外となります。

アップグレード先のCitrixリリースでサポートされているSQL Serverのバージョンについては、そのリリースのシステム要件の記事を参照してください。

Controllerをアップグレードする際、Citrixインストーラーは、サイト、モニター、および構成ログデータベースに使用されている現在インストールされているSQL Serverのバージョンを確認します。

- チェックの結果、現在インストールされているSQL Serverのバージョンが、アップグレード先のCitrixリリースでサポートされているバージョンではないと判断された場合：

  - グラフィカルインターフェイス：アップグレードはメッセージとともに停止します。「**了解**」をクリックし、次に「**キャンセル**」をクリックしてCitrixインストーラーを閉じます。（アップグレードを続行することはできません。）
  - コマンドラインインターフェイス：コマンドは失敗します（コマンドに`/ignore_db_check_failure`オプションを含めた場合でも）。

  SQL Serverのバージョンをアップグレードしてから、Citrixのアップグレードを再度開始してください。
- チェックで現在インストールされているSQL Serverのバージョンを特定できない場合は、現在インストールされているバージョンがアップグレード先のバージョンでサポートされているかどうかを確認してください（システム要件）。
  - グラフィカルインターフェイス: アップグレードがメッセージとともに停止します。
    - 現在インストールされているSQL Serverのバージョンがサポートされている場合は、**I understand**をクリックしてメッセージを閉じ、**Next**をクリックしてCitrixのアップグレードを続行します。
    - 現在インストールされているSQL Serverのバージョンがサポートされていない場合は、**I understand**をクリックしてメッセージを閉じ、**Cancel**をクリックしてCitrixのアップグレードを終了します。SQL Serverをサポートされているバージョンにアップグレードしてから、Citrixのアップグレードを再度開始してください。
  - コマンドラインインターフェイス: コマンドがメッセージとともに失敗します。メッセージを閉じた後:
    - 現在インストールされているSQL Serverのバージョンがサポートされている場合は、`/ignore_db_check_failure`オプションを指定してコマンドを再度実行します。
    - 現在インストールされているSQL Serverのバージョンがサポートされていない場合は、SQL Serverをサポートされているバージョンにアップグレードします。コマンドを再度実行してCitrixのアップグレードを開始します。

SQL Serverのアップグレード

新しいSQL Serverサーバーを立ち上げてサイトデータベースを移行する場合、接続文字列を更新する必要があります。

サイトが現在、サイトデータベースにSQL Server Expressを使用している場合 (Citrixがサイト作成時に自動的にインストールしたもの):

1. 最新のSQL Server Expressバージョンをインストールします。

2. データベースをデタッチします。
3. データベースを新しいSQL Server Expressにアタッチします。
4. 接続文字列を移行します。

詳細については、接続文字列の構成およびMicrosoft SQL Serverの製品ドキュメントを参照してください。

SQL Server Express LocalDBの置き換え

Microsoft SQL Server Express LocalDB は、Local Host Cache がスタンドアロンで使用する SQL Server Express の機能です。Local Host Cache は、SQL Server Express LocalDB 以外の SQL Server Express のコンポーネントを必要としません。

Delivery Controller を Citrix Virtual Apps and Desktops バージョン 2203 LTSR 以降のバージョンにアップグレードする場合、サポートされるバージョンは SQL Server Express LocalDB 2019 または SQL Server Express LocalDB 2022 です。

SQL Server Express LocalDBを更新する方法は2つあります。

- 自動更新
- 手動更新

自動更新

Delivery Controllerをアップグレードすると、メタインストーラーはSQL Server Express LocalDBの最新の互換バージョンを自動的にインストールします。メタインストーラーは古いLocalDBバージョンをアンインストールしません。新しいバージョンが正しく動作することを確認した後、古いバージョンを手動でアンインストールする必要があります。

新しいSQL Server Express LocalDBのインストールを確認する

古いバージョンをアンインストールする前に、新しいSQL Server Express LocalDBのインストールが正しく動作していることを確認してください。

1. コマンドプロンプトを使用してSqlLocalDBインスタンスに移動します。
    - SQL LocalDB 2014 の場合: `cd C:\Program Files\Microsoft SQL Server\120\Tools\Binn`
    - SQL LocalDB 2017 の場合: `cd C:\Program Files\Microsoft SQL Server\140\Tools\Binn`

- SQL LocalDB 2019 の場合: `cd C:\Program Files\Microsoft SQL Server\150\Tools\Binn`
- SQL LocalDB 2022 の場合: `cd C:\Program Files\Microsoft SQL Server\160\Tools\Binn`

2. `SqlLocalDB i`を実行します。

   CitrixHA と MSSQLLocalDB の 2 つのファイルが表示されるはずです。

手動更新

前提条件

- Citrix Virtual Apps and Desktopsのインストールメディア。
- Windows SysinternalsツールボックスのPsExecツール。

手順

1. Citrix Virtual Apps and Desktopsのコンポーネント、データベース、およびサイトのアップグレードを完了します。（これらのデータベースアップグレードは、サイト、監視、および構成ログデータベースに影響します。SQL Server Express LocalDBを使用するローカルホストキャッシュデータベースには影響しません。）
2. SQL Server Express LocalDBを更新するDelivery Controllerにログオンします。
3. MicrosoftからPsExecをダウンロードし、そのDelivery Controller上のアクセスしやすい場所（例: C:\Temp）に配置します。
4. WindowsシステムサービスからDelivery Controller上のCitrix High Availability Serviceを停止します。
5. Delivery Controllerでコマンドプロンプトを開き、PsExecがある場所（例: `C:\Temp`）に移動し、次のコマンドを実行してNetwork Serviceアカウントでコマンドプロンプトを昇格させます:

   ```
   psexec -i -u "NT AUTHORITY\NETWORKSERVICE" cmd
   ```

6. `whoami`を実行して、コマンドプロンプトがNetwork Serviceアカウントとして実行されていることを確認します。次の出力が表示されるはずです: `nt authority\networkservice`。
7. コマンドプロンプトを使用してSQL LocalDBインスタンスに移動します:

   - SQL LocalDB 2014からアップグレードする場合:

```
cd "C:\Program Files\Microsoft SQL Server\120\Tools\Binn"
```

- SQL LocalDB 2017からアップグレードする場合:

```
cd "C:\Program Files\Microsoft SQL Server\140\Tools\Binn"
```

- SQL LocalDB 2019からアップグレードする場合:

```
cd "C:\Program Files\Microsoft SQL Server\150\Tools\Binn"
```

8. SQL LocalDBインスタンスを停止して削除します: `CitrixHA`。

```
SqlLocalDB stop CitrixHA



SqlLocalDB delete CitrixHA
```

9. Delivery Controllerから以下のファイルを削除します:

```
C:\Windows\ServiceProfiles\NetworkService\HADatabaseName.*

C:\Windows\ServiceProfiles\NetworkService\HADatabaseName_log.*

C:\Windows\ServiceProfiles\NetworkService\HAImportDatabaseName.* (if
exists)

C:\Windows\ServiceProfiles\NetworkService\HAImportDatabaseName_log.*
(if exists)
```

10. プログラムを削除するためのWindowsネイティブ機能を使用して、Delivery Controllerから既存のSQL LocalDB SQL Server Expressをアンインストールします。
11. アンインストールが完了したら、Delivery Controllerを再起動します。
12. WindowsシステムサービスからDelivery Controller上のCitrix High Availability Serviceを停止します。
13. Citrix Virtual Apps and Desktopsインストールメディアを Delivery Controllerにマウントします。

14. Delivery ControllerにSQL Server Express LocalDB 2022を管理者としてインストールします。

    a. Citrix Virtual Apps and Desktopsインストールメディアの`Support > SQLLocalDB`フォルダーにある`sqllocaldb.msi`ファイルを使用します。たとえば、インストールメディアが`E drive`ドライブ文字にマウントされている場合、ファイルは`E:\Support\SQLLocalDB\sqllocaldb.msi`にあります。インストールを完了するには再起動が必要です。

    b. 新しいSQL LocalDBは`C:\Program Files\Microsoft SQL Server\160\Tools\Binn`にある必要があります。

15. WindowsシステムサービスからDelivery Controller上のCitrix High Availability Serviceを開始します。

16. Delivery Controllerのコマンドプロンプトで、`C:\Program Files\Microsoft SQL Server\160\Tools\Binn`に移動し、`SqlLocalDB i`を実行してCitrixHAインスタンスが作成されたことを確認します。返されたインスタンスのリストに`CitrixHA`が含まれている必要があります。

    > **注:**
    >
    > Citrix High Availability Serviceの開始後、CitrixHAデータベースが作成されるまでに最大15分かかる場合があります。

17. 必要に応じてHigh Availability Service（セカンダリブローカー）が引き継ぐことができることを確認するために、ローカルホストキャッシュデータベースファイルが作成されていることを確認します。

    a. Delivery Controllerで、`C:\Windows\ServiceProfiles\NetworkService`を参照します。

    b. `HaDatabaseName.mdf`と`HaDatabaseName_log.ldf`が作成されていることを確認します。

18. 残りのDelivery Controllerで手順を繰り返します。

VDAアップグレードエージェントのプロキシサポート

VDAアップグレードエージェントのプロキシサポートは、2311 VDAで追加されました。

2311 VDA (バージョン: 7.40) のVDAアップグレードエージェントは、プロキシを介してトラフィックを認識し、送信できます。

VDAアップグレードエージェント (VUA) は、Hostname:Port (IP:Port) およびPACファイルの形式でプロキシをサポートしています。

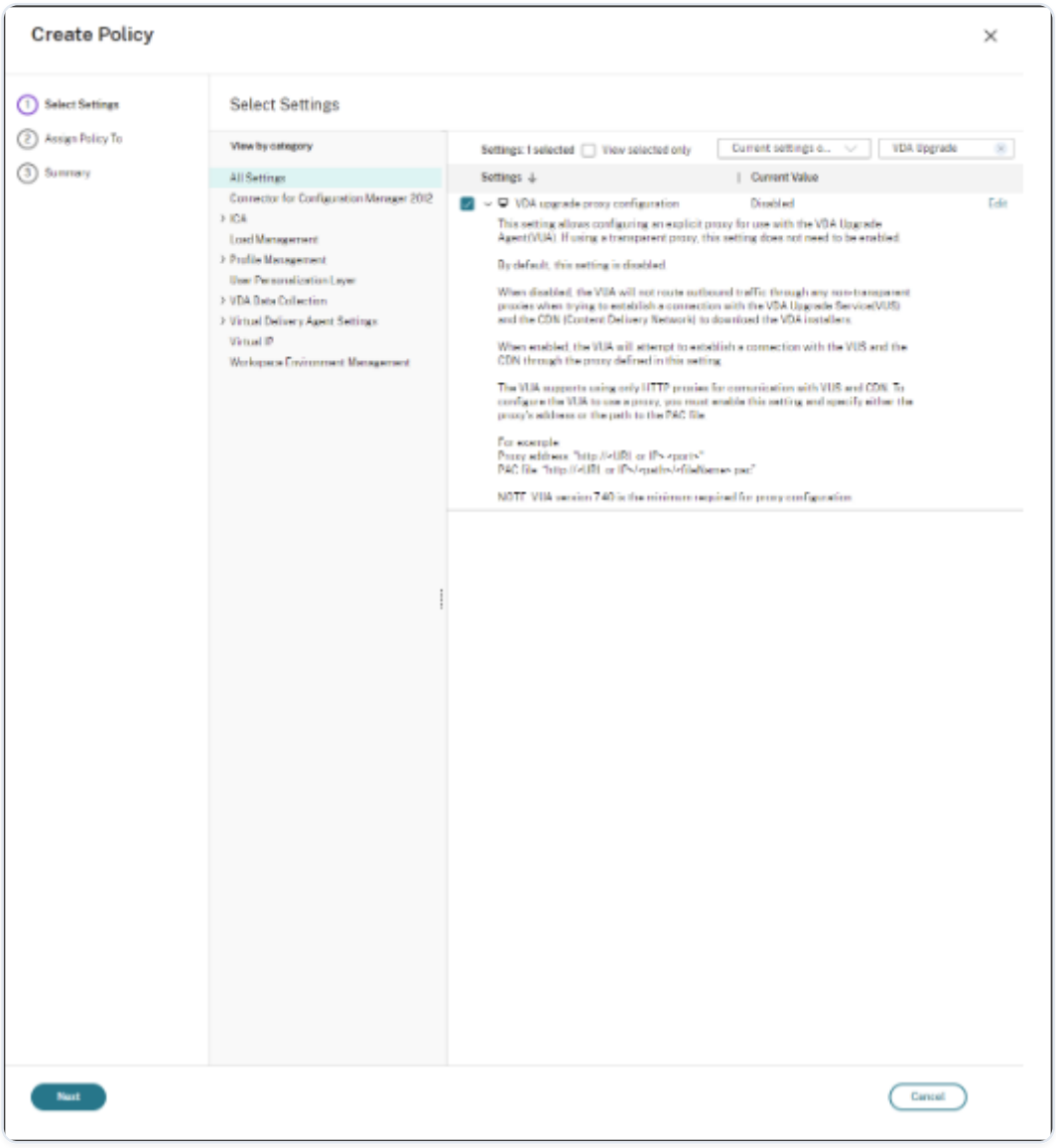
HTTPプロキシのみがサポートされています。 パケットの復号化と検査はサポートされていません。

プロキシ認証はサポートされていません。 SOCKS5はサポートされていません。

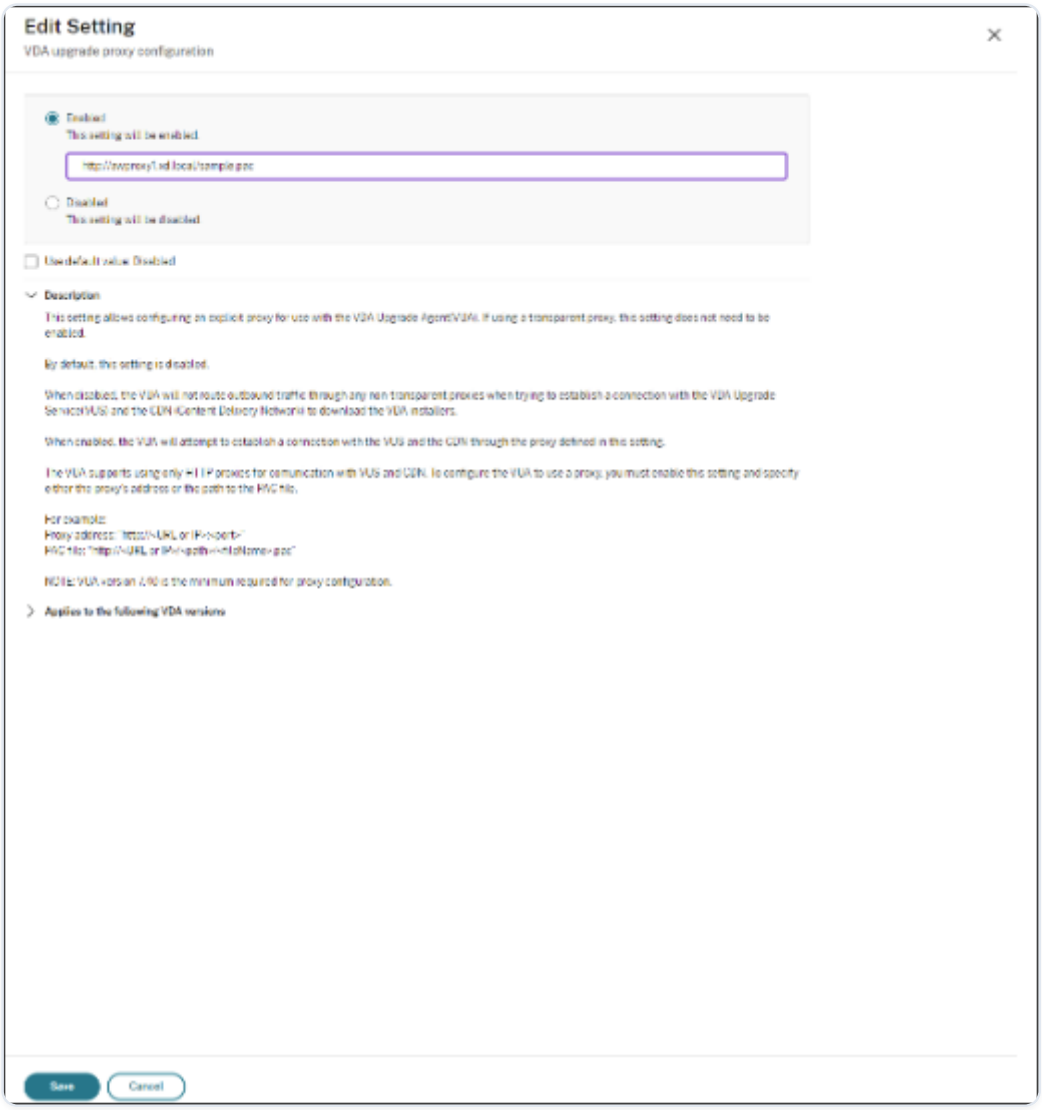
VDAアップグレードエージェントプロキシの構成

VDAアップグレードエージェントプロキシは、次の2つの方法で構成できます。

1. **Webstudioポリシー**を使用した**VDAアップグレードエージェントポリシーの構成**。
2. **ポリシーの作成**ページで、**設定**から**VDAアップグレードプロキシ構成**を選択します。



3. この設定を有効にします。デフォルトでは、この設定は無効になっています。



4. レジストリキーを使用したVDAアップグレードエージェントの構成。

   レジストリキーは、VDAインストール中にMeta-Installerに設定されます。

   レジストリ:

   キー: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent`

   値の型: 文字列

   値の名前: ProxySettings

   値のデータ: プロキシアドレスまたはPACファイルへのパス。

   例:

   a. プロキシアドレス: `http://<URL or IP>:<port>`
   b. Pacファイル: `http://<URL or IP>/<path/<filename>.pac`

セキュリティ

Citrix Virtual Apps and Desktops™ は、セキュリティニーズに合わせて環境を調整できる、設計段階から安全なソリューションを提供します。

モバイルワーカーに関してIT部門が直面するセキュリティ上の懸念の1つは、データの紛失または盗難です。Citrix Virtual Apps and Desktops™ は、アプリケーションとデスクトップをホストすることで、すべてのデータをデータセンターに保持し、機密データと知的財産をエンドポイントデバイスから安全に分離します。データ転送を許可するポリシーが有効になっている場合、すべてのデータは暗号化されます。

Citrix Virtual Apps and Desktops のデータセンターは、一元化された監視および管理サービスにより、インシデント対応も容易にします。Director を使用すると、IT部門はネットワーク全体でアクセスされているデータを監視および分析でき、Studio を使用すると、IT部門は各エンドユーザーデバイスでローカルに問題を修正する代わりに、データセンター内のほとんどの脆弱性をパッチ適用して修復できます。

Citrix Virtual Apps and Desktops は、監査と規制コンプライアンスも簡素化します。調査官は、一元化された監査証跡を使用して、誰がどのアプリケーションとデータにアクセスしたかを判断できるためです。Director は、構成ログと OData API にアクセスすることで、システムへの更新とユーザーデータ使用量に関する履歴データを収集します。

委任管理により、Citrix Virtual Apps and Desktops へのアクセスをきめ細かく制御するための管理者ロールを設定できます。これにより、組織内で特定の管理者にタスク、操作、スコープへのフルアクセスを許可し、他の管理者には制限されたアクセスを許可する柔軟性が得られます。

シトリックス バーチャルアプリ＆デスクトップは、ローカルレベルから組織単位レベルまで、ネットワークのさまざまなレベルでポリシーを適用することにより、管理者にユーザーに対するきめ細かな制御を提供します。このポリシーの制御により、ユーザー、デバイス、またはユーザーとデバイスのグループが接続、印刷、コピー/貼り付け、またはローカルドライブのマッピングができるかどうかが決定され、サードパーティの臨時作業者に関するセキュリティ上の懸念を最小限に抑えることができます。管理者は、デスクトップロック機能も使用でき、エンドユーザーが仮想デスクトップのみを使用できるようにし、エンドユーザーデバイスのローカルオペレーティングシステムへのアクセスを防止します。

管理者は、サイトを構成して、Controller の、またはエンドユーザーと Virtual Delivery Agents (VDA) 間の Transport Layer Security (TLS) プロトコルを使用するようにすることで、Citrix Virtual Apps または Citrix Virtual Desktops のセキュリティを強化できます。このプロトコルは、TCP/IP 接続のサーバー認証、データストリーム暗号化、およびメッセージ整合性チェックを提供するために、サイトで有効にすることもできます。

Citrix Virtual Apps and Desktops は、Windows または特定のアプリケーションの多要素認証もサポートしています。多要素認証は、Citrix Virtual Apps and Desktops によって提供されるすべてのリソースを管理するためにも使用できます。これらの方法には以下が含まれます。

- トークン
- スマートカード
- RADIUS
- ケルベロス
- 生体認証

Citrix Virtual Desktops は、ID管理からウイルス対策ソフトウェアまで、多くのサードパーティ製セキュリティソリューションと統合できます。サポートされている製品のリストは `<http://www.citrix.com/ready>` で確認できます。

Citrix Virtual Apps and Desktops の一部のリリースは、Common Criteria 標準の認定を受けています。これらの標準のリストについては、`<https://www.commoncriteriaportal.org/cc/>` にアクセスしてください。

フェデレーション認証サービス

Citrix Federated Authentication Service (FAS) は、SAML や OpenID Connect (OIDC) などの最新のIDプロバイダーを介してユーザーが認証し、Windowsパスワードを提供しない環境において、Citrix仮想デスクトップおよびアプリケーションへのシングルサインオン (SSO) を可能にし、Active Directoryドメインに参加しているセッションホストへのシームレスなアクセスを保証します。

フェデレーション認証サービスを使用して展開を保護する方法の詳細については、フェデレーション認証サービス ドキュメントを参照してください。

FIDO2 および WebAuthn 認証

FIDO2 および WebAuthn を使用したローカル認証と仮想認証

ユーザーは、FIDO2セキュリティキーと、TPM 2.0およびWindows Helloを搭載した統合生体認証デバイスを使用して、仮想セッション内でFIDO2またはWebAuthnを活用するアプリケーションに認証できます。

FIDO2の詳細については、「FIDO2: WebAuthn & CTAP」を参照してください。

この機能の使用方法については、「FIDO2 redirection」を参照してください。

> **注**
>
> この機能は、WebAuthn または FIDO2 を使用した仮想セッションへのログオンをサポートしていません。この機能では、仮想セッション内のアプリケーションでこれらの認証方法を使用することのみが可能です。

前提条件と構成

サポート可能性マトリックス

セッションホストのオペレーティングシステム	WEBアプリケーション認証	UWPアプリケーション認証
ウィンドウズ サーバー 2016	USBリダイレクト経由でサポート	サポートされていません
ウィンドウズ サーバー 2019	サポート済み	サポートされていません
ウィンドウズ サーバー 2022	サポート済み	サポート済み
ウィンドウズ サーバー 2025	サポート済み	サポート済み
ウィンドウズ 10	サポート済み	サポート済み
ウィンドウズ 11	サポート済み	サポート済み

> **注:**

> 上記の認証方法のサポートは、基盤となるオペレーティングシステムの機能に依存します。たとえば、OSの制限により、UWPアプリケーションはWindows Server 2019ではサポートされていません。

> 詳細については、以下の要件を確認してください。

Webアプリケーション認証

要件

WebアプリケーションでFIDO2およびWebAuthn認証を使用するための要件は次のとおりです。

CITRIX® コントロールプレーン

- シトリックス バーチャル アプリケーションズ アンド デスクトップ™ 2203 以降

セッションホスト

- オペレーティングシステム
  - Windows 10 22H2以降
  - ウィンドウズ 11
  - Windows Server 2019 以降のバージョン
- VDA
  - Windows: バージョン2203以降

クライアントデバイス

- オペレーティングシステム
  - Windows 10 22H2以降
  - ウィンドウズ 11
  - Linux: Workspace app for Linuxのシステム要件を参照してください。
  - Mac: Workspace app for Macのシステム要件を参照してください。
- Workspace アプリ
  - Windows: バージョン2402以降
  - Linux: 2303以降
  - Mac: 2307以降

WEBブラウザーの要件

- 32ビットおよび64ビットブラウザー

サポートされている認証方法

- FIDO2セキュリティキー
- Windows ハロー
  - TPM 2.0
  - 統合生体認証
    - 顔認証
    - 指紋スキャナー
  - WebAuthn
- パスキー

> **注:**
>
> - 上記の認証方法のサポートは、基盤となるクライアントオペレーティングシステムの機能に依存します。
> - パスキーは、Windows 10クライアントデバイスおよび/またはセッションホストではサポートされていません。

UWPアプリケーション認証

Citrix Virtual Apps and Desktops™ 2112のリリースにより、CitrixはUWPアプリケーションでのWebAuthnおよびFIDO2認証をサポートします。

Microsoft Teams、Microsoft Outlook for Office 365、OneDriveなどのアプリケーションは、Microsoft Entra IDへのリンクとして認証にUWPアプリケーションを使用します。Citrixは現在、これらのアプリケーションを認証するためにFIDO2の使用をサポートしています。

要件

UWPアプリケーションでFIDO2およびWebAuthn認証を使用するための要件は次のとおりです。

CITRIXコントロールプレーン

- シトリックス Virtual Apps and Desktops 2112 以降

セッションホスト

- オペレーティングシステム
  - Windows 10 22H2以降
  - ウィンドウズ 11
  - ウィンドウズ サーバー 2022 以降
- VDA
  - Windows: バージョン2203以降

クライアントデバイス

- オペレーティングシステム
  - Windows 10 22H2以降
  - ウィンドウズ 11
  - Linux: Workspace app for Linuxのシステム要件を参照してください。
  - Mac: Workspace app for Macのシステム要件を参照してください。
- Workspace アプリ
  - Windows: バージョン2402以降
  - Linux: 2303 以降
  - Mac: 2307 以降

UWPアプリケーションの要件

- 32ビットおよび64ビットアプリケーション

サポートされる認証方法

- FIDO2セキュリティキー
- Windows ハロー
  - TPM 2.0
  - 統合された生体認証
    - 顔認識
    - 指紋スキャナー
  - WebAuthn

- パスキー

> **注:**
>
> 上記の認証方法のサポートは、基盤となるオペレーティングシステムの機能に依存します。

> FIDO2リダイレクトが利用できないシナリオ（クライアント、VDA、またはオペレーティングシステムでこの機能がサポートされていないため）では、USBベースのFIDO2キーをUSBリダイレクトを使用してリダイレクトできます。 FIDO2リダイレクトが利用可能なシナリオでも、USBリダイレクトを使用してUSBベースのFIDO2キーをリダイレクトすることが可能です。この場合、FIDO2リダイレクトを無効にし、適切なUSBリダイレクトルールを構成する必要があります。 USBリダイレクトルールを使用してFIDO2キーを構成する方法の詳細については、USBリダイレクトデバイスルールのドキュメントを参照してください。

構成

FIDO2リダイレクトはデフォルトで有効になっています。Chrome、Edge、Brave、およびFirefoxブラウザで実行されているアプリケーションへの認証に追加の構成は必要ありません。関連するポリシー設定については、FIDO2リダイレクト設定を参照してください。

FIDO2認証を必要とするその他のアプリケーションを使用している企業の場合、レジストリに追加の構成が必要です。詳細については、高度な構成を参照してください。

> **注:**
>
> 中間ホップVDAにインストールされているWindows用Citrix Workspaceアプリがバージョン2503以降である限り、FIDO2リダイレクトはダブルホップシナリオでサポートされます。さらに、これは2番目のホップ接続がICA経由の場合にのみサポートされます。

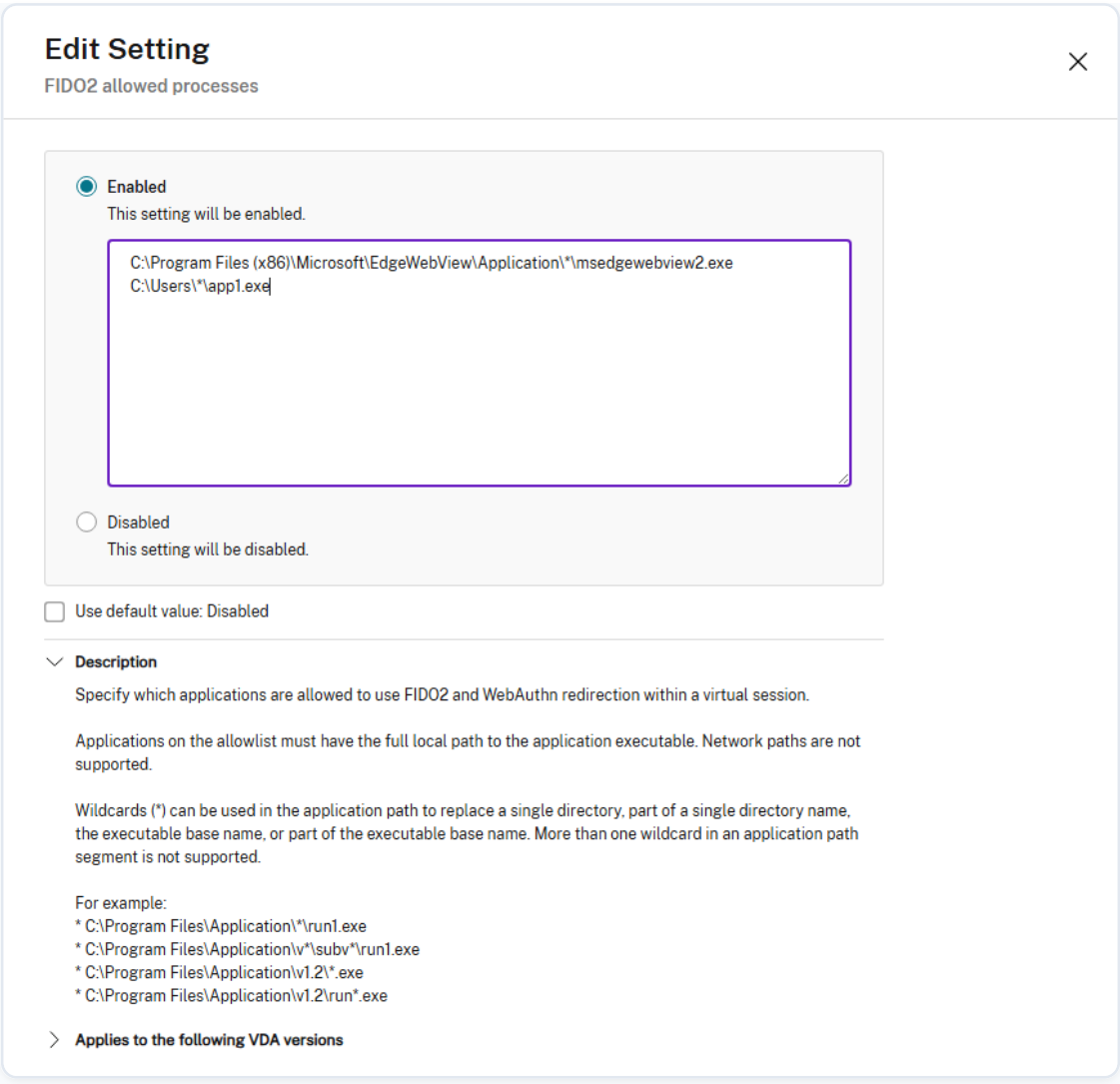
カスタムアプリケーションの高度な構成

その他のWebアプリケーション (Chrome、Edge、Firefox、Braveを除く) を使用している企業の場合、HDXセッション内でFIDO2リダイレクトを機能させるには、以下の変更を行う必要があります。

1. Studioで**FIDO2許可プロセス**ポリシー設定を構成します。

- テキストフィールドにアプリケーションのフルパスを追加します。ポリシー設定の使用方法に関する追加の詳細は、ポリシーセクションで確認できます。

> **注:**
>
> ワイルドカード (*) の使用がサポートされています。アプリケーションのバージョンに基づいてディレクトリ名や実行可能ファイル名が変更される場合、またはアプリケーションがユーザープロファイルにインストールされている場合にワイルドカードを使用できます。



2. 以下のレジストリキーと値を追加します。

   a. 64ビットアプリケーションの場合 (例: "app1.exe"):

   - キー:

     `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook\app1.exe`

b. 32ビットアプリケーションの場合:

- キー:
  `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHo`

3. app1.exeでFIDO2リダイレクトを有効にするためにレジストリ値を設定した後、VDAを再起動します。

注:

- `msedgewebview2.exe`はStudioポリシー設定でのみ構成する必要があります。ステップ2と3は`msedgewebview2.exe`には必要ありません。
- レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrixは、.
- レジストリエディターの誤った使用によって生じる問題が解決されることを保証できません。
- レジストリエディターの使用は自己責任で行ってください。編集する前に必ずレジストリをバックアップしてください。
- ステップ2で構成されたレジストリキーは、VDAのアップグレード後も保持されます。

トラブルシューティング

FIDO2リダイレクトの問題をトラブルシューティングするには、次の手順に従ってください。

1. **システム要件を確認する**

   a. 公式のCitrixドキュメントに基づき、FIDO2リダイレクトのシステム要件が満たされていることを確認します。

2. **デバイス接続を確認する**

   a. 物理FIDO2キーの場合：

      i. FIDO2キーが正しく挿入され、クライアントエンドポイントで認識されていることを確認します。

      ii. オペレーティングシステムのデバイスマネージャー（例：Windowsのデバイスマネージャー、macOSのシステム情報）を使用して、デバイスが認識され機能していることを確認します。

iii. デバイスが検出されない場合：

i. キーを挿し直すか、別のUSBポートを使用してみてください。

ii. ハードウェアの問題を除外するために、別のデバイスでキーをテストします。

b. 組み込み認証機能（例：Windows Helloなど）の場合 -

i. クライアントデバイスで機能が有効になり、構成されていることを確認します。

c. クライアントデバイスがFIDO2キーを認識しない場合、CitrixはそれをHDXセッションにリダイレクトできないため、これは重要です。

3. **Citrixポリシー設定と構成を確認する**

a. CitrixポリシーでFIDO2/WebAuthnリダイレクトおよびUSBリダイレクトの設定を確認します。

i. FIDO2リダイレクトポリシーが有効になっています。

ii. EdgeWebView2またはカスタムデスクトップアプリケーションが使用されている場合、適切なファイルパスが**FIDO2 allowed processes**ポリシー設定に追加されます。

iii. FIDO2キーが汎用USBリダイレクトを使用してデバイスをリダイレクトするためのデバイスルールは**設定されていません**。

b. Citrixコンポーネントが最近更新された場合は、構成が新しいバージョンと一致していることを確認してください。

4. **診断にHDX Monitorを使用する**

a. HDXセッションを起動し、WebブラウザまたはUWPアプリケーションを開いて認証ページに移動します。

b. サインイン方法としてセキュリティキー、Webauthn、またはFIDO2を選択します。FIDO2呼び出しがリダイレクトされた結果、wfica32.exeプロセスからのダイアログプロンプトが表示されるはずです（添付のスクリーンショットを参照）。そうでない場合：

i. キーが汎用USB仮想チャネルを使用してリダイレクトされていないことを確認してください。キーがHDXセッション内でリダイレクトされている場合、「セキュリティキーをUSBポートに挿入してください」というダイアログプロンプトが表示される可能性があります。これを解決するには、USBリダイレクトを無効にするか、セキュリティキーがHDXセッション内でリダイレクトされないようにしてください。

ii. HDXセッションでHDX Monitorを開き、**FIDO2 - Webauthn Redirection**ノードに移動します。

iii. FIDO2リダイレクト許可ポリシーが**True**に設定されており、FIDO2/WebAuthn認証を必要とするアプリケーションが**FIDO2 Redirection Hooked Applications**にリストされていることを確認してください。アプリケーションが存在しない場合は、高度な構成の情報に基づいて適切なレジストリの場所にそれを追加してください。

iv. FIDO2/WebAuthn認証を必要とするアプリケーションのフルパスが**FIDO2 allowed processes**ポリシー設定にリストされていることを確認してください。フルパスが存在しない場合は、Studioの**FIDO2 allowed processes**ポリシー設定に追加してください。詳細については、構成セクションを参照してください。

v. (レガシー) FIDO2リダイレクトがレガシーレジストリベースの設定を使用して構成されている場合は、構成をStudioの**FIDO2 allowed processes**ポリシー設定に移行し、FIDO2/WebAuthn認証を必要とするアプリケーションのフルパスが含まれていることを確認してください。詳細については、構成セクションを参照してください。

> **注:**
>
> セッションホストにHDX Monitorがまだインストールされていない場合は、Citrix Virtual Apps and Desktopsインストーラーの**Support**フォルダーからインストールできます。

1. **ログを収集し、テクニカルサポートに連絡する**

   a. 上記の手順を実行しても問題が解決しない場合 -

      i. HDX Monitorの出力、Citrix Workspaceアプリ、VDA CDFログを収集します。

      ii. 実行したすべてのトラブルシューティング手順と発生したエラーメッセージを文書化します。

      iii. ITサポートチームまたはCitrixサポートに連絡し、収集した情報を提供して迅速な解決を図ります。

一般的な問題と解決策

1. **Microsoft Edgeブラウザを使用して開いたWebページでFIDO2認証が機能しない場合があります**

   a. **考えられる原因**: AppContainerを持つEdgeのサンドボックス化されたインスタンスでは、Citrixがプロセスにフックできないため、WebAuthn呼び出しのリダイレクトが機能しません。

b. **解決策**: これは、グループポリシーエディターまたはIntuneで適切な設定を更新することで対処できます。この詳細については、こちらを参照してください。または、**DynamicCodeSettings**レジストリ値を0に設定することでも問題の解決に役立ちます。

- **キー**: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge\`
- **値の名前**: `DynamicCodeSettings`
- **値の型**: `DWORD`
- **値のデータ**: 0

2. **WebブラウザでFIDO2（例: Yubikey）のリダイレクトが機能しない**

a. **考えられる原因**: ブラウザに関連するFSLogixプロファイル管理のAppMaskingルールにより、Citrix FIDO2サービスがブラウザがインストールされているファイルパスを表示および検証できない可能性があります。

b. **解決策**: Citrix FIDO2サービスからChromeのファイルパスを非表示にするFSLogixの関連する非表示ルールを無効にすると、Yubikeyが正常にリダイレクトされ、ブラウザに表示されるようになります。

シトリックス Virtual Apps and Desktops™ と シトリックス ゲートウェイ の統合

StoreFront™ サーバーは、公開されたリソースとデータへのアクセスを管理するために展開および構成されます。リモートアクセスの場合、StoreFront の前に Citrix Gateway を追加することをお勧めします。

> **注:**

> Citrix Virtual Apps and Desktops と Citrix Gateway を統合する方法の詳細な構成手順については、StoreFront のドキュメントを参照してください。

> 次の図は、Citrix Gateway を含む簡素化された Citrix 展開の例を示しています。Citrix Gateway は StoreFront と通信し、Citrix Virtual Apps and Desktops™ によって提供されるアプリとデータを保護します。ユーザーデバイスは Citrix Workspace™ アプリを実行して、安全な接続を作成し、アプリ、デスクトップ、ファイルにアクセスします。

Citrix Gateway を含む簡素化された Citrix 展開(/en-us/citrix-virtual-apps-desktops/current-release/media/sample-deployment-overview.png)

ユーザーは Citrix Gateway を使用してログオンし、認証します。Citrix Gateway は DMZ に展開され、保護されています。2 要素認証が構成されています。ユーザー資格情報に基づいて、ユーザーには関連するリソースとアプリケーションが提供されます。アプリケーションとデータは適切なサーバー上にあります（図には示されていません）。セキュリティ上機密性の高いアプリケーションとデータには、個別のサーバーが使用されます。

セキュリティに関する考慮事項とベストプラクティス

> **注:**
>
> 組織は、規制要件を満たすために特定のセキュリティ標準に準拠する必要がある場合があります。このようなセキュリティ標準は時間とともに変化するため、このドキュメントではこの主題については扱いません。セキュリティ標準とCitrix製品に関する最新情報については、Citrix Trust Centerを参照してください。

ファイアウォール

環境内のすべてのマシンを、必要に応じてエンクレーブ境界を含め、境界ファイアウォールで保護します。

環境内のすべてのマシンは、パーソナルファイアウォールによって保護されている必要があります。コアコンポーネントとVDAをインストールする際、Windowsファイアウォールサービスが検出された場合（ファイアウォールが有効になっていない場合でも）、コンポーネントと機能の通信に必要なポートを自動的に開くように選択できます。これらのファイアウォールポートを手動で構成することもできます。別のファイアウォールを使用する場合は、手動で構成する必要があります。必要なポートの詳細については、Tech Paper: Citrixテクノロジーで使用される通信ポートを参照してください。

従来の環境をこのリリースに移行する場合、既存の境界ファイアウォールの再配置や新しい境界ファイアウォールの追加が必要になる場合があります。たとえば、データセンター内の従来のクライアントとデータベースサーバーの間に境界ファイアウォールがあるとします。このリリースを使用する場合、その境界ファイアウォールは、仮想デスクトップとユーザーデバイスが一方にあり、データセンター内のデータベースサーバーとDelivery Controllerがもう一方にあるように配置する必要があります。したがって、データベースサーバーとControllerを格納するために、データセンター内にエンクレーブを作成することを検討してください。また、ユーザーデバイスと仮想デスクトップの間に保護を設けることも検討してください。

> **注:**
>
> TCPポート1494と2598はICAとCGPに使用されるため、データセンター外のユーザーがアクセスできるようにファイアウォールで開かれている可能性が高いです。Citrixは、管理インターフェイスが意図せず攻撃にさらされる可能性を避けるため、これらのポートを他の目的で使用しないことを推奨します。ポート1494と2598は、Internet Assigned Number Authority (http://www.iana.org/) に正式に登録されています。

Delivery Controller™とのセキュアな通信

HTTPSを使用した通信の暗号化

StoreFrontとNetScaler Gatewayは、HTTPまたはHTTPSを介してDelivery Controllerで実行されているXMLサービスと通信します。構成によっては、VDAはWebSocketを使用してDelivery Controllerと通信する場合があります。Directorは、HTTPまたはHTTPSを介してODataを使用して監視データと通信します。HTTPSを有効にし、HTTPを無効にすることをお勧めします。これには、(/ja-jp/citrix-virtual-apps-desktops/current-release/secure/tls-ddc.html)が必要です。

- StoreFrontをHTTPSを使用して接続するように構成するには、(/ja-jp/storefront/current-release/configure-manage-stores/manage-controllers#add-resource-feeds-for-citrix-virtual-apps-and-desktops)および(/ja-jp/storefront/current-release/integrate-with-citrix-gateway-and-citrix-adc/configure-citrix-gateway#add-citrix-gateway-appliance)を参照してください。
- NetScaler GatewayをHTTPSを使用してDelivery Controllerに接続するように構成するには、NetScaler GatewayでのSecure Ticket Authorityの構成を参照してください。

セキュリティキー

承認されたStoreFrontサーバーとNetScalerサーバーのみがクラウドコネクタを介してDaaSに接続できるように、(/ja-jp/citrix-virtual-apps-desktops/current-release/manage-deployment/security-keys.html)を使用できます。これは、XML信頼を有効にしている場合に特に重要です。

XML信頼

デフォルトでは、StoreFrontが列挙や起動などのアクションのためにDelivery Controllerに接続する場合、DaaSがユーザーを認証し、ユーザーのグループメンバーシップを確認できるように、StoreFrontはユーザーのActive Directory資格情報を渡す必要があります。ただし、ドメインパススルー、スマートカード、SAMLなどの他の認証方法を使用する場合、StoreFrontはActive Directoryパスワードを持っていません。この場合、「XML信頼」を有効にする必要があります。XML信頼が有効になっている場合、Citrix Virtual Apps and Desktopsは、ユーザーのパスワードを検証する

ことなく、アプリケーションの列挙や起動など、ユーザーに代わってStoreFrontがアクションを実行することを許可します。XML信頼を有効にする前に、信頼できるStoreFrontサーバーのみがDelivery Controllerに接続できるように、(/ja-jp/citrix-virtual-apps-desktops/current-release/manage-deployment/security-keys.html)またはファイアウォールやIPsecなどの別のメカニズムを使用してください。

XML信頼設定を確認、有効化、または無効化するには、Citrix Virtual Apps and Desktops PowerShell SDKを使用します。

- XML信頼設定の現在の値を確認するには、`Get-BrokerSite`を実行し、`TrustRequestsSentToTheXMLServicePort`の値を調べます。
- XML信頼を有効または無効にするには、パラメーター`TrustRequestsSentToTheXmlServicePort`を指定して`Set-BrokerSite`を実行します。

VDAとDelivery Controller間の通信

VDAがコントローラーと通信するためのメカニズムは2つあります。

- ウィンドウズ コミュニケーション ファンデーション

  Windows Communication Foundation (WCF) のメッセージレベル保護により、Delivery ControllerとVDA間の通信が保護されます。これにより、TLSを使用した追加のトランスポートレベル保護の必要がなくなります。VDAとDelivery Controller間の通信に使用されるデフォルトポートは80です。ただし、ポートはカスタマイズできます。詳細については、「VDAのカスタマイズ」を参照してください。

  WCFでのメッセージセキュリティの詳細については、Microsoftドキュメント「WCFでのメッセージセキュリティ」を参照してください。

  WCF構成では、ControllerとVDA間の相互認証にKerberosを使用します。暗号化には256ビットキーのCBCモードでAESを使用します。メッセージの整合性にはSHA-1を使用します。

  Microsoftによると、WCFで使用されるセキュリティプロトコルは、WS-SecurityPolicy 1.2を含むOASIS（Organization for the Advancement of Structured Information Standards）の標準に準拠しています。また、Microsoftは、WCFがSecurity Policy 1.2に記載されているすべてのアルゴリズムスイートをサポートしていると述べています。

  ControllerとVDA間の通信には、前述のアルゴリズムであるbasic256アルゴリズムスイートを使用します。

  WCF構成では、メッセージレベルのセキュリティ暗号化とともに、SOAP over HTTPプロトコルを使用します。

- WebSockets

  これはWCFの現代的な代替手段です。VDAからDelivery Controllerへの通信にTLSポート443のみを使用するという利点があります。現在、MCSプロビジョニングされたマシンでのみ利用可能です。詳細については、「VDAとDelivery Controller間のWebSocket通信」を参照してください。

Delivery ControllerとLicense Server間のセキュアな通信

Delivery ControllerはHTTPS経由でLicense Serverと通信します。デフォルトでは自己署名証明書を使用しますが、これをエンタープライズまたはパブリック認証局が発行した証明書に置き換えることをお勧めします。詳細については、「Citrix Licensing ManagerおよびWeb Services for Licensingで使用される証明書を手動でインストールする」を参照してください。

WebブラウザとWeb StudioおよびDirector間の通信を保護する

Web StudioとDirectorは、Delivery Controllerと同じマシンまたは別のマシンにインストールできます。ユーザーはWebブラウザを使用してWeb StudioとDirectorに接続します。デフォルトでは、Web Studioは自己署名証明書を使用してHTTPSを有効にしますが、スタンドアロンでインストールされたDirectorはHTTPSを構成しません。適切な証明書を使用して、Web StudioおよびDirectorでTLSを有効にすることをお勧めします。

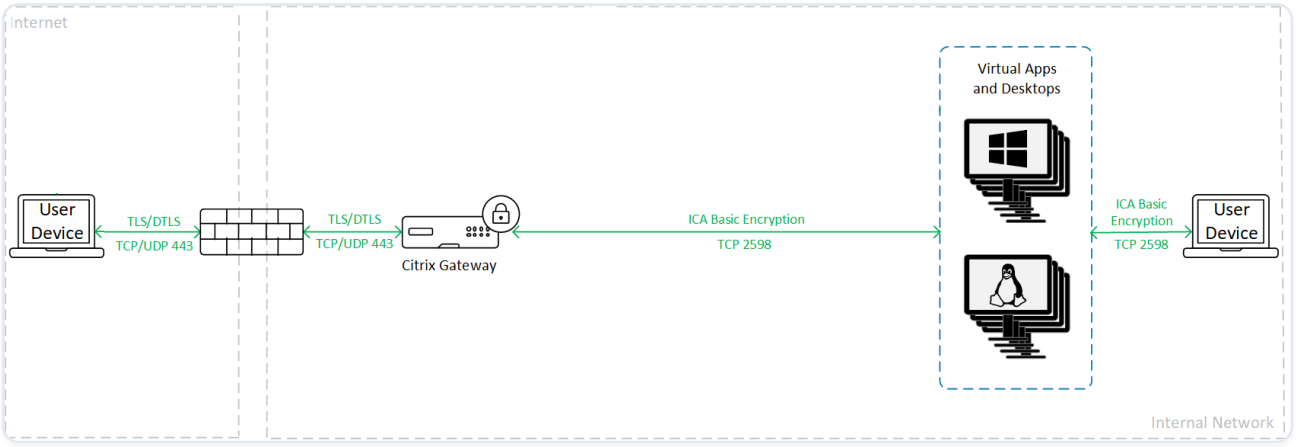
ICA®通信の保護

Citrix Virtual Apps and Desktops™は、クライアントとVDA間のICAトラフィックを保護するためのいくつかのオプションを提供します。利用可能なオプションは次のとおりです。

- **基本暗号化:** デフォルト設定です。
- **SecureICA:** RC5 (128ビット) 暗号化を使用してセッションデータを暗号化できます。
- **VDA TLS/DTLS:** TLS/DTLSを使用したネットワークレベルの暗号化を可能にします。

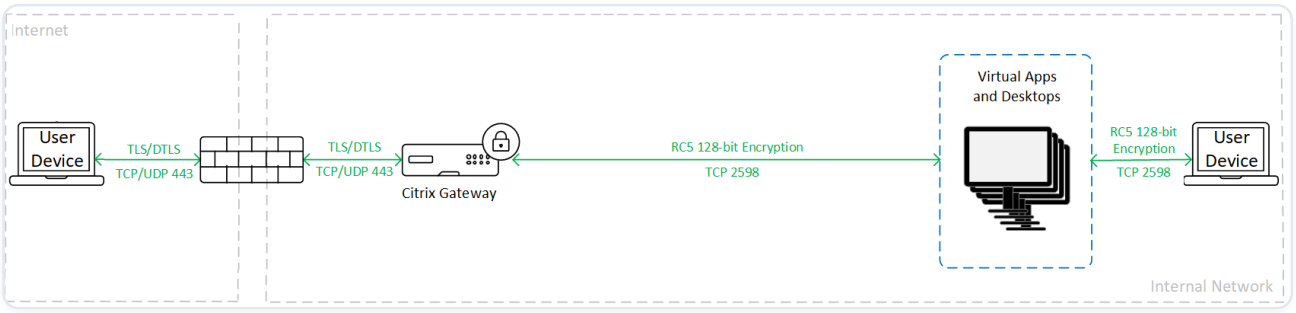
基本暗号化

基本暗号化を使用する場合、トラフィックは次の図に示すように暗号化されます。



SecureICA

SecureICAを使用する場合、トラフィックは次の図に示すように暗号化されます。



詳細については、セキュリティポリシー設定を参照してください。

> **注1：**
>
> SecureICAは、Workspace app for HTML5ではサポートされていません。

> **注2：**
>
> Citrix SecureICAはICA/HDXプロトコルの一部ですが、Transport Layer Security (TLS) のような標準準拠のネットワークセキュリティプロトコルではありません。

VDA TLS/DTLS

VDA TLS/DTLS暗号化を使用する場合、トラフィックは次の図に示すように暗号化されます。

TLS/DTLS使用時のトラフィック暗号化(/en-us/citrix-virtual-apps-desktops/current-release/media/vda-tls.png)

VDA TLS/DTLSを構成するには、VDAのTLS設定を参照してください。

仮想チャネル

環境で許可されるCitrix以外の仮想チャネルを制御するには、仮想チャネル許可リストを使用します。

印刷サーバーとの安全な通信

Virtual Delivery Agent (VDA) とユニバーサルプリントサーバー間のTCPベースの接続にTLSを有効にできます。詳細については、「Universal Print ServerでのTransport Layer Security (TLS)」を参照してください。

サイトデータベースとの安全な通信

サイトデータベースへのTLSを有効にする方法については、「CTX137556」を参照してください。

VDAマシンのセキュリティ

一般的な推奨事項

VDAが最新のオペレーティングセキュリティ更新プログラムとウイルス対策ソフトウェアで常に最新の状態に保たれていることを確認してください。

アプリケーションセキュリティ

管理者以外のユーザーが悪意のある操作を実行するのを防ぐため、Citrix®は、VDAホスト上のインストーラー、アプリケーション、実行可能ファイル、およびスクリプトに対してWindows AppLockerルールを構成することを推奨します。

8.3形式のファイル名

VDAで8.3形式のファイル名を無効にできます。「Microsoft fsutil documentation」を参照してください。

データストレージに関する考慮事項

デスクトップ環境は、プールされたデスクトップや専用デスクトップなど、さまざまな種類のデスクトップで構成されている場合があります。ユーザーは、プールされたデスクトップなど、ユーザー間で共有されるデスクトップにデータを保存してはなりません。ユーザーが専用デスクトップにデータを保存した場合、そのデスクトップが後で他のユーザーに利用可能になった場合は、そのデータを削除する必要があります。

ユーザーアカウント管理

アカウント管理にはWindowsのベストプラクティスを適用してください。Machine Creation ServicesまたはProvisioning Servicesによって複製される前に、テンプレートまたはイメージ上にアカウントを作成しないでください。保存された特権ドメインアカウントを使用してタスクをスケジュールしないでください。共有Active Directoryマシンアカウントを手動で作成しないでください。これらの慣行は、マシン攻撃がローカルの永続的なアカウントパスワードを取得し、それらを使用して他のユーザーに属するMCS/PVS共有イメージにログオンするのを防ぐのに役立ちます。

ユーザーには必要な機能のみを付与します。Microsoft Windowsの特権は、通常の方法でデスクトップに適用され続けます。特権はユーザー権利の割り当てを通じて、グループメンバーシップはグループポリシーを通じて構成します。このリリースの利点の1つは、デスクトップが保存されているコンピューターに対する物理的な制御を付与することなく、ユーザーにデスクトップへの管理者権限を付与できることです。

デスクトップの特権を計画する際は、以下に注意してください。

- デフォルトでは、非特権ユーザーがデスクトップに接続すると、自身のユーザーデバイスのタイムゾーンではなく、デスクトップを実行しているシステムのタイムゾーンが表示されます。ユーザーがデスクトップを使用する際にローカルタイムを表示できるようにする方法については、「デリバリーグループの管理」の記事を参照してください。
- デスクトップの管理者であるユーザーは、そのデスクトップを完全に制御できます。デスクトップが専用デスクトップではなくプールされたデスクトップである場合、そのユーザーは、将来のユーザーを含む、そのデスクトップの他のすべてのユーザーに関して信頼できる必要があります。デスクトップのすべてのユーザーは、この状況によってデータセキュリティに潜在的に永続的なリスクがあることを認識する必要があります。この考慮事項は、単一ユーザーのみが使用する専用デスクトップには適用されません。そのユーザーは、他のどのデスクトップの管理者であってもなりません。
- デスクトップの管理者であるユーザーは、一般的に、悪意のあるソフトウェアを含むソフトウェアをそのデスクトップにインストールできます。また、そのユーザーは、デスクトップに接続されているネットワーク上のトラフィックを監視または制御できる可能性もあります。

ログオン権限の管理

ログオン権限は、ユーザーアカウントとコンピューターアカウントの両方に必要です。Microsoft Windowsの特権と同様に、ログオン権限は通常の方法でデスクトップに適用され続けます。ログオン権限はユーザー権利の割り当てを通じて、グループメンバーシップはグループポリシーを通じて構成します。

Windowsのログオン権限は、ローカルログオン、リモートデスクトップサービス経由のログオン、ネットワーク経由のログオン（ネットワークからこのコンピューターにアクセス）、バッチジョブとしてログオン、サービスとしてログオンです。

コンピューターアカウントの場合、コンピューターには必要なログオン権限のみを付与します。「ネットワークからこのコンピューターにアクセス」のログオン権限は、デリバリーコントローラーのコンピューターアカウントに必要です。

ユーザーアカウントの場合、ユーザーには必要なログオン権限のみを付与します。

Microsoftによると、デフォルトでは、Remote Desktop Usersグループには「リモートデスクトップサービス経由でのログオンを許可」のログオン権限が付与されています（ドメインコントローラーを除く）。

組織のセキュリティポリシーによっては、このグループをそのログオン権限から削除するよう明示的に規定している場合があります。次のアプローチを検討してください。

- マルチセッションOS用Virtual Delivery Agent (VDA) は、Microsoft Remote Desktop Servicesを使用します。Remote Desktop Usersグループを制限付きグループとして構成し、Active Directoryグループポリシーを介してグループのメンバーシップを制御できます。詳細については、Microsoftのドキュメントを参照してください。
- シングルセッションOS用VDAを含むCitrix Virtual Apps and Desktops™のその他のコンポーネントでは、Remote Desktop Usersグループは不要です。したがって、これらのコンポーネントの場合、Remote Desktop Usersグループには「リモートデスクトップサービスによるログオンを許可」のログオン権限は不要であり、削除できます。さらに：
    - リモートデスクトップサービスを介してそれらのコンピューターを管理する場合、そのようなすべての管理者がすでにAdministratorsグループのメンバーであることを確認してください。
    - それらのコンピューターをリモートデスクトップサービス経由で管理しない場合は、それらのコンピューターでリモートデスクトップサービス自体を無効にすることを検討してください。

ログイン権限「リモートデスクトップサービス経由でのログオンを拒否」にユーザーとグループを追加することは可能ですが、ログオン拒否権限の使用は一般的に推奨されません。詳細については、Microsoftのドキュメントを参照してください。

Delivery Controllerのセキュリティ

Delivery Controller上のWindowsサービス

Delivery Controllerのインストールにより、以下のWindowsサービスが作成されます。

- Citrix AD Identity Service (NT SERVICE\CitrixADIdentityService): VMのMicrosoft Active Directoryコンピューターアカウントを管理します。
- Citrix Analytics (NT SERVICE\CitrixAnalytics): サイト管理者が承認した場合、Citrixが使用するためのサイト構成の使用状況情報を収集します。その後、この情報をCitrixに送信し、製品の改善に役立てます。
- Citrix App Library (NT SERVICE\CitrixAppLibrary): AppDiskの管理とプロビジョニング、AppDNA統合、およびApp-Vの管理をサポートします。
- Citrix Broker Service (NT SERVICE\CitrixBrokerService): ユーザーが利用できる仮想デスクトップまたはアプリケーションを選択します。
- Citrix Configuration Logging Service (NT SERVICE\CitrixConfigurationLogging): 管理者がサイトに対して行ったすべての構成変更およびその他の状態変更を記録します。
- Citrix Configuration Service (NT SERVICE\CitrixConfigurationService): 共有構成のためのサイト全体のリポジトリ。
- Citrix Delegated Administration Service (NT SERVICE\CitrixDelegatedAdmin): 管理者に付与された権限を管理します。
- Citrix Environment Test Service (NT SERVICE\CitrixEnvTest): 他のDelivery Controllerサービスのセルフテストを管理します。
- Citrix Host Service (NT SERVICE\CitrixHostService): Citrix Virtual AppsまたはCitrix Virtual Desktops展開で使用されるハイパーバイザーインフラストラクチャに関する情報を保存し、コンソールがハイパーバイザープール内のリソースを列挙するために使用する機能も提供します。
- Citrix Machine Creation Services (NT SERVICE\CitrixMachineCreationService): デスクトップVMの作成をオーケストレーションします。
- Citrix Monitor Service (NT SERVICE\CitrixMonitor): Citrix Virtual AppsまたはCitrix Virtual Desktopsのメトリックを収集し、履歴情報を保存し、トラブルシューティングおよびレポートツール用のクエリインターフェイスを提供します。
- Citrix StoreFront Service (NT SERVICE\ CitrixStorefront): StoreFrontの管理をサポートします。（StoreFrontコンポーネント自体の一部ではありません。）
- Citrix StoreFront Privileged Administration Service (NT SERVICE\CitrixPrivilegedService): StoreFrontの特権管理操作をサポートします。（StoreFrontコンポーネント自体の一部ではありません。）

- Citrix Config Synchronizer Service (NT SERVICE\CitrixConfigSyncService): メインサイトデータベースからローカルホストキャッシュに構成データを伝播します。
- Citrix High Availability Service (NT SERVICE\CitrixHighAvailabilityService): メインサイトデータベースが利用できない場合に、ユーザーが利用できる仮想デスクトップまたはアプリケーションを選択します。

Delivery Controllerのインストールでは、以下のWindowsサービスも作成されます。これらは、他のCitrixコンポーネントと一緒にインストールされた場合にも作成されます。

- Citrix Diagnostic Facility COM Server (NT SERVICE\CdfSvc): Citrixサポートが使用するための診断情報の収集をサポートします。
- Citrix Telemetry Service (NT SERVICE\CitrixTelemetryService): Citrixによる分析のために診断情報を収集し、管理者が分析結果と推奨事項を表示してサイトの問題の診断に役立てられるようにします。

Delivery Controllerのインストールでは、以下のWindowsサービスも作成されます。これは現在使用されていません。有効になっている場合は、無効にしてください。

- Citrix リモート ブローカー プロバイダー (NT SERVICE\XaXdCloudProxy)

Delivery Controllerのインストールでは、以下のWindowsサービスも作成されます。これらは現在使用されていませんが、有効にする必要があります。無効にしないでください。

- Citrix オーケストレーション サービス (NT SERVICE\CitrixOrchestration)
- Citrix トラスト サービス (NT SERVICE\CitrixTrust)

Citrix StoreFront™ Privileged Administration Serviceを除き、これらのサービスには「サービスとしてログオン」のログオン権限と、「プロセスのメモリクォータの調整」、「セキュリティ監査の生成」、「プロセスレベルトークンの置き換え」の特権が付与されます。これらのユーザー権限を変更する必要はありません。これらの特権はDelivery Controllerでは使用されず、自動的に無効になります。

Citrix StoreFront Privileged AdministrationサービスとCitrix Telemetry Serviceを除き、前述のDelivery Controller WindowsサービスはNETWORK SERVICE IDとしてログオンするように構成されています。これらのサービス設定を変更しないでください。

Citrix Config Synchronizer Service は、Delivery Controller 上のローカル管理者グループに NETWORK SERVICE アカウントが属している必要があります。これにより、ローカルホストキャッシュが正しく機能します。

Citrix StoreFront Privileged Administration サービスは、ローカルシステム (NT AUTHORITY\SYSTEM) としてログオンするように構成されています。これは、通常サービスでは利用できない Delivery Controller StoreFront の操作 (Microsoft IIS サイトの作成を含む) に必要です。サービス設定を変更しないでください。

Citrix Telemetry Service は、サービス固有の ID としてログオンするように構成されています。

Citrix Telemetry Service は無効にできます。このサービスと、すでに無効になっているサービスを除き、これらの Delivery Controller Windows サービスの他のサービスを無効にしないでください。

ログオン権限の管理

VDA のコンピューターアカウントには、「ネットワークからこのコンピューターにアクセス」というログオン権限が必要です。(/ja-jp/advanced-concepts/implementation-guides/ad-ou-controller-discovery.html)「Active Directory OU ベースのコントローラー検出」を参照してください。

クライアントアクセス

クライアントアクセスは通常、(/ja-jp/storefront)Citrix StoreFront を展開することで提供されます。StoreFront のセキュリティ保護の詳細については、(/ja-jp/storefront/current-release/install-standard/secure)StoreFront のドキュメントを参照してください。

リモートユーザーが StoreFront および VDA に安全に接続できるようにするには、NetScaler® Gateway を展開します。

Citrix は、クライアントが Citrix Workspace アプリを使用して StoreFront に接続することを推奨しています。詳細については、各オペレーティングシステム用の Citrix Workspace アプリの(/ja-jp/citrix-workspace-app.html)ドキュメントのセキュリティセクションを参照してください。または、ユーザーは Web ブラウザーを使用して StoreFront にアクセスすることもできます。

ユーザーが Citrix Workspace™ アプリ以外のアプリケーションを実行する能力が限られているシンクライアントをユーザーに提供することを検討してください。デバイスが組織によって管理されている場合は、オペレーティングシステムのセキュリティ更新プログラムとウイルス対策ソフトウェアの展開を確実にするためのポリシーを導入する必要があります。ただし、多くの場合、ユーザーは組織の管理外にある管理されていないデバイスから接続できる必要があります。次の機能の使用を検討してください。

- Endpoint Analysis を使用して、オペレーティングシステムやウイルス対策などのセキュリティ情報についてエンドポイントをスキャンし、セキュリティ要件を満たさないクライアントへのアクセスを拒否します。

- (/ja-jp/citrix-workspace-app/app-protection.html)App Protection は、キーロガーと画面キャプチャをブロックします。

混在バージョン環境

VDA が Delivery Controller と異なるバージョンである場合など、混在バージョン環境は一部のアップグレード中に避けられません。ベストプラクティスに従い、異なるバージョンの Citrix コンポーネントが共存する時間を最小限に抑えてください。混在バージョン環境では、たとえばセキュリティポリシーが一律に適用されない場合があります。

> **注:**
>
> これは他のソフトウェア製品にも共通しています。以前のバージョンの Active Directory を使用すると、後のバージョンの Windows ではグループポリシーが部分的にしか適用されません。

以下のシナリオでは、特定の混在バージョンCitrix環境で発生する可能性のあるセキュリティ問題について説明します。Citrix Receiver 1.7を使用してXenAppおよびXenDesktop 7.6 Feature Pack 2のVDAを実行している仮想デスクトップに接続すると、サイトでポリシー設定 が有効になりますが、XenAppおよびXenDesktop 7.1を実行しているDelivery Controllerでは無効にできません。これは、製品の後のバージョンでリリースされたポリシー設定を認識しないためです。このポリシー設定により、ユーザーはファイルを仮想デスクトップにアップロードおよびダウンロードできるようになり、これがセキュリティ問題となります。この問題を回避するには、Delivery Controller（またはStudioのスタンドアロンインスタンス）をバージョン7.6 Feature Pack 2にアップグレードし、グループポリシーを使用してポリシー設定を無効にします。または、影響を受けるすべての仮想デスクトップでローカルポリシーを使用します。

Remote PC Accessのセキュリティに関する考慮事項

Remote PC Accessは、次のセキュリティ機能を実装しています。

- スマートカードの使用がサポートされています。
- リモートセッションが接続されると、オフィスPCのモニターは空白で表示されます。
- Remote PC Accessは、CTRL+ALT+DEL、USB対応スマートカード、生体認証デバイスを除くすべてのキーボードおよびマウス入力をリモートセッションにリダイレクトします。
- SmoothRoamingは、単一ユーザーのみがサポートされます。

- ユーザーがオフィスPCにリモートセッションを接続している場合、そのユーザーのみがオフィスPCへのローカルアクセスを再開できます。ローカルアクセスを再開するには、ユーザーはローカルPCでCtrl-Alt-Delを押し、リモートセッションで使用したのと同じ資格情報でログオンします。システムに適切なサードパーティの資格情報プロバイダー統合がある場合、ユーザーはスマートカードを挿入するか、生体認証を利用してローカルアクセスを再開することもできます。このデフォルトの動作は、グループポリシーオブジェクト（GPO）を介して高速ユーザー切り替えを有効にするか、レジストリを編集することで上書きできます。

> **注:**

> Citrixでは、VDA管理者権限を一般セッションユーザーに割り当てないことをお勧めします。

自動割り当て

デフォルトでは、Remote PC Accessは複数のユーザーのVDAへの自動割り当てをサポートしています。XenDesktop 5.6 Feature Pack 1では、管理者はRemotePCAccess.ps1 PowerShellスクリプトを使用してこの動作を上書きできます。このリリースでは、複数の自動リモートPC割り当てを許可または禁止するためにレジストリエントリを使用します。この設定はサイト全体に適用されます。

> **注意:**

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

> 自動割り当てを単一ユーザーに制限するには：

サイト内の各Controllerで、次のレジストリエントリを設定します。

```
HKEY_LOCAL_MACHINE\Software\Citrix|DesktopServer

Name: AllowMultipleRemotePCAssignments

Type: REG_DWORD
```

```
Data: 0 = Disable multiple user assignment, 1 = (Default) Enable multiple
user assignment.
```

既存のユーザー割り当てがある場合は、SDKコマンドを使用してそれらを削除し、VDAが単一の自動割り当ての対象となるようにします。

- VDAから割り当てられているすべてのユーザーを削除します: `$machine.AssociatedUserNames | %{ Remove-BrokerUser-Name $_ -Machine $machine`
- デリバリーグループからVDAを削除します: `$machine | Remove-BrokerMachine -DesktopGroup $desktopGroup`

物理的なオフィスPCを再起動します。

証明書を管理する

TLS は、2 つの当事者間の信頼を確立するために証明書を使用します。サービスを提供する各サーバーに適切な証明書をインストールし、そのサーバーに接続するマシンがその証明書を信頼することを確認する必要があります。証明書に署名するためのオプションは次のとおりです。

- 自己署名証明書。これらは推奨されません。この証明書を信頼する必要がある他のマシンに手動でコピーする必要があるため、管理が困難です。
- エンタープライズ認証局。既存の PKI が導入されている場合、これは通常、内部デバイス間で使用する証明書に署名する最も簡単なオプションです。
- 公開認証局。これには、ドメインの所有権を認証局に証明する必要があります。管理されていないクライアントデバイスは、通常、主要な公開認証局からの証明書を信頼するように事前設定されているという利点があります。

新しい証明書を作成する

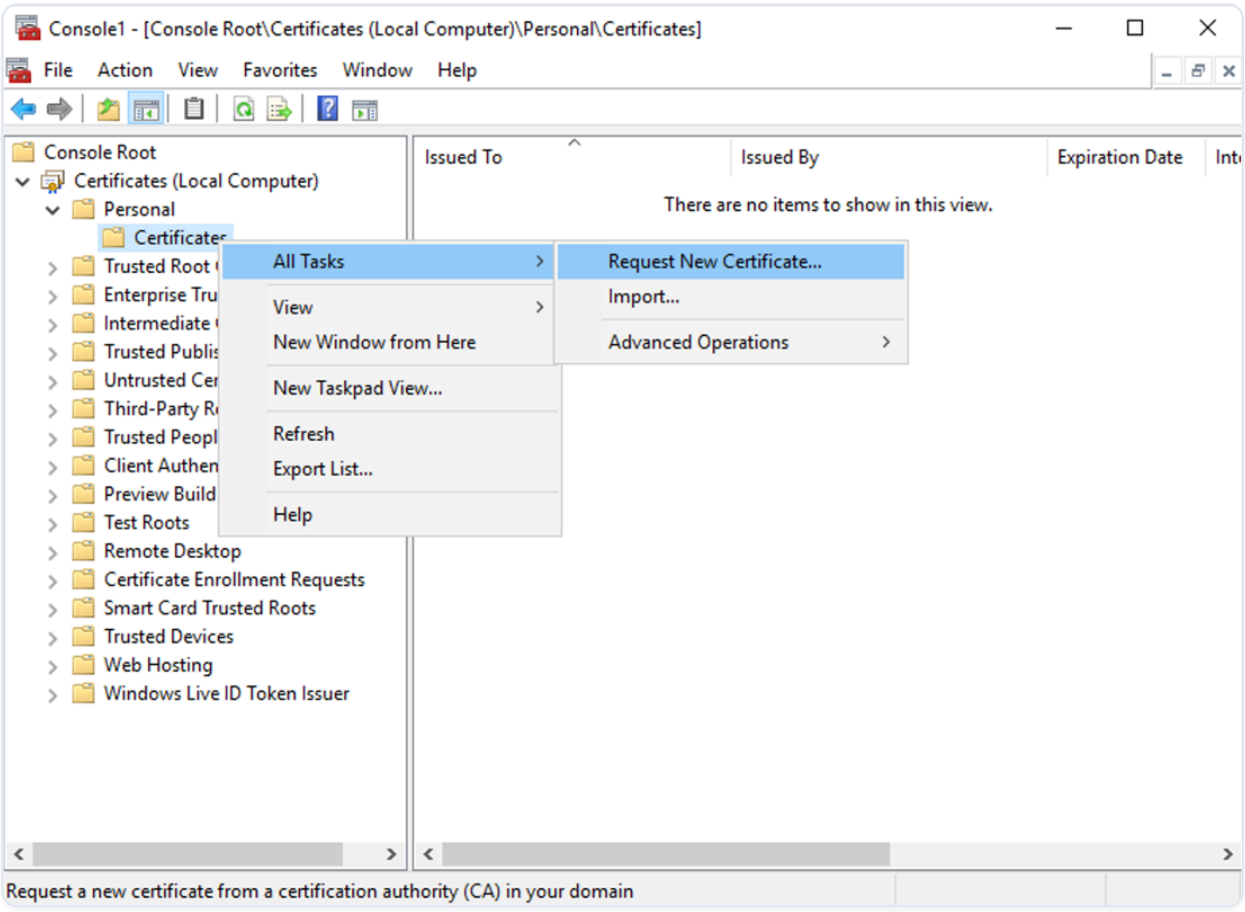
証明書の作成については、組織のポリシーと手順に従ってください。

Microsoft 証明機関を使用して証明書を作成する

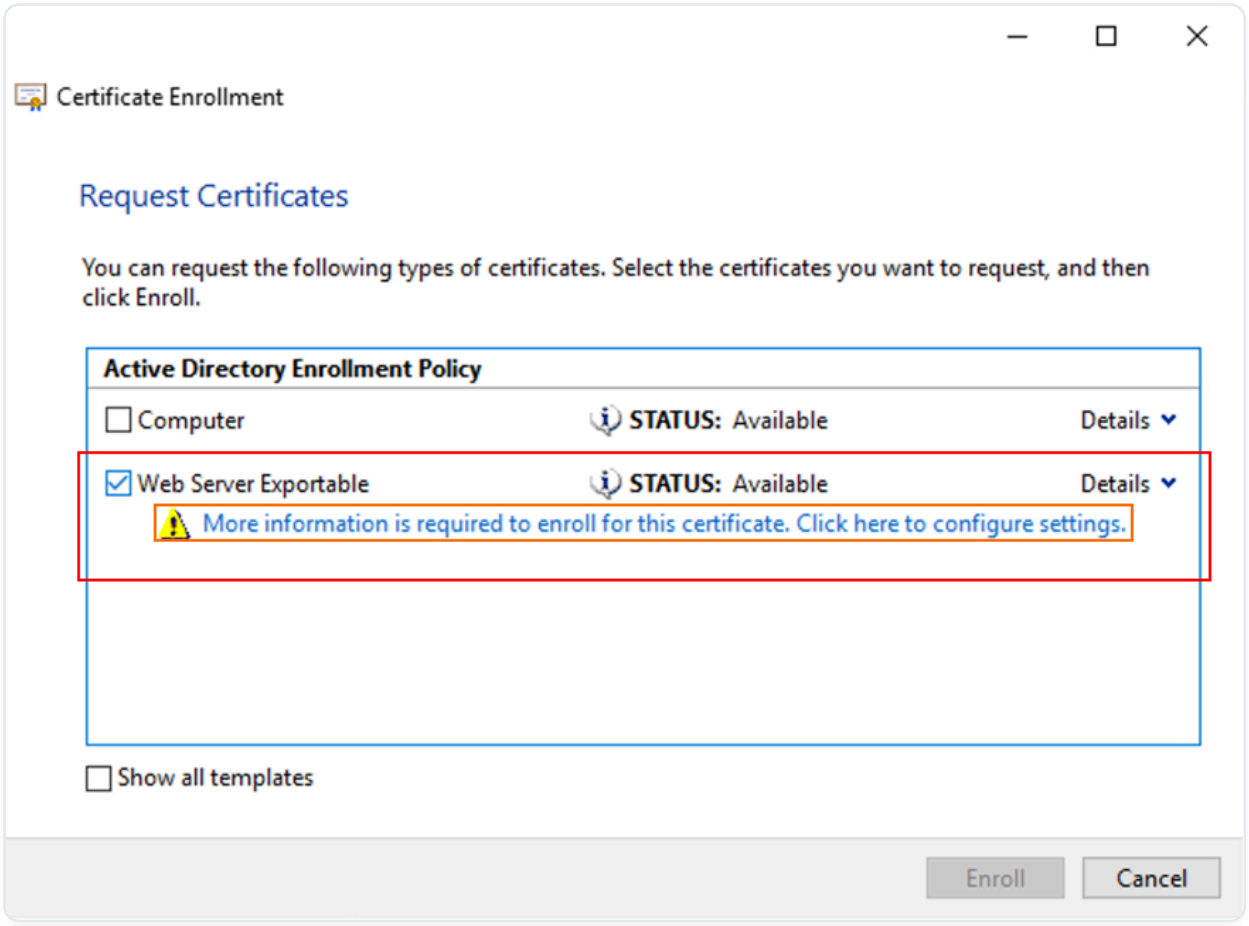
Microsoft 証明機関が Active Directory ドメインまたは Delivery Controller が参加している信頼されたフォレストに統合されている場合、証明書 MMC スナップインの証明書登録ウィザードから証明書を取得できます。Microsoft 証明機関は、Web サーバーでの使用に適した証明書テンプレートを公開している必要があります。

ルート証明書は、グループポリシーを使用してドメイン上の他のマシンに自動的に展開されます。したがって、ドメイン上の他のすべてのマシンは、Microsoft 証明機関を使用して作成された証明書を信頼します。ドメイン上にないマシンがある場合は、ルート認証機関証明書をエクスポートして、それらのマシンにインポートする必要があります。

1. サーバーで、MMC コンソールを開き、証明書スナップインを追加します。プロンプトが表示されたら、 を選択します。
2. **個人 > 証明書**を展開し、**すべてのタスク > 新しい証明書の要求**コンテキストメニューコマンドを使用します。



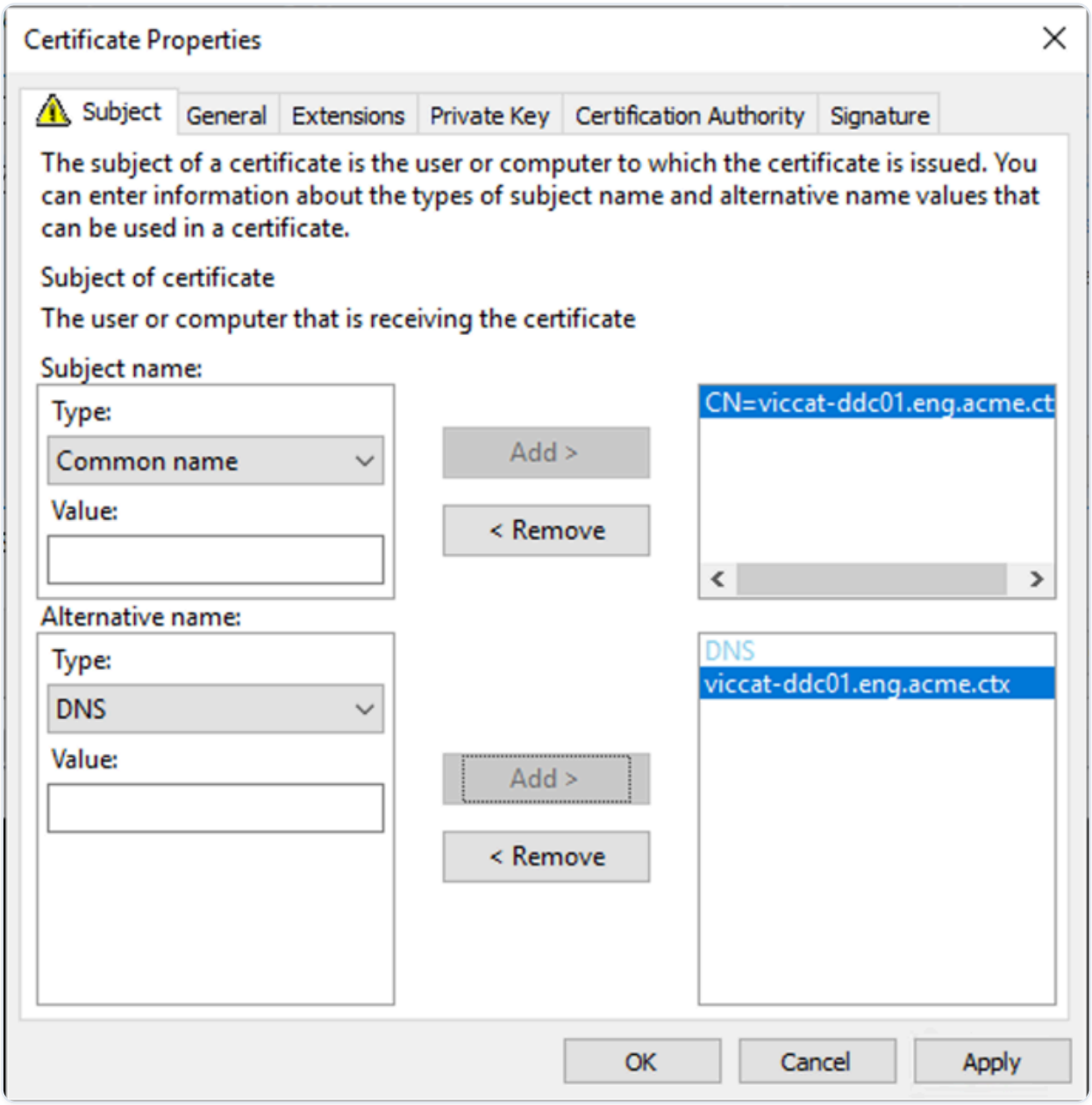
3. **次へ**をクリックして開始し、**次へ**をクリックして Active Directory 登録から証明書を取得することを確認します。
4. **Web Server Exportable** など、適切なテンプレートを選択します。テンプレートが Subject の値を自動的に提供するように設定されている場合は、詳細を指定せずに **Enroll** をクリックできます。それ以外の場合は、**More information is required to enroll for this certificate. Click here to configure settings.** をクリックします。



5. 証明書テンプレートの詳細を指定するには、**詳細**の矢印ボタンをクリックして、以下を構成します。

   サブジェクト名: を選択し、サーバーの FQDN を追加します。

   代替名: を選択し、サーバーの FQDN を追加します。



6. **OK**を押します。
7. **Enroll** を押して証明書を作成します。証明書の一覧に表示されます。

   個人証明書のスクリーンショット(/en-us/citrix-virtual-apps-desktops/current-release/media/personal-certificates.png)

IIS を使用して証明書要求を作成する

IIS がサーバーにインストールされている場合は、次の手順を実行します。

1. **インターネット インフォメーション サービス (IIS) マネージャー**を開きます
2. 接続リストでサーバーノードを選択します。
3. **サーバー証明書**を開きます。 「サーバー証明書」の場所を示すスクリーンショット(/en-us/citrix-virtual-apps-desktops/current-release/media/iis-server-certificates.png)

4. **操作**ペインから、**証明書要求の作成...** を選択します。 「証明書要求の作成」が強調表示された操作メニューのスクリーンショット(/en-us/citrix-virtual-apps-desktops/current-release/media/iis-create-certificate-request.png)
5. **識別名プロパティ**を入力します。 識別名プロパティ画面のスクリーンショット(/en-us/citrix-virtual-apps-desktops/current-release/media/iis-request-certificate-properties.png)
6. **暗号化サービスプロバイダーのプロパティ**画面で、**暗号化サービスプロバイダー**は既定のままにします。キーサイズは**2048**以上に設定します。 暗号化サービスプロバイダーのプロパティ画面のスクリーンショット(/en-us/citrix-virtual-apps-desktops/current-release/media/iis-request-certificate-crypto.png)
7. ファイル名を選択し、**完了**を押します。 ファイル名画面のスクリーンショット(/en-us/citrix-virtual-apps-desktops/current-release/media/iis-request-certificate-file-name.png)
8. CSR を証明機関にアップロードします。
9. 証明書を受け取ったら、**操作**ペインから**証明書要求の完了...** を選択します。 「証明書要求の完了」が強調表示された操作メニューのスクリーンショット(/en-us/citrix-virtual-apps-desktops/current-release/media/iis-complete-certificate-request.png)
10. 証明書を選択し、**フレンドリ名**を指定して**OK**を押します。 証明書応答の完了ウィンドウのスクリーンショット(/en-us/citrix-virtual-apps-desktops/current-release/media/iis-certificate-authority-response.png)

サブジェクトの別名を設定する方法はありません。そのため、証明書は共通名を使用して指定されたサーバーに限定されます。

証明書スナップインから証明書署名要求を作成する

証明書MMCスナップイン内から、証明書署名要求を作成できます。これにより、証明書を提供する認証局に送信できるファイルが生成されます。その後、証明書をインポートして、ローカルの秘密鍵と結合する必要があります。

1. サーバーで、MMCコンソールを開き、証明書スナップインを追加します。プロンプトが表示されたら、を選択します。
2. **個人** > **証明書**を展開します。
3. **すべてのタスク** > **高度な操作** > **カスタム要求の作成**を選択します。
4. **開始する前に**で、**次へ**を選択します。
5. **証明書登録ポリシーの選択**画面で、適切な既存のポリシーを選択するか、**登録ポリシーなしで続行**を選択します。

6. **カスタム要求**画面で、登録ポリシーを使用している場合は、利用可能な場合は**Web Server Exportable**などの適切なテンプレートを選択します。
7. **証明書情報**画面で、**詳細**を展開し、**プロパティ**を選択します。
8. **証明書のプロパティ**ウィンドウの**全般**タブで、適切なフレンドリ名を入力します。
9. **サブジェクト**タブで、次のようにします。
    a. **サブジェクト名**の下で、**共通名**を選択し、サーバーのFQDNを入力します。ワイルドカードを入力できます。**追加**を選択します。
    b. **サブジェクト名**の下で、組織、組織単位、地域、都道府県、国に適切な値を追加します。
    c. **代替名**の下で、**DNS**を選択します。サーバーのFQDNを追加します。複数のサーバーFQDNまたはワイルドカードFQDNを追加できます。
10. **拡張機能**タブで、次のようにします。
    - **キー使用法**の下で、**デジタル署名**と**キーの暗号化**を追加します。
    - 「**拡張キー使用法 (アプリケーションポリシー)**」で、「**サーバー認証**」と「**クライアント認証**」を追加します。
11. 「**秘密キー**」タブで。
    - 「**暗号化サービスプロバイダー (CSP) の選択**」で、適切なプロバイダーを選択します。
    - 「**キーオプション**」で、適切なキーサイズを選択します。RSAプロバイダーの場合、最小で2048のキーサイズを使用します。セキュリティを強化するために4096を選択することもできますが、パフォーマンスにわずかな影響があります。
    - 「**キーオプション**」で、「**秘密キーをエクスポート可能にする**」を選択します。
12. **OK**を選択します。
13. **次へ**を選択します。
14. 「**参照**」を選択し、要求を保存します。
15. 「**完了**」を選択します。
16. CSRを証明機関にアップロードします。
17. 証明書を受け取ったら、秘密キーにリンクされるように、同じサーバーに(#import-existing-certificate)インポートします。

新しい自己署名証明書を作成する

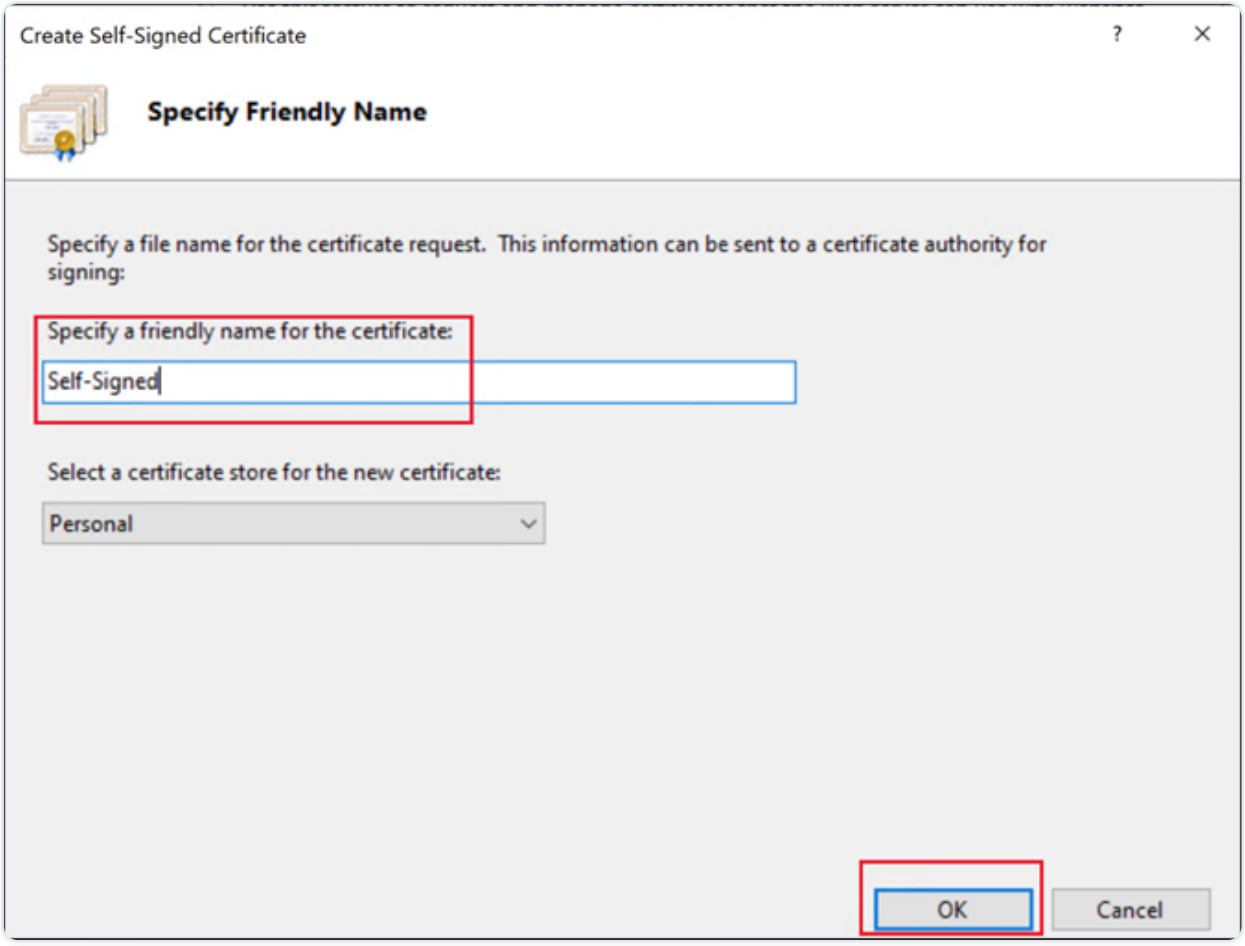
自己署名証明書は、デリバリーコントローラー™とWeb Studioのインストール中に作成されます。新しい自己署名証明書を生成し、既存の証明書を置き換えるために使用できます。

IISマネージャーを使用する

サーバーにIISがインストールされている場合は、次の手順を実行できます。

1. 管理者としてサーバーにログオンします。
2. IISマネージャーを開きます
3. 「**サーバー証明書**」を開きます
4. 「**操作**」ペインで、「**自己署名証明書の作成**」を選択します。

   サーバー証明書(/en-us/citrix-virtual-apps-desktops/current-release/media/server-certificates.png)
5. 「**自己署名証明書の作成**」で、証明書の名前を入力し、「**OK**」をクリックします。自己署名証明書が作成されます。



PowerShellの使用

PowerShellを使用して自己署名証明書を作成できます。

```
$certSubject = "CN=myddc.example.com" # The FQDN of the server.

$friendlyName = "Self-Signed-3"

$expireYears = 5



## Create new self-signed certificate under LocalMachine\My

$certificate = New-SelfSignedCertificate -Subject $certSubject
-CertStoreLocation "Cert:\LocalMachine\My\" -KeyExportPolicy Exportable
-KeySpec Signature -KeyLength 2048 -KeyAlgorithm RSA -HashAlgorithm SHA256
-FriendlyName $friendlyName -NotAfter $
([System.DateTime]::Now.AddYears($expireYears))



# Add to trusted root certificates

$rootCertStore = Get-Item "Cert:\LocalMachine\Root\"

$rootCertStore.Open([System.Security.Cryptography.X509Certificates.OpenFla
gs]::ReadWrite)

$rootCertStore.Add($certificate)
```

既存の証明書をインポートする

以下のいずれかの方法を使用して、既存の証明書をサーバーにインポートできます。

証明書のインポートウィザード

1. PFXファイルをダブルクリックするか、ファイルを右クリックして「**PFXのインストール**」を選択します。これにより、「**証明書のインポートウィザード**」が開きます。
2. 「**ストアの場所**」で、「**ローカルコンピューター**」を選択します。

   証明書のインポートウィザードのスクリーンショット(/en-us/citrix-virtual-apps-desktops/current-release/media/certificate-import-wizard.png)
3. 必要に応じてパスワードを入力します。

証明書のインポートウィザード、秘密キーの保護手順のスクリーンショット(/en-us/citrix-virtual-apps-desktops/current-release/media/key-protection.png)

4. 「**証明書ストア**」を選択します。サーバー証明書の場合は、「**個人**」を選択します。このマシンから信頼したいルート証明書または自己署名証明書である場合は、「**信頼されたルート証明機関**」を選択します。

   証明書のインポートウィザード、証明書ストアの手順のスクリーンショット(/en-us/citrix-virtual-apps-desktops/current-release/media/certificate-store.png)

コンピューター証明書の管理コンソールを使用する

1. コンピューター証明書の管理コンソールを開き、適切な証明書ストアに移動します。サーバー証明書の場合、通常は「**個人**」 > 「**証明書**」です。ルート証明書または自己署名証明書を信頼するには、「**信頼されたルート証明機関**」 > 「**証明書**」を選択します。
2. 証明書を右クリックし、「**すべてのタスク**」>「**インポート...**」を選択します。

   コンピューター証明書の管理コンソール(/en-us/citrix-virtual-apps-desktops/current-release/media/manage-computer-certificates-console.png)

3. 「**参照...**」を選択し、ファイルを選択します。
4. 必要に応じてパスワードを入力します。

PowerShell を使用する

証明書をインポートするには、PowerShell コマンドレット Import-PfxCertificate を使用します。たとえば、パスワード `123456` を使用して証明書 `certificate.pfx` を個人証明書ストアにインポートするには、次のコマンドを実行します。

```
Import-PfxCertificate -Password $(ConvertTo-SecureString -String "123456"
-AsPlainText -Force) -CertStoreLocation Cert:\LocalMachine\My\ -FilePath .
\Desktop\certificate.pfx
```

信頼されたルート証明書をインポートするには、`CertStoreLocation` を `Cert:\LocalMachine\Root\` に設定します。

秘密キーなしで証明書をエクスポートする

証明書を他のデバイスにインポートして信頼できるようにエクスポートするには、秘密キーを除外する必要があります。

1. コンピューター証明書の管理を開きます。「**個人**」>「**証明書**」に移動し、エクスポートする証明書を選択します。
2. 「**操作**」メニューから「**すべてのタスク**」を選択し、次に「**エクスポート**」を選択します。

   エクスポートメニューのある証明書管理のスクリーンショット(/en-us/citrix-virtual-apps-desktops/current-release/media/certificate-export.png)
3. 「**いいえ、秘密キーをエクスポートしません**」を選択し、「**次へ**」を押します。

   証明書のエクスポート(/en-us/citrix-virtual-apps-desktops/current-release/media/certificate-export-no-private-key.png)
4. 形式「**DER encoded binary X.509 (.CER)**」（デフォルト）を選択し、「**次へ**」を押します。
5. ファイル名を入力し、「**次へ**」を押します。

   「証明書のエクスポートウィザード、ファイル名」のスクリーンショット(/en-us/citrix-virtual-apps-desktops/current-release/media/certificate-export-file.png)
6. 「**完了**」を選択します。

   「証明書のエクスポートウィザード、エクスポート成功」のスクリーンショット(/en-us/citrix-virtual-apps-desktops/current-release/media/certificate-export-complete.png)

秘密キーを含む証明書のエクスポート

証明書を他のサーバーで使用できるようにエクスポートするには、秘密キーを含める必要があります。

1. コンピューター証明書の管理を開きます。「**個人**」>「**証明書**」に移動し、エクスポートする証明書を選択します。
2. 「**操作**」メニューから「**すべてのタスク**」を選択し、次に「**エクスポート**」を選択します。

   「エクスポート」メニューを含む証明書管理のスクリーンショット(/en-us/citrix-virtual-apps-desktops/current-release/media/certificate-export.png)
3. 「**はい、秘密キーをエクスポートします**」を選択し、次に「**次へ**」を選択します。

   「証明書のエクスポート」(/en-us/citrix-virtual-apps-desktops/current-release/media/certificate-export-private-key.png)
4. 「**セキュリティ**」タブでパスワードを入力し、「**次へ**」を選択します。

   「証明書のエクスポートウィザード、セキュリティ手順」のスクリーンショット(/en-us/citrix-virtual-apps-desktops/current-release/media/certificate-export-password.png)

5. ファイル名を入力し、「**次へ**」を選択します。

   「証明書のエクスポートウィザード、ファイル名」のスクリーンショット(/en-us/citrix-virtual-apps-desktops/current-release/media/certificate-export-file.png)

6. 「**完了**」を選択します。

   証明書のエクスポートウィザード、エクスポート成功のスクリーンショット](/en-us/citrix-virtual-apps-desktops/current-release/media/certificate-export-complete.png)

証明書をPEM形式に変換する

デフォルトでは、Windowsは秘密鍵を含む.pfxファイルとして、PKCS#12形式で証明書をエクスポートします。NetScaler® Gatewayまたはライセンスサーバーで証明書を使用するには、証明書と秘密鍵をPEM形式の別々のファイルに抽出する必要があります。これはopensslを使用して実行できます。

証明書をPEM形式でエクスポートするには、以下を実行します。

```
openssl pkcs12 -in name.pfx -clcerts -nokeys -out name.cer
```

既存のパスワードと新しいパスフレーズの入力を求められます

キーをPEM形式でエクスポートするには、以下を実行します。

```
openssl pkcs12 -in name.pfx -nocerts -out name.key
```

証明書の信頼

- 公開認証局の証明書を使用する場合、デバイスには通常、ルート証明書が事前に構成されています。
- エンタープライズ認証局を使用する場合、その証明書を信頼する必要があるすべてのデバイスにルート証明書を展開する必要があります。Active Directory証明書サービスを使用している場合、ルート証明書はグループポリシーを使用してドメイン上のすべてのマシンにも展開されます。NetScalerゲートウェイや他のドメイン上のマシンなど、ドメインに参加していないマシンには、ルート証明書を手動でインポートする必要があります。
- 自己署名証明書を使用している場合は、その証明書を信頼する必要があるすべてのマシンに手動でインストールする必要があります。

Windowsから自己署名証明書または信頼されたルート証明書をエクスポートするには、秘密鍵なしで証明書をエクスポートするを参照してください。

Windowsが証明書を信頼するようにするには、**信頼されたルート証明機関**ストアに証明書をインポートする必要があります。PowerShellを使用する場合は、ストア**Cert:\LocalMachine\Root**を入力します。

NetScalerが証明書を信頼するようにするには、まず証明書をPEM形式に変換する、次にルート証明書をインストールする必要があります。

スマートカード

スマートカードおよび同等のテクノロジーは、この記事で説明されているガイドライン内でサポートされています。Citrix Virtual AppsまたはCitrix Virtual Desktops™でスマートカードを使用するには、次の手順を実行します。

- スマートカードの使用に関する組織のセキュリティポリシーを理解します。これらのポリシーには、たとえば、スマートカードの発行方法やユーザーがスマートカードを保護する方法が記載されている場合があります。これらのポリシーの一部は、Citrix Virtual Apps™またはCitrix Virtual Desktops環境で再評価する必要がある場合があります。
- スマートカードで使用するユーザーデバイスの種類、オペレーティングシステム、および公開アプリケーションを決定します。
- スマートカードテクノロジーと、選択したスマートカードベンダーのハードウェアおよびソフトウェアに精通してください。
- 分散環境でデジタル証明書を展開する方法を理解します。

> **注:**
>
> (/ja-jp/citrix-virtual-apps-desktops/current-release/secure/smart-cards.html#fast-smart-card)ではスマートカードの登録はサポートされていません。スマートカードの登録は、高速スマートカードが無効になっている場合に機能する可能性がありますが、スマートカードとミドルウェアの種類によって異なります。Citrix Virtual Apps and Desktopsとの統合および仮想セッションを介したスマートカード登録のサポートについては、スマートカードおよびミドルウェアベンダーにお問い合わせください。

スマートカードの種類

企業向けスマートカードと消費者向けスマートカードは、同じ寸法、電気コネクタを持ち、同じスマートカードリーダーに適合します。

企業向けスマートカードにはデジタル証明書が含まれています。これらのスマートカードはWindowsログオンをサポートし、ドキュメントやメールのデジタル署名および暗号化のためのアプリケーションでも使用できます。Citrix Virtual Apps and Desktops™はこれらの用途をサポートしています。

消費者向けスマートカードにはデジタル証明書は含まれていません。共有シークレットが含まれています。これらのスマートカードは、支払い（チップアンドサインまたはチップアンドPINクレジットカードなど）をサポートできます。Windowsログオンや一般的なWindowsアプリケーションはサポートしていません。これらのスマートカードを使用するには、特殊なWindowsアプリケーションと適切なソフトウェアインフラストラクチャ（たとえば、決済カードネットワークへの接続を含む）が必要です。これらの特殊なアプリケーションをCitrix Virtual AppsまたはCitrix Virtual Desktopsでサポートする方法については、Citrixの担当者にお問い合わせください。

企業向けスマートカードには、同様の方法で使用できる互換性のある同等品があります。

- スマートカードと同等のUSBトークンは、USBポートに直接接続します。これらのUSBトークンは通常、USBフラッシュドライブと同じサイズですが、携帯電話で使用されるSIMカードと同じくらい小さい場合もあります。これらはスマートカードとUSBスマートカードリーダーの組み合わせとして表示されます。
- Windows Trusted Platform Module (TPM)を使用する仮想スマートカードは、スマートカードとして表示されます。これらの仮想スマートカードは、Citrix Workspace app（最小バージョンCitrix Receiver 4.3）を使用するWindows 8およびWindows 10でサポートされています。
    - XenApp and XenDesktop 7.6 FP3より前のバージョンのCitrix Virtual Apps and Desktops（旧XenApp and XenDesktop）は、仮想スマートカードをサポートしていません。
    - 仮想スマートカードの詳細については、仮想スマートカードの概要を参照してください。

    注記: 「仮想スマートカード」という用語は、ユーザーコンピューターに保存されているデジタル証明書を指すためにも使用されます。これらのデジタル証明書は、厳密にはスマートカードと同等ではありません。

Citrix Virtual Apps and Desktopsのスマートカードサポートは、Microsoft Personal Computer/Smart Card (PC/SC) 標準仕様に基づいています。最低要件として、スマートカードおよびスマートカードデバイスは、基盤となるWindowsオペレーティングシステムによってサポートされ、対象となるWindowsオペレーティングシステムを実行するコンピューターで使用するために、Microsoft Windows Hardware Quality Labs (WHQL) によって承認されている必要があります。ハードウェアのPC/SC準拠に関する追加情報については、Microsoftのドキュメントを参照してください。他の種類のユーザーデバイスもPS/SC標準に準拠している場合があります。詳細については、Citrix Readyプログラムを参照してください。

通常、各ベンダーのスマートカードまたは同等のものには、個別のデバイスドライバーが必要です。ただし、スマートカードがNIST個人識別検証（PIV）標準などの標準に準拠している場合、さまざまなスマートカードに単一のデバイスドライバーを使用できる可能性があります。デバイスドライバーは、ユーザーデバイスとVirtual Delivery Agent (VDA) の両方にインストールする必要があります。デバイスドライバーは、Citrixパートナーから入手できるスマートカードミドルウェアパッケージの一部として提供されることが多く、スマートカードミドルウェアパッケージは高度な機能を提供します。デバイスドライバーは、暗号化サービスプロバイダー（CSP）、キーストレージプロバイダー（KSP）、またはミニドライバーとも呼ばれる場合があります。

Windowsシステム用の以下のスマートカードとミドルウェアの組み合わせは、Citrixによってそのタイプの代表的な例としてテストされています。ただし、他のスマートカードとミドルウェアも使用できます。Citrix互換のスマートカードとミドルウェアに関する詳細については、`<http://www.citrix.com/ready>`を参照してください。

ミドルウェア	対応カード
Gemalto .NETカード用ミニドライバー	ジェムアルト ドットネット v2以降

他の種類のデバイスでのスマートカードの使用に関する情報については、そのデバイスのCitrix Workspace™アプリのドキュメントを参照してください。

リモートPCアクセス

スマートカードは、Windows 10、Windows 8、またはWindows 7を実行している物理的なオフィスPCへのリモートアクセスでのみサポートされています。

Remote PC Accessでテストされたスマートカードは次のとおりです。

ミドルウェア	対応カード
Gemalto .NETミニドライバー	ジェムアルト ドットネット v2以降

高速スマートカード

高速スマートカードは、既存のHDX PC/SCベースのスマートカードリダイレクトを改善したものです。高遅延のWAN環境でスマートカードを使用する場合にパフォーマンスが向上します。遅延が大きい場合、パフォーマンスの向上は大幅なものになります（例えば、Windowsの高速スマートカードログオンでは15秒、PC/SCベースのスマートカードリダイレクトでは1分以上）。

高速スマートカードは、現在サポートされているWindows VDAを搭載したホストマシンでデフォルトで有効になっています。ホスト側で高速スマートカードを無効にするには（例えば診断目的で）、'Disable Cryptographic Redirection' レジストリ設定をゼロ以外の値に設定します。

```
HKLM\SOFTWARE\Citrix\SmartCard

CryptographicRedirectionDisable (DWORD)
```

クライアント側で高速スマートカードを有効にするには、関連するStoreFrontサイトの*default.ica*ファイルにSmartCardCryptographicRedirection ICAパラメーターを含めます。

```
[WFClient]

SmartCardCryptographicRedirection=On
```

さらに、クライアント側では、以下のレジストリ設定を使用して、高速スマートカードを強制的に有効または無効にできます（例えば診断目的で）。

- HKLM\SOFTWARE\Citrix\ICA Client\SmartCard\ForceEnableCryptographicRedirection (ゼロ以外のDWORDとして)

または

- HKLM\SOFTWARE\Citrix\ICA Client\SmartCard\ForceDisableCryptographicRedirection (ゼロ以外のDWORDとして)

クライアントマシンが64ビットの場合、32ビットレジストリハイブを指定する必要があります（`WOW6432Node`を使用）。

制限事項:

- Windows版Citrix Workspaceアプリのみが高速スマートカードをサポートしています。default.icaファイルで高速スマートカードを設定した場合、Windows版ではないCitrix Workspaceアプリは、既存のPC/SCリダイレクトを依然として使用します。
- 高速スマートカードがサポートする唯一のダブルホップシナリオは、両方のホップで高速スマートカードが有効になっているICA® > ICAです。高速スマートカードはICA > RDPダブルホップシナリオをサポートしていないため、これらのシナリオは機能しません。
- 高速スマートカードはCryptography Next Generationをサポートしていません。したがって、高速スマートカードは楕円曲線暗号 (ECC) スマートカードをサポートしていません。
- 高速スマートカードは読み取り専用のキーコンテナ操作のみをサポートしています。

- 高速スマートカードはスマートカードPINの変更をサポートしていません。

VDAバージョン2203およびWindows版Citrix Workspaceアプリバージョン2202（またはそれ以降）以降、高速スマートカードはCryptography Next Generation (CNG) と互換性があります。さらに、楕円曲線暗号 (ECC) スマートカードは、ECDSAとECDHの両方で、P-256、P-384、P-521ビットの以下の曲線に対応しています。

VDAバージョン2203以降、高速スマートカードは、同じユーザーのログオンセッション内のアプリケーション間でスマートカードPINをキャッシュする機能を追加します。例えば、**セッションPINキャッシュ**が有効になっており、エンドユーザーが以前にOutlookにスマートカードPINを提供している場合、その後Wordを使用してドキュメントに署名すると、Wordはすでにキャッシュされているスマートカードpin（Outlookに送信されたもの）を使用します。**セッションPINキャッシュ**は、ユーザーがスマートカードPINを入力する回数を減らすことで、ユーザーエクスペリエンスを向上させます。さらに、スマートカードがVDAへのログオンに使用される場合、Windowsスマートカードログオンpinをオプションで**セッションPINキャッシュ**に保存できます。これにより、ユーザーエクスペリエンスがさらに向上します。

セッションPINキャッシュはデフォルトで無効になっています。VDA上の以下のレジストリ設定で有効化および制御できます。

HKLM\SOFTWARE\Citrix\SmartCard: で:

- `EnablePinSessionCache` をDWORDとして (有効にするにはゼロ以外)
- `EnableLogonPinSessionCache` をDWORDとして (有効にするにはゼロ以外)
- `PinSessionCacheEntryStaleTimeout` をDWORDとして (エントリが古くなるまでの秒数、デフォルトは1時間)

スマートカードリーダーの種類

スマートカードリーダーは、ユーザーデバイスに内蔵されている場合や、ユーザーデバイスに別途接続されている場合 (通常はUSBまたはBluetooth経由) があります。USB Chip/Smart Card Interface Devices (CCID) 仕様に準拠した接触型カードリーダーがサポートされています。これらには、ユーザーがスマートカードを挿入するスロットまたはスワイプ部分があります。Deutsche Kreditwirtschaft (DK) 規格では、接触型カードリーダーの4つのクラスが定義されています。

- クラス1スマートカードリーダーは最も一般的で、通常はスロットを備えています。クラス1スマートカードリーダーは、通常、オペレーティングシステムに付属の標準CCIDデバイスドライバーでサポートされます。
- クラス2スマートカードリーダーには、ユーザーデバイスからアクセスできないセキュアキーパッドも搭載されています。クラス2スマートカードリーダーは、セキュアキーパッドが統合

されたキーボードに組み込まれている場合があります。クラス2スマートカードリーダーについては、Citrixの担当者にお問い合わせください。セキュアキーパッド機能を有効にするには、リーダー固有のデバイスドライバーが必要になる場合があります。

- クラス3スマートカードリーダーには、セキュアディスプレイも搭載されています。クラス3スマートカードリーダーはサポートされていません。
- クラス4スマートカードリーダーには、セキュアトランザクションモジュールも搭載されています。クラス4スマートカードリーダーはサポートされていません。

注:

スマートカードリーダーのクラスは、USBデバイスクラスとは関係ありません。

スマートカードリーダーは、対応するデバイスドライバーをインストールしてユーザーデバイスにインストールする必要があります。

サポートされているスマートカードリーダーについては、使用しているCitrix Workspaceアプリのドキュメントを参照してください。Citrix Workspaceアプリのドキュメントでは、サポートされているバージョンは、スマートカードに関する記事またはシステム要件に関する記事に記載されています。

ユーザーエクスペリエンス

スマートカードのサポートは、Citrix Virtual Apps and Desktopsに統合されており、特定のICA/HDXスマートカード仮想チャネルを使用します。これはデフォルトで有効になっています。

重要: スマートカードリーダーに汎用USBリダイレクトを使用しないでください。これはスマートカードリーダーではデフォルトで無効になっており、有効にしてもサポートされません。

同じユーザーデバイス上で複数のスマートカードと複数のリーダーを使用できますが、パススルー認証が使用されている場合は、ユーザーが仮想デスクトップまたはアプリケーションを起動するときに、スマートカードを1枚だけ挿入する必要があります。アプリケーション内でスマートカードを使用する場合（たとえば、デジタル署名や暗号化機能の場合）、スマートカードの挿入やPINの入力に関する追加のプロンプトが表示されることがあります。これは、複数のスマートカードが同時に挿入されている場合に発生する可能性があります。

- スマートカードがすでにリーダーに挿入されているにもかかわらず、スマートカードの挿入を促すプロンプトが表示された場合は、ユーザーはキャンセルを選択する必要があります。
- PINの入力を求められた場合は、ユーザーはPINを再度入力する必要があります。

カード管理システムまたはベンダーユーティリティを使用してPINをリセットできます。

> **重要:**
>
> Citrix Virtual AppsまたはCitrix Virtual Desktopsセッション内で、Microsoft Remote Desktop Connectionアプリケーションとスマートカードを併用することはサポートされていません。これは「ダブルホップ」使用と呼ばれることがあります。

スマートカードを展開する前に

- スマートカードリーダー用のデバイスドライバーを入手し、ユーザーデバイスにインストールします。多くのスマートカードリーダーは、Microsoftが提供するCCIDデバイスドライバーを使用できます。
- スマートカードベンダーからデバイスドライバーと暗号化サービスプロバイダー（CSP）ソフトウェアを入手し、ユーザーデバイスと仮想デスクトップの両方にインストールします。ドライバーとCSPソフトウェアはCitrix Virtual Apps and Desktopsと互換性がある必要があります。互換性についてはベンダーのドキュメントを確認してください。ミニドライバーモデルをサポートおよび使用するスマートカードを使用する仮想デスクトップの場合、スマートカードミニドライバーは自動的にダウンロードされますが、http://catalog.update.microsoft.comまたはベンダーから入手することもできます。また、PKCS#11ミドルウェアが必要な場合は、カードベンダーから入手してください。
- 重要: Citrixは、Citrixソフトウェアをインストールする前に、物理コンピューターにドライバーとCSPソフトウェアをインストールしてテストすることを推奨します。
- Windows 10でInternet Explorerを使用してスマートカードを使用するユーザーのために、Citrix Receiver™ for WebのURLを信頼済みサイトリストに追加します。Windows 10では、信頼済みサイトの場合、Internet Explorerはデフォルトで保護モードで実行されません。
- 公開鍵インフラストラクチャ（PKI）が適切に構成されていることを確認してください。これには、Active Directory環境向けに証明書とアカウントのマッピングが正しく構成されており、ユーザー証明書の検証が正常に実行できることを確認することが含まれます。
- 展開が、Citrix WorkspaceアプリやStoreFrontなど、スマートカードで使用される他のCitrixコンポーネントのシステム要件を満たしていることを確認してください。
- サイト内の以下のサーバーへのアクセスを確保してください。
    - スマートカード上のログオン証明書に関連付けられているユーザーアカウントのActive Directoryドメインコントローラー

- デリバリーコントローラー™
- シトリックス ストアフロント
- シトリックス ゲートウェイ/シトリックス アクセス ゲートウェイ 10.x
- VDA
- (Remote PC Access の場合、オプション): Microsoft Exchange Server

スマートカードの使用を有効にする

ステップ 1. カード発行ポリシーに従って、ユーザーにスマートカードを発行します。

ステップ 2. (オプション) ユーザーがRemote PC Access を利用できるようにスマートカードを設定します。

ステップ 3. スマートカードのリモート処理のために、Delivery Controller と StoreFront (まだインストールされていない場合) をインストールして構成します。

ステップ 4. スマートカードの使用のためにStoreFront を有効にします。詳細については、StoreFront ドキュメントの「スマートカード認証の構成」を参照してください。

ステップ 5. スマートカードの使用のためにCitrix Gateway/Access Gateway を有効にします。詳細については、NetScaler ドキュメントの「認証と承認の構成」および「Web Interface を使用したスマートカードアクセスの構成」を参照してください。

ステップ 6. スマートカードの使用のためにVDA を有効にします。

- VDA に必要なアプリケーションと更新プログラムがあることを確認します。
- ミドルウェアをインストールします。
- スマートカードのリモート処理を設定し、ユーザーデバイス上のCitrix Workspace アプリと仮想デスクトップセッション間のスマートカードデータの通信を有効にします。

ステップ 7. ユーザーデバイス (ドメイン参加済みまたは非ドメイン参加済みマシンを含む) でスマートカードの使用を有効にします。詳細については、StoreFront ドキュメントの「スマートカード認証の構成」を参照してください。

- 証明機関のルート証明書と発行証明機関の証明書をデバイスのキーストアにインポートします。
- ベンダーのスマートカードミドルウェアをインストールします。

- Windows 用Citrix Workspace アプリをインストールして構成します。その際、グループポリシー管理コンソールを使用してicaclient.adm をインポートし、スマートカード認証を有効にしてください。

ステップ 8. 展開をテストします。テストユーザーのスマートカードを使用して仮想デスクトップを起動し、展開が正しく構成されていることを確認します。可能なすべてのアクセスメカニズム（たとえば、Internet Explorer および Citrix Workspace アプリを介したデスクトップへのアクセス）をテストします。

スマートカードリーダーの挿入回数を追跡する

スマートカードのリモート処理を使用すると、SCardGetStatusChange 関数を使用して、スマートカードがリーダーに挿入または取り外された回数を追跡できます。この関数は、監視するリーダーごとに 1 つの SCARD_READERSTATE データ構造の配列を更新します。各 SCARD_READERSTATE の dwEventState フィールドのハイワード（16 ビット）には、リーダーのカウントが含まれています。詳細については、Microsoft の記事 SCardGetStatusChangeA function および SCARD_READERSTATEA structure を参照してください。

リーダー挿入回数レポート設定は、デフォルトで無効になっています。追跡を有効にするには、次のレジストリキーを追加します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard

名前: EnableReaderInsertCountReporting

種類: DWORD

値: ゼロ以外の任意の値

セッションが切断されると、カウントはゼロにリセットされます。

リーダー挿入回数レポートは、サードパーティのスマートカードミドルウェアと互換性があります。

スマートカードの展開

この製品バージョンおよびこのバージョンを含む混在環境では、以下の種類のスマートカード展開がサポートされています。その他の構成も動作する可能性がありますが、サポートされていません。

タイプ	STOREFRONT™ 接続
ローカルのドメイン参加済みコンピューター	直接接続
ドメイン参加済みコンピューターからのリモートアクセス	Citrix Gateway 経由で接続
ドメインに参加していないコンピューター	直接接続
ドメインに参加していないコンピューターからのリモートアクセス	Citrix Gateway 経由で接続
ドメインに参加していないコンピューターおよびシンクライアントがDesktop Applianceサイトにアクセス	Desktop Applianceサイト経由で接続
XenApp® Services URL を介してStoreFrontにアクセスするドメイン参加済みコンピューターおよびシンクライアント	XenApp Services URL 経由で接続

展開タイプは、スマートカードリーダーが接続されているユーザーデバイスの特性によって定義されます。

- デバイスがドメイン参加済みか、非ドメイン参加済みか。
- デバイスがStoreFrontにどのように接続されているか。
- 仮想デスクトップとアプリケーションを表示するためにどのソフトウェアが使用されているか。

さらに、Microsoft WordやMicrosoft Excelなどのスマートカード対応アプリケーションをこれらの展開で使用できます。これらのアプリケーションを使用すると、ユーザーはドキュメントにデジタル署名したり、暗号化したりできます。

バイモーダル認証

これらの展開のそれぞれにおいて可能な場合、Receiverはスマートカードの使用とユーザー名およびパスワードの入力の選択肢をユーザーに提供することで、バイモーダル認証をサポートします。これは、スマートカードが使用できない場合（たとえば、ユーザーが自宅に忘れた場合やログオン証明書が期限切れになった場合）に役立ちます。

非ドメイン参加デバイスのユーザーはReceiver for Windowsに直接ログオンするため、ユーザーが明示的な認証にフォールバックできるようにすることができます。バイモーダル認証を構成する

と、ユーザーは最初にスマートカードとPINを使用してログオンするように求められますが、スマートカードに問題が発生した場合は明示的な認証を選択するオプションがあります。

Citrix Gatewayを展開する場合、ユーザーはデバイスにログオンし、Receiver for WindowsによってCitrix Gatewayへの認証を求められます。これは、ドメイン参加済みデバイスと非ドメイン参加済みデバイスの両方に適用されます。ユーザーは、スマートカードとPIN、または明示的な資格情報を使用してCitrix Gatewayにログオンできます。これにより、Citrix Gatewayログオンに対してバイモーダル認証をユーザーに提供できます。Citrix GatewayからStoreFrontへのパススルー認証を構成し、スマートカードユーザーの資格情報検証をCitrix Gatewayに委任することで、ユーザーはStoreFrontにサイレント認証されます。

複数のActive Directoryフォレストに関する考慮事項

Citrix環境では、スマートカードは単一のフォレスト内でサポートされます。フォレストをまたがるスマートカードログオンには、すべてのユーザーアカウントへの直接的な双方向フォレスト信頼が必要です。スマートカードを含むより複雑なマルチフォレスト展開（つまり、信頼が一方通行であるか、異なるタイプである場合）はサポートされていません。

リモートデスクトップを含むCitrix環境でスマートカードを使用できます。この機能は、ローカル（スマートカードが接続されているユーザーデバイス上）またはリモート（ユーザーデバイスが接続するリモートデスクトップ上）にインストールできます。

スマートカード取り外しポリシー

製品に設定されているスマートカード取り外しポリシーは、セッション中にリーダーからスマートカードを取り外した場合に何が起こるかを決定します。スマートカード取り外しポリシーは、Windowsオペレーティングシステムを介して構成および処理されます。

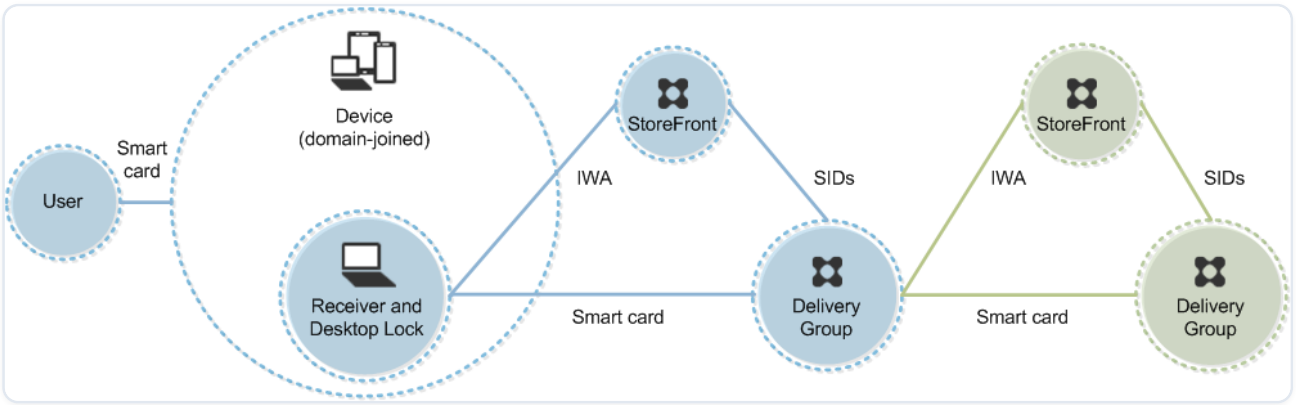
ポリシー設定	デスクトップの動作
何もしない	何もしない。
ワークステーションをロックする	デスクトップセッションが切断され、仮想デスクトップがロックされます。
強制ログオフ	ユーザーは強制的にログオフされます。ネットワーク接続が失われ、この設定が有効になっている場合、セッションがログオフされ、ユーザーはデータを失う可能性があります。
リモートターミナルサービスセッションの場合に切断する	セッションが切断され、仮想デスクトップがロックされます。

証明書失効チェック

証明書失効チェックが有効になっていて、ユーザーが無効な証明書を含むスマートカードをカードリーダーに挿入した場合、ユーザーは認証できず、その証明書に関連するデスクトップまたはアプリケーションにアクセスできません。たとえば、無効な証明書がメールの復号化に使用されている場合、メールは暗号化されたままになります。認証に使用されるものなど、カード上の他の証明書がまだ有効な場合、それらの機能はアクティブなままです。

展開例：ドメイン参加済みコンピューター

この展開では、Desktop Viewer を実行し、StoreFront に直接接続するドメイン参加済みユーザーデバイスを使用します。



ユーザーはスマートカードとPINを使用してデバイスにログオンします。Receiver は、統合Windows認証 (IWA) を使用してユーザーをStoreFrontサーバーに認証します。StoreFront は、ユーザーセキュリティ識別子 (SID) を Citrix Virtual Apps または Citrix Virtual Desktops に渡します。ユーザーが仮想デスクトップまたはアプリケーションを起動すると、Receiver でシングルサインオン機能が構成されているため、PIN の再入力を求められることはありません。

この展開は、2番目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiver は、2番目のStoreFrontサーバーに認証します。この2番目の接続には、任意の認証方法を使用できます。最初のホップで示された構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例: ドメイン参加済みコンピューターからのリモートアクセス

この展開では、Desktop Viewer を実行し、Citrix Gateway/Access Gateway を介して StoreFront に接続するドメイン参加済みユーザーデバイスが関与します。

展開例: ドメイン参加済みコンピューターからのリモートアクセス(/en-us/citrix-virtual-apps-desktops/current-release/media/smartcard2_1.png)

ユーザーはスマートカードとPINを使用してデバイスにログオンし、その後Citrix Gateway/Access Gatewayに再度ログオンします。この2回目のログオンは、Receiverがこの展開でバイモーダル認証を許可しているため、スマートカードとPIN、またはユーザー名とパスワードのいずれかで行うことができます。

ユーザーはStoreFrontに自動的にログオンし、StoreFrontはユーザーセキュリティ識別子（SID）をCitrix Virtual Apps™またはCitrix Virtual Desktopsに渡します。ユーザーが仮想デスクトップまたはアプリケーションを起動しても、Receiverでシングルサインオン機能が構成されているため、PINの再入力を求められることはありません。

この展開は、2台目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2台目のStoreFrontサーバーに対して認証を行います。この2番目の接続には、任意の認証方法を使用できます。最初のホップで示された構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例: ドメイン非参加コンピューター

この展開では、Desktop Viewer を実行し、StoreFront に直接接続するドメイン非参加ユーザーデバイスが関与します。

展開例: ドメイン非参加コンピューター(/en-us/citrix-virtual-apps-desktops/current-release/media/smartcard3_1.png)

ユーザーはデバイスにログオンします。通常、ユーザーはユーザー名とパスワードを入力しますが、デバイスがドメインに参加していないため、このログオンの資格情報はオプションです。この展開ではバイモーダル認証が可能であるため、Receiverはユーザーにスマートカードと PIN、またはユーザー名とパスワードのいずれかを要求します。その後、ReceiverはStorefrontに対して認証を行います。

StoreFrontはユーザーセキュリティ識別子（SID）をCitrix Virtual AppsまたはCitrix Virtual Desktopsに渡します。ユーザーが仮想デスクトップまたはアプリケーションを起動すると、この展開ではシングルサインオン機能が利用できないため、PINの再入力を求められます。

この展開は、2台目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2台目のStoreFrontサーバーに対して認証を行います。この2番目の接続には、任意の認証方法を使用できます。最初のホップで示された構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例: ドメイン非参加コンピューターからのリモートアクセス

この展開では、Desktop Viewer を実行し、StoreFront に直接接続するドメイン非参加ユーザーデバイスが関与します。

展開例: ドメイン非参加コンピューターからのリモートアクセス(/en-us/citrix-virtual-apps-desktops/current-release/media/smartcard4_1.png)

ユーザーがデバイスにログオンします。通常、ユーザーはユーザー名とパスワードを入力しますが、デバイスがドメインに参加していないため、このログオンの資格情報はオプションです。この展開ではバイモーダル認証が可能なため、ReceiverはスマートカードとPIN、またはユーザー名とパスワードのいずれかをユーザーに要求します。その後、ReceiverはStorefrontに対して認証を行います。

StoreFrontはユーザーセキュリティ識別子（SID）をCitrix Virtual AppsまたはCitrix Virtual Desktopsに渡します。ユーザーが仮想デスクトップまたはアプリケーションを起動すると、この展開ではシングルサインオン機能が利用できないため、ユーザーは再度PINを要求されます。

この展開は、2番目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2番目のStoreFrontサーバーに対して認証を行います。この2番目の接続には、任意の認証方法を使用できます。最初のホップに示されている構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例：ドメインに参加していないコンピューターとシンクライアントがDesktop Applianceサイトにアクセスする場合

この展開には、Desktop Lockを実行し、Desktop Applianceサイトを介してStoreFrontに接続する可能性のある、ドメインに参加していないユーザーデバイスが含まれます。

Desktop Lockは、Citrix Virtual Apps、Citrix Virtual Desktops、およびVDI-in-a-Boxとともにリリースされる個別のコンポーネントです。これはDesktop Viewerの代替であり、主に再利用されたWindowsコンピューターとWindowsシンクライアント向けに設計されています。Desktop Lockは、これらのユーザーデバイスのWindowsシェルとタスクマネージャーを置き換え、ユーザーが基盤となるデバイスにアクセスするのを防ぎます。Desktop Lockを使用すると、ユーザーはWindows Server MachineデスクトップとWindows Desktop Machineデスクトップにアクセスできます。Desktop Lockのインストールはオプションです。

展開例：ドメインに参加していないコンピューターとシンクライアントがDesktop Applianceサイトにアクセスする場合(/en-us/citrix-virtual-apps-desktops/current-release/media/smartcard5_1.png)

ユーザーはスマートカードを使用してデバイスにログオンします。デバイスでDesktop Lockが実行されている場合、デバイスはキオスクモードで実行されているInternet Explorerを介してDesktop Applianceサイトを起動するように構成されています。サイト上のActiveXコントロールがユーザーにPINを要求し、それをStoreFrontに送信します。StoreFrontはユーザーセキュリティ識別子（SID）をCitrix Virtual AppsまたはCitrix Virtual Desktopsに渡します。割り当てられたデスクトップグループのアルファベット順リストで最初に利用可能なデスクトップが起動します。

この展開は、2番目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2番目のStoreFrontサーバーに対して認証を行います。この2番目の接続には、任意の認証方法を使用できます。最初のホップに示されている構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例：ドメインに参加しているコンピューターとシンクライアントがXenApp Services URLを介してStoreFrontにアクセスする場合

この展開には、Desktop Lockを実行し、XenApp Services URLを介してStoreFrontに接続するドメインに参加しているユーザーデバイスが含まれます。

Desktop Lockは、Citrix Virtual Apps、Citrix Virtual Desktops、およびVDI-in-a-Boxとともにリリースされる個別のコンポーネントです。これはDesktop Viewerの代替であり、主に再利用されたWindowsコンピューターとWindowsシンクライアント向けに設計されています。Desktop Lockは、これらのユーザーデバイスのWindowsシェルとタスクマネージャーを置き換え、ユーザーが基盤となるデバイスにアクセスするのを防ぎます。Desktop Lockを使用すると、ユーザーはWindows Server MachineデスクトップとWindows Desktop Machineデスクトップにアクセスできます。Desktop Lockのインストールはオプションです。

展開例：ドメインに参加しているコンピューターとシンクライアントがXenApp Services URLを介してStoreFrontにアクセスする場合(/en-us/citrix-virtual-apps-desktops/current-release/media/smartcard6.png)

ユーザーはスマートカードとPINを使用してデバイスにログオンします。デバイスでDesktop Lockが実行されている場合、統合Windows認証（IWA）を使用してユーザーをStorefrontサーバーに認証します。StoreFrontはユーザーセキュリティ識別子（SID）をCitrix Virtual AppsまたはCitrix Virtual Desktopsに渡します。ユーザーが仮想デスクトップを起動すると、Receiverでシングルサインオン機能が構成されているため、ユーザーは再度PINを要求されません。

この展開は、2番目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2番目のStoreFrontサーバーに対して認証を行います。この2番目の接続には、任意の認証方法を使用できます。最初

のホップに示されている構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

スマートカードによるパススルー認証とシングルサインオン

パススルー認証

スマートカードによる仮想デスクトップへのパススルー認証は、Windows 10、Windows 8、Windows 7 SP1 EnterpriseおよびProfessional Editionを実行しているユーザーデバイスでサポートされています。

スマートカードによるホスト型アプリケーションへのパススルー認証は、Windows Server 2012およびWindows Server 2008 R2 SP1を実行しているサーバーでサポートされています。

スマートカードホスト型アプリケーションでパススルー認証を使用するには、サイトの認証方法としてスマートカードによるパススルーを構成する際に、Kerberosの使用を有効にしてください。

注：スマートカードによるパススルー認証の利用可能性は、以下を含む（ただしこれらに限定されない）多くの要因に依存します。

- パススルー認証に関する組織のセキュリティポリシー。
- ミドルウェアの種類と構成。
- スマートカードリーダーの種類。
- ミドルウェアのPINキャッシュポリシー。

スマートカードによるパススルー認証はCitrix StoreFrontで構成されます。詳細については、StoreFrontのドキュメントを参照してください。

シングルサインオン

シングルサインオンは、仮想デスクトップおよびアプリケーションの起動時にパススルー認証を実装するCitrixの機能です。この機能は、ドメイン参加済み、StoreFrontへの直接接続、およびドメイン参加済み、NetScalerからStoreFrontへのスマートカード展開で使用でき、ユーザーがPINを入力する回数を減らすことができます。これらの展開タイプでシングルサインオンを使用するには、StoreFrontサーバーにあるdefault.icaファイルで以下のパラメーターを編集します。

- ドメイン参加済み、StoreFrontへの直接接続スマートカード展開 — DisableCtrlAltDelをOffに設定
- ドメイン参加済み、NetScalerからStoreFrontへのスマートカード展開 — UseLocalUserAndPasswordをOnに設定

これらのパラメーターの設定に関する詳細な手順については、StoreFrontまたはCitrix Gatewayのドキュメントを参照してください。

シングルサインオン機能の利用可否は、以下を含む多くの要因に依存します（ただし、これらに限定されません）。

- シングルサインオンに関する組織のセキュリティポリシー。
- ミドルウェアの種類と構成。
- スマートカードリーダーの種類。
- ミドルウェアのPINキャッシュポリシー。

> **注:**
>
> ユーザーがスマートカードリーダーが接続されたマシン上のVirtual Delivery Agent (VDA) にログオンすると、スマートカードやパスワードなど、以前に成功した認証モードを表すWindowsタイルが表示されることがあります。その結果、シングルサインオンが有効になっている場合、シングルサインオンタイルが表示されることがあります。ログオンするには、シングルサインオンタイルは機能しないため、ユーザーは別のタイルを選択するために**ユーザーの切り替え**を選択する必要があります。

Delivery Controller で TLS を有効にする

既定では、HTTPとHTTPSの両方が有効になっています。HTTPSは、サーバーのFQDNを共通名として使用する自己署名証明書を使用しますが、これはStoreFront™やWebブラウザによって信頼されていません。

delivery controller™ で TLS を有効にするには、次の操作を行う必要があります。

- すべての Delivery Controller にサーバー証明書を取得、インストール、登録します。詳細については、「証明書の要求とインストール」を参照してください。
- TLS 証明書を使用してポートを構成します。詳細については、「証明書のインストール」を参照してください。
- モニターサービスで HTTPS を有効にする。
- HTTP を無効にして HTTPS トラフィックを強制します。詳細については、「HTTPS トラフィックのみを強制するHTTPS トラフィックのみを強制する」を参照してください。

- 必要に応じて、Controller が HTTP および HTTPS トラフィックをリッスンするために使用するポートを変更できます。詳細については、「HTTP または HTTPS ポートの変更」を参照してください。

証明書の要求とインストール

TLSを使用するには、共通名またはサブジェクト代替名がサーバーのFQDNと一致する証明書をインストールする必要があります。Delivery Controllerの前にロードバランサーを使用している場合は、サーバーとロードバランサーの両方のFQDNをサブジェクト代替名として含めます。詳細については、証明書を参照してください。StoreFrontがDelivery Controllerに接続するには、RSAデジタル署名アルゴリズムを使用する必要があります。StoreFrontはECDSAアルゴリズムを使用する証明書をサポートしていません。

SSL/TLS リスナーポートの構成

Web Studio および Director の一部としてインストールされる IIS Windows コンポーネントが同じサーバーにインストールされている場合、IIS を使用して TLS を構成できます。詳細については、「Web Studio および Director で TLS を有効にする」を参照してください。それ以外の場合は、PowerShell を使用して証明書を構成するには、次の手順を実行します。

1. 既存の証明書がバインドされているかどうかを確認するには、コマンドプロンプトを開き、`netsh http show sslcert` を実行します:

   ```
   netsh http show sslcert
   ```

2. 既存のバインドがある場合は、それを削除します。

   ```
   netsh http delete sslcert ipport=0.0.0.0:443
   ```

   既存のバインドで特定の IP アドレスとポートが指定されていた場合は、`0.0.0.0:443` をその IP アドレスとポートに置き換えます。

3. 以前にインストールした証明書のサムプリントを見つけます。サムプリントを表示するには、**コンピューター証明書の管理**を開き、証明書を参照して開き、**詳細**タブに移動します。

   サムプリントを示す証明書のプロパティのスクリーンショット(/en-us/citrix-virtual-apps-desktops/current-release/media/certificate-thumbprint.png)

   または、PowerShellを使用することもできます。たとえば、次のスクリプトは、共通名がサーバーのホスト名と一致する証明書を検索し、サムプリントを出力します。

```
$HostName =
([System.Net.Dns]::GetHostByName(($env:computerName))).Hostname

$Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object
{$_.Subject -match ("CN=" + $HostName)}).Thumbprint -join ';'

Write-Host -Object "Certificate Thumbprint for $($HostName): $
($Thumbprint)" -Foreground Yellow
```

証明書の共通名がホスト名と一致しない場合、これは失敗します。ホスト名に対して複数の証明書がある場合、これは連結された複数のサムプリントを返し、適切なサムプリントを選択する必要があります。

次の例では、フレンドリ名で証明書を検索します。

```
$friendlyName = "My certificate name"

$Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object
{$_.FriendlyName -eq $friendlyNam}).Thumbprint -join ';'

Write-Host -Object "Certificate Thumbprint for $friendlyName: $
($Thumbprint)" -Foreground Yellow
```

指定されたフレンドリ名を持つ証明書が複数ある場合、これは連結された複数のサムプリントを返し、適切なサムプリントを選択する必要があります。

4. 証明書をポートにバインドするには、`netsh http add sslcert`コマンドを使用します。

```
netsh http add sslcert ipport=[IP address]:443 certhash=[certificate
hash] appid=[application GUID] disablelegacytls=enable
```

- `ipport`: IPアドレスとポート。0.0.0.0:443を使用すると、すべてのIPアドレスに適用されます。代わりに、特定のIPアドレスを指定することもできます。
- `certhash`: 前の手順で特定した証明書のサムプリント。
- `appid`: シトリックス ブローカー サービスのGUID。

> **注:**

> 証明書を更新または再バインドする場合は、任意の GUID ではなく、Broker Service に関連付けられている特定の `appid` を使用します。 Citrix Broker Service の正しい `appid` を見つけるには、次の手順を実行します。

a. 管理者としてPowerShellコマンドウィンドウを開き、次のコマンドを実行します。

```
Get-WmiObject -Class Win32_Product | Select-String -Pattern
"broker"
```

b. 出力でCitrix Broker ServiceのIdentifyingNumber (GUID) を見つけます（例：`{D333C884-187F-447C-8C67-463F33989C8F}`）。このGUIDを`appid`パラメーターに使用します。

- `disablelegacytls=enable`: レガシーバージョンのTLSを無効にします。このパラメーターはWindows 2022以降で利用可能です。Windows 2022ではTLS 1.0と1.1を無効にします。Windows 2025では、TLS 1.0と1.1がデフォルトで無効になっているため、これは不要です。

例えば、すべてのIPアドレスで、サムプリント `bc96f958848639fd101a793b87915d5f2829b0b6` の証明書をポート `443` にバインドするには、次のコマンドを実行します。

```
netsh http add sslcert ipport=0.0.0.0:443
certhash=bc96f958848639fd101a793b87915d5f2829b0b6 appid={91fe7386-
e0c2-471b-a252-1e0a805febac} disablelegacytls=enable
```

HTTPS が有効になったら、StoreFront deployments と NetScaler Gateway を、デリバリーコントローラーへの接続に HTTP ではなく HTTPS を使用するように構成します。

HTTPS 用のモニターサービス OData API を構成する

モニターサービスは、Citrix® およびサードパーティアプリケーションがデータを照会できるように、OData v3 および v4 API を提供します。Director は OData API V3 を使用して監視サービスに接続します。HTTPS 用のモニター OData API を構成するには、次の手順を完了します。

1. 次のPowerShellを実行します。

```
$serviceGroup = Get-ConfigRegisteredServiceInstance -ServiceType
Monitor | Select -First 1 ServiceGroupUid

Remove-ConfigServiceGroup -ServiceGroupUid
$serviceGroup.ServiceGroupUid

& 'C:\Program Files\Citrix\Monitor\Service\citrix.monitor.exe'
-ConfigureFirewall -RequireODataTls –OdataPort 443 -RequireODataSdkTls
–OdataSdkPort 443

get-MonitorServiceInstance | register-ConfigServiceInstance

Get-ConfigRegisteredServiceInstance -ServiceType Config | Reset-
MonitorServiceGroupMembership
```

2. テキストエディターでファイル `C:\Program Files\Citrix\Monitor\Service\Citrix.Monitor.exe.Config` を開きます。要素 `<add key="owin:baseAddress" value="http://localhost/citrix/monitor/odata/v4" />` を見つけて、`<add key="owin:baseAddress" value="https://localhost/citrix/monitor/odata/v4" />` に変更します。

暗号スイートを構成する

暗号スイートの順序リストには、`TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` または `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` の暗号スイート（またはその両方）を含める必要があります。また、これらの暗号スイートは、`TLS_DHE_` の暗号スイートよりも前に配置する必要があります。

1. Microsoft グループポリシーエディターを使用して、**コンピューターの構成 > 管理用テンプレート > ネットワーク > SSL 構成設定** に移動します。
2. 「SSL 暗号スイートの順序」ポリシーを編集します。デフォルトでは、このポリシーは「未構成」に設定されています。このポリシーを「有効」に設定します。
3. スイートを正しい順序に並べ替えます。使用したくない暗号スイートはすべて削除します。

`TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` または `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` が、`TLS_DHE_` の暗号スイートよりも前に配置されていることを確認してください。

Microsoft Learn で、TLS 暗号スイートの順序の構成 も参照してください。

HTTPS トラフィックのみを強制する

XML Service が HTTP トラフィックを無視するように構成することをお勧めします。

1. `regedit` を実行します。
2. `HKLM\Software\Citrix\DesktopServer\`を開く
3. `XmlServicesEnableNonSsl`という名前の新しいDWORD値を作成し、0に設定します。
4. Broker Serviceを再起動します。

HTTPSトラフィックを無視するために作成できる対応するレジストリDWORD値`XmlServicesEnableSsl`があります。これが0に設定されていないことを確認してください。

HTTPまたはHTTPSポートを変更する

デフォルトでは、Controller上のXMLサービスは、HTTPトラフィックにはポート80を、HTTPSトラフィックにはポート443をリッスンします。デフォルト以外のポートを使用することもできますが、Controllerを信頼できないネットワークに公開することによるセキュリティリスクに注意してください。デフォルトを変更するよりも、スタンドアロンのStoreFrontサーバーを展開する方が望ましいです。

Controllerで使用されるデフォルトのHTTPまたはHTTPSポートを変更するには、Studioから次のコマンドを実行します。

```
BrokerService.exe -StoreFrontPort <http-port> -StoreFrontTlsPort <https-port>
```

ここで：

- `<http-port>`はHTTPトラフィックのポート番号です
- `<https-port>`はHTTPSトラフィックのポート番号です。

> **注:**

> ポートを変更した後、Studioはライセンスの互換性とアップグレードに関するメッセージを表示する場合があります。この問題を解決するには、次のPowerShellコマンドレットシーケンスを使用してサービスインスタンスを再登録します。

```
Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding XML_HTTPS
|

Unregister-ConfigRegisteredServiceInstance

Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" |

Register-ConfigServiceInstance
```

Web StudioとDirectorでTLSを有効にする

Web StudioおよびDirectorへの接続を保護するために、HTTPSを有効にして常にTLSを使用することをお勧めします。この記事では、Web StudioとDirectorを構成して、信頼された証明書を使用し、HTTPS経由で安全なアクセスを確保する方法について説明します。

デフォルトの動作

Web Studioをインストールすると、インストーラーは自己署名証明書を作成し、現在のサーバーのポート443にバインドします。ローカルサーバー上のWebブラウザーからHTTPS経由でWeb StudioおよびDirectorにアクセスできます。

ただし、別のマシンからHTTPS経由でWeb StudioまたはDirectorにアクセスしようとすると、ブラウザーは証明書を信頼しないため、セキュリティエラーを表示します。

> **注:**
>
> Web StudioなしでDirectorをインストールした場合、インストーラーは自己署名証明書を作成しません。

HTTPS経由で安全なアクセスを有効にする

Web Studioサーバー以外のマシンからHTTPS経由でWeb StudioまたはDirectorへのアクセスを許可するには、次の手順に従います。

1. 信頼された証明書を作成またはインポートする。
2. IISで証明書をポート443にバインドする。
3. (オプション) HTTP Strict Transport Security (HSTS) を有効にする。

4. Web Studioがプロキシとして構成されていない場合 (クライアントマシンがWeb StudioとDelivery Controllerの両方に接続する場合)、Delivery ControllerでTLSを有効にする。

> **注:**
>
> 自己署名証明書の使用は、各マシンで手動構成が必要なため推奨されません。詳細については、自己署名証明書を使用するを参照してください。

信頼された証明書を作成またはインポートする

サーバーに接続するマシンによって信頼されている、エンタープライズまたはパブリック認証局からの証明書を使用することをお勧めします。

詳細については、新しい証明書の作成 および 既存の証明書のインポート を参照してください。証明書の共通名またはサブジェクトの別名は、ユーザーがWeb StudioまたはDirectorに接続するために使用するFQDNと一致する必要があります。サーバーの前にロードバランサーが展開されている場合は、ロードバランサーのFQDNを使用してください。

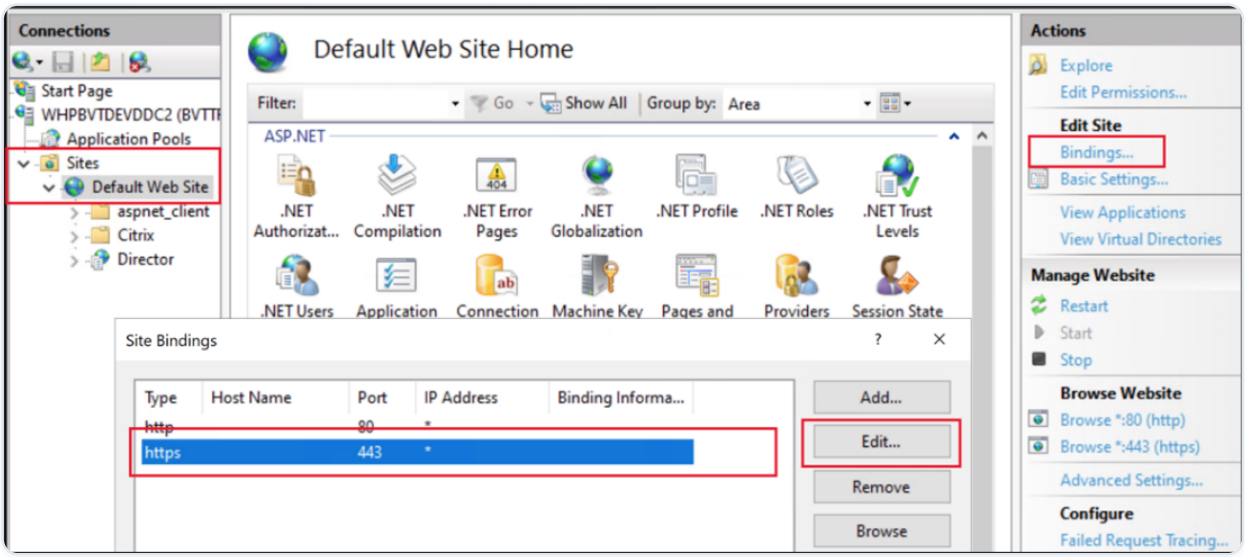
証明書をポート443にバインドする

信頼された証明書を作成またはインポートした後、IISでポート `443` にバインドします。これはインストール前でもインストール後でも実行できます。ポート `443` の証明書バインドがすでに構成されている場合、インストーラーは変更を行いません。

> **注:**
>
> デフォルトでは、Web StudioとDirectorはセキュアなHTTPSアクセスにポート443を使用します。必要に応じてポート番号を変更できます。詳細については、デフォルトのポート番号の変更 を参照してください。

> 証明書をポート `443` にバインドするには、次の手順に従います。

1. 管理者としてサーバーにログオンします。
2. IISマネージャーを開き、**サイト > 既定のWebサイト > バインド** に移動します。
3. 種類が **https** の既存のバインドがある場合は、それを選択して **編集...** をクリックします。**https** バインドがない場合は、**追加** をクリックします。



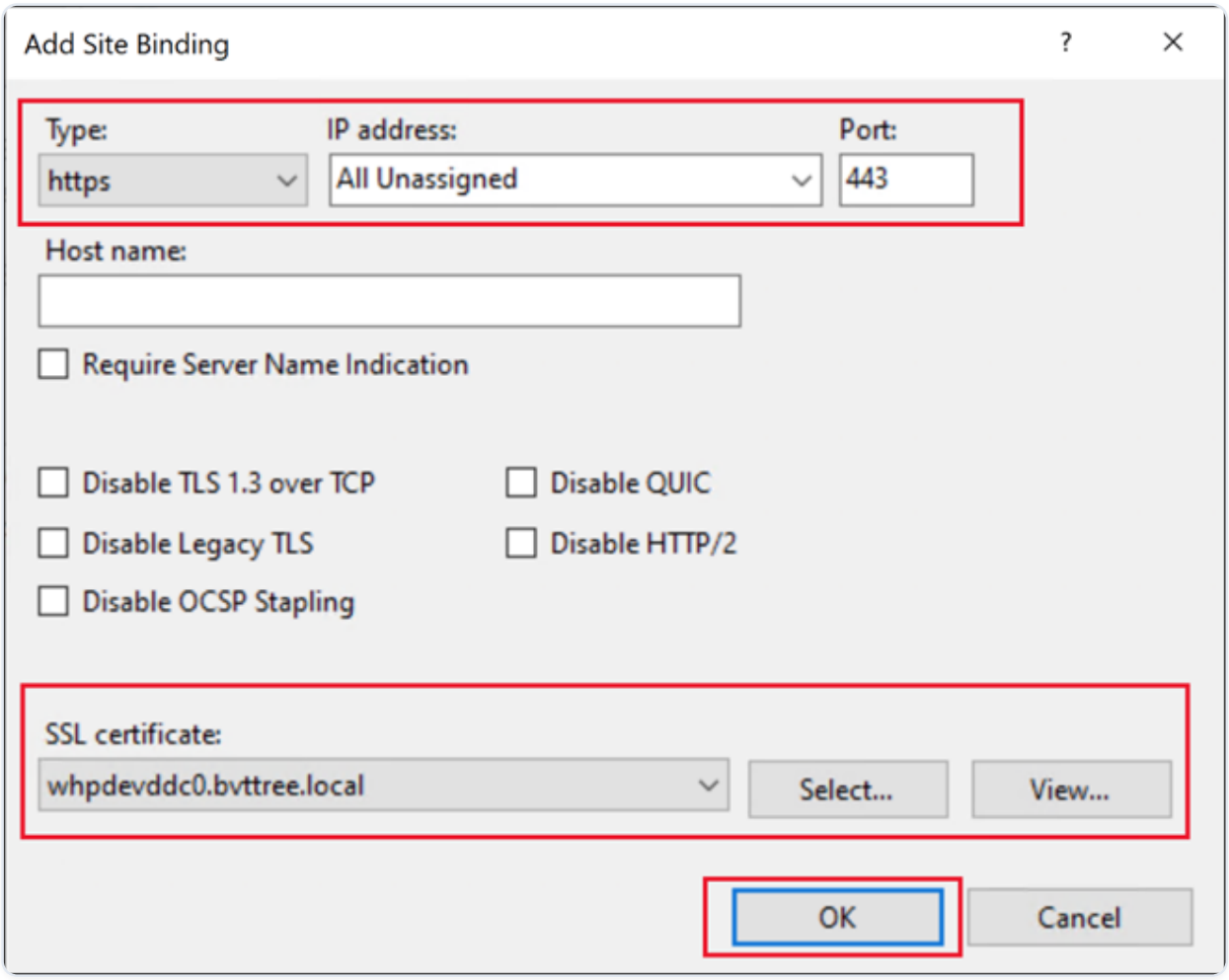
4. サイトバインドを作成または編集します。

   a. 新しいバインドの場合、種類を **https** に、ポートを `443` に設定します。

   b. 適切なSSL証明書を選択します。

   c. Windows Server 2022以降では、オプションで **レガシーTLSを無効にする** を選択して、ユーザーが最新のTLSバージョンのみを使用して接続できるようにします。

   d. **OK**をクリックします。



または、PowerShellを使用して証明書を変更することもできます。たとえば、次のスクリプトは、指定された共通名を持つ証明書を検索し、それをすべてのIPアドレス、ポート443にバインドし、レガシーTLSバージョンを無効にします。

```
$certSName = 'CN=whpdevddc0.bvttree.local'  # The subject name of the
certificate

$certificate = Get-ChildItem -Path Cert:\LocalMachine\My\ | ? {$_.Subject
-eq $certSName}

netsh http add sslcert ipport=0.0.0.0:443 certhash=$
($certificate.Thumbprint) certstorename=My appid="{91fe7386-e0c2-471b-
a252-1e0a805febac}" disablelegacytls=enable
```

なお、`appid` は、どのアプリケーションが証明書を追加したかを識別するために使用できる任意の GUID です。

自己署名証明書を使用する

既存の自己署名証明書を使用できますが、サーバーにアクセスする各マシンを手動で構成する必要があるため、推奨されません。

Web Studio に接続する必要があるマシンに自己署名証明書をインストールするには、次の手順を実行します。

1. Web Studio および Delivery Controller サーバーから既存の自己署名証明書を(/ja-jp/citrix-virtual-apps-desktops/current-release/secure/certificates.html#export-certificate-without-private-key)します。
2. サーバーにアクセスする必要があるマシンの **信頼されたルート証明書** ストアに証明書を(/ja-jp/citrix-virtual-apps-desktops/current-release/secure/certificates.html#import-existing-certificate)します。

(オプション) HTTP Strict Transport Security (HSTS) を有効にする

HTTP Strict Transport Security (HSTS) は、Web ブラウザーに対し、サイトへのアクセス時に HTTPS のみを使用するよう指示します。ユーザーが HTTP を使用して URL にアクセスしようとすると、ブラウザーは自動的に HTTPS に切り替わります。この設定により、クライアント側とサーバー側の両方で安全な接続検証が保証されます。ブラウザーは、構成された期間、この検証を維持します。

Windows Server 2019 以降では、IIS で HSTS を構成できます。

1. **インターネット インフォメーション サービス (IIS) マネージャー** を開きます。
2. **既定の Web サイト** (または適切な Web サイト) を選択します。
3. 右側の **操作** ペインで、**HSTS...** を選択します。
4. **有効にする** を選択し、最大有効期間を入力します (例: 1 年の場合は 31536000)。
5. **HTTP を HTTPS にリダイレクト** を選択します。

> **注:**
>
> Web Studio は、Studio Web サイトにアクセスする際に HTTP を HTTPS にリダイレクトする **URL 書き換え** ルールを自動的に構成します。ただし、このオプションは Director および IIS サイト上の他のすべてのアプリケーションにも適用されます。

6. **OK**をクリックします。

HSTS設定のスクリーンショット(/en-us/citrix-virtual-apps-desktops/current-release/media/iis-hsts.png)

(オプション) デフォルトのポート番号を変更する

デフォルトでは、Web StudioとDirectorはセキュアなHTTPSアクセスにポート443を使用します。このポート番号を変更するには、`Default Web Site`で目的のポートのサイトバインディングを作成するために、以下の手順に従ってください。

手順:

1. Web Studioをホストしているサーバーで、**インターネットインフォメーションサービス (IIS) マネージャー**を開きます。
2. **接続**ペインで、サーバーノードを展開し、**サイト**の下にある**既定のWebサイト**を選択します。
3. 右側の**操作**ペインで、**バインディング**をクリックします。
4. **サイトバインディング**ウィンドウで、**追加**をクリックします。
5. サイトバインディングの追加ウィンドウで、新しいバインディングに対して以下を設定します。
   a. **種類**: **https**を選択します。
   b. **IPアドレス**: 適切なIPアドレスを選択するか、該当する場合はすべて未割り当てのままにします。
   c. **ポート**: 目的のポート番号を入力します (例: 444)。
   d. **SSL証明書**: セキュアな通信のために適切なSSL証明書を選択します。

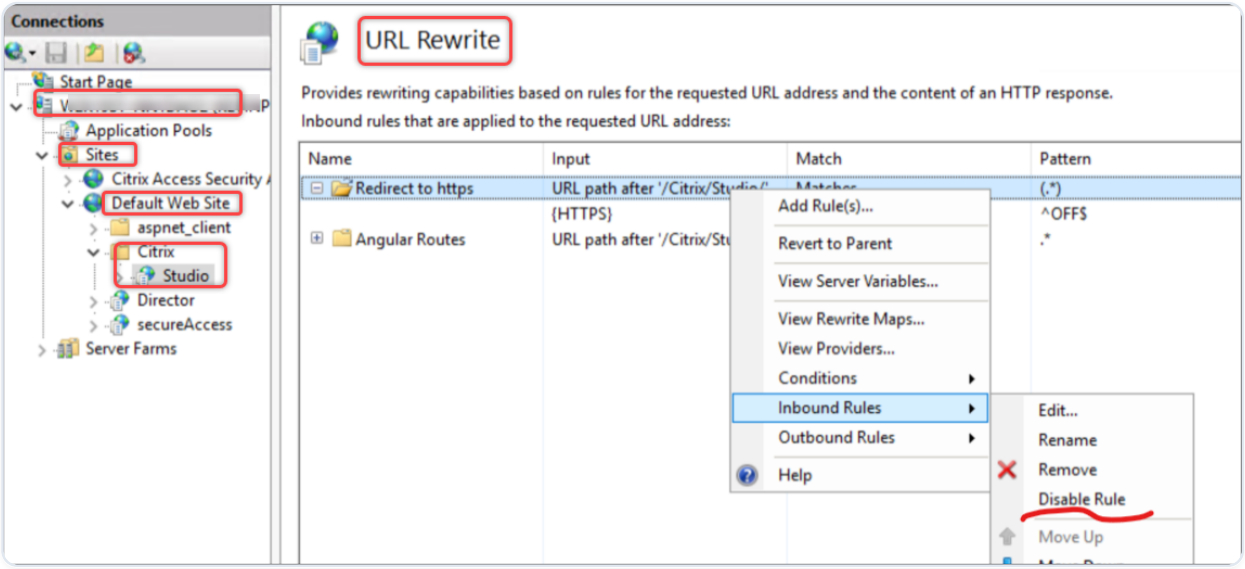
> **注:**
>
> Delivery Controller™とWeb Studioが別々のマシンにインストールされており、サーバーに他のサービスやWebサイトが展開されていない場合は、ポート443を削除できます。そうでない場合は、オーケストレーションサービスや他のFMAサービスとの通信問題を避けるために、このポートを維持してください。

6. 「**OK**」をクリックしてバインディングを保存し、「**サイトバインディング**」ウィンドウを閉じます。
7. **IIS マネージャー**で、サーバーノードをクリックし、**操作**ペインで「**再起動**」をクリックして新しいバインディングを適用します。

（オプション）HTTPS リダイレクトを無効にする

Web Studio をインストールすると、デフォルトで、すべての HTTP アクセスが HTTPS に自動的にリダイレクトされます。このリダイレクトを無効にして HTTP アクセスを許可することも可能です。この方法は、HTTP アクセスをブロックするための他の対策を講じている場合にのみ推奨されます。Web Studio の前に TLS 終端ロードバランサーがある場合でも、ロードバランサーと Web Studio の間で HTTPS を使用することをお勧めします。

1. Web Studio サーバーにログオンします。
2. **インターネットインフォメーションサービス (IIS) マネージャー**を開き、*Server_name* **> サイト > Default Web Site > URL Rewrite** に移動します。
3. 次のスクリーンショットに示すように、**https へのリダイレクト**の**受信規則**を無効にします。



IIS で HSTS を有効にしている場合は、**Redirect Http to Https** もクリアする必要があります。

VDAでTLS / DTLSを有効にする

Citrix Workspace™アプリとVirtual Delivery Agent (VDA) 間でTLS接続を有効にするには、次のタスクを完了します。

- VDAに証明書をインストールします。詳しくは、「証明書を要求してインストールする」を参照してください。
- VDAがインストールされているマシンでTLSを構成します。（便宜上、VDAがインストールされているマシンは、以降「VDA」と表記します）。Citrixが提供するPowerShellスクリプトを使用してTLS/DTLSを構成することを強くお勧めします。詳しくは、「PowerShellスクリプトを使用してVDAでTLSを構成する」を参照してください。ただし、TLS/DTLSを手動で構成する場合は、「VDAでTLSを手動で構成する」を参照してください。

- Studioで一連のPowerShellコマンドレットを実行して、VDAを含むデリバリーグループでTLSを構成します。詳細については、(#configure-tls-on-delivery-groups)を参照してください。

要件と考慮事項:

- コンポーネントをインストールし、サイトを作成し、マシンカタログを作成し、デリバリーグループを作成した後で、デリバリーグループとVDAでTLSを構成します。
- デリバリーグループでTLSを構成するには、Controllerのアクセスルールを変更する権限が必要です。フル管理者にはこの権限があります。
- VDAでTLSを構成するには、VDAがインストールされているマシンでWindows管理者である必要があります。
- Machine Creation Services™またはProvisioning ServicesによってプロビジョニングされたプールされたVDAでは、VDAマシンイメージは再起動時にリセットされ、以前のTLS設定が失われます。VDAが再起動されるたびにPowerShellスクリプトを実行して、TLS設定を再構成してください。

デリバリーグループには、TLS が構成されている VDA と TLS が構成されていない VDA を混在させることはできません。デリバリーグループの TLS を構成する前に、そのデリバリーグループ内のすべての VDA に対して TLS がすでに構成されていることを確認してください。

VDA で TLS を構成すると、インストールされている TLS 証明書のアクセス許可が変更され、ICA® Service に証明書の秘密キーへの読み取りアクセス権が付与され、ICA Service に次の情報が通知されます。

- TLSに使用する証明書ストア内の証明書。
- TLS接続に使用するTCPポート番号。

  Windows ファイアウォール（有効な場合）は、この TCP ポートでの受信接続を許可するように構成する必要があります。この構成は、PowerShell スクリプトを使用すると自動的に行われます。
- 許可するTLSプロトコルのバージョン。

> **重要:**
>
> Citrixでは、TLS 1.2以降の使用を推奨しています。SSLおよびそれ以前のバージョンのTLSは非推奨です。

> サポートされている TLS プロトコルバージョンは、階層（最低から最高）に従います: SSL 3.0、TLS 1.0、TLS 1.1、TLS 1.2、および TLS 1.3。許可される最小バージョンを指定します。そのバージョンまたはそれより高いバージョンを使用するすべてのプロトコル接続が許可されます。

たとえば、TLS 1.1を最小バージョンとして指定した場合、TLS 1.1、TLS 1.2、TLS 1.3プロトコル接続が許可されます。SSL 3.0を最小バージョンとして指定した場合、サポートされているすべてのバージョンの接続が許可されます。TLS 1.3を最小バージョンとして指定した場合、TLS 1.3接続のみが許可されます。

- 許可するTLS暗号スイート。

暗号スイートは、接続に使用される暗号化を選択します。クライアントとVDAは、異なる暗号スイートのセットをサポートできます。クライアント（Citrix Workspaceアプリ）が接続してサポートされているTLS暗号スイートのリストを送信すると、VDAはクライアントの暗号スイートの1つを、構成されている暗号スイートの独自のリスト内の暗号スイートの1つと照合し、接続を受け入れます。一致する暗号スイートがない場合、VDAは接続を拒否します。

VDAは、3つの暗号スイートセット（コンプライアンスモードとも呼ばれます）をサポートしています：GOV（政府）、COM（商用）、およびALL。許容される暗号スイートは、Windows FIPSモードにも依存します。Windows FIPSモードの詳細については、`<http://support.microsoft.com/kb/811833>`を参照してください。次の表に、各セットの暗号スイートを示します。

暗号スイート	すべて	COM	GOV	すべて	COM	GOV
FIPSモード	オフ	オフ	オフ	オン	オン	オン
TLS_AES_256_GCM_SHA384	X		X	X		X
TLS_AES_128_GCM_SHA256	X			X		X
TLS_ECDHE_RS	X		X	X		X

暗号スイート	すべて	COM	GOV	すべて	COM	GOV
A_WITH_AES_256_GCM_SHA384						
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	X		X	X		X
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	X	X		X	X	

注:

VDAはDHE暗号スイート（例：TLS_DHE_RSA_WITH_AES_256_GCM_SHA384、TLS_DHE_RSA_WITH_AES_256_CBC_SHA、TLS_DHE_RSA_WITH_AES_128_GCM_SHA256、TLS_DHE_RSA_WITH_AES_128_CBC_SHA）をサポートしていません。Windowsによって選択された場合、接続は失敗します。

NetScaler Gatewayを使用している場合は、バックエンド通信の暗号スイートサポートに関する情報について、NetScalerのドキュメントを参照してください。TLS暗号スイートのサポートについては、「Citrix ADCアプライアンスで利用可能な暗号」を参照してください。DTLS暗号スイートのサポートについては、「DTLS暗号のサポート」を参照してください。

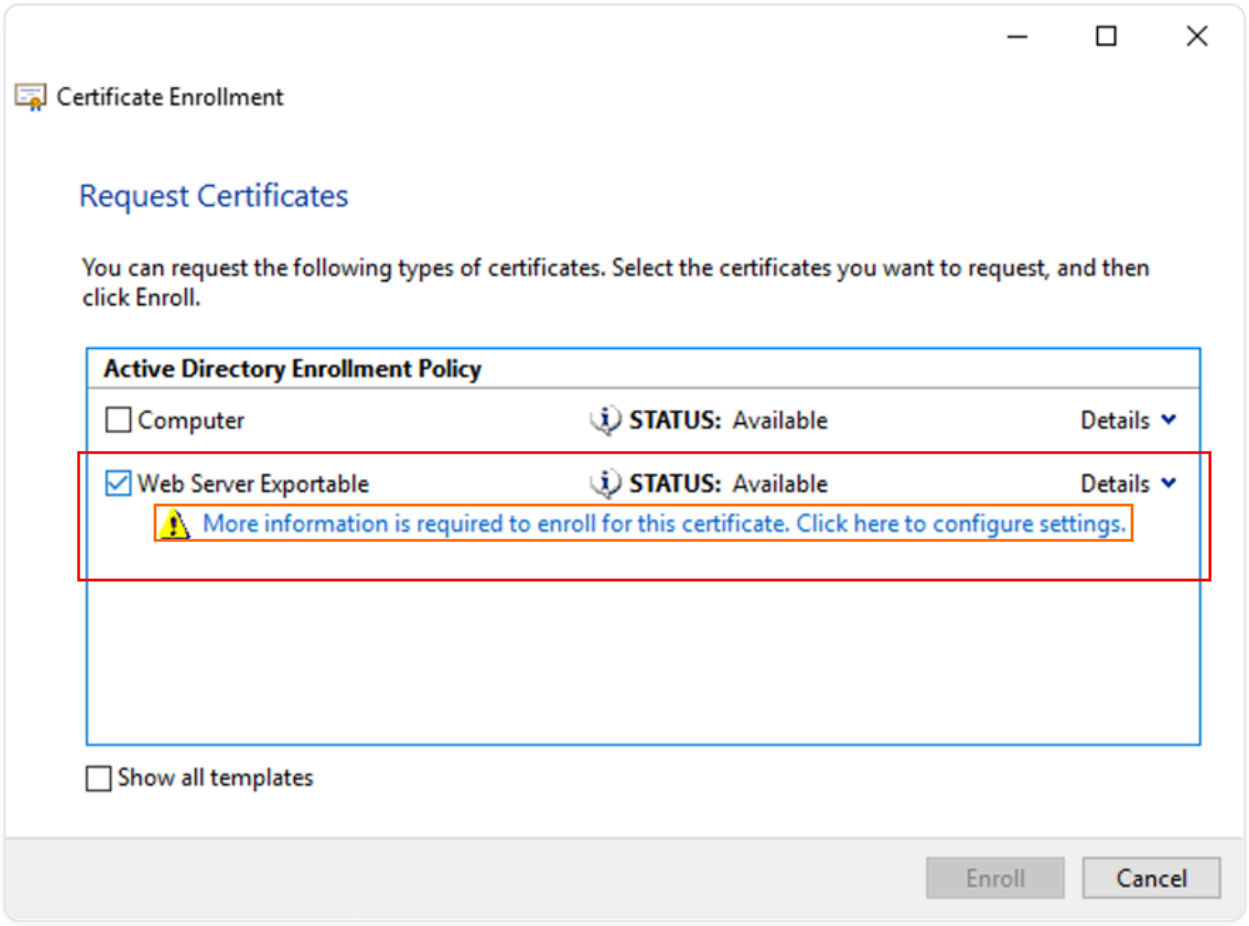
証明書の要求とインストール

TLSを使用するには、代替名にVDAのFQDNが含まれる証明書をインストールする必要があります。この証明書は、VDAに直接接続する（Citrix Gatewayを介さない）すべてのクライアントによって信頼されている必要があります。証明書を簡単に展開できない管理対象外のデバイスがVDAに接続できるようにするには、NetScaler® Gatewayの展開を検討してください。

Microsoft証明機関を使用して証明書を作成する

クライアントとVDAが信頼されたフォレストにあり、Microsoft証明機関がある場合、証明書MMCスナップインの証明書登録ウィザードから証明書を取得できます。

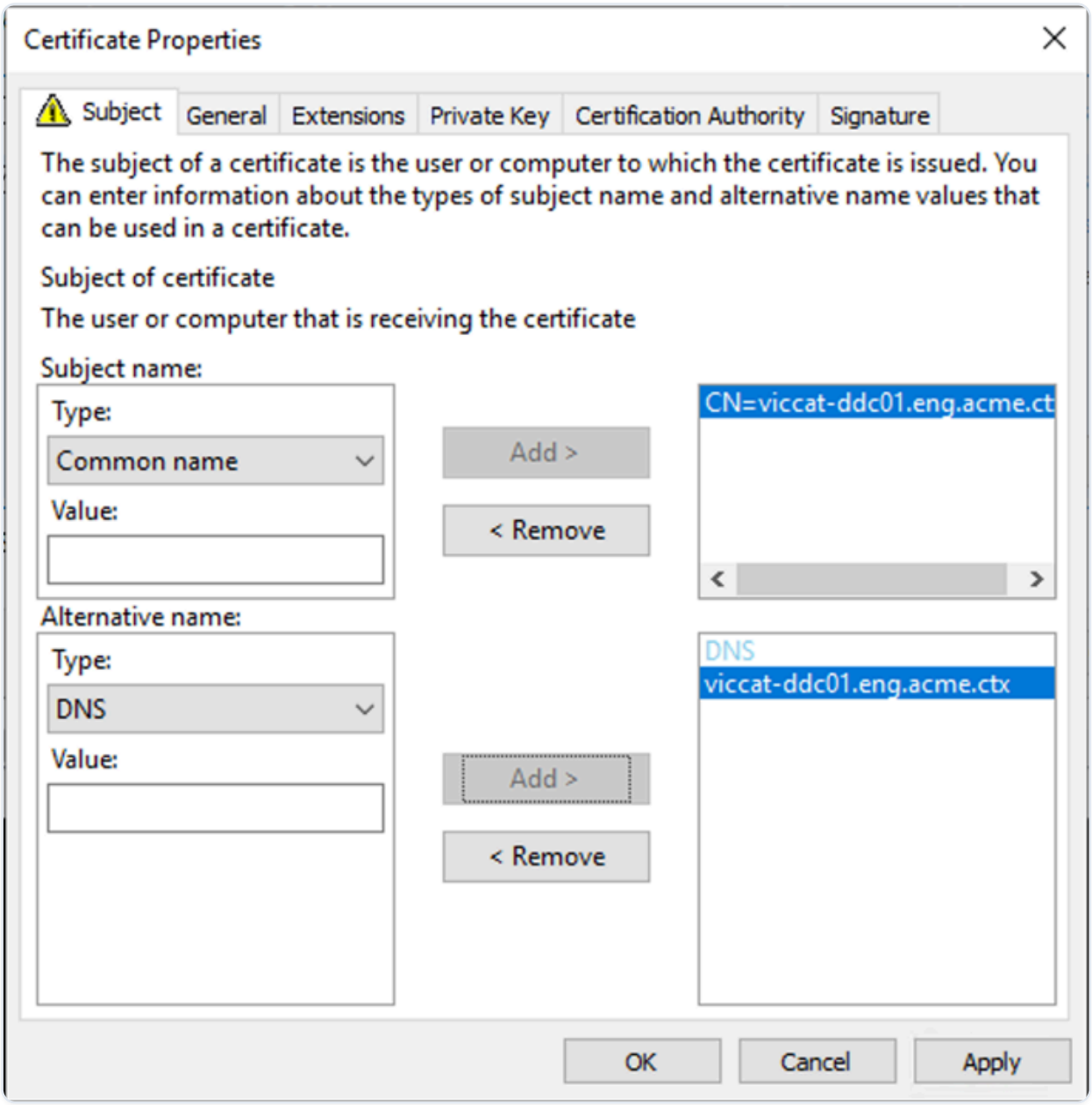
1. VDAで、MMCコンソールを開き、証明書スナップインを追加します。プロンプトが表示されたら、コンピューターアカウントを選択します。
2. **個人 > 証明書**を展開し、コンテキストメニューコマンド**すべてのタスク > 新しい証明書の要求**を使用します。
3. **次へ**をクリックして開始し、**次へ**をクリックして Active Directory 登録から証明書を取得することを確認します。
4. サーバー認証証明書のテンプレートを選択します。デフォルトの Windows **コンピューター** または **Web サーバー (エクスポート可能)** の両方を使用できます。テンプレートが Subject の値を自動的に提供するように設定されている場合は、詳細を指定せずに **登録** をクリックできます。



5. 証明書テンプレートの詳細を指定するには、**詳細** をクリックして以下を構成します。

   サブジェクト名 — タイプ **共通名** を選択し、VDA の FQDN を追加します。

   代替名 — タイプ **DNS** を選択し、VDA の FQDN を追加します。



注:

Active Directory証明書サービス証明書の自動登録を使用して、VDAへの証明書の発行と展開を自動化します。これについては、「証明書の自動登録を有効にする」で説明されています）。

ワイルドカード証明書を使用して、単一の証明書で複数の VDA を保護できます。

サブジェクト名 — タイプ **共通名** を選択し、VDA の *.primary.domain を入力します。

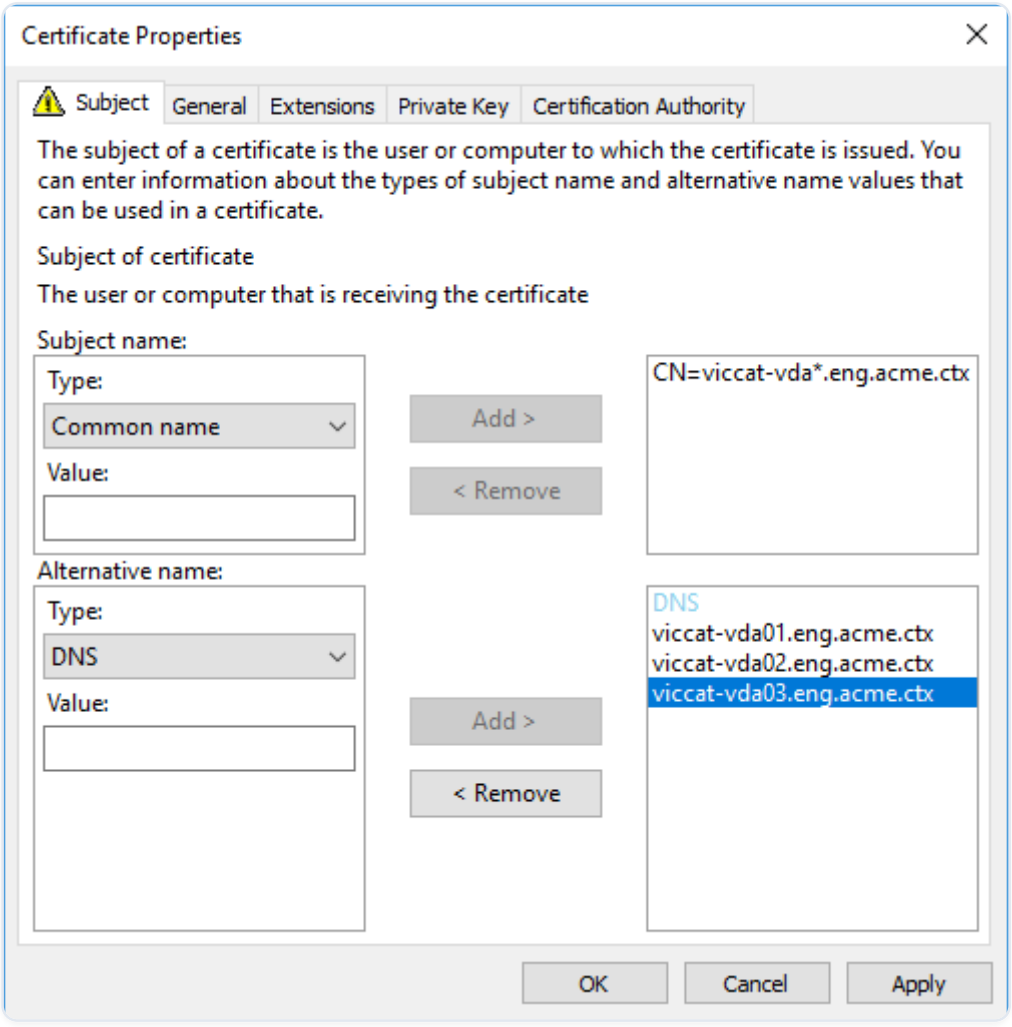
代替名 — タイプ **DNS** を選択し、VDA の *.primary.domain を追加します。

ワイルドカード証明書要求ダイアログ(/en-us/citrix-virtual-apps-desktops/current-release/media/tls-request-certificates-wildcard.png)

SAN 証明書を使用して、単一の証明書で複数の特定の VDA を保護できます。

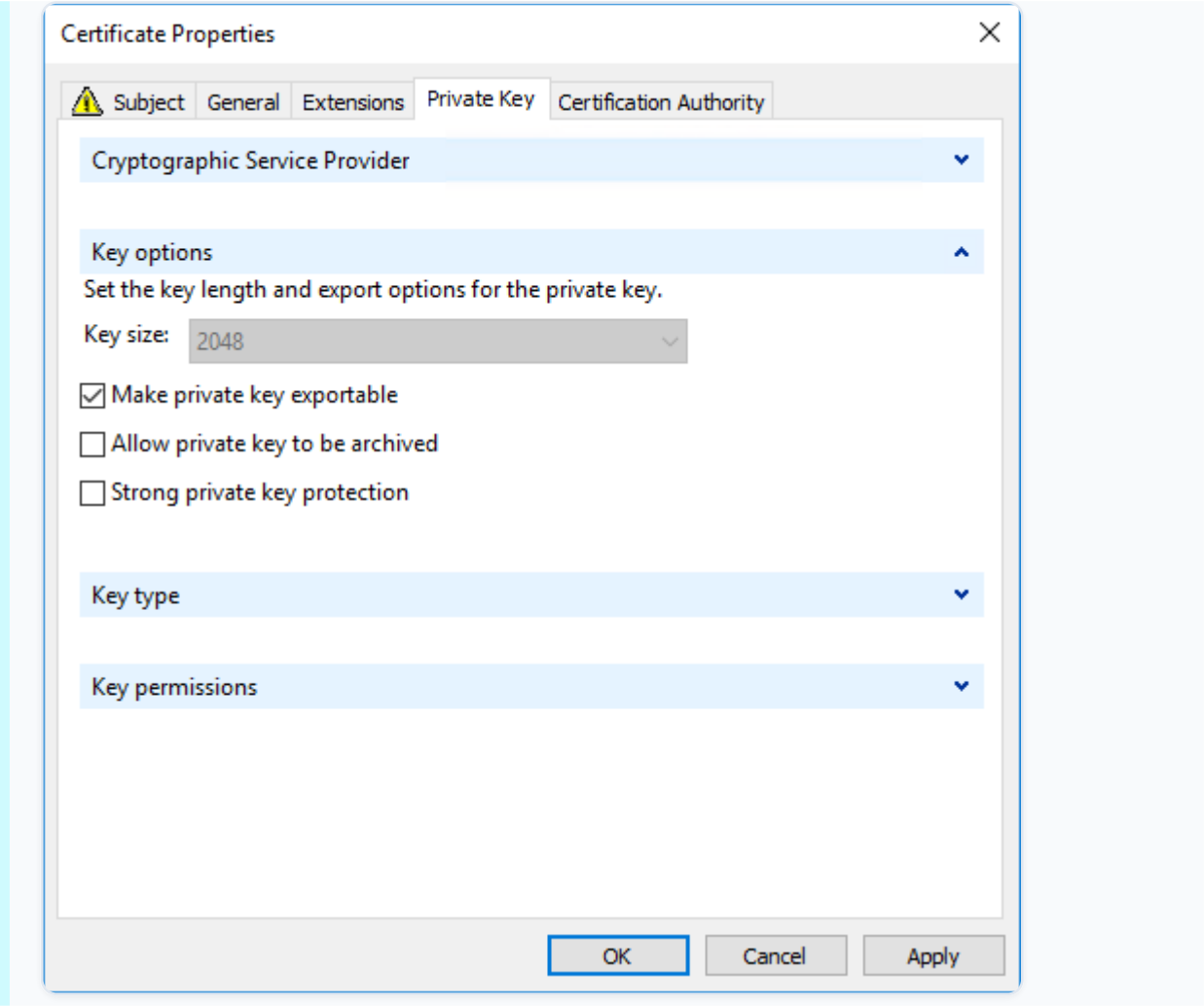
サブジェクト名 — タイプ **共通名** を選択し、証明書の使用状況を識別するのに役立つ文字列を入力します。

代替名 — タイプ **DNS** を選択し、各 VDA の FQDN のエントリを追加します。最適な TLS ネゴシエーションを確保するために、代替名の数を最小限に抑えてください。



注:

ワイルドカード証明書とSAN証明書の両方で、［秘密キー］タブの**［秘密キーをエクスポート可能にする］**が選択されている必要があります。



PowerShellスクリプトを使用してVDAでTLSを構成する

証明書ストアの［ローカルコンピューター］>［個人］>［証明書］領域にTLS証明書をインストールします。その場所に複数の証明書がある場合は、証明書のサムプリントをPowerShellスクリプトに指定します。

> **注:**
>
> XenAppおよびXenDesktop 7.15 LTSR以降、PowerShellスクリプトはVDAのFQDNに基づいて正しい証明書を検索します。VDAのFQDNに対して単一の証明書のみが存在する場合、サムプリントを指定する必要はありません。

Enable-VdaSSL.ps1スクリプトは、VDAでTLSリスナーを有効または無効にします。このスクリプトは、インストールメディアの*Support* > *Tools* > *SslSupport*フォルダーにあります。

TLSを有効にすると、DHE暗号スイートは無効になります。ECDHE暗号スイートは影響を受けません。

TLSを有効にすると、スクリプトは指定されたTCPポートの既存のWindowsファイアウォール規則をすべて無効にします。次に、ICAサービスがTLS TCPポートとUDPポートでのみ受信接続を受け入れることを許可する新しい規則を追加します。また、次のWindowsファイアウォール規則も無効にします。

- Citrix ICA（デフォルト：1494）
- Citrix CGP（デフォルト：2598）
- Citrix WebSocket（デフォルト：8008）

その結果、ユーザーはTLSまたはDTLSを使用してのみ接続できます。TLSまたはDTLSなしでは、ICA/HDX、セッションの信頼性を備えたICA/HDX、またはWebSocket経由のHDXを使用できません。

> **注:**
>
> DTLSは、UDPリアルタイムトランスポート経由のICA/HDXオーディオ、またはICA/HDX Framehawkではサポートされていません。
>
> 「ネットワークポート」を参照してください。(/ja-jp/tech-zone/build/tech-papers/citrix-communication-ports.html#citrix-virtual-apps-and-desktops).

スクリプトには以下の構文説明と追加の例が含まれています。この情報はNotepad++などのツールを使用して確認できます。

> **重要:**
>
> EnableまたはDisableパラメーターと、CertificateThumbPrintパラメーターを指定します。その他のパラメーターはオプションです。

構文

```
Enable-VdaSSL {-Enable | -Disable} -CertificateThumbPrint "<thumbprint>" [-SSLPort <port>] [-SSLMinVersion "<min-ssl-version>"] [-SSLCipherSuite"\<suite>"]
```

パラメーター	説明
有効	VDAにTLSリスナーをインストールして有効にします。このパラメーターまたはDisableパラメーターのいずれかが必要です。
無効	VDA上のTLSリスナーを無効にします。このパラメーターまたはEnableパラメーターのいずれかが必要です。このパラメーターを指定した場合、他のパラメーターは無効になります。
証明書サムプリント "<thumbprint>"	引用符で囲まれた、証明書ストア内のTLS証明書のサムプリント。スクリプトは指定されたサムプリントを使用して、使用する証明書を選択します。このパラメーターを省略すると、誤った証明書が選択されます。
SSLポート <port>	TLSポート。デフォルト: 443
SSL最小バージョン "<version>"	引用符で囲まれた最小TLSプロトコルバージョン。有効な値: `SSL_3.0`、`TLS_1.0` (デフォルト)、`TLS_1.1`、`TLS_1.2`、および `TLS_1.3`。`TLS_1.3`は、Windows 11またはWindows Server 2022以降が必要です。
SSL暗号スイート "<suite>"	TLS暗号スイート。引用符で囲みます。有効な値: "GOV"、"COM"、および "ALL" (デフォルト)。

例

次のスクリプトは、TLSプロトコルバージョン値をインストールして有効にします。サムプリント (この例では「12345678987654321」と表記) は、使用する証明書を選択するために使用されます。

```
Enable-VdaSSL -Enable -CertificateThumbPrint "12345678987654321"
```

次のスクリプトは、TLSリスナーをインストールして有効にし、TLSポート400、GOV暗号スイート、および最小TLS 1.2プロトコル値を指定します。サムプリント (この例では「12345678987654321」と表記) は、使用する証明書を選択するために使用されます。

```
Enable-VdaSSL -Enable

-CertificateThumbPrint "12345678987654321"

-SSLPort 400 -SSLMinVersion "TLS_1.2"

-SSLCipherSuite "All"
```

次のスクリプトは、VDA上のTLSリスナーを無効にします。

```
Enable-VdaSSL -Disable
```

VDAでTLSを手動で構成する

VDAでTLSを手動で構成する場合、各VDA上の適切なサービスに対して、TLS証明書の秘密キーへの一般的な読み取りアクセスを許可します。WindowsシングルセッションOS用VDAの場合はNT SERVICE\PorticaService、またはWindowsマルチセッションOS用VDAの場合はNT SERVICE\TermServiceです。VDAがインストールされているマシンで:

手順 1. Microsoft管理コンソール (MMC) を起動します。 > > mmc.exe。

手順 2. MMCに証明書スナップインを追加します。

1. > を選択します。
2. を選択し、 をクリックします。
3. 「このスナップインは常に次の証明書を管理します:」というプロンプトが表示されたら、「コンピューターアカウント」を選択し、 をクリックします。
4. 「このスナップインで管理するコンピューターを選択してください」というプロンプトが表示されたら、「ローカルコンピューター」を選択し、 をクリックします。

手順 3. > > で、証明書を右クリックし、 > を選択します。

手順 4. アクセス制御リストエディターに「(FriendlyName) の秘密キーのアクセス許可」が表示されます。ここで(FriendlyName)はTLS証明書の名前です。次のいずれかのサービスを追加し、読み取りアクセス権を付与します。

- WindowsシングルセッションOS用VDAの場合、「PORTICASERVICE」
- Windows Multi-session OS 用 VDA の場合、「TERMSERVICE」

手順 5. インストールされている TLS 証明書をダブルクリックします。証明書ダイアログで、 タブを選択し、一番下までスクロールします。 をクリックします。

手順 6. regedit を実行し、HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd に移動します。

1. SSL Thumbprint キーを編集し、TLS 証明書の拇印の値をこのバイナリ値にコピーします。 ダイアログボックスの不明な項目（「0000」や特殊文字など）は無視しても問題ありません。
2. SSLEnabled キーを編集し、DWORD 値を 1 に変更します。（後で SSL を無効にするには、DWORD 値を 0 に変更します。）
3. デフォルト設定を変更する場合（オプション）は、同じレジストリパスで以下を使用します。

   SSLPort DWORD – SSL ポート番号。デフォルト: 443。

   SSLMinVersion DWORD – 1 = SSL 3.0, 2 = TLS 1.0, 3 = TLS 1.1, 4 = TLS 1.2, 5 = TLS 1.3。デフォルト: 2 (TLS 1.0)。

   SSLCipherSuite DWORD – 1 = GOV、2 = COM、3 = ALL。デフォルト: 3 (ALL)。

手順 7. TLS の TCP および UDP ポートがデフォルトの 443 でない場合、Windows ファイアウォールで開いていることを確認します。（Windows ファイアウォールで受信規則を作成する際は、そのプロパティで「接続を許可する」と「有効」が選択されていることを確認してください。）

手順 8. 他のアプリケーションやサービス（IIS など）が TLS TCP ポートを使用していないことを確認します。

ステップ9. マルチセッションVDAの場合、変更を有効にするにはマシンを再起動します。(シングルセッションVDAマシンを再起動する必要はありません。)

ステップ10. 接続の問題を回避するために、VDAでサポートされている暗号スイートが最も高い優先順位を持つように、Windowsの暗号スイート設定を変更します。

> **重要:**

> 以下に概説するグループポリシーの変更は、システムを再起動した後にのみ有効になります。

> MCSまたはPVSでプロビジョニングされた非永続セッションホストを使用している場合は、これらの設定をマスターイメージに適用する必要があります。

オプション1:

グループポリシーエディターを使用して、 > > > > > に移動します。以下の暗号スイートがリストの最上位にあることを確認してください。

```
TLS_AES_256_GCM_SHA384_P384

TLS_AES_256_GCM_SHA384_P256

TLS_AES_128_GCM_SHA256_P384

TLS_AES_128_GCM_SHA256_P256

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
```

注:

TLS_AES_256_GCM_SHA384およびTLS_AES_128_GCM_SHA256は、Windows 11およびWindows Server 2022以降にのみ適用されます。古いオペレーティングシステムを使用している場合は、これらの暗号スイートをリストに含めないでください。

リストされている暗号スイートは、楕円曲線P384またはP256も指定しており、「curve25519」が選択されないようにします。FIPSモードは「curve25519」の使用を妨げません。

リストから暗号スイートを削除する必要はありません。これらの設定はシステム全体に適用されるため、暗号スイートを削除する場合は、セッションホストで実行されているアプリ

ケーションやサービスによってそれらが必要とされていないことを確認する必要があります。

オプション2:

グループポリシーエディターを使用して、 > > > > > に移動します。以下の暗号スイートがリストの最上位にあることを確認してください。

```
TLS_AES_256_GCM_SHA384

TLS_AES_128_GCM_SHA256

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
```

注:

TLS_AES_256_GCM_SHA384およびTLS_AES_128_GCM_SHA256は、Windows 11およびWindows Server 2022以降にのみ適用されます。古いオペレーティングシステムを使用している場合は、これらの暗号スイートをリストに含めないでください。

リストから暗号スイートを削除する必要はありません。これらの設定はシステム全体に適用されるため、暗号スイートを削除する場合は、セッションホストで実行されているアプリケーションやサービスによってそれらが必要とされていないことを確認する必要があります。

グループポリシーエディターを使用して、 > > > > > に移動します。設定を有効にし、リストに次の曲線を含めます。

```
NistP384

NistP256
```

> **注:**
>
> これにより、「curve25519」が選択されないようにします。FIPSモードは「curve25519」の使用を妨げません。

> VDAは、グループポリシーリストと、選択されたコンプライアンスモード（COM、GOV、またはALL）のリストの両方に表示される場合にのみ、暗号スイートを選択します。暗号スイートは、クライアント（Citrix Workspaceアプリ）から送信されたリストにも表示されている必要があります。

デリバリーグループでTLSを構成する

TLS接続用に構成したVDAを含む各デリバリーグループに対して、この手順を完了してください。

1. StudioからPowerShellコンソールを開きます。
2. **Get-BrokerAccessPolicyRule -DesktopGroupName '\<*delivery-group-name*>' \| Set-BrokerAccessPolicyRule -HdxSslEnabled $true** を実行します。
3. **Set-BrokerSite -DnsResolutionEnabled $true** を実行します。

自動登録を使用したプールされたVDAのSSL有効化

プールされたVDAを使用する場合、マスターイメージに証明書を追加すると、すべてのVDAが同じイメージを共有します。ワイルドカード証明書を使用できますが、欠点は、いずれかのVDAが侵害された場合、この強力な証明書により、すべてのVDAに属するHDX™接続が危険にさらされることです。

代わりに、より安全な代替策として、Microsoft Active Directory証明書サービスを活用して、グループポリシーを使用して証明書を自動的にプロビジョニングする方法があります。VDA上でスタートアップスクリプトを使用して、新しい証明書を動的にプロビジョニングし、VDAでSSLを有効にすることができます。

このアプローチは、シングルセッションのデスクトップVDAでのみ機能することに注意してください。マルチセッションVDAの場合、証明書が自動的にプロビジョニングされる前に、ブートプロセス中にICAリスナーが早すぎる段階で起動されます。

Active Directory証明書サービスは内部のエンタープライズ証明機関を使用するため、すべてのWindowsインストールによって自動的に信頼されるわけではありません。クライアントが企業によって管理され、ドメインフォレストの一部である場合、信頼されたCA証明書はグループポリシーを使用して自動的に配布できます。BYODやその他のドメインに参加していないデバイスの場

合、信頼されたCA証明書を他のメカニズム（ダウンロードリンクの提供など）でユーザーに配布するか、NetScaler Gatewayを使用する必要があります。

証明書の自動登録を有効にする

まず、VDAドメインフォレスト内のサーバーにActive Directory証明書サービスロールがインストールされており、エンタープライズCAが提供されていることを確認してください。そうでない場合、自動登録はできません。

VDAは起動ごとに証明書要求を送信するため、これによりエンタープライズCAに通常よりもかなり高い負荷がかかる可能性があることに注意してください。負荷に対処するためにCAサーバーに十分なCPUとメモリを割り当て、本番環境に移行する前に、常にラボ環境で展開のスケーラビリティをテストしてください。

グループポリシー管理エディターで、SSLが有効なプールされたVDAを含む組織単位に適用される新しいポリシーを次のように作成します。

1. コンピューターの構成 -> ポリシー -> Windowsの設定 -> セキュリティの設定 -> 公開キーのポリシー を展開します
2. 「証明書サービス クライアント – 自動登録ポリシー」オブジェクトのプロパティを編集します
3. 以下のスクリーンショットに示すように構成します。
4. 自動証明書要求コンテナを右クリックし、「新規 -> 自動証明書要求...」を選択します。
5. 自動証明書要求セットアップウィザードで、「次へ」をクリックします。
6. コンピューター証明書テンプレートが選択されていることを確認し、「次へ」をクリックします。
7. 「完了」をクリックします。

登録ポリシーのスクリーンショット (/en-us/citrix-virtual-apps-desktops/current-release/media/ssltask-autoenrollment-policy.png)

Windowsマスターイメージの準備

Enable-VdaSsl.ps1スクリプトを、製品インストールメディアの`Support\Tools\SslSupport`フォルダーからVDAマスターイメージにコピーします。HDX SSL接続に使用する証明書は、マスターイメージに含まれていない必要があります。証明書は、MCSまたはPVSマシンカタログが作成されるときにプロビジョニングされます。次に、次のように新しいスケジュールされたタスクを作成します（この時点ではスケジュールされたタスクを実行しないでください）。

1. タスクスケジューラを開きます。

2. **操作**ペインで、「**タスクの作成...**」を押します。
3. 「全般」タブで:

   - **名前**を入力します（例: `Enable VDA SSL`）。
   - 「**ユーザーまたはグループの変更...**」をクリックし、「ユーザーまたはグループの選択」ダイアログボックスで`SYSTEM`と入力して「**OK**」をクリックします。

   タスクの作成「操作」タブのスクリーンショット (/en-us/citrix-virtual-apps-desktops/current-release/media/ssltask-general.png)
4. 「トリガー」タブを選択します。
5. 「**新規...**」をクリックします。「**新しいトリガー**」ダイアログで:

   a. 「**タスクの開始**」を「**イベント時**」に設定します。
   b. 「**ログ**」を「**Microsoft-Windows-CertificateServicesClient-Lifecycle-System/Operational**」に設定します。
   c. 「**ソース**」を「**Microsoft-Windows-CertificateServicesClient-Lifecycle-System**」に設定します。
   d. 「**イベントID**」を`1006`に設定します。
   e. 「**OK**」をクリックしてトリガーを保存します。

   新しいトリガーウィンドウのスクリーンショット(/en-us/citrix-virtual-apps-desktops/current-release/media/ssltask-trigger.png)
6. 「**アクション**」タブを選択します。
7. 「**新規...**」をクリックします。
8. 「**新しいアクション**」ダイアログで:

   a. 「**アクション**」を「**プログラムの開始**」に設定します。
   b. 「プログラム/スクリプト」フィールドに`powershell.exe`を入力します。
   c. 「引数の追加」フィールドに、PowerShellスクリプトへのパスを含めて`-ExecutionPolicy RemoteSigned Enable-VdaSsl.ps1 -Enable -Confirm:$False`を入力します。
   d. 「**OK**」を押してアクションを保存します。

   新しいアクションウィンドウのスクリーンショット(/en-us/citrix-virtual-apps-desktops/current-release/media/ssltask-action.png)
9. 「**OK**」を押してタスクを保存します。

トラブルシューティング

接続エラーが発生した場合は、VDAのシステムイベントログを確認してください。

Windows版Citrix Workspaceアプリを使用しているときに、TLSエラーを示す接続エラーが発生した場合は、Desktop Viewerを無効にしてから、再度接続を試みてください。接続は引き続き失敗しますが、根本的なTLS問題の説明が提供される場合があります。（たとえば、証明機関から証明書を要求する際に誤ったテンプレートを指定したなど。）

HDX Adaptive Transport を使用するほとんどの構成は、Citrix Workspace app、Citrix Gateway、および VDA の最新バージョンを使用するものを含め、DTLS で正常に動作します。Citrix Workspace app と Citrix Gateway の間で DTLS を使用し、かつ Citrix Gateway と VDA の間で DTLS を使用する一部の構成では、追加のアクションが必要です。

次の場合、追加の操作が必要です。

- Citrix ReceiverのバージョンがHDX Adaptive TransportおよびDTLSをサポートしている場合：Receiver for Windows (4.7, 4.8, 4.9)、Receiver for Mac (12.5, 12.6, 12.7)、Receiver for iOS (7.2, 7.3.x) またはReceiver for Linux (13.7)

以下のいずれかに該当する場合も同様です。

- Citrix GatewayのバージョンはVDAへのDTLSをサポートしているが、VDAのバージョンはDTLSをサポートしていない（バージョン7.15以前）。
- VDAのバージョンはDTLSをサポートしている（バージョン7.16以降）が、Citrix GatewayのバージョンはVDAへのDTLSをサポートしていない。

Citrix Receiver™ からの接続が失敗するのを避けるには、次のいずれかを実行します。

- Citrix Receiverを、Receiver for Windowsバージョン4.10以降、Receiver for Mac 12.8以降、またはReceiver for iOSバージョン7.5以降に更新する。
- Citrix Gatewayを、VDAへのDTLSをサポートするバージョンに更新する。
- VDAをバージョン7.16以降に更新する。
- VDAでDTLSを無効にする。
- HDX Adaptive Transportを無効にする。

> **注:**

> Receiver for Linuxの適切なアップデートはまだ利用できません。Receiver for Android（バージョン3.12.3）は、Citrix Gateway経由のHDX Adaptive TransportおよびDTLSをサポートしていないため、影響を受けません。

> VDAでDTLSを無効にするには、VDAファイアウォール構成を変更してUDPポート443を無効にします。(/ja-jp/tech-zone/build/tech-papers/citrix-communication-ports.html#citrix-virtual-apps-and-desktops)を参照してください。

TLS と HTML5 ビデオリダイレクト、およびブラウザコンテンツリダイレクト

HTML5 ビデオリダイレクトとブラウザコンテンツリダイレクトを使用して、HTTPS Web サイトをリダイレクトできます。これらの Web サイトに挿入された JavaScript は、VDA で実行されている Citrix HDX HTML5 ビデオリダイレクトサービスへの TLS 接続を確立する必要があります。これを実現するために、HTML5 ビデオリダイレクトサービスは、VDA の証明書ストアに 2 つのカスタム証明書を生成します。サービスを停止すると、証明書は削除されます。

HTML5 ビデオリダイレクトポリシーは、デフォルトで無効になっています。

ブラウザコンテンツリダイレクトは、デフォルトで有効になっています。

HTML5 ビデオリダイレクトの詳細については、「マルチメディアポリシー設定」を参照してください。

Universal Print Server で TLS を有効にする

トランスポート層セキュリティ (TLS) プロトコルは、Virtual Delivery Agent (VDA) と Universal Print Server 間の TCP ベースの接続でサポートされています。

> **警告:**

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

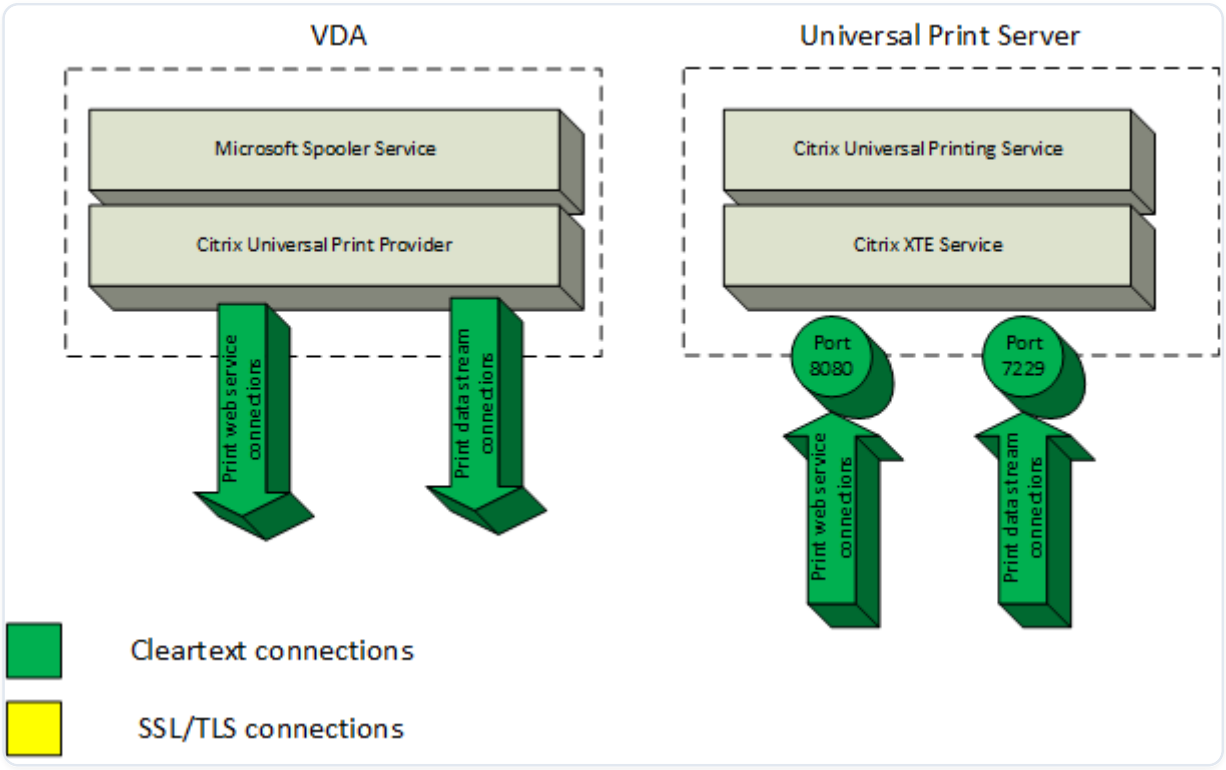
VDA と Universal Print Server 間の印刷接続の種類

クリアテキスト接続

印刷に関連する以下の接続は、VDA から発信され、Universal Print Server のポートに接続します。これらの接続は、**SSL enabled** ポリシー設定が **Disabled** (デフォルト) に設定されている場合にのみ行われます。

- クリアテキスト印刷 Web サービス接続 (TCP ポート 8080)
- クリアテキスト印刷データストリーム (CGP) 接続 (TCP ポート 7229)

Microsoft のサポート記事 Service overview and network port requirements for Windows には、Microsoft Windows Print Spooler サービスが使用するポートが記載されています。このドキュメントの SSL/TLS 設定は、Windows Print Spooler サービスによって行われる NetBIOS および RPC 接続には適用されません。**Universal Print Server enable** ポリシー設定が **Enabled with fallback to Windows' native remote printing** に設定されている場合、VDA は Windows Network Print Provider (win32spl.dll) をフォールバックとして使用します。

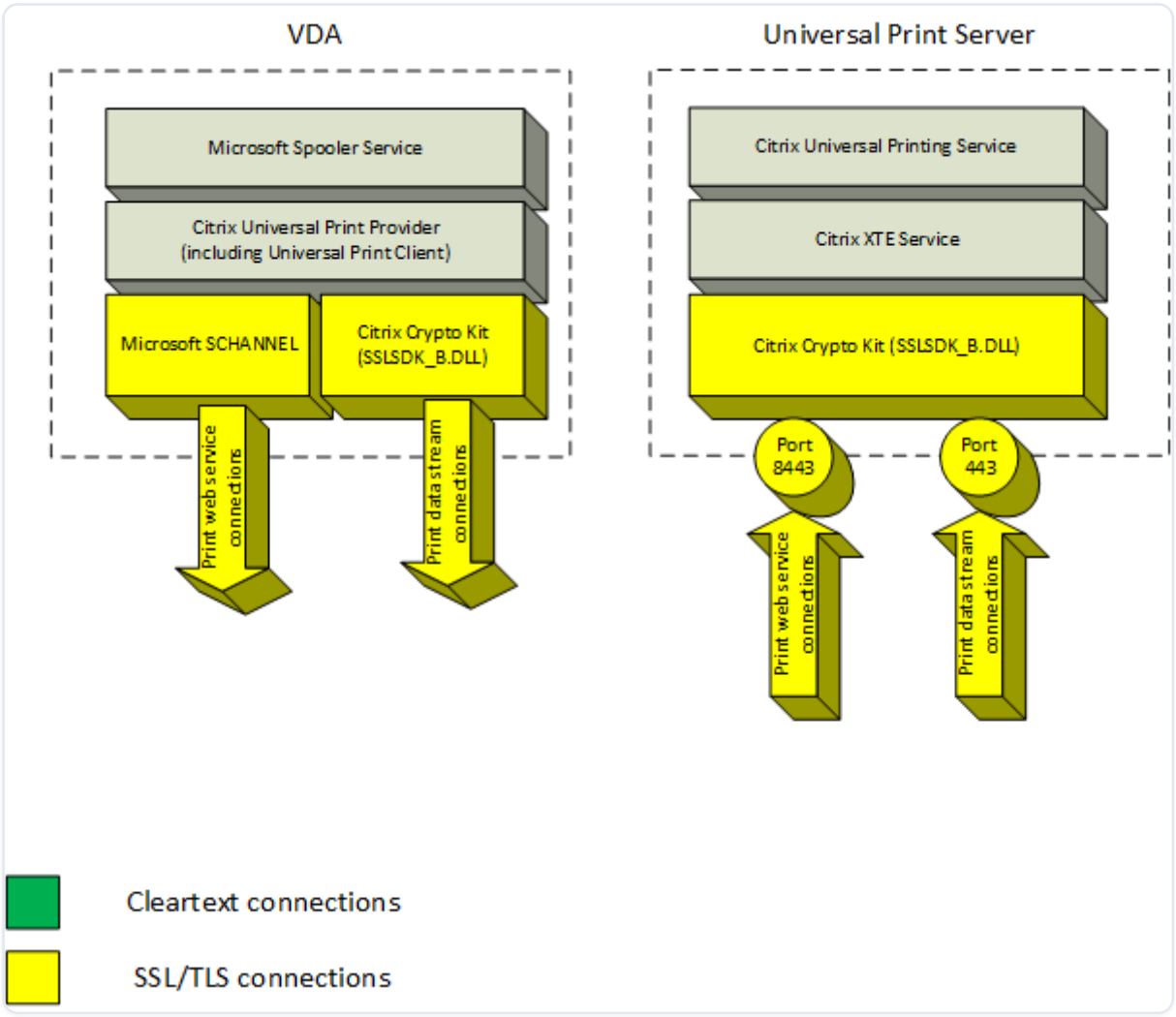


暗号化された接続

印刷に関連するこれらの SSL/TLS 接続は、VDA から発信され、Universal Print Server のポートに接続します。これらの接続は、**SSL enabled** ポリシー設定が **Enabled** に設定されている場合にのみ行われます。

- 暗号化された印刷 Web サービス接続 (TCP ポート 8443)

- 暗号化された印刷データストリーム (CGP) 接続 (TCP ポート 443)



SSL/TLS クライアント構成

VDA は SSL/TLS クライアントとして機能します。

Microsoft Group Policy とレジストリを使用して、暗号化された印刷 Web サービス接続 (TCP ポート 8443) 用の Microsoft SCHANNEL SSP を構成します。Microsoft サポート記事「TLS Registry Settings」には、Microsoft SCHANNEL SSP のレジストリ設定が記載されています。

VDA のグループポリシーエディターで、 **> > > >** に移動します。TLS 1.3 が設定されている場合は、次の順序を選択します。

TLS_AES_256_GCM_SHA384 TLS_AES_128_GCM_SHA256

TLS 1.2 が設定されている場合は、次の順序を選択します。

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256

> **注:**
>
> このグループポリシー設定が構成されている場合、VDA は、暗号化された印刷 Web サービス接続 (デフォルトポート: 8443) の暗号スイートを、接続が両方の SSL 暗号スイートリストに表示されている場合にのみ選択します。

- グループポリシー SSL 暗号スイート順序リスト
- 選択した SSL 暗号スイートポリシー設定 (COM、GOV、または ALL) に対応するリスト

> このグループポリシー構成は、VDA 上の他の TLS アプリケーションおよびサービスにも影響します。アプリケーションが特定の暗号スイートを必要とする場合は、このグループポリシー暗号スイート順序リストに追加する必要がある場合があります。

> **重要:**
>
> TLS 構成のグループポリシーの変更は、オペレーティングシステムの再起動後にのみ有効になります。

> Citrix ポリシーを使用して、暗号化された印刷データストリーム (CGP) 接続 (TCP ポート 443) の SSL/TLS 設定を構成します。

SSL/TLS サーバー構成

Universal Print Server は SSL/TLS サーバーとして機能します。

SSL/TLS設定を構成するには、`Enable-UpsSsl.ps1` PowerShellスクリプトを使用します。

Universal Print ServerにTLS証明書をインストールする

HTTPSの場合、VDAによって信頼されているSSLサーバー証明書をUniversal Print Serverにインストールする必要があります。Microsoft Active Directory証明書サービスまたは別の認証局を使用して、Universal Print Serverの証明書を要求します。

Microsoft Active Directory 証明書サービスを使用して証明書を登録または要求する際には、以下の点を考慮してください。

1. 証明書をローカルコンピューターの**個人**証明書ストアに配置します。
2. 証明書のサブジェクト識別名（Subject DN）の**共通名**属性を、Universal Print Serverの完全修飾ドメイン名（FQDN）に設定します。これは証明書テンプレートで指定します。
3. 証明書要求と秘密キーの生成に使用される暗号化サービスプロバイダー（CSP）を**Microsoft Enhanced RSA and AES Cryptographic Provider (Encryption)**に設定します。これは証明書テンプレートで指定します。
4. キーサイズを2048ビット以上に設定します。これは証明書テンプレートで指定します。

証明書の作成とインストールについて詳しくは、「証明書の管理」を参照してください。

Universal Print ServerでのSSLの構成

Universal Print Server上のXTEサービスは、着信接続をリッスンします。SSLが有効な場合、SSLサーバーとして機能します。着信接続には、印刷コマンドを含む印刷Webサービス接続と、印刷ジョブを含む印刷データストリーム接続の2種類があります。これらの接続でSSLを有効にできます。SSLは、これらの接続の機密性と整合性を保護します。デフォルトでは、SSLは無効になっています。

SSLの構成に使用されるPowerShellスクリプトは、インストールメディアにあり、ファイル名は次のとおりです: `\Support\Tools\SslSupport\Enable-UpsSsl.ps1.`.

Universal Print Serverでのリスニングポート番号の構成

XTEサービスのデフォルトポートは次のとおりです。

- クリアテキスト印刷Webサービス（HTTP）TCPポート: 8080
- クリアテキスト印刷データストリーム (CGP) TCPポート: 7229
- 暗号化された印刷Webサービス (HTTPS) TCPポート: 8443
- 暗号化された印刷データストリーム (CGP) TCPポート: 443

Universal Print Server の XTE サービスで使用されるポートを変更するには、管理者として PowerShell で次のコマンドを実行します (Enable-UpsSsl.ps1 PowerShell スクリプトの使用に関する注意点については、後のセクションを参照してください):

1. `Stop-Service CitrixXTEServer, UpSvc`
2. `Enable-UpsSsl.ps1 -Enable -HTTPSPort <port> -CGPSSLPort <port>` または `Enable-UpsSsl.ps1 -Disable -HTTPPort <port> -CGPPort <port>`

3. `Start-Service CitrixXTEServer`

ユニバーサル プリント サーバーの TLS 設定

負荷分散構成で複数の Universal Print Server を使用している場合は、すべての Universal Print Server で **TLS** 設定が一貫して構成されていることを確認してください。

Universal Print Server で TLS を構成すると、インストールされている TLS 証明書のアクセス許可が変更され、Universal Printing Service に証明書の秘密キーへの読み取りアクセス権が付与されます。また、Universal Printing Service に次の情報が通知されます。

- TLS に使用する証明書ストア内の証明書。
- TLS 接続に使用する TCP ポート番号。

Windows ファイアウォール (有効な場合) は、これらの TCP ポートでの受信接続を許可するように構成する必要があります。この構成は、Enable-UpsSsl.ps1 PowerShell スクリプトを使用すると自動的に行われます。

- 許可する TLS プロトコルのバージョン。

Universal Print Server は TLS プロトコルバージョン 1.3 および 1.2 をサポートしています。許可される最小バージョンを指定します。

デフォルトの TLS プロトコルバージョンは 1.2 です。

> **注:**
>
> TLS 1.1 および 1.0 は、Citrix Virtual Apps and Desktops バージョン 2311 以降ではサポートされなくなりました。

- 許可する TLS 暗号スイート。

暗号スイートは、接続に使用される暗号アルゴリズムを選択します。VDAとUniversal Print Serverは、異なる暗号スイートのセットをサポートできます。VDAが接続してサポートされているTLS暗号スイートのリストを送信すると、Universal Print Serverはクライアントの暗号スイートの1つを、自身の構成済み暗号スイートのリストにある暗号スイートの1つと照合し、接続を受け入れます。一致する暗号スイートがない場合、Universal Print Serverは接続を拒否します。

Universal Print Serverは、OPEN、FIPS、およびSP800-52ネイティブCrypto Kitモード用に、GOV（政府）、COM（商用）、およびALLと名付けられた次の暗号スイートのセットをサポートしています。許容される暗号スイートは、**SSL FIPSモード**ポリシー設定とWindows FIPSモードにも

依存します。Windows FIPSモードの詳細については、このMicrosoftサポート記事を参照してください。

暗号スイート（優先順位の降順）	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
TLS_ECDHE_RSA_AES256_GCM_SHA384	X		X	X		X	X		X
TLS_ECDHE_RSA_AES256_CBC_SHA384	X		X	X		X	X		X
TLS_ECDHE_RSA_AES256_C	X	X		X	X		X	X	

暗号スイート（優先順位の降順）	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
BC_SHA									

PowerShellスクリプトを使用してUniversal Print ServerでTLSを構成する

証明書ストアの**ローカルコンピューター > 個人 > 証明書**領域にTLS証明書をインストールします。その場所に複数の証明書がある場合は、証明書のサムプリントを`Enable-UpsSsl.ps1` PowerShellスクリプトに指定します。

> **注:**
>
> PowerShellスクリプトは、Universal Print ServerのFQDNに基づいて正しい証明書を検索します。Universal Print ServerのFQDNに対して証明書が1つしかない場合は、証明書のサムプリントを指定する必要はありません。

> `Enable-UpsSsl.ps1`スクリプトは、VDAからUniversal Print ServerへのTLS接続を有効または無効にします。このスクリプトは、インストールメディアの**Support > Tools > SslSupport**フォルダーにあります。

TLSを有効にすると、スクリプトはUniversal Print ServerのTCPポートに対する既存のWindowsファイアウォール規則をすべて無効にします。その後、XTEサービスがTLS TCPおよびUDPポートでのみ受信接続を受け入れることを許可する新しい規則を追加します。また、以下のWindowsファイアウォール規則も無効にします。

- クリアテキスト印刷Webサービス接続（デフォルト：8080）
- クリアテキスト印刷データストリーム（CGP）接続（デフォルト：7229）

その結果、VDAはTLSを使用している場合にのみこれらの接続を行うことができます。

> **注:**

TLSを有効にしても、VDAからUniversal Print ServerへのWindows Print Spooler RPC/SMB接続には影響しません。

重要:

最初のパラメーターとして**Enable**または**Disable**のいずれかを指定します。ローカルコンピューターの個人証明書ストアにUniversal Print ServerのFQDNを持つ証明書が1つしかない場合、CertificateThumbprintパラメーターはオプションです。その他のパラメーターもオプションです。

構文

```
Enable-UpsSSL.ps1 -Enable [-HTTPPort &lt;port&gt;] [-CGPPort &lt;port&gt;] [-HTTPSPort &lt;port&gt;] [-CGPSSLPort &lt;port&gt;] [-SSLMinVersion &lt;version&gt;] [-SSLCipherSuite &lt;name&gt;] [-CertificateThumbprint &lt;thumbprint&gt;] [-FIPSMode &lt;Boolean&gt;] [-ComplianceMode &lt;mode&gt;]

Enable-UpsSSL.ps1 -Disable [-HTTPPort &lt;portnum&gt;] [-CGPPort &lt;portnum&gt;]
```

パラメーター	説明
有効にする	XTEサーバーでSSL/TLSを有効にします。このパラメーターまたはDisableパラメーターのいずれかが必要です。
無効にする	XTEサーバーでSSL/TLSを無効にします。このパラメーターまたはEnableパラメーターのいずれかが必要です。
CertificateThumbprint `"<thumbprint>"`	ローカルコンピューターの個人証明書ストアにあるTLS証明書のサムプリント。引用符で囲まれています。スクリプトは、指定されたサムプリントを使用して、使用する証明書を選択します。
HTTPポート `<port>`	クリアテキスト印刷Webサービス (HTTP/SOAP) ポート。デフォルト: 8080

パラメーター	説明
CGPポート `<port>`	クリアテキスト印刷データストリーム (CGP) ポート。デフォルト: 7229
HTTPSポート `<port>`	暗号化された印刷Webサービス (HTTPS/SOAP) ポート。デフォルト: 8443
CGPSSLポート `<port>`	暗号化された印刷データストリーム (CGP) ポート。デフォルト: 443
SSLMinVersion `"<version>"`	最小TLSプロトコルバージョン。引用符で囲まれています。有効な値: 「TLS_1.2」および「TLS_1.3」。デフォルト: TLS_1.2。
SSLCipherSuite `"<name>"`	TLS暗号スイートパッケージの名前。引用符で囲まれています。有効な値: 「GOV」、「COM」、および「ALL」(デフォルト)。
FIPSモード `<Boolean>`	XTEサーバーでFIPS 140モードを有効または無効にします。有効な値: FIPS 140モードを有効にする場合は$true、FIPS 140モードを無効にする場合は$false。

例

次のスクリプトはTLSを有効にします。サムプリント（この例では「12345678987654321」として表されています）は、使用する証明書を選択するために使用されます。

```
Enable-UpsSsl.ps1 –Enable -CertificateThumbprint "12345678987654321"
```

次のスクリプトはTLSを無効にします。

```
Enable-UpsSsl.ps1 –Disable
```

FIPSモードの構成

米国連邦情報処理標準（FIPS）モードを有効にすると、Universal Print Serverの暗号化された接続にはFIPS 140準拠の暗号化のみが使用されるようになります。

クライアントでFIPSモードを構成する前に、サーバーでFIPSモードを構成してください。

Windows FIPSモードの有効化または無効化については、Microsoftのドキュメントサイトをご確認ください。

クライアントでのFIPSモードの有効化

Delivery Controller™でWeb Studioを実行し、**UPS FIPS Mode** Citrixポリシー設定を**Enabled**に設定します。Citrixポリシーを有効にします。

各VDAで以下を実行します。

1. Windows FIPSモードを有効にします。
2. VDAを再起動します。

サーバーでのFIPSモードの有効化

各Universal Print Serverで以下を実行します。

1. Windows FIPSモードを有効にします。
2. このPowerShellコマンドを管理者として実行します: `stop-service CitrixXTEServer, UpSvc`
3. `-Enable -FIPSMode $true` パラメーターを指定して、`Enable-UpsSsl.ps1` スクリプトを実行します。
4. Universal Print Serverを再起動します。

クライアントでのFIPSモードの無効化

Web Studioで、**UPS FIPS Mode** Citrixポリシー設定を**Disabled**に設定します。Citrixポリシーを有効にします。**UPS FIPS Mode** Citrixポリシー設定を削除することもできます。

各VDAで次の操作を行います:

1. Windows FIPSモードを無効にします。
2. VDAを再起動します。

サーバーでのFIPSモードの無効化

各Universal Print Serverで次の操作を行います:

1. Windows FIPSモードを無効にします。
2. このPowerShellコマンドを管理者として実行します: `stop-service CitrixXTEServer, UpSvc`
3. `-Enable -FIPSMode $false` パラメーターを指定して、`Enable-UpsSsl.ps1` スクリプトを実行します。
4. Universal Print Serverを再起動します。

> **注:**
>
> SSLプロトコルバージョンがTLS 1.3に設定されている場合、FIPSモードはサポートされません。

SSL/TLSプロトコルバージョンの構成

デフォルトのSSL/TLSプロトコルバージョンはTLS 1.2です。TLS 1.2とTLS 1.3は、運用環境での使用が推奨されるSSL/TLSプロトコルバージョンです。トラブルシューティングのために、非運用環境で一時的にSSL/TLSプロトコルバージョンを変更する必要がある場合があります。

Universal Print Serverでは、SSL 2.0およびSSL 3.0はサポートされていません。

サーバーでのSSL/TLSプロトコルバージョンの設定

各Universal Print Serverで、次の手順を実行します。

1. 管理者としてこのPowerShellコマンドを実行します: `stop-service CitrixXTEServer, UpSvc`
2. `-Enable -SSLMinVersion` バージョンパラメーターを指定して、`Enable-UpsSsl.ps1` スクリプトを実行します。テストが完了したら、これをTLS 1.2またはTLS 1.3に戻すことを忘れないでください。
3. Universal Print Serverを再起動します。

クライアントでのSSL/TLSプロトコルバージョンの設定

Studioで、**SSLプロトコルバージョン**ポリシー設定を目的のプロトコルバージョンに設定し、ポリシーを有効にします。

VDAのオペレーティングシステムが選択したTLSバージョンをサポートしていることを確認してください。Windowsでサポートされているバージョンについては、「Microsoft Learn - TLS protocol version support」を参照してください。デフォルトを上書きするようにレジストリを構成するには、「Microsoft Learn - TLS, DTLS, and SSL protocol version settings」を参照してください。

トラブルシューティング

接続エラーが発生した場合は、Universal Print Server上のC:\Program Files (x86)\Citrix\XTE\logs\error.logファイルを確認してください。

SSL/TLSハンドシェイクが失敗した場合、このログファイルにエラーメッセージ**SSL handshake from client failed**が表示されます。このような失敗は、VDAとUniversal Print ServerのSSL/TLSプロトコルバージョンが一致しない場合に発生する可能性があります。

Universal Print Serverのホスト名を含む以下のポリシー設定で、Universal Print ServerのFQDNを使用します。

- セッションプリンター
- プリンターの割り当て
- 負荷分散用のUniversal Print Server

Universal Print ServerとVDAでシステムクロック（日付、時刻、タイムゾーン）が正しいことを確認してください。

仮想チャネル許可リスト

仮想チャネル許可リストは、Citrix以外の仮想チャネルのうち、どのチャネルを環境で許可するかを制御できる機能です。デフォルトでは、仮想チャネル許可リスト機能は有効になっています。その結果、Citrix Virtual Apps and Desktops™セッションでは、Citrix仮想チャネルのみが開くことが許可されます。自社製またはサードパーティ製のカスタム仮想チャネルを使用する必要がある場合は、それらを明示的に許可リストに追加する必要があります。

構成

仮想チャネル許可リストはデフォルトで有効になっています。この機能は、Citrixポリシーの以下の設定を使用して構成できます。

- **仮想チャネル許可リスト**: この機能を有効または無効にし、仮想チャネルをリストに追加します。
- **仮想チャネル許可リストログのスロットリング**: 仮想チャネル許可リストのイベントログのスロットリング期間を設定します。
- **仮想チャネル許可リストのログ記録**: 仮想チャネル許可リストのログレベルを設定します。

仮想チャネルを許可リストに追加する

仮想チャネルを許可リストに追加するには、以下の情報が必要です。

1. コードで定義されている仮想チャネル名。最大7文字です。例: `CTXCVC1`。
2. VDAマシン上で仮想チャネルを開くプロセスのパス。例: `C:\Program Files\Application\run.exe`。

必要な情報が揃ったら、仮想チャネル許可リストポリシー設定を使用して、仮想チャネルを許可リストに追加する必要があります。リストに仮想チャネルを追加するには、仮想チャネル名の後にコンマ、そして仮想チャネルにアクセスするプロセスのパスを入力します。複数のプロセスがある場合は、各プロセスをコンマで区切って追加できます。

単一プロセスの場合

前の例を使用して、以下のエントリをリストに追加します。

```
CTXCVC1,C:\Program Files\Application\run.exe
```

複数のプロセスの場合

複数のプロセスがある場合は、次のエントリをリストに追加します。

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application\run2.exe
```

ワイルドカードの使用

ワイルドカード (*) の使用がサポートされています。アプリケーションのバージョンに基づいてディレクトリ名または実行可能ファイル名が変更される場合、またはサードパーティコンポーネントがユーザープロファイルにインストールされている場合に、ワイルドカードを使用できます。

次のシナリオでワイルドカードを使用できます。

- 完全なディレクトリ名を置き換える場合。 例: `C:\Program Files\Application*\run1.exe`
- ディレクトリ名の一部を置き換える場合。 例: `C:\Program Files\Application\v*\run1.exe`
- 実行可能ファイル名を置き換える場合。 例: `C:\Program Files\Application\v1.2*.exe`
- 実行可能ファイル名の一部を置き換える場合。 例: `C:\Program Files\Application\v1.2\run*.exe`

次の制限が適用されます。

- ワイルドカードは、単一のディレクトリを置き換えるためにのみ使用できます。たとえば、実行可能ファイルが `C:\Program Files\Application\v1.2\run1.exe` にある場合
  - 許可: `C:\Program Files\Application*\run1.exe`
  - 不許可: `C:\Program Files*\run1.exe`

- エントリにはファイル名拡張子を含める必要があります。
  - 許可: `C:\Program Files\Application\v1.2*.exe`
  - 不許可: `C:\Program Files\Application\v1.2*`
- すべてのパスはローカルである必要があります。

注:

- ネットワークパスは許可されていません。
- ワイルドカードサポートは、Citrix Virtual Apps and Desktops™ 2206から利用可能です。
- ワイルドカードのサポートは、Citrix Virtual Apps and Desktops 2203 LTSRのCU2から利用可能です。

システム環境変数の使用

許可リスト内の信頼されたプロセスの定義を簡素化するために、システム環境変数を使用できます。`%programfiles%`、`%programfiles(x86)%`、`%systemdrive%`、`%systemroot%`などの標準変数を使用できます。

システムレベルで定義されている限り、カスタム環境変数も使用できます。

以下の例は、標準の環境変数を示しています。

- `%programfiles%\Application\v1.2\run.exe`
- `%programfiles%\Application*\run.exe`
- `%programfiles(x86)%\Application\v1.*\run.exe`

以下の例は、カスタムシステム環境変数を示しています。

- カスタム変数名: `app`
- カスタム変数値: `%programfiles%\Application\`
- 許可リストエントリ: `CTXCVC1,%app%\run.exe`

注:

> ユーザー環境変数はサポートされていません。

> 環境変数のサポートは、Citrix Virtual Apps and Desktopsバージョン2209以降で利用可能です。

仮想チャネル名とプロセスを取得する

VDAマシン上で仮想チャネル名とそれを開くプロセスを取得する最も簡単な方法は、仮想チャネルを提供した開発者またはサードパーティベンダーから情報を入手することです。

または、機能のログを適用し、以下の手順に従って情報を取得することもできます。

1. カスタム仮想チャネルのクライアントおよびサーバーコンポーネントが配置されたら、仮想アプリケーションまたは仮想デスクトップを起動します。
2. VDAマシンのシステムイベントログで、カスタム仮想チャネルの名前と、それを開こうとしたプロセスを探します。利用可能なイベントの詳細については、「イベントログ」を参照してください。
3. セッションからログアウトします。
4. 識別された仮想チャネルとプロセスに対して、仮想チャネル許可リストポリシー設定にエントリを追加します。
5. マシンを再起動します。
6. VDAが登録されたら、仮想アプリケーションまたは仮想デスクトップを実行して、カスタム仮想チャネルが正常に開くことを検証します。

Citrix仮想チャネルに関する考慮事項

すべての組み込みCitrix仮想チャネルは信頼されており、追加設定なしで開くことができます。ただし、以下の2つの機能は、外部依存関係のため、許可リストに明示的なエントリが必要です。

- マルチメディアリダイレクト
- スカイプ フォー ビジネス 用 HDX RealTime Optimization Pack

マルチメディアリダイレクト

Windows Media Player以外のメディアプレーヤーをシステムメディアプレーヤーとして使用する場合、それを信頼されたプロセスとして許可リストに追加する必要があります。許可リストのエントリには、以下の情報が必要です。

- 仮想チャネル名: `CTXMM`

- プロセス: VDAマシンで使用されるメディアプレーヤーへのパス。例: `C:\Program Files (x86)\Windows Media Player\wmplayer.exe`。
- 許可リストエントリ: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

スカイプ フォー ビジネス 用 HDX RealTime Optimization Pack

許可リストのエントリには、以下の情報が必要です。

- 仮想チャネル名: `CTXRMEP`
- プロセス: VDAマシン内のSkype for Business実行可能ファイルへのパス。これはSkype for Businessのバージョンやカスタムインストールパスの使用によって異なる場合があります。例: `C:\Program Files\Microsoft Office\root\Office16\lync.exe.`.
- 許可リストエントリ: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

VDA と Delivery Controller™ 間の WebSocket 通信

この記事では、WCF 通信の代替として、VDA と Delivery Controller 間の通信に WebSocket 接続を設定する方法について説明します。これにより、VDA から Delivery Controller への通信に TLS ポート 443 のみが使用できるという利点があります。

動作の仕組み

以下のセクションでは、Delivery ControllerとVDA間のWebSocket通信のワークフローについて説明します。

通常のブローカー処理操作中

1. Citrix Virtual Apps and Desktops™管理者は、Machine Creation Service (MCS)を使用してVDAをプロビジョニングすることでプロセスを開始します。
2. MCSプロビジョニングプロセス中に、MCSは各VDAの公開鍵と秘密鍵のペアを生成し、Delivery Controller上のFMAトラストサービスに公開鍵を登録します。MCSは、公開鍵と秘密鍵のペアをVDAのIDディスク下のファイルとして保存します。
3. VDAマシンが起動すると、VDAマシンにインストールされているMCSエージェントは、IDディスクからキーペアを読み取り、この情報をVDAレジストリの場所に書き込みます。
4. VDA にインストールされているブローカーエージェントは、レジストリからキーペアを読み取り、秘密鍵で署名されたサービスキーを使用して、SSL 対応の WebSocket リクエストを Delivery Controller に生成します。

5. Delivery Controller は、FMA 信頼サービスからの公開鍵を使用して、署名されたサービスキー認証ヘッダーを検証します。
6. 検証が完了すると、システムはVDAとDelivery Controller間のWebSocket接続を確立します。

LHCモードがアクティブになるとき

LHCのWebsocketサポートを有効にすると、LHCモード中に、VDAがHigh Availability ServiceとのWebsocket接続を確立しようとすると、High Availability Serviceは、署名されたサービスキー認証ヘッダーをローカルデータベースからの公開鍵で検証します。これにより、Websocket接続が認証され、LHCモードでもVDAとDelivery Controller間のWebSocket接続が成功します。

WebSocket のサポート

始める前に

1. サイトを構成します。詳しくは、「サイトの作成」を参照してください。
2. Delivery Controller に TLS 証明書をインストールします。詳しくは、「Controller への TLS サーバー証明書のインストール」を参照してください。
3. Delivery Controller を信頼するために、VDA にルートCAと中間CAをインストールします。

手順

WebSocket 接続を設定するには、次の手順に従います。

1. Delivery ControllerでWebSocket接続を有効にします。サイト上の各Delivery Controllerで次のコマンドを実行します。

   `New-ItemProperty "HKLM:\SOFTWARE\Citrix\DesktopServer\WorkerProxy" -Name "WebSocket_Enabled" -PropertyType "DWord" -Value 1 -Force`

2. WebSocketを有効にした後、Broker Serviceを再起動します。
3. LHCモードでWebSocketサポートを有効にします。サイト上の各Delivery Controllerで次のコマンドを実行します。

   ```
   New-ItemProperty "HKLM:\SOFTWARE\Citrix\DesktopServer\LHC" -Name "WebSocketEnabledLhc" -PropertyType "DWord" -Value 1 -Force
   ```

4. MCSプロビジョニングを使用して、AD参加済みVDA用のマシンカタログを作成します。詳細については、マシンカタログの作成を参照してください。
5. デリバリーグループを作成し、VDAを追加します。詳細については、デリバリーグループの作成を参照してください。

6. VDAでWebSocket接続を有効にします。VDAで次のPowerShellコマンドを実行します。

```
New-ItemProperty
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CitrixBrokerAgent
\WebSocket" -Name "Enabled" -PropertyType "DWord" -Value 1 -Force
```

- WebSocketが有効になっているか確認するには、次のレジストリキーの値を確認します。`Enabled`の値は1である必要があります。

  キー:

  ```
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CitrixBrokerAge
  nt\WebSocket
  ```

  名前: Enabled

  種類: REG_DWORD

  値: 1

HDX™ 接続性

Citrix HDXは、あらゆるデバイスおよびあらゆるネットワーク上で、集中型アプリケーションおよびデスクトップのユーザーに高精細なエクスペリエンスを提供する幅広いテクノロジーのセットを表しています。

HDXは、次の3つの技術原則に基づいて設計されています。

- インテリジェントなリダイレクト
- 適応型圧縮
- データ重複排除

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

HDXの提供機能内で、独自のプロプライエタリなトランスポートプロトコルを介して接続し、セッション確立時に最大伝送ユニットを利用し、Citrix SD-WANで接続を最適化できます。

アダプティブトランスポート

アダプティブトランスポートは、Citrix Virtual Apps and Desktops™のメカニズムであり、優先トランスポートプロトコルを使用してHDXセッションの接続を確立し、優先プロトコルでの接続が利用できない場合はTCPへのフォールバックを提供します。

次のトランスポートプロトコルがサポートされています。

- エンライトンド データ トランスポート (EDT)
- 伝送制御プロトコル (TCP)

構成

アダプティブトランスポートはデフォルトで有効になっています。アダプティブトランスポートは、次のモードで動作するように構成できます。

- **優先**: (デフォルト) クライアントは優先プロトコルで接続を試行し、優先プロトコルでの接続が利用できない場合はTCPにフォールバックします。

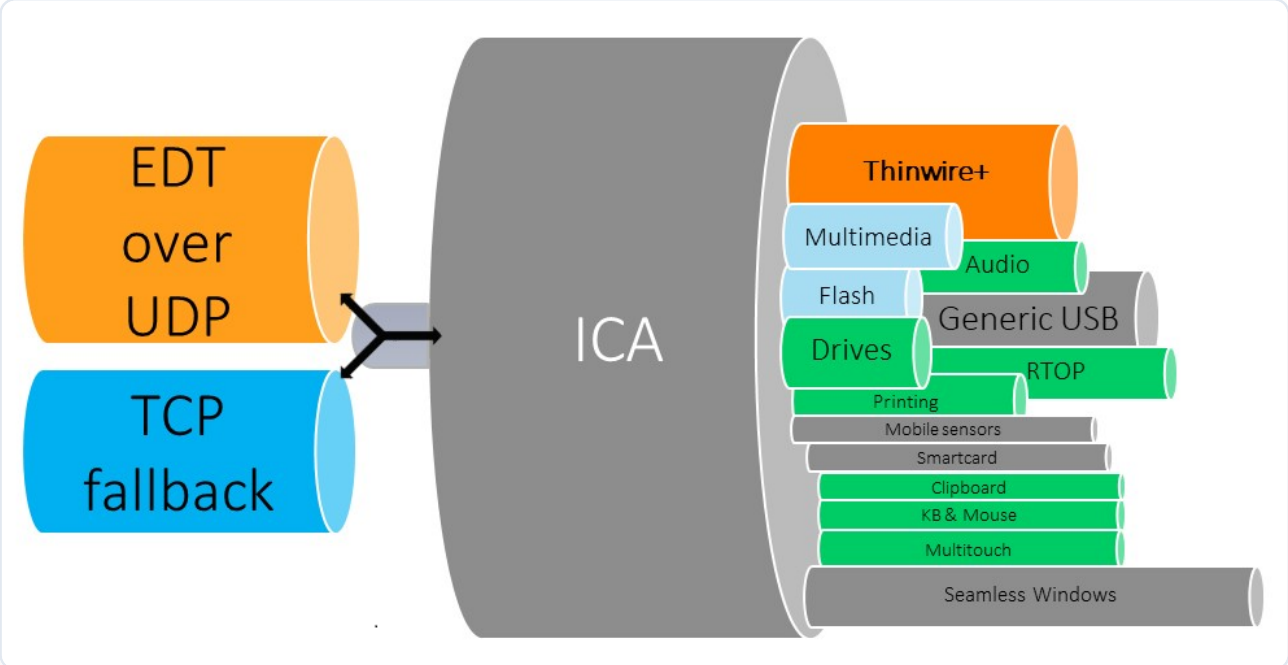
- **診断モード**: クライアントは優先プロトコルのみを使用して接続を試行します。TCPへのフォールバックは無効になります。
- **オフ**: クライアントはTCPのみを使用して接続を試行します。

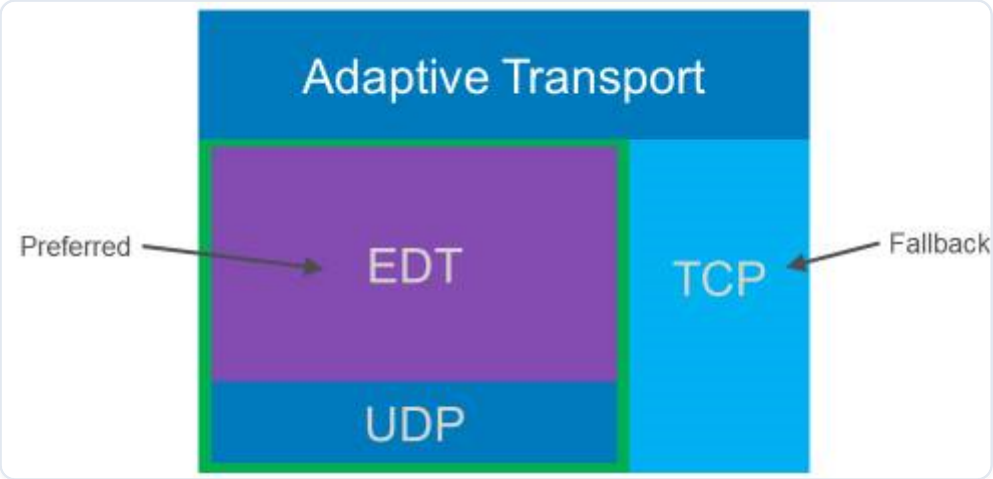
動作の仕組み

アダプティブトランスポートが`Preferred`に設定されている場合、クライアントは優先プロトコルとTCPの両方を使用してセッションに並行して接続を試行します。これにより、優先プロトコルで接続できない場合にクライアントがTCPの使用にフォールバックする必要がある場合でも、接続時間を最適化できます。TCPを使用して接続が確立された場合、クライアントは5分ごとにバックグラウンドで優先プロトコルでの接続を試行します。

アダプティブトランスポートが`Diagnostic mode`に設定されている場合、クライアントは優先プロトコルのみを使用してセッションに接続します。クライアントが優先プロトコルを使用して接続を確立できない場合、TCPへのフォールバックは行われず、接続は失敗します。

アダプティブトランスポートが`Off`に設定されている場合、**アダプティブトランスポート**は無効になり、クライアントはTCPのみを使用してセッションに接続します。





システム要件

アダプティブトランスポートとEDTを使用するための要件は次のとおりです。

- コントロールプレーン
  - シトリックス DaaS (旧 Citrix Virtual Apps and Desktops™ サービス)
  - Citrix Virtual Apps and Desktops: 現在サポートされているバージョン
- バーチャル デリバリー エージェント
  - Windows: 現在サポートされているバージョン (2402以降を推奨)
  - Linux: 現在サポートされているバージョン (2402以降を推奨)
- シトリックス ワークスペース™ アプリ
  - Windows: 現在サポートされているバージョン (2402以降を推奨)
  - Linux: 現在サポートされているバージョン (2402以降を推奨)
  - Mac: 現在サポートされているバージョン (2402以降を推奨)
  - iOS: Apple App Storeで入手可能な最新バージョン
  - Android: Google Playで入手可能な最新バージョン
- Citrix NetScaler® ゲートウェイ
  - 14.1.12.30以降 (推奨)
  - 13.1.17.42以降 (13.1-52.19以降を推奨)

> **注:**

Linux VDAの詳細については、Linux Virtual Delivery Agentのドキュメントを参照してください。

ネットワーク要件

以下は、アダプティブトランスポートでEDTを使用するためのネットワーク要件です。

セッションホスト

セッションホストにWindows Defender ファイアウォールなどのファイアウォールがある場合、内部接続のために以下のインバウンドトラフィックを許可する必要があります。

説明	送信元	プロトコル	ポート
内部接続 - セッションの信頼性が有効	クライアント	UDP	2598
内部接続 - セッションの信頼性が無効			1494
内部接続 - HDX™ DirectまたはVDA SSL			443

注:

VDAインストーラーは、Windows Defender ファイアウォールに適切な受信規則を追加します。別のファイアウォールを使用している場合は、上記の規則を追加する必要があります。

内部ネットワーク

以下の表は、ネットワークでEDTを使用するために必要なファイアウォール規則を示しています。

説明	プロトコル	送信元	宛先	宛先ポート
直接内部接続 - セッションの信頼性が有効	UDP	クライアントネットワーク	VDAネットワーク	2598

説明	プロトコル	送信元	宛先	宛先ポート
直接内部接続 - セッションの信頼性が無効				1494
直接内部接続 - HDX DirectまたはVDA SSL				443
NetScaler ゲートウェイ		NetScaler SNIP		2598
ネットスケーラー ゲートウェイ - VDA SSL				443

注:

Citrix Gateway Serviceを使用している場合、トランスポートプロトコルとしてEDTを使用するには、**Rendezvous**を有効にする必要があります。システムおよびネットワーク要件については、Rendezvousのドキュメントを参照してください。

クライアントネットワーク

以下の表は、クライアントデバイスの接続要件を示しています。

説明	プロトコル	送信元	宛先	宛先ポート
内部接続 - セッションの信頼性が有効	UDP	クライアントIP	VDAネットワーク	2598
内部接続 - セッションの信頼性が無効				1494

説明	プロトコル	送信元	宛先	宛先ポート
内部接続 - HDX Directまたは SSL VDA				443
外部接続 - NetScaler Gateway			NetScaler GatewayのパブリックIPアドレス	443
外部接続 - Citrix Gateway Service			シトリックスゲートウェイサービス	443

注:

Citrix Gateway Serviceを使用している場合、クライアントは`<https://*.*.nssvc.net>`に到達できる必要があります。`<https://*.*.nssvc.net>`を使用してすべてのサブドメインを許可できない場合は、代わりに`<https://*.c.nssvc.net>`と`<https://*.g.nssvc.net>`を使用できます。詳細については、Knowledge Centerの記事CTX270584を参照してください。

適応型データ転送

Enlightened Data Transport (EDT) は、User Datagram Protocol (UDP) 上に構築されたCitrix独自のトランスポートプロトコルです。これは、困難な長距離接続で優れたユーザーエクスペリエンスを提供し、サーバーのスケーラビリティを維持します。EDTは、信頼性の低いネットワーク上のすべてのICA®仮想チャネルのデータスループットを向上させ、より良く、より一貫したユーザーエクスペリエンスを提供します。

Adaptive Transport が有効になっている場合、EDTが優先プロトコルです。

知っておくべきこと

- NetScaler® GatewayおよびCitrix Gateway Serviceで**MTU Discovery**とEDTを使用するには、**Session Reliability**を有効にする必要があります。
- パケットの断片化は、パフォーマンスの低下や、場合によってはセッションを開くことの失敗を引き起こす可能性があります。これを防ぐには、EDT MTUをネットワークに適した値に調

整する必要があります。EDT MTU Discoveryを使用するか、非標準MTUのネットワークでEDTを使用する場合のMSSの構成方法で説明されている手動の回避策を使用できます。

- NetScaler GatewayでEDTの使用を有効にする方法の詳細については、NetScaler GatewayでEnlightened Data Transportをサポートするように構成するを参照してください。

EDT MTU検出

MTU Discoveryにより、EDTはセッション確立時に最大転送単位 (MTU) を自動的に決定できます。これにより、パフォーマンスの低下やセッション確立の失敗につながる可能性のあるEDTパケットの断片化を防ぎます。

MTU Discoveryはデフォルトで有効になっています。無効にする必要がある場合は、詳細についてレジストリで管理されるHDX機能を参照してください。

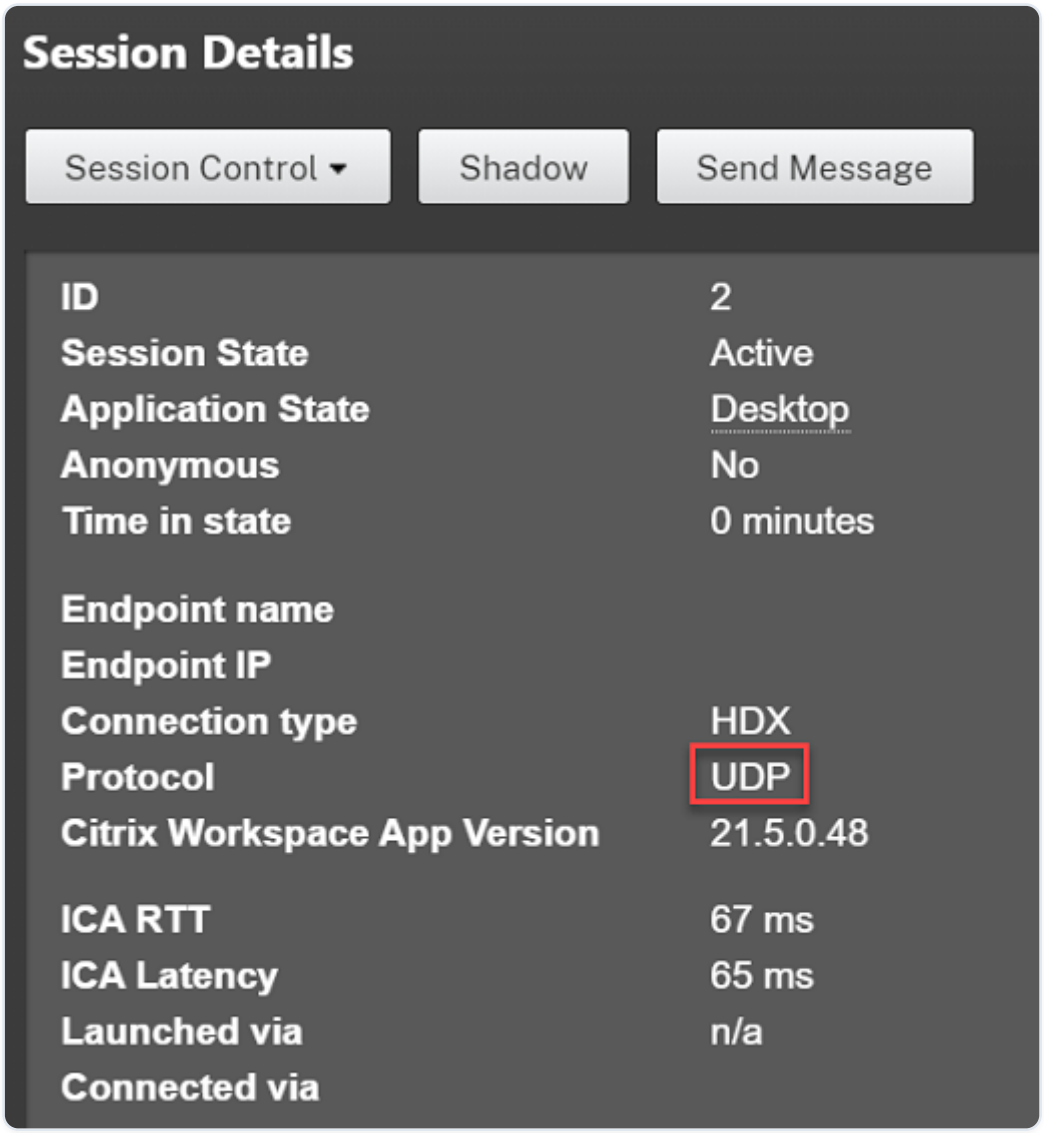
非対称パスを介した動的ルーティングによってセッションのMTUが変更される可能性があるシナリオでは、MTU検出はセッションのMTUを適切に検出して調整することもできます。再検出はデフォルトで無効になっています。これを有効にするには、HDX features managed through the registryを参照してください。

> **注:**
>
> - MTU Discoveryが機能するには、**Session Reliability**を有効にする必要があります。
> - Multi-Stream ICAでのMTU Discoveryは、VDAバージョン2209以降で利用可能です。

トラブルシューティング

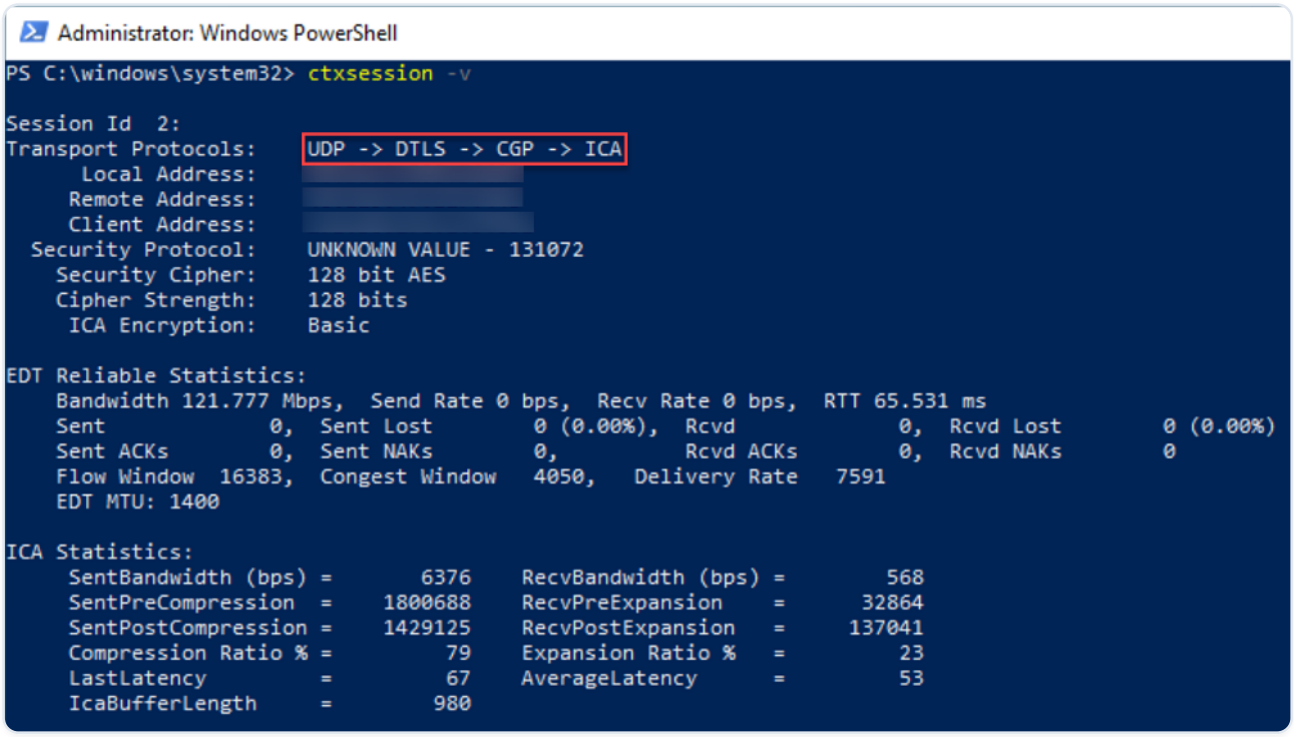
セッションのトランスポートプロトコルとしてEDTが使用されていることを確認するには、DirectorまたはVDA上の`CtxSession.exe`コマンドラインユーティリティを使用できます。

Directorでセッションを検索し、**詳細**を選択します。**接続の種類**が`HDX™`で、**プロトコル**が`UDP`の場合、EDTがセッションのトランスポートプロトコルとして使用されています。



CtxSession.exeユーティリティを使用するには、セッション内でコマンドプロンプトまたはPowerShellを起動し、`ctxsession.exe`を実行します。詳細な統計情報を表示するには、`ctxsession.exe -v`を実行します。EDTが使用されている場合、トランスポートプロトコルは次のいずれかを表示します。

- **UDP > ICA®** (セッションの信頼性が無効)
- **UDP > CGP > ICA** (セッションの信頼性が有効)
- **UDP > DTLS > CGP > ICA** (ICAはDTLSでエンドツーエンド暗号化されています)



EDTでセッションが接続に失敗する場合

Adaptive Transportと**EDT**のトラブルシューティングには、以下をお勧めします。

1. システム要件、ネットワーク要件、既知の問題、および留意事項を確認し、すべての項目が対処されていることを確認してください。
2. StudioまたはGPOに、目的の**HDX Adaptive Transport**設定を上書きするCitrix®ポリシーがないか確認します。
3. クライアントに、目的のHDX Adaptive Transport設定を上書きする設定がないか確認します。これは、GPO設定、オプションのWorkspace app管理テンプレートを使用して構成された設定、またはレジストリまたはクライアントの構成ファイルにおける**HDXoverUDP**設定の手動構成である可能性があります。
4. マルチセッションVDAマシンで、UDPリスナーがアクティブであることを確認します。VDAマシンでコマンドプロンプトを開き、`netstat -a -p udp`を実行します。詳細については、「HDX Enlightened Data Transportプロトコルを確認する方法」を参照してください。
5. ネットワークファイアウォールとVDAマシンで実行されているファイアウォールの両方で、適切なファイアウォールルールが構成されているか確認します。
6. NetScaler® GatewayまたはCitrix Gateway Serviceをバイパスして、内部で直接セッションを起動し、使用中のプロトコルを確認します。セッションがEDTを使用している場合、VDAはNetScaler GatewayまたはCitrix Gateway Serviceを介した外部接続にEDTを使用する準備ができています。

7. EDTが直接内部接続では機能するが、NetScaler GatewayまたはCitrix Gateway Serviceを介するセッションでは機能しない場合：

   - **セッションの信頼性**が有効になっていることを確認します。
   - NetScaler Gatewayを使用している場合は、Enlightened Data TransportおよびHDX Insightをサポートするように NetScaler Gatewayを構成するに記載されている必要な構成に準拠していることを確認してください。

8. Citrix Gateway Serviceを使用している場合は、Rendezvousが有効になっていて機能していることを確認します。
9. ユーザーの接続に非標準のMTUが必要かどうかを確認します。実効MTUが1500バイト未満の接続では、EDTパケットの断片化が発生し、パフォーマンスに影響を与えたり、セッション起動の失敗を引き起こしたりする可能性があります。この問題は、VPN、一部のWi-Fiアクセスポイント、および4Gや5Gなどのモバイルネットワークを使用する場合によく発生します。MTU検出が有効になっているか、非標準MTUのネットワークでEDTを使用する場合のMSSの構成方法に記載されているようにカスタムMTUを設定していることを確認してください。

既知の問題

- 非対称ネットワークパスは、NetScaler GatewayまたはCitrix Gateway Serviceを介さない接続でMTU検出が失敗する原因となる可能性があります。この問題に対処するには、VDAバージョン2103以降にアップグレードしてください。
- NetScaler Gatewayを使用している場合、非対称ネットワークパスはMTU検出が失敗する原因となる可能性があります。これは、Gatewayの問題により、EDTパケットヘッダーのDon't Fragment（DF）ビットが伝播されないためです。この問題の修正は、ファームウェアリリース13.1ビルド17.42以降で利用可能です。修正を有効にする方法の詳細については、NetScaler Gatewayのドキュメントを参照してください。
- DS-Liteネットワークを介して接続するユーザーの場合、MTU検出が失敗することがあります。一部のモデムでは、パケット処理が有効になっている場合にDFビットが尊重されず、MTU検出が断片化を検出できなくなります。この状況では、以下のオプションが利用可能です。

  - ユーザーのモデムでパケット処理を無効にします。
  - **MTU検出**を無効にし、非標準MTUのネットワークでEDTを使用する場合のMSSの構成方法に記載されているようにハードコードされたMTUを使用します。
  - セッションにTCPの使用を強制するために**アダプティブトランスポート**を無効にします。ユーザーの一部のみが影響を受ける場合は、他のユーザーがEDTを引き続き使用できるように、クライアント側で無効にすることを検討してください。

HDX™ ダイレクト

Citrixが提供するリソースにアクセスする場合、HDX Directは、直接通信が可能な場合、内部および外部のクライアントデバイスがセッションホストとの安全な直接接続を確立することを可能にします。

システム要件

HDX Directを使用するためのシステム要件は以下のとおりです。

- コントロールプレーン
  - シトリックス DaaS™
  - シトリックス Virtual Apps and Desktops™ 2503 以降
- 仮想配信エージェント (VDA)
  - Windows: バージョン 2503 以降
- Workspace アプリ
  - Windows: バージョン 2503 以降
  - Linux: バージョン 2411 以降
  - Mac: バージョン 2411 以降
- アクセス層
  - シトリックス ワークスペース™
  - シトリックス ストアフロント™ 2503 以降
  - シトリックス ゲートウェイ サービス
  - Citrix NetScaler® ゲートウェイ

ネットワーク要件

HDX Directを使用するためのネットワーク要件は以下のとおりです。

セッションホスト

セッションホストにWindows Defender ファイアウォールなどのファイアウォールがある場合、内部接続のために以下のインバウンドトラフィックを許可する必要があります。

説明	送信元	プロトコル	ポート
直接内部接続	クライアント	TCP	443
直接内部接続	クライアント	UDP	443

注:

VDA インストーラーは、Windows Defender ファイアウォールに適切な受信規則を追加します。別のファイアウォールを使用する場合は、上記の規則を追加する必要があります。

クライアントネットワーク

以下の表は、内部および外部ユーザー向けのクライアントネットワークについて説明しています。

内部ユーザー

説明	プロトコル	送信元	ソースポート	宛先	宛先ポート
直接内部接続	TCP	クライアントネットワーク	1024–65535	VDAネットワーク	443
直接内部接続	UDP	クライアントネットワーク	1024–65535	VDAネットワーク	443

外部ユーザー

説明	プロトコル	送信元	ソースポート	宛先	宛先ポート
STUN (外部ユーザーのみ)	UDP	クライアントネットワーク	1024–65535	インターネット (下記の注記を参照)	3478, 19302
外部ユーザー接続	UDP	クライアントネットワーク	1024–65535	データセンターのパブリックIPアドレス	1024–65535

データセンターネットワーク

以下の表は、内部ユーザーと外部ユーザー向けのデータセンターネットワークについて説明しています。

内部ユーザー

説明	プロトコル	送信元	ソースポート	宛先	宛先ポート
直接内部接続	TCP	クライアントネットワーク	1024–65535	VDAネットワーク	443
直接内部接続	UDP	クライアントネットワーク	1024–65535	VDAネットワーク	443

外部ユーザー

説明	プロトコル	送信元	ソースポート	宛先	宛先ポート
STUN (外部ユーザーのみ)	UDP	VDAネットワーク	1024–65535	インターネット (下記の注記を参照)	3478, 19302
外部ユーザー接続	UDP	DMZ / 内部ネットワーク	1024–65535	VDAネットワーク	55000–55250
外部ユーザー接続	UDP	VDAネットワーク	55000–55250	クライアントのパブリックIP	1024–65535

注：

VDAとWorkspaceアプリの両方が、以下のサーバーに同じ順序でSTUNリクエストを送信しようとします。

- stun.cloud.com:3478

- stun.cloudflare.com:3478
- stun.l.google.com:19302

HDX Directポート範囲ポリシー設定を使用して外部ユーザー接続のデフォルトポート範囲を変更する場合、対応するファイアウォール規則はカスタムポート範囲と一致する必要があります。

構成

HDX Directはデフォルトで無効になっています。この機能は、Citrixポリシーの**HDX Direct**設定を使用して構成できます。

- **HDX Direct**: 機能を有効または無効にする。
- 「**HDX Directモード**」：**HDX Direct**が内部クライアントのみで利用可能か、内部クライアントと外部クライアントの両方で利用可能かを決定します。
- 「**HDX Directポート範囲**」：VDAが外部クライアントからの接続に使用するポート範囲を定義します。

必要に応じて、HDX Directで使用されるSTUNサーバーのリストは、以下のレジストリ値を編集することで変更できます。

- キー：HKLM\SOFTWARE\Citrix\HDX-Direct
- 値の型: REG_MULTI_SZ
- 値の名前：STUNServers
- データ：stun.cloud.com:3478 stun.cloudflare.com:3478 stun.l.google.com:19302

注：

外部ユーザー向けのHDX Directは、トランスポートプロトコルとしてEDT (UDP) を使用する場合にのみ利用可能です。したがって、アダプティブトランスポートを有効にする必要があります。

考慮事項

HDX Directを使用する際の考慮事項は次のとおりです。

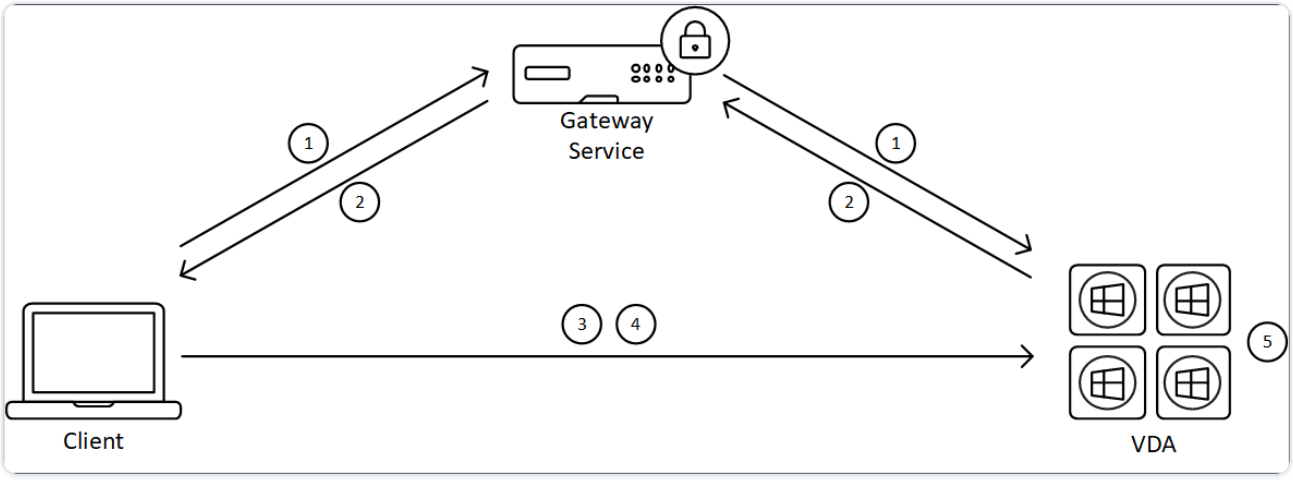
- 外部ユーザー向けのHDX Directは、トランスポートプロトコルとしてEDT (UDP) を使用する場合にのみ利用可能です。したがって、**アダプティブトランスポート**を有効にする必要があります。
- **HDX Insight**を使用している場合、**HDX Direct**を使用すると、セッションがNetScaler Gatewayを介してプロキシされなくなるため、HDX Insightのデータ収集が妨げられることに注意してください。
- マルチセッションセッションホストの環境では、HDX Direct はユーザーログオンが 1 分以内に完了することを要求します。ログオン時間がこのしきい値を超えると、HDX Direct はトリガーされず、セッションは Gateway を介して接続されたままになります。より長いログオン時間をサポートするために、HDX Direct のタイムアウトを増やすことができます。詳細については、レジストリで管理される HDX 機能 を参照してください。

動作の仕組み

HDX Directを使用すると、直接通信が可能な場合にクライアントがセッションホストへの直接接続を確立できます。HDX Directを使用して直接接続が行われる場合、自己署名証明書が使用され、ネットワークレベルの暗号化 (TLS/DTLS) で直接接続を保護します。

内部ユーザー

次の図は、内部ユーザーのHDX Direct接続プロセスの概要を示しています。



1. クライアントはGateway Serviceを介してHDXセッションを確立します。
2. 接続が成功すると、VDAはHDX接続を介して、VDAマシンのFQDN、そのIPアドレスのリスト、およびVDAマシンの証明書をクライアントに送信します。
3. クライアントは、VDAに直接到達できるかどうかを確認するためにIPアドレスをプローブします。

4. クライアントが共有されたいずれかのIPアドレスでVDAに直接到達できる場合、クライアントはVDAとの直接接続を確立します。この接続は、手順(2)で交換された証明書と一致する証明書を使用して(D)TLSで保護されます。
5. 直接接続が正常に確立されると、セッションは新しい接続に転送され、Gateway Serviceへの接続は終了します。

> **注:**
>
> 上記の手順2で接続を確立した後、セッションはアクティブになります。その後の手順は、ユーザーが仮想アプリケーションまたはデスクトップを使用する能力を遅延させたり、妨げたりすることはありません。その後の手順のいずれかが失敗した場合でも、Gatewayを介した接続はユーザーのセッションを中断することなく維持されます。

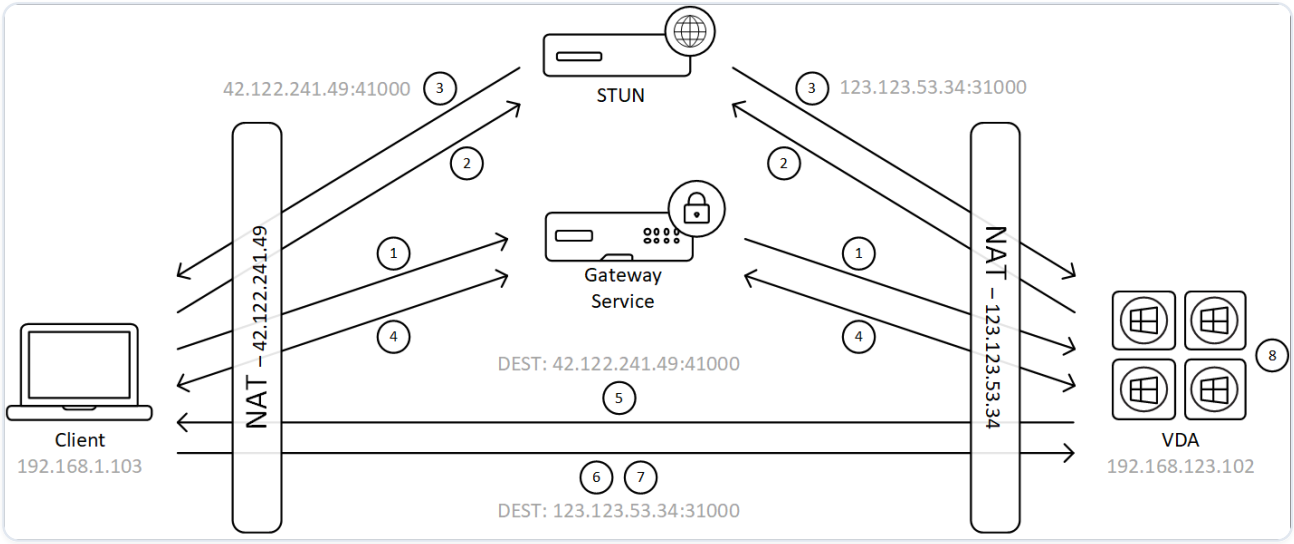
従来の直接接続

Storefront、Direct Workload Connectionを使用するWorkspace、または内部接続専用に構成されたWorkspaceを使用する場合、クライアントとセッションホスト間の直接接続は、最初にGatewayを介してルーティングする必要なく確立されます。

これらの場合、接続は本質的に直接的であるため、HDX Directはトリガーされません。ただし、HDX Directが有効になっている場合、これらの接続はHDX Direct証明書を利用してセッションを保護します。

外部ユーザー

次の図は、外部ユーザー向けのHDX Direct接続プロセスの概要を示しています。



1. クライアントはGateway Serviceを介してHDXセッションを確立します。

2. 接続が成功すると、クライアントとVDAの両方がSTUNリクエストを送信して、それぞれのパブリックIPアドレスとポートを検出します。
3. STUNサーバーは、クライアントとVDAにそれぞれのパブリックIPアドレスとポートで応答します。
4. HDX接続を介して、クライアントとVDAはそれぞれのパブリックIPアドレスとUDPポートを交換し、VDAはクライアントに証明書を送信します。
5. VDAは、クライアントのパブリックIPアドレスとUDPポートにUDPパケットを送信します。クライアントは、VDAのパブリックIPアドレスとUDPポートにUDPパケットを送信します。
6. VDAからのメッセージを受信すると、クライアントはセキュアな接続要求で応答します。
7. DTLSハンドシェイク中に、クライアントは証明書がステップ(4)で交換された証明書と一致することを確認します。検証後、クライアントは認証トークンを送信します。これでセキュアな直接接続が確立されます。
8. 直接接続が正常に確立されると、セッションは新しい接続に転送され、Gateway Serviceへの接続は終了します。

> **注:**
>
> 上記のステップ2で接続を確立した後、セッションはアクティブになります。その後の手順は、ユーザーが仮想アプリケーションまたはデスクトップを使用する能力を遅らせたり、妨げたりすることはありません。その後の手順のいずれかが失敗した場合でも、ユーザーのセッションを中断することなく、Gatewayを介した接続は維持されます。

証明書管理

概要

HDX™ダイレクト接続は、ネットワークレベルの暗号化で保護されています。これを容易にするため、各セッションホストには、一意の自己署名ルートCA証明書と、その自己署名ルートCA証明書によって署名された対応するサーバー証明書があります。

このソリューションには、次の利点があります。

- **セキュリティの合理化:** HDXダイレクト接続は、環境内で証明書を管理する管理上のオーバーヘッドなしに保護されます。
- **攻撃対象領域の縮小:** 各ホストが一意のキーと証明書のセットを持つため、攻撃対象領域は単一のホストに限定されます。

- **非永続環境のセキュリティ強化:** 非永続セッションホストがある環境では、再起動時に新しいキーと証明書が生成されるため、セキュリティがさらに強化されます。

セッションホスト

Citrix ClxMtp Serviceと**Citrix Certificate Manager Service**は、各セッションホストで証明書を管理する2つのサービスです。ClxMtp Serviceはキーの生成とローテーションを処理し、Certificate Manager Serviceは証明書を生成および管理します。

自己署名ルートCAとサーバー証明書の2つの証明書が作成されます。どちらも2年間の有効期間で発行されますが、キーがローテーションされると置き換えられます。さらに、非永続マシンが再起動するたびに新しい証明書が生成されます。

各証明書の詳細は次のとおりです。

- **自己署名ルートCA**
  - 発行先は CA-Citrix-Certificate-Manager です
  - 発行元はCA-Citrix-Certificate-Managerです。
  - 発行者の詳細: 組織はCitrix Systems, Inc.です。
- **サーバー証明書**
  - 発行先: \<ホストFQDN\> (例: FTLW11-001.ctxlab.net)
  - 発行元はCA-Citrix-Certificate-Managerです。
  - 発行者の詳細: 組織はCitrix Systems, Inc.です。

> **注：**

> Citrix Certificate Manager Serviceは、2048ビットキーを利用するRSA証明書を生成します。

> Citrix Certificate Manager Serviceによって作成された既存のマシン証明書があり、サブジェクト名がマシンのFQDNと一致しない場合、新しい証明書が生成されます。

キーのローテーション

Citrix ClxMtp Serviceは、6か月ごとにキーを自動的にローテーションします。ただし、セッションホストのレジストリでローテーションカウンターを増やすことで、手動でキーのローテーションをトリガーできます。

キーをローテーションするには、次の値を更新します。

- キー: SOFTWARE\Citrix\ClxMtpConnectorSvcRotateKeyPairs
- 値の型: DWORD
- 値の名前: ClxMtpRotateRequestCounter
- データ: 整数 (10進数)

注：

初めてキーをローテーションする場合:

1. ClxMtpConnectorSvcRotateKeyPairsキーを作成します。
2. ClxMtpRotateRequestCounter値を1に作成して設定します。

その後のキーのローテーションでは、ClxMtpRotateRequestCounter値を1増やします。

値が更新されると、**Citrix ClxMtp Service**は再起動を必要とせずにキーを自動的にローテーションします。その後、**Citrix Certificate Manager Service**は新しいキーを検出すると、自動的に新しい証明書を生成します。

クライアントデバイス

ルートCA証明書は、WorkspaceまたはStorefront™によって、すでに確立されている安全で信頼された接続パスを介してクライアントに送信されます。これにより、CA証明書をクライアントデバイスの証明書ストアに配布する必要がなくなり、クライアントがHDX Direct接続のセキュリティ保護に使用される証明書を信頼するようになります。

カスタム証明書の使用

HDX Directは、独自のPKIによって発行および管理される証明書の使用をサポートしています。以下の手順では、証明書のインストール方法、必要な権限の構成方法、セッションマネージャーサービスへのバインド方法、および必要なTLSリスナーの有効化方法について説明します。

1. マシンでHDX Directが無効になっている場合は、手順2に進みます。HDX Directが有効になっている場合は、以下の手順に従います。

   a. レジストリエディター (regedit.exe) を開き、「**HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd**」に移動します。
   b. **SSLEnabled** の値を **0** に設定します。
   c. **HKLM\Software\Citrix\HDX-Direct** に移動します。
   d. **HdxDirectCaInTls** の値を **0** に設定します。

2. PKIによって発行された適切な証明書を、マシンの証明書ストアにインストールします。
3. セッションマネージャーサービスに、証明書の秘密キーへの読み取りアクセス権を付与します。

   a. Microsoft管理コンソール (**MMC**) を起動します: > > mmc.exe。
   b. **>** に移動します。
   c. を選択し、 をクリックします。
   d. を選択し、 をクリックします。
   e. を選択し、 をクリックします。
   f. **証明書 (ローカル コンピューター) > 個人 > 証明書**」に移動します。
   g. 適切な証明書を右クリックし、「**すべてのタスク > 秘密キーの管理**」を選択します。
   h. 次のいずれかのサービスを追加し、読み取りアクセス権を付与します。

      - **シングルセッションVDA**の場合: `NT SERVICE\PorticaService`
      - **マルチセッションVDA**の場合: `NT SERVICE\TermService`

   i. 「**適用**」をクリックし、次に「**OK**」をクリックします。

4. 証明書をセッションマネージャーサービスにバインドします。

   a. 証明書の拇印を取得します (証明書をダブルクリック > 「**詳細**」 > 「**拇印**」)。
   b. レジストリエディター (regedit.exe) を開き、「**HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd**」に移動します。
   c. **SSLThumbprint**の値を編集し、証明書の拇印を貼り付けます。

5. Citrix TLSリスナーを有効にします。

   a. 同じレジストリの場所で、**SSLEnabled**の値を**1**に設定します。

6. HDX Directを有効にします (Citrixポリシー内)。

Citrix Virtual Apps and Desktopsのインストールメディアには、これらのタスクのいくつかを自動化するPowerShellスクリプト (Enable-VdaSSL.ps1) が含まれています。

- 証明書のキーのアクセス許可を設定する
- 証明書をセッションマネージャーサービスにバインドする
- Citrix TLSリスナーを有効にする

このスクリプトは、Support > Tools > SslSupport ディレクトリにあります。詳細については、「PowerShellスクリプトを使用してVDAでTLSを構成する」を参照してください。

> **注：**
>
> 独自の証明書を使用している場合、セッションホストに接続するデバイスには、正しいルートCA証明書と中間CA証明書がインストールされている必要があります。

NAT互換性

外部ユーザーデバイスとセッションホスト間の直接接続を確立するために、HDX™ DirectはNATトラバーサルのためにホールパンチングを利用し、クライアントデバイスとセッションホストのパブリックIPアドレスおよびポートマッピングの交換を容易にするためにSTUNを利用します。これは、VoIP、ユニファイドコミュニケーション、P2Pソリューションの仕組みに似ています。

ファイアウォールやその他のネットワークコンポーネントが、STUNリクエストおよびHDXセッションのUDPトラフィックを許可するように構成されている限り、外部ユーザー向けのHDX Directは機能すると予想されます。ただし、ユーザーおよびセッションホストネットワークのNATタイプが互換性のない組み合わせとなり、HDX Directが失敗する特定のシナリオがあります。

検証

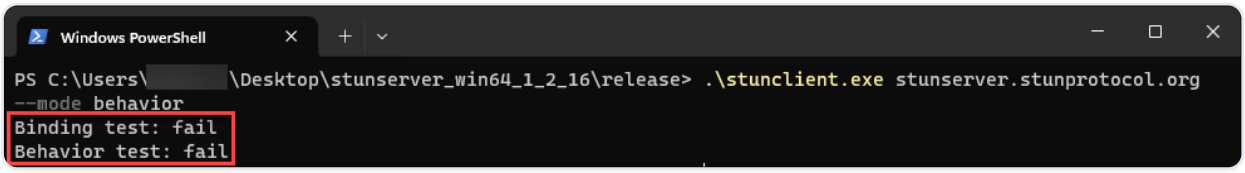
クライアントおよびセッションホスト上のNATタイプとフィルタリングは、STUNTMANのSTUNクライアントユーティリティを使用して検証できます。

1. stunprotocol.orgからターゲットプラットフォームに適したパッケージをダウンロードし、その内容を抽出します。
2. ターミナルプロンプトを開き、内容が抽出されたディレクトリに移動します。
3. NATバインディングおよび動作テストを実行するには、次のコマンドを実行します。
   `stunclient.exe stunserver2025.stunprotocol.org --mode behavior`

4. バインディングテストと動作テストが成功した場合、**バインディングテスト**と**動作テスト**の両方が成功を報告し、NAT動作が指定されます。



テストが失敗した場合、**バインディングテスト**および/または**動作テスト**が失敗を報告します。



5. NATバインディングおよびフィルタリングテストを実行するには、次のコマンドを実行します。 `stunclient.exe stunserver2025.stunprotocol.org --mode filtering`

6. バインディングテストとフィルタリングテストが成功した場合、**バインディングテスト**と**フィルタリングテスト**の両方が成功を報告し、NATフィルタリングタイプが指定されます。

   テストが失敗した場合、**バインディングテスト**および/または**フィルタリングテスト**が失敗を報告します。

上記のテストを実行した後、NATの動作とフィルタリングの組み合わせに基づいて、外部ユーザー向けのHDX Directが動作すると予想されるかどうかを判断するために、次の表を確認してください。

クライアントNATの動作	クライアントNATのフィルタリング	セッションホストNATの動作	セッションホストNATのフィルタリング	動作が期待されますか？
エンドポイント独立マッピング	任意	エンドポイント独立マッピング	任意	はい
エンドポイント独立マッピング	エンドポイント独立フィルタリング	アドレス依存マッピング	任意	はい
エンドポイント独立マッピング	アドレス依存フィルタリング	アドレス依存マッピング	任意	いいえ

クライアントNATの動作	クライアントNATのフィルタリング	セッションホストNATの動作	セッションホストNATのフィルタリング	動作が期待されますか？
エンドポイント独立マッピング	アドレスおよびポート依存フィルタリング	アドレス依存マッピング	任意	いいえ
エンドポイント独立マッピング	エンドポイント独立フィルタリング	アドレスおよびポート依存マッピング	エンドポイント独立フィルタリング	はい
エンドポイント独立マッピング	アドレス依存フィルタリング	アドレス依存マッピング	任意	いいえ
エンドポイント独立マッピング	アドレスおよびポート依存フィルタリング	アドレス依存マッピング	任意	いいえ
アドレス依存マッピング	任意	エンドポイント独立マッピング	エンドポイント独立フィルタリング	はい
アドレス依存マッピング	任意	エンドポイント独立マッピング	アドレス依存フィルタリング	いいえ
アドレス依存マッピング	任意	エンドポイント独立マッピング	アドレスおよびポート依存フィルタリング	いいえ
アドレス依存マッピング	任意	アドレス依存マッピング	任意	いいえ
アドレス依存マッピング	任意	アドレスおよびポート依存マッピング	任意	いいえ
アドレスおよびポート依存マッピング	任意	エンドポイント独立マッピング	エンドポイント独立フィルタリング	はい

クライアントNATの動作	クライアントNATのフィルタリング	セッションホストNATの動作	セッションホストNATのフィルタリング	動作が期待されますか？
アドレスおよびポート依存マッピング	任意	エンドポイント独立マッピング	アドレス依存フィルタリング	いいえ
アドレスおよびポート依存マッピング	任意	エンドポイント独立マッピング	アドレスおよびポート依存フィルタリング	いいえ
アドレスおよびポート依存マッピング	任意	アドレス依存マッピング	任意	いいえ
アドレスおよびポート依存マッピング	任意	アドレスおよびポート依存マッピング	任意	いいえ
失敗	任意	任意	任意	いいえ
任意	任意	失敗	任意	いいえ
失敗	任意	失敗	任意	いいえ

トラブルシューティング

HDX Direct が直接接続を正常に確立したことを確認するには、VDA マシンで `CtxSession.exe` ユーティリティを使用できます。

`CtxSession.exe` ユーティリティを使用するには、セッション内でコマンドプロンプトまたは PowerShell を起動し、`ctxsession.exe -v` を実行します。**HDX Direct** 接続が正常に確立されている場合、**HDX Direct Status** は `Connected` です。

HDX Direct のトラブルシューティング(/en-us/citrix-virtual-apps-desktops/current-release/media/hdx-direct-troubleshooting.png)

セッションホストのイベントログで、HDX™ Direct 接続が正常に確立されたか、または失敗したかに関する情報を確認することもできます。詳細については、「**イベントログ**」セクションを参照してください。

> 注:

> 環境およびセッションホストで利用可能な IP アドレスの数によっては、HDX Direct 接続が確立されるまでに最大 5 分かかる場合があります。

HDX Direct が直接接続を確立できない場合

HDX Direct が直接接続を確立できない場合は、次の手順を確認してください。

1. 使用している VDA バージョンと Workspace アプリバージョンが、システム要件に従ってこの機能をサポートしていることを確認してください。
2. HDX Direct を有効にするポリシーが VDA に適用されており、この機能を無効にする優先度の高い他のポリシーがないことを確認してください。
3. 目的の HDX Direct モードを設定するポリシーが VDA に適用されており、この構成を上書きする優先度の高い他のポリシーがないことを確認してください。
4. Citrix ClxMtp Service がセッションホストで実行されていることを確認してください。
5. Citrix Certificate Manager Service がセッションホストで実行されていることを確認してください。実行されていない場合は、手動で開始してみてください。HDX Direct が無効になっている場合、このサービスは自動的に停止します。
6. セッションホストに自己署名ルート CA 証明書があるかどうかを確認します。
    a. 発行先: `CA-Citrix-Certificate-Manager`
    b. 発行元: `CA-Citrix-Certificate-Manager`
    c. 発行者情報: 組織はCitrix Systems, Inc.です。
7. セッションホストに自己署名サーバー証明書があるか確認します。
    a. 発行先: `<host FQDN>` (例: FTLW11-001.ctxlab.net)
    b. 発行元: `CA-Citrix-Certificate-Manager`
    c. 発行者情報: 組織はCitrix Systems, Inc.です。
8. 証明書が見つからない場合は、Citrixテクニカルサポートにお問い合わせください。
9. 証明書が存在する場合:
    a. セッションホストでCitrix Certificate Manager Serviceを停止します。
    b. 自己署名ルートCA証明書と自己署名サーバー証明書の両方を削除します。

c. セッションホストでCitrix Certificate Manager Serviceを開始します。サービスは開始されると新しい証明書を作成します。

10. 内部ユーザーの場合:

a. セッションホストのファイアウォールが、HDX over EDTの場合はUDP 443、HDX over TCPの場合はTCP 443の受信トラフィックをブロックしていないことを確認します。

b. クライアントネットワークとセッションホストネットワーク間のUDP 443およびTCP 443のトラフィックをネットワークファイアウォールがブロックしていないことを確認します。

11. 外部ユーザーの場合:

a. セッションホストにSTUNサーバーのリストが含まれていることを確認します。

- キー: HKLM\SOFTWARE\Citrix\HDX-Direct
- 値の型: REG_MULTI_SZ
- 値の名前: STUNServers
- データ: stun.cloud.com:3478 stun.cloudflare.com:3478 stun.l.google.com:19302

b. クライアントとセッションホストのNATタイプを確認し、その組み合わせが正常に機能することを確認します。詳細については、「NAT互換性」セクションを参照してください。

c. クライアントまたはセッションホストのいずれかでNATテストが失敗した場合:

i. システムでファイアウォールが実行されている場合は、UDP 3478での送信トラフィックをブロックしていないことを確認してください。

ii. ネットワークファイアウォールがUDP 3478での送信トラフィックをブロックしていないことを確認してください。

iii. ファイアウォールがSTUNサーバーの応答をブロックしていないことを確認してください。

d. ネットワークファイアウォールに、必要なすべてのトラフィックを許可するための適切なルールが構成されていることを確認してください。詳細については、ネットワーク要件セクションを参照してください。

e. HDX Directポート範囲ポリシー設定を使用してデフォルトのポート範囲を変更する場合は、ファイアウォールルールがカスタムポート範囲に設定されていることを確認してください。

イベントログ

以下のイベントがVDAマシンのイベントログに記録されます:

ログ	ID	送信元	レベル	説明
アプリケーションとサービスログ > Citrix-HostCore-HDX Direct/操作	1	HDX ダイレクト	情報	内部ユーザー `<username>` のHDX Direct接続が確立されました。
アプリケーションとサービスログ > Citrix-HostCore-HDX Direct/操作	2	HDX ダイレクト	情報	外部ユーザー `<username>` のHDX Direct接続が確立されました。
アプリケーションとサービスログ > Citrix-HostCore-HDX Direct/操作	3	HDX ダイレクト	情報	ユーザー `<username>` のHDX Direct接続に失敗しました。
アプリケーションとサービスログ > Citrix-HostCore-HDX Direct/操作	4	HDX ダイレクト	情報	STUN サーバー `<URL:PORT>` は、ユーザー `<username>` のセッションホスト IP およびポートマッピングとして以下を提供しました: `<IP>:<PORT>` 。
アプリケーションとサービスログ > Citrix-HostCore-HDX Direct/操作	5	HDX ダイレクト	情報	ユーザー `<username>` の構成済み STUN サーバーのいずれからも、セッションホストによって

ログ	ID	送信元	レベル	説明
				応答が受信されませんでした。
アプリケーションとサービスログ > Citrix-HostCore-HDX Direct/操作	6	HDX ダイレクト	情報	クライアントはユーザー `<username>` の外部マッピングとして `<IP>:<PORT>` を提供しました。
アプリケーションとサービスログ > Citrix-HostCore-HDX Direct/操作	7	HDX ダイレクト	情報	クライアントからユーザー `<username>` の外部マッピングは提供されませんでした。

既知の問題

- Rendezvousが無効になっている場合、Gateway Service を使用するWorkspace環境では、外部ユーザー向けのHDX Directが失敗する可能性があります。この問題を解決するには、Rendezvous が有効になっていることを確認してください。
- 既に **HDX Direct** が有効になっているマシンで VDA のインプレースアップグレードを実行した後、HDX Direct が動作しなくなる可能性があります。この問題を解決するには、次の手順を実行します。

  a. セッションホスト上でCitrix Certificate Managerサービスを停止します。
  b. 自己署名ルートCA証明書および自己署名サーバー証明書を削除します。
  c. レジストリを開きます。
  d. `HKLM\Software\Citrix\HDX-Direct` キーを削除します。
  e. `HKLM\SYSTEM\CurrentControlSet\Control\TerminalServer\Wds\icawd` に移動します。
  f. **SSLEnabled** の値を `0` に設定します。
  g. **SSLThumbprint** の値の内容を削除します。
  h. **Citrix Certificate Managerサービス**を開始します。

セキュアHDX™

セキュアHDXは、トラフィックパス内のネットワーク要素がHDXトラフィックを検査できないようにするアプリケーションレベル暗号化 (ALE) ソリューションです。これは、AES-256-GCM暗号化を使用して、Citrix Workspace™アプリ (クライアント) とVDA (セッションホスト) の間でアプリケーションレベルで真のエンドツーエンド暗号化 (E2EE) を提供することで実現されます。

システム要件

以下の一覧は、セキュアHDXを使用するためのシステム要件を示しています。

- コントロールプレーン
  - シトリックス DaaS™
  - シトリックス Virtual Apps and Desktops™ 2503 以降
- セッションホスト
  - オペレーティングシステム
    - Windows 10 22H2 バージョン
    - Windows 11 22H2以降
    - Windows Server 2019 以降のバージョン
  - 仮想配信エージェント (VDA)
    - Windows: バージョン 2503 以降
    - Linux: バージョン2407以降
- Workspaceアプリ
  - Windows: バージョン 2503 以降
  - Linux: バージョン 2408 以降
  - Mac: バージョン 2409 以降
  - Chrome OS: バージョン 2409 以降
  - HTML5: バージョン 2408 以降
  - Android: バージョン 2503 以降
  - iOS: バージョン 2503 以降
- アクセス層

- シトリックス ワークスペース
- Citrix StoreFront™ 2402 以降

> **注：**
>
> Linux VDA で Secure HDX を構成する方法の詳細については、Linux VDA のドキュメントを参照してください。

構成

Secure HDX はデフォルトで無効になっています。この機能は、Citrix ポリシーの Secure HDX 設定を使用して構成できます。

Secure HDX: この機能を有効にするか無効にするかを定義します。

> **重要:**
>
> Secure HDX を有効にするデリバリーグループで Secure ICA® が有効になっている場合は、まず Secure ICA を無効にする必要があります (デリバリーグループの編集 > ユーザー設定)。

HDX インサイトとスマートコントロール

Secure HDX が有効な場合に、NetScaler Gateway で HDX Insight と SmartControl を使用するための要件は次のとおりです。

- NetScaler 14.1 Build 47.46 以降 (EDT サポートには 14.1 Build 72.57 以降が必要)。
- **ネットワークテレメトリ**は Citrix ポリシーで有効にする必要があります。詳細については、ネットワークテレメトリを参照してください。
- **セッションの信頼性**を有効にする必要があります。この設定はデフォルトで有効になっているため、無効にするポリシーがないことを確認してください。

> **注:**
>
> Secure HDX を使用した HDX Insight と SmartControl は、次のシナリオでのみ利用可能です。

- NetScaler 14.1 Build 47.46 以降 (EDT には 14.1 Build 72.57 以降が必要) を使用する場合
- IPv4 を使用する接続

考慮事項

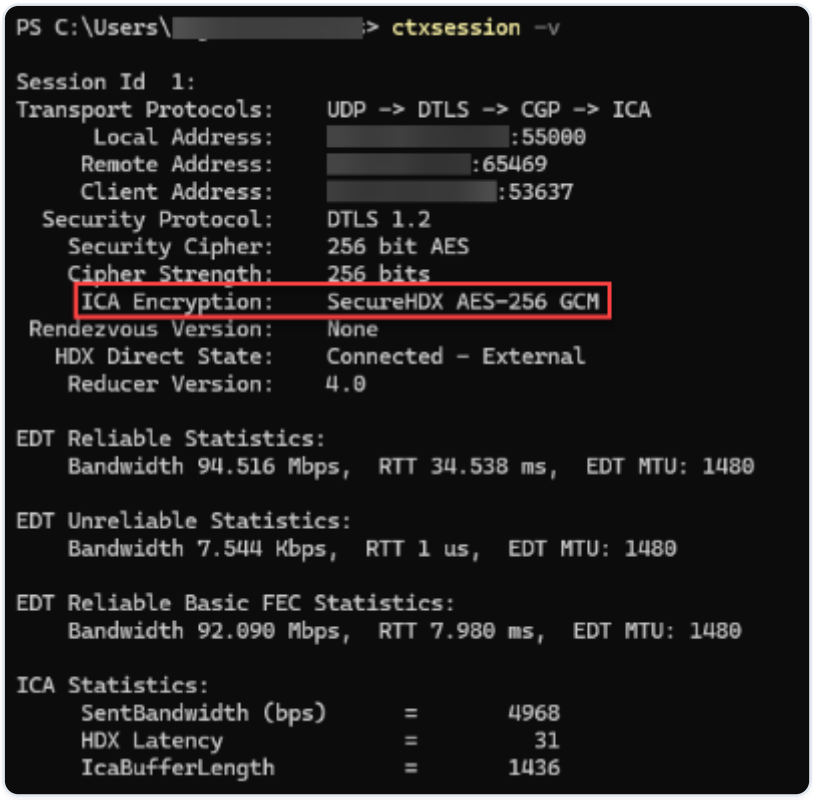
Secure HDX を使用する際の考慮事項は次のとおりです。

- ユーザーが Secure HDX が有効なセッションホストに、その機能をサポートしないクライアントを使用して接続しようとすると、接続は拒否されます。
- Secure HDXでは、(/ja-jp/citrix-workspace/optimize-cvad/service-continuity-for-connectorless.html)のみがサポートされています。標準バージョンのService Continuityを使用している場合、クラウドサービスが停止すると、Secure HDXが有効になっているセッションホストに接続できなくなります。
- Secure HDXが有効になっている場合、Multi-Stream ICAはサポートされません。
- HDXトラフィックの検査に依存するサードパーティソリューションを使用している場合、Secure HDXを有効にするとHDXトラフィックが暗号化されるため、それらのソリューションは機能しなくなります。

トラブルシューティング

Secure HDXがアクティブであることを確認するには、VDAマシンで`ctxsession.exe`ユーティリティを使用できます。

`CtxSession.exe`ユーティリティを使用するには、セッション内でコマンドプロンプトまたはPowerShellを開き、`ctxsession.exe -v`を実行します。Secure HDXが使用されている場合、ICA Encryptionには`SecureHDX AES-256 GCM`と表示されます。



セッションでSecure HDXが有効にならない場合

- 使用中のVDAバージョンがシステム要件に従ってこの機能をサポートしていることを確認してください。
- Secure HDXを有効にするポリシーがVDAに適用されており、この機能を無効にする優先度の高い他のポリシーがないことを確認してください。
- Secure HDXを構成したときにセッションホストがすでに実行されていた場合は、変更を有効にするためにマシンを再起動してください。

ネットワーク テレメトリ

ネットワークメトリックは、Citrixセッションのトラブルシューティングにとって重要です。なぜなら、Citrixセッションのパフォーマンスと安定性は、基盤となるネットワークの状態に大きく依存しているからです。ローカルアプリケーションとは異なり、Citrixセッションはインタラクティブなデスクトップまたはアプリケーションのエクスペリエンスをネットワーク経由でストリーミングします。これは、ネットワークの不安定性やボトルネックがユーザーのパフォーマンス認識に直接影響することを意味します。

Citrix MonitorおよびDirectorで利用可能なネットワークメトリックの詳細については、セッションパフォーマンスの問題を診断するを参照してください。

システム要件

ネットワークテレメトリを使用するためのシステム要件は次のとおりです。

- コントロールプレーン
  - シトリックス DaaS
  - シトリックス バーチャルアプリ アンド デスクトップ 2503 以降
- バーチャル デリバリー エージェント (VDA)
  - Windows: バージョン2503以降
  - Linux: バージョン2507以降
  - Mac: バージョン2507以降
- Workspaceアプリ
  - Windows: バージョン2503以降
  - Linux: バージョン2508以降
  - Mac: バージョン 2505 以降
- アクセス層
  - シトリックス ワークスペース
  - シトリックス ストアフロント 2402 以降
  - シトリックス ゲートウェイ サービス
  - Citrix NetScaler Gateway 14.1 Build 47.46 以降 (EDT サポートには 14.1 Build 72.57 以降が必要)

ネットワーク要件

Citrix Gateway Service を使用している場合、追加のネットワーク要件はありません。ただし、NetScaler Gateway を使用している場合は、ネットワークテレメトリを使用するための追加要件があり、それらを以下に示します。

セッションホスト

セッションホストに Windows Defender ファイアウォールなどのファイアウォールがある場合、NetScaler Gateway からの接続に対して以下の受信トラフィックを許可する必要があります。

説明	送信元	プロトコル	ポート
NetScaler Gateway からの接続	NetScaler SNIP	UDP	443
NetScaler Gateway からの接続	NetScaler SNIP	TCP	443

注:

VDA インストーラーは、Windows Defender ファイアウォールに適切な受信規則を追加します。別のファイアウォールを使用する場合は、上記の規則を追加する必要があります。

内部ネットワーク

内部ネットワークのファイアウォール要件は次のとおりです。

説明	プロトコル	送信元	ソースポート	宛先	宛先ポート
NetScaler Gatewayからの接続	UDP	NetScaler SNIP	1024-65535	VDAネットワーク	443
NetScaler Gatewayからの接続	TCP	NetScaler SNIP	1024-65535	VDAネットワーク	443

構成

ネットワークテレメトリはデフォルトで無効になっています。この機能は、Studio の Citrix ポリシーで以下の設定を使用して構成できます。

- **ネットワークテレメトリ:** この機能を有効にするか無効にするかを定義します。

考慮事項

ネットワークテレメトリを使用する際の考慮事項は以下のとおりです。

- 転送中の監視データのセキュリティを確保するため、ネットワークテレメトリが有効になっている場合、NetScaler Gateway からセッションホストへの接続は TLS/DTLS で保護されます。その結果、接続はデフォルトで UDP 443 (EDT 経由の HDX) および TCP 443 (TCP 経由の

HDX) ポートで確立されます。ポート番号を変更する場合は、(/ja-jp/citrix-virtual-apps-desktops/current-release/policies/reference/hdx-registry-settings.html#secure-connection-port) を参照してください。

- セッション接続のネットワークレベル暗号化を容易にするために、自己管理証明書が使用されます。証明書管理の詳細については、(/ja-jp/citrix-daas/hdx-transport/certificate-management) を参照してください。ネットワークテレメトリを有効にしても、HDX Direct は有効にならないことに注意してください。
- EDT 用のネットワークテレメトリは、NetScaler バージョン **14.1 Build 72.57** 以降でサポートされています。古いバージョンの NetScaler を使用している場合、ネットワークテレメトリが有効になっていると、セッションは強制的に TCP を使用します。

仮想チャネル許可リスト

仮想チャネル許可リストは、Citrix以外の仮想チャネルのうち、どのチャネルを環境で許可するかを制御できる機能です。デフォルトでは、仮想チャネル許可リスト機能は有効になっています。その結果、Citrix Virtual Apps and Desktops™セッションでは、Citrix仮想チャネルのみが開くことが許可されます。自社製またはサードパーティ製のカスタム仮想チャネルを使用する必要がある場合は、それらを明示的に許可リストに追加する必要があります。

構成

仮想チャネル許可リストはデフォルトで有効になっています。この機能は、Citrixポリシーの以下の設定を使用して構成できます。

- **仮想チャネル許可リスト**: この機能を有効または無効にし、仮想チャネルをリストに追加します。
- **仮想チャネル許可リストログのスロットリング**: 仮想チャネル許可リストのイベントログのスロットリング期間を設定します。
- **仮想チャネル許可リストのログ記録**: 仮想チャネル許可リストのログレベルを設定します。

仮想チャネルを許可リストに追加する

仮想チャネルを許可リストに追加するには、次の情報が必要です。

1. コードで定義されている仮想チャネル名。最大7文字です。例: `CTXCVC1`。
2. VDAマシン上で仮想チャネルを開くプロセスのパス。例: `C:\Program Files\Application\run.exe`。

必要な情報が揃ったら、仮想チャネル許可リストポリシー設定を使用して、仮想チャネルを許可リストに追加する必要があります。リストに仮想チャネルを追加するには、仮想チャネル名の後にコンマ、そして仮想チャネルにアクセスするプロセスのパスを入力します。複数のプロセスがある場合は、各プロセスをコンマで区切って追加できます。

単一プロセスの場合

前の例を使用して、以下のエントリをリストに追加します。

```
CTXCVC1,C:\Program Files\Application\run.exe
```

複数のプロセスの場合

複数のプロセスがある場合は、次のエントリをリストに追加します。

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application\run2.exe
```

ワイルドカードの使用

ワイルドカード (*) の使用がサポートされています。アプリケーションのバージョンに基づいてディレクトリ名や実行可能ファイル名が変更される場合、またはサードパーティコンポーネントがユーザープロファイルにインストールされている場合に、ワイルドカードを使用できます。

次のシナリオでワイルドカードを使用できます。

- 完全なディレクトリ名を置き換える場合。 例: `C:\Program Files\Application*\run1.exe`
- ディレクトリ名の一部を置き換える場合。 例: `C:\Program Files\Application\v*\run1.exe`
- 実行可能ファイル名を置き換える場合。 例: `C:\Program Files\Application\v1.2*.exe`
- 実行可能ファイル名の一部を置き換える場合。 例: `C:\Program Files\Application\v1.2\run*.exe`

次の制限が適用されます。

- ワイルドカードは、単一のディレクトリを置き換えるためにのみ使用できます。たとえば、実行可能ファイルが `C:\Program Files\Application\v1.2\run1.exe` にある場合
  - 許可: `C:\Program Files\Application*\run1.exe`
  - 不許可: `C:\Program Files*\run1.exe`

- エントリにはファイル名拡張子を含める必要があります。
  - 許可: `C:\Program Files\Application\v1.2*.exe`
  - 不許可: `C:\Program Files\Application\v1.2*`
- すべてのパスはローカルである必要があります。

注:

- ネットワークパスは許可されていません。
- ワイルドカードサポートは、Citrix Virtual Apps and Desktops™ 2206から利用可能です。
- ワイルドカードのサポートは、Citrix Virtual Apps and Desktops 2203 LTSRのCU2から利用可能です。

システム環境変数の使用

許可リスト内の信頼されたプロセスの定義を簡素化するために、システム環境変数を使用できます。`%programfiles%`、`%programfiles(x86)%`、`%systemdrive%`、`%systemroot%`などの標準変数を使用できます。

システムレベルで定義されている限り、カスタム環境変数も使用できます。

以下の例は、標準の環境変数を示しています。

- `%programfiles%\Application\v1.2\run.exe`
- `%programfiles%\Application*\run.exe`
- `%programfiles(x86)%\Application\v1.*\run.exe`

以下の例は、カスタムシステム環境変数を示しています。

- カスタム変数名: `app`
- カスタム変数値: `%programfiles%\Application\`
- 許可リストエントリ: `CTXCVC1,%app%\run.exe`

注:

> ユーザー環境変数はサポートされていません。

> 環境変数のサポートは、Citrix Virtual Apps and Desktopsバージョン2209以降で利用可能です。

仮想チャネル名とプロセスを取得する

仮想チャネルの名前と、VDAマシン上でそれを開くプロセスを取得する最も簡単な方法は、その仮想チャネルを提供した開発者またはサードパーティベンダーから情報を入手することです。

または、機能のログを適用し、以下の手順に従って情報を取得することもできます。

1. カスタム仮想チャネルのクライアントおよびサーバーコンポーネントが配置されたら、仮想アプリケーションまたは仮想デスクトップを起動します。
2. VDAマシンのシステムイベントログで、カスタム仮想チャネルの名前と、それを開こうとしたプロセスを探します。利用可能なイベントの詳細については、「イベントログ」を参照してください。
3. セッションからログアウトします。
4. 特定された仮想チャネルとプロセスに対して、仮想チャネル許可リストポリシー設定にエントリを追加します。
5. マシンを再起動します。
6. VDAが登録されたら、仮想アプリケーションまたは仮想デスクトップを実行して、カスタム仮想チャネルが正常に開くことを検証します。

Citrix仮想チャネルに関する考慮事項

すべての組み込みCitrix仮想チャネルは信頼されており、追加設定なしで開くことができます。ただし、以下の2つの機能は、外部依存関係のため、許可リストに明示的なエントリが必要です。

- マルチメディアリダイレクト
- スカイプ フォー ビジネス 用 HDX RealTime Optimization Pack

マルチメディアリダイレクト

Windows Media Player以外のメディアプレーヤーをシステムメディアプレーヤーとして使用する場合、それを信頼されたプロセスとして許可リストに追加する必要があります。許可リストのエントリには、以下の情報が必要です。

- 仮想チャネル名: `CTXMM`

- プロセス: VDAマシンで使用されるメディアプレーヤーへのパス。例: `C:\Program Files (x86)\Windows Media Player\wmplayer.exe`。
- 許可リストエントリ: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

スカイプ フォー ビジネス 用 HDX RealTime Optimization Pack

許可リストのエントリには、以下の情報が必要です。

- 仮想チャネル名: `CTXRMEP`
- プロセス: VDAマシン内のSkype for Business実行可能ファイルへのパス。これはSkype for Businessのバージョンやカスタムインストールパスの使用によって異なる場合があります。例: `C:\Program Files\Microsoft Office\root\Office16\lync.exe.`.
- 許可リストエントリ: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

サードパーティ製仮想チャネルに関する考慮事項

一部のサードパーティ製仮想チャネルは信頼されており、追加設定なしで開くことが許可されています。その他のすべてのサードパーティ製仮想チャネルは、許可リストに明示的なエントリが必要です。信頼されているサードパーティ製仮想チャネルは次のとおりです。

- マイクロソフト チームズ
- VDI向けZoomミーティング

> **重要:**

> 信頼されているサードパーティ製仮想チャネルは、関連するアプリケーションがデフォルトのインストールパスにインストールされている場合にのみ自動的に信頼されます。アプリケーションが別のパスにインストールされている場合は、仮想チャネルを許可リストに明示的に追加する必要があります。

マイクロソフト チームズ

以下は、Microsoft Teamsの仮想チャネルとプロセスのデフォルトインストールパスです。

- 仮想チャネル名: `MSTEAMS`, `MSTEAM1`, および `MSTEAM2`
- プロセス: `ms-teams.exe`

- デフォルトのインストールパス: `C:\Program Files\WindowsApps\MSTeams.<app version>_x64_8wekyb3d8bbwe\`

Microsoft Teamsの仮想チャネルに関する追加情報は、Microsoftドキュメントで入手できます。

VDI向けZoomミーティング

以下は、Zoom Meetings for VDIの仮想チャネルとプロセスのデフォルトインストールパスです。

- 仮想チャネル名: `ZOOMHDX`, `ZOOMHDC`, `ZOOMPHX`, `ZOOMCVX`, `ZOOMCCX`, `ZOOMAUS`
- プロセス: `Zoom.exe` および `ZoomVDITool.exe`
- 既定のインストールパス:
  - 32ビット: `C:\Program Files (x86)\ZoomVDI\bin\`
  - 64ビット: `C:\Program Files\ZoomVDI\bin\`

Zoom Meetings for VDI 仮想チャネルに関する追加情報は、Zoom ドキュメントで入手できます。

トラブルシューティング

カスタム仮想チャネルが開かない場合は、次の手順を確認してください。

1. 正しいVDAバージョンを使用していることを確認してください。
2. 仮想チャネル許可リストにカスタム仮想チャネルを含むポリシーがVDAに適用されており、この構成を上書きする優先度の高い他のポリシーがないことを確認してください。
3. VDAのイベントログを確認し、報告されている仮想チャネル名が許可リストで定義されているものと一致することを確認してください。
   a. 複数のプロセスがある場合は、仮想チャネルを許可リストに追加するで説明されているように、これらが適切に定義されていることを確認してください。
   b. 定義されたプロセスパスでワイルドカードを使用している場合は、ワイルドカードの使用のガイドラインに従っていることを確認してください。
   c. 定義されたプロセスパスで環境変数を使用している場合は、システム環境変数の使用のガイドラインに従っていることを確認してください。

イベントログ

次のイベントがVDAマシンのイベントログに記録されます。

シングルセッションVDA

次のイベントがシングルセッションVDAマシンのイベントログに記録されます。

ログ名	ID	送信元	レベル	説明
システム	2001	`Picadd`	情報	カスタム仮想チャネル `<vcName>` はプロセス `<processName>` によって開かれました
システム	2002	`Picadd`	警告	カスタム仮想チャネル `<vcName>` はプロセス `<processName>` によって開くことができません
システム	2003	`Picadd`	情報	`<username>` がカスタム仮想チャネル `<vcName>` を開きました
システム	2004	`Picadd`	警告	`<username>` がカスタム仮想チャネル `<vcName>` を開こうとしました
システム	2005	`Picadd`	エラー	ポリシー `<pathInPolicy>` で指定されたパスはプロセスパスに解決できません
システム	2007	`Picadd`	情報	ロードされたプロセスパスは

ログ名	ID	送信元	レベル	説明
				`<processPath>` です
システム	2008	`Picadd`	エラー	VCポリシーパス内の環境変数 `<varName>` が見つかりません

マルチセッションVDA

マルチセッションVDAマシンのイベントログに次のイベントが記録されます:

ログ名	ID	送信元	レベル	説明
システム	13	`Rpm`	情報	カスタム仮想チャネル `<vcName>` はプロセス `<processName>` によって開かれました
システム	14	`Rpm`	警告	カスタム仮想チャネル `<vcName>` はプロセス `<processName>` によって開くことができません
システム	15	`Rpm`	情報	`<username>` がカスタム仮想チャネル `<vcName>` を開きました
システム	16	`Rpm`	警告	`<username>` がカスタム仮想チャネル `<vcName>` を

ログ名	ID	送信元	レベル	説明
				開こうとしました
システム	17	`Rpm`	エラー	ポリシー `<pathInPolicy>` で指定されたパスをプロセスパスに解決できません
システム	18	`Rpm`	情報	ロードされたプロセスパスは `<processPath>` です
システム	19	`Rpm`	エラー	VCポリシーパス内で環境変数 `<varName>` が見つかりません

既知のサードパーティ仮想チャネル

以下は、カスタムCitrix®仮想チャネルを使用する既知のサードパーティソリューションです。このリストには、カスタムCitrix仮想チャネルを使用するすべてのソリューションが含まれているわけではありません。

- カーナー
- ControlUp
- シスコ ウェブエックス チームズ
- シスコ ウェブエックス ミーティングス バーチャルデスクトップ ソフトウェア
- エピック ワープドライブ
- エピック スリングショット
- インプリバタ ワンサイン
- マイクロソフト チームズ
- ミッドマーク IQPath クライアント拡張機能
- ニュアンス PowerMic クライアント拡張機能

- ニュアンス ドラゴン メディカル ネットワーク エディション 360 vSync
- ズーム ミーティングス for VDI
- アルティマ IA-Connect

関連する仮想チャネルを許可リストに追加するための詳細については、ソリューションのベンダーにお問い合わせください。または、仮想チャネル名とプロセスの取得セクションに記載されている手順に従ってください。

DVC用仮想チャネル許可リスト

DVC用仮想チャネル許可リストを使用して、環境で許可されるカスタム動的仮想チャネルを制御できます。デフォルトでは、動的仮想チャネルは許可されていません。動的仮想チャネルが必要な場合は、それらを明示的に許可リストに追加する必要があります。

構成

DVC用仮想チャネル許可リストは、デフォルトで有効になっています。この機能は、Citrix®ポリシーの以下の設定を使用して構成できます。

- DVC用仮想チャネル許可リスト: 機能を有効または無効にし、動的仮想チャネルをリストに追加します。
- 仮想チャネル許可リストのログスロットリング: 仮想チャネル許可リストのイベントログ記録のスロットリング期間を設定します。
- 仮想チャネル許可リストのログ記録: 仮想チャネル許可リストのログレベルを設定します。

許可リストへの動的仮想チャネルの追加

許可リストに動的仮想チャネルを追加するには、次の情報が必要です。

1. クライアント上のDVCプラグインの名前。例: `DvcPlugin1.dll`。
2. DVCリスナーの名前。例: `ListenerName1`。
3. VDAマシン上で動的仮想チャネルにアクセスするプロセスのパス。例: `C:\Program Files\Application\run.exe`。

必要な情報が揃ったら、DVC用仮想チャネル許可リストポリシー設定を使用して、動的仮想チャネルを許可リストに追加する必要があります。リストに動的仮想チャネルを追加するには、セッションホストでDVCにアクセスするプロセスのパスを入力し、その後にコンマ、クライアント側のプラグイン名、コンマ、およびプラグインが使用するリスナーの名前を入力します。複数のリスナー名はコンマで区切って追加できます。

単一リスナーの場合

前の例を使用して、次のエントリをリストに追加します。 `C:\Program Files\App\run1.exe,DvcPlugin1,ListenerName1`

複数リスナーの場合

複数のリスナーがある場合は、リストに次のエントリを追加します。 `C:\Program Files\App\run1.exe,DvcPlugin1,ListenerName1,ListenerName2`

ワイルドカードの使用

ワイルドカード (*) の使用がサポートされています。アプリケーションのバージョンに基づいてディレクトリ名または実行可能ファイル名が変更される場合、またはサードパーティコンポーネントがユーザープロファイルにインストールされている場合に、ワイルドカードを使用できます。

次のシナリオでワイルドカードを使用できます。

- ディレクトリ名を完全に置き換える場合。例: `C:\Program Files\App*\run1.exe`
- ディレクトリ名の一部を置き換える場合。例: `C:\Program Files\App\v*\run1.exe`
- 実行可能ファイル名を置き換える場合。例: `C:\Program Files\App\v1.2*.exe`
- 実行可能ファイル名の一部を置き換える場合。例: `C:\Program Files\App\v1.2\run*.exe`

次の制限が適用されます。

- ワイルドカードは、単一のディレクトリを置き換えるためにのみ使用できます。たとえば、実行可能ファイルが `C:\Program Files\App\v1.2\run1.exe` にある場合
  - 許可: `C:\Program Files\App*\run1.exe`
  - 不許可: `C:\Program Files*\run1.exe`
- エントリにはファイル名拡張子を含める必要があります。
  - 許可: `C:\Program Files\App\v1.2*.exe`
  - 不許可: `C:\Program Files\App\v1.2*`
- すべてのパスはローカルである必要があります。

デバイス

HDX™は、あらゆる場所のあらゆるデバイスで高精細なユーザーエクスペリエンスを提供します。デバイスセクションの記事では、以下のデバイスについて説明します。

- スキャン
- 汎用USBデバイス
- クライアントドライブマッピング
- モバイルおよびタッチスクリーンデバイス
- シリアルデバイス
- 特殊キーボード
- Webカメラ

最適化されたUSBデバイスと汎用USBデバイス

最適化されたUSBデバイスとは、Citrix Workspace™アプリが特定のサポートを提供しているデバイスです。たとえば、HDXマルチメディア仮想チャネルを使用してWebカメラをリダイレクトする機能などです。汎用デバイスとは、Citrix Workspaceアプリで特定のサポートがないUSBデバイスです。

デフォルトでは、汎用USBリダイレクトは、汎用モードに設定しない限り、最適化された仮想チャネルサポートを持つUSBデバイスをリダイレクトできません。

一般的に、USBデバイスは汎用モードよりも最適化モードの方が優れたパフォーマンスを発揮します。ただし、最適化モードではUSBデバイスが完全な機能を持たない場合があります。その機能に完全にアクセスするには、汎用モードに切り替える必要があるかもしれません。

USB大容量記憶装置では、Citrix®ポリシーによって制御されるクライアントドライブマッピングまたは汎用USBリダイレクト、あるいはその両方を使用できます。主な違いは次のとおりです。

汎用USBリダイレクトとクライアントドライブマッピングポリシーの両方が有効になっていて、セッション開始前または開始後にマスストレージデバイスが挿入された場合、そのデバイスはクライアントドライブマッピングを使用してリダイレクトされます。

これらの条件が真の場合、マスストレージデバイスは汎用USBリダイレクトを使用してリダイレクトされます。

- 汎用USBリダイレクトとクライアントドライブマッピングポリシーの両方が有効になっている。
- デバイスが自動リダイレクト用に構成されている。
- セッション開始前または開始後にマスストレージデバイスが挿入される。

詳細については、`<http://support.citrix.com/article/CTX123015>`を参照してください。

機能	クライアントドライブマッピング	汎用USBリダイレクト
デフォルトで有効	はい	いいえ
読み取り専用アクセスを構成可能	はい	いいえ
暗号化されたデバイスアクセス	はい、仮想セッションでデバイスにアクセスする前に暗号化が解除されている場合。	シトリックス バーチャル デスクトップ™ のみ

スキャン

スキャナーは、画像、印刷されたテキスト、手書き文字、またはオブジェクトを光学的にスキャンし、デジタル画像に変換するデバイスです。

スキャナーを使用しており、お使いのコンピューターがWindowsを実行している場合、WIAスキャナードライバーを使用している可能性が高いです。このドライバーは、コンピューターとスキャナー間の通信を担当します。

- **Windows Image Acquisition** (WIA) は、ソフトウェアがスキャナーなどのイメージングハードウェアと通信できるようにする、Microsoft のドライバーモデルおよびアプリケーションプログラミングインターフェイス (API) です。
- **TWAIN** (Windows および Mac) は、標準インターフェイスを提供することでスキャナーとアプリケーションを接続する、もう1つのスキャンプロトコルです。TWAIN を使用すると、アプリケーションは TWAIN 準拠デバイス (スキャナー、デジタルカメラなど) から画像を取得できます。
- **SANE:** スキャンプロトコルは、ソフトウェアアプリケーションがイメージスキャナーと通信し、制御できるようにするための一連の標準とガイドラインです。SANE は **S**canner **A**ccess

Now **E**asy の略で、そのプロトコルは、異なるコンピューターシステムで実行されているソフトウェアによってスキャナーハードウェアがどのようにアクセス、管理、制御されるかを定義します。

TWAINリダイレクト

はじめに

ユーザーは、Citrix HDX™セッション内のアプリケーションから、クライアントエンドポイントに接続されたTWAIN準拠のスキャナーを使用してドキュメントをスキャンできます。Citrixスキャンモジュールは、スキャン要求をクライアントエンドポイントにリダイレクトして処理します。完了すると、スキャンされた情報はVDAホストに送り返されます。

要件

Citrixコントロールプレーン

- シトリックス仮想アプリおよびデスクトップ™ 1912 以降
- シトリックス DaaS™

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - ウィンドウズ 11
  - ウィンドウズ サーバー 2022 以降
- VDA
  - バージョン1912以降
- アプリケーション
  - 32ビットアプリケーション
  - 64ビットアプリケーション

> **注:**

- セッションホストで64ビットアプリケーションのスキャン機能を有効にするには、64ビットTWAINデータソースマネージャー（twaindsm.dll）が必要です。このコンポーネントはオペレーティングシステムによってプリインストールされていません。
- 64ビットスキャンアプリケーションにこのファイルが含まれていない場合は、アプリケーションベンダーに連絡して64ビットのtwaindsm.dllを入手してください。
- 入手後、管理者はファイルをセッションホストの**System32**フォルダーに手動でコピーし、マシンを再起動する必要があります。

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - ウィンドウズ 11
- Workspace アプリ
  - Windows: バージョン1912以降
- スキャナー
  - TWAIN準拠スキャナー
  - クライアントエンドポイントにTWAINドライバーをインストールする

構成

TWAINリダイレクトはデフォルトで有効になっています。TWAINリダイレクトを構成し、スキャンエクスペリエンスを最適化するために、以下のポリシー設定が利用可能です。

- **クライアントTWAINデバイスリダイレクト:** TWAINリダイレクトを有効または無効にするには。
- **TWAIN圧縮レベル:** クライアントからVDAに転送される画像の圧縮レベルを設定します。

詳細については、TWAINデバイスポリシー設定を参照してください。

トラブルシューティング

TWAINリダイレクト機能は、公開されているテストアプリTwackerでテストできます。このアプリは、このURLからダウンロードできます。

HDXセッション内でTWAIN機能を検証するには、以下の手順に従ってください。

1. VDAホストに**Twacker**をインストールします。
2. **Twacker**（32ビットまたは64ビットバージョン）を起動します。
3. **File > Select Source**をクリックし、リストからスキャナーを選択します。
4. **File > Acquire**をクリックします。
5. **Scan button**をクリックして、スキャナーをテストします。

Twackerが正常にスキャンできる場合、**Citrix Virtual Apps and Desktops™**のセットアップが以下であることを確認できます。

- TWAINリダイレクトを使用するように正しく構成されている
- すべてのローカルクライアントデバイス要件を満たしている

特定のアプリケーション内でスキャンに関する問題が引き続き発生する場合は、ソフトウェアの問題である可能性が高いです。

WIAデバイス

デジタルカメラやスキャナーなどのWIAデバイスは、WIAフレームワークを使用して、サーバーでホストされている画像処理アプリケーションと通信します。

前提条件

- スキャナーはWIA準拠である必要があります。
- WIAドライバーをローカルデバイスにインストールします。サーバーには必要ありません。
- スキャナーをローカルに接続します（例：USB経由）。
- スキャナーがローカルのWindows Image Acquisitionサービスを使用しており、TWAINドライバーを使用していないことを確認してください。
- テストに使用されるユーザーアカウントに、ICA®セッション内の帯域幅を制限するポリシーが適用されていないことを確認してください。たとえば、クライアントUSBリダイレクト帯域幅制限などです。

要件

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - ウィンドウズ 11

- ウィンドウズ サーバー 2022 以降

- VDA
  - バージョン2511以降

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - ウィンドウズ 11
- Workspace アプリ
  - Windows: バージョン2411以降

構成

WIAリダイレクトはデフォルトで無効になっています。Citrix®ポリシーで次の設定を有効にできます。

- WIAリダイレクト: この設定は、ユーザーがユーザーデバイス上のWIAデバイスにアクセスすることを許可または禁止します。

Citrix Virtual Apps and Desktops 2511以降では、VDA側のレジストリに追加の変更は必要ありません。

既知の問題

ポリシー設定については、「WIAデバイスポリシー設定」を参照してください。

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

はじめに

ユーザーは、ChromeOSおよびLinuxエンドポイントからCitrix®セッション内のTWAINアプリケーションからドキュメントをスキャンできます。ユーザーがアプリケーションからドキュメントをスキャンしようとすると、Citrixスキャンモジュールは要求をクライアントエンドポイントにリダイレクトしてスキャナーからのスキャンを実行し、スキャンが完了するとファイルはVDAに送信されます。

要件

Citrixコントロールプレーン

- Citrix Virtual Apps and Desktops™ バージョン 2411 以降
- シトリックス DaaS™

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - ウィンドウズ 11
  - Windows Server 2019 以降のバージョン
- VDA
  - バージョン2411以降

クライアントデバイス

- オペレーティングシステム
  - ChromeOS v129以降
- Workspace アプリ
  - ChromeOS: バージョン2409以降
  - Linux: バージョン2508.10以降
- スキャナー
  - スキャナーは、基盤となるクライアントオペレーティングシステムでサポートされている必要があります。
  - USB経由でクライアントエンドポイントにローカルに接続されている必要があります。

構成

この機能を有効にするための追加設定は不要です。この機能はデフォルトで有効になっています。

> **注:**

この機能を無効にするには、Web Studio/DaaSコンソールを開きます。SANEスキャナーリダイレクトポリシー設定を「禁止」に設定します。

トラブルシューティング

イベントログ

管理者は、さまざまなスキャン関連のイベントメッセージを表示できます。

以下に、さまざまなスキャン関連操作のためにVDAホストのイベントビューアーに記録されるイベントメッセージを示します。これらは、Windowsログの「アプリケーション」セクションで、イベントソースとしてHDX™ Scannerを使用して表示できます。

イベントID	イベントテキスト	説明
2	AllowScannerSANERedirectionポリシーが無効になっています。スキャナーはリダイレクトされません。	SaneRedirectionポリシーが無効になっていることを示します。
3	スキャン詳細: ページ数 - '[pages]'、アプリケーション - '[application]'、スキャナー - '[scanner]'、ユーザー - '[user]'、ページあたりの平均時間 - '[time]' ミリ秒。	スキャンが完了したときに生成されます。
101	スキャンするページが見つかりません。	ドキュメントが検出されないときに生成されます。
102	スキャン失敗 - デバイスのドキュメントフィーダーが詰まっています。	スキャナーのドキュメントフィーダーでの紙詰まりによりスキャンが失敗したときに生成されます。
103	スキャン失敗 - '[failure]'。スキャナーアプリケーションを閉じて再起動してください。	サポートされていない操作、ファイル終端エラー、アクセス拒否エラーなどのエラーによりスキャンが失敗したときに生成されます。

イベントID	イベントテキスト	説明
104	アプリケーションでメモリ障害が発生しました。アプリケーションを再起動してください。	メモリ不足によりスキャンが失敗した場合に生成されます。
201	ユーザーによってスキャン操作がキャンセルされました。	ユーザーによってスキャン操作がキャンセルされた場合に生成されます。
202	スキャン中にセッションが切断されました。	スキャン中にHDXセッションが切断された場合に生成されます。
203	'[capability]' のTWAINとSANE間の変換はサポートされていません。スキャナー/アプリケーションがサポートされているか確認してください。	指定された機能のTWAINとSANE間の変換がサポートされていないことを示します。
205	スキャナー '[scanner]' をアクティブに設定できませんでした。スキャナーの電源が入っていて接続されているか確認してください。	スキャナーへの接続を開くのに失敗した場合に生成されます。
206	スキャナーが見つかりません。スキャナーの電源が入っていて、接続されているか確認してください。	クライアントエンドポイントでスキャナーが検出されない場合に生成されます。

既知の制限事項

1. ネットワーク認証されたスキャナーはサポートされていません。
2. VDA上のFujitsu Paperstreamアプリなど、一部の独自スキャンアプリケーションでは、リダイレクトされたスキャナーがサポート対象として表示されない場合があります。
3. ネイティブUIを使用する場合、ページ幅、ページ高さ、用紙サイズ、明るさ、コントラストなど、一部のスキャナー設定は、サードパーティAPIの制限により尊重されない場合があります。

USB デバイス

はじめに

汎用USBリダイレクト機能により、USBデバイスをクライアントマシンからHDX™セッションにリダイレクトでき、エンドユーザーはHDXセッションで幅広い汎用USBデバイスを操作できます。これは、最適化されたサポートがない、または不適切な特殊デバイスを使用する必要があるシナリオで役立ちます。

> **注:**
>
> 仮想チャネルサポート用に最適化されていないUSBデバイスは、生のUSBリダイレクトを使用して汎用USB仮想チャネルにフォールバックします。

仕組み?

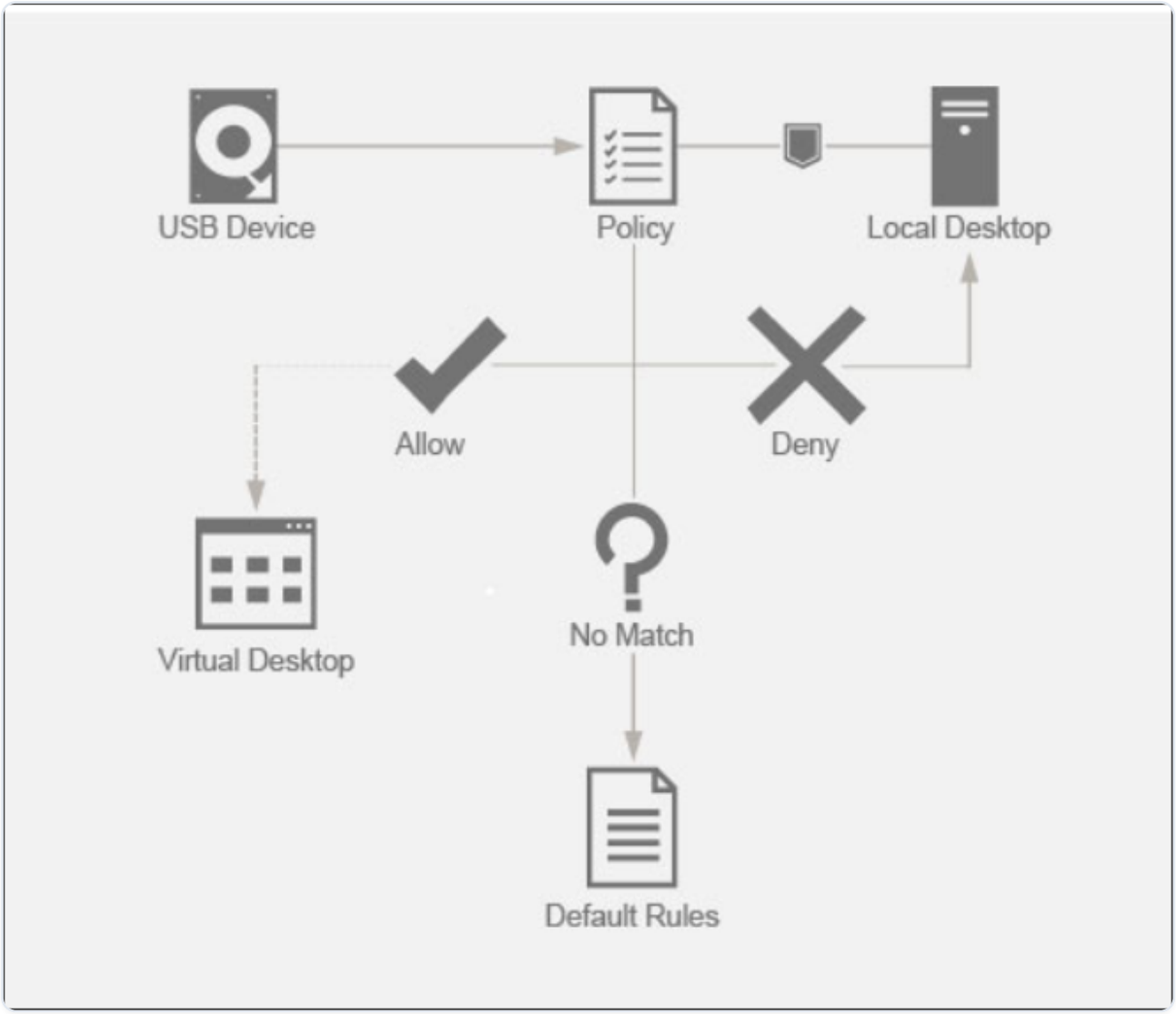
汎用USBリダイレクトは低レベルで機能し、クライアントマシンとXenDesktop®仮想デスクトップ間でUSB要求および応答メッセージをリダイレクトします。

クライアントマシンに互換性のあるデバイスドライバーが必要なくなり、ドライバーは仮想デスクトップでのみサポートされることが期待されます。USBリダイレクトポリシー規則は、DDCポリシー規則が評価および適用された後、クライアント側のポリシーとデフォルト規則が尊重されるように、特定の優先順位に従います。これにより、Citrix管理者は、不正なデバイスや偽装されたデバイスがセッション内にリダイレクトされるのを防ぐことができます。

さらに、リモートセッションへのアクセスを試みる不正なデバイスのイベントログを監査およびフラグ付けでき、管理者はデータ漏洩を防ぐための追加措置を講じることができます。

ユーザーがUSBデバイスを接続すると、セッションホストは一致が見つかるまで各ポリシー規則と連続して照合します。任意のデバイスに対する最初の一致が最終的なものと見なされます。

- 最初の一致が許可規則である場合、デバイスは仮想デスクトップにリダイレクトされます。
- 最初の一致が拒否規則である場合、デバイスはセッションにリダイレクトされず、ローカルユーザーデバイスでのみ使用できます。一致が見つからない場合は、デフォルト規則が使用されます。



汎用USBリダイレクトとの互換性

以下のCitrix Workspace™アプリは、汎用USBリダイレクトをサポートしています:

- Citrix Workspaceアプリ for Windows。詳しくは、Citrix Workspaceアプリ for Windowsを参照してください。
- Citrix Workspaceアプリ for Mac。詳しくは、Citrix Workspaceアプリ for Macを参照してください。
- Citrix Workspaceアプリ for Linux。詳しくは、Citrix Workspaceアプリ for Linuxを参照してください。
- Chrome OS 向け Citrix Workspace アプリについては、Citrix Workspace app for Chromeを参照してください。

Citrix Workspace アプリのバージョンについては、Citrix Workspace app feature matrixを参照してください。

構成

USBリダイレクトはデフォルトで無効になっています。Citrix®ポリシーで以下の設定を使用して、汎用USBリダイレクトを構成できます。

- **クライアントUSBデバイスリダイレクト**: USBリダイレクトを有効または無効にする
- **クライアントUSBデバイスリダイレクト規則**: 特定のデバイスアクション、つまり特定のデバイスへのアクセスを許可または拒否するように指定する
- **クライアントUSBデバイスリダイレクト規則（バージョン2）**: USBデバイスのフィルタリング、分割、自動接続の規則を指定する
- **クライアントUSBデバイス最適化規則**: 最適化を無効にするか、最適化モードを変更する
- **既存のUSBデバイスの自動接続を許可する**: HDX™セッションの開始時にクライアントエンドポイントに接続されている既存のUSBデバイスの自動接続を許可または防止する
- **新しく接続されたUSBデバイスの自動検出を許可する**: HDXセッション中にクライアントエンドポイントに接続されるUSBデバイスの自動接続を許可または防止する

詳細については、「USBポリシー設定」を参照してください。

USBリダイレクトの構成方法

デフォルトでは、USBリダイレクト構成は無効になっています。使用するには、USBリダイレクトポリシーと特定のリダイレクト規則をDDCで有効にして構成する必要があります。

> **注:**
>
> バージョン2212より前のコンポーネントを使用している場合、またはLinux/Mac版Workspaceアプリを使用している場合は、USBリダイレクトの構成方法の詳細について「レガシーUSBリダイレクト構成」を参照してください。

汎用USBリダイレクトの有効化

1. **Citrix Web Studio™ポリシー**を開き、**［ポリシー］**タブをクリックします。
2. **［ポリシーの作成］をクリックし、［ICA®］>［USBデバイスポリシー］**を展開します。
3. **クライアントUSBデバイスリダイレクトポリシー**を編集します。
4. 「**許可**」を選択し、「**保存**」をクリックします。

USBリダイレクトポリシー規則の作成

ユーザーがUSBデバイスをVirtual Desktopにリダイレクトしようとすると、一致が見つかるまで各USBポリシー規則に対して順にチェックされます。いずれかのデバイスに対する最初の一致が最終と見なされます。最初の一致が**許可**規則である場合、一致したデバイスは仮想デスクトップにリダイレクトが許可されます。最初の一致が**拒否**規則である場合、一致したデバイスはローカルデスクトップでのみ利用可能です。一致が見つからない場合は、デフォルトの規則が使用されます。

デバイス規則

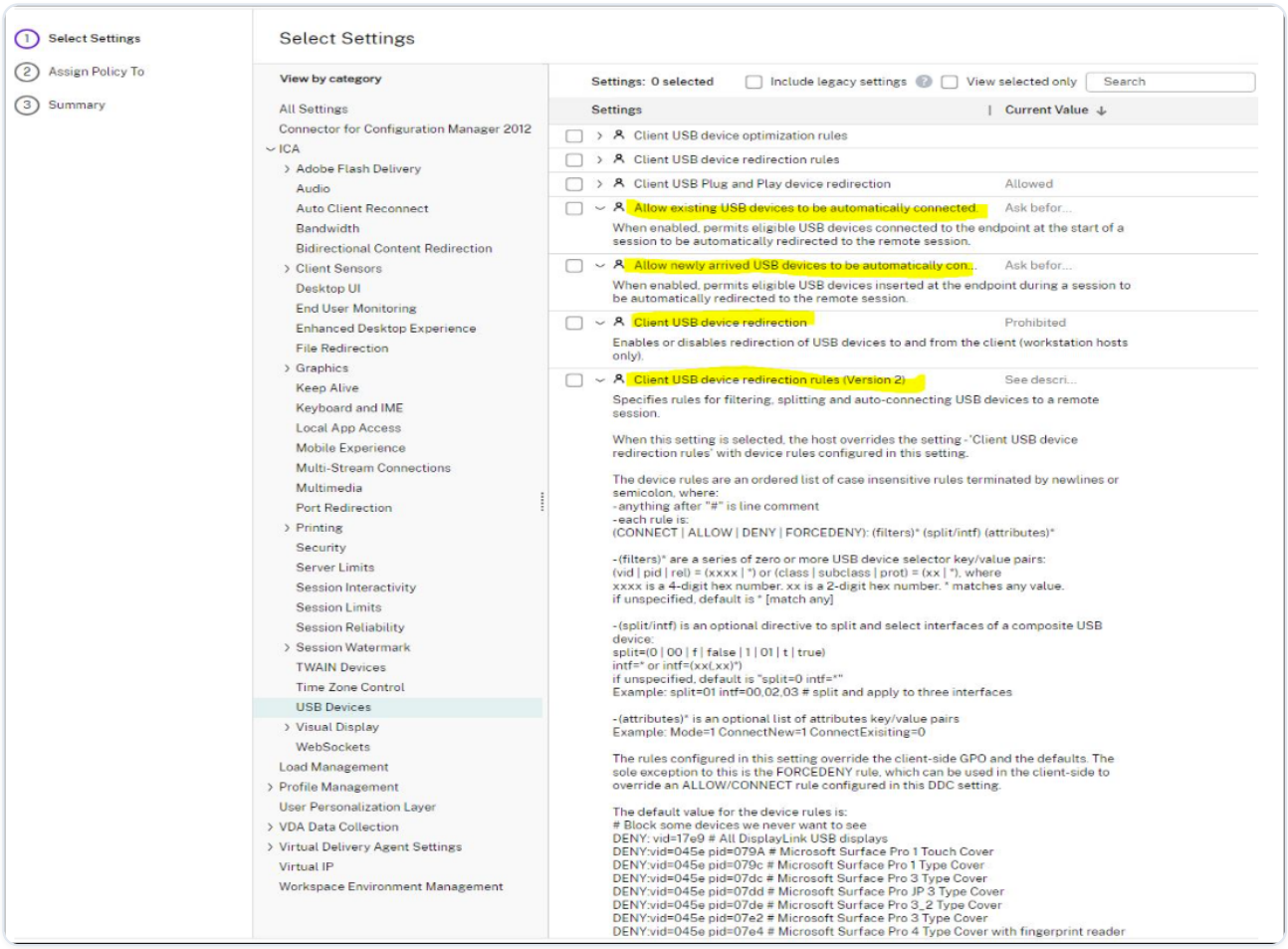
通常のUSBデバイスと同様に、ポリシーまたはエンドポイント上のクライアントCitrix Workspace™ app構成で設定されたデバイス規則により、転送するデバイスが選択されます。Citrix Workspace appはこれらの規則を使用して、どのUSBデバイスをリモートセッションへの転送を許可または防止するかを決定します。

各規則は、アクションキーワード（**Allow、Connect、またはDeny**）、コロン（:）、およびエンドポイントのUSBサブシステムにある実際のデバイスと一致する0個以上のフィルターパラメーターで構成されます。これらのフィルターパラメーターは、すべてのUSBデバイスが自身を識別するために使用するUSBデバイス記述子メタデータに対応しています。

デバイスルールはクリアテキストであり、各ルールは1行に記述され、#文字の後にオプションのコメントが続きます。ルールは上から下へ（優先順位の降順で）照合されます。デバイスまたは子インターフェイスに一致する最初のルールが適用されます。同じデバイスまたはインターフェイスを選択する後続のルールは無視されます。

例: 許可: VID=1050 PID=0421 #デバイス1 **例:** 接続: VID=xxxx PID=yyyy Class=03 #デバイス2

キーワード	説明
CONNECT	このキーワードを使用して、USB仮想チャネル経由でのデバイスのリダイレクトを許可し、セッション起動時および挿入時の自動リダイレクトを有効にします。
ALLOW	このキーワードを使用して、USB仮想チャネル経由でのデバイスのリダイレクトを許可します。
DENY	このキーワードを使用して、USB仮想チャネル経由でのデバイスのリダイレクトを拒否します。



DDC でポリシーを設定する:

1. **Citrix Web Studio ポリシー**」を開き、「**ポリシー**」タブをクリックします。
2. **ポリシーの作成**」をクリックし、「**ICA > USB デバイス ポリシー**」を展開します。
3. **クライアント USB デバイス リダイレクト規則**」を編集します (「**バージョン 2**」)。
4. リダイレクトする必要がある各 USB デバイスの説明に記載されている例に基づいて値を設定し、「保存」をクリックします。

   例: 許可: VID=056A PID=00A4 #STU-430 拒否: Class=08 subclass=05 # マスストレージ

> **注:**
>
> Citrix 管理者が「**既定値を使用**」をオンにして「**保存**」をクリックすると、既定の規則は VDA の次のレジストリにあります。

> **注意!**

> レジストリエディターを使用する前に、この記事の最後にある免責事項を参照してください。

> `HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules`

注:

> グループポリシーデバイス規則を使用してクライアントデバイスにポリシーを設定することは引き続き可能ですが、CVAD および CWA の新しいバージョンでは不要になりました。

> USB デバイスのレガシー構成については、「レガシー USB リダイレクト構成」を参照してください。

USB デバイスの自動リダイレクトを構成する (オプション)

USB サポートが有効になっている場合、USB デバイスは自動的にリダイレクトされます。また、USB ユーザー設定は、USB デバイスを自動的に接続するように設定されています。すべての USB デバイスをリダイレクトすることが常に最適であるとは限りません。ユーザーは、自動的にリダイレクトされない USB デバイスリストからデバイスを明示的にリダイレクトできます。USB デバイスが一覧表示されたりリダイレクトされたりするのを防ぐには、クライアントエンドポイントまたは DDC ポリシーのいずれかで DeviceRules を使用します。 このポリシーは、DDC、GPO を使用するクライアント、Citrix Workspace Preferences、または CDViewer の タブのいずれかで設定できます。これらのすべての方法は以下で説明されています。

DDC でポリシーを設定する:

USB デバイスの自動リダイレクトを許可するように設定できる DDC 上のポリシーは 2 つあります。

- 既存のUSBデバイスの自動接続を許可する
- 新しく接続されたUSBデバイスの自動接続を許可する

a. 「**Citrix Web Studioポリシー**」を開き、「**ポリシー**」タブをクリックします。

b. 「**ポリシーの作成**」をクリックし、「**ICA > USBデバイスポリシー**」を展開します。

c. 既存のUSBデバイスを自動的に接続することを**許可**する設定を編集します。

d. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクト**」を選択して、「**保存**」をクリックします。

e. 新しく接続されたUSBデバイスを自動的に接続することを**許可**する設定を編集します。

f. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクト**」を選択して、「**保存**」をクリックします。

USBデバイスリダイレクトルールの理解

Citrix Client USBリダイレクトを使用する場合、異なるルールがどのように優先され、適用されるかを理解することが重要です。これは一連の指示のようなものと考えてください。システムは特定の順序でルールをチェックし、特定のデバイスに対して最初に見つかったルールが適用されます。その**同じデバイス**に対してリストのさらに下で見つかった他のルールは無視されます。

デバイスルールが評価される順序は次のとおりです。

- **クライアントUSBデバイスリダイレクトルール（バージョン2）**: このポリシー設定によって構成されたデバイスルールには、最高の優先順位が与えられます。特定のデバイスに対するルールがここで見つかった場合、そのルールが適用され、その特定のデバイスに対する他のルールは考慮されません。
- **クライアントUSBデバイスリダイレクトルール**: 次に、Citrix Studio内のこのレガシー設定で定義されたルールが続きます。バージョン2ポリシーでデバイスのルールが見つからなかった場合、システムはこのポリシー設定で定義されたルールをチェックします。ここでも、デバイスのルールが見つかった場合、それが適用され、システムはその特定のデバイスのルールを探すのを停止します。

> **注:**
>
> 上記のポリシー設定は、Studioで**クライアントUSBデバイスリダイレクトルール（バージョン2）が設定されていない場合、またはCitrix Workspace App for Windows**のバージョンが2212より古い場合にのみ適用されます。

- **クライアント側グループポリシーオブジェクト（GPO）**: 両方のStudioポリシー設定をチェックした後でもデバイスに適用されたルールがない場合、システムはクライアント側グループポリシーオブジェクトを介して構成されたルールに従います。
- **クライアント側レジストリ設定**: 最後に、クライアント側レジストリ設定が最も低い優先順位で適用されます。

この階層により、特定のデバイスに対してより具体的または新しい構成が優先され、USBデバイスリダイレクトを管理するための明確で予測可能な方法が提供されます。階層が評価の順序を決定する一方で、上位レベルでデバイスに対して見つかったルールは、その**同じデバイス**に対する下位レベルでのルールの適用を妨げることを覚えておくことが重要です。 ただし、下位レベルで設定されたルールが完全に無視されるわけではありません。まだルールが適用されていないデバイスについては、引き続き評価されます。

この階層的なアプローチは、**後方互換性**も保証します。Citrix Virtual Apps and Desktops™またはCitrix Workspace appの以前のバージョンからアップグレードする場合、既存のクライアント側構成は保持されます。これにより、企業管理者は、Studioのより高度な**バージョン2デバイスルール**ポリシー設定への移行パスを、即座の中断なしに計画する時間を確保できます。

例:

例えば、ベンダーID (VID) `xxxx` および製品ID (PID) `yyyy` を持つ特定のUSBデバイスがあるとします。

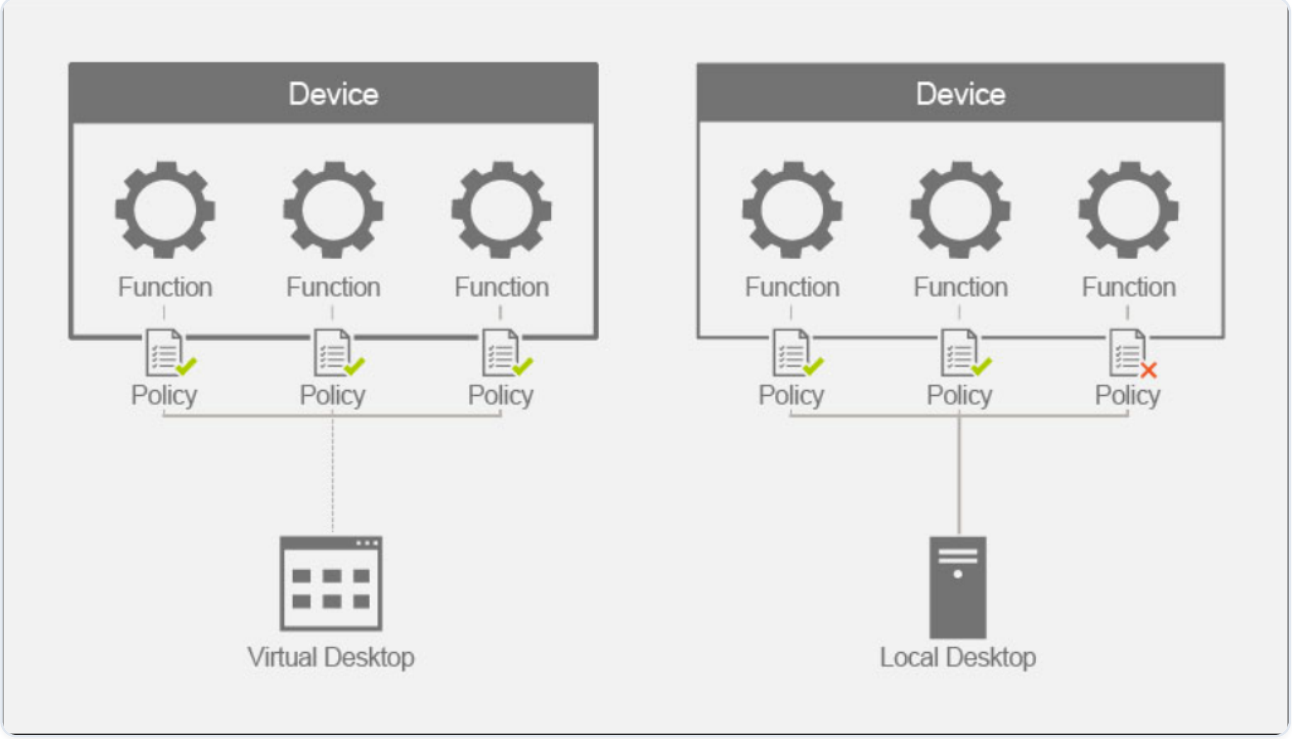
- Citrix Studioの**クライアントUSBデバイスリダイレクトルール (バージョン2)** ポリシー設定には、ルールセット `CONNECT VID=xxxx PID=yyyy` があります。
- 別途、クライアント側の**グループポリシーオブジェクト (GPO)** には、同じデバイスに対して `DENY` ルール `DENY: VID=xxxx PID=yyyy` があります。

このデバイスがクライアントエンドポイントに接続されると、システムはまずバージョン2 Studioポリシーのルールを評価します。システムは `CONNECT` ルール `VID=xxxx PID=yyyy` を見つけます。このルールは最も高い優先順位レベルにあるため、すぐに適用されます。その後、システムはこの特定のデバイスに対するそれ以上のルールを無視します。したがって、クライアント側のGPOに `DENY` ルールが存在するにもかかわらず、それは無視され、デバイスは正常にリダイレクトされます。

複合デバイスとデバイス分割

複合USBデバイスは、コンピューターに接続された複数の独立したUSBデバイスのように機能する単一のデバイスです。単一のUSBコネクターを持ちますが、それぞれ独自の機能セットを持つ複数のインターフェイスをコンピューターに公開できます。ユーザーが複合USBデバイスを接続すると、ホストデバイスはすべての機能（インターフェイス）を各ポリシー規則と照合します。いずれかの機能（インターフェイス）に対する最初の照合が拒否規則である場合、その規則は複合デバイスに対して最終的なものと見なされ、デバイスは拒否されます。機能（インターフェイス）に対する最初の照合が許可規則である場合、ホストデバイスは次の機能（インターフェイス）に対して規則の照合を続行します。ポリシー規則によってどの機能（インターフェイス）も拒否されない場合、複合デバイスは許可されます。複合デバイスに対する最終的な照合が拒否規則である場

合、デバイスはローカルデスクトップでのみ利用可能であり、それ以外の場合は仮想デスクトップにリモート接続されます。一致が見つからない場合は、デフォルト規則が使用されます。



複合デバイスの特定の機能のみを許可するために、デバイスリダイレクト規則（バージョン2）ポリシーで適切な規則を使用して複合デバイスを分割できます。たとえば、FIDO2キーのHID機能のみを使用し、スマートカード機能は使用したくない場合があります。その場合、以下に示すように規則を設定します。

1. Connect: VID=1050 PID=0407 class=03 split=01 intf=00,01 #Yubikeyシリーズ5のFIDO2 HID機能は許可されています。
2. Deny: VID=1050 PID=0407 split=01 intf=02 #Yubikeyシリーズ5のスマートカード機能はブロックされています。

> **ヒント:**
>
> 新しいポリシー規則を作成する際は、USB Webサイトで入手可能なUSBクラスコードを参照してください。

署名パッドの構成

1. VDAホストに適切なデバイスドライバーをインストールします。
2. **Citrix Web Studio™**で**クライアントUSBデバイスリダイレクト**ポリシー設定を有効にします。

3. **クライアントUSBデバイスリダイレクト規則（バージョン2）**ポリシー設定を編集します。
    a. リダイレクトする必要がある署名パッドの**VID**および**PID**情報を設定し、**保存**をクリックします。例：**Connect**: VID=06A8 PID=0057 class=03 #Topaz HSB
4. **クライアントUSBデバイス最適化規則**ポリシー設定を編集します。
    a. モードとその他のデバイス情報を設定します。例：Mode=00000004 VID=06A8 PID=0057 class=03 #キャプチャモードで動作する入力デバイス
5. **既存のUSBデバイスの自動接続を許可する**ポリシー設定を編集します。
6. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクト**」を選択し、「**保存**」をクリックします。
7. ポリシー設定「**新しく接続されたUSBデバイスの自動接続を許可**」を編集します。
8. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクト**」を選択し、「**保存**」をクリックします。

これらの設定が構成されると、以降のセッション起動では、デバイスが自動的にリダイレクトされ、追加のエンドユーザー操作は不要になります。

> **注:**
>
> VIDとPIDを、リダイレクトするデバイスの実際のVIDとPIDに置き換えます。

USBリダイレクトを使用したBloombergキーボードの構成

1. **Citrix Web Studio**でポリシー設定「**クライアントUSBデバイスリダイレクト**」を有効にします。
2. Bloomberg 5キーボードは、ポリシー設定「**クライアントUSBデバイスリダイレクト規則(バージョン2)**」でデフォルトで設定されており、追加の管理者操作は不要です。
3. ポリシー設定「**既存のUSBデバイスの自動接続を許可**」を編集します。
4. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクト**」を選択し、「**保存**」をクリックします。
5. ポリシー設定「**新しく接続されたUSBデバイスの自動接続を許可**」を編集します。
6. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクト**」を選択し、「**保存**」をクリックします。

これらの設定が構成されると、Bloombergキーは以降のHDX™セッションで自動的に表示され、追加のエンドユーザー操作は不要になります。

USBリダイレクトを使用したFIDO2キーの構成

Citrixでは、HDXセッションでFIDO2キーを使用するためにFIDO2リダイレクトを使用することをお勧めします。ただし、代わりにUSBリダイレクトを使用してFIDO2キーをリダイレクトする必要がある状況もあります。これには、クライアント、VDA、またはオペレーティングシステム（例: Windows Server 2016）で機能がサポートされていないためにFIDO2リダイレクトが利用できないシナリオが含まれます。

キーに複数のモードが有効になっている場合でも、HDXセッションでその一部のみを許可したい状況もあります。たとえば、FIDO2とOTPは許可したいが、スマートカードはブロックしたい場合などです。

次の手順は、USBリダイレクトを使用してFIDO2キー（Yubikey vid=1050, pid=0407）を構成する方法を示しています。

1. **Citrix Web Studio**で**クライアントUSBデバイスリダイレクト**ポリシー設定を有効にします。
2. **クライアントUSBデバイスリダイレクト規則（バージョン2）**ポリシー設定を編集します。
    a. セッションでリダイレクトするFIDO2キーの**VID**および**PID**情報と、分割デバイス構成を設定し、**保存**をクリックします。
    b. **接続**: VID=1050 PID=0407 class=03 split=01 intf=00,01 #Yubikeyシリーズ5で許可されるFIDO2 HID機能。
    c. **拒否**: VID=1050 PID=0407 split=01 intf=02 # Yubikeyシリーズ5のスマートカード機能はブロックされました。
3. ポリシー設定**既存のUSBデバイスの自動接続を許可する**を編集します。
4. **デフォルト値を使用**チェックボックスをオフにし、ドロップダウンメニューから**利用可能なUSBデバイスを自動的にリダイレクト**を選択して、**保存**をクリックします。
5. ポリシー設定**新しく接続されたUSBデバイスの自動接続を許可する**を編集します。
6. **デフォルト値を使用**チェックボックスをオフにし、ドロップダウンメニューから**利用可能なUSBデバイスを自動的にリダイレクト**を選択して、**保存**をクリックします。

これらの設定が構成されると、FIDO2キーボードは以降のHDXセッションで自動的に表示され、エンドユーザーによる追加の操作は不要になります。

USBリダイレクトを使用した3Dマウスの構成

現在、3dConnexionスペースマウスドライバーはワークステーションOS（Win 10およびWin11）でのみサポートされています。サーバーOSでは動作しません。以下は、ワークステーションOS（vid=046D, pid=C016）でSpaceMouse Enterpriseを構成する手順です。

1. VDAホストに最新のWindowsドライバーをインストールします。
2. 「**Citrix Web Studio**」で「**クライアントUSBデバイスリダイレクト**」ポリシー設定を有効にします。
3. 「**クライアントUSBデバイスリダイレクト規則**」（**バージョン2**）ポリシー設定を編集します。
    a. リダイレクトする必要がある署名パッドの**VID**と**PID**情報を追加し、**保存**をクリックします。例：**Connect**: VID=046D PID=C016 #SpaceMouse Enterprise
4. 「**クライアントUSBデバイス最適化規則**」ポリシー設定を編集します。
    a. 他のデバイス情報とともにモードを設定します。例：Mode=00000004 VID=046D PID=C016 class=03 #Input device operating in capture mode
5. 「**既存のUSBデバイスの自動接続を許可する**」ポリシー設定を編集します。
6. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクトする**」を選択して、**保存**をクリックします。
7. 「**新しく接続されたUSBデバイスの自動接続を許可する**」ポリシー設定を編集します。
8. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクトする**」を選択して、**保存**をクリックします。

異なるデバイス規則を使用してUSBリダイレクトで2つ以上のデバイスを構成する

複数のデバイスを、異なるデバイス規則を使用してHDXセッション内でリダイレクトできます。管理者は、一方のデバイスを自動的にリダイレクトし、もう一方のデバイスをエンドユーザーがリダイレクトするオプションを提供したい場合があります。以下に、異なる規則で2つのデバイスを構成する手順を示します。

1. 「**Citrix Web Studio**」で「**クライアントUSBデバイスリダイレクト**」ポリシー設定を有効にします。
2. 「**クライアントUSBデバイスリダイレクト規則**」（**バージョン2**）ポリシー設定を編集します。
    a. セッション内で適切なデバイス規則を使用してリダイレクトする2つのデバイスの**VID**と**PID**情報を追加し、**保存**をクリックします。

b. **許可**: VID=0911 PID=0c1c #フィリップス製スピーチマイク.

c. **接続**: VID=06A8 PID=0043 class=03 # Topaz HSB署名パッド

3. ポリシー設定 **既存のUSBデバイスの自動接続を許可する** を編集します。
4. **デフォルト値を使用** チェックボックスをオフにし、ドロップダウンメニューから **利用可能なUSBデバイスを自動的にリダイレクト** を選択し、**保存** をクリックします。
5. ポリシー設定 **新しく接続されたUSBデバイスの自動接続を許可する** を編集します。
6. **デフォルト値を使用** チェックボックスをオフにし、ドロップダウンメニューから **利用可能なUSBデバイスを自動的にリダイレクト** を選択し、**保存** をクリックします。

これらの設定が構成されると、Topaz HSB署名パッドは、その後のHDXセッションで自動的に表示され、追加のエンドユーザー操作は不要になります。一方、Phillipsスピーチマイクは、エンドユーザーがConnection CenterまたはCDViewerのタブでリダイレクトを有効にする必要があります。

トラブルシューティング

USBリダイレクト関連の問題をトリアージするには、次の手順に従ってください。

1. USBリダイレクトのシステム要件が満たされていることを確認します。これには、正しいCVADおよびCWAバージョン、サポートされているデバイス、および検討中のOSプラットフォーム上のデバイスドライバーが含まれます。
2. 環境で使用されているコンポーネントのバージョンとプラットフォームに基づいて、構成が適切であることを確認します。(/ja-jp/citrix-virtual-apps-desktops/current-release/devices/usb-devices/legacy-usb-redirection-configuration.html)を必要とするコンポーネントの詳細については、「レガシーUSBリダイレクト構成」の注記を参照してください。
3. デバイスがクライアントによって列挙されたデバイスの下にリストされていることを確認します。

   a. Workspace Preferencesツールバー: WorkspaceアプリのPreferencesツールバーのタブに列挙されているデバイスを確認します (右クリック **CWAアイコン > 接続センター > 環境設定**... **デバイス**タブをクリック)。

   b. `CtxUsbDiagnostics.exe` (推奨): このツールをコマンドプロンプトウィンドウで実行します。出力には、特定のセッションのデバイス固有の情報が表示されます。デバイスがリダイレクトされているかどうか、またデバイスルールセットがデバイスのリダイレクトを妨げているかどうかがわかります。詳細については、診断ツールを参照してください。

c. USBViewまたはその他のサードパーティツール: エンドポイント/クライアントマシンでUSBViewのようなサードパーティツールを実行し、デバイスがエンドポイントで検出されていることを確認します。

4. デバイスが列挙されている場合:

a. 特定のデバイスについてCtxUsbDiagnosticsツールの出力に拒否ルールが表示される場合は、Studioで構成されているポリシーを確認し、バージョン2ポリシーでルールが正しく設定されていることを確認します。拒否ルールがStudioポリシーに表示されない場合は、クライアント側ポリシー、そして最後にクライアント側デフォルトの順に確認して、一致する拒否ルールを見つけます。

b. CtxUsbDiagnostics出力に拒否ルールがない場合、CWAは設定ウィンドウのタブ (>) で適切なボタンをチェック/クリックすることで、デバイスのリダイレクトを許可します。一度リダイレクトされたデバイスはセッションで利用可能になります。これは、HDXセッションでデバイスマネージャー/USBViewまたは同様のアプリケーションをチェックすることで確認できます。

5. セッション内にデバイスが表示されない場合:

a. VDAホストに正しいデバイスドライバーが正しくインストールされていない可能性があります。VDAホストに最新バージョンのデバイスドライバーが正しくインストールされていることを確認してください。一部のデバイスドライバーはターミナルサーバーマシンではサポートされていないため、リダイレクトしようとしているデバイスがそうでないことを確認してください。

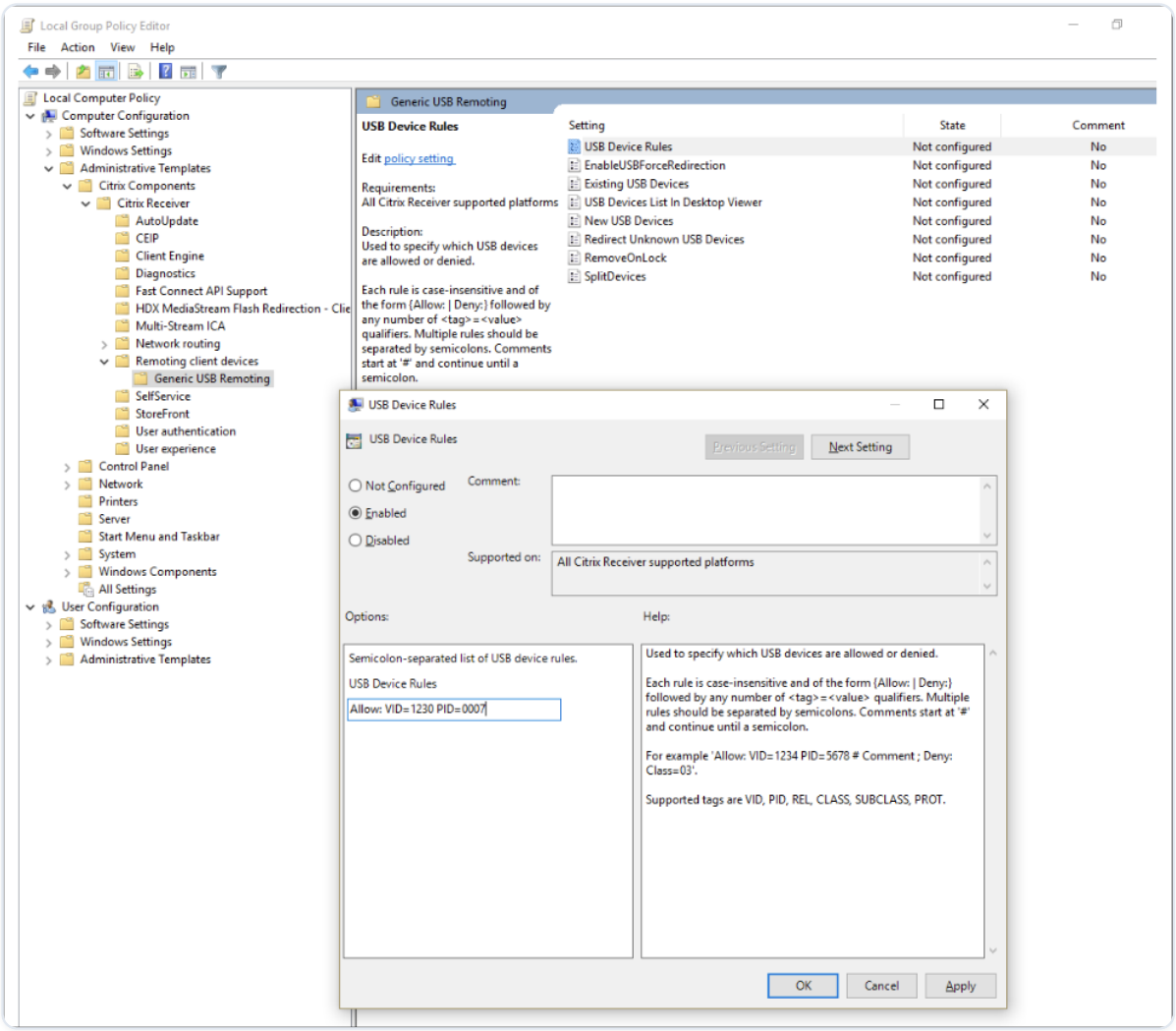
b. デバイスがクライアントエンドポイントで使用されていないことを確認します。一部のデバイスはクライアントエンドポイントにもドライバーのインストールが必要であり、これによりセッションでのリダイレクトが妨げられる可能性があります。

6. クライアントエンドポイントでUSB関連のルールが正しく設定されていることを確認します。

a. **Windows向けCWA：**

i. クライアントのグループポリシー（詳細とSSを追加）が適切に設定されており、Studioで設定されたルールと競合しないことを確認します。

ii. クライアントのレジストリ内のデフォルトルールを検証します。



`(HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules) are appropriately set and not in conflict with the rules set in Studio and client group policy.`.

b. CWA for Linux - CWA for Linux の問題のトリアージについては、CWA for Linux の USB ドキュメントを参照してください。

c. CWA for Mac - CWA for Mac の問題のトリアージについては、CWA for Mac を参照してください。

注:

- TSVDA では、オーディオデバイスはデフォルトで USB リダイレクトの使用がブロックされています。これらのデバイスを使用する推奨される方法は、最適化されたオーディオ VC を使用することです。

- デバイスを分割するための正しいデバイスリダイレクトルールが設定されていても、USB 複合デバイスが自動的に分割されない場合があります。この問題は、デバイスが低電力モードになっているために発生します。このような場合、低電力モードになった子デバイスがデバイスリストに表示されないことがあります。この問題を解決するには、次の回避策を使用できます。
  - セッションを切断し、USB デバイスを挿入して、セッションに再接続します。
  - USB デバイスのプラグを抜き、再度差し込みます。この操作により、デバイスは低電力モードから復帰します。
- バッテリー寿命を最適化するために、USB バッテリーセーバー設定が有効になっている場合があります。クライアントエンドポイントがスリープ状態になると、USB デバイスが切断されることがあります。このようなシナリオでは、セッションでデバイスを再度表示するために、デバイスを切断して再接続する必要がある場合があります。

イベントログ

管理者は、ユーザーがリダイレクトしようとする不正なデバイスを監視し、適切な措置を講じることができるようになりました。以下に、リダイレクトが許可されているデバイスと許可されていないデバイスについて、VDA ホストのイベントビューアーに記録されるイベントメッセージの一部を示します。

Id	1000
Name	UsbEventAcceptDevice
Severity	Informational
Facility	System
Text	The Citrix USB Service allows the USB Device with Product ID: %2, Vendor ID: %3, and Device ID: %4 to be remoted.
Comment	This message logs the device info of a device redirected in an HDX session

Id	1001
Name	UsbEventPolicyRejectsDeviceV1
Severity	Warning
Facility	System
Text	The USB device with Product ID: 0x%2, Vendor ID: 0x%3, and Device ID: 0x%4 is not being redirected because the Citrix USB policy, "DENY: ...%5..." is in effect. If you wish to redirect the device, please set an allow rule that matches the device in the "Client USB device redirection rules" policy in Citrix Studio.
Comment	This message displays a message of the device not getting redirected if a DENY rule is being enforced by the legacy “Client USB device redirection rules” policy rule.
Arguments	

Id	1002
Name	UsbEventPolicyRejectsDeviceV2
Severity	Warning
Facility	System
Text	The USB device with Product ID: 0x%2, Vendor ID: 0x%3, and Device ID: 0x%4 is not being redirected because the Citrix USB policy, "DENY: ...%5..." is in effect. If you wish to redirect the device, please set an allow rule that matches the device in the "Client USB device redirection rules (Version 2)" policy in Citrix Studio.
Comment	This message displays a message of the device not getting redirected if a DENY rule is being enforced by the "Client USB device redirection rules (Version 2)" policy rule. For instance, if the studio policy rule allows an approved set of devices and denies all other devices and an end user tries to create a new rule on the client endpoint via group policy, this event will get logged. This message would be indicative of an unauthorized device redirection attempt.
Arguments	

USB診断ツール

`CtxUsbDiagnostics.exe`は、Citrix管理者がクライアントで発生するUSBデバイスリダイレクトの問題を迅速に診断し解決するのに役立つ、VDA上のコマンドラインツールです。このユーティリティツールは、HDXセッション内でリダイレクトに失敗しているクライアントに接続されたUSBデバイスに関連する構成の問題をトリアージするために必要な重要な情報を収集します。

注：

- ツールがシステムレベルの操作を実行するために必要な権限を持っていることを確認するには、コマンドプロンプトまたはPowershellを管理者として実行する必要があります。

- `CtxUsbDiagnostics.exe`は`C:\Program Files\Citrix\HDX\bin\CtxUsbDiagnostics.exe`にあります。 そして、すでに環境変数の一部です。このパスに移動する必要はなく、昇格された権限でコマンドプロンプトからこのツールを直接実行できます。

要件

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - Windows 11 21H2 以降
  - ウィンドウズ サーバー 2016 以降
- VDA
  - Windows版: Citrix Virtual Apps and Desktops™ バージョン 2311 以降

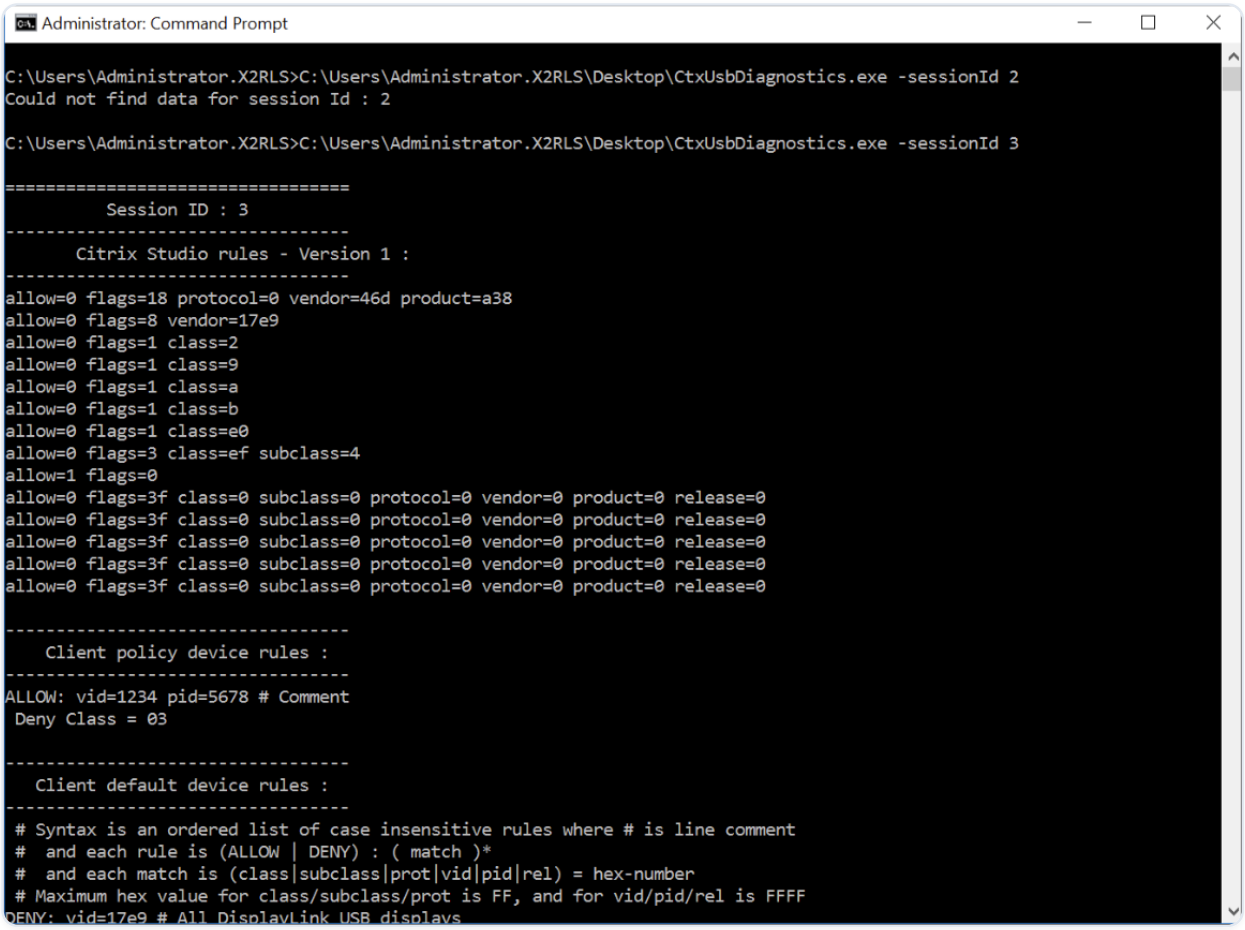
クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
- ワークスペースアプリ
  - Windows: バージョン 2311 以降

ツールの機能?

このツールは現在、以下を提供します。

- SessionID
- VDAデバイスポリシー（Studioで設定されたデバイスルール）
- クライアントデバイスとクライアントデバイスポリシー（デバイスルール）
- デバイスのリスト、そのリダイレクト状態、および許可または拒否された理由



> **注記：**
>
> 管理者は、すべてのアクティブなセッションのデバイス情報を確認できます。

表示される情報

- **Citrix Studio ルール - バージョン 1/2**
  - DDCルールは、Studioにおけるレガシーな「**クライアントUSBデバイスリダイレクトルール**」または「**クライアントUSBデバイスリダイレクトルール (バージョン 2)**」ポリシーの使用を示します。このセクションに記載されている情報は、Citrix®管理者が構成したすべてのルールを一覧表示します。

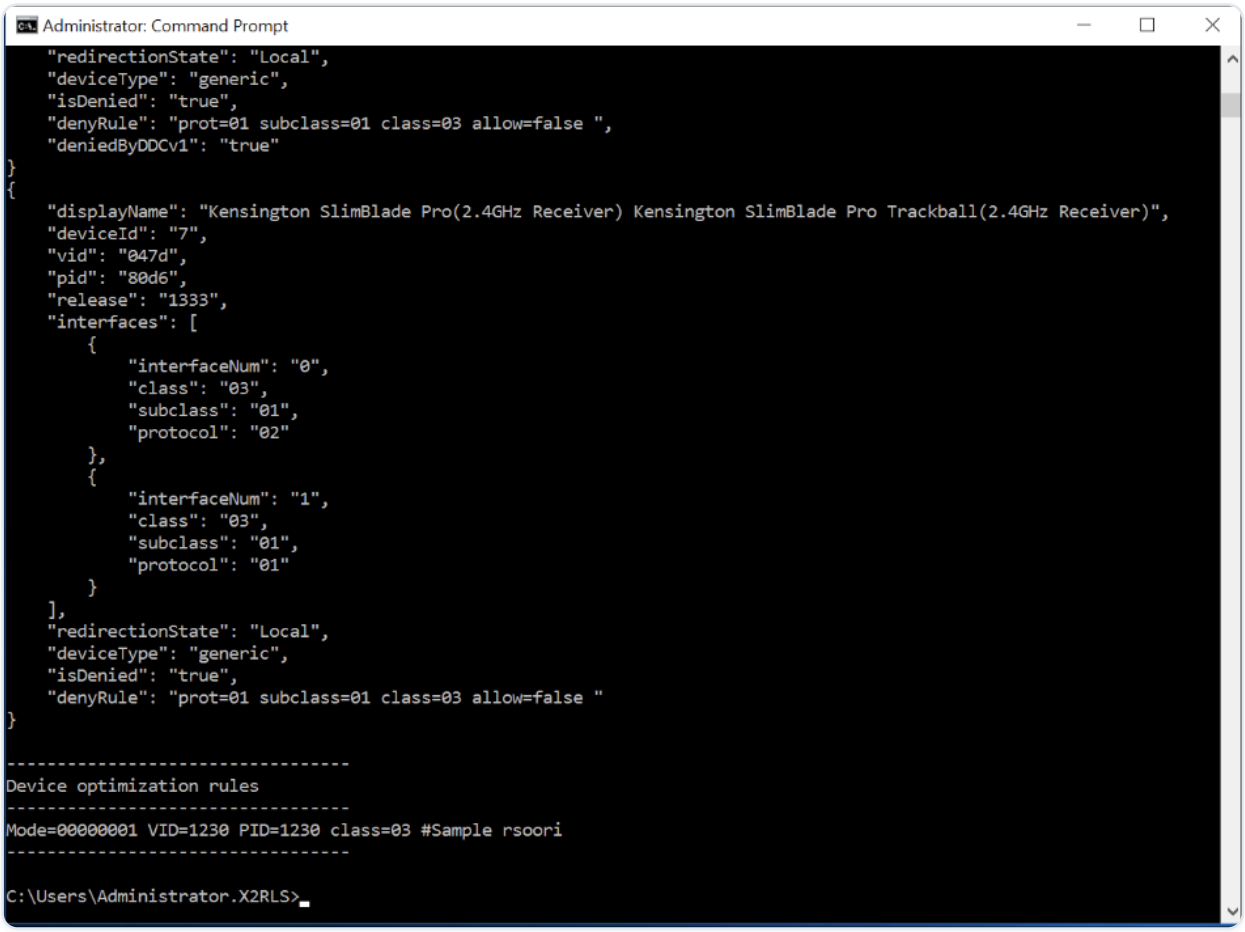
```
C:\Program Files\Citrix\HDX\bin>CtxUsbDiagnostics.exe

---------------------------------
          Session ID : 1
---------------------------------
       Citrix Studio rules - Version 2 :
---------------------------------
DENY: vid=046D pid=0A38
# Block some devices we never want to see
DENY: vid=17e9 # All DisplayLink USB displays
```

- **クライアントのデフォルトデバイスルール**
  - このセクションには、クライアントのレジストリに設定されているルールが一覧表示されます。

```
---------------------------------
   Client default device rules :
---------------------------------
 # Syntax is an ordered list of case insensitive rules where # is line comment
 #   and each rule is (ALLOW | DENY) : ( match )*
 #   and each match is (class|subclass|prot|vid|pid|rel) = hex-number
 # Maximum hex value for class/subclass/prot is FF, and for vid/pid/rel is FFFF
DENY: vid=17e9 # All DisplayLink USB displays
CONNECT: vid=1188 pid=A101 # Bloomberg 5 Biometric module
DENY: vid=1188 pid=A001 split=01 intf=00 # Bloomberg 5 Primary keyboard
CONNECT: vid=1188 pid=A001 split=01 intf=01 # Bloomberg 5 Keyboard HID
DENY: vid=1188 pid=A301 split=01 intf=02 # Bloomberg 5 Keyboard Audio Channel
CONNECT: vid=1188 pid=A301 split=01 intf=00,01 # Bloomberg 5 Keyboard Audio HID
DENY: class=02 # Communications and CDC-Control
DENY: class=09 # Hub devices
DENY:vid=045e pid=079A # Microsoft Surface Pro 1 Touch Cover
DENY:vid=045e pid=079c # Microsoft Surface Pro 1 Type Cover
DENY:vid=045e pid=07dc # Microsoft Surface Pro 3 Type Cover
DENY:vid=045e pid=07dd # Microsoft Surface Pro JP 3 Type Cover
DENY:vid=045e pid=07de # Microsoft Surface Pro 3_2 Type Cover
DENY:vid=045e pid=07e2 # Microsoft Surface Pro 3 Type Cover
DENY:vid=045e pid=07e4 # Microsoft Surface Pro 4 Type Cover with fingerprint reader
DENY:vid=045e pid=07e8 # Microsoft Surface Pro 4_2 Type Cover
DENY:vid=03eb pid=8209 # Surface Pro Atmel maXTouch Digitizer
ALLOW:vid=056a pid=0315 class=03 # Wacom Intuos tablet
ALLOW:vid=056a pid=0314 class=03 # Wacom Intuos tablet
ALLOW:vid=056a pid=00fb class=03 # Wacom DTU tablet
DENY: class=03 subclass=01 prot=01 # HID Boot keyboards
DENY: class=03 subclass=01 prot=02 # HID Boot mice
DENY: class=0a # CDC-Data
DENY: class=0b # Smartcard
DENY: class=e0 # Wireless controller
DENY: class=ef subclass=04 # Miscellaneous network devices
ALLOW: # Otherwise allow everything else
```

- **デバイス最適化ルール**
  - このセクションには、「クライアントUSBデバイス最適化ルール」で設定されているデバイス最適化ルールが一覧表示されます。



デバイスリスト

このセクションには、クライアントエンドポイントに接続されている各デバイスに関する貴重な情報（ハードウェア情報、リダイレクトされているかどうか、正しいデバイスリダイレクトルールが設定されているかどうかなど）が一覧表示されます。

タグ名	説明
displayName	デバイスの一般的な名前を一覧表示します。
ベンダーID	ベンダーID
製品ID	製品ID
インターフェイス	このサブセクションでは、複合デバイスが複数の子デバイスに分割されている場合に、すべてのインターフェイスを一覧表示します。
InterfaceNum	インターフェイス記述子のインデックスを示します
クラス	クラスコード

タグ名	説明
サブクラス	サブクラスコード
プロトコル	プロトコル
リダイレクト状態	**ローカル**は、デバイスがICA®セッションでリダイレクトされていないことを示します。**このセッション**は、デバイスがICAセッションでリダイレクトされていることを示します。**他のセッション**は、デバイスが別のICAセッションでリダイレクトされていることを示します。
デバイスタイプ	**汎用**は、デバイスに最適化された仮想チャネルがなく、トラフィックがUSB仮想チャネルを介して流れていることを示します。**最適化済み**は、デバイスに関連付けられたデータ転送が専用の仮想チャネルを介して行われていることを意味します。
拒否済み	**true**は、管理者が設定したポリシー規則によりデバイスがリダイレクトされないことを示します。`false`は、適用されたポリシーによりデバイスがリダイレクトされることを示します。
拒否ルール	このフィールドは、**拒否済み**が`true`に設定されている場合に役立ちます。これは、デバイスがリダイレクトされない原因となっているポリシーで設定された特定のルールを管理者に伝えます。
デバイスドライバー	このフィールドは、VDIホストに対応するドライバーが存在するかどうかを示します。

さらに、各デバイスの概要セクションが含まれており、HDXセッション内でのデバイスの可用性をユーザーに知らせます。

推奨事項

このセクションでは、さまざまなデバイスルールと、修正または調査が必要な問題（もしあれば）の簡単な概要を説明します。

レガシーUSBリダイレクトの構成

バージョン2212より古いコンポーネントを使用している場合、またはLinux版CWAを使用している場合は、このガイドに従って環境でUSBリダイレクトを構成してください。

汎用USBリダイレクトの有効化

1. **Citrix Web Studio™ポリシー**を開き、**ポリシー**タブをクリックします。
2. **ポリシーの作成**をクリックし、**ICA® > USBデバイスポリシー**を展開します。
3. **クライアントUSBデバイスリダイレクト**ポリシー設定を編集します。
4. **許可**を選択し、**保存**をクリックします。

USBリダイレクトポリシー規則の作成

ユーザーがUSBデバイスを仮想デスクトップにリダイレクトしようとすると、一致が見つかるまで各USBポリシー規則と照合されます。いずれかのデバイスに対する最初の一致が最終と見なされます。最初の一致が許可規則である場合、一致したデバイスは仮想デスクトップにリダイレクトが許可されます。最初の一致が拒否規則である場合、一致したデバイスはローカルデスクトップでのみ利用可能です。一致が見つからない場合は、デフォルト規則が使用されます。

Studioコンソールで適切なデバイス規則を設定する:

1. **Citrix Web Studioポリシー**を開き、**ポリシー**タブをクリックします。
2. **ポリシーの作成**をクリックし、**ICA > USBデバイスポリシー**を展開します。
3. **クライアントUSBデバイスリダイレクト規則**ポリシー設定を編集します。
4. リダイレクトする必要がある各USBデバイスについて、説明に記載されている例に基づいて値を設定し、をクリックします。 例： Allow: VID=056A PID=00A4 #STU-430 Deny: Class=08 subclass=05 # Mass Storage

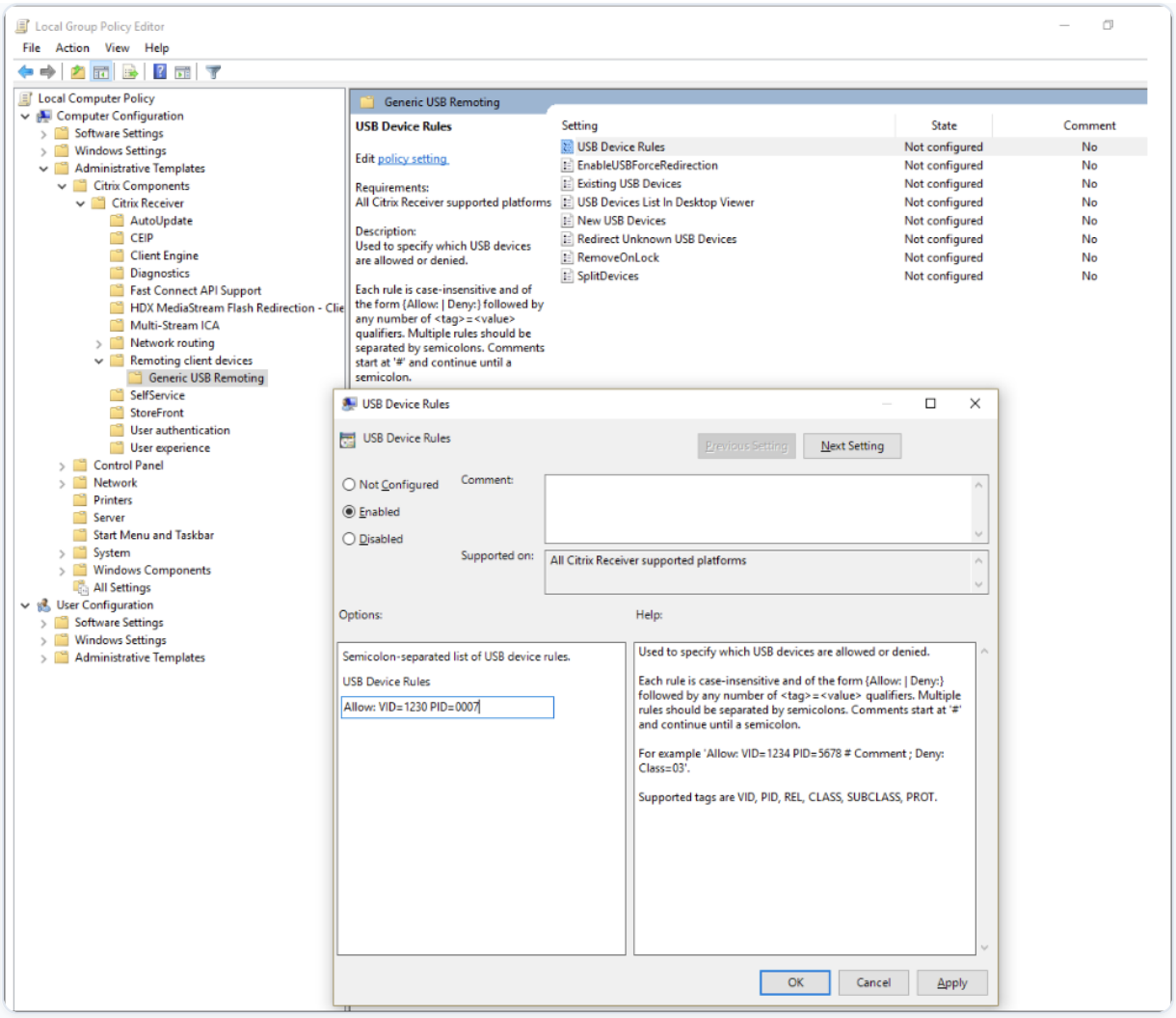
> **注:**
>
> Citrix®管理者が「デフォルト値を使用」をチェックし、「保存」をクリックすると、VDAの以下のレジストリでデフォルト規則が見つかります。
>
> **注意:**
>
> レジストリエディターを使用する前に、この記事の最後にある免責事項を参照してください。 `HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules`

クライアントで適切なGPOを設定する:

1. **ローカル グループ ポリシー エディター**を開き、**管理用テンプレート > Citrix Components > Citrix Receiver™ > Remoting client devices > Generic USB Remoting**に移動します。
2. **USBデバイスルール**設定を開き、**有効**に設定します。次の例のようにUSBデバイスルールを追加します。 Allow: VID=1230 PID=0007ルールは、ベンダーID 1230および製品ID 0007のデバイスを許可します。

注:

特定のデバイスをデバイスルールリストの最上位に配置する必要がある場合は、Allow: VID=xxxx PID=xxxxルールを使用します。



注:

> USBViewやConnectionツールバーなどのツールを使用して、VIDやPIDなどのデバイスの詳細を特定できます。

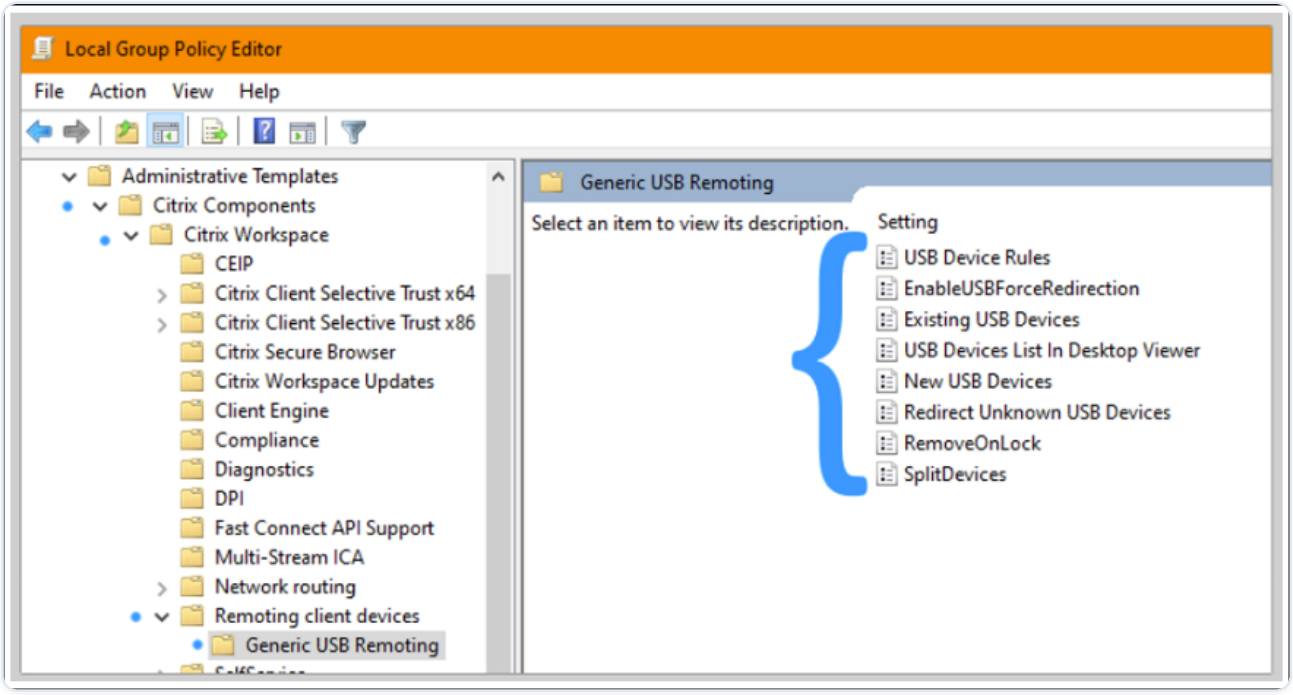
USBデバイスの自動リダイレクトを構成する

USBサポートが有効になっている場合、USBデバイスは自動的にリダイレクトされます。また、USBユーザー設定はUSBデバイスを自動的に接続するように設定されています。すべてのUSBデバイスをリダイレクトすることが常に最適とは限りません。ユーザーは、自動的にリダイレクトされないUSBデバイスリストからデバイスを明示的にリダイレクトできます。USBデバイスが一覧表示されたりリダイレクトされたりするのを防ぐには、クライアントエンドポイントでDeviceRulesポリシー設定を使用します。

このポリシーは、GPO、クライアント側レジストリ、Citrix Workspace™ Preferences、またはCDViewerのConnectionsタブを使用してクライアントで設定できます。これらの方法はすべて以下に説明されています。

クライアントでGPOを使用する:

1. **ローカル グループ ポリシー エディター**を開き、**管理用テンプレート > Citrix Components > Citrix Receiver > Remoting client devices > Generic USB Remoting**に移動します。
2. **新しいUSBデバイス**を開き、**有効**を選択して、**OK**をクリックします。
3. **既存のUSBデバイス**を開き、**有効**を選択して、**OK**をクリックします。

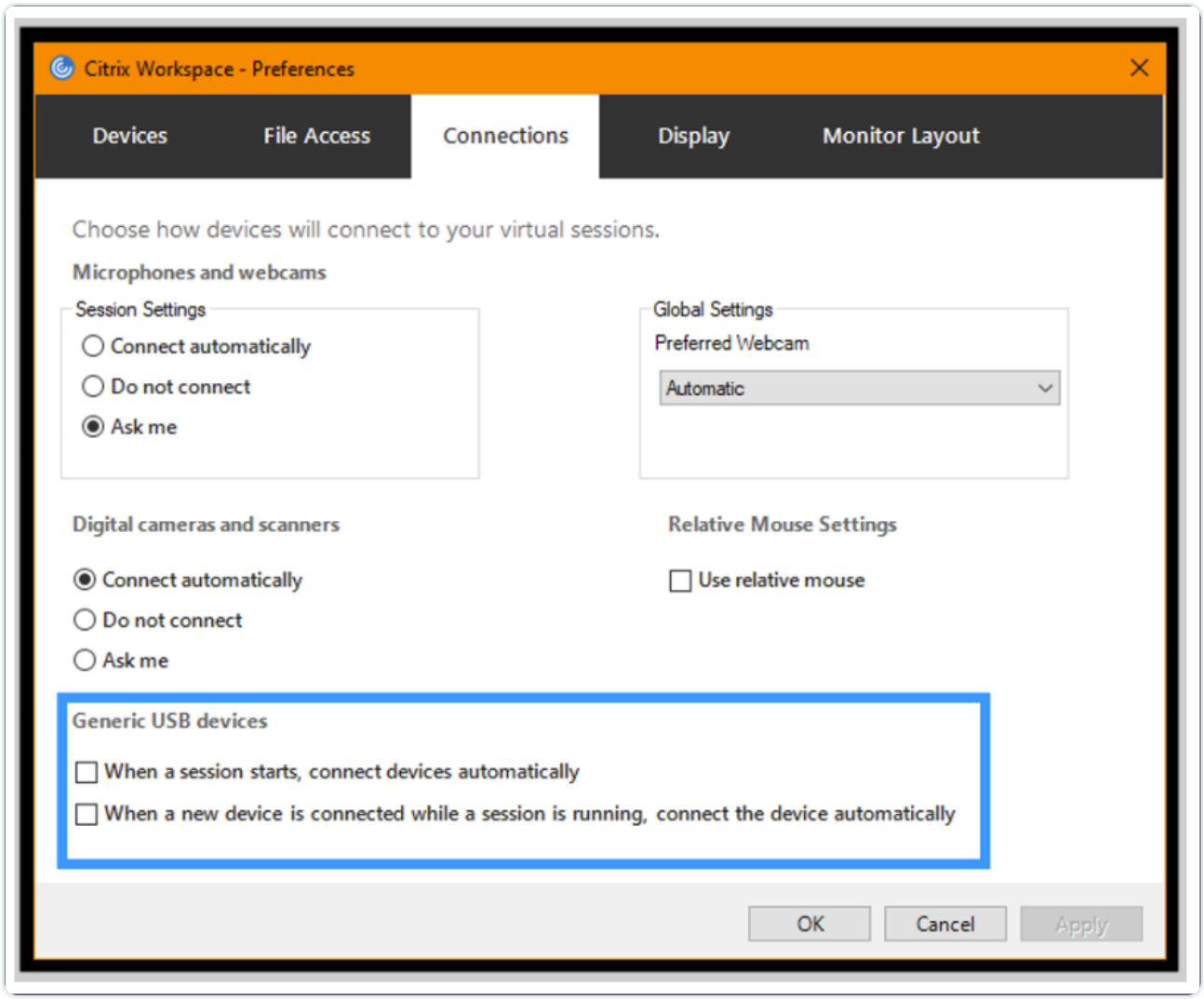


Citrix Connection Center を使用する方法:

1. **Citrix Workspace Preferences > Connections** に移動してください。
2. 次のオプションが選択されていることを確認します。
    a. セッション開始時にデバイスを自動的に接続する
    b. セッション実行中に新しいデバイスが接続された場合、そのデバイスを自動的に接続する。
3. **OK**をクリックします。

CDViewer 接続ツールバーの使用:

1. セッション開始後、「**CDViewer**」ドロップダウンをクリックし、「**Citrix Workspace Preferences > Connections**」タブを選択します。
2. 次のオプションが選択されていることを確認します。
    a. セッション開始時にデバイスを自動的に接続する
    b. セッション実行中に新しいデバイスが接続された場合、そのデバイスを自動的に接続する。
3. ポリシーを保存するには、**適用**と**OK**をクリックします。



クライアントベースの構成の場合、レジストリキーは次の場所にあるクライアントデバイスに設定されます。

> **注意:**
>
> レジストリエディターを使用する前に、この記事の最後にある免責事項を参照してください。 `HKLM\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB`

異なるデバイスルールを持つUSBリダイレクトを使用して2つ以上のデバイスを構成する

複数のデバイスを、異なるデバイスルールでHDX™セッション内にリダイレクトできます。管理者は、一方のデバイスを自動的にリダイレクトし、もう一方のデバイスはエンドユーザーにリダイレクトのオプションを提供したい場合があります。以下に、異なるルールで2つのデバイスを構成する手順を示します。

1. **Citrix Web Studio**で**クライアントUSBデバイスリダイレクト**ポリシー設定を有効にします。

2. クライアント側のGPOで**USBデバイスルール**設定を編集します。

    a. **ローカルグループポリシーエディター**を開き、**管理用テンプレート > Citrixコンポーネント > Citrix Receiver > クライアントデバイスのリモート処理 > Generic USB Remoting**に移動します。

    b. **USBデバイスルール設定**を開き、この設定を有効にします。この例のようにUSBデバイスルールを追加します。**Allow: VID=0911 PID=0c1c**ルールは、**ベンダーID 0911**および**製品ID 0c1c**のデバイスを許可しますが、自動的にはリダイレクトされません。**Connect: VID=06A8 PID=0043**ルールは、ステップ3で述べられている自動リダイレクトポリシーが設定されている場合、**ベンダーID 06A8**および**製品ID 0043**のデバイスを自動的にリダイレクトします。

    c. **Allow**: VID=0911 PID=0c1c #Phillips スピーチマイク.

    d. **Connect**: VID=06A8 PID=0043 class=03 # Topaz HSB シグネチャパッド

3. **ローカルグループポリシーエディター**を開き、**管理用テンプレート > Citrixコンポーネント > Citrix Receiver > クライアントデバイスのリモート処理 > Generic USB Remoting**に移動します。
4. **新しいUSBデバイス**を開き、**有効**を選択して**OK**をクリックします。
5. **既存のUSBデバイス**を開き、**有効**を選択して**OK**をクリックします。

これらの設定が構成されると、TopazシグネチャパッドはHDXセッション内に自動的にリダイレクトされ、セッション内でPhillipsスピーチマイクをリダイレクトするには、追加のエンドユーザー操作（接続センターまたはCD Viewerのタブでオプションを選択）が必要になります。

> **注:**
>
> ステップ2と3の上記の設定は、GenericUSBキー（HKLM\SOFTWARE\Wow6432Citrix\ICA Client\GenericUSB）の下にあるクライアント側のレジストリ値**DeviceRules**に直接適用することもできますが、これは推奨される方法ではありません。

汎用USBリダイレクトとクライアントドライブに関する考慮事項

HDX™テクノロジーは、ほとんどの一般的なUSBデバイスに対して**最適化されたサポート**を提供します。最適化されたサポートは、WAN経由でパフォーマンスと帯域幅の効率を向上させ、ユーザーエクスペリエンスを改善します。特に高遅延またはセキュリティに敏感な環境では、最適化されたサポートが通常最良の選択肢です。

HDXテクノロジーは、最適化されたサポートがない、または不適切な特殊なデバイスに対して**汎用USBリダイレクト**を提供します。例を次に示します。

- USBデバイスに、マウスやWebカメラのボタンの増加など、最適化されたサポートに含まれない高度な機能がある場合。
- ユーザーが最適化されたサポートに含まれない機能を必要とする場合。
- USBデバイスが、テストおよび測定機器や産業用コントローラーなどの特殊なデバイスである場合。
- アプリケーションがUSBデバイスとしてデバイスに直接アクセスする必要がある場合。
- USBデバイスにWindowsドライバーしか利用できない場合。たとえば、スマートカードリーダーには、Citrix Workspace™ app for Android用のドライバーが利用できない場合があります。
- Citrix Workspace appのバージョンが、この種類のUSBデバイスに対して最適化されたサポートを提供していない場合。

汎用USBリダイレクトでは、次のようになります。

- ユーザーはユーザーデバイスにデバイスドライバーをインストールする必要がありません。
- USBクライアントドライバーはVDAマシンにインストールされます。

> **重要:**
>
> - 汎用USBリダイレクトは、最適化されたサポートと組み合わせて使用できます。汎用USBリダイレクトを有効にする場合は、汎用USBリダイレクトと最適化されたサポートの両方について、CitrixのUSBデバイスポリシー設定を構成してください。
> - クライアントUSBデバイスの最適化ルールのCitrixポリシー設定は、特定のUSBデバイスに対する汎用USBリダイレクトの特定のポリシー設定です。ここで説明する最適化されたサポートには適用されません。

USBデバイスのパフォーマンスに関する考慮事項

ネットワークの遅延と帯域幅は、一部の種類のUSBデバイスで汎用USBリダイレクトを使用する場合、ユーザーエクスペリエンスとUSBデバイスの動作に影響を与える可能性があります。たとえば、タイミングに敏感なデバイスは、高遅延で低帯域幅のリンクでは正しく動作しない場合があります。可能な場合は、代わりに最適化されたサポートを使用してください。

一部のUSBデバイスは、使用可能にするために高帯域幅を必要とします。たとえば、3Dマウス（通常、高帯域幅を必要とする3Dアプリで使用）などです。帯域幅を増やすことができない場合は、帯域幅ポリシー設定を使用して他のコンポーネントの帯域幅使用量を調整することで、問題を軽減できる場合があります。詳細については、「クライアントUSBデバイスリダイレクトの帯域幅ポリシー設定」および「マルチストリーム接続ポリシー設定」を参照してください。

USBデバイスのセキュリティに関する考慮事項

一部のUSBデバイスは、スマートカードリーダー、指紋リーダー、署名パッドなど、本質的にセキュリティに敏感です。USBストレージデバイスなどの他のUSBデバイスは、機密データである可能性のあるデータを送信するために使用できます。

USBデバイスは、マルウェアを配布するためによく使用されます。Citrix Workspace appとCitrix Virtual Apps and Desktops™の設定により、これらのUSBデバイスからのリスクを軽減できますが、排除することはできません。この状況は、汎用USBリダイレクトを使用する場合でも、最適化されたサポートを使用する場合でも当てはまります。

重要:

セキュリティに敏感なデバイスとデータについては、常にHDX接続を保護してください。「クライアントとVDA間の通信」を参照してください。

必要なUSBデバイスのサポートのみを有効にしてください。このニーズを満たすように、汎用USBリダイレクトと最適化されたサポートの両方を構成してください。

USBデバイスを安全に使用するためのガイダンスをユーザーに提供してください。

- 信頼できる情報源から入手したUSBデバイスのみを使用してください。
- インターネットカフェなど、開かれた環境でUSBデバイスを放置しないでください。
- 複数のコンピューターでUSBデバイスを使用するリスクを説明してください。

USBマスストレージデバイスのセキュリティ制御

USBマスストレージデバイスには、最適化されたサポートが提供されます。このサポートは、Citrix Virtual Apps and Desktopsのクライアントドライブマッピングの一部です。ユーザーがログオンすると、ユーザーデバイス上のドライブが仮想デスクトップ上のドライブ文字に自動的に

マッピングされます。ドライブは、マッピングされたドライブ文字を持つ共有フォルダーとして表示されます。クライアントドライブマッピングを構成するには、**クライアントリムーバブルドライブ**設定を使用します。この設定は、ICAポリシー設定のファイルリダイレクトポリシー設定セクションにあります。

USBマスストレージデバイスでは、クライアントドライブマッピングまたは汎用USBリダイレクト、あるいはその両方を使用できます。これらはCitrix®ポリシーを使用して制御します。主な違いは次のとおりです。

機能	クライアントドライブマッピング	汎用USBリダイレクト
デフォルトで有効	はい	いいえ
読み取り専用アクセスを構成可能	はい	いいえ

注:

USBリダイレクトは、50 Kbpsなどの低帯域幅接続でもサポートされます。ただし、大きなファイルのコピーは機能しません。

クライアントドライブマッピング (CDM)

クライアントドライブマッピングは、クライアントエンドポイント上のストレージドライブをCitrix HDX™セッション内で利用可能にし、ファイルやフォルダーをクライアントからセッションホストへ、またはその逆に転送できるようにします。この機能は、読み取りおよび書き込みの両方の権限でデフォルトで有効になっています。マップされたクライアントデバイス上のファイルやフォルダーをユーザーが追加または変更できないようにするには、**読み取り専用クライアントドライブアクセス**ポリシー設定を有効にします。この設定をポリシーに追加する際は、**クライアントドライブリダイレクト**設定が**許可**に設定され、ポリシーにも追加されていることを確認してください。

セキュリティ上の予防措置として、エンドポイントドライブはデフォルトで実行権限なしでマップされます。ユーザーがマップされたクライアントドライブから直接実行可能ファイルを実行できるようにするには、セッションホストで**ExecuteFromMappedDrive**レジストリ値を編集します。詳細については、**レジストリで管理されるHDX機能**セクションのマップされたクライアントドライブを参照してください。

要件

CDMを使用するための要件は次のとおりです。

Citrixコントロールプレーン

- シトリックス仮想アプリおよびデスクトップ™ 1912 以降
- シトリックス DaaS™

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - ウィンドウズ サーバー 2016 以降
  - Linux: Linux VDAのシステム要件を参照してください
- VDA
  - Windows: Citrix Virtual Apps and Desktops™ 1912以降のバージョン
  - Linux: Linux VDAのドキュメントを参照してください

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - Linux: Workspace app for Linuxのシステム要件を参照してください。

関連ポリシー

CDM設定については、ポリシー設定リファレンスセクションを参照してください。

ダブルホップシナリオ

CDMはダブルホップシナリオでサポートされています。デフォルトでは、クライアントエンドポイントのドライブはセカンドホップセッションにマップされ、ファーストホップのドライブは利用できません。ただし、クライアントエンドポイントのドライブの代わりに、ファーストホップのドライブがセカンドホップセッションにマップされるように設定することも可能です。

この機能を構成するには、以下のレジストリ値を編集します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientDrive\
- 値の名前: NativeDriveMapping
- 値の型: REG_SZ
- 値のデータ:
  - True - 最初のホップセッションのドライブを2番目のホップセッションにマップします
  - False - クライアントエンドポイントのドライブを2番目のホップセッションにマップします

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

モバイルデバイスとタッチスクリーンデバイス

Citrix Virtual Apps and Desktops™ を使用すると、ユーザーは公開されたアプリケーションやデスクトップにモバイルおよびタッチスクリーンクライアントデバイスからアクセスできます。

要件

Citrix® コントロールプレーン

- シトリックス仮想アプリおよびデスクトップ™ 1912 以降
- シトリックス DaaS™

セッションホスト

- オペレーティングシステム
  - Windows 10 1903 以降
  - Windows 11 21H2 以降
- VDA

    - ウィンドウズ: シトリックス バーチャル アプリケーションズ アンド デスクトップス バージョン 7.15 以降

クライアントデバイス

- オペレーティングシステム
    - Windows 10 1809 以降
    - Windows 11 21H2 以降
- Windows 用 Citrix Workspace™ アプリ バージョン 1808 以降

Windows Continuum を使用するタッチスクリーンデバイスのタブレットモード

Continuum は、クライアントデバイスの使用方法に適応する Windows 10 の機能です。VDA は、タッチ対応クライアントでキーボードまたはマウスの存在を検出すると、クライアントをデスクトップモードにします。キーボードまたはマウスが存在しない場合、VDA はクライアントをタブレット/モバイルモードにします。この検出は、セッションの接続時および再接続時、ならびにセッション中にキーボードまたはマウスが接続または切断されたときに発生します。

この機能はデフォルトで有効になっています。この機能を無効にするには、ポリシー設定タブレットモード切り替えポリシー設定を構成します。

上記のタッチスクリーンデバイスの要件に加えて、Windows Continuumには以下が必要です。

ゼノサーバー (旧 シトリックス ハイパーバイザー™)

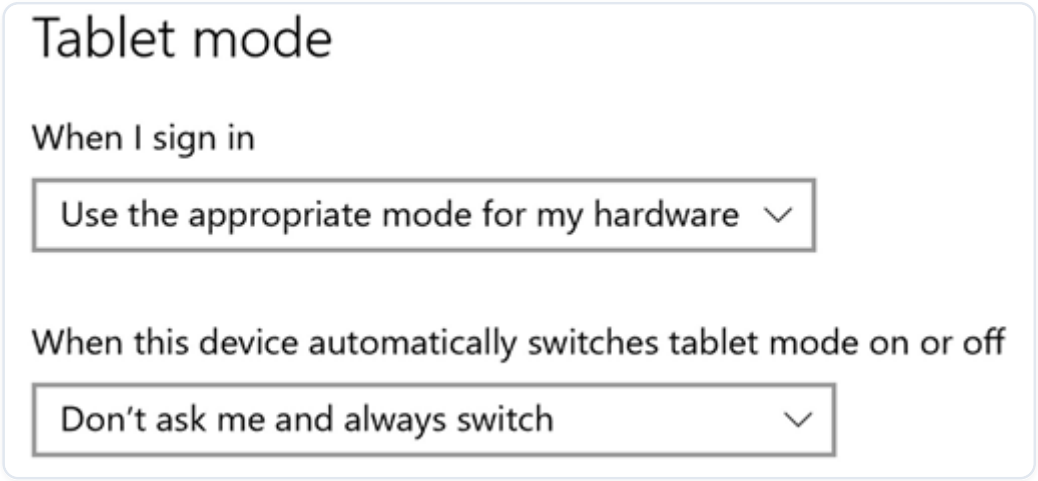
- シトリックス ハイパーバイザー 8.2 以降
- ラップトップ/タブレットの切り替えを許可するには、XenServer CLIコマンドを実行します。
  xe vm-param-set uuid=\<VM_UUID\> platform:acpi_laptop_slate=1

> **重要:**

> メタデータ設定を変更した後に既存のマシンカタログのベースイメージを更新しても、以前にプロビジョニングされたVMには影響しません。XenServer VMのベースイメージを変更した後、カタログを作成し、ベースイメージを選択して、新しいMachine Creation Services™ (MCS) マシンをプロビジョニングします。

セッションホスト

- オペレーティングシステム
  - Windows 10 1903 以降
  - Windows 11 21H2 以降
- VDA
  - Windows: バージョン 7.16 以降
  - **現在のオペレーティングシステム構成の制限により、ユーザーは最初のICA®セッションを開始してVDAを再起動した後、ドロップダウンメニューから以下のオプションを設定する必要があります。**
    - **設定 > システム > タブレットモード**
      - ハードウェアに適したモードを使用する
      - 常に切り替える（確認しない）



タブレットモードは、タッチスクリーンにより適したユーザーインターフェイスを提供します。

- ボタンが少し大きくなります。
- スタート画面と起動するすべてのアプリが全画面で開きます。
- タスクバーに「戻る」ボタンが含まれます。
- タスクバーからアイコンが削除されます。

ファイルエクスプローラーにアクセスできます。



Windows 10 は、この更新された BIOS に基づいて、ターゲット仮想マシンに GPIO ドライバーをロードします。これは、仮想マシン内でタブレットモードとデスクトップモードを切り替えるために使用されます。

HTML5 用 Citrix Workspace アプリは、Windows Continuum 機能をサポートしていません。

デスクトップモードは、PCとキーボード、マウスを使用するのと同じ方法で操作できる、従来のユーザーインターフェイスを提供します。

マイクロソフト Surface Pro および Surface Book ペン

Windows Inkベースのアプリケーションで標準のペン機能をサポートしています。サポートには、ポインティング、消去、ペン圧、Bluetooth信号、およびオペレーティングシステムのファームウェアとペンモデルに応じたその他の機能が含まれます。例えば、ペン圧は最大4096レベルまで可能です。この機能はデフォルトで有効になっています。

ペン機能のサポートに関する要件は次のとおりです。

Citrixコントロールプレーン

- Citrix Virtual Apps and Desktops のバージョン1903以降
- シトリックス DaaS

セッションホスト

- オペレーティングシステム
  - Windows 10 1809以降
  - Windows 11 21H2 以降
- VDA

- Windows: Citrix Virtual Apps and Desktops 1903 以降のバージョン

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - Windows 11 21H2 以降
- Windows向けCitrix Workspaceアプリ バージョン1902以降

Windows Ink とペンの機能のデモンストレーションについては、このグラフィックをクリックしてください。



この機能を無効または有効にするには、レジストリを介して管理される機能のリストにある Microsoft Surface Pro および Surface Book のペン を参照してください。

既知の問題

ペンサポートに関する既知の問題は次のとおりです。

- Windows Server 2k22 の OS 制限により、2k22 サーバーアプリケーションまたはデスクトップに接続している場合、ユーザーはペンのショートカットを設定したり、コントロールパネルでペン/インクの設定を調整したりすることはできません。
- OS の制限により、ペン対応の Windows 11 クライアントからのペンのショートカットは認識されません。

シリアルポート

ほとんどの新しいPCには、内蔵のシリアル（COM）ポートがありません。USBコンバーターを使用すれば、これらのポートを簡単に追加できます。シリアルポートに適したアプリケーションには、センサー、コントローラー、古いチェックリーダー、パッドなどがよく含まれます。一部のUSB仮想COMポートデバイスは、Windowsが提供するドライバー（usbser.sys）の代わりに、ベンダー固有のドライバーを使用します。これらのドライバーを使用すると、USBデバイスの仮想COMポートを、異なるUSBソケットに接続しても変更されないように強制できます。これは、**デバイスマネージャー > ポート (COM と LPT) > プロパティ**から、またはデバイスを制御するアプリケーションから実行できます。

クライアントCOMポートマッピングを使用すると、ユーザーのエンドポイントのCOMポートに接続されたデバイスを仮想セッション中に使用できます。これらのマッピングは、他のネットワークマッピングと同様に使用できます。

各COMポートに対して、オペレーティングシステムのドライバーはCOM1やCOM2などのシンボリックリンク名を割り当てます。アプリケーションは、そのリンクを使用してポートにアクセスします。

> **重要:**

> デバイスがUSBを直接使用してエンドポイントに接続できるからといって、汎用USBリダイレクトを使用してリダイレクトできるとは限りません。一部のUSBデバイスは仮想COMポートとして機能し、アプリケーションは物理シリアルポートと同じ方法でアクセスできます。オペレーティングシステムはCOMポートを抽象化し、ファイル共有のように扱うことができます。仮想COMの一般的なプロトコルは、CDC ACMまたはMCTの2つです。RS-485ポートを介して接続した場合、アプリケーションがまったく機能しない可能性があります。RS-485をCOMポートとして使用するには、RS-485-to-RS232コンバーターを入手してください。
> **重要:**

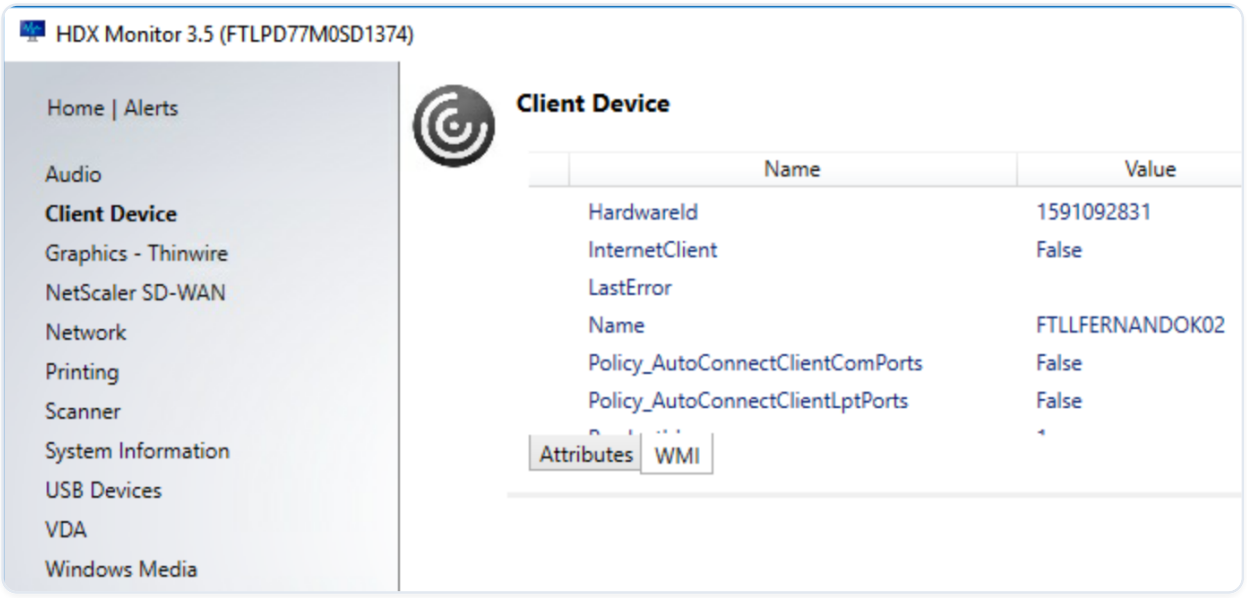
> 一部のアプリケーションは、デバイス（署名パッドなど）がクライアントワークステーションのCOM1またはCOM2に接続されている場合にのみ、一貫して認識します。

クライアントCOMポートをサーバーCOMポートにマッピングする

クライアントCOMポートをCitrix®セッションにマッピングするには、次の3つの方法があります。

- Studioポリシー。ポリシーの詳細については、「ポートリダイレクトポリシー設定」を参照してください。
- VDAコマンドプロンプト。
- リモートデスクトップ（ターミナルサービス）構成ツール。

1. **クライアントCOMポートリダイレクト**ポリシーと**クライアントCOMポートの自動接続Studio**ポリシーを有効にします。適用後、一部の情報はHDX™ Monitorで利用できます。



2. **クライアントCOMポートの自動接続**でポートのマッピングに失敗した場合は、手動でポートをマッピングするか、ログオンスクリプトを使用できます。VDAにログオンし、コマンドプロンプトウィンドウで次のように入力します。

   NET USE COMX: `\CLIENT\COMZ`:

   または

   NET USE COMX: `\CLIENT\CLIENTPORT:COMZ`:

   X はVDA上のCOMポートの番号です（ポート1～9がマッピングに利用可能です）。**Z** はマッピングするクライアントCOMポートの番号です。

   操作が成功したことを確認するには、VDAのコマンドプロンプトで **NET USE** と入力します。表示されるリストには、マップされたドライブ、LPTポート、およびマップされたCOMポートが含まれます。



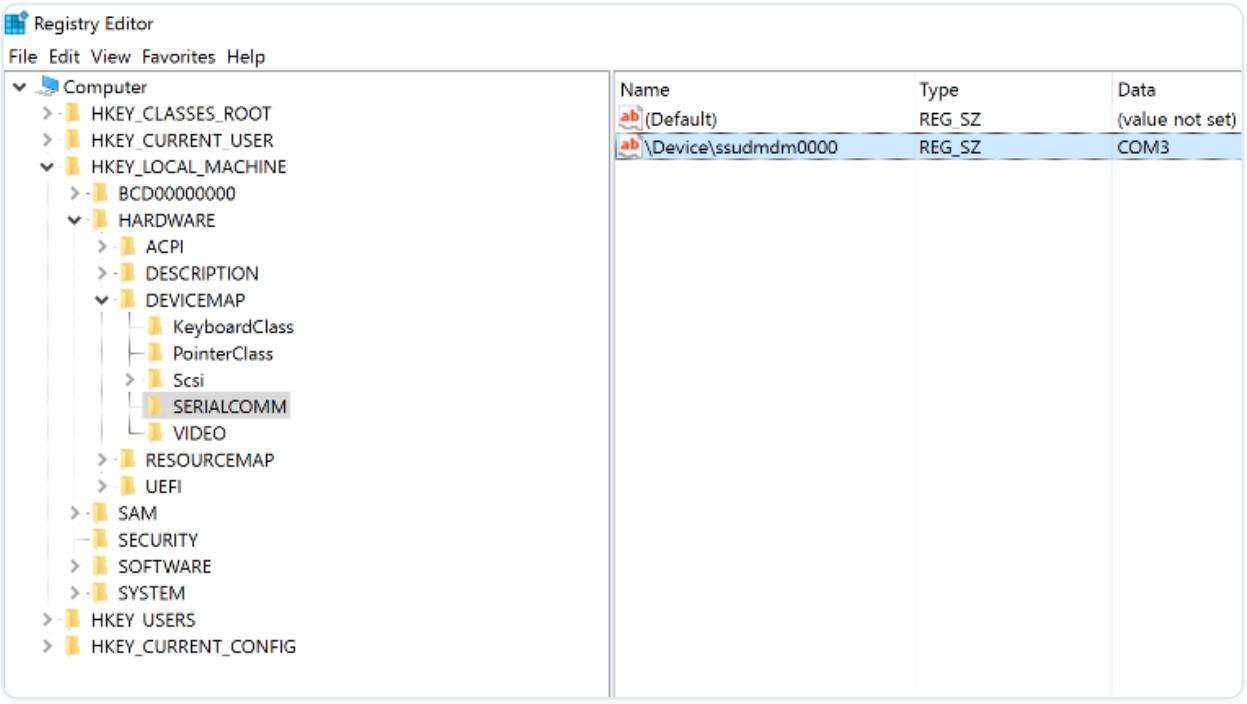
3. このCOMポートを仮想デスクトップまたはアプリケーションで使用するには、ユーザーデバイスアプリケーションをインストールし、マップされたCOMポート名を指定します。たとえば、クライアント上のCOM1をサーバー上のCOM3にマップする場合、VDAにCOMポートデバイスアプリケーションをインストールし、セッション中にCOM3を指定します。このマップされたCOMポートは、ユーザーデバイス上のCOMポートと同様に使用します。

重要:

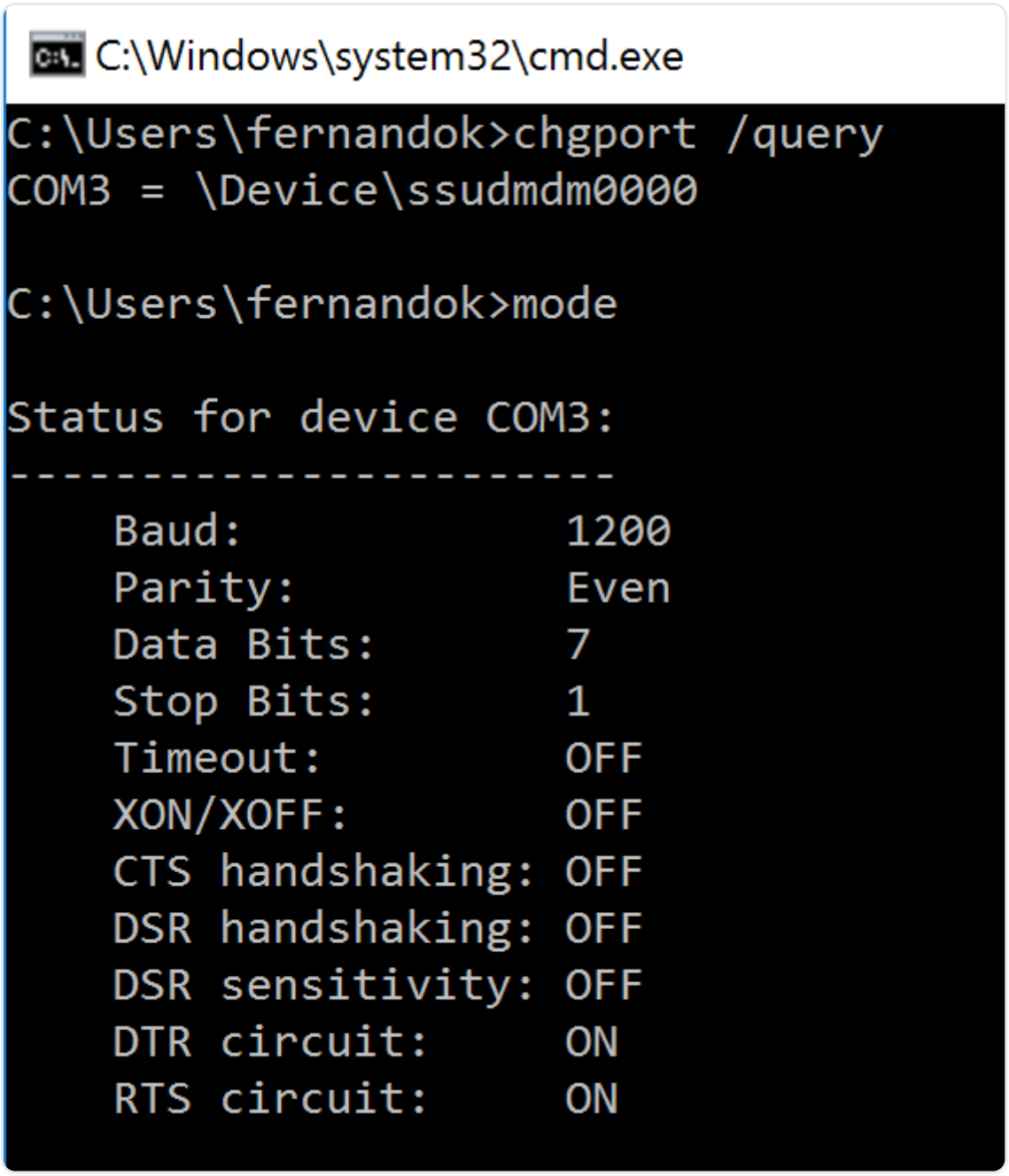
COMポートマッピングはTAPI互換ではありません。Windows Telephony Application Programming Interface (TAPI) デバイスをクライアントCOMポートにマップすることはできません。TAPIは、アプリケーションがデータ、FAX、音声通話の電話機能を制御するための標準的な方法を定義します。TAPIは、ダイヤル、応答、通話終了などのシグナリングを管理します。また、保留、転送、会議通話などの付加サービスも管理します。

トラブルシューティング

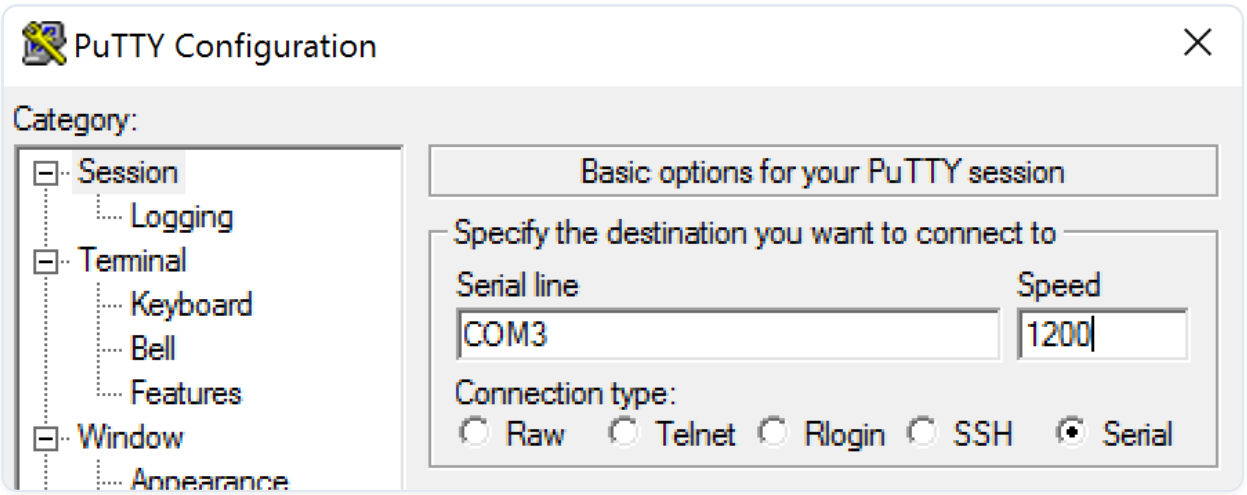
1. Citrixをバイパスして、エンドポイントからデバイスに直接アクセスできることを確認してください。ポートがVDAにマップされていない間は、Citrixセッションに接続されていません。デバイスに付属のトラブルシューティング手順に従い、まずローカルで動作することを確認してください。 シリアルCOMポートにデバイスが接続されると、ここに示されているハイブにレジストリキーが作成されます。



この情報は、コマンドプロンプトで **chgport /query** を実行することでも確認できます。



デバイスのトラブルシューティング手順が利用できない場合は、PuTTYセッションを開いてみてください。**Session** を選択し、**Serial line** でCOMポートを指定します。



ローカルコマンドウィンドウで**MODE**を実行できます。出力には、使用中のCOMポートと、PuTTYセッションで必要となるボーレート/パリティ/データビット/ストップビットが表示される場合があります。PuTTY接続が成功した場合、**Enter**キーを押してデバイスからのフィードバックを確認します。入力した文字が画面に繰り返されたり、応答されたりする場合があります。この手順が失敗した場合、仮想セッションからデバイスにアクセスすることはできません。

2. ローカルのCOMポートをVDAにマップし (ポリシーまたは**NET USE COMX: `\CLIENT\COMZ`:**を使用して)、前の手順と同じPuTTYの手順を繰り返しますが、今回はVDAのPuTTYから実行します。PuTTYがエラー「**Unable to open connection to COM1. Unable to open serial port**」を表示する場合、別のデバイスがCOM1を使用している可能性があります。

3. **chgport /query**を実行します。VDA上の組み込みWindowsシリアルドライバーが \Device\Serial0をVDAのCOM1ポートに自動割り当てしている場合、次の手順を実行します。
   A. VDAでCMDを開き、**NET USE**と入力します。

   B. VDA上の既存のマッピング（例：COM1）を削除します。

   NET USE COM1 /DELETE

   C. デバイスをVDAにマッピングします。

   NET USE COM1: `\CLIENT\COM3`:

   D. VDA上のアプリケーションをCOM3にポイントします。

   最後に、ローカルのCOMポート (例: COM3) をVDA上の別のCOMポート (COM1以外、例: COM3) にマップしてみてください。アプリケーションがそれを指していることを確認してください: **NET USE COM3: `\CLIENT\COM3`**

4. ポートがマッピングされていることが確認でき、PuTTYは動作しているもののデータが通過しない場合、それは競合状態である可能性があります。アプリケーションがマッピングされる前にポートに接続して開いてしまい、マッピングをロックしている可能性があります。次のいずれかを試してください。

   - 同じサーバーで公開されている2番目のアプリケーションを開きます。ポートがマッピングされるまで数秒待ち、その後、ポートを使用しようとする実際のアプリケーションを開きます。
   - Studioではなく、Active Directoryのグループポリシーエディターから COMポートリダイレクトポリシーを有効にします。これらのポリシーは「**Client COM port redirection**」と「**Auto connect client COM ports**」です。このように適用されたポリシーは、Studioポリ

シーよりも前に処理され、COMポートが確実にマッピングされるようにする可能性があります。Citrixポリシーは VDAにプッシュされ、次の場所に保存されます。
`HKLN\SOFTWARE\Policies\Citrix \<user session ID\>`

- ユーザーにこのログオンスクリプトを使用するか、アプリケーションを公開する代わりに、まずVDA上のマッピングを削除し、仮想COMポートを再マッピングしてからアプリケーションを起動する.batスクリプトを公開します。

@echo off NET USE COM1 /delete NET USE COM2 /delete NET USE COM1: `\CLIENT\COM1` : NET USE COM2: `\CLIENT\COM2` : MODE COM1: BAUD=1200 (または必要な値) MODE COM2: BAUD=9600 PARITY=N Data=8 Stop=1 (または必要な値) START C:\ \Program Files\\\<Your Software Path>\\\<your_software.exe>

5. SysinternalsのProcess Monitorは、最後の手段となるツールです。VDAでこのツールを実行する際、COM3、picaser.sys、CdmRedirectorなどのオブジェクト、特に\<your_app\>.exeを見つけてフィルターします。エラーは「アクセス拒否」またはそれに類するものとして表示される場合があります。

特殊キーボード

Bloombergキーボード

> **警告:**

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

> Citrix Virtual Apps and Desktops™は、Bloombergモデル5、モデル4 Starboardキーボード（およびそれ以前のモデル3）をサポートしています。このキーボードにより、金融業界のお客様は、キーボードの特殊機能を使用して金融市場データにアクセスし、迅速な取引を実行できます。

> **重要:**

> Bloombergキーボードは1つのセッションでのみ使用することをお勧めします。複数の同時セッション（1つのクライアントから複数のセッションへ）でキーボードを使用することはお勧めしません。

> Bloombergキーボードは、1つの物理シェルに複数のUSBデバイスを搭載したUSB複合デバイスです。

- キーボード。
- 指紋リーダー。
- 音量を上げ下げするキー、およびスピーカーとマイクをミュートするキーを備えたオーディオデバイス。このデバイスには、オンボードスピーカー、マイク、およびマイクとヘッドセット用のジャックが含まれています。
- これらすべてのデバイスをシステムに接続するためのUSBハブ。

要件:

- Citrix Workspace™ app for Windowsが接続するセッションは、USBデバイスをサポートしている必要があります。
- Bloombergキーボードモデル5をサポートするには、Citrix Workspace app 2207 for Linux以降が必要です。
- Bloombergキーボードモデル5をサポートするには、Citrix Workspace app 2109 for Windows以降が必要です。
- Bloombergキーボードモデル3および4をサポートするには、Citrix Workspace app 1808 for WindowsまたはCitrix Receiver for Windows 4.8以降が必要です。
- モデル4でKVMモード（2本のUSBケーブルのうち1本がKVMを介してルーティングされる）を使用するには、Citrix Workspace app 1808 for WindowsまたはCitrix Receiver for Windows 4.12以降が必要です。

Citrix Workspace app for WindowsでのBloombergキーボードの構成については、Bloombergキーボードの構成を参照してください。

Bloombergキーボードのサポートを有効にするには、レジストリを介して管理される機能のリストでBloombergキーボードを参照してください。

サポートを確認する:

Citrix WorkspaceアプリでBloombergキーボードのサポートが有効になっているかを確認するには、Desktop ViewerがBloombergキーボードのデバイスを正しく報告しているかを確認します。

デスクトップシナリオ:

Desktop Viewerを開きます。Bloombergキーボードのサポートが有効になっている場合、Desktop ViewerにはUSBアイコンの下に3つのデバイスが表示されます。

Bloomberg 5キーボードの場合:

- ブルームバーグLP ブルームバーグ生体認証モジュール
- Bloomberg LP Keyboard (2つのインターフェイスを持つ複合デバイス)
- Bloomberg LP Keyboard Audio (3つのインターフェイスを持つ複合デバイス)

Bloomberg 3および4キーボードの場合:

- ブルームバーグ指紋スキャナー
- ブルームバーグキーボード機能
- ブルームバーグLP キーボード 2013

シームレスアプリケーションのみのシナリオ:

Citrix Workspaceアプリの通知領域アイコンから**接続センター**メニューを開きます。Bloombergキーボードのサポートが有効になっている場合、3つのデバイスが**デバイス**メニューに表示されます。

これらの各デバイスのチェックマークは、それらがセッションにリモート接続されていることを示します。

Windows VDAでのダブルホップにおけるキーイベントシーケンス処理のサポート

この機能により、クライアントデバイスが非WindowsでUnicodeモードで動作している場合、Windows Virtual Desktop Agent (VDA) でキーイベントが順次送信されるようになります。これにより、以下のような特定の入力関連の問題が解決されます。

1. RDPをセカンドホップとするダブルホップシナリオ。
    - ドイツ語キーボードレイアウトを使用している場合、**AltGr**キーを押しながら**q**を押すと、出力として**@**が生成されるはずです。しかし、この機能がない場合、実際の出力は**q**になります。
2. キーショートカット機能

- Android版Citrix Workspace™ App (CWA) を使用している場合、Windows VDAで**Alt+Tab**ショートカットが常に機能しないことがあります。

この機能を有効にすることで、これらの入力の不整合が解決されます。これにより、正確なキーイベント処理とユーザビリティの向上が保証されます。

この機能はデフォルトで無効になっています。この機能の切り替えは、レジストリ設定で`EnableSendUnicodeKeyQueue`です。

新しいレジストリ`HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\icawd\EnableSendUnicodeKeyQueue` DWORD = 0/1 が使用され、値が1の場合に新しい実装に切り替わります。

デフォルトでは、値は0です。

> **注:**
>
> ダブルホップ使用シナリオの場合、上記のレジストリキーを1stホップWindows VDAに設定します。

Windows - キーボードおよびIMEサポートツール

これは、キーボードと入力メソッドエディターに関連する問題を診断できるセルフサービスコマンドラインツールです。

さまざまなユーザー要件を満たし、プラットフォームの汎用性を提供し、ユーザーにパーソナライズされたニーズを提供するために、キーボードと入力メソッドエディター（IME）の機能は、VDAおよびCitrix Workspace™アプリのさまざまな構成と機能に依存しています。

VDAまたはクライアント側の設定が正しくないと、予期しない入力動作が発生する可能性があります。

ただし、Citrix®はいくつかの一般的な使用シナリオに推奨設定を提供しており、これらの推奨事項は診断結果にも含まれています。

このツールを使用すると、以下のカテゴリの問題を特定できます。

- **キーボードタイプ不一致:** VDAキーボードタイプとクライアントキーボードタイプをチェックし、不一致がないか確認します。たとえば、VDAが101英語キーボードを使用しているのに、

クライアントが日本語106キーボードを使用している場合などです。この診断は、JP 106/109キーボードおよびKO 103/106キーボードの使用例を対象としています。

- **キーボードレイアウト同期モードの不一致:** キーボードレイアウト同期設定、レジストリ設定、グループポリシーをチェックし、特定の環境における同期モード構成の問題を解決します。
- **クライアントキーボードレイアウトとVDAキーボードレイアウトの不一致:** クライアントキーボードレイアウトがVDAキーボードレイアウトと同じであるかを確認します。
- **リモート言語バーがアプリケーションセッションに表示されない:** エンドユーザーがアプリケーションセッションを起動し、複数のキーボードレイアウトを使用している場合に、リモート言語バーが表示されているかを確認します。

このコマンドラインツールはWindows VDA - `CtxKbImeDiagnostics.exe` にホストされています。 コマンドラインインターフェースは以下のとおりです。

インターフェース	説明	注
`CtxKbimeDiagnostics`	現在のICA®セッションのみの診断結果を表示	ユーザーが管理者権限を持っている場合、すべてのアクティブなICAセッションの診断を表示します。ユーザーが管理者権限を持っていない場合、現在のユーザーのICAセッションの診断を表示します。
`CtxKbimeDiagnostics [-v]`	現在のセッションの設定情報と診断結果を表示	ユーザーが管理者権限を持っている場合、すべてのアクティブなICAセッションの診断を表示します。
`CtxKbimeDiagnostics [-v] [-s Session_Id]`	このセッションの設定情報と診断結果を表示する	
`CtxKbimeDiagnostics [-s Session_Id]`	セッションを指定し、そのセッションの診断結果を表示する	管理者権限は他のICAセッションを照会できます/通常ユーザーは自身のICAセッションのみを照会できます
`CtxKbimeDiagnostics [-s Session_Id] [-v]`	セッションを指定し、そのセッションのすべての設定情報と診断結果を表示する	管理者権限は他のICAセッションを照会できます。通常

インターフェース	説明	注
		ユーザーは自身のICAセッションのみを照会できます
`CtxKbimeDiagnostics [-h]`	サポートされている引数/パラメーターと例を表示する	「ヘルプ」インターフェース
`CtxKbimeDiagnostics [-V]`	現在のツールバージョンを表示する	

注:

このバージョンでは、クライアントとしてのCWA Windowsのみがサポートされています。

Webカメラ

高解像度Webカメラストリーミング

Webカメラは、仮想セッション内で実行されているビデオ会議アプリケーションで使用できます。サーバー上のアプリケーションは、サポートされているフォーマットタイプに基づいてWebカメラのフォーマットと解像度を選択します。セッションが開始されると、クライアントはWebカメラ情報をサーバーに送信します。ビデオ会議アプリケーションからWebカメラを選択します。Webカメラとアプリケーションの両方が高解像度レンダリングをサポートしている場合、アプリケーションは高解像度を使用します。Webカメラの解像度は最大1920x1080までサポートしています。

この機能には、Citrix Receiver for Windowsバージョン4.10以降が必要です。HDX Webカメラリダイレクトをサポートするクライアントプラットフォームのリストについては、「Citrix Workspace app feature matrix」を参照してください。

高解像度Webカメラストリーミングの詳細については、「HDX video conferencing and webcam video compression」を参照してください。

レジストリキーを使用してこの機能を無効または有効にし、特定の解像度を構成できます。詳細については、レジストリで管理される機能のリストにある「High-definition webcam streaming and High-definition webcam resolution」を参照してください。

グラフィックス

Citrix HDXグラフィックスには、Citrix Virtual Apps and Desktopsからのリッチグラフィックスアプリケーションの配信を最適化する、広範なグラフィックスアクセラレーションおよびエンコーディングテクノロジーが含まれています。これらのグラフィックテクノロジーは、グラフィックスを多用する仮想アプリケーションをリモートで操作する際に、物理デスクトップを使用するのと同じエクスペリエンスを提供します。

グラフィックスレンダリングには、ソフトウェアまたはハードウェアを使用できます。ソフトウェアレンダリングには、ソフトウェアラスタライザーと呼ばれるサードパーティライブラリが必要です。たとえば、WindowsにはDirectXベースのグラフィックス用のWARPラスタライザーが含まれています。場合によっては、代替のソフトウェアレンダラーを使用したいと思うかもしれません。ハードウェアレンダリング（ハードウェアアクセラレーション）には、グラフィックスプロセッサ（GPU）が必要です。

HDX™ Graphicsは、最も一般的なユースケース向けに最適化されたデフォルトのエンコーディング構成を提供します。Citrixポリシーを使用することで、IT管理者はさまざまなグラフィックス関連設定を構成して、さまざまな要件を満たし、望ましいユーザーエクスペリエンスを提供することもできます。

シンワイヤー

Thinwireは、Citrix Virtual Apps and Desktops™で使用されるCitrixのデフォルトのディスプレイリモートテクノロジーです。

ディスプレイリモートテクノロジーにより、あるマシンで生成されたグラフィックスを、通常はネットワーク経由で別のマシンに送信して表示できます。グラフィックスは、キーボード入力やマウス操作などのユーザー入力の結果として生成されます。

エイチディーエックス スリーディー プロ

Citrix Virtual Apps and DesktopsのHDX 3D Pro機能を使用すると、ハードウェアアクセラレーションにグラフィックス処理ユニット（GPU）を使用して最高のパフォーマンスを発揮するデスクトップとアプリケーションを配信できます。これらのアプリケーションには、OpenGLおよびDirectXベースの3Dプロフェッショナルグラフィックスアプリケーションが含まれます。標準VDAはDirectXのGPUアクセラレーションのみをサポートします。

WindowsシングルセッションOS向けGPUアクセラレーション

HDX 3D Proを使用すると、グラフィックスを多用するアプリケーションを、ホストされたデスクトップまたはシングルセッションOSマシン上のアプリケーションの一部として配信できます。HDX 3D Proは、物理ホストコンピューター（デスクトップ、ブレード、ラックワークステーションを含む）と、XenServer®、vSphere、Hyper-V（パススルーのみ）ハイパーバイザーが提供するGPUパススルーおよびGPU仮想化テクノロジーをサポートします。

GPUパススルーを使用すると、専用のグラフィックス処理ハードウェアに排他的にアクセスできるVMを作成できます。ハイパーバイザーに複数のGPUをインストールし、これらのGPUのそれぞれにVMを1対1で割り当てることができます。

GPU仮想化を使用すると、複数の仮想マシンが単一の物理GPUのグラフィックス処理能力に直接アクセスできます。

WindowsマルチセッションOS向けGPUアクセラレーション

HDX 3D Proを使用すると、WindowsマルチセッションOSセッションで実行されているグラフィックス負荷の高いアプリケーションを、サーバーのグラフィックス処理ユニット（GPU）でレンダリングできます。OpenGL、DirectX、Direct3D、およびWindows Presentation Foundation（WPF）のレンダリングをサーバーGPUに移行することで、グラフィックスレンダリングがサーバーCPUの速度を低下させることはありません。また、ワークロードがCPUとGPUに分割されるため、サーバーはより多くのグラフィックスを処理できます。

フレームホーク

> **重要:**

> Citrix Virtual Apps and Desktops 7 1903以降、Framehawkはサポートされなくなりました。代わりに、Thinwireをアダプティブトランスポートを有効にして使用してください。

> Framehawkは、ブロードバンドワイヤレス接続（Wi-Fiおよび4G/LTEセルラーネットワーク）を使用するモバイルワーカー向けのディスプレイリモートテクノロジーです。Framehawkは、スペクトル干渉やマルチパス伝播の課題を克服し、仮想アプリおよびデスクトップのユーザーにスムーズでインタラクティブなユーザーエクスペリエンスを提供します。

テキストベースのセッションウォーターマーク

テキストベースのセッションウォーターマークは、データ盗難を抑止し、追跡を可能にするのに役立ちます。この追跡可能な情報は、写真やスクリーンキャプチャを使用してデータを盗む者への抑止力として、セッションデスクトップに表示されます。テキストのレイヤーであるウォーターマークを指定できます。ウォーターマークは、元のドキュメントの内容を変更することなく、セッション画面全体に表示できます。テキストベースのセッションウォーターマークにはVDAのサポートが必要です。

アダプティブ リフレッシュ レート

新しいスケーラビリティの改善により、HDXは仮想モニターのリフレッシュレートをターゲットFPSポリシー設定に合わせます。アダプティブ リフレッシュ レート（ARR）は、シングルセッションVDAとマルチセッションVDAの両方で利用でき、GPUアクセラレーションシナリオと非GPUシナリオの両方で機能します。

ロス許容モード

ロス許容モードは、パケットロスが検出された場合でもセッションがインタラクティブな状態を維持するように徹底的に再設計されています。

関連情報

- HDX 3D プロ
- WindowsシングルセッションOSのGPUアクセラレーション
- WindowsマルチセッションOSのGPUアクセラレーション
- フレームホーク
- シンワイヤー
- テキストベースのセッションウォーターマーク(/ja-jp/citrix-virtual-apps-desktops/current-release/graphics/introduction/session-watermark-introduction.html)

シンワイヤー

Thinwireは、Citrix HDXの中核となるディスプレイリモートテクノロジーであり、Citrix Virtual Apps and Desktops™環境でスムーズでインタラクティブな視覚体験を提供する役割を担っています。

Thinwireは、画面コンテンツを分析し、変更を識別し、画面上のグラフィックデータをエンコードして、VDAからユーザーのエンドポイントデバイスへネットワーク経由で効率的に送信します。こ

れにより、情報が可能な限り効率的に送信され、帯域幅の消費を最小限に抑え、特に困難なネットワーク条件下でのパフォーマンスを最適化します。

Thinwireを搭載したHDX™ Graphicsは、高性能で適応性があり、効率的なリモートデスクトップおよびアプリケーションエクスペリエンスを提供するように設計されたCitrixの高度なディスプレイテクノロジーです。グラフィックデータをインテリジェントに分析および圧縮することで、Thinwireは多様なネットワーク条件とエンドポイントデバイス全体で最適なパフォーマンスを保証します。

HDX GraphicsとThinwireの主な機能

- **適応型ディスプレイ圧縮:** Thinwireは、コンテンツタイプとネットワーク条件に基づいて圧縮アルゴリズムを動的に調整し、画質と帯域幅効率のバランスを確保します。この適応性により、帯域幅が制限された環境でもスムーズなパフォーマンスが可能になります。
- **グラフィック処理ユニット:** HDX Graphicsは、VDAで利用可能な場合、ハードウェアエンコーディングのためにGPUの機能を自動的に活用します。
- **効率的なマルチメディアリダイレクト:** マルチメディアコンテンツをローカルレンダリングのためにエンドポイントに直接リダイレクトすることで、Thinwireはサーバー側の処理とネットワーク負荷を軽減し、ユーザーにシームレスなマルチメディアエクスペリエンスをもたらします。
- **最適化されたテキストと画像レンダリング:** ロスレステキスト圧縮やインテリジェントな画像キャッシュなどの技術を利用することで、Thinwireは鮮明なテキストとシャープな画像を提供し、可読性と視覚的な明瞭さを向上させます。
- **高解像度ディスプレイのサポート:** Thinwireは、最大8台のモニターまでの高解像度およびマルチモニター設定を効率的に処理し、さまざまなディスプレイ構成で一貫した高品質の視覚体験をユーザーに提供します。
- **高フレームレートのサポート:** HDXは最大120フレーム/秒 (fps) のフレームレートをサポートし、高モーションアプリケーションやシナリオでスムーズで応答性の高いパフォーマンスを保証します。この機能は、特にゲーム、ビデオ編集、その他のグラフィックを多用するワークロードにおいて、ユーザーエクスペリエンスを向上させます。
- **10ビットハイダイナミックレンジ:** 10ビットハイダイナミックレンジ (HDR) 仮想デスクトップセッションでは、拡張された色域、より高いコントラストと明るさで高品質の画像とビデオをレンダリングするために、強化されたエンコードおよびデコード機能を使用できます。

MicrosoftのRemote Desktop Protocol (RDP)、VMwareのBlast Extreme、AmazonのNICE DCVなどの他の業界ソリューションと比較して、CitrixのHDX GraphicsとThinwireは、現代のリモートワーク環境の要求を満たすように調整された包括的な機能セットを提供することで際立っていま

す。さまざまなネットワーク条件に適応する能力と、効率的なリソース利用、優れた画質を組み合わせることで、堅牢で柔軟なリモートディスプレイソリューションを求める組織にとって主要な選択肢となっています。

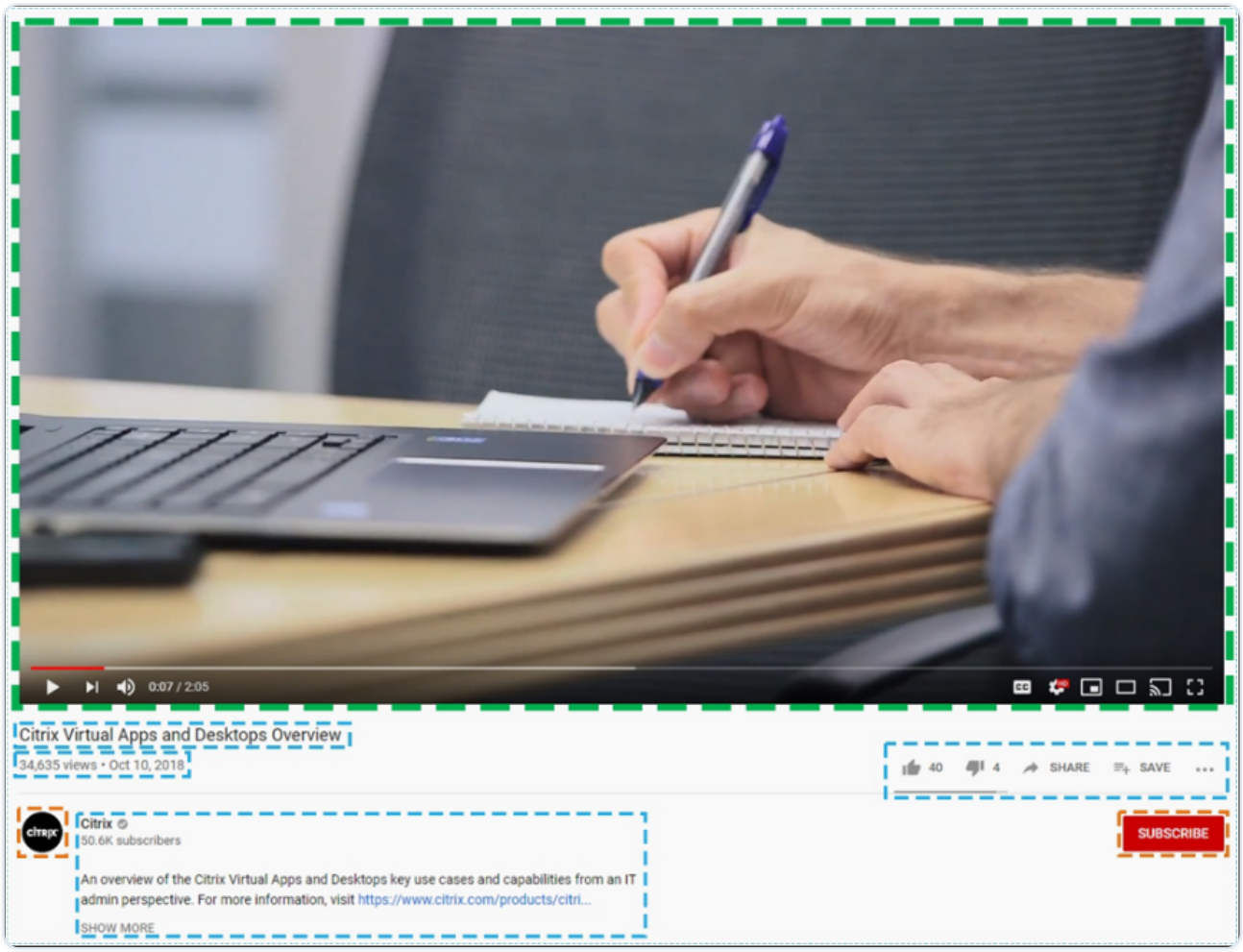
HDX Graphicsは、エンコードとレンダリングのハードウェアアクセラレーションのために、VDA上のサーバーサイドグラフィック処理ユニット (GPU) をサポートします。HDX Graphicsは、GPUが存在するかどうかを自動的に検出し、GPUの機能を自動的に使用します。

VDAにGPUを追加することは、グラフィックデザイン、ビデオレンダリング、3D CAD、データ処理および視覚化アプリケーションなどのユースケースで、グラフィックを多用するアプリケーションを高速化するのにも役立ちます。

Thinwire 分析

Thinwire は、画面上のコンテンツをリアルタイムで分析し、表示データを動的に次の3つのタイプに分類します。

- テキスト、シンプルな画像、および単色
- 静止画像コンテンツ
- 動的 (または流動的) な画像



上記の例では、テキストまたはシンプルなグラフィックは青色で、静止画像はオレンジ色で、動的 (または流動的) な画像は緑色で強調表示されています。

画面分析後、Twinwire は、VDA の機能と設定された Thinwire 構成ポリシーに基づいて、各表示データカテゴリを可能な限り効率的に圧縮およびエンコードするために異なるアプローチを取ります。

Thinwire の構成

Thinwire は、その構成に応じて異なるグラフィックエンコードモードで動作できます。Thinwire の主な構成ポリシーは、「圧縮にビデオコーデックを使用する」ポリシーです。

- 優先する場合に使用 (デフォルト)
- アクティブに変化する領域の場合
- 画面全体の場合
- ビデオコーデックを使用しない

以下のセクションでは、各モードについて詳しく説明します。

圧縮設定にビデオコーデックを使用	テキスト	画像	動画とビデオ	ユースケース
優先する場合に使用 (GPU)	ロスレス	JPEG	インテリジェントビルドからロスレス/ビデオコーデック*	グラフィックを多用するアプリケーションを含む、ほとんどのワークロードのデフォルト
優先する場合に使用 (GPUなし)	ロスレス	JPEG	ビデオコーデック	ほとんどのワークロードのデフォルト
頻繁に変化する領域向け	ロスレス	JPEG	ビデオコーデック	
画面全体向け	ビデオコーデック	ビデオコーデック	ビデオコーデック	ゲームなどのグラフィックを多用するアプリケーションで、ビルドトゥロスレスが推奨されない場合
ビデオコーデックを使用しない	ロスレス	JPEG	アダプティブ JPEG	セッションの対話性よりも画質が優先される場合。GPU使用率が最小限に抑えられるため、最高の拡張性を提供します。

*インテリジェントビルドトゥロスレスは、特定の条件が満たされた場合にのみ使用されます。

ほとんどのユースケースでは、Thinwire の設定をデフォルトのままにしておくことで、最高のパフォーマンスと表示品質が得られます。

さまざまなユースケースの詳細については、Techzone ドキュメントの HDX Graphics の設計上の決定事項 を参照してください。

Thinwire フルスクリーンエンコーダー

概要

Citrix Virtual Apps and Desktops™ 2503 以降のリリースに伴い、「3Dグラフィックワークロード向けに最適化」ポリシーは非推奨となり、削除されました。

このポリシーはフルスクリーンエンコーダーに置き換えられました。フルスクリーンエンコーダーは、特定のグラフィック負荷の高いワークロード向けに、機能強化とユーザーエクスペリエンスの向上を提供します。

フルスクリーンエンコーダーは、「圧縮にビデオコーデックを使用」ポリシーを「画面全体」に設定することで構成できます。

フルスクリーンエンコーダーは、構成を簡素化しながら、グラフィック負荷の高いワークロードに対して堅牢なパフォーマンスを提供します。画面分析や帯域幅の最適化を省略し、画面全体がビデオコーデックを使用してエンコードされることを保証することで、フレームレートとインタラクティブ性を最大化します。

このモードは、一貫したグラフィック忠実度が最重要である3Dアプリケーションやワークロードに特に適しています。

フルスクリーンエンコーダーの主な利点は、YUV444カラースペースを活用できることです。さらに、フルスクリーンエンコーディングは、セレクティブエンコーダーと比較して、最大120フレーム/秒 (FPS) の可能な限り最高のフレームレートを提供できますが、その結果、より多くの帯域幅とリソースを使用します。

フルスクリーンエンコーダーを使用する場合

グラフィックを多用するアプリケーションの場合、フルスクリーンエンコーダーを試す前に、Build to Lossless を検討する必要があります。Build to Lossless は、「視覚品質」ポリシーを「Build to Lossless」に設定し、「圧縮にビデオコーデックを使用」ポリシーをデフォルト設定の「優先時に使用」のままにすることで設定できます。

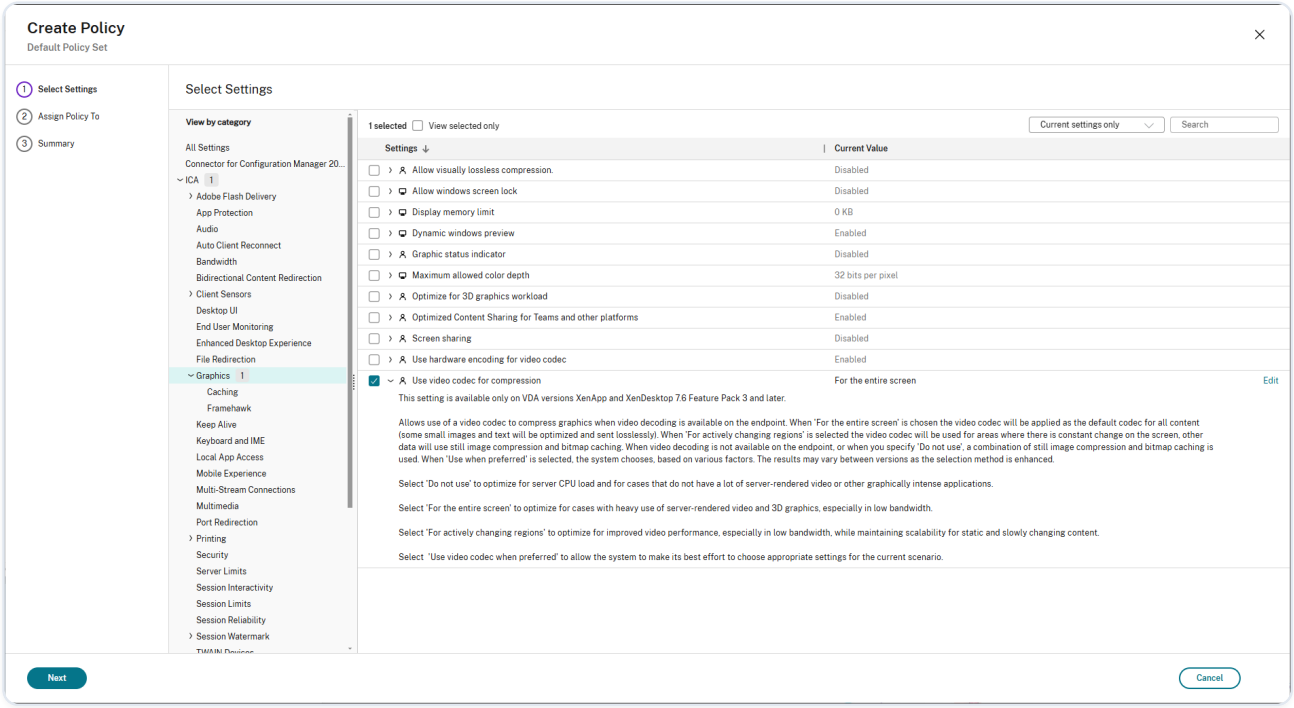
フルスクリーンエンコーダーは、YUV444 色空間をサポートしているため（「視覚的にロスレスを許可」ポリシーを参照）、より高い動画品質が必要な場合にのみ推奨されます。ビデオ編集は、この追加の忠実度が必要となる良い例ですが、これにはかなり高い帯域幅のコストがかかります。

構成

フルスクリーンエンコーダーを有効にするには:

1. Citrix Studio でグラフィックポリシー設定に移動します。
2. 「圧縮にビデオコーデックを使用する」ポリシーを見つけます。
3. ポリシーを「画面全体」に設定します。
4. ポリシーの変更を適用し、デリバリーグループに伝播します。

コーデックの動作と構成に関する追加の詳細については、A自動ビデオコーデック構成 のドキュメントを参照してください。



監視

フルスクリーンエンコーダーを監視するには、セッション内でグラフィックスステータスインジケーターを使用できます。現在、グラフィックスステータスインジケーターはデフォルトでは有効になっていません。

グラフィックスステータスインジケーターを有効にするには：

1. Citrix Studioでグラフィックポリシー設定に移動します。
2. 「グラフィックスステータスインジケーター」ポリシーを見つけます。
3. ポリシーを「有効」に設定します。
4. ポリシーの変更をデリバリーグループに適用して伝播します。

グラフィックスエンコーダー(/en-us/citrix-virtual-apps-desktops/current-release/media/policy-enable-gsi.png)

グラフィックスステータスインジケーターは、リモートセッションのタスクトレイで利用可能になります。

フルスクリーンエンコーダーを使用する場合、グラフィックスステータスインジケーターには以下が表示されます：

グラフィックスFS(/en-us/citrix-virtual-apps-desktops/current-release/media/gsi-fs.png)

廃止されたポリシー - 3Dグラフィックワークロード向けに最適化

以前は、「3Dグラフィックワークロード向けに最適化」ポリシーは、フルスクリーンエンコーダーと同様の機能を提供していました。しかし、このポリシーには高度な機能がありませんでした。

このポリシーを削除することで、構成が簡素化され、さまざまなワークロードと環境においてパフォーマンスの一貫性が確保されます。

補足事項

高性能GPUを利用する環境では、フルスクリーンエンコーダーがその潜在能力を最大限に引き出し、複雑な視覚アプリケーションのスムーズな配信を保証します。

YUV444は、デフォルトのYUV420と比較して、帯域幅の使用量が増加する代わりに、より高い色忠実度を提供することに注意してください。詳細については、カラー空間のセクションを参照してください。

Thinwire 選択的エンコーダー

選択的エンコードは、Thinwire のデフォルトの動作モードです。このモードでは、Thinwire は画面コンテンツをリアルタイムで分析し、最高の視覚品質、セッション忠実度、および帯域幅使用量のために、画面の各部分をエンコードする最適な方法を選択します。

選択的エンコードは以下を使用します。

- テキスト: ロスレスエンコード
- シンプルな画像と単色: ロスレスエンコード
- 複雑な画像/写真画像: JPEG エンコード
- 一時的なコンテンツと動画: ビデオコーデック、YUV 4:2:0 カラーモードの H.264 / H.265 / AV1。

選択的エンコードには次の特徴があります。

- アダプティブディスプレイ: Thinwire のアダプティブディスプレイテクノロジーは、動画（ビデオ、動いている3D）を識別し、画像が動いている画面の部分でビデオコーデックを使用します。
- インテリジェントビルドトゥロスレス: GPU が存在する場合、インテリジェントビルドトゥロスレスを使用して、動きが検出されたときに最高のセッションインタラクティビティを提供し、動きが停止したときにピクセルパーフェクトな画像を保証できます。Thinwire は、応答時間監視や画面アクティビティを含むいくつかの要因に基づいて、モニターごとにインテリジェントビルドトゥロスレスを自動的に有効にします。
- ハードウェアアクセラレーション: Virtual Delivery Agent (VDA) に GPU が存在する場合、フルスクリーンエンコーダーは GPU を活用してハードウェアアクセラレーションによるエンコードを行い、CPU 使用率を削減し、パフォーマンスを向上させます。
- 自動ビデオコーデック選択: 使用されるビデオコーデックは、VDA とクライアントの機能に基づいて動的に選択されます。サポートされているコーデックは次のとおりです。
  - AV1: 効率性と高品質な圧縮のために推奨されます。
  - H.265 (HEVC): AV1 をサポートしないシステムのためのフォールバックとして使用されます。
  - H.264 (AVC): レガシーまたは低機能のシナリオ、または VDA に GPU が存在しない場合に使用されます。

選択的エンコーダーを使用する場合

このモードはほとんどのユースケースで推奨されており、利用可能な帯域幅に基づいて画質を自動的に調整します。これらのユースケースには、以下が含まれます（ただし、これらに限定されません）。

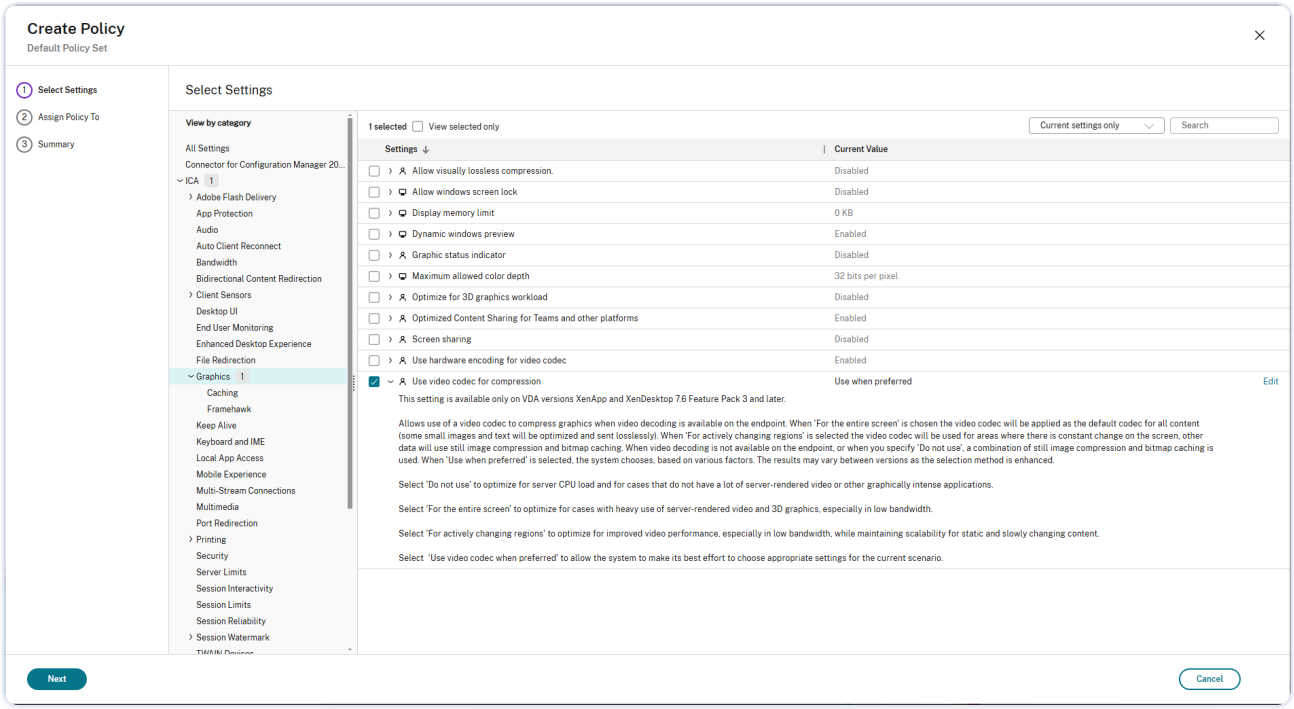
- オフィスワーカーと開発者。オフィスワーカーと開発者は、選択的エンコーダーによって提供される高画質と鮮明なテキスト品質の恩恵を受けます。
- 金融トレーダー：金融トレーダーは通常、複数の高解像度モニターを使用します。
- 2D CAD：2D CADのユースケースでは、鮮明な線と高解像度が重要です。Thinwire Selective Encoderの一部であるインテリジェントなBuild to Losslessは、動きが停止したときに高速な応答時間とピクセルパーフェクトな画像を保証します。
- 医用画像処理：選択的エンコーディングは、ロスレス画質と組み合わせることで、医療ユースケース向けにピクセルパーフェクトな画像を提供できます。（FDA承認待ち）

構成

選択的エンコーディングはデフォルトの動作モードであるため、追加の設定は不要です。デフォルトでは、サーバー側GPUが利用可能な場合、選択的エンコーディングはインテリジェントビルドトゥロスレスを使用します。

選択的エンコーディングを明示的に設定するには：

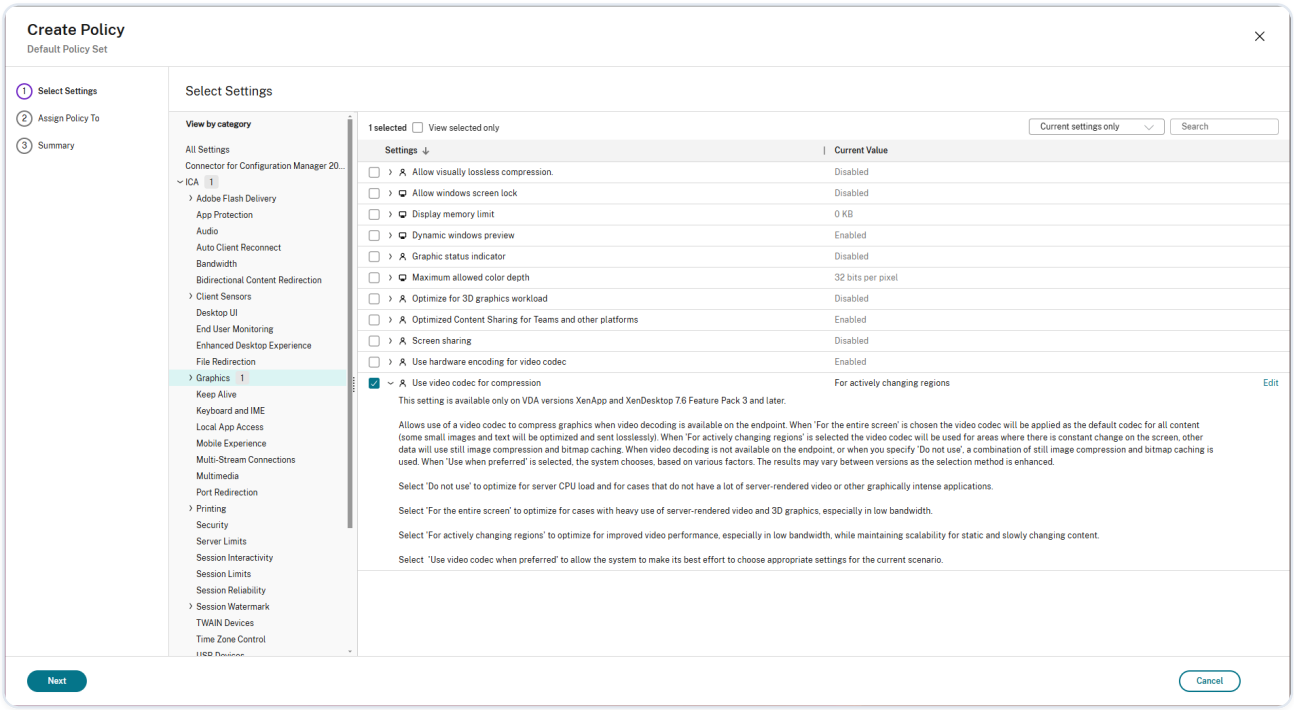
1. Citrix Studioでグラフィックポリシー設定に移動します。
2. 「圧縮にビデオコーデックを使用」ポリシーを見つけます。
3. ポリシーを「優先時に使用」に設定します。
4. ポリシーの変更を適用し、デリバリーグループに伝播します。



インテリジェントビルドトゥロスレスは、Citrix Virtual Apps and Desktops™バージョン2503で導入されました。2503より前のCVADバージョンでは、選択的エンコーディングはインテリジェントビルドトゥロスレスなしで動作します。

GPUを搭載したVDAでインテリジェントビルドトゥロスレスなしで選択的エンコーディングを使用するには（2503より前のバージョンのレガシー動作を設定するため）：

1. Citrix Studioでグラフィックポリシー設定に移動します。
2. 「圧縮にビデオコーデックを使用」ポリシーを見つけます。
3. ポリシーを「アクティブに変更される領域の場合」に設定します。
4. ポリシーの変更を適用し、デリバリーグループに伝播します。



2503より前のバージョンでは、「優先時に使用」と「アクティブに変更される領域の場合」は同じでした。2503では、「優先時に使用」のデフォルト設定には、GPUが利用可能な場合にインテリジェントビルドトゥロスレスが含まれます。GPUがない場合、「優先時に使用」は「アクティブに変更される領域の場合」と同じです。

ロスレス構築

ロスレス構築は、対話性と最終的な画質のためにグラフィック配信を最適化する、特別なThinwire構成です。この設定は、視覚品質ポリシーを「ロスレス構築」に設定することで有効にできます。

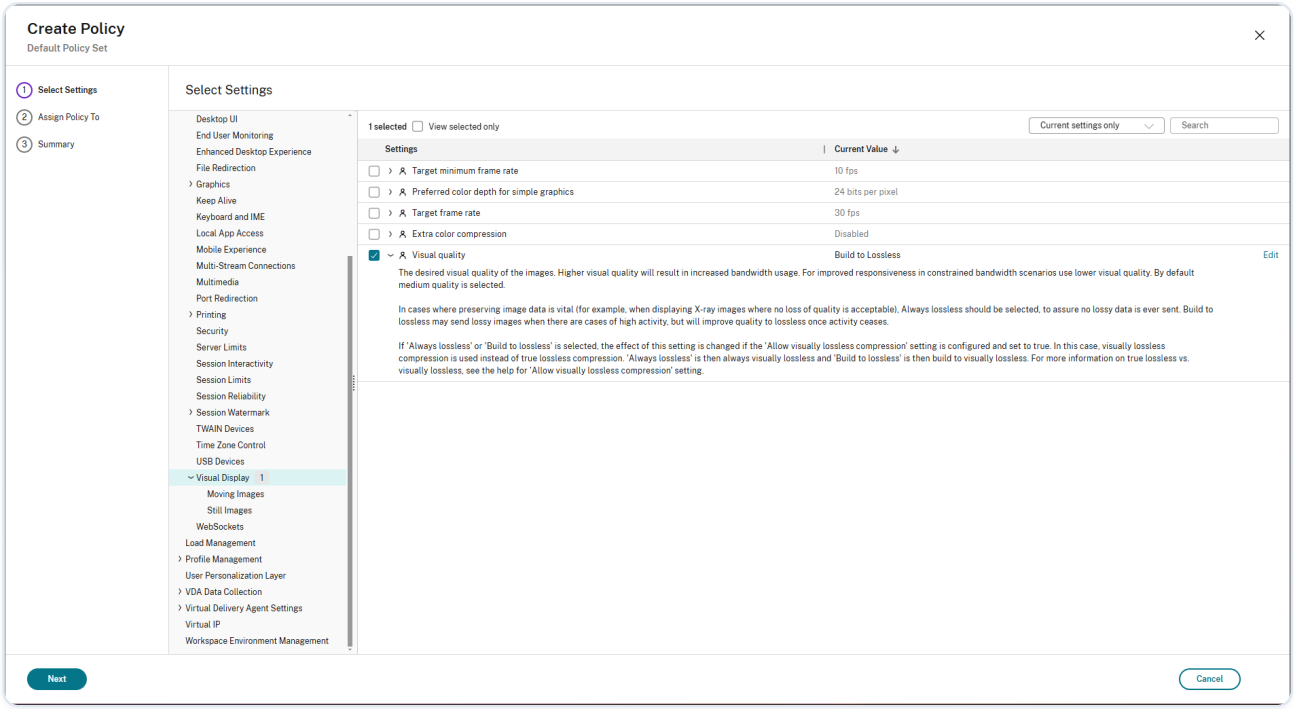
ロスレス構築は、可能な限り軽量になるように設計されており、通常の選択的エンコードで実行されるThinwire画像分析のほとんどを無効にします。これは「ファジーファースト」のアプローチを採用しており、可逆圧縮コーデックが動画に対してより良いパフォーマンスを提供すると仮定し、動きが停止すると、保証されたロスレス画像に徐々に構築していきます。

ロスレス構築は、画面アクティビティ中に選択されたビデオコーデック（AV1、H.265、またはH.264）を使用して画面を圧縮し、アクティビティが停止すると、ピクセルパーフェクト（ロスレス）にシャープ化します。可逆圧縮の画質は、可能な限り最高のフレームレートを維持するために、利用可能なリソースに適応します。シャープ化のステップは、マウスカーソルから外側に向かって放射状に徐々に行われます。これにより、シャープ化が開始された直後にユーザーが画面アクティビティを開始した場合でも、即座の応答が可能になります。たとえば、モデルを選択して回転させる場合などです。

通常のロスレス構築では、有効にするとすべてのモニターがロスレス構築モードで動作します。特定のモニターでロスレス構築を実行する機能をお探しの場合は、下記の新しいインテリジェントロスレス構築機能を参照してください。

ロスレス構築は、視覚品質ポリシー設定を使用することで有効にできます。

1. Citrix Studioでグラフィックポリシー設定に移動します。
2. 「視覚品質」ポリシーを見つけます。
3. ポリシーを「ロスレス構築」に設定します。
4. ポリシーの変更を適用し、デリバリーグループに伝播します。



通常のビルド・トゥ・ロスレスを使用する場合

通常のビルド・トゥ・ロスレスは、以下のユースケース向けに設計されています

- 全画面3D CAD
- 全画面2D CAD
- 医用画像処理向けの特定のモダリティ
- 金融 / トレーダー

これらすべてのユースケースにおいて、Citrix®セッション内で複数のモニターを使用する場合は、通常のビルド・トゥ・ロスレスよりもインテリジェント・ビルド・トゥ・ロスレスの使用をご検討ください。

インテリジェントビルドトゥロスレス

この記事では、Citrix HDX のインテリジェントビルドトゥロスレスグラフィックモードについて説明します。この機能の仕組み、設定方法、動作の検証と監視方法について解説します。また、このモードを既存のビルドトゥロスレスおよび常時ロスレスビジュアル品質設定と比較します。

混合ワークロードを念頭に置いて設計されたインテリジェントビルドトゥロスレスは、Thinwire Selective Encoding の進化形であり、新しいデフォルトのグラフィックモードです。既存のビルドトゥロスレス設定と同様に、インテリジェントビルドトゥロスレスは、大規模でアクティブに変化する画面領域でビデオコーデックを使用して、スムーズなセッショングラフィックを維持します。画面のアクティビティが停止すると、ピクセルパーフェクトになるまで画像を段階的に洗練します。インテリジェントビルドトゥロスレスが既存のビルドトゥロスレス設定と異なる点は、モードの切り替え方法です。ビルドトゥロスレスを有効にするかどうかの選択は、もはやポリシー決定だけでなく、画面のアクティビティやその他の要因に基づいています。さらに、この決定はモニターごとに下され、Thinwire Selective Encoding とビルドトゥロスレスの組み合わせが、初めて同じセッション内で可能になります。

インテリジェントビルドトゥロスレスは、VDA に GPU が存在する場合、Citrix Virtual Apps and Desktops™ バージョン 2503 以降でデフォルトで有効になっています。VDA に GPU が存在しない場合は、インテリジェントビルドトゥロスレスなしの Selective Encoding が使用されます。これは、バージョン 2503 以前の Selective Encoding の動作と本質的に同じです。

インテリジェントビルドトゥロスレスを利用するために、Citrix Workspace™ アプリのアップグレードは不要です。

グラフィックモードの比較

以下の表は、Intelligent BTL、BTL、およびAlways Losslessの主な違いをまとめたものです。

機能	インテリジェント ロスレスビルド (推奨)	ロスレスビルド	常時ロスレス
構成	デフォルトで有効。GPU対応VDAの「ビデオコーデックを使用して圧縮する」ポリシーで制御されます。	視覚品質ポリシーがBuild to Losslessに設定されています。	視覚品質ポリシーがAlways Losslessに設定されています。
アクティベーション	動的。Thinwireは画面コンテンツに基づいてインテリジェントにアクティブ化および非アクティブ化します。	セッション期間全体にわたって常にオンです。	セッション期間全体にわたって常にオンです。
スコープ	モニターごと。Build to Losslessが必要な	セッションに接続されているすべてのモ	セッションに接続されているすべてのモ

機能	インテリジェント ロスレスビルド (推奨)	ロスレスビルド	常時ロスレス
	モニターでのみ、リアルタイムでアクティブ化および非アクティブ化します。	ニターに影響し、その結果、生産性向上アプリ（例：メール）が2回のパスでレンダリングされる可能性があります。	ニターに影響します。
帯域幅の消費	画面のアクティビティに応じて、中程度から低程度。	画面のアクティビティに応じて、中程度。	高。
ユースケース	GPU対応VDAのすべてのユースケースにおけるデフォルトモード。GPUのないVDAの場合、2503以前のVDAと同様に、選択的エンコーディングが使用されます。	Intelligent Build to Losslessに置き換えられました。GPU対応VDAを使用する新規展開には推奨されません。	動きのある間を含め、すべてのフレームがロスレスである必要があるユースケース。

前提条件

Intelligent Build to Losslessは、GPU対応VDAのすべてのユースケースにおいて新しいデフォルトモードです。

VDA

Intelligent Build to Losslessは、Windows、Linux、MacのVDAで利用可能です。

重要な点として、CVADのバージョン要件はオペレーティングシステムによって異なります。

- **Windows VDA:** CVAD 2503以降
- **Linux VDA:** CVAD 2503以降
- **MacOS VDA:** 2507以降

VDAハードウェア: サーバー側のGPUが必要です (NVIDIA、AMD、またはIntel)。

詳細については、Linux VDA向けIntelligent Build to Losslessを参照してください。

> **注**:

> Intelligent Build to Losslessは、GPUのないVDAでは利用できません。

Citrix Workspace™アプリ

Citrix Workspaceアプリ: 現在サポートされているすべてのバージョン。

Intelligent Build to Losslessは、クライアントのハードウェアに依存せず、クライアント側のGPUがあるかどうかにかかわらず、すべてのクライアントで動作します。

インテリジェントビルドトゥロスレスを使用するタイミング

インテリジェントビルドトゥロスレスは、すべてのワークロードとネットワークシナリオに適しています。特に、エンドユーザーが複数のモニターと高解像度ディスプレイを使用する混合ワークロードやユースケース（たとえば、ハイエンドの金融トレーダーなど）に非常に適しています。

インテリジェントビルドトゥロスレスは、Citrix Virtual Apps and Desktops™ バージョン2503以降を実行し、サーバー側GPUを搭載しているVDAでデフォルトで有効になっています。

追加のエンドポイント要件はありません。ただし、Citrix®は常に、利用可能な最新のCWAクライアントバージョンを使用することを推奨しています。

VDAのバージョン	サーバー側GPU	インテリジェントビルドトゥロスレス
VDAバージョン2503以前	はい	いいえ
VDAバージョン2503以前	いいえ	いいえ
VDA 2503以降	**はい**	**はい**
VDA2503以降	いいえ	いいえ

Citrixは、以下のシナリオでインテリジェントビルドトゥロスレスの使用を推奨しています。

医用画像処理：

X線、MRI、CTスキャンなどの診断画像を閲覧する場合。圧縮アーティファクトが詳細を不明瞭にし、臨床精度を損なう可能性があるためです。

3D CAD/CAM & エンジニアリング:

複雑で精巧なモデルや設計図を扱う際、設計と製造の両方において、正確な線の鮮明さが不可欠です。

プリプレスおよびグラフィックデザイン:

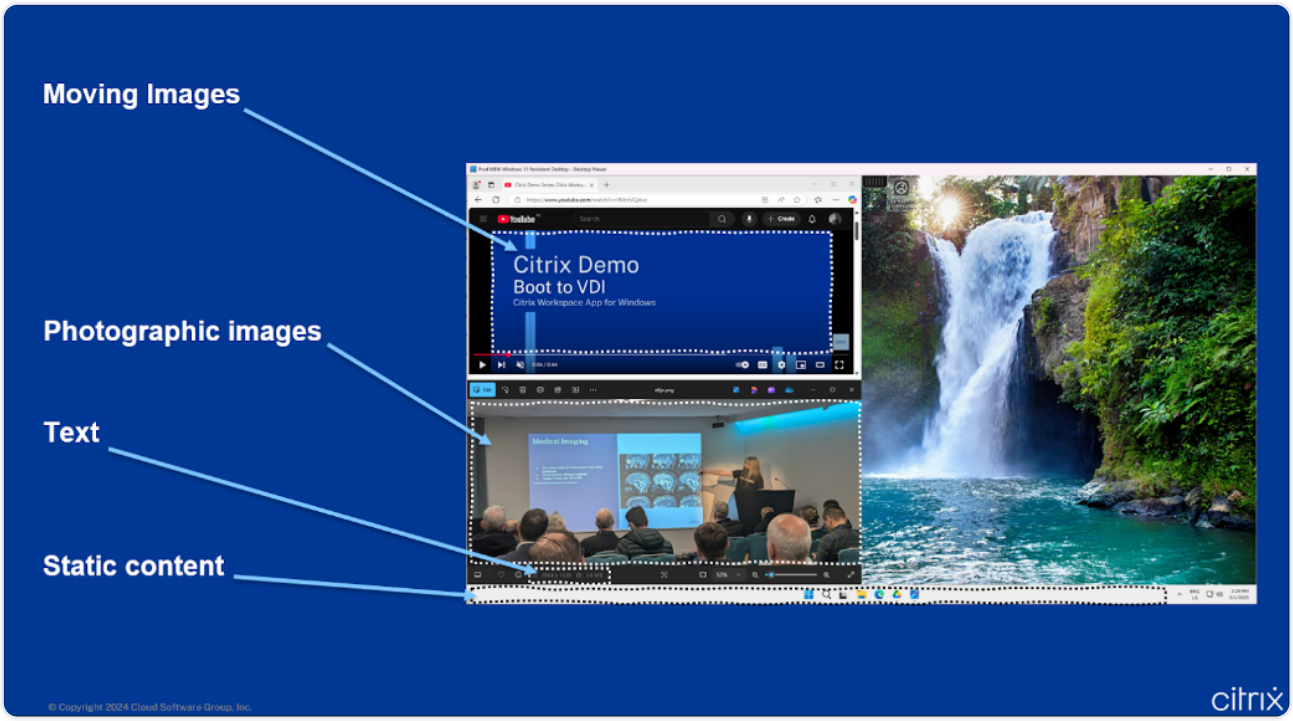
カラープルーフ、高解像度画像、またはテキストレイアウトを確認する際、品質管理のために実際の高品質なソース素材を見ることが求められます。

金融サービス:

複数の高解像度モニターを使用する際、トレーディングフロアで高密度なリアルタイムデータを表示する場合、静的なチャートや数値の絶対的な鮮明さが分析に不可欠です。

動作の仕組み

この機能は、HDX™ Thinwire ディスプレイプロトコルの一部として動作します。



1. Thinwire は、動画を含む画面領域を検出すると、VDA とクライアントの機能に応じて、設定されたビデオコーデック (H.264、H.265、または AV1) を使用してその領域をエンコードします。これにより、フレームレートと応答性が優先されます。
2. 画面の領域が静止状態になったとき、つまり動きが検出されなくなったとき、Thinwire は静止領域に対して一連の改良更新を通じて、その領域を徐々にロスレス状態に構築します。

構成

Citrix Virtual Apps and Desktops™ リリース 2503 以降では、Intelligent Build to Lossless は、サポートされている GPU を搭載した VDA でデフォルトで有効になっています。これを有効にする

ためにポリシーを作成する必要はありません。動作は、「ビデオコーデックを使用して圧縮する」ポリシーの状態によって制御されます。

Intelligent Build to Lossless を有効にするには（デフォルトの動作）

「ビデオコーデックを使用して圧縮する」ポリシーを *未構成* のままにします。または、*「ビデオコーデックを使用して圧縮する」ポリシー* を明示的に *「優先する場合に使用」* に設定することもできます。

Intelligent Build to Lossless を無効にするには（非推奨）

「ビデオコーデックを使用して圧縮する」ポリシーを明示的に「アクティブに変化する領域の場合」に設定します。

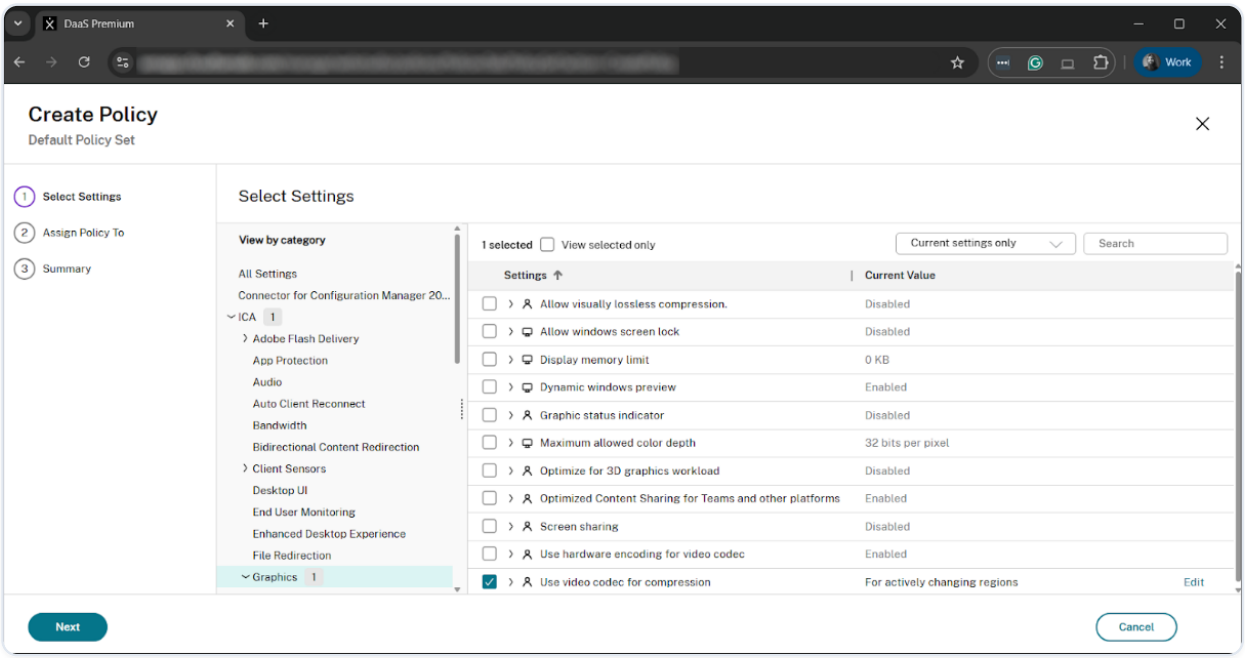
「アクティブに変化する領域の場合」を選択すると、Thinwire は、サーバー側 GPU を搭載した 2503 より前の VDA と同様に、選択的エンコードを使用します。

詳細な手順

Citrix Studio を使用して Intelligent Build to Lossless ポリシーを明示的に無効にするには、以下の手順に従ってください。

CITRIX STUDIO (GUIを使用)

1. Citrix Studio を**開きます**。
2. 左側のペインで、**ポリシー**に移動します。
3. **ポリシーの作成**をクリックするか、ターゲットユーザーまたはデリバリーグループに適用される既存のポリシーを編集します。
4. ポリシー構成ウィンドウで、検索バーを使用して、**ICA®** > **グラフィック**カテゴリの下にある **「ビデオコーデックを使用して圧縮する」**ポリシーを見つけます。
5. ポリシーを**選択**し、**編集**をクリックします。
6. デフォルトでは、このポリシーは**「優先する場合に使用」**に設定されています。**「デフォルト値を使用」**オプションのチェックを外します。
7. アクティブに変更される領域の値を変更します。
8. **OK**をクリックしてポリシー設定を保存します。
9. ポリシーが有効になっており、適切に優先順位が付けられ、適切な**デリバリーグループ**またはユーザーフィルターに適用されていることを確認します。



> **注:**
>
> ビジュアル品質ポリシーが明示的に「Build to Lossless」または「Always Lossless」に設定されている場合、これらの設定が常に優先され、新しいインテリジェントビルドツーロスレス機能よりも優先されます。最良の結果を得るには、「ビジュアル品質」ポリシーと「圧縮にビデオコーデックを使用する」設定をデフォルト値のままにしてください。

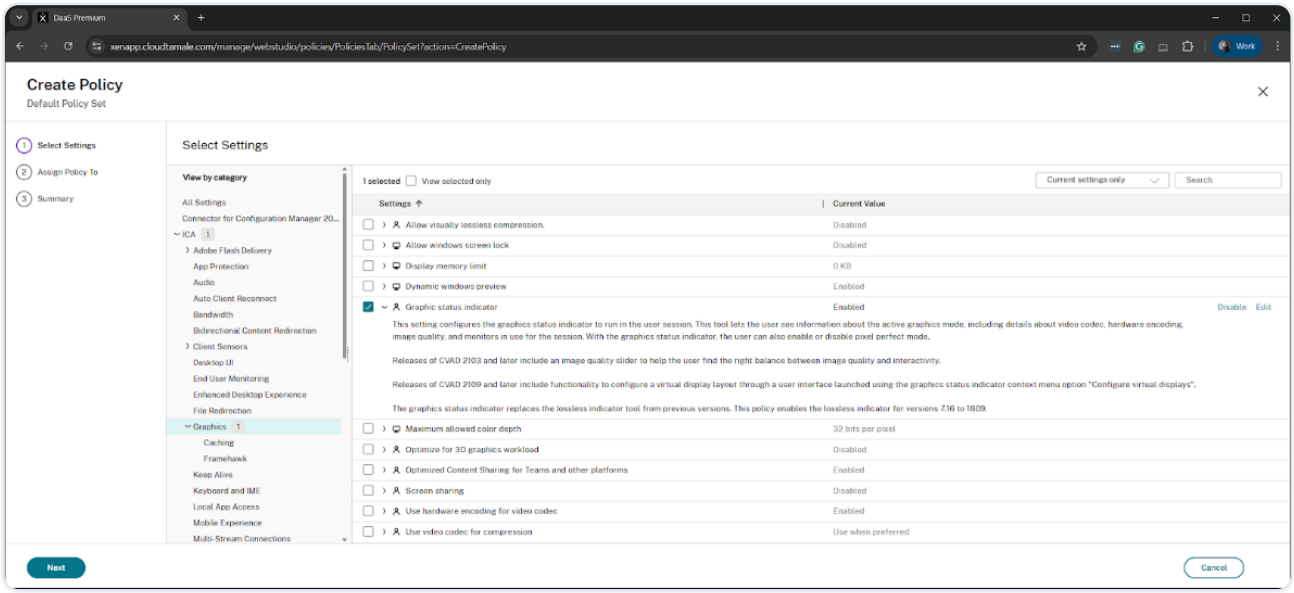
インテリジェントビルドトゥロスレスの監視

Intelligent Build to Lossless は、Citrix® セッション内からグラフィックステータスインジケーターで監視できます。現在、グラフィックステータスインジケーターはデフォルトでは有効になっていません。

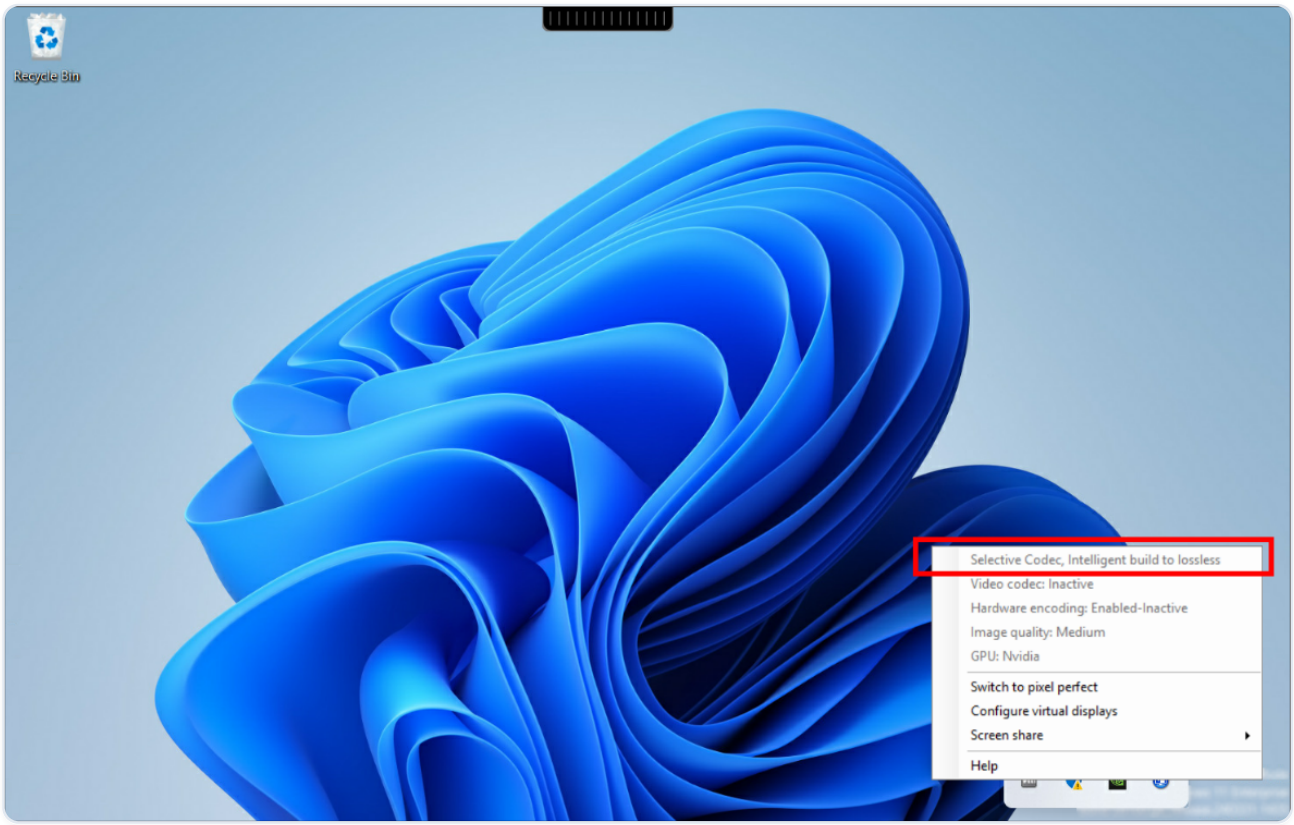
グラフィックステータスインジケーターを有効にするには

1. Citrix Studio を開きます。
2. 左側のペインで、**ポリシー**に移動します。
3. **ポリシーの作成**をクリックするか、ターゲットユーザーまたはデリバリーグループに適用される既存のポリシーを編集します。
4. ポリシー構成ウィンドウで、検索バーを使用して、**ICA®** > **グラフィック**カテゴリにある**グラフィックステータスインジケーター**ポリシーを見つけます。
5. **ポリシー**を選択し、**有効**をクリックします。
6. **OK**をクリックしてポリシー設定を保存します。

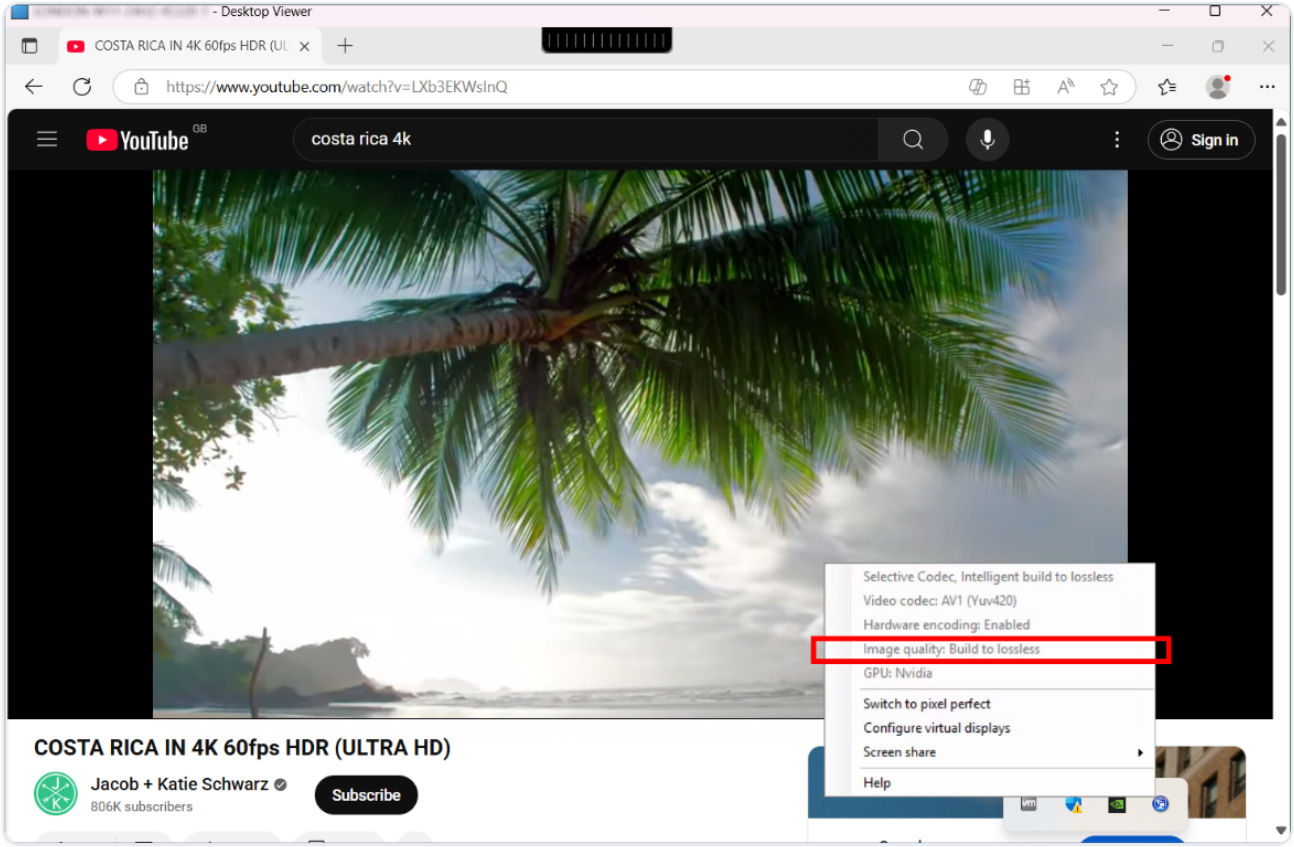
7. ポリシーが有効になっており、正しく優先順位付けされており、適切な**デリバリーグループ**またはユーザーフィルターに適用されていることを確認します。



Intelligent Build to Lossless がユーザーセッションで利用可能であるが、まだアクティブ化されていない場合、セッションは通常の選択的エンコーディングを使用し、グラフィックステータスインジケーターは、これを最上行に「Selective Codec, Intelligent Build to Lossless」と表示します。Intelligent Build to Lossless がまだ有効になっていないため、「Visual Quality」には、現在構成されている視覚品質（例: 低、中、高）が表示されます。

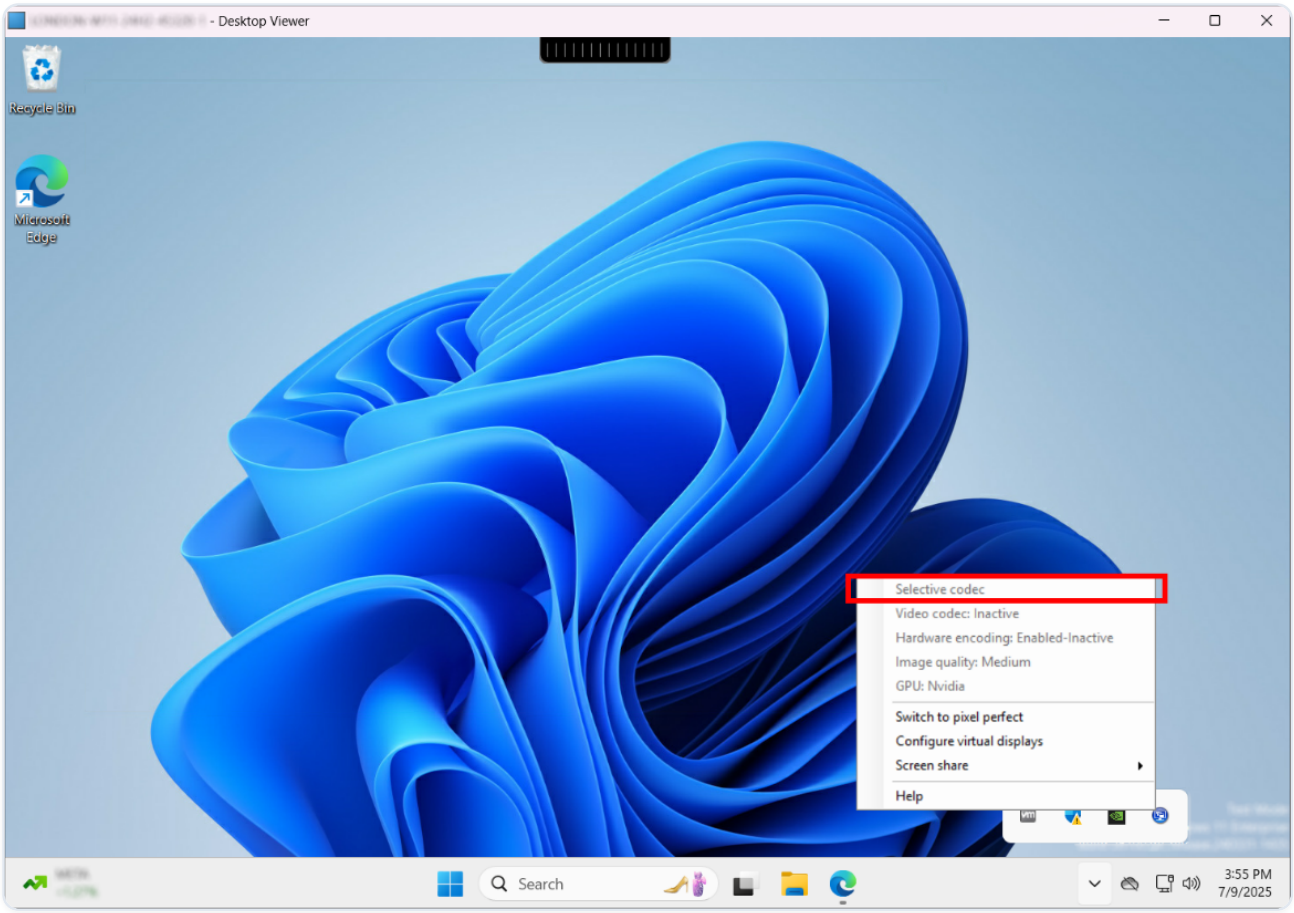


Thinwire が1つ以上の接続されたモニターでIntelligent Build to Lossless を有効にするのに好ましい条件を検出すると、グラフィックステータスインジケーターは、4行目の「Visual Quality」を「Build to Lossless」に変更します。これが、Intelligent Build to Lossless がアクティブであることを示す主要なインジケーターです。



ThinwireがBuild to Losslessの必要性がなくなったと判断すると、ピクセルパーフェクトな画像に徐々に構築し、その後、通常のSelective Encodingに戻ります。グラフィックステータスインジケーターは、画質を構成済みのVisual Qualityモード（例：低、中、高）に戻します。

Intelligent Build to Losslessが利用できない場合（たとえば、2503より前のリリースのVDAを使用している場合、サーバー側GPUのないVDAを使用している場合、またはIntelligent Build to Losslessが明示的に無効になっている場合）、グラフィックステータスインジケーターは、代わりに最上行に「Selective Codec」と表示します。



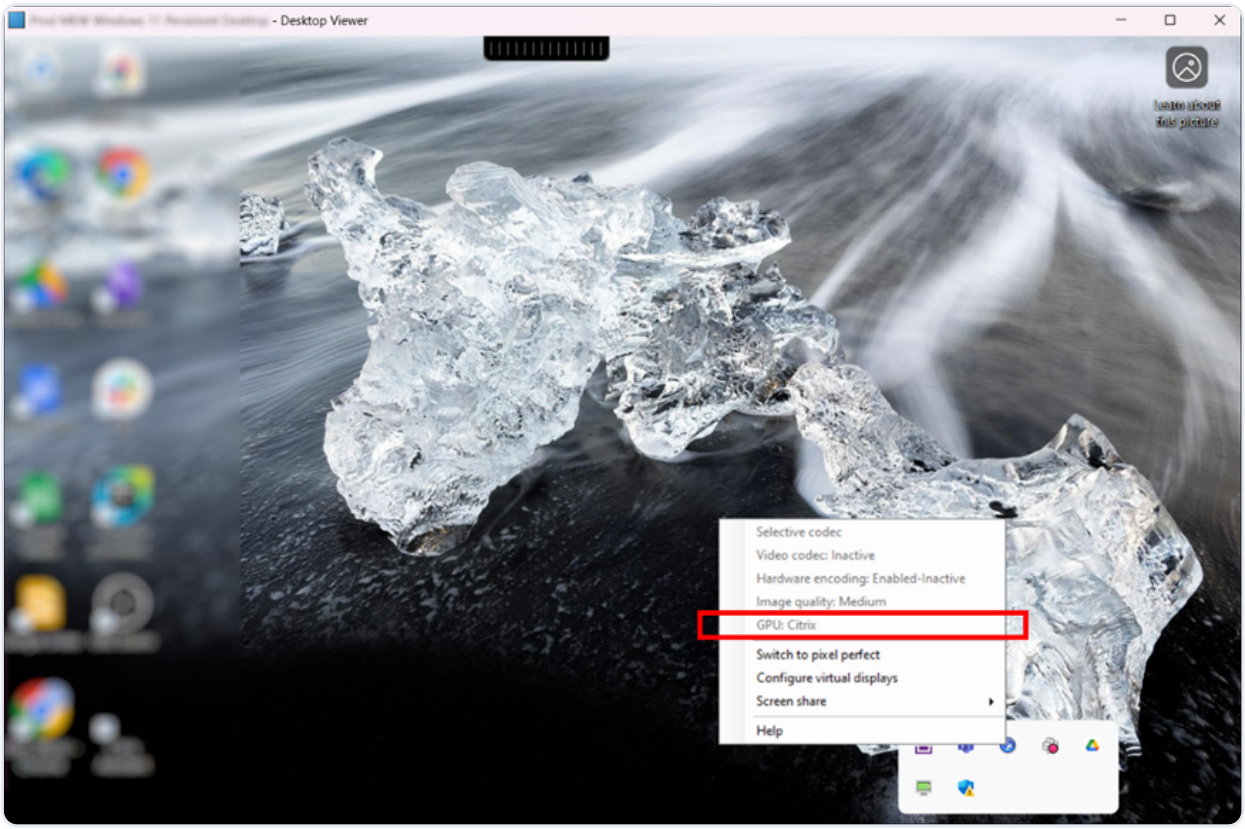
Intelligent Build to Losslessのより詳細なテストと監視のために、どのモニターがBuild to Losslessモードであるかを示すモニターごとの視覚インジケーターを有効にすることもできます。

この設定は、テストとトラブルシューティングのみを目的としており、製品環境では使用しないでください。詳細については、Intelligent Build to Losslessの視覚インジケーターを有効にするためのKB記事を参照してください。

トラブルシューティング

セッションでIntelligent Build to Losslessが利用できない場合は、以下の要件を確認してください。

1. VDAがバージョン2503以降で実行されていることを確認してください。
2. セッションでサーバー側のGPUが利用可能であることを確認してください。これを検証する最も簡単な方法は、グラフィックスステータスインジケーターを使用して、GPU行にGPUベンダー名（例：NVIDIA、Intel、AMD）が表示されているかを確認することです。GPUが存在せず利用できない場合、GPUベンダー名は「Citrix」と表示されます。



あるいは、Citrix Monitorを使用して、VDAのサーバー側GPUの有無を確認し、GPU使用率のトラブルシューティングを行うことができます。

3. 「圧縮にビデオコーデックを使用する」ポリシーが、設定されていない（デフォルト値を使用している）か、または「優先する場合に使用」に設定されていることを検証してください。

ポリシーモデリングウィザードを使用して、ポリシーがセッションに正しく適用されているかを確認できます。

DaaS側の詳細については、ポリシープロセスを参照してください。

ビデオコーデックは使用しないでください

リモートセッションのエンコードにビデオコーデックを使用することには、いくつかの利点があります。高速で比較的軽量です。ビデオコーデックは、リモートセッションでよくあるように、動画の処理に優れており、そのために設計されています。

しかし、画質や色精度が最優先される場合など、ビデオコーデックの使用が最適なソリューションではないシナリオもあります。当社の選択的エンコーダーは、ほとんどの場合、画面のどの部分がビデオコーデックによるエンコードの恩恵を受けるかを非常にうまく判断します。また、Thinwireに画面圧縮のためにビデオコーデックを一切使用しないように強制することもできます。

Thinwireがビデオコーデックを使用しないように設定されている場合、Twinwireは圧縮にJPEGとロスレスRLEのみを使用し、可能な限り最高の画質を維持します。Thinwireは、選択的エンコードまたはフルスクリーンエンコードを使用する場合よりも、かなり多くの帯域幅を使用します。

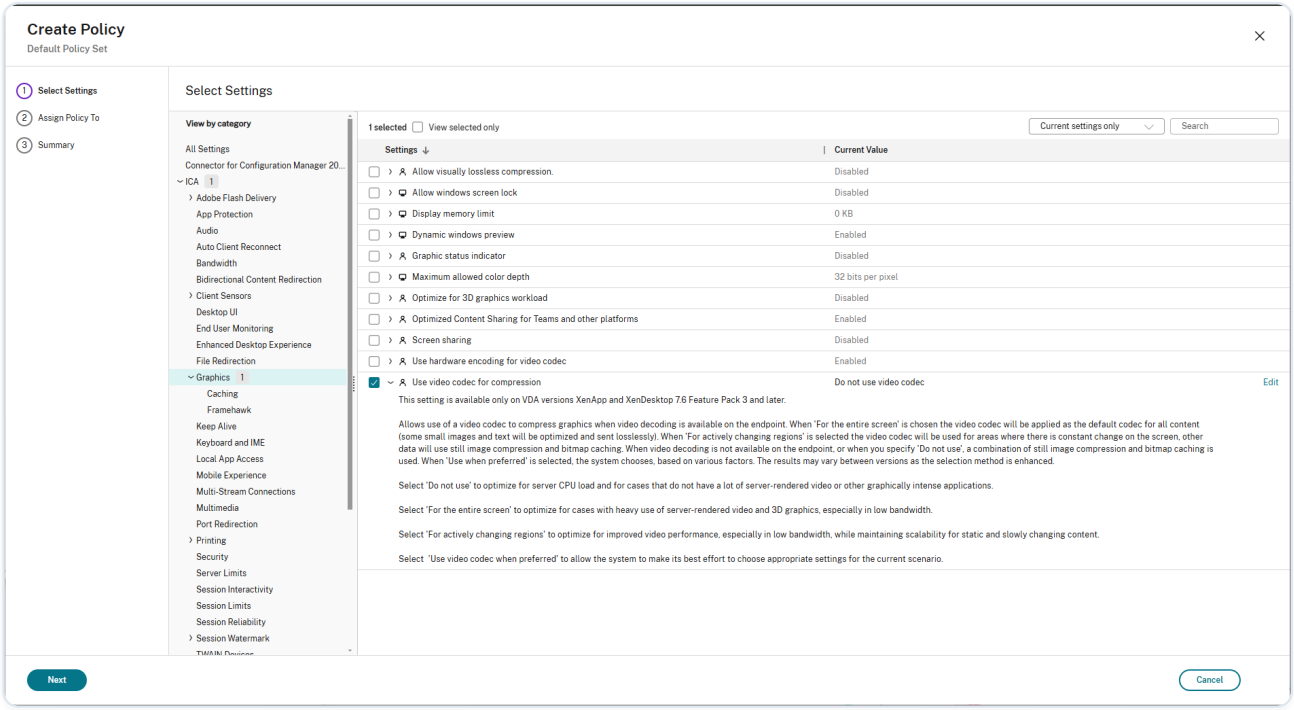
ビデオコーデックを使用しない場合

画質とVDAのスケーラビリティが最も重要な要素となるシナリオでは、当社のThinwireフルスクリーンエンコーダーモードの使用を検討できます。ビデオコーデックを使用しないことで、一般的に圧縮にビデオコーデックを使用する場合よりもCPUオーバーヘッドが低いため、VDAのスケーラビリティを最大化できます。

ただし、これらのほとんどのケースでは、当社の選択的エンコーダーは、特にBuild to losslessまたはインテリジェントBuild to losslessと組み合わせた場合、ビデオコーデック圧縮を使用しない場合よりも、同じ品質、より優れたパフォーマンス、およびより低い帯域幅を提供します。

構成

Thinwireポリシー「圧縮にビデオコーデックを使用する」を「ビデオコーデックを使用しない」に設定します。

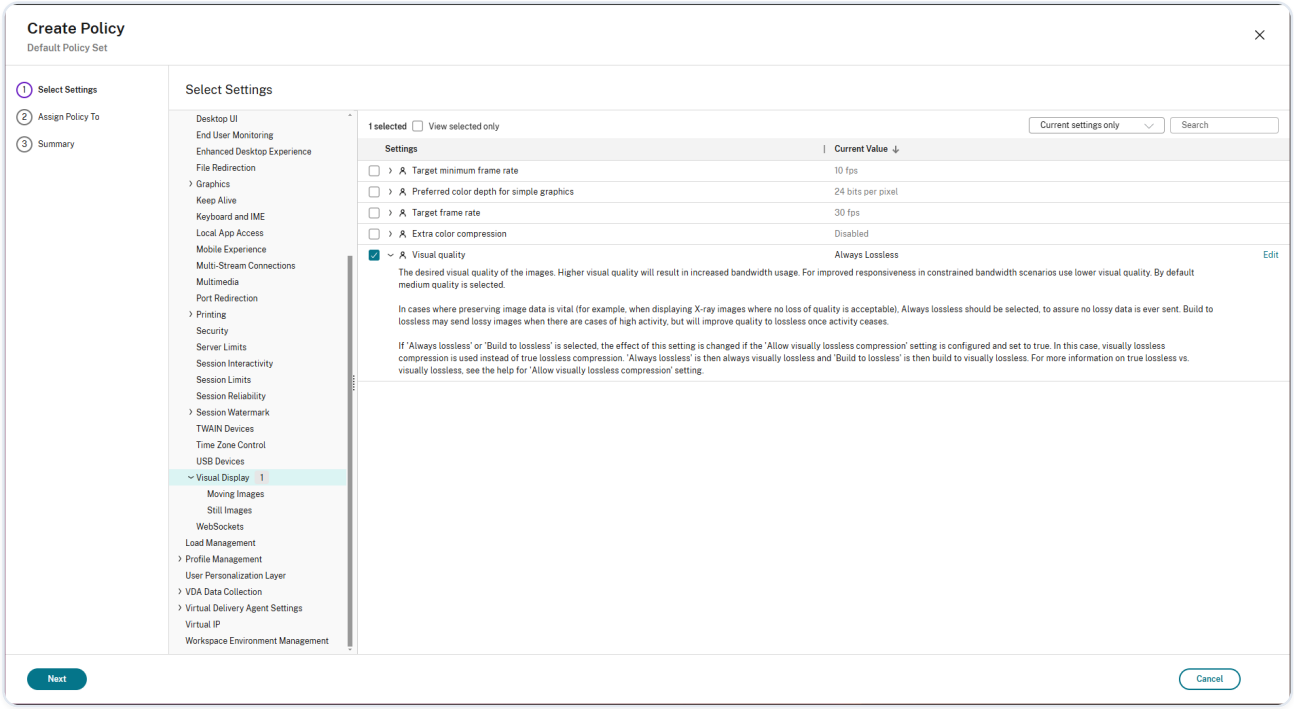


常時ロスレスモード

常時ロスレスモードを使用すると、画像が劣化したデータがクライアントに送信されることはありません。つまり、すべてのフレームはロスレスコーデックでのみエンコードされ、品質はピクセルパーフェクトになります。

常時ロスレスの圧縮率は、他のモードを使用する場合ほど良くなく、常時ロスレスモードを設定すると、かなりの帯域幅が使用されます。これにより、十分な帯域幅が利用できない場合、インタラクティブ性に大きな影響を与える可能性があります。

Citrix® は、医用画像処理のユースケースなど、ロスレスの画質が要求される特定のユースケースでのみ、この設定の使用を推奨しています。

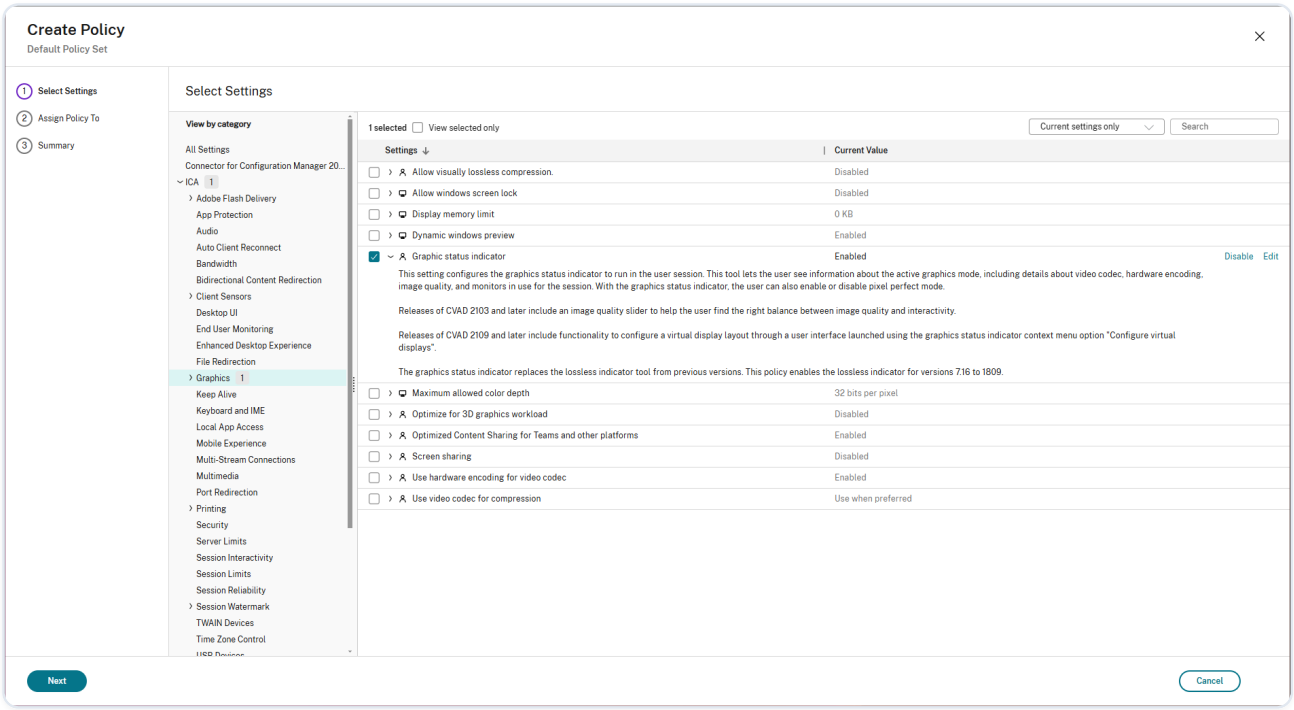


常時ロスレスモードを明示的に設定するだけでなく、エンドユーザーはグラフィックステータスインジケーターが利用可能な場合、セッション中にロスレスモードを切り替えることもできます。

現在、グラフィックステータスインジケーターはデフォルトでは有効になっていません。

グラフィックステータスインジケーターを有効にするには：

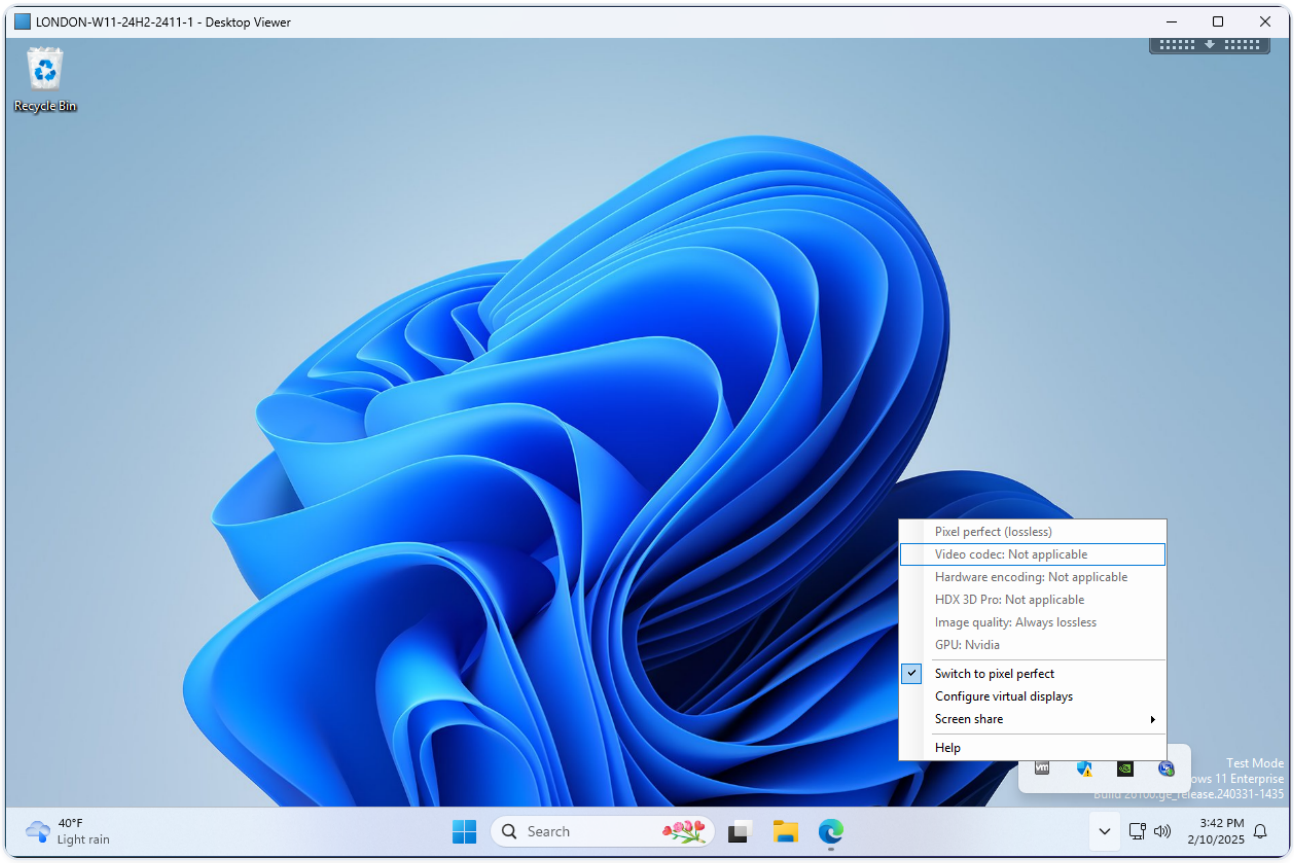
1. Citrix Studio でグラフィックポリシー設定に移動します。
2. 「グラフィックステータスインジケーター」ポリシーを見つけます。
3. ポリシーを「有効」に設定します。
4. ポリシーの変更を適用し、デリバリーグループに伝播します。



エンドユーザーとして常時ロスレスモードを切り替えるには：

1. タスクトレイでグラフィックステータスインジケーターを見つけます。
2. VDAのタスクトレイにあるグラフィックスステータス 1. 1. インジケーターを右クリックします。
3. 「ピクセルパーフェクトに切り替え」を選択します。

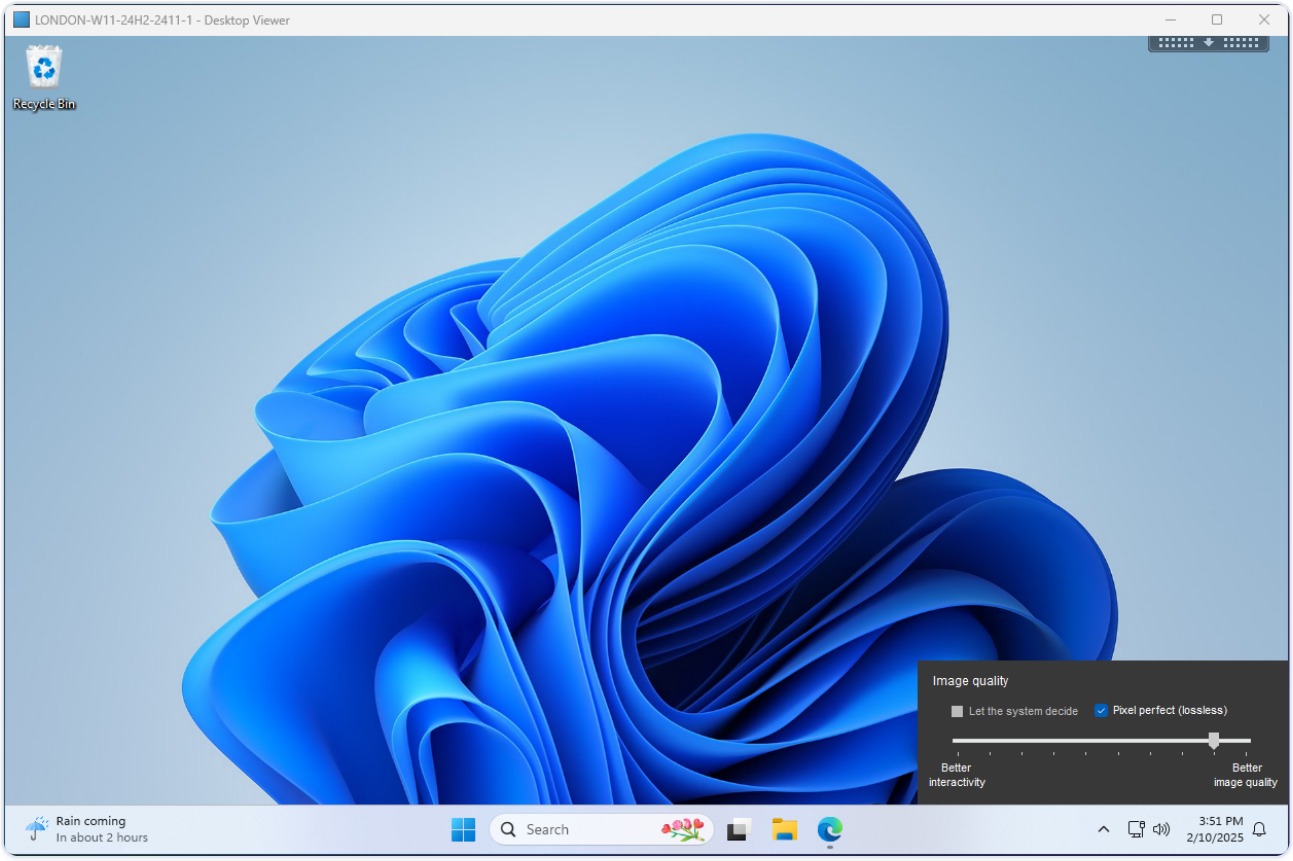
グラフィックスステータスインジケーターのアイコンに緑色のインジケーターが表示され、ロスレスモードが有効になっていることを示します。



または:

1. タスクトレイにあるグラフィックスステータスインジケーターを見つけます。
2. VDAのタスクトレイにあるグラフィックスステータスインジケーターをクリックします。
3. 「システムに決定させる」の選択を解除します。
4. 「ピクセルパーフェクト (ロスレス)」を選択します。

グラフィックスステータスインジケーターのアイコンに緑色のインジケーターが表示され、ロスレスモードが有効になっていることを示します。



カラースペース

これは、YUV 4:2:0 および YUV 4:4:4 のカラースペースと色圧縮設定について説明する新しいセクションです。

概要

選択されたカラースペースによって、HDX™ Graphics が使用する色圧縮モード（クロマサブサンプリングとも呼ばれます）が決まります。デフォルトでは、HDX Graphics は YUV 4:2:0 クロマサブサンプリングを使用します。

クロマサブサンプリングは、VDAからクライアントにビデオデータを送信するために必要な帯域幅を削減するために使用される技術です。人間の目は色の変化（色度）よりも明るさ（輝度）の変化に敏感であるため、送信される色情報の量を減らすことで機能します。

4:2:0、4:2:2、4:4:4 のような比率で示される、さまざまなクロマサブサンプリング方式が存在します。これらの比率は、輝度情報に対してサンプリングされる色度情報の量を表します。

4:4:4 - クロマサブサンプリングなし。すべての色情報が保持されます。これにより、最高の画質と色精度が得られますが、最も多くの帯域幅を必要とします。

4:2:0 - 色度情報は、水平方向と垂直方向の両方で2分の1にサブサンプリングされます。これにより、最大の帯域幅削減が実現されますが、目立つ色のにじみが発生する可能性があります。



Citrix HDX グラフィックは、仮想デスクトップ環境での帯域幅の使用を最適化するためにクロマサブサンプリングを利用します。デフォルトでは、HDX は画面コンテンツのエンコードに YUV 4:2:0 を使用します。これにより、一般的なオフィス生産性アプリケーション/ほとんどのユースケースにおいて、画質と帯域幅効率の良好なバランスが提供されます。

画面全体がビデオコーデック（フルスクリーンエンコーダーを使用）でエンコードされると、色圧縮により、テキストなどの高コントラストの詳細が劣化し、ぼやけて読みにくくなる可能性があります。

医療画像処理、ビデオ編集、CAD/CAM アプリケーションなど、色精度が最重要となるシナリオでは、HDX は YUV 4:4:4 もサポートしています。

これにより、エンコード中に色情報が失われないことが保証され、可能な限り最高の画像忠実度と色精度が提供されます。YUV 4:4:4 は YUV 4:2:0 よりも大幅に多くの帯域幅を使用することに注意してください。

帯域幅の輻輳に関連する問題を回避するため、実稼働環境で YUV 4:4:4 を有効にする前に、テストシナリオで帯域幅の使用状況を検証してください。

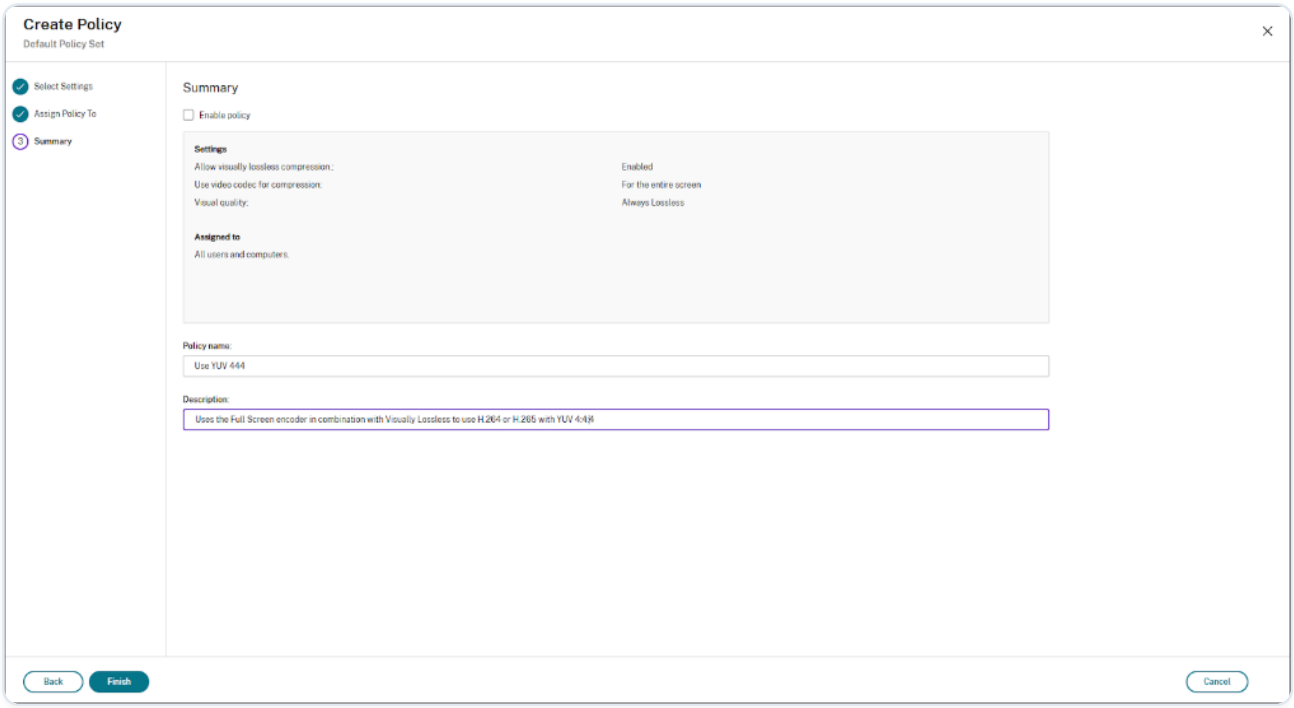
構成

YUV 4:4:4でより高い画質と色精度を使用するには、Citrix Studio内でいくつかのHDX™ポリシー設定を調整してYUV 4:4:4を有効にする必要があります。

圧縮にビデオコーデックを使用: これを「画面全体」に設定して、ビデオコーデック（および選択されたクロマサブサンプリング）を画面全体のコンテンツに適用します。

視覚品質: 帯域幅の消費よりも画質を優先するには、「ロスレスにビルド」または「常にロスレス」を選択します。

視覚的にロスレスを許可: 視覚的にロスレスな圧縮を可能にするには、このポリシーを有効にします。



デフォルトでは、ThinwireはH.264 YUV 4:4:4を使用し、クライアントで互換性のあるハードウェアが検出された場合、Thinwireは自動的にH.265 YUV 4:4:4ハードウェアデコードを使用します。

H.265 YUV 4:4:4を使用すると、社内テストでは、H.264 4:4:4と比較してフレーム/秒 (FPS) が4倍に増加し、H.264と比較してフレームあたりのサイズが2.5倍に削減されることが示されています。これはH.265の優れた効率性によるものです。

要件

H.264 を使用する YUV 4:4:4 には追加要件はありません。H.265 YUV 4:4:4 には以下のクライアント要件があります。

- Windows 用 Citrix Workspace™ アプリ 2305 以降
- H.265 サポートを有効にする
- H.265 4:4:4 デコードをサポートするクライアント GPU:
  - NVIDIA Turing 以降
  - Intel 第10世代以降

> **注:**
>
> 本稿執筆時点では、AMD は H.265 4:4:4 デコードをサポートしていません。

> VDA が自動ビデオコーデック選択で YUV 4:4:4 を使用するように構成されている場合、H.265 YUV 4:4:4 が自動的に使用されます。詳細については、自動ビデオコーデック のドキュメントを参照してください。

高解像度ディスプレイ

Citrix Virtual Apps and Desktops™ を使用して高解像度ディスプレイ（6K、8K、および同等のメガピクセル数）を展開するお客様は、パフォーマンスの問題や、マウストラッキングの不整合、ディスプレイのスケーリング、DPI関連の問題などを経験する可能性があります。

一般的なオフィスモニターの従来の解像度は4K、6K、または8Kであり、「K」表記は水平解像度を示します。

6Kディスプレイの例としては、Apple Pro Display XDR（解像度6016 × 3384）とDell UltraSharp U3224KB（解像度6144 × 3456）があります。

現在、8Kモニターはごくわずかしかなく、その一例としてDell UltraSharp UP3218K（解像度7680 x 4320）があります。

Barcoは、モニターの解像度ではなく、MPまたはメガピクセル数で表示しています。最新のBarcoモニターは32MPモニターで、公称解像度は6848 x 4560です。

Citrix® は、ハードウェアリソースに応じて最大8台のモニターをサポートします。使用するGPUによっては、この最大値に他のハードウェア制限がある場合があります。

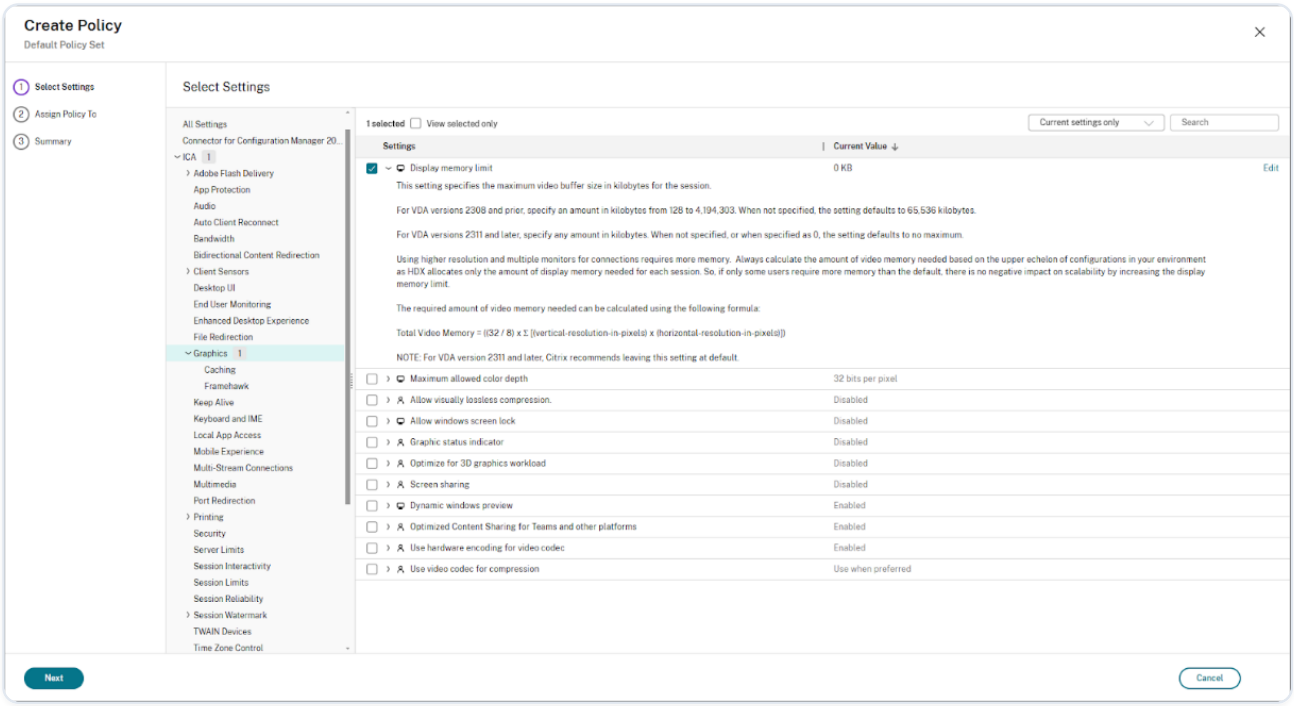
高解像度ディスプレイでのパフォーマンスを最適化し、潜在的な問題を軽減するために、CitrixはCVAD 2402の使用を推奨しています。

VDAバージョン2402以降

VDA 2402以降の場合、「Display Memory Limit」ポリシーはデフォルトの0（ディスプレイメモリ制限なし）のままにしてください。これにより、VDAは必要なディスプレイメモリを動的に割り当てることができます。

以前のVDAバージョン（2402より前）

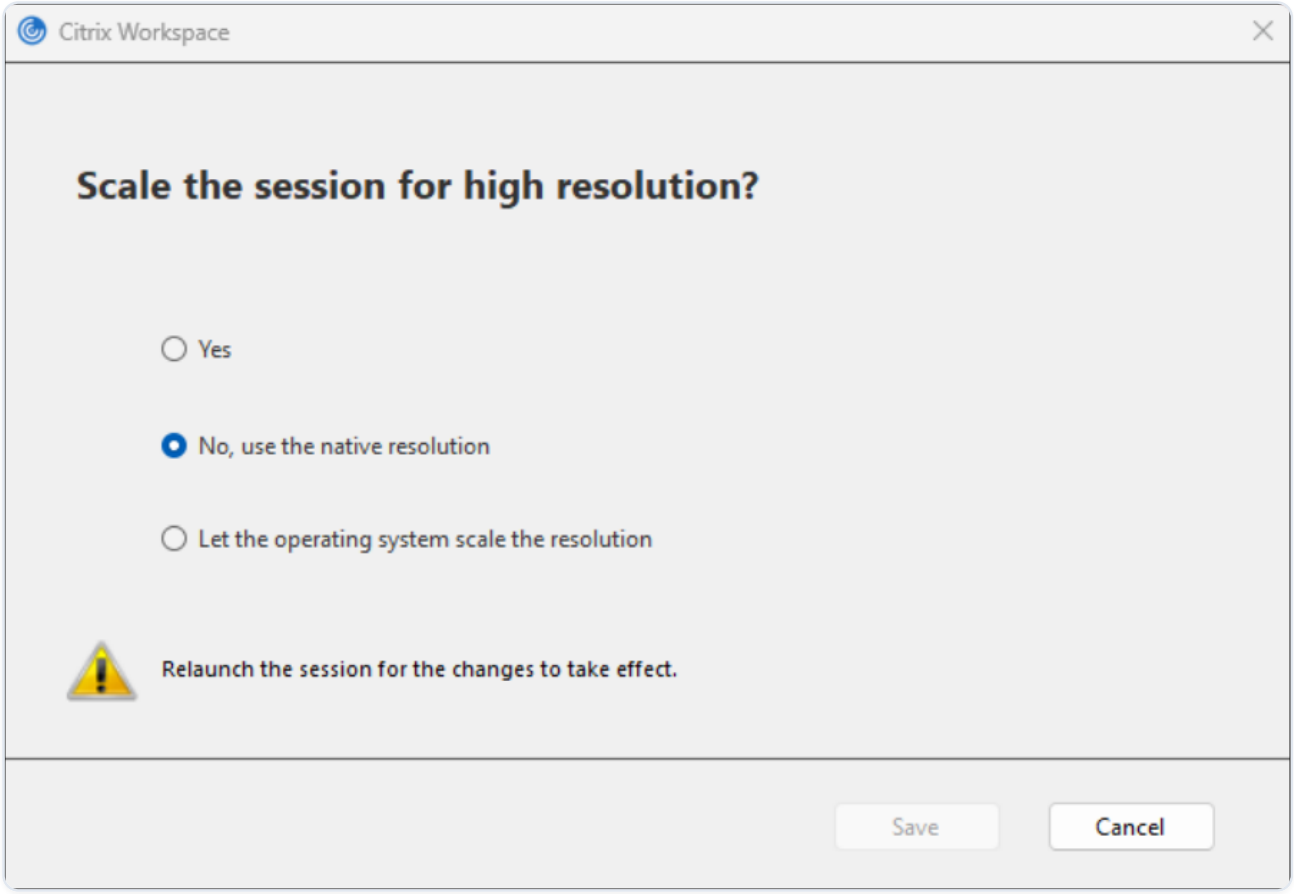
CVAD 2402以降へのアップグレードが不可能な場合は、「Display memory limit」ポリシーを最大値の4,194,303 KBに構成してください。これにより、VDAに利用可能な最大ディスプレイメモリが提供されます。



DPI スケーリング

Windows 用 CWA は、ローカルの Windows クライアントのディスプレイ解像度と DPI スケール設定を Citrix® セッションに一致させます。これは、以下のシステム要件を満たすすべてのケースで推奨されるモードです。

- シトリックス バーチャル アプリケーションズ アンド デスクトップ™ 2203 LTSR 以降
- Windows Server 2019 以降で実行されているマルチセッション OS VDA
- Windows 10 以降で実行されているシングルセッション OS VDA
- Windows 用 CWA 2203 LTSR 以降



Citrix は、Citrix Workspace™ アプリケーション バージョン 2402 以降の使用を推奨します。

詳細については、Citrix Workspace ドキュメントを参照してください。

GPU

高解像度ディスプレイの場合、使用するGPU（VDAとエンドポイントの両方）が高解像度ディスプレイを駆動するための要件を満たしていることを確認してください。サポートされている解像度とリフレッシュレートについては、GPUベンダーのドキュメントを参照してください。

サーバー側GPUを使用する場合、Citrix®は以下の最小GPUフレームバッファサイズを推奨します。

モニターと解像度	推奨フレームバッファサイズ
1 x 4K	2GB
4 x 1080p	2GB
2 x 4K	4GB
1 x 6K	4GB

モニターと解像度	推奨フレームバッファサイズ
1 x 8K	8GB
2 x 6K	8GB
4 x 4K	8GB

注:

これらは、HDX™グラフィックスエンコーディングの最小推奨フレームバッファサイズです。アプリケーションのフレームバッファ要件を参照し、サイジングにこれらを考慮してください。

NVDIA GPUのフレームバッファサイジングに関する詳細については、NVIDIAサイジングガイドを参照してください。

Intel GPUのGPUサイジングに関する詳細については、Intel Virtual Desktop Infrastructure (VDI) Performance on Intel® Data Center GPU Flex Series Whitepaperを参照してください。

詳細情報については、こちらを参照してください。

パフォーマンスとスケーラビリティに関する考慮事項

高解像度とモニターの数は、セッションパフォーマンスとサーバーのスケーラビリティに直接影響します。

高解像度化と複数のモニターの使用により、帯域幅の消費が増加します。帯域幅の制約は、フレームレートを制限し、画質を低下させる可能性があり、その結果、セッションのインタラクティブ性やユーザーエクスペリエンスに影響を与えます。

エンドポイントデバイスは、目的のディスプレイ構成をサポートするために十分なハードウェアリソースを備えている必要があります。これは、十分なCPUリソース、場合によってはグラフィックワークロードを処理できるGPUが必要であることを意味する可能性があります。

既知の問題

NVIDIA GPUとフルスクリーンビデオコーデック、H.265エンコーディング、および4096x4096を超える解像度の組み合わせにおいて、既知の問題があります。

詳細情報については、こちらを参照してください。

回避策として、デフォルトの**「圧縮にビデオコーデックを使用する」グラフィックポリシー設定を使用するか、ポリシーを明示的に「システムに決定させる」か「アクティブに変化する領域」に設定します**。

グラフィックスのロス許容モード

グラフィックスのロス許容モードは、パケット損失と遅延が大きいネットワーク上のインタラクティブセッションのユーザーエクスペリエンスを向上させます。

これは、グラフィックスデータ伝送戦略を動的に調整することで、セッションの応答性を維持します。グラフィックスのロス許容モードは、デフォルトで有効になっています。

グラフィックのロス許容モードを使用するタイミング

パケット損失や遅延が大きいなど、ネットワークの状態が悪い環境でユーザーが仮想アプリやデスクトップに接続すると、セッションの対話性やエクスペリエンスが著しく損なわれる可能性があります。

これにより、ラグや視覚的な途切れを特徴とするユーザーエクスペリエンスの低下が生じ、生産性やユーザー満足度に悪影響を及ぼす可能性があります。

このような劣悪なネットワーク状態の影響を軽減するため、グラフィックのロス許容モードは、パケット損失と遅延が設定されたしきい値を超えると、Citrix®グラフィックエンコーダーをより積極的なパケット配信メカニズムに自動的に切り替えます。このモードは、パケット損失のレベルに比例して帯域幅の使用量を積極的に増加させ、データが効果的に配信され、セッションが対話性を維持するようにします。

グラフィックのロス許容モードには、以下の利点があります。

- **ユーザーエクスペリエンスの向上:** 困難なネットワーク環境でも、よりスムーズで応答性の高いグラフィックエクスペリエンスを提供します。
- **シームレスな操作:** このモードは、ユーザーの介入なしに、リアルタイムのネットワーク状態に基づいて自動的にアクティブ化および非アクティブ化されます。
- **生産性の維持:** ユーザーは、劣悪なネットワーク品質に妨げられることなく、効果的に作業を継続できます。

システム要件

- Citrix Virtual Delivery Agent (VDA) バージョン 2311 以降
- Citrix Workspace™ アプリ Windows用 2311 以降。

> **注:**
>
> この機能が動作するには、グラフィックポリシーの**HDX™ Adaptive Transport (EDT)とロス許容モード**の両方を有効にする必要があります。

重要な要件に関する考慮事項

帯域幅のしきい値

CVAD 2507 以降のバージョンでは、グラフィックのロス許容モードをアクティブにするには、最低 30 Mbps の帯域幅が必要です。遅延とパケット損失のしきい値が満たされていても、利用可能なセッション内帯域幅が 30 Mbps 未満の場合、この機能は有効になりません。この帯域幅のしきい値はハードコードされた値であり、構成することはできません。

構成

この機能は、Web StudioまたはグループポリシーCitrix®ポリシーを通じて管理されます。

グラフィックの損失許容モードは、デフォルトで有効になっています。

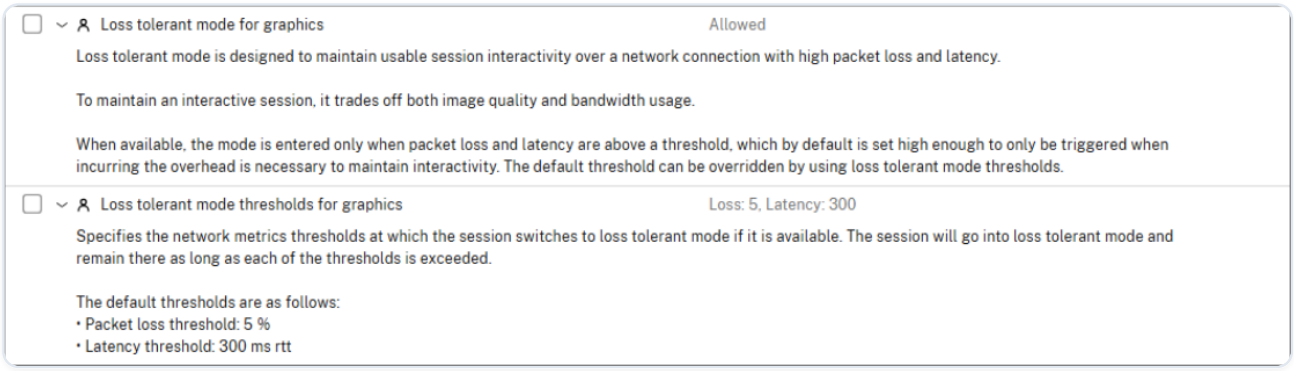
- ポリシー: グラフィックの損失許容モード
- デフォルト: 有効

グラフィックの損失許容モード機能をオフにするには、このポリシーを**無効**に設定します。

グラフィックの損失許容モードのしきい値を構成するには:

- ポリシー: グラフィックの損失許容モードのしきい値
- デフォルト値:
  - パケット損失: 5%
  - 遅延: 300 ms

このポリシーを使用すると、グラフィックの損失許容モードをトリガーするネットワーク状態のしきい値を調整できます。このモードは、パケット損失と遅延の両方の値が満たされるか超え、かつ利用可能な帯域幅が30 Mbps以上の場合にアクティブになります。



HDXグラフィック超解像度アップスケーリング

HDX グラフィックス スーパーレゾリューション アップスケーリング

HDX グラフィックス スーパーレゾリューションは、グラフィックを多用するワークロードやマルチメディアを多用するワークロードの帯域幅消費を削減しつつ、ユーザーが知覚する視覚品質を維持する、インテリジェントなクライアント支援テクノロジーです。

エンコード中にビデオ領域に追加の圧縮を選択的に適用し、クライアントのグラフィックス処理ユニット (GPU) を使用してエンドポイントで元の品質を再構築することで、HDX グラフィックス スーパーレゾリューションは、サーバー側の CPU または GPU 使用率を増加させることなく、セッションの効率を向上させます。

Citrix Virtual Apps and Desktops (CVAD) 2603以降、HDXグラフィックのスーパー解像度は一般提供 (GA) され、デフォルトで有効になっています。

主な利点

- ビデオおよび高モーションコンテンツの帯域幅消費の削減
- 帯域幅が制限されたネットワークまたは可変ネットワークでのエクスペリエンスの向上
- サーバー側 GPU の要件なし
- ユーザー操作不要の透過的な操作
- ポリシー制御による自動モードでのデフォルトで安全なアクティベーション

HDX グラフィックス スーパーレゾリューションの仕組み

HDX グラフィックス スーパーレゾリューションでは、Thinwire がまずセッション内のビデオまたは高モーション領域 (ビデオ再生やアニメーションコンテンツなど) を識別します。

Virtual Delivery Agent (VDA) は、これらの領域に意図的に追加の圧縮を適用し、エンコード中にこれらの領域を実効解像度を下げてエンコードします。 解像度が低下した領域は、大幅に少ない帯域幅を使用して送信されます。

エンドポイントでは、Citrix Workspace アプリがクライアント側の GPU を使用して、影響を受ける領域を元の解像度と視覚品質にアップスケールします。 テキストおよび静的領域は影響を受けず、可能な限り最高の品質で配信され続けます。

このアプローチにより、高品質なユーザーエクスペリエンスを維持しながら帯域幅の使用量を削減できます。

自動操作 (デフォルトの動作)

CVAD 2603では、HDXグラフィックのスーパー解像度はデフォルトで有効になっており、自動モードで動作します。自動モードでは、Thinwireが利用可能な帯域幅をリアルタイムで監視し、HDXグラフィックのスーパー解像度をいつアクティブにするかを決定します。

この機能は、以下の両方の条件が満たされた場合にのみアクティブになります。

- 互換性のあるクライアント側GPUが検出された場合
- Citrixがネットワークの状態が最適ではないと判断した場合

ネットワークの状態が改善すると、HDXグラフィックスのスーパーレゾリューションは自動的に解除され、ネットワーク品質が許す限りロスレス配信が優先されます。

この自動モードにより、管理者は手動で調整することなく、この機能を安全に有効にしておくことができます。

ポリシー構成

HDXグラフィックスのスーパーレゾリューションは、「HDX graphics super resolution」ポリシーを使用して制御されます。

管理者は、**HDX Graphics super resolution** Studioポリシーを使用して、HDXグラフィックスのスーパーレゾリューションのデフォルトの自動動作を変更できます。

HDXグラフィックスのスーパーレゾリューションモード

モード	説明	推奨される使用法
自動（デフォルト）	クライアントの機能とネットワークの状態に基づいて、	一般的なエンタープライズ環境

モード	説明	推奨される使用法
	スーパーレゾリューションを動的にアクティブ化します	
オン	超解像はすべてのビデオ領域で使用されます	帯域幅が制限されている環境、またはマルチメディアを多用する環境
オフ	超解像を明示的に無効にします	ロスレス、診断、または規制ワークフロー

自動モードを使用する場合（推奨）

- ネットワーク品質が変動したり、最適でない状態
- ユーザーワークロードが混在している
- 管理オーバーヘッドを最小限に抑えたい場合

ほとんどの環境で構成は不要です

強制的にオンにする場合

- WAN帯域幅が常に制限されている
- ビデオまたは高モーションコンテンツがワークロードの大部分を占める
- 予測可能な帯域幅削減が必要な場合

超解像を無効にする場合

- 規制または診断用のロスレスイメージングが必要な場合
- ピクセルパーフェクトなレビューワークフローが必須の場合
- 全画面エンコードが意図的に構成されている場合

他のHDXグラフィックモードとの互換性

HDXグラフィックスのスーパーレゾリューションは、デフォルトの選択的エンコードモードと連携して動作します。

「圧縮ポリシーにビデオコーデックを使用する」を以下に設定して全画面エンコードを使用する場合、スーパーレゾリューションは利用できません。

- 画面全体

「視覚品質」が以下に設定されている場合：

- 常にロスレスの視覚品質

または、視覚的にロスレスな圧縮が使用されている場合：

- 視覚的にロスレスな圧縮を使用するが有効になっている

これらのポリシー設定は、HDXグラフィックスのスーパーレゾリューションと互換性がありません。これらの設定を有効にすると、HDXグラフィックスのスーパーレゾリューションが**自動**または**有効**に設定されているかどうかにかかわらず、スーパーレゾリューションは無効になります。

自動ビデオコーデック選択

HDXグラフィックスのスーパーレゾリューションは、自動ビデオコーデック選択と連携して動作し、VDAがサーバーとクライアント間の互換性に基づいて最適なコーデックを選択できるようにします。VDAにサーバー側GPUがない場合など、ハードウェアエンコードが利用できない場合でも、スーパーレゾリューションはH.264ビデオコーデックを使用して機能します。サーバー側GPUが存在する場合、HDXグラフィックスのスーパーレゾリューションは、可能な場合はH.265またはAV1を使用したハードウェアエンコードを自動的に利用します。

システム要件

仮想配信エージェント (VDA)

- Windows VDA 2603以降
- サーバー側GPUは不要
- 追加のVDA構成は不要

クライアント要件

- Windows向けCitrix Workspaceアプリ 2603以降*
- サポートされているクライアント側GPU

*Nvidiaクライアント側GPUにはx64 Citrix Workspace Clientが必要です。

サポートされているクライアントGPU

Intel GPUのサポート

HDXグラフィックのスーパー解像度は、統合GPU（iGPU）とディスクリートクライアントGPUの両方に対応しています。

統合GPU

サポートされている統合GPU（iGPU）ファミリー：

- インテル Iris Xe (第11世代以降)
- インテル Iris Xe Max
- インテル Iris Plus グラフィックス
- インテル UHD グラフィックス (710, 730, 750, 770, P750)
- 第11世代、第12世代、第13世代プロセッサー向けIntel UHD Graphics

ディスクリートGPU

- Intel Arc – デスクトップ
  - Arc Aシリーズ: A310, A380, A580, A750, A770
  - Intel Bシリーズ: B570, B580
- Intel Arc – モバイル
  - Arc Aシリーズ モバイル: A350M, A370M, A530M, A550M, A570M, A730M, A77M
- Intel Arc – ワークステーション (Arc Pro)
  - Arc Proシリーズ: A30M, A40, A50, A60M, A60
  - Arc Pro Bシリーズ: B50, B60

Nvidia GPUのサポート

デスクトップGPU

サポートされているファミリー:

- GeForce 20シリーズ (Turing)
  - RTX 2050 – RTX 2080 デスクトップおよびモバイル (TiおよびSuperバリアントを含む)
  - タイタン RTX
- GeForce 30シリーズ (Ampere)
  - RTX 3050 – RTX 3090 デスクトップおよびモバイル (TiおよびSuperバリアントを含む)
- GeForce 40シリーズ (Ada Lovelace)
  - RTX 4050 – RTX 4090 デスクトップおよびモバイル (TiおよびSuperバリアントを含む)

- GeForce 50シリーズ (Blackwell)
  - RTX 5050–5090 デスクトップおよびモバイル

プロフェッショナルおよびワークステーションGPU

- NVIDIA Quadro (レガシーブランド)
  - Quadro RTXシリーズ: 3000、4000、5000、6000、8000 (デスクトップおよびモバイル)
  - Quadro Tシリーズ: T400、T500、T600、T1000、T1200 (デスクトップおよびモバイル)
- NVIDIA RTX (旧Quadro) – Ampereワークステーション
  - RTX Aシリーズ: A1000–A6000 デスクトップおよびモバイル
  - A800 アクティブ
- NVIDIA RTX – Ada世代ワークステーション
  - RTX Ada シリーズ: 2000, 4000, 4000 SFF, 4500, 5000, 5880, 6000
  - RTX Ada ノートPCシリーズ: RTX 500–5000 Ada (モバイル)
  - RTX PRO 6000 Blackwell ワークステーション

これは、HDXグラフィックのスーパー解像度と互換性があるはずのクライアント側GPUの網羅的ではないリストです。このリストはベンダーのドキュメントから作成されたものであり、記載されているすべてのGPUがCitrixによって検証されているわけではないことに注意してください。

Citrixは、最高のパフォーマンスを得るために、GPUベンダーから提供される最新のGPUドライバーを使用することを推奨します。

マルチGPU構成

マルチGPUエンドポイントでは、プライマリGPUアダプターのみがHDXグラフィックのスーパー解像度に使用されます。 マルチGPU構成は、マルチメディアに特化したノートPCデバイスで一般的に見られます。

HDXグラフィックのスーパー解像度プレビューからの移行

このセクションでは、HDXグラフィックのスーパー解像度プレビューからアップグレードする際の変更点と、管理者が何を期待すべきかについて説明します。

領域	プレビュー時の動作 (CVAD 2507 および 2511)	CVAD 2603以降
有効化	VDAおよびクライアント上の手動レジストリキー	デフォルトで自動的に有効
制御モデル	レジストリベース	ポリシーベース
デフォルトの状態	無効	デフォルトで自動的に有効
アクティベーションロジック	有効にすると常にアクティブ	ネットワークの状態に基づいて条件付きで適用（デフォルトの動作）*
サポートされているクライアントGPU	一部のIntel GPUおよびiGPUのみ	一部のIntel GPUおよび一部のNVIDIA GPU

HDXグラフィックのスーパーレゾリューションは、**HDXグラフィックのスーパーレゾリューションポリシー**を使用して制御されるようになりました。このポリシーは、プレビュー中に使用されていたすべてのレジストリベースの有効化を置き換えます。

必要なアクション

管理者は、Public Tech Previewでスーパー解像度を有効にするために必要だったVDAおよびクライアントのレジストリキーを安全に削除できます。CVAD 2603にアップグレードした後、HDXグラフィックのスーパー解像度を有効にするための追加のアクションは必要ありません。クライアントがWindows向けCitrix Workspaceアプリ 2603以降を実行していることを確認してください。

管理者は、帯域幅またはコンプライアンス要件に合わせて、HDXグラフィックのスーパーレゾリューションポリシーを任意で確認または調整できます。

監視とトラブルシューティング

HDXグラフィックススーパーレゾリューションは、低解像度で送信されるビデオ領域を再構築するために、クライアント側のGPU処理に依存します。その結果、スーパーレゾリューションがアクティブな場合、クライアント側のGPU使用率が増加することは予期される動作です。

> **注:**
>
> スーパーレゾリューションを有効にすると、ノートパソコンがバッテリー電源で動作している場合に、バッテリー寿命に悪影響を与える可能性があることに注意してください。

> GPU使用率のレベルは以下に依存します。

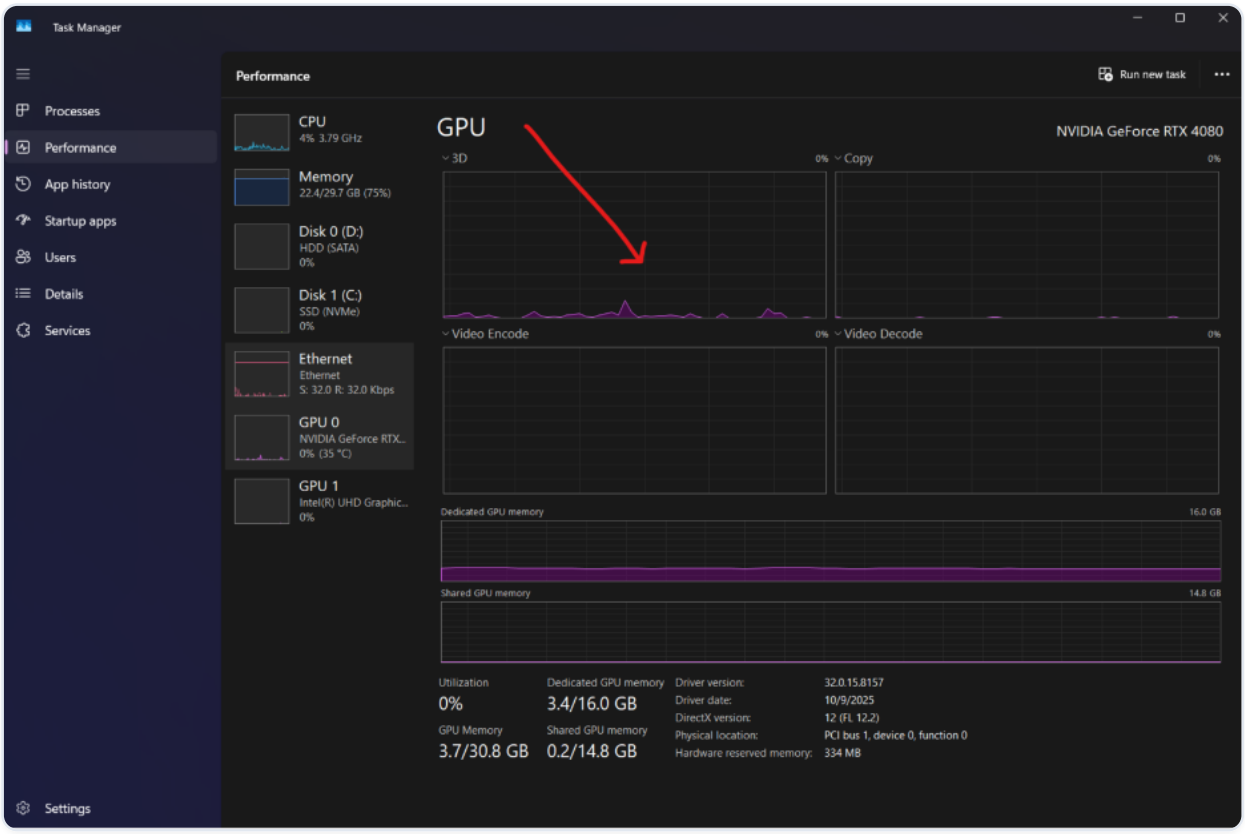
- ビデオ領域のサイズ
- コンテンツのフレームレート
- 接続されているディスプレイの数と解像度
- クライアントGPUの機能

このセクションでは、HDXグラフィックススーパーレゾリューションを使用する際に、管理者とエンドユーザーがクライアント側の活動を監視、検証、トラブルシューティングする方法について説明します。

クライアントGPU使用率の監視 (Windows)

管理者とエンドユーザーは、Windowsタスクマネージャーを使用してクライアント側のGPU使用状況を監視できます。

1. タスクマネージャーを開く
2. パフォーマンス]タブを選択する
3. 左側のメニューからを選択する
4. 以下を観察します。
    - ビデオまたは高モーションコンテンツ中のGPU使用率 (%)



HDXグラフィックのスーパー解像度がアクティブな場合、ビデオ再生中または高モーションワークロード中にGPUアクティビティが増加することが予想されます。

スーパー解像度がアクティブであることの確認

管理者は、以下の組み合わせによってHDXグラフィックのスーパー解像度がアクティブであることを確認できます。

- クライアント側のGPU使用率の増加
- ポリシーがオフに設定されている場合と比較して、セッション帯域幅の使用量が削減されること
- 表示されるアップスケーリングインジケーター (有効な場合)

ビデオ再生中にGPU使用率が増加しない場合:

- クライアントGPUがサポートされていることを確認してください
- HDXグラフィックのスーパー解像度ポリシーがオフに設定されていないことを確認してください
- 競合するグラフィックモードが有効になっていないことを確認してください

一般的なトラブルシューティングシナリオ

クライアントGPU使用率の増加なし

考えられる原因:

- HDXグラフィックのスーパー解像度ポリシーがオフに設定されている
- ネットワークの状態が良い（自動モードがアクティブにならない）
- サポートされていない、または互換性のないクライアントGPU
- GPUドライバーが古い

クライアントでのGPU使用率は、ビデオ領域のサイズとGPUの機能の両方に大きく依存します。より強力なGPUは、使用率への影響が少なくなります。

ビデオの途切れや、期待よりも低いフレームレート

考えられる原因：

- GPUドライバーが古い
- パフォーマンスの低いGPU
- ビデオ領域のサイズが大きすぎる

クライアントのGPU使用状況を監視してください。GPU使用率が予想よりも著しく高い場合、クライアントのGPUは、使用されている解像度に対してスーパー解像度アップスケーリングに対応できない可能性があります。

クライアントのパフォーマンスに関する懸念

ユーザーが応答性の低下やパフォーマンスの低下を経験した場合：

- エンドポイントのGPU総使用率を監視する
- 可能な場合は、ビデオ再生の解像度またはフレームレートを下げる
- ポリシーモードを「オン」ではなく「自動」の使用を検討する
- マルチモニターまたは高解像度のワークロードに対して、エンドポイントハードウェアが推奨仕様を満たしていることを検証します

サポートデータ収集の推奨事項

スーパーレゾリューションでのクライアント側の動作をトラブルシューティングする際は、Citrixは以下の情報を収集および確認することを推奨します。

- Citrix Workspaceアプリのバージョン

- クライアントGPUモデルとドライバーバージョン
- 接続されているモニターの数と解像度
- HDXグラフィックのスーパーレゾリューションポリシー設定
- 再現時のクライアントGPU使用率

この情報は、観察された動作が予期されたものか、ハードウェアに関連するものかを判断するのに役立ちます。

シンワイヤー

Thinwireを搭載したHDX™ Graphicsは、高性能で適応性が高く、効率的なリモートデスクトップおよびアプリケーションエクスペリエンスを提供する、Citrixの高度なディスプレイ技術です。

Thinwireは、グラフィックデータをインテリジェントに分析、キャッシュ、圧縮することにより、多様なネットワーク条件やエンドポイントデバイス全体で最適なパフォーマンスを保証します。

HDX™ 3D プロ

HDX 3D Pro（現在はHDX Graphicsとして知られています）は、要求の厳しいグラフィックワークロードに対して高性能なユーザーエクスペリエンスを提供します。デフォルトでは、GPUを活用してDirectXおよびOpenGLアプリケーションの両方にハードウェアアクセラレーションを提供します。以前はHDX 3D Proに関連付けられていたこの機能は、追加のポリシーや構成を必要とせずに、すべてのユーザーが標準で利用できるようになりました。

ハードウェアアクセラレーションを使用することで、設計、エンジニアリング、マルチメディア制作などの分野で使用される、最もグラフィックを多用するアプリケーションであっても、ユーザーにシームレスで応答性の高いエクスペリエンスを提供できます。

Citrix Virtual Apps and Desktops™のHDX 3D Pro機能を使用すると、ハードウェアアクセラレーションのためにグラフィック処理ユニット（GPU）を使用すると最高のパフォーマンスを発揮するデスクトップとアプリケーションを提供できます。これらのアプリケーションには、OpenGLおよびDirectXベースの3Dプロフェッショナルグラフィックアプリケーションが含まれます。標準VDAは、DirectXのGPUアクセラレーションのみをサポートします。

HDX 3D Proポリシー設定については、「3Dグラフィックワークロードの最適化」(/ja-jp/citrix-virtual-apps-desktops/current-release/policies/reference/ica-policy-settings/graphics-policy-settings.html#optimize-for-3d-graphics-workload)を参照してください。

サポートされているすべてのCitrix Workspaceアプリは、3Dグラフィックで使用できます。複雑な3Dワークロード、高解像度モニター、マルチモニター構成、高フレームレートアプリケーションで最高のパフォーマンスを得るには、Citrix Workspace app for WindowsおよびCitrix Workspace app for Linuxの最新バージョンをお勧めします。Citrix Workspaceアプリのサポートされているバージョンに関する詳細については、Citrix Workspaceアプリのライフサイクルマイルストーンを参照してください。

3Dプロフェッショナルアプリケーションの例は次のとおりです。

- コンピューター支援設計、製造、エンジニアリング (CAD/CAM/CAE) アプリケーション
- 地理情報システム (GIS) ソフトウェア
- 医用画像処理通信システム (PACS)
- 最新のOpenGL、DirectX、NVIDIA CUDA、OpenCL、およびWebGLバージョンを使用するアプリケーション
- 並列コンピューティングにNVIDIA Compute Unified Device Architecture (CUDA) GPUを使用する計算集約型の非グラフィックアプリケーション

HDX 3D Proは、あらゆる帯域幅で最高のユーザーエクスペリエンスを提供します。

- WAN接続の場合：1.5 Mbpsという低い帯域幅のWAN接続でも、インタラクティブなユーザーエクスペリエンスを提供します。
- LAN接続の場合：LAN接続でローカルデスクトップと同等のユーザーエクスペリエンスを提供します。

  複雑で高価なワークステーションを、グラフィック処理をデータセンターに移動して一元管理することで、よりシンプルなユーザーデバイスに置き換えることができます。

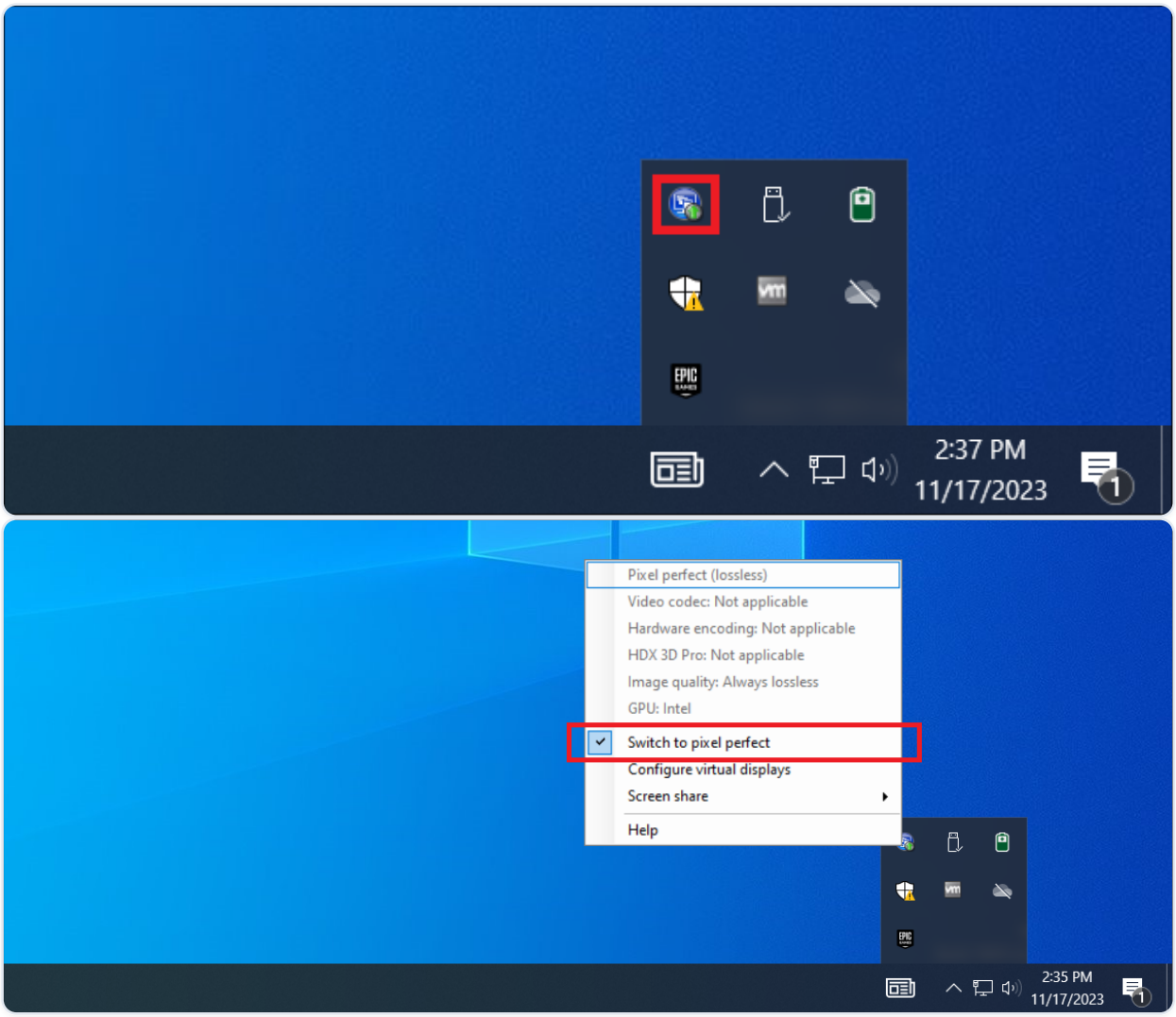
特殊なユースケース向けのロスレス圧縮オプション

HDX 3D Proは、医用画像処理など、ピクセルパーフェクトなグラフィックが必要なアプリケーションをサポートするために、CPUベースのロスレスコーデックも提供します。真のロスレス圧縮は、より多くのネットワークリソースと処理リソースを消費するため、特殊なユースケースでのみ推奨されます。

ロスレス圧縮を使用する場合：

- 通知領域アイコンであるグラフィックステータスインジケーターのロスレスインジケーターは、表示されている画面がロッシーフレームかロスレスフレームかをユーザーに通知します。

このアイコンは、**視覚品質**ポリシー設定で**ロスレスにビルド**が指定されている場合に役立ちます。送信されるフレームがロスレスの場合、ロスレスインジケーターは緑色に変わります。



- ロスレススイッチを使用すると、セッション中にいつでも**常にロスレス**モードに変更できます。セッション内で**ロスレス**を選択または解除するには、アイコンを右クリックして**ピクセルパーフェクトに切り替え**をクリックするか、ショートカットALT+SHIFT+1を使用します。
    - ロスレス圧縮の場合：HDX 3D Proは、ポリシーで選択されたコーデックに関係なく、ロスレスコーデックを圧縮に使用します。
    - ロッシー圧縮の場合：HDX 3D Proは、デフォルトまたはポリシーによって選択された元のコーデックを使用します。 ロスレススイッチの設定は、以降のセッションでは保持されません。すべての接続でロスレスコーデックを使用するには、**視覚品質ポリシー**設定で**常にロスレス**を選択します。

セッション内でロスレスを選択または選択解除するためのデフォルトのショートカットALT+SHIFT+1を上書きできます。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\LLIndicator`で新しいレジストリ設定を構成します。

- 名前: HKEY_LOCAL_MACHINE_HotKey, 種類: String
- ショートカットの組み合わせを設定する形式は、C=0|1, A=0|1, S=0|1, W=0|1, K=val です。キーはコンマ「,」で区切る必要があります。キーの順序は関係ありません。
- A、C、S、W、Kはキーであり、C=Control、A=ALT、S=SHIFT、W=Win、K=有効なキーです。Kに許可される値は、0〜9、a〜z、および任意の仮想キーコードです。
- 例： F10の場合、K=0x79を設定 Ctrl + F10の場合、C=1, K=0x79を設定 Alt + Aの場合、A=1, K=a または A=1, K=A または K=A, A=1を設定 Ctrl + Alt + 5の場合、C=1, A=1, K=5 または A=1, K=5, C=1を設定 Ctrl + Shift + F5の場合、A=1, S=1, K=0x74を設定

HDX 3D Proのユーザーエクスペリエンスを最適化する

複数のユーザーが限られた帯域幅の接続を共有している場合（たとえば、支店など）、各ユーザーが利用できる帯域幅を制限するために、全体セッション帯域幅制限ポリシー設定を使用することをお勧めします。この設定を使用すると、ユーザーがログオンおよびログオフしても、利用可能な帯域幅が大きく変動しないようにすることができます。HDX 3D Proは利用可能なすべての帯域幅を使用するように自動的に調整されるため、ユーザーセッション全体で利用可能な帯域幅が大きく変動すると、パフォーマンスに悪影響を及ぼす可能性があります。 たとえば、20人のユーザーが60 Mbpsの接続を共有している場合、各ユーザーが利用できる帯域幅は、同時ユーザー数に応じて3 Mbpsから60 Mbpsの間で変動する可能性があります。このシナリオでユーザーエクスペリエンスを最適化するには、ピーク時にユーザーごとに必要な帯域幅を決定し、常にその量にユーザーを制限します。 3Dマウスのユーザーの場合、汎用USBリダイレクト仮想チャネルの優先度を0に上げることをお勧めします。仮想チャネルの優先度を変更する方法については、Knowledge Centerの記事CTX128190を参照してください。 HDX Monitorツールを使用して、HDX視覚化テクノロジーの操作と構成を検証し、HDXの問題を診断およびトラブルシューティングします。このツールは、Citrix Virtual Apps and Desktops™インストールメディアの**Support**フォルダーにあります。

GPU アクセラレーション

HDX™ Graphics は、Virtual Delivery Agent (VDA) とエンドポイントデバイスの両方で GPU ハードウェアをシームレスに活用します。

以前は HDX 3D Pro として知られていたこのすぐに使えるハードウェアアクセラレーションは、デフォルトで有効になっており、シングルセッションおよびマルチセッションオペレーティングシ

ステムの両方で、グラフィックを多用する DirectX および OpenGL アプリケーションのパフォーマンスを大幅に向上させます。

Citrix Virtual Apps and Desktops™ は、Windows マルチセッション OS セッションで実行されるグラフィックを多用するアプリケーションを、サーバーのグラフィック処理ユニット (GPU) でレンダリングすることをサポートします。OpenGL、DirectX、Direct3D、および Windows Presentation Foundation (WPF) のレンダリングをサーバーの GPU に移動することで、サーバーの CPU をより効率的に使用できます。

Windows Server はマルチユーザーオペレーティングシステムであるため、複数のユーザーが GPU 仮想化 (vGPU) を必要とせずに Citrix Virtual Apps™ によってアクセスされる GPU を共有できます。

レジストリの編集を伴う手順については、注意してください。レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題を引き起こす可能性があります。Citrix® は、レジストリエディターの誤った使用によって生じる問題が解決できることを保証できません。レジストリエディターは自己責任で使用してください。編集する前にレジストリをバックアップしてください。

GPU 共有

GPU 共有により、リモートデスクトップセッションで OpenGL および DirectX アプリケーションの GPU ハードウェアレンダリングが可能になります。次の特性があります。

- アプリケーションのスケーラビリティとパフォーマンスを向上させるために、ベアメタルまたは仮想マシンで使用できます。
- 複数の同時セッションで GPU リソースを共有できます (ほとんどのユーザーは専用 GPU のレンダリングパフォーマンスを必要としません)。
- 特別な設定は必要ありません。

GPU は、ハイパーバイザーおよび GPU ベンダーの要件に従って、フルパススルーモードまたは仮想 GPU (vGPU) モードのいずれかで Windows Server 仮想マシンに割り当てることができます。物理 Windows Server マシンへのベアメタル展開もサポートされています。

GPU 共有は、特定のグラフィックカードに依存しません。

- 仮想マシンについては、使用中のハイパーバイザーと互換性のあるグラフィックカードを選択してください。XenServer のハードウェア互換性リストについては、「Hypervisor Hardware Compatibility List」を参照してください。

- ベアメタルで実行する場合、オペレーティングシステムによって単一のディスプレイアダプターが有効になっていることを推奨します。複数の GPU がハードウェアにインストールされている場合は、デバイスマネージャーを使用して、1 つを除くすべてを無効にしてください。

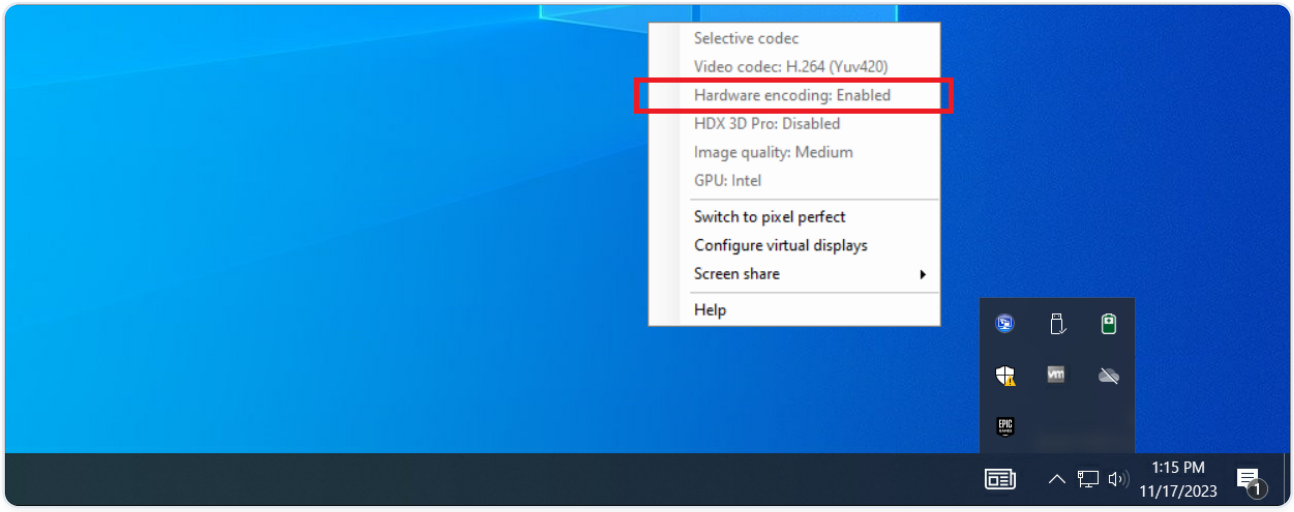
GPU Sharing を使用したスケーラビリティは、いくつかの要因によって異なります。

- 実行されているアプリケーション
- 消費するビデオ RAM の量
- グラフィックカードの処理能力

一部のアプリケーションは、他のアプリケーションよりもビデオ RAM の不足をうまく処理します。ハードウェアが過負荷になると、グラフィックカードドライバーの不安定化やクラッシュが発生する可能性があります。このような問題を回避するには、同時ユーザー数を制限してください。

- NVIDIA GPU および Intel Iris Pro グラフィックプロセッサ用の高性能ビデオエンコーダーへのアクセス。ポリシー設定（デフォルトで有効）がこの機能を制御し、H.264 エンコード（利用可能な場合）にハードウェアエンコードの使用を許可します。このようなハードウェアが利用できない場合、VDA はソフトウェアビデオコーデックを使用した CPU ベースのエンコードにフォールバックします。詳しくは、「グラフィックポリシー設定」を参照してください。

GPU アクセラレーションが機能していることを確認するには、グラフィックステータスインジケーターを使用できます。



DirectX、Direct3D、および WPF レンダリング

DirectX、Direct3D、および WPF レンダリングは、ディスプレイドライバーインターフェイス（DDI）バージョン 9ex、10、または 11 をサポートする GPU を搭載したサーバーでのみ利用できます。

- Windows Server 2016 以降では、RD セッションホストサーバー上の Remote Desktop Services (RDS) セッションは、Microsoft Basic Render Driver をデフォルトのアダプターとして使用します。Windows Server 2016 以降の RDS セッションで GPU を使用するには、グループポリシーの **ローカルコンピューターポリシー** \> **コンピューターの構成** \> **管理用テンプレート** \> **Windows コンポーネント** \> **Remote Desktop Services** \> **リモートデスクトップセッションホスト** \> **リモートセッション環境** で、**すべての Remote Desktop Services セッションにハードウェアの既定のグラフィックアダプターを使用する** 設定を有効にします。
- WPF アプリケーションがサーバーの GPU を使用してレンダリングできるようにするには、Windows マルチセッション OS セッションを実行しているサーバーのレジストリに設定を作成します。レジストリ設定の詳細については、レジストリで管理される機能のリストにある「Windows Presentation Foundation (WPF) レンダリング」を参照してください。

CUDAまたはOpenCLアプリケーションのGPUアクセラレーション

ユーザーセッションで実行されているCUDAおよびOpenCLアプリケーションのGPUアクセラレーションは、デフォルトで無効になっています。

CUDA アクセラレーション機能を使用するには、レジストリ設定を有効にします。詳細については、レジストリで管理される機能のリストにある「CUDA または OpenCL アプリケーションの GPU アクセラレーション」を参照してください。

10ビットハイダイナミックレンジ (HDR)

10ビットハイダイナミックレンジ (HDR) 仮想デスクトップセッションを使用すると、強化されたエンコードおよびデコード機能を利用して、拡張された色域、より高いコントラストと輝度を持つ高品質な画像やビデオをレンダリングできます。

システム要件

エンドポイント:

- NVIDIA GPU 用 Citrix Workspace™ アプリ for Windows 2209 以降
- エンドポイント上で10ビットHEVC (H.265) 444デコードをサポートするNVIDIA GPU
- 10ビットHDR対応モニター。ディスプレイ設定を使用して、すべてのモニターで10ビットHDRを有効にする必要があります。

サーバー:

- NVIDIA GPU 用 Windows シングルセッションOS VDA 2209 以降、およびIntel GPU 用 VDA 2308 以降

- VDA上で10ビットHEVC 444エンコードをサポートするNVIDIA GPU

必要なポリシー

エンドポイント:

- グラフィックのH.265デコードを有効にする

サーバー:

- 3Dグラフィックワークロード向けに最適化
- グラフィックステータスインジケーター (オプション)

サーバー構成

10ビットHDR対応のエンドポイントモニターでCitrix®セッションを起動すると、HDRセッションがデフォルトで有効になります。マルチモニターHDRセッションでは、すべてのエンドポイントモニターで10ビットHDRが有効になっている必要があります。HDRセッションは、ウィンドウモードと全画面モードの両方でサポートされます。

参照白色レベル

この設定は、ニット値によって白色輝度レベルを定義します。セッション内の相対的なHDR画面の明るさを制御します。デフォルト値は80ニットです。異なるニット値を定義するには、次のレジストリキーを設定します。

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- 種類: REG_DWORD
- 名前: RefWhiteLevel

設定を有効にするには、セッションのサイズを変更するか、セッションを切断して再起動する必要があります。

EDIDのオーバーライド

VDAをHDRセッションでエンドポイントモニターのEDIDを使用するように構成できます。これにより、色域と輝度範囲を一致させることで、モニターの表示機能を最大限に活用できます。デフォルトでは、HDRセッションはHDR1000対応のディスプレイを想定しています。 エンドポイントモニターのEDIDは、NVIDIAまたはその他のツールを使用してエクスポートできます。次のレジストリキーを使用してVDAに適用します。

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics

- 種類: REG_BINARY
- 項目名: EDIDOverride

EDIDをレジストリに保存する際、コンマ、スペース、または特殊文字を含めてはなりません。オーバーライドEDIDを有効にするには、サインアウトして新しいセッションを起動します。

視覚的にロスレスなエクスペリエンス

視覚的にロスレスなエクスペリエンスを実現するには、次のポリシーを有効にします。

- 視覚的にロスレス圧縮を許可する
- 視覚品質: 常にロスレスまたはロスレスに構築

ポリシーが設定された後、グラフィックスステータスインジケーターを使用して、イメージ品質スライダーを使用するか、ピクセルパーフェクトモードに切り替えることで、HDRセッションの品質を制御できます。

Windowsの画面ロックを許可する

このポリシーを使用すると、画面ロックを含むすべてのWindowsディスプレイタイムアウトを、ワークステーションOS上のCitrix Virtual Desktopセッションに適用できます。この設定は、Citrix StudioのCitrixグループポリシーオブジェクトを使用して設定できます。

デフォルトでは、この設定が有効になっていない場合、アクティブなセッション中にCitrix Virtual Desktopはセッションロック、スクリーンセーバー、またはディスプレイオフのタイムアウトに応答しません。

ワークステーションVDAでパスワード保護されたスクリーンセーバーが構成されている場合、スクリーンセーバーのタイムアウトに達したときにCitrix Virtual Desktopセッションが自動的にロックされるようにするには、この設定を有効にする必要があります。

VDAでディスプレイオフタイムアウトが構成されているときにこの設定を有効にすると、そのタイムアウトの期限切れにより、ユーザーがセッションとの対話を再開するまで更新されないセッションになります。たとえば、表示されている時間は更新されず、新しい通知も表示されません。

その他の考慮事項

- 仮想GPU上で最大4台のモニターで10ビットHDRセッションを起動できます。
- 次の場合、Citrixセッションは8ビットの非HDRモードに戻ります。
    - いずれかのエンドポイントモニターで10ビットHDRが有効になっていない場合
    - 画面共有を有効にする。

- VDAで仮想ディスプレイレイアウトを設定する。
- **視覚的にロスレス圧縮を許可**ポリシーを設定せずにピクセルパーフェクトモードに切り替える。

アダプティブ リフレッシュレート

アダプティブ リフレッシュレートを使用すると、HDX™ は仮想モニターのリフレッシュレートをターゲットFPSポリシー設定に合わせます。アダプティブ リフレッシュレートは、シングルセッションVDAとマルチセッションVDAの両方で、パフォーマンスとスケーラビリティを向上させます。

ターゲットフレームレート(/en-us/citrix-virtual-apps-desktops/current-release/media/targetframerate_60.png)

DirectX診断ツール(/en-us/citrix-virtual-apps-desktops/current-release/media/directx-diagnostic-tool.png)

> **注**
>
> アダプティブ リフレッシュレートは、Citrix Indirect DisplayまたはIDDが使用されている場合（Citrix Virtual Apps and Desktops™のデフォルトによる）にのみ利用可能であり、ベンダー提供のディスプレイアダプターを使用している場合は利用できません。

グラフィック用ロス許容モード

損失許容モードは、信頼性の低いネットワーク上で最高のパフォーマンスと対話性を確保します。

ネットワークの状態が、事前に定義された帯域幅、遅延、パケット損失のしきい値を超えて悪化すると、Citrix®グラフィックエンコーダーは自動的に、より積極的なパケット配信モードに切り替わり、パケット損失の影響を克服します。

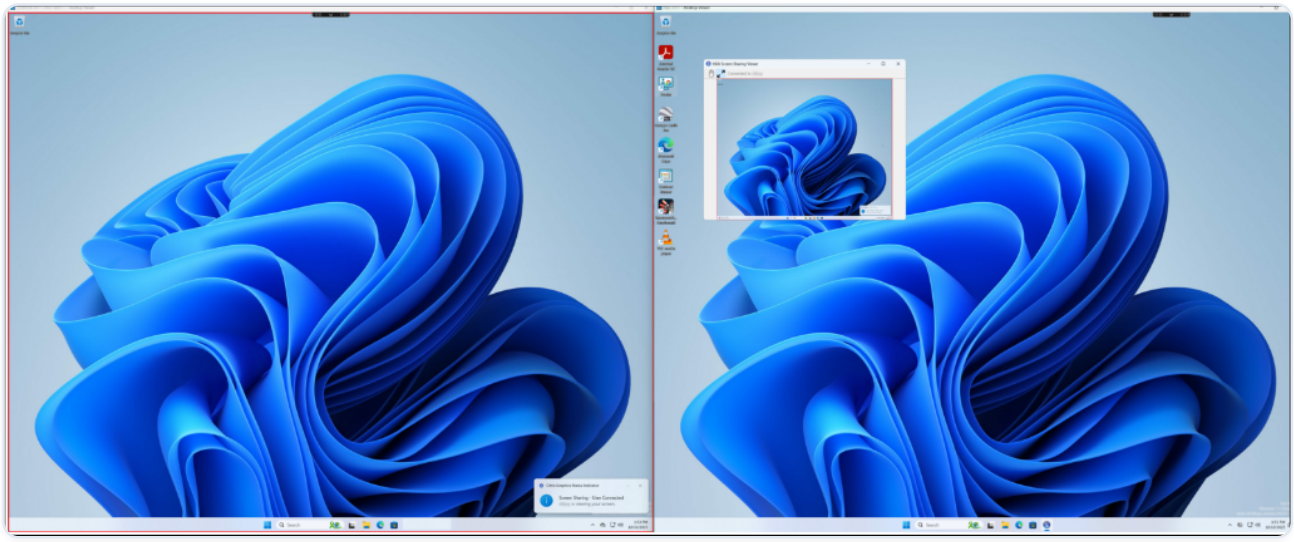
グラフィックの損失許容モードは、パケット損失が検出されたときにセッションが対話性を維持するように、徹底的に再設計されています。ネットワークの状態が、事前に定義された帯域幅、遅延、パケット損失のしきい値を超えて悪化すると、Citrixグラフィックエンコーダーは自動的に、より積極的なパケット配信モードに切り替わり、パケット損失の影響を克服します。その結果、帯域幅の使用量はパケット損失量に比例して増加します。その後、状態が改善すると、Citrixグラ

フィックエンコーダーはシームレスに元に戻ります。しきい値はポリシーを介して構成でき、デフォルトは300ミリ秒の遅延と5%のパケット損失です。

現在、Windows 2311 用のCitrix Workspace™アプリがサポートされています。他のプラットフォームのサポートは、今後のCitrix Workspaceアプリのリリースで追加される予定です。この機能の以前のバージョンと同様に、この機能が動作するにはHDX™ Adaptive Transport (EDT) を有効にする必要があります。さらに、Citrix Gateway Service を介して接続する場合、グラフィックの損失許容モードもGatewayで有効にする必要があります。

HDX画面共有

HDX画面共有は、Citrix Virtual Apps and Desktopsに組み込まれたネイティブな高性能機能であり、ユーザーが仮想セッション画面をリアルタイムで他のユーザーと共有できるようにします。低遅延と高品質を実現するように設計されており、サードパーティのソフトウェアソリューションを導入することなく、コラボレーション、サポート、トレーニングのシナリオでシームレスなエクスペリエンスを提供します。



HDX画面共有機能はHDXプロトコルに直接統合されており、セッションパフォーマンスへの影響を最小限に抑えながら、共有セッションのセキュリティと効率性を確保します。

HDX画面共有を使用すると、ユーザーはキーボードとマウスの制御を含むCitrixセッションのコンテンツ全体を、1人以上の参加者と共有できます。

この機能は高解像度ディスプレイをサポートし、最大8台のモニターに対応できます。

HDX画面共有は、Windows、Linux、macOSを含むすべてのVDAプラットフォームで利用でき、クロス互換性を提供します。これは、Windows VDAのユーザーがLinuxおよびmacOS VDAのユーザーと画面を共有できることを意味し、その逆も可能です。

さらに、HDX画面共有はクライアントコンポーネントに依存しないため、モバイルデバイスを含むすべてのクライアントプラットフォームでアクセス可能です。

主要な概念

- **共有者:** 仮想デスクトップセッションから画面共有を開始し、仮想セッションのデスクトップを他のユーザーに表示するユーザー
- **閲覧者:** 共有者のセッションに接続して画面を閲覧するユーザー（または複数のユーザー）。画面共有参加者とも呼ばれます。
- **接続コード:** 共有者が閲覧者に共有セッションへのアクセスを提供するために使用する、システム生成の一意のセキュリティコード。
- **グラフィックステータスインジケーター:** 通知領域に表示されるユーザーインターフェイス要素で、画面共有セッションの開始、停止、管理を制御します。
- **画面共有プレーヤー:** 閲覧者が共有者のセッションを閲覧するために使用するセッション内ツール。

ユースケースと使用例のシナリオ

HDX Screen Sharing を適切に構成し活用することで、IT サポートから共同開発、トレーニングまで、さまざまな組織のニーズに対応できます。

シナリオ 1: IT ヘルプデスクとリモートサポート

IT 管理者は、ユーザーが仮想デスクトップ内で経験している問題をトラブルシューティングする必要があります。問題を再現しようとする代わりに、IT 管理者は Citrix Director から HDX Screen sharing を介して Remote Assist を開始できます。 管理者はユーザーの正確な画面をリアルタイムで確認でき、問題の特定と解決が迅速になります。キーボードとマウスの制御を要求する機能により、管理者は直接操作を行うことができます。 HDX Screen sharing は、CVAD 2511 以降のバージョンから Citrix Director にも統合されています。Citrix Director を介した HDX Screen sharing の使用に関する詳細については、Citrix Director ドキュメント を参照してください。

シナリオ 2: エンドユーザーとの共同作業

エンジニアのチームは、仮想デスクトップ内のグラフィックを多用するアプリケーションで複雑な 3D モデルに取り組んでいます。彼らは一緒にデザインをレビューし、リアルタイムで調整を行う必要があります。

1 人のエンジニアがセッションを共有でき、チーム全体がモデルを表示し、変更を提案し、さらには交代でアプリケーションを制御して編集を行うことができます。これにより、ファイルの書き出しやサードパーティの画面共有ツールを使用する必要がなくなります。

シナリオ 3: 従業員のオンボーディングとトレーニング

新入社員が独自の基幹業務アプリケーションの使用方法を学んでいます。トレーナーは、新入社員の仮想セッション内でアプリケーションの機能を直接デモンストレーションできます。

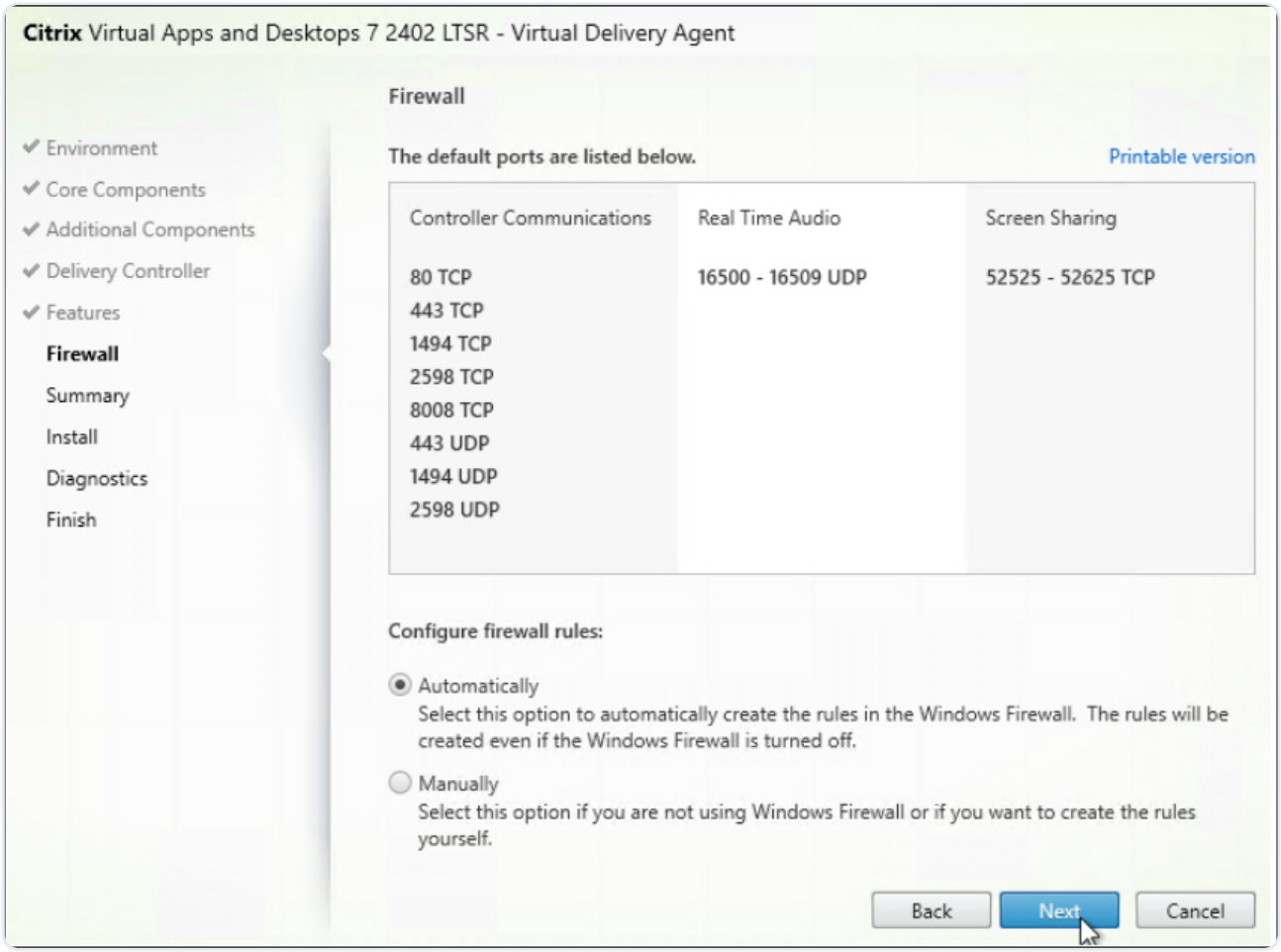
トレーナーは新入社員を段階的に指導できます。色付きの境界線インジケーター (赤または黄) は、セッションが共有されていることを明確に示し、学習環境の視覚的な合図となります。

システム要件

HDX Screen sharing はすべての VDA プラットフォームでサポートされていますが、特定のプラットフォームでは追加要件がある場合があります。詳細については、以下を参照してください。

HDX Screen sharing は、デフォルトで 52525 から 52625 の範囲の TCP ポートを使用します。

VDA バージョン 2112 以降をインストールする際、VDA インストーラーは HDX Screen sharing のデフォルトのファイアウォールポートを自動的に開くように構成できます。



VDA のインストール中にこれが実行されなかった場合、またはカスタムポート範囲が構成されている場合は、VDA 上でこれらのポートを手動で開いてください。

注:

セッションをホストする VDA と、共有セッションに接続するマシンとの間にネットワーク接続が必要です。

最大64人のビューアーが単一の画面共有セッションに接続できます。ポート範囲は、マルチセッション環境で画面共有を開始できるユーザーの最大数を制御します。ユーザーごとに1つのポートが必要です。

注:

セッションに接続されているすべてのモニターが共有されます。個々のモニターを選択することはできません。

AV1およびH.265ビデオコーデックと10ビットカラーモードはサポートされていません。アクティブな画面共有中は、セッションは自動的にH.264ビデオエンコーディングにフォールバックします。画面共有セッションが終了すると、AV1とH.265が再び利用可能になります。

ウィンドウズ ブイディーエー

- Windows: シングルセッションまたはマルチセッションOS VDA
- グラフィックステータスインジケーターを有効にする必要があります。

注:

デスクトップセッションのみ共有できます。

リナックス ブイディーエー

- 複数のLinux VDA間でセッション共有を行う場合、キーボード入力の問題を回避するために、同じVDAバージョンにアップグレードすることをお勧めします。
- Citrix Workspace™アプリをスキャンコードモードを使用するように構成することをお勧めします
- システムトレイアイコンを有効にする必要があります

Linux VDAのHDX画面共有に関する詳細については、HDX画面共有に関するLinux VDAドキュメントを参照してください。

macOS VDA

- Qt 5、リビジョン5.15.13以降。

HDX画面共有に関するすべてのVDAで統一されたユーザーエクスペリエンスを合わせるには、Qtフレームワークをインストールする必要があります。最小互換バージョンはQt 5（リビジョン5.15.13以降）です。

VDA への Qt 5 のインストールは、たとえば homebrew を使用して、次の コマンドを実行することで実行できます。

```
brew install qt@5
```

MacOS VDA 向けの HDX 画面共有に関する詳細については、HDX 画面共有に関する MacOS VDA ドキュメントを参照してください。

構成

HDX 画面共有はデフォルトで無効になっており、この機能は Citrix® ポリシーを通じて有効化および構成できます。

これらのポリシーにより、HDX 画面共有の構成をきめ細かく制御できます。

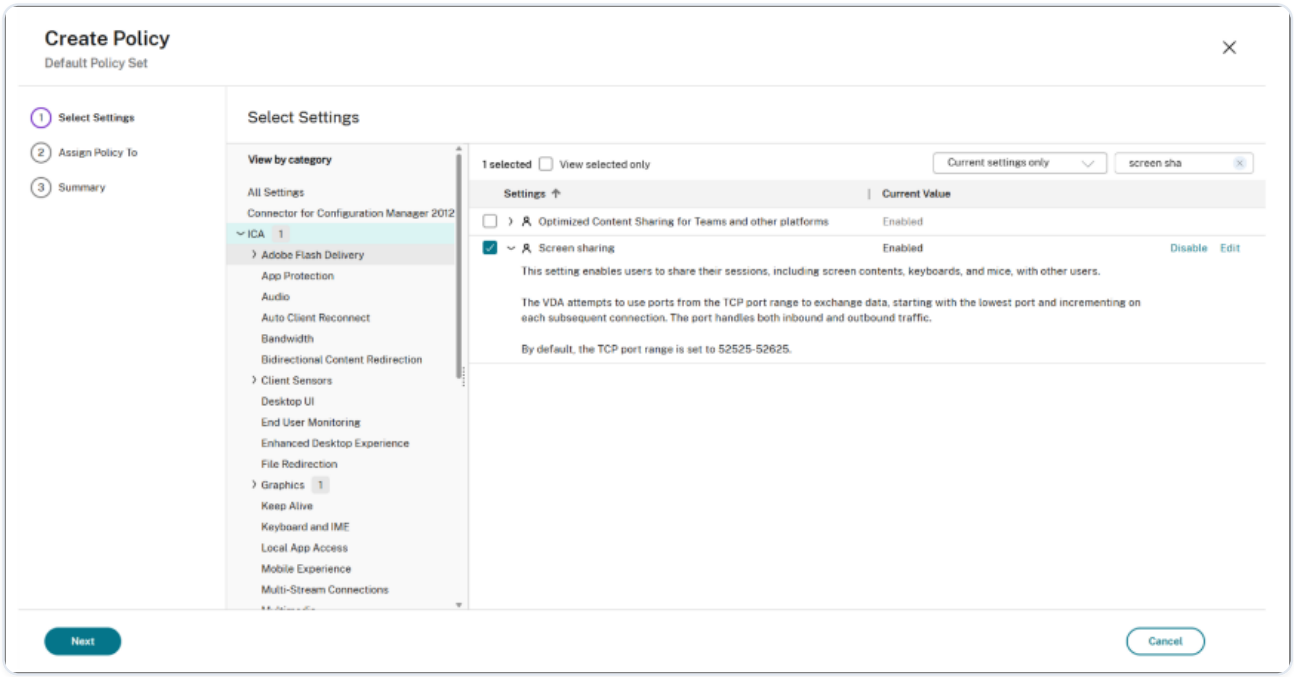
エンドユーザー向け HDX 画面共有の有効化

HDX 画面共有はデフォルトで無効になっています。エンドユーザーが HDX 画面共有を介して画面を共有できるようにするには、機能を次のように有効化および構成する必要があります。

- HDX 画面共有ポリシーを有効にする
- グラフィックステータスインジケーターを有効にする
- **オプション:** VDA ファイアウォールでカスタムポートを構成して開く

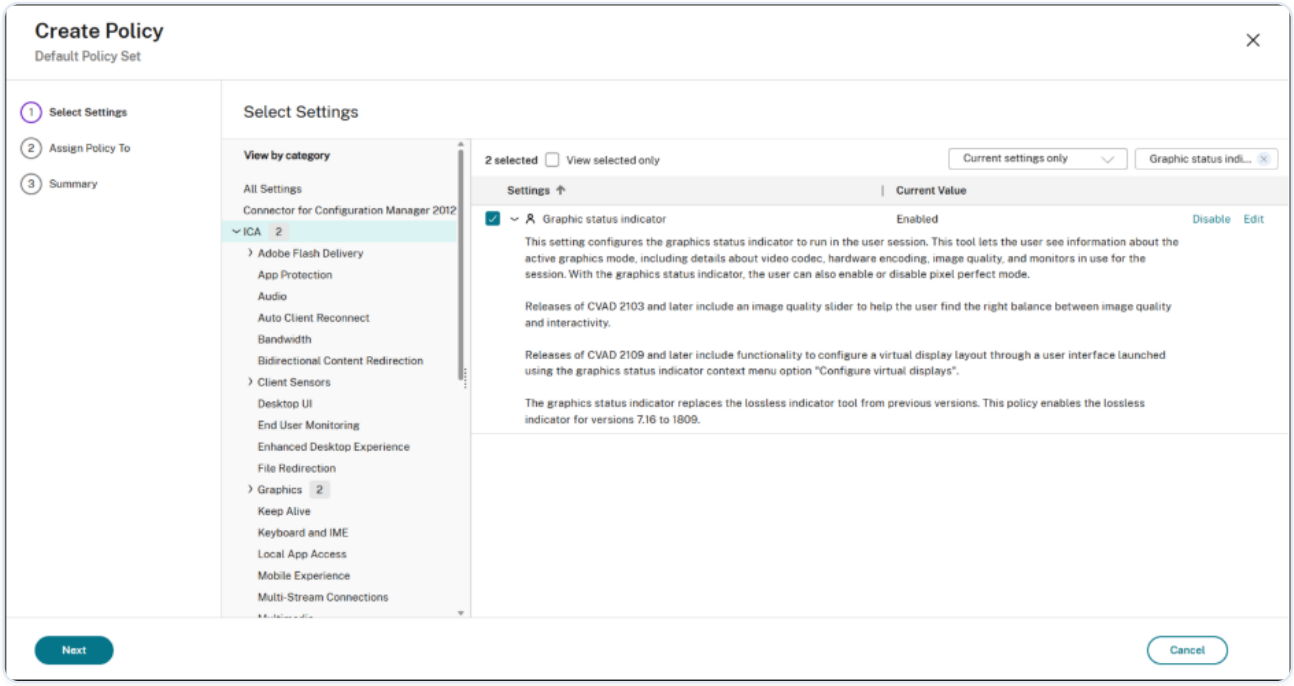
ステップ 1: HDX 画面共有を有効にする

HDX 画面共有を有効にするには、**画面共有**ポリシーに移動し、ポリシーを**有効**に設定します。



ステップ 2: グラフィックステータスインジケーターを有効にする

グラフィックステータスインジケーターに移動し、ポリシーを**有効**に設定します。



追加のHDX画面共有構成

デフォルトでは、HDX画面共有は通信に以下のTCPポートを使用します。

- TCP開始ポート: 52525
- TCP終了ポート: 52625

デフォルトのTCPポート範囲は、「HDX画面共有ポート」ポリシーで調整できます。

TCPポート範囲を調整するには、「HDX画面共有ポート」ポリシーを参照し、ポート範囲を希望のポート範囲に設定します。

ポート構成は、マルチセッションVDAで画面を共有する同時ユーザーの数を制限するために使用できます。

> **注:**
>
> ポート構成は、DirectorのHDX画面共有と重複しないようにしてください。

> HDX画面共有接続コードは、デフォルトでは期限切れにならず、画面共有セッション中にそのセッションに参加するために無期限に使用できます。

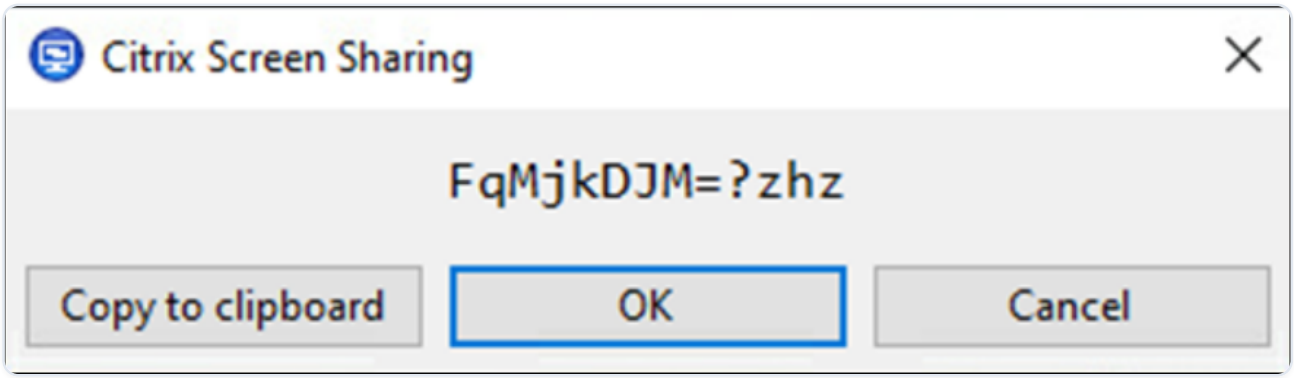
セキュリティを強化するために、接続コードが期限切れになるタイムアウト設定を構成できます。指定されたタイムアウト期間が経過すると、以前に生成された接続コードは無効になり、新しいユーザーはこのコードを使用して画面共有セッションに参加できなくなります。共有者は新しいセッション接続コードを再生成する必要があります。

さらに、画面共有セッションが開始され、構成されたタイムアウト期間内にビューアーが接続しなかった場合、画面共有は自動的に停止します。画面共有を再開するには、共有者はHDX画面共有を再起動し、接続コードを共有する必要があります。

HDX画面共有セッションのタイムアウトを構成するには、「HDX画面共有タイムアウト」ポリシーを参照し、希望のタイムアウト値を分単位で設定します。

接続コードの構成 (プレビュー)

デフォルトでは、HDX画面共有は40文字の接続コードを使用します。CVAD 2411以降、管理者はHDX画面共有用の新しい短い接続コードの使用を構成できます。新しい接続コードは13文字と短く、共有者が接続コードを潜在的なビューアーに口頭で伝えやすくするために、曖昧な文字は含まれていません。



現在、設定はVDAのレジストリ設定として提供されています。新しい、より短い接続コードは、古いVDAとの下位互換性を 提供しないことに注意してください。

> **注:**
>
> 新しい短い接続コードは、古いVDAとの下位互換性を提供しません。

前提条件

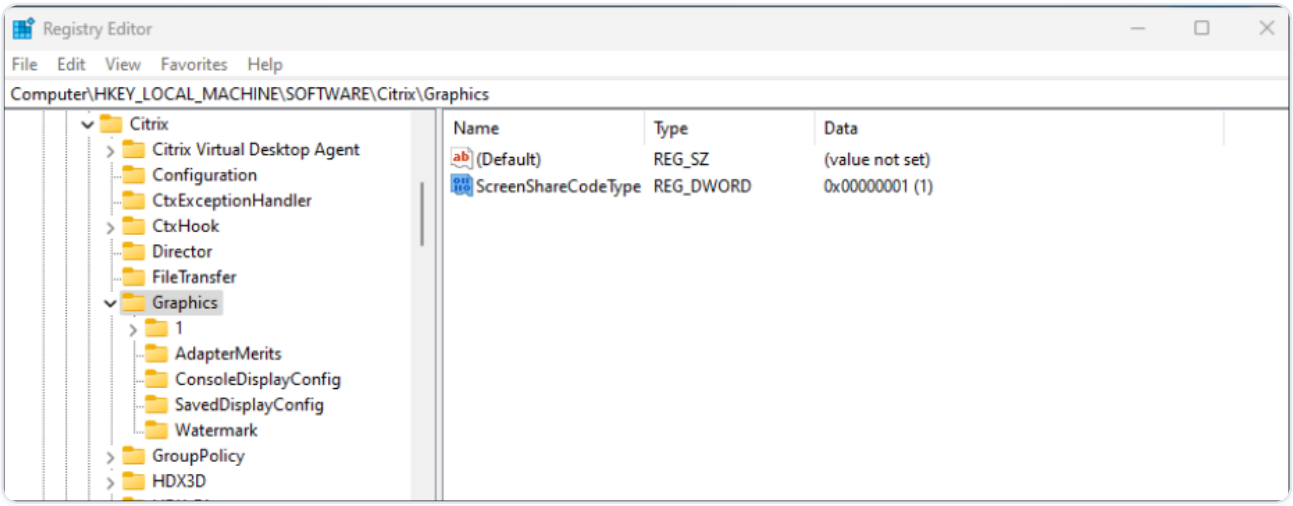
VDA - CVAD 2411以降

接続設定

新しい短い接続コードを有効にするには：

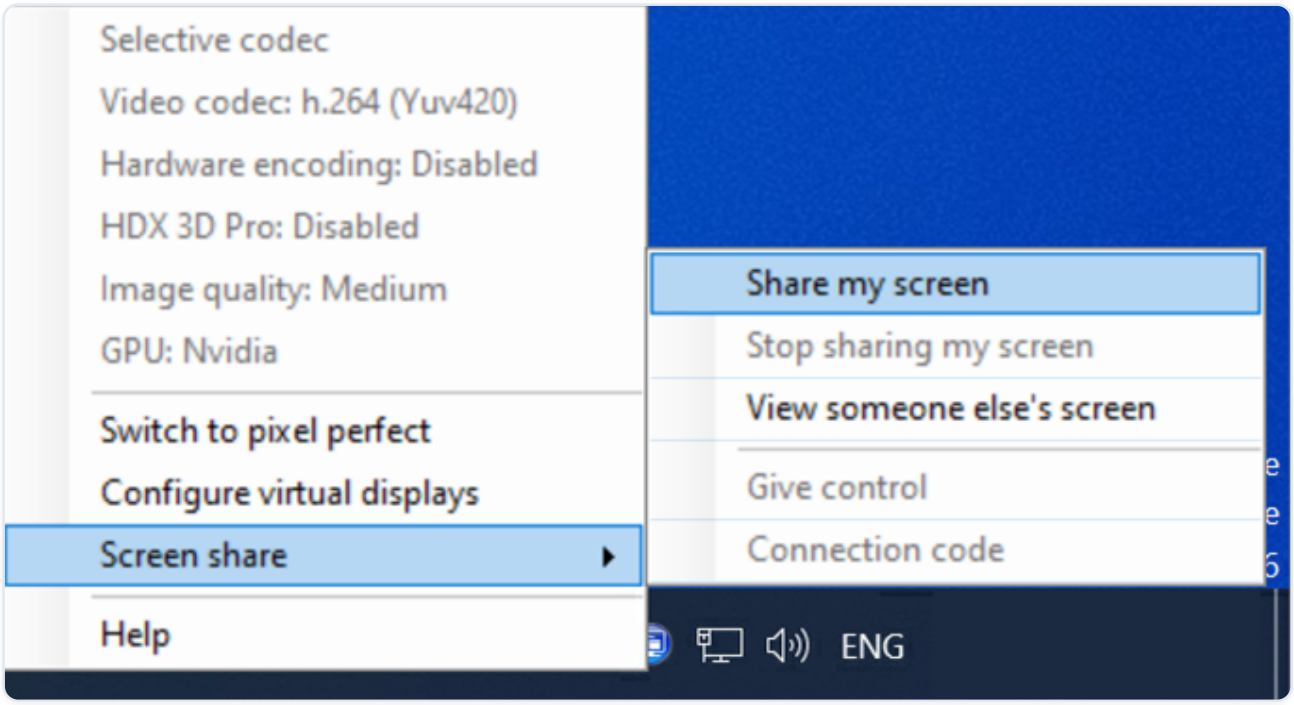
1. regedit.exe を使用して Windows レジストリエディターを開きます。
2. `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\ScreenShare` に移動します。
3. **CodeType**という名前の**DWORD**値を作成し、値を1に設定します。

このキーは使用する接続コードを制御します。0は古い長い接続コード用、1は新しい短いコード用です。



画面共有セッションの開始

共有者としてセッションを共有するには、Windowsの通知領域にあるHDXグラフィックステータスインジケーターアイコンを探します。それを右クリックしてメニューを表示し、「画面共有」>「自分の画面を共有」を選択します。



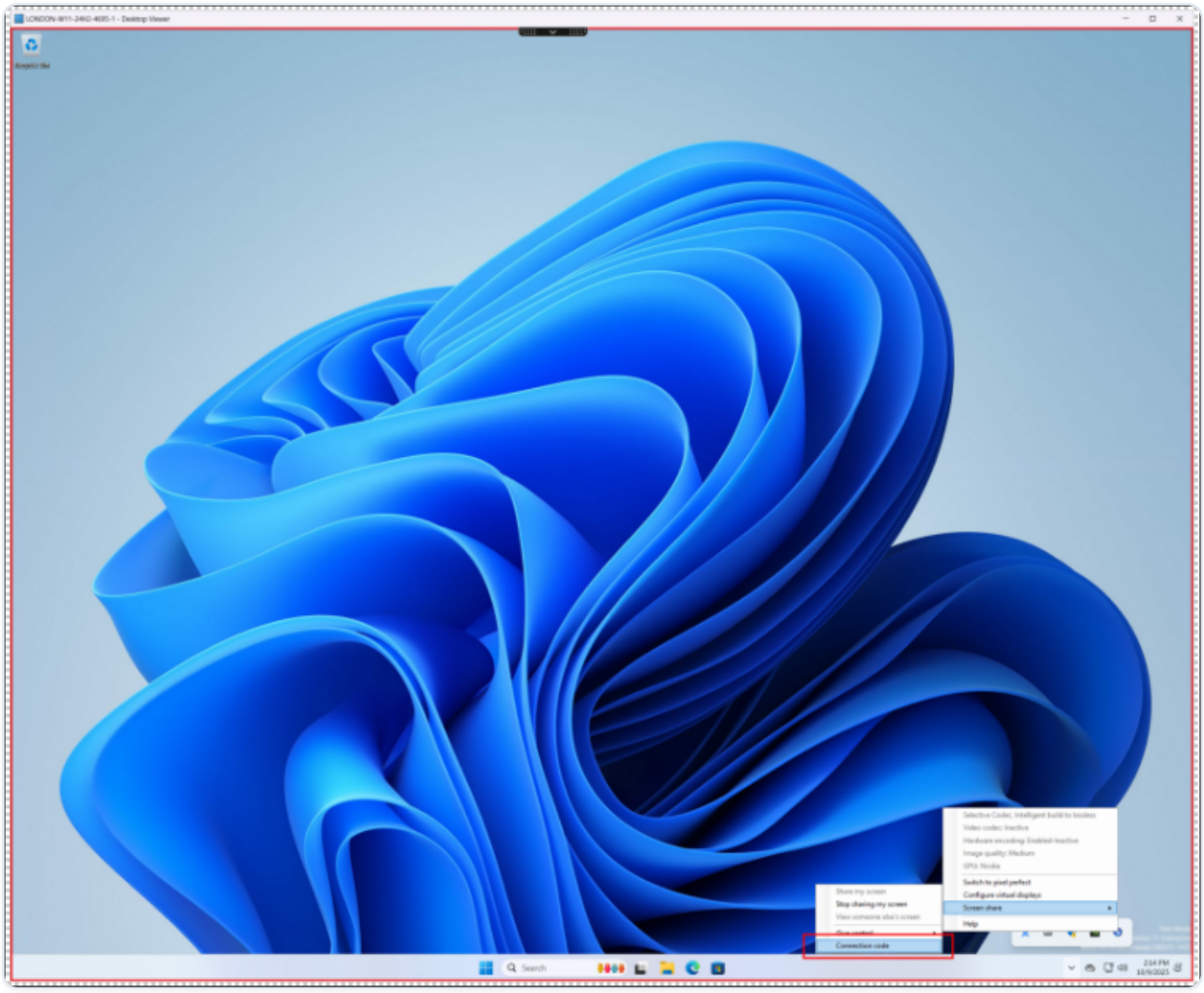
画面共有が開始されると、画面共有セッションに参加するために使用できる接続コードを含むダイアログボックスが表示されます。このコードは、1人以上の視聴者が画面共有セッションに接続するために使用できます。

「クリップボードにコピー」をクリックするか、ダイアログボックスに表示されている接続コードを手動で選択してコピーします。

接続コードは、他のユーザーに配布するために、メールアプリケーションやMicrosoft Teamsなど、選択したアプリケーションに貼り付けることができます。

接続コードがコピーされたら、「OK」をクリックするか、右上隅の「x」をクリックしてダイアログボックスを閉じることができます。

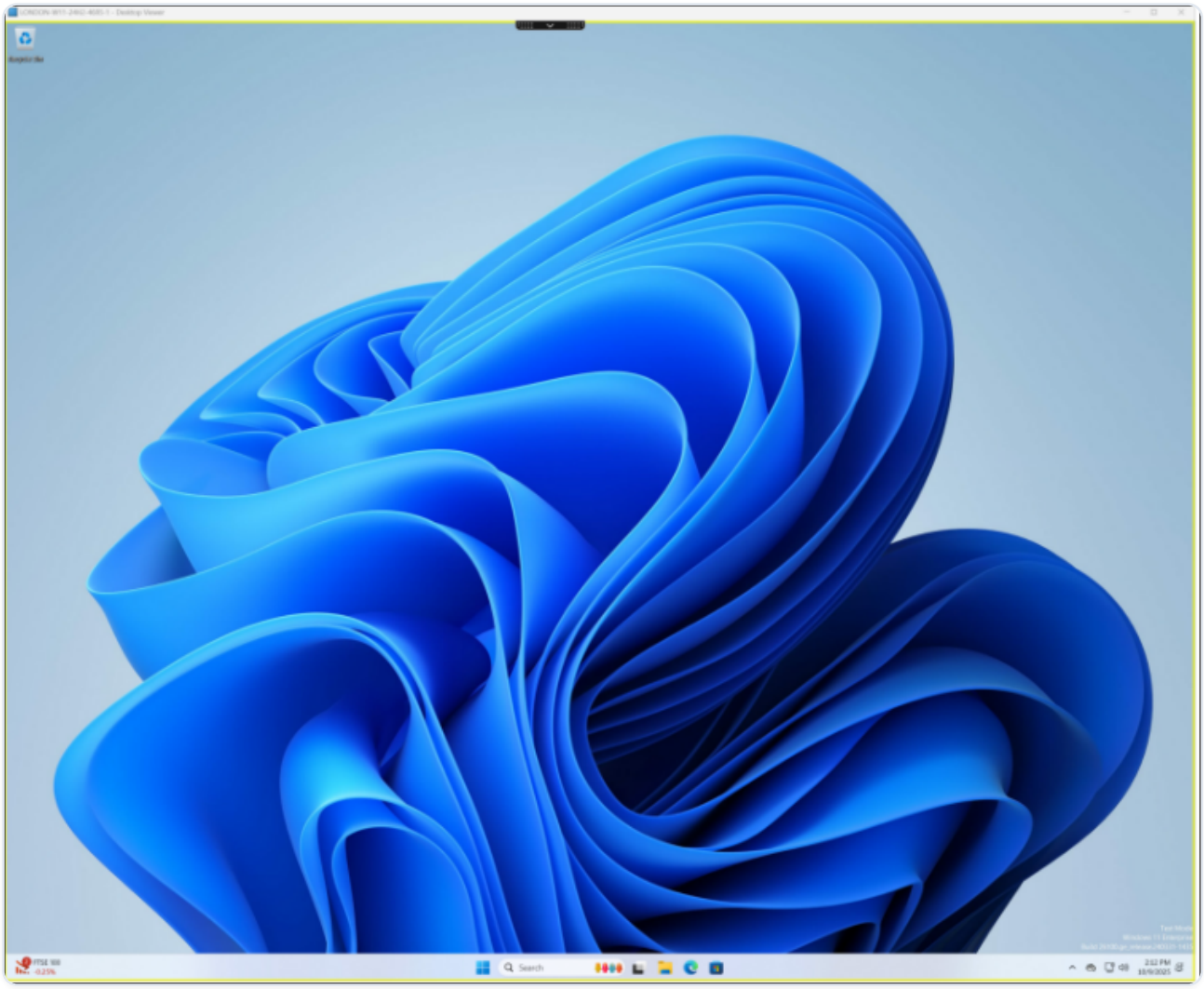
セッションが共有されている間はいつでも、「画面共有」>「接続コード」メニューオプションから現在アクティブな接続コードを取得できます。



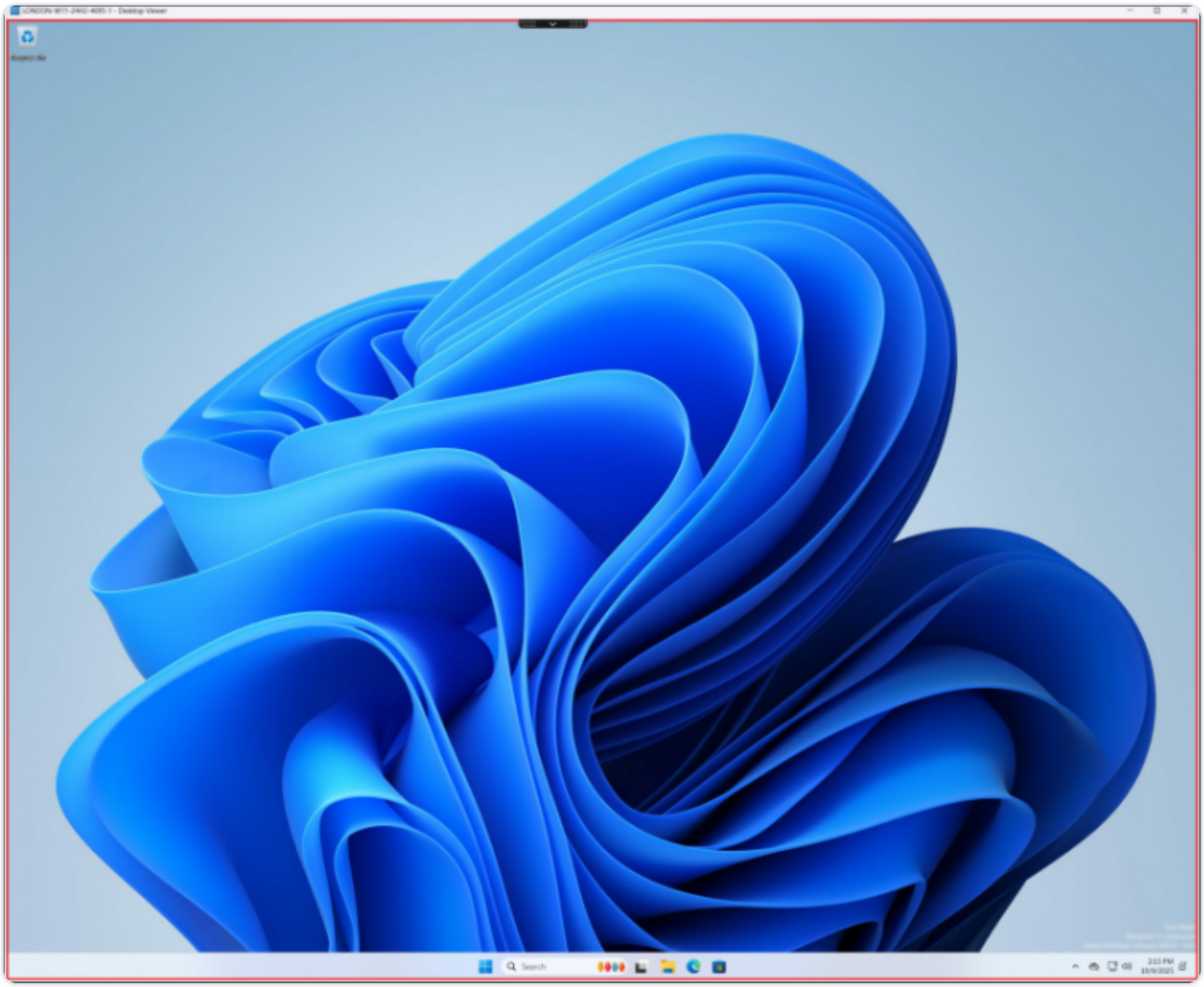
注:

接続コードを共有する相手には注意してください。接続コードを共有したすべてのユーザーは、アクティブな画面共有セッションに接続できる可能性があります。

画面共有セッションが開始されると、Citrixセッションの周囲に黄色の枠が表示され、HDX画面共有がアクティブであるが、まだ視聴者が参加していないことを示します。



視聴者が画面共有セッションに接続すると、枠の色が赤に変わり、画面共有セッションがアクティブで視聴者が接続されていることを示します。



Citrixセッションで複数の画面がアクティブになっている場合、すべての画面が画面共有を介して共有され、視聴者はセッション内の接続されているすべての画面を見ることができることに注意してください。

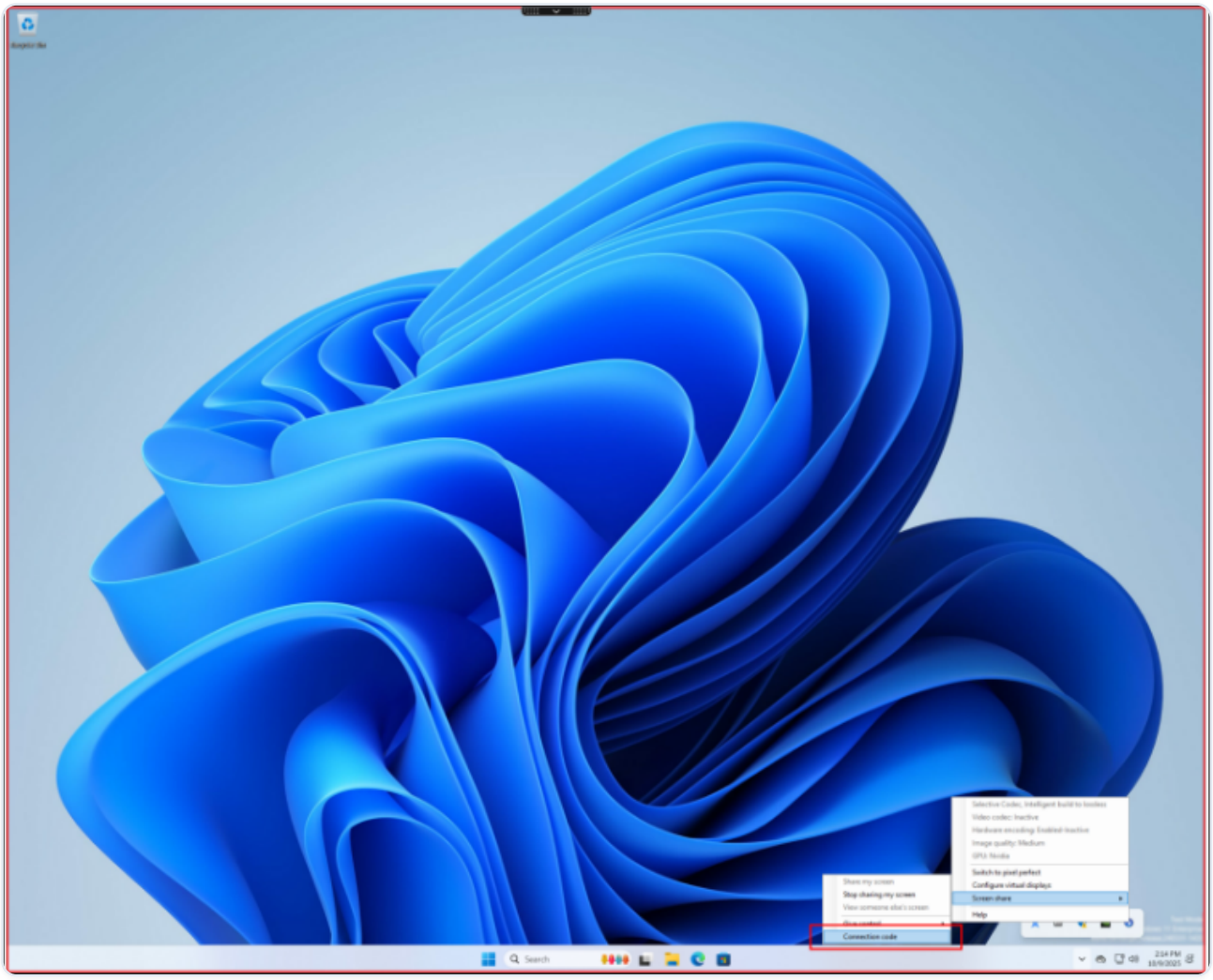
現在、セッション内で単一のモニターまたは接続されているモニターのサブセットのみを共有するサポートはありません。

デフォルトでは、最大100人の視聴者が単一の画面共有セッションに接続できますが、この制限はCitrix管理者が制限する場合があります。

新しい接続コードを再生成する

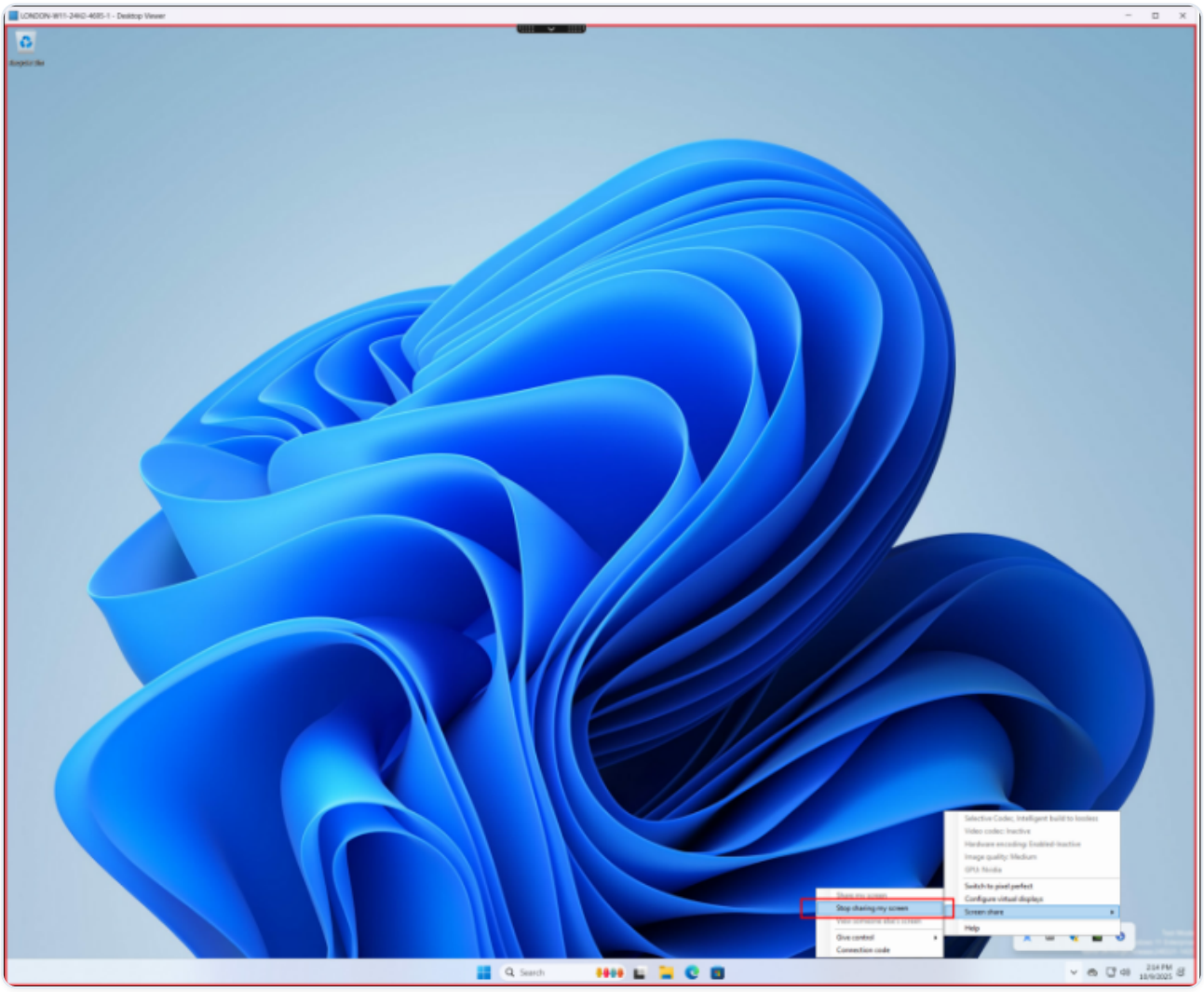
接続コードがアクティブである限り、新しいユーザーは接続コードを使用して画面共有セッションに参加できます。コードの有効期限が切れた場合、既存の視聴者は接続されたままになりますが、新しいユーザーは画面共有セッションに接続できなくなります。新しいユーザーがセッションに接続できるようにするには、新しい接続コードを再生成する必要があります。

セッションが共有されている間はいつでも、「画面共有」>「接続コード」メニューオプションから新しい接続コードを取得できます。



画面共有の停止

画面共有を停止するには、Windows の通知領域にある HDX グラフィックステータスインジケーターアイコンを探します。それを右クリックしてメニューを表示し、「画面共有」>「画面の共有を停止」を選択します。画面共有はすぐに停止され、現在のすべてのビューアーはセッションから切断されます。画面共有が停止したことを示す赤い枠線は消えます。

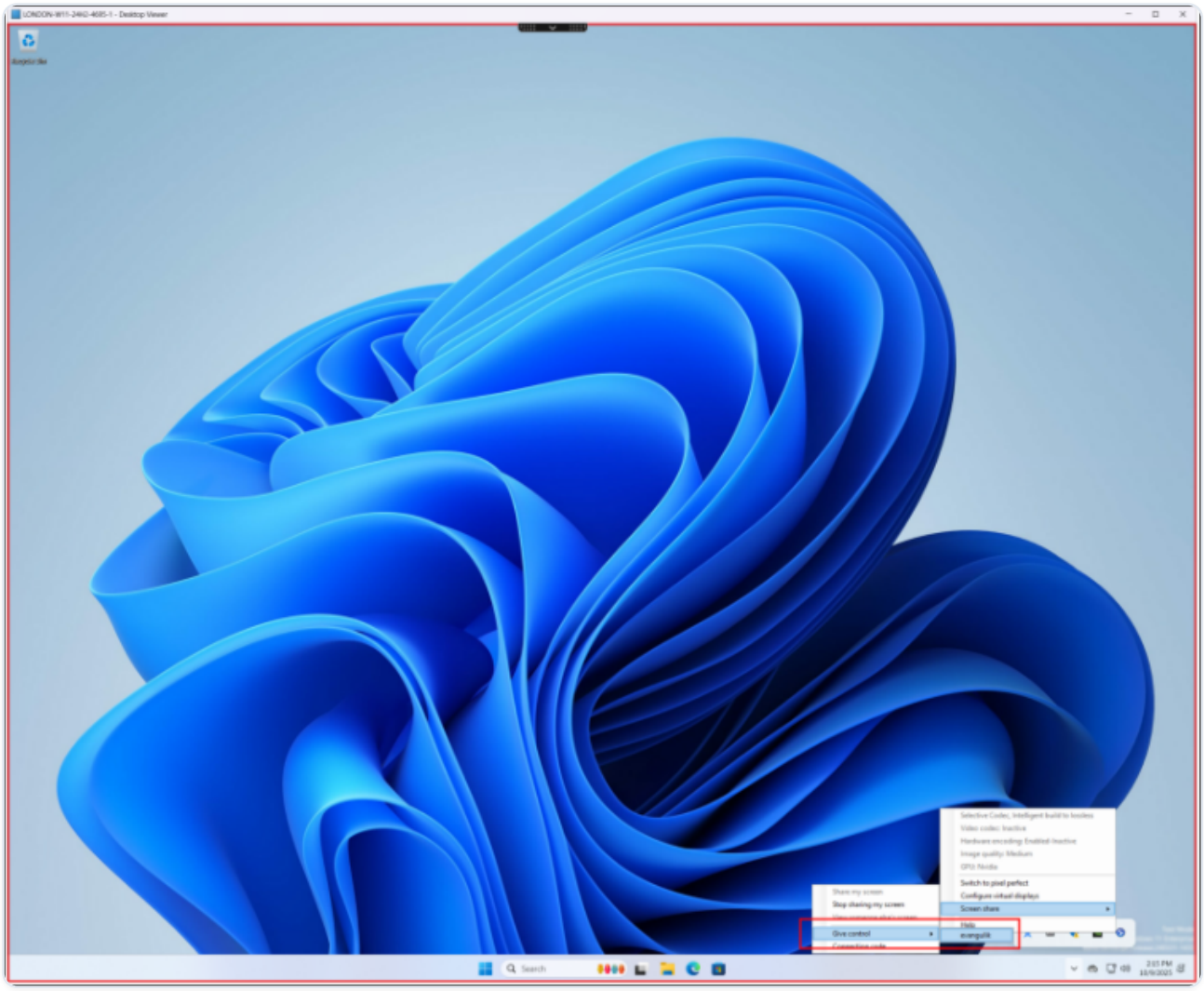


マウスとキーボードの制御を付与する

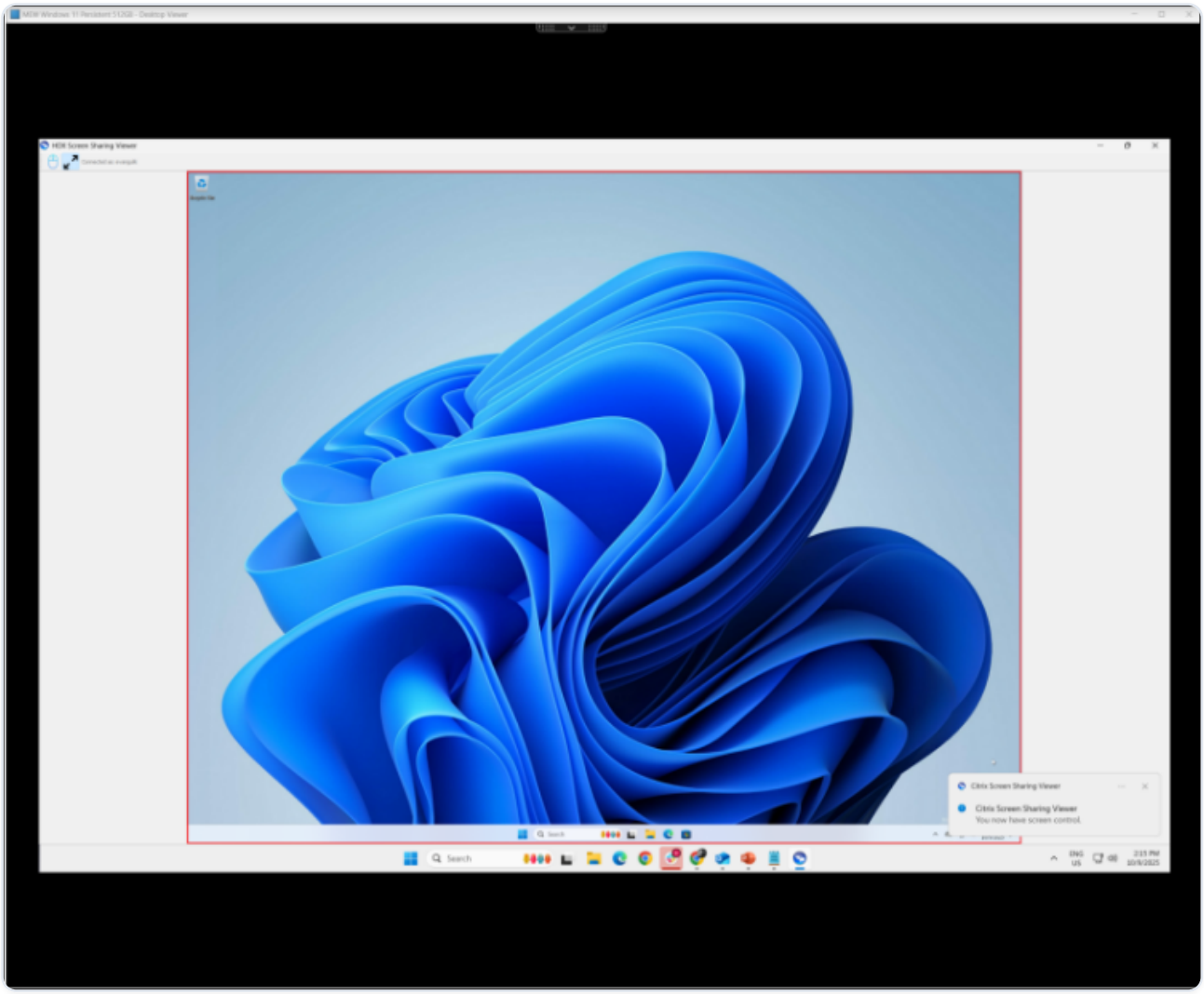
画面共有セッション中の任意の時点で、共有者として、マウスとキーボードの制御を特定のビューアーに引き渡すことができます。

引き渡されると、そのビューアーは Citrix セッションであなたのマウスとキーボードの完全な制御をあなたと共有します。

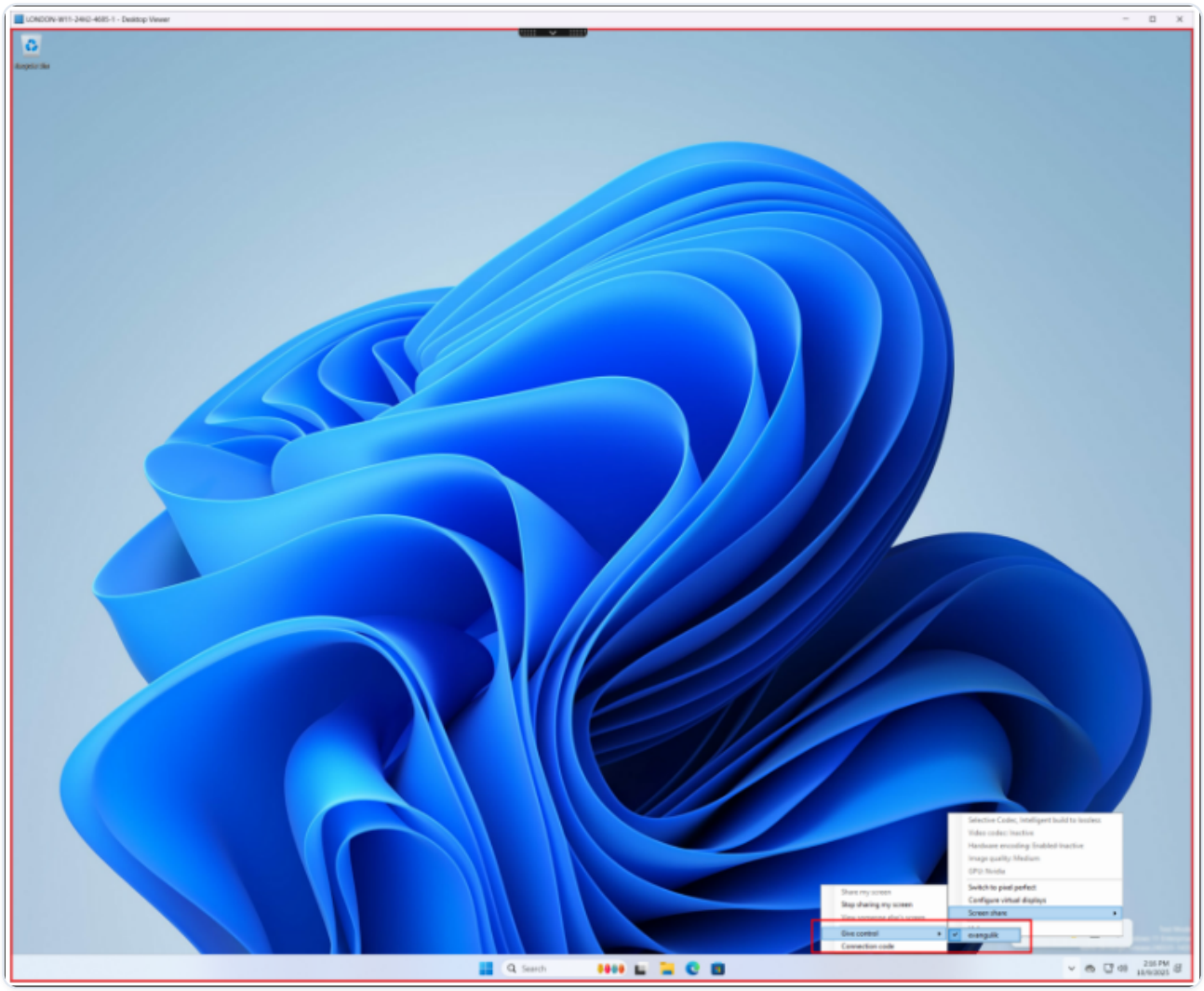
マウスとキーボードの制御を共有するには、Windows の通知領域にあるグラフィックステータスインジケーターアイコンを開きます。それを右クリックしてメニューを表示し、「画面共有」>「制御を付与」を選択し、制御を引き渡すアクティブなビューアーのいずれかを選択します。



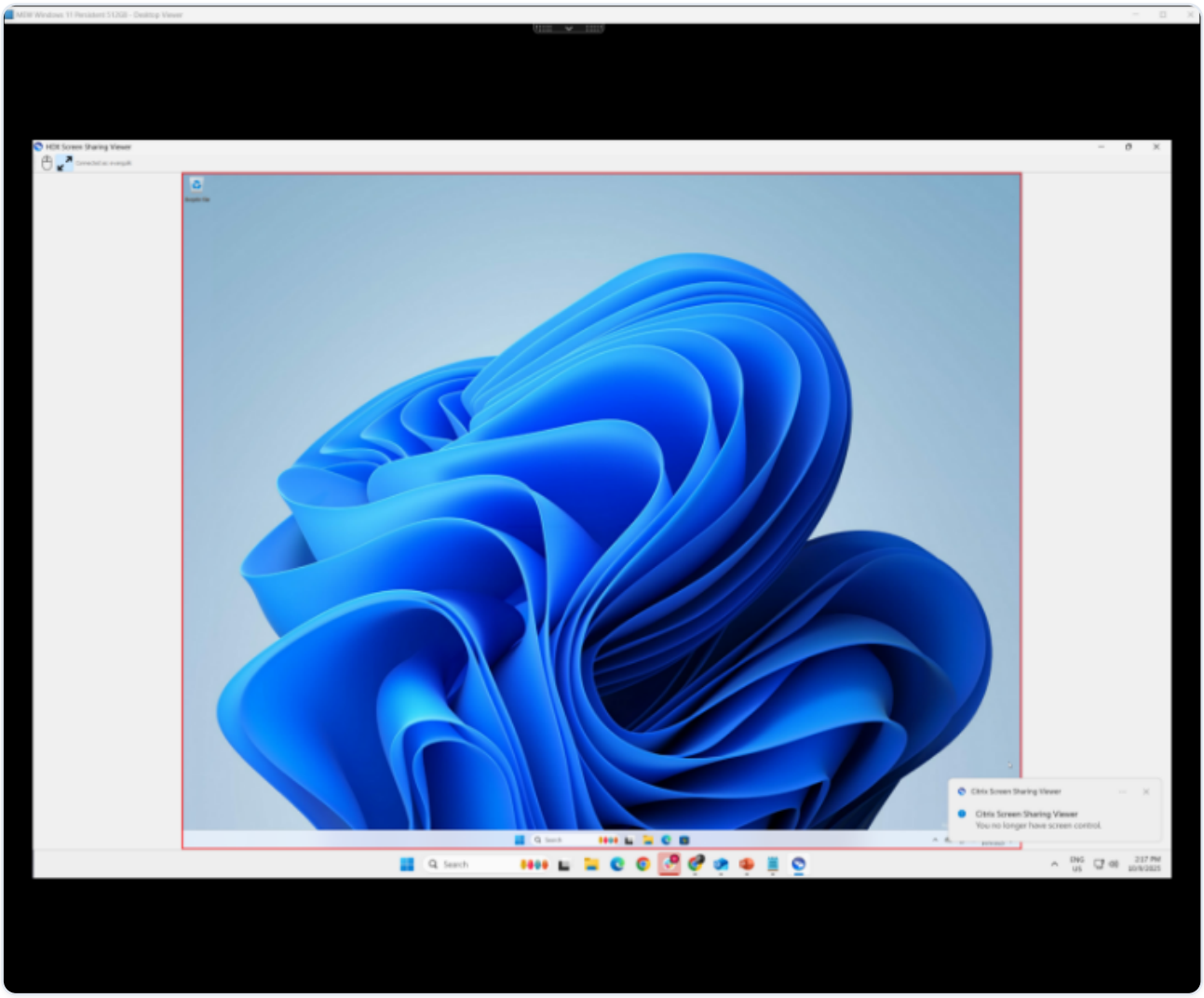
選択されたビューアーには、マウスとキーボードの制御権があることを示す通知が届きます。



マウスとキーボードの共有を停止し、制御を取り戻すには、Windows の通知領域にあるグラフィックステータスインジケーターアイコンを開きます。それを右クリックしてメニューを表示し、「画面共有」>「制御を付与」を選択し、アクティブなビューアーの選択を解除します。

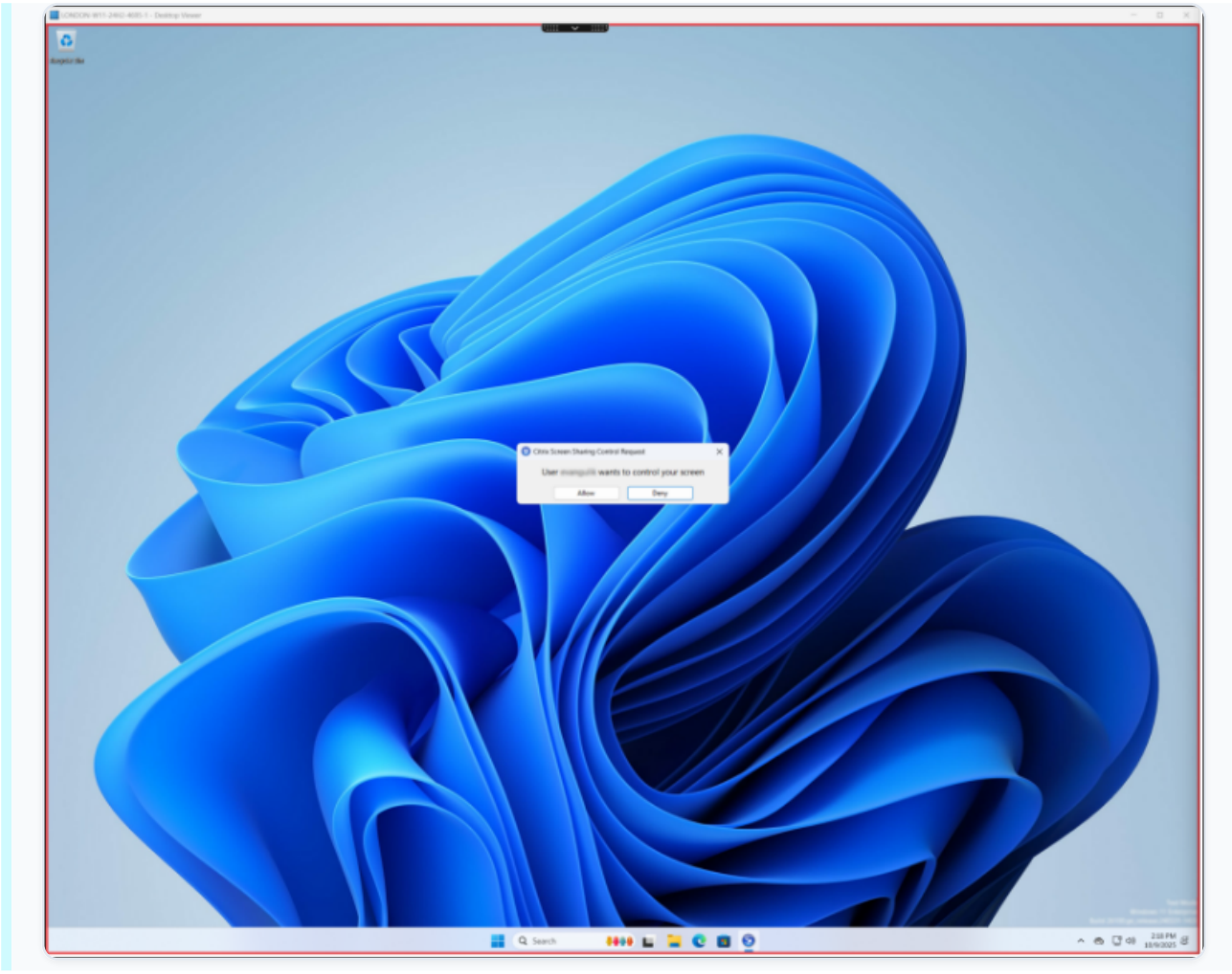


ビューアーには、マウスとキーボードの制御を失ったことが通知されます。



注:

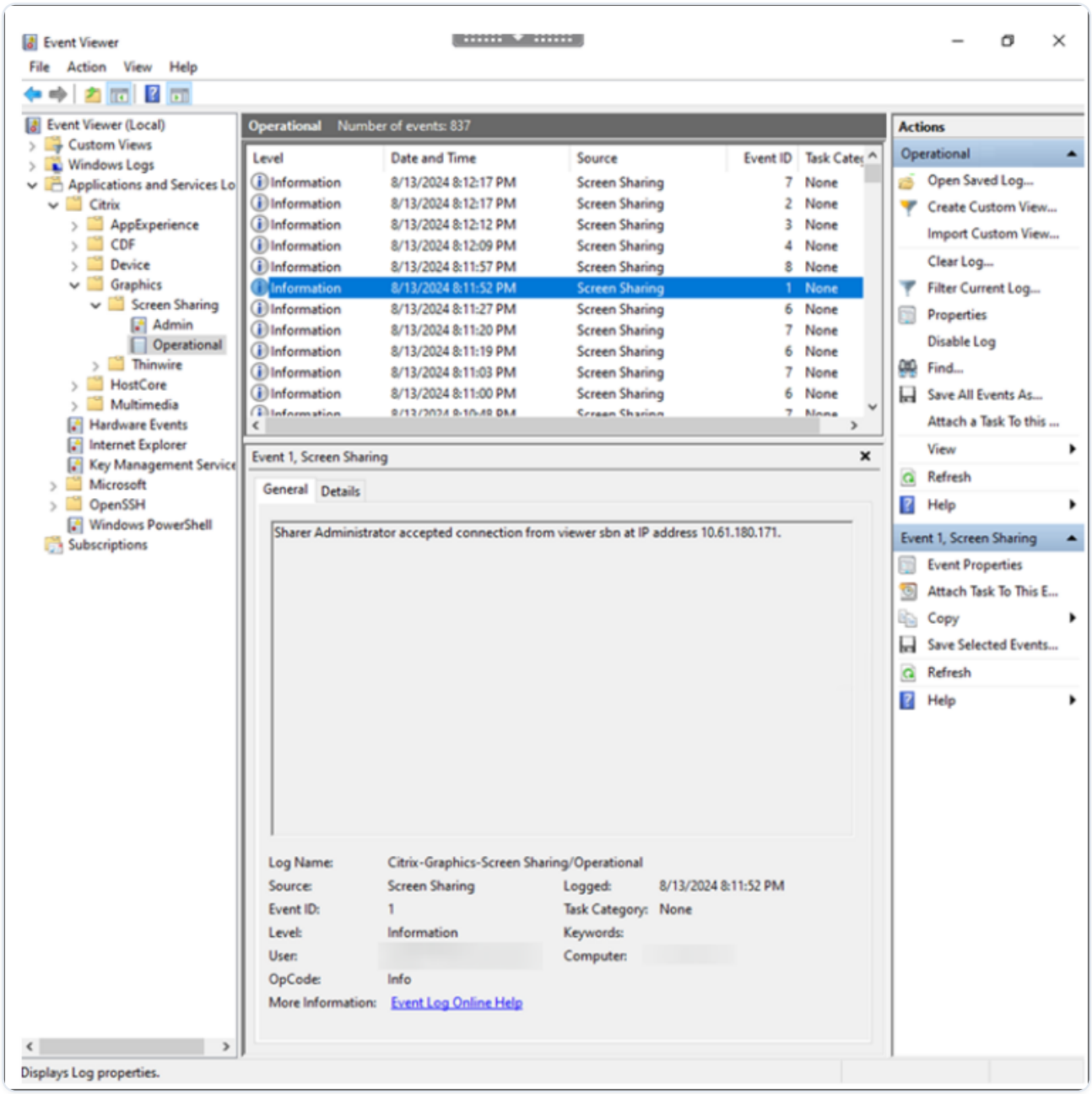
マウスとキーボードの制御は、一度に1人のビューアーとのみ共有できます。ビューアーは、マウスとキーボードの制御を要求することもできます。この場合、要求が通知され、その要求を許可するか拒否するかを選択できます。



イベントログ

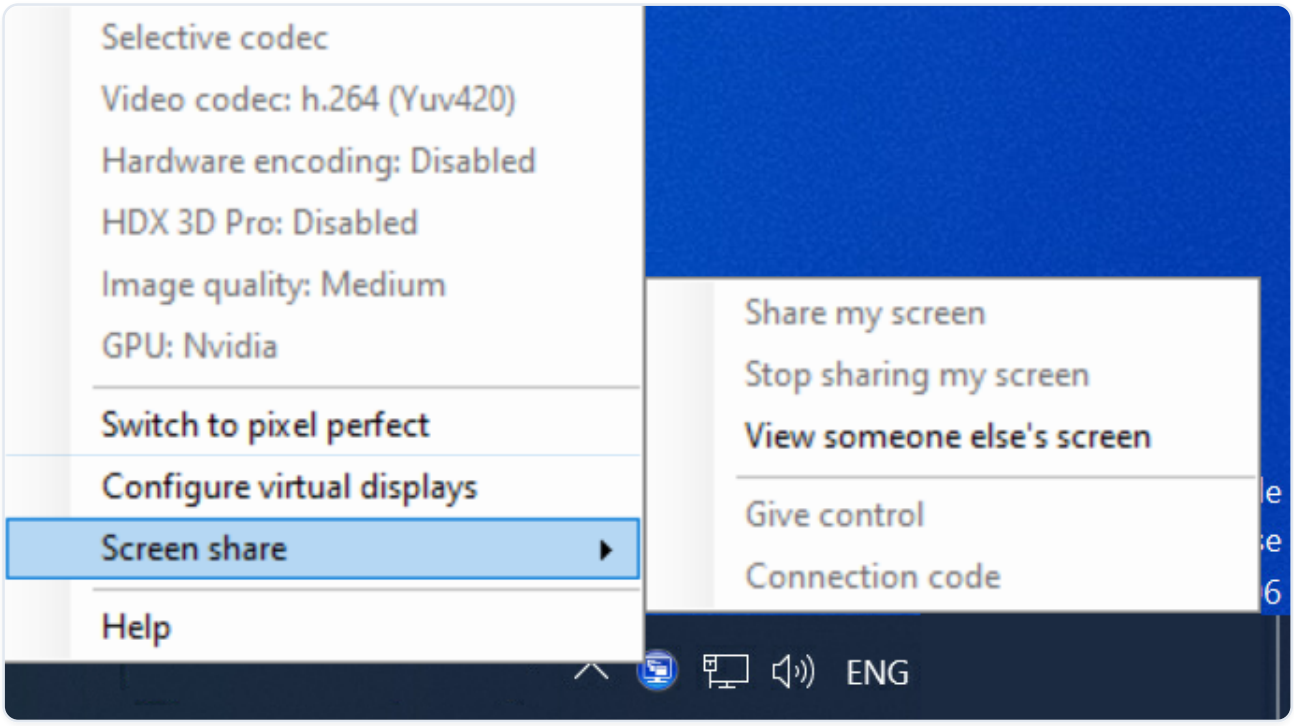
セキュリティおよび監査の目的で、共有者VDAでの画面共有イベントが収集され、ログに記録されるようになりました。これにより、管理者は共有者VDAでの画面共有アクティビティを追跡できるようになります。画面共有中に、次の情報とイベントがログに記録されます。 セッション:

- 共有の開始/停止 – 画面共有セッションの開始と停止を示すイベント
- 接続要求 – 接続を要求したビューアーのIPとユーザー名、使用された接続コード、および接続決定（認証失敗または共有者の決定による接続許可/拒否）
- 画面制御要求 – 画面制御を要求したビューアーのIPとユーザー名、および決定（許可/拒否）
- ビューアーのアクション - 画面共有セッションから切断した、または共有者の画面の制御を解除したビューアーのIPとユーザー名。



画面共有セッションの表示

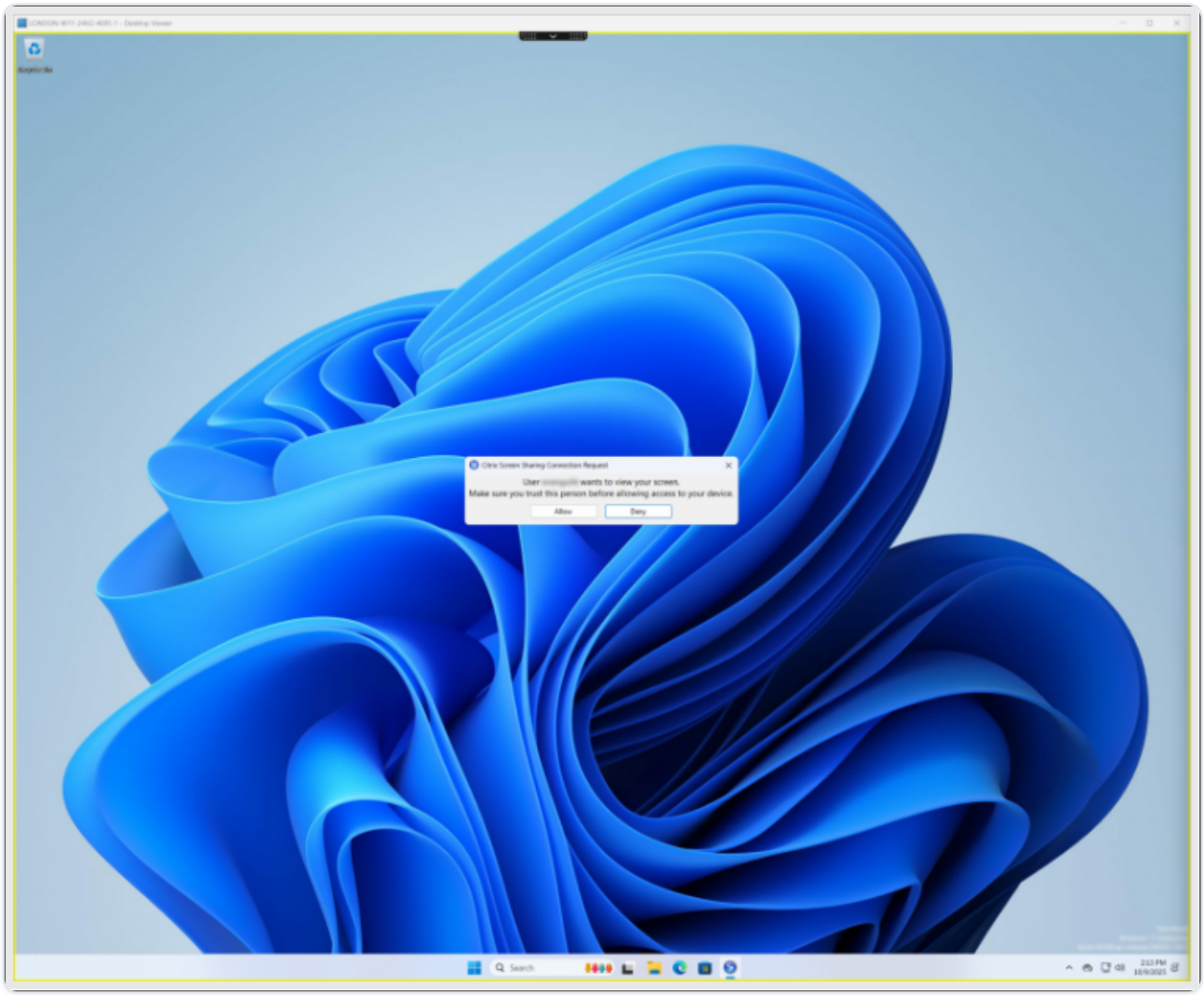
他のユーザーのセッションに接続するには、Windows通知領域にあるHDXグラフィックステータスインジケーターアイコンを探します。右クリックしてメニューを表示し、「画面共有」>「他のユーザーの画面を表示」を選択します。



接続コードの入力を求められます。HDX画面共有者がこのコードを提供します。セッションを共有しているユーザーから提供されたセッションの接続文字列をテキストボックスに入力または貼り付けます。

「接続」をクリックすると、接続コードが検証され、検証が成功すると、共有者のセッションへの画面共有接続が確立され、画面共有ビューアーが自動的に開き、共有者の画面（または複数の画面）が表示されます。

セッションに接続すると、共有者はあなたの画面共有セッションへの参加を通知されます。



ディスプレイのスケーリングを調整する

共有者が自分のモニター解像度よりも高い解像度を使用している場合、またはセッション中に複数のモニターを使用している場合、画面共有プレーヤーは自動的に解像度を調整します。スケーリングを無効にして共有者のモニターのネイティブ解像度を表示するには、画面共有プレーヤーの左上隅にある対角線矢印を選択します。

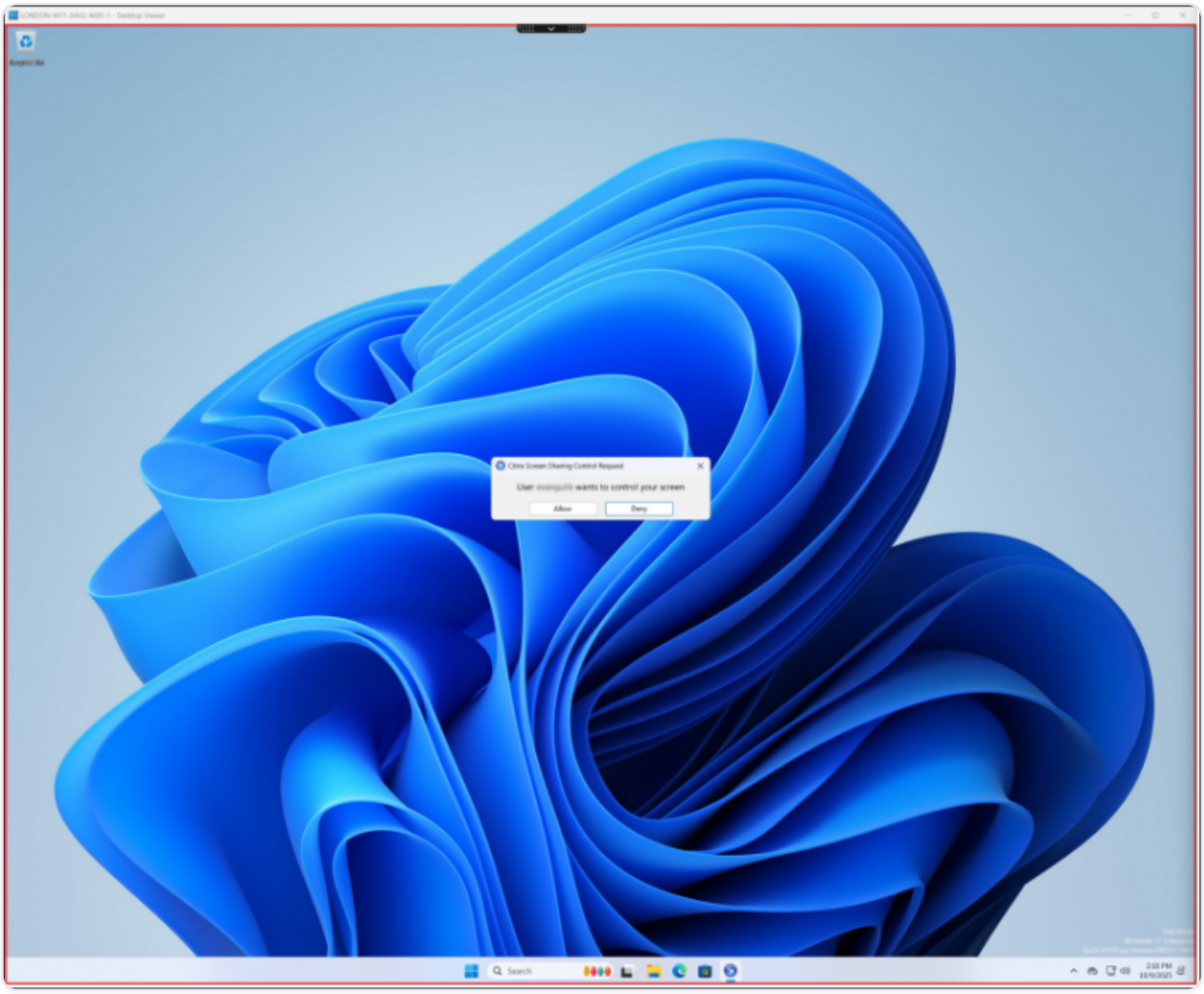
画面共有セッションから切断する

画面共有セッションから切断するには、いつでも画面共有プレーヤーを閉じます。再接続するには、接続コードが期限切れになっていない場合、同じコードを使用して共有者との画面共有セッションに再参加できます。接続コードが期限切れになっている場合、共有者は新しいコードを再生成する必要があります。接続コードの有効期限は、管理者が設定できる接続タイムアウト画面共有ポリシーによって制御されます。

マウスとキーボードの制御を要求する

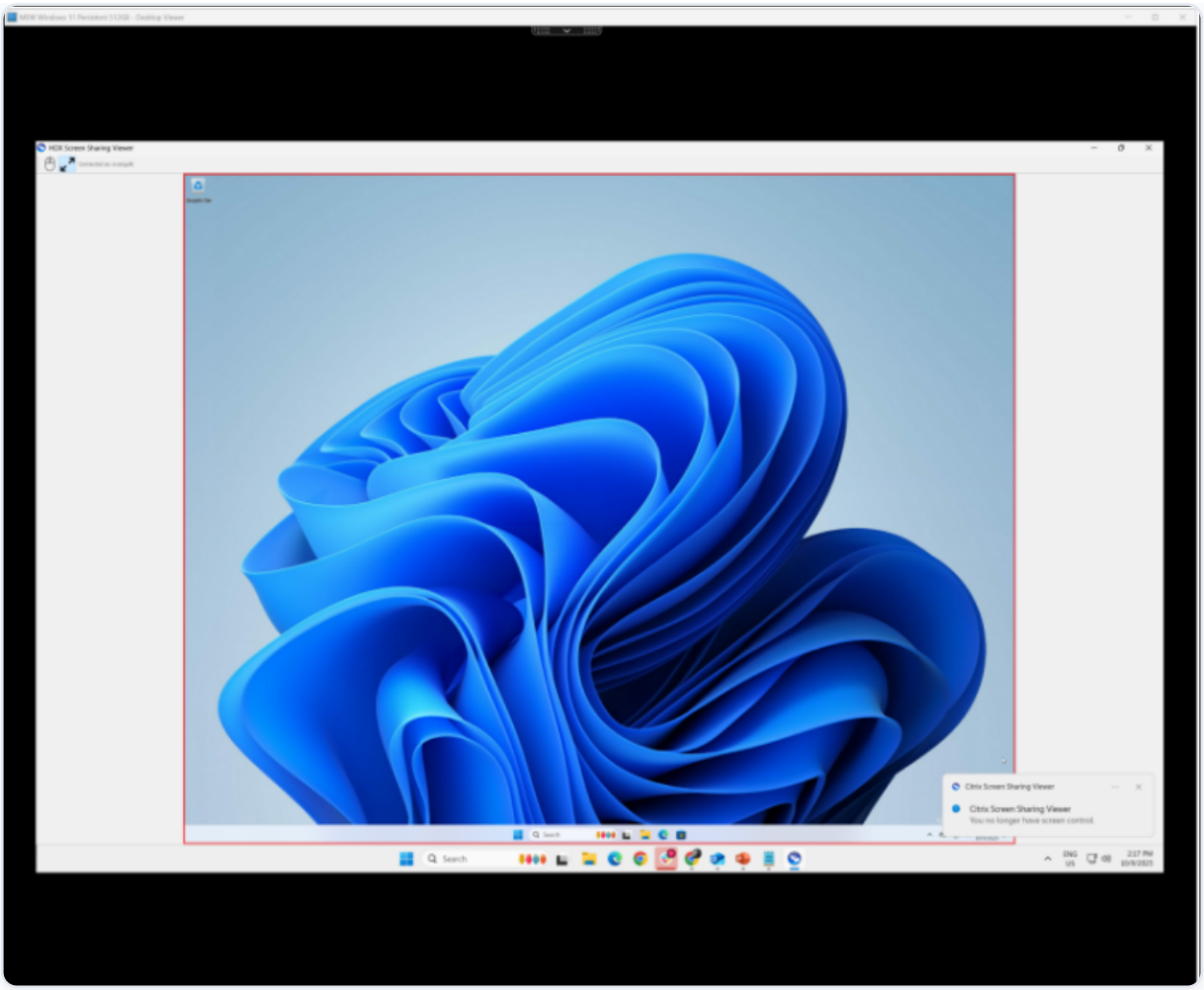
デフォルトでは、画面共有セッションにおけるマウスとキーボードの制御は共有者が完全に保持しています。視聴者として、共有者にマウスとキーボードの制御を要求できます。

マウスとキーボードの制御を要求するには、画面共有ビューアの左上にある「マウスアイコン」をクリックします。共有者にはあなたの要求が通知され、許可または拒否できます。共有者がマウスとキーボードの制御要求を承認すると、視聴者であるあなたと画面共有の共有者の両方がセッション内でマウスとキーボードの制御を共有します。



注:

共有者はいつでもマウスとキーボードの排他的な制御を取り戻すことができます。



仮想ディスプレイレイアウト

仮想ディスプレイ構成を使用すると、ライブセッション内でVDA上のセッションモニターごとに仮想ディスプレイレイアウトを定義できます。この機能により、各セッションモニターを個別に複数の仮想モニターに分割できます。

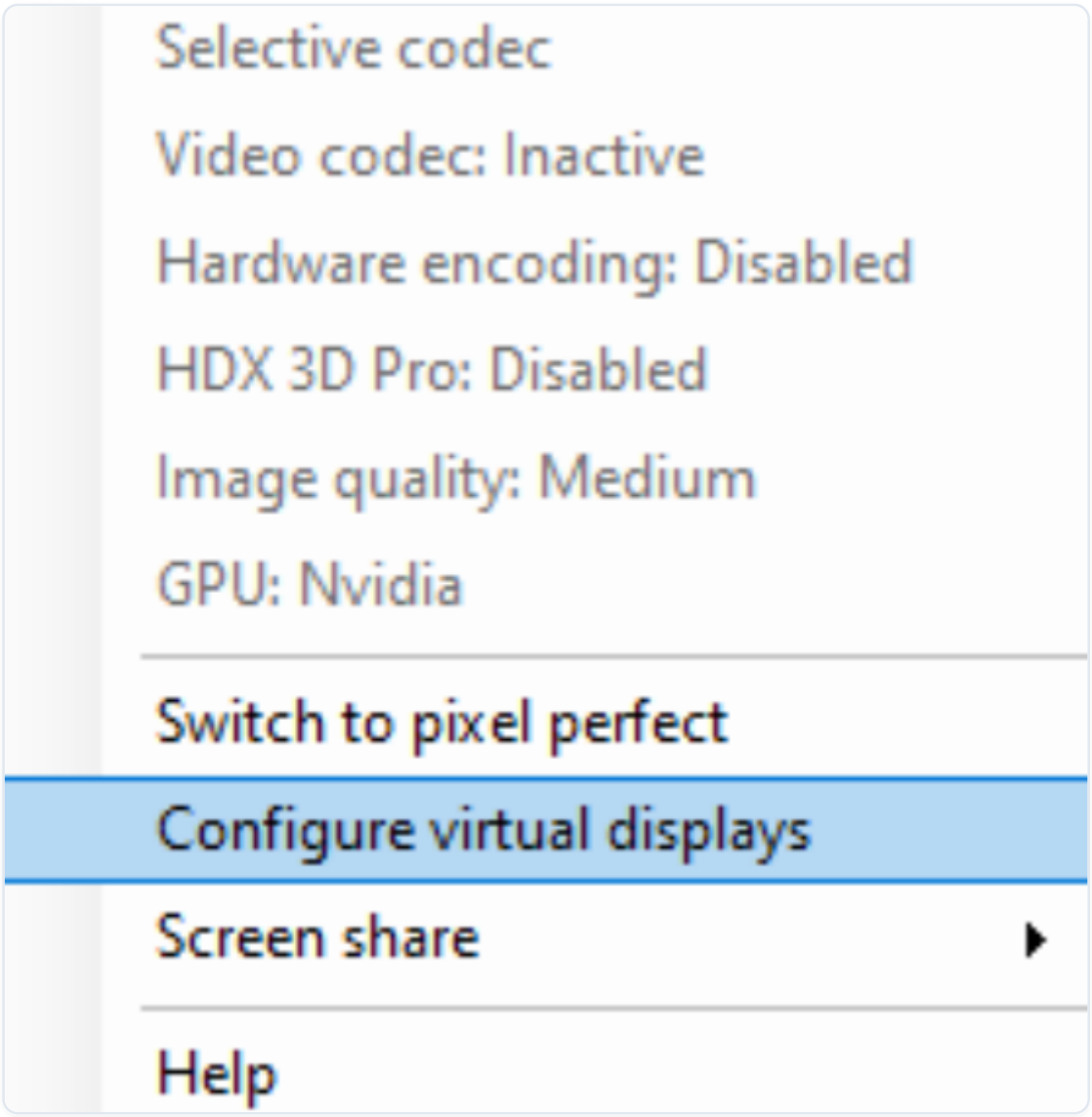
仮想ディスプレイ構成UIを使用すると、ライブセッション内でVDA上のセッションモニターごとに仮想ディスプレイレイアウトを定義できます。この機能により、各セッションモニターを個別に複数の仮想モニターに分割できます。リモートデスクトップでは、合計8つの仮想モニターに分割できます。また、ディスプレイのセッションプライマリモニターとDPI設定を更新することもできます。

システム要件

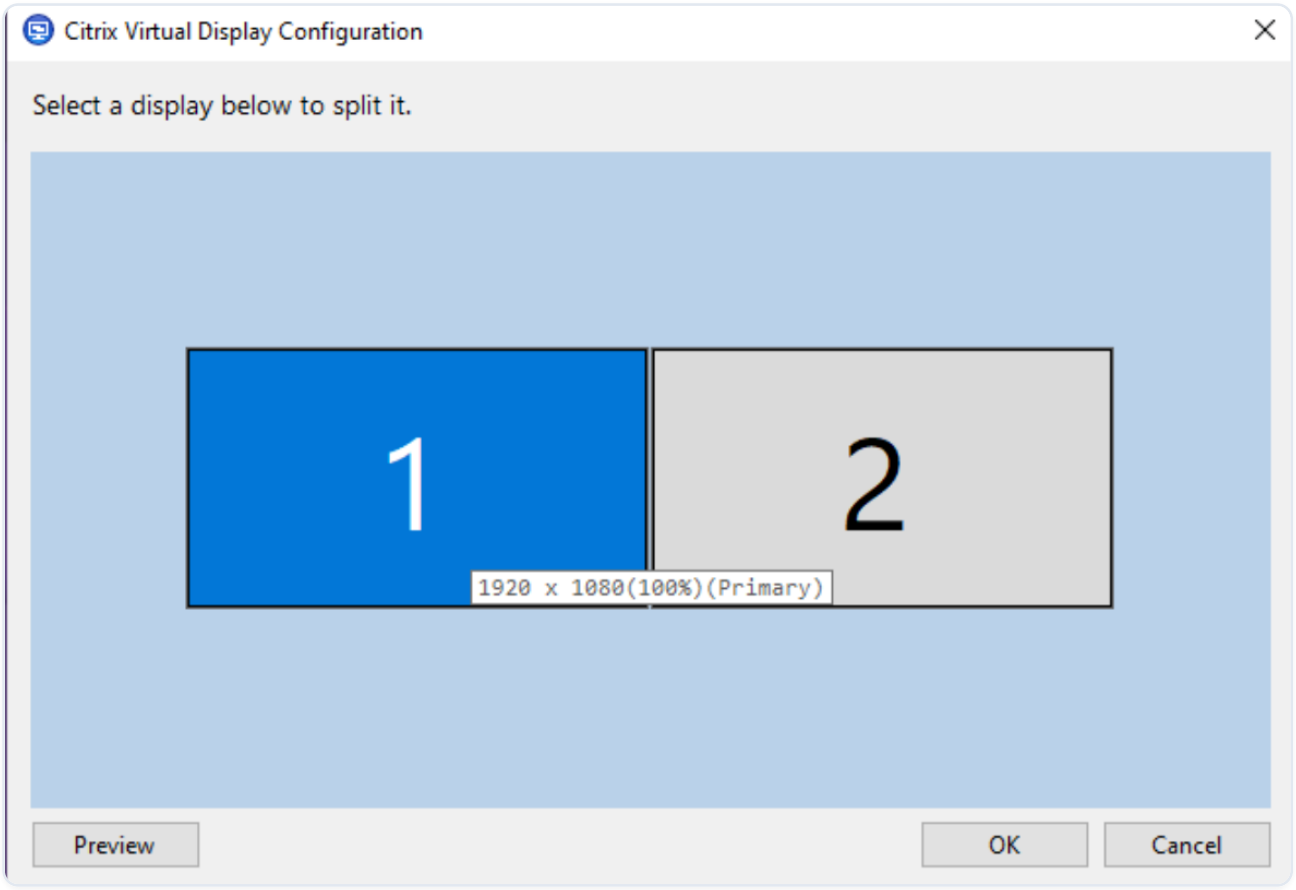
- Windows: シングルセッションまたはマルチセッションOS VDA
- グラフィックステータスインジケーターポリシーを有効にする必要があります
- デスクトップセッションのみ構成できます。

構成

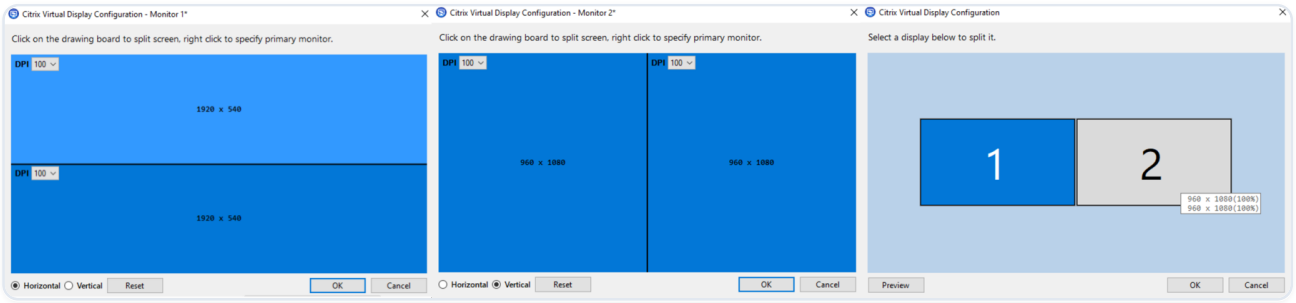
仮想ディスプレイレイアウトを構成するには、グラフィックステータスインジケーターアイコンを右クリックし、「仮想ディスプレイの構成」オプションを選択します。仮想ディスプレイ構成UIが起動します。



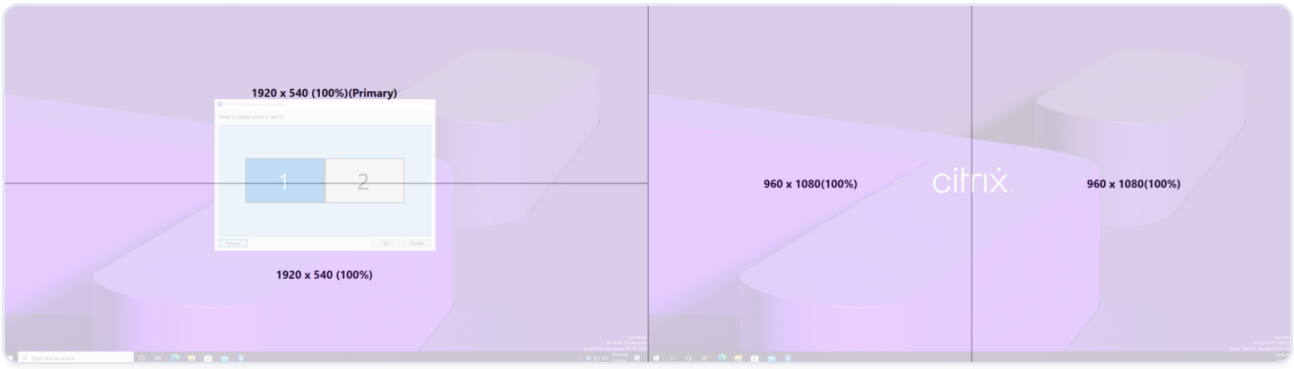
UIには現在のセッションディスプレイレイアウトが表示され、青色はセッションのプライマリモニターを示します。ディスプレイにカーソルを合わせると、ディスプレイ設定のツールヒントが表示されます。このツールヒントには、特定のセッションモニターで定義されている現在の仮想ディスプレイレイアウトに関する情報が表示されます。



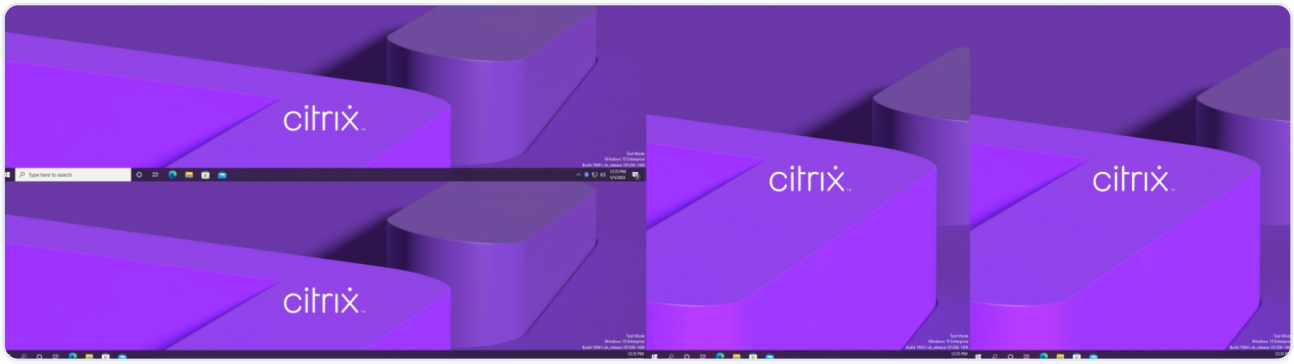
ディスプレイを選択すると、対話型UIに移行し、選択したセッションモニターの仮想ディスプレイを構成できます。水平線または垂直線を描画して、画面を仮想モニターに分割できます。画面は、セッションモニターの解像度の指定されたパーセンテージに従って分割されます。仮想ディスプレイを右クリックしてプライマリモニターとしてマークし、DPIドロップダウンリストを使用して仮想ディスプレイの優先スケーリング係数を設定します。仮想ディスプレイレイアウトを定義したら、**OK**をクリックしてレイアウトを一時的に保存するか、**キャンセル**をクリックして変更を破棄します。**リセット**を使用して構成を元に戻し、セッションモニターの元のレイアウトを復元できます。



現在構成されている仮想ディスプレイレイアウトをプレビューするには、**プレビュー**ボタンをクリックします。セッション内の仮想ディスプレイの予想される位置と解像度を強調表示するウィンドウが表示されます。



OKをクリックして、仮想ディスプレイレイアウトをすぐに適用して保存します。**キャンセル**をクリックしてUIを閉じ、すべての変更を破棄します。



その他の考慮事項

- 必要な最小仮想ディスプレイ解像度は640 x 480です。
- UIで定義された仮想ディスプレイDPIは、指定されたディスプレイ解像度に対するOSのスケーリングサポートに依存します。
- Citrix Workspace™アプリの既存の仮想ディスプレイ機能と同時にこの機能を使用しないでください。
- プレビュー機能はServer 2016ではサポートされていません。

セッションベースのウォーターマーク

テキストベースのセッションウォーターマークは、データ盗難を抑止し、追跡を可能にするのに役立ちます。この追跡可能な情報は、写真やスクリーンキャプチャを使用してデータを盗む者への抑止力として、セッションデスクトップに表示されます。テキストのレイヤーであるウォーターマークを指定できます。

ウォーターマークは、元のドキュメントの内容を変更することなく、セッション画面全体に表示できます。テキストベースのセッションウォーターマークには、VDAのサポートが必要です。

> **重要:**

> テキストベースのセッションウォーターマークは、セキュリティ機能ではありません。このソリューションはデータ盗難を完全に防ぐものではありませんが、ある程度の抑止力と追跡可能性を提供します。この機能を使用した場合の完全な情報追跡可能性は保証しませんが、必要に応じて他のセキュリティソリューションと組み合わせて使用することをお勧めします。

> セッションウォーターマークはテキストであり、ユーザーに配信されるセッションに適用されます。セッションウォーターマークには、データ盗難を追跡するための情報が含まれています。最も重要なデータは、スクリーンイメージが取得された現在のセッションのログオンユーザーのIDです。データ漏洩をより効果的に追跡するために、サーバーまたはクライアントのインターネットプロトコルアドレスや接続時間などの他の情報を含めます。

ユーザーエクスペリエンスを調整するには、セッションウォーターマークポリシー設定 を使用して、画面上の配置とウォーターマークの外観を構成します。

要件:

仮想配信エージェント:

マルチセッションOS 7.17 シングルセッションOS 7.17

制限事項:

- セッションウォーターマークは、ローカルアプリアクセス、Windowsメディアリダイレクト、MediaStream、ブラウザコンテンツリダイレクト、およびHTML5ビデオリダイレクトが使用されているセッションではサポートされていません。セッションウォーターマークを使用するには、これらの機能が無効になっていることを確認してください。
- セッションが全画面ハードウェアアクセラレーションモード（全画面H.264またはH.265エンコーディング）で実行されている場合、セッションウォーターマークはサポートされず、表示されません。
- これらのHDX™ポリシーを設定すると、ウォーターマーク設定は有効にならず、セッション表示にウォーターマークは表示されません。

ビデオコーデックにハードウェアエンコーディングを使用 を **有効** **圧縮にビデオコーデックを使用** を **画面全体**

- これらのHDXポリシーを設定すると、動作は未定義となり、ウォーターマークが表示されない場合があります。

ビデオコーデックにハードウェアエンコーディングを使用 を **有効** **圧縮にビデオコーデックを使用** を **優先する場合にビデオコーデックを使用**

ウォーターマークが表示されるようにするには、**ビデオコーデックにハードウェアエンコーディングを使用** を **無効** に設定するか、**圧縮にビデオコーデックを使用** を **アクティブに変更される領域** または **ビデオコーデックを使用しない** に設定します。

- セッションウォーターマークは、Thinwireグラフィックモードのみをサポートします。
- セッションレコーディングを使用している場合、記録されたセッションにはウォーターマークは含まれません。
- Windowsリモートアシスタンスを使用している場合、ウォーターマークは表示されません。
- ユーザーが画面をキャプチャするために **Print Screen** キーを押した場合、VDA側でキャプチャされた画面にはウォーターマークは含まれません。キャプチャされた画像がコピーされるのを防ぐための対策を講じることをお勧めします。

Citrix スニッピングツール

概要

Citrix Snipping Toolを使用すると、ユーザーはCitrix Virtual Apps and Desktopsセッション内のオーバーレイおよびリダイレクトされたコンテンツのスクリーンショットをシームレスにキャプチャできます。

従来、ネイティブのセッション内スクリーンショットツールでは、クライアントエンドポイントに最適化またはオフロードされたコンテンツをキャプチャできません。このメディアはサーバー (VDA) ではなくローカルでレンダリングされるため、Microsoft Teamsのビデオやブラウザコンテンツリダイレクト (BCR) ウィンドウなどの最適化された要素は、通常、標準のスクリーンショットでは真っ黒なボックスまたはプレースホルダーグラフィックとして表示されます。

Citrix Snipping Toolは、すべてのリダイレクトされたコンテンツのセッション内スクリーンショットを可能にすることで、このギャップを埋めます。これにより、ドキュメント作成、トラブルシューティング、コラボレーションのために、ユーザーが見ているとおりにセッションをキャプチャし、完全で正確なキャプチャが保証されます。

サポートされるコンテンツ

Citrix Snipping Toolは、以下の機能によって最適化されたコンテンツを正常にキャプチャします。

- **ブラウザコンテンツリダイレクト (BCR):** オフロードされたWebレンダリングをキャプチャします。この機能の詳細については、ブラウザコンテンツリダイレクトのドキュメントを参照してください。
- **HTML5マルチメディアリダイレクト:** 最適化されたHTML5ビデオ要素をキャプチャします。この機能の詳細については、HTML5マルチメディアリダイレクトのドキュメントを参照してください。
- **Windowsメディアリダイレクト:** リダイレクトされたWindowsメディア再生をキャプチャします。この機能の詳細については、Windowsメディアリダイレクトのドキュメントを参照してください。
- **ユニファイドコミュニケーション (UC) の最適化:** HDX WebRTC / UCSDK最適化アプリケーション (Microsoft Teams VDI 1.0、Amazon Connect、Five9、Ring Centralなど) およびサードパーティ最適化アプリケーション (Microsoft Teams VDI 2.0 (SlimCore)、Zoom、Webexなど) のオーバーレイビデオとUI要素をキャプチャします。

システム要件

- **Virtual Delivery Agent (VDA):** バージョン2603以降。
- **Citrix Workspaceアプリ:** Windows版Citrix Workspaceアプリ バージョン2603以降。
- **サポートされるエンドポイントオペレーティングシステム:** Windowsのみ。(注: macOS、Linux、ChromeOSは現在サポートされていません)。

構成

Citrix Snipping ToolはCitrixポリシーによって制御されます。デフォルトでは、リダイレクトされたコンテンツをキャプチャする機能は有効になっています。

ポリシーを構成するには:

1. **Citrix Studio (またはWeb Studio)** を開き、ポリシーに移動します。
2. **Screenshot Redirected Content** ポリシー設定を見つけます。
3. ユーザーがオーバーレイコンテンツをキャプチャできるように**Enabled** を選択するか、お使いの環境にスクリーンキャプチャを禁止する厳格なセキュリティ要件がある場合はDisabled を選択します。

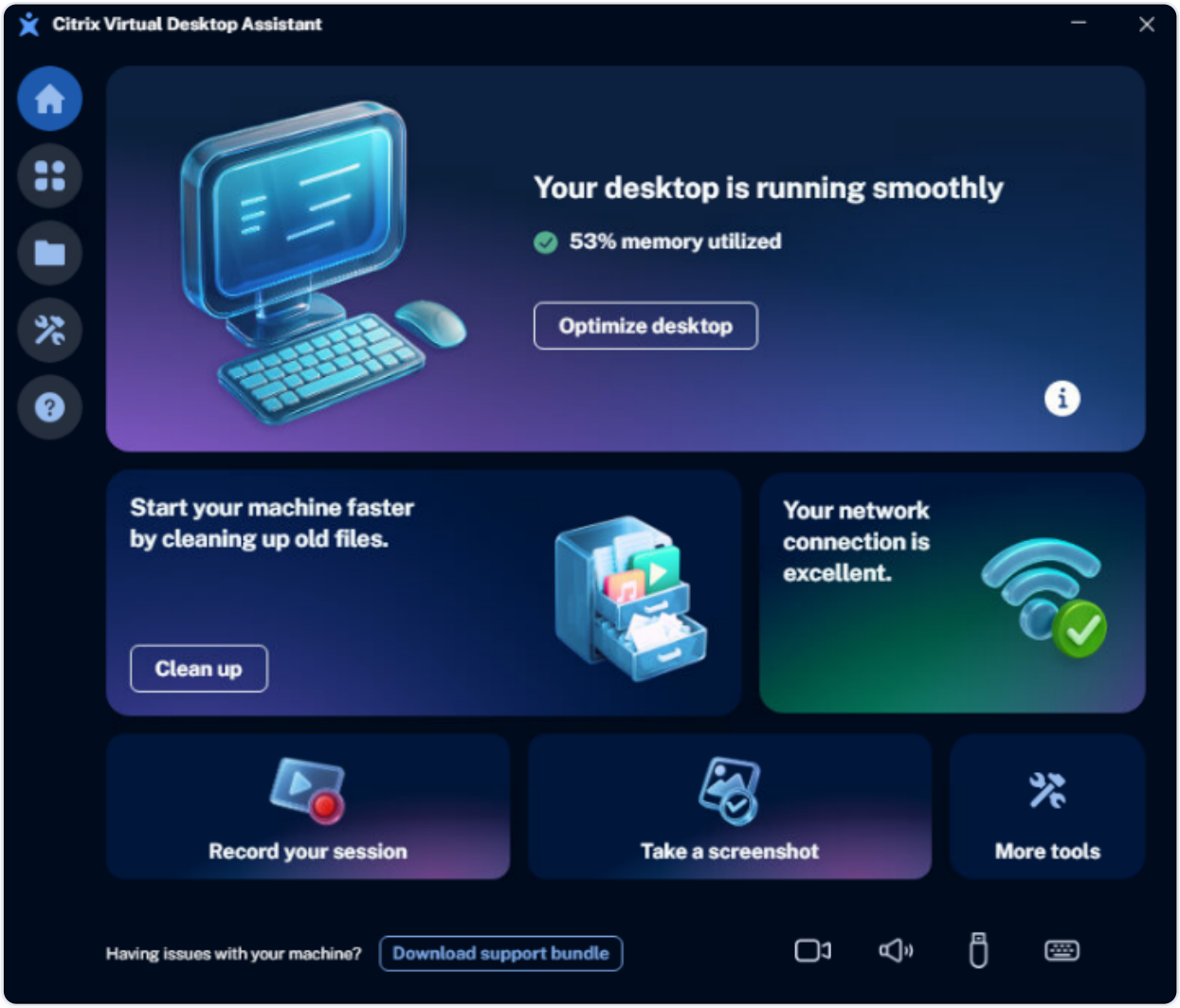
> **注:**

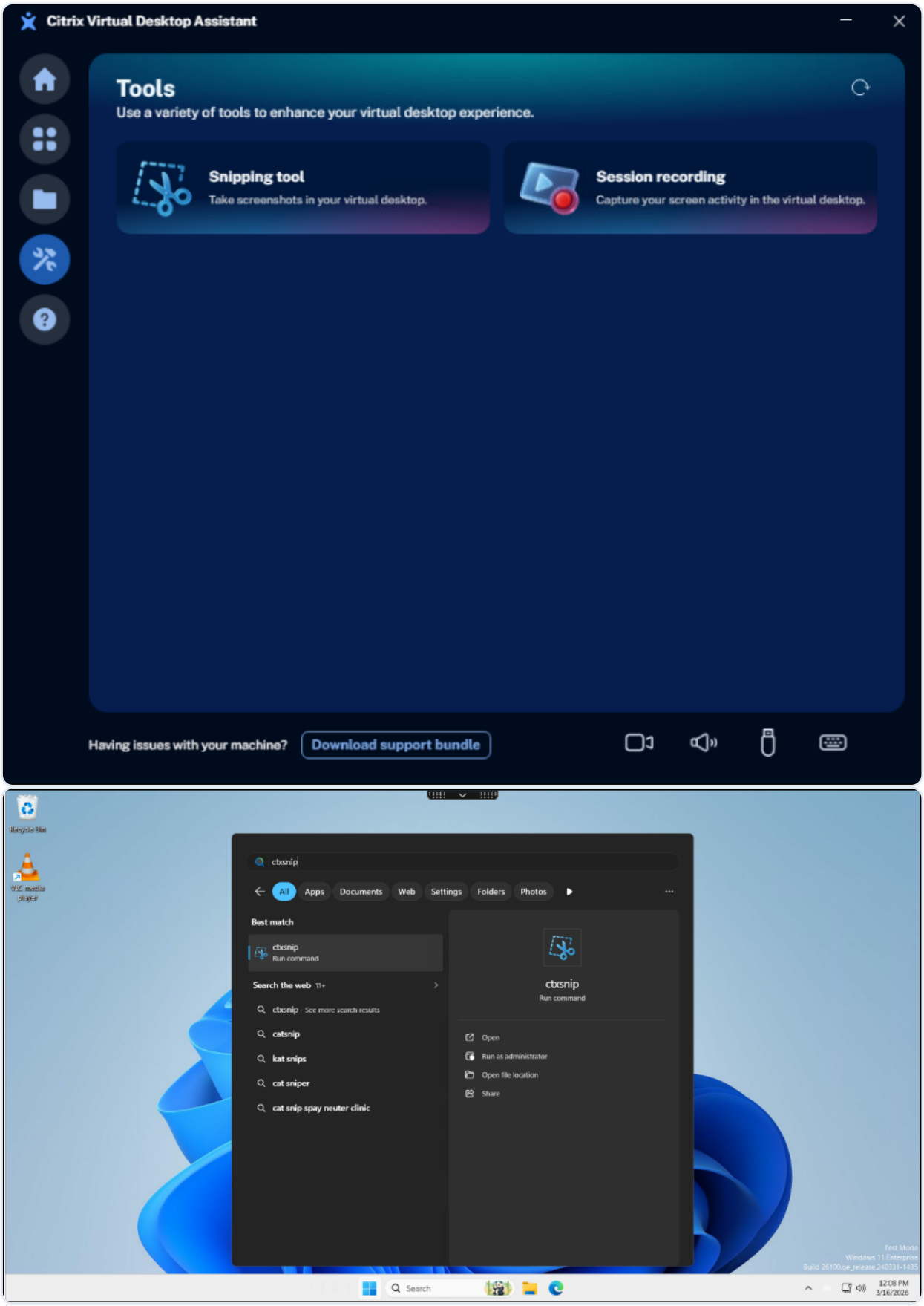
> Citrix Snipping Tool は、既存のセキュリティ境界を尊重します。Citrix App Protection がアクティブな場合、このツールはデータ漏洩を防ぐために、リダイレクトされたコンテンツのキャプチャを自動的に無効にします。詳細については、App Protection のドキュメントを参照してください。

使用方法

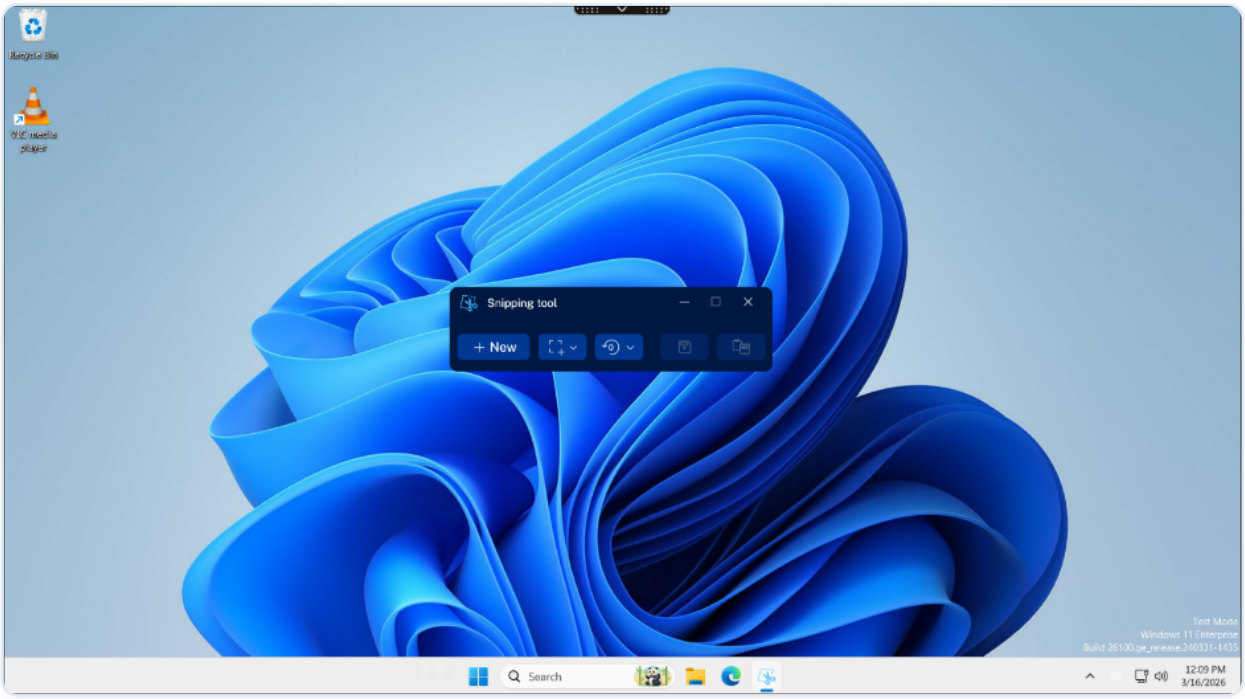
最適化された、またはリダイレクトされたオーバーレイコンテンツを含むセッション内のスクリーンショットをキャプチャするには、次の手順に従います。

1. Citrix は、Citrix Snipping Tool を Citrix Assistant (ホームページの から) から直接起動することをお勧めします。アプリケーションの詳細については、Citrix Assistant のドキュメント を参照してください。(または、仮想デスクトップセッション内で Windows のスタートメニューを開いて Citrix Snipping Tool を起動することもできます)

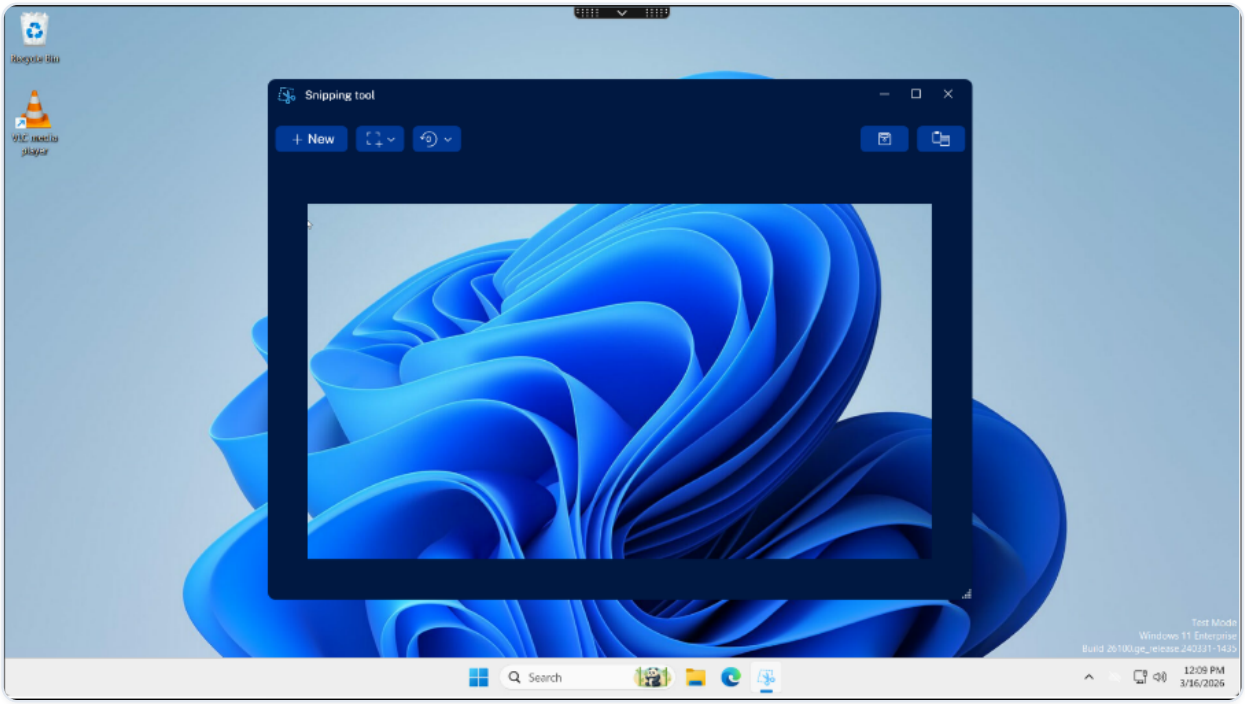




2. ボタンをクリックして、キャプチャを開始します。



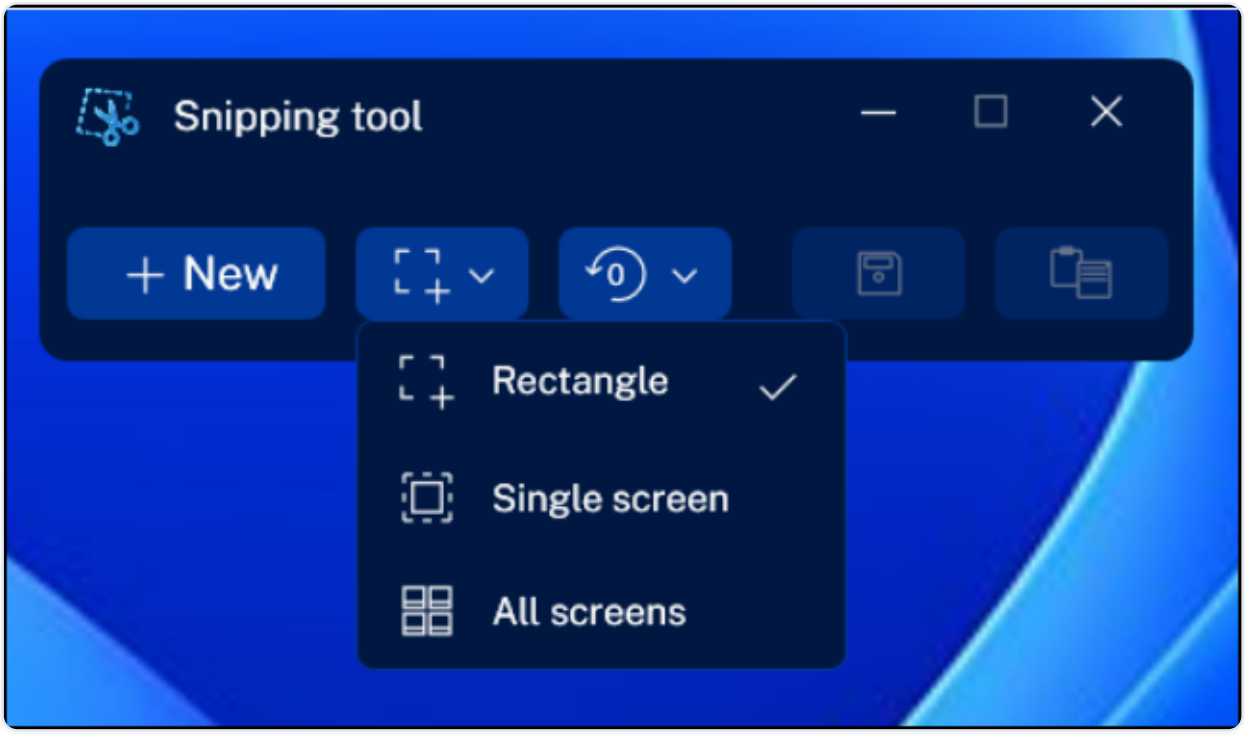
3. カーソルをクリックしてドラッグし、キャプチャしたい画面の特定の領域を選択します。スクリーンショットがキャプチャされたら、画像をクリップボードに直接コピーするか、.PNG または .BMP ファイルとして保存できます。



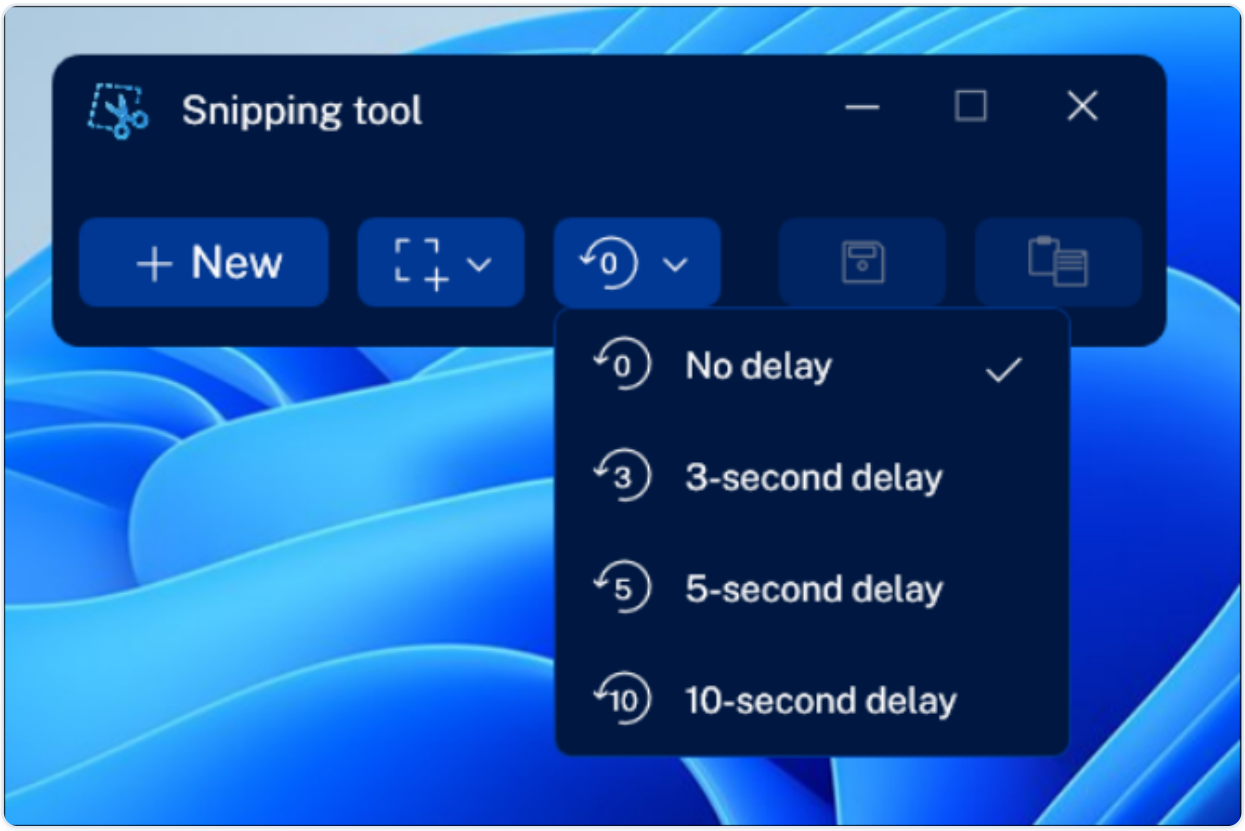
その他のオプション

Citrix Snipping Tool には、スクリーンショットをカスタマイズするための追加設定が含まれています。

- **切り取り領域:** デフォルトでは、このツールは画面のカスタムのユーザー定義領域をキャプチャします。このモードを変更して、セッション全体のフルスクリーンショットをキャプチャできます。マルチモニター設定を使用している場合、フルスクリーンモードはすべてのアクティブな画面をキャプチャします。



- 遅延タイマー: ドロップダウンメニューやホバーステートなど、一時的な画面要素をキャプチャするには、「遅延」ボタンを使用してカウントダウンタイマーを選択します。ツールは、指定された時間待機してから画面をフリーズし、スニップをキャプチャします。



トラブルシューティング

オーバーレイコンテンツがキャプチャされない

- Citrix Studioで「スクリーンショットのリダイレクトされたコンテンツ」ポリシーが「有効」に設定されていることを確認してください。
- Virtual Delivery Agent (VDA) と Citrix Workspace アプリの両方が、最小バージョン要件 (2603 以降) を満たしていることを確認してください。
- App Protection またはその他の画面キャプチャ防止セキュリティポリシーがアクティブになっていないか確認してください。これらのセキュリティ境界が有効になっている場合、データ漏洩を防ぐためにツールの機能が意図的にブロックされます。

スクリーンショットに黒いバーまたはプレースホルダーメッセージが残る

- 画面をキャプチャするために Citrix Snipping Tool を積極的に使用していることを確認してください。ネイティブ OS のスクリーンショットユーティリティ (デフォルトの Windows Snipping Tool など) やサードパーティのキャプチャアプリケーションでは、最適化されたオーバーレイコンテンツをインターセプトできず、依然として黒いボックスが表示されます。

Citrix Snipping Tool が利用できない、または見つからない

- Virtual Delivery Agent (VDA) がバージョン 2603 以降に更新されていることを確認してください。古い VDA リリースでは、このアプリケーションは存在しないか、サポートされていません。

シームレス

Citrix Published Applications は Citrix Virtual Apps and Desktops の主要な機能です。これにより、顧客は完全なデスクトップを必要とせずに、個々の Windows または Linux アプリケーションをユーザーに直接配信できます。

これにより、ユーザーはアプリケーションをローカルにインストールして管理する必要がなくなり、ワークフローが簡素化され、IT の負担が軽減されます。ユーザーは完全なリモートデスクトップ環境と対話する代わりに、アプリケーションウィンドウと直接対話し、シームレスで合理化されたエクスペリエンスを実現します。

シームレス(/en-us/citrix-virtual-apps-desktops/current-release/media/seamless-1.png)

公開アプリケーション（シームレスアプリケーションとも呼ばれます）の背後にあるテクノロジーにより、アプリケーションはリモートサーバー上で実際に動作しているにもかかわらず、ユーザーのローカルデバイスで直接実行されているかのようにユーザーに配信できます。これは、アプリケーションがホストされている Windows Server デスクトップを隠し、アプリケーションをユーザーにシームレスに提示することで実現されます。

シームレスアプリケーションは、Windows VDA と Linux VDA の両方で利用できます。Windows VDA の場合、シームレスアプリケーションは、Microsoft Windows Server オペレーティングシステムを実行する TSVDA と、Microsoft Windows 10 または Windows 11 を実行する WSVDA の両方をサポートします。

シームレスアプリケーションには、次のような多くの利点があります。

- **ユーザーエクスペリエンスの向上:** ユーザーは、基盤となるオペレーティングシステムを気にすることなく、あらゆるデバイスからアプリケーションにアクセスできます。
- **セキュリティの強化:** アプリケーションはリモートサーバーで実行されるため、マルウェアやその他の脅威から保護するのに役立ちます。
- **IT コストの削減:** シームレスアプリケーションは、アプリケーションの管理と展開を簡素化することで、IT コストの削減に役立ちます。
- **一元管理:** アプリケーションは一元的に管理および更新できるため、IT 管理が簡素化され、組織全体で一貫性が確保されます。これにより、パッチ、更新、および新しいアプリケーションの展開に必要な時間と労力が削減されます。

- **アプリケーションの互換性:** 標準化されたサーバー環境でアプリケーションを実行することで、異なるクライアントオペレーティングシステムやハードウェア構成から生じる可能性のある互換性の問題を軽減できます。
- **合理化されたアプリケーション配信:** Citrix は、HDX™ のような高度なテクノロジーを活用して、公開デスクトップと公開アプリケーションの両方で、帯域幅が制限された接続でも、リッチでインタラクティブなエクスペリエンスをユーザーに提供します。
- **異種アプリケーションのサポート:** 管理者は、Linux アプリケーションを Windows アプリケーションと並行して公開できるため、両方のプラットフォームからアプリケーションにシームレスにアクセスできます。

シームレスアプリケーションを公開する

> **注:**
>
> バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

はじめに

展開でデリバリーグループのみを使用している場合（アプリケーショングループは使用しない場合）、アプリケーションはデリバリーグループに追加します。アプリケーショングループも使用している場合は、通常、代わりにアプリケーショングループにアプリケーションを追加します。このガイダンスにより、管理が容易になります。アプリケーションは常に少なくとも1つのデリバリーグループまたはアプリケーショングループに属している必要があります。

アプリケーションの追加ウィザードでは、1つ以上のデリバリーグループ、または1つ以上のアプリケーショングループを選択できますが、両方は選択できません。後でアプリケーションのグループ関連付けを変更することはできますが（たとえば、アプリケーショングループからデリバリーグループにアプリケーションを移動するなど）、ベストプラクティスでは、そのような複雑さを追加することは推奨されません。アプリケーションは1種類のグループに保持してください。

アプリケーションを複数のグループに関連付ける場合、それらのすべてのグループでアプリケーションを表示するのに十分な権限がないと、可視性の問題が発生する可能性があります。そのよ

うな場合は、より高い権限を持つ管理者に相談するか、アプリケーションが関連付けられているすべてのグループを含むようにスコープを拡張してください。

同じ名前の2つのアプリケーション（異なるグループからのものなど）を同じユーザーに公開する場合、Web Studioで`Application name (for user)`プロパティを変更します。そうしないと、ユーザーはCitrix Workspace™アプリで重複する名前を目にすることになります。

アプリケーションのプロパティ（設定）は、追加時または後で変更できます。アプリケーションが配置されているアプリケーションフォルダーも、アプリケーションの追加時または後で変更できます。

詳細については、以下を参照してください。

- 「デリバリーグループの作成」(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/delivery-groups-create.html)
- アプリケーショングループの作成
- タグ

アプリケーションの追加

デリバリーグループまたはアプリケーショングループを作成するときにアプリケーションを追加できます。これらの手順については、デリバリーグループの作成およびアプリケーショングループの作成で詳しく説明されています。次の手順では、グループ作成後にアプリケーションを追加する方法について説明します。

知っておくと良いこと:

- Remote PC Accessデリバリーグループにアプリケーションを追加することはできません。
- アプリケーションの追加ウィザードを使用して、デリバリーグループまたはアプリケーショングループからアプリケーションを削除することはできません。これは別の操作です。

1つ以上のアプリケーションを追加するには：

1. 左ペインで**アプリケーション**を選択し、アクションバーで**アプリケーションの追加**を選択します。
2. アプリケーションの追加ウィザードが**はじめに**ページとともに起動します。このページは、今後のウィザードの起動時に表示しないように設定できます。
3. ウィザードは、**グループ**、**アプリケーション**、**概要**の各ページを案内します。各ページの作業が完了したら、**概要**ページに到達するまで**次へ**をクリックします。

単一のデリバリーグループまたはアプリケーショングループにアプリケーションを追加する場合の、手順1の代替方法：

- **1つのデリバリーグループにのみアプリケーションを追加するには：** 手順1で、Web Studioの左ペインで**デリバリーグループ**を選択し、中央ペインでデリバリーグループを選択してから、アクションバーで**アプリケーションの追加**を選択します。ウィザードには**グループ**ページが表示されません。
- **1つのアプリケーショングループにのみアプリケーションを追加するには：** 手順1で、Web Studioの左ペインで**アプリケーション**を選択し、中央ペインでアプリケーショングループを選択してから、アクションバーでアプリケーショングループ名の下にある**アプリケーションの追加**エントリを選択します。ウィザードには**グループ**ページが表示されません。

グループページ

このページには、サイト内のすべてのデリバリーグループが一覧表示されます。アプリケーショングループも作成している場合は、アプリケーショングループとデリバリーグループが一覧表示されます。どちらかのグループを選択できますが、両方のグループを選択することはできません。つまり、アプリケーショングループとデリバリーグループに同時にアプリケーションを追加することはできません。通常、アプリケーショングループを使用している場合は、デリバリーグループではなくアプリケーショングループにアプリケーションを追加します。

アプリケーションを追加するときは、少なくとも1つのデリバリーグループ（または、利用可能な場合はアプリケーショングループ）の横にあるチェックボックスをオンにします。すべてのアプリケーションは、常に少なくとも1つのグループに関連付けられている必要があります。

アプリケーションページ

追加をクリックして、アプリケーションソースを表示します。

- **スタートメニューから**：選択したデリバリーグループ内のマシンで検出されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストが表示された新しいページが起動します。追加するアプリケーションのチェックボックスをオンにして、「**OK**」をクリックします。

  このソースは、(1)関連付けられたデリバリーグループがないアプリケーショングループを選択した場合、(2)関連付けられたデリバリーグループにマシンが含まれていないアプリケーショングループを選択した場合、または(3)マシンが含まれていないデリバリーグループを選択した場合は、選択できません。

- **手動：** デリバリーグループ内のVDAまたはネットワーク上の別の場所にあるアプリケーション。このソースを選択すると、新しいページが開き、次の方法で追加するアプリケーションを指定できます。

  - 実行可能ファイルへのパス、作業ディレクトリ、オプションのコマンドライン引数、および管理者とユーザーの表示名を入力します。
  - デリバリーグループ内のVDAからアプリケーションを選択します。これを行うには、**参照**をクリックし、VDAにアクセスするための資格情報を入力し、VDAに接続されるまで待機してから、VDAからアプリケーションを選択します。選択したアプリケーションのプロパティが、ページのフィールドに自動的に入力されます。

- **既存:** 以前サイトに追加されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストを含む新しいページが起動します。追加するアプリケーションのチェックボックスを選択し、**OK**をクリックします。

  サイトにアプリケーションがない場合、このソースは選択できません。

- **アプリケーションパッケージ:** App-V、MSIX、MSIX app attach、またはFlexAppアプリケーションパッケージ内のアプリケーション。このソースを選択すると、**パッケージからのアプリケーションの追加**ページが起動します。アプリケーションパッケージソースを選択し、表示された結果から追加するアプリケーションを選択して、**OK**を選択します。詳しくは、「Appパッケージの展開と配信」を参照してください。

- **アプリケーショングループ**: アプリケーショングループ。このソースを選択すると、アプリケーショングループのリストを含む新しいページが起動します。（表示には各グループ内のアプリケーションもリストされますが、個々のアプリケーションではなくグループのみを選択できます。）選択したグループ内の現在および将来のすべてのアプリケーションが追加されます。追加するアプリケーショングループのチェックボックスを選択し、**OK**をクリックします。

  このソースは、(1) アプリケーショングループがない場合、または (2) 選択したデリバリーグループがアプリケーショングループをサポートしていない場合（たとえば、静的に割り当てられたマシンを持つデリバリーグループ）には選択できません。

表に示されているように、**追加**リストの一部のソースは、そのタイプの有効なソースがない場合、選択できません。互換性のないソース（たとえば、アプリケーショングループにアプリケーショングループを追加できないなど）はリストに含まれません。選択したグループに既に追加されているアプリケーションは選択できません。

このページまたは後で、アプリケーションのプロパティ（設定）を変更できます。

デフォルトでは、追加されたアプリケーションは`Applications`という名前のアプリケーションフォルダーに配置されます。このページまたは後で、アプリケーションを変更できます。アプリ

ケーションを追加しようとして、同じ名前のアプリケーションが同じフォルダーに存在する場合、追加しようとしているアプリケーションの名前を変更するよう求められます。提示された新しい名前を受け入れるか、拒否してアプリケーションの名前を変更するか、別のフォルダーを選択できます。たとえば、**Applications**フォルダーに`app`が既に存在し、そのフォルダーに`app`という名前の別のアプリケーションを追加しようとすると、新しい名前`app_1`が提示されます。

概要ページ

10個以下のアプリケーションを追加する場合、その名前は**追加するアプリケーション**にリストされます。10個を超えるアプリケーションを追加する場合、合計数が指定されます。

概要情報を確認し、**「完了」**をクリックします。

アプリケーションのグループ関連付けを変更する

アプリケーションを追加した後、そのアプリケーションが関連付けられているデリバリーグループとアプリケーショングループを変更できます。

アプリケーションを別のグループにドラッグできます。これは、アクションバーのコマンドを使用する代替手段です。

アプリケーションがアプリケーショングループを使用するか直接使用するかに関わらず、複数のデリバリーグループに関連付けられている場合、グループの優先順位を使用して、複数のグループが評価される順序を指定できます。アクセスポリシー、ユーザーリスト、スマートアクセスタグなどの要因に基づいてグループを考慮対象から除外でき、ゾーンの優先順位、起動準備、タグの制限などの要因によって、グループから選択される特定のマシンが影響を受ける可能性があります。デフォルトでは、すべてのグループの優先順位は0（最高）です。デリバリーグループの優先順位が同じ場合、アプリケーションの起動には最も負荷の低いデリバリーグループが選択されます。この場合、垂直負荷分散は考慮されません。

アプリケーションは、アプリケーションを配信できる共有（プライベートではない）マシンを含むデリバリーグループに関連付けることができます。また、共有マシンを含むデリバリーグループがデスクトップのみを配信する場合でも、(1) デリバリーグループに共有マシンが含まれており、XenDesktop 7.xバージョン7.9より前に作成された場合、および (2) `Edit delivery group`権限がある場合は、そのデリバリーグループを選択できます。プロパティダイアログがコミットされると、デリバリーグループの種類は自動的に`desktops and applications`に変換されます。

1. Web Studioにサインインし、左ペインで**Applications**を選択し、アプリケーションを選択します。
2. アクションバーで**「プロパティ」**を選択します。
3. **「グループ」**ページを選択します。

- グループを追加するには、**「追加」をクリックし、「アプリケーショングループ」または「デリバリーグループ」を選択します。（アプリケーショングループを作成していない場合、唯一の項目は「デリバリーグループ」**です。）次に、1つ以上の利用可能なグループを選択します。アプリケーションと互換性のないグループ、またはすでにアプリケーションに関連付けられているグループは選択できません。
- グループを削除するには、1つ以上のグループを選択し、**「削除」**をクリックします。グループの関連付けを削除した結果、アプリケーションがどのグループとも関連付けられなくなる場合、アプリケーションが削除されることを警告されます。
- グループの優先度を変更するには、グループを選択し、**「優先度の編集」をクリックします。優先度値を選択し、「OK」**をクリックします。

4. 完了したら、**「適用」をクリックして変更を適用し、ウィンドウを開いたままにするか、「OK」**をクリックして変更を適用し、ウィンドウを閉じます。

アプリケーションの複製、有効化または無効化、名前の変更、または削除

次のアクションが利用可能です。

- **複製：** 異なるパラメーターまたはプロパティを持つ別のバージョンを作成するために、アプリケーションを複製したい場合があります。アプリケーションを複製すると、一意のサフィックスで自動的に名前が変更され、元のアプリケーションの隣に配置されます。また、アプリケーションを複製してから、別のグループに追加したい場合もあります。（複製後、アプリケーションを移動する最も簡単な方法はドラッグすることです。）
- **有効化または無効化：** アプリケーションの有効化と無効化は、デリバリーグループまたはアプリケーショングループの有効化と無効化とは異なるアクションです。
- **名前の変更：** 一度に1つのアプリケーションのみ名前を変更できます。アプリケーションの名前を変更しようとして、同じ名前のアプリケーションが同じフォルダーまたはグループに存在する場合、別の名前を指定するように求められます。
- **削除：** アプリケーションを削除すると、関連付けられていたデリバリーグループおよびアプリケーショングループから削除されますが、元々アプリケーションを追加するために使用されたソースからは削除されません。アプリケーションの削除は、デリバリーグループまたはアプリケーショングループから削除するのとは異なるアクションです。

アプリケーションを複製、有効化、無効化、名前変更、または削除するには：

1. 左ペインで **Applications** を選択します。

2. 中央ペインで1つ以上のアプリケーションを選択し、アクションバーで適切なタスクを選択します。
3. プロンプトが表示されたら、アクションを確認します。

デリバリーグループからアプリケーションを削除する

アプリケーションは、少なくとも1つのデリバリーグループまたはアプリケーショングループに関連付けられている（属している）必要があります。アプリケーションをデリバリーグループから削除しようとしたときに、そのアプリケーションがどのデリバリーグループまたはアプリケーショングループとも関連付けがなくなる場合、続行するとアプリケーションが削除されるという通知が表示されます。その場合、そのアプリケーションを配信したい場合は、有効なソースから再度追加する必要があります。

1. 左側のペインで、**［デリバリーグループ］**を選択します。
2. デリバリーグループを選択します。中央下のペインの タブで、削除するアプリケーションを選択します。
3. アクションバーから を選択します。
4. 削除を確認します。

アプリケーショングループからアプリケーションを削除する

アプリケーションは、少なくとも1つのデリバリーグループまたはアプリケーショングループに属している必要があります。アプリケーションをアプリケーショングループから削除しようとしたときに、そのアプリケーションがどのグループにも属さなくなる場合、続行するとアプリケーションが削除されるという通知が表示されます。その場合、そのアプリケーションを配信したい場合は、有効なソースから再度追加する必要があります。

1. 左ペインで **Applications** を選択します。
2. 中央のペインでアプリケーショングループを選択し、1つまたは複数のアプリケーションを選択します。
3. アクションバーで を選択します。
4. 削除を確認します。

アプリケーションのプロパティを変更する

アプリケーションのプロパティは、一度に1つしか変更できません。

アプリケーションのプロパティを変更するには：

1. 左ペインで **Applications** を選択します。
2. アプリケーションを選択し、アクションバーで を選択します。
3. 変更するプロパティが含まれるページを選択します。
4. 完了したら、 をクリックして変更を適用し、ウィンドウを開いたままにするか、 をクリックして変更を適用してウィンドウを閉じます。

次のリストでは、ページが括弧内に表示されます。

プロパティ	ページ
Citrix Workspaceアプリにアプリケーションが表示されるカテゴリまたはフォルダー	配信
コマンドライン引数。「公開アプリケーションへのパラメーターの受け渡し」を参照してください。	場所
アプリケーションが利用可能なデリバリーグループとアプリケーショングループ	グループ
説明	識別
ファイル名拡張子とファイルの種類関連付け：アプリケーションが自動的に開く拡張子	ファイルの種類関連付け
アイコン	配信
StoreFront™のキーワード	識別
制限; アプリケーション制限の構成を参照	配信
名前: ユーザーおよび管理者に表示される名前	識別
実行可能ファイルへのパス; 公開アプリケーションへのパラメーターの受け渡しを参照	場所
ユーザーのデスクトップ上のショートカット: 有効または無効	配信
可視性: Citrix Workspaceアプリでアプリケーションを表示できるユーザーを制限します。非表示のアプリケーションでも起動できます。利	可視性の制限

プロパティ	ページ
用不可かつ非表示にするには、別のグループに追加します。	
作業ディレクトリ	場所

アプリケーションの変更は、現在のアプリケーションユーザーがセッションからログオフするまで有効にならない場合があります。

アプリケーション制限を構成する

アプリケーションの使用状況を管理するために、アプリケーション制限を構成します。たとえば、アプリケーション制限を使用して、アプリケーションに同時にアクセスするユーザーの数を管理できます。同様に、アプリケーション制限は、リソースを大量に消費するアプリケーションの同時インスタンス数を管理するためにも使用できます。この制限は、サーバーのパフォーマンスを維持し、サービスの劣化を防ぐのに役立ちます。

この機能は、Controller によって仲介されるアプリケーションの起動数（Citrix Workspace アプリや StoreFront からの起動など）を制限するものであり、他の方法で起動できる実行中のアプリケーションの数を制限するものではありません。これは、アプリケーション制限が同時使用を管理する際に管理者を支援するものの、すべてのシナリオで強制力を持つわけではないことを意味します。たとえば、Controller が停止モードの場合、アプリケーション制限は適用できません。

デフォルトでは、同時に実行できるアプリケーションインスタンスの数に制限はありません。アプリケーション制限の設定はいくつかあります。それらのいずれか、またはすべてを構成できます。

- デリバリーグループ内のすべてのユーザーによるアプリケーションの同時インスタンスの最大数。
- デリバリーグループ内のユーザーごとのアプリケーションのインスタンス数（1つ）。
- マシンごとのアプリケーションの同時インスタンスの最大数（PowerShell のみ）。

制限が構成されている場合、ユーザーが構成された制限を超えるアプリケーションインスタンスを起動しようとすると、エラーメッセージが生成されます。複数の制限が構成されている場合、最初に到達した制限でエラーが報告されます。

アプリケーション制限の使用例：

- **同時インスタンス数の最大制限:** デリバリーグループで、アプリケーション `Alpha` の同時インスタンスの最大数を 15 に構成します。その後、そのデリバリーグループのユーザーは、そ

のアプリケーションのインスタンスを 15 個同時に実行しています。そのデリバリーグループのいずれかのユーザーが `Alpha` を起動しようとすると、エラーメッセージが生成されます。`Alpha` は、構成された同時アプリケーションインスタンス制限（15）を超えるため、起動されません。

- **ユーザーごとのインスタンス数制限:** 別のデリバリーグループで、アプリケーション `Beta` のユーザーごとのインスタンス数オプションを有効にします。ユーザー Tony はアプリケーション `Beta` を正常に起動します。その日の後半、そのアプリケーションが Tony のセッションでまだ実行されている間に、彼は `Beta` の別のインスタンスを起動しようとします。エラーメッセージが生成され、`Beta` はユーザーごとのインスタンス数制限を超えるため、起動されません。
- **同時インスタンス数の最大制限とユーザーごとのインスタンス数制限:** 別のデリバリーグループで、同時インスタンスの最大数を 10 に構成し、アプリケーション `Delta` のユーザーごとのインスタンス数オプションを有効にします。その後、そのデリバリーグループの 10 人のユーザーがそれぞれ `Delta` のインスタンスを実行している場合、そのデリバリーグループの他のユーザーが `Delta` を起動しようとすると、エラーメッセージが表示されます。`Delta` は起動されません。現在の 10 人の `Delta` ユーザーのいずれかがそのアプリケーションの 2 番目のインスタンスを起動しようとすると、エラーメッセージが表示され、2 番目のインスタンスは起動されません。
- **マシンごとの同時インスタンス数の最大制限とタグ制限の使用:** アプリケーション `Charlie` には、特定のサーバーで同時に実行できるインスタンスの数を規定するライセンスおよびパフォーマンス要件があります。これらの要件は、サイト内のすべてのサーバーで同時に実行できるインスタンスの数も規定します。

  アプリケーションのインスタンス数/マシン制限は、サイト内のすべてのサーバーに影響します（特定のデリバリーグループ内のマシンだけでなく）。サイトに 3 台のサーバーがあるとします。アプリケーション `Charlie` の場合、マシンあたりのアプリインスタンス制限を 2 に構成します。したがって、サイト全体でアプリケーション `Charlie` のインスタンスは 6 つまでしか起動できません。（これは、3 台のサーバーそれぞれで Charlie のインスタンスが 2 つという制限です。）

  アプリケーションの使用をデリバリーグループ内の特定のコンピューターのみに制限するには（サイト全体のすべてのコンピューターでのインスタンス制限に加えて）：

  - それらのマシンにタグ付け機能を使用します。
  - そのアプリケーションのマシンごとの最大インスタンス数を構成します。

アプリケーションがControllerの仲介以外の方法（たとえば、Controllerが停止モードの場合など）で起動され、構成された制限を超過した場合、ユーザーは制限を超過しないように十分な数のインスタンスを閉じるまで、それ以上のインスタンスを起動できません。制限を超過したインスタンスは強制的にシャットダウンされません。ユーザーが閉じるまで継続して実行が許可されます。

セッションローミングを無効にする場合は、ユーザーごとのアプリケーションインスタンス数制限を無効にします。ユーザーごとのアプリケーションインスタンス数制限を有効にする場合は、新しいデバイスでの新しいセッションを許可する2つの値のいずれも構成しないでください。ローミングについて詳しくは、「セッション」を参照してください。

デリバリーグループごとの最大インスタンス数制限と、ユーザーごとのインスタンス数制限を構成するには：

1. 左側のペインで **［アプリケーション］** を選択し、アプリケーションを選択します。
2. アクションバーで **［アプリケーションプロパティの編集］** を選択します。
3. **［配信］** ページで、次のいずれかのオプションを選択します。
    - **アプリケーションの無制限の使用を許可する**。同時に実行されるインスタンスの数に制限はありません。これがデフォルトです。
    - **アプリケーションの制限を設定する**。制限の種類は2つあります。いずれかまたは両方を指定します。
        - マシンごとに同時に実行できるインスタンスの最大数を指定します
        - ユーザーごとにアプリケーションのインスタンスを1つに制限する
4. **［OK］** をクリックして変更を適用し、ダイアログボックスを閉じます。または、 **［適用］** をクリックして変更を適用し、ダイアログボックスを開いたままにします。

マシンごとの最大インスタンス数制限を構成するには（PowerShellのみ）：

- PowerShellで（Citrix Cloud™展開の場合はRemote PowerShell SDKを、オンプレミス展開の場合はPowerShell SDKを使用して）、適切な `BrokerApplication` コマンドレットを `MaxPerMachineInstances` パラメーターとともに指定します。
- ガイダンスについては、`Get-Help` コマンドレットを使用してください。例:

```
Get-Help Set-BrokerApplication –Parameter MaxPerMachineInstances
```

公開アプリケーションにパラメーターを渡す

アプリケーションのプロパティの**場所**ページを使用して、コマンドラインを入力し、公開アプリケーションにパラメーターを渡します。

公開アプリケーションをファイルの種類に関連付けると、`"%*"` (二重引用符で囲まれたパーセント記号とアスタリスク記号) がアプリケーションのコマンドラインの末尾に追加されます。これらの記号は、ユーザーデバイスに渡されるパラメーターのプレースホルダーとして機能します。

公開アプリケーションが期待どおりに起動しない場合は、そのコマンドラインに正しい記号が含まれていることを確認してください。デフォルトでは、`"%*"` 記号が追加されると、ユーザーデバイスから提供されるパラメーターが検証されます。ユーザーデバイスから提供されるカスタマイズされたパラメーターを使用する公開アプリケーションの場合、コマンドライン検証をバイパスするために、`"%**"` 記号がコマンドラインに追加されます。アプリケーションのコマンドラインにこれらの記号が表示されない場合は、手動で追加してください。

実行可能ファイルへのパスにスペースを含むディレクトリ名が含まれている場合 (例: `"C:\Program Files"`)、スペースがコマンドラインの一部であることを示すために、アプリケーションのコマンドラインを二重引用符で囲みます。これを行うには、パスを二重引用符で囲み、`%*` 記号を別の二重引用符で囲みます。パスの閉じ引用符と `%*` 記号の開始引用符の間にスペースを含めるようにしてください。

たとえば、公開アプリケーションであるWindows Media Playerのコマンドラインは次のとおりです。

```
"C:\Program Files\Windows Media Player\mplayer1.exe" "%*"
```

> **注:**
>
> 公開アプリケーションを起動するためのコマンドラインの最大文字数 (引数を含む) は203文字です。

公開アプリケーションでのセッションサインアウトの問題のトラブルシューティング

アプリケーションを公開する場合、公開アプリケーションのメインの実行可能ファイルのみが指定されます。ただし、一部のアプリケーションは、バックグラウンドで実行され、メインの公開アプリケーションが閉じられたときに、対応するメインの実行可能ファイルによって閉じられない追加の (子) プロセスを生成する場合があります。追加のプロセスは、実行されるスクリプトや、`Run` や `RunOnceKey` のような特定のレジストリキーから作成されることもあります。これらのアプリケーションは、正常なサインアウトを妨げ、セッションが残存またはハングアップする原因となり、セッションが閉じられず、ユーザーがサインアウトされない可能性があります。

この場合、Citrix Director を使用してこれらのセッションをリセットまたは終了する必要があります。

セッションが適切にサインアウトされない問題を特定し、トラブルシューティングするために、Citrix は3つのレジストリエントリを提供しています。これらの問題によりセッションが適切にログオフされないことの特定とトラブルシューティングは、次の3段階のプロセスです。

1. どのセッションが公開アプリケーションによって正常なサインアウトを妨げているかを特定する
2. それらの公開アプリケーションが追加の (子) プロセスを生成するかどうかを特定する
3. これらのプロセスを指定されたレジストリエントリに追加して、サインアウトを妨げないようにする

ステップ2：公開アプリケーションが追加の（子）プロセスを生成するかどうかを特定する

公開アプリケーションが正常なサインアウトを妨げていると特定されたら、次のステップは、このアプリケーションが実行時に追加のプロセスを生成するかどうかを判断することです。

公開アプリケーションが閉じられたときに、`HKCU\Software\CitrixVolatile\Seamless\Sessions\[ID]\LogoffCheckerBlockingProcess` を読んで、どのプロセスが正常なサインアウトをブロックしているかを判断できます。

以下の例では、キー `LogoffCheckerBlockingProcess` に次のエントリが含まれています。

```
PhoneExperienceHost.exe

SkypeApp.exe

SkypeBackgroundHost.exe
```

これらのプロセスが正常なサインアウトを妨げていました。

> **注:**

> 確認したいセッションの正しいセッションIDで を置き換えてください。

ステップ3：これらのプロセスを指定されたレジストリエントリに追加して、サインアウトを妨げないようにする

これらのプロセスを以下のレジストリキーに追加することで、今後のセッションでサインアウトが妨げられるのを防ぐことができます。

```
Add the process file name to the following registry key:

Caution! Refer to the Disclaimer at the end of this article before using the Registry Editor.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI

Value Name:LogoffCheckSysModules

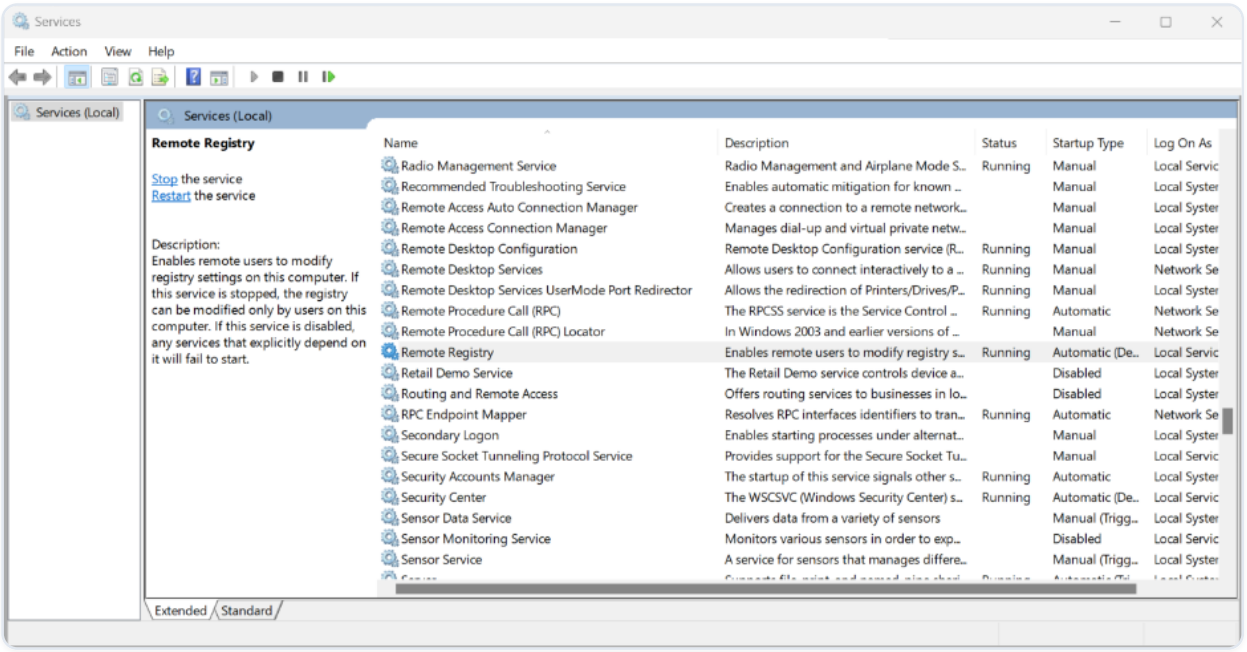
Type:REG_SZ

String:MyAppName.exe
```

`LogoffCheckSysModules` の詳細については、公開アプリケーションからの正常なログオフによりセッションがアクティブ状態になる を参照してください。

ステップバイステップのトラブルシューティングガイド

1. テスト対象のVDAでリモートレジストリサービスを開始します。
    a. コントロールパネルで、**管理ツール > サービス** を選択します。
    b. **リモートレジストリサービス** を右クリックし、**プロパティ** を選択します。
    c. **スタートアップの種類** で、ドロップダウンメニューから **自動** を選択します。



2. テスト対象のVDAでWindowsファイアウォールをオフにするか、ポート455を有効にする受信ファイアウォール規則を作成します:

   a. コントロールパネルで、**Windows Defender ファイアウォール > 詳細設定**を選択します。

   b. **受信の規則**を右クリックし、**新しい規則**を選択します。

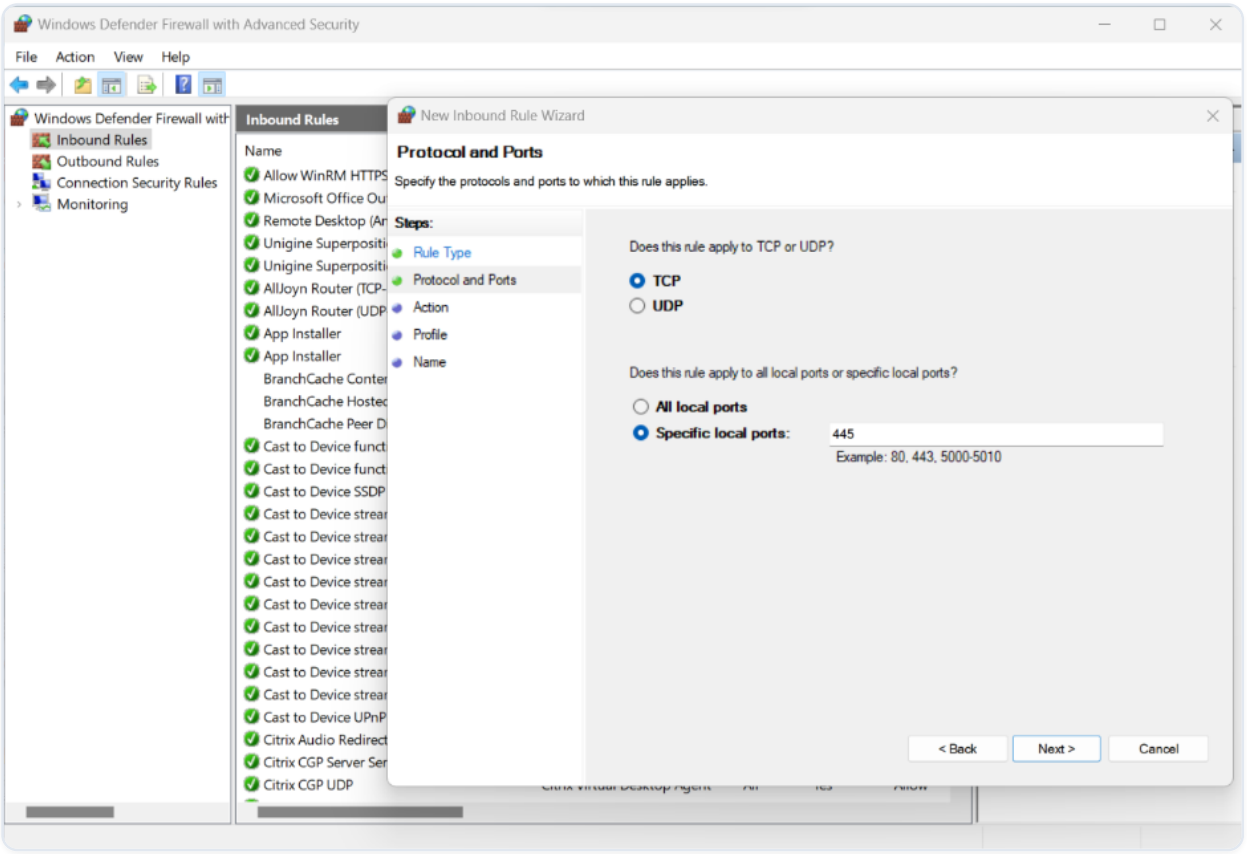
   c. **新しい受信の規則ウィザード**で、**ポート**を選択します。

   d. **プロトコルおよびポート**ページで、**TCP および特定のローカルポート**を選択します。ローカルポートとして `445` を入力します。

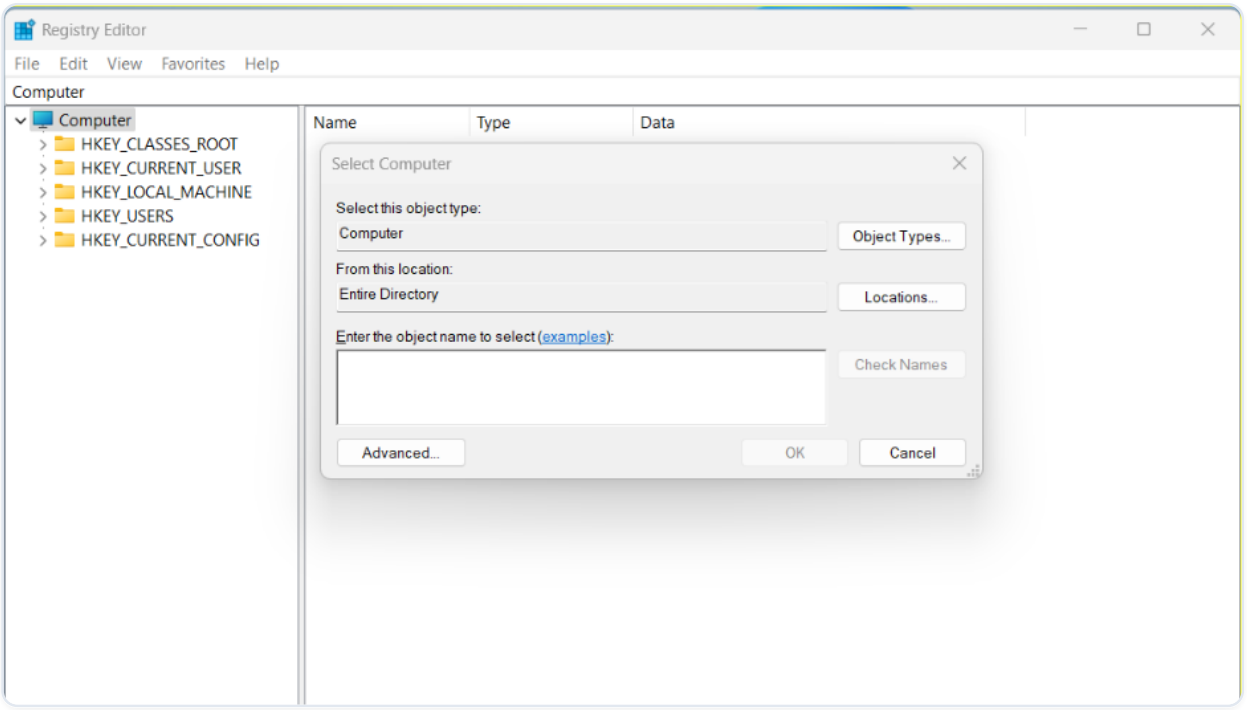
   e. **操作**ページで**接続を許可する**を選択します。

   f. 新しい受信規則を適用するファイアウォールプロファイルを選択します。

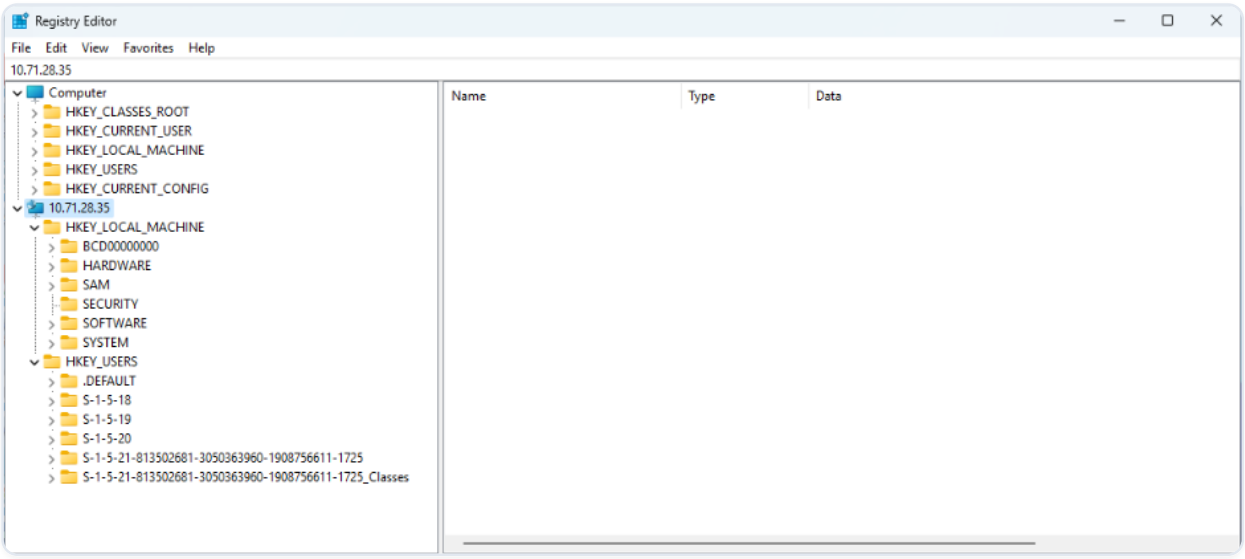
   g. ファイアウォール規則に名前を付け、**完了**を選択して**新しい受信の規則ウィザード**を終了します。



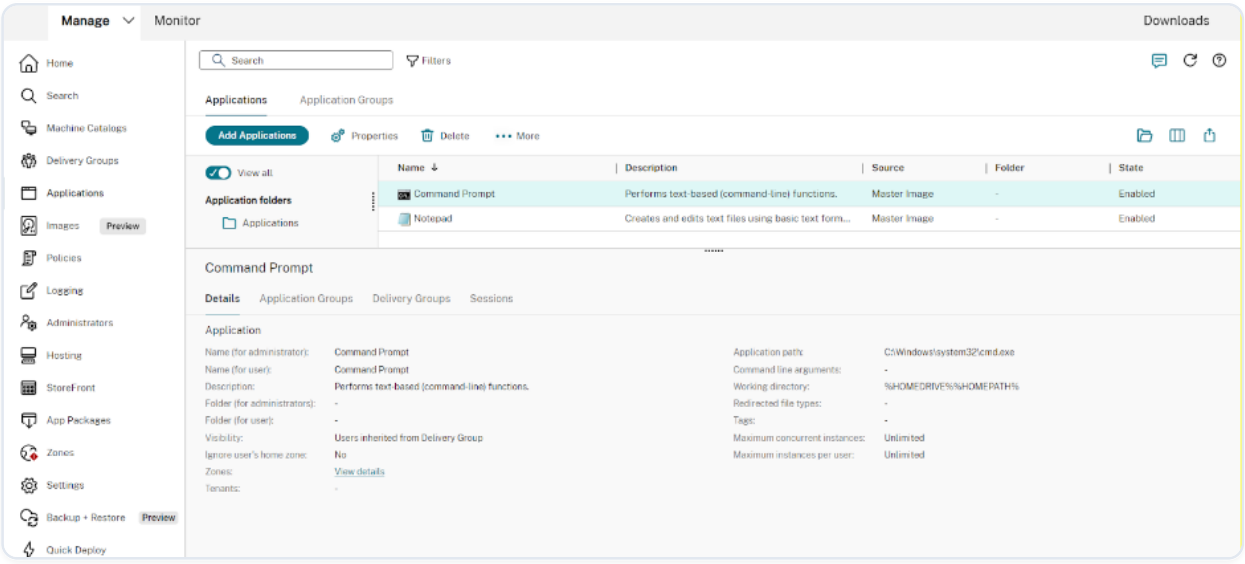
3. 同じドメイン上の別のVM（DC、DDC、または別のVDAでも可）から、`Regedit` を実行し、リモートレジストリに接続します。



4. テスト対象のVDAのIPアドレスを入力し、**OK**をクリックします。`regedit` ツリーには、テスト対象のVDAのブランチが表示されるはずです。



5. **コマンドプロンプト**公開アプリケーションを開きます。



Citrix Workspace に **コマンドプロンプト** アプリが表示されます。

公開アプリのコマンドプロンプト(/en-us/citrix-virtual-apps-desktops/current-release/media/published-app-cmd-prompt.png)

6. クライアントで **Connection Center** を開きます。これは、開いているシームレスアプリを閉じた後にセッションがサインアウトされたときに監視するために使用されます。次の画像では、リモート VDI でコマンドプロンプトプロセス `c:\Windows\system32\cmd.exe` がアクティブになっていることがわかります。

   公開アプリの接続(/en-us/citrix-virtual-apps-desktops/current-release/media/published-app-citrix-workspace-connection-center.png)

7. **regedit** が実行されている VDA から、次のリモート IP の場所に移動します。
   `HKEY_USERS\S-1-X-XX-XXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-XXXX\SOFTWARE\CitrixVolatile\Seamless\Sessions\X\`

> **注:**
>
> 新しいセッションを開くたびにこのパスは変更されます。

8. ここで読み取るキーは 2 つあります (ここでは変更しないでください)。**LogoffCheckBlockingProcess** と **LogoffCheckerBlockingVisibleProcess** です。これらのキーは、サインアウトをブロックしているプログラムを表示します。最初のキーには、それが開いていてまだ閉じられていないため、`C:\Windows\System32\cmd.exe` が表示されているはずです。

   > **注:**
   >
   > **LogoffCheckBlockingProcess** と **LogoffCheckerBlockingVisibleProcess** は手動で編集しないでください。これらのレジストリ値を手動で編集すると、セッションが不安定になる可能性があります。

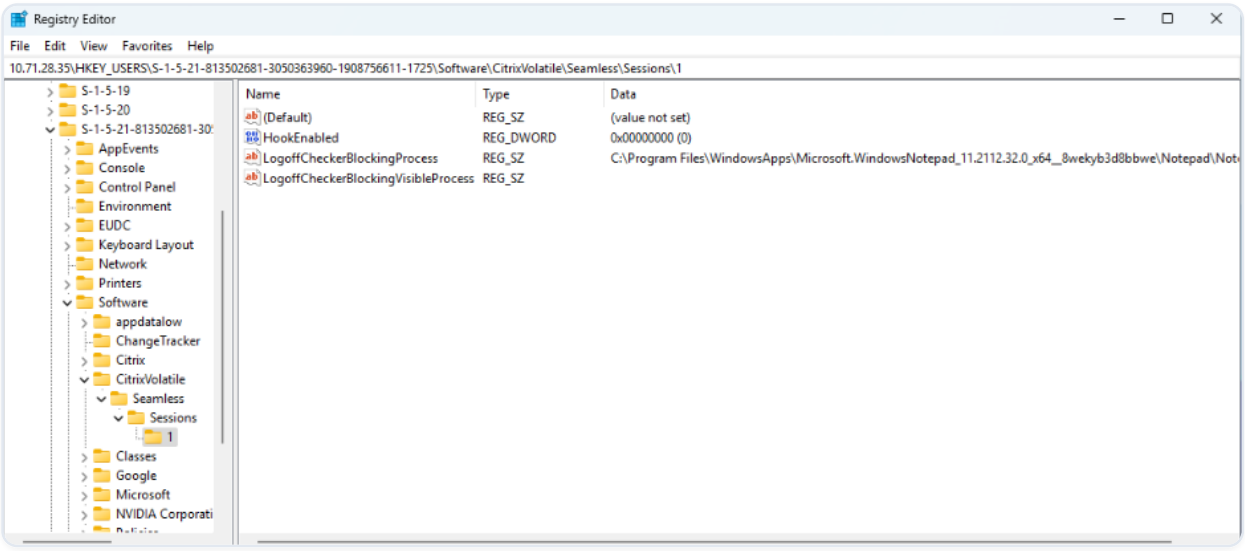
   > 公開アプリ 2(/en-us/citrix-virtual-apps-desktops/current-release/media/published-app-regedit-2.png)

9. 右上隅の **X** をクリックして **Seamless CMD** を終了します。
10. セッションが閉じるかどうか、接続センターを確認します。閉じるまでに最大 30 秒かかる場合があります。閉じれば、正常なサインアウトを妨げたアプリケーションやプロセスはなかったことになります。

    正常なサインアウト(/en-us/citrix-virtual-apps-desktops/current-release/media/published-app-bwd.png)

11. セッションが閉じなかった場合は、F5 キーで **regedit** の出力を更新します。
12. **LogoffCheckBlockingProcess** と **LogoffCheckerBlockingVisibleProcess** の内容を再度確認します。CMD は表示されなくなっているはずですが、別のプロセスが一覧表示されているはずです。現在セッションのサインアウトをブロックしているプロセスがここに表示されているはずです。

    この場合、コマンドプロンプトが閉じられる前に、公開されたコマンドプロンプトから **Notepad.exe** が開かれており、このリモートのメモ帳プロセスが正常なサインアウトを妨げています。



13. この実行可能ファイルへのパスと、それが表示されたキーをメモし、リモートツリーの下にある以下のレジストリキーに入力します。

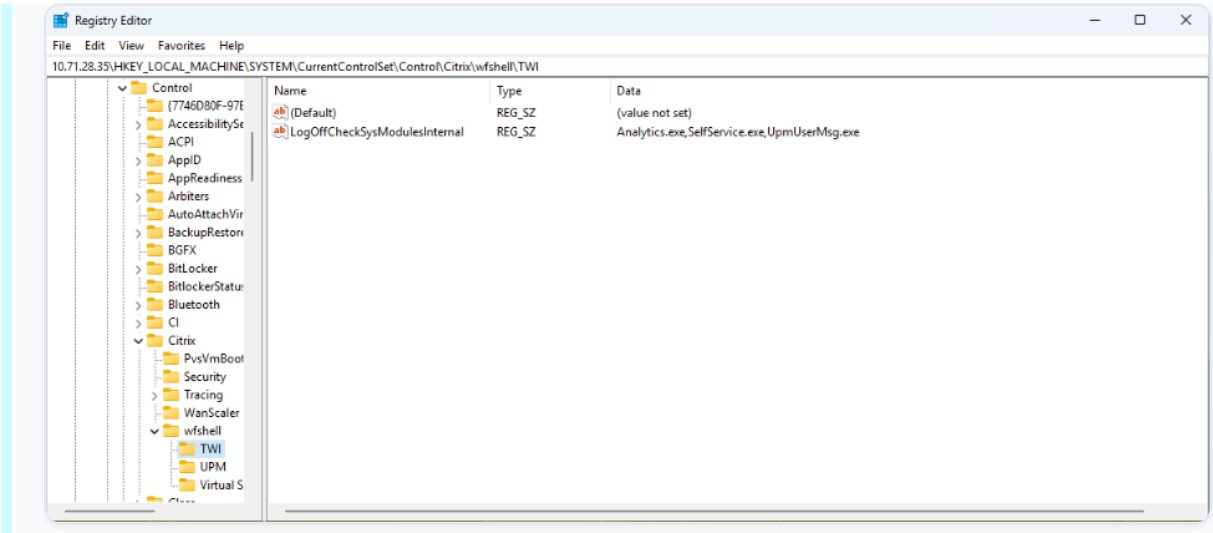
    - **LogoffCheckBlockingProcess** に表示される場合:

      `HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWILogoffCheckSysModulesInterna`

    - **LogoffCheckerBlockingVisibleProcess** に表示される場合:

      `HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWILogoffCheckVisibleSysModules`

> **注:**
>
> キーにすでに1つ以上のエントリがある場合は、末尾にコンマを追加し、そのコンマの後に新しいエントリを配置します。



14. クライアントの接続センターからセッションをサインアウトし、リモートアプリケーションを再度開きます。

15. リモートアプリケーションを閉じてから30秒以内にセッションが自動的にサインアウトされるまで、手順9〜16を繰り返します。

> **注:**
>
> トラブルシューティング後、必要に応じて、リモートレジストリへのアクセスを許可するための一時的なファイアウォールの変更を元に戻します。

公開アプリケーションを開くときにWindowsの免責事項メッセージを全画面表示で見るためにLogonUIを変更する方法

認証パススルーが発生しないシナリオ向けに、**LogonUI**ウィンドウのスケーリングが改善されました。**LogonUI**ウィンドウは、使用されているモニターの解像度とDPI設定に基づいてスケーリングされ、これにより、完全な**LogonUI**ウィンドウがクリッピングなしで表示されることが保証されます。

ピクセル単位のウィンドウサイズは、レジストリで手動で設定することもできます。

1. **ファイル名を指定して実行**コマンドで`regedit`を使用して**レジストリエディター**を開きます。
2. `HKEY_LOCAL_MACHINE\Software\Citrix\CtxHook\AppInit_DLLS\Seamless Hook\`に移動します。
3. 2つの新しいDWORDキー、**LogonUIWidth**と**LogonUIHeight**を作成します。
4. **LogonUI**ウィンドウのキーの値を、必要な幅と高さ（ピクセル単位）に設定します。

   LogonUI ウィンドウのサイズを手動で設定すると、自動スケーリングは無効になります。

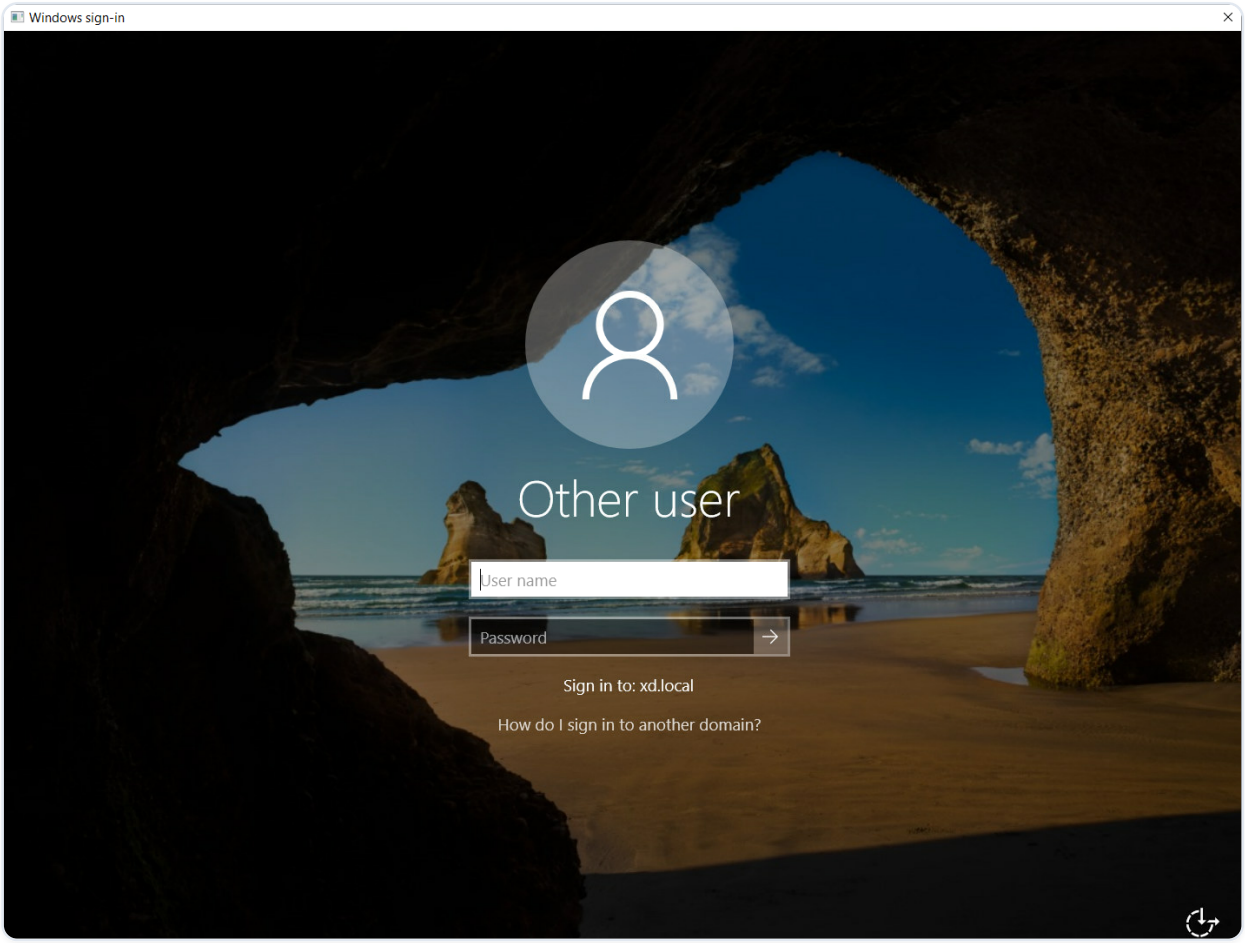
> **注:**
>
> これらのレジストリパスは2407以降変更されました。古いレジストリ値は無視され、非推奨です。

> デフォルトでは、**LogonUI** ウィンドウにはタイトルバーと閉じるボタンが含まれており、必要に応じてエンドユーザーがセッションから切断できるようになっています。

タイルバーを無効にする

LogonUI ウィンドウのタイルバーは、以下のレジストリキーで無効にできます。

1. **ファイル名を指定して実行** コマンドで `regedit` を使用してレジストリエディターを開きます。
2. `HKEY_LOCAL_MACHINE\Software\Citrix\CtxHook\AppInit_DLLS\Seamless Hook\` に移動します。
3. 新しいDWORDキー: **LogonUICaption** を作成し、そのキーの値を `0` に設定します。



アプリケーションフォルダーの管理

デフォルトでは、デリバリーグループに追加する新しいアプリケーションは、**Applications**という名前のフォルダーに配置されます。デリバリーグループの作成時、アプリケーションの追加時、または後で別のフォルダーを指定できます。

知っておくと良いこと:

- Applicationsフォルダーの名前を変更したり削除したりすることはできませんが、その中に含まれるすべてのアプリケーションを、作成した他のフォルダーに移動することはできます。

- フォルダー名には1〜64文字を含めることができます。スペースも使用できます。
- フォルダーは最大5レベルまでネストできます。
- フォルダーにアプリケーションを含める必要はありません。空のフォルダーも許可されます。
- フォルダーは、移動したり、作成時に別の場所を指定したりしない限り、Web Studioでアルファベット順に表示されます。
- 同じ名前のフォルダーを複数持つことができますが、それぞれ異なる親フォルダーを持つ必要があります。同様に、同じ名前のアプリケーションを複数持つことができますが、それぞれ異なるフォルダーに存在する必要があります。
- フォルダー内のアプリケーションを表示するには`View Applications`権限が必要です。また、アプリケーションを含むフォルダーを削除、名前変更、または削除するには、そのフォルダー内のすべてのアプリケーションに対して`Edit Application Properties`権限が必要です。
- 以下のほとんどの手順では、Web Studio のアクションバーを使用してアクションを要求します。または、右クリックメニューを使用するか、項目をドラッグすることもできます。たとえば、意図しない場所にフォルダーを作成または移動した場合、ドラッグアンドドロップで正しい場所に移動できます。
- Web Studioのすべてのノード（**マシンカタログ**、**デリバリーグループ**、**アプリケーション**、**アプリケーショングループ**など）は、バックエンドで同じフォルダーツリーを共有します。フォルダーの名前変更または移動時に名前の競合を避けるため、異なるノード間で最上位フォルダーに一意の名前を使用してください。

  `New-BrokerAdminFolder` SDK コマンドレットを使用してフォルダーを作成し、それを**アプリケーション**ノードの下に表示させたい場合は、`Set-BrokerAdminFolderMetadata`コマンドレットを使用して`ContainsApplications`メタデータを追加する必要があります。

  例:

  ```
  Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
  ContainsApplications -Value true
  ```

アプリケーションフォルダーを管理するには、左ペインで**アプリケーション**を選択します。以下のリストを参考にしてください。

- **すべてのフォルダー（ネストされたフォルダーを除く）を表示するには：** フォルダーリストの上にある**すべて表示**をクリックします。

- **最上位レベル（ネストされていない）にフォルダーを作成するには：** **アプリケーション**フォルダーを選択します。新しいフォルダーを**アプリケーション**以外の既存のフォルダーの下に配置するには、そのフォルダーを選択します。次に、アクションバーで**フォルダーの作成**を選択します。名前を入力します。
- **フォルダーを移動するには：** フォルダーを選択し、アクションバーで**フォルダーの移動**を選択します。ネストされたフォルダーが含まれていない限り、一度に1つのフォルダーしか移動できません。（フォルダーを移動する最も簡単な方法は、ドラッグすることです。）
- **フォルダーの名前を変更するには：** フォルダーを選択し、アクションバーで**フォルダー名の変更**を選択します。名前を入力します。
- **フォルダーを削除するには：** フォルダーを選択し、アクションバーで**フォルダーの削除**を選択します。アプリケーションや他のフォルダーを含むフォルダーを削除すると、それらのオブジェクトも削除されます。アプリケーションを削除すると、デリバリーグループからのアプリケーション割り当てが削除されます。マシンからは削除されません。
- **アプリケーションをフォルダーに移動するには：** 1つまたは複数のアプリケーションを選択します。次に、アクションバーで**アプリケーションの移動**を選択します。フォルダーを選択します。

デリバリーグループまたはアプリケーショングループを作成する際に、**アプリケーション**ページで追加するアプリケーションをフォルダーに配置することもできます。デフォルトでは、追加されたアプリケーションは**アプリケーション**フォルダーに入ります。**変更**をクリックしてフォルダーを選択または作成します。

公開デスクトップでのアプリケーションのローカル起動を制御する

ユーザーが公開デスクトップ内から公開アプリケーションを起動する際、そのデスクトップセッションでアプリケーションを起動するか、公開アプリケーションとして起動するかを制御できます。Citrix Workspaceアプリは、VDA上のWindowsレジストリでアプリケーションのインストールパスを検索し、存在する場合はアプリケーションのローカルインスタンスを起動します。それ以外の場合は、ホストされたアプリケーションのインスタンスが起動されます。VDAにインストールされていないアプリケーションを起動すると、ホストされたアプリケーションが起動されます。詳細については、「vPrefer起動」を参照してください。

PowerShell（Citrix Cloud展開環境ではRemote PowerShell SDK、オンプレミス展開環境ではPowerShell SDKを使用）で、このアクションを変更できます。

`New-Broker` Applicationまたは`Set-BrokerApplication` コマンドレットで、`LocalLaunchDisabled` オプションを使用します。例：

```
Set-BrokerApplication -LocalLaunchDisabled <Boolean>
```

デフォルトでは、このオプションの値はfalse（`-LocalLaunchDisabled $false`）です。公開デスクトップ内から公開アプリケーションを起動すると、そのデスクトップセッション内でアプリケーションが起動されます。

オプションの値をtrue（`-LocalLaunchDisabled $true`）に設定すると、公開アプリケーションが起動されます。これにより、公開デスクトップから公開アプリケーションへの個別の追加セッションが（Citrix Workspaceアプリ for Windowsを使用して）作成されます。

要件と制限：

- アプリケーションの`ApplicationType`の値は`HostedOnDesktop`である必要があります。
- このオプションは、適切なPowerShell SDKを介してのみ利用可能です。現在、Web Studioのグラフィカルインターフェイスでは利用できません。
- このオプションには、StoreFront 3.14、Citrix Receiver for Windows 4.11、およびDelivery Controller 7.17が最低限必要です。

アプリケーショングループ

> **注:**
>
> バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

はじめに

アプリケーショングループを使用すると、アプリケーションのコレクションを管理できます。異なるデリバリーグループ間で共有されるアプリケーション、またはデリバリーグループ内のユーザーのサブセットによって使用されるアプリケーションに対してアプリケーショングループを作成します。アプリケーショングループはオプションであり、同じアプリケーションを複数のデリバリーグループに追加する代替手段を提供します。デリバリーグループを複数のアプリケーショングループに関連付けたり、アプリケーショングループを複数のデリバリーグループに関連付けたりできます。

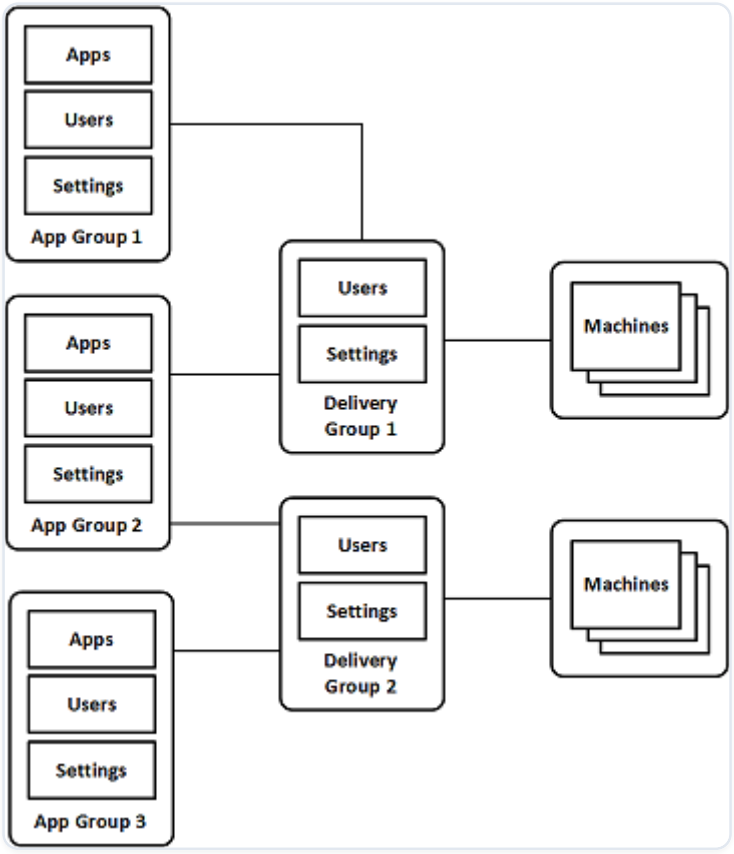
アプリケーショングループを使用すると、より多くのデリバリーグループを使用する場合と比較して、アプリケーション管理とリソース制御の利点が得られます。

- アプリケーションとその設定を論理的にグループ化することで、それらのアプリケーションを単一の単位として管理できます。たとえば、同じアプリケーションを個々のデリバリーグループに1つずつ追加（公開）する必要はありません。
- アプリケーショングループ間のセッション共有は、リソース消費を節約できます。それ以外の場合、アプリケーショングループ間のセッション共有を無効にすることが有益な場合もあります。
- タグ制限機能を使用すると、選択したデリバリーグループ内のマシンのサブセットのみを考慮して、アプリケーショングループからアプリケーションを公開できます。タグ制限を使用すると、既存のマシンを複数の公開タスクに使用できるため、追加のマシンの展開と管理に関連するコストを節約できます。タグ制限は、デリバリーグループ内のマシンを細分化（またはパーティション分割）するものと考えることができます。タグ制限付きのアプリケーショングループまたはデスクトップを使用すると、デリバリーグループ内のマシンのサブセットを分離してトラブルシューティングする際に役立ちます。

構成例

例 1:

次のグラフィックは、アプリケーショングループを含むCitrix Virtual Apps and Desktops™展開を示しています。



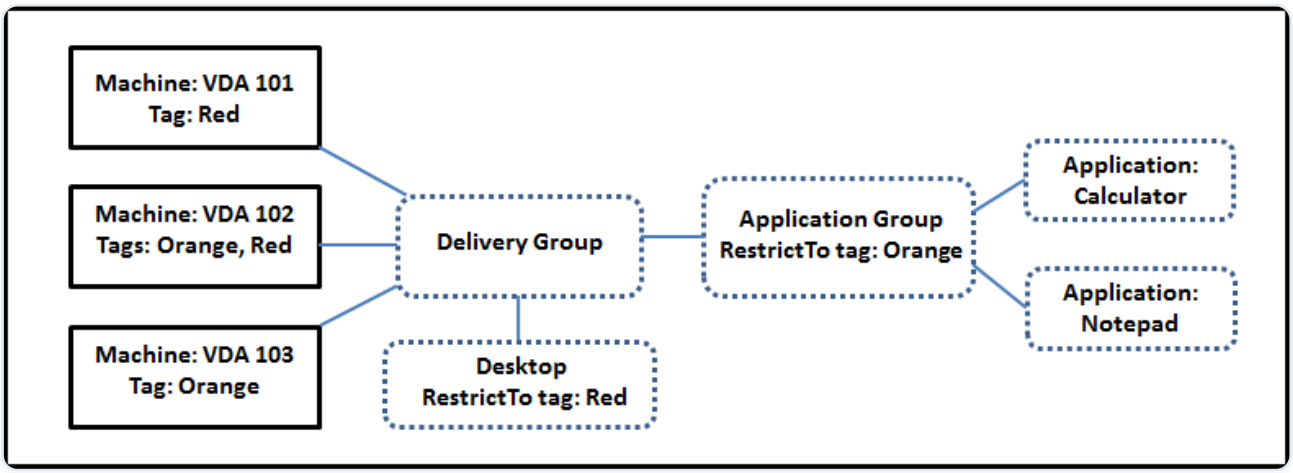
この構成では、アプリケーションはデリバリーグループではなくアプリケーショングループに追加されます。デリバリーグループは、どのマシンが使用されるかを指定します。（図には示されていませんが、マシンはマシンカタログ内にあります。）

アプリケーショングループ1はデリバリーグループ1に関連付けられています。アプリケーショングループ1で指定されたユーザーがアプリケーショングループ1のアプリケーションにアクセスします。これらのグループは、デリバリーグループ1のユーザーリストにも含まれている場合にのみ表示されます。この構成は、アプリケーショングループのユーザーリストが、関連付けられたデリバリーグループのユーザーリストのサブセット（制限）であるというガイダンスに従います。アプリケーショングループ1の設定（アプリケーショングループ間のアプリケーションセッション共有、関連付けられたデリバリーグループなど）は、そのグループ内のアプリケーションとユーザーに適用されます。デリバリーグループ1の設定は、アプリケーショングループ1と2のユーザーに適用されます。これは、これらのアプリケーショングループがそのデリバリーグループに関連付けられているためです。

アプリケーショングループ2は、2つのデリバリーグループ（1と2）に関連付けられています。これらの各デリバリーグループには、アプリケーショングループ2で優先度が割り当てられ、アプリケーションが起動されるときにデリバリーグループがチェックされる順序を示します。優先度が等しいデリバリーグループはロードバランスされます。アプリケーショングループ2で指定されたユーザーがアプリケーショングループ2のアプリケーションにアクセスします。ただし、それらのユーザーはデリバリーグループ1とデリバリーグループ2のユーザーリストにも含まれている必要があります。

例 2:

このシンプルなレイアウトでは、タグ制限を使用して、特定のデスクトップおよびアプリケーションの起動に考慮されるマシンを制限します。このサイトには、1つの共有デリバリーグループ、1つの公開デスクトップ、および2つのアプリケーションで構成された1つのアプリケーショングループがあります。



3台のマシン（VDA 101～103）のそれぞれにタグが追加されています。

アプリケーショングループは「Orange」タグ制限付きで作成されました。その各アプリケーションは、そのデリバリーグループ内で「Orange」タグを持つマシン（VDA 102および103）でのみ起動されます。

アプリケーショングループ（およびデスクトップ）でタグ制限を使用するためのより包括的な例とガイダンスについては、「タグ」を参照してください。

ガイダンスと考慮事項

Citrixでは、アプリケーションをアプリケーショングループまたはデリバリーグループのいずれかに追加することをお勧めします。両方に追加することはお勧めしません。そうしないと、2種類のグループにアプリケーションが存在することで複雑さが増し、管理が難しくなる可能性があります。

デフォルトでは、アプリケーショングループは有効になっています。アプリケーショングループを作成した後、グループを編集してこの設定を変更できます。「アプリケーショングループの管理」を参照してください。

デフォルトでは、アプリケーショングループ間のアプリケーションセッション共有は有効になっています。「アプリケーショングループ間のセッション共有」を参照してください。

Citrixでは、デリバリーグループを現在のバージョンにアップグレードすることをお勧めします。このプロセスには、次のものが必要です。

1. デリバリーグループで使用されているマシン上のVDAをアップグレードする。
2. それらのマシンを含むマシンカタログのアップグレード。
3. デリバリーグループのアップグレード。

詳細については、「デリバリーグループの管理」を参照してください。

アプリケーショングループを使用するには、コアコンポーネントが最小バージョン7.9である必要があります。

アプリケーショングループを作成するには、Delivery Group Administrator の組み込みロールの委任管理権限が必要です。詳細については、「委任管理」(/ja-jp/citrix-virtual-apps-desktops/current-release/manage-deployment/delegated-administration.html) を参照してください。

この記事では、アプリケーションを複数のアプリケーショングループに「関連付ける」ことについて言及しています。これは、利用可能なソースからそのアプリケーションのインスタンスを追加

する操作とは区別されます。同様に、デリバリーグループは、互いの追加やコンポーネントではなく、アプリケーショングループに関連付けられます。

アプリケーショングループとのセッション共有

アプリケーションセッション共有が有効になっている場合、すべてのアプリケーションは同じアプリケーションセッションで起動します。これにより、より多くのアプリケーションセッションを起動するコストが削減され、コピー＆ペースト操作など、クリップボードを使用するアプリケーション機能の使用が可能になります。ただし、状況によってはセッション共有をクリアできます。

アプリケーショングループを使用する場合、デリバリーグループのみを使用する場合に利用できる標準のセッション共有動作を拡張する、次の3つの方法でアプリケーションセッション共有を構成できます。

- アプリケーショングループ間でセッション共有が有効。
- 同じアプリケーショングループ内のアプリケーション間でのみセッション共有が有効。
- セッション共有が無効。

アプリケーショングループ間のセッション共有

アプリケーショングループ間でアプリケーションセッション共有を有効にすることも、または、同じアプリケーショングループ内のアプリケーションにのみアプリケーションセッション共有を制限するために無効にすることもできます。

- **アプリケーショングループ間のセッション共有を有効にすることが役立つ例:**

  アプリケーショングループ1にはWordやExcelなどのMicrosoft Officeアプリケーションが含まれています。アプリケーショングループ2にはメモ帳や電卓などの他のアプリケーションが含まれており、両方のアプリケーショングループが同じデリバリーグループに接続されています。両方のアプリケーショングループにアクセスできるユーザーがWordを起動してアプリケーションセッションを開始し、次にメモ帳を起動します。コントローラーが、ユーザーの既存のWordを実行しているセッションがメモ帳の実行に適していると判断した場合、メモ帳は既存のセッション内で起動されます。既存のセッションからメモ帳を実行できない場合（たとえば、タグ制限によってセッションが実行されているマシンが除外される場合など）、セッション共有を使用するのではなく、適切なマシン上に新しいセッションが作成されます。

- **アプリケーショングループ間のセッション共有を無効にすることが役立つ例:**

  同じマシンにインストールされている他のアプリケーションとうまく相互運用できない一連のアプリケーションの構成。たとえば、同じソフトウェアスイートの2つの異なるバージョン

や、同じWebブラウザーの2つの異なるバージョンなどです。ユーザーが同じセッションで両方のバージョンを起動することを許可しないようにしたい場合。

ソフトウェアスイートのバージョンごとにアプリケーショングループを作成し、各バージョンのソフトウェアスイートのアプリケーションを対応するアプリケーショングループに追加します。これらのアプリケーショングループのそれぞれでグループ間のセッション共有が無効になっている場合、それらのグループで指定されたユーザーは、同じバージョンのアプリケーションを同じセッションで実行できます。ユーザーは同時に他のアプリケーションを実行できますが、同じセッションでは実行できません。異なるバージョンのアプリケーション、またはアプリケーショングループに含まれていないアプリケーションを起動すると、そのアプリケーションは新しいセッションで起動されます。

このアプリケーショングループ間のセッション共有機能は、セキュリティサンドボックス機能ではありません。これは完璧ではなく、ユーザーが他の手段（例えば、Windows Explorer経由など）でセッションにアプリケーションを起動するのを防ぐことはできません。

マシンが容量に達している場合、新しいセッションはそのマシンでは開始されません。必要に応じて、セッション共有を使用して、新しいアプリケーションがそのマシンの既存のセッションで開始されます。

アプリケーションセッション共有が許可されているアプリケーショングループに対してのみ、事前起動セッションを利用可能にできます。（セッションリンガー機能を使用するセッションは、すべてのアプリケーショングループで利用可能です。）これらの機能は、アプリケーショングループに関連付けられている各デリバリーグループで有効にして構成する必要があります。アプリケーショングループ内でこれらを構成することはできません。

デフォルトでは、アプリケーショングループを作成する際に、アプリケーショングループ間のアプリケーションセッション共有が有効になります。グループ作成時にこれを変更することはできません。アプリケーショングループを作成した後、グループを編集してこの設定を変更できます。アプリケーショングループの管理を参照してください。

アプリケーショングループ内でのセッション共有を無効にする

同じアプリケーショングループ内のアプリケーション間でのアプリケーションセッション共有を防ぐことができます。

- **アプリケーショングループ内でのセッション共有を無効にすることが役立つ例:**

  ユーザーに、別々のモニターでアプリケーションの複数の同時フルスクリーンセッションにアクセスさせたい場合。

  アプリケーショングループを作成し、そこにアプリケーションを追加します。

デフォルトでは、アプリケーショングループを作成すると、アプリケーションセッション共有が有効になります。グループの作成時にこの設定を変更することはできません。アプリケーショングループを作成した後、グループを編集してこの設定を変更できます。「アプリケーショングループの管理」を参照してください。

アプリケーショングループを作成する

アプリケーショングループを作成するには：

1. Web Studioにサインインします。
2. 左ペインで**アプリケーション**を選択し、**アプリケーショングループ**タブを選択します。
3. フォルダーを使用してアプリケーショングループを整理するには、**アプリケーショングループ**ルートフォルダーの下にフォルダーを作成します。詳細については、フォルダーを使用してアプリケーショングループを整理するを参照してください。
4. グループを作成するフォルダーを選択し、**アプリケーション グループの作成**をクリックします。グループ作成ウィザードが**はじめに**ページで起動します。このページは、今後のウィザード起動時に表示しないように設定できます。
5. ウィザードに従って、以下に説明するページで設定を構成します。各ページでの作業が完了したら、**次へ**を選択して**概要**ページに進みます。

手順1. デリバリーグループ

デリバリーグループページには、すべてのデリバリーグループと、各グループに含まれるマシンの数が一覧表示されます。

- 「**互換性のあるデリバリーグループ**」リストには、選択可能なデリバリーグループが含まれています。互換性のあるデリバリーグループには、ランダムな（永続的または静的に割り当てられていない）マルチセッションまたはシングルセッションOSマシンが含まれます。
- 「**互換性のないデリバリーグループ**」リストには、選択できないデリバリーグループが含まれています。各エントリには、静的に割り当てられたマシンが含まれるなど、互換性がない理由が説明されています。

アプリケーショングループは、アプリケーションを配信できる共有（プライベートではない）マシンを含むデリバリーグループに関連付けることができます。

以下の両方の条件が満たされている場合、デスクトップのみを配信する共有マシンを含むデリバリーグループを選択することもできます。

- デリバリーグループに共有マシンが含まれており、XenDesktopバージョン7.9より前のバージョンで作成されていること。

- デリバリーグループの編集権限があること。

アプリケーショングループ作成ウィザードがコミットされると、デリバリーグループの種類は自動的に「デスクトップとアプリケーション」に変換されます。

関連付けられたデリバリーグループがないアプリケーショングループを作成することはできますが（アプリケーションを整理するため、または現在使用されていないアプリケーションのストレージとして機能させるためなど）、少なくとも1つのデリバリーグループが指定されるまで、そのアプリケーショングループをアプリケーションの配信に使用することはできません。また、デリバリーグループが指定されていない場合、「**スタートから**」メニューソースからアプリケーショングループにアプリケーションを追加することはできません。

選択したデリバリーグループは、アプリケーションの配信に使用されるマシンを指定します。アプリケーショングループに関連付けるデリバリーグループの横にあるチェックボックスをオンにします。

タグ制限を追加するには、**タグを持つマシンへの起動を制限する**を選択し、ドロップダウンリストからタグを選択します。

手順2. ユーザー

アプリケーショングループでアプリケーションユーザーを指定します。前のページで選択したデリバリーグループ内のすべてのユーザーとユーザーグループを許可するか、それらのデリバリーグループから特定のユーザーとユーザーグループを選択します。指定されたユーザーに利用を制限する場合、デリバリーグループで指定されたユーザーのうち、アプリケーショングループで指定されたユーザーのみが、このグループのアプリケーションにアクセスできます。基本的に、アプリケーショングループのユーザーリストは、デリバリーグループのユーザーリストに対するフィルターとして機能します。

認証されていないユーザーによるアプリケーションの使用の有効化または無効化は、アプリケーショングループではなく、デリバリーグループでのみ利用できます。

展開でユーザーリストが指定される場所については、「ユーザーリストが指定される場所」を参照してください。

ステップ3. アプリケーション

知っておくと良いこと:

- デフォルトでは、追加する新しいアプリケーションは「**Applications**」という名前のフォルダーに配置されます。別のフォルダーを指定できます。アプリケーションを追加しようとしたときに、そのフォルダーに同じ名前のアプリケーションが存在する場合、追加しようとしてい

るアプリケーションの名前を変更するよう求められます。提案された一意の名前に同意すると、その新しい名前でアプリケーションが追加されます。そうでない場合は、追加する前に自分で名前を変更する必要があります。詳細については、「アプリケーションフォルダーの管理」を参照してください。

- アプリケーションのプロパティ（設定）は、追加時または後で変更できます。「アプリケーションプロパティの変更」を参照してください。同じ名前の2つのアプリケーションを同じユーザーに公開する場合、Web Studioで「**アプリケーション名（ユーザー向け）**」プロパティを変更します。そうしないと、ユーザーはCitrix Workspaceアプリで重複する名前を目にします。
- アプリケーションを複数のアプリケーショングループに追加する場合、それらのすべてのグループでアプリケーションを表示するのに十分な権限がないと、表示の問題が発生する可能性があります。そのような場合は、より高い権限を持つ管理者に相談するか、アプリケーションが追加されたすべてのグループを含むようにスコープを拡張してください。

アプリケーションソースを表示するには、ドロップダウンメニューから「**追加**」をクリックします。

- **スタートメニューから**：選択したデリバリーグループ内のマシンで検出されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストが表示された新しいページが起動します。追加するアプリケーションのチェックボックスをオンにして、「**OK**」をクリックします。

  以下のいずれかを選択した場合、このソースは選択できません。

  - 関連付けられたデリバリーグループがないアプリケーショングループ。
  - 関連付けられたデリバリーグループにマシンが含まれていないアプリケーショングループ。
  - マシンが含まれていないデリバリーグループ。

- **手動で定義**：サイト内またはネットワーク内の別の場所にあるアプリケーション。このソースを選択すると、実行可能ファイルへのパス、作業ディレクトリ、オプションのコマンドライン引数、管理者とユーザーの表示名を入力する新しいページが起動します。この情報を入力したら、「**OK**」をクリックします。
- **既存**：以前にサイトに追加されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストが表示された新しいページが起動します。追加するアプリケーションのチェックボックスをオンにして、「**OK**」をクリックします。サイトにアプリケーションがない場合、このソースは選択できません。

- **App-V**：App-Vパッケージ内のアプリケーション。このソースを選択すると、**App-Vサーバー**または**アプリケーションライブラリ**を選択する新しいページが起動します。表示された画面から、追加するアプリケーションのチェックボックスをオンにして、「**OK**」をクリックします。詳細については、「App-Vアプリケーションの展開と配信」を参照してください。サイトでApp-Vが構成されていない場合、このソースは選択できません（または表示されない場合があります）。

記載されているように、「**追加**」ドロップダウンメニューの一部のエントリは、その種類の有効なソースがない場合、選択できません。互換性のないソースはまったく表示されません（たとえば、アプリケーショングループにアプリケーショングループを追加することはできないため、アプリケーショングループを作成するときにそのソースは表示されません）。

ステップ4. スコープ

このページは、以前にカスタムスコープを作成した場合にのみ表示されます。デフォルトでは、**すべて**のスコープが選択されています。詳細については、委任管理を参照してください。

ステップ5. 概要

アプリケーショングループの名前を入力します。説明を（オプションで）入力することもできます。

概要情報を確認し、**「完了」**をクリックします。

公開コンテンツ

> **注:**
>
> バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

Microsoft WordドキュメントやWebリンクなど、リソースへのURLまたはUNCパスであるアプリケーションを公開できます。この機能は「公開コンテンツ」として知られています。コンテンツを公開する機能により、ユーザーへのコンテンツ配信方法に柔軟性が加わります。既存のアクセス制御とアプリケーション管理の恩恵を受けることができます。また、コンテ

> ンツを開くためにローカルアプリケーションを使用するか、公開アプリケーションを使用するかを指定することもできます。

公開されたコンテンツは、StoreFront™およびCitrix Workspace™アプリの他のアプリケーションと同様に表示されます。ユーザーはアプリケーションにアクセスするのと同じ方法でアクセスします。クライアントでは、リソースは通常どおり開きます。

- ローカルにインストールされたアプリケーションが適切な場合、そのアプリケーションが起動されてリソースが開かれます。
- ファイルの種類に関連付けが定義されている場合、公開されたアプリケーションが起動されてリソースが開かれます。

コンテンツはPowerShell SDKを使用して公開します。Web Studioを使用してコンテンツを公開することはできません。ただし、公開後にWeb Studioを使用してアプリケーションのプロパティを編集することはできます。

構成の概要と準備

コンテンツの公開には、次の主要なプロパティを持つ `New-BrokerApplication` コマンドレットを使用します。（すべてのコマンドレットプロパティの説明については、コマンドレットのヘルプを参照してください。）

```
New-BrokerApplication –ApplicationType PublishedContent
-CommandLineExecutable location -Name app-name -DesktopGroup delivery-
group-name
```

`ApplicationType` プロパティは `PublishedContent` である必要があります。

`CommandLineExecutable` プロパティは、公開コンテンツの場所を指定します。以下の形式がサポートされており、255文字の制限があります。

- HTMLウェブサイトアドレス（例: `<http://www.citrix.com>`）
- ウェブサーバー上のドキュメントファイル（例: `https://www.citrix.com/press/pressrelease.doc`）
- FTPサーバー上のディレクトリ（例: `ftp://ftp.citrix.com/code`）
- FTPサーバー上のドキュメントファイル（例: `ftp://ftp.citrix.com/code/Readme.txt` >）
- UNC ディレクトリパス (例: `file://myServer/myShare or \\\\myServer\\myShare`)

- UNC ファイルパス (例: `file://myServer/myShare/myFile.asf` または `\\myServer\myShare\myFile.asf`)

正しいSDKがあることを確認してください。

- Citrix DaaS (旧Citrix Virtual Apps and Desktopsサービス) の展開の場合、ダウンロード して、Citrix Virtual Apps and Desktops Remote PowerShell SDKをインストールします。
- オンプレミスのCitrix Virtual Apps and Desktops展開の場合、Delivery Controllerとともにインストールされているの PowerShell SDKを使用します。公開コンテンツアプリケーションを追加するには、最低バージョン7.11のDelivery Controllerが必要です。

以下の手順では例を使用します。例では、次のようになります:

- マシンカタログが作成されています。
- `PublishedContentApps` という名前のデリバリーグループが作成されています。このグループは、カタログからマルチセッションOSマシンを使用します。WordPadアプリケーションがグループに追加されています。
- デリバリーグループ名、`CommandLineExecutable` の場所、およびアプリケーション名が割り当てられます。

はじめに

PowerShell SDKを含むマシンで、PowerShellを開きます。

次のコマンドレットは、適切なPowerShell SDKスナップインを追加し、返されたデリバリーグループレコードを割り当てます。

`Add-PsSnapin Citrix* $dg = Get-BrokerDesktopGroup –Name PublishedContentApps`

Citrix DaaSを使用している場合は、Citrix Cloud™の資格情報を入力して認証します。複数の顧客がいる場合は、1つを選択します。

URLを公開する

場所とアプリケーション名を割り当てた後、次のコマンドレットは、Citrixのホームページをアプリケーションとして公開します。

```
$citrixUrl = "https://www.citrix.com/"

$appName = "Citrix Home Page"
```

```
New-BrokerApplication –ApplicationType PublishedContent –
CommandLineExecutable $citrixURL –Name $appName –DesktopGroup $dg.Uid
```

成功を確認します:

- StoreFrontを開き、PublishedContentAppsデリバリーグループ内のアプリケーションにアクセスできるユーザーとしてログオンします。デフォルトのアイコンを持つ新しく作成されたアプリケーションが表示されます。アイコンのカスタマイズについては、`<https://www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-xd7/>`を参照してください。
- **Citrix Home Page**アプリケーションをクリックします。URLは、ローカルで実行されているデフォルトブラウザの新しいタブで起動します。

UNCパスにあるリソースを公開する

この例では、管理者は`PublishedResources`という名前の共有をすでに作成しています。場所とアプリケーション名を割り当てた後、以下のコマンドレットはその共有内のRTFファイルとDOCXファイルをリソースとして公開します。

```
$rtfUNC = "\\GMSXJ-EDGE0.xd.local\\PublishedResources\\PublishedRTF.rtf"

$rtfAppName = "PublishedRTF"



New-BrokerApplication –ApplicationType PublishedContent

–CommandLineExecutable $rtfUNC -Name $rtfAppName

-DesktopGroup $dg.Uid



$docxUNC = "\\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedDOCX.docx"

$docxAppName = "PublishedDOCX"
```

```
New-BrokerApplication –ApplicationType PublishedContent

–CommandLineExecutable $docxUNC -Name $docxAppName

-DesktopGroup $dg.Uid
```

成功を確認します:

- StoreFrontウィンドウを更新して、新しく公開されたドキュメントを表示します。
- **PublishedRTF**および**PublishedDOCX**アプリケーションをクリックします。各ドキュメントは、ローカルで実行されているWordPadで開きます。

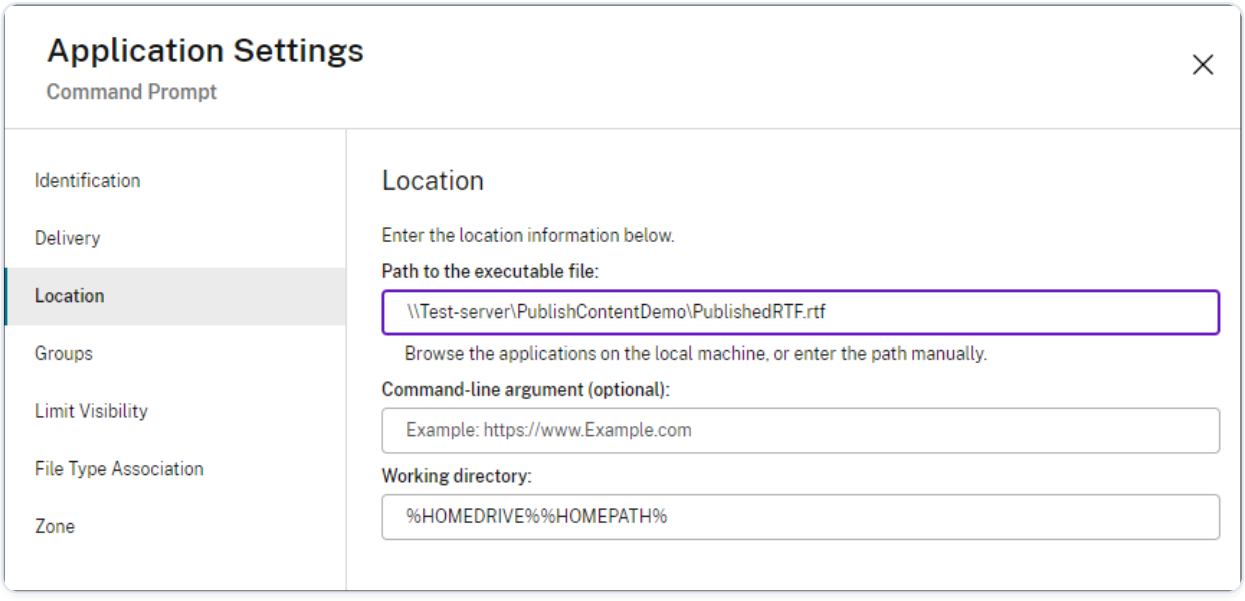
PublishedContentアプリケーションの表示と編集

公開されたコンテンツは、他のアプリケーションタイプに使用するのと同じ方法で管理します。

`PublishedContent`アプリケーションを表示および編集するには、次の手順に従います。

1. Web Studioにサインインし、左側のペインで**アプリケーション**を選択します。
2. **アプリケーション**タブで、PublishedContentアプリケーションを選択し、**プロパティ**を選択します。

   アプリケーションのプロパティ（ユーザーの可視性、グループの関連付け、ショートカットなど）は、公開されたコンテンツに適用されます。ただし、**場所**ページでは、コマンドライン引数または作業ディレクトリのプロパティを変更することはできません。
3. リソースを変更するには、そのページの**実行可能ファイルへのパス**フィールドを変更します。



4. 公開アプリケーションを使用して`PublishedContent`アプリケーション（ローカルアプリケーションではなく）を開くには、次の手順に従います。

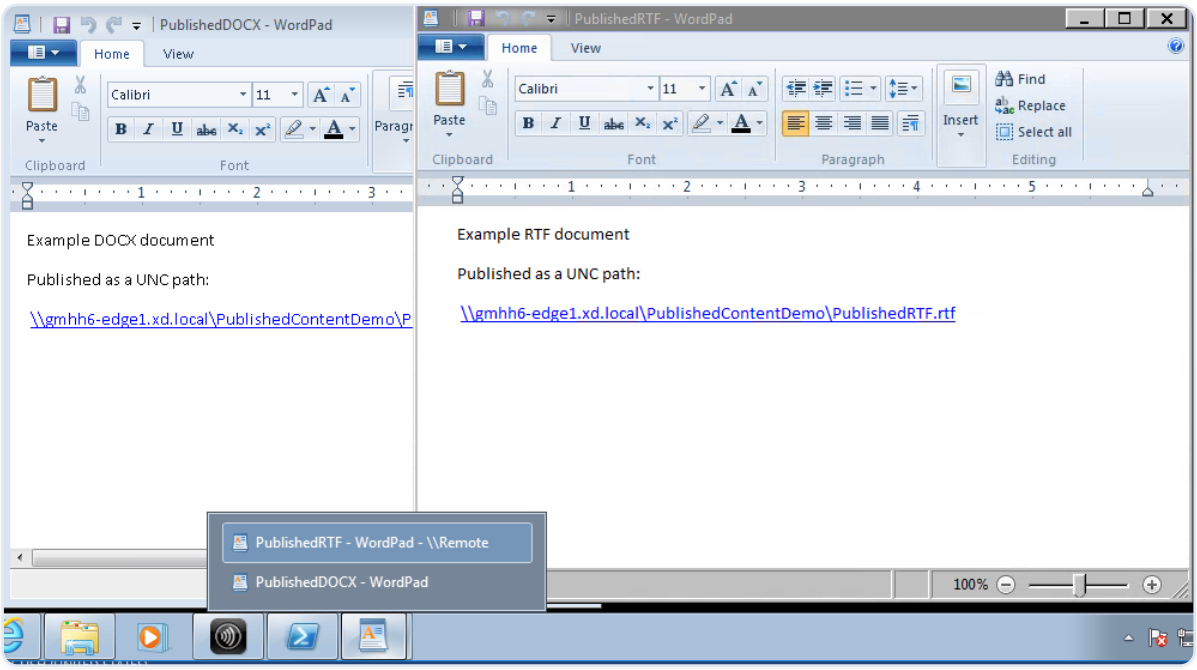
   この例では、公開されたWordPadアプリケーションが編集され、.rtfファイル用のファイルタイプ関連付けが作成されます。

   a. デリバリーグループのメンテナンスモードをオンにします。

   b. **ファイルタイプ関連付け**プロパティを編集します。

   c. 完了したら、メンテナンスモードをオフにします。

   d. StoreFrontを更新してファイルタイプ関連付けの変更を読み込み、**PublishedRTF**および**PublishedDOCX**アプリケーションをクリックします。違いに注目してください。**PublishedDOCX**は引き続きローカルのWordPadで開きます。しかし、**PublishedRTF**はファイルタイプ関連付けにより、公開されたWordPadで開くようになりました。



詳細情報

- マシンカタログの作成
- 「デリバリーグループの作成」(/ja-jp/citrix-virtual-apps-desktops/current-release/install-configure/delivery-groups-create.html)
- アプリケーションプロパティの変更

アプリパッケージ

アプリパッケージは、Citrix® が管理する事前構成されたアプリケーション展開です。これにより、アプリケーションを仮想化できます。これは、アプリケーションがユーザーデバイスのオペレーティングシステムやインターフェイスから独立して実行されることを意味します。

アプリパッケージは、アプリケーション管理を簡素化し、ITのオーバーヘッドを削減し、アプリケーションがライフサイクル全体を通じて安全かつ機能的であることを保証します。

Citrix は、ユーザーにアプリケーションを配信するために、以下のパッケージングテクノロジーをサポートしています。

- App-V アプリケーション
- MSIX および MSIX app attach アプリケーション
- FlexApp アプリケーション
- Elastic App アプリケーション
- Cloudpaging アプリケーション

この記事では、Citrix Virtual Apps and Desktops™ 環境でこれらのパッケージ化されたアプリケーションを展開および配信する方法について説明します。

> **注:**
>
> - バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™ の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。
> - アプリケーションパッケージの展開と配信に Web Studio と Citrix Studio を相互に利用することはお勧めしません。それぞれ異なるメカニズムを使用しているため、App-V サーバーの情報が一方では正しく表示されるが、もう一方では表示されないといった不一致が生じる可能性があります。また、Citrix Studio は App-V のみをサポートしていることに注意してください。

App-V アプリケーション

Application Virtualization (App-V) は、エンドユーザーのデバイスにインストールすることなく、アプリケーションをストリーミングしてアクセスできるようにする Microsoft のテクノロジーです。Citrix Virtual Apps and Desktops は App-V を使用してアプリケーションを配信でき、さまざまなクライアントマシン間でアプリケーションを管理するための集中化された効率的な方法を提供します。

App-V パッケージアプリケーションを配信する際に操作するコンポーネントと概念の詳細については、Microsoft のドキュメント「Application Virtualization (App-V) for Windows client overview」を参照してください。

重要な用語

- **管理サーバー**: App-V インフラストラクチャを管理するための一元化されたコンソールを提供し、App-V デスクトップクライアントとリモートデスクトップサービスクライアントの両方に仮想アプリケーションを配信します。App-V 管理サーバーは、管理者に必要なセキュリティ、測定、監視、およびデータ収集を認証、要求、提供します。このサーバーは、Active Directory とサポートツールを使用してユーザーとアプリケーションを管理します。
- **パブリッシングサーバー**: 特定のユーザー向けにアプリケーションをApp-Vクライアントに提供し、ストリーミング用の仮想アプリケーションパッケージをホストします。パッケージは管理サーバーから取得します。
- **動的構成ファイル**: App-Vパッケージは動的構成ファイルを使用してカスタマイズできます。これをパッケージに適用すると、その特性を変更できます。たとえば、追加のアプリケーションショートカットや動作を定義するために使用できます。詳細については、「動的構成ファイル」を参照してください。

動的構成ファイル

Citrix App-Vは、両方の種類の動的構成ファイルをサポートしています。ファイル設定は、アプリケーションの起動時に適用されます。

- **展開構成ファイル**: すべてのユーザーに対してマシン全体の構成を提供します。これらのファイルは`<packageFileName>_DeploymentConfig.xml`という名前で、適用先のApp-Vパッケージと同じフォルダーにある必要があります。これらのファイルは、シングルおよびデュアル管理者管理でサポートされています。
- **ユーザー構成ファイル**: パッケージに対するユーザーごとのカスタマイズをサポートする、ユーザー固有の構成を提供します。シングル管理者では、`<packageFileName>_[UserSID |`

`Username | GroupSID |GroupName_]UserConfig.xml`という形式で名前が付けられ、適用先のApp-Vパッケージと同じフォルダーにあるユーザー構成ファイルがサポートされます。

特定のパッケージに対して複数のユーザー構成ファイルが存在する場合、それらは次の優先順位で適用されます。

a. ユーザーSID
b. ユーザー名
c. ADグループSID (最初に見つかったものが優先)
d. ADグループ名 (最初に見つかったものが優先)
e. デフォルト

例:

```
MyAppVPackage_S-1-5-21-000000001-0000000001-000000001-001_UserConfig.xml

MyAppVPackage_joeblogs_UserConfig.xml

MyAppVPackage_S-1-5-32-547_UserConfig.xml

MyAppVPackage_Power Users_UserConfig.xml

MyAppVPackage_UserConfig.xml
```

注:

ファイル名のユーザー固有の部分は、オプションで末尾に配置することもできます (例: `MyAppVPackage_UserConfig_joeblogs.xml`)。

重要:

パッケージ内のアプリケーションでユーザーセッションが開いている場合、動的展開構成に変更を適用することはできません。他のユーザー（ただし現在のユーザーではない）がパッケージ内のアプリケーションを開いている場合、動的ユーザー構成ファイルに変更を適用できます。

動的構成ファイルの場所

シングル管理者管理では、Citrix App-Vコンポーネントは、App-Vパッケージと同じフォルダーにある動的構成ファイルのみを処理します。

パッケージ内のアプリケーションが起動されると、対応する動的構成ファイルへの変更が再適用されます。動的構成ファイルがパッケージとは異なる場所にある場合は、マッピングファイルを使用してパッケージを展開構成ファイルにマッピングします。

マッピングファイルを作成するには:

1. 新しいテキストファイルを開きます。
2. 各動的構成ファイルについて、`<PackageGuid> : path`の形式を使用してパッケージへのパスを指定する行を追加します。

   例:

   ```
   F1f4fd78ef044176aad9082073a0c780 : c:\widows\file\packagedeploy.xml
   ```

3. ファイルを`ctxAppVDynamicConfigurations.cfg`として、パッケージと同じフォルダーに保存します。

App-Vパッケージと同じUNC共有上のディレクトリ階層全体が、パッケージ内のアプリケーションが起動されるたびに、このファイルについて再帰的に上位検索されます。

方法

App-Vパッケージを配信および管理するには、次の方法を使用できます:

- **デュアル管理者**: この方法では、Citrix Virtual Apps and Desktops と App-V サーバーが連携してパッケージを配信および管理します。この方法では、Citrix Virtual Apps and Desktops が App-V サーバーの状態のスナップショットビューを定期的に更新する必要があります。これには、ハードウェア、インフラストラクチャ、および管理のオーバーヘッドが発生します。Citrix Virtual Apps and Desktops と App-V サーバーは、特にユーザー権限に関して同期を維持する必要があります。

  この方法は、App-VとCitrixが密接に連携する展開で最適に機能します。この方法では:

  - **App-V管理サーバー**は動的構成ファイルを処理します
  - **App Packages Delivery Component** (VDAマシンにインストール): アプリケーションの起動に必要な適切な公開サーバーの登録を管理します。

これにより、公開サーバーが適切なタイミングでユーザーと同期されます。公開サーバーは、構成されている設定を使用して、アプリケーションパッケージのライフサイクルの他の側面（ログオン時の更新や接続グループなど）を維持します。

- **シングル管理者**: アプリケーションパッケージはネットワーク共有に保存されます。Citrix Virtual Apps and Desktops は、パッケージを独立して配信および管理します。

  この方法により、展開においてApp-Vサーバーとデータベースインフラストラクチャが不要になるため、オーバーヘッドが削減されます。

  この方法では、App-Vパッケージをネットワーク共有に保存し、その場所からメタデータを環境にアップロードします。その後、VDAマシンにインストールされているApp Packages Delivery Componentが、次のようにアプリケーションを管理および配信します。

  - アプリケーションが起動されたときに、展開構成ファイルとユーザー構成ファイルを処理します。
  - ホストマシン上のパッケージのライフサイクルのすべての側面を管理します。

注:

- 1つまたは両方の管理方法を同時に使用できます。つまり、アプリケーションをデリバリーグループに追加すると、アプリケーションはApp-Vサーバーまたはネットワーク共有にあるApp-Vパッケージから取得できます。
- 両方の管理方法を同時に使用しており、App-Vパッケージが両方の場所に動的構成ファイルを持っている場合、App-Vサーバー内のファイル（デュアル管理）が使用されます。
- Web Studioのナビゲーションペインで App packagesを選択すると、パッケージ名と種類が表示されます。**Package type**列は、パッケージの配信に使用されるテクノロジーと、**Application Library**で参照される場所を示します。パッケージを選択すると、詳細ペインにパッケージ内のアプリケーションとショートカットが一覧表示されます。

MSIXおよびMSIXアプリ添付アプリケーション

MSIXはWindowsアプリパッケージ形式であり、すべてのWindowsアプリに最新のパッケージングエクスペリエンスを提供します。MSIXは、Win32、.NET、UWPアプリなど、さまざまなWindowsアプリケーションタイプに適しています。

MSIXアプリ添付は、パッケージの内容をストリーミングするのではなく、仮想ハードディスクに事前に展開され、必要に応じてターゲットマシンにマウントできるMSIXパッケージを利用します。これにより、展開時間を短縮し、ネットワークトラフィックを削減し、ターゲットマシンでのIOPSを低減できますが、アプリ添付ディスクの作成と維持には追加の作業が必要です。

Citrix Virtual Apps and Desktops は、VDA マシンにインストールされている**App Packages Delivery Component**を介して、MSIX および MSIX app attach アプリケーションをユーザーに配信します。このコンポーネントは、ホストマシン上のパッケージのライフサイクルに関するすべての側面を管理します。

MSIX および MSIX app attach の詳細については、Microsoft のドキュメント「MSIX documentation」と「App Attach in Azure Virtual Desktop」をそれぞれ参照してください。

> **注:**
>
> - ネイティブの MSIX パッケージはデスクトップおよびサーバー VDA でサポートされており、MSIX app attach はデスクトップ VDA の `.vhd`、`.vhdx`、および `.cim` ディスクイメージ形式でのみサポートされています。
> - Microsoft は Server 2019 用の AppAttach 実装を提供していません。AppAttach は Server 2022 および 2025 に存在しますが、Microsoft はこれらのバージョンでのサポートを提供していません。したがって、弊社も Server 2022 および 2025 での AppAttach をサポートしていません。
> - Windows Server 2019 でサイドローディングを有効にします。
> - VDA がパッケージの署名に使用されている証明書を信頼していることを確認してください。

FlexApp アプリケーション

FlexApp は Liquidware が開発したアプリケーションレイヤリングソリューションで、従来のアプリケーションインストールプロセスを通じて基盤となるベースイメージを変更することなく、任意のアプリケーションを Windows セッションにアタッチします。

FlexApp One アプリケーションは、単一の共有可能なファイルにカプセル化されており、Windows セッションに追加のアプリケーションレイヤーを必要とせずに動作できます。ユーザーはコンテナファイルをクリックすることでアプリケーションを起動でき、1つまたは複数のアプリケーションを Windows ワークスペースに迅速に統合できます。

Citrix は、VDA マシンにインストールされている App Packages Delivery Component と FlexApp delivery agent を介して、FlexApp アプリケーションをユーザーに提供します。これら2つのコンポーネントは、ホストマシン上のパッケージのライフサイクルのあらゆる側面を管理します。

Elastic App アプリケーション

Elastic App テクノロジーは、Citrix App Layering の機能であり、アプリケーションレイヤーをベースイメージにインストールするのではなく、ログオン時にユーザーに動的に割り当てることができます。Elastic App テクノロジーを使用すると、アプリケーションは異なる仮想マシン間でユーザーに追従し、マスターイメージを肥大化させることなく、必要なアプリに常にアクセスできるようにします。

Citrix Virtual Apps and Desktopsは、Citrix PersonalizationコンポーネントとApplication Layering Enterprise Layer Manager (ELM) を介して、Elastic Appアプリケーションをユーザーに配信します。これら2つのコンポーネントは、ホストマシン上のパッケージのライフサイクルのすべての側面を管理します。Application Layering Enterprise Layer Managerの詳細については、Citrix App Layering™ ドキュメントを参照してください。

Cloudpaging アプリケーション

Cloudpaging は、Numecent のアプリケーションストリーミングテクノロジーであり、ベースイメージに変更を加えることなく、Windows セッションにアプリケーションを配信します。

Cloudpaging を使用すると、コードのごく一部（通常は 10% 未満）のみが最初にストリーミングされるため、アプリケーションはほぼ瞬時に起動します。残りのコンポーネントは、ユーザーがアクセスしたときにバックグラウンドでストリーミングされ、シームレスなエクスペリエンスを提供します。

Citrix 環境では、VDA 上の App Packages Delivery Component が Numecent Cloudpaging Player と連携してアプリケーションのライフサイクルを管理します。Citrix コンポーネントは配信を調整し、Cloudpaging Player はセッション内でのオンデマンドストリーミングと実行を処理します。

構成要件

次の構成の詳細を考慮してください。

クラウドページング プレイヤー と LogoffCheckSysModules

Cloudpaging コンテナで仮想公開アプリケーションを使用する場合、セッションのログオフを許可するには、次の設定を構成します。

設定	値
レジストリキー	`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI`
値の名前	`LogoffCheckSysModules`
値の型	`REG_SZ`
値データ	`CoreHelper.exe`

ホワイトリスト登録用のURL

標準のURLホワイトリスト登録要件に加えて、VDAは次のエンドポイントへのアクセスを必要とします。

パラメーター	値
URL	`external-api.cloudpager.net`
ポート	443
クライアント	Cloudpager PoSh モジュール
Webベースのフォワードプロキシ構成	• アウトバウンドアクセス許可 • 認証バイパスが必要
説明	Cloudpager PowerShellモジュール

オプションで、Cloudpagerの検出のみを実行するために使用されるVDAを含む専用のデリバリーグループを作成して、必要なホワイトリストURLを制限できます。**VDAバージョン2511以降**と**App packages Delivery Component**がインストールされているマシンを含むデリバリーグループを作成することをお勧めします。

Cloudpagerクライアントのネットワークおよびファイアウォールの要件の詳細については、Numecentナレッジベースの記事を参照してください。

アプリケーションパッケージの展開と配信

前提条件

App-V、MSIX、MSIX app attach、FlexAppパッケージ、Elastic Appアプリケーション、およびCloudpagingパッケージの配信をサポートするには、まずVDAマシンに**App Packages Delivery Component**をインストールする必要があります。詳細については、VDAマシンにApp Packages Delivery Componentをインストールするを参照してください。

VDAマシンへのApp Packages Delivery Componentのインストール

App Packages Delivery Componentは、App-V、MSIX、MSIX app attach、FlexApp、Elastic App、およびCloudpaging形式のアプリケーションパッケージの公開プロセスを管理します。このコンポーネントは、VDAをインストールするときにデフォルトではインストールされません。このコンポーネントは、VDAのインストール中またはインストール後にインストールできます。

VDAのインストール中にコンポーネントをインストールするには、次のいずれかの方法を使用します。

- インストールウィザードで、**追加コンポーネント**ページに移動し、**App Packages Delivery Component**チェックボックスを選択します。
- コマンドラインインターフェイスで、`/includeadditional "Citrix Personalization for App-V – VDA"`オプションを使用します。

VDAのインストール後にコンポーネントをインストールするには、次の手順に従います。

1. VDAマシンで、**コントロールパネル > プログラム > プログラムと機能**に移動し、**Citrix Virtual Delivery Agent**を右クリックして、**変更**を選択します。
2. 表示されるウィザードで、**追加コンポーネント**ページに進み、**App Packages Delivery Component**チェックボックスを有効にします。

> **注:**
>
> - Microsoft App-V Desktop Client は、ユーザーデバイスで App-V パッケージから仮想アプリケーションを実行するコンポーネントです。Windows 10 (1607 以降) および Windows Server 2019 以降には、この App-V クライアントソフトウェアがすでに含まれています。VDA マシンでのみ有効にする必要があります。詳細については、この Microsoft ドキュメント記事を参照してください: App-V インボックスクライアントを有効にする。

- FlexApp アプリケーションの場合は、App Packages Delivery Component とともに VDA に FlexApp One Agent をインストールします。
- Elastic App アプリケーションの場合は、App Packages Delivery Component とともに VDA に App Layering 対応イメージをインストールします。
- Cloudpaging アプリケーションの場合は、App Packages Delivery Component とともに VDA に Cloudpaging Playerをインストールします。

FlexApp One Agent をインストールする

1. VDA で管理者コマンドプロンプトを起動します。
2. 任意の FlexApp One Package のネットワークパスを見つけます。
3. 次のコマンドを入力します。

```
\\path\to\any\FlexAppOnePackage.exe --install
```

4. 表示されるプロンプトをすべて承認します。

App Layering 対応イメージをインストールする

1. アプリレイヤリングを設定します。 Citrix App Layering ドキュメントの指示に従ってください。プロセスには以下が含まれます。
   a. Enterprise Layer Manager (ELM) を設定します。
   b. ゴールド OS イメージをインポートします。
   c. プラットフォームレイヤーを作成します。
   d. アプリケーションレイヤーを作成します。
   e. ELMで、配信する各アプリケーションレイヤーに対して、**Studio App Packagesでの使用をこのApp Layerで有効にする**チェックボックスを選択します。
2. Elastic Layeringコンポーネントを含むイメージをVDAマシンにインストールします。次のいずれかの方法を使用できます。
   a. Elastic Layeringを有効にして、ELMからイメージを展開します。
   b. マシンにVDAを手動でインストールし、セットアップ中にElastic Layeringコンポーネントを選択します。

Cloudpaging Playerをインストールする

1. VDAで管理者コマンドプロンプトを開きます。
2. Cloudpaging Playerインストーラーが含まれているフォルダーに移動します。
3. プレーヤーをサイレントインストールし、SaaSコンソールURLを構成するには、次のコマンドを実行します。必要に応じてプレースホルダー値を置き換えてください。

```
cloudpaging-player-setup-x64-release.exe /S /v"/qn ADDLOCAL=ALL
REG_BASTOKENPATHORURL=https://your-tenant-url/api/token"
```

4. (オプション) インストール後に、次のレジストリ値を確認して構成を検証します。
   - **パス:** `HKEY_LOCAL_MACHINE\SOFTWARE\Numecent\StreamingCore\Settings\Launcher`
   - **名前:** `BaseTokenPathOrURL`
   - **データ:** 値は、インストール時に指定したURLと一致する必要があります。

パッケージ化されたアプリケーションを配信する

前提条件のインストールが完了したら、パッケージ化されたアプリケーションをユーザーに配信するには、次の操作を行います。

1. アプリケーションパッケージをネットワーク共有に保存する。
2. アプリケーションパッケージを環境にアップロードする。
3. アプリケーションをデリバリーグループに追加する。
4. 相互依存するApp-Vパッケージの自動配信を有効にするには、分離グループを作成します。

アプリケーションパッケージをネットワーク共有に保存する

インフラストラクチャをセットアップしたら、アプリケーションパッケージを生成し、UNCまたはSMBネットワーク共有、あるいはAzureファイル共有などのネットワークロケーションに保存します。

詳細な手順は次のとおりです。

1. アプリケーションパッケージを生成します。詳細については、Microsoftのドキュメント「App-V仮想化アプリケーションの作成と管理」を参照してください。
2. アプリケーションパッケージをネットワークロケーションに保存します。
   - **App-V Single Admin**の場合：パッケージと対応する動的構成ファイル（App-V）をUNCまたはSMBネットワーク共有、あるいはAzureファイル共有に保存します。

- **App-V Dual Admin**の場合：UNCパスからApp-V管理サーバーにパッケージを公開します。（HTTP URLからの公開はサポートされていません。）
- **MSIXまたはMSIX app attach**の場合：パッケージをUNCまたはSMBネットワーク共有、あるいはAzureファイル共有に保存します。
- **FlexApp**の場合：パッケージをUNCまたはSMBネットワーク共有、あるいはAzureファイル共有に保存します。
- **Elastic App**の場合：パッケージをUNCまたはSMBネットワーク共有、あるいはAzureファイル共有に保存します。
- **Cloudpaging**の場合: パッケージをUNCまたはSMBネットワーク共有、あるいはAzureファイル共有に保存します。

3. VDAがパッケージストレージパスに対する読み取り権限を持っていることを確認してください。

   - ADドメイン内のUNCまたはSMBネットワーク共有にパッケージを保存する場合、VDAマシンにストレージパスへの読み取り権限を付与します。そのためには、マシンのADアカウントに共有への読み取り権限を明示的に付与するか、その権限を持つADグループにアカウントを含めることができます。
   - Azureファイル共有にパッケージを保存する場合は、まずAzureのストレージパスにユーザーアカウントの読み取り権限を付与します。次に、VDAマシンで実行されている `ctxAppVService` を、そのユーザーアカウントを使用してパッケージストレージパスにアクセスするように構成します。詳細な手順については、ユーザーログオンアカウントの変更を参照してください。

ユーザーログオンアカウントの変更

以下の2つのシナリオでユーザーログオンアカウントを変更します。

- リンクされたADアカウントを使用してAzureファイル共有上のパッケージにアクセスするには：
  - 接続エンティティは、マシンアカウントではなくユーザーアカウントである必要があります。これは、Microsoft Entra IDがファイル共有上のマシンアカウントに読み取り権限を付与しないためです。
- MSIXおよびMSIX AppAttachパッケージにサービスが含まれている場合：
  - パッケージは、非管理者ユーザーに公開する前に、ローカルマシンで管理者権限を持つユーザーアカウントを使用して公開する必要があります。これは、パッケージ化された

サービスをインストールするために必要であり、パッケージはマシンではなくユーザーにのみ公開できるため、デフォルトのLocalServiceアカウントは不適切です。

VDAは`ctxAppVService`を呼び出して、パッケージストレージパスにアクセスし、管理者権限を必要とする操作を実行します。デフォルトでは、`ctxAppVService`はマシンのLocalServiceアカウントのコンテキストで実行され、マシンのIDを使用してADに認証するため、上記のシナリオには適していません。

いずれの場合も、サービスは、ローカルで管理者権限を持ち、パッケージの保存場所（SMB共有またはAzureファイル共有）への読み取りアクセス権が付与されているADユーザーアカウントを使用するように再構成する必要があります。手順は次のとおりです。

1. **サービス**を開始し、**ctxAppVService**を右クリックし、**プロパティ**を選択します。
2. **ログオン**タブで、**このアカウント**を選択します。
    a. ローカル管理者権限とパッケージストレージパスへの読み取り権限を持つユーザーアカウントを入力します
    b. ユーザーのパスワードを2回入力します。
3. **OK**をクリックします。

アプリケーションパッケージを環境にアップロードする

必要に応じてアプリケーションパッケージをネットワークの場所に保存した後、配信のために環境にアップロードします。必要に応じて、以下のいずれかの方法を使用します。

- 一括アップロード
- 1つずつアップロード

準備

Citrix Virtual Apps and Desktops は、パッケージ検出のためのネットワークロケーションへの接続を設定するために VDA マシンを使用します。したがって、事前にデリバリーグループを作成し、グループ内の少なくとも1つの VDA が次の要件を満たしていることを確認してください。

- VDAバージョン:
    - App-Vパッケージを検出する場合: 2203以降
    - MSIXおよびMSIXアプリ添付パッケージを検出する場合: 2209以降
    - FlexAppパッケージを検出する場合: 2311以降およびFlexApp Agentソフトウェア
    - ElasticAppパッケージを検出するには：2511以降、およびApp Layeringが有効なイメージ
    - CloudpagerコンソールからCloudpagingパッケージを検出する場合: 2511以降

    - ネットワーク共有からCloudpagingパッケージを検出する場合: 2603以降

- アプリケーションパッケージ配信コンポーネント: インストール済み
- パッケージの場所に対するアクセス許可: 読み取り (詳細については、ネットワーク共有にアプリケーションパッケージを保存するを参照してください。)
- 電源: オン
- 状態: 登録済み

アプリケーションパッケージを一括でアップロードする

ネットワーク上の場所にあるパッケージを環境にアップロードします。アップロードする前に、次の項目が準備されていることを確認してください。

- 準備の要件を満たすデリバリーグループ
- ネットワークの場所のパス

パッケージを一括でアップロードするには、次の手順に従います。

1. 左側のペインで、**App packages**を選択します。
2. 「**パッケージ検出**」タブで、「**検出プロファイルの作成**」ボタンをクリックします。「**検出プロファイルの作成**」ページが表示されます。
3. **名前**フィールドに、プロファイルの説明的な名前を入力します。
4. **デリバリーグループ**フィールドで、**デリバリーグループの選択**をクリックします。次に、準備に記載されている要件を満たすデリバリーグループを選択し、**OK**をクリックします。
5. **場所の種類**フィールドで、パッケージの保存場所に応じて**Microsoft App-Vサーバー**、**ネットワーク共有**、または**Numecent Cloudpager**を選択し、対応する設定を完了します。

    - **Microsoft App-Vサーバー**を選択した場合は、次の情報を入力します。

        - 管理サーバーのURL。例: `http://appv-server.example.com`
        - 管理サーバー管理者のログイン資格情報。
        - 公開サーバーのURLとポート番号。例: `http://appv-server.example.com:3330`

    - **ネットワーク共有**を選択した場合は、次の情報を指定します。

        - ネットワーク共有のUNCパスを入力します (例: `\\Package-Server\apps\`)。*Elastic App*パッケージの場合は、ELMの**System's Network File Share SMB path**からUNCパスを入力します。

    - アップロードするパッケージの種類を選択します。オプションには、**App-V**、**MSIX**、**MSIX app attach**、**FlexApp**、**Elastic App**、**Cloudpaging**が含まれます。
    - パッケージのサブフォルダーを検索するかどうかを指定します。

      > **注:**
      >
      > `cim`イメージを含むフォルダー構造でMSIX app attachパッケージを検索する場合は、**サブフォルダーを検索**を選択していることを確認してください。そうしないと、ディスクが正しく検出されません。

- **Numecent Cloudpager** を選択した場合（Cloudpaging アプリが Cloud Pager Console に保存されていることを意味します）、次の情報を入力します。
    - Cloudpager コンソールの URL。例: `https://cloudpagerconsole.my.org`
    - PowerShell APIキー。
    - AppLauncher MSID。

6. **検出プロファイルの作成**をクリックします。

「**検出プロファイルの作成**」ページが閉じ、新しく追加されたプロファイルがプロファイルリストに表示されます。Citrix Virtual Apps and Desktops は、デリバリーグループ内の VDA を使用してパッケージを環境にアップロードします。アップロードが完了すると、 フィールドに *インポート成功* と表示されます。対応するパッケージは「**パッケージ**」タブに表示されます。

> **注:**
>
> ソースの場所でパッケージの更新を確認し、環境にインポートするには、プロファイルリストで場所を選択し、**更新の確認** をクリックします。

アプリケーションパッケージを1つずつアップロードする

ネットワーク共有から環境にアプリケーションパッケージをアップロードします。アップロードする前に、次の項目が準備されていることを確認してください。

- 準備に記載されている要件を満たすデリバリーグループ
- ネットワークの場所のパス。

パッケージを環境にアップロードするには、次の手順に従います。

1. 左側のペインで、**アプリパッケージ**を選択します。
2. **パッケージ**タブで、**パッケージの追加**ボタンをクリックします。**パッケージの追加**ページが表示されます。
3. 「**デリバリーグループ**」フィールドで、「**デリバリーグループの選択**」をクリックします。次に、準備に記載されている要件を満たすデリバリーグループを選択し、「**OK**」をクリックします。
4. 「**パッケージのフルパス**」フィールドに、必要に応じてパスを入力します。
   - 複数のパッケージを一度にアップロードするには、セミコロン (`;`) で区切って、それらのフルパスを入力します。例: `\\Package-Server\apps\office365.appv;\\Package-Server\apps\skype.msix;\\Package-Server\apps\slack.vhd`
   - ネットワーク共有にあるすべてのパッケージをアップロードするには、ストレージパスを入力します。例: `\\package-Server\apps\`
5. 「**パッケージの追加**」をクリックします。

   アプリケーションパッケージが「**パッケージ**」タブに表示されます。

アプリケーションをデリバリーグループに追加する

アプリケーションパッケージが環境に完全にアップロードされたら、必要に応じて、そのアプリケーションを1つ以上のデリバリーグループに追加します。その結果、それらのデリバリーグループに関連付けられたユーザーはアプリケーションにアクセスできるようになります。

注:

- デリバリーグループを介して、パッケージ化されたアプリケーションをシングルセッションVDAおよびマルチセッションVDAに配信できます。
- デフォルトでは、エンドユーザーは、*シングルセッション* (または*デスクトップ*と呼ばれる) VDAに関連付けられたデリバリーグループに割り当てられているすべてのパッケージ化されたアプリケーションにアクセスできます。*デスクトップ*VDA上のパッケージ化されたアプリケーションの可視性を特定のユーザーまたはグループに制限するには、「**アプリケーション**」ノードに移動し、アプリケーションを選択して、「**アプリケーションプロパティの編集 > 可視性の制限**」を選択して変更を加えます。アプリケーションの可視性を制限するを参照してください。

パッケージ内の1つ以上のアプリケーションを複数のデリバリーグループに追加するには、次の手順に従います。

1. 左ペインで、**App Packages**を選択します。
2. **Packages**タブで、必要に応じてパッケージを選択します。
3. アクションバーで、**Add Delivery Groups**をクリックします。**Assign Applications to Delivery Groups**ページが表示されます。
4. 必要に応じてパッケージ内のアプリケーションを1つ以上選択し、「**次へ**」をクリックします。
5. デリバリーグループのリストで、アプリケーションを割り当てるグループを選択し、**Next**をクリックします。

   注:

   - MSIXまたはMSIXアプリ添付パッケージを選択した場合、VDAバージョンが2106以降のデリバリーグループのみがリストに表示されます。
   - *FlexApp*パッケージを選択した場合、VDAバージョンが2402以降のデリバリーグループのみがリストに表示されます。
   - *Elastic App* パッケージを選択した場合、VDA バージョンが 2511 以降のデリバリーグループのみがリストに表示されます。
   - *Cloudpaging*パッケージを選択した場合、VDAバージョンが2511以降のデリバリーグループのみがリストに表示されます。

6. **完了**をクリックします。

さまざまなパッケージのアプリケーションを複数のデリバリーグループに追加するには、次の手順に従います。

1. 左ペインで、**App Packages**を選択します。
2. **Applications**タブで、**Add Applications**を選択します。
3. **Groups**ページで、必要に応じて1つ以上のデリバリーグループを選択します。
4. **Applications**ページで、次のように1つ以上のアプリケーションパッケージを選択します。
   a. **Add**をクリックし、**Application packages**を選択します。

b. 必要なパッケージプロファイルの種類を選択します（例: App-V Single Admin）。この種類のすべてのパッケージが表示されます。

c. 必要に応じて1つ以上のパッケージを選択します。

d. **OK**をクリックし、次に**Next**をクリックします。

e. 異なるパッケージタイプのアプリケーションをさらに追加するには、手順aからdを繰り返します。

5. **完了**をクリックします。

次の場合に、パッケージ化されたアプリケーションをデリバリーグループに追加することもできます。

- デリバリーグループを作成する場合。詳細については、「デリバリーグループの作成」を参照してください。
- 既存のデリバリーグループまたはアプリケーショングループを編集する場合。詳細については、「アプリケーションの追加」を参照してください。

（オプション）App-Vパッケージの分離グループを作成する

相互依存するApp-Vパッケージを自動的に配信できるように、分離グループを作成できます。

> **注:**
>
> 分離グループは、App-Vシングル管理者方式でサポートされています。App-Vデュアル管理者方式を使用している場合は、Microsoft App-Vインフラストラクチャで*接続グループ*を作成することで同じ目標を達成できます。詳細については、Microsoftのドキュメント記事「接続グループファイルについて」を参照してください。

分離グループについて

分離グループとは、仮想環境を作成するために同じWindows Sandboxで実行する必要がある、相互依存するアプリケーションパッケージの集合です。Citrix App-V分離グループは、App-V接続グループに似ていますが、同一ではありません。分離グループには、次の2種類のパッケージが含まれます。

- **明示的なアプリケーションパッケージ**：特定のライセンス要件を持つアプリケーション。これらのアプリケーションをデリバリーグループに追加することで、特定のユーザー範囲に制限できます。

- **自動アプリケーションパッケージ**：デリバリーグループに追加されているかどうかに関係なく、常にすべてのユーザーが利用できるアプリケーション。

たとえば、アプリケーション`app-a`を実行するにはJRE 1.7が必要です。app-a（*明示的*としてマーク）とJRE 1.7（*自動*としてマーク）を含む分離グループを作成できます。次に、`app-a`のApp-Vパッケージを1つ以上のデリバリーグループに追加します。ユーザーがapp-aを起動すると、JRE 1.7が自動的に展開されます。

ユーザーが分離グループ内で *Explicit* とマークされたApp-Vアプリケーションを起動すると、Citrix Virtual Apps and Desktopsはデリバリーグループ内のアプリケーションに対するユーザーのアクセス権限を確認します。ユーザーがアプリケーションにアクセスする権限を持っている場合、同じ分離グループ内の *Automatic* アプリケーションパッケージはユーザーに利用可能になります。

*自動*パッケージをデリバリーグループに追加する必要はありません。分離グループに別の*明示的*アプリケーションパッケージがある場合、そのパッケージは同じデリバリーグループにある場合にのみユーザーが利用できます。

APP-V分離グループを作成する

分離グループを作成し、相互依存するアプリケーションパッケージを追加します。詳細な手順は次のとおりです。

1. **「分離グループ」**タブで、「分離グループの追加」**をクリックします。
2. 分離グループの名前と説明を入力します。環境内のすべてのApp-Vシングル管理者パッケージが**「利用可能なパッケージ」**リストに表示されます。
3. **「利用可能なパッケージ」**リストから、必要に応じてアプリケーションを選択し、右矢印をクリックします。選択したアプリケーションが「分離グループ内のパッケージ」**リストに表示されます。
4. 「**展開**」フィールドで、アプリケーションに対して「**明示的**」または「**自動**」を選択します。
5. さらにパッケージを追加するには、手順2〜3を繰り返します。
6. リスト内のパッケージの順序を調整するには、上矢印または下矢印をクリックします。
7. 「**保存**」をクリックします。

> **注:**
>
> 隔離グループ構成により、VDA上にApp-V接続グループが作成されます。展開シナリオは複雑になる可能性があり、App-Vクライアントは一度に1つのアクティブな接続グループにのみ

> 存在するパッケージをサポートします。同じパッケージを、同じデリバリーグループに追加された2つの異なる隔離グループに追加することは避けることをお勧めします。

ベストプラクティス

- App-Vパッケージを展開するには、PowerShellコマンド`Enable-AppV`を使用してVDAでApp-Vサブシステムを有効にします。
- MSIX（およびAppAttach）パッケージを展開するには、VDAがパッケージの署名に使用されている証明書を信頼する必要があります。
- Windows Server 2019では、MSIXパッケージを展開するためにサイドローディングを有効にします。Windows 10、11、Windows Server 2022、および2025ではサイドローディングは不要です。
- App AttachはWindows Server 2019では全く実装されておらず、Windows Server 2022または2025ではMicrosoft（およびCitrixも同様に）によって現在サポートされていません。

詳細設定

以下の高度なトピックでは、基本的なアプリパッケージのワークフローを超えて、Citrix Virtual Apps and Desktops でパッケージ化されたアプリケーションがどのように検出、更新、配信されるかを微調整するための追加の構成オプションと制御について説明します。

パッケージ化されたアプリケーションの公開を自動化する

PowerShellコマンドを使用して、パッケージ化されたアプリケーションの公開を自動化できます。

Delivery Controller™上で、以下のPowerShellコマンドを実行します:

1. パッケージ検出モジュールに存在するコマンドをロードするには:

```
Import-Module "D:
\Support\Tools\Scripts\Citrix.Cloud.AppLibrary.Admin.v1.psm1"
```

> **注:**
>
> パッケージ検出モジュールのバージョンは、Citrix Virtual Apps and Desktops ISOの、手順1で述べたパスにあります。

2. パッケージ検出モジュールは、公開するパッケージタイプもサポートするCitrix Virtual Apps and DesktopsバージョンのISOから取得する必要があります。つまり、FlexAppOneアプリケーションには2311以降が必要です。利用可能な最新バージョンを使用することをお勧めします。
3. 関連するデリバリーグループIDとパッケージ化されたアプリケーションIDを取得するには:

```
Get-BrokerDesktopGroup | Format-Table Uid, Name

Get-AppLibAppVApplication | Format-Table Uid, Name
```

4. パッケージを公開し、適切なBrokerMachineConfigurationを作成するには:

```
Publish-PackagedApplication -AppLibararyApplicationUid
<AppLibararyApplication.Uid > -DesktopGroupUid <DesktopGroup.Uid>
```

5. Broker構成を同期するには、これは後でVDA上のBrokerエージェントに送信されます:

```
Update-DesktopGroupMachineConfigurations -DesktopGroupUid
<DesktopGroup.Uid>
```

> **注:**
>
> PowerShellコマンドラインを介してデリバリーグループからパッケージ化されたアプリケーションを公開または削除した後には、PowerShellコマンド `Update-DesktopGroupMachineConfigurations` を必ず実行してください。そうしないと、公開されたアプリケーションに関する情報がVDAに正しく送信されず、起動に失敗します。

アプリケーションの可視性を制限する

Citrix Virtual Apps and Desktops環境では、パッケージからのアプリケーションがデスクトップに公開されると、システムはそれらのアプリケーションに対するActive Directory (AD) のユーザーおよびグループの可視性設定を尊重します。ただし、ユーザーがパッケージ内の1つのアプリケーションに対してのみ可視性を持っている場合でも、個々のパッケージコンポーネントはVDA上で細分化できないため、パッケージ全体を仮想デスクトップ（またはシームレスアプリ）セッションに展開する必要があります。さらに、VDAバージョン2503より前では、最初の公開後にアプリケーションの可視性を低下させる変更を行っても、その後のデスクトップ起動時に以前に公開さ

れたパッケージがクリーンアップされることはありません。また、デスクトップとワークスペースの可視性など、他の可視性レイヤーは、これらのAD可視性割り当ての上に動作します。

パッケージ化されたアプリケーションがWorkspaceに表示されるべきか、ユーザーのVDIデスクトップセッションに展開されるべきかを制御できます。パッケージ化されたアプリケーションが公開されたら、PowerShellコマンド `Set-BrokerApplication -Name "MyApp" -PackagedApplicationVisibility "Workspace|Desktop|WorkspaceAndDesktop"` を使用して、`BrokerApplictaion` の `PackagedApplicationVisibility` プロパティを更新できます。

`PackagedApplicationVisibility` のデフォルト値は `WorkspaceAndDesktop` です。

値 `Workspace`: アプリはWorkspaceAppにのみ表示され、シームレスなAppLaunchに利用できますが、ユーザーが開始するデスクトップセッションには自動的に公開されません。

値 `Desktop`: アプリのアイコンをWorkspaceAppから非表示にし、シームレスなAppLaunchでは利用できなくなりますが、ユーザーがADグループ設定を通じてアクセスできる場合、アプリは引き続きユーザーのデスクトップセッションに展開できます。

> **注:**
>
> シングルセッション静的デスクトップに公開されたパッケージアプリケーションは、この設定で構成された値に関係なく、Workspace Appでは利用できません。

App-Vフルインフラストラクチャからシングル管理者ワークフローへの移行

Microsoft App-Vフルインフラストラクチャ（デュアル管理者）は、サポート終了が近づいています。App-Vパッケージやその他のサポートされているコンテナ形式の提供を継続するには、Citrixシングル管理者モデルに移行してください。

シングル管理者モデルは、App-V管理サーバーと公開サーバーへの依存関係を排除し、Studioでパッケージ管理を一元化します。

シングル管理者モデルの利点

シングル管理者ワークフローに移行することで、アーキテクチャが簡素化され、パッケージ管理が効率化されます。

簡素化されたアーキテクチャ

シングル管理者モデルでは、VDAはファイル共有から直接パッケージを取得します。Citrixはメタデータ、公開、および分離ロジックを管理します。

機能	フルインフラストラクチャ（デュアル管理者）	シングル管理者（CITRIX管理）
管理	App-V管理コンソール	シトリックス スタジオ または ウェブ スタジオ
データベース	必須 (SQL Server)	なし (メタデータはCitrixサイトデータベースに保存されます)
公開	App-V パブリッシングサーバー	シトリックス VDA (`ctxAppVService`)
パッケージソース	UNC共有 (管理サーバーに同期)	UNC共有、SMB共有、またはAzure Files
ロジック	接続グループ	Citrix分離グループ

戦略的利点

Single Adminに移行することで、**同期ラグ**も解消されます。

- Dual Admin モデルでは、App-V 管理サーバーを同期し、その後 Studio を同期する必要があります。
- Single Admin モデルでは、ファイル共有上のパッケージを更新し、Studio で を選択すると、更新されたパッケージは次回のユーザーログオン時に利用可能になります。

移行ワークフロー

既存の App-V フルインフラストラクチャを Citrix Single Admin ワークフローに移行するには、次の手順に従います。

1. ステップ 1: ターゲット環境を準備する
2. ステップ 2: パッケージを Citrix ライブラリにインポートする

ステップ 1: ターゲット環境を準備する

パッケージをインポートする前に、インフラストラクチャと VDA が Single Admin モデルをサポートする準備ができていることを確認してください。

1. **共有リポジトリ**

   a. `.appv` パッケージをホストする UNC 共有を特定します。

   b. VDA マシンアカウント（例: ドメインコンピューター）が、共有と NTFS の両方のアクセス許可に対して **読み取り** アクセス権を持っていることを確認してください。

2. **VDA**

   すべての VDA に **App Packages Delivery Component** がインストールされていることを確認してください。インストール後にこのコンポーネントを追加するには：

   a. VDA インストーラーを実行します。

   b. で を選択します。

   c. 「**App Packages Delivery Component**」を追加します。

3. **「XML構成ファイル」**

   `_DeploymentConfig.xml`と`_UserConfig.xml`ファイルを、対応する`.appv`ファイルと*同じ*フォルダーに移動します。

   Single Adminモデルでは、VDAは中央のApp-Vデータベースからではなく、ファイル共有上のパッケージフォルダーから構成ファイルを読み取ります。

ステップ2：パッケージをCitrixライブラリにインポートする

環境を準備したら、既存のApp-VパッケージをCitrixアプリケーションライブラリにインポートします。

1. Citrix Studioで、**構成** > **App Packages**に移動します。
2. 完全に移行する場合は、App-V Management Serverへの既存の接続をすべて削除します。
3. 「**Add Package**」を選択し、パッケージのUNCパスを指定します。
4. Citrixはフォルダーをスキャンし、パッケージ名、バージョン、およびアプリケーションIDをCitrixアプリケーションライブラリにインポートします。

インポート後、必要に応じてアプリケーションをデリバリーグループに割り当てることができます。

> **注:**

> 「**vPreferポリシー（オプション）**：アプリケーションをリモートサーバーにリダイレクトする代わりにローカルVDAで起動する場合は、VDAで**vPrefer** GPOを有効にします。

App-Vアプリケーションのトラブルシューティング（Single Adminモデル）

App-Vパッケージ（Single Adminモデル）が起動しない、またはユーザーセッションに表示されない場合は、以下のガイダンスを使用して一般的な問題を特定し、解決してください。

問題	説明	解決策
パッケージの検出と「カタログ化に失敗しました」エラー	Studio でパッケージを追加すると、ファイルにアクセスできないか、メタデータが無効であることを示すエラーが表示されます。	1. 権限を確認します。Delivery Controller マシンアカウント（例: `DOMAIN\DDC01$`）が、パッケージをホストする UNC パスの共有レベルと NTFS レベルの両方で**読み取り**権限を持っていることを確認します。 2. XML の整合性を確認します。`.appv` ファイルと `_DeploymentConfig.xml` ファイルのファイル名プレフィックスが同

問題	説明	解決策	
		じで、同じフォルダーにあることを確認します。	
アプリケーションが起動しない (エラーコード: 0x80070005 または 0x80040154)	ユーザーがアプリケーションアイコンをクリックすると、**Citrix splash** 画面が表示されますが、アプリケーションは開きません。	1. VDAコンポーネントを確認します。VDAに**App Packages Delivery Component**がインストールされていることを確認します。次のファイルが存在することを確認します: `C:\Program Files\Citrix\AppV\ctxAppVService.exe`。 2. VDAの権限を確認します。VDAはファイル共有からパッケージをプルするため、VDAマシンアカウント（例: `DOMAIN\VDA-HR01$`）はUNCパスへの**読み取り**アクセス権を	

問題	説明	解決策	
		持っている必要があります。 3. App-Vクライアント構成を検証します。 • VDA で次の PowerShell コマンドを実行します: `Get-AppvClientConfiguration`. • パッケージにスクリプトが必要な場合は、`EnablePackageScripts` が `$True` に設定されていることを確認してください。	
分離グループの競合	Excel アドインなどのプラグインは、その親アプリケーションを認識できません。	1. Studio で、**App Packages** > **Isolation Groups** に移動します。 2. 両方のパッケージが同じ分離グループに追加されていることを確認します。シングル管理者モデルでは、	

問題	説明	解決策	
		VDA 上の App-V クライアントが、Delivery Controller によって配信された構成に基づいて、それらのアプリケーションの仮想接続を管理します。	
初回起動が遅い（バッファリング）	AutoCADやArcGISのような大規模なApp-Vパッケージの初回起動には数分かかります。	1. VDAで、以下のレジストリを確認します。`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\AppV\Client\Streaming` 2. 以降の起動パフォーマンスを向上させるため、`Autoload`を`2`（以前使用したすべてのパッケージを自動ロード）に設定します。 3. ネットワークパフォーマンスを確認します。ネットワーク共有でのSMB署名	

問題	説明	解決策	
		またはウイルス対策スキャンが転送速度を制限していないことを確認してください。	

便利なPowerShellコマンド（VDAで実行）

Citrixがパッケージを VDAに正常に配信したかどうかを確認するには、PowerShellウィンドウで次のコマンドを実行します。

コマンド	目的
`Get-AppvClientPackage`	VDAに現在キャッシュされているか、公開されているすべてのApp-Vパッケージを表示します。
`Get-CtxAppvPackage`	Citrixエージェントによって管理されているパッケージを表示します。
`Start-Service ctxAppVService`	Citrix App-Vオーケストレーションサービスを再起動します。

UWP アプリケーションを公開する

ユニバーサル Windows プラットフォーム (UWP) アプリについては、以下の Microsoft ドキュメントを参照してください。

- ユニバーサル Windows プラットフォーム (UWP) アプリとは
- Windows パッケージマネージャー

要件と制限

Citrix Virtual Apps and Desktops™ は、以下の Windows マシン上の VDA で UWP アプリを使用することをサポートしています。

- Windows 10 以降のバージョン

- Windows Server 2016 以降のバージョン

VDA はバージョン 7.11 以降である必要があります。

UWP アプリを使用する場合、以下の Citrix Virtual Apps and Desktops™ 機能はサポートされていないか、制限されます。

- ファイルタイプの関連付けはサポートされていません。
- ローカルアプリアクセスはサポートされていません。
- 動的プレビュー：セッションで実行中のアプリが重なっている場合、プレビューにはデフォルトのアイコンが表示されます。動的プレビューに使用される Win32 API は、UWP アプリではサポートされていません。
- アクションセンターのリモート処理：UWP アプリは、セッション内のメッセージを表示するためにアクションセンターを使用できます。これらのメッセージは現在、ユーザーに表示するためにエンドポイントにリダイレクトされません。

同じサーバーから UWP アプリと非 UWP アプリを起動することはサポートされていません。代わりに、UWP アプリと非 UWP アプリを別々のデリバリーグループまたはアプリケーショングループに配置してください。

マシンにインストールされているすべてのUWPアプリが列挙されるため、Citrix®はWindowsストアへのユーザーアクセスを無効にすることを推奨します。これにより、あるユーザーがインストールしたUWPアプリが別のユーザーによってアクセスされるのを防ぎます。

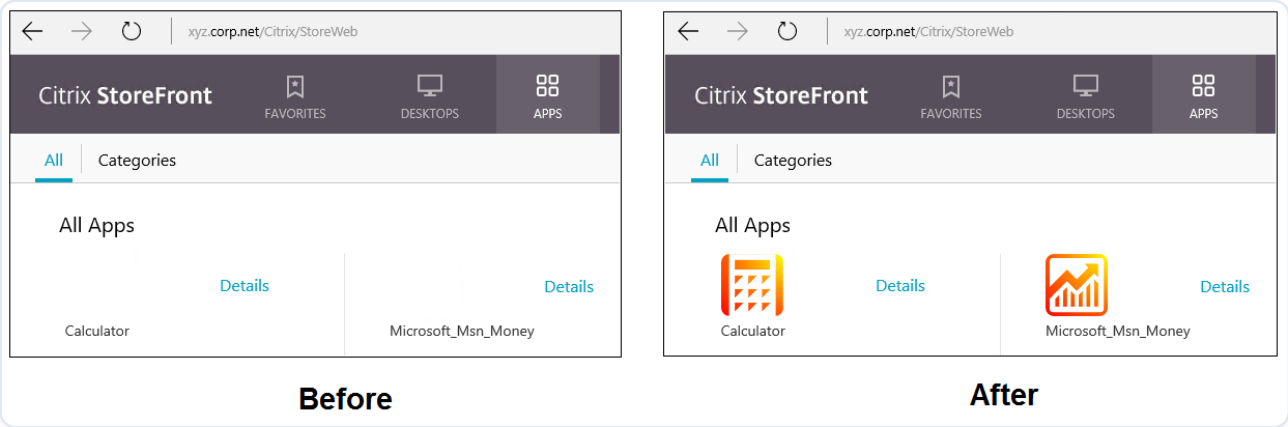
サイドローディング中、UWPアプリはマシンにインストールされ、他のユーザーが使用できるようになります。別のユーザーがアプリを起動すると、アプリがインストールされ、OSはそのAppXデータベースを更新して、そのユーザーによって「インストール済み」であることを示します。

固定ウィンドウまたはシームレスウィンドウで起動された公開UWPアプリから開始された正常なログオフにより、VDAセッションが閉じなくなり、ユーザーが強制的にログオフされる可能性があります。この場合、VDAセッションに残っているいくつかのプロセスが、セッションが適切に閉じられるのを妨げます。これを解決するには、VDAセッションが閉じない原因となっているプロセスを特定し、CTX891671のガイダンスに従って、「LogoffCheckSysModules」レジストリキー値に追加します。

UWPアプリのアプリケーション表示名と説明が正しくない場合があります。アプリケーションをデリバリーグループに追加する際に、これらのプロパティを編集して修正してください。

その他の問題については、既知の問題を確認してください。

現在、いくつかのUWPアプリは透明度が有効な白いアイコンを使用しており、StoreFront表示の白い背景に対してアイコンが見えなくなることがあります。この問題を回避するには、背景を変更できます。たとえば、StoreFrontマシンでファイル`C:\inetpub\wwwroot\Citrix\StoreWeb\custom\style.css`を編集します。ファイルの最後に`.storeapp-icon {background-image: radial-gradient( circle at top right, yellow, red ); }`を追加します。次の図は、この例の変更前と変更後を示しています。



Windows Server 2016以降のバージョンでは、UWPアプリの起動時にサーバーマネージャーも起動する場合があります。これを防ぐには、`HKLM\Software\Microsoft\ServerManager\DoNotOpenServerManagerAtLogon`レジストリキーを使用して、ログオン時にサーバーマネージャーが自動起動しないように無効にできます。詳細については、`<https://blogs.technet.microsoft.com/rmilne/2014/05/30/how-to-hide-server-manager-at-logon/>`を参照してください。

UWPアプリのインストールと公開

UWPアプリのサポートはデフォルトで有効になっています。

VDA（またはマスターイメージ）に1つ以上のUWPアプリをインストールするには、次のいずれかの方法を使用します。

- Windows Store for Businessからオフラインインストールを完了し、Deployment Image Servicing and Management (DISM) などのツールを使用してアプリをデスクトップイメージに展開します。詳細については、Windows Package Managerを参照してください。
- アプリをサイドロードします。詳細については、Windows クライアントデバイスで基幹業務 (LOB) アプリをサイドロードするを参照してください。
- 各対象ユーザー向けに、Windows Store for Businessから直接UWPアプリをインストールします。

Citrix Virtual AppsまたはCitrix Virtual Desktops™で1つ以上のUWPアプリを追加（公開）するには：

1. マシンにUWPアプリがインストールされたら、UWPアプリをデリバリーグループまたはアプリケーショングループに追加します。これは、グループの作成時または後で行うことができます。**アプリケーション**ページで、**追加**メニューから**スタートメニューから**を選択します。
2. アプリケーションリストが表示されたら、公開するUWPアプリを選択します。
3. ウィザードを続行するか、編集ダイアログを閉じます。

VDAでユニバーサルアプリの使用を無効にするには、`HKLM\Software\Citrix\VirtualDesktopAgent\FeatureToggle`にレジストリ設定**EnableUWASeamlessSupport**を追加し、**0**に設定します。

UWPアプリのアンインストール

`Remove-AppXPackage`のようなコマンドでUWPアプリをアンインストールすると、その項目は管理者に対してのみアンインストールされます。アプリを起動して使用した可能性のあるユーザーのマシンからアプリを削除するには、各マシンで削除コマンドを実行します。1つのコマンドですべてのユーザーのマシンからAppXパッケージをアンインストールすることはできません。

Linux VDA 公開アプリケーション

Linux VDAバージョン7.13で、Citrixはサポートされているすべてのプラットフォームにシームレスアプリケーション機能を追加しました。この機能を使用するために、特定のインストール手順は必要ありません。

> **ヒント:**
>
> Linux VDAバージョン1.4で、Citrixは非シームレス公開アプリケーションとセッション共有のサポートを追加しました。

Citrix Studioを使用したアプリケーションの公開

デリバリーグループを作成するとき、または既存のデリバリーグループにアプリケーションを追加するときに、Linux VDAにインストールされているアプリケーションを公開できます。このプロセスは、Windows VDAにインストールされているアプリケーションを公開するのと同様です。詳しくは、Citrix Virtual Apps and Desktopsのドキュメント（使用しているCitrix Virtual Apps and Desktopsのバージョンに基づく）を参照してください。

> **注:**

- デリバリーグループを構成するときは、デリバリーの種類が**デスクトップとアプリケーション**または**アプリケーション**に設定されていることを確認してください。
- アプリケーションとデスクトップのデリバリーには、個別のVDAとデリバリーグループを作成することをお勧めします。
- シームレスアプリケーションを使用するには、StoreFrontでシームレスモードを無効にしないでください。シームレスモードはデフォルトで有効になっています。「TWIMode=Off」を設定してすでに無効にしている場合は、「TWIMode=On」に変更するのではなく、この設定を削除してください。そうしないと、公開されたデスクトップを起動できない可能性があります。

制限事項

Linux VDAは、単一ユーザーによる同じアプリケーションの複数の同時インスタンスの起動をサポートしていません。

アプリセッションでは、アプリケーションに固有のショートカットのみが期待どおりに機能します。

既知の問題

アプリケーションの公開中に、以下の既知の問題が確認されています。

- 非矩形ウィンドウはサポートされていません。ウィンドウの角にサーバー側の背景が表示される場合があります。
- 公開されたアプリケーションのウィンドウコンテンツのプレビューはサポートされていません。
- 複数のLibreOfficeアプリケーションを実行すると、これらのアプリケーションはプロセスを共有するため、最初に起動されたものだけがCitrix Studioに表示されます。
- 「Dolphin」のような公開されたQt5ベースのアプリケーションでは、アイコンが表示されない場合があります。この問題を解決するには、`<https://wiki.archlinux.org/title/Qt>`の記事を参照してください。
- Linuxアプリケーションには、使用中のアプリケーションに関する情報を含む「バージョン情報」ウィンドウがよくあり、詳細情報へのWebリンクがそれらのウィンドウによく見られます。「バージョン情報」ウィンドウのWebリンクをクリックすると、**calc**、**gedit**、**calendar**、**LibreOffice Suite**などの公開アプリケーション内からWebブラウザが起動する可能性があります。意図しないWebブラウザの起動は、アプリケーションの分離を迂回し、セキュリティを

侵害する可能性があります。この問題を解決するには、以下の手順を実行してデフォルトのWebブラウザを変更します。

a. カスタムの場所にnone.shファイルを作成します。例:

```
sudo mkdir /home/none


sudo touch /home/none/none.sh


sudo chmod +x /home/none/none.sh
```

b. none.shファイルに次の行を追加します。

```
#!/bin/bash


echo "NONE"
```

c. sudoを使用して/etc/xdg/mimeapps.listファイルを作成し、その後、mimeapps.listファイルに次の行を追加します。

```
[Default Applications]


text/html=none.desktop


x-scheme-handler/http=none.desktop


x-scheme-handler/https=none.desktop
```

```
x-scheme-handler/about=none.desktop


x-scheme-handler/unknown=none.desktop
```

d. sudoを使用して/usr/share/applications/none.desktopファイルを作成し、その後、none.desktopファイルに次の行を追加します。

```
[Desktop Entry]


Encoding=UTF-8


Version=1.0


Type=Application


Terminal=false


Exec=/home/none/none.sh


Name=None

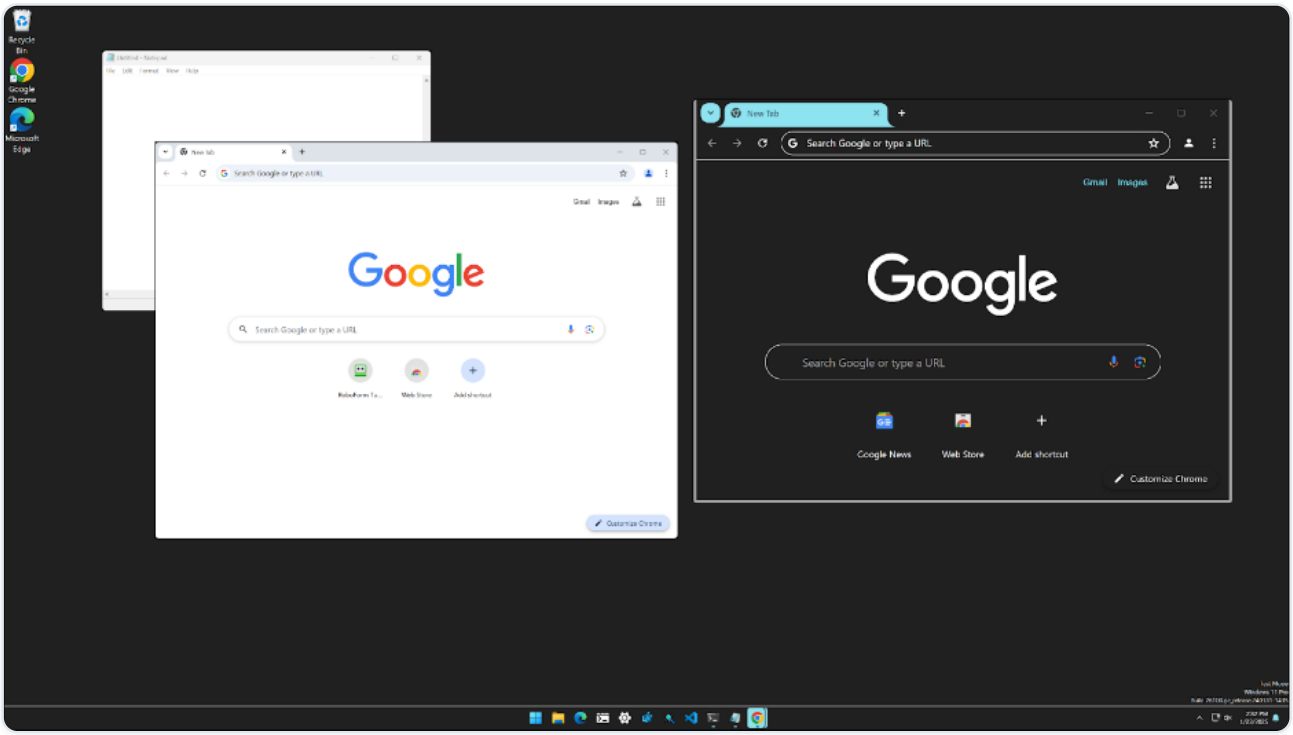

Icon=/home/none/none.sh
```

none.shファイルをカスタムの場所に配置できるため、none.desktopがnone.shファイルを正しく参照できることを確認してください。

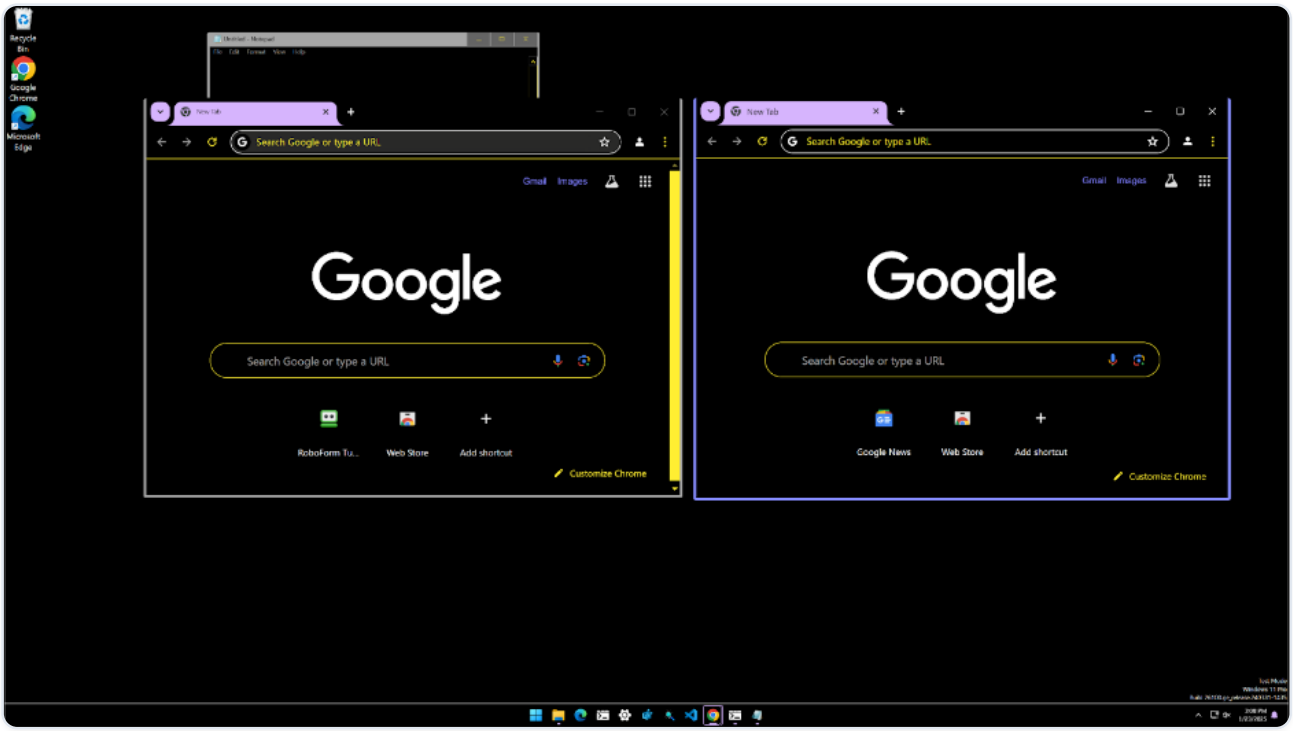
Windows アクセシビリティ設定

Seamless Applications の Windows アクセシビリティ設定は、起動時にユーザーのローカルエンドポイントから公開されたアプリセッションにアクセシビリティ設定のサブセットを自動的にミラーリングします。セッション中、ローカルエンドポイントのアクセシビリティ設定への変更は、可能な場合、リモートセッションに自動的に適用されます。

Seamless アプリケーションの Windows アクセシビリティ設定が有効になっていない場合:



Seamless アプリケーションの Windows アクセシビリティ設定が有効になっている場合:



Seamless Applications の Windows アクセシビリティ設定は、セッション中にリモートアプリケーションに設定を自動的かつ動的に適用します:

アクセシビリティミラーリングは、ユーザーのローカルエンドポイントからVDAに以下のローカルアクセシビリティ設定を自動的にミラーリングします。現在、以下のアクセシビリティ設定がサポートされています:

- ハイコントラストテーマ
- ダークモード
- マウスカーソルサイズ
- テキストサイズ

前提条件と構成

シームレスアプリケーションのアクセシビリティ設定の前提条件は次のとおりです。

- Windows用CWA 2503以降を実行しているWindowsエンドポイント
- VDA 2503以降を実行しているWindows VDA

アクセシビリティミラーリングは、以下のVDAオペレーティングシステムで利用可能です。

- ウィンドウズ サーバー 2022
- ウィンドウズ サーバー 2025
- Windows 10 マルチセッション
- Windows 11 シングルセッションおよびマルチセッション

および以下のクライアントオペレーティングシステムで利用可能です。

- ウィンドウズ 10
- ウィンドウズ 11

有効にする方法

Citrix Virtual Apps and Desktops 2511およびCWA for Windows 2511以降、シームレスアプリケーションのアクセシビリティ設定の伝播はデフォルトで有効になっています。

この機能には、管理者またはエンドユーザーによる構成は必要ありません。

管理者向け

CVAD 2511以降を実行しているVDAの場合、レジストリによってアクセシビリティ設定のミラーリングを明示的に無効にすることができます。

1. regedit.exeを使用して**Windowsレジストリエディター**を開きます。
2. `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI\`に移動します。
3. AccessibilityMirroringという名前の**DWORD**値を作成し、無効にするには値を0に設定します。

そのVDAでホストされているシームレスアプリケーションにアクセスするすべてのユーザーは、クライアントのアクセシビリティ設定がシームレスアプリケーションに伝播されません。

エンドユーザー向け

エンドポイントからシームレスアプリケーションへのアクセシビリティ設定のミラーリングを望まない場合、エンドポイントでアクセシビリティミラーリングを明示的に無効にすることで、デフォルトの動作を変更できます。

1. regedit.exe を使用して Windows レジストリエディターを開きます。
2. HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TWIに移動します。
3. AccessibilityMirroringという名前のDWORD値を作成し、無効にするにはその値を0に設定します。

これにより、エンドポイントで設定されたWindowsアクセシビリティ設定が、そのエンドポイントから起動されるすべてのシームレスアプリケーションに伝播されなくなります。

以前のVDAとクライアントの構成

古いVDA (2503以降) およびエンドポイント (CWA for Windows 2503.10以降) の場合、シームレスアプリケーションのWindowsアクセシビリティ設定の伝播はデフォルトで無効になっています。

VDAでは、シームレスアプリケーションのアクセシビリティ設定は、以下のレジストリ設定で有効にできます。

1. `regedit.exe`を使用して、**Windows レジストリエディター**を開きます。
2. `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI\`に移動します。
3. `AccessibilityMirroring`という名前の**DWORD**値を作成し、値を**1**に設定して有効にします。

CWA 2503では、シームレスアプリケーションのアクセシビリティ設定も、デフォルトでクライアント上で無効になります。以下のレジストリ設定で有効にできます。

1. `regedit.exe`を使用して、**Windows レジストリエディター**を開きます。
2. `HKEY_CURRENT_USER\Software\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TWI`に移動します。
3. `AccessibilityMirroring`という名前の**DWORD**値を作成し、その値を**1**に設定して有効にします。

> **注：**
>
> シームレスアプリケーションのアクセシビリティ設定が機能するには、レジストリキーがVDAとクライアントの両方に存在する必要があります。

> シームレスアプリケーションの新しいアクセシビリティ設定を有効にするために、追加のユーザー操作や構成は必要ありません。

ウィンドウのドラッグ

ウィンドウのドラッグなど、シームレスアプリケーションを操作する際、クライアント側ドラッグとサーバー側ドラッグを区別します。ほとんどのユースケースでは、サーバー側ドラッグよりもクライアント側ドラッグが推奨されます。クライアント側ドラッグははるかにスムーズなエクスペリエンスを提供し、ウィンドウドラッグ操作はサーバー上ではなくローカルで実行されます。

ほとんどの場合、HDX™は自動的にクライアント側ドラッグを実行しますが、特定のアプリケーションではサーバー側ドラッグのみが許可される場合があります。サーバー側ドラッグは、ウィンドウをドラッグしているときにアプリケーションの「背後」に黒いバーが表示されることで識別できます。タイトルバーの別の部分を選択すると、通常はクライアント側ドラッグになります。

クライアント側ドラッグとサーバー側ドラッグの違いについては、以下を参照してください。

Google Chromeのようなアプリケーションでは、タブをドラッグして並べ替えることができます。

これは、場合によってはサーバー側ドラッグになることもあります。これは予期される動作です。

シームレスアプリケーションの透明なウィンドウ

概要

Citrix Virtual Apps and Desktops 2511以降、シームレスアプリケーションは透明なウィンドウをサポートするようになりました。 ウィンドウの透明度とは、ウィンドウの境界線やアプリケーションウィンドウ全体を不透明ではなく半透明にし、ユーザーがデスクトップの背景や他のウィンドウなど、その背後にあるものを見ることができるようにする視覚効果です。

{シームレスな透明アプリの画像を含める}

> **注:**

> シームレスアプリケーションで透過機能を使用すると、サーバーのスケーラビリティと帯域幅の使用量に影響を与える可能性があります。最適なパフォーマンスを得るには、可能であれば、アプリケーション内の透過効果を無効にしてください。

前提条件

シームレスアプリケーションの透明なウィンドウのサポートの前提条件は次のとおりです。

- CWA for Windows 2511以降を実行しているWindowsエンドポイント
- VDA 2511以降を実行しているWindows VDA

シームレスアプリケーションの透過ウィンドウサポートは、以下のVDAオペレーティングシステムで利用できます。

- ウィンドウズ サーバー 2025
- ウィンドウズ サーバー 2025
- Windows 11 シングルセッションおよびマルチセッション

> **注:**

> - Windows 10またはServer 2022以前で公開されているシームレスアプリケーションでは、透明なウィンドウのサポートは利用できませんのでご注意ください。
> - 追加の構成は不要で、すぐにサポートが提供されます。

トラブルシューティング

公開アプリケーションでのセッションサインアウトの問題のトラブルシューティング

アプリケーションを公開する場合、公開アプリケーションのメインの実行可能ファイルのみが指定されます。ただし、一部のアプリケーションは、バックグラウンドで実行され、メインの公開アプリケーションが閉じられたときに、対応するメインの実行可能ファイルによって閉じられない追加の (子) プロセスを生成する場合があります。追加のプロセスは、実行されるスクリプトや、`Run` や `RunOnceKey` のような特定のレジストリキーから作成されることもあります。これらのアプリケーションは、正常なサインアウトを妨げ、セッションが残存またはハングアップする原因となり、セッションが閉じられず、ユーザーがサインアウトされない可能性があります。

この場合、Citrix Director を使用してこれらのセッションをリセットまたは終了する必要があります。

セッションが適切にサインアウトされない問題を特定し、トラブルシューティングするために、Citrix は3つのレジストリエントリを提供しています。これらの問題によりセッションが適切にログオフされないことの特定とトラブルシューティングは、次の3段階のプロセスです。

1. どのセッションが公開アプリケーションによって正常なサインアウトを妨げているかを特定する
2. それらの公開アプリケーションが追加の (子) プロセスを生成するかどうかを特定する
3. これらのプロセスを指定されたレジストリエントリに追加して、サインアウトを妨げないようにする

ステップ2：公開アプリケーションが追加の（子）プロセスを生成するかどうかを特定する

公開アプリケーションが正常なサインアウトを妨げていると特定されたら、次のステップは、このアプリケーションが実行時に追加のプロセスを生成するかどうかを判断することです。

公開アプリケーションが閉じられたときに、`HKCU\Software\CitrixVolatile\Seamless\Sessions\[ID]\LogoffCheckerBlockingProcess` を読んで、どのプロセスが正常なサインアウトをブロックしているかを判断できます。

以下の例では、キー `LogoffCheckerBlockingProcess` に次のエントリが含まれています。

```
PhoneExperienceHost.exe

SkypeApp.exe

SkypeBackgroundHost.exe
```

これらのプロセスが正常なサインアウトを妨げていました。

注:

確認したいセッションの正しいセッションIDで を置き換えてください。

ステップ3：これらのプロセスを指定されたレジストリエントリに追加して、サインアウトを妨げないようにする

これらのプロセスを以下のレジストリキーに追加することで、今後のセッションでサインアウトが妨げられるのを防ぐことができます。

```
Add the process file name to the following registry key:

Caution! Refer to the Disclaimer at the end of this article before using
the Registry Editor.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI

Value Name:LogoffCheckSysModules

Type:REG_SZ

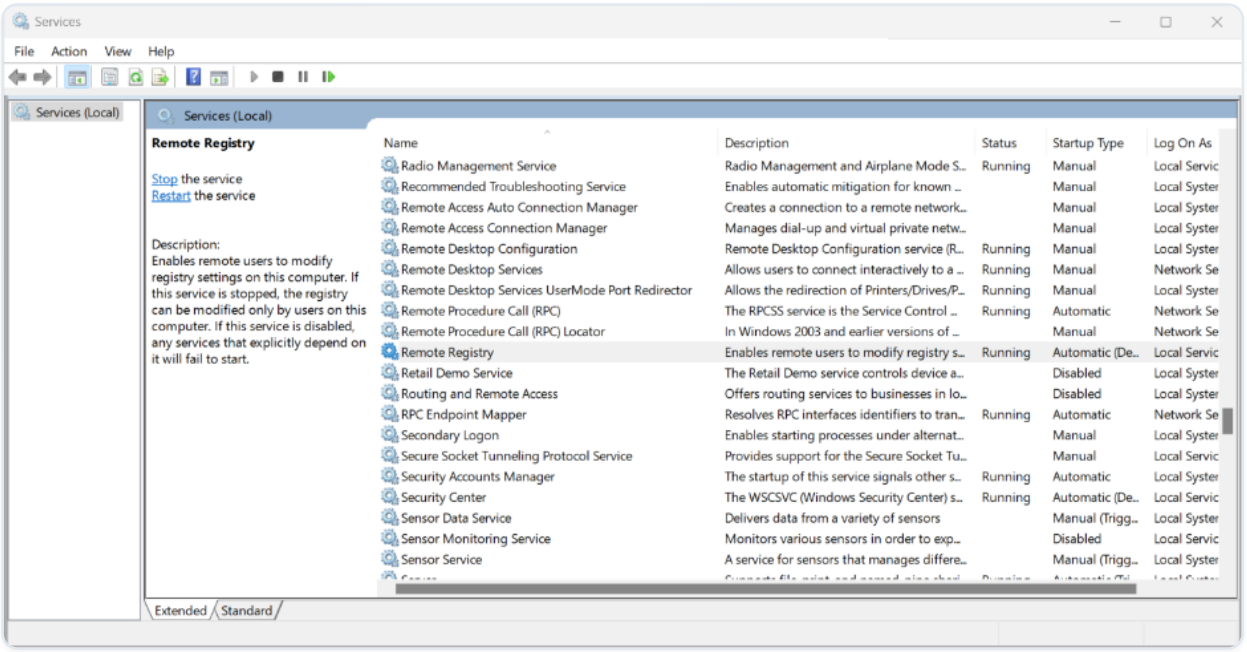
String:MyAppName.exe
```

`LogoffCheckSysModules` の詳細については、公開アプリケーションからの正常なログオフによりセッションがアクティブ状態になる を参照してください。

ステップバイステップのトラブルシューティングガイド

1. テスト対象のVDAでリモートレジストリサービスを開始します。
    a. コントロールパネルで、**管理ツール > サービス** を選択します。
    b. **リモートレジストリサービス** を右クリックし、**プロパティ** を選択します。

c. **スタートアップの種類** で、ドロップダウンメニューから **自動** を選択します。



2. テスト対象のVDAでWindowsファイアウォールをオフにするか、ポート455を有効にする受信ファイアウォール規則を作成します:

   a. コントロールパネルで、**Windows Defender ファイアウォール > 詳細設定**を選択します。

   b. **受信の規則**を右クリックし、**新しい規則**を選択します。

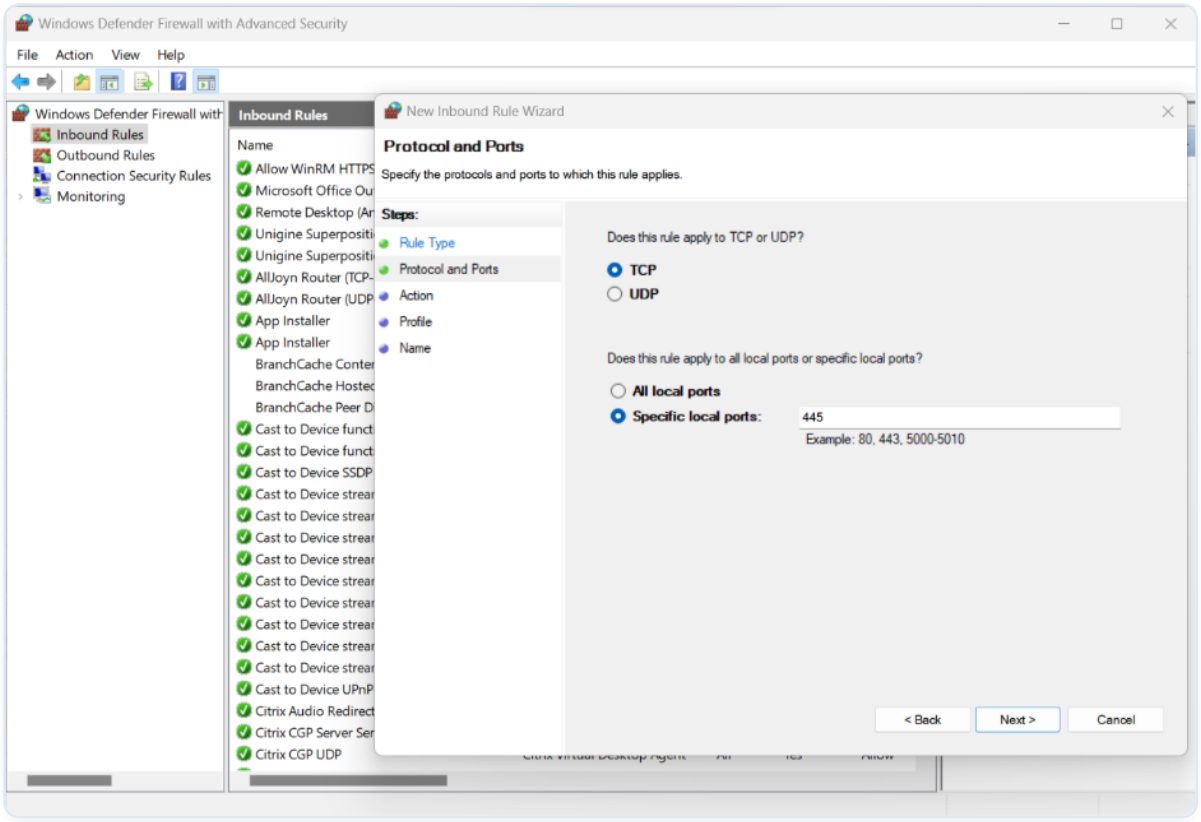
   c. **新しい受信の規則ウィザード**で、**ポート**を選択します。

   d. **プロトコルおよびポート**ページで、**TCP および特定のローカルポート**を選択します。ローカルポートとして `445` を入力します。

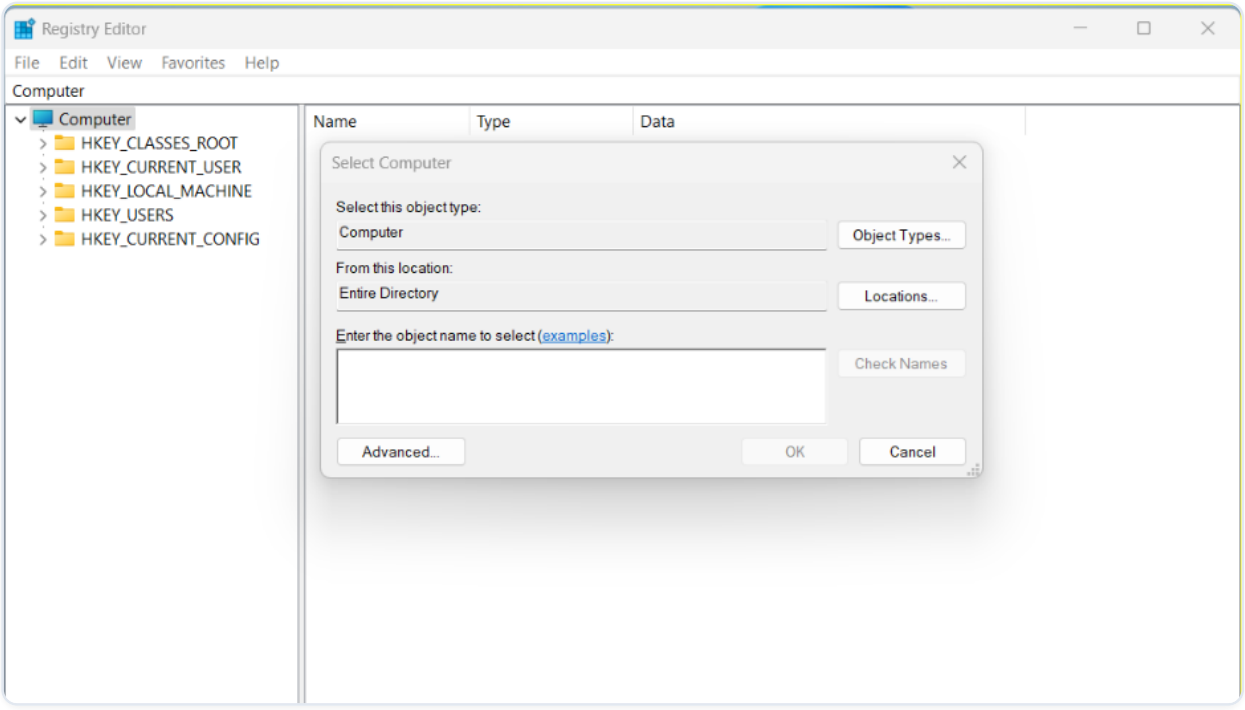
   e. **操作**ページで**接続を許可する**を選択します。

   f. 新しい受信規則を適用するファイアウォールプロファイルを選択します。

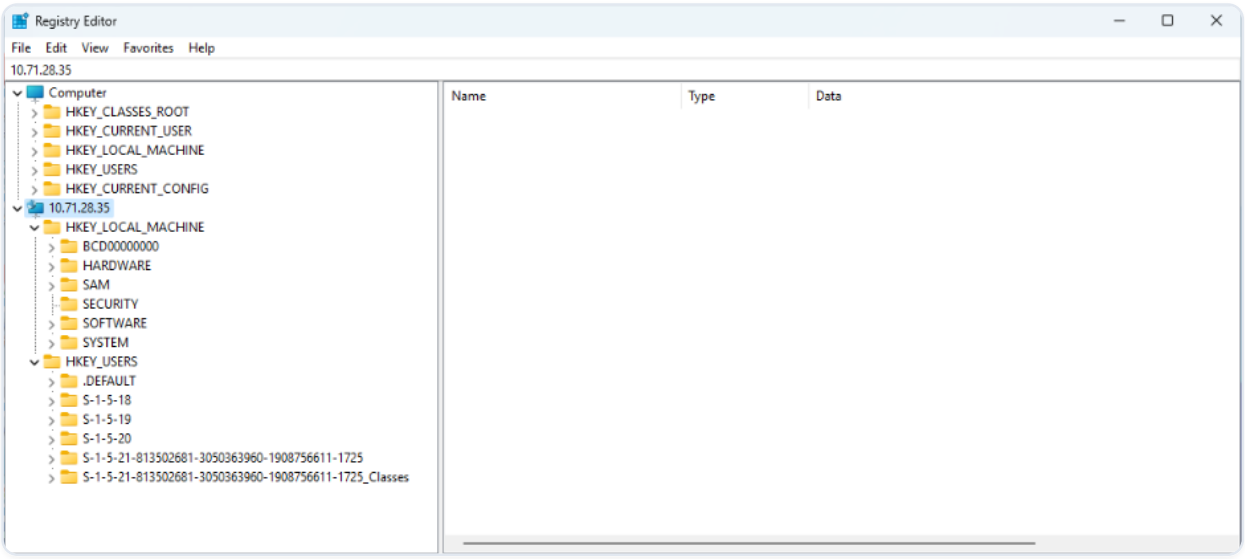
   g. ファイアウォール規則に名前を付け、**完了**を選択して**新しい受信の規則ウィザード**を終了します。



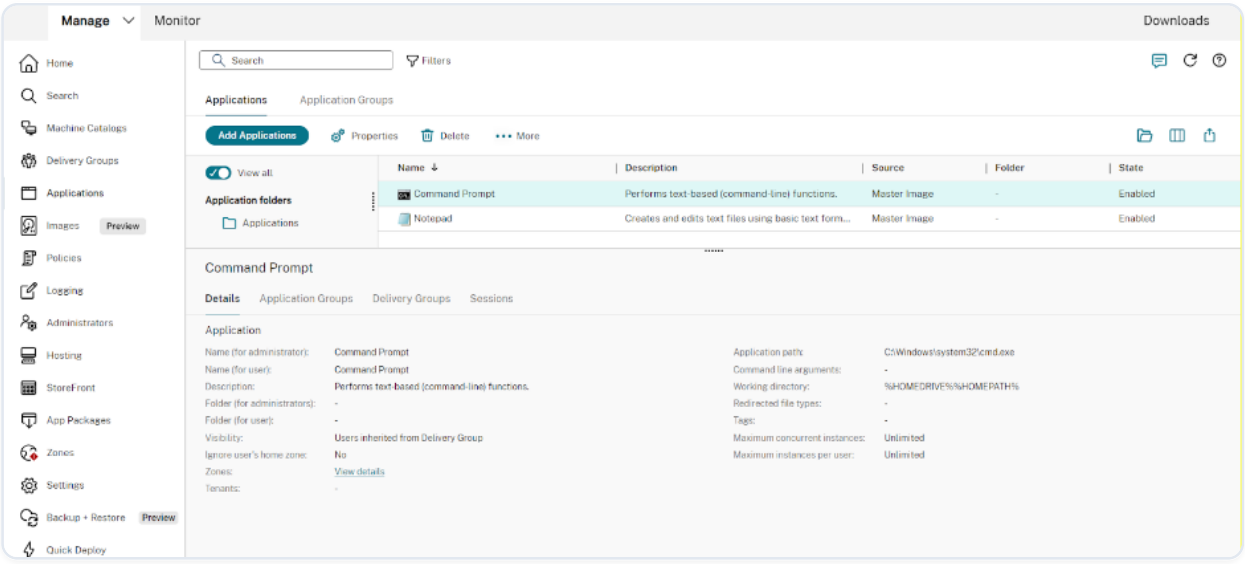
3. 同じドメイン上の別のVM（DC、DDC、または別のVDAでも可）から、`Regedit` を実行し、リモートレジストリに接続します。



4. テスト対象のVDAのIPアドレスを入力し、**OK**をクリックします。`regedit` ツリーには、テスト対象のVDAのブランチが表示されるはずです。



5. **コマンドプロンプト**公開アプリケーションを開きます。



Citrix Workspace に **コマンドプロンプト** アプリが表示されます。

公開アプリのコマンドプロンプト(/en-us/citrix-virtual-apps-desktops/current-release/media/published-app-cmd-prompt.png)

6. クライアントで **Connection Center** を開きます。これは、開いているシームレスアプリを閉じた後にセッションがサインアウトされたときに監視するために使用されます。次の画像では、リモート VDI でコマンドプロンプトプロセス `c:\Windows\system32\cmd.exe` がアクティブになっていることがわかります。

   公開アプリの接続(/en-us/citrix-virtual-apps-desktops/current-release/media/published-app-citrix-workspace-connection-center.png)

7. **regedit** が実行されている VDA から、次のリモート IP の場所に移動します。
   `HKEY_USERS\S-1-X-XX-XXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-XXXX\SOFTWARE\CitrixVolatile\Seamless\Sessions\X\`

> **注:**
>
> 新しいセッションを開くたびにこのパスは変更されます。

8. ここで読み取るキーは 2 つあります (ここでは変更しないでください)。**LogoffCheckBlockingProcess** と **LogoffCheckerBlockingVisibleProcess** です。これらのキーは、サインアウトをブロックしているプログラムを表示します。最初のキーには、それが開いていてまだ閉じられていないため、`C:\Windows\System32\cmd.exe` が表示されているはずです。

   > **注:**
   >
   > **LogoffCheckBlockingProcess** と **LogoffCheckerBlockingVisibleProcess** は手動で編集しないでください。これらのレジストリ値を手動で編集すると、セッションが不安定になる可能性があります。

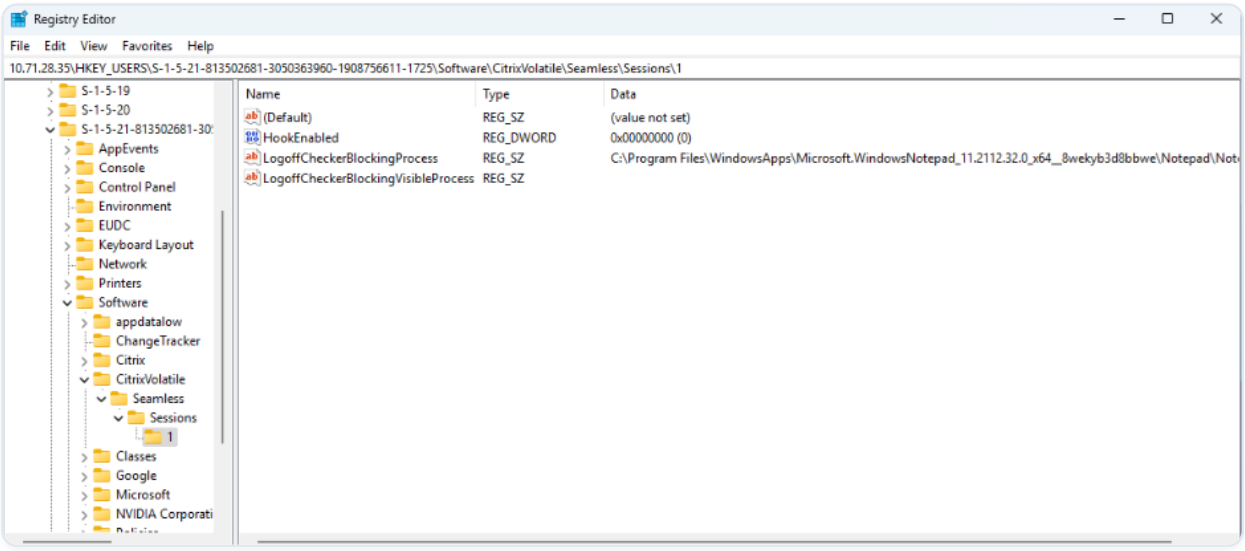
   > 公開アプリ 2(/en-us/citrix-virtual-apps-desktops/current-release/media/published-app-regedit-2.png)

9. 右上隅の **X** をクリックして **Seamless CMD** を終了します。
10. セッションが閉じるかどうか、接続センターを確認します。閉じるまでに最大 30 秒かかる場合があります。閉じれば、正常なサインアウトを妨げたアプリケーションやプロセスはなかったことになります。

    正常なサインアウト(/en-us/citrix-virtual-apps-desktops/current-release/media/published-app-bwd.png)

11. セッションが閉じなかった場合は、F5 キーで **regedit** の出力を更新します。
12. **LogoffCheckBlockingProcess** と **LogoffCheckerBlockingVisibleProcess** の内容を再度確認します。CMD は表示されなくなっているはずですが、別のプロセスが一覧表示されているはずです。現在セッションのサインアウトをブロックしているプロセスがここに表示されているはずです。

    この場合、コマンドプロンプトが閉じられる前に、公開されたコマンドプロンプトから **Notepad.exe** が開かれており、このリモートのメモ帳プロセスが正常なサインアウトを妨げています。



13. この実行可能ファイルへのパスと、それが表示されたキーをメモし、リモートツリーの下にある以下のレジストリキーに入力します。

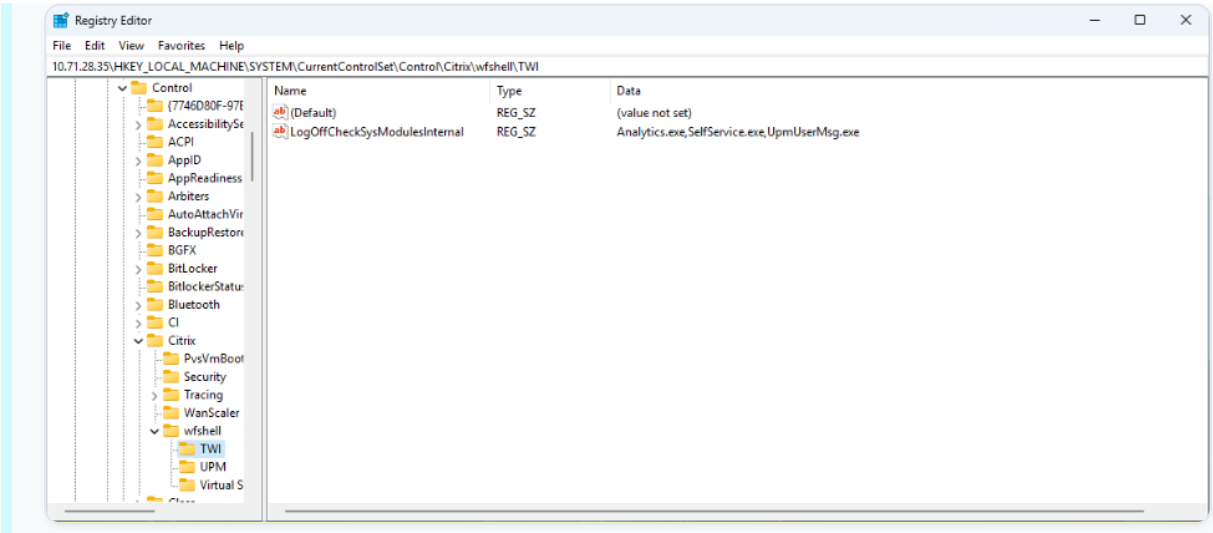
    - **LogoffCheckBlockingProcess** に表示される場合:

      `HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWILogoffCheckSysModulesInterna`

    - **LogoffCheckerBlockingVisibleProcess** に表示される場合:

      `HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWILogoffCheckVisibleSysModules`

> **注:**
>
> キーにすでに1つ以上のエントリがある場合は、末尾にコンマを追加し、そのコンマの後に新しいエントリを配置します。



14. クライアントの接続センターからセッションをサインアウトし、リモートアプリケーションを再度開きます。

15. リモートアプリケーションを閉じてから30秒以内にセッションが自動的にサインアウトされるまで、手順9〜16を繰り返します。

> **注:**
>
> トラブルシューティング後、必要に応じて、リモートレジストリへのアクセスを許可するための一時的なファイアウォールの変更を元に戻します。

公開アプリケーションを開くときにWindowsの免責事項メッセージを全画面表示で見るためにLogonUIを変更する方法

認証パススルーが発生しないシナリオ向けに、**LogonUI**ウィンドウのスケーリングが改善されました。**LogonUI**ウィンドウは、使用されているモニターの解像度とDPI設定に基づいてスケーリングされ、これにより、完全な**LogonUI**ウィンドウがクリッピングなしで表示されることが保証されます。

ピクセル単位のウィンドウサイズは、レジストリで手動で設定することもできます。

1. **ファイル名を指定して実行**コマンドで`regedit`を使用して**レジストリエディター**を開きます。
2. `HKEY_LOCAL_MACHINE\Software\Citrix\CtxHook\AppInit_DLLS\Seamless Hook\`に移動します。
3. 2つの新しいDWORDキー、**LogonUIWidth**と**LogonUIHeight**を作成します。
4. **LogonUI**ウィンドウのキーの値を、必要な幅と高さ（ピクセル単位）に設定します。

   LogonUI ウィンドウのサイズを手動で設定すると、自動スケーリングは無効になります。

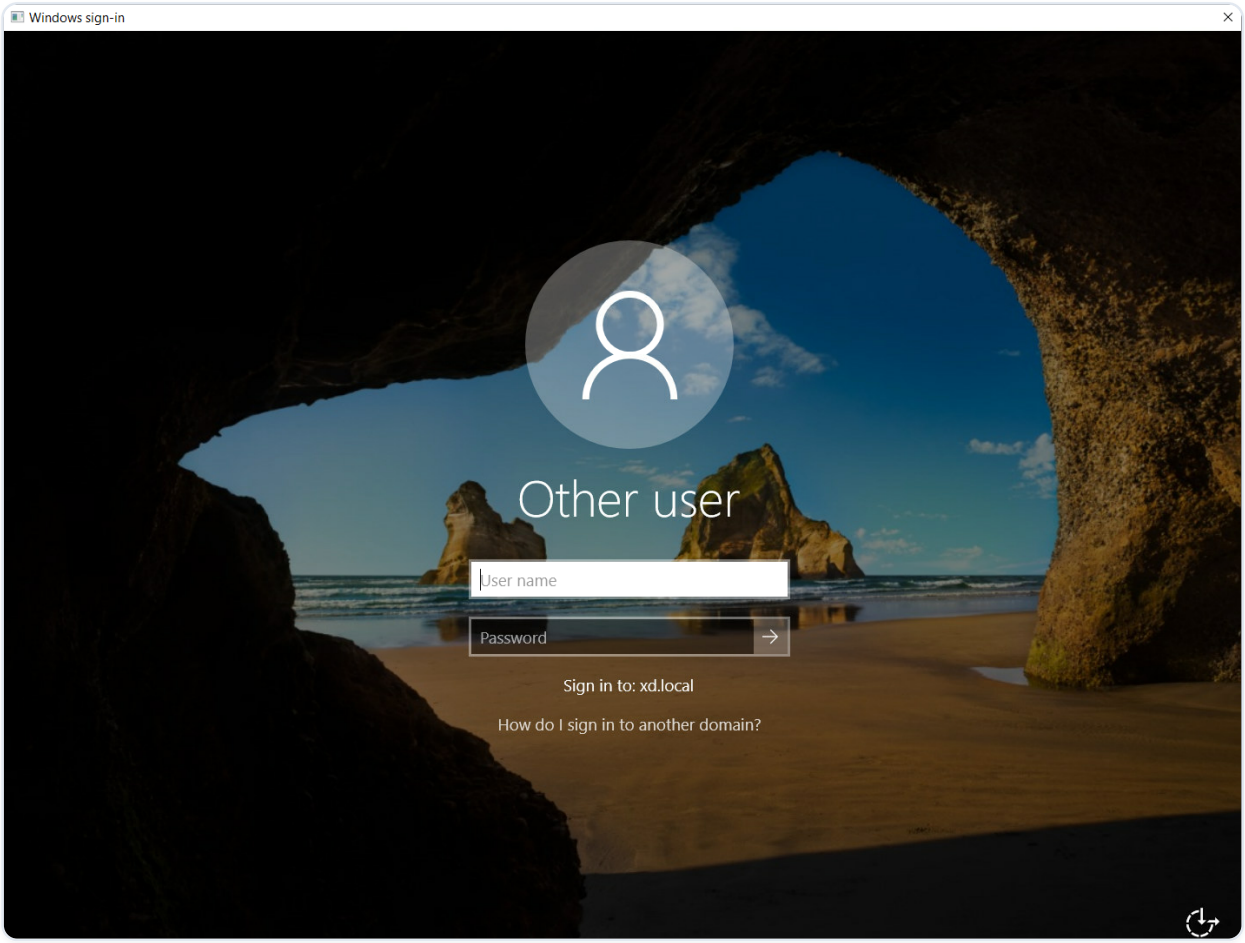
> **注:**
>
> これらのレジストリパスは2407以降変更されました。古いレジストリ値は無視され、非推奨です。

> デフォルトでは、**LogonUI** ウィンドウにはタイトルバーと閉じるボタンが含まれており、必要に応じてエンドユーザーがセッションから切断できるようになっています。

タイルバーを無効にする

LogonUI ウィンドウのタイルバーは、以下のレジストリキーで無効にできます。

1. **ファイル名を指定して実行** コマンドで `regedit` を使用してレジストリエディターを開きます。
2. `HKEY_LOCAL_MACHINE\Software\Citrix\CtxHook\AppInit_DLLS\Seamless Hook\` に移動します。
3. 新しいDWORDキー: **LogonUICaption** を作成し、そのキーの値を `0` に設定します。



公開アプリケーションが表示されない

公開アプリケーションが起動しない、または起動中に消える場合、あるいは表示されない場合のトラブルシューティングについては、サポート記事を参照してください。

インスタンスのトラブルシューティングを行うには

追加のシームレス構成設定

ほとんどの場合、デフォルトのサーバー設定はほとんどのアプリケーションで十分であり、公開アプリケーションに追加の設定は必要ありません。

場合によっては、指定されたアプリケーションウィンドウの対話と表示の制御、および公開アプリケーション環境自体の設定を含む、追加の構成が必要です。

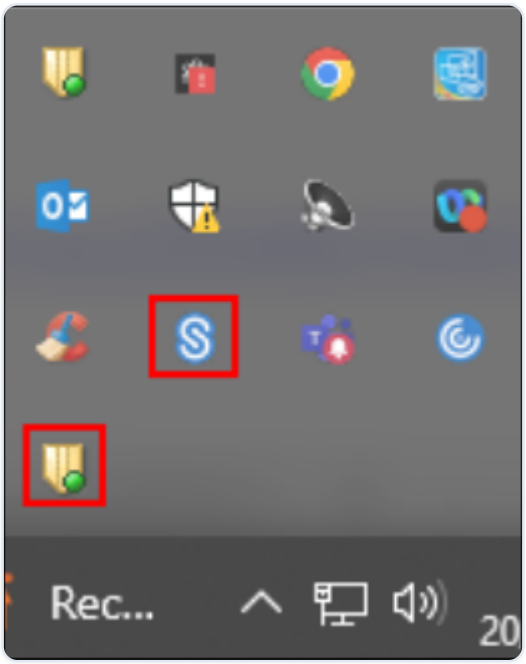
> **注:**
>
> Citrixサポートから明示的に指示されない限り、Citrixはこれらの構成設定を変更することを推奨しません

> これらの設定は、シームレス構成設定KB記事に概説されています。

システムトレイアイコンのリダイレクト

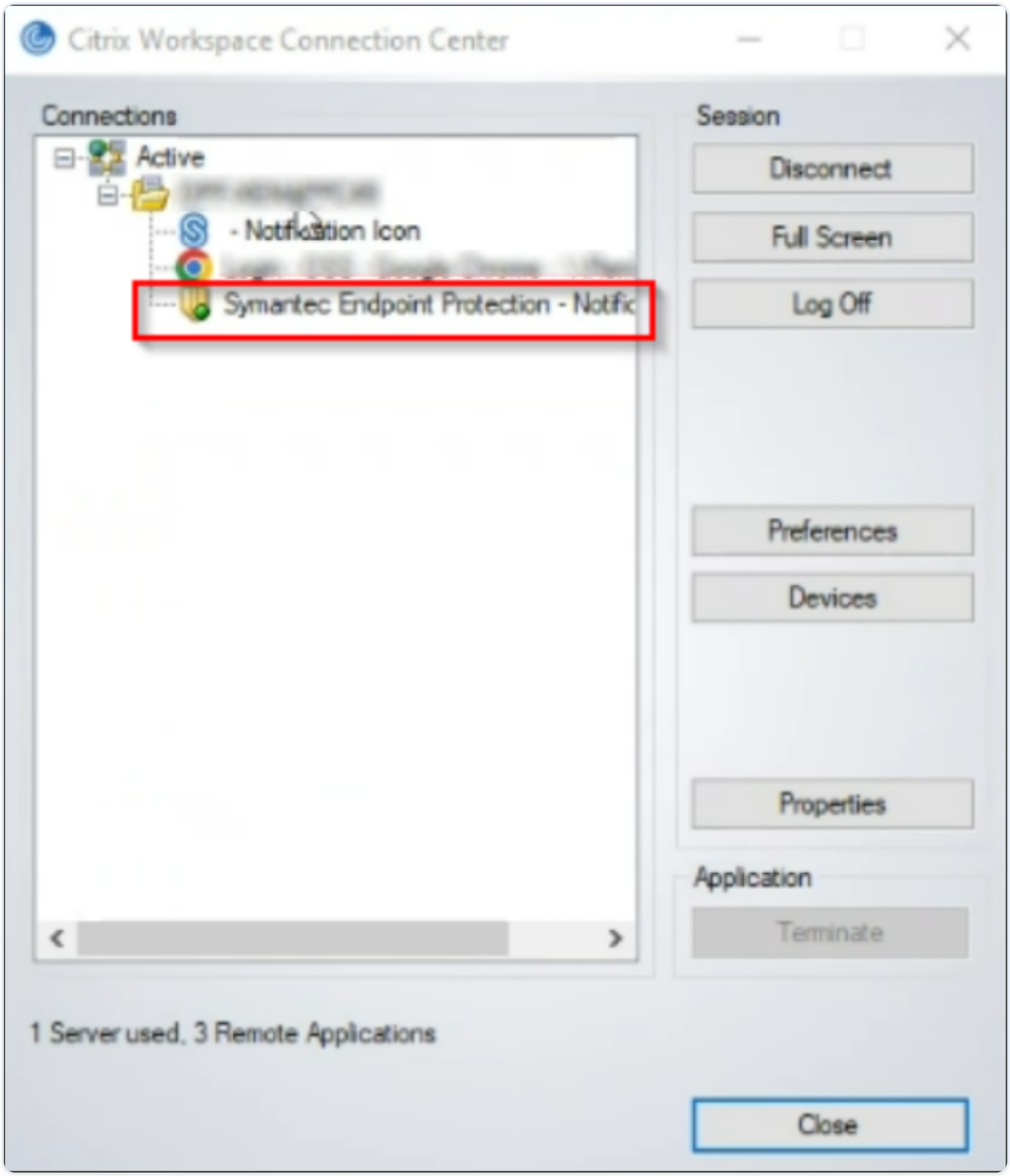
Citrix Virtual Apps and Desktops™ リリース 2212 以降、シームレスアプリケーションを使用している場合、VDA 上にあるリモートのシステムトレイアイコンはクライアントに自動的にリダイレクトされます。

シームレスアプリケーションをホストしている VDA 上のすべてのシステムトレイアイコンは、エンドポイントにリダイレクトされます。



上記の例では、Sharefile と Symantec のマークされたシステムトレイアイコンが VDA からクライアントにリダイレクトされています。

これらのアイコンは、Citrix Workspace™ Connection Center にも表示されます。



エンドユーザーは、これらのリダイレクトされたシステムトレイアイコンを、ローカルのシステムトレイアイコンと同じ方法で操作できます。

異なる VDA でホストされているシームレスアプリケーションを使用している場合、VDA が同一のシステムトレイアイコンを持っていると、エンドポイントに重複するシステムトレイアイコンが表示される可能性があります。

この動作はデフォルトで有効になっており、現在は構成できません。

マルチメディア

HDX™ テクノロジースタックは、2つの補完的なアプローチを通じてマルチメディアアプリケーションの配信をサポートします。

- サーバー側レンダリングによるマルチメディア配信
- クライアント側レンダリングによるマルチメディアリダイレクト

この戦略により、優れたユーザーエクスペリエンスで幅広いマルチメディア形式を配信できると同時に、サーバーのスケーラビリティを最大化してユーザーあたりのコストを削減できます。

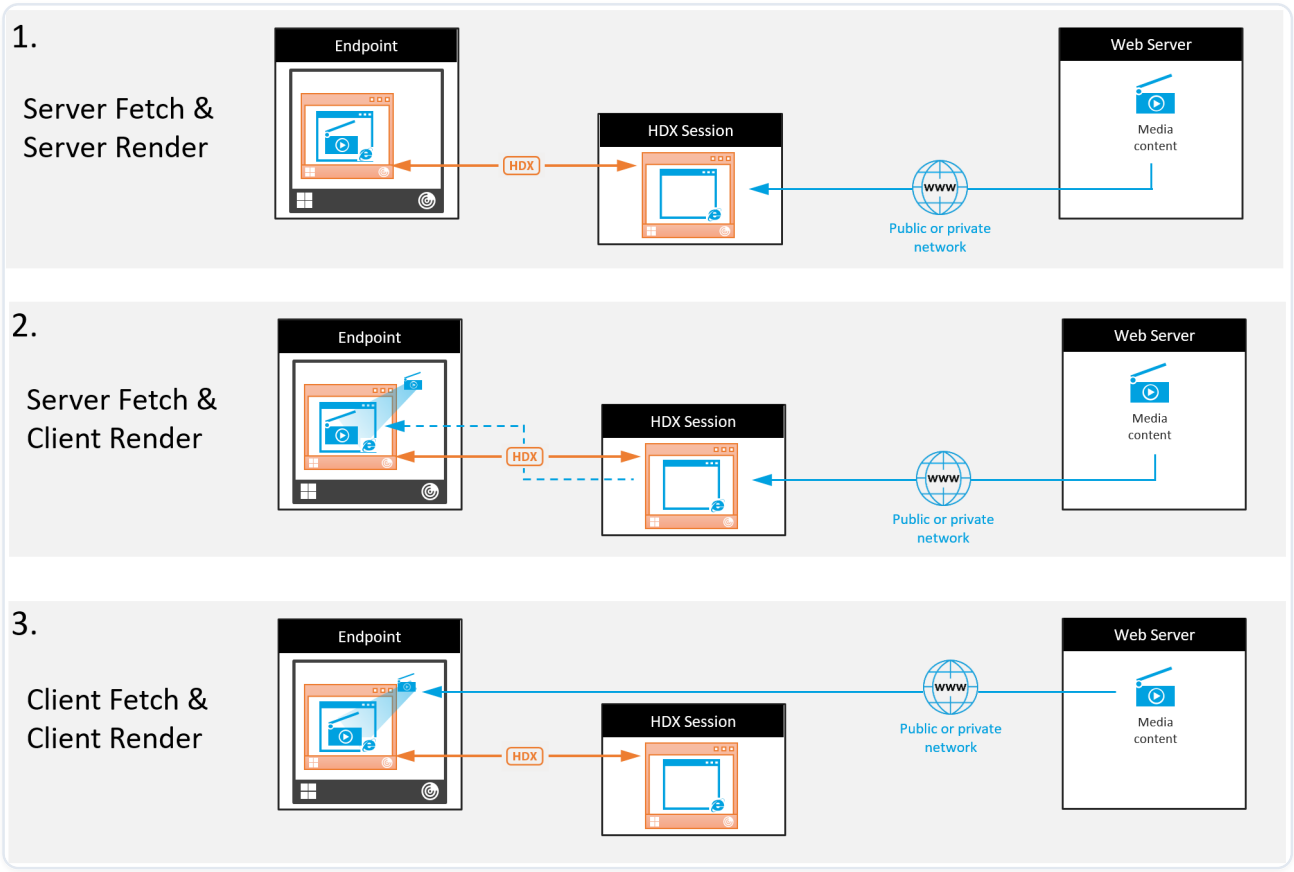
サーバー側でレンダリングされるマルチメディア配信では、オーディオおよびビデオコンテンツはアプリケーションによってCitrix Virtual Apps and Desktopsサーバー上でデコードおよびレンダリングされます。その後、コンテンツは圧縮され、ICAプロトコルを使用してユーザーデバイス上のCitrix Workspaceアプリに配信されます。この方法は、さまざまなアプリケーションおよびメディア形式との互換性を最大限に高めます。ビデオ処理は計算負荷が高いため、サーバー側でレンダリングされるマルチメディア配信は、オンボードのハードウェアアクセラレーションから大きな恩恵を受けます。たとえば、DirectX Video Acceleration (DXVA) のサポートにより、H.264デコードを個別のハードウェアで実行することでCPUの負荷を軽減します。Intel Quick Sync、AMD RapidFire、NVIDIA NVENCテクノロジーは、ハードウェアアクセラレーションによるH.264エンコーディングを提供します。

ほとんどのサーバーはビデオ圧縮のためのハードウェアアクセラレーションを提供しないため、すべてのビデオ処理がサーバーCPUで行われる場合、サーバーのスケーラビリティは悪影響を受けます。多くのマルチメディア形式をローカルレンダリングのためにユーザーデバイスにリダイレクトすることで、高いサーバーのスケーラビリティを維持できます。

- Windows Mediaリダイレクトは、通常Windows Media Playerに関連付けられているさまざまなメディア形式について、サーバーの負荷を軽減します。
- HTML5ビデオは普及しており、Citrix®はこの種のコンテンツ向けにリダイレクトテクノロジーを導入しました。HTML5、HLS、DASH、またはWebRTCを使用するWebサイトには、ブラウザコンテンツリダイレクトをお勧めします。
- 一般的なコンテンツリダイレクトテクノロジーであるホストからクライアントへのリダイレクトとローカルアプリアクセスをマルチメディアコンテンツに適用できます。

これらのテクノロジーを組み合わせると、リダイレクトを設定しない場合、HDXはサーバー側レンダリングを実行します。 リダイレクトを設定した場合、HDXはサーバーフェッチとクライアントレンダリング、またはクライアントフェッチとクライアントレンダリングのいずれかを使用します。これらの方法が失敗した場合、HDXは必要に応じてサーバー側レンダリングにフォールバックし、フォールバック防止ポリシーの対象となります。

シナリオ例



シナリオ1. (サーバーフェッチとサーバーレンダリング):

1. サーバーはソースからメディアファイルを取得し、デコードしてから、オーディオデバイスまたはディスプレイデバイスにコンテンツを提示します。
2. サーバーは、提示された画像またはサウンドをそれぞれディスプレイデバイスまたはオーディオデバイスから抽出します。
3. サーバーはオプションでそれを圧縮し、その後クライアントに送信します。

このアプローチでは、高いCPUコスト、高い帯域幅コスト（抽出された画像/音声が効率的に圧縮されていない場合）、および低いサーバー拡張性が発生します。

Thinwireおよびオーディオ仮想チャネルがこのアプローチを処理します。このアプローチの利点は、クライアントのハードウェアおよびソフトウェア要件を削減できることです。このアプローチ

を使用すると、デコードはサーバーで行われ、より幅広い種類のデバイスとフォーマットで動作します。

シナリオ2。（サーバーフェッチとクライアントレンダリング）：

このアプローチは、メディアコンテンツがデコードされ、オーディオまたはディスプレイデバイスに提示される前に傍受できることに依存しています。圧縮されたオーディオ/ビデオコンテンツは代わりにクライアントに送信され、そこでローカルでデコードおよび提示されます。このアプローチの利点は、クライアントデバイスにオフロードされ、サーバーのCPUサイクルを節約できることです。

しかし、これはクライアントに追加のハードウェアおよびソフトウェア要件ももたらします。クライアントは、受信する可能性のある各フォーマットをデコードできる必要があります。

シナリオ3。（クライアントフェッチとクライアントレンダリング）：

このアプローチは、メディアコンテンツのURLがソースからフェッチされる前に傍受できることに依存しています。URLはクライアントに送信され、そこでメディアコンテンツがフェッチ、デコード、およびローカルで提示されます。このアプローチは概念的にシンプルです。その利点は、サーバーが制御コマンドのみを送信するため、サーバーのCPUサイクルと帯域幅の両方を節約できることです。ただし、メディアコンテンツが常にクライアントからアクセスできるとは限りません。

フレームワークとプラットフォーム：

シングルセッションオペレーティングシステム（Windows、Mac OS X、Linux）は、マルチメディアアプリケーションのより迅速な開発を可能にするマルチメディアフレームワークを提供します。この表は、より一般的なマルチメディアフレームワークの一部をリストしています。各フレームワークは、メディア処理をいくつかの段階に分け、パイプラインベースのアーキテクチャを使用します。

フレームワーク	プラットフォーム
DirectShow	Windows (98以降)
メディア ファンデーション	ウィンドウズ (ビスタ以降)
Gストリーマー	リナックス
クイックタイム	マック オーエス テン

メディアリダイレクト技術によるダブルホップサポート

オーディオリダイレクト	いいえ
ブラウザコンテンツリダイレクト	いいえ
HDX Webカメラリダイレクト	はい
HTML5ビデオのリダイレクト	はい
Windows Mediaリダイレクト	はい

オーディオ機能

HDXオーディオ機能を最適化するポリシーに、以下のCitrixポリシー設定を構成して追加できます。使用方法の詳細、および他のポリシー設定との関係と依存関係については、「オーディオポリシー設定」、「帯域幅ポリシー設定」、および「マルチストリーム接続ポリシー設定」を参照してください。

アダプティブオーディオ

アダプティブオーディオを使用すると、VDAでオーディオ品質ポリシーを手動で構成する必要がありません。アダプティブオーディオは、環境に合わせて設定を最適化し、古いオーディオ圧縮形式を置き換えて、優れたユーザーエクスペリエンスを提供します。

アダプティブオーディオはデフォルトで有効になっています。アダプティブオーディオを無効にするには、「オーディオポリシー設定」を参照してください。

重要:

リアルタイムオーディオアプリケーションが必要な場合、Citrix®はTCPではなくUser Datagram Protocol（UDP）を使用してオーディオを配信することを推奨します。UDP経由で利用できるオーディオトランスポートオプションは次のとおりです。

- UDP経由のオーディオ
- HDX™ アダプティブ トランスポート (エンライトンド データ トランスポート)

DTLSを使用したUDPオーディオ暗号化は、Citrix GatewayとCitrix Workspace™ appの間でのみ利用可能です。そのため、TCPトランスポートを使用する方が望ましい場合があります。TCPは、VDAからCitrix Workspace appへのエンドツーエンドのTLS暗号化をサポートします。

アダプティブオーディオとUDPオーディオの詳細については、「UDPリアルタイムトランスポート経由のオーディオとオーディオUDPポート範囲」を参照してください。

オーディオのロストレラントモード

バージョン2308以降、損失許容モードがオーディオをサポートするようになりました。この機能は、リアルタイムストリーミングのユーザーエクスペリエンスを向上させ、ユーザーが遅延やパケット損失のあるネットワーク経由で接続している場合のEDTでのオーディオ品質を改善します。

損失許容モードとEDTの詳細については、Citrix Virtual Apps and Desktopsドキュメントの「追加情報」を参照してください。

オーディオの損失許容モードはデフォルトで有効になっています。無効になっている場合、または再度有効にする場合は、次の手順を実行します。

1. HDXアダプティブトランスポート（EDT）を有効にします。
2. オーディオの損失許容モードを有効にします。

クライアントの要件と設定

損失許容モードをサポートするCitrix Workspaceアプリの最小バージョンは次のとおりです。

- Windows向けCitrix Workspaceアプリ 2309
- Linux向けCitrix Workspaceアプリ 2311
- Mac向けCitrix Workspaceアプリ 2311

さらに、以下にご注意ください。

- (オプション) Citrix WorkspaceアプリとVDA間の直接接続の場合、VDAでDTLSを有効にするが必要です。
- (オプション) リモート接続の場合、Citrix Gateway ServiceまたはNetScaler Gatewayでも損失許容モードがサポートされている必要があります。

オーディオ品質

一般的に、音質が高いほど、より多くのオーディオデータをユーザーデバイスに送信するため、より多くの帯域幅とサーバーCPU使用率を消費します。サウンド圧縮を使用すると、音質とセッション全体のパフォーマンスのバランスを取ることができます。Citrixポリシー設定を使用して、サウンドファイルに適用する圧縮レベルを構成します。

デフォルトでは、TCPトランスポートが使用されている場合、**オーディオ品質ポリシー**設定は「高 - 高精細オーディオ」に設定されています。UDPトランスポート（推奨）が使用されている場合、ポリシーは「中 - 音声に最適化」に設定されます。**高精細オーディオ**設定は、高忠実度のステレオオーディオを提供しますが、他の品質設定よりも多くの帯域幅を消費します。最適化されていない音声チャットまたはビデオチャットアプリケーション（ソフトフォンなど）には、このオーディオ品質を使用しないでください。その理由は、リアルタイム通信に適さない遅延をオーディオパスに導入する可能性があるためです。選択されたトランスポートプロトコルに関係なく、リアルタイムオーディオには音声に最適化されたポリシー設定を推奨します。

帯域幅が制限されている場合（衛星接続やダイヤルアップ接続など）は、オーディオ品質を**Low**に下げると、消費される帯域幅が最小限になります。この状況では、低帯域幅接続のユーザー向けに個別のポリシーを作成し、高帯域幅接続のユーザーが悪影響を受けないようにします。

設定の詳細については、「オーディオポリシー設定」を参照してください。ユーザーデバイスでClient audio settingsを有効にすることを忘れないでください。

オーディオ再生と録音の帯域幅ガイドライン：

- アダプティブオーディオ（デフォルト。VoIPおよびすべてのユースケースに推奨）
    - ビットレート: 可変アダプティブ
    - チャンネル数: 再生用2（ステレオ）、マイクキャプチャ用1（モノラル）
    - 周波数: 48000 Hz
    - ビット深度: 16ビット
- 高音質
    - ビットレート：再生で約100 kbps（最小75、最大175 kbps）/マイクキャプチャで約70 kbps
    - チャンネル数：再生で2（ステレオ）、マイクキャプチャで1（モノラル）
    - 周波数：44100 Hz
    - ビット深度: 16ビット

- 中品質
  - ビットレート: 再生時 ~16 kbps (最小20 kbps、最大40 kbps)、マイクキャプチャ時 ~16 kbps
  - チャンネル数: 再生とキャプチャの両方で1 (モノラル)
  - 周波数: 16000 Hz (広帯域)
  - ビット深度: 16ビット
- 低品質
  - ビットレート: 再生時 ~11 kbps (最小10 kbps、最大25 kbps)、マイクキャプチャ時 ~11 kbps
  - チャンネル数: 再生とキャプチャの両方で1 (モノラル)
  - 周波数: 8000 Hz (狭帯域)
  - ビット深度: 16ビット

EDT損失許容モード用オーディオ品質エンハンサー

2507バージョン以降、EDTを介したアダプティブオーディオの場合、オーディオ品質エンハンサーはデフォルトで有効になっていますオーディオのロス許容モード。

オーディオ品質エンハンサーは、短時間のネットワーク中断中もクリアなオーディオを維持します。この機能は、ネットワークの状態に適応し、再生中および録音中の一貫したオーディオパフォーマンスを保証します。

> **注:**
>
> この機能が動作するには、適応型オーディオを有効にする必要があります。

クライアントオーディオリダイレクト

ユーザーデバイス上のスピーカーまたはその他のサウンドデバイスを介して、サーバー上のアプリケーションからオーディオを受信できるようにするには、**クライアントオーディオリダイレクト**設定を**許可**のままにします。これはデフォルトです。

クライアントオーディオマッピングは、サーバーとネットワークに余分な負荷をかけます。ただし、クライアントオーディオリダイレクトを禁止すると、すべてのHDXオーディオ機能が無効になります。

設定の詳細については、「オーディオポリシー設定」を参照してください。ユーザーデバイスでクライアントオーディオ設定を有効にすることを忘れないでください。

クライアントマイクのリダイレクト

ユーザーデバイス上のマイクなどの入力デバイスを使用してユーザーがオーディオを録音できるようにするには、**クライアントマイクのリダイレクト**設定をデフォルト（許可）のままにします。

セキュリティのため、ユーザーデバイスは、信頼できないサーバーがマイクへのアクセスを試みた場合に、ユーザーに警告します。ユーザーはマイクを使用する前に、アクセスを許可するか拒否するかを選択できます。ユーザーはCitrix Workspaceアプリでこの警告を無効にできます。

設定の詳細については、「オーディオポリシー設定」を参照してください。ユーザーデバイスでClient audio settingsを有効にすることを忘れないでください。

オーディオプラグアンドプレイ

オーディオプラグアンドプレイポリシー設定は、複数のオーディオデバイスを使用してサウンドを録音および再生することを許可または禁止します。この設定は、デフォルトで**有効**になっています。オーディオプラグアンドプレイにより、オーディオデバイスが認識されるようになります。ユーザーセッションが開始されるまで接続されていなくても、デバイスは認識されます。

この設定は、WindowsマルチセッションOSマシンにのみ適用されます。

設定の詳細については、「オーディオポリシー設定」を参照してください。

オーディオリダイレクト帯域幅制限とオーディオリダイレクト帯域幅制限の割合

オーディオリダイレクト帯域幅制限ポリシー設定は、セッションでのオーディオの再生と録音の最大帯域幅（キロビット/秒）を指定します。

オーディオリダイレクト帯域幅制限の割合設定は、オーディオリダイレクトの最大帯域幅を、利用可能な総帯域幅の割合として指定します。

デフォルトでは、両方の設定でゼロ（最大なし）が指定されています。両方の設定が構成されている場合、帯域幅制限が最も低い方が使用されます。

設定の詳細については、「帯域幅ポリシー設定」を参照してください。ユーザーデバイスでクライアントオーディオ設定を有効にすることを忘れないでください。

UDPリアルタイムトランスポート経由のオーディオとオーディオUDPポート範囲

デフォルトでは、ユーザーデータグラムプロトコル（UDP）リアルタイムトランスポート経由のオーディオは許可されています（インストール時に選択した場合）。これは、UDPリアルタイムトランスポート経由のオーディオを使用する接続のために、サーバー上にUDPポートを開きます。ネットワークの輻輳やパケット損失がある場合は、可能な限り最高のユーザーエクスペリエンスを確保するために、オーディオにUDP/RTPを構成することをお勧めします。ソフトフォンアプリケーションなどのリアルタイムオーディオの場合、EDTよりもUDPオーディオが推奨されます。UDPは再送信なしでパケット損失を許容するため、パケット損失が多い接続で遅延が追加されることはありません。

重要:

Citrix Gatewayが経路にない場合、UDPで送信されるオーディオデータは暗号化されません。Citrix GatewayがCitrix Virtual Apps and Desktops™リソースにアクセスするように構成されている場合、エンドポイントデバイスとCitrix Gateway間のオーディオトラフィックはDTLSプロトコルを使用して保護されます。

オーディオUDPポート範囲は、Windows VDAがユーザーデバイスとオーディオパケットデータを交換するために使用するポート番号の範囲を指定します。

デフォルトでは、範囲は16500から16509です。

注:

適応型オーディオにUDPリアルタイムトランスポート経由のオーディオが必要ない場合、Citrixはポリシー設定を「無効」に構成することを推奨します。これにより、Citrix WorkspaceアプリクライアントがUDP接続のオープンを要求したり、不要なCitrix Workspaceアプリクライアントのファイアウォール構成ダイアログウィンドウが表示されたりするのを防ぐことができます。

UDPリアルタイムトランスポート経由のオーディオに関する設定の詳細については、オーディオポリシー設定を参照してください。オーディオUDPポート範囲の詳細については、マルチストリーム接続ポリシー設定を参照してください。ユーザーデバイスでクライアントオーディオ設定を有効にすることを忘れないでください。

UDP経由のオーディオにはWindows VDAが必要です。Linux VDAでサポートされているポリシーについては、ポリシーサポートリストを参照してください。

ユーザーデバイスのオーディオ設定ポリシー

1. グループポリシーオブジェクト管理用テンプレートの構成に従って、グループポリシーテンプレートをロードします。
2. グループポリシーエディターで、**管理用テンプレート > Citrixコンポーネント > Citrix Workspace > ユーザーエクスペリエンス**を展開します。
3. **クライアントオーディオ設定**で、**未構成**、**有効**、または**無効**を選択します。
   - **未構成**。デフォルトでは、オーディオリダイレクトは高品質オーディオまたは以前に構成されたカスタムオーディオ設定を使用して有効になっています。
   - **有効**。選択したオプションを使用してオーディオリダイレクトを有効にします。
   - **無効**。オーディオリダイレクトを無効にします。
4. **有効**を選択した場合、音質を選択します。UDPオーディオの場合は、**中**（デフォルト）を使用します。
5. UDPオーディオの場合のみ、**リアルタイムトランスポートを有効にする**を選択し、ローカルのWindowsファイアウォールで開く受信ポートの範囲を設定します。
6. Citrix Gateway で UDP Audio を使用するには、**Allow Real-Time Transport Through gateway** を選択します。Citrix Gateway を DTLS で構成します。詳細については、こちらの記事を参照してください。

管理者として、これらの変更を行うためのエンドポイントデバイスを制御できない場合は、StoreFront の default.ica 属性を使用して UDP Audio を有効にします。たとえば、BYOD (個人所有デバイス) や自宅のコンピューターの場合などです。

1. StoreFront マシンで、メモ帳などのエディターを使用して C:\inetpub\wwwroot\Citrix\\\<Store Name>\App_Data\default.ica を開きます。
2. セクションに以下のエントリを作成します。

   ; このテキストはリアルタイムトランスポートを有効にします

   RTPオーディオを有効にする=true

   ; このテキストはゲートウェイ経由のリアルタイムトランスポートを許可します

   ゲートウェイ経由のUDPを有効にする=true

; このテキストはオーディオ品質を「中」に設定します

AudioBandwidthLimit=1

; UDP ポート範囲

RtpAudioLowestPort=16500

RtpAudioHighestPort=16509

default.ica を編集してユーザーデータグラムプロトコル (UDP) オーディオを有効にすると、そのストアを使用しているすべてのユーザーに対して UDP オーディオが有効になります。

マルチメディア会議中のエコーを回避する

オーディオまたはビデオ会議のユーザーはエコーを聞くことがあります。エコーは通常、スピーカーとマイクが互いに近すぎるときに発生します。そのため、オーディオおよびビデオ会議にはヘッドセットの使用をお勧めします。

HDXは、エコーを最小限に抑えるエコーキャンセレーションオプション（デフォルトで有効）を提供します。エコーキャンセレーションの有効性は、スピーカーとマイクの間の距離に影響されます。デバイスが互いに近すぎたり遠すぎたりしないようにしてください。

レジストリ設定を変更して、エコーキャンセレーションを無効にできます。詳細については、レジストリを介して管理される機能のリストにあるマルチメディア会議中のエコーを回避するを参照してください。

ソフトフォン

ソフトフォンは、電話インターフェースとして機能するソフトウェアです。ソフトフォンを使用して、コンピューターやその他のスマートデバイスからインターネット経由で電話をかけます。ソフトフォンを使用すると、画面を使って電話番号をダイヤルしたり、その他の電話関連機能を実行したりできます。

Citrix Virtual Apps and Desktops™は、ソフトフォンの配信のためにいくつかの代替手段をサポートしています。

- **制御モード**。ホストされているソフトフォンが物理的な電話機を制御します。このモードでは、Citrix Virtual Apps and Desktopsサーバーを介してオーディオトラフィックは流れません。
- **HDX RealTime最適化ソフトフォンサポート（推奨）**。メディアエンジンはユーザーデバイス上で実行され、Voice over Internet Protocolトラフィックはピアツーピアで流れます。例については、以下を参照してください。

  - Microsoft Teams向けHDX最適化
  - HDX RealTime Optimization Pack（Microsoft Skype for Businessの配信を最適化します）
  - Cisco Jabber Softphone for VDI (シスコ ジャバー ソフトフォン フォー VDI)（旧称VXME）
  - VDI向け シスコ Webex ミーティング
  - Avaya VDI Equinox (アバイア VDI エクイノックス)（旧称VDI Communicator）
  - Zoom VDI Plugin (ズーム VDI プラグイン)
  - Genesys PureEngage クラウド
  - Nuance Dragon PowerMic ディクテーションデバイス

- **ローカルアプリアクセス**。Citrix Virtual Apps and Desktopsの機能で、ソフトフォンなどのアプリケーションをWindowsユーザーデバイス上でローカルに実行しながら、仮想/公開デスクトップとシームレスに統合されているように見せることができます。この機能は、すべてのオーディオ処理をユーザーデバイスにオフロードします。詳細については、「ローカルアプリアクセスとURLリダイレクト」を参照してください。
- **HDX RealTime汎用ソフトフォンサポート**。ICA経由のVoice over Internet Protocol。

汎用ソフトフォンサポート

汎用ソフトフォンサポートにより、データセンターのXenAppまたはXenDesktopで、変更されていないソフトフォンをホストできます。オーディオトラフィックは、Citrix ICAプロトコル（できればUDP/RTPを使用）を介して、Citrix Workspaceアプリを実行しているユーザーデバイスに送信されます。

汎用ソフトフォンサポートは、HDX RealTimeの機能です。このソフトフォン配信アプローチは、特に次の場合に役立ちます。

- ソフトフォンを配信するための最適化されたソリューションが利用できず、ユーザーがLocal App Accessを使用できるWindowsデバイスを使用していない場合。
- ソフトフォンの最適化された配信に必要なメディアエンジンがユーザーデバイスにインストールされていないか、ユーザーデバイスで実行されているオペレーティングシステムのバージョンで利用できない場合。このシナリオでは、汎用HDX RealTimeが貴重なフォールバックソリューションを提供します。

Citrix Virtual Apps and Desktopsを使用する際のソフトフォン配信には、次の2つの考慮事項があります。

- ソフトフォンアプリケーションが仮想/公開デスクトップにどのように配信されるか。

- ユーザーのヘッドセット、マイク、スピーカー、またはUSB電話機にオーディオがどのように配信されるか。

Citrix Virtual Apps and Desktopsには、汎用ソフトフォン配信をサポートするための多数のテクノロジーが含まれています。

- リアルタイムオーディオの高速エンコードと帯域幅効率のためのOptimized-for-Speechコーデック。
- 低遅延オーディオスタック。
- ネットワーク遅延が変動したときにオーディオをスムーズにするサーバー側ジッターバッファ。
- サービス品質のためのパケットタグ付け (DSCP および WMM)。
    - RTPパケットのDSCPタグ付け (レイヤー3)
    - Wi-FiのWMMタグ付け

Windows、Linux、Chrome、Mac版のCitrix Workspaceアプリも、Voice over Internet Protocolに対応しています。Windows版Citrix Workspaceアプリは、以下の機能を提供します。

- クライアント側のジッターバッファ - ネットワーク遅延が変動しても、スムーズなオーディオを保証します。
- エコーキャンセル - ヘッドセットを使用しない作業者向けに、マイクとスピーカー間の距離の変動を大きく許容します。
- オーディオプラグアンドプレイ - オーディオデバイスは、セッションを開始する前に接続する必要はありません。いつでも接続できます。
- オーディオデバイスルーティング - ユーザーは着信音をスピーカーに、音声パスをヘッドセットにルーティングできます。
- マルチストリームICA - ネットワーク上で柔軟なサービス品質ベースのルーティングを可能にします。
- ICAは4つのTCPストリームと2つのUDPストリームをサポートします。UDPストリームの1つは、RTPを介したリアルタイムオーディオをサポートします。

Citrix Workspaceアプリの機能の概要については、Citrix Receiver Feature Matrixを参照してください。

システム構成の推奨事項

クライアントハードウェアとソフトウェア: 最適なオーディオ品質を得るには、最新バージョンのCitrix Workspaceアプリと、音響エコーキャンセル (AEC) 機能を備えた高品質のヘッドセットをお勧めします。Windows、Linux、Mac版のCitrix Workspaceアプリは、Voice over Internet Protocolをサポートしています。また、Dell WyseはThinOS (WTOS) 向けにVoice over Internet Protocolをサポートしています。

CPUに関する考慮事項: VDAのCPU使用率を監視して、各仮想マシンに2つの仮想CPUを割り当てる必要があるかどうかを判断します。リアルタイムの音声とビデオはデータ集約型です。2つの仮想CPUを構成すると、スレッド切り替えの遅延が減少します。したがって、Citrix Virtual Desktops™ VDI環境では2つのvCPUを構成することをお勧めします。

2つの仮想CPUを持つことは、物理CPUの数を2倍にすることを必ずしも意味しません。物理CPUはセッション間で共有できるためです。

Citrix Gateway Protocol (CGP) は、セッション信頼性機能に使用され、CPU 消費も増加させます。高品質のネットワーク接続では、VDA の CPU 消費を削減するためにこの機能を無効にできます。強力なサーバーでは、上記のいずれのステップも不要な場合があります。

UDPオーディオ: UDP経由のオーディオは、ネットワークの輻輳とパケット損失に対して優れた耐性を提供します。利用可能な場合は、TCPの代わりにこれをお勧めします。

LAN/WAN構成: 良好なリアルタイムオーディオ品質のためには、ネットワークの適切な構成が不可欠です。通常、過剰なブロードキャストパケットはジッターを引き起こす可能性があるため、仮想LAN (VLAN) を構成する必要があります。IPv6対応デバイスは多くのブロードキャストパケットを生成する可能性があります。IPv6サポートが不要な場合は、それらのデバイスでIPv6を無効にできます。Quality of Serviceをサポートするように構成してください。

WAN接続の使用設定: LANおよびWAN接続を介してボイスチャットを使用できます。WAN接続では、オーディオ品質は接続の遅延、パケット損失、およびジッターに依存します。WAN接続のユーザーにソフトフォンを配信する場合、データセンターとリモートオフィス間でNetScaler® SD-WANを使用することをお勧めします。これにより、高いQuality of Serviceが維持されます。NetScaler SD-WANは、UDPを含むMulti-Stream ICAをサポートしています。また、単一のTCPストリームの場合、さまざまなICA仮想チャネルの優先順位を区別して、高優先度のリアルタイムオーディオデータが優先的に処理されるようにすることが可能です。

DirectorまたはHDX Monitorを使用して、HDX構成を検証します。

リモートユーザー接続: Citrix Gatewayは、UDP/RTPトラフィックをネイティブに（TCPでのカプセル化なしで）配信するためにDTLSをサポートしています。 ポート443経由のUDPトラフィックに対してファイアウォールを双方向に開きます。

コーデックの選択と帯域幅の消費: ユーザーデバイスとデータセンター内のVDAの間では、**Optimized-for-Speech**コーデック設定（中品質オーディオとも呼ばれます）を使用することをお勧めします。VDAプラットフォームとIP-PBXの間では、ソフトフォンは構成またはネゴシエートされたコーデックを使用します。例：

- G711は良好な音声品質を提供しますが、1コールあたり80キロビット/秒から100キロビット/秒の帯域幅要件があります（ネットワークレイヤー2のオーバーヘッドに依存）。
- G729は良好な音声品質を提供し、1コールあたり30キロビット/秒から40キロビット/秒の低い帯域幅要件があります（ネットワークレイヤー2のオーバーヘッドに依存）。

仮想デスクトップへのソフトフォンアプリケーションの配信

XenDesktop®仮想デスクトップにソフトフォンを配信するには、2つの方法があります。

- アプリケーションは仮想デスクトップイメージにインストールできます。
- アプリケーションはMicrosoft App-Vを使用して仮想デスクトップにストリーミングできます。このアプローチには、仮想デスクトップイメージが整理された状態に保たれるため、管理上の利点があります。仮想デスクトップにストリーミングされた後、アプリケーションは通常の方法でインストールされたかのようにその環境で実行されます。すべてのアプリケーションがApp-Vと互換性があるわけではありません。

ユーザーデバイスとの間のオーディオ配信

汎用HDX RealTimeは、ユーザーデバイスとの間でオーディオを配信する2つの方法をサポートしています。

- **Citrix Audio Virtual Channel**。Citrix Audio Virtual Channelはオーディオ転送専用に設計されているため、一般的に推奨されます。
- **Generic USB Redirection**。ユーザーデバイスがCitrix Virtual Apps and Desktopsサーバーへの LANまたはLANに似た接続上にある場合、ボタンまたはディスプレイ（あるいはその両方）を備えたオーディオデバイス、ヒューマンインターフェースデバイス（HID）をサポートします。

Citrix オーディオ仮想チャネル

双方向のCitrixオーディオ仮想チャネル（CTXCAM）により、オーディオをネットワーク経由で効率的に配信できます。汎用HDX RealTimeは、ユーザーのヘッドセットまたはマイクからのオーディオを取得して圧縮します。その後、ICAを介して仮想デスクトップ上のソフトフォンアプリケーションに送信します。同様に、ソフトフォンのオーディオ出力は圧縮され、逆方向にユーザーのヘッドセットまたはスピーカーに送信されます。この圧縮は、ソフトフォン自体が使用する圧縮（G.729やG.711など）とは独立しています。これは、Optimized-for-Speechコーデック（中品

質）を使用して行われます。その特性は、Voice over Internet Protocolに最適です。エンコード時間が短く、ネットワーク帯域幅はピーク時で約56キロビット/秒（各方向28 Kbps）しか消費しません。このコーデックは、デフォルトのオーディオコーデックではないため、Studioコンソールで明示的に選択する必要があります。デフォルトはHDオーディオコーデック（高品質）です。このコーデックは高忠実度のステレオサウンドトラックに優れていますが、Optimized-for-Speechコーデックと比較してエンコードが遅いです。

汎用 USB リダイレクト

Citrix Generic USB Redirectionテクノロジー（CTXGUSB仮想チャネル）は、複合デバイス（オーディオとHID）およびアイソクロナスUSBデバイスを含むUSBデバイスをリモートで利用するための汎用的な手段を提供します。このアプローチは、LAN接続されたユーザーに限定されます。その理由は、USBプロトコルがネットワーク遅延に敏感であり、かなりのネットワーク帯域幅を必要とする傾向があるためです。アイソクロナスUSBリダイレクトは、一部のソフトフォンを使用する場合にうまく機能します。このリダイレクトは、優れた音声品質と低遅延を提供します。ただし、Citrix Audio Virtual Channelはオーディオトラフィックに最適化されているため、こちらが推奨されます。主な例外は、ボタン付きのオーディオデバイスを使用している場合です。たとえば、データセンターにLAN接続されたユーザーデバイスに接続されたUSB電話などです。この場合、Generic USB Redirectionは、ソフトフォンに信号を送り返すことで機能を制御する、電話機またはヘッドセットのボタンをサポートします。デバイス上でローカルに機能するボタンには問題ありません。

オーディオ診断コマンドラインツール

VDA上のオーディオ診断コマンドラインツールは、オーディオポリシー、構成、データ転送に関連するセッションデータを照会するために使用できます。

使用方法

コマンドプロンプトを開き、`C:\Program Files\Citrix\HDX\bin`フォルダーから`CtxAudio.exe`を実行します。

- 管理者としてツールを実行すると、すべてのアクティブなICAセッションのオーディオ情報が表示されます。
- 非管理者としてツールを実行すると、現在ユーザーのICAセッションオーディオ情報が表示されます。

出力

このツールは、セッション内のオーディオ関連の問題の診断に役立つさまざまな構成設定を出力します。

セクション	説明
ポリシー情報	現在のセッションに適用されているオーディオポリシー。
設定情報	レジストリに保存されているオーディオ関連の構成設定。
状態情報	現在のセッションに適用されているオーディオの状態、バージョン、コーデック、およびトランスポート。
デバイス情報	セッションで使用されているデバイス名、その役割、およびステータス。

> **注:**
>
> 出力は、マルチセッション (TS) VDA またはシングルセッション VDA (WSVDA) のどちらでツールを実行するかによって異なります。

制限事項

クライアントにオーディオデバイスをインストールし、オーディオリダイレクトを有効にして、RDSセッションを開始します。オーディオファイルが再生に失敗し、エラーメッセージが表示されることがあります。

回避策として、RDSマシンにレジストリキーを追加し、マシンを再起動します。詳細については、レジストリで管理される機能のリストにあるオーディオの制限を参照してください。

ブラウザコンテンツリダイレクト

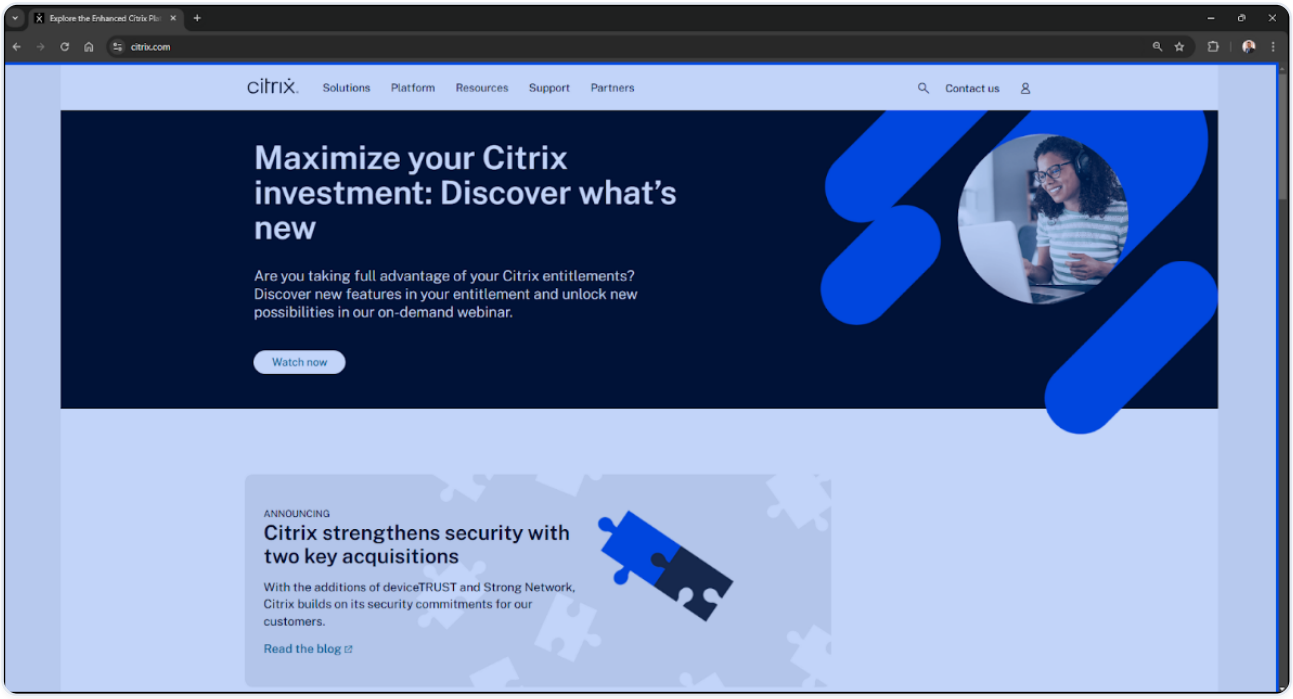
はじめに

Browser Content Redirection (BCR) は、Citrix Virtual Apps and Desktops™ 環境におけるウェブブラウジングのユーザーエクスペリエンスを向上させます。ウェブページのレンダリングをユーザーのローカルマシンにオフロードすることで、BCR はサーバーの負荷を軽減し、特に複雑なウェブサイトやリソースを大量に消費するウェブサイトのパフォーマンスを向上させます。

動作の仕組み

BCR は Citrix Workspace™ アプリを利用して、ユーザーデバイス上にセキュアなブラウジング環境を作成します。ユーザーが許可されたウェブページにアクセスすると、ブラウザウィンドウのビューポートがクライアントにリダイレクトされます。その後、クライアント側のブラウザエンジンはローカルマシンのリソースを活用してページをレンダリングし、読み込み時間の短縮とよりスムーズなインタラクションを実現します。

ブラウザのビューポートのみがリダイレクトされることに注意してください。ビューポートとは、ブラウザでコンテンツが表示される長方形の領域です。ビューポートには、アドレスバー、お気に入りツールバー、ステータスバーなどは含まれません。これらの項目はユーザーインターフェイスにあり、VDA のブラウザで引き続き実行されます。



主な利点

Browser Content Redirection はウェブトラフィックをインテリジェントに管理し、インフラストラクチャへの負担を軽減しながら、ユーザーに優れたエクスペリエンスを提供します。

組織にとってのメリットは次のとおりです。

- **コスト削減:** リソースを大量に消費するウェブページをユーザーデバイスにオフロードすることで、貴重なサーバーリソースを解放し、帯域幅の消費を削減します。これにより、ハードウェアコストとネットワークコストが削減されます。
- **ユーザーエクスペリエンスの向上:** グラフィックを多用するウェブサイトでも、よりスムーズで応答性の高いブラウジングエクスペリエンスをユーザーに提供します。ネイティブのようなパフォーマンスを提供し、遅延をなくし、生産性を向上させます。

- **セキュリティの向上:** 内部および外部リソースへのアクセスを許可しながら、セキュアな環境を維持します。
- **柔軟性の向上:** 基本的なウェブブラウジングから、プロキシトラバーサルや SSO 認証を必要とする複雑なウェブアプリケーションまで、幅広いユースケースをサポートします。Citrix Web Studio™ で詳細なポリシー制御を使用して、リダイレクト設定を簡単に管理できます。

システム要件

サーバー側コンポーネント

シトリックス バーチャル アプリケーションズ アンド デスクトップ

- 長期サービスリリース
  - 最小要件 - サポート終了していない LTSR Citrix Virtual Apps and Desktops リリース
  - 推奨されるバージョン - Citrix Virtual Apps and Desktops 2402 以降
- 現在のリリース
  - 最小要件 - サポート終了していない CR Citrix Virtual Apps and Desktops リリース
  - 推奨 - 最新のCitrix Virtual Apps and Desktopsリリース

ブラウザコンポーネント

- ブラウザ
  - マイクロソフト エッジ
  - グーグル クローム
- ブラウザリダイレクト拡張機能
  - Google Chromeストア
  - Microsoft Edgeストア
- 最高のパフォーマンスを得るために、ブラウザの最新バージョンを使用することをお勧めします。

> **注:**
>
> ブラウザコンテンツリダイレクトまたは双方向コンテンツリダイレクトを有効にするには、Microsoft Edgeアドオンストアからブラウザリダイレクト拡張機能を使用する予定がある場

> 合、Virtual Delivery Agent (VDA) バージョン2503があることを確認してください。古いVDAバージョンでは、Microsoft Edgeブラウザ内でChromeウェブストアから拡張機能をインストールすることで、同じ機能を実現できます。

> 上記で提供されている拡張機能リンクは一般提供 (GA) されており、本番レベルの展開に関連しています。GA拡張機能に加えて、CitrixはGoogle Chromeストアで特にベータ版 (GA + 1) 拡張機能も公開しています。

> Citrixは、今後のアップデートがテストされ、問題が早期に報告されるように、お客様がベータ版でテストユーザーを持つことを推奨しています。これにより、GA拡張機能が正式に展開される際にスムーズなプロセスが保証されます。

> 拡張機能のリリースは通常、Citrix Workspaceアプリのリリースと一致します。

クライアント側コンポーネント

ウィンドウズ

- Windows 10 または 11
- Citrix Workspaceアプリ
  - 最小要件 - サポート終了していないCitrix Workspaceアプリ
  - 推奨
    - 長期サービスリリース - Citrix Workspace App for Windows 2402 CU4 以降、Citrix Workspace App for Windows 2507
    - 現行リリース - Citrix Workspace App 2405以降

> **注:**
>
> - ブラウザコンテンツリダイレクトは、Citrix Workspace App Windows LTSRリリース1912および2203.1ではサポートされていません。
> - ブラウザコンテンツリダイレクトに必要なクライアント側ブラウザエンジンは、Citrix Workspace Appの現行リリースではデフォルトでインストールされます。

- ブラウザコンテンツリダイレクトに必要なクライアント側ブラウザエンジンは、Citrix Workspace App 2402 LTSRリリースではデフォルトでインストールされません。管理者は、ADDLOCALスイッチを利用して、Citrix Workspace AppにBCRブラウザコンポーネントをインストールできます。
- Windows向けCitrix Workspaceアプリ2507以降、ブラウザコンテンツリダイレクト（BCR）はモジュールコンポーネントとして管理されますが、引き続きCitrix Workspaceアプリにパッケージ化されています。BCRコンポーネントはLTSRバージョンでもデフォルトでインストールされるようになり、CRとLTSRの間の一貫性が確保されます。さらに、通常のCitrix Workspaceアプリのリリースサイクル外で独立したアップデートや暫定的なパッチが必要な状況のために、スタンドアロンのBCRパッケージが公開されます。詳細については、Citrix Workspace App Windows documentationを参照してください。

リナックス

- Citrix Workspace アプリ
  - 最小要件 - サポート終了していないCitrix Workspace App
  - 推奨 - Citrix Workspace App 2408以降 詳細については、Citrix Workspace App for Linuxのドキュメントを参照してください。

注:

Linux向けCitrix Workspaceアプリ2601以降、ブラウザコンテンツリダイレクト（BCR）はモジュールコンポーネントとして管理されます。BCRコンポーネントは引き続きLinux向けCitrix Workspaceアプリにデフォルトでパッケージ化およびインストールされ、一貫したユーザーエクスペリエンスを保証します。さらに、通常のCitrix Workspaceアプリのリリースサイクル外で独立したアップデートや暫定的なパッチが必要な状況のために、スタンドアロンのBCRパッケージが公開されます。詳細については、Citrix Workspace App Linux documentationを参照してください。

ChromeOS

- Citrix Workspace アプリ
  - Chromeウェブストアの最新バージョン

MacOS

- Citrix Workspace アプリ
  - 最小要件 - Citrix Workspaceアプリ for Mac 2411以降

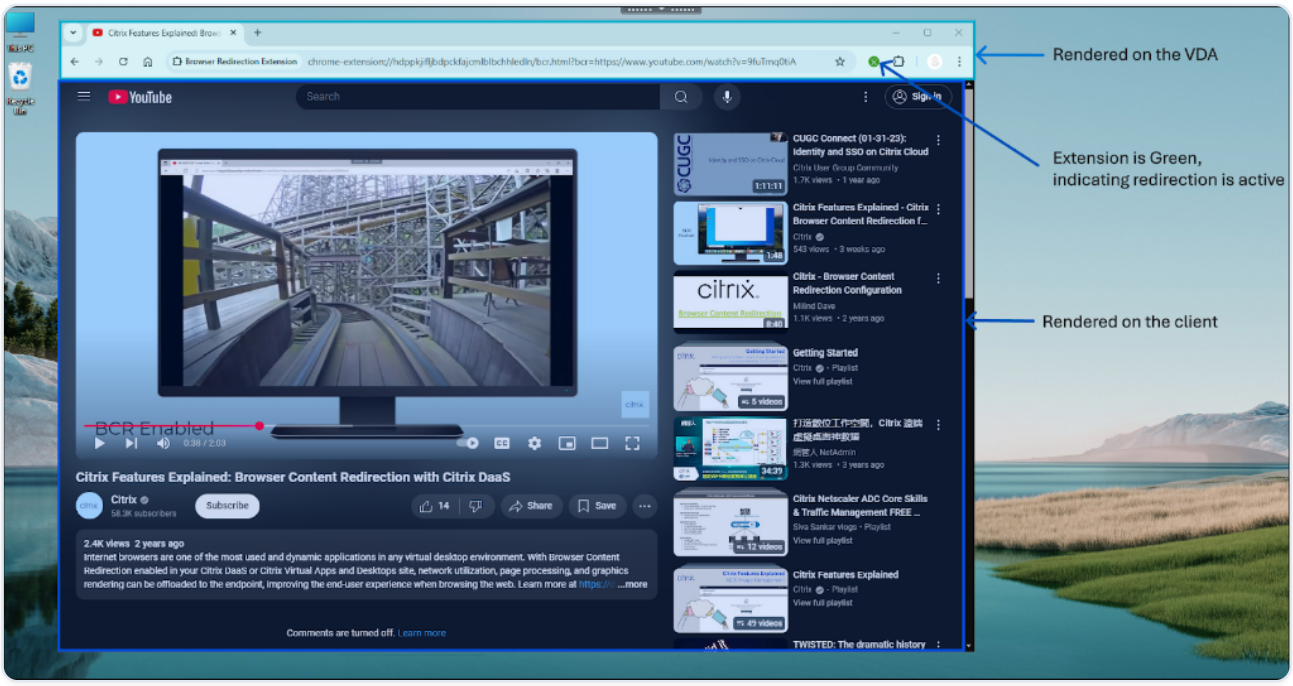
> **注:**
>
> - macOSの場合、ブラウザコンテンツリダイレクトパッケージはCitrix Workspaceアプリとは独立しており、常に最新バージョンです。したがって、このパッケージは、指定された最小バージョンよりも新しい複数のCWAバージョンと互換性があります。
> - Citrix Workspaceアプリ for Macへの依存がないため、ブラウザコンテンツリダイレクトのバージョン番号はCitrix Workspaceアプリ for Macのバージョンとは一致しません。
> - クライアント側のブラウザエンジンはCitrix Workspaceアプリ for Macにはパッケージされていません。Mac用のクライアント側をCitrixダウンロードからダウンロードしてインストールしてください。
> - IntelおよびARMパッケージは別々です。したがって、macOSエンドポイントに適したバージョンをインストールする必要があります。
> - Citrix Workspaceアプリ 2511.1 for Mac以降、モジュラーBCRコンポーネントはデフォルトでインストールされますが、Citrix Workspaceアプリにはパッケージされていません。これにより、Citrix Downloadsからコンポーネントを手動でダウンロードしてインストールする必要がなくなります。定期的なCitrix Workspaceアプリのリリースサイクル外で独立した更新や暫定パッチが必要な状況のために、スタンドアロンのBCRパッケージが公開されます。詳細については、Citrix Workspaceアプリ Mac版のドキュメントを参照してください。

設定手順

1. システム要件に従って、クライアント側およびサーバー側のコンポーネントをインストールします
   - 拡張機能の展開の詳細については、「拡張機能の展開」セクションを参照してください
2. Studioポリシーを構成します
   - Web Studioポリシーは、さまざまなユースケースに合わせてブラウザコンテンツリダイレクトを構成するためのきめ細かな方法を提供します

- 基本ポリシーにより、管理者はブラウザコンテンツリダイレクトで許可/不許可にする必要があるURLを構成できます
- URLはワイルドカードを使用して構成できます

3. サポートされているWebブラウザを開き、許可されたURLに移動します
   - 許可リストで一致が見つかった場合、ウェブサイトはクライアントにリダイレクトされます
   - Citrix Workspaceアプリは、シームレスなエクスペリエンスのために、ビューポートをVDA側のブラウザにブレンドします。
4. 拡張機能のロゴの色は、コンテンツリダイレクトのステータスを示します。
   - 緑：アクティブで接続済み
   - 灰色：現在タブで非アクティブ/アイドル状態
   - 赤：破損/動作していません



> **注:**
>
> - HTML5ビデオリダイレクトとブラウザコンテンツリダイレクトは独立した機能です。この機能が動作するためにHTML5ビデオリダイレクトポリシーは必要ありません。ただし、Citrix HDX™ HTML5ビデオリダイレクトサービスはブラウザコンテンツリダイレクトに使用されます。

- すべての設定はWeb Studioを介して行い、レジストリキーを使用しないことをお勧めします。

機能と構成オプション

ブラウザコンテンツリダイレクトは、さまざまな顧客環境のユースケースに合わせて構成するためのさまざまな方法を提供します。ポリシー設定の詳細については、ブラウザコンテンツリダイレクトポリシー設定を参照してください。

リダイレクトメカニズム

クライアントフェッチクライアントレンダー

デフォルトでは、ブラウザコンテンツリダイレクトはこのモードで動作します。つまり、クライアント側のブラウザエンジンがWebページに直接アクセスします。これには、クライアントネットワークからWebページへの必要なアクセスが必要です。クライアントフェッチクライアントレンダーのシナリオでは、Citrix VDAからクライアントへのネットワーク、CPU、およびRAMの使用量をすべてオフロードし、ブラウザコンテンツリダイレクトを構成する最も最適な方法です。

ポリシー構成オプション

- ブラウザコンテンツリダイレクト：許可
- ブラウザコンテンツリダイレクトACL構成
  - リダイレクトする必要があるURLを指定します。デフォルトでは、YouTubeのみがリダイレクト用に構成されているWebサイトです。
- ブラウザコンテンツリダイレクトブロックリスト構成
  - 特定URL/サブURLのリダイレクトをブロックするためのオプションの構成オプション。最大限のカスタマイズを行うには、上記のオプションと組み合わせてこのオプションを活用してください。

サーバーフェッチクライアントレンダリング

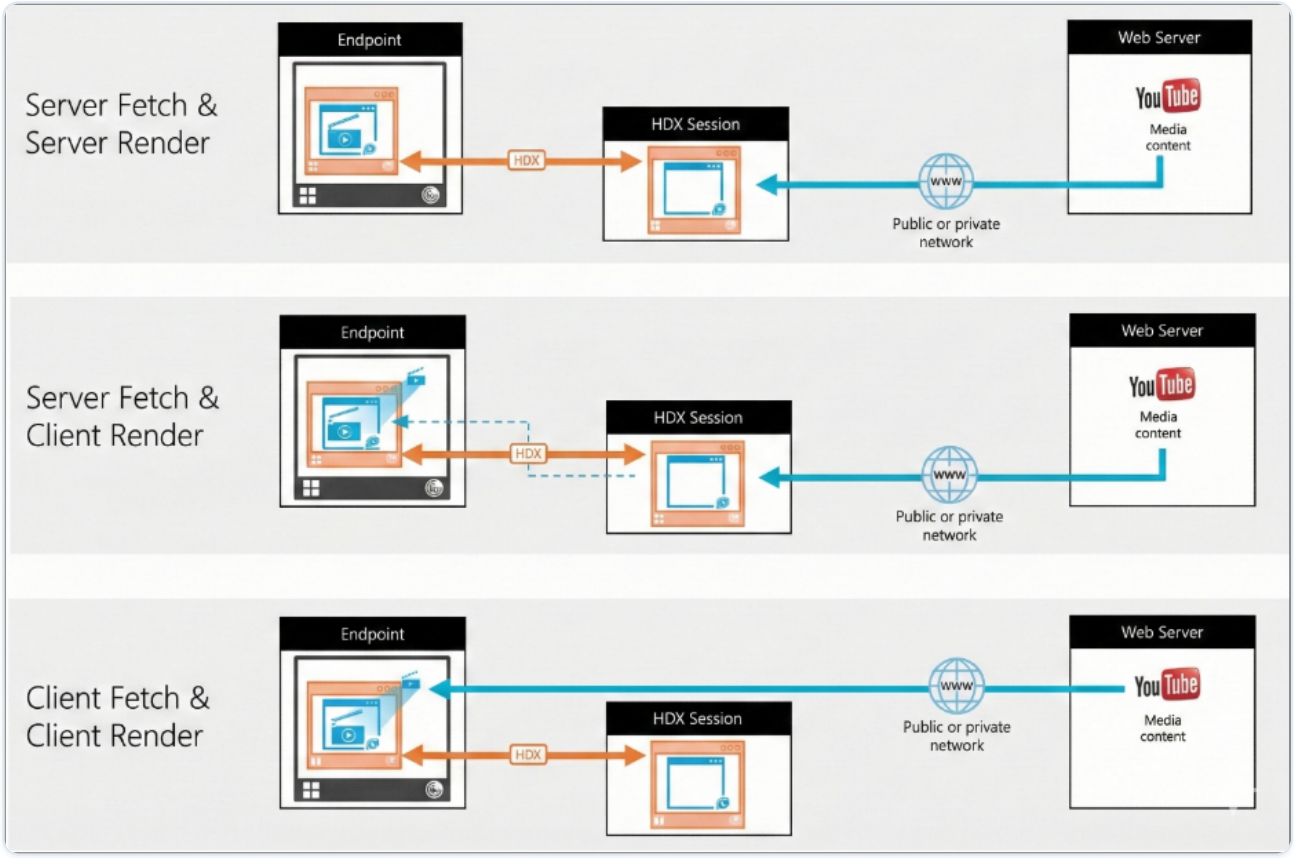
この場合、クライアント側のブラウザエンジンは、仮想チャネルを使用してVDAを介してWebサーバーからコンテンツにアクセスし、フェッチします。このオプションは、クライアントがインターネットにアクセスできない場合（シンクライアントなど）に役立ちます。VDAでのCPUとRAMの消費は少ないですが、ICA®仮想チャネルで帯域幅が消費されます。

このシナリオには3つの動作モードがあります。「プロキシ」という用語は、VDAがインターネットアクセスを取得するためにアクセスするプロキシデバイスを指します。

ポリシー構成オプション

- 「クライアントフェッチクライアントレンダリング」セクションで指定されたポリシーに加えて、以下を構成します
- ブラウザコンテンツリダイレクトプロキシ構成
  - **直接または透過:** サーバーフェッチクライアントレンダリングを活用し、VDAからWebページへの直接アクセスまたは透過プロキシアクセスがある場合は、これを構成します。ポリシーにはキーワード「DIRECT」を構成する必要があります。
  - **明示的プロキシ:** サーバーフェッチクライアントレンダリングを活用し、VDAからWebページへの明示的プロキシアクセスがある場合は、これを構成します。
  - **PACファイル:** VDA内のブラウザが指定されたURLをフェッチするための適切なプロキシサーバーを自動的に選択できるPACファイルに依存している場合は、これを構成します。

フォールバックモード



クライアントリダイレクトが失敗する場合があります。たとえば、クライアントマシンがインターネットに直接アクセスできない場合、エラー応答がVDAに戻されることがあります。そのような場合、VDA上のブラウザはページを再読み込みし、サーバー上でレンダリングできます。

認証の処理

認証サイト

現在のBrowser Content Redirectionの実装では、リダイレクトメカニズムに関わらず、Browser Content Redirectionがウェブサイトへのログインを処理できるように、認証サイトを構成する必要があります。

例:

1. Browser Content Redirection ACL構成で`<https://www.youtube.com/*/>`のみが構成されており、認証サイトが構成されていない場合、ウェブサイトにサインインする際にBCRはサーバー側レンダリングにフォールバックし、そこで処理を続行します。
2. この場合、BCRが認証サイトを処理できるように、`<https://www.accounts.google.com/*/>`と必要に応じてIdPウェブサイトなどの他の認証サイトを構成してください。各ウェブサイトのサインインは異なる動作をするため、必ずリストに含めてください。
3. 構成されている場合、BCRは認証を処理します。例えば、クライアントフェッチクライアントレンダリングでは、シームレスなサインインエクスペリエンスのために、認証もクライアント側ブラウザエンジンから行われます。

ポリシー構成オプション

リダイレクトメカニズムのセクションで言及されているポリシーに加えて、Browser Content Redirection認証サイトポリシーを構成します。

> **注:**
>
> - BCRクライアント側ブラウザは、リダイレクトされたウィンドウが閉じられた後、クッキー（認証を含む）を永続化しません。これは、BCRウィンドウが完全に閉じられて再度開かれたときに、ウェブサイトに再ログインする必要があるという形で現れます。
> - BCRクライアント側ブラウザは、VDA側ブラウザからクッキーを読み取りません。そのため、ユーザーのパーソナライゼーションと設定はVDAブラウザと同期しません。

統合Windows認証

Browser Content Redirectionは、VDAと同じドメイン内で統合Windows認証 (IWA) とともに構成されている場合、ウェブサイトへのシームレスな認証方法を提供できます。

ポリシー構成オプション

- Browser Content Redirection統合Windows認証サポートポリシーを構成します。

シングルサインオンを有効にする前に、以下を完了してください。

- Kerberosインフラストラクチャを構成して、ホスト名から構築されたサービスプリンシパル名 (SPN) のチケットを発行します。例: HTTP/serverhostname.com。
- サーバーフェッチクライアントレンダリングの場合: サーバーフェッチモードでブラウザコンテンツリダイレクトを使用する場合は、VDAでDNSが適切に構成されていることを確認してください。
- クライアントフェッチクライアントレンダリングの場合: クライアントフェッチモードでブラウザコンテンツリダイレクトを使用する場合は、クライアントデバイスでDNSが適切に構成されており、オーバーレイからWebサーバーのIPアドレスへのTCP接続を許可していることを確認してください。

プロキシ認証

ブラウザコンテンツリダイレクトは、サーバーからコンテンツをフェッチする際に、Webプロキシへのシームレスな認証方法を提供できます。有効にすると、ブラウザコンテンツリダイレクトはKerberosサービスチケットを自動的に取得して使用し、プロキシで認証します。

ポリシー構成オプション

- ブラウザコンテンツリダイレクトのサーバーフェッチプロキシ認証ポリシーを構成します。

サーバーフェッチプロキシ認証ポリシーを有効にする前に、以下を完了してください。

- PACファイルを構成して、ダウンストリームWebプロキシ経由でトラフィックをルーティングし、プロキシがKerberos認証を使用するように設定する必要があります。

サーバー側証明書検証

ブラウザコンテンツリダイレクトは、証明書検証のサポートによりさらに強化されています。クライアントからリダイレクトされたWebサイトにアクセスする場合、クライアントオーバーレイブラウザは、サーバーまたはMitMプロキシからの証明書を信頼しない場合があります。このような場合、BCRはVDAの証明書ストアに対してホストまたはプロキシの証明書を検証できるようになりました。

最小要件

この機能はデフォルトで有効になっており、以下の要件が満たされれば構成は不要です。

- シトリックス バーチャルアプリおよびデスクトップ 2507
- シトリックス ワークスペースアプリ for Windows 2511
- Citrix Workspace アプリ Linux 用 2604

- ブラウザリダイレクト拡張機能 (ChromeまたはEdge) 25.11以降。

シングルサインオンのサポート

ブラウザコンテンツリダイレクトは、シングルサインオンのサポートによりユーザーエクスペリエンスを合理化し、VDA側の認証とCookie共有を可能にします。この機能強化により、冗長なログインが排除され、BCRウィンドウが閉じられた後でもBCRセッション全体で認証とCookieの永続性が維持されるため、生産性が向上します。このシームレスなエクスペリエンスは、認証がクライアントではなくVDAから行われることを保証することで、セキュリティをさらに強化します。

この機能の詳細については、「シングルサインオンのサポート」セクションを参照してください。

リダイレクトされたコンテンツをスクリーンショットでキャプチャする

ブラウザコンテンツリダイレクトはWebページをエンドポイントでレンダリングするため、標準のセッション内スクリーンショットツールでは、リダイレクトされたコンテンツが空白領域としてキャプチャされます。このコンテンツをスクリーンショットに含めるには、Citrix Snipping Toolを使用してください。Citrixでは、簡単に見つけられるようにCitrix Virtual Desktop Assistantから起動することをお勧めします。詳細については、Citrix Virtual Desktop Assistant documentationを参照してください。

ユースケース

ブラウザコンテンツリダイレクト（BCR）は、特にリソースを大量に消費し、企業が頻繁にアクセスする幅広いWebサイトで利用できます。これには、YouTubeのようなビデオストリーミングプラットフォームが含まれ、レンダリングをエンドポイントデバイスにオフロードすることで、サーバー負荷を大幅に軽減し、コストを節約できます。さらに、BCRは、ビデオ会議やコラボレーションツール（Google Meet、Teams Web、Zoom Web）などのユニファイドコミュニケーションアプリケーションや、コンタクトセンターアプリケーション（Genesys Cloud）に最適であり、スムーズなパフォーマンスと強化されたユーザーエクスペリエンスを保証します。BCRを活用することで、企業はリソースを最適化し、さまざまなWebベースのアプリケーションで効率を向上させることができます。特定のWebサイトの設定方法については、CTX238236を参照してください。

拡張機能の展開

手動で展開

ブラウザリダイレクト拡張機能は、ChromeおよびEdgeのWebストアで公開されています。この拡張機能はVDA上のブラウザにのみ必要であり、クライアント側には必要ありません。拡張機能をインストールするには、Chrome / Edge Webストアに移動し、ブラウザリダイレクト拡張機能を

検索して、それぞれのブラウザに追加します。この方法は個々のユーザーに有効です。多数のユーザーに拡張機能を展開するには、グループポリシーを使用して拡張機能を展開します。

(/en-us/citrix-virtual-apps-desktops/current-release/media/deploy-manually-bcr.png)

グループポリシーを使用した展開

前提条件

- **アクセス:** グループポリシーを構成するマシンまたはActive Directory環境で管理者権限が必要です。
- **ADMXファイル:** お使いのChromeのバージョンに対応するGoogle Chrome ADMXファイル（管理用テンプレート）をダウンロードします。これらはGoogle Chrome Enterprise Helpページで見つけることができます。
- **Edgeテンプレート:** Microsoft Edge Enterprise landingページからMicrosoft Edgeの管理用テンプレート（ADMXファイル）をダウンロードします。
- **拡張機能IDと更新URL:** Citrix Browser Content Redirection拡張機能の拡張機能IDと更新URL。

GOOGLE CHROMEの手順

1. ADMXファイルのインポート:
    - Chrome ADMX ファイルを管理用テンプレートの中央ストアにコピーします。これは通常、ドメインコントローラー上の %SystemRoot%\PolicyDefinitions です。
2. グループポリシー管理を開く:
    - グループポリシー管理コンソール (gpmc.msc) を起動します。
3. GPOを作成または編集します。
    - 新しいグループポリシーオブジェクト (GPO) を作成するか、拡張機能を展開するユーザーまたはコンピューターに適用される既存のGPOを編集します。
4. 拡張機能の設定に移動します。
    - GPOエディターで、以下に移動します。
        - ユーザーの構成 > 管理用テンプレート > 従来の管理用テンプレート (ADM) > Google > Google Chrome > 拡張機能
5. 「強制インストールするアプリと拡張機能のリストを構成する」を有効にします。
    - このポリシー設定をダブルクリックし、「有効」を選択します。

- 「強制インストールするアプリと拡張機能のリストを構成する」設定が無効に設定されている場合、拡張機能はすべてのユーザーのChromeから自動的に削除されます。

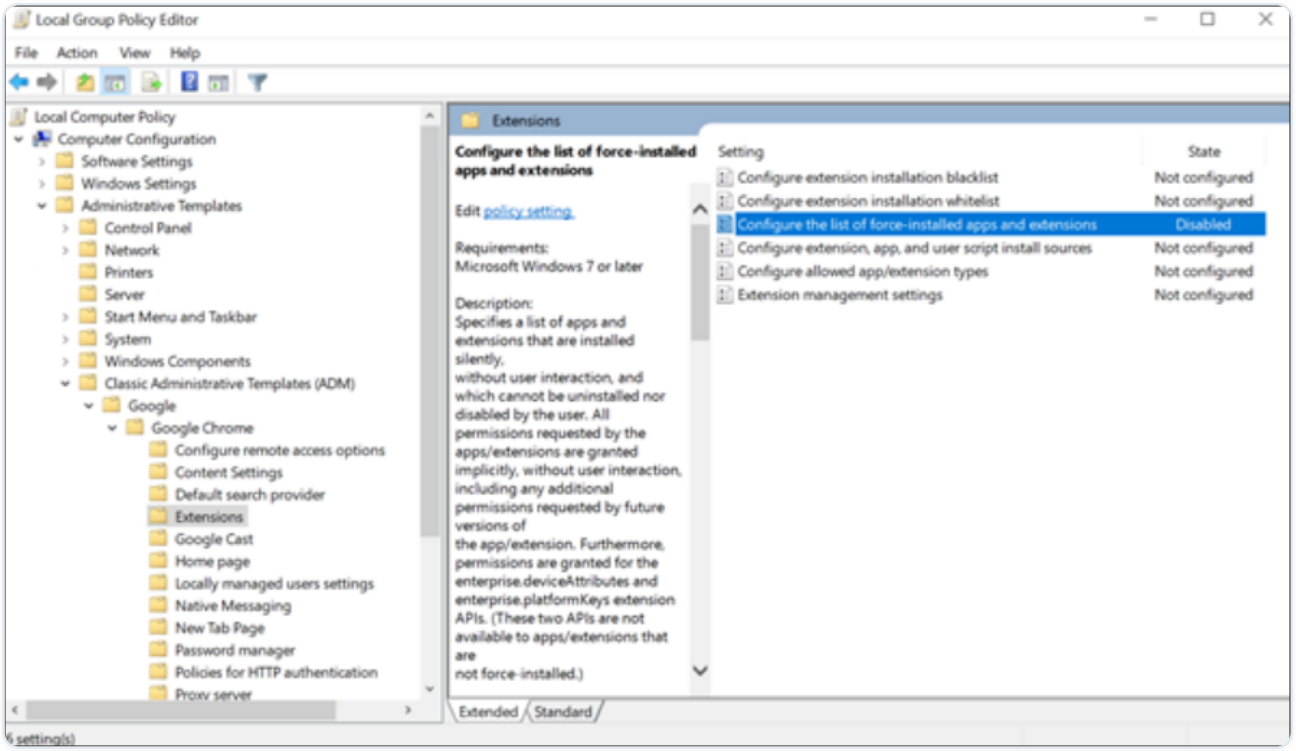
6. 拡張機能IDと更新URLを追加します。
   - 「表示」ボタンをクリックします。
   - 拡張機能IDと更新URLを次の形式で入力します: <extension_id>;<update_url>
   - 値は次のとおりです: hdppkjifljbdpckfajcmlblbchhledln; `<https://clients2.google.com/service/update2/crx/>` (更新URL)
7. GPOを適用します。
   - Active Directory構造内の適切な組織単位 (OU) にGPOをリンクします。
8. グループポリシーを更新:
   - ターゲットマシンで、gpupdate /force を実行してポリシーをすぐに適用するか、ポリシーが自動的に更新されるのを待ちます。

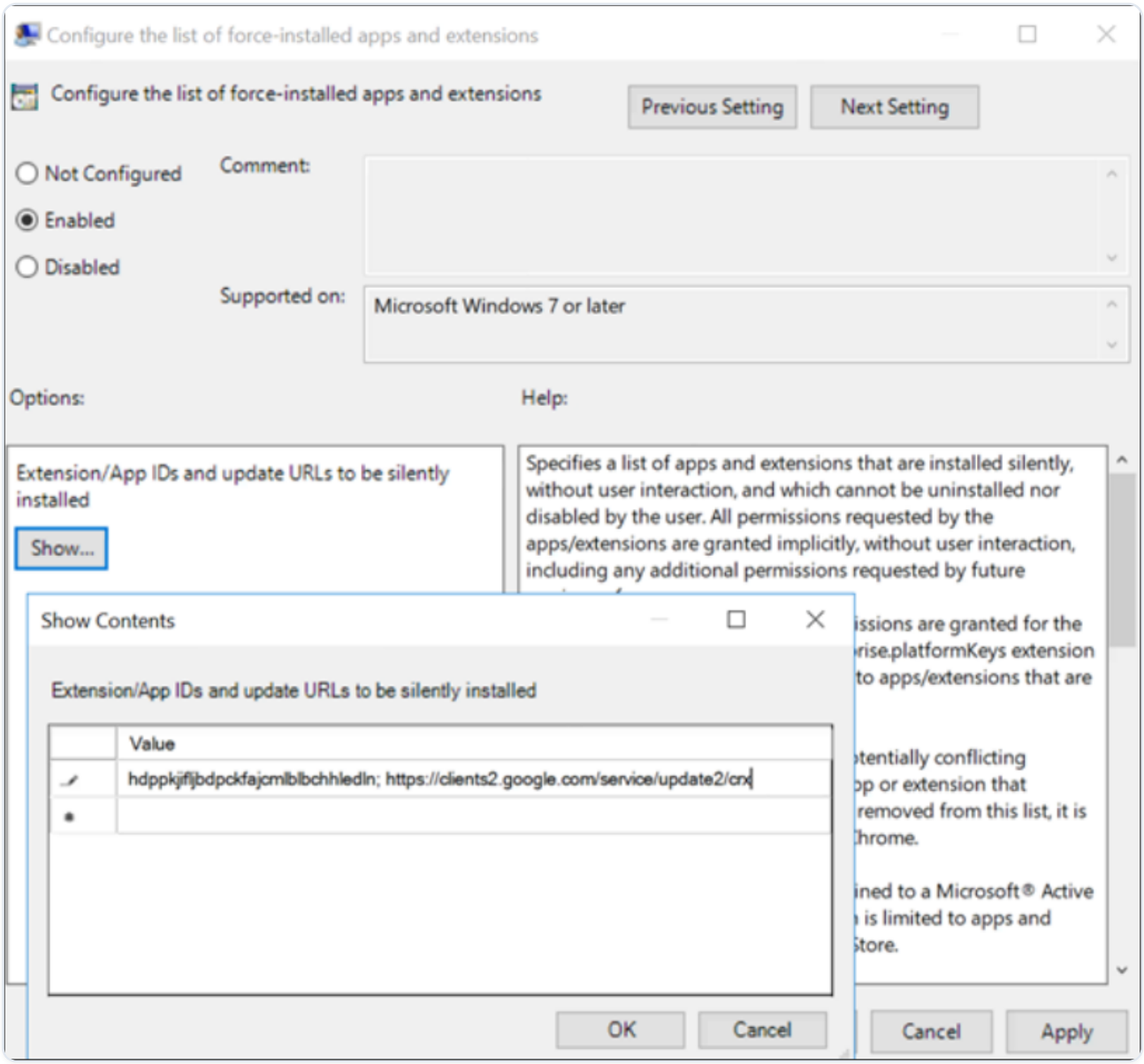
MICROSOFT EDGE の手順

1. ADMXファイルをインポート:
   - Edge ADMXファイルを、管理用テンプレートの中央ストア (%SystemRoot%\PolicyDefinitions) にコピーします。
2. グループポリシー管理を開く:
   - グループポリシー管理コンソール (gpmc.msc) を起動します。
3. GPOを作成または編集:
   - 新しいGPOを作成するか、既存のGPOを編集します。
4. 拡張機能の設定に移動:
   - GPOエディターで、以下に移動します:
     - コンピューターの構成 > ポリシー > 管理用テンプレート > Microsoft Edge > 拡張機能
5. 「サイレントインストールされる拡張機能を制御する」を有効にする:
   - このポリシー設定をダブルクリックし、「有効」を選択します。
6. 拡張機能IDと更新URLを追加:

- 「表示」ボタンをクリックします。
- 拡張機能IDと更新URLを次の形式で入力します: <extension_id>;<update_url>
- 値: hdppkjifljbdpckfajcmlblbchhledln; `<https://clients2.google.com/service/update2/crx/>` (URLを更新)

7. GPOを適用します:
   - Active Directory構造内の適切な組織単位 (OU) にGPOをリンクします。
8. グループポリシーを更新します:
   - ターゲットマシンで、gpupdate /forceを実行するか、自動更新を待ちます。





トラブルシューティング

トラブルシューティング情報については、ナレッジセンターの記事「ブラウザコンテンツリダイレクトのトラブルシューティング方法」を参照してください。

ブラウザコンテンツリダイレクトの制限事項

サーバー側の制限事項 (VDA)

ブラウザコンテンツリダイレクトは、以下のユースケースをサポートできません。記載されているシナリオまたは新しいシナリオで機能強化が必要な場合は、Citrix製品チームにお問い合わせください。

- ポップアップウィンドウは、ブラウザコンテンツリダイレクトではサポートされていません。

- ブラウザコンテンツリダイレクトを使用している場合、HTML5ビデオのリダイレクトポリシーは無効にする必要があります。
- セッションの切断/再接続のシナリオでは、BCRを再度有効にするためにVDAブラウザウィンドウを更新する必要があります。
- BCRでリダイレクトされたウィンドウからの印刷およびファイルのダウンロードはサポートされていません。
- ブラウザコンテンツリダイレクトをブラウザプロファイル共有と併用する場合、複数のプロファイルでのSSO永続性はサポートされていません。
- シークレットモードまたはプライベートブラウジングモードは、ブラウザコンテンツリダイレクトではサポートされていません。

クライアント側の制限 (CWA)

- ブラウザコンテンツリダイレクトは、ARMhfフレームワークではサポートされていません。
- BCRは、1つのブラウザで最大25個のリダイレクトされたタブ、および2つのブラウザで合計30個のリダイレクトされたタブをサポートします。

シングルサインオンのサポート

はじめに

ブラウザコンテンツリダイレクトは、シングルサインオンのサポートにより合理化されたユーザーエクスペリエンスを提供するようになり、VDA側での認証とCookie共有を可能にします。

この機能強化により、重複するログインが不要になり、BCRウィンドウが閉じられた後でもBCRセッション全体で認証とCookieの永続性を維持することで、生産性が向上します。

このシームレスなエクスペリエンスは、認証がクライアントではなくVDAから行われるようにすることで、セキュリティをさらに強化します。

シングルサインオンなしの場合

- BCR内で認証されたページを開くには、ユーザーは毎回資格情報を再入力する必要があり、SSOの永続性が失われました。
- SSOはBCRウィンドウが開いている間のみ維持されました。ウィンドウを閉じて再度開くと、ユーザーはログインプロセスを繰り返す必要がありました。
- 認証フローはクライアントから行われ、管理者はクライアントデバイスからセキュアな認証サイトへのネットワークアクセスを提供する必要がありました。

シングルサインオンありの場合

- (VDAで既に認証されている場合) SSOがVDAブラウザからシームレスに保持されるため、ユーザーは資格情報の入力を求められなくなります。
- 認証はVDAから行われるため、クライアント側のネットワーク要件と露出を制限することでセキュリティ体制が向上し、大幅に改善された中断のないエクスペリエンスを提供します。

最小要件

- シトリックス バーチャルアプリおよびデスクトップ 2507
- シトリックス ワークスペースアプリ for Windows 2511
- シトリックス ワークスペースアプリ for Linux 2601
- ブラウザリダイレクト拡張機能 (Chrome または Edge) 25.11 以降

サポートされている認証シーケンス

現在、BCRシングルサインオンでサポートされている認証シーケンスは2種類あります。

リダイレクトベースの認証

この標準的な方法では、アプリケーションはHTTPリダイレクトを使用して、ユーザーを認証専用ページに強制的に移動させます。

例えば、ユーザーが必要なセッションクッキーなしで `<https://my.intranet.app>` にアクセスしようとすると、ウェブアプリケーションは `<https://my.intranet.app/auth>` のような認証エンドポイントに HTTP 302 リダイレクトで応答します。

ユーザーがそのページで認証に成功すると、ブラウザは元のアプリケーションURLにリダイレクトされ、必要な認証Cookieが含まれるようになります。

ページ内フォームベース認証

この方法では、ユーザーを目的のアプリケーションURLに留まらせたまま、ログインインターフェイスを動的に表示します。

例えば、ユーザーが `<https://my.intranet.app>` のような保護されたページに移動すると、必要なクッキーがないため、ページはリダイレクトをトリガーすることなく認証フォームを直接ロードします。このプロセスには、ページインターフェースとIDP（Identity Provider）間のいくつかの内部的なやり取りが含まれる場合があります。これらのやり取りは、最終的に有効なクッキーが提供され、利用されて、ユーザーが元のページのコンテンツにアクセスできるようになるまで続きます。

> **注:**
>
> 上記のメカニズムでシナリオがカバーされておらず、上記のメカニズムを使用するようにWeb アプリを設定できない場合は、Citrix 製品チームにお問い合わせください。

構成

ステップ0: はじめに

BCRでシングルサインオンを構成する方法は2つあります。構成方法は、目的のBCR Webサイトの認証メカニズムと、シングルサインオンをサポートするために複数のWebアプリケーションを構成する必要がある柔軟性によって異なります。

方法1: この方法では、Web Studioの既存のBCRポリシーを使用して、シングルサインオンのサポートを実現します。

シングルサインオンのサポートが導入される前は、ブラウザコンテンツリダイレクト認証サイトポリシーを使用して、認証（または中間ページ）に使用されるURLを指定し、フローの中断がないようにクライアントにリダイレクトしていました。

シングルサインオンサポートの導入により、BCRはVDA側のブラウザの認証Cookieを利用するため、認証サイトポリシーのURLは、代わりにブラウザコンテンツリダイレクトブロックリストポリシーで構成する必要があります。これにより、認証がVDAを介して行われることが保証されます。

方法2: この方法は方法1と同様のロジックで動作しますが、URLは代わりにJSON（`bcrconfig.json`）を介して構成され、ホストされているJSON URLがBCR ACLポリシーで呼び出されます。JSON構成は、追加の柔軟性を提供します。

1. 企業は環境内で複数のWebアプリケーションを使用しており、各アプリケーションは実装に基づいて異なる認証メカニズムを使用する場合があります。新しいJSONメソッドにより、構成がより直感的で堅牢かつスケーラブルになります。
2. **ページ内フォームベース認証**を扱う場合、方法1では、そのような構成をサポートする既存のポリシーがないため、特定の認証Cookieを設定する方法が提供されません。したがって、Webサイトで**ページ内フォームベース認証**が必要な場合、JSONが唯一の方法です。

将来を見据えると、JSONはより堅牢な機能を導入するためのスケーラブルな方法を提供するため、CitrixはJSONベースの構成を試すことを推奨します。

ステップ1：認証メカニズムの決定

構成に使用する方法を決定するには、まずアプリケーションがどのような認証メカニズムを使用しているかを判断する必要があります。Webアプリケーションの認証方法を正確に判断するには、Webアプリケーション管理者に問い合わせるのが最善の方法です。

それが選択肢にない場合は、BCR拡張機能が**インストールされていない状態で**認証フローを実行しながら、ブラウザの開発者ツールのタブで要求/応答のやり取りを検査する必要があります。次の結果は、認証タイプを判断するのに役立ちます。

リダイレクトベースの認証の場合: 列で1つ以上の302（リダイレクト）応答を探します。302応答には、認証ページを指すロケーションヘッダーが含まれている必要があります。このページURLは、方法1を使用している場合はブラウザコンテンツリダイレクトブロックリストポリシーに設定し、方法2を使用している場合は`bcrconfig.json`ファイルのアプリ構成の`denyList`セクションに設定する必要があります。

ページ内フォームベース認証の場合: 列で複数のPOST要求を探します。POST要求に対する後続の応答の1つは、Webアプリ固有の認証Cookieを含むset-cookieヘッダーを返す必要があります。このCookieは、`bcrconfig.json`ファイルのアプリ構成のcookiesセクションに設定する必要があります。方法1はページ内フォームベース認証をサポートしていないため、このシナリオでは方法2が唯一の構成オプションです。

例: github.comの例を次に示します。この方法は、BCRでリダイレクトし、適切な構成であることを確認したい任意のWebサイトに使用できます。

1. **Chrome**を開き、**CTRL+SHIFT+I**を押して開発者ツールを表示します。
2. タブをクリックします。
3. 設定をオンにします。
4. ネットワークログを簡素化するために、 フィルターをクリックします。
5. 「**名前**」の横を右クリックし、「**URL**」列を追加します。
6. 開発者ツールを開いたまま、**github.com** にアクセスします。
7. **github.com** にサインインします。
8. github.com の初期ページから、ログオン後の最終ページまでのすべての中間ホップをメモします。
9. 上記で指定された認証タイプを特定するために、要求/応答ヘッダーを分析します。

ステップ2：構成方法を選択する

1. リダイレクトベースの認証のみを扱っており、さまざまなニーズを持つ複数のWebアプリケーション（例：リダイレクトベースの認証を使用するWebアプリケーションと、ページ内フォームベースの認証を使用する別のWebアプリケーション）をリダイレクトする必要がない場合は、方法1を選択してシングルサインオンを構成できます。
2. ページ内フォームベースの認証を扱っている場合、または異なる認証メカニズムを持つ複数のWebアプリケーションを扱っている場合、あるいはリダイレクトベースの認証のみであってもより柔軟性を求める場合は、方法2を選択できます。

ステップ3：構成

方法1：既存のポリシーでBCRシングルサインオンを構成する

1. `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDXMediaStream key: Dword BrowserProfileSharing value 1` に次のレジストリ値を作成して、VDAで機能を有効にします。
2. リダイレクトするWebサイトでブラウザーコンテンツリダイレクトACL構成ポリシーを構成します。この点での構成変更はありません。
3. 認証サイトポリシーにURLがすでに構成されている場合は、それらをブラウザーコンテンツリダイレクトブロックリストポリシーにコピーし、認証サイトポリシーを無効にします。
4. 以前に認証/中間サイトを構成していない場合は、中間URL（BCR拡張機能がインストールされていない**状態で**認証フローを実行中に、ブラウザーの開発者ツールの「ネットワーク」タブにある要求/応答のやり取りから）を特定し、ブロックリストに構成します。

方法2：JSONでBCRシングルサインオンを構成する

bcrconfig.json の作成

`bcrconfig.json` には、複数の Web アプリ構成を含めることができます。BCR 拡張機能は、要求された URL を apps 配列内のいずれかのアプリで指定された `allowList` のいずれかに一致させ、関連するルールを動的に適用して、ページのリダイレクトとシングルサインオン処理を決定します。BCR 拡張機能が Web アプリをどのように処理するかを制御するために、次のキーを使用できます（JSON 仕様 に従って、*ブール*値は小文字である必要があることに注意してください - **true** または **false** のみ）。

- **appName** : これは主に拡張機能の内部およびログ記録の目的で使用されます。
- **allowList** : アプリには `allowList` に少なくとも 1 つの URL を含める必要があります。これは、クライアントがページをレンダリングし、VDA がレンダリングしないようにリダイレクトされることを意図した URL です。複数の URL を定義でき、ワイルドカードも使用できます。ワイルドカードのルールは、ブラウザコンテンツリダイレクト ACL 構成 とまったく同じで

す。たとえば、すべての Google アプリをリダイレクトするように構成するには、次の配列を使用します。

- **denyList** : 認証が必要な場合に Web アプリケーションがユーザーをリダイレクトする URL を定義します。この構成は、主にリダイレクトベースの認証に不可欠ですが、一部のフォームベースの認証フローで特定の転送を防止するためにも使用できます。このキーにリストされている URL はリダイレクトされないため、サーバー側の認証が行われます。プロファイル共有が不要な場合に、ドメインの特定のサブ URL がクライアントにリダイレクトされないように制限するためにも使用できます。
- **profileSharing** : これは、シングルサインオン認証 Cookie およびユーザー設定を保存するその他の Cookie が共有されるように設定する必要があるキー値であり、サーバー側とクライアント側でレンダリングされるページ間の一貫した動作を保証します。
- **cookies** : Web アプリケーションがユーザーにプロンプトを表示せずに読み込まれるために必要な認証 Cookie を 1 つ以上定義します。拡張機能は、ここにリストされているすべての Cookie が指定された Web アプリ URL に対して設定されていると検出されるまで、クライアント側のリダイレクトを防止します。この設定は主にページ内フォームベース認証に使用されますが、特定のシナリオで denyList を指定することに加えて、リダイレクトベース認証にも利用できます。
- **deleteClientCache**: `bcrconfig.json` 構成メカニズムが使用されている場合、BCR クライアントはセキュリティ強化のためにデフォルトでブラウザキャッシュを削除します。このプロセスは、ユーザーがリダイレクトされたすべてのタブを閉じるか、セッションで初めてリダイレクトされたページを開始したときに発生します。この動作を防止するには、このキーの値を **false** に設定します。クライアントデバイスが信頼されている場合、このキーを **false** に設定すると、ユーザーエクスペリエンスが向上します。クライアントデバイスが信頼されていない場合、このキーを設定しない（または）このキーを **true** に設定すると、セキュリティ体制が強化されます。
- **schemaVersion** : これは主に拡張機能の内部およびログ記録の目的で使用されます。この記事の執筆時点では、その値は **2511** に設定されている必要があります。

構成例

```
{

  "apps": [

    {

      "appName": "myWebApp1",
```

```
    "allowList": [
      "https://myWebApp1.com/*"
    ],
    "denyList": [],
    "requires": {
      "profileSharing": false,
      "cookies": []
    }
  },
  {
    "appName": "myWebApp2",
    "allowList": [
      "https://myWebApp2.com/*"
    ],
    "denyList": [
      "https://myWebApp2.com/authPortal/*"
    ],
    "requires": {
      "profileSharing": true,
      "cookies": []
    }
  },
```

```
    {
      "appName": "myWebApp3",
      "allowList": [
        "https://*.myWebApp3.com/"
      ],
      "denyList": [
        "https://myWebApp3.com/authPortal/*"
      ],
      "requires": {
        "profileSharing": true,
        "cookies": [
          "requiredAuthCookie1",
          "requiredAuthCookie2"
        ]
      }
    }
  ],
  "preferences": {
    "deleteClientCache": true
  },
  "schemaVersion": "2511"
```

```
}
```

以下に `bcrconfig.json` ファイルのサンプルを示します。その要素については、以下で詳しく説明します。

上記の JSON 構造には、異なる構成を持つ 3 つのアプリが含まれています。

myWebApp1 シナリオ、SSO なし:

- `allowList` キーの文字列配列値は、`<https://myWebApp1.com>` 内のすべてのパスがクライアントにリダイレクトされるべきであることを指定します。ただし、`denyList` キーにリストされている値がある場合は除きます。
- `denyList` キーの文字列配列値は空であるため、認証サイトのリダイレクトは防止されません。したがって、認証は厳密にサーバー側で行われるわけではありません。
- `profileSharing` キーのブール値が **false** に設定されているため、`allowList` エントリに関連するクッキーはクライアントと共有されません。
- cookies キーの文字列配列は空ですが、`profileSharing` 共有キーが **false** に設定されているため、いずれにしても無視されます。

myWebApp2、リダイレクトベースの認証シナリオ:

- `allowList` キーの文字列配列値は、`<https://myWebApp2.com>` 内のすべてのパスがクライアントにリダイレクトされるべきであることを指定します。ただし、`denyList` キーにリストされている値がある場合は除きます。
- `denyList` キーの文字列配列値は、**myWebApp2.com** ドメイン下の `/authPortal/` で始まるパスがクライアント側のリダイレクトから除外され、サーバー側の認証が実行されるように指定します。
- `profileSharing` キーのブール値が **true** に設定されているため、allowList エントリに関連するクッキーはクライアントと共有され、シングルサインオンが実行されます。
- cookies キーの文字列配列は空であるため、拡張機能は、サーバー側認証後に特定のクッキーが設定されるのを待たずに、クライアントと共有します。

myWebApp3、フォームベースの認証シナリオ:

- `allowList` キーの文字列配列値は、`<https://myWebApp3.com>` 内のすべてのパスがクライアントにリダイレクトされるべきであることを指定します。ただし、`denyList` キーにリストされている値がある場合は除きます。

- `denyList` キーの文字列配列値は、**myWebApp3.com** ドメイン下の `/authPortal/` で始まるパスがクライアント側のリダイレクトから除外され、サーバー側の認証が実行されるように指定します。
- `profileSharing` キーのブール値が **true** に設定されているため、`allowList` エントリに関連するクッキーはクライアントと共有されます。
- cookies キーの文字列配列にはクッキー名が含まれているため、拡張機能はサーバー側認証後にこのクッキーが設定されるのを待ちます。`allowList` の関連 URL のクッキーはクライアントと共有され、クライアント側のリダイレクトが発生します。

環境設定

- `deleteClientCache` キーは **true** に設定されているため、BCR クライアントはセキュリティ強化のためにデフォルトでブラウザキャッシュを削除します。これは、キーが設定されていない場合でもデフォルトの動作です。

BCR ポリシーの構成

`bcrconfig.json` を作成したら、以下の手順に従って Browser Content Redirection ACL configuration を構成し、JSON ファイルのコンテンツを使用します。

- ファイルに `.bcrconfig.json` 拡張子を付けて名前を付けます。例: `myrules.bcrconfig.json`
- JSON ファイルを VDA からアクセス可能な Web サーバーでホストし、URL をメモします。

> **注:**
>
> サーバーはファイルのダウンロードを許可する必要があります。Microsoft IIS サイトは、デフォルトで JSON ファイルのダウンロードを許可しています。

- Citrix Studio の で、前の手順で取得した URL を 設定に追加します。

> **注:**
>
> 設定の他のエントリはそのまま残すことができます。競合が発生した場合、BCR 拡張機能は `bcrconfig.json` 設定を優先します。Citrix は、管理の容易さ、アプリケーションレベルの構成、およびスケーラビリティのために、構成全体を JSON に移行することを推奨します。

- ポリシーを保存し、セッションを起動してポリシー構成をテストします。

> **注:**
>
> ポリシーを設定した後、ホストされている `bcrconfig.json` ファイルをいつでも編集して調整できます。ファイルは、BCR 拡張機能を実行しているメインのブラウザプロセスが起動または再起動したときにのみ再ロードされ、変更が適用されます。

> **注:**
>
> - 要するに、ポリシーの観点からは、ブラウザコンテンツリダイレクトポリシー（デフォルトで有効）を有効にし、JSON ファイルを指す URL を使用してブラウザコンテンツリダイレクト ACL 構成ポリシーを構成するだけで済みます。
> - JSON 構成は現在、以下のポリシーに適用され、それらを柔軟にします。ただし、残りのポリシーは以前と同じ動作を継続します。
>
> - **ブラウザコンテンツリダイレクト ACL 構成:** ACL 内の URL は、`allowList` キーを介して JSON で構成できるようになりました。
> - **ブラウザコンテンツリダイレクトブロックリスト構成:** ブロックリストは、`denyList` キーを介して JSON で構成できるようになりました。
> - **ブラウザコンテンツリダイレクト認証サイト:** 認証サイトも、`denyList` キーを介して JSON で構成できます。

ウェブカメラのリダイレクトとビデオ圧縮

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

> 仮想セッション内で実行されているアプリケーションは、HDXウェブカメラビデオ圧縮またはHDXプラグアンドプレイ汎用USBリダイレクトを使用してウェブカメラを利用できます。モードを切り替えるには、**Citrix Workspace™アプリ > 環境設定 > デバイス**を使用します。可能であれば、常にHDXウェブカメラビデオ圧縮を使用することをお勧めします。HDX汎用USBリダイレクトは、HDXビデオ圧縮とのアプリケーション互換性の問題がある場合、またはウェブカメラの高度なネイティブ機能が必要な場合にのみ推奨されます。パフォーマンスを向上させるため、CitrixはVirtual Delivery Agentに少なくとも2つの仮想CPUを搭載することを推奨します。

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

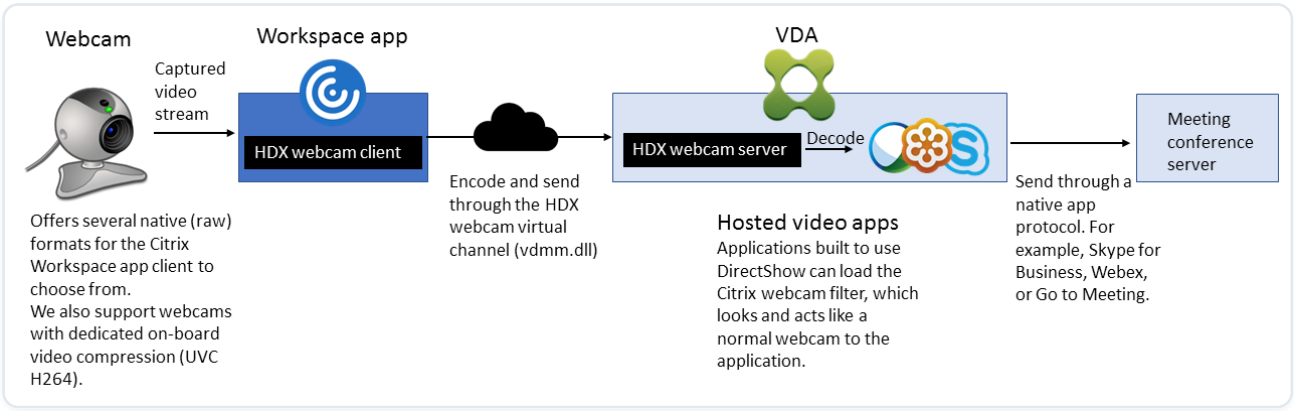
HDXウェブカメラビデオ圧縮

HDXウェブカメラビデオ圧縮は、**最適化された**ウェブカメラモードとも呼ばれます。この種類のウェブカメラビデオ圧縮は、H.264ビデオを仮想セッションで実行されているビデオ会議アプリケーションに直接送信します。VDAリソースを最適化するため、HDXウェブカメラ圧縮はウェブカメラビデオのエンコード、トランスコード、デコードを行いません。この機能はデフォルトで有効になっています。

サーバーからビデオ会議アプリへの直接ビデオストリーミングを無効にするには、VDAでレジストリキーを0に設定します。詳しくは、レジストリで管理される機能の一覧にあるウェブカメラビデオ圧縮を参照してください。

ビデオリソースをストリーミングするためのデフォルト機能を無効にすると、HDXウェブカメラビデオ圧縮は、クライアントオペレーティングシステムの一部であるマルチメディアフレームワークテクノロジーを使用して、キャプチャデバイスからのビデオをインターセプトし、トランスコードして圧縮します。キャプチャデバイスの製造元は、OSカーネルストリーミングアーキテクチャに接続するドライバーを提供します。

クライアントはウェブカメラとの通信を処理します。その後、クライアントはビデオを適切に表示できるサーバーにのみ送信します。サーバーはウェブカメラを直接処理しませんが、その統合によりデスクトップで同じエクスペリエンスが得られます。Workspaceアプリは、帯域幅を節約し、WANシナリオでの回復性を向上させるためにビデオを圧縮します。



HDXウェブカメラビデオ圧縮には、**マルチメディア会議**ポリシーを有効にする必要があります。このポリシーはデフォルトで有効になっています。

ウェブカメラがハードウェアエンコードをサポートしている場合、HDXビデオ圧縮はデフォルトでハードウェアエンコードを使用します。ハードウェアエンコードは、ソフトウェアエンコードよりも多くの帯域幅を消費する可能性があります。ソフトウェア圧縮を強制するには、クライアントでレジストリキーを編集します。詳しくは、レジストリで管理される機能の一覧にあるウェブカメラソフトウェア圧縮を参照してください。

HDXウェブカメラビデオ圧縮の要件

HDXウェブカメラビデオ圧縮は、Citrix Workspaceアプリの次のバージョンをサポートしています。

プラットフォーム	プロセッサー
Windows版 Citrix Workspaceアプリ	Windows向けCitrix Workspaceアプリは、XenAppおよびXenDesktop 7.17以降で32ビットおよび64ビットアプリのWebカメラビデオ圧縮をサポートしています。それ以前のバージョンでは、Windows向けCitrix Workspaceアプリは32ビットアプリのみをサポートしています。
Mac向けCitrix Workspaceアプリ	Mac向けCitrix Workspaceアプリ2006以降は、XenAppおよびXenDesktop 7.17以降で64ビットアプリのWebカメラビデオ圧縮をサポートしています。それ以前のバージョンでは、Mac向けCitrix Workspaceアプリは32ビットアプリのみをサポートしています。

プラットフォーム	プロセッサー
Linux向け Citrix Workspace アプリ	Linux向けCitrix Workspaceアプリは、仮想デスクトップ上で32ビットおよび64ビットの両方のアプリをサポートしています。
Chrome向けCitrix Workspaceアプリ	一部のARM ChromebookはH.264エンコーディングをサポートしていないため、32ビットアプリのみが最適化されたHDX Webカメラビデオ圧縮を使用できます。

Media Foundationベースのビデオアプリケーションは、Windows 10以降およびWindows Server 2019以降でHDX Webカメラビデオ圧縮をサポートしています。詳しくは、Knowledge Centerの記事CTX132764を参照してください。

その他のユーザーデバイス要件:

- サウンドを生成するための適切なハードウェア。
- DirectShow互換のWebカメラ（Webカメラのデフォルト設定を使用してください）。ハードウェアエンコーディング対応のWebカメラは、クライアント側のCPU使用率を低減します。
- HDX Webカメラビデオ圧縮の場合、可能であれば、カメラメーカーから入手したWebカメラドライバーをクライアントにインストールしてください。デバイスドライバーのインストールはサーバー上では不要です。

Webカメラによってフレームレート、明るさ、コントラストのレベルが異なります。Webカメラのコントラストを調整すると、アップストリームトラフィックを大幅に削減できます。Citrixは、初期機能検証のために以下のWebカメラを使用しています:

- Microsoft LifeCam VXモデル（2000、3000、5000、7000）
- クリエイティブ ライブ！カム オプティア プロ
- ロジクール クイックカム メッセンジャー
- ロジクール C600、C920
- HP デラックス ウェブカメラ

優先ビデオフレームレートを調整するには、クライアントでレジストリキーを編集します。詳細については、レジストリで管理される機能のリストにあるWebcam video compression frame rateを参照してください。

高解像度Webカメラストリーミング

サーバー上のビデオ会議アプリケーションは、サポートされているフォーマットタイプに基づいてWebカメラのフォーマットと解像度を選択します。セッションが開始されると、クライアントはWebカメラ情報をサーバーに送信します。アプリケーションからWebカメラを選択します。Webカメラとビデオ会議アプリケーションが高解像度レンダリングをサポートしている場合、アプリケーションは高解像度を使用します。すべてのWebカメラ解像度をサポートしています。

この機能には、Citrix Workspaceアプリ for Windows バージョン1808以降、またはCitrix Receiver for Windows バージョン4.10以降が必要です。

レジストリキーを使用して、この機能を無効または有効にできます。詳細については、レジストリで管理される機能のリストにあるHigh-definition webcam streamingを参照してください。

メディアタイプのネゴシエーションが失敗した場合、HDXはデフォルトのVGA解像度（640 x 480 ピクセル）にフォールバックします。クライアントのレジストリキーを使用して、デフォルトの解像度を構成できます。カメラが指定された解像度をサポートしていることを確認してください。詳細については、レジストリで管理される機能のリストにあるHigh-definition webcam resolutionを参照してください。

HDX Webカメラビデオ圧縮は、プラグアンドプレイの汎用USBリダイレクトと比較して帯域幅を大幅に削減し、WAN接続でも良好に機能します。帯域幅を調整するには、クライアントでレジストリキーを設定します。詳細については、レジストリで管理される機能のリストにあるHigh-definition webcam bandwidthを参照してください。

ビット/秒単位で値を入力します。帯域幅を指定しない場合、ビデオ会議アプリケーションはデフォルトで350000 bpsを使用します。

HDXプラグアンドプレイ汎用USBリダイレクト

HDXプラグアンドプレイ汎用USBリダイレクト（アイソクロナス）は、**汎用**Webカメラモードとも呼ばれます。HDXプラグアンドプレイ汎用USBリダイレクトの利点は、シンクライアント/エンドポイントにドライバーをインストールする必要がないことです。USBスタックは仮想化されており、ローカルクライアントに接続したものはすべてリモートVMに送信されます。リモートデスクトップは、ネイティブに接続したかのように動作します。Windowsデスクトップは、ハードウェアとのすべてのやり取りを処理し、プラグアンドプレイロジックを実行して正しいドライバーを見つけます。ほとんどのWebカメラは、ドライバーがサーバーに存在し、ICA経由で動作する場合に機能します。汎用Webカメラモードは、USBプロトコルで非圧縮ビデオをネットワーク経由で送信するため、大幅に多くの帯域幅（毎秒数メガビット）を使用します。

WebカメラリダイレクトによるMicrosoft仮想カメラのサポート

2603以降、Windows VDA（Windows 11およびWindows Server 2025）は、Microsoftの組み込み仮想カメラ機能を使用してWebカメラリダイレクトとカメラエクスペリエンスをアップグレードします。利点には、より多くのアプリケーションとの互換性の拡張、セキュリティとプライバシーの向上、ローカルおよびネイティブのカメラエクスペリエンスに近い提供が含まれます。この機能はデフォルトで有効になっています。

> **注:**
>
> この機能には、システム設定で**カメラアクセス**が有効になっている必要があります。Windows Server 2025では、この設定はデフォルトで無効になっています。

HTML5 マルチメディアリダイレクト

> **注:**
>
> HTML5 マルチメディアリダイレクトは、将来のリリースで非推奨となる予定です。お客様は、継続的な機能性を確保するために、推奨される代替テクノロジーであるブラウザコンテンツリダイレクト (BCR) への移行をお勧めします。

> HTML5 マルチメディアリダイレクトは、HDX™ MediaStream のマルチメディアリダイレクト機能を拡張し、HTML5 オーディオとビデオを含みます。特にモバイルデバイスへのマルチメディアコンテンツのオンライン配信の増加により、ブラウザ業界はオーディオとビデオを提示するためのより効率的な方法を開発しました。

Flash は標準でしたが、プラグインが必要で、すべてのデバイスで動作せず、モバイルデバイスではバッテリー消費量が多くなります。YouTube、Netflix、および Mozilla、Google、Microsoft の新しいブラウザバージョンなどの企業は、HTML5 に移行しており、これが新しい標準となっています。

HTML5 ベースのマルチメディアには、独自のプラグインに比べて多くの利点があります。

- 企業に依存しない標準 (W3C)
- 簡素化されたデジタル著作権管理 (DRM) ワークフロー
- プラグインによって引き起こされるセキュリティ問題なしにパフォーマンスの向上

HTTP プログレッシブダウンロード

HTTP プログレッシブダウンロードは、HTML5 をサポートする HTTP ベースの疑似ストリーミング方式です。プログレッシブダウンロードでは、ブラウザは HTTP Web サーバーからダウンロード中に単一のファイル（単一の品質でエンコードされたもの）を再生します。ビデオは受信時にドライブに保存され、ドライブから再生されます。ビデオを再視聴する場合、ブラウザはキャッシュからビデオを読み込むことができます。

プログレッシブダウンロードの例については、HTML5 ビデオ リダイレクト テスト ページ を参照してください。ウェブページ内のビデオ要素を検査し、HTML5 ビデオタグ内のソース (mp4 コンテナ形式) を見つけるには、ブラウザの開発者ツールを使用します。

HTML5 と Flash の比較

機能	HTML5	フラッシュ
独自のプレーヤーが必要	いいえ	はい
モバイルデバイスで実行	はい	一部
さまざまなプラットフォームでの実行速度	高	低速
iOSでサポート	はい	いいえ
リソース使用量	少ない	多い
より速くロード	はい	いいえ

要件

mp4形式のプログレッシブダウンロードのリダイレクトのみをサポートしています。WebMおよびDASH/HLSのようなアダプティブビットレートストリーミング技術はサポートしていません。

以下をサポートしており、ポリシーを使用してこれらを制御します。詳細については、「マルチメディアポリシー設定」を参照してください。

- サーバー側レンダリング
- サーバーフェッチクライアントレンダリング
- クライアント側フェッチとレンダリング

Citrix Workspace™アプリおよびCitrix Receiver™の最小バージョン:

- Windows向けCitrix Workspaceアプリ1808
- シトリックス レシーバー for Windows 4.5
- シトリックス ワークスペース アプリ 1808 for Linux
- シトリックス レシーバー for Linux 13.5

最小VDAブラウザバージョン	WINDOWS オペレーティングシステム バージョン/ビルド/サービスパック
インターネット エクスプローラー 11.0	Windows 10 x86 (1607 RS1) および x64 (1607 RS1); Windows 7 x86 および x64; Windows サーバー 2016 RTM 14393 (1607); Windows サーバー 2012 R2
Firefox 47 証明書を手動でFirefoxの証明書ストアに追加するか、Windowsの信頼された証明書ストアから証明書を検索するようにFirefoxを構成します。詳細については、`https://wiki.mozilla.org/CA:AddRootToFirefox`を参照してください。	ウィンドウズ 10 x86 (1607 RS1) および x64 (1607 RS1); ウィンドウズ 7 x86 および x64; ウィンドウズ サーバー 2016 RTM 14393 (1607); ウィンドウズ サーバー 2012 R2
クローム 51	ウィンドウズ 10 x86 (1607 RS1) および x64 (1607 RS1); ウィンドウズ 7 x86 および x64; ウィンドウズ サーバー 2016 RTM 14393 (1607); ウィンドウズ サーバー 2012 R2

HTML5ビデオリダイレクトソリューションのコンポーネント

- **HdxVideo.js** - Webサイト上のビデオコマンドをインターセプトするJavaScriptフック。HdxVideo.jsは、セキュアWebSocket (SSL/TLS) を使用してWebSocketServiceと通信します。
- **WebSocket SSL証明書**
  - CA (ルート) の場合: **Citrix XenApp/XenDesktop HDX In-Product CA** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp and XenDesktop Engineering; CN = Citrix XenApp and XenDesktop HDX In-Product CA) 場所: **証明書 (ローカルコンピューター) > 信頼されたルート証明機関 > 証明書**。
  - エンドエンティティ (リーフ) の場合: **Citrix XenApp/XenDesktop HDX Service** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp and XenDesktop Engineering; CN = Citrix XenApp and XenDesktop HDX Service) 場所: **証明書 (ローカルコンピューター) > 個人 > 証明書**。

- **WebSocketService.exe** - ローカルシステムで実行され、SSL終端とユーザーセッションマッピングを実行します。TLS Secure WebSocketは127.0.0.1ポート9001でリッスンしています。
- **WebSocketAgent.exe** - ユーザーセッションで実行され、WebSocketServiceコマンドの指示に従ってビデオをレンダリングします。

HTML5ビデオのリダイレクトを有効にするにはどうすればよいですか?

このリリースでは、この機能は制御されたWebページでのみ利用可能です。HTML5マルチメディアコンテンツが利用可能なWebページに、HdxVideo.js JavaScript（Citrix Virtual Apps and Desktopsインストールメディアに含まれています）を追加する必要があります。たとえば、社内トレーニングサイトのビデオなどです。

youtube.comのような、アダプティブビットレート技術（例: HTTP Live Streaming (HLS) および Dynamic Adaptive Streaming over HTTP (DASH)）に基づいたウェブサイトはサポートされていません。

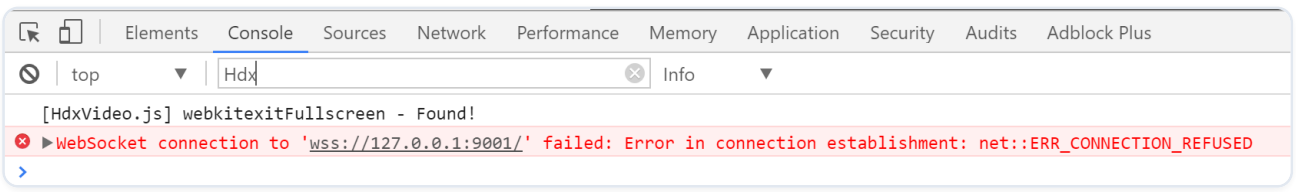
詳細については、「*マルチメディアポリシー設定*」を参照してください。

リダイレクトされたコンテンツをスクリーンショットでキャプチャする

HTML5マルチメディアリダイレクトはエンドポイントでビデオをレンダリングするため、標準のセッション内スクリーンショットツールでは、リダイレクトされたビデオが空白領域としてキャプチャされます。このコンテンツをスクリーンショットに含めるには、Citrix Snipping Toolを使用してください。Citrixでは、見つけやすくするためにCitrix Virtual Desktop Assistantから起動することをお勧めします。詳細については、「Citrix Virtual Desktop Assistantドキュメント」を参照してください。

トラブルシューティングのヒント

WebページがHdxVideo.jsを実行しようとすると、エラーが発生する可能性があります。JavaScriptの読み込みに失敗すると、HTML5リダイレクトメカニズムも失敗します。ブラウザの開発者ツールウィンドウでコンソールを検査し、HdxVideo.jsに関連するエラーがないことを確認してください。例:



Microsoft Teams の最適化 (新規)

Citrix® は、VDI 環境で Microsoft Teams のオーディオとビデオを最適化する 2 つの方法をサポートしています。Citrix HDX™ Optimization と、Microsoft が提供する Teams 用の新しい VDI ソリューションです。Classic Teams はサポート終了に達したため、このページで説明されている最適化アプローチは現在の Microsoft Teams クライアントに適用されます。

> **注:**

> Microsoft は、Windows エンドポイントにおける WebRTC ベースの Citrix HDX Optimization for Microsoft Teams の非推奨化を発表しました。以下の 2 つのマイルストーンが適用されます。

> - October 1, 2026 - サポート終了: Microsoft または Citrix による公式サポートは終了します。
> - April 1, 2027 - 提供終了: WebRTC ベースの最適化は機能しなくなります。レガシー最適化のための Citrix Studio ポリシーは適用されなくなります。

> お客様は、Teams 用の新しい VDI ソリューションへの移行をお勧めします。この変更は Windows エンドポイントのみに影響します。macOS、Linux、ChromeOS、および HTML5 エンドポイントは影響を受けません。詳細については、Microsoft Blog を参照してください。

最適化アプローチ

- **Citrix HDX Optimization (MTOP)**: Citrix と Microsoft の組み合わせソリューションで、Citrix が所有する仮想チャネル (CTXMTOP) を使用します。メディアオフロードは、Citrix Workspace™ アプリの `HdxRtcEngine` によって処理されます。このソリューションは、従来 MTOP と呼ばれています。
- **Teams 用の新しい VDI ソリューション**: Microsoft が所有および管理する新しい最適化で、Microsoft が所有する仮想チャネル (MSTEAMS、MSTEAM1、MSTEAM2) を使用します。Windows および Mac エンドポイントで利用できます。詳細については、Microsoft ドキュメントの Teams 用の新しい VDI ソリューション を参照してください。

> **注:**

どの最適化アプローチを使用しても、Microsoft Teams のビデオと画面共有はエンドポイントでレンダリングされます。その結果、標準のセッション内スクリーンショットツールでは、このコンテンツが空白領域としてキャプチャされます。スクリーンショットに含めるには、Citrix Snipping Tool を使用してください。Citrix は、見つけやすくするために Citrix Virtual Desktop Assistant から起動することをお勧めします。詳細については、Citrix Virtual Desktop Assistant ドキュメント を参照してください。

主な違い

CITRIX HDX 最適化	TEAMS 用の新しい VDI ソリューション
最適化は、Citrix と Microsoft の組み合わせソリューションであり、Citrix が所有する仮想チャネル (CTXMTOP) を使用します。	最適化ソリューションは Microsoft が所有および管理しており、Microsoft が所有する仮想チャネル (MSTEAMS、MSTEAM1、MSTEAM2) を使用します。
メディアオフロードは、Citrix Workspaceアプリにある`HdxRtcEngine`によって処理されます。	メディアオフロードは、WindowsおよびMacエンドポイント上のSlimCoreメディアエンジンによって処理されます。
Citrix Workspaceアプリのインストールを除き、エンドポイントに追加のコンポーネントは不要です。	追加コンポーネント - **Teams VDIプラグイン**は、さまざまな方法でエンドポイントに展開する必要があります。このプラグインは、SlimCoreメディアエンジンのダウンロードと更新を管理します。
エンドポイントプラットフォーム (Windows、macOS、Linux、ChromeOS) で利用可能です。	エンドポイントプラットフォーム (WindowsおよびMac) で利用可能です。
新機能はCitrixとMicrosoftの連携により管理されます。	新機能はMicrosoftによって管理されます。ユーザーは、Citrix HDX最適化では利用できない一部の新機能にアクセスできます。
関連するコンポーネントに応じて、CitrixとMicrosoftの両方によってサポートされます。お客様はCitrixまたはMicrosoftのいずれかにケースをオープンでき、必要に応じて適切なチームにリダイレクトされます。	Microsoftが所有し、サポートしています。Citrixは、Citrix Workspaceアプリ、仮想チャネル許可リスト、プラグイン展開メカニズムなど、関連するCitrixコンポーネントをサポートします。

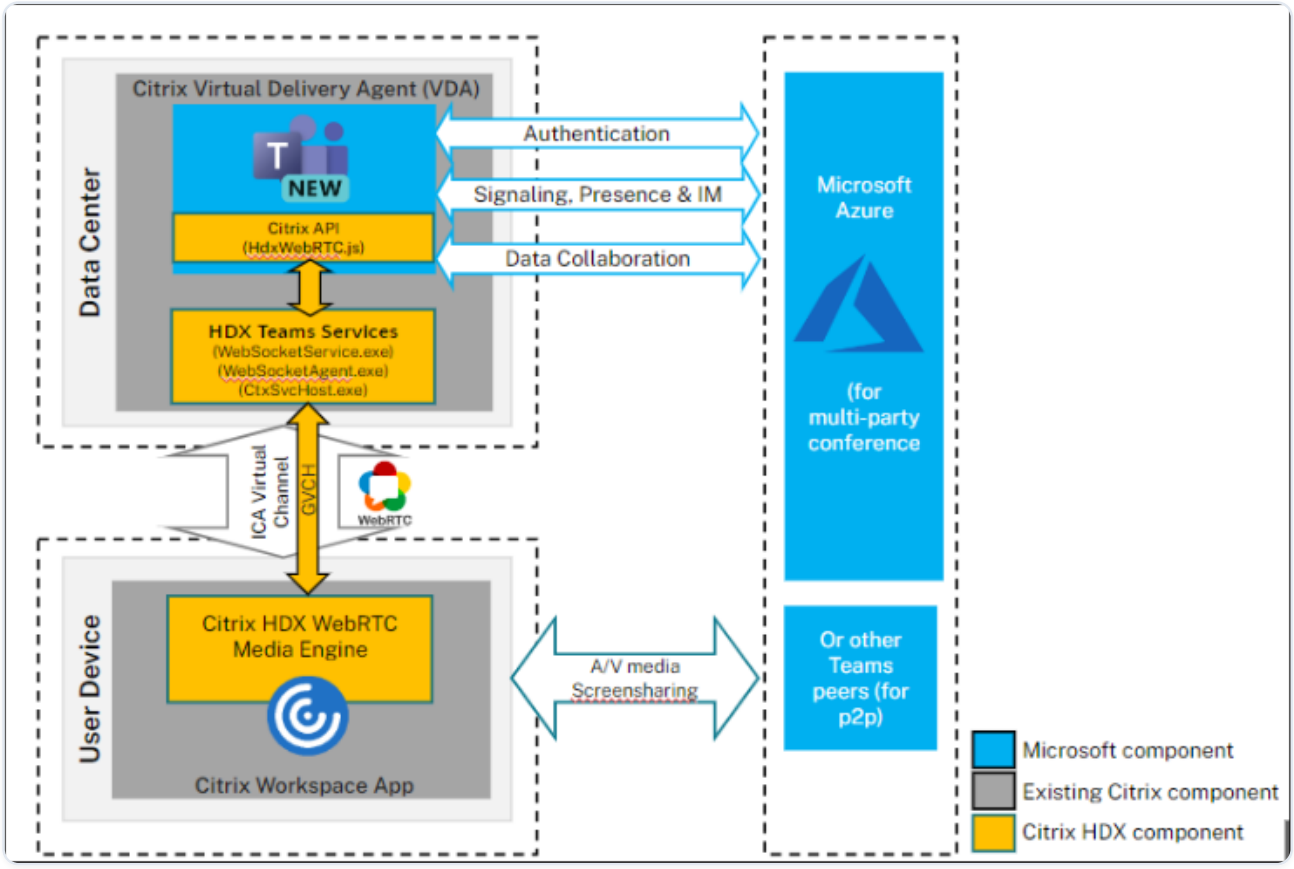
相互運用性とローミング

Citrix HDX最適化とTeams向けの新VDIソリューションは並行して存在できますが、Teamsクライアントは一度にいずれか一方のみを使用します。

- Teamsアプリの起動時に、次の順序で最適化が選択されます。Teams向けの新VDIソリューション、次にCitrix HDX最適化 (WebRTC)、次に標準のオーディオ/ビデオリダイレクト。
- Teams向けの新VDIソリューションが失敗した場合、TeamsはWebRTCではなく、標準のオーディオ/ビデオリダイレクトに直接フォールバックします。選択を再実行し、適切な最適化を選択するには、Teamsアプリの再起動が必要です。
- エンドポイント間のローミングはシームレスであり、Teamsアプリの再起動は不要です。これには、Teams向けの新VDIソリューションをサポートするエンドポイントとサポートしないエンドポイントの間でユーザーがローミングする場合も含まれます。

Citrix HDX™ 最適化

Citrix HDX (WebRTC 最適化) では、オフロードされたメディアの処理を担当するエンドポイント上のメディアエンジン (HdxRtcEngine) は Citrix Workspace™ アプリに組み込まれており、Citrix Workspace アプリをインストールすると、エンジンも自動的にインストールされます。



システム要件

このセクションでは、新しい Teams クライアントをサポートするために必要な最小バージョンと推奨バージョンを示します。最小バージョンでは、一部の重要なバグ修正や最新機能が利用できない場合があることに注意してください。最新の修正と機能で最高の体験を得るには、推奨バージョンを展開してください。

VDI オペレーティングシステム

詳細については、Microsoft ドキュメントに記載されている推奨事項を参照してください。

注:

- Windows Server 2016 はサポートされていません。Citrix は、それに応じてアップグレードを計画することをお勧めします。
- バージョンは頻繁に更新されるため、ここで言及されているバージョンはサポート終了となる可能性があります。したがって、さまざまなコンポーネントのサポートされているバージョンを使用していることを確認するために、Citrix Workspace app および Citrix Virtual Apps and Desktops の製品ライフサイクルページを参照してください。
- Citrix Virtual Apps and Desktops™ 1912 LTSR をご利用の場合、2024年12月にサポート終了となるため、Citrix はアップグレードを計画することをお勧めします。

仮想配信エージェント (VDA)

最小バージョン	推奨バージョン
1912 LTSR CU8+; 2203 LTSR (任意のCU); 2212 CR	2203 LTSR CU5+ (または) 2402 LTSR およびそれ以降のCRバージョン

Citrix Workspaceアプリ

最小バージョン	推奨バージョン
Windows 2203 LTSR (最新の累積更新プログラム); Windows 2302 CR; Linux 2207; Mac 2302; Chrome/HTML5 2301	ウィンドウズ 2402 LTSR; ウィンドウズ 2405 CR; リナックス 2405; マック 2405; クローム OS/HTML5 2405

展開

1. VDIに新しいTeamsクライアントをインストールします。詳細については、VDI向け新しいTeamsの展開を参照してください。
2. 新しいTeamsを最適化するために、VDAで以下のレジストリキーを構成します。
   - **場所**: `HKLM\SOFTWARE\WOW6432Node\Citrix\WebSocketService`
   - **キー (REG_Multi_SZ)**: `ProcessWhitelist`
   - **値**: `msedgewebview2.exe`

   > **注:**
   >
   > Citrix Virtual Apps and Desktops 2402 LTSR (または) Citrix Virtual Apps and Desktops 2203 LTSR CU5+ 以降では、`msedgewebview2.exe` レジストリエントリはデフォルトで許可リストに含まれているため、手動で構成する必要はありません。

3. Microsoft Teamsリダイレクト ポリシーが有効になっていることを確認してください。このポリシーはデフォルトで有効になっています。
4. クライアント側で追加の構成は必要ありません。ウィザードの指示に従ってCitrix Workspaceアプリをインストールしてください。

App レイヤリング

新しいMicrosoft Teamsはインストール方法が変更され、C:\Program Files\WindowsApps にインストールされるようになりました。この変更をサポートするには、App Layeringバージョン2403.2以降を実行する必要があります。この修正を含むアップグレードディスクは、App Layeringダウンロード ページからダウンロードできます。

詳細については、App Layering ドキュメントを参照してください。

Citrix プロファイル管理

New Microsoft Teams のローミングを有効にする方法については、Citrix Profile Management のドキュメントを参照してください。Citrix Profile Management の現在の最小バージョンガイダンスは 2402 LTSR (または) 2203 LTSR CU5+ です。

ネットワークに関する考慮事項

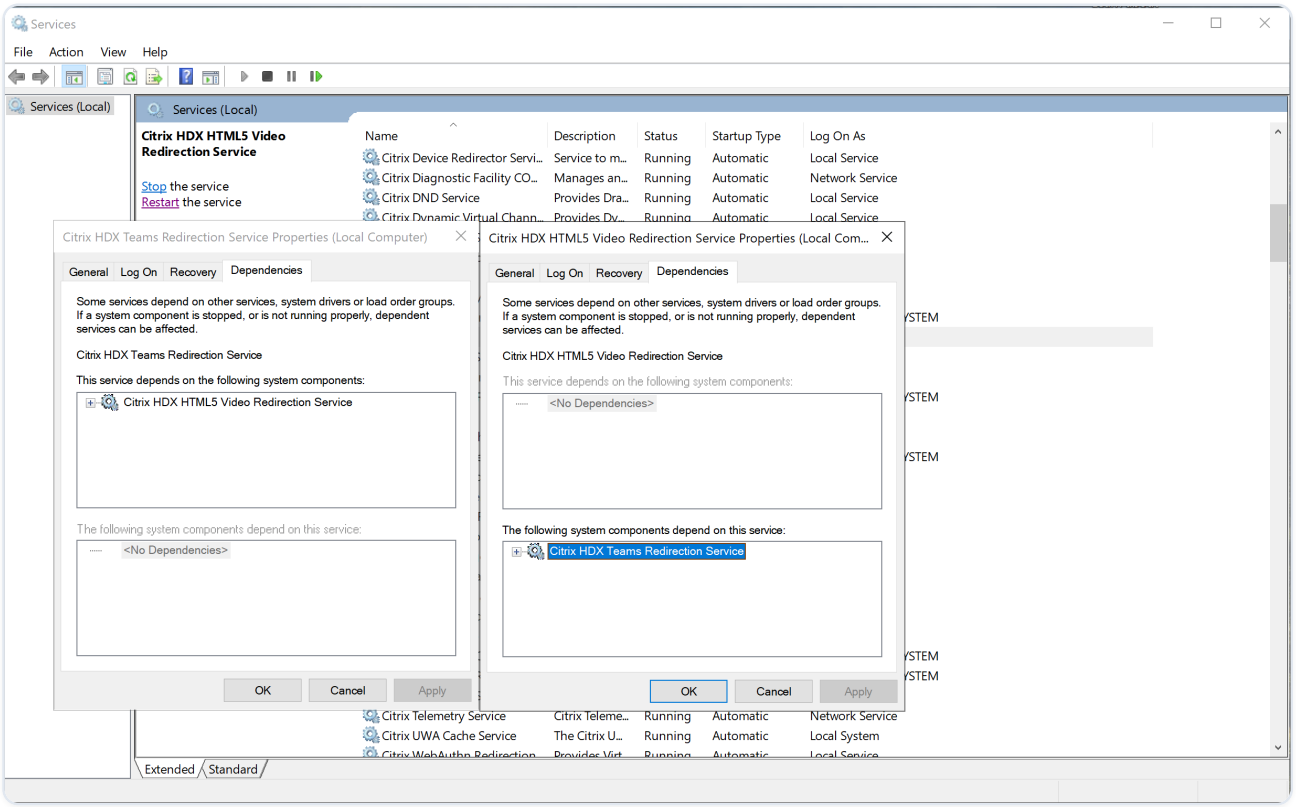
New Teams のネットワーク要件は Classic Teams と変わりません。したがって、Classic Teams ドキュメントのネットワーク要件セクションを参照してください。

機能リファレンス

Microsoft Teams 最適化の明示的なサービス依存関係

Citrix Virtual Apps / Desktops 2603以降、**Citrix HDX Teams Redirection Service**（HDX最適化Microsoft TeamsおよびUCSDK最適化アプリケーションで使用）は、**Citrix HDX HTML5 Video Redirection Service (WebSocketService)**への依存関係を明示的に宣言するようになりました。

この更新により、Teamsサービスが起動したときにHTML5サービスが自動的に検証され、開始されることが保証され、サービスが厳密に管理されている環境においてMicrosoft TeamsおよびUCSDK統合アプリケーションの最適化の失敗を防ぎます。



パフォーマンスとユーザーエクスペリエンスを向上させる最適化されたオーバーレイクリッピング

CVAD 2511以降、HDX Microsoft Teams OptimizationやUCSDK Optimizationなどの機能におけるリダイレクトされたビデオオーバーレイを処理するメカニズムは、ユーザーエクスペリエンスとサーバーパフォーマンスの両方を向上させるために再設計されました。

主な利点

- **視覚的な正確性の向上:** この機能強化により、ポップアップメニューや通知などのアプリケーション要素がビデオコンテンツの背後に誤って表示される視覚的な不具合が解決されます。新しいロジックにより、すべてのコンポーネントが正しい順序でレンダリングされ、よりシームレスで予測可能なエクスペリエンスが提供されます。

- **パフォーマンスの向上:** この最適化により、Virtual Delivery AgentのCPU使用率が大幅に削減されます。古いリソース集約型のポーリング方法をより効率的なグラフィックスベースのアプローチに置き換えることで、この変更はサーバーのスケーラビリティを向上させ、より高いユーザー密度を可能にします。

> **注:**
>
> この機能は、将来のバージョンのMicrosoft Teams（またはその他のUCSDKパートナーアプリケーション）に依存し、Citrix Workspace App for Windows 2511が必要です。

機能マトリックスとバージョンサポート

バージョンは頻繁に更新されるため、ここで言及されている一部の古いバージョンはサポート終了となる可能性があります。したがって、さまざまなコンポーネントのサポートされているバージョンを使用していることを確認するために、Citrix Workspace App および Citrix Virtual Apps and Desktops の製品ライフサイクルページを参照してください。

> **注:**
>
> - ここで言及されているバージョンは、特定の機能がサポートされる最小バージョン、または New Teams がサポートされる最小バージョンのうち、いずれか高い方です。
> - 最小バージョンセクションに記載されているCitrix Virtual Apps and Desktops™ 1912 LTSR CU8+は、2024年12月にサポート終了となるため、以下の表には記載されていません。ただし、それまでは引き続きサポートされるバージョンです。
> - Citrix Virtual Apps and Desktops の最小バージョンが `N/A` となっている機能は、VDA側で変更がなかったことを意味します。

機能	VDA (最小バージョン)	WINDOWS 用 CITRIX WORKSPACE アプリ (最小バージョン)	MAC 向け CITRIX WORKSPACE アプリ (最小バージョン)	LINUX 向け CITRIX WORKSPACE アプリ (最小バージョン)	CHROMEOS 用 CITRIX WORKSPACE アプリ (最小バージョン)
オーディオ/ビデオ (p2p および会議)	2203 LTSR (任意の CU)、2212 CR	2203 LTSR 最新 CU、2302 CR	2302	2207	2301
画面共有	2203 LTSR (任意の CU)、2212 CR	2203 LTSR 最新 CU、2302 CR	2302	2207	2301
i. 画面インジケーターの赤い枠線	2203 LTSR (任意の CU)、2212 CR	2203 LTSR 最新 CU、2302 CR	2302	2207	いいえ
ii. キャプチャを Desktop Viewerに制限	2203 LTSR (任意の CU)、2212 CR	2203 LTSR 最新 CU、2302 CR	2302	2207	いいえ
iii. マルチモニター	2203 LTSR (任意の CU)、2212 CR	2203 LTSR 最新 CU、2302 CR	2302	2207	いいえ
DTMF	該当なし	2203 LTSR 最新 CU、2302 CR	2302	2207	2301
プロキシサーバーのサポート	該当なし	2203 LTSR 最新 CU、2302 CR	2302	2207	2305

機能	VDA (最小バージョン)	WINDOWS 用 CITRIX WORKSPACE アプリ (最小バージョン)	MAC 向け CITRIX WORKSPACE アプリ (最小バージョン)	LINUX 向け CITRIX WORKSPACE アプリ (最小バージョン)	CHROMEOS 用 CITRIX WORKSPACE アプリ (最小バージョン)
アプリ共有	2203 LTSR (任意の CU)、2212 CR	2203 LTSR 最新 CU、2302 CR	2302	2209	いいえ
ライブキャプション	該当なし	2203 LTSR 最新 CU、2302 CR	2302	2207	2303
動的e911	該当なし	2203 LTSR 最新 CU、2302 CR	2302	2207	2301
制御を付与	該当なし	2203 LTSR 最新 CU、2302 CR	2302	2207	いいえ
制御を要求	該当なし	2203 LTSR 最新 CU、2302 CR	2302	2207	2303
マルチウィンドウ	2203 LTSR (任意の CU)、2212 CR	2203 LTSR 最新 CU、2302 CR	2302	2207	2303
会議の文字起こし	2203 LTSR (任意の CU)、2212 CR	2203 LTSR 最新 CU、2302 CR	2302	2207	2303
背景のぼかし	2203 LTSR (任意の	2203 LTSR 最新 CU、2302 CR	2302	2212	2303

機能	VDA (最小バージョン)	WINDOWS 用 CITRIX WORKSPACE アプリ (最小バージョン)	MAC 向け CITRIX WORKSPACE アプリ (最小バージョン)	LINUX 向け CITRIX WORKSPACE アプリ (最小バージョン)	CHROMEOS 用 CITRIX WORKSPACE アプリ (最小バージョン)
	CU)、2212 CR				
画面共有 (App Protection 使用時)	2203 LTSR (任意の CU)、2212 CR	2402 LTSR、2309.1 CR	2308	2311	いいえ
サイマルキャスト	2203 LTSR (任意の CU)、2212 CR	2402 LTSR、2305 CR	2305	2305	2312
セカンダリリンガー	2203 LTSR (任意の CU)、2212 CR	2402 LTSR、2307.1 CR	2308	2308	2312
システムオーディオの共有	2203 LTSR (任意の CU)、2212 CR	2402 LTSR、2403 CR	2405	2402	いいえ

トラブルシューティングとその他の考慮事項

新しいTeamsについては、CTX253754、Microsoft Teamsのトラブルシューティングを参照してください。新しいTeamsに関連する最新情報については、CTX585013を参照してください。

既知の制限事項

Citrix Workspaceアプリの制限事項

- HIDサポート - 通話の応答と終了はサポートされていません。音量の上げ下げはサポートされています。

- ユーザーは、VDAでSnipping Toolを使用している間、Microsoft Teamsのコンテンツのスクリーンショットを撮ることはできません。ただし、クライアント側でSnipping Toolを使用した場合、コンテンツをキャプチャできます。
- システムオーディオ共有の制限
  - RAVEおよびBCRリダイレクトされたアプリまたはタブで画面を共有している場合、この機能を使用してオーディオを共有することはできません。
  - この機能は、公開デスクトップでのみサポートされています。

VDAに関する制限事項

- 公開された（シームレスな）アプリケーションとしての新しいTeamsはサポートされていません。
  - CVAD 2402 LTSR、2203 LTSR CU5以降で修正済み
- Citrix WorkspaceアプリのHigh DPI設定を「はい」に構成すると、リダイレクトされたビデオウィンドウがずれて表示されます。この制限は、モニターのDPIスケーリング係数が100%を超えて設定されている場合に発生します。
- Microsoft Teams 2.1は、一度に1つのWebカメラのリダイレクトのみをサポートします。ただし、シングルセッションVDAでは、複数のWebカメラのリダイレクトやプラグアンドプレイ（PnP）Webカメラのリダイレクトはサポートしていません。

Citrix WorkspaceアプリとVDAに関する制限事項

- 最適化された通話の音量は、クライアントマシンの音量バーを使用してのみ制御できます。VDA上では制御できません。

Microsoftからの制限事項の詳細については、「VDIでサポートされていない機能」を参照してください。

Teams向け新しいVDIソリューション

> **注:**
>
> Teams向け新しいVDIソリューションは、現在、Citrix®上のWindowsおよびMacエンドポイント向けに一般提供されています。このソリューションには、最小バージョンのMicrosoft Teamsが必要です。「システム要件」(#system-requirements)を参照してください。

Teams向け新しいVDIソリューションでは、MicrosoftはCitrix Virtual Channel SDKを使用してカスタム仮想チャネルを構築します。エンドポイントでは、メディアは`HdxRtcEngine`ではなく、Microsoftメディアエンジン (SlimCore) にオフロードされます。カスタム仮想チャネルは、VDA上のTeamsとエンドポイント上のメディアエンジン間の通信を伝送します。

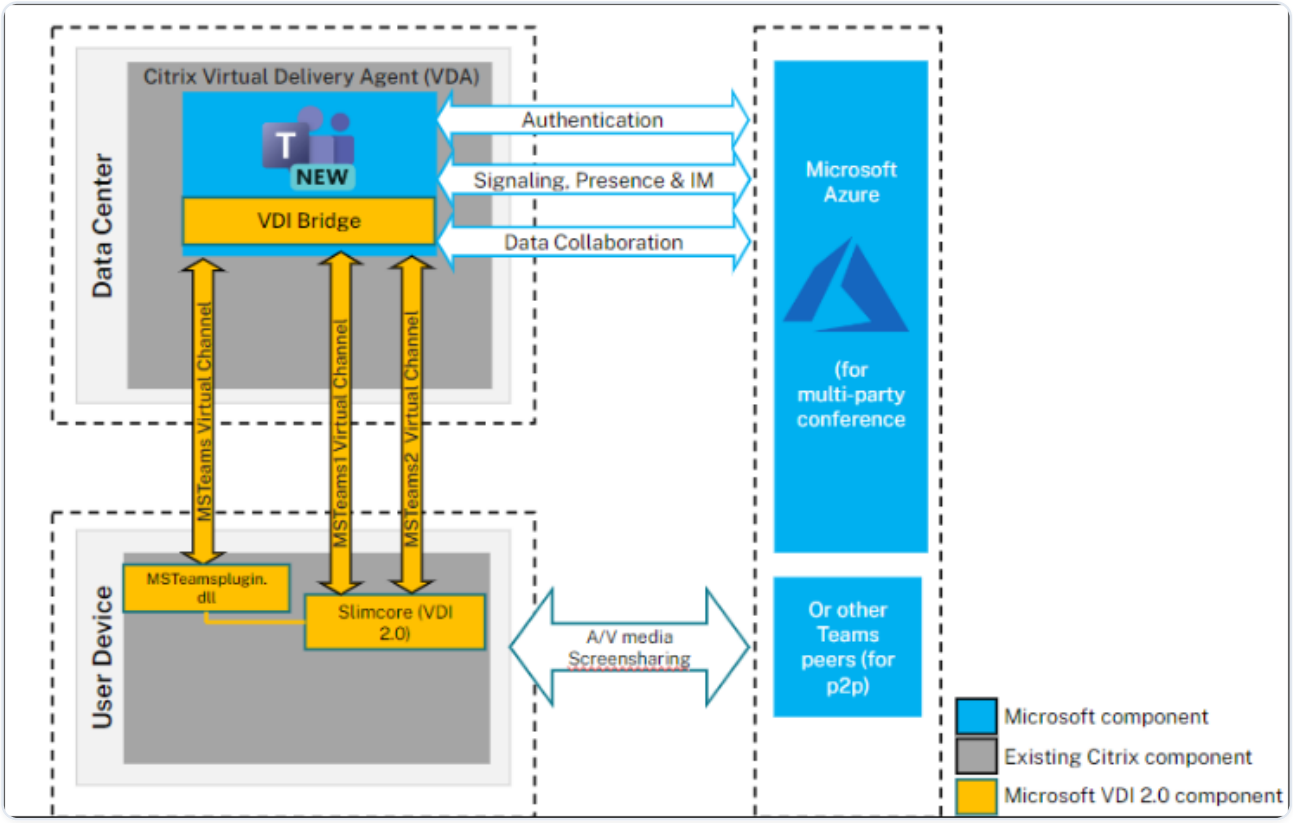
注:

Microsoftは、WindowsエンドポイントにおけるWebRTCベースのCitrix HDX™ Optimization for Microsoft Teamsの廃止を発表しました。2つのマイルストーンが適用されます。

- October 1, 2026 - サポート終了: MicrosoftまたはCitrixによって公式にサポートされなくなります。
- April 1, 2027 - 提供終了: WebRTCベースの最適化は機能しなくなります。レガシー最適化用のCitrix Studioポリシーは適用されなくなります。

お客様は、Teams向け新しいVDIソリューションへの移行をお勧めします。この変更はWindowsエンドポイントのみに影響します。macOS、Linux、ChromeOS、およびHTML5エンドポイントは影響を受けません。詳細については、Microsoftブログを参照してください。

このソリューションはMicrosoftが所有および管理しています。Citrixは、関連するCitrixコンポーネント（Citrix Workspace™アプリ、仮想チャネル許可リスト、およびこのページで説明されているプラグイン展開メカニズム）をサポートします。Microsoftが所有するアーキテクチャと詳細については、MicrosoftドキュメントのTeams向け新しいVDIソリューションを参照してください。



システム要件

このセクションでは、Teams向け新しいVDIソリューションをサポートするために必要な最小バージョンと推奨バージョンを一覧表示します。最小バージョンでは、一部の重要なバグ修正や最新機能が利用できない場合があります。最良のエクスペリエンスを得るには、推奨バージョンを展開してください。

仮想配信エージェント (VDA)

> **注:**
>
> 2203 LTSR CU2以前、または2303 CR以前をご利用の場合は、これらのバージョンの制限を理解し、アップグレードを計画するためにCTX682593を参照してください。

最小バージョン	推奨バージョン
2203 LTSR CU3; 2305 CR	2203 LTSR CU5+; 2402 LTSR およびそれ以降のCR

Windows版 Citrix Workspaceアプリ

最小バージョン	推奨バージョン
2203 LTSR (最新 CU); 2302 CR	2402 LTSR; 2405 CR またはそれ以降

Mac向けCitrix Workspaceアプリ

最小バージョン	推奨バージョン
2508.10	2607 またはそれ以降

MacエンドポイントにはmacOS 14、15、または26が必要です。macOS 26では、Citrix Workspaceアプリ2511以降が必要です。Citrix Workspaceアプリ for Mac 2508.10では、プラグインを手動でインストールする必要があります。Citrix Workspaceアプリ、クライアントアプリ管理、または仮想チャネルプラグインマネージャーを介してプラグインをインストールするオプションは、Citrix Workspaceアプリ for Mac 2603以降で利用可能です。

最小Microsoft Teamsバージョン、エンドポイントOS要件、およびハードウェア要件については、Microsoftドキュメントを参照してください。

コンポーネント

- 新しいTeams `vdiBridge`: Teamsにバンドルされているサーバー側仮想チャネルモジュール。
- カスタム仮想チャネル (VC): Microsoft Teamsが所有するカスタムVC。
- プラグイン: クライアント側VC DLL。メディアエンジンのダウンロードとクリーンアップを担当します。
- メディアエンジン (SlimCore): MicrosoftによってMSIXパッケージとして提供される、オペレーティングシステム固有のメディアエンジン。

展開

1. 前提条件に記載されているMicrosoft Teamsのバージョンがあることを確認してください。
2. Microsoft Teamsの仮想チャネルを許可するように、**仮想チャネル許可リスト**ポリシーを構成します。これらのチャネルにより、Teamsクライアントはクライアント側プラグインに接続できます。詳細については、仮想チャネルセキュリティを参照してください。

   このソリューションには、3つのカスタム仮想チャネルが必要です。ワイルドカードを使用して、`ms-teams.exe`実行可能ファイルとカスタム仮想チャネルを許可します。

```
MSTEAMS,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe

MSTEAM1,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe

MSTEAM2,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe
```

注:

- VDA 2603以降では、これら3つの仮想チャネルがデフォルトで許可されます。これらのバージョンでは、Studioポリシーの構成は不要です。
- 仮想チャネル許可リストポリシーのワイルドカードは、CVAD 2203 LTSR CU2以降、またはCitrix Virtual Apps and Desktops™ 2206 CR以降で利用できます。
- ポリシーを有効にするには、VDAマシンを再起動する必要があります。
- MSTeamsのインストールパスはMSIXアプリケーションであるため変更されるため、ワイルドカードが必要です。上記に示されている正確な行を許可します。

3. このソリューションは、Citrixポリシーではなく、Microsoft Teams側のポリシーによって制御されます。デフォルトで有効になっています。特定のユーザーグループに対して有効または無効にするには、Microsoftドキュメントを参照してください。
4. エンドポイントにTeamsプラグインを展開します。Teamsプラグインをインストールするオプションを参照してください。
5. メディアエンジンのステージングと登録、およびMSIXのインストールをブロックする可能性のあるグループポリシーについては、Microsoftのドキュメントを参照してください。

Teamsプラグインをインストールするオプション

インストール方法に関わらず、プラグインはエンドポイントのCitrix Workspaceアプリの場所に配置されます。

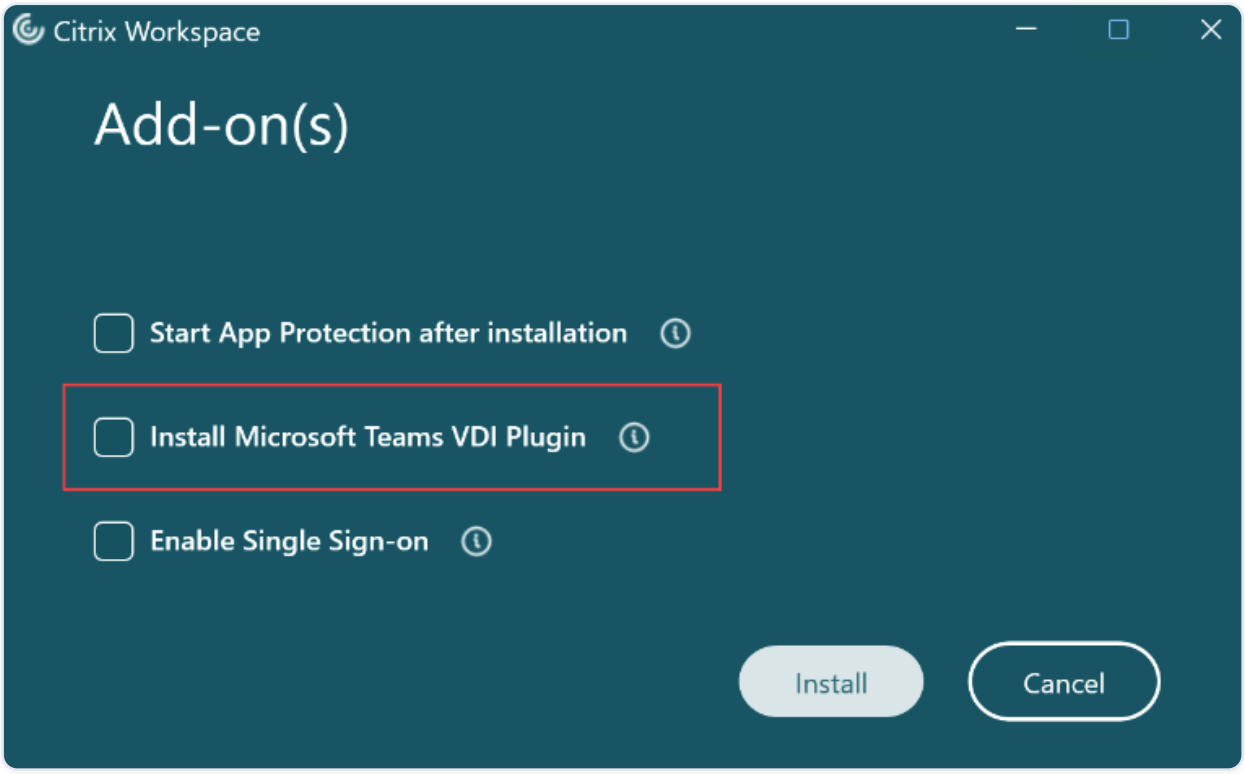
- Windows (`MsTeamsPluginCitrix.dll`): 64ビット `C:\Program Files (x86)\Citrix\ICA Client`; 32ビット `C:\Program Files\Citrix\ICA Client`
- Mac: `/Applications/Utilities/MsTeamsVdi.Plugin.app`

注:

- Windowsでは、仮想チャネルが正しく開くように、Citrix Workspaceアプリを管理者モードでインストールしてください。Citrix Workspaceアプリのユーザーごとのインストールはサポートされていません。
- Microsoft StoreからCitrix Workspaceアプリをインストールした場合、Microsoft Teams VDIプラグインはサポートされません。
- エンドポイントにCitrix Workspaceアプリが見つからない場合、プラグインのインストールは停止します。
- Windowsでは、プラグインとCitrix Workspaceアプリは同じアーキテクチャである必要があります。32ビットのCitrix Workspaceアプリは64ビットのプラグインをロードできません。
- プラグインはアップグレードまたは修復できますが、ダウングレードはできません。また、アクティブなセッションがない場合にのみ可能です。

オプション1: Citrix Workspaceアプリのインストールによる方法

- **Windows:** 新規インストールまたは手動アップグレード中に、**アドオン**ページで**Microsoft Teams VDIプラグインのインストール**を選択します。Citrix Workspaceアプリ for Windows 2508以降では、このオプションはデフォルトで選択されています。インストールをスキップするには、このチェックを外してください。アップグレード時には、以前の選択が記憶されます。



コマンドラインから `/InstallMSTeamsPlugin` スイッチを使用してインストールすることもできます。例えば、`CitrixWorkspaceApp.exe /InstallMSTeamsPlugin=Y` はプラグインをインストールし、`/InstallMSTeamsPlugin=N` はそれを阻止します。

新規インストールの場合、最小要件はCitrix Workspaceアプリ for Windows 2402 LTSRです。インプレースアップグレードの場合、最小要件はCitrix Workspaceアプリ for Windows 2405 CRです。最新の詳細については、サードパーティ製プラグインのインストールを参照してください。

- **Mac:** Citrix Workspaceアプリのインストール中にプラグインをインストールするオプションは、Citrix Workspaceアプリ for Mac 2603以降で利用可能であり、ユーザーによる操作が必要です。Citrix Workspaceアプリ for Mac 2607では、プラグインがデフォルトで自動的にインストールされます。Citrix Workspaceアプリ for Mac 2508.10では、プラグインを手動でインストールしてください。オプション2: プラグインを直接ダウンロードするを参照してください。

オプション2: プラグインを直接ダウンロードする

- **Windows:** MSIをダウンロードし、サポートされている任意のCitrix Workspaceアプリのバージョンに、SCCMやIntuneなどのツールを使用して展開します。
  - 32ビット版Citrix Workspaceアプリ: aka.ms/plugin
  - 64ビット版Citrix Workspaceアプリ: aka.ms/plugin_x64
  - ArmベースのCitrix Workspaceアプリ: aka.ms/plugin_arm64
- **Mac:** aka.ms/macpluginからプラグインをダウンロードし、JAMFなどのツールを使用して展開します。

オプション3: クライアントアプリ管理 (旧Global App Configurationサービス)

クライアントアプリ管理 (旧Global App Configurationサービス、またはGACS) は、管理対象および非管理対象のエンドポイントのアプリ設定を管理し、Teamsプラグインをエンドポイント全体に展開できます。Macでは、Citrix Workspaceアプリ for Mac 2603以降が必要です。Microsoft Teams VDIプラグイン管理を参照してください。

オプション4: 仮想チャネルプラグインマネージャー

仮想チャネルプラグインマネージャーは、Teams向けの新VDIソリューションを含む、エンドポイントコンポーネントを必要とするアプリケーションのために、クライアントエンドポイント全体にプラグインを展開します。VDAで実行されているアプリケーションを検出し、ユーザーにエンドポイントへのプラグインのインストールを促します。管理者はBYODシナリオでこれを使用できます。Macでは、Citrix Workspaceアプリ for Mac 2603以降が必要です。仮想チャネルプラグインマネージャーを参照してください。

プラグインの更新シナリオ

プラグインがオプション1、3、または4を通じてインストールされている場合、CitrixはTeamsプラグインの更新をシームレスに処理します。プラグインが手動でインストールされている場合 (オプション2)、Citrixは更新を処理しません。

- プラグインの自動更新のために、Citrix Workspaceアプリの自動更新がオンになっていることを確認してください。
- Citrix Workspaceアプリ for Windows 2405以降であることを確認してください。Citrix Workspaceアプリ for Windows 2508以降では、Citrix Workspaceアプリが自動更新される際にプラグインが自動的にインストールされます。
- Citrixはプラグインのアンインストールを処理しません。必要に応じて、プラグインを個別にアンインストールしてください。

> **注:**
>
> CitrixはTeamsプラグインの更新を処理しますが、メディアエンジンは処理しません。Microsoftがメディアエンジンを提供し、更新します。

Citrix公開アプリとしてのTeams

Citrix Virtual Appsアプリケーションとして公開されたTeamsは、必要なすべてのコンポーネントが最小バージョンを満たしている場合、このソリューションで最適化できます。必要なバージョンと既知の制限については、Microsoftドキュメントを参照してください。

相互運用性とローミング

Teams向けNew VDIソリューションとCitrix HDX最適化がどのように相互運用され、ローミングがどのように動作するかについては、Microsoft Teamsの最適化を参照してください。

ネットワークに関する考慮事項

Microsoftドキュメントのネットワークに関する考慮事項を参照してください。

機能サポート

機能セットと実装はMicrosoftが所有しています。Microsoftドキュメントの機能リストを参照してください。

トラブルシューティング

Microsoft Teamsクライアントは最適化ステータスを報告し、最適化が失敗した場合はエラーコードを報告します。これらのステータスインジケーターとエラーコードはMicrosoftによって定義されています。完全なリストとエンドツーエンドのトラブルシューティングについては、Microsoftドキュメントの Teams向けNew VDIソリューションのトラブルシューティング を参照してください。

Citrix Monitorは、このソリューションの最適化状態を可視化します。セッションの詳細では、セッショントポロジビューに、アプリケーションが最適化されているかどうか、およびプラグインマネージャー、プラグインとそのバージョン、仮想チャネルの状態、仮想チャネル許可リストのステータスなど、不足しているコンポーネントが示されます。詳細については、リアルタイム通信最適化の可視性を参照してください。

一部のMicrosoftエラーコードは、Citrix側の構成を示しています。一般的なCitrixの確認事項：

- Teamsクライアントがカスタム仮想チャネルがブロックされていると報告した場合（Microsoftエラー2003）、仮想チャネル許可リストにMSTEAMS、MSTEAM1、およびMSTEAM2が含まれていることを確認してください。
- Teamsクライアントがプラグインが検出されないと報告した場合（Microsoftエラー2000）、プラグインがインストールされ、ロードされていることを確認してください。Process Explorerで `wfica32.exe` を選択し、下部ペインを表示して、DLLタブで `MsTeamsPluginCitrix.dll` を確認してください。
- TeamsクライアントがサポートされていないCitrix Workspaceアプリのバージョンを報告した場合（Microsoftエラー2004）、サポートされているバージョンにアップグレードしてください。システム要件を参照してください。

既知の制限事項

機能と実装はMicrosoftが所有しています。Microsoftのドキュメントで既知の問題を参照してください。

Microsoft Teams (Classic) の最適化

> **注:**
>
> 新しいMicrosoft Teams 2.1は、VDAで一般提供されるようになりました。このMicrosoft Teamsのバージョンは、WebRTC (VDI 1.0) を使用したCitrix Microsoft Teams最適化と互換性があります。

> Citrix Virtual Apps and Desktops 2402以降では、`msedgewebview2.exe`レジストリエントリはデフォルトで許可リストに含まれているため、手動で構成する必要はありません。

> 公開アプリケーションは、新しいMicrosoft Teamsでサポートされるようになりました。

> Citrixは、Citrix Virtual Apps and Desktops™およびCitrix Workspace™アプリを使用して、デスクトップベースのMicrosoft Teams向けに最適化を提供します。デフォルトでは、必要なすべてのコンポーネントをCitrix WorkspaceアプリとVirtual Delivery Agent (VDA) にバンドルしています。

Microsoft Teams向けのCitrixの最適化には、VDA側のHDX™サービスと、Microsoft Teamsホスト型アプリと連携してコマンドを受信するAPIが含まれています。これらのコンポーネントは、Citrix Workspaceアプリ側のメディアエンジンへの制御仮想チャネル (CTXMTOP) を開きます。エンドポイントはマルチメディアをローカルでデコードして提供し、Citrix Workspaceアプリのウィンドウをホスト型Microsoft Teamsアプリに戻します。

認証とシグナリングは、他のMicrosoft Teamsサービス (チャットやコラボレーションなど) と同様に、Microsoft Teamsホスト型アプリでネイティブに発生します。オーディオ/ビデオのリダイレクトはこれらに影響しません。

`CTXMTOP`はコマンドおよび制御仮想チャネルです。これは、Citrix WorkspaceアプリとVDAの間でメディアが交換されないことを意味します。

クライアントフェッチ/クライアントレンダリングのみが利用可能です。

このビデオデモンストレーションでは、Citrix仮想環境でMicrosoft Teamsがどのように機能するかを理解できます。



Microsoft Teamsのインストール

CitrixとMicrosoftは、Microsoft Teamsの最新バージョンを使用し、常に最新の状態に保つことを推奨しています。 現在のバージョンのリリース日から90日以上古いリリース日のMicrosoft Teamsデスクトップアプリのバージョンはサポートされていません。 サポートされていないMicrosoft Teamsデスクトップアプリのバージョンでは、ユーザーにブロックページが表示され、アプリの更新が要求されます。

最新の利用可能なバージョンについては、Microsoft Teamsアプリ（デスクトップおよびMac）の更新履歴を参照してください。

Microsoft Teamsの全ユーザー向けインストールガイドラインに従うことをお勧めします。Microsoft Teamsを`AppData`にインストールする.exeインストーラーの使用は避けてください。代わりに、コマンドラインから`ALLUSER=1`フラグを使用して`C:\Program Files (x86)\Microsoft\Teams`にインストールしてください。

```
msiexec /i <path_to_msi> /l*v <install_logfile_name> ALLUSER=1 ALLUSERS=1
```

この例では、`ALLUSERS=1`パラメーターも使用しています。このパラメーターを設定すると、Microsoft Teams Machine-Wide Installerが**コントロールパネル**の**プログラムと機能**に表示されます。また、コンピューターのすべてのユーザーのWindows設定の**アプリと機能**にも表示されます。これにより、管理者資格情報を持つすべてのユーザーがMicrosoft Teamsをアンインストールできます。

`ALLUSERS=1`と`ALLUSER=1`の違いを理解することが重要です。`ALLUSERS=1`パラメーターは、非VDI環境とVDI環境の両方で使用できます。`ALLUSER=1`パラメーターは、マシンごとのインストールを指定するためにVDI環境でのみ使用してください。

`ALLUSER=1`モードでは、新しいバージョンがリリースされてもMicrosoft Teamsアプリケーションは自動更新されません。このモードは、Windows ServerまたはWindows 10のランダム/プールされたカタログからのホスト型共有アプリやデスクトップなど、非永続的な環境に推奨されます。詳細については、「MSIを使用してMicrosoft Teamsをインストールする」（VDIインストールセクション）を参照してください。

Windows 10専用の永続VDI環境があるとします。Microsoft Teamsアプリケーションを自動更新し、Microsoft Teamsを`Appdata/Local`の下にユーザーごとにインストールすることを希望する場合、`.exe`インストーラーまたは`ALLUSER=1`なしのMSIを使用してください。

> **注:**
>
> Citrixでは、ゴールデンイメージにMicrosoft Teamsをインストールする前にVDAをインストールすることを推奨しています。このインストール順序は、`ALLUSER=1`フラグを有効にするために必要です。VDAをインストールする前に仮想マシンにMicrosoft Teamsをインストールした場合は、Microsoft Teamsをアンインストールして再インストールしてください。

Remote PC Accessの場合

Citrixでは、VDAのインストール後にMicrosoft Teamsバージョン1.4.00.22472以降をインストールすることを推奨しています。そうしないと、Microsoft TeamsがVDAを正しく検出するために、一度サインアウトして再度サインインする必要があります。バージョン1.4.00.22472以降には、VDA

検出のためにMicrosoft Teamsの起動時およびサインイン時に実行される拡張ロジックが含まれています。これらのバージョンには、アクティブなセッションタイプ識別（HDX、RDP、またはクライアントマシンにローカル接続）も含まれています。ローカル接続の場合、以前のバージョンのMicrosoft Teamsでは、特定の機能やUI要素（ブレイクアウトルーム、会議やチャットのポップアウトウィンドウ、会議のリアクションなど）の検出と無効化に失敗する可能性があります。

> **重要:**
>
> ローカルセッションからHDXセッションにローミングし、Microsoft Teamsがバックグラウンドで開いたまま実行されている場合、HDXで正しく最適化するには、Microsoft Teamsを終了して再起動する必要があります。 逆に、最適化されたHDXセッションを介してMicrosoft Teamsをリモートで使用している場合は、HDXセッションを切断し、デバイスで同じWindowsセッションにローカルで再接続します。オフィスで作業している場合は、Microsoft TeamsがリモートPCアクセス状態（HDXまたはローカル）を正しく検出できるように、Microsoft Teamsを再起動する必要があります。これは、Microsoft TeamsがVDIモードを評価できるのはアプリ起動時のみであり、バックグラウンドで既に実行されている間は評価できないためです。再起動しないと、Microsoft Teamsはポップアウトウィンドウ、ブレイクアウトルーム、会議のリアクションなどの機能を読み込めない可能性があります。

App Layeringの場合

Citrix App Layeringを使用してVDAとMicrosoft Teamsのインストールを異なるレイヤーで管理する場合、コマンドラインから`ALLUSER=1`フラグを使用してMicrosoft Teamsをインストールする前に、Windows VDA上にレジストリキーを作成する必要があります。詳細については、「」(/ja-jp/citrix-virtual-apps-desktops/current-release/policies/reference/hdx-registry-settings.html#multimedia)の「*Citrix App Layeringを使用したMicrosoft Teamsの最適化*」セクションを参照してください。

プロファイル管理の推奨事項

Windows ServerおよびプールされたVDI Windows 10環境には、マシン全体のインストーラーを使用することをお勧めします。

コマンドラインからMSIに**ALLUSER=1**フラグ（全ユーザー向けインストーラー）が渡されると、Microsoft Teamsアプリは`C:\Program Files (x86)`（約300 MB）にインストールされます。このアプリは、ログに`AppData\Local\Microsoft\TeamsMeetingAddin`を、ユーザー固有の構

成、ユーザーインターフェイス要素のキャッシュなどに`AppData\Roaming\Microsoft\Teams`（約600〜700 MB）を使用します。

> **重要:**

> **ALLUSER=1**フラグを渡さない場合、MSIはTeams.exeインストーラーと`setup.json`を`C:\Program Files (x86)\Teams Installer`に配置します。レジストリキー（TeamsMachineInstaller）は`HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`の下に追加されます。

> その後のユーザーログオンにより、代わりに**AppData**に最終インストールがトリガーされます。

マシン全体のインストーラー

以下は、Windows Server 64ビットVMにMicrosoft Teamsの全ユーザー向けインストーラーをインストールすることによって作成されるフォルダー、デスクトップショートカット、およびレジストリの例です。

フォルダー:

- `C:\Program Files (x86)\Microsoft\Teams`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

デスクトップショートカット:

`C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

レジストリ:

- `HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- 名前: `Teams`
- 種類: `REG_SZ`

- 値: `C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

> **注:**
>
> レジストリの場所は、基盤となるオペレーティングシステムとビット数によって異なります。

推奨事項

- Microsoft Teams のレジストリキーを削除して自動起動を無効にすることをお勧めします。これにより、同時に発生する多数のログオン（たとえば、勤務開始時など）によって VM の CPU 使用率が急上昇するのを防ぎます。
- 仮想デスクトップにGPU/vGPUがない場合、パフォーマンスを向上させるために、Microsoft Teamsの**設定**で**GPUハードウェアアクセラレーションを無効にする**ことをお勧めします。この設定（`"disableGpu":true`）は、`desktop-config.json`の`%Appdata%\Microsoft\Teams`に保存されます。ログオンスクリプトを使用してそのファイルを編集し、値を`true`に設定できます。
- Citrix Workspace Environment Management™ (WEM) を使用している場合は、Microsoft Teams のプロセッサ消費を管理するために **CPU スパイク保護**を有効にしてください。

ユーザーごとのインストーラー

`.exe`インストーラーを使用する場合、インストールプロセスは異なります。すべてのファイルはAppDataに配置されます。

フォルダー:

- `C:\Users\<username>\AppData\Local\Microsoft\Teams`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsPresenceAddin`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsMeetingAddin`
- `C:\Users\<username>\AppData\Local\SquirrelTemp`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

デスクトップショートカット:

`C:\Users\<username>\AppData\Local\Microsoft\Teams\Update.exe --processStart "Teams.exe"`

レジストリ:

`HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

ベストプラクティス

ベストプラクティスの推奨事項は、ユースケースシナリオに基づいています。 非永続的な設定でMicrosoft Teamsを使用する場合、効率的なMicrosoft Teamsランタイムデータ同期のためにプロファイルキャッシュマネージャーが必要です。プロファイルキャッシュマネージャーを使用すると、ユーザーセッション中に適切なユーザー固有の情報がキャッシュされます。たとえば、ユーザー固有の情報には、ユーザーデータ、プロファイル、設定が含まれます。これら2つのフォルダーのデータを同期します。

- `C:\Users\<username>\AppData\Local\Microsoft\IdentityCache`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

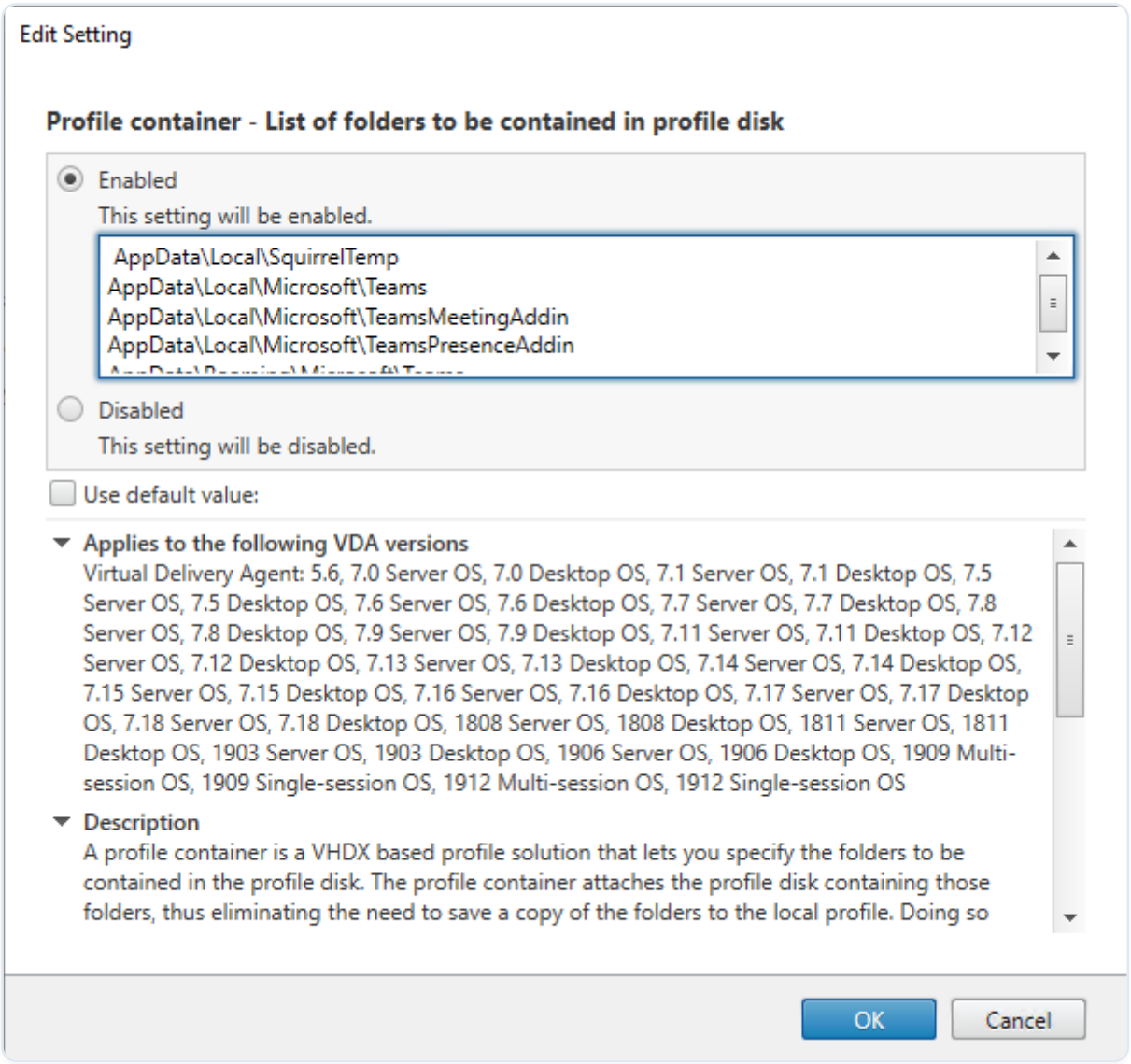
非永続的セットアップ向けの Microsoft Teams キャッシュコンテンツ除外リスト

Microsoft ドキュメントに記載されているように、Microsoft Teams のキャッシュフォルダーからファイルとディレクトリを除外します。この操作により、ユーザーのキャッシュサイズを削減し、非永続的セットアップをさらに最適化できます。

ユースケース: シングルセッションシナリオ

このシナリオでは、エンドユーザーは一度に1つの場所でMicrosoft Teamsを使用します。同時に2つのWindowsセッションでMicrosoft Teamsを実行する必要はありません。一般的な仮想デスクトップ展開では、各ユーザーに1つのデスクトップが割り当てられ、Microsoft Teamsは仮想デスクトップに1つのアプリケーションとして展開されます。 Citrix Profileコンテナを有効にし、ユーザーごとのインストーラーにリストされているユーザーごとのディレクトリをコンテナにリダイレクトすることをお勧めします。

1. ゴールデンイメージにMicrosoft Teamsのコンピューター全体インストーラー (**ALLUSER=1**) を展開します。
2. Citrix Profile Managementを有効にし、適切な権限でユーザープロファイルストアを設定します。
3. 次のProfile Managementポリシー設定を有効にします: **ファイルシステム > 同期 > プロファイルコンテナ – プロファイルディスクに含めるフォルダーのリスト。**



この構成内のすべてのユーザーごとのディレクトリをリストします。これらの設定は、Citrix Workspace Environment Management（WEM）サービスを使用して構成することもできます。

4. 設定を適切なデリバリーグループに適用します。
5. ログインして展開を検証します。

システム要件

推奨される最小バージョン - Delivery Controller (DDCs) 1906.2

以前のバージョンを使用している場合は、Microsoft Teamsの最適化を有効にするを参照してください:

サポートされているオペレーティングシステム:

- Windows Server 2022、2019、2016、2012R2 StandardおよびDatacenterエディション、ならびにServer Coreオプション

最小バージョン - Virtual Delivery Agents (VDA) 1906.2

サポートされているオペレーティングシステム:

- ウィンドウズ 11
- Windows 10 64ビット、バージョン1607以降。VMホスト型アプリは、Citrix Workspaceアプリ for Windows 2109.1以降でサポートされています。
- Windows Server 2022, 2019, 2016, および 2012 R2 (Standard および Datacenter エディション)

要件:

- BCR_x64.msi - Microsoft Teamsの最適化コードを含み、GUIから自動的に起動するMSI。VDAインストールのコマンドラインインターフェイスを使用している場合は、除外しないでください。

推奨バージョン – Citrix Workspaceアプリ for Windows最新CRおよび最小バージョン - Citrix Workspaceアプリ 1907 for Windows

- ウィンドウズ 11。
- Windows 10 (32ビットおよび64ビットエディション、Embeddedエディションを含む) (Windows 7のサポートはバージョン2006で終了しました) (Windows 8.1のサポートはバージョン2204.1で終了しました)。
- Windows 10 IoT Enterprise 2016 LTSB (v1607) および 2019 LTSC (v1809) に対応しています。
- サポートされているプロセッサ（CPU）アーキテクチャ: x86およびx64（ARMはサポートされていません）。
- エンドポイント要件: ピアツーピアのビデオ会議中に720p HD解像度をサポートできる、約2.2～2.4 GHzのデュアルコアCPU。
- デュアルコアまたはクアッドコアCPUで、ベース速度が低く（約1.5 GHz）、Intel Turbo BoostまたはAMD Turbo Coreを搭載し、少なくとも2.4 GHzまでブーストできるもの。
- 動作確認済みHPシンクライアント: t630/t640、t730/t740、mt44/mt45。
- 動作確認済みDellシンクライアント: 5070、5470 Mobile TCおよびAIO。
- 動作確認済み10ZiGシンクライアント: 4510および5810q。
- 動作確認済みエンドポイントの完全なリストについては、「シンクライアント」を参照してください。
- Citrix Workspaceアプリには、最低600 MBの空きディスク容量と1 GBのRAMが必要です。

- Microsoft .NET Frameworkの最小要件はバージョン4.8です。Citrix Workspaceアプリは、システムに.NET Frameworkが存在しない場合、自動的にダウンロードしてインストールします。

管理者は、Microsoft Teams最適化ポリシーを変更することで、最適化モードでMicrosoft Teamsを有効/無効にできます。Citrix Workspaceアプリで最適化モードで起動するユーザーは、Microsoft Teamsを無効にできません。

最小バージョン - Linux用Citrix Workspaceアプリ2006

詳しくは、Citrix WorkspaceアプリfoLinuxのドキュメントにあるMicrosoft Teamsの最適化を参照してください。

ソフトウェア:

- `GStreamer` 1.0以降またはCairo 2
- `libc++-9.0` 以降
- `libgdk` 3.22 以降
- OpenSSL 1.1.1d
- `libnsl`
- Ubuntu 20.04 以降

認証の強化:

- Libsecretライブラリ
- libunwind-12ライブラリ。詳しくは、llvm-12のlibunwind-12ライブラリ依存関係の追加を参照してください。

ハードウェア:

- ピアツーピアのビデオ会議通話中に720p HD解像度をサポートできる最小1.8 GHzデュアルコアCPU
- ベース速度1.8 GHz、Intel Turbo Boostの高速化が少なくとも2.9 GHzのデュアルコアまたはクアッドコアCPU

検証済みエンドポイントの完全なリストについては、Thin Clientsを参照してください。

詳細については、Citrix Workspaceアプリをインストールするための前提条件を参照してください。

`/opt/Citrix/ICAClient/config/module.ini`ファイルで**VDWEBRTC**フィールドの値をOffに更新することで、Microsoft Teamsの最適化を無効にできます。デフォルトはVDWEBRTC=Onです。更新が完了したら、セッションを再起動してください。(ルート権限が必要です)。

最小バージョン - Mac用Citrix Workspaceアプリ2012

サポートされているオペレーティングシステム:

- macOS カタリナ (10.15)。
- macOS Big Sur 11.0.1以降。
- macOS モントレー。

サポートされている機能:

- オーディオ
- ビデオ
- 画面共有の最適化 (送受信)

> **注:**

> Citrix Viewerアプリが画面共有を機能させるには、macOSの「セキュリティとプライバシー」設定へのアクセスが必要です。ユーザーは、**Appleメニュー > システム環境設定 > セキュリティとプライバシー > プライバシータブ > 画面収録**でこの設定を構成し、**Citrix Viewer**を選択します。

> Microsoft Teamsの最適化は、Citrix Workspaceアプリ2012以降およびmacOS 10.15でデフォルトで機能します。

Microsoft Teamsの最適化を無効にするには、ターミナルでこのコマンドを実行し、Citrix Workspaceアプリを再起動します。

```
defaults write com.citrix.receiver.nomas mtopEnabled -bool NO
```

最小バージョン - 最新バージョンのChromeOSで実行されているCitrix Workspaceアプリfor ChromeOSの最新バージョン

ハードウェア:

- Intel i3、クアッドコア2.4 GHzと同等以上の性能を持つプロセッサ。

サポートされている機能:

- オーディオ
- ビデオ
- 画面共有の最適化（送受信） - デフォルトでは無効になっています。有効にする方法については、これらの設定を参照してください。

シングルサーバーのスケーラビリティ

このセクションでは、単一の物理ホストでサポートできるユーザー数または仮想マシン (VM) 数を推定するための推奨事項とガイダンスを提供します。これは一般的にCitrix Virtual Apps and Desktops™ Single Server Scalability (SSS) と呼ばれます。Citrix Virtual Apps (CVA) またはセッション仮想化のコンテキストでは、ユーザー密度としても知られています。その目的は、主要なハイパーバイザーを実行している単一のハードウェアで、どれだけのユーザーまたはVMを実行できるかを明らかにすることです。

> **注:**
>
> このセクションには、SSSを推定するためのガイダンスが含まれています。このガイダンスは大まかなものであり、お客様固有の状況や環境に必ずしも当てはまらない場合があります。Citrix Virtual Apps and DesktopsのSSSを真に理解する唯一の方法は、Login VSIなどのスケーラビリティまたは負荷テストツールを使用することです。Citrixは、SSSを迅速に推定するためだけに、このガイダンスとこれらの簡単なルールを使用することを推奨します。ただし、特にハードウェアを購入したり、財務上の決定を下したりする前に、結果を検証するためにLogin VSIまたは選択した負荷テストツールを使用することをCitrixは推奨します。

ハードウェア (テスト対象システム)

- デル パワーエッジ R740
- Intel Xeon (Gold) 6126 @ 2.60 GHz (最大ターボ 3.70 GHz)、ソケットあたり 12 コア、ハイパースレッディング有効のデュアルソケット
- 382 GB の RAM
- ローカル SSD RAID 0 ストレージ (11 ディスク) 6 TB

ソフトウェア

Citrix Virtual Apps and Desktops 2106 を実行する Windows 2019 (TSVDA) を搭載した単一の仮想マシン (40 論理プロセッサ) VMware ESXi 6.7

用語

- ナレッジワーカーのワークロード: Acrobat Reader、Freemind/Java、フォトビューアー、Edge、および Excel、Outlook、PowerPoint、Word などの MS Office アプリが含まれます。
- ベースライン: ナレッジワーカーのワークロード (Microsoft Teams なし) で実行されるサーバーのスケーラビリティテスト。
- Microsoft Teams ワークロード: ナレッジワーカーの一般的なワークロード + Microsoft Teams。

Microsoft Teams のストレステスト方法

- Microsoft Teams は HDX で最適化されています。そのため、すべてのマルチメディア処理はエンドポイントまたはクライアントにオフロードされ、測定には含まれません。
- ワークロードが開始される前に、すべてのMicrosoft Teamsプロセスが停止または終了されます。
- Microsoft Teams を開く（コールドスタート）。
- Microsoft Teams がロードされ、Microsoft Teams のプライマリウィンドウがフォーカスを取得するまでにかかる時間を測定します。
- キーボードショートカットを使用してチャットウィンドウに切り替える。
- キーボードショートカットを使用してカレンダーウィンドウに切り替える。
- キーボードショートカットを使用して、特定のユーザーにチャットメッセージを送信します。
- キーボードショートカットを使用してMicrosoft Teamsウィンドウに切り替える。

結果

- ベースライン（137ユーザー）と比較して、Microsoft Teams ワークロード（81ユーザー）ではスケーラビリティに40%の影響があります。
- サーバー容量を約40%（CPUで）増やすと、ベースラインワークロードの場合と同じユーザー数に戻ります。
- ベースラインと比較して、Microsoft Teams ワークロードでは20%の追加メモリが必要です。
- ユーザーあたりのストレージサイズを512〜1024 MB増やします。
- IOPS書き込みが約50%増加、IOPS読み取りが約100%増加。Microsoft Teamsは、ストレージが遅い環境では大きな影響を与える可能性があります。

機能マトリックスとバージョンサポート

機能	MICROSOFT TEAMS (最小バージョン)	VDA (最小バージョン)	WINDOWS CR 向け CITRIX WORKSPACE アプリ (最小バージョン)	CITRIX WORKSPACEアプリ FOR MAC（最小バージョン）	CITRIX WORKSPACEアプリ FOR LINUX（最小バージョン）	CITRIX WORKSPACEアプリ FOR CHROME OS（最小バージョン）
オーディオ/ビデオ (P2P および会議)	現在のバージョンから90日前	1906	1907	2009	2004	2105.5
画面共有	現在のバージョンから90日遡ったもの	1906	1907	2012	2006	2105.5
i. 画面インジケーターの赤い枠線	現在のバージョンから90日遡ったもの	1906	2002	2012	2006	いいえ
ii. キャプチャを Desktop Viewerに制限	現在のバージョンから90日遡ったもの	1906	2009.5	2012	2006	いいえ
iii. マルチモニター	現在のバージョンから90日遡ったもの	1912 CU6+	2106 (1)	2106	2106	いいえ
DTMF	現在のバージョンから90	該当なし	2102	2101	2101	2111.1

機能	MICROSOFT TEAMS (最小バージョン)	VDA (最小バージョン)	WINDOWS CR 向け CITRIX WORKSPACE アプリ (最小バージョン)	CITRIX WORKSPACEアプリ FOR MAC（最小バージョン）	CITRIX WORKSPACEアプリ FOR LINUX（最小バージョン）	CITRIX WORKSPACEアプリ FOR CHROME OS（最小バージョン）
	日遡ったもの					
プロキシサーバーのサポート	現在のバージョンから90日遡ったもの	該当なし	2012 (2)	2104 (3)	2101 (3)	2305
アプリ共有	現在のバージョンから90日遡ったもの	2109	2109.1	2203.1	2209	いいえ
ライブキャプション	現在のバージョンから90日遡ったもの	N/A (4)	2109.1	2109	2109	2303
動的e911	現在のバージョンから90日遡ったもの	該当なし	2112.1	2112	2112	2112
制御を付与	現在のバージョンから90日遡ったもの	該当なし	2112.1	2203.1	いいえ	いいえ
制御を要求	現在のバージョ	該当なし	2112.1	2203.1	2203	2303

機能	MICROSOFT TEAMS (最小バージョン)	VDA (最小バージョン)	WINDOWS CR 向け CITRIX WORKSPACE アプリ (最小バージョン)	CITRIX WORKSPACEアプリ FOR MAC（最小バージョン）	CITRIX WORKSPACEアプリ FOR LINUX（最小バージョン）	CITRIX WORKSPACEアプリ FOR CHROME OS（最小バージョン）
	ンから90日遡ったもの					
マルチウィンドウ	1.5.00.11865	2112, 1912 CU6 (5)	2112.1	2203.1	2203	2303
会議の文字起こし	現在のバージョンから90日遡ったもの	2112.1, 1912 CU6+	2112	2203.1	2203	2303
背景ぼかし	現在のバージョンから90日遡ったもの	2112, 1912 CU6+	2207	2301	2212	2303

1. CD Viewerは全画面モードのみ。SHIFT+F2はサポートされていません。
2. Negotiate/Kerberos、NTLM、Basic、およびDigest。`Pac`ファイルもサポートされています。
3. 匿名のみ。
4. VDAが2112以降の場合、ライブキャプションは、Citrix Workspaceアプリのバージョンが Mac用2203.1、Linux用2203、またはWindows用2112の場合にのみ機能します。これは、Microsoft Teamsがシングルウィンドウ UIモードまたはマルチウィンドウモードの場合、ライブキャプションの動作が異なるためです。
5. マルチウィンドウは2112 VDAで導入されましたが、VDA 1912 LTSR CU6リリースにバックポートされました。

> **注:**

- **Citrix Workspace app for Windows 1912 CU6 (またはそれ以降)**に記載されているすべての機能は、Citrix Workspace app for Windows 2203.1 LTSR CU1に適用されます。
- Microsoftは、Microsoft Teamsにおけるシングルウィンドウモードのサポートを非推奨としました。これに対応するため、VDAを1912 CU6+ LTSRに、Citrix Workspaceアプリを2203 CU2+以降にアップグレードする必要があります。これらはマルチウィンドウモードをサポートしています。

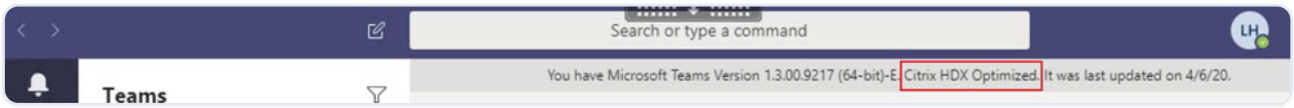
Microsoft Teamsの最適化を有効にする

Microsoft Teamsの最適化を有効にするには、Microsoft Teams redirectionポリシーで説明されている管理ポリシーを使用します。このポリシーはデフォルトで**ON**です。このポリシーが有効になっていることに加えて、HDXはCitrix Workspaceアプリのバージョンが少なくとも必要な最小バージョンであることを確認します。ポリシーを有効にし、Citrix Workspaceアプリのバージョンがサポートされている場合、VDA上で**HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream\MSTeamsRedirSupport**が自動的に**1**に設定されます。Microsoft Teamsは、VDIモードでロードするためにこのキーを読み取ります。

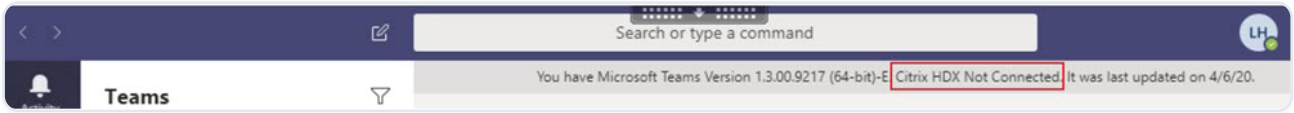
注:

バージョン1906.2以降のVDA、またはManageコンソール（Studio）でポリシーが利用できない古いコントローラーバージョン（バージョン7.15など）を使用している場合でも、VDAを最適化できます。Microsoft TeamsのHDX最適化は、VDAでデフォルトで有効になっています。

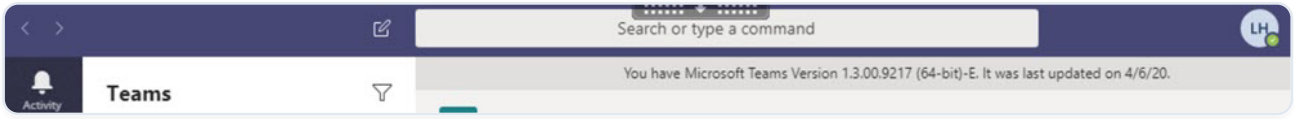
About > Versionをクリックすると、**Citrix HDX Optimized**の凡例が表示されます。



Citrix HDX Not Connectedと表示される場合、Citrix APIはMicrosoft Teamsにロードされています。APIのロードはリダイレクトへの最初のステップです。しかし、スタックの後続の部分でエラーが発生しています。このエラーは、VDAサービスまたはCitrix Workspaceアプリにある可能性が最も高いです。



凡例が表示されない場合、Microsoft TeamsはCitrix APIの読み込みに失敗しています。通知領域のアイコンを右クリックしてMicrosoft Teamsを終了し、再起動してください。Manageポリシーが**Prohibited**に設定されておらず、Citrix Workspaceアプリのバージョンがサポートされていることを確認してください。



重要: セッションの再接続

- 接続性が変更された場合、HDX最適化セッションを取得するためにMicrosoft Teamsを再起動する必要がある場合があります。たとえば、サポートされていないエンドポイント（iOS、Android、またはWindows/Linux/Macの古いバージョンのWorkspaceアプリ）からサポートされているエンドポイント（Windows/Linux/Mac/ChromeOS/HTML5のWorkspaceアプリ）にローミングする場合、またはその逆の場合です。
- VDAにMicrosoft Teamsの.exeインストーラーを使用してアプリをインストールした場合も、Microsoft Teamsの再起動が必要です。.exeインストーラーは、永続的なVDI展開に推奨されます。このような場合、HDXセッションが切断状態にある間にMicrosoft Teamsが自動更新されることがあります。そのため、HDXセッションに再接続するユーザーは、Microsoft Teamsが最適化されて実行されていないことに気づくでしょう。
- ローカルセッションからHDXセッションにローミングする場合、HDXで最適化するためにMicrosoft Teamsを再起動する必要があります。この操作は、Remote PC Accessシナリオで必要です。

ネットワーク要件

Microsoft Teamsは、会議や多人数通話のためにMicrosoft 365のメディアプロセッササーバーに依存しています。また、Microsoft Teamsは、以下のシナリオでMicrosoft 365トランスポートリレーに依存しています。

- ポイントツーポイント通話の2つのピアが直接接続されていない
- 参加者がメディアプロセッサに直接接続されていない。

したがって、ピアとMicrosoft 365クラウド間のネットワークの状態が通話のパフォーマンスを決定します。ネットワーク計画に関する詳細なガイドラインについては、Microsoft 365 network connectivity principlesを参照してください。

クラウド音声およびビデオの全体的な展開に影響を与える可能性のあるリスクと要件を特定するために、環境を評価することをお勧めします。 ネットワークがMicrosoft Teamsに対応しているかテストするには、Skype for Business Network Assessment Toolを使用してください。サポート情報については、Supportを参照してください。

Real Time Protocol (RTP) トラフィックに関する主要なネットワーク推奨事項の概要

- 支社からMicrosoft 365ネットワークにできるだけ直接接続します。
- 支社で十分な帯域幅を計画し、提供します。
- 各支社のネットワーク接続と品質を確認します。
- 支店で以下のいずれかを使用する必要がある場合は、RTP/UDPトラフィック（Citrix WorkspaceアプリのHdxRtcEngine.exeによって処理される）が妨げられないことを確認してください。
    - プロキシサーバーをバイパスする
    - ネットワークSSLインターセプト
    - ディープパケットインスペクションデバイス
    - VPNヘアピン（可能であればスプリットトンネリングを使用）

> **重要: VPNスプリットトンネル構成**

> HdxRtcEngine.exeのトラフィックはVPNトンネルから迂回させ、ユーザーのローカルインターネット接続を使用してサービスに直接接続できるようにする必要があります。これを実現する方法は、使用するVPN製品とマシンプラットフォームによって異なりますが、ほとんどのVPNソリューションでは、このロジックを適用するための簡単なポリシー設定が可能です。VPNプラットフォーム固有の分割トンネルガイダンスの詳細については、このMicrosoftの記事を参照してください。

> WorkspaceアプリのWebRTCメディアエンジン（HdxRtcEngine.exe）は、クライアントにオフロードされるマルチメディアストリームにSecure Real-time Transport Protocol (SRTP) を使用します。SRTPはRTPに機密性と認証を提供します。この機能では、AES暗号化方式を使用してメディアおよび制御メッセージを暗号化するために、対称鍵（DTLSとネゴシエートされる）が使用されます。

良好なユーザーエクスペリエンスのために、以下のメトリックが推奨されます。

メトリック	エンドポイントからMICROSOFT 365まで
遅延 (片道)	< 50 ミリ秒
遅延 (RTT)	< 100 ミリ秒
パケット損失	15秒間隔で1%未満
パケット到着間隔ジッター	15秒間隔で30ミリ秒未満

詳細については、Microsoft Teams 用に組織のネットワークを準備するを参照してください。

帯域幅要件については、Microsoft Teams の最適化では、オーディオ (OPUS/G.722/PCM G711) およびビデオ (H264) 用にさまざまなコーデックを使用できます。

ピアは、セッション記述プロトコル (SDP) Offer/Answer を使用して、通話確立プロセス中にこれらのコーデックをネゴシエートします。 Citrix のユーザーあたりの最小推奨事項は次のとおりです。

タイプ	帯域幅	コーデック
音声 (双方向)	約 90 kbps	G.722
音声 (双方向)	約 60 kbps	オーパス*
ビデオ (双方向)	約 700 kbps	H264 360p で 30 fps 16:9
画面共有	約 300 kbps	H264 1080p、15フレーム/秒

* Opusは、6 kbpsから510 kbpsまでの定ビットレートおよび可変ビットレートエンコーディングをサポートしています。

OpusとH264は、ピアツーピアおよび電話会議に推奨されるコーデックです。

重要:

パフォーマンスについてですが、クライアントマシンでのCPU使用量に関して、エンコードはデコードよりもコストがかかります。LinuxおよびWindows版Citrix Workspaceアプリで、最大エンコード解像度をハードコードできます。「エンコーダーパフォーマンス見積もり」および「Microsoft Teamsの最適化」を参照してください。

プロキシサーバー

プロキシの場所に応じて、以下を考慮してください。

- VDAでのプロキシ構成:

  VDAで明示的なプロキシサーバーを構成し、localhostへの接続をプロキシ経由でルーティングすると、リダイレクトは失敗します。プロキシを正しく構成するには、 **>>>** で 設定を選択し、`127.0.0.1:9002`をバイパスする必要があります。

  PACファイルを使用する場合、PACファイルからのVDAプロキシ構成スクリプトは、`wss://127.0.0.1:9002`に対して **DIRECT** を返す必要があります。そうでない場合、最適化は失敗します。スクリプトが **DIRECT** を返すことを確認するには、`shExpMatch(url, "wss://127.0.0.1:9002/*")`を使用します。

- Citrix Workspaceアプリでのプロキシ構成:

  支社がプロキシ経由でインターネットにアクセスするように構成されている場合、以下のバージョンがプロキシサーバーをサポートします。

  - Citrix Workspaceアプリ for Windowsバージョン2012 (Negotiate/Kerberos、NTLM、Basic、Digest。`Pac`ファイルもサポートされています)
  - Citrix Workspaceアプリ for Windowsバージョン1912 CU5 (Negotiate/Kerberos、NTLM、Basic、Digest。`Pac`ファイルもサポートされています)
  - Citrix Workspaceアプリ for Linuxバージョン2101 (匿名認証)
  - Citrix Workspaceアプリ for Macバージョン2104 (匿名認証)

以前のバージョンのCitrix Workspaceアプリを搭載したクライアントデバイスは、プロキシ構成を読み取ることができません。これらのデバイスは、トラフィックをMicrosoft 365 TURNサーバーに直接送信します。

> **重要:**

> - クライアントデバイスがDNS解決を行うためにDNSサーバーに接続できることを確認してください。クライアントデバイスは、以下のMicrosoft Teamsリレーサーバーの FQDN を解決できる必要があります。
>
>   - `worldaz.relay.teams.microsoft.com`

- `inaz.relay.teams.microsoft.com`
- `uaeaz.relay.teams.microsoft.com`
- `euaz.relay.teams.microsoft.com`
- `usaz.relay.teams.microsoft.com`
- `turn.dod.teams.microsoft.us`
- `turn.gov.teams.microsoft.us`

DNS要求が失敗した場合、外部ユーザーとのP2P通話およびメディア確立を伴う会議通話は失敗します。

- 会議サーバーの場所は、最初の参加者の仮想デスクトップの場所に基づいて選択されます（クライアントではありません）。

通話の確立とメディアフローパス

可能な場合、Citrix WorkspaceアプリのHDX WebRTCメディアエンジン（HdxRtcEngine.exe）は、ピアツーピア通話でユーザーデータグラムプロトコル（UDP）を介した直接ネットワークのセキュアリアルタイムトランスポートプロトコル（SRTP）接続を確立しようとします。UDPハイポートがブロックされている場合、メディアエンジンはTCP/TLS 443にフォールバックします。

HDXメディアエンジンは、候補の検出と接続の確立のために、ICE、NAT用セッショントラバーサルユーティリティ（STUN）、およびNAT周辺リレーを使用したトラバーサル（TURN）をサポートしています。このサポートは、エンドポイントがDNS解決を実行できる必要があることを意味します。

2つのピア間、またはピアと会議サーバー間に直接パスがなく、多人数通話または会議に参加しているシナリオを考えてみましょう。HdxRtcEngine.exeは、Microsoft 365のMicrosoft Teamsトランスポートリレーサーバーを使用して、他のピアまたは会議がホストされているメディアプロセッサに到達します。クライアントマシンは、3つのMicrosoft 365サブネットIPアドレス範囲と4つのUDPポート（UDPがブロックされている場合はフォールバックとしてTCP/TLS 443）にアクセスできる必要があります。詳細については、通話設定 および Office 365 URLとIPアドレス範囲 ID 11 のアーキテクチャ図を参照してください。

ID	カテゴリ	アドレス	宛先ポート
11	最適化が必要	13.107.64.0/18, 52.112.0.0/14, 52.122.0.0/15	**UDP:** 3478, 3479, 3480, 3481, **TCP:** 443 (フォールバック)

これらの範囲には、トランスポートリレーとメディアプロセッサの両方が含まれており、Azure Load Balancerによってフロントエンドされています。 Microsoft Teamsトランスポートリレーは STUNおよびTURN機能を提供しますが、ICEエンドポイントではありません。また、Microsoft Teamsトランスポートリレーはメディア、TLSを終端したり、トランスコーディングを行ったりしません。他のピアまたはメディアプロセッサにトラフィックを転送する際に、TCP（HdxRtcEngine.exeがTCPを使用する場合）をUDPにブリッジできます。

WorkspaceアプリのWebRTCメディアエンジンは、Microsoft 365クラウド内で最も近いMicrosoft Teamsトランスポートリレーに接続します。メディアエンジンは、エニーキャストIPとポート3478～3481 UDP（ワークロードごとに異なるUDPポートですが、多重化が発生する可能性があります）、またはフォールバックとして443 TCP/TLSを使用します。通話品質は基盤となるネットワークプロトコルに依存します。UDPは常にTCPよりも推奨されるため、ブランチオフィスでUDPトラフィックに対応できるようにネットワークを設計することをお勧めします。

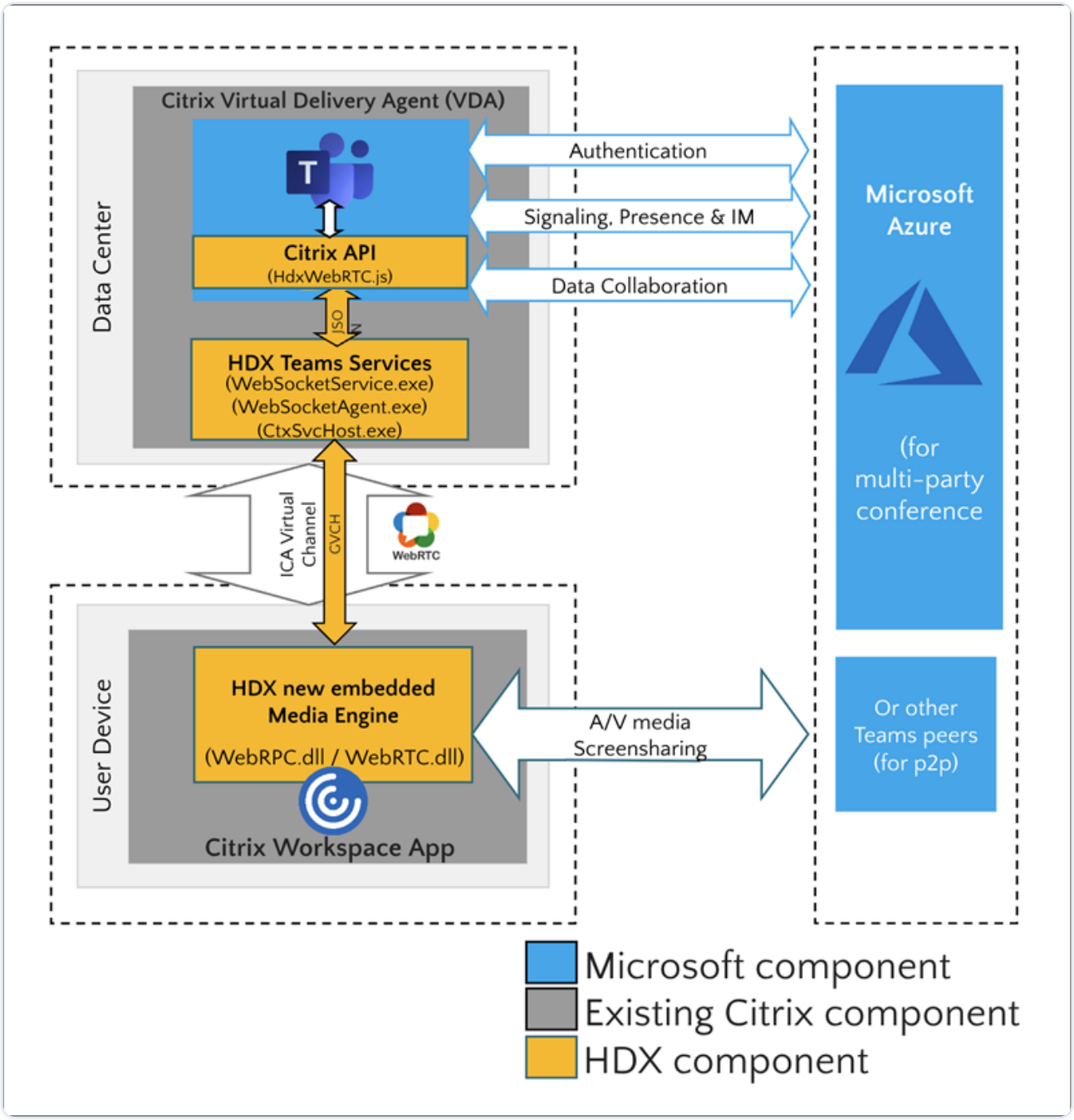
Microsoft Teamsが最適化モードでロードされ、HdxRtcEngine.exeがエンドポイントで実行されている場合、ICEの障害により通話設定の失敗や、音声/ビデオが片方向のみになる可能性があります。通話が完了できない場合やメディアストリームが全二重でない場合は、まずエンドポイントの**Wiresharkトレース**を確認してください。ICE候補収集プロセスに関する詳細については、サポートセクションの「ログの収集」を参照してください。

> **注:**
>
> エンドポイントにインターネットアクセスがない場合でも、両方のユーザーが同じLAN上にいれば、ピアツーピア通話を行うことができる場合があります。会議は失敗します。この場合、通話設定が開始されるまでに30秒のタイムアウトが発生します。

通話設定

このアーキテクチャ図を、通話フローシーケンスの視覚的な参照として使用してください。対応する手順は図に示されています。

アーキテクチャ



1. Microsoft Teams を起動します。
2. Microsoft Teams は O365 に対して認証を行います。テナントポリシーは Microsoft Teams クライアントにプッシュされ、関連する TURN およびシグナリングチャネル情報がアプリに中継されます。
3. Microsoft Teams は VDA で実行されていることを検出し、Citrix JavaScript API に API 呼び出しを行います。
4. Microsoft Teams 内の Citrix JavaScript は、VDA で実行されている WebSocketService.exe に対してセキュアな WebSocket 接続を開き、これによりユーザーセッション内で WebSocketAgent.exe が生成されます。

5. WebSocketAgent.exe は、Citrix HDX Microsoft Teams Redirection Service (CtxSvcHost.exe) を呼び出すことによって、汎用仮想チャネルをインスタンス化します。
6. Citrix Workspace アプリの wfica32.exe (HDX エンジン) は、HdxRtcEngine.exe と呼ばれる新しいプロセスを生成します。これは、Microsoft Teams の最適化に使用される新しい WebRTC エンジンです。
7. Citrix メディアエンジンと Teams.exe は双方向仮想チャネルパスを持ち、マルチメディア要求の処理を開始できます。

   -----ユーザー通話------

8. **ピア A** が **通話** ボタンをクリックします。Teams.exe は Microsoft 365 の Microsoft Teams サービスと通信し、**ピア B** とのエンドツーエンドのシグナリングパスを確立します。Microsoft Teams は HdxRtcEngine に、サポートされている一連の通話パラメーター (コーデック、解像度など。これはセッション記述プロトコル (SDP) オファーとして知られています) を要求します。これらの通話パラメーターは、シグナリングパスを使用して Microsoft 365 の Microsoft Teams サービスに中継され、そこからもう一方のピアに中継されます。
9. SDPオファー/アンサー（シングルパスネゴシエーション）はシグナリングチャネルを介して行われ、ICE接続チェック（STUNバインド要求を使用したNATおよびファイアウォールトラバーサル）が完了します。その後、Secure Real-time Transport Protocol (SRTP)メディアは、HdxRtcEngine.exeと他のピア間（会議の場合はMicrosoft 365会議サーバー）で直接流れます。

マイクロソフト 電話システム

Phone Systemは、Microsoft Teamsを使用してMicrosoft 365クラウドで通話制御とPBXを可能にするMicrosoftのテクノロジーです。Microsoft Teamsの最適化は、Microsoft 365 Calling PlansまたはDirect Routingを使用してPhone Systemをサポートします。Direct Routingを使用すると、追加のオンプレミスソフトウェアなしで、サポートされている独自のセッションボーダーコントローラーをMicrosoft Phone Systemに直接接続できます。 通話キュー、転送、フォワード、保留、ミュート、通話再開がサポートされています。

DTMF

デュアルトーン多周波（DTMF）機能は、以下のバージョンのCitrix Workspaceアプリ（およびそれ以降）でサポートされています。

- Citrix Workspace アプリ for Windows バージョン 2102
- Citrix Workspaceアプリ Windows版 LTSR 1912 CU5 (Windows 10 OSのみ)
- Citrix Workspaceアプリ for Linux バージョン 2101
- Citrix Workspaceアプリ for Mac バージョン 2101

- ChromeOS向けCitrix Workspaceアプリ バージョン2111.1

動的e911のサポート

バージョン2112以降、Citrix Workspaceアプリは動的緊急通報をサポートしています。Microsoft Calling Plans、Operator Connect、およびDirect Routingで使用する場合、以下のことが可能になります。

- 緊急通報の設定とルーティング。
- セキュリティ担当者への通知。

通知は、VDAで実行されているMicrosoft Teamsクライアントではなく、エンドポイントで実行されているCitrix Workspaceアプリの現在の場所に基づいて提供されます。

Ray Baum法では、911通報者の派遣可能な位置情報を適切な公共安全応答拠点（PSAP）に送信することが義務付けられています。HDXによるMicrosoft Teamsの最適化は、以下のバージョンのCitrix Workspaceアプリで使用する場合、Ray Baum法に準拠しています。

- Citrix Workspaceアプリ for Windows バージョン 2112.1 以降
- Citrix Workspaceアプリ for Linux バージョン 2112 以降
- Citrix Workspaceアプリ for Mac バージョン 2112 以降
- Citrix Workspaceアプリ for ChromeOS バージョン 2112 以降

動的な緊急通報を有効にするには、管理者はMicrosoft Teams管理センターを使用して、ネットワークまたは緊急ロケーションマップを作成するために以下を構成する必要があります。

- ネットワーク設定
- ロケーション情報サービス (LIS)

動的緊急通報の詳細については、Microsoft のドキュメントを参照してください。

Citrix WorkspaceアプリがMicrosoft Teamsに中継するディスパッチ可能な位置情報は次のとおりです。

- イーサネット/スイッチ接続用のリンク層検出プロトコル (LLDP) を使用したシャーシ ID / ポート ID。イーサネット/スイッチ (LLDP) は以下でサポートされています。
  - Windows バージョン 8.1 および 10
  - LLDP 有効化ソフトウェアを必要とする macOS。LLDP 有効化ソフトウェアをダウンロードするには、`www.microsoft.com`にアクセスして「LLDP enablement software」を検索してください。

    - Linux。シンクライアントのオペレーティングシステム (OS) ディストリビューションに LLDP ライブラリを含める必要があります。

- Citrix Workspace アプリがインストールされているエンドポイントの WLAN BBSID および {IPv4-IPv6; サブネット; MAC アドレス}。

    - サブネットおよび WiFi ベースのロケーションは、Windows、Linux、Mac 用 Workspace アプリでサポートされています。

- Citrix Workspaceアプリがインストールされ ているOSレベルでユーザーの許可が与えられている場合（権限がHDX RTC Engineに設定されている場合）の緯度と経度

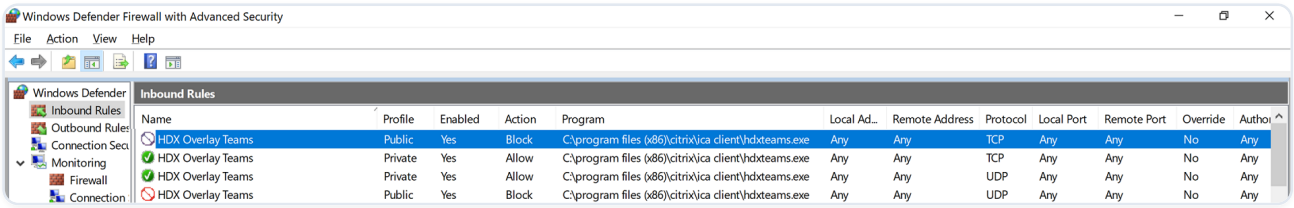
    - すべてのWorkspaceアプリプラットフォームでサポートされています。ただし、Citrix Workspace for Linuxの場合、シンクライアントのOSディストリビューションに`libgps`ライブラリを含める必要があります（>sudo apt-get install libgps23 gpsd lldpd）。

ファイアウォールの考慮事項

ユーザーが Microsoft Teams クライアントを使用して最適化された通話を初めて開始すると、**Windows ファイアウォール**設定に関する警告が表示されることがあります。この警告は、HdxTeams.exe または HdxRtcEngine.exe (HDX Overlay Microsoft Teams) の通信を許可するようユーザーに求めます。

ファイアウォールの警告](/en-us/citrix-virtual-apps-desktops/current-release/media/firewall1.png)

「**Windows Defender ファイアウォール > セキュリティが強化されたWindows Defender ファイアウォール**」コンソールの**受信の規則**に、次の4つのエントリが追加されます。必要に応じて、より制限の厳しい規則を適用できます。



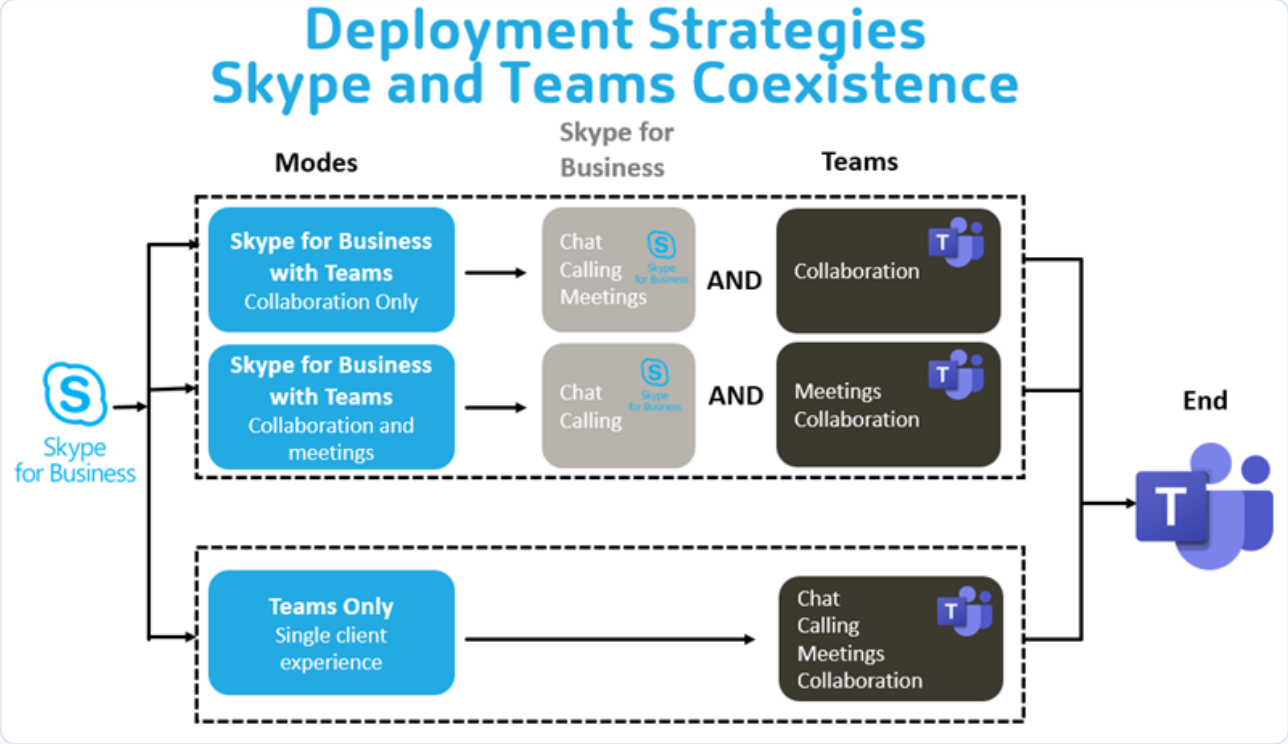
Microsoft Teams と Skype for Business の共存について

Microsoft TeamsとSkype for Businessは、機能が重複する2つの個別のソリューションとして並行して展開できます。 詳細については、「Microsoft TeamsとSkype for Businessの共存と相互運用性を理解する」を参照してください。

Citrix RealTime Optimization PackとMicrosoft Teamsマルチメディアエンジン用のHDX最適化は、環境で設定された構成を尊重します。例としては、アイランドモードや、Microsoft Teamsとの

Skype for Businessコラボレーションなどがあります。また、Microsoft TeamsとのSkype for Businessコラボレーションと会議も含まれます。

周辺機器へのアクセスは、一度に1つのアプリケーションにのみ許可されます。たとえば、通話中にRealTime Media EngineがWebカメラにアクセスすると、通話中はイメージングデバイスがロックされます。デバイスが解放されると、Microsoft Teamsで利用できるようになります。



Citrix SD-WAN™: Microsoft Teams向けに最適化されたネットワーク接続

最適なオーディオおよびビデオ品質には、低遅延、低ジッター、低パケット損失のMicrosoft 365クラウドへのネットワーク接続が必要です。支社のCitrix Workspaceアプリユーザーからデータセンターを経由してインターネットに接続する前に、Microsoft Teamsのオーディオ/ビデオRTPトラフィックをバックホールすると、過剰な遅延が発生する可能性があります。また、WANリンクで輻輳を引き起こす可能性もあります。Citrix SD-WANは、Microsoft 365のネットワーク接続原則に従って、Microsoft Teamsの接続を最適化します。Citrix SD-WANは、Microsoft RESTベースのMicrosoft 365 IPアドレスとWebサービス、および近接DNSを使用します。これは、Microsoft Teamsトラフィックを識別、分類、および誘導するために使用されます。

多くの地域で、ビジネスブロードバンドインターネット接続は、断続的なパケット損失、過剰なジッター期間、および停止に悩まされています。

Citrix SD-WANは、ネットワークの状態が不安定または劣化している場合に、Microsoft Teamsのオーディオ/ビデオ品質を維持するための2つのソリューションを提供します。

- Microsoft Azureを使用している場合、Azure VNETに展開されたCitrix SD-WAN仮想アプライアンス（VPX）は、高度な接続最適化を提供します。これらの最適化には、シームレスなリンクフェイルオーバーとオーディオパケットレーシングが含まれます。
- Citrix SD-WANのお客様は、Citrix Cloud™ Directサービスを介してMicrosoft 365に接続できます。このサービスは、すべてのインターネット向けトラフィックに対して信頼性の高い安全な配信を提供します。

支社のインターネット接続の品質が問題にならない場合は、遅延を最小限に抑えるだけで十分かもしれません。遅延を最小限に抑えるために、Microsoft TeamsトラフィックをCitrix SD-WANブランチアプライアンスから最寄りのMicrosoft 365フロントドアに直接誘導します。詳細については、「Citrix SD-WAN Office 365の最適化」を参照してください。

シトリックス SD-WAN](/en-us/citrix-virtual-apps-desktops/current-release/media/sd-wan.png)

マルチウィンドウ会議とチャット

Windows版Microsoft Teamsでは、複数の会議またはチャットウィンドウを使用できます。ポップアウト機能の詳細については、Microsoft 365サイトのMicrosoft Teams Pop-Out Windows for Chats and Meetingsを参照してください。

> **注:**

> この機能は、Citrix Workspaceアプリ for Windows 2112.1、Mac 2203、Linux 2203、ChromeOS 2303でサポートされています。VDA 2112以降が必要で、1912 CU6+ LTSRにバックポートされました。

背景のぼかしと背景効果

Windows、Mac、Linux、ChromeOS/HTML5 用 Citrix Workspace アプリは、HDX を使用した Microsoft Teams の最適化において、背景のぼかしと背景効果をサポートしています。

背景をぼかしたり、デフォルトの画像に置き換えたりすることで、会話がシルエット（体と顔）に集中できるようにし、予期せぬ邪魔を避けることができます。この機能は、P2P または電話会議で使用できます。

> **注:**

> この機能は、Microsoft Teams の UI/ボタンと統合されています。マルチウィンドウのサポートは、VDA を 2112 以降に更新する必要がある前提条件です。詳細については、「マルチウィンドウ会議とチャット」を参照してください。

> 背景のぼかしと効果に関する Microsoft Teams UI コントロールには、以下の最小バージョンが必要です。

- Windows 2207 用 Citrix Workspace アプリ
- Mac 2301 用 Citrix Workspace アプリ
- Citrix Workspaceアプリ Linux向け 2307
- ChromeOS 2303 用 Citrix Workspace アプリ

制限事項:

- クライアントは、背景画像をMicrosoft Teamsのデフォルト画像に置き換える間、インターネットに接続されている必要があります。
- 管理者およびユーザー定義の背景画像の置き換えは、Microsoft Teams UIではサポートされていません。カスタム背景画像は、画像がクライアントにも保存されている場合、クライアント上の構成設定を使用して構成できます。

カスタム背景画像の設定

以下のレジストリキーは、Microsoft Teams UIを使用してこの機能を制御する予定がない場合、または管理者がデフォルトの動作を上書きしたい場合にのみ必要です。たとえば、エンドポイントの性能が十分でないため、背景のぼかしを無効にする場合などです。

Windowsの場合

カスタム背景画像を設定するには、管理者またはエンドユーザーがクライアントまたはエンドポイントで以下のレジストリキーを構成する必要があります。

場所: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`

- 名前: VideoBackgroundEffect
- 種類: DWORD
- 値: 0 (無効), 1 (有効), 2 (背景画像の置き換え)

1に設定された値は背景をぼかします。この値はエンドユーザーまたは管理者が設定できます。

値を2に設定した場合、**VideoBackgroundImage** キーも存在する必要があります。この値は管理者のみが設定できます。以下のキーは、背景画像を置き換えたい場合のみ必要であり、ぼかしには必要ありません。

- 名前: VideoBackgroundImage
- 種類: REG_SZ
- 値: my_image_name.jpeg

ビデオの背景画像は`C:\Program Files (x86)\Citrix\ICA Client`ディレクトリに存在する必要があります。

このレジストリ構成は、Microsoft Teams UIセレクターなしでCitrix Workspaceアプリ2206での背景ぼかしまたは画像置換を有効にするためにも使用できます。言い換えれば、環境またはVDAがマルチウィンドウをサポートしていない場合でも、Citrix Workspaceアプリ2206以降でHKCUレジストリの回避策を適用して同様の結果を得ることができます。ただし、ユーザーはHDXセッション中またはMicrosoft Teams通話中に機能を制御することはできません。

レジストリキーの変更は、HDXセッションが接続したときにのみ有効になります。

Macの場合

ユーザーがダウンロードした画像の場所: */Users/username/Downloads/any_image.png*

カスタム画像をデフォルト画像として設定するには、次のコマンドを実行します。

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundEffect -int 2
```

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundImage -string "/Users/username/Downloads/any_image.png"
```

Linuxの場合

ユーザーがダウンロードした画像の場所: */home/username/Downloads/any_image.jpg*

ファイル */var/.config/citrix/hdx_rtc_engine/config.json* を作成し、以下の構成キーをJSON形式で追加します。例：

```
{



"VideoBackgroundEffect":2,


```

```
"VideoBackgroundImage":"/home/username/Downloads/any_image.jpg"



}
```

HTML5の場合

1. **HTML5Client** フォルダー内の **configuration.js** ファイルに移動します。
2. 属性 **backgroundEffects** を追加し、属性を **true** に設定します。例:

```
'features' : {

    'msTeamsOptimization' :

    {

        'backgroundEffects' : true

    }

}
```

3. 変更を保存します。

クライアントCPU消費に関する考慮事項

ぼかし機能はCPUへの負荷が低いですが、消費量の増加が予想されます。たとえば、4コア、1.5 GHz Intel® Pentium® Silverチップ（TurboBoostで最大2.8 GHz）を搭載したシンクライアントでは、背景のぼかしによりCPU使用率が約2%増加します。平均CPU使用率は20%未満です。

Microsoft Teamsのギャラリービューとアクティブスピーカー

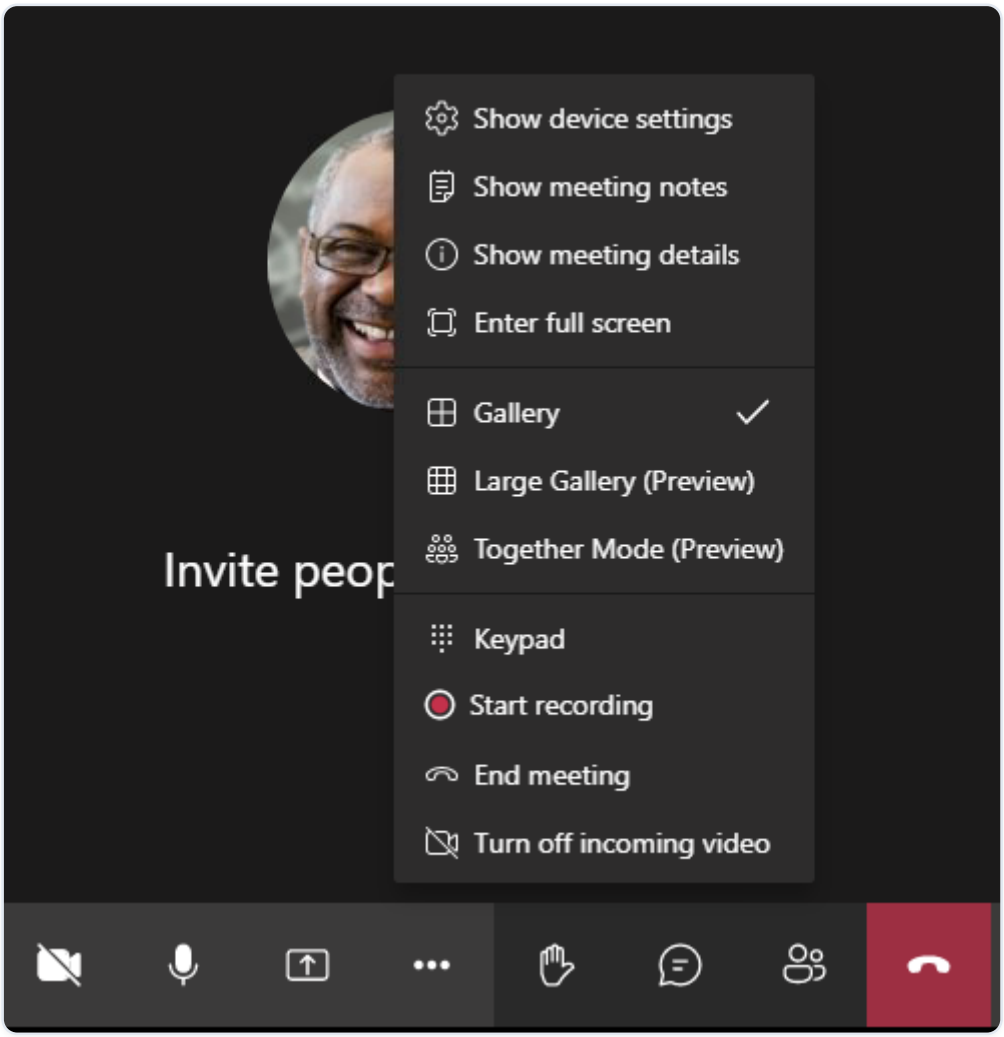
Microsoft Teamsは、**ギャラリー**、**大規模ギャラリー**、および**Together**モードのレイアウトをサポートしています。

Microsoft Teamsは、4人の参加者のビデオストリームを2x2のグリッドで表示します（**ギャラリー**として知られています）。この場合、Microsoft Teamsは4つのビデオストリームをクライアントデバイスに送信してデコードします。4人を超える参加者がビデオを共有している場合、画面には最後に最もアクティブだった4人の話者のみが表示されます。

Microsoft Teamsは、最大7x7のグリッドを持つ大規模ギャラリービューも提供します。その結果、Microsoft Teams会議サーバーは単一のビデオフィードを合成し、それをクライアントデバイスに送信してデコードするため、CPU消費量が低減されます。この単一のマトリックス形式のフィードには、ユーザーのセルフプレビュービデオも含まれる場合があります。

最後に、Microsoft Teamsは新しい会議エクスペリエンスの一部である**Togetherモード**をサポートしています。AIセグメンテーション技術を使用して参加者を共有背景にデジタル配置することで、Microsoft Teamsはすべての参加者を同じ講堂に配置します。

ユーザーは、会議中に省略記号メニューで**ギャラリー**、**大規模ギャラリー**、または**Togetherモード**のレイアウトを選択することで、これらのモードを制御できます。



ビデオアスペクト比の制約のサポート（Citrix Workspaceアプリ for Windows 2102、Citrix Workspaceアプリ for Linux 2106、Citrix Workspaceアプリ for MAC 2106以降）：

- **フレームに合わせる**オプションは、ギャラリー/大規模ギャラリービューで利用できます。このオプションは、サブウィンドウに収まるようにビデオサイズをトリミングします。一方、**フレームにフィット**は、ビデオの側面に黒いバー（レターボックス）を表示するため、トリミングは行われません。

次の表は、ギャラリーレイアウトと大規模ギャラリーレイアウトの比較を示しています。

	ギャラリービュー 2X2 (デフォルト)	ラージギャラリービュー
レイアウト/グリッド	4人の参加者のビデオストリームを含む2x2のグリッドを表示します。画面には直近の最もアクティブな4人のスピーカーのみが表示され、他の参加者はグリッドに表示されません。	49人の参加者のビデオストリームを含む7x7のグリッドを表示します。
ミキシング技術	メディアルーターは、各参加者からの個々のストリームをすべてのユーザーに転送します。	中央の会議サーバーがすべてのオーディオまたはビデオをミキシングおよびトランスコードし、各参加者向けにカスタマイズされた複合レイアウトを作成します。この処理により、追加の遅延が発生します。
アクティブスピーカー	新しいアクティブスピーカーは、グリッド内で最もアクティブでないスピーカーと置き換わります。	アクティブか非アクティブかに関わらず、すべての参加者を表示します。
エンドポイントでのエンコード	Simulcastが有効になっている場合、1つ以上のビデオストリームがエンドポイントでエンコードされることがあります。Simulcastのサポートの詳細については、「Simulcast」を参照してください。	Simulcastが有効になっている場合、1つ以上のビデオストリームがエンドポイントでエンコードされることがあります。Simulcastのサポートの詳細については、「Simulcast」を参照してください。
エンドポイントでのデコード	各参加者は最大4つの個別のメディアストリームを受信します。これにより、HdxRtcEngine.exeによるエンドポイントでのCPU消費量が増加します（デコード/レンダリングのため）。	各参加者は、オーディオとビデオの単一ストリームのみを取得します。この設定により、エンドポイントでのCPU消費が削減されます。

	ギャラリービュー 2X2 (デフォルト)	ラージギャラリービュー
最大解像度	720p。4人の参加者がビデオを共有している場合、ビデオフィードあたりの最大解像度は360pです。4人未満の参加者がビデオを共有している場合、ビデオフィードあたりの解像度は高くなる可能性があります。	複合レイアウトまたはミキシングの場合は720p。複合レイアウトでは、参加者ごとに高品質のビデオストリームは必要ありません。この条件のため、各送信者は解像度またはアップロードビットレートを削減します。
「低速ユーザー」の問題	送信者は、各モダリティ（オーディオ/ビデオ/画面共有）の品質を、参加者間の最低共通ネットワーク品質に調整します。このマルチメディアストリームは、他のすべての参加者に転送されます。その結果、ネットワーク状態の悪い参加者が、通話中の他の全員の品質に影響を与えます。	最低共通ネットワーク品質のシナリオの影響を受けにくい。会議サーバーは、個々の参加者のネットワーク状態に基づいて異なる品質を提供します。
セルフプレビュー	自分自身を小さなサムネイルでリアルタイムに表示します。	自分自身をサムネイルで表示し、他のビデオフィードと混合します。その結果、メインのビデオレイアウトに自分自身が追加の遅延とともに含まれて表示されることがあります。

Microsoft Teamsでの画面共有

Microsoft Teamsは、ビデオベースの画面共有（VBSS）に依存しており、共有されているデスクトップをH264などのビデオコーデックで効率的にエンコードし、高精細ストリームを作成します。HDX最適化を使用すると、受信する画面共有はビデオストリームとして扱われます。

Windows、Linux、Mac向けのCitrix Workspaceアプリ2109以降、およびChromeOS向けのCitrix Workspaceアプリ2303以降では、ユーザーは画面とビデオカメラを同時に共有できます。

以前のバージョンでは、ビデオ通話中に相手がデスクトップの共有を開始すると、元のカメラビデオフィードは一時停止されます。代わりに、画面共有ビデオフィードが表示されます。その後、相手は手動でカメラ共有を再開する必要があります。

PowerPoint Liveに関する注意

PowerPoint Liveからコンテンツを共有している場合、この制限は存在しません。その場合、他のピアは引き続きあなたのウェブカメラとコンテンツを見ることができ、他のスライドを確認するために前後に移動できます。このシナリオでは、スライドはVDA上でレンダリングされます。PowerPoint Liveのスライドデッキにアクセスするには、「Share tray」ボタンをクリックし、提案されたPowerPointスライドのいずれかを選択するか、「Browse」をクリックしてコンピューターまたはOneDrive上のPowerPointファイルを見つけます。

送信画面共有も最適化され、Citrix Workspaceアプリにオフロードされます。この場合、メディアエンジンはCitrix Desktop Viewer (CDViewer.exe) ウィンドウのみをキャプチャして送信し、その周囲には赤い枠線が描画されます。Desktop Viewerと重なるローカルアプリケーションはキャプチャされません。

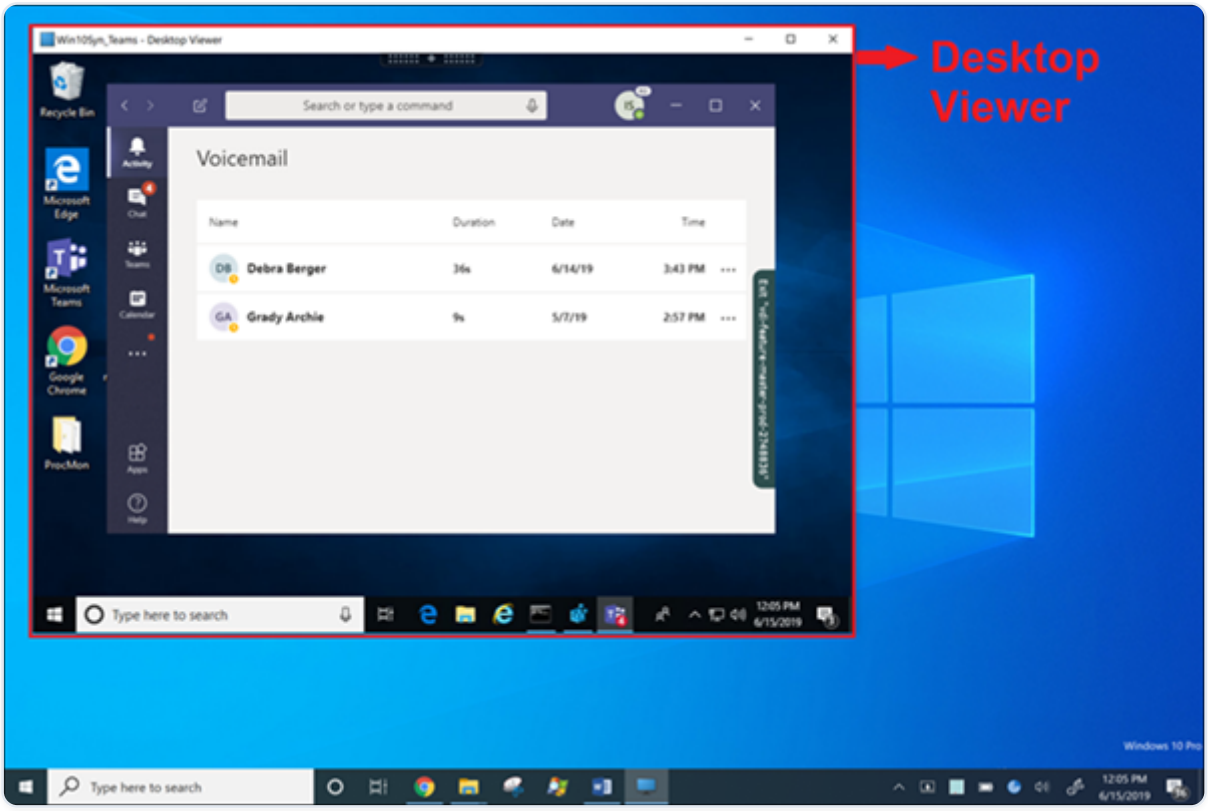
注

Mac版Citrix Workspaceアプリで画面共有を有効にするには、特定の権限を設定してください。詳細については、システム要件を参照してください。

既知の制限:

- Desktop Viewerが無効になっている場合、またはDesktop Lockが使用されている場合、Microsoft Teamsの画面ピッカーではマルチモニター選択は利用できません。Desktop Viewerは、`.ICA`ファイルテンプレートを編集するか、`StoreFront web.config`によって無効にすることができます。SHIFT+F2ホットキーはマルチモニター画面共有と互換性がありません。
- Workspaceアプリのバージョン2106より前では、プライマリモニターのみが共有されます。仮想デスクトップ内のアプリケーションをプライマリモニターにドラッグすると、通話中の他のピアがそれを見ることができます。
- Citrix Workspaceアプリを仮想モニターレイアウト機能（単一の物理モニターの論理パーティション）で構成した場合、マルチモニター画面共有が機能しない可能性があります。この場合、すべての仮想モニターは複合画像として共有されます。

- Citrix Workspaceアプリ for Windowsの古いバージョン（1907から2008まで）では、クライアントマシンで実行されているローカルアプリケーションも共有されます。この共有は、ローカルアプリがDesktop Viewerの上にオーバーレイされている場合にのみ可能です。この動作は、2009.6以降および1912 CU5以降で削除されました。
- 画面共有中にウィンドウモードからフルスクリーンに変更すると、画面共有が停止します。画面共有を機能させるには、一度停止して再度共有する必要があります。
- 最適化されたMicrosoft Teamsでは、共有コントロールを特定の場所にピン留めすることはできません。
- 最小化されたアプリを共有すると、アプリのタイトルバーも共有される場合があります。



シームレスアプリケーションからの画面共有:

Microsoft Teamsをスタンドアロンのシームレスアプリケーションとして公開している場合、画面共有は物理エンドポイントのローカルデスクトップをキャプチャします。Citrix Workspaceアプリの最小バージョン1909が必要です。

アプリ共有

Citrix Workspaceアプリ for Windows 2112.1およびVDA 2112以降、Microsoft Teamsはアプリ共有をサポートしています。

Citrix Workspaceアプリ for Windows 2109、Mac 2203、Linux 2209、およびVDA 2109以降、Microsoft Teamsは仮想セッションで実行されている特定のアプリの画面共有をサポートしていま

す。最適化されたMicrosoft Teamsを使用して、Javaなどのカスタム社内アプリケーションを共有することもできます。特定のアプリを共有するには：

1. リモートセッション内でMicrosoft Teamsアプリに移動します。
2. Microsoft Teams UIで**コンテンツを共有**をクリックします。
3. 会議で共有するアプリを選択します。選択したアプリの周囲に赤い枠が表示され、通話中のピアは共有されたアプリを見ることができます。

別のアプリを共有するには、もう一度**コンテンツを共有**をクリックして、新しいアプリを選択します。

アプリ共有を無効にする場合は、VDAの`HKLM\SOFTWARE\Citrix\Graphics`に次のレジストリキーを作成します。 名前: `UseWsProvider` 種類: `DWORD` 値: 0

> **注:**
>
> - アプリを最小化すると、Microsoft Teamsは共有アプリの最後の画像を表示します。画面共有を再開するには、ウィンドウを最大化できます。
> - 画面共有は、VDA側でのウィンドウのキャプチャに依存します。コンテンツは最大レートでCitrix Workspaceアプリに中継されます。最大レートは1秒あたり30フレームです。Citrix Workspaceアプリは、コンテンツをピアまたは会議サーバーに転送します。

> Microsoft Teamsのアプリ共有](/en-us/citrix-virtual-apps-desktops/current-release/media/ms-teams-app-sharing.png)

特定のアプリの画面共有に関する既知の制限：

- アプリを画面共有しているとき、マウスカーソルは表示されません。
- アプリを共有中に最小化すると、スクリーンピッカーにはアプリのアイコンのみが表示されます。アプリのサムネイルはスクリーンピッカーでプレビューされません。アプリを最大化するまで、コンテンツを共有できず、赤い枠も表示されません。
- LAAアプリは、VDAの最適化されたMicrosoft Teamsでデスクトップアプリと共有できるアプリのリストを表示します。ただし、リストからアプリを選択しても、期待どおりの結果にならない場合があります。

アプリ保護との互換性 特定のアプリの画面共有は、HDX最適化されたMicrosoft Teamsのアプリ保護機能と互換性があります。アプリ保護が有効になっているデリバリーグループからアプリまたはデスクトップを起動した場合、特定のアプリを画面共有できます。

Microsoft Teams UIで**コンテンツを共有**をクリックすると、スクリーンピッカーから**デスクトップ**オプションが削除されます。開いているアプリを共有するには、**ウィンドウ**オプションのみを選択できます。

> **注:**
>
> アプリ保護が有効になっているデリバリーグループからアプリまたはデスクトップを起動する場合、Citrix Workspaceアプリ for Windows 2202以前を使用していると、受信ビデオまたは画面共有を表示できません。

Microsoft Teamsで制御を付与および要求する

この機能は、Citrix Workspaceアプリの以下のバージョンでサポートされています（VDAバージョンやオペレーティングシステム、シングルセッションまたはマルチセッションには依存しません）。

- Citrix Workspaceアプリ for Windows バージョン2112.1以降
- Citrix Workspaceアプリ for Mac バージョン2203.1以降
- Citrix Workspaceアプリ for Linux バージョン2203以降
- ChromeOS 版 Citrix Workspace アプリ バージョン 2303 以降

Microsoft Teams通話中に参加者が画面を共有している場合、制御を要求できます。制御を取得すると、共有画面に対して選択、編集、その他のキーボードおよびマウス操作を行うことができます。

画面が共有されているときに制御するには、Microsoft Teams UI の ボタンをクリックします。画面を共有している会議参加者は、要求を許可または拒否できます。

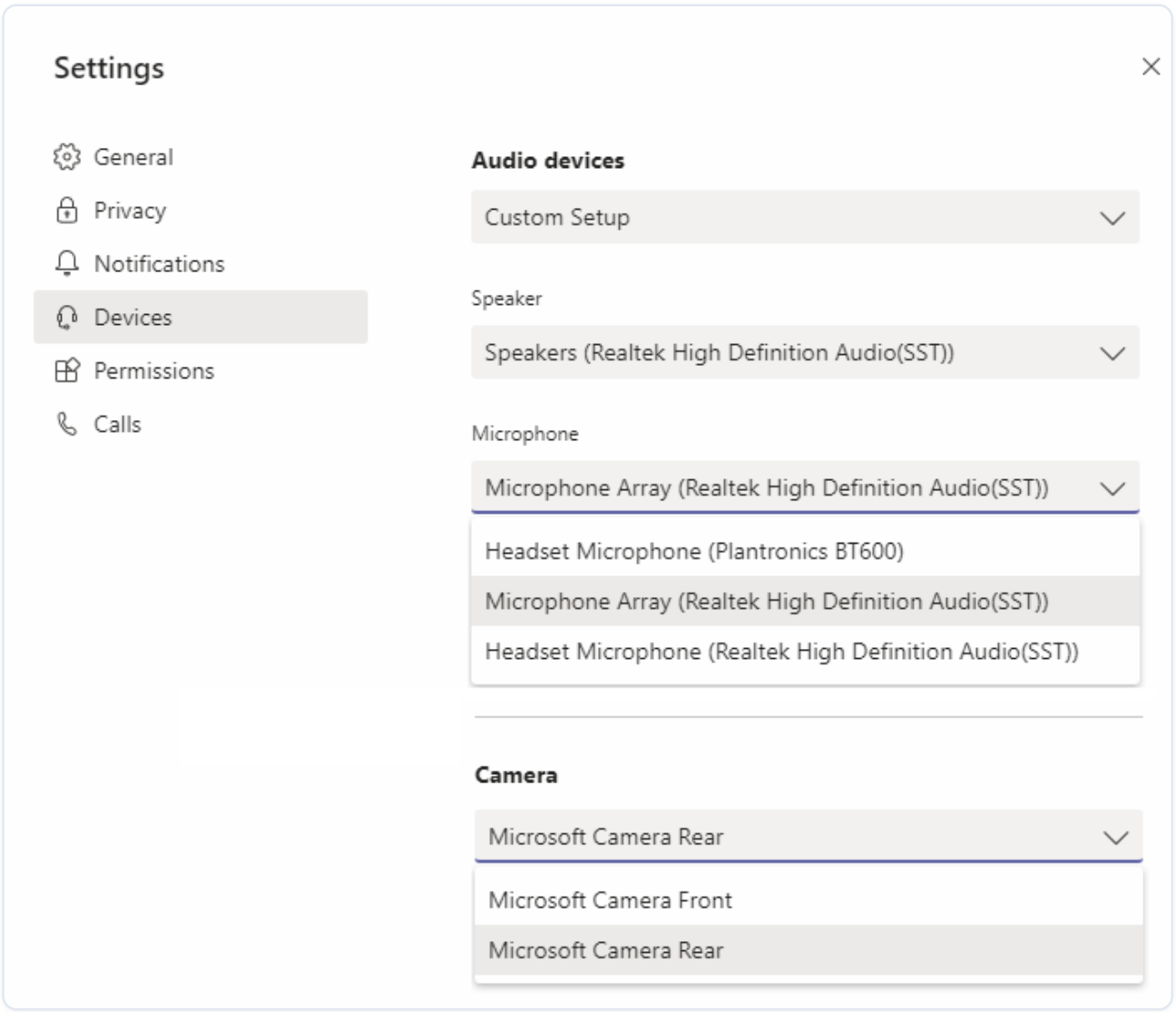
制御中は、共有画面の選択、編集、その他の変更を行うことができます。これらの操作には、キーボードとマウスの両方を使用できます。完了したら、 をクリックします。

> **制限事項:**

- ユーザーが単一のアプリを共有している場合 (アプリ共有とも呼ばれます)、制御の付与と要求は利用できません。デスクトップ全体またはモニターを共有する必要があります。
- コントロールバーを特定の場所に固定する機能は利用できません。

Microsoft Teamsでの周辺機器

Microsoft Teamsの最適化が有効な場合、Citrix Workspaceアプリは周辺機器（ヘッドセット、マイク、カメラ、スピーカーなど）にアクセスします。その後、周辺機器はMicrosoft Teams UIの（**設定 > デバイス**）に適切に一覧表示されます。



Microsoft Teamsはデバイスに直接アクセスしません。代わりに、メディアの取得、キャプチャ、処理のためにWorkspaceアプリのWebRTCメディアエンジンに依存します。Microsoft Teamsは、ユーザーが選択できるようにデバイスを一覧表示します。

Microsoft Teams のアクティブ中に挿入された周辺機器は、デフォルトでは選択されません。Microsoft Teams UI の > 画面から周辺機器を手動で選択する必要があります。周辺機器が選択されると、Microsoft Teams は周辺機器の情報をキャッシュします。その結果、同じエンドポイントからセッションに再接続すると、周辺機器が自動的に選択されます。

推奨事項:

- エコーキャンセレーション機能が内蔵された Microsoft Teams 認定ヘッドセット。マイクとスピーカーが別々のデバイスにある追加の周辺機器を使用するセットアップでは、エコーが発生する可能性があります。例としては、内蔵マイク付きのウェブカメラとスピーカー付きのモニターがあります。外部スピーカーを使用する場合は、マイクからできるだけ離して配置してください。また、音をマイクに屈折させる可能性のある表面からも離して配置してください。詳細については、`www.microsoft.com` にアクセスし、Microsoft Teams 認定ヘッドセットを検索してください。
- Microsoft Teams 認定カメラ。ただし、Skype for Business 認定周辺機器は Microsoft Teams と互換性があります。詳細については、<www.microsoft.com> にアクセスし、Microsoft Teams 認定カメラと Skype for Business 認定周辺機器を検索してください。
- Citrix Workspaceアプリのメディアエンジンは、オンボードH.264エンコーディング（UVC 1.1および1.5）を実行するWebカメラではCPUオフロードを利用できません。

> **注:**
>
> Windows用Workspaceアプリ2009.6は、24ビットまたは96 kHzを超える周波数のオーディオ形式に対応した周辺機器を取得できるようになりました。
>
> HdxTeams.exe（Windows用Citrix Workspaceアプリ2009以前の場合）は、これらの特定のオーディオデバイス形式（チャンネル、ビット深度、サンプルレート）のみをサポートします。
>
> - 再生デバイス: 最大2チャンネル、16ビット、最大96,000 Hzの周波数
> - 録音デバイス: 最大4チャンネル、16ビット、最大96,000 Hzの周波数
>
> スピーカーまたはマイクのいずれかが予期される設定と一致しない場合でも、Microsoft Teamsでのデバイス列挙は失敗し、**設定 > デバイス**の下に**なし**と表示されます。

HdxTeams.exeの**Webrpc**ログには、この種類の情報が表示されます。

`Mar 27 20:58:22.885 webrtcapi.WebRTCEngine Info: init. initializing...`.

`Mar 27 20:58:23.190 webrtcapi.WebRTCEngine Error: init. couldn't create audio module!` !

回避策として、特定のデバイスを無効にするか、次のいずれかを実行します。

1. **サウンドコントロールパネル** (mmsys.cpl) を開きます。
2. 再生デバイスまたは録音デバイスを選択します。
3. **プロパティ > 詳細設定**に移動し、設定をサポートされているモードに変更します。

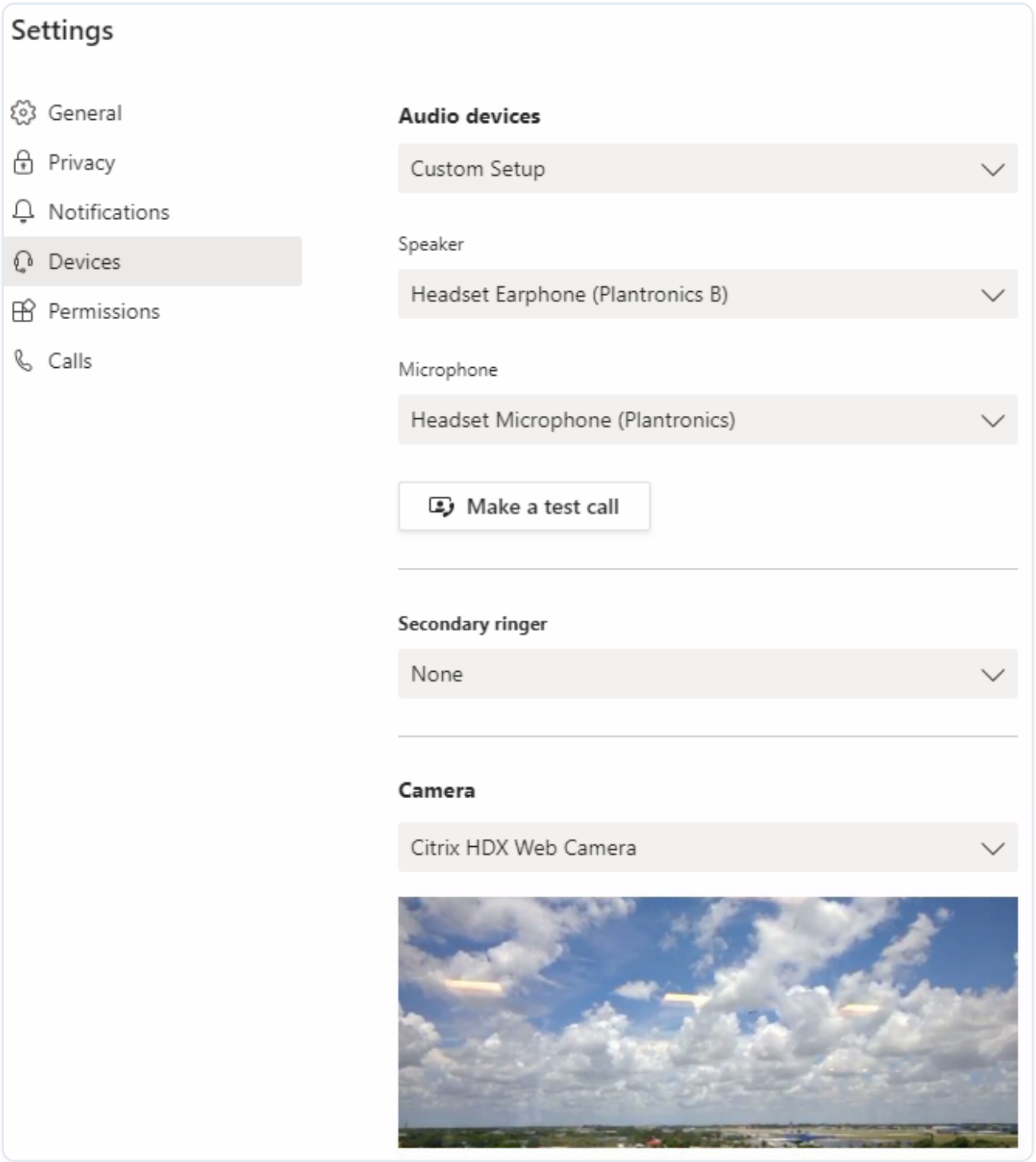
フォールバックモード

Microsoft Teams が最適化された VDI モードでロードに失敗した場合 (Microsoft Teams/バージョン情報/バージョンで「Citrix HDX Not Connected」と表示される場合)、VDA はレガシー HDX テクノロジーにフォールバックします。レガシー HDX テクノロジーには、Web カメラのリダイレクト、クライアントのオーディオとマイクのリダイレクトが含まれる場合があります。Microsoft Teams の最適化をサポートしない Workspace アプリのバージョン/プラットフォーム OS を使用している場合、フォールバックレジストリキーは適用されません。 フォールバックモードでは、周辺機器は VDA にマッピングされます。周辺機器は、仮想デスクトップにローカルで接続されているかのように Microsoft Teams アプリに表示されます。

VDA でレジストリキーを設定することで、フォールバックメカニズムをきめ細かく制御できるようになりました。詳細については、レジストリで管理される機能のリストにある Microsoft Teams フォールバックモード を参照してください。

この機能には、Microsoft Teamsバージョン1.3.0.13565以降が必要です。

Microsoft Teams アプリの **>** タブで、最適化モードか非最適化モードかを判断するには、カメラ名が主な違いとなります。Microsoft Teams が非最適化モードでロードされると、レガシー HDX テクノロジーが起動します。Web カメラ名には、次の図に示すように **Citrix HDX** のサフィックスが付いています。スピーカーとマイクのデバイス名は、最適化モードと比較してわずかに異なる (または切り詰められる) 場合があります。



レガシー HDX テクノロジーが使用されている場合、Microsoft Teams はオーディオ、ビデオ、画面共有の処理をエンドポイントの Citrix Workspace アプリ WebRTC メディアエンジンにオフロードしません。代わりに、HDX テクノロジーはサーバー側レンダリングを使用します。ビデオをオンにすると、VDA で高い CPU 消費が予想されます。リアルタイムオーディオのパフォーマンスは最適ではない可能性があります。

既知の制限事項

Citrixの制限事項

Citrix Workspaceアプリの制限事項：

- HID ボタン - 通話の応答と終了はサポートされていません。音量アップとダウンはサポートされています。
- Microsoft Teamsの管理センターでのQoS設定は、VDIユーザーには適用されません。
- ユーザーは、VDA でスニッピングツールを使用している間は、Microsoft Teams のコンテンツのスクリーンショットを撮ることができません。ただし、クライアント側でスニッピングツールを使用すると、コンテンツをキャプチャできます。

VDAの制限事項：

- **Citrix Workspace アプリの高 DPI** 設定を `Yes` に構成すると、リダイレクトされたビデオウィンドウがずれて表示されます。この制限は、モニターの DPI スケーリング係数が 100% を超える値に設定されている場合に発生します。

Citrix Workspace アプリと VDA の制限事項:

- 最適化された通話の音量は、VDAではなく、クライアントマシンの音量バーを使用してのみ制御できます。

サイマルキャスト

最適化されたMicrosoft Teamsビデオ会議通話のサイマルキャストサポートは、WindowsおよびMacで有効になっています。Linuxについては、シンクライアントベンダーにご確認ください。 サイマルキャストを使用すると、すべての通話者にとって最適な通話体験のために適切な解像度に調整することで、異なるエンドポイント間でのビデオ会議通話の品質とエクスペリエンスが向上します。

この改善されたエクスペリエンスにより、各ユーザーは、エンドポイントの機能、ネットワークの状態など、いくつかの要因に応じて、異なる解像度（たとえば、720p、360pなど）で複数のビデオストリームを配信できます。受信側のエンドポイントは、処理できる最大品質の解像度を要求し、すべてのユーザーに最適なビデオエクスペリエンスを提供します。

> **注:**
>
> この機能は、Microsoft Teamsからのアップデートが展開された後にのみ利用可能です。ETAについては、`<https://www.microsoft.com/>` にアクセスし、Microsoft 365ロードマップ

を検索してください。Microsoftによってアップデートが展開されたら、ドキュメントの更新と発表についてはCTX253754 を確認してください。

Microsoftの制限事項

- 3x3ギャラリービューはサポートされていません。Microsoft Teamsの依存関係 – 3x3グリッドがいつ提供されるかについてはMicrosoftにお問い合わせください。
- Skype for Businessとの相互運用性は音声通話に限定されており、ビデオモダリティはありません。
- 送受信ビデオストリームの最大解像度は720pです。
- PSTN通話の呼び出し音はサポートされていません。
- ダイレクトルーティングのメディアバイパスはサポートされていません。
- ブロードキャストおよびライブイベントのプロデューサーおよびプレゼンターの役割はサポートされていません。出席者の役割はサポートされていますが、最適化されていません（代わりにVDAでレンダリングされます）。
- Microsoft Teamsのズームインおよびズームアウト機能はサポートされていません。
- ロケーションベースルーティングとメディアバイパスはサポートされていません。
- 通話のマージはサポートされていません（ユーザーインターフェイスにオプションが表示されません）。

CitrixとMicrosoftの制限事項

- 画面共有を行う際、**システムオーディオを含める**オプションは利用できません。
- サイマルキャストはChromeOSではサポートされていません。

今後のMicrosoft Teamsシングルウィンドウの EOL

January 31, 2024に、MicrosoftはVDI Microsoft Teams最適化を使用している場合、シングルウィンドウUIに対するMicrosoft Teamsのサポートを終了し、マルチウィンドウエクスペリエンスのみをサポートします。Microsoftは、この非推奨化について9/8/2023にM365管理者センター（投稿ID: MC674419）で通知しました。 マルチウィンドウ機能に関する公開されている詳細は、Tech Communityの記事：New Meeting and Calling Experience in Microsoft Teamsで確認できます。

注:

Citrixは、ビデオおよび画面共有のためにMicrosoft Teamsを最適化モードで引き続き使用するには、VDAとCitrix Workspaceアプリをサポートされているバージョンにアップグレードすることを推奨します。インフラストラクチャとエンドポイントをアップグレードしてマルチウィンドウをサポートしない場合、通話、ビデオ通話、および画面共有は最適化されなくなります。これにより、通話品質の問題、レイテンシーの増加、およびサーバーへの負荷の増加が発生する可能性があります。

次の表は、Citrix VDIでMicrosoft Teamsの最適化された通話を継続して使用するために必要なVDAおよびCitrix Workspaceアプリの最小バージョン、LTSRバージョン、推奨バージョンを示しています。

コンポーネント	最小バージョン (1)	LTSRサポートバージョン (2)	推奨バージョン (3)
マイクロソフト チームズ	1.5.00.11865	該当なし	最新
VDA	1912 CU6 LTSR, 2109 CR, 2203 LTSR	1912 CU8+, 2203 LTSR CU2+ (4)	2308 CR+
Windows版 Citrix Workspaceアプリ	2112.1 CR	2203 CU2+ (4)	2309 CR以降
Mac版 Citrix Workspaceアプリ	2203 CR	該当なし	2308 CR+
Linux向け Citrix Workspace アプリ	2202 CR	該当なし	2308 CR+
ChromeOSまたはHTML5版 Citrix Workspaceアプリ	2303 CR	該当なし	2309 CR以降

注:

1. 最小バージョン: これはマルチウィンドウが最初に導入されたバージョンです。ここに記載されている最小バージョンの一部は、サポート終了となっている場合があります。

2. LTSRサポート対象バージョン: これは、Citrixがマルチウィンドウ向けにサポートしているLTSRバージョンです。これらのLTSRリリースの古いバージョンは動作する可能性がありますが、新しいLTSR CUバージョンがリリースされると、それらのバージョンに対するサポートは利用できなくなります。LTSRサポートポリシーの詳細については、`<https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX205549/faq-citrix-virtual-apps-and-desktops-and-citrix-hypervisor-long-term-service-release-ltsr>`を参照してください。
3. 推奨バージョン: これは、ユーザー/顧客がソフトウェアのアップグレードを選択した場合にCitrixが推奨するソフトウェアのバージョンです。これらはすべてCRバージョンです。
4. VDAおよびCWAベースバージョンのバージョン2203 LTSRには、マルチウィンドウ機能が含まれています。これらのバージョンは、公式にサポートされている最新のCUに置き換えられています。お客様は、これらのサポート対象外のバージョンを自己責任で引き続き使用できます。Citrixは、LTSRリリースをご利用のお客様に最新のCUへのアップグレードを推奨しています。

WebRTCからのSDP形式（プランB）の非推奨のお知らせ

Citrixは、将来のリリースでWebRTCからの現在のSDP形式 (プランB) のサポートを廃止する予定です。最適化されたMicrosoft Teamsの機能に対応するには、WebRTCでUnified Planを使用する必要があります。

影響を受ける製品

Citrix Workspaceアプリケーションの将来のリリースにおいて、Citrix Workspaceアプリの今後のリリースを使用するエンドポイントと、Citrix Workspaceアプリ2108以前のバージョンを使用するエンドポイント間の通話はサポートされません。この通話の非互換性には、1912 LTSR Citrix Workspaceアプリクライアント (CWA) が含まれます。以下のCWAクライアントが影響を受けます。

- Windows向けCitrix Workspaceアプリ
- Linux向け Citrix Workspace アプリ
- Mac向けCitrix Workspaceアプリ
- Chrome向けCitrix Workspaceアプリ

プランBの代替

Citrix Workspaceアプリのバージョン2109より古いバージョンを実行している場合は、サポートされているバージョン（できれば最新のCRリリース）にアップグレードする必要があります。そうしないと、将来のリリースまたは新しいエンドポイントとの通話は接続に失敗します。将来のリリースとフェデレーション通信パートナー間の通話も、フェデレーションパートナーがCitrix Workspaceをアップグレードしていない場合、完了に失敗する可能性があります。

Citrix Workspaceアプリバージョン2108は2023年3月にサポート期限が終了しており、新しいバージョンにアップグレードする必要があります。詳細については、Citrix Workspaceアプリのバージョンサポートに関するWorkspace Appを参照してください。

プランBの廃止に関する詳細については、WebRTCドキュメントを参照してください。

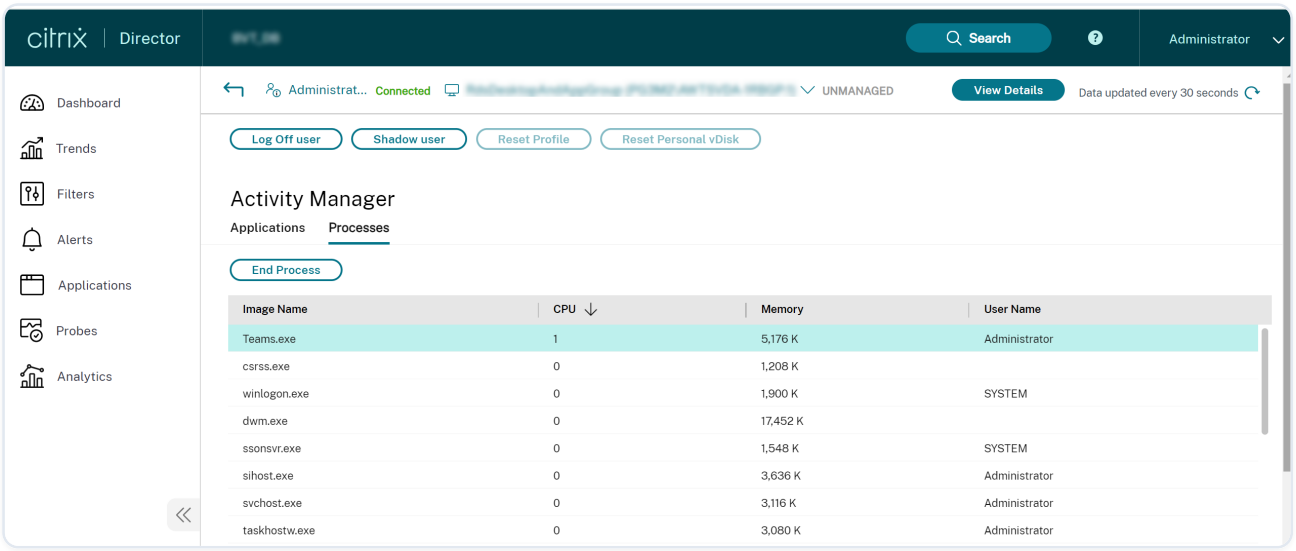
追加情報

- Microsoft Teams の監視、トラブルシューティング、サポート
- VM への Microsoft Teams デスクトップアプリの展開
- MSI を使用した Microsoft Teams のインストール (VDI インストールセクション)
- シンクライアント
- Skype for Business ネットワーク評価ツール
- Microsoft Teams と Skype for Business の共存と相互運用性を理解する

Microsoft Teamsの監視、トラブルシューティング、サポート

Teamsの監視

このセクションでは、HDXによるMicrosoft Teamsの最適化を監視するためのガイドラインを提供します。 最適化モードで実行中で、`HdxRtcEngine.exe`がクライアントマシンで実行されている場合、VDA上の`WebSocketAgent.exe`というプロセスがセッションで実行されています。Directorの**アクティビティマネージャー**を使用してアプリケーションを確認します。



Microsoft Teamsの最適化ステータスは、Director > **ユーザー詳細**ページ > **セッション詳細**パネル > **MS Teams最適化**フィールドで確認できます。Microsoft Teamsが最適化されていることは、クリアなオーディオやビデオなど、より良いユーザーエクスペリエンスのために重要です。この機能はVDAバージョン2311以降で利用可能です。サポートされているCitrix Workspace™アプリのバージョンは、「Microsoft Teamsの最適化」に記載されています。Directorは、Microsoft Teamsが公開アプリケーションとして、または公開デスクトップ内で実行されている場合にのみ、Microsoft Teamsの最適化ステータスを表示します。 詳しくは、「Microsoft Teamsの最適化ステータス」を参照してください。

VDAの最小バージョン1912では、Citrix HDX Monitor（最小バージョン3.11）を使用してアクティブなTeams通話を監視できます。Citrix Virtual Apps and Desktops製品ISOには、フォルダー `layout\image-full\Support\HDX Monitor` に最新の `hdxmonitor.msi` が含まれています。VDAの最小バージョン1912では、Citrix HDX Monitor（最小バージョン3.11）を使用してアクティブなMicrosoft Teams通話を監視できます。Citrix Virtual Apps and Desktops製品ISOには、フォルダー `layout\image-full\Support\HDX Monitor` に最新の `hdxmonitor.msi` が含まれています。

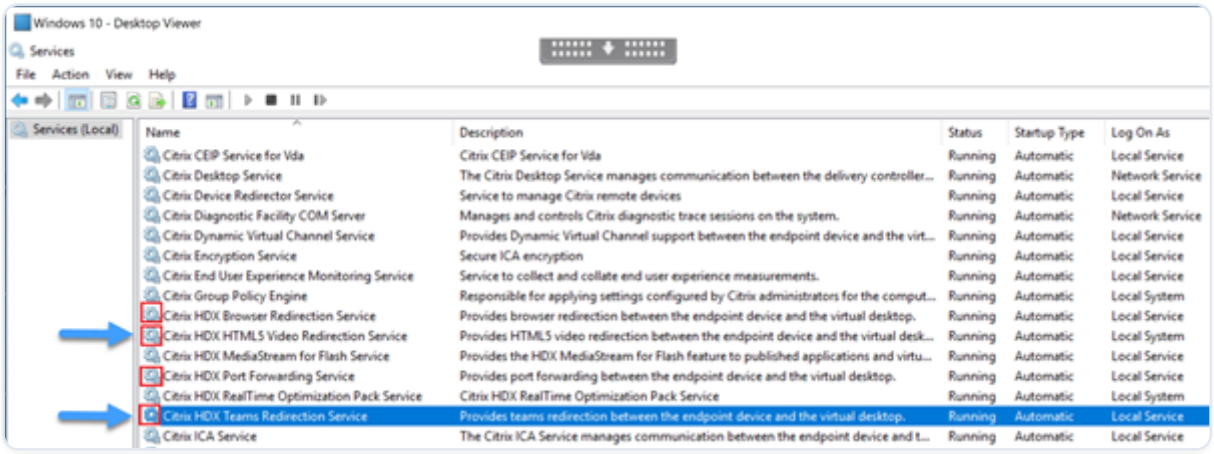
詳しくは、Knowledge Centerの記事「CTX253754」の「*監視*」を参照してください。

トラブルシューティング

このセクションでは、Microsoft Teamsの最適化を使用する際に発生する可能性のある問題のトラブルシューティングのヒントを提供します。詳しくは、「CTX253754」を参照してください。

バーチャル デリバリー エージェント上で

BCR_x64.msiによって4つのサービスがインストールされます。このうち2つだけがVDAでのMicrosoft Teamsリダイレクトを担当します。



- **Citrix HDX Teams Redirection Service**は、Microsoft Teamsで使用される仮想チャネルを確立します。このサービスはCtxSvcHost.exeに依存しています。
- **Citrix HDX HTML5 Video Redirection Service**は、WebSocketService.exeとして実行され、127.0.0.1:9002 TCPでリッスンします。WebSocketService.exeは主に2つの機能を実行します。

  i. **セキュア WebSocket の TLS 終端**は、Microsoft Teams アプリ内のコンポーネントである vdiCitrixPeerConnection.js からセキュア WebSocket 接続を受信します。これは Process Monitor で追跡できます。

  一部のアンチウイルスソフトウェアやデスクトップセキュリティソフトウェアは、`WebSocketService.exe`とその証明書の適切な機能に干渉します。Citrix HDX HTML5 Video Redirectionサービスが`services.msc`コンソールで実行されている場合でも、netstatで確認すると、localhost `127.0.0.1:9002` TCPソケットはリッスンモードになりません。サービスを再起動しようとすると、ハングアップします（「停止中...」）。`WebSocketService.exe`プロセスに適切な除外を適用してください。

  「プロセスモニター」(/en-us/citrix-virtual-apps-desktops/current-release/media/team-process-monitor.png)

  ii. **ユーザーセッションマッピング。** Microsoft Teamsアプリケーションが起動すると、WebSocketService.exeはVDAのユーザーセッションでWebSocketAgent.exeプロセスを開始します。WebSocketService.exeはLocalSystemアカウントとしてセッション0で実行されます。

  「WebSocketAgent.exeサービス」(/en-us/citrix-virtual-apps-desktops/current-release/media/websocketservice-websocketagent.png)

  VDAでWebSocketService.exeサービスがアクティブなリッスン状態にあるかどうかを確認するには、`netstat`を使用できます。

  昇格されたコマンドプロンプトウィンドウから`netstat -anob -p tcp`を実行します。

「netstatの例を実行」(/en-us/citrix-virtual-apps-desktops/current-release/media/teams-netstat.png)

接続が成功すると、状態はESTABLISHEDに変わります。

「netstatの成功例」(/en-us/citrix-virtual-apps-desktops/current-release/media/teams-netstat-success.png)

重要:

WebSocketService.exeは、2つのTCPソケット（127.0.0.1:9001と127.0.0.1:9002）でリッスンします。ポート9001は、ブラウザコンテンツリダイレクトとHTML5ビデオのリダイレクトに使用されます。ポート9002は、Microsoft Teamsのリダイレクトに使用されます。Teams.exeとWebSocketService.exe間の直接通信を妨げる可能性のあるプロキシ構成がVDAのWindows OSにないことを確認してください。Internet Explorer 11で明示的なプロキシ（**インターネットオプション > 接続 > LANの設定 > プロキシサーバー**）を構成すると、接続が割り当てられたプロキシサーバーを経由する場合があります。手動および明示的なプロキシ設定を使用する場合は、**ローカルアドレスにはプロキシサーバーを使用しない**がチェックされていることを確認してください。

サービスの位置と説明

サービス	WINDOWS SERVER OSの実行可能ファイルへのパス	ログオンアカウント	説明
Citrix HTML5ビデオリダイレクトサービス	"C:\Program Files (x86)\Citrix\System32\WebSocketService.exe" /service	ローカルシステムアカウント	仮想デスクトップとエンドポイントデバイス間でメディアリダイレクトを実行するために必要な初期フレームワークを、複数のHDXマルチメディアサービスに提供します。
Citrix HDXブラウザリダイレクトサービス	"C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g BrowserRedirSvcs	このアカウント（ローカルサービス）	エンドポイントデバイスと仮想デスクトップ間でブラウザ

サービス	WINDOWS SERVER OSの実行可能ファイルへのパス	ログオンアカウント	説明
			コンテンツリダイレクトを提供します。
Citrixポート転送サービス	"C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g PortFwdSvcs	このアカウント（ローカルサービス）	ブラウザコンテンツリダイレクトのために、エンドポイントデバイスと仮想デスクトップ間でポート転送を提供します。
Citrix HDX Teamsリダイレクトサービス	"C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g TeamsSvcs	ローカルシステムアカウント	エンドポイントデバイスと仮想デスクトップ間でMicrosoft Teamsリダイレクトを提供します。

Citrix Workspaceアプリ

ユーザーのエンドポイントでは、Windows用Citrix WorkspaceアプリがHdxTeams.exeまたはHdxRtcEngine.exeという新しいサービスをインスタンス化します。これは、VDAでMicrosoft Teamsが起動し、ユーザーがセルフプレビューで通話しようとしたり、周辺機器にアクセスしようとしたりするときに行われます。このサービスが表示されない場合は、以下を確認してください。

1. Windows 用 Workspace アプリ バージョン 1905 以降がインストールされていることを確認します。Workspace アプリのインストールパスに HdxTeams.exe または HdxRtcEngine.exe と webrpc.dll バイナリが表示されますか？
2. 手順1を確認したら、HdxTeams.exe または HdxRtcEngine.exe が起動しているかどうかを確認するために、次の操作を行います。
    a. VDA 上の Microsoft Teams を終了します。
    b. VDA で services.msc を起動します。
    c. Citrix HDX Teams Redirection Service を停止します。
    d. ICA® セッションを切断します。
    e. ICA セッションを接続します。
    f. Citrix HDX Teams Redirection Service を開始します。
    g. Citrix HDX HTML5 Video Redirection Service を再起動します。

h. VDA 上で Microsoft Teams を起動します。

3. クライアントエンドポイントで HdxTeams.exe または HdxRtcEngine.exe が起動しない場合は、次の操作を行います。

   a. VDA を再起動します。

   b. クライアントエンドポイントを再起動します。

サポート

Citrix と Microsoft は、Microsoft Teams の最適化を使用して、Citrix Virtual Apps and Desktops™ からの Microsoft Teams の配信を共同でサポートしています。この共同サポートは、両社の緊密な連携の成果です。有効なサポート契約があり、このソリューションで問題が発生した場合は、問題の原因となっていると思われるコードのベンダーにサポートチケットをオープンしてください。つまり、Teams の場合は Microsoft、最適化コンポーネントの場合は Citrix です。 Citrix または Microsoft がチケットを受け取り、問題をトリアージし、必要に応じてエスカレートします。各社のサポートチームに連絡する必要はありません。

問題が発生した場合は、Teams UI で **>** をクリックすることをお勧めします。VDA 側のログは、技術的な問題をより迅速に解決するために、Citrix と Microsoft の間で自動的に共有されます。

ログの収集

HDXメディアエンジンログはユーザーのマシン上（VDA上ではない）にあります。問題が発生した場合は、サポートケースにログを添付してください。

Windowsログ：

Windowsログは、**HDXTeams**フォルダー内の%TEMP%にあります（AppData/Local/Temp/HDXTeamsまたはAppData/Local/Temp/HdxRtcEngine）。webrpc_Day_Month_timestamp_Year.txtという名前の.txtファイルを探してください。Citrix Workspaceアプリの新しいバージョン（Citrix Workspaceアプリ2009.5以降など）を使用している場合は、ログをAppData\Local\Temp\HdxRtcEngineに保存します。

各セッションはログ用の個別のフォルダーを作成します。

Macログ：

1. VDWEBRTCログ - 仮想チャネルの実行を記録します。

   場所：`/Users/<User Name>/Library/Logs/Citrix Workspace/CitrixViewer_<Y_M_D_H_M_S>.txt`

2. HdxRtcEngineログ - HdxRtcEngine上のプロセスの実行を記録します。

場所: `$TMPDIR/hdxrtcengine/<W_M_D_H_M_S_Y>/hdxrtcengine.log`

HdxRtcEngineログはデフォルトで有効になっています。

3. Webrpcログ - webrtcライブラリのラップアップの実行を記録する最も重要なログです。

場所: `/Users/<USERNAME>/Library/Logs/HdxRtcEngine/<W_M_D_H_M_S_Y>/webrpc.log`

Linuxログ：

Linuxログは`/tmp/webrpc/<current date>/ and /tmp/hdxrtcengine/<current date>/`フォルダーにあります。 Webrtcログ：`/tmp/webrpc/<current date>/webrtc.log` カーネルログ：`/var/log/syslog`

ICE/STUN/TURN/ログ：

通話を確立する際には、次の4つのICEフェーズが必要です。

- 候補収集
- 候補交換
- 接続チェック (STUNバインド要求)
- 候補昇格

HdxRtcEngine.exeログでは、以下のエントリが関連するInteractive Connectivity Establishment (ICE) エントリです。これらのエントリは、通話設定が成功するために必要です。収集段階のサンプルスニペットを以下に示します。

```
RPCStubs Info: -> device id = \\?
\display#int3470#4&1835d135&0&uid13424#{65e8773d-8f56-11d0-
a3b9-00a0c9223196}\{bf89b5a5-61f7-4127-a279-e187013d7caf} label =
Microsoft Camera Front groupId =



webrtcapi.RTCPeerConnection Info: createOffer. audio = 1 video = 1

webrtcapi.RTCPeerConnection Info: setLocalDescription.

>>> begin:sdp

[…]
```

```
webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
HaveLocalOffer



webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state = Gathering



[…]

>>> begin:sdp

candidate:840548147 1 udp 2122194687 10.108.124.215 56927 typ host
generation 0 ufrag oVk6 network-id 1

<<< end:sdp

[…]

>>> begin:sdp

candidate:1938109490 1 udp 24911871 52.114.xxx.xxx 52786 typ relay raddr
73.205.xxx.x rport 25651 generation 0 ufrag dDML network-id 1 network-cost
10

<<< end:sdp

[…]

>>> begin:sdp

candidate:4271145120 1 udp 1685987071 66.xxx.xxx.xxx 55839 typ srflx raddr
10.108.124.215 rport 55839 generation 0 ufrag uAVH network-id 1

<<< end:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state = Complete
webrtcapi.RTCPeerConnection Info: setRemoteDescription.
```

```
>>> begin:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
HaveRemotelOffer
```

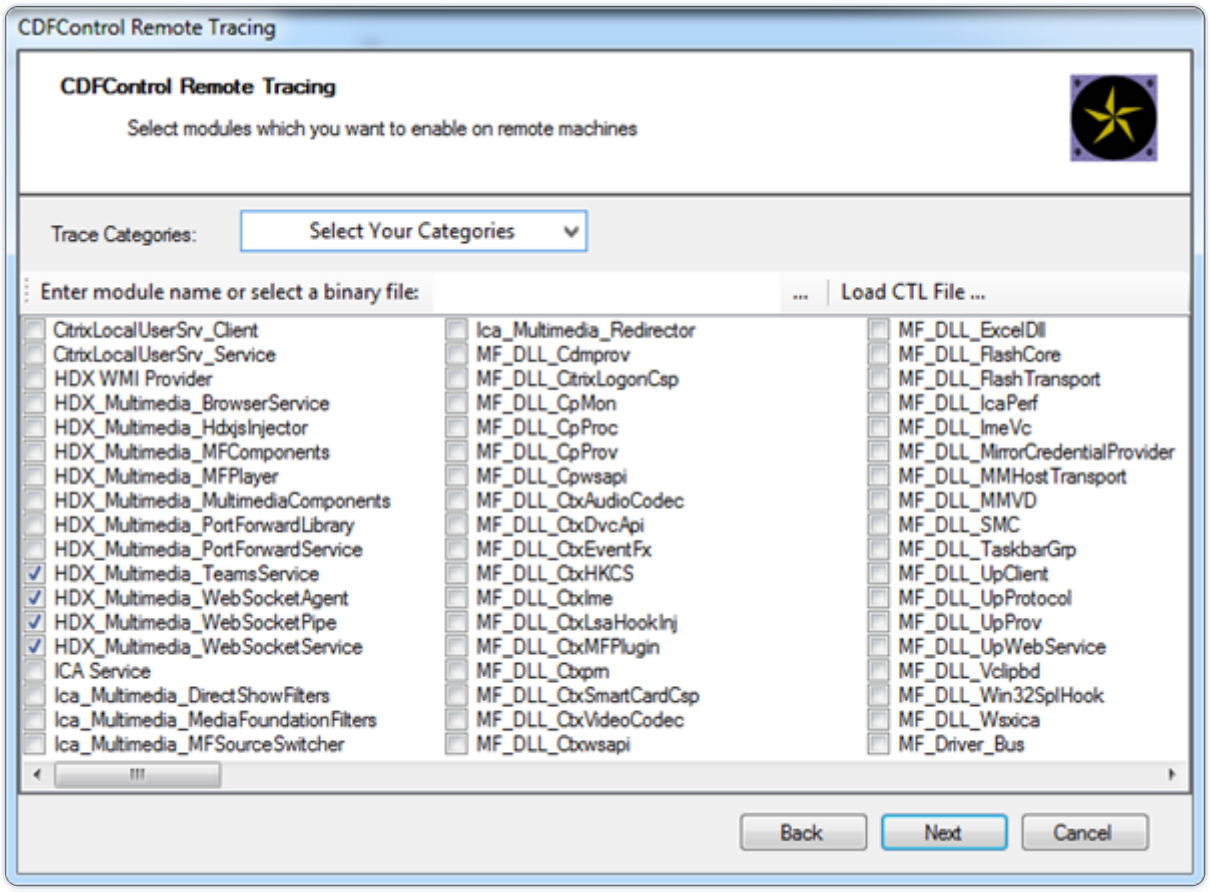
複数のICE候補がある場合、優先順位は次のとおりです。

1. ホスト
2. ピア反射型
3. サーバー反射型
4. トランスポートリレー

問題が発生し、それを一貫して再現できる場合は、Microsoft Teamsで**ヘルプ > 問題の報告**をクリックすることをお勧めします。Microsoftにケースをオープンした場合、技術的な問題を解決するためにログがCitrixとMicrosoftの間で共有されます。 Citrixサポートに連絡する前にCDFトレースをキャプチャすることも有益です。詳細については、Knowledge Centerの記事CDFcontrolを参照してください。

CDFトレース収集の推奨事項については、Knowledge Centerの記事Recommendations for Collecting the CDF Tracesを参照してください。

VDA側CDFトレース - 次のCDFトレースプロバイダーを有効にします。



Workspaceアプリ側CDFトレース - 次のCDFトレースプロバイダーを有効にします。

Workspace App 側の CDF トレース(/en-us/citrix-virtual-apps-desktops/current-release/media/team-cwa-cdf-traces.png)

- IcaClient_DriversVd_TeamsRedir (オプション)
- IcaClient_Multimedia_HdxTeams (Citrix Workspace app 2012 以降が必要)

Windows Media リダイレクト

Windows Media リダイレクトは、サーバーがストリーミングオーディオとビデオをユーザーに配信する方法を制御し、最適化します。メディアのランタイムファイルをサーバーではなくクライアントデバイスで再生することで、Windows Media リダイレクトは、マルチメディアファイルの再生に必要な帯域幅を削減します。Windows Media リダイレクトは、仮想Windowsデスクトップで実行されているWindows Media Playerおよび互換性のあるプレーヤーのパフォーマンスを向上させます。

Windows Media クライアント側コンテンツフェッチの要件が満たされない場合、メディア配信は自動的にサーバー側フェッチを使用します。この方法はユーザーには透過的です。使用されている方法を特定するには、Citrix Scoutを使用してHostMMTransport.dllからCitrix Diagnosis Facility

(CDF) トレースを実行できます。詳しくは、「Citrix Scout」(/ja-jp/citrix-virtual-apps-desktops/current-release/manage-deployment/cis/scout.html)を参照してください。

Windows Media リダイレクトは、ホストサーバーでメディアパイプラインをインターセプトし、メディアデータをネイティブの圧縮形式でキャプチャし、コンテンツをクライアントデバイスにリダイレクトします。クライアントデバイスは、ホストサーバーから受信したメディアデータを解凍してレンダリングするために、メディアパイプラインを再構築します。Windows Media リダイレクトは、Windowsオペレーティングシステムを実行しているクライアントデバイスでうまく機能します。これらのデバイスには、ホストサーバーに存在していたメディアパイプラインを再構築するために必要なマルチメディアフレームワークがあります。Linuxクライアントは、同様のオープンソースメディアフレームワークを使用してメディアパイプラインを再構築します。

ポリシー設定の**Windows Media リダイレクト**は、この機能を制御し、デフォルトで**許可**されています。通常、この設定により、サーバーからレンダリングされるオーディオおよびビデオの品質が、クライアントデバイスでローカルに再生されるコンテンツに匹敵するレベルに向上します。まれに、Windows Media リダイレクトを使用して再生されるメディアが、基本的なICA®圧縮と通常のオーディオを使用してレンダリングされるメディアよりも悪く見えることがあります。この機能を無効にするには、**Windows Media リダイレクト**設定をポリシーに追加し、その値を**禁止**に設定します。

ポリシー設定について詳しくは、「マルチメディアポリシー設定」(/ja-jp/citrix-virtual-apps-desktops/current-release/policies/reference/ica-policy-settings/multimedia-policy-settings.html)を参照してください。

リダイレクトされたコンテンツをスクリーンショットでキャプチャする

Windows Media リダイレクトはエンドポイントでメディアをレンダリングするため、標準のセッション内スクリーンショットツールではリダイレクトされたビデオが空白領域としてキャプチャされます。スクリーンショットにこのコンテンツを含めるには、Citrix Snipping Toolを使用します。Citrixでは、Citrix Virtual Desktop Assistantから起動して見つけやすくすることをお勧めします。詳しくは、「Citrix Virtual Desktop Assistantのドキュメント」(/ja-jp/citrix-virtual-apps-desktops/current-release/manage-deployment/assistant-app.html#tools-page)を参照してください。

制限事項

セッション内でWindows Media PlayerとRemote Audio & Video Extensions (RAVE) を有効にしている場合、黒い画面が表示されることがあります。この黒い画面は、ビデオコンテンツを右クリックして**常に「再生中」を最前面に表示**を選択した場合に表示されることがあります。

仮想チャネルプラグインマネージャー

はじめに

仮想チャネルプラグインマネージャーは、指定されたアプリケーション向けにクライアントエンドポイント全体にプラグインを展開するように設計されています。プラグインマネージャーは、VDAで実行されている特定のアプリケーションを検出し、アプリケーションの実行時に最高の体験を得るために、エンドポイントにプラグインをインストールするようユーザーに促します。

ユーザーは、プラグインをインストールするか、スキップするか、またはインストールを拒否するかを選択できます。プラグインマネージャーは、管理対象か非管理対象かを問わず、すべてのエンドポイントでプラグインを管理する柔軟性を提供します。

例: Microsoft Teams は新しいアーキテクチャ (SlimCore Optimization) を採用しており、最適化を機能させるにはエンドポイントにプラグインをインストールする必要があります。仮想チャネルプラグインマネージャーは、エンドポイント全体にプラグインを展開できます。詳細については、Teams の新しい VDI ソリューション を参照してください。

システム要件

仮想チャネルプラグインマネージャーの最小要件は次のとおりです。

- 仮想デスクトップエージェント (VDA)
  - 2411 CR
- DDC
  - Cloud 121 リリース
  - 2407 CR
- Citrix Workspace™ アプリ (Citrix Workspace アプリ)
  - Windows 2409 用 Citrix Workspace アプリ
- シトリックス ワークスペース アプリ Mac 2508

> **注:**
>
> この機能は現在、Windowsエンドポイントに適用されます。

サポートされるアプリケーション

- 現在サポートされているアプリケーションは以下のとおりです。
    - Microsoft Teams - Teams の新しい VDI ソリューション を参照してください。

仮想チャネルプラグインマネージャーの概要

機能の理解

Citrix® は、お客様の環境が複雑になる可能性があり、管理対象および管理対象外のエンドポイント全体にプラグインを展開するにはかなりの労力が必要であることを理解しています。この機能は、そのプロセスを簡素化するように設計されています。

この機能には2つのコンポーネントが含まれています。1つはVDA側（検出プロセス）、もう1つはCitrix Workspace™ App側（インストーラープロセス）です。管理者が、ポリシーの有効化、レジストリエントリの作成、監視するアプリケーションの指定など、上記の前提条件を満たすと、次のようになります。

- VDA側の検出プロセスは、エンドユーザーが仮想デスクトップにログオンすると、アプリケーションの起動を監視します
- 検出プロセスはCitrix Workspace App側に通知し、指定されたアプリケーションを最適化するために必要なプラグインをインストールするようユーザーに促します
- ユーザーは画面にプラグインに関する簡単な詳細情報が表示されたポップアップを受け取ります。ユーザーはプラグインをインストールするか、スキップするか、またはインストールしないことを選択できます。
    - ユーザーがインストールプロセスをスキップした場合、そのセッションではポップアップが再度表示されません。インストールプロンプトはセッションの再接続時に表示されます。
    - ユーザーがプラグインをインストールしないことを選択した場合、その選択はユーザープロファイルに記録され、管理者が確認できるようになります。
- ユーザーがプラグインをインストールすることを選択した場合、Citrix Workspace App側がエンドポイントにプラグインをダウンロードしてインストールします。
    - インストールが成功すると、プラグインを有効にするためにセッションを再接続するようユーザーにメッセージが表示されます。ユーザーはすぐに再接続するか、成功メッセージを閉じて後で再接続するかを選択できます。
    - インストールが失敗した場合、ユーザーにはエラーメッセージが表示され、失敗は管理者が確認できるように記録されます。

仮想チャネルプラグインマネージャーの構成

展開

1. Microsoft Teamsリダイレクトポリシーが有効になっているか確認します。詳細については、Microsoft Teamsリダイレクトポリシーを参照してください。

   このポリシーは、監視対象のアプリケーションに関わらず有効にする必要があります。将来、より多くのアプリケーションがサポートされ、Microsoft Teamsの代わりにそれらのアプリケーションを監視したい場合でも、このポリシーは有効にしておく必要があります。このポリシーはデフォルトで有効になっています。

2. 仮想チャネルプラグインマネージャーポリシーを有効にする必要があります。ポリシーを有効にする方法の詳細については、仮想チャネルプラグインマネージャーポリシー設定を参照してください。

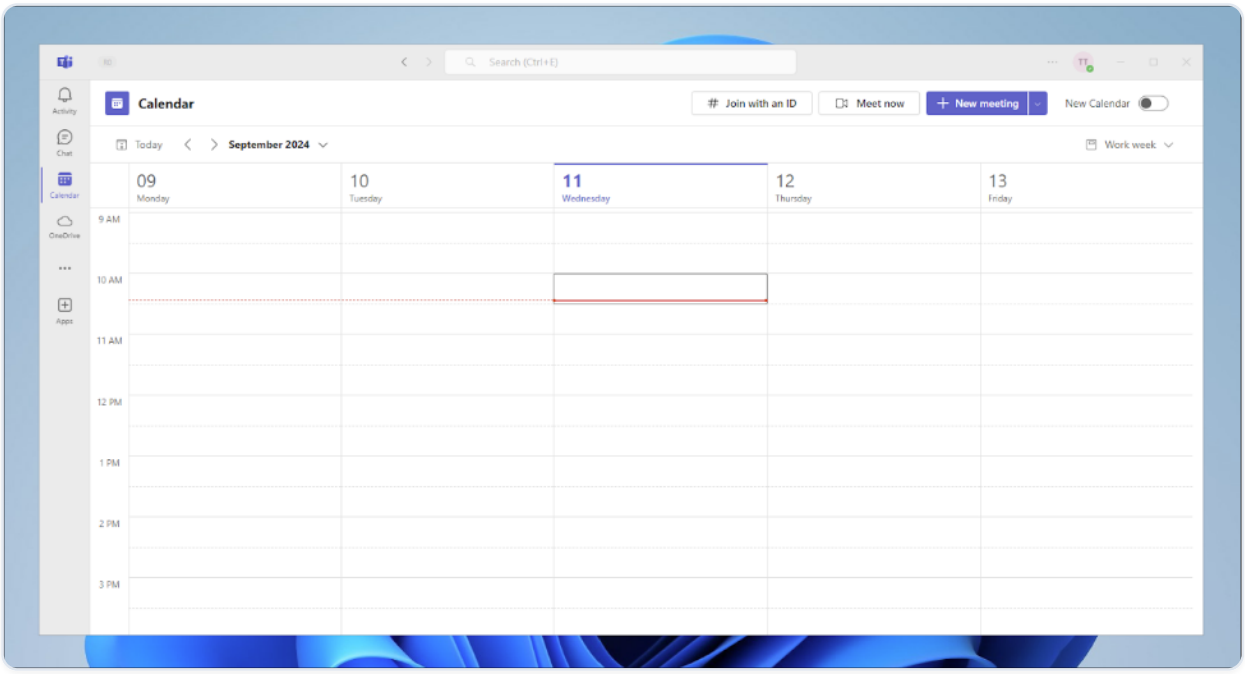
   このポリシーは、Citrix Studioのマルチメディアポリシー設定で利用できます。このポリシーを有効にすると、監視するアプリケーション名（例: 「Microsoft Teams」）を指定できます。このポリシーはデフォルトで無効になっています。

3. Citrix Workspace™アプリはシステムワイドモードでインストールする必要があります。

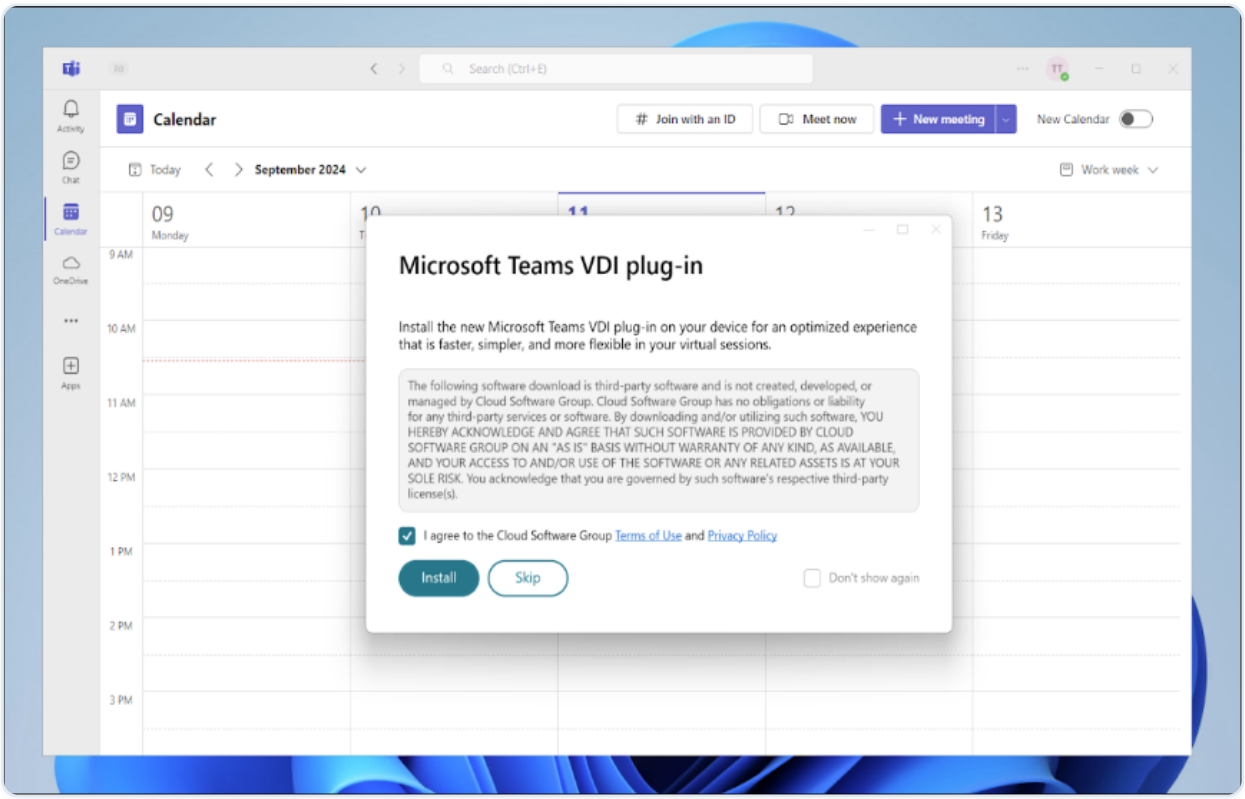
> **注:**
>
> プラグインは、サードパーティのCDNからエンドポイントにダウンロードされます。たとえば、Microsoft Teamsを選択した場合、プラグインはMicrosoft CDNからダウンロードされます。したがって、エンドポイントはサードパーティのCDNにアクセスできる必要があります。そうでない場合、プラグインのインストールは失敗します。

手順

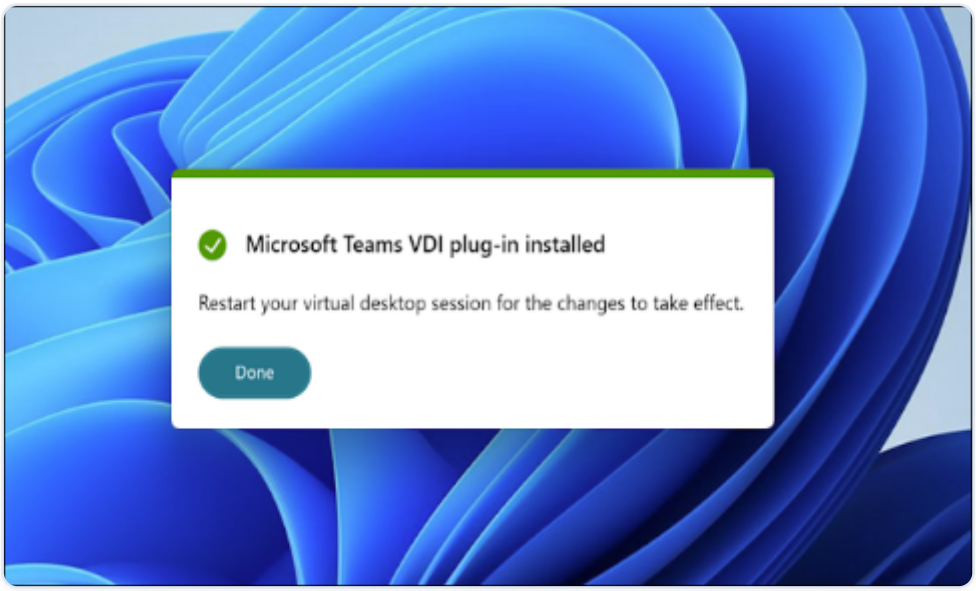
1. ユーザーはCitrixセッションでアプリケーションを起動します。例: Microsoft Teams。



2. ユーザーは、より良いエクスペリエンスのためにエンドポイントにTeams VDIプラグインをインストールするためのポップアップを受け取ります。プラグインはエンドポイントにインストールされるため、ポップアップはセッション内ではなくセッションの上に表示されます。



3. ユーザーがインストールボタンをクリックすると、プラグインがインストールされます。変更を有効にするには、仮想デスクトップセッションを再起動する必要があります。



既知の問題と制限事項

- 2407 VDAでは、機能をアクティブ化するためにポリシーに加えて、以下のレジストリ設定をVDA上で1に設定する必要があります。このレジストリ設定は、2411 VDA以降では自動的に許可され、構成する必要はありません。

  `HKLM\SOFTWARE\Citrix\HDXMediaStream

  Name: EnableAppDetector Type: DWORD`
- 今後、制限事項が追加される予定です

ユニファイドコミュニケーションSDKの最適化

はじめに

Citrix Virtual Apps and Desktopsを使用すると、さまざまなエンドポイントデバイス上のユーザーにアプリケーションを配信できます。これらのアプリケーションの多くには、音声会議やビデオ会議などのリアルタイム通信 (RTC) 機能が含まれています。しかし、仮想化環境でこれらのアプリケーションを配信する際には課題が生じることがあります。従来の配信方法では、メディアストリーム (オーディオ/ビデオ) をクライアントデバイスからデータセンター内のVDIサーバーにルーティングし、その後エンドポイントに送り返します。この「ヘアピン化」は、特に帯域幅を大量に消費するオーディオおよびビデオ通話において、サーバーに不要なトラフィックと処理オーバーヘッドをもたらします。

Citrix Unified Communications SDK (UCSDK) は、テクノロジーベンダーがこれらのRTCアプリケーションをCitrix環境で使用するために最適化できるようにするテクノロジーです。アプリケーションが最適化されると、ローカルデスクトップで実行されているアプリケーションと同等か、

それ以上のユーザーエクスペリエンスを提供できます。今日の世の中では、シームレスなリアルタイム通信は生産性とコラボレーションに不可欠です。仮想環境内でアプリケーションを使用する場合、音声通話やビデオ通話、画面共有、その他の通信機能がローカルデスクトップと同じくらいスムーズに動作することが重要です。最適化されたアプリケーションは、このエクスペリエンスを提供します。

この製品ドキュメントでは、Citrixのお客様がUCSDK最適化アプリケーションを学習し、展開するために必要なすべてを詳しく説明します。

動作の仕組み

Citrixは、VDI内のリアルタイム通信アプリケーション向けに最適化された配信方法を提供しています。このアプローチでは、Unified Communications SDK (UCSDK) を活用して、仮想化されたアプリケーションを次の2つの部分に分割します。

- **ユーザーインターフェイス (UI):** ユーザーインターフェイスは仮想ホスト内に残り、仮想デスクトップまたはアプリケーションウィンドウ内にシームレスに表示されます。
- **メディアエンジン:** メディア処理タスク (オーディオとビデオのエンコード/デコード) は、ユーザーのローカルデバイスにオフロードされます。これにより、サーバーの負荷が最小限に抑えられ、ネットワーク使用量が最適化されます。

通常、Citrixはリアルタイム通信分野のテクノロジーベンダーにUCSDKを提供し、それらのアプリケーションにUCSDKを統合するために協力しています。統合されると、UCSDK最適化アプリケーションを使用するCitrixのお客様は、強化されたエクスペリエンスを得ることができます。Citrix UCSDKは、カスタムの社内アプリケーションが構築されている場合にも、Citrixのお客様が利用できます。ただし、ほとんどの場合、お客様はUCSDKを利用して開発する必要はなく、最適化されたエクスペリエンスを実現するためにCitrix環境とアプリケーションを構成するだけで済みます。

> **注:**
>
> Citrix WebRTC SDK (または) HDX™最適化アプリケーションへの言及は、Citrix UCSDKとの統合を示しており、互換的に使用できます。

主な利点

Citrix UCSDKで最適化されたアプリケーションを使用する場合、次のことが期待できます。

- プロセッサ負荷の高いメディアエンコード/デコードをCitrix Virtual Delivery Agent (VDA) からクライアントエンドポイントにオフロードすることで、メディア処理パフォーマンスが向上し、エンドユーザーの全体的な応答性が高まります。
- Citrix VDAでのCPUおよび帯域幅使用量が削減され、IT部門はホストあたりの同時ユーザー数を増やし、企業はCitrix仮想デスクトップの展開を費用対効果の高い方法で拡張できます。
- 最適化されたエンドポイントがレガシー仮想デスクトップの寿命を延ばし、ホストインフラストラクチャの必要性を減らすため、企業の総所有コストが削減され、時間の経過とともに設備投資と運用コストが削減されます。
- Windows、Mac、Linux、ChromeOS、およびHTML5エンドポイントプラットフォームのサポート。

ユースケース

UCSDKは、WebRTC標準に準拠したリアルタイム通信アプリケーションを最適化するために特別に構築されています。以下に、UCSDKを使用できる/すでに使用しているWebRTCベースのアプリケーションの主要なシナリオと種類を示します。

- **サービスとしてのコンタクトセンター (CCaaS) / クラウドコンタクトセンタープラットフォーム:** 主に複数のチャネルにわたる顧客とのやり取りを管理し、エージェントのワークフローを最適化します。
    - 例: アマゾン コネクト、トゥイリオ、アバイア エクスペリエンス プラットフォーム、トークデスク、コンテンツ グル
- **サービスとしてのユニファイドコミュニケーション (UCaaS) / クラウドビジネスコミュニケーション:** 音声、ビデオ、チームメッセージング、プレゼンスを統合し、包括的なビジネスコミュニケーションを実現します。
    - 例: リング セントラル、8x8、インターメディア、アルカテル・ルーセント レインボー
- **サービスとしてのコミュニケーションプラットフォーム (CPaaS):** リアルタイム通信機能をカスタムアプリケーションに直接組み込むためのAPIを提供します。
    - 例: トゥイリオ、リボン コミュニケーションズ
- **エンタープライズビデオ会議およびコラボレーション:** 高品質なビデオ会議、カンファレンス、高度なコラボレーション機能のための専用プラットフォームです。
    - 例: Pexip

- **金融取引通信:** 金融市場の独自の、高性能でコンプライアンスに準拠した通信ニーズのために設計されています。
    - 例: IPC Unigy
- **仮想学習およびトレーニングプラットフォーム:** インタラクティブで高品質な仮想教室およびトレーニング体験のために設計されています。
    - 例: ヴィテロ

Citrix UCSDKの基盤となるWebRTCは、その最適化機能がWebRTCベースのあらゆる通信アプリケーションに拡張できることを意味します。これにより、現在UCSDKで最適化されているとリストされていないアプリケーションであっても、リアルタイムインタラクションにWebRTCを利用する幅広いアプリケーションを最適化する道が開かれます。お客様には、最適化を希望するユースケースやアプリケーションについてCitrixにお問い合わせいただくことをお勧めします。

UCSDK アーキテクチャ

UCSDK アーキテクチャ (/en-us/citrix-virtual-apps-desktops/current-release/media/ucsdk-architecture.png)

- ベンダーアプリケーション: これは、UCSDK を統合した、デスクトップベースまたはブラウザベースのサードパーティ製リアルタイム通信アプリケーションです。
- UCSDK JS: UCSDK JS は、ベンダーアプリケーションがオーディオ/ビデオをエンドポイントにオフロードするために利用する API を提供します。
- HdxRtcEngine: これは、Citrix Workspace アプリに組み込まれている WebRTC メディアエンジンで、オフロードされたオーディオ/ビデオ通話を処理および管理します。

SDK がロードされて使用されると、リダイレクトが成功した場合、クライアントエンドポイントで `HdxRtcEngine.exe` プロセスが起動されます。クライアントエンドポイントで `HdxRtcEngine.exe` が起動されると、すべてのシグナリングおよびペイロードデータは Citrix VDA からクライアントエンドポイントに流れ、クラウドに到達し、クライアントエンドポイントに戻ってから VDA に転送されます。たとえば、フローの完全な往復は次のようになります。

`Vendor App -> CitrxWebrtc.js SDK -> Citrix VDA components -> Citrix Client Endpoint components -> Cloud -> Citrix Client Endpoint components -> Citrix VDA components -> CitrxWebrtc.js SDK -> Vendor App`

システム要件

システム要件は、UCSDK の最新バージョン (5.0.0) で必要となる Citrix コンポーネントのさまざまなバージョンを示しています。SDK の古いバージョンおよび特定の機能要件に関する互換性の詳細については、以下の バージョンと機能マトリックス の表を参照してください。

注:

お客様が UCSDK に追加された機能を使用するには、ベンダーアプリケーションが適切な UCSDK バージョンを統合し、その機能を有効にしていること、および環境で適切な VDA および CWA バージョンを使用していることを確認してください。

完全互換バージョン

完全互換バージョンとは、これらのバージョンの Citrix コンポーネントを UCSDK の最新バージョンと組み合わせて使用することで、お客様が利用可能なすべての機能を活用できることを示します。UCSDK の現在の最新バージョン (5.0.0) の場合、Citrix コンポーネントの完全互換バージョンは以下のとおりです。

- **シトリックス仮想アプリおよびデスクトップ™：** 2603
- **Citrix Workspace アプリ ウィンドウズ:** 2603
- **Citrix Workspaceアプリ Mac:** リリース予定
- **Citrix Workspace アプリ リナックス:** 2603
- **Citrix Workspaceアプリ ChromeOS/HTML5:** リリース予定

注:

UCSDK最適化は、Windows、Mac、Linux、ChromeOS、HTML5のすべてのエンドポイントプラットフォームでサポートされています。上記のリストで特定のEndpoint Platformに「リリース予定」と表示されている場合、それは最新のUCSDK機能と完全に互換性のあるバージョンがまだリリースされていないことを意味します。したがって、お客様は、新しいUCSDKを使用している場合でも、Citrix Workspaceアプリの古いバージョンを使用して既存の機能を継続して使用できます。

構成

UCSDKの機能は、ベンダーが統合したUCSDKのバージョンとベンダーが有効にした機能、Citrix Virtual Apps and Desktops、および使用中のCitrix Workspaceアプリのバージョンの3つの要因に依存します。

Citrix側では、最適化されたアプリケーションが最適化されるように、以下が構成されていることを確認してください。

1. Microsoft Teamsリダイレクトポリシーがオンになっていることを確認します。詳細については、マルチメディアポリシー設定を参照してください。このポリシーはデフォルトでオンになっています。
2. `CitrixWebrtc.js` SDKを利用するサードパーティのElectronまたはブラウザベースのアプリケーションは、デフォルトではサポートされていません。`CtxHdxWebSocketService` (`WebSocketService.exe`) は、許可リストにないアプリケーションからの接続を許可しません。目的のアプリケーションバイナリ実行可能ファイル名をホワイトリストレジストリキーに追加する必要があります。

> **注:**
>
> CVAD 2603以降、Citrix Unified Communications SDK (UCSDK) を使用するアプリケーションの最適化は、**Microsoft Teamsリダイレクト**ポリシーに依存しなくなりました。管理者は、他のUCSDK統合アプリケーションに影響を与えることなく、Microsoft Teamsの最適化を無効にできるようになりました。この分離を使用するには、ベンダーアプリケーションは、CVAD 2603と併せてBootstrapメソッド（UCSDK 4.0で初めて導入）を利用する必要があります。詳細については、Unified Communications SDK documentationを参照してください。

VDA上

- キーパスを作成します: `HKLM\Software\WOW6432Node\Citrix\WebSocketService`
- キー名: `ProcessWhitelist`
- 種類: `MULTISZ`
- キー値: `Mytestapp.exe`

複数のアプリケーションがある場合は、各アプリケーションを新しい行に入力します。テキストファイルからコピー＆ペーストしたり、コンマを挿入したりしないでください。指定された名前

がアプリケーションの実行可能ファイル名と一致していることを確認してください。このレジストリ値は大文字と小文字を区別しません。

アプリケーションが本格的なデスクトップアプリケーションではなくブラウザ経由でアクセスされる場合、レジストリ値で例えば`chrome.exe`を許可する必要があります。

上記のレジストリが正常に構成されたら、VDAを再起動するか、`CtxHdxWebSocketService`を再起動してホワイトリストの設定を完了します。

クライアント上

構成は不要です。Citrix Workspaceアプリをインストールするだけです。

各ベンダーは非常に具体的なアプリケーション名を持っている場合があります。したがって、WebSocketServiceで許可する必要があるアプリケーション名を決定するには、現在のベンダーサポートセクションにリンクされているベンダーのドキュメントを参照してください。

機能リファレンス

リダイレクトされたコンテンツをスクリーンショットでキャプチャする

UCSDK最適化アプリケーションにビデオまたは共有画面オーバーレイが含まれる場合、そのコンテンツはエンドポイントでレンダリングされるため、標準のセッション内スクリーンショットツールでは空白領域としてキャプチャされます。このコンテンツをスクリーンショットに含めるには、Citrix Snipping Toolを使用してください。Citrixでは、見つけやすくするためにCitrix Virtual Desktop Assistantから起動することをお勧めします。詳しくは、Citrix Virtual Desktop Assistantのドキュメントを参照してください。

Smart Syncによる通話接続時間の短縮

UCSDK 5.0.0で導入されたSmart Sync機能は、VDAとクライアントエンドポイント間の通信を効率化することで、通話接続時間を短縮します。この機能強化により、全体的に通話設定が高速化され、特に高遅延ネットワーク環境で最も顕著なパフォーマンス向上が実現されます。

Citrixは、この機能を活用するために、お客様がアプリケーションベンダーに連絡してUCSDK 5.0.0にアップグレードすることを推奨します。

> **注:**

この機能は、UCSDK 5.0.0とCitrix Workspaceアプリのみに依存します。正確なクライアントバージョンについては、バージョンと機能マトリックスを参照してください。VDAのバージョン依存性はないため、以前のサポートされているVDAも引き続き使用できます。

UCSDKとHDX Microsoft Teams最適化の分離

この機能は、Unified Communications SDK (UCSDK) の最適化ロジックをMicrosoft Teamsの最適化ポリシーから分離します。以前は、「Microsoft Teamsリダイレクト」ポリシーがマスター切り替えスイッチとして機能しており、Teamsに対してこれを無効にすると、他のすべてのUCSDKベースのアプリケーションが意図せずサーバー側レンダリングにフォールバックされていました。

この機能強化により、WebRTCリダイレクトに必要な仮想チャネルは、Teamsポリシーの状態に関係なく、サードパーティアプリケーションで引き続き利用可能になります。

- **利点**
  - **きめ細かな制御:** 管理者は、Amazon Connect、Five9、RingCentral、その他のUCSDK統合アプリケーションなどの重要なビジネスアプリケーションの最適化に影響を与えることなく、Microsoft Teamsの最適化ポリシーを選択的に管理できます。
  - **運用安定性:** UCSDK最適化アプリケーションにおける意図しないパフォーマンス低下を防ぐことで、ビジネス継続性を確保します。管理者は、主要なビジネスツールの高精細オーディオ/ビデオエクスペリエンスを損なうことなく、トラブルシューティングやコンプライアンス上の理由でHDX Teams最適化を無効にできます。
- **要件**
  - **VDA要件:** Citrix Virtual Apps/Desktops 2603以降
  - **アプリケーションの互換性:** サードパーティ製アプリケーションは、UCSDKブートストラップ初期化メソッドを利用する必要があります

注:

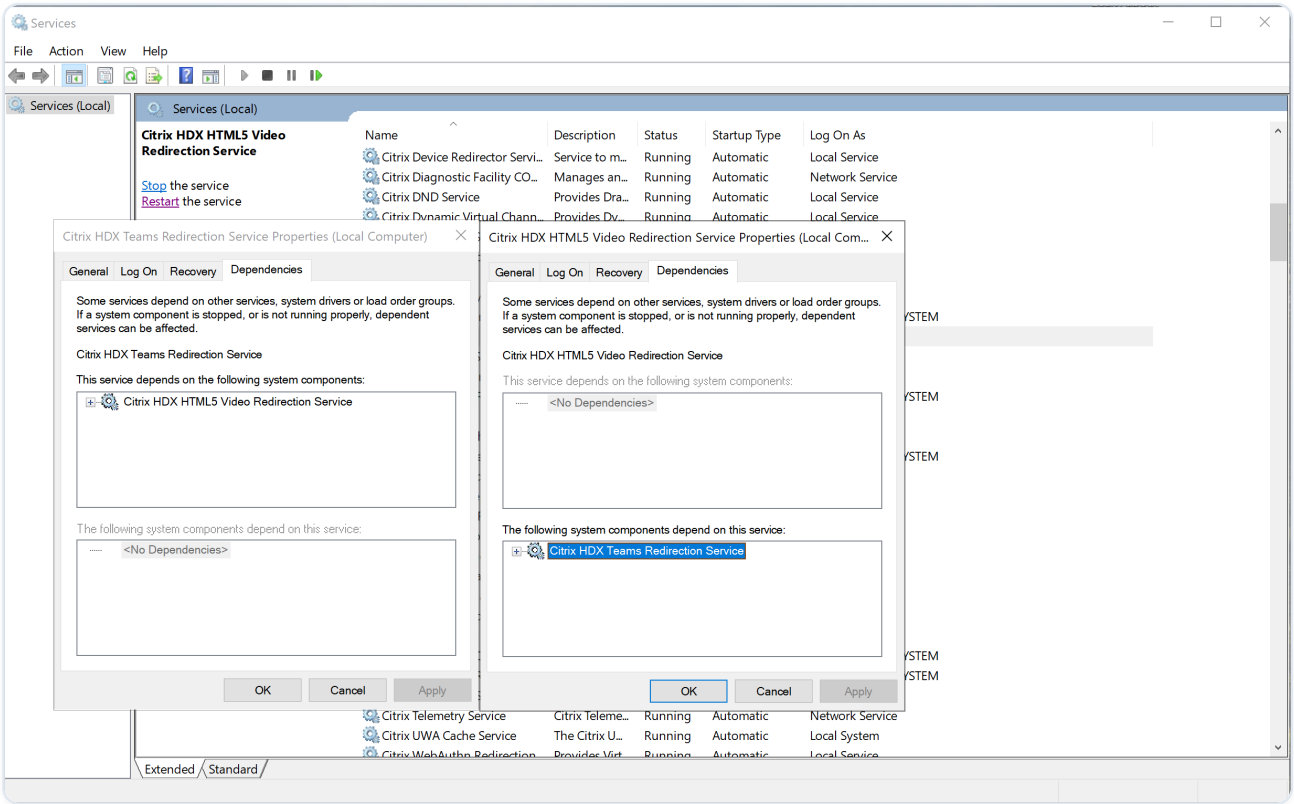
- この機能は、Microsoft Teams SlimCore最適化には影響しません。SlimCore最適化は、Microsoft独自の仮想チャネルを使用して独立して動作し、Citrix CTXMTOP仮想チャネルには依存しません。
- この機能を活用するには、サードパーティ製アプリケーションがUCSDK 4.0以降で構築されている必要があります。お客様は、アプリケーションベンダー（例：Amazon

> Connect、Five9、RingCentral）に、特定のバージョンがブートストラップ初期化を使用していることを確認する必要があります。

Microsoft Teams最適化のための明示的なサービス依存関係

Citrix Virtual Apps / Desktops 2603以降、**Citrix HDX Teams Redirection Service**（HDX最適化Microsoft TeamsおよびUCSDK最適化アプリケーションで使用）は、**Citrix HDX HTML5 Video Redirection Service (WebSocketService)**への依存関係を明示的に宣言するようになりました。

このアップデートにより、Teamsサービスが起動する際にHTML5サービスが自動的に検証および開始されるようになり、サービスが厳密に管理されている環境でのMicrosoft TeamsおよびUCSDK統合アプリケーションの最適化の失敗を防ぎます。



パフォーマンスとユーザーエクスペリエンスを向上させるための最適化されたオーバーレイクリッピング

CVAD 2511以降、HDX Microsoft Teams最適化やUCSDK最適化などの機能におけるリダイレクトされたビデオオーバーレイを処理するメカニズムは、ユーザーエクスペリエンスとサーバーパフォーマンスの両方を向上させるために再設計されました。

主な利点

- **視覚的な正確性の向上:** この機能強化により、ポップアップメニューや通知などのアプリケーション要素がビデオコンテンツの背後に誤って表示される視覚的な不具合が解決されます。新しいロジックにより、すべてのコンポーネントが正しい順序でレンダリングされ、よりシームレスで予測可能なエクスペリエンスが提供されます。
- **パフォーマンスの向上:** この最適化により、Virtual Delivery AgentでのCPU使用率が大幅に削減されます。古いリソース集約型のポーリングメソッドをより効率的なグラフィックスベースのアプローチに置き換えることで、この変更はサーバーのスケーラビリティを向上させ、より高いユーザー密度を可能にします。

> **注:**
>
> この機能は、将来のバージョンのMicrosoft Teams（またはその他のUCSDKパートナーアプリケーション）に依存し、Citrix Workspace App for Windows 2511が必要です。

バージョンと機能マトリックス

バージョン更新は頻繁に行われるため、特定のバージョンがサポートされていることを確認するには、Citrix Virtual Apps and DesktopsおよびCitrix Workspace appの製品ライフサイクルページを参照してください。多くの古い機能については、表に記載されているバージョンは、このドキュメントの作成時点での最終サポート対象のCurrent Release (CR) バージョンです。

機能	UCSDK バージョン	VDA	CWA ウィンドウズ	CWA MAC	CWA リナックス	CWA CHROME OS/ HTML5
オーディオ/ビデオ (p2p & 会議)	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新CU / 2311 CR	2311	2311	2312
画面共有	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新CU / 2311 CR	2311	2311	2312
DTMF	3.1.0	2203 LTSR 最	2402 LTSR 最	2311	2311	2312

機能	UCSDK バージョン	VDA	CWA ウィンドウズ	CWA MAC	CWA リナックス	CWA CHROME OS/ HTML5
		新 CU / 2311 CR	新CU / 2311 CR			
プロキシサーバーのサポート	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新CU / 2311 CR	2311	2311	2312
アプリ共有	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新CU / 2311 CR	2311	2311	該当なし
動的e911	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新CU / 2311 CR	2311	2311	2312
マルチウィンドウ	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新CU / 2311 CR	2311	2311	2312
SDP統合プランのサポート	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新CU / 2311 CR	2311	2311	2312
ストリーム解像度 / シマルキャスト	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新CU / 2311 CR	2311	2311	2312
リモートオーディオ (ループあり)	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新CU / 2311 CR	2311	2311	2405

機能	UCSDK バージョン	VDA	CWA ウィンドウズ	CWA MAC	CWA リナックス	CWA CHROME OS/ HTML5
ブラウザベースの UCSDK (ブートストラップサポート)	4.0.2	2407 CR	2402 LTSR 最新CU / 2311 CR	2311	2311	2312
Web HID API	4.0.2	2203 LTSR 最新 CU / 2311 CR	2409.10	2411	2411	2505
ウェブオーディオAPI	4.0.2	2203 LTSR 最新 CU / 2311 CR	2405	2405	2405	該当なし
ICE の再起動	4.1.0	2203 LTSR 最新 CU / 2311 CR	2503.2	2503	2503	2502.10
画面録画 (プレビュー)[1]	4.1.0	2503	2503.2	該当なし	該当なし	該当なし
スマートシンク	5.0.0	2203 LTSR 最新 CU / 2311 CR	2603	該当なし	2604	該当なし

注:

画面録画用の新しいポリシーを導入したため、CVAD 2503に付属するdelivery controller™のバージョン2503が必要です。

現在のベンダーサポート

複数のサードパーティベンダーが、Unified Communications SDKを自社製品に統合しています。ベンダーとそのサポートドキュメントの現在のリストは以下のとおりです。

ベンダー	ドキュメント
スプリンクラー	Citrix 音声通話用メディアオフロード - スプリンクラー
マイクロソフト ダイナミクス 365	Dynamics 365 Contact Center ドキュメント
アマゾンコネクト	Citrix Cloud Desktops 向け Amazon Connect オーディオの最適化
リングセントラル	Citrix VDI 環境での RingCentral の使用
ファイブナイン	Citrix 環境での Five9 WebRTC
トゥイリオ	Citrix VDIにおけるTwilio Flex
アバイア	「Citrix向けAvaya Experience Platform Public Cloud VDIソリューション」(https://documentation.avaya.com/bundle/ExperiencePlatform_Administering_10/page/Avaya__Experience_Platform_VDI_solution_for_Citrix_1.html)
8x8	Citrix VDIとデスクトップおよびウェブ向け8x8 Workの統合
コンテンツ・グル	カンテン・グル Citrix統合
リボン・コミュニケーションズ	リボン・コミュニケーションズ Citrix WebRTC SDK
インターメディア	「Citrix Virtual Apps and DesktopsへのIntermedia Uniteのインストール」(https://support.intermedia.com/app/articles/detail/a_id/24355)
アルカテル・ルーセント・レインボー	「Rainbowデスクトップアプリケーション向けCitrix最適化」(https://help.openrainbow.com/

ベンダー	ドキュメント
	hc/ja-jp/articles/23752823816850-CITRIX-Optimization-for-Rainbow-Desktop-application)
トークデスク	Talkdesk Agent Workspace VDI コネクト
IPC	IPC Unigy ソフトクライアント Citrix VDI
ヴィテロ	Citrix VDI 向けヴィテロ インスパイア
ペクシプ	Citrix Pexip Infinity Docs で Connect デスクトップアプリを展開する
ズーム ウェブアプリ	Zoom Web App の WebRTC リダイレクトを構成する

トラブルシューティング

トラブルシューティング情報については、Citrix Unified Communications SDK で最適化されたアプリのトラブルシューティングガイダンスを参照してください。

既知の問題と制限事項

このセクションでは、現在認識されている既知の問題と制限事項について説明します。

一般的なコンテンツリダイレクト

コンテンツリダイレクトを使用すると、ユーザーがサーバーで公開されているアプリケーションを使用するか、ユーザーデバイスでローカルに実行されているアプリケーションを使用するかによって、情報にアクセスする方法を制御できます。

クライアントフォルダーリダイレクト(/ja-jp/citrix-virtual-apps-desktops/current-release/general-content-redirection/client-folder-redirection.html)

クライアントフォルダーリダイレクトは、クライアント側のファイルがホスト側のセッションでアクセス可能になる方法を変更します。

- サーバーでクライアントドライブマッピングのみを有効にすると、クライアント側のフルボリュームは、Universal Naming Convention (UNC) リンクとしてセッションに自動的にマッピングされます。
- サーバーでクライアントフォルダーリダイレクトを有効にし、ユーザーがWindowsデスクトップデバイスでそれを構成すると、ユーザーが指定したローカルボリュームの一部がリダイレクトされます。

ホストからクライアントへのリダイレクト(/ja-jp/citrix-virtual-apps-desktops/current-release/general-content-redirection/host-to-client-redirection.html)

特定のまれなユースケースでは、ホストからクライアントへのリダイレクトの使用を検討してください。通常、他の形式のコンテンツリダイレクトの方が優れている場合があります。このタイプのリダイレクトは、マルチセッションOS VDAでのみサポートされており、シングルセッションOS VDAではサポートされていません。

ローカルアプリアクセスとURLリダイレクト(/ja-jp/citrix-virtual-apps-desktops/current-release/general-content-redirection/laa-url-redirect.html)

ローカルアプリアクセスは、ローカルにインストールされたWindowsアプリケーションをホストされたデスクトップ環境にシームレスに統合します。これは、あるコンピューターから別のコンピューターに切り替えることなく行われます。

クライアントフォルダーリダイレクト

クライアントフォルダーリダイレクトは、クライアント側のファイルがホスト側のセッションでアクセスされる方法を変更します。サーバーでクライアントドライブマッピングのみを有効にすると、クライアント側の完全なボリュームは、Universal Naming Convention (UNC) リンクとしてセッションに自動的にマッピングされます。サーバーでクライアントフォルダーリダイレクトを有効にし、ユーザーがユーザーデバイスでそれを構成すると、ユーザーが指定したローカルボリュームの一部がリダイレクトされます。

ユーザーが指定したフォルダーのみが、セッション内でUNCリンクとして表示されます。つまり、ユーザーデバイス上の完全なファイルシステムではなく、指定されたフォルダーのみが表示されます。レジストリを介してUNCリンクを無効にすると、クライアントフォルダーはセッション内でマップされたドライブとして表示されます。

クライアントフォルダーリダイレクトは、WindowsシングルセッションOSマシンでのみサポートされています。

外部USBドライブのクライアントフォルダーリダイレクトは、デバイスの取り外しと再接続時に保存されません。

サーバーでクライアントフォルダーリダイレクトを有効にします。次に、クライアントデバイスで、リダイレクトするフォルダーを指定します。クライアントフォルダーオプションを指定するために使用するアプリケーション (CtxCFRUI.exe) は、このリリースで提供されるCitrix Workspaceアプリに含まれています。

要件:

サーバーの場合:

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

クライアントの場合:

- ウィンドウズ 10
- ウィンドウズ 11

サーバーでクライアントフォルダーリダイレクトを有効にするには、レジストリを介して管理される機能のリストにあるクライアントフォルダーリダイレクトを参照してください。

ユーザーデバイスで、リダイレクトするフォルダーを指定します:

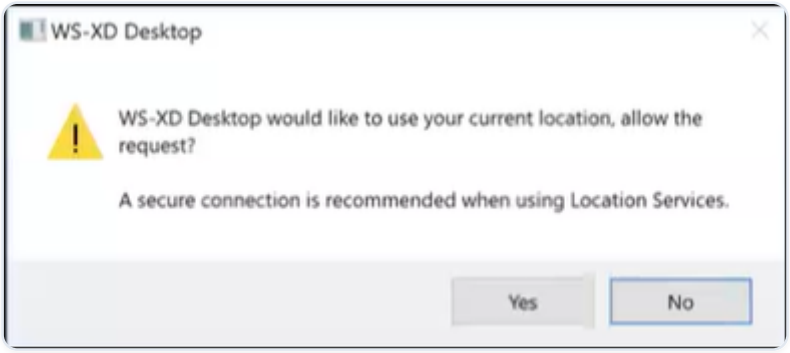
1. Citrix Workspace™アプリの最新バージョンがインストールされていることを確認してください。
2. Citrix Workspaceアプリのインストールディレクトリから、CtxCFRUI.exe **(..\Citrix\ICA Client\CtxCFRUI.exe)** を起動します。
3. **Custom** ラジオボタンを選択し、フォルダーを追加、編集、または削除します。
4. 設定を有効にするには、セッションを切断して再接続します。

クライアント位置情報リダイレクト

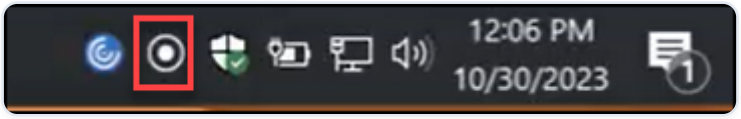
クライアント位置情報リダイレクトを有効にすると、VDAでホストされているアプリとデスクトップセッションが、クライアントの現在の位置情報にシームレスにアクセスできるようになります。マルチセッションオペレーティングシステム（TS VDAまたはマルチセッションWS VDA）では、各セッションは接続されたクライアントによって提供される独自の場所を持ちます。この機能を使用すると、位置情報に依存するVDA上のアプリケーションは、クライアントの正確な位置情報を取得できます。

詳細については、Microsoftドキュメントを参照してください。

クライアント位置情報リダイレクトが有効になり、サーバー側とクライアント側の両方で位置情報へのアクセスが許可されると、位置情報にアクセスするアプリケーションまたはデスクトップを起動したときに、クライアントは次のダイアログボックスで現在の位置情報を共有するように求めます。



クライアント位置情報リダイレクトを有効にすると、VDAでホストされているアプリまたはデスクトップが現在の位置情報を照会したときに、クライアントのタスクバーに次のアイコンが表示されます。



システム要件

サーバーの場合：

- シングルセッション（Win10/11）またはマルチセッション（Win 11 22H2およびServer 2022 23H2以降）OS VDA
- Windows、iOS、またはAndroid用Citrix Workspace™アプリ

構成

この機能が動作するには、Citrix®ポリシーを使用してクライアント位置情報リダイレクトを有効にする必要があります。クライアント位置情報リダイレクトはデフォルトで無効になっています。

クライアント位置情報リダイレクトを有効にするには、次の手順を実行します。

Windows VDAおよびクライアント側で：

1. **設定 > プライバシー > 位置情報**で、次のオプションを有効にします。
    - **このデバイスの位置情報へのアクセスを許可する**
    - **アプリが位置情報にアクセスできるようにする**
    - **デスクトップアプリに位置情報へのアクセスを許可する**
2. マルチセッションOSの場合、**Location Override**設定を有効にします。

Controller/DDC側で:

Studio > ポリシー > 位置情報 > 設定 > アプリケーションがクライアントデバイスの物理的な位置情報を使用することを許可するポリシーを有効にします。 詳細については、クライアントセンサーポリシー設定を参照してください。

双方向コンテンツリダイレクト

双方向コンテンツリダイレクトにより、Webブラウザー内のHTTPまたはHTTPS URL、あるいはアプリケーションに埋め込まれたURLを、Citrix VDAセッションとクライアントエンドポイント間で双方向に転送できます。Citrixセッションで実行されているブラウザーに入力されたURLは、クライアントのデフォルトブラウザーを使用して開くことができます。逆に、クライアントで実行されているブラウザーに入力されたURLは、公開アプリケーションまたはデスクトップのいずれかを使用して、Citrixセッションで開くことができます。双方向コンテンツリダイレクトの一般的なユースケースには、次のようなものがあります。

- 開始ブラウザーがソースへのネットワークアクセスを持たない場合のWeb URLのリダイレクト。
- ブラウザーの互換性およびセキュリティ上の理由によるWeb URLのリダイレクト。
- Citrixセッションまたはクライアントでwebブラウザーを実行したくない場合に、アプリケーションに埋め込まれたWeb URLのリダイレクト。

システム要件

- シングルセッションまたはマルチセッションOS VDA
- Citrix Workspace™ アプリ for Windows 2311 以降
- Citrix Workspace™ アプリ for Linux 2503 以降
- Citrix Workspace™ アプリ for Mac 2607 以降

ブラウザー：

- Citrix ブラウザリダイレクト拡張機能を使用する Google Chrome
  - Google Chrome 拡張機能
- Citrix ブラウザリダイレクト拡張機能を使用する Microsoft Edge
  - Microsoft Edge 拡張機能

構成

Citrix Virtual Apps and Desktops™ バージョン 2311 以降、双方向コンテンツリダイレクトは Citrix Studio を介してのみ構成されます。以前のリリースでは、クライアントエンドポイントと Studio の両方でポリシー設定が構成されていました。双方向コンテンツリダイレクトはデフォルトで無効になっています。

VDA の構成については、**ICA ポリシー**設定の 双方向コンテンツリダイレクト を参照してください。

ブラウザーリダイレクトを機能させるには、表示されているコマンドを使用して、元のブラウザー（URL のリダイレクト元）にブラウザー拡張機能を登録する必要があります。使用しているブラウザーに基づいて、必要に応じて VDA とクライアントでコマンドを実行します。

ブラウザー	VDA	クライアント
グーグル クローム	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /regChrome	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /regChrome
マイクロソフト エッジ	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /regEdge	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /regEdge
利用可能なすべてのブラウザ	コマンド: "%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /regall	コマンド: "%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /regall

ブラウザ拡張機能を登録解除するには：

ブラウザー	VDA	クライアント
グーグル クローム	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /unregChrome	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /unregChrome
マイクロソフト エッジ	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /unregEdge	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /unregEdge
利用可能なすべてのブラウザ	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /unregall	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /unregall

注:

- これらのコマンドを管理者権限でコマンドプロンプト（CMD）ウィンドウで実行します。

- 登録コマンドを実行すると、ChromeおよびEdgeブラウザは、初回起動時にCitrix Browser Redirection Extensionを有効にするようユーザーに促します。
- 登録コマンドは、Browser Redirection Extensionをネイティブメッセージングホストにリンクさせ、拡張機能がネイティブコードと通信できるようにします。これがなければ、ブラウザは通信をブロックします。
- Google Chromeウェブストアからブラウザ拡張機能を手動でインストールすることもできます。Microsoft Edgeアドオンストアから Browser Redirection Extensionを使用するには、Virtual Delivery Agent (VDA) バージョン2503以降が必要です。古いVDAバージョンの場合は、Microsoft Edgeブラウザ内でGoogle Chromeウェブストアから拡張機能をインストールしてください（ChromeウェブストアからMicrosoft Edgeに拡張機能を追加するを参照）。
- システム要件に記載されているCitrix Workspaceアプリのバージョンは、双方向コンテンツリダイレクトとOAuthリダイレクトの両方をサポートするために必要な最小バージョンです。
- Macの場合：公証済みアプリケーションに対するmacOSのセキュリティ要件のため、カスタムOAuthコールバックURLスキームはCitrixに事前登録されている必要があり、インストール後に動的に変更することはできません。デフォルトでは`citrix-oauth-redir`のみがサポートされています。URLスキームを登録するには、Citrix製品チームにお問い合わせください。

Citrix VDAからクライアントへのワイルドカードリダイレクト

双方向コンテンツリダイレクトは、リダイレクトするURLを定義する際にワイルドカードの使用をサポートします。双方向コンテンツリダイレクトを構成するには、構成の手順を参照してください。

VDAからクライアントへのカスタムプロトコルリダイレクト

双方向コンテンツリダイレクトは、Citrix VDAからクライアントへのカスタムプロトコルのリダイレクトをサポートします。HTTPまたはHTTPS以外のプロトコルがサポートされています。双方向コンテンツリダイレクトを構成するには、構成の手順を参照してください。

Web Studioで、**双方向コンテンツリダイレクト**のカスタムプロトコルを設定します。

注:

- これらのコマンドを実行するには、管理者権限が必要です。
- クライアントには、プロトコルを処理するために登録されたアプリケーションが必要です。そうでない場合、URLはクライアントにリダイレクトされますが、起動に失敗します。
- ChromeおよびEdgeブラウザーで入力または起動するカスタムプロトコルURLはサポートされておらず、リダイレクトされません。
- 次のプロトコルはサポートされていません: `rtsp://, rtspu://, pnm://, mms://`。

その他の考慮事項

- ブラウザの要件と構成は、リダイレクトを開始するブラウザにのみ適用されます。リダイレクトが成功した後にURLが開かれる宛先ブラウザは、サポートの対象外です。VDAからクライアントにURLをリダイレクトする場合、サポートされるブラウザ構成はVDA上でのみ必要です。逆に、クライアントからVDAにURLをリダイレクトする場合、サポートされるブラウザ構成はクライアント上でのみ必要です。リダイレクトされたURLは、方向に応じて、クライアントまたはVDAのいずれかの宛先マシンで構成されているデフォルトのブラウザに渡されます。VDAとクライアントで同じブラウザタイプを使用する必要はありません。
- リダイレクトルールがループ構成にならないことを確認してください。たとえば、VDAポリシーが `https://www.citrix.com` をリダイレクトするように設定され、クライアントポリシーが同じURLをリダイレクトするように設定されている場合、無限ループが発生します。
- URL短縮サービスはサポートされていません。
- クライアントからVDAへのリダイレクトには、Windowsクライアントが管理者権限でインストールされている必要があります。
- 宛先ブラウザがすでに開いている場合、リダイレクトされたURLは新しいタブで開きます。そうでない場合、URLは新しいブラウザウィンドウで開きます。
- 双方向コンテンツリダイレクトは、ローカルアプリアクセス (LAA) が有効になっている場合は機能しません。

ホストからクライアントへのリダイレクト

ホストからクライアントへのリダイレクトにより、Citrix®セッションで実行されているアプリケーションにハイパーリンクとして埋め込まれたURLを、ユーザーのエンドポイントデバイス上の対応するアプリケーションを使用して開くことができます。ホストからクライアントへのリダイレクトの一般的なユースケースには、次のようなものがあります。

- Citrixサーバーがソースへのインターネットまたはネットワークアクセスを持たない場合のWebサイトのリダイレクト。
- セキュリティ、パフォーマンス、互換性、またはスケーラビリティの理由から、Citrixセッション内でWebブラウザを実行することが望ましくない場合のWebサイトのリダイレクト。
- URLを開くために必要なアプリケーションがCitrixサーバーにインストールされていない場合の特定のURLタイプのリダイレクト。

ホストからクライアントへのリダイレクトは、Webページでアクセスしたり、Citrixセッションで実行されているWebブラウザのアドレスバーに入力したりするURLを対象としていません。Webブラウザでのリダイレクトについては、「双方向URLリダイレクト」または「ブラウザコンテンツリダイレクト」を参照してください。

システム要件

- マルチセッションOS VDA
- サポートされているクライアント：
  - Windows向けCitrix Workspace™アプリ
  - Mac向けCitrix Workspaceアプリ
  - Linux向け Citrix Workspace アプリ
  - HTML5向けCitrix Workspaceアプリ
  - Chrome向けCitrix Workspaceアプリ

クライアントデバイスには、URLタイプのリダイレクトを処理するためのアプリケーションがインストールされ、構成されている必要があります。

構成

この機能を有効にするには、ホストからクライアントへのリダイレクト Citrixポリシーを使用します。**ホストからクライアントへのリダイレクト**は、デフォルトで無効になっています。ホストからクライアントへのリダイレクトポリシーを有効にすると、Citrix Launcherアプリケーションは Windowsサーバーに登録され、URLをインターセプトしてクライアントデバイスに送信できるようになります。

次に、必要なURLタイプのデフォルトアプリケーションとしてCitrix Launcherを使用するように Windowsグループポリシーを構成する必要があります。CitrixサーバーVDAで、ServerFTAdefaultPolicy.xmlファイルを作成し、次のXMLコードを挿入します。

```
<?xml version="1.0" encoding="UTF-8"?>



<DefaultAssociations>



<Association Identifier="http" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />



<Association Identifier="https" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />



</DefaultAssociations>
```

グループポリシー管理コンソールから、**コンピューターの構成 > 管理用テンプレート > Windows コンポーネント > エクスプローラー > 既定の関連付け構成ファイルを設定する** に移動し、ServerFTAdefaultPolicy.xmlファイルを保存します。

注:

Citrixサーバーにグループポリシー設定がない場合、WindowsはURLを開くためのアプリケーションを選択するようユーザーに促します。

デフォルトでは、次のURLタイプのリダイレクトをサポートしています。

- HTTP
- HTTPS
- RTSP
- RTSPU
- PNM
- MMS

リダイレクト用のリストに、追加の標準またはカスタムURLタイプを含めるには、以前に参照したServerFTAdefaultPolicy.xmlファイルに新しい**Association Identifier**行を作成します。例：

```
<Association Identifier="ftp" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />

<Association Identifier="mailto" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />

<Association Identifier="customtype1" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />

<Association Identifier="customtype2" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

リストにURLタイプを追加するには、クライアント構成も必要です。Windowsクライアントで以下のレジストリキーと値を作成します。

注:

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

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA
- 値の名前: ExtraURLProtocols
- 値の型: REG_SZ
- 値のデータ: 必要なURLタイプをセミコロンで区切って指定します。URLのオーソリティ部分より前のすべてを含めます。例： `ftp://;mailto:;customtype1://;custometype2://`

URLの種類はWindowsクライアントにのみ追加できます。上記のレジストリ設定がないクライアントは、Citrixセッションへのリダイレクトを拒否します。クライアントには、指定されたURLの種類を処理するようにインストールおよび構成されたアプリケーションが必要です。

デフォルトのリダイレクトリストからURLタイプを削除するには、サーバーVDAで以下のレジストリキーと値を作成します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- 値の名前: DisableServerFTA
- 値の型: DWORD
- 値のデータ: 1
- 値の名前: NoRedirectClasses
- 値の型: REG_MULTI_SZ
- 値のデータ: 次の値の任意の組み合わせを指定します: `http`、`https`、`rtsp`、`rtspu`、`pnm`、または `mms`。複数の値を別々の行に入力します。例:

`http`

`https`

`rtsp`

特定のWebサイトセットに対してホストからクライアントへのリダイレクトを有効にするには、サーバーVDAでレジストリキーと値を作成します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- 値の名前: ValidSites
- 値の型: REG_MULTI_SZ
- 値のデータ: 完全修飾ドメイン名 (FQDN) の任意の組み合わせを指定します。複数のFQDNを別々の行に入力します。プロトコル (`http://` または `https://`) を含めず、FQDNのみを含めます。FQDNには、アスタリスク (`*`) をワイルドカード文字として左端の位置にのみ含めることができます。このワイルドカードは、RFC 6125のルールに準拠した単一レベルのドメインに一致します。例:

`www.exmaple.com`

`*.example.com`

> **注:**
>
> **ValidSites**キーを**DisableServerFTA**キーおよび**NoRedirectClasses**キーと組み合わせて使用することはできません。

サーバーVDAのデフォルトブラウザ構成

このセクションで参照されているホストからクライアントへのリダイレクトを有効にすると、サーバーVDA上の以前のデフォルトブラウザ構成はすべて上書きされます。Web URLがリダイレクトされない場合、Citrix Launcherは、`command_backup` レジストリキーで構成されているブラウザにURLを渡します。このキーはデフォルトでInternet Explorerを指していますが、別のブラウザへのパスを含むように変更できます。詳細については、レジストリを介して管理される機能のリストにある サーバーVDAのデフォルトブラウザ構成 を参照してください。

ローカルアプリアクセスとURLリダイレクト

はじめに

Local App Accessは、ローカルにインストールされたWindowsアプリケーションを、デスクトップを切り替えることなくホストされたデスクトップ環境にシームレスに統合します。Local App Accessを使用すると、次のことが可能になります。

- 物理的なラップトップ、PC、またはその他のデバイスにローカルにインストールされているアプリケーションに、仮想デスクトップから直接アクセスできます。
- 柔軟なアプリケーション配信ソリューションを提供します。仮想化できない、またはIT部門が保守していないローカルアプリケーションをユーザーが持っている場合でも、それらのアプリケーションは仮想デスクトップにインストールされているかのように動作します。
- アプリケーションが仮想デスクトップとは別にホストされている場合のダブルホップの遅延を解消します。これを行うには、公開されたアプリケーションへのショートカットをユーザーのWindowsデバイスに配置します。
- 次のようなアプリケーションを使用します。
    - GoToMeetingなどのビデオ会議ソフトウェア。
    - まだ仮想化されていない特殊なアプリケーションまたはニッチなアプリケーション。
    - そうでなければ、ユーザーデバイスからサーバーへ、そしてサーバーからユーザーデバイスへと大量のデータを転送するようなアプリケーションと周辺機器。たとえば、DVDバーナーやTVチューナーなど。

Citrix Virtual Apps and Desktops™では、ホストされたデスクトップセッションは、URLリダイレクトを使用してLocal App Accessアプリケーションを起動します。URLリダイレクトにより、アプリケーションは複数のURLアドレスで利用可能になります。デスクトップセッション内のブラウザで埋め込みリンクを選択することにより、ローカルブラウザ（ブラウザのURLブロックリスト

に基づく）を起動します。ブロックリストにないURLに移動すると、そのURLはデスクトップセッションで再度開かれます。

URLリダイレクトはデスクトップセッションでのみ機能し、アプリケーションセッションでは機能しません。アプリケーションセッションで使用できる唯一のリダイレクト機能は、ホストからクライアントへのコンテンツリダイレクトです。これは、サーバーFTA（ファイルタイプ関連付け）リダイレクトの一種です。このFTAは、HTTP、HTTPS、RTSP、MMSなどの特定のプロトコルをクライアントにリダイレクトします。たとえば、HTTPで埋め込みリンクのみを開く場合、リンクはクライアントアプリケーションで直接開かれます。URLブロックリストまたは許可リストのサポートはありません。

Local App Accessが有効になっている場合、ローカルで実行されているアプリケーション、ユーザーがホストするアプリケーションからのリンクとして、またはデスクトップ上のショートカットとしてユーザーに表示されるURLは、次のいずれかの方法でリダイレクトされます。

- ユーザーのコンピューターからホストされたデスクトップへ
- Citrix Virtual Apps and Desktops™サーバーからユーザーのコンピューターへ
- 起動された環境でレンダリングされる（リダイレクトされない）

特定のWebサイトからのコンテンツのリダイレクトパスを指定するには、Virtual Delivery AgentでURL許可リストとURLブロックリストを構成します。これらのリストには、URLリダイレクトポリシー設定を指定する複数文字列のレジストリキーが含まれています。詳細については、「ローカルアプリアクセス ポリシー設定」を参照してください。

URLは、以下の例外を除き、VDAでレンダリングできます。

- 地域/ロケール情報 — msn.comやnews.google.comなど、ロケール情報を必要とするWebサイト（地域に基づいて国固有のページを開きます）。たとえば、VDAが英国のデータセンターからプロビジョニングされ、クライアントがインドから接続している場合、ユーザーはin.msn.comが表示されることを期待しますが、実際にはuk.msn.comが表示されます。
- マルチメディアコンテンツ — リッチメディアコンテンツを含むWebサイトは、クライアントデバイスでレンダリングされると、エンドユーザーにネイティブなエクスペリエンスを提供し、高遅延ネットワークでも帯域幅を節約します。この機能は、Silverlightなどの他のメディアタイプを含むサイトをリダイレクトします。このプロセスは安全な環境で行われます。つまり、管理者が承認したURLはクライアントで実行され、残りのURLはVDAにリダイレクトされます。

URLリダイレクトに加えて、FTAリダイレクトを使用できます。FTAは、セッション内でファイルが検出されたときにローカルアプリケーションを起動します。ローカルアプリが起動された場合、そのローカルアプリはファイルを開くためにファイルへのアクセス権を持っている必要があ

ります。したがって、ローカルアプリケーションを使用して開くことができるファイルは、ネットワーク共有上またはクライアントドライブ上（クライアントドライブマッピングを使用）にあるファイルのみです。たとえば、PDFファイルを開く際に、PDFリーダーがローカルアプリである場合、そのPDFリーダーを使用してファイルが開かれます。ローカルアプリはファイルに直接アクセスできるため、ファイルを開くためのICA®を介したネットワーク転送は発生しません。

要件、考慮事項、および制限事項

WindowsマルチセッションOS用VDAおよびWindowsシングルセッションOS用VDAの有効なオペレーティングシステムで、ローカルアプリアクセスをサポートしています。ローカルアプリアクセスには、Citrix Workspaceアプリ for Windowsバージョン4.1（最小）が必要です。以下のブラウザーがサポートされています。

- Edge、最新バージョン
- Firefox、最新バージョンおよび延長サポートリリース
- Chrome、最新バージョン

ローカルアプリアクセスとURLリダイレクトを使用する際の以下の考慮事項と制限事項を確認してください。

- ローカルアプリアクセスは、すべてのモニターにまたがる全画面の仮想デスクトップ向けに設計されています。
    - ウィンドウモードで実行される仮想デスクトップや、すべてのモニターをカバーしない仮想デスクトップでローカルアプリアクセスを使用すると、ユーザーエクスペリエンスが混乱する可能性があります。
    - 複数モニター — 1つのモニターが最大化されると、そのセッションで起動されたすべてのアプリケーションのデフォルトデスクトップになります。このデフォルトは、後続のアプリケーションが通常別のモニターで起動される場合でも発生します。
    - この機能は1つのVDAをサポートします。複数の同時VDAとの統合はありません。
- 一部のアプリケーションは予期しない動作をし、ユーザーに影響を与える可能性があります。
    - ドライブ文字は、仮想デスクトップのC:ドライブではなくローカルのC:ドライブのように表示されるため、ユーザーを混乱させる可能性があります。
    - 仮想デスクトップで利用可能なプリンターは、ローカルアプリケーションでは利用できません。
    - 昇格された権限を必要とするアプリケーションは、クライアントホスト型アプリケーションとして起動できません。

  - シングルインスタンスアプリケーション（Windows Media Playerなど）に対する特別な処理はありません。
  - ローカルアプリケーションは、ローカルマシンのWindowsテーマで表示されます。
  - 全画面表示アプリケーションはサポートされていません。これには、PowerPointのスライドショーやデスクトップ全体を覆うフォトビューアーなど、全画面で開くアプリケーションが含まれます。
  - ローカルアプリアクセスは、ローカルアプリケーションのプロパティ（クライアントのデスクトップやスタートメニューのショートカットなど）をVDAにコピーします。ただし、ショートカットキーや読み取り専用属性などの他のプロパティはコピーしません。
  - 重なり合うウィンドウの順序の処理方法をカスタマイズするアプリケーションは、予期しない結果をもたらす可能性があります。たとえば、一部のウィンドウが非表示になることがあります。
  - マイコンピューター、ごみ箱、コントロールパネル、ネットワークドライブのショートカット、フォルダーのショートカットなど、ショートカットはサポートされていません。
  - 次のファイルの種類とファイルはサポートされていません：カスタムファイルの種類、関連付けられたプログラムがないファイル、zipファイル、隠しファイル。
  - 32ビットと64ビットのクライアントホスト型またはVDAアプリケーションが混在している場合、タスクバーのグループ化はサポートされていません。つまり、32ビットのローカルアプリケーションと64ビットのVDAアプリケーションをグループ化することはできません。
  - COMを使用してアプリケーションを起動することはできません。たとえば、Officeアプリケーション内から埋め込みOfficeドキュメントをクリックした場合、プロセスの起動が検出されず、ローカルアプリケーションの統合は失敗します。

- ユーザーが別の仮想デスクトップセッション内から仮想デスクトップを起動するダブルホップシナリオはサポートされていません。
- URLリダイレクトは明示的なURL（つまり、ブラウザのアドレスバーに表示されるURL、またはブラウザに応じてブラウザ内ナビゲーションを使用して見つかるURL）のみをサポートします。
- URLリダイレクトはデスクトップセッションでのみ機能し、アプリケーションセッションでは機能しません。
- VDAセッションのローカルデスクトップフォルダーでは、ユーザーはファイルを作成できません。
- ローカルで実行されているアプリケーションの複数のインスタンスは、仮想デスクトップ用に設定されたタスクバー設定に従って動作します。ただし、ローカルで実行されているアプリ

ケーションへのショートカットは、それらのアプリケーションの実行中のインスタンスとグループ化されません。また、ホストされたアプリケーションの実行中のインスタンスや、ホストされたアプリケーションへのピン留めされたショートカットともグループ化されません。ユーザーは、タスクバーからローカルで実行されているアプリケーションのウィンドウのみを閉じることができます。ユーザーはローカルアプリケーションウィンドウをデスクトップのタスクバーやスタートメニューにピン留めできますが、これらのショートカットを使用するとアプリケーションが常に起動するとは限りません。

- **ローカルアプリアクセスを許可**ポリシー設定を**有効**に設定した場合、ブラウザーコンテンツリダイレクトはサポートされません。デフォルトでは、ローカルアプリアクセスは禁止されています。

Windowsとの連携

ローカルアプリアクセスとWindowsとの連携には、次の動作が含まれます。

- Windows 8およびWindows Server 2012のショートカットの動作
  - クライアントにインストールされているWindowsストアアプリケーションは、ローカルアプリアクセスのショートカットの一部として列挙されません。
  - 画像ファイルとビデオファイルは、デフォルトでWindowsストアアプリケーションを使用して開かれます。ただし、ローカルアプリアクセスはWindowsストアアプリケーションを列挙し、デスクトップアプリケーションでショートカットを開きます。
- ローカルプログラム
  - Windows 7の場合、フォルダーはスタートメニューで利用できます。
  - Windows 8の場合、ローカルプログラムは、ユーザーがスタート画面からカテゴリとして**すべてのアプリ**を選択した場合にのみ利用できます。すべてのサブフォルダーがローカルプログラムに表示されるわけではありません。
- アプリケーション向けのWindows 8グラフィック機能
  - デスクトップアプリケーションはデスクトップ領域に制限されており、スタート画面およびWindows 8スタイルのアプリケーションによって覆われます。
  - ローカルアプリアクセスアプリケーションは、マルチモニターモードではデスクトップアプリケーションのように動作しません。マルチモニターモードでは、スタート画面とデスクトップが異なるモニターに表示されます。
- Windows 8とローカルアプリアクセスURLリダイレクト

- Windows 8のInternet Explorerではアドオンが有効になっていないため、URLリダイレクトを有効にするにはデスクトップ版Internet Explorerを使用してください。
- Windows Server 2012では、Internet Explorerはデフォルトでアドオンを無効にします。URLリダイレクトを実装するには、Internet Explorerの拡張構成を無効にします。その後、Internet Explorerのオプションをリセットして再起動し、標準ユーザー向けにアドオンが有効になっていることを確認します。

ローカルアプリアクセスとURLリダイレクトの構成

Citrix Workspace™アプリでローカルアプリアクセスとURLリダイレクトを使用するには：

- ローカルクライアントマシンにCitrix Workspaceアプリをインストールします。Citrix Workspaceアプリのインストール中に両方の機能を有効にするか、グループポリシーエディターを使用してローカルアプリアクセステンプレートを有効にすることができます。
- **ローカルアプリアクセスを許可**ポリシー設定を**有効**に設定します。URLリダイレクトのURL許可リストおよびブロックリストポリシー設定も構成できます。詳しくは、「ローカルアプリアクセス ポリシー設定」を参照してください。

ローカルアプリアクセスとURLリダイレクトを有効にする

すべてのローカルアプリケーションでローカルアプリアクセスを有効にするには、次の手順に従います。

1. Web Studioにサインインし、左側のペインで**ポリシー**をクリックします。
2. アクションバーで、**ポリシーの作成**をクリックします。
3. ［ポリシーの作成］ウィンドウで、検索ボックスに「Allow Local App Access」と入力し、**選択**をクリックします。
4. 設定の編集ウィンドウで、**許可**を選択します。デフォルトでは、**ローカルアプリアクセスを許可**ポリシーは禁止されています。この設定が許可されている場合、VDAは、公開アプリケーションとローカルアプリアクセスのショートカットをセッションで有効にするかどうかをエンドユーザーが決定できるようにします。（この設定が禁止されている場合、公開アプリケーションとローカルアプリアクセスのショートカットの両方がVDAで機能しません。）このポリシー設定は、マシン全体とURLリダイレクトポリシーに適用されます。
5. ［ポリシーの作成］ウィンドウで、検索ボックスに「URL redirection allow list」と入力し、**選択**をクリックします。URLリダイレクト許可リストは、リモートセッションのデフォルトブラウザーで開くURLを指定します。
6. 「設定の編集」ウィンドウで、「**追加**」をクリックしてURLを追加し、「**OK**」をクリックします。

7. ［ポリシーの作成］ウィンドウで、検索ボックスに「URL redirection block list」と入力し、**選択**をクリックします。URLリダイレクトブロックリストは、エンドポイントで実行されているデフォルトブラウザーにリダイレクトされるURLを指定します。
8. 「設定の編集」ウィンドウで、「**追加**」をクリックしてURLを追加し、「**OK**」をクリックします。
9. 「設定」ページで、「**次へ**」をクリックします。
10. 「ユーザーとマシン」ページで、該当するデリバリーグループにポリシーを割り当て、「**次へ**」をクリックします。
11. 「概要」ページで設定を確認し、「**完了**」をクリックします。

Citrix Workspaceアプリのインストール中にすべてのローカルアプリケーションでURLリダイレクトを有効にするには、次の手順に従います。

1. マシン上のすべてのユーザーに対してCitrix Workspaceアプリをインストールするときに、URLリダイレクトを有効にします。これにより、URLリダイレクトに必要なブラウザーアドオンも登録されます。
2. コマンドプロンプトから、以下のいずれかのオプションを使用してCitrix Workspaceアプリをインストールするための適切なコマンドを実行します。
   - CitrixReceiver.exeの場合は、`/ALLOW_CLIENTHOSTEDAPPSURL=1`を使用します。
   - CitrixReceiverWeb.exeの場合は、`/ALLOW_CLIENTHOSTEDAPPSURL=1`を使用します。

グループポリシーエディターを使用してローカルアプリアクセス テンプレートを有効にする

注:

- グループポリシーエディターを使用してローカルアプリアクセステンプレートを有効にする前に、receiver.admx/admlテンプレートファイルをローカルGPOに追加します。
- Windows向けCitrix Workspaceアプリのテンプレートファイルは、CitrixBase.admx/CitrixBase.admlを%systemroot%\policyDefinitionsフォルダーに追加した場合にのみ、ローカルGPOの**管理用テンプレート > Citrixコンポーネント > Citrix Workspace**フォルダーで利用できます。

> グループポリシーエディターを使用してローカルアプリアクセス テンプレートを有効にするには、次の手順に従います。

1. **gpedit.msc**を実行します。
2. **コンピューターの構成 > 管理用テンプレート > クラシック管理用テンプレート (ADM) > Citrix Components > Citrix Workspace > ユーザーエクスペリエンス**に移動します。
3. **ローカルアプリアクセス設定**をクリックします。
4. **有効**を選択し、**URLリダイレクトを許可**を選択します。URLリダイレクトの場合、この記事の後半にある「*ブラウザーアドオンの登録*」セクションで説明されているコマンドラインを使用して、ブラウザーアドオンを登録します。

公開アプリケーションのみにアクセスを提供する

レジストリエディターまたはPowerShell SDKを使用して、公開アプリケーションへのアクセスを提供できます。

レジストリエディターについては、レジストリを介して管理される機能のリストにある「公開アプリケーションのローカルアプリアクセス」を参照してください。

PowerShell SDKを使用するには：

1. Delivery Controller™が実行されているマシンでPowerShellを開きます。
2. 次のコマンドを入力します: `set-configsitemetadata -name "studio_clientHostedAppsEnabled" -value "true"`。

クラウドサービス展開で**ローカルアプリアクセスアプリケーションの追加**にアクセスするには、Citrix DaaS Remote PowerShell SDKを使用します。詳しくは、「Citrix DaaS Remote PowerShell SDK」を参照してください。

1. インストーラーをダウンロードします:

   `<https://download.apps.cloud.com/CitrixPoshSdk.exe>`

2. 次のコマンドを実行します:

   a. `asnp citrix.*`.

   b. `Get-XdAuthentication`

3. 次のコマンドを入力します: `set-configsitemetadata -name "studio_clientHostedAppsEnabled" -value "true"`。

該当する前の手順を完了したら、以下の手順に従って続行します。

1. Web Studioにサインインし、左側のペインで**アプリケーション**を選択します。
2. 上部中央ペインで、空白領域を右クリックし、コンテキストメニューから**Add Local App Access Application**を選択します。アクションバーの**Add Local App Access Application**をクリックすることもできます。アクションバーにAdd Local App Access Applicationオプションを表示するには、**Refresh**をクリックします。
3. ローカルアプリアクセスアプリケーションを公開します。

    - ローカルアプリケーションアクセスウィザードが起動し、紹介ページが表示されます。このページは、今後のウィザードの起動時に表示しないように設定できます。
    - ウィザードは、以下で説明するグループ、場所、識別、配信、および概要の各ページを案内します。各ページの作業が完了したら、概要ページに到達するまで**次へ**をクリックします。
    - グループページで、新しいアプリケーションを追加するデリバリーグループを1つ以上選択し、**次へ**をクリックします。
    - ページで、ユーザーのローカルマシン上のアプリケーションの完全な実行可能パスを入力し、アプリケーションが配置されているフォルダーへのパスを入力します。Citrixでは、システム環境変数パスを使用することをお勧めします。例: %ProgramFiles(x86)%\Internet Explorer\iexplore.exe。
    - 識別ページで、デフォルト値を受け入れるか、必要な情報を入力してから**次へ**をクリックします。
    - ページで、このアプリケーションをユーザーに配信する方法を構成し、**次へ**をクリックします。選択したアプリケーションのアイコンを指定できます。また、仮想デスクトップ上のローカルアプリケーションへのショートカットを、スタートメニュー、デスクトップ、またはその両方に表示するかどうかを指定できます。
    - 概要ページで設定を確認し、**完了**をクリックしてローカルアプリケーションアクセスウィザードを終了します。

ブラウザアドオンを登録する

> **注:**
>
> URLリダイレクトに必要なブラウザーアドオンは、コマンドラインから / ALLOW_CLIENTHOSTEDAPPSURL=1 オプションを使用してCitrix Workspaceアプリをインストールすると、自動的に登録されます。

1つまたはすべてのアドオンを登録および登録解除するには、次のコマンドを使用します。

- クライアントデバイスにアドオンを登録するには: \<*client-installation-folder*>\redirector.exe /reg\<*browser*>
- クライアントデバイスのアドオンを登録解除するには: \<*client-installation-folder*>\redirector.exe /unreg\<*browser*>
- VDAにアドオンを登録するには: \<*VDAinstallation-folder*>\VDARedirector.exe /reg\<*browser*>
- VDAのアドオンを登録解除するには: \<*VDAinstallation-folder*>\VDARedirector.exe /unreg\<*browser*>

ここで、\<*browser*>はInternet Explorer、Firefox、Chrome、またはAllです。

たとえば、次のコマンドは、Citrix Workspaceアプリを実行しているデバイスにInternet Explorerアドオンを登録します。

C:\Program Files\Citrix\ICA Client\redirector.exe/regIE

次のコマンドは、WindowsマルチセッションOS VDA上のすべてのアドオンを登録します。

C:\Program Files (x86)\Citrix\HDX\bin\VDARedirector.exe /regAll

ブラウザ間のURLインターセプト

- デフォルトでは、Internet Explorerは指定されたURLをリダイレクトします。URLがブロックリストにないが、ブラウザまたはWebサイトが別のURLにリダイレクトする場合、最終的なURLはリダイレクトされません。ブロックリストにある場合でもリダイレクトされません。

URLリダイレクトが正しく機能するように、ブラウザからプロンプトが表示されたらアドオンを有効にしてください。インターネットオプションを使用しているアドオン、またはプロンプト内のアドオンが無効になっている場合、URLリダイレクトは正しく機能しません。

- Firefoxのアドオンは常にURLをリダイレクトします。

アドオンがインストールされると、Firefoxは新しいタブページにアドオンのインストールを許可するか、または防止するかを促します。機能が動作するようにアドオンを許可してください。

- Chromeのアドオンは、入力されたURLではなく、常にナビゲートされた最終URLをリダイレクトします。

拡張機能は外部からインストールされています。拡張機能を無効にすると、ChromeでURLリダイレクト機能が動作しません。シークレットモードでURLリダイレクトが必要な場合は、ブラウザの設定でそのモードでの拡張機能の実行を許可してください。

ログオフ時および切断時のローカルアプリケーションの動作を構成する

注:

これらの手順に従って設定を構成しない場合、デフォルトでは、ユーザーが仮想デスクトップからログオフまたは切断しても、ローカルアプリケーションは実行を継続します。再接続後、ローカルアプリケーションが仮想デスクトップで利用可能な場合、それらは再統合されます。

ログオフ時および切断時のローカルアプリケーションの動作を構成するには、レジストリを介して管理される機能のリストにあるログオフ時および切断時のローカルアプリケーションの動作を参照してください。

印刷

効率的な印刷管理は、Citrix Virtual Apps and Desktops™ (CVAD) 環境における生産的で効率的なIT運用の要です。ユーザーは印刷リソースへのシームレスで信頼性の高いアクセスを必要とし、管理者は印刷インフラストラクチャを構成、管理、保護、トラブルシューティングするための堅牢なツールを必要とします。

このドキュメントは、既存のナレッジベースを刷新し、IT管理者にCVAD印刷のあらゆる側面を徹底的に理解させることを目的とした、包括的で専門家レベルのガイドとして機能します。

印刷は、多くのビジネスワークフローにとって基本的な要件であり続けています。Citrix Virtual Apps and Desktops™ (CVAD) 環境では、ユーザーセッションと物理プリンターハードウェアとの分離があるため、仮想セッションから物理デバイスへの印刷要求を効率的に管理することは、特有の課題を提示します。

CVADは、このギャップを埋めるために設計された包括的なテクノロジーとポリシーのスイートを提供し、多様なプリンターの種類、ネットワーク条件、ユーザー要件に対応する柔軟性を提供しながら、最適なパフォーマンスと管理の簡素化を目指しています。

Citrix Universal™ プリントドライバー (UPD)

重要事項:

Citrix Virtual Apps and Desktops™ の第4四半期リリースで、**ユニバーサルドライバーの優先順位**ポリシー設定のデフォルトの順序が変更されます。新しいデフォルトの順序は次のとおりです。

- EMF
- XPS
- PCL5c (ピーシーエルファイブシー)
- PCL4
- PDF

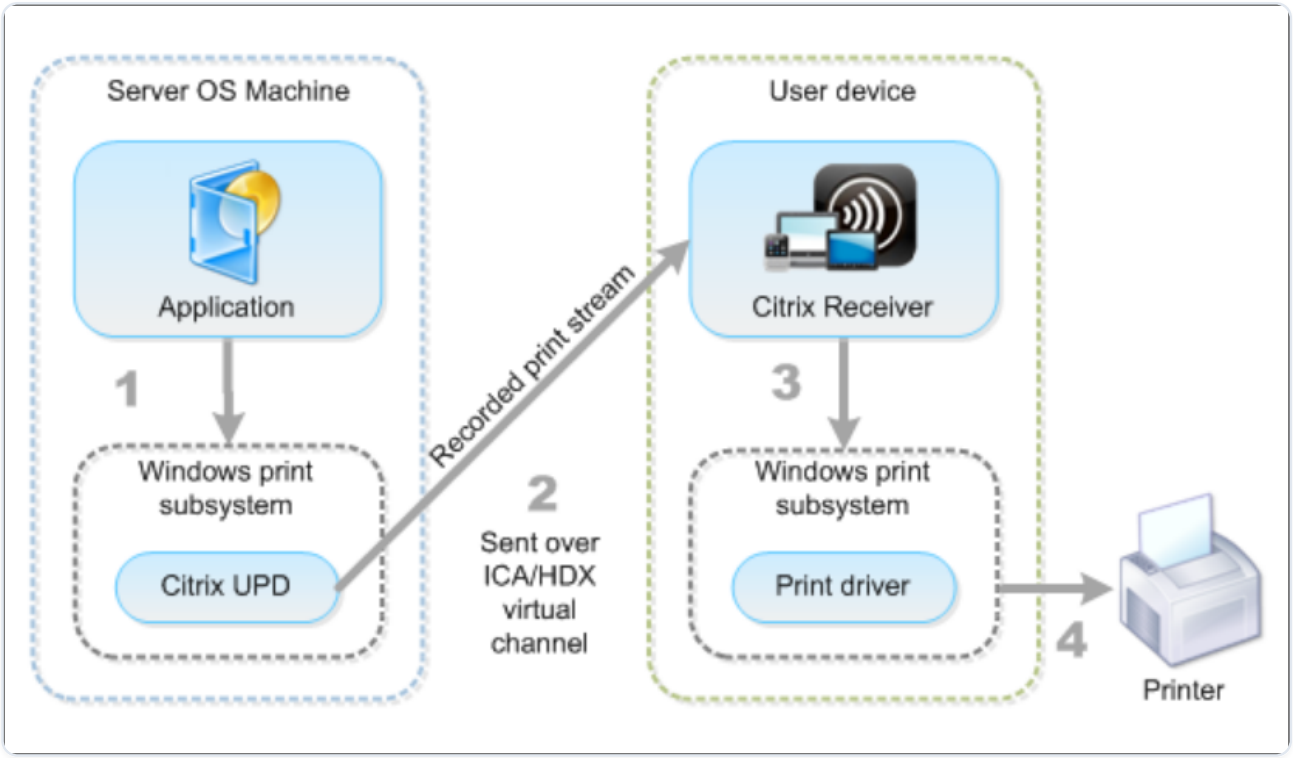
- PS

詳細については、ユニバーサルドライバーの優先順位 ページを参照してください。

Citrix Universal Print Driver (UPD) は単一のドライバーではなく、サーバー (VDA) とクライアント (Workspace アプリがインストールされたエンドポイント) の両方にコンポーネントが含まれる技術です。

- **サーバーコンポーネント:** VDA とともにインストールされ、これには「Citrix Universal Printer」(EMF 形式を使用) や「Citrix XPS Universal Printer」(XPS 形式を使用) など、実際の汎用プリントドライバーが含まれ、PDF および PS 形式もサポートします。その役割は、VDA で実行されているアプリケーションによって生成された印刷出力を、デバイスに依存しない形式でキャプチャすることです。
- **クライアントコンポーネント:** Citrix Workspace™ アプリのインストールに含まれており、このコンポーネントは VDA から送信された印刷ストリームを受信します。その後、エンドポイントデバイス上のローカル Windows 印刷サブシステムと連携して、ターゲットプリンター用にローカルにインストールされている適切なデバイス固有のドライバーを使用して印刷ジョブをレンダリングします。

次の図は、ユニバーサルプリントドライバーのコンポーネントと、デバイスにローカルに接続されたプリンターの一般的なワークフローを示しています。



UPD の主な目的は、Citrix® 環境内でのプリンタードライバー管理を簡素化することです。VDA 上で組み込みドライバーを使用することで、管理者は、不安定性や競合の一般的な原因となる、数百もの異なるメーカー固有のドライバーをインストールおよび保守する手間を省くことができます。UPD は、幅広いプリンターとの互換性を目指し、仮想セッションとクライアントの印刷機能との間にユニバーサルインターフェイスを提供します。

サポートされている形式

UPDテクノロジーは複数の印刷データ形式をサポートしており、印刷ジョブの処理方法とレンダリング方法に柔軟性をもたらします。

- **EMF (Enhanced Metafile Format):** 「Citrix Universal Printer」ドライバーで使用されるデフォルトの形式です。32ビットのWindowsネイティブベクター形式です。EMFを使用した印刷は一般的に効率的ですが、通常、レンダリングにはWindowsベースのクライアントエンドポイントが必要です。
- **XPS (XML Paper Specification):** 「Citrix XPS Universal Printer」ドライバーで使用されます。XPSは、Microsoftが開発したXMLベースのページ記述言語で、PDFと概念が似ており、プラットフォームに依存しないように設計されています。
- **PS (PostScript):** Adobeが開発したページ記述言語で、複雑なグラフィックやタイポグラフィの処理能力で知られ、出版業界やさまざまなプリンター、複合機でよく使用されます。Linuxクライアントは、UPDでPostScript印刷を利用することがよくあります。
- **PDF:** PDFは、ドキュメント交換のための広く使用されているオープン標準です。テキスト、フォント、グラフィック、および表示に必要なその他の情報を含む、固定レイアウトのフラットドキュメントの完全な記述をカプセル化します。プラットフォームに依存しないように設計されており、異なるシステムやアプリケーション間でドキュメントの忠実性を維持するのに理想的です。

UPDを使用すると、いくつかの潜在的な利点があります。

- **ドライバー管理の削減:** VDAイメージに必要なドライバーの数を大幅に減らし、イメージの作成とメンテナンスを簡素化します。
- **安定性の向上:** ドライバーが少ないということは、潜在的な競合が少なくなり、ドライバー関連のスプーラークラッシュやシステム不安定性のリスクが低減されることを意味します。
- **印刷ジョブの最適化:** 特定のUPD形式、特にEMFは、ネイティブドライバーと比較して印刷ジョブのサイズが小さくなることがあります。
- **高度な機能のサポート:** クライアント上のネイティブドライバーがMicrosoftの標準Print Capabilityテクノロジーを通じてこれらの機能を公開している場合、EMFおよびXPS UPDコンポーネントは高度な印刷機能（ステープル、トレイ選択など）をサポートできます。

構成

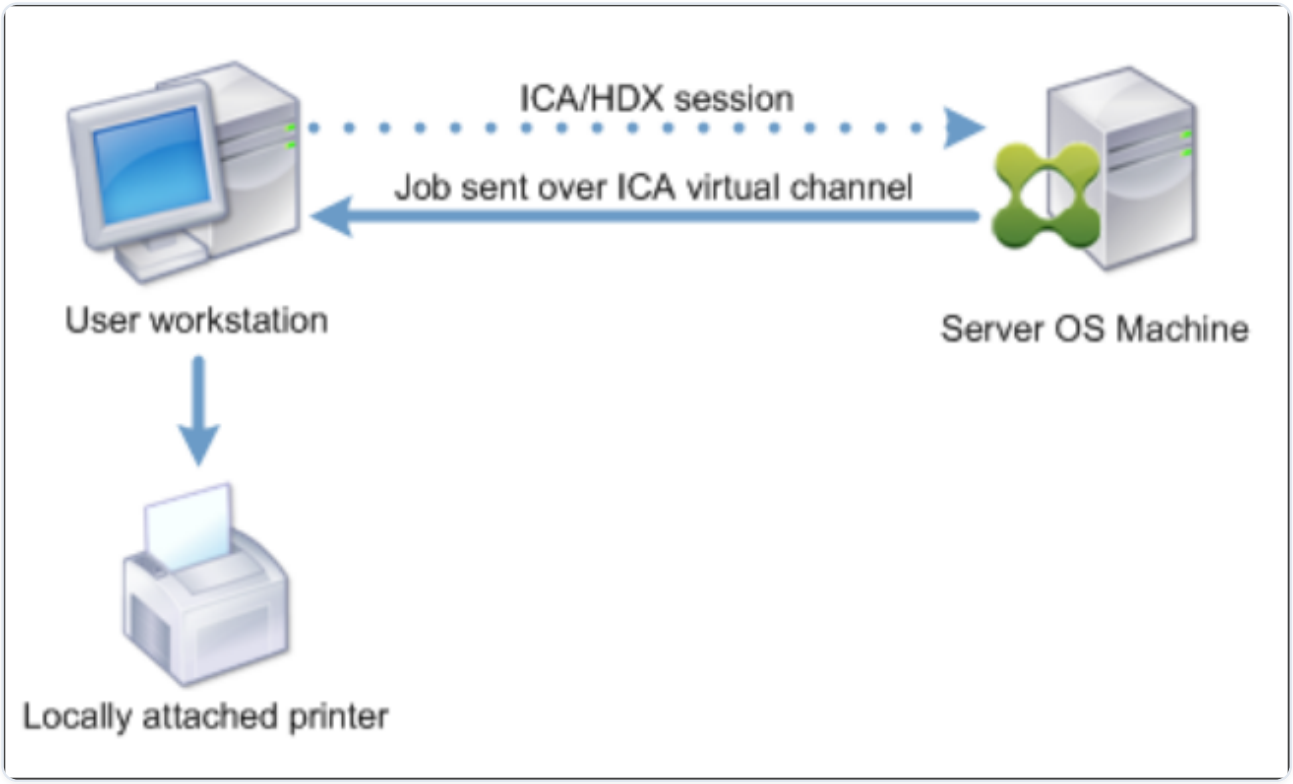
ニーズと環境に最も適した印刷構成オプションを選択することで、管理を簡素化できます。

選択できるオプションは次のとおりです。

- シトリックス ユニバーサル™ 印刷サーバー
- クライアントプリンターリダイレクト
- ネットワークプリンター

クライアントプリンターリダイレクト

これは多くの場合、既定のメカニズムであり、ユーザーがログオンすると、ユーザーのエンドポイントデバイスで構成されたプリンターがCitrix®セッションに自動的にマッピングされます。これには、クライアントに直接接続されているプリンター (USB、LPTなど) や、クライアントマシンにマッピングされているネットワークプリンターが含まれます。エンドユーザーは通常、どのローカルプリンターがリダイレクトされるかを手動で選択することはできません。これは管理ポリシーによって制御されます。



セットアップ手順

この機能はデフォルトで有効になっています。関連する設定と構成は、「クライアントプリンター」テンプレートにあります。このテンプレートのポリシー設定を使用して、クライアントプリンターリダイレクトのエクスペリエンスをさらにカスタマイズおよび最適化できます。

クライアントプリンターリダイレクトに関連するポリシーは、クライアントプリンターポリシー設定で確認できます。

考慮事項

主な課題は、多数のプリンターがクライアントエンドポイントにマッピングされ、リダイレクトされる場合に、パフォーマンスの低下と不安定性が発生する可能性があることです。さらに、ドライバーの非互換性やクライアント側の問題が原因で、プリンターマッピングの失敗が発生する可能性があります。信頼性は、クライアントデバイスの構成と健全性に大きく依存します。一部の管理者は、潜在的な負荷とドライバー管理の複雑さのため、クライアントプリンターの自動作成を完全に回避することを好みます。

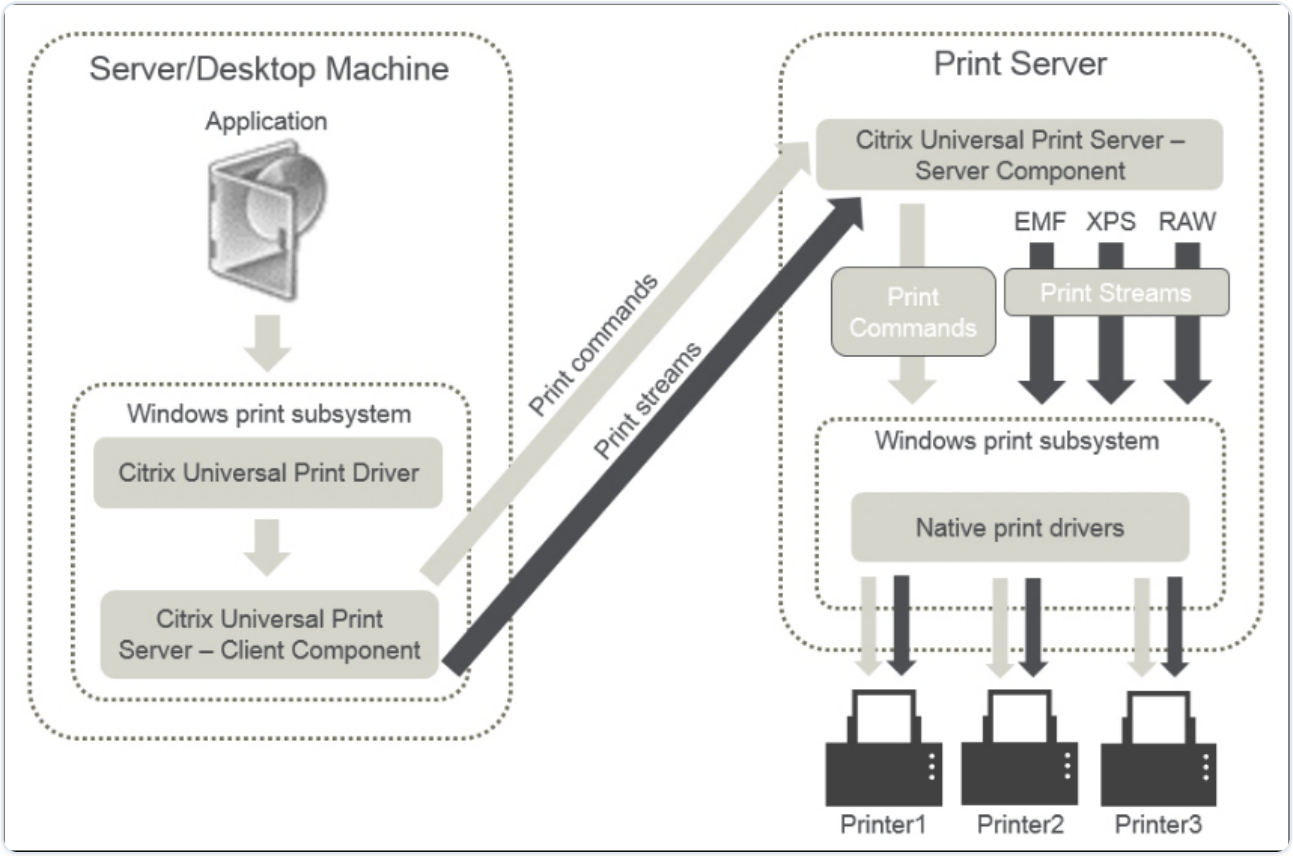
ユースケース

ローカルマシンに直接接続されているプリンター (USB、LPT、COM、クライアントにのみマッピングされているネットワークプリンター) へのアクセスを必要とするユーザー。

Citrix Universal™ プリントサーバー (UPS)

UPS は、ネットワーク印刷を最適化および管理するために設計されたオプションの Citrix® コンポーネントです。これは次の2つの部分で構成されています。

- **UPServer** コンポーネントは、ネットワーク内の1つ以上の Windows プリントサーバーにインストールされます。
- **UPClient** コンポーネントは、VDA インストールの一部です。ポリシーによって有効にすると、VDA は UPServer と通信してネットワークプリンターへの接続を確立し、通常は Citrix Universal Print Driver (UPD) を活用します。



UPS は、特に WAN リンクを介したネットワーク印刷や大規模な環境において、いくつかの利点を提供します。

- ネットワーク最適化: VDA と UPServer 間で送信される印刷データは最適化および圧縮され、帯域幅の消費を削減します。これは特に WAN 接続において重要です。
- 集中型ドライバー管理: ネットワークプリンターに Citrix UPD を活用できるため、VDA に多数のネイティブプリンタードライバーをインストールおよび管理する必要がなくなります。
- 高可用性: 複数の UPServer 間での負荷分散と、サーバーが利用できなくなった場合の自動フェイルオーバーをサポートします。

要件

- Microsoft Visual C++ 2015–2022 再頒布可能パッケージ
- マイクロソフト .NET フレームワーク 4.8 (最小)
- UPServer の OS 要件
  - ウィンドウズ サーバー 2025
  - ウィンドウズ サーバー 2022
  - ウィンドウズ サーバー 2019

構成/セットアップ手順

この機能はデフォルトで無効になっています。関連する設定と構成は、「Universal Print Server」テンプレートにあります。このテンプレートのポリシー設定を使用して、Universal Print server のエクスペリエンスをさらにカスタマイズおよび最適化できます。

有効化設定に加えて、いくつかのポリシー設定で UPS の動作を微調整できます。

- 通信用のポート構成 (HTTP/SOAP、CGP、およびそれらの SSL/TLS 同等物)。
- 印刷ストリームの入力帯域幅制限。
- ロードバランシング用のUPSサーバーのリスト。 フェールオーバー検出のためのサービス停止しきい値。
- Webサービス接続のタイムアウト。
- セキュアな通信のためのSSL/TLS構成設定。

詳細については、「Citrix UPSポリシー設定」を参照してください。

ベストプラクティス

- WANリンクを介したネットワーク印刷にUPSを使用して、パフォーマンスを最適化します。
- Citrix Universal Print Driver (UPD) を利用して、VDAでのドライバー管理を削減します。
- 高可用性を実現するために、複数のUPSサーバー間でロードバランシングを構成します。

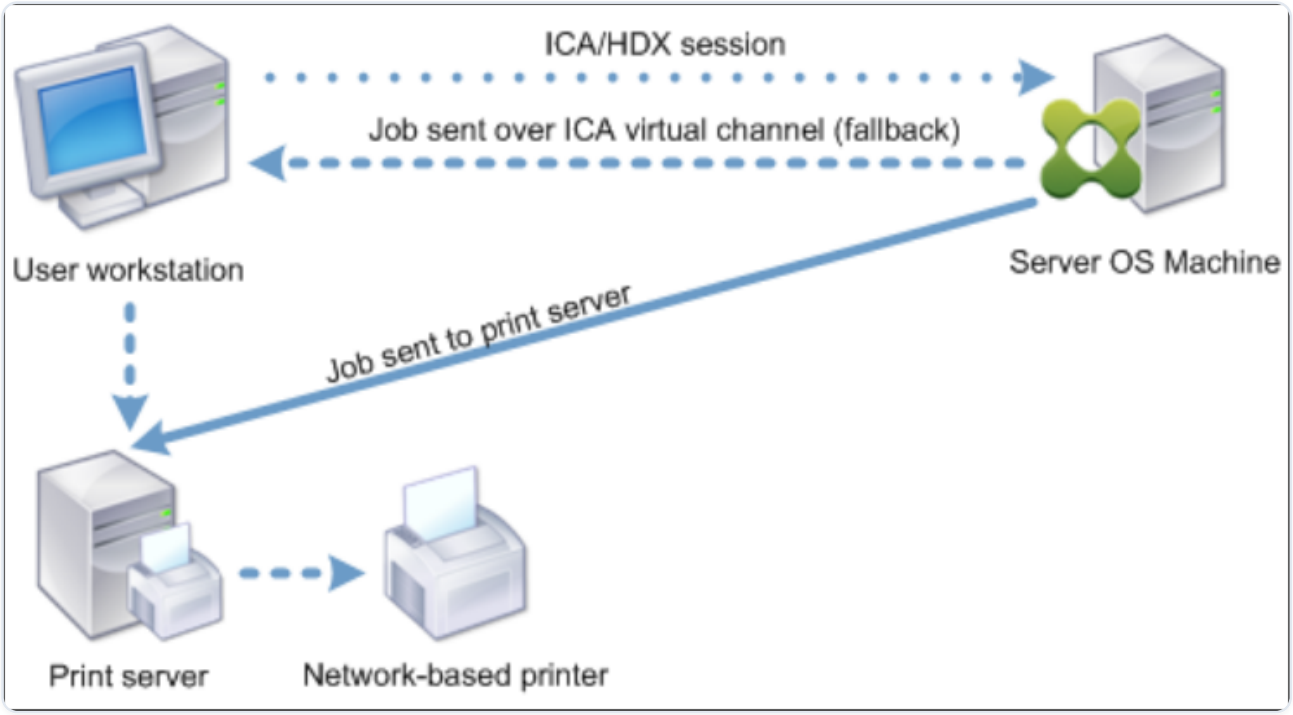
ユースケース

Citrixは、WANリンクを含むリモートプリントサーバーのシナリオにUPSを明示的に推奨しています。また、VDAドライバーのフットプリントを最小限に抑えたい、ネットワーク印刷のパフォーマンスを向上させたい、ネットワーク印刷の高可用性を提供したい、またはネットワークロケーションに基づいて近接印刷を実装したい環境にも最適です。ネットワークプリンターに直接接続できないシンクライアントは、VDAを介してUPSを利用できます。

ネットワークプリンター (VDA上)

ここでは、印刷ジョブはVDAからネットワーク経由でネットワークプリントサーバー（標準のWindowsプリントサーバーまたはCitrix Universal™ Print Serverのいずれか）に直接送信されます。この経路は、VDAと同じローカルエリアネットワーク（LAN）上にあるプリンターの場合、一般的に高速です。これは、直接接続が有効になっている場合のネットワークプリンターのデフォルトの経路です。公開されたアプリケーションまたはデスクトップがプリントサーバーにアクセスできない場合、またはネイティブプリンタードライバーがマルチセッションOSマシンにイン

ストールされていない場合、印刷ジョブはICA接続経由でルーティングされるようにフォールバックします。



要件

- 必要なプリンタードライバーは、ネットワークプリンターをホストしているプリントサーバーの種類によって異なります。
  - プリンターが標準のWindowsプリントサーバーでホストされている場合、対応するネイティブプリンタードライバーがVDAにインストールされている必要があります。
  - プリンターがCitrix Universal Print Server (UPS) でホストされている場合、接続にはネイティブドライバーまたはCitrix UPDのいずれかを使用できます。
- VDAからプリントサーバーへのネットワーク接続。
- ログインしているユーザーに対する適切な権限。

ネットワークプリンターの接続と構成に関するガイダンス（ポリシー設定）

- UNCパス（例: “\\PrintServer\PrinterName”）経由でプリンターを接続する
- **セッションプリンター:** この方法の主要なポリシーです。管理者はUNCパスを入力するか、ネットワークを参照してプリンターを追加します。特定のユーザー、グループ、クライアントIPなどをターゲットにするために、ポリシーにフィルターを適用できます。
- **プリンター割り当て:** 複数のユーザーまたはデバイスに多数のプリンターを同時に割り当てるのに役立つ代替ポリシーです。これにより、セッションプリンターと、それらの割り当てのデフォルトプリンターの両方を設定できます。

ベストプラクティス（N/Wプリンターへの直接接続を許可する）

- ルーティング（VDAからサーバーへの直接接続、またはクライアント/ICA経由）には、「ネットワークプリンターへの直接接続」ポリシーを検討してください。
    - 有効にすると（デフォルト設定）、LAN経由での印刷パフォーマンスが最適になります。このシナリオでの印刷トラフィックは非圧縮です。
    - VDAとプリントサーバーが同じネットワークにない場合（WANシナリオ）、このポリシー設定を無効にします。これにより、印刷トラフィックはクライアントエンドポイントを経由するよう強制され、ICA®圧縮が活用されますが、遅延が発生します。

直接接続を有効にするとLANのパフォーマンスが向上しますが、VDAとプリントサーバー間のネットワークトラフィックは非圧縮になります。無効にすると、トラフィックはクライアント経路を強制的に経由し、ICA圧縮を活用します。これはWANシナリオに有益ですが、遅延が増加します。

ユースケース

共有の部署プリンターまたはオフィスプリンターに仮想セッションから直接アクセスします。VDAにネイティブドライバーがインストールされている必要があります。

制限事項

不安定なネットワーク環境（WAN）では、印刷パフォーマンスが低下します。さらに、ドライバー管理はIT管理者にとって大きな負担となります。

トラブルシューティング

体系的なアプローチ

複雑なCitrix Virtual Apps and Desktops™ (CVAD)環境での印刷問題のトラブルシューティングには、当てずっぽうではなく、体系的なアプローチが必要です。推奨されるプロセスは次のとおりです。

1. **症状の特定:** 問題を明確に定義します（例：プリンターが表示されない、ジョブが停止する、出力が間違っている、印刷が遅い）。
2. **範囲の特定:** 影響を受けているユーザー（1人のユーザー、複数のユーザー、特定のアプリケーション）、関連するプリンター、および問題が発生しているVDAまたはクライアントデバイスを特定します。

3. **基本の確認:** ネットワーク接続（VDAからプリントサーバー、クライアントからVDA）を確認し、プリンターがオンラインでCitrix®外で機能していることを確認し、クライアントからのローカル印刷をチェックします（リダイレクトの問題の場合）。
4. **ポリシーの確認:** Citrix Group Policy Modelingウィザードなどのツールを使用するか、VDAで適用されているポリシー設定を確認して、影響を受けるユーザー/セッションに適用されている関連するCitrixポリシー設定を調べます。ポリシー設定が意図どおりに構成されており、明らかな競合がないことを確認します。
5. **ログの確認:** VDA、クライアントデバイス、およびプリントサーバー（該当する場合）でWindowsイベントログ（アプリケーションログ、システムログ、PrintServiceログ）を確認します。有効になっている場合は、Citrix固有のログを確認します。3
6. **コンポーネントのテスト:** 問題を特定のコンポーネントに分離することを試みます。別のアプリケーションから印刷を試みたり、別のプリンターを試したり、汎用ドライバー（UPDやMicrosoft XPS Document Writerなど）でテストしたり、Print SpoolerおよびCitrix Print Managerサービスのステータスを確認したりします。
7. **リソースの参照:** 既知の問題と解決策については、製品ドキュメント、サポート記事、およびコミュニティフォーラムを活用します。

一般的な問題と解決策

現場で報告されている一般的な印刷問題と推奨されるトラブルシューティング手順の一部を以下に示します。

- **プリンターの自動作成の失敗 / セッションにプリンターが表示されない:**
    - **考えられる原因:** クライアントプリンターリダイレクトポリシーが無効になっている。クライアントプリンターの自動作成ポリシーが「なし」に設定されているか、誤ってフィルターされている。クライアントデバイスのプリントスプーラーの問題。Workspaceアプリの問題。クライアントとVDA間のネットワーク接続の問題。Citrix Print Manager Service (CpSvc.exe)がVDAで実行されていないかクラッシュしている。VDAに必要なプリンタードライバーがない（ネイティブドライバーが必要な場合）。Citrixポリシーがセッションに正しく適用されていない。
    - **トラブルシューティング手順:**
        a. クライアントプリンターリダイレクトポリシーが「許可」されており、クライアントプリンターの自動作成がユーザー/セッションに対して正しく構成されていることを確認します。
        b. VDA で CpSvc.exe サービスの状態を確認します。必要に応じて再起動します。

c. VDA とクライアントの両方で Windows Print Spooler サービスの状態を確認します。必要に応じて再起動します。

d. 基本的なネットワーク接続を確認します。

e. クライアントデバイスでローカル印刷をテストします。

f. 互換性のある Workspace アプリのバージョンがインストールされていることを確認します。

g. VDA のイベントログで、CpSvc またはプリンター作成に関連するエラーを確認します。

h. VDA でポリシーの更新を強制します (gpupdate /force)。

i. VDA に適用されているポリシーを確認し、期待される設定が存在することを確認します。

j. ネイティブドライバーが必要な場合は、VDA にインストールされていることを確認します。

k. VDA のローカル/グループポリシーで、RDS/ターミナルサーバーのプリンターリダイレクト設定を確認します。

l. VDA レジストリ内の孤立したプリンターエントリを検索してクリーンアップします。

- **Print Spooler のクラッシュ / サービス応答なし (VDA またはプリントサーバー上):**
  - **考えられる原因:** 欠陥のある、または互換性のないプリンタードライバー (多くの場合サードパーティ製); キュー内の破損した印刷ジョブ; ドライバーの競合; システムリソースの不足。
  - **トラブルシューティングの手順:**

a. Windows イベントログ (アプリケーションログにスプーラーのクラッシュがよく表示されます) を使用して、障害のあるプロセス/モジュールを特定します。

b. Print Spoolerサービス」の再起動を試行します。

c. 再起動に失敗した場合、または問題が再発する場合は、手動で印刷キューをクリアしてみてください（Spoolerサービスを停止し、C:\Windows\System32\spool\PRINTERS 内のファイルを削除し、Spoolerサービスを開始します）。

d. 問題のあるプリンタードライバーを特定して削除します。完全に削除するには、レジストリの編集が必要になる場合があります。

e. Citrix UPDまたは汎用Microsoftドライバーでテストします。

f. レジストリ内の孤立したプリントプロセッサを確認し、クリーンアップします。

- **ポリシーの競合 / 設定の無視:**
  - **考えられる原因:** GPO設定がCitrixポリシーを上書きしている。Citrixポリシーの優先順位またはフィルターが競合している。ポリシー処理中にエラーが発生している。
  - **トラブルシューティングの手順:**
    a. Citrixグループポリシーモデリングウィザードを使用して、影響を受けるユーザー/VDAに対するポリシー適用をシミュレートします。
    b. ポリシーフィルター（ユーザーグループ、クライアントIPなど）が正しいことを確認します。
    c. Studio/Web Studioでポリシーの優先順位を確認します。
    d. Citrixポリシーの問題を特定するために、VDAのOUでGPOの継承を一時的にブロックします。
    e. VDA上のポリシー処理結果を調べます（例: gpresult /h report.htmlを使用）。
    f. ユーザー/VDAに適用されるポリシーセットを簡素化し、競合を見つけるためにポリシーを段階的に追加し直します。
- **ドライバーの問題（全般 - 互換性、破損、マッピング）:**
  - **考えられる原因:** ドライバーがVDA OSまたはCitrixバージョンと互換性がない。ドライバーのインストールが破損している。ポリシーで必要なドライバーがVDAにない。複数のドライバー間の競合。プリンタードライバーマッピングポリシーの設定が正しくない。
  - **トラブルシューティングの手順:**
    a. Citrix UPDを使用して印刷を試す（ユニバーサルプリントドライバー使用ポリシーを設定する）。
    b. 適用されているポリシーに基づいて、正しいドライバー（ネイティブまたはUPD）が選択されていることを確認する。
    c. 必要なネイティブドライバーがVDAに正しくインストールされていることを確認する（使用する場合）。
    d. CVADおよびVDA OSバージョンとのドライバーの互換性について、ベンダーのドキュメントを確認する。
    e. 問題のあるドライバーをクリーン再インストールする（アンインストール、再起動、インストール）。
    f. プリンタードライバーマッピングポリシーのルールを慎重に確認し、テストする。
    g. VDAにインストールされているドライバーの数を最小限に抑える。

- **印刷速度の低下 / パフォーマンスの問題:**
  - **考えられる原因:** ネットワークの混雑または高遅延（特にWAN）。大規模で複雑な印刷ジョブ（例：高解像度グラフィック）。非効率なプリンタードライバー。印刷最適化（圧縮、キャッシュ）が無効になっているか、誤って設定されている。非効率なルーティング（例：低速WAN経由の直接接続）。
  - **トラブルシューティングの手順:**
    a. VDA、クライアント、プリントサーバー間のネットワークパスとパフォーマンスを分析する。
    b. 印刷用のCitrix帯域幅制限ポリシーを設定する。
    c. ユニバーサル印刷ポリシーを介して、UPD最適化（画像圧縮、フォント/画像キャッシュ）を有効にして設定する。
    d. WANリンクの場合、「印刷サーバーへの直接接続」ポリシーを無効にして、圧縮されたICA®チャネル経由でトラフィックを強制します。
    e. UPSを使用している場合は、ネットワーク用に最適に構成されていることを確認してください。
    f. 印刷ジョブ自体を分析し、可能であれば解像度または複雑さを軽減します。
    g. 別のドライバー（例：UPDとネイティブ）でテストします。
- **出力の誤り（文字の欠落、書式設定エラー、向きの誤り）：**
  - **考えられる原因：** ドキュメント/アプリケーションに必要なVDA上のフォントの欠落。不適切なフォント置換。プリンタードライバーの非互換性。特定のUPD形式（例：EMFとXPS）に関する問題。アプリケーションのバグ。ローカルクライアントプリンターで有効になっている高度な印刷機能との競合。
  - **トラブルシューティングの手順：**
    a. 必要なすべてのフォントがVDAにインストールされていることを確認します。
    b. ユニバーサルドライバーの優先ポリシーの順序を変更してみてください（例：EMFの前にXPSを試す）。
    c. 別のアプリケーションから同じドキュメントを印刷してテストします。
    d. 別の物理プリンターまたは仮想プリンター（例：Microsoft XPS Document Writer）に印刷してテストします。
    e. 別のプリンタードライバー（UPDとネイティブ、または異なるネイティブバージョン）を使用してみてください。

f. アプリケーションの印刷設定とページ設定を確認します。

g. クライアントデバイスのローカルプリンターのプロパティで「詳細な印刷機能」を無効にします。

h. ユーザー設定とポリシーで印刷の向きの設定を確認します。

- **シトリックス プリントマネージャーサービス (CpSvc.exe) のクラッシュ/ハング:**
  - **考えられる原因:** 応答しないプリンタードライバーがレジストリに孤立したオブジェクトを残している。印刷に関連するCitrixポリシーデータが破損している。システムリソースの競合。
  - **トラブルシューティングの手順:**

    a. VDAレジストリから孤立したプリンターおよび印刷プロセッサーのエントリをクリーンアップする手順に従ってください。まず、Print SpoolerサービスとCpSvcサービスを停止する必要があります。

    b. 問題のあるプリンタードライバーを特定して削除します。

    c. VDA上のCitrixポリシーキャッシュフォルダー/レジストリキーをクリーンアップし、ポリシーの強制更新を検討してください。

    d. VDAのリソース使用量 (CPU、メモリ) を監視します。

    e. CpSvcサービスとPrint Spoolerサービスを再起動します。

- **PDFプリンターの問題:**
  - **考えられる原因:** PDFユニバーサルプリンターの自動作成ポリシーが無効になっている。互換性のないVDAまたはWorkspaceアプリのバージョン。クライアントエンドポイントにPDFビューアーがインストールされていない。サポートされていないブラウザーが使用されている (例: Edge)、またはHTML5構成エラー (CSPヘッダー、config.js)。
  - **トラブルシューティングの手順:**

    a. PDFユニバーサルプリンターの自動作成ポリシーが有効になっており、適用されていることを確認します。

    b. VDAとWorkspaceアプリが最小バージョン要件を満たしていることを確認します。

    c. サポートされているPDFビューアー (例: Adobe Reader、Chrome) がクライアントにインストールされ、デフォルトとして設定されていることを確認します。

    d. HTML5 Workspaceアプリを使用している場合は、ブラウザーの互換性を確認し、configuration.jsおよびCSPヘッダーの設定を確認します。

    e. ポリシー変更後にCitrixセッションを再起動します。

基本的なエンドユーザーのトラブルシューティング

組織のポリシーで許可されている場合、簡単な印刷の問題を経験しているユーザーは、IT部門にエスカレートする前に、基本的な手順で問題を解決できる場合があります。

- HDX™セッションから完全にログオフし、再度ログインします。
- エンドポイントデバイス上のローカルプリンターのステータスを確認します（オンラインであること、一時停止されていないこと、エラーがないことを確認します）。
- ローカルエンドポイントデバイスを再起動します。

ベストプラクティス

- **ユニバーサルプリントサーバー (UPS) を活用する:** 最適化と集中管理の利点があるため、特にWANを介したネットワーク印刷に推奨されます。
- **ユニバーサルプリントドライバー (UPD) を採用する:** ドライバーの数と競合を最小限に抑えるための主要なドライバー戦略としてUPDを使用します。
- **検証済みのネイティブドライバーを選択的に使用する:** 特定のプリンター機能にネイティブドライバーが必要な場合は、それらが徹底的にテストされていることを確認してください。
- **ドライバーのフットプリントを最小限に抑える:** VDAイメージにインストールするプリンタードライバーの数を可能な限り少なくします。
- **ドライバーマッピングを活用する:** プリンタードライバーマッピングと互換性ポリシーを使用して、問題のあるドライバーを置き換えたり、UPDの使用を強制したりします。
- **厳密にテストする:** テストされていないドライバーを本番環境に展開しないでください。
- **ドライバーの更新を慎重に管理する:** インプレース更新は避け、クリーンアンインストール、再起動、再インストールのプロセスを推奨します。
- **不要なドライバーをクリーンアップする:** 不要になったドライバーは定期的に削除します。
- **ルーティングを最適化する:** 印刷ジョブが最も効率的なパスを通るようにします（例：LAN上のVDAからプリントサーバーへの直接接続を有効にして直接接続する。WANの場合は直接接続を無効にしてICA/クライアント経由でルーティングする）。
- **分散プリントサーバーを検討する:** UPSを使用していない大規模で地理的に分散した組織の場合、各物理ロケーションにプリントサーバーを配置することで、管理と負荷分散に役立ちます（ただし、負荷分散を備えたUPSは、より統合されたCitrix®ソリューションを提供します）。
- **古い印刷ジョブをパージする:** 印刷キューからスタックしたジョブや古いジョブを定期的にクリアします。

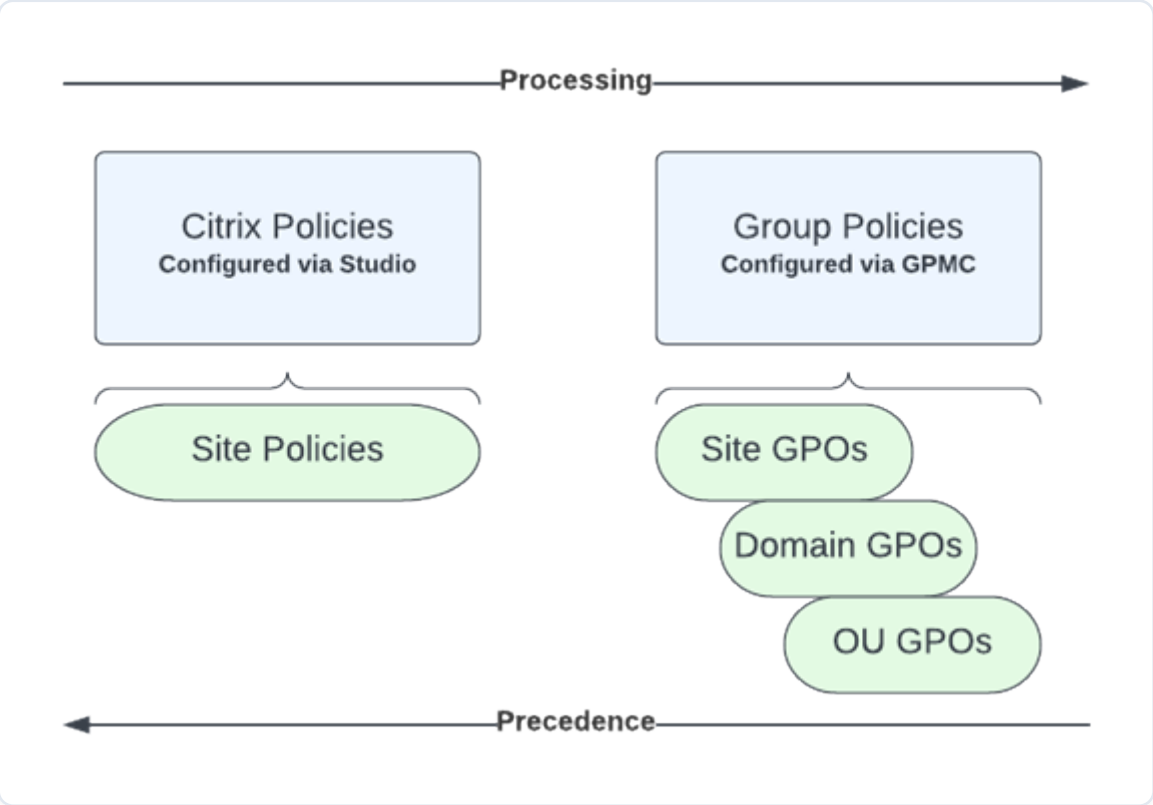
設計上の考慮事項

- **プロビジョニングを調整する:** ユーザー要件に基づいてプロビジョニング方法（自動作成、セッションプリンター、UPS、PDFプリンター）を選択します（例：ローミングユーザーは近接印刷やPDF印刷の恩恵を受け、静的ワークステーションはセッションプリンターを使用する場合があります）。
- **ルーティングを計画する:** エンドポイント、VDA、プリントサーバーのネットワークロケーションに基づいて印刷ジョブのルーティングを設計します。
- **冗長性を確保する:** 特にUPSを使用している場合は、負荷分散ポリシーを介してプリントサーバーの冗長性を実装します。

ポリシー

ポリシーは、ユーザー、デバイス、または接続タイプのグループに対して、セッション、帯域幅、およびセキュリティがどのように管理されるかを定義する設定の集合です。

ポリシー設定は、物理マシンおよび仮想マシン、またはユーザーに適用できます。設定は、ローカルレベルの個々のユーザー、またはActive Directoryのセキュリティグループに適用できます。構成は特定の基準とルールを定義します。ポリシーを明示的に割り当てない場合、設定はすべての接続に適用されます。



ポリシーはネットワークのさまざまなレベルに適用できます。組織単位GPOレベルに配置されたポリシー設定は、ネットワーク上で最も高い優先順位を持ちます。ドメインGPOレベルのポリシーは、サイトグループポリシーオブジェクトレベルのポリシーを上書きします。サイトグループポリシーオブジェクトレベルは、MicrosoftおよびCitrixローカルポリシーレベルの両方における競合するポリシーを上書きします。

すべてのCitrixローカルポリシーは、Web Studioコンソールで作成および管理され、サイトデータベースに保存されます。グループポリシーは、Microsoftグループポリシー管理コンソール

（GPMC）を使用して作成および管理され、Active Directoryに保存されます。Microsoftローカルポリシーは、Windowsオペレーティングシステムで作成され、レジストリに保存されます。

Studioは、モデリングウィザードを使用して、管理者がテンプレートとポリシー内の構成設定を比較し、競合する設定や冗長な設定を排除するのに役立ちます。管理者はGPMCを使用してGPOを設定し、設定を構成できます。また、それらをネットワークのさまざまなレベルのターゲットユーザーセットに適用することもできます。

これらのGPOはActive Directoryに保存されます。これらの設定の管理へのアクセスは、セキュリティ上の理由からほとんどのIT担当者に対して制限されています。

設定は優先順位とその条件に従ってマージされます。無効な設定は、下位の有効な設定を上書きします。未構成のポリシー設定は無視され、下位の設定を上書きしません。

ローカルポリシーは、Active Directory内のグループポリシーと競合することもあり、状況によっては互いに上書きし合う可能性があります。

すべてのポリシーは次の順序で処理されます。

1. エンドユーザーはドメイン資格情報を使用してマシンにログオンします。
2. 資格情報はドメインコントローラーに送信されます。
3. Active Directoryはすべてのポリシー（エンドユーザー、エンドポイント、組織単位、およびドメイン）を適用します。
4. エンドユーザーはCitrix Workspace™アプリにログオンし、アプリケーションまたはデスクトップにアクセスします。
5. CitrixおよびMicrosoftのポリシーは、エンドユーザーとリソースをホストするマシンに対して処理されます。
6. Active Directoryはポリシー設定の優先順位を決定します。その後、それらをエンドポイントデバイスのレジストリと、リソースをホストするマシンに適用します。
7. エンドユーザーがリソースからログオフします。エンドユーザーおよびエンドポイントデバイスに対するCitrixポリシーは、アクティブではなくなります。
8. エンドユーザーがユーザーデバイスからログオフすると、GPOユーザーポリシーが解放されます。
9. エンドユーザーがデバイスの電源を切ると、GPOマシンポリシーが解放されます。

ユーザー、デバイス、マシンのグループに対してポリシーを作成する場合、一部のメンバーは異なる要件を持つ可能性があり、一部のポリシー設定に例外が必要になる場合があります。例外

は、ポリシーが誰または何に影響するかを決定するStudioおよびGPMCのフィルターによって作成されます。

> **注:**
>
> 同じGPO内でWindowsポリシーとCitrixポリシーを混在させることはサポートされていません。

概要

> **注:**
>
> バージョン2511以降、Citrix Web Studio™（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix® Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

> ポリシーとは、ユーザー、デバイス、または接続の種類グループに対して、セッション、帯域幅、およびセキュリティがどのように管理されるかを定義する設定の集まりです。Citrix®ポリシーは、これらの側面を一元的に管理する効率的な方法を提供します。各ポリシーには、環境に合わせて調整された複数の設定とフィルター（オブジェクト割り当て）を含めることができます。

ポリシー管理ツール

- ウェブスタジオ

  Web Studioを使用して作成されたポリシーはサイトデータベースに保存され、以下のいずれかが発生したときに更新がVDAにプッシュされます。

  - そのVDAがブローカーに登録されたとき
  - ユーザーがセッションを起動したとき

- グループポリシー管理コンソール (GPMC)

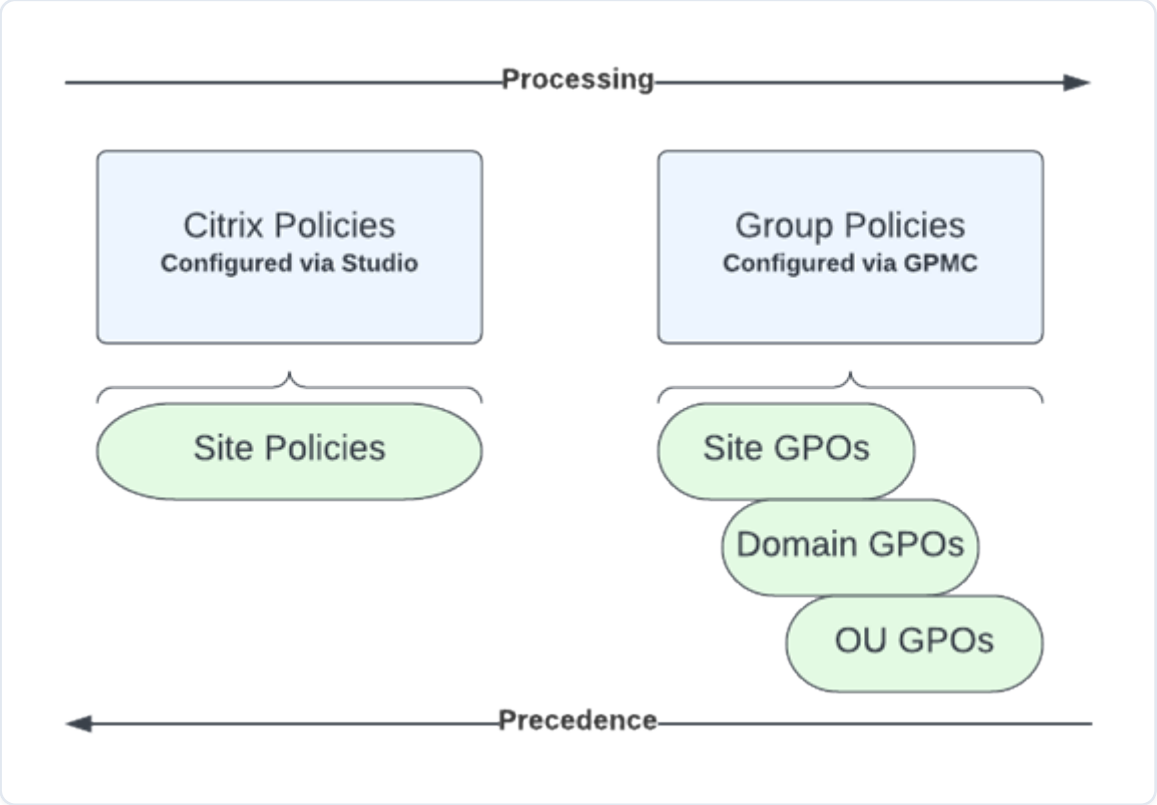
  ネットワーク環境でActive Directoryを使用しており、グループポリシーを管理する権限がある場合は、GPMCを使用してポリシーを作成および編集できます。

GPMCでは、必要な設定とフィルターを使用してグループポリシーオブジェクト（GPO）を構成できます。これらのポリシーは、Web Studioで構成されたポリシーよりも優先されます。詳細については、「CTX238166」を参照してください。

ポリシー処理順序

グループポリシー設定は、次の順序で処理されます。

1. サイトレベルのGPO（サイトデータベースに保存）
2. ドメインレベルのGPO
3. 組織単位 (OU) GPO



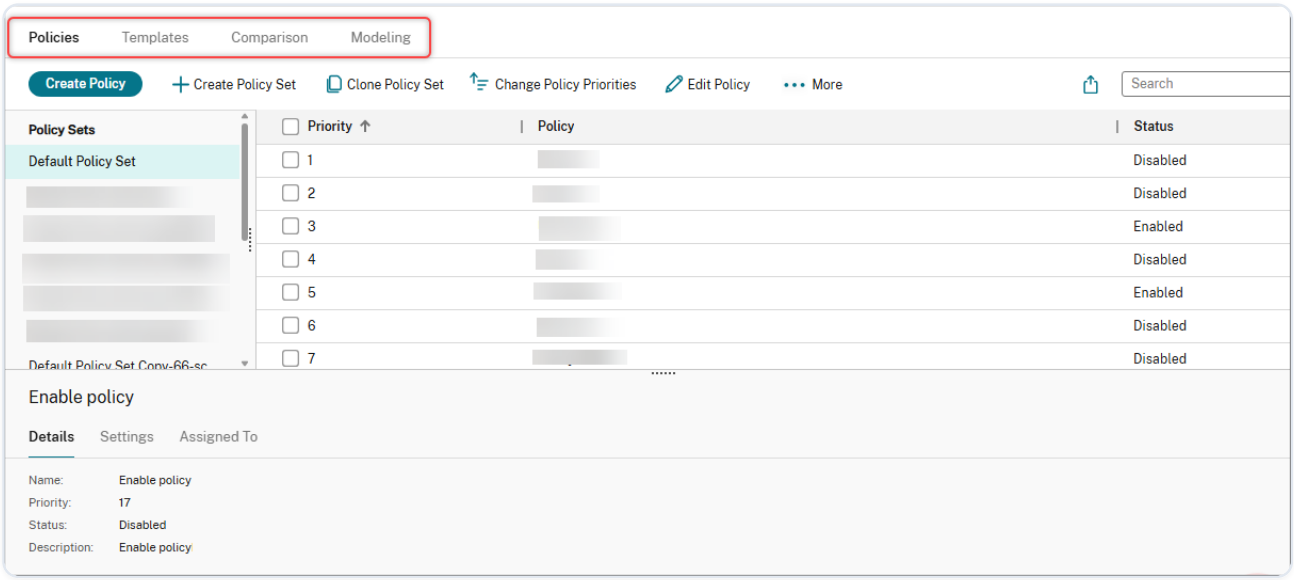
2つのGPOで同じポリシーに異なる設定が適用されている場合、最後に処理されたポリシー設定が、以前に処理された設定を上書きします。この構成は、ポリシー設定が次の順序で優先されることを意味します。

1. OU GPO（最優先）
2. ドメインレベルのGPO
3. サイトレベルのGPO（最低優先度）

競合する設定を持つ複数のポリシーを使用している場合は、ポリシーの優先順位を割り当てることで優先順位を制御できます。詳細については、「ポリシー割り当ての例外を管理する」を参照してください。

Web Studio > ポリシーインターフェイスについて

ポリシー、設定、またはテンプレートにアクセスするには、Web Studioにサインインし、左側のペインで を選択します。



- **ポリシー**タブでは、ポリシーセットとポリシーを作成および管理できます。ポリシーセットからポリシーを選択すると、次のタブが表示されます。
  - **概要** – ポリシー名、優先度、ステータス、および説明を表示します。
  - **設定** – 設定されているすべての設定を一覧表示します。
  - **割り当て先** – 割り当てられているデリバリーグループを表示します。割り当てを編集または削除できます。ポリシーは、セッションを実行しているデスクトップのデリバリーグループに基づいて適用されます。詳細については、「ポリシーの作成」を参照してください。
- **テンプレート**タブでは、ポリシーテンプレートを作成し、Citrix提供のテンプレートとカスタムテンプレートを管理できます。テンプレートを選択すると、次のタブが表示されます。
  - **説明** – テンプレートの目的を説明します。
  - – 構成された設定を一覧表示します。詳細については、「テンプレートの作成」を参照してください。
- タブでは、ポリシーまたはテンプレートの設定を他の設定と比較できます。この機能を使用して、コンプライアンスまたは相違点を確認します。詳細については、「ポリシーとテンプレートの比較」を参照してください。
- タブでは、接続シナリオをシミュレートし、有効なポリシー結果を表示できます。詳細については、「ポリシーのシミュレーションと評価」を参照してください。

ポリシー構成ワークフロー

Web Studioを使用してCitrixポリシーを構成するには、次のワークフローに従います。

1. ポリシーの作成。
    a. ポリシー設定を構成します。

        環境に必要な設定を追加および構成します。

    b. ポリシーを割り当てます。

        ポリシーを適切なマシンオブジェクトとユーザーオブジェクトに割り当てます。
2. ポリシーの優先順位の設定。

    どの設定が優先されるかを決定するために、ポリシーを優先順位で並べ替えます。
3. 有効なポリシーの確認。

    ポリシーモデリングウィザードを使用して、適用された設定を確認します。

テンプレートを作成する

> **注:**
>
> バージョン2511以降、Citrix Web Studio™（Webベース）は、Citrix Virtual Apps and Desktops™ の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

テンプレートは、ポリシーを作成するための事前定義された開始点を提供します。Citrixでは、特定の環境とネットワーク条件に最適化された組み込みテンプレートを提供しています。これらのテンプレートを使用して、次のことができます。

- サイト間で共有する独自のポリシーとテンプレートを作成する。
- 展開間の比較時に参照する。たとえば、「...CitrixテンプレートXまたはYを使用する場合...」など。
- テンプレートをインポートまたはエクスポートして、Citrixサポートまたは信頼できるサードパーティとポリシー構成を共有する。

組み込みテンプレート

次の組み込みテンプレートが利用可能です。

- **非常に高精細なユーザーエクスペリエンス**。このテンプレートは、ユーザーエクスペリエンスを最大化するデフォルト設定を適用します。複数のポリシーが優先順位に従って処理されるシナリオでこのテンプレートを使用します。
- **高いサーバー拡張性**。このテンプレートを適用して、サーバーリソースを節約します。このテンプレートは、ユーザーエクスペリエンスとサーバーの拡張性のバランスを取ります。単一サーバーでホストできるユーザー数を増やしながら、優れたユーザーエクスペリエンスを提供します。このテンプレートは、グラフィックの圧縮にビデオコーデックを使用せず、サーバー側のマルチメディアレンダリングを防止します。
- **高いサーバー拡張性 - レガシーOS**。この高いサーバー拡張性テンプレートは、Windows Server 2008 R2またはWindows 7以前を実行しているVDAにのみ適用されます。このテンプレートは、これらのオペレーティングシステムにより効率的なレガシーグラフィックモードに依存しています。
- **NetScaler SD-WANに最適化**。Citrix Virtual Desktopsの配信を最適化するためにNetScaler SD-WANを使用している支社のユーザーにこのテンプレートを適用します。(NetScaler SD-WANはCloudBridgeの新しい名称です)。
- **WANに最適化**。このテンプレートは、共有WANまたは低帯域幅接続のリモートロケーションを使用する支社のタスクワーカー向けです。ワーカーは、グラフィック的にシンプルなユーザーインターフェースとほとんどマルチメディアコンテンツのないアプリケーションにアクセスします。このテンプレートは、ビデオ再生エクスペリエンスと一部のサーバー拡張性を犠牲にして、帯域幅効率を最適化します。
- **WANに最適化 - レガシーOS**。このテンプレートは、Windows Server 2008 R2またはWindows 7以前を実行しているVDAにのみ適用されます。このテンプレートは、これらのオペレーティングシステムにより効率的なレガシーグラフィックモードに依存しています。
- **セキュリティと制御**。リスク許容度が低い環境でこのテンプレートを使用し、Citrix Virtual Apps and Desktops™でデフォルトで有効になっている機能を最小限に抑えます。このテンプレートには、以下へのアクセスを無効にする設定が含まれています。
  - 印刷
  - クリップボード
  - 周辺機器
  - ドライブマッピング
  - ポートリダイレクト

- ユーザーデバイスでのFlashアクセラレーション

このテンプレートを適用すると、より多くの帯域幅を使用し、サーバーあたりのユーザー密度が低下する可能性があります。

組み込みテンプレートのデフォルト設定を使用することをお勧めしますが、**WANテンプレート**の**セッション全体の帯域幅制限**など、一部の設定は、管理者が展開固有の調整を行えるように未構成のままになっています。

テンプレートのデフォルト設定画像(/en-us/citrix-virtual-apps-desktops/current-release/media/template-default-settings.png)

XenAppおよびXenDesktop 7.6 FP3より前の展開（ポリシー管理およびVDA）を使用しているとします。また、高サーバー拡張性とWAN向け最適化テンプレートが必要です。この場合、該当する場合はこれらのテンプレートのレガシーOSバージョンを使用してください。

> **注:**
>
> 組み込みテンプレートはCitrixが作成および更新します。これらのテンプレートを変更または削除することはできません。

テンプレートの作成

テンプレートからテンプレートを作成するには：

1. Web Studio で、左側のペインで **ポリシー** を選択します。
2. **テンプレート**タブを選択し、テンプレートを作成する元のテンプレートを選択します。
3. **テンプレートの作成**タブを選択します。**設定の選択**画面が表示されます。
4. テンプレートに含めるポリシー設定を選択して構成します。
5. **次へ**をクリックします。**概要**画面が表示されます。
6. テンプレートの名前を入力します。
7. 「**完了**」をクリックします。新しいテンプレートが「**テンプレート**」タブに表示されます。

ポリシーに基づいてテンプレートを作成するには：

1. Web Studio で、左側のペインで **ポリシー** を選択します。
2. 「**ポリシー**」タブで、テンプレートを作成するポリシーを選択します。
3. 「**その他**」タブをクリックします。

4. 「**テンプレートとして保存**」を選択します。「**設定の選択**」画面が表示されます。
5. テンプレートに含める新しいポリシー設定を選択して構成します。
6. 「**次へ**」をクリックします。「**概要**」画面が表示されます。
7. テンプレートの名前と説明を入力し、「**完了**」をクリックします。

ポリシーの作成

> **注:**
>
> バージョン2511以降、Citrix Web Studio™（Webベース）は、Citrix Virtual Apps and Desktops™ の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

ポリシーは次の2つの部分を定義します。

- ユーザー、デバイス、または接続の種類ごとに、セッション、帯域幅、およびセキュリティがどのように管理されるかを定義する設定のグループ。
- ポリシーを割り当てるユーザーとマシン。ポリシーを作成する前に、それが影響するユーザーまたはデバイスのグループを決定します。職務、接続の種類、デバイスプラットフォーム、または地理的な場所に基づいてポリシーを作成することもできます。

ポリシーを作成するときは、ポリシーテンプレートの設定に基づいて、必要に応じてカスタマイズできます。また、最初から必要な設定を手動で追加することもできます。このセクションでは、次のトピックについて説明します。

- ポリシーの仕組み
- 最初からポリシーを作成する
- テンプレートからポリシーを作成する

> **ヒント**

> グループにポリシーが存在する場合は、新規作成するのではなく、既存のポリシーを編集することを検討してください。特定の設定を有効にするためだけ、または特定のユーザーを除外するためだけにポリシーを作成することは避けてください。

ポリシーの仕組み

ユーザーがログオンすると、接続の割り当てに一致するすべてのポリシーが特定されます。これらのポリシーは優先度順にランク付けされ、任意の設定の複数のインスタンスが比較されます。各設定について、最も優先度の高いポリシーの値が適用されます。優先度の高いポリシーが設定を無効にしている場合、その設定は、それが有効になっている優先度の低いポリシーを上書きします。構成されていない設定は無視されます。

> **重要:**
>
> グループポリシー管理コンソールを使用してActive DirectoryポリシーとCitrixポリシーの両方を構成している場合、割り当てと設定が期待どおりに適用されないことがあります。詳細については、CTX127461を参照してください。

フィルターなしのポリシー

「**Unfiltered**」というデフォルトポリシーを提供しています。

- Web StudioでCitrix®ポリシーを管理する場合、Unfilteredポリシーの設定は、サイト内のすべてのサーバー、デスクトップ、および接続に適用されます。
- 設定を適用するには、サイトと接続がポリシーを含むGPOのスコープ内にある必要があります。

  例: **Sales-US**という名前のGPOが**Sales** OUにリンクされており、すべての米国の営業チームメンバーが含まれています。このGPOは、いくつかのユーザー設定を含む**Unfiltered**ポリシーで構成されています。営業マネージャーがログオンすると、ユーザーが**Sales-US** GPOに属しているため、**Unfiltered**ポリシー設定が適用されます。

割り当てモード

割り当てモードは、接続基準がどのように一致するかに基づいてポリシーが適用されるかどうかを制御します。

- **許可** (デフォルト): 接続が割り当て基準に一致する場合にのみポリシーを適用します。
- **拒否**: 接続が基準に一致しない場合にポリシーを適用します。

例 1: 同じ割り当てタイプ、異なるモード

ポリシー1には以下が含まれます。

- 割り当てA: 営業グループ、モード = 許可
- 割り当てB: 営業マネージャーのアカウント、モード = 拒否

ユーザーは営業グループに属していますが、拒否割り当てが優先されます。営業マネージャーがログオンしても、ポリシーは適用されません。

例 2: 異なる割り当てタイプ、同じモード

ポリシー2には以下が含まれます。

- 割り当て C: 営業グループ (ユーザー)、モード = 許可
- 割り当て D: 企業 IP 範囲 (クライアント IP)、モード = 許可

ポリシーは、両方の割り当てが満たされた場合にのみ適用されます。営業マネージャーがオフィスからログオンした場合、両方の条件が満たされ、ポリシーが適用されます。

ポリシー 3 には以下が含まれます。

- 割り当て E: 営業グループ (ユーザー)、モード = 許可
- 割り当て F: NetScaler Gateway 接続 (アクセス制御)、モード = 許可

営業マネージャーがオフィスから (NetScaler 経由ではなく) ログオンした場合、割り当て F は満たされないため、ポリシーは適用されません。

ポリシー設定: 親子関係

一部のポリシー設定は親設定に依存します。たとえば、子設定が利用可能になる前に、**セッション全体の帯域幅制限**を構成する必要があります。

Web Studio でポリシーを構成するときは、子設定にカーソルを合わせると、どの親を最初に構成する必要があるかを確認できます。親が無効になっている場合、関連する子設定は自動的に無効になります。

依存ポリシー設定(/en-us/citrix-virtual-apps-desktops/current-release/media/dependent-policy-settings.png)

次の表に、親設定とそれに対応する子設定を示します。

親ポリシー	依存子ポリシー
セッション全体の帯域幅制限	オーディオリダイレクトの帯域幅制限（パーセント）
	クリップボードリダイレクトの帯域幅制限（パーセント）
	COMポートリダイレクトの帯域幅制限（パーセント）
	ファイルリダイレクトの帯域幅制限（パーセント）
	HDX™ MediaStreamマルチメディアアクセラレーションの帯域幅制限（パーセント）
	LPTポートリダイレクトの帯域幅制限（パーセント）
	プリンターリダイレクトの帯域幅制限（パーセント）
	クライアントUSBデバイスリダイレクトの帯域幅制限（パーセント）
	TWAINデバイスリダイレクト帯域幅制限の割合
双方向コンテンツリダイレクトを許可する	クライアントにリダイレクトされる許可されたURL
	VDAにリダイレクトされる許可されたURL
CPU使用率	CPU使用率から除外されるプロセスの優先度
レガシーグラフィックモード	プログレッシブ圧縮レベル
セッションウォーターマークを有効にする	ウォーターマークのカスタムテキスト
	セッションウォーターマークのスタイル
	透かしの透明度

親ポリシー	依存子ポリシー
HDXアダプティブトランスポート	オーディオのロストレラントモード

ポリシー設定の状態

一部のポリシー設定には、次のいずれかの状態があります。

- **許可**または**禁止**: 設定によって制御されるアクションを許可または防止します。ユーザーがセッション内で設定のアクションを管理することを許可または防止される場合があります。たとえば、メニューアニメーションが「許可」に設定されている場合、ユーザーはセッション内でそれを制御できます。
- **有効**または**無効**: 設定をオンまたはオフにします。優先度の高いポリシーで設定が無効になっている場合、優先度の低いポリシーで有効になっていても、その設定は適用されません。

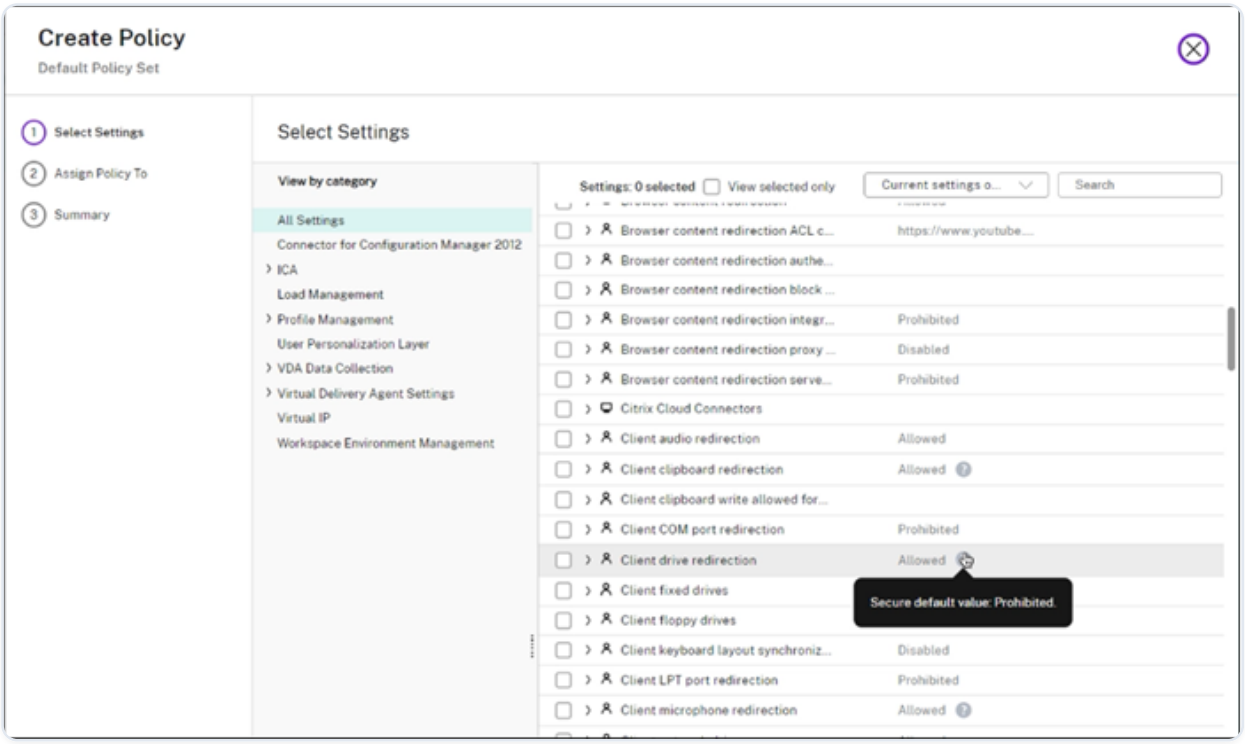
セキュアなデフォルト設定

VDAのインストール中にセキュアなデフォルト設定が有効になっている場合、ポリシー設定の優先順位は次のとおりです。

1. カスタマイズされた設定
2. セキュアなデフォルト設定
3. デフォルト設定

セキュアなデフォルト値を表示するには：

1. Web Studioで、左ペインの**ポリシー**をクリックします。
2. **ポリシー**タブで、**ポリシーの作成**をクリックします。
3. 「**設定の選択**」テーブルで、現在の値が「**許可**」になっている設定にマウスカーソルを合わせると、「**セキュアなデフォルト値: 禁止**」と表示されます。



ポリシー設定の有効性

一部の設定は、組み合わせて使用し、有効にする必要があります。たとえば、ユーザーがローカルデバイス上のネットワークドライブにアクセスできるようにするには、次の設定が必要です。

- **クライアントドライブリダイレクト**を有効にする必要があります
- **クライアントネットワークドライブ**も含まれている必要があります

クライアントドライブリダイレクトが無効になっている場合、**クライアントネットワークドライブ**が有効になっていても、ユーザーはネットワークドライブにアクセスできません。

一般に、マシン関連の設定の変更は、VDAが再起動するか、ユーザーがログオンしたときに有効になります。ユーザー関連の設定の変更は、次回のログオン時に適用されます。

ポリシーに設定を追加する際、「デフォルト値を使用」を選択して変更を防止できます。このオプションは手動設定を無効にし、以前に入力された値に関係なく、デフォルト値のみを適用します。

ベストプラクティス

- ポリシーは個々のユーザーではなく、グループに割り当ててください。グループにポリシーを割り当てると、グループにユーザーを追加または削除したときに、割り当てが自動的に更新されます。
- 使用されていないポリシーは無効にしてください。設定が追加されていないポリシーは、不要な処理オーバーヘッドを発生させます。

ポリシーを最初から作成する

ポリシーを作成するには：

1. Web Studioで、左ペインの**ポリシー**をクリックします。
2. 「**ポリシー**」タブで、「**ポリシーの作成**」をクリックします。
3. 「**設定の選択**」ページで、設定を選択して構成し、「**次へ**」をクリックします。
4. 「**ポリシーの割り当て先**」ページで、このポリシーが存在するポリシーセットを選択し、ポリシーを割り当てるオブジェクトを選択します。「**次へ**」をクリックします。
5. 「**概要**」ページで、次の設定を完了します。
   a. ポリシーの名前と説明を入力します。
   b. ポリシーを有効にするには、「**ポリシーを有効にする**」を選択します。
6. **完了**をクリックします。

ステップ1：ポリシー設定の選択と構成

ポリシー設定は機能別にグループ化されています。たとえば、プロファイル管理に関連する設定は、「**プロファイル管理**」カテゴリにあります。

設定には次の2種類があります。

- **コンピューター設定**：マシンに適用され、仮想デスクトップの起動時（ユーザーがログオンしていなくても）に有効になります。これらは仮想デスクトップの動作を定義します。
- **ユーザー設定**：ユーザーが接続または再接続したときに適用されます。これらはユーザーエクスペリエンスを定義します。

設定を選択して構成するには：

1. 「**設定の選択**」ページで、VDAバージョン別に設定を表示するには、右上のドロップダウンリストオプションから次のいずれかを選択します。
   - **すべての設定**：すべてのVDAバージョンのすべての設定を表示します
   - **現在の設定のみ**：現在のVDAバージョンにのみ設定を表示
   - **レガシー設定のみ**：非推奨のVDAバージョンにのみ設定を表示
2. 設定を検索するには、検索ボックスに設定の完全な名前または部分的な名前を入力します。
3. 設定を選択します。**有効**をクリックしてオンにするか、**編集**をクリックして値を指定します。
4. ステップ3を繰り返して、ポリシーの他の設定を選択して構成します。

注:

ポリシー設定は、有効、無効、または未構成にすることができます。デフォルトでは、ポリシー設定は構成されていません。つまり、ポリシーに追加されていません。設定は、ポリシーに追加された場合にのみ適用されます。

ステップ2：ポリシー割り当てを指定する

ポリシー割り当ては、ポリシーが適用されるユーザーとマシンを定義します。割り当てがポリシーの動作にどのように影響するかについては、「ポリシーのしくみ」を参照してください。

ポリシー割り当てを指定するには：

1. **ポリシーの割り当て先**ページで、**フィルターされたユーザーとコンピューター**を選択します。
2. 割り当て（*フィルター*とも呼ばれます）を指定して、ユーザーまたはコンピューターを選択します。利用可能な割り当てタイプについては、次の表を参照してください。

注:

- 割り当てを指定しないか、無効にした場合、ポリシーは**すべて**の接続に適用されます。
- ポリシーの*割り当て*は、ポリシーの*フィルター*とも呼ばれます。詳細については、「ポリシーのフィルターを作成、変更、または削除する」および「フィルターはどのように適用されますか？」を参照してください。

割り当て名	ポリシーの適用基準
アクセスコントロール	クライアントが接続しているアクセス制御条件。*接続の種類* - NetScaler® Gatewayを使用する接続と使用しない接続のどちらにポリシーを適用するか。*NetScaler Gatewayファーム名* - NetScaler Gateway仮想サーバーの名前。*アクセス条件* - 使用するエンド

割り当て名	ポリシーの適用基準
	ポイント分析ポリシーまたはセッションポリシーの名前。
NetScaler SD-WAN	ユーザーセッションがNetScaler SD-WANを介して起動されるかどうか。**注:** 1つのポリシーにNetScaler SD-WANの割り当てを1つだけ追加できます。
クライアントIPアドレス	クライアントが接続しているIPアドレス。これは、クライアントがセッションに接続する方法によって異なります。 - 直接内部ネットワーク接続: IPアドレスはクライアントのプライベートIPアドレスになります。 - NetScaler Gateway接続: IPアドレスはNetScalerのサブネットIPアドレスになります。 - ゲートウェイサービス接続。 - Rendezvousが無効になっている場合、IPアドレスはCloud ConnectorのIPアドレスのいずれかになります。 - Rendezvousが有効になっている場合、IPアドレスはGateway Serviceの

割り当て名	ポリシーの適用基準	
	パブリックIPアドレスになります。 IPv4の例: 12.0.0.0, 12.0.0.*, 12.0.0.1-12.0.0.70, 12.0.0.1/24; IPv6の例: 2001:0db8:3c4d:0015:0:0:abcd:ef12, 2001:0db8:3c4d:0015::/54	
クライアント名	ユーザーデバイスの名前。完全一致: ClientABCName。ワイルドカードの使用: Client*Name。	
デリバリーグループ	デリバリーグループのメンバーシップ。	
クライアントプラットフォーム	セッションへの接続に使用されるユーザーデバイスのOSタイプ（Windows、Linux、iOS、Android、HTML5など）。必要なVDAバージョン: 2503以降。	
デリバリーグループの種類	デスクトップまたはアプリケーションの種類: プライベートデスクトップ、共有デスクトップ、プライベートアプリケーション、または共有アプリケーション。**注:** プライベートデスクトップと共有デスクトップのフィルターオプションは、Citrix Virtual Apps and Desktops 7.xでのみ利用可能です。詳細については、	

割り当て名	ポリシーの適用基準
	CTX219153を参照してください。
組織単位 (OU)	組織単位。
タグ	タグ。**注:** このポリシーをすべてのタグ付きマシンに適用します。アプリケーションタグは含まれません。
ユーザーまたはグループ	ユーザーまたはグループ名。

ユーザーがログオンすると、接続の割り当てに一致するすべてのポリシーが特定されます。これらのポリシーは優先順位順に並べ替えられ、設定の複数のインスタンスが比較されます。各設定は、ポリシーの優先順位に従って適用されます。無効になっているポリシー設定は、有効になっている下位ランクの設定よりも優先されます。構成されていないポリシー設定は無視されます。

重要:

グループポリシー管理コンソールを使用してActive DirectoryポリシーとCitrixポリシーの両方を構成する場合、割り当てと設定が期待どおりに適用されないことがあります。詳細については、CTX127461を参照してください。

クライアントIPポリシーフィルターが常にクライアントのプライベートIPアドレスを使用するように設定するには、セッションホストで次のレジストリ設定を構成します。

- キー: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Ica\GroupPolicy`
- 値の型: `DWORD`
- 値の名前: `UseClientDeviceIpForPolicyFilter`
- 値のデータ: `1`

「Unfiltered」という名前のポリシーがデフォルトで提供されます。

- Web Studio を使用して Citrix ポリシーを管理する場合、Unfiltered ポリシーに追加した設定は、サイト内のすべてのサーバー、デスクトップ、および接続に適用されます。
- ローカルグループポリシーエディターを使用して Citrix ポリシーを管理する場合、Unfiltered ポリシーに追加した設定は、すべてのサイトと接続に適用されます。サイトと接続は、ポリシーを含むグループポリシーオブジェクト (GPO) のスコープ内にある必要があります。たとえば、Sales OU には、米国の営業チームのすべてのメンバーを含む Sales-US という GPO が含まれています。Sales-US GPO は、いくつかのユーザーポリシー設定を含む Unfiltered ポリシーで構成されています。米国の営業マネージャーがサイトにログオンすると、Unfiltered ポリシーの設定がセッションに自動的に適用されます。この構成は、ユーザーが Sales-US GPO のメンバーであるためです。

割り当てのモードは、ポリシーがすべての割り当て基準に一致する接続にのみ適用されるかどうかを決定します。モードが (デフォルト) に設定されている場合、ポリシーは割り当て基準に一致する接続にのみ適用されます。モードが に設定されている場合、接続が割り当て基準に一致しない場合にポリシーが適用されます。以下の例は、複数の割り当てが存在する場合に割り当てモードが Citrix ポリシーにどのように影響するかを示しています。

- **例: モードが異なる同種の割り当て** - 同じ種類の2つの割り当てがあり、一方が に設定され、もう一方が に設定されているポリシーでは、接続が両方の割り当てを満たす場合、 に設定された割り当てが優先されます。例:

  ポリシー 1 には次の割り当てが含まれます。

  - 割り当て A は Sales グループを指定します。モードは に設定されています。
  - 割り当て B は営業マネージャーのアカウントを指定します。モードは に設定されています。

  割り当て B のモードが に設定されているため、ユーザーが Sales グループのメンバーであっても、営業マネージャーがサイトにログオンしたときにポリシーは適用されません。

- **例: モードが同じでタイプが異なる割り当て** - タイプが異なる2つ以上の割り当てがあり、 に設定されているポリシーでは、ポリシーが適用されるためには、接続が各タイプの少なくとも1つの割り当てを満たす必要があります。例:

  ポリシー 2 には次の割り当てが含まれます。

  - 割り当て C は、Sales グループを指定するユーザー割り当てです。モードは に設定されています。
  - 割り当て D は、10.8.169.* (企業ネットワーク) を指定するクライアント IP アドレス割り当てです。モードは に設定されています。

営業マネージャーがオフィスからサイトにログオンすると、接続が両方の割り当てを満たすため、ポリシーが適用されます。

ポリシー3には、次の割り当てが含まれます。

- 割り当てEは、営業グループを指定するユーザー割り当てです。モードは「許可」に設定されています。
- 割り当てFは、NetScaler Gatewayの接続条件を指定するアクセスコントロール割り当てです。モードは「許可」に設定されています。

営業マネージャーがオフィスからサイトにログオンしても、接続が割り当てFを満たさないため、ポリシーは適用されません。

テンプレートからポリシーを作成する

Citrix 提供またはカスタムテンプレート に基づいてポリシーを作成できます。結果として作成されるポリシーは、元のテンプレートとは独立しています。

テンプレートからポリシーを作成するには:

1. Web Studio で、左側のペインで **ポリシー** を選択します。
2. 「**テンプレート**」タブを選択し、使用するテンプレートを選択します。
3. アクションバーで「**テンプレートからポリシーを作成**」をクリックします。「**ポリシーの作成**」ページが表示され、選択したテンプレートで事前設定されたすべての設定が表示されます。
4. 必要に応じて設定を変更し、さらに設定を追加してから、「**次へ**」をクリックします。
5. 「**ポリシーの割り当て先**」ページで、このポリシーが存在するポリシーセットを選択し、ポリシーを割り当てるオブジェクトを選択します。「**次へ**」をクリックします。
6. 「**概要**」ページで、ポリシーの名前と説明を入力します。
7. 「**完了**」をクリックします。新しいポリシーは、「**ポリシー**」タブの指定されたポリシーセットに表示されます。

次のステップ

- ポリシーの優先順位付け
- ポリシーのシミュレーションと評価

ポリシーセットの作成

注:

バージョン2511以降、Citrix Web Studio™（Webベース）は、Citrix Virtual Apps and Desktops™ の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

ポリシーセットは、簡素化されたロールベースのアクセスと容易な管理を可能にするためにポリシーを集約する、Citrix Virtual Apps and Desktops™ のオブジェクトです。作成されると、スコープとデリバリーグループがポリシーセットに割り当てられ、承認された管理者のみが、関連するユーザーとマシンに適用されるポリシーを管理できるようになります。

ポリシーセットは、Citrix® ポリシーを論理グループに編成することで、より効率的に管理するのに役立ちます。ポリシーセットをデリバリーグループに割り当てると、デリバリーグループはそのセット内のポリシーのみを使用します。

このセクションでは、ポリシーセットの動作、作成および割り当て方法、ならびにスコープとフィルターとの相互作用について説明します。

利点

ポリシーセットには、いくつかの主要な利点があります。

- 分散型管理者チーム向けのロールベースのアクセス制御
- 合併、買収、および統合の簡素化
- 制限された障害ドメイン
- ポリシーのマルチテナントサポート

次の表は、ポリシーがポリシーセットの有無にかかわらずどのように機能するかを比較したものです。

ポリシーセットなし	ポリシーセットあり
すべてのポリシー、設定、フィルター（割り当て）、および優先度は、1つの中央の場所で管理されます。	各ポリシーセットには、独自のポリシー、設定、フィルター（割り当て）、および優先度があります。

ポリシーセットなし	ポリシーセットあり
1つのポリシーを管理する場合、すべてのポリシーを管理する必要があります。	フル管理者は、特定のポリシーセットを個別に管理する機能を下位レベルの管理者に委任できます。
大規模で分散された環境のポリシーは、複雑になり管理が困難になります。	大規模で分散された環境のポリシーは、簡単に分割して管理できます。

動作の仕組み

ポリシーセットはデリバリーグループに割り当てられ、特定の管理者にスコープが設定されます。セット内のポリシーは、引き続きフィルター（割り当て）を使用して、どのユーザーまたはマシンに適用されるかを決定します。

主な動作:

- ポリシーセットはデリバリーグループに割り当てられます
  - デリバリーグループは一度に1つのポリシーセットのみを使用できます。
  - 1つのポリシーセットを複数のデリバリーグループに割り当てることができます。
  - デリバリーグループにポリシーセットが割り当てられていない場合、**Default Policy Set**が使用されます。
- ポリシーがセット内にあるかどうかにかかわらず、ポリシーのフィルターは引き続き適用されます。
- ポリシーセットには、1つまたは複数のスコープを設定できます。
  - スコープは、管理者が管理できるオブジェクト（例: 接続、カタログ、デリバリーグループ、アプリケーショングループ）のコレクションを表します。
  - 管理者は、承認された管理者のみがポリシーセットを表示または編集できるように、ポリシーセットのスコープを定義できます。スコープは、ポリシーセットの作成時または後でセットを編集するときに設定できます。
- **Default Policy Set**は、デフォルトで**Bypass scope control for this resource**が選択されています。この設定により、ポリシーセットはすべての管理者から引き続き表示されます。スコープ制御を適用するには、ポリシーセットを編集し、**Bypass scope control for this resource**チェックボックスをオフにしてから、目的のスコープを選択します。

ポリシーフィルターと割り当ては、ポリシーセットがない場合と同じように機能します。詳細については、「フィルターの適用方法」を参照してください。

ポリシーセットを有効にする

Web Studioで、 > に移動し、 設定をオンにします。

> **注:**
>
> - ポリシーセットを作成する前に、ポリシーセットを有効にする必要があります。
> - ポリシーセットを有効にすると、既存のすべてのポリシーが**デフォルトポリシーセット**にグループ化されます。このセットは、別のセットを割り当てない限り、すべてのデリバリーグループに自動的に割り当てられます。新しいポリシーセットがデリバリーグループに割り当てられると、そのグループはデフォルトポリシーセットの使用を停止します。

ポリシーセットを作成する

管理者チームや会社の論理的な区分を反映するようにポリシーセットを作成できます。たとえば、地理的地域、事業部門、または特定のユースケースごとにポリシーセットを作成できます。

ポリシーセットは次の2つの方法で作成できます。

- ポリシーセットを最初から作成する
- 既存のポリシーセットをコピーして作成する

または、Citrix Virtual Apps and Desktops PowerShell SDKを使用してポリシーセットを作成および管理することもできます。

ポリシーセットを最初から作成する

1. Web Studioで、左ペインの**** ノードを選択します。
2. タブをクリックします。
3. を選択します。
4. タブをクリックし、ポリシーセットの名前と説明を入力します。
5. 「**割り当て**」タブをクリックし、1つ以上のデリバリーグループを選択します。
6. 「**スコープ**」タブをクリックし、ポリシーセットを適用できるオブジェクトを定義するスコープを選択します。
7. 「**作成**」をクリックして完了します。

ポリシーセットの複製

1. Web Studioで、左側のペインにある「**ポリシー**」ノードを選択します。
2. 「**ポリシー**」タブをクリックします。
3. 「**ポリシーセットの複製**」を選択します。
4. ポリシーセットの名前を更新します。
5. ポリシーセットの割り当てを更新または作成し、「**次へ**」をクリックします。
6. 複製されたポリシーセットに含めるポリシーを選択またはクリアします。
7. ポリシーのスコープを更新します。
8. **作成**をクリックします。

ポリシーの優先順位付け

> **注:**
>
> バージョン2511以降、Citrix Web Studio™（Webベース）は、Citrix Virtual Apps and Desktops™ の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

> 複数のポリシーが接続に適用される場合、Citrix Virtual Apps and Desktops™ はそれらを優先順位に従って評価します。数値が小さいほど優先度が高くなります (1が最高)。ポリシー間で競合する設定が存在する場合、最も優先度の高いポリシーの設定が適用されます。

Web Studio または PowerShell を使用してポリシーの優先順位を変更できます。

Web Studio を使用してポリシーの優先順位を変更する

1. **Web Studio** で、左ペインの **ポリシー** を選択します。
2. **ポリシー** タブで、アクションバーから **ポリシーの優先順位の変更** を選択します。
3. **ポリシーの優先順位の変更** ページで、以下のいずれかの方法を使用してポリシーの順序を変更します。
   - ポリシーをドラッグして目的の位置に移動します。
   - **上** または **下** 矢印アイコンをクリックして、1つ位置を移動します。

- **一番上** または **一番下** 矢印アイコンをクリックして、最初または最後の位置に移動します。
- **編集** アイコンをクリックし、優先順位番号を入力して、**保存** をクリックします。

4. **保存** をクリックして変更を適用します。

PowerShell を使用してポリシーの優先順位を変更する

`Set-GpoPolicyPriority.ps1` スクリプトを使用して、プログラムでポリシーの優先順位を並べ替えます。このスクリプトは、ポリシー名とターゲットの優先順位番号を受け入れ、内部でポリシー GUID を解決し、`Set-BrokerGpoPolicyPriorities` を使用して更新された順序を適用します。Web Studio コンソールの代わりに自動化によってポリシーの優先順位を管理する場合に、このアプローチを使用します。

ネイティブの `Set-BrokerGpoPolicyPriorities` コマンドレットは、ポリシー GUID の完全に順序付けられたリストを必要とします。このスクリプトは、ポリシー名と希望する優先順位を受け入れることでその複雑さを解消し、その後、GUID の解決を自動的に処理します。

始める前に

スクリプトを実行する前に、以下の要件を満たしていることを確認してください。

- Broker SDKがインストールされた、サポート対象のCitrix Virtual Apps and Desktopsのバージョン
- スクリプトは、Citrix Broker SDKがインストールされたDelivery Controller™で実行する必要があります。
- PowerShellスナップイン: `Citrix.Broker.Admin.V2` (スクリプトによって自動的にロードされます)

スクリプトを実行する

1. `Set-GpoPolicyPriority.ps1`をDelivery Controllerにコピーします。
2. Delivery Controller で PowerShell セッションを開きます。
3. 必要なパラメーターを指定してスクリプトを実行します。

```
.\Set-GpoPolicyPriority.ps1 -PolicyName "<PolicyName>" -NewPriority
<Number>
```

`<PolicyName>`をポリシー名に、`<Number>`をターゲットの優先順位に置き換えます。

スクリプトは、現在の優先順位とターゲットの優先順位を出力し、変更を確認し、検証ステップを実行します。スクリプトが適用する前の並べ替えの詳細を表示するには、`-Verbose`を追加します。

パラメーター

パラメーター	必須	説明
`-PolicyName`	はい	優先順位を変更するポリシーの名前
`-NewPriority`	はい	ターゲットの優先順位 (1 = 最高)。ポリシーを最高位に移動するには0または負の数を使用し、最下位に移動するにはポリシー数を超える数を使用します。
`-PolicySetGuid`	いいえ	特定のポリシーセットのGUID。`DefaultSitePolicies`をターゲットにする場合は省略します。

例

デフォルトのポリシーセットでポリシーを最高の優先順位に設定します。

```
.\Set-GpoPolicyPriority.ps1 -PolicyName "MyPolicy" -NewPriority 1
```

ポリシーを最低の優先順位に設定します。

```
.\Set-GpoPolicyPriority.ps1 -PolicyName "MyPolicy" -NewPriority 9999
```

特定のポリシーセットでポリシーを優先順位5に設定します。

```
.\Set-GpoPolicyPriority.ps1 -PolicyName "MyPolicy" -NewPriority 5
-PolicySetGuid "12345678-1234-1234-1234-123456789012"
```

ポリシー割り当ての例外を管理する

> **注:**
>
> バージョン2511以降、Citrix Web Studio™（Webベース）は、Citrix Virtual Apps and Desktops™ の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

フィルターを使用してユーザー、ユーザーデバイス、またはマシンのグループにポリシーを割り当てるとき、グループの一部のメンバーには異なる設定が必要になる場合があります。このような場合でも、個々のメンバーごとに完全に個別のポリシーを作成することなく対応できます。

グループ内の特定のユーザーまたはマシンに対して、次の方法で例外を作成できます。

- それらのグループメンバー専用の個別のポリシーを作成し、より高い優先順位を付与する
- ポリシーに追加された割り当てに*拒否*モードを使用する

例外に拒否モードを使用する

モードが*拒否*に設定された割り当ては、ポリシーが割り当て基準に一致しない接続に適用されることを意味します。たとえば、ポリシーに次の割り当てが含まれているとします。

- *割り当てA*: クライアントIPアドレス割り当て範囲 `208.77.88.*`、モード = *許可*。
- *割り当てB*: 特定のユーザーアカウント、モード = *拒否*。

このポリシーは、指定されたIP範囲から接続するユーザーに適用されますが、*割り当てB*で定義されたユーザーは**除外**されます。

> **注:**
>
> **ポリシーの割り当て**手順で、**有効にする**チェックボックスをオフにすると、割り当てが無効になります。ポリシーに有効な割り当てがない場合、そのポリシーはサイト内のすべてのオブジェクトに適用されます。

関連コンテンツ

- ポリシーの優先順位付け
- ポリシーのシミュレーションと評価

ポリシーのシミュレーションと評価

注:

バージョン2511以降、Citrix Web Studio™（Webベース）は、Citrix Virtual Apps and Desktops™ の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

Web Studioの比較ツールとポリシーモデリングツールを使用して、構成の検証、ポリシーの動作テスト、および展開前にどの設定が適用されるかの評価を行います。

注:

- **モデリング**タブは、お客様のリクエストによって有効にされた場合にのみ利用できます。
- フィルターが適用された有効なポリシーのみがモデル化されます。無効なポリシーは適用されません。フィルターが適用されていない有効なポリシーは常に適用されます。

ポリシーとテンプレートの比較

Web Studioの比較機能を使用して、ポリシー、テンプレート、またはデフォルト設定間の違いを表示します。これにより、構成の一貫性を検証し、ベストプラクティスへの準拠を維持し、予期しない動作のトラブルシューティングを行うことができます。

次のことができます。

- ポリシーまたはテンプレートの設定を別のものと比較する
- 設定をデフォルト値と比較する

- ポリシー間の競合する構成または不足している構成を特定する

ポリシーとテンプレートを比較するには：

1. Web Studio で、左側のペインで **ポリシー** を選択します。
2. **比較**タブをクリックし、**選択**をクリックします。
3. 比較するポリシーまたはテンプレートを選択します。
4. （オプション）デフォルトを含めるには、**デフォルト設定と比較**を選択します。
5. **比較**をクリックします。設定が列に表示されます。
    - すべての設定を表示するには、**すべての設定を表示**を選択します。
    - デフォルトビューに戻るには、「**共通設定の表示**」を選択します。

ポリシーモデリングウィザードを実行する

1. Web Studioで、**ポリシー**を選択します。
2. 「**モデリング**」タブを選択します。
3. アクションバーで**ポリシーモデリング**を選択します。
4. 「**はじめに**」ページを読み、「**次へ**」をクリックします。
5. ユーザーまたはコンピューターを選択します。コンテナー、特定のユーザー、またはコンピューターを参照することもできます。「**次へ**」をクリックします。
6. フィルターエビデンスを選択します。オプションで、「**デリバリーグループ**」、「**タグ**」、「**クライアントIPアドレス**」などの詳細を指定してシミュレーションを絞り込むことができます。「**次へ**」をクリックします。
7. 概要を確認し、「**実行**」をクリックします。

モデリング結果の表示と管理

ウィザードの実行後、確認、操作、エクスポートが可能なレポートが生成されます。

レポートを確認する

- ドロップダウンメニューを使用して、「**すべての設定**」、「**コンピューター設定**」、または「**ユーザー設定**」を表示します。
- 特定の設定を検索します。
- 設定をクリックして、それが適用された理由または適用されなかった理由を確認します。
- 結果をJSONまたはHTML形式でエクスポートします。

レポートの管理

シミュレーションの実行後、アクションバーで次のオプションが利用可能です。

オプション	説明
モデリングレポートの表示	結果を確認またはエクスポートします。
ポリシーモデリングの再実行	同じ基準を使用して再度実行します。
モデリングレポートの削除	現在のレポートを削除します。

結果ポリシーセットを使用してポリシー適用を評価する

接続が期待どおりに動作しない場合、ポリシーの競合が原因である可能性があります。優先度の高いポリシーは、他のポリシーを上書きできます。結果ポリシーセット（RSoP）を使用して、特定の接続にどの設定が適用されるかを評価します。

2つのRSoPメソッドが利用可能です。

- **Citrixグループポリシーモデリングウィザード**

  ユーザーと割り当て条件を指定して、接続シナリオをシミュレートします。

- **グループポリシーの結果**

  ユーザーとVirtual Delivery Agent (VDA) に適用されるCitrixポリシーのレポートを生成します。

> **注:**
>
> **Web Studio** で作成されたサイトポリシー設定は、グループポリシー管理コンソール (GPMC) からCitrixグループポリシーモデリングウィザードを実行しても、ポリシーの結果セットには含まれません。最も包括的な結果を得るには、GPMCのみを使用してポリシーを作成する場合を除き、**Web Studio** からポリシーモデリングウィザードを開始してください。

ポリシーの問題のトラブルシューティング

ユーザー、IPアドレス、およびその他の割り当てられたオブジェクトには、複数のポリシーが同時に適用される可能性があり、予期しない動作につながることがあります。

ポリシーモデリングウィザードを実行してもユーザー接続にポリシーが適用されない場合、次の理由が考えられます。

- 評価基準に一致する割り当てを持つポリシーがない。
- 割り当てに一致するポリシーに設定が構成されていない。
- 割り当てに一致するポリシーが無効になっている。

これらの問題を解決するには：

- 関連するポリシーを有効にします。
- 各ポリシーに少なくとも1つの設定を構成します。

> **注:**
>
> ダブルホップシナリオ（たとえば、シングルセッションOS VDAがマルチセッションOS VDAに接続する場合）では、Citrixポリシーはシングルセッション OS VDAをユーザーデバイスとして扱います。セカンドホップ用にキャッシュされたイメージは、ファーストホップマシンに適用されます。

Directorで適用済みポリシーを表示する

管理者以外のユーザーは、**Director** を使用して、ユーザーセッションに適用されるポリシーを表示できます。これは、Web Studioへのアクセスを必要とせずに、どのポリシー設定が有効になっているかを確認するのに役立ちます。

レガシーMMCグループポリシーテンプレートをWeb Studioに移行する

> **注:**
>
> バージョン2511以降、Citrix Web Studio™（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

> レガシーMMC Studioグループポリシーテンプレートは、MMC Studioが実行されているローカルコンピューターの管理者のユーザープロファイルに保存されます。Web Studioテンプレートはサイトデータベースに保存され、どのコンピューターからでもすべての管理者がアクセスできます。これら2つの形式間には直接のエクスポートまたはインポートパスがないため、ポリシーを仲介役として使用してレガシーテンプレートを移行します。

始める前に

- レガシーテンプレートが保存されているMMC Studioのインストールにアクセスできることを確認してください。
- Web Studioが同じCitrix Virtual Apps and Desktops™サイトにアクセスできることを確認してください。
- 移行後に設定を確認できるように、レガシーテンプレートの設定をメモしておいてください。

テンプレートを移行する

1. MMC Studioで、移行したいテンプレートに移動します。
2. **アクション**ペインで、**テンプレートからポリシーを作成**を選択します。
3. ウィザードに従ってポリシーを作成します。便宜上、テンプレートと同じ名前を使用してください。
4. ポリシーがWeb Studioに表示されるまで最大5分間待ちます。この時間は、サイトサービスがポリシーデータをMMC形式からWeb Studio形式に変換するために必要です。
5. Web Studioを開き、左ペインで**ポリシー**を選択します。
6. ポリシーリストにポリシーが表示されていることを確認します。
7. ポリシーを選択し、リボンで**...その他**を選択して**テンプレートとして保存**をクリックします。
8. ウィザードに従ってWeb Studioテンプレートを作成します。

移行後、テンプレートはサイトデータベースに保存され、任意のコンピューターからWeb Studioを使用するすべての管理者がアクセスできます。

移行の確認

1. Web Studioで、**Policies**ノードの**Templates**タブを選択します。
2. 移行されたテンプレートが表示されていることを確認します。
3. 設定が元のMMCテンプレートと一致することを確認するために比較します。

移行を確認したら、元のMMCテンプレートを廃止できます。MMCテンプレートは、作成されたコンピューターにローカルに残ります。

例

次の例は、複数のサイトで共有されるウォーターマーク構成を含む、*Watermark Settings*という名前のテンプレートを移行する方法を示しています。

1. MMC Studioで、*Watermark Settings*テンプレートを見つけます。**Actions**ペインで、**Create Policy from Template**をクリックします。

   MMCテンプレート(/en-us/citrix-virtual-apps-desktops/current-release/media/policy-migrate-example1.png)

2. ウィザードに従ってポリシーを作成します。便宜上、テンプレートと一致するようにポリシーに*Watermark Settings*という名前を付けます。

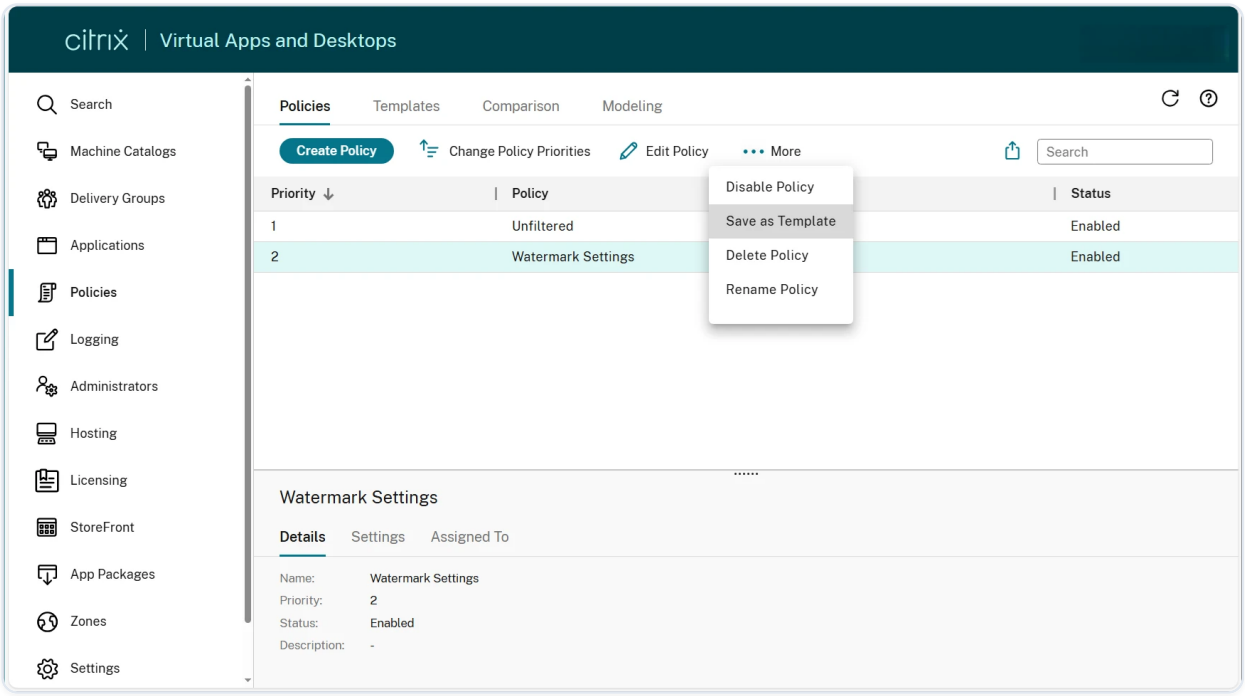
   テンプレートからポリシーを作成(/en-us/citrix-virtual-apps-desktops/current-release/media/policy-migrate-example2.png)

3. 最大5分間待ってからWeb Studioを開きます。ポリシーリストに*Watermark Settings*ポリシーが表示されていることを確認します。

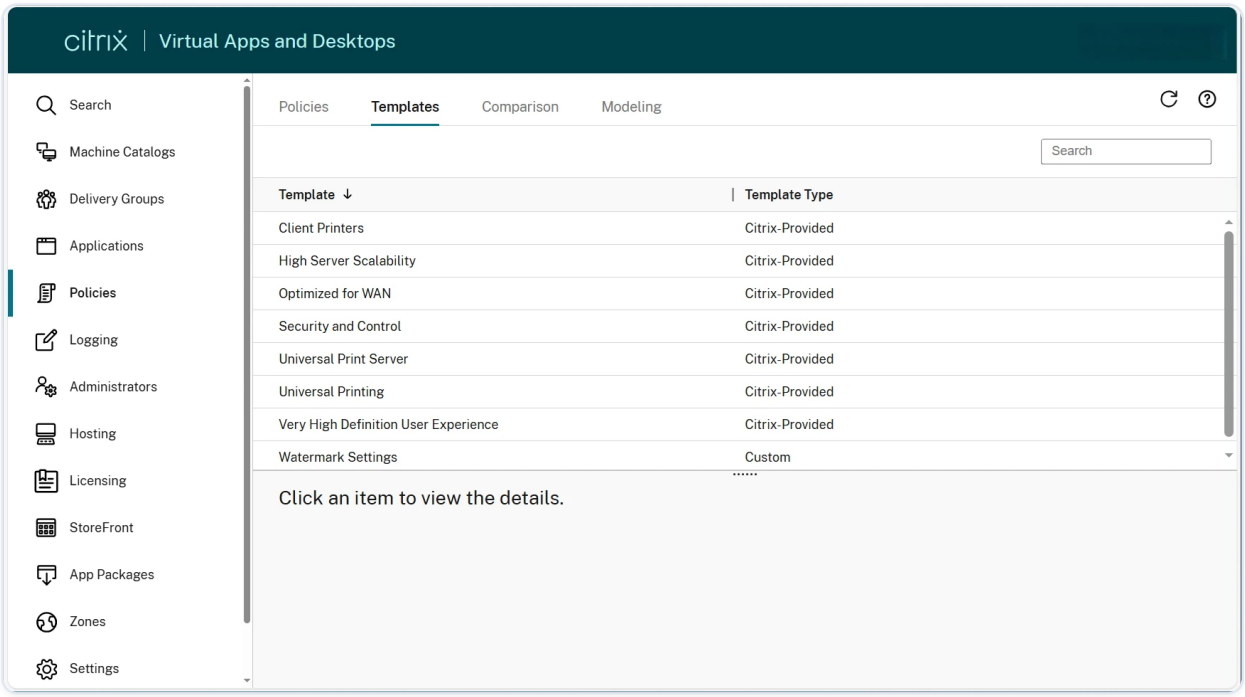
   Web Studioでポリシーを表示(/en-us/citrix-virtual-apps-desktops/current-release/media/policy-migrate-example3.png)

   > **注:**
   >
   > この時点では、テンプレートはまだ**Templates**タブに表示されません。ポリシーは仲介役であり、次のステップでWeb Studioテンプレートを作成するために使用します。

4. *Watermark Settings*ポリシーを選択し、リボンで**... More**を選択して**Save as Template**をクリックします。



5. ウィザードに従ってWeb Studioテンプレートを作成します。
6. 「**テンプレート**」タブを選択します。*Watermark Settings*テンプレートは、サイトにアクセスできるすべてのコンピューターから、すべての管理者が表示およびアクセスできるようになりました。



関連コンテンツ

Web Studioでのテンプレートの管理について詳しくは、「ポリシーテンプレートの管理」を参照してください。

アップグレード後に非推奨のポリシー設定を削除する

Citrix® が製品コンポーネントを非推奨にすると、それに関連するポリシー設定は無効になります。アップグレード後、`GpoClean.ps1` を使用して、Citrix Virtual Apps and Desktops™ ポリシーからこれらの非推奨設定を特定して削除します。これには、結果として空になるポリシーも含まれます。

始める前に

スクリプトを実行する前に、以下の要件を満たしていることを確認してください。

- **Broker SDK** と **Group Policy Management** がインストールされている、サポート対象バージョンの Citrix Virtual Apps and Desktops
- Delivery Controller™ 上での **Citrix ポリシー管理** 権限

> **注:**
>
> スクリプトは、`Citrix.Broker.Admin.V2` と `Citrix.Common.GroupPolicy` スナップインを自動的にロードします。

非推奨のポリシー設定を削除する

非推奨のポリシー設定を削除するには、`GpoClean.ps1` を実行します。

1. **Citrix policy administration** 権限を持つ Delivery Controller に `GpoClean.ps1` をコピーします。
2. Delivery Controller で PowerShell セッションを開きます。
3. スクリプトを実行します。パラメーターは不要です。

```
.\GpoClean.ps1
```

> **注:**
>
> 設定ごとの詳細なログ記録には、`-Verbose` を追加します: `.\GpoClean.ps1 -Verbose`。

スクリプトは2つのフェーズで実行されます。

フェーズ	内容
フェーズ 1	`Test-BrokerDesktopPolicy`を実行し、`DeprecatedSetting`エラーを特定し、影響を受ける各設定を`NotConfigured`に設定します
フェーズ 2	`Test-BrokerDesktopPolicy`を再実行し、設定されていないポリシー(`PolicyHasNoSettings`)を特定し、それらを削除します

すべての変更は、1回の書き込み操作で保存されます。概要には、削除された設定とポリシーの数が報告されます。非推奨の設定が見つからない場合、スクリプトは変更なしで終了します。

注:

- `Unfiltered`ポリシーは、設定が含まれていない場合でも削除されません。

スクリプト

以下のコンテンツを`GpoClean.ps1`として保存し、次に、非推奨のポリシー設定を削除するで説明されているように実行します。

```
<#

.Synopsis



    Cleans up deprecated settings from Citrix policies and removes
policies that no longer have any settings.



.Description
```

```
    This script runs Test-BrokerDesktopPolicy to identify deprecated
settings in policies. When a setting is

    deprecated (DeprecatedSetting error), the script removes the setting
from the policy using the Citrix Group Policy

    PowerShell Provider. After removing deprecated settings, if a policy
has no settings remaining

    (PolicyHasNoSettings error), the policy is removed automatically,
except for the 'Unfiltered' policy which is

    preserved.



    This script is useful for cleaning up policies after upgrading to a
newer version where some settings have been

    deprecated.



.Requirements



    Run this script on a DDC that has the Citrix Group Policy Management
and Citrix Broker SDK installed.

#>



[CmdletBinding()]

param()



Write-Host "Checking Citrix policies for deprecated settings..."
```

```
# Load the Citrix Broker PowerShell Snapin.
$BrokerSnapin = "Citrix.Broker.Admin.V2"
$loaded = Get-PSSnapin $BrokerSnapin -ErrorAction SilentlyContinue
if ($loaded -eq $null)
{
    Add-PSSnapin $BrokerSnapin
}

# First pass: Run Test-BrokerDesktopPolicy to check for errors.
Write-Host "Running policy validation..."
$testResults = Test-BrokerDesktopPolicy | Select-Object -Property *

if ($testResults -eq $null -or $testResults.Count -eq 0)
{
    Write-Host "No policy errors found. All policies are clean."
    exit 0
}

# Check if there are any DeprecatedSetting errors.
$hasDeprecatedSettings = $false
foreach ($result in $testResults)
{
```

```
    if ([string]$result.ErrorCode -eq 'DeprecatedSetting')

    {

        $hasDeprecatedSettings = $true

        break

    }

}



if (-not $hasDeprecatedSettings)

{

    Write-Host "No deprecated settings found. Policy errors exist but do
not require cleaning."

    Write-Host "Run 'Test-BrokerDesktopPolicy' to see other policy
issues."

    exit 0

}



# Load the Citrix Group Policy PowerShell Provider (only if we need to
clean).

Write-Host "`nDeprecated settings found. Loading Group Policy provider for
cleanup..."

$GpSnapin = "Citrix.Common.GroupPolicy"

$Provider = "CitrixGroupPolicy"

$SiteName = "CitrixGP"
```

```
$loaded = Get-PSSnapin $GpSnapin -ErrorAction SilentlyContinue

if ($loaded -eq $null)

{

    Add-PSSnapin $GpSnapin

}



# Mount the provider drive if it has not been mounted.

$GpDrive = Get-PSDrive $SiteName -ErrorAction SilentlyContinue

if ($GpDrive -eq $null)

{

    [void] ($GpDrive = New-PSDrive -PSProvider $Provider -Name $SiteName
-Root \ -Controller localhost)

}



$uRoot = $SiteName + ":\User\"

$cRoot = $SiteName + ":\Computer\"



$GpDrive.AutoWriteBack = $false



$settingsRemoved = 0

$policiesRemoved = 0
```

```
$settingNameMappings = @{

    'PvsIntegrationEnabled' = 'ImageProviderIntegrationEnabled'

}



function Remove-SettingFromPolicy

{

    param(

        [string] $policyName,

        [string] $settingName

    )



    $targetSettingName = Split-Path -Path $settingName -Leaf



    if ($settingNameMappings.ContainsKey($targetSettingName))

    {

        $mappedSettingName = $settingNameMappings[$targetSettingName]

        Write-Verbose "Mapping deprecated setting name
'$targetSettingName' to '$mappedSettingName'"

        $targetSettingName = $mappedSettingName

    }



    $searchPattern = $SiteName + ":\" + "*\" + $policyName + "\Settings\*"
```

```
    Write-Verbose "Searching for settings matching '$targetSettingName' in
policy '$policyName'..."

    $allSettings = Get-ChildItem -Path $searchPattern -Recurse
-ErrorAction SilentlyContinue |

        Where-Object {

            ($_.PSObject.Properties['State'] -and $_.State -ne
'NotConfigured') -or

            ($_.Name -eq 'Values' -and $_.Values -ne $null -and $_.Values
-ne '')

        }



    $found = $false

    foreach ($setting in $allSettings)

    {

        $RootPath = "{0}\{1}::{2}:" -f $GpSnapin, $Provider, $SiteName

        $relativePath = $setting.PSPath.Substring($RootPath.Length)

        Write-Verbose "  Checking configured setting: $relativePath"

        $currentSettingName = Split-Path -Path $setting.PSPath -Leaf

        if ($currentSettingName -ne $targetSettingName) { continue }

        Write-Verbose "  Found matching setting: $relativePath"

        Set-ItemProperty -Path $setting.PSPath -Name State -Value
NotConfigured

        Write-Host "  Set setting '$relativePath' to NotConfigured"

        $Script:settingsRemoved++
```

```
        $found = $true

    }



    if (-not $found)

    {

        Write-Warning "Could not find setting '$targetSettingName' in
policy '$policyName'"

    }

}



function Remove-PolicyByName

{

    param(

        [string] $policyName

    )



    if ($policyName -eq 'Unfiltered')

    {

        Write-Host "  Skipping removal of 'Unfiltered' policy (reserved
policy)"

        return

    }
```

```
    $uPath = $uRoot + $policyName

    $cPath = $cRoot + $policyName



    if (Test-Path $uPath)

    {

        $uSettings = Get-ChildItem -Path ($uPath + "\Settings") -Recurse
-ErrorAction SilentlyContinue |

            Where-Object {

                ($_.PSObject.Properties['State'] -and $_.State -ne
'NotConfigured') -or

                ($_.Name -eq 'Values' -and $_.Values -ne $null -and
$_.Values -ne '')

            }

        if ($uSettings.Count -eq 0)

        {

            Remove-Item -Path $uPath -Force -Recurse

            Write-Host "  Removed policy: \User\$policyName"

            $Script:policiesRemoved++

        }

    }



    if (Test-Path $cPath)

    {
```

```
        $cSettings = Get-ChildItem -Path ($cPath + "\Settings") -Recurse
-ErrorAction SilentlyContinue |

            Where-Object {

                ($_.PSObject.Properties['State'] -and $_.State -ne
'NotConfigured') -or

                ($_.Name -eq 'Values' -and $_.Values -ne $null -and
$_.Values -ne '')

            }

        if ($cSettings.Count -eq 0)

        {

            Remove-Item -Path $cPath -Force -Recurse

            Write-Host "  Removed policy: \Computer\$policyName"

            $Script:policiesRemoved++

        }

    }

}



# Phase 1: Remove deprecated settings.

Write-Host "`nPhase 1: Removing deprecated settings (this may take some
time)..."

foreach ($result in $testResults)

{

    if ([string]$result.ErrorCode -eq 'DeprecatedSetting')

    {
```

```
        Write-Host "`nPolicy '$($result.PolicyName)' has deprecated
settings:"

        if ($result.Settings -ne $null)

        {

            foreach ($setting in $result.Settings)

            {

                Write-Host "  - Setting '$($setting.SettingName)' is
deprecated"

                Remove-SettingFromPolicy -policyName $result.PolicyName
-settingName $setting.SettingName

            }

        }

    }

}



# Phase 2: Remove empty policies.

Write-Host "`nPhase 2: Checking for policies with no settings..."

$testResults2 = Test-BrokerDesktopPolicy | Select-Object -Property *



if ($testResults2 -eq $null -or $testResults2.Count -eq 0)

{

    Write-Host "No policy errors found."

}
```

```
else

{

    foreach ($result in $testResults2)

    {

        if ([string]$result.ErrorCode -eq 'PolicyHasNoSettings')

        {

            Write-Host "`nPolicy '$($result.PolicyName)' has no settings
remaining:"

            Remove-PolicyByName -policyName $result.PolicyName

        }

    }

}



# Save all changes.

if ($settingsRemoved -gt 0 -or $policiesRemoved -gt 0)

{

    Write-Host "`nSaving changes..."

    $GpDrive.Save()

}



Remove-PSDrive $SiteName
```

```
Write-Host "`n========================================="

Write-Host "Policy Cleanup Summary:"

Write-Host "  Settings removed: $settingsRemoved"

Write-Host "  Policies removed: $policiesRemoved"

Write-Host "========================================="



if ($settingsRemoved -eq 0 -and $policiesRemoved -eq 0)

{

    Write-Host "`nNo issues found. All policies are clean."

}

else

{

    Write-Host "`nCleanup completed successfully."

}



exit 0
```

関連コンテンツ

各リリースでの非推奨設定の詳細については、ポリシーの変更を参照してください。

ポリシー設定リファレンス

ポリシーには、ポリシーが適用されるときに適用される設定が含まれます。このセクションの説明では、機能を有効にするためにより多くの設定が必要かどうか、または設定に類似しているかどうかも示します。

クイックリファレンス

以下の表に、ポリシー内で構成できる設定を示します。左の列で完了したいタスクを見つけ、右の列で対応する設定を見つけてください。

.CHM (コンパイル済みHTML) 形式および .CSV 形式で、すべてのポリシー設定の完全なリストが利用可能です。これらのファイルは、ブローカー (デリバリーコントローラー) がインストールされているサーバーの `\program files\citrix\grouppolicy` フォルダーにあります。ポリシー設定の最新バージョンは、こちらをクリックしてダウンロードすることもできます。

オーディオ

このタスクの場合	このポリシー設定を使用
複数のオーディオデバイスの使用を許可するかどうかを制御する	オーディオプラグアンドプレイ
ユーザーデバイスのマイクからのオーディオ入力を許可するかどうかを制御する	クライアントマイクのリダイレクト
ユーザーデバイスのオーディオ品質を制御する	オーディオ品質
ユーザーデバイスのスピーカーへのオーディオマッピングを制御する	クライアントオーディオリダイレクト

ユーザーデバイスの帯域幅

使用される帯域幅を制限するには	このポリシー設定を使用
クライアントオーディオマッピング	オーディオリダイレクト帯域幅制限またはオーディオリダイレクト帯域幅制限率
ローカルクリップボードを使用した切り取りと貼り付け	クリップボードリダイレクト帯域幅制限またはクリップボードリダイレクト帯域幅制限率
セッションでのローカルクライアントドライブへのアクセス	ファイルリダイレクト帯域幅制限またはファイルリダイレクト帯域幅制限率
HDX™ MediaStream マルチメディアアクセラレーション	HDX MediaStream マルチメディアアクセラレーション帯域幅制限またはHDX MediaStream マルチメディアアクセラレーション帯域幅制限率

使用される帯域幅を制限するには	このポリシー設定を使用
クライアントセッション	セッション全体の帯域幅制限
印刷	プリンターリダイレクト帯域幅制限またはプリンターリダイレクト帯域幅制限率
TWAINデバイス（カメラやスキャナーなど）	TWAINデバイスリダイレクト帯域幅制限またはTWAINデバイスリダイレクト帯域幅制限率
USBデバイス	クライアントUSBデバイスリダイレクト帯域幅制限またはクライアントUSBデバイスリダイレクト帯域幅制限率

クライアントドライブとユーザーデバイスのリダイレクト

このタスクの場合	このポリシー設定を使用する
ユーザーがサーバーにログオンしたときに、ユーザーデバイス上のドライブを接続するかどうかを制御します	クライアントドライブの自動接続
サーバーとローカルクリップボード間のカットアンドペーストデータ転送を制御します	クライアントクリップボードリダイレクト
ユーザーデバイスからドライブがどのようにマップされるかを制御します	クライアントドライブのリダイレクト
ユーザーのローカルハードドライブがセッションで利用可能かどうかを制御します	クライアント固定ドライブとクライアントドライブのリダイレクト
ユーザーのローカルフロッピーディスクドライブがセッションで利用可能かどうかを制御します	クライアントフロッピーディスクドライブとクライアントドライブのリダイレクト
ユーザーのネットワークドライブがセッションで利用可能かどうかを制御します	クライアントネットワークドライブとクライアントドライブのリダイレクト
ユーザーのローカルCD、DVD、またはBlu-rayドライブがセッションで利用可能かどうかを制御します	クライアント光学ドライブとクライアントドライブのリダイレクト

このタスクの場合	このポリシー設定を使用する
ユーザーのローカルリムーバブルドライブがセッションで利用可能かどうかを制御します	クライアントリムーバブルドライブとクライアントドライブリダイレクト
スキャナーやカメラなどのユーザーのTWAINデバイスがセッションで利用可能かどうかを制御し、画像データ転送の圧縮を制御します	クライアントTWAINデバイスリダイレクト; TWAIN圧縮リダイレクト
USBデバイスがセッションで利用可能かどうかを制御します	クライアントUSBデバイスリダイレクトとクライアントUSBデバイスリダイレクト規則
WAN経由でクライアントディスクへのファイルの書き込みおよびコピーの速度を向上させます	非同期書き込みを使用する

コンテンツリダイレクト

このタスクの場合	このポリシー設定を使用する
サーバーからユーザーデバイスへのコンテンツリダイレクトを使用するかどうかを制御します	ホストからクライアントへのリダイレクト

デスクトップUI

このタスクの場合	このポリシー設定を使用する
ユーザーセッションでデスクトップの壁紙を使用するかどうかを制御します	デスクトップの壁紙
ウィンドウのドラッグ中にウィンドウの内容を表示します	ドラッグ中のウィンドウの内容を表示

グラフィックとマルチメディア

> **重要:**

Flashポリシーは、古いVDAを使用している顧客が新しいコントローラー（たとえば、バージョン1912コントローラー）を使用し、引き続きFlashを使用できるようにするためにのみ残されています。このVDAバージョンはFlashをサポートしていません。

このタスクの場合	このポリシー設定を使用します
仮想デスクトップからユーザーデバイスに送信される1秒あたりの最大フレーム数を制御します。	ターゲットフレームレート
ユーザーデバイスに表示される画像の視覚的な品質を制御します。	視覚的な品質
セッションでアクセスされたときに、Webサイトがflashコンテンツを表示できるかどうかを制御します。	Flashサーバー側コンテンツ取得URLリスト; Flash URL互換性リスト; Flashビデオフォールバック防止ポリシー設定; Flashビデオフォールバック防止エラー *.swf
サーバーでレンダリングされたビデオの圧縮を制御します。	圧縮にビデオコーデックを使用。ビデオコーデックにハードウェアエンコードを使用。
ユーザーへのHTML5マルチメディアWebコンテンツの配信を制御します。	HTML5ビデオリダイレクト

マルチストリームネットワークトラフィックの優先順位付け

このタスクの場合	このポリシー設定を使用
複数の接続にわたるICA®トラフィックのポートを指定し、ネットワークの優先順位を確立します。	マルチポートポリシー
サーバーとユーザーデバイス間のマルチストリーム接続のサポートを有効にします。	マルチストリーム (コンピューターとユーザーの設定)

印刷

このタスクの場合	このポリシー設定を使用
ユーザーデバイス上のクライアントプリンターの作成を制御します。	クライアントプリンターの自動作成とクライアントプリンターのリダイレクト
プリンタープロパティが保存される場所を制御します。	プリンタープロパティの保持
クライアントまたはサーバーが印刷要求を処理するかどうかを制御する	印刷サーバーへの直接接続
ユーザーが自分のユーザーデバイスに接続されているプリンターにアクセスできるかどうかを制御する	クライアントプリンターリダイレクト
クライアントおよびネットワークプリンターを自動的に作成する際のネイティブWindowsドライバーのインストールを制御する	インボックスプリンタードライバーの自動インストール
ユニバーサルプリンタードライバーをいつ使用するかを制御する	ユニバーサルプリンタードライバーの使用
ローミングユーザーセッション情報に基づいてプリンターを選択する	既定のプリンター
ユニバーサルプリントサーバーの負荷分散とフェールオーバースレッショルドの設定	負荷分散のためのユニバーサルプリントサーバー。サービス停止しきい値のユニバーサルプリントサーバー

注:

ポリシーを使用して、デスクトップまたはアプリケーションセッションでスクリーンセーバーを有効にすることはできません。スクリーンセーバーを必要とするユーザーの場合、スクリーンセーバーはユーザーデバイス上で実装できます。

ICA® ポリシー設定

注:

> このページでは、ICAポリシー設定の説明とサポートされている構成値を提供します。ポリシーの操作の詳細については、「ポリシーの操作」セクションを参照してください。

アダプティブトランスポート

この設定により、EDTをプライマリとして、TCPをフォールバックとしてデータ転送を行うことを許可または禁止します。

デフォルトでは、アダプティブトランスポートは有効（**優先**）になっており、可能な場合はEDTが使用され、TCPにフォールバックします。必要に応じて設定を変更できます。

- **優先**。可能な場合はEDT経由のアダプティブトランスポートが使用され、TCPにフォールバックします。
- **診断モード**。EDTが強制的にオンになり、TCPへのフォールバックは無効になります。この設定はトラブルシューティングの場合にのみ推奨されます。
- **オフ**。TCPが強制的にオンになり、EDTは無効になります。

詳細については、「アダプティブトランスポート」を参照してください。

ドラッグアンドドロップ設定

この設定により、クライアントと仮想アプリケーションまたはデスクトップの間でファイルをドラッグすることを許可または禁止します。デフォルトでは、ドラッグアンドドロップポリシーは無効になっています。必要に応じて、このポリシーを有効にできます。

アプリケーション起動待機タイムアウト

この設定は、セッションが最初のアプリケーションの起動を待機するミリ秒単位の待機タイムアウト値を指定します。アプリケーションの起動がこの期間を超えると、セッションは終了します。

デフォルトの時間（10,000ミリ秒）を選択するか、ミリ秒単位の数値を指定できます。

クライアントクリップボードリダイレクト

この設定は、ユーザーデバイスのクリップボードがサーバー上のクリップボードにマップされることを許可または禁止します。

デフォルトでは、クリップボードのリダイレクトは許可されています。

セッションとローカルクリップボード間のコピー＆ペーストデータ転送を禁止するには、**禁止**を選択します。ユーザーは、セッション内で実行されているアプリケーション間では引き続きデータをコピー＆ペーストできます。

この設定を許可した後、クライアント接続でクリップボードが消費できる最大許容帯域幅を構成します。**クリップボードリダイレクト帯域幅制限**または**クリップボードリダイレクト帯域幅制限率**の設定を使用します。

クライアントクリップボード書き込み許可形式

クライアントクリップボード書き込みの制限設定が**有効**の場合、ホストクリップボードデータはクライアントエンドポイントと共有できません。この設定を使用して、特定のデータ形式をクライアントエンドポイントのクリップボードと共有することを許可できます。この設定を使用するには、有効にして、許可する特定の形式を追加します。

次のクリップボード形式はシステム定義です。

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY

- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

XenAppおよびXenDesktopとCitrix Virtual Apps and Desktops™には、以下のカスタム形式が事前定義されています。

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8
- CFX_FILE

HTML形式はデフォルトで無効になっています。この機能を有効にするには:

- **クライアントクリップボードリダイレクト**が**許可**に設定されていることを確認します。
- **クライアントクリップボード書き込みの制限**が**有効**に設定されていることを確認します。
- **クライアントクリップボード書き込み許可形式**に**CF_HTML**（およびサポートしたいその他の形式）のエントリを追加します。

カスタム形式をさらに追加できます。カスタム形式名は、システムに登録される形式と一致している必要があります。形式名は大文字と小文字を区別します。

この設定は、**クライアントクリップボードリダイレクト**ポリシーが**禁止**に設定されている場合、または**クライアントクリップボード書き込みの制限**ポリシーが**無効**に設定されている場合には適用されません。

> **注:**
>
> HTML形式のクリップボードコピーサポート（CF_HTML）を有効にすると、コピーされたコンテンツのソースから宛先にスクリプトがコピーされます。コピーを進める前に、ソースを信頼できることを確認してください。スクリプトを含むコンテンツをコピーした場合、それらは宛先ファイルをHTMLファイルとして保存して実行した場合にのみ有効になります。

クリップボードのクライアントからセッションへの転送サイズを制限する

この設定は、ユーザーが単一のコピー＆ペースト操作中にクライアントエンドポイントから仮想セッションに転送できるクリップボードデータの最大サイズを指定します。

クリップボードの転送サイズを制限するには、**クリップボードのクライアントからセッションへの転送サイズを制限する**設定を有効にします。次に、**サイズ制限**フィールドにキロバイト単位の値を入力して、ローカルクリップボードとセッション間のデータ転送サイズを定義します。

既定では、この設定は無効になっており、クライアントからセッションへの転送に制限はありません。

HDX™ ダイレクト

HDX Direct を使用すると、直接通信が可能な場合に、クライアントがセッションホストとの直接接続を自動的に確立できます。接続は、ネットワークレベルの暗号化を使用して安全に確立されます。

HDX Direct モード

HDX Direct は、内部クライアントと外部クライアントの両方でセッションホストとの直接接続を確立するために使用できます。この設定は、HDX Direct が内部クライアントのみに利用可能か、内部クライアントと外部クライアントの両方に利用可能かを決定します。

内部のみに設定されている場合、HDX Direct は内部ネットワーク内のクライアントに対してのみ直接接続を確立しようとします。

内部および**外部**に設定されている場合、HDX Direct は内部クライアントと外部クライアントの両方に対して直接接続を確立しようとします。

既定では、HDX Direct は内部クライアントのみに設定されています。

HDX Direct ポート範囲

外部ユーザーからの接続に HDX Direct が使用するポートの範囲です。 既定では、HDX Direct はポート範囲 55000～55250 を使用します。

クリップボードのセッションからクライアントへの転送サイズを制限する

この設定は、ユーザーが単一のコピー＆ペースト操作中に仮想セッションからクライアントエンドポイントに転送できるクリップボードデータの最大サイズを指定します。

クリップボードの転送サイズを制限するには、**クリップボードのセッションからクライアントへの転送サイズを制限する**設定を有効にします。次に、**サイズ制限**フィールドにキロバイト単位の値を入力して、セッションとローカルクリップボード間のデータ転送サイズを定義します。

既定では、この設定は無効になっており、セッションからクライアントへの転送に制限はありません。

クライアントクリップボードへの書き込みを制限する

この設定が**有効**な場合、ホストのクリップボードデータはクライアントエンドポイントと共有できません。**クライアントクリップボード書き込み許可形式**設定を有効にすることで、特定の形式を許可できます。

デフォルトでは、この設定は**無効**です。

セッションクリップボードへの書き込みを制限する

この設定が**有効**な場合、クライアントのクリップボードデータはセッションアプリケーションと共有できません。**セッションクリップボード書き込み許可形式**設定を有効にすることで、特定の形式を許可できます。

デフォルトでは、この設定は**無効**です。

セッションクリップボード書き込み許可形式

セッションクリップボードへの書き込みを制限する設定が**有効**な場合、クライアントのクリップボードデータはセッションアプリケーションと共有できません。この設定を使用して、特定のデータ形式をセッションクリップボードと共有することを許可できます。

以下のクリップボード形式はシステム定義です。

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT

- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

以下のカスタム形式は、XenApp and XenDesktop および Citrix Virtual Apps and Desktops™ で事前定義されています。

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8

HTML形式はデフォルトで無効になっています。この機能を有効にするには：

- **クライアントクリップボードリダイレクト**が**許可**に設定されていることを確認します。
- **セッションクリップボード書き込みの制限**が**有効**に設定されていることを確認します。
- **セッションクリップボード書き込み許可形式**に**CF_HTML**（およびサポートしたいその他の形式）のエントリを追加します。

カスタム形式を追加できます。カスタム形式名は、システムに登録される形式と一致する必要があります。形式名は大文字と小文字を区別します。

この設定は、**クライアントクリップボードリダイレクト**ポリシーが**禁止**に設定されている場合、または**セッションクリップボード書き込みの制限**ポリシーが**無効**に設定されている場合には適用されません。

> **注:**

> HTML形式のクリップボードコピーサポート (CF_HTML) を有効にすると、コピーされたコンテンツのソースから宛先にスクリプトがコピーされます。コピーを進める前に、ソースを

> 信頼できることを確認してください。スクリプトを含むコンテンツをコピーした場合、それらは宛先ファイルをHTMLファイルとして保存して実行した場合にのみ有効になります。

デスクトップの起動

この設定は、VDA Direct Access Usersグループの非管理者ユーザーがICA接続を使用してそのVDA上のセッションに接続することを許可または禁止します。

デフォルトでは、非管理者ユーザーはこれらのセッションに接続できません。

この設定は、RDP接続を使用しているVDAダイレクトアクセスユーザーグループ内の非管理者ユーザーには影響しません。これらのユーザーは、この設定が有効または無効になっている場合でもVDAに接続できます。この設定は、VDAダイレクトアクセスユーザーグループに属していない非管理者ユーザーには影響しません。これらのユーザーは、この設定が有効または無効になっている場合、VDAに接続できません。

FIDO2リダイレクト

この設定は、FIDO2リダイレクトを有効または無効にします。FIDO2リダイレクトにより、ユーザーは仮想マシン内のローカルエンドポイントFIDO2コンポーネントを活用できます。ユーザーは、TPM 2.0とWindows Helloを搭載したデバイスで、FIDO2セキュリティキーまたは統合生体認証を介して仮想セッションを認証できます。

この設定が**許可**されている場合、ユーザーはローカルエンドポイント機能を使用してFIDO2認証を行うことができます。デフォルトでは、この設定は**許可**されています。

FIDO2許可プロセス

この設定により、管理者は仮想セッション内でFIDO2およびWebAuthnリダイレクトの使用が許可されるアプリケーションを指定できます。

許可リスト内のアプリケーションには、アプリケーション実行可能ファイルへの完全なローカルパスが必要です。ネットワークパスはサポートされていません。

アプリケーションパスでは、ワイルドカード(*)を使用して、単一のディレクトリ、ディレクトリ名の一部、実行可能ファイルのベース名、または実行可能ファイルのベース名の一部を置き換えることができます。

ICAリスナー接続タイムアウト

この設定は、ICAプロトコルを使用した接続が完了するまでの最大待機時間を指定します。

デフォルトでは、最大待機時間は120,000ミリ秒、つまり2分です。

ICAリスナーポート番号

この設定は、サーバー上のICAプロトコルによって使用されるTCP/IPポート番号を指定します。

デフォルトでは、ポート番号は1494に設定されています。

有効なポート番号は0～65535の範囲内である必要があり、他のよく知られているポート番号と競合してはなりません。ポート番号を変更した場合は、新しい値を有効にするためにサーバーを再起動してください。サーバーのポート番号を変更した場合は、サーバーに接続するすべてのCitrix Workspace™アプリまたはプラグインでも変更する必要があります。

キーボードと入力方式エディター (IME)

この設定は、次の項目を有効または無効にします。

- 動的キーボードレイアウト同期
- 入力方式エディター (IME)
- Unicode キーボードレイアウトマッピング
- キーボードレイアウト切り替え通知ダイアログメッセージを非表示または表示します
- タッチデバイスのエンドユーザー向け自動タッチキーボード表示

1. Web Studioで、**キーボードとIME**を選択します。
2. VDAでの動的なキーボードレイアウト同期と汎用クライアント入力方式エディター (IME) 機能を制御するには、**クライアントキーボードレイアウトの同期とIMEの改善**を選択します。設定できる項目は次のとおりです。

   無効 - 動的なキーボードレイアウト同期と汎用クライアント入力方式エディター (IME)。

   動的なクライアントキーボードレイアウト同期をサポート - 動的なキーボードレイアウト同期を有効にします。

   動的なクライアントキーボードレイアウト同期とIMEの改善をサポート - 動的なキーボードレイアウト同期と汎用クライアント入力方式エディター (IME) の両方を有効にします。
3. Unicodeキーボードマッピングを有効または無効にするには、**Unicodeキーボードレイアウトマッピングを有効にする**を選択します。
4. ユーザーがクライアントキーボードレイアウトを変更したときに、キーボードレイアウトが同期中であることを示すメッセージを表示するかどうかを制御するには、**キーボードレイアウト切り替えポップアップメッセージボックスを非表示にする**を選択します。メッセージが表示されないようにすると、ユーザーは誤った文字入力にならないように、入力する前に数秒待つ必要があります。

5. 入力フィールドに入るときまたは離れるときに、クライアント側のソフト/タッチキーボードを自動的に表示または非表示にするかどうかを許可または禁止するには、**自動キーボード表示**を選択します。

デフォルト設定：

- **クライアントキーボードレイアウトの同期とIMEの改善**
  - Windows Server 2019/2022/2025、およびマルチセッションの Windows 10/11 では無効
  - シングルセッションの Windows 10/11 では有効
- **Unicode キーボードレイアウトマッピング**
  - 禁止（Unicode キーボードレイアウトマッピングはデフォルトで無効であることを示します。エンドユーザーが CWA で Unicode 入力モードを使用している場合は、構成して許可する必要があります）
- **キーボードレイアウト切り替えポップアップメッセージボックスを非表示にする**
  - 禁止 (ポップアップメッセージボックスが表示されることを示します)
- **キーボードの自動表示**
  - 禁止 (入力フィールドに入力または入力フィールドから離れるときに、クライアント側のソフト/タッチキーボードが自動的に表示または非表示にならないことを示します)

このポリシーは、ポリシー設定の**説明**セクションに記載されているレジストリ設定を置き換えます。

ログオフチェッカーの起動遅延

この設定は、ログオフチェッカーの起動を遅延させる期間を指定します。このポリシーを使用して、クライアントセッションがセッションを切断するまでに待機する時間（秒単位）を設定します。

この設定は、ユーザーがサーバーからログオフするのにかかる時間も増加させます。

ロス許容モード

> **重要:**

- この機能には、Windows 用 Citrix Workspace アプリ 2002 以降が必要です。VDA のこのバージョンは、利用可能になった時点でこれをサポートします。
- グラフィックの損失許容モードは Citrix Gateway および Citrix Gateway Service でサポートされています。このモードは、直接接続でのみ利用可能です。

この設定は、グラフィックのロス許容モードを有効または無効にします。

デフォルトでは、グラフィックのロス許容モードは**許可**されています。

許可されている場合、パケット損失と遅延がしきい値を超えると、このモードに入ります。しきい値は、ロス許容しきい値ポリシーを使用して設定できます。

ロス許容しきい値

ロス許容モードが利用可能な場合、この設定は、セッションがグラフィックのロス許容モードに切り替わるネットワークメトリックのしきい値を指定します。

デフォルトのしきい値は次のとおりです。

- パケット損失: 5%
- 遅延: 300 ms (RTT)

詳細については、損失許容モードを参照してください。

オーディオのロストレラントモード

この設定は、オーディオの損失許容モードを有効または無効にします。

有効にすると、オーディオは損失許容モードで送信されます。

デフォルトでは、オーディオの損失許容モードは**禁止**されています。

ポリシーを有効にするには、オーディオポリシーの損失許容モードのレジストリを**許可**に編集します。

オーディオの損失許容モードを有効にするには、EDTトランスポートが必要です。

Rendezvous プロトコル

この設定は、Citrix Gateway Serviceを使用する際のHDXセッションのプロキシ方法を変更します。有効にすると、HDXトラフィックはCitrix Cloud Connectorを経由しなくなります。代わり

に、VDAはCitrix Gateway Serviceに直接アウトバウンド接続を確立します（Cloud Connectorのスケーラビリティが向上します）。

重要:

Citrix Cloud™の機能トグルとHDXポリシー設定がこの機能を制御します。Citrix Cloudの機能トグルはデフォルトで有効になっていますが、HDX設定はデフォルトで無効になっています。HDX設定は、Citrix Gateway Serviceを介して確立されたHDXセッションにのみ影響します。この設定は、クライアントとVDA間で直接確立されたセッションや、オンプレミスのCitrix Gatewayを介して確立されたセッションには影響しません。

詳細については、Rendezvousプロトコルを参照してください。

Rendezvousプロキシ構成

この設定により、Rendezvousプロトコルで使用する明示的なプロキシを構成できます。透過型プロキシを使用している場合、この設定を有効にする必要はありません。

デフォルトでは、この設定は無効になっています。

無効にすると、VDAはGateway ServiceとのRendezvous接続を確立しようとするときに、非透過型プロキシを介してアウトバウンドトラフィックをルーティングしません。

有効にすると、VDAはこの設定で定義されたプロキシを介してGateway ServiceとのRendezvous接続を確立しようとします。

VDAは、Rendezvous接続にHTTPおよびSOCKS5プロキシの使用をサポートしています。Rendezvous接続にプロキシを使用するようにVDAを構成するには、この設定を有効にする必要があります。また、プロキシのアドレスまたはPACファイルへのパスを指定します。例：

- プロキシアドレス: `http://<URL or IP>:<port>` または `socks5://<URL or IP>:<port>`
- PACファイル: `http://<URL or IP>/<path>/<filename>.pac`

  VDAバージョン2103は、PACファイルを使用したプロキシ構成でサポートされる最小バージョンです。SOCKS5プロキシのPACファイルスキーマの詳細については、「プロキシ構成」を参照してください。

注:

> SOCKS5プロキシのみがEDTを介したデータ転送をサポートします。HTTPプロキシの場合は、ICAのトランスポートプロトコルとしてTCPを使用してください。

> 詳細については、「Rendezvousプロトコル」を参照してください。

クライアント接続中の非公開プログラムの起動

この設定は、サーバー上でRDPを介して初期アプリケーションの起動を許可するかどうかを指定します。

デフォルトでは、サーバー上でRDPを介して初期アプリケーションの起動は許可されていません。

セッションメトリックの収集

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

オペレーティングシステム、稼働時間、コンピューターシステム情報、ビデオコントローラーの詳細、VDA バージョン、展開タイプ、ドメイン参加ステータスなどのデータが収集されます。さらに、製品改善の取り組みを支援するために、いくつかのセッション構成、パフォーマンスおよび信頼性データを収集できます。カスタマーエクスペリエンス向上プログラムの詳細については、以下を参照してください。

- `<https://more.citrix.com/XD-CEIP>`
- `<https://docs.citrix.com/ja-jp/linux-virtual-delivery-agent/current-release/configure/administration/linux-vda-data-collection-program>`
- `<https://docs.citrix.com/ja-jp/mac-vda/configure/session/supportability-service>`

デフォルトでは、この設定は有効になっています。

タブレットモード切り替えポリシー設定

タブレットモードの切り替えは、VDA上のストアアプリ、Win32アプリ、およびWindowsシェルを最適化します。これは、電話やタブレットなどの小型デバイス、またはタッチ対応デバイスから接続する際に、仮想デスクトップを自動的にタブレットモードに切り替えることで実現されます。

このポリシーが無効になっている場合、VDAはユーザーが設定したモードになり、クライアントの種類に関係なく、そのモードを維持します。

自動クライアント再接続ポリシー設定

自動クライアント再接続セクションには、セッションの自動再接続を制御するためのポリシー設定が含まれています。

自動クライアント再接続

この設定は、接続が中断された後に同じクライアントによる自動再接続を許可または禁止します。

Citrix Receiver for Windows 4.7以降およびCitrix Workspaceアプリ1808以降では、自動クライアント再接続はCitrix Studioからのポリシー設定のみを使用します。Studioでこれらのポリシーを更新すると、自動クライアント再接続がサーバーからクライアントに同期されます。以前のバージョンのCitrix Receiver for Windowsで自動クライアント再接続を構成するには、Studioポリシーを使用し、レジストリまたはdefault.icaファイルを変更します。

自動クライアント再接続を許可すると、接続が切断されたときに中断された場所からユーザーが作業を再開できるようになります。自動再接続は、切断された接続を検出し、ユーザーをセッションに再接続します。

セッションIDと資格情報へのキーを含むCitrix Workspace™アプリのCookieが使用されない場合、自動再接続によって新しいセッションが開始される可能性があります。つまり、既存のセッションに再接続するのではなく、新しいセッションが開始されます。Cookieは、有効期限が切れている場合は使用されません。たとえば、再接続の遅延や、資格情報の再入力が必要な場合などにCookieの有効期限が切れることがあります。ユーザーが意図的に切断した場合、自動クライアント再接続はトリガーされません。

再接続が進行中の場合、セッションウィンドウはグレー表示されます。カウントダウンタイマーは、セッションが再接続されるまでの残り時間を表示します。セッションがタイムアウトすると、切断されます。

アプリケーションセッションの場合、自動再接続が許可されていると、通知領域にカウントダウンタイマーが表示されます。このタイマーは、セッションが再接続されるまでの残り時間を指定します。Citrix Workspaceアプリは、再接続が成功するか、ユーザーが再接続の試行をキャンセルするまで、セッションへの再接続を試みます。

ユーザーセッションの場合、自動再接続が許可されていると、Citrix Workspaceアプリは、再接続が成功するか、ユーザーが再接続の試行をキャンセルしない限り、指定された期間セッションへの再接続を試みます。デフォルトでは、この期間は2分です。この期間を変更するには、ポリシーを編集します。

デフォルトでは、自動クライアント再接続は許可されています。ポリシーを**禁止**に設定することで無効にできます。

自動クライアント再接続認証

この設定は、自動クライアント再接続に認証が必要かどうかを指定します。

ユーザーが最初にログオンすると、資格情報は暗号化され、メモリに保存され、暗号化キーを含むCookieが作成されます。このCookieはCitrix Workspaceアプリに送信されます。この設定が構成されている場合、Cookieは使用されません。代わりに、Citrix Workspaceアプリが自動的に再接続を試みるときに、資格情報を要求するダイアログボックスがユーザーに表示されます。

デフォルトでは、認証は不要です。

自動クライアント再接続ログ

この設定は、イベントログへの自動クライアント再接続の記録を有効または無効にします。

ログ記録が有効な場合、サーバーのシステムログは、成功および失敗した自動再接続イベントに関する情報をキャプチャします。サイトは、すべてのサーバーの再接続イベントの結合されたログを提供しません。

デフォルトでは、ログ記録は無効です。

自動クライアント再接続のタイムアウト

デフォルトでは、自動クライアント再接続のタイムアウトは120秒に設定されており、自動クライアント再接続のタイムアウトの最大設定可能値は300秒です。このポリシーを使用してタイムアウト値を設定します。

再接続UIの透明度レベル

この設定により、セッションの信頼性再接続中にXenAppまたはXenDesktop®セッションウィンドウに適用される不透明度レベルを指定できます。

デフォルトでは、再接続UIの透明度は80%に設定されています。

オーディオポリシー設定

オーディオセクションには、パフォーマンスを低下させることなく、ユーザーデバイスがセッションでオーディオを送受信できるようにするポリシー設定が含まれています。

アダプティブオーディオ

この設定は、アダプティブオーディオを有効または無効にします。このポリシーを有効にすると、最高のユーザーエクスペリエンスを提供するためにオーディオ品質設定が動的に調整されます。この設定は、Citrix Virtual Apps and Desktops™ 2109以降を使用するVDAのシングルセッションOSおよびマルチセッションOSセッションの両方に適用されます。

この設定が禁止されている場合、オーディオ品質ポリシーが適用されます。詳細については、「オーディオ品質」を参照してください。

デフォルトでは、アダプティブオーディオポリシーは有効になっています。

UDPリアルタイムトランスポート経由のオーディオ

この設定は、User Datagram Protocol (UDP) を使用してRTP経由でVDAとユーザーデバイス間でオーディオを送受信することを許可または禁止します。この設定が無効になっている場合、オーディオはTCP経由で送受信されます。

デフォルトでは、UDP経由のオーディオは許可されています。

オーディオプラグアンドプレイ

この設定は、複数のオーディオデバイスを使用してサウンドを録音および再生することを許可または禁止します。

デフォルトでは、複数のオーディオデバイスの使用は許可されています。

この設定は、WindowsマルチセッションOSマシンにのみ適用されます。

オーディオ品質

この設定は、ユーザーセッションで受信されるサウンドの品質レベルを指定します。

デフォルトでは、サウンド品質は「高 - 高精細オーディオ」に設定されています。

サウンド品質を制御するには、次のいずれかのオプションを選択します。

- 低帯域幅接続の場合は、「低 - 低速接続用」を選択します。ユーザーデバイスに送信されるサウンドは最大16 Kbpsに圧縮されます。この圧縮により、サウンドの品質は大幅に低下しますが、低帯域幅接続でも適切なパフォーマンスが得られます。
- 「中」を選択 - 音声に最適化されており、Voice over Internet Protocolアプリケーションを提供します。この設定は、512 Kbps未満の回線、または著しい輻輳やパケット損失があるような、困難なネットワーク接続でメディアアプリケーションを提供します。このコーデックはエンコード時間が速いため、サーバー側のメディア処理が必要な場合に、ソフトフォンやユニファイドコミュニケーションアプリケーションでの使用に最適です。

  ユーザーデバイスに送信されるオーディオは、最大64 Kbpsに圧縮されます。この圧縮により、ユーザーデバイスで再生されるオーディオの品質は中程度に低下しますが、低遅延で低帯域幅の消費を実現します。Voice over Internet Protocolの品質が不十分な場合は、「Audio over UDP Real-time Transport」ポリシー設定が「許可」に設定されていることを確認してください。

現在、UDP経由のリアルタイムトランスポート（RTP）は、このオーディオ品質が選択されている場合にのみサポートされます。低速（512 Kbps未満）回線のような困難なネットワーク接続でメディアアプリケーションを配信する場合でも、このオーディオ品質を使用してください。また、ネットワークに輻輳やパケット損失がある場合も同様です。

- 「高」を選択 - 帯域幅が豊富で音質が重要な接続には、高精細オーディオを使用します。クライアントはネイティブレートでサウンドを再生できます。サウンドはCD品質まで維持される高音質レベルで圧縮され、最大112 Kbpsの帯域幅を使用します。この量のデータを送信すると、CPU使用率が増加し、ネットワークが輻輳する可能性があります。

帯域幅は、オーディオの録音中または再生中にのみ消費されます。両方が同時に発生する場合、帯域幅の消費量は2倍になります。

最大帯域幅を指定するには、**オーディオリダイレクト帯域幅制限**または**オーディオリダイレクト帯域幅制限率**の設定を構成します。

クライアントオーディオリダイレクト

この設定は、サーバーでホストされているアプリケーションが、ユーザーデバイスにインストールされているサウンドデバイスを介してサウンドを再生できるかどうかを指定します。この設定は、ユーザーがオーディオ入力を録音できるかどうかも指定します。

デフォルトでは、オーディオリダイレクトは許可されています。

この設定を許可した後、オーディオの再生または録音によって消費される帯域幅を制限できます。オーディオによって消費される帯域幅の量を制限すると、アプリケーションのパフォーマンスが向上する可能性がありますが、オーディオ品質が低下する可能性もあります。帯域幅は、オーディオの録音中または再生中にのみ消費されます。両方が同時に発生する場合、帯域幅の消費量は2倍になります。最大帯域幅を指定するには、**オーディオリダイレクト帯域幅制限**または**オーディオリダイレクト帯域幅制限率**の設定を構成します。

WindowsマルチセッションOSマシンでは、複数のオーディオデバイスをサポートするために、**オーディオプラグアンドプレイ**設定が有効になっていることを確認してください。

重要：クライアントオーディオリダイレクトを禁止すると、すべてのHDX™オーディオ機能が無効になります。

クライアントマイクのリダイレクト

この設定は、クライアントマイクのリダイレクトを有効または無効にします。有効にすると、ユーザーはセッションでマイクを使用してオーディオ入力を録音できます。

デフォルトでは、マイクのリダイレクトは許可されています。

セキュリティのため、デバイスによって信頼されていないサーバーがマイクにアクセスしようとすると、ユーザーに警告が表示されます。ユーザーはアクセスを許可するかどうかを選択できます。ユーザーはCitrix Workspace™アプリで警告を無効にできます。

WindowsマルチセッションOSマシンでは、複数のオーディオデバイスをサポートするために、オーディオプラグアンドプレイ設定が有効になっていることを確認してください。

ユーザーデバイスで**クライアントオーディオリダイレクト**設定が無効になっている場合、このルールは無効になります。

帯域幅ポリシー設定

「**帯域幅**」セクションには、クライアントセッションの帯域幅使用に関連するパフォーマンスの問題を回避するためのポリシー設定が含まれています。

重要: これらのポリシー設定を**マルチストリームポリシー**設定と併用すると、予期しない結果が生じる可能性があります。ポリシーでマルチストリーム設定を使用する場合は、これらの帯域幅制限ポリシー設定が含まれていないことを確認してください。

オーディオリダイレクト帯域幅制限

この設定は、ユーザーセッションでオーディオを再生または録音するために許可される最大帯域幅を指定します。許可される最大帯域幅は、1秒あたりのキロビット単位で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**オーディオリダイレクト帯域幅制限の割合**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

オーディオリダイレクトの帯域幅制限（パーセント）

この設定は、オーディオの再生または録音に許可される最大帯域幅制限を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**オーディオリダイレクト帯域幅制限**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

クライアントUSBデバイスリダイレクト帯域幅制限

この設定は、USBデバイスのクライアントとの間のリダイレクトに許可される最大帯域幅を指定します。許可される最大帯域幅は、1秒あたりのキロビット単位で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**クライアントUSBデバイスリダイレクト帯域幅制限の割合**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

クライアントUSBデバイスリダイレクトの帯域幅制限（パーセント）

この設定は、クライアントとの間でUSBデバイスをリダイレクトするために許可される最大帯域幅を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**クライアントUSBデバイスリダイレクト帯域幅制限**設定にも値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

クリップボードリダイレクト帯域幅制限

この設定は、セッションとローカルクリップボード間のデータ転送に許可される最大帯域幅を指定します。許可される最大帯域幅は、キロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**クリップボードリダイレクト帯域幅制限（パーセント）**設定にも値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

クリップボードリダイレクトの帯域幅制限（パーセント）

この設定は、セッションとローカルクリップボード間のデータ転送に許可される最大帯域幅を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**クリップボードリダイレクト帯域幅制限**設定にも値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

COMポートリダイレクトの帯域幅制限

> **注:**
>
> Virtual Delivery Agent 7.0から7.8の場合、この設定はレジストリを使用して構成します。詳細については、「レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。

この設定は、クライアント接続でCOMポートにアクセスするために許可される最大帯域幅をキロビット/秒で指定します。この設定に値を入力し、**COMポートリダイレクト帯域幅制限（パーセント）**設定にも値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

COMポートリダイレクトの帯域幅制限（パーセント）

注：Virtual Delivery Agent 7.0から7.8の場合、この設定はレジストリを使用して構成します。詳細については、「レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。

この設定は、クライアント接続でCOMポートにアクセスするために許可される最大帯域幅を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**COMポートリダイレクト帯域幅制限**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な総帯域幅を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

ファイルリダイレクト帯域幅制限

この設定は、ユーザーセッションでクライアントドライブにアクセスするために許可される最大帯域幅を指定します。許可される最大帯域幅は、キロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**ファイルリダイレクト帯域幅制限の割合**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

ファイルリダイレクトの帯域幅制限（パーセント）

この設定は、クライアントドライブにアクセスするために許可される最大帯域幅制限を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**ファイルリダイレクト帯域幅制限**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な総帯域幅を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

HDX™ MediaStream マルチメディアアクセラレーション帯域幅制限

この設定は、HDX MediaStream マルチメディアアクセラレーションを使用してストリーミングオーディオおよびビデオを配信するために許可される最大帯域幅制限を指定します。許可される最大帯域幅は、キロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**HDX MediaStream Multimedia Acceleration帯域幅制限パーセント**設定の両方に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

HDX MediaStream Multimedia Acceleration帯域幅制限パーセント

この設定は、HDX MediaStream Multimedia Accelerationを使用してストリーミングオーディオおよびビデオを配信するために許可される最大帯域幅を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**HDX MediaStream Multimedia Acceleration帯域幅制限**設定の両方に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

LPTポートリダイレクト帯域幅制限

注：Virtual Delivery Agent 7.0から7.8の場合、この設定はレジストリを使用して構成します。詳細については、「レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。

この設定は、単一ユーザーセッションでLPTポートを使用する印刷ジョブに許可される最大帯域幅を指定します。許可される最大帯域幅は、キロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**LPTポートリダイレクト帯域幅制限パーセント**設定の両方に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

LPTポートリダイレクトの帯域幅制限（パーセント）

注：Virtual Delivery Agent 7.0から7.8の場合、この設定はレジストリを使用して構成します。詳細については、「レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。

この設定は、単一クライアントセッションでLPTポートを使用する印刷ジョブの帯域幅制限を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**LPTポートリダイレクト帯域幅制限**設定の両方に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

セッション全体の帯域幅制限

この設定は、ユーザーセッションで利用可能な総帯域幅を、1秒あたりのキロビット単位で指定します。

適用可能な最大帯域幅の上限は20 Mbps (20,000 Kbps)です。デフォルトでは、最大値（ゼロ）は指定されていません。

クライアント接続によって消費される帯域幅の量を制限すると、クライアント接続外の他のアプリケーションが限られた帯域幅を競合している場合に、パフォーマンスが向上する可能性があります。

プリンターリダイレクト帯域幅制限

この設定は、ユーザーセッションでクライアントプリンターにアクセスするために許可される最大帯域幅を指定します。許可される最大帯域幅は、1秒あたりのキロビット単位で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**Printer redirection bandwidth limit percent** 設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

プリンターリダイレクトの帯域幅制限（パーセント）

この設定は、クライアントプリンターにアクセスするために許可される最大帯域幅を、総セッション帯域幅の割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**Printer redirection bandwidth limit** 設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な総帯域幅を指定する**Overall session bandwidth limit** 設定も構成する必要があります。

TWAINデバイスリダイレクト帯域幅制限

この設定は、公開アプリケーションからTWAINイメージングデバイスを制御するために許可される最大帯域幅を指定します。許可される最大帯域幅は、1秒あたりのキロビット単位で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**TWAIN device redirection bandwidth limit percent** 設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

TWAINデバイスリダイレクト帯域幅制限の割合

この設定は、公開アプリケーションからTWAINイメージングデバイスを制御するために許可される最大帯域幅を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**TWAIN device redirection bandwidth limit** 設定にも値を入力した場合、最も制限の厳しい設定（値が小さい方）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**Overall session bandwidth limit** 設定も構成する必要があります。

双方向コンテンツリダイレクトポリシー設定

「**双方向コンテンツリダイレクト**」セクションには、クライアントからVDAへのURLリダイレクトとVDAからクライアントへのURLリダイレクトを有効または無効にするポリシー設定があります。

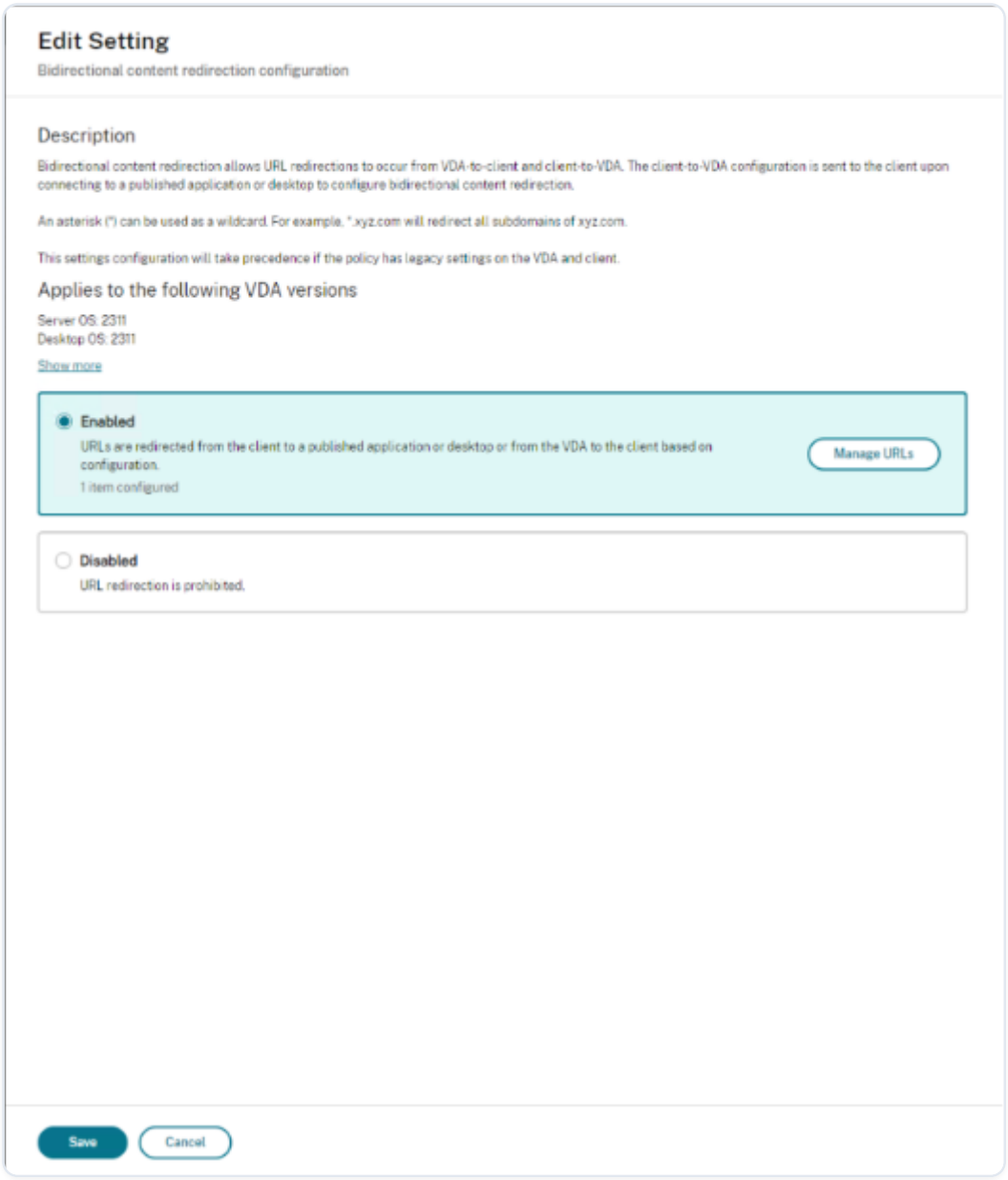
サーバーポリシーはStudioで設定されます。Citrix Workspace™アプリバージョン2311以降、この設定は、Studioの以下の3つのレガシー設定（非推奨）に置き換わります。

- 双方向コンテンツリダイレクトを許可する
- VDAにリダイレクトされる許可されたURL
- クライアントにリダイレクトされる許可されたURL

また、Windowsクライアント上の以下の3つのローカルGroup Policy Object (GPO) 設定も置き換えます。

- 双方向コンテンツリダイレクト
- 双方向コンテンツリダイレクトのオーバーライド
- OAuthリダイレクト

この設定が有効になっている場合、公開されたアプリまたはデスクトップに接続すると、双方向コンテンツリダイレクトを構成するためのクライアントからVDAへの設定がクライアントに送信されます。



この設定が構成されている場合、Studioおよびクライアントのレガシー設定よりも優先されます。Citrix®は、予期しない動作を避けるため、新しいポリシー設定のみを使用し、すべてのレガシー設定を削除することを推奨します。

VDAとDDCがバージョン2311以降を実行している場合、クライアントポリシーを設定してはなりません。そうでない場合、クライアントポリシーはCitrix WorkspaceアプリのGroup Policy Object管理テンプレートから設定されます。

Citrixは、ホストからクライアントへのリダイレクトと、クライアントからURLへのリダイレクトのためのLocal App Accessを提供しています。ただし、Citrixは、ドメイン参加済みWindowsクライアントには双方向コンテンツリダイレクトを使用することを推奨しています。

Citrixは、Studioの新しいUIを使用してこの機能を構成することを推奨します。

ワイルドカードリダイレクト

双方向コンテンツリダイレクトは、リダイレクトするURLを定義する際にワイルドカードの使用をサポートしています。双方向コンテンツリダイレクトの詳細と構成については、構成の手順を参照してください。 Studioで、`hostToClientUrls`配列または`clientToHostUrls`配列内の`url`キーの値としてJSON文字列を編集して、ワイルドカードURLを設定します。

> **注:**
>
> - 無限ループを避けるため、`hostToClientUrls`と`clientToHostUrls`に同じURLを設定しないでください。
> - トップレベルドメインはサポートされていません。たとえば、`<https://www.citrix.*>`や`<http://www.citrix.co*>`はリダイレクトされません。

双方向コンテンツリダイレクトの構成

このポリシーを`Enabled`に設定して機能の構成を開始し、**Manage URLs**をクリックします。次の構成を設定します。

- **VDAからクライアントへのリダイレクト**
- **クライアントからVDAへのリダイレクト**

VDAからクライアントへのリダイレクト

VDAからクライアントにURLをリダイレクトするには、1行に1つのURLを入力します。ワイルドカードを使用できます。 OAuthリダイレクトを使用すると、クライアントエンドポイントのブラウザーを使用して認証を実行し、トークンをVDAに送り返すことができます。

利点:

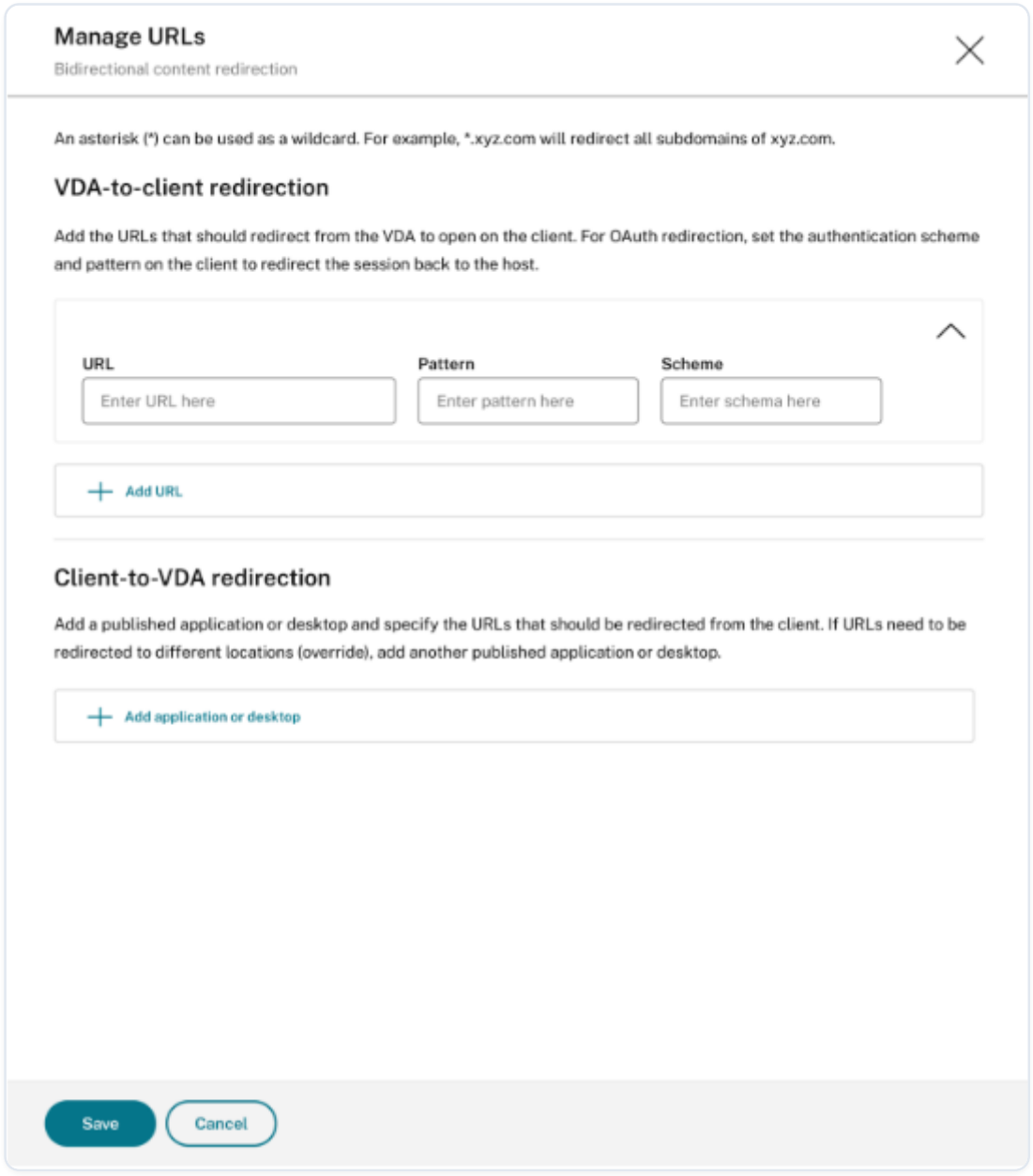
- これらの資格情報をホスト環境に保存しないようにできます。
- エンドポイントで利用可能で、VDAでは利用できない生体認証機能を使用できます。

構成：

URLのVDAからクライアントへのリダイレクトを構成するには、以下を指定します。

- **URL**（必須）VDAからリダイレクトしてクライアントで開く必要があるURLを追加します。**OAuthリダイレクト**の場合、セッションをホストにリダイレクトするように、クライアントで認証スキームとパターンを設定します。

- **パターン**：（オプション）VDAからクライアントへのURLリダイレクトを介してクライアントにリダイレクトされたときに、OAuth認証フローが開始されたかのように追跡され、フローが完了したとき（結果のスキームまたはリダイレクトURLパターンが開かれたことによって検出される）、その結果のURLがそのフローを開始したホストVDAにリダイレクトされるURL正規表現。
- **スキーム**：（オプション）**スキーム**が指定されている場合、終了URLは`<scheme>`://`<something>`の形式であると想定されます。スキームが指定されていない（空である）とします。その場合、元の結果のURLパターンは、正規表現キャプチャグループ（パターンで指定する必要がある）を介してパターンから抽出され、元のURLは`citrix-oauth-redir://`リダイレクトURLを使用するように書き換えられます。フローが完了すると、元のリダイレクトURLはホスト（VDA）にリダイレクトされます。この場合、OAuth認証サーバーは`citrix-oauth-redir://byIndex/1 (2, 3, ... N)`リダイレクトURLを許可するように構成する必要があります。



注:

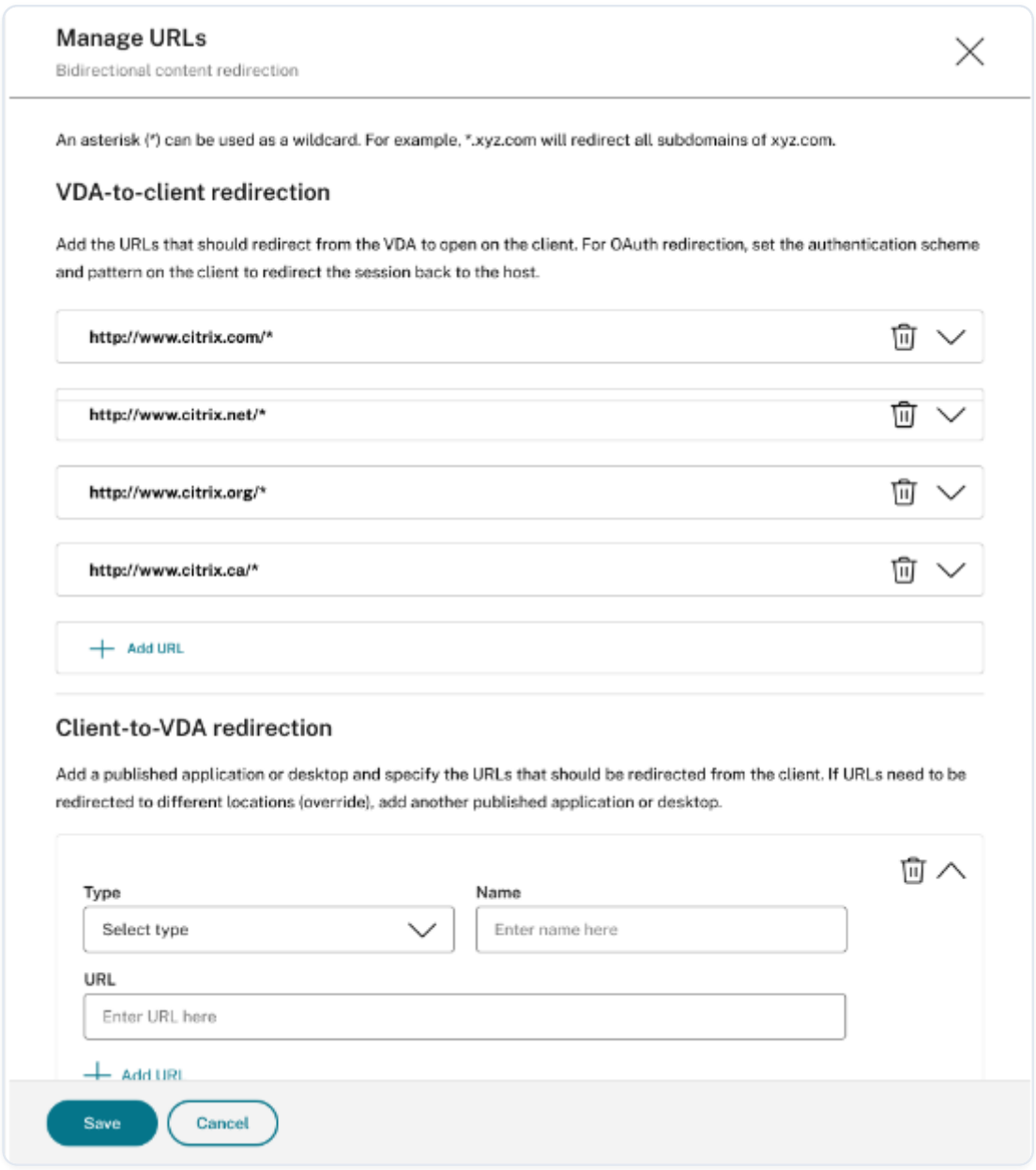
パターンと**スキーム**はどちらもオプションですが、**パターン**が指定されている場合は、**スキーム**も指定する必要があります。

クライアントからVDAへのリダイレクト

クライアントからVDAにURLをリダイレクトするには、次の手順を実行します。

1. クライアントURLの宛先を構成します。
2. 公開アプリケーションまたは公開デスクトップのいずれかを選択します。
3. そのリソースの名前を指定します。

4. そのリソースにリダイレクトする必要があるすべてのURLを追加します。 新しいアプリケーションまたはデスクトップを追加し、そのリソースにリダイレクトするURLを指定することで、このデフォルトのリソースを上書きできます。



OAuthリダイレクト

OAuthリダイレクトを使用すると、クライアントエンドポイントブラウザを使用して認証し、トークンをVDAに送り返すことができます。

利点：

- これらの資格情報をホストされた環境に保存することを回避できます。
- エンドポイントで利用可能で、VDAでは利用できない生体認証機能を使用できます。

URLのOAuthリダイレクトを構成するには、次のパラメーターを指定します。

- **oAuthRedirectionPattern**: (オプション) VDAからクライアントへのURLリダイレクトを介してクライアントにリダイレクトされたときに、OAuth認証フローが開始されたかのように追跡されるURL正規表現。フローが完了したとき（結果のスキームまたはリダイレクトURLパターンが開かれたことによって検出される）、その結果のURLは、そのフローを開始したホストVDAにリダイレクトされます。
- **oAuthScheme**: (オプション) スキームが指定されている場合、終了URLは`<scheme>`://`<something>`の形式であると想定されます。スキームが指定されていない（空である）とします。その場合、元の結果URLパターンは、正規表現キャプチャグループ（パターンで指定する必要がある）を介してパターンから抽出され、元のURLは`citrix-oauth-redir://`リダイレクトURLを使用するように書き換えられます。フローが完了すると、元のリダイレクトURLはホスト（VDA）にリダイレクトされます。この場合、任意のOAuth認証サーバーは、`citrix-oauth-redir://byIndex/1 (2, 3, ... N)`リダイレクトURLを許可するように構成されている必要があります。

クライアントからVDAへのリダイレクトの場合、リダイレクトする各リソースに対して**clientToHostConfig**を作成します。 各リソースには、次のパラメーターを含めます。

- **publishedAppOrDesktopNameType**: (必須) Studioで構成された公開デスクトップ（「Desktop」）または公開アプリケーション（「Application」）のいずれか。リソースが無効な場合、リダイレクトは正しく機能しません。
- **publishedAppOrDesktopName**: (必須) Studioで構成されたリソース名。
- **clientToHostUrls**: (必須) クライアントからホスト（VDA）にリダイレクトされるURLのリスト。ワイルドカードが許可されます。

既知の制限

PowerShellを使用してカスタムURLスキーム（HTTPまたはHTTPSではない）でブラウザを起動すると、カスタムURLはクライアントにリダイレクトされません。

ブラウザコンテンツリダイレクトポリシー設定

ブラウザコンテンツリダイレクト (BCR) は、Citrix Virtual Apps and Desktops™環境内でのWebブラウジングのユーザーエクスペリエンスを向上させます。Webページのレンダリングをユーザーのローカルマシンにオフロードすることで、BCRはサーバー負荷を軽減し、特に複雑なWebサイトやリソースを大量に消費するWebサイトでパフォーマンスを向上させます。 このドキュメントでは、ブラウザコンテンツリダイレクトで利用可能な各ポリシー設定オプションについて詳しく説明します。

ブラウザコンテンツリダイレクト

この設定は、ブラウザコンテンツリダイレクトの主要なオン/オフスイッチとして機能します。

- **機能:** Webページがサーバーでレンダリングされるか、ローカルデバイスでレンダリングされるかを決定します。有効にすると、Citrix Workspace™アプリは、よりスムーズなエクスペリエンスのために、Webコンテンツをデバイスでフェッチして表示しようとします。それが失敗した場合、サーバーでのレンダリングにフォールバックします。
- **オプション:**
  - **許可:** (デフォルト) ブラウザコンテンツリダイレクトを有効にします。
  - **禁止:** ブラウザコンテンツリダイレクトを無効にします。
- **注意点:** 許可されている場合、Citrix Workspaceアプリはクライアントフェッチとクライアントレンダリングを試行します。クライアントフェッチとクライアントレンダリングが失敗した場合、ブラウザコンテンツリダイレクトはサーバー側レンダリングにフォールバックします。サーバーフェッチとクライアントレンダリングを有効にするには、「Browser Content Redirection Proxy Configuration」設定を有効にします。

ブラウザコンテンツリダイレクトACL構成

この設定により、ブラウザコンテンツリダイレクトの使用を許可または禁止するWebサイト（URL）のリストを作成できます。

- **機能:** ブラウザコンテンツリダイレクトで最適化されるWebサイトをきめ細かく制御できます。Webサイト全体または特定のページを指定できます。
- **動作:**
  - **許可されたURL:** このリストにあるWebサイトは、そのコンテンツがデバイスに表示されます。ワイルドカード（）*を使用して、複数のページまたはサブドメイン（例：* `<https://www.example.com/>` または `<http://*.example.com/>`）を含めることができます。URLのプロトコル内ではワイルドカードは許可されません。
- **デフォルト:** `<https://www.youtube.com/*>`
- **例:**
  - **許可されたパターン:** <http://www.xyz.com/index.html, `<https://www.xyz.com/*>` , `<http://www.xyz.com/*videos>` *> , `<http://*.xyz.com/<>` >
  - **許可されていません:** `<http://*.*.com/>`
  - URLでパスを指定することで、より詳細な粒度を実現できます。たとえば、`<https://www.xyz.com/sports/index.html>` を指定した場合、index.htmlページのみがリダイレクトされます

ブラウザーコンテンツリダイレクトブロックリスト構成

この設定は、「Browser Content Redirection ACL Configuration」設定と連携して機能します。

- **機能:** ACL構成で許可されている場合でも、特定のWebサイトやページをブロックできるようにすることで、追加の制御レイヤーを提供します。ブロックリストが優先されます。
- **動作:** ACL構成によって一般的に許可されている場合でも、デバイスにリダイレクトされたくないWebサイトやページを指定します。
- **デフォルト:** URLは構成されていません
- **ワイルドカード:** ACL構成と同様に、ワイルドカード (*) を使用して複数のページまたはサブドメインをブロックできます。
- **例:** Webサイトのindex.htmlページのみをブロックするには、次のように入力します。
  `<https://www.example.com/sports/index.html>`

ブラウザーコンテンツリダイレクト認証サイト

この設定により、外部のIDプロバイダー (IdP) を使用してログインするWebサイトでのBrowser Content Redirectionの動作を管理できます。

- **機能:** 認証のために別のWebサイトにリダイレクトされた場合でも (WebサイトがOktaやその他のサービスをログインに使用する場合など)、Browser Content Redirectionがアクティブな状態を維持するようにします。
- **動作:** 認証WebサイトのURLをこのリストに追加することで、ログイン中にリダイレクトプロセスが中断されないようにします。
- **デフォルト:** URLは構成されていません
- **例:** www.example.com が認証に www.example.okta.com を使用する場合、www.example.com/ を Browser content redirection ACL configuration に、認証Webサイト www.example.okta.com を Browser content redirection authentication sites に追加します。
- **詳細情報:** 詳細については、Citrix Knowledge Centerの記事CTX238236および「Browser Content Redirection」の「マルチメディア」セクションを参照してください。

ブラウザコンテンツリダイレクトのプロキシ構成

この設定により、ブラウザコンテンツリダイレクトがネットワークのプロキシサーバーをどのように使用するかをより詳細に制御できます。また、環境でクライアントフェッチクライアントレンダリングが許可されていない場合に、サーバーフェッチクライアントレンダリングを容易にします。

- **機能:** Citrix Workspaceアプリに、Webコンテンツの取得にサーバーフェッチ方式の使用を強制します。有効にすると、常にサーバーからコンテンツを取得し、デバイスに表示しようとします。
- **オプション:**
  - 明示的なプロキシ: 特定のプロキシサーバーを使用します。プロキシサーバーのアドレスとポート番号（例：`<http://proxy.example.com:80>`）を指定する必要があります。
    - 許可されるパターン:
    - http://<hostname/ip address\>:\<port\> | 例: `<http://proxy.example.citrix.com:80>` `<http://10.10.10.10:8080>`
  - PAC/WPAD: PACファイルまたはWPADを使用して、プロキシ設定を自動的に決定します。PACファイルのURL（例：`<http://wpad.myproxy.com:30/configuration/pac/Proxy.pac>`）を指定する必要があります。
    - PAC/WPADファイルに許可されるパターン:
    - http://<hostname/ip address\>:<port\>/<path\>/<Proxy\>.pac | 例: `<http://wpad.myproxy.com:30/configuration/pac/Proxy.pac>`
    - https://<hostname/ip address\>:<port\>/<path\>/<wpad.dat\> | 例: `<http://10.10.10.10/configuration/pac/wpad.dat>`
  - 直接/透過: プロキシサーバーを使用しないか、透過プロキシを使用します。
    - キーワード「DIRECT」を構成します
    - このキーワードは大文字と小文字を区別します
- **既定値:** 禁止 (無効)

ブラウザコンテンツリダイレクトの統合Windows認証サポート

この設定により、統合Windows認証 (IWA) を使用するWebサイトへのログインが簡素化されます。

- **動作:** ブラウザコンテンツリダイレクトが既存のWindows資格情報を使用してWebサイトに自動的にログインできるようにします。これにより、ユーザー名とパスワードを繰り返し入力する必要がなくなります。
- **オプション:**
  - **許可:** IWAを使用するWebサイト向けにシングルサインオン (SSO) を有効にします。
  - **禁止:** (既定値) SSOを無効にし、毎回資格情報を入力する必要があります。

ブラウザコンテンツリダイレクトのサーバーフェッチプロキシ認証

この設定は、サーバーからコンテンツをフェッチする際に、ブラウザコンテンツリダイレクトがWebプロキシとどのように対話するかを制御します。

- **動作:** ブラウザコンテンツリダイレクトがWindows資格情報を使用してプロキシサーバーで認証できるようにし、Webコンテンツへの安全なアクセスを確保します。
- **仕組み:** 有効にすると、ブラウザコンテンツリダイレクトはKerberosサービスチケットを自動的に取得して使用し、プロキシで認証します。
- **要件:** PACファイルを構成してダウンストリームWebプロキシを介してトラフィックをルーティングし、プロキシがKerberos認証を使用するように設定する必要があります。
- **オプション:**
  - **許可:** プロキシサーバーとのKerberos認証を有効にします。
  - **禁止:** (既定値) ブラウザコンテンツリダイレクトは、プロキシで認証するために基本認証またはその他の利用可能な資格情報を使用します。

クライアントセンサーポリシー設定

クライアントセンサーセクションには、ユーザーセッションでモバイルデバイスのセンサー情報がどのように処理されるかを制御するためのポリシー設定が含まれています。

アプリケーションによるクライアントデバイスの物理的な位置情報の使用を許可する

この設定は、モバイルデバイス上のセッションで実行されているアプリケーションが、ユーザーデバイスの物理的な位置情報を使用できるかどうかを決定します。

デフォルトでは、位置情報の使用は禁止されています。

この設定が禁止されている場合、アプリケーションが位置情報を取得しようとすると、「アクセス拒否」の値が返されます。

この設定が許可されている場合、ユーザーはCitrix Workspace™アプリの位置情報へのアクセス要求を拒否することで、位置情報の使用を禁止できます。AndroidおよびiOSデバイスでは、各セッションで位置情報が最初に要求されたときにプロンプトが表示されます。

「アプリケーションによるクライアントデバイスの物理的な位置情報の使用を許可する」設定を使用するホスト型アプリケーションを開発する際は、以下を考慮してください。

- 位置情報が有効なアプリケーションが位置情報の利用可能性に依存しないようにしてください。その理由は次のとおりです。
  - ユーザーが位置情報へのアクセスを許可しない可能性があります。

  - アプリケーションの実行中に位置情報が利用できない、または変更される可能性があります。
  - ユーザーが位置情報をサポートしていない別のデバイスからアプリケーションセッションに接続する可能性があります。

- 位置情報が有効なアプリケーションは、次の条件を満たす必要があります。
  - 位置情報機能をデフォルトでオフにする。
  - アプリケーションの実行中に、ユーザーがその機能を許可または禁止するオプションを提供する。
  - アプリケーションがキャッシュする位置データをクリアするオプションをユーザーに提供します。(Citrix Workspaceアプリは位置データをキャッシュしません。)
- 位置情報対応アプリケーションは、位置情報の粒度を管理する必要があります。この管理により、取得されたデータがアプリケーションの目的に適切であることが保証されます。また、関連するすべての法域の規制に準拠します。
- 位置情報サービスを使用する場合は、安全な接続 (TLS または VPN の使用など) を強制します。Citrix Workspaceアプリを信頼できるサーバーに接続します。
- 位置情報サービスの使用に関して、法的助言を得ることを検討してください。

デスクトップUIポリシー設定

デスクトップUIセクションには、デスクトップの壁紙、メニューアニメーション、ドラッグイメージなどの視覚効果を制御するポリシー設定が含まれています。これらのポリシー設定は、クライアント接続で使用される帯域幅の管理に役立ちます。帯域幅の使用量を制限することで、WANでのアプリケーションパフォーマンスを向上させることができます。

> **重要:**
>
> このリリースでは、レガシーグラフィックモードとデスクトップコンポジションリダイレクト（DCR）はサポートされていません。このポリシーは、以下を使用する場合の旧バージョンとの互換性のためだけに含められています。
>
> - XenApp 7.15 LTSR
> - XenDesktop 7.15 LTSR
> - Windows 7およびWindows 2008 R2を使用している以前のVDAリリース。

デスクトップコンポジションリダイレクト

この設定は、ユーザーによりスムーズなWindowsデスクトップエクスペリエンスを提供するために、ローカルのDirectXグラフィックレンダリングに以下の処理能力を使用するかどうかを指定します。

- ユーザーデバイス上のグラフィック処理ユニット（GPU）
- または、,
- ユーザーデバイス上の統合グラフィックプロセッサ（IGP）

有効にすると、**デスクトップコンポジションリダイレクト**は、サーバーの高いスケーラビリティを維持しながら、応答性の高いWindowsエクスペリエンスを提供します。

デフォルトでは、**デスクトップコンポジションリダイレクト**は無効になっています。

デスクトップコンポジションリダイレクトの選択を解除し、ユーザーセッションで必要な帯域幅を削減するには、この設定をポリシーに追加するときに、**無効**を選択します。

デスクトップコンポジションリダイレクトのグラフィック品質

この設定は、デスクトップコンポジションリダイレクトに使用されるグラフィックの品質を指定します。

デフォルトは「高」です。

「高」、「中」、「低」、または「ロスレス」品質から選択します。

デスクトップの壁紙

この設定は、ユーザーセッションでの壁紙の表示を許可または禁止します。

デフォルトでは、ユーザーセッションで壁紙を表示できます。

デスクトップの壁紙を選択解除し、ユーザーセッションで必要な帯域幅を削減するには、この設定をポリシーに追加する際に「**禁止**」を選択します。

メニューアニメーション

この設定は、ユーザーセッションでのメニューアニメーションを許可または禁止します。

デフォルトでは、メニューアニメーションは許可されています。

メニューアニメーションは、アクセシビリティのためのMicrosoftの個人設定です。有効にすると、短い遅延の後、スクロールまたはフェードインによってメニューが表示されます。メニューの下部には矢印アイコンが表示されます。その矢印をポイントするとメニューが表示されます。

このポリシー設定が「**許可**」に設定されており、メニューアニメーションのMicrosoft個人設定が有効になっている場合、デスクトップでメニューアニメーションが有効になります。

> **注:**
>
> メニューアニメーションのMicrosoft個人設定への変更は、デスクトップに影響を与えます。セッション終了時に変更を破棄するようにデスクトップを設定している場合を考慮してください。この場合、メニューアニメーションを有効にしているユーザーは、その後のセッションでメニューアニメーションを利用できない可能性があります。メニューアニメーションを必要とするユーザーに対しては、デスクトップのメインイメージでMicrosoft設定を有効にするか、デスクトップがユーザーの変更を保持するようにしてください。

ドラッグ中のウィンドウコンテンツの表示

この設定は、画面上でウィンドウをドラッグする際にウィンドウコンテンツの表示を許可または禁止します。

デフォルトでは、ウィンドウコンテンツの表示は許可されています。

「**許可**」に設定すると、ウィンドウをドラッグしたときにウィンドウ全体が移動するように見えます。「**禁止**」に設定すると、ドロップするまでウィンドウのアウトラインのみが移動するように見えます。

エンドユーザー監視ポリシー設定

「**エンドユーザー監視**」セクションには、セッションのトラフィックを測定するためのポリシー設定が含まれています。

エンドポイントの位置情報データ収集

デフォルトでは、このポリシーは無効になっています。 有効にすると、エンドポイントデバイスのパブリックIPアドレス、国、都市、インターネットサービスプロバイダー（ISP）を含むエンドポイントの位置情報が収集されます。 収集されたデータは、選択したユーザーセッションの**セッションパフォーマンス**タブの下にあるCitrix DirectorまたはMonitorに表示されます。

エンドポイントネットワーク遅延測定間隔

デフォルトでは、このポリシーは無効になっています。 この設定は、エンドポイントがネットワーク遅延を測定する頻度を秒単位で指定します。 有効にすると、収集されたデータは、選択したユーザーセッションの**セッションパフォーマンス**タブの下にあるCitrix DirectorまたはMonitorに表示されます。

エンドポイント統計間隔

ネットワークインターフェースタイプ、信号強度、リンク速度、スループット（送信）、スループット（受信）などのエンドポイント統計は、DirectorまたはMonitor UIのセッショントポロジでエンドポイントテレメトリとして利用できます。このテレメトリは、エンドユーザーセッションの問題のトリアージに役立ちます。 エンドポイント統計間隔は、DirectorまたはMonitor UIのセッショントポロジでエンドポイントテレメトリが更新される頻度を秒単位で示します。デフォルトでは、エンドポイントテレメトリは有効になっており、60秒ごとに更新されます。 収集されたデータは、選択したユーザーセッションの**セッションパフォーマンス**タブの下にあるCitrix DirectorまたはMonitorに表示されます。

ICA®ラウンドトリップ計算

この設定は、アクティブな接続に対してICAラウンドトリップ計算が実行されるかどうかを決定します。

デフォルトでは、アクティブな接続の計算は有効になっています。

デフォルトでは、各ICAラウンドトリップ測定の開始は遅延されます。この遅延は、ユーザーインタラクションを示すトラフィックが発生するまで続きます。この遅延は無期限に続く可能性があり、ICAラウンドトリップ測定がICAトラフィックの唯一の原因となるのを防ぐように設計されています。

ICAラウンドトリップ計算間隔

この設定は、ICAラウンドトリップ計算が実行される頻度を秒単位で指定します。

デフォルトでは、ICAラウンドトリップは15秒ごとに計算されます。

アイドル接続のICAラウンドトリップ計算

この設定は、アイドル接続に対してICAラウンドトリップ計算が実行されるかどうかを決定します。

デフォルトでは、アイドル接続に対して計算は実行されません。

デフォルトでは、各ICAラウンドトリップ測定の開始は遅延されます。この遅延は、ユーザー操作を示すトラフィックが発生するまで続きます。この遅延は無期限になる可能性があり、ICAラウンドトリップ測定がICAトラフィックの唯一の原因となるのを防ぐように設計されています。

強化されたデスクトップエクスペリエンスポリシー設定

強化されたデスクトップエクスペリエンスポリシー設定は、ローカルのWindows 7デスクトップのように見えるサーバーオペレーティングシステム上でセッションを実行します。

デフォルトでは、この設定は許可されています。

仮想デスクトップ上にWindowsクラシックテーマのユーザープロファイルが存在する場合、このポリシーはそのユーザーに強化されたデスクトップエクスペリエンスを提供しません。Windows 7テーマのユーザープロファイルを持つユーザーが、Windows Server 2012を実行している仮想デスクトップにログオンする場合を考えます。また、このポリシーが構成されていないか、無効になっている場合、そのユーザーはテーマの適用に失敗したことを示すエラーメッセージを目にします。

どちらの場合も、ユーザープロファイルをリセットすることで問題が解決します。

アクティブなユーザーセッションを持つ仮想デスクトップでポリシーを無効にすると、それらのセッションのインターフェイスは、Windows 7およびWindows Classicデスクトップで一貫性がなくなります。この不整合を避けるために、このポリシー設定を変更した後、仮想デスクトップを再起動してください。その後、仮想デスクトップ上のすべてのローミングプロファイルを削除します。Citrix®は、プロファイル間の不整合を避けるために、仮想デスクトップ上の他のユーザープロファイルも削除することを推奨します。

環境でローミングユーザープロファイルを使用しているとします。この場合、プロファイルを共有するすべての仮想デスクトップで、強化されたデスクトップエクスペリエンス機能が有効または無効になっていることを確認してください。

Citrixは、サーバーオペレーティングシステムとクライアントオペレーティングシステムを実行している仮想デスクトップ間でローミングプロファイルを共有することを推奨しません。クライアントおよびサーバーオペレーティングシステムのプロファイルは異なります。両方のタイプ間でローミングプロファイルを共有すると、ユーザーが両者の間を移動する際にプロファイルプロパティに不整合が生じる可能性があります。

ファイルリダイレクトポリシー設定

ファイルリダイレクトセクションには、クライアントドライブマッピングおよびクライアントドライブ最適化に関連するポリシー設定が含まれています。

クライアントドライブの自動接続

この設定は、ユーザーがログオンしたときのクライアントドライブの自動接続を許可または禁止します。

デフォルトでは、自動接続は許可されています。

この設定をポリシーに追加するときは、自動接続するドライブの種類の設定を必ず有効にしてください。たとえば、ユーザーのCD-ROMドライブの自動接続を許可するには、この設定と**クライアント光学ドライブ**設定を構成します。

関連するポリシー設定は次のとおりです。

- **クライアントドライブリダイレクト**
- **クライアントフロッピーディスクドライブ**
- **クライアント光学ドライブ**
- **クライアント固定ドライブ**
- **クライアントネットワークドライブ**
- **クライアントリムーバブルドライブ**

クライアントドライブリダイレクト

この設定は、ユーザーデバイス上のドライブとの間でファイルリダイレクトを有効または無効にします。

デフォルトでは、ファイルリダイレクトは有効になっています。

> **注:**
>
> クライアントドライブリダイレクトポリシー設定は、汎用USBリダイレクトを使用してセッションにマップされたドライブには適用されません。

> 有効にすると、ユーザーはすべてのクライアントドライブにファイルを保存できます。無効にすると、すべてのファイルリダイレクトが防止されます。この構成は、個々のファイルリダイレクト設定の状態に関係なく適用されます。個々のファイルリダイレクト設定には、クライアントフロッピードライブとクライアントネットワークドライブが含まれます。

関連するポリシー設定は次のとおりです。

- **クライアントフロッピードライブ**
- **クライアント光学ドライブ**
- **クライアント固定ドライブ**
- **クライアントネットワークドライブ**
- **クライアントリムーバブルドライブ**

クライアント固定ドライブ

この設定により、ユーザーはユーザーデバイス上の固定ドライブにアクセスしたりファイルを保存したりできるようになります。

デフォルトでは、クライアント固定ドライブへのアクセスは許可されています。

この設定をポリシーに追加する場合は、**クライアントドライブリダイレクト**設定が存在し、許可に設定されていることを確認してください。これらの設定が無効になっている場合、クライアント固定ドライブはマップされず、**クライアント固定ドライブ**設定の状態に関係なく、ユーザーはこれらのドライブに手動でアクセスできません。

ユーザーがログオンしたときに固定ドライブが自動的に接続されるように、**クライアントドライブの自動接続**設定を構成します。

クライアントフロッピードライブ

この設定により、ユーザーはユーザーデバイス上のフロッピードライブにアクセスしたりファイルを保存したりできるようになります。

デフォルトでは、クライアントフロッピードライブへのアクセスは許可されています。

この設定をポリシーに追加する場合、「**クライアントドライブのリダイレクト**」設定が存在し、「許可」に設定されていることを確認してください。これらの設定が無効になっている場合、クライアントフロッピーディスクドライブはマップされず、ユーザーは「**クライアントフロッピーディスクドライブ**」設定の状態にかかわらず、これらのドライブに手動でアクセスできません。

ユーザーがログオンしたときにフロッピーディスクドライブが自動的に接続されるようにするには、「**クライアントドライブの自動接続**」設定を構成します。

クライアントネットワークドライブ

この設定は、ユーザーがユーザーデバイスを介してネットワーク（リモート）ドライブにファイルにアクセスしたり保存したりすることを許可または禁止します。

デフォルトでは、クライアントネットワークドライブへのアクセスは許可されています。

この設定をポリシーに追加する場合、「**クライアントドライブのリダイレクト**」設定が存在し、「許可」に設定されていることを確認してください。これらの設定が無効になっている場合、クライアントネットワークドライブはマップされず、ユーザーはこれらのドライブに手動でアクセスできません。この構成は、「**クライアントネットワークドライブ**」設定の状態にかかわらず適用されます。

ユーザーがログオンしたときにネットワークドライブが自動的に接続されるようにするには、「**クライアントドライブの自動接続**」設定を構成します。

クライアント光学ドライブ

この設定は、ユーザーが以下の場所にファイルにアクセスしたり保存したりすることを許可または禁止します。

- ユーザーデバイス上のCD-ROM
- ユーザーデバイス上のDVD-ROM
- ユーザーデバイス上のBD-ROMドライブ。

デフォルトでは、クライアント光学ドライブへのアクセスは許可されています。

この設定をポリシーに追加する場合、「**クライアントドライブのリダイレクト**」設定が存在し、「**許可**」に設定されていることを確認してください。これらの設定が無効になっている場合、クライアント光学ドライブはマップされず、ユーザーはこれらのドライブに手動でアクセスできません。この構成は、「**クライアント光学ドライブ**」設定の状態にかかわらず適用されます。

ユーザーがログオンしたときに光学ドライブが自動的に接続されるようにするには、「**クライアントドライブの自動接続**」設定を構成します。

クライアントリムーバブルドライブ

この設定により、ユーザーはユーザーデバイス上のUSBドライブへのファイルアクセスまたは保存を許可または禁止されます。

デフォルトでは、クライアントリムーバブルドライブへのアクセスは許可されています。

この設定をポリシーに追加する際は、**クライアントドライブのリダイレクト**設定が存在し、「許可」に設定されていることを確認してください。これらの設定が無効になっている場合、クライアントリムーバブルドライブはマップされず、ユーザーはこれらのドライブに手動でアクセスできません。この構成は、**クライアントリムーバブルドライブ**設定の状態に関係なく適用されます。

ユーザーがログオンしたときにリムーバブルドライブが自動的に接続されるように、**クライアントドライブの自動接続**設定を構成します。

ホストからクライアントへのリダイレクト

この設定により、URLおよび一部のメディアコンテンツのファイルタイプ関連付けを有効または無効にし、ユーザーデバイスで開くことができます。無効にすると、コンテンツはサーバーで開かれます。

デフォルトでは、ファイルタイプ関連付けは無効になっています。

この設定を有効にすると、以下のURLタイプがローカルで開かれます。

- HTTP
- HTTPS
- リアルプレーヤーおよびQuickTime (RTSP)
- リアルプレーヤーおよびQuickTime (RTSPU)
- レガシーReal Player (PNM)
- マイクロソフト メディア サーバー (MMS)

クライアントドライブ文字の保持

この設定により、クライアントドライブをセッション内で同じドライブ文字にマップすることを有効または無効にします。

デフォルトでは、クライアントドライブ文字は保持されません。

この設定をポリシーに追加する場合は、**クライアントドライブのリダイレクト**設定が存在し、許可に設定されていることを確認してください。

読み取り専用クライアントドライブアクセス

この設定は、ユーザーとアプリケーションが以下の操作を行うことを許可または禁止します。

- マップされたクライアントドライブ上にファイルを作成する
- マップされたクライアントドライブ上のファイルを変更する
- マップされたクライアントドライブ上のフォルダーを変更する

デフォルトでは、マップされたクライアントドライブ上のファイルとフォルダーは変更できます。

有効に設定されている場合、ファイルとフォルダーは読み取り専用権限でアクセスできます。

この設定をポリシーに追加する場合は、**クライアントドライブのリダイレクト**設定が存在し、許可に設定されていることを確認してください。

特殊フォルダーのリダイレクト

この設定は、Citrix Workspace™アプリおよびWeb Interfaceのユーザーが、セッションからローカルのドキュメントおよびデスクトップの特殊フォルダーを表示することを許可または禁止します。

デフォルトでは、特殊フォルダーのリダイレクトは許可されています。

この設定は、ポリシーによってフィルター処理されたオブジェクトが特殊フォルダーのリダイレクトを持つことを防ぎます。これは、他の場所に存在する設定に関係なく適用されます。この設定が禁止されている場合、StoreFront™、Web Interface、またはCitrix Workspaceアプリに指定された関連設定はすべて無視されます。

どのユーザーが特殊フォルダーのリダイレクトを使用できるかを定義するには、**許可**を選択し、この機能を適用したいユーザーでフィルター処理されたポリシーにこの設定を含めます。この設定は、他のすべての特殊フォルダーのリダイレクト設定を上書きします。

ユーザーがローカルハードドライブ上のファイルにアクセスしたり保存したりするのを防ぐポリシー設定は、特殊フォルダーリダイレクトの動作も妨げます。この状況は、特殊フォルダーリダイレクトがユーザーデバイスと対話する必要があるために発生します。

この設定をポリシーに追加する際は、**クライアント固定ドライブ**設定が存在し、「許可」に設定されていることを確認してください。

ファイル転送ポリシー

デフォルトでは、ファイル転送は有効になっています。これらのポリシーは、**ユーザー設定 - ICA\ファイルリダイレクト**の下にあります。Web Studioを使用して変更してください。ファイル転送ポリシーを使用する際は、以下を考慮してください。

- **Chrome OS/HTML5向けCitrix Workspaceアプリのファイル転送** - ユーザーがCitrix Virtual Apps and Desktopsセッションとデバイス間でファイルを転送することを許可または禁止します。
- **Chrome OS/HTML5向けCitrix Workspaceアプリのファイルアップロード** - ユーザーがデバイスからCitrix Virtual Apps and Desktopsセッションにファイルをアップロードすることを許可または禁止します。
- **Chrome OS/HTML5向けCitrix Workspaceアプリのファイルダウンロード** - ユーザーがCitrix Virtual Apps and Desktopsセッションからデバイスにファイルをダウンロードすることを許可または禁止します。

> **注:**
>
> ファイル転送ポリシーは、HTML5向けCitrix WorkspaceアプリおよびChrome OS向けCitrix Workspaceアプリにのみ適用されます。

非同期書き込みの使用

この設定は、非同期ディスク書き込みを有効または無効にします。

デフォルトでは、非同期書き込みは無効になっています。

非同期ディスク書き込みは、比較的高い帯域幅と高い遅延が特徴であるWAN経由でのファイル転送速度とクライアントディスクへの書き込み速度を向上させることができます。ただし、接続またはディスクに障害が発生した場合、書き込み中のクライアントファイルが未定義の状態になる可能性があります。この未定義の状態が発生した場合、ポップアップウィンドウで影響を受けるファイルがユーザーに通知されます。ユーザーは、再接続時またはディスク障害が修正されたときに中断されたファイル転送を再開するなどの是正措置を講じることができます。

Citrix®は、リモート接続が必要で、良好なファイルアクセス速度を持ち、接続またはディスク障害が発生した場合に失われたファイルやデータを容易に回復できるユーザーに対してのみ、非同期ディスク書き込みを有効にすることを推奨します。

この設定をポリシーに追加する際は、**クライアントドライブリダイレクト**設定が存在し、「許可」に設定されていることを確認してください。この設定が無効になっている場合、非同期書き込みは行われません。

クリップボードリダイレクト

クリップボードリダイレクトは、Citrix Virtual Apps and Desktops™ の基本的な機能であり、ユーザーのローカルエンドポイントと仮想Citrixセッション間でデータのシームレスなコピー＆ペーストを可能にします。

クリップボードリダイレクトにより、ユーザーはテキスト、画像、ファイルなどのデータを、ローカルデバイスで実行されているアプリケーションとCitrixセッション内のアプリケーション間でコピー＆ペーストできます。これは、ユーザーデバイス上のクリップボードをVDA上のクリップボードにマッピングすることで実現されます。デフォルトでは、クリップボードリダイレクトは許可されています。

クリップボードリダイレクトは、HDX™ プロトコル内の個別の仮想チャネルを介して機能します。ファイル転送とドラッグ＆ドロップには、追加の仮想チャネルが使用されます。ユーザーがローカルデバイスでデータをコピーすると、Citrix Workspace™ アプリがそのデータをインターセプトし、セッションで実行されているアプリケーションにペーストできるようにします。実際のデータは、VDA上のアプリケーションにペーストされた場合に転送されます。このプロセスは、Citrixセッションからクライアントにコピーする場合も同様に機能します。

このクライアントからセッションへ、およびセッションからクライアントへのクリップボードリダイレクトの組み合わせは、双方向クリップボードリダイレクトとも呼ばれます。

> **注:**

> 詳細については、Citrix Virtual Channels を参照してください。

主要な概念

クライアントからセッションへ (Endpoint to Session または client to VDA とも呼ばれます)。ユーザーのローカルデバイスでコピーされたデータ（クリップボードに置かれたデータ）は、仮想セッション内にペーストできるようになります。

セッションからクライアントへ (Session to Endpoint または VDA to client とも呼ばれます)。仮想セッション内のアプリケーションからコピーされたデータは、ユーザーのローカルデバイスにペーストできるようになります。

クロスセッション (セッション間またはVDA間)。ローカルエンドポイントのクリップボードに保存されることなく、あるCitrixセッションからコピーされたデータを別のCitrixセッションにペーストできる新しいクリップボード転送方法です。この機能は、Citrix Virtual Apps and Desktops™ バージョン2507でプレビュー機能として利用可能であり、クロスセッションクリップボード交換機能と呼ばれています。詳細については、「クロスセッションクリップボード」を参照してください。

構成

クリップボードリダイレクトは、Citrix®ポリシーによって制御されます。これらのポリシーは、クリップボードリダイレクトの動作を細かく調整するためのさまざまな設定を提供します。

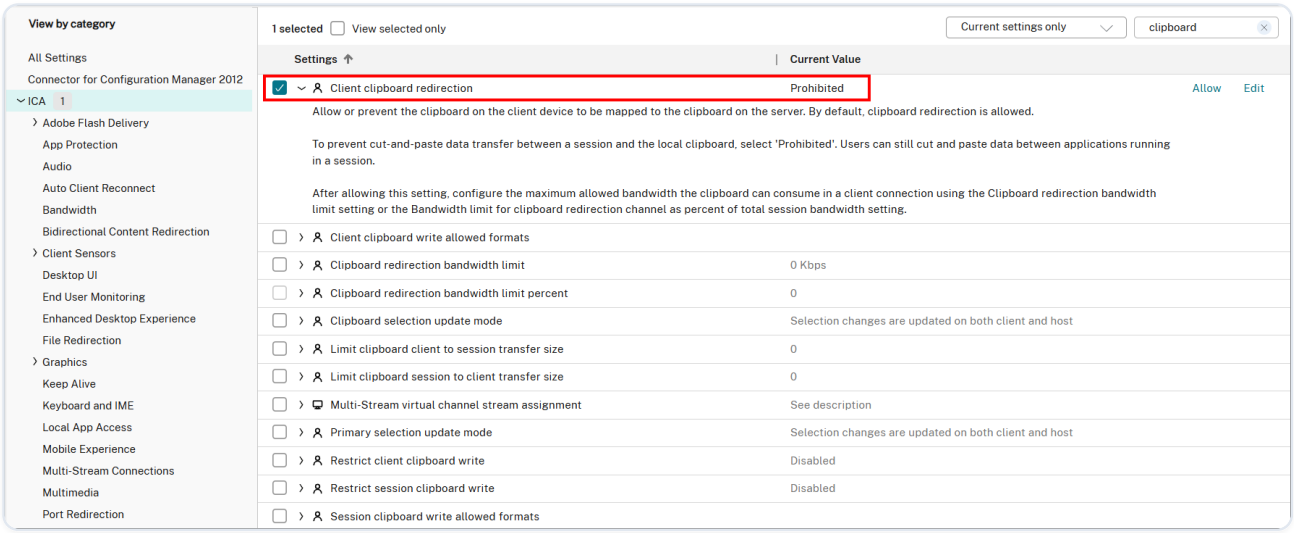
デフォルトでは、双方向クリップボードリダイレクトが有効になっています。ユーザーはCitrixセッションからローカルエンドポイントへ、またはその逆方向へデータをコピー＆ペーストできます。

コア設定

コアとなるクリップボードリダイレクトの設定は、「クライアントクリップボードリダイレクトポリシー」です。このポリシーは、クリップボードリダイレクトが許可されるかどうかを制御します。デフォルトでは、クリップボードリダイレクトは許可されています。

クリップボードリダイレクトを無効にすると、Citrix仮想環境外への機密データの偶発的または悪意のある転送を防ぐことで、セキュリティを向上させることができます。また、クリップボードを介して潜在的に有害なデータがCitrix環境に導入されるのを防ぐのにも役立ちます。ただし、これはエンドユーザーエクスペリエンスに悪影響を与える可能性があります。

クリップボードリダイレクトを禁止するには、「クライアントクリップボードリダイレクトポリシー」を「禁止」に設定します。



「禁止」に設定されている場合、クリップボードリダイレクトは完全に無効になり、他のすべてのクリップボード関連ポリシーは無視されます。

ユーザーは、Citrixセッション内で実行されているアプリケーションとローカルエンドポイントデバイスの間でデータをコピー＆ペーストすることはできますが、Citrixセッションとの間でコピー＆ペーストすることはできません。

方向性クリップボード制御

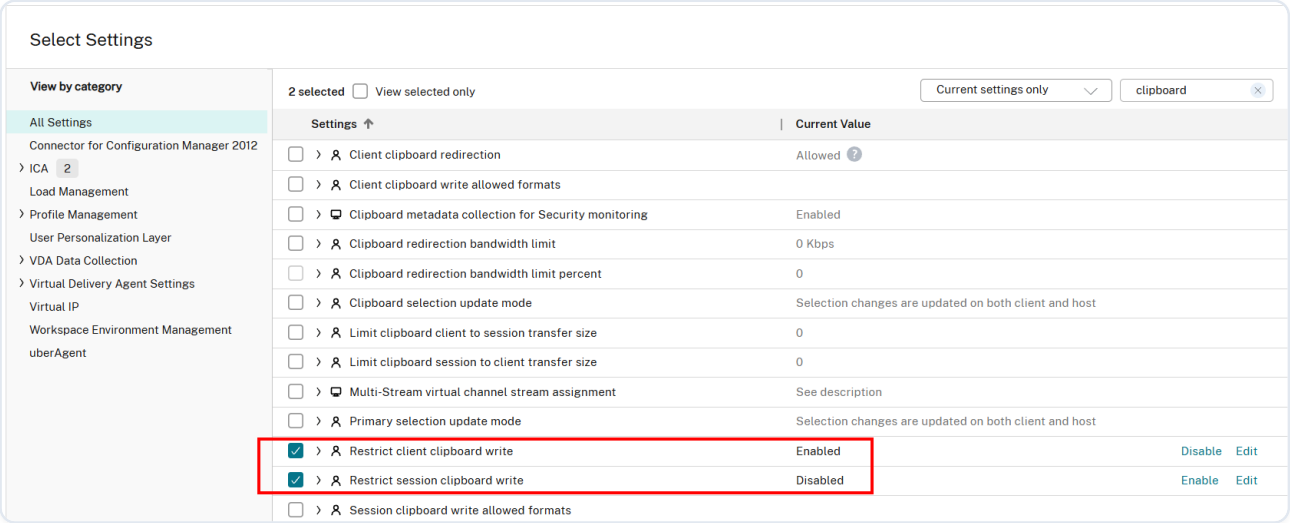
方向性クリップボード制御により、管理者はクリップボードデータフローの方向をきめ細かく制御できます。これは単方向クリップボード制御とも呼ばれます。

単方向制御には、主に2つのモードがあります。

- **クライアントからセッションへ:** この構成では、「クライアントクリップボード書き込みの制限」ポリシーが使用され、クリップボードデータはユーザーのエンドポイントデバイス（クライアント）からリモートCitrixセッションへ排他的に流れることが許可されます。これは、ユーザーがローカルマシンから情報をコピーしてCitrixセッション内で実行されているアプリケーションに貼り付けることはできるが、Citrixセッションからデータをコピーしてローカルマシンに貼り戻すことはできないことを意味します。このモードは、セキュアなセッションから制御の少ないエンドポイントへのデータ漏洩が重大な懸念事項であるシナリオで役立ちます。
- **セッションからクライアントへ:** この構成では、「セッションクリップボード書き込みの制限」ポリシーにより、クリップボードデータはCitrixセッションからクライアントデバイスへ排他的に流れることが許可されます。ユーザーはリモートセッション内のアプリケーションから情報をコピーしてローカルマシンに貼り付けることはできるが、ローカルマシンからデータをコピーしてCitrixセッションに貼り付けることはできません。この設定は、エンドポイントからセキュアなCitrix環境への潜在的に悪意のある、または不正なデータの導入を防ぐことが主な目的である場合によく使用されます。

次の表は、単方向クリップボード制御のためのCitrixクリップボードポリシーについて説明しています。

クリップボードの方向性	クリップボードポリシー
双方向 - セッションからクライアント、およびクライアントからセッション	クライアントクリップボードリダイレクト: 有効 (デフォルト)
一方向 - クライアントからセッションのみ	クライアントクリップボードリダイレクト: 有効 (デフォルト)
クライアントクリップボード書き込みの制限: 有効	一方向 - セッションからクライアントのみ
クライアントクリップボードリダイレクト: 有効 (デフォルト)	セッションクリップボード書き込みの制限: 有効



上記の例では、両方の方向性クリップボードポリシーが強調表示されており、この構成では、「クライアントクリップボード書き込みの制限」設定が「有効」に設定されているため、クライアントからセッションへのクリップボードリダイレクトのみが許可されます。

クリップボード形式の制御

Citrixのクリップボード形式制御ポリシーは、データ転送を特定のクリップボード形式に制限することでクリップボードのセキュリティを強化し、セッションとクライアント間、およびその逆方向でコピー＆ペーストできるデータの種類を制御します。これにより、特定のクリップボードデータ形式を選択的に許可または拒否できます。

クリップボード交換形式は、マルチメディアプログラムから複雑なスプレッドシートやワープロまで、さまざまなアプリケーション間で情報をシームレスに転送するために使用されます。これら

の形式は、コピー、切り取り、貼り付けが可能なデータの構造とエンコーディングを定義し、アプリケーションが交換されるコンテンツを理解し処理できるようにします。

例えば、Webブラウザからテキストをコピーして Word文書に貼り付ける場合、クリップボードはテキストベースの形式を使用します。しかし、コピーされたコンテンツに画像、表、またはリッチテキスト形式が含まれている場合、クリップボードは元の外観と構造を保持するために、RTF（リッチテキスト形式）やHTML（ハイパーテキストマークアップ言語）のようなより高度な形式を利用します。同様に、CADプログラムとプレゼンテーションツールのような特殊なアプリケーション間でデータを交換する場合、クリップボードはグラフィックデータや複雑なデータの正確な表現を保証するために、アプリケーション固有の形式または一般的なメタファイル形式を使用することがあります。

クリップボード形式制御ポリシーは、方向性クリップボード制御ポリシーと連携して機能するように設計されています。

クリップボード形式制御を使用すると、管理者は例えばどの形式が許可されるかを設定できます。

- 両方向でプレーンテキストのみを許可する
- セッションからクライアントへのクリップボード転送をプレーンテキストと画像のみに許可する

または、クライアントからセッションへの貼り付けが可能な形式を制限しつつ、セッションからクライアントへの貼り付けはすべての形式を許可する組み合わせも可能です。

クリップボード形式の動作を制御する主要なポリシーは2つあります。

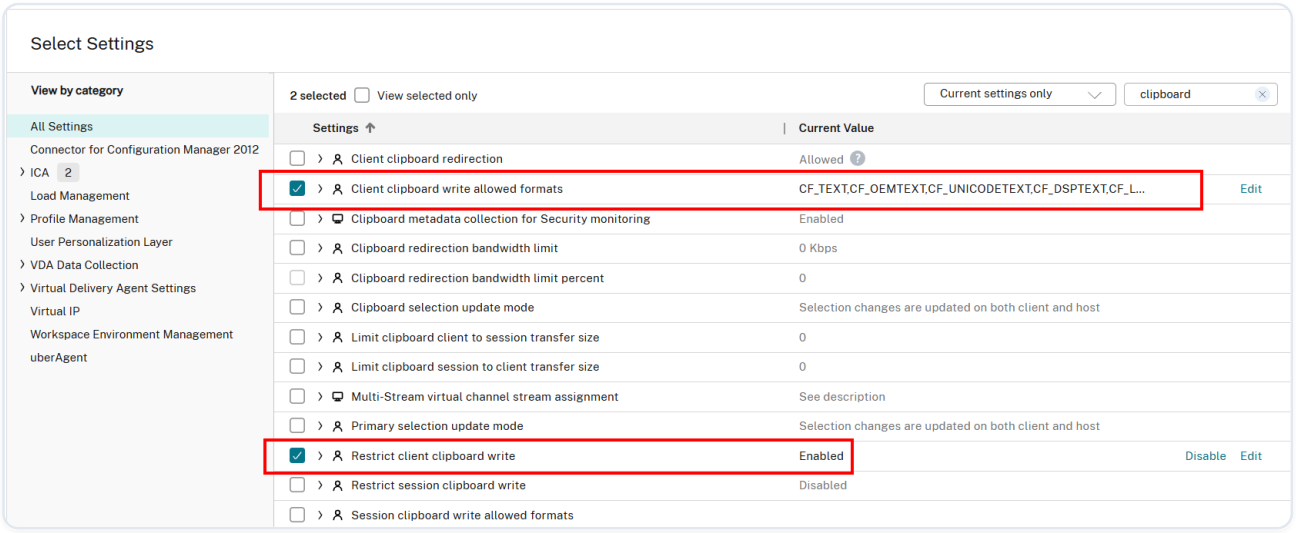
クライアントクリップボード書き込み許可形式: このポリシーは、リモートセッションからクライアントクリップボードに書き込むことが許可されるクリップボードデータ形式を明示的に規定します。例えば、管理者はこのポリシーを設定して、プレーンテキストのみをクライアントにコピーできるようにし、悪意のある可能性のあるリッチテキスト、画像、またはファイルの転送を防ぐことができます。

セッションクリップボード書き込み許可形式: 次に、このポリシーは、クライアントからリモートセッションにコピーすることが許可されるクリップボードデータ形式を指定します。このポリシーは、リモート環境に転送できる情報の種類を制御するために不可欠です。組織は、これをプレーンテキストのみに制限することで、ユーザーが誤ってまたは意図的にローカルマシンから機密ファイルや画像を、セキュリティの低いまたは不正なリモートアプリケーションに貼り付けるのを防ぐことができます。

注:

クリップボードの許可形式は、対応する一方向クリップボードポリシーも設定されている場合にのみ評価されます。

クライアントクリップボードの書き込み形式をテキストベースのデータ形式のみに制限するには、「クライアントクリップボード書き込みの制限」ポリシーと「クライアントクリップボード書き込み許可形式」の両方を構成する必要があります。この例では、「クライアントクリップボード書き込みの制限」を**有効**に設定し、「クライアントクリップボード書き込み許可形式」にはすべてのクリップボードテキスト形式を含める必要があります。



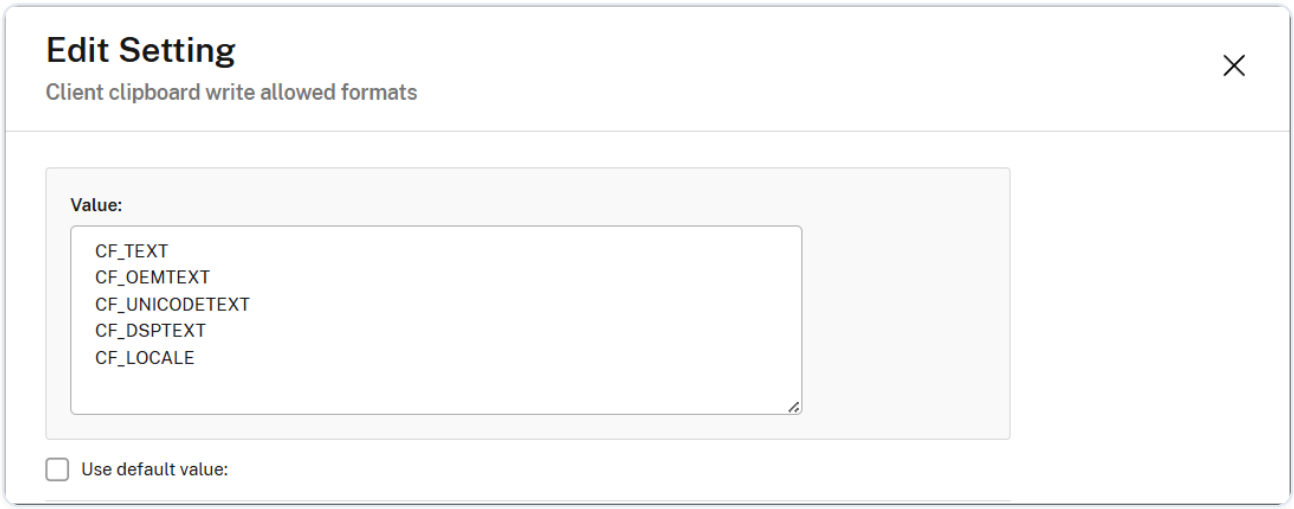
書き込み形式の制限を構成するには、対応するポリシーを編集し、各エントリが別々の行に配置されていることを確認してください。

例として：

CF_TEXT CF_BITMAP

は正しいですが、以下は正しくありません：

CF_TEXT,CF_BITMAP



標準クリップボード形式

以下の表は、標準クリップボード形式について説明しています。

クリップボード形式	タイプ	説明
CF_TEXT	テキスト形式	標準ANSI文字セットのテキスト。各行は復帰/改行 (CR-LF) の組み合わせで終わります。
CF_OEMTEXT	テキスト形式	Original Equipment Manufacturer (OEM) 文字セットを使用したテキスト。CF_TEXT に類似しています。
CF_UNICODETEXT	テキスト形式	Unicode形式のテキスト。ヌル終端文字は不要です。
CF_LOCALE	テキスト形式	クリップボードテキストに関連付けられたロケール識別子へのハンドル。これにより、テキストの言語と地域設定を正しく解釈できます。
CF_HTML*	テキスト形式	HTML形式のテキストを表し、リッチテキスト、リンク、画像をサポートするアプリケーション間でコピー＆ペーストできます。

クリップボード形式	タイプ	説明
CF_BITMAP	画像形式	デバイス依存のビットマップ。画像データは特定の出力デバイスに固有です。
CF_DIB	画像形式	デバイス非依存のビットマップ。この形式には色情報と寸法が含まれており、どのデバイスでも正しく表示できます。
CF_DIBV5	画像形式	CF_DIB (デバイス非依存ビットマップ、バージョン5) の拡張で、カラープロファイルや透明度用のアルファチャンネルなど、より高度な機能が含まれています。
CF_PALETTE	画像形式	カラーパレットへのハンドル。アプリケーションが他のクリップボードデータ（通常はビットマップ）の色を制御するために使用します。
CF_TIFF	画像形式	タグ付き画像ファイル形式。出版や写真で使われる一般的な高品質画像形式です。
CF_METAFILEPIC	メタファイル形式	メタファイルピクチャ構造体へのハンドル。これは、画像を再作成するためのGDI (Graphics Device Interface) 関数のコレクションを保存する古い形式です。
CF_ENHMETAFILE**		拡張メタファイルへのハンドル。これはCF_METAFILEPICTのより現代的で堅牢なバージョンであり、より優れた画質とデバイス非依存性を提供します。

注:

- HTML形式はデフォルトで無効になっています。HTML形式のクリップボードサポートを有効にすると、セキュリティリスクが生じる可能性があります。Webページからコンテンツをコピーすると、埋め込まれたスクリプトもコピーされます。このコンテンツがHTMLをレンダリングするアプリケーションに貼り付けられると、スクリプトが実行される可能性があります。この形式を有効にする際は注意してください。
- Citrix Virtual Apps and Desktops™ 2511より前のバージョンでは、拡張メタファイルクリップボード転送は利用できません。 これらの標準形式に加えて、Citrix®はデータ交換形式や特殊形式などの特定のクリップボードデータ形式もサポートしています。

データ交換形式

クリップボードのデータ交換形式は、マルチメディアプログラムやスプレッドシートなどのさまざまなアプリケーション間でのデータ転送を容易にします。

クリップボード形式	説明
CF_SYLK	シンボリックリンク形式。MicrosoftがMicrosoft Excelのようなスプレッドシートアプリケーション間でデータを交換するために作成した古い形式です。
CF_DIF	データ交換形式。スプレッドシートプログラム間でデータを交換するためのテキストベースの形式です。
CF_RIFF	リソース交換ファイル形式。オーディオやビデオなどのマルチメディアデータを保存するためのコンテナ形式です。
CF_WAVE	波形オーディオ形式。オーディオデータを表します。

特殊形式とシステム形式

これらの形式は、ファイルのドロップ、プライベートデータ、カスタムレンダリングの処理など、特殊な目的に使用されます。

クリップボード形式	説明
CF_HDROP	ドロップされたファイルのリストへのハンドル。これは、ファイルシステムからのドラッグアンドドロップ操作（例: アプリケーションウィンドウへのファイルのドロップ）に使用されます。
CF_PENDATA	ペンコンピューティングアプリケーションで使用される、ペンまたはスタイラスからのデータを表します。
CF_OWNERDISPLAY	クリップボードにデータを配置した元のウィンドウが、クリップボードビューア内のコンテンツの描画と更新を担当する形式です。

CF_DSPTEXT、CF_DSPBITMAP、CF_DSPMETAFILEPICT、CF_DISPENHMETAFILE は、標準形式（TEXT、BITMAP など）に対応する「表示」形式ですが、クリップボードビューアアプリケーション内でレンダリングできるプライベートデータに使用されます。これらはアプリケーション固有の使用を目的としています。

CITRIX VIRTUAL APPS AND DESKTOPS™ クリップボード形式

CFX クリップボード形式は、カスタマイズされた Citrix Virtual Apps and Desktops™ クリップボード形式です。これらは、通常のクリップボード形式と比較して高度に最適化されています。

クリップボード形式	説明
CFX_RICHTEXT	異なるフォント、サイズ、色、太字や斜体などのスタイルを含む、書式設定されたテキストを効率的に転送するために使用されます
CFX_OfficeDrawingShape	Microsoft Office の描画オブジェクトを処理します。これにより、ユーザーは Office アプリケーション (Word、Excel、PowerPoint など) で作成されたベクターシェイプ、図、その他のグラフィックをコピー＆ペーストできます
CFX_BIFF8	これは BIFF8 (Binary Interchange File Format 8) に対応し、Microsoft Excel 97-2003 のネイティブファイル形式です。CFX_BIFF8 は、Excel スプレッドシート間でデータと数式をコ

クリップボード形式	説明
	ピー＆ペーストするための Citrix に最適化されたバージョンです。
CFX_FILE*	ファイルオブジェクトの転送に使用されます。ローカルコンピューターでファイルをコピーし、仮想デスクトップに貼り付ける (またはその逆を行う) とき、この形式がデータ転送を管理します。これは標準の CF_HDROP 形式に代わる最適化されたものです。

注:

ファイルのコピー＆ペーストとドラッグ＆ドロップを許可するには、CFX_FILE を許可された形式に明示的に追加する必要があります。

カスタムクリップボード形式

これらのクリップボード形式の他に、追加のカスタムクリップボード形式も構成できます。これは、VDA上のオペレーティングシステムに登録されている形式にのみ適用されます。

詳細については、カスタム登録クリップボード形式を参照してください。

変換可能なクリップボード形式

Microsoft Windowsは、さまざまなクリップボード形式をネイティブでサポートしています。クリップボードの内容をコピーして貼り付ける際、Windowsはクリップボードデータを他の互換性のあるクリップボード形式に自動的に変換しようとし、異なるアプリケーションにコンテンツを貼り付けやすくします。

データ形式がクリップボードに投稿されると、Windowsは、他のアプリケーションへの貼り付けが成功する可能性を高めるために、元々投稿された形式のいずれかから変換して取得できる追加の形式を自動的に追加します。

ターゲットアプリケーションが、ソースが直接提供できない形式を要求した場合、Windowsはクリップボードデータをある形式から別の形式に自動的に変換します。

たとえば、ワープロから書式設定されたテキストをコピーすると、Windowsは、元の書式設定されたテキストだけでなく、プレーンテキストなどの他の形式を要求元のアプリケーションで利用できるようにします。

別の例として、クリップボードデータにCF_TEXTクリップボード形式のプレーンテキストデータが含まれており、データを貼り付けるアプリケーションがCF_UNICODETEXT形式のUnicodeテキストを要求した場合、Windowsは貼り付け処理中にクリップボードデータを自動的に変換します。

注:

一部の変換では、たとえばリッチテキストをプレーンテキストに自動変換する場合など、情報が失われる可能性があります。

クリップボード形式	説明
CF_TEXT	CF_TEXT
	CF_OEMTEXT
	CF_UNICODETEXT
	CF_LOCALE
CF_BITMAP	CF_BITMAP
	CF_DIB
	CF_DIBV5
CF_METAFILEPICT	CF_METAFILEPICT
	CF_ENHMETAFILE
CF_OEMTEXT	CF_TEXT
	CF_OEMTEXT
	CF_UNICODETEXT
	CF_LOCALE
CF_DIB	CF_BITMAP

クリップボード形式	説明
	CF_DIB
	CF_DIBV5
CF_UNICODETEXT	CF_TEXT
	CF_OEMTEXT
	CF_UNICODETEXT
	CF_LOCALE
CF_ENHMETAFILE	CF_METAFILEPICT
	CF_ENHMETAFILE
CF_DIBV5	CF_BITMAP
	CF_DIB
	CF_DIBV5

注:

クリップボード形式の変換はWindows OSに依存しており、この表は将来のOSバージョンで変更される可能性があります。

Windowsのクリップボードシステムがすべての形式間で自由に変換するわけではないことを理解することが重要です。自動変換は、主に異なるテキストエンコーディング間やビットマップのバリエーション間など、いくつかの主要なタイプに限定されています。

その他のほとんどの形式では、ソースアプリケーションが複数の形式を一度にクリップボードに配置することで互換性が実現されます。たとえば、Excelからグラフをコピーすると、データがOffice描画図形 (CFX_OfficeDrawingShape)、拡張メタファイル (CF_ENHMETAFILE)、および単純なビットマップ (CF_DIB) として配置される場合があります。これはクリップボードによる変換ではなく、異なる貼り付けシナリオのためにソースアプリケーションが複数の表現を提供しているものです。

クリップボード形式の制御と変換可能な形式
クリップボード形式制御ポリシーとセッション間クリップボード構成を設計する際には、変換可能な形式を考慮に入れる必要があります。たとえば、クライアントからクリップボードへのテキストベースのコンテンツのみを明示的に許可したい場合、「セッションクリップボード書き込み許可形式」ポリシーにすべてのテキストベースの形式を追加する必要があります。この例では、次の形式をポリシーに追加する必要があります。

CF_TEXT

CF_UNICODETEXT

CF_DSPTEXT

CF_LOCALE

CF_OEMTEXT

同様に、あるセッションから別のセッションにそのような種類のデータをコピーする際に、すべてのファイル形式をセッション間で転送したい場合は、すべてのファイルクリップボード形式をCrossSessionFormats構成に追加する必要があります。

CFX_FILES

CFX_HFDROP

クリップボード転送サイズ制限

クリップボード転送サイズ制限を使用すると、1回のコピー＆ペーストのクリップボード操作で転送できるデータのサイズに制限を設定できます。デフォルトでは、これらの設定は無効になっており、クライアントからセッションへ、およびセッションからクライアントへのクリップボード転送に制限はありません。

転送サイズ制限は、帯域幅管理に役立ちます。大規模なクリップボード転送は、特に多数の同時ユーザーがいる環境では、かなりのネットワーク帯域幅を消費する可能性があります。制限を設定することで、管理者はすべてのユーザーに対してよりスムーズなパフォーマンスを確保し、ネットワークの輻輳を防ぐことができます。

無制限のクリップボード転送は、セキュリティリスクをもたらす可能性があります。悪意のあるソフトウェアや不正なユーザーが、セッション内外で大量の機密データをコピーする可能性があります。転送サイズを制限することは、このようなデータ漏洩に対する予防策となります。

クリップボード転送サイズ制限を構成する際、管理者は以下を考慮する必要があります。

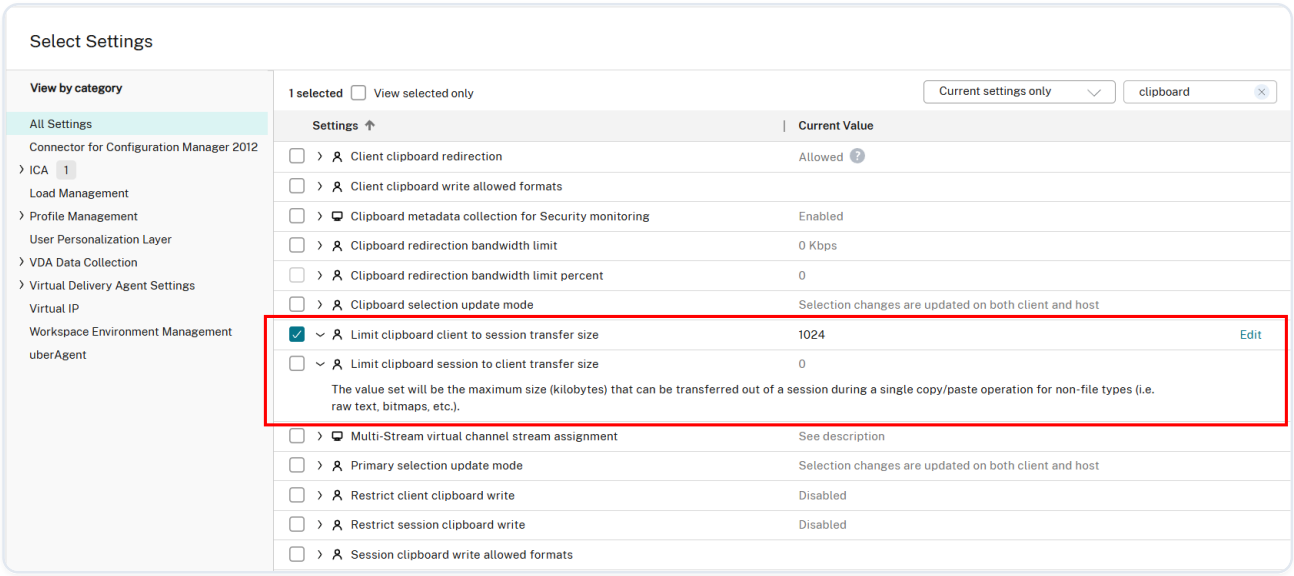
- ユーザーのニーズ: ユーザーの一般的なコピー＆ペースト要件は何ですか？過度に制限的な制限を課すと、生産性が妨げられる可能性があります。
- 帯域幅の使用状況: 利用可能なネットワーク帯域幅はどのくらいで、予想される同時ユーザー数は何人ですか？
- 関連するセキュリティポリシー: 組織のデータセキュリティおよびコンプライアンス要件は何ですか？

クリップボードデータ転送をきめ細かく制御するための2つの主要な設定があります。

クリップボードのクライアントからセッションへの転送サイズを制限: この設定は、ユーザーのローカルデバイス（クライアント）からコピーされ、リモートセッション（仮想デスクトップやシームレスアプリケーションなど）に貼り付けられるデータの最大サイズをキロバイト単位で構成します。

クリップボードのセッションからクライアントへの転送サイズを制限: 次に、この設定は、リモートセッション内からコピーされ、ユーザーのローカルデバイスに貼り付けられるデータの最大サイズをキロバイト単位で制御します。これは、ユーザーが仮想化環境内で機密データを扱っており、クライアントへの大量のデータ流出を防ぐ必要がある場合に特に重要です。

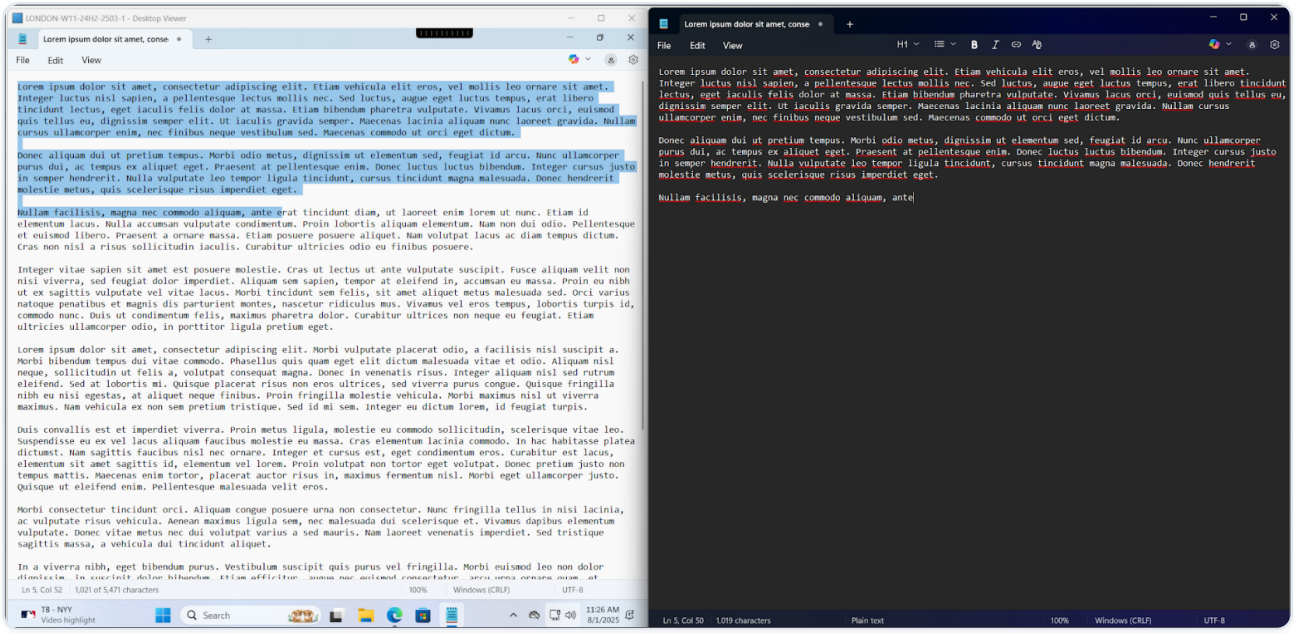
この例では、クライアントからセッションへのクリップボード制限は1024キロバイトに制限されています。



> **注:**
>
> サイズ制限は、固定の文字数ではなく、データサイズ（キロバイト、KB）に基づいています。可変文字エンコーディング（Unicodeなど）のため、コピーできる文字数は異なりま

> す。たとえば、10 KBの制限では、標準のANSIテキストよりもUnicodeテキストの方が保持できる文字数が少なくなります。

> 次の例では、「クリップボードのセッションからクライアントへの転送サイズを制限」ポリシーが1 KBに設定されています。



このクリップボード転送サイズ制限が適用されている場合、選択されたテキストは、左側のCitrix®セッションから右側のローカルのメモ帳に転送できる最大文字数です。ユーザーがこのCitrixセッションからクライアントにこれ以上の文字をコピーしようとすると、テキストは切り捨てられず、代わりに貼り付け操作全体が失敗します。画像やファイルなどの他のデータ型をコピーしようとした場合も、コンテンツが設定された最大転送サイズよりも大きい場合は失敗します。

このポリシーを設定する際は、ユーザーが扱うテキストデータの種類を考慮してください。多言語コンテンツやリッチテキストを頻繁に扱う場合は、Unicodeテキストのデータサイズが大きくなるため、より高いキロバイト制限を設定する必要があるかもしれません。

クリップボード転送サイズ制限は、**許可されているすべてのクリップボード形式**に適用されます。

クリップボードのサイズ制限は、許可されているすべてのクリップボード形式で普遍的に適用されます。これは、データ型（テキスト、画像、ファイルなど）に関係なく、転送できるデータの最大量を制限が決定することを意味します。

セッション間クリップボード交換 (プレビュー)

セッション間クリップボード交換は、クリップボードの新しいデータ損失防止および軽減制御です。 これにより、Citrix®セッション間でクリップボードデータを、データをローカルエンドポイントのクリップボードに配置することなく共有できます。

セッション間クリップボード交換は、現在のクリップボードポリシーと連携して機能し、VDAとクライアント間でクリップボードデータを共有するためのより安全な方法を提供します。

この機能は現在プレビュー中です。

ユーザーがVDAのクリップボードにデータを配置すると、「クライアントクリップボードリダイレクトポリシー」クリップボードポリシーが有効になっている場合、クリップボードデータは自動的にエンドポイントと共有されます。これにより、ユーザーはリモートセッションからクライアントにデータをコピー＆ペーストできます。

ユーザーは複数のソースから複数のリモートセッションやアプリケーションにアクセスでき、クリップボードを介してこれらのセッション間でデータを共有できます。この場合、クリップボードデータはデフォルトでローカルエンドポイントのクリップボードでも利用可能になります。

機密データを扱う環境では、お客様はリモートセッションからクライアントクリップボードへのクリップボードデータの共有を禁止することを選択できます。ただし、これによりCitrixセッション間のクリップボード機能も制限されます。

セッション間クリップボード交換は、異なるサーバーやセッションで公開されている可能性のあるCitrixセッション間（シームレスセッションとデスクトップセッションの両方）でのクリップボード転送を可能にし、クリップボードデータがローカルエンドポイントのクリップボードを通過するのを防ぐことで、データ流出のリスクや偶発的なデータ損失を防ぎながら、ユーザーエクスペリエンスを向上させます。

要件

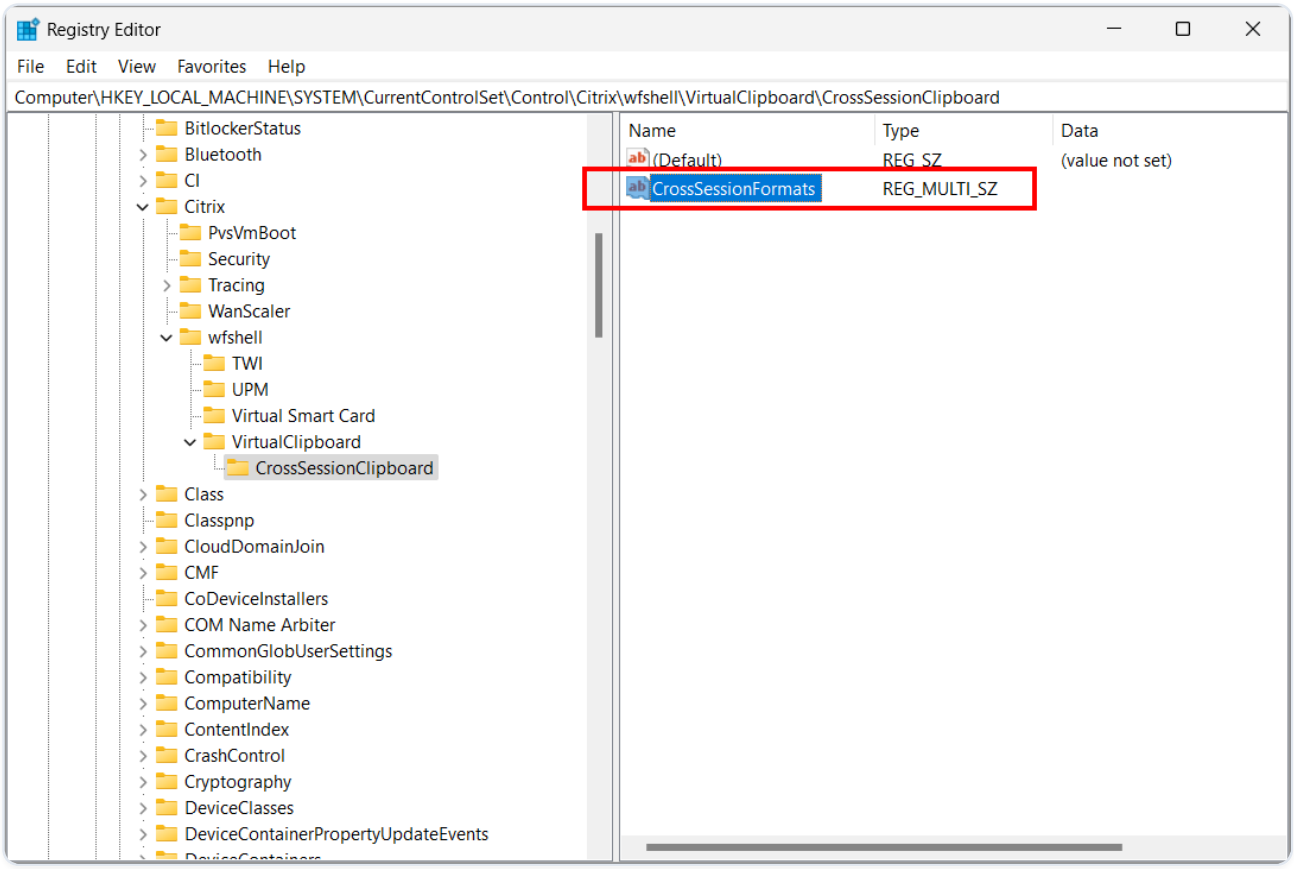
セッション間クリップボード交換プレビューの前提条件は次のとおりです。

- WindowsエンドポイントがCWA for Windows 2507 LTSR以降を実行していること。
- Windows VDAがVDA 2507 LTSR以降を実行していること。

構成

「クロスセッションクリップボードプレビュー」は、VDAで以下のレジストリエントリを作成することで有効にできます。

1. regedit.exe を使用して Windows レジストリエディターを開きます。
2. `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\wfshell\Virtual Clipboard\CrossSessionClipboard\` に移動します。
3. `CrossSessionFormats` という名前のREG_MULTI_SZ値を作成します。



CrossSessionFormatsは、クロスセッションクリップボードを介してトンネルされるクリップボード形式のリストで構成できます。各エントリは別々の行に入力する必要があります。

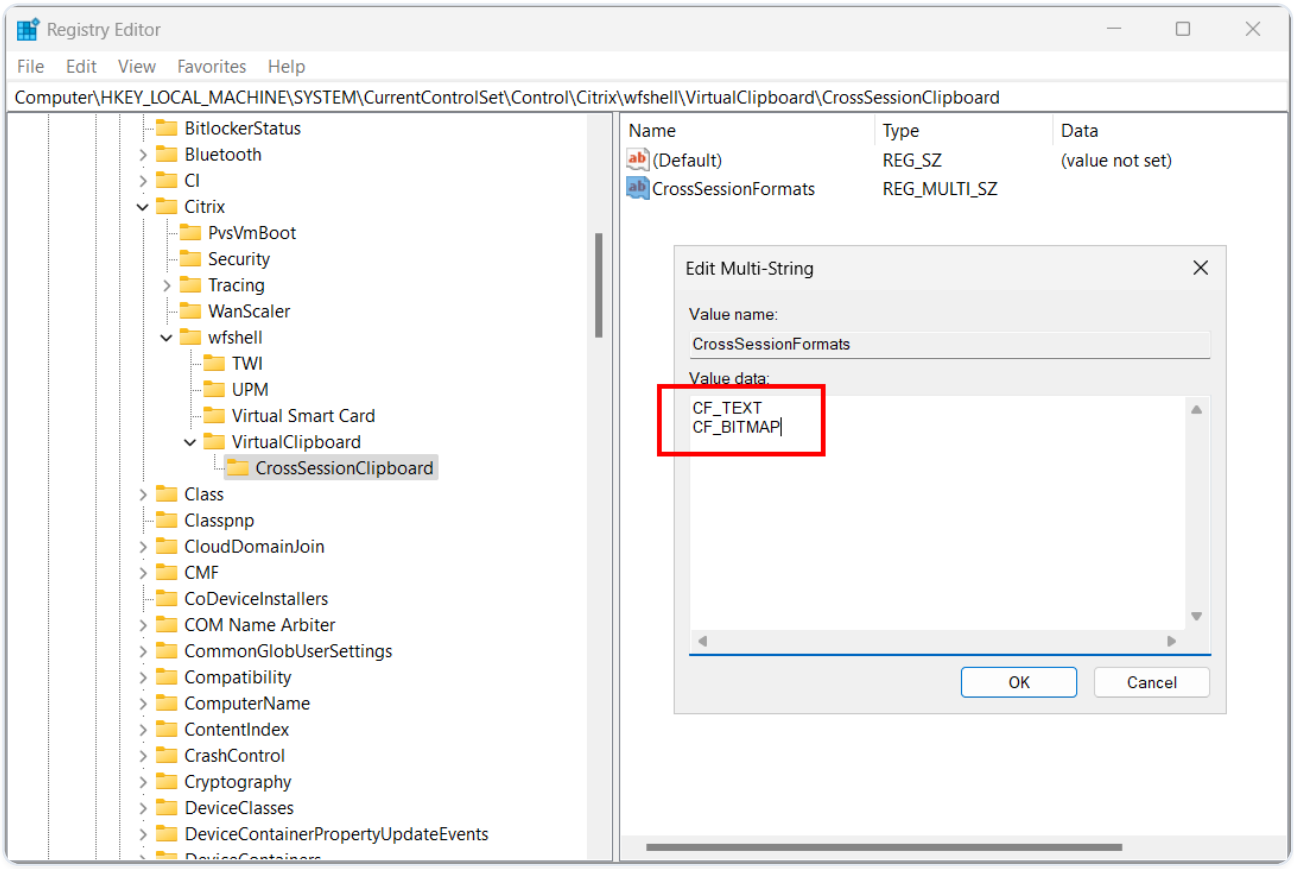
例として：

CF_TEXT

CF_BITMAP

は正しいですが、以下は正しくありません。 CF_TEXT,CF_BITMAP

次の例では、CF_TEXTおよびCF_BITMAPクリップボード項目は、これらのデータ形式をあるセッションから別のセッションにコピーする際に、クロスセッションを介してトンネルされて送信されます。



クロスセッションクリップボードが機能するためには、ユーザーがクリップボードデータを共有したいすべてのVDAで、目的のクリップボードデータ形式がクロスセッションに設定されている必要があります。

設定されたクロスセッションクリップボード形式は、クロスセッションをサポートしていないクライアント（CWA for Windows 2507以前のCWAクライアント）からはブロックされます。

送信側と受信側の両方のCitrix®セッションで、クロスセッション用に一致するクリップボードデータ形式が設定されている必要があります。

セッション間でコピーされるクリップボードコンテンツは、セッション間でコピーする必要があるクリップボードデータが一致する場合にのみ許可されます。受信側のVDAでクリップボード形式がクロスセッション用に設定されていない場合、クリップボード転送は拒否され、ユーザーは受信側のCitrixセッションにデータを貼り付けることができません。

注:

両方のVDAで、設定されているすべてのクロスセッションクリップボード形式が一致している必要はありませんが、両方のCrossSessionFormats設定に存在する形式のみがセッション間で共有されます。

例えば、i

注:

- クロスセッション構成は、セッション間のみを対象としています。設定されている場合、設定された構成に基づいてセッションからクライアントへの動作が変更される可能性があります。クロスセッションクリップボードは、クライアントからセッションへのクリップボードを変更しません。クライアントからセッションへの構成は、クライアントからセッションに関連するクリップボードポリシーのみを介して行われます。
- ユーザーがクロスセッションクリップボード用に構成されたCitrixセッションに接続しているにもかかわらず、そのクライアントがクロスセッションをサポートしていない場合（例：Citrix Workspaceアプリのバージョン2507より前を使用している場合、またはCWA Linuxのようなサポートされていないクライアントから接続している場合）、クロスセッション構成にリストされている形式のクリップボード転送は、Citrixセッションからクライアントへの転送が拒否されます。

ポリシーとレジストリの優先順位

クロスセッションクリップボード交換レジストリ設定は、クリップボードポリシーと連携して機能します。

「client clipboard redirection」ポリシーを「prohibit」に設定することで、ポリシーによってクリップボードリダイレクトが明示的に禁止されている場合、クロスセッションクリップボードレジストリ設定は無視され、レジストリがどのように構成されていても、Citrix®セッション間のクリップボード転送も禁止されます。

「xxx」ポリシー設定によってクリップボードデータ形式が明示的に禁止されているが、そのクリップボードデータ形式がクロスセッションで有効になっている場合、そのクリップボード形式は禁止されます。クロスセッションレジストリの設定は無視されます。

セッション間のクロスセッションクリップボード交換を通じて共有されるクリップボードデータに対しても、クリップボードサイズの制限が適用されます。
例
例1
すべてデフォルト

ただし：

- CF_TEXT、CF_UNICODETEXT、CF_DSPTEXT、CF_OEMTEXT、CF_LOCALE の両方のVDAでクロスセッションが構成されている

クロスセッションクリップボード交換レジストリ設定で構成されたデータ形式は、クロスセッションを介してトンネリングされ、クライアントでは利用できません。この場合、テキスト形式はソースVDAから受信VDAへ共有が許可されます。ポリシーで許可されている他のすべての形式は、引き続きクライアントおよびリモートセッションで許可されます。リモートセッションからコピーされた場合、クライアントクリップボードではテキスト形式のみが禁止されます。

クライアントからセッションへのクリップボードデータ転送は制限されません。
例2
すべてデフォルト

ただし：

- セッションクリップボード書き込みの制限: 両方のVDAで有効に設定済み
- CF_TEXT の両方のVDAでクロスセッションが構成されている

「セッションクリップボード書き込みの制限」が両方のVDAで有効になっているため、クリップボードデータはセッション間で共有されません。この設定はクロスセッション構成よりも優先されます。

クライアントからセッションへのクリップボードデータの転送も、その同じポリシーによって禁止されます。

CF_TEXTがクロスセッション用に構成されているため、クロスセッション構成によりブロックされるため、CF_TEXTはVDAからクライアントへコピーできないことも意味します。

その他のすべてのクリップボード形式は、セッションからクライアントへ利用可能です。
例3
すべてデフォルト

例外:

- セッションクリップボード書き込み許可形式は、両方のVDAでCF_TEXTに制限されています
- クロスセッションは、両方のVDAですべてのクリップボードデータ形式に対して構成されています

セッションクリップボード書き込み許可形式は、クロスセッションクリップボード構成よりも優先され、CF_TEXTデータのみがクリップボードを介して受信VDAへコピーを許可されます。

クロスセッションにリストされているすべてのクリップボード形式は、クライアントクリップボードへのコピーが防止されます。
例 4
すべてデフォルト

例外:

- セッションクリップボード書き込み許可形式は、CF_TEXTを除くすべてに設定されています
- クロスセッションは、両方のVDAでCF_TEXTに対して構成されています

セッションクリップボード書き込み許可形式は、クロスセッションクリップボード構成よりも優先され、CF_TEXTデータはVDA間でクリップボードを介して共有が許可されません。

クリップボードのシナリオとユースケースの例

クリップボードリダイレクトポリシーを適切に構成することは、ユーザーの生産性と企業セキュリティのバランスを取る上で重要です。最適な構成は、特定のユースケースによって異なります。

以下に一般的なユースケースの例をいくつか示します。

標準的なナレッジワーカー

ナレッジワーカーや一般的なオフィスユーザーのようなほとんどのユーザーにとって、目標はローカルアプリケーションとリモートアプリケーション間でテキストや簡単な画像をシームレスにコピー＆ペーストすることです。このシナリオでは、デフォルトのポリシー構成で十分な場合が多いです。

構成:

- クライアントクリップボードリダイレクト: **許可** (デフォルト)

機密データのユースケース

ユーザーがセキュアなセッションに情報（例: 患者データをEHRに）を貼り付ける必要があるが、機密データをローカルデバイスにコピーすることを防ぐ必要がある医療機関や金融機関を考えてみましょう。これは、クリップボードを介した偶発的なデータ漏洩を防ぐのに役立ちます。

構成:

- クライアントクリップボードリダイレクト: **許可**
- クライアントクリップボード書き込みの制限: **有効** (セッションからクライアントへのコピーをブロック)

- セキュリティを強化するには、「セッションクリップボード書き込みの制限」を有効にし、「セッションクリップボード書き込み許可形式」を使用してプレーンテキスト (CF_TEXT) のみを許可します。

あるいは、お客様は新しいクロスセッションクリップボード機能 (プレビュー) を使用して、セッション間のクリップボードを許可しつつ、セッションからクライアントへのリダイレクトを防ぐことができます。
開発者とIT管理者
これらのユーザーは、スクリプト、ログファイル、インストーラーなどのファイルを、ローカルマシンとVDA間でコピーする機能を必要とすることがよくあります。これには、より寛容な構成が必要です。

構成:

- クライアントクリップボードリダイレクト: **許可**
- セッションからクライアントへのファイルコピーを有効にするには、 が **無効** になっていることを確認するか、有効になっている場合は、CFX_FILE形式をリストに追加します。
- クライアントからセッションへのファイルコピーを有効にするには、 が **無効** になっていることを確認するか、有効になっている場合は、CFX_FILEをリストに追加します。

これらのポリシーは、個々のユーザーをポリシーに追加するのではなく、開発者またはIT管理者が含まれる関連グループを対象とするように構成します。

グラフィックポリシー設定

グラフィックセクションには、ユーザーセッションで画像がどのように処理されるかを制御するためのポリシー設定が含まれています。

視覚的にロスレスな圧縮を許可する

この設定により、グラフィックに対して、真のロスレス圧縮の代わりに視覚的にロスレスな圧縮を使用できます。視覚的にロスレスな圧縮は、真のロスレス圧縮よりもパフォーマンスが向上しますが、目視では気づかない程度のわずかな損失があります。この設定は、視覚品質設定の値の使用方法を変更します。

デフォルトでは、この設定は無効になっています。

グラフィックステータスインジケーター

この設定は、グラフィックステータスインジケーターがユーザーセッションで実行されるように構成します。このツールを使用すると、ユーザーはアクティブなグラフィックモードに関する情報を確認できます。

この情報には、ビデオコーデック、ハードウェアエンコード、画質、およびセッションで使用されているモニターに関する詳細が含まれます。グラフィックステータスインジケーターを使用すると、ユーザーはピクセルパーフェクトモードを有効または無効にすることもできます。

Citrix Virtual Apps and Desktops™ 2103以降のリリースには、画質とインタラクティブ性の適切なバランスをユーザーが見つけるのに役立つ画質スライダーが含まれています。

Citrix Virtual Apps and Desktops™ 2109以降のリリースには、グラフィックステータスインジケーターを使用して起動されるユーザーインターフェイスを介して仮想ディスプレイレイアウトを構成する機能が含まれています。

グラフィックステータスインジケーターは、以前のバージョンのロスレスインジケーターツールを置き換えます。このポリシーは、Citrix Virtual Apps and Desktopsバージョン7.16から1809までででロスレスインジケーターを有効にします。

> **注:**
>
> **グラフィックステータスインジケーター**は、デスクトップセッションでのみ利用可能であり、シームレスアプリケーションセッションでは利用できません。

画面共有

この設定により、ユーザーは画面コンテンツ、キーボード、マウスを含むセッションを他のユーザーと共有できます。

デフォルトでは、この設定は無効になっています。

VDAは、TCPポート範囲のポートを使用してデータを交換しようとします。これは、最も低いポートから始まり、その後の接続ごとに増分されます。このポートは、インバウンドトラフィックとアウトバウンドトラフィックの両方を処理します。

既定では、TCPポート範囲は52525〜52625に設定されています。

画面共有に使用されるポートは、ファイアウォールの例外リストに追加する必要があります。このオプションは、VDAのインストール時にチェックボックスとして表示されます。既定では、このオプションはチェックされていません。

ディスプレイメモリ制限

この設定は、セッションの最大ビデオバッファサイズをキロバイト単位で指定します。

VDAバージョン2308以前の場合、128から4,194,303までのキロバイト単位の量を指定します。指定しない場合、設定は既定で65,536キロバイトになります。

VDAバージョン2311以降の場合、任意のキロバイト単位の量を指定します。指定しない場合、または0として指定した場合、設定は既定で最大値なしになります。

> **注:**
>
> VDAバージョン2311以降の場合、Citrix®は、この設定を既定のままにすることをお勧めします。

> 接続に高解像度と複数のモニターを使用すると、より多くのメモリが必要になります。HDX™は各セッションに必要なディスプレイメモリの量のみを割り当てるため、常に環境内の構成の上位層に基づいて必要なビデオメモリの量を計算してください。したがって、一部のユーザーのみが既定値よりも多くを必要とする場合でも、ディスプレイメモリ制限を増やすことによるスケーラビリティへの悪影響はありません。

必要なビデオメモリの量は、次の式を使用して計算されます。

合計ビデオメモリ = ((32 / 8) x Σ)

例1

次の例では、2つのモニターを持つセッションを使用します。1つは1920x1080の解像度、もう1つは1280x720の解像度です。

1. 解像度の積の合計を計算します。
   - (1080 x 1920) + (720 x 1280)
   - = 2073600 + 921600
   - = 2995200
2. 合計ビデオメモリを計算:
   - ((32 / 8) x 2995200)
   - = (4 x 2995200)
   - = 11,980,800バイトまたは11,700キロバイト

この例では、これら2つのモニター構成を持つセッションをサポートするために、11,700キロバイトのビデオメモリが必要になります。

例2

4台の4Kモニターを使用する場合、上記の式を用いると、これらのセッションには最低129,600キロバイトのビデオメモリが必要になります。

どちらの例でも、VDAバージョン2311以降を使用している場合、Citrixはディスプレイメモリ制限をデフォルトのままにすることを推奨します。

表示モードの劣化優先順位

> **注:**
>
> Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

> セッションの表示メモリ制限に達した場合、この設定は、色深度と解像度のどちらが先に劣化するかを指定します。

デフォルトでは、色深度が先に劣化します。

セッションメモリ制限に達すると、表示される画像の品質を低下させることができます。この品質は、色深度と解像度のどちらを先に劣化させるかを選択することで低下させることができます。色深度が先に劣化する場合、表示される画像はより少ない色を使用します。解像度が先に劣化する場合、表示される画像は1インチあたりのピクセル数が少なくなります。

色深度または解像度が劣化した場合にユーザーに通知するには、「表示モードが劣化した場合にユーザーに通知」設定を構成します。

動的ウィンドウプレビュー

この設定は、シームレスウィンドウの表示を有効または無効にします。

- フリップ-
- フリップ 3D
- タスクバープレビュー
- Windows ピーク

WINDOWS AERO プレビューオプション	説明
タスクバープレビュー	ユーザーがウィンドウのタスクバーアイコンにマウスカーソルを合わせると、そのウィンドウの画像がタスクバーの上に表示されます。
Windows ピーク	ユーザーがタスクバーのプレビュー画像にマウスカーソルを合わせると、ウィンドウのフルサイズの画像が画面に表示されます。
フリップ	ユーザーが ALT+TAB を押すと、開いている各ウィンドウの小さなプレビューアイコンが表示されます。
フリップ 3D	ユーザーが TAB+Windows ロゴキーを押すと、開いているウィンドウの大きな画像が画面にカスケード表示されます。

デフォルトでは、この設定は有効になっています。

イメージキャッシュ

> **注:**
>
> Virtual Delivery Agent 7.x の場合、このポリシー設定は、レガシーグラフィックモードのポリシー設定が有効になっている場合にのみ適用されます。

この設定は、セッション内の画像のセクションのキャッシュと取得を有効または無効にします。画像をセクションにキャッシュし、必要に応じてこれらのセクションを取得すると、次のことが可能になります。

- ユーザーデバイスでのスクロールがよりスムーズになる
- ユーザーデバイスでのネットワーク経由で送信されるデータ量を削減する
- ユーザーデバイスで必要な処理を削減する

デフォルトでは、画像キャッシュ設定は有効になっています。

> **注:**

> 画像キャッシュ設定は、画像がどのようにキャッシュされ、取得されるかを制御します。この設定は、画像がキャッシュされるかどうかを制御するものではありません。画像は、レガシーグラフィックモード設定が有効になっている場合にキャッシュされます。

レガシーグラフィックモード - サポートされていません。下位互換性のためのみ

> **重要:**
>
> このリリースでは、レガシーグラフィックモードとデスクトップコンポジションリダイレクト (DCR) はサポートしていません。このポリシーは、XenApp 7.15 LTSR、XenDesktop 7.15 LTSR、およびWindows 7とWindows 2008 R2を使用する以前のVDAリリースとの下位互換性のためのみに含まれています。

> この設定は、リッチグラフィックエクスペリエンスを無効にします。この設定を使用して、レガシーグラフィックエクスペリエンスに戻し、WANまたはモバイル接続での帯域幅消費を削減します。XenAppおよびXenDesktop 7.13で導入された帯域幅削減により、このモードは廃止されました。

デフォルトでは、この設定は無効になっており、ユーザーにはリッチグラフィックエクスペリエンスが提供されます。

レガシーグラフィックモードは以下でサポートされています。

- ウィンドウズ 7
- ウィンドウズ サーバー 2008 R2 VDA。

レガシーグラフィックモードは以下ではサポートされていません。

- Windows 8.xおよび10
- Windows Server 2012、2012 R2、および2016。

XenAppおよびXenDesktop 7.6 FP3以降でのグラフィックモードとポリシーの最適化について詳しくは、CTX202687を参照してください。

最大許容色深度

> **注:**

> Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

> この設定は、セッションで許可される最大色深度を指定します。

デフォルトでは、最大許容色深度は32ビット/ピクセルです。

この設定は、Thinwireドライバーと接続にのみ適用されます。プライマリディスプレイドライバーとしてThinWire以外のドライバーを使用するVDAには適用されません。これらのVDAは、Windows Display Driver Model（WDDM）ドライバーをプライマリディスプレイドライバーとして使用するVDAです。Windows 8などのWDDMドライバーをプライマリディスプレイドライバーとして使用するシングルセッションOS VDAの場合、この設定は無効です。Windows Server 2019などのWDDMドライバーを使用するWindowsマルチセッションOS VDAの場合、この設定によりユーザーがVDAに接続できなくなる可能性があります。

高い色深度を設定すると、より多くのメモリが必要になります。メモリ制限に達したときに色深度を低下させるには、**表示モードの低下設定**を構成します。色深度が低下すると、表示される画像はより少ない色を使用します。

表示モードが低下したときにユーザーに通知する

> **注:**

> Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

> この設定は、色深度または解像度が低下したときに、ユーザーに簡単な説明を表示します。

デフォルトでは、ユーザーへの通知は無効になっています。

3Dグラフィックワークロード向けに最適化

この設定は、グラフィックを多用するワークロードに最適なデフォルト設定を構成します。グラフィックを多用するアプリケーションに重点を置くユーザーに対して、この設定を有効にします。このポリシーは、セッションでGPUが利用可能な場合にのみ適用してください。このポリシーによって設定されたデフォルト設定を明示的に上書きするその他の設定が優先されます。

デフォルトでは、3Dグラフィックワークロード向けに最適化は無効になっています。

キューイングとトッシング

> **注:**
>
> Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

> この設定は、別の画像に置き換えられたキュー内の画像を破棄します。

デフォルトでは、キューイングとトッシングは有効になっています。

この設定は、グラフィックがユーザーデバイスに送信される際の応答を改善します。この設定を構成すると、フレームがドロップされるため、アニメーションが途切れることがあります。

圧縮にビデオコーデックを使用する

エンドポイントでビデオデコードが利用可能な場合、グラフィックの圧縮にビデオコーデックの使用を許可します。「**画面全体**」が選択されている場合、ビデオコーデックはすべてのデフォルトコーデックとして適用されます。「**アクティブに変化する領域**」が選択されている場合、ビデオコーデックは画面上で常に変化する領域に使用され、その他のデータは静止画圧縮とビットマップキャッシュを使用します。エンドポイントでビデオデコードが利用できない場合、または「**ビデオコーデックを使用しない**」を指定した場合、静止画圧縮とビットマップキャッシュの組み合わせが使用されます。「**推奨時に使用**」が選択されている場合、システムはさまざまな要因に基づいて選択します。選択方法が強化されるにつれて、バージョン間で結果が異なる場合があります。

現在のシナリオに適切な設定をシステムが最善を尽くして選択できるようにするには、「**推奨時に使用**」を選択します。

特にサーバーレンダリングされたビデオや3Dグラフィックを多用する場合に、ユーザーエクスペリエンスと帯域幅の向上を最適化するには、「**画面全体**」を選択します。

特に低帯域幅でビデオパフォーマンスを向上させ、静的およびゆっくりと変化するコンテンツのスケーラビリティを維持するために最適化するには、「**アクティブに変化する領域**」を選択します。この設定はマルチモニター展開でサポートされています。

サーバーのCPU負荷を最適化し、多数のサーバーレンダリングされたビデオやその他のグラフィックを多用するアプリケーションがない場合に最適化するには、「**ビデオコーデックを使用しない**」を選択します。

デフォルトは「**推奨時に使用**」です。

ビデオにハードウェアエンコーディングを使用する

この設定により、利用可能な場合、グラフィックハードウェアを使用してビデオコーデックで画面要素を圧縮できます。そのようなハードウェアが利用できない場合、VDAはソフトウェアビデオコーデックを使用したCPUベースのエンコーディングにフォールバックします。

このポリシー設定のデフォルトオプションは「**有効**」です。

複数のモニターがサポートされています。

ビデオデコードをサポートするCitrix Workspace™アプリは、ハードウェアエンコードで使用できます。

NVIDIA

NVIDIA GRID GPUの場合、ハードウェアエンコードはマルチセッションOSおよびシングルセッションOS用のVDAでサポートされています。

NVIDIA GPUはNVENCハードウェアエンコードをサポートしている必要があります。サポートされているGPUのリストについては、NVIDIA video codec SDKを参照してください。

NVIDIA GRIDにはドライバーバージョン3.1以降が必要です。NVIDIA Quadroにはドライバーバージョン362.56以降が必要です。CitrixはNVIDIA Release R361ブランチのドライバーを推奨しています。

ロスレステキストはNVENCハードウェアエンコードと互換性がありません。ロスレステキストを有効にした場合、ロスレステキストがNVENCハードウェアエンコードよりも優先されます。

アクティブに変化する領域に対するH.264ハードウェアコーデックの選択的な使用がサポートされています。

視覚的にロスレス（YUV 4:4:4）圧縮がサポートされています。視覚的にロスレス（グラフィックポリシー設定、視覚的にロスレス圧縮を許可）には、Citrix Workspaceアプリ1808以降またはCitrix Receiver for Windows 4.5以降が必要です。

インテル

Intel Iris Proグラフィックプロセッサの場合、ハードウェアエンコードはシングルセッションOSおよびマルチセッションOS用のVDAでサポートされています。

Intel Broadwellプロセッサファミリー以降のIntel Iris Proグラフィックプロセッサがサポートされています。Intel Remote Displays SDKバージョン1.0が必要であり、IntelのWebサイトからダウンロードできます: Remote Displays SDK。

ロスレステキストは、ビデオコーデックポリシーが画面全体に設定され、**3Dグラフィックワークロード向けに最適化**ポリシーが無効になっている場合にのみサポートされます。

視覚的にロスレス（YUV 4:4:4）はサポートされていません。

Intelエンコーダーは、最大8つのエンコードセッション（たとえば、1人のユーザーが8台のモニターを使用する場合、または8人のユーザーがそれぞれ1台のモニターを使用する場合）で良好なユーザーエクスペリエンスを提供します。8つ以上のエンコードセッションが必要な場合は、仮想マシンが接続するモニターの数を確認してください。管理者は、良好なユーザーエクスペリエンスを維持するために、このポリシー設定をユーザーごとまたはマシンごとに構成するかどうかを決定します。

AMD

AMDの場合、シングルセッションOS用VDAでハードウェアエンコードがサポートされています。

AMD GPUはRapidFire SDKをサポートする必要があります。例えば、AMD Radeon ProまたはFirePro GPUなどです。

エンコードを機能させるには、最新のAMDドライバーをインストールしてください。これらのドライバーは`<https://www.amd.com/en/support>`からダウンロードできます。

ロスレステキストはAMDハードウェアエンコードと互換性がありません。ロスレステキストを有効にした場合、ロスレステキストがAMDハードウェアエンコードよりも優先されます。

活発に変化する領域向けのH.264ハードウェアコーデックの選択的な使用がサポートされています。

キャッシュポリシー設定

このセクションには、クライアント接続の帯域幅が制限されている場合に、ユーザーデバイスで画像データをキャッシュすることを可能にするポリシー設定が含まれています。

永続キャッシュしきい値

注: Virtual Delivery Agent 7.xの場合、このポリシー設定は、**レガシーグラフィックモード**ポリシー設定が有効になっている場合にのみ適用されます。

この設定は、ユーザーデバイスのハードドライブにビットマップをキャッシュし、それにより、以前のセッションからの大きく頻繁に使用される画像の再利用を可能にします。

デフォルトでは、しきい値は1秒あたり3000000ビットです。

しきい値は、永続キャッシュ機能が有効になる下限を表します。たとえば、デフォルト値を使用すると、帯域幅が3000000 bpsを下回った場合、ビットマップはユーザーデバイスのハードドライブにキャッシュされます。

キープアライブ ポリシー設定

Keep Alive セクションには、ICA® キープアライブメッセージを管理するためのポリシー設定が含まれています。

ICA キープアライブ タイムアウト

この設定は、連続するICAキープアライブメッセージ間の秒数を指定します。

デフォルトでは、キープアライブメッセージ間の間隔は60秒です。

ICAキープアライブメッセージを送信する1～3600秒の間隔を指定します。ネットワーク監視ソフトウェアが非アクティブな接続を閉じる役割を担っている場合は、この設定を構成しないでください。

ICA キープアライブメッセージ

この設定は、定期的なICAキープアライブメッセージの送信を有効または無効にします。

デフォルトでは、キープアライブメッセージは送信されません。

この設定を有効にすると、切断された接続が切断されるのを防ぎます。サーバーがアクティビティを検出しない場合、この設定により、Remote Desktop Services (RDS) がセッションを切断するのを防ぎます。サーバーは数秒ごとにキープアライブメッセージを送信し、セッションがアクティブであるかどうかを検出します。セッションがアクティブでなくなった場合、サーバーはそのセッションを切断済みとしてマークします。

セッションの信頼性を使用している場合、ICAキープアライブは機能しません。セッションの信頼性を使用していない接続に対してのみ、ICAキープアライブを構成してください。

関連するポリシー設定: セッションの信頼性接続。

ローカルアプリアクセス ポリシー設定

ローカルアプリアクセスセクションには、ユーザーのローカルにインストールされたアプリケーションとホストされたアプリケーションを管理するポリシー設定が含まれています。これらのポリシー設定は、ホストされたデスクトップ環境での統合を管理します。

ローカルアプリアクセスを許可

この設定は、ユーザーのローカルにインストールされたアプリケーションとホストされたアプリケーションの統合を許可または禁止します。これらのポリシー設定は、ホストされたデスクトップ環境での統合を管理します。

ユーザーがローカルにインストールされたアプリケーションを起動すると、そのアプリケーションは実際にはローカルで実行されているにもかかわらず、仮想デスクトップ内で実行されているように見えます。

ローカルアプリアクセスを許可ポリシー設定を**有効**にすると、ブラウザコンテンツリダイレクトはサポートされず、デスクトップセッションにクライアント側の通知領域のバッテリーステータスは表示されません。

デフォルトでは、**ローカルアプリアクセスを許可**は禁止されています。

URLリダイレクトブロックリスト

この設定は、ローカルのWebブラウザにリダイレクトされて起動されるWebサイトを指定します。これらのWebサイトには、次のものが含まれる場合があります。

- msn.comやnewsgoogle.comなど、ロケール情報を必要とするWebサイト
- ユーザーデバイスでより適切にレンダリングされるリッチメディアコンテンツを含むWebサイト。

デフォルトでは、サイトは指定されていません。

URLリダイレクト許可リスト

この設定は、起動された環境でレンダリングされるWebサイトを指定します。

デフォルトでは、サイトは指定されていません。

モバイルエクスペリエンスポリシー設定

「**モバイルエクスペリエンス**」セクションには、Citrix Mobility Packを処理するためのポリシー設定が含まれています。

キーボードの自動表示

この設定は、モバイルデバイスの画面でのキーボードの自動表示を有効または無効にします。

デフォルトでは、キーボードの自動表示は無効になっています。

タッチ最適化デスクトップの起動

この設定は無効になっており、Windows 10またはWindows Server 2016マシンでは使用できません。

この設定は、Citrix Workspace™アプリの全体的なインターフェイス動作を決定します。この設定により、タブレットデバイス向けに最適化されたタッチフレンドリーなインターフェイスを許可または禁止します。

デフォルトでは、タッチフレンドリーなインターフェイスが使用されます。

Windowsインターフェイスのみを使用するには、このポリシー設定を「禁止」に設定します。

コンボボックスのリモート化

この設定は、モバイルデバイスのセッションで表示できるコンボボックスの種類を決定します。このポリシー設定を「許可」に設定すると、デバイスネイティブのコンボボックスコントロールが表示されます。この設定が許可されている場合、ユーザーはCitrix Workspace app for iOSセッション設定を変更して、Windowsコンボボックスを使用できます。

デフォルトでは、**コンボボックスのリモート化**機能は禁止されています。

マルチメディアポリシー設定

「**マルチメディア**」セクションには、ユーザーセッションにおけるストリーミングHTML5およびWindowsのオーディオとビデオを管理するためのポリシー設定が含まれています。

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

マルチメディアポリシー

デフォルトでは、Delivery Controller™で設定されたすべてのマルチメディアポリシーは、以下のレジストリに保存されます。

マシンポリシー:

HKEY_LOCAL_MACHINE\Software\Policies\Citrix\MultimediaPolicies

ユーザーポリシー:

HKEY_LOCAL_MACHINE\Software\Policies\Citrix{ユーザーセッションID}\User\MultimediaPolicies

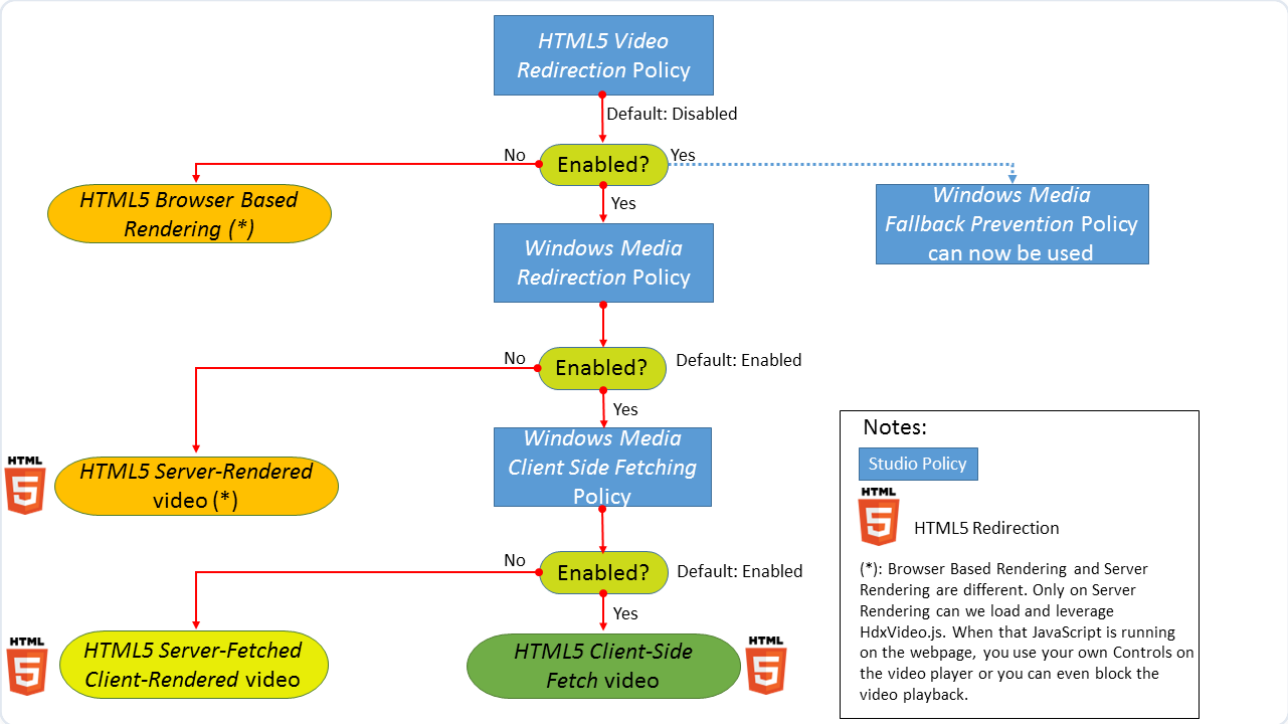
現在のユーザーセッションIDを見つけるには、Windowsコマンドラインで**qwinsta**コマンドを発行します。

HTML5ビデオリダイレクト

Citrix Virtual Apps and Desktops™サーバーがHTML5マルチメディアWebコンテンツをユーザーに配信する方法を制御し、最適化します。

デフォルトでは、この設定は無効になっています。

HTML5リダイレクトのグラフィックイメージ



このリリースでは、この機能は制御されたWebページでのみ利用可能です。HTML5マルチメディアコンテンツが利用可能なWebページ（例: 社内トレーニングサイトのビデオ）にJavaScriptを追加する必要があります。

HTML5ビデオリダイレクトを構成するには:

1. VDAインストール時の%Program Files%/Citrix/ICA Service/HTML5 Video Redirectionから、ファイル**HdxVideo.js**を社内Webページの場所にコピーします。
2. この行をWebページに挿入します（Webページに他のスクリプトがある場合は、それらのスクリプトの前に**HdxVideo.js**を含めます）。 `<script src="HdxVideo.js" type="text/javascript"\></script>`

注：HdxVideo.jsがWebページと同じ場所にない場合は、**src**属性を使用してそのフルパスを指定します。

JavaScriptが管理対象のWebページに追加されておらず、ユーザーがHTML5ビデオを再生する場合を考慮してください。この場合、Citrix Virtual Apps and Desktops™はデフォルトでサーバー側レンダリングになります。

HTML5ビデオのリダイレクトを機能させるには、***Windows Media Redirection***を許可します。このポリシーは、Server Fetch Client Renderには必須であり、Client Side Fetchingには必要です。Client Side Fetchingは、*Windows Media client-side content fetching*も許可されている必要があります。

Microsoft Edgeはこの機能をサポートしていません。

HdxVideo.jsは、ブラウザのHTML5プレーヤーコントロールを独自のコントロールに置き換えます。特定のWebサイトでHTML5ビデオリダイレクトポリシーが有効になっていることを確認するには、プレーヤーコントロールを、**HTML5ビデオリダイレクト**ポリシーが禁止されているシナリオと比較します。

（ポリシーが許可されている場合のCitrixカスタムコントロール）



（ポリシーが禁止されているか、構成されていない場合のネイティブWebページコントロール）



以下のビデオコントロールがサポートされています。

- 再生
- 一時停止
- シーク
- 繰り返し
- オーディオ
- 全画面表示

HTML5ビデオリダイレクトテストページを表示できます。

TLS、HTML5ビデオリダイレクト、およびブラウザーコンテンツリダイレクト

HTML5ビデオリダイレクトは、次の目的で使用できます。

- HTTPS Webサイトからのビデオのリダイレクト
- または
- Webサイト全体をリダイレクトするためのブラウザーコンテンツリダイレクト

これらのWebサイトに挿入されたJavaScriptは、VDAで実行されているCitrix HDX HTML5 Video Redirection Service (WebSocketService.exe) へのTLS接続を確立する必要があります。VDAの証明書ストアにあるCitrix HDX HTML5 Video Redirection Serviceは、次の目的で2つのカスタム証明書を生成します。

- ビデオのリダイレクトを実現する
- WebページのTLS整合性を維持する

HdxVideo.jsは、Secure WebSocketsを使用して、VDAで実行されているWebSocketService.exeと通信します。このプロセスはローカルシステムアカウントとして実行され、SSL終端とユーザーセッションマッピングを行います。

WebSocketService.exeは、127.0.0.1ポート9001でリッスンしています。

ビデオ品質の制限

この設定は、Windows Mediaにのみ適用され、HTML5には適用されません。**WAN経由のWindows Mediaマルチメディアリダイレクトの最適化**を有効にする必要があります。

この設定は、HDX™接続で許可される最大ビデオ品質レベルを指定します。設定すると、最大ビデオ品質は指定された値に制限され、環境内でマルチメディアのサービス品質 (QoS) が維持されます。

デフォルトでは、この設定は構成されていません。

許可される最大ビデオ品質レベルを制限するには、次のいずれかのオプションを選択します。

- 1080p/8.5Mbps
- 720p/4.0Mbps
- 480p/720Kbps
- 380p/400Kbps
- 240p/200Kbps

同じサーバーで複数のビデオを同時に再生すると、大量のリソースが消費され、サーバーのスケーラビリティに影響を与える可能性があります。

Microsoft Teamsのリダイレクト

この設定は、HDXテクノロジーに基づいてMicrosoft Teamsの最適化を有効にします。

このポリシーが有効で、サポートされているバージョンのCitrix Workspace™アプリを使用している場合、このレジストリキーはVDAで**1**に設定されます。Microsoft Teamsアプリケーションは、VDIモードでロードするためにこのキーを読み取ります。 レジストリキーを手動で設定する必要はありません。

HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream

名前: MSTeamsRedirSupport

値: DWORD (1 - オン, 0 - オフ)

> **注:**
>
> Web Studioでポリシーが利用できない古いバージョンのController（例: バージョン7.15）で、バージョン1906.2以降のVDAを使用しているとします。この場合、HDX最適化はVDAでデフォルトで有効になっています。Workspaceアプリのバージョンが1907以降の場合、Microsoft Teamsは最適化モードで起動します。7.15 LTSR ControllerとCR VDAを混在させる場合の注意点については、Knowledge Centerの記事CTX205549を参照してください。

> この場合、特定のユーザーに対して機能を無効にするには、レジストリ設定を上書きできます。ユーザーの組織単位にログオンスクリプトを適用するグループポリシーを使用して、レジストリ設定を上書きします。

> デフォルトでは、Microsoft Teamsリダイレクトは有効になっています。

マルチメディア会議

この設定により、ビデオ会議アプリケーションによる最適化されたWebカメラリダイレクトテクノロジーの使用を許可または禁止します。

デフォルトでは、ビデオ会議のサポートは許可されています。

この設定をポリシーに追加する際は、**Windows Mediaリダイレクト**設定が存在し、**許可**（デフォルト）に設定されていることを確認してください。

マルチメディア会議を使用する場合は、次の条件が満たされていることを確認してください。

- マルチメディア会議に使用するWebカメラのメーカー提供ドライバーがクライアントにインストールされていること。
- ビデオ会議セッションを開始する前に、Webカメラをユーザーデバイスに接続します。サーバーは、一度に1つのインストールされたWebカメラのみを使用します。複数のWebカメラがユーザーデバイスにインストールされている場合、サーバーは各Webカメラを順番に試行します。この試行は、ビデオ会議セッションが正常に作成されるまで続行されます。

汎用USBリダイレクトを使用してWebカメラをリダイレクトする場合、このポリシーは必要ありません。その場合は、WebカメラドライバーをVDAにインストールしてください。

WAN経由のWindows Mediaマルチメディアリダイレクトの最適化

この設定はWindows Mediaにのみ適用され、HTML5には適用されません。この設定により、以下が可能になります。

- リアルタイムマルチメディアトランスコーディング
- 劣化したネットワーク経由でのモバイルデバイスへのオーディオおよびビデオメディアストリーミングを許可
- WAN経由でWindows Mediaコンテンツが配信される方法を改善することで、ユーザーエクスペリエンスを向上させます。

デフォルトでは、WAN経由でのWindows Mediaコンテンツの配信は最適化されています。

この設定をポリシーに追加する際は、**Windows Media Redirection**設定が存在し、**Allowed**に設定されていることを確認してください。

この設定が有効になっている場合、メディアストリーミングを可能にするために、必要に応じてリアルタイムのマルチメディアトランスコーディングが自動的に展開されます。また、極端なネットワーク条件下でもシームレスなユーザーエクスペリエンスを提供します。

WAN経由でのWindows Mediaマルチメディアリダイレクトの最適化にGPUを使用する

この設定はWindows Mediaにのみ適用され、リアルタイムのマルチメディアトランスコーディングをVirtual Delivery Agent (VDA) のグラフィックス処理ユニット (GPU) で実行できるようにします。これにより、サーバーのスケーラビリティが向上します。GPUトランスコーディングは、VDAがハードウェアアクセラレーションをサポートするGPUを搭載している場合にのみ利用可能です。そうでない場合、トランスコーディングはCPUにフォールバックします。

注: GPUトランスコーディングはNVIDIA GPUでのみサポートされています。

デフォルトでは、WAN経由でのWindows Mediaコンテンツの配信を最適化するためにVDA上のGPUを使用することは禁止されています。

この設定をポリシーに追加する際は、以下の設定が存在し、Allowedに設定されていることを確認してください。

- **Windows Mediaリダイレクト**
- **WAN経由でのWindows Mediaマルチメディアリダイレクト設定の最適化**

Windows Mediaフォールバック防止

この設定は、ブラウザコンテンツリダイレクト、HTML5、およびWindows Mediaに適用されます。HTML5をサポートするには、**HTML5 video redirection**ポリシーを**Allowed**に設定します。

管理者は、**Windows Media fallback prevention**ポリシー設定を使用して、ストリーミングコンテンツをユーザーに配信するために試行される方法を指定できます。

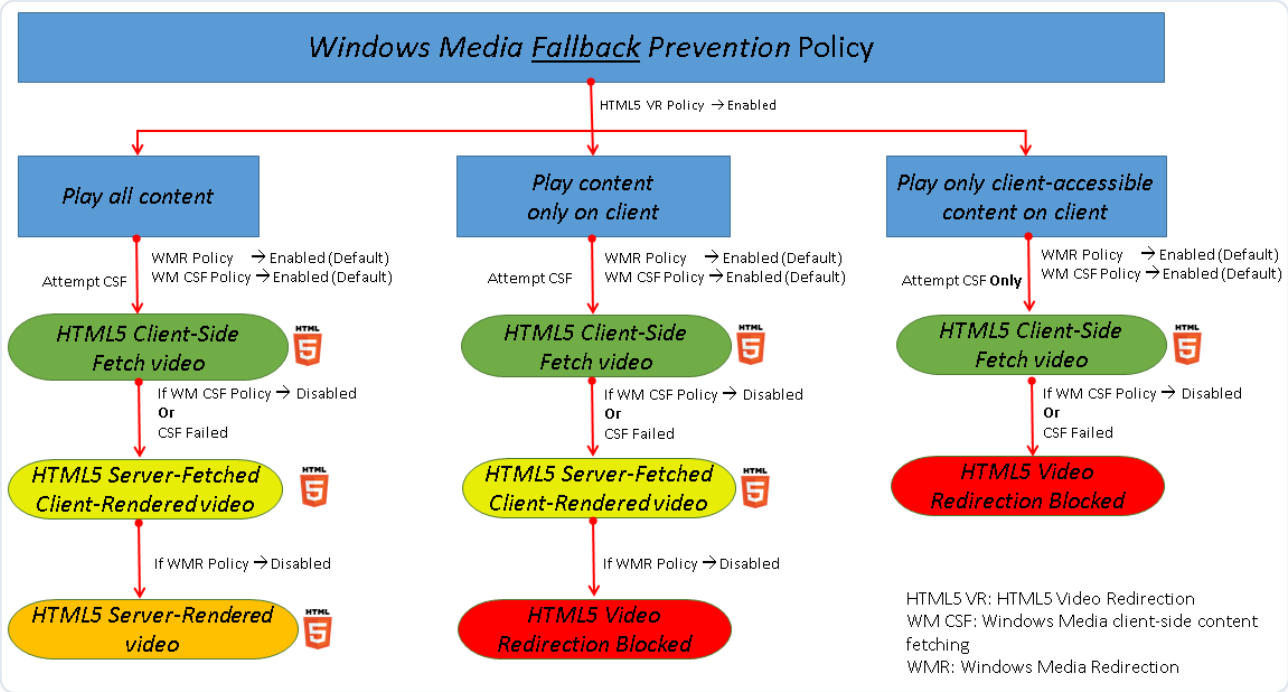
デフォルトでは、この設定は構成されていません。設定が「構成されていません」に設定されている場合、動作は**すべてのコンテンツを再生**と同じになります。

この設定を構成するには、次のいずれかのオプションを選択します。

- **すべてのコンテンツを再生する**。クライアント側でのコンテンツ取得を試行し、次にWindows Mediaリダイレクトを試行します。失敗した場合は、サーバーでコンテンツを再生します。
- **すべてのコンテンツをクライアントでのみ再生する**。クライアント側での取得を試行し、次にWindows Mediaリダイレクトを試行します。失敗した場合、コンテンツは再生されません。
- **クライアントでクライアントがアクセス可能なコンテンツのみを再生する**。クライアント側での取得のみを試行します。失敗した場合、コンテンツは再生されません。

コンテンツが再生されない場合、プレーヤーウィンドウに次のエラーメッセージが表示されます（デフォルトの表示時間は5秒）。

「リソース不足のため、会社がビデオをブロックしました」



このエラーメッセージの表示時間は、VDA上の次のレジストリキーでカスタマイズできます。レジストリエントリが存在しない場合、表示時間はデフォルトで5秒になります。

レジストリパスは、VDAのアーキテクチャによって異なります。

```
\HKLM\SOFTWARE\Wow6432Node\Citrix\HdxMediastream
```

または

\HKLM\SOFTWARE\Citrix\HdxMediastream

レジストリキー：

名前: VideoLoadManagementErrDuration

種類: DWORD

範囲: 1 - DWORD制限まで（デフォルト = 5）

単位: 秒

Windows Mediaクライアント側コンテンツ取得

この設定はHTML5とWindows Mediaの両方に適用されます。この設定により、ユーザーデバイスは、XenAppまたはXenDesktop®ホストサーバーを介さずに、インターネットまたはイントラネット上のソースプロバイダーからマルチメディアファイルを直接ストリーミングできるようになります。

デフォルトでは、この設定は**許可**されています。この設定を許可すると、ネットワーク使用率とサーバーのスケーラビリティが向上します。この改善は、メディアに関するあらゆる処理をホストサーバーからユーザーデバイスに移動することで実現されます。また、Microsoft DirectShowやMedia Foundationなどの高度なマルチメディアフレームワークをユーザーデバイスにインストールする必要がなくなります。ユーザーデバイスには、URLからファイルを再生する機能のみが必要です。

この設定をポリシーに追加するときは、**Windows Mediaリダイレクト**設定が存在し、**許可**に設定されていることを確認してください。**Windows Mediaリダイレクト**が無効になっている場合、ソースプロバイダーからユーザーデバイスへのマルチメディアファイルの直接ストリーミングも無効になります。

Windows Mediaリダイレクト

この設定はHTML5とWindows Mediaの両方に適用され、サーバーがストリーミングオーディオとビデオをユーザーに配信する方法を制御および最適化します。

デフォルトでは、この設定は**許可**されています。HTML5の場合、ポリシー**HTML5ビデオのリダイレクト**が**禁止**されている場合、この設定は有効になりません。

この設定が有効になっている場合、サーバーからレンダリングされるオーディオとビデオの品質は、ユーザーデバイスでローカルに再生されるオーディオとビデオに匹敵するレベルに向上します。サーバーはマルチメディアを元の圧縮形式でクライアントにストリーミングし、ユーザーデバイスがメディアを解凍してレンダリングできるようにします。

Windows Mediaリダイレクトは、Microsoft DirectShow、DirectX Media Objects (DMO)、およびMedia Foundationの標準に準拠するコーデックでエンコードされたマルチメディアファイルを最適化します。特定のマルチメディアファイルを再生するには、そのマルチメディアファイルのエンコード形式と互換性のあるコーデックがユーザーデバイスに存在する必要があります。

デフォルトでは、Citrix Workspaceアプリでオーディオは無効になっています。ユーザーがICA®セッションでマルチメディアアプリケーションを実行できるようにするには、オーディオをオンにするか、Citrix Workspaceアプリインターフェイスでオーディオをオンにする権限をユーザーに付与します。

Windows Mediaリダイレクトを使用してメディアを再生したときの品質が、基本的なICA圧縮と通常のオーディオを使用してレンダリングした場合よりも悪い場合にのみ、**禁止**を選択してください。このような状況はまれですが、たとえばキーフレームの頻度が低いメディアの場合など、低帯域幅の条件下で発生する可能性があります。

Windows Mediaリダイレクトのバッファサイズ

この設定はレガシーであり、HTML5には適用されません。

この設定は、マルチメディアアクセラレーションのバッファサイズを1～10秒で指定します。

デフォルトでは、バッファサイズは5秒です。

Windows Mediaリダイレクトのバッファサイズの使用

この設定はレガシーであり、HTML5には適用されません。

この設定は、**Windows Media Redirection buffer size** 設定で指定されたバッファサイズの使用を有効または無効にします。

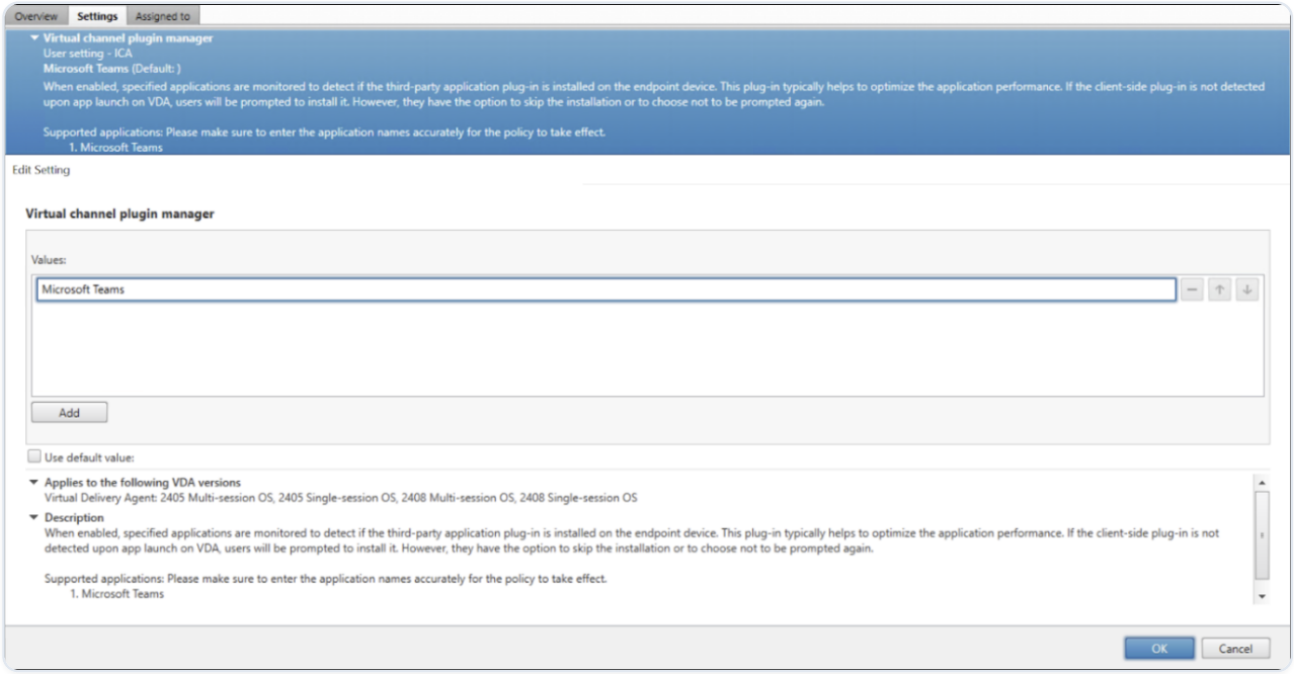
デフォルトでは、指定されたバッファサイズは使用されません。

この設定が無効になっている場合、または**Windows Media Redirection buffer size** 設定が構成されていない場合、サーバーはデフォルトのバッファサイズ値（5秒）を使用します。

仮想チャネルプラグインマネージャーポリシー

仮想チャネルプラグインマネージャーセクションには、この機能を構成するためのポリシー設定が含まれています。

仮想チャネルプラグインマネージャーは、特定の指定されたアプリケーションに対してクライアントエンドポイント全体にプラグインを展開するように設計されています。プラグインマネージャーは、VDAで実行されている特定のアプリケーションを検出し、アプリケーションの実行時に最高のエクスペリエンスを得るために、エンドポイントにプラグインをインストールするようユーザーに促します。



- 管理者はポリシーを使用して、エンドポイント全体にプラグインをインストールする必要があるアプリケーションを指定できます。
- アプリケーション名は、ポリシーの説明にある「サポートされているアプリケーション」に記載されている名前と同じである必要があります。
- デフォルトでは、ポリシーは無効になっています。
- 現在サポートされているアプリケーション
    - 「マイクロソフト チームズ」
- 今後、さらに多くのアプリケーションがサポートされる予定です。

マルチストリーム接続ポリシー設定

「**マルチストリーム接続**」セクションには、セッション内の複数のICA®接続のサービス品質の優先順位付けを管理するためのポリシー設定が含まれています。

> **注:**
>
> マルチストリーム接続ポリシーが有効になっている場合、MTU検出はサポートされません。

UDP経由のオーディオ

この設定は、サーバー上でのUDP経由のオーディオを許可または禁止します。

デフォルトでは、サーバー上でのUDP経由のオーディオは許可されています。

有効にすると、この設定はサーバー上でUDPポートを開き、UDP経由のオーディオリアルタイムトランスポートを使用するように構成されたすべての接続をサポートします。

オーディオUDPポート範囲

この設定は、Virtual Delivery Agent (VDA) によって使用されるポート番号の範囲（最小ポート番号、最大ポート番号）を指定します。この指定は、ユーザーデバイスとの間でオーディオパケットデータを交換するのに役立ちます。VDAは、ユーザーデバイスとデータを交換するために各UDPポートペアを使用しようとします。最小値から開始し、その後の試行ごとに2ずつ増やします。各ポートは、インバウンドトラフィックとアウトバウンドトラフィックの両方を処理します。

デフォルトでは、この範囲は16500,16509に設定されています。

マルチポートポリシー

この設定は、ICAトラフィックに使用するTCPポートを指定し、各ポートのネットワーク優先順位を確立します。

デフォルトでは、プライマリポート (2598) は高優先度です。

ポートを構成するとき、次の優先順位を割り当てることができます。

- **非常に高い:** ウェブカメラ会議などのリアルタイムアクティビティ用
- **高:** 画面、キーボード、マウスなどの対話型要素用
- **中:** クライアントドライブマッピングなどのバルク処理用
- **低:** 印刷などのバックグラウンドアクティビティ用

各ポートには一意の優先順位が必要です。たとえば、CGPポート1とCGPポート3の両方に「非常に高」の優先順位を割り当てることはできません。

ポートを優先順位付けから削除するには、ポート番号を0に設定します。プライマリポートを削除したり、その優先順位レベルを変更したりすることはできません。

この設定を構成するときは、サーバーを再起動してください。この設定は、**Multi-Stream computer**設定ポリシー設定が有効になっている場合にのみ有効になります。

マルチストリーム コンピューター設定

この設定は、サーバー上でMulti-Streamを有効または無効にします。

デフォルトでは、Multi-Streamは無効になっています。Citrix SD-WAN™またはサードパーティ製ルーターを使用して目的のQuality of Serviceを実現する場合は、Multi-Stream computerポリシー設定を構成してください。

Multi-Streamが有効になっている場合、Adaptive Transportの機能であるMTU Discoveryはサポートされません。

この設定を構成するときは、変更が有効になるようにサーバーを再起動してください。

> **重要:**
>
> このポリシー設定を、セッション全体の帯域幅制限などの帯域幅制限ポリシー設定と組み合わせて使用すると、予期しない結果が生じる可能性があります。この設定をポリシーに含める場合は、帯域幅制限設定が含まれていないことを確認してください。

マルチストリーム ユーザー設定

この設定は、ユーザーデバイス上でMulti-Streamを有効または無効にします。

デフォルトでは、Multi-Streamはすべてのユーザーに対して無効になっています。Citrix SD-WANまたはサードパーティ製ルーターを使用して目的のQuality of Serviceを実現する場合は、Multi-Stream user設定を構成してください。

この設定は、**マルチストリームコンピューター**設定ポリシー設定が有効になっているホストでのみ有効になります。

> **重要:**
>
> このポリシー設定を、全体的なセッション帯域幅制限などの帯域幅制限ポリシー設定と併用すると、予期しない結果が生じる可能性があります。この設定をポリシーに含める場合は、帯域幅制限設定を含めないようにしてください。

マルチストリーム仮想チャネル割り当て設定

この設定は、マルチストリームが使用されている場合に仮想チャネルが割り当てられるICAストリームを指定します。

これらの設定を構成しない場合、仮想チャネルはデフォルトのストリームに保持されます。仮想チャネルをICAストリームに割り当てるには、仮想チャネル名の横にある**ストリーム番号**リストから目的のストリーム番号（0、1、2、3）を選択します。

環境でカスタム仮想チャネルが使用されている場合は、**追加**をクリックし、**仮想チャネル**の下のテキストボックスに仮想チャネル名を指定し、その横にある**ストリーム番号**リストから目的のストリーム番号を選択します。指定する名前は、フレンドリ名ではなく、実際の仮想チャネル名である必要があります。たとえば、Citrix Browser AccelerationではなくCTXSBRです。

これらの設定は、マルチストリームコンピューター設定を有効にした場合にのみ有効になります。

デフォルトでは、仮想チャネルとそのストリーム割り当ては次のとおりです。

- AppFlow®: 2
- オーディオ: 0
- ブラウザコンテンツリダイレクト: 2
- クライアントCOMポートマッピング: 3

- クライアントドライブマッピング: 2
- クライアントプリンターマッピング: 3
- クリップボード: 2
- CTXDND: 1 (**注:** これは、Citrixセッションとローカルエンドポイント間でファイルをドラッグアンドドロップする機能をサポートします。)
- DVCプラグイン (DVCプラグインのフレンドリ名から自動生成された静的VC名、または管理者によって割り当てられたもの): 2
- エンドユーザーエクスペリエンス監視: 1
- ファイル転送 (HTML5 Receiver): 2
- 汎用データ転送: 2
- ICA制御: 1
- 入力メソッドエディター: 1
- レガシー クライアント プリンター マッピング (COM1): 1, 3
- レガシー クライアント プリンター マッピング (COM2): 2, 3
- レガシー クライアント プリンター マッピング (LPT1): 1, 3
- レガシー クライアント プリンター マッピング (LPT2): 2, 3
- ライセンス管理: 1
- Microsoft Teams/WebRTC リダイレクト: 1
- モバイルレシーバー: 1
- マルチタッチ: 1
- ポートフォワーディング: 2
- リモートオーディオおよびビデオ拡張機能 (RAVE): 2
- シームレス (透過ウィンドウ統合): 1
- センサーと位置情報: 1
- スマートカード: 1
- Thinwire グラフィック: 1
- 透過UI統合/ログオンステータス: 2
- TWAIN リダイレクト: 2
- USB: 2
- ゼロ遅延フォントおよびキーボード: 2

- ゼロ遅延データチャネル: 2

仮想チャネルの割り当てと優先度について詳しくは、Knowledge Center の記事 CTX131001 を参照してください。

ポートリダイレクトポリシー設定

ポートリダイレクトセクションには、クライアントLPTおよびCOMポートマッピングのポリシー設定が含まれています。

Virtual Delivery Agentのバージョンが**7.0より前**の場合、ポートリダイレクトを構成するには以下のポリシー設定を使用します。VDAバージョン**7.0から7.8**の場合、これらの設定はレジストリを使用して構成します。詳細については、「レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。VDAバージョン**7.9**の場合、以下のポリシー設定を使用します。

クライアントCOMポートの自動接続

この設定は、ユーザーがサイトにログオンしたときに、ユーザーデバイス上のCOMポートの自動接続を有効または無効にします。

デフォルトでは、クライアントCOMポートは自動的に接続されません。

クライアントLPTポートの自動接続

この設定は、ユーザーがサイトにログオンしたときに、ユーザーデバイス上のLPTポートの自動接続を有効または無効にします。

デフォルトでは、クライアントLPTポートは自動的に接続されません。

クライアントCOMポートリダイレクト

この設定は、ユーザーデバイス上のCOMポートへのアクセスを許可または禁止します。

デフォルトでは、COMポートリダイレクトは禁止されています。

関連するポリシー設定は次のとおりです。

- COMポートリダイレクトの帯域幅制限
- COMポートリダイレクトの帯域幅制限（パーセント）

クライアントLPTポートリダイレクト

この設定は、ユーザーデバイス上のLPTポートへのアクセスを許可または禁止します。

デフォルトでは、LPTポートリダイレクトは禁止されています。

LPTポートは、LPTポートに印刷ジョブを送信するレガシーアプリケーションでのみ使用されます。これらのポートは、ユーザーデバイス上の印刷オブジェクトに印刷ジョブを送信するレガシーアプリケーションでは使用されません。現在のほとんどのアプリケーションは、印刷ジョブをプリンターオブジェクトに送信できます。このポリシー設定は、LPTポートに印刷するレガシーアプリケーションをホストするサーバーにのみ必要です。

クライアントCOMポートリダイレクトは双方向ですが、LPTポートリダイレクトは出力のみであり、ICAセッション内では`\client\LPT1`および`\client\LPT2`に制限されます。

以下のポリシー設定は関連しています。

- LPTポートリダイレクト帯域幅制限
- LPTポートリダイレクトの帯域幅制限（パーセント）

FIDO2 ポリシー設定

この設定は、FIDO2リダイレクトを有効または無効にします。FIDO2リダイレクトにより、ユーザーは仮想マシン内のローカルエンドポイントFIDO2コンポーネントを活用できます。ユーザーは、TPM 2.0とWindows Helloを搭載したデバイスで、FIDO2セキュリティキーまたは統合生体認証を介して仮想セッションを認証できます。

この設定が**許可**されている場合、ユーザーはローカルエンドポイント機能を使用してFIDO2認証を行うことができます。デフォルトでは、この設定は**許可**されています。

印刷ポリシー設定

印刷セクションには、クライアント印刷を管理するためのポリシー設定が含まれています。

クライアントプリンターリダイレクト

この設定は、ユーザーがセッションにログオンしたときに、クライアントプリンターがサーバーにマップされるかどうかを制御します。

デフォルトでは、クライアントプリンターのマッピングは許可されています。この設定が無効になっている場合、セッション用のPDFプリンターは自動作成されません。

関連するポリシー設定: クライアントプリンターの自動作成

デフォルトプリンター

この設定は、ユーザーデバイス上のデフォルトプリンターがセッションでどのように確立されるかを指定します。

デフォルトでは、ユーザーの現在のプリンターがセッションのデフォルトプリンターとして使用されます。

デフォルトプリンターに現在のRemote Desktop ServicesまたはWindowsユーザープロファイル設定を使用するには、「ユーザーのデフォルトプリンターを調整しない」を選択します。このオプションを選択した場合、デフォルトプリンターはプロファイルに保存されず、他のセッションまたはクライアントプロパティに従って変更されることもありません。セッション内のデフォルトプリンターは、セッションで最初に自動作成されたプリンターであり、次のいずれかです。

- **コントロールパネル > デバイス**と**プリンター**でWindowsサーバーにローカルに追加された最初のプリンター。
- サーバーにローカルに追加されたプリンターがない場合、最初に自動作成されたプリンター。

このオプションを使用すると、プロファイル設定を通じてユーザーに最も近いプリンターを提示できます（近接印刷として知られています）。

プリンターの割り当て

この設定は、デフォルトプリンターとセッションプリンターの設定の代替手段を提供します。個別のデフォルトプリンターとセッションプリンターの設定を使用して、サイト、大規模グループ、または組織単位の動作を構成します。**プリンター割り当て**設定を使用して、多数のプリンターを複数のユーザーに割り当てます。

この設定は、リストされたユーザーデバイス上のデフォルトプリンターがセッションでどのように確立されるかを指定します。

デフォルトでは、ユーザーの現在のプリンターがセッションのデフォルトプリンターとして使用されます。

各ユーザーデバイスのセッションで自動作成されるネットワークプリンターも指定します。デフォルトでは、プリンターは指定されていません。

- デフォルトプリンターの値を設定する場合：

  ユーザーデバイスの現在のデフォルトプリンターを使用するには、「Do not adjust」を選択します。

  デフォルトプリンターに現在のRemote Desktop ServicesまたはWindowsユーザープロファイル設定を使用するには、「Do no adjust」を選択します。このオプションを選択すると、デフォルトプリンターはプロファイルに保存されず、他のセッションまたはクライアントのプロパティに応じて変更されません。セッション内のデフォルトプリンターは、セッションで最初に自動作成されたプリンターであり、次のいずれかです。

  - Windowsサーバーにローカルで追加された最初のプリンター（**コントロールパネル > デバイス**とプリンター）。
  - サーバーにローカルで追加されたプリンターがない場合、最初に自動作成されたプリンター。

- **セッションプリンターの値：プリンターを追加する**を設定する場合、自動作成したいプリンターのUNCパスを入力します。または、**参照**をクリックして、ネットワーク全体からプリンターを検索します。プリンターサーバーのFQDNまたはNetBIOS名を入力してプリンターを検索することもできます。詳細については、セッションプリンターを参照してください。プリンターを追加した後、ログオンごとに現在のセッションにカスタマイズされた設定を適用できます。

プリンターの自動作成イベントログ設定

この設定は、プリンターの自動作成プロセス中にログに記録されるイベントを指定します。エラーや警告をログに記録しない、エラーのみをログに記録する、またはエラーと警告をログに記録する、のいずれかを選択できます。

デフォルトでは、エラーと警告がログに記録されます。

警告の例としては、プリンターのネイティブドライバーをインストールできず、代わりにUniversal print driverがインストールされるイベントがあります。このシナリオでUniversal print driverを使用するには、Universal print driverの使用設定を「Use universal printing only」または「Use universal printing only if the requested driver is unavailable」に構成します。

セッションプリンター

この設定は、セッションで自動作成されるネットワークプリンターを指定します。ICA/HDXセッション内では、Citrix Print Managerサービス（CpSvc.exe）が、**セッションプリンター**ポリシー設定で指定された各ネットワークプリンターに対して、セッションログオン中にネットワークプリンター接続を作成します。セッションログオフ中にプリンターを削除します。デフォルトでは、プリンターは指定されていません。

セッションプリンターポリシー設定では、ネットワークプリンターはWindows Print ServerまたはCitrix Universal™ Print Server上に存在できます。

- **Windows Print Server:** 1つ以上のネットワークプリンターを共有します。また、ネットワークプリンターを使用するために必要なネイティブプリンタードライバーも備えています。
- **Universal Print Server:** Citrix Universal Print Serverソフトウェアがインストールされている Windows Print Server。

Windows Print Server を使用する場合、Citrix Print Manager サービスはネイティブプリンタードライバーを使用してネットワークプリンター接続を作成します。Citrix Virtual Apps™ サーバーには、ネイティブプリンタードライバーがインストールされている必要があります。

Citrix Universal Print Server を使用する場合、Citrix Print Manager サービスは、ネイティブプリンタードライバー、Citrix Universal Printer Driver、または Citrix Universal XPS Printer Driver のいずれかを使用してネットワークプリンター接続を作成します。使用するドライバーは、Universal Print Driver の使用ポリシー設定によって制御されます。

すべての Windows プリンタードライバーは現在、v3 または v4 ドライバーバージョンのいずれかに分類されます。詳細については、「Support for the Microsoft V3 and V4 Printer Driver Architectures」を参照してください。

セッションプリンターを追加し、それらがセッションに表示されることを確認するには、次の手順を実行します。

1. Web Studio にサインインし、左ペインで を選択し、 タブをクリックします。
2. ポリシーを選択し、 をクリックします。
3. ページで、 チェックボックスをオフにし、 をクリックして、次の手順に従ってプリンターを追加します。

   a. プリンターの UNC パスを `\\<FQDN of the printer server>\<printer name>.` の形式で入力します。または、 をクリックしてネットワーク全体からプリンターを検索します。プリンターサーバーの FQDN または NetBIOS 名を入力してプリンターを検索することもできます。

   > **注:**
   >
   > を使用して特定のプリンターを検索できるようにするには、プリンターを構成する際に、 **> >** の下にある オプションが選択されていることを確認してください。

   b. デフォルトでは、プリンターサーバーを参照するためにユーザー名とパスワードが使用されます。異なるドメイン資格情報が必要な場合は、 を選択し、必要なユーザー名とパスワードを入力して、 をクリックします。

   c. 「**完了**」をクリックします。

4. ポリシーが設定された後、公開されたアプリケーションにセッションプリンターが表示されない場合があります。この問題は、Citrix Virtual Apps サーバーにプリンタードライバーがないか、ポリシーが作成されたものの有効になっていないために発生する可能性があります。

   > **注:**
   >
   > セッションプリンターにネイティブプリンタードライバーが必要で、そのネイティブプリンタードライバーが VDA にインストールされていない場合、セッションプリンターはセッションに作成されない可能性があります。

5. 公開されたデスクトップを起動し、 **>** でセッションプリンターを手動で追加します。
6. これが失敗した場合は、Citrix Virtual Apps サーバーとプリントサーバー間の通信を調査します。RDP を使用してテストを実行することを検討してください。

プリンターが作成されるのを待つ

Delivery Controller のポリシーを使用して、Citrix Virtual Desktops でこの機能を有効にします。

プリンターの作成を待機する (サーバーデスクトップ):

この設定により、セッションへの接続を遅延させ、クライアントリダイレクトされたプリンターを自動作成できます。

デフォルトでは、接続遅延は発生しません。

プリンターの作成を待機する (Citrix Virtual Apps):

次の PowerShell コマンドレットを実行すると、マルチセッションホストで実行されている仮想アプリへの接続を遅延させ、アプリケーションが開かれる前にクライアントリダイレクトされたプリンターを自動作成できます。

```
Set-BrokerApplication -Name <VirtualAppName> -WaitForPrinterCreation $true
```

デフォルトでは、接続遅延は発生しません。

クライアントプリンターポリシー設定

クライアントプリンターセクションには、クライアントプリンターのポリシー設定が含まれています。これには、クライアントプリンターの自動作成、プリンタープロパティの保持、プリントサーバーへの接続に関する設定が含まれます。

クライアントプリンターの自動作成

この設定は、自動作成されるクライアントプリンターを指定します。この設定は、デフォルトのクライアントプリンター自動作成設定を上書きします。

デフォルトでは、すべてのクライアントプリンターが自動作成されます。

この設定は、**クライアントプリンターリダイレクト**設定が存在し、**許可**に設定されている場合にのみ有効になります。

この設定をポリシーに追加する際は、オプションを選択してください。

- **すべてのクライアントプリンターを自動作成**すると、ユーザーデバイス上のすべてのプリンターが自動的に作成されます。
- **クライアントのデフォルトプリンターのみを自動作成**すると、ユーザーデバイスでデフォルトプリンターとして選択されているプリンターのみが自動的に作成されます。
- **ローカル（非ネットワーク）クライアントプリンターのみを自動作成**すると、LPT、COM、USB、TCP/IP、またはその他のローカルポートを介してユーザーデバイスに直接接続されているプリンターのみが自動的に作成されます。
- **クライアントプリンターを自動作成しない**を選択すると、ユーザーがログオンしたときにすべてのクライアントプリンターの自動作成が無効になります。このオプションを選択すると、クライアントプリンターの自動作成に関するRemote Desktop Services (RDS) の設定が、優先度の低いポリシーのこの設定を上書きします。

汎用ユニバーサルプリンターの自動作成

この設定は、セッション用の汎用Citrix Universal™ Printerオブジェクトの自動作成を有効または無効にします。これらのセッションには、ユニバーサル印刷と互換性のあるユーザーデバイスが使用されているセッションのみが含まれます。

デフォルトでは、汎用ユニバーサルプリンターオブジェクトは自動作成されません。

関連するポリシー設定は次のとおりです。

- ユニバーサルプリントドライバーの使用状況
- ユニバーサルドライバーの優先順位

PDFユニバーサルプリンターの自動作成

この設定は、以下のセッションでCitrix PDFプリンターの自動作成を有効または無効にします。

- Windows向けCitrix Workspaceアプリ（VDA 7.19以降）
- Linux向けCitrix Workspace™アプリ

- macOS向けCitrix Workspaceアプリ
- HTML5向けCitrix Workspaceアプリ
- Chrome向けCitrix Workspaceアプリ

デフォルトでは、Citrix PDFプリンターは自動作成されません。

クライアントプリンター名

この設定は、自動作成されたクライアントプリンターの命名規則を選択します。

デフォルトでは、標準のプリンター名が使用されます。

「**標準プリンター名**」を選択すると、「HPLaserJet 4 from client name in session 3」のようなプリンター名が使用されます。

「**レガシープリンター名**」を選択すると、旧式のクライアントプリンター名が使用され、製品のXenDesktopバージョンに存在したレガシープリンター名との下位互換性が維持されます。このオプションは、現在のCitrix Virtual Apps and Desktopsバージョンの製品でも使用できます。レガシープリンター名の例は「Client/clientname#/HPLaserJet 4」です。このオプションはセキュリティが低下します。

Citrix Workspaceアプリ for HTML5から起動したセッションでCitrix PDFプリンターを使用する場合、「**クライアントプリンター名**」設定をデフォルトにするか、「**標準プリンター名**」を選択してください。「**レガシープリンター名**」を選択すると、Citrix Workspaceアプリ for HTML5はCitrix PDFプリンターオプションをサポートしません。

印刷サーバーへの直接接続

この設定は、仮想デスクトップまたはサーバーホスティングアプリケーションからクライアントプリンター用の印刷サーバーへの直接接続を有効または無効にします。ここで、クライアントプリンターはアクセス可能なネットワーク共有でホストされます。

デフォルトでは、直接接続が有効になっています。

ネットワークプリントサーバーが仮想デスクトップまたはサーバーホスティングアプリケーションからWANを介していない場合は、直接接続を有効にします。ネットワークプリントサーバーと仮想デスクトップまたはサーバーホスティングアプリケーションが同じLAN上にある場合、直接通信により印刷が高速化されます。

ネットワークがWANを介している場合、または大幅な遅延や帯域幅の制限がある場合は、直接接続を無効にします。印刷ジョブはユーザーデバイスを介してルーティングされ、そこでネットワークプリントサーバーにリダイレクトされます。ユーザーデバイスに送信されるデータは圧縮されるため、WANを介してデータが転送される際の帯域幅の消費が少なくなります。

2つのネットワークプリンターが同じ名前を持つ場合、ユーザーデバイスと同じネットワーク上のプリンターが使用されます。

プリンタードライバーのマッピングと互換性

この設定は、自動作成されたクライアントプリンターのドライバー置換ルールを指定します。

この設定は、Microsoft OneNoteおよびXPS Document Writerを自動作成されたクライアントプリンターリストから除外するように構成されています。

ドライバー置換ルールを定義する際、指定されたドライバーでプリンターが作成されることを許可または禁止できます。また、作成されたプリンターがユニバーサルプリントドライバーのみを使用することを許可することもできます。ドライバー置換は、ユーザーデバイスが提供するプリンタードライバー名を上書きまたはマッピングし、サーバー上の同等のドライバーに置き換えます。これらのルールにより、サーバーアプリケーションは、サーバーと同じドライバーを持つがドライバー名が異なるクライアントプリンターにアクセスできるようになります。

次のことができます。

- ドライバーマッピングを追加する
- 既存のマッピングを編集する
- マッピングのカスタム設定を上書きする
- マッピングを削除する
- リスト内のドライバーエントリの順序を変更する

マッピングを追加する際は、クライアントプリンタードライバー名を入力し、置き換えたいサーバードライバーを選択します。

プリンタープロパティの保持

この設定は、プリンターのプロパティを保存するかどうか、およびどこに保存するかを指定します。

デフォルトでは、システムはプリンターのプロパティがユーザーデバイスに保存されるか（利用可能な場合）、またはユーザープロファイルに保存されるかを決定します。

この設定をポリシーに追加するときは、オプションを選択してください。

- クライアントデバイスのみに保存は、保存されない必須プロファイルまたは移動プロファイルを持つユーザーデバイス向けです。
- ユーザープロファイルのみに保持は、帯域幅によって制約されるユーザーデバイス（このオプションはネットワークトラフィックを削減します）およびログオン速度、またはレガシープラ

グインを使用するユーザー向けです。このオプションは、プリンターのプロパティをサーバー上のユーザープロファイルに保存し、ユーザーデバイスとのプロパティ交換を防ぎます。このオプションは、Remote Desktop Services (RDS) の移動プロファイルが使用されている場合にのみ適用されます。

- クライアントに保存されていない場合のみプロファイルに保持は、システムがプリンターのプロパティをどこに保存するかを決定できるようにします。プリンターのプロパティは、利用可能な場合はユーザーデバイスに、またはユーザープロファイルに保存されます。このオプションは最も柔軟ですが、ログオン時間を遅くしたり、システムチェックのために余分な帯域幅を使用したりする可能性があります。
- プリンターのプロパティを保持しないは、プリンターのプロパティの保存を防ぎます。

保持および復元されたクライアントプリンター

この設定は、ユーザーデバイス上のプリンターの保持と再作成を有効または無効にします。デフォルトでは、クライアントプリンターは自動的に保持および復元されます。

保持されたプリンターとは、次回のセッション開始時に再度作成される、または記憶されるユーザー作成のプリンターです。Citrix Virtual Apps™ が保持されたプリンターを再作成する場合、**クライアントプリンターの自動作成**設定を除くすべてのポリシー設定が考慮されます。

復元されたプリンターとは、管理者が完全にカスタマイズし、クライアントポートに永続的にアタッチされた保存状態を持つプリンターです。

CITRIX PDFユニバーサルプリンタードライバー

Citrix PDFユニバーサルプリンタードライバーを使用すると、ユーザーはホストされたアプリケーションで開かれたドキュメントや、Citrix Virtual Apps and Desktopsによって提供される仮想デスクトップで実行されているアプリケーションを印刷できます。ユーザーが**Citrix PDFプリンター**オプションを選択すると、ドライバーはファイルをPDFに変換し、PDFをローカルデバイスに転送します。その後、PDFは表示のために開かれ、ローカルに接続されたプリンターから印刷されます。PDFは、Citrix Universal Printingでサポートされている形式の1つです（EMFおよびXPSに加えて）。 PDFプリンターは、Citrixポリシーを使用して有効化、構成、およびデフォルトとして設定できます。**Citrix PDFプリンター**オプションは、Windows、Linux、MacOS、Chrome、およびHTML5用のCitrix Workspaceアプリのユーザーが利用できます。

> **注:**
>
> WindowsエンドポイントにはPDFビューアーが必要です。クライアントには、PDFファイルを開くためにWindowsにファイルタイプ関連付けが登録されているアプリケーションが必要です。

ドライバーポリシー設定

「**ドライバー**」セクションには、プリンタードライバーに関連するポリシー設定が含まれています。

インボックスプリンタードライバーの自動インストール

> **注**
>
> このリリースでは、このポリシーはVDAをサポートしていません。

この設定は、以下のプリンタードライバーの自動インストールを有効または無効にします。

- Windowsインボックスドライバーセット
- `pnputil.exe /a`を使用してホストにステージングされたドライバーパッケージ

デフォルトでは、これらのドライバーは必要に応じてインストールされます。

ユニバーサルドライバーの優先順位

> **注:**
>
> このポリシー設定のデフォルトの順序は、Citrix Virtual Apps and Desktops™の第4四半期リリースで変更されます。新しいデフォルトの順序は次のとおりです。

- EMF
- XPS
- PCL5c (ピーシーエルファイブシー)
- PCL4
- PDF
- PS

この設定は、リストの最初のエントリから始まる、ユニバーサルプリンタードライバーが使用される順序を指定します。

デフォルトでは、優先順位は次のとおりです。

- EMF
- XPS
- PCL5c (ピーシーエルファイブシー)
- PCL4
- PS

ドライバーの追加、編集、削除、およびリスト内のドライバーの順序変更が可能です。

ユニバーサルプリントドライバーの使用

この設定は、ユニバーサル印刷を使用するタイミングを指定します。

既定では、要求されたドライバーが利用できない場合にのみ、ユニバーサル印刷が使用されます。

ユニバーサル印刷では、標準のモデル固有ドライバーの代わりに汎用プリンタードライバーが使用されるため、ホストコンピューターでのドライバー管理の負担が軽減される可能性があります。ユニバーサル印刷ドライバーの可用性は、ユーザーデバイス、ホスト、および印刷サーバーソフトウェアの機能によって異なります。特定の構成では、ユニバーサル印刷が利用できない場合があります。

この設定をポリシーに追加するときは、次の表からオプションを選択します。

オプション	説明
プリンターモデル固有のドライバーのみを使用する	クライアントプリンターが、サインイン時に自動作成される標準のモデル固有ドライバーのみを使用することを指定します。要求されたドライバーが利用できない場合、クライアントプリンターは自動作成できません。
ユニバーサル印刷のみを使用する	標準のモデル固有ドライバーは使用されないことを指定します。プリンターの作成には、ユニバーサル印刷ドライバーのみが使用されます。
要求されたドライバーが利用できない場合にのみユニバーサル印刷を使用する	利用可能な場合は、プリンター作成に標準のモデル固有ドライバーを使用します。ドライバーがサーバーで利用できない場合、クライ

オプション	説明
	アントプリンターは適切なユニバーサルドライバーで自動的に作成されます。
ユニバーサル印刷が利用できない場合にのみプリンターモデル固有のドライバーを使用する	利用可能な場合は、ユニバーサル印刷ドライバーを使用します。ドライバーがサーバーで利用できない場合、クライアントプリンターは適切なモデル固有のプリンタードライバーで自動的に作成されます。

ユニバーサルプリントサーバーのポリシー設定

ユニバーサルプリントサーバーセクションには、ユニバーサルプリントサーバーを処理するためのポリシー設定が含まれています。

SSL暗号スイート

この設定は、暗号化された印刷データストリーム (CGP) 接続のためにUniversal Print Clientで使用されるSSL/TLS暗号スイートのセットを指定します。

暗号化された印刷Webサービス (HTTPS/SOAP) 接続のためにUniversal Print Clientで使用される暗号スイートパッケージを制御するには、を参照してください。

デフォルト値: ALL

この設定には次の値があります: ALL、COM、またはGOV。

各値に対応する暗号スイートは次のとおりです:

ALL:

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

TLS_ECDHE_RSA_AES128_CBC_SHA

COM:

TLS_ECDHE_RSA_AES128_CBC_SHA

GOV:

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

SSL準拠モード

この設定は、Universal Print Clientが暗号化された印刷データストリーム (CGP) 接続に使用するNIST Special Publication 800-52への準拠レベルを指定します。

デフォルト値: なし。

この設定には次の値があります:

なし。

暗号化された印刷データストリーム (CGP) 接続は、デフォルトの準拠モードを使用します。

SP800-52。

暗号化された印刷データストリーム (CGP) 接続は、NIST Special Publication 800-52準拠モードを使用します。

SSL有効

この設定は、Universal Print Clientが以下の目的でSSL/TLSを使用するかどうかを指定します:

- 印刷データストリーム (CGP) 接続
- Webサービス (HTTP/SOAP) 接続

Universal Print Server enable を **Enabled with fallback to Windows' native remote printing** に設定すると、Microsoft Windows Network Print Providerによってフォールバック接続が行われます。この設定は、これらのフォールバック接続には影響しません。

既定値: 無効

この設定は次の値をとります。

有効。

ユニバーサルプリントクライアントは、Universal Print Serverへの接続にSSL/TLSを使用します。

無効。

ユニバーサルプリントクライアントは、Universal Print Serverへの接続にSSL/TLSを使用します。

SSL FIPSモード

この設定は、Universal Print Clientが印刷データストリーム（CGP）接続のために使用するSSL/TLS暗号化モジュールがFIPSモードで実行されるかどうかを指定します。

既定値: 無効

この設定は次の値をとります。

有効。

FIPSモードがオンになります。

無効。

FIPSモードがオフになります。

SSLプロトコルバージョン

この設定は、Universal Print Client が使用する SSL/TLS プロトコルバージョンを指定します。

デフォルト値: ALL

この設定には次の値があります。

ALL。

TLS バージョン 1.0、1.1、または 1.2 を使用します。

ティーエルエスv1.

TLS バージョン 1.0 を使用します。

TLSv1.1。

TLS バージョン 1.1 を使用します。

TLSv1.2。

TLS バージョン 1.2 を使用します。

SSL UNIVERSAL PRINT SERVER 暗号化印刷データストリーム (CGP) ポート

この設定は、Universal Print Server 暗号化印刷データストリーム (CGP) ポートの TCP ポート番号を指定します。このポートは、印刷ジョブのデータを受信します。

デフォルト値: 443

SSL UNIVERSAL PRINT SERVER 暗号化 WEB サービス (HTTPS/SOAP) ポート

この設定は、Universal Print Serverの暗号化されたWebサービス（HTTPS/SOAP）ポートのTCPポート番号を指定します。このポートは、印刷コマンドのデータを受信します。

デフォルト値: 8443

UNIVERSAL PRINT SERVERの有効化

このポリシーは、Citrix Universal Print Server (UPS) の使用を有効または無効にします。このポリシー設定は、仮想デスクトップまたはサーバーホスティングアプリケーションを含む組織単位 (OU) に適用します。このポリシー設定には、Citrix UPSコンポーネントが要求されたプリントサーバーにインストールされていないか、利用できない場合に、ネイティブのWindowsリモート印刷サービスを使用してプリントサーバーへの接続を許可するフォールバックオプションが含まれています。このポリシーへの変更は、VDAが再起動された後にのみ適用されます。

デフォルトでは、Universal Print Serverは無効になっています。

この設定をポリシーに追加するときは、次のいずれかのオプションを選択します。

- **Windowsネイティブのリモート印刷へのフォールバックを有効にする**: 可能な場合、Universal Print Serverはネットワークプリンター接続を処理します。Universal Print Serverが利用できない場合、Windows Print Providerが使用されます。Windows Print Providerは、以前にWindows Print Providerで作成されたすべてのプリンターを引き続き処理します。
- **Windowsネイティブのリモート印刷へのフォールバックなしで有効にする**: Universal Print Serverは、ネットワークプリンター接続を排他的に処理します。Universal Print Serverが利用できない場合、ネットワークプリンター接続は失敗します。この設定は、Windows Print Providerを介したネットワーク印刷を実質的に無効にします。この設定を含むポリシーがアクティブな間は、以前にWindows Print Providerで作成されたプリンターは作成されません。
- **無効**: Universal Print Server機能は無効です。UNC名を持つネットワークプリンターに接続する際、Universal Print Serverへの接続は試行されません。リモートプリンターへの接続は、引き続きWindowsネイティブのリモート印刷機能を使用します。

UNIVERSAL PRINT SERVER印刷データストリーム (CGP) ポート

この設定は、Universal Print Server印刷データストリームのCommon Gateway Protocol (CGP) リスナーが使用するTCPポート番号を指定します。このポリシー設定は、プリントサーバーを含むOUにのみ適用します。

デフォルトでは、ポート番号は7229に設定されています。

有効なポート番号は1～65535の範囲である必要があります。

UNIVERSAL PRINT SERVER印刷ストリーム入力帯域幅制限 (KBPS)

この設定は、印刷データの転送速度の上限（キロビット/秒）を指定します。転送速度は、各印刷ジョブからCGPを使用してUniversal Print Serverに配信される印刷データに対して計算されます。このポリシー設定は、仮想デスクトップまたはサーバーホスティングアプリケーションを含むOUに適用します。

デフォルトでは、値は0であり、上限がないことを指定します。

UNIVERSAL PRINT SERVER WEBサービス (HTTP/SOAP) ポート

この設定は、Universal Print ServerのWebサービス (HTTP/SOAP) リスナーが使用するTCPポート番号を指定します。Universal Print Serverは、ネットワーク印刷シナリオでCitrixユニバーサル印刷ドライバーの使用を可能にするオプションコンポーネントです。

Universal Print Serverが使用される場合、印刷コマンドはCitrix Virtual Apps and Desktopsホストから SOAP over HTTPを介してUniversal Print Serverに送信されます。この設定は、Universal Print Serverが受信HTTP/SOAPリクエストをリッスンするデフォルトのTCPポートを変更します。

ホストと印刷サーバーのHTTPポートは両方とも同じように構成する必要があります。ポートを同じように構成しない場合、ホストソフトウェアはUniversal Print Serverに接続しません。この設定は、Citrix Virtual Apps and Desktops上のVDAを変更します。さらに、Universal Print Serverのデフォルトポートも変更する必要があります。

デフォルトでは、ポート番号は8080に設定されています。

有効なポート番号は0～65535の範囲である必要があります。

負荷分散用のUNIVERSAL PRINT SERVER

この設定は、他のCitrix®印刷ポリシー設定を評価した後、セッション起動時に確立されたプリンター接続の負荷分散に使用されるUniversal Print Serverを一覧表示します。プリンター作成時間を最適化するために、Citrixはすべての印刷サーバーが同じ共有プリンターのセットを持つことを推奨します。負荷分散のために追加できる印刷サーバーの数に上限はありません。

この設定は、印刷サーバーのフェイルオーバー検出とプリンター接続の回復も実装します。印刷サーバーは定期的に可用性がチェックされます。サーバー障害が検出された場合、そのサーバーは負荷分散スキームから削除されます。また、そのサーバー上のプリンター接続は、他の利用可能な印刷サーバーに再配布されます。障害が発生した印刷サーバーが回復すると、負荷分散スキームに戻されます。

Validate Servers をクリックして、各サーバーが印刷サーバーであること、サーバーリストに重複するサーバー名が含まれていないこと、およびすべてのサーバーに同一の共有プリンターセットがインストールされていることを確認します。この操作には時間がかかる場合があります。

UNIVERSAL PRINT SERVERサービス停止しきい値

この設定は、ロードバランサーが利用できない印刷サーバーが回復するのをどれくらいの期間待つかを指定します。この期間が過ぎると、サーバーは永続的にオフラインであると判断され、その負荷は他の利用可能な印刷サーバーに再配布されます。

デフォルトでは、しきい値は180（秒）に設定されています。

UNIVERSAL PRINT SERVER WEBサービス (HTTP/SOAP) 接続タイムアウト

この設定は、Universal Print ClientがUniversal Print Server Webサービスのconnect()操作がタイムアウトするまで待機する秒数を指定します。この設定には以下の値があります。これらの値はすべて数値であり、単位（時間）は秒です。

- 最小値は0です。
- 最大値は60です。
- デフォルト値は10です。

タイムアウトが1から60（両端を含む）の場合、Universal Print Clientは、操作が完了するまで指定された時間待機します。この操作は、TCPソケット接続操作です。ソケットは、TCP/IPネットワークを介したプロセス間通信を可能にするWindowsオペレーティングシステムの機能です。

タイムアウトが0の場合、Universal Print Clientは、オペレーティングシステムによって定義されたデフォルトのタイムアウトを使用します。この構成は、この変更前のUniversal Print Clientの以前のバージョンで利用可能だった構成です。

Universal Print Clientは、Universal Print Serverと通信するVirtual Delivery Agent (VDA) のコンポーネントです。

> **注:**
>
> このポリシー設定は、VDAバージョン7.35以降に適用されます。

UNIVERSAL PRINT SERVER WEBサービス (HTTP/SOAP) 受信タイムアウト

この設定は、Universal Print ClientがUniversal Print Server Webサービスのrecv()操作がタイムアウトするまで待機する秒数を指定します。この設定には次の値があり、これらの値はすべて数値で、単位（時間）は秒です。

- 最小値は0です。
- 最大値は60です。
- デフォルト値は10です。

タイムアウトが1から60（両端を含む）の場合、Universal Print Clientは、操作が完了するまで指定された時間待機します。この操作は、TCPソケット受信操作です。ソケットは、TCP/IPネットワークを介したプロセス間通信を可能にするWindowsオペレーティングシステムの機能です。

タイムアウトが0の場合、Universal Print Clientは、オペレーティングシステムによって定義されたデフォルトのタイムアウトを使用します。この構成は、この変更前のUniversal Print Clientの以前のバージョンで利用可能だった構成です。

Universal Print Clientは、Universal Print Serverと通信するVirtual Delivery Agent (VDA) のコンポーネントです。

> **注:**
>
> このポリシー設定は、VDAバージョン7.35以降で適用されます。

UNIVERSAL PRINT SERVER WEBサービス (HTTP/SOAP) 送信タイムアウト

この設定は、Universal Print Client が Universal Print Server Webサービスの send() 操作がタイムアウトするまで待機する秒数を指定します。この設定には次の値があります。これらの値はすべて数値であり、単位（時間）は秒です。

- 最小値は0です。
- 最大値は60です。
- デフォルト値は10です。

タイムアウトが1から60（両端を含む）の場合、Universal Print Client は操作が完了するまで指定された時間待機します。この操作はTCPソケット送信操作です。ソケットは、TCP/IPネットワークを介したプロセス間通信を可能にするWindowsオペレーティングシステムの機能です。

タイムアウトが0の場合、Universal Print Client はオペレーティングシステムによって定義されたデフォルトのタイムアウトを使用します。この構成は、この変更前のUniversal Print Clientの以前のバージョンで利用可能だった構成です。

Universal Print Client は、Universal Print Server と通信するVDAのコンポーネントです。

> **注:**
>
> このポリシー設定は、VDAバージョン7.35以降で適用されます。

ユニバーサル印刷ポリシー設定

ユニバーサル印刷セクションには、ユニバーサル印刷を管理するためのポリシー設定が含まれています。

ユニバーサル印刷EMF処理モード

この設定は、Windowsユーザーデバイス上のEMFスプールファイルの処理方法を制御します。

デフォルトでは、EMFレコードはプリンターに直接スプールされます。

この設定をポリシーに追加するときは、オプションを選択します。

- プリンター用のEMFを再処理すると、EMFスプールファイルが再処理され、ユーザーデバイス上のGDIサブシステムを介して送信されます。この設定は、EMFの再処理を必要とするが、セッションで自動的に選択されない可能性のあるドライバーに使用できます。
- Citrix Universal™プリンタードライバーで使用する場合、プリンターに直接スプールすると、EMFレコードがスプールされ、処理のためにユーザーデバイスに配信されます。通常、これらのEMFスプールファイルはクライアントのスプールキューに直接挿入されます。EMF形式と互換性のあるプリンターおよびドライバーの場合、これが最速の印刷方法です。

ユニバーサル印刷画像圧縮制限

この設定は以下を指定します:

- Citrix Universal Print Driverで印刷される画像に利用可能な最大品質
- Citrix Universal Print Driverで印刷される画像に利用可能な最小圧縮レベル

デフォルトでは、画像圧縮制限は「最高品質（ロスレス圧縮）」に設定されています。

「圧縮なし」が選択されている場合、EMF印刷のみ圧縮が無効になります。

この設定をポリシーに追加するときは、オプションを選択します。

- 圧縮なし
- 最高品質 (ロスレス圧縮)
- 高音質
- 標準品質
- 低品質 (最大圧縮)

この設定を**ユニバーサル印刷最適化のデフォルト**設定を含むポリシーに追加する場合は、次の点に注意してください。

- **ユニバーサル印刷画像圧縮制限**設定の圧縮レベルが、**ユニバーサル印刷最適化のデフォルト**設定で定義されているレベルよりも低い場合を考慮してください。この場合、画像はユニバーサル印刷画像圧縮制限設定で定義されているレベルで圧縮されます。

- 圧縮が無効になっている場合、ユニバーサル印刷最適化のデフォルト設定の「希望する画質」および「ヘビーウェイト圧縮を有効にする」オプションは、ポリシーに影響を与えません。

ユニバーサル印刷最適化のデフォルト

この設定は、セッション用にユニバーサル印刷ドライバーが作成される際の印刷最適化のデフォルト値を指定します。

- 希望する画質は、ユニバーサル印刷に適用されるデフォルトの画像圧縮制限を指定します。デフォルトでは、標準品質が有効になっており、ユーザーは標準または低品質の圧縮を使用してのみ画像を印刷できます。
- ヘビーウェイト圧縮を有効にするは、希望する画質で設定された圧縮レベルを超えて帯域幅を削減するかどうかを有効または無効にします。画質は低下しません。デフォルトでは、ヘビーウェイト圧縮は無効になっています。
- 画像とフォントのキャッシュ設定は、印刷ストリームに複数回出現する画像とフォントをキャッシュするかどうかを指定します。この設定により、各固有の画像またはフォントがプリンターに一度だけ送信されることが保証されます。デフォルトでは、埋め込み画像とフォントはキャッシュされます。これらの設定は、ユーザーデバイスがこの動作をサポートしている場合にのみ適用されます。
- 非管理者によるこれらの設定の変更を許可するは、ユーザーがセッション内でデフォルトの印刷最適化設定を変更できるかどうかを指定します。デフォルトでは、ユーザーはデフォルトの印刷最適化設定を変更できません。

注: これらのオプションはすべてEMF印刷でサポートされています。XPS印刷では、「希望する画質」オプションのみがサポートされています。

この設定を**ユニバーサル印刷画像圧縮制限**設定を含むポリシーに追加する場合は、次の点に注意してください。

- **ユニバーサル印刷画像圧縮制限**設定の圧縮レベルが、**ユニバーサル印刷最適化のデフォルト**設定で定義されているレベルよりも低い場合を考慮してください。この場合、画像はユニバーサル印刷画像圧縮制限設定で定義されているレベルで圧縮されます。
- 圧縮が無効になっている場合、ポリシーでは、ユニバーサル印刷最適化のデフォルト設定の「希望する画質」と「ヘビーウェイト圧縮を有効にする」オプションは無効になります。

ユニバーサル印刷プレビューの優先設定

この設定は、自動作成されたプリンターまたは汎用ユニバーサルプリンターに対して印刷プレビュー機能を使用するかどうかを指定します。

デフォルトでは、自動作成されたプリンターまたは汎用ユニバーサルプリンターに対して印刷プレビューは使用されません。

この設定をポリシーに追加するときは、オプションを選択します。

- 自動作成されたプリンターまたは汎用ユニバーサルプリンターに対して印刷プレビューを使用しない
- 自動作成されたプリンターに対してのみ印刷プレビューを使用する
- 汎用ユニバーサルプリンターに対してのみ印刷プレビューを使用する
- 自動作成されたプリンターと汎用ユニバーサルプリンターの両方に対して印刷プレビューを使用する

ユニバーサル印刷の印刷品質制限

この設定は、セッションで印刷出力を生成するために利用できる最大ドット/インチ (dpi) を指定します。

デフォルトでは、「制限なし」が有効になっており、ユーザーは接続先のプリンターで許可されている最高の印刷品質を選択できます。

この設定が構成されている場合、出力解像度の観点から、ユーザーが利用できる最大印刷品質が制限されます。印刷品質自体と、ユーザーが接続するプリンターの印刷品質機能の両方が、構成された設定に制限されます。

たとえば、中解像度 (600 DPI) に構成されている場合、ユーザーは最大 600 DPI の品質でしか出力を印刷できません。また、**ユニバーサルプリンター**ダイアログボックスの**詳細設定**タブにある**印刷品質**設定には、中品質 (600 DPI) までの解像度設定のみが表示されます。

この設定をポリシーに追加するときは、オプションを選択します。

- 下書き (150 DPI)
- 低解像度 (300 DPI)
- 中解像度 (600 DPI)
- 高解像度 (1200 DPI)
- 制限なし

セキュリティポリシー設定

セキュリティセクションには、セッション暗号化とログオンデータの暗号化を構成するためのポリシー設定が含まれています。

SecureICAの最小暗号化レベル

この設定は、サーバーとユーザーデバイス間で送信されるセッションデータを暗号化する最小レベルを指定します。

重要: Virtual Delivery Agent 7.xの場合、このポリシー設定は、RC5 128ビット暗号化によるログオンデータの暗号化を有効にするためにのみ使用できます。その他の設定は、Citrix Virtual Apps and Desktopsのレガシーバージョンとの下位互換性のためにのみ提供されています。

VDA 7.xの場合、セッションデータの暗号化はVDAのDelivery Groupの基本設定を使用して行われます。Delivery GroupでEnable Secure ICAが選択されている場合、セッションデータはRC5 (128ビット) 暗号化を使用して暗号化されます。Delivery GroupでEnable Secure ICAが選択されていない場合、セッションデータは基本暗号化で暗号化されます。

この設定をポリシーに追加するときは、オプションを選択してください。

- Basicは、非RC5アルゴリズムを使用してクライアント接続を暗号化します。これにより、データストリームが直接読み取られるのを防ぎますが、復号化は可能です。デフォルトでは、サーバーはクライアント-サーバー間のトラフィックにBasic暗号化を使用します。
- RC5 (128ビット) ログオンは、RC5 128ビット暗号化を使用してログオンデータのみを暗号化し、クライアント接続にはBasic暗号化を使用します。
- RC5 (40ビット) は、RC5 40ビット暗号化を使用してクライアント接続を暗号化します。
- RC5 (56ビット) は、RC5 56ビット暗号化を使用してクライアント接続を暗号化します。
- RC5 (128ビット) は、RC5 128ビット暗号化を使用してクライアント接続を暗号化します。

クライアント-サーバー暗号化に指定する設定は、環境内の他の暗号化設定やWindowsオペレーティングシステムと相互作用する可能性があります。サーバーまたはユーザーデバイスのいずれかで、より高い優先度の暗号化レベルが設定されている場合を考慮してください。この場合、公開リソースに指定した設定が上書きされる可能性があります。

特定のユーザーの通信とメッセージの整合性をさらに保護するために、暗号化レベルを上げることができます。ポリシーでより高い暗号化レベルが必要な場合、より低い暗号化レベルを使用しているCitrix Receiversは接続を拒否されます。

SecureICAは認証やデータ整合性のチェックを行いません。サイトにエンドツーエンドの暗号化を提供するには、SecureICAをTLS暗号化と組み合わせて使用してください。

SecureICAはFIPS準拠のアルゴリズムを使用しません。この設定が問題となる場合は、SecureICAを使用しないようにサーバーとCitrix Receiverを構成してください。

SecureICAは、機密保持のためにRFC 2040で説明されているRC5ブロック暗号を使用します。ブロックサイズは64ビット（32ビットワード単位の倍数）です。キー長は128ビットです。ラウンド数は12です。

RC5ブロック暗号のキーは、セッションが作成されるときにネゴシエートされます。ネゴシエーションはDiffie-Hellmanアルゴリズムを使用して実行されます。このネゴシエーションでは、Diffie-Hellman公開パラメーターが使用されます。これらのパラメーターは、Virtual Delivery Agentのインストール時にWindowsレジストリに保存されます。公開パラメーターは秘密ではありません。Diffie-Hellmanネゴシエーションの結果は秘密キーであり、そこからRC5ブロック暗号のセッションキーが導出されます。ユーザーログオン用とデータ転送用に個別のセッションキーが使用されます。また、Virtual Delivery Agentとの間のトラフィックにも個別のセッションキーが使用されます。したがって、各セッションには4つのセッションキーがあります。秘密キーとセッションキーは保存されません。RC5ブロック暗号の初期化ベクトルも秘密キーから導出されます。

サーバー制限ポリシー設定

サーバー制限セクションには、アイドル接続を制御するためのポリシー設定が含まれています。

サーバーアイドルタイマー間隔

この設定は、ユーザーからの入力がない場合に、中断されないユーザーセッションがどのくらいの期間維持されるかを決定します。データはミリ秒で計算されます。

デフォルトでは、アイドル接続は切断されません（サーバーアイドルタイマー間隔 = 0）。Citrix®は、この値を最低60000ミリ秒（60秒）に設定することを推奨します。

ポリシーを表示するには、**複数のバージョン**を選択し、シングルセッションOSのバージョンをクリアしてから、**サーバー制限**を選択します。

> **注**
>
> このポリシー設定が使用されている場合、セッションが指定された時間アイドル状態であったときに、ユーザーに「アイドルタイマーの期限切れ」ダイアログボックスが表示されることがあります。Citrixポリシー設定は、このMicrosoftダイアログボックスメッセージを制御しません。詳細については、`<http://support.citrix.com/article/CTX118618>`を参照してください。

セッション制限ポリシー設定

セッション制限セクションには、セッションが強制的にログオフされるまでに接続を維持する期間を制御するポリシー設定が含まれています。

切断されたセッションタイマー

この設定は、切断されロックされたデスクトップが、セッションがログオフされるまでにロックされたままになる期間を指定するタイマーを有効または無効にします。

このタイマーが有効になっている場合、タイマーの期限が切れると、切断されたセッションはログオフされます。

デフォルトでは、切断されたセッションはログオフされません。

Remote PC Accessの切断されたセッションタイマー

この設定は、タイマーの期限が切れた後に切断されたユーザーセッションをログオフするタイマーを有効または無効にします。この設定を有効にする場合は、**切断されたセッションタイマー間隔**設定を使用して、ユーザーセッションがログオフされるまでに切断されたデスクトップがロックされたままになる期間を分単位で指定します。

デフォルトでは、この設定は無効になっています。

切断されたセッションタイマー間隔

この設定は、切断されロックされたデスクトップが、セッションがログオフされるまでにロックされたままになる期間を分単位で指定します。

デフォルトでは、期間は1,440分（24時間）です。

切断されたセッションタイマー – マルチセッション

この設定は、切断されたRDSセッションがログオフされるまでにどのくらいの期間持続できるかを決定するタイマーを有効または無効にします。デフォルトでは、このタイマーは無効になっており、切断されたセッションはログオフされません。

切断されたセッションタイマー間隔 – マルチセッション

この設定は、切断されたRDSセッションがログオフされるまでにどのくらいの期間（分単位）持続できるかを決定します。デフォルトでは、期間は1440分（24時間）です。

セッション接続タイマー

この設定は、ユーザーデバイスとデスクトップ間の途切れない接続の最大継続時間を指定するタイマーを有効または無効にします。このタイマーが有効になっている場合、タイマーの期限が切れるとセッションは切断されるか、ログオフされます。Microsoft の「**時間制限に達したときにセッションを終了する**」設定が、セッションの次の状態を決定します。

デフォルトでは、このタイマーは無効になっています。

セッション接続タイマー間隔

この設定は、ユーザーデバイスとデスクトップ間の途切れない接続の最大分数（時間）を指定します。

デフォルトでは、最大継続時間は1,440分（24時間）です。

セッション接続タイマー – マルチセッション

この設定は、ユーザーデバイスとターミナルサーバー間の途切れない接続の最大継続時間を指定するタイマーを有効または無効にします。デフォルトでは、このタイマーは無効になっています。

セッション接続タイマー間隔 – マルチセッション

この設定は、ユーザーデバイスとRDSセッション間の途切れない接続の最大分数（時間）を指定します。デフォルトでは、最大継続時間は1440分（24時間）です。

セッションアイドルタイマー

ユーザーが何も入力しない場合、この設定は以下を有効または無効にするために使用されます。

- デスクトップへの途切れないユーザーデバイス接続が維持される期間を指定するタイマー。

このタイマーの期限が切れると、セッションは切断状態になり、**「切断されたセッションタイマー」**が適用されます。**「切断されたセッションタイマー」**が無効になっている場合、セッションはログオフされません。

デフォルトでは、このタイマーは有効になっています。

セッションアイドルタイマー間隔

ユーザーからの入力がない場合、この設定は以下を指定するために使用されます。

- デスクトップへのユーザーデバイスの途切れない接続が維持される分数。

デフォルトでは、アイドル状態の接続は1,440分（24時間）維持されます。

セッションアイドルタイマー – マルチセッション

この設定は、ユーザーデバイスとターミナルサーバー間のアイドル接続の最大期間を決定するタイマーを有効または無効にします。デフォルトでは、このタイマーは無効になっています。

セッションアイドルタイマー間隔 – マルチセッション

この設定は、ユーザーデバイスとRDSセッション間のアイドル接続が何分間維持されるかを指定します。デフォルトでは、最大期間は1440分（24時間）です。

> **注:**

Citrix®ポリシーを使用して構成されたマルチセッションマシンのタイマー設定は、Microsoftグループポリシーを通じて構成されたタイマー設定を上書きすることが想定されています。予期しない動作を避けるため、いずれかの方法を使用してタイマー設定を構成することをお勧めします。

セッションの信頼性ポリシー設定

セッションの信頼性セクションには、セッションの信頼性接続を管理するためのポリシー設定が含まれています。

セッションの信頼性接続

この設定により、ネットワーク接続が失われたときにセッションを開いたままにするかどうかが決まります。セッションの信頼性は、自動クライアント再接続と連携して、ネットワーク障害から回復した後にユーザーがCitrix Workspace™アプリセッションに自動的に再接続できるようにします。デフォルトでは、セッションの信頼性は許可されています。

Web Studioの設定は、以下のクライアントに適用されます。

- Citrix Workspaceアプリ1808以降
- Citrix Receiver for Windows 4.7以降のバージョン。

Web Studioポリシーは、クライアント上のCitrix Receiver™グループポリシーオブジェクトを上書きします。Web Studioでこれらのポリシーを更新すると、セッションの信頼性がサーバーからクライアントに同期されます。

注:

- Citrix Receiver for Windows 4.7以降およびCitrix Workspaceアプリ for Windows - Web Studioでポリシーを設定します。
- Citrix Receivers for Windows 4.7より前のバージョン - Web Studioでポリシーを設定します。また、一貫した動作のために、クライアントでCitrix Receiverグループポリシーオブジェクトテンプレートを設定します。

ネットワーク接続が中断された場合、セッションの信頼性によりセッションがアクティブな状態に保たれ、ユーザーの画面に表示されます。ユーザーは、ネットワーク接続が再開されるまで、使用しているアプリケーションを引き続き見ることができます。

セッションの信頼性を使用して、サーバー上でセッションをアクティブな状態に保ちます。接続が失われたことを示すために、ユーザーのディスプレイは不透明になります。ユーザーは中断中にフリーズしたセッションを見る可能性があります。ネットワーク接続が復元されると、ユーザーはアプリケーションとの対話を再開できます。セッションの信頼性により、再認証のプロンプトなしでユーザーが再接続されます。

セッションの信頼性と自動クライアント再接続の両方を使用する場合、これら2つの機能は順番に動作します。セッションの信頼性は、セッションの信頼性タイムアウト設定で指定された時間の経過後にユーザーセッションを閉じ（または切断し）ます。その後、自動クライアント再接続設定が有効になり、切断されたセッションにユーザーを再接続しようとします。

デフォルトでは、セッションの信頼性は許可されています。

> **注:**
>
> Citrix ADCを使用している場合、ICA接続をプロキシするには、Citrix StoreFront > **Manage Citrix Gateways** / **Secure Ticket Authority**で**セッションの信頼性を有効にする**を選択する必要があります。

セッションの信頼性ポート番号

この設定は、受信セッションの信頼性接続に使用するTCPポート番号を指定します。

デフォルトでは、ポート番号は2598に設定されています。

セッションの信頼性タイムアウト

この設定は、セッションの信頼性プロキシがユーザーの再接続を待機し、セッションが切断されるまでの時間を秒単位で指定します。

セッションが開いている時間を延長することはできますが、この機能は利便性のためであり、ユーザーに再認証を促すものではありません。セッションが開いている時間が長くなるほど、ユーザーがデバイスを放置し、不正なユーザーがアクセスする可能性が高まります。

デフォルトでは、タイムアウトは180秒（3分）に設定されています。

セッションウォーターマークポリシー設定

セッションウォーターマークセクションには、この機能を構成するためのポリシー設定が含まれています。 この機能を有効にすると、VDAマシンのネットワーク帯域幅とCPU使用率が大幅に増

加します。利用可能なハードウェアリソースに基づいて、選択したVDAマシンにセッションウォーターマークを構成することをお勧めします。

重要

他のウォーターマークポリシー設定を有効にするには、セッションウォーターマークを有効にします。より良いユーザーエクスペリエンスを実現するために、2つを超えるウォーターマークテキスト項目を有効にしないでください。

セッションウォーターマークを有効にする

この設定を有効にすると、セッションディスプレイには、セッション固有の情報を表示する不透明なテキストウォーターマークが表示されます。他のウォーターマーク設定は、この設定が有効になっているかどうかに依存します。

デフォルトでは、セッションウォーターマークは無効になっています。

クライアントIPアドレスを含める

この設定を有効にすると、セッションは現在のクライアントIPアドレスをウォーターマークとして表示します。

デフォルトでは、クライアントIPアドレスを含めるは無効になっています。

接続時間を含める

この設定を有効にすると、セッションウォーターマークに接続時間が表示されます。形式はyyyy/mm/dd hh:mmです。表示される時刻は、システムクロックとタイムゾーンに基づいています。

デフォルトでは、接続時間を含めるは無効になっています。

ログオンユーザー名を含める

この設定を有効にすると、セッションは現在のログオンユーザー名をウォーターマークとして表示します。表示形式はUSERNAME@DOMAINNAMEです。ユーザー名は最大20文字にすることをお勧めします。ユーザー名が20文字を超えると、文字フォントが過度に小さくなったり、切り捨てられたりして、ウォーターマークの効果が低下する可能性があります。

デフォルトでは、ログオンユーザー名を含めるは有効になっています。

VDAホスト名を含める

この設定を有効にすると、セッションは現在のICA®セッションのVDAホスト名をウォーターマークとして表示します。

デフォルトでは、VDAホスト名を含める設定が有効になっています。

VDA IPアドレスを含める

この設定を有効にすると、セッションは現在のICAセッションのVDA IPアドレスをウォーターマークとして表示します。

デフォルトでは、VDA IPアドレスは無効になっています。

セッションウォーターマークのスタイル

この設定は、単一のウォーターマークテキストラベルを表示するか、複数のラベルを表示するかを制御します。「**値**」ドロップダウンメニューから「**複数**」または「**単一**」を選択します。

「**複数**」は、セッションに5つのウォーターマークラベルを表示します。中央に1つ、四隅に4つです。

「**単一**」は、セッションの中央に単一のウォーターマークラベルを表示します。

デフォルトでは、セッションウォーターマークスタイルは「複数」です。

ウォーターマークのカスタムテキスト

この設定を使用すると、カスタムテキスト（たとえば、会社名）をセッションウォーターマークに表示できます。空でない文字列を設定すると、ウォーターマークで有効になっている他の情報に加えて、新しい行にテキストが表示されます。ウォーターマークのカスタムテキストは25 Unicode文字に制限されています。より長い文字列を設定した場合、25文字に切り詰められます。

デフォルトのテキストはありません。

Citrix Virtual Apps and Desktops™ 7 2206以降、テキストにカスタムタグを使用してさらにカスタマイズを追加できます。その結果、カスタムテキストの最大文字数は1024に増加しました。

ウォーターマーク設定で利用可能なタグは、次の表に記載されています。

タグ	説明	例
`<font=value>`	ウォーターマークテキストのフォントを変更できます。値は、VDAで利用可能なフォントの名前です。	`<font=Courier New>`
`<fontzoom=value>`	フォントのズーム率を設定できます。ウォーターマークテ	`<fontzoom=200>`

タグ	説明	例
	キストの200%ズームの場合、値は200です。	
`<position=value>`	ウォーターマークテキストの位置を変更できます。値は `center`、`topleft`、`topright`、`bottomleft`、および `bottomright` です。このタグはシングルスタイルでのみ適用可能です。	`<position=topright>`
`<rotation=value>`	ウォーターマークテキストを回転できます。値は度数で指定され、範囲は-360から360です。	`<rotation=45>`
`<style=value>`	表示スタイルを変更できます。このタグはセッションウォーターマークスタイルポリシーを上書きします。	`<style=single>`

利用可能なウォーターマークスタイルは次のとおりです。

- シングルスタイル - セッションの中央に単一のウォーターマークテキストラベルが表示されます。位置タグを使用して場所を変更できます。
- xスタイルまたは複数 - セッションに5つのウォーターマークラベルが表示されます。中央に1つ、各コーナーに1つずつです。
- タイル - セッションに複数のラベルが表示されます。ウォーターマークテキストは画面全体に均等に配置されます。

ウォーターマークテキストを変更するために利用可能なタグは、次の表に記載されています。

タグ	説明
`<clientip>`	エンドポイントのIPアドレス。
`<date>`	セッションが確立された日付。
`<domain>`	ログインしているユーザーアカウントのドメイン名。

タグ	説明
`<hostname>`	VDAのマシン名。
`<newline>`	追加の行を作成します。
`<serverip>`	VDAのIPアドレス。
`<time>`	セッションが確立された時刻。
`<username>`	ユーザーの名前。

注:

- **ウォーターマークカスタムテキスト**ポリシーは、**セッションウォーターマークを有効にする**ポリシーが有効になっている場合にのみ適用されます。デフォルト値は*無効*です。
- ウォーターマークテキストを変更するためにタグを使用する場合、**セッションウォーターマークを有効にする**を除く他のすべてのセッションウォーターマークポリシーは無視されます。ウォーターマークテキスト設定にタグを使用する場合、他のすべてのウォーターマークポリシーを使用できます。

透かしの透明度

ウォーターマークの不透明度を0から100まで指定できます。指定する値が大きいほど、ウォーターマークは不透明になります。

デフォルトでは、値は17です。

タイムゾーン制御ポリシー設定

タイムゾーン制御セクションには、セッションでのローカル時間の使用に関連するポリシー設定が含まれています。

レガシークライアントのローカル時間を推定する

この設定は、ユーザーデバイスのローカルタイムゾーンの推定を有効または無効にします。これらのデバイスには、サーバーに不正確なタイムゾーン情報を送信するユーザーデバイスが含まれます。

デフォルトでは、サーバーは必要に応じてローカルタイムゾーンを推定します。

この設定は、サーバーに詳細なタイムゾーン情報を送信しないレガシーなCitrix ReceiverまたはICAクライアントでの使用を目的としています。この設定が、サーバーに詳細なタイムゾーン情報を送信するCitrix Receiver（例: Windows版Citrix Receiver™のサポート対象バージョン）で使用される場合を考慮してください。この場合、この設定は効果がありません。

セッション切断またはログオフ時にデスクトップOSのタイムゾーンを復元する

ユーザーがセッションを切断またはログオフした場合を考慮してください。この場合、この設定は、シングルセッションOS VDAのタイムゾーン設定がマシンの元のタイムゾーンに復元されるかどうかを決定します。この設定を有効にすると、ユーザーが切断またはログオフしたときに、VDAはマシンのタイムゾーンを元の設定に復元します。この設定を有効にするには、**クライアントのローカル時間を使用**を**クライアントのタイムゾーンを使用**に設定します。

デフォルトでは、この設定は有効になっています。

クライアントのローカル時間を使用

この設定は、ユーザーセッションのタイムゾーン設定を決定します。選択肢は、セッションホストのタイムゾーン（サーバータイムゾーン）またはユーザーデバイスのタイムゾーン（クライアントタイムゾーン）です。

デフォルトでは、セッションホストのタイムゾーンが使用されます。

この設定を**マルチセッション**セッションホストで有効にするには、グループポリシーエディターで**タイムゾーンのリダイレクトを許可**設定を有効にします。この設定は、**ローカルコンピューターポリシー** > **コンピューターの構成** > **管理用テンプレート** > **Windowsコンポーネント** > **リモートデスクトップサービス** > **リモートデスクトップセッションホスト** > **デバイスとリソースのリダイレクト**にあります。

> **重要:**
>
> シングルセッションVDAを使用する場合、VDAのインストール中に**Citrix Portica Timezone Service (CtxPicaTzSvc)がタイムゾーンの変更**ユーザー権利の割り当てポリシーに自動的に追加されます。これらのポリシーからユーザーまたはプロセスを削除するポリシーやプロセスがある場合は、Citrixサービスが削除されないようにそれらを変更してください。そうしないと、タイムゾーンのリダイレクトは機能しません。

TWAINデバイスのポリシー設定

TWAINデバイスセクションには、以下のポリシー設定が含まれています。

- デジタルカメラやスキャナーなどのクライアントTWAINデバイスのマッピング
- サーバーからクライアントへの画像転送の最適化

> **注:**
>
> Citrix Receiver for Windows 4.5では、TWAIN 2.0がサポートされています。

クライアントTWAINデバイスのリダイレクト

TWAINデバイスは、TWAINプロトコルを使用して、サーバーでホストされている画像処理アプリケーションと通信します。

この設定は、ユーザーがユーザーデバイス上のTWAINデバイスにアクセスすることを許可または禁止します。デフォルトでは、TWAINデバイスのリダイレクトは許可されています。

関連するポリシー設定は次のとおりです。

- TWAIN圧縮レベル
- TWAINデバイスのリダイレクト帯域幅制限
- TWAINデバイスリダイレクト帯域幅制限の割合

TWAIN圧縮レベル

この設定は、クライアントからサーバーへの画像転送の圧縮レベルを指定します。最良の画質には「低」、良好な画質には「中」、低い画質には「高」を使用します。デフォルトでは、中程度の圧縮が適用されます。

USBデバイスポリシー設定

USBデバイスセクションには、USBデバイスのファイルリダイレクトを管理するためのポリシー設定が含まれています。

クライアントUSBデバイス最適化ルール

クライアントUSBデバイス最適化ルールは、最適化を無効にするか、最適化モードを変更するためにデバイスに適用できます。

ユーザーがUSB入力デバイスを接続すると、ホストは**USBポリシー**設定がそのデバイスを許可するかどうかを確認します。デバイスが許可されている場合、ホストはデバイスの**クライアントUSBデバイス最適化ルール**を確認します。ルールが指定されていない場合、デバイスは最適化されません。キャプチャモード (04) は、署名デバイスに推奨されるモードです。高遅延によってパ

フォーマンスが低下する他のデバイスの場合、管理者はインタラクティブモード (02) を有効にできます。この記事の表で利用可能なモードの説明を参照してください。

知っておくとよいこと

- Wacomの署名パッドおよびタブレットを使用する場合は、スクリーンセーバーを無効にすることをお勧めします。スクリーンセーバーを無効にする手順は、このセクションの最後にあります。
- Wacom STU署名パッドおよびタブレットシリーズ製品の最適化のサポートは、Citrix Virtual Apps and Desktops™ポリシーのインストール時に事前設定されています。
- 署名デバイスはCitrix Virtual Apps and Desktops全体で動作し、署名デバイスとして使用するためにドライバーを必要としません。Wacomには、デバイスをさらにカスタマイズするためにインストールできる追加のソフトウェアがあります。`<http://www.wacom.com/>`を参照してください。
- 描画タブレット。特定の描画入力デバイスは、PCI/ACPIバス上でHIDデバイスとして表示される場合があり、サポートされていません。これらのデバイスは、Citrix Virtual Desktopsセッション内でリダイレクトされるように、クライアント上のUSBホストコントローラーに接続してください。

ポリシールールは、空白で区切られたtag=value形式の式を取ります。以下のタグがサポートされています。

タグ名	説明
モード	最適化モードは、class=**03**の入力デバイスでサポートされています。サポートされているモードは次のとおりです。最適化なし - 値**01**。インタラクティブモード - 値**02**。ペンタブレットや3D Proマウスなどのデバイスに推奨されます。キャプチャモード - 値**04**。署名パッドなどのデバイスに推奨されます。
VID	デバイス記述子からのベンダーID（4桁の16進数）。
PID	デバイス記述子からの製品ID（4桁の16進数）。
REV	デバイス記述子からのリビジョンID（4桁の16進数）。

タグ名	説明
クラス	デバイス記述子またはインターフェース記述子のいずれかからのクラス。
サブクラス	デバイス記述子またはインターフェース記述子のいずれかからのサブクラス。
保護	デバイス記述子またはインターフェース記述子のいずれかからのプロトコル。

例

Mode=00000004 VID=067B PID=1230 class=03 #キャプチャモードで動作する入力デバイス

Mode=00000002 VID=067B PID=1230 class=03 #インタラクティブモードで動作する入力デバイス（デフォルト）

Mode=00000001 VID=067B PID=1230 class=03 #最適化なしで動作する入力デバイス

Mode=00000100 VID=067B PID=1230 #デバイスセットアップの最適化が無効（デフォルト）

Mode=00000200 VID=067B PID=1230 #デバイスセットアップの最適化が有効

Wacom署名パッドデバイスのスクリーンセーバーを無効にする

Wacom署名パッドおよびタブレットを使用するには、Citrix®はスクリーンセーバーを次のように無効にすることをお勧めします。

1. デバイスをリダイレクトした後、**Wacom-STU-Driver**をインストールします。
2. 署名パッドのコントロールパネルにアクセスするには、**Wacom-STU-Display MSI**をインストールします。
3. **コントロールパネル > Wacom STU Display > STU430** または **STU530** に移動し、お使いのモデルのタブを選択します。
4. 「**変更**」を選択し、UACセキュリティウィンドウが表示されたら「**はい**」を選択します。
5. 「**スライドショーを無効にする**」を選択し、「**適用**」を選択します。

1つの署名パッドモデルに対して設定が行われると、その設定はすべてのモデルに適用されます。

クライアントUSBデバイスのリダイレクト

この設定は、USBデバイスのユーザーデバイスとの間のリダイレクトを許可または禁止します。

デフォルトでは、USBデバイスはリダイレクトされません。

クライアントUSBデバイスリダイレクト規則

この設定は、USBデバイスのリダイレクトルールを指定します。

デフォルトでは、ルールは指定されていません。

ユーザーがUSBデバイスを接続すると、ホストデバイスは一致が見つかるまで各ポリシー規則と照合して確認します。いずれかのデバイスに対する最初の一致が最終的なものと見なされます。最初の一致が許可ルールである場合、そのデバイスは仮想デスクトップにリモート接続されます。最初の一致が拒否ルールである場合、そのデバイスはローカルデスクトップでのみ利用可能です。一致が見つからない場合、デフォルトのルールが使用されます。

ポリシー規則は{Allow:|Deny:}の形式をとり、その後に空白で区切られたtag=value式のセットが続きます。次のタグがサポートされています。

タグ名	説明
VID	デバイス記述子からのベンダーID
PID	デバイス記述子からの製品ID
REL	デバイス記述子からのリリースID
クラス	デバイス記述子またはインターフェイス記述子のいずれかからのクラス
サブクラス	デバイス記述子またはインターフェース記述子のいずれかからのサブクラス
プロトコル	デバイス記述子またはインターフェイス記述子のいずれかからのプロトコル

ポリシー規則を作成する際は、次の点に注意してください。

- 規則では大文字と小文字は区別されません。
- 規則の末尾にはオプションのコメントを付けることができます。コメントは#で始まります。
- 空行と純粋なコメント行は無視されます。
- タグは一致演算子 = を使用する必要があります (例: VID=067B_。
- 各ルールは新しい行で開始するか、セミコロンで区切られたリストの一部である必要があります。

- USB Implementers Forum, Inc. の Web サイトで入手可能な USB クラスコードを参照してください。

管理者定義の USB ポリシールールの例:

- 許可: VID=067B PID=0007 # 別の産業、別のフラッシュドライブ
- 拒否: Class=08 subclass=05 # マスストレージ
- すべての USB デバイスを拒否するルールを作成するには、他のタグなしで「DENY:」を使用します。

クライアント USB プラグアンドプレイデバイスのリダイレクト

この設定により、カメラや販売時点情報管理 (POS) デバイスなどのプラグアンドプレイデバイスをクライアントセッションで使用することを許可または禁止します。

デフォルトでは、プラグアンドプレイデバイスのリダイレクトは許可されています。「許可」に設定すると、特定のユーザーまたはグループのすべてのプラグアンドプレイデバイスがリダイレクトされます。「禁止」に設定すると、デバイスはリダイレクトされません。

USB デバイスの自動リダイレクトを構成する

USB サポートが有効になっている場合、USB デバイスは自動的にリダイレクトされます。また、USB ユーザー設定は USB デバイスを自動的に接続するように設定されています。

> **注:**

> Receiver for Windows 4.2 では、デスクトップアプライアンスモードで動作している場合も USB デバイスは自動的にリダイレクトされます。また、接続バーは表示されません。以前のバージョンの Citrix Receiver for Windows では、USB デバイスは以下のモードで動作している場合も自動的にリダイレクトされます。

> - デスクトップアプライアンスモード
> - 仮想マシン (VM) ホスト型アプリケーション

> すべてのUSBデバイスをリダイレクトすることが常に最適であるとは限りません。ユーザーは、自動的にリダイレクトされないUSBデバイスリストからデバイスを明示的にリダイレクトできます。USBデバイスがリストに表示されたり、リダイレクトされたりするのを防ぐに

は、クライアントエンドポイントまたはDDCポリシーのいずれかでDeviceRulesを使用します。詳細については、管理者ガイドを参照してください。

注意:

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

USBデバイスの自動リダイレクトに関するユーザー設定

ポリシー:

1. **ローカルグループポリシーエディター**を開き、**管理用テンプレート > Citrixコンポーネント > Citrix Receiver™ > クライアントデバイスのリモート処理 > 汎用USBリモーティング**に移動します。
2. **新しいUSBデバイス**を開き、**有効**を選択し、**OK**をクリックします。
3. **既存のUSBデバイス**を開き、**有効**を選択し、**OK**をクリックします。

シトリックス レシーバー:

1. **Citrix Receiverの環境設定 > 接続**に移動します。
2. 以下に示すオプションが選択されていることを確認します。
   - セッションの開始時に、デバイスを自動的に接続する
   - セッションの実行中に新しいデバイスが接続された場合、デバイスを自動的に接続する。
3. **OK**をクリックします。

すべてのレジストリキーとポリシーの変更は、Windowsクライアントデバイスに適用されます。

通常のUSBプリンターのリダイレクト

通常のUSBプリンターに最適なソリューションは、専用のユニバーサルプリンタードライバーと仮想チャネルを使用して印刷を実行することです。デフォルトでは、通常のUSBプリンターは自動的にリダイレクトされません。

通常のプリンターはヒューリスティックを使用して検出されます。また、例えばスキャン機能を備えた高度なプリンターは、完全に機能させるにはUSBサポートを使用してリダイレクトする必要がある場合があります。

通常のプリンターが自動的にリダイレクトされるかどうかを構成するには、このレジストリを使用します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectPrinters

種類: DWORD

データ: 00000000

デフォルト値は0です（自動的にリダイレクトしません）。値を0より大きい任意の数値に変更すると、通常のUSBプリンターをリダイレクトするためのUSBサポートが有効になります。

Active Directoryポリシーをこのレジストリキーに展開し、両方が存在する場合は非ポリシー値を上書きすることもできます。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectPrinters

種類: DWORD

データ: 00000000

通常のオーディオデバイスのリダイレクト

通常のプリンターと同様に、通常のオーディオデバイスからオーディオデータを送信するには、ICA®の専用オーディオ仮想チャネルを使用することで最高のユーザーエクスペリエンスが実現されます。ただし、一部の特殊なデバイスはUSBサポートを使用してリダイレクトする必要がある場合があります。どのデバイスが通常のオーディオデバイスであるかを判断するためにヒューリスティックが使用されます。

通常のオーディオデバイスが自動的にリダイレクトされるかどうかを構成するには、クライアントエンドポイントでこのレジストリを使用します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectAudio

種類: DWORD

データ: 00000000

デフォルトは0に設定されています (自動的にリダイレクトしません)。値を0以外に変更すると、USBサポート付きのプレーンなUSBオーディオデバイスがリダイレクトされます。

Active Directoryポリシーを使用して、この値をレジストリキーに展開し、両方が存在する場合は非ポリシー値を上書きできます。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectAudio

種類: DWORD

データ: 00000000

プレーンなストレージデバイス (マスストレージデバイス) のリダイレクト

プレーンなストレージデバイスの場合、最適化も行うクライアントドライブマッピングなど、専用の仮想チャネルを使用することで、最高のユーザーエクスペリエンスを実現できます。ファイルの単純な読み書きに加えて、CD/DVDの書き込みや暗号化されたファイルシステムデバイスへのアクセスなど、特定の特殊なタスクを実行するには、ジェネリックUSBサポートを使用してデバイスをリダイレクトする必要がある場合があります。

どのデバイスがプレーンなストレージデバイスであるかを判断するために、ヒューリスティックが使用されます。プレーンなストレージデバイスを自動的にリダイレクトするかどうかを設定するには、このレジストリキーを使用します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectStorage

種類: DWORD

データ: 00000000

デフォルトは0に設定されています (自動的にリダイレクトしません)。値を0以外に変更すると、ジェネリックUSBサポートを使用してプレーンなUSBストレージデバイスがリダイレクトされます。

Active Directoryポリシーを使用して、この値を以下のレジストリキーに展開し、両方が存在する場合は非ポリシー値を上書きすることもできます。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectStorage

種類: DWORD

データ: 00000000

> **注:**
>
> 汎用USBサポートを使用している場合、プレーンストレージデバイスへの読み取り専用アクセスは構成できませんが、CDMを使用している場合は構成できます。

ハードウェア暗号化機能付きUSBフラッシュドライブのリダイレクト

ハードウェア暗号化機能付きUSBフラッシュドライブは、通常、暗号化されたストレージパーティションと、暗号化されたパーティションをロック解除するためのユーティリティが含まれる2番目のユーティリティパーティションで構成されています。USBフラッシュドライブデバイスの場合、最適化も実行する専用のクライアントドライブマッピング/動的サムドライブマッピングHDX仮想チャネルを使用することで、最高のユーザーエクスペリエンスを実現できます。

汎用USBリダイレクトは、以下の場合に必要です。

- Windows以外のクライアント (例: Linuxクライアント)
- 顧客がクライアント上のローカル機能へのユーザーアクセスを制限 (ロックダウン) しているクライアント

汎用USBリダイレクトは、ハードウェア暗号化なしで任意のUSBストレージデバイスをシングルセッションOSおよびマルチセッションOS VDAセッションの両方にリダイレクトできます。

Citrix Virtual Apps and Desktops™ 7 1808より前は、ハードウェア暗号化機能付きUSBフラッシュドライブをシングルセッションOSまたはマルチセッションOS VDAセッションに実用的な方法でリダイレクトできませんでした。Citrix Virtual Apps and Desktops 7 1808で導入された新機能強化により、ハードウェア暗号化機能付きUSBフラッシュドライブの汎用USBリダイレクトがシングルセッションOSおよびマルチセッションOS VDAセッションにサポートされます。 デバイスがリダイレクトされた後、そのドライブはローカルクライアントに表示されません。したがって、ドライブのロック解除が必要な場合は、セッション内で実行してください。この機能にはWindows Update KB4074590が必要です。

プレーン静止画デバイス (スキャナーおよびデジタルカメラ)

プレーン静止画デバイスの場合、最適化も実行する専用の仮想チャネル (TWAIN仮想チャネルなど) を使用することで、最高のユーザーエクスペリエンスを実現できます。これらのデバイスは業

界標準に準拠している必要があります。デバイスが非準拠であるか、元の意図に従って使用されていないと見なされる場合、汎用USBリダイレクトがデバイスを使用する唯一の方法となる可能性があります。どのデバイスがプレーン静止画デバイスであるかを判断するためにヒューリスティックが使用されます。

このレジストリキーを使用して、プレーン静止画デバイスが自動的にリダイレクトされるかどうかを構成します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectImage

種類: DWORD

データ: 00000000

デフォルトは0に設定されています（自動的にリダイレクトされません）。値を0以外に変更すると、汎用USBのプレーンなUSB静止画デバイスがリダイレクトされます。

Active Directoryポリシーを使用して、この値をこのレジストリキーに展開することもでき、両方が存在する場合は非ポリシー値を上書きします。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectImage

種類: DWORD

データ: 00000000

デバイス固有の設定

Citrix最適化可能デバイスを選択するために使用されるヒューリスティックは、必ずしもユーザーの希望と一致するとは限りません。Citrix最適化可能デバイスの例としては、プリンター、オーディオ、ビデオ、ストレージ、静止画デバイスなどがあります。上記にリストされていないデバイスの自動リダイレクトを制御したい場合があります。デバイス固有の基準で自動リダイレクトを制御できます。

例として、DemoTech 2,000バーコードリーダーはUSBサポートを使用してリダイレクトする必要はありません。ベンダー識別子は12AB、製品識別子は5678です。これらの16進数はデバイスマネージャーで確認できます。

これが自動的にリダイレクトされるのを防ぐには、このデバイス固有のレジストリキーを作成します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

名前: AutoRedirect

種類: DWORD

データ: 00000000

値が0の場合、デバイスは自動的にリダイレクトされません。0以外の値は、デバイスが自動リダイレクトの対象となることを示します（ユーザー設定による）。ベンダー識別子と製品識別子の間には単一のスペース文字があります。

Active Directoryポリシーを使用して、この値をこのレジストリキーに展開することもできます。両方が存在する場合、非ポリシー値を上書きします。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

名前: AutoRedirect

種類: DWORD

データ: 00000000

デバイス固有のAutoRedirect設定は、上記で説明したより一般的なAutoRedirectXXX値よりも優先されます。Citrix最適化デバイスのデフォルトのヒューリスティックは、デバイスを汎用として誤って解釈する可能性があります。したがって、デバイス固有のAutoRedirect値を1に設定して、自動的にリダイレクトします。

既存のUSBデバイスの自動接続を許可する

この設定は、セッション開始時にエンドポイントに接続されている既存のUSBデバイスをリモートセッションに自動接続することを許可または防止します。

この設定をポリシーに追加するときは、次のいずれかのオプションを選択します。

- 利用可能なUSBデバイスをリダイレクトする前に確認する。
- 利用可能なUSBデバイスを自動的にリダイレクトしない。
- 利用可能なUSBデバイスを自動的にリダイレクトする。

デフォルトでは、**利用可能なUSBデバイスをリダイレクトする前に確認する**オプションが選択されています。選択されたポリシーに基づいて、クライアントの**環境設定** > **デバイス**セクションで選択されたオプションを上書きできます。

> **注:**
>
> 現在、**既存のUSBデバイスの自動接続を許可する**ポリシーは、Citrix Workspace™ app for Windowsにのみ適用されます。

新しく接続されたUSBデバイスの自動接続を許可する

この設定は、セッション中にエンドポイントに挿入されたUSBデバイスをリモートセッションに自動接続することを許可または防止します。

この設定をポリシーに追加するときは、次のいずれかのオプションを選択します。

- 利用可能なUSBデバイスをリダイレクトする前に確認する。
- 利用可能なUSBデバイスを自動的にリダイレクトしない。
- 利用可能なUSBデバイスを自動的にリダイレクトします。

デフォルトでは、**利用可能なUSBデバイスをリダイレクトする前に確認する**オプションが選択されています。選択されたポリシーに基づいて、クライアントの**基本設定** > **デバイス**セクションで選択されたオプションが上書きされる場合があります。

> **注:**
>
> 現在、**新しく接続されたUSBデバイスの自動接続を許可する**ポリシーは、Citrix Workspace アプリ for Windowsにのみ適用されます。

クライアントUSBデバイスリダイレクト規則 (バージョン2)

この設定は、USBデバイスをリモートセッションにフィルタリング、分割、および自動接続するためのルールを指定します。

この設定が選択されている場合、ホストは*クライアントUSBデバイスリダイレクトルール*設定を、この設定で構成されたデバイスルールで上書きします。

詳しくは、「複合USBデバイスリダイレクトの構成」を参照してください。

仮想チャネル許可リストポリシー設定

仮想チャネル許可リストポリシー設定は、ICA®セッションで開くことが許可されている仮想チャネルを指定する許可リストの使用を有効にします。

無効にすると、すべての仮想チャネルが許可されます。

有効にすると、Citrix®仮想チャネルのみが許可されます。

カスタムまたはサードパーティの仮想チャネルを使用するには、仮想チャネルをリストに追加します。仮想チャネルをリストに追加するには：

1. 仮想チャネル名の後にコンマを入力します。
2. 仮想チャネルにアクセスするプロセスのパスを入力します。

複数の実行可能パスをリストでき、パスはコンマで区切られます。

例:

```
CTXCVC1,C:\VC1\vchost.exe
```

```
CTXCVC2,C:\VC2\vchost.exe,C:\Program Files\Third Party\vcaccess.exe
```

Citrix Virtual Apps and Desktops 7 2109以降、仮想チャネル許可リストはデフォルトで有効になっています。許可リストに仮想チャネルを追加する方法の詳細については、「許可リストへの仮想チャネルの追加」を参照してください。

Skype for Business 用の HDX RealTime Optimization Pack を使用している場合は、仮想チャネルを許可リストに追加します。詳細については、「HDX RealTime Optimization Pack のドキュメント」を参照してください。

> **重要:**
>
> 設定を有効にするには、VDAマシンを再起動する必要があります。
>
> 仮想チャネルの詳細については、「ICA仮想チャネル」を参照してください。

仮想チャネル許可リストのログ記録

このポリシー設定を使用して、仮想チャネル許可リストのログ記録レベルを構成できます。

次のオプションが利用可能です。

オプション	説明
無効	すべてのログイベントを無効にします。

警告のみをログに記録	許可リストに含まれていない、開こうとするカスタム仮想チャネルに対してのみイベントがログに記録されます。
すべてのイベントをログに記録	すべてのイベントがログに記録されます

仮想チャネル許可リストのログスロットリング

このポリシー設定を使用して、アクティブなセッションのイベントログ記録の頻度を構成できます。

各仮想チャネルのすべてのイベントは、最初に発生したときにログに記録されます。セッションがアクティブな間、スロットリング期間中は繰り返し発生するイベントは抑制されます。セッションが切断された場合、スロットリング期間はリセットされます。

DVCの仮想チャネル許可リスト

ICAセッションで開くことを許可されている動的仮想チャネルを指定する許可リストの使用を有効にします。

無効にすると、すべての動的仮想チャネルが許可されます。

有効にすると、動的仮想チャネルは許可されません。この機能で動的仮想チャネル (DVC) を使用するには、DVCをリストに追加する必要があります。リストにDVCを追加するには、セッションホストでDVCにアクセスするプロセスのパスを入力し、その後にコンマ、次にクライアント側プラグイン名、その後にコンマ、そしてプラグインが使用するリスナー名を入力します。複数のリスナー名はコンマで区切って追加できます。

ワイルドカードを使用して、プラグインがサポートするすべてのリスナーを許可できます。

ワイルドカードを使用して、プロセスパス内の単一のディレクトリ名を置き換えたり、プロセスパス内のディレクトリ名の一部を置き換えたり、実行可能ファイル名を置き換えたり、実行可能ファイル名の一部を置き換えたりすることもできます。

この設定への変更は、セッションホストを再起動した後にのみ適用されます。

例: クライアント側プラグイン: `DvcPlugin1.dll`, `DvcPlugin2.dll`, `DvcPlugin3.dll`

許可リストエントリ: `C:\Program Files\App\run1.2.exe,DvcPlugin1,` ListenerName1 `C:\Program Files*\run*.exe,DvcPlugin2,ListenerName1,ListenerName2` `C:\Program Files\App\run1.2.exe,DvcPlugin3,*`

視覚表示ポリシー設定

視覚表示セクションには、仮想デスクトップからユーザーデバイスに送信される画像の品質を制御するためのポリシー設定が含まれています。

シンプルなグラフィックの優先色深度

このポリシー設定は、VDAバージョン7.6 FP3以降で利用可能です。8ビットオプションは、VDAバージョン7.12以降で利用可能です。

この設定により、シンプルなグラフィックがネットワーク経由で送信される際の色深度を下げることができます。ピクセルあたり8ビットまたは16ビットに下げることで、低帯域幅接続での応答性が向上する可能性があります。ただし、この操作は画質のわずかな劣化を招く可能性があります。(/ja-jp/citrix-virtual-apps-desktops/current-release/policies/reference/ica-policy-settings/graphics-policy-settings.html)ポリシー設定が**画面全体**に設定されている場合、8ビットの色深度はサポートされません。

デフォルトの優先色深度はピクセルあたり24ビットです。

8ビット設定がVDAバージョン7.11以前に適用された場合、VDAは24ビット（デフォルト）の色深度にフォールバックします。

ターゲットフレームレート

この設定は、仮想デスクトップからユーザーデバイスに送信される1秒あたりの最大フレーム数を指定します。

デフォルトでは、最大は1秒あたり30フレームです。

1秒あたりのフレーム数を高く設定する（例：30）と、ユーザーエクスペリエンスは向上しますが、より多くの帯域幅が必要になります。1秒あたりのフレーム数を減らす（例：10）と、ユーザーエクスペリエンスを犠牲にしてサーバーのスケーラビリティが最大化されます。CPUが遅いユーザーデバイスの場合、ユーザーエクスペリエンスを向上させるために低い値を指定してください。

1秒あたりの最大サポートフレームレートは60です。

視覚品質

この設定は、ユーザーデバイスに表示される画像の希望する視覚品質を指定します。

デフォルトでは、この設定は「中」です。

画像の品質を指定するには、次のいずれかのオプションを選択します。

- **低** - 帯域幅が制限されたネットワークで、対話性のために視覚的な品質を犠牲にできる場合に推奨されます。
- **中** - ほとんどのユースケースで最高のパフォーマンスと帯域幅効率を提供します。
- **高** - 視覚的にロスレスな画質が必要な場合に推奨されます。
- **ロスレスにビルド** - ネットワークアクティビティが高い期間はロッシー画像をユーザーデバイスに送信し、ネットワークアクティビティが低下した後はロスレス画像を送信します。この設定により、帯域幅が制限されたネットワーク接続でのパフォーマンスが向上します。
- **常にロスレス** - 画像データの保持が不可欠な場合は、「**常にロスレス**」を選択して、ロッシーデータがユーザーデバイスに送信されないようにします。たとえば、画質の低下が許されないX線画像を表示する場合などです。

動きのある画像ポリシー設定

動きのある画像セクションには、動的な画像の圧縮を削除または変更できる設定が含まれています。

最小画像品質

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、アダプティブディスプレイの許容される最小画像品質を指定します。圧縮が少ないほど、表示される画像の品質は高くなります。超高、非常に高、高、標準、低のいずれかの圧縮を選択します。

デフォルトでは、これは標準に設定されています。

動きのある画像の圧縮

この設定は、アダプティブディスプレイが有効になっているかどうかを指定します。アダプティブディスプレイは、利用可能な帯域幅に基づいて、スライドショー内のビデオやトランジションスライドの画像品質を自動的に調整します。アダプティブディスプレイが有効になっている場合、ユーザーは品質の低下なしにスムーズなプレゼンテーションを見ることができます。

デフォルトでは、アダプティブディスプレイは有効になっています。

VDAバージョン7.0から7.6の場合、この設定はレガシーグラフィックモードが有効になっている場合にのみ適用されます。VDAバージョン7.6 FP1以降の場合、この設定はレガシーグラフィックモードが有効になっている場合、またはレガシーグラフィックモードが無効でビデオコーデックがグラフィックの圧縮に使用されていない場合に適用されます。

レガシーグラフィックモードが有効になっている場合、ポリシーの変更を有効にするにはセッションを再起動する必要があります。アダプティブディスプレイはプログレッシブディスプレイと

相互排他的です。アダプティブディスプレイを有効にするとプログレッシブディスプレイが無効になり、その逆も同様です。ただし、プログレッシブディスプレイとアダプティブディスプレイの両方を同時に無効にすることができます。プログレッシブディスプレイはレガシー機能であるため、XenAppまたはXenDesktopでは推奨されません。プログレッシブしきい値レベルを設定すると、アダプティブディスプレイが無効になります。

プログレッシブ圧縮レベル

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、詳細度は低いものの、より高速な画像の初期表示を提供します。

デフォルトでは、プログレッシブ圧縮は適用されません。

通常の非可逆圧縮設定で定義された、より詳細な画像は、利用可能になったときに表示されます。写真などの帯域幅を多く消費するグラフィックの表示を改善するには、非常に高または超高圧縮を使用します。

プログレッシブ圧縮を有効にするには、その圧縮レベルが「ロッシー圧縮レベル」設定よりも高くする必要があります。

注：プログレッシブ圧縮に関連する圧縮レベルの増加は、クライアント接続を介した動的画像の対話性も向上させます。回転する3Dモデルなどの動的画像の品質は、画像が動きを停止するまで一時的に低下し、その時点で通常のロッシー圧縮設定が適用されます。

関連するポリシー設定は次のとおりです。

- プログレッシブ圧縮しきい値
- プログレッシブヘビーウェイト圧縮

プログレッシブ圧縮しきい値

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、プログレッシブ圧縮が適用される接続の最大帯域幅を1秒あたりのキロビットで表します。これは、この帯域幅以下のクライアント接続にのみ適用されます。

デフォルトでは、しきい値は1秒あたり2147483647キロビットです。

関連するポリシー設定は次のとおりです。

- プログレッシブ圧縮しきい値

- プログレッシブヘビーウェイト圧縮

目標最小フレームレート

この設定は、低帯域幅の条件下で、動的画像に対してシステムが維持しようとする1秒あたりの最小フレームレートを指定します。

デフォルトでは、これは10fpsに設定されています。

VDAバージョン7.0から7.6の場合、この設定はレガシーグラフィックモードが有効になっている場合にのみ適用されます。VDAバージョン7.6 FP1以降の場合、この設定はレガシーグラフィックモードが無効または有効になっている場合に適用されます。

> **注:**
>
> 目標最小フレームレートポリシーは非推奨となり、10 fpsに設定されています。これは、グラフィックステータスインジケーターの品質スライダーを使用してエンドユーザーが変更できます。

静止画像ポリシー設定

静止画像セクションには、静止画像の圧縮を削除または変更できる設定が含まれています。

追加の色圧縮

この設定は、帯域幅が制限されているクライアント接続を介して配信される画像に対する追加の色圧縮の使用を有効または無効にし、表示される画像の品質を低下させることで応答性を向上させます。

デフォルトでは、追加の色圧縮は無効になっています。

有効にすると、追加の色圧縮は、クライアント接続の帯域幅が「追加の色圧縮しきい値」を下回っている場合にのみ適用されます。クライアント接続の帯域幅がしきい値を超えている場合、または「無効」が選択されている場合、追加の色圧縮は適用されません。

追加の色圧縮しきい値

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、追加の色圧縮が適用される接続の最大帯域幅をキロビット/秒で表します。クライアント接続の帯域幅が設定値を下回ると、有効になっている場合、追加の色圧縮が適用されます。

デフォルトでは、しきい値は8192キロビット/秒です。

ヘビーウェイト圧縮

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、より高度でCPU負荷の高いグラフィックアルゴリズムを使用することで、画質を損なうことなくプログレッシブ圧縮を超えて帯域幅を削減することを有効または無効にします。

デフォルトでは、ヘビーウェイト圧縮は無効になっています。

有効にすると、ヘビーウェイト圧縮はすべての非可逆圧縮設定に適用されます。Citrix Workspace™アプリでサポートされていますが、他のプラグインには影響しません。

関連するポリシー設定は次のとおりです。

- プログレッシブ圧縮レベル
- プログレッシブ圧縮しきい値

非可逆圧縮レベル

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、帯域幅が制限されているクライアント接続を介して配信される画像に使用される非可逆圧縮の度合いを制御します。このような場合、圧縮なしで画像を表示すると遅くなることがあります。

デフォルトでは、中程度の圧縮が選択されています。

帯域幅を多く消費する画像の応答性を向上させるには、高圧縮を使用します。画質の劣化が許容されないX線画像を表示する場合など、画像データの保持が不可欠な場合は、非可逆圧縮を使用しない方がよいでしょう。

関連ポリシー設定：非可逆圧縮しきい値

非可逆圧縮しきい値

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、非可逆圧縮が適用される接続の最大帯域幅を1秒あたりのキロビット数で表します。

デフォルトでは、しきい値は1秒あたり2147483647キロビットです。

ポリシーに非可逆圧縮レベル設定を追加し、しきい値を指定しないことで、LAN経由での写真などの高精細ビットマップの表示速度を向上させることができます。

関連ポリシー設定：非可逆圧縮レベル

WebSocketsポリシー設定

WebSocketsセクションには、HTML5向けCitrix Workspace™アプリを使用して仮想デスクトップおよびホスト型アプリケーションにアクセスするためのポリシー設定が含まれています。WebSockets機能は、ブラウザベースのアプリケーションとサーバー間の双方向通信を行うことで、セキュリティを向上させ、オーバーヘッドを削減します。この機能は、複数のHTTP接続を開くことなくこれを実現します。

WebSockets接続

この設定では、WebSockets接続を許可または禁止します。

デフォルトでは、WebSocket接続は禁止されています。

WebSocketsポート番号

この設定では、受信WebSocket接続のポートを識別します。

デフォルトでは、値は8008です。

WebSockets信頼済みオリジンサーバーリスト

この設定では、通常はWeb向けCitrix Workspaceアプリである、URLとして表現された信頼済みオリジンサーバーのコンマ区切りリストを提供します。サーバーは、これらのアドレスのいずれかから発信されたWebSockets接続のみを受け入れます。

デフォルトでは、ワイルドカード * を使用して、Web向けCitrix WorkspaceアプリのすべてのURLを信頼します。

リストにアドレスを入力する場合は、次の構文を使用します。

\<protocol>://\<ホストの完全修飾ドメイン名>:

プロトコルはHTTPまたはHTTPSである必要があります。ポートが指定されていない場合、HTTPにはポート80が、HTTPSにはポート443が使用されます。

ワイルドカード `*` は、IPアドレスの一部として使用する場合を除き (`10.105.*.*`)、URL内で使用できます。

WIA デバイスのポリシー設定

WIA デバイスセクションには、Windows Image Acquisition (WIA) を使用したスキャナーリダイレクトを管理するためのポリシー設定が含まれています。

WIA リダイレクト

デジタルカメラやスキャナーなどの WIA デバイスは、WIA フレームワークを使用して、サーバーでホストされている画像処理アプリケーションと通信します。この設定により、ユーザーがユーザーデバイス上の WIA デバイスにアクセスすることを許可または禁止します。デフォルトでは、WIA リダイレクトは禁止されています。

WIA 準拠デバイスの詳細については、「WIA デバイス」を参照してください。

FIDO2 ポリシー設定

この設定は、FIDO2リダイレクトを有効または無効にします。FIDO2リダイレクトにより、ユーザーは仮想マシン内のローカルエンドポイントFIDO2コンポーネントを活用できます。ユーザーは、TPM 2.0とWindows Helloを搭載したデバイスで、FIDO2セキュリティキーまたは統合生体認証を介して仮想セッションを認証できます。

この設定が**許可**されている場合、ユーザーはローカルエンドポイント機能を使用してFIDO2認証を行うことができます。デフォルトでは、この設定は**許可**されています。

レジストリで管理されるHDX™機能

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

> レジストリエディターを開くには、サーバーで `regedit.exe` を実行します。次に、設定を追加または編集するレジストリキーに移動します。

デバイス

Bloombergキーボード

Citrix Virtual Apps and Desktops™は、Bloombergモデル4およびモデル3のスターボードキーボードをサポートしています。デフォルトでは、拡張Bloombergキーボードのサポートは無効になっています。

Bloombergキーボードのサポートを有効にするには、接続を開始する前にクライアントマシンで次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICAClient\GenericUSB`
- **値の名前**: `EnableBloombergHID`
- **値の型**: `DWORD`
- **値のデータ**:
  - `0` - 無効
  - `1` - 有効

詳しくは、「Bloombergキーボード」を参照してください。

マップされたクライアントドライブ

セキュリティ上の予防措置として、ユーザーがCitrix Virtual Apps and Desktops™にログオンすると、デフォルトでサーバーはユーザーの実行権限なしでクライアントドライブをマップします。マップされたクライアントドライブに存在する実行可能ファイルをユーザーが実行できるようにするには、サーバーのレジストリを編集してこのデフォルトを上書きします。

アクセスを許可するには、次のレジストリ値を編集します (**CDMSettings**が存在しない場合は作成します)。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\CDMSettings`
- **値の名前**: `ExecuteFromMappedDrive`
- **値の型**: `DWORD`
- **値のデータ**:
  - `1` - 許可
  - `0` - マップされたドライブでのアクセスを拒否

この変更は、レジストリを編集した後に接続されたセッションに適用されます。

Citrix Virtual Apps and Desktops 7 2006は、このレジストリの場所を含む最初のバージョンです。以前のバージョンのCitrix Virtual Apps and Desktopsでは、異なるレジストリの場所が使用されていました。

詳しくは、「クライアントドライブマッピング」を参照してください。

マイクロソフト Surface Pro および Surface Book ペン

Citrix Virtual Apps and Desktopsは、Windows Inkベースのアプリケーションで標準のペン機能をサポートしています。デフォルトでは、この機能は有効になっています。

この機能を無効または有効にするには、次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Citrix Virtual Desktop Agent\PenApi`
- **値の名前**: `DisablePen`
- **値の型**: `DWORD`
- **値のデータ**:
  - `1` - 無効
  - `0` - 有効

詳細については、「Microsoft Surface Pro および Surface Book のペン」を参照してください。

Windows Image Acquisitionアプリケーションの許可リスト

この設定により、VDA 上のどのアプリケーションが Windows イメージ取得スキャナーリダイレクトにアクセスできるかを制御できます。

デフォルトでは、どのアプリケーションも Windows イメージ取得にアクセスできません。

VDA 上のアプリケーションに対して Windows イメージ取得を調整するには、次のレジストリ設定を作成します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`
- **値の名前**: `WIAAllowedProcesses`

  WIAAllowedProcesses を選択して右クリックします。「**新規 > 複数行文字列値**」を選択し、新しい値の名前を **AllowProcesses** に変更します。
- 値のデータ: Windows イメージ取得にアクセスできる各アプリケーションの完全なパスとプロセス名を入力します。各アプリケーションは新しい行に入力してください。

この設定への変更は、次回 VDA でセッションを起動したときに有効になります。

全般

セキュア接続ポート

VDAでTLS/DTLSが有効になっている場合、デフォルトの接続ポート番号は443です。ポートを変更するには、次のレジストリ値を変更します。

- **キー**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd`
- **値の名前**: `SSLPort`
- **値の型**: `DWORD`
- **値のデータ**: `443` (10進数)

HDX ダイレクト

マルチセッションセッションホストにおける HDX Direct のデフォルトのタイムアウトは 60 秒です。タイムアウトを変更するには、次のレジストリ値を変更します。

- **キー**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd\HdxDirect`
- **値の名前**: `HdxDirectInitiateTimeoutInSeconds`
- **値の型**: `DWORD`
- **値のデータ**: `60` (10進数)

HDX リデューサー

セッションホストで使用するHDX圧縮アルゴリズム（Reducer）のバージョンを構成できます。

シングルセッションVDAでReducer V4を有効にするには、次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy\Defaults\WDSettings`
- **値の名前**: `ReducerOverrideMask`
- **値の型**: `DWORD`
- **値のデータ**: `23` (10進数)

マルチセッションVDAでReducer V4を有効にするには、次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd`
- **値の名前**: `ReducerOverrideMask`
- **値の型**: `DWORD`
- **値のデータ**: `23` (10進数)

Rendezvousバージョンの構成

使用するRendezvousのバージョンを構成するには、次のレジストリ値を設定します:

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent`
- **値の型**: `DWORD`
- **値の名前**: `GctRegistration`
- **値のデータ**:
  - `1` - V2を有効にするには
  - `0` - V1を有効にするには

VDAへの自動ログオンを構成する

この設定により、Windows 10シングルセッションOSおよびマルチセッションOSのVDAで、Microsoftポリシー設定の**常にパスワードを要求する**を有効または無効にできます。

もし**常にパスワードを要求する**が有効になっている場合、ユーザーはリモートセッションを開始するときにVDAで資格情報を入力する必要があります。この設定が無効になっている場合、ユーザーはVDAで資格情報を提供することなく、自動的にリモートセッションに接続します。

デフォルトでは、Microsoftポリシー設定は無効になっています。**常にパスワードを要求する**設定を有効または無効にするには、VDAで次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Portica`
- **値の名前**: `AutoLogon`
- **値の型**: `DWORD`
- **値のデータ**:
  - `1` - Microsoftポリシー設定を無効にし、ユーザーがリモートセッションに自動的にサインインできるようにします。
  - `0` – Microsoftポリシー設定を有効にし、ユーザーがリモートセッションを起動するときに資格情報の入力を求めます。

タイムアウト警告を無効にする

デフォルトでは、非アクティブまたはアイドル状態のセッションを持つユーザーは、セッションが自動的に切断される2分前に警告メッセージを受け取ります。

この設定は、以下のアイドルセッションタイムアウト制限に達したユーザーに対する警告メッセージを無効にし、削除します。

- ウィンドウズ サーバー 2004
- Windows 10マルチセッション2004以降のマルチセッションOS

警告を削除するには、VDAで以下のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Winstations\ICA-CGP`
- **値の名前**: `fEnableTimeoutWarning`
- **値の型**: `DWORD`
- **値のデータ**:
  - `1` - 警告メッセージを無効にする
  - `0` - 警告メッセージを有効にする

警告メッセージを表示するには、レジストリ値を削除するか、`0` に設定します。

EDT MTU検出

MTU検出により、EDTはセッション確立時に最大転送単位（MTU）を自動的に決定できます。これにより、パフォーマンスの低下やセッション確立の失敗につながる可能性のあるEDTパケットの断片化を防ぎます。

この設定はデフォルトで有効になっています。EDT MTU Discovery を無効にするには、以下のレジストリ値を構成し、セッションホストを再起動します。

- **キー**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd`
- **値の名前**: `MtuDiscovery`
- **値の型**: `DWORD`
- **値のデータ**: `0`

MTU Rediscovery を有効にするには、以下のレジストリ値を構成し、セッションホストを再起動します。

- **キー:** `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd\MtuRediscovery`
- **値の名前:** `MtuReDiscovery`
- **値の型:** `DWORD`
- **値のデータ:** `1`
- **キー:** `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd\MtuRediscovery`

- **値の名前:** `MtuReDiscoveryFrequency`
- **値の型:** `DWORD`
- **値のデータ:** `1`

これらの設定はマシン全体に適用され、サポートされているクライアントから接続するすべてのセッションに影響します。

EDT タイムアウト

VDA の EDT タイムアウトは、5 秒から 25 秒の間の任意の値に設定できます。デフォルトの EDT タイムアウト値は 10 秒です。

- **キー**: `HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd\Tds\udp\UDPStackParameters`
- **値の型**: `DWORD`
- **値の名前**: `edtConnectionTimeout`
- **値のデータ**: 5から25までの秒数（10進数）

Citrix Workspaceアプリ for Windowsバージョン2409.10以前の場合、EDTタイムアウトを設定することもできます:

- **キー**: `HKLM\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\EDT`
- **値の型**: `String / REG_SZ`
- **値の名前**: `edtConnectionTimeout`
- **値のデータ**: 5から25までの秒数（10進数）

> **注：**
>
> バージョン2503以降のCitrix Workspaceアプリでは、VDAからのタイムアウト設定が使用されるため、クライアントデバイスでタイムアウトを設定する必要がなくなります。

一般的なコンテンツリダイレクト

ホストからクライアントへのリダイレクトにURLタイプを追加する

デフォルトでは、HTTP、HTTPS、RTSP、RTSPU、PNM、MMSのURLタイプのリダイレクトをサポートしています。Windowsクライアントで以下のレジストリキーと値を作成することで、URLタイプをリストに追加できます。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA`
- **値の名前**: `ExtraURLProtocols`
- **値の型**: `REG_SZ`
- **値のデータ**: 必要なURLタイプをセミコロンで区切って指定します。URLの権限部分より前のすべてを含めます。例: `ftp://;mailto:;customtype1://;custometype2://`

URLタイプはWindowsクライアントにのみ追加できます。このレジストリ設定がないクライアントは、Citrixセッションへのリダイレクトを拒否します。クライアントには、指定されたURLタイプを処理するようにインストールおよび構成されたアプリケーションが必要です。

詳細については、「ホストからクライアントへのリダイレクト」を参照してください。

クライアントフォルダーリダイレクト

クライアントフォルダーリダイレクトは、クライアント側のファイルがホスト側のセッションでアクセス可能になる方法を変更します。サーバーでクライアントフォルダーリダイレクトを有効にし、ユーザーがユーザーデバイスでそれを構成するとします。この場合、ユーザーが指定したローカルボリュームの一部がリダイレクトされます。

サーバーでクライアントフォルダーリダイレクトを有効にするには、次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection`
- **値の名前**: `CFROnlyModeAvailable`
- **値の型**: `DWORD`
- **値のデータ**: `1`

詳細については、クライアントフォルダーリダイレクトを参照してください。

特定のWebサイトセットに対するホストからクライアントへのリダイレクト

特定のWebサイトセットに対してホストからクライアントへのリダイレクトを有効にするには、サーバーVDAで次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA`
- **値の名前**: `ValidSites`
- **値の型**: `REG_MULTI_SZ`
- **値のデータ**: 完全修飾ドメイン名（FQDN）の任意の組み合わせを指定します。複数のFQDNを別々の行に入力します。プロトコル（`http://`または`https://`）なしで、FQDNのみを含めます。FQDNには、最も左の位置にのみワイルドカード文字としてアスタリスク（`*`）を含めることができます。このワイルドカードは、RFC 6125の規則と一致する単一レベルのドメインに一致します。例:

`www.example.com`

`*.example.com`

詳細については、ホストからクライアントへのリダイレクトを参照してください。

ログオフ時および切断時のローカルアプリケーションの動作

デフォルトでは、ユーザーが仮想デスクトップからログオフまたは切断しても、ローカルアプリケーションは実行を継続します。再接続後、ローカルアプリケーションが仮想デスクトップで利用可能な場合、それらは再統合されます。ログオフ時および切断時のローカルアプリケーションの動作を構成するには、ホストされたデスクトップで次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Citrix\Client Hosted Apps\Policies`
- **値の名前**: `Session State`
- **値の型**: `DWORD`
- **値のデータ**:
  - `1` - ユーザーが仮想デスクトップからログオフまたは切断しても、ローカルアプリケーションは引き続き実行されます。再接続すると、ローカルアプリケーションが仮想デスクトップで利用可能な場合、再統合されます。
  - `3` - ユーザーが仮想デスクトップからログオフまたは切断すると、ローカルアプリケーションは閉じます。

詳しくは、「Local App Access and URL redirection」を参照してください。

ホストからクライアントへのリダイレクトのデフォルトリストからURLタイプを削除する

デフォルトのリダイレクトリストからURLタイプを削除するには、サーバーVDAで以下のレジストリキーと値を作成します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA`
- **値の名前**: `DisableServerFTA`
- **値の型**: `DWORD`
- **値のデータ**: `1`
- **値の名前**: `NoRedirectClasses`
- **値の型**: `REG_MULTI_SZ`
- **値のデータ**: `http`、`https`、`rtsp`、`rtspu`、`pnm`、または`mms`のいずれかの値を組み合わせて指定します。複数の値を指定する場合は、別々の行に入力します。例:

`http`

`https`

`rtsp`

詳しくは、「Host to client redirection」を参照してください。

サーバーVDAのデフォルトブラウザ構成

ホストからクライアントへのリダイレクトを有効にすると、Server VDA のデフォルトのブラウザ設定を上書きできます。Web URL がリダイレクトされない場合、Citrix ランチャーは `command_backup` レジストリキーで構成されているブラウザに URL を渡します。このキーはデフォルトで Internet Explorer を指していますが、別のブラウザへのパスを含むように変更できます。

- Internet Explorer (デフォルト)
  - **キー**: `HKEY_CLASSES_ROOT\http\shell\open\command_backup`
  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"c:\program files\internet explorer\iexplore.exe" "%1"`
  - **キー**: `HKEY_CLASSES_ROOT\https\shell\open\command_backup`
  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"c:\program files\internet explorer\iexplore.exe" "%1"`
- グーグル クローム

  - **キー**: `HKEY_CLASSES_ROOT\http\shell\open\command_backup`
  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" "%1"`
  - **キー**: `HKEY_CLASSES_ROOT\https\shell\open\command_backup`
  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" "%1"`

- マイクロソフト エッジ
  - **キー**: `HKEY_CLASSES_ROOT\http\shell\open\command_backup`
  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" "%1"`
  - **キー**: `HKEY_CLASSES_ROOT\https\shell\open\command_backup`
  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" "%1"`

公開アプリケーションのローカルアプリアクセス

ローカルアプリアクセスは、ローカルにインストールされたWindowsアプリケーションを、デスクトップを切り替えることなくホストされたデスクトップ環境にシームレスに統合します。公開アプリケーションへのアクセスを提供するには、サーバーで次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\DesktopStudio`
- **値の名前**: `ClientHostedAppsEnabled`
- **値の型**: `DWORD`
- **値のデータ**:

- `1` - 有効
- `0` - 無効

詳細については、ローカルアプリアクセスとURLリダイレクトを参照してください。

グラフィック

CUDAまたはOpenCLアプリケーションのGPUアクセラレーション

ユーザーセッションで実行されているCUDAおよびOpenCLアプリケーションのGPUアクセラレーションは、デフォルトで無効になっています。

CUDAアクセラレーションのPOC機能を使用するには、次のレジストリ設定を有効にします。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\GraphicsHelper`
- **値の名前**: `CUDA`
- **値の型**: `DWORD`
- **値のデータ**: `00000001`

OpenCLアクセラレーションのPOC機能を使用するには、次のレジストリ設定を有効にします。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\GraphicsHelper`
- **値の名前**: `OpenCL`
- **値の型**: `DWORD`
- **値のデータ**: `00000001`

詳細については、WindowsマルチセッションOSのGPUアクセラレーションを参照してください。

プログレッシブモード

プログレッシブモードはデフォルトで無効になっています。以下のレジストリ値でプログレッシブモードの状態を変更できます:

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics`
- **値の型**: `REG_DWORD`
- **値の名前**: `ProgressiveDisplay`

- **値のデータ**:
  - `0` - 常にオフ (プログレッシブモードを無効にします。この値がデフォルトです。)
  - `1` - 自動 (ネットワークの状態に基づいて切り替えます。)
  - 2 = 常にオン

詳細については、プログレッシブモードを参照してください。

> **注:**
>
> プログレッシブモードは非推奨になりました。Thinwireは、画像の配信を最適化し、キャッシュ効率を維持しながら、プログレッシブモードのほぼすべての利点を提供する代替オプションです。

Windows Presentation Foundation (WPF) レンダリング

HDX 3D Proを使用すると、WindowsマルチセッションOSセッションで実行されているグラフィック負荷の高いアプリケーションを、サーバーのグラフィック処理ユニット (GPU) でレンダリングできます。Windows Presentation Foundation (WPF) のレンダリングをサーバーのGPUに移行することで、グラフィックレンダリングがサーバーのCPUを遅くすることはありません。

サーバーのGPUを使用してWPFアプリケーションのレンダリングを有効にするには、WindowsマルチセッションOSを実行しているサーバーのレジストリに次の設定を作成します。

1. VDAでレジストリエディターを開き、次のキーに移動します。

   `HKLM\Software\Citrix\CtxHook\AppInit_DLLs\Graphics Helper`
2. 次のレジストリ値を作成または編集します。
   - AdapterHandle = 0x00000001
   - DevicePath = 0x00000001
   - フラグ = 0x00000412
   - WPF = 0x00000001
3. WPFアプリの実行可能ファイル名でサブキーを作成します。たとえば、アプリが「mywpfapp.exe」という名前の場合、次のキーを作成します。

   `HKLM\Software\Citrix\CtxHook\AppInit_DLLs\Graphics Helper\mywpfapp.exe`
4. 設定を有効にするには、サーバーを再起動します。

詳細については、WindowsマルチセッションOSのGPUアクセラレーションおよびWindowsマルチセッションOSでWPFアプリを最大限に活用するのブログを参照してください。

マルチメディア

Webカメラのソフトウェア圧縮

Webカメラがハードウェアエンコードをサポートしている場合、HDXビデオ圧縮はデフォルトでハードウェアエンコードを使用します。ハードウェアエンコードは、ソフトウェアエンコードよりも多くの帯域幅を消費する可能性があります。ソフトウェア圧縮を強制するには、クライアントに次の値を追加します。

- **キー**: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HdxRealTime`
- **値の名前**: `DeepCompress_ForceSWEncode`
- **値の型**: `DWORD`
- **値のデータ**: `1`

詳細については、HDX webcam video compressionを参照してください。

ウェブカメラのビデオ解像度

メディアタイプのネゴシエーションが失敗した場合、HDXはデフォルトのVGA解像度（640 x 480ピクセル）にフォールバックします。クライアント上のレジストリキーを使用して、デフォルトの解像度を構成できます。以下のレジストリキーを設定する前に、カメラが指定された解像度をサポートしていることを確認してください。

- **キー**: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime`
- 幅
  - **値の名前**: `DefaultWidth`
  - **値の型**: `DWORD`
  - **値のデータ**: 10進数で指定する希望の幅（例：1280）
- 高さ
  - **値の名前**: `DefaultHeight`
  - **値の型**: `DWORD`
  - **値のデータ**: 10進数で指定する希望の高さ（例：720）

ウェブカメラのビデオ圧縮フレームレート

優先ビデオフレームレートを調整するには、クライアントで次のレジストリ値を編集します。

- **キー**: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime`
- **値の名前**: `FramesPerSecond`
- **値の型**: `DWORD`
- **値のデータ**: `15`

ウェブカメラが指定されたフレームレートをサポートしていない場合、アプリケーションはデフォルトで15 FPSを使用します。

詳細については、HDXウェブカメラビデオ圧縮を参照してください。

Microsoft Teamsのフォールバックモード

Microsoft Teamsが最適化されたVDIモードでロードに失敗した場合 (Teams/About/Versionで「Citrix HDX Not Connected」と表示される場合)、VDAはウェブカメラのリダイレクトやクライアントオーディオおよびマイクのリダイレクトなど、従来のHDXテクノロジーにフォールバックします。Microsoft Teamsの最適化をサポートしないWorkspaceアプリのバージョン/プラットフォームOSを使用している場合、フォールバックレジストリキーは適用されません。

フォールバックメカニズムを制御するには、VDA上で以下のいずれかのレジストリ値を設定します。

- **キー** (いずれか1つのみ必要):
  - **コンピューター設定:** `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Teams`
  - **ユーザー設定:** `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Teams`
- **値の名前**: `DisableFallback`
- **値の型**: `DWORD`
- 値のデータ:
  - `1` - フォールバックモードを無効にする
  - `2` - オーディオのみを有効にする

値が存在しないか0に設定されている場合、フォールバックモードが有効になります。この機能には、Microsoft Teamsバージョン1.3.0.13565以降が必要です。詳細については、「Microsoft Teamsの最適化」を参照してください。

Citrix App Layering™を使用したMicrosoft Teamsの最適化

Citrix App Layeringを使用してVDAとMicrosoft Teamsのインストールを異なるレイヤーで管理している場合は、コマンドラインから`ALLUSER=1`フラグを使用してMicrosoft Teamsをインストール

する前に、Windows上に**PortICA**という名前の空のレジストリキーを作成します。既定の値の名前、種類、データはそのままにします。

- レジストリエディターの32ビット版のキー:
  `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\PortICA`
- レジストリエディターの64ビット版のキー:
  `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

詳細については、「Microsoft Teamsの最適化」を参照してください。

ロード管理ポリシー設定

ロード管理セクションには、Windowsマルチセッション OSマシンを提供するサーバー間のロード管理を有効化および構成するためのポリシー設定が含まれています。

ロード評価インデックスの計算については、CTX202150を参照してください。

同時ログオン許容数

この設定は、サーバーが受け入れ可能な同時ログオンの最大数を指定します。

デフォルトでは、この値は2に設定されています。

この設定が有効な場合、負荷分散は、指定された数を超えるログオンが同時にサーバーVDAでアクティブにならないように試みます。ただし、この制限は厳密には適用されません。制限を適用し（指定された数を超える同時ログオンを失敗させる）、次のレジストリキーを作成します。

> HKLM\Software\Citrix\DesktopServer\LogonToleranceIsHardLimit 種類: DWORD 値: 1

CPU使用率

この設定は、サーバーがフルロードを報告するCPU使用率のレベルをパーセンテージで指定します。有効にすると、サーバーがフルロードを報告するデフォルト値は90%です。

デフォルトでは、この設定は無効になっており、CPU使用率は負荷計算から除外されます。

CPU使用率から除外されるプロセスの優先度

> **注:**

> Workspace Environment Managementがマシンを管理するシナリオでは、この設定をCPU Priority設定と併用すると、意図しない結果が生じる可能性があります。CPU Priority設定を使用する場合は、この設定を無効にすることをお勧めします。

> この設定は、プロセスのCPU使用率がCPU使用率負荷インデックスから除外される優先度レベルを指定します。

デフォルトでは、この値は**標準以下**または**低**に設定されています。

ディスク使用量

この設定は、サーバーが75%のフルロードを報告するディスクキューの長さを指定します。有効にすると、ディスクキューのデフォルト値は8です。

デフォルトでは、この設定は無効になっており、ディスク使用率は負荷計算から除外されます。

セッションの最大数

この設定は、サーバーがホストできるセッションの最大数を指定します。有効にすると、サーバーがホストできるセッションの最大数のデフォルト設定は250になります。

デフォルトでは、この設定は有効になっています。

メモリ使用量

この設定は、サーバーがフルロードを報告するメモリ使用量のレベルをパーセンテージで指定します。有効にすると、サーバーがフルロードを報告するデフォルト値は90%になります。

デフォルトでは、この設定は無効になっており、メモリ使用量は負荷計算から除外されます。

メモリ使用量のベースロード

この設定は、ベースオペレーティングシステムのメモリ使用量の近似値を指定します。また、サーバーがゼロロードと見なされるメモリ使用量をMB単位で定義します。

デフォルトでは、この値は768 MBに設定されています。

プロファイル管理ポリシー設定

このセクションには、プロファイル管理を有効化および構成するためのポリシー設定が含まれています。

以下のようなその他の情報については、プロファイル管理ポリシーを参照してください。

- 対応する.iniファイル設定の名前
- ポリシー設定に必要なプロファイル管理のバージョン

高度なポリシー設定

ロックされたファイルへのアクセス時の再試行回数

ロックされたファイルへのアクセス時の再試行回数を設定します。

このポリシーが無効になっている場合、デフォルト値の5回の再試行が使用されます。このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここでも.iniファイルでも構成されていない場合、デフォルト値が使用されます。

ログオフ時にインターネットCookieファイルを処理する

一部の展開では、`Index.dat`が参照しない余分なインターネットCookieが残されます。継続的なブラウジングの後、ファイルシステムに残された余分なCookieは、プロファイルの肥大化につながる可能性があります。このポリシーを使用すると、Profile Managementを有効にしてIndex.datの処理を強制し、余分なCookieを削除できます。このポリシーはログオフ時間を増加させるため、この問題が発生した場合にのみ有効にしてください。

構成の優先順位:

1. このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
2. このポリシーがここでも.iniファイルでも構成されていない場合、Index.datの処理は行われません。

自動構成を無効にする

Profile Managementは、Citrix Virtual Desktops™環境（パーソナルvDiskの有無など）を検査し、それに応じてグループポリシーを構成します。「未構成」状態のProfile Managementポリシーのみが調整されるため、行ったカスタマイズはすべて保持されます。

このポリシーにより、展開を高速化し、最適化を簡素化できます。このポリシーを構成する必要はありません。ただし、次のいずれかの操作を行う場合は、自動構成を無効にできます。

- 以前のバージョンからの設定を保持するためにアップグレードする
- トラブルシューティング

自動構成は、実行時に環境に応じてデフォルトのポリシー設定を自動的に構成する動的な構成チェッカーと見なすことができます。これにより、設定を手動で構成する必要がなくなります。実行時環境には以下が含まれます。

- ウィンドウズ OS
- Windows OS のバージョン
- シトリックス バーチャル デスクトップの有無
- パーソナル vDisk の有無

環境が変更された場合、自動構成によって以下のポリシーが変更される可能性があります。

- アクティブライトバック
- 常にキャッシュ
- ログオフ時にローカルにキャッシュされたプロファイルを削除
- キャッシュされたプロファイルを削除するまでの遅延
- プロファイルストリーミング

異なる OS でのポリシーのデフォルトの状態については、次の表を参照してください。

	マルチセッションOS	シングルセッションOS
アクティブライトバック	有効	Personal vDiskが使用されている場合は*無効*。それ以外の場合は、有効。
常にキャッシュ	無効	Personal vDiskが使用されている場合は*無効*。それ以外の場合は、有効。
ログオフ時にローカルにキャッシュされたプロファイルを削除	有効	次のいずれかの状況が発生した場合、*無効*になります: Personal vDiskが使用されている、Citrix Virtual Desktopsが割り当てられている、またはCitrix Virtual Desktopsがインストールされていない。それ以外の場合は、有効。
キャッシュされたプロファイルを削除するまでの遅延	0秒	ユーザーの変更が永続的でない場合は60秒。それ以外の場合は0秒。

	マルチセッションOS	シングルセッションOS
プロファイルストリーミング	有効	Personal vDiskが使用されている場合は*無効*。それ以外の場合は、有効。

ただし、自動構成が無効になっている場合、上記のすべてのポリシーはデフォルトで**無効**になります。

> **重要:**
>
> Personal vDiskは非推奨です。詳細については、PVD、AppDisk、およびサポートされていないホストの削除を参照してください。

Profile Management 1909以降、Windows 10（バージョン1607以降）のスタートメニューで改善されたエクスペリエンスを得ることができます。この改善は、以下のポリシーの自動構成によって実現されます。

- `Appdata\Local\Microsoft\Windows\Caches`と`Appdata\Local\Packages`を**ミラーリングするフォルダー**に追加します。
- `Appdata\Local\Microsoft\Windows\UsrClass.Dat*`を**同期するファイル**に追加します。

構成の優先順位:

1. この設定がここで構成されていない場合、.iniファイルの値が使用されます。
2. この設定がここでも.iniファイルでも構成されていない場合、自動構成が有効になります。この場合、環境が変更されると、Profile Managementの設定が変更される可能性があります。

問題が発生した場合にユーザーをログオフする

問題が発生した場合に Profile Management がユーザーをログオフさせるかどうかを指定できます。

このポリシーが無効になっているか、構成されていない場合、問題が発生すると Profile Management はユーザーに一時プロファイルを提供します。たとえば、ユーザー ストアが利用できない場合などです。

有効になっている場合、エラーメッセージが表示され、ユーザーはログオフされます。この設定により、問題のトラブルシューティングが簡素化されます。

構成の優先順位:

1. この設定がここで構成されていない場合、.ini ファイルの値が使用されます。
2. この設定がここでも .ini ファイルでも構成されていない場合、一時プロファイルが提供されます。

カスタマー エクスペリエンス向上プログラム

デフォルトでは、カスタマー エクスペリエンス向上プログラムが有効になっており、匿名統計と使用状況データを収集することで、Citrix® 製品の品質とパフォーマンスの向上に役立てています。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

Outlook の検索インデックス ローミングを有効にする

ユーザープロファイルとともに Outlook 検索データを自動的にローミングすることで、ユーザーベースの Outlook 検索エクスペリエンスを許可します。この機能には、Outlook の検索インデックスを保存するために、ユーザー ストアに追加のスペースが必要です。

このポリシーを有効にするには、ログオフしてから再度ログオンしてください。

Outlook 検索インデックス データベース – バックアップと復元

Outlook の検索インデックス ローミングを有効にするポリシーが有効になっている場合に、ログオン中に Profile Management が何を行うかを指定できます。

このポリシーが有効になっている場合、Profile Management は、ログオン時に検索インデックス データベースが正常にマウントされるたびに、そのデータベースをバックアップします。Profile Management は、そのバックアップを検索インデックス データベースの良好なコピーとして扱います。データベースの破損により検索インデックス データベースのマウントが失敗した場合、Profile Management は検索インデックス データベースを最後に確認された良好なコピーに戻します。

> 注:
>
> 新しいバックアップが正常に保存されると、Profile Managementは以前に保存されたバックアップを削除します。バックアップは利用可能なVHDXストレージを消費します。

OUTLOOK検索データローミングの同時セッションサポートを有効にする

Profile Managementにより、同じユーザーの同時セッションでネイティブのOutlook検索エクスペリエンスが提供されます。このポリシーは、Outlookの検索インデックスローミングポリシーと併用してください。

このポリシーが有効な場合、各同時セッションは個別のOutlook OSTファイルを使用します。

デフォルトでは、Outlook OSTファイルを保存するために使用できるVHDXディスクは2つだけです（ディスクごとに1ファイル）。ユーザーがさらにセッションを開始した場合、そのOutlook OSTファイルはローカルユーザープロファイルに保存されます。Outlook OSTファイルを保存するためのVHDXディスクの最大数を指定できます。

ONEDRIVEコンテナを有効にする

OneDriveフォルダーをユーザーとともにローミングできるようにします。

OneDriveコンテナは、VHDXベースのフォルダーローミングソリューションです。Profile Managementは、ファイル共有上にユーザーごとにVHDXファイルを作成し、ユーザーのOneDriveフォルダーをVHDXファイルに保存します。VHDXファイルは、ユーザーがログオンするときにアタッチされ、ログオフするときにデタッチされます。

UWPアプリのローミング

UWP (Universal Windows Platform) アプリをユーザーとともにローミングできるようにします。その結果、ユーザーは異なるデバイスから同じUWPアプリにアクセスできます。

このポリシーが有効な場合、Profile ManagementはUWPアプリを個別のVHDXディスクに保存することで、ユーザーとともにローミングできるようにします。これらのディスクは、ユーザーのログオン中にアタッチされ、ログオフ中にデタッチされます。

構成の優先順位:

1. この設定がここで構成されていない場合、.iniファイルの値が使用されます。
2. この設定がここでも.iniファイルでも構成されていない場合、この機能は無効になります。

UWPアプリのロード高速化を有効にする

UWPアプリの読み込み高速化を有効にします。これにより、UWPアプリの読み込みを高速化し、非永続環境での一貫性を向上させることができます。デフォルトでは、WindowsはUWPアプリの登録情報を各マシンにローカルに保存しますが、非永続環境では再起動時に失われる可能性があります。このポリシーを有効にすると、Profile Managementは各マシン用にVHDXコンテナを作成してUWPアプリの登録データを保存し、ユーザーログオンを高速化し、再起動時のデータ損失を防ぎます。

構成の優先順位:

1. この設定がGPO、Studio、またはWorkspace Experience Management (WEM) を使用して構成されていない場合、.iniファイルの値が使用されます。
2. この設定がどこにも構成されていない場合、この機能は無効になります。

ログオン時のユーザーグループポリシーの非同期処理を有効にする

Windowsは、ユーザーグループポリシーに同期モードと非同期モードの2つの処理モードを提供します。Windowsは、次のユーザーログオンの処理モードを決定するためにレジストリ値を使用します。レジストリ値が存在しない場合、同期モードが適用されます。レジストリ値はマシンレベルの設定であり、ユーザーとともにローミングされません。したがって、ユーザーが次の場合、非同期モードは期待どおりに適用されません。

- 異なるマシンにログオンする。
- ログオフ時にローカルにキャッシュされたプロファイルを削除するポリシーが有効になっている同じマシンにログオンする。

このポリシーを有効にすると、レジストリ値はユーザーとともにローミングされます。その結果、ユーザーがログオンするたびに処理モードが適用されます。

VHDディスクの圧縮をトリガーする空き領域の比率

VHDディスクの圧縮を有効にする が有効な場合に適用されます。VHDディスクの圧縮をトリガーする空き領域の比率を指定できます。ユーザーログオフ時に空き領域の比率が指定された値を超えると、ディスクの圧縮がトリガーされます。

空き領域の比率 = (現在のVHDファイルサイズ – 必要な最小VHDファイルサイズ*) ÷ 現在のVHDファイルサイズ

* Microsoft Windowsオペレーティングシステムの `MSFT_Partition` クラスのGetSupportedSizeメソッドを使用して取得されます。

VHDディスクの圧縮をトリガーするログオフ回数

VHDディスクの圧縮を有効にする が有効な場合に適用されます。VHDディスクの圧縮をトリガーするユーザーログオフ回数を指定できます。

最後の圧縮以降のログオフ回数が指定された値に達すると、ディスク圧縮が再度トリガーされます。

VHDディスク圧縮のデフラグを無効にする

VHDディスク圧縮を有効にする が有効な場合に適用されます。VHDディスク圧縮のファイルデフラグを無効にするかどうかを指定できます。

VHDディスク圧縮が有効な場合、VHDディスクファイルはまずWindowsに組み込まれている `defrag` ツールを使用して自動的にデフラグされ、その後圧縮されます。VHDディスクのデフラグはより良い圧縮結果をもたらしますが、無効にするとシステムリソースを節約できます。

プロファイルコンテナのマルチセッションライトバックを有効にする

マルチセッションシナリオでプロファイルコンテナのライトバックを有効にします。有効にすると、すべてのセッションでの変更がプロファイルコンテナに書き戻されます。そうでない場合、プロファイルコンテナでは最初のセッションのみが読み取り/書き込みモードであるため、最初のセッションでの変更のみが保存されます。Citrix Profile Managementプロファイルコンテナは Citrix Profile Management 2103以降でサポートされています。FSLogix Profile ContainerはCitrix Profile Management 2003以降でサポートされています。

FSLogix Profile Containerでこのポリシーを使用するには、以下の前提条件が満たされていることを確認してください。

- FSLogix Profile Container機能がインストールされ、有効になっていること。
- FSLogixでプロファイルタイプが **読み取り/書き込みプロファイルを試行し、読み取り専用にフォールバックする** に設定されていること。

ユーザーストアをレプリケートする

リモートユーザープロファイルストアを、ログオンおよびログオフごとに複数のパスにレプリケートできます。これにより、Profile Managementはユーザーログオンのプロファイル冗長性を提供できます。

このポリシーを有効にすると、システムI/Oが増加し、ログオフが長くなる可能性があります。

> **注:**
>
> この機能は、ファイルベースとコンテナベースの両方のプロファイルソリューションで利用できます。

ユーザーストアへの資格情報ベースのアクセスを有効にする

デフォルトでは、Citrix Profile Managementは現在のユーザーを偽装してユーザーストアにアクセスします。ユーザーストアへのアクセス時にProfile Managementが現在のユーザーを偽装しないようにする場合は、この機能を有効にしてください。現在のユーザーがアクセス権を持たないストレージリポジトリ（Azure Filesなど）にユーザーストアを配置できます。

Profile Management がユーザー ストアにアクセスできるようにするには、プロファイル ストレージ サーバーの資格情報を Workspace Environment Management™ (WEM) または Windows 資格情報マネージャーに保存します。Profile Management が実行される各マシンで同じ資格情報を構成する必要をなくすために、Workspace Environment Management を使用することをお勧めします。Windows 資格情報マネージャーを使用する場合は、ローカル システム アカウントを使用して資格情報を安全に保存してください。

> **注:**
>
> このポリシーは、ファイルベースと VHDX ベースの両方のユーザー ストアで利用できます。Profile Management のバージョン 2212 より前では、このポリシーは VHDX ベースのユーザー ストアでのみ利用できます。

構成の優先順位:

1. ここでこの設定が構成されていない場合、.ini ファイルの値が使用されます。
2. ここで、または .ini ファイルでこの設定が構成されていない場合、デフォルトで無効になります。

VHDX ファイルのストレージ パスをカスタマイズする

Profile Management は、プロファイル コンテナー、Outlook の検索インデックス ローミング、フォルダー ミラーリングの高速化といった VHDX ベースのポリシーを提供します。デフォルトでは、VHDX ファイルはユーザー ストアに保存されます。このポリシーを使用すると、それらを保存する別のパスを指定できます。

VHD コンテナーのデフォルト容量

VHD コンテナーのデフォルトのストレージ容量 (GB 単位) を指定できます。

構成の優先順位:

1. ここでこのポリシーが構成されていない場合、.ini ファイルの値が使用されます。
2. ここで、または .ini ファイルでこのポリシーが構成されていない場合、デフォルトは 50 (GB) です。

セッションで VHDX ディスクを自動的に再アタッチする

このポリシーを有効にすると、Profile Management は VHDX ベースのポリシーの高い安定性を確保します。デフォルトでは、このポリシーは有効になっています。

このポリシーが有効になっている場合、Profile Management は VHDX ベースのポリシーで使用されている VHDX ディスクを監視します。いずれかのディスクがデタッチされた場合、Profile Management はそのディスクを自動的に再アタッチします。

プロファイルコンテナの自動拡張しきい値

プロファイルコンテナが自動拡張をトリガーするストレージ容量の使用率を指定できます。

構成の優先順位:

- このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
- このポリシーがここまたは.iniファイルで構成されていない場合、デフォルトはストレージ容量の90%です。

プロファイルコンテナの自動拡張増分

自動拡張がトリガーされたときに、プロファイルコンテナが自動的に拡張するストレージ容量（GB単位）を指定できます。

構成の優先順位:

- このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
- このポリシーがここまたは.iniファイルで構成されていない場合、デフォルトは10 GBです。

プロファイルコンテナの自動拡張制限

自動拡張がトリガーされたときに、プロファイルコンテナが自動的に拡張できる最大ストレージ容量（GB単位）を指定できます。

構成の優先順位:

- このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
- このポリシーがここまたは.iniファイルで構成されていない場合、デフォルトは80 GBです。

ユーザーレベルのポリシー設定を有効にする

このポリシーを有効にすると、マシンレベルのポリシー設定がユーザーレベルで機能し、ユーザーレベルの設定がマシンレベルの設定を上書きします。

構成の優先順位:

1. ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。
2. ここででも.iniファイルでもこのポリシーが構成されていない場合、無効になります。

ユーザーグループの優先順位を設定する

ユーザーグループの優先順位を指定できます。この順序は、ユーザーが異なるポリシー設定を持つ複数のグループに属している場合に、どのグループが優先されるかを決定します。

ユーザーが競合するポリシー設定を持つ複数のグループに属している場合、以下を考慮してください:

- ユーザーがこのポリシーで定義されている1つ以上のグループに属している場合、最も優先順位の高いグループが優先されます。
- ユーザーがこのポリシーで定義されているどのグループにも属していない場合、アルファベット順で最も早くリストされているSIDを持つグループが優先されます。

ユーザーストアの選択方法

複数のユーザーストアが利用可能な場合に、ユーザーストアの選択方法を指定できます。オプションは次のとおりです:

- **構成順序。** Profile Managementは、最初に構成されたストアを選択します。
- **アクセスパフォーマンス。** Profile Managementは、最高のアクセスパフォーマンスを持つストアを選択します。

構成の優先順位:

1. ここでこの設定が構成されていない場合、.ini ファイルの値が使用されます。
2. ここでも .ini ファイルでもこの設定が構成されていない場合、**構成順序**が使用されます。

ユーザー ストア間のセッション内プロファイル コンテナー フェールオーバーを有効にする

デフォルトでは、複数のユーザー ストアが展開されている場合、プロファイル コンテナーのフェールオーバーはユーザー ログオン時にのみ発生します。その結果、プロファイルの冗長性はユーザー ログオン時にのみ利用可能です。このポリシーを使用すると、フェールオーバーの範囲をセッション全体に拡大し、セッション全体でプロファイルの冗長性を確保できます。このポリシーを有効にすると、セッション中に Profile Management がアクティブなプロファイル コンテナーへの接続を失った場合、自動的に別の利用可能なコンテナーに切り替わります。

構成の優先順位:

1. ここでこのポリシーが構成されていない場合、.ini ファイルの値が使用されます。
2. ここでも .ini ファイルでもこのポリシーが構成されていない場合、この設定は無効になります。

プロファイル読み込みタイムアウト

プロファイル読み込みタイムアウト機能を有効にし、タイムアウト期間を構成できます。Citrix Profile Management は、一時プロファイルに切り替える前に、ユーザー プロファイルが読み込まれるまで指定されたタイムアウト時間待機します。 デフォルトでは、**プロファイル読み込みタイムアウト**設定は 45 秒で、有効な範囲は 0 ～ 1800 秒です。プロファイルの読み込みをバイパスして一時プロファイルを使用するには、タイムアウトを 0 秒に設定します。

構成の優先順位:

1. ここでこのポリシーが構成されていない場合、.ini ファイルの値が使用されます。
2. ここでも .ini ファイルでもこのポリシーが構成されていない場合、このポリシーはデフォルトで無効になります。

ログオフ時のプロファイル同期を制限する

ユーザー ログオフ時に同期されるユーザー ストアの数を指定できます。 デフォルトでは、Citrix Profile Management はログオフ中にすべてのユーザー ストアを同期し、すべてのストアでプロファイルが同期されるまでログオフは完了しません。 同期されるストアの数を減らすと、ログオフが高速化されます。非永続マシンでは、未同期のストアは次回のユーザー セッション中に更新され、永続マシンでは、未同期のストアはバックグラウンドで同期されます。

構成の優先順位:

1. このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
2. このポリシーがここでも.iniファイルでも構成されていない場合、ポリシーはデフォルトで無効になります。\n\n注: この設定は、ユーザー ストアのレプリケートポリシーが有効になっている場合にのみ適用されます。

プロファイルサイズがクォータを超過した場合にユーザーに通知する

ユーザープロファイルのクォータを設定し、プロファイルサイズがそれを超過した場合にユーザーに通知できます。

構成の優先順位:

1. このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
2. このポリシーがここでも.iniファイルでも構成されていない場合、この設定は無効になります。

プロファイルサイズがクォータを超過した場合の通知メッセージ

プロファイルサイズがクォータを超過した場合にユーザーに通知するポリシーが有効な場合に適用されます。ユーザーが受け取る通知メッセージを設定できます。

構成の優先順位:

1. このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
2. このポリシーがここでも.iniファイルでも構成されていない場合、この設定は無効になります。

マシン休止状態のマルチセッションサポートを有効にする

休止状態中にディスクの状態を維持することで、システム休止状態のサポートを有効にできます。これにより、休止状態のセッションで使用されているVHDXディスクが、他の同時実行セッションに再割り当てされないようにします。その結果、マシンが休止状態から回復した後もユーザープロファイルを再開でき、一貫したセッションの継続性が保証されます。

構成の優先順位:

1. このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。
2. このポリシーがここでも .ini ファイルでも構成されていない場合、設定は無効になります。

基本的なポリシー設定

このセクションには、Profile Management の基本的な構成に関連するポリシー設定が含まれています。

Profile Management を有効にする

デフォルトでは、展開を容易にするため、Profile Management はログオンまたはログオフを処理しません。Profile Management は、他のすべてのセットアップタスクを実行し、Citrix® ユーザープロファイルが環境でどのように動作するかをテストした後にのみ有効にしてください。

このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、Profile Management は Windows ユーザープロファイルを一切処理しません。

処理されるグループ

コンピューターローカルグループとドメイングループ（ローカル、グローバル、ユニバーサル）の両方を使用できます。ドメイングループは、DOMAIN NAME\GROUP NAME の形式で指定する必要があります。

このポリシーがここで構成されている場合、Profile Management はこれらのユーザーグループのメンバーのみを処理します。このポリシーが無効になっている場合、Profile Management はすべてのユーザーを処理します。このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、すべてのユーザーグループのメンバーが処理されます。

除外されるグループ

コンピューターローカルグループとドメイングループ（ローカル、グローバル、ユニバーサル）を使用して、特定のユーザープロファイルが処理されないようにすることができます。ドメイングループは、DOMAIN NAME\ GROUP NAME の形式で指定します。

この設定がここで構成されている場合、Profile Management はこれらのユーザーグループのメンバーを除外します。この設定が無効になっている場合、Profile Management はどのユーザーも除外しません。この設定がここで構成されていない場合、.ini ファイルの値が使用されます。この設定がここでも .ini ファイルでも構成されていない場合、どのグループのメンバーも除外されません。

ローカル管理者によるログオンの処理

BUILTIN\Administrators グループのメンバーのログオンを処理するかどうかを指定します。Citrix Virtual Apps 環境などのマルチセッションオペレーティングシステムでは、このポリシーが無効になっているか、構成されていないと見なされます。この場合、Profile Management は、ドメインユーザーによるログオンは処理されるが、ローカル管理者によるログオンは処理されないと想定します。シングルセッションオペレーティングシステム（Citrix Virtual Desktops 環境など）では、ローカル管理者のログオンが処理されます。このポリシーにより、ローカル管理者権限を持つドメインユーザー（通常は仮想デスクトップが割り当てられた Citrix Virtual Desktops ユーザー）は、次のことが可能になります。

- 処理をバイパスする
- ログオンする
- Profile Managementで問題が発生しているデスクトップのトラブルシューティング

注：ドメインユーザーのログオンは、通常、製品ライセンスへの準拠を確実にするために、グループメンバーシップによって課される制限の対象となる場合があります。 このポリシーが無効になっている場合、Profile Managementはローカル管理者によるログオンを処理しません。このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここでも.iniファイルでも構成されていない場合、管理者は処理されません。

ユーザーストアへのパス

ユーザー設定（レジストリの変更と同期されたファイル）が保存されるディレクトリ（ユーザーストア）へのパスを設定します。

パスは次のいずれかです。

- 相対パス。ホームディレクトリ（通常、Active Directoryのユーザーの#homeDirectory#属性として構成されます）に対する相対パスである必要があります。

- UNCパス。通常、サーバー共有またはDFS名前空間を指定します。
- 無効または未構成。この場合、#homeDirectory#\Windowsの値が想定されます。

このポリシーでは、次の種類の変数を使用できます。

- パーセント記号で囲まれたシステム環境変数（例：%ProfVer%）。システム環境変数は通常、追加のセットアップが必要です。
- ハッシュで囲まれたActive Directoryユーザーオブジェクトの属性（例：#sAMAccountName#）。
- Profile Management変数。詳しくは、Profile Management変数の製品ドキュメントを参照してください。

`%username%`と`%userdomain%`を除き、ユーザー環境変数は使用できません。場所やユーザーなどを完全に定義するために、カスタム属性を作成することもできます。属性では大文字と小文字が区別されます。

例:

- `\\server\share#sAMAccountName#`は、ユーザー設定をUNCパス`\\server\share\JohnSmith`に保存します（現在のユーザーの#sAMAccountName#がJohnSmithに解決される場合）。
- `\\server\profiles$\%USERNAME%.%USERDOMAIN%\!CTX_OSNAME!!CTX_OSBITNESS!`は`\\server\profiles$\JohnSmith.DOMAINCONTROLLER1\Win8x64`に展開される場合があります。

重要：使用する属性または変数に関係なく、このポリシーがNTUSER.DATを含むフォルダーの1つ上のフォルダーに展開されることを確認してください。たとえば、このファイルが`\\server\profiles$\JohnSmith.Finance\Win8x64\UPM_Profile`に含まれる場合、ユーザー ストアへのパスを`\\server\profiles$\JohnSmith.Finance\Win8x64`に設定します（\UPM_Profileサブフォルダーではありません）。

ユーザー ストアへのパスを指定する際に変数を使用する方法について詳しくは、次のトピックを参照してください。

- 複数のファイルサーバーでCitrixユーザープロファイルを共有する
- OU内およびOU間でプロファイルを管理する
- Profile Managementによる高可用性と災害復旧

ユーザーストアへのパスが無効になっている場合、ユーザー設定はホームディレクトリのWindowsサブディレクトリに保存されます。

このポリシーが無効になっている場合、ユーザー設定はホームディレクトリのWindowsサブディレクトリに保存されます。このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここでも.iniファイルでも構成されていない場合、ホームドライブのWindowsディレクトリが使用されます。

ユーザーストアの移行

ユーザー設定（レジストリの変更と同期されたファイル）が以前に保存されていたフォルダーへのパス（以前使用していたユーザーストアパス）を指定します。

この設定が構成されている場合、以前のユーザー ストアに保存されているユーザー設定は、「ユーザー ストアへのパス」ポリシーで指定された現在のユーザー ストアに移行されます。

パスは、絶対UNCパスまたはホームディレクトリに対する相対パスにすることができます。

どちらの場合も、次の種類の変数を使用できます。

- パーセント記号で囲まれたシステム環境変数
- ハッシュ記号で囲まれたActive Directoryユーザーオブジェクトの属性

例:

- フォルダー `Windows\%ProfileVer%` は、ユーザー設定をユーザーストアの `Windows\W2K3` というサブフォルダーに保存します（%ProfileVer% がW2K3に解決されるシステム環境変数である場合）。
- `\\server\share#SAMAccountName#` は、ユーザー設定をUNCパス `\\server\share\<JohnSmith>` に保存します（`#SAMAccountName#` が現在のユーザーに対してJohnSmithに解決される場合）。

パスでは、`%username%` と `%userdomain%` を除くユーザー環境変数を使用できます。

この設定が無効になっている場合、ユーザー設定は現在のユーザーストアに保存されます。

この設定がここで構成されていない場合、.iniファイルの対応する設定が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、ユーザー設定は現在のユーザーストアに保存されます。

アクティブライトバック

変更されたファイルとフォルダー（レジストリエントリを除く）は、ログオフする前にセッション中にユーザーストアに同期できます。

このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここでも.iniファイルでも構成されていない場合、有効になります。

オフラインプロファイルのサポート

このポリシーにより、プロファイルは可能な限り早い機会にユーザー ストアと同期できます。これは、ローミングするラップトップまたはモバイルデバイスのユーザーを対象としています。ネットワーク接続が切断された場合でも、再起動または休止状態の後でも、プロファイルはラップトップまたはデバイス上でそのまま維持されます。モバイルユーザーが作業すると、プロファイルはローカルで更新されます。また、ネットワーク接続が再確立されると、最終的にユーザー ストアと同期されます。

このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここでも.iniファイルでも構成されていない場合、オフラインプロファイルは無効になります。

アクティブライトバックレジストリ

「アクティブライトバック」と合わせてこのポリシーを使用してください。変更されたレジストリエントリは、セッション中にユーザーストアに同期できます。

ここでこの設定を構成しない場合、.iniファイルの値が使用されます。

ここでも.iniファイルでもこの設定を構成しない場合、アクティブライトバックレジストリは無効になります。

セッションロックおよび切断時のアクティブライトバック

このポリシーと**アクティブライトバック**ポリシーの両方が有効になっている場合、プロファイルファイルとフォルダーは、セッションがロックまたは切断されたときにのみ書き戻されます。

このポリシーと**アクティブライトバック**および**アクティブライトバックレジストリ**ポリシーの両方が有効になっている場合、レジストリエントリは、セッションがロックまたは切断されたときにのみ書き戻されます。

オフラインプロファイルのサポート

オフラインプロファイル機能を有効にします。この機能は、ネットワークから頻繁に切断されるコンピューター向けです。たとえば、サーバーやデスクトップではなく、ラップトップやモバイルデバイスなどです。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここでも.iniファイルでもこの設定が構成されていない場合、オフラインプロファイルのサポートは無効になります。

クロスプラットフォームポリシー設定

このセクションには、**Profile Management cross-platform** 設定機能の構成に関連するポリシー設定が含まれています。

クロスプラットフォーム設定を有効にする

既定では、展開を容易にするため、クロスプラットフォーム設定は無効になっています。この機能を十分に計画しテストした後にのみ、このポリシーを有効にして処理をオンにしてください。

ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、クロスプラットフォーム設定は適用されません。

クロスプラットフォーム設定ユーザーグループ

1つ以上のWindowsユーザーグループを入力します。たとえば、このポリシーを使用して、テストユーザーグループのプロファイルのみを処理できます。このポリシーが構成されている場合、Profile Managementのクロスプラットフォーム設定機能は、これらのユーザーグループのメンバーのみを処理します。このポリシーが無効になっている場合、この機能は、処理済みグループポリシーで指定されたすべてのユーザーを処理します。

ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、すべてのユーザーグループが処理されます。

クロスプラットフォーム定義へのパス

ダウンロードパッケージからコピーした定義ファイルのネットワーク上の場所を識別します。このパスはUNCパスである必要があります。ユーザーはこの場所への読み取りアクセス権を持ち、管理者は書き込みアクセス権を持っている必要があります。この場所は、Server Message Block (SMB) またはCommon Internet File System (CIFS) ファイル共有である必要があります。

ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、クロスプラットフォーム設定は適用されません。

クロスプラットフォーム設定ストアへのパス

ユーザーのクロスプラットフォーム設定が保存されるフォルダーであるクロスプラットフォーム設定ストアへのパスを設定します。ユーザーはこの領域への書き込みアクセス権を持っている必要があります。パスは絶対UNCパスまたはホームディレクトリに対する相対パスにすることができます。

この領域は、複数のプラットフォームで共有されるプロファイルデータが配置されるユーザーストアの共通領域です。ユーザーはこの領域への書き込みアクセス権を持っている必要があります。パスは絶対UNCパスまたはホームディレクトリに対する相対パスにすることができます。**Path to user store** と同じ変数を使用できます。

このポリシーが無効になっている場合、パス Windows\PM_CP が使用されます。ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、既定値が使用されます。

クロスプラットフォーム設定を作成するためのソース

このポリシーがそのプラットフォームのOUで有効になっている場合、プラットフォームをベースプラットフォームとして指定します。このポリシーは、ベースプラットフォームのプロファイルからクロスプラットフォーム設定ストアにデータを移行します。

各プラットフォーム独自のプロファイルセットは、別々のOUに保存されます。クロスプラットフォーム設定ストアをシードするために、どのプラットフォームのプロファイルデータを使用するかを決定する必要があります。これはベースプラットフォームと呼ばれます。クロスプラットフォーム設定ストアにデータのない定義ファイルが含まれている場合、または単一プラットフォームプロファイルのキャッシュデータがストア内の定義データよりも新しい場合を考慮してください。この場合、このポリシーを無効にしない限り、プロファイル管理は単一プラットフォームプロファイルからストアにデータを移行します。

> **重要:**
>
> このポリシーが複数のOU、または複数のユーザーオブジェクトやマシンオブジェクトで有効になっている場合、最初にユーザーがログオンしたプラットフォームがベースプロファイルになります。 デフォルトでは、このポリシーは有効になっています。

ファイルシステム ポリシー設定

このセクションには、以下の設定を行うポリシーが含まれています。

- ユーザープロファイル内のどのファイルが、プロファイルがインストールされているシステムとユーザー ストアの間で同期されるか
- ユーザープロファイル内のどのディレクトリが、プロファイルがインストールされているシステムとユーザー ストアの間で同期されるか

除外ポリシー設定

このセクションでは、ユーザープロファイル内のどのファイルとディレクトリを同期プロセスから除外するかを設定するためのポリシー設定について説明します。

除外リスト - ファイル

同期中に無視されるファイルのリスト。ファイル名はユーザープロファイル (%USERPROFILE%) に対する相対パスである必要があります。ワイルドカードはファイル名とフォルダー名でサポートされていますが、ファイル名のワイルドカードのみが再帰的に適用されます。

例:

- `Desktop\Desktop.ini` は `Desktop` フォルダー内のファイル `Desktop.ini` を無視します。
- `%USERPROFILE%*.tmp` はプロファイル全体で拡張子 `.tmp` を持つすべてのファイルを無視します。
- `AppData\Roaming\MyApp*.tmp` はプロファイルの一部で拡張子 `.tmp` を持つすべてのファイルを無視します。
- `Downloads*\a.txt` は `Downloads` フォルダーの直下のサブフォルダーにある `a.txt` を無視します。

このポリシーが無効になっている場合、ファイルは除外されません。このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、ファイルは除外されません。

デフォルトの除外リストを有効にする - ディレクトリ

同期中に無視されるディレクトリのデフォルトリスト。このポリシーを使用して、GPO 除外ディレクトリを手動で入力することなく指定できます。

このポリシーを無効にすると、Profile Management はデフォルトでどのディレクトリも除外しません。

このポリシーをここで構成しない場合、Profile Management は .ini ファイルの値を使用します。このポリシーをここでも .ini ファイルでも構成しない場合、Profile Management はデフォルトでどのディレクトリも除外しません。

除外リスト - ディレクトリ

同期中に無視されるフォルダーのリスト。フォルダー名はユーザープロファイル (%USERPROFILE%) に対する相対パスとして指定する必要があります。フォルダー名でのワイルドカードはサポートされていますが、再帰的には適用されません。

例:

- `Desktop` はユーザープロファイル内の `Desktop` フォルダーを無視します

このポリシーが無効になっている場合、フォルダーは除外されません。このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここでも.iniファイルでも構成されていない場合、フォルダーは除外されません。

ログオン除外チェック

この設定は、ユーザーストア内のプロファイルに除外されたファイルまたはフォルダーが含まれている場合に、Profile Managementが何を行うかを構成します。可能なポリシー設定と対応するアクションを次の表に示します。

ポリシー設定	アクション
設定が無効になっているか、「ログオン時に除外されたファイルまたはフォルダーを同期する」の値がデフォルトに設定されている	ユーザーがログオンすると、Profile Managementはユーザーストアからローカルプロファイルに除外されたファイルまたはフォルダーを同期します。
設定が「ログオン時に除外されたファイルまたはフォルダーを無視する」に設定されている	ユーザーがログオンすると、Profile Managementはユーザーストア内の除外されたファイルまたはフォルダーを無視します。
設定が「ログオン時に除外されたファイルまたはフォルダーを削除する」に設定されている	ユーザーがログオンすると、Profile Managementはユーザーストア内の除外されたファイルまたはフォルダーを削除します。
Web Studioで設定が構成されていない	.iniファイルの値が使用されます
Web Studioまたは.iniファイルで設定が構成されていない	ユーザーがログオンすると、除外されたファイルまたはフォルダーはユーザーストアからローカルプロファイルに同期されます。

大容量ファイルの処理 - シンボリックリンクとして作成されるファイル

ログオンパフォーマンスを向上させ、サイズの大きいファイルを処理するために、Profile Management はこのリスト内のファイルをコピーする代わりにシンボリックリンクを作成します。

ファイルを参照するポリシーではワイルドカードを使用できます。例: `!ctx_localappdata!\Microsoft\Outlook*.OST`。

Microsoft Outlook のオフラインフォルダーファイル (`*.ost`) を処理するには、**Outlook** フォルダーが Profile Management の対象から除外されていないことを確認してください。

これらのファイルは、複数のセッションで同時にアクセスすることはできません。

同期ポリシー設定

同期セクションでは、ユーザープロファイル内のどのファイルとフォルダーを、プロファイルがインストールされているシステムとユーザー ストアの間で同期するかを指定するためのポリシー設定について説明します。

同期するディレクトリ

デフォルトでは、Profile Management は、ユーザープロファイルがインストールされているシステムとユーザー ストアの間でユーザープロファイルを同期します。同期からフォルダーを除外した場合、このポリシーを使用すると、除外されたフォルダーのサブフォルダーを同期に含めることができます。

このリストのパスは、ユーザープロファイルに対する相対パスである必要があります。フォルダー名でのワイルドカードはサポートされていますが、再帰的には適用されません。

このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、ユーザープロファイル内の除外されていないフォルダーのみが同期されます。

同期するファイル

デフォルトでは、Profile Management は、ユーザープロファイルがインストールされているシステムとユーザー ストアの間でユーザープロファイルを同期します。同期からフォルダーを除外した場合、このポリシーを使用すると、除外されたフォルダー内のファイルを同期に含めることができます。

このリストのパスは、ユーザープロファイルに対する相対パスである必要があります。ファイル名とフォルダー名でワイルドカードがサポートされていますが、ファイル名のワイルドカードのみが再帰的に適用されます。ワイルドカードをネストすることはできません。

例:

- `AppData\Local\Microsoft\Office\Access.qat` は、デフォルト構成で除外されているフォルダーの下にあるファイルを指定します。
- `AppData\Local\MyApp*.cfg` は、プロファイルフォルダー `AppData\Local\MyApp` およびそのサブフォルダー内の拡張子 `.cfg` を持つすべてのファイルを指定します。

このポリシーを無効にすると、有効にして空のリストを構成した場合と同じ効果があります。

このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、ユーザープロファイル内の除外されていないファイルのみが同期されます。

ミラーリングするフォルダー

このポリシーを使用すると、トランザクションフォルダー（参照フォルダーとも呼ばれる）に関連する問題を解決できます。このフォルダーには、相互に依存するファイルが含まれており、あるファイルが別のファイルを参照しています。

フォルダーのミラーリングにより、プロファイル管理はトランザクションフォルダーとその内容を単一のエンティティとして処理し、プロファイルの肥大化を防ぐことができます。たとえば、**Internet Explorer の Cookie** フォルダーをミラーリングして、Index.dat がインデックス化する Cookie と同期されるようにすることができます。このような状況では、「最後の書き込みが優先されます」。そのため、複数のセッションで変更されたミラーリングされたフォルダー内のファイルは、最後の更新によって上書きされ、プロファイル変更が失われます。

たとえば、次の表は、ユーザーがインターネットを閲覧している間に Index.dat が Cookie をどのように参照するかを示しています。

シナリオ	INDEX.DAT が COOKIE を参照する方法	
ユーザーは2つの Internet Explorer セッションを持っており、それぞれ異なるサーバー上にあり、各セッションで異なるサイトを訪れます。	各サイトからの Cookie は、適切なサーバーに追加されます。	各サイトからの Cookie は、適切なサーバーに追加されます。
ユーザーは最初のセッションからログオフするか、セッションの途中でログオフします（アクティブなライトバック機能が構成されている場合）。	2番目のセッションからの Cookie は、最初のセッションからの Cookie を置き換える必要があります。	
最初のセッションと2番目のセッションがマージされ、Index.dat 内の Cookie への参照が古くなります。	新しいセッションでのその後の閲覧は、繰り返しのマージと肥大化した Cookie フォルダーにつながります。	

Cookie フォルダーをミラーリングすることで、この問題が解決されます。この場合、ユーザーがログオフするたびに、Cookie は最後のセッションからの Cookie で上書きされます。これにより、Index.dat は常に最新の状態に保たれます。

ここでこのポリシーが構成されていない場合、.ini ファイルの値が使用されます。ここで、または .ini ファイルでこのポリシーが構成されていない場合、フォルダーはミラーリングされません。

フォルダーのミラーリングを高速化する

このポリシーと**ミラーリングするフォルダー**ポリシーの両方が有効になっている場合、**プロファイル管理はミラーリングされた**フォルダーを VHDX ベースの仮想ディスクに保存します。ログオン中に仮想ディスクをアタッチし、ログオフ中にデタッチします。このポリシーを有効にすると、ユーザー ストアとローカル プロファイルの間でフォルダーをコピーする必要がなくなり、フォルダーのミラーリングが高速化されます。

ファイル重複排除ポリシー設定

ユーザーストア内のさまざまなユーザープロファイルに同一のファイルが存在する場合があります。ユーザーストアにファイルの重複インスタンスが保存されていると、ストレージコストが増加します。

ファイル重複排除ポリシーにより、Profile Management はユーザーストアから重複ファイルを削除し、それらの単一インスタンスを中央の場所 (*共有ストア* と呼ばれる) に保存できます。これにより、ユーザーストアでのファイルの重複が回避され、ストレージコストが節約されます。

重複排除のために共有ストアに含めるファイル

ファイル重複排除を有効にし、重複排除のために共有ストアに含めるファイルを指定できます。

共有ストアから除外するファイル

共有ストアから除外するファイルを指定できます。このポリシーは、*重複排除のために共有ストアに含めるファイル* ポリシーと併用してください。

プロファイルコンテナから重複排除するファイルの最小サイズ

プロファイルコンテナから重複排除するファイルの最小サイズを指定できます。サイズは 256 MB 以上である必要があります。

構成の優先順位:

1. ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。
2. この設定がここまたは .ini ファイルのいずれかで構成されていない場合、値は 256 です。

フォルダーリダイレクトのポリシー設定

このセクションには、プロファイルに一般的に表示されるフォルダーを共有ネットワークの場所にリダイレクトするかどうかを指定するポリシー設定が含まれています。

管理者アクセスの許可

この設定により、管理者はユーザーのリダイレクトされたフォルダーの内容にアクセスできるようになります。

> **注:**
>
> この設定は、ドメインへの完全かつ無制限のアクセス権を持つ管理者に対して権限を付与します。

> デフォルトでは、この設定は無効になっており、ユーザーにはリダイレクトされたフォルダーの内容への排他的なアクセス権が付与されます。

ドメイン名を含める

この設定により、`%userdomain%` 環境変数を UNC パスの一部として組み込むことができます。この UNC パスは、リダイレクトされたフォルダーに対して指定されます。

デフォルトでは、この設定は無効になっています。そして、リダイレクトされたフォルダーに対して指定される UNC パスの一部として、`%userdomain%` 環境変数は含まれません。

AppData(Roaming) ポリシー設定

このセクションには、**AppData(Roaming)** フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

APPDATA(ROAMING) パス

この設定は、**AppData(Roaming)** フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

APPDATA(ROAMING) のリダイレクト設定

この設定は、**AppData(Roaming)** フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツは UNC パスにリダイレクトされます。詳細については、ユーザー ストアへのパス セクションを参照してください。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

デスクトップポリシー設定

このセクションには、`Desktop` フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

デスクトップパス

この設定は、**デスクトップ**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

デスクトップのリダイレクト設定

この設定は、**デスクトップ**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツは UNC パスにリダイレクトされます。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

ドキュメントポリシー設定

このセクションには、**ドキュメント**フォルダーの内容を共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

ドキュメントパス

この設定は、**ドキュメント**フォルダー内のファイルがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

ドキュメントパス設定は、**ドキュメント**フォルダーへのファイルのリダイレクトだけでなく、**ミュージック**、**ピクチャ**、**ビデオ**フォルダーへのファイルのリダイレクトのためにも有効にする必要があります。

ドキュメントのリダイレクト設定

この設定は、**ドキュメント**フォルダーの内容をリダイレクトする方法を指定します。

デフォルトでは、内容は UNC パスにリダイレクトされます。

ドキュメントフォルダーの内容をリダイレクトする方法を制御するには、次のいずれかのオプションを選択します。

- 次の UNC パスにリダイレクトします。ドキュメントパスポリシー設定で指定された UNC パスにコンテンツをリダイレクトします。
- ユーザーのホームディレクトリにリダイレクトします。コンテンツをユーザーのホームディレクトリにリダイレクトします。これは通常、Active Directory のユーザーの #homeDirectory# 属性として構成されます。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

ダウンロードのポリシー設定

このセクションには、**ダウンロード**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

ダウンロードパス

この設定は、**ダウンロード**フォルダー内のファイルがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

ダウンロードのリダイレクト設定

この設定は、**ダウンロード**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツはUNCパスにリダイレクトされます。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

リンクポリシー設定

このセクションには、**リンク**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

リンクパス

この設定は、**リンク**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

リンクのリダイレクト設定

この設定は、**リンク**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツは UNC パスにリダイレクトされます。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

音楽ポリシー設定

このセクションには、**Music**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

音楽パス

この設定は、**Music**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

音楽のリダイレクト設定

この設定は、**Music**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツはUNCパスにリダイレクトされます。

Musicフォルダーのコンテンツをリダイレクトする方法を制御するには、次のいずれかのオプションを選択します。

- 次のUNCパスにリダイレクトします。Musicパスポリシー設定で指定されたUNCパスにコンテンツをリダイレクトします。
- ドキュメントフォルダーを基準にリダイレクトします。ドキュメントフォルダーを基準としたフォルダーにコンテンツをリダイレクトします。

Documentsフォルダーを基準としたフォルダーにコンテンツをリダイレクトするには、**Documents path**設定を有効にする必要があります。

ここでこの設定が構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

画像ポリシー設定

このセクションには、**画像**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

画像パス

この設定は、**画像**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

画像のリダイレクト設定

この設定は、**画像**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツは UNC パスにリダイレクトされます。

画像フォルダーのコンテンツをリダイレクトする方法を制御するには、次のいずれかのオプションを選択します。

- 次の UNC パスにリダイレクトします。コンテンツを「画像パス」ポリシー設定で指定された UNC パスにリダイレクトします。
- ドキュメントフォルダーを基準にリダイレクトします。コンテンツをドキュメントフォルダーを基準としたフォルダーにリダイレクトします。

コンテンツを**ドキュメント**フォルダーを基準としたフォルダーにリダイレクトするには、**ドキュメントパス**設定を有効にする必要があります。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

保存されたゲームのポリシー設定

このセクションには、**保存されたゲーム**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

保存されたゲームのリダイレクト設定

この設定は、**保存されたゲーム**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツはUNCパスにリダイレクトされます。

ここでこの設定が構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

保存されたゲームのパス

この設定は、**保存されたゲーム**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

Searchesポリシー設定

このセクションには、**Searches**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

SEARCHESのリダイレクト設定

この設定は、**Searches**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツはUNCパスにリダイレクトされます。

ここでこの設定が構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

SEARCHESパス

この設定は、**Searches**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

ビデオポリシー設定

このセクションには、**ビデオ**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

ビデオのリダイレクト設定

この設定は、**ビデオ**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツはUNCパスにリダイレクトされます。

ビデオフォルダーのコンテンツをリダイレクトする方法を制御するには、次のいずれかのオプションを選択します。

- 次のUNCパスにリダイレクトします。コンテンツを、ビデオパスポリシー設定で指定されたUNCパスにリダイレクトします。
- ドキュメントフォルダーを基準にリダイレクトします。コンテンツを、ドキュメントフォルダーを基準としたフォルダーにリダイレクトします。

コンテンツを**ドキュメント**フォルダーを基準としたフォルダーにリダイレクトするには、**ドキュメントパス**設定を有効にする必要があります。

この設定がここで構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

ビデオパス

この設定は、**ビデオ**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

この設定がここで構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

ログポリシー設定

このセクションには、Profile Management のログ記録を構成するポリシー設定が含まれています。

Active Directory のアクション

この設定は、Active Directory で実行されるアクションの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定が Web Studio で構成されていない場合、.ini ファイルの値が使用されます。

この設定が Web Studio または .ini ファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

一般情報

この設定は、一般情報の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

一般的な警告

この設定は、一般的な警告の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログの有効化**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログの有効化

この設定は、デバッグ（詳細ログ）モードでのProfile Managementログを有効または無効にします。デバッグモードでは、"%SystemRoot%\System32\Logfiles\UserProfileManager" にあるログファイルに詳細なステータス情報が記録されます。

デフォルトでは、この設定は無効になっており、エラーのみがログに記録されます。

Citrix®は、Profile Managementのトラブルシューティングを行う場合にのみ、この設定を有効にすることをお勧めします。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、エラーのみがログに記録されます。

ファイルシステムのアクション

この設定は、ファイルシステムで実行されたアクションの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログの有効化**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ファイルシステム通知

この設定は、ファイルシステム通知の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする際は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログオフ

この設定は、ユーザーログオフの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする際は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログオン

この設定は、ユーザーログオンの詳細ログ記録を有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログファイルの最大サイズ

この設定は、Profile Managementログファイルの最大許容サイズをバイト単位で指定します。

デフォルトでは、この値は1048576バイト（1 MB）に設定されています。

十分なディスク容量がある場合、Citrixはこのファイルのサイズを5 MB以上に増やすことを推奨します。ログファイルが最大サイズを超えて増加した場合：

- 既存のファイルのバックアップ（.bak）が削除されます
- ログファイルは.bakに名前が変更されます
- 新しいログファイルが作成されます

ログファイルは`%SystemRoot%\System32\Logfiles\UserProfileManager`に作成されます。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここで、または.iniファイルで構成されていない場合、デフォルト値が使用されます。

ログファイルへのパス

この設定は、Profile Managementログファイルを保存するための代替パスを指定します。

デフォルトでは、この設定は無効になっており、ログファイルはデフォルトの場所である%SystemRoot%\System32\Logfiles\UserProfileManagerに保存されます。

パスは、ローカルドライブまたはリモートのネットワークベースドライブ (UNCパス) を指すことができます。リモートパスは大規模な分散環境で役立つ場合がありますが、大量のネットワークトラフィックを生成する可能性があり、ログファイルには不適切かもしれません。永続的なハードドライブを持つプロビジョニングされた仮想マシンの場合は、そのドライブへのローカルパスを設定します。この設定により、マシンの再起動時にログファイルが保持されます。永続的なハードドライブを持たない仮想マシンの場合は、UNCパスを設定することでログファイルを保持できます。ただし、マシンのシステムアカウントはUNC共有への書き込みアクセス権を持っている必要があります。オフラインプロファイル機能によって管理されるラップトップには、ローカルパスを使用してください。

ログファイルにUNCパスを使用する場合、Citrixはログファイルフォルダーに適切なアクセス制御リストを適用することを推奨します。この設定により、承認されたユーザーまたはコンピューターアカウントのみが保存されたファイルにアクセスできるようになります。

ここでこの設定が構成されていない場合、.ini ファイルの値が使用されます。

ここまたは .ini ファイルでこの設定が構成されていない場合、デフォルトの場所 %SystemRoot%\System32\Logfiles\UserProfileManager が使用されます。

パーソナライズされたユーザー情報

この設定は、パーソナライズされたユーザー情報の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合、**ログの有効化**設定も有効になっていることを確認してください。

ここでこの設定が構成されていない場合、.ini ファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログオン時とログオフ時のポリシー値

この設定は、ユーザーがログオンおよびログオフするときのポリシー値の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合、**ログの有効化**設定も有効になっていることを確認してください。

ここでこの設定が構成されていない場合、.ini ファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

レジストリアクション

この設定は、レジストリで実行されたアクションの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする際は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログオフ時のレジストリの相違点

この設定は、ユーザーがログオフしたときのレジストリの相違点の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする際は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー

- 一般情報

プロファイル処理ポリシー設定

このセクションには、Profile Management がユーザープロファイルを処理する方法を指定するポリシー設定が含まれています。

キャッシュされたプロファイルを削除するまでの遅延

この設定は、Profile Management がログオフ時にローカルにキャッシュされたプロファイルを削除するまでの遅延を、分単位で任意に延長する時間を指定します。

値が 0 の場合、ログオフプロセスの終了時にプロファイルがすぐに削除されます。Profile Management は 1 分ごとにログオフをチェックします。その結果、値が 60 の場合、ユーザーがログオフしてから 1 ～ 2 分の間にプロファイルが削除されることが保証されます。このアクションは、最後のチェックがいつ行われたかによって異なります。ログオフ中にプロセスがファイルまたはユーザーレジストリハイブを開いたままにしていることがわかっている場合、遅延を延長すると便利です。大規模なプロファイルの場合、このプロセスはログオフを高速化することもできます。

デフォルトでは、この値は 0 に設定されており、Profile Management はローカルにキャッシュされたプロファイルをすぐに削除します。

この設定を有効にする場合は、「ログオフ時にローカルにキャッシュされたプロファイルを削除する」も有効になっていることを確認してください。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここまたは.iniファイルでこの設定が構成されていない場合、プロファイルはすぐに削除されます。

ログオフ時にローカルにキャッシュされたプロファイルを削除する

この設定は、ユーザーがログオフした後にローカルにキャッシュされたプロファイルが削除されるかどうかを指定します。

この設定が有効になっている場合、ユーザーのローカルプロファイルキャッシュはログオフ後に削除されます。Citrix® は、ターミナルサーバーに対してこの設定を有効にすることを推奨しています。

デフォルトでは、この設定は無効になっており、ユーザーのローカルプロファイルキャッシュはログオフ後も保持されます。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここまたは.iniファイルでこの設定が構成されていない場合、キャッシュされたプロファイルは削除されません。

ローカルプロファイルの競合処理

この設定は、ユーザープロファイルが以下の両方に存在する場合のProfile Managementの動作を構成します。

- ユーザーストア
- ローカルWindowsユーザープロファイル（Citrixユーザープロファイルではない）

デフォルトでは、Profile Management はローカルの Windows プロファイルを使用しますが、それを一切変更しません。

Profile Management の動作を制御するには、次のいずれかのオプションを選択します。

- ローカルプロファイルを使用する。Profile Management はローカルプロファイルを使用しますが、それを一切変更しません。
- ローカルプロファイルを削除する。Profile Management はローカルの Windows ユーザープロファイルを削除し、その後ユーザー ストアから Citrix ユーザープロファイルをインポートします。
- ローカルプロファイルの名前を変更する。Profile Management はローカルの Windows ユーザープロファイルの名前を変更し (バックアップ目的)、その後ユーザー ストアから Citrix ユーザープロファイルをインポートします。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がここで、または .ini ファイルで構成されていない場合、既存のローカルプロファイルが使用されます。

既存プロファイルの移行

この設定は、ユーザーがユーザー ストアに現在のプロファイルを持っていない場合に、ログオン中にユーザー ストアに移行されるプロファイルの種類を指定します。

ユーザーがユーザーストアにプロファイルを持っていない場合、Profile Managementはログオン中に既存のプロファイルを「その場で」移行できます。その後、以下の両方でユーザーストアプロファイルがProfile Managementによって使用されます。

- 現在のセッション
- 同じユーザー ストアへのパスで構成されたその他のセッション

デフォルトでは、ローカルプロファイルと移動プロファイルの両方がログオン中にユーザー ストアに移行されます。

ログオン中にユーザー ストアに移行されるプロファイルの種類を指定するには、次のいずれかのオプションを選択します。

- ローカルプロファイルと移動プロファイル
- ローカル
- ローミング
- なし (無効)

なしを選択すると、Profile Managementがインストールされていない環境であるかのように、システムは既存のWindowsメカニズムを使用してプロファイルを作成します。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、既存のローカルプロファイルとローミングプロファイルが移行されます。

既存のアプリケーションプロファイルの自動移行

この設定は、異なるオペレーティングシステム間で既存のアプリケーションプロファイルを自動的に移行するかどうかを有効または無効にします。アプリケーションプロファイルには、`AppData`フォルダー内のアプリケーションデータと、`HKEY_CURRENT_USER\SOFTWARE`の下のレジストリエントリの両方が含まれます。この設定は、異なるオペレーティングシステム間でアプリケーションプロファイルを移行したい場合に役立ちます。

たとえば、オペレーティングシステム（OS）をWindows 10バージョン1803からWindows 10バージョン1809にアップグレードするとします。この設定が有効になっている場合、各ユーザーが最初にログオンするときに、Profile Managementは既存のアプリケーション設定をWindows 10バージョン1809に自動的に移行します。その結果、`AppData`フォルダー内のアプリケーションデータとHKEY_CURRENT_USER\SOFTWAREの下のレジストリエントリが移行されます。

複数の既存のアプリケーションプロファイルがある場合、Profile Managementは次の優先順位で移行を実行します。

1. 同じOSタイプのプロファイル（シングルセッションOSからシングルセッションOS、マルチセッションOSからマルチセッションOS）。
2. 同じWindows OSファミリーのプロファイル（例：Windows 10からWindows 10、またはWindows Server 2016からWindows Server 2016）。

3. 以前のバージョンのOSのプロファイル（例：Windows 7からWindows 10、またはWindows Server 2012からWindows 2016）。
4. 最も近いOSのプロファイル。

注： ユーザーストアパスに変数「!CTX_OSNAME!」を含めることで、OSの短い名前を指定する必要があります。これにより、Profile Managementは既存のアプリケーションプロファイルを特定できます。

ここでこの設定が構成されていない場合、.iniファイルの設定が使用されます。

ここまたは.iniファイルでこの設定が構成されていない場合、デフォルトで無効になります。

テンプレートプロファイルへのパス

この設定は、Profile Managementがユーザープロファイルを作成するためのテンプレートとして使用するプロファイルへのパスを指定します。

指定されたパスは、NTUSER.DATレジストリファイルと、テンプレートプロファイルに必要なその他のフォルダーおよびファイルを含むフォルダーへの完全なパスである必要があります。

注: パスにNTUSER.DATを含めないでください。たとえば、ファイル`\\myservername\myprofiles\template\ntuser.dat`の場合、場所を`\\myservername\myprofiles\template`として設定します。

絶対パスを使用します。これはUNCパスまたはローカルマシン上のパスのいずれかです。後者を使用すると、たとえば、Citrix Provisioning™ Servicesイメージ上にテンプレートプロファイルを永続的に指定できます。相対パスはサポートされていません。

注: この設定は、Active Directory属性、システム環境変数、または`%USERNAME%`および`%USERDOMAIN%`変数の展開をサポートしていません。

デフォルトでは、この設定は無効になっており、新しいユーザープロファイルは、ユーザーが最初にログオンするデバイスのデフォルトユーザープロファイルから作成されます。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここまたは.iniファイルでこの設定が構成されていない場合、テンプレートは使用されません。

テンプレートプロファイルがローカルプロファイルを上書きする

この設定により、ユーザープロファイルの作成時にテンプレートプロファイルがローカルプロファイルを上書きできるようになります。

ユーザーがCitrixユーザープロファイルを持たず、ローカルのWindowsユーザープロファイルを持っているとします。この場合、この値が有効になっていると、デフォルトでローカルプロファイルが使用され、ユーザーストアに移行されます。このポリシー設定を有効にすると、ユーザープロファイルの作成時に使用されるローカルプロファイルをテンプレートプロファイルが上書きできるようになります。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

この設定がここまたは.iniファイルで構成されていない場合、テンプレートは使用されません。

テンプレートプロファイルが移動プロファイルを上書きする

この設定により、ユーザープロファイルの作成時にテンプレートプロファイルが移動プロファイルを上書きできるようになります。

ユーザーがCitrixユーザープロファイルを持たず、移動Windowsユーザープロファイルを持っているとします。この場合、この値が有効になっていると、デフォルトで移動プロファイルが使用され、ユーザーストアに移行されます。このポリシー設定を有効にすると、ユーザープロファイルの作成時に使用される移動プロファイルをテンプレートプロファイルが上書きできるようになります。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここまたは.iniファイルで構成されていない場合、テンプレートは使用されません。

すべてのログオンでCitrix必須プロファイルとして使用されるテンプレートプロファイル

この設定により、Profile Managementはテンプレートプロファイルをすべてのユーザープロファイルを作成するためのデフォルトプロファイルとして使用できるようになります。

デフォルトでは、この設定は無効になっており、新しいユーザープロファイルは、ユーザーが最初にログオンしたデバイスのデフォルトユーザープロファイルから作成されます。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここまたは.iniファイルで構成されていない場合、テンプレートは使用されません。

プロファイルコンテナのポリシー設定

プロファイルコンテナ

ユーザープロファイルに関連付けられた大きなフォルダーは、ログオンの遅延を引き起こします。Citrix Profile Managementは、プロファイルディスク（VHDXファイル）に含めるフォルダーを指定できるVHDXベースのプロファイルソリューションを提供します。このソリューションは、指定されたフォルダーをネットワークに保存されているプロファイルディスクにマッピングすること

で、ログオン時間を短縮します。プロファイルコンテナは、ログオン時にこれらのフォルダーを含むプロファイルディスクをアタッチするため、フォルダーのコピーをローカルプロファイルに保存する必要がなくなります。これにより、ログオン時間が短縮されます。

プロファイルコンテナのローカルキャッシュを有効にする

このポリシーは、Citrix Profile Managementプロファイルコンテナのローカルキャッシュサポートを有効にします。ポリシーが**有効**に設定されている場合、各ローカルプロファイルは、そのCitrix Profile Managementプロファイルコンテナのローカルキャッシュとして機能します。プロファイルストリーミングが使用されている場合、ローカルにキャッシュされたファイルはオンデマンドで作成されます。それ以外の場合は、ユーザーログオン時に作成されます。ローカルキャッシュ機能を使用するには、ユーザープロファイル全体をCitrix Profile Managementプロファイルコンテナに配置します。

プロファイルコンテナから除外するフォルダー

Citrix Profile Managementプロファイルコンテナから除外するフォルダーのリスト。

プロファイルコンテナに含めるフォルダー

親フォルダーが除外されている場合に、Citrix Profile Managementプロファイルコンテナに保持するフォルダーのリスト。

このリストのフォルダーは、除外されたフォルダーのサブフォルダーである必要があります。そうでない場合、この設定は機能しません。

プロファイルコンテナに含めるファイル

Citrix Profile Managementプロファイルコンテナに含めるファイルのリスト。

このリストのファイルは、除外されたフォルダー内にある必要があります。そうでない場合、この設定は機能しません。

プロファイルコンテナから除外するファイル

Citrix Profile Managementプロファイルコンテナから除外するファイルのリスト。

VHDディスクの圧縮を有効にする

Profile ManagementのVHDディスク圧縮を有効にできます。有効にすると、特定の条件が満たされたときに、ユーザーのログオフ時にVHDディスクが自動的に圧縮されます。このポリシーにより、プロファイルコンテナ、OneDriveコンテナ、およびミラーフォルダコンテナによって消費されるストレージスペースを節約できます。

必要性と利用可能なリソースに応じて、詳細設定にある「**VHDディスク圧縮をトリガーする空き領域の比率**」、「**VHDディスク圧縮をトリガーするログオフ回数**」、「**VHDディスク圧縮のデフ**

ラグを無効にする」の各ポリシーを使用して、デフォルトのVHD圧縮設定と動作を調整できます。

プロファイルコンテナのVHD自動拡張を有効にする

プロファイルコンテナのVHD自動拡張を有効にするかどうかを指定できます。有効にすると、すべてのVHD自動拡張設定がプロファイルコンテナに適用されます。

構成の優先順位:

- ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。
- ここでも.iniファイルでもこのポリシーが構成されていない場合、無効になります。

VHDコンテナへの排他的アクセスを有効にする

デフォルトでは、VHDコンテナは同時アクセスを許可します。この設定を有効にすると、一度に1つのアクセスのみが許可されます。この機能は、プロファイルコンテナとOneDriveコンテナに適用されます。

> **注:**
>
> コンテナベースのプロファイルソリューションでプロファイルコンテナに対してこの設定を有効にすると、「*プロファイルコンテナのマルチセッションライトバックを有効にする*」設定が自動的に無効になります。

> 構成の優先順位:

1. ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。
2. ここでも.iniファイルでもこのポリシーが構成されていない場合、設定は無効になります。

ログオン時にプロファイルコンテナが利用できない場合にユーザーをログオフする

ユーザーログオン時にプロファイルコンテナが利用できない場合にユーザーを強制的にログオフさせ、(オプションで)ユーザーに表示されるエラーメッセージをカスタマイズできます。

構成の優先順位:

1. ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。
2. ここでも.iniファイルでもこのポリシーが構成されていない場合、設定は無効になります。

プロファイルコンテナにアクセスするユーザーとグループ

プロファイルコンテナに対する`Read & Execute`権限を持つADドメインユーザーとグループを指定できます。デフォルトでは、プロファイルコンテナはその所有者のみがアクセスできます。

構成の優先順位:

1. このポリシーがここで構成されていない場合、.iniファイルの設定が使用されます。
2. このポリシーがここでも.iniファイルでも構成されていない場合、プロファイルコンテナはその所有者のみがアクセスできます。

BindLinkリダイレクトを有効にする

プロファイルコンテナ内のファイルシステムリダイレクトを処理するためにMicrosoft BindLink APIを使用するかどうかを指定します。この機能はデフォルトで無効になっており、Windows 11 24H2、Windows Server 2025、またはそれ以降（バージョン10.0.25314.0以降）でのみサポートされています。

レジストリポリシー設定

このセクションには、Profile Management の処理から含める、または除外するレジストリキーを指定するポリシー設定が含まれています。

除外リスト

ログオフ時に無視されるHKCUハイブ内のレジストリキーのリスト。

例: Software\Policies

このポリシーが無効になっている場合、レジストリキーは除外されません。ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、レジストリキーは除外されません。

包含リスト

ログオフ時に処理されるHKCUハイブ内のレジストリキーのリスト。

例: Software\Adobe。

このポリシーが有効になっている場合、このリストにあるキーのみが処理されます。このポリシーが無効になっている場合、HKCUハイブ全体が処理されます。ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、HKCUのすべてが処理されます。

デフォルトの除外リストを有効にする - Profile Management 5.5

ユーザープロファイルに同期されないHKCUハイブ内のレジストリキーのデフォルトリスト。このポリシーを使用して、GPO除外ファイルを手動で入力することなく指定できます。

このポリシーを無効にすると、Profile Management はデフォルトでレジストリキーを除外しません。ここでこのポリシーを構成しない場合、Profile Management は .ini ファイルの値を使用します。ここで、または .ini ファイルでこのポリシーを構成しない場合、Profile Management はデフォルトでレジストリキーを除外しません。

NTUSER.DATのバックアップ

NTUSER.DATの最後に正常だったコピーのバックアップを有効にし、破損がある場合にロールバックします。

ここでこのポリシーを構成しない場合、Profile Management は .ini ファイルの値を使用します。ここで、または .ini ファイルでこのポリシーを構成しない場合、Profile Management は NTUSER.DAT をバックアップしません。

アプリケーションアクセス制御ポリシー設定

ルールを使用して、ファイル、フォルダー、レジストリキー、および値へのユーザーアクセスを制御したり、ファイル、フォルダー、レジストリキー、および値に対するマシンレベルのリダイレクトを実装したりできます。

アプリケーションルールを作成するには、次の2つの方法があります。

- GUIベースのツール – **WEM Tool Hub > アプリケーションアクセス制御用ルールジェネレーター**
- PowerShellツール – Profile Managementインストールパッケージで利用可能

ストリーム配信ユーザープロファイルポリシー設定

このセクションには、Profile Management がストリーム配信ユーザープロファイルを処理する方法を指定するポリシー設定が含まれています。

常にキャッシュ

この設定は、ユーザーのログオン後、Profile Management がストリーム配信ファイルをできるだけ早くキャッシュするかどうかを指定します。ユーザーのログオン後にファイルをキャッシュすると、ネットワーク帯域幅が節約され、ユーザーエクスペリエンスが向上します。

この設定は、**プロファイルストリーミング**設定と組み合わせて使用します。

デフォルトでは、この設定は無効になっており、ユーザーのログオン後、ストリーム配信ファイルはできるだけ早くキャッシュされません。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも .ini ファイルでも構成されていない場合、無効になります。

常にキャッシュするサイズ

この設定は、ストリーム配信されるファイルのサイズの下限を MB 単位で指定します。Profile Management は、このサイズ以上のファイルを、ユーザーのログオン後できるだけ早くキャッシュします。

デフォルトでは、値は 0 (ゼロ) に設定されており、プロファイル全体をキャッシュする機能が使用されます。プロファイル全体をキャッシュする機能が有効になっている場合、Profile Management は、ユーザーのログオン後、ユーザーストア内のすべてのプロファイルコンテンツをバックグラウンドタスクとしてフェッチします。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも .ini ファイルでも構成されていない場合、無効になります。

プロファイルストリーミング

この設定は、Citrix® ストリーム配信ユーザープロファイル機能を有効または無効にします。有効にすると、プロファイルファイルとフォルダーは、ユーザーがログオン後にアクセスした場合にのみ、ユーザーストアからローカルコンピューターにフェッチされます。レジストリエントリと保留領域のファイルはすぐにフェッチされます。

デフォルトでは、プロファイルストリーミングは無効になっています。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも .ini ファイルでも構成されていない場合、無効になります。

ストリーム配信ユーザープロファイルグループ

この設定は、Windows ユーザーグループに基づいて、OU 内のどのユーザープロファイルをストリーム配信するかを指定します。

有効にすると、指定されたユーザーグループ内のユーザープロファイルのみがストリーミングされます。その他のすべてのユーザープロファイルは通常どおり処理されます。

デフォルトでは、この設定は無効になっており、OU内のすべてのユーザープロファイルは通常どおり処理されます。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、すべてのユーザープロファイルが処理されます。

プロファイルストリーミング除外を有効にする

プロファイルストリーミング除外が有効な場合：

- Profile Managementは、除外リスト内のフォルダーをストリーミングしません
- ユーザーがログオンすると、すべてのフォルダーがユーザーストアからローカルコンピューターに即座にフェッチされます

詳細については、「ユーザープロファイルのストリーム」を参照してください。

ペンディングエリアロックファイルのタイムアウト

この設定は、ストレージサーバーが応答しなくなったときにユーザーストアがロックされたままの場合、ペンディングエリアからユーザーストアにユーザーファイルが書き戻されるまでの日数を指定します。この動作により、ペンディングエリアの肥大化が防止され、ユーザーストアに常に最新のファイルが含まれることが保証されます。

デフォルトでは、この設定は1日（1）に設定されています。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、デフォルト値が使用されます。

ペンディングエリアのプロファイルストリーミングを有効にする

ペンディングエリア内のファイルとフォルダーに対してプロファイルストリーミング機能を有効にできます。

ペンディングエリアは、プロファイルストリーミングが有効になっている間、プロファイルの一貫性を確保するために使用されます。これは、同時セッションで変更されたプロファイルファイルとフォルダーを一時的に保存します。

既定では、このポリシーは無効になっており、ログオン時に保留領域内のすべてのファイルとフォルダーがローカルプロファイルにフェッチされます。このポリシーを有効にすると、保留領域内のファイルは要求されたときにのみローカルプロファイルにフェッチされます。このポリシーをプロファイルストリーミングポリシーと組み合わせて使用すると、同時セッションシナリオで最適なログオンエクスペリエンスを確保できます。

このポリシーは、フォルダーのプロファイルストリーミングを有効にするポリシーが有効になっている場合に、保留領域内のフォルダーに適用されます。

ユーザーパーソナライゼーションポリシー設定

Virtual Delivery Agent内でユーザーレイヤーのマウントを有効にするには、構成パラメータを使用して以下を指定します。

- ネットワーク上のどこでユーザーレイヤーにアクセスするか。
- 新しいユーザーレイヤーディスクがどのくらい大きくなるか。

そのため、利用可能なポリシーのリストには、次の2つのポリシーが表示されます。

- ユーザーレイヤーリポジトリパス - 「値」フィールドに「\\サーバー名またはアドレス\フォルダー名」の形式でパスを入力します。
- ユーザーレイヤーサイズGB - デフォルトのユーザーレイヤーサイズである10 GBは、Citrix®が推奨する最小値です。ユーザーレイヤーは、使用されるスペースに応じて設定されたサイズまで拡張されるシンプロビジョニングディスクです。ユーザーレイヤーのサイズが小さくなることはありません。

> **注:**
>
> ユーザーレイヤーサイズを増やすと、新しいユーザーレイヤーに影響を与え、既存のユーザーレイヤーを拡張します。レイヤーサイズを減らすと、新しいユーザーレイヤーにのみ影響します。既存のユーザーレイヤーのサイズが小さくなることはありません。

詳細については、「ユーザーパーソナライゼーションレイヤー」を参照してください。

Virtual Delivery Agent ポリシー設定

Virtual Delivery Agent (VDA) セクションには、VDA とサイトのコントローラー間の通信を制御するポリシー設定が含まれています。

重要: 自動更新機能を使用しない場合、VDA は Delivery Controller™ に登録するために、これらの設定によって提供される情報を必要とします。この情報は登録に必要であるため、VDA のインストール中にこの情報を提供しない限り、グループポリシーエディターを使用して以下の設定を構成する必要があります。

- コントローラー登録 IPv6 ネットマスク
- コントローラー登録ポート
- コントローラー SID
- コントローラー

- IPv6 コントローラー登録のみを使用
- サイト GUID

コントローラー登録 IPv6 ネットマスク

このポリシー設定により、管理者は VDA を優先サブネットのみに制限できます（グローバル IP が登録されている場合でも）。この設定は、VDA が登録する IPv6 アドレスとネットワークを指定します。VDA は、指定されたネットマスクに一致する最初のアドレスにのみ登録します。この設定は、「IPv6 コントローラー登録のみを使用」ポリシー設定が有効になっている場合にのみ有効です。

デフォルトでは、この設定は空白です。

コントローラー登録ポート

この設定は、**コントローラーの自動更新を有効にする** 設定が無効になっている場合にのみ使用してください。

この設定は、レジストリベースの登録を使用する際に、VDA がコントローラーに登録するために使用する TCP/IP ポート番号を指定します。

デフォルトでは、ポート番号は80に設定されています。

コントローラーSID

この設定は、**コントローラーの自動更新を有効にする**設定が無効になっている場合にのみ使用してください。

この設定は、VDAがレジストリベースの登録を使用する際にコントローラーに登録するために使用する、スペース区切りのコントローラーセキュリティ識別子（SID）のリストを指定します。この設定はオプションであり、登録に使用されるコントローラーのリストを制限するために**コントローラー**設定と組み合わせて使用される場合があります。

デフォルトでは、この設定は空白です。

コントローラー

この設定は、**コントローラーの自動更新を有効にする**設定が無効になっている場合にのみ使用してください。

この設定は、VDAがレジストリベースの登録を使用する際にコントローラーに登録するために使用する、スペース区切りのコントローラー完全修飾ドメイン名（FQDN）のリストを指定します。

この設定はオプションであり、**コントローラーSID**設定と組み合わせて使用される場合があります。

デフォルトでは、この設定は空白です。

コントローラーの自動更新を有効にする

この設定により、VDAはインストール後にコントローラーに自動的に登録できるようになります。

VDAが登録されると、登録先のコントローラーは現在のコントローラーFQDNとSIDのリストをVDAに送信します。VDAはこのリストを永続ストレージに書き込みます。各コントローラーは、90分ごとにサイトデータベースをチェックしてコントローラー情報を確認します。以下のいずれかの状況が発生した場合、コントローラーは登録済みのVDAに更新されたリストを送信します。

- 前回のチェック以降にコントローラーが追加または削除された場合
- ポリシーの変更が発生した場合

VDAは、受信した最新のリストにあるすべてのコントローラーからの接続を受け入れます。

デフォルトでは、この設定は有効になっています。

IPv6コントローラー登録のみを使用

この設定は、VDAがControllerに登録するために使用するアドレス形式を制御します。

- 有効にすると、VDAはマシンのIPv6アドレスを使用してControllerに登録します。VDAがControllerと通信する場合、次のアドレス順序を使用します: グローバルIPアドレス、ユニークローカルアドレス (ULA)、リンクローカルアドレス (他のIPv6アドレスが利用できない場合)。
- 無効にすると、VDAはマシンのIPv4アドレスを使用してControllerに登録し、通信します。

デフォルトでは、この設定は無効になっています。

サイトGUID

この設定は、**コントローラーの自動更新を有効にする**設定が無効になっている場合にのみ使用してください。

この設定は、Active Directoryベースの登録を使用する際に、VDAがControllerに登録するために使用するサイトのグローバル一意識別子 (GUID) を指定します。

デフォルトでは、この設定は空白です。

HDX™ 3D Pro ポリシー設定

HDX 3D Proセクションには、ユーザー向けの画質構成ツールを有効化および構成するためのポリシー設定が含まれています。このツールを使用すると、ユーザーは利用可能な帯域幅の使用を最適化できます。この最適化のために、画質と応答性のバランスがリアルタイムで調整されます。

ロスレスを有効にする

この設定は、ユーザーが画質構成ツールを使用してロスレス圧縮を有効または無効にできるかどうかを指定します。デフォルトでは、ユーザーにロスレス圧縮を有効にするオプションは提供されません。

ユーザーがロスレス圧縮を有効にしたとします。この場合、画質は画質構成ツールで利用可能な最大値に自動的に設定されます。デフォルトでは、ユーザーデバイスとホストコンピューターの機能に応じて、GPUベースまたはCPUベースの圧縮のいずれかを使用できます。

HDX 3D Pro 品質設定

この設定は、画質構成ツールでユーザーが利用できる最小値と最大値を指定します。これらの値を使用すると、画質構成ツールで画質調整の範囲を定義できます。

画質の値は0から100（両端を含む）の間で指定します。最大値は最小値以上である必要があります。

監視ポリシー設定

「**監視**」セクションには、プロセス、リソース監視、およびアプリケーション障害監視のポリシー設定が含まれています。

これらのポリシーのスコープは、以下に基づいて定義できます。

- サイト
- デリバリーグループ
- デリバリーグループの種類
- 組織単位
- タグ

プロセスおよびリソース監視のポリシー

CPU、メモリ、およびプロセスの各データポイントはVDAから収集され、監視データベースに保存されます。VDAからデータポイントを送信するとネットワーク帯域幅を消費し、それらを保存すると監視データベースの相当なスペースを消費します。特定のスコープ（たとえば、特定のデリバリーグループまたは組織単位）に対して、リソースデータまたはプロセスデータ、あるいはその

両方を監視したくない場合を考慮してください。この場合、ポリシーを無効にすることをお勧めします。

プロセス監視を有効にする

この設定を有効にすると、VDAがインストールされているマシンで実行されているプロセスを監視できます。CPU使用率やメモリ使用量などの統計情報は、監視サービスに送信されます。これらの統計情報は、Directorでのリアルタイム通知および履歴レポートに使用されます。

この設定のデフォルトは無効です。

リソース監視を有効にする

この設定を有効にすると、VDAがインストールされているマシンで重要なパフォーマンスカウンターを監視できます。統計情報（CPU使用率、メモリ使用量、IOPS、ディスク待機時間データなど）は監視サービスに送信されます。これらの統計情報は、Directorでのリアルタイム通知および履歴レポートに使用されます。

この設定のデフォルトは有効です。

スケーラビリティ

CPUおよびメモリデータは、各VDAから5分間隔でデータベースにプッシュされます。プロセスデータ（有効な場合）は10分間隔でデータベースにプッシュされます。IOPSおよびディスク待機時間データは1時間間隔でデータベースにプッシュされます。

CPUとメモリデータ

CPUとメモリデータは、デフォルトで**有効**です。データ保持期間の値は次のとおりです (Platinumライセンス):

データ粒度	日数
5分データ	1日
10分データ	7日
時間データ	30日
日次データ	90日

IOPSとディスク待機時間データ

IOPSとディスク待機時間データは、デフォルトで**有効**です。データ保持期間の値は次のとおりです (Platinumライセンス):

データ粒度	日数
時間データ	3日間
日次データ	90日間

データ保持設定では、1つのVDAに対して1年間、以下を保存するために約276 KBのディスク容量が必要です。

- CPU
- メモリ
- IOPS
- ディスク遅延データ

マシン数	必要なストレージ容量（概算）
1	276 KB
1K	270 MB
40K	10.6 GB

プロセスデータ

プロセスデータはデフォルトで**無効**です。必要に応じて、一部のマシンでプロセスデータを有効にすることをお勧めします。プロセスデータのデフォルトのデータ保持設定は次のとおりです。

データ粒度	日数
10分データ	1日
1時間データ	7日

プロセスデータがデフォルトの保持設定で有効になっている場合、プロセスデータは1年間でVDAあたり約1.5 MB、ターミナルサービスVDA (TS VDA) あたり3 MBを消費します。

マシン数	必要なストレージの目安 VDA	必要なストレージの目安 TS VDA
1	1.5 MB	3 MB

マシン数	必要なストレージの目安 VDA	必要なストレージの目安 TS VDA
1K	1.5 GB	3 GB

注:

以前に提示された数値には、インデックス領域は含まれていません。また、すべての計算は概算であり、展開によって異なります。

オプションの構成

必要に応じて、デフォルトの保持設定を変更できます。ただし、この構成は追加のストレージを消費します。以下の設定を有効にすることで、プロセス使用率データの精度を高めることができます。有効にできる構成は次のとおりです。

ENABLEMINUTELEVELGRANULARITYPROCESSUTILIZATION

ENABLEDAYLEVELGRANULARITYPROCESSUTILIZATION

これらの構成は、監視PowerShellコマンドレットから有効にできます: Set-MonitorConfiguration

アプリケーション障害監視のポリシー

デフォルトでは、**アプリケーション障害**タブには、マルチセッションOS VDAからのアプリケーション障害のみが表示されます。アプリケーション障害監視の設定は、以下の監視ポリシーで変更できます。

アプリケーション障害の監視を有効にする

この設定を使用して、アプリケーション障害監視を構成し、アプリケーションエラーまたは障害（クラッシュおよび未処理の例外）、あるいはその両方を監視します。 **値**を**None**に設定すると、アプリケーション障害監視が無効になります。 この設定のデフォルトは「アプリケーション障害のみ」です。

シングルセッションOS VDAでのアプリケーション障害の監視を有効にする

デフォルトでは、マルチセッションOS VDAでホストされているアプリケーションからの障害のみが監視されます。シングルセッションOS VDAを監視するには、ポリシーを**Allowed**に設定します。 この設定のデフォルトは**Prohibited**です。

障害監視から除外されるアプリケーションのリスト

障害監視の対象としないアプリケーションのリストを指定します。 デフォルトでは、このリストは空です。

Analytics 用データ収集のポリシー

ANALYTICS 用 VDA データ収集

このポリシーを使用して、パフォーマンスおよびセキュリティ分析のために、Monitor サービスが VDA のパフォーマンスおよびセキュリティ関連のメトリックを収集するかどうかを有効または無効にします。デフォルトでは、このポリシーは**許可**されています。VDA からのデータ収集を停止するには、ポリシーを**禁止**に設定します。

セキュリティ監視のためのクリップボード場所メタデータ収集

このポリシーを使用して、セキュリティ監視、監査、およびコンプライアンスのために、Broker サービスによるクリップボード場所メタデータ収集を有効または無効にします。デフォルトでは、このポリシーは**有効**です。VDA からのデータ収集を停止するには、ポリシーを**無効**に設定します。

パフォーマンス監視のための診断データ収集

このポリシーを使用して、監視サービスがセッション情報、UPM/EUEM サービスの状態、Microsoft Teams の最適化、接続プロトコルなどの診断データを収集できるようにします。デフォルトでは、このポリシーは**有効**です。VDA からのデータ収集を停止するには、ポリシーを**無効**に設定します。

ストレージ計画のヒント

グループポリシー。リソースデータまたはプロセスデータの監視に関心がない場合は、グループポリシーを使用して、いずれかまたは両方をオフにすることができます。詳しくは、「ポリシーの作成」の**「グループポリシー」**セクションを参照してください。

データグルーミング。デフォルトのデータ保持設定を変更して、データを早期にグルーミングし、ストレージスペースを解放できます。グルーミング設定について詳しくは、「API を使用したデータアクセス」の「データの粒度と保持」を参照してください。

仮想IPポリシー設定

> **重要:**

- Windows 10 Enterprise multi-session は Remote Desktop IP Virtualization (Virtual IP) をサポートしていません。また、Windows 10 Enterprise multi-session では Remote Desktop IP Virtualization または仮想ループバックをサポートしていません。
- リモートデスクトップIP仮想化 (仮想IP) は、クラウドホスト型マシンではサポートされていません。詳細については、Microsoftドキュメントを参照してください。

> **仮想IP**セクションには、セッションが独自の仮想ループバックアドレスを持つかどうかを制御するポリシー設定が含まれています。

仮想IPループバックのサポート

この設定が有効な場合、各セッションは独自の仮想ループバックアドレスを持ちます。無効な場合、セッションは個別のループバックアドレスを持ちません。

デフォルトでは、この設定は無効になっています。

仮想IP仮想ループバックプログラムリスト

この設定は、仮想ループバックアドレスを使用できるアプリケーション実行可能ファイルを指定します。プログラムをリストに追加する際は、実行可能ファイル名のみを指定してください。完全なパスを指定する必要はありません。

デフォルトでは、実行可能ファイルは指定されていません。

仮想IPループバックポートの除外

アプリケーションがこの設定で指定されたポート上のループバックアドレスを呼び出す場合、仮想ループバックは呼び出しをセッション固有のループバックアドレスに変更しません。

Workspace Environment Management™ のポリシー設定

Workspace Environment Management (WEM) セクションには、WEM エージェントの動作を管理するのに役立つポリシー設定が含まれています。

(WEM サービスのみ) エージェントプロキシ構成

現在、DaaS 展開でのみ利用可能です。

WEM エージェントが Citrix Cloud と通信するために使用するプロキシサーバーを指定します。形式: `http://<FQDN or IP address>:<port number>` (例: `<http://10.108.125.51:8080>`)。

(オンプレミス WEM のみ) エージェントサービスポート

現在、DaaS 展開でのみ利用可能です。

WEM エージェントが WEM インフラストラクチャサーバーに接続するために使用するポートを指定します。デフォルトポートは **8286** で、`AgentPort` コマンドライン引数に対応します。

(オンプレミス WEM のみ) キャッシュデータ同期ポート

現在、DaaS 展開でのみ利用可能です。

(WEM 1912 以降に適用) WEM エージェントがローカルキャッシュを WEM インフラストラクチャサーバーと同期するために使用するポートを指定します。デフォルトポートは **8288** で、`CachedDataSyncPort` コマンドライン引数に対応します。

(WEM サービスのみ) Citrix Cloud Connector

WEM エージェントが接続する Citrix Cloud Connector マシンを指定します。高可用性を確保するために、各リソースの場所に少なくとも 2 つの Cloud Connector を展開してください。Cloud Connector とエージェントマシンが同じ AD ドメインにあることを確認してください。

基本展開のカスタム設定

現在、DaaS 展開でのみ利用可能です。

基本的な展開に使用されるエージェント設定をカスタマイズします。利用可能な設定の詳細については、Workspace Environment Managementのドキュメントを参照してください。

(WEMサービスのみ) CVADサービスからCitrix Cloud Connectorを検出する

現在、DaaS展開でのみ利用可能です。

Cloud Connectorが構成されていない場合に、WEMエージェントがCitrix DaaS展開からCloud Connectorを自動的に検出できるようにします。検出が成功すると、エージェントは対応するCloud Connectorマシンに接続します。

重要: この設定は、エージェントのインストール中にCloud Connectorが構成された場合、または **Citrix Cloud Connectors**ポリシー設定がすでに有効になっている場合には適用されません。

(オンプレミスWEMのみ) インフラストラクチャサーバー

現在、DaaS展開でのみ利用可能です。

WEMインフラストラクチャサーバーの完全修飾ドメイン名 (FQDN) またはIPアドレスを指定します。WEMエージェントはこのサーバーに接続して、構成を取得し、ローカルキャッシュを更新し、監視データを報告します。

エージェント展開タイプを上書きする

現在、DaaS展開でのみ利用可能です。

デフォルトのWEMエージェント展開タイプを上書きします。次のいずれかのオプションを選択してください。

- クラウドサービス – エージェントをCitrix CloudのWEMサービスに接続し、WEMの全機能を提供します。
- オンプレミス – エージェントをオンプレミスのWEM展開に接続し、WEMの全機能を提供します。
- 基本的な展開 – WEMを単一マシンモードで、限られた機能で実行し、WEMインフラストラクチャには接続しません。
- 無効 – エージェントがインストールされているマシン上のすべてのWEM機能を無効にします。

レジストリを使用してCOMポートおよびLPTポートリダイレクト設定を構成する

VDAバージョン7.0から7.8では、**COMポートおよびLPTポート**設定は、レジストリを使用してのみ構成できます。VDAバージョン7.0より前、およびVDAバージョン7.9以降では、これらの設定はWeb Studioで構成できます。詳しくは、「ポートリダイレクトポリシー設定」および「帯域幅ポリシー設定」を参照してください。

COMポートおよびLPTポートリダイレクトのポリシー設定は、VDAイメージまたはマシン上のHKLM\Software\Citrix\GroupPolicy\Defaults\Deprecatedにあります。

COMポートおよびLPTポートリダイレクトを有効にするには、次のようにREG_DWORD型の新しいレジストリキーを追加します。

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

レジストリキー	説明	許可される値
AllowComPortRedirection	COMポートリダイレクトを許可または禁止する	1 (許可) または 0 (禁止)
LimitComBw	COMポートリダイレクトチャネルの帯域幅制限	数値

レジストリキー	説明	許可される値
LimitComBWPercent	COMポートリダイレクトチャネルの帯域幅制限（セッションの総帯域幅に対する割合）	0から100までの数値
AutoConnectClientComPorts	ユーザーデバイスからCOMポートを自動的に接続する	1 (許可) または 0 (禁止)
AllowLptPortRedirection	LPTポートリダイレクトを許可または禁止する	1 (許可) または 0 (禁止)
LimitLptBw	LPTポートリダイレクトチャネルの帯域幅制限	数値
LimitLptBwPercent	LPTポートリダイレクトチャネルの帯域幅制限（セッション全体の帯域幅に対する割合）	0から100までの数値
AutoConnectClientLptPorts	ユーザーデバイスからLPTポートを自動的に接続する	1 (許可) または 0 (禁止)

これらの設定を構成した後、マシンカタログを変更して、新しいマスターイメージまたは更新された物理マシンを使用するようにします。デスクトップは、ユーザーが次回ログオフしたときに新しい設定で更新されます。

デフォルトのポリシー設定

以下の表に、ポリシー設定、そのデフォルト値、およびそれらが適用されるVirtual Delivery Agent (VDA) のバージョンを示します。

ICA®

名前	デフォルト設定	VDA
アダプティブトランスポート	オフ。優先される場合に使用します	VDA 7.13～7.15、VDA 7.16以降
クライアントクリップボードリダイレクト	許可	すべてのVDAバージョン

名前	デフォルト設定	VDA
クライアントクリップボード書き込み許可形式	形式は指定されていません	VDA 7.6以降
デスクトップの起動	禁止	マルチセッションOS用VDA 7以降
ICAリスナーポート番号	1494	すべてのVDAバージョン
クライアント接続中の非公開プログラムの起動	禁止	マルチセッションOS用VDA 7以降
クリップボードのクライアントからセッションへの転送サイズを制限する	無効	VDA 2009
クリップボードのセッションからクライアントへの転送サイズを制限する	無効	VDA 2009
ロス許容モード	許可	VDA 2003。注: 損失許容モードはまだ利用できません。VDA のこのバージョンは、利用可能になった時点でこれをサポートします。
ロス許容しきい値	損失許容モードが利用可能な場合: パケット損失: 5%、遅延: 300 ms (RTT)	VDA 2003 以降
Rendezvous プロトコル	無効	Citrix Cloud を介して確立された HDX セッションにのみ適用されます。
クライアントクリップボードへの書き込みを制限する	禁止	VDA 7.6 以降
セッションクリップボードへの書き込みを制限する	禁止	VDA 7.6 以降
セッションクリップボード書き込み許可形式	形式は指定されていません	VDA 7.6 以降

名前	デフォルト設定	VDA
タブレットモードの切り替え	有効	VDA 7.16 以降; VDA 7.14 および 7.15 LTSR の場合、この設定はレジストリを使用して構成します。
仮想チャネル許可リスト	有効	VDA 2109 以降
セッションメトリックの収集	許可	7.42 から現在まで

ICA/Adobe Flash 配信/Flash リダイレクト

名前	デフォルト設定	VDA
Flashビデオのフォールバック防止	未構成	VDA 7.6 FP3 から現在まで
Flashビデオのフォールバック防止エラー *.swf	VDA 7.6 FP3 から現在まで	

ICA/オーディオ

名前	デフォルト設定	VDA
アダプティブオーディオ	有効	Citrix Virtual Apps and Desktops™ 2109以降を使用するVDAの、シングルセッションOSおよびマルチセッションOSの両方のセッションに適用されます。
UDPリアルタイムトランスポート経由のオーディオ	許可	すべてのVDAバージョン
オーディオプラグアンドプレイ	許可	マルチセッションOS用VDA 7 から現在まで
オーディオ品質	高 - 高精細オーディオ	すべてのVDAバージョン
クライアントオーディオリダイレクト	許可	すべてのVDAバージョン

名前	デフォルト設定	VDA
クライアントマイクのリダイレクト	許可	すべてのVDAバージョン
オーディオのロストレラントモード	禁止	VDAバージョン2411以前

ICA/自動クライアント再接続

名前	デフォルト設定	VDA
自動クライアント再接続	許可	すべてのVDAバージョン
自動クライアント再接続認証	認証を要求しない	すべてのVDAバージョン
自動クライアント再接続ログ	自動再接続イベントをログに記録しない	すべてのVDAバージョン
自動クライアント再接続タイムアウト	120秒	VDA 7.13から現在まで
再接続UIの透過レベル	80%	VDA 7.13 から現在まで

ICA/帯域幅

名前	デフォルト設定	VDA
オーディオリダイレクトの帯域幅制限	ゼロ Kbps	すべてのVDAバージョン
オーディオリダイレクトの帯域幅制限（パーセント）	0	すべてのVDAバージョン
クライアントUSBデバイスリダイレクトの帯域幅制限	ゼロ Kbps	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7 から現在まで、シングルセッションOS用VDA 7 から現在まで
クライアントUSBデバイスリダイレクトの帯域幅制限（パーセント）	0	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7 から現在まで、シングルセッションOS用VDA 7 から現在まで

名前	デフォルト設定	VDA
クリップボードリダイレクトの帯域幅制限	ゼロ Kbps	すべてのVDAバージョン
クリップボードリダイレクトの帯域幅制限（パーセント）	0	すべてのVDAバージョン
COMポートリダイレクトの帯域幅制限	0 キロビット/秒	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します。
COMポートリダイレクトの帯域幅制限（パーセント）	0	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します。
ファイルリダイレクト帯域幅制限	0 キロビット/秒	すべてのVDAバージョン
ファイルリダイレクトの帯域幅制限（パーセント）	0	すべてのVDAバージョン
HDX MediaStreamマルチメディアアクセラレーション帯域幅制限	ゼロ Kbps	VDA 5.5、5.6 FP1、Multi-session OS用VDA 7およびSingle-session OS用VDA 7から現在のMulti-session OS用VDAおよびSingle-session OS用VDA
HDX MediaStreamマルチメディアアクセラレーション帯域幅制限パーセント	0	VDA 5.5、5.6 FP1、VDA for Multi-session OS 7から現在まで、VDA for Single-session OS 7から現在まで
LPTポートリダイレクト帯域幅制限	ゼロ Kbps	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します。
LPTポートリダイレクトの帯域幅制限（パーセント）	0	すべてのVDAバージョン。VDA 7.0から7.8までは、レジ

名前	デフォルト設定	VDA
		ストリを使用してこの設定を構成します。
セッション全体の帯域幅制限	0 キロビット/秒	すべてのVDAバージョン
プリンターリダイレクト帯域幅制限	0 キロビット/秒	すべてのVDAバージョン
プリンターリダイレクトの帯域幅制限（パーセント）	0	すべてのVDAバージョン
TWAINデバイスリダイレクト帯域幅制限	0 キロビット/秒	VDA 5.5、5.6 FP1、Multi-session OS 用 VDA 7 以降、Single-session OS 用 VDA 7 以降
TWAINデバイスリダイレクト帯域幅制限の割合	0	VDA 5.5、5.6 FP1、Multi-session OS 用 VDA 7 以降、Single-session OS 用 VDA 7 以降

ICA/双方向コンテンツリダイレクト

名前	デフォルト設定	VDA
双方向コンテンツリダイレクトを許可する	禁止	VDA 7.13 以降
クライアントにリダイレクトを許可するURL	空	VDA 7.13 から現在まで
VDAにリダイレクトされる許可されたURL	空	VDA 7.13 から現在まで
双方向コンテンツリダイレクトの構成	無効	VDA 2311 から現在まで

ICA/ブラウザコンテンツリダイレクト

名前	デフォルト設定	VDA
ブラウザコンテンツリダイレクト	許可	VDA 7.16 から現在まで
ブラウザコンテンツリダイレクトACL構成	`https://www.youtube.com/*`	VDA 7.16 から現在まで
ブラウザコンテンツリダイレクト統合Windows認証のサポート	禁止	VDA 2106 から現在まで
ブラウザコンテンツリダイレクトプロキシ構成	空	VDA 7.16 から現在まで
ブラウザコンテンツリダイレクトサーバーフェッチWebプロキシ認証	禁止	VDA 2012から現在まで

ICA/クライアントセンサー

名前	デフォルト設定	VDA
アプリケーションによるクライアントデバイスの物理的な場所の使用を許可する	禁止	VDA 5.6 FP1、マルチセッションOS用VDA 7から現在まで、シングルセッションOS用VDA 7から現在まで

ICA/デスクトップUI

名前	デフォルト設定	VDA
デスクトップコンポジションリダイレクト	無効 (7.6 FP3から現在まで); 有効 (5.6から7.6 FP2まで)	VDA 5.6、シングルセッションOS用VDA 7から7.15まで
デスクトップコンポジションリダイレクトのグラフィック品質	中	VDA 5.6、シングルセッションOS用VDA 7から7.15まで
デスクトップの壁紙	許可	すべてのVDAバージョン

名前	デフォルト設定	VDA
メニューアニメーション	許可	すべてのVDAバージョン
ドラッグ中にウィンドウの内容を表示	許可	すべてのVDAバージョン

ICA/エンドユーザー監視

名前	デフォルト設定	VDA
ICAラウンドトリップ計算	有効	すべてのVDAバージョン
ICAラウンドトリップ計算間隔	15秒	すべてのVDAバージョン
アイドル接続のICAラウンドトリップ計算	無効	すべてのVDAバージョン

ICA/強化されたデスクトップエクスペリエンス

名前	デフォルト設定	VDA
強化されたデスクトップエクスペリエンス	許可	マルチセッションOS 7以降のVDA

ICA/ファイルリダイレクト

名前	デフォルト設定	VDA
クライアントドライブの自動接続	許可	すべてのVDAバージョン
クライアントドライブのリダイレクト	許可	すべてのVDAバージョン
クライアント固定ドライブ	許可	すべてのVDAバージョン
クライアントフロッピードライブ	許可	すべてのVDAバージョン
クライアントネットワークドライブ	許可	すべてのVDAバージョン

名前	デフォルト設定	VDA
クライアント光学ドライブ	許可	すべてのVDAバージョン
クライアントリムーバブルドライブ	許可	すべてのVDAバージョン
ホストからクライアントへのリダイレクト	無効	マルチセッションOS向けVDA 7以降
クライアントドライブ文字を保持する	無効	VDA 5、5.5、5.6 FP1、シングルセッションOS向けVDA 7以降
読み取り専用クライアントドライブアクセス	無効	VDA 5.5、5.6 FP1、マルチセッションOS向けVDA 7以降、シングルセッションOS向けVDA 7以降
特殊フォルダーのリダイレクト	許可	Web Interface展開のみ。マルチセッションOS向けVDA 7以降
非同期書き込みを使用する	無効	すべてのVDAバージョン

ICA/グラフィック

名前	デフォルト設定	VDA
視覚的にロスレスな圧縮を許可する	無効	VDA 7.6以降
表示メモリ制限	65,536 Kb	VDA 5、5.5、5.6 FP1、シングルセッションOS向けVDA 7以降
ディスプレイモードの劣化設定	最初に色深度を劣化させる	すべてのVDAバージョン
動的ウィンドウプレビュー	有効	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

名前	デフォルト設定	VDA
グラフィックステータスインジケーター	無効	VDA 7.16以降
イメージキャッシュ	有効	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
レガシーグラフィックモード	無効	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
許可される最大色深度	32ビット/ピクセル	すべてのVDAバージョン
ディスプレイモードが劣化した場合にユーザーに通知する	無効	マルチセッションOS用VDA 7以降
3Dグラフィックワークロード向けに最適化	無効	VDA 7.17から現在まで
キューイングとトッシング	有効	すべてのVDAバージョン
画面共有	無効	VDA 2112
圧縮にビデオコーデックを使用	優先される場合にビデオコーデックを使用	VDA 7.6 FP3から現在まで
ビデオコーデックにハードウェアエンコードを使用	有効	VDA 7.11から現在まで

ICA/グラフィック/キャッシュ

名前	デフォルト設定	VDA
永続キャッシュしきい値	3,000,000 ビット/秒	マルチセッションOS用VDA 7から現在まで

ICA/グラフィック/Framehawk

名前	デフォルト設定	VDA
Framehawkディスプレイチャネル	無効	VDA 7.6 FP2 以降
Framehawkディスプレイチャネルのポート範囲	3224,3324	VDA 7.6 FP2 以降

ICA/キープアライブ

名前	デフォルト設定	VDA
ICAキープアライブタイムアウト	60秒	すべてのVDAバージョン
ICAキープアライブ	ICAキープアライブメッセージを送信しない	すべてのVDAバージョン

ICA/キーボードおよびIME

名前	デフォルト設定	VDA
クライアントキーボードレイアウト同期およびIMEの改善	無効	1912 LTSR CU2 以降にのみ適用されます。
Unicodeキーボードレイアウトマッピング	許可 (2407, 2411, 2503); 禁止 (以前のバージョン, 2507)	1912 LTSR CU2以降にのみ適用されます。
キーボードレイアウト切り替えポップアップメッセージボックスを非表示にする	禁止	1912 LTSR CU2以降にのみ適用されます。

ICA/ローカルアプリアクセス

名前	デフォルト設定	VDA
ローカルアプリアクセスを許可	禁止	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

名前	デフォルト設定	VDA
URLリダイレクトブロックリスト	サイトは指定されていません	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
URLリダイレクト許可リスト	サイトは指定されていません	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ICA/モバイルエクスペリエンス

名前	デフォルト設定	VDA
自動キーボード表示	禁止	VDA 5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
タッチ最適化デスクトップの起動	許可	VDA 5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降。この設定は無効になっており、Windows 10およびWindows Server 2016マシンでは利用できません。
コンボボックスのリモート処理	禁止	VDA 5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ICA/マルチメディア

名前	デフォルト設定	VDA
HTML5ビデオリダイレクト	禁止	VDA 7.12以降
ビデオ品質の制限	未構成	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

名前	デフォルト設定	VDA
Microsoft Teamsリダイレクト	許可	マルチセッションOS用VDA 1906以降、シングルセッションOS用VDA 1906以降。
マルチメディア会議	許可	すべてのVDAバージョン
WAN経由のWindows Media マルチメディアリダイレクトの最適化	許可	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
WAN経由のWindows Media マルチメディアリダイレクトの最適化にGPUを使用	禁止	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
Windows Mediaフォールバックの防止	未構成	VDA 7.6 FP3以降
Windows Mediaクライアント側コンテンツフェッチ	許可	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
Windows Mediaリダイレクト	許可	すべてのVDAバージョン
Windows Mediaリダイレクトバッファサイズ	5秒	VDA 5、5.5、5.6 FP1から現在まで
Windows Mediaリダイレクトバッファサイズの使用	無効	VDA 5、5.5、5.6 FP1から現在まで

ICA/マルチストリーム接続

名前	デフォルト設定	VDA
UDP経由のオーディオ	許可	VDA for Multi-session OS 7から現在まで
オーディオUDPポート範囲	16500、16509	VDA 5.5、5.6 FP1、VDA for Multi-session OS 7から現在まで、VDA for Single-session OS 7から現在まで

名前	デフォルト設定	VDA
マルチポートポリシー	プライマリポート (2598) は高優先度	VDA 5.5、5.6 FP1、VDA for Multi-session OS 7から現在まで、VDA for Single-session OS 7から現在まで
マルチストリーム コンピューター設定	無効	VDA 5.5、5.6 FP1、VDA for Multi-session OS 7から現在まで、VDA for Single-session OS 7から現在まで
マルチストリーム ユーザー設定	無効	VDA 5.5、5.6 FP1、VDA for Multi-session OS 7から現在まで、VDA for Single-session OS 7から現在まで
マルチストリーム仮想チャネルストリーム割り当て設定	デフォルトのストリーム割り当てについては、マルチストリーム仮想チャネル割り当て設定を参照してください。	VDA 2003

ICA/ポートリダイレクト

名前	デフォルト設定	VDA
クライアントCOMポートの自動接続	無効	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します
クライアントLPTポートの自動接続	無効	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します
クライアントCOMポートリダイレクト	禁止	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します
クライアントLPTポートリダイレクト	禁止	すべてのVDAバージョン。VDA 7.0から7.8までは、レジ

名前	デフォルト設定	VDA
		ストリを使用してこの設定を構成します

ICA/印刷

名前	デフォルト設定	VDA
クライアントプリンターリダイレクト	許可	すべてのVDAバージョン
デフォルトプリンター	デフォルトプリンターをクライアントのメインプリンターに設定する	すべてのVDAバージョン
プリンターの割り当て	ユーザーの現在のプリンターがセッションのデフォルトプリンターとして使用されます	すべてのVDAバージョン
プリンターの自動作成イベントログの優先順位	エラーと警告をログに記録	すべてのVDAバージョン
セッションプリンター	プリンターが指定されていません	すべてのVDAバージョン
プリンターが作成されるまで待機する (デスクトップ)	無効	すべてのVDAバージョン

ICA/印刷/クライアントプリンター

名前	デフォルト設定	VDA
クライアントプリンターを自動作成	すべてのクライアントプリンターを自動作成	すべてのVDAバージョン
汎用ユニバーサルプリンターを自動作成	無効	すべてのVDAバージョン
クライアントプリンター名	標準プリンター名	VDA 5.6
印刷サーバーへの直接接続	有効	すべてのVDAバージョン

名前	デフォルト設定	VDA
プリンタードライバーのマッピングと互換性	ルールは指定されていません	すべてのVDAバージョン
プリンタープロパティの保持	クライアントに保存されていない場合にのみプロファイルに保持	すべてのVDAバージョン
保持および復元されたクライアントプリンター	許可	VDA 5、5,5、5.6 FP1

ICA/Printing/Drivers

名前	デフォルト設定	VDA
インボックスプリンタードライバーの自動インストール	有効	すべてのVDAバージョン
ユニバーサルドライバーの優先順位	イーエムエフ; エックスピーエス; ピーシーエルファイブシー; ピーシーエルフォー; ピーエス	すべてのVDAバージョン
ユニバーサル印刷ドライバーの使用	要求されたドライバーが利用できない場合にのみユニバーサル印刷を使用する	すべてのVDAバージョン

ICA/印刷/ユニバーサルプリントサーバー

名前	デフォルト設定	VDA
ユニバーサルプリントサーバーを有効にする	無効	すべてのVDAバージョン
ユニバーサルプリントサーバー印刷データストリーム (CGP) ポート	7229	すべてのVDAバージョン
ユニバーサルプリントサーバー印刷ストリーム入力帯域幅制限 (kbps)	0	すべてのVDAバージョン

名前	デフォルト設定	VDA
ユニバーサルプリントサーバーWebサービス (HTTP/SOAP) ポート	8080	すべてのVDAバージョン
負荷分散用のUniversal Print Server	VDAバージョン7.9から現在まで	
ユニバーサルプリントサーバーのサービス停止しきい値	180 (秒)	VDA バージョン 7.9 から現在まで

ICA/印刷/ユニバーサル印刷

名前	デフォルト設定	VDA
ユニバーサル印刷 EMF 処理モード	プリンターに直接スプールする	すべての VDA バージョン
ユニバーサル印刷画像圧縮制限	最高品質 (ロスレス圧縮)	すべての VDA バージョン
ユニバーサル印刷最適化のデフォルト	画像圧縮: 希望する画質 = 標準品質, ヘビーウェイト圧縮を有効にする = 無効; 画像とフォントのキャッシュ: 埋め込み画像のキャッシュを許可する = 有効; 管理者以外のユーザーがこれらの設定を変更することを許可する = 無効;	すべての VDA バージョン
ユニバーサル印刷プレビュー設定	自動作成されたプリンターまたは汎用ユニバーサルプリンターには印刷プレビューを使用しない	すべてのVDAバージョン
ユニバーサル印刷の印刷品質制限	制限なし	すべてのVDAバージョン

ICA/セキュリティ

名前	デフォルト設定	VDA
SecureICAの最小暗号化レベル	基本	マルチセッションOS用VDA 7以降

ICA/サーバー制限

名前	デフォルト設定	VDA
サーバーアイドルタイマー間隔	0ミリ秒	マルチセッションOS用VDA 7以降

ICA/セッション制限

名前	デフォルト設定	VDA
切断されたセッションタイマー	無効	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
リモートPCアクセス切断セッションタイマー	無効	シングルセッションOS用VDA 7以降
切断セッションタイマー間隔	1,440分	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
セッション接続タイマー	無効	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
セッション接続タイマー間隔	1,440分	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
セッションアイドルタイマー	有効	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降

名前	デフォルト設定	VDA
セッションアイドルタイマー間隔	1,440分	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降

ICA/セッションの信頼性

名前	デフォルト設定	VDA
セッションの信頼性接続	許可	すべてのVDAバージョン
セッションの信頼性ポート番号	2598	すべてのVDAバージョン
セッションの信頼性タイムアウト	180秒	すべてのVDAバージョン

ICA/タイムゾーン制御

名前	デフォルト設定	VDA
レガシークライアントのローカル時刻を推定する	有効	マルチセッションOS 7以降のVDA
セッション切断またはログオフ時にシングルセッションOSのタイムゾーンを復元する	有効	現在のVDAバージョン
クライアントのローカル時刻を使用する	サーバーのタイムゾーンを使用する	すべてのVDAバージョン

ICA/TWAINデバイス

名前	デフォルト設定	VDA
クライアントTWAINデバイスリダイレクト	許可	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

名前	デフォルト設定	VDA
TWAIN圧縮レベル	中	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ICA/USBデバイス

名前	デフォルト設定	VDA
クライアントUSBデバイス最適化ルール	有効 (VDA 7.6 FP3以降); 無効 (VDA 7.11以降); デフォルトでは、ルールは指定されていません	VDA 7.6 FP3以降
クライアントUSBデバイスのリダイレクト	禁止	すべてのVDAバージョン
クライアントUSBデバイスリダイレクト規則	ルールは指定されていません	すべてのVDAバージョン
クライアントUSBプラグアンドプレイデバイスリダイレクト	許可	マルチセッションOS 用 VDA 7 以降、シングルセッション OS 用 VDA 7 以降

ICA/ビジュアルディスプレイ

名前	デフォルト設定	VDA
単純なグラフィックの優先色深度	24ビット/ピクセル	VDA 7.6 FP3 以降
ターゲットフレームレート	30 フレーム/秒	すべてのVDAバージョン
画質	中	マルチセッションOS 用 VDA 7 以降、シングルセッション OS 用 VDA 7 以降

ICA/ビジュアルディスプレイ/動画

名前	デフォルト設定	VDA
最小画質	標準	VDA 5.5、5.6 FP1、マルチセッションOS 用 VDA 7 以降、シングルセッションOS 用 VDA 7 以降
動画圧縮	有効	VDA 5.5、5.6 FP1、マルチセッションOS 用 VDA 7 以降、シングルセッションOS 用 VDA 7 以降
プログレッシブ圧縮レベル	なし	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
プログレッシブ圧縮のしきい値	2,147,483,647 キロビット/秒	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
目標最小フレームレート	10 フレーム/秒	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

注:

「**目標最小フレームレート**」ポリシーは廃止されました。

ICA/視覚表示/静止画像

名前	デフォルト設定	VDA
追加の色圧縮	無効	すべてのVDAバージョン
追加の色圧縮のしきい値	8,192 キロビット/秒	すべてのVDAバージョン

名前	デフォルト設定	VDA
高負荷圧縮	無効	すべてのVDAバージョン
非可逆圧縮レベル	中	すべてのVDAバージョン
非可逆圧縮しきい値	2,147,483,647 ケービーピーエス	すべてのVDAバージョン

ICA/WebSockets

名前	デフォルト設定	VDA
WebSockets接続	禁止	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
WebSocketsポート番号	8008	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
WebSockets信頼済みオリジンサーバーリスト	ワイルドカード「*」は、すべてのReceiver for Web URLを信頼するために使用されます	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

負荷管理

名前	デフォルト設定	VDA
同時ログオン許容数	2	マルチセッションOS用VDA 7以降
CPU使用率	無効	マルチセッションOS用VDA 7以降
CPU使用率から除外されるプロセスの優先度	標準以下または低	マルチセッションOS用VDA 7以降
ディスク使用量	無効	マルチセッションOS用VDA 7以降

名前	デフォルト設定	VDA
最大セッション数	250	マルチセッションOS用VDA 7以降
メモリ使用量	無効	マルチセッションOS用VDA 7以降
メモリ使用量のベース負荷	ゼロ負荷: 768 MB	マルチセッションOS用VDA 7以降

プロファイル管理/詳細設定

名前	デフォルト設定	VDA
自動構成を無効にする	無効	すべてのVDAバージョン
問題が発生した場合にユーザーをログオフする	無効	すべてのVDAバージョン
ロックされたファイルへのアクセス時の再試行回数	5	すべてのVDAバージョン
ログオフ時にインターネットCookieファイルを処理する	無効	すべてのVDAバージョン

プロファイル管理/基本設定

名前	デフォルト設定	VDA
アクティブライトバック	無効	すべてのVDAバージョン
Profile Management を有効にする	無効	すべてのVDAバージョン
除外されるグループ	無効。すべてのユーザーグループのメンバーが処理されます。	すべてのVDAバージョン
オフラインプロファイルのサポート	無効	すべてのVDAバージョン
ユーザーストアへのパス	ウィンドウズ	すべてのVDAバージョン

名前	デフォルト設定	VDA
ローカル管理者によるログオンの処理	無効	すべてのVDAバージョン
処理されるグループ	無効。すべてのユーザーグループのメンバーが処理されます。	すべてのVDAバージョン

プロファイル管理/クロスプラットフォーム設定

名前	デフォルト設定	VDA
クロスプラットフォーム設定ユーザーグループ	無効。処理済みグループで指定されたすべてのユーザーグループが処理されます	すべてのVDAバージョン
クロスプラットフォーム設定を有効にする	無効	すべてのVDAバージョン
クロスプラットフォーム定義へのパス	無効。パスは指定されていません。	すべてのVDAバージョン
クロスプラットフォーム設定ストアへのパス	無効。Windows\PM_CMが使用されます。	すべてのVDAバージョン
クロスプラットフォーム設定の作成元	無効	すべてのVDAバージョン

プロファイル管理/ファイルシステム/除外

名前	デフォルト設定	VDA
除外リスト - ディレクトリ	無効。ユーザープロファイル内のすべてのフォルダーが同期されます。	すべてのVDAバージョン
除外リスト - ファイル	無効。ユーザープロファイル内のすべてのファイルが同期されます。	すべてのVDAバージョン

プロファイル管理/ファイルシステム/同期

名前	デフォルト設定	VDA
同期するディレクトリ	無効。除外されていないフォルダーのみが同期されます。	すべてのVDAバージョン
同期するファイル	無効。除外されていないファイルのみが同期されます。	すべてのVDAバージョン
ミラーリングするフォルダー	無効。フォルダーはミラーリングされません。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト

名前	デフォルト設定	VDA
管理者アクセスを許可する	無効	すべてのVDAバージョン
ドメイン名を含める	無効	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/AppData(Roaming)

名前	デフォルト設定	VDA
AppData(Roaming)パス	無効。場所は指定されていません。	すべてのVDAバージョン
AppData(Roaming)のリダイレクト設定	コンテンツは、AppData(Roaming)パスのポリシー設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/連絡先

名前	デフォルト設定	VDA
連絡先パス	無効。場所は指定されていません。	すべてのVDAバージョン
連絡先のリダイレクト設定	コンテンツは、**連絡先パスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/デスクトップ

名前	デフォルト設定	VDA
デスクトップパス	無効。場所は指定されていません。	すべてのVDAバージョン
デスクトップのリダイレクト設定	コンテンツは、**デスクトップパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ドキュメント

名前	デフォルト設定	VDA
ドキュメントパス	無効。場所は指定されていません。	すべてのVDAバージョン
ドキュメントのリダイレクト設定	コンテンツは、**ドキュメントパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ダウンロード

名前	デフォルト設定	VDA
ダウンロードパス	無効。場所は指定されていません。	すべてのVDAバージョン
ダウンロードのリダイレクト設定	コンテンツは、**ダウンロードパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/お気に入り

名前	デフォルト設定	VDA
お気に入りパス	無効。場所は指定されていません。	すべてのVDAバージョン

名前	デフォルト設定	VDA
お気に入りのリダイレクト設定	コンテンツは、**お気に入りパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/リンク

名前	デフォルト設定	VDA
リンクパス	無効。場所は指定されていません。	すべてのVDAバージョン
リンクのリダイレクト設定	コンテンツは、**リンクパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ミュージック

名前	デフォルト設定	VDA
ミュージックパス	無効。場所は指定されていません。	すべてのVDAバージョン
ミュージックのリダイレクト設定	コンテンツは、「**ミュージックパスポリシー**」設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ピクチャ

名前	デフォルト設定	VDA
ピクチャパス	無効。場所は指定されていません。	すべてのVDAバージョン
ピクチャのリダイレクト設定	コンテンツは、「**ピクチャパスポリシー**」設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/保存されたゲーム

名前	デフォルト設定	VDA
保存されたゲームパス	無効。場所は指定されていません。	すべてのVDAバージョン
保存されたゲームのリダイレクト設定	コンテンツは、「**保存されたゲームパスポリシー**」設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/検索

名前	デフォルト設定	VDA
検索パス	無効。場所は指定されていません。	すべてのVDAバージョン
検索のリダイレクト設定	コンテンツは、**検索パスポリシー**設定で指定されたUNCパスにリダイレクトされます。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/スタートメニュー

名前	デフォルト設定	VDA
スタートメニューパス	無効。場所は指定されていません。	すべてのVDAバージョン
スタートメニューのリダイレクト設定	コンテンツは、スタートメニューパスポリシー設定で指定されたUNCパスにリダイレクトされます。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ビデオ

名前	デフォルト設定	VDA
ビデオパス	無効。場所は指定されていません。	すべてのVDAバージョン

名前	デフォルト設定	VDA
ビデオのリダイレクト設定	コンテンツは、**ビデオパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/ログ設定

名前	デフォルト設定	VDA
Active Directory のアクション	無効	すべてのVDAバージョン
一般情報	無効	すべてのVDAバージョン
一般的な警告	無効	すべてのVDAバージョン
ログの有効化	無効	すべてのVDAバージョン
ファイルシステムのアクション	無効	すべてのVDAバージョン
ファイルシステム通知	無効	すべてのVDAバージョン
ログオフ	無効	すべてのVDAバージョン
ログオン	無効	すべてのVDAバージョン
ログファイルの最大サイズ	1048576	すべてのVDAバージョン
ログファイルへのパス	無効。ログファイルはデフォルトの場所 (%SystemRoot%\System32\Logfiles\UserProfileManager) に保存されます。	すべてのVDAバージョン
パーソナライズされたユーザー情報	無効	すべてのVDAバージョン
ログオン時とログオフ時のポリシー値	無効	すべてのVDAバージョン
レジストリアクション	無効	すべてのVDAバージョン

名前	デフォルト設定	VDA
ログオフ時のレジストリの相違点	無効	すべてのVDAバージョン

プロファイル管理/プロファイルの処理

名前	デフォルト設定	VDA
キャッシュされたプロファイルを削除するまでの遅延	0	すべてのVDAバージョン
ログオフ時にローカルにキャッシュされたプロファイルを削除する	無効	すべてのVDAバージョン
ローカルプロファイルの競合処理	ローカルプロファイルを使用する	すべてのVDAバージョン
既存プロファイルの移行	ローカルとローミング	すべてのVDAバージョン
テンプレートプロファイルへのパス	無効。新しいユーザープロファイルは、ユーザーが最初にログオンしたデバイスのデフォルトユーザープロファイルから作成されます。	すべてのVDAバージョン
テンプレートプロファイルがローカルプロファイルを上書きする	無効	すべてのVDAバージョン
テンプレートプロファイルが移動プロファイルを上書きする	無効	すべてのVDAバージョン
すべてのログオンでCitrix®必須プロファイルとして使用されるテンプレートプロファイル	無効	すべてのVDAバージョン

プロファイル管理/レジストリ

名前	デフォルト設定	VDA
除外リスト	無効。ユーザーがログオフすると、HKCUハイブ内のすべてのレジストリキーが処理されます。	すべてのVDAバージョン
包含リスト	無効。ユーザーがログオフすると、HKCUハイブ内のすべてのレジストリキーが処理されます。	すべてのVDAバージョン

プロファイル管理/ストリーム配信ユーザープロファイル

名前	デフォルト設定	VDA
常にキャッシュ	無効	すべてのVDAバージョン
常にキャッシュサイズ	0 MB	すべてのVDAバージョン
プロファイルストリーミング	無効	すべてのVDAバージョン
ストリーミングされたユーザープロファイルグループ	無効。OU内のすべてのユーザープロファイルは通常どおり処理されます。	すべてのVDAバージョン
保留中のエリアロックファイルのタイムアウト (日数)	1日	すべてのVDAバージョン

レシーバー

名前	デフォルト設定	VDA
StoreFront™アカウントリスト	ストアは指定されていません	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ユーザーパーソナライゼーションレイヤー

名前	デフォルト設定	VDA
ユーザーレイヤーリポジトリパス	無効。パスは指定されていません。	VDA 19.12以降のバージョン
ユーザーレイヤーサイズ(GB)	10 GB。ユーザーレイヤーは、設定されたサイズまで拡張するシンプロビジョニングディスクです。ユーザーレイヤーのサイズが小さくなることはありません。	VDA 19.12以降のバージョン

バーチャル デリバリー エージェント

名前	デフォルト設定	VDA
コントローラー登録IPv6ネットマスク	ネットマスクは指定されていません	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
コントローラー登録ポート	80	すべてのVDAバージョン
コントローラーSID	SIDは指定されていません	すべてのVDAバージョン
コントローラー	コントローラーは指定されていません	すべてのVDAバージョン
コントローラーの自動更新を有効にする	有効	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
IPv6コントローラー登録のみを使用する	無効	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
サイトGUID	GUIDは指定されていません	すべてのVDAバージョン

バーチャル デリバリー エージェント/HDX 3D Pro

名前	デフォルト設定	VDA
ロスレスを有効にする	有効	VDA 5.5、5.6 FP1
HDX 3D Pro品質設定	VDA 5.5、5.6 FP1	

バーチャル デリバリー エージェント/監視

名前	デフォルト設定	VDA
プロセス監視を有効にする	無効	VDA 7.11以降
リソース監視を有効にする	有効	VDA 7.11以降

仮想IP

名前	デフォルト設定	VDA
仮想IPループバックサポート	無効	VDA 7.6 以降
仮想IP仮想ループバックプログラムリスト	なし	VDA 7.6 以降

ポリシーの変更

次の表に、Citrix Virtual Apps and Desktops™ 7 2603 のポリシー更新（追加、削除、名前の変更、デフォルト状態の変更を含む）を示します。

ポリシー設定	変更点
プロファイル管理 > プロファイルコンテナ設定 > BindLinkリダイレクトを有効にする	BindLinkリダイレクトを有効にするための新しいポリシーです。詳細はこちら(/ja-jp/profile-management/current-release/policies/descriptions-and-defaults#enable-bindlink-redirection)。
次のSCCM設定	2026年第4四半期に廃止予定です。

ポリシー設定	変更点
• 事前警告頻度間隔	
事前警告メッセージボックスの本文	
事前警告メッセージボックスのタイトル	
事前警告期間	
エージェントタスクを実行する通常の時間間隔	
最終強制ログオフメッセージボックスの本文	
最終強制ログオフメッセージボックスのタイトル	
強制ログオフ猶予期間	
強制ログオフメッセージボックスの本文	
強制ログオフメッセージボックスのタイトル • 再起動メッセージボックスの本文 • イメージ管理モード	
次のXenApp設定	2026年第4四半期に非推奨となる予定です。
• Flash品質調整 (AllowSpeedFlash) • 新しく利用可能になったPVSイメージの期限計算	

ポリシー設定	変更点	
時間 (PvsImageUpdateDeadlinePeriod) • ファーム名 (FarmName) • ワークロード名 (WorkloadName) • 仮想IP拡張互換性 (EnableEnhancedCompatibility) • 仮想IP互換性プログラムリスト (EnhancedCompatibilityProgramsList) • 仮想IPアダプターアドレスフィルタリング (FilterAdapterAddresses) • 仮想IPフィルターアダプターアドレスプログラムリスト (FilterAdapterAddressesProgramsList)		
クライアントプリンターポリシー設定 > 保持および復元されたクライアントプリンター	2402以降非推奨	
ユニバーサルドライバーの優先順位	Citrix Virtual Apps and Desktops™の第4四半期リリースで、ユニバーサルプリンタードライバーのデフォルトの優先順位が変更されます。新しいデフォルトの順序は、EMF > XPS > PCL5c >	

ポリシー設定	変更点
	PCL4 > PDF > PS となります。

注:

- アップグレードする前に、すべての非推奨設定を削除してください。非推奨設定が使用されたままの場合、アップグレードはエラーで失敗する可能性があります。
- 既にアップグレード済みの場合、非推奨の設定がまだ含まれているポリシーとテンプレートをクリーンアップするには、アップグレード後に非推奨のポリシー設定を削除するを使用してください。

管理

Citrix Virtual Apps and Desktops™ サイトの管理には、さまざまな項目とタスクが含まれます。

ライセンス

サイトを作成するときは、Citrix License Server への有効な接続が必要です。後で、Studio から、ライセンスの追加、ライセンスの種類やモデルの変更、ライセンス管理者の管理など、いくつかのライセンス関連タスクを実行できます。Studio から License Administration Console にアクセスすることもできます。

アプリケーション

デリバリーグループ、およびオプションでアプリケーショングループ内のアプリケーションを管理します。

ゾーン

地理的に分散した展開では、ゾーンを使用してアプリケーションとデスクトップをエンドユーザーの近くに配置し、パフォーマンスを向上させることができます。サイトをインストールして構成すると、すべてのコントローラー、マシンカタログ、およびホスト接続は1つのプライマリゾーンに配置されます。後で、Studio を使用して、これらの項目を含むサテライトゾーンを作成できます。サイトに複数のゾーンがある場合、新しく作成されたマシンカタログ、ホスト接続、または追加されたコントローラーをどのゾーンに配置するかを指定できます。ゾーン間で項目を移動することもできます。

接続とリソース

アプリケーションとデスクトップをユーザーに提供するマシンをホストするためにハイパーバイザーまたはその他のサービスを使用している場合、サイトを作成するときに、そのハイパーバイザーまたはその他のサービスへの最初の接続を作成します。その接続のストレージとネットワークの詳細は、そのリソースを構成します。後で、その接続とそのリソースを変更したり、さらに接続を作成したりできます。構成済みの接続を使用するマシンを管理することもできます。

ローカルホストキャッシュ

ローカルホストキャッシュにより、Delivery Controller™ とサイトデータベース間の接続が失敗した場合でも、サイトでの接続ブローカー操作を続行できます。

仮想IPと仮想ループバック

Microsoft の仮想IPアドレス機能は、公開アプリケーションにセッションごとに一意の動的に割り当てられたIPアドレスを提供します。Citrix の仮想ループバック機能を使用すると、localhost との通信に依存するアプリケーションを、localhost 範囲内の一意の仮想ループバックアドレスを使用するように構成できます。

デリバリーコントローラー

この記事では、サイトへのControllerの追加と削除に関する考慮事項と手順について説明します。また、Controllerを別のゾーンまたはサイトに移動する方法、およびVDAを別のサイトに移動する方法についても説明します。

ControllerへのVDA登録

VDAがアプリケーションとデスクトップの配信を支援するには、Controllerに登録（通信を確立）する必要があります。Controllerのアドレスはいくつかの方法で指定でき、それについてはこの記事で説明します。サイトでControllerが追加、移動、削除される際に、VDAが最新の情報を持っていることが重要です。

セッション

セッションアクティビティを維持することは、最高のユーザーエクスペリエンスを提供するために不可欠です。いくつかの機能により、セッションの信頼性を最適化し、不便さ、ダウンタイム、生産性の損失を軽減できます。

- セッションの信頼性
- クライアントの自動再接続
- ICA®キープアライブ
- ワークスペースコントロール
- セッションローミング

Studioでの検索の使用

Studioでマシン、セッション、マシンカタログ、アプリケーション、またはデリバリーグループに関する情報を表示したい場合は、柔軟な検索機能を使用します。

タグ

タグを使用して、マシン、アプリケーション、グループ、ポリシーなどのアイテムを識別します。その後、特定のタグを持つアイテムに適用されるように特定の操作を調整できます。

IPv4/IPv6

Citrix Virtual Apps and Desktops™ は、純粋な IPv4、純粋な IPv6、および重複する IPv4 と IPv6 ネットワークを使用するデュアルスタック展開をサポートしています。この記事では、これらの展開について説明し、図解します。また、IPv4 または IPv6 の使用を制御する Citrix ポリシー設定についても説明します。

ユーザープロファイル

デフォルトでは、VDA をインストールすると Citrix Profile Management が自動的にインストールされます。このプロファイルソリューションを使用する場合は、一般的な情報についてこの記事を確認してください。詳細については、Profile Management のドキュメントを参照してください。

Citrix Diagnostic Facility (CDF) トレースの収集

CDFControl ユーティリティは、さまざまな Citrix トレースプロバイダーから表示される Citrix Diagnostic Facility (CDF) トレースメッセージをキャプチャするためのイベントトレースコントローラーまたはコンシューマーです。これは、複雑な Citrix 関連の問題のトラブルシューティング、フィルターサポートの解析、およびパフォーマンスデータの収集のために作成されています。

シトリックス インサイト サービス

Citrix Insight Services (CIS) は、計測、テレメトリ、およびビジネスインサイト生成のための Citrix プラットフォームです。

シトリックス スカウト

Citrix Scout は、診断情報を収集し、ヘルスチェックを実行します。結果は、Citrix Virtual Apps and Desktops 展開におけるプロアクティブなメンテナンスに利用できます。Citrix は、Citrix Insight Services を通じて、診断コレクションの包括的な自動分析を提供します。また、Scout を使用して、単独で、または Citrix サポートのガイダンスを受けて問題をトラブルシューティングすることもできます。

アプリケーション

> **注:**
>
> バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™ の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除され

> ました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

はじめに

展開でデリバリーグループのみを使用している場合（アプリケーショングループは使用しない場合）、アプリケーションはデリバリーグループに追加します。アプリケーショングループも使用している場合は、通常、代わりにアプリケーショングループにアプリケーションを追加します。このガイダンスにより、管理が容易になります。アプリケーションは常に少なくとも1つのデリバリーグループまたはアプリケーショングループに属している必要があります。

アプリケーションの追加ウィザードでは、1つ以上のデリバリーグループ、または1つ以上のアプリケーショングループを選択できますが、両方は選択できません。後でアプリケーションのグループ関連付けを変更することはできますが（たとえば、アプリケーショングループからデリバリーグループにアプリケーションを移動するなど）、ベストプラクティスでは、そのような複雑さを追加することは推奨されません。アプリケーションは1種類のグループに保持してください。

アプリケーションを複数のグループに関連付ける場合、それらのすべてのグループでアプリケーションを表示するのに十分な権限がないと、可視性の問題が発生する可能性があります。そのような場合は、より高い権限を持つ管理者に相談するか、アプリケーションが関連付けられているすべてのグループを含むようにスコープを拡張してください。

同じ名前の2つのアプリケーション（異なるグループからのものなど）を同じユーザーに公開する場合、Web Studioで `Application name (for user)` プロパティを変更します。そうしないと、ユーザーはCitrix Workspace™アプリで重複する名前を目にすることになります。

アプリケーションのプロパティ（設定）は、追加時または後で変更できます。アプリケーションが配置されているアプリケーションフォルダーも、アプリケーションの追加時または後で変更できます。

詳細については、以下を参照してください。

- デリバリーグループの作成
- アプリケーショングループの作成
- タグ

アプリケーションの追加

デリバリーグループまたはアプリケーショングループを作成するときにアプリケーションを追加できます。これらの手順については、デリバリーグループの作成およびアプリケーショングループ

の作成で詳しく説明されています。次の手順では、グループ作成後にアプリケーションを追加する方法について説明します。

知っておくと良いこと:

- Remote PC Accessデリバリーグループにアプリケーションを追加することはできません。
- アプリケーションの追加ウィザードを使用して、デリバリーグループまたはアプリケーショングループからアプリケーションを削除することはできません。これは別の操作です。

1つ以上のアプリケーションを追加するには：

1. 左ペインで**アプリケーション**を選択し、アクションバーで**アプリケーションの追加**を選択します。
2. アプリケーションの追加ウィザードが**はじめに**ページとともに起動します。このページは、今後のウィザードの起動時に表示しないように設定できます。
3. ウィザードは、**グループ**、**アプリケーション**、**概要**の各ページを案内します。各ページの作業が完了したら、**概要**ページに到達するまで**次へ**をクリックします。

単一のデリバリーグループまたはアプリケーショングループにアプリケーションを追加する場合の、手順1の代替方法：

- **1つのデリバリーグループにのみアプリケーションを追加するには：** 手順1で、Web Studioの左ペインで**デリバリーグループ**を選択し、中央ペインでデリバリーグループを選択してから、アクションバーで**アプリケーションの追加**を選択します。ウィザードには**グループ**ページが表示されません。
- **1つのアプリケーショングループにのみアプリケーションを追加するには：** 手順1で、Web Studioの左ペインで**アプリケーション**を選択し、中央ペインでアプリケーショングループを選択してから、アクションバーでアプリケーショングループ名の下にある**アプリケーションの追加**エントリを選択します。ウィザードには**グループ**ページが表示されません。

グループページ

このページには、サイト内のすべてのデリバリーグループが一覧表示されます。アプリケーショングループも作成している場合は、アプリケーショングループとデリバリーグループが一覧表示されます。どちらかのグループを選択できますが、両方のグループを選択することはできません。つまり、アプリケーショングループとデリバリーグループに同時にアプリケーションを追加することはできません。通常、アプリケーショングループを使用している場合は、デリバリーグループではなくアプリケーショングループにアプリケーションを追加します。

アプリケーションを追加するときは、少なくとも1つのデリバリーグループ（または、利用可能な場合はアプリケーショングループ）の横にあるチェックボックスをオンにします。すべてのアプリケーションは、常に少なくとも1つのグループに関連付けられている必要があります。

アプリケーションページ

追加をクリックして、アプリケーションソースを表示します。

- **スタートメニューから：** 選択したデリバリーグループ内のマシンで検出されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストを含む新しいページが起動します。追加するアプリケーションのチェックボックスをオンにして、**OK**をクリックします。

  このソースは、(1)関連付けられたデリバリーグループがないアプリケーショングループを選択した場合、(2)関連付けられたデリバリーグループにマシンが含まれていないアプリケーショングループを選択した場合、または(3)マシンが含まれていないデリバリーグループを選択した場合は、選択できません。
- **手動：** デリバリーグループ内のVDAまたはネットワーク上の別の場所にあるアプリケーション。このソースを選択すると、新しいページが開き、次の方法で追加するアプリケーションを指定できます。
  - 実行可能ファイルへのパス、作業ディレクトリ、オプションのコマンドライン引数、および管理者とユーザーの表示名を入力します。
  - デリバリーグループ内のVDAからアプリケーションを選択します。これを行うには、**参照**をクリックし、VDAにアクセスするための資格情報を入力し、VDAに接続されるまで待機してから、VDAからアプリケーションを選択します。選択したアプリケーションのプロパティが、ページのフィールドに自動的に入力されます。
- **既存:** 以前サイトに追加されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストを含む新しいページが起動します。追加するアプリケーションのチェックボックスを選択し、**OK**をクリックします。

  サイトにアプリケーションがない場合、このソースは選択できません。
- **アプリケーションパッケージ:** App-V、MSIX、MSIX app attach、またはFlexAppアプリケーションパッケージ内のアプリケーション。このソースを選択すると、**パッケージからのアプリケーションの追加**ページが起動します。アプリケーションパッケージソースを選択し、表示された結果から追加するアプリケーションを選択して、**OK**を選択します。詳しくは、「Appパッケージの展開と配信」を参照してください。

- **アプリケーショングループ**: アプリケーショングループ。このソースを選択すると、アプリケーショングループのリストを含む新しいページが起動します。（表示には各グループ内のアプリケーションもリストされますが、個々のアプリケーションではなくグループのみを選択できます。）選択したグループ内の現在および将来のすべてのアプリケーションが追加されます。追加するアプリケーショングループのチェックボックスを選択し、**OK**をクリックします。

  このソースは、(1) アプリケーショングループがない場合、または (2) 選択したデリバリーグループがアプリケーショングループをサポートしていない場合（たとえば、静的に割り当てられたマシンを持つデリバリーグループ）には選択できません。

表に示されているように、**追加**リストの一部のソースは、そのタイプの有効なソースがない場合、選択できません。互換性のないソース（たとえば、アプリケーショングループにアプリケーショングループを追加できないなど）はリストに含まれません。選択したグループに既に追加されているアプリケーションは選択できません。

このページまたは後で、アプリケーションのプロパティ（設定）を変更できます。

デフォルトでは、追加されたアプリケーションは`Applications`という名前のアプリケーションフォルダーに配置されます。このページまたは後で、アプリケーションを変更できます。アプリケーションを追加しようとして、同じ名前のアプリケーションが同じフォルダーに存在する場合、追加しようとしているアプリケーションの名前を変更するよう求められます。提示された新しい名前を受け入れるか、拒否してアプリケーションの名前を変更するか、別のフォルダーを選択できます。たとえば、**Applications**フォルダーに`app`が既に存在し、そのフォルダーに`app`という名前の別のアプリケーションを追加しようとすると、新しい名前`app_1`が提示されます。

概要ページ

10個以下のアプリケーションを追加する場合、その名前は**追加するアプリケーション**にリストされます。10個を超えるアプリケーションを追加する場合、合計数が指定されます。

概要情報を確認し、**「完了」**をクリックします。

アプリケーションのグループ関連付けを変更する

アプリケーションを追加した後、そのアプリケーションが関連付けられているデリバリーグループとアプリケーショングループを変更できます。

アプリケーションを別のグループにドラッグできます。これは、アクションバーのコマンドを使用する代替手段です。

アプリケーションがアプリケーショングループを使用するか直接使用するかに関わらず、複数のデリバリーグループに関連付けられている場合、グループの優先順位を使用して、複数のグループが評価される順序を指定できます。アクセスポリシー、ユーザーリスト、スマートアクセスタグなどの要因に基づいてグループを考慮対象から除外でき、ゾーンの優先順位、起動準備、タグの制限などの要因によって、グループから選択される特定のマシンが影響を受ける可能性があります。デフォルトでは、すべてのグループの優先順位は0（最高）です。デリバリーグループの優先順位が同じ場合、アプリケーションの起動には最も負荷の低いデリバリーグループが選択されます。この場合、垂直負荷分散は考慮されません。

アプリケーションは、アプリケーションを配信できる共有（プライベートではない）マシンを含むデリバリーグループに関連付けることができます。また、共有マシンを含むデリバリーグループがデスクトップのみを配信する場合でも、(1) デリバリーグループに共有マシンが含まれており、XenDesktop 7.xバージョン7.9より前に作成された場合、および (2) `Edit delivery group` 権限がある場合は、そのデリバリーグループを選択できます。プロパティダイアログがコミットされると、デリバリーグループの種類は自動的に `desktops and applications` に変換されます。

1. Web Studioにサインインし、左ペインで**Applications**を選択し、アプリケーションを選択します。
2. アクションバーで**「プロパティ」**を選択します。
3. **「グループ」**ページを選択します。

    - グループを追加するには、**「追加」をクリックし、「アプリケーショングループ」または「デリバリーグループ」を選択します。（アプリケーショングループを作成していない場合、唯一の項目は**「デリバリーグループ」**です。）次に、1つ以上の利用可能なグループを選択します。アプリケーションと互換性のないグループ、またはすでにアプリケーションに関連付けられているグループは選択できません。
    - グループを削除するには、1つ以上のグループを選択し、**「削除」**をクリックします。グループの関連付けを削除した結果、アプリケーションがどのグループとも関連付けられなくなる場合、アプリケーションが削除されることを警告されます。
    - グループの優先度を変更するには、グループを選択し、**「優先度の編集」をクリックします。優先度値を選択し、**「OK」**をクリックします。

4. 完了したら、**「適用」をクリックして変更を適用し、ウィンドウを開いたままにするか、**「OK」**をクリックして変更を適用し、ウィンドウを閉じます。

アプリケーションの複製、有効化または無効化、名前の変更、または削除

次のアクションが利用可能です。

- **複製：** 異なるパラメーターまたはプロパティを持つ別のバージョンを作成するために、アプリケーションを複製したい場合があります。アプリケーションを複製すると、一意のサフィックスで自動的に名前が変更され、元のアプリケーションの隣に配置されます。また、アプリケーションを複製してから、別のグループに追加したい場合もあります。（複製後、アプリケーションを移動する最も簡単な方法はドラッグすることです。）
- **有効化または無効化：** アプリケーションの有効化と無効化は、デリバリーグループまたはアプリケーショングループの有効化と無効化とは異なるアクションです。
- **名前の変更：** 一度に1つのアプリケーションのみ名前を変更できます。アプリケーションの名前を変更しようとして、同じ名前のアプリケーションが同じフォルダーまたはグループに存在する場合、別の名前を指定するように求められます。
- **削除：** アプリケーションを削除すると、関連付けられていたデリバリーグループおよびアプリケーショングループから削除されますが、元々アプリケーションを追加するために使用されたソースからは削除されません。アプリケーションの削除は、デリバリーグループまたはアプリケーショングループから削除するのとは異なるアクションです。

アプリケーションを複製、有効化、無効化、名前変更、または削除するには：

1. 左ペインで**「アプリケーション」**を選択します。
2. 中央ペインで1つ以上のアプリケーションを選択し、アクションバーで適切なタスクを選択します。
3. プロンプトが表示されたら、アクションを確認します。

デリバリーグループからアプリケーションを削除する

アプリケーションは、少なくとも1つのデリバリーグループまたはアプリケーショングループに関連付けられている（属している）必要があります。アプリケーションをデリバリーグループから削除しようとしたときに、そのアプリケーションがどのデリバリーグループまたはアプリケーショングループとも関連付けがなくなる場合、続行するとアプリケーションが削除されるという通知が表示されます。その場合、そのアプリケーションを配信したい場合は、有効なソースから再度追加する必要があります。

1. 左側のペインで、 を選択します。
2. デリバリーグループを選択します。中央下のペインの タブで、削除するアプリケーションを選択します。
3. アクションバーから を選択します。
4. 削除を確認します。

アプリケーショングループからアプリケーションを削除する

アプリケーションは、少なくとも1つのデリバリーグループまたはアプリケーショングループに属している必要があります。アプリケーションをアプリケーショングループから削除しようとしたときに、そのアプリケーションがどのグループにも属さなくなる場合、続行するとアプリケーションが削除されるという通知が表示されます。その場合、そのアプリケーションを配信したい場合は、有効なソースから再度追加する必要があります。

1. 左側のペインで、 を選択します。
2. 中央のペインでアプリケーショングループを選択し、1つまたは複数のアプリケーションを選択します。
3. アクションバーで を選択します。
4. 削除を確認します。

アプリケーションのプロパティを変更する

アプリケーションのプロパティは、一度に1つしか変更できません。

アプリケーションのプロパティを変更するには：

1. 左側のペインで を選択します。
2. アプリケーションを選択し、アクションバーで を選択します。
3. 変更するプロパティが含まれるページを選択します。
4. 完了したら、 をクリックして変更を適用し、ウィンドウを開いたままにするか、 をクリックして変更を適用してウィンドウを閉じます。

次のリストでは、ページが括弧内に表示されます。

プロパティ	ページ
Citrix Workspaceアプリにアプリケーションが表示されるカテゴリまたはフォルダー	配信
コマンドライン引数。「公開アプリケーションへのパラメーターの受け渡し」を参照してください。	場所
アプリケーションが利用可能なデリバリーグループとアプリケーショングループ	グループ
説明	識別

プロパティ	ページ
ファイル名拡張子とファイルの種類関連付け：アプリケーションが自動的に開く拡張子	ファイルの種類関連付け
アイコン	配信
StoreFront™のキーワード	識別
制限; アプリケーション制限の構成を参照	配信
名前: ユーザーおよび管理者に表示される名前	識別
実行可能ファイルへのパス; 公開アプリケーションへのパラメーターの受け渡しを参照	場所
ユーザーのデスクトップ上のショートカット: 有効または無効	配信
可視性: Citrix Workspaceアプリでアプリケーションを表示できるユーザーを制限します。非表示のアプリケーションでも起動できます。利用不可かつ非表示にするには、別のグループに追加します。	可視性の制限
作業ディレクトリ	場所

アプリケーションの変更は、現在のアプリケーションユーザーがセッションからログオフするまで有効にならない場合があります。

アプリケーション制限を構成する

アプリケーションの使用状況を管理するために、アプリケーション制限を構成します。たとえば、アプリケーション制限を使用して、アプリケーションに同時にアクセスするユーザーの数を管理できます。同様に、アプリケーション制限は、リソースを大量に消費するアプリケーションの同時インスタンス数を管理するためにも使用できます。この制限は、サーバーのパフォーマンスを維持し、サービスの劣化を防ぐのに役立ちます。

この機能は、Controller によって仲介されるアプリケーションの起動数（Citrix Workspace アプリや StoreFront からの起動など）を制限するものであり、他の方法で起動できる実行中のアプリケーションの数を制限するものではありません。これは、アプリケーション制限が同時使用を管

理する際に管理者を支援するものの、すべてのシナリオで強制力を持つわけではないことを意味します。たとえば、Controller が停止モードの場合、アプリケーション制限は適用できません。

デフォルトでは、同時に実行できるアプリケーションインスタンスの数に制限はありません。アプリケーション制限の設定はいくつかあります。それらのいずれか、またはすべてを構成できます。

- デリバリーグループ内のすべてのユーザーによるアプリケーションの同時インスタンスの最大数。
- デリバリーグループ内のユーザーごとのアプリケーションのインスタンス数（1つ）。
- マシンごとのアプリケーションの同時インスタンスの最大数（PowerShell のみ）。

制限が構成されている場合、ユーザーが構成された制限を超えるアプリケーションインスタンスを起動しようとすると、エラーメッセージが生成されます。複数の制限が構成されている場合、最初に到達した制限でエラーが報告されます。

アプリケーション制限の使用例：

- **同時インスタンス数の最大制限:** デリバリーグループで、アプリケーション `Alpha` の同時インスタンスの最大数を 15 に構成します。その後、そのデリバリーグループのユーザーは、そのアプリケーションのインスタンスを 15 個同時に実行しています。そのデリバリーグループのいずれかのユーザーが `Alpha` を起動しようとすると、エラーメッセージが生成されます。`Alpha` は、構成された同時アプリケーションインスタンス制限（15）を超えるため、起動されません。
- **ユーザーごとのインスタンス数制限:** 別のデリバリーグループで、アプリケーション `Beta` のユーザーごとのインスタンス数オプションを有効にします。ユーザー Tony はアプリケーション `Beta` を正常に起動します。その日の後半、そのアプリケーションが Tony のセッションでまだ実行されている間に、彼は `Beta` の別のインスタンスを起動しようとします。エラーメッセージが生成され、`Beta` はユーザーごとのインスタンス数制限を超えるため、起動されません。
- **同時インスタンス数の最大制限とユーザーごとのインスタンス数制限:** 別のデリバリーグループで、同時インスタンスの最大数を 10 に構成し、アプリケーション `Delta` のユーザーごとのインスタンス数オプションを有効にします。その後、そのデリバリーグループの 10 人のユーザーがそれぞれ `Delta` のインスタンスを実行している場合、そのデリバリーグループの他のユーザーが `Delta` を起動しようとすると、エラーメッセージが表示されます。`Delta` は起動されません。現在の 10 人の `Delta` ユーザーのいずれかがそのアプリケーションの 2 番目のインスタンスを起動しようとすると、エラーメッセージが表示され、2 番目のインスタンスは起動されません。

- **マシンごとの同時インスタンス数の最大制限とタグ制限の使用:** アプリケーション `Charlie` には、特定のサーバーで同時に実行できるインスタンスの数を規定するライセンスおよびパフォーマンス要件があります。これらの要件は、サイト内のすべてのサーバーで同時に実行できるインスタンスの数も規定します。

  アプリケーションのインスタンス数/マシン制限は、サイト内のすべてのサーバーに影響します（特定のデリバリーグループ内のマシンだけでなく）。サイトに 3 台のサーバーがあるとします。アプリケーション `Charlie` の場合、マシンあたりのアプリインスタンス制限を 2 に構成します。したがって、サイト全体でアプリケーション `Charlie` のインスタンスは 6 つまでしか起動できません。（これは、3 台のサーバーそれぞれで Charlie のインスタンスが 2 つという制限です。）

  アプリケーションの使用をデリバリーグループ内の特定のコンピューターのみに制限するには（サイト全体のすべてのコンピューターでのインスタンス制限に加えて）：

  - それらのマシンにタグ付け機能を使用します。
  - そのアプリケーションのマシンごとの最大インスタンス数を構成します。

アプリケーションがControllerの仲介以外の方法（たとえば、Controllerが停止モードの場合など）で起動され、構成された制限を超過した場合、ユーザーは制限を超過しないように十分な数のインスタンスを閉じるまで、それ以上のインスタンスを起動できません。制限を超過したインスタンスは強制的にシャットダウンされません。ユーザーが閉じるまで継続して実行が許可されます。

セッションローミングを無効にする場合は、ユーザーごとのアプリケーションインスタンス数制限を無効にします。ユーザーごとのアプリケーションインスタンス数制限を有効にする場合は、新しいデバイスでの新しいセッションを許可する2つの値のいずれも構成しないでください。ローミングについて詳しくは、「セッション」を参照してください。

デリバリーグループごとの最大インスタンス数制限と、ユーザーごとのインスタンス数制限を構成するには：

1. 左側のペインで **［アプリケーション］** を選択し、アプリケーションを選択します。
2. アクションバーで **［アプリケーションプロパティの編集］** を選択します。
3. **［配信］** ページで、次のいずれかのオプションを選択します。

   - **アプリケーションの無制限の使用を許可する。** 同時に実行されるインスタンスの数に制限はありません。これがデフォルトです。
   - **アプリケーションの制限を設定する。** 制限の種類は2つあります。いずれかまたは両方を指定します。

    - マシンごとに同時に実行できるインスタンスの最大数を指定します
    - ユーザーごとにアプリケーションのインスタンスを1つに制限する

4. **［OK］** をクリックして変更を適用し、ダイアログボックスを閉じます。または、 **［適用］** をクリックして変更を適用し、ダイアログボックスを開いたままにします。

マシンごとの最大インスタンス数制限を構成するには（PowerShellのみ）：

- PowerShellで（Citrix Cloud™展開の場合はRemote PowerShell SDKを、オンプレミス展開の場合はPowerShell SDKを使用して）、適切な `BrokerApplication` コマンドレットを `MaxPerMachineInstances` パラメーターとともに指定します。
- ガイダンスについては、`Get-Help` コマンドレットを使用してください。例:

  ```
  Get-Help Set-BrokerApplication –Parameter MaxPerMachineInstances
  ```

公開アプリケーションにパラメーターを渡す

アプリケーションのプロパティの**場所**ページを使用して、コマンドラインを入力し、公開アプリケーションにパラメーターを渡します。

公開アプリケーションをファイルの種類に関連付けると、`"%*"` (二重引用符で囲まれたパーセント記号とアスタリスク記号) がアプリケーションのコマンドラインの末尾に追加されます。これらの記号は、ユーザーデバイスに渡されるパラメーターのプレースホルダーとして機能します。

公開アプリケーションが期待どおりに起動しない場合は、そのコマンドラインに正しい記号が含まれていることを確認してください。デフォルトでは、`"%*"` 記号が追加されると、ユーザーデバイスから提供されるパラメーターが検証されます。ユーザーデバイスから提供されるカスタマイズされたパラメーターを使用する公開アプリケーションの場合、コマンドライン検証をバイパスするために、`"%**"` 記号がコマンドラインに追加されます。アプリケーションのコマンドラインにこれらの記号が表示されない場合は、手動で追加してください。

実行可能ファイルへのパスにスペースを含むディレクトリ名が含まれている場合 (例: `"C:\Program Files"`)、スペースがコマンドラインの一部であることを示すために、アプリケーションのコマンドラインを二重引用符で囲みます。これを行うには、パスを二重引用符で囲み、`%*` 記号を別の二重引用符で囲みます。パスの閉じ引用符と `%*` 記号の開始引用符の間にスペースを含めるようにしてください。

たとえば、公開アプリケーションであるWindows Media Playerのコマンドラインは次のとおりです。

```
"C:\Program Files\Windows Media Player\mplayer1.exe" "%*"
```

注:

公開アプリケーションを起動するためのコマンドラインの最大文字数 (引数を含む) は203文字です。

公開アプリケーションでのセッションサインアウトの問題のトラブルシューティング

アプリケーションを公開する場合、公開アプリケーションのメインの実行可能ファイルのみが指定されます。ただし、一部のアプリケーションは、バックグラウンドで実行され、メインの公開アプリケーションが閉じられたときに、対応するメインの実行可能ファイルによって閉じられない追加の (子) プロセスを生成する場合があります。追加のプロセスは、実行されるスクリプトや、`Run` や `RunOnceKey` のような特定のレジストリキーから作成されることもあります。これらのアプリケーションは、正常なサインアウトを妨げ、セッションが残存またはハングアップする原因となり、セッションが閉じられず、ユーザーがサインアウトされない可能性があります。

この場合、Citrix Director を使用してこれらのセッションをリセットまたは終了する必要があります。

セッションが適切にサインアウトされない問題を特定し、トラブルシューティングするために、Citrix は3つのレジストリエントリを提供しています。これらの問題によりセッションが適切にログオフされないことの特定とトラブルシューティングは、次の3段階のプロセスです。

1. どのセッションが公開アプリケーションによって正常なサインアウトを妨げているかを特定する
2. それらの公開アプリケーションが追加の (子) プロセスを生成するかどうかを特定する
3. これらのプロセスを指定されたレジストリエントリに追加して、サインアウトを妨げないようにする

ステップ2：公開アプリケーションが追加の（子）プロセスを生成するかどうかを特定する

公開アプリケーションが正常なサインアウトを妨げていると特定されたら、次のステップは、このアプリケーションが実行時に追加のプロセスを生成するかどうかを判断することです。

公開アプリケーションが閉じられたときに、
`HKCU\Software\CitrixVolatile\Seamless\Sessions\[ID]`

`\LogoffCheckerBlockingProcess` を読んで、どのプロセスが正常なサインアウトをブロックしているかを判断できます。

以下の例では、キー `LogoffCheckerBlockingProcess` に次のエントリが含まれています。

```
PhoneExperienceHost.exe

SkypeApp.exe

SkypeBackgroundHost.exe
```

これらのプロセスが正常なサインアウトを妨げていました。

> **注:**
>
> 確認したいセッションの正しいセッションIDで を置き換えてください。

ステップ3：これらのプロセスを指定されたレジストリエントリに追加して、サインアウトを妨げないようにする

これらのプロセスを以下のレジストリキーに追加することで、今後のセッションでサインアウトが妨げられるのを防ぐことができます。

```
Add the process file name to the following registry key:

Caution! Refer to the Disclaimer at the end of this article before using
the Registry Editor.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI

Value Name:LogoffCheckSysModules

Type:REG_SZ

String:MyAppName.exe
```

`LogoffCheckSysModules` の詳細については、公開アプリケーションからの正常なログオフによりセッションがアクティブ状態になる を参照してください。

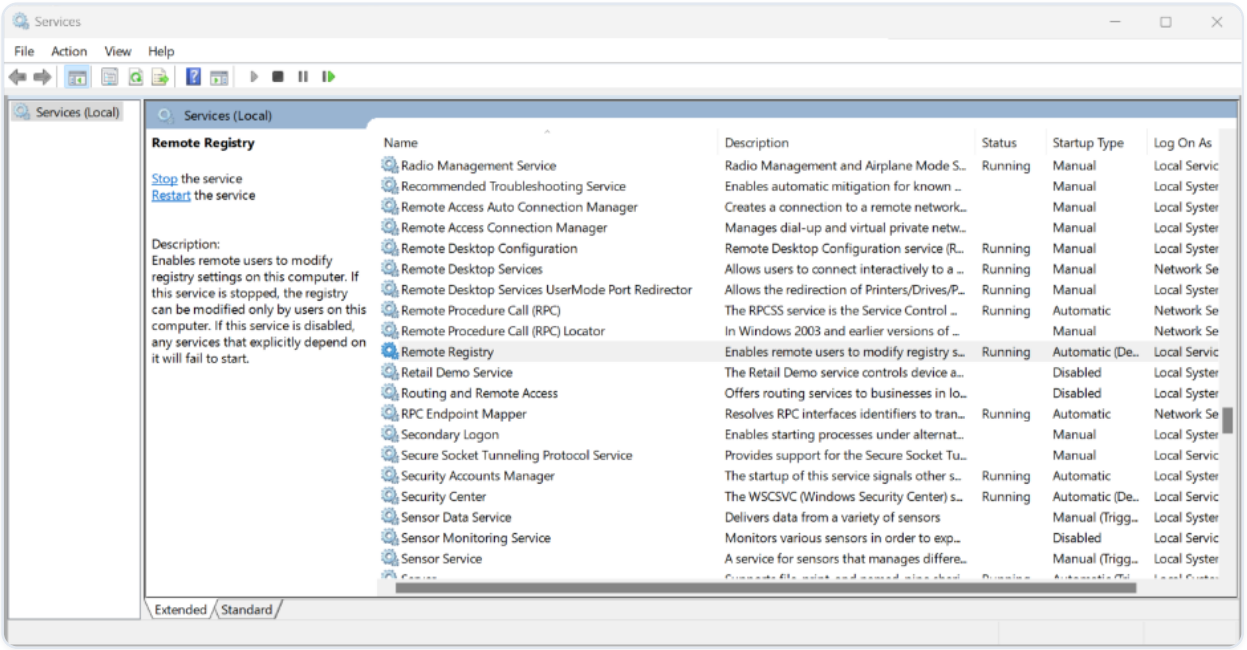
ステップバイステップのトラブルシューティングガイド

1. テスト対象のVDAでリモートレジストリサービスを開始します。

   a. コントロールパネルで、**管理ツール > サービス** を選択します。

   b. **リモートレジストリサービス** を右クリックし、**プロパティ** を選択します。

   c. **スタートアップの種類** で、ドロップダウンメニューから **自動** を選択します。



2. テスト対象のVDAでWindowsファイアウォールをオフにするか、ポート455を有効にする受信ファイアウォール規則を作成します:

   a. コントロールパネルで、**Windows Defender ファイアウォール > 詳細設定**を選択します。

   b. **受信の規則**を右クリックし、**新しい規則**を選択します。

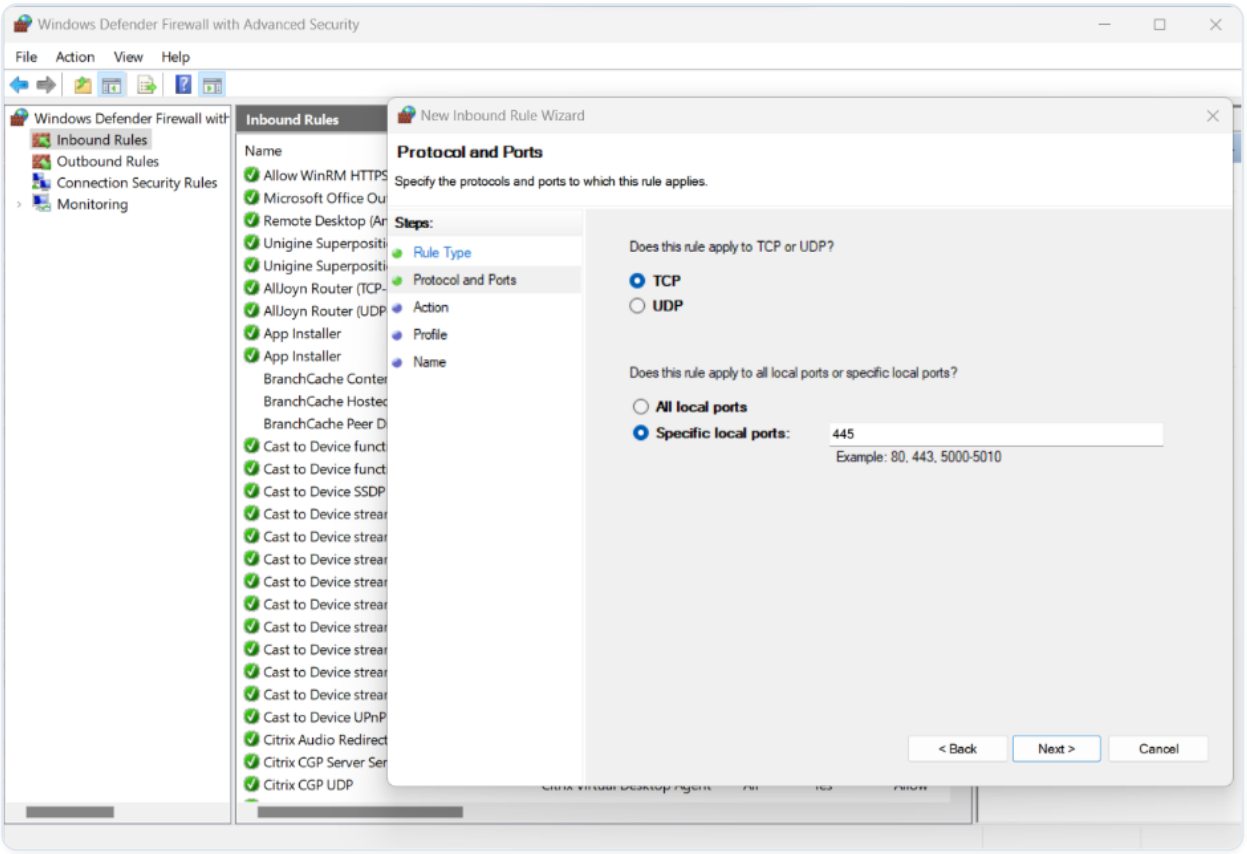
   c. **新しい受信の規則ウィザード**で、**ポート**を選択します。

   d. **プロトコルおよびポート**ページで、**TCP および特定のローカルポート**を選択します。ローカルポートとして `445` を入力します。

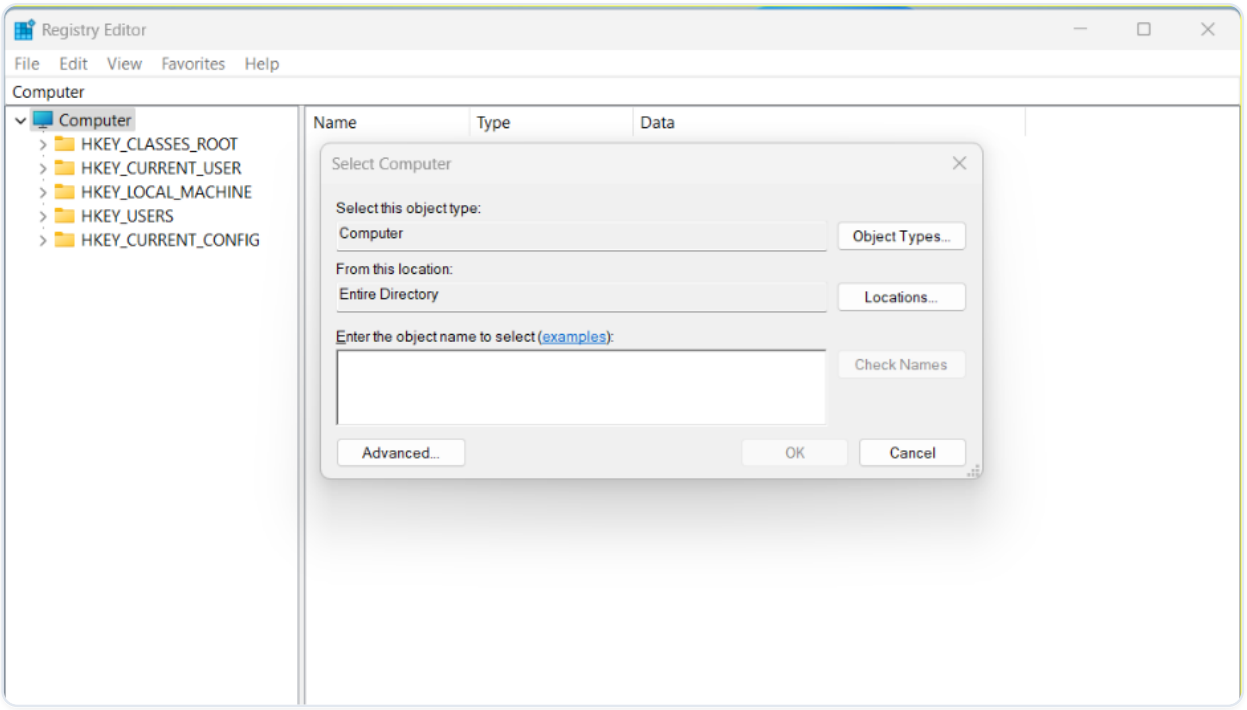
   e. **操作**ページで**接続を許可する**を選択します。

   f. 新しい受信規則を適用するファイアウォールプロファイルを選択します。

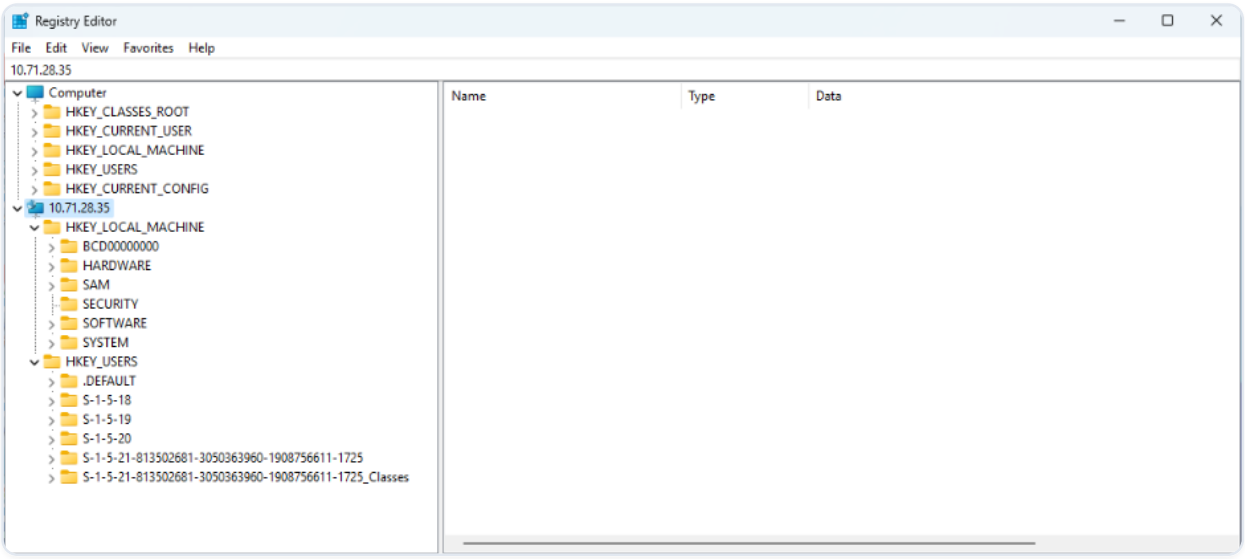
   g. ファイアウォール規則に名前を付け、**完了**を選択して**新しい受信の規則ウィザード**を終了します。



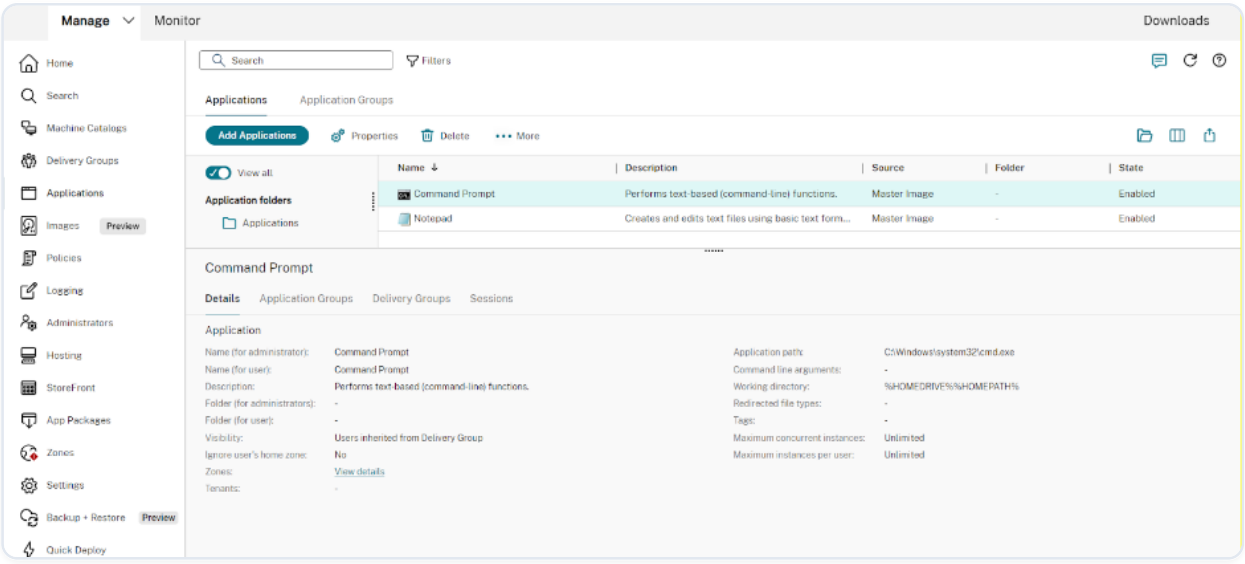
3. 同じドメイン上の別のVM（DC、DDC、または別のVDAでも可）から、`Regedit` を実行し、リモートレジストリに接続します。



4. テスト対象のVDAのIPアドレスを入力し、**OK**をクリックします。`regedit` ツリーには、テスト対象のVDAのブランチが表示されるはずです。



5. **コマンドプロンプト**公開アプリケーションを開きます。



Citrix Workspace に **コマンドプロンプト** アプリが表示されます。

公開アプリのコマンドプロンプト(/en-us/citrix-virtual-apps-desktops/current-release/media/published-app-cmd-prompt.png)

6. クライアントで **Connection Center** を開きます。これは、開いているシームレスアプリを閉じた後にセッションがサインアウトされたときに監視するために使用されます。次の画像では、リモート VDI でコマンドプロンプトプロセス `c:\Windows\system32\cmd.exe` がアクティブになっていることがわかります。

   公開アプリの接続(/en-us/citrix-virtual-apps-desktops/current-release/media/published-app-citrix-workspace-connection-center.png)

7. **regedit** が実行されている VDA から、次のリモート IP の場所に移動します。
   `HKEY_USERS\S-1-X-XX-XXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-XXXX\SOFTWARE\CitrixVolatile\Seamless\Sessions\X\`

> **注:**
>
> 新しいセッションを開くたびにこのパスは変更されます。

8. ここで読み取るキーは 2 つあります (ここでは変更しないでください)。**LogoffCheckBlockingProcess** と **LogoffCheckerBlockingVisibleProcess** です。これらのキーは、サインアウトをブロックしているプログラムを表示します。最初のキーには、それが開いていてまだ閉じられていないため、`C:\Windows\System32\cmd.exe` が表示されているはずです。

   > **注:**
   >
   > **LogoffCheckBlockingProcess** と **LogoffCheckerBlockingVisibleProcess** は手動で編集しないでください。これらのレジストリ値を手動で編集すると、セッションが不安定になる可能性があります。

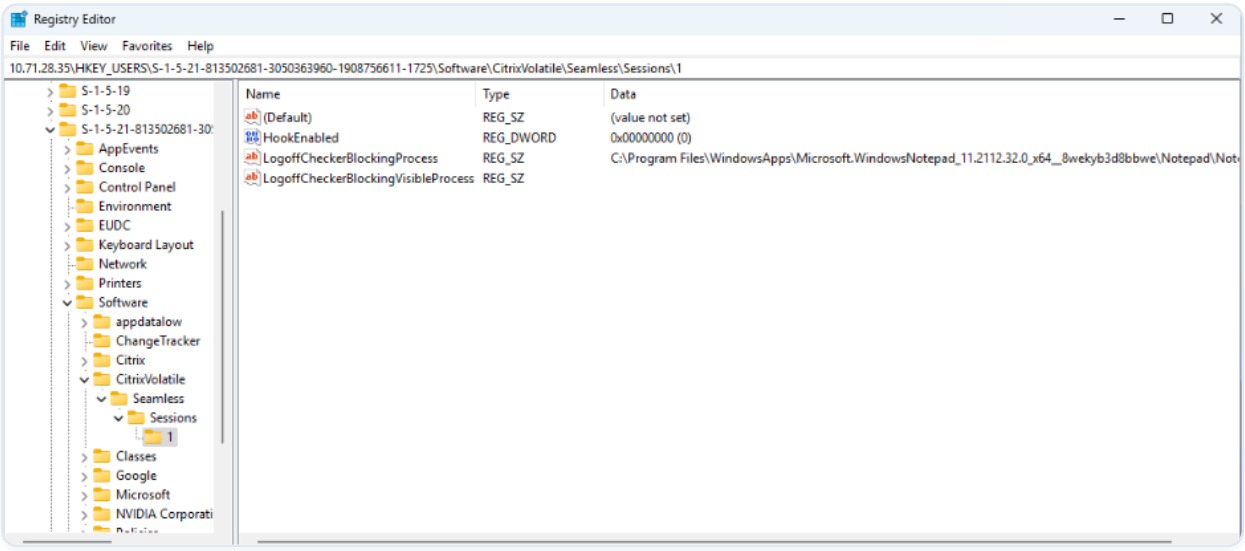
   > 公開アプリ 2(/en-us/citrix-virtual-apps-desktops/current-release/media/published-app-regedit-2.png)

9. 右上隅の **X** をクリックして **Seamless CMD** を終了します。
10. セッションが閉じるかどうか、接続センターを確認します。閉じるまでに最大 30 秒かかる場合があります。閉じれば、正常なサインアウトを妨げたアプリケーションやプロセスはなかったことになります。

    正常なサインアウト(/en-us/citrix-virtual-apps-desktops/current-release/media/published-app-bwd.png)

11. セッションが閉じなかった場合は、F5 キーで **regedit** の出力を更新します。
12. **LogoffCheckBlockingProcess** と **LogoffCheckerBlockingVisibleProcess** の内容を再度確認します。CMD は表示されなくなっているはずですが、別のプロセスが一覧表示されているはずです。現在セッションのサインアウトをブロックしているプロセスがここに表示されているはずです。

    この場合、コマンドプロンプトが閉じられる前に、公開されたコマンドプロンプトから **Notepad.exe** が開かれており、このリモートのメモ帳プロセスが正常なサインアウトを妨げています。



13. この実行可能ファイルへのパスと、それが表示されたキーをメモし、リモートツリーの下にある以下のレジストリキーに入力します。

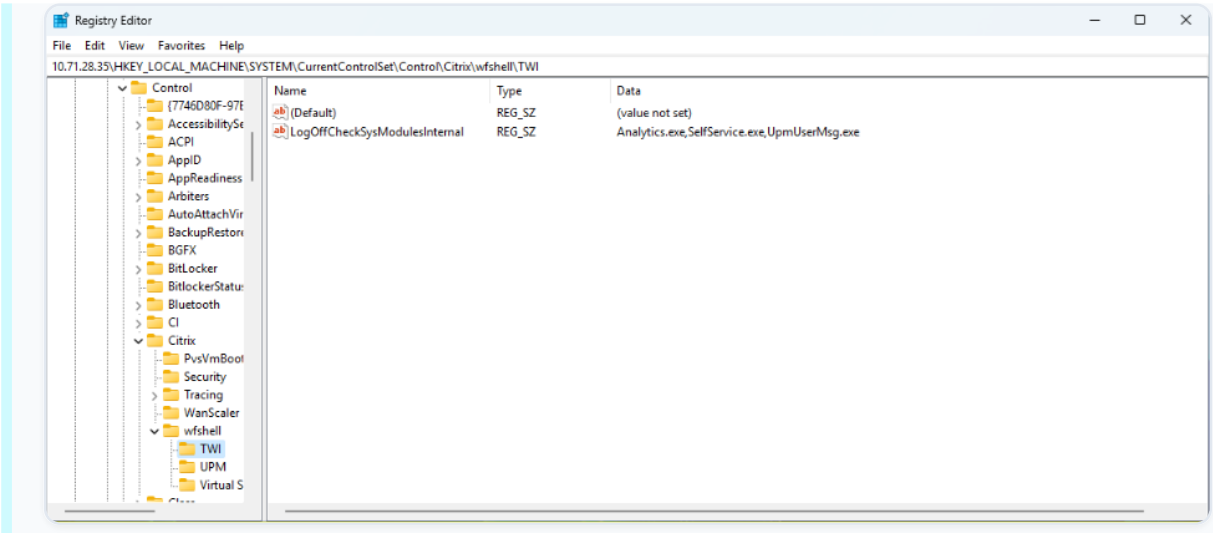
    - **LogoffCheckBlockingProcess** に表示される場合:

      `HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWILogoffCheckSysModulesInterna`

    - **LogoffCheckerBlockingVisibleProcess** に表示される場合:

      `HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWILogoffCheckVisibleSysModules`

> **注:**
>
> キーにすでに1つ以上のエントリがある場合は、末尾にコンマを追加し、そのコンマの後に新しいエントリを配置します。



14. クライアントの接続センターからセッションをサインアウトし、リモートアプリケーションを再度開きます。

15. リモートアプリケーションを閉じてから30秒以内にセッションが自動的にサインアウトされるまで、手順9〜16を繰り返します。

> **注:**
>
> トラブルシューティング後、必要に応じて、リモートレジストリへのアクセスを許可するための一時的なファイアウォールの変更を元に戻します。

公開アプリケーションを開くときにWindowsの免責事項メッセージを全画面表示で見るためにLogonUIを変更する方法

認証パススルーが発生しないシナリオ向けに、**LogonUI**ウィンドウのスケーリングが改善されました。**LogonUI**ウィンドウは、使用されているモニターの解像度とDPI設定に基づいてスケーリングされ、これにより、完全な**LogonUI**ウィンドウがクリッピングなしで表示されることが保証されます。

ピクセル単位のウィンドウサイズは、レジストリで手動で設定することもできます。

1. **ファイル名を指定して実行**コマンドで`regedit`を使用して**レジストリエディター**を開きます。
2. `HKEY_LOCAL_MACHINE\Software\Citrix\CtxHook\AppInit_DLLS\Seamless Hook\`に移動します。
3. 2つの新しいDWORDキー、**LogonUIWidth**と**LogonUIHeight**を作成します。
4. **LogonUI**ウィンドウのキーの値を、必要な幅と高さ（ピクセル単位）に設定します。

   LogonUI ウィンドウのサイズを手動で設定すると、自動スケーリングは無効になります。

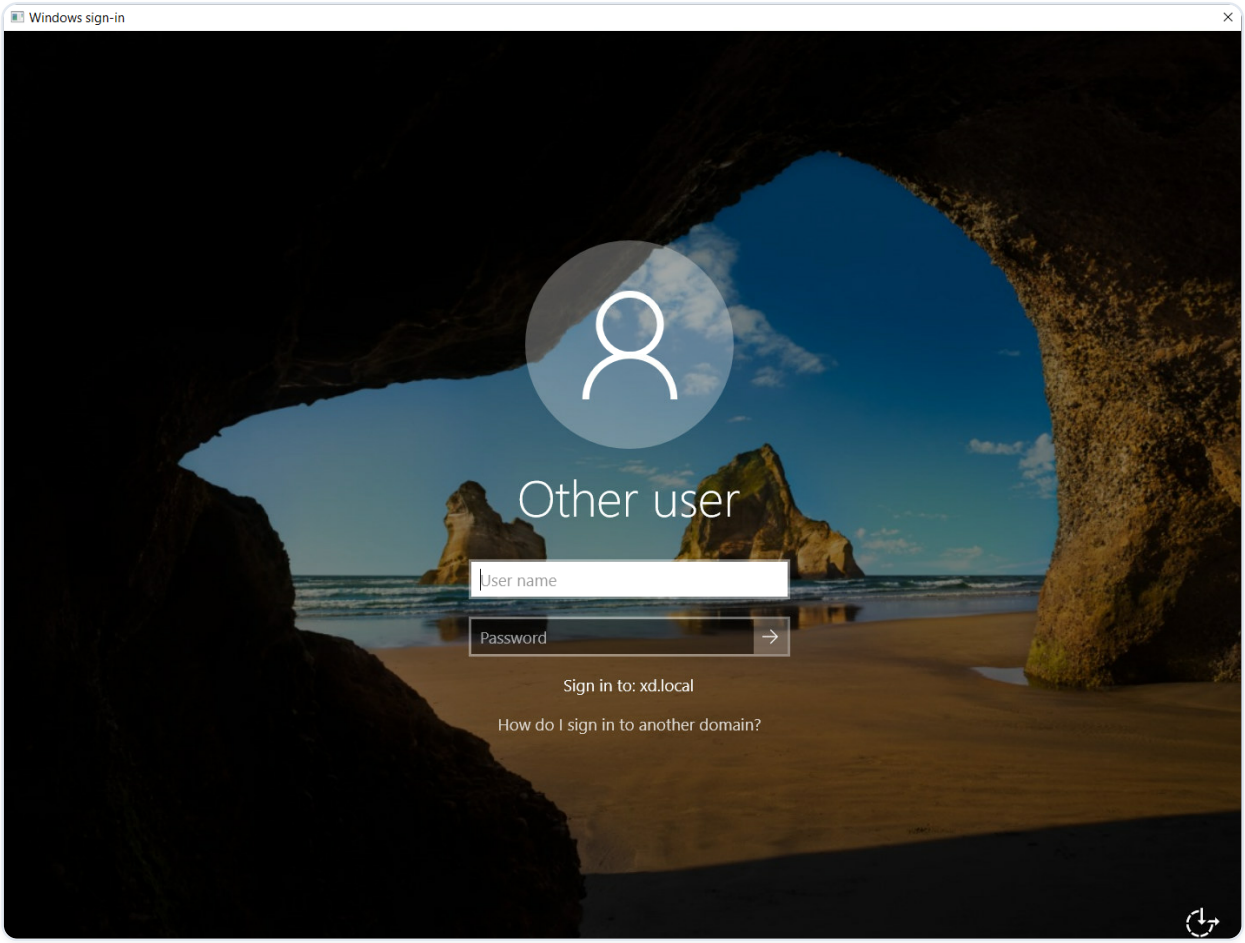
> **注:**
>
> これらのレジストリパスは2407以降変更されました。古いレジストリ値は無視され、非推奨です。

> デフォルトでは、**LogonUI** ウィンドウにはタイトルバーと閉じるボタンが含まれており、必要に応じてエンドユーザーがセッションから切断できるようになっています。

タイルバーを無効にする

LogonUI ウィンドウのタイルバーは、以下のレジストリキーで無効にできます。

1. **ファイル名を指定して実行** コマンドで `regedit` を使用してレジストリエディターを開きます。
2. `HKEY_LOCAL_MACHINE\Software\Citrix\CtxHook\AppInit_DLLS\Seamless Hook\` に移動します。
3. 新しいDWORDキー: **LogonUICaption** を作成し、そのキーの値を `0` に設定します。



アプリケーションフォルダーの管理

デフォルトでは、デリバリーグループに追加する新しいアプリケーションは、**Applications**という名前のフォルダーに配置されます。デリバリーグループの作成時、アプリケーションの追加時、または後で別のフォルダーを指定できます。

知っておくと良いこと:

- Applicationsフォルダーの名前を変更したり削除したりすることはできませんが、その中に含まれるすべてのアプリケーションを、作成した他のフォルダーに移動することはできます。

- フォルダー名には1～64文字を含めることができます。スペースも使用できます。
- フォルダーは最大5レベルまでネストできます。
- フォルダーにアプリケーションを含める必要はありません。空のフォルダーも許可されます。
- フォルダーは、移動したり、作成時に別の場所を指定したりしない限り、Web Studioでアルファベット順に表示されます。
- 同じ名前のフォルダーを複数持つことができますが、それぞれ異なる親フォルダーを持つ必要があります。同様に、同じ名前のアプリケーションを複数持つことができますが、それぞれ異なるフォルダーに存在する必要があります。
- フォルダー内のアプリケーションを表示するには`View Applications`権限が必要です。また、アプリケーションを含むフォルダーを削除、名前変更、または削除するには、そのフォルダー内のすべてのアプリケーションに対して`Edit Application Properties`権限が必要です。
- 以下のほとんどの手順では、Web Studio のアクションバーを使用してアクションを要求します。または、右クリックメニューを使用するか、項目をドラッグすることもできます。たとえば、意図しない場所にフォルダーを作成または移動した場合、ドラッグアンドドロップで正しい場所に移動できます。
- Web Studio のすべてのノード（**マシンカタログ**、**デリバリーグループ**、**アプリケーション**、**アプリケーショングループ**など）は、バックエンドで同じフォルダーツリーを共有します。フォルダーの名前変更や移動の際に名前の競合を避けるため、異なるノード間で最上位フォルダーには一意の名前を使用してください。

  `New-BrokerAdminFolder` SDK コマンドレットを使用してフォルダーを作成し、それを**アプリケーション**ノードの下に表示させたい場合は、`Set-BrokerAdminFolderMetadata`コマンドレットを使用して`ContainsApplications`メタデータを追加する必要があります。

  例:

  ```
  Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
  ContainsApplications -Value true
  ```

アプリケーションフォルダーを管理するには、左ペインで**アプリケーション**を選択します。以下のリストを参考にしてください。

- **すべてのフォルダー（ネストされたフォルダーを除く）を表示するには：** フォルダーリストの上にある**すべて表示**をクリックします。

- **最上位レベル（ネストされていない）にフォルダーを作成するには：** **アプリケーション**フォルダーを選択します。新しいフォルダーを**アプリケーション**以外の既存のフォルダーの下に配置するには、そのフォルダーを選択します。次に、アクションバーで**フォルダーの作成**を選択します。名前を入力します。
- **フォルダーを移動するには：** フォルダーを選択し、アクションバーで**フォルダーの移動**を選択します。ネストされたフォルダーが含まれていない限り、一度に1つのフォルダーしか移動できません。（フォルダーを移動する最も簡単な方法は、ドラッグすることです。）
- **フォルダーの名前を変更するには：** フォルダーを選択し、アクションバーで**フォルダー名の変更**を選択します。名前を入力します。
- **フォルダーを削除するには：** フォルダーを選択し、アクションバーで**フォルダーの削除**を選択します。アプリケーションや他のフォルダーを含むフォルダーを削除すると、それらのオブジェクトも削除されます。アプリケーションを削除すると、デリバリーグループからのアプリケーション割り当てが削除されます。マシンからは削除されません。
- **アプリケーションをフォルダーに移動するには：** 1つまたは複数のアプリケーションを選択します。次に、アクションバーで**アプリケーションの移動**を選択します。フォルダーを選択します。

デリバリーグループまたはアプリケーショングループを作成する際に、**アプリケーション**ページで追加するアプリケーションをフォルダーに配置することもできます。デフォルトでは、追加されたアプリケーションは**アプリケーション**フォルダーに入ります。**変更**をクリックしてフォルダーを選択または作成します。

公開デスクトップでのアプリケーションのローカル起動を制御する

ユーザーが公開デスクトップ内から公開アプリケーションを起動する際、そのデスクトップセッションでアプリケーションを起動するか、公開アプリケーションとして起動するかを制御できます。Citrix Workspaceアプリは、VDA上のWindowsレジストリでアプリケーションのインストールパスを検索し、存在する場合はアプリケーションのローカルインスタンスを起動します。それ以外の場合は、ホストされたアプリケーションのインスタンスが起動されます。VDAにインストールされていないアプリケーションを起動すると、ホストされたアプリケーションが起動されます。詳細については、「vPrefer起動」を参照してください。

PowerShell（Citrix Cloud展開環境ではRemote PowerShell SDK、オンプレミス展開環境ではPowerShell SDKを使用）で、このアクションを変更できます。

`New-Broker` Applicationまたは`Set-BrokerApplication` コマンドレットで、`LocalLaunchDisabled` オプションを使用します。例：

```
Set-BrokerApplication -LocalLaunchDisabled <Boolean>
```

デフォルトでは、このオプションの値はfalse（`-LocalLaunchDisabled $false`）です。公開デスクトップ内から公開アプリケーションを起動すると、そのデスクトップセッション内でアプリケーションが起動されます。

オプションの値をtrue（`-LocalLaunchDisabled $true`）に設定すると、公開アプリケーションが起動されます。これにより、公開デスクトップから公開アプリケーションへの個別の追加セッションが（Citrix Workspaceアプリ for Windowsを使用して）作成されます。

要件と制限：

- アプリケーションの`ApplicationType`の値は`HostedOnDesktop`である必要があります。
- このオプションは、適切なPowerShell SDKを介してのみ利用可能です。現在、Web Studioのグラフィカルインターフェイスでは利用できません。
- このオプションには、StoreFront 3.14、Citrix Receiver for Windows 4.11、およびDelivery Controller 7.17が最低限必要です。

アプリパッケージ

アプリパッケージは、Citrix® が管理する事前構成されたアプリケーション展開です。これにより、アプリケーションを仮想化できます。これは、アプリケーションがユーザーデバイスのオペレーティングシステムやインターフェイスから独立して実行されることを意味します。

アプリパッケージは、アプリケーション管理を簡素化し、ITのオーバーヘッドを削減し、アプリケーションがライフサイクル全体を通じて安全かつ機能的であることを保証します。

Citrix は、ユーザーにアプリケーションを配信するために、以下のパッケージングテクノロジーをサポートしています。

- App-V アプリケーション
- MSIX および MSIX app attach アプリケーション
- FlexApp アプリケーション
- Elastic App アプリケーション
- Cloudpaging アプリケーション

この記事では、Citrix Virtual Apps and Desktops™ 環境でこれらのパッケージ化されたアプリケーションを展開および配信する方法について説明します。

> **注:**

- バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™ の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。
- アプリケーションパッケージの展開と配信に Web Studio と Citrix Studio を相互に利用することはお勧めしません。それぞれ異なるメカニズムを使用しているため、App-V サーバーの情報が一方では正しく表示されるが、もう一方では表示されないといった不一致が生じる可能性があります。また、Citrix Studio は App-V のみをサポートしていることに注意してください。

App-V アプリケーション

Application Virtualization (App-V) は、エンドユーザーのデバイスにインストールすることなく、アプリケーションをストリーミングしてアクセスできるようにする Microsoft のテクノロジーです。Citrix Virtual Apps and Desktops は App-V を使用してアプリケーションを配信でき、さまざまなクライアントマシン間でアプリケーションを管理するための集中化された効率的な方法を提供します。

App-V パッケージアプリケーションを配信する際に操作するコンポーネントと概念の詳細については、Microsoft のドキュメント「Application Virtualization (App-V) for Windows client overview」を参照してください。

重要な用語

- **管理サーバー**: App-V インフラストラクチャを管理するための一元化されたコンソールを提供し、App-V デスクトップクライアントとリモートデスクトップサービスクライアントの両方に仮想アプリケーションを配信します。App-V 管理サーバーは、管理者に必要なセキュリティ、測定、監視、およびデータ収集を認証、要求、提供します。このサーバーは、Active Directory とサポートツールを使用してユーザーとアプリケーションを管理します。
- **パブリッシングサーバー**: 特定のユーザー向けにアプリケーションをApp-Vクライアントに提供し、ストリーミング用の仮想アプリケーションパッケージをホストします。パッケージは管理サーバーから取得します。
- **動的構成ファイル**: App-Vパッケージは動的構成ファイルを使用してカスタマイズできます。これをパッケージに適用すると、その特性を変更できます。たとえば、追加のアプリケーションショートカットや動作を定義するために使用できます。詳細については、「動的構成ファイル」を参照してください。

動的構成ファイル

Citrix App-Vは、両方の種類の動的構成ファイルをサポートしています。ファイル設定は、アプリケーションの起動時に適用されます。

- **展開構成ファイル**: すべてのユーザーに対してマシン全体の構成を提供します。これらのファイルは`<packageFileName>_DeploymentConfig.xml`という名前で、適用先のApp-Vパッケージと同じフォルダーにある必要があります。これらのファイルは、シングルおよびデュアル管理者管理でサポートされています。
- **ユーザー構成ファイル**: パッケージに対するユーザーごとのカスタマイズをサポートする、ユーザー固有の構成を提供します。シングル管理者では、`<packageFileName>_[UserSID | Username | GroupSID |GroupName_]UserConfig.xml`という形式で名前が付けられ、適用先のApp-Vパッケージと同じフォルダーにあるユーザー構成ファイルがサポートされます。

  特定のパッケージに対して複数のユーザー構成ファイルが存在する場合、それらは次の優先順位で適用されます。

  a. ユーザーSID
  b. ユーザー名
  c. ADグループSID (最初に見つかったものが優先)
  d. ADグループ名 (最初に見つかったものが優先)
  e. デフォルト

  例:

```
MyAppVPackage_S-1-5-21-000000001-0000000001-000000001-001_UserConfig.xml

MyAppVPackage_joeblogs_UserConfig.xml

MyAppVPackage_S-1-5-32-547_UserConfig.xml

MyAppVPackage_Power Users_UserConfig.xml

MyAppVPackage_UserConfig.xml
```

> **注:**

> ファイル名のユーザー固有の部分は、オプションで末尾に配置することもできます (例: `MyAppVPackage_UserConfig_joeblogs.xml`)。

重要:

パッケージ内のアプリケーションでユーザーセッションが開いている場合、動的展開構成に変更を適用することはできません。他のユーザー（ただし現在のユーザーではない）がパッケージ内のアプリケーションを開いている場合、動的ユーザー構成ファイルに変更を適用できます。

動的構成ファイルの場所

シングル管理者管理では、Citrix App-Vコンポーネントは、App-Vパッケージと同じフォルダーにある動的構成ファイルのみを処理します。

パッケージ内のアプリケーションが起動されると、対応する動的構成ファイルへの変更が再適用されます。動的構成ファイルがパッケージとは異なる場所にある場合は、マッピングファイルを使用してパッケージを展開構成ファイルにマッピングします。

マッピングファイルを作成するには:

1. 新しいテキストファイルを開きます。
2. 各動的構成ファイルについて、`<PackageGuid> : path`の形式を使用してパッケージへのパスを指定する行を追加します。

   例:

   ```
   F1f4fd78ef044176aad9082073a0c780 : c:\widows\file\packagedeploy.xml
   ```

3. ファイルを`ctxAppVDynamicConfigurations.cfg`として、パッケージと同じフォルダーに保存します。

App-Vパッケージと同じUNC共有上のディレクトリ階層全体が、パッケージ内のアプリケーションが起動されるたびに、このファイルについて再帰的に上位検索されます。

方法

App-Vパッケージを配信および管理するには、次の方法を使用できます:

- **デュアル管理者**: この方法では、Citrix Virtual Apps and Desktops と App-V サーバーが連携してパッケージを配信および管理します。この方法では、Citrix Virtual Apps and Desktops が App-V サーバーの状態のスナップショットビューを定期的に更新する必要があります。これには、ハードウェア、インフラストラクチャ、および管理のオーバーヘッドが発生します。Citrix Virtual Apps and Desktops と App-V サーバーは、特にユーザー権限に関して同期を維持する必要があります。

  この方法は、App-VとCitrixが密接に連携する展開で最適に機能します。この方法では:

  - **App-V管理サーバー**は動的構成ファイルを処理します
  - **App Packages Delivery Component** (VDAマシンにインストール): アプリケーションの起動に必要な適切な公開サーバーの登録を管理します。

  これにより、公開サーバーが適切なタイミングでユーザーと同期されます。公開サーバーは、構成されている設定を使用して、アプリケーションパッケージのライフサイクルの他の側面（ログオン時の更新や接続グループなど）を維持します。
- **シングル管理者**: アプリケーションパッケージはネットワーク共有に保存されます。Citrix Virtual Apps and Desktops は、パッケージを独立して配信および管理します。

  この方法により、展開においてApp-Vサーバーとデータベースインフラストラクチャが不要になるため、オーバーヘッドが削減されます。

  この方法では、App-Vパッケージをネットワーク共有に保存し、その場所からメタデータを環境にアップロードします。その後、VDAマシンにインストールされているApp Packages Delivery Componentが、次のようにアプリケーションを管理および配信します。

  - アプリケーションが起動されたときに、展開構成ファイルとユーザー構成ファイルを処理します。
  - ホストマシン上のパッケージのライフサイクルのすべての側面を管理します。

注:

- 1つまたは両方の管理方法を同時に使用できます。つまり、アプリケーションをデリバリーグループに追加すると、アプリケーションはApp-Vサーバーまたはネットワーク共有にあるApp-Vパッケージから取得できます。
- 両方の管理方法を同時に使用しており、App-Vパッケージが両方の場所に動的構成ファイルを持っている場合、App-Vサーバー内のファイル（デュアル管理）が使用されます。

- Web Studioのナビゲーションペインで App packagesを選択すると、パッケージ名と種類が表示されます。**Package type**列は、パッケージの配信に使用されるテクノロジーと、**Application Library**で参照される場所を示します。パッケージを選択すると、詳細ペインにパッケージ内のアプリケーションとショートカットが一覧表示されます。

MSIXおよびMSIXアプリ添付アプリケーション

MSIXはWindowsアプリパッケージ形式であり、すべてのWindowsアプリに最新のパッケージングエクスペリエンスを提供します。MSIXは、Win32、.NET、UWPアプリなど、さまざまなWindowsアプリケーションタイプに適しています。

MSIXアプリ添付は、パッケージの内容をストリーミングするのではなく、仮想ハードディスクに事前に展開され、必要に応じてターゲットマシンにマウントできるMSIXパッケージを利用します。これにより、展開時間を短縮し、ネットワークトラフィックを削減し、ターゲットマシンでのIOPSを低減できますが、アプリ添付ディスクの作成と維持には追加の作業が必要です。

Citrix Virtual Apps and Desktops は、VDA マシンにインストールされている**App Packages Delivery Component**を介して、MSIX および MSIX app attach アプリケーションをユーザーに配信します。このコンポーネントは、ホストマシン上のパッケージのライフサイクルに関するすべての側面を管理します。

MSIX および MSIX app attach の詳細については、Microsoft のドキュメント「MSIX documentation」と「App Attach in Azure Virtual Desktop」をそれぞれ参照してください。

注:

- ネイティブの MSIX パッケージはデスクトップおよびサーバー VDA でサポートされており、MSIX app attach はデスクトップ VDA の `.vhd`、`.vhdx`、および `.cim` ディスクイメージ形式でのみサポートされています。
- Microsoft は Server 2019 用の AppAttach 実装を提供していません。AppAttach は Server 2022 および 2025 に存在しますが、Microsoft はこれらのバージョンでのサポートを提供していません。したがって、弊社も Server 2022 および 2025 での AppAttach をサポートしていません。
- Windows Server 2019 でサイドローディングを有効にします。
- VDA がパッケージの署名に使用されている証明書を信頼していることを確認してください。

FlexApp アプリケーション

FlexApp は Liquidware が開発したアプリケーションレイヤリングソリューションで、従来のアプリケーションインストールプロセスを通じて基盤となるベースイメージを変更することなく、任意のアプリケーションを Windows セッションにアタッチします。

FlexApp One アプリケーションは、単一の共有可能なファイルにカプセル化されており、Windows セッションに追加のアプリケーションレイヤーを必要とせずに動作できます。ユーザーはコンテナファイルをクリックすることでアプリケーションを起動でき、1つまたは複数のアプリケーションを Windows ワークスペースに迅速に統合できます。

Citrix は、VDA マシンにインストールされている App Packages Delivery Component と FlexApp delivery agent を介して、FlexApp アプリケーションをユーザーに提供します。これら2つのコンポーネントは、ホストマシン上のパッケージのライフサイクルのあらゆる側面を管理します。

Elastic App アプリケーション

Elastic App テクノロジーは、Citrix App Layering の機能であり、アプリケーションレイヤーをベースイメージにインストールするのではなく、ログオン時にユーザーに動的に割り当てることができます。Elastic App テクノロジーを使用すると、アプリケーションは異なる仮想マシン間でユーザーに追従し、マスターイメージを肥大化させることなく、必要なアプリに常にアクセスできるようにします。

Citrix Virtual Apps and Desktopsは、Citrix PersonalizationコンポーネントとApplication Layering Enterprise Layer Manager (ELM) を介して、Elastic Appアプリケーションをユーザーに配信します。これら2つのコンポーネントは、ホストマシン上のパッケージのライフサイクルのすべての側面を管理します。Application Layering Enterprise Layer Managerの詳細については、Citrix App Layering™ ドキュメントを参照してください。

Cloudpaging アプリケーション

Cloudpaging は、Numecent のアプリケーションストリーミングテクノロジーであり、ベースイメージに変更を加えることなく、Windows セッションにアプリケーションを配信します。

Cloudpaging を使用すると、コードのごく一部（通常は 10% 未満）のみが最初にストリーミングされるため、アプリケーションはほぼ瞬時に起動します。残りのコンポーネントは、ユーザーがアクセスしたときにバックグラウンドでストリーミングされ、シームレスなエクスペリエンスを提供します。

Citrix 環境では、VDA 上の App Packages Delivery Component が Numecent Cloudpaging Player と連携してアプリケーションのライフサイクルを管理します。Citrix コンポーネントは配信を調整し、Cloudpaging Player はセッション内でのオンデマンドストリーミングと実行を処理します。

構成要件

次の構成の詳細を考慮してください。

クラウドページング プレイヤー と LOGOFFCHECKSYSMODULES

Cloudpaging コンテナで仮想公開アプリケーションを使用する場合、セッションのログオフを許可するには、次の設定を構成します。

設定	値
レジストリキー	`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI`
値の名前	`LogoffCheckSysModules`
値の型	`REG_SZ`
値データ	`CoreHelper.exe`

ホワイトリスト登録用のURL

標準のURLホワイトリスト登録要件に加えて、VDAは次のエンドポイントへのアクセスを必要とします。

パラメーター	値
URL	`external-api.cloudpager.net`
ポート	443
クライアント	Cloudpager PoSh モジュール
Webベースのフォワードプロキシ構成	• アウトバウンドアクセス許可 • 認証バイパスが必要
説明	Cloudpager PowerShellモジュール

オプションで、Cloudpagerの検出のみを実行するために使用されるVDAを含む専用のデリバリーグループを作成して、必要なホワイトリストURLを制限できます。**VDAバージョン2511以降**と**App packages Delivery Component**がインストールされているマシンを含むデリバリーグループを作成することをお勧めします。

Cloudpagerクライアントのネットワークおよびファイアウォールの要件の詳細については、Numecentナレッジベースの記事を参照してください。

アプリケーションパッケージの展開と配信

前提条件

App-V、MSIX、MSIX app attach、FlexAppパッケージ、Elastic Appアプリケーション、およびCloudpagingパッケージの配信をサポートするには、まずVDAマシンに**App Packages Delivery Component**をインストールする必要があります。詳細については、VDAマシンにApp Packages Delivery Componentをインストールするを参照してください。

VDAマシンへのAPP PACKAGES DELIVERY COMPONENTのインストール

App Packages Delivery Componentは、App-V、MSIX、MSIX app attach、FlexApp、Elastic App、およびCloudpaging形式のアプリケーションパッケージの公開プロセスを管理します。このコンポーネントは、VDAをインストールするときにデフォルトではインストールされません。このコンポーネントは、VDAのインストール中またはインストール後にインストールできます。

VDAのインストール中にコンポーネントをインストールするには、次のいずれかの方法を使用します。

- インストールウィザードで、**追加コンポーネント**ページに移動し、**App Packages Delivery Component**チェックボックスを選択します。
- コマンドラインインターフェイスで、`/includeadditional "Citrix Personalization for App-V – VDA"`オプションを使用します。

VDAのインストール後にコンポーネントをインストールするには、次の手順に従います。

1. VDAマシンで、**コントロールパネル > プログラム > プログラムと機能**に移動し、**Citrix Virtual Delivery Agent**を右クリックして、**変更**を選択します。
2. 表示されるウィザードで、**追加コンポーネント**ページに進み、**App Packages Delivery Component**チェックボックスを有効にします。

> **注:**

- Microsoft App-V Desktop Client は、ユーザーデバイスで App-V パッケージから仮想アプリケーションを実行するコンポーネントです。Windows 10 (1607 以降) および Windows Server 2019 以降には、この App-V クライアントソフトウェアがすでに含まれています。VDA マシンでのみ有効にする必要があります。詳細については、この Microsoft ドキュメント記事を参照してください: App-V インボックスクライアントを有効にする。
- FlexApp アプリケーションの場合は、App Packages Delivery Component とともに VDA に FlexApp One Agent をインストールします。
- Elastic App アプリケーションの場合は、App Packages Delivery Component とともに VDA に App Layering 対応イメージをインストールします。
- Cloudpaging アプリケーションの場合は、App Packages Delivery Component とともに VDA に Cloudpaging Playerをインストールします。

FLEXAPP ONE AGENT をインストールする

1. VDA で管理者コマンドプロンプトを起動します。
2. 任意の FlexApp One Package のネットワークパスを見つけます。
3. 次のコマンドを入力します。

```
\\path\to\any\FlexAppOnePackage.exe --install
```

4. 表示されるプロンプトをすべて承認します。

APP LAYERING 対応イメージをインストールする

1. アプリレイヤリングを設定します。 Citrix App Layering ドキュメントの指示に従ってください。プロセスには以下が含まれます。
   a. Enterprise Layer Manager (ELM) を設定します。
   b. ゴールド OS イメージをインポートします。
   c. プラットフォームレイヤーを作成します。
   d. アプリケーションレイヤーを作成します。
   e. ELMで、配信する各アプリケーションレイヤーに対して、**Studio App Packagesでの使用をこのApp Layerで有効にする**チェックボックスを選択します。
2. Elastic Layeringコンポーネントを含むイメージをVDAマシンにインストールします。次のいずれかの方法を使用できます。

a. Elastic Layeringを有効にして、ELMからイメージを展開します。
b. マシンにVDAを手動でインストールし、セットアップ中にElastic Layeringコンポーネントを選択します。

CLOUDPAGING PLAYERをインストールする

1. VDAで管理者コマンドプロンプトを開きます。
2. Cloudpaging Playerインストーラーが含まれているフォルダーに移動します。
3. プレーヤーをサイレントインストールし、SaaSコンソールURLを構成するには、次のコマンドを実行します。必要に応じてプレースホルダー値を置き換えてください。

```
cloudpaging-player-setup-x64-release.exe /S /v"/qn ADDLOCAL=ALL
REG_BASTOKENPATHORURL=https://your-tenant-url/api/token"
```

4. (オプション) インストール後に、次のレジストリ値を確認して構成を検証します。

- **パス:** `HKEY_LOCAL_MACHINE\SOFTWARE\Numecent\StreamingCore\Settings\Launcher`
- **名前:** `BaseTokenPathOrURL`
- **データ:** 値は、インストール時に指定したURLと一致する必要があります。

パッケージ化されたアプリケーションを配信する

前提条件のインストールが完了したら、パッケージ化されたアプリケーションをユーザーに配信するには、次の操作を行います。

1. アプリケーションパッケージをネットワーク共有に保存する。
2. アプリケーションパッケージを環境にアップロードする。
3. アプリケーションをデリバリーグループに追加する。
4. 相互依存するApp-Vパッケージの自動配信を有効にするには、分離グループを作成します。

アプリケーションパッケージをネットワーク共有に保存する

インフラストラクチャをセットアップしたら、アプリケーションパッケージを生成し、UNCまたはSMBネットワーク共有、あるいはAzureファイル共有などのネットワークロケーションに保存します。

詳細な手順は次のとおりです。

1. アプリケーションパッケージを生成します。詳細については、Microsoftのドキュメント「App-V仮想化アプリケーションの作成と管理」を参照してください。
2. アプリケーションパッケージをネットワークロケーションに保存します。

- **App-V Single Admin**の場合：パッケージと対応する動的構成ファイル（App-V）をUNCまたはSMBネットワーク共有、あるいはAzureファイル共有に保存します。
- **App-V Dual Admin**の場合：UNCパスからApp-V管理サーバーにパッケージを公開します。（HTTP URLからの公開はサポートされていません。）
- **MSIXまたはMSIX app attach**の場合：パッケージをUNCまたはSMBネットワーク共有、あるいはAzureファイル共有に保存します。
- **FlexApp**の場合：パッケージをUNCまたはSMBネットワーク共有、あるいはAzureファイル共有に保存します。
- **Elastic App**の場合：パッケージをUNCまたはSMBネットワーク共有、あるいはAzureファイル共有に保存します。
- **Cloudpaging**の場合: パッケージをUNCまたはSMBネットワーク共有、あるいはAzureファイル共有に保存します。

3. VDAがパッケージストレージパスに対する読み取り権限を持っていることを確認してください。

   - ADドメイン内のUNCまたはSMBネットワーク共有にパッケージを保存する場合、VDAマシンにストレージパスへの読み取り権限を付与します。そのためには、マシンのADアカウントに共有への読み取り権限を明示的に付与するか、その権限を持つADグループにアカウントを含めることができます。
   - Azureファイル共有にパッケージを保存する場合は、まずAzureのストレージパスにユーザーアカウントの読み取り権限を付与します。次に、VDAマシンで実行されている `ctxAppVService` を、そのユーザーアカウントを使用してパッケージストレージパスにアクセスするように構成します。詳細な手順については、ユーザーログオンアカウントの変更を参照してください。

ユーザーログオンアカウントの変更

以下の2つのシナリオでユーザーログオンアカウントを変更します。

- リンクされたADアカウントを使用してAzureファイル共有上のパッケージにアクセスするには：
  - 接続エンティティは、マシンアカウントではなくユーザーアカウントである必要があります。これは、Microsoft Entra IDがファイル共有上のマシンアカウントに読み取り権限を付与しないためです。
- MSIXおよびMSIX AppAttachパッケージにサービスが含まれている場合：

- パッケージは、非管理者ユーザーに公開する前に、ローカルマシンで管理者権限を持つユーザーアカウントを使用して公開する必要があります。これは、パッケージ化されたサービスをインストールするために必要であり、パッケージはマシンではなくユーザーにのみ公開できるため、デフォルトのLocalServiceアカウントは不適切です。

VDAは`ctxAppVService`を呼び出して、パッケージストレージパスにアクセスし、管理者権限を必要とする操作を実行します。デフォルトでは、`ctxAppVService`はマシンのLocalServiceアカウントのコンテキストで実行され、マシンのIDを使用してADに認証するため、上記のシナリオには適していません。

いずれの場合も、サービスは、ローカルで管理者権限を持ち、パッケージの保存場所（SMB共有またはAzureファイル共有）への読み取りアクセス権が付与されているADユーザーアカウントを使用するように再構成する必要があります。手順は次のとおりです。

1. **サービス**を開始し、**ctxAppVService**を右クリックし、**プロパティ**を選択します。
2. **ログオン**タブで、**このアカウント**を選択します。
   a. ローカル管理者権限とパッケージストレージパスへの読み取り権限を持つユーザーアカウントを入力します
   b. ユーザーのパスワードを2回入力します。
3. **OK**をクリックします。

アプリケーションパッケージを環境にアップロードする

必要に応じてアプリケーションパッケージをネットワークの場所に保存した後、配信のために環境にアップロードします。必要に応じて、以下のいずれかの方法を使用します。

- 一括アップロード
- 1つずつアップロード

準備

Citrix Virtual Apps and Desktops は、パッケージ検出のためのネットワークロケーションへの接続を設定するために VDA マシンを使用します。したがって、事前にデリバリーグループを作成し、グループ内の少なくとも1つの VDA が次の要件を満たしていることを確認してください。

- VDAバージョン:
  - App-Vパッケージを検出する場合: 2203以降
  - MSIXおよびMSIXアプリ添付パッケージを検出する場合: 2209以降
  - FlexAppパッケージを検出する場合: 2311以降およびFlexApp Agentソフトウェア

    - ElasticAppパッケージを検出するには：2511以降、およびApp Layeringが有効なイメージ
    - CloudpagerコンソールからCloudpagingパッケージを検出する場合: 2511以降
    - ネットワーク共有からCloudpagingパッケージを検出する場合: 2603以降

- アプリケーションパッケージ配信コンポーネント: インストール済み
- パッケージの場所に対するアクセス許可: 読み取り (詳細については、ネットワーク共有にアプリケーションパッケージを保存するを参照してください。)
- 電源: オン
- 状態: 登録済み

アプリケーションパッケージを一括でアップロードする
ネットワーク上の場所にあるパッケージを環境にアップロードします。アップロードする前に、次の項目が準備されていることを確認してください。

- 準備の要件を満たすデリバリーグループ
- ネットワークの場所のパス

パッケージを一括でアップロードするには、次の手順に従います。

1. 左側のペインで、**App packages**を選択します。
2. 「**パッケージ検出**」タブで、「**検出プロファイルの作成**」ボタンをクリックします。「**検出プロファイルの作成**」ページが表示されます。
3. **名前**フィールドに、プロファイルの説明的な名前を入力します。
4. **デリバリーグループ**フィールドで、**デリバリーグループの選択**をクリックします。次に、準備に記載されている要件を満たすデリバリーグループを選択し、**OK**をクリックします。
5. **場所の種類**フィールドで、パッケージの保存場所に応じて**Microsoft App-Vサーバー**、**ネットワーク共有**、または**Numecent Cloudpager**を選択し、対応する設定を完了します。

    - **Microsoft App-Vサーバー**を選択した場合は、次の情報を入力します。
        - 管理サーバーのURL。例: `http://appv-server.example.com`
        - 管理サーバー管理者のログイン資格情報。
        - 公開サーバーのURLとポート番号。例: `http://appv-server.example.com:3330`
    - **ネットワーク共有**を選択した場合は、次の情報を指定します。

- ネットワーク共有のUNCパスを入力します (例: `\\Package-Server\apps\`)。*Elastic App*パッケージの場合は、ELMの**System's Network File Share SMB path**からUNCパスを入力します。
- アップロードするパッケージの種類を選択します。オプションには、**App-V**、**MSIX**、**MSIX app attach**、**FlexApp**、**Elastic App**、**Cloudpaging**が含まれます。
- パッケージのサブフォルダーを検索するかどうかを指定します。

> **注:**
>
> `cim`イメージを含むフォルダー構造でMSIX app attachパッケージを検索する場合は、**サブフォルダーを検索**を選択していることを確認してください。そうしないと、ディスクが正しく検出されません。

- **Numecent Cloudpager** を選択した場合（Cloudpaging アプリが Cloud Pager Console に保存されていることを意味します）、次の情報を入力します。
  - Cloudpager コンソールの URL。例: `https://cloudpagerconsole.my.org`
  - PowerShell APIキー。
  - AppLauncher MSID。

6. **検出プロファイルの作成**をクリックします。

「**検出プロファイルの作成**」ページが閉じ、新しく追加されたプロファイルがプロファイルリストに表示されます。Citrix Virtual Apps and Desktops は、デリバリーグループ内の VDA を使用してパッケージを環境にアップロードします。アップロードが完了すると、 フィールドに *インポート成功* と表示されます。対応するパッケージは「**パッケージ**」タブに表示されます。

> **注:**
>
> ソースの場所でパッケージの更新を確認し、環境にインポートするには、プロファイルリストで場所を選択し、**更新の確認** をクリックします。

アプリケーションパッケージを1つずつアップロードする
ネットワーク共有から環境にアプリケーションパッケージをアップロードします。アップロードする前に、次の項目が準備されていることを確認してください。

- 準備に記載されている要件を満たすデリバリーグループ
- ネットワークの場所のパス。

パッケージを環境にアップロードするには、次の手順に従います。

1. 左側のペインで、**アプリパッケージ**を選択します。
2. **パッケージ**タブで、**パッケージの追加**ボタンをクリックします。**パッケージの追加**ページが表示されます。
3. 「**デリバリーグループ**」フィールドで、「**デリバリーグループの選択**」をクリックします。次に、準備に記載されている要件を満たすデリバリーグループを選択し、「**OK**」をクリックします。
4. 「**パッケージのフルパス**」フィールドに、必要に応じてパスを入力します。
   - 複数のパッケージを一度にアップロードするには、セミコロン (`;`) で区切って、それらのフルパスを入力します。例: `\\Package-Server\apps\office365.appv;\\Package-Server\apps\skype.msix;\\Package-Server\apps\slack.vhd`
   - ネットワーク共有にあるすべてのパッケージをアップロードするには、ストレージパスを入力します。例: `\\package-Server\apps\`
5. 「**パッケージの追加**」をクリックします。

   アプリケーションパッケージが「**パッケージ**」タブに表示されます。

アプリケーションをデリバリーグループに追加する

アプリケーションパッケージが環境に完全にアップロードされたら、必要に応じて、そのアプリケーションを1つ以上のデリバリーグループに追加します。その結果、それらのデリバリーグループに関連付けられたユーザーはアプリケーションにアクセスできるようになります。

> **注:**
>
> - デリバリーグループを介して、パッケージ化されたアプリケーションをシングルセッションVDAおよびマルチセッションVDAに配信できます。
> - デフォルトでは、エンドユーザーは、*シングルセッション* (または*デスクトップ*と呼ばれる) VDAに関連付けられたデリバリーグループに割り当てられているすべてのパッケージ化されたアプリケーションにアクセスできます。*デスクトップ*VDA上のパッケージ化されたアプリケーションの可視性を特定のユーザーまたはグループに制限するには、「**アプリケーション**」ノードに移動し、アプリケーションを選択して、「**アプリケーショ**

> **ンプロパティの編集 > 可視性の制限**」を選択して変更を加えます。アプリケーションの可視性を制限するを参照してください。

パッケージ内の1つ以上のアプリケーションを複数のデリバリーグループに追加するには、次の手順に従います。

1. 左ペインで、**App Packages**を選択します。
2. **Packages**タブで、必要に応じてパッケージを選択します。
3. アクションバーで、**Add Delivery Groups**をクリックします。**Assign Applications to Delivery Groups**ページが表示されます。
4. 必要に応じてパッケージ内のアプリケーションを1つ以上選択し、「**次へ**」をクリックします。
5. デリバリーグループのリストで、アプリケーションを割り当てるグループを選択し、**Next**をクリックします。

> **注:**
>
> - MSIXまたはMSIXアプリ添付パッケージを選択した場合、VDAバージョンが2106以降のデリバリーグループのみがリストに表示されます。
> - *FlexApp*パッケージを選択した場合、VDAバージョンが2402以降のデリバリーグループのみがリストに表示されます。
> - *Elastic App* パッケージを選択した場合、VDA バージョンが 2511 以降のデリバリーグループのみがリストに表示されます。
> - *Cloudpaging*パッケージを選択した場合、VDAバージョンが2511以降のデリバリーグループのみがリストに表示されます。

6. **完了**をクリックします。

さまざまなパッケージのアプリケーションを複数のデリバリーグループに追加するには、次の手順に従います。

1. 左ペインで、**App Packages**を選択します。
2. **Applications**タブで、**Add Applications**を選択します。
3. **Groups**ページで、必要に応じて1つ以上のデリバリーグループを選択します。

4. **Applications**ページで、次のように1つ以上のアプリケーションパッケージを選択します。
    a. **Add**をクリックし、**Application packages**を選択します。
    b. 必要なパッケージプロファイルの種類を選択します（例: App-V Single Admin）。この種類のすべてのパッケージが表示されます。
    c. 必要に応じて1つ以上のパッケージを選択します。
    d. **OK**をクリックし、次に**Next**をクリックします。
    e. 異なるパッケージタイプのアプリケーションをさらに追加するには、手順aからdを繰り返します。
5. **完了**をクリックします。

次の場合に、パッケージ化されたアプリケーションをデリバリーグループに追加することもできます。

- デリバリーグループを作成する場合。詳細については、「デリバリーグループの作成」を参照してください。
- 既存のデリバリーグループまたはアプリケーショングループを編集する場合。詳細については、「アプリケーションの追加」を参照してください。

（オプション）APP-Vパッケージの分離グループを作成する

相互依存するApp-Vパッケージを自動的に配信できるように、分離グループを作成できます。

> **注:**
>
> 分離グループは、App-Vシングル管理者方式でサポートされています。App-Vデュアル管理者方式を使用している場合は、Microsoft App-Vインフラストラクチャで*接続グループ*を作成することで同じ目標を達成できます。詳細については、Microsoftのドキュメント記事「接続グループファイルについて」を参照してください。

分離グループについて
分離グループとは、仮想環境を作成するために同じWindows Sandboxで実行する必要がある、相互依存するアプリケーションパッケージの集合です。Citrix App-V分離グループは、App-V接続グループに似ていますが、同一ではありません。分離グループには、次の2種類のパッケージが含まれます。

- **明示的なアプリケーションパッケージ**：特定のライセンス要件を持つアプリケーション。これらのアプリケーションをデリバリーグループに追加することで、特定のユーザー範囲に制限できます。
- **自動アプリケーションパッケージ**：デリバリーグループに追加されているかどうかに関係なく、常にすべてのユーザーが利用できるアプリケーション。

たとえば、アプリケーション`app-a`を実行するにはJRE 1.7が必要です。app-a（*明示的*としてマーク）とJRE 1.7（*自動*としてマーク）を含む分離グループを作成できます。次に、`app-a`のApp-Vパッケージを1つ以上のデリバリーグループに追加します。ユーザーがapp-aを起動すると、JRE 1.7が自動的に展開されます。

ユーザーが分離グループ内で *Explicit* とマークされたApp-Vアプリケーションを起動すると、Citrix Virtual Apps and Desktopsはデリバリーグループ内のアプリケーションに対するユーザーのアクセス権限を確認します。ユーザーがアプリケーションにアクセスする権限を持っている場合、同じ分離グループ内の *Automatic* アプリケーションパッケージはユーザーに利用可能になります。

*自動*パッケージをデリバリーグループに追加する必要はありません。分離グループに別の*明示的*アプリケーションパッケージがある場合、そのパッケージは同じデリバリーグループにある場合にのみユーザーが利用できます。
App-V分離グループを作成する
分離グループを作成し、相互依存するアプリケーションパッケージを追加します。詳細な手順は次のとおりです。

1. **「分離グループ」**タブで、「分離グループの追加」**をクリックします。
2. 分離グループの名前と説明を入力します。環境内のすべてのApp-Vシングル管理者パッケージが**「利用可能なパッケージ」**リストに表示されます。
3. **「利用可能なパッケージ」**リストから、必要に応じてアプリケーションを選択し、右矢印をクリックします。選択したアプリケーションが「分離グループ内のパッケージ」**リストに表示されます。
4. 「**展開**」フィールドで、アプリケーションに対して「**明示的**」または「**自動**」を選択します。
5. さらにパッケージを追加するには、手順2〜3を繰り返します。
6. リスト内のパッケージの順序を調整するには、上矢印または下矢印をクリックします。
7. 「**保存**」をクリックします。

> **注:**

> 隔離グループ構成により、VDA上にApp-V接続グループが作成されます。展開シナリオは複雑になる可能性があり、App-Vクライアントは一度に1つのアクティブな接続グループにのみ存在するパッケージをサポートします。同じパッケージを、同じデリバリーグループに追加された2つの異なる隔離グループに追加することは避けることをお勧めします。

ベストプラクティス

- App-Vパッケージを展開するには、PowerShellコマンド`Enable-AppV`を使用してVDAでApp-Vサブシステムを有効にします。
- MSIX（およびAppAttach）パッケージを展開するには、VDAがパッケージの署名に使用されている証明書を信頼する必要があります。
- Windows Server 2019では、MSIXパッケージを展開するためにサイドローディングを有効にします。Windows 10、11、Windows Server 2022、および2025ではサイドローディングは不要です。
- App AttachはWindows Server 2019では全く実装されておらず、Windows Server 2022または2025ではMicrosoft（およびCitrixも同様に）によって現在サポートされていません。

詳細設定

以下の高度なトピックでは、基本的なアプリパッケージのワークフローを超えて、Citrix Virtual Apps and Desktops でパッケージ化されたアプリケーションがどのように検出、更新、配信されるかを微調整するための追加の構成オプションと制御について説明します。

パッケージ化されたアプリケーションの公開を自動化する

PowerShellコマンドを使用して、パッケージ化されたアプリケーションの公開を自動化できます。

Delivery Controller™上で、以下のPowerShellコマンドを実行します:

1. パッケージ検出モジュールに存在するコマンドをロードするには:

```
Import-Module "D:
\Support\Tools\Scripts\Citrix.Cloud.AppLibrary.Admin.v1.psm1"
```

> **注:**
>
> パッケージ検出モジュールのバージョンは、Citrix Virtual Apps and Desktops ISOの、手順1で述べたパスにあります。

2. パッケージ検出モジュールは、公開するパッケージタイプもサポートするCitrix Virtual Apps and DesktopsバージョンのISOから取得する必要があります。つまり、FlexAppOneアプリケーションには2311以降が必要です。利用可能な最新バージョンを使用することをお勧めします。
3. 関連するデリバリーグループIDとパッケージ化されたアプリケーションIDを取得するには:

```
Get-BrokerDesktopGroup | Format-Table Uid, Name

Get-AppLibAppVApplication | Format-Table Uid, Name
```

4. パッケージを公開し、適切なBrokerMachineConfigurationを作成するには:

```
Publish-PackagedApplication -AppLibararyApplicationUid
<AppLibararyApplication.Uid > -DesktopGroupUid <DesktopGroup.Uid>
```

5. Broker構成を同期するには、これは後でVDA上のBrokerエージェントに送信されます:

```
Update-DesktopGroupMachineConfigurations -DesktopGroupUid
<DesktopGroup.Uid>
```

> **注:**
>
> PowerShellコマンドラインを介してデリバリーグループからパッケージ化されたアプリケーションを公開または削除した後には、PowerShellコマンド `Update-DesktopGroupMachineConfigurations` を必ず実行してください。そうしないと、公開されたアプリケーションに関する情報がVDAに正しく送信されず、起動に失敗します。

アプリケーションの可視性を制限する

Citrix Virtual Apps and Desktops環境では、パッケージからのアプリケーションがデスクトップに公開されると、システムはそれらのアプリケーションに対するActive Directory (AD) のユーザーおよびグループの可視性設定を尊重します。ただし、ユーザーがパッケージ内の1つのアプリケーションに対してのみ可視性を持っている場合でも、個々のパッケージコンポーネントはVDA上で細分化できないため、パッケージ全体を仮想デスクトップ（またはシームレスアプリ）セッションに展開する必要があります。さらに、VDAバージョン2503より前では、最初の公開後にアプリケーションの可視性を低下させる変更を行っても、その後のデスクトップ起動時に以前に公開さ

れたパッケージがクリーンアップされることはありません。また、デスクトップとワークスペースの可視性など、他の可視性レイヤーは、これらのAD可視性割り当ての上に動作します。

パッケージ化されたアプリケーションがWorkspaceに表示されるべきか、ユーザーのVDIデスクトップセッションに展開されるべきかを制御できます。パッケージ化されたアプリケーションが公開されたら、PowerShellコマンド `Set-BrokerApplication -Name "MyApp" -PackagedApplicationVisibility "Workspace|Desktop|WorkspaceAndDesktop"` を使用して、`BrokerApplictaion` の `PackagedApplicationVisibility` プロパティを更新できます。

`PackagedApplicationVisibility` のデフォルト値は `WorkspaceAndDesktop` です。

値 `Workspace`: アプリはWorkspaceAppにのみ表示され、シームレスなAppLaunchに利用できますが、ユーザーが開始するデスクトップセッションには自動的に公開されません。

値 `Desktop`: アプリのアイコンをWorkspaceAppから非表示にし、シームレスなAppLaunchでは利用できなくなりますが、ユーザーがADグループ設定を通じてアクセスできる場合、アプリは引き続きユーザーのデスクトップセッションに展開できます。

> **注:**
>
> シングルセッション静的デスクトップに公開されたパッケージアプリケーションは、この設定で構成された値に関係なく、Workspace Appでは利用できません。

App-Vフルインフラストラクチャからシングル管理者ワークフローへの移行

Microsoft App-Vフルインフラストラクチャ（デュアル管理者）は、サポート終了が近づいています。App-Vパッケージやその他のサポートされているコンテナ形式の提供を継続するには、Citrixシングル管理者モデルに移行してください。

シングル管理者モデルは、App-V管理サーバーと公開サーバーへの依存関係を排除し、Studioでパッケージ管理を一元化します。

シングル管理者モデルの利点

シングル管理者ワークフローに移行することで、アーキテクチャが簡素化され、パッケージ管理が効率化されます。

簡素化されたアーキテクチャ

シングル管理者モデルでは、VDAはファイル共有から直接パッケージを取得します。Citrixはメタデータ、公開、および分離ロジックを管理します。

機能	フルインフラストラクチャ（デュアル管理者）	シングル管理者（CITRIX管理）
管理	App-V管理コンソール	シトリックス スタジオ または ウェブ スタジオ
データベース	必須 (SQL Server)	なし (メタデータはCitrixサイトデータベースに保存されます)
公開	App-V パブリッシングサーバー	シトリックス VDA (`ctxAppVService`)
パッケージソース	UNC共有 (管理サーバーに同期)	UNC共有、SMB共有、またはAzure Files
ロジック	接続グループ	Citrix分離グループ

戦略的利点

Single Adminに移行することで、**同期ラグ**も解消されます。

- Dual Admin モデルでは、App-V 管理サーバーを同期し、その後 Studio を同期する必要があります。
- Single Admin モデルでは、ファイル共有上のパッケージを更新し、Studio で を選択すると、更新されたパッケージは次回のユーザーログオン時に利用可能になります。

移行ワークフロー

既存の App-V フルインフラストラクチャを Citrix Single Admin ワークフローに移行するには、次の手順に従います。

1. ステップ 1: ターゲット環境を準備する
2. ステップ 2: パッケージを Citrix ライブラリにインポートする

ステップ 1: ターゲット環境を準備する

パッケージをインポートする前に、インフラストラクチャと VDA が Single Admin モデルをサポートする準備ができていることを確認してください。

1. **共有リポジトリ**
    a. `.appv` パッケージをホストする UNC 共有を特定します。

b. VDA マシンアカウント（例: ドメインコンピューター）が、共有と NTFS の両方のアクセス許可に対して **読み取り** アクセス権を持っていることを確認してください。

2. **VDA**

   すべての VDA に **App Packages Delivery Component** がインストールされていることを確認してください。インストール後にこのコンポーネントを追加するには：

   a. VDA インストーラーを実行します。

   b. で を選択します。

   c. 「**App Packages Delivery Component**」を追加します。

3. 「**XML構成ファイル**」

   `_DeploymentConfig.xml`と`_UserConfig.xml`ファイルを、対応する`.appv`ファイルと*同じ*フォルダーに移動します。

   Single Adminモデルでは、VDAは中央のApp-Vデータベースからではなく、ファイル共有上のパッケージフォルダーから構成ファイルを読み取ります。

ステップ2：パッケージをCITRIXライブラリにインポートする

環境を準備したら、既存のApp-VパッケージをCitrixアプリケーションライブラリにインポートします。

1. Citrix Studioで、**構成** > **App Packages**に移動します。
2. 完全に移行する場合は、App-V Management Serverへの既存の接続をすべて削除します。
3. 「**Add Package**」を選択し、パッケージのUNCパスを指定します。
4. Citrixはフォルダーをスキャンし、パッケージ名、バージョン、およびアプリケーションIDをCitrixアプリケーションライブラリにインポートします。

インポート後、必要に応じてアプリケーションをデリバリーグループに割り当てることができます。

> **注:**
>
> 「**vPreferポリシー（オプション）**：アプリケーションをリモートサーバーにリダイレクトする代わりにローカルVDAで起動する場合は、VDAで**vPrefer** GPOを有効にします。

App-Vアプリケーションのトラブルシューティング（Single Adminモデル）

App-Vパッケージ（Single Adminモデル）が起動しない、またはユーザーセッションに表示されない場合は、以下のガイダンスを使用して一般的な問題を特定し、解決してください。

問題	説明	解決策	
パッケージの検出と「カタログ化に失敗しました」エラー	Studio でパッケージを追加すると、ファイルにアクセスできないか、メタデータが無効であることを示すエラーが表示されます。	1. 権限を確認します。Delivery Controller マシンアカウント（例: `DOMAIN\DDC01$`）が、パッケージをホストする UNC パスの共有レベルと NTFS レベルの両方で**読み取り**権限を持っていることを確認します。 2. XML の整合性を確認します。`.appv` ファイルと `_DeploymentConfig.xml` ファイルのファイル名プレフィックスが同じで、同じフォルダーにあることを確認します。	

問題	説明	解決策
アプリケーションが起動しない (エラーコード: 0x80070005 または 0x80040154)	ユーザーがアプリケーションアイコンをクリックすると、**Citrix splash** 画面が表示されますが、アプリケーションは開きません。	1. VDAコンポーネントを確認します。 VDAに**App Packages Delivery Component**がインストールされていることを確認します。次のファイルが存在することを確認します: `C:\Program Files\Citrix\AppV\ctxAppVService.exe`。 2. VDAの権限を確認します。 VDAはファイル共有からパッケージをプルするため、VDAマシンアカウント（例: `DOMAIN\VDA-HR01$`）はUNCパスへの**読み取り**アクセス権を持っている必要があります。

問題	説明	解決策	
		3. App-Vクライアント構成を検証します。 • VDA で次の PowerShell コマンドを実行します: `Get-AppvClientConfiguration`. • パッケージにスクリプトが必要な場合は、`EnablePackageScripts` が `$True` に設定されていることを確認してください。	
分離グループの競合	Excel アドインなどのプラグインは、その親アプリケーションを認識できません。	1. Studio で、**App Packages** > **Isolation Groups** に移動します。 2. 両方のパッケージが同じ分離グループに追加されていることを確認します。シングル管理者モデルでは、VDA 上の App-V クライアント	

問題	説明	解決策	
		が、Delivery Controller によって配信された構成に基づいて、それらのアプリケーションの仮想接続を管理します。	
初回起動が遅い（バッファリング）	AutoCADやArcGISのような大規模なApp-Vパッケージの初回起動には数分かかります。	1. VDAで、以下のレジストリを確認します。`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\AppV\Client\Streaming` 2. 以降の起動パフォーマンスを向上させるため、`Autoload`を`2`（以前使用したすべてのパッケージを自動ロード）に設定します。 3. ネットワークパフォーマンスを確認します。ネットワーク共有でのSMB署名またはウイルス対策スキャンが	

問題	説明	解決策	
		転送速度を制限していないことを確認してください。	

便利なPowerShellコマンド（VDAで実行）

Citrixがパッケージを VDAに正常に配信したかどうかを確認するには、PowerShellウィンドウで次のコマンドを実行します。

コマンド	目的
`Get-AppvClientPackage`	VDAに現在キャッシュされているか、公開されているすべてのApp-Vパッケージを表示します。
`Get-CtxAppvPackage`	Citrixエージェントによって管理されているパッケージを表示します。
`Start-Service ctxAppVService`	Citrix App-Vオーケストレーションサービスを再起動します。

ユニバーサル Windows プラットフォームアプリ

ユニバーサル Windows プラットフォーム (UWP) アプリについては、以下の Microsoft ドキュメントを参照してください。

- ユニバーサル Windows プラットフォーム (UWP) アプリとは
- Windows パッケージマネージャー

要件と制限

Citrix Virtual Apps and Desktops™ は、以下の Windows マシン上の VDA で UWP アプリを使用することをサポートしています。

- Windows 10 以降のバージョン
- Windows Server 2016 以降のバージョン

VDA はバージョン 7.11 以降である必要があります。

UWPアプリを使用する場合、以下のCitrix Virtual Apps and Desktops™機能はサポートされていないか、制限があります。

- ファイルタイプの関連付けはサポートされていません。
- ローカルアプリアクセスはサポートされていません。
- 動的プレビュー：セッションで実行中のアプリが重なっている場合、プレビューにはデフォルトのアイコンが表示されます。動的プレビューに使用される Win32 API は、UWP アプリではサポートされていません。
- アクションセンターのリモート処理：UWP アプリは、セッション内のメッセージを表示するためにアクションセンターを使用できます。これらのメッセージは現在、ユーザーに表示するためにエンドポイントにリダイレクトされません。

同じサーバーから UWP アプリと非 UWP アプリを起動することはサポートされていません。代わりに、UWP アプリと非 UWP アプリを別々のデリバリーグループまたはアプリケーショングループに配置してください。

マシンにインストールされているすべてのUWPアプリが列挙されるため、Citrix®はWindowsストアへのユーザーアクセスを無効にすることを推奨します。これにより、あるユーザーがインストールしたUWPアプリが別のユーザーによってアクセスされるのを防ぎます。

サイドローディング中、UWPアプリはマシンにインストールされ、他のユーザーが使用できるようになります。別のユーザーがアプリを起動すると、アプリがインストールされ、OSはそのAppXデータベースを更新して、そのユーザーによって「インストール済み」であることを示します。

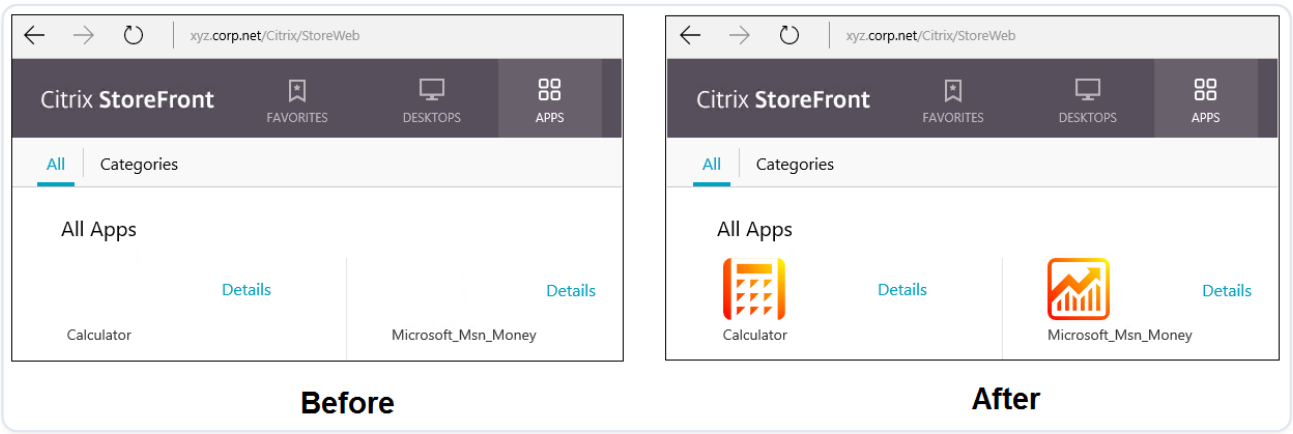
固定ウィンドウまたはシームレスウィンドウで起動された公開UWPアプリから開始された正常なログオフにより、VDAセッションが閉じなくなり、ユーザーが強制的にログオフされる可能性があります。この場合、VDAセッションに残っているいくつかのプロセスが、セッションが適切に閉じられるのを妨げます。これを解決するには、VDAセッションが閉じない原因となっているプロセスを特定し、CTX891671のガイダンスに従って、「LogoffCheckSysModules」レジストリキー値に追加します。

UWPアプリのアプリケーション表示名と説明が正しくない場合があります。アプリケーションをデリバリーグループに追加する際に、これらのプロパティを編集して修正してください。

その他の問題については、既知の問題を確認してください。

現在、いくつかのUWPアプリは透明度が有効な白いアイコンを使用しており、StoreFront表示の白い背景に対してアイコンが見えなくなることがあります。この問題を回避するには、背景を変更できます。たとえば、StoreFrontマシンでファイル`C:\inetpub\wwwroot\Citrix\StoreWeb\custom\style.css`を編集します。ファイルの最後

に`.storeapp-icon {background-image: radial-gradient( circle at top right, yellow, red ); }`を追加します。次の図は、この例の変更前と変更後を示しています。



Windows Server 2016以降のバージョンでは、UWPアプリの起動時にサーバーマネージャーも起動する場合があります。これを防ぐには、`HKLM\Software\Microsoft\ServerManager\DoNotOpenServerManagerAtLogon`レジストリキーを使用して、ログオン時にサーバーマネージャーが自動起動しないように無効にできます。詳細については、`<https://blogs.technet.microsoft.com/rmilne/2014/05/30/how-to-hide-server-manager-at-logon/>`を参照してください。

UWPアプリのインストールと公開

UWPアプリのサポートはデフォルトで有効になっています。

VDA（またはマスターイメージ）に1つ以上のUWPアプリをインストールするには、次のいずれかの方法を使用します。

- Windows Store for Businessからオフラインインストールを完了し、Deployment Image Servicing and Management (DISM) などのツールを使用してアプリをデスクトップイメージに展開します。詳細については、Windows Package Managerを参照してください。
- アプリをサイドロードします。詳細については、Windows クライアントデバイスで基幹業務 (LOB) アプリをサイドロードするを参照してください。
- 各対象ユーザー向けに、Windows Store for Businessから直接UWPアプリをインストールします。

Citrix Virtual AppsまたはCitrix Virtual Desktops™で1つ以上のUWPアプリを追加（公開）するには：

1. マシンにUWPアプリがインストールされたら、UWPアプリをデリバリーグループまたはアプリケーショングループに追加します。これは、グループの作成時または後で行うことができます。**アプリケーション**ページで、**追加**メニューから**スタートメニューから**を選択します。

2. アプリケーションリストが表示されたら、公開するUWPアプリを選択します。
3. ウィザードを続行するか、編集ダイアログを閉じます。

VDAでユニバーサルアプリの使用を無効にするには、`HKLM\Software\Citrix\VirtualDesktopAgent\FeatureToggle`にレジストリ設定**EnableUWASeamlessSupport**を追加し、**0**に設定します。

UWPアプリのアンインストール

`Remove-AppXPackage`のようなコマンドでUWPアプリをアンインストールすると、その項目は管理者に対してのみアンインストールされます。アプリを起動して使用した可能性のあるユーザーのマシンからアプリを削除するには、各マシンで削除コマンドを実行します。1つのコマンドですべてのユーザーのマシンからAppXパッケージをアンインストールすることはできません。

構成のバックアップまたは移行

この機能は、構成のバックアップを取るのに役立ちます。バックアップは、復元機能と合わせて、オンプレミスからクラウドへ、またはあるクラウドサイトから別のクラウドサイトへのサイト情報の移行を容易にします。また、緊急時にはサイトの即時復旧も容易にします。

バックアップを取るには、以下の方法を使用できます。

1. バックアップ + 復元
    a. Web Studioと統合されています。
2. 自動構成ツール (ACT)
    a. PowerShellベースのツールです。使用するにはツールをインストールしてください。「自動構成のダウンロード」を参照してください。

バックアップは以下の目的で使用できます。

1. 復元
2. 移行

Citrix®は、説明されているシナリオに対して以下のツールを推奨します。

バックアップ

環境	ユースケース	推奨ツール	特別な考慮事項	リンク
DaaS とオンプレミス	オンデマンドおよびスケジュールされたバックアップ	バックアップ + 復元	Citrix がバックアップを保持し、必要に応じてユーザーがダウンロードできます	Web Studioを使用したバックアップと復元
DaaS とオンプレミス	オンデマンドおよびスケジュールされたバックアップ	ACT	ユーザーがバックアップを保持します	Automated Configuration Tool を使用したバックアップと復元

移行

環境	ユースケース	推奨ツール	特別な考慮事項	リンク
オンプレミスからクラウドへ	1つのオンプレミスサイトをDaaSに移行する	ACT		オンプレミスからクラウドへの移行
	複数のオンプレミスサイトを1つのDaaSサイトに統合する	ACT	サイトのマージ	複数のオンプレミスサイトを単一のクラウドサイトにマージする
オンプレミスからオンプレミスへ	1つのオンプレミスサイトを別のオンプレミスサイトに移行する	ACT		POCガイド:自動構成ツール - オンプレミスからオンプレミスへの移行
	複数のオンプレミスサイトを別のオンプレミスサイトに統合する	ACT	サイトのマージ	POCガイド:自動構成ツール オンプレミスからオンプレミスへの移行

環境	ユースケース	推奨ツール	特別な考慮事項	リンク
				複数のオンプレミスサイトを単一のクラウドサイトにマージする
クラウドからクラウドへ	1つのDaaSサイトを別のDaaSサイトに移行する	ACT		クラウドからクラウドへの移行 (/ja-jp/citrix-virtual-apps-desktops/current-release/manage-deployment/migrate-cloud-to-cloud.html)
複数のDaaSサイトを1つのDaaSサイトに統合する	サイトのマージ	ACT		クラウドからクラウドへの移行 (/ja-jp/citrix-virtual-apps-desktops/current-release/manage-deployment/migrate-cloud-to-cloud.html)
				複数のオンプレミスサイトを単一のクラウドサイトに移行する (/ja-jp/citrix-virtual-apps-desktops/current-release/manage-deployment/multi-site-merge.html)

構成のバックアップと復元

この機能により、管理者はクラウド構成のバックアップを作成できます。これにより、Citrix®構成のコピーが常に利用可能で、すぐに使用できる状態に保たれます。バックアップ機能と復元機能は、オンプレミスからクラウドへ、またはあるクラウドサイトから別のクラウドサイトへのサイト情報の移行を容易にします。誤って変更が発生した場合でも、バックアップを選択して復元を選択するだけで、数回のクリックで再び稼働できます。特定のコンポーネントをバックアップおよび復元することもできます。

この機能では、以下をバックアップおよび復元できます。

- タグ
- AdminRoles
- AdminScopes
- HostConnections

> **注:**
>
> ホスト接続をバックアップできるようになりました。シークレットは毎回入力する必要があります。インポートまたは更新されるホスト接続に対してのみシークレットを要求するために、インポート前チェックモードが実行されます。

- StoreFront™
- デリバリーグループ
- ApplicationGroups
- アプリケーション
- AppVIsolationGroups
- AppLibPackageDiscovery
- GroupPolicies
- UserZonePreference
- 手動でプロビジョニングされた、またはPVSでプロビジョニングされたマシンカタログ
- 管理フォルダー
  - アプリケーションフォルダー
  - デリバリーグループフォルダー

    - マシンカタログフォルダー
- サイト設定

> **重要:**
>
> - 異なるコンポーネントを復元するには、リストの順序に従ってください。たとえば、アプリケーション、デリバリーグループ、およびグループポリシーを復元する場合は、次の順序に従う必要があります。
>
>   - デリバリーグループ
>   - アプリケーション
>   - グループポリシー
>
> - MCS マシンカタログをバックアップまたは復元することはできません。

バックアップの種類

要件に応じてバックアップを実行するには、次のオプションを使用します。

- **オンデマンド**: サイト構成をリアルタイムでバックアップします。このアクションは、現在の Citrix Cloud™ サイト構成をバックアップします。
- **スケジュール済み**: スケジュールされた間隔でサイト構成をバックアップします。これは、指定された間隔で繰り返されます。

> **注:**
>
> フル権限を持つ管理者とクラウド管理者のみが、オンデマンドまたはスケジュールされたバックアップと復元を実行できます。

Web Studio を使用したバックアップと復元

この記事では、コンソールの左ペインにある **バックアップと復元** ノードで実行できるアクションについて説明します。

バックアップと復元 を使用すると、管理者は Web Studio からバックアップを取得できます。

ストレージの場所を設定する

バックアップを作成する前に、バックアップを保存するストレージの場所を設定する必要があります。

1. Web Studio から、**管理** をクリックします。
2. 左側のメニューから、**バックアップ+復元** を選択します。
3. **バックアップと復元** タブ内で、**ストレージの設定** をクリックします。

   バックアップのストレージの場所を設定する (/en-us/citrix-virtual-apps-desktops/current-release/media/first-time-backup-storage-1.png)
4. ドロップダウンリストから、**ストレージの種類** を選択します。ストレージの種類は、ファイルストレージまたはAzureストレージにすることができます。

   > **注:**
   >
   > - その場所は、すべてのDelivery Controllerからアクセスできる必要があります。
   > - フォルダーへのアクセスにユーザー名とパスワードが必要な場合は、企業のパスワードポリシーによってパスワードの有効期間が制限されないようにしてください。

5. 以下を選択します。
   - 最大バックアップ数
   - 最大ピン留めバックアップ数
   - 自動ピン留めバックアップの最大数
6. **保存**をクリックしてストレージの場所を保存するか、**保存してバックアップを作成**をクリックしてストレージの場所を保存し、バックアップを作成します。

ストレージの場所を設定したら、バックアップを作成できます。

オンデマンドバックアップの作成

1. Web Studioから、**管理**をクリックします。
2. 左側のメニューから、**バックアップと復元**を選択します。
3. ストレージの場所が設定されているがバックアップが存在しない場合、バックアップを作成するように求められます。

初期バックアップの作成(/en-us/citrix-virtual-apps-desktops/current-release/media/backup-after-storage-creation.png)

既存のバックアップがある場合は、**バックアップの作成**をクリックできます。

4. **バックアップの作成**ページで、メモを入力し、**バックアップの作成**をクリックします。

   バックアップをトリガーした管理者の名前でバックアップされるバックアップコンポーネントを示す概要アクティビティが表示されます。

5. バックアップが正常に完了すると、**バックアップと復元**タブの下に項目として表示されます。
6. 特定のバックアップを選択すると、**詳細**タブでそのバックアップに関する詳細情報が表示されます。
7. バックアップを削除するには、バックアップを右クリックし、**バックアップの削除**をクリックします。

バックアップをピン留めする

Citrix® は最新の30個のバックアップを保存します。30個を超えるバックアップを作成すると、システムは作成された順序で古いバックアップを削除します。30個のバックアップ制限に加えて新しいバックアップが作成されるたびに、システムは最初に作成されたバックアップを削除します。バックアップのピン留めは、特定のバックアップが自動的に削除されるのを防ぐために使用されます。最大5個のバックアップをピン留めできます。ピン留めされたバックアップがある場合、30個のバックアップに加えてすべてのピン留めされたバックアップを保持します。つまり、最大で35個のバックアップ（ピン留めされていない30個とピン留めされた5個）を保持できます。

1. バックアップをピン留めするには、右クリックします。

スケジュールされたバックアップを作成する

バックアップと復元プロセスを自動化するために、組織の要件に合わせたバックアップスケジュールを作成します。バックアップは、選択した頻度（毎日、毎週、毎月、またはその他の適切な頻度）でバックグラウンドで実行されます。

1. スケジュールタブに移動し、**スケジュールを作成**を選択します。
2. **スケジュールを作成**ページで、以下を入力します。

   - **このスケジュールを有効にする**: このバックアップスケジュールを有効にするには、**はい**を選択します。
   - **名前**: バックアップスケジュールの名前を入力します。
   - **説明**: 説明を入力します。

- **タイムゾーン**: 任意のタイムゾーンを選択します。
- **頻度**: バックアップを実行する頻度を選択します。
- **繰り返し間隔**: スケジュールを繰り返す日数（間隔）を入力します。
- **開始日**: 開始日を入力します。
- **バックアップ開始時刻**: バックアップを開始したい時刻を24時間形式で入力します。

3. **完了**を選択します。

スケジュールされたバックアップを制限する

同一のバックアップを避けるため、スケジュールされたバックアップを1日1回に制限できます。

1. **バックアップと復元**ノードの**設定**タブに移動します。
2. **スケジュールされたバックアップ**ボックスで**変更**をクリックします。
3. トグルを切り替えて、スケジュールされたバックアップを1日1回に制限する機能を有効にします。

スケジュールされたバックアップの自動ピン留め

スケジュールされたバックアップの自動ピン留めは、選択したスケジュールによって作成されたバックアップを自動的にピン留めします。自動ピン留めには、1つのスケジュールのみを選択できます。

スケジュールされたバックアップの自動ピン留めを使用すると、最大6つのスケジュールされたバックアップを保持できます。最大制限に達すると、最も古い自動ピン留めされたバックアップが削除されます。

> **注:**
>
> Citrixは最大6つの自動ピン留めされたバックアップを保存します。システムは、6番目のバックアップ以降に作成された古いバックアップを、作成された順序で削除します。6つのバックアップ制限に加えて新しく作成されるバックアップごとに、システムは最初に作成されたバックアップを削除します。

1. **バックアップと復元**ノードの**設定**タブに移動します。
2. 自動ピン留めするスケジュールされたバックアップを選択します。
3. トグルを切り替えて、自動ピン留めされたスケジュールを有効にします。

4. スケジュールを選択し、**保存**をクリックします。

バックアップストレージの編集

バックアップストレージ設定を編集して、ストレージの種類と場所、最大バックアップ数、最大ピン留めバックアップ数、および最大自動ピン留めバックアップ数を変更できます。

1. 「**バックアップと復元**」ノードの「**設定**」タブに移動します。
2. 「**ストレージ**」ボックスで「**変更**」をクリックします。
3. 「**バックアップストレージの編集**」ダイアログでストレージ設定を変更します。

復元

この機能により、管理者はバックアップからサイト構成を復元できます。一度に1つのコンポーネントのみを復元できます。

> **注:**
>
> - 一度に1つのコンポーネントのみを復元することで、コンポーネント間の依存関係による復元中の競合を防ぎます。
> - ホスト接続の復元ワークフローは、ホスト接続を復元しようとするたびにシークレットを入力する必要があるため、他のコンポーネントとは異なります。「**バックアップの復元**」をクリックすると、シークレットを入力するダイアログが表示されます。たとえば、Azureでは、接続の作成に使用した英数字のアプリケーションシークレットを入力します。

1. Web Studioから、「**管理**」をクリックします。
2. 左側のメニューから、「**バックアップと復元**」を選択します。
3. リストから特定のバックアップをクリックします。
4. 「**バックアップの復元**」をクリックします。
5. 「**バックアップの復元**」ウィンドウで、以下を入力します。
    - **コンポーネント**: 復元するコンポーネントを選択します。
    - **フィルター**: 復元するメンバー名をコンマ区切りのリストで指定します。たとえば、*chrome* という単語でフィルターすると、chrome という名前のオブジェクトのみが復元されます。同様に、`chr` というフレーズは、`chr` で始まるオブジェクトを復元します。

コンポーネントメンバーを表示するには、バックアップを選択し、「**詳細 > コンポーネント**」に移動します。コンポーネントを選択し、「**コンポーネントメンバーの表示**」をクリックします。

- **チェックモード**: 実際の復元操作が実行されたときに何を復元する必要があるかを確認するには、「**はい**」を選択します。このオプションは、実際の復元をトリガーすることなく、復元に必要なすべてを事前に評価します。たとえば、アプリケーションコンポーネントの復元プロセスが実行されたときに復元されるアプリケーションのリストが表示されます。

> **注:**
>
> チェックモードでは、実際の復元は実行されません。このオプションでは、コンポーネント間の依存関係もチェックされません。最適な結果を得るには、チェックモードを一度に1つのコンポーネントで使用することをお勧めします。

- **復元タイプ**: いずれかを選択します。
  - **不足しているもののみ**: この復元タイプを使用して、コンポーネントとメンバーをサイトに追加します。このオプションは、復元されるバックアップの構成が異なっていても、既存のコンポーネントとメンバーを変更しません。
  - **不足しているものと既存のものを更新**: この復元タイプを使用して、コンポーネントをサイトに追加および更新します。このオプションは、既存のコンポーネントとメンバーの構成が異なる場合、バックアップの構成で更新します。
- **メモ**: メモを入力します。

6. **復元**を選択します。

復元アクションが完了すると、復元結果が**復元**ウィンドウに表示されます。すべての復元アクションは、**履歴**タブに一覧表示されます。

履歴

履歴タブで、すべてのバックアップおよび復元アクションを追跡できます。

アクションの下に、削除されたすべてのバックアップとバックアップ履歴が表示されます。

バックアップの詳細を表示するには：

1. **履歴**タブに移動します。
2. バックアップアクションを選択し、**詳細の表示**をクリックします。

バックアップ結果には、次の詳細が表示されます。

- 期間
- 注
- 管理者名
- バックアップされたコンポーネント

「**履歴**」ページの右上にある検索バーを使用して、特定のバックアップを検索します。たとえば、特定の管理者によって実行されたバックアップや、特定の日に実行されたバックアップを検索できます。

自動構成ツールを使用したバックアップと復元

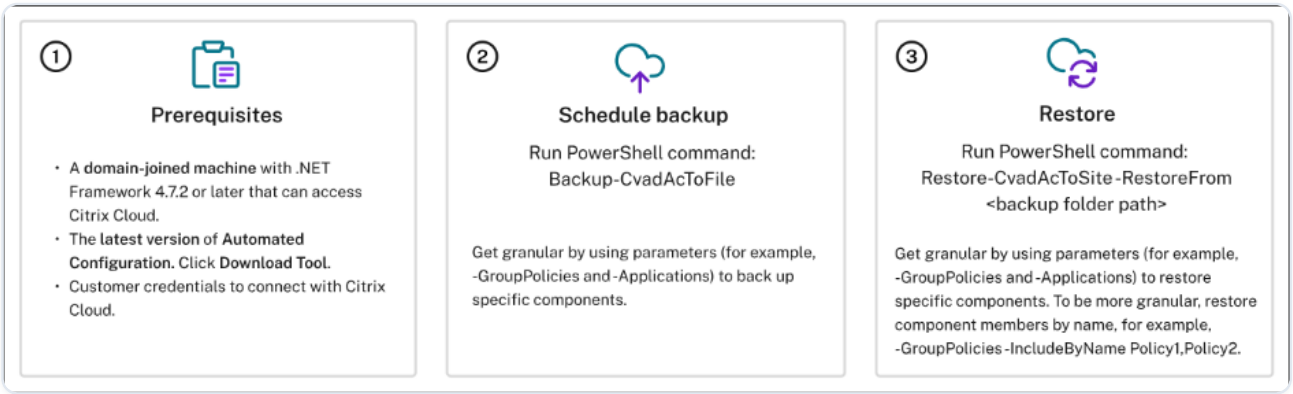
自動構成ツールを使用すると、以下の環境でオンデマンドおよびスケジュールされたバックアップを実行できます。

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

自動構成ツールは、以下の目的で使用できます。

- バックアップと復元（オンデマンドおよびスケジュールされたバックアップ）
- 移行（オンデマンドバックアップ）

移行のための自動構成ツール



シトリックス バーチャル アプリケーションズ アンド デスクトップス™

構成をバックアップするための前提条件

- Citrix Virtual Apps and Desktops のすべてのバージョン。
- Auto Config を実行するマシン。このデバイスは次のいずれかです。

- デリバリーコントローラー™
- ドメインに参加しているマシンで、.NET Framework 4.7.2 以降と Citrix PowerShell SDK がインストールされていること。Citrix PowerShell を使用するには、Web Studio をインストールする必要があります。

バックアップ

1. Automated Configuration をインストールします。詳細については、「Download Automated Configuration」を参照してください。
2. **Auto-Config** をダブルクリックします。
3. PowerShell ウィンドウで、コマンド `Backup-CvadAcToFile` を実行してすべてのコンポーネントをエクスポートします。オンプレミス構成をエクスポートしても、構成は変更されません。

コマンドを初めて実行すると、プロセスによって `.yml` 構成ファイルを含むフォルダーが次の場所に作成されます。 `%HOMEPATH%\Documents\Citrix\AutoConfig`。

このフォルダーには、最近エクスポートされたバックアップファイルが含まれており、以前の各バックアップはサブフォルダーに保存されます。

復元

1. **Auto-Config** をダブルクリックします。
2. 復元を実行するには、次のコマンドを実行します。

```
Restore-CvadAcToSite -Environment OnPrem -RestoreFolder <folder path of
the backup files>
```

3. コマンドを実行した後、エクスポートの状態を確認します。ログフォルダーは次の場所にあります: `%HOMEPATH%\Documents\Citrix\AutoConfig`。
4. エラーまたは例外がある場合は、ログファイルの **Fixups** セクションを参照してください。

DaaS

構成をバックアップするための前提条件

- アクティブなリソースの場所とコネクタがインストールされている DaaS 環境。
- Citrix Cloud にアクセスするサイトへの接続。詳細については、「System and Connectivity Requirements」を参照してください。

> **注**
>
> Automated Configuration を使用して、クラウドから MCS をバックアップすることはできません。

バックアップ

次のファイルをバックアップします。

- 顧客 ID、クライアント ID、およびシークレットキー情報を含む `CustomerInfo.yml` ファイル。顧客 ID、クライアント ID、およびシークレットキーを取得するプロセスについて詳しくは、「顧客 ID、クライアント ID、およびシークレットキーの生成」を参照してください。この情報を `CustomerInfo.yml` ファイルに追加する方法については、「顧客情報ファイルの入力」を参照してください。
- クラウド内のリソースの場所をマッピングする情報を含む `ZoneMapping.yml` ファイル。ゾーンをマッピングする方法について詳しくは、「ゾーンマッピングファイルの入力」を参照してください。
- ホスト接続に関する情報を含む `CvadAcSecurity.yml` ファイル。

1. Automated Configuration をインストールします。詳細については、「Automated Configuration のインストール」を参照してください。

> **注**
>
> DaaS のバックアップの場合、Automated Configuration は、インターネットアクセスがあり、管理者が直接アクセスできるマシンにインストールしてください。

1. **Auto Config** をダブルクリックします。
2. PowerShell ウィンドウで、次のコマンドを実行してバックアップを作成します: `Export-CvadAcToFile`

コマンドを初めて実行すると、プロセスによって次の場所に .yml 構成ファイルを含むフォルダーが作成されます。 `%HOMEPATH%\Documents\Citrix\AutoConfig`

このフォルダーには、最近のエクスポートからのバックアップファイルが含まれており、以前の各バックアップはサブフォルダーに保存されます。

復元

1. 「**Auto Config**」をダブルクリックします。
2. PowerShellウィンドウで、次のコマンドを実行して復元します。

```
Restore-CvadAcToSite -RestoreFolder <folder path of the backup files>
```

3. コマンドを実行したら、エクスポートの状態を確認し、ログフォルダーは`%HOMEPATH%\Documents\Citrix\AutoConfig`にあります。
4. エラーまたは例外がある場合は、ログファイルの「**Fixups**」セクションを参照してください。

詳細な移行

> **注**
>
> コンポーネントの移行順序の詳細については、「」(/ja-jp/citrix-virtual-apps-desktops/current-release/manage-deployment/migrate.html#component-migration-order)を参照してください。

コンポーネント全体を復元する

コンポーネントを復元するには、1つ以上のパラメーターを選択する必要があります。

たとえば、デリバリーグループとマシンカタログコンポーネント全体を復元するには、次のコマンドを実行します。

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%
\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss -DeliveryGroups
-MachineCatalogs
```

コンポーネントメンバーを復元する

1つ以上のコンポーネントメンバーを復元するには、`IncludeByName`機能を使用します。選択したコンポーネントとインクルージョンリストとともに、`Restorefolder`パラメーターを指定して`Restore`コマンドレットを呼び出す必要があります。

たとえば、バックアップから2つのグループポリシーを復元するには：

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%
\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss -GroupPolicies
-IncludeByName Policy1,Policy2
```

クラウドサイト構成全体を復元する

すべてのコンポーネントまたはクラウドサイト全体を復元するには、次のコマンドを実行します。

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%
\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

バックアップと復元のためのAutomated Configurationツール

Automated Configuration ツールのコマンドは、Web Studio が使用するバックアップおよび復元 API をトリガーします。

`BckRstr` コマンドレットはコンソールにログを記録します。ログ情報を含むフォルダーは `\Documents\Citrix\AutoConfig` には作成されません。

注:

Citrix Virtual Apps and DesktopsおよびCitrix DaaS™で構成をバックアップするための前提条件は、PowerShellセッションのAutomated Configurationツールと同じです。

バックアップ

Delivery Controllerで新しいバックアップアクションを開始するには、PowerShellウィンドウで `New-BckRstrBackup` を実行します。

復元

既存のバックアップから単一コンポーネントのメンバーを復元するには、PowerShellウィンドウで `Restore-BckRstrBackups` を実行します。

コマンドの完全なリストについては、「バックアップと復元のためのAutomated Configuration ツールコマンドレット」を参照してください。

バックアップと復元のベストプラクティス

この記事では、バックアップと復元の計画をより適切に行うのに役立ついくつかの推奨事項を提供します。

カテゴリ	ベストプラクティス
バックアップのスケジュール設定	サイト構成の変更頻度に基づいて、毎日、毎週、または毎月の頻度で実行できるデフォルトのバックアップスケジュールを設定します。このデフォルトスケジュールは、アクティビティの少ない時間帯（週末や深夜など）に設定してください。スケジュールされたバックアップの詳細については、「スケジュールされたバックアップの作成」を参照してください。
	同じ日に実行される可能性のある複数のバックアップスケジュールが定義されている場合は、**Backup and Restore**ノードの**Settings**タブを使用して、1日あたりのバックアップ制限を1つにリセットします。
バックアップの管理	30個のバックアップ制限に達しても保持されるように、常にゴールデンコピーのバックアップをピン留めしてください。選択したバックアップをピン留めするには、バックアップを右クリックします。

よくある質問

カスタム管理者はバックアップと復元を実行できますか?

いいえ。バックアップと復元機能は、フル権限を持つ管理者のみに制限されています。

特定のコンポーネントをバックアップできますか?

いいえ。現在、オンデマンドおよびスケジュールされたバックアップは、サイト構成全体をバックアップします。コンポーネントにはいくつかの依存関係と前提条件があります。これらの依存関係が適切に解決されるように、コンポーネント全体をバックアップできます。ただし、特定のコンポーネントを復元することはできます。

バックアップをダウンロードできますか?

現在、バックアップをダウンロードするにはACTを使用します。Automated Configuration for Virtual Apps and DesktopsからACTをダウンロードできます。

MCSカタログをバックアップおよび復元できますか?

現在、MCSカタログをバックアップおよび復元することはできません。ACTを使用してMCSカタログをバックアップし、別のサイトにインポートできます。

構成をCitrix Cloud™に移行する

Automated Configuration Tool (ACT) を使用すると、Citrix Virtual Apps and Desktops™ の構成 (ポリシー、アプリケーション、カタログ、管理者ロール、スコープなど) を、1つ以上のオンプレミスサイトからCitrix Cloudでホストされているサービス Citrix DaaSに移行できます。また、異なるクラウドリージョンまたはテナント間で情報を移行するためにも使用できます。

このツールは、1つ以上のオンプレミスサイトを構成ファイルのコレクションとして検出し、エクスポートします。これらのファイルはオプションで編集できます。これらのファイルの構成は、Citrix DaaSにインポートできます。 移行は、ツールを複数回実行することで段階的に行われ、目的の構成状態を簡単に実現できます。

ACTは、一度きりの移行ツールではありません。日常のクラウド運用を管理するために使用できます。例えば、次のとおりです。

- テストまたはステージングのクラウドアカウントから本番クラウドアカウントへの転送を自動化する
- 構成のバックアップと復元
- 1つのクラウド環境を複数のクラウドに分割する

次の*2分間*のビデオでは、Automated Configurationのクイックツアーを提供します。

<iframe src="https://www.youtube.com/embed/uyQ9o2L1DXQ" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
Automated Configurationに関する追加情報については、Tech Zoneの概念実証: Automated Configuration Toolを参照してください。

展開の移動と、移行のためのオンプレミス構成の準備に関する詳細については、Tech Zoneの展開ガイド: オンプレミスからCitrix CloudへのCitrix Virtual Apps and Desktopsの移行を参照してください。

既知の制限事項

- Machine Creation Services™ を介してプロビジョニングされたマシンカタログには、特別な考慮事項があります。MCSの詳細については、Machine Creation Servicesでプロビジョニングされたカタログの移行についてを参照してください。

構成を移行するための前提条件

Citrix Virtual Apps and Desktops™ から構成を*エクスポート*するには、以下が必要です。

- Citrix Virtual Apps and Desktops: 現在のリリースとその直前のリリース、またはCitrix Virtual Apps and Desktops、XenApp and XenDesktop® LTSRs: すべてのバージョン
- .NET Framework 4.7.2以降とCitrix PowerShell SDKがインストールされたドメイン参加済みマシン。これはDelivery Controllerに自動的にインストールされます。(オンプレミスのDelivery Controller以外のマシンで実行するには、Studioが適切なPowerShellスナップインをインストールするため、Citrix Studioをインストールする必要があります。Studioインストーラーは Citrix Virtual Apps and Desktopsのインストールメディアにあります。)

Citrix DaaSに構成を*インポート*するには、以下が必要です。

- Citrix Cloudにアクセスできるマシン。これはDelivery Controller™やドメイン参加済みマシンである必要はありません。
- Citrix DaaSがプロビジョニングされていること。
- Connectorがインストールされ、オンプレミス環境と同じドメインに参加しているアクティブなリソースの場所。
- Citrix Cloudにアクセスするサイトへの接続が許可され、利用可能である必要があります。詳細については、システムおよび接続要件を参照してください。

> **注:**
>
> Automated ConfigurationはCloud Connectorシステムにはインストールできません。

主な手順

1. Automated Configuration Toolをダウンロードし、システム要件を確認します。Automated Configurationのダウンロードを参照してください。
2. Citrix Cloudポータルから生成された`CustomerName`、`CustomerID`、および`SecretKey`の値で`CustomerInfo.yml`ファイルを埋めます。顧客ID、クライアントID、およびシークレットキーの生成と顧客情報ファイルの入力を参照してください。
3. オンプレミスサイトに複数のゾーンが含まれている場合は、ゾーンをCitrix DaaSリソースの場所にマッピングするように`ZoneMapping.yml`ファイルを更新します。ゾーンマッピングファイルの入力を参照してください。

4. サイトに複数のホスティング接続が含まれている場合は、Citrix DaaSに移行する各ホストタイプの接続情報で`CvadAcSecurity.yml`ファイルを更新します。ホスト接続が1つしかない場合は、ホスト接続の接続情報で`CvadACSecurity.yml`ファイルを更新します。ホスト接続のセキュリティファイルの更新を参照してください。
5. ACTを開き、`Export-CvadAcToFile`コマンドを使用してオンプレミスサイトをエクスポートします。移行でサポートされているコンポーネントのリストについては、サポートされている移行オブジェクトを参照してください。エクスポートの手順については、オンプレミス構成のエクスポートを参照してください。
6. `Merge-CvadAcToSite`コマンドを使用して、コンポーネントを段階的にインポートします。または、サイト全体を一度に移行します。コンポーネントの移行順序に記載されている順序でコンポーネントを移行してください。インポートの手順については、インポートの実行を参照してください。
7. クラウドサイトをアクティブ化します。サイトのアクティブ化を参照してください。

Automated Configurationをダウンロードする

Citrix DownloadsからAutomated Configurationツールをダウンロードしてインストールします。

Automated Configurationをアップグレードする

機能のエラーを防ぐため、常にACTの最新バージョンを使用してください。

ツールのバージョンを確認するには、次の手順を実行します。

1. **Auto Config**アイコンをダブルクリックします。PowerShellウィンドウが表示されます。
2. バージョン番号を確認するには、次のコマンドを実行します。

```
Get-CvadAcStatus
```

3. Citrix Downloadsに記載されているバージョンとツールのバージョンを比較します。ツールの最新バージョンはそこにあります。
4. ツールの最新バージョンをダウンロードしてインストールします。Automated Configurationをアップグレードするために、古いバージョンをアンインストールする*必要はありません*。

> **注:**

> Automated Configurationでクラウドにアクセスするためにコマンドレットを実行すると、ダウンロード可能な新しいバージョンがある場合にツールが通知します。コマンドレットの詳細については、Automated Configurationツールコマンドレットを参照してください。

顧客ID、クライアントID、およびシークレットキーを生成する

オンプレミスサイトをCitrix DaaSに移行するには、Citrix Cloudポータルから顧客ID、クライアントID、およびシークレットキーを使用して`CustomerInfo.yml`ファイルを入力します。

顧客IDを取得するには：

1. Citrix Cloudアカウントにサインインし、顧客を選択します。
2. グリッドアイコンをクリックし、**ID およびアクセス管理**を選択します。
3. **API アクセス > サービスプリンシパル**に移動します。顧客 ID がページに表示されます。

クライアントIDとシークレットキーを取得するには：

1. サービスプリンシパルページで、クライアント ID とシークレットを生成するためにサービスプリンシパルを作成します。
2. クライアントIDとシークレットキーを安全な場所にコピーし、この情報を含む`.csv`ファイルをダウンロードします。`.csv`ファイルを使用して`CustomerInfo.yml`ファイルを生成します。

> **注:**
>
> - サービスプリンシパルのシークレットの有効期限は構成可能です。シークレットが侵害された場合は、シークレットをローテーションできます。詳細については、「Citrix Cloud API の使用を開始する」を参照してください。
> - シークレットキーは、紛失または忘れた場合、取得できません。新しいクライアントIDとシークレットキーを作成する必要があります。

顧客情報ファイルを生成する

`CustomerInfo.yml`ファイルを使用すると、コマンドレットを実行するたびに顧客情報パラメーターを指定する必要がなくなります。顧客情報のいずれかは、コマンドレットパラメーターを使用して上書きできます。

`New-CvadAcCustomerInfoFile` コマンドレットを使用して、`CustomerInfo.yml` ファイルを作成します。

> **重要:**
>
> `CustomerInfo.yml` ファイルを手動で編集しないでください。手動で編集すると、意図しない書式設定エラーが発生する可能性があります。

`New-CvadAcCustomerInfoFile` コマンドレットには、次の必須パラメーターがあります。

- CustomerId: 顧客のID。
- ClientId: Citrix Cloud で作成された顧客のクライアントID。
- Secret: Citrix Cloud で作成された顧客のシークレット。

例:

```
New-CvadAcCustomerInfoFile -CustomerId markhof123 -ClientId
6813EEA6-46CC-4F8A-BC71-539F2DAC5984 -Secret TwBLaaaaaaaaaaaaaaaaw==
```

ダウンロードした `security.csv` ファイルを指す `SecurityCsvFileSpec` パラメーターを使用して、`CustomerInfo.yml` を作成することもできます。CustomerId も指定する必要があります。

```
New-CvadAcCustomerInfoFile -SecurityCsvFileSpec C:
\Users\my_user_name\downloads/security.csv -CustomerId markhof123
```

`CustomerInfo.yml` ファイルを更新するには、`Set-CvadAcCustomerInfoFile` コマンドレットを使用します。このコマンドレットはクライアントIDのみを変更します。

```
Set-CvadAcCustomerInfoFile -ClientId C80487EE-7113-49F8-85DD-2CFE30CC398E
```

以下は、CustomerInfo.yml ファイルのサンプルです。

```
# Created/Updated on 2020/01/29 16:46:47

CustomerId: ‘markhof123’
```

```
ClientId: ‘6713FEA6-46CC-4F8A-BC71-539F2DDK5384’

Secret: ‘TwBLaaabbbaaaaaaaaaaw==’

Environment: Production

AltRootUrl: ‘’

StopOnError: False

AlternateFolder: ‘’

Locale: ‘en-us’

Editor: ‘C:\Program Files\Notepad++\notepad++.exe’

Confirm: True

DisplayLog: True
```

ゾーンマッピングファイルにデータを入力する

オンプレミスゾーンは、クラウドのリソースの場所と同等です。他のサイトコンポーネントとは異なり、オンプレミスゾーンをクラウドに自動的にインポートすることはできません。代わりに、`ZoneMapping.yml` ファイルを使用して手動でマッピングする必要があります。ゾーン名が既存のリソースの場所名に関連付けられていない場合、インポートが失敗する可能性があります。

オンプレミスサイトにゾーンが1つしかなく、クラウドサイトにリソースの場所が1つしかない場合、自動構成ツールが正しい関連付けを行うため、`ZoneMapping.yml` ファイルを手動で管理する必要はありません。

ただし、オンプレミスサイトに複数のゾーンがある場合、またはクラウドサイトに複数のリソースの場所がある場合は、`ZoneMapping.yml` ファイルを手動で更新して、オンプレミスゾーンとクラウドのリソースの場所の正しいマッピングを反映させる必要があります。

`ZoneMapping.yml` ファイルは `%HOMEPATH%\Documents\Citrix\AutoConfig` にあります。`.yml` ファイルの内容は、ゾーン名をキー、リソースの場所名を値とする辞書です。

たとえば、「Zone-1」というプライマリゾーンと「Zone-2」というセカンダリゾーンを持つオンプレミスの Citrix Virtual Apps and Desktops サイトが、「Cloud-RL-1」と「Cloud-RL-2」という2

つの新しく作成されたクラウドのリソースの場所を持つ Citrix DaaS 展開に移行されます。この場合、ZoneMapping.yml は次のように構成されます。

```
            Zone-1: Cloud-RL-1



            Zone-2: Cloud-RL-2
```

注:

コロンとリソースロケーション名の間にスペースを追加します。ゾーンまたはリソースロケーション名にスペースが含まれている場合は、名前を引用符で囲みます。

ホスト接続用のセキュリティファイルを更新する

ホスト接続とそれに関連付けられたハイパーバイザーは、ACTを使用してエクスポートおよびインポートできます。

ホスト接続にハイパーバイザーを追加するには、ハイパーバイザーの種類に固有のセキュリティ情報が必要です。この情報は、セキュリティ上の理由からオンプレミスサイトからエクスポートできません。Automated Configurationがホスト接続とハイパーバイザーをクラウドサイトに正常にインポートできるように、この情報を手動で提供する必要があります。

エクスポートプロセスでは、特定のハイパーバイザータイプに必要な各セキュリティ項目のプレースホルダーを含む `%HOMEPATH%\Documents\Citrix\AutoConfig` に `CvadAcSecurity.yml` ファイルが作成されます。クラウドサイトにインポートする前に、`CvadAcSecurity.yml` ファイルを更新する必要があります。管理者による更新は、必要に応じて新しいセキュリティプレースホルダーが追加され、複数のエクスポートにわたって保持されます。セキュリティ項目が削除されることはありません。詳細については、「CvadAcSecurity.ymlファイルを更新する」を参照してください。

```
HostConn1:

ConnectionType: XenServer®

UserName: root

PasswordKey: rootPassword
```

```
HostCon2:

ConnectionType: AWS

ApiKey: 78AB6083-EF60-4D26-B2L5-BZ35X00DA5CH

SecretKey: TwBLaaaaaaaaaaaaaaaaw==

Region: East
```

ハイパーバイザーごとのセキュリティ情報

各ハイパーバイザータイプに必要なセキュリティ情報を以下に示します。

- ゼノサーバー、ハイパーブイ、ヴイエムウェア
  - ユーザー名
  - クリアテキストパスワード
- マイクロソフト アジュール
  - サブスクリプションID
  - アプリケーションID
  - アプリケーションシークレット
- AWS
  - サービスアカウントID
  - アプリケーションシークレット
  - 地域

セキュリティに関する特別な考慮事項

すべてのセキュリティ情報はクリアテキストとして入力されます。クリアテキストが推奨されない場合は、ホスト接続と関連するハイパーバイザーを**Studio**を使用して手動で作成できます。ホスト接続とハイパーバイザー名は、オンプレミスの対応するものと正確に一致している必要があります。そうすることで、ホスト接続を使用するマシンカタログを正常にインポートできます。

Citrix Virtual Apps and Desktopsのオンプレミス構成をエクスポートする

`export` PowerShellコマンドを使用して、既存のオンプレミス構成をエクスポートし、必要な`.yml`ファイルを取得できます。これらのファイルは、目的の構成をCitrix Cloudにインポートするために使用されます。

サポートされている移行オブジェクト

自動構成は、以下のコンポーネントの構成の移動をサポートしています。

- タグ
- 委任管理
  - スコープ
  - ロール
- ホスト接続
  - 単一のリソースプール
  - 管理者スコープ
- マシンカタログ
  - 管理者スコープ
  - マシン
  - リモートPCアクセス、物理、プール、プロビジョニング済み、MCS、割り当て済み
- StoreFront™
- デリバリー グループ
  - アクセスポリシー
  - 管理スコープの関連付け
  - アプリケーションアクセスポリシー
  - 割り当てポリシー
  - エンタイトルメント/デスクトップポリシー
  - 電源スケジュール
  - セッションの残存
  - セッションの事前起動
  - 再起動スケジュール

    - タグ
- アプリケーション グループ
    - 管理スコープの関連付け
    - デリバリー グループ
    - ユーザーとグループ
- アプリケーション
    - アプリケーション フォルダー
    - アイコン
    - アプリケーション
    - ブローカー構成済みFTA
    - タグ
- グループ ポリシー
- ユーザーゾーンの基本設定

オンプレミス構成のエクスポート

1. **Auto Config** アイコンをダブルクリックします。PowerShell ウィンドウが表示されます。
2. すべてのコンポーネントをエクスポートするには、次のコマンドを実行します。オンプレミス構成をエクスポートしても、その構成が変更されることは*ありません*。

```
Export-CvadAcToFile
```

任意のコマンドレットを初めて実行すると、`.yml` 構成ファイルとログを含むエクスポートフォルダーが作成されます。このフォルダーは `%HOMEPATH%\Documents\Citrix\AutoConfig` にあります。エクスポートを繰り返すたびにサブフォルダーが作成されます。親フォルダー `%HOMEPATH%\Documents\Citrix\AutoConfig` には、常に最新のエクスポートからのエクスポートファイルが含まれています。

注:

Delivery Controller に Automated Configuration がインストールされていない場合は、PowerShell を介してツールを使用する前に `import-module`

> `Citrix.AutoConfig.Commands` を実行します。**Auto Config** アイコンを使用して Automated Configuration を開く場合は、この手順は不要です。

> エラーまたは例外が発生した場合は、ログファイルの **Fixups** セクションを参照してください。

構成を Citrix DaaS にインポートする

> **重要:**
>
> - オンプレミス展開をクラウドに移行する際は、Citrix 設定を含むドメインおよびOU GPOがクラウドに移行されていることを確認してください。Citrix Web Studio™はGPMCをサポートしていないため、ドメインおよびOU GPOはWeb Studioに表示されません。Citrixポリシーエンジンは、ドメインおよびOU内のVDAとユーザーにドメインおよびOU GPOを適用します。VDAにログインした後、ユーザーはドメインおよびOU GPOからのポリシーがセッションに適用されていることを確認できる場合があります。ただし、管理者はこれらのポリシーと設定を確認できないため、混乱を招く可能性があります。

コンポーネントの移行順序

コンポーネントとその依存関係をここに示します。コンポーネントをインポートまたはマージする前に、その依存関係が配置されている必要があります。依存関係が不足している場合、インポートまたはマージコマンドが失敗する可能性があります。インポートまたはマージが失敗した場合、ログファイルの **Fixups** セクションに不足している依存関係が表示されます。

1. タグ
    - 事前依存関係なし
2. 委任管理者
    - 事前依存関係なし
3. ホスト接続
    - CvadAcSecurity.yml のセキュリティ情報
4. マシンカタログ
    - Active Directory に存在するマシン

- ホスト接続
- タグ

5. StoreFront
6. デリバリーグループ
    - Active Directory に存在するマシン
    - Active Directory に存在するユーザー
    - マシンカタログ
    - タグ
7. アプリケーショングループ
    - デリバリーグループ
    - タグ
8. アプリケーション
    - デリバリーグループ
    - アプリケーショングループ
    - タグ
9. グループポリシー
    - デリバリーグループ
    - タグ
10. ユーザーゾーン設定

インポートを実行する

1. **Auto Config**アイコンをダブルクリックします。PowerShellウィンドウが表示されます。
2. すべてのコンポーネントをインポートするには、次のコマンドを実行します。

```
Merge-CvadAcToSite
```

期待される状態と新しい現在の状態を確認します。さまざまなインポートオプションにより、インポート結果がオンプレミスサイトと同一であるか、そのサブセットであるかが制御されます。

コマンドレットを実行すると、`.yml`構成ファイルとログを含むエクスポートフォルダーが作成されます。フォルダーは`%HOMEPATH%\Documents\Citrix\AutoConfig`にあります。

エラーまたは例外が発生した場合は、ログファイルの**Fixups**セクションを参照してください。

> **注:**
>
> Delivery ControllerにAutomated Configurationがインストールされていない場合は、PowerShellを介してツールを使用する前に`import-module Citrix.AutoConfig.Commands`を実行してください。**Auto Config**アイコンを使用してAutomated Configurationを開く場合は、この手順は不要です。

> 元のCitrix DaaS構成に戻すには、Citrix DaaS構成のバックアップを参照してください。

インポート操作を理解する

インポートプロセスは、更新を正確に実行し、必要な更新のみを実行し、すべての更新が正しく行われたことを確認するように設計されています。すべてのインポート操作で以下の手順が実行されます。

1. エクスポートされた.ymlファイル（期待される状態）を読み取ります。
2. クラウド（現在の状態）を読み取ります。
3. インポート前のクラウドの状態を.ymlファイルにバックアップします（必要に応じて、事前バックアップを復元できます）。
4. 期待される状態と現在の状態の差分を評価します。これにより、どの更新を行うかが決定されます。
5. 更新を実行します。
6. クラウドを再読み込みします（新しい現在の状態）。
7. インポート後のクラウドの状態を.ymlファイルにバックアップします（必要に応じて、事後バックアップを復元できます）。
8. 新しい現在の状態を期待される状態と比較します。
9. 比較結果を報告します。

詳細な移行

> **重要:**

> コンポーネントの移行順序の詳細については、「コンポーネントの移行順序」を参照してください。

> コンポーネントのみ、またはコンポーネント名のみを選択的に移行できます。

- サポートされているコンポーネントパラメーターには、`MachineCatalogs`、`Tags` などがあります。
- サポートされているコンポーネント名パラメーターには、`IncludeByName` および `ExcludeByName` パラメーターなどがあります。

パラメーターとその使用方法の詳細については、「きめ細かな移行パラメーター」を参照してください。

サイトをアクティブ化する

オンプレミスサイトとクラウドサイトの両方にあるデリバリーコントローラーは、デスクトップ、アプリケーションの仲介、マシンの再起動などのリソースを制御します。2つ以上のサイトによって共通のリソースセットが制御されると、問題が発生します。このような状況は、オンプレミスサイトからクラウドサイトに移行する際に発生する可能性があります。オンプレミスとクラウドの両方のデリバリーコントローラーが同じリソースセットを管理する可能性があります。このような二重管理は、リソースが利用できなくなり、管理不能になる可能性があり、診断が困難になる場合があります。

サイトのアクティブ化により、アクティブなサイトがどこで制御されるかを制御できます。

サイトのアクティブ化は、デリバリーグループのメンテナンスモードを使用して管理されます。サイトが非アクティブな場合、デリバリーグループはメンテナンスモードになります。アクティブなサイトのデリバリーグループからはメンテナンスモードが解除されます。

サイトのアクティブ化は、VDA登録やマシンカタログに影響を与えたり、管理したりすることはありません。

- `Set-CvadAcSiteActiveStateCloud`
- `Set-CvadAcSiteActiveStateOnPrem`

すべてのコマンドレットは、`IncludeByName` および `ExcludeByName` フィルタリング をサポートしています。このパラメーターを使用すると、メンテナンスモードを変更できるデリバリーグループを選択できます。デリバリーグループは必要に応じて選択的に変更できます。

インポートとクラウドへの制御の移行

オンプレミスサイトからクラウドサイトへ制御をインポートおよび転送する方法の概要を以下に示します。

1. オンプレミスサイトをクラウドにエクスポートおよびインポートします。`-SiteActive` パラメーターがインポートコマンドレットのいずれにも存在しないことを確認してください。オンプレミスサイトはアクティブで、クラウドサイトは非アクティブです。デフォルトでは、クラウドサイトのデリバリーグループはメンテナンスモードになっています。
2. クラウドのコンテンツと構成を確認します。
3. 営業時間外に、オンプレミスサイトを非アクティブに設定します。`-SiteActive` パラメーターは存在しない必要があります。すべてのオンプレミスサイトのデリバリーグループはメンテナンスモードになっています。
   - `Set-CvadAcSiteActiveStateOnPrem`
4. クラウドサイトをアクティブに設定します。`-SiteActive` パラメーターは存在する必要があります。クラウドサイトのデリバリーグループはメンテナンスモードではありません。
   - `Set-CvadAcSiteActiveStateCloud -SiteActive`
5. クラウドサイトがアクティブで、オンプレミスサイトが非アクティブであることを確認します。

オンプレミスサイトに制御を戻す

クラウドサイトからオンプレミスサイトに制御を転送するには：

1. 営業時間外に、クラウドサイトを非アクティブに設定します。すべてのクラウドサイトのデリバリーグループはメンテナンスモードになっています。
   - `Set-CvadAcSiteActiveStateCloud`
2. オンプレミスサイトをアクティブに設定します。オンプレミスサイトのデリバリーグループはメンテナンスモードではありません。
   - `Set-CvadAcSiteActiveStateOnPrem -SiteActive`

その他のサイトアクティベーション情報

- 電源管理されているマシンがなく、再起動スケジュールもない場合（通常、ホスト接続もないことを意味します）、すべてのクラウドデリバリーグループをアクティブとしてインポートできます。インポート後に `Merge-CvadAcToSite` / `Import-CvadAcToSite` に `-SiteActive` を追加するか、`Set-CvadAcSiteActiveStateCloud -SiteActive` を実行してください。

- マシンが電源管理されている場合、または再起動スケジュールがある場合は、別のプロセスが必要です。たとえば、この状況でオンプレミスからクラウドに切り替える場合、`Set-CvadAcSiteActiveStateOnPrem` を使用してオンプレミスサイトを非アクティブに設定します。次に、`Set-CvadAcSiteActiveStateCloud -SiteActive` を使用してクラウドサイトをアクティブに設定します。
- `Set-CvadAcSiteActiveStateCloud` および `Set-CvadAcSiteActiveStateOnPrem` コマンドレットは、プロセスを逆にするためにも使用されます。たとえば、`-SiteActive` パラメーターなしで `Set-CvadAcSiteActiveStateCloud` を実行し、次に `-SiteActive` パラメーターを指定して `Set-CvadAcSiteActiveStateOnPrem` を実行します。

Machine Creation Servicesでプロビジョニングされたカタログの移行について理解する

> **注:**
>
> この機能はバージョン3.0以降でのみ利用可能です。Automated Configuration内で `Get-CvadAcStatus` を使用してバージョンを確認してください。

> Machine Creation Services (MCS) カタログは、2種類のカタログを作成します。

- マシンに加えられた変更が失われるか元に戻される場合（一般的にアプリケーションが公開されるサーバーOS） – これはプールされたVDI / マルチセッションのユースケースです
- マシンに加えられた変更が再起動後も保持される場合（一般的に専用ユーザーを持つクライアントOS） – これは静的VDIのユースケースです

カタログの種類は、Citrix Studioのカタログノードでカタログの「User data:」値を確認することで確認できます。

> **注:**
>
> MCSは、Automated Configurationを使用してクラウドからバックアップすることはできません。

プールされたVDI / マルチセッションカタログ

「User data: Discard」のカタログはプールされたVDIカタログであり、メインイメージと構成のみを移行できます。これらのカタログ内の仮想マシンは移行されません。これは、仮想マシンのライフサイクルがインポート元のサイトによって維持されており、マシンが起動されるたびにその

状態が変化する可能性があるためです。これにより、仮想マシンのインポートデータがすぐに同期されなくなるため、インポートは不可能になります。

このツールを使用してこれらのカタログを移行する場合、カタログメタデータが作成され、メインイメージの作成が開始されますが、マシンはインポートされません。

メインイメージのサイズに基づいてこのプロセスの作成には時間がかかる場合があるため、ツール内のインポートコマンドはMCSカタログの作成を開始するだけで、完了を待機しません。インポートが完了したら、クラウド展開のStudioを使用してカタログ作成の進行状況を監視してください。

メインイメージが作成されたら、マシンをプロビジョニングできます。オンプレミスでの使用から容量が消費されるため、容量に関する考慮事項を検討してください。

そのカタログを使用する他のすべてのオブジェクト（デリバリーグループ、アプリケーション、ポリシーなど）はインポートでき、メインイメージの作成を待つ必要はありません。カタログの作成が完了したら、インポートされたカタログにマシンを追加でき、その後ユーザーはリソースを起動できます。

> **注:**
>
> カタログおよびその他すべてのオブジェクトを移行するには、ツール内で利用可能な同じコマンドを使用します。

静的VDIカタログ

> **注:**
>
> この操作はデータベースに保存されている低レベルの詳細をインポートするため、このプロセスはデータベースアクセス権を持つマシンから実行する必要があります。

> 静的VDIカタログは、メインイメージ、構成、およびすべての仮想マシンを移行します。プールされたVDIのユースケースとは異なり、イメージを作成する必要はありません。

VDAがクラウドに登録されるように、コネクタを指すように設定する必要があります。

クラウドサイトをアクティブにするには、サイトのアクティブ化セクションを参照してください。これにより、再起動スケジュール、電源管理、その他の項目がクラウドによって制御されます。

移行が完了した後、オンプレミスサイトからこのカタログを削除したい場合は、**VMとADアカウントを残す**を選択する必要があります。そうしないと、それらは削除され、クラウドサイトは削除されたVMを指したままになります。

移行後に孤立したリソースを検出するためにMCSタグを更新する

オンプレミス構成からクラウドサイトへ、またはクラウド構成から別のクラウドサイトへ移行した後、永続VMの場合に孤立したリソースが正しく検出されるように、MCSサイトIDタグを更新する必要があります。これを行うには、PowerShellコマンド`Set-ProvResourceTags`を使用します。現在、この機能はAzureに適用されます。

詳細な手順は次のとおりです。

1. 新しいCitrixサイトからPowerShellコマンド `Set-ProvResourceTags` を使用してMCSサイトIDタグを更新します。例:

   ```
   Set-ProvResourceTags -ProvisioningSchemeUid xxxxx  [-VMName <String>]
   [-VMBatchSize XX] [-ResourceType XX]
   ```

   または、,

   ```
   Set-ProvResourceTags -ProvisioningSchemeName xxxxx  [-VMName <String>]
   [-VMBatchSize XX] [-ResourceType XX]
   ```

パラメーターの詳細は次のとおりです。

- `ProvisioningSchemeUid` または `ProvisioningSchemeName` は必須パラメーターです。
- `VMName` はオプションパラメーターです。`VMName` が指定されていない場合、このマシンカタログのすべてのVMのタグが更新されます。
- `VMBatchSize` は、すべてのVMをバッチに分割するためのオプションパラメーターです。`VMBatchSize` が指定されていない場合、デフォルト値 (10) が適用されます。範囲は1から60です。
- `ResourceType` は次のいずれかです。
  - `MachineCatalog`: マシンカタログリソースのタグを更新する場合。
  - `VirtualMachine`: VM関連リソースのタグを更新する場合。
  - `All`: (デフォルトのResourceType): マシンカタログとVM関連リソースの両方のタグを更新する場合。

複数のサイトを単一のサイトに統合する

自動構成のマルチサイトサポートは、複数のオンプレミスサイトを単一のクラウドサイトに統合する方法を提供します。

マルチサイトサポートは、オンプレミスサイトごとにコンポーネント名に一意のプレフィックスとサフィックスを追加し、複数のオンプレミスサイトが単一のクラウドサイトに統合された後の名前の一意性を確保します。

プレフィックスとサフィックスは、オンプレミスサイトごとに次の各コンポーネントに割り当てることができます。

- `AdminScope`
- `AdminRole`
- `ApplicationAdmin`
- `ApplicationFolder`
- `ApplicationGroup`
- `ApplicationUser`
- `DeliveryGroup`
- `GroupPolicy`
- `HostConnection`
- `MachineCatalog`
- `StoreFront™`
- `Tag`

アプリケーションフォルダーは、プレフィックス、サフィックス、およびルートの再設定をサポートしています。ルートの再設定により、アプリケーションの既存のフォルダー構造に最上位のフォルダーが追加されます。

プレフィックスとサフィックスのルール

1. プレフィックスとサフィックスには、次の特殊文字を含めることはできません。`\ , / ; : # . * ? = < > | ( ) " ' { } [ ]`
2. プレフィックスとサフィックスには末尾のスペースを含めることができますが、先頭のスペースは含めることはできません。
3. プレフィックスとサフィックスは、末尾のスペースを含めるために二重引用符で囲む必要があります。

4. プレフィックスとサフィックスは、インポート、マージ、追加の際に適用されます。ソースの.ymlファイルは変更されません。
5. プレフィックスとサフィックスのプロセスは、該当する場合、依存するコンポーネント名に自動的にプレフィックスまたはサフィックスを付けます。たとえば、マシンカタログ名に「East」というプレフィックスが付いている場合、それらを参照するデリバリーグループにも「East」というプレフィックスが付けられます。
6. コンポーネント名がすでにプレフィックスまたはサフィックスで始まっている場合、プレフィックスまたはサフィックスは追加されません。コンポーネント名に、同じプレフィックスまたはサフィックスが二重に含まれることはできません。
7. プレフィックスとサフィックスは個別に、または組み合わせて使用できます。
8. コンポーネントへのプレフィックスまたはサフィックスの使用はオプションです。

> **注:**
>
> Studioはコンポーネントをアルファベット順に表示します。

サイト別にコンポーネントをグループ化する

プレフィックスを使用して、単一サイトのコンポーネントを視覚的にグループ化します。各サイトは独自のグループにリストされ、プレフィックスによって異なるサイトグループの順序がアルファベット順に制御されます。

名前でコンポーネントをグループ化

複数のサイトから同じ名前のコンポーネントを視覚的にグループ化するには、サフィックスを使用します。異なるサイトの同じ名前のコンポーネントは、視覚的に交互に表示されます。

プレフィックスとサフィックスのマッピングファイル

サイトのプレフィックス付けは、1つ以上のオンプレミスサイトのサイトプレフィックスとサフィックスのマッピングを含むSiteMerging.ymlファイルから始まります。SiteMerging.ymlファイルは手動で管理することも、複数のオンプレミスサイトをマージするコマンドレットセクションに記載されている利用可能なコマンドレットを使用して管理することもできます。

オンプレミスサイトのエクスポート

オンプレミスサイトをエクスポートするまで、マージを開始することはできません。オンプレミスサイトをエクスポートするには、オンプレミス構成のエクスポートを参照してください。

中央エクスポートターゲットフォルダー

このセクションで説明する方法では、複数のサイトのエクスポートを中央のファイル共有場所に配置します。`SiteMerging.yml` ファイル、`CustomerInfo.yml` ファイル、およびすべてのエクスポートファイルは、そのファイル共有場所に存在するため、オンプレミスサイトとは独立して1つの場所からインポートを実行できます。

クラウドアクセス操作は、オンプレミスサイトやActive Directoryを参照しないため、どこからでもクラウドアクセス操作を実行できます。

直接ファイル共有

これを行うには、2つの方法があります。

- 直接ファイル共有: 直接ファイル共有からインポート、マージ、または追加するには、どのマシンからクラウドアクセス操作を実行するかを決定する必要があります。
- `SiteMerging.yml`を使用したファイル共有参照: この方法では、サイトのプレフィックスセットの`SiteRootFolder`メンバーを使用し、エクスポート、インポート、マージ、または追加の際に誤ったフォルダーをターゲットにする可能性を減らします。

中央ファイル共有方法を使用しない場合は、個々のDelivery Controllerからインポート、結合、または追加を実行します。クラウドに移行される各Delivery Controllerで `SiteMerging.yml` ファイルを作成し、レプリケートします。デフォルトの場所は `%HOMEPATH%\Documents\Citrix\AutoConfig` です。正しいサイトプレフィックスを選択するには、`-SiteName` パラメーターを指定する必要があります。

直接ファイル共有

エクスポート、インポート、マージ、および新規/追加操作では、デフォルトのフォルダーである*%HOMEPATH%\Documents\Citrix\AutoConfig*以外のフォルダーをターゲットまたはソースとするパラメーターが提供されます。以下の例では、管理者がすでにアクセス権を持ち、必要に応じて資格情報を提供している`\\share.central.net`にある中央ファイル共有を使用します。

エクスポートをサイト固有のフォルダーにターゲット設定するには、`-TargetFolder` パラメーターを使用します。

東 デリバリーコントローラー™から::

```
mkdir \\share.central.net\AutoConfig\SiteEast
```

```
Export-CvadAcToFile -TargetFolder \\share.central.net\AutoConfig\SiteEast
```

西 デリバリーコントローラーから::

```
mkdir \\share.central.net\AutoConfig\SiteWest
```

```
Export-CvadAcToFile –TargetFolder \\share.central.net\AutoConfig\SiteWest
```

エクスポートが完了したら、`CustomerInfo.yml`と`SiteMerging.yml`ファイルを作成し、`\\share.central.net\AutoConfig`に配置します。

> **注:**
>
> この直接ファイル共有参照方法を使用する場合、`SitePrefixes.yml`を作成する際に`SiteRootFolder`パラメーターを使用しないでください。

> 直接ファイル共有からインポート、マージ、または追加するには、どのマシンからクラウドアクセス操作を実行するかを決定する必要があります。オプションは次のとおりです。

- ツールがすでにインストールされているオンプレミスの Delivery Controller のいずれか。
- ファイル共有をホストしているマシン。
- 別のマシン。

Automated Configurationは、クラウドにアクセスするマシンにインストールする必要があります。オンプレミスのPowerShell SDK、Delivery Controller、Active Directoryは使用されないため、クラウドアクセス実行要件はエクスポート要件よりもシンプルです。

East Delivery Controllerをクラウドに統合するには：

```
Merge-CvadAcToSite –SiteName East –SourceFolder \
\share.central.net\AutoConfig\SiteEast -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

West Delivery Controllerをクラウドに統合するには：

```
Merge-CvadAcToSite –SiteName West –SourceFolder \
\share.central.net\AutoConfig\SiteWest -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

以下は、前の例で使用された`SitePrefixes.yml`ファイルのサンプルです。

```
East:

  SiteRootFolder: "" # Important: leave this empty

  AdminScopePrefix: "East_"

  AdminRolePrefix: "East_"

  ApplicationAdminPrefix: "East_"

  ApplicationFolderPrefix: "" # Note that a new parent root folder is used
instead

  ApplicationFolderRoot: "East"

  ApplicationGroupPrefix: "East_"

  ApplicationUserPrefix: "East_"

  DeliveryGroupPrefix: "East_"

  GroupPolicyPrefix: "East_"

  HostConnectionPrefix: "East_"

  MachineCatalogPrefix: "East_"

  StoreFrontPrefix: "East_"

  TagPrefix: "East_"

  AdminScopeSuffix: "_east"

  AdminRoleSuffix: "_east"

  ApplicationAdminSuffix: "_east"

  ApplicationFolderSuffix: "_east"

  ApplicationGroupSuffix: "_east"

  ApplicationUserSuffix: "_east"
```

```
  DeliveryGroupSuffix: "_east"

  GroupPolicySuffix: "_east"

  HostConnectionSuffix: "_east"

  MachineCatalogSuffix: "_east"

  StoreFrontSuffix: "_east"

  TagSuffix: "_east"

West:

  SiteRootFolder: "" # Important: leave this empty

  AdminScopePrefix: "Western "

  AdminRolePrefix: "Western "

  ApplicationAdminPrefix: "Western "

  ApplicationFolderPrefix: "" # Note that a new parent root folder is used
instead

  ApplicationFolderRoot: "Western"

  ApplicationGroupPrefix: "Western "

  ApplicationUserPrefix: "Western "

  DeliveryGroupPrefix: "Western "

  GroupPolicyPrefix: "Western "

  HostConnectionPrefix: "Western "

  MachineCatalogPrefix: "Western "

  StoreFrontPrefix: "Western "

  TagPrefix: "Western "
```

```
AdminScopeSuffix: ""

AdminRoleSuffix: ""

ApplicationAdminSuffix: ""

ApplicationFolderSuffix: ""

ApplicationGroupSuffix: ""

ApplicationUserSuffix: ""

DeliveryGroupSuffix: ""

GroupPolicySuffix: ""

HostConnectionSuffix: ""

MachineCatalogSuffix: ""

StoreFrontSuffix: ""

TagSuffix: ""
```

SiteMerging.yml を使用したファイル共有参照

この方法では、サイトのプレフィックスセットの`SiteRootFolder`メンバーを使用します。直接ファイル共有方法よりも複雑ですが、この方法を使用すると、エクスポート、インポート、マージ、または追加時に誤ったフォルダーをターゲットにする可能性が低減されます。

まず、SiteMerging.ymlファイルで各サイトの`SiteRootFolder`を設定します。これは共有場所で行う必要があります。

`New-CvadAcSiteMergingInfo –SiteName East –SiteRootFolder \ \\share.central.net\AutoConfig\SiteEast -SitePrefixesFolder \ \\share.central.net\AutoConfig`

`New-CvadAcSiteMergingInfo –SiteName West –SiteRootFolder SiteWest -SitePrefixesFolder \\share.central.net\AutoConfig`

この例では、Eastは完全修飾フォルダー指定であり、Westは相対フォルダー指定です。

SiteMerging.ymlファイルを使用して、エクスポートをサイト固有のフォルダーにターゲット設定するには：

イースト デリバリー コントローラーから:

```
mkdir \\share.central.net\AutoConfig\SiteEast
```

```
Export-CvadAcToFile -SiteName East -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

ウェスト デリバリーコントローラー から:

```
mkdir \\share.central.net\AutoConfig\SiteWest
```

```
Export-CvadAcToFile -SiteName West -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

エクスポートコマンドレットは、`CustomerInfo.yml`フォルダーの場所を使用して`SiteMerging.yml`ファイルを特定します。Eastの場合、`SiteRootFolder`は完全修飾されています。それはそのまま使用されます。Westの場合、`SiteRootFolder`は完全修飾されていません。それは`CustomerInfo.yml`フォルダーの場所と組み合わされて、Westの完全修飾されたフォルダーの場所を取得します。

East Delivery Controller をクラウドにマージするには:

```
Merge-CvadAcToSite –SiteName East -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

West Delivery Controller をクラウドにマージするには:

```
Merge-CvadAcToSite –SiteName West -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

以下は、前の例で使用された `SitePrefixes.yml` ファイルのサンプルです。

```
East:

SiteRootFolder: "\\\\share.central.net\\AutoConfig\\SiteEast"

AdminScopePrefix: "East_"

AdminRolePrefix: "East_"
```

```
  ApplicationAdminPrefix: "East_"

  ApplicationFolderPrefix: "" # Note that a new parent root folder is used
instead

  ApplicationFolderRoot: "East"

  ApplicationGroupPrefix: "East_"

  ApplicationUserPrefix: "East_"

  DeliveryGroupPrefix: "East_"

  GroupPolicyPrefix: "East_"

  HostConnectionPrefix: "East_"

  MachineCatalogPrefix: "East_"

  StoreFrontPrefix: "East_"

  TagPrefix: "East_"

  AdminScopeSuffix: "_east"

  AdminRoleSuffix: "_east"

  ApplicationAdminSuffix: "_east"

  ApplicationFolderSuffix: "_east"

  ApplicationGroupSuffix: "_east"

  ApplicationUserSuffix: "_east"

  DeliveryGroupSuffix: "_east"

  GroupPolicySuffix: "_east"

  HostConnectionSuffix: "_east"

  MachineCatalogSuffix: "_east"
```

```
  StoreFrontSuffix: "_east"

  TagSuffix: "_east"

West:

  SiteRootFolder: "\\\\share.central.net\\AutoConfig\\SiteWest"

  AdminScopePrefix: "Western "

  AdminRolePrefix: "Western "

  ApplicationAdminPrefix: "Western "

  ApplicationFolderPrefix: "" # Note that a new parent root folder is used
instead

  ApplicationFolderRoot: "Western"

  ApplicationGroupPrefix: "Western "

  ApplicationUserPrefix: "Western "

  DeliveryGroupPrefix: "Western "

  GroupPolicyPrefix: "Western "

  HostConnectionPrefix: "Western "

  MachineCatalogPrefix: "Western "

  StoreFrontPrefix: "Western "

  TagPrefix: "Western "

  AdminScopeSuffix: ""

  AdminRoleSuffix: ""

  ApplicationAdminSuffix: ""

  ApplicationFolderSuffix: ""
```

```
ApplicationGroupSuffix: ""

ApplicationUserSuffix: ""

DeliveryGroupSuffix: ""

GroupPolicySuffix: ""

HostConnectionSuffix: ""

MachineCatalogSuffix: ""

StoreFrontSuffix: ""

TagSuffix: ""
```

中央ファイル共有方法が使用されず、インポート、統合、または追加が個々のDelivery Controllerから行われる場合、クラウドに移行される各Delivery Controllerで`SiteMerging.yml`ファイルを作成してレプリケートします。デフォルトの場所は *%HOMEPATH%\Documents\Citrix\AutoConfig* です。正しいサイトプレフィックスを選択するには、`-SiteName`パラメーターを指定する必要があります。

サイトをマージする

Citrix®は、クラウド操作を段階的に実行し、次のクラウド操作を行う前に各結果を完全にレビューすることを推奨しています。たとえば、3つのサイトを単一のクラウドサイトにマージする場合：

1. 適切な`SiteName`値を使用して、最初のサイトをクラウドにマージします。
2. Studioで結果を確認します。
3. 結果が正しくない場合は、問題とその原因を特定し、修正してからマージを再実行します。必要に応じて、クラウドコンポーネントを削除し、選択したコンポーネントとメンバーに`Remove-CvadAcFromSite`を使用して最初からやり直します。結果が正しい場合は、続行します。
4. 最初のマージが正しければ、2番目のサイトを単一のクラウドサイトにマージします。
5. 手順2と3を繰り返します。
6. 2番目のマージが正しければ、3番目のサイトを単一のクラウドサイトにマージします。
7. 手順2と3を繰り返します。

8. ユーザーの視点からリソースを確認し、ビューが目的の状態であることを確認します。

サイトプレフィックスを使用してコンポーネントを削除する

`Remove-CvadAcFromSite` コマンドレットの `-IncludeByName` パラメーターにプレフィックスを使用することで、単一サイトのコンポーネントを選択的に削除できます。次の例では、West Delivery Controller のデリバリーグループが正しくありません。West サイトのみのデリバリーグループを削除するには:

```
Remove-CvadAcFromSite -DeliveryGroups -IncludeByName “Western *”
```

すべてのWestコンポーネントを削除するには、次のコマンドレットを順番に実行します。

1. `Remove-CvadAcFromSite -GroupPolicies -IncludeByName “Western *”`
2. `Remove-CvadAcFromSite -Applications -IncludeByName “Western *”`
3. `Remove-CvadAcFromSite - ApplicationGroups -IncludeByName “Western *”`
4. `Remove-CvadAcFromSite -DeliveryGroups -IncludeByName “Western *”`
5. `Remove-CvadAcFromSite -MachineCatalogs -IncludeByName “Western *”`
6. `Remove-CvadAcFromSite -HostConnections -IncludeByName “Western *”`
7. `Remove-CvadAcFromSite -Tags -IncludeByName “Western *”`

東コンポーネントのグループポリシーを削除するには、次のサフィックスを使用します。

```
Remove-CvadAcFromSite -GroupPolicies -IncludeByName “*_east”
```

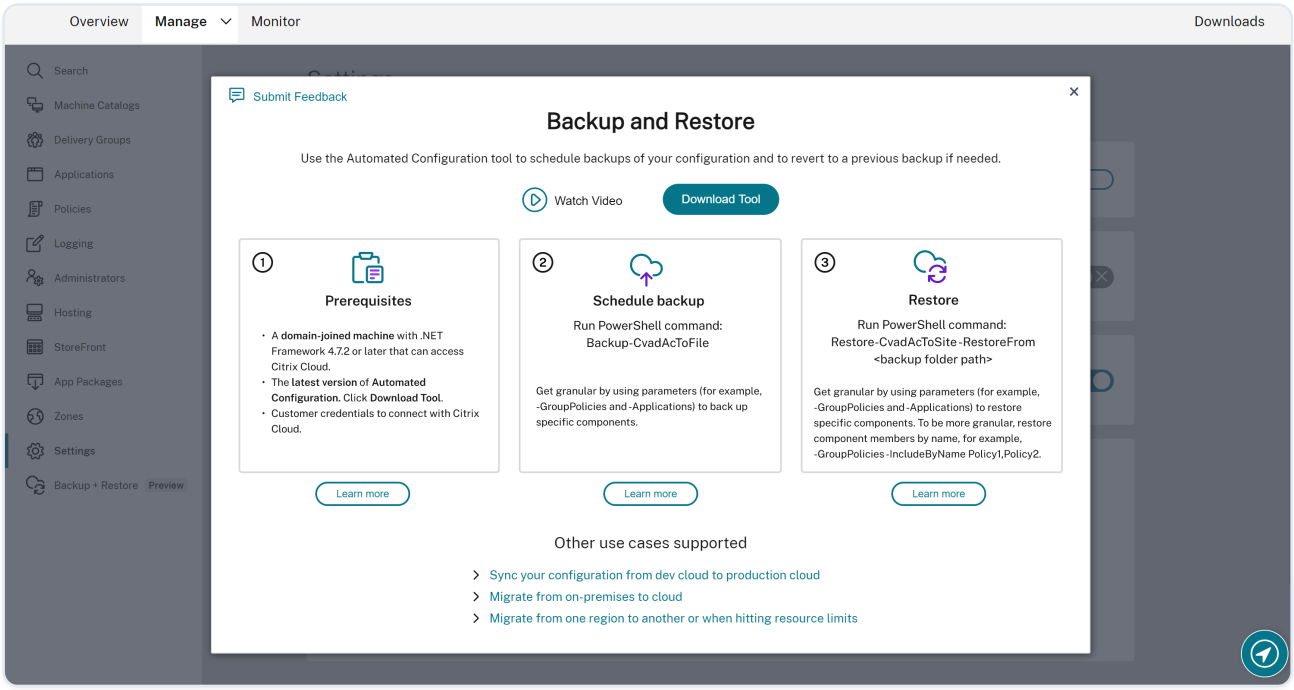
クラウドからクラウドへの移行

自動構成を使用すると、クラウド構成を別のクラウドサイトに移動したり、独自のクラウドサイトを復元したりする作業を自動化できます。

自動構成を使用すると、多くのユースケースを解決できます。

- テストまたはステージング環境から本番環境へのサイトの同期
- 構成のバックアップと復元
- リソース制限への到達
- あるリージョンから別のリージョンへの移行

Citrix Cloud™ のStudioで、自動構成と、それがクラウドからクラウドへの構成の移行にどのように使用できるかについては、ノードを参照してください。



構成を移行するための前提条件

構成をバックアップおよび復元するには、以下が必要です。

- Citrix DaaS™ がプロビジョニングされていること。
- Connector がインストールされたアクティブなリソースの場所。
- Citrix Cloudにアクセスするサイトへの接続が許可され、利用可能である必要があります。詳細については、システムおよび接続要件を参照してください。

> **注:**
>
> MCSは、Automated Configurationを使用してクラウドからバックアップすることはできません。

Citrix DaaS の構成をバックアップする

要件

Citrix DaaS の構成をバックアップする前に、次の操作を実行します。

1. `CustomerInfo.yml` ファイルに、顧客 ID、クライアント ID、および含まれているシークレット キー情報を入力します。顧客 ID、クライアント ID、およびシークレット キーの取得方法の詳細については、「顧客 ID、クライアント ID、およびシークレット キーを生成する」を

参照してください。この情報を `CustomerInfo.yml` ファイルに追加する方法については、「顧客情報ファイルに入力する」を参照してください。

バックアップ コマンドを実行するときは、`CustomerInfo.yml` に、バックアップ元となるソース サイトの顧客の詳細が含まれている必要があります。

復元コマンドを実行するときは、`CustomerInfo.yml` に、構成を復元する宛先サイトの顧客の詳細が含まれている必要があります。

1. `ZoneMapping.yml` ファイルに、クラウド内のリソースの場所をマッピングする情報を入力します。ゾーンのマッピング方法の詳細については、「ゾーン マッピング ファイルに入力する」を参照してください。
2. ホスト接続がある場合は、対応する情報を `CvadAcSecurity.yml` ファイルに入力する必要があります。「ホスト接続のセキュリティ ファイルを更新する」を参照してください。

Citrix DaaS 構成をバックアップする手順

1. Automated Configuration をインストールする。

> **注:**
>
> クラウド間移行の場合、Automated Configuration は、管理者が直接アクセスできるインターネットに接続されたマシンにインストールできます。

2. **Auto Config**アイコンをダブルクリックします。PowerShellウィンドウが表示されます。
3. バックアップを実行するには、次のコマンドを実行します。

```
Backup-CvadAcToFile
```

初めてコマンドレットを実行すると、`.yml` 構成ファイルとログを含むエクスポートフォルダーが作成されます。フォルダーは `%HOMEPATH%\Documents\Citrix\AutoConfig` にあります。

エラーまたは例外が発生した場合は、ログファイルの **Fixups** セクションを参照してください。

Citrix DaaS に構成を復元する

1. **Auto Config**アイコンをダブルクリックします。PowerShellウィンドウが表示されます。
2. 復元を実行するには、次のコマンドを実行します。

```
Restore-CvadAcToSite -RestoreFolder <folder path of the backup files>
```

新しい現在の状態と期待される状態を検証します。

コマンドレットを実行すると、`.yml` 構成ファイルとログを含むエクスポートフォルダーが作成されます。フォルダーは *%HOMEPATH%\Documents\Citrix\AutoConfig* にあります。

エラーまたは例外が発生した場合は、ログファイルの **Fixups** セクションを参照してください。

バックアップおよび復元プロセスは、意図しないクラウドサイト構成の変更や破損から保護します。自動構成は変更が行われるたびにバックアップを作成しますが、このバックアップは変更前のクラウドサイト構成の状態を反映しています。自身を保護するには、クラウドサイト構成を定期的にバックアップし、安全な場所に保存する必要があります。望ましくない変更や破損が発生した場合、バックアップを使用して、きめ細かいレベルまたは完全なサイト構成レベルで変更や破損を修正できます。

詳細な移行

> **重要:**

> コンポーネントの移行順序の詳細については、「コンポーネントの移行順序」を参照してください。

すべてのコンポーネントを復元する

1つのコンポーネントを復元するには、1つ以上のコンポーネントパラメーターを選択します。

復元するには:

- デリバリーグループ全体とマシンカタログコンポーネント
- 完全なクラウドサイト構成

この例に従ってください。

```
Restore-CvadAcToSite   -RestoreFolder   %HOMEPATH%
\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

コンポーネントメンバーを復元する

1つ以上のコンポーネントメンバーを復元するには、`IncludeByName`機能を使用します。`Restore`コマンドレットは、選択した単一のコンポーネントとインクルージョンリストとともに`RestoreFolder`パラメーターで呼び出されます。

バックアップから2つのグループポリシーを復元するには、次の例に従ってください。

```
Restore-CvadAcToSite   -RestoreFolder   %HOMEPATH%
\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss



-GroupPolicies -IncludeByName   Policy1,Policy2



-DeliveryGroups -MachineCatalogs
```

サイトをアクティブ化する

サイトのアクティブ化により、アクティブなサイトを制御し、リソースを管理できます。詳しくは、「」(/ja-jp/citrix-virtual-apps-desktops/current-release/manage-deployment/migrate.html#activate-sites)を参照してください。

クラウド構成をオンプレミスに移行する

この記事では、クラウド構成をバックアップし、オンプレミスサイトに移行する方法について説明します。

構成を移行するための前提条件

- Citrix Virtual Apps and Desktops™ オンプレミス環境（登録済みVDAが1つ以上あること）。
- Citrix Virtual Apps and Desktops™ オンプレミス環境で、以下のいずれかのバージョンで実行されていること:
  - 最新のLong-Term Service Release (LTSR) バージョン - 2402。
  - いずれかのCurrent Releases (CR) バージョン - 2308、2311。
- .Net 4.7.2以降のバージョンがインストールされたドメイン参加済みマシンで、Automated Configuration tool (ACT) コマンドを実行します。

- Citrix PowerShell SDKがインストールされたマシン。PowerShell SDKは、Citrix Delivery Controller™のインストール可能ファイルに含まれています。

> **注:**
>
> - 別のマシンでACTを実行している場合は、そのマシンがドメインに参加しており、Studioに適切なPowerShellスナップインがインストールされている必要があります。インストーラーを入手するには、Citrix Virtual Apps and DesktopsダウンロードWebサイトにアクセスしてください。
> - オンプレミスサイトでは、ACTをDelivery Controllerにインストールすることをお勧めします。ACTはデスクトップアイコンから起動できます。
> - ACTを標準のPowershellウィンドウから使用する場合は、次のコマンドを実行する必要があります: `Import-Module Citrix.AutoConfig.Commands`

> ACTはシステムPowerShellパスの一部ではないため、明示的にインポートする必要があります

主な手順

クラウド構成をオンプレミスに移行するには、以下の手順に従ってください。

1. クラウド構成のバックアップ
2. YMLファイルを変更する
3. オンプレミスに構成をインポートする

クラウド構成のバックアップ

1. **Automated Configuration**をインストールします.
2. **CustomerInfo.yml** ファイルを作成するには、`New-CvadAcCustomerInfoFile` を実行します。詳細については、顧客情報ファイルの入力 を参照してください。
3. クラウド構成のバックアップを作成するには、コマンド`Backup-CvadAcToFile`を実行します。

> **注:**

- 初めてコマンドレットを実行すると、.yml 構成ファイルとログを含むエクスポートフォルダーが作成されます。フォルダーは `%HOMEPATH%\Documents\Citrix\AutoConfig` にあります。
- エラーまたは例外が発生した場合は、ログファイルの**Fixups**セクションを参照してください。
- Backup-CvadToFileは、パラメーター `IncludeByName` または `ExcludeByName` をサポートしていません。

重要:

Citrixでは、すべてのコンポーネントをまとめてバックアップすることをお勧めします。

YMLファイルを変更する

`%HOMEPATH%\Documents\Citrix\AutoConfig` にある `.yml` ファイルを、次の表に示すようにオンプレミスの詳細を含めるように変更します。

YMLファイル	パラメーター	説明	例
CustomerInfo.yml	環境	環境をOnPremに変更します。環境パラメーターの値は大文字と小文字を区別します。	
ZoneMapping.yml	DaaS:CVAD	クラウドのリソースの場所をオンプレミスのゾーンにマッピングします。	old:newゾーンである必要があります
CvadAcSecurity.yml	ハイパーバイザー: 接続タイプ: ‘ ‘ ユーザー名: ‘ ’ パスワード: ‘ ‘	ハイパーバイザーのユーザー名とパスワードを追加します。	ハイパーバイザーがXenServerの場合、 XenServer: ConnectionType: ‘XenServer’ Username: ‘root’ Password: ‘ ‘

オンプレミスに構成をインポートする

1. 要件に基づいて、オンプレミスサイトで次のいずれかのコマンドを実行します。

   a. `Merge-CvadAcToSite` - オンプレミスサイトが稼働しており、クラウド構成をそれにマージしたい場合。

   b. `Import-CvadAcToSite -Environment OnPrem` - オンプレミス構成が利用できず、クラウド構成をインポートして新しいものを作成する場合。

> **重要:**
>
> 競合を避けるため、Citrixでは一度に1つのコンポーネントをインポートすることをお勧めします。

オンプレミス構成をオンプレミスサイトに移行する

この記事では、Automated Configuration Tool (ACT) を使用して、オンプレミス構成をあるオンプレミスサイトから別のオンプレミスサイトに移行する手順について説明します。

要件

- 両方のオンプレミスサイトが同じドメインにドメイン参加している必要があります。
- Citrix Virtual Apps and Desktops™ バージョン 2305 以降を使用してください。

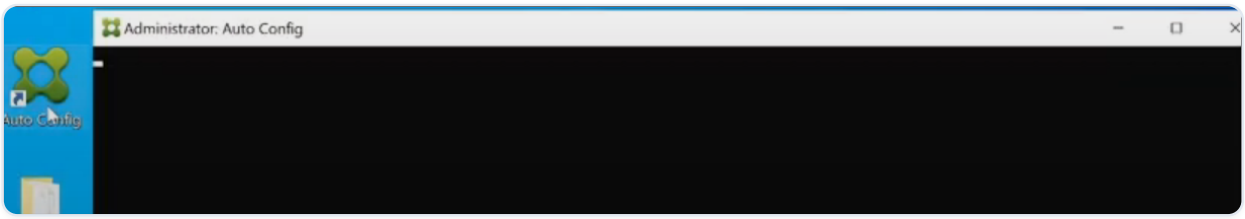
手順

1. Automated Configuration Toolをダウンロードし、システム要件を確認します。Automated Configurationのダウンロードを参照してください。
2. ACT を開き、次のコマンドを使用してオンプレミスサイトをエクスポートします。

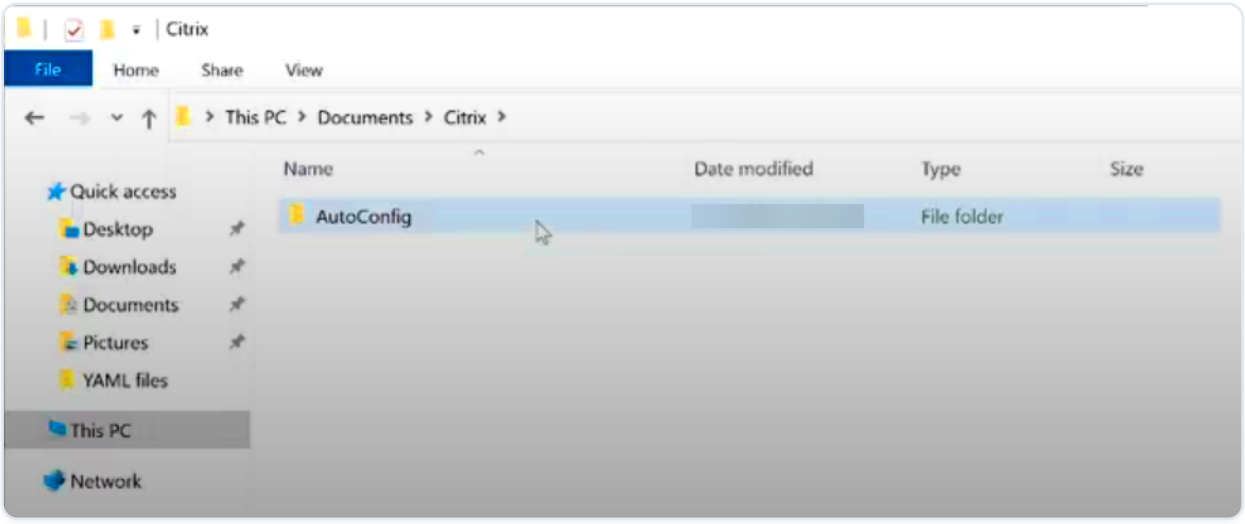
   ```
   Export-CvadAcToFile
   ```

   移行でサポートされているコンポーネントのリストについては、「サポートされている移行オブジェクト」を参照してください。エクスポートの手順については、「オンプレミス構成のエクスポート」を参照してください。親フォルダー `%HOMEPATH%\\Documents\\Citrix\\AutoConfig` には、常に最新のエクスポートからのエクスポートされたファイルが含まれています。

3. ターゲットサイトで ACT を起動します。`%HOMEPATH%\\Documents\\Citrix` に `AutoConfig` フォルダーが作成されていることを確認してください。



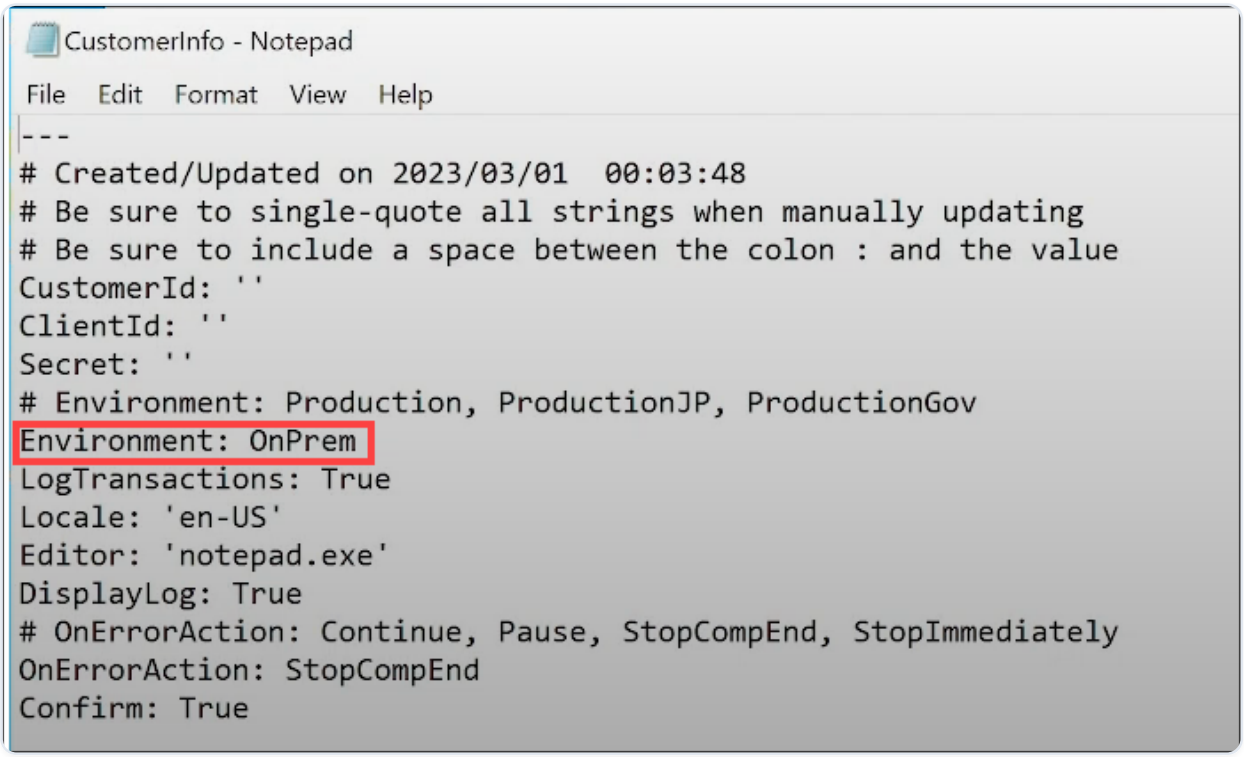
4. ソースサイトの **Export** フォルダーから `.yml` ファイルをターゲットサイトの `%HOMEPATH%\\Documents\\Citrix\\AutoConfig` フォルダーにコピーします。



5. `Set-CvadAcCustomerInfoFile` コマンドを使用して、作業中の環境を指定します。例:

```
Set-CvadAcCustomerInfoFile -Environment OnPrem
```

このコマンドは、環境で **CustomerInfo** ファイルを更新します。



6. 次のコマンドを使用して構成ファイルを移行します。

```
Import-CvadAcToFile
```

`AutoConfig` フォルダー以外のフォルダーからインポートする場合は、次を実行します。

```
Import-CvadAcToFile -Sourcefolder PATH
```

注:

ホスト接続を移行する場合は、各ホストタイプの接続情報で `CvadAcSecurity.yml` ファイルを更新してください。「ホスト接続のセキュリティファイルを更新する」を参照してください。

エラーまたは例外が発生した場合は、ログファイルの「Fixups」セクションを参照してください。

7. Web Studioを使用して、構成がターゲットサイトに移行されていることを確認します。

移行のための自動構成ツールコマンドレット

このページでは、移行ユースケース向けにツールでサポートされているすべてのコマンドレットとパラメータを一覧表示します。

すべてのコマンドレットは、次のいずれかの型のパラメータを受け取ります。

- 文字列
- 文字列のリスト
- ブール値: `$true` または `$false`
- SwitchParameter: パラメータが存在する場合は `$true` を意味し、パラメータが存在しない場合は `$false` を意味します。

注:

SwitchParameter は真偽の選択に推奨される方法ですが、レガシーな問題により、ツールではブール値も引き続き使用されています。

次の表は、すべてのコマンドレットの概要です。各コマンドレットがサポートするパラメータについては、各セクションを参照してください。

カテゴリ	コマンドレット	説明
オンプレミスからクラウドへの移行	`Export-CvadAcToFile`	オンプレミスファイルをYAMLファイルにエクスポートします。
	`Import-CvadAcToSite`	YAMLファイルをクラウドにインポートします。作成、更新、削除の操作をサポートします。
	`Merge-CvadAcToSite`	YAMLファイルをクラウドにインポートします。作成および更新の操作をサポートします。
	`New-CvadAcToSite`	YAMLファイルをクラウドにインポートします。作成およ

カテゴリ	コマンドレット	説明
		び更新の操作をサポートします。
	`Sync-CvadAcToSite`	1つのステップでエクスポートとインポートを行います。
	きめ細かな移行 コンポーネントの場合は、上記のコマンドでパラメーターを使用します。例: `MachineCatalogs`、`Tags`。コンポーネント名の場合は、上記のコマンドでパラメーターを使用します。例: `IncludeByName`、`ExcludeByName`。	コンポーネントまたはコンポーネント名のみを選択的に移行する
クラウドからクラウドへのコマンドレット	`Backup-CvadAcToFile`	クラウドサイトからすべての構成をバックアップします。
	`Restore-CvadAcToSite`	バックアップYAMLファイルをクラウドサイトに復元します。このクラウドサイトは、ソースクラウドサイトと同じでも異なっていてもかまいません。
	`Remove-CvadAcFromSite`	クラウドからコンポーネントメンバーを削除します。
	きめ細かな移行 コンポーネントの場合は、上記のコマンドでパラメーターを使用します。例: `MachineCatalogs`、`Tags`。コンポーネント名の場合は、上記のコマンドでパラメーターを使用します。例: `IncludeByName`、`ExcludeByName`。	コンポーネントまたはコンポーネント名のみを選択的に移行する

カテゴリ	コマンドレット	説明
その他の基本コマンドレット	`Compare-CvadAcToSite`	オンプレミスの.ymlファイルをクラウド構成と比較します。
前提条件関連のコマンドレット	`New-CvadAcCustomerInfoFile`	顧客情報ファイルを作成します。
	`Set-CvadAcCustomerInfoFile`	既存の顧客情報ファイルを更新します。
サポートおよびトラブルシューティングのコマンドレット	`New-CvadAcZipInfoForSupport`	すべてのログファイルと.ymlファイルを単一のzipファイルに圧縮し、サポートのためにCitrix®に送信します。
	`Get-CvadAcStatus`	接続をテストし、すべての前提条件が満たされていることを確認するために使用します。バージョン番号、クラウドとの接続、コネクタの状態など、ツールに関する情報を返します。
	`Test-CvadAcConnectionWithSite`	クラウドサイトとの接続をテストします。
	`Find-CvadAcConnector`	既存のコネクタを特定し、その実行状態を判断します。
	`Get-CvadAcCustomerSites`	すべての顧客サイトのリストを返します。
	`New-CvadAcTemplateToFile`	選択したコンポーネントのテンプレートファイルを作成します。
	`Show-CvadAcDocument`	このドキュメントをデフォルトのブラウザに表示します。
	`Find-CvadAcInFile`	「ファイル内検索」は、ワイルドカードを含む可能性のある1つ以上の名前に一致する

カテゴリ	コマンドレット	説明
		メンバーを探して、コンポーネントのYAMLファイルを検索します。
サイトアクティベーションコマンドレット(#site-activation-cmdlets)	`Set-CvadAcSiteActiveStateOnPrem`	オンプレミスサイトの状態をアクティブまたは非アクティブに設定します。
	`Set-CvadAcSiteActiveStateCloud`	クラウドサイトの状態をアクティブまたは非アクティブに設定します。
複数のオンプレミスサイトをマージするコマンドレット(#merging-multiple-on-premises-sites-cmdlets)	`New-CvadAcSiteMergingInfo`	サイトマージのプレフィックス/サフィックス情報セットを作成します。
	`Set-CvadAcSiteMergingInfo`	既存のサイトマージのプレフィックス/サフィックス情報セットを更新します。
	`Remove-CvadAcSiteMergingInfo`	既存のサイトマージのプレフィックス/サフィックス情報セットを削除します。

パラメーターとその使用方法の詳細については、「きめ細かな移行パラメーター」を参照してください。

基本的なコマンドレット

オンプレミスからクラウドへのコマンドレット

- `Export-CvadAcToFile` - オンプレミスファイルをYAMLファイルにエクスポートします。

  オンプレミス設定から構成をエクスポートします。これは、自動構成のデフォルトのエクスポート操作です。オンプレミスサイトの構成には変更が加えられません。エクスポートされたファイルは、一意の名前が付けられた **Export** サブフォルダー内のディレクトリ *%HOMEPATH%\Documents\Citrix\AutoConfig* に配置されます。フォルダー *%HOMEPATH%\Documents\Citrix\AutoConfig* には、常に最新のエクスポートされたオンプレミスサイト構成が含まれています。

  パラメーター:

名前	説明	必須ですか?	タイプ
コンポーネントによる移行	を参照してください(#migrate-by-components)		SwitchParameters
オブジェクト名によるフィルタリング	「オブジェクト名によるフィルタリング」を参照してください(#filtering-by-object-names)		文字列のリスト
`TargetFolder`	エクスポート先のフォルダーを指定します。		文字列
`Locale`	エクスポート可能な人間が判読できるテキストの言語を指定します。		文字列
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter
`AdminAddress`	エクスポートがDelivery Controllerで実行されていない場合に、Delivery ControllerのDNSまたはIPアドレスを指定します。		文字列
`CheckUserAndMachines`	ユーザーとマシンがActive Directoryに存在するかどうかを確認します。Active Directoryに存在しないユーザーとマシンは、インポートの失敗につながる可能性があります。		`$true` または `$false`

名前	説明	必須ですか?	タイプ
`ZipResults`	バックアップされたYAMLファイルを単一のzipファイルに圧縮します。このファイルは、バックアップされたYAMLファイルと同じフォルダーにあり、フォルダーと同じ名前を持ちます。		SwitchParameter

戻り値:

- Cmdlet の戻り値 を参照してください

データをクラウドにインポートする方法は3つあります。特定のコマンドレットを実行すると、クラウドサイトで次の3つのアクションの組み合わせのいずれかが発生します。

- 追加、更新、および削除
- 追加と更新のみ
- 追加のみ

コマンドレット	追加	更新	削除
インポート	X	X	X
マージ	X	X	
新規	X		

- `Import-CvadAcToSite` - YAMLファイルをクラウドにインポートします。作成、更新、削除操作をサポートします。

  すべてのオンプレミスファイルをクラウドにインポートします。このコマンドは、クラウドの最終状態がオンプレミスの状態と同一であることを保証します。このオプションは、クラウドに存在する変更をすべて削除します。インポートされたサイト構成ファイルは、*%HOMEPATH%\Documents\Citrix\AutoConfig* から取得されます。*注意して使用してください。*

パラメーター:

名前	説明	必須ですか?	タイプ
コンポーネントによる移行	コンポーネントによる移行を参照してください。		SwitchParameters
オブジェクト名によるフィルタリング	オブジェクト名によるフィルタリングを参照してください。		文字列のリスト
クラウドアクセスパラメータ	クラウドアクセスパラメーターを参照してください。		SwitchParameters
`SourceFolder`	*%HOMEPATH%\Documents\Citrix\AutoConfig* の代替ルートフォルダーを識別します。		文字列
`Locale`	エクスポート可能な人間が判読できるテキストの言語を指定します。		文字列
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false`に設定します。		`$true` または `$false`
`Merge`	`$true`に設定すると、コンポーネントはクラウドサイトにのみ追加されます。コンポーネントは削除されません。コン		`$true` または `$false`

名前	説明	必須ですか?	タイプ
	ポーネントを削除するには、`$false`に設定します。		
`AddOnly`	`$true`に設定すると、新しいコンポーネントのみが追加され、既存のコンポーネントは更新または削除されません。更新と削除を許可するには、`$false`に設定します。このパラメーターが`$true`の場合、`Merge`は無視されます。		`$true`または`$false`
`MergePolicies`	ポリシー設定とフィルターをマージします。マージは、インポートされるポリシーがクラウドDDCにすでに存在する場合にのみ行われます。ポリシーをマージした結果、クラウドDDCポリシーには、既存の設定とフィルターに加えて、新しくインポートされる設定とフィルターが含まれることになります。設定とフィルターの競合が発生した場合、インポートされた値が優先されることに注意してください。		SwitchParameter

名前	説明	必須ですか?	タイプ
`OnErrorAction`	を参照してください (/ja-jp/citrix-virtual-apps-desktops/current-release/manage-deployment/auto-config-troubleshoot.html#onerroraction-parameter)。		文字列

戻り値:

- Cmdlet の戻り値 を参照してください

- `Merge-CvadAcToSite` - YAMLファイルをクラウドにインポートします。作成および更新操作をサポートします。

  オンプレミスファイルをクラウドにマージしますが、クラウドまたはオンプレミスサイトのコンポーネントを削除することは*ありません*。これにより、クラウドで既に行われた変更が保持されます。Citrix Cloud に同じ名前のコンポーネントが存在する場合、このコマンドはそのコンポーネントを変更できます。これは、自動構成のデフォルトのインポート操作です。マージされたサイト構成ファイルは、*%HOMEPATH%\Documents\Citrix\AutoConfig* から取得されます。

  パラメーター:

名前	説明	必須ですか?	タイプ
コンポーネントによる移行	コンポーネントによる移行を参照してください。		SwitchParameters
オブジェクト名によるフィルタリング	オブジェクト名によるフィルタリングを参照してください。		文字列のリスト
クラウドアクセスパラメータ	クラウドアクセスパラメーターを参照してください。		SwitchParameters

名前	説明	必須ですか?	タイプ
`SourceFolder`	*%HOMEPATH%\Documents\Citrix\AutoConfig* の代替ルートフォルダーを識別します。		文字列
`Locale`	エクスポート可能な人間が判読できるテキストの言語を指定します。		文字列
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false`に設定します。		`$true` または `$false`
`Merge`	`$true`に設定すると、コンポーネントはクラウドサイトにのみ追加されます。コンポーネントは削除されません。コンポーネントを削除するには、`$false`に設定します。		`$true` または `$false`
`AddOnly`	`$true`に設定すると、新しいコンポーネントのみが追加され、既存のコンポーネントは更新または削除されません。更新と削除を許可するには、`$false`に設定します。このパラメーターが		`$true` または `$false`

名前	説明	必須ですか?	タイプ
	`$true`の場合、`Merge`は無視されます。		
`MergePolicies`	ポリシー設定とフィルターをマージします。マージは、インポートされるポリシーがクラウドDDCにすでに存在する場合にのみ行われます。ポリシーをマージした結果、クラウドDDCポリシーには、既存の設定とフィルターに加えて、新しくインポートされる設定とフィルターが含まれることになります。設定とフィルターの競合が発生した場合、インポートされた値が優先されることに注意してください。		SwitchParameter
`OnErrorAction`	を参照してください(/ja-jp/citrix-virtual-apps-desktops/current-release/manage-deployment/auto-config-troubleshoot.html#onerroraction-parameter)。		文字列

戻り値:

- Cmdlet の戻り値 を参照してください

- `New-CvadAcToSite` - YAMLファイルをクラウドにインポートします。作成および更新操作をサポートします。

  オンプレミスサイト構成をクラウドにインポートしますが、新しいコンポーネントのみを追加します。既存のクラウドサイトコンポーネントは更新も削除もされません。既存のクラウドサイトコンポーネントを変更しない必要がある場合は、このコマンドを使用してください。

  パラメーター:

名前	説明	必須ですか?	タイプ
コンポーネントによる移行	コンポーネントによる移行を参照してください。		SwitchParameters
オブジェクト名によるフィルタリング	オブジェクト名によるフィルタリングを参照してください。		文字列のリスト
クラウドアクセスパラメータ	クラウドアクセスパラメーターを参照してください。		SwitchParameters
`SourceFolder`	*%HOMEPATH%\Documents\Citrix\AutoConfig* の代替ルートフォルダーを識別します。		文字列
`Locale`	エクスポート可能な人間が判読できるテキストの言語を指定します。		文字列
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false`に設定します。		`$true` または `$false`

名前	説明	必須ですか?	タイプ
`OnErrorAction`	を参照してください(/ja-jp/citrix-virtual-apps-desktops/current-release/manage-deployment/auto-config-troubleshoot.html#onerroraction-parameter)。		文字列

戻り値:

- Cmdlet の戻り値 を参照してください

- `Sync-CvadAcToSite` - 1つのステップでエクスポートとインポートを実行します。

  同期は、エクスポートとインポートの両方を1つのステップで実行します。`SourceTargetFolder` パラメーターを使用して、エクスポート/インポート先のフォルダーを指定します。

  パラメーター:

名前	説明	必須ですか?	タイプ
コンポーネントによる移行	を参照してください(#migrate-by-components)		SwitchParameters
オブジェクト名によるフィルタリング	「オブジェクト名によるフィルタリング」を参照してください(#filtering-by-object-names)		文字列のリスト
クラウドアクセスパラメータ	「クラウドアクセスパラメータ」を参照してください(#cloud-accessing-parameters)		SwitchParameters

名前	説明	必須ですか?	タイプ
`SourceTargetFolder`	エクスポート/インポート先のフォルダを指定します。		文字列
`Locale`	エクスポート可能な人間が判読できるテキストの言語を指定します。		文字列
`AdminAddress`	エクスポートがデリバリーコントローラーで実行されていない場合に、デリバリーコントローラーのDNSまたはIPアドレスを指定します。		文字列
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false`に設定します。		`$true` または `$false`
`Merge`	`$true`に設定すると、コンポーネントはクラウドサイトにのみ追加されます。コンポーネントは削除されません。コンポーネントを削除するには、`$false`に設定します。		`$true` または `$false`
`AddOnly`	`$true`に設定すると、新しいコンポーネントのみが追加さ		`$true` または `$false`

名前	説明	必須ですか?	タイプ
	れ、既存のコンポーネントは更新または削除されません。更新と削除を許可するには、`$false`に設定します。このパラメーターが`$true`の場合、`Merge`は無視されます。		
`MergePolicies`	ポリシー設定とフィルターをマージします。マージは、インポートされるポリシーがクラウドDDCにすでに存在する場合にのみ行われます。ポリシーをマージした結果、クラウドDDCポリシーには、既存の設定とフィルターに加えて、新しくインポートされる設定とフィルターが含まれることになります。設定とフィルターの競合が発生した場合、インポートされた値が優先されることに注意してください。		SwitchParameter

戻り値:

- Cmdlet の戻り値 を参照してください

クラウド間コマンドレット

- `Backup-CvadAcToFile` - クラウドサイトからすべての構成をバックアップします。

クラウド構成を .yml ファイルにエクスポートします。このバックアップは、バックアップおよび復元プロセスで失われたコンポーネントを復元するために使用できます。

パラメーター:

名前	説明	必須?	タイプ
コンポーネントによる移行	コンポーネントによる移行を参照してください		SwitchParameters
クラウドアクセスパラメーター	クラウドアクセスパラメーターを参照してください		SwitchParameters
`TargetFolder`	エクスポート先のフォルダーを指定します。		文字列
`Locale`	エクスポート可能な、人間が判読できるテキストの言語を指定します。		文字列
`Quiet`	コンソールへのログ出力を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false`に設定します。		`$true` または `$false`
`ZipResults`	バックアップされたYAMLファイルを単一のzipファイルに圧縮します。このファイルは、バックアップされたYAMLファイルと同じフォルダーにあり、フォ		SwitchParameter

名前	説明	必須?	タイプ
	ルダーと同じ名前です。		

戻り値:

- コマンドレットの戻り値を参照してください

- `Restore-CvadAcToSite` - バックアップされたYAMLファイルをクラウドサイトに復元します。このクラウドサイトは、ソースクラウドサイトと同じでも異なっていてもかまいません。

  クラウドサイトを以前の構成に復元します。インポートされたファイルは、`-RestoreFolder` パラメーターを使用して指定されたフォルダーから取得されます。このパラメーターは、クラウドサイトに復元する.ymlファイルを含むフォルダーを識別します。これは、完全修飾フォルダー指定である必要があります。このコマンドレットは、以前の構成に戻すため、またはクラウドサイトをバックアップおよび復元するために使用できます。このコマンドは、クラウドサイトの追加、削除、更新を行うことができます。

  パラメーター:

名前	説明	必須?	タイプ
コンポーネントによる移行	「コンポーネントによる移行」を参照してください(#migrate-by-components)。		SwitchParameters
オブジェクト名によるフィルタリング	「オブジェクト名によるフィルタリング」を参照してください(#filtering-by-object-names)。		文字列のリスト
クラウドアクセスパラメーター	「クラウドアクセスパラメータ」を参照してください(#cloud-accessing-parameters)。		SwitchParameters

名前	説明	必須?	タイプ
`RestoreFolder`	クラウドサイトに復元する.ymlファイルを含むフォルダを識別します。これは完全修飾されたフォルダ指定である必要があります。		文字列
`Locale`	エクスポート可能な、人間が判読できるテキストの言語を指定します。		文字列
`Quiet`	コンソールへのログ出力を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false`に設定します。		`$true` または `$false`
`Merge`	`$true`に設定すると、クラウドサイトにコンポーネントのみを追加します。コンポーネントは削除されません。コンポーネントを削除するには`$false`に設定します。		`$true` または `$false`
`AddOnly`	`$true`に設定すると、新しいコンポーネントのみを追加し、既存のコンポーネントを更新または削除しません。更新と削除を許可するには`$false`に設定		`$true` または `$false`

名前	説明	必須?	タイプ
	します。このパラメーターが `$true` の場合、 `Merge` は無視されます。		
`MergePolicies`	ポリシー設定とフィルターをマージします。マージは、インポートされるポリシーがクラウドDDCに既に存在する場合にのみ行われます。ポリシーをマージした結果、クラウドDDCポリシーには、既存の設定とフィルターに加えて、インポートされる新しい設定とフィルターが含まれます。設定とフィルターの競合が発生した場合、インポートされた値が優先されることに注意してください。		SwitchParameter
`OnErrorAction`	OnErrorAction parameterを参照してください。		文字列

戻り値:

- コマンドレットの戻り値を参照してください

- `Remove-CvadAcFromSite` – クラウドからコンポーネントメンバーを削除します。

  サイト全体をリセットしたり、コンポーネントからメンバー項目を削除したりできます (たとえば、カタログのリストから1つのマシンカタログを削除する場合など)。これは、

`IncludeByName`パラメーターと組み合わせて使用すると、特定のメンバーを選択的に削除できます。

パラメーター:

名前	説明	必須?	タイプ
コンポーネントによる移行	コンポーネントによる移行を参照してください		SwitchParameters
オブジェクト名によるフィルタリング	オブジェクト名によるフィルタリングを参照してください		文字列のリスト
クラウドアクセスパラメーター	クラウドアクセスパラメーターを参照してください		SwitchParameters
`Quiet`	コンソールへのログ出力を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false`に設定します。		`$true` または `$false`

戻り値:

- コマンドレットの戻り値を参照してください

その他の基本コマンドレット

- `Compare-CvadAcToSite` - オンプレミスの.ymlファイルをクラウド構成と比較し、`Import`、`Merge`、または`Restore`コマンドレットによって行われた変更のレポートを生成します。

パラメーター:

名前	説明	必須?	タイプ
コンポーネントによる移行	コンポーネントによる移行を参照。		SwitchParameters
オブジェクト名によるフィルタリング	オブジェクト名によるフィルタリングを参照。		文字列のリスト
クラウドアクセスパラメータ	クラウドアクセスパラメータを参照。		SwitchParameters
`SourceFolder`	*%HOMEPATH%\Documents\Citrix\AutoConfig* の代替ルートフォルダーを識別します。		文字列
`Locale`	エクスポート可能な人間が判読できるテキストの言語を指定します。		文字列
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false` に設定します。		`$true` または `$false`
`Merge`	`$true` に設定すると、クラウドサイトにコンポーネントのみを追加します。コンポーネントは削除されません。コンポーネントを削除するには、`$false` に設定します。		`$true` または `$false`

名前	説明	必須?	タイプ
`AddOnly`	`$true` に設定すると、新しいコンポーネントのみを追加し、既存のコンポーネントを更新または削除しません。更新と削除を許可するには、`$false` に設定します。このパラメーターが `$true` の場合、`Merge` は無視されます。		`$true` または `$false`
`OnErrorAction`	「OnErrorAction パラメーター」を参照してください(/ja-jp/citrix-virtual-apps-desktops/current-release/manage-deployment/auto-config-troubleshoot.html#onerroraction-parameter)。		文字列

戻り値:

- 「Cmdlet の戻り値」を参照してください(#cmdlet-return-values)

きめ細かい移行パラメーター

コンポーネントによる移行

それらをサポートするコマンドレットで、以下のコンポーネントを指定できます。コンポーネントパラメーターが指定されていない場合、`All` オプションが自動的に選択されます。エラーを避けるため、コンポーネントを以下の順序で移行することをお勧めします。

- `All`
- `Tags`
- `AdminRoles`

- `AdminScopes`
- `HostConnections`
- `MachineCatalogs`
- `StoreFronts`
- `DeliveryGroups`
- `ApplicationGroups`
- `ApplicationFolders`
- `Applications`
- `GroupPolicies`
- `UserZonePreference`

オブジェクト名によるフィルタリング

コンポーネント名による移行

`IncludeByName`および`ExcludeByName`パラメーターを使用すると、名前でコンポーネントメンバーをコマンドレットに含めたり除外したりできます。サポートされているコマンドレットでは、一度に1つのコンポーネント（たとえば、デリバリーグループ）のみを選択できます。コンポーネントメンバーが両方の領域にある場合、除外は他のすべてのパラメーターを上書きし、除外されたコンポーネントとメンバー名を識別するエントリがログ修正リストに作成されます。

`IncludeByName`と`ExcludeByName`は、コンポーネントメンバー名のリストを受け取ります。任意の名前には、1つ以上のワイルドカードを含めることができます。2種類のワイルドカードがサポートされています。メンバー名に特殊文字が含まれている場合、コンポーネントメンバー名のリストは単一引用符で囲む必要があります。

- * 任意の数の文字に一致します
- ？1つの文字に一致します

`IncludeByName`と`ExcludeByName`は、各メンバーが明示的であるかワイルドカードを含むことができるメンバーのリストを含むファイルも受け取ることができます。ファイルの各行には1つのメンバーを含めることができます。メンバー名から先頭と末尾のスペースはトリミングされます。ファイル名の前には@記号を付け、単一引用符で囲む必要があります（@が再解釈されないようにするためのPowerShellの要件）。メンバー名と混在させることに加えて、複数のファイルをリストすることもできます。

名前が`DgSite1`で始まり、`Home2`を含むすべてのデリバリーグループをマージする例は、次のように記述されます。

```
Merge-CvadAcToSite –DeliveryGroups –IncludeByName DgSite1*,*Home2*
```

デリバリーグループ名別

`ByDeliveryGroupName` は、アプリケーションおよびアプリケーショングループのデリバリーグループ名でフィルタリングします。このパラメーターは常に、デリバリーグループの関連付けに基づいて含めるメンバーを識別するインクルージョンリストです。

`ByDeliveryGroupName` は、デリバリーグループ名のリストを受け取ります。任意の名前には、1つ以上のワイルドカードを含めることができます。2種類のワイルドカードがサポートされています。

- * は任意の数の文字に一致します
- ? は単一の文字に一致します

次の例では、`EastDg` で始まるすべてのデリバリーグループ名を参照するすべてのアプリケーションをマージします。

```
Merge-CvadAcToSite –Applications –ByDeliveryGroupName EastDg*
```

無効なものを除外

`ExcludeDisabled` は、無効になっているすべてのアプリケーションおよびアプリケーショングループをインポート操作から除外します。`ExcludeDisabled` の既定値は `false` であり、これはすべてのアプリケーションおよびアプリケーショングループが有効状態に関係なくインポートされることを意味します。

マシン名別

`ByMachineName` は、マシンカタログおよびデリバリーグループのマシン名でフィルタリングします。このパラメーターは常に、マシン名の関連付けに基づいて含めるメンバーを識別するインクルージョンリストです。

`ByMachineName` は、任意の名前が1つ以上のワイルドカードを含むことができるマシン名のリストを受け取ります。2種類のワイルドカードがサポートされています。

- * は任意の数の文字に一致します
- ? は単一の文字に一致します

エクスポートまたはインポート時に `ByMachineName` を使用し、マシン名フィルターによってマシンカタログまたはデリバリーグループにマシンが存在しない場合、そのマシンカタログまたはデリバリーグループはエクスポートまたはインポートから除外されます。

> **注:**

> 任意のインポート型コマンドレットで`ByMachineName`を使用すると、`MergeMachines`が`$true`に設定されます。

マシンのマージ

`MergeMachines`を`$true`に設定すると、インポート操作はマシンをマシンカタログまたはデリバリーグループにのみ追加するように指示します。マシンは削除されないため、増分的な追加操作が可能です。

`MergeMachines`のデフォルトはfalseであり、これはマシンカタログまたはデリバリーグループの.ymlファイルに存在しないマシンは削除されることを意味します。`ByMachineName`が使用されると`MergeMachines`は`$true`に設定されますが、`MergeMachines`をfalseに設定することで上書きできます。

前提条件関連のコマンドレット

- `New-CvadAcCustomerInfoFile` - 顧客情報ファイルを作成します。デフォルトでは、顧客情報ファイルは *%HOMEPATH%\Documents\Citrix\AutoConfig* にあります。

  パラメーター:

名前	説明	必須？	タイプ
`CustomerId`	顧客ID。	x	文字列
`ClientId`	Citrix Cloud で作成された顧客のクライアント ID。このパラメーターを使用する場合は、CustomerId と Secret を指定する必要があります。	条件付き	文字列
`Secret`	Citrix Cloud で作成された顧客のシークレットキー。このパラメーターを使用する場合は、CustomerId と	条件付き	文字列

名前	説明	必須？	タイプ
	ClientId を指定する必要があります。		
`Environment`	Production、ProductionGov、またはProductionJP環境。		列挙
`LogFileName`	ログファイルプレフィックスをCitrixLogから別のものに変更します。		文字列
`AltRootUrl`	Citrixの指示の下でのみ使用してください。		文字列
`StopOnError`	最初のエラーで操作を停止します。		`$true` または `$false`
`TargetFolder`	ルートフォルダとして、*%HOMEPATH%\Documents\Citrix\AutoConfig* の代わりに指定されたフォルダを使用します。		文字列
`Locale`	ツールが実行されているシステムから派生したロケールの代わりに、指定されたロケールを使用します。		文字列
`Editor`	各コマンドレットの完了時にログを表示するために、指定されたエディターを使用します。Notepad.exeがデフォルトのエディ		文字列

名前	説明	必須？	タイプ
	ターです。このパラメーターには、エディターへの完全修飾ファイル指定を含める必要があり、エディターはログファイル指定を唯一のパラメーターとして受け取る必要があります。		
`SecurityCsvFileSpec`	Citrix Identity and Access Managementからダウンロードされた SecurityClient.csv ファイルを指す完全修飾ファイル指定。このパラメーターを使用する場合、CustomerIdを指定する必要があります。		文字列

戻り値:

- コマンドレットの戻り値を参照してください

- `Set-CvadAcCustomerInfoFile` - 既存の顧客情報ファイルを更新します。指定されたコマンドレットパラメーターのみが変更されます。CustomerInfo.ymlファイル内の指定されていないすべてのパラメーター値は変更されません。

  パラメーター:

名前	説明	必須？	タイプ
`CustomerId`	顧客ID。		文字列
`ClientId`	Citrix Cloudで作成された顧客のクライアントID。		文字列

名前	説明	必須？	タイプ
`Secret`	Citrix Cloudで作成されたお客様のシークレットキー。		文字列
`Environment`	Production、ProductionGov、またはProductionJP環境。		列挙
`LogFileName`	ログファイルプレフィックスをCitrixLogから別のものに変更します。		文字列
`StopOnError`	最初のエラーで操作を停止します。		`$true` または `$false`
`TargetFolder`	ルートフォルダとして、*%HOMEPATH%\Documents\Citrix\AutoConfig* の代わりに指定されたフォルダを使用します。		文字列
`Locale`	ツールが実行されているシステムから派生したロケールの代わりに、指定されたロケールを使用します。		文字列
`Editor`	各コマンドレットの完了時にログを表示するために、指定されたエディターを使用します。Notepad.exeがデフォルトのエディターです。このパラメーターには、エ		文字列

名前	説明	必須？	タイプ
	ディターへの完全修飾ファイル指定を含める必要があり、エディターはログファイル指定を唯一のパラメーターとして受け取る必要があります。		
`SecurityCsvFileSpec`	Citrix Identity and Access Managementからダウンロードされた SecurityClient.csv ファイルを指す完全修飾ファイル指定。このパラメーターを使用する場合、CustomerIdを指定する必要があります。		文字列

戻り値:

- コマンドレットの戻り値を参照してください

前提条件関連のパラメーター

クラウドアクセスパラメーターに加えて、前提条件関連のコマンドレットで以下のパラメーターを使用できます。

- `Environment` – ProductionまたはProductionGov環境。
- `LogFileName` – ログファイルプレフィックスをCitrixLogから別のものに変更します。
- `StopOnError` – 最初のエラーで操作を停止します。
- `AlternateRootFolder` – *%HOMEPATH%\Documents\Citrix\AutoConfig* の代わりに、指定されたフォルダーをルートフォルダーとして使用します。
- `Locale` – ツールが実行されているシステムから派生したロケールの代わりに、指定されたロケールを使用します。

- `Editor` – 各コマンドレットの完了時にログを表示するために、指定されたエディターを使用します。Notepad.exe がデフォルトのエディターです。このパラメーターには、エディターへの完全修飾ファイル指定を含める必要があり、エディターはログファイル指定を唯一のパラメーターとして受け取る必要があります。

サポートおよびトラブルシューティングのコマンドレット

- `New-CvadAcZipInfoForSupport` - すべてのログファイルと .yml ファイルを単一のzipファイルに圧縮し、サポートのためにCitrixに送信します。顧客の機密情報 (CustomerInfo.yml および CvadAcSecurity.yml) はzipに含まれません。Icon.yml ファイルもサイズが大きいため除外されます。zipファイルは *%HOMEPATH%\Documents\Citrix\AutoConfig* に配置され、日付とタイムスタンプに基づいて *CvadAcSupport_yyyy_mm_dd_hh_mm_ss.zip* という名前が付けられます。このzipファイルはバックアップとしても機能します。

  パラメーター:

名前	説明	必須?	タイプ
`TargetFolder`	zipファイルを作成して保存するターゲットフォルダーを指定します。		文字列
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter

  戻り値:

  - zipファイル名と場所を含むzipファイルがコマンドプロンプトに表示されます。

- `Get-CvadAcStatus` - 接続をテストし、すべての前提条件が満たされていることを確認するために使用します。ツールに関する情報（バージョン番号、クラウドとの接続、コネクターステータスなど）を返します。

  パラメーター:

名前	説明	必須?	タイプ
クラウドアクセスパラメータ	クラウドアクセスパラメータ を参照してください。		SwitchParameters

名前	説明	必須?	タイプ
`SiteId`	接続先のサイトを識別します。		文字列
`AdminAddress`	これは、管理者のアクセスレベルを確認するために使用されるオンプレミスのDelivery ControllerのDNSまたはIPアドレスです。ツールがDelivery Controllerで実行されていない場合に必要です。		文字列

戻り値:

- 各項目の結果を表示します。

- `Test-CvadAcConnectionWithSite` – クラウドサイトとの接続をテストし、通信接続が機能していることを確認します。このコマンドレットは、クラウドアクセスパラメータまたはCustomerInfo.ymlファイルを使用して、顧客の接続情報を指定します。

  パラメーター:

名前	説明	必須?	タイプ
クラウドアクセスパラメータ	クラウドアクセスパラメータ を参照してください。		SwitchParameters
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter

  戻り値:

  - テスト結果はコマンドラインに表示されます。

- `Find-CvadAcConnector` - 既存のコネクタを特定し、その実行状態を判断します。このコマンドレットは、CustomerInfo.yml ファイルまたは顧客 ID パラメーターからの情報を使用して、顧客のコネクタを特定します。

  パラメーター:

名前	説明	必須?	タイプ
`CustomerInfoFileSpec`	デフォルトの場所と名前を上書きする顧客情報ファイルを指すファイル指定。このパラメーターは、`CustomerId` パラメーターが指定されている場合は無視されます。		文字列
`CustomerId`	顧客のID。このパラメータは、CustomerInfo.yml ファイル内の同じ値を上書きします。		文字列

  戻り値:

  - 結果はコマンドラインに表示されます。

- `Get-CvadAcCustomerSites` - すべての顧客サイトのリストを返します。このコマンドレットは、クラウドアクセスパラメータまたは CustomerInfo.yml ファイルを使用して、顧客の接続情報を指定します。

  パラメーター:

  - クラウドアクセスパラメータ を参照してください。

  戻り値:

  - 見つかった顧客サイトIDのリストを表示します。

- `New-CvadAcTemplateToFile` – 選択したコンポーネントのテンプレートファイルを作成し、手動でインポートファイルを作成できるようにします。

  パラメーター:

名前	説明	必須?	タイプ
コンポーネントによる移行	コンポーネントによる移行を参照		SwitchParameters
`TargetFolder`	エクスポート先のフォルダーを指定します。		文字列

戻り値:

- コマンドレットの戻り値を参照

- `Show-CvadAcDocument` - このドキュメントをデフォルトのブラウザーに表示します。

  パラメーター:

  - なし。

  戻り値:

  - このWebページをデフォルトのWebブラウザーに表示します。

- `Find-CvadAcInFile` - ファイル内検索は、ワイルドカードを含む1つ以上の名前に一致するメンバーを探して、コンポーネントのYAMLファイルを検索します。結果は、見つかったメンバーのレポートです。ファイル内検索は、一度に1つのコンポーネントしか検索できません。ファイル内検索は、現在のフォルダーおよびすべてのサブフォルダー内のすべてのYAMLファイルを検索します。検索するファイルの数を制限するには、`FindSourceFolder`を使用します。

  パラメーター:

名前	説明	必須?	タイプ
コンポーネントによる移行	コンポーネントによる移行を参照してください。注: `-All` の値は無効です。		SwitchParameters
`IncludeByName`	サイトのアクティブ状態をアクティブに設定する際に含めるデリバリーグループ		文字列のリスト

名前	説明	必須?	タイプ
	の名前を指定するリスト。名前に「*」と「?」のワイルドカードがサポートされています。		
`Unique`	一意に見つかったメンバーのみを報告します。		SwitchParameter
`IncludeYaml`	メンバー固有のYAMLを含めます。		SwitchParameter
`FindSourceFolder`	検索を開始するフォルダー。		文字列
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false` に設定します。		SwitchParameter
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter

戻り値:

◦ 指定されたコンポーネントについて、検出されたメンバーを含むレポートを作成します。

サイトアクティベーションコマンドレット

サイトのアクティベーションとこれらのコマンドレットの使用方法の詳細については、「サイトのアクティベーション」を参照してください。

- `Set-CvadAcSiteActiveStateOnPrem` - オンプレミスサイトの状態をアクティブまたは非アクティブに設定します。

  パラメーター:

名前	説明	必須ですか？	タイプ
クラウドアクセスパラメーター	クラウドアクセスパラメーターを参照してください		SwitchParameters
`SiteActive`	存在する場合、オンプレミスサイトをアクティブに設定し、すべてのデリバリーグループからメンテナンスモードを削除します。このパラメーターが存在しない場合、すべてのデリバリーグループにメンテナンスモードが設定されます。		SwitchParameter
`IncludeByName`	サイトのアクティブ状態をアクティブに設定する際に含めるデリバリーグループの名前を指定するリスト。名前に「*」と「?」のワイルドカードがサポートされています。		文字列のリスト
`ExcludeByName`	サイトのアクティブ状態をアクティブに設定する際に除外するデリバリーグループの名前を指定するリスト。名前に「*」と「?」のワイルドカードがサポートされています。		文字列のリスト
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter

名前	説明	必須ですか？	タイプ
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false` に設定します。		`$true or $false`

戻り値:

- Cmdlet の戻り値 を参照してください。

- `Set-CvadAcSiteActiveStateCloud` - クラウドサイトの状態をアクティブまたは非アクティブのいずれかに設定します。

  パラメーター:

名前	説明	必須ですか？	タイプ
クラウドアクセスパラメーター	クラウドアクセスパラメーターを参照してください		SwitchParameters
`SiteActive`	存在する場合、クラウドサイトをアクティブに設定し、すべてのデリバリーグループからメンテナンスモードを削除します。このパラメーターが存在しない場合、すべてのデリバリーグループでメンテナンスモードが設定されます。		SwitchParameter
`IncludeByName`	サイトのアクティブ状態をアクティブに設定する際に含めるデリバリーグループの名前を指定するリスト。名前に「*」		文字列のリスト

名前	説明	必須ですか？	タイプ
	と「?」のワイルドカードがサポートされています。		
`ExcludeByName`	サイトのアクティブ状態をアクティブに設定する際に除外するデリバリーグループの名前を指定するリスト。名前に「*」と「?」のワイルドカードがサポートされています。		文字列のリスト
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false` に設定します。		`$true or $false`

戻り値:

- Cmdlet の戻り値 を参照してください。

複数のオンプレミスサイトをマージするコマンドレット

サイトのマージとこれらのコマンドレットの使用方法の詳細については、複数のサイトを単一のサイトにマージする を参照してください。

- `New-CvadAcSiteMergingInfo` - サイトマージのプレフィックス/サフィックス情報セットを作成します。最初からすべてのプレフィックスまたはサフィックスを知っている必要はありません。これらは `Set-CvadAcSiteMergingInfo` で、または SiteMerging.yml ファイルを手動で編集することで更新できます。 パラメーター:

名前	説明	必須ですか？	タイプ
`SiteName`	特定のサイトのプレフィックス/サフィックスのセットを識別するために使用される名前。実際のサイト名と一致してもよいし、一致しなくてもよい。	x	文字列
サイト統合パラメーター	サイト統合パラメーターを参照してください		SwitchParameters
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter

戻り値:

- なし

- `Set-CvadAcSiteMergingInfo` - 既存のサイト統合プレフィックス/サフィックス情報セットを更新します。

  パラメーター:

名前	説明	必須ですか？	タイプ
`SiteName`	特定のサイトのプレフィックス/サフィックスのセットを識別するために使用される名前。実際のサイト名と一致してもよいし、一致しなくてもよい。	x	文字列
サイト統合パラメーター	サイト統合パラメーターを参照してください		SwitchParameters

名前	説明	必須ですか？	タイプ
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter

戻り値:

- なし

- `Remove-CvadAcSiteMergingInfo` - 既存のサイト統合プレフィックス/サフィックス情報セットを削除します。

  パラメーター:

  - `SiteName` – サイトのプレフィックスとサフィックスのセットを識別します。これは文字列であり、必須です。

  戻り値:

  - なし

サイト統合パラメーター

サイト統合コマンドレットの実行時に、以下のパラメーターを使用できます。リストされているすべてのパラメーターは文字列です。

- `SiteName` – 特定のサイトのプレフィックス/サフィックスのセットを識別するために使用される名前。実際のサイト名と一致してもよいし、一致しなくてもよい。SiteName は必須パラメーターです。
- `AdminScopedPrefix` – 管理者スコープに適用するプレフィックス。
- `ApplicationPrefix` – アプリケーションに適用するプレフィックス。
- `ApplicationFolderPrefix` – アプリケーションフォルダーに適用するプレフィックス。`ApplicationFolderPrefix` は `ApplicationFolderRoot` と組み合わせることができます。
- `ApplicationFolderRoot` – アプリケーションフォルダーの新しいルートフォルダー。これにより、追加のフォルダー階層が作成されます。`ApplicationFolderRoot` は `ApplicationFolderPrefix` と組み合わせることができます。
- `ApplicationGroupPrefix` – アプリケーショングループのプレフィックス。
- `ApplicationUserPrefix` – ユーザーに表示されるアプリケーション名に適用するプレフィックス。

- `ApplicationAdminPrefix` – 管理者に表示されるアプリケーション名に適用するプレフィックス。
- `DeliveryGroupPrefix` – デリバリーグループに適用するプレフィックス。
- `GroupPolicyPrefix` – ポリシー名に適用するプレフィックス。
- `HostConnectionPrefix` – ホスト接続に適用するプレフィックス。
- `MachineCatalogPrefix` – マシンカタログに適用するプレフィックス。
- `StoreFrontPrefix` – StoreFront™ 名に適用するプレフィックス。
- `TagPrefix` – タグに適用するプレフィックス。
- `AdminScopedSuffix` – 管理者スコープに適用するサフィックス。
- `ApplicationSuffix` - アプリケーションに適用するサフィックス。
- `ApplicationFolderSuffix` – アプリケーションフォルダーに適用するサフィックス。`ApplicationFolderSuffix` は `ApplicationFolderRoot` と組み合わせることができます。
- `ApplicationGroupSuffix` – アプリケーショングループのサフィックス。
- `ApplicationUserSuffix` – ユーザーに表示されるアプリケーション名に適用するサフィックス。
- `ApplicationAdminSuffix` – 管理者に表示されるアプリケーション名に適用するサフィックス。
- `DeliveryGroupSuffix` – デリバリーグループに適用するサフィックス。
- `GroupPolicySuffix` – ポリシー名に適用するサフィックス。
- `HostConnectionSuffix` – ホスト接続に適用するサフィックス。
- `MachineCatalogSuffix` – マシンカタログに適用するサフィックス。
- `StoreFrontSuffix` – StoreFront名に適用するサフィックス。
- `TagSuffix` – タグに適用するサフィックス。
- `SiteRootFolder` – エクスポートおよびインポートに使用する完全修飾フォルダー名。ローカルフォルダーまたはファイル共有にすることができます。

汎用パラメーター

クラウドアクセスパラメーター

クラウドにアクセスするすべてのコマンドレットは、次の追加パラメーターをサポートしています。

> **注:**
>
> CustomerId、ClientId、および Secret は、CustomerInfo.yml ファイルに配置するか、次のパラメーターを使用してコマンドレットで指定できます。両方の場所で指定されている場合、コマンドレットパラメーターが優先されます。

- `CustomerId` – Rest API で使用される顧客 ID であり、すべての Rest API にアクセスするために必要です。顧客 ID は Citrix Cloud にあります。
- `ClientId` – Citrix Cloud Identity and Access Management Web サイトで作成された clientID。これは、すべての Rest API の認証に必要なベアラートークンを取得するために必要です。
- `Secret` – Citrix Cloud Identity and Access Management Web サイトで作成された秘密鍵。これは、すべての Rest API の認証に必要なベアラートークンを取得するために必要です。
- `CustomerInfoFileSpec` – デフォルトの場所と名前を上書きするための顧客情報ファイルを指すファイル指定。

移行モードパラメーター

クラウドサイト構成を変更するコマンドレット (`Import` , `Restore` , `Merge` , `New` , および `Sync`) は、さらなる柔軟性を提供するために次の追加パラメーターをサポートしています。

- `CheckMode` – インポート操作を実行しますが、変更は*行いません*。すべての予期される変更は、インポートが完了する前に報告されます。このコマンドを使用して、インポートが実行される前にテストできます。
- `BackupFirst` – クラウド設定を変更する前に、クラウドコンテンツを.ymlファイルにバックアップします。これはデフォルトで有効になっています。
- `Confirm` – trueの場合、クラウドサイト構成に変更を加えることをユーザーに確認するよう促します。 `Remove` コマンドレットは、その破壊的な性質のためプロンプトを表示します。自動スクリプト内で実行する場合など、プロンプトが不要な場合はfalseに設定します。 `Confirm` はデフォルトでtrueです。
- `SecurityFileFolder` – CustomerInfo.ymlファイルを含む完全修飾フォルダーです。これは、ローカルフォルダーまたは認証制御下にある可能性のあるネットワーク共有フォルダーを指す場合があります。ツールは資格情報を要求しません。ツールを実行する前に、制御されたリソースへのアクセスを取得する必要があります。
- `SiteName` – インポート時に使用するサイトマージのプレフィックスとサフィックスのセットを指定します。

- `SiteActive` – インポートされたサイトがアクティブか非アクティブかを指定します。デフォルトでは、このパラメーターは `$false` に設定されており、インポートされたサイトは非アクティブであることを意味します。

ログ表示パラメーター

`Export`、`Import`、`Sync`、`Restore`、`Backup`、`Compare`、および `Remove` コマンドレットは、操作が完了するとログファイルを表示します。`-DisplayLog` パラメーターを `$false` に設定することで、表示を抑制できます。ログファイルの表示には、デフォルトでNotepad.exeが使用されます。CustomerInfo.ymlファイルで別のエディターを指定できます。

`Editor: C:\Program Files\Notepad++\notepad++.exe`

コマンドレットの戻り値

ActionResult

すべてのコマンドレットは次の値を返します。

```
public class ActionResult

{

    public bool                         Overall_Success;

    public Dictionary&lt;string, string>   Individual_Success;

    public object                       CustomResult;

}
```

`Overall_Success` は、選択されたすべてのコンポーネントにおけるコマンドレット全体の成功を示す単一のブール値を返します。trueは成功、falseは失敗を意味します。

`Individual_Success` は、各主要コンポーネントに対して1つまたは3つの値を返します。コンポーネントの結果は、Success、Failure、またはSkippedのいずれかになります。Skippedは、そのコンポーネントがコマンドレットによる実行のために選択されなかったことを示します。

`CustomResult` はコマンドレット固有です。

CustomResult

`Import`、`Merge`、`Restore`、`Sync`、`Compare`、`Compare File`、および `Remove` は、`EvaluationResultData` の単一インスタンスに次のカスタム結果情報を返します。

注:

`Export` および `Template` コマンドレットはカスタム結果を返しません。

```
 public class EvaluationResultData

 {

     public Dictionary&lt;string, Dictionary&lt;string, ActionResultValues
>> EvaluationResults;

     public int                  Added;

     public int                  Updated;

     public int                  Deleted;

     public int                  NoChange;

     public int                  TotalChanged;

     public EvaluationResults     OverallResult;

     public string               CloudBackupFolder;

     public string               SourceBackupFolder;

 }

 Where:

 public enum ActionResultValues

{

     Add,

     Update,

     Delete,
```

```
    Identical,

    DoNothing

}

public enum EvaluationResults

{

    Success,

    Failure,

    Skipped

}
```

`EvaluationResults` は、選択されたコンポーネントごとに 1 つのエントリを持つリストを表示します。キーはコンポーネント名で、値は各コンポーネントメンバーのリストと、そのコンポーネントメンバーに対して実行されたアクションです。アクションは `ActionResultValues` のいずれかの値になります。

`Added`、`Updated`、`Deleted`、および `NoChange` は、追加、更新、削除、またはアクションなしのコンポーネントメンバーの総数をこの順序で示します。

`TotalChanged` は、`Added`、`Updated`、および `Deleted` の合計です。

`OverallResult` は、コマンドレットの結果を示す単一のブール値です。True はすべてのコンポーネントでの完全な成功を示し、False は 1 つ以上のコンポーネントの処理の失敗を示します。

`CloudBackupFolder` は、コマンドレットがクラウド変更アクションを実行する前の、クラウドサイト構成バックアップの完全修飾ファイル指定です。

`SourceBackupFolder` は、コマンドレットの完了後に作成されたソースファイルバックアップの完全修飾ファイル指定です。デフォルトでは、これらのファイルは *%HOMEPATH%\Documents\Citrix\AutoConfig* にあります。

PowerShell ヘルプ

各コマンドレットの PowerShell ヘルプが利用可能です。すべてのパラメーターは、コマンドレットの簡単な説明とともに各コマンドレットに記載されています。任意のコマンドレットのヘルプにアクセスするには、コマンドレットの前に `Get-Help` と入力します。

```
Get-Help Import-CvadAcToSite
```

バックアップと復元のための自動構成ツール コマンドレット

このページでは、Web Studio が使用するバックアップおよび復元 API をトリガーするためにツールがサポートするすべてのコマンドレットとパラメーターを一覧表示します。

バックアップストレージ コマンドレット

Get-BckRstrStorage

このコマンドレットはオンプレミスのみに適用されます。バックアップが保存されるストレージの詳細を取得します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud を参照してください。

パラメーター	説明
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。

Set-BckRstrStorage

このコマンドレットはオンプレミスのみに適用されます。バックアップが保存される新しいストレージを設定します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、

パラメーター	説明
	ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`MaximumBackups`	新しいバックアップが作成されたときに、バックアップクリーンアッププロセスが最も古いバックアップを削除するまで保持される、固定されていないバックアップの最大数。
`MaximumPinnedBackups`	保持される固定されたバックアップの最大数。これらのバックアップはクリーンアッププロセスによって削除されません。
`BlobStorageType`	ストレージのタイプ: `FileStorage` または `CustomerAzureStorage`。
`FileStoragefolder`	`BlobStorageType` `FileStorage` オプションの完全修飾フォルダー指定。
`Info1`	`FileStorage` の場合、オプションの `UserName` `CustomerAzureStorage` の場合、Azure SAS URL
`Info2`	`FileStorage` の場合、オプションの Password
`Info3` および `Info4`	使用されていません

Test-BckRstrStorage コマンドレット

このコマンドレットはオンプレミスのみに適用されます。定義されたストレージが有効であることを確認するためにテストします。

`FileStorage`の場合、テストは、そのフォルダーが存在し、書き込み可能であることを確認します。

`CustomerAzureStorage`の場合、テストは、SAS URLが正しい権限を持ち、現在の日付がURLの開始日と終了日の間にあることを確認します。

有効な場合は`true`を返し、無効な場合は`false`を返します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ：Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。

バックアップコマンドレット

Get-BckRstrBackups

バックアップまたは復元BLOBストレージの場所に保存されているバックアップを列挙します。Citrix Virtual Apps and Desktops™の場合、この場所は管理者がWebStudioを通じて設定します。DaaSの場合、これは既存の顧客Azureストレージです。各バックアップに関する完全な情報については、`Get-BckRstrBackupsWithDetiails`を使用してください。バックアップの詳細は次のとおりです。

- バックアップ名
- 注
- ピン留め済み（trueまたはfalse）
- バックアップの日時
- 履歴UID
- 関連UID (最後の復元履歴レコードのUID)
- 関連日時
- チェックモードで実行された場合に関連付けられる
- 期間（秒）
- 管理者名
- 各コンポーネントと各コンポーネントのメンバー数を列挙した詳細。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。

パラメーター	説明
`ProfileName`	以前のパラメータの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメータ。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメータ。

Get-BckRstrBackupsMembers

選択したバックアップに保存されている単一のコンポーネントのメンバーを列挙します。メンバー名は単純なリストで返されます。

コンポーネントは次のとおりです。

- タグ
- AdminScopes
- AdminRoles
- AdminAdministrators (オンプレミスのみ)
- HostConnections
- アイコン
- AdminFolders
- MachineCatalogs
- StoreFronts
- DeliveryGroups
- ApplicationGroups
- ApplicationFolders
- アプリケーション
- AppVServers
- AppLibPackageDiscovery

- AppVIsolationGroups
- グループポリシー
- ユーザーゾーン設定
- サイトデータ
- ゾーン (オンプレミスのみ)

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud を参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`BackupName`	バックアップの名前。`.zip` 拡張子はオプションです。
`Component`	バックアップに含めるコンポーネント。

New-BckRstrBackup

Delivery Controllerで新しいバックアップアクションを開始します。このアクションは、`New-BckRstrBackup` コマンドレットに対して非同期です。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される、既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud を参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`Notes`	バックアップに関するメモ。
`PollForCompletion`	アクションが完了するまで、Delivery Controllerで実行中のアクションをポーリングするためのパラメーター。`Quite` パラメーターが指定されていない限り、ポーリングは進行状況と完了結果をコンソールにログ記録します。

バックアップをピン留めするコマンドレット

Set-BckRstrPinBackups

Delivery Controllerのバックアップクリーンアッププロセスの一部として削除されないように、バックアップをピン留めします。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`BackupName`	バックアップの名前。`.zip`拡張子はオプションです。

Set-BckRstrUnpinBackups

バックアップのピン留めを解除し、Delivery Controllerのバックアップクリーンアッププロセスで削除できるようにします。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`BackupName`	バックアップの名前。`.zip`拡張子はオプションです。

バックアップ削除コマンドレット

Remove-BckRstrBackup コマンドレット

1つ以上のバックアップを削除します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。

パラメーター	説明
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される、既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`IncludeByName`	復元対象とするコンポーネントメンバーを指定するフィルター。これは、コンマ区切りのフィルター値のリストであり、ワイルドカード文字`*`および`?`を使用できます。

スケジュールされたバックアップコマンドレット

Get-BckRstrSchedules

バックアップスケジュールのリストを取得します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。

パラメーター	説明
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`BackupName`	バックアップの名前。`.zip`拡張子はオプションです。
`Notes`	設定または変更するメモ。

New-BckRstrSchedule

新しいバックアップスケジュールを作成します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。

パラメーター	説明
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	既存のセキュリティプロファイルを識別するためのパラメーターで、以前のパラメーターの代わりに使用されます。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境の種類: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`Name`	スケジュール名。
`Frequency`	頻度の種類: 毎日、毎週、または毎月。
`Day`	頻度が毎日の場合。
`DaysInWeek`	頻度が毎週の場合。
`DayInMonth`	頻度が毎月の場合。
`WeekInMonth`	頻度が毎月の場合。
`StartDate`	形式は`M/d/yy`です
`StartTime`	24時間形式で指定された開始時刻。
`FrequencyFactor`	毎日（値 = 1）または隔日（値 = 2）のように、n回ごとに実行します。
`Description`	スケジュールされたバックアップの説明

パラメーター	説明
`Enabled`	このバックアップスケジュールを有効にするためのパラメーター。有効な場合は`True`、無効な場合は`false`。
`TimeZoneId`	WindowsタイムゾーンID

Set-BckRstrSchedule

既存のバックアップスケジュールを変更します。変更するスケジュールを選択するために、名前またはUidを指定します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される、既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、(https://www.citrix.com/blogs/2016/07/01/introducing-remote-powershell-sdk-v2-for-citrix-cloud/)を参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。

パラメーター	説明
`Name`	スケジュール名。
`Uid`	スケジュール名を変更する場合。
`Frequency`	頻度の種類: 毎日、毎週、または毎月。
`Day`	頻度が毎日の場合。
`DaysInWeek`	頻度が毎週の場合。
`DayInMonth`	頻度が毎月の場合。
`WeekInMonth`	頻度が毎月の場合。
`StartDate`	形式は `M/d/yy` です。
`StartTime`	24時間形式で指定された開始時刻。
`FrequencyFactor`	毎日 (値 = 1) または隔日 (値 = 2) のように、n 回ごとに実行します。
`Description`	スケジュールされたバックアップの説明。
`Enabled`	このバックアップスケジュールを有効にするためのパラメーター。有効な場合は `True`、無効な場合は `false`。
`TimeZoneId`	Windows タイムゾーン ID。

Set-BckRstrScheduleEnabled

既存のバックアップスケジュールを有効にします。有効にするスケジュールを選択するには、名前または Uid を指定します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客 ID。

パラメーター	説明
`CientId`	ベアラートークンを取得するために必要なクライアント ID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud を参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するパラメーター。
`Name`	スケジュール名。
`Uid`	スケジュール名を変更する場合。

Set-BckRstrScheduleDisabled

既存のバックアップスケジュールを無効にします。無効にするスケジュールを選択するには、名前またはUidを指定します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。

パラメーター	説明
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するパラメーター。
`Name`	スケジュール名。
`Uid`	スケジュール名を変更する場合。

バックアップの制限コマンドレット

Set-BckRstrOptions

同一のバックアップを避けるため、スケジュールされたバックアップを1日1回に制限します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。

パラメーター	説明
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`OneScheduledBackupPerDay`	同一のバックアップを避けるため、スケジュールされたバックアップを1日1回に制限するパラメーター。

復元コマンドレット

レストア-バックリストアバックアップス

既存のバックアップから単一コンポーネントのメンバーを復元します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。

パラメーター	説明
`ProfileName`	以前のパラメーターの代わりに使用される、既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`BackupName`	バックアップの名前。`.zip`拡張子はオプションです。
`Component`	バックアップに含めるコンポーネント。
`Notes`	バックアップに関するメモ。
`CheckMode`	復元されるはずのコンポーネントメンバーを識別するためのパラメーターですが、実際の復元は実行しません。
`RestoreType`	復元タイプ: MissingOnly または MissingUpdateExisting
`IncludeByName`	復元対象とするコンポーネントメンバーを指定するためのフィルター。これは、フィルター値のコンマ区切りリストであり、ワイルドカード文字`*`および`?`を含めることができます。

履歴コマンドレット

Get-BckRstrHistory

すべてのアクションの履歴詳細のリストを取得します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production, ProductionGov, ProductionJP, OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。

Get-BckRstrSpecificBackupHistory

特定のバックアップの履歴詳細のリストを取得します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。

パラメーター	説明
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production, ProductionGov, ProductionJP, OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`BackupName`	バックアップの名前。`.zip`拡張子はオプションです。

Set-BckRstrNotes

履歴レコード内のメモを設定または変更します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される、既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイ

パラメーター	説明
	ルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production, ProductionGov, ProductionJP, OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`BackupName`	バックアップの名前。`.zip`拡張子はオプションです。
`Notes`	設定または変更するメモ。

自動構成のトラブルシューティングと追加情報

> **重要:**

> 自動構成でよく発生するエラーメッセージと対応する解決策については、Knowledge Centerの記事CTX277730の*トラブルシューティングFAQ*を参照してください。

自動構成ツールのエラー

自動構成ツールの操作中にエラーが発生する場合があります。この場合、マシンカタログ、デリバリーグループ、グループポリシーなどのコンポーネントの処理中に障害が発生することがあります。`OnErrorAction`と継続パラメーターを使用すると、処理中にエラーを捕捉し、解決して、中断したところから再開できます。

デフォルトの`OnErrorAction`値は`StopCompEnd`です。エラーが発生すると、ツールは現在のコンポーネントの処理を完了します。追加のコンポーネントは処理されず、エラーは下流の依存コンポーネントに引き継がれません。エラーを解決した後、継続パラメーターを適用してcmdletを再実行できます。

OnErrorActionパラメーター

コンポーネントの処理中にツールが検出したエラーへの応答方法を制御するために、移行コマンドで`OnErrorAction`パラメーター値を定義できます。

この表は、パラメーター値とその説明を示しています。

値	説明
`Continue`	すべてのコンポーネントを可能な限り多く処理しようとします。
`Pause`	処理の最後に一時停止し、続行するか停止するかを尋ねます。
`StopCompEnd`	コンポーネントを可能な限り多く処理しようとします。コンポーネントの完了後に停止します。(デフォルト)
`StopImmediately`	エラーが検出されると処理が停止します。

移行cmdlet

次の移行コマンドに`OnErrorAction`パラメーターを適用できます。

- `Compare-CvadAcToSite`
- `Import-CvadAcToSite`
- `Merge-CvadAcToSite`
- `New-CvadAcToSite`
- `Restore-CvadAcToSite`

例: `Merge-CvadAcToSite -OnErrorAction StopImmediately`

再開パラメーター

これらのパラメーターは、操作がエラーのために一時停止または停止した後にツールがどのように再開するかを定義します。

次の `OnErrorAction` パラメーター値のいずれかを含む移行コマンドレットに、再開パラメーターを適用できます。

- `Pause`
- `StopCompEnd`
- `StopImmediately`

この表は、パラメーター値とその説明を示しています。

値	説明
`-AllRemaining`	開始コンポーネントが必要です。処理は開始コンポーネントから始まり、残りのすべてのコンポーネントを処理します。複数のコンポーネントが処理されます。
`-Resume`	`CurrentComponent.txt` からのコンポーネントを開始点として使用します。残りのすべてはtrueに設定されます。複数のコンポーネントが処理されます。
`-Repeat`	`CurrentComponent.txt` からのコンポーネントを開始点として使用します。残りのすべてはfalseに設定されます。1つのコンポーネントのみが処理されます。

最後に処理されたコンポーネントは、AutoConfigフォルダー内の `CurrentComponent.txt` ファイルに保存されます。このファイルの編集は推奨されません。 `-Resume` または `-Repeat` を指定し、 `CurrentComponent.txt` が見つからないか無効な場合、処理は停止し、コンポーネントを選択するように求められます。

CustomerInfo.ymlファイルでのOnErrorActionの設定

`CustomerInfo.yml` ファイルで `OnErrorAction` の値を設定することもできます。次のコマンドレットを使用して値を設定します。

- 新しいファイルの場合: `New-CvadAcCustomerInfoFile -OnErrorAction Continue | Pause | StopCompEnd | StopImmediately`
- 既存のファイルの場合: `Set-CvadAcCustomerInfoFile -OnErrorAction Continue | Pause | StopCompEnd | StopImmediately`

ログ

いずれかのコマンドレットを実行すると、ログファイルが作成され、メインの履歴ログファイルにエントリが追加されます。すべての操作ログファイルはバックアップフォルダーに配置されます。すべてのログファイル名は `CitrixLog` で始まり、その後に自動構成操作とコマンドレット実行の日付とタイムスタンプが表示されます。ログは自動削除されません。

メインの履歴ログは `*%HOMEPATH%\Documents\Citrix\AutoConfig*` にある **History.Log** というファイルにあります。各コマンドレットの実行により、実行の日付、操作、結果、バックアップ、およびログファイルの場所を含むメインログエントリが作成されます。

また、`New-CvadAcZipInfoForSupport` コマンドレットを使用して、サポートのためにCitrixに送信するログを収集することもできます。このコマンドレットは、すべてのログファイルと.ymlファイルを1つのzipファイルに圧縮します。顧客の機密情報 (CustomerInfo.ymlおよびCvadAcSecurity.yml) はzipに含まれません。Icon.ymlファイルもサイズが大きいため除外されます。zipファイルは *%HOMEPATH%\Documents\Citrix\AutoConfig* に配置され、日付とタイムスタンプに基づいて *CvadAcSupport_yyyy_mm_dd_hh_mm_ss.zip* という名前が付けられます。このzipファイルはバックアップとしても機能します。

各ログファイルには以下が含まれます。

- 操作の名前と、チェックモードが有効になっているかどうか
- 開始日時と終了日時
- 各コンポーネントのアクションと成功/失敗の通知に関する複数のエントリ
- 実行されたアクションの概要（作成されたオブジェクトのさまざまな数を含む）
- 該当する場合の推奨される修正
- 該当する場合のバックアップフォルダーの場所
- メインログの場所
- 期間

診断ファイル

診断ファイルは、問題の特定と解決に役立ちます。操作が実行されると、次のファイルが作成されます。これらは、*%HOMEPATH%\Documents\Citrix\AutoConfig* の下にあるアクション固有のサブフォルダーにあります。問題解決のサポート情報を提供する際には、これらのファイルを含めてください。

エクスポート

`PoshSdk_yyyy_mm_dd_hh_mm_ss.ps1`

このファイルは、サイト構成をファイルにエクスポートするために行われたすべてのBroker PowerShell SDK呼び出しをカウントします。

インポート、マージ、復元、同期、バックアップ、比較

`Transaction_yyyy_mm_dd_hh_mm_ss.txt`

このファイルは、各Rest API呼び出しと関連情報を記録します。

`RestApiContent_yyyy_mm_dd_hh_mm_ss.txt`

このファイルには、すべての `Add`、`Update`、および `Delete` Rest APIコンテンツが含まれています。

依存関係に起因する問題

インポートとマージは、依存関係の欠落が原因で失敗する可能性があります。一般的な問題は次のとおりです。

1. グループポリシーにデリバリーグループフィルターがありません。通常の原因は、インポートされていないデリバリーグループです。
2. アプリケーションのインポートまたはマージが失敗します。通常の原因は、インポートされていないデリバリーグループまたはアプリケーショングループです。
3. アプリケーショングループにRestrictToTagがありません。通常の原因は、インポートされていないタグです。
4. ホスト接続が失敗します。通常の原因は、CvadAcSecurity.ymlファイルにセキュリティ情報がないことです。
5. マシンカタログが失敗します。通常の原因は、インポートされなかったホスト接続です。
6. マシンカタログとデリバリーグループからマシンが欠落しています。通常の原因は、Active Directoryで見つからなかったマシンです。
7. デリバリーグループからユーザーが欠落しています。通常の原因は、Active Directoryで見つからなかったユーザーです。

推奨事項

- 自動構成の複数のインスタンスを同時に実行しないでください。複数のインスタンスを同時に実行すると、クラウドサイトで予測できない結果が生じます。この問題が発生した場合は、自動構成の1つのインスタンスを再実行して、サイトを予期される状態に戻してください。
- 自動構成の実行中にStudioで作業したり、データを変更したりしないでください。
- クラウドサイトが期待どおりであることを確認するために、Studioでマージ、インポート、または復元の結果を常に視覚的に検証してください。

フォルダー

デフォルトのフォルダーのルート場所

すべての自動構成ツール操作は、ルートフォルダーまたはその中のサブフォルダーで行われます。ルートフォルダーは、*%HOMEPATH%\Documents\Citrix\AutoConfig*にあります。

エクスポート

すべてのエクスポートされたファイルは、使いやすさとエクスポート履歴を提供するために、2つのフォルダーの場所に配置されます。エクスポートは常にルートフォルダーに配置されます。コピーは、エクスポートの日時とともに**Export**という名前のサブフォルダーに配置されます。

ルートフォルダーには常に、最新のエクスポートされたオンプレミスサイト構成が含まれています。各**Export**サブフォルダーには、指定された日時に行われたエクスポートが含まれており、エクスポートの履歴が保持されます。任意の**Export**サブフォルダーを使用して、クラウドサイトを構成できます。自動構成は、既存のエクスポートサブフォルダーを削除または変更しません。

インポート/マージ/同期/比較

`Import`、`Merge`、および`Compare`操作は、常にルートフォルダーにあるファイルから取得されます。各操作によりサブフォルダーが作成され、ルートフォルダー内のファイルがそこにコピーされ、クラウドサイトの変更元ファイルの履歴が提供されます。

復元

`Restore`操作は、既存のサブフォルダーを使用してクラウドサイトを構成します。ソースフォルダーは、必須の`-RestoreFolder`パラメーターで指定されます。他のコマンドとは異なり、`Restore`操作は既存のサブフォルダーを使用するため、新しいサブフォルダーは作成されません。復元フォルダーはルートフォルダーにすることができますが、それでも`-RestoreFolder`パラメーターで指定する必要があります。

バックアップ

自動構成は、クラウドサイト構成を初期化、更新、およびバックアップします。長期間使用すると、クラウドサイトでさまざまな構成が変更される可能性があります。長期的な使用を容易にし、履歴の変更を保持するために、自動構成は保存スキームを使用してこの変更履歴を保存し、以前の状態を復元する方法を提供します。

クラウドサイト構成のバックアップは、常にバックアップの日時とともに**Backup**という名前のサブフォルダーに作成されます。自動構成は、既存のエクスポートサブフォルダーを削除または変更しません。

バックアップを使用して、特定のコンポーネントまたは構成全体を復元できます。デリバリーグループとマシンカタログコンポーネント全体を復元するには、次のコマンドレットを使用します。

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\AutoConfig\Backup_yyyy_mm_dd_hh_mm_ss -DeliveryGroups -MachineCatalogs
```

> **注:**
>
> 前述のコマンドレットのバックアップファイル情報は、独自のバックアップに基づいています。

> クラウドサイト構成全体を復元するには、次のコマンドレットを使用します。

`Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\AutoConfig\Backup_yyyy_mm_dd_hh_mm_ss`

> **注:**
>
> 前述のコマンドレットのバックアップファイル情報は、独自のバックアップに基づいています。

デフォルトのルートフォルダーの変更

`Export`、`Import`、`Merge`、`Sync`、および`Compare`操作は、`-AlternateFolder`パラメーターを使用してデフォルトのルートフォルダーを変更できます。操作ごとのサブフォルダーの作成と管理は、前述のとおりです。

サブフォルダーにコピーされたファイル

以下のファイルを除き、拡張子が「.yml」のすべてのファイルは操作サブフォルダーにコピーされます。

- CustomerInfo.yml
- ZoneMapping.yml
- CvadAcSecurity.yml

自動フェイルセーフクラウドサイトバックアップ

現在のクラウドサイト構成のバックアップは、構成を変更する操作を実行する前に作成されます。これには、`Import`、`Merge`、`Sync`、および`Restore`パラメーターが含まれます。バックアップは常に、運用サブフォルダーの下のサブフォルダーに保存されます。

`Restore`の場合、バックアップフォルダーは`-RestoreFolder`パラメーターで指定されたフォルダーのサブフォルダーです。

自動化

自動構成ツールコマンドレットは、プロンプトとコマンドレット完了時のログ結果の表示を抑制することで、管理者による介入なしに自動化スクリプトで実行できます。CustomerInfo.ymlファイルを使用して、同じことを行うようにパラメーターを設定することもできます。

プロンプトの表示を抑制するには、クラウド変更コマンドレットに次のパラメーターを追加します。

```
-Confirm $false
```

コマンドレットの完了時にログの表示を抑制するには、コマンドレットに次のパラメーターを追加します。

```
-DisplayLog $false
```

PowerShellコマンドウィンドウへのログ記録を抑制するには、コマンドレットに次のパラメーターを追加します。

```
-Quiet
```

別の方法として、次のパラメーターをCustomerInfo.ymlファイルに配置できます。

```
Confirm: False
```

```
DisplayLog: False
```

Delivery Controller™以外のPCからのエクスポート

自動構成ツールは、複数のCitrix PowerShell SDKを使用して、オンプレミスサイト構成をファイルにエクスポートします。これらのSDKはDelivery Controllerに自動的にインストールされるため、追加の操作なしでツールをDelivery Controllerで実行できます。Delivery Controller以外のマシンで実行する場合は、ツールに必要なCitrix PowerShell SDKのセットをインストールする必要があります。このSDKセットはCitrix Studioの一部であり、Citrix Virtual Apps and Desktops™インストールメディアからインストールできます。

> **注:**
>
> 自動構成はCloud Connectorでは実行できません。

Citrix Cloud™ GovernmentおよびJapan Control Planeへの移行

Citrix Cloud GovernmentおよびJapan Control Plane環境では、認証およびアクセストークンの割り当てに異なるアクセスポイントを使用します。この固有の要件は、クラウドにアクセスするすべての自動構成ツールに適用されます。これらの環境で自動構成を使用するには、次の手順を実行します。

1. *%HOMEPATH%\Documents\Citrix\AutoConfig*フォルダーで、CustomerInfo.ymlを編集します。
2. 接続したい環境に応じて、CustomerInfo.yml に以下のいずれかの行を追加します (既に存在する場合は変更します)。

   ```
   Environment: 'ProductionGov'
   ```

   または

   ```
   Environment: 'ProductionJP'
   ```

これらの環境で自動構成を使用できるようになりました。

Citrix Cloud のデータ収集

Citrix Cloud が収集する情報については、「Citrix Cloud Services Customer Content and Log Handling」を参照してください。

その他のリソース

ディスカッションフォーラム

Citrix Discussion forum for Automated Configuration にアクセスしてください。

ビデオ

YouTube で Citrix Virtual Apps and Desktops の自動構成ツールの内部構造 をご覧ください。

トレーニング

クラウドラーニングセンターには、この記事で説明されているタスクを含む、サービス展開を構築するためのステップバイステップのビデオガイドがあります。「Migrating Citrix Virtual Apps and Desktops to Citrix Cloud Learning Path」を参照してください。

オートスケール™

> **注:**

> この機能はWeb Studioでのみ利用可能です。

> Autoscaleは、マシンをプロアクティブに電力管理するための、一貫性のある高性能なソリューションを提供する機能です。コストとユーザーエクスペリエンスのバランスを取ることを目的としています。

Autoscaleは、デリバリーグループ内の登録されているすべてのシングルセッションおよびマルチセッションOSマシンのプロアクティブな電源管理を可能にします。

Autoscaleの機能は次のとおりです。

- スケジュールベースおよび負荷ベースの設定(/ja-jp/citrix-virtual-apps-desktops/current-release/manage-deployment/autoscale/schedule-based-and-load-based-settings.html)
- 動的セッションタイムアウト(/ja-jp/citrix-virtual-apps-desktops/current-release/manage-deployment/autoscale/dynamic-session-timeout.html)
- Autoscaleタグ付きマシン（クラウドバースト）(/ja-jp/citrix-virtual-apps-desktops/current-release/manage-deployment/autoscale/autoscale-tagged-machines.html)
- ユーザーログオフ通知(/ja-jp/citrix-virtual-apps-desktops/current-release/manage-deployment/autoscale/force-user-logoff.html)

一般的なユースケース

以下は、AutoScaleが一般的に使用されるシナリオです。

- 予想されるワークロードを処理するためのスケジュールベースのマシンの電源オン

  Autoscaleを使用すると、管理者は電源オン容量を30分単位で変動させることができ、異なる日に異なるスケジュールを設定できます。ボラティリティの高いワークロードが予想される場合は、ユーザーがマシンの電源がオンになるのを待つ必要がないように、容量バッファを設定することをお勧めします。

- クラウドバーストのユースケース

  Autoscaleは、デリバリーグループ内のマシンの一部のみを電源管理する柔軟性を提供します。これを実現するには、1つ以上のマシンにタグを適用し、その後、Autoscaleを構成してタグ付きマシンのみを電源管理します。

  この機能は、クラウドベースのリソースが追加の需要（つまり、バーストワークロード）に対応する前に、オンプレミスリソース（または予約済みのパブリッククラウドインスタンス）を使用してワークロードを処理したいクラウドバーストのユースケースで役立ちます。

- ゆっくりと増加するユーザーまたは季節的なユーザー

  組織がユーザーをゆっくりとオンボーディングしており、事前にすべての容量をプロビジョニングしたくない場合、動的プロビジョニング機能が役立ちます。この機能は、デリバリーグループの負荷を常に評価し、現在の負荷状況に基づいてデリバリーグループ内のマシンの数を動的にスケールアップまたはスケールダウンします。管理者は、マシンを作成するためにデリバリーグループの負荷のハイウォーターマークとローウォーターマークを定義する必要があります。管理者は、プロビジョニングするマシンの最大数と、これらのマシンに適用するタグをオプションで定義できます。

サポートされているVDAホスティングプラットフォーム

Autoscaleは、Citrix Virtual Apps and Desktopsがサポートするすべてのプラットフォームをサポートしています。これには、XenServer、Amazon Web Services、Google Cloud Platform、Microsoft Azure Resource Manager、VMware vSphereなど、さまざまなインフラストラクチャプラットフォームが含まれます。サポートされているプラットフォームの完全なリストについては、Citrix Virtual Apps and Desktopsのシステム要件を参照してください。

> **注:**
>
> パブリッククラウドホスト接続をデプロイに追加する場合、Hybrid Rights Licenseが必要です。Hybrid Rights Licenseの詳細については、Transition and Trade-Up (TTU) with Hybrid Rightsを参照してください。ライセンスの追加については、サイトの作成を参照してください。

サポートされているワークロード

Autoscaleは、マルチセッションOSとシングルセッションOSの両方のデリバリーグループをサポートしています。注意すべきユーザーインターフェイスは3つあります。

- マルチセッションOSデリバリーグループ（旧RDSデリバリーグループ）用のAutoscaleユーザーインターフェイス
- シングルセッションOSランダム（プール型）デリバリーグループ（旧プール型VDIデリバリーグループ）用のAutoscaleユーザーインターフェイス
- シングルセッションOS静的デリバリーグループ（旧静的VDIデリバリーグループ）用のAutoscaleユーザーインターフェイス

さまざまなデリバリーグループのユーザーインターフェイスの詳細については、Autoscaleユーザーインターフェイスを参照してください。

利点

Autoscale機能には、次の利点があります。

- デリバリーグループ内のマシンを電源管理するための、単一で一貫したメカニズムを提供します。
- 負荷ベースまたはスケジュールベースの電源管理、あるいはその両方の組み合わせでマシンに電力を供給することにより、可用性を確保し、コストを管理します。
- コスト削減やキャパシティ使用率などのメトリックを監視し、通知を有効にするには、Directorを使用します。

2分間のビデオを見る

次のビデオでは、Autoscaleの簡単なツアーを提供します。

<iframe src="https://www.youtube.com/embed/5yxERrFZQ68" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>

Autoscale™ の使用を開始する

Autoscale は、構成されたスケジュールまたは負荷の要求に基づいてデリバリーグループをプロアクティブにスケーリングするための、一貫性のある高性能な電源管理ソリューションを提供する機能です。

Autoscale は、すべての種類のデリバリーグループに適用されます。

- シングルセッション静的OS
- シングルセッションランダムOS
- マルチセッションランダムOS

この記事では、Autoscale に関連する基本的な概念について説明し、デリバリーグループで Autoscale を有効にして構成する方法に関するガイダンスを提供します。

基本的な概念

開始する前に、Autoscale の次の基本的な概念について学習してください。

- 容量とマシンの登録
- 複数のマシンカタログにわたるスケーリング

- マシンのプロビジョニングとセッションの需要
- インスタンスサイズの考慮事項
- スケジュール
- ピーク時とオフピーク時
- シャットダウン遅延
- プールサイズ
- 容量バッファ
- 負荷インデックス
- Autoscaleとメンテナンスモード
- マシンコスト
- デリバリーグループのスケールアップ
- デリバリーグループのスケールダウン
- ドレイン状態

容量とマシンの登録

Autoscaleは、容量を決定する際に、サイトに登録されているマシンのみを含めます。登録されていない電源オンのマシンはセッション要求を受け入れることができません。その結果、それらはデリバリーグループの全体的な容量には含まれません。

複数のマシンカタログにわたるスケール

一部のサイトでは、複数のマシンカタログが単一のデリバリーグループに関連付けられている場合があります。Autoscaleは、スケジュールまたはセッションの需要要件を満たすために、各カタログからマシンをランダムに電源オンにします。

たとえば、あるデリバリーグループには2つのマシンカタログがあります。カタログAには3台のマシンが電源オンになっており、カタログBには1台のマシンが電源オンになっています。Autoscaleが追加のマシンを電源オンにする必要がある場合、カタログAまたはカタログBのいずれかのマシンを電源オンにする可能性があります。

マシンのプロビジョニングとセッションの需要

デリバリーグループに関連付けられているマシンカタログには、需要の増減に応じて電源をオン/オフするのに十分なマシンが必要です。セッション需要がデリバリーグループ内の登録済みマシンの総数を超えた場合、Autoscaleはすべての登録済みマシンの電源がオンになっていることを保証します。ただし、**Autoscaleは追加のマシンをプロビジョニングしません。**

注:

デリバリーグループに63台のマシンがあり、営業時間外に10%のバッファ容量が設定されている場合、Autoscaleの計算に従って、営業時間外には6.3台のマシンがオンになっている必要があります。小数値を処理するためのルールは次のとおりです。

- 最も近い値に丸める：たとえば、値が6.4の場合、6台のマシンがオンになります。値が6.7の場合、7台のマシンがオンになります。
- 1未満のゼロ以外の値はすべて1に丸める：たとえば、値が0.2または0.9の場合、1台のマシンがオンになります。

インスタンスサイズの考慮事項

パブリッククラウドでインスタンスを適切にサイジングすると、コストを最適化できます。ワークロードのパフォーマンスと容量要件に合致する限り、より小さなインスタンスをプロビジョニングすることをお勧めします。

小さいインスタンスは、大きいインスタンスよりも少ないユーザーセッションをホストします。そのため、最後のユーザーセッションがログオフされるまでの時間が短いため、Autoscaleはマシンをより速くドレイン状態にします。結果として、Autoscaleは小さいインスタンスの電源をより早くオフにし、コストを削減します。

スケジュール

Autoscaleは、設定したスケジュールに基づいて、デリバリーグループ内のマシンの電源をオン/オフします。

スケジュールには、各タイムスロットのアクティブなマシンの数と、ピーク時およびオフピーク時が定義されています。

スケジュールの設定は、デリバリーグループの種類によって異なります。詳細については、以下を参照してください。

- マルチセッションOSデリバリーグループ
- シングルセッションOSランダムデリバリーグループ
- シングルセッションOS静的デリバリーグループ

ピーク時とオフピーク時

ピーク時とオフピーク時は、1日の特定の期間にどの容量バッファ値を使用するかを示すために使用されます。ピーク時間を定義し、残りの未定義の時間をオフピーク時間として残すことができます。

電源オフ遅延

電源オフ遅延とは、Autoscaleがマシンを電源オフにする前に、マシンが電源オンになってから経過しなければならない最小分数です。これにより、セッション需要が不安定なときにマシンが頻繁にオン/オフを繰り返すのを防ぎます。デフォルトでは、電源オフ遅延は30分です。0〜60分の範囲で設定できます。

プールサイズ

プールサイズとは、1日の特定の期間に電源オンの状態を維持する必要があるマシンの数です。

容量バッファ

容量バッファは、動的な負荷増加に対応するために、現在の需要に予備容量を追加するために使用されます。注意すべき2つのシナリオがあります。

- マルチセッションOSデリバリーグループの場合、容量バッファは、ロードインデックスの観点から、デリバリーグループの総容量のパーセンテージとして定義されます。
- シングルセッションOSデリバリーグループの場合、容量バッファは、デリバリーグループ内のマシンの総数のパーセンテージとして定義されます。

容量バッファはローリングバッファであり、構成されたプールサイズに加えて計算および適用されるのではなく、現在の使用状況に基づいて計算および適用されます。

たとえば、10台のマシンを持つデリバリーグループがあり、現在の期間のプールサイズが1台のマシンで、容量バッファが10%であるとします。スケジュールで定義された1台の電源オンのマシンが、10%の容量バッファが満たされなくなるまでロードされたときに、追加のマシンが電源オンになります。2台目のマシンの電源をオンにした後で負荷が減少し、10%の容量バッファを満たすのに十分すぎるほどの空き負荷容量がある場合、Autoscaleは1台のマシンの電源オフを準備します。

ロードインデックス

> **重要:**
>
> ロードインデックスは、マルチセッションデリバリーグループにのみ適用されます。

> ロードインデックスメトリックは、マシンがユーザーログオン要求を受信する可能性を決定します。これは、同時ログオン、セッション、CPU、ディスク、メモリの使用量に対して構成された**Citrix Load Management policy**設定を使用して計算されます。

ロードインデックスは0から10,000の範囲です。デフォルトでは、マシンが250セッションをホストしている場合、完全にロードされていると見なされます。

- 「0」はアンロードされたマシンを示します。ロードインデックス値が0のマシンは、ベースライン負荷状態です。
- 「10,000」は、これ以上セッションを実行できない完全にロードされたマシンを示します。

Autoscaleとメンテナンスモード

メンテナンスモードのマシンは、その可用性ステータスに関係なく、全体のプールサイズの計算の一部として考慮されます。したがって、プール内のすべてのマシンがメンテナンスモードになる可能性があります。ただし、これらのマシンは容量バッファの計算から除外され、即座に利用可能であることが保証されます。ユーザー接続のために特定の割合のマシンがアクセス可能であることを保証するには、プールサイズとバッファ値をそれに応じて調整してください。

マシンコスト

1時間あたりのマシンインスタンスコストは、使用されているコンピューティング容量の1時間あたりのコスト（米ドル）です。この設定は、Autoscale設定によるコスト削減を計算するために使用されます。節約額を表示するには、 **> >** に移動します。

デリバリーグループのスケールアップ

Autoscaleは、Autoscaleが有効なデリバリーグループで、次の場合に追加のマシンの電源をオンにします。

1. デリバリーグループのAutoscaleスケジュールが、現在の期間により多くのマシンの電源をオンにする必要があることを示している場合。
2. デリバリーグループの現在の負荷が容量バッファを超えている場合。

マシンの電源をオンにする条件：

1. メンテナンスモードではないこと。
2. ハイパーバイザーはメンテナンスモードではありません。
3. 電源がオフで、登録されていません。
4. スケールアップが必要なデリバリーグループに属している
5. 保留中の電源操作はありません。

デリバリーグループをスケールダウンする

Autoscale は、Autoscale が有効なデリバリーグループ内のマシンの電源を、次の場合にオフにします。

1. Autoscale スケジュールで、現在の期間に設定されたマシン数に合わせるために、マシンの電源をオフにする必要があると指定されている場合。
2. デリバリーグループの現在の負荷が減少し、プールサイズと容量バッファを満たすために必要な数よりも多くの電源オン状態のマシンが存在する場合。

Autoscale は、プールサイズと容量バッファを満たすために必要な数を超える余分なマシンの電源をオフにすることで、デリバリーグループをスケールダウンします。

スケールダウンプロセスには、次の2つのステップがあります。

1. 必要な数のマシンをドレイン状態にします。
2. ドレイン状態のすべてのマシンを電源オフのために選択します。

電源オフの対象となるマシンは、次の条件を満たしている必要があります。

1. メンテナンスモードではない
2. ハイパーバイザーがメンテナンスモードではない
3. 現在電源オンの状態である
4. 利用可能として登録されているか、起動後に登録を待機している
5. ドレイン状態であり、アクティブなセッションがない
6. 保留中の電源操作がない
7. 電源オフ遅延を満たしている

ドレイン状態

Autoscale は、デリバリーグループ内の電源オン状態のマシンの数を、構成されたプールサイズと容量バッファにまでスケールダウンしようとします。

この目標を達成するために、Autoscale はセッション数が最も少ない余分なマシンを「ドレイン状態」にし、すべてのセッションがログオフされたときにそれらの電源をオフにします。この動作は、セッションの需要が減少し、スケジュールで電源オンになっているマシンよりも少ないマシンが必要な場合に発生します。

マシンがドレイン状態になる条件:

1. 電源オンである

2. メンテナンスモードではない
3. ハイパーバイザーがメンテナンスモードではない
4. スケールダウンが必要なデリバリーグループに属している
5. 現在のアクティブセッション数が最も少ない

注:

- 電源オフ遅延で指定された時間以上電源がオンになっているマシンが、ドレインの対象として優先されます。
- ドレイン状態のマシンは、新しいセッションの起動をホストしなくなり、既存のセッションがログオフされるのを待ちます。マシンは、すべてのセッションがログオフされた場合にのみシャットダウンされます。ただし、セッション起動にすぐに利用できるマシンがない場合、Autoscale は、マシンの電源をオンにするよりも、ドレイン状態のマシンにセッション起動を誘導することを優先します。

Autoscale は、余分なマシンを「ドレイン状態」に1台ずつ移行します。

- 2台以上のマシンが同じ数のアクティブセッションを持っている場合、Autoscale は、指定された電源オフ遅延の間電源がオンになっていたマシンをドレインします。

  そうすることで、最近電源がオンになったマシンがドレイン状態になるのを避けることができます。なぜなら、それらのマシンはセッション数が最も少ない可能性が高いからです。
- 2台以上のマシンが指定された電源オフ遅延の間電源がオンになっていた場合、Autoscale はそれらのマシンをランダムに1台ずつドレインします。

ドレイン状態のマシンは、新しいセッションの起動をホストしなくなり、既存のセッションがログオフされるのを待っています。マシンは、すべてのセッションがログオフされた場合にのみシャットダウンの候補になります。ただし、セッション起動にすぐに利用できるマシンがない場合、Autoscale は、マシンの電源をオンにするよりも、ドレイン状態のマシンにセッション起動を誘導することを優先します。

次のいずれかの条件が満たされると、マシンはドレイン状態から解除されます。

- マシンの電源がオフになる。
- マシンが属するデリバリーグループで Autoscale が無効になっている。

- Autoscale は、スケジュールまたは負荷需要の要件を満たすためにマシンを使用します。このケースは、スケジュール（スケジュールベースのスケーリング）または現在の需要（負荷ベースのスケーリング）が、現在電源がオンになっているマシンの数よりも多くのマシンを必要とする場合に発生します。

> **重要:**
>
> セッション起動にすぐに利用できるマシンがない場合、Autoscale は、マシンの電源をオンにするよりも、ドレイン状態のマシンにセッション起動を誘導することを優先します。セッション起動をホストするドレイン状態のマシンは、ドレイン状態のままになります。

ドレイン状態の表示

PowerShellまたはWeb Studioを使用して、どのマシンがドレイン状態にあるかを判断できます。PowerShell を使用する `Get-BrokerMachineV2` PowerShellコマンドレットを実行して、マシンの**IsDraining**および**DrainingReason**プロパティを表示します。

例：`Get-BrokerMachineV2 -Property IsDraining,DrainingReason,MachineName | Format-Table MachineName,IsDraining,DrainingReason`

- **IsDraining:** このブール値プロパティは、マシンがドレイン状態の場合に `True`、そうでない場合に `False` になります。
- **DrainingReason:** このプロパティは、マシンがドレイン状態にある特定の理由を提供します。デフォルト値は `NotDraining` です。マシンがドレイン中の場合、**DrainingReason**は次のいずれかの値を表示します。
  - **AutoscaleScaleDown:** Autoscaleは、構成されたプールサイズと容量バッファの要件を満たすために、デリバリーグループ内の電源オン状態のマシン数をスケールダウンするためにドレイン状態を開始しました。これは、セッション需要が減少した場合、またはスケジュールで必要なマシン数が少ない場合に発生します。
  - **NaturalRebootCycle:** マシンは、「セッション終了を待機」再起動モードでのスケジュールされた再起動サイクルの一部としてドレイン中です。マシンは、再起動する前にアクティブなセッションが終了するのを待機します。
  - **RebootCycle:** マシンは、「強制ログオフ」再起動モードでのスケジュールされた再起動サイクルの一部としてドレイン中です。マシンが再起動する前に、アクティブなセッションは強制的にログオフされます。
  - **MaintenanceMode:** 管理者がマシンをメンテナンスモードにしました。

- **HypervisorInMaintenanceMode:** マシンをホストしているハイパーバイザー接続がメンテナンスモードになっています。
- **MaintenanceCycle:** マシンは、OSディスクのリセットなど、VUSメンテナンスサイクル操作の一部としてドレイン中です。
- **GuestOSDraining:** ゲストオペレーティングシステムは、明示的に自身をドレインモードに設定します（たとえば、レジストリ設定を介して）。この理由は、マルチセッションマシンにのみ適用されます。
- **GuestOSDrainingUntilRestart:** ゲストオペレーティングシステムは、次回の再起動まで持続するドレインモードに自身を設定します。この理由は、マルチセッションマシンにのみ適用されます。

Web Studio を使用する

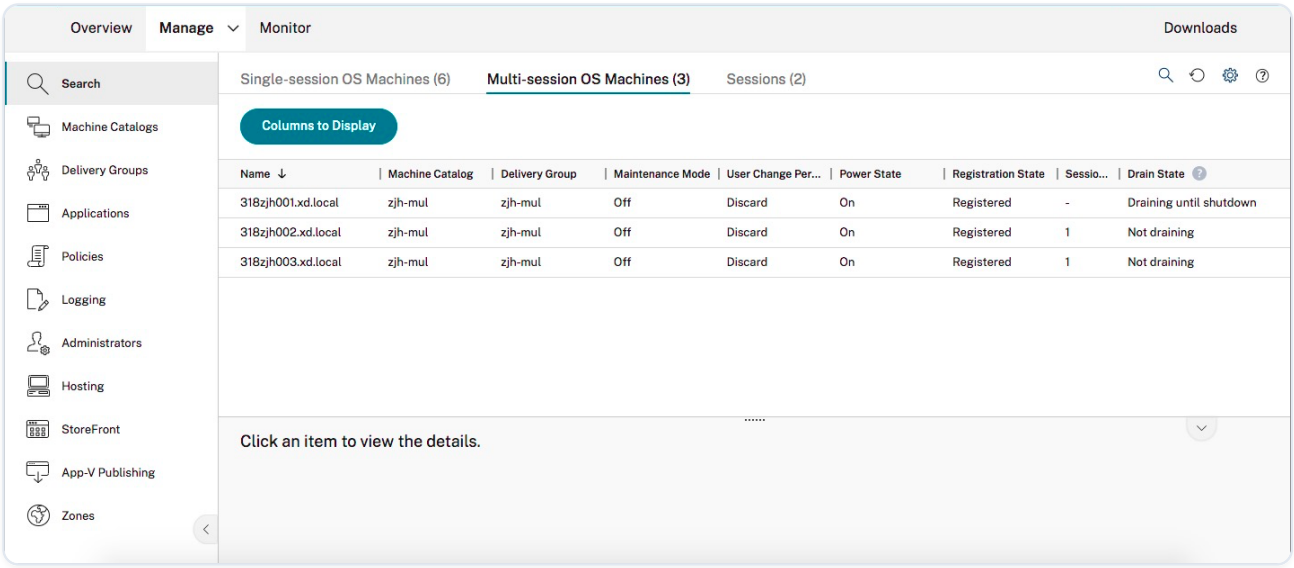
> **注:**
>
> `IsDraining` と `DrainingReason` のプロパティはシングルセッションマシンとマルチセッションマシンの両方に適用されますが（`GuestOSDraining` の理由はマルチセッション固有です）、Web Studio の **ドレイン状態** 列は、これらの状態を表示するために、これまでマルチセッションマシンにのみ適用されていました。

Web Studio でドレイン状態のマシンを表示するには:

1. **検索**ノードに移動し、**表示する列**をクリックします。
2. **表示する列**ウィンドウで、**ドレイン状態**の横にあるチェックボックスをオンにします。
3. **保存**をクリックして、**表示する列**ウィンドウを終了します。

ドレイン状態列には、次の情報が表示されます。

- **シャットダウンまでドレイン中。** マシンがシャットダウンされるまでドレイン状態にある場合に表示されます。
- **ドレイン中ではありません。** マシンがまだドレイン状態にない場合に表示されます。

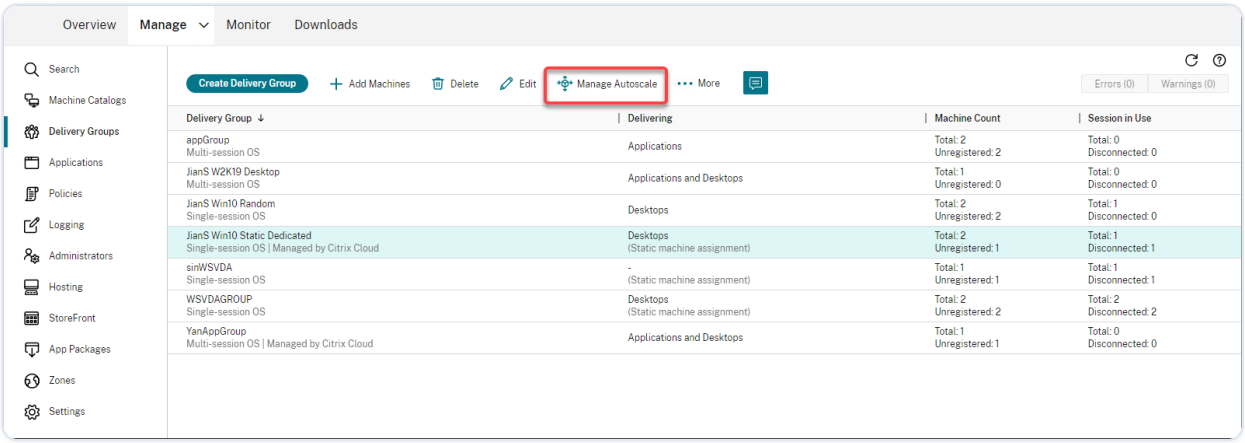


デリバリーグループのAutoscaleを有効にする

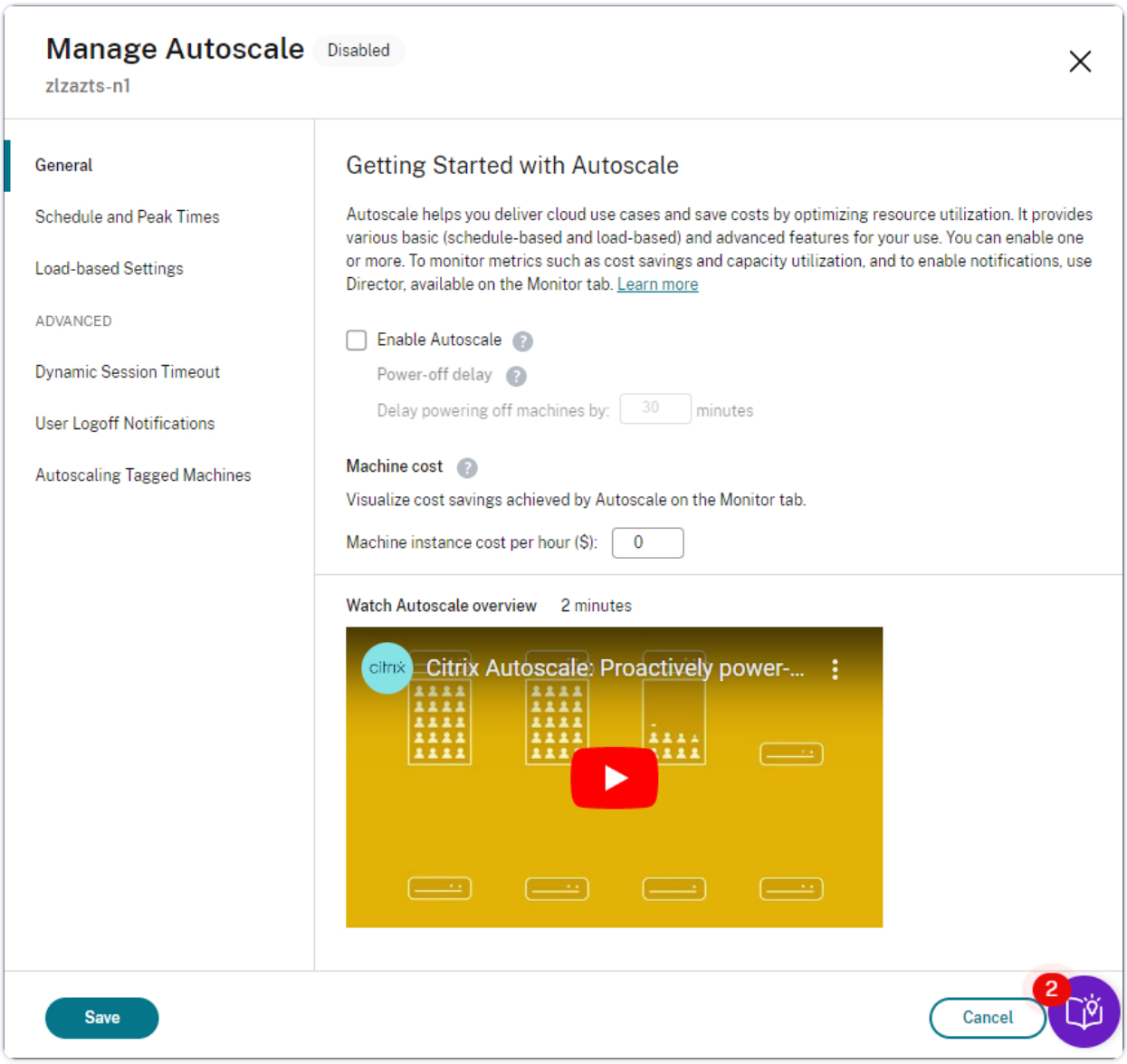
デリバリーグループを作成すると、Autoscaleはデフォルトで無効になります。Web Studioを使用してデリバリーグループのAutoscaleを有効にして構成するには、次の手順に従います。

PowerShellコマンドを使用して、デリバリーグループのAutoscaleを有効にして構成することもできます。詳細については、Broker PowerShell SDKコマンドを参照してください。

1. 左側のペインで を選択します。
2. 管理するデリバリーグループを選択し、**Autoscaleの管理**をクリックします。



3. ページで、 チェックボックスをオンにしてAutoscaleを有効にします。Autoscaleを有効にすると、ページ上のオプションが有効になります。



4. 組織のニーズに基づいてデフォルト設定を変更するには、次の設定を完了します。

   - スケジュールを設定する
   - 非アクティブなマシンをより効率的に電源オフにするには、動的セッションタイムアウトとユーザーログオフ通知を使用します。
   - デリバリーグループ内のマシンの一部を電源管理するには、タグ付きマシンのAutoscaleを使用します。

Autoscaleを無効にするには、 チェックボックスをオフにします。ページ上のオプションがグレー表示され、選択したデリバリーグループでAutoscaleが無効になっていることを示します。

> **重要:**

- Autoscaleを無効にすると、Autoscaleによって管理されているすべてのマシンは、無効化時の状態のままになります。
- Autoscaleを無効にすると、ドレイン状態のマシンはドレイン状態から解除されます。ドレイン状態の詳細については、ドレイン状態を参照してください。
- **負荷ベースの設定**ページにあるシングルセッションOS静的デリバリーグループおよびシングルセッションOSランダムデリバリーグループの**電源ポリシー**アクションは、Autoscaleの設定（有効または無効）とは独立しています。

ドレイン中のマシンをAutoscaleの計算から除外する

この機能を使用すると、再起動スケジュールが原因でドレイン中のマシンが Autoscale の容量ターゲットにカウントされるのを防ぐことができます。これらのマシンを除外することで、リソースプロビジョニングを最適化し、過剰なプロビジョニングを回避できます。

例: Autoscale と定期的な再起動スケジュールで構成されたマルチセッション OS マシンのデリバリーグループがあるとします。マシンが再起動のためにドレイン状態になると、Autoscale は通常、それらを利用可能な容量としてカウントします。これにより、不要な追加マシンのプロビジョニングがトリガーされる可能性があります。この機能を有効にすると、Autoscale は容量を計算する際にこれらのドレイン中のマシンを無視するように指示されます。これにより、アクティブに利用可能なマシンのみがターゲットに貢献し、より効率的なリソース利用と運用コストの削減につながります。

適用範囲

この機能は、**マルチセッション OS マシン (RDS)** を含むデリバリーグループに適用されます。

制限事項

- この機能はシングルセッション OS マシンには適用されません。
- Autoscale を「マシンの数」（「割合」ではなく）に基づいて構成する場合、システムはドレイン状態のマシンを Autoscale の計算から除外しません。

重要な考慮事項

- プロパティ `ExcludeNaturalRebootDrainingFromAutoscale` はデリバリーグループで構成されます。
- プロパティ `ExcludeNaturalRebootDrainingFromAutoscale` のデフォルト値は `False` です。これは、ドレイン中のマシンがデフォルトで Autoscale の計算に含まれることを意味します。

前提条件

- マルチセッションOSデリバリーグループを構成します。
- ターゲットのデリバリーグループに対してAutoscaleを有効にして構成します。スケーリングには「マシンの割合」を使用することをお勧めします。
- マシンをドレイン状態にするために、デリバリーグループの再起動スケジュールを構成します。

構成方法

この機能は、PowerShellコマンドを使用してデリバリーグループレベルで構成します。

1. 機能トグル `ExcludeNaturalRebootDrainingFromAutoscale` が有効になっていることを確認します。これは、PowerShellで `Get-ConfigEnabledFeature` を実行し、出力リストでトグルを確認することで検証できます。

   > **注:**
   >
   > トグルが無効になっている場合、デリバリーグループのプロパティを変更することはできません。

2. ドレイン中のマシンを除外するようにデリバリーグループのプロパティを設定します。

   a. 管理者権限でPowerShellを開きます。

   b. マルチセッションOSデリバリーグループを特定します。

   c. `Set-BrokerDesktopGroup` コマンドレットを使用して、デリバリーグループの `ExcludeNaturalRebootDrainingFromAutoscale` プロパティを `$True` に設定します。

   ```
   Set-BrokerDesktopGroup -Name "<YourDeliveryGroupName>"
   -ExcludeNaturalRebootDrainingFromAutoscale $True
   ```

   `<YourDeliveryGroupName>` をデリバリーグループの実際の名前で置き換えます。

   d. 実行して、プロパティが `True` に設定されていることを確認します。

   ```
   Get-BrokerDesktopGroup -Name "<YourDeliveryGroupName>" | Select
   Name, ExcludeNaturalRebootDrainingFromAutoscale
   ```

出力には `ExcludeNaturalRebootDrainingFromAutoscale : True` が表示されるはずです。

3. Autoscaleと再起動スケジュールを構成します（まだ構成されていない場合）。

   デリバリーグループでAutoscaleが有効になっており、マシンがドレイン状態になるように再起動スケジュールが構成されていることを確認します。

   a. Web Studio で、デリバリーグループを編集します。

   b. **Manage Autoscale** に移動し、ピーク/オフピークのスケジュールを構成して、Autoscale が有効になっていることを確認します。ドレイン中のマシンを除外する場合は、「マシンの割合」に基づいてスケジュールを設定します。

   c. **Restart Schedule** に移動し、マシンがドレイン状態になるスケジュールを作成または編集します（例：Cloud の場合は **Graceful restart**、オンプレミス展開の場合は **Re-start all machines after draining session** を使用します）。

監視とトラブルシューティング

問題: この機能を有効にしても、セッションがドレイン中のマシンで起動することがあります。

原因: これは予期される動作です。ドレイン状態のマシンは、他の適切なドレイン中でないマシンが利用できない場合の「最後の手段」として、セッション起動に引き続き利用できます。この機能は主に、プロビジョニング/プロビジョニング解除のための Autoscale 計算に影響します。ブローカーのセッション起動ロジック自体には影響しません。

解決策: これは問題ではなく、意図された設計です。ドレイン中のマシンへのセッションを最小限に抑えるには、Autoscale のバッファと容量が、需要を満たすのに十分な数のドレイン中でないマシンを維持できることを確認してください。

ユーザーセッションを持つVMのAutoscaleオプション

Autoscaleは、割り当て済みマシンとプールされたマシンの両方を管理し、それらの電源と可用性を最適化できます。以下のコンテンツでは、割り当て済みマシンとプールされたマシン向けに、ピーク時とオフピーク時、およびユーザーセッションに基づいてマシンの電源状態を制御するためのPowerShellコマンドとUI設定を提供します。

割り当てられたマシンは単一ユーザー専用ですが、プールされたマシンは複数のユーザー間で共有されます。

> **注:**

- Citrix Studioのセッション制限ポリシー、特に*切断されたセッションタイマー*と*セッションアイドルタイマー*は、Citrix Autoscaleが有効になっていない場合でもユーザーセッションを管理するために不可欠です。これらのポリシーは、セッションが終了するまでに切断またはアイドル状態を維持できる期間を定義し、リソースの利用を確保し、ロックアウトされたセッションを防ぎます。このポリシー設定は、割り当てられたマシンとプールされたマシンの両方、特にマルチセッションVDAを実行しているマシンで使用できます。詳細については、セッション制限ポリシー設定を参照してください。
- `Get-BrokerMachine` PowerShellコマンドは非推奨です。代わりに`Get-BrokerMachineV2`を使用してください。

割り当てられたマシンについて

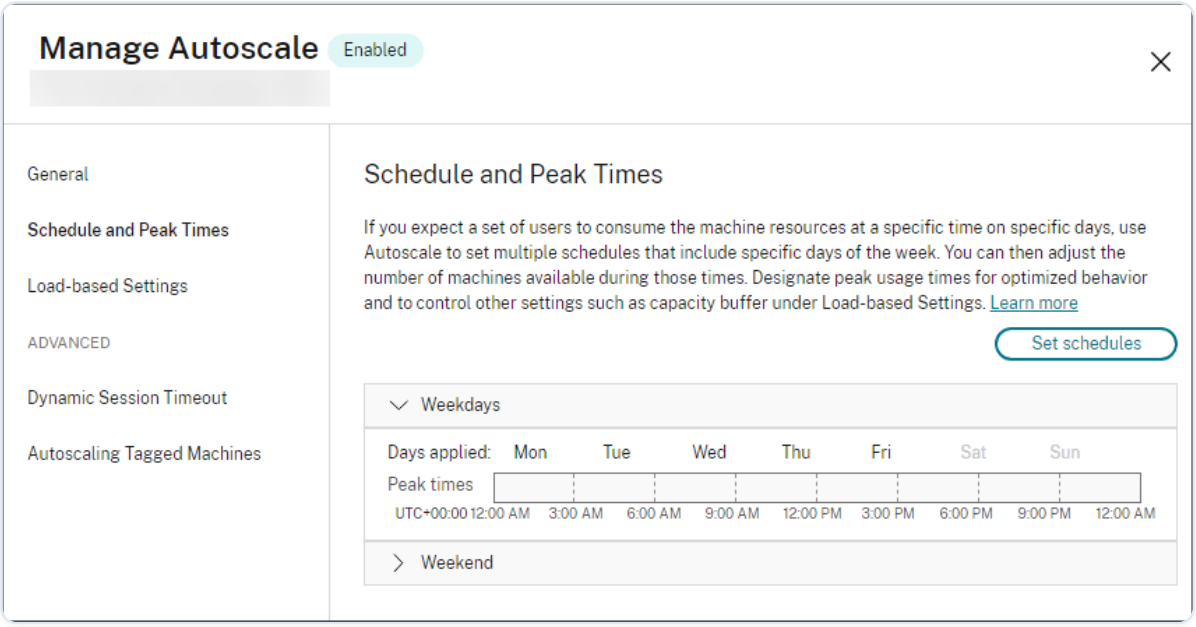
- ピーク時間の開始時に、静的デリバリーグループ内の割り当てられたシングルセッションマシンを自動的に電源オンにするには、PowerShellコマンドを使用します。

```
Set-BrokerDesktopGroup "Desktop Group Name"
-AutomaticPowerOnForAssigned $True
```

- ピーク時間中にオフになっていることが判明した割り当てられたマシンが再起動されるようにするには、`AutomaticPowerOnForAssignedDuringPeak`も有効にします。

```
Set-BrokerDesktopGroup "Desktop Group Name"
-AutomaticPowerOnForAssigned $True
-AutomaticPowerOnForAssignedDuringPeak $True
```

- ユーザーがセッションを起動したときにのみVMをオンにしたい場合は、次のいずれかを実行します。
  - `AutomaticPowerOnForAssigned`と`AutomaticPowerOnForAssignedDuringPeak`を`False`に設定します。
  - UIインターフェースを使用して、すべての時間をピーク時間なしのオフピークとして定義します。スケジュールベースの設定を参照してください。オフピーク時には、Autoscaleで管理されている割り当てられたマシンは、ユーザーセッションがない場合にシャットダウンされます。



- ピーク時にすべてのマシンがAutoscaleによって電源オンにされる場合、UIインターフェースを使用して、待機時間（分）と、Autoscaleによってマシンが電源オンになった後にユーザーがログオンしない場合の「アクションなし」、「一時停止」、「シャットダウン」などのアクションを設定します。電源ポリシーを参照してください。

プールされたマシンについて

セッションログオフ後にプールされたマシンを自動的にシャットダウンするには、デリバリーグループに対してPowerShellコマンド`ShutdownAfterUse`を`True`に設定します。例:

```
Set-BrokerDesktopGroup -Name “DesktopGroupName” -ShutdownDesktopsAfterUse $true
```

メトリックの監視

デリバリーグループでAutoscaleを有効にすると、DirectorからAutoscaleで管理されているマシンの以下のメトリックを監視できます。

- マシンの使用状況
- 推定節約額
- マシンとセッションのアラート通知
- マシンのステータス
- 負荷評価の傾向

注:

> デリバリーグループでAutoscaleを最初に有効にした後、そのデリバリーグループの監視データが表示されるまでに数分かかる場合があります。 Autoscaleが有効になり、その後デリバリーグループで無効になった場合でも、監視データは引き続き利用可能です。Autoscaleは5分間隔で監視データを収集します。

> メトリックの詳細については、「Autoscaleで管理されるマシンの監視」を参照してください。

休止状態のVMでのAutoscale

Autoscaleの構成可能な設定を通じてVMを休止状態にできます。PowerShellコマンド `Get-BrokerDesktopGroups`、`New-BrokerDesktopGroups`、または `Set-BrokerDesktopGroups` を使用して、パラメーター `AutoscaleScaleDownActionDuringPeak`（ピーク時）または `AutoscaleScaleDownActionDuringOffPeak`（オフピーク時）に以下の正の値を設定し、電源アクションを定義します。

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

休止状態にできないVMはシャットダウンされます。

デリバリーグループで休止状態が有効になっている場合、休止状態のVMの再起動スケジュールを構成できます。再起動サイクルでは、VMは再開され、その後シャットダウンされます。再起動スケジュールは、毎週、毎日、毎月、および1回に設定できます。複数のスケジュールを構成できます。ただし、休止状態から再開するVMには数分かかる場合があります。

Autoscaleは、ピーク時にセッションがない休止状態のマルチセッションRemote Desktop Services (RDS) および共有シングルセッションVMの電源をオンにすることもできます。VMはMCSおよび非MCSマシンカタログのいずれでも可能です。

詳細情報

Autoscaleの詳細については、Tech ZoneのCitrix Autoscaleを参照してください。

スケジュールベースおよび負荷ベースの設定

Autoscale™によるマシンの電源管理方法

Autoscaleは、選択されたスケジュールに基づいてマシンの電源をオン/オフします。Autoscaleを使用すると、特定の曜日を含む複数のスケジュールを設定し、その時間帯に利用可能なマシンの数を調整できます。特定の曜日の特定の時間に一連のユーザーがマシンリソースを消費すると予想

される場合、Autoscaleは最適化されたエクスペリエンスの提供に役立ちます。これらのマシンは、セッションが実行されているかどうかにかかわらず、スケジュール中に電源がオンになることに注意してください。

> **注:**
>
> Autoscaleは、電源管理されているすべてのマシンをサポートします。

> スケジュールは、デリバリーグループの**タイムゾーン**に基づいています。タイムゾーンを変更するには、デリバリーグループのユーザー設定を変更します。詳しくは、「デリバリーグループの管理」を参照してください。

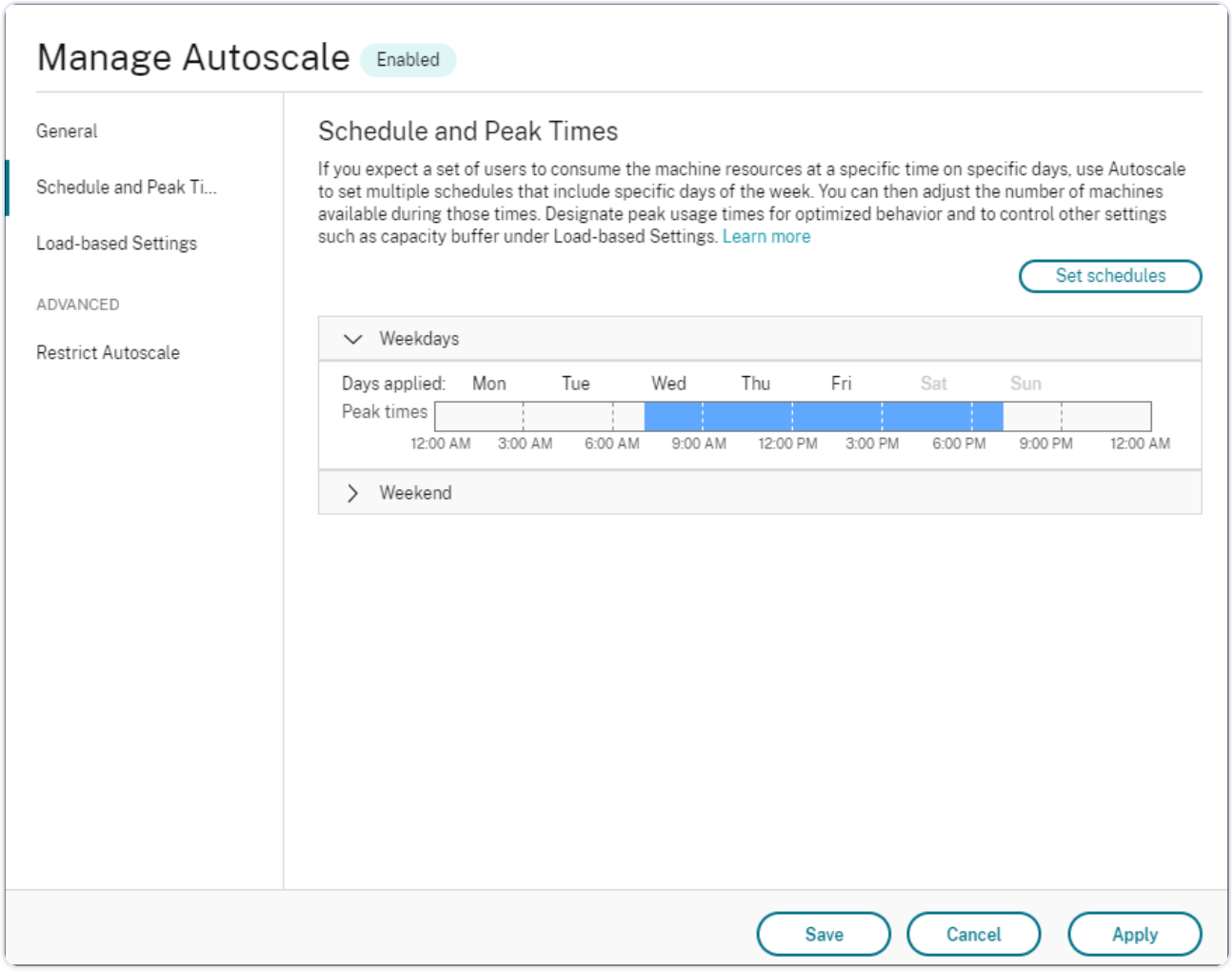
Autoscaleには、*平日*（月曜日から金曜日）と*週末*（土曜日と日曜日）の2つのデフォルトスケジュールがあります。デフォルトでは、**平日**スケジュールでは、ピーク時に午前7時から午後6時30分まで1台のマシンの電源がオンになり、オフピーク時には電源がオンになりません。デフォルトの容量バッファは、ピーク時とオフピーク時ともに10%に設定されています。デフォルトでは、**週末**スケジュールでは、マシンの電源はオンになりません。

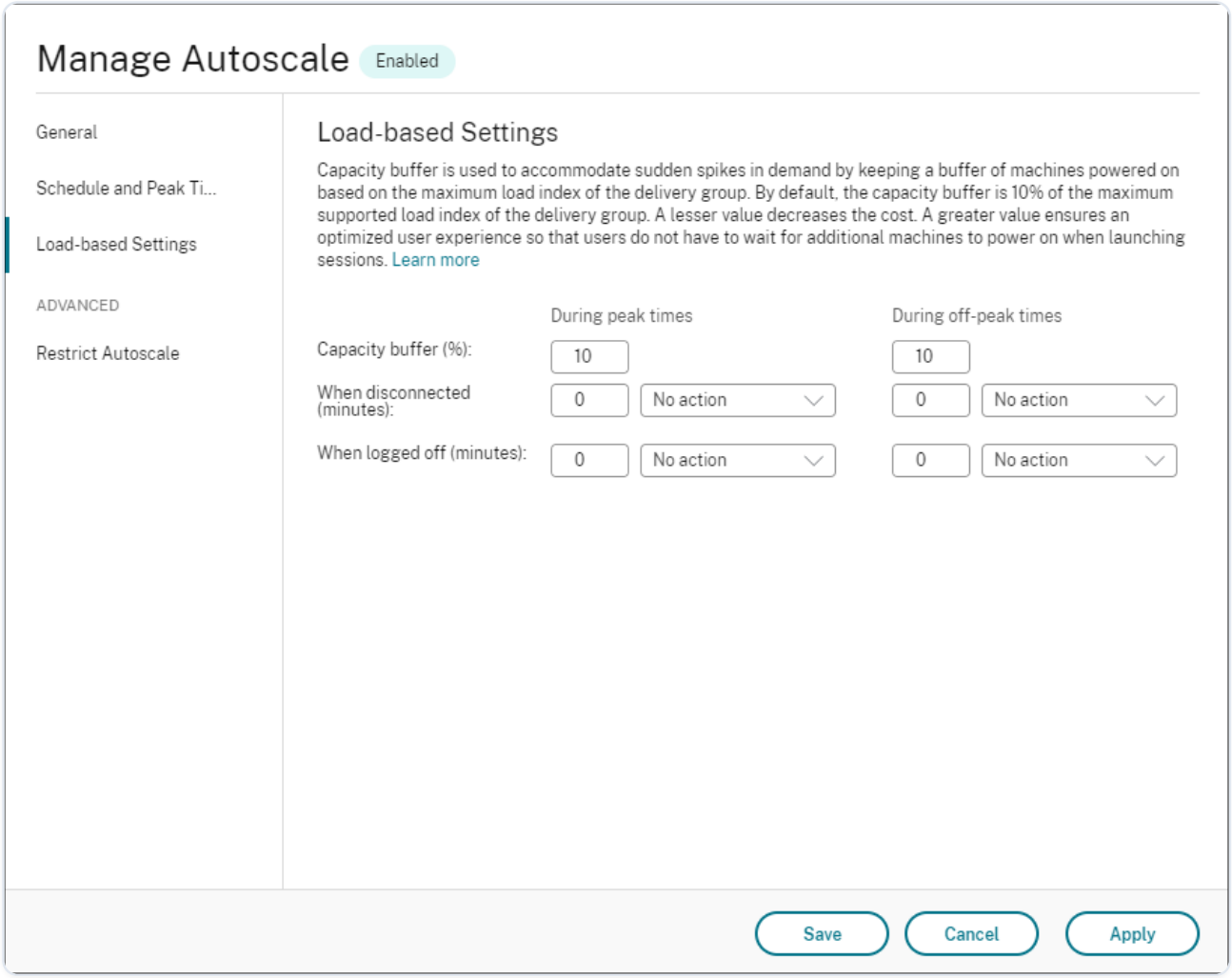
> **注:**
>
> Autoscaleは、サイトに登録されているマシンのみを、計算における利用可能な容量の一部として扱います。「登録済み」とは、マシンが使用可能であるか、すでに使用中であることを意味します。これにより、ユーザーセッションを受け入れられるマシンのみがデリバリーグループの容量に含まれるようになります。

ユーザーインターフェイス

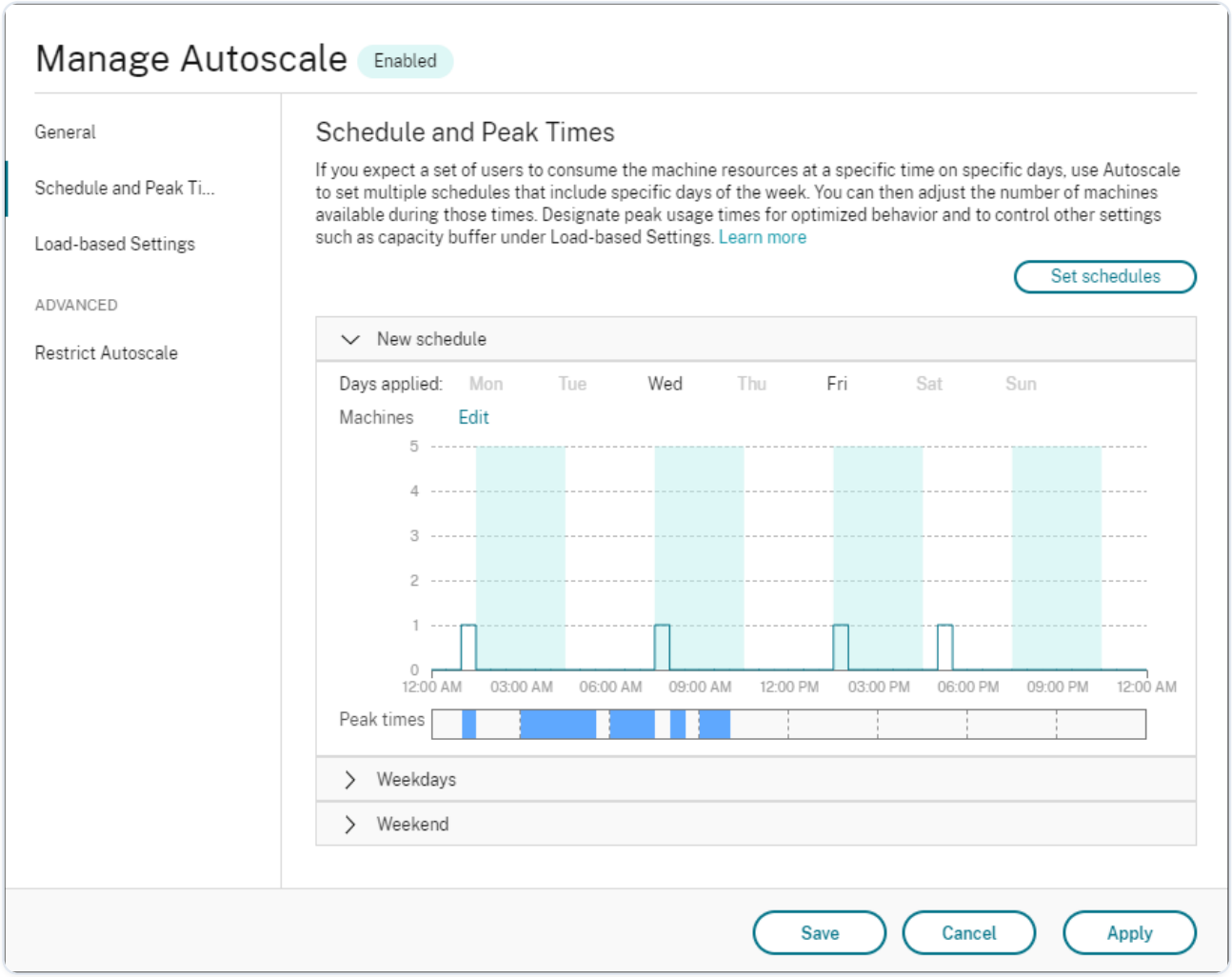
留意すべきユーザーインターフェイスは3種類あります。

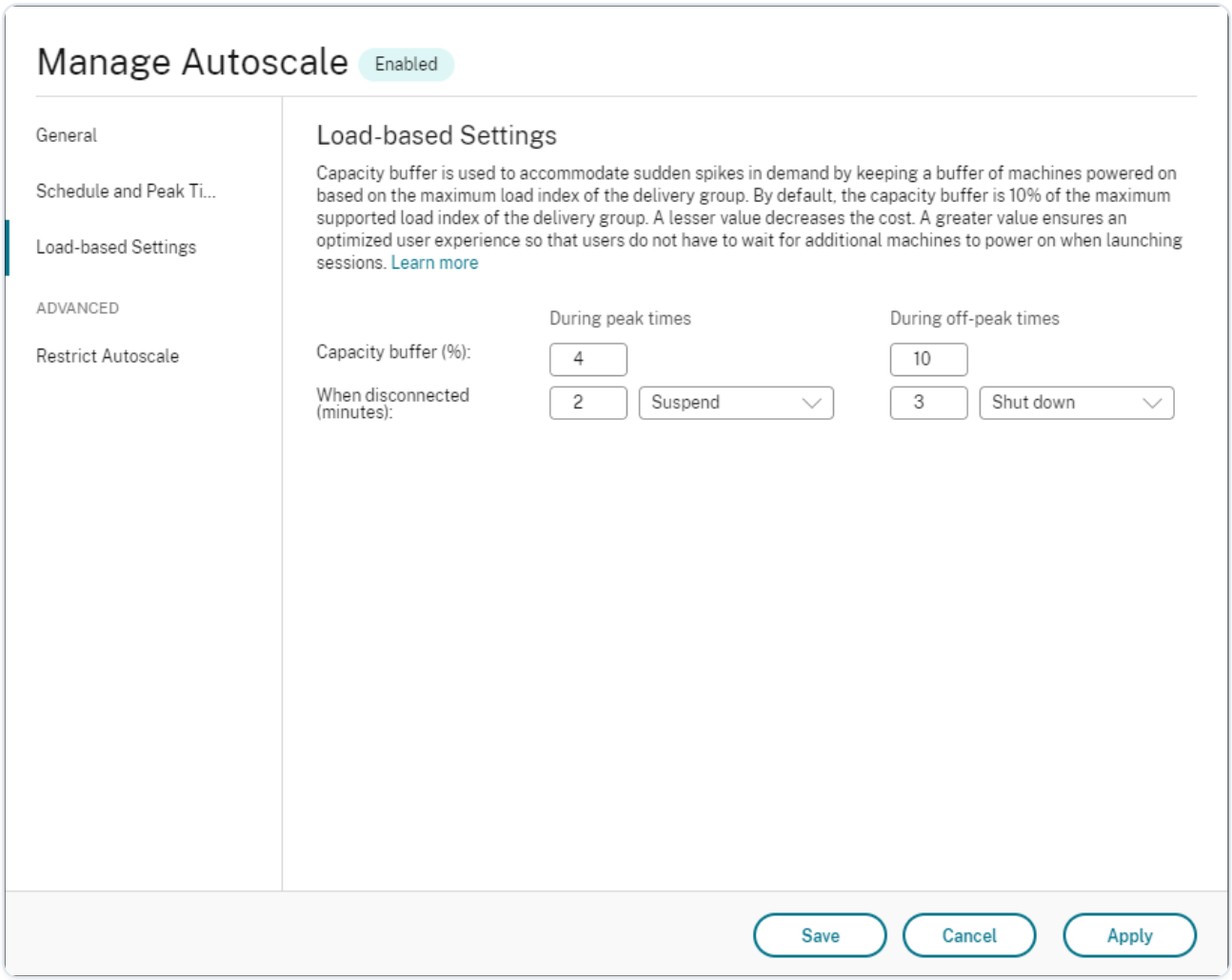
*シングルセッションOS静的デリバリーグループ*のユーザーインターフェイス：


Manage Autoscale
Enabled
General
Schedule and Peak Ti...
Load-based Settings
ADVANCED
Restrict Autoscale
Schedule and Peak Times
If you expect a set of users to consume the machine resources at a specific time on specific days, use Autoscale to set multiple schedules that include specific days of the week. You can then adjust the number of machines available during those times. Designate peak usage times for optimized behavior and to control other settings such as capacity buffer under Load-based Settings. Learn more
Set schedules
Weekdays
Days applied: Mon Tue Wed Thu Fri Sat Sun
Peak times
12:00 AM 3:00 AM 6:00 AM 9:00 AM 12:00 PM 3:00 PM 6:00 PM 9:00 PM 12:00 AM
Weekend
Save
Cancel
Apply

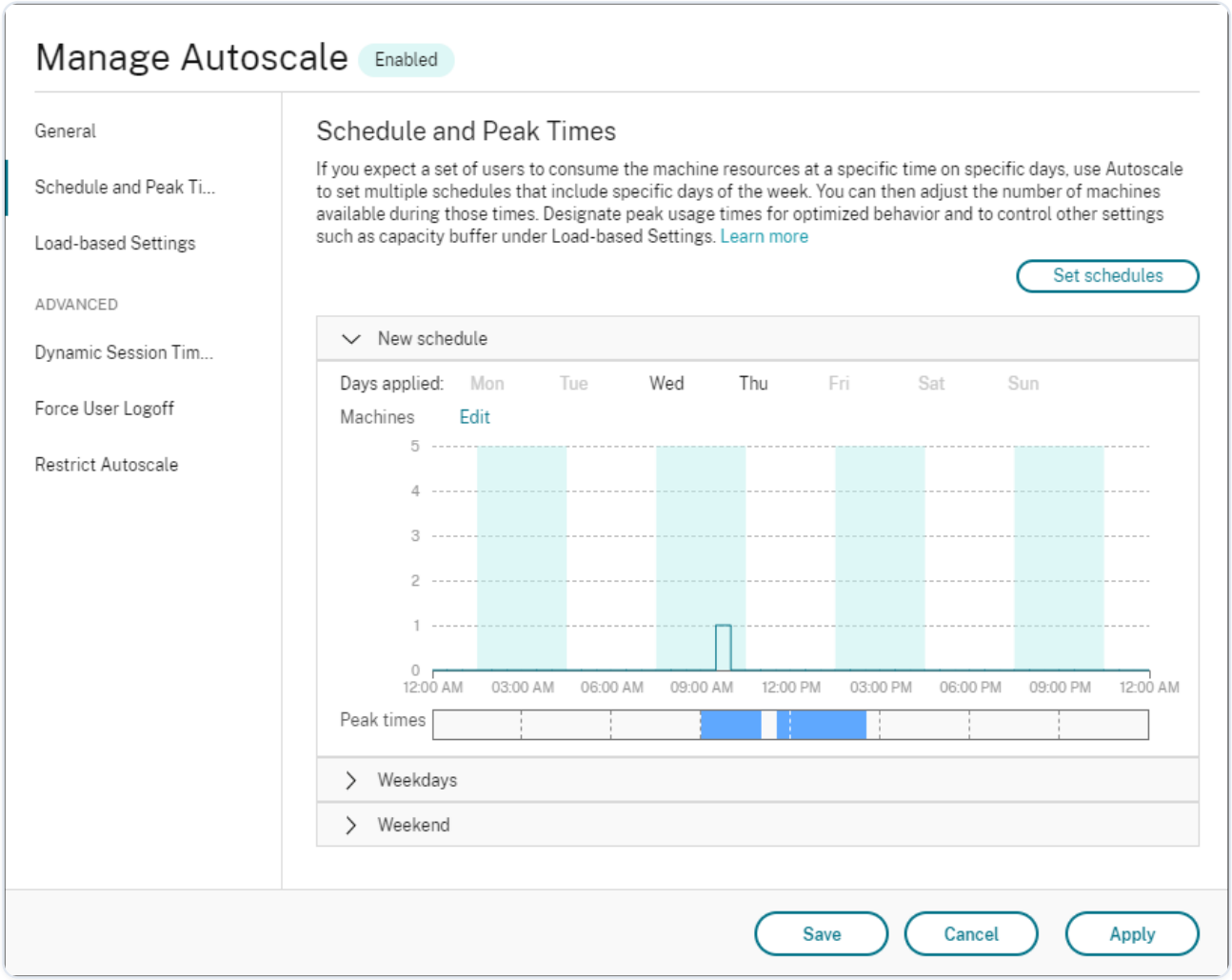


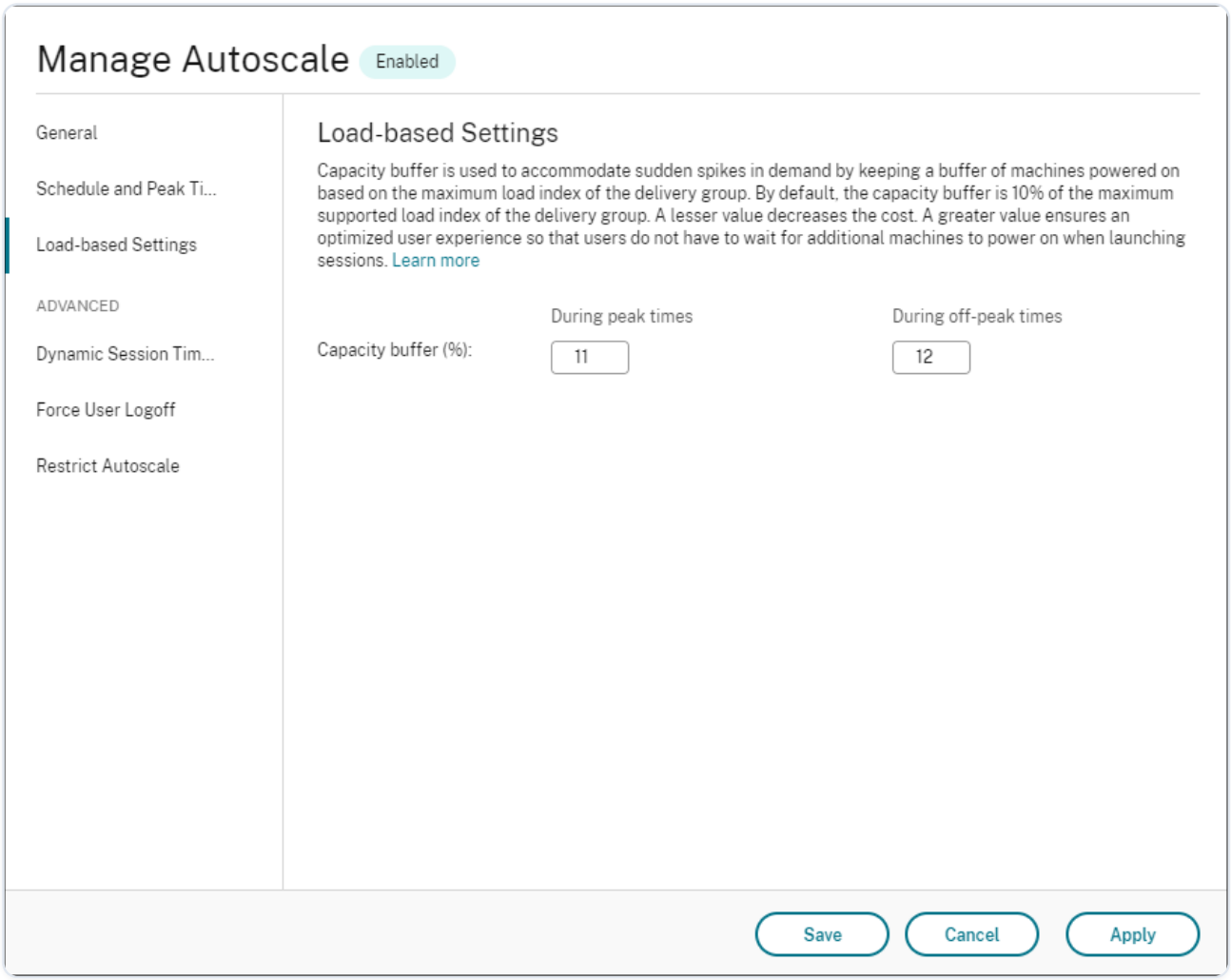
*シングルセッションOSランダムデリバリーグループの*Autoscaleユーザーインターフェイス：


Manage Autoscale
Enabled
General
Schedule and Peak Ti...
Load-based Settings
ADVANCED
Restrict Autoscale
Schedule and Peak Times
If you expect a set of users to consume the machine resources at a specific time on specific days, use Autoscale to set multiple schedules that include specific days of the week. You can then adjust the number of machines available during those times. Designate peak usage times for optimized behavior and to control other settings such as capacity buffer under Load-based Settings. Learn more
Set schedules
New schedule
Days applied: Mon Tue Wed Thu Fri Sat Sun
Machines Edit
5
4
3
2
1
0
12:00 AM 03:00 AM 06:00 AM 09:00 AM 12:00 PM 03:00 PM 06:00 PM 09:00 PM 12:00 AM
Peak times
Weekdays
Weekend
Save
Cancel
Apply



マルチセッションOSデリバリーグループのAutoscaleユーザーインターフェイス:


Manage Autoscale
Enabled
General
Schedule and Peak Ti...
Load-based Settings
ADVANCED
Dynamic Session Tim...
Force User Logoff
Restrict Autoscale
Schedule and Peak Times
If you expect a set of users to consume the machine resources at a specific time on specific days, use Autoscale to set multiple schedules that include specific days of the week. You can then adjust the number of machines available during those times. Designate peak usage times for optimized behavior and to control other settings such as capacity buffer under Load-based Settings. Learn more
Set schedules
New schedule
Days applied: Mon Tue Wed Thu Fri Sat Sun
Machines Edit
5
4
3
2
1
0
12:00 AM 03:00 AM 06:00 AM 09:00 AM 12:00 PM 03:00 PM 06:00 PM 09:00 PM 12:00 AM
Peak times
Weekdays
Weekend
Save
Cancel
Apply



スケジュールベースの設定

Autoscaleスケジュール。スケジュールの追加、編集、選択、削除が可能です。

適用日。選択したスケジュールに適用した日を強調表示します。残りの日はグレー表示されます。

編集。マシンを1時間ごとまたは30分ごとに割り当てることができます。マシンは数値またはパーセンテージで割り当てることができます。

> **注:**
>
> - このオプションは、マルチセッションOSおよびシングルセッションOSのランダムデリバリーグループ用のAutoscaleユーザーインターフェイスでのみ利用可能です。
> - **編集**の横にあるヒストグラムは、異なるタイムスロットで実行されているマシンの数または割合を示します。

- **ピーク時間**の上にある**編集**をクリックして、各タイムスロットに**マシンを割り当てる**ことができます。**起動するマシン**ウィンドウのメニューから選択したオプションに応じて、マシンを数値またはパーセンテージで割り当てることができます。
- マルチセッションOSデリバリーグループの場合、各日において30分単位で実行中のマシンの最小数を個別に設定できます。シングルセッションOSランダムデリバリーグループの場合、各日において60分単位で実行中のマシンの最小数を個別に設定できます。

独自のスケジュールを定義するには、次の手順に従います。

1. **Autoscaleの管理**ウィンドウの**スケジュールとピーク時間**ページで、**スケジュールを設定**をクリックします。
2. **Autoscaleスケジュールの編集**ウィンドウで、各スケジュールに適用する日を選択します。必要に応じてスケジュールを削除することもできます。
3. **完了**をクリックしてスケジュールを保存し、**スケジュールとピーク時間**ページに戻ります。
4. 該当するスケジュールを選択し、必要に応じて構成します。
5. **適用**をクリックして、**Autoscaleの管理**ウィンドウを終了するか、他のページで設定を構成します。

重要:

- Autoscaleでは、異なるスケジュールで同じ曜日が重複することはできません。たとえば、schedule1で月曜日を選択した後、schedule2で月曜日を選択すると、schedule1の月曜日は自動的にクリアされます。
- スケジュール名は大文字と小文字を区別しません。
- スケジュール名は空白にしたり、スペースのみを含めたりすることはできません。
- Autoscaleでは、文字間に空白スペースを入れることができます。
- スケジュール名には、次の文字を含めることはできません: \ / ; : # . * ? = < > \| ( ) { } " ' `。
- Autoscaleは重複するスケジュール名をサポートしていません。各スケジュールに異なる名前を入力してください。
- Autoscaleは空のスケジュールをサポートしていません。つまり、曜日が選択されていないスケジュールは保存されません。

注:

選択したスケジュールに含まれる曜日は強調表示され、含まれない曜日はグレー表示されます。

負荷ベースの設定

ピーク時間。選択したスケジュールに適用した日のピーク時間を定義できます。これを行うには、横棒グラフを右クリックします。ピーク時間を定義すると、残りの未定義の時間はデフォルトでオフピーク時間になります。**デフォルト**では、選択したスケジュールに含まれる日のピーク時間として、午前7時から午後7時までの時間帯が定義されています。

重要:

- マルチセッションOSデリバリーグループの場合、ピーク時間の棒グラフは容量バッファに使用されます。
- シングルセッションOSデリバリーグループの場合、ピーク時間の棒グラフは容量バッファに使用され、ログオフ後または切断後にトリガーされるアクションを制御します。
- マルチセッションOSおよびシングルセッションOSデリバリーグループの両方で、スケジュールに含まれる日のピーク時間を30分単位で細かく定義できます。または、代わりに`New-BrokerPowerTimeScheme PowerShell`コマンドを使用することもできます。詳細については、「Broker PowerShell SDKコマンド」を参照してください。

キャパシティバッファー。稼働中のマシンのバッファーを維持できます。値が小さいほどコストが削減されます。値が大きいほど、セッション起動時にユーザーが追加のマシンの電源がオンになるのを待つ必要がなくなり、最適化されたユーザーエクスペリエンスが保証されます。デフォルトでは、ピーク時とオフピーク時のキャパシティバッファーは10%です。
キャパシティバッファーを0に設定すると、セッション起動時にユーザーが追加のマシンの電源がオンになるのを待つ必要がある場合があります。Autoscaleでは、ピーク時とオフピーク時でキャパシティバッファーを個別に決定できます。

その他の設定

ヒント:

- Broker PowerShell SDKを使用して、その他の設定を構成できます。詳しくは、「Broker PowerShell SDKコマンド」を参照してください。
- 切断時およびログオフ時の設定に関連するSDKコマンドについては、`<https://citrix.github.io/delivery-controller-sdk/Broker/about_Broker_PowerManagement/#power-policy>`を参照してください。

切断時。セッション切断後、切断されロックされたマシンが、中断またはシャットダウンされるまでにどのくらいの時間電源がオンのままになるかを指定できます。時間値を指定すると、構成したアクションに応じて、指定された切断時間が経過したときにマシンが中断またはシャットダウンされます。デフォルトでは、切断されたマシンにはアクションが割り当てられません。ピーク時とオフピーク時でアクションを個別に定義できます。そのためには、下矢印をクリックし、メニューから次のいずれかのオプションを選択します。

- **アクションなし**。選択すると、セッション切断後もマシンは電源がオンのままになります。Autoscaleはそれに対してアクションを実行しません。
- **中断**。選択すると、指定された切断時間が経過したときに、Autoscaleはマシンをシャットダウンせずに一時停止します。**中断**を選択すると、次のオプションが使用可能になります。
  - **再接続なしの場合（分）**。中断されたマシンは、切断されたユーザーが再接続する際には利用可能ですが、新しいユーザーには利用できません。すべてのワークロードを処理するためにマシンを再度利用可能にするには、シャットダウンします。Autoscaleがマシンをシャットダウンするまでのタイムアウトを分単位で指定します。
- **シャットダウン**。選択すると、指定された切断時間が経過したときに、Autoscaleはマシンをシャットダウンします。

注:

このオプションは、シングルセッションOSのランダムおよび静的デリバリーグループ用のAutoscaleユーザーインターフェイスでのみ使用できます。

ログオフ時。セッションログオフ後、マシンが中断またはシャットダウンされるまでにどのくらいの時間電源がオンのままになるかを指定できます。時間値を指定すると、構成したアクションに応じて、指定されたログオフ時間が経過したときにマシンが中断またはシャットダウンされます。デフォルトでは、ログオフされたマシンにはアクションが割り当てられま

せん。ピーク時とオフピーク時でアクションを個別に定義できます。そのためには、下矢印をクリックし、メニューから次のいずれかのオプションを選択します。

- **アクションなし**。選択すると、セッションログオフ後もマシンは電源がオンのままになります。Autoscaleはそれに対してアクションを実行しません。
- **中断**。選択すると、指定されたログオフ時間が経過したときに、Autoscaleはマシンをシャットダウンせずに一時停止します。
- **シャットダウン**。選択すると、指定されたログオフ時間が経過したときに、Autoscaleはマシンをシャットダウンします。

注:

このオプションは、シングルセッションOSの静的デリバリーグループ用のAutoscaleユーザーインターフェイスでのみ使用できます。

切断されたセッションを持つ、異なる時間帯に移行するシングルセッションOSマシンの電源管理

重要:

- この機能強化は、切断されたセッションを持つシングルセッションOSマシンにのみ適用されます。ログオフされたセッションを持つシングルセッションOSマシンには適用されません。
- この機能強化を有効にするには、該当するデリバリーグループでAutoscaleを有効にする必要があります。そうしないと、期間移行時に切断電源ポリシーアクションはトリガーされません。

以前のリリースでは、アクション（切断アクション = 「**一時停止**」または「**シャットダウン**」）が必要な時間帯に移行するシングルセッションOSマシンは、電源が入ったままでした。このシナリオは、マシンがアクション（切断アクション = 「**何もしない**」）が不要な時間帯（ピーク時またはオフピーク時）に切断された場合に発生しました。

このリリース以降、Autoscaleは、指定された切断時間が経過すると、移行先の時間帯に設定されている切断アクションに応じて、マシンを一時停止またはシャットダウンします。

例えば、シングルセッションOSデリバリーグループに対して、以下の電源ポリシーを設定します。

- `PeakDisconnectAction`を「Nothing」に設定します
- `OffPeakDisconnectAction`を「Shutdown」に設定します
- 「OffPeakDisconnectTimeout」を「10」に設定します

> **注:**
>
> 切断アクション電源ポリシーの詳細については、`<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policy>`および`<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/>`を参照してください。

> 以前のリリースでは、ピーク時にセッションが切断されたシングルセッションOSマシンは、ピークからオフピークに移行しても電源が入ったままでした。このリリース以降、期間移行時に`OffPeakDisconnectAction`および`OffPeakDisconnectTimeout`ポリシーアクションがシングルセッションOSマシンに適用されます。その結果、マシンはオフピークに移行してから10分後に電源がオフになります。

以前の動作（つまり、切断されたセッションを持つマシンがピークからオフピークへ、またはオフピークからピークへ移行しても何もしない）に戻したい場合は、次のいずれかを実行します。

- 「LegacyPeakTransitionDisconnectedBehaviour」レジストリ値を1（true; 以前の動作を有効にする）に設定します。デフォルトでは、値は0（false; 期間移行時に切断電源ポリシーアクションをトリガーする）です。
  - パス: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer
  - 名前: LegacyPeakTransitionDisconnectedBehaviour
  - 種類: REG_DWORD
  - データ: 0x00000001 (1)
- `Set-BrokerServiceConfigurationData` PowerShellコマンドを使用して設定を構成します。例:

- `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

期間移行時に電源ポリシーアクションを適用する前に、マシンは次の基準を満たす必要があります。

- 切断されたセッションがあります。
- 保留中の電源操作がない。
- 異なる時間帯に移行するシングルセッションOSデリバリーグループに属している。
- 特定時間帯（ピーク時またはオフピーク時）にセッションが切断され、電源操作が割り当てられている期間に移行する。

容量バッファの仕組み

容量バッファは、動的な負荷増加に対応するために、現在の需要に予備容量を追加するために使用されます。注意すべき2つのシナリオがあります。

- マルチセッションOSデリバリーグループの場合、容量バッファは、ロードインデックスの観点からデリバリーグループの総容量の割合として定義されます。ロードインデックスの詳細については、「ロードインデックス」を参照してください。
- シングルセッションOSデリバリーグループの場合、容量バッファは、マシンの数の観点からデリバリーグループの総容量の割合として定義されます。

> **注:**

> Autoscaleをタグ付きマシンに制限するシナリオでは、容量バッファは、ロードインデックスの観点からデリバリーグループ内のタグ付きマシンの総容量の割合として定義されます。

> Autoscaleでは、ピーク時とオフピーク時で容量バッファを個別に設定できます。容量バッファフィールドの値が小さいほど、Autoscaleが起動する予備容量が少なくなるため、コストが削減されます。値が大きいほど、ユーザーはセッション起動時により多くのマシンが起動するのを待つ必要がなくなり、最適化されたユーザーエクスペリエンスが保証されます。デフォルトでは、容量バッファは10%です。

> **重要:**

容量バッファにより、総予備容量がデリバリーグループの総容量の「X」パーセントを下回るレベルに低下した場合にマシンが起動されます。これにより、必要な割合の予備容量が確保されます。

マルチセッションOSデリバリーグループ

マシンはいつ起動されますか?

重要:

スケジュールが選択されている場合、Autoscaleはスケジュールで起動するように構成されているすべてのマシンを起動します。Autoscaleは、負荷に関係なく、スケジュール中に指定された数のマシンを起動したままにします。

デリバリーグループ内の起動済みマシンの数が、ロードインデックスの観点からバッファ容量を維持するために必要なバッファを満たせなくなった場合、Autoscaleは追加のマシンを起動します。たとえば、デリバリーグループに20台のマシンがあり、スケジュールベースのスケーリングの一部として、容量バッファ20%で3台のマシンが起動するようにスケジュールされているとします。最終的に、負荷がない場合でも4台のマシンが起動されます。これは、バッファとして4 x 10kのロードインデックスが必要なため、少なくとも4台のマシンが起動される必要があるためです。このケースは、ピーク時、マシンの負荷増加、新しいセッションの起動、およびデリバリーグループに新しいマシンを追加する際に発生する可能性があります。Autoscaleは、次の条件を満たすマシンのみを起動することに注意してください。

- マシンがメンテナンスモードではない。
- マシンが実行されているハイパーバイザーがメンテナンスモードではない。
- マシンは現在電源オフの状態です。
- マシンに保留中の電源操作はありません。

マシンはいつ電源オフになりますか?

重要:

- スケジュールが選択されている場合、Autoscale はスケジュールに基づいてマシンの電源をオフにします。

- Autoscale は、スケジュール中に電源オンになるようにスケジュールで構成されたマシンの電源をオフにしません。

デリバリーグループのターゲットとなる電源オン状態のマシン数（バッファを含む）をサポートするのに十分すぎるほどのマシンがある場合、Autoscale は余分なマシンの電源をオフにします。このケースは、オフピーク時、マシンの負荷が減少したとき、セッションログオフ時、およびデリバリーグループからマシンを削除したときに発生する可能性があります。Autoscale は、以下の条件を満たすマシンのみ電源をオフにします。

- マシンと、マシンが実行されているハイパーバイザーがメンテナンスモードではありません。
- マシンは現在電源オンの状態です。
- マシンは利用可能として登録されているか、起動後に登録を待機しています。
- マシンにアクティブなセッションはありません。
- マシンに保留中の電源操作はありません。
- マシンは指定された電源オフ遅延を満たしています。これは、マシンが少なくとも「X」分間電源オンの状態であったことを意味します。「X」はデリバリーグループに指定された電源オフ遅延です。

例のシナリオ

次のシナリオを想定します。

- **デリバリーグループの構成**。Autoscale で電源管理するデリバリーグループには、10台のマシン（M1～M10）が含まれています。
- **Autoscale の構成**
  - キャパシティバッファは10%に設定されています。
  - 選択されたスケジュールにはマシンが含まれていません。

シナリオは次の順序で実行されます。

1. ユーザーはログオンしません。
2. ユーザーセッションが増加します。
3. より多くのユーザーセッションが開始されます。
4. セッション終了により、ユーザーセッションの負荷が減少します。
5. セッション負荷がオンプレミスリソースのみで処理されるまで、ユーザーセッションの負荷はさらに減少します。

上記のシナリオでAutoscaleがどのように機能するかについては、以下を参照してください。

- ユーザー負荷なし（初期状態）
  - 1台のマシン（例: M1）が電源オンになります。このマシンは、構成されたキャパシティバッファのために電源オンになります。この場合、10（マシン数）x 10,000（負荷インデックス）x 10%（構成されたキャパシティバッファ）は10,000に等しくなります。したがって、1台のマシンが電源オンになります。
  - 電源オンになったマシン（M1）の負荷インデックス値は、ベースライン負荷（負荷インデックスは0）です。
- 最初のユーザーがログオンします
  - セッションはマシンM1でホストされるように指示されます。
  - 電源オンになったマシンM1の負荷インデックスが増加し、マシンM1はベースライン負荷ではなくなります。
  - 構成されたキャパシティバッファにより、Autoscale は需要を満たすために追加のマシン (M2) の電源をオンにし始めます。
  - マシン M2 の負荷インデックス値はベースライン負荷にあります。
- ユーザーが負荷を増加させます
  - セッションはマシン M1 と M2 の間で負荷分散されます。その結果、起動中のマシン (M1 と M2) の負荷インデックスが増加します。
  - 総予備容量は、負荷インデックスの観点から依然として 10,000 を超えるレベルにあります。
  - マシン M2 の負荷インデックス値はもはやベースライン負荷ではありません。
- より多くのユーザーセッションが開始されます
  - セッションはマシン (M1 と M2) の間で負荷分散されます。その結果、起動中のマシン (M1 と M2) の負荷インデックスがさらに増加します。
  - 負荷インデックスの観点から総予備容量が 10,000 を下回るレベルに低下すると、Autoscale は構成されたキャパシティバッファにより、需要を満たすために追加のマシン (M3) の電源をオンにし始めます。
  - マシン M3 の負荷インデックス値はベースライン負荷にあります。
- さらに多くのユーザーセッションが開始されます

    - セッションはマシン (M1 から M3) の間で負荷分散されます。その結果、起動中のマシン (M1 から M3) の負荷インデックスが増加します。
    - 総予備容量は、負荷インデックスの観点から 10,000 を超えるレベルにあります。
    - マシン M3 の負荷インデックス値はもはやベースライン負荷ではありません。

- セッション終了によりユーザーセッションの負荷が減少します
    - ユーザーがセッションからログオフするか、アイドルセッションがタイムアウトすると、M1からM3までのマシンで解放された容量が、他のユーザーが開始したセッションをホストするために再利用されます。
    - ロードインデックスの観点から総予備容量が10,000を超えるレベルに増加すると、Autoscaleはマシンの1つ（たとえばM3）をドレイン状態にします。その結果、新しい変更が発生しない限り、他のユーザーが開始したセッションはそのマシンに転送されなくなります。たとえば、エンドユーザーの負荷が再び増加したり、他のマシンの負荷が最も低くなったりした場合です。
- ユーザーセッションの負荷は減少し続けます
    - マシンM3上のすべてのセッションが終了し、指定された電源オフ遅延がタイムアウトすると、AutoscaleはマシンM3の電源をオフにします。
    - さらに多くのユーザーがセッションを終了すると、電源がオンになっているマシン（M1とM2）で解放された容量が、他のユーザーが開始したセッションをホストするために再利用されます。
    - ロードインデックスの観点から総予備容量が10,000を超えるレベルに増加すると、Autoscaleはマシンの1つ（たとえばM2）をドレイン状態にします。その結果、他のユーザーが開始したセッションはそのマシンに転送されなくなります。
- セッションがなくなるまでユーザーセッションの負荷は減少し続けます
    - マシンM2上のすべてのセッションが終了し、指定された電源オフ遅延がタイムアウトすると、AutoscaleはマシンM2の電源をオフにします。
    - 電源がオンになっているマシン（M1）のロードインデックス値はベースライン負荷です。構成された容量バッファーのため、AutoscaleはマシンM1をドレイン状態にしません。

> **注:**

> マルチセッションOSデリバリーグループの場合、ユーザーがセッションからログオフすると、デスクトップへのすべての変更は失われます。ただし、構成されている場合、ユーザー固有の設定はユーザープロファイルとともにローミングされます。

シングルセッションOSランダムデリバリーグループ

容量バッファーは、デリバリーグループ内のマシンの総数に基づいて、電源がオンになっているマシンのバッファーを維持することで、需要の急増に対応するために使用されます。デフォルトでは、容量バッファーはデリバリーグループ内のマシンの総数の10%です。

マシンの数（容量バッファーを含む）が現在電源がオンになっているマシンの総数を超える場合、需要を満たすために追加のマシンの電源がオンになります。マシンの数（容量バッファーを含む）が現在電源がオンになっているマシンの総数よりも少ない場合、余分なマシンは、構成したアクションに応じてシャットダウンまたは中断されます。

電源ポリシー

さまざまなシナリオでマシンの電源を管理するポリシーを構成します。各シナリオについて、待機時間（分単位）と、指定された時間が終了した後に実行するアクションを指定できます。電源ポリシーは、シングルセッションOSランダムデリバリーグループおよびシングルセッションOS静的デリバリーグループに適用されます。

電源ポリシーのアクション(/en-us/citrix-virtual-apps-desktops/current-release/media/power-policies-actions.png)

切断後、ピーク時とオフピーク時の両方で、以下の設定が適用されます。

- ドロップダウンから、待機時間を分単位で設定し、「アクションなし」、「一時停止」、「シャットダウン」などのアクションを選択できます。
- 一時停止アクションを選択した場合、マシンをシャットダウンするための追加の待機時間を構成します。

> **注:**
>
> - ピーク時およびオフピーク時において、シャットダウンアクションの待機時間は、一時停止の待機時間よりも長くする必要があります。
> - 一時停止されたマシンは、切断されたユーザーが再接続した場合にのみアクセス可能です。一時停止されたマシンを新規ユーザーが利用できるようにするには、シャットダウンしてください。

- 一時停止フィールドとシャットダウンフィールドの時刻設定が正しく構成されていない場合、**保存**オプションが無効になり、設定エラーを示す赤い点もナビゲーション項目の横に表示されます。

シングルセッションOSランダムDG電源ポリシー設定(/en-us/citrix-virtual-apps-desktops/current-release/media/single-session-os-random-dg-power-policies-settings.png)

例

- 待機時間を12分に設定し、最初のアクションを「アクションなし」に選択した場合、12分経過後もマシンは電源オン状態を維持します。
- 待機時間を15分に設定し、最初のアクションを「一時停止」、2番目の待機時間を20分に選択した場合、15分経過後にマシンは一時停止されます。2番目の待機時間経過後にマシンはシャットダウンされます。
- 待機時間を18分に設定し、最初のアクションを「シャットダウン」に選択した場合、18分経過後にマシンはシャットダウンされます。

例のシナリオ

次のシナリオを想定します。

- **デリバリーグループの構成**。Autoscaleで電源管理するデリバリーグループには、10台のマシン（M1～M10）が含まれています。
- **Autoscaleの構成**
  - 容量バッファは10%に設定されています。
  - 選択されたスケジュールにはマシンが含まれていません。

シナリオは次の順序で実行されます。

1. ユーザーはログオンしません。
2. ユーザーセッションが増加します。
3. さらに多くのユーザーセッションが開始されます。
4. セッション終了により、ユーザーセッションの負荷が減少します。
5. オンプレミスリソースのみでセッション負荷が処理されるまで、ユーザーセッションの負荷はさらに減少します。

上記のシナリオでAutoscaleがどのように機能するかについては、以下を参照してください。

- ユーザー負荷なし（初期状態）
  - 1台のマシン（M1）が電源オンになります。このマシンは、構成された容量バッファのために電源オンになります。この場合、10（マシンの数）x 10%（構成された容量バッファ）は1に等しくなります。したがって、1台のマシンが電源オンになります。
- 最初のユーザーがログオンします
  - ユーザーがデスクトップを使用するために初めてログオンすると、電源オンになっているマシンでホストされているデスクトップのプールからデスクトップが割り当てられます。この場合、ユーザーにはマシンM1からデスクトップが割り当てられます。
  - Autoscaleは、構成された容量バッファのために需要を満たすために、追加のマシン（M2）の電源をオンにし始めます。
- 2番目のユーザーがログオンします
  - ユーザーにはM2マシンからデスクトップが割り当てられます。
  - 設定されたキャパシティバッファにより需要を満たすため、Autoscaleは追加のマシン（M3）の電源をオンにし始めます。
- 3人目のユーザーがログオンします
  - ユーザーにはM3マシンからデスクトップが割り当てられます。
  - 設定されたキャパシティバッファにより需要を満たすため、Autoscaleは追加のマシン（M4）の電源をオンにし始めます。
- ユーザーがログオフします
  - ユーザーがログオフするか、ユーザーのデスクトップがタイムアウトすると、解放された容量（例：M3）がバッファとして利用可能になります。その結果、キャパシティバッファが10%に設定されているため、AutoscaleはM4マシンの電源をオフにし始めます。
- ユーザーがいなくなるまで、さらに多くのユーザーがログオフします
  - さらに多くのユーザーがログオフした後、Autoscaleはマシン（例：M2またはM3）の電源をオフにします。
  - ユーザーが残っていなくても、そのマシンは予備容量として予約されているため、Autoscaleは残りの1台のマシン（例：M1）の電源をオフにしません。

> **注:**

> シングルセッションOSのランダムデリバリーグループの場合、ユーザーがセッションをログオフすると、デスクトップへのすべての変更は失われます。ただし、設定されている場合、ユーザー固有の設定はユーザープロファイルとともにローミングされます。

シングルセッションOSの静的デリバリーグループ

キャパシティバッファは、デリバリーグループ内の未割り当てマシンの総数に基づいて、未割り当てマシンのバッファの電源をオンに保つことで、急な需要の急増に対応するために使用されます。デフォルトでは、キャパシティバッファはデリバリーグループ内の未割り当てマシンの総数の10%です。

> **重要:**
>
> デリバリーグループ内のすべてのマシンが割り当てられた後、キャパシティバッファはマシンの電源オン/オフには関与しません。

> マシンの数（キャパシティバッファを含む）が現在電源がオンになっているマシンの総数を超える場合、需要を満たすために追加の未割り当てマシンが電源オンになります。マシンの数（キャパシティバッファを含む）が現在電源がオンになっているマシンの総数よりも少ない場合、設定したアクションに応じて、余分なマシンは電源オフまたは一時停止されます。

シングルセッションOS静的デリバリーグループの場合、Autoscaleは次のようになります。

- 適用されるシングルセッションOSデリバリーグループの`AutomaticPowerOnForAssigned`プロパティがtrueに設定されている場合にのみ、ピーク時に割り当てられたマシンをオンにし、オフピーク時にオフにします。
- マシンがオフになっていて、そのマシンが属するデリバリーグループの`AutomaticPowerOnForAssignedDuringPeak`プロパティがtrueに設定されている場合、ピーク時に自動的にマシンをオンにします。

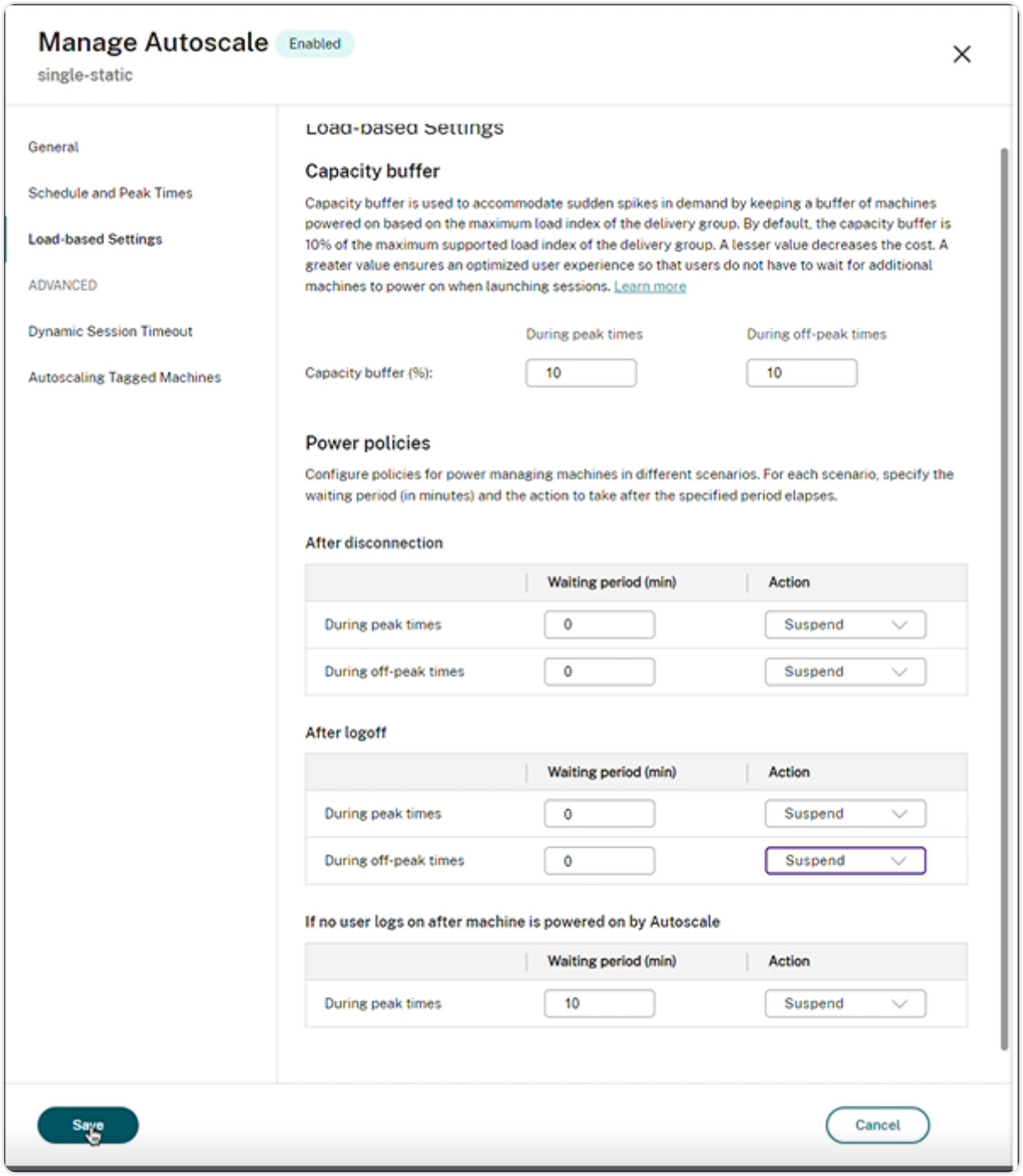
割り当てられたマシンで容量バッファがどのように機能するかを理解するには、以下を考慮してください。

- 容量バッファは、デリバリーグループに1台以上の未割り当てのマシンがある場合にのみ機能します。
- デリバリーグループに未割り当てのマシンがない場合（デリバリーグループ内のすべてのマシンが割り当てられている場合）、容量バッファはマシンの電源オン/オフには関与しません。

- `AutomaticPowerOnForAssignedDuringPeak`プロパティは、ピーク時に割り当てられたマシンの電源がオンになるかどうかを決定します。trueに設定されている場合、Autoscaleはピーク時にマシンの電源をオンのままにします。Autoscaleは、電源がオフになっている場合でも、それらの電源をオンにします。

電源ポリシー

さまざまなシナリオに合わせてマシンの電源を管理するポリシーを構成します。各シナリオについて、待機時間（分単位）と、指定された時間が終了した後に実行するアクションを指定できます。電源ポリシーは、シングルセッションOSランダムデリバリーグループとシングルセッションOS静的デリバリーグループに適用されます。



切断後および**ログオフ後**の場合、以下の設定はピーク時とオフピーク時の両方に適用されます。ドロップダウンから、待機時間（分単位）と、アクション（アクションなし、一時停止、シャットダウンなど）を設定できます。

Autoscaleによってマシンの電源がオンになった後、ユーザーがログオンしない場合、以下の設定はピーク時にのみ適用されます。ピーク時にドロップダウンから、待機時間（分単位）と、アクション（アクションなし、一時停止、シャットダウンなど）を設定できます。

例のシナリオ

次のシナリオを想定します。

- **デリバリーグループの構成**。Autoscaleで電源管理したいデリバリーグループには、10台のマシン（M1～M10）が含まれています。
- **Autoscaleの構成**
  - M1からM3までのマシンは割り当て済みで、M4からM10までのマシンは未割り当てです。
  - ピーク時およびオフピーク時のキャパシティバッファは10%に設定されています。
  - 選択されたスケジュールに従って、Autoscaleは午前9時から午後6時までマシンの電源を管理します。

上記のシナリオでAutoscaleがどのように機能するかについては、以下を参照してください。

- スケジュールの開始 – 午前9時
  - AutoscaleはマシンM1からM3の電源をオンにします。
  - 設定されたキャパシティバッファのため、Autoscaleは追加のマシン（例：M4）の電源をオンにします。マシンM4は未割り当てです。
- 最初のユーザーがログオンします
  - ユーザーがデスクトップを使用するために初めてログオンすると、未割り当ての電源オン状態のマシンでホストされているデスクトップのプールからデスクトップが割り当てられます。この場合、ユーザーにはマシンM4からデスクトップが割り当てられます。そのユーザーによるその後のログオンは、初回使用時に割り当てられた同じデスクトップに接続されます。
  - 設定されたキャパシティバッファのため、Autoscaleは需要を満たすために追加のマシン（例：M5）の電源をオンにし始めます。
- 2番目のユーザーがログオンします

    - ユーザーには、未割り当ての電源オン状態のマシンからデスクトップが割り当てられます。この場合、ユーザーにはマシンM5からデスクトップが割り当てられます。そのユーザーによるその後のログオンは、初回使用時に割り当てられた同じデスクトップに接続されます。
    - 設定されたキャパシティバッファのため、Autoscaleは需要を満たすために追加のマシン（例：M6）の電源をオンにし始めます。

- ユーザーがログオフします
    - ユーザーがデスクトップからログオフするか、デスクトップがタイムアウトすると、Autoscaleは午前9時から午後6時までマシンM1からM5の電源をオンのままにします。それらのユーザーが次回ログオンするときは、初回使用時に割り当てられた同じデスクトップに接続されます。
    - 割り当てられていないマシン M6 は、新しく割り当てられていないユーザーにデスクトップを提供するのを待機しています。

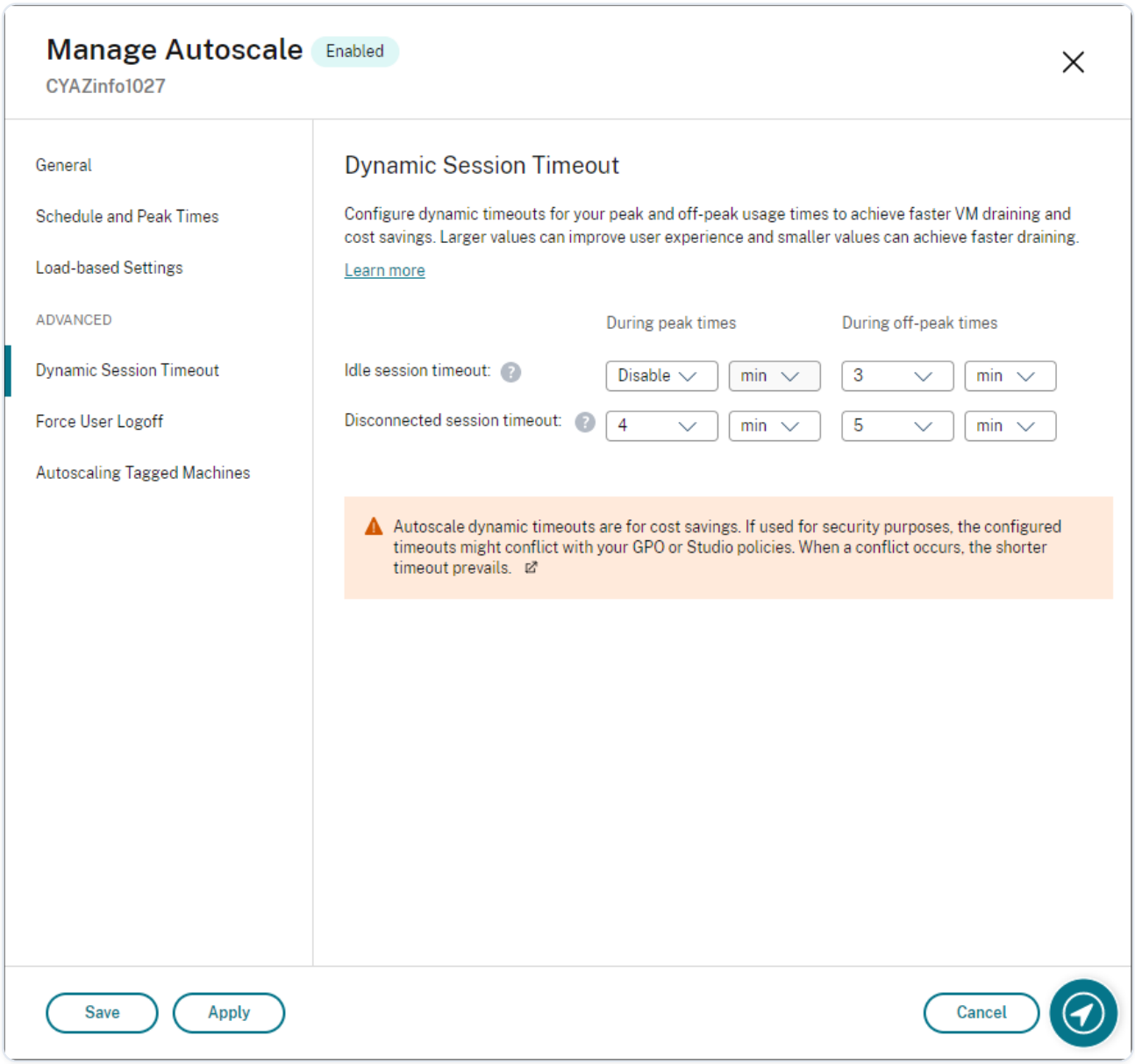
- スケジュールの終了 – 午後 6 時
    - 午後 6 時に、Autoscale はマシン M1 から M5 の電源をオフにします。
    - Autoscale は、構成された容量バッファのため、割り当てられていないマシン M6 の電源をオンのままにします。そのマシンは、新しく割り当てられていないユーザーにデスクトップを提供するのを待機しています。
    - デリバリーグループでは、マシン M6 から M10 は割り当てられていないマシンです。

動的セッションタイムアウト

この機能を使用すると、ピーク時とオフピーク時の使用時間に合わせて切断セッションとアイドルセッションのタイムアウトを設定し、マシンのドレインを高速化してコストを削減できます。この機能は以下に適用されます。

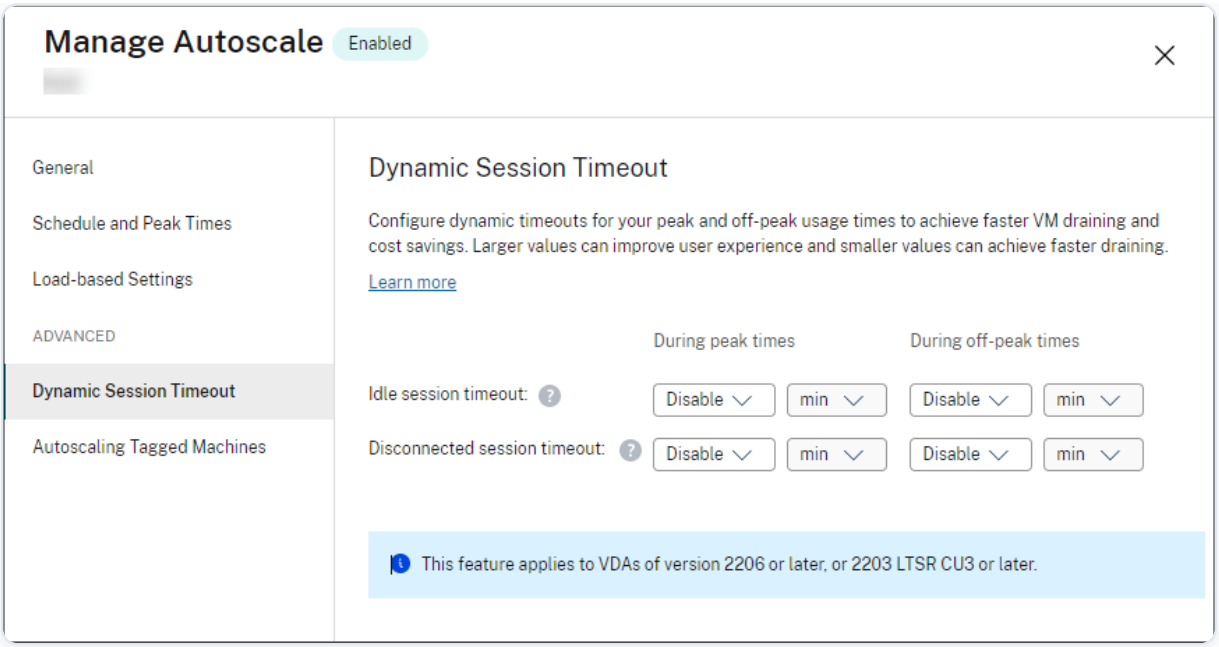
- シングルセッションおよびマルチセッションOSマシン。
- オートスケール用にタグ付けされているかどうかにかかわらず、デリバリーグループ内のすべてのマシン。

VDAは、10分以上アイドル状態のセッションのアイドル時間を報告するため、動的セッションタイムアウトは、アイドル状態になってから10分以内にアイドルセッションを切断することはできません。値を小さくすると、残存するセッションがより早く削除され、コストが削減されます。



注:

- この機能は、マルチセッションOSデリバリーグループで常に利用可能です。
- シングルセッションOSデリバリーグループの場合、この機能はバージョン2206 CR以降、または2203 LTSR CU3以降のVDAに適用されます。これらのVDAがCitrix Cloud™に少なくとも1回登録されていることを確認してください。利用できない場合、次のユーザーインターフェイスが表示されます。



- Autoscale™の動的タイムアウトはコスト削減を目的としています。セキュリティ目的で使用する場合、設定されたタイムアウトがGPOまたは管理コンソールポリシーと競合する可能性があります。競合が発生した場合、短い方のタイムアウトが優先されます。

アイドルセッションタイムアウト。ユーザー入力がない場合に、中断されていないユーザー接続が維持される時間を指定するタイマーを有効または無効にします。タイマーが期限切れになると、セッションは切断状態になり、**切断セッションタイムアウト**が適用されます。**切断セッションタイムアウト**が無効になっている場合、セッションはログオフされません。

重要:

- 10分（600秒）以下の値を指定した場合、Autoscaleは関連するセッションが10分間アイドル状態になった後に切断します。これは、AutoscaleがVDAが報告するセッションのアイドル時間に依存しているためです。VDAは、10分以上アイドル状態のセッションに対してのみアイドル時間を報告します。
- アイドルセッションは、アイドルセッションタイムアウトに達するまでの最後の5分以内にユーザーが操作した場合でも、切断状態になることがあります。

> **切断セッションタイムアウト**。切断されたデスクトップがログオフされるまでロックされたままになる時間を指定するタイマーを有効または無効にします。有効になっている場合、タイマーが期限切れになると切断されたセッションはログオフされます。

よくある質問

動的セッションタイムアウト機能は、オートスケール用にタグ付けされたマシンにのみ適用されます?

動的セッションタイムアウト機能は、オートスケール用にタグ付けされているかどうかにかかわらず、デリバリーグループ内のすべてのマシンに適用されます。

動的セッションタイムアウトによりセッションがログオフされた場合、タグ付けされていないマシンも、タグ付けされたマシンのオートスケールターゲットに含まれます?

動的セッションタイムアウト機能は、オートスケールのタグ付け機能とは関係ありません。動的セッションタイムアウトによってセッションが終了した場合、マシンがシャットダウンまでドレインされている限り、タグ付けされていないマシンもその過程でシャットダウンされる可能性があります。

タグ付けされたマシンのオートスケール (クラウドバースト)

> **注:**
>
> この機能は以前、Restrict Autoscale と呼ばれていました。

はじめに

Autoscaleは、デリバリーグループ内のマシンの一部のみを電源管理する柔軟性を提供します。これを実現するには、1つ以上のマシンにタグを適用し、その後、Autoscaleを構成してタグ付きマシンのみを電源管理します。

この機能は、クラウドベースのリソースが追加の需要 (つまり、バーストワークロード) に対応する前に、オンプレミスリソース (または予約済みのパブリッククラウドインスタンス) を使用してワークロードを処理したいクラウドバーストのユースケースで役立ちます。オンプレミスのマシン (または予約済みインスタンス) に最初にワークロードを処理させるには、タグ制限とゾーン優先度を併用する必要があります。

タグ制限は、Autoscale によって電源管理されるマシンを指定します。ゾーン優先度は、ユーザー起動要求を処理する優先ゾーン内のマシンを指定します。詳細については、「タグ」および「ゾーン優先度」を参照してください。

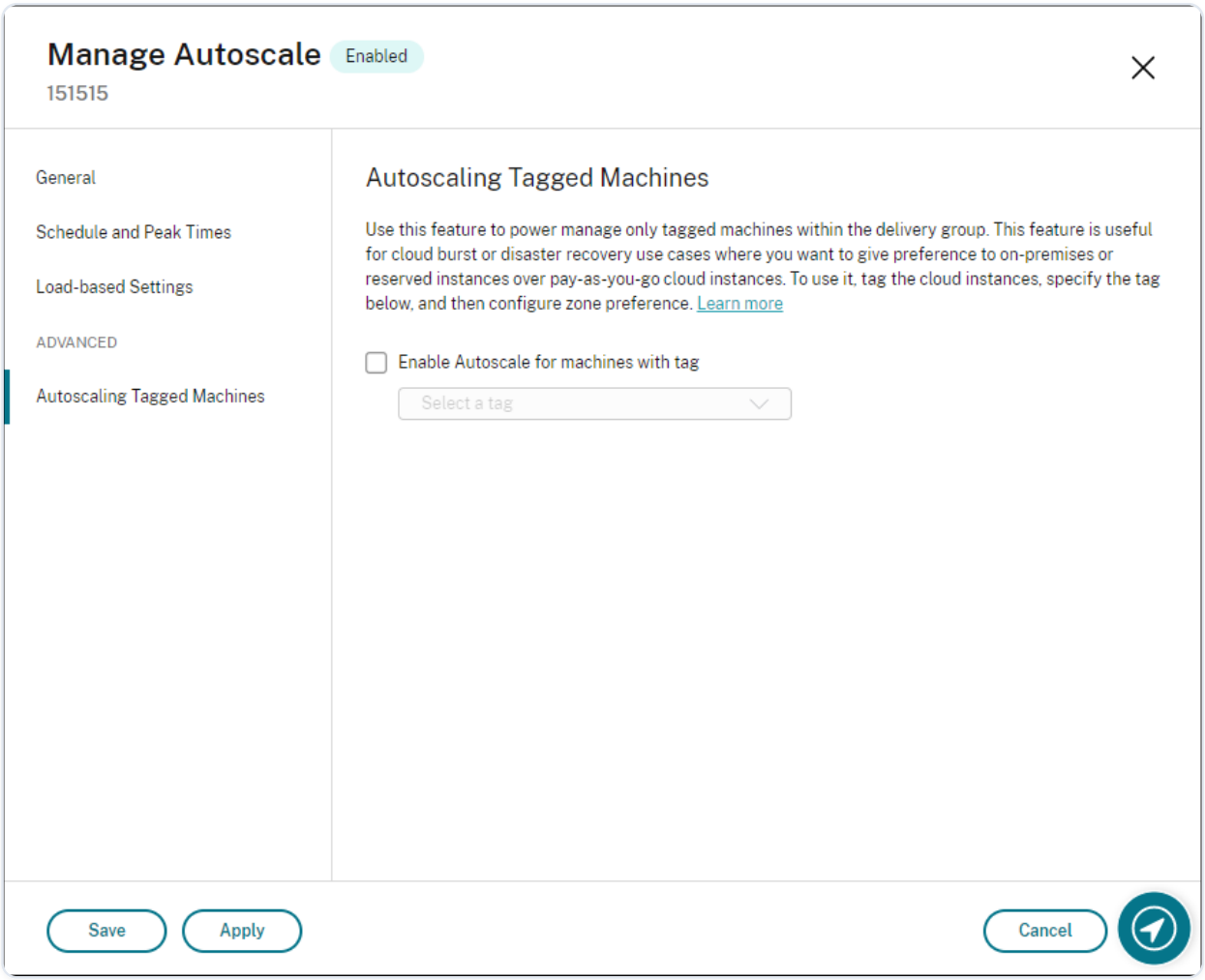
特定のタグ付きマシンをオートスケールするには、Manage コンソールまたは PowerShell を使用できます。

Manage コンソールを使用して特定のタグ付きマシンをオートスケールする

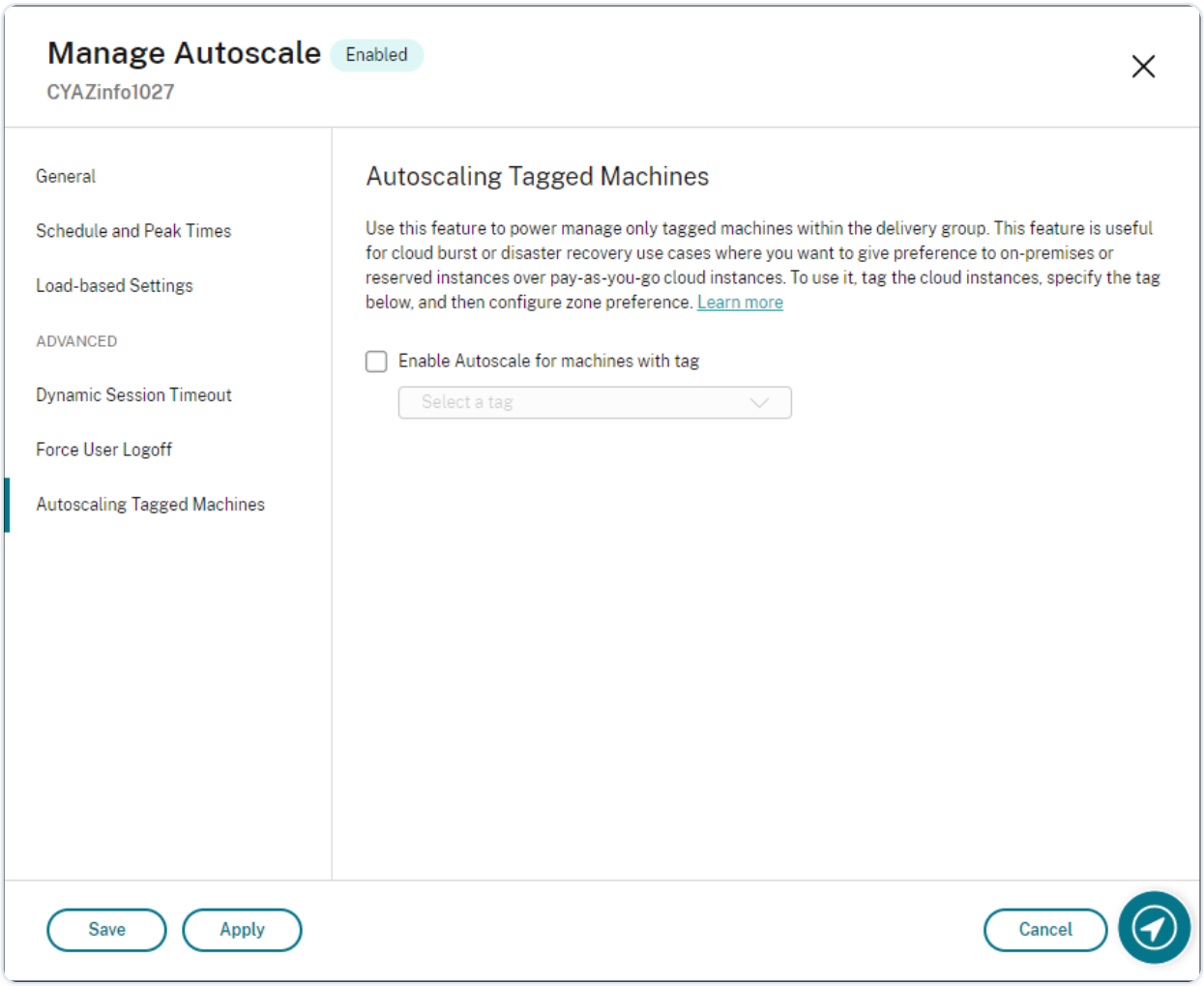
特定のタグ付きマシンをオートスケールするには、次の手順を実行します。

1. タグを作成し、そのタグをデリバリーグループ内の該当するマシンに適用します。詳細については、「タグとタグ制限の管理」を参照してください。
2. デリバリーグループを選択し、**Manage Autoscale** ウィザードを開きます。
3. **タグ付きマシンのオートスケール**ページで、**タグ付きマシンのオートスケールを有効にする**を選択し、リストからタグを選択して、**適用**をクリックして変更を保存します。

   シングルセッションOSの*静的*および*ランダム*なデリバリーグループのユーザーインターフェイス:



マルチセッションOSデリバリーグループのユーザーインターフェイス:



警告:

- 特定のタグを持つマシンをオートスケールすると、ヒストグラムが自動的に更新され、タグごとのマシンの数が反映される場合があります。**スケジュールとピーク時間**ページで、必要に応じて、各時間帯にマシンを手動で割り当てることができます。
- タグ付けされたマシンで使用されているタグは削除できません。タグを削除するには、まずタグの制限を解除する必要があります。

タグの制限を適用した後、後でデリバリーグループから削除したい場合があります。そのためには、**Autoscaleの管理 > タグ付けされたマシンのAutoscale**ページに移動し、**タグ付きマシンのAutoscaleを有効にする**のチェックを外します。

警告:

- **タグ付きマシンのAutoscaleを有効にする**のチェックを外さずに、該当するマシンからタグを削除すると、**Autoscaleの管理**ウィザードを開いたときに警告が表示されることがあります。マシンからタグを削除すると、Autoscaleで指定したタグが無効になるため、Autoscaleが管理するマシンがなくなる可能性があります。この警告を解決するには、**タグ付けされたマシンのAutoscale**ページに移動し、無効なタグを削除してから、**適用**をクリックして変更を保存します。

Autoscaleがリソースの電源をオンにするタイミングを制御する

タグ付けされていないマシンの使用状況に基づいて、Autoscaleがタグ付けされたマシンの電源をオンにし始めるタイミングを制御することもできます。これにより、タグ付けされたワークロードまたはパブリッククラウドワークロードの消費をさらに最適化できます。

これを行うには、次の手順を完了します。

1. **タグ付けされたマシンのAutoscale**ページで、**Autoscaleがタグ付けされたマシンの電源をオンにし始めるタイミングを制御する**を選択します。
2. ピーク時とオフピーク時の両方で到達させたいタグ付けされていないマシンの使用率をパーセンテージで入力し、**適用**をクリックします。サポートされる値: 0〜100。

Autoscaleがタグ付けされたマシンの電源をオンにし始めるタイミングを制御する(/en-us/citrix-virtual-apps-desktops/current-release/media/autoscale-powers-on-tagged-machines.png)

ヒント:

このパーセンテージは、Autoscaleがタグ付けされたマシンの電源をオンにし始めるタイミングを制御します。パーセンテージがしきい値（デフォルトは10%）を下回ると、Autoscaleはタグ付けされたマシンの電源をオンにし始めます。パーセンテージがしきい値を超えると、Autoscaleは電源オフモードになります。パーセンテージを入力する際は、次の2つのシナリオを考慮してください。

- シングルセッションOSデリバリーグループの場合: この値は、アイドル状態のタグ付けされていないマシンの総数に対するパーセンテージとして定義されます。例: タグ付けさ

れていないシングルセッションOSマシンが10台あります。セッションがないマシンが1台だけになったときに、Autoscaleはタグ付けされたマシンの電源をオンにし始めます。

- マルチセッションOSデリバリーグループの場合: この値は、利用可能なタグ付けされていないマシンの総容量（負荷インデックスの観点から）に対するパーセンテージとして定義されます。例: タグ付けされていないマルチセッションOSマシンが10台あります。それらが90%ロードされたときに、Autoscaleはタグ付けされたマシンの電源をオンにし始めます。

PowerShellを使用して特定のタグ付けされたマシンをAutoscaleする

注:

`Get-BrokerMachine` PowerShellコマンドは非推奨です。代わりに`Get-BrokerMachineV2`を使用してください。

PowerShell SDKを直接使用するには、次の手順を完了します。

1. **タグを作成します。** New-Brokertag PowerShellコマンドを使用してタグを作成します。
   - 例: `$managed = New-BrokerTag Managed`。この場合、タグ名は「Managed」です。New-Brokertag PowerShellコマンドの詳細については、`<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/New-BrokerTag/>`を参照してください。
2. **タグをマシンに適用します**。Get-Brokermachine PowerShellコマンドを使用して、Autoscaleで電源管理するカタログ内のマシンにタグを適用します。
   - 例: `Get-BrokerMachine -CatalogName "cloud" | Add-BrokerTag $managed.Name`。この場合、カタログ名は「cloud」です。
   - Get-Brokermachine PowerShellコマンドの詳細については、`<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerMachine/>`を参照してください。

注:

> タグを適用した後で、新しいマシンをカタログに追加する場合があります。その場合、タグは新しいマシンに自動的に適用*されません*。

3. **タグ付けされたマシンを、Autoscaleで電源管理するデリバリーグループに追加します。** Get-BrokerDesktopGroup PowerShellコマンドを使用して、マシンを含むデリバリーグループにタグ制限を追加します（つまり、「タグXを持つマシンへの起動を制限する」）。
   - 例: `Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscaleTagUid $managed.Uid`。この場合、デリバリーグループのUIDは1です。
   - Get-BrokerDesktopGroup PowerShellコマンドの詳細については、`<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/>`を参照してください。

タグ制限を適用した後、後でデリバリーグループから削除したい場合があります。その場合は、Get-BrokerDesktopGroup PowerShellコマンドを使用します。

例: `Get-BrokerDesktopGroup –Uid 1 | Set-BrokerDesktopGroup –RestrictAutoscaleTagUid $null`。この場合、デリバリーグループのUIDは1です。

> **注:**
>
> タグ付けされていないマシンは、ユーザーが電源を切った後に自動的に再起動します。この動作により、ワークロードをより早く処理できるようになります。これは、`Set-BrokerDesktopGroup`の`AutomaticRestartForUntaggedMachines`プロパティを使用して、デスクトップグループごとに有効または無効にできます。詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>`を参照してください。

例のシナリオ

次のシナリオを想定します。

- **マシンカタログの構成**。2つのマシンカタログ（C1とC2）があります。
  - カタログC1には、オンプレミス展開でローカルにある5台のマシン（M1～M5）が含まれています。

    - カタログC2には、クラウド展開でリモートにある5台のマシン（M6～M10）が含まれています。

- **タグの制限**。「Cloud」という名前のタグが作成され、カタログC2内のマシンM6からM10に適用されます。
- **ゾーン構成**。2つのゾーン（Z1とZ2）が作成されます。
    - カタログC1を含むゾーンZ1は、オンプレミス展開に対応します。
    - カタログC2を含むゾーンZ2は、クラウド展開に対応します。
- **デリバリーグループ構成**
    - デリバリーグループには10台のマシン（M1～M10）が含まれており、そのうち5台はカタログC1（M1～M5）から、残りの5台はカタログC2（M6～M10）からのものです。
    - マシンM1からM5は手動で電源がオンにされ、スケジュール期間中ずっと電源がオンのままになります。
- **Autoscale構成**
    - 容量バッファは10%に設定されています。
    - Autoscaleは、「Cloud」タグが付いたマシンのみを電源管理します。この場合、Autoscaleはクラウドマシン M6からM10を電源管理します。
- **公開アプリケーションまたはデスクトップ構成**。公開デスクトップ（例）にはゾーン設定が構成されており、ユーザー起動要求ではゾーンZ2よりもゾーンZ1が優先されます。
    - ゾーンZ1は、公開デスクトップの優先ゾーン（ホームゾーン）として構成されています。

このシナリオは、次の順序で実行されます。

1. ユーザーはログオンしません。
2. ユーザーセッションが増加します。
3. ユーザーセッションは、利用可能なすべてのオンプレミス マシンが消費されるまでさらに増加します。
4. さらに多くのユーザーセッションが開始されます。
5. セッション終了により、ユーザーセッションが減少します。
6. セッション負荷がオンプレミス マシンのみで処理されるまで、ユーザーセッションはさらに減少します。

上記のシナリオでAutoscaleがどのように機能するかについては、以下を参照してください。

- ユーザー負荷なし（初期状態）
  - オンプレミス マシン M1～M5 はすべて電源がオンになっています。
  - クラウド内の1台のマシン（例: M6）の電源がオンになります。このマシンは、構成された容量バッファのために電源がオンになります。この場合、10（マシン数）x 10,000（負荷インデックス）x 10%（構成された容量バッファ）は10,000に等しくなります。したがって、1台のマシンの電源がオンになります。
  - 電源がオンになっているすべてのマシン（M1～M6）の負荷インデックス値は、ベースライン負荷（負荷インデックスは0）です。
- ユーザーがログオンします
  - セッションは、構成されたゾーン設定を通じてマシン M1～M5 でホストされるように指示され、これらのオンプレミス マシン間で負荷分散されます。
  - 電源がオンになっているマシン（M1～M5）の負荷インデックス値が増加します。
  - 電源がオンになっているマシン M6 の負荷インデックス値は、ベースライン負荷です。
- ユーザーが負荷を増やし、すべてのオンプレミス リソースを消費します
  - セッションは、構成されたゾーン設定を通じてマシン M1～M5 でホストされるように指示され、これらのオンプレミス マシン間で負荷分散されます。
  - 起動中のすべてのマシン (M1～M5) のロードインデックス値が10,000に達しました。
  - 起動中のマシンM6のロードインデックス値は、ベースライン負荷のままです。
- もう1人のユーザーがログオンします
  - セッションはゾーン設定を超過し、クラウドマシンM6でホストされるように指示されます。
  - 起動中のすべてのマシン (M1～M5) のロードインデックス値が10,000に達しました。
  - 起動中のマシンM6のロードインデックス値は増加し、ベースライン負荷ではなくなります。ロードインデックスで合計予備容量が10,000を下回るレベルに低下すると、構成された容量バッファのため、Autoscaleは需要を満たすために追加のマシン (M7) の電源をオンにし始めます。マシンM7の電源をオンにするには時間がかかる場合があることに注意してください。そのため、マシンM7が準備できるまでに遅延が発生する可能性があります。
- さらに多くのユーザーがログオンします
  - セッションはマシンM6でホストされるように指示されます。
  - 起動中のすべてのマシン (M1～M5) のロードインデックス値が10,000に達しました。

  - 起動中のマシンM6のロードインデックス値はさらに増加しますが、ロードインデックスで合計予備容量は10,000を上回るレベルにあります。
  - 起動中のマシンM7のロードインデックス値は、ベースライン負荷のままです。
- さらに多くのユーザーがログオンします
  - マシンM7の準備ができた後、セッションはマシンM6とM7でホストされるように指示され、これらのマシン間で負荷分散されます。
  - 起動中のすべてのマシン (M1～M5) のロードインデックス値が10,000に達しました。
  - マシンM7のロードインデックス値は、ベースライン負荷ではなくなります。
  - 稼働中のマシン (M6 および M7) の負荷インデックス値が増加します。
  - 負荷インデックスの観点から、総予備容量は依然として10,000を超えるレベルにあります。
- セッション終了により、ユーザーセッションの負荷が減少します。
  - ユーザーがセッションからログオフするか、アイドルセッションがタイムアウトすると、マシンM1からM7で解放された容量は、他のユーザーが開始したセッションをホストするために再利用されます。
  - 負荷インデックスの観点から総予備容量が10,000を超えるレベルに増加すると、Autoscaleはクラウドマシン (M6からM7) の1つをドレイン状態にします。その結果、新しい変更が発生しない限り、他のユーザーが開始したセッションはそのマシン (たとえばM7) には転送されなくなります。たとえば、ユーザー負荷が再び増加したり、他のクラウドマシンの負荷が最も低くなったりした場合です。
- 1つ以上のクラウドマシンが不要になるまで、ユーザーセッションの負荷はさらに減少します。
  - マシンM7上のすべてのセッションが終了し、指定された電源オフ遅延がタイムアウトすると、Autoscaleはマシンの電源をオフにします。
  - 稼働中のすべてのマシン (M1からM5) の負荷インデックス値は、10,000を下回るレベルに低下する可能性があります。
  - 稼働中のマシン (M6) の負荷インデックス値が減少します。
- クラウドマシンが不要になるまで、ユーザーセッションはさらに減少します。
  - マシンM6にユーザーセッションがない場合でも、Autoscaleは予備容量として予約されているため、電源をオフにしません。

- Autoscaleは、構成された容量バッファのため、残りのクラウドマシンM6の電源をオンのままにします。そのマシンは、着信するユーザーにデスクトップを提供するのを待機しています。
- オンプレミス環境のマシンに利用可能な容量がある限り、セッションはマシンM6でホストされるようには転送されません。

Autoscale™ プラグイン

Autoscale プラグインは、VM の電源管理に直接アクションを実行できるプラグインモデルです。VM の電源管理に関連する標準の Autoscale 設定から逸脱し、代わりに、さまざまなシナリオに合わせて異なる設定を行うことができます。現在、使用できるプラグインは次のとおりです。

- Autoscale ホリデープラグイン
- Intelligent Autoscale スケジュールプラグイン

Autoscale ホリデープラグイン

Autoscale ホリデープラグインを使用して、休日に対して異なる設定を処理できます。たとえば、平日にはほとんどの VM を電源オンにしたいとします。ただし、デフォルトでは (プラグインなしでは)、平日スケジュールが祝日にも適用されます。このシナリオを処理するために、プラグインは指定された休日に VM を電源オフにすることを許可します。

Studio を使用してカスタムホリデースケジュールを作成する

Studio を使用してカスタムスケジュールを作成し、休日などの特定の日にデリバリーグループ内の未使用の VM を電源オフにして、不要なリソース消費を削減します。

> **注:**
>
> - カスタムスケジュールは作成の翌日に有効になります。
> - タグ付けされたマシンの場合、この機能はデリバリーグループ内のタグ付けされたマシンにのみ適用されます。

カスタムスケジュールを作成するには:

1. Studio で、**Delivery groups** に移動します。デリバリーグループを右クリックし、**Manage Autoscale** を選択します。
2. **General** ページで、**Enable Autoscale** を選択します。

3. **Schedule**ページで、**Create schedule**をクリックします。
4. スケジュールの名前を入力します。
5. デリバリーグループ内の VM を電源オフにする日付を1つまたは複数選択します。

   このスケジュールを他のデリバリーグループで使用するためのテンプレートとして保存する場合は、**Save as template** をクリックします。
6. カスタムスケジュールを作成するには、**完了**をクリックします。

   これで、**スケジュール**ページの**カスタム**の下に作成されたカスタムスケジュールが表示されるはずです。

カスタムスケジュールを編集するには:

1. 編集したいスケジュールについて、**アクション**の下にある鉛筆アイコンをクリックします。次の編集が可能です:
   - カスタムスケジュールを無効にする: **有効**トグルボタンをオフにします。
   - テンプレートを変更または適用します。
   - スケジュールの名前を変更します。
   - スケジュールの日付を変更します。
2. 変更を適用するには、**完了**をクリックします。

カスタムスケジュールを削除することもできます。

> **注:**
>
> デリバリーグループを削除すると、そのカスタムスケジュールも削除されます。保存されたテンプレートは削除されません。

PowerShell を使用して休日の日付を構成する

Autoscale ホリデープラグインをデリバリーグループに関連付け、休日の日付を構成します。これにより、プラグインは構成された日付に VM の電源をオフにできるようになります。これを実現するには、次のコマンドを実行します:

1. `Get-BrokerAutoscalePlugin` を実行して、ホリデープラグインの UID を取得します。

```
(Get-BrokerAutoscalePlugin -Name
Citrix.AutoscalePlugin.HolidaySchedule).Uid
```

`HolidaySchedule` プラグインの UID 値をメモします。`HolidaySchedule` プラグインの UID が 1 であると仮定します。

2. プラグインを関連付けたいデリバリーグループのUIDを取得します。例：

```
$dgUid = (Get-BrokerDesktopGroup 'My Group Name').Uid
```

3. `HolidaySchedule` プラグインをデリバリーグループ `(-AutoscalePluginUid “<HolidaySchedule plugin UID>”)` に関連付け、必要な祝日を指定します。例：

```
New-BrokerAutoscaleGroupPlugin -Name "Company Holidays"
-DesktopGroupUid $dgUid -AutoscalePluginUid 1 -Configuration
'{"Holidays":["2024-11-28","2024-11-29","2024-12-25"]}'
```

作成された `AutoscaleGroupPlugin`（プラグインとデリバリーグループ間の関連付け）のUIDをメモします。

> **注:**
>
> 関連付けの名前は、特定のデリバリーグループの関連付けの中で一意である必要があります。たとえば、1つのデリバリーグループに対して「Company Holidays」という名前の関連付けは1つしか存在できませんが、他の1つ以上のデリバリーグループも「Company Holidays」という名前の関連付けを持つことができます。

祝日を変更する

指定された祝日は、`Set-BrokerAutoscaleGroupPlugin` PowerShellコマンドを使用し、`AutoscaleGroupPlugin` のUIDを指定することで変更できます。たとえば、`AutoscaleGroupPlugin` のUIDが2であると仮定します。

```
Set-BrokerAutoscaleGroupPlugin 2 -Configuration '{"Holidays":
["2024-11-28","2024-11-29"]}'
```

重要な考慮事項

Autoscaleホリデープラグインを使用する際は、次の点を考慮してください。

- Autoscaleホリデープラグインがアクティブな場合、すべてのVDAはオフになり、システムは容量を削減して動作しません。新しい起動要求は処理されますが、VDAの起動準備のため、ユーザーは遅延を経験する可能性があります。
- デリバリーグループにはタイムゾーンが指定されている必要があります。
- 日付形式は「yyyy-mm-dd」である必要があります。
- スケジュールの上書き（標準のAutoscale設定を上書きするもの）は、前日の22:00に1日前に生成されます。22:00以降は、翌日のスケジュールの上書きを追加、削除、または変更することはできません。
- 同じAutoscaleプラグインを複数のデリバリーグループに関連付けることができます。各デリバリーグループに対して`New-BrokerAutoscaleGroupPlugin`を実行し、そのグループに必要な祝日を構成します。
- 最新の`Set-BrokerAutoscalePlugin -Configuration`コマンドは、既存のすべての祝日を、指定された新しい祝日で上書きします。

Intelligent Autoscaleスケジュールプラグイン

Intelligent Autoscaleは、最小限の管理設定でデリバリーグループのパフォーマンスターゲットを構成できる、データ駆動型のAutoscale機能です。パフォーマンスターゲット値は1から99の範囲で、この値はユーザーエクスペリエンスとコストの間の目標バランスを指定します。

- 値が低いほどコスト削減を優先します。
- 値が高いほどユーザーエクスペリエンスを優先します。

パフォーマンスターゲットは、過去の使用状況データと組み合わされて、1 日の 30 分ごとのブロックに対して最適なバッファ容量 (電源をオンにする VM の数) を計算します。したがって、毎日開始時に 48 の最適なバッファ容量が計算されます。

最適なバッファ容量は、利用可能なマシンを管理するために、ピーク時/オフピーク時のバッファ容量とプールサイズを置き換えます。

最適なバッファ容量を計算するために使用される過去の使用状況データは次のとおりです。

- 顧客のログオン率（1分あたりのユーザー数）
- 平均VM電源オン時間（分）
- 平均VM密度（VMあたりのユーザー数）.

前提条件

Intelligent Autoscaleを有効にするための要件は次のとおりです。

- デリバリーグループは共有デリバリーグループである必要があります。
- デリバリーグループはAutoscaleが有効になっている必要があります。
- デスクトップグループにIntelligent Autoscaleを設定する前に、デリバリーグループには少なくとも90日分の履歴データが必要です。`ConnectionLogLifetimeHours`を48時間から90日に増やすには、次のコマンドを使用します。

```
Set-BrokerServiceConfigurationData Logging.ConnectionLogLifetimeHours
-SettingValue 2160.
```

重要な考慮事項

- デリバリーグループにはタイムゾーンが指定されている必要があります。
- スケジュールの上書きは、前日の22:00に1日前に生成されます。22:00以降は、翌日のスケジュールの上書きを追加、削除、または変更することはできません。
- 同じAutoscaleプラグインを複数のデリバリーグループに関連付けることができます。各デリバリーグループに対して`New-BrokerAutoscaleGroupPlugin`を実行し、そのグループに必要なパフォーマンスターゲットを設定します。
- 最新の`Set-BrokerAutoscalePlugin -Configuration`コマンドは、既存のすべての休日を、指定された新しい休日で上書きします。

パフォーマンスターゲットの構成

`IntelligentAutoscaleSchedules`プラグインをデリバリーグループに関連付け、パフォーマンスターゲットを設定します。これにより、パフォーマンスターゲットと過去の使用状況データを組み合わせて、1日の30分ごとのブロックに最適なバッファ容量を計算できます。これを実現するには、次のコマンドを実行します。

1. Intelligent AutoscaleプラグインのUIDを取得するには、`Get-BrokerAutoscalePlugi`を実行します。`IntelligentAutoscaleSchedules`プラグインのUID値をメモします。

```
(Get-BrokerAutoscalePlugin -Name
Citrix.AutoscalePlugin.IntelligentAutoscaleSchedules).Uid
```

   `IntelligentAutoscaleSchedules`プラグインのUIDが2であると仮定します。

2. プラグインを関連付けたいデリバリーグループのUIDを取得します。例:

```
$dgUid = (Get-BrokerDesktopGroup 'My Group Name').Uid
```

3. `IntelligentAutoscaleSchedules`プラグインをデリバリーグループ(`-AutoscalePluginUid “<IntelligentAutoscaleSchedules value>”`)に関連付け、パフォーマンスターゲット値を指定します。

```
New-BrokerAutoscaleGroupPlugin -DesktopGroupUid $dgUid
-AutoscalePluginUid 2 -Configuration '{"PerformanceTarget":70}'
```

4. 作成された`AutoscaleGroupPlugin`のUIDをメモします (プラグインとデリバリーグループ間の関連付け)。

パフォーマンスターゲット値の更新

`Set-BrokerAutoscaleGroupPlugin` PowerShellコマンドを使用し、`AutoscaleGroupPlugin`のUIDを指定することで、指定されたパフォーマンスターゲット値を更新できます。例えば、AutoscaleGroupPluginのUIDが2であると仮定します。

```
Set-BrokerAutoscaleGroupPlugin 2 -Configuration '{"PerformanceTarget":70}'
```

Autoscaleグループプラグインの自動承認を構成する

スケジュールの上書き (標準のAutoscale設定を上書きする) を許可するには、`BrokerAutoscaleGroupPlugin`で以下の2つのプロパティを構成します。

- `AutoApprove`
  - `True`の場合: プラグインによって生成されたスケジュールの上書きが自動的に承認されることを示します。
  - `False`の場合: スケジュールは、ターゲット日付がApprovedUntilプロパティで指定された日付以前である場合にのみ承認されます。

  `AutoApprove`が`False`で、`ApprovedUntil`の日付が設定されていないか、過去のものである場合、生成されたスケジュールの上書きは使用されずに破棄されます。
- `ApprovedUntil`:
  - `AutoApprove`が`False`で、`ApprovedUntil`の日付を指定した場合、プラグインによって生成されたスケジュールの上書きは、ターゲット日付のスケジュールとして自動的に承認されます。

例えば、`AutoscaleGroupPlugin`のUIDが2であると仮定します。

- そのデスクトップグループの自動承認を有効にするには:

```
Set-BrokerAutoscaleGroupPlugin 2 -AutoApprove $true
```

- 将来の特定の日付まで自動承認を有効にするには:

```
Set-BrokerAutoscaleGroupPlugin 2 -ApprovedUntil "2025-01-01"
```

ユーザーログオフ通知（旧称：ユーザー強制ログオフ）

重要:

この機能は、マルチセッションアプリベースのデリバリーグループ向けのAutoscale™ユーザーインターフェイスでのみ利用可能です。

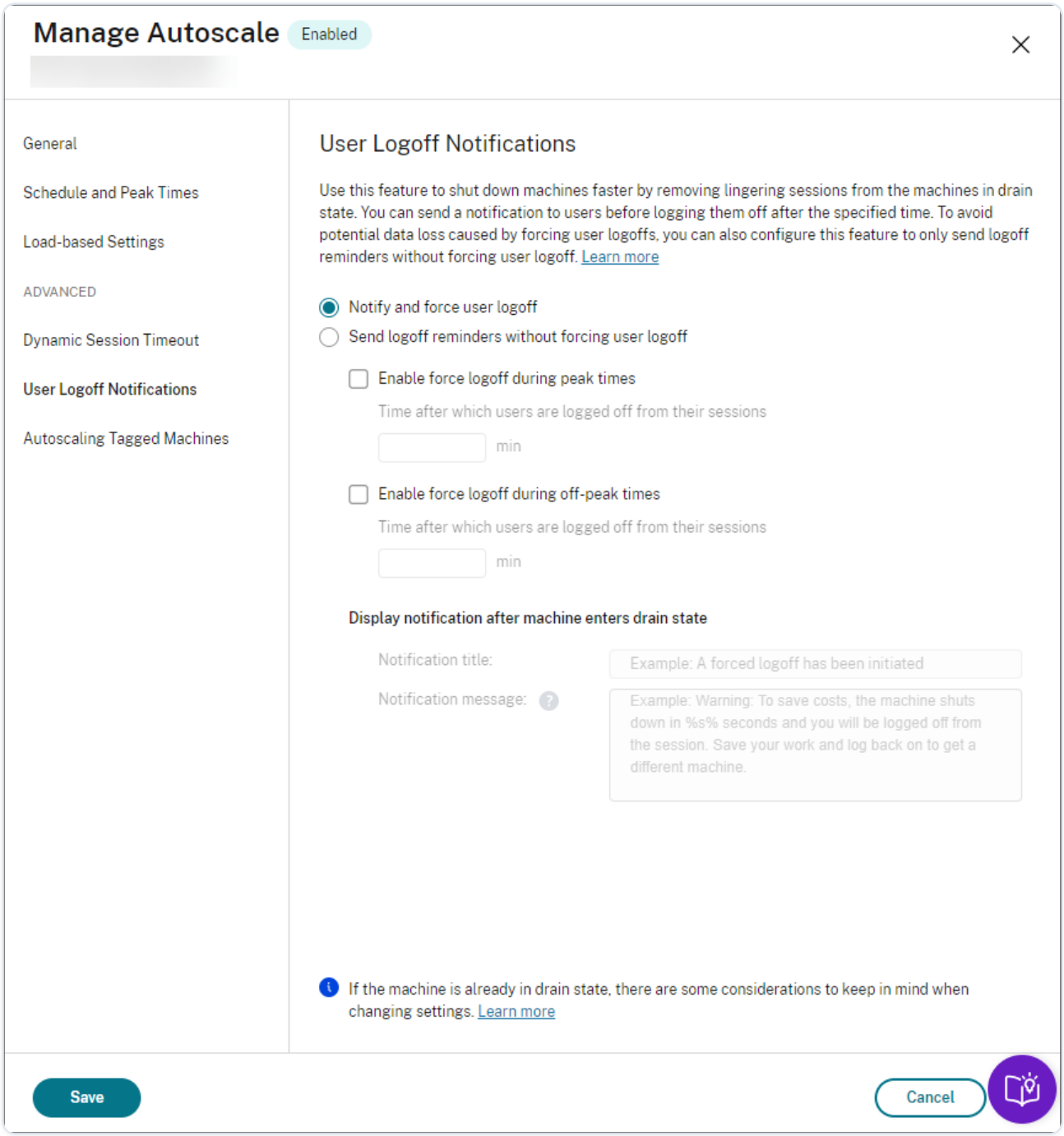
コスト削減をより効果的に実現するため、Autoscaleでは、残存セッションを強制的にログオフできます。これは、ユーザーにカスタム通知を送信し、セッションが強制的にログオフされるまでの猶予期間を指定することで行われます。これは、ドレイン状態のマシンに対してのみ行われ、すべての電源オンのマシンに対して行われるわけではありません。ユーザーの強制ログオフによって発生する可能性のあるデータ損失を回避するために、この機能は、ユーザーのログオフを強制することなく、ログオフのリマインダーのみを送信するように構成することもできます。

以下の2つのオプションがあります。

- **ユーザーに通知してログオフを強制する**
- **ユーザーのログオフを強制せずにログオフのリマインダーを送信する**

ユーザーに通知してログオフを強制する

これを選択すると、Autoscaleは、以下で指定された時間が経過した後、ユーザーをセッションからログオフします。



ピーク時の強制ログオフを有効にする。これを選択すると、Autoscaleは、指定された時間が経過したピーク時に、それらのユーザーをセッションからログオフします。

オフピーク時の強制ログオフを有効にする。これを選択すると、Autoscaleは、指定された時間が経過したオフピーク時に、それらのユーザーをセッションからログオフします。

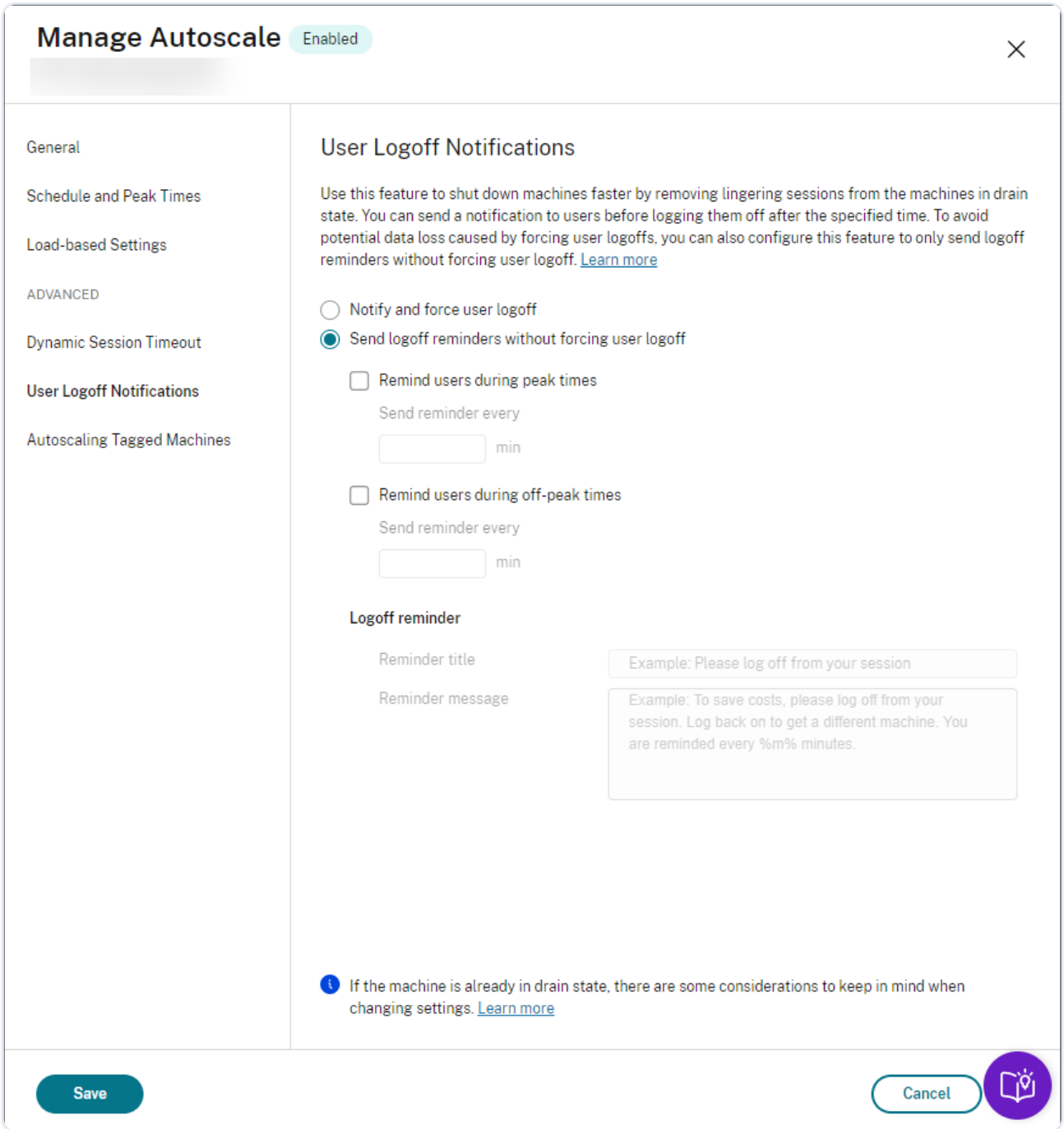
マシンがドレイン状態になった後に通知を表示する。マシンがドレイン状態になった後、ユーザーに通知を送信できます。

- **通知のタイトル。**ユーザーに送信する通知のタイトルを指定できます。例: `A forced logoff has been initiated.`.

- **通知メッセージ**。ユーザーに送信する通知の内容を指定できます。メッセージ内で指定された時間を示す変数として、%s% または %m% を使用できます。時間を秒で表すには %s% を使用します。時間を分で表すには %m% を使用します。例: `Warning: To save costs, the machine shuts down in %s% seconds and you will be logged off from the session. Save your work and log back on to get a different machine.`.

ユーザーのログオフを強制せずにログオフリマインダーを送信する

選択した場合、ユーザーはマシンがドレイン状態になった後、マシンからログオフするようリマインダーを受け取ります。このリマインダーは、以下で指定された間隔で送信されるように構成できます。



ピーク時にユーザーにリマインダーを送信する。選択した場合、ユーザーはピーク時にX分ごとにセッションからログオフするようリマインダーを受け取ります（Xは指定された時間を示します）。

オフピーク時にユーザーにリマインダーを送信する。選択した場合、ユーザーはオフピーク時にX分ごとにセッションからログオフするようリマインダーを受け取ります（Xは指定された時間を示します）。

ログオフリマインダー。マシンがドレイン状態になった後、ユーザーに送信されるリマインダーを構成できます。

- **リマインダーのタイトル。**ユーザーに送信するリマインダーのタイトルを指定できます。例: `Please log off from your session`。
- **リマインダーメッセージ。**ユーザーに送信するメッセージを指定できます。例: `Please log off from your session and log back on to save costs`。

考慮事項

マシンがすでにドレイン状態である場合、設定を変更する際には以下を考慮してください。

- 設定を「**ユーザーのログオフを強制せずにログオフリマインダーを送信する**」から「**ユーザーのログオフを通知して強制する**」に変更した場合、新しい設定はすぐに有効になります。
- 設定を「**ユーザーのログオフを通知して強制する**」から「**ユーザーのログオフを強制せずにログオフリマインダーを送信する**」に変更した場合、新しい設定はマシンが次にドレイン状態になるまで有効になりません。ユーザーは引き続きログオフを強制されます。

Autoscale™ 設定の有効性を分析する

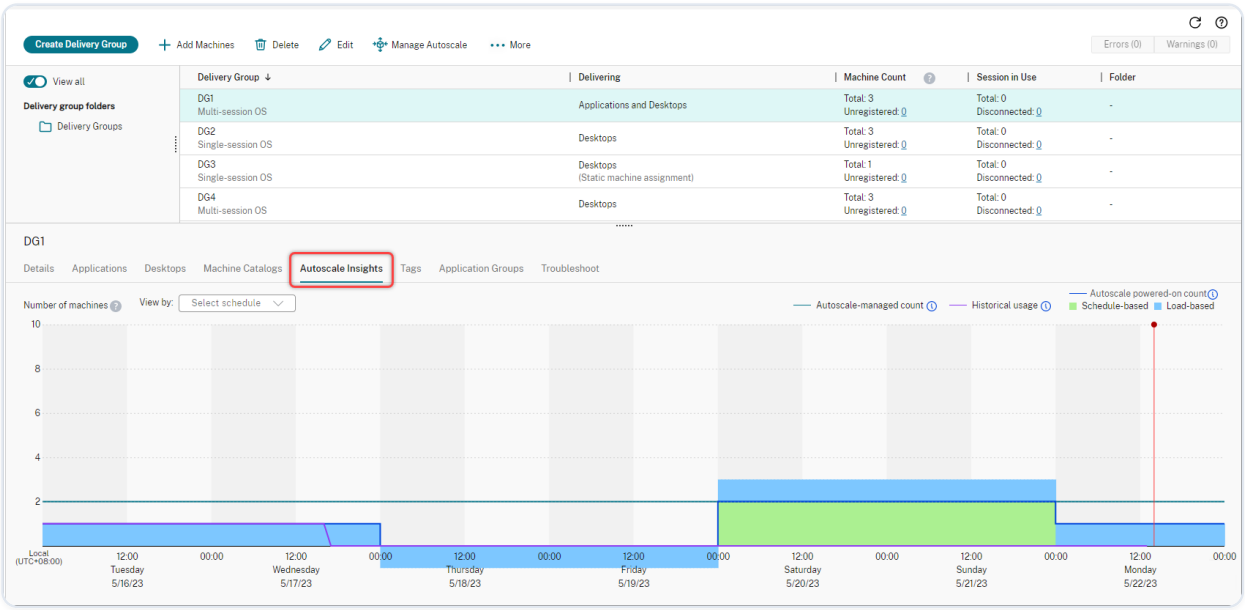
この記事では、前週のマシン使用状況に基づいてAutoscale設定の有効性を分析する方法について説明します。この分析を通じて、Autoscale設定の有効性に関する以下の洞察を得ることができます。

- 過剰プロビジョニングに起因する財政的な無駄を特定する。
- プロビジョニング不足によりユーザーエクスペリエンスが負の影響を受けているかどうかを判断する。
- プロビジョニングされた容量がマシン使用状況と適切に一致していることを確認します。

この目標を達成するには、次の手順に従います。

1. Autoscale が有効なデリバリーグループを選択します。
2. 下部のペインで、**Autoscale Insights** タブをクリックします。

次のグラフが表示され、前週のマシン使用状況データと、Autoscale 設定に基づいて電源をオンにするマシンの数を比較して示しています。



* 赤い垂直線は現在の時刻を示します。

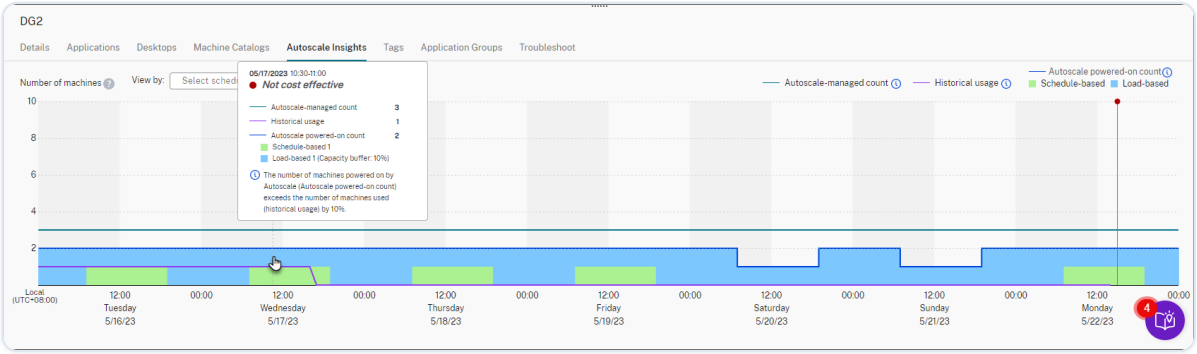
次の表は、このグラフに表示されるメトリックの説明を示しています。

メトリック	説明
Autoscale管理対象数	Autoscaleによって管理されるマシンの総数。Autoscale管理対象数 = デリバリーグループ内のマシンの総数 – メンテナンスモードのマシンの数 – Autoscale用にタグ付けされていないマシンの数 (タグ付きAutoscale機能が有効な場合)。
Autoscale電源オン数	Autoscaleによって電源がオンにされたマシンの総数。Autoscale電源オン数 = スケジュールベースのマシン数 + 負荷ベースのマシン数。
履歴使用状況	ユーザーに提供されたマシンの数。
スケジュールベース	Autoscaleのスケジュールベース設定に基づいて電源がオンにされるマシンの数 (**注:** スケジュールベース設定は、静的シングルセッションOSタイプのデリバリーグループには適用されません)。

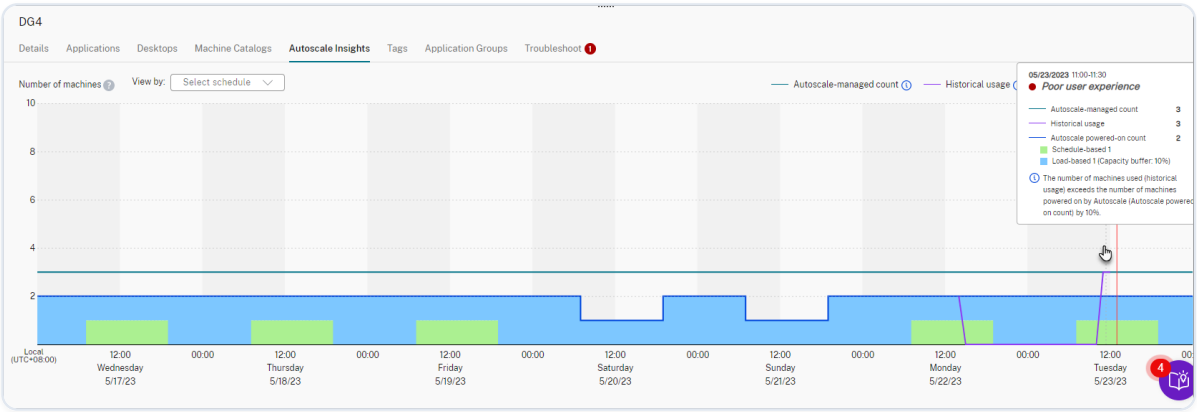
メトリック	説明
負荷ベース	Autoscaleの負荷ベース設定に基づいて電源がオンにされるマシンの数。

3. 特定の時間帯におけるAutoscale設定の有効性を確認するには、グラフ上のその時間帯にマウスを合わせます。比較結果と詳細なマシン数が表示された情報ボックスが表示されます。

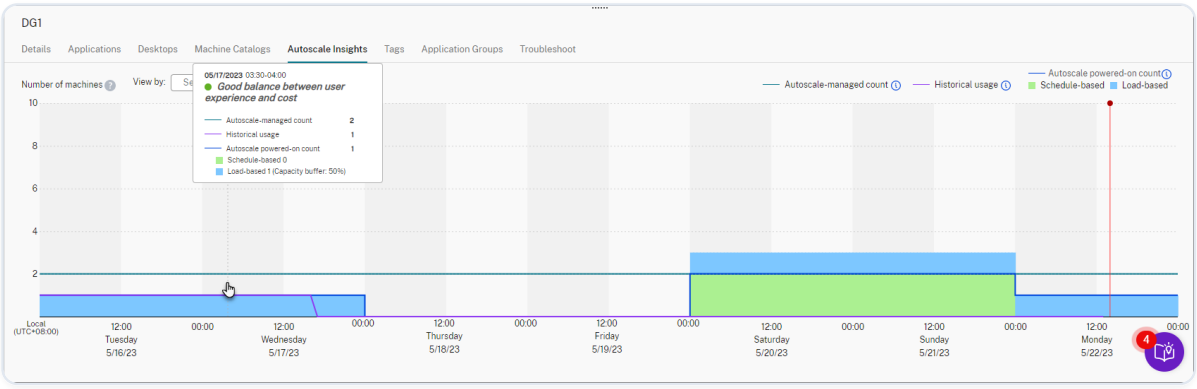
   - **費用対効果が低い**。履歴使用状況がAutoscale設定 (Autoscale電源オン数) の90%未満です。その結果、無駄な容量が存在する可能性があります。



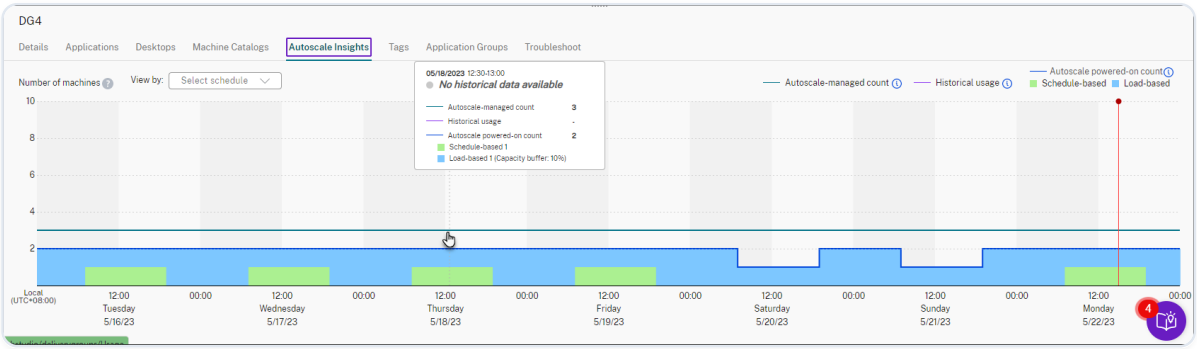
   - **ユーザーエクスペリエンスが低い**。履歴使用状況がAutoscale設定 (Autoscale電源オン数) の110%を超えています。その結果、ユーザーはマシンの電源がオンになるまで長い待機時間を経験する可能性があります。



   - **ユーザーエクスペリエンスとコストの良好なバランス**。過去の使用状況とAutoscale設定（Autoscaleの電源オン数）の差が10%未満です。Autoscale設定は過去の使用状況と一致しています。



- **履歴データがありません。**履歴データが利用できません。考えられる原因としては、Autoscaleがデリバリーグループに対して1週間未満前に有効化されたことなどが挙げられます。



4. Autoscaleスケジュールに基づいて日付範囲を強調表示するには、「**表示方法**」フィールドからスケジュールを選択します。
5. 分析に基づいて、Autoscale設定を調整します。詳細については、「スケジュールベースおよび負荷ベースの設定」を参照してください。

Broker PowerShell SDKコマンド

Broker PowerShell SDKを使用して、デリバリーグループのAutoscaleを構成できます。PowerShellコマンドを使用してAutoscaleを構成するには、PowerShell SDKバージョン7.21.0.12以降を使用する必要があります。PowerShell SDKの詳細については、「SDKとAPI」(/ja-jp/citrix-virtual-apps-desktops/current-release/sdk-api.html)を参照してください。

Set-BrokerDesktopGroup

既存のBrokerDesktopGroupを無効または有効にするか、その設定を変更します。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>`を参照してください。

例

PowerShellコマンドレットの使用方法の詳細については、以下の例を参照してください。

Autoscale™を有効にする

- 名前が「MyDesktop」であるデリバリーグループに対してAutoscaleを有効にしたいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -AutoscalingEnabled $true`

ピーク時とオフピーク時で容量バッファを個別に構成する

- 名前が「MyDesktop」であるデリバリーグループに対して、容量バッファをピーク時で20%、オフピーク時で10%に設定したいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakBufferSizePercent 20 -OffPeakBufferSizePercent 10`

切断時のタイムアウト設定を構成する

- 名前が「MyDesktop」であるデリバリーグループに対して、**切断時のタイムアウト**値をピーク時で60分、オフピーク時で30分に設定したいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakDisconnectTimeout 60 -OffPeakDisconnectTimeout 30`

ログオフ時のタイムアウト設定を構成する

- 名前が「MyDesktop」であるデリバリーグループに対して、**ログオフ時のタイムアウト**値をピーク時で60分、オフピーク時で30分に設定したいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakLogOffTimeout 60 -OffPeakLogOffTimeout 30`

電源オフ遅延設定を構成する

- 名前が「MyDesktop」であるデリバリーグループに対して、電源オフ遅延を15分に設定したいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PowerOffDelay 15`

電源オフ遅延が適用されない期間を構成する

- 「MyDesktop」という名前のデリバリーグループに対して、電源オフ遅延が30分経過するまで適用されるようにしたいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例:
  - `C:\PS> Set-BrokerDesktopGroup "MyDesktop" -SettlementPeriodBeforeAutoShutdown 30`。

マシンインスタンスコスト設定を構成する

- 「MyDesktop」という名前のデリバリーグループに対して、1時間あたりのマシンインスタンスコストを0.2ドルに設定したいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -MachineCost 0.2`

メンテナンスモードのVMをオートスケールプールから除外する

- 10台のマシンを持つデリバリーグループがあり、そのうち2台のマシンがメンテナンスモードであるとします。オートスケールのバッファ容量は50%に設定されています。メンテナンスモードのVMをオートスケールプールから除外したい場合は、`PoolSizeExcludesMaintenanceMode`を`True`に設定します。これにより、メンテナンスモードの2台のマシンがマシンプールに含まれないため、オートスケールは4台のマシンを起動します。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例:
  - `PS C:\> Set-BrokerDesktopGroup -PoolSizeExcludesMaintenanceMode $true`

  シングルセッションデリバリーグループの`PoolSizeExcludesMaintenanceMode`のデフォルト値は`False`です。

  マルチセッションデリバリーグループの`PoolSizeExcludesMaintenanceMode`のデフォルト値は`True`です。

New-BrokerPowerTimeScheme

デリバリーグループのBrokerPowerTimeSchemeを作成します。詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerPowerTimeScheme/>`を参照してください。

例

UID値が3のデリバリーグループに対して電源時間スキームを作成したいとします。新しいスキームは週末、月曜日、火曜日を対象とします。午前8時から午後6時30分までの時間帯は、スキームに含まれる日のピーク時間として定義されます。ピーク時間の場合、プールサイズ（電源がオン

のまま維持されるマシンの数）は20です。オフピーク時間の場合、プールサイズは5です。`Set-BrokerDesktopGroup` PowerShellコマンドを使用できます。例:

- `PS C:\> $ps48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37) { 5 } else { 20 } } )`
- `PS C:\> $pt48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37) { $false } else { $true } } )`
- `PS C:\> New-BrokerPowerTimeScheme -Name 'First Half Week' -DaysOfWeek Weekend,Monday,Tuesday -DesktopGroupUid 3 -PeakHalfHours $pt48 -PoolSize $ps48`

動的セッションタイムアウトのパラメーター

以下のBroker PowerShell SDKコマンドレットは、複数の新しいパラメーターをサポートすることで、動的セッションタイムアウト用に拡張されました。

- Get-BrokerDesktopGroup
- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup

これらのパラメーターには以下が含まれます。

- **DisconnectPeakIdleSessionAfterSeconds** – ピーク時にアイドル状態のセッションが切断されるまでの時間を秒単位で表します。このプロパティのデフォルト値は0で、ピーク時の関連動作が無効になっていることを示します。0より大きい値は、ピーク時のみデリバリーグループの動作を有効にします。
- **DisconnectOffPeakIdleSessionAfterSeconds** - オフピーク時にアイドル状態のセッションが切断されるまでの時間を秒単位で表します。このプロパティのデフォルト値は0で、オフピーク時の関連動作が無効になっていることを示します。0より大きい値は、オフピーク時のみデリバリーグループの関連動作を有効にします。
- **LogoffPeakDisconnectedSessionAfterSeconds** - ピーク時に切断されたセッションが終了されるまでの時間を秒単位で表します。このプロパティのデフォルト値は0で、ピーク時の関連動作が無効になっていることを示します。0より大きい値は、ピーク時のみデリバリーグループの関連動作を有効にします。
- **LogoffOffPeakDisconnectedSessionAfterSeconds** - オフピーク時に切断されたセッションが終了されるまでの時間を秒単位で表します。このプロパティのデフォルト値は0で、オフピーク時の関連動作が無効になっていることを示します。0より大きい値は、オフピーク時のみデリバリーグループの関連動作を有効にします。

例

たとえば、「MyDesktop」という名前のデリバリーグループに対して、ピーク時のアイドルセッションタイムアウトを3,600秒に設定したいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例:

- `C:\PS> Set-BrokerDesktopGroup "MyDesktop" -DisconnectOffPeakIdleSessionAfterSeconds 3600`

これにより、「MyDesktop」という名前のデスクトップグループでは、オフピーク時に1時間以上アイドル状態だったセッションが切断されます。

シトリックス インサイト サービス

Citrix Insight Services (CIS)は、計測、テレメトリ、ビジネスインサイト生成のためのCitrixプラットフォームです。その計測およびテレメトリ機能により、技術ユーザー（顧客、パートナー、エンジニア）は問題を自己診断して修正し、環境を最適化できます。CISとその仕組みに関する詳細および最新情報については、`<https://cis.citrix.com>`を参照してください（Citrixアカウントの資格情報が必要です）。

Citrixにアップロードされるすべての情報は、トラブルシューティングと診断の目的、および製品の品質、信頼性、パフォーマンスの向上のために使用されます。ただし、以下に従います。

- シトリックス インサイト サービス ポリシー (https://cis.citrix.com/legal)
- Citrixプライバシーポリシー（`<https://www.cloud.com/privacy-policy>`）

このCitrix Virtual Apps and Desktops™リリースは、以下のテクノロジーをサポートしています。

- Citrix Virtual Apps and Desktops™のインストールおよびアップグレード分析
- Citrixカスタマーエクスペリエンス向上プログラム（CEIP）
- シトリックス コール ホーム
- シトリックス スカウト

インストールおよびアップグレード分析

フルプロダクトインストーラーを使用してCitrix Virtual Apps and Desktopsコンポーネントを展開またはアップグレードすると、インストールプロセスに関する匿名情報が収集され、コンポーネントをインストール/アップグレードしているマシンに保存されます。このデータは、Citrixが顧客のインストールエクスペリエンスを向上させるのに役立てられます。

この情報は、`%ProgramData%\Citrix\CTQs`にローカルに保存されます。

このデータの自動アップロードは、フルプロダクトインストーラーのグラフィカルインターフェイスとコマンドラインインターフェイスの両方で、デフォルトで有効になっています。

- レジストリ設定のデフォルト値を変更できます。インストール/アップグレード前にレジストリ設定を変更した場合、フルプロダクトインストーラーを使用する際にその値が使用されます。
- コマンドでオプションを指定することにより、コマンドラインインターフェイスでインストール/アップグレードする際にデフォルト設定を上書きできます。

自動アップロードの制御:

- インストール/アップグレード分析の自動アップロードを制御するレジストリ設定 (デフォルト = 1):
  - 場所: `HKLM:\Software\Citrix\MetaInstall`
  - 名前: SendExperienceMetrics
  - 値: 0 = 無効、1 = 有効
- PowerShell を使用すると、次のコマンドレットでインストール/アップグレード分析の自動アップロードが無効になります:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\MetaInstall -Name
SendExperienceMetrics -PropertyType DWORD -Value 0
```

- XenDesktopServerSetup.exe または XenDesktopVDASetup.exe コマンドで自動アップロードを無効にするには、`/disableexperiencemetrics` オプションを含めます。

  XenDesktopServerSetup.exe または XenDesktopVDASetup.exe コマンドで自動アップロードを有効にするには、`/sendexperiencemetrics` オプションを含めます。

Citrix カスタマーエクスペリエンス向上プログラム

Citrix カスタマーエクスペリエンス向上プログラム (CEIP) に参加すると、匿名の統計情報と使用状況情報が Citrix に送信され、Citrix 製品の品質とパフォーマンスの向上に役立てられます。詳細については、https://more.citrix.com/XD-CEIP を参照してください。

サイト作成時またはアップグレード時の登録

サイトを作成すると (最初のDelivery Controller™をインストールした後)、CEIPに自動的に登録されます。最初のデータアップロードは、サイト作成後約7日後に行われます。

サイト作成後、いつでも参加を停止できます。Web Studioの左ペインで**設定**ノードを選択し、**Citrixカスタマーエクスペリエンス向上プログラム**設定をオフにします。

Citrix Virtual Apps and Desktops 展開をアップグレードする場合:

- CEIP をサポートしていないバージョンからアップグレードする場合、参加するかどうかを尋ねられます。
- CEIPをサポートしていたバージョンからアップグレードし、参加が有効になっていた場合、アップグレードされたサイトでCEIPが有効になります。
- CEIPをサポートしていたバージョンからアップグレードし、参加が無効になっていた場合、アップグレードされたサイトでCEIPが無効になります。
- CEIPをサポートしていたバージョンからアップグレードし、参加状況が不明な場合、参加を希望するかどうか尋ねられます。

収集された情報は匿名であるため、Citrix Insight Servicesにアップロードされた後は閲覧できません。

VDAインストール時の登録

デフォルトでは、Windows VDAをインストールすると、CEIPに自動的に登録されます。このデフォルト設定はレジストリ設定で変更できます。VDAをインストールする前にレジストリ設定を変更した場合、その値が使用されます。

CEIPへの自動登録を制御するレジストリ設定（デフォルト = 1）：

場所: HKLM: `\\Software\Citrix\Telemetry\CEIP` 名前: Enabled 値: 0 = 無効, 1 = 有効

デフォルトでは、`Enabled` プロパティはレジストリに隠されています。指定されていない場合、自動アップロード機能は有効になります。

PowerShellを使用すると、次のコマンドレットでCEIPへの登録を無効にできます。

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name Enabled
-PropertyType DWORD -Value 0
```

収集されたランタイムデータポイントは、定期的にファイルとして出力フォルダー（デフォルト %programdata%/Citrix/VdaCeip）に書き込まれます。

データの初回アップロードは、VDAのインストール後約7日で行われます。

その他の製品およびコンポーネントのインストール時の登録

関連するCitrix製品、コンポーネント、テクノロジー（Citrix Provisioning™、AppDNA、Citrix License Server、Windows向けCitrix Workspace™アプリ、Universal Print Server、Session Recordingなど）をインストールする際にも、CEIPに参加できます。インストールと参加のデフォルト値の詳細については、それぞれのドキュメントを参照してください。

Citrix コールホーム

Citrix Virtual Apps and Desktops に特定のコンポーネントと機能をインストールすると、Citrix Call Home に参加する機会が提供されます。Call Home は診断データを収集し、そのデータを含むテレメトリパッケージを分析とトラブルシューティングのために Citrix Insight Services に直接（デフォルトポート 443 の HTTPS 経由で）定期的にアップロードします。

Citrix Virtual Apps and Desktopsでは、Call HomeはCitrix Telemetry Serviceという名前のバックグラウンドサービスとして実行されます。

Call Home のスケジュール機能は Citrix Scout でも利用できます。詳しくは、Citrix Scout を参照してください。

収集される情報

Citrix Diagnostic Facility (CDF) トレースは、トラブルシューティングに役立つ情報をログに記録します。Call Homeは、VDA登録やアプリケーション/デスクトップの起動など、一般的な障害のトラブルシューティングに役立つCDFトレースのサブセットを収集します。このテクノロジーは、常時オンのトレース (AOT) として知られています。AOTログは、C:\ProgramData\Citrix\TelemetryService\CitrixAOTにディスク保存されます。

> **注:**
>
> `ProgramData`フォルダーは非表示になっています。表示するには、**表示** > **表示/非表示** > **隠しファイル** をクリックします。

> Call Home は、その他の Event Tracing for Windows (ETW) 情報を収集せず、またそのように構成することもできません。

Call Home は、次のようなその他の情報も収集します。

- `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix` の下に Citrix Virtual Apps and Desktops によって作成されたレジストリ。

- Citrix 名前空間下の Windows Management Instrumentation (WMI) 情報。
- 実行中のプロセスの一覧。
- %PROGRAM `DATA%\Citrix\CDF` に保存されているCitrixプロセスのクラッシュダンプ。
- インストールおよびアップグレード情報。これには、製品の完全なメタインストーラーログ、失敗した MSI ログ、MSI ログアナライザーからの出力、StoreFront™ ログ、ライセンス互換性チェックログ、および予備的なサイトアップグレードテストの結果が含まれる場合があります。

トレース情報は、収集時に圧縮されます。Citrix Telemetry Service は、最大 10 MB の圧縮された最新のトレース情報を、最大 8 日間保持します。

- データを圧縮することで、Call Home は VDA 上で小さなフットプリントを維持できます。
- プロビジョニングされたマシンでの IOPs を回避するために、トレースはメモリに保持されます。
- トレースバッファは、トレースをメモリに保持するために循環メカニズムを使用します。

Call Home は、Call Home の主要データポイント に記載されている主要なデータポイントを収集します。

構成と管理の概要

Call Home には、製品版インストールウィザードを使用するか、後で PowerShell コマンドレットを使用して登録できます。登録すると、デフォルトで診断情報が収集され、毎週日曜日の現地時間午前 3 時頃に Citrix にアップロードされます。アップロードは、指定された時刻から 2 時間の間隔でランダム化されます。これは、デフォルトのスケジュールを使用するアップロードが午前 3 時から午前 5 時の間に行われることを意味します。

診断情報を定期的にアップロードしたくない場合（またはスケジュールを変更したい場合）は、PowerShell コマンドレットを使用して診断情報を手動で収集してアップロードするか、ローカルに保存することができます。

スケジュールされた Call Home アップロードに登録する場合、および診断情報を手動で Citrix にアップロードする場合、Citrix アカウントまたは Citrix Cloud™ の資格情報を提供します。Citrix は、資格情報をアップロードトークンと交換します。このトークンは、顧客を識別し、データをアップロードするために使用されます。資格情報は保存されません。

アップロードが行われると、Citrix アカウントに関連付けられているアドレスに通知メールが送信されます。

コンポーネントのインストール時に Call Home を有効にした場合、後で無効にできます。

前提条件

- マシンは PowerShell 3.0 以降を実行している必要があります。
- Citrix Telemetry Service がマシン上で実行されている必要があります。
- システム変数 `PSModulePath` は、Telemetryのインストールパス（例: `C:\Program Files\Citrix\Telemetry Service\`）に設定されている必要があります。

コンポーネントのインストール中に Call Home を有効にする

VDA のインストールまたはアップグレード中: 製品版インストーラーのグラフィカルインターフェイスを使用して Virtual Delivery Agent をインストールまたはアップグレードする際に、Call Home に参加するかどうかを尋ねられます。次の 2 つのオプションがあります。

- Call Home に参加する。
- Call Home に参加しない。

VDAをアップグレードしていて、以前にCall Homeに登録していた場合、そのウィザードページは表示されません。

Controllerのインストールまたはアップグレード中: グラフィカルインターフェイスを使用してDelivery Controllerをインストールまたはアップグレードすると、Call Homeに参加するかどうかを尋ねられます。3つのオプションがあります。

Controllerをインストールする際、そのサーバーに「サービスとしてログオン」ポリシー設定が適用されたActive Directory GPOがある場合、インストールウィザードのCall Homeページで情報を構成することはできません。詳細については、CTX218094を参照してください。

Controllerをアップグレードしていて、以前にCall Homeに登録していた場合、参加について尋ねられることはありません。

PowerShellコマンドレット

PowerShellヘルプには、これらの一般的なユースケースでは使用されないコマンドレットとパラメーターの説明を含む、包括的な構文が記載されています。

アップロードにプロキシサーバーを使用するには、「プロキシサーバーの構成」を参照してください。

- **スケジュールされたアップロードを有効にする:** 診断コレクションはCitrixに自動的にアップロードされます。カスタムスケジュール用の追加のコマンドレットを入力しない場合、デフォルトのスケジュールが使用されます。

```
$cred = Get-Credential

Enable-CitrixCallHome -Credential $cred
```

スケジュールされたアップロードが有効になっていることを確認するには、`Get-CitrixCallHome`と入力します。有効になっている場合、戻り値は`IsEnabled=True`と`IsMasterImage=False`です。

- **マスターイメージから作成されたマシンに対するスケジュールされたアップロードを有効にする:** マスターイメージでスケジュールされたアップロードを有効にすると、マシンカタログで作成される各マシンを構成する必要がなくなります。

  `Enable-CitrixCallHome -Credential $cred -MasterImage`

  スケジュールされたアップロードが有効になっていることを確認するには、**Get-CitrixCallHome**と入力します。有効になっている場合、戻り値は`IsEnabled=True`と`IsMasterImage=True`です。

- **カスタムスケジュールを作成する:** 診断コレクションとアップロードの毎日または毎週のスケジュールを作成します。

```
$timespan = New-TimeSpan –Hours hours -Minutes minutes

Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek day
-UploadFrequency {Daily|Weekly}
```

例:

次のコマンドレットは、毎晩22:20にデータをバンドルしてアップロードするスケジュールを作成します。Hoursパラメーターは24時間形式を使用します。`UploadFrequency`パラメーターの値がDailyの場合、`DayOfWeek`パラメーターは指定されていても無視されます。

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20

Set-CitrixCallHomeSchedule –TimeOfDay $timespan -UploadFrequency Daily
```

スケジュールを確認するには、`Get-CitrixCallHomeSchedule`と入力します。上記の例では、`StartTime=22:20:00, DayOfWeek=Sunday (ignored), Upload Frequency=Daily`が返されます。

次のコマンドレットは、毎週水曜日の夜10時20分にデータをバンドルしてアップロードするスケジュールを作成します。

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20

Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek Wed
-UploadFrequency Weekly
```

スケジュールを確認するには、`Get-CitrixCallHomeSchedule`と入力します。上記の例では、`StartTime=22:20:00, DayOfWeek=Wednesday, Upload Frequency=Weekly`が返されます。

Call Homeを無効にする

PowerShellコマンドレットを使用するか、Citrix Scoutを介してCall Homeを無効にできます。

Call Homeのスケジュールされたアップロードが無効になっている場合でも、AOTログは収集され、ディスクに保存されます。(スケジュールされたアップロードが無効になっている場合、AOTログはCitrixに自動的にアップロードされません。) AOTログの収集とローカルストレージを無効にすることができます。

PowerShellでCall Homeを無効にする

次のコマンドレットを実行すると、診断データはCitrixに自動的にアップロードされなくなります。(Citrix ScoutまたはテレメトリPowerShellコマンドレットを使用して、診断データをアップロードすることは引き続き可能です。)

`Disable-CitrixCallHome`

Call Homeが無効になっていることを確認するには、`Get-CitrixCallHome`と入力します。無効になっている場合、戻り値は`IsEnabled=False`と`IsMasterImage=False`です。

Citrix Scoutを使用して収集スケジュールを無効にする

Citrix Scoutを使用して診断収集スケジュールを無効にするには、コレクションのスケジュールのガイダンスに従ってください。ステップ3で、**オフ**をクリックして、選択したマシンのスケジュールをキャンセルします。

AOTログの収集を無効にする

次のコマンドレットを実行すると(`Enabled`フィールドを`false`に設定すると)、AOTログは収集されなくなります。

`Enable-CitrixTrace -Listen'{"trace":{"enabled":false,"persistDirectory":"C:\Users\Public","maxSizeBytes":1000000, "sliceDurationSeconds":300}}'`

`Listen`パラメーターには、JSON形式の引数が含まれています。

Call Homeアップロード用のプロキシサーバーを構成する

Call Homeが有効になっているマシンで、次のタスクを完了します。以下の手順の例の図には、サーバーアドレスとポート10.158.139.37:3128が含まれています。お客様の情報は異なります。

1. ブラウザーにプロキシサーバー情報を追加します。Internet Explorer で、 **\> \>** を選択します。「**LAN にプロキシ サーバーを使用する**」を選択し、プロキシサーバーのアドレスとポート番号を入力します。
2. PowerShell で `netsh winhttp import proxy source=ie` を実行します。

   プロキシサーバーを構成する際の netsh コマンド実行例(/en-us/citrix-virtual-apps-desktops/current-release/media/call-home-proxy-ie.png)
3. テキストエディターを使用して、`C:\Program Files\Citrix\Telemetry Service` にある TelemetryService.exe 構成ファイルを編集します。赤枠で示されている情報を追加します。

   TelemetryService.exe ファイルにプロキシ情報を追加(/en-us/citrix-virtual-apps-desktops/current-release/media/call-home-proxy-config.png)
4. テレメトリサービスを再起動します。

PowerShell で Call Home コマンドレットを実行します。

診断情報を手動で収集してアップロードする

CIS Webサイトを使用して、診断情報バンドルをCISにアップロードできます。PowerShell コマンドレットを使用して、診断情報を収集し、CISにアップロードすることもできます。

CIS Webサイトを使用してバンドルをアップロードするには：

1. Citrixアカウントの資格情報を使用して、Citrix Insight Servicesにログオンします。
2. を選択します。
3. を選択し、データの場所に移動します。

CISは、データアップロードを管理するいくつかのPowerShellコマンドレットをサポートしています。このドキュメントでは、2つの一般的なケースのコマンドレットについて説明します。

- `Start-CitrixCallHomeUpload` コマンドレットを使用して、診断情報バンドルを手動で収集し、CISにアップロードします。（バンドルはローカルに保存されません。）
- `Start-CitrixCallHomeUpload` コマンドレットを使用して、データを手動で収集し、診断情報バンドルをローカルに保存します。これにより、データをプレビューできます。その後、

`Send-CitrixCallHomeBundle` コマンドレットを使用して、そのバンドルのコピーをCISに手動でアップロードします。(最初に保存したデータはローカルに残ります。)

PowerShellヘルプには、これらの一般的なユースケースでは使用されないコマンドレットとパラメーターの説明を含む、包括的な構文が記載されています。

CISにデータをアップロードするコマンドレットを入力すると、アップロードの確認を求められます。アップロードが完了する前にコマンドレットがタイムアウトした場合は、システムイベントログでアップロードのステータスを確認してください。サービスがすでにアップロードを実行している場合、アップロード要求は拒否される可能性があります。

データの収集とバンドルのCISへのアップロード:

```
Start-CitrixCallHomeUpload [-Credential] PSCredential [-InputPath string]
[-Description string] [-IncidentTime string] [-SRNumber string] [-Name
string] [-UploadHeader string] [-AppendHeaders string] [-Collect string]
[<CommonParameters>]
```

データの収集とローカルへの保存:

```
Start-CitrixCallHomeUpload -OutputPath <String> [-InputPath string] [-
Description string] [-IncidentTime string] [-SRNumber string] [-Name
string] [-UploaderHeader string] [-AppendHeaders string] [-Collect
strings] [<CommonParameters>]
```

次のパラメーターが有効です。

- **Credential:** CISへのアップロードを指示します。
- **InputPath:** バンドルに含めるzipファイルの場所。これは、Citrixサポートが要求する追加ファイルである可能性があります。.zip拡張子を含めるようにしてください。
- **OutputPath:** 診断情報が保存される場所。このパラメーターは、Call Homeデータをローカルに保存する場合に必須です。
- **Description and Incident Time:** アップロードに関する自由形式の情報。
- **SRNumber:** Citrixテクニカルサポートのインシデント番号。
- **Name:** バンドルを識別する名前。
- **UploadHeader:** CISにアップロードされるアップロードヘッダーを指定するJSON形式の文字列。
- **AppendHeaders:** CISにアップロードされる追加ヘッダーを指定するJSON形式の文字列。

- **Collect:** 収集または省略するデータを指定するJSON形式の文字列で、{'collector': {'enabled':Boolean}} の形式で、Booleanはtrueまたはfalseです。 有効なコレクター値は次のとおりです。

  - 'WMI'
  - 'プロセス'
  - 'レジストリ
  - 'クラッシュレポート'
  - 'トレース'
  - 'ファイル'
  - 'MSI'
  - 'ローカルデータ'
  - 'サイトデータ'
  - 'SFB'

  デフォルトでは、「sfb」を除くすべてのコレクターが有効になっています。

  「sfb」コレクターは、Skype for Businessの問題を診断するためにオンデマンドで使用するように設計されています。「enabled」パラメーターに加えて、「sfb」コレクターは、ターゲットユーザーを指定するための「account」および「accounts」パラメーターをサポートしています。次のいずれかの形式を使用します。

  - "-収集 "`{'sfb':{'account':'domain\\user1'}}`"
  - "-収集 "{'sfb':{'accounts':}}"

- **共通パラメーター:** PowerShellのヘルプを参照してください。

以前にローカルに保存されたデータをアップロードする:

`Send-CitrixCallHomeBundle -Credential <PSCredentia\> -Path string [<CommonParameters>]`

`Path` パラメーターは、以前に保存されたバンドルの場所を指定します。

例:

以下のコマンドレットは、Call Home データ（WMI コレクターからのデータを除く）を CIS にアップロードするよう要求します。このデータは、Citrix Support ケース 123456 について午後 2 時 30 分に記録された Citrix Provisioning VDA の登録失敗に関連しています。Call Home データに

加えて、ファイル「`c:\Diagnostics\ExtraData.zip`」がアップロードされたバンドルに組み込まれます。

```
C:\PS\>Start-CitrixCallHomeUpload -InputPath "c:
\Diagnostics\ExtraData.zip" -Description "Registration failures with
Citrix Provisioning VDAs" -IncidentTime "14:30" -SRNumber 123456 -Name
"RegistrationFailure-021812016" -Collect "{'wmi':{'enabled':false}}"
-UploadHeader "{'key1':'value1'}" -AppendHeaders "{'key2':'value2'}"
```

以下のコマンドレットは、午前 8 時 15 分に記録された Citrix Support ケース 223344 に関連する Call Home データを保存します。データはネットワーク共有上のファイル mydata.zip に保存されます。Call Home データに加えて、ファイル「`c:\Diagnostics\ExtraData.zip`」が保存されたバンドルに組み込まれます。

```
C:\PS\>Start-CitrixCallHomeUpload -OutputPath \
\mynetwork\myshare\mydata.zip -InputPath "c:\Diagnostics\ExtraData.zip"
-Description "Diagnostics for incident number 223344" -IncidentTime "8:15"
-SRNumber 223344
```

以下のコマンドレットは、以前に保存したデータバンドルをアップロードします。

```
$cred=Get-Credential

C:\PS>Send-CitrixCallHomeBundle –Credential $cred -Path \
\mynetwork\myshare\mydata.zip
```

シトリックス スカウト

はじめに

Citrix Scout は診断情報を収集し、ヘルスチェックを実行します。その結果を使用して、Citrix Virtual Apps and Desktops™ の展開を維持できます。Citrix は、Citrix Insight Services を通じて、診断情報収集の包括的な自動分析を提供します。また、Scout を使用して、単独で、または Citrix サポートのガイダンスを受けて、問題をトラブルシューティングすることもできます。

収集ファイルを Citrix にアップロードして、Citrix サポートからの分析とガイダンスを受けることができます。または、収集をローカルに保存して自分で確認し、後で収集ファイルを Citrix にアップロードして分析することもできます。

Scout は次の手順を提供します。

- **収集:** サイトで選択したマシンに対して、1回限りの診断情報収集を実行します。その後、ファイルをCitrixにアップロードするか、ローカルに保存できます。
- **トレースと再現:** 選択したマシンで手動トレースを開始します。次に、それらのマシンで問題を再現します。問題を再現すると、トレースは停止されます。その後、Scoutはその他の診断情報を収集し、ファイルをCitrixにアップロードするか、ファイルをローカルに保存します。
- **スケジュール:** 選択したマシンで、指定した時間に毎日または毎週診断情報収集が実行されるようにスケジュールします。ファイルは自動的に Citrix にアップロードされます。
- **ヘルスチェック:** サイトとそのコンポーネントの健全性と可用性を測定するチェックを実行します。Delivery Controller、Virtual Delivery Agent (VDA)、StoreFront™ サーバー、および Citrix License Server のヘルスチェックを実行できます。チェック中に問題が発見された場合、Scout は詳細なレポートを提供します。Scout が起動するたびに、更新されたヘルスチェックスクリプトがチェックされます。新しいバージョンが利用可能な場合、Scout はそれらを自動的にダウンロードし、次回のヘルスチェック実行時に使用します。

> **注:**
>
> **トレースと再現、スケジュール、ヘルスチェック**の手順は、現在 Linux VDA では利用できません。

> この記事で説明されているグラフィカルインターフェイスは、Scout を使用する主要な方法です。または、PowerShell を使用して、1 回限りまたはスケジュールされた診断情報収集とアップロードを構成することもできます。(/ja-jp/citrix-virtual-apps-desktops/current-release/manage-deployment/cis.html#citrix-call-home)を参照してください。

Scout の実行場所:

- オンプレミス展開では、Delivery Controller™からScoutを実行して、1つ以上のVirtual Delivery Agent（VDA）、Delivery Controller、StoreFrontサーバー、Federated Authentication Service（FAS）サーバー、およびライセンスサーバーの診断情報を取得したり、チェックを実行したりします。VDAからScoutを実行して、ローカル診断情報を収集することもできます。

  > **注:**
  >
  > 現在、FAS構成の問題を診断するための*ヘルスチェック*は、FASサーバー上のScoutではサポートされていません。

- Citrix DaaS (旧 Citrix Virtual Apps and Desktops™ サービス) を使用する Citrix Cloud 環境では、VDA から Scout を実行してローカル診断情報を収集します。

Scout アプリケーションのログは `C:\ProgramData\Citrix\TelemetryService\ScoutUI.log` に保存されます。このファイルはトラブルシューティングに使用できます。

収集される情報

Scoutによって収集される診断情報には、Citrix Diagnostic Facility（CDF）トレースログファイルが含まれます。Always-on Tracing（AOT）と呼ばれるCDFトレースのサブセットも含まれます。AOT情報は、VDA登録やアプリケーション/デスクトップの起動などの一般的な問題のトラブルシューティングに役立ちます。その他のEvent Tracing for Windows（ETW）情報は収集されません。

収集される情報には以下が含まれます。

- Citrix Virtual Apps and Desktopsによって `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix` の下に作成されたレジストリエントリ。
- **Citrix名前空間**の下のWindows Management Instrumentation（WMI）情報。
- 実行中のプロセス。
- `%PROGRAMDATA%\Citrix\CDF` に保存されているCitrixプロセスのクラッシュダンプ。
- Citrixポリシー情報（CSV形式）。
- インストールおよびアップグレード情報。収集される情報には、製品の完全なメタインストーラーログ、失敗したMSIログ、MSIログアナライザーからの出力、StoreFrontログ、ライセンス互換性チェックログ、および予備的なサイトアップグレードテストの結果が含まれる場合があります。

トレース情報について：

- トレース情報は収集時に圧縮され、マシン上のフットプリントを小さく保ちます。
- 各マシンで、Citrix Telemetry Serviceは圧縮された最新のトレース情報を最大8日間保持します。
- Citrix Virtual Apps and Desktops 7 1808以降、AOTトレースはデフォルトでローカルディスクに保存されます。（以前のバージョンでは、トレースはメモリに保持されていました。）デフォルトパス = `C:\Users\CitrixTelemetryService\AppData\Local\CitrixAOT`。
- Citrix Virtual Apps and Desktops 7 1811以降、ネットワーク共有に保存されたAOTトレースは、他の診断情報とともに収集されます。

- `Enable-CitrixTrace` cmdletまたは`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Telemetry` `DefaultListen`レジストリ文字列を使用して、最大サイズ（デフォルト = 10 MB）とスライス期間を変更できます。
- トレースは、ファイルが`MaxSize`の10%に達するまでファイルに追加されます。

Scoutが収集するデータポイントのリストについては、「Call Home key datapoints」を参照してください。

Scoutの構成

ScoutはLinux VDAで動作するように構成できます。Linux VDAとテレメトリの詳細については、「Citrix Telemetry Serviceとの統合」を参照してください。

Linux VDAは、`ctxtelemetry`ソケットポートまたはテレメトリサービス用のポートを自動的に変更する場合があります。その場合は、ポートを手動で構成する必要があります。

1. C:\Program Files\Citrix\Telemetry Serviceに移動します。
2. ScoutUI.exe.configファイルを開きます。
3. LinuxVDATelemetryServicePortまたはLinuxVDATelemetryWakeupPortの値を、Linux VDAで構成された値に変更します。

- `<add key="LinuxVDATelemetryServicePort" value="7502"/>`
- `<add key="LinuxVDATelemetryWakeupPort" value="7503"/>`

1. 変更を保存してファイルを閉じます。
2. 最新の構成が読み込まれていることを確認するために、Scoutを再度開きます。

ヘルスチェックについて

ヘルスチェックデータは、`C:\ProgramData\Citrix\TelemetryService\`の下のフォルダーに保存されます。

サイトのヘルスチェック

サイトのヘルスチェックは、FlexCast Management Architecture (FMA) サービスを包括的に評価する環境テストサービスに含まれています。これらのチェックでは、サービスの可用性を確認するだけでなく、データベース接続などの他のヘルスインジケーターも確認します。

サイトのヘルスチェックはDelivery Controllerで実行されます。サイトの規模によっては、これらのチェックの完了に最大1時間かかる場合があります。

DELIVERY CONTROLLER の構成チェック

サイトの健全性チェックの一環として、Delivery Controller の構成チェックでは、Virtual Apps and Desktops サイトに関する Citrix の推奨事項に基づいて、以下の問題が存在するかどうかを確認します。

- 1 つ以上の Delivery Controller が失敗状態にある。
- サイトに Delivery Controller が 1 つしかない。
- Delivery Controller のバージョンが異なる。

健全性チェックの 権限と要件 を満たすことに加えて、Delivery Controller の構成チェックには以下が必要です。

- 少なくとも 1 つの Controller の電源がオンになっていること。
- Controller 上で Broker Service が実行されていること。
- Controller からサイトデータベースへの接続が機能していること。

VDA の健全性チェック

VDA の健全性チェックは、一般的な VDA 登録、セッション起動、およびタイムゾーンリダイレクトの問題の考えられる原因を特定します。

VDA での登録について、Scout は以下をチェックします。

- VDA ソフトウェアのインストール
- VDA マシンのドメインメンバーシップ
- VDA 通信ポートの可用性
- VDA サービスステータス
- Windows ファイアウォール構成
- Controller との通信
- Controller との時刻同期
- VDA 登録ステータス

VDA でのセッション起動について、Scout は以下をチェックします。

- セッション起動通信ポートの可用性
- セッション起動サービスのステータス
- セッション起動 Windows ファイアウォール構成
- VDA リモートデスクトップサービス クライアントアクセスライセンス

- VDA アプリケーション起動パス
- セッション起動レジストリ設定

VDA でのタイムゾーンリダイレクトについて、Scout は以下をチェックします。

- Windows ホットフィックスのインストール
- Citrix ホットフィックスのインストール
- Microsoft グループポリシー設定
- Citrix グループポリシー設定

VDA 上の Profile Management について、Scout は以下をチェックします。

- ハイパーバイザーの検出
- プロビジョニングの検出
- シトリックス バーチャル アプリケーションズ アンド デスクトップ
- Personal vDisk の構成
- ユーザー ストア
- Profile Management Service の状態検出
- Winlogon.exe フックテスト

Profile Management のチェックを実行するには、VDA に Profile Management をインストールして有効にする必要があります。Profile Management の構成チェックの詳細については、Knowledge Center の記事 CTX132805 を参照してください。

StoreFront のヘルスチェック

StoreFront のチェックでは、以下を確認します。

- Citrix Default Domain サービスが実行中であること
- Citrix Credential Wallet サービスが実行中であること
- StoreFront サーバーから Active Directory ポート 88 への接続
- StoreFrontサーバーからActive Directoryポート389への接続
- ベースURLが有効なFQDNであること
- ベースURLから正しいIPアドレスを取得できること
- IISアプリケーションプールが.NET 4.0を使用していること
- 証明書がホストURLのSSLポートにバインドされているかどうか
- 証明書チェーンが完全であるかどうか

- 証明書の有効期限が切れているかどうか
- 証明書がまもなく（30日以内に）期限切れになるかどうか

ライセンスサーバーのチェック

ライセンスサーバーのチェックでは、以下を確認します。

- Delivery Controllerからのライセンスサーバー接続
- ライセンスサーバーのファイアウォールリモートアクセスステータス
- Citrix Licensingサービスのステータス
- ライセンスサーバーのライセンスキャッシュモードの状態
- ライセンスサーバーポートの接続
- Citrix ベンダーデーモン (CITRIX) が実行されているかどうか
- システムクロックが同期されているかどうか
- Citrix Licensing サービスがローカルサービスアカウントで実行されているかどうか
- `CITRIX.opt` ファイルの存在
- カスタマーサクセスサービス資格日
- Citrix ライセンスサーバーの更新
- ライセンスサーバー証明書がDelivery Controllerの信頼されたルートストアにあるかどうか

ヘルスチェックの権限と要件を満たすことに加えて、ライセンスサーバーはドメインに参加している必要があります。そうでない場合、ライセンスサーバーは検出されません。

ヘルスチェックの実行

ヘルスチェック手順は、マシンの選択、チェックの開始、および結果レポートの確認で構成されます。

1. Scout を起動します。マシンの メニューから、 **>** を選択します。開始ページで、 をクリックします。
2. マシンを選択します。**Find machine**をクリックしてマシンを検出します。**Select machines** ページには、サイトで検出されたすべてのVDA、Delivery Controller、およびLicense Serverが一覧表示されます。マシン名で表示をフィルタリングできます。診断情報を収集する各マシンの横にあるチェックボックスを選択し、**Continue**をクリックします。

   その他のコンポーネントタイプ（StoreFront サーバーや VDA マシンなど）を追加するには、「Add machines manually」および「Import VDA machines」を参照してください。Citrix Provisioning™ サーバーまたはライセンスサーバーを手動で追加することはできません。

Scoutは、選択された各マシンで検証テストを自動的に起動し、検証テストに記載されている基準を満たしていることを確認します。検証に失敗した場合、**Status**列にメッセージが表示され、そのマシンのチェックボックスがオフになります。次のいずれかを実行できます。

- 問題を解決し、そのマシンのチェックボックスを再度選択します。これにより、検証テストが再試行されます。
- そのマシンをスキップします（チェックボックスは選択解除のままにします）。そのマシンではヘルスチェックは実行されません。

検証テストが完了したら、**続行**をクリックします。

3. 選択したマシンでヘルスチェックを実行します。概要には、テストが実行されたマシン（検証テストに合格した選択済みのマシン）が一覧表示されます。**チェック開始**をクリックします。

   チェック中およびチェック後：

   - **ステータス**列は、マシンの現在のチェック状態を示します。
   - 進行中のすべてのチェックを停止するには、ページ右下隅にある**チェック停止**をクリックします。（単一のマシンのヘルスチェックをキャンセルすることはできず、選択したすべてのマシンのみをキャンセルできます。チェックが完了したマシンからの情報は保持されます。）.
   - 選択したすべてのマシンのチェックが完了すると、右下隅の**チェック停止**ボタンが**完了**に変わります。
   - チェックが失敗した場合は、**アクション**列の**再試行**をクリックできます。
   - チェックが問題なく完了した場合、**アクション**列は空になります。
   - チェックで問題が見つかった場合は、**詳細表示**をクリックして結果を表示します。
   - 選択したすべてのマシンのチェックが完了した後、**戻る**をクリックしないでください。（クリックすると、チェック結果が失われます。）

4. チェックが完了したら、**完了**をクリックしてScoutの開始ページに戻ります。

ヘルスチェックの結果

レポートを生成するCitrixチェックの場合、レポートには以下が含まれます。

- 結果レポートが生成された日時
- チェックされたマシン
- ターゲットマシンでチェックが探した条件

権限と要件

権限:

- 診断情報を収集するには:
  - 診断情報を収集する各マシンで、ローカル管理者およびドメインユーザーである必要があります。
  - 各マシンで LocalAppData ディレクトリへの書き込み権限が必要です。
- ヘルスチェックを実行するには:
  - ドメインユーザーグループのメンバーである必要があります。
  - フル管理者であるか、サイトに対する読み取り専用および **Run Environment Tests** 権限を持つカスタムロールを持っている必要があります。
  - スクリプトの実行を許可するには、スクリプト実行ポリシーを少なくとも `RemoteSigned` に設定します。例: `Set-ExecutionPolicy RemoteSigned`。**注:** 他のスクリプト実行権限でも機能する場合があります。
- Scout の起動時には、**管理者として実行**を使用します。

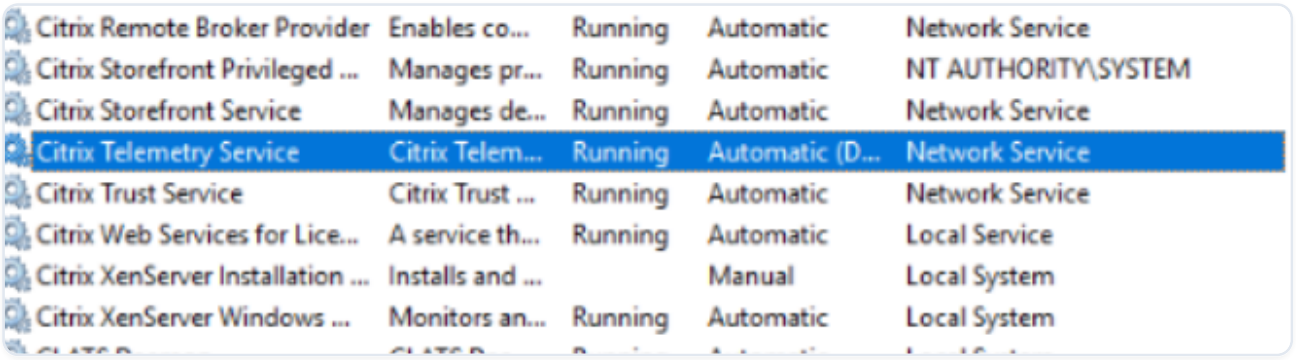
診断情報を収集したり、ヘルスチェックを実行したりする各マシンについて:

- Scout がマシンと通信できる必要があります。
- ファイルとプリンターの共有がオンになっている必要があります。
- PSRemotingとWinRMを有効にする必要があります。マシンではPowerShell 3.0以降も実行されている必要があります。
- マシンでCitrix Telemetry Serviceが実行されている必要があります。
- マシンでWindows Management Infrastructure (WMI) アクセスが有効になっている必要があります。
- 診断コレクションのスケジュールを設定するには、マシンで互換性のあるScoutバージョンが実行されている必要があります。

パス名で指定するユーザー名にドル記号 ($) を使用しないでください。診断情報の収集が妨げられます。

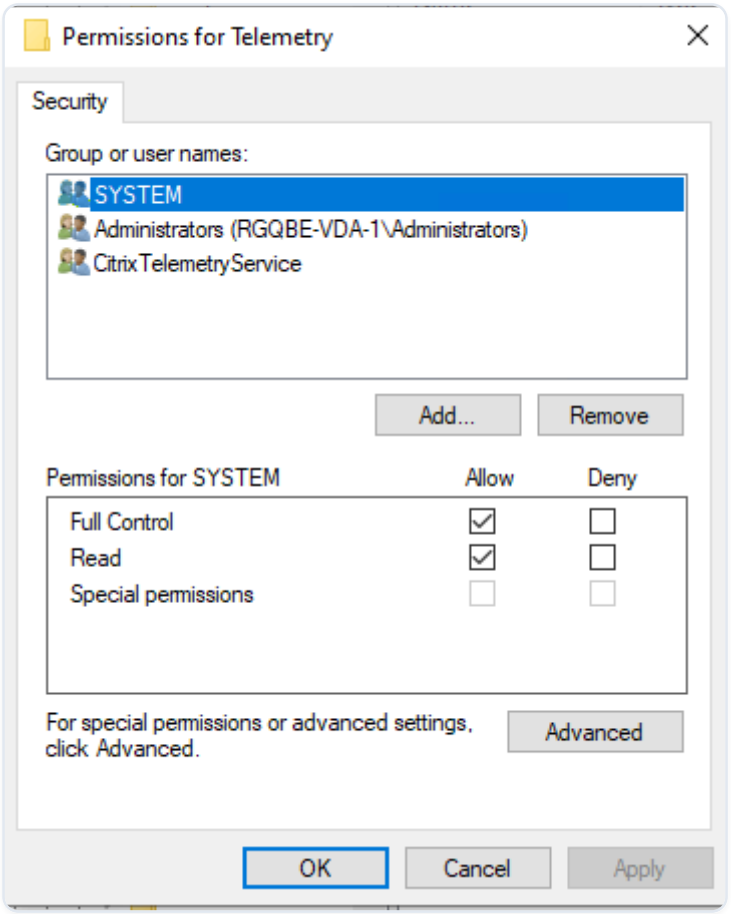
Scoutは、選択したマシンで検証テストを実行し、これらの要件が満たされていることを確認します。

Windows用Telemetry Serviceは、ネットワークサービスで実行されます。

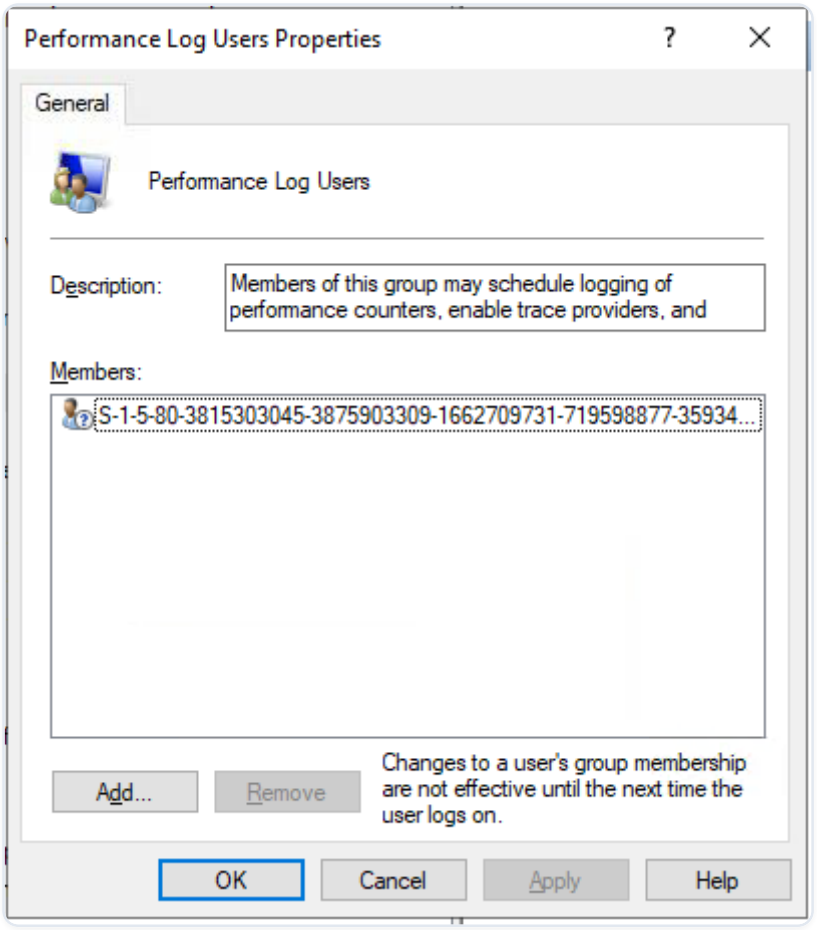


AOTトレースフォルダーは`C:\ProgramData\Citrix\TelemetryService\CitrixAOT`に保存されます。

Administratorグループ、System、およびTelemetry Service SIDのユーザーのみが、`HKEYLOCALMACHINE:SOFTWARE\Citrix\Telemetry`レジストリにアクセスする権限を持っています。



Telemetry Serviceをアンインストールした後も、Telemetry Service SIDはPerformance Log Usersグループに残りますが、手動で削除できます。



検証テスト

診断収集またはヘルスチェックが開始される前に、選択された各マシンに対して検証テストが自動的に実行されます。これらのテストは、要件が満たされていることを確認します。マシンのテストが失敗した場合、Scoutは推奨される是正措置を含むメッセージを表示します。

- **Scoutがこのマシンに到達できません** - 以下を確認してください。
  - マシンが電源オンになっていること。
  - ネットワーク接続が正常に機能していること。(これには、ファイアウォールが適切に構成されていることの確認が含まれる場合があります。)
  - ファイルとプリンターの共有がオンになっていること。手順については、Microsoftのドキュメントを参照してください。
- **PSRemotingとWinRMを有効にする** - PowerShellリモート処理とWinRMを同時に有効にできます。**管理者として実行**を使用して、`Enable-PSRemoting`コマンドレットを実行します。詳細については、コマンドレットに関するMicrosoftのヘルプを参照してください。
- **ScoutにはPowerShell 3.0 (最小) が必要です** - マシンにPowerShell 3.0 (またはそれ以降) をインストールし、PowerShellリモート処理を有効にしてください。

- **このマシン上の LocalAppData ディレクトリにアクセスできません** - アカウントに、マシン上の LocalAppData ディレクトリへの書き込み権限があることを確認してください。
- **Citrix Telemetry Serviceが見つかりません** - Citrix Telemetry Serviceがマシンにインストールされ、開始されていることを確認してください。
- **スケジュールを取得できません** - マシンを(最小) XenApp and XenDesktop 7.14にアップグレードしてください。
- **WMIがマシンで実行されていません** - Windows Management Instrumentation (WMI) アクセスが有効になっていることを確認してください。
- **WMI接続がブロックされています** - WindowsファイアウォールサービスでWMIを有効にしてください。
- **より新しいバージョンのCitrix Telemetry Serviceが必要です** - (バージョンはCollectおよびTrace & Reproduceでのみチェックされます。) マシン上のTelemetry Serviceのバージョンをアップグレードしてください (インストールとアップグレードを参照)。サービスをアップグレードしない場合、そのマシンは**Collect**または**Trace & Reproduce**アクションに含まれません。
- **Scoutがこのマシン上のsystemdソケットに接続できません** - 以下を確認してください。
  - ポート 7503 が開いていること。`systemd ctxtelemetry.socket` がマシン上のポート 7503 でリッスンしていることを確認してください。`ctxtelemetry.socket` ポートが変更されている場合、ポートが異なる可能性があります。ポートを調整するには、Scout の構成 を参照してください。
  - ネットワーク接続が正しく機能していることを確認します。（これには、ファイアウォールが適切に構成されていることの確認が含まれる場合があります。）
- **このマシンでLinux VDAテレメトリーサービスが開始されていません** - 以下を確認してください。
  - ポート7502が開いていることを確認します。Linux VDAテレメトリーサービスがマシンにインストールされ、開始されていることを確認します。テレメトリーサービスポートが変更されている場合、ポートが異なる可能性があります。ポートを調整するには、Scoutの構成を参照してください。
  - ネットワーク接続が正しく機能していることを確認します。（これには、ファイアウォールが適切に構成されていることの確認が含まれる場合があります。）

バージョン互換性

このバージョンのScout (3.x) は、Citrix Virtual Apps and Desktops (または最低でもXenApp and XenDesktop 7.14) のコントローラーおよびVDAで実行することを目的としています。

| 機能 | スカウト 2.23 | スカウト 3.0 | --- | --- | ---| -- | Citrix Virtual Apps and Desktops (および XenApp and XenDesktop 7.14〜7.18) をサポート | はい | はい XenDesktop 5.x、7.1〜7.13をサポート | はい | いいえ XenApp 6.x、7.5〜7.13をサポート | はい | いいえ 製品に同梱 | 7.1〜7.13 | 7.14以降 CTX記事からダウンロード可能 | はい | いいえ CDFトレースをキャプチャ | はい | はい Always-on-Traces (AOT) をキャプチャ | いいえ | はい 診断データの収集を許可 | 一度に最大10台のマシン（デフォルト） | 無制限（リソースの可用性による） 診断データをCitrixに送信することを許可 | はい | はい 診断データをローカルに保存することを許可 | はい | はい Citrix Cloud™資格情報をサポート | いいえ | はい Citrix資格情報をサポート | はい | はい アップロード用のプロキシサーバーをサポート | はい | はい スケジュールを調整 | 該当なし | はい スクリプトのサポート | コマンドライン（ローカルControllerのみ） | Call Homeコマンドレットを使用したPowerShell（Telemetry Serviceがインストールされているすべてのマシン） ヘルスチェック | いいえ | はい データマスキング | いいえ | 3.17以降

インストールとアップグレード

デフォルトでは、VDAまたはControllerをインストールまたはアップグレードすると、Citrix Telemetry Serviceの一部としてScoutが自動的にインストールまたはアップグレードされます。

VDAのインストール時にCitrix Telemetry Serviceを省略した場合、または後でサービスを削除した場合は、Citrix Virtual Apps and Desktopsインストールメディアの`x64\Virtual Desktop Components`または`x86\Virtual Desktop Components`フォルダーから`TelemetryServiceInstaller_xx.msi`を実行します。

Collectまたは**Trace & Reproduce**アクションを選択すると、マシンで古いバージョンのCitrix Telemetry Serviceが実行されている場合に通知されます。Citrixでは、サポートされている最新バージョンを使用することをお勧めします。そのマシンでTelemetry Serviceをアップグレードしない場合、そのマシンは**Collect**または**Trace & Reproduce**アクションに含まれません。Telemetry Serviceをアップグレードするには、インストールと同じ手順を使用します。

アップロードの承認

診断コレクションをCitrixにアップロードする予定がある場合は、Citrixアカウントまたは Citrix Cloudアカウントが必要です。（これらは、Citrixダウンロードにアクセスしたり、Citrix Cloud Control Centerにアクセスしたりするために使用する資格情報です。）アカウントの資格情報が検証されると、トークンが発行されます。

CitrixアカウントまたはCitrix Cloudアカウントで認証する場合は、リンクをクリックして、デフォルトのブラウザーでHTTPSを使用してCitrix Cloudにアクセスします。Citrix Cloudの資格情報を入力すると、トークンが表示されます。トークンをコピーしてScoutに貼り付けます。その後、Scoutウィザードを続行できます。

トークンは、Scoutを実行しているマシンにローカルに保存されます。次回**Collect**または**Trace & Reproduce**を実行するときにそのトークンを使用できるようにするには、**Store token and skip this step in the future**チェックボックスをオンにします。

Scoutの開始ページで**Schedule**を選択するたびに、再承認する必要があります。スケジュールを作成または変更するときに、保存されたトークンを使用することはできません。

アップロードにプロキシを使用する

プロキシサーバーを使用してコレクションをCitrixにアップロードする場合は、ブラウザーのインターネットプロパティ用に構成されたプロキシ設定を使用するようにScoutに指示できます。または、プロキシサーバーのIPアドレスとポート番号を指定することもできます。

マシンの検索

Collect、**Trace & Reproduce**、および**Schedule**の手順では、Scoutは自動的に検出したControllerとVDAを一覧表示します。

Delivery ControllerからScout Health Checkを実行するときに、**Find machine**をクリックすると、デリバリーコントローラー、VDA、ライセンスサーバー、StoreFrontサーバーなどのマシンが検出されます。

ドメインに参加しているがDelivery ControllerではないマシンからScout Health Checkを実行すると、Scoutはマシンを自動的に検出できません。手動でマシンを追加するか、VDAマシンをインポートする必要があります。

マシンを手動で追加する

Scout が検出したコントローラーと VDA を一覧表示した後、StoreFront サーバー、ライセンスサーバー、Citrix Provisioning サーバーなど、展開内の他のマシンを手動で追加できます。

ヘルスチェック の実行時：

- ドメイン内の Citrix ライセンスサーバーは自動的に検出されます。ライセンスサーバーを手動で追加することはできません。
- ヘルスチェックは現在、Citrix Provisioning サーバーをサポートしていません。

検出されたマシンを一覧表示するScoutの任意のページで、**+ Add machine**をクリックします。追加するマシンのFQDNを入力し、**Continue**をクリックします。必要に応じて、他のマシンを追加するために繰り返します。（FQDNの代わりにDNSエイリアスを入力しても有効に見えることがありますが、ヘルスチェックが失敗する可能性があります。）

手動で追加されたマシンは、常に検出されたマシンよりも上の、マシンリストの先頭に表示されます。

手動で追加されたマシンを識別する簡単な方法は、行の右端にある赤い削除ボタンです。そのボタンがあるのは手動で追加されたマシンのみです。検出されたマシンにはありません。

手動で追加されたマシンを削除するには、行の右端にある赤いボタンをクリックします。削除を確認します。他の手動で追加されたマシンを削除するために繰り返します。

Scout は、手動で追加されたマシンを削除するまで記憶しています。Scout を閉じてから再度開くと、手動で追加されたマシンは引き続きリストの先頭に表示されます。

StoreFront サーバーで **Trace & Reproduce** を使用する場合、CDF トレースは収集されません。ただし、その他のすべてのトレース情報は収集されます。

> **ヒント：**
>
> Scoutは、Citrix Virtual Apps and Desktops LTSR 2507バージョン以降のStoreFrontタイプのマシンで実行されている場合、**Collect**ページに**+ Add machine**ボタンを表示することをサポートしています。このオプションにより、ユーザーは同じクラスター内の複数のStoreFront Serverマシンを手動で追加し、同時に収集をトリガーできます。*TelemetryService*の古いバージョンはこの機能をサポートしていません。

VDA マシンをインポートする

ヘルスチェック の実行時に、展開内の VDA マシンをインポートできます。

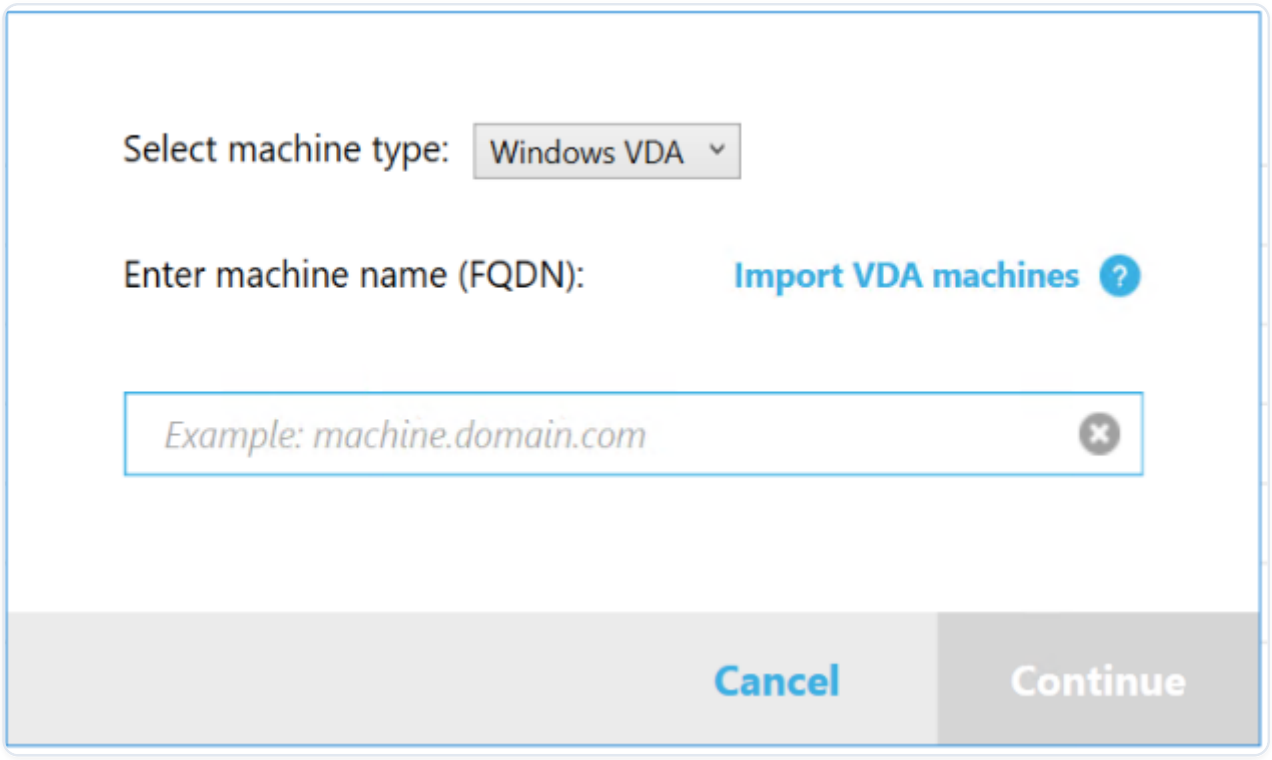
1. Delivery Controller または Connector で、PowerShell コマンドを使用してマシンリストファイルを生成します。Connector では、Citrix 資格情報を入力し、ポップアップダイアログで顧客を選択する必要があります。

   ```
   Get-BrokerMachine| foreach { $_.DnsName } | out-file C:\machineList.txt
   ```

2. machineList.txtファイルを、Scout Health Checkを起動するドメイン参加済みマシンにコピーします。
3. Scout Health Check ページで、 をクリックします。
4. マシンタイプを選択します。
5. をクリックします。
6. machineList.txt ファイルを選択します。

7. をクリックします。

インポートされた VDA マシンが Scout Health Check ページに一覧表示されます。



診断情報の収集

手順には、マシンの選択、診断情報収集の開始、および収集を含むファイルを Citrix にアップロードするかローカルに保存する作業が含まれます。

1. Scout を起動します。マシンの メニューから、 **>** を選択します。開いたページで、 をクリックします。
2. マシンを選択します。

   - Controller では、 ページにサイト内のすべての VDA と Controller が一覧表示されます。マシン名で表示をフィルターできます。他のマシン（StoreFront や Citrix Provisioning サーバーなど）を手動で追加するには、「マシンを手動で追加する」を参照してください。
   - StoreFrontでは、「**マシンの選択**」ページにローカルマシンのみが表示されます。同じクラスター内の他のStoreFrontマシンを追加するには、「手動でマシンを追加」を参照してください。
   - その他のコンポーネント（VDA サーバーなど）では、 ページにはローカルマシンのみが表示されます。マシンの手動追加はサポートされていません。

   診断情報を収集する各マシンの横にあるチェックボックスをオンにし、「**続行**」をクリックします。

Scoutは、選択された各マシンで検証テストを自動的に起動し、検証テストに記載されている基準を満たしていることを確認します。検証に失敗した場合、「**ステータス**」列にメッセージが表示され、そのマシンのチェックボックスはオフになります。次のいずれかを実行できます。

- 問題を解決してから、そのマシンのチェックボックスを再度オンにします。これにより、検証テストが再試行されます。
- そのマシンをスキップします（チェックボックスをオフのままにします）。そのマシンからは診断情報は収集されません。

検証テストが完了したら、**続行**をクリックします。

3. 診断情報を収集します。概要には、診断情報が収集されるすべてのマシン（検証テストに合格した選択済みのマシン）が一覧表示されます。**収集開始**をクリックします。

   収集中:

   - **ステータス**列には、マシンの現在の収集状態が表示されます。
   - 単一マシンでの進行中の収集を停止するには、そのマシンの**アクション**列にある**キャンセル**をクリックします。
   - 進行中のすべての収集を停止するには、ページの右下隅にある**収集を停止**をクリックします。収集が完了したマシンからの診断情報は保持されます。収集を再開するには、各マシンの**アクション**列にある**再試行**をクリックします。
   - 選択したすべてのマシンで収集が完了すると、右下隅にある**収集を停止**ボタンが**続行**に変わります。
   - 診断情報を再度収集するには、そのマシンの**アクション**列にある**再度収集**をクリックします。新しい収集は以前の収集を上書きします。
   - 収集に失敗した場合は、**アクション**列にある**再試行**をクリックできます。正常に収集されたもののみがアップロードまたは保存されます。
   - 選択したすべてのマシンで収集が完了した後、**戻る**をクリックしないでください。（クリックすると、収集は失われます。）

   収集が完了したら、**続行**をクリックします。

4. コレクションを保存またはアップロードします。ファイルをCitrixにアップロードするか、ローカルマシンに保存するかを選択します。

   今すぐファイルをアップロードする場合は、手順5に進みます。

   ファイルをローカルに保存することを選択した場合:

- Windowsの**保存**ダイアログボックスが表示されます。目的の場所に移動します。
- ローカル保存が完了すると、ファイルのパス名が表示され、リンクされます。ファイルを表示できます。後でファイルをCitrixにアップロードできます。CTX136396を参照してください。

完了をクリックしてScoutの開始ページに戻ります。この手順でこれ以上ステップを完了する必要はありません。

5. アップロードの認証を行い、必要に応じてプロキシを指定します。詳細については、(#upload-authorization)を参照してください。

   - Scoutを通じて認証していない場合は、この手順に進みます。
   - Scoutを通じて認証済みの場合、保存されている認証トークンがデフォルトで使用されます。これを行う場合は、このオプションを選択して**続行**をクリックします。このコレクションの資格情報は要求されません。手順6に進みます。
   - 以前に認証済みだが、再認証して新しいトークンを取得したい場合は、**変更/再認証**をクリックしてこの手順に進みます。

   アップロードを認証するためにCitrix資格情報を使用するか、Citrix Cloud資格情報を使用するかを選択します。**続行**をクリックします。資格情報ページは、保存されたトークンを使用していない場合にのみ表示されます。

   資格情報ページで:

   - ファイルアップロードにプロキシサーバーを使用したい場合は、**プロキシの構成**をクリックします。Scoutにブラウザのインターネットプロパティに設定されているプロキシ設定を使用するように指示できます。または、プロキシサーバーのIPアドレスとポート番号を入力することもできます。プロキシダイアログボックスを閉じます。
   - Citrix Cloudアカウントの場合、**トークンの生成**をクリックします。デフォルトのブラウザがCitrix Cloudページに起動し、トークンが表示されます。トークンをコピーし、Scoutページに貼り付けます。
   - Citrixアカウントの場合、資格情報を入力します。

   完了したら、「**続行**」をクリックします。

6. アップロードに関する情報を入力します。

   - 名前フィールドには、収集された診断ファイルのデフォルト名が含まれています。ほとんどのコレクションではこれで十分ですが、名前を変更することもできます。(デフォルト名を削除して名前フィールドを空のままにすると、デフォルト名が使用されます。)

- 必要に応じて、8桁のCitrixサポートケース番号を指定します。
- オプションの「**説明**」フィールドに、問題について説明し、該当する場合は問題が発生した時期を示します。

完了したら、「**アップロードの開始**」をクリックします。

アップロード中、ページの左下部分にアップロードの完了率が概算で表示されます。進行中のアップロードをキャンセルするには、「**アップロードの停止**」をクリックします。

アップロードが完了すると、その場所のURLが表示され、リンクされます。リンクをたどってCitrixの場所にアクセスし、アップロードの分析を表示したり、リンクをコピーしたりできます。

「**完了**」をクリックして、Scoutの開始ページに戻ります。

トレースと再現

「**トレースと再現**」手順は、マシンの選択、トレースの開始、問題の再現、診断コレクションの完了、そしてファイルをCitrixにアップロードするかローカルに保存することから構成されます。

この手順は標準の「**収集**」手順に似ています。ただし、マシンでトレースを開始し、それらのマシンで問題を再作成することができます。すべての診断コレクションにはAOTトレース情報が含まれています。この手順では、トラブルシューティングに役立つCDFトレースが追加されます。

1. Scoutを起動します。マシンの「**スタート**」メニューから「**Citrix > Citrix Scout**」を選択します。開始ページで、「**トレースと再現**」をクリックします。
2. マシンを選択します。**マシンを選択**ページには、サイト内のすべてのVDAとコントローラーが一覧表示されます。マシン名で表示をフィルターできます。トレースと診断を収集する各マシンの横にあるチェックボックスをオンにします。次に、**続行**をクリックします。

   その他のマシンを手動で追加するには (StoreFrontまたはCitrix Provisioningサーバーなど)、マシンを手動で追加するを参照してください。

   Scoutは、選択した各マシンで検証テストを自動的に起動し、検証テストに記載されている基準を満たしていることを確認します。マシンの検証が失敗した場合、**ステータス**列にメッセージが表示され、そのマシンのチェックボックスはオフになります。次のいずれかを実行できます。

   - 問題を解決してから、そのマシンのチェックボックスを再度オンにします。これにより、検証テストが再試行されます。

- そのマシンをスキップします（チェックボックスをオフのままにします）。そのマシンからは診断情報とトレースは収集されません。

検証テストが完了したら、**Continue** をクリックします。

3. トレースを開始します。概要には、トレースが収集されるすべてのマシンが一覧表示されます。**Start Tracing** をクリックします。

   選択したマシンのいずれかまたは複数で、発生した問題を再現します。その間、トレースの収集は続行されます。問題の再現が完了したら、Scout で **Continue** をクリックします。これによりトレースが停止します。

   トレースを停止した後、トレース中に問題を再現したかどうかを示します。

4. マシンから診断情報を収集します。**Start Collecting** をクリックします。収集中に：

   - **Status** 列には、マシンの現在の収集状態が表示されます。
   - 単一マシンで進行中の収集を停止するには、そのマシンの **Action** 列にある **Cancel** をクリックします。
   - 進行中のすべての収集を停止するには、ページの右下隅にある **Stop Collection** をクリックします。収集が完了したマシンからの診断情報は保持されます。収集を再開するには、各マシンの **Action** 列にある **Retry** をクリックします。
   - 選択したすべてのマシンで収集が完了すると、右下隅の **Stop Collection** ボタンが **Continue** に変わります。
   - マシンから診断情報を再度収集するには、そのマシンの **Action** 列にある **Collect Again** をクリックします。新しい収集は以前のものを上書きします。
   - 収集が失敗した場合、**Action** 列にある **Retry** をクリックできます。正常に収集されたもののみがアップロードまたは保存されます。
   - 選択したすべてのマシンで収集が完了したら、**Back** をクリックしないでください。（クリックすると、収集は失われます。）

   収集が完了したら、**続行**をクリックします。

5. コレクションを保存またはアップロードします。ファイルをCitrixにアップロードするか、ローカルに保存するかを選択します。

   今すぐファイルをアップロードする場合は、手順6に進みます。

   ファイルをローカルに保存する場合:

   - Windowsの保存ダイアログボックスが表示されます。目的の場所を選択します。

- ローカル保存が完了すると、ファイルのパス名が表示され、リンクされます。ファイルを表示できます。注意: ファイルは後でCitrixからアップロードできます。Citrix Insight Servicesについては、CTX136396を参照してください。

完了をクリックしてScoutの開始ページに戻ります。この手順でこれ以上完了する必要のある手順はありません。

6. アップロードの認証を行い、必要に応じてプロキシを指定します。このプロセスの詳細については、アップロード認証を確認してください。

   - Scoutを介して認証していない場合は、この手順に進みます。
   - Scoutを介して認証した場合、保存されている認証トークンがデフォルトで使用されます。この操作を行う場合は、このオプションを選択して**続行**をクリックします。このコレクションの資格情報は要求されません。手順7に進みます。
   - 以前に認証済みで、再認証して新しいトークンを取得したい場合は、**変更/再認証**をクリックしてこの手順に進みます。

   アップロードを認証するために、Citrix資格情報を使用するか、Citrix Cloud資格情報を使用するかを選択します。**続行**をクリックします。資格情報ページは、保存されたトークンを使用していない場合にのみ表示されます。

   資格情報ページで:

   - ファイルアップロードにプロキシサーバーを使用する場合は、**プロキシの構成**をクリックします。Scoutに、ブラウザーのインターネットプロパティで構成されているプロキシ設定を使用するように指示できます。または、プロキシサーバーのIPアドレスとポート番号を入力することもできます。プロキシダイアログボックスを閉じます。
   - Citrix Cloudアカウントの場合、**トークンの生成**をクリックします。デフォルトのブラウザーがCitrix Cloudページを起動し、トークンが表示されます。トークンをコピーし、Scoutページに貼り付けます。
   - Citrixアカウントの場合は、資格情報を入力します。

   完了したら、**続行**をクリックします。

7. アップロードに関する情報を提供します。

   アップロードの詳細を入力します。

   - 名前フィールドには、収集された診断ファイルのデフォルト名が含まれています。ほとんどの収集ではこれで十分ですが、名前を変更することもできます。(デフォルト名を削除して名前フィールドを空のままにした場合、デフォルト名が使用されます。)

- オプションで、8桁のCitrixサポートケース番号を指定します。
- オプションの「説明」フィールドに、問題について説明し、該当する場合は問題が発生した時期を示します。

完了したら、**アップロードの開始**をクリックします。

アップロード中、ページの左下部分にアップロードの完了率が概算で表示されます。進行中のアップロードをキャンセルするには、**アップロードの停止**をクリックします。

アップロードが完了すると、その場所のURLが表示され、リンクされます。リンクをたどってCitrixの場所に移動し、アップロードの分析を表示したり、リンクをコピーしたりできます。

完了をクリックして、Scoutの開始ページに戻ります。

ScoutはTraceLoggingプロバイダーをサポート

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

Citrix Virtual Apps and Desktops バージョン 2411 以降、Scout は TraceLogging プロバイダーをサポートしています。このプロバイダーは追加のデコードファイルを必要とせず、同じプロバイダーに対して最大 8 つのトレースセッションからイベントを有効にして受信できます。この機能はデフォルトで有効になっています。

追加のログ収集を有効にする

追加のログ収集を有効にする機能を使用すると、perfmon、Netsh、DebugView、Wiresharkなどのツールでトレースおよび再現機能を使用できます。

2407 リリース以降、追加のログ収集を有効にすると、Scout はマシンにインストールされている CDC 関連ツールを自動的に検出し、CDC ツール関連のトレースログを zip パッケージに自動収集します。これらの zip ファイルをカスタマイズして Scout に添付できます。この自動化により、Citrix Scout をより効果的に使用でき、問題を迅速に診断するのに役立ちます。

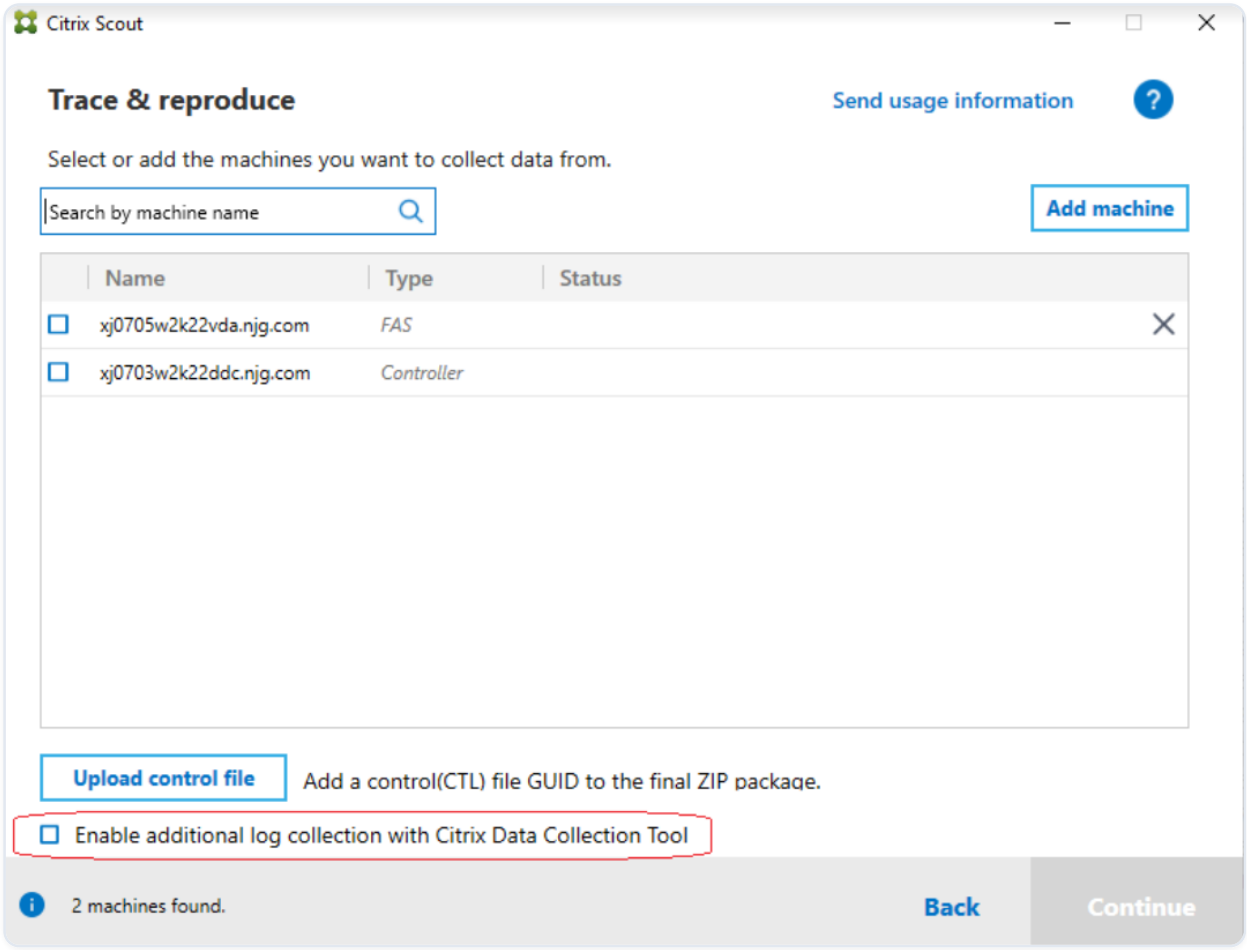
> **注:**
>
> これはローカルマシンにのみ適用されます。
>
> 追加のログ収集を有効にするには、次の必要なツールがインストールされており、指定された場所にディレクトリが手動で作成されていることを確認してください。

ツールのインストール場所:

- **Procdump** ログ: **Procdump** をダウンロードし、%ProgramData%\Citrix\TelemetryService\CDC\Lib\Resources\Tools\Procdump\procdump.exe に配置します。
- **StoreFront** ログ: **DbgView** をダウンロードし、%ProgramData%\Citrix\TelemetryService\CDC\Lib\Resources\Tools\DebugView\Dbgview.exe に配置します。
- **Procmon** ログ: **Process Monitor** をダウンロードし、%ProgramData%\Citrix\TelemetryService\CDC\Lib\Resources\Tools\ProcessMonitor\Procmon.exe に配置します。
- **Wireshark** ログ: システムに **Wireshark** を手動でインストールします。

追加のログを収集するには：

1. Scout のホームページで、**トレースと再現**をクリックします。
2. データを収集する **マシンの選択または追加** ページで、ローカルマシンのチェックボックスをオンにします。ステータスは *Verified* と表示されている必要があります。
3. **Citrix Data Collection Tool を使用した追加のログ収集を有効にする** チェックボックスをオンにして、追加のログ収集を有効にします。
4. 「**コントロールファイルのアップロード**」ボタンをクリックして、1つのCTLファイルをロードします。このボタンを使用すると、ScoutでのAOTコレクションのために、AOTコレクションリストに追加のGUIDを追加できます。
5. 「**続行**」をクリックし、トレースと再現の手順に従います。
6. 完了後、zip ファイル内のログを確認します。ログは *CDCLogs* フォルダーに圧縮されています。



注:

トレースに Procmon ツールが選択されている場合、Process Monitor のログはすぐに大きくなる可能性があります。必要なツールのみを選択するようにしてください。ログのサイズは *%temp%\Scout-CDC-Log* で監視することもできます。

コレクションのスケジュール設定

注:

現在、コレクションはスケジュールできますが、ヘルスチェックはできません。

スケジュール手順は、マシンを選択し、スケジュールを設定またはキャンセルすることで構成されます。スケジュールされたコレクションは、Citrixに自動的にアップロードされます。(PowerShellインターフェイスを使用して、スケジュールされたコレクションをローカルに保

> 存できます。(/ja-jp/citrix-virtual-apps-desktops/current-release/manage-deployment/cis.html#citrix-call-home)を参照してください。)

1. Scoutを起動します。マシンのスタートメニューから、**Citrix > Citrix Scout**を選択します。開いたページで、**Schedule**をクリックします。
2. マシンを選択します。サイト内のすべてのVDAとコントローラーが一覧表示されます。マシン名で表示をフィルターできます。

   グラフィカルインターフェイスを使用してVDAとコントローラーをインストールしたときに、Call Homeスケジュールを設定した場合 ((/ja-jp/citrix-virtual-apps-desktops/current-release/manage-deployment/cis.html#citrix-call-home)を参照)、Scoutはデフォルトでそれらの設定を表示します。このバージョンのScoutを使用して、スケジュールされたコレクションを初めて開始したり、以前に構成したスケジュールを変更したりできます。

   コンポーネントのインストール中にマシンごとにCall Homeを有効/無効にした場合でも、Scoutで構成されたスケジュールは、選択したすべてのマシンに影響します。

   診断情報を収集する各マシンの横にあるチェックボックスをオンにして、「**続行**」をクリックします。

   その他のマシン (StoreFrontサーバーやCitrix Provisioningサーバーなど) を手動で追加するには、(#add-machines-manually)を参照してください。

   Scoutは、選択した各マシンで検証テストを自動的に起動し、検証テストの基準を満たしていることを確認します。マシンの検証が失敗した場合、**ステータス**列にメッセージが表示され、そのマシンのチェックボックスはオフになります。次のいずれかを実行できます。

   - 問題を解決してから、マシンのチェックボックスをもう一度選択します。これにより、検証テストが再試行されます。
   - そのマシンをスキップします（チェックボックスをオフのままにします）。そのマシンからは診断（またはトレース）は収集されません。

   検証テストが完了したら、**Continue**をクリックします。

   概要ページには、スケジュールが適用されるマシンが一覧表示されます。**Continue**をクリックします。
3. スケジュールを設定します。診断情報を収集するタイミングを指定します。注意：スケジュールは、選択したすべてのマシンに影響します。

   - 選択したマシンに週次スケジュールを構成するには、**Weekly**をクリックします。曜日を選択します。コレクションを開始する時刻 (24時間形式) を入力します。

- 選択したマシンに日次スケジュールを構成するには、**Daily**をクリックします。コレクションを開始する時刻 (24時間形式) を入力します。
- 選択したマシンに対する既存のスケジュールをキャンセルし（別のスケジュールに置き換えない）、 をクリックします。これにより、それらのマシンに対して以前に構成されていたスケジュールがすべてキャンセルされます。

続行をクリックします。

4. アップロードの認証を行い、必要に応じてプロキシを指定します。このプロセスの詳細については、アップロード認証 を参照してください。注意：Scout スケジュールを使用している場合、保存されたトークンを使用して認証することはできません。

   アップロードの認証に Citrix 資格情報を使用するか、Citrix Cloud 資格情報を使用するかを選択します。 をクリックします。

   資格情報ページで：

   - ファイルのアップロードにプロキシサーバーを使用する場合は、 をクリックします。Scout に、ブラウザーのインターネットプロパティで構成されているプロキシ設定を使用するように指示できます。または、プロキシサーバーの IP アドレスとポート番号を入力することもできます。プロキシダイアログボックスを閉じます。
   - Citrix Cloud アカウントの場合は、 をクリックします。デフォルトのブラウザーが Citrix Cloud ページに起動し、トークンが表示されます。トークンをコピーし、Scout ページに貼り付けます。
   - Citrix アカウントの場合は、資格情報を入力します。

   完了したら、 をクリックします。

   構成されたスケジュールを確認します。 をクリックして Scout の開始ページに戻ります。

   コレクション中、選択された各マシンの Windows アプリケーションログには、コレクションとアップロードに関するエントリが含まれます。

データマスキング

Citrix Scout を使用して収集された診断情報には、セキュリティ上機密性の高い情報が含まれる場合があります。Citrix Scout のデータマスキング機能を使用すると、診断ファイルを Citrix にアップロードする前に、機密データをマスクできます。

Scout のデータマスキングは、IP アドレス、マシン名、ドメイン名、ユーザー名、ハイパーバイザー名、デリバリーグループ名、カタログ名、アプリケーション名、および SID をマスクするように構成されています。

> **注:**
>
> CDF トレースは暗号化されており、マスクできません。
>
> Linux VDA ログは `.tar.gz2` 形式に圧縮されており、マスクできません。

新しい診断情報を収集し、データマスキングを実行する

Citrix Scoutのデータマスキング機能を使用するには、コマンドラインからScoutを起動します。

1. Windowsで、コマンドプロンプトを管理者として開きます。
2. Scoutがインストールされているディレクトリに移動します: `cd C:\Program Files\Citrix\Telemetry Service`。
3. Scoutを起動します: `ScoutUI.exe datamasking`。
4. 診断情報を収集するには、**Collect** または **Trace & Reproduce** をクリックします。
5. 収集が完了したら、**Enable data masking** を選択します。このオプションはデフォルトで有効になっています。
6. データマスクを構成します。デフォルトのルールを使用することも、ルールをカスタマイズすることもできます。
7. 診断情報コレクションをアップロードするか保存するかを選択します。
   - **Upload the diagnostics collection to Citrix** を選択すると、マスクされた診断ファイルがCitrixにアップロードされます。
   - **Save the diagnostics collection on your local machine** を選択すると、元の診断情報とマスクされた診断情報の両方が指定された場所に保存されます。

既存の診断情報に対してデータマスキングを実行する

1. Windowsで、コマンドプロンプトを管理者として開きます。
2. Scoutがインストールされているディレクトリに移動します: `cd C:\Program Files\Citrix\Telemetry Service`。
3. データマスキングモードでScoutを直接起動します: `ScoutUI.exe datamasking filePath`。
4. 「データマスキングを有効にする」を選択して続行します。このオプションはデフォルトで有効になっています。

5. データマスクを構成します。デフォルトのルールでデータマスキングを実行することも、ルールをカスタマイズすることもできます。
6. 診断コレクションをアップロードするか保存するかを選択します。

    - **診断コレクションをCitrixにアップロード**を選択した場合、マスクされた診断ファイルがCitrixにアップロードされます。
    - **診断コレクションをローカルマシンに保存**を選択した場合、元の診断とマスクされた診断の両方が指定された場所に保存されます。

マスクされたデータファイルとマッピングファイルの場所

診断コレクションをアップロードまたは保存した後、リンクをクリックして元の診断とマスクされた診断を開き、マッピング情報ファイルを開きます。

使用状況データ収集

Scoutを使用すると、CitrixはGoogle Analyticsを使用して匿名の使用状況データを収集し、将来の製品機能と改善に役立てます。データ収集はデフォルトで有効になっています。

使用状況データの収集とアップロードを変更するには、Scout UIの**設定**アイコンをクリックします。その後、**はい**または**いいえ**を選択し、**保存**をクリックして情報を送信するかどうかを選択できます。

Scoutの使用状況データ収集(/en-us/citrix-virtual-apps-desktops/current-release/media/scout-usage.png)

Scout 機能のコマンドラインインターフェイス

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

以下の機能にコマンドが追加されました。

- ヘルプ
- 診断の収集
- トレースの開始
- トレースの停止
- 進行中のトレースセッションのリスト
- CDC の開始と停止

注:

リモートトレースセッションを実行する場合、新しいテレメトリバージョンが VDA と DDC の両方にインストールされている必要があります。Scout コマンドラインは Citrix Virtual Apps and Desktops バージョン 2411 以降でサポートされており、以前のバージョンの `TelemetryService` はこの機能をサポートしていないため、このインストールが必要です。

次の表に、新しく追加されたコマンドを示します。

ヘルプ

コマンドラインインターフェイス	説明	例
`ScoutCLI.exe -h`	コンテキストに応じたヘルプを表示します。	`ScoutCLI.exe -h` `ScoutCLI.exe -help`

診断情報を収集するためのコマンド

コマンドラインインターフェイス	説明	例
`ScoutCLI.exe Collect -exclude <collector>`	指定されたコレクター（Windows Management Instrumentation (WMI) プロセス、レジストリ、クラッシュレポート、ヘッダー、トレース、`msi`、`vcu`、ツールテレメトリ、ローカルデータ）からの診断情報を除外します。	`ScoutCLI.exe collect -exclude wmi, localdata -output "C:/Logs/mydata.zip"`
`ScoutCLI.exe Collect -output <filename>`	出力ログファイルを、`.zip` をサフィックスとして保存する場所を指定します。	
`ScoutCLI.exe Collect -fqdn <hostname>`	サイト内の指定されたマシンで診断情報を収集します。	`ScoutCLI.exe collect -fqdn hostname -exclude`

コマンドラインインターフェイス	説明	例
		`wmi, localdata -output "C:/Logs/mydata.zip"`

トレースの開始

コマンドラインインターフェイス	説明	例
`ScoutCLI.exe StartTrace -guids <filename (xxx.ctl)>`	指定されたGUIDのターゲットモジュールのログを収集します。	ローカルマシンのトレース開始の例 - `ScoutCLI.exe StartTrace -guids C:\Logs\provider1.ctl -output C:\Logs\xxx.etl -name session1 -level 16 -max 50`; リモートマシンのトレース開始の例 - `ScoutCLI.exe StartTrace -fqdn hostname -guids C:\Logs\provider1.ctl -output C:\Logs\xxx.etl -name session1 -level 16 -max 50`
`ScoutCLI.exe StartTrace -output <filename>`	出力ログファイルを、.etl をサフィックスとして保存する場所を指定します。	
`ScoutCLI.exe StartTrace -name <session name>`	トレースセッションの名前を定義します。	
`ScoutCLI.exe StartTrace -level <value>`	ターゲット診断の詳細をログに記録するログレベルを選択します。デフォルト値は16です。	
`ScoutCLI.exe StartTrace -max <value>`	最大ログファイルサイズをMB単位で指定します。デフォルト値は50です。	
`ScoutCLI.exe StartTrace -fqdn <hostname>`	サイト内の指定されたマシンでトレースを開始します。	

トレースの停止

コマンドラインインターフェイス	説明	例
`ScoutCLI.exe StopTrace -name <session name>`	指定されたトレースセッションを停止します。	`ScoutCLI.exe StopTrace -name session1`

コマンドラインインターフェイス	説明	例
`ScoutCLI.exe StopTrace -fqdn <hostname>`	サイト内の指定されたマシンでトレースを停止します。リモートの `.etl` がコピーされるローカルパスを割り当てるには、-o オプションが必要です。	`ScoutCLI.exe StopTrace -fqdn hostname -name session1 -output C:\Logs\xxx.etl`
`ScoutCLI.exe StopTrace -output <filename>`	出力ログファイルをサフィックス .etl で保存する場所を指定します。	

進行中のトレースセッションを一覧表示

コマンドラインインターフェイス	説明	例
`ScoutCLI.exe ListSession -name <session name>`	指定されたトレースセッションの詳細を表示します。名前が指定されていない場合は、実行中のすべてのトレースセッションの詳細を表示します。	`ScoutCLI.exe ListSession -name session1`
`ScoutCLI.exe ListSession -fqdn <hostname>`	サイト内の指定されたマシンでトレースの詳細を表示します。	`ScoutCLI.exe ListSession -fqdn hostname -name session1`

CDC の開始と停止

コマンドラインインターフェイス	説明	例
`ScoutCLI.exe StartCDC -config <filename>`	Citrix Diagnostic Collectors (CDC) ツールのパラメーターの JSON 構成ファイルを指定します。	`ScoutCLI.exe StartCDC -config xxx.json -path C:\Logs`
`ScoutCLI.exe StartCDC -path <folder>`	出力ログファイルの保存場所を指定します。	

コマンドラインインターフェイス	説明	例
`ScoutCLI.exe StopCDC`	CDC ツールの収集を停止します。	`ScoutCLI.exe StopCDC`

Call Home の主要データポイント

Call Home は、以下の主要データポイントを収集します。

(M) = 手動収集時のみ取得 (PowerShell コマンドレット `Start-CitrixCallHomeUpload`)

ファイル名	カテゴリ	データグループ
		マシン
		エックスディーサイト
		サイト情報
		ブローカーDB情報 (M)
		インストールされているDBバージョン (M)
		ブローカーサービスステータス (M)
		登録済みサービスインスタンス (M)
		ブローカーライセンステスト (M)
		アクティブなHDX™セッション (M)
		ブローカー管理者
		ブローカー管理者権限

		RDS構成 (LicensingSettings、SessionSettings、SpecifiedLicenseServers、およびRegisteredLicenseServersを含む)
		監視サービス (M) (MonitorConfiguration、MonitorDataStore、MonitorDBConnection、MonitorDBSchemaVersion、MonitorService、MonitorServiceAddedCapability、MonitorServiceInstance、MonitorServiceStatus、およびMonitorInstalledDBVersionを含む)
		構成ログ
		接続ログ
		ハイパーバイザー接続 (M)
		ブローカーハイパーバイザー接続
		ハイパーバイザーアラート
		カタログ
		マルチセッションOSエージェント (M)
		シングルセッションOSエージェント (M)
		公開アプリケーション
		デリバリー グループ

		構成済みデリバリーエージェント

		Citrixインストール済みコンポーネント
		Citrix Brokerサービス情報
		ブローカーサービス構成ファイル
		Machine Creation Services™ 構成ファイル
		ホストサービス構成ファイル
		AD IDサービス構成ファイル
		構成サービス構成ファイル
		構成ログサービス構成ファイル
		委任管理サービス構成ファイル
		環境テストサービス構成ファイル
		監視サービス構成ファイル
		Storefront™ サービス構成ファイル
		ワークステーションエージェント構成ファイル
		Citrix VDA情報
		Citrix XD ホットフィックス
		Citrix_VirtualChannel_Graphics_Enum

		Citrix_VirtualChannel_Flash_Enum
		Citrix_VirtualChannel_Printer_Enum

		コンピューター
		BIOS
		メモリ情報
		プロセッサ
		PNP デバイス
		デバイス
		ディスクドライブ
		論理ドライブ
		ページファイル使用状況
		ネットワークアダプター
		ネットワークアダプター構成
		ipConfig
		ビデオコントローラー
		IDE コントローラー
		SCSI コントローラー

		HKLM:\Software\Wow6432Node\Citrix

		HKLM: \System\CurrentControlSet\Control\Citrix
		HKLM: \SOFTWARE\Policies\Citrix
		HKLM: \Software\Microsoft\Cryptography
		HKLM: \Software\Wow6432Node\Microsoft\Cryptography
		HKLM: \Software\Microsoft\Windows NT\CurrentVersion\Windows
		HKLM: \Software\Microsoft\Windows NT\CurrentVersion\Winlogon
		HKLM: \Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
		HKLM: \Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer
		HKLM: \SYSTEM\CurrentControlSet\Control\Print\Environments
		HKLM: \System\CurrentControlSet\Control\Session Manager

		HKLM:\System\CurrentControlSet\Control\Terminal Server
		HKCU:\Control Panel\Desktop
		HKLM:\SOFTWARE\Classes\ShockwaveFlash.ShockwaveFlash\CurVer
		HKLM:\SYSTEM\CurrentControlSet\Control\SystemInformation
		HKLM:\SYSTEM\CurrentControlSet\Control\FileSystem
		HKLM:\SYSTEM\CurrentControlSet\Control\Windows
		HKLM:\SYSTEM\CurrentControlSet\Control\TimeZoneInformation

		ドライバー
		EnvVariables
		OS
		プロセス
		サービス
		サービスパック
		ジーピーリザルト
		Microsoft ホットフィックス

		ネットスタット
		PNP ドライバー

		システムイベントログ
		AOT (常時オンのトレース)
		クラッシュダンプ

		アップタイム
		メモリ
		コンピューターシステム
		プロセッサ
		ビデオコントローラー
		ディスクドライブ
		ブラウザ情報
		再起動回数
		メモリ使用量
		ディスク使用量
		ICAセッション解像度
		ICAカラー深度
		メタインストーラーCEIPマシンID

		ストア数
		サーバーグループ内のサーバー数

		ストアあたりのDelivery Controller™数
		HTTPS有効
		Citrix Receiver™のクラシックエクスペリエンスが有効
		Citrix レシーバー 用の HTML5 レシーバー設定
		Citrix Receiver向けワークスペースコントロールの有効化
		ストア向けリモートアクセスの有効化
		ゲートウェイ数
		統合されたNetScaler®認証用の明示的なJSONサービス

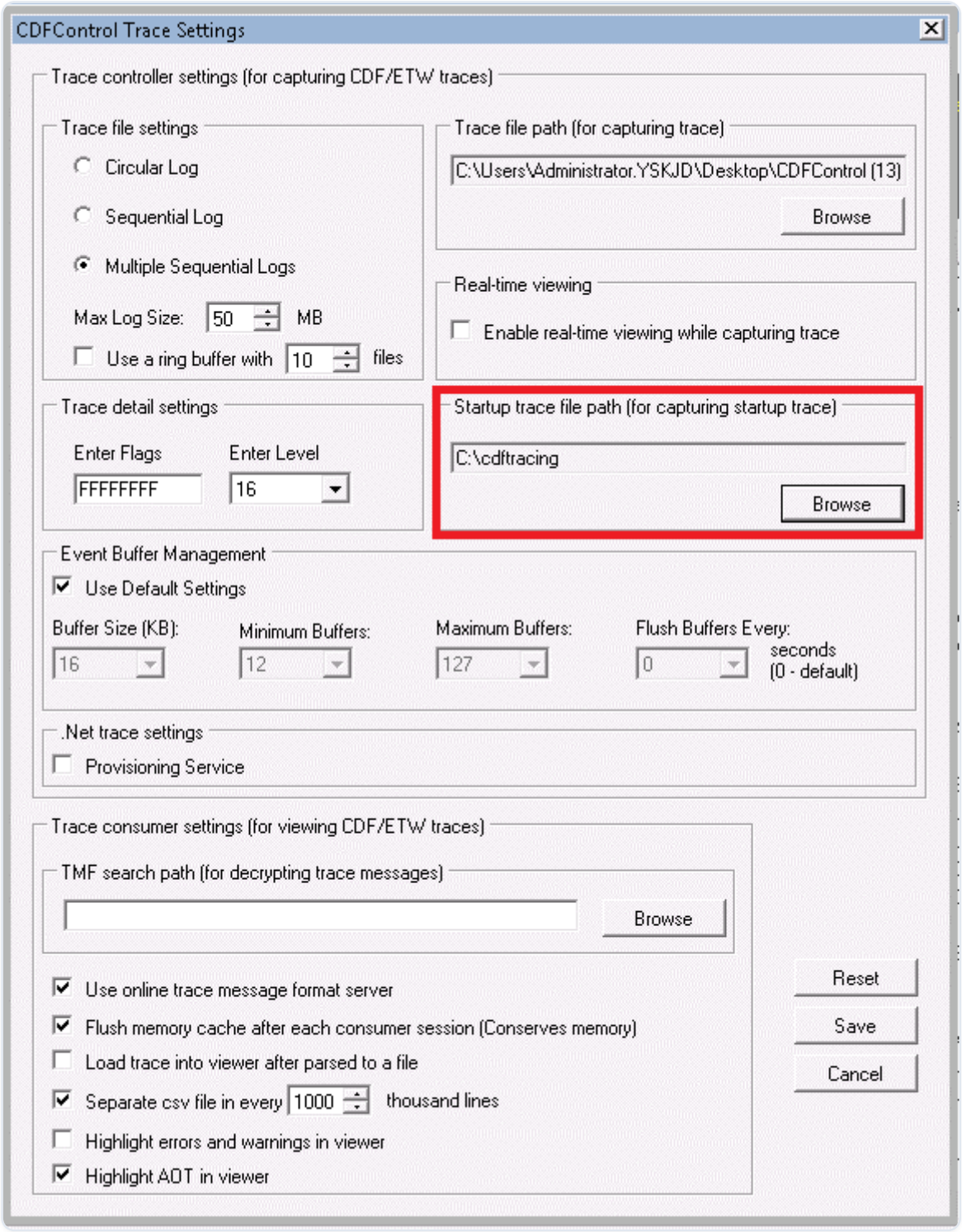
システム起動時にCitrix Diagnostic Facility (CDF) トレースを収集する

CDFControlユーティリティは、さまざまなCitrixトレースプロバイダーから表示されるCitrix Diagnostic Facility (CDF) トレースメッセージをキャプチャするためのイベントトレースコントローラーまたはコンシューマーです。これは、複雑なCitrix関連の問題のトラブルシューティング、フィルターサポートの解析、およびパフォーマンスデータの収集を目的としています。CDFControlユーティリティをダウンロードするには、CTX111961を参照してください。

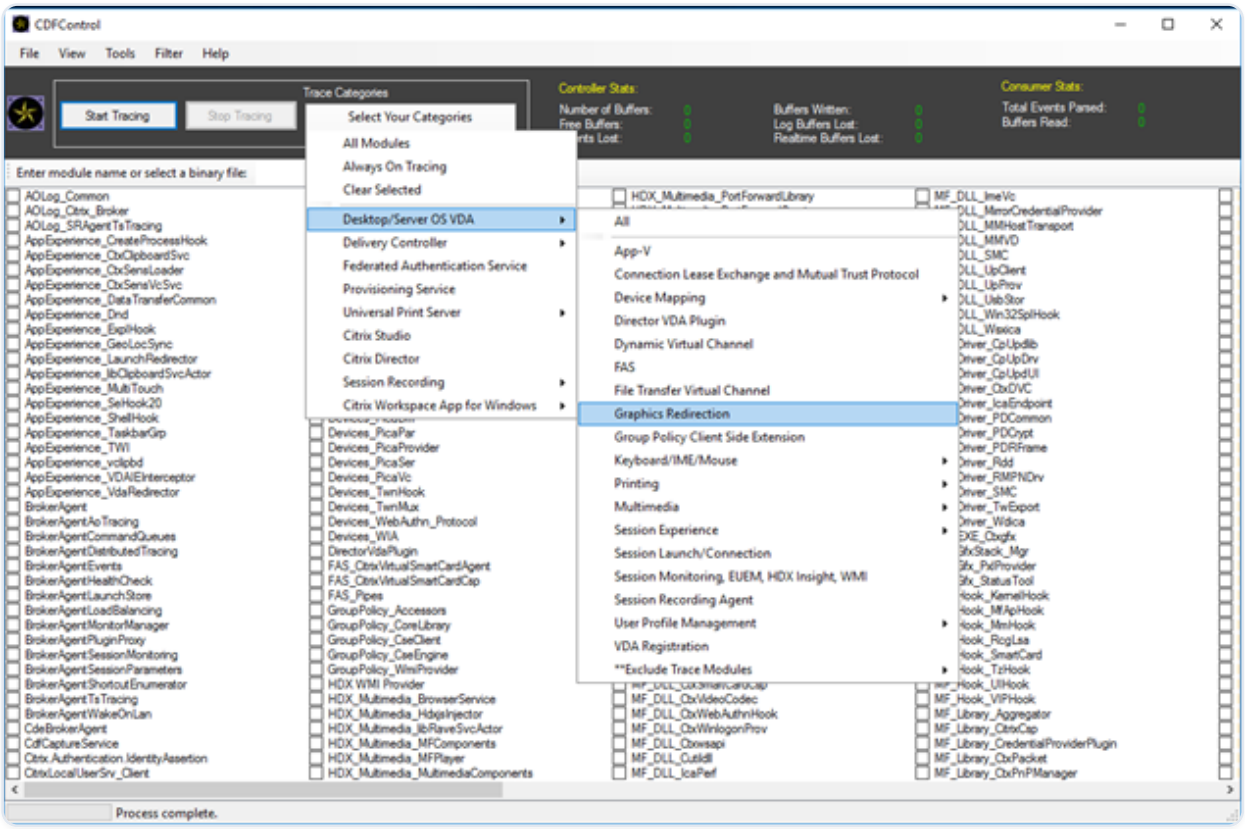
システム起動時にトレースを収集する

システム起動時にCDFトレースを収集するには、次の手順を使用します。管理者権限が必要です。

1. **CDFControl**を起動し、**ツール**メニューから**オプション**を選択します。
2. **起動トレースをキャプチャするための起動トレースファイルパス**セクションで、トレースファイルのパスを指定します。次に、**保存**をクリックします。



3. Citrixサポートが推奨する**トレースカテゴリ**を選択します。（以下の例では、**グラフィックリダイレクト**が選択されています。この選択は単なる例です。トラブルシューティングしている特定の問題に対してプロバイダーを有効にすることをお勧めします。）



4. **起動トレース**を選択し、**ツール**メニューから**有効にする**を選択します。

   有効にするを選択すると、アニメーションバーがスクロールを開始します。このアクティビティは手順に影響しません。次のステップに進みます。

5. **起動トレース**が有効になったら、**CDFControlユーティリティ**を閉じ、システムを再起動します。

6. **CDFControl**ユーティリティを起動します。システムが再起動し、エラーが表示されたら、**ツール**メニューから**起動トレース**を選択し、**無効にする**をクリックして起動トレースを無効にします。

7. 手順2で指定したトレースファイルパスに移動し、分析のためにトレースログファイル（.etl）を収集します。

委任管理

> **注:**

> バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

委任管理モデルは、ロールベースおよびオブジェクトベースの制御を使用して、組織が管理アクティビティを委任する方法に合わせる柔軟性を提供します。委任管理は、あらゆる規模の展開に対応し、展開の複雑さが増すにつれて、より詳細な権限の粒度を構成できるようにします。委任管理では、管理者、ロール、スコープという3つの概念を使用します。

- **管理者:** 管理者は、Active Directoryアカウントによって識別される個人またはグループを表します。各管理者は、1つ以上のロールとスコープのペアに関連付けられています。
- **ロール:** ロールは職務を表し、それに関連付けられた定義済みの権限を持ちます。たとえば、Delivery Group Administratorロールには、「Delivery Groupの作成」や「Delivery Groupからのデスクトップの削除」などの権限があります。管理者はサイトに対して複数のロールを持つことができるため、ある人物がDelivery Group AdministratorとMachine Catalog Administratorの両方になることができます。ロールは組み込みまたはカスタムにすることができます。

  組み込みロールは次のとおりです。

ロール	権限
フル管理者	すべてのタスクと操作を実行できます。フル管理者 (Full Administrator) は常に「すべて」のスコープと組み合わされます。
読み取り専用管理者	グローバル情報に加えて、指定されたスコープ内のすべてのオブジェクトを表示できますが、何も変更することはできません。たとえば、Scope=Londonの読み取り専用管理者 (Read Only Administrator) は、すべてのグローバルオブジェクト（構成ログなど）と、ロンドンにスコープが設定されたオブジェクト（ロンドンデリバリーグループなど）を表示できます。ただし、その管理者はニューヨークのスコープ内のオブジェクトを表示できません（ロンドンとニューヨークのスコープが重複しないと仮定した場合）。
ヘルプデスク管理者	デリバリーグループを表示し、それらのグループに関連付けられたセッションとマシンを管理できます。監視対象のデリバリーグループの「マシンカタログ」とホスト情報を表示できます。また、それらのデリバリーグ

ロール	権限
	ループ内のマシンのセッション管理およびマシン電源管理操作を実行できます。
マシンカタログ管理者	マシンカタログを作成および管理し、それらにマシンをプロビジョニングできます。仮想化インフラストラクチャ、Provisioning Services、および物理マシンからマシンカタログを構築できます。このロールはベースイメージを管理し、ソフトウェアをインストールできますが、アプリケーションやデスクトップをユーザーに割り当てることはできません。
デリバリーグループ管理者	アプリケーション、デスクトップ、およびマシンを配信できます。また、関連するセッションを管理できます。ポリシーや電源管理設定などのアプリケーションおよびデスクトップ構成も管理できます。
ホスト管理者	ホスト接続とその関連リソース設定を管理できます。ユーザーにマシン、アプリケーション、またはデスクトップを配信することはできません。
コスト管理者	Azure MCSカタログのコスト詳細を監視および表示できます。具体的には、過去30日間に発生した総コストと、現在および以前の30日間期間の比較を表示できます。

特定の製品エディションでは、組織の要件に合わせてカスタムロールを作成し、より詳細な権限を委任できます。カスタムロールを使用して、コンソール内のアクションまたはタスクの粒度で権限を割り当てることができます。

- **スコープ:** スコープはオブジェクトのコレクションを表します。スコープは、組織に関連する方法でオブジェクトをグループ化するために使用されます (たとえば、営業チームが使用するデリバリーグループのセット)。オブジェクトは複数のスコープに属することができます。オブジェクトが1つ以上のスコープでラベル付けされていると考えることができます。組み込みスコープが1つあります。「すべて」で、すべてのオブジェクトが含まれます。フル管理者ロールは常に**すべて**スコープとペアになります。

例

XYZ社は、部門（経理、営業、倉庫）とデスクトップオペレーティングシステム（Windows 7またはWindows 8）に基づいてアプリケーションとデスクトップを管理することにしました。管理者は5つのスコープを作成し、各デリバリーグループに2つのスコープをラベル付けしました。1つは使用される部門用、もう1つは使用されるオペレーティングシステム用です。

次の管理者が作成されました。

管理者	ロール	スコープ
domain/fred	フル管理者	すべて (フル管理者ロールは常に「すべて」スコープを持ちます)
domain/rob	読み取り専用管理者	すべて
domain/heidi	読み取り専用管理者、ヘルプデスク管理者	すべての営業
domain/warehouseadmin	ヘルプデスク管理者	倉庫
domain/peter	デリバリーグループ管理者、マシンカタログ管理者	Win7

- Fredはフル管理者であり、システム内のすべてのオブジェクトを表示、編集、削除できます。
- Robはサイト内のすべてのオブジェクトを表示できますが、それらを編集または削除することはできません。
- Heidiはすべてのオブジェクトを表示でき、Salesスコープ内のデリバリーグループに対してヘルプデスクタスクを実行できます。これにより、彼女はそれらのグループに関連付けられたセッションとマシンを管理できます。ただし、マシンの追加や削除など、デリバリーグループに変更を加えることはできません。
- warehouseadmin Active Directoryセキュリティグループのメンバーである人は誰でも、Warehouseスコープ内のマシンを表示し、ヘルプデスクタスクを実行できます。
- PeterはWindows 7のスペシャリストであり、すべてのWindows 7マシンカタログを管理でき、どの部署スコープに属していても、Windows 7アプリケーション、デスクトップ、およびマシンを提供できます。管理者は、PeterをWin7スコープのフル管理者にすることを検討しました。しかし、フル管理者は「サイト」や「管理者」など、スコープが設定されていないすべてのオブジェクトに対しても完全な権限を持つため、彼女はこれに反対しました。

委任管理の使用方法

一般的に、管理者の数と権限の粒度は、展開の規模と複雑さによって異なります。

- 小規模な展開や概念実証の展開では、1人または数人の管理者がすべての作業を行います。委任はありません。この場合、各管理者を、すべてのスコープを持つ組み込みのフル管理者ロールで作成します。
- マシン、アプリケーション、デスクトップが多い大規模な展開では、より多くの委任が必要です。複数の管理者が、より具体的な機能的責任（ロール）を持つ場合があります。たとえば、2人がフル管理者で、他の管理者がヘルプデスク管理者である場合があります。また、管理者がマシンカタログなど、特定のオブジェクトグループ（スコープ）のみを管理する場合もあります。この場合、新しいスコープを作成し、組み込みロールのいずれかと適切なスコープを持つ管理者を作成します。
- さらに大規模な展開では、より多くの（またはより具体的な）スコープと、型にはまらないロールを持つ異なる管理者が必要になる場合があります。この場合、より多くのスコープを編集または作成し、カスタムロールを作成し、既存および新規のスコープに加えて、組み込みまたはカスタムロールを持つ各管理者を作成します。

柔軟性と構成の容易さのために、管理者を作成するときにスコープを作成できます。マシンカタログまたは接続を作成または編集するときにスコープを指定することもできます。

管理者の作成と管理

ローカル管理者としてサイトを作成すると、ユーザーアカウントは自動的に、すべてのオブジェクトに対する完全な権限を持つフル管理者になります。サイトが作成された後、ローカル管理者には特別な権限はありません。

フル管理者ロールには常にすべてのスコープが割り当てられます。これは変更できません。

既定では、管理者は有効になっています。管理者を今作成しても、その人が後で管理業務を開始しない場合は、管理者を無効にする必要があるかもしれません。既存の有効な管理者については、オブジェクト/スコープを再編成している間に複数人を無効にし、更新された構成で稼働準備が整ったときに再度有効にしたい場合があります。有効なフル管理者がいなくなる場合、フル管理者を無効にすることはできません。管理者の作成、コピー、または編集時に、有効/無効チェックボックスが利用可能です。

管理者をコピー、編集、または削除する際にロール/スコープのペアを削除すると、その管理者に対するロールとスコープ間の関連付けのみが削除されます。ロールまたはスコープ自体は削除されません。また、そのロール/スコープのペアで構成されている他の管理者には影響しません。

管理者を作成および管理するには、次の手順に従います。

1. Web Studioにサインインし、左側のペインで**管理者**をクリックし、次に**管理者**タブをクリックします。
2. 実行するタスクの手順に従います。

    - **管理者を作成する:** アクションバーで**管理者を作成**をクリックします。ユーザーアカウント名を入力または参照し、スコープを選択または作成し、ロールを選択します。新しい管理者は既定で有効になっています。これは変更できます。
    - **管理者をコピーする:** 管理者を選択し、アクションバーで**管理者をコピー**をクリックします。ユーザーアカウント名を入力または参照します。ロール/スコープのペアを選択して編集または削除したり、新しいペアを追加したりできます。新しい管理者は既定で有効になっています。これは変更できます。
    - **管理者を編集する:** 管理者を選択し、アクションバーで**管理者を編集**をクリックします。ロール/スコープのペアを編集または削除したり、新しいペアを追加したりできます。
    - **管理者を削除する:** 管理者を選択し、アクションバーで**管理者を削除**をクリックします。有効なフル管理者がいなくなる場合、フル管理者を削除することはできません。

上部のペインには、作成した管理者が表示されます。管理者を選択すると、下部のペインにその詳細が表示されます。**警告**列は、管理者に関連付けられているロールとスコープのペアに、使用できないロールまたはスコープが含まれているかどうかを示します。関連付けられているロールとスコープのペアに、使用できないロールまたはスコープが含まれている場合、次の警告メッセージが表示されます。

- 関連付けられているロールまたはスコープが使用できません

> **重要:**
>
> 警告メッセージは、関連付けられているロールとスコープのペアに、使用できないロール、スコープ、またはその両方が含まれている場合にのみ表示されます。

管理者からロールとスコープのペアを削除するには、次のいずれかの手順を実行します。

- ロールとスコープのペアを削除します。

    a. アクションバーで、**管理者編集**をクリックします。

    b. **管理者名と詳細**ウィンドウで、役割とスコープのペアを選択し、**削除**をクリックします。

    c. 終了するには**保存**をクリックします。

- 管理者を削除します。

  a. アクションバーで、**管理者削除**をクリックします。

  b. 確認ウィンドウで、**削除**をクリックします。

役割の作成と管理

管理者が役割を作成または編集する場合、自分自身が持っている権限のみを有効にできます。これにより、管理者が現在持っている権限よりも多くの権限を持つ役割を作成し、それを自分自身に割り当てたり（または既に割り当てられている役割を編集したりする）ことを防ぎます。

役割名には最大64個のUnicode文字を含めることができます。ただし、バックスラッシュ、スラッシュ、セミコロン、コロン、ポンド記号、コンマ、アスタリスク、疑問符、等号、左右の矢印、パイプ、左右の角括弧、左右の丸括弧、引用符、アポストロフィは含めることができません。説明には最大256個のUnicode文字を含めることができます。

組み込みの役割を編集または削除することはできません。カスタム役割が管理者によって使用されている場合、その役割を削除することはできません。

> **注:**
>
> 特定の製品エディションのみがカスタム役割をサポートしています。カスタム役割をサポートするエディションのみが、アクションバーに関連エントリを持っています。

役割を作成および管理するには、次の手順に従います。

1. Web Studioにサインインし、左ペインで**管理者**をクリックし、**役割**タブをクリックします。
2. 完了したいタスクの手順に従います。

   - **役割の詳細を表示:** 役割を選択します。下部のペインに、役割のオブジェクトタイプと関連する権限が一覧表示されます。下部のペインにある**管理者**タブをクリックすると、現在この役割を持つ管理者の一覧が表示されます。
   - **カスタムロールの作成:** アクションペインで**ロールの作成**をクリックします。名前と説明を入力します。オブジェクトの種類と権限を選択します。
   - **ロールのコピー:** ロールを選択し、アクションバーで**ロールのコピー**をクリックします。必要に応じて、名前、説明、オブジェクトの種類、および権限を変更します。
   - **カスタムロールの編集:** ロールを選択し、アクションバーで**ロールの編集**をクリックします。必要に応じて、名前、説明、オブジェクトの種類、および権限を変更します。

- **カスタムロールの削除:** ロールを選択し、アクションバーで**ロールの削除**をクリックします。プロンプトが表示されたら、削除を確定します。

スコープの作成と管理

サイトを作成するときに利用できるスコープは「すべて」スコープのみであり、これは削除できません。

次の手順でスコープを作成できます。管理者を作成するときにもスコープを作成できます。各管理者は、少なくとも1つのロールとスコープのペアに関連付けられている必要があります。デスクトップ、マシンカタログ、アプリケーション、またはホストを作成または編集するときに、それらを既存のスコープに追加できます。スコープに追加しない場合、それらは「すべて」スコープの一部として残ります。

サイトの作成はスコープ化できず、委任管理オブジェクト（スコープとロール）もスコープ化できません。ただし、スコープ化できないオブジェクトは「すべて」スコープに含まれます。（フル管理者は常に「すべて」スコープを持っています。）マシン、電源操作、デスクトップ、およびセッションは直接スコープ化されません。管理者は、関連付けられたマシンカタログまたはデリバリーグループを介して、これらのオブジェクトに対する権限を割り当てることができます。

スコープの作成と管理に関するルール:

- スコープ名には、最大64個のUnicode文字を含めることができます。スコープ名には、バックスラッシュ、スラッシュ、セミコロン、コロン、ポンド記号、コンマ、アスタリスク、疑問符、等号、左矢印、右矢印、パイプ、左角かっこまたは右角かっこ、左丸かっこまたは右丸かっこ、引用符、アポストロフィを含めることはできません。
- スコープの説明には、最大256個のUnicode文字を含めることができます。
- スコープをコピーまたは編集する際は、スコープからオブジェクトを削除すると、それらのオブジェクトに管理者がアクセスできなくなる可能性があることに留意してください。編集されたスコープが1つ以上のロールとペアになっている場合、スコープの更新によってどのロール/スコープのペアも使用できなくならないようにしてください。

スコープを作成および管理するには、次の手順に従います。

1. Web Studioにサインインし、左ペインで**管理者**をクリックしてから、**スコープ**タブをクリックします。
2. 完了したいタスクの手順に従います。

    - **スコープの作成:** アクションバーで**新しいスコープの作成**をクリックします。名前と説明を入力します。特定の種類のすべてのオブジェクト（例: デリバリーグループ）を含めるに

は、オブジェクトの種類を選択します。特定のオブジェクトを含めるには、種類を展開し、個々のオブジェクト（例: 営業チームが使用するデリバリーグループ）を選択します。

- **スコープをコピー:** スコープを選択し、アクションバーで**スコープのコピー**をクリックします。名前と説明を入力します。必要に応じて、オブジェクトの種類とオブジェクトを変更します。
- **スコープを編集:** スコープを選択し、アクションバーで**スコープの編集**をクリックします。必要に応じて、名前、説明、オブジェクトの種類、およびオブジェクトを変更します。
- **スコープを削除:** スコープを選択し、アクションバーで**スコープの削除**をクリックします。プロンプトが表示されたら、削除を確認します。

テナント管理をセットアップする

単一のCitrix Virtual Apps and Desktops™サイト内に管理パーティションを作成するために、テナント管理をセットアップします。各テナントには、マシンカタログやデリバリーグループなどの分離されたリソースと構成があります。特定のテナントへのアクセス権を持つ管理者は、そのテナントに関連付けられたリソースと構成のみを管理できます。使用例としては、単一サイト内に異なるビジネスサイロ（独立した部門または個別のIT管理チーム）を持つ企業が挙げられます。

大まかに言えば、テナント管理をセットアップするためのワークフローには以下が含まれます。

1. テナントを作成する
2. テナントの管理者を追加する

テナントを作成する

テナントスコープを作成してテナントを作成します。詳細な手順は次のとおりです。

1. Web Studioにサインインし、左ペインで**管理者**をクリックし、**スコープ**タブをクリックします。
2. *スコープの作成** をクリックしてテナントの作成を開始します。
3. テナントスコープの以下の詳細を入力します。

    a. スコープのわかりやすい名前を入力します。この名前はテナントの識別子としても機能します。

    b. （オプション）簡単な説明を入力します。

    c. **テナントスコープ**を選択します。

    d. 必要に応じて、テナントに関連付けられているオブジェクトを選択します。オブジェクトの作成時または管理時に、テナントスコープにオブジェクトを追加することもできます。

e. **OK**をクリックして作成を完了します。

完了後、以下を確認できます。

- 新しいテナントスコープレコードがスコープリストに表示され、**種類**列で**テナント**として識別されます。
- スコープ名は、Web Studioの右上隅にある**すべてのテナント**ドロップダウンリストに表示されます。

テナントスコープを操作する際は、以下の考慮事項に留意してください。

- テナントプロパティは、ホスティング > マシンカタログ > デリバリーグループ > アプリケーションという階層的な割り当て順序に従います。下位レベルのオブジェクトは、上位レベルのオブジェクトからテナントプロパティを継承します。たとえば、テナントスコープのデリバリーグループを選択する場合は、関連するホスティングとマシンカタログも選択するようにしてください。そうしないと、デリバリーグループはテナントのプロパティを継承できません。
- テナントスコープを作成した後、オブジェクトを変更することでテナントの割り当てを編集できます。テナントの割り当てが変更された場合でも、同じテナントまたはそれらのテナントのサブセットに割り当てる必要があるという制約が適用されます。ただし、テナントの割り当てが変更されても、下位レベルのオブジェクトは再評価されません。テナントの割り当てを変更する際は、オブジェクトが適切に制限されていることを確認してください。たとえば、マシンカタログが`TenantA`と`TenantB`で利用可能な場合、`TenantA`用と`TenantB`用のデリバリーグループを作成できます。（`TenantA`と`TenantB`は両方ともそのマシンカタログに関連付けられています。）その後、マシンカタログを`TenantA`のみに関連付けられるように変更できます。その結果、`TenantB`に関連付けられているデリバリーグループは無効になります。

テナントの管理者を追加する

管理者ロールとテナントを持つユーザーアカウントを割り当てることで、テナントの管理者を追加します。

テナントの管理者を追加するには、次の手順に従います。

1. Web Studioにサインインし、左ペインの**管理者**をクリックしてから、**管理者**タブをクリックします。
2. **管理者を追加**をクリックし、次の手順に従って完了します。

   a. ユーザーアカウント名を入力または参照して、**次へ**をクリックします。

b. 「**カスタムアクセス**」を選択し、必要に応じて1つ以上の役割（例：マシンカタログ管理者）を選択します。

c. 各役割の横にある「**スコープの編集**」をクリックし、スコープを「**すべて**」から目的のテナントスコープに変更して、「**保存**」をクリックします。

3. **Next**をクリックします。
4. 「**確認と確定**」ページで、「**招待状を送信**」をクリックします。

レポートの作成

委任管理レポートには、次の2種類を作成できます。

- 管理者に関連付けられている役割/スコープのペアと、各種類のオブジェクト（例：デリバリーグループとマシンカタログ）の個々の権限を一覧表示するHTMLレポート。このレポートはWeb Studioから生成します。

  このレポートを作成するには、次の手順に従います。

  a. Web Studioにサインインし、左ペインで「**管理者**」をクリックします。

  b. 管理者を選択し、アクションバーで「**レポートの作成**」をクリックします。

  管理者の作成、コピー、または編集時に、このレポートを要求することもできます。

- すべての組み込み役割とカスタム役割を権限にマッピングするHTMLまたはCSVレポート。このレポートは、OutputPermissionMapping.ps1という名前のPowerShellスクリプトを実行して生成します。

  このスクリプトを実行するには、フル管理者、読み取り専用管理者、または役割を読み取る権限を持つカスタム管理者である必要があります。スクリプトは、Program Files\Citrix\DelegatedAdmin\SnapIn\Citrix.DelegatedAdmin.Admin.V1\Scriptsにあります。

  構文：

  `OutputPermissionMapping.ps1 [-Help] [-Csv] [-Path string] [-AdminAddress string] [-Show] [CommonParameters]`

パラメーター	説明
`-Help`	スクリプトのヘルプを表示します。
`-Csv`	CSV出力を指定します。デフォルト = HTML

パラメーター	説明
`-Path string`	出力の書き込み先。デフォルト = stdout
`-AdminAddress string`	接続先のDelivery Controller™のIPアドレスまたはホスト名。デフォルト = localhost
`-Show`	(`-Path` パラメーターも指定されている場合にのみ有効) 出力をファイルに書き込むと、`-Show` によって出力がWebブラウザーなどの適切なプログラムで開かれます。
共通パラメーター	`Verbose`、`Debug`、`ErrorAction`、`ErrorVariable`、`WarningAction`、`WarningVariable`、`OutBuffer`、および `OutVariable`。詳細については、Microsoftのドキュメントを参照してください。

次の例では、HTMLテーブルをRoles.htmlという名前のファイルに書き込み、そのテーブルをWebブラウザーで開きます。

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"

-Path Roles.html –Show
```

次の例では、CSVテーブルをRoles.csvという名前のファイルに書き込みます。テーブルは表示されません。

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"

–CSV -Path Roles.csv
```

Windowsのコマンドプロンプトから、上記の例のコマンドは次のとおりです。

```
powershell -command "& '%ProgramFiles%\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1'

-CSV -Path Roles.csv"
```

デリバリーコントローラー

注:

バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

Delivery Controllerは、ユーザーアクセスの管理、接続の仲介と最適化を担当するサーバー側コンポーネントです。コントローラーは、デスクトップおよびサーバーイメージを作成するMachine Creation Services™も提供します。

サイトには少なくとも1つのコントローラーが必要です。最初のコントローラーをインストールした後、サイトの作成時または後でコントローラーを追加できます。サイトに複数のコントローラーを配置することには、主に2つの利点があります。

- **冗長性:** ベストプラクティスとして、本番サイトでは、常に異なる物理サーバー上に少なくとも2つのコントローラーを配置してください。1つのコントローラーが故障した場合でも、他のコントローラーが接続を管理し、サイトを管理できます。
- **スケーラビリティ:** サイトのアクティビティが増加すると、コントローラーのCPU使用率とデータベースのアクティビティも増加します。追加のコントローラーにより、より多くのユーザー、アプリケーション、およびデスクトップ要求を処理できるようになり、全体的な応答性を向上させることができます。

各コントローラーはサイトデータベースと直接通信します。複数のゾーンがあるサイトでは、各ゾーンのコントローラーは、プライマリゾーンのサイトデータベースと通信します。

重要:

> サイトの構成後、コントローラーのコンピューター名またはドメインメンバーシップを変更しないでください。

VDAがコントローラーに登録する方法

VDAを使用する前に、サイト内のDelivery Controllerに登録（通信を確立）する必要があります。VDA登録の詳細については、「VDA registration with Controllers」を参照してください。

コントローラーの追加、削除、または移動

コントローラーを追加、削除、または移動するには、「Databases」の記事に記載されているサーバーロールとデータベースロールの権限が必要です。

SQLクラスタリングまたはSQLミラーリングインストール内のノードにコントローラーをインストールすることはサポートされていません。

サイトにDelivery Controller™を追加するときは、高可用性のために使用するすべてのレプリカSQL Serverに、そのマシンのログオン資格情報を追加してください。

展開でデータベースミラーリングを使用している場合:

- コントローラーを追加、削除、または移動する前に、プリンシパルデータベースとミラーデータベースの両方が実行されていることを確認してください。さらに、SQL Server Management Studioでスクリプトを使用している場合は、スクリプトを実行する前にSQLCMDモードを有効にしてください。
- コントローラーを追加、削除、または移動した後にミラーリングを確認するには、PowerShell `Get-configdbconnection` コマンドレットを実行します。このコマンドレットは、ミラーへの接続文字列にフェールオーバーパートナーが設定されていることを確認します。

Controller を追加、削除、または移動した後:

- 自動更新が有効になっている場合、VDA は 90 分以内に更新された Controller のリストを受け取ります。
- 自動更新が有効になっていない場合は、すべての VDA で Controller ポリシー設定または ListOfDDCs レジストリキーが更新されていることを確認してください。Controller を別のサイトに移動した後、両方のサイトでポリシー設定またはレジストリキーを更新してください。

Controller を追加する

サイトの作成時および後から Controller を追加できます。このソフトウェアの以前のバージョンでインストールされた Controller を、このバージョンで作成されたサイトに追加することはできません。

1. サポートされているオペレーティングシステムを含むサーバーでインストーラーを実行します。Delivery Controller コンポーネントと、必要なその他のコアコンポーネントをインストールします。インストールウィザードを完了します。
2. まだサイトを作成していない場合は、この Controller で Citrix Site Manager を実行してサイトを作成します。この Controller の IP アドレスは、新しいサイトに自動的に追加されます。

   データベースを初期化するスクリプトを生成する予定がある場合は、スクリプトを生成する前に Controller を追加してください。
3. すでにサイトを作成している場合は、次の手順に従います。

   a. この Controller で Citrix Site Manager を実行し、 をクリックして、参加するサイトの Controller のアドレスを入力します。

   b. Web Studio に Controller を追加するには、Studio 構成ツール を実行します。

Controller を削除する

サイトから Controller を削除しても、Citrix ソフトウェアやその他のコンポーネントがアンインストールされるわけではありません。この操作は、Controller をデータベースから削除し、接続の仲介やその他のタスクに使用できなくするものです。Controller を削除しても、後で同じサイトまたは別のサイトに再度追加できます。サイトには少なくとも 1 つの Controller が必要であるため、Web Studio に表示されている最後の Controller を削除することはできません。

サイトから Controller を削除しても、データベースサーバーへの Controller のログオンは削除されません。これにより、同じマシン上の他の製品のサービスで使用されているログオンが誤って削除されるのを防ぎます。ログオンが不要になった場合は、手動で削除する必要があります。ログオンを削除するには、`securityadmin` サーバーロールの権限が必要です。

Controller を削除した後:

- 自動更新を使用しているVDAは、他の利用可能なコントローラーに再登録します。この再登録は、自動更新メカニズムが有効になっており、VDAが他のコントローラー（削除されたコントローラーと同じセカンダリゾーン内、またはオンプレミス展開のプライマリゾーン内）に到達できる場合にのみ発生します。
- Citrix StoreFrontでコントローラー情報を更新します。詳細については、「コントローラーの管理」を参照してください。

- Citrix StoreFrontで、Citrix Gatewayを介したリモートアクセス用のSecure Ticket Authority (STA) URLを更新します。詳細については、「Secure Ticket Authority の管理」を参照してください。
- Citrix Gatewayで、仮想サーバーのSTA URLを更新します。詳細については、「Citrix Gateway」を参照してください。

重要:

サイトからコントローラーを削除するまでは、Active Directoryからコントローラーを削除しないでください。

1. Web Studioが、削除するコントローラーをロードして表示できるように、コントローラーの電源がオンになっていることを確認してください。
2. Web Studioがコントローラーを完全にロードしたら、コントローラー上のすべてのサービスが実行されており、コントローラーの電源がオンのままであることを確認します。
3. Web Studioにサインインし、左ペインで を選択します。
4. タイルを見つけて、 をクリックします。
5. ページで、削除するコントローラーを選択します。
6. を選択します。適切なデータベースロールと権限がない場合は、データベース管理者がコントローラーを削除できるようにするスクリプトを生成するオプションが提示されます。

   Web Studioは、コントローラーを削除する前に事前チェックを実行します。コントローラーの電源がオフで、以下のサービスステータスではない場合、安全に削除できます。

   - 不明
   - 失敗保留中
   - 古いバージョン
   - 新しいバージョン
   - バージョン変更が進行中
   - 必須機能が不足しています

   Controller の電源がオフになっておらず、上記のいずれかのサービスステータスである場合、Web Studio は Controller の電源をオフにするよう求めます。
7. データベースサーバーから Controller のマシンアカウントを削除する必要があります。削除する前に、別サービスがそのアカウントを使用していないことを確認してください。

Web Studio を使用して Controller を削除した後、現在のタスクが適切に完了するように、その Controller へのトラフィックがしばらく残る場合があります。短時間で Controller の削除を強制したい場合は、Citrix は、インストールされていたサーバーをシャットダウンするか、そのサーバーを Active Directory から削除することを推奨します。その後、サイト上の他の Controller を再起動して、削除された Controller とのそれ以上の通信がないことを確認してください。

Controller を別のゾーンに移動する

サイトに複数のゾーンが含まれている場合、Controller を別のゾーンに移動できます。この移動が VDA 登録やその他の操作にどのように影響するかについては、「ゾーン」を参照してください。

1. 左ペインで を選択します。
2. 中央ペインでゾーンを選択し、Controller を選択します。
3. アクションバーで を選択します。
4. 表示される ページで、Controller を移動するゾーンを選択します。
5. 「**保存**」をクリックします。

VDA を別のサイトに移動する

Citrix Provisioning™ を使用してプロビジョニングされた VDA、または既存のイメージである VDA は、アップグレード時や、テストサイトで作成された VDA イメージを本番サイトに移動する際に、別のサイト（サイト 1 からサイト 2 へ）に移動できます。Machine Creation Services (MCS) を使用してプロビジョニングされた VDA は、あるサイトから別のサイトに移動できません。MCS は、VDA が Controller に登録するためにチェックする ListOfDDCs の変更をサポートしていません。MCS を使用してプロビジョニングされた VDA は、常に作成されたサイトに関連付けられた ListOfDDCs をチェックします。

VDA を別のサイトに移動する方法は、インストーラーを使用する方法と Citrix ポリシーを使用する方法の 2 つがあります。

インストーラー

インストーラーを実行し、サイト2のControllerのFQDN（DNSエントリ）を指定してControllerを追加します。

インストーラーでControllerを指定するのは、Controllerポリシー設定が使用されていない場合のみです。

グループポリシーエディター

次の例では、複数のVDAをサイト間で移動します。

1. サイト1で以下の設定を含むポリシーを作成し、そのポリシーをデリバリーグループレベルにフィルターして、サイト間の段階的なVDA移行を開始します。
   - Controller: サイト2の1つ以上のControllerのFQDN（DNSエントリ）を含みます。
   - Controllerの自動更新を有効にする: 無効に設定します。
2. デリバリーグループ内の各VDAは、新しいポリシーが適用されてから90分以内に通知を受け取ります。VDAは受信したControllerのリストを無視し（自動更新が無効になっているため）、ポリシーで指定されたControllerの1つを選択します。このポリシーにはサイト2のControllerがリストされています。
3. VDAがサイト2のControllerに正常に登録されると、サイト2のListOfDDCsとポリシー情報を受け取ります。これらはデフォルトで自動更新が有効になっています。VDAがサイト1で登録されていたControllerは、サイト2のControllerから送信されたリストには含まれていません。そのため、VDAはサイト2のリストにあるControllerの中から選択して再登録します。それ以降、VDAはサイト2からの情報で自動的に更新されます。

グループポリシーエディターの使用方法については、Citrixポリシーのドキュメントを参照してください。

Web Studioのホームページ

Web Studioのホームページには、Citrix Virtual Apps and Desktops™展開とワークロードの概要、およびサブスクリプションを最大限に活用するのに役立つ情報が表示されます。この記事では、このページで利用できるウィジェットを紹介します。

- サイトの詳細
- リソース
- セッション
- 最近
- エラーと警告
- 開始

ニーズに合わせてウィジェットを追加、削除、または再配置することで、このホームページをカスタマイズできます。

サイトの詳細

このウィジェットは、Citrix Virtual Apps and Desktopsサイトの概要を一目で確認できます。ライセンスの種類、Studioのバージョン、Delivery Controllerのバージョンとステータスなどの主要な情報が表示されます。

サイトの問題を診断するには、**サイトのテスト**を選択して、データベースの健全性、接続性、委任管理、VDA 更新の準備状況、登録状態などのチェックを実行します。このアクションは、アップグレード中に特に役立ち、展開の前後でサイトが安定して準備ができていることを確認するのに役立ちます。

リソース

このウィジェットは、Citrix Virtual Apps and Desktops展開の概要を提供します。

- **リソース**。展開されたリソースの数と、カテゴリごとのカウントを表示します。

リソース	カテゴリ別にカウントを表示するには
マシン	**マシン**をクリックし、状態を選択してから、ドーナツグラフにカーソルを合わせると詳細が表示されます。利用可能なオプション: **可用性状態** (利用可能、使用中、オフ、利用不可)、**登録状態** (登録済み、未登録)、**メンテナンス状態** (メンテナンス中、メンテナンス中でない)。可用性状態別にマシンのカウントを表示している場合、状態をクリックすると対応するマシンの詳細を表示できます。
アプリケーション	**アプリケーション**をクリックし、ドーナツグラフにカーソルを合わせると詳細が表示されます。
デリバリー グループ	**デリバリーグループ**をクリックし、ドーナツグラフにカーソルを合わせると詳細が表示されます。
マシンカタログ	**マシンカタログ**をクリックし、ドーナツグラフにカーソルを合わせると詳細が表示されます。

- **過去7日間に起動されたセッション**。過去7日間の各日に起動されたデスクトップおよびアプリセッションの数を表示します。詳細を確認するには、Directorに移動をクリックします。

セッション

このウィジェットは、過去7日間のCitrix Virtual Apps and Desktopsワークロードの概要を提供します。過去7日間に毎日起動されたデスクトップおよびアプリセッションの数を表示します。

最近

このウィジェットには、Web Studioで最近アクセスしたオブジェクトの履歴が表示されます。オブジェクトのアクセス履歴をすばやく確認するのに役立ちます。リスト内のオブジェクト名をクリックすると、そのオブジェクトがそれぞれのノード内で直接開きます。

以下に留意してください。

- リストはブラウザのキャッシュにローカルに保存されます。キャッシュをクリアしたり、ブラウザを切り替えたり、シークレットモードを使用したりすると、リストはリセットされます。
- リストは、過去30日間にアクセスした最新の100個のオブジェクトに限定されます。
- このリストには、個々のオブジェクトの表示または操作のみが記録されます。一度に*複数*のオブジェクトを選択しても、リストには記録*されません*。
- 以下のオブジェクトは追跡*されません*。
    - **設定**、**ライセンス**、**ログ**ノード内のオブジェクト。
    - **ポリシー**ノードの**比較**タブと**モデリング**タブ内のオブジェクト。
    - **バックアップと復元**ノードの**履歴**タブと**設定**タブ内のオブジェクト。

はじめに

このウィジェットは、Citrix Virtual Apps and Desktopsの展開をセットアップするのに役立つ一連の質問に答えることで、展開を迅速に構成できます。

エラーと警告

展開からのエラーと警告を一元的に表示します。

- 以下の構成ノードに存在するエラー数と警告数を一覧表示します: ゾーン、マシン、マシンカタログ、デリバリーグループ、ホスティング、およびイメージ。数字をクリックすると、対応するノードのUIにリンクされます。
- サイト内の優先度の高いエラーを一覧表示し、推奨されるアクションも示します。

ホームページのカスタマイズ

ホームページをカスタマイズするには、次の手順に従います。

1. Web Studioにサインインします。

   ホームページが表示されます。
2. ホームページの右上隅にある**編集**アイコンをクリックします。
3. ウィジェットを再配置するには、目的の位置にドラッグします。
4. ホームページからウィジェットを削除するには、ウィジェットの右上にある**削除**アイコンをクリックします。
5. ウィジェットをホームページに戻すには、ホームページの右上隅にある**ウィジェットの追加**アイコンをクリックします。
6. 変更を保存するには、**完了**をクリックします。

IPv4/IPv6 のサポート

このリリースでは、純粋な IPv4、純粋な IPv6、および重複する IPv4 と IPv6 ネットワークを使用するデュアルスタック展開をサポートしています。

次のコンポーネントは IPv4 のみをサポートします。その他すべてのコンポーネントは IPv4 と IPv6 をサポートします。

- XenServer®
- **IPv6 Controller 登録のみを使用**ポリシー設定によって制御されていないVirtual Delivery Agent (VDA)

IPv6 通信は、VDA 接続に関連する2つの Citrix® ポリシー設定によって制御されます。

- **IPv6 の使用を強制する主要な設定:** IPv6 Controller 登録のみを使用。

  このポリシー設定は、VDA が Delivery Controller に登録するために使用するアドレス形式を制御します。

  有効にすると、VDA は次の優先順位で選択された単一の IPv6 アドレスを使用して Controller と登録および通信します: グローバル IP アドレス、ユニークローカルアドレス (ULA)、リンクローカルアドレス (他の IPv6 アドレスが利用できない場合のみ)。

  無効にすると、VDA はマシンの IPv4 アドレスを使用して Controller と登録および通信します。これがデフォルト値です。

  チームが頻繁に IPv6 ネットワークを使用する場合は、**IPv6 Controller 登録のみを使用**ポリシー設定が有効になっているイメージまたは組織単位 (OU) に基づいて、それらのユーザー向けにデスクトップとアプリケーションを公開します。

チームが頻繁に IPv4 ネットワークを使用する場合は、**IPv6 Controller 登録のみを使用**ポリシー設定が無効になっているイメージまたは OU に基づいて、それらのユーザー向けにデスクトップとアプリケーションを公開します。

- **IPv6 ネットマスクを定義する依存設定:** Controller 登録 IPv6 ネットマスク。

  マシンは複数の IPv6 アドレスを持つことができます。このポリシー設定により、管理者は、登録されている場合に、VDA をグローバル IP ではなく、優先サブネットのみに制限できます。この設定は、VDA が登録するネットワークを指定します。VDA は、指定されたネットマスクに一致する最初のアドレスにのみ登録します。

  この設定は、**IPv6 Controller 登録のみを使用**ポリシー設定が有効になっている場合にのみ有効です。デフォルト = 空の文字列

展開に関する考慮事項

環境に IPv4 と IPv6 の両方のネットワークが含まれている場合は、IPv4 のみのクライアントと IPv6 ネットワークにアクセスできるクライアント用に個別のデリバリーグループ構成を作成します。ユーザーを区別するために、命名、手動の Active Directory グループ割り当て、または SmartAccess フィルターの使用を検討してください。 接続が IPv6 ネットワークで開始され、その後 IPv4 アクセスのみを持つクライアントから再接続しようとすると、セッションの再接続が失敗する可能性があります。

注記 - DNS解決が有効になっている場合は、これらの考慮事項は適用されません。

Web Studio を使用した Citrix Virtual Apps and Desktops™ のライセンス

> **注:**
>
> - バージョン 2511 以降、Citrix Web Studio (Web ベース) は、Citrix Virtual Apps and Desktops™ の唯一の管理コンソールです。Citrix Studio (MMC ベース) はインストーラーから削除されました。この記事は Web Studio にのみ適用されます。Citrix Studio については、Citrix Virtual Apps and Desktops 7 2212 以前の同等の記事を参照してください。
> - License Activation Service (LAS) は、従来の Citrix® レガシーライセンスに代わる新しいクラウドベースのライセンスソリューションです。LAS はアクティベーション用の新しいモジュールを導入し、ライセンス管理へのシームレスで最新のアプローチを保証します。詳細については、「License Activation Service」を参照してください。

> Web Studio から、ライセンスサーバーが Web Studio と同じドメイン内にあるか、信頼されたドメイン内にある場合、ライセンスを管理および追跡できます。ライセンスタスクの詳細については、「ライセンスドキュメント」および「複数タイプのライセンス」を参照してください。

次の表に、サポートされているエディションとライセンスモデルを示します。

製品	エディション	ライセンスモデル
シトリックス バーチャル アプリ	プレミアム、アドバンスト、スタンダード	同時使用
シトリックス バーチャル デスクトップ	プレミアム、アドバンスト、スタンダード	ユーザー/デバイスおよび同時使用

詳細については、「同時使用ライセンス」および「ユーザー/デバイスライセンス」を参照してください。

サポートされている現在のリリース (CR) および長期サービスリリース (LTSR) のバージョン

Citrixは、機能やセキュリティの改善の恩恵を受けるために、常にCitrix License Serverの最新バージョンを使用することを強く推奨します。

> **注:**
>
> License Server VPXは非推奨となり、今後のメンテナンスやセキュリティ修正は提供されません。License Server VPXのバージョン11.16.6以前を使用しているお客様は、できるだけ早くWindows用License Serverの最新バージョンに移行することをお勧めします。

> Citrix製品のライフサイクル日付の詳細については、製品マトリックスを参照してください。

レガシー製品および製品バージョンについては、「レガシー製品マトリックス」を参照してください。

以下のタスクを完了するには、完全なライセンス管理者である必要があります。Web Studioでライセンス情報を表示するには、管理者は少なくとも「ライセンスの読み取り」委任管理権限を持っている必要があります。組み込みの「完全管理者」および「読み取り専用管理者」の役割には、その権限があります。

Web Studioを使用してCitrixからライセンスをダウンロードしてインストールする

1. Web Studioにサインインし、左ペインで**Licensing**を選択します。
2. アクションバーで**Allocate Licenses**を選択します。
3. ライセンスアクセスコードを入力します。このコードは、ライセンスの購入または更新後にCitrixからメールで届きます。
4. 製品を選択し、**Allocate Licenses**を選択します。その製品で利用可能なライセンスが割り当てられ、ダウンロードされます。特定のライセンスアクセスコードのすべてのライセンスを割り当ててダウンロードした後、そのライセンスアクセスコードを再利用することはできません。同じコードで他のトランザクションを行うには、My Accountにログオンしてください。

ローカルコンピューターまたはネットワークに保存されているライセンスを追加する

1. Web Studioにサインインし、左ペインで**Licensing**を選択します。
2. アクションバーで**Add Licenses**を選択します。
3. ライセンスファイルを参照し、ライセンスサーバーに追加します。

ライセンスサーバーを変更する

1. Web Studioにサインインし、左ペインで**Licensing**を選択します。
2. アクションバーで**Change License Server**を選択します。
3. ライセンスサーバーのアドレスを*name:port*の形式で入力します。ここで、nameはDNS、NetBIOS、またはIPアドレスです。ポート番号を指定しない場合、デフォルトポート（27000）が使用されます。

使用するライセンスの種類を選択する

- サイトを構成する際、ライセンスサーバーを指定した後、使用するライセンスの種類を選択するよう求められます。サーバーにライセンスがない場合、ライセンスなしで製品を30日間試用するオプションが自動的に選択されます。
- サーバーにライセンスがある場合、その詳細が表示され、そのうちの1つを選択できます。または、ライセンスファイルをサーバーに追加してから、そのファイルを選択することもできます。

製品エディションとライセンスモデルを変更する

1. Web Studioにサインインし、左側のペインで**［ライセンス］**を選択します。

2. アクションバーで**［製品エディションの編集］**を選択します。
3. 適切なオプションを更新します。

License Administration Consoleにアクセスするには、アクションバーで**［License Administration Console］**を選択します。コンソールがすぐに表示されるか、ダッシュボードがパスワードで保護されている場合は、License Administration Consoleの資格情報の入力を求められます。コンソールの使用方法の詳細については、ライセンスドキュメントを参照してください。

> **注:**
>
> Web Studioでライセンスを切り替えると、その変更がCitrix Directorに反映されるまでに最大5分かかります。たとえば、AdvancedとPremiumを切り替える場合などです。

ライセンス管理者を追加する

1. Web Studioにサインインし、左側のペインで**［ライセンス］**を選択します。
2. **［ライセンス管理者］**タブを選択します。
3. アクションバーで**［ライセンス管理者の追加］**を選択します。
4. 管理者として追加するユーザーを参照し、アクセス許可を選択します。

ライセンス管理者のアクセス許可を変更またはライセンス管理者を削除する

1. Web Studioにサインインし、左側のペインで**［ライセンス］**を選択します。
2. **［ライセンス管理者］**タブを選択し、管理者を選択します。
3. アクションバーで**ライセンス管理者編集**または**ライセンス管理者削除**のいずれかを選択します。

ライセンス管理者グループを追加する

1. Web Studioにサインインし、左ペインで**ライセンス**を選択します。
2. **ライセンス管理者**タブを選択します。
3. アクションバーで**ライセンス管理者グループの追加**を選択します。
4. ライセンス管理者として機能させたいグループを参照し、権限を選択します。Active Directoryグループを追加すると、そのグループ内のユーザーにライセンス管理者権限が付与されます。

ライセンス管理者グループの権限を変更または削除する

1. Web Studioにサインインし、左ペインで**ライセンス**を選択します。
2. **ライセンス管理者**タブを選択し、管理者グループを選択します。
3. アクションバーで**ライセンス管理者グループの編集**または**ライセンス管理者グループの削除**のいずれかを選択します。

ライセンス情報を表示する

Web Studioにサインインし、左ペインで**ライセンス**を選択します。サイトのライセンス使用状況と設定の概要が、指定されたライセンスサーバーに現在インストールされているすべてのライセンスのリストとともに表示されます。

製品タイプ、ライセンスエディション、ライセンスモデルを含むサイトのライセンス設定が、構成済みのライセンスサーバーが使用するライセンスと一致していることを確認してください。一致しない場合は、サイトのライセンス設定に合わせて既存のライセンスをダウンロードまたは割り当てる必要がある場合があります。

次のライセンス情報を取得するには、コマンド`Get-Brokersite`を実行します。

- TotalUniqueLicenseUsers
- PeakConcurrentLicenseUsers
- PeakConcurrentLicensedDevice

> **注:**
>
> Citrix DaaSで情報を取得するには、クラウドライセンスAPIを使用します。クラウドライセンスAPIの詳細については、「Citrix Cloudライセンスを管理するためのAPI」を参照してください。

ライセンス有効期限アラートを表示する

Web Studioは、Citrix License Serverからライセンスファイルの有効期限を照会します。ライセンスファイルの有効期限が近づいているか、すでに期限切れになっている場合、Web Studioは概要タブで管理者に警告します。

関連リンク

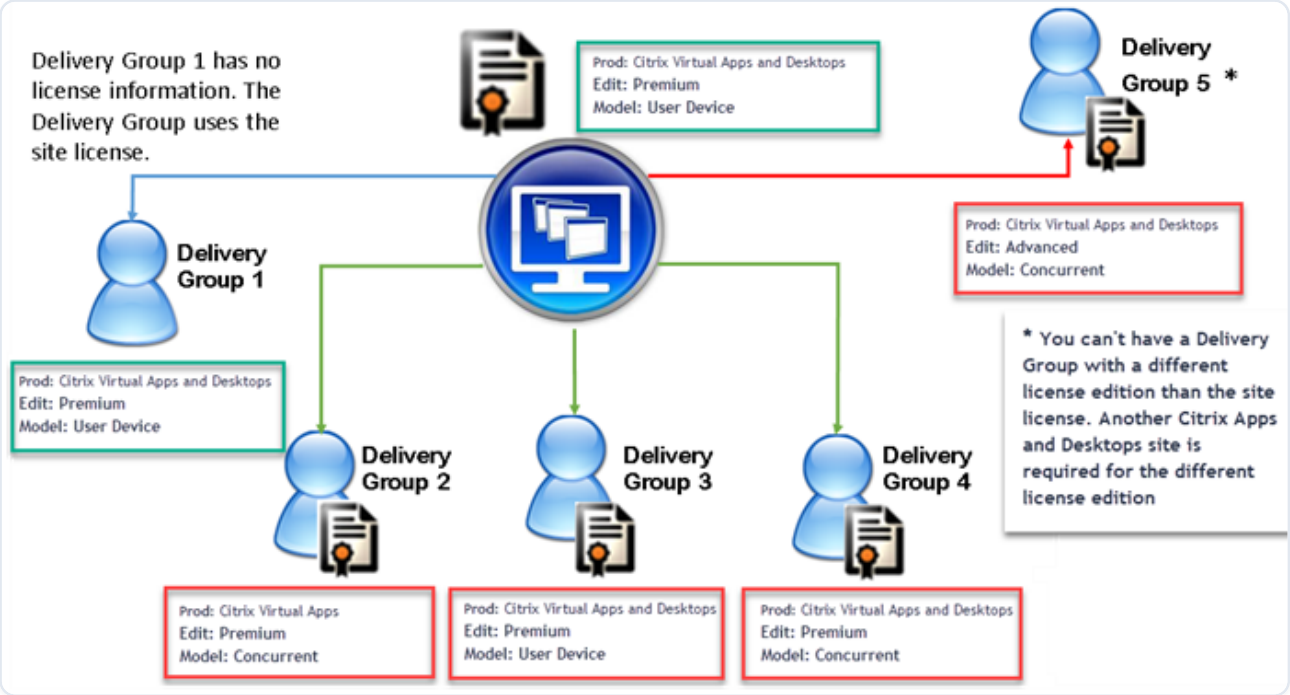
- 年間および期間ベースの小売ライセンスのCitrixオンプレミスサブスクリプションを参照してください。
- ハイブリッド権限による移行とアップグレード (TTU)を参照してください。

マルチタイプライセンス

> **注:**
>
> - ライセンスアクティベーションサービス はマルチタイプライセンスをサポートしていません。
> - デリバリーグループレベルのライセンス上書きは非推奨になりました。Citrix Virtual Apps and Desktops は、サイトレベルのライセンス設定のみを使用するようになりました。

マルチタイプライセンスは、単一の Citrix Virtual Apps and Desktops サイト上のデリバリーグループに対して、異なるライセンスタイプの消費をサポートします。**タイプ**は、製品ID（XDTまたはMPS）とモデル（UserDeviceまたはConcurrent）の単一の組み合わせです。デリバリーグループは、サイトレベルで構成されているものと同じ製品エディション（PLT/PremiumまたはENT/Advanced）を使用する必要があります。Citrix Virtual Apps and Desktops の展開でマルチタイプライセンスを構成する際は、この記事の最後にある特別な考慮事項 に注意してください。

マルチタイプライセンスが構成されていない場合、異なるライセンスタイプは、個別のサイト用に構成されている場合にのみ使用できます。デリバリーグループはサイトライセンスを使用します。マルチタイプライセンスが構成されている場合の重要な通知の制限については、特別な考慮事項 を参照してください。



異なる種類のライセンスを消費するデリバリーグループを特定するには、以下の Broker PowerShell コマンドレットを使用します。

- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup
- Get-BrokerDesktopGroup

ライセンスをインストールするには、以下を使用します。

- シトリックス スタジオ
- シトリックス ライセンシング マネージャー
- citrix.com

Customer Success Services の日付は、各ライセンスファイル、各製品、およびモデルに固有です。異なる設定のデリバリーグループは、互いに異なる Customer Success Services の日付を持つ場合があります。

特別な考慮事項

マルチタイプライセンスは、通常のCitrix Virtual Apps and Desktops™ライセンスとは異なる機能を持ちます。

サイト構成とは異なるタイプを使用するように構成されたデリバリーグループの場合、DirectorまたはStudioからのアラートや通知はありません。

- ライセンス制限に近づいている場合、またはライセンスバーストモードのトリガーや有効期限が切れた場合の情報はありません。
- 特定のグループに問題がある場合の通知はありません。

マルチタイプライセンス用に構成されたデリバリーグループは、そのライセンスタイプのみを消費し、完全に消費されてもサイト構成にフォールバックしません。

Citrix Virtual Apps StandardとCitrix Virtual Desktops™ Standardのライセンスエディション名はどちらもStandardであることを示していますが、これらは同じエディションではありません。マルチタイプライセンスは、Citrix Virtual Apps StandardおよびCitrix Virtual Desktop Standardライセンスでは利用できません。

ライセンス互換性マトリックス

この表は、古い製品名、新しい製品名、および関連する機能名を詳述しています。4つの互換性列は、どの製品とライセンスモデルの組み合わせがマルチタイプライセンスと互換性があるかを指定します。CCUとCCSは同時接続ライセンスを表し、UDはユーザー/デバイスライセンスを表します。

Old Name	New Name	Feature	Multi-type licensing compatibility			
			STD	ADV	ENT	PLT
Citrix XenApp Standard	Citrix XenApp Standard	MPS_STD_CCU	X			
Citrix XenApp Advanced	Citrix Virtual Apps Standard	MPS_ADV_CCU		X		
Citrix XenApp Enterprise	Citrix Virtual Apps Advanced	MPS_ENT_CCU			X	
Citrix XenApp Platinum	Citrix Virtual Apps Premium	MPS_PLT_CCU				X
Citrix XenDesktop VDI Edition (XDT-U)	Citrix Virtual Desktops Standard- Per User/Device	XDT_STD_UD	X			
Citrix XenDesktop VDI Edition (XDT-C)	Citrix Virtual Desktops Standard - Concurrent	XDT_STD_CCS	X			
Citrix XenDesktop Enterprise Edition (XDT-C)	Citrix Virtual Apps and Desktops Advanced - Concurrent	XDT_ENT_CCS			X	
Citrix XenDesktop Enterprise Edition (XDT-U)	Citrix Virtual Apps and Desktops Advanced - Per User/Device	XDT_ENT_UD			X	
Citrix XenDesktop Platinum Edition (XDT-C)	Citrix Virtual Apps and Desktops Premium - Concurrent	XDT_PLT_CCS				X
Citrix XenDesktop Platinum Edition (XDT-U)	Citrix Virtual Apps and Desktops Premium - Per User/Device	XDT_PLT_UD				X

ブローカー PowerShell SDK

DesktopGroup オブジェクトには、関連するNew-BrokerDesktopGroupおよびSet-BrokerDesktopGroupコマンドレットを使用して操作できる次の2つのプロパティがあります。

名前	値	制限
LicenseModel	グループのライセンスモデルを指定するパラメーター (Concurrent または UserDevice)。指定されていない場合、サイト全体のライ	機能トグルが無効になっている場合、プロパティを設定しようとすると失敗します。

名前	値	制限
	センスモデルが使用されます。	
ProductCode	XDT (Citrix Virtual Desktops用) またはMPS (Citrix Virtual Apps™用) のテキスト文字列で、グループのライセンス製品IDを指定します。指定されていない場合、サイト全体の製品コードが使用されます。	機能トグルが無効になっている場合、プロパティを設定しようとすると失敗します。

LicenseModelとProductCodeの詳細については、about_Broker_Licensingを参照してください。

New-BrokerDesktopGroup

デスクトップグループのブローカーを管理するためのデスクトップグループを作成します。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerDesktopGroup/>`を参照してください。

Set-BrokerDesktopGroup

既存のブローカーデスクトップグループを無効または有効にするか、その設定を変更します。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>`を参照してください。

Get-BrokerDesktopGroup

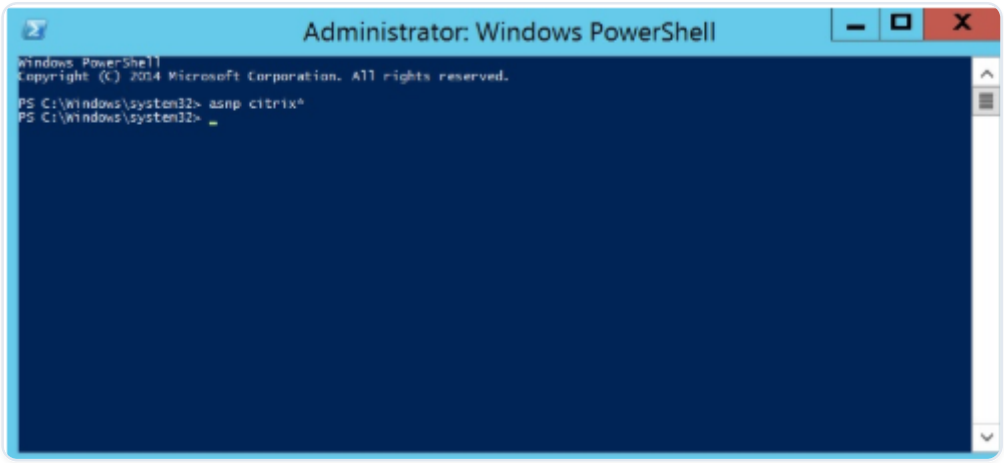
指定された条件に一致するデスクトップグループを取得します。Get-BrokerDesktopGroupコマンドレットの出力には、グループの**ProductCode**および**LicenseModel**プロパティが含まれます。New-BrokerDesktopGroupまたはSet-BrokerDesktopGroupを使用してプロパティが設定されていない場合、null値が返されます。nullの場合、サイト全体のライセンスモデルと製品コードが使用されます。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/Get-BrokerDesktopGroup/>`を参照してください。

デリバリーグループごとに異なるライセンス製品とモデルを構成する

> **注:**

> 単一のデリバリーグループで、2つ以上の異なる種類の製品、エディション、またはライセンスモデルを構成することはできません。異なる種類の製品、エディション、またはライセンスモデルがある場合は、それらを別々のデリバリーグループで構成してください。

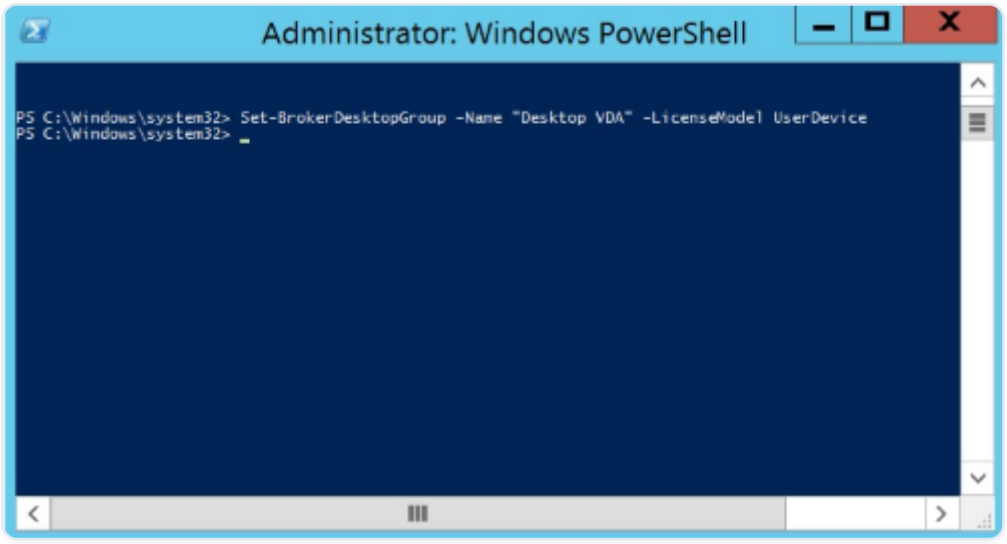
1. 管理者権限でPowerShellを開き、Citrixスナップインを追加します。



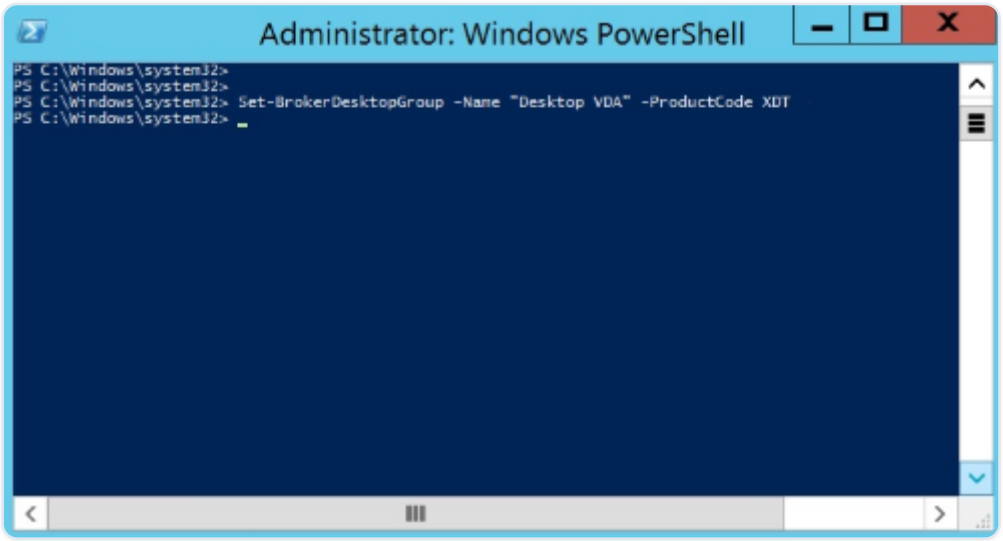
2. コマンド **Get-BrokerDesktopGroup –Name “DeliveryGroupName”** を実行して、現在のライセンス構成を表示します。パラメーター **LicenseModel** と **ProductCode** を見つけます。これらのパラメーターを以前に構成していない場合、空白になっている可能性があります。

> **注:**
>
> デリバリーグループにライセンス情報が設定されていない場合、デフォルトで**サイトレベルのサイトライセンス**になります。
>
> PowerShellコマンド(/en-us/citrix-virtual-apps-desktops/current-release/media/license-configuration-2.png)

3. コマンド **Set-BrokerDesktopGroup –Name “DeliveryGroupName” –LicenseModel LicenseModel** を実行して、ライセンスモデルを変更します。



4. コマンドを実行してライセンス製品を変更します: **Set-BrokerDesktopGroup –Name “DeliveryGroupName” –ProductCode ProductCode**。



5. 変更を検証するには、コマンド **Get-BrokerDesktopGroup –Name “DeliveryGroupName”** を入力します。

> **注:**
>
> 同じサイト内でエディションを混在させることはできません。たとえば、Premiumライセンスとライセンスなどです。異なるエディションのライセンスがある場合は、複数のサイトが必要です。

> PowerShellコマンド(/en-us/citrix-virtual-apps-desktops/current-release/media/license-configuration-5.png)

6. 前の手順で説明したのと同じ **Set-BrokerDesktopGroup** コマンドを実行し、値を **$null** に設定して、ライセンス構成を削除します。

> **注:**
>
> Studioでは、各デリバリーグループのライセンス構成は表示されません。現在の構成を表示するには、PowerShellを使用します。
>
> PowerShellコマンド(/en-us/citrix-virtual-apps-desktops/current-release/media/license-configuration-6.png)

例

このPowerShellコマンドレットの例は、既存の2つのデリバリーグループにマルチタイプライセンスを設定し、3つ目のデリバリーグループを作成して設定する方法を示しています。

デリバリーグループに関連付けられているライセンス製品とライセンスモデルを確認するには、**Get-BrokerDesktopGroup** PowerShellコマンドレットを使用します。

1. 最初のデリバリーグループをXenApp®およびConcurrentに設定しました。

   Set-BrokerDesktopGroup -Name "シトリックス バーチャル アプリケーションズ プレミアム コンカレント 用のデリバリーグループ" -ProductCode MPS -LicenseModel Concurrent

2. 2番目のデリバリーグループをXenDesktop®およびConcurrentに設定しました。

   Set-BrokerDesktopGroup -Name "シトリックス バーチャル デスクトップス プレミアム コンカレント 用のデリバリーグループ" -ProductCode XDT -LicenseModel Concurrent

3. 3番目のデリバリーグループをXenDesktopおよびUserDevice用に作成して設定します。

   New-BrokerDesktopGroup -Name "Citrix Virtual Desktops Premium UserDevice 用のデリバリーグループ" -PublishedName "MyDesktop" -DesktopKind Private -ProductCode XDT -LicenseModel UserDevice

ライセンスアクティベーションサービス

ライセンスアクティベーションサービス (LAS) は、従来のCitrix®レガシーライセンスに代わる、新しいクラウドベースのライセンスソリューションです。LASは、アクティベーション用の新しいモジュールを導入し、ライセンス管理へのシームレスで最新のアプローチを保証します。

LASはCitrixライセンスエクスペリエンスを簡素化します。ライセンスサーバーで生成、ダウンロード、またはインストールするライセンスアクセスコードやファイルは不要になりました。ライセンスサーバーをアップグレードし、Citrix Cloudに登録するだけです。互換性のある製品がライセンスサーバーを指すように設定されると、自動的にアクティベートできます。

アクティベーション後、ライセンスサーバーはライセンスアクティベーションサービスと定期的に通信し、アクティベーションを最新の状態に保ちます。LASはクラウドテクノロジーで構築されており、パフォーマンスを向上させ、ダウンタイムがないことを保証します。何らかの理由でライセンスサーバーまたはLASに到達できない場合、システムはライセンスキャッシュモードに入ります。これは、システムのライセンスが失われるのを防ぎ、停止を回避するように設計されています。詳細については、「ライセンスキャッシュモード」を参照してください。

LASの詳細については、ライセンスドキュメントの「ライセンスアクティベーションサービス」を参照してください。

ライセンスに関する FAQ については、「ライセンスに関する FAQ」を参照してください。

前提条件

- ライセンスサーバーをバージョン11.17.2ビルド53100以降にインストールまたは更新します。
- ライセンスサーバー用の信頼性の高い継続的なインターネット接続。

考慮事項

- Web Studio がアクティベーションを促す前に、すべての Delivery Controller が LAS と互換性がある必要があります。単一のサイトでは、レガシーライセンスまたは LAS のいずれかを使用できます。
- 同じCitrix Cloud ID (CCID) またはOrgIDに複数のライセンスサーバーを登録できます。ただし、サイトは1つのライセンスサーバーのみを指すように構成できます。

制限事項

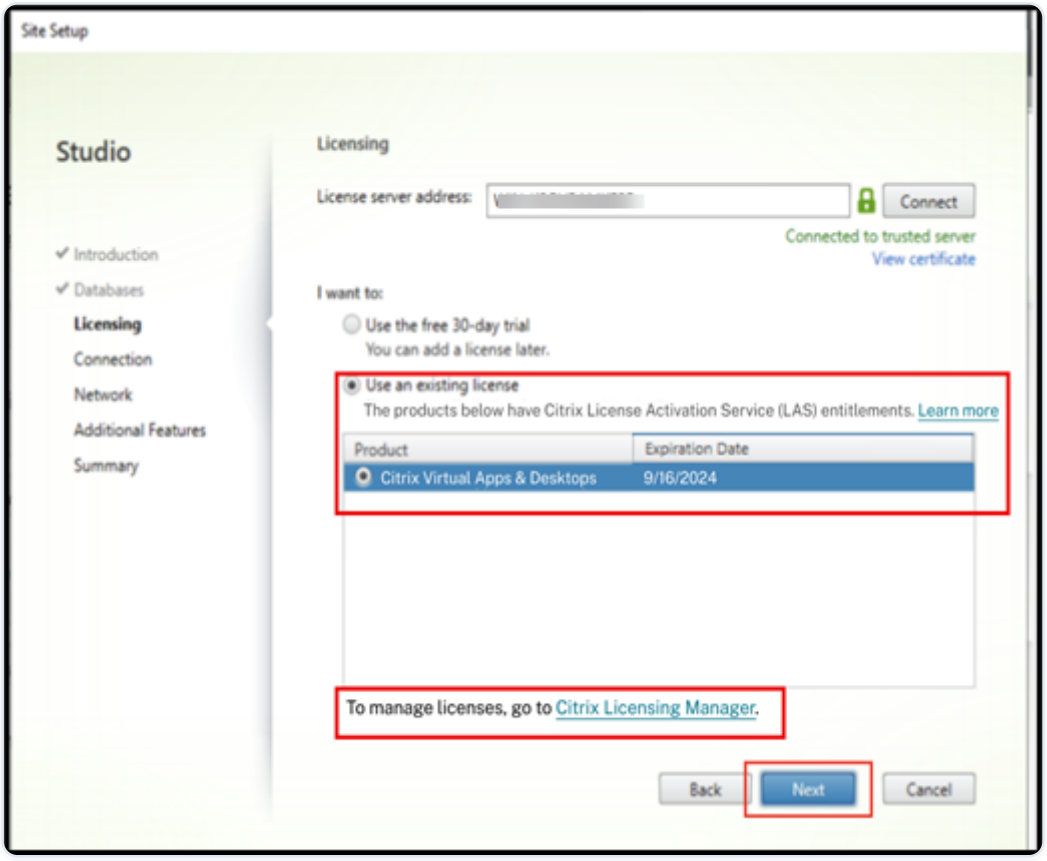
- LASへの移行により、製品エディションは**Premium**に、ライセンスモデルは**Concurrent**に設定されますが、これは将来変更される可能性があります。PowerShellを使用してライセンス構成を変更しないでください。登録やセッション起動に影響を与える可能性があります。
- 既存のレガシーライセンスからLASへのCitrix Virtual Apps and Desktops™サイトの移行は、Web Studioのみを使用して行うことができます。

主な手順

1. ライセンスサーバーをバージョン11.17.2ビルド53100以降にインストールまたはアップグレードし、「ライセンスアクティベーションサービス用にライセンスサーバーを構成する方法」に記載されている手順に従ってLASを構成します。
2. Citrix Virtual Apps and Desktops™ バージョン 2411 以降をインストールします。Citrix Delivery Controller、Citrix Studio、Web Studio、Citrix Director などのコアコンポーネントをインストールします。

> **注:**
>
> Citrix Virtual Apps and Desktopsサイト内のすべてのDelivery Controllerは、LASと互換性がある必要があります。

3. 必要なコンポーネントをインストールした後、Citrix Site Managerを使用してサイトを作成します。サイトの作成については、「サイトの作成」を参照してください。ライセンスサーバーがLASを使用するように構成されている場合、Metainstallerはエンタイトルメントを表示します。エンタイトルメントは、対応するライセンス有効期限とともに提供されます。



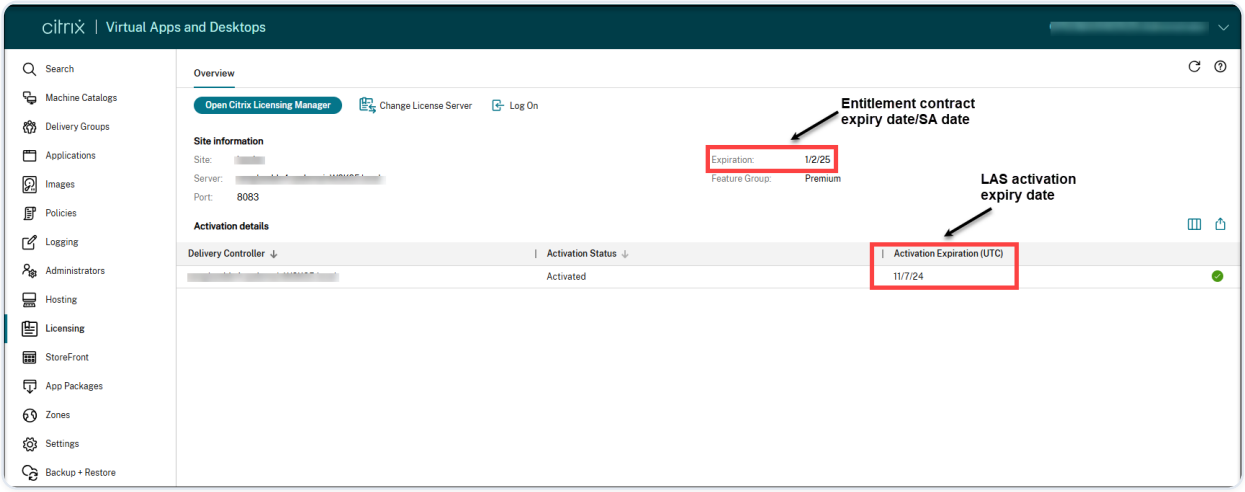
> **注:**
>
> License Serverが最新のLicense Serverバージョンにアップグレードされていない場合、エラーメッセージが表示されます。

4. ライセンスの詳細を確認する。
5. レガシーライセンスをLASに移行する。

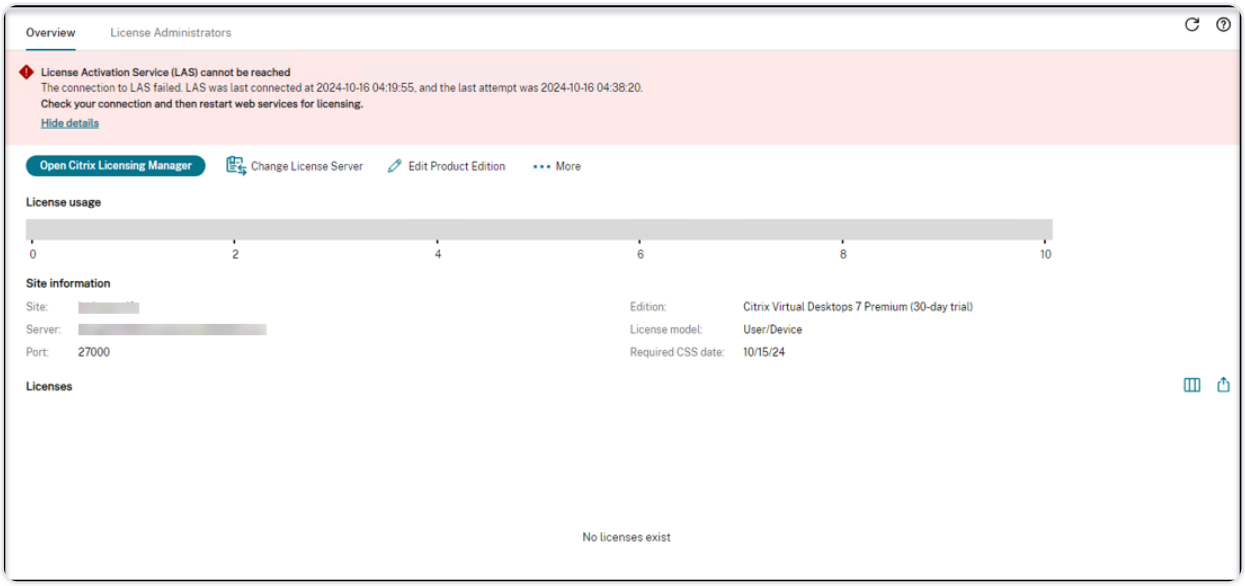
ライセンスの詳細を確認する

サイトを作成したら、Web Studioを使用してライセンスの詳細を確認します。

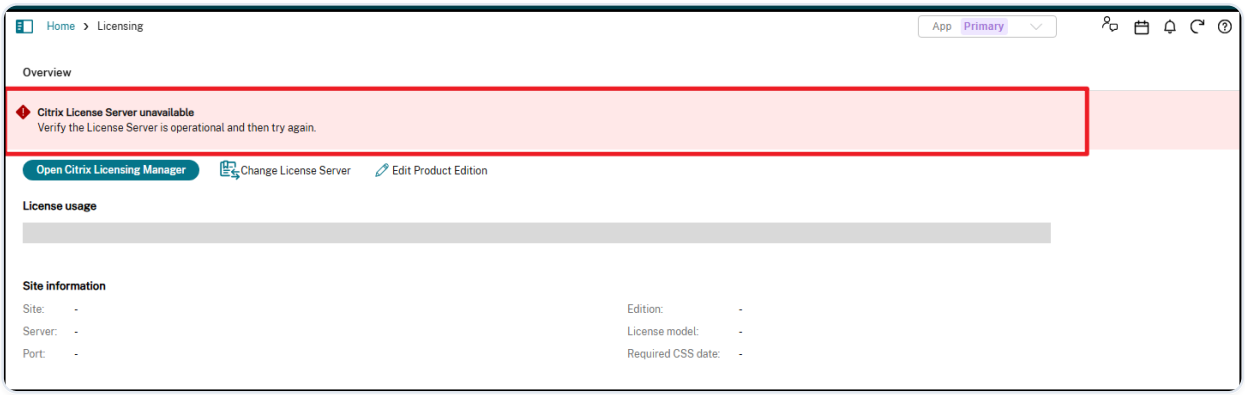
1. Web Studioで、**［ライセンス］**ノードを選択します。
2. **［概要］**タブで、Citrix Virtual Apps and Desktopsサイトに適切なライセンスがあるか、またはLAS機能の使用中にライセンスの有効期限が切れていないかを確認します。



LASに到達できない場合、エラーメッセージが表示されることがあります。



ライセンスサーバーが利用できない場合、エラーメッセージが表示されることがあります。



ライセンスサーバーがまだ古いレガシーライセンスを使用しており、Citrix Virtual Apps and DesktopsサイトがLAS対応である場合、Web Studioはライセンスサーバーを Citrix Cloudに登録するよう促します。

LASを使用するためにライセンスサーバーを登録する(/en-us/citrix-virtual-apps-desktops/current-release/media/register-license-server.png)

レガシーライセンスをLASに移行する

Citrix Cloudにライセンスサーバーを登録済みで、必要なエンタイトルメントがある場合は、ユーザーセッションに影響を与えることなく、既存のCitrix Virtual Apps and Desktopsサイトをレガシーライセンスから LASに移行するために、以下の特定の手順に従う必要があります。

1. **ライセンスサーバーのアップグレード:** ライセンスサーバーをサポートされている最小バージョンにアップグレードします。
2. **Delivery Controllerのアップグレード:** サイト内のすべてのDelivery ControllerをLASでサポートされているバージョンにアップグレードします。
3. **デリバリーグループのライセンス割り当てを削除する:**
   - **Migrate to LAS**をクリックする前に、サイトレベルより下に設定されているライセンス割り当てを手動で削除します (つまり、デリバリーグループレベルのライセンス割り当てを削除します)。
4. **割り当ての確認:** LASの割り当てが正確であることを確認します。
5. **Migrate to LASをクリックする:**
   - 前の手順が完了したら、**Migrate to LAS**をクリックします。

     レガシーライセンスからLASに移行する(/en-us/citrix-virtual-apps-desktops/current-release/media/migrate-to-las.png)

- LASに移行すると、Citrix Virtual Apps and Desktopsサイトの**ライセンスエディション**は**Citrix Virtual Apps and Desktops Premium**に設定され、**ライセンスモデル**は**Concurrent**に構成されます。

LASからレガシーライセンスへのロールバック

LASからレガシーライセンスにロールバックするには、次の手順を実行します。

1. 次のPowerShellコマンドを実行します。

```
Set-ConfigSite -UseLicenseActivationService $false
```

2. Web Studioでレガシーライセンスを構成します。

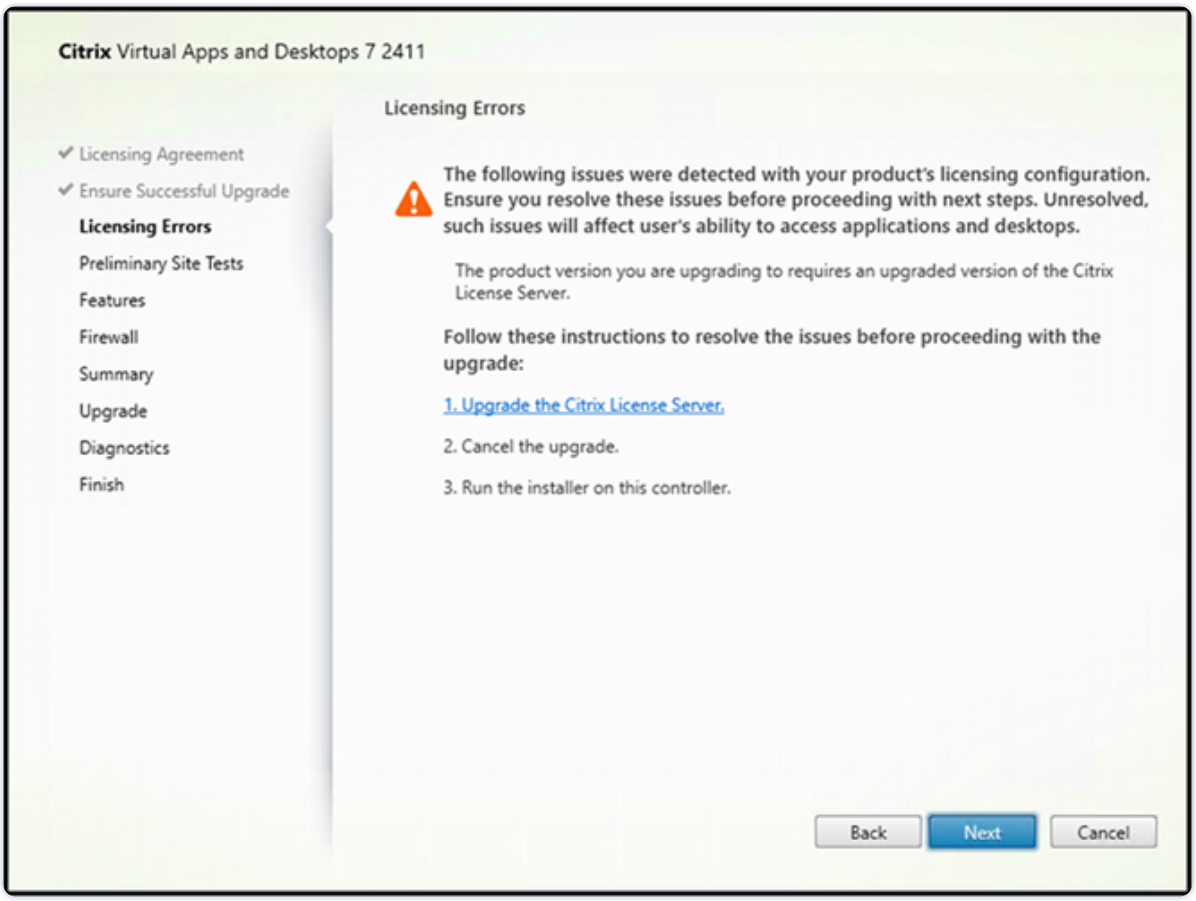
注:

これらの手順は、一時的なトラブルシューティングのみを目的としています。レガシーライセンスファイルは、サポート終了 (EOL) に近づいており、April 15, 2026 以降は機能しません。サービスの中断を避けるため、License Activation Service (LAS) への移行をお勧めします。詳細については、お知らせを参照してください。

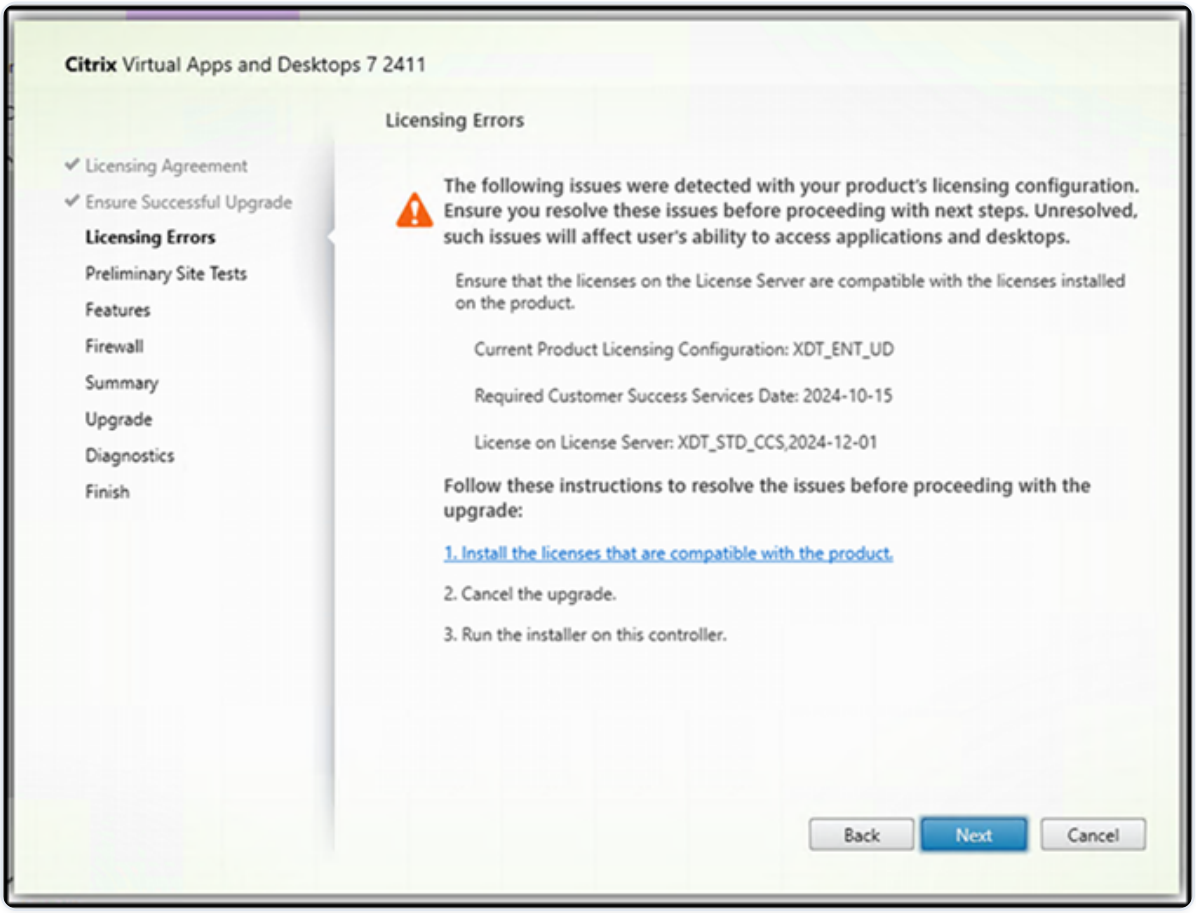
アップグレードに関する重要な考慮事項

以前のCitrix Virtual Apps and Desktopsバージョンから2411以降にアップグレードする場合は、License Serverを最新バージョン（バージョン11.2.17ビルド53100以降）にアップグレードしてください。

- メタインストーラーUIを使用してアップグレードする際に、ライセンスエラーページで次のエラーが発生します。
  - 最新のLicense Serverバージョンにアップグレードしない場合：



- 古いLicense Serverやライセンスの利用不可など、互換性の問題がある場合：



- コマンドラインを使用してアップグレードする場合、アップグレードの失敗を避けるために次のコマンドを実行します (マウントされたISOの\x64フォルダー内にいると仮定して)：

1. 次を実行します：

   ```
   \x64\Licensing\CitrixLicensing.exe /quiet
   ```

   ライセンスバイナリをローカルドライブのいずれかにコピーしている場合、次のコマンドを実行します：

   ```
   \x64\Licensing\CitrixLicensing.exe /quiet /l install.log
   ```

2. 次を実行します：

   ```
   \x64\XenDesktop Setup\XenDesktopServerSetup.exe /components
   "CONTROLLER,WEBSTUDIO,DESKTOPDIRECTOR" /CONFIGURE_FIREWALL
   ```

コアコンポーネントのアンインストール

アップグレード中に、コマンド `\x64\Licensing\CitrixLicensing.exe /quiet` または `\x64\Licensing\CitrixLicensing.exe /quiet /l install.log` を使用してLicense Serverを最初にインストールし、その後コアコンポーネントをインストールした場合、アンインストールも同じ順序で行ってください：

1. コマンドラインを使用してライセンスサーバーをアンインストールします。

   ```
   CitrixLicensing.exe /quiet /uninstall /l uninstall.log
   ```

2. GUIまたはコマンドラインを使用してコンポーネントをアンインストールします。詳細については、「コンポーネントの削除」を参照してください。

コマンドライン `XenDesktopServerSetup.exe` または `removeall` を使用してライセンスサーバーとコンポーネントをアンインストールした場合は、レジストリエントリと残りのファイルをクリーンアップします。

レジストリエントリをクリーンアップするには：

1. レジストリキー `Citrix Licensing` を検索し、そのエントリを削除します。ほとんどの場合、エントリは次の場所にあります。

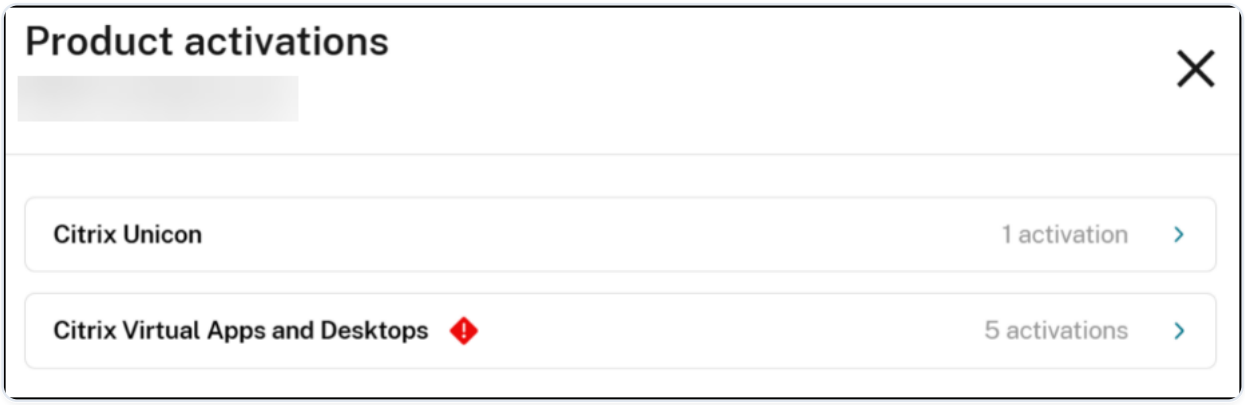
```
"Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\
```

2. レジストリキーの**Uninstall String**が指すフォルダーを削除します。

トラブルシューティング

Citrix Cloudでライセンスサーバーのステータスが緑色以外で表示されている場合は、問題が発生している可能性のあるアクティベーションの詳細を把握するために、次の手順を実行します。

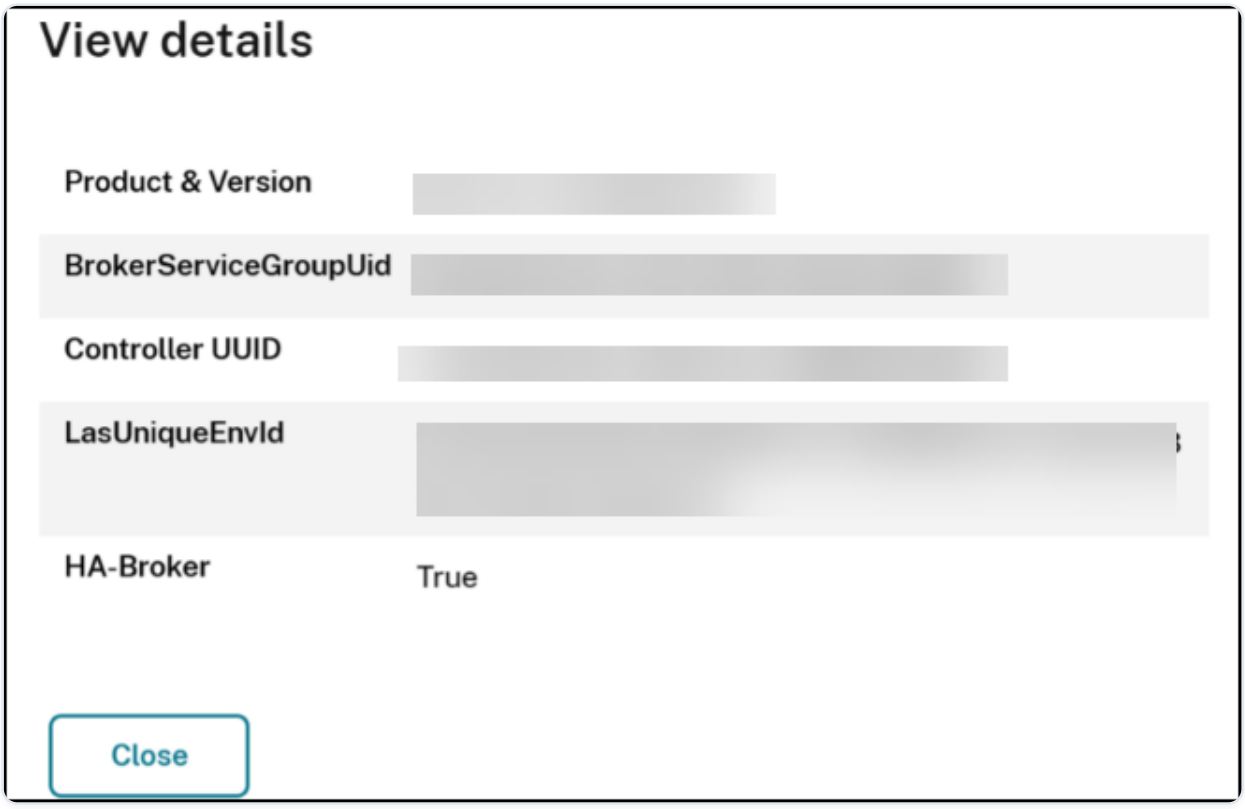
1. Citrix Cloud で、**ライセンス > ライセンス済み展開 > ライセンスサーバー**に移動します。
2. Citrix Virtual Apps and Desktopsの**>**展開ボタンをクリックして、アクティベートされたDelivery Controllerのリストを表示します。



3. アクティベーションの**［View details］**をクリックして、詳細を表示します。

   IDは、アクティベーションを識別するための一意の識別子です。

   次の詳細が提供されます。



- **製品とバージョン**：LASでアクティベートするときに製品が使用するように構成されているProduct_Edition_ModelとBurn In Date。BurnInDateは通常、製品のリリース日です。
- **BrokerServiceGroupUid**: ブローカーサービスグループの UID。
- **コントローラー UUID**: デリバリーコントローラーの UUID。
- **LasUniqueEnvId**: アクティベーションのために LAS によって提供されるインスタンスの一意の ID。
- **HA-Broker**: HA ブローカーかメインブローカーかを示す True または False。

アクティブ化されたホストの詳細を実際のホストにマッピングするには、ホストで次のコマンドを実行します。

- `Get-BrokerSite`: 画面に表示される **BrokerServiceGroupUid** の値を、コマンドの `BrokerServiceGroupId` 出力と比較します。
- `Get-BrokerController`: 画面に表示される **Controller UUID** の値を、コマンドの UUID 出力と比較します。

ライセンスイベントに関連するイベントビューアーログ

イベントID	説明
1112	Citrix Broker Service は、ユーザーからリソースへの接続を仲介できませんでした。サイト

イベントID	説明
	の製品およびエディションのライセンス構成では、このタイプのリソースは許可されていません。このサイトに正しいライセンスが選択されていることを確認してください。
1150	Citrix Broker Service はライセンスサーバーへの接続に成功しました。
1151	Citrix Broker Service はライセンスサーバーに接続できません。ライセンスサーバーが正しく機能していること、および XenDesktop 構成でライセンスサーバーを識別する詳細が正しいことを確認してください。
1152	このXenDesktopサイトには、ライセンスサーバーに必要な製品ライセンスがありません。ライセンス管理コンソールを使用して、関連する製品ライセンスをライセンスサーバーに追加してください。
1153	このXenDesktopサイトのライセンスの有効期限が切れました。Citrix Brokerサービスは、ライセンスサーバーから新しいライセンスを要求します。
1154	このコントローラーは、ライセンスサーバーに接続できなかったため、ライセンスキャッシュモードに入りました。このコントローラーがデスクトップおよびアプリケーションセッションの提供を停止するまで、残り2時間です。
1155	Citrix Brokerサービスは、デスクトップおよびアプリケーションセッションの提供を停止します。このコントローラーは、ライセンスサーバーとの通信が継続的に失敗したため、ライセンスキャッシュモードではなくなりました、またはライセンスキャッシュモードに入ることができませんでした。ライセンスサーバーが機能していることを確認し、必要に応じて、ライセンス管理コンソールを使用して関

イベントID	説明
	連するライセンスをライセンスサーバーに追加してください。
1156	Citrix Brokerサービスは、ライセンスサーバーと正常に通信しています。このコントローラーは、ライセンスキャッシュモードではなくなりました。
1157	実行中のライセンスサーバーのバージョンは、Citrix Brokerサービスのバージョンよりも古く、互換性がありません。ライセンスサーバーをアップグレードするか、XenDesktop構成で正しいバージョンのライセンスサーバーの場所を指定してください。
1158	Citrix Brokerサービスは、このエディションのこのサイトでライセンスサーバーが利用可能なライセンス数を超過していることを検出しました。ライセンスサーバーは、オーバードラフトライセンスを付与しました。
1159	Citrix Brokerサービスは、このサイトにインストールされているライセンスの最大数を超過したため、デスクトップ接続を拒否しました。このエディションには3つのライセンスがインストールされていますが、このエディションで許可されているライセンスの最大数は2つです。ライセンス制限に準拠するために、ライセンスサーバーから関連するライセンスを削除してください。
1160	Citrix Brokerサービスは、ライセンス管理中に内部エラーを検出しました。ライセンスサーバーが正しく機能していること、およびXenDesktop構成でライセンスサーバーを識別する詳細が正しいことを確認してください。Citrix Brokerサービスを再起動すると、問題が解決する場合もあります。この問題が解決しない場合は、Citrix XenDesktop Controllerを再インストールしてください。Citrix Knowledge Baseの記事CTX126990を参照してください。

イベントID	説明
1161	ライセンスの初期化中にエラーが発生しました。ライセンスサーバーの接続を確認してください。
1162	ライセンスの停止中にエラーが発生しました。ライセンスサーバーの接続を確認してください。
1163	接続ライセンスがありません。解決するには、不要なセッションを閉じてライセンスを解放するか、ライセンスを追加してください。
1164	接続ライセンスのチェックアウト中にエラーが発生しました。ライセンスサーバーの接続を確認してください。
1165	接続ライセンスのチェックイン中にエラーが発生しました。ライセンスサーバーの接続を確認してください。
1166	ライセンスの可用性確認中にエラーが発生しました。ライセンスサーバーの接続を確認してください。
1167	ライセンスの開始に失敗しました。ライセンスサーバーの接続を確認してください。
1168	ライセンスユーザー通知設定の読み取り中にエラーが発生しました。ライセンスサーバーの接続を確認してください。
1169	ライセンスサーバーで適切なライセンスが見つからなかったため、このコントローラーは初期設定のライセンスキャッシュモードに入りました。このコントローラーがデスクトップおよびアプリケーションセッションの提供を停止するまで、残り2時間です。
1170	Citrix Broker Serviceは、ライセンスサーバーで適切なライセンスを正常に検出しました。

イベントID	説明
	このコントローラーは、初期設定のライセンスキャッシュモードではなくなりました。
1171	ライセンスサーバーが指定されていません。有効なライセンスサーバーが指定されるまで、Citrix Broker Serviceはユーザーにデスクトップとアプリケーションを提供できません。Citrix StudioまたはCitrix PowerShell SDKのSet-ConfigSiteコマンドレットを使用して、ライセンスサーバーを指定できます。
1172	ライセンスサーバーの適合性確認中にエラーが発生しました。Citrix Broker Serviceは、マシンがライセンスサーバーとして使用するのに適しているかを確認する際に、予期しない応答を受け取りました。コントローラーからマシンに接続できること、およびマシンのファイアウォールがコントローラーからの接続を許可していることを確認してください。マシンにライセンスサーバーがインストールされている場合は、それが正しく構成され、動作していることを確認してください。
1173	このXenDesktopサイトには、ライセンスサーバーに必要な起動ライセンスがありません。License Administration Consoleを使用して、関連するライセンスをライセンスサーバーに追加してください。
1174	このXenDesktopサイトに構成されている製品エディションはアプリケーションをサポートしていません。アプリケーションリソースは利用できません。
1176	構成された製品エディションはマルチセッションマシンをサポートしていません。登録は拒否されました。
1177	構成された製品エディションはシングルセッションマシンをサポートしていません。登録は拒否されました。

イベントID	説明
1178	構成された製品エディションはRemotePCをサポートしていません。登録は拒否されました。
1179	構成された製品エディションは、クラウドシステムにプロビジョニングされたマシンをサポートしていません。登録は拒否されました。
1180	このXenDesktopサイト用に構成された製品エディションは、シングルセッション（ワークステーションOS）マシン上のアプリケーションをサポートしていません。アプリケーションリソースの起動は拒否されました。
1181	このXenDesktopサイト用に構成された製品エディションは、マルチセッション（サーバーOS）マシン上のアプリケーションをサポートしていません。アプリケーションリソースの起動は拒否されました。
1182	このXenDesktopサイト用に構成された製品エディションは、シングルセッション（ワークステーションOS）マシン上のデスクトップをサポートしていません。デスクトップリソースの起動は拒否されました。
1183	このXenDesktopサイト用に構成された製品エディションは、マルチセッション（サーバーOS）マシン上のデスクトップをサポートしていません。デスクトップリソースの起動が拒否されました。
1196	このコントローラーは、ライセンスサーバー上の使用可能なすべてのライセンスを使い果たしたため、ライセンスバーストモードに入りました。これを解決するには、さらにライセンスを追加してください。このコントローラーがデスクトップおよびアプリケーションセッションの提供を停止するまで、残り2時間です。

イベントID	説明
1197	Citrix Broker Serviceは、デスクトップおよびアプリケーションセッションの提供を停止します。このコントローラーは、ライセンスサーバー上のライセンス不足のため、ライセンスバーストモードを終了したか、またはライセンスバーストモードに入ることができませんでした。関連するライセンスをライセンスサーバーに追加するには、ライセンス管理コンソールを使用してください。
1198	Citrix Broker Serviceは、ライセンスサーバーからライセンスを正常に消費しています。現在の需要を満たすのに十分なライセンスがサーバー上にあります。このコントローラーは、ライセンス枯渇によって引き起こされたライセンスバーストモードを終了しました。
1199	Citrix Broker Serviceは、デスクトップおよびアプリケーションセッションの提供を停止します。ライセンスサーバーにライセンスがインストールされていないため、このコントローラーはライセンスキャッシュモードを終了したか、またはライセンスキャッシュモードに入ることができませんでした。関連するライセンスをライセンスサーバーに追加するには、ライセンス管理コンソールを使用してください。
1205	ソフトウェアメンテナンスの有効期限が切れました。Citrix環境は現在サポートされていません。ライセンスサーバーで期限切れのライセンスを確認し、削除してください。ユーザーが警告メッセージを受け取り始める前に、30日間のライセンスキャッシュモードがあります。
1206	ライセンス証明書のハッシュが無効です。Citrixライセンス証明書のハッシュが無効です。

イベントID	説明
1300	Citrix Broker Serviceは、デスクトップおよびアプリケーションセッションの提供を停止します。ライセンスサーバーのシステムクロックに問題があります。
1301	ライセンスサーバーのシステムクロックに関する問題が修正されました。Citrix Broker Serviceは正常な動作を再開します。
1302	このコントローラーは、接続ライセンスのチェックインまたはチェックアウトに再度失敗しました。以前に検出された障害はまだ存在します。過剰なイベントログを避けるため、問題が解決されるまで、サービスは関連メッセージ（イベントID 1163、1164、1165）を抑制しています。ライセンスの試行は継続されます。
1303	このコントローラーは、関連メッセージ（イベントID 1163、1164、1165）の抑制を停止しました。
1304	Citrix Broker ServiceはLASに正常に接続しました。
1305	Citrix Broker ServiceはLASに接続できません。LASが正しく機能していること、およびLASを識別する詳細がXenDesktop構成で正しいことを確認してください。

詳細情報

サイトのLAS状態の確認、またはサイトがライセンスキャッシュモードであるかどうかの確認については、以下を参照してください。

- サイトのLAS状態を確認するにはどうすればよいですか？
- サイトがライセンスキャッシュモードであるかどうかを確認するにはどうすればよいですか？

コマンドの詳細については、以下を参照してください。

- Get-BrokerController

- Get-ConfigSite

Citrix Virtual Apps and Desktops™ テレメトリデータ要素

ブローカー

使用方法

ヘッダー

キー	説明	例
バージョン	テレメトリイベントのバージョンを示します。	1
id	使用状況イベントの一意の識別子を示します。	d4ce7919-5d80-44de-a8fa-102923fe0ead
タイプ	Citrix Analytic Service がクラウド使用状況イベントを識別するために使用するイベントタイプを示します。	SendBrokerTelemetryData
st	Broker でイベントが生成されたときのタイムスタンプを示します。	2011-08-12T20:17:46.384Z
本番	使用状況イベントの発生元となる製品と展開を識別します。	XenDesktop.Broker (クラウド) OnPrem.Broker (On Prem)
prodVer	Citrix DaaS/Citrix Virtual Apps and Desktops の製品バージョンを示します。	7.25.0.0

ペイロード

フィールド	説明	例
TotalPublishedApps	公開されているアプリケーションの総数を示します。	10
TotalPublishedDesktops	公開されているデスクトップの総数を示します。	10
VDAs.Total	VDAの総数を示します。	10
VDAs.OSTypes	Windows、Linux、MacなどのOSタイプ別のVDAの総数を示します。	10
VDAs.OSVersions	Windows 10、11、2022、2019などのOSバージョン別の総数を示します。	10
VDAs.HostingLocations.Azure	Azure、AWS、GCP、Nutanix、VMWare、XenServer、HyperVなど、サポートされている各ホスティングロケーションのVDA数を示します。	10
VDAs.HostingLocations.AWS		
VDAs.HostingLocations.Nutanix		
VDAs.HostingLocations.VMWare		
VDAs.HostingLocations.XenServer		
VDAs.HostingLocations.HyperV		
VDAs.ProvisionedMethod.MCS	Machine Creation Service (MCS) によってプロビジョニングされたマシンの数を示します。	10

フィールド	説明	例
VDAs.ProvisionedMethod.ManualOr3P	手動または3Pでプロビジョニングされたマシンの数を示します。	10
VDAs.SessionSupport.StaticSingle	静的に割り当てられたシングルセッションのマシンの数を示します。	10
VDAs.SessionSupport.DynamicSingle	動的に割り当てられたシングルセッションのマシンの数を示します。	10
VDAs.SessionSupport.Multi	マルチセッションマシンの総数を示します。	10
VDAs.RemotePCAccess.Windows	OSタイプ (Win、Mac、Linux) 別のRemote PC Accessマシンの数を示します。	10
VDAs.RemotePCAccess.Linux		
VDAs.RemotePCAccess.MacOS		
VDAs.ActiveSessionRecordingAgents	アクティブなセッション記録エージェントを持つVDAの数を示します。	5
VDAs.Subscriptions	VDAのパブリッククラウドサブスクリプションの数を示します。	2
VDAs.LocationTypes	VDAのロケーションタイプの数を示します。	2
AutoScale.DGWithAutoscaleEnabled	**Autoscale** が有効になっているデリバリーグループの数を示します。	2
AutoScale.TotalMachinesCtrlByAutoscale	Autoscaleによって制御されるマシンの数を示します。	5

フィールド	説明	例
AutoScale.VerticalAutoscaleEnabledByDGandSite	DGとサイトによって**Vertical Autoscale**が有効になっているマシンの数を示します。	2
AutoScale.TaggedBasedAutoscaledDG	タグベースのAutoscaleが適用されたデリバリーグループの数を示します。	2
DeliveryGroup.TotalRebootSchedulesEnabled	**再起動スケジュール**が有効になっているデリバリーグループの数を示します。	2
DeliveryGroup.Total	デリバリーグループの総数を示します。	10
Policy.TotalPolicySets	ポリシーセットの数を示します。	3
Policy.TotalPolicies	グループポリシーの数を示します。	2
Policy.TotalPolicySettings	グループ設定の数を示します。	2
PublishedPackageApps.AppVSingleAdmin	AppVシングルアドミンモードで公開されているパッケージ化されたアプリの総数を示します。	2
PublishedPackageApps.AppVDualAdmin	AppVデュアルアドミンモードで公開されているパッケージ化されたアプリの総数を示します。	2
PublishedPackageApps.Msix	MSIXモードで公開されているパッケージ化されたアプリの総数を示します。	2
PublishedPackageApps.AppAttach	AppAttachモードで公開されているパッケージ化されたアプリの総数を示します。	2

フィールド	説明	例
PublishedPackageApps.FlexApp	FlexAppモードで公開されたパッケージ化されたアプリの総数を示します。	2

セッション

ヘッダー

フィールド	説明	例
バージョン	ライセンス使用状況イベントのバージョンを示します。	1
id	使用状況イベントの一意の識別子を示します。	d4ce7919-5d80-44de-a8fa-102923fe0ead
タイプ	Citrix Analytic Serviceがクラウド使用状況イベントを識別するために使用するイベントタイプを示します。	Cloud.Licensing
st	Brokerでイベントが生成されたときのタイムスタンプを示します。	2011-08-12T20:17:46.384Z
本番	使用状況イベントの発生元製品と展開を識別します。	XenDesktop.Broker (クラウド) OnPrem.Broker (OnPrem)
prodVer	Citrix DaaSまたはCitrix Virtual Apps and Desktopsの製品バージョンを示します。	7.25.0.0

フィールド	説明	例
ユーザー	セッション起動を開始するユーザーを一意に識別するためのユーザーIDを特定します。**値はスクランブルされています。**	fullName: C648FE671A44B3F7 **(常にスクランブルされています)** samName:C758LH671A44B3F7 **(常にスクランブルされています)** upn: C7948FE671A44B3F7 **(常にスクランブルされています)** userLicenseId:C265FE671A44B3F7 **(常にスクランブルされています)** userSid: C097FE671A44B3F7 **(常にスクランブルされています)**
テナント -> ID	Citrix Cloud™アカウントの顧客IDを示します。オンプレミス展開の場合、このフィールドは適用されず、値はありません。	ジョジ1mh0598tj
dvc から dvcId	セッション起動が開始されたデバイスを一意に識別するためのデバイスIDを示します。	AE18C4D5

フィールド	説明	例
デバイス -> デバイス名	デバイスのフレンドリ名を示します。**値はスクランブルされています。**	C758LH671A44B3F7 **(常にスクランブルされています)**

ペイロード

フィールド	説明	例
appProtectionKeyLoggingRequired	セッションがキーロギング保護を有効にして起動されたかどうかを示します。	いいえ
appProtectionScreenCaptureRequired	セッションが画面キャプチャ保護を有効にして起動されたかどうかを示します。	いいえ
cspTenantCustomerId	CSPテナントのCitrix Cloudアカウントの顧客IDを示します。オンプレミス展開の場合、このフィールドは適用されず、値はありません。	6c2vtxgxyftt
isAnonymousUser	認証されていないセッションが起動されたかどうかを示します。	いいえ
licenseActivityTimeStamp	ペイロードが生成されたときのタイムスタンプを示します。	2011-08-12T20:17:46.384Z
licenseActivityType	ライセンスイベントの種類を示します。このフィールドは、ライセンスイベント	接続

フィールド	説明	例
	の種類が割り当てアクションかリリースアクションかを示します。	
licenseModel	展開のライセンスモデルを示します。	UserDevice
productEdition	展開の製品エディションを示します。	プレミアム
productId	展開内の製品の製品IDを示します。	CAVDS
プロトコル	セッションの起動に使用されたプロトコルを示します。	HDX™
sessionKey	セッションの一意の識別子を示します。	uq390c5fc3-86eb-4df3-bd9a-f4a8fed2c9e2
sessionSupport	セッションサポートの種類を示します。	SingleSession
sessionType	セッションの種類を示します。	アプリケーション
バージョン	ペイロードのバージョンを示します。	1.3
workerSid	セッションに使用されるVDAの一意の識別子を示します。**値はスクランブルされます。**	1E5LH671A44B3F7 **(常にスクランブルされます)**
isWindows365	セッションがWindows 365向けに起動されたかどうかを示します。	はい

フィールド	説明	例
entitlementType	お客様のライセンスエンタイトルメントタイプを示します。	本番
siteId	サイトの一意の識別子を示します。	a35647d0-901c-4477-87e0-dcd781d455f4
desktopGroupId	デスクトップまたはデリバリーグループの一意の識別子を示します。	e9d859dc-1bfc-4b3e-bad3-41806bb4e694
clientType	Citrix Workspace™ アプリのタイプを示します。	ウィンドウズ
clientVersion	Citrix Workspaceアプリのバージョンを示します。	23.5.1.83
workerCloudType	VDAプロビジョニングに使用されるパブリッククラウドの種類を示します。	アジュール
enabledFeatures	セッションで有効になっている機能を示します。たとえば、`AppProtectionScreenCaptureRequired` と `SessionRecording` が有効になっているセッションでは、このフィールドの値は 66 です。	66
launchRequestSource	起動を要求するために使用された製品を記録します。オンプ	0 (StoreFront or 3P)

フィールド	説明	例
	レミスStoreFront™またはCloud StoreFrontのいずれかです。	1 (ワークスペース)
isEvents	{{page.lic}}における重大な障害を示します。	STデータベースを作成できません。
heartBeatTime	CISまたはCitrix Analytic Serviceへのライセンスサーバーのハートビート時間を示します。	1689058813
vdaTelemetry	App Layering、User Personalization Layer、User Profile management、Workspace Environment Management™、およびHDX機能のためにキャプチャされるペイロードを示します。	vdaTelemetry SessionTelemetry CPM_feature: 32 HDX1: 66 HDX2: 0 MachineTelemetry AL_productVersion: 23.12.0.1001 UPL_isEnabled: 1 CPM_version: 22.3.4000 wem_enableMethod: 1 wem_agentVersion: 2402.1

スタジオ

使用方法

ヘッダー

フィールド	説明	例
バージョン	ライセンス使用状況イベントのバージョンを示します。	1
id	使用状況イベントの一意の識別子を示します。	8c2e20a5-ca3f-4401-ad69-d037933c40a0
タイプ	Citrix Analytic Service がクラウド使用状況イベントを識別するために使用するイベントタイプを示します。	Studio.Usage
st	Studio でイベントが生成されたときのタイムスタンプを示します。	2024-03-22T01:32:23.4056195Z
本番	使用状況イベントの発生元となる製品と展開を識別します。	XenDesktop.Studio
prodVer	Citrix DaaS/Citrix Virtual Apps and Desktops の製品バージョンを示します。	7.42.0.0

ペイロード

フィールド	説明	例
AdminLoginList	一意の管理者 SamAccountName のリストを示します。**値はスクランブルされています。**	{AdminLoginList: [UFMJ+JvXOTHO9mQDsOweiw= =]}**(常にスクランブルされています)**
TotalApiRequests	オーケストレーションサービスの API リクエストを示します。	{TotalApiRequests: 1000}

フィールド	説明	例
BackupCount	Studio 管理者によって操作されたバックアップの数を示します。	{BackupCount: 200}
RestoreCount	Studio管理者によって実行された復元回数を示します。	{RestoreCount: 20}

ディレクター

使用状況レポート

ヘッダー

フィールド	説明	例
バージョン	ライセンス使用状況イベントのバージョンを示します。	1
id	使用状況イベントの一意の識別子を示します。	8c2e20a5-ca3f-4401-ad69-d037933c40a0
タイプ	Citrix Analytic Serviceがクラウド使用状況イベントを識別するために使用するイベントタイプを示します。	テレメトリ
st	Studioでイベントが生成されたときのタイムスタンプを示します。	2024-03-22T01:32:23.4056195Z
本番	使用状況イベントの発生元製品と展開を識別します。	XenApp.Monitor
prodVer	Director製品のバージョンを示します。	7.42.0.0
dvcName	サーバーの名前	C758LH671A44B3F7

ペイロード

フィールド	説明	例
AdminLoginCount	これは、管理者ログインの数を提供するペイロードのセクションです。	type: 管理者ログイン統計 0: 1 1: 7
FeatureUsageCount	ペイロードのこのセクションには、Director で使用されている主要な機能の数が含まれています。	type: 機能使用状況統計 0: 15 1: 20 5: 10
OdataUsageCount	このペイロードのセクションには、OData APIの使用状況のカウントが含まれています。	タイプ: OData_v3 統計 0: 1 2: 7 5: 9 タイプ: OData_v4 統計 0: 1 2: 8 6: 7
AppUsage	公開されたアプリケーションの週ごとの使用状況メトリックを示します。	タイプ: AppUsage ヘッダー: applicationName,processName,totalDurationInMinutes

フィールド	説明	例
		期間: 01/05/24-07/05/24 値: [Calc_AWTSVDA-1907R,calc.exe,0.13, Notepad_AWTSVDA-1907R,notepad.exe,4]
UniqueAppUsers	公開されたアプリケーションについて、1か月あたりのユニークユーザー数とアプリケーションの合計起動回数を示します。	タイプ: ユニークアプリユーザー ヘッダー: アプリケーション名,総起動回数,総ユニークユーザー数 期間: 04/24 値: [Calc_AWTSVDA-1907R,100,10, Notepad_AWTSVDA-1907R,200,20]
DesktopUsage	公開デスクトップの週次使用状況メトリックを示します。	タイプ: DesktopUsage ヘッダー: desktopGroupName,sessionSupport,totalDurationInMinutes 期間: 01/05/24-07/05/24 値: [

フィールド	説明	例
		RdsDesktopAndAppGroup,1,10]
UniqueDesktopUsers	公開デスクトップの月間ユニークユーザー数と合計起動回数を示します。	タイプ: UniqueDesktopUsers ヘッダー: desktopGroupName,totalLaunches,totalUniqueUsers 期間: 04/24 値: [RdsDesktopAndAppGroup,10,5]
AvgLogonDuration	平均ログオン期間を示します。	タイプ: AvgLogonDuration ヘッダー: totalUserLogons, avgLogonDurationInSeconds 期間: 01/05/24-07/05/24 値: [200,4]
CostSaved	顧客が1か月あたりに節約したコストを示します。	タイプ: CostSaved ヘッダー: hypervisor,costSaved,currency 期間: 04/24 値: [

フィールド	説明	例	
		1,221.02,1 2,301.02,2]	

Storefront構成

使用方法

ヘッダー

フィールド	説明	例
バージョン	ライセンス使用状況イベントのバージョンを示します。	1.0
id	使用イベントの一意の識別子を示します。	d4ce7919-5d80-44de-a8fa-102923fe0ead
タイプ	CAS がクラウド使用状況イベントを識別するために使用するイベントの種類を示します。	構成
st	StoreFront でイベントが生成されたときのタイムスタンプを示します。	2011-08-12T20:17:46.384Z
本番	使用イベントの発生元の製品と展開を識別します。	OnPrem.StoreFront
prodVer	StoreFront のバージョン (内部) を示します。	3.30.0.0

ペイロード

フィールド	説明	例
serverName	StoreFront が実行されているサービスのホスト名を示します。	storefront-01.storefront.local

フィールド	説明	例
deploymentId	StoreFront の展開の一意の識別子を示します。	f47ac10b-58cc-4372-a567-0e02b2c3d479
installedWithCVAD	StoreFront が CVAD と一緒にインストールされたかどうかを示します。	偽
cpuCores	CPU コアの総数を示します。	4
cpuModel	StoreFront を実行している CPU を示します。	第12世代 Intel(R) Core(TM) i7-1255U 1.70 GHz
ramGb	RAM の合計容量 (GB) を示します。	16
numServersInGroup	サーバーグループ内のサーバーの数を示します。	3
ストア	StoreFront Store構成JSONブロブを示します。Storeオブジェクトの配列です。**一部の値はスクランブルされています**	例
rfWebSites	StoreFront RFWeb構成JSONブロブを示します。RFWeb構成オブジェクトの配列です。	例
ゲートウェイ	JSONブロブとしてのゲートウェイ構成オブジェクトを示します。ゲートウェイオブジェクトの配列です。	例
authServices	JSONブロブとしての認証サービス構成オブジェクトを示します。認証サービスオブジェクトの配列です。	例
IsPiiScrambled	真	

フィールド STORES の例

```
[{

            "BaseUrl": "baseUrl",

            "StorePath": "/",

            "EnabledFeatures": 21 bit bitmap,

            "ResourceTypeFilteringEnabled": "disabled|
Citrix.MPS.Application;Citrix.MPS.Desktop",

            "DefaultRfWebSite": "/Citrix/StoreWeb",

            "GatewaysUsed": [

                "gatewayId"

            ],

            "VdaLogonDataProvider": "",

            "ResourceFeeds": [

                {

                    "FeedName": "<resourceFeedName>|scrambled",

                    "Type": "CVAD",

                    "LoadBalancingEnabled": true,

                }

            ],

            "AdvancedAggregation": {

                 "Enabled": true,

                 "GroupingCount": 1,

                 "ControllersPushIdenticalResources": true,
```

```
                "LoadBalanced": true,

                "AnyPrimaryFarms": true,

                "AnyBackupFarms": true,

            }

}]
```

ストアが見つからない場合、それは空の配列になります 。

フィールド RFWEBSITES の例

```
[{

    "SiteId": "siteId",

    "BaseUrl": "baseUrl",

    "StorePath": "storePath",

    "UiExperienced": 0,

    "EnabledFeatures": 9 bit,

    "AuthMethodsEnabled": [

        "ad"

    ],

    "CanUsersDownloadApps": {

        "Enabled": true,

        "Windows": "exe",

        "MacOS": "dmg"

    },

    "WorkspaceControl": {
```

```
        "Enabled": true,
        "LogoffAction": 0,
        "AutoReconnectAtLogon": true,
        "ShowReconnectButton": true,
        "ShowDisconnectButton": true
    },
    "MultiClickTimeout": 1,
    "UiViews": [
        "apps",
        "desktops"
    ],
    "DefaultTab": 0,
}]
```


rfWebサイトが見つからない場合、それは空の配列になります 。

フィールド GATEWAYS の例


```
[{
            "GatewayId": "gatewayId",
            "IsCloudGateway": true,
            "LoadBalancingSTAEnabled": true,
            "SessionReliabilityEnabled": true,
            "RequestTicketsFromTwoSTA": true,
            "Version": "1234",
```

```
            "LogonType": "domain",

            "SmartCardFallbackEnabled": true

}]
```

ゲートウェイが見つからない場合、それは空の配列になります 。

フィールド AUTHSERVICES の例

```
[{

    "SiteId": "SiteId",

    "Store": "StoreAuth",

    "AuthMethodsEnabled": [

        "ad"

    ],

    "PasswordChangeWhenExpired": 0,

    "PasswordRemindersForm": 1,

    "DelegateCredentialValidationToCitrix": true,

    "ValidatePasswordsOnDeliveryControllers": true

}]
```

認証サービスが見つからない場合、それは空の配列になります 。

ストアフロントログイン

使用方法

ヘッダー

フィールド	説明	例
バージョン	ライセンス使用状況イベントのバージョンを示します。	1.0
id	使用状況イベントの一意の識別子を示します。	d4ce7919-5d80-44de-a8fa-102923fe0ead
タイプ	CASがクラウド使用状況イベントを識別するために使用するイベントタイプを示します。	ログイン
st	Brokerでイベントが生成されたときのタイムスタンプを示します。	2011-08-12T20:17:46.384Z
本番	使用状況イベントの発生元製品と展開を識別します。	OnPrem.StoreFront
prodVer	StoreFrontバージョン（内部）	3.30.0.0

ペイロード

フィールド	説明	例
ユーザー	起動を開始したユーザー。**値はスクランブルされています**	fullName: C648FE671A44B3F7 **(常にスクランブルされています)** samName:C758LH671A44B3F7 **(常にスクランブルされています)**

フィールド	説明	例
		upn: C7948FE671A44B3F7 **(常にスクランブルされています)** userLicenseId:C265FE671A44B3F7 **(常にスクランブルされています)** userSid: C097FE671A44B3F7 **(常にスクランブルされています)**
serverName	StoreFrontが稼働しているサービスのホスト名を示します	storefront-01.storefront.local
loginMethodRfWeb	ユーザーがRFWebからStoreFrontにログインするために使用した方法を示します	0
loginMethodAuth	ユーザーが認証サービスからStoreFrontにログインするために使用した方法を示します	0
gatewayURL	ログイン中に使用されたNetscaler Gatewayを示します	netscaler-gateway.com
enabledFeatures	有効な機能のビットマスクを示します	12
userAgent	ログインに使用されたクライアントの	CitrixReceiver/ 22.11.0.19 Linux/ 5.17.15 X1Class

フィールド	説明	例
	UserAgentを示します	CWACapable CWA/22.11.0.19
baseUrl	ユーザーがログインしたストアを示します	storefront-dev.storefront.dev
storePath	ユーザーがログインしたストアを示します	/Citirx/StoreWeb
apiUsed	クライアントがStoreまたはPNAgent APIを使用しているかどうかを示します	0
deviceId	StoreFrontへのログインに使用されたデバイスを示します。**値はスクランブルされています**	ジョン・ドウ
transactionId	単一のトランザクション中に送信/生成されるトランザクションIDを示します。	773aba9e-5b91-4ef9-8782-c4afb75698e7

委任管理

使用方法

ヘッダー

キー	説明	例
バージョン	ライセンス使用状況イベントのバージョンを示します。	1
id	使用状況イベントの一意の識別子を示します。	8c2e20a5-ca3f-4401-ad69-d037933c40a0

キー	説明	例
タイプ	Citrix Analytic Service がクラウド使用状況イベントを識別するために使用するイベントタイプを示します。	DelegatedAdmin.Usage
st	Delegated Admin でイベントが生成されたときのタイムスタンプを示します。	2024-03-22T01:32:23.4056195Z
本番	使用状況イベントの発生元製品と展開を識別します。	XenDesktop.DelegatedAdmin (クラウド)
		OnPrem.DelegatedAdmin (OnPrem)
prodVer	Citrix DaaS または Citrix Virtual Apps and Desktops の製品バージョンを示します。	7.42.0.0

ペイロード

キー	説明	例
TotalCustomScopes	カスタムスコープの総数を示します。	2
TotalCustomRoles	カスタムロールの総数を示します。	4

ライセンス テレメトリ データを難読化する

ライセンス テレメトリで送信される情報の機密性を考慮し、Citrix はデータを難読化するオプションを提供します。

次の表に、難読化できるデータを示します。

フィールド	説明	例
ユーザー	セッション起動を開始するユーザーを一意に識別するためのユーザー ID を識別します。	• fullName: `C648FE671A44B3F7` • samName: `C758LH671A44B3F7` • ユーピーエヌ: `C7948FE671A44B3F7` • userLicenseId: `C265FE671A44B3F7` • userSid: `C097FE671A44B3F7`
デバイス -> デバイス名	デバイスのフレンドリ名を示します。	`C758LH671A44B3F7`
workerSid	セッションに使用されるVDAの一意の識別子を示します。	`1E5LH671A44B3F7`
AdminLoginList	一意の管理者SamAccountNameのリストを示します	`{AdminLoginList: [UFMJ+JvXOTHO9mQDsOweiw= =]}`
ストア	StoreFrontストア構成のJSONブロブを示します。ストアオブジェクトの配列です。**一部の値はスクランブルされています**	例

フィールド	説明	例
deviceId	StoreFrontへのログインに使用されるデバイスを示します。	ジョン・ドウ

スクランブルを有効または無効にするには、Delivery Controllerで次のPowerShellコマンドを実行します。

> **注:**
>
> Citrix Service Provider™ (CSP) のお客様の場合、スクランブルは常に無効になっています。CSP のお客様は、PowerShell コマンドを使用してスクランブルを有効にすることはできません。

1. Delivery ControllerホストからPowerShellウィンドウを開きます。
2. コマンド `asnp citrix` を実行して、Citrix固有のPowerShellモジュールをロードします。
3. スクランブルを有効または無効にするには、次のコマンドを実行します。

   デフォルトでは、値は`1`または`true`であり、ライセンステレメトリデータのスクランブルを有効にします。

   無効にするには：

   ```
   Set-BrokerServiceConfigurationData Core.ScrambleLicensingData
   -SettingValue $false
   ```

   スクランブルを無効にした後、次のコマンドを使用して有効にできます。

   ```
   Set-BrokerServiceConfigurationData Core.ScrambleLicensingData
   -SettingValue $true
   ```

ライセンスに関するFAQ

> **注:**

- COVID-19パンデミックに関連する事業継続リソースについては、CTX27055を参照してください。
- 事業継続の維持に関する一般情報については、Business continuity — on demandを参照してください。
- 現在のCitrix License Serverに関する詳細については、Licensingを参照してください。

Citrix®ライセンス

License Activation Serviceとは何ですか?

License Activation Service (LAS) は、オンプレミスのCitrix License Server向けの最新のクラウドベースのライセンスソリューションです。これは、従来のファイルベースのライセンス方法に代わる合理化された選択肢を提供します。

ライセンスファイルを手動でアップロードする代わりに、ライセンスサーバーをCitrix Cloud™に接続してオンラインアクティベーションを行うことができます。これにより、ライセンスが自動的にライセンスサーバーに配信され、ライセンスファイルのライフサイクル管理が不要になります。

クラウドに接続できないライセンスサーバーの場合、LASはオフラインアクティベーションオプションも提供し、さまざまなネットワーク環境での柔軟性を確保します。このサービスは、Citrix製品ライセンスを管理するためのシームレスで最新のアプローチを導入します。

詳細については、License Activation Serviceを参照してください。

ライセンスファイルはどのように入手できますか?

ライセンスアクセスコードは電子メールで送信されます。ライセンスアクセスコードを使用してライセンスファイルを生成する方法は3つあります。

- `citrix.com` のMyAccountページから**ライセンスの管理**。詳細については、citrix.comでライセンスを管理するを参照してください。
- Web Studioを使用して購入を割り当てると、ライセンスファイルがCitrix License Serverに自動的にインストールされます。
- Citrix License Server内のCitrix Licensing Managerで、ご購入を割り当ててライセンスファイルをインストールします。詳細については、Install licensesを参照してください。

MyAccountでライセンスを割り当てる方法?

ライセンスの割り当てを参照してください。

割り当てられたライセンスをライセンスサーバーに追加する方法?

ライセンスの変更を参照してください。

Citrixライセンスが使用するTCPポート?

- ライセンスサーバーのポート番号は27000です。
- ベンダーデーモンのポート番号は7279です。
- ライセンス用Webサービスのポートは8083です。

Citrixライセンスサーバー?

Citrixライセンスサーバーは、ネットワーク全体でライセンスを共有できるシステムです。詳細については、「ライセンス操作の概要」を参照してください。

Citrix License Serverを仮想化またはクラスター化できますか?

はい。Citrixライセンスサーバーを仮想化またはクラスター化できます。詳細については、「クラスター化されたライセンスサーバー」を参照してください。

Citrix License Serverを仮想化した場合、どのようなメリットがありますか?

Citrixライセンスサーバーを仮想化すると、冗長なソリューションが提供されます。このソリューションにより、ダウンタイムなしで複数の物理サーバー間を移動できます。

Citrixライセンスサーバーを仮想化する場合、考慮すべき制限はありますか?

いいえ。

Citrix License Serverは、Citrix Virtual Apps and Desktops™展開のすべてのライセンスを管理しますか?

Citrix License Serverは、Citrix Virtual Apps™およびDesktop用に受け取るすべてのライセンスを管理します。ただし、Citrix Gatewayで使用されるPremium Editionのライセンスは除きます。これらのセキュリティ指向のネットワークデバイスに必要な、ネットワークアプライアンスに組み込まれたライセンスサーバーが、それらのライセンスを管理します。

Citrix Licensing Managerとは何ですか?

Citrix Licensing Managerを使用すると、Citrix Licensing ManagerをインストールしたLicense Serverからライセンスファイルをダウンロードして割り当てることができます。Citrix Licensing Managerは、推奨されるLicense Server管理方法であり、次のことが可能になります。

- License ServerのCitrix Cloudへのショートコード登録と、登録の簡単な削除。
- ユーザーアカウントとグループアカウントを構成する。

- ダッシュボードを使用して、インストール済み、使用中、期限切れ、および利用可能なライセンスと、Customer Success Servicesの期日を表示する。
- レポート作成に使用するため、ライセンス使用状況データをエクスポートする。
- 履歴使用状況データの保持期間を構成する。デフォルトのデータ保持期間は180日です。
- ライセンスアクセスコードまたはダウンロードしたファイルを使用して、License Serverへのライセンスファイルのインストールを簡素化する。
- ライセンスバーストモードを有効化および無効化する。
- Customer Experience Improvement Program (CEIP)およびCall Homeを構成する。
- Customer Success Servicesの更新ライセンスを自動または手動で確認し、見つかった場合は通知するか、ライセンスをインストールします。
- License Serverの状態（起動ライセンスの不足、時間に関する問題、アップローダーの失敗）を通知する。
- これらのポートを変更します。
    - ライセンスサーバー (デフォルト 27000)
    - ベンダーデーモン (デフォルト 7279)
    - ライセンス用Webサービス (デフォルト 8083)

詳細については、Citrix Licensing Managerを参照してください。

Citrix License Administration Consoleはどこにありますか?

License Administration Consoleはサポートされなくなり、License Serverバージョン11.16.6から削除されました。Citrix Licensing Managerの使用をお勧めします。

License ServerがStudioと同じドメイン内にあるか、信頼されたドメイン内にある場合、Studioを使用してライセンスを管理および追跡できます。

詳細については、Citrix Licensing Managerを参照してください。

ライセンス割り当て期間?

ライセンス割り当て期間とは、Citrix Virtual Apps and Desktopsライセンスがユーザーまたはデバイスに割り当てられる期間のことです。デフォルトのライセンス割り当て期間は90日間です。

組織が購入したライセンス数の確認方法?

購入したすべてのライセンスは、`<https://www.citrix.com>`の**My Account**ページにある安全な**Manage Licenses**ツールボックスから、いつでも（24時間365日）確認およびアクセスできます。

現在使用中のライセンス数を確認する方法?

Citrix Licensing ManagerとStudioは、リアルタイムのライセンス使用状況に関する詳細情報を提供します。

ライセンスサーバーのディザスターリカバリとメンテナンス

ライセンスサーバーのディザスターリカバリとメンテナンスについては、Citrix Licensingのドキュメントの「ディザスターリカバリとメンテナンス」を参照してください。

Citrix Virtual Apps and Desktopsのライセンス

Citrix Virtual Apps and Desktopsはどのようにライセンスされますか?

Citrix Virtual Apps and Desktopsのライセンスは、ユーザー単位とデバイス単位、および同時使用ライセンスモデルを提供します。

ユーザー/デバイス:

柔軟なユーザー/デバイスモデルは、以下と連携します。

- 全社的なデスクトップ利用。
- 基盤となるMicrosoftデスクトップ仮想化ライセンス。
- 仮想デスクトップとアプリへのアクセスが時々しか必要ないユーザーを持つ顧客向けの同時使用ライセンス。

ユーザー/デバイスライセンスにより、ユーザーは無制限のデバイスから仮想デスクトップとアプリにアクセスできます。デバイスライセンスにより、無制限のユーザーが単一のデバイスから仮想デスクトップとアプリにアクセスできます。このアプローチは、最大限の柔軟性を提供し、Microsoftデスクトップ仮想化ライセンスとの整合性を向上させます。

> **重要:**

> ライセンスをユーザーまたはデバイスに手動で割り当てることはできません。ライセンスサーバーまたはクラウドサービスがライセンスを割り当てます。ユーザー/デバイスライセンスでは、一度割り当てられたライセンスは、90日間非アクティブになるまで別のユーザーに割り当てることはできません。

> **同時使用:**

同時使用ライセンスは、任意のユーザーおよび任意のデバイスに対して、無制限の数の仮想アプリおよびデスクトップへの1つの接続を許可します。ライセンスはアクティブなセッション中にのみ消費されます。セッションが切断または終了した場合、ライセンスはプールに戻されます。

ユーザー/デバイスライセンスの詳細については、ユーザー/デバイスライセンス を参照してください。同時使用ライセンスについては、同時使用ライセンス を参照してください。

ライセンスを購入する前にCitrix Virtual Apps and Desktopsを試用することはできますか?

はい。Citrix Virtual Apps and Desktopsソフトウェアをダウンロードし、試用モードで実行できます。試用モードでは、ライセンスなしで、オンプレミスでCitrix Virtual Apps and Desktopsを30日間、10接続まで使用できます。詳細については、評価ライセンス を参照してください。

Citrix Cloud向けのCitrix DaaS™ (旧Citrix Virtual Apps and Desktopsサービス) は、承認に基づいて試用サービスとして利用できます。詳細については、Citrix担当者にお問い合わせください。

CitrixはCitrix Virtual Apps and Desktopsの同時使用をどのように定義していますか?

Citrix Virtual Apps and Desktopsの同時接続モデルでは、任意のユーザーと任意のデバイスに対して、無制限の数の仮想アプリとデスクトップへの1つの接続を許可します。ライセンスはアクティブなセッション中にのみ消費されます。セッションが切断または終了した場合、ライセンスは再発行のためにプールに戻されます。詳細については、「同時接続ライセンス」を参照してください。

共通のライセンスサーバーにCitrix Virtual Apps and Desktopsライセンスの複数のエディションを展開できますか?

はい。ライセンスサーバーは、Citrix Virtual AppsとCitrix Virtual Desktopsの両方のライセンスを同時に管理します。最新のライセンスサーバーバージョンをインストールすることをお勧めします。お使いのライセンスサーバーのバージョンが最新であるか不明な場合は、Citrixダウンロードサイトの番号とご自身のバージョンを比較して確認してください。

単一のサイトでCitrix Virtual AppsとCitrix Virtual Apps and Desktopsの両方のライセンスを使用できます?

バージョンによっては、単一のCitrix Virtual AppsまたはCitrix Virtual Apps and Desktopsサイトで、ユーザー/デバイスまたは同時接続の両方のライセンスモデルをサポートできます。単一のCitrix Virtual AppsまたはCitrix Virtual Apps and Desktopsサイトは、1つのエディションのみをサポートできます。詳細については、「マルチタイプライセンス」を参照してください。

マルチタイプライセンスをサポートする最小バージョンは、XenAppおよびXenDesktop 7.15 Long Term Service Release (LTSR) とCitrix Virtual Apps and Desktops 7 1808です。

ライセンスサーバーにCitrix Virtual Apps and Desktopsユーザー/デバイスまたはCitrix Virtual Apps and Desktops同時接続ライセンスがインストールされている場合、製品モデルとしてCitrix Virtual Apps同時接続を選択できます?

Citrix Virtual AppsをCitrix Virtual Apps and Desktops AdvancedまたはPremium Editionの機能として使用する場合、Citrix Virtual Appsのライセンスモデルは、Citrix Virtual Apps and DesktopsのAdvancedまたはPremium Editionと同じになります。Citrix Virtual Apps and Desktopsを購入した場合、Citrix Virtual Appsの機能のみを使用する予定であっても、ライセンスをCitrix Virtual Apps and Desktopsとして構成してください。製品モデルとしてCitrix Virtual Appsを選択するのは、ライセンスサーバーにCitrix Virtual Apps同時接続スタンドアロンライセンスがインストールされている場合のみです。

各Citrix Virtual AppsおよびCitrix Virtual Apps and Desktopsエディションには、どのような製品コンポーネントが含まれていますか?

エディションごとの全機能マトリックスについては、「Citrix Virtual Apps and Desktopsの機能」を参照してください。

Citrix Virtual Apps and Desktops EULAに準拠して、Citrix Virtual Desktops™環境のライセンスを付与するにはどうすればよいですか?

Citrix Virtual Apps and Desktops EULAに準拠して、ユーザー/デバイスまたは同時接続ライセンスモデルでCitrix Virtual Apps and Desktopsを展開するには、ライセンスファイルをライセンスサーバーに適用します。ライセンスサーバーは、ライセンスコンプライアンスを制御および監視します。購入した製品に基づいて製品を構成することをお勧めします。たとえば、Citrix Virtual Apps and Desktops Premiumを購入したが、Citrix Virtual Apps機能のみを使用したい場合は、コンプライアンスを満たすために製品をCitrix Virtual Apps and Desktopsに構成してください。詳細については、「製品ライセンスコンプライアンスセンター」を参照してください。

Citrix Virtual Apps EULAに準拠して、Citrix Virtual Apps環境のライセンスを付与するにはどうすればよいですか?

Citrix Virtual Apps EULAに準拠して、同時接続ライセンスモデルでCitrix Virtual Appsを展開するには、ライセンスファイルをライセンスサーバーに適用します。ライセンスサーバーは、ライセンスコンプライアンスを制御および監視します。

Citrix Virtual Apps and Desktopsのサービスオプション（Long Term Service Release (LTSR)またはCurrent Release (CR)）にライセンス要件はありますか?

Long-Term Service ReleaseなどのCitrix Virtual Apps and Desktopsのサービスオプションは、Customer Success Servicesプログラムの特典です。LTSRの特典を受けるには、アクティブなCustomer Success Servicesが必要です。詳しくは、「[Citrix Virtual Apps、Citrix Virtual Apps and Desktops、およびXenServerのサービスオプション」を参照してください。

Remote Browser Isolation (RBI) サービスのプールされた時間はどのように機能しますか?

サービスを最低25ユーザー購入すると、すべてのユーザーで共有される5000時間のサービス利用権が付与されます。その後のユーザー権限の購入では、プールされた時間の権利は増加しません。サービス時間の権利を増やすには、アドオンパックを購入してください。

CCUライセンスでRemote PC Accessを使用できますか?

はい。

Remote PC Accessの詳細については、「Remote PC Access」を参照してください。

Citrix環境のソフトウェアメンテナンスの有効期限が切れるとどうなりますか?

ソフトウェアメンテナンス (SWM) またはサブスクリプションの有効期限が切れると、ソフトウェアアップグレードとテクニカルサポートへのアクセスが一時停止されます。また、ライセンスの種類と製品バージョンによっては、エンドユーザーと管理者に、環境がサポートされていないことを示す特定の警告通知が届きます。

これらの通知は、サーバー上のすべてのライセンスの有効期限が切れた場合にのみトリガーされます。

エンドユーザーエクスペリエンス

ユーザーはセッション起動後に警告メッセージを受け取ります。メッセージには次のように表示されます。

```
Citrix Virtual Apps and Desktops warning: Your corporate Citrix
environment is currently unsupported. Please contact your IT department to
resolve.
```

管理者エクスペリエンス

管理者は、Citrix Studioコンソール内で、間もなく期限切れになる、または現在期限切れになっていることを警告するアラートを確認できます。

ライセンスの種類による有効期限の動作

これらのメッセージの表示タイミングは、ライセンスの種類とインストールされているCitrix Virtual Apps and Desktopsのバージョンによって異なります。

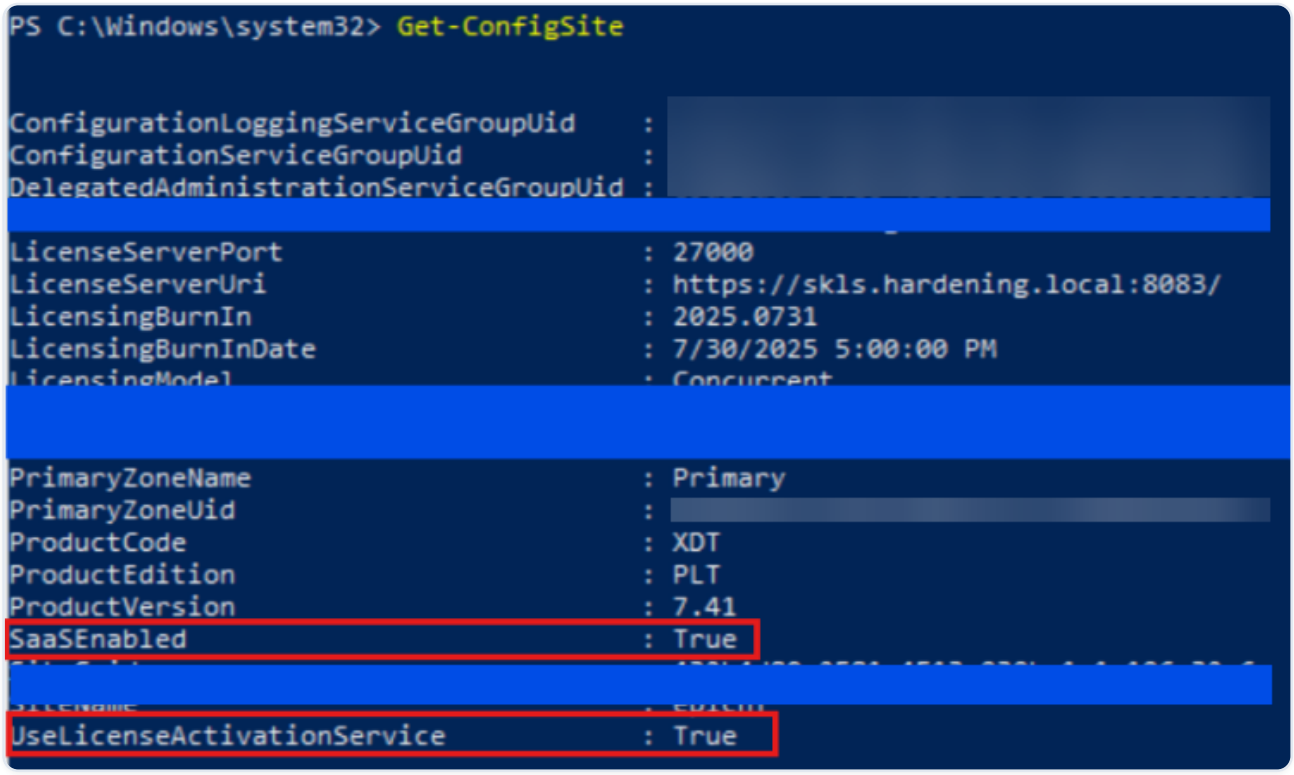
オンプレミスサブスクリプションライセンス

- エンドユーザー警告: サブスクリプションの有効期限が切れた後、猶予期間中に表示されます。
- 管理者警告: サブスクリプションの有効期限が切れる30日前にStudioに表示されます。

- サポートされているバージョン:
  - 現在のリリース: Citrix Virtual Apps and Desktops 2411以降。
  - LTSR: 2203 CU6、2402 CU1、およびそれ以降のLTSRリリース

サイトのLAS状態を確認するにはどうすればよいですか?

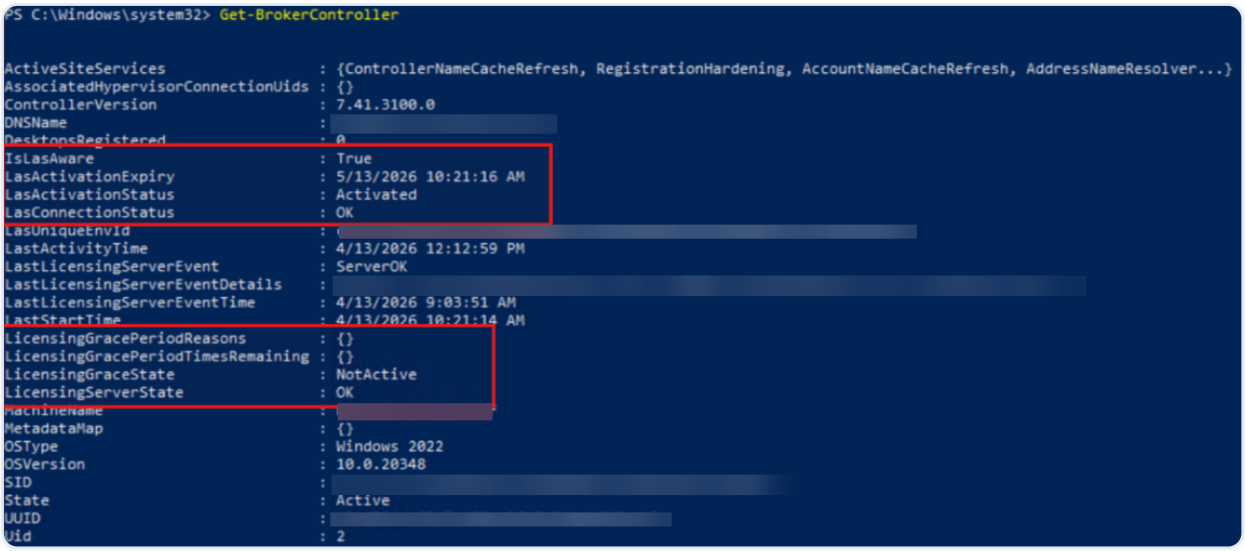
LASアクティベーションの状態とSaaSビットのステータスを確認するには、`Get-configsite`を実行します。



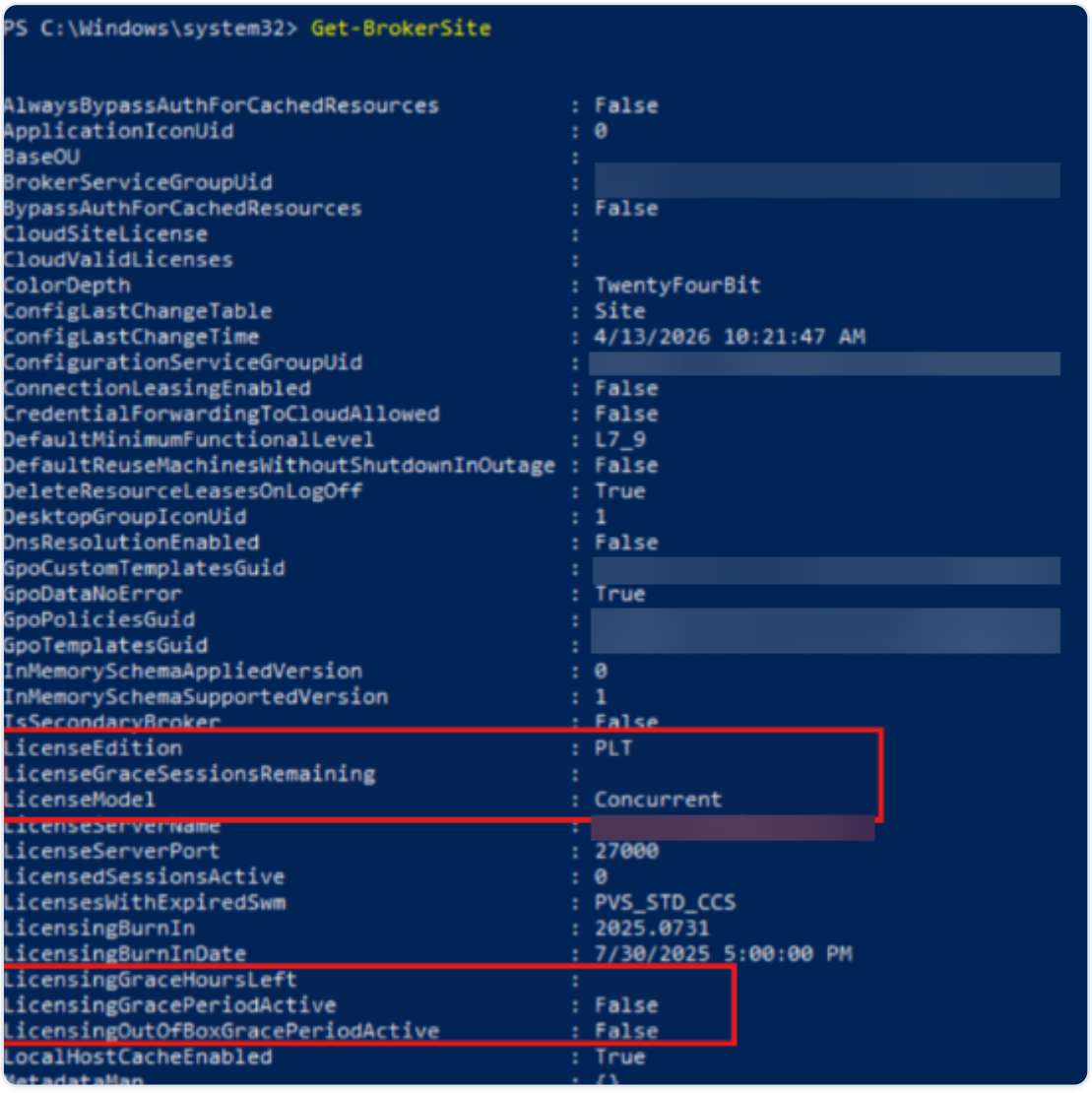
サイトがライセンスキャッシュモードになっているか確認するにはどうすればよいですか?

キャッシュモードと残り時間の詳細を取得するには、`Get-Brokercontroller`と`Get-brokersite`を実行します。

- `Get-Brokercontroller`出力：



- `Get-brokersite`出力：



コマンドの詳細については、以下を参照してください。

- Get-BrokerController

- Get-ConfigSite

ライセンスに関するDelivery Controllerのイベントビューアーログについては、「ライセンスイベントに関連するイベントビューアーログ」を参照してください。

ユーザー/デバイスライセンス

Citrixは、ユーザー/デバイスライセンスモデルでユーザーにライセンスをどのように割り当てますか?

ユーザー/デバイスライセンスモデルでは、ライセンスサーバーは一意のユーザーIDにライセンスを割り当てます。これにより、その単一ユーザーは無制限のデバイスから無制限の接続を行うことができます。ユーザーがデスクトップまたはデバイスに接続する場合、仮想デスクトップまたはアプリケーションにアクセスするには、そのユーザーに割り当てられた1つのライセンスが必要です。ライセンスサーバーまたはクラウドサービスがライセンスを割り当てます。これらのライセンスを手動で割り当てることはできません。ライセンスは共有デバイスではなく、ユーザーに割り当てられます。一度ライセンスが割り当てられると、90日間非アクティブになるまで、別のユーザーに割り当てることはできません。詳細については、「ユーザー/デバイスライセンス」を参照してください。

Citrixは、ユーザー/デバイスライセンスモデルでライセンスデバイスをどのように定義しますか?

ライセンスデバイスには、一意のエンドポイントデバイスIDが必要です。ユーザー/デバイスモデルでは、デバイスとは、Citrix Virtual Apps and Desktopsのインスタンスにアクセスするために、個人が使用することを承認したあらゆる機器を指します。共有デバイスの場合、単一のCitrix Virtual Apps and Desktopsユーザー/デバイスライセンスで、デバイスを共有する複数のユーザーをサポートできます。たとえば、共有デバイスは、教室のワークステーションや病院の臨床ワークステーションなどです。

Citrix Virtual Desktops Standard Editionの同時使用ライセンスをユーザー単位とデバイス単位のモデルに変換できますか?

Citrix Virtual Desktops Standard Editionの同時使用ライセンスをCitrix Virtual Desktops Standard Editionのユーザー/デバイスライセンスに変換することはできません。同様に、Citrix Virtual Desktops Standard Editionのユーザー/デバイスライセンスをCitrix Virtual Desktops Standard Editionの同時使用ライセンスに変換することもできません。

Citrix Virtual Desktops Standard Editionの同時使用ライセンスをお持ちで、ユーザー/デバイスライセンスモデルをご希望の場合は、Citrix Virtual Apps and Desktops AdvancedまたはPremium Editionにアップグレードしてください。

元	STANDARD同時使用へ	STANDARDユーザー/デバイスへ	ADVANCEDユーザー/デバイスへ	PREMIUMユーザー/デバイスへ
Citrix Virtual Desktops Standard Editionの同時使用ライセンス	該当なし	同時使用からユーザー/デバイスへの変換は許可されていません	ライセンスモデルを変換することはできませんが、Citrix Virtual Apps and Desktops AdvancedまたはPremium Editionにアップグレードすることはできます。	ライセンスモデルを変換することはできませんが、Citrix Virtual Apps and Desktops AdvancedまたはPremium Editionにアップグレードすることはできます。
シトリックス バーチャル デスクトップス スタンダード エディション ユーザー/デバイス ライセンス	ユーザー/デバイスから同時使用への変換は許可されていません	該当なし	該当なし	該当なし

同時使用ライセンスとユーザー/デバイスライセンスの違い?

同時使用ライセンスは、デバイスの同時接続に基づいています。同時使用ライセンスは、デバイスがアクティブな接続を確立している場合にのみ使用されます。接続が終了すると、同時使用ライセンスはすぐに使用可能なライセンスプールに戻されます。このライセンスモデルは、一時的な使用におすすめです。ユーザー/デバイスライセンスは一定期間リースされ、リース期間が終了するまで他のユーザーは利用できません。

ユーザー/デバイスモデルにおける、同じ企業内でのユーザーとデバイスへのライセンス割り当て?

はい。両方のタイプを同じ企業内で使用できます。ライセンスサーバーは、使用状況に基づいてユーザーまたはデバイスにライセンスを最適に割り当てます。これらのライセンスを手動で割り当てることはできません。

ライセンスを付与するユーザーまたはデバイスの数をどのように決定すればよいですか?

適切なライセンス数を決定するために、ユースケースの要件を評価してください。ユーザー/デバイスライセンスは、無制限の数のデバイスから無制限の仮想デスクトップと仮想アプリへの無制限のアクセスを可能にします。同時使用ライセンスは、無制限の数のユーザーが使用できる単一の

デバイスから無制限の仮想デスクトップと仮想アプリへの無制限のアクセスを可能にします。次の式を考慮してください。

```
(Number of total users) – (number of users that only access exclusively

 with shared devices) + (number shared devices) = total number

 of licenses to buy.



For example, there are 1000 total users at the hospital. If 700 of them
access only

Citrix Virtual Desktops from 300 shared devices in the hospital, the
number of

licenses to purchase is 1000 – 700 + 300 = 600 licenses.
```

ユーザー/デバイスモデルでは、ライセンスを持つユーザーが自分の環境に接続するために使用できるデバイスの最大数はいくつですか?

各ライセンスユーザーは、接続されているかオフラインであるかにかかわらず、無制限のデバイスを使用できます。

ユーザー/デバイスモデルでは、ライセンスデバイスにアクセスできるユーザーの最大数?

各ライセンスデバイスは、組織内で無制限のユーザーにサービスを提供できます。

ユーザー/デバイスモデルでは、ライセンスユーザーが一度に利用できる仮想デスクトップまたはRBI Webアプリケーションの最大数?

各ライセンスユーザーは、無制限の仮想デスクトップまたはWebアプリケーションに接続できます。

既存のCitrix Virtual Apps and Desktops環境で、ライセンスユーザー/デバイスの数を増やすためにCitrix Virtual Apps and Desktopsライセンスを購入できますか?

はい。既存のCitrix Virtual Apps and Desktops環境で、ライセンスユーザー/デバイスの数を増やすためにCitrix Virtual Apps and Desktopsライセンスを購入できます。

承認されたユーザー/デバイスライセンスを解放するにはどうすればよいですか?

承認されたユーザー/デバイスの割り当てを解放するには、EULAの条項に従って`udadmin`ユーティリティを使用します。その後、ライセンスサーバーは次の適切なユーザー/デバイスにライセ

ンスを割り当てます。詳細については、「ユーザーまたはデバイスのライセンスの表示または解放」を参照してください。

購入したユーザー/デバイスライセンス数を超過した場合、どうなりますか?

ユーザー/デバイスライセンスには10%の超過分が含まれており、これはライセンスが生成される際に含まれます。この超過分は、インストール済みのライセンス数にも含まれます。使用量の急増が、超過分を含むインストール済みの数を超えた場合、追加ユーザーのアクセスは拒否されます。より多くのユーザーがアクセスできるように、新しいライセンスを購入して展開してください。

ライセンスの超過分を含め、すべてのライセンスが使用中の場合、ライセンスバーストモードにより製品への無制限の接続が可能になります。ライセンスバーストモードは、最大ライセンス数を超過した理由を特定し、ユーザーを中断することなく追加のライセンスを購入するための時間を提供します。この期間は、15日が経過するか、追加の小売ライセンスをインストールするかのいずれか早い方まで続きます。詳細については、「ライセンスバーストモード」を参照してください。

Director はライセンスキャッシュモードの状態を表示します。詳細については、「Director ダッシュボードのパネル」(/ja-jp/citrix-virtual-apps-desktops/current-release/director/site-analytics.html#panels-on-the-director-dashboard) を参照してください。

ライセンスユーザーが一度に利用できる仮想アプリケーションの最大数はいくつですか?

各ライセンスユーザーは、無制限の仮想アプリケーションに接続できます。

ライセンスユーザーが組織を離れた場合、どうなりますか?

既存のライセンスユーザーが組織を離れる場合、Citrixに通知することなく、そのユーザーのライセンスを解放できます。ライセンスを解放するには、`udadmin`ユーティリティを使用します。ライセンスを解放しない場合、ライセンスサーバーは90日間の非アクティブ状態の後、自動的にライセンスを解放します。この情報は、EULAに指定された条件に従います。

ライセンスユーザーが長期間不在の場合、どうなりますか?

既存のライセンスユーザーが長期間不在の場合、Citrix に通知することなくライセンスを解放し、再割り当てできるようにすることができます。ライセンスを解放するには、`udadmin` ユーティリティを使用します。

組織内のライセンスデバイスを交換した場合、どうなりますか?

既存のライセンスデバイスを交換する場合、Citrix に通知することなくライセンスを解放し、再割り当てできるようにすることができます。ライセンスを解放するには、`udadmin` ユーティリティを使用します。

ライセンスデバイスが長期間サービス停止した場合、どうなりますか?

既存のライセンスデバイスが長期間サービス停止した場合、Citrixに通知することなくライセンスを解放し、再割り当てできるようにすることができます。ライセンスを解放するには、`udadmin`ユーティリティを使用してください。ライセンスを解放しない場合、ライセンスサーバーは90日間アクティビティがないと自動的にライセンスを解放します。この情報は、EULAに規定されている条件に従います。

デバイスまたはユーザーにライセンスを割り当てた後で、ユーザーライセンスをデバイスライセンスに、またはその逆に切り替えることはできますか?

はい、この変更は自動的に行われます。ライセンスサーバーは、使用パターンに基づいてユーザーまたはデバイスのいずれかにライセンスを割り当てます。使用パターンが変更された場合、ライセンスサーバーは新しい使用状況に基づいて割り当てを切り替えることがあります。ライセンスサーバーは常に、お客様にとって最も経済的な方法でライセンスを割り当てます。また、ライセンスサーバーは、90日間の割り当て期間後に**未使用**のライセンスを特定するためにライセンスを監視します。90日間の割り当て期間後に未使用と識別されたライセンスは、他のユーザーまたはデバイスに再割り当てできます。

同時使用ライセンス

同時使用モデルでは、Citrix Virtual Apps and Desktops のライセンスユーザーが一度に消費できる仮想デスクトップの最大数はいくつですか?

エンドポイントは多数のユーザーにサービスを提供でき、無制限の接続を許可します。

以前のバージョンの Citrix Virtual Apps and Desktops の同時使用ライセンスと、新しいユーザー/デバイスライセンスまたは同時使用ライセンスを、単一のライセンスサーバーに展開できます?

はい。同じライセンスサーバーを使用して、ユーザー/デバイスまたは同時使用ライセンスの展開をサポートし続けることができます。

単一のライセンスサーバーに、同時使用ライセンスとユーザー/デバイスライセンス、または同時使用ライセンスを展開できます?

はい。引き続き同じライセンスサーバーを使用して、同時使用ライセンスとユーザー/デバイスライセンス、または同時使用ライセンスの展開をサポートできます。

Citrix Virtual Apps and Desktops AdvancedおよびPremiumエディションには、Citrix Virtual Appsの同時使用ライセンスが含まれていますか?

Citrix Virtual Apps and Desktops AdvancedおよびPremiumのユーザー/デバイスライセンスには、互換性のためのみにCitrix Virtual Appsの同時使用ライセンスが含まれています。これらの同時使用

ライセンスは、ユーザー/デバイスライセンスと互換性のない以前の製品バージョンでのみ使用できます。ユーザー/デバイスライセンスに含まれる同時使用互換ライセンスの使用は、XenApp 6.5より前のバージョンおよびXenDesktop 5.0 Service Pack 1より前のバージョンでのみ許可されます。

購入した同時使用ライセンス数を超過した場合、どうなりますか?

すべてのライセンスが使用中の場合、ライセンスバーストモードにより、製品への無制限の接続が可能になります。ライセンスバーストモードは、最大ライセンス数を超過した理由を特定し、ユーザーを中断することなく追加のライセンスを購入する時間を与えます。この期間は、15日経過するか、追加のリテールライセンスをインストールするかのいずれか早い方まで続きます。詳細については、「ライセンスバーストモード」を参照してください。

Directorは猶予期間の状態を表示します。詳細については、「Directorダッシュボードのパネル」を参照してください。

超過ライセンス

超過ライセンスはどのように入手できますか?

ユーザー/デバイス、ユーザー、またはデバイスライセンスモデルをサポートする製品（Citrix Cloudを除く）には、アクセス拒否を防ぐために限られた数の追加ライセンスを使用できるライセンス超過機能が含まれています。当社は、超過機能をライセンスエンタイトルメントとしてではなく、便宜のために提供しています。同時使用ライセンスおよびサーバーライセンスには超過機能は含まれていません。使用された超過ライセンスは、初回使用から30日以内に購入する必要がありますが、使用期間は30日に限定されません。Citrixは、新しい製品リリースで超過機能を削除する権利を留保します。詳細については、ライセンス超過を参照してください。

ライセンス超過をどのように識別できますか?

Citrix Licensing Managerで、オーバードラフト中のライセンス数を含む使用状況情報を表示できます。Studioにもオーバードラフトの使用状況情報が含まれています。

超過ライセンスが消費されるとどうなりますか?

Citrix Virtual Apps and Desktops環境へのアクセスを有効にするために、インストールされているライセンスからライセンスが割り当てられます。この超過ライセンスは、他のライセンスと同等のアクセスと機能を提供します。

超過ライセンスが消費されたときにアラートを受け取ることはできますか?

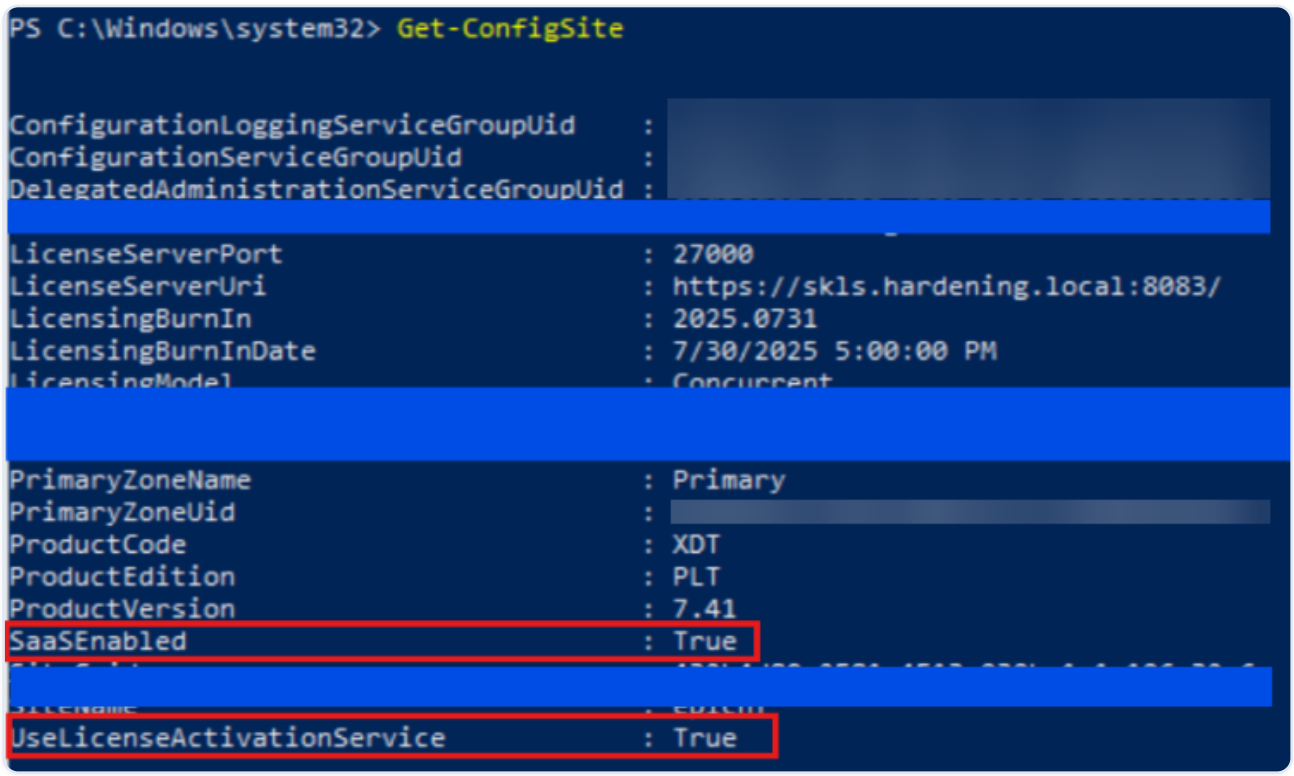
現在、オーバードラフトライセンスが消費されたときに提供される特定の警告はありません。

オーバードラフトライセンスはどのくらいの期間消費できます?

最初に使用してから30日以内に使用されたオーバードラフトライセンスを購入してください。

サイトのLAS状態を確認するにはどうすればよいですか?

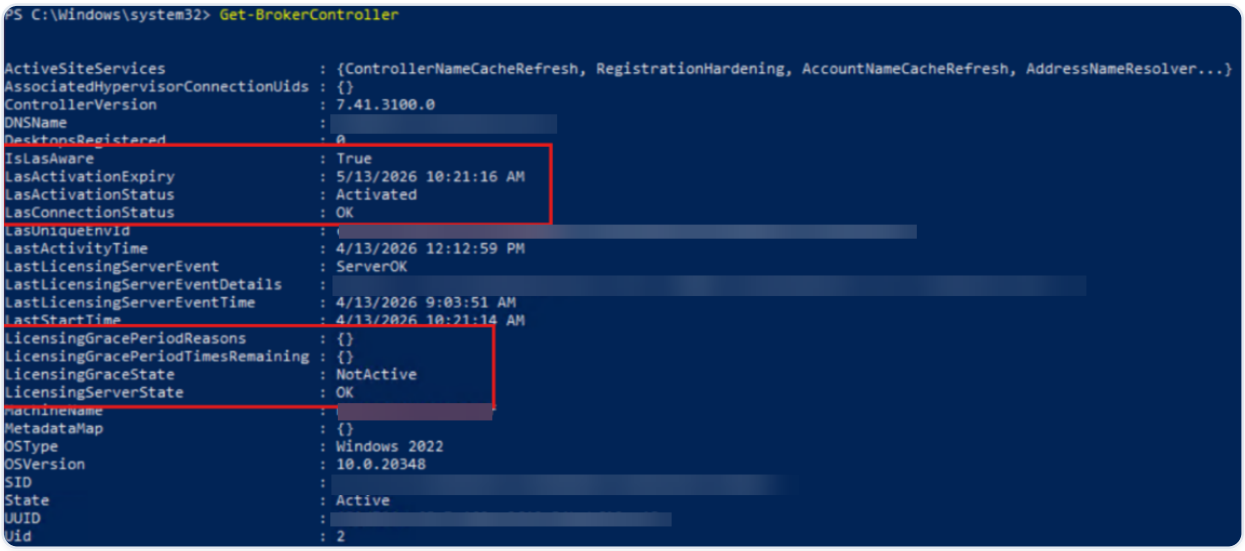
LASアクティベーション状態とSaaSビットステータスを確認するには、`Get-configsite`を実行します。



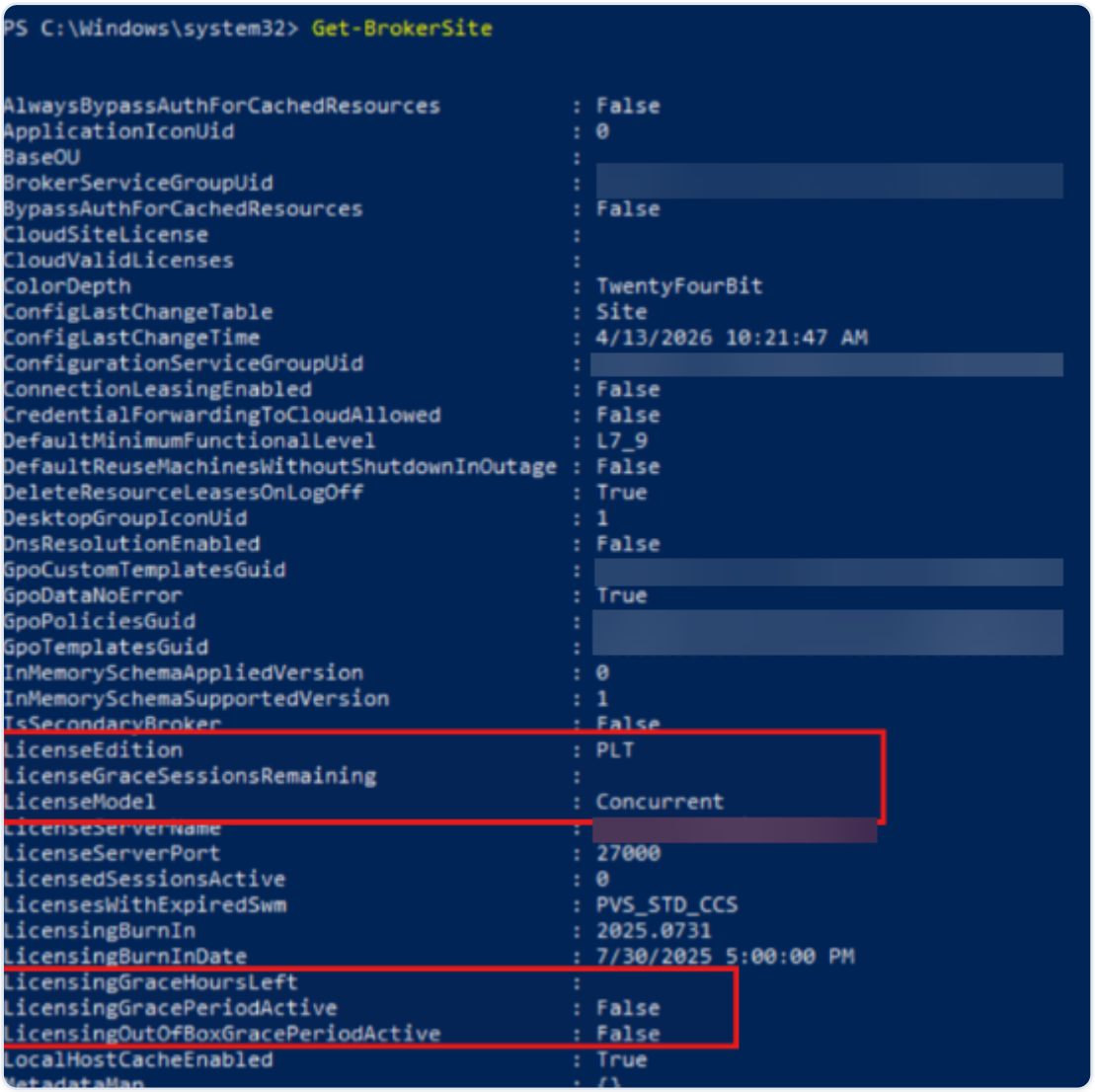
サイトが緊急ライセンスキャッシュモードになっているかを確認する方法?

緊急キャッシュモードと残り時間の詳細を取得するには、`Get-Brokercontroller`と`Get-brokersite`を実行します。

- `Get-Brokercontroller`の出力:



- `Get-brokersite`の出力:



コマンドの詳細については、以下を参照してください。

- Get-BrokerController

- Get-ConfigSite

ライセンスに関するDelivery Controllerのイベントビューアーログについては、「ライセンスイベントに関連するイベントビューアーログ」を参照してください。

その他の製品固有のライセンス情報

- シトリックス ADC
- シトリックス クラウド
- シトリックス エンドポイント マネジメント
- シトリックス ゲートウェイ
- XenServer
- シトリックス ライセンシング

ローカルホストキャッシュ

Citrix Virtual Apps and Desktopsサイトデータベースが常に利用可能であることを保証するため、CitrixはMicrosoftの高可用性ベストプラクティスに従って、フォールトトレラントなSQL Server展開から始めることを推奨します。(サポートされているSQL Serverの高可用性機能については、データベースを参照してください。)しかし、ネットワークの問題や中断により、ユーザーがアプリケーションやデスクトップに接続できなくなる可能性があります。

ローカルホストキャッシュ機能により、障害発生時にサイトでの接続仲介操作を継続できます。障害は、オンプレミスのCitrix®環境でDelivery Controller™とサイトデータベース間の接続が失敗したときに発生します。サイトデータベースに90秒間アクセスできない場合、ローカルホストキャッシュが作動します。

XenAppおよびXenDesktop 7.16以降、接続リース機能（以前のリリースにおける先行の高可用性機能）は製品から削除され、利用できなくなりました。

データコンテンツ

ローカルホストキャッシュには、メインデータベースの情報の一部である以下の情報が含まれます。

- サイトから公開されたリソースへの権限が割り当てられているユーザーおよびグループの ID。
- 現在使用している、または最近使用した、サイトから公開されたリソースのユーザーの ID。
- サイトで構成されている VDA マシン（リモート PC アクセス マシンを含む）の ID。

- 公開されたリソースへの接続に積極的に使用されているクライアントCitrix Receiver™マシンのID（名前とIPアドレス）。

また、メインデータベースが利用できなかった間に確立された、現在アクティブな接続に関する情報も含まれます。

- Citrix Receiverによって実行されたクライアントマシンのエンドポイント分析の結果。
- サイトに関与するインフラストラクチャマシン（NetScaler GatewayやStoreFront™サーバーなど）のID。
- ユーザーによる最近のアクティビティの日時と種類。

動作の仕組み

次の図は、通常の操作中のローカルホストキャッシュのコンポーネントと通信パスを示しています。

ローカルホストキャッシュの通常の操作中の通信パスの図(/en-us/citrix-virtual-apps-desktops/current-release/media/lhc-normal1.png)

通常の操作中

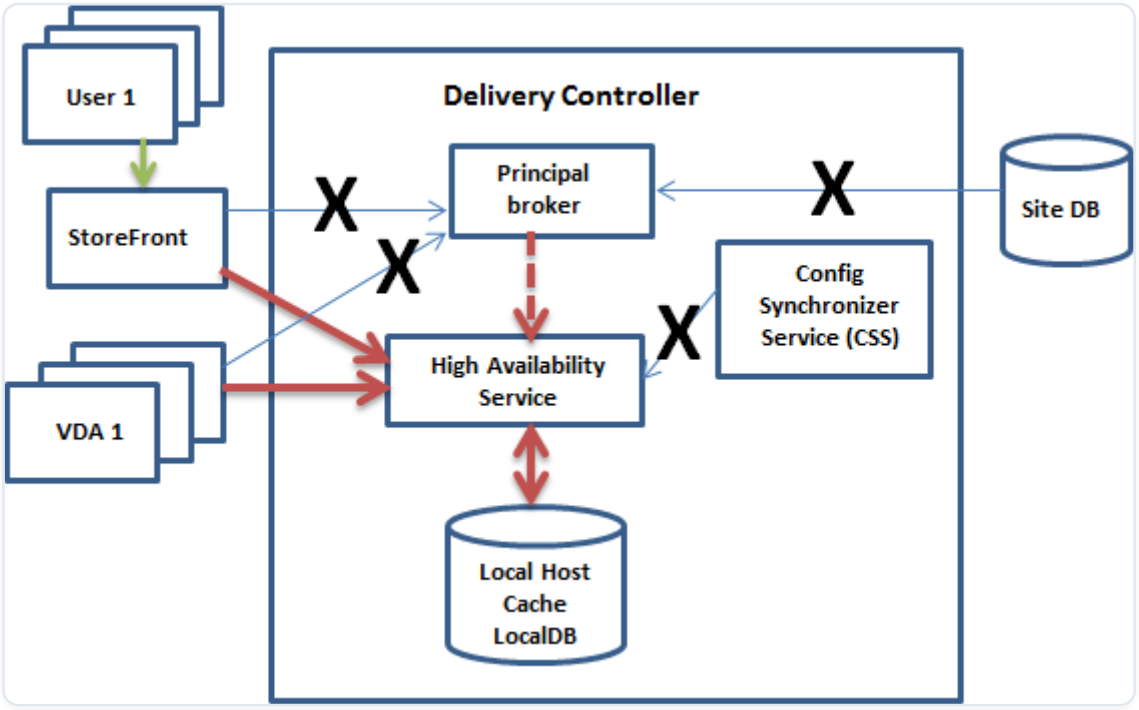
- Controller上の *プリンシパルブローカー* (Citrix Broker Service) は、StoreFrontからの接続要求を受け入れます。ブローカーはサイトデータベースと通信し、ユーザーをControllerに登録されているVDAに接続します。
- Citrix Config Synchronizer Service (CSS) は、約5分ごとにブローカーに問い合わせて、変更があったかどうかを確認します。これらの変更は、管理者によって開始されたもの（デリバリーグループのプロパティの変更など）またはシステムアクション（マシンの割り当てなど）である可能性があります。
- 前回のチェック以降に構成変更があった場合、CSS は情報を Controller 上のセカンダリブローカーに同期 (コピー) します。(セカンダリブローカーは高可用性サービスとも呼ばれます。)

  前回のチェック以降に変更された項目だけでなく、すべての構成データがコピーされます。CSS は構成データを Controller 上の Microsoft SQL Server Express LocalDB データベースにインポートします。このデータベースはローカルホストキャッシュデータベースと呼ばれます。CSS は、ローカルホストキャッシュデータベースの情報がサイトデータベースの情報と一致することを確認します。ローカルホストキャッシュデータベースは、同期が行われるたびに再作成されます。

Microsoft SQL Server Express LocalDB (ローカルホストキャッシュデータベースで使用) は、Controller をインストールするときに自動的にインストールされます。(コマンドラインから Controller をインストールする際に、このインストールを禁止できます。) ローカルホストキャッシュデータベースは、複数の Controller 間で共有できません。ローカルホストキャッシュデータベースをバックアップする必要はありません。構成変更が検出されるたびに再作成されます。

- 前回のチェック以降に変更がない場合、データはコピーされません。

次の図は、プリンシパルブローカーがサイトデータベースとの接続を失った場合 (停止が開始された場合) の通信パスの変化を示しています。



停止中

停止が開始されると:

- セカンダリブローカーは接続要求のリッスンと処理を開始します。
- 停止が開始されると、セカンダリブローカーは最新の VDA 登録データを持っていませんが、VDA がセカンダリブローカーと通信すると、登録プロセスがトリガーされます。そのプロセス中に、セカンダリブローカーはその VDA に関する現在のセッション情報も取得します。
- セカンダリブローカーが接続を処理している間、ブローカリングプリンシパルは接続を監視し続けます。接続が復元されると、ブローカリングプリンシパルはセカンダリブローカーに接続情報のリッスンを停止するよう指示し、ブローカリングプリンシパルはブローカリング操作を再開します。次に VDA がブローカリングプリンシパルと通信するときに、登録プロセスがト

リガーされます。セカンダリブローカーは、以前の停止からの残りの VDA 登録をすべて削除します。CSS は、展開で構成変更が発生したことを認識すると、情報の同期を再開します。

同期中に停止が開始されるという万が一の事態が発生した場合、現在のインポートは破棄され、最後に認識された構成が使用されます。

イベントログ には、同期と停止に関する情報が提供されます。

停止モードでの運用に時間制限はありません。

通常モードと停止モード間の移行は、既存のセッションには影響しません。新しいセッションの起動のみに影響します。

意図的に停止をトリガーすることもできます。その理由と方法の詳細については、Force an outageを参照してください。

複数のControllerがあるサイト

CSSは、他のタスクの中でも、ゾーン内のすべてのControllerに関する情報をセカンダリブローカーに定期的に提供します。(展開に複数のゾーンが含まれていない場合、このアクションはサイト内のすべてのControllerに影響します。)その情報を持つことで、各セカンダリブローカーは、ゾーン内の他のControllerで実行されているすべてのピアセカンダリブローカーについて認識します。

セカンダリブローカーは、別のチャネルで相互に通信します。これらのブローカーは、停止が発生した場合にゾーン内でブローカー操作を行うセカンダリブローカーを決定（選出）するために、実行されているマシンのFQDN名のアルファベット順リストを使用します。停止中、すべてのVDAは選出されたセカンダリブローカーに登録します。ゾーン内の選出されていないセカンダリブローカーは、受信接続およびVDA登録要求を積極的に拒否します。

停止中に選出されたセカンダリブローカーが失敗した場合、別のセカンダリブローカーが引き継ぐために選出され、VDAは新しく選出されたセカンダリブローカーに登録します。

停止中にControllerが再起動された場合：

- そのControllerが選出されたブローカーでない場合、再起動による影響はありません。
- そのControllerが選出されたブローカーである場合、別のControllerが選出され、VDAが登録されます。再起動されたControllerが起動すると、自動的にブローカー処理を引き継ぎ、VDAが再度登録されます。このシナリオでは、登録中にパフォーマンスが影響を受ける可能性があります。

通常の操作中にControllerの電源をオフにし、停止中に電源をオンにした場合、そのControllerがブローカーとして選出されても、そのControllerではローカルホストキャッシュを使用できません。

イベントログは、選出に関する情報を提供します。

停止中に利用できないもの、およびその他の違い

停止モードでの運用に時間制限はありません。ただし、Citrixは可能な限り迅速に接続を復元することを推奨しています。

停止中：

- Studioを使用できません。
- PowerShell SDKへのアクセスは制限されます。
    - まず、次の操作を行う必要があります。
        - 値が1のレジストリキー `EnableCssTestMode` を追加します: `New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTestMode -PropertyType DWORD -Value 1`
        - ポート89を使用します: `Get-BrokerMachine -AdminAddress localhost:89 | Select MachineName, ControllerDNSName, DesktopGroupName, RegistrationState`
    - これらのコマンドを実行すると、以下にアクセスできます。
        - すべての `Get-Broker*` コマンドレット。
- ハイパーバイザーの資格情報はホストサービスから取得できません。すべてのマシンは不明な電源状態になり、電源操作は発行できません。ただし、電源がオンになっているホスト上のVMは、接続要求に使用できます。
- 割り当てられたマシンは、通常の操作中に割り当てが行われた場合にのみ使用できます。停止中は新しい割り当てを行うことはできません。
- リモートPCアクセス マシンの自動登録と構成はできません。ただし、通常の操作中に登録および構成されたマシンは使用できます。
- サーバーでホストされているアプリケーションおよびデスクトップのユーザーは、リソースが異なるゾーンにある場合、構成されているセッション制限よりも多くのセッションを使用する可能性があります。
- ユーザーは、現在アクティブ/選出されているセカンダリブローカーを含むゾーン内の登録済みVDAからのみアプリケーションとデスクトップを起動できます。停止中は、ゾーンをまたいだ

起動（あるゾーンのセカンダリブローカーから別のゾーンのVDAへの起動）はサポートされません。

- デリバリーグループ内のVDAのスケジュールされた再起動が開始される前にサイトデータベースの停止が発生した場合、再起動は停止が終了したときに開始されます。これにより、予期しない結果が生じる可能性があります。詳しくは、「データベースの停止によりスケジュールされた再起動が遅延する」を参照してください。
- ゾーン優先度 は構成できません。構成されている場合でも、セッション起動時には優先度は考慮されません。
- タグがゾーンの指定に使用されるタグ制限 は、セッション起動ではサポートされません。このようなタグ制限が構成され、StoreFrontストアの高度なヘルスチェック オプションが有効になっている場合、セッションの起動が断続的に失敗する可能性があります。

アプリケーションとデスクトップのサポート

LHCは、次の種類のVDAと配信モデルをサポートしています。

VDAタイプ	配信モデル	LHCイベント中のVDAの可用性
マルチセッションOS	アプリケーションとデスクトップ	常に利用可能。
シングルセッションOS静的（割り当て済み）	デスクトップ	常に利用可能。
電源管理されたシングルセッションOSランダム（プール）	デスクトップ	デフォルトでは利用できません。プールされたデリバリーグループ内の電源管理されたVDAへのすべてのセッション起動試行は、デフォルトで失敗します。LHCイベント中に新しい接続で利用できるようにすることができます。詳細については、Web Studio を使用して

VDAタイプ	配信モデル	LHCイベント中のVDAの可用性	
		有効にする および PowerShell を使用して有効にする を参照してください。 **重要：** 電源管理されたシングルセッションのプールされたマシンへのアクセスを有効にすると、以前のユーザーセッションからのデータと変更が後続のセッションに存在する可能性があります。	

注:

プールされたデリバリーグループで電源管理されたデスクトップVDAへのアクセスを有効にしても、通常の操作中に構成された `ShutdownDesktopsAfterUse` プロパティの動作には影響しません。LHC中にこれらのデスクトップへのアクセスが有効になっている場合、LHCイベント完了後にVDAは自動的に再起動しません。プールされたデリバリーグループの電源管理されたデスクトップVDAは、VDAが再起動するまで、以前のセッションのデータを保持できます。VDAの再起動は、LHC以外の操作中にユーザーがVDAからログオフしたとき、または管理者がVDAを再起動したときに発生する可能性があります。

Web Studio を使用して、電源管理されたシングルセッションOSプールVDAのLHCを有効にする

Web Studio を使用して、デリバリーグループごとにLHCイベント中にこれらのマシンを新しい接続で利用できるようにすることができます。

- デリバリーグループの作成中にこの機能を有効にするには、デリバリーグループの作成を参照してください。

- 既存のデリバリーグループでこの機能を有効にするには、「デリバリーグループの管理」を参照してください。

注:

この設定は、電源管理されたVDAを提供するプールされたデスクトップデリバリーグループの場合にのみ、Web Studio で利用できます。

PowerShellを使用して、電源管理されたシングルセッションOSのプールされたVDAに対してLHCを有効にする

特定のデリバリーグループ内のVDAに対してLHCを有効にするには、次の手順に従います。

1. このコマンドを実行して、サイトレベルでこの機能を有効にします。

   ```
   Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
   ```

2. デリバリーグループ名を指定してこのコマンドを実行し、デリバリーグループのLHCを有効にします。

   ```
   Set-BrokerDesktopGroup -Name "name" -ReuseMachinesWithoutShutdownInOutage $true
   ```

新しく作成された電源管理VDAを持つプール型デリバリーグループのデフォルトのLHC可用性を変更するには、次のコマンドを実行します。

```
Set-BrokerSite -DefaultReuseMachinesWithoutShutdownInOutage $true
```

RAM サイズに関する考慮事項

LocalDBサービスは、約1.2 GBのRAM（データベースキャッシュに最大1 GB、SQL Server Express LocalDBの実行に200 MB）を使用できます。障害が長期間続き、多くのログオンが発生する場合（たとえば、10,000ユーザーで12時間）、セカンダリブローカーは最大1 GBのRAMを使用できます。これらのメモリ要件は、コントローラーの通常のRAM要件に追加されるため、合計RAM容量を増やす必要がある場合があります。

サイトデータベースにSQL Server Expressインストールを使用している場合、サーバーには2つのsqlserver.exeプロセスがあります。

CPU コアとソケット構成に関する考慮事項

コントローラーのCPU構成、特にSQL Server Express LocalDBで利用可能なコア数は、メモリ割り当てよりもさらに、ローカルホストキャッシュのパフォーマンスに直接影響します。このCPUオーバーヘッドは、データベースに到達できず、セカンダリブローカーがアクティブな障害期間中にのみ観測されます。

LocalDBは複数のコア（最大4つ）を使用できますが、単一のソケットに制限されています。ソケットを追加してもパフォーマンスは向上しません（たとえば、1コアずつ4つのソケットがある場合）。代わりに、Citrixは複数のコアを持つ複数のソケットを使用することを推奨しています。Citrixのテストでは、2x3（2ソケット、3コア）構成は4x1および6x1構成よりも優れたパフォーマンスを提供しました。

ストレージに関する考慮事項

障害中にユーザーがリソースにアクセスすると、LocalDBは増大します。たとえば、1秒あたり10ログオンで実行されるログオン/ログオフテスト中に、データベースは2〜3分ごとに1 MB増加しました。通常の操作が再開されると、ローカルデータベースが再作成され、スペースが返されます。ただし、障害中のデータベースの増大を許容するために、LocalDBがインストールされているドライブに十分なスペースが利用可能である必要があります。ローカルホストキャッシュは、障害中により多くのI/Oも発生させます。約3 MB/秒の書き込みと、数十万回の読み取りです。

パフォーマンスに関する考慮事項

障害発生時には、1つのセカンダリブローカーがすべての接続を処理するため、通常の操作中に複数のコントローラー間で負荷分散を行うサイト（またはゾーン）では、選出されたセカンダリブローカーが障害発生時に通常よりもはるかに多くの要求を処理する必要がある場合があります。したがって、CPUの要求は高くなります。サイト（ゾーン）内のすべてのセカンダリブローカーは、ローカルホストキャッシュデータベースと影響を受けるすべてのVDAによって課される追加の負荷を処理できる必要があります。これは、障害発生時に選出されるセカンダリブローカーが変更される可能性があるためです。

VDIの制限:

- シングルゾーンVDI展開では、障害発生時に最大10,000台のVDAを効果的に処理できます。
- マルチゾーンVDI展開では、停止中に各ゾーンで最大10,000のVDA、サイト全体で最大40,000のVDAを効果的に処理できます。例えば、以下の各サイトは停止中に効果的に処理できます。
    - 4つのゾーンを持ち、各ゾーンに10,000のVDAを含むサイト。
    - 7つのゾーンを持ち、1つは10,000のVDAを含み、残りの6つはそれぞれ5,000のVDAを含むサイト。

停止中、サイト内の負荷管理が影響を受ける可能性があります。負荷評価器（特にセッション数ルール）が超過する可能性があります。

すべてのVDAがセカンダリブローカーに登録するのにかかる間、そのサービスは現在のセッションに関する完全な情報を持っていない可能性があります。そのため、その期間中のユーザー接続要求は、既存のセッションへの再接続が可能であったとしても、新しいセッションが起動される結果となる可能性があります。この期間（「新しい」セカンダリブローカーが再登録中にすべてのVDAからセッション情報を取得する間）は避けられません。停止が開始されたときに接続されているセッションは移行期間中に影響を受けませんが、新しいセッションやセッションの再接続は影響を受ける可能性があります。

この期間は、VDAが登録する必要がある場合に発生します。

- 停止が開始されたとき: プリンシパルブローカーからセカンダリブローカーに移行するとき。
- 停止中のセカンダリブローカーの障害: 障害が発生したセカンダリブローカーから新しく選出されたセカンダリブローカーに移行するとき。
- 停止からの復旧: 通常の操作が再開され、プリンシパルブローカーが制御を再開するとき。

Citrix Broker Protocolの`HeartbeatPeriodMs`レジストリ値（デフォルト = 600000 ms、つまり10分）を下げることで、間隔を短縮できます。このハートビート値は、VDAがpingに使用する間隔の2倍であるため、デフォルト値では5分ごとにpingが実行されます。

例えば、次のコマンドはハートビートを5分（300000ミリ秒）に変更し、2.5分ごとにpingが実行されるようにします。

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer -Name HeartbeatPeriodMs -PropertyType DWORD –Value 300000
```

ハートビート値を変更する際は注意してください。頻度を上げると、通常モードと停止モードの両方でControllerへの負荷が増大します。

VDAがどれだけ迅速に登録されても、この間隔を完全に排除することはできません。

セカンダリブローカー間の同期にかかる時間は、オブジェクト（VDA、アプリケーション、グループなど）の数が増えるにつれて長くなります。例えば、5000のVDAを同期するには10分以上かかる場合があります。

XenApp 6.xリリースとの違い

このローカルホストキャッシュの実装は、XenApp 6.xおよびそれ以前のXenAppリリースにおけるローカルホストキャッシュ機能と同じ名前を共有していますが、大幅な改善が施されています。この実装は、より堅牢で破損の影響を受けません。定期的な`dsmaint`コマンドの必要性を排除する

など、メンテナンス要件が最小限に抑えられています。このローカルホストキャッシュは、技術的には全く異なる実装です。

ローカルホストキャッシュの管理

ローカルホストキャッシュが正しく機能するには、各ControllerのPowerShell実行ポリシーをRemoteSigned、Unrestricted、またはBypassに設定する必要があります。

SQL Server エクスプレス ローカルDB

ローカルホストキャッシュが使用するMicrosoft SQL Server Express LocalDBソフトウェアは、Controllerをインストールするか、バージョン7.9より前のControllerをアップグレードする際に自動的にインストールされます。このデータベースと通信するのはセカンダリブローカーのみです。PowerShellコマンドレットを使用して、このデータベースに関する何かを変更することはできません。LocalDBは複数のController間で共有できません。

SQL Server Express LocalDBデータベースソフトウェアは、ローカルホストキャッシュが有効になっているかどうかにかかわらずインストールされます。

そのインストールを防ぐには、`XenDesktopServerSetup.exe`コマンドを使用してControllerをインストールまたはアップグレードし、`/exclude "Local Host Cache Storage (LocalDB)"`オプションを含めます。ただし、ローカルホストキャッシュ機能はデータベースなしでは機能せず、セカンダリブローカーで別のデータベースを使用することはできないことに注意してください。

このLocalDBデータベースのインストールは、サイトデータベースとして使用するためにSQL Server Expressをインストールするかどうかには影響しません。

以前のSQL Server Express LocalDBバージョンを新しいバージョンに置き換える方法については、「Replace SQL Server Express LocalDB」を参照してください。

製品のインストールとアップグレード後のデフォルト設定

Citrix Virtual Apps and Desktopsの新規インストール時（最小バージョン7.16）には、ローカルホストキャッシュが有効になります。

アップグレード後（バージョン7.16以降）は、展開全体で10,000未満のVDAがある場合、ローカルホストキャッシュが有効になります。

ローカルホストキャッシュの有効化と無効化

- ローカルホストキャッシュを有効にするには、次のように入力します。

```
Set-BrokerSite -LocalHostCacheEnabled $true
```

ローカルホストキャッシュが有効になっているかどうかを確認するには、`Get-BrokerSite` と入力します。`LocalHostCacheEnabled` プロパティが `True` であることを確認します。

- ローカルホストキャッシュを無効にするには、次のように入力します。

```
Set-BrokerSite -LocalHostCacheEnabled $false
```

注意: XenAppおよびXenDesktop 7.16以降、接続リース（バージョン7.6からローカルホストキャッシュに先行していた機能）は製品から削除され、利用できなくなりました。

ローカルホストキャッシュが機能していることを確認する

ローカルホストキャッシュが正しく設定され、機能していることを確認するには：

- 同期インポートが正常に完了していることを確認します。イベントログを確認してください。
- 各Delivery ControllerにSQL Server Express LocalDBデータベースが作成されていることを確認します。これにより、必要に応じてセカンダリブローカーが引き継ぐことができることが確認されます。
  - Delivery Controllerサーバーで、`C:\Windows\ServiceProfiles\NetworkService` を参照します。
  - `HaDatabaseName.mdf` と `HaDatabaseName_log.ldf` が作成されていることを確認します。
- Delivery Controllerで障害を強制的に発生させます。ローカルホストキャッシュが機能することを確認したら、すべてのControllerを通常モードに戻すことを忘れないでください。これには約15分かかる場合があります。

イベントログ

イベントログは、同期と障害が発生した時期を示します。イベントビューアログでは、障害モードは*HA モード*と呼ばれます*。

構成同期サービス:

通常の操作中、CSSがローカルホストキャッシュブローカーを使用して構成データをローカルホストキャッシュデータベースにインポートする際に、次のイベントが発生する可能性があります。

- 503: Citrix Config Sync Serviceが更新された構成を受信しました。このイベントは、同期プロセスの開始を示します。
- 504: Citrix Config Sync Serviceが更新された構成をインポートしました。構成のインポートが正常に完了しました。

- 505: Citrix Config Sync Serviceがインポートに失敗しました。構成のインポートは正常に完了しませんでした。以前に正常な構成が利用可能な場合、障害発生時にそれが使用されます。ただし、それは現在の構成から古くなっています。以前の構成が利用できない場合、サービスは障害発生時にセッションブローカーに参加できません。この場合、トラブルシューティングセクションを参照し、Citrixサポートに連絡してください。
- 507: システムが障害モードであり、ローカルホストキャッシュブローカーがブローカー処理に使用されているため、Citrix Config Sync Serviceがインポートを中止しました。サービスは新しい構成を受信しましたが、障害が発生したためインポートは中止されました。これは予期される動作です。
- 510: プライマリ構成サービスから構成サービス構成データが受信されませんでした。
- 517: プライマリブローカーとの通信中に問題が発生しました。
- 518: セカンダリブローカー（高可用性サービス）が実行されていないため、構成同期スクリプトが中止されました。

高可用性サービス:

このサービスは、ローカルホストキャッシュブローカーとも呼ばれます。

- 3502: 停止が発生し、ローカルホストキャッシュブローカーがブローカー操作を実行しています。
- 3503: 停止が解決され、通常の操作が再開されました。
- 3504: どのローカルホストキャッシュブローカーが選出されたか、および選出に関与した他のローカルホストキャッシュブローカーを示します。
- 3507: 2分ごとにローカルホストキャッシュのステータス更新を提供し、選出されたブローカーでローカルホストキャッシュモードがアクティブであることを示します。停止期間、VDA登録、セッション情報を含む停止の概要が含まれます。
- 3508: 選出されたブローカーでローカルホストキャッシュがアクティブでなくなり、通常の操作が復元されたことを通知します。停止期間、ローカルホストキャッシュイベント中に登録されたマシンの数、LHCイベント中の正常な起動の数を含む停止の概要が含まれます。
- 3509: 選出されていないブローカーでローカルホストキャッシュがアクティブであることを通知します。2分ごとの停止期間が含まれ、選出されたブローカーを示します。
- 3510: 選出されていないブローカーでローカルホストキャッシュがアクティブでなくなったことを通知します。停止期間が含まれ、選出されたブローカーを示します。

停止を強制する

意図的に停止を強制したい場合があります。

- ネットワークが繰り返しダウンする場合。ネットワークの問題が解決されるまで停止を強制すると、通常モードと停止モード間の継続的な移行（およびその結果として頻繁に発生するVDA登録ストーム）を防ぐことができます。
- ディザスタリカバリ計画をテストするため。
- ローカルホストキャッシュが正しく機能していることを確認するため。
- サイトデータベースサーバーの交換または保守中。

停止を強制するには、Delivery Controller を含む各サーバーのレジストリを編集します。`HKLM\Software\Citrix\DesktopServer\LHC`で、`OutageModeForced`を`REG_DWORD`として`1`に作成して設定します。この設定により、データベースの状態に関係なく、ローカルホストキャッシュブローカーは停止モードに入ります。値を`0`に設定すると、ローカルホストキャッシュブローカーは停止モードを終了します。

イベントを確認するには、`C:\ProgramData\Citrix\WorkspaceCloud\Logs\Plugins\HighAvailabilityService`にある`Current_HighAvailabilityService`ログファイルを監視します。

トラブルシューティング

ローカルホストキャッシュデータベースへの同期インポートが失敗し、505イベントが投稿された場合、いくつかのトラブルシューティングツールが利用可能です。

CDFトレース: `ConfigSyncServer`および`BrokerLHC`モジュールのオプションが含まれています。これらのオプションは、他のブローカーモジュールとともに、問題を特定するのに役立つでしょう。

レポート: 同期インポートが失敗した場合、レポートを生成できます。このレポートは、エラーの原因となっているオブジェクトで停止します。このレポート機能は同期速度に影響するため、Citrixは使用しないときは無効にすることを推奨します。

CSSトレースレポートを有効にして生成するには、次のコマンドを入力します。

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -PropertyType DWORD -Value 1
```

HTMLレポートは`C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\CitrixBrokerConfigSyncReport.htm`に投稿されます。

レポートが生成されたら、レポート機能を無効にするには次のコマンドを入力します。

`Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -Value 0`

ブローカー構成のエクスポート: デバッグ目的で正確な構成を提供します。

`Export-BrokerConfiguration | Out-File <file-pathname>`

例: `Export-BrokerConfiguration | Out-File C:\\BrokerConfig.xml`。

ローカルホストキャッシュのPowerShellコマンド

PowerShellコマンドを使用して、Delivery Controllerでローカルホストキャッシュ（LHC）を管理できます。

PowerShellモジュールは、Delivery Controllerの次の場所にあります。

`C:\Program Files\Citrix\Broker\Service\ControlScripts`

> **重要:**
>
> このモジュールはDelivery Controllerでのみ実行してください。

PowerShell モジュールのインポート

モジュールをインポートするには、Delivery Controllerで次を実行します。

`cd C:\Program Files\Citrix\Broker\Service\ControlScripts Import-Module .\HighAvailabilityServiceControl.psm1`

LHC を管理するための PowerShell コマンド

以下のコマンドは、Delivery Controller で LHC モードをアクティブ化および管理するのに役立ちます。

コマンドレット	機能
`Enable-LhcForcedOutageMode`	ブローカーを LHC モードにします。`Enable-LhcForcedOutageMode` が適切に機能するには、ConfigSync Service によって LHC データベースファイルが正常に作成されている必要があります。この cmdlet は、実行された Delivery Controller 上でのみ LHC を強制します。LHC をアクティブにするには、こ

コマンドレット	機能
	のコマンドをゾーン内のすべての Delivery Controller で実行する必要があります。
`Disable-LhcForcedOutageMode`	ブローカーを LHC モードから解除します。この cmdlet は、実行された Delivery Controller 上でのみ LHC モードを無効にします。`Disable-LhcForcedOutageMode` は、ゾーン内のすべての Delivery Controller で実行する必要があります。
`Set-LhcConfigSyncIntervalOverride`	Citrix Config Synchronizer Service (CSS) がサイト内の構成変更をチェックする間隔を設定します。時間間隔は、60 秒 (1 分) から 3600 秒 (1 時間) の範囲で指定できます。この設定は、実行された Delivery Controller にのみ適用されます。Delivery Controller 間で一貫性を持たせるには、各 Delivery Controller でこの cmdlet を実行することを検討してください。例: `Set-LhcConfigSyncIntervalOverride -Seconds 1200`
`Clear-LhcConfigSyncIntervalOverride`	Citrix Config Synchronizer Service (CSS) がサイト内の構成変更をチェックする間隔を、デフォルト値の 300 秒 (5 分) に設定します。この設定は、実行された Delivery Controller にのみ適用されます。Delivery Controller 間で一貫性を持たせるには、各 Delivery Controller でこの cmdlet を実行することを検討してください。
`Enable-LhcHighAvailabilitySDK`	実行された Delivery Controller 内のすべての `Get-Broker*` cmdlet へのアクセスを有効にします。
`Disable-LhcHighAvailabilitySDK`	実行された Delivery Controller 内の Broker cmdlet へのアクセスを無効にします。

注:

- Delivery Controller で `Get-Broker*` cmdlet を実行するときは、ポート 89 を使用します。例:
  - `Get-BrokerMachine -AdminAddress localhost:89`
- LHC モードでない場合、Delivery Controller 上の LHC Broker は構成情報のみを保持します。
- LHC モード中、選出された Delivery Controller 上の LHC Broker は次の情報を保持します。
  - リソースの状態
  - セッションの詳細
  - VDA登録
  - 構成情報

マシンとセッション (Search > デフォルトビュー)

注:

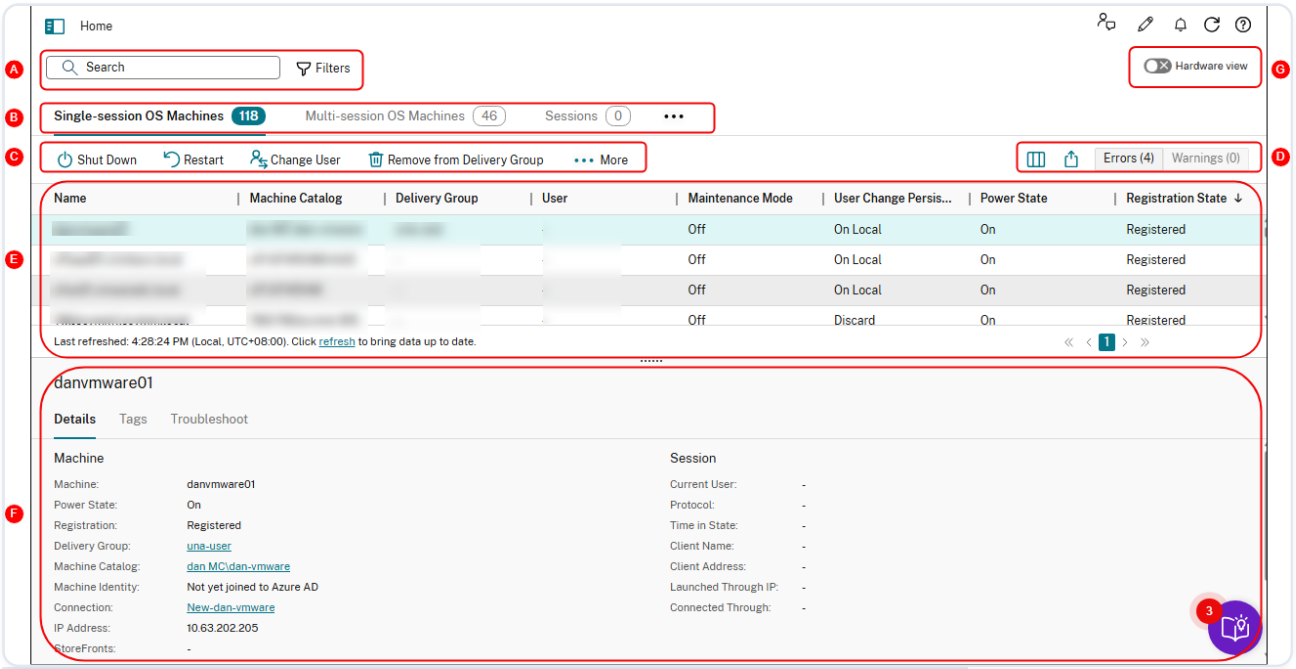
バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

この記事では、**検索**ノード内のデフォルトビューを使用してマシンとセッションを監視および管理する方法について説明します。以下のトピックが含まれています。

- デフォルトビューについて学ぶ
- マシンとセッションを検索する
- 表示する列をカスタマイズする
- マシンとセッションを管理する
- マシンまたはセッションデータをCSVファイルにエクスポートする

デフォルトビューについて

検索ノード内のデフォルトビューは、マシンとユーザーセッションを監視および管理するための一元的な場所を提供します。



コールアウト	エリア	説明
A	検索バー	複雑な検索条件を定義できるクイック検索とフィルターベースの検索を提供します。詳細については、「インスタンスの検索」を参照してください。
B	タイプタブ	マシンをタイプ別に一覧表示したり、すべてのセッションを一覧表示したりするためのタブを表示します。インスタンス数はタブ名に表示されます。
C	インスタンスレベルのアクション	*選択したインスタンス*（マシンまたはセッション）に対して実行できるアク

コールアウト	エリア	説明
		ションを表示します。詳細については、マシンアクションおよびセッションアクションを参照してください。
D	リストレベルのアクション	現在の*リスト*に対して実行できるアクションを表示します。 • **エクスポート**アイコン: メインビューに表示されているインスタンスのリストをCSVファイルにエクスポートします。 • 「**表示する列**」アイコン: リストのメインビューをカスタマイズします。 • **エラー**ラベル: このラベルを有効にすると、メインビューにエラーのある未登録のマシンのみが表示されます。問題の詳細を表示するには、**詳細**ペインの**トラブル**

コールアウト	エリア	説明
		シューティングタブに移動します。 • **警告**ラベル: このラベルを有効にすると、メインビューに警告のある未登録のマシンのみが表示されます。問題の詳細を表示するには、**詳細**ペインの**トラブルシューティング**タブに移動します。
E	メインビュー	インスタンスとそのプロパティを表示します。**表示する列**アイコンを選択して、メインビューをカスタマイズできます。利用可能な列の詳細については、マシン列およびセッション列を参照してください。
F	詳細ペイン	次の詳細が表示されます: • 選択したインスタンス（マシンまたはセッション）の詳細

コールアウト	エリア	説明
		• 選択したマシンに適用されているタグ • 選択したマシンに関するエラーまたは警告の詳細。問題、考えられる原因、推奨される解決策が含まれます。
G	ハードウェアビューに切り替える	デフォルトビューからハードウェアビューに切り替えるには、クリックします。

インスタンスの検索

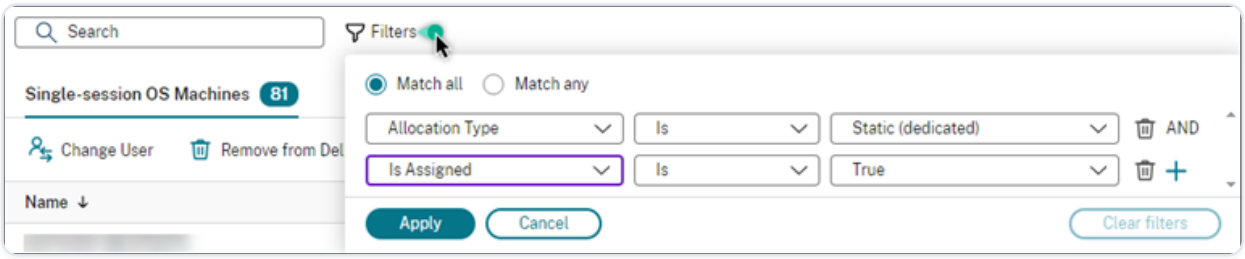
検索機能を使用して、特定のマシンとセッションを見つけます。

- フィルターを使用した検索
- クイック検索のために現在のフィルターセットを保存する
- 検索バーにフィルターフィールドをピン留めする
- クイック検索ボックスを使用して検索
- 検索を強化するためのヒント

フィルターを使用した検索

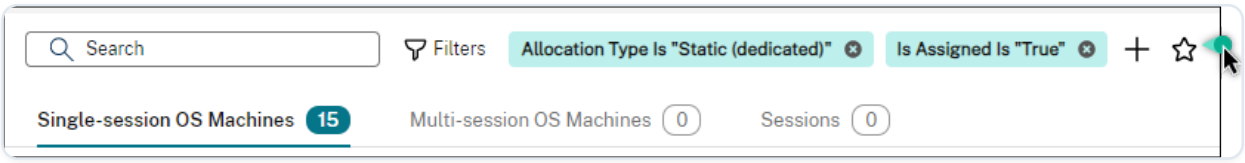
たとえば、*静的でユーザーに割り当てられている*すべてのシングルセッションOSマシンを見つけるには、次の手順に従います。

1. **シングルセッションOSマシン**タブで、**フィルター**アイコンをクリックします。フィルターパネルが表示されます。
2. 必要なフィルター条件を追加します。



3. すべてのフィルター条件に一致する結果を検索で返す場合は、**すべて一致**（AND演算子）を選択します。いずれかのフィルター条件に一致する結果を検索で返す場合は、**いずれか一致**（OR演算子）を選択します。
4. **適用**をクリックします。

   フィルターされたリストには、静的でユーザーに割り当てられているすべてのシングルセッションOSマシンが表示されます。



クイック検索のために現在のフィルターセットを保存する

たとえば、静的でユーザーに割り当てられているシングルセッションOSマシンのフィルターセットを将来使用するために保存するには、次の手順に従います。

1. フィルターベースの検索を実行した後、前の図に示すように、検索バーの**星**アイコンをクリックします。
2. 表示されるページで、このフィルターセットの名前を入力します（例：*静的および割り当て済みマシン*）。
3. 「**保存**」をクリックします。

   検索ボックスをクリックすると、保存されたフィルターセットが検索履歴リストに表示されます。

   検索フィルターセット(/en-us/citrix-virtual-apps-desktops/current-release/media/search-filter-set.png)

> **注:**
>
> フィルターセットはユーザーアカウントごとに保存されます。保存されたフィルターセットを管理するには、**管理**を選択します。

検索バーにフィルターフィールドをピン留めする

頻繁に使用するフィルター*フィールド*を検索バーにピン留めすると、簡単にアクセスできます。たとえば、フィルターベースの検索を実行した後、**割り当てタイプ**を検索バーにピン留めしたいとします。次の手順に従います。

1. 検索バーの*フィルター設定*をクリックします。
2. 表示されるパネルで、検索バーにフィルターフィールド（この例では*割り当てタイプ*）をピン留めするには、**ピン**アイコンをクリックします。 検索フィルターのピン(/en-us/citrix-virtual-apps-desktops/current-release/media/search-filter-pin.png)

クイック検索ボックスを使用して検索する

クイック検索ボックスを使用すると、名前関連のプロパティまたは保存されたフィルターセットに基づいてインスタンスを検索する便利な方法が提供されます。詳細な手順は次のとおりです。

1. 検索ボックスをクリックします。最近の検索と保存されたフィルターセットがドロップダウンリストに表示されます。以前の検索またはフィルターセットをクリックして、クイック検索を実行できます。
2. 新しい検索を開始するには、次のオプションから完全または部分的な名前を入力します。

    - マシン名またはDNS名
    - マシンカタログ名
    - デリバリーグループ名
    - セッションユーザー名
    - セッションクライアント名
    - セッションをホストしているVMのフレンドリ名（ハイパーバイザーで使用されるもの）
    - ホストサーバー名

検索を強化するためのヒント

検索機能を使用する際は、以下のヒントを考慮してください。

- **検索**ノードで、任意の列を選択して項目を並べ替えます。
- 検索および並べ替えが可能な表示に含める特性を増やすには、**表示する列**を選択するか、任意の列をクリックして**表示する列**を選択します。**表示する列**ウィンドウで、表示したい項目の横にあるチェックボックスをオンにし、**保存**を選択して終了します。

> **注:**

> パフォーマンスを低下させる列には、**パフォーマンスを低下させる**というラベルが付けられています。

- マシンに接続されているユーザーデバイスを見つけるには、**クライアント (IP)** と **Is** を使用し、デバイスのIPアドレスを入力します。
- アクティブなセッションを見つけるには、**セッション状態**、**Is**、および **接続済み** を使用します。
- 配信グループ内のすべてのマシンを一覧表示するには、左ペインで**配信グループ**を選択します。グループを選択し、アクションバーまたはコンテキストメニューから**マシンの表示**を選択します。
- 特定のプロパティでMCSプロビジョニングされたマシンをすばやく絞り込むには、ハードウェアビューで利用可能な**検索**バーを使用します。

並べ替え操作を実行する際は、以下の点を考慮してください。

- 項目の数が5,000を超えない限り、任意の列をクリックして項目を並べ替えることができます。数が5,000を超えると、名前または現在のユーザー（現在表示しているタブによる）でのみ並べ替えることができます。並べ替えを有効にするには、フィルターを使用して項目の数を5,000以下に減らしてください。
- アイテム数が500より多く、5,000以下の場合:
  - ソートパフォーマンスを向上させるため、すべてのデータをローカルにキャッシュします。**シングルセッションOSマシン**タブと**マルチセッションOSマシン**タブでは、ソートのために列（**名前**列を除く任意の列）を初めてクリックしたときにデータをキャッシュします。**セッション**タブでは、ソートのために列（**現在のユーザー**列を除く任意の列）を初めてクリックしたときにデータをキャッシュします。その結果、ソートの完了に時間がかかります。パフォーマンスを向上させるには、名前または現在のユーザーでソートするか、フィルターを使用してアイテム数を減らしてください。
  - テーブルの下に表示される次のメッセージは、データがキャッシュされていることを示します: 最終更新: `<the time when you refreshed the table>`。この場合、ソート操作は以前にロードされたアイテムに基づいています。これらのアイテムは最新ではない可能性があります。最新の状態にするには、更新アイコンをクリックしてください。

表示する列をカスタマイズする

日々の運用に不可欠なプロパティとステータスを表示するパーソナライズされたメインビューを作成します。詳細な手順は次のとおりです。

1. **検索**ノードで、必要に応じて**マルチセッションOSマシン**、**シングルセッションOSマシン**、または**セッション**タブを選択します。
2. アクションバーの**表示する列**アイコンをクリックし、列を選択します。

   利用可能な列とその説明の詳細については、マシン列およびセッション列を参照してください。

列を選択する際、**パフォーマンスを低下させる**というラベルが付いた列が表示されることがあります。これらの列を選択すると、コンソールのパフォーマンスが低下する可能性があります。以下の考慮事項に留意してください:

- カスタマイズが完了すると、選択した列を表示するためにテーブルが更新されます。これらの列が存在すると、テーブルの更新時に遅延が発生する可能性があります。
- ブラウザを更新するか、コンソールからサインアウトして再度サインインすると、それらの列を保持するかどうかを尋ねるメッセージが表示されます。保持することを選択した場合、最適なコンソールパフォーマンスのために、テーブルの更新は1分間に1回までに制限されます。より頻繁に更新するには、パフォーマンスを低下させる列をすべて削除してください。

マシンとセッションの管理

検索ノードのアクションを使用して、マシンとセッションの問題をトラブルシューティングしたり、ユーザー要求を処理したりします。

知っておくとよいこと

マシンはさまざまなレベルで管理できます:

- 個々のマシンレベルで。**検索**ノードを使用して、ターゲットマシンを特定し、アクションを実行します。
- マシンカタログレベルで、カタログのマスターイメージの変更、カタログからのマシンの削除、カタログへのマシンの追加などを行います。詳細については、「マシンカタログの管理」を参照してください。
- デリバリーグループレベルで、グループ内のマシンのメンテナンスモードのオン/オフを切り替えるなどを行います。詳細については、「デリバリーグループの管理」を参照してください。

個々のセッションレベルに加えて、デリバリーグループレベルでセッションを管理することもできます。たとえば、デリバリーグループのセッションの事前起動と残存を構成できます。詳細については、「デリバリーグループの管理」を参照してください。

マシンまたはセッションでアクションを実行する

個々のインスタンスレベルでマシンまたはセッションを管理するには、次の手順に従います。

1. **検索**ノードで、**マルチセッションOSマシン**、**シングルセッションOSマシン**、または**セッション**タブを選択します。
2. 必要に応じて、1つ以上のインスタンスを選択します。
3. アクションバーまたは右クリックメニューから、それらのインスタンスで発生した問題やユーザー要求に基づいてアクションを選択します。

   利用可能なアクションとその説明の詳細については、「マシンアクション」および「セッションアクション」を参照してください。

> **注:**
>
> 2つ以上のインスタンスを選択した場合、それらすべてに適用されるアクションのみが利用可能です。

マシンまたはセッションデータをCSVファイルにエクスポートする

タブに表示されているインスタンス（マシンまたはセッション）のリスト（最大30,000項目）をCSVファイルにエクスポートします。詳細な手順は次のとおりです。

1. **検索**ノードで、必要に応じて**マルチセッションOSマシン**、**シングルセッションOSマシン**、または**セッション**タブを選択します。
2. 右上隅にある「**エクスポート**」アイコンをクリックします。
3. 表示されるダイアログボックスで、「**続行**」をクリックします。

   エクスポートが完了するまでに数分かかる場合があります。ファイルはブラウザのデフォルトのダウンロードフォルダにあります。

> **注:**
>
> **検索**ノードの各タブでは、エクスポートの実行中に別のエクスポートを実行することはできません。

マシンのアクションと列

この記事では、参照用にマシンのアクションと列を説明とともに一覧表示します。

アクション

マシンで実行できるアクションとその説明を表示します。

アクション	説明	適用対象
デリバリーグループから削除	デリバリーグループからマシンを削除します。	シングルセッションおよびマルチセッション
デリバリーグループに追加	マシンをデリバリーグループに追加します。	シングルセッションおよびマルチセッション
セッションの表示	マシンで実行中のセッションを表示します	シングルセッションおよびマルチセッション
タグの管理	マシンにタグを追加して管理します。タグの一般的な使用例について詳しくは、「タグ」を参照してください。	シングルセッションおよびマルチセッション
メンテナンスモードをオンにする	パッチを適用する前、またはトラブルシューティングのために、マシンをメンテナンスモードにします。 このモードでは、そのマシンへの新しい接続が防止されます。ユーザーはそのマシン上の既存のセッションに接続できますが、そのマシン上で新しいセッションを開始することはできません。	シングルセッションおよびマルチセッション
メンテナンスモードをオフにする	マシンのメンテナンスモードをオフにします。	シングルセッションおよびマルチセッション
VDAのアップグレード	マシンのVDAをアップグレードします。	特定の要件を満たすシングルセッションまたはマルチセッションOSマシン: 詳細はこちら。

アクション	説明	適用対象
ログオフ	マシンを強制的にログオフする	シングルセッションおよびマルチセッション
削除	マシンカタログからVMを削除しますが、ハイパーバイザーまたはクラウドサービス上ではそのまま残します。	シングルセッションおよびマルチセッション
ユーザーの変更	特定のユーザーにマシンを割り当てます。	シングルセッションの*静的*マシン。
起動	マシンを起動します。	シングルセッションおよびマルチセッション
シャットダウン	マシンをシャットダウンします。	シングルセッションおよびマルチセッション
再起動	マシンを再起動します	シングルセッションおよびマルチセッション
サスペンド	マシンを休止状態または中断状態にします。マシンを中断すると、Delivery Controllerはマシンのメモリ内容をファイルに保存し、マシンをシャットダウンします。	シングルセッションOSマシン
再開	中断されたマシンを再開します。中断されたマシンを再開すると、Delivery Controllerはマシンを起動し、以前の状態に復元します。	シングルセッションOSマシン
強制再起動	マシンを強制的に再起動します。	シングルセッションOSマシン
強制シャットダウン	マシンを強制的にシャットダウンします。	シングルセッションOSマシン

列

タイプ別にすべてのマシン列とその説明を表示します。

- マシン
- マシンの詳細
- アプリケーション
- ホスティング
- 接続
- 登録
- セッションの詳細
- セッション

マシン

マシンカテゴリの列。

列	説明	適用対象
名前	マシンのDNSホスト名。	シングルセッションおよびマルチセッション
マシンカタログ	マシンが属するカタログの名前。	シングルセッションおよびマルチセッション
デリバリーグループ	マシンが属するデリバリーグループの名前。	シングルセッションおよびマルチセッション
ユーザー表示名	マシンに関連付けられているユーザーのフルネーム（通常は `Firstname Lastname` の形式）。関連付けられているユーザーとは、共有マシンの現在のユーザーと、専用マシンに割り当てられているユーザーのことです。	シングルセッションおよびマルチセッション

列	説明	適用対象
ユーザー	マシンに関連付けられているユーザーのユーザー名（「domain\user」の形式）。関連付けられているユーザーとは、共有マシンの現在のユーザーと、専用マシンに割り当てられているユーザーのことです。	シングルセッションおよびマルチセッション
ユーザープリンシパル名	マシンに関連付けられているユーザーのユーザープリンシパル名（「user@domain」の形式）。関連付けられているユーザーとは、共有マシンの現在のユーザーと、専用マシンに割り当てられているユーザーのことです。	シングルセッションおよびマルチセッション
デスクトップ表示名	セッションの起動に元々使用されたマシンの公開名。Citrix Workspace™ アプリまたはStoreFrontに表示される名前です。	シングルセッションのみ
	注：デスクトップの表示を変更するには、**マシンの更新を実行**権限が必要です。表示名の変更にはマシンプロパティ	

列	説明	適用対象
	の更新が含まれるためです。	
デスクトップの状態	マシンに対する未解決のデスクトップ状態のリスト。可能な値：Unknown、CPU、ICALatency、および UPMLogonTime。	シングルセッションおよびマルチセッション
割り当ての種類	マシンの割り当ての種類：ユーザーに永続的に割り当てられる場合は**永続**。ランダムに割り当てられる場合は**ランダム**。	シングルセッションおよびマルチセッション
メンテナンスモード	マシンがメンテナンスモードであるかどうかを示します。	シングルセッションおよびマルチセッション
Windows接続設定	Windowsによって報告されるログオンモード。	マルチセッションのみ
	指定可能な値: LogonEnabled、Draining、DrainingUntilRestart、および LogonDisabled。	
割り当て済み	専用デスクトップがユーザーまたはクライアント (名前/アドレス) に割り当てられているかどうかを示します。ユーザーは明示的に割り当てることも、マシンの初回使用時に割り当	シングルセッションおよびマルチセッション

列	説明	適用対象
	てることもできます。	
物理マシン	マシンが物理マシンであるかどうかを示します。`True` はマシンが物理マシンであることを示し、Delivery Controller によって電源管理されていないことを意味します。`False` はそうでないことを示します。	シングルセッションおよびマルチセッション
プロビジョニングの種類	マシンがどのようにプロビジョニングされたか。指定可能な値 • 手動: PVSまたはMCSを使用してプロビジョニングされていません。 • PVS: PVSを使用してプロビジョニング済み (物理マシン、ブレードマシン、仮想マシン) • MCS: MCSを使用してプロビジョニング済み (VMのみ)	シングルセッションおよびマルチセッション

列	説明	適用対象	
スケジュールされた再起動	マシンに対してスケジュールされた再起動操作の状態。指定可能な値 • なし: 再起動はスケジュールされていません。 • 保留中: 再起動を待機中ですが、使用可能です。 • ドレイン中: 再起動を待機しており、新しいセッションには利用できません。ただし、既存の接続への再接続は引き続き許可されます。 • 進行中: スケジュールされた再起動がアクティブに進行中です。 • 自然: 自然な再起動が進行中です。マシンは再起動を待機しています。	シングルセッションおよびマルチセッション	

列	説明	適用対象
ゾーン	マシンが配置されているゾーンの名前。	シングルセッションおよびマルチセッション
状態	マシンに関連付けられているデスクトップの全体的な状態。これは、セッション状態、登録状態、電源状態など、さまざまな特定の状態から派生しています。	シングルセッションおよびマルチセッション
	可能な状態: オフ、未登録、利用可能、切断済み、使用中、準備中。	
タグ	マシンに関連付けられているタグのリスト。	シングルセッションおよびマルチセッション
VDAアップグレード	VDAパッケージのアップグレードアクションのマシン状態。	シングルセッションおよびマルチセッション
	指定可能な値: MissingUpgradeType、UpgradeScheduled、UpgradeAvailable、UpToDate、および Unknown。	
サスペンド可能	マシンが電源操作 (サスペンドと再開) をサポートしているかどうかを示します。	シングルセッションおよびマルチセッション

列	説明	適用対象
ロード評価インデックス	マシンの全体的な実効負荷インデックス（パーセンテージ）。詳細については、CTX202150 を参照してください。	マルチセッションのみ
ロードインデックス	現在のロードインデックス。詳細については、詳細はこちらを参照してください。	マルチセッションのみ
ドレイン状態	マシンがドレイン中であり、マシン上のすべてのセッションが終了した後にシャットダウンするかどうかを示します。True は、電源管理されたマルチセッションマシンでのみ表示されます。	マルチセッションのみ
	注: マシンがメンテナンスモードの場合、シャットダウンしません。メンテナンスモードを解除した後にのみシャットダウンします。	

マシンの詳細

マシンの詳細カテゴリの列。

列	説明	適用対象
エージェントバージョン	マシンにインストールされているCitrix Virtual Delivery Agent (VDA) のバージョン。	シングルセッションおよびマルチセッション

列	説明	適用対象
IPアドレス	マシンのIPアドレスです。	シングルセッションおよびマルチセッション
割り当て済み	専用デスクトップがユーザーまたはクライアント（名前/アドレス）に割り当てられているかどうかを示します。ユーザーは明示的に割り当てることも、マシンの初回使用時に割り当てることもできます。	シングルセッションおよびマルチセッション
OSの種類	マシンで実行されているオペレーティングシステムの種類です。	シングルセッションのみ

アプリケーション

アプリケーションカテゴリの列。

列	説明	適用対象
使用中のアプリケーション	マシンで使用中のアプリケーションのリスト（ブラウザ名として表示されます）。	シングルセッションおよびマルチセッション
公開アプリケーション	マシンによって公開されたアプリケーションのリスト（ブラウザ名として表示されます）。	シングルセッションおよびマルチセッション

接続

接続カテゴリの列。

列	説明	適用対象
クライアント (IP)	マシンに接続されているクライアントのIPアドレス。	シングルセッションのみ
クライアント	マシンに接続されているクライアントのホスト名。	シングルセッションのみ

列	説明	適用対象
プラグインバージョン	接続されているクライアント上のCitrix Workspaceアプリのバージョン。	シングルセッションのみ
接続元	受信接続のホスト名。通常、ゲートウェイ、ルーター、またはクライアントです。	シングルセッションのみ
接続元 (IP)	受信接続のIPアドレス。通常、ゲートウェイ、ルーター、またはクライアントです。	シングルセッションのみ
接続タイプ	セッションに使用されるプロトコル。可能な値：HDX、RDP、およびConsole。注：XenDesktop® 5 VDA上のコンソールセッションの場合、このフィールドは空白になります。	シングルセッションのみ
最終接続時刻 (UTC)	失敗または成功した、最後に検出された接続試行の時刻。	シングルセッションおよびマルチセッション
最終接続ユーザー	最後にマシンへの接続を試行したユーザーのSAM名（「DOMAIN\user」の形式）。SAM名が利用できない場合は、SIDが使用されます。	シングルセッションおよびマルチセッション
Secure ICA® アクティブ	現在のセッションでSecureICAがアクティブであるかどうかを示します。マルチセッションマシンでは常にnullです。	シングルセッションおよびマルチセッション

ホスティング

ホスティングカテゴリの列。

列	説明	適用対象
VM	セッションを実行しているホストされたマシンの、ハイパーバイザーによって使用されるフレンドリ名。マシンのDNS名またはAD名のいずれとも一致するとは限りません。	シングルセッションおよびマルチセッション
ホスティングサーバー名	管理対象の場合、マシンをホストしているハイパーバイザーのDNS名。	シングルセッションおよびマルチセッション
接続	セッションをホストしているマシンに割り当てられているホスト接続の名前。	シングルセッションおよびマルチセッション
保留中の更新	ホストされているマシンのVMイメージが古くなっており、次回の再起動時に新しいイメージに更新される必要があるかどうかを示します。	シングルセッションおよびマルチセッション
ユーザー変更の永続性	ユーザーの変更がどのように処理されるかを示し、変更が永続的であるかどうかを示します: • OnLocal: 永続的。ユーザーの変更はローカルに保存されます。	シングルセッションおよびマルチセッション

列	説明	適用対象	
	• 破棄: 非永続的。ユーザーの変更は破棄されます。		
保留中の電源操作	マシンに対して保留中の電源操作があるかどうかを示します。	シングルセッションおよびマルチセッション	
電源状態	マシンの電源状態。設定可能な値: 管理対象外、不明、利用不可、オフ、オン、サスペンド、起動中、シャットダウン中、サスペンド中、再開中。	シングルセッションおよびマルチセッション	
使用後にシャットダウンされます	電源管理されたシングルセッションマシンにのみ適用されます。マシンが汚染されており、すべてのセッションが終了した後にシャットダウンされるかどうかを示します。	シングルセッションのみ	
	注: マシンがメンテナンスモードの場合、シャットダウンされません。メンテナンスモードから解除された後にのみシャットダウンされます。		

登録

登録カテゴリの列。

列	説明	適用対象
最終登録失敗	ブローカーへのマシンの最終登録解除の理由。 可能な値は、AgentShutdown、AgentSuspended、AgentRequested、IncompatibleVersion、AgentAddressResolutionFailed、AgentNotContactable、AgentWrongActiveDirectoryOU、EmptyRegistrationRequest、MissingRegistrationCapabilities、MissingAgentVersion、InconsistentRegistrationCapabilities、NotLicensedForFeature、UnsupportedCredentialSecurityVersion、InvalidRegistrationRequest、SingleMultiSessionMismatch、FunctionalLevelTooLowForCatalog、FunctionalLevelTooLowForDesktopGroup、PowerOff、DesktopRestart、	シングルセッションおよびマルチセッション

列	説明	適用対象
	DesktopRemoved、AgentRejectedSettingsUpdate、SendSettingsFailure、SessionAuditFailure、SessionPrepareFailure、ContactLost、SettingsCreationFailure、UnknownError、およびBrokerRegistrationLimitReachedです。	
最終登録失敗時刻 (UTC)	マシンの最終登録解除時刻。	シングルセッションおよびマルチセッション
登録状態	マシンの登録状態。可能な値：Unregistered、Initializing、Registered、およびAgentError。	シングルセッションおよびマルチセッション
障害状態	マシンの現在の障害状態の概要。可能な値： • なし: 障害なし。マシンは正常です。 • FailedToStart: マシンの最後の電源投入操作が失敗しました。	シングルセッションおよびマルチセッション

列	説明	適用対象	
	• StuckOnBoot: 電源投入後、マシンが起動に失敗しました。		
	未登録。マシンが予期された期間内に登録に失敗したか、その登録が拒否されました。		
	最大容量。マシンが最大容量に達していると報告しています。		

セッションの詳細

セッションの詳細カテゴリの列。

列	説明	適用対象
起動元	現在のブローカーセッションの起動に使用されたStoreFrontサーバーのホスト名。マルチセッションマシンでは常にnullです。	シングルセッションおよびマルチセッション
起動元 (IP)	現在のブローカーセッションの起動に使用されたStoreFrontサーバーのIPアドレス。マルチセッションマシンでは常にnullです。	シングルセッションおよびマルチセッション
セッション変更時刻 (UTC)	現在のセッションの最後の状態変更時刻。	シングルセッションのみ
SmartAccessフィルター	現在のセッションのSmart Accessタグ。マルチセッションマシンでは常にヌルです。	シングルセッションおよびマルチセッション

セッション

セッションカテゴリの列。

列	説明	適用対象
セッションの状態	現在のセッションの状態。可能な値: Other、PreparingSession、Connected、Active、Disconnected、Reconnecting、NonBrokeredSession、Unknown。	シングルセッションのみ
現在のユーザー	現在のセッションのユーザー名（「DOMAIN\user」の形式）。	シングルセッションのみ
開始時刻 (UTC)	現在のセッションの開始時刻。	シングルセッションのみ
セッション数	マシン上のセッション数。	マルチセッションのみ

セッションのアクションと列

この記事では、参照用にマシンのアクションと列を説明とともに一覧表示します。

アクション

セッションで実行できるアクションとその説明を表示します。

アクション	説明	適用対象セッション
ログオフ	セッションからユーザーをログオフします。	シングルセッションOSマシンまたはマルチセッションOSマシン
メッセージを送信	セッションのユーザーにメッセージを送信します。	シングルセッションOSマシンまたはマルチセッションOSマシン

アクション	説明	適用対象セッション
マシンの表示	セッションのホストマシンを表示します。	シングルセッションOSマシンまたはマルチセッションOSマシン
切断	セッションを切断します。セッションが切断されても、セッションはアクティブなままでアプリケーションは実行され続けますが、ユーザーデバイスはDelivery Controllerと通信しなくなります。	シングルセッションOSマシンまたはマルチセッションOSマシン
マシンのシャットダウン	セッションに関連付けられているマシンをシャットダウンします。	シングルセッションOSマシン
マシンの再起動	セッションに関連付けられているマシンを再起動します。	シングルセッションOSマシン

列

セッションの列とその説明を表示します。

列	説明
現在のユーザー	ユーザーの名前。ユーザーのユーザープリンシパル名(UPN)。
名前	セッションをホストしているマシンのDNSホスト名。
デリバリーグループ	セッションをホストしているマシンを含むデリバリーグループの名前。
マシンカタログ	セッションをホストしているマシンを含むマシンカタログの名前。

列	説明
エージェントバージョン	セッションをホストしているマシンにインストールされているCitrix Virtual Delivery Agent (VDA) のバージョン。
使用中のアプリケーション	セッションで使用されているアプリケーションのリスト。管理名で識別されます。
自律的に仲介済み	これは、仲介されずに直接接続によって確立されたHDX™セッションであるかどうか。
仲介時間 (UTC)	セッションが仲介された時刻。
仲介ユーザー名	ブローカーユーザーの名前。
クライアント (IP)	セッションに接続されているクライアントのIPアドレス。
クライアント	セッションに接続されているクライアントのホスト名。
プラグインバージョン	セッションに接続されているクライアントで実行されているCitrix Workspace™アプリのバージョン。
接続元	受信接続のホスト名。通常はゲートウェイ、ルーター、またはクライアントです。
接続元 (IP)	受信接続のIPアドレス。通常、ゲートウェイ、ルーター、またはクライアントです。
割り当ての種類	セッションが共有か専用か。

列	説明
非表示	セッションがユーザーから非表示になっていて、再接続できないかどうか。
VM	セッションをホストしているVMの、ハイパーバイザーで使用されているフレンドリ名。マシンのDNS名またはAD名のいずれとも一致するとは限りません。
ホスティングサーバー名	セッションのホストマシンをホストしているハイパーバイザーのDNS名。
接続	セッションをホストしているマシンに割り当てられているホスト接続の名前。
保留中の更新	ホストされているマシンのVMイメージが古く、次回の再起動時に新しいイメージに更新される予定であるかどうか。
メンテナンスモード	セッションをホストしているマシンがメンテナンスモードであるかどうか。
IPアドレス	セッションをホストしているマシンのIPアドレス。
物理マシン	セッションをホストしているマシンが物理マシンであるかどうか。`True` は、マシンが物理マシンであり、Delivery Controllerによって電源管理されていないことを示します。`False` はその逆を示します。

列	説明
起動元	セッションの起動に使用されたStoreFront™サーバーのホスト名。セッションがWorkspace経由で起動された場合は空白です。
起動元 (IP)	セッションの起動に使用されたStoreFrontサーバーのIPアドレス。セッションがWorkspace経由で起動された場合は空白。
OSの種類	セッションをホストしているオペレーティングシステムの識別文字列。
ユーザー変更の永続性	ユーザーの変更がどのように処理されるかを示し、変更が永続的であるかどうかを示します: • OnLocal: 永続的。ユーザーの変更はローカルに保存されます。 • 破棄: 非永続的。ユーザーの変更は破棄されます。
接続タイプ	セッションに使用されるプロトコル（HDX、RDP、Consoleなど）。 **注:** XenDesktop® 5 VDA上のコンソールセッションの場合、このフィールドは空白です。

列	説明
プロビジョニングの種類	セッションをホストしているマシンがどのようにプロビジョニングされたか • 手動: PVSまたはMCSを使用してプロビジョニングされていません。 • PVS: PVSによってプロビジョニングされたもの（物理マシン、ブレードマシン、仮想マシン）。 • MCS: MCSによってプロビジョニングされたもの（VMのみ）。
Secure ICA® アクティブ	セッションでSecureICAがアクティブであるかどうか。
セッションの状態	セッションの状態。可能な値: Connected、Active、Disconnected。L7より前の機能レベルのマシン上のセッションでは、PreparingSession、Reconnecting、NonBrokeredSession、Other、Unknownなどの他の状態が発生する場合があります。
セッション変更時刻	セッションの最新の状態変更時刻。
アプリケーションの状態	セッション内のアプリケーションの状態。可能な値: PreLogon、PreLaunched、Active、Desktop、Lingering、NoApps。

列	説明
セッションサポート	セッションをホストしているマシンが複数セッションをサポートするか、単一セッションをサポートするか。
ゾーン	セッションをホストしているマシンが配置されているゾーンの名前。
SmartAccessフィルター	セッションのSmart Accessタグ。
開始時刻 (UTC)	セッションが開始された日時。
状態	マシンの概要状態。可能な値: Unregistered、Disconnected、またはInUse。
状態時間 (UTC)	セッションが現在の状態になってからの時間。
デリバリーコントローラー™	セッションのホストマシンが登録されているコントローラーのDNSホスト名。
ユーザー表示名	ユーザーのフルネーム。
デスクトップ表示名	セッションの起動に元々使用されたマシンの公開名。Citrix Workspaceアプリまたは StoreFrontに表示される名前です。アプリケーションセッションの場合、そのアプリケーションが終了していても、セッションに起動された最初のアプリケーションの名前です。リソースが後で名前変更または削除されても、名前は変更されません。

MCSプロビジョニング済みマシン (検索 > ハードウェアビュー)

この記事では、**検索**ノード内の**ハードウェアビュー**を使用して、MCSプロビジョニングされたマシンとそのプロパティを表示する方法を説明します。

ハードウェアビューについて学ぶ

「**検索**」ノード内のハードウェアビューには、MCSプロビジョニングされたマシンと、マシンのセキュリティ設定、ネットワークの詳細、イメージ、マシンプロファイルの詳細を含む重要なプロパティが表示されます。

検索ノード > ハードウェアビュー(/en-us/citrix-virtual-apps-desktops/current-release/media/search-hw-view-phase1.png)

コールアウト	エリア	説明
A	検索バー	クイック検索と、複雑な検索条件を定義できるフィルターベースの検索を提供します。詳細については、「マシンの検索」を参照してください。 **ヒント:** 特定のプロパティでマシンをすばやく絞り込むには、フィルターを使用します。たとえば、**保留中のイメージ更新 = はい**と**IDタイプ = ActiveDirectory**を組み合わせて、イメージ更新が保留中のすべてのActive Directoryマシンを表示します。

コールアウト	エリア	説明
B	デフォルトビューに切り替える	ハードウェアビューからデフォルトビューに切り替えます。
C	メインビュー	MCSプロビジョニングされたマシンとその重要なプロパティを表示します。「**表示する列**」アイコンを選択して、ビューをカスタマイズできます。利用可能な列の詳細については、マシン列を参照してください。
D	詳細ペイン	選択したマシンの詳細情報を表示します。
E	リストレベルのアクション	表示されているリスト全体に対して実行できるアクションを表示します： • 「**エクスポート**」アイコン: メインビューに表示されているマシンのリストをCSVファイルにエクスポートします。 • 「**表示する列**」アイコン: リストのメイン

コールアウト	エリア	説明
		ビューをカスタマイズします。

リファレンス: マシン列

この表は、ハードウェアビューのすべての列とその説明を一覧表示します。

列	説明
名前	マシンのDNSホスト名。
プロビジョニングスキーム名	マシンのプロビジョニングに使用されるプロビジョニングスキームの名前。
CPUコア	マシンに割り当てられたCPUコア数。
メモリ (MB)	マシンに割り当てられたメモリ量 (MB)。
永続性	マシンのディスクとデータが再起動後も保持されるかどうかを示します。
IDの種類	マシンのIDの種類。
保留中のイメージ更新	マシンのVMイメージが古くなっており、次回の再起動時に新しいイメージに更新される予定であるかどうかを示します。
最終起動時刻 (UTC)	マシンが最後に起動された日時 (UTC)。
WBCを使用	マシンがWBC (MCSIOとも呼ばれる) で構成されているかどうかを示します。
WBCディスクサイズ (GB)	マシンのMCSIOディスクキャッシュサイズ。
WBCメモリサイズ (MB)	マシンのMCSIOメモリキャッシュサイズ。
IDプロバイダー	マシンのIDプロバイダー。
アクティベーションの種類	Windows VDAにのみ有効です。マシンのWindowsライセンス認証の種類。値には、サポートされていないVDA、キー管理サービ

列	説明
	ス、マルチプルアクティベーションキー、および無効が含まれます。

セキュリティキー

重要:

- この機能は、StoreFront™ 1912 LTSR CU2以降と組み合わせて使用する必要があります。
- Secure XML機能は、Citrix ADCおよびCitrix Gatewayリリース12.1以降でのみサポートされています。

注:

バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

この機能を使用すると、承認されたStoreFrontおよびCitrix Gatewayマシンのみが Delivery Controllerと通信できるようになります。この機能を有効にすると、キーを含まないすべての要求はブロックされます。この機能を使用して、内部ネットワークからの攻撃から保護するための追加のセキュリティ層を追加します。

この機能を使用するための一般的なワークフローは次のとおりです。

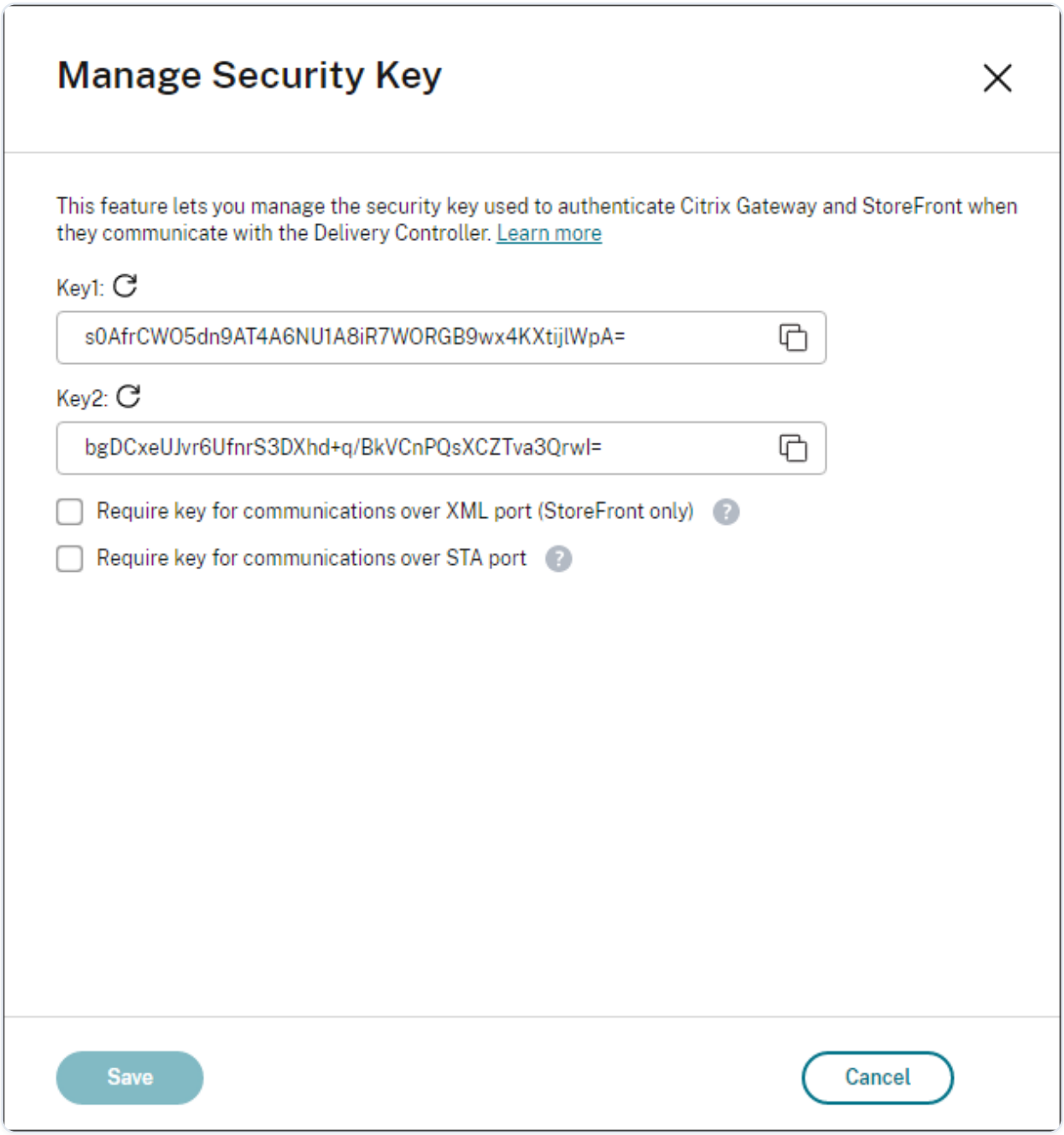
1. Web Studioを有効にして、機能設定を表示します。
2. サイトの設定を構成します。
3. StoreFrontの設定を構成します。
4. Citrix ADCの設定を構成します。

サイトの設定を構成する

Web StudioまたはPowerShellを使用して、サイトのセキュリティキー設定を構成できます。

Web Studioを使用する

1. Web Studioにサインインし、左ペインで**「設定」**を選択します。
2. **「セキュリティキーの管理」タイルを見つけて「編集」をクリックします。**「セキュリティキーの管理」**ページが表示されます。



3. 更新アイコンをクリックしてキーを生成します。

> **重要:**

- 使用できるキーは2つあります。XMLポートおよびSTAポートを介した通信には、同じキーまたは異なるキーを使用できます。一度に1つのキーのみを使用することをお勧めします。未使用のキーは、キーローテーションにのみ使用されます。
- 使用中のキーを更新するために更新アイコンをクリックしないでください。クリックすると、サービスが中断されます。

4. 通信にキーが必要な場所を選択します。
   - **XMLポートを介した通信にキーを要求する（StoreFrontのみ）**。選択した場合、XMLポートを介した通信を認証するためにキーが必要になります。StoreFrontはこのポートを介してCitrix Cloudと通信します。XMLポートの変更については、Knowledge Centerの記事CTX127945を参照してください。
   - **STAポートを介した通信にキーを要求する**。選択した場合、STAポートを介した通信を認証するためにキーが必要になります。Citrix GatewayとStoreFrontはこのポートを介してCitrix Cloudと通信します。STAポートの変更については、Knowledge Centerの記事CTX101988を参照してください。
5. **「保存」**をクリックして変更を適用し、ウィンドウを閉じます。

PowerShell を使用する

以下は、Web Studioの操作に相当するPowerShellの手順です。

1. Citrix Virtual Apps and Desktops™ リモート パワーシェル SDK を実行します。
2. コマンドウィンドウで、次のコマンドを実行します。
   - `Add-PSSnapIn Citrix*`
3. キーを生成し、Key1を設定するには、次のコマンドを実行します。
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey1 <the key you generated>`
4. 以下のコマンドを実行してキーを生成し、Key2 をセットアップします。
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey2 <the key you generated>`
5. 通信の認証でキーの使用を有効にするには、以下のコマンドのいずれか、または両方を実行します。

- XMLポート経由の通信を認証するには:
  - `Set-BrokerSite -RequireXmlServiceKeyForNFuse $true`
- STAポート経由の通信を認証するには:
  - `Set-BrokerSite -RequireXmlServiceKeyForSta $true`

ガイダンスと構文については、PowerShellコマンドのヘルプを参照してください。

StoreFrontの設定を構成する

サイトの構成が完了したら、PowerShellを使用してStoreFrontの関連設定を構成する必要があります。

StoreFront サーバーで、以下の PowerShell コマンドを実行します。

XMLポートを介した通信用のキーを構成するには、コマンドを使用します。例:

```
$store = Get-STFStoreService -VirtualPath [Path to store]

$farm = Get-STFStoreFarm -StoreService $store -FarmName [Resource feed
name]

Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true
-XMLValidationSecret [secret]
```

次のパラメータに適切な値を入力します。

- `Path to store`
- `Resource feed name`
- `secret`

STAポート経由の通信用にキーを構成するには、`New-STFSecureTicketAuthority`および`Set-STFRoamingGateway`コマンドを使用します。例:

```
$gateway = Get-STFRoamingGateway -Name [Gateway name]

$sta1 = New-STFSecureTicketAuthority -StaUrl [STA1 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

$sta2 = New-STFSecureTicketAuthority -StaUrl [STA2 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]
```

```
Set-STFRoamingGateway -Gateway $gateway -SecureTicketAuthorityObjs
$sta1,$sta2
```

次のパラメータに適切な値を入力します。

- `Gateway name`
- `STA URL`
- `Secret`

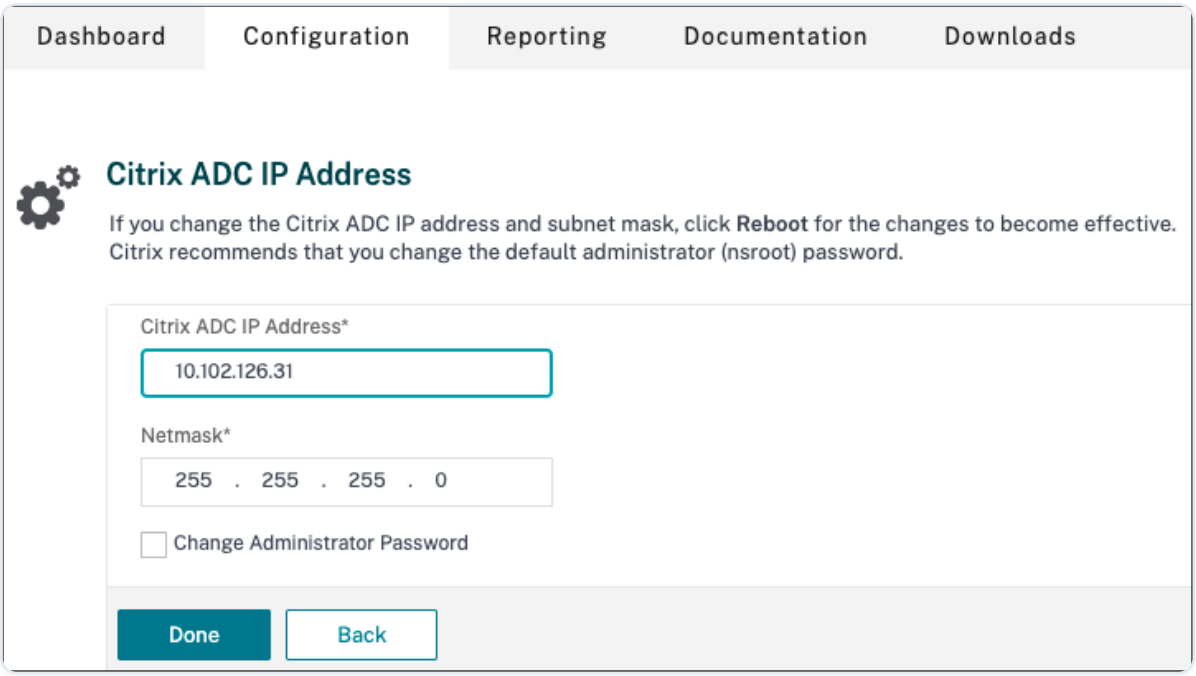
ガイダンスと構文については、PowerShellコマンドのヘルプを参照してください。

Citrix ADCの設定を構成する

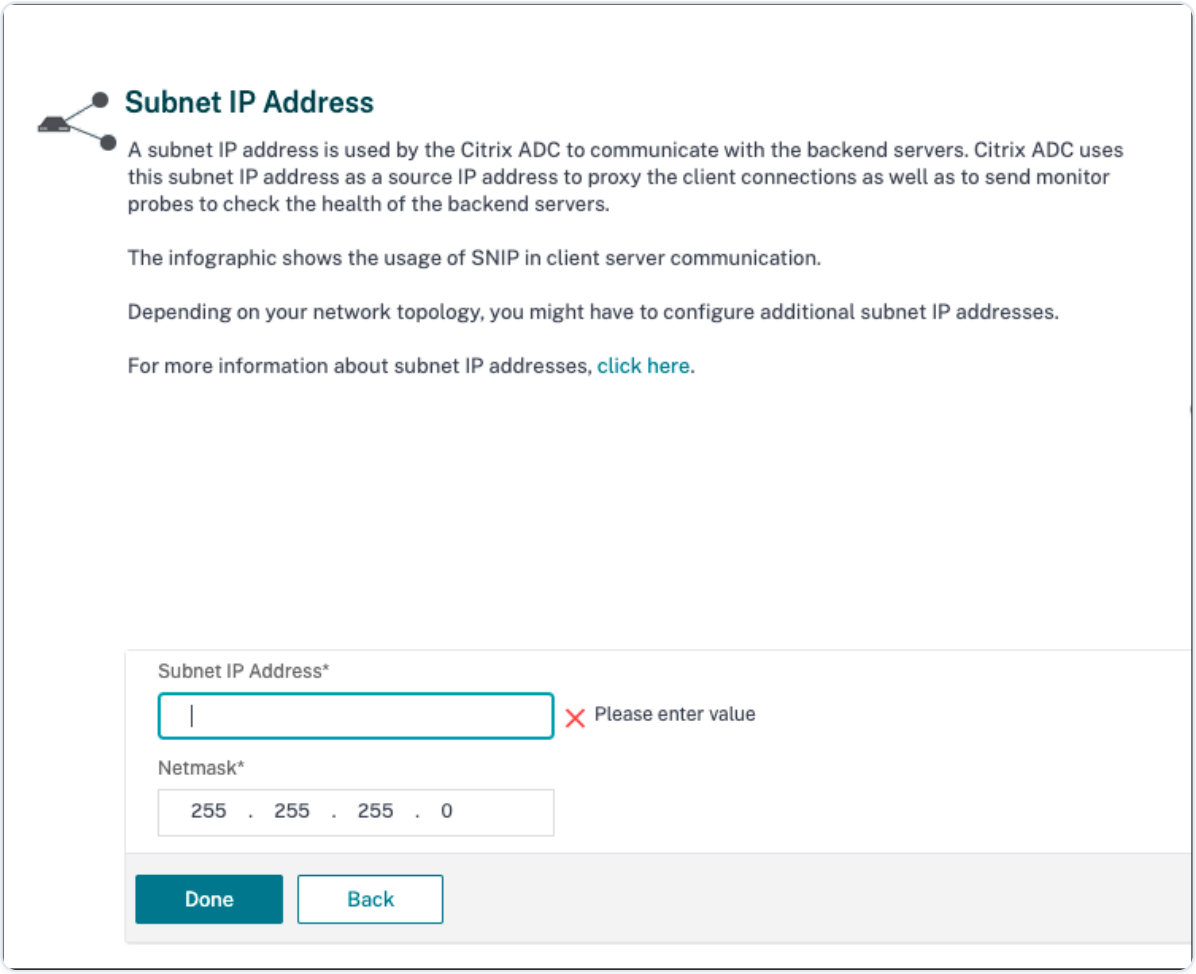
注:

Citrix ADCをゲートウェイとして使用しない限り、Citrix ADCのこの機能の構成は不要です。Citrix ADCを使用する場合は、次の手順に従います。

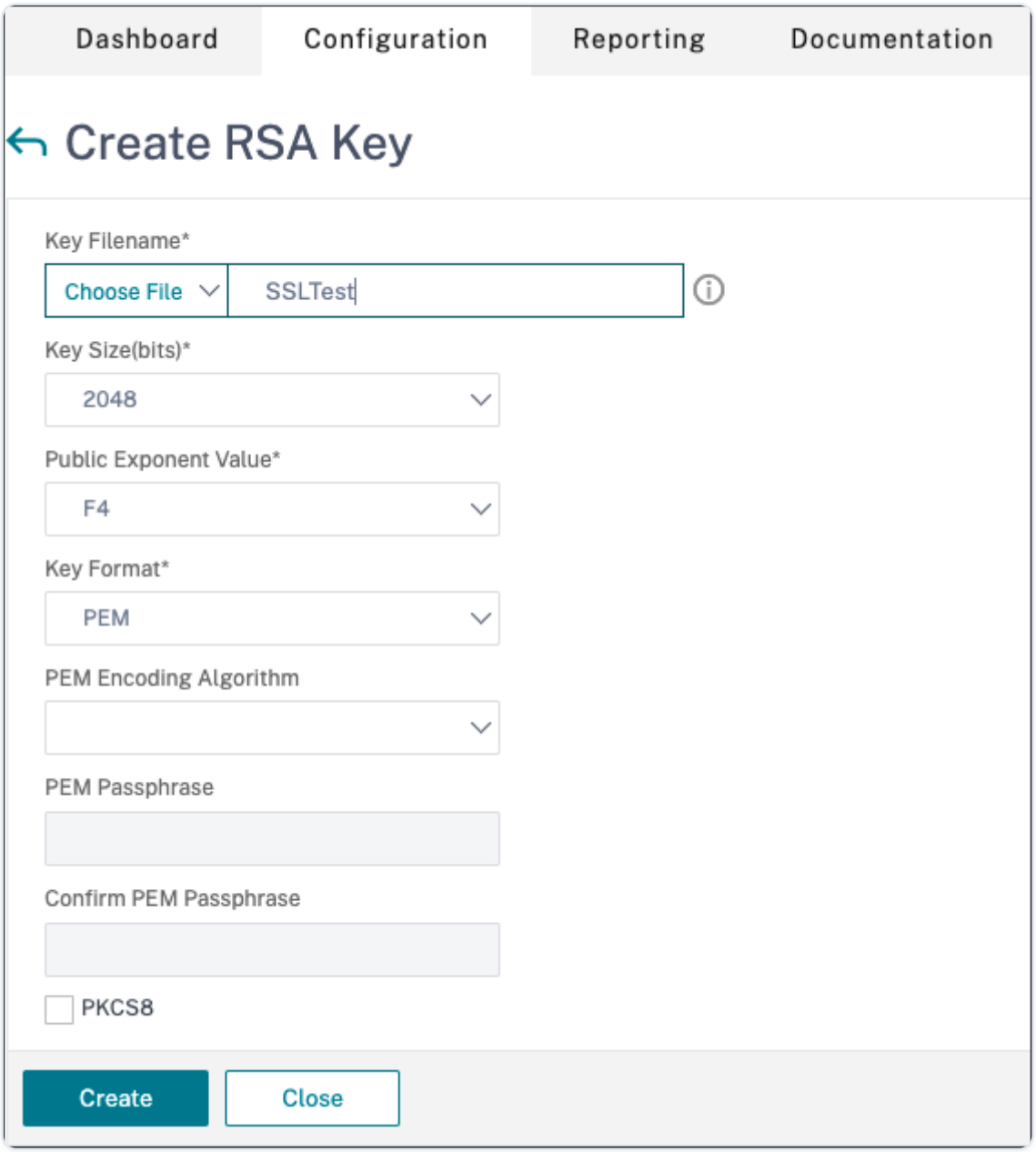
1. 次の前提条件となる構成がすでに設定されていることを確認してください。
    - 次のCitrix ADC関連のIPアドレスが構成されています。
        - Citrix ADCコンソールにアクセスするための Citrix ADC管理IP (NSIP) アドレス。詳細については、「NSIPアドレスの構成」を参照してください。



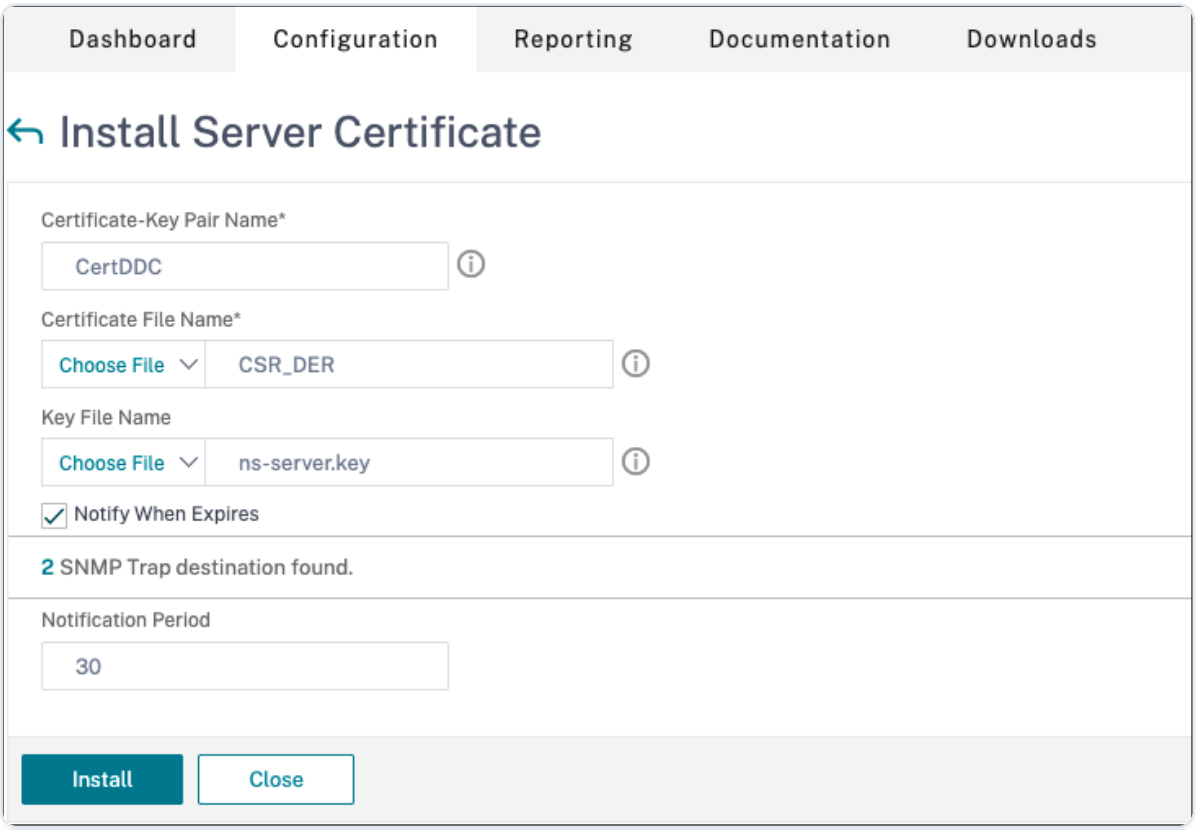
- Citrix ADCアプライアンスとバックエンドサーバー間の通信を有効にするためのサブネットIP（SNIP）アドレス。詳細については、「サブネットIPアドレスの構成」を参照してください。
- セッション起動のためにADCアプライアンスにログインするためのCitrix Gateway仮想IPアドレスとロードバランサー仮想IPアドレス。詳細については、「仮想サーバーの作成」を参照してください。

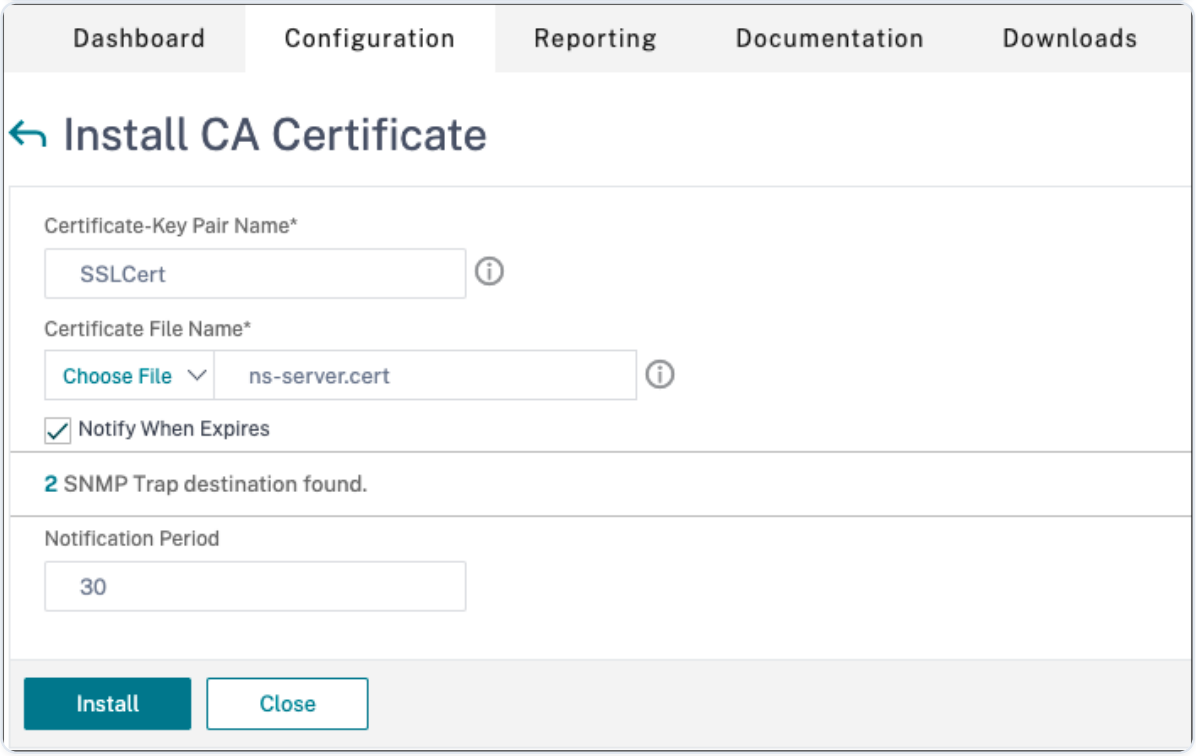


- Citrix ADCアプライアンスで必要なモードと機能が有効になっています。
  - モードを有効にするには、Citrix ADC GUIで **System > Settings > Configure Mode** に移動します。
  - 機能を有効にするには、Citrix ADC GUIで **System > Settings > Configure Basic Features** に移動します。
- 証明書関連の構成が完了しています。
  - 証明書署名要求（CSR）が作成されます。詳細については、「証明書の作成」を参照してください。

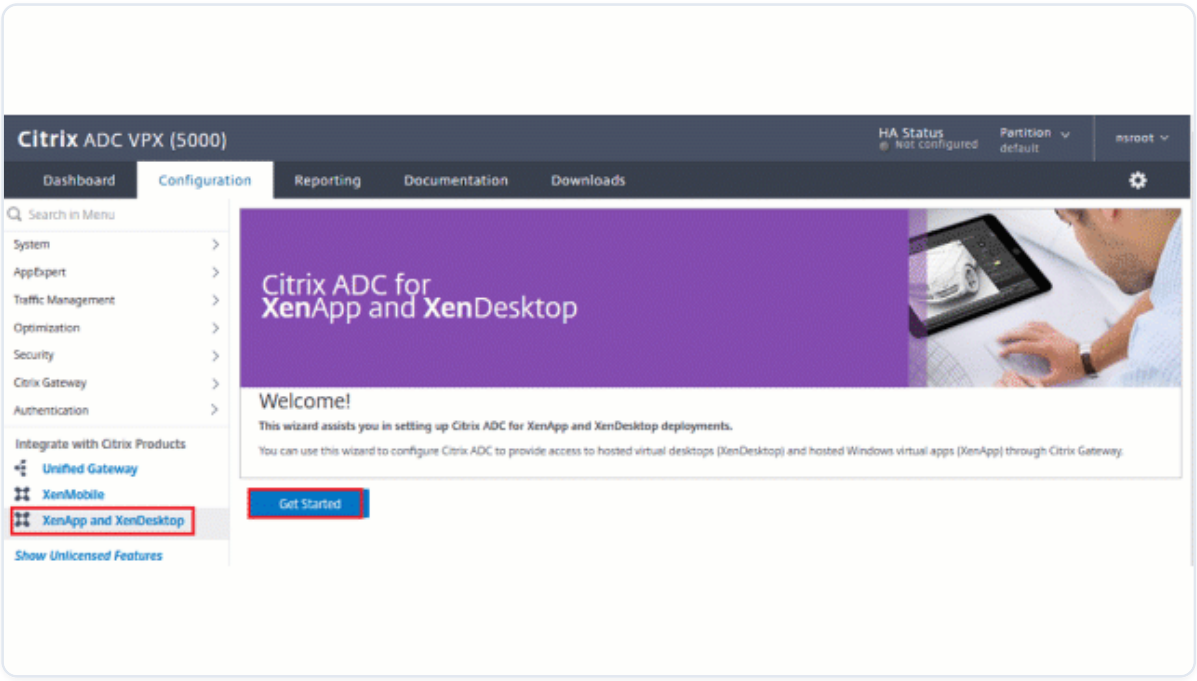


- サーバー証明書、CA証明書、およびルート証明書がインストールされます。詳細については、「インストール、リンク、および更新」を参照してください。





- Citrix Virtual Desktops用にCitrix Gatewayが作成されました。仮想サーバーがオンラインであることを確認するには、**Test STA Connectivity**ボタンをクリックして接続をテストします。詳細については、「Setting up Citrix ADC for Citrix Virtual Apps and Desktops」を参照してください。



2. リライトアクションを追加します。詳細については、「リライトアクションの構成」を参照してください。

   a. 「**AppExpert > Rewrite > Actions**」に移動します。

   b. 新しい書き換えアクションを追加するには、**追加**をクリックします。アクションの名前は「set Type to INSERT_HTTP_HEADER」にすることができます。

   書き換えアクションの追加(/en-us/citrix-virtual-apps-desktops/current-release/media/adc-appexpert-rewrite-action.png)

   a. **タイプ**で、**INSERT_HTTP_HEADER**を選択します。

   b. **ヘッダー名**に「X-Citrix-XmlServiceKey」と入力します。

   c. **式**に、引用符付きで`<XmlServiceKey1 value>`を追加します。XmlServiceKey1 の値は、Desktop Delivery Controller™ の構成からコピーできます。

   XMLサービスキーの値(/en-us/citrix-virtual-apps-desktops/current-release/media/xml-service-key-values.png)

3. 書き換えポリシーを追加します。詳細については、「書き換えポリシーの構成」を参照してください。

   a. 「**AppExpert > Rewrite > Policies**」に移動します。

   b. 新しいポリシーを追加するには、**追加**をクリックします。

   書き換えポリシーの追加(/en-us/citrix-virtual-apps-desktops/current-release/media/adc-appexpert-rewrite-policy.png)

a. **アクション**で、前の手順で作成したアクションを選択します。

b. **式**に「HTTP.REQ.IS_VALID」を追加します。

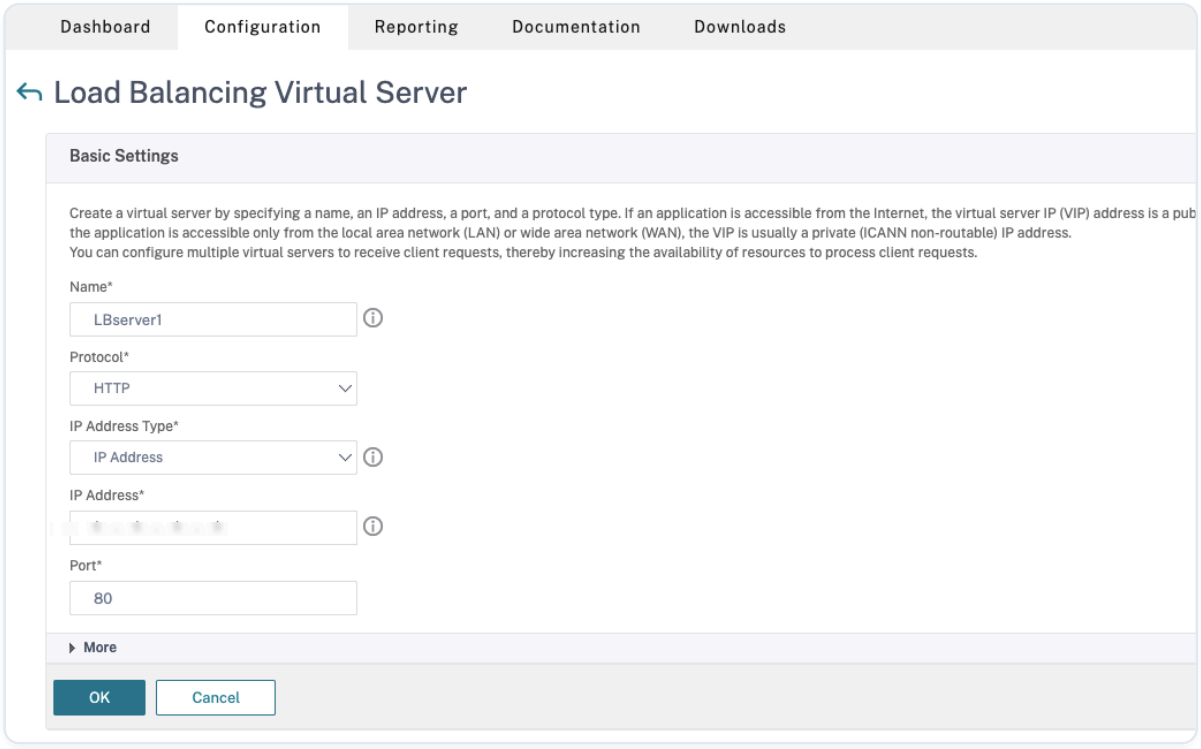
c. **OK**をクリックします。

4. 負荷分散を設定します。STAサーバーごとに1つの負荷分散仮想サーバーを構成する必要があります。構成しない場合、セッションの起動に失敗します。

   詳細については、基本的な負荷分散のセットアップを参照してください。

   a. 負荷分散仮想サーバーを作成します。

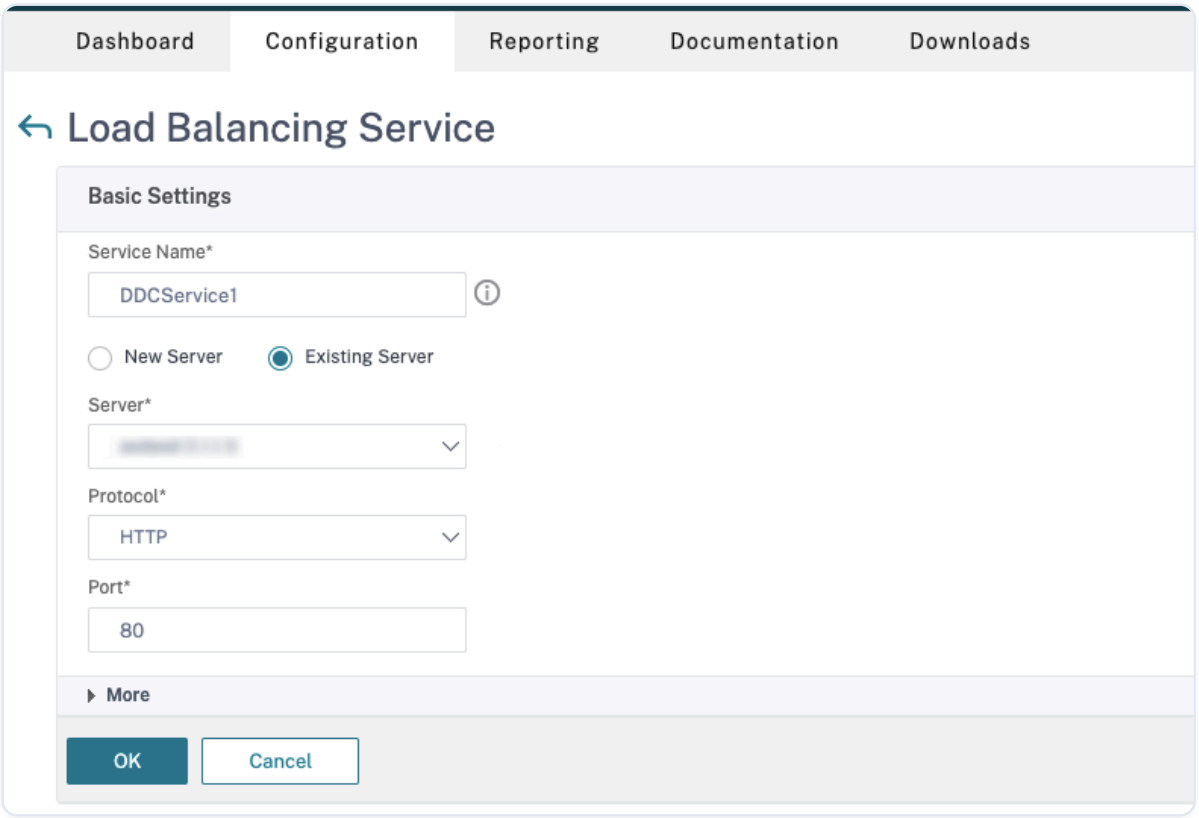
      - **トラフィック管理 > ロードバランシング > サーバー**に移動します。
      - **Virtual Servers**ページで、**Add**をクリックします。



      - **Protocol**で、**HTTP**を選択します。
      - 負荷分散仮想IPアドレスを追加し、**Port**で**80**を選択します。
      - **OK**をクリックします。

   b. 負荷分散サービスを作成します。

      - **トラフィック管理 > ロードバランシング > サービス**に移動します。



- **Existing Server**で、前のステップで作成した仮想サーバーを選択します。
- **Protocol**で**HTTP**を選択し、**Port**で**80**を選択します。
- **OK**をクリックし、その後**Done**をクリックします。

c. サービスを仮想サーバーにバインドします。

- 以前に作成した仮想サーバーを選択し、**編集**をクリックします。
- **サービスとサービスグループ**で、**ロードバランシング仮想サーバーサービスバインディングなし**をクリックします。

仮想サーバーにサービスをバインド(/en-us/citrix-virtual-apps-desktops/current-release/media/adc-bind-service-to-lbvserver.png)

- **Service Binding**で、以前に作成したサービスを選択します。
- **バインド**をクリックします。

d. 以前に作成した書き換えポリシーを仮想サーバーにバインドします。

- 以前に作成した仮想サーバーを選択し、**編集**をクリックします。
- **詳細設定**で、**ポリシー**をクリックし、次に**ポリシー**セクションで**+**をクリックします。

書き換えポリシーをバインド(/en-us/citrix-virtual-apps-desktops/current-release/media/adc-bind-rewrite-policy.png)

- **ポリシーの選択**で**書き換え**を選択し、**タイプの選択**で**要求**を選択します。
- **続行**をクリックします。
- **ポリシーの選択**で、以前に作成した書き換えポリシーを選択します。
- **バインド**をクリックします。
- 「**完了**」をクリックします。

e. 必要に応じて、仮想サーバーの永続性を設定します。

- 以前に作成した仮想サーバーを選択し、**編集**をクリックします。
- **詳細設定**で、**永続性**をクリックします。

永続性の設定(/en-us/citrix-virtual-apps-desktops/current-release/media/adc-lb-vserver-persistence.png)

- 永続性の種類として**その他**を選択します。
- 仮想サーバーによって選択されたサービスのIPアドレス（宛先IPアドレス）に基づいて永続性セッションを作成するには、**DESTIP**を選択します。
- **IPv4ネットマスク**で、DDCと同じネットワークマスクを追加します。
- **OK**をクリックします。

f. 他の仮想サーバーについても、これらの手順を繰り返します。

Citrix ADCアプライアンスがCitrix Virtual Desktops™で既に構成されている場合の構成の変更点

Citrix ADCアプライアンスをCitrix Virtual Desktopsで既に構成している場合、Secure XML機能を使用するには、以下の構成変更を行う必要があります。

- セッション起動前に、ゲートウェイの**セキュリティチケット機関URL**を、負荷分散仮想サーバーのFQDNを使用するように変更します。
- `TrustRequestsSentToTheXmlServicePort` パラメーターがFalseに設定されていることを確認してください。デフォルトでは、`TrustRequestsSentToTheXmlServicePort` パラメーターはFalseに設定されています。ただし、顧客がCitrix Virtual Desktops用にCitrix ADCを既に構成している場合、`TrustRequestsSentToTheXmlServicePort` はTrueに設定されます。

1. Citrix ADC GUIで、**構成 > Citrix製品との統合**に移動し、**XenApp and XenDesktop®**をクリックします。
2. ゲートウェイインスタンスを選択し、編集アイコンをクリックします。

   既存のゲートウェイ構成を編集(/en-us/citrix-virtual-apps-desktops/current-release/media/edit-gateway-instance.png)
3. StoreFrontペインで、編集アイコンをクリックします。

   StoreFrontの詳細を編集(/en-us/citrix-virtual-apps-desktops/current-release/media/edit-storefront-details.png)
4. **Secure Ticket Authority URL**を追加します。

   - Secure XML機能が有効になっている場合、STA URLはロードバランシングサービスのURLである必要があります。
   - Secure XML機能が無効になっている場合、STA URLはSTAのURL（DDCのアドレス）である必要があり、DDC上の`TrustRequestsSentToTheXmlServicePort`パラメーターはTrueに設定されている必要があります。

   STA URLを追加(/en-us/citrix-virtual-apps-desktops/current-release/media/add-sta-urls.png)

セッションの回復性設定

セッションアクティビティを維持することは、最高のユーザーエクスペリエンスを提供するために不可欠です。信頼性の低いネットワーク、変動の大きいネットワーク遅延、ワイヤレスデバイスの範囲制限による接続の喪失は、ユーザーの不満につながる可能性があります。デバイス間を素早く移動し、ログオンするたびに同じアプリケーションにアクセスすることは、医療従事者などの多くのモバイルワーカーにとって優先事項です。

この記事で説明する機能は、セッションの信頼性を最適化し、不便さ、ダウンタイム、生産性の損失を軽減します。これらの機能を使用することで、モバイルユーザーはデバイス間を迅速かつ簡単にローミングできます。

セッションの信頼性

セッションの信頼性により、ネットワーク接続が中断されてもセッションはアクティブな状態を保ち、ユーザーの画面に表示されます。ユーザーは、ネットワーク接続が再開されるまで、使用しているアプリケーションを引き続き見ることができます。

この機能は、ワイヤレス接続を使用するモバイルユーザーにとって特に便利です。たとえば、ワイヤレス接続を使用しているユーザーが鉄道トンネルに入り、一時的に接続が失われたとします。通常、セッションは切断されてユーザーの画面から消え、ユーザーは切断されたセッションに再接続する必要があります。セッションの信頼性を使用すると、セッションはマシン上でアクティブなままになります。接続が失われたことを示すために、ユーザーのディスプレイはフリーズし、カーソルはトンネルの反対側で接続が再開されるまで回転する砂時計に変わります。ユーザーは中断中もディスプレイにアクセスし続け、ネットワーク接続が復元されるとアプリケーションとの対話を再開できます。セッションの信頼性により、再認証のプロンプトなしでユーザーが再接続されます。

Citrix Workspace™アプリのユーザーは、Controllerの設定を上書きできません。

セッションの信頼性は、トランスポート層セキュリティ (TLS) とともに使用できます。TLSは、ユーザーデバイスとCitrix Gatewayの間で送信されるデータのみを暗号化します。

次のポリシー設定でセッションの信頼性を有効にして構成します。

- セッションの信頼性接続ポリシー設定は、セッションの信頼性を許可または禁止します。
- セッションの信頼性タイムアウトポリシー設定のデフォルトは180秒、つまり3分です。セッションの信頼性がセッションを開いたままにする時間を延長することはできますが、この機能はユーザーの利便性のために設計されています。そのため、ユーザーに再認証を促すことはありません。セッションを開いたままにする時間を延長すると、ユーザーが注意散漫になり、ユーザーデバイスから離れてしまう可能性が高まります。これらの行動は、セッションを不正なユーザーがアクセスできる状態にする可能性があります。
- 受信セッションの信頼性接続は、セッションの信頼性ポート番号ポリシー設定でポート番号を変更しない限り、ポート2598を使用します。
- ユーザーが再認証なしで中断されたセッションに再接続するのを防ぐには、自動クライアント再接続機能を使用します。自動クライアント再接続認証ポリシー設定を構成して、中断されたセッションに再接続する際にユーザーに再認証を促すことができます。

セッションの信頼性と自動クライアント再接続の両方を使用する場合、これら2つの機能は順次動作します。セッションの信頼性は、セッションの信頼性タイムアウトポリシー設定で指定した時間の経過後、ユーザーセッションを閉じるか、切断します。その後、自動クライアント再接続ポリシー設定が有効になり、切断されたセッションにユーザーを再接続しようとします。

クライアントの自動再接続

自動クライアント再接続機能を使用すると、Citrix WorkspaceアプリはICA®セッションの意図しない切断を検出し、影響を受けるセッションにユーザーを自動的に再接続できます。この機能が

サーバーで有効になっている場合、ユーザーは作業を続行するために手動で再接続する必要はありません。

アプリケーションセッションの場合、Citrix Workspaceアプリは、再接続が成功するか、ユーザーが再接続の試行をキャンセルするまで、セッションへの再接続を試みます。

デスクトップセッションの場合、Citrix Workspaceアプリは、再接続が成功するか、ユーザーが再接続の試行をキャンセルしない限り、指定された期間、セッションへの再接続を試行します。デフォルトでは、この期間は5分です。この期間を変更するには、ユーザーデバイスで以下のレジストリ設定を編集します（`seconds` は、セッションの再接続がそれ以上試行されなくなるまでの秒数です）。

`HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds; DWORD;<seconds>`

以下のポリシー設定でAuto Client Reconnectを有効にして構成します。

- **Auto Client Reconnect:** 接続が中断された後にCitrix Workspaceアプリによる自動再接続を有効または無効にします。
- **Auto Client Reconnect authentication:** 自動再接続後のユーザー認証の要件を有効または無効にします。
- **Auto Client Reconnect logging:** イベントログへの再接続イベントのログ記録を有効または無効にします。ログ記録はデフォルトで無効になっています。有効にすると、サーバーのシステムログに、成功および失敗した自動再接続イベントに関する情報が記録されます。各サーバーは、再接続イベントに関する情報を独自のシステムログに保存します。サイトは、すべてのサーバーの再接続イベントの統合ログを提供しません。

> **注:**
>
> 再認証なしのAuto Client Reconnectは、パスワード認証でのみサポートされています。フェデレーション認証サービスまたはスマートカード認証を使用している場合、再認証なしのAuto Client Reconnectはサポートされません。そのような場合、ユーザーはログイン画面にリダイレクトされます。

> Auto Client Reconnectは、暗号化されたユーザー資格情報に基づく認証メカニズムを組み込んでいます。ユーザーが最初にログオンすると、サーバーはユーザー資格情報を暗号化してメモリに保存します。サーバーはまた、暗号化キーを含むCookieを作成し、Citrix Workspaceアプリに送信します。Citrix Workspaceアプリは、再接続のためにキーをサー

> バーに送信します。サーバーは資格情報を復号化し、認証のためにWindowsログオンに送信します。Cookieの有効期限が切れると、ユーザーはセッションに再接続するために再認証する必要があります。

Auto Client Reconnect認証設定を有効にすると、Cookieは使用されません。代わりに、Citrix Workspaceアプリが自動的に再接続を試みるときに、資格情報を要求するダイアログボックスがユーザーに表示されます。

ユーザー資格情報とセッションを最大限に保護するために、クライアントとサイト間のすべての通信に暗号化を使用してください。

icaclient.admファイルを使用して、Windows版Citrix WorkspaceアプリでAuto Client Reconnectを無効にします。詳細については、お使いのWindows版Citrix Workspaceアプリのバージョンのドキュメントを参照してください。

接続の設定もAuto Client Reconnectに影響します。

- デフォルトでは、前述のとおり、Auto Client Reconnectはサイトレベルのポリシー設定によって有効になっています。ユーザーの再認証は不要です。ただし、サーバーのICA TCP接続が、通信リンクが切断されたセッションをリセットするように構成されている場合、自動再接続は行われません。Auto Client Reconnectは、接続が切断されたかタイムアウトした場合にサーバーがセッションを切断する場合にのみ機能します。このコンテキストでは、ICA TCP接続とは、TCP/IPネットワーク上のセッションに使用されるサーバーの仮想ポート（実際のネットワーク接続ではなく）を指します。
- デフォルトでは、サーバー上のICA TCP接続は、切断された接続またはタイムアウトした接続を持つセッションを切断するように設定されています。切断されたセッションはシステムメモリにそのまま残り、Citrix Workspaceアプリによる再接続が可能です。
- 接続は、切断された接続またはタイムアウトした接続を持つセッションをリセットまたはログオフするように構成できます。セッションがリセットされると、再接続を試みると新しいセッションが開始されます。使用中のアプリケーションでユーザーを同じ場所に戻すのではなく、アプリケーションが再起動されます。
- サーバーがセッションをリセットするように構成されている場合、Auto Client Reconnectは新しいセッションを作成します。このプロセスでは、ユーザーがサーバーにログオンするために資格情報を入力する必要があります。
- Citrix Workspaceアプリまたはプラグインが誤った認証情報を送信した場合、自動再接続が失敗することがあります。これは、攻撃中に発生したり、サーバーが切断された接続を検出してから時間が経ちすぎたと判断した場合に起こりえます。

ICA キープアライブ

ICA Keep-Alive機能を有効にすると、途切れた接続が切断されるのを防ぎます。有効にすると、サーバーがアクティビティを検出しない場合、この機能によりリモートデスクトップサービスがそのセッションを切断するのを防ぎます。アクティビティがない例としては、クロックの変更、マウスの移動、画面の更新がないことなどが挙げられます。サーバーは数秒ごとにキープアライブパケットを送信して、セッションがアクティブであるかどうかを検出します。セッションがアクティブでなくなった場合、サーバーはそのセッションを切断済みとしてマークします。

> **重要:**

> ICA Keep-Aliveは、セッションの信頼性を使用していない場合にのみ機能します。セッションの信頼性には、途切れた接続が切断されるのを防ぐ独自のメカニズムがあります。ICA Keep-Aliveは、セッションの信頼性を使用しない接続に対してのみ構成してください。

> ICA Keep-Alive設定は、Windowsグループポリシーで構成されているキープアライブ設定を上書きします。

次のポリシー設定を使用して、ICA Keep-Aliveを有効にして構成します。

- **ICAキープアライブタイムアウト:** ICAキープアライブメッセージの送信に使用される間隔（1～3600秒）を指定します。途切れた接続が非常にまれで、ユーザーがセッションに再接続できることが問題にならない環境で、ネットワーク監視ソフトウェアに非アクティブな接続を閉じさせたい場合は、このオプションを構成しないでください。

  デフォルトの間隔は60秒です。ICA Keep-Aliveパケットは60秒ごとにユーザーデバイスに送信されます。ユーザーデバイスが60秒以内に応答しない場合、ICAセッションのステータスは切断済みに変わります。
- **ICAキープアライブ:** ICAキープアライブメッセージの送信を許可または禁止します。

ワークスペースコントロール

ワークスペースコントロールにより、デスクトップとアプリケーションはユーザーに追従し、デバイス間を移動できます。このローミング機能により、ユーザーはログオンするだけで、各デバイスでデスクトップやアプリケーションを再起動することなく、どこからでもすべてのデスクトップや開いているアプリケーションにアクセスできます。たとえば、ワークスペースコントロールは、病院で異なるワークステーション間を素早く移動し、ログオンするたびに同じアプリケーションセットにアクセスする必要がある医療従事者を支援できます。ワークスペースコントロールオプションを許可するように構成すると、これらの医療従事者は1つのクライアントデバイスで複数の

アプリケーションから切断し、別のクライアントデバイスで同じアプリケーションを開くために再接続できます。

ワークスペースコントロールは、次のアクティビティに影響します。

- **ログオン:** デフォルトでは、ワークスペースコントロールにより、ユーザーはログオン時に実行中のすべてのデスクトップとアプリケーションに自動的に再接続でき、手動で再開する必要がなくなります。ワークスペースコントロールを通じて、ユーザーは切断されたデスクトップまたはアプリケーション、および別のクライアントデバイスでアクティブなものを開くことができます。デスクトップまたはアプリケーションから切断しても、それはサーバー上で実行されたままになります。一部のデスクトップまたはアプリケーションを1つのクライアントデバイスで実行したままにし、別のクライアントデバイスでデスクトップまたはアプリケーションのサブセットに再接続する必要があるローミングユーザーがいる場合、ユーザーが以前に切断したデスクトップまたはアプリケーションのみを開くようにログオン再接続動作を構成できます。
- **再接続:** サーバーにログオンした後、ユーザーは「再接続」をクリックすることで、いつでもすべてのデスクトップまたはアプリケーションに再接続できます。デフォルトでは、「再接続」は切断されたデスクトップまたはアプリケーション、および現在別のクライアントデバイスで実行中のものを開きます。ユーザーが以前に切断したデスクトップまたはアプリケーションのみを開くように「再接続」を構成できます。
- **ログオフ:** StoreFront™を介してデスクトップまたはアプリケーションを開くユーザーの場合、**ログオフ**コマンドを構成して、ユーザーをStoreFrontとすべてのアクティブなセッションからログオフさせるか、StoreFrontからのみログオフさせることができます。
- **切断:** ユーザーは、個別に切断する必要なく、実行中のすべてのデスクトップとアプリケーションから一度に切断できます。

ワークスペースコントロールは、Citrix StoreFront接続を介してデスクトップおよびアプリケーションにアクセスするCitrix Workspaceアプリユーザーのみが利用できます。デフォルトでは、ワークスペースコントロールは仮想デスクトップセッションでは無効になっていますが、ホスト型アプリケーションでは有効になっています。公開されたデスクトップと、それらのデスクトップ内で実行されている公開されたアプリケーションとの間で、セッション共有はデフォルトでは行われません。

ユーザーが新しいクライアントデバイスに移動すると、ユーザーポリシー、クライアントドライブマッピング、およびプリンター構成が適切に変更されます。ポリシーとマッピングは、ユーザーがセッションにログオンしているクライアントデバイスに応じて適用されます。たとえば、医療従事者が救急治療室のデバイスからログオフし、X線検査室のワークステーションにログオンする場

合、X線検査室でのセッションに適したポリシー、プリンターマッピング、およびクライアントドライブマッピングがセッション開始時に有効になります。

ユーザーが場所を変更したときに表示されるプリンターをカスタマイズできます。また、ユーザーがローカルプリンターに印刷できるかどうか、ユーザーがリモートで接続したときに消費される帯域幅の量、およびその他の印刷エクスペリエンスの側面を制御することもできます。

ユーザー向けにワークスペースコントロールを有効化および構成する方法については、StoreFrontのドキュメントを参照してください。

セッションローミング

> **注:**
>
> 以下の情報は、PowerShellを使用してセッションローミングを構成する方法を説明しています。代わりにWeb Studioを使用することもできます。詳細については、「デリバリーグループの管理」を参照してください。

> デフォルトでは、セッションはユーザーとともにクライアントデバイス間をローミングします。ユーザーがセッションを起動し、別のデバイスに移動すると、同じセッションが使用され、両方のデバイスでアプリケーションが利用可能になります。アプリケーションは、デバイスや現在のセッションの有無にかかわらず追従します。多くの場合、アプリケーションに割り当てられたプリンターやその他のリソースも追従します。

このデフォルトの動作には多くの利点がありますが、すべての場合に理想的とは限りません。PowerShell SDKを使用してセッションローミングを防止できます。

例1：医療従事者が2つのデバイスを使用しており、デスクトップPCで保険フォームを完成させ、タブレットで患者情報を閲覧しています。

- セッションローミングが有効になっている場合、両方のアプリケーションが両方のデバイスに表示されます（1つのデバイスで起動されたアプリケーションは、使用中のすべてのデバイスで表示されます）。これはセキュリティ要件を満たさない可能性があります。
- セッションローミングが無効になっている場合、患者記録はデスクトップPCに表示されず、保険フォームはタブレットに表示されません。

例2：生産管理者が自分のオフィスにあるPCでアプリケーションを起動します。デバイス名と場所によって、そのセッションで利用可能なプリンターやその他のリソースが決まります。その日の後半、彼は会議のために隣の建物のオフィスに行き、プリンターを使用する必要があります。

- セッションローミングが有効になっている場合、生産管理者は会議室近くのプリンターにアクセスできない可能性があります。なぜなら、彼がオフィスで以前に起動したアプリケーションによって、その場所近くのプリンターやその他のリソースが割り当てられたためです。
- セッションローミングが無効になっている場合、彼が別のマシンに（同じ資格情報を使用して）ログオンすると、新しいセッションが開始され、近くのプリンターやリソースが利用可能になります。

セッションローミングの構成

セッションローミングを構成するには、「SessionReconnection」プロパティを持つ以下のエンタイトルメントポリシー規則コマンドレットを使用します。オプションで、「LeasingBehavior」プロパティも指定できます。

デスクトップセッションの場合：

```
Set-BrokerEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection <value> -LeasingBehavior Allowed|Disallowed
```

アプリケーションセッションの場合：

```
Set-BrokerAppEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection <value> -LeasingBehavior Allowed|Disallowed
```

`value` には、次のいずれかを指定できます。

- **Always:** セッションは、クライアントデバイスやセッションが接続されているか切断されているかに関係なく、常にローミングします。これがデフォルト値です。
- **DisconnectedOnly:** 既に切断されているセッションにのみ再接続します。それ以外の場合は、新しいセッションを起動します。（セッションは、最初に切断するか、Workspace Control を使用して明示的にローミングすることで、クライアントデバイス間をローミングできます。）別のクライアントデバイスからのアクティブな接続済みセッションは使用されません。代わりに、新しいセッションが起動されます。
- **SameEndpointOnly:** ユーザーは、使用するクライアントデバイスごとに一意のセッションを取得します。これにより、ローミングが完全に無効になります。ユーザーは、以前セッションで使用したのと同じデバイスにのみ再接続できます。

「LeasingBehavior」プロパティについては、以下で説明します。

その他の設定による影響：

セッションローミングを無効にすると、デリバリーグループのアプリケーションのプロパティにあるアプリケーション制限 **ユーザーごとにアプリケーションのインスタンスを1つのみ許可する** の影響を受けます。

- セッションローミングを無効にする場合は、「アプリケーションのインスタンスを1つのみ許可する...」アプリケーション制限も無効にします。
- 「アプリケーションのインスタンスを1つのみ許可する...」アプリケーション制限を有効にする場合は、新しいデバイスで新しいセッションを許可する2つの値のいずれも構成しないでください。

ログオン間隔

デスクトップVDAを含む仮想マシンがログオンプロセス完了前に閉じられた場合、そのプロセスにより多くの時間を割り当てることができます。バージョン7.6以降のデフォルトは180秒です（バージョン7.0〜7.5のデフォルトは90秒です）。

マシン（またはマシンカタログで使用されるマスターイメージ）で、次のレジストリキーを設定します。

キー: `HKLM\SOFTWARE\Citrix\PortICA`

- 値: `AutoLogonTimeout`
- 種類: `DWORD`
- 0〜3600の範囲で、10進数の時間を秒単位で指定します。

マスターイメージを変更した場合は、カタログを更新します。

この設定は、デスクトップVDAを持つVMにのみ適用されます。Microsoftは、サーバーVDAを持つマシンでのログオンタイムアウトを制御します。

設定

> **注:**
>
> バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

> Web Studio を使用して、次の管理タスクを実行できます。

- 認証の管理
- Studioログインページのデフォルトドメイン名を設定する
- Citrixカスタマーエクスペリエンス向上プログラム
- デリバリーコントローラーの削除
- データベースの場所を変更する
- Studio での個人設定の管理
- サイト管理の一元化
- リモートPCアクセスでの複数ユーザーの自動割り当てを有効にする
- DNS解決の有効化
- XML信頼の有効化
- セキュリティキーの管理
- Studioコンソールの非アクティブタイムアウトの設定
- サイト管理の一元化
- Studioログインページにカスタム通知を設定する(#set-a-custom-notice-on-the-studio-login-page)
- StudioログインページにアクティブなddcのFQDNを表示する(#display-the-fqdn-of-active-ddc-on-the-studio-login-page)
- ログサーバーの構成
- Microsoft Entra シングルサインオンの構成

認証の管理

デフォルトでは、ユーザーはドメインのユーザー名とパスワードを使用してWeb Studioにログオンします。スマートカード認証や統合Windows認証など、ユーザーに対して別の認証方法を選択することもできます。

Studio を使用して管理

ユーザーの認証方法を選択するには、次の手順に従います。

1. Web Studio にサインインし、左ペインで を選択します。
2. タイルを見つけて をクリックし、オプションを選択します。
    - **ドメイン資格情報**

- **ドメイン資格情報または統合 Windows 認証**

  統合 Windows 認証が有効になっている場合、ユーザーは Windows 資格情報 (Kerberos/NTLM) またはクライアント証明書を使用して Web Studio にアクセスできます。

  Web Studio と Delivery Controller™ が異なるマシンにインストールされている場合、統合 Windows 認証を機能させるには、クロスオリジンアクセスを許可し、Web Studio サーバーの URL を許可リストに追加します。

  > **重要**
  >
  > Web Studio が Delivery Controller のプロキシとして構成されている場合、統合 Windows 認証は機能しません。

- **スマートカード認証**
- **ドメイン資格情報またはスマートカード認証**

  スマートカード認証を有効にするには、追加の構成が必要です。詳細については、「Web Studio のスマートカード認証を設定する」を参照してください。

PowerShell スクリプトを使用して管理

認証方法は Delivery Controller データベースで構成されます。次の PowerShell スクリプトを使用して認証方法を設定できます。

1. Delivery Controller で次のコマンドを実行して、現在のサイト ID を取得します。

   ```
   Get-ConfigSite | Select SiteGuid
   ```

2. 以下のスクリプトを実行して認証方法を設定します。

```
# Generate a new bearer token

$bearerData = New-TrustBearerToken

# Define the Delivery Controller DNS name and Site ID

$ddc = "ddc.dc.com" # replace this with the Delivery Controller's DNS
name

$siteid = "c68a8f89-42af-4bea-a6e9-c8c936353f49" # replace this with
the site ID you get from step #1
```

```
# Define the URL and headers

$url = "https://$ddc/citrix/orchestration/api/CitrixOnPremises/Sites/
$siteid/Settings"

$headers = @{

"Content-Type" = "application/json"

"Authorization" = "Bearer $($bearerData.Token)"

}

# Define the JSON body

$body = @{

SupportedAuthenticators = "BasicAndSmartCard" # replace this with a
required authentication method: "Basic" for "Domain credentials";
"BasicAndIntegratedWindowsAuthentication" for "Domain credentials or
integrated Windows authentication"; "BasicAndSmartCard" for "Domain
credentials or smart card authentication"; "SmartCard" for "Smart card
authentication"

} | ConvertTo-Json -Depth 10

# Send the PATCH request

Invoke-RestMethod -Uri $url -Method Patch -Headers $headers -Body $body
```

統合Windows認証用にブラウザーを構成する

ドメイン資格情報または統合Windows認証を使用して*統合Windows認証*を有効にすると、次回ユーザーがサインインするときに自動的にサインインされます。ユーザーとして自動的にサインインできない場合は、以下の手順に従ってWebブラウザーを構成し、統合Windows認証を許可してください。

Google Chromeの場合：

1. コントロールパネルから、**インターネットオプション**を選択します。
2. **詳細設定**タブを選択します。

3. **統合Windows認証を有効にする**を選択します。
4. **セキュリティ**タブを選択します。
5. **ローカルイントラネット > サイト > 詳細設定**を選択します。
6. **このWebサイトをゾーンに追加する**ボックスで：
    - Web StudioとDelivery Controllerが同じサーバー上にある場合は、Web Studioを実行しているホストのURLを入力します。
    - そうでない場合は、ワイルドカードドメインを入力します。例：Delivery Controllerが `ddc.domain.com` にある場合、`*.domain.com` と入力します。
7. **追加 > 閉じる**をクリックします。

Mozilla Firefoxの場合：

1. ブラウザーから、URLボックスに `about:config` と入力します。
2. 「**検索**」ボックスに「`network negotiate`」と入力します。
3. **network.negotiate-auth.trusted-uris** を右クリックし、「**変更**」を選択します。
4. 「**文字列値を入力**」ボックスで、次のようにします。
    - Web Studio と Delivery Controller が同じサーバー上にある場合は、Web Studio をホストしているサーバー名を参照する URL および/またはエイリアスのコンマ区切りリストを追加します。
    - そうでない場合は、次のように URL を追加します。例: Delivery Controller が `ddc.domain.com` にある場合、「`*.domain.com`」と入力します。

ブラウザーを設定したら、サインインページで「**Windows 統合サインイン**」をクリックして再試行できます。

Web Studio と Delivery Controller が異なるマシンにインストールされている場合、統合 Windows 認証を機能させるには、「**クロスオリジンアクセスを許可**」を有効にする必要があります。

「**クロスオリジンアクセスを許可**」を有効にするには、次の手順に従います。

1. 「**クロスオリジンアクセスを許可**」チェックボックスをオンにします。
2. Web Studio サーバーの URL を許可リストに追加します。
3. 「**URL を入力**」フィールドに URL を入力します。必要に応じて、「**追加**」をクリックしてさらに追加します。

注

- URL は正しい形式 `<scheme>://<hostname>` に従う必要があります。パスや末尾のスラッシュを含まないようにしてください。
- IP アドレスと FQDN がサポートされています。URL を追加するときは、Web Studio へのアクセス方法と一致していることを確認してください。たとえば、IP アドレスを使用して Web Studio にアクセスする場合は、IP アドレスベースの URL をリストに追加します。
- デフォルト以外のポートを使用する場合は、ポート番号を含めるようにしてください。

4. 必要に応じて、「**追加**」をクリックしてさらに追加します。
5. 完了したら、「**完了**」をクリックして保存し、終了します。

Studioログインページのデフォルトドメイン名を設定する

Studioログインページの**ドメイン**フィールドにドメイン名を自動入力するには、次の手順に従います。

1. Web Studioにサインインし、左ペインで設定を選択します。
2. **ドメイン名の構成**タイルで、必要に応じてドメイン名を入力します。
3. **適用**をクリックします。

   管理者がStudioログインページにアクセスすると、設定したドメイン名が*ドメイン*フィールドに自動的に入力されます。

Studio で個人設定を管理する

設定ノードの下にある「**個人設定**」タブを使用して、Studio での個人の表示設定と操作設定を管理します。これらの設定は自分のアカウントにのみ適用され、他の管理者には影響しません。利用可能なオプションは次のとおりです。

- **日付と時刻**: デフォルトのタイムゾーン、日付形式、時刻形式を設定します。これらの設定は、スケジュールされた再起動や自動スケーリングなど、時刻に関連する表示のためにStudio全体で使用されます。
- **フォルダービュー**: **マシンカタログ**、**デリバリーグループ**、および**アプリケーション**ノードでフォルダービューを表示するか非表示にするかを選択します。

- **検索でのタブ順序**: **検索**ノード内のタブ順序をカスタマイズします。

Studio で優先ビューを設定するには、次の手順に従います。

1. Studio で、**設定 > 個人設定**に移動します。
2. 「**編集**」をクリックします。
3. 「**日付と時刻**」タイルで、次の形式設定を構成します。
   - **日付形式**: 日付の表示方法を選択します（例: yyyy/MM/dd）。Studio で選択した言語に関連付けられた日付形式を使用するには、「**コンソール言語に合わせる**」を選択します。
   - **時刻形式:** 12時間形式（例: 午後09:00）または24時間形式（例: 21:00）を選択します。Studioで選択した言語に関連付けられた時刻形式を使用するには、**コンソール言語に合わせる**を選択します。
   - **タイムゾーン:** 優先するタイムゾーンを選択します。コンピューターのタイムゾーンを使用するには、**コンソール言語に合わせる**を選択します。

     > **注:**
     >
     > - 日付、時刻、またはタイムゾーンにコンピューターの地域設定を使用するには、**コンソール言語に合わせる**を選択します。
     > - Studioでは、表示されている時刻にカーソルを合わせると、ローカルタイムゾーンでの同等の時刻を表示できます。
4. **フォルダービュー**タイルで、**マシンカタログ**、**デリバリーグループ**、および**アプリケーション**ノードでフォルダービューを表示するか非表示にするかを選択します。
5. **検索でのタブ順序**タイルで、**検索**ノード内のタブをドラッグして並べ替えます。
6. **適用**をクリックして、変更をすぐに保存し適用します。

DNS解決を有効にする

ICA®ファイルでIPアドレスの代わりにDNS名を表示するには、次の手順に従います。

1. Web Studioにサインインし、左側のペインで**設定**を選択します。
2. **DNS解決を有効にする**設定をオンにします。

Studioコンソールの非アクティビティタイムアウトを設定する

管理者がStudioコンソールから自動的にサインアウトされるまでの非アクティビティ期間を設定できます。

1. Web Studioにサインインし、左側のペインで**設定**を選択します。
2. 10分から24時間の範囲で期間を入力します。
3. この設定を適用するには、ページを更新するか、サインアウトしてから再度サインインします。

サイト管理の一元化

この機能を使用すると、1つのWeb Studioコンソールで複数のCitrix Virtual Apps and Desktopsサイトを管理できます。詳細については、「複数のサイト管理を有効にする」を参照してください。

Studioログインページにカスタム通知を設定する

サインインページの通知を設定するには、次の手順に従います。

1. Web Studioにサインインし、左ペインで**設定**を選択します。
2. **ログインページ通知**タイルを見つけて、**ログインページに通知を表示**チェックボックスをオンにします。
3. **編集**をクリックして**ログインページ通知**ページを開き、必要に応じてログインページ通知を入力します。
4. 「**保存**」をクリックします。

StudioログインページにアクティブなDDCのFQDNを表示する

現在のセッションで使用されているDDCのFQDNをStudioサインインページに表示するには、次の手順に従います。

1. Web Studioにサインインし、左ペインで**設定**を選択します。
2. **接続されているDelivery Controllerを表示**をオンにします。

ログサーバーを構成する

AOT (Always-on Tracing) ログサーバーを構成し、ログ記録スコープを定義します。**Director**はログサーバーに接続して、監視とトラブルシューティングのためのログを取得します。

ログサーバーを構成し、ログ記録スコープを定義するには、次の手順に従います。

1. 「**Web Studio**」にサインインし、左ペインで「**Settings**」を選択します。

2. ログサーバーが構成されていない場合は、「**Log server**」タイルで「**Add**」をクリックします。
3. 表示される「**Log server**」ページで、「**Enable log forwarding to log server**」を選択します。
4. ログをログサーバーに転送するコンポーネントを選択します。

    - **Delivery Controllerを含める:** すべてのDelivery Controllerからのログをログサーバーに転送します。
    - **デリバリーグループを選択:** 特定のデリバリーグループ内のVDAからのログをログサーバーに転送します。デフォルトでは、**すべてのデリバリーグループ**が選択されており、すべてのデリバリーグループ内のVDAからのログが転送されます。特定のデリバリーグループ内のVDAからのログのみを転送するには、**特定のデリバリーグループを選択**を選択し、含めるグループを選択します。

5. ログサーバーによって生成された**Authkey**を入力します。**Director**はこのキーを使用してログサーバーにアクセスします。
6. 「**Save**」をクリックして構成を適用します。

ログサーバーを更新するか、ログ記録スコープを変更するには、「**Settings > Log server**」タイルで「**Edit**」をクリックします。

Microsoft Entraシングルサインオン (SSO) を構成する

Microsoft Entraシングルサインオン (SSO) を設定します。SSOを構成すると、ユーザーはMicrosoft Entra参加済みまたはMicrosoft Entraハイブリッド参加済みのセッションホストで、Microsoft Entra ID資格情報を使用して仮想アプリとデスクトップにサインインできます。

> **注:**
>
> Microsoft Entra SSOは現在、Microsoft Entraハイブリッド参加済みのセッションホストでのみサポートされています。

始める前に

SSOを構成する前に:

- 必要なリソースアプリケーションを登録します。
- Microsoft Entraテナントでクライアントアプリケーションを作成します。

要件の詳細については、「Microsoft Entra single sign-on」(/ja-jp/citrix-daas/install-configure/session-authentication/entra-sso.html)を参照してください。

ワークフロー

1. **Web Studio**にサインインし、左ペインで**設定**を選択します。
2. **Microsoft Entra single sign-on (SSO)** タイルで、**Configure** をクリックします。
3. **Application (client) ID** に、クライアントアプリケーションのアプリケーションIDを入力します。 例: `12345678-1234-1234-1234-123456789abc`
4. **Redirect URI (reply URL)** に、ログオン後にユーザーをリダイレクトするURLを入力します。 例: `https://access.mycitrix.com/Citrix/MyStoreWeb`
5. **Authentication URL** に、認証エンドポイントURL (`https://login.microsoftonline.com/<tenantID>`) を入力します。 例: `https://login.microsoftonline.com/c23fc678-1bc4-1234-bd3a-123456789abc`
6. **リソースアプリケーションID URI**で、次のいずれかのオプションを選択します。
   - **商用、政府機関**、または**日本**。リソースアプリケーションID URIには、Citrixが提供する値が自動的に入力されます。
   - **カスタム**。カスタムアプリケーションID URIを入力します。
7. を選択します。

構成を保存すると、Microsoft Entra single sign-on (SSO)がサイトで有効になります。

タグ

> **注:**
>
> バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

はじめに

タグは、マシン、アプリケーション、デスクトップ、デリバリーグループ、アプリケーショングループ、ポリシーなどの項目を識別する文字列です。タグを作成して項目に追加すると、特定のタグを持つ項目にのみ適用されるように特定の操作を調整できます。

- Web Studioでの検索表示を調整します。

  たとえば、テスター向けに最適化されたアプリケーションのみを表示するには、「test」という名前のタグを作成し、それらのアプリケーションに追加（適用）します。これで、Web Studioの検索を「test」タグでフィルタリングできます。
- アプリケーショングループからアプリケーションを公開したり、デリバリーグループから特定のデスクトップを公開したりする際に、選択したデリバリーグループ内のマシンの一部のみを考慮します。これは*タグ制限*と呼ばれます。

  タグ制限を使用すると、既存のマシンを複数の公開タスクに使用できるため、より多くのマシンを展開および管理するコストを節約できます。タグ制限は、デリバリーグループ内のマシンを細分化（またはパーティション分割）するものと考えることができます。その機能は、XenApp 7.xより前のリリースにおけるワーカーグループと似ていますが、同一ではありません。

  タグ制限付きのアプリケーショングループまたはデスクトップを使用すると、デリバリーグループ内のマシンの一部を分離してトラブルシューティングする際に役立ちます。
- デリバリーグループ内のマシンの一部に対して定期的な再起動をスケジュールします。

  マシンにタグ制限を使用すると、新しいPowerShellコマンドレットを使用して、デリバリーグループ内のマシンの一部に対して複数の再起動スケジュールを構成できます。例と詳細については、「デリバリーグループの管理」を参照してください。
- 指定されたタグを持つ（または持たない）デリバリーグループ、デリバリーグループの種類、またはOU内のマシンの一部にCitrixポリシーの適用（割り当て）を調整します。

  たとえば、より強力なワークステーションにのみCitrixポリシーを適用したい場合は、それらのマシンに「high power」という名前のタグを追加します。次に、ポリシー作成ウィザードの**ポリシーの割り当て**ページで、そのタグと**有効にする**チェックボックスを選択します。デリバリーグループにタグを追加し、そのグループにCitrixポリシーを適用することもできます。詳細については、「ポリシーの作成」を参照してください。

タグは以下に適用できます。

- マシン

- アプリケーション
- マシンカタログ（PowerShellのみ。詳細については、「マシンカタログのタグ」を参照してください）
- デリバリーグループ
- アプリケーショングループ

Web Studioで以下を作成または編集する際に、タグ制限を構成できます。

- 共有デリバリーグループ内のデスクトップ
- アプリケーショングループ

> **重要:**
>
> タグは、明示的にマシンに適用することも、マシンカタログまたはデリバリーグループレベルで明示的に適用することもできます。タグがマシンカタログまたはデリバリーグループレベルで適用されると、そのカタログまたはデリバリーグループ内のすべてのマシンが暗黙的にそのタグを継承します。これらの継承されたタグは、マシンレベルで削除することはできません。タグの効果を削除するには、マシンカタログまたはデリバリーグループレベルからタグを削除する必要があります。

デスクトップまたはアプリケーショングループのタグ制限

タグ制限にはいくつかの手順があります。

- タグを作成し、マシンに追加（適用）します。
- タグ制限付きのグループを作成または編集します（つまり、「タグxを持つマシンへの起動を制限する」）。

タグ制限は、ブローカーのマシン選択プロセスを拡張します。ブローカーは、アクセスポリシー、構成されたユーザーリスト、ゾーン設定、起動準備、およびタグ制限（存在する場合）に従って、関連付けられたデリバリーグループからマシンを選択します。アプリケーションの場合、ブローカーは優先順位に従って他のデリバリーグループにフォールバックし、検討対象の各デリバリーグループに同じマシン選択ルールを適用します。

例1：シンプルなレイアウト

この例では、タグ制限を使用して、特定のデスクトップおよびアプリケーションの起動に考慮されるマシンを制限するシンプルなレイアウトを紹介します。このサイトには、1つの共有デリバ

リーグループ、1つの公開デスクトップ、および2つのアプリケーションで構成された1つのアプリケーショングループがあります。

シンプルなレイアウトでタグ制限を使用する例。(/en-us/citrix-virtual-apps-desktops/current-release/media/tags-example.png)

- 3台のマシン（VDA 101～103）のそれぞれにタグが追加されています。
- 共有デリバリーグループ内のデスクトップは、「Red」という名前のタグ制限付きで作成されました。デスクトップは、そのデリバリーグループ内で「Red」タグを持つマシン（VDA 101および102）でのみ起動できます。
- アプリケーショングループは「Orange」タグ制限付きで作成されたため、そのアプリケーション（CalculatorとNotepad）はそれぞれ、「Orange」タグを持つデリバリーグループ内のマシン（VDA 102および103）でのみ起動できます。

マシンVDA 102は両方のタグ（RedとOrange）を持っているため、アプリケーションとデスクトップの起動に考慮されます。

例2：より複雑なレイアウト

この例には、タグ制限付きで作成された複数のアプリケーショングループが含まれています。これにより、デリバリーグループのみを使用した場合に必要となるよりも少ないマシンで、より多くのアプリケーションを配信できるようになります。

例2の構成方法は、この例でタグを作成および適用し、タグ制限を構成するために使用される手順を示しています。

複雑なレイアウトでタグ制限を使用する例。(/en-us/citrix-virtual-apps-desktops/current-release/media/tags-example2.png)

この例では、10台のマシン（VDA 101～110）、1つのデリバリーグループ（D01）、および3つのアプリケーショングループ（A100、A200、A300）を使用します。各マシンにタグを適用し、各アプリケーショングループの作成時にタグ制限を指定することで、次のことが可能になります。

- グループ内の経理ユーザーは、5台のマシン（VDA 101～105）で必要なアプリにアクセスできます
- グループ内のCAD設計者は、5台のマシン（VDA 106-110）で必要なアプリにアクセスできます
- グループ内でOfficeアプリケーションを必要とするユーザーは、10台のマシン（VDA 101～110）でOfficeアプリにアクセスできます

使用されるマシンは10台のみで、デリバリーグループは1つだけです。デリバリーグループのみを使用する場合（アプリケーショングループなし）は、マシンが1つのデリバリーグループにしか属せないため、2倍の数のマシンが必要になります。

タグとタグ制限の管理

タグは、Web Studioの**［タグの管理］**アクションを通じて、選択したアイテムに対して作成、追加（適用）、編集、削除されます。

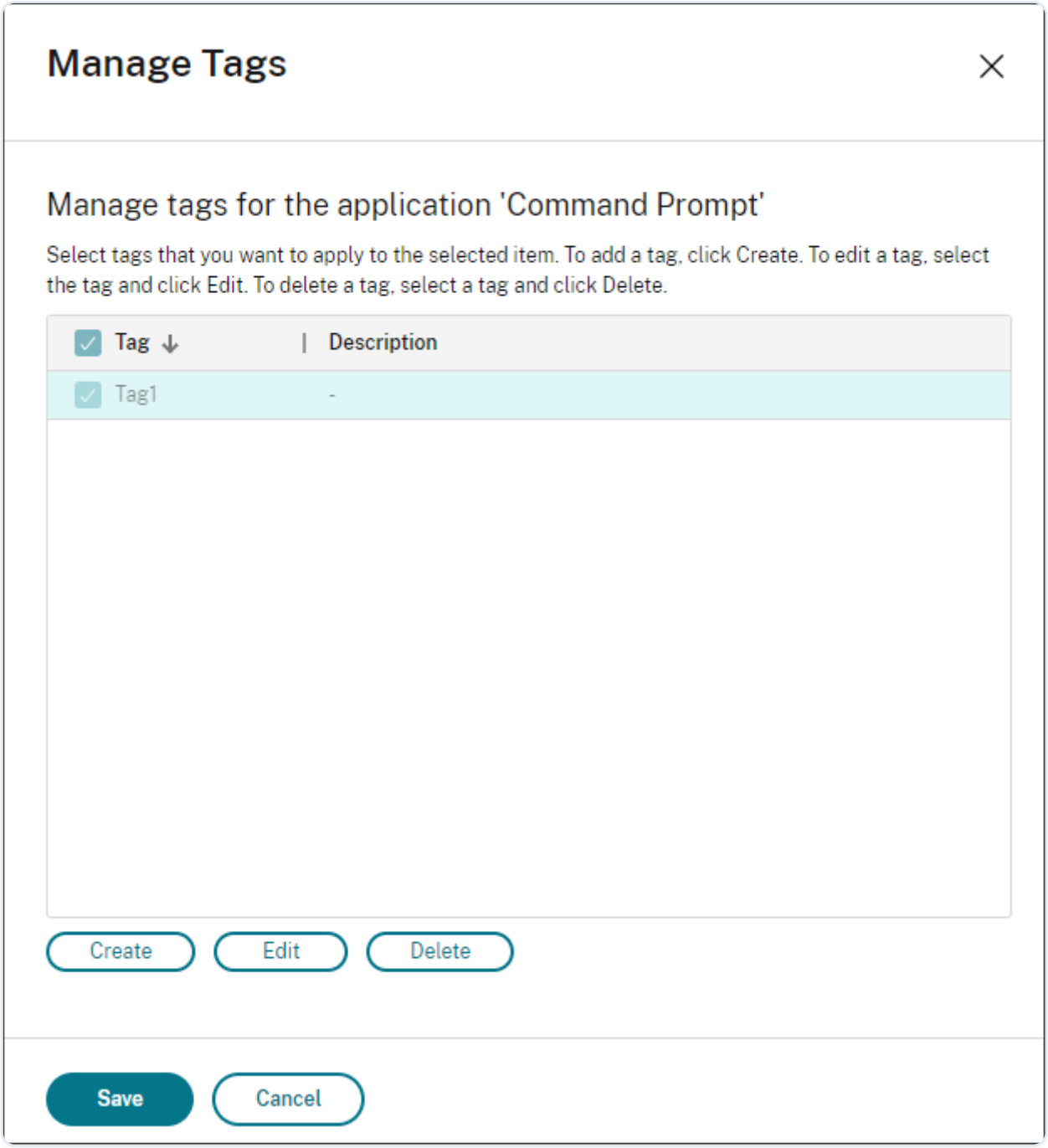
（例外：ポリシー割り当てに使用されるタグは、Web Studioの**［タグの管理］**アクションを通じて作成、編集、削除されます。ただし、タグはポリシーの作成時に適用（割り当て）されます。詳細については、「ポリシーの作成」を参照してください。）

タグ制限は、デリバリーグループでデスクトップを作成または編集するとき、およびアプリケーショングループを作成および編集するときに構成されます。

Web Studioで［タグの管理］ダイアログを使用する

Web Studioで、タグを適用するアイテム（1つまたは複数のマシン、アプリケーション、デスクトップ、デリバリーグループ、またはアプリケーショングループ）を選択し、アクションバーで**［タグの管理］**を選択します。ダイアログボックスには、選択したアイテムだけでなく、サイトで作成されたすべてのタグが一覧表示されます。

- チェックマークが付いたチェックボックスは、そのタグが選択したアイテムに既に追加されていることを示します。（以下のスクリーンショットでは、選択したマシンに「Tag1」という名前のタグが適用されています。）
- 複数のアイテムを選択した場合、ハイフンが付いたチェックボックスは、選択したアイテムの一部にのみそのタグが追加されていることを示します。



次のアクションは、**［タグの管理］**ダイアログボックスから利用できます。タグの操作に関する注意点を必ず確認してください。

- **タグを作成するには:**

  作成をクリックします。名前と説明を入力します。タグ名は一意である必要があり、大文字と小文字は区別されません。次に、**OK**をクリックします。（タグを作成しても、選択した項目に自動的に適用されるわけではありません。チェックボックスを使用してタグを適用します。）

- **1つ以上のタグを追加（適用）するには:**

タグ名の横にあるチェックボックスをオンにします。複数の項目を選択していて、タグの横にあるチェックボックスにハイフンが含まれている場合（選択した項目の一部にのみタグが適用されていることを示す）、それをチェックマークに変更すると、選択したすべてのマシンに影響します。

1つ以上のマシンにタグを追加しようとして、そのタグがアプリケーショングループで制限として使用されている場合、その操作によってそれらのマシンが起動可能になる可能性があるという警告が表示されます。それが意図したとおりであれば、続行してください。

- **1つ以上のタグを削除するには:**

  タグ名の横にあるチェックボックスをオフにします。複数の項目を選択していて、タグの横にあるチェックボックスにハイフンが含まれている場合（選択した項目の一部にのみタグが適用されていることを示す）、チェックボックスをオフにすると、選択したすべてのマシンからタグが削除されます。

  タグを制限として使用しているマシンからタグを削除しようとすると、その操作が起動対象となるマシンに影響を与える可能性があるという警告が表示されます。それが意図したとおりであれば、続行してください。

- **タグを編集するには:**

  タグを選択し、**編集**をクリックします。新しい名前、説明、またはその両方を入力します。一度に編集できるタグは1つだけです。

- **1つ以上のタグを削除するには:**

  タグを選択し、**削除**をクリックします。「タグの削除」ダイアログボックスには、現在選択されているタグを使用している項目の数が表示されます（例：「2台のマシン」）。項目をクリックすると、詳細情報が表示されます。たとえば、「2台のマシン」項目をクリックすると、そのタグが適用されている2台のマシンの名前が表示されます。タグを削除するかどうかを確認します。

  Web Studioを使用して、制限として使用されているタグを削除することはできません。まず、アプリケーショングループを編集してタグ制限を削除するか、別のタグを選択してください。

タグの管理ダイアログボックスでの作業が完了したら、**保存**をクリックします。

マシンにタグが適用されているかどうかを確認するには、左ペインで**デリバリーグループ**を選択します。中央ペインでデリバリーグループを選択し、アクションバーで**マシンの表示**を選択します。中央ペインでマシンを選択し、**詳細**ペインで**タグ**タブを選択します。

タグ制限を管理する

タグ制限の構成は複数の手順からなるプロセスです。まずタグを作成し、それをマシンに追加/適用します。次に、アプリケーショングループまたはデスクトップに制限を追加します。

- **タグを作成して適用する：**

  タグを作成し、前述の**タグの管理**アクションを使用して、タグ制限の影響を受けるマシンにそのタグを追加（適用）します。

- **アプリケーショングループにタグ制限を追加するには：**

  アプリケーショングループを作成または編集します。**デリバリーグループ**ページで、**タグを持つマシンへの起動を制限する**を選択し、リストからタグを選択します。

- **アプリケーショングループのタグ制限を変更または削除するには：**

  グループを編集します。**デリバリーグループ**ページで、リストから別のタグを選択するか、**タグを持つマシンへの起動を制限する**のチェックを外してタグ制限を完全に削除します。

- **デスクトップにタグ制限を追加するには：**

  デリバリーグループを作成または編集します。**デスクトップ**ページで、**追加**または**編集**をクリックします。「デスクトップの追加」ダイアログボックスで、**タグを持つマシンへの起動を制限する**を選択し、メニューからタグを選択します。

- **デリバリーグループのタグ制限を変更または削除するには：**

  グループを編集します。デスクトップページで、**編集**をクリックします。ダイアログボックスで、リストから別のタグを選択するか、**タグを持つマシンへの起動を制限する**のチェックを外してタグ制限を完全に削除します。

タグを使用する際の注意点

アイテムに適用されたタグはさまざまな目的に使用できるため、タグの追加、削除、および削除が意図しない影響を与える可能性があることに留意してください。Web Studioの検索フィールドでマシンの表示を並べ替えるためにタグを使用できます。アプリケーショングループまたはデスクトップを構成する際に、同じタグを制限として使用できます。タグは、そのタグを持つ指定されたデリバリーグループ内のマシンのみに起動の考慮を制限します。

デスクトップまたはアプリケーショングループのタグ制限として構成されたタグをマシンに追加しようとすると、警告が表示されます。そのタグを追加すると、マシンが追加のアプリケーションまたはデスクトップの起動に利用可能になる可能性があります。それが意図したものであれば、続行してください。そうでない場合は、操作をキャンセルできます。

例えば、「Red」タグ制限付きのアプリケーショングループを作成したとします。その後、そのアプリケーショングループで使用されているのと同じデリバリーグループに、さらにいくつかのマシンを追加します。そのマシンに「Red」タグを追加しようとすると、Web Studioは次のようなメッセージを表示します。「タグ「Red」は、以下のアプリケーショングループの制限として使用されています。このタグを追加すると、選択したマシンがこのアプリケーショングループでアプリケーションを起動できるようになる可能性があります。」その後、それらの追加マシンにそのタグを追加するかどうかを確認またはキャンセルできます。

同様に、アプリケーショングループが起動を制限するためにタグを使用している場合、Web Studioは、そのタグを制限として削除するためにグループを編集するまで、タグを削除できないことを警告します。（アプリケーショングループで制限として使用されているタグを削除することが許可された場合、そのアプリケーショングループに関連付けられているデリバリーグループ内のすべてのマシンでアプリケーションの起動が許可される可能性があります。）デスクトップの起動の制限としてタグが使用されている場合も、タグの削除に対する同じ禁止が適用されます。そのタグ制限を削除するために、アプリケーショングループまたはデリバリーグループ内のデスクトップを編集した後、タグを削除できます。

すべてのマシンが同じアプリケーションセットを持っているとは限りません。ユーザーは複数のアプリケーショングループに属することができ、それぞれ異なるタグ制限と、デリバリーグループからの異なるまたは重複するマシンセットを持っています。以下の表は、マシンの考慮事項がどのように決定されるかを示しています。

アプリケーションが追加された場合	選択されたデリバリーグループ内のこれらのマシンが起動対象と見なされます
タグ制限のない1つのアプリケーショングループ	任意のマシン。
タグ制限Aのある1つのアプリケーショングループ	タグAが適用されているマシン。
2つのアプリケーショングループ（1つはタグ制限A、もう1つはタグ制限B）	タグAとタグBを持つマシン。利用可能なマシンがない場合は、タグAまたはタグBを持つマシン。
2つのアプリケーショングループ（1つはタグ制限A、もう1つはタグ制限なし）	タグAを持つマシン。利用可能なマシンがない場合は、任意のマシン。

マシン再起動スケジュールでタグ制限を使用した場合、タグの適用または制限に影響を与える変更は、次のマシン再起動サイクルに影響します。変更が行われている間に進行中の再起動サイクルには影響しません。

例2の構成方法

以下の手順では、タグを作成して適用し、2番目の例で示されているアプリケーショングループのタグ制限を構成する手順を示します。

VDAとアプリケーションはすでにマシンにインストールされており、デリバリーグループも作成されています。

マシンにタグを作成して適用します。

1. Web Studioで、デリバリーグループD01を選択し、アクションバーで**マシンを表示**を選択します。
2. マシンVDA 101～105を選択し、アクションバーで**タグの管理**を選択します。
3. タグの管理ダイアログボックスで、**作成**をクリックし、`CADApps`という名前のタグを作成します。**OK**をクリックします。
4. もう一度**作成**をクリックし、OfficeAppsという名前のタグを作成します。**OK**をクリックします。
5. **タグの管理**ダイアログボックスにいる間に、新しく作成したタグを、各タグの名前（`CADApps`と`OfficeApps`）の横にあるチェックボックスを有効にすることで、選択したマシンに追加（適用）します。完了したら、ダイアログボックスを閉じます。
6. デリバリーグループD01を選択し、アクションバーで**マシンを表示**を選択します。
7. マシンVDA 106～110を選択し、アクションバーで**タグの管理**を選択します。
8. **タグの管理**ダイアログボックスで、**作成**をクリックします。`AcctgApps`という名前のタグを作成します。**OK**をクリックします。
9. 新しく作成した`AcctgApps`タグと`OfficeApps`タグを、各タグ名の横にあるチェックボックスをクリックして、選択したマシンに適用し、ダイアログボックスを閉じます。

タグ制限付きのアプリケーショングループを作成します。

1. Web Studioで、左ペインの**アプリケーション**を選択し、**アプリケーショングループ**タブを選択し、アクションバーで**アプリケーショングループの作成**を選択します。アプリケーショングループ作成ウィザードが起動します。
2. ウィザードの**デリバリーグループ**ページで、デリバリーグループD01を選択します。**タグを持つマシンへの起動を制限する**を選択し、リストから`AcctgApps`タグを選択します。
3. ウィザードを完了し、会計ユーザーと会計アプリケーションを指定します。(アプリケーションを追加する際は、`AcctgApps`タグを持つマシン上のアプリケーションを検索する****ソースを選択します。) ****ページで、グループに`A100`という名前を付けます。

4. 前述の手順を繰り返して、`CADApps`タグを持つマシンと、適切なユーザーおよびアプリケーションを指定し、アプリケーショングループ`A200`を作成します。
5. 手順を繰り返して、`OfficeApps`タグを持つマシンと、適切なユーザーおよびアプリケーションを指定し、アプリケーショングループ`A300`を作成します。

マシンカタログのタグ

マシンカタログでタグを使用できます。タグを作成してカタログに適用する全体的な手順は、前述のとおりです。ただし、カタログへのタグの適用はPowerShellインターフェイスを介してのみサポートされています。Web Studioを使用してカタログにタグを適用したり、カタログからタグを削除したりすることはできません。Web Studioのカタログ表示では、タグが適用されているかどうかは示されません。

概要: Web StudioまたはPowerShellを使用して、カタログで使用するタグを作成または削除できます。PowerShellを使用して、タグをカタログに適用します。

カタログでタグを使用する例をいくつか示します。

- デリバリーグループには複数のカタログのマシンが含まれていますが、特定のカタログ内のマシンのみに操作（再起動スケジュールなど）を適用したい場合があります。そのカタログにタグを適用することで、これが実現します。
- アプリケーショングループでは、アプリケーションセッションを特定のカタログ内のマシンに制限したい場合があります。そのカタログにタグを適用することで、これが実現します。

影響を受けるPowerShellコマンドレット:

- `Add-BrokerTag`や`Remove-BrokerTag`などのコマンドレットにカタログオブジェクトを渡すことができます。
- `Get-BrokerTagUsage`は、タグを含むカタログの数を示します。
- `Get-BrokerCatalog`には、`Tags`という名前のプロパティがあります。

たとえば、次のコマンドレットは、`acctg`という名前のカタログに`fy2018`という名前のタグを追加します。`Get-BrokerCatalog -Name acctg | Add-BrokerTag fy2018`。(このタグは、以前にWeb StudioまたはPowerShellを使用して作成されています。)

詳細なガイダンスと構文については、PowerShellコマンドレットのヘルプを参照してください。

自動タグ

自動タグを使用すると、マシン、アプリケーショングループ、アプリケーション、デスクトップグループ、またはデスクトップに対するタグの自動追加および削除のルールを定義できます。定義さ

れたルールを満たさない場合、タグは自動的に削除されます。この機能強化により、環境最適化のために定期的に実行されるさまざまなスクリプトを維持する必要がなくなります。

ユースケース

自動タグ付けを使用すると、コスト削減、インフラストラクチャの最適化、消費の促進など、ビジネスドライバーに関連するルールを実装できます。以下にいくつかのユースケースを示します。

- **未使用のVDIを再利用** - 事前設定された日数以上使用されていない専用ワークロードを、利用可能なプールに解放するため。
- **アプリの煩雑さを解消** - 事前設定された日数以上使用されていないアプリケーションを特定することで、アプリケーションの煩雑さを軽減するため。
- **X未満の機能レベルを持つDG** - 特定の機能レベル未満のデリバリーグループを見つけるため。
- **非アクティブユーザー** - 事前設定された日数以上ログオンしていないユーザーのリソースを再利用するため。

> **注:**
>
> 30日以上使用されていないマシンにアタッチされたタグは、ユーザーが30日後にそのマシンにログオンした場合、次回実行時にそのマシンから削除されます。

PowerShellコマンド

PowerShellコマンドを使用して自動タグを作成できます。自動タグルールが作成されると、3600秒の頻度で評価されます。詳細については、New-BrokerAutoTagRuleを参照してください。

`New-BrokerAutoTagRule`のパラメーターは次のとおりです。

- 名前: ルールの汎用名
- オブジェクトタイプ: マシン
- ルールテキスト: ルールを定義するフィルター。
- タグUid: 関連付けたいタグID。

例

1. 30日以上使用されていない専用VDIにタグを付けるには:

```
New-BrokerAutoTagRule -Name ‘UnusedVdi’ -ObjectType ‘Machine’ -RuleText
“-AllocationType Static -IsAssigned $true -Filter { SummaryState -ne
`”InUse`” -and ( LastConnectionTime -lt ‘-30’ -or LastConnectionTime
-eq `$null ) }” -TagUid 123
```

ルールが構成された後、タグ **unused-VDI** が付いたマシンは解放されます。

2. X未満の機能レベルを持つデリバリーグループにタグを付けるには (**L7_20** をしきい値機能レベルとして使用):

```
New-BrokerAutoTagRule -Name 'LowFL' -ObjectType 'DesktopGroup'
-RuleText " -Filter { MinimumFunctionalLevel -lt 'L7_20' } " -TagUid
143
```

3. フォルダーなしで公開された、ユーザーに表示されるアプリにタグを付けるには:

```
New-BrokerAutoTagRule -Name 'NoFolder' -ObjectType 'Application'
-RuleText "-Enabled $true -Filter { ClientFolder -eq $null } " -TagUid
153`
```

詳細情報

ブログ投稿: 特定のサーバーにデスクトップを割り当てる方法。

タスクセンターのタスク

Task Center は、Citrix Virtual Apps and Desktops™ のスケジュールされたタスクと定期的なタスクを一元的に表示します。Studio の単一の場所から、タスクのステータスをリアルタイムで追跡し、タスクを管理できます。

> **注:**
>
> このリリースでは、Task Center は Machine Creation Services (MCS) タスクをサポートしています。追加のタスクタイプは今後のリリースで導入される予定です。

タスクセンターへのアクセス

1. Studioコンソールを開きます。

2. 右上隅で、**カレンダー**アイコンを選択します。

   Task Center パネルが開き、タスクアクティビティが表示されます。

   タスクセンター(/en-us/citrix-virtual-apps-desktops/current-release/media/whatsnew-task-center.png)

タスクの表示と管理

Task Center では、次のことができます。

- 検索バーを使用してタスクを検索およびフィルター処理します。
- リアルタイムのタスクステータスを追跡します。
- タスクに対して、キャンセルや再実行などのアクションを実行します。

各タスクエントリには、次の詳細が表示されます。

フィールド	説明
ステータス	タスクの現在の状態: 成功、キャンセル済み、進行中、または失敗
タスクターゲット	タスクが適用されるリソース
タスクタイプ	操作の種類 (例: OSディスクのリセット、VMのバックアップ)
説明	操作の概要
タスクID	追跡用の一意の識別子

サポートされているタスクの種類

- ハードウェアの更新
- OSディスクのリセット

ユーザープロファイル

デフォルトでは、Virtual Delivery Agentをインストールすると、Citrix Profile Managementはマスターイメージにサイレントインストールされますが、プロファイルソリューションとしてProfile Managementを使用する必要はありません。

ユーザーのさまざまなニーズに合わせて、Citrix Virtual Apps and Desktops™ポリシーを使用して、各デリバリーグループのマシンに異なるプロファイル動作を適用できます。たとえば、あるデリバリーグループでは、テンプレートが1つのネットワークロケーションに保存されているCitrix強制プロファイルが必要な場合があります。一方、別のデリバリーグループでは、複数のリダイレクトされたフォルダーを持つ別のロケーションに保存されているCitrixローミングプロファイルが必要な場合があります。

- 組織内の他の管理者がCitrix Virtual Apps and Desktops™ポリシーを担当している場合は、彼らと協力して、デリバリーグループ全体でプロファイル関連のポリシーが設定されていることを確認してください。
- Profile Managementポリシーは、グループポリシー、Profile Management .iniファイル、および個々の仮想マシン上でローカルに設定することもできます。プロファイル動作を定義するこれらの複数の方法は、次の順序で読み取られます。

  a. グループポリシー（.admまたは.admxファイル）

  b. ポリシーノード内のCitrix Virtual Apps and Desktopsポリシー

  c. ユーザーが接続する仮想マシン上のローカルポリシー

  d. Profile Management .iniファイル

  たとえば、グループポリシーとポリシーノードの両方で同じポリシーを構成した場合、システムはグループポリシーのポリシー設定を読み取り、Citrix Virtual Apps and Desktopsポリシー設定を無視します。

どのプロファイルソリューションを選択しても、Director管理者は診断情報にアクセスし、ユーザープロファイルのトラブルシューティングを行うことができます。詳細については、Directorのドキュメントを参照してください。

自動構成

デスクトップの種類は、Virtual Delivery Agentのインストールに基づいて自動的に検出され、Studioで行う構成の選択に加えて、それに応じてProfile Managementのデフォルトを設定します。

Profile Managementが調整するポリシーを次の表に示します。デフォルト以外のポリシー設定はすべて保持され、この機能によって上書きされることはありません。各ポリシーの詳細については、Profile Managementのドキュメントを参照してください。プロファイルを作成するマシンの種類は、調整されるポリシーに影響します。主な要因は、マシンが永続的かプロビジョニング済みか、および複数のユーザーで共有されるか、1人のユーザー専用であるかです。

永続システムには何らかのローカルストレージがあり、その内容はシステムがオフになっても永続することが期待されます。永続システムは、SANなどのストレージテクノロジーを使用して、ローカルディスクのエミュレーションを提供する場合があります。対照的に、プロビジョニングシステムは、ベースディスクと何らかのIDディスクから「オンザフライ」で作成されます。ローカルストレージは通常、RAMディスクまたはネットワークディスクによってエミュレートされ、後者は高速リンクを備えたSANによって提供されることがよくあります。プロビジョニングテクノロジーは通常、Citrix ProvisioningまたはMachine Creation Services™（あるいはサードパーティの同等品）です。プロビジョニングシステムが永続的なローカルストレージを持つこともあります。これらは永続的として分類されます。

これら2つの要素を合わせると、以下のマシンタイプが定義されます。

- **永続的かつ専用**。例としては、Machine Creation Servicesで作成された静的割り当てと永続的なローカルストレージを持つシングルセッションOSマシン、物理ワークステーション、ラップトップなどがあります。
- **永続的かつ共有**。例としては、Machine Creation Servicesで作成されたマルチセッションOSマシン、およびCitrix Virtual Appsサーバーなどがあります。
- **プロビジョニング済みかつ専用**。例としては、静的割り当てを持つが永続ストレージを持たないシングルセッションOSマシンで、Citrix Provisioning Service (Citrix Virtual Desktops™内) で作成されたものなどがあります。
- **プロビジョニング済みかつ共有**。例としては、ランダム割り当てを持つシングルセッションOSマシンで、Citrix Provisioning™ Service (Citrix Virtual Desktops内) で作成されたもの、およびCitrix Virtual Appsサーバーなどがあります。

以下のProfile Managementポリシー設定は、異なるマシンタイプに対する推奨ガイドラインです。ほとんどの場合にうまく機能しますが、展開の要件に応じてこれらから逸脱することもできます。

> **重要:**
>
> **ログオフ時にローカルにキャッシュされたプロファイルを削除、プロファイルストリーミング**、および**常にキャッシュ**は、自動構成機能によって適用されます。その他のポリシーは手動で調整してください。

永続マシン

ポリシー	永続的かつ専用	永続的かつ共有
ログオフ時にローカルにキャッシュされたプロファイルを削除する	無効	有効
プロファイルストリーミング	無効	有効
常にキャッシュ	有効 (注1)	無効 (注2)
アクティブライトバック	無効	無効 (注3)
ローカル管理者によるログオンの処理	有効	無効 (注4)

プロビジョニング済みマシン

ポリシー	プロビジョニング済みと専用の両方	プロビジョニング済みと共有の両方
ログオフ時にローカルにキャッシュされたプロファイルを削除する	無効 (注5)	有効
プロファイルストリーミング	有効	有効
常にキャッシュ	無効 (注6)	無効
アクティブライトバック	有効	有効
ローカル管理者によるログオンの処理	有効	有効 (注7)

1. このマシンタイプでは**Profile streaming**が無効になっているため、**Always cache**設定は常に無視されます。
2. **Always cache**を無効にします。ただし、このポリシーを有効にし、ファイルサイズ制限 (MB単位) を定義することで、ログオン後できるだけ早く大きなファイルがプロファイルにロードされるようにすることができます。このサイズ以上のファイルは、できるだけ早くローカルにキャッシュされます。

3. Citrix Virtual Appsサーバー間をローミングするユーザーのプロファイルに変更を保存する場合を除き、**Active write back**を無効にします。この場合は、このポリシーを有効にします。
4. ホスト型共有デスクトップの場合を除き、**Process logons of local administrators**を無効にします。この場合は、このポリシーを有効にします。
5. **Delete locally cached profiles on logoff**を無効にします。この設定は、ローカルにキャッシュされたプロファイルを保持します。マシンはログオフ時にリセットされますが、個々のユーザーに割り当てられているため、プロファイルがキャッシュされているとログオンが高速になります。
6. **Always cache**を無効にします。ただし、このポリシーを有効にし、ファイルサイズ制限 (MB単位) を定義することで、ログオン後できるだけ早く大きなファイルがプロファイルにロードされるようにすることができます。このサイズ以上のファイルは、できるだけ早くローカルにキャッシュされます。
7. Citrix Virtual Apps and Desktopsサーバー間をローミングするユーザーのプロファイルの場合を除き、**Process logons of local administrators**を有効にします。この場合は、このポリシーを無効にします。

フォルダーリダイレクト

フォルダーリダイレクトを使用すると、プロファイルが保存されている場所とは異なるネットワーク共有にユーザーデータを保存できます。フォルダーリダイレクトはプロファイルのサイズとロード時間を削減しますが、ネットワーク帯域幅に影響を与える可能性があります。フォルダーリダイレクトは、Citrixユーザープロファイルが使用されていることを必要としません。独自のユーザープロファイルを管理し、フォルダーをリダイレクトすることもできます。

StudioのCitrixポリシーを使用してフォルダーリダイレクトを構成します。

- リダイレクトされたフォルダーのコンテンツを保存するために使用されるネットワークの場所が利用可能であり、適切な権限を持っていることを確認してください。場所のプロパティは検証されます。
- リダイレクトされたフォルダーはネットワーク上に設定され、その内容はログオン時にユーザーの仮想デスクトップから取り込まれます。

フォルダーリダイレクトは、CitrixポリシーまたはActive Directoryグループポリシーオブジェクトのいずれか一方のみを使用して構成し、両方は使用しないでください。両方のポリシーエンジンを使用してフォルダーリダイレクトを構成すると、予期しない動作が発生する可能性があります。

高度なフォルダーリダイレクト

複数のオペレーティングシステム（OS）を使用する展開では、ユーザープロファイルの一部を各OSで共有したい場合があります。プロファイルの残りの部分は共有されず、1つのOSでのみ使用されます。OS間で一貫したユーザーエクスペリエンスを確保するには、各OSで異なる構成、つまり高度なフォルダーリダイレクトが必要です。たとえば、2つのOSで実行されているアプリケーションの異なるバージョンが共有ファイルを読み取ったり編集したりする必要がある場合、両方のバージョンがアクセスできる単一のネットワーク場所にリダイレクトすることを選択できます。あるいは、**スタートメニュー**フォルダーの内容が2つのOSで異なる構造になっているため、両方ではなく1つのフォルダーのみをリダイレクトすることを選択できます。このアプローチにより、各OSで**スタートメニュー**フォルダーとその内容が分離され、ユーザーに一貫したエクスペリエンスが保証されます。

展開で高度なフォルダーリダイレクトが必要な場合は、ユーザーのプロファイルデータの構造を理解し、そのどの部分をOS間で共有できるかを判断する必要があります。フォルダーリダイレクトが正しく使用されないと、予期しない動作が発生する可能性があります。

高度な展開でフォルダーをリダイレクトするには：

- 各OSに個別のデリバリーグループを使用します。
- 仮想デスクトップ上の仮想アプリケーションを含む、仮想アプリケーションがユーザーデータと設定をどこに保存するか、およびデータがどのように構造化されているかを理解します。
- 安全にローミングできる共有プロファイルデータ（各OSで同じ構造であるため）については、各デリバリーグループ内のコンテナフォルダーをリダイレクトします。
- ローミングできない非共有プロファイルデータについては、デスクトップグループのいずれか1つ（通常は最も使用されているOSまたはデータが最も関連性の高いOS）のコンテナフォルダーをリダイレクトします。あるいは、OS間でローミングできない非共有データについては、両方のシステムのコンテナフォルダーを別々のネットワーク場所にリダイレクトします。

高度な展開の例

この展開には、Windows 10デスクトップで実行されるMicrosoft OutlookおよびInternet Explorerのバージョンを含むアプリケーションと、Windows Server 2019によって配信されるOutlookおよびInternet Explorerの他のバージョンを含むアプリケーションがあります。2つのOS用に2つのデリバリーグループを既に設定しています。ユーザーは、両方のアプリケーションのバージョンで同じ**連絡先**と**お気に入り**のセットにアクセスしたいと考えています。

重要： 以下の決定とアドバイスは、説明されているOSと展開に有効です。組織では、リダイレクトするフォルダーとそれらを共有するかどうかの決定は、特定の展開に固有のさまざまな要因によって異なります。

- デリバリーグループに適用されるポリシーを使用して、次のフォルダーをリダイレクトするように選択します。

フォルダ	WINDOWS 10でリダイレクトされますか？	WINDOWS SERVER 2019でリダイレクトされますか？
マイドキュメント	はい	はい
アプリケーションデータ	いいえ	いいえ
連絡先	はい	はい
デスクトップ	はい	いいえ
ダウンロード	いいえ	いいえ
お気に入り	はい	はい
リンク	はい	いいえ
マイミュージック	はい	はい
マイピクチャ	はい	はい
マイビデオ	はい	はい
検索	はい	いいえ
保存されたゲーム	いいえ	いいえ
スタートメニュー	はい	いいえ

- 共有され、リダイレクトされるフォルダーの場合：
  - OutlookとInternet Explorerの異なるバージョンによって保存されたデータの構造を分析した結果、**連絡先**フォルダーと**お気に入り**フォルダーを共有しても安全であると判断しました。
  - **マイドキュメント**、**マイミュージック**、**マイピクチャ**、**マイビデオ**フォルダーの構造はOS間で標準的であることがわかっています。そのため、これらのフォルダーを各デリバリーグループで同じネットワークロケーションに保存しても安全です。
- 共有されない、リダイレクトされるフォルダーの場合：

  - Windows Serverデリバリーグループでは、デスクトップ、リンク、検索、または**スタートメニュー**フォルダーをリダイレクトしません。これらのフォルダー内のデータは2つのOSで異なる方法で整理されているためです。したがって、共有することはできません。
  - この共有されないデータの予測可能な動作を保証するために、Windows 10デリバリーグループでのみリダイレクトします。Windows 10は、ユーザーが日常業務でより頻繁に使用します。ユーザーはWindows Serverによって提供されるアプリケーションにたまにしかアクセスしません。また、この場合、共有されないデータはアプリケーション環境よりもデスクトップ環境により関連性が高くなります。たとえば、デスクトップショートカットは**デスクトップ**フォルダーに保存され、Windows 10マシンから作成されたものであれば役立つ可能性がありますが、Windows Serverマシンから作成されたものではありません。

- リダイレクトされないフォルダーの場合:
  - ユーザーがダウンロードしたファイルでサーバーを煩雑にしたくないため、ダウンロードフォルダーをリダイレクトしないことを選択します
  - 個々のアプリケーションからのデータは互換性やパフォーマンスの問題を引き起こす可能性があるため、アプリケーションデータフォルダーをリダイレクトしないことを決定します

フォルダーリダイレクトの詳細については、「フォルダーリダイレクト、オフラインファイル、および移動ユーザープロファイルの概要」を参照してください。

フォルダーリダイレクトと除外

Citrix Profile Management（Studioではない）では、パフォーマンス強化により、除外を使用してフォルダーが処理されないようにすることができます。この機能を使用する場合、リダイレクトされたフォルダーを除外しないでください。フォルダーリダイレクト機能と除外機能は連携して動作します。リダイレクトされたフォルダーが除外されないようにすることで、後でリダイレクトしないと決定した場合でも、Profile Managementはそれらをプロファイルフォルダー構造に戻し、データの整合性を維持できます。除外の詳細については、「項目の含める/除外」を参照してください。

VDA登録

はじめに

> **注:**

> オンプレミス環境では、VDAはDelivery Controllerに登録します。Citrix Cloudサービス環境では、VDAはCloud Connectorに登録します。ハイブリッド環境では、一部のVDAはDelivery Controllerに登録し、他のVDAはCloud Connectorに登録します。

> VDAを使用する前に、サイト上の1つ以上のControllerまたはCloud Connectorに登録（通信を確立）する必要があります。VDAは、`ListofDDCs`と呼ばれるリストを確認して、ControllerまたはConnectorを見つけます。VDA上の`ListOfDDCs`には、そのVDAをサイト上のControllerまたはCloud Connectorにポイントするエントリが含まれています。負荷分散のために、VDAはリスト内のすべてのControllerまたはCloud Connectorに接続を自動的に分散します。

VDA登録がそれほど重要であるのはなぜですか？

- セキュリティの観点から、登録は機密性の高い操作です。ControllerまたはCloud ConnectorとVDAの間で接続を確立しています。このような機密性の高い操作では、すべてが完璧な状態でない場合、接続を拒否するのが期待される動作です。事実上、VDAからControllerまたはCloud Connectorへ、およびControllerまたはCloud ConnectorからVDAへの2つの別々の通信チャネルを確立しています。接続にはKerberosが使用されるため、時刻同期とドメインメンバーシップの問題は許容されません。Kerberosはサービスプリンシパル名（SPN）を使用するため、負荷分散されたIP\ホスト名を使用することはできません。
- Controller（またはCloud Connector）を追加および削除する際に、VDAが正確で最新のControllerまたはCloud Connector情報を持っていない場合、VDAは、リストにないControllerまたはCloud Connectorによって仲介されるセッション起動を拒否する可能性があります。無効なエントリは、仮想デスクトップシステムソフトウェアの起動を遅らせる可能性があります。VDAは、不明で信頼できないControllerまたはCloud Connectorからの接続を受け入れません。

`ListofDDCs`に加えて、`ListOfSIDs`（セキュリティID）は、`ListofDDCs`内のどのマシンが信頼されているかを示します。`ListofSIDs`は、Active Directoryの負荷を軽減したり、侵害されたDNSサーバーからの潜在的なセキュリティ脅威を回避したりするために使用できます。詳細については、ListOfSIDsを参照してください。

`ListofDDCs`が複数のControllerまたはCloud Connectorを指定している場合、VDAはランダムな順序でそれらに接続しようとします。オンプレミス展開では、`ListofDDCs`にはControllerグループも含まれる場合があります。VDAは、`ListofDDCs`内の他のエントリに移動する前に、グループ内の各Controllerに接続しようとします。

Citrix Virtual Apps and Desktops™は、VDAのインストール中に構成されたControllerまたはCloud Connectorへの接続を自動的にテストします。ControllerまたはCloud Connectorに到達できない場合、エラーが表示されます。ControllerまたはCloud Connectorに接続できないという警告を無視し

た場合（またはVDAのインストール中にControllerまたはCloud Connectorのアドレスを指定しなかった場合）、メッセージが表示されて通知されます。

ControllerまたはCloud Connectorアドレスを構成する方法

管理者は、VDAが初めて登録するとき（初回登録）に使用する構成方法を選択します。初回登録中に、VDA上に永続的なキャッシュが作成されます。その後の登録では、構成の変更が検出されない限り、VDAはこのローカルキャッシュからControllerまたはCloud Connectorのリストを取得します。

その後の登録でそのリストを取得する最も簡単な方法は、自動更新機能を使用することです。自動更新はデフォルトで有効になっています。詳細については、「自動更新」を参照してください。

VDA上でControllerまたはCloud Connectorアドレスを構成する方法はいくつかあります。

- ポリシーベース（LGPOまたはGPO）
- レジストリベース（手動、グループポリシー設定（GPP）、VDAインストール時に指定）
- Active Directory OUベース（レガシーOU検出）
- MCSベース (personality.ini)

VDAをインストールする際に、初期登録方法を指定します。(自動更新を無効にした場合、VDAインストール時に選択した方法がその後の登録に使用されます。)

次の図は、VDAインストールウィザードの**Delivery Controller**ページを示しています。

VDAインストールウィザードのDelivery Controllerページ(/en-us/citrix-virtual-apps-desktops/current-release/media/vda-install-controllers-all.png)

ポリシーベース (LGPO\\GPO)

Citrix®は、初期VDA登録にGPOを使用することを推奨します。これは最も高い優先順位を持ちます。(自動更新が最も高い優先順位としてリストされていますが、自動更新は初期登録後にのみ使用されます。) ポリシーベースの登録は、構成にグループポリシーを使用することによる一元化の利点を提供します。

この方法を指定するには、以下の両方の手順を完了します。

- VDAインストールウィザードの**Delivery Controller**ページで、**後で実行 (詳細設定)** を選択します。VDAインストール中にControllerアドレスを指定しない場合でも、ウィザードはControllerアドレスを指定するよう何度か通知します。(VDA登録はそれほど重要です。)

- `Virtual Delivery Agent Settings > Controllers`設定を使用して、Citrixポリシーを介してポリシーベースのVDA登録を有効または無効にします。(セキュリティが最優先事項である場合は、`Virtual Delivery Agent Settings > Controller SIDs`設定を使用します。)

この設定は`HKLM\Software\Policies\Citrix\VirtualDesktopAgent (ListOfDDCs)`に保存されます。

レジストリベース

この方法を指定するには、以下のいずれかの手順を完了します。

- VDAインストールウィザードの**Delivery Controller**ページで、**手動で実行** を選択します。次に、インストールされているControllerのFQDNを入力し、**追加** をクリックします。複数のControllerをインストールしている場合は、それらのアドレスを追加します。
- コマンドラインVDAインストールの場合、/controllersオプションを使用し、インストールされているControllerまたはCloud ConnectorのFQDNを指定します。

この情報は、レジストリキー`HKLM\Software\Citrix\VirtualDesktopAgent`または`HKLM\Software\Wow6432Node\Citrix\VirtualDesktopAgent`の下のレジストリ値`ListOfDDCs`に保存されます。

このレジストリキーを手動で構成することも、グループポリシー設定 (GPP) を使用することもできます。この方法は、ポリシーベースの方法よりも好ましい場合があります (たとえば、異なるControllerまたはCloud Connectorの条件付き処理が必要な場合。例: XDW-001-で始まるコンピューター名にはXDC-001を使用する)。

`ListOfDDCs` レジストリキーを更新します。このキーには、サイト内のすべてのControllerまたはCloud ConnectorのFQDNが一覧表示されます。(このキーはActive DirectoryサイトOUに相当します。)

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfDDCs (REG_SZ)`

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent` レジストリの場所に`ListOfDDCs` と `FarmGUID` の両方のキーが含まれている場合、ControllerまたはCloud Connectorの検出には `ListOfDDCs` が使用されます。VDAのインストール中にサイトOUが指定された場合、`FarmGUID` が存在します。(これはレガシー展開で使用される場合があります。)

オプションで、`ListOfSIDs` レジストリキーを更新します (詳細については、「ListOfSIDs」を参照してください)。

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs (REG_SZ)`

注意: Citrixポリシーを介してポリシーベースのVDA登録も有効にする場合、ポリシーはより優先度の高い方法であるため、VDAインストール時に指定した設定は上書きされます。

Active Directory OUベース (レガシー)

この方法は主に下位互換性のためにサポートされており、推奨されません。まだこの方法を使用している場合は、別の方法に変更することをお勧めします。

この方法を指定するには、以下の両方の手順を完了します。

- VDAインストールウィザードの **Delivery Controller** ページで、**Active Directoryから場所を選択** を選択します。
- `Set-ADControllerDiscovery.ps1` スクリプト (すべてのControllerで利用可能) を使用します。また、各VDAで `FarmGuid` レジストリエントリを構成して、適切なOUを指すようにします。この設定はグループポリシーを使用して構成できます。

MCSベース

MCSを使用してVMをプロビジョニングする場合、MCSはControllerまたはCloud Connectorのリストを設定します。この機能は自動更新と連携します。カタログの作成時、MCSは初期プロビジョニング中にControllerまたはCloud Connectorのリストを `Personality.ini` ファイルに挿入します。自動更新により、リストは最新の状態に保たれます。

この方法を指定するには、VDAインストールウィザードの **Delivery Controller** ページで、**Machine Creation Services™に任せる** を選択します。

レビューと推奨事項

ベストプラクティスとして:

- 初期登録にはグループポリシー登録方法を使用します。
- 自動更新（デフォルトで有効）を使用して、Controller のリストを最新の状態に保ちます。
- マルチゾーン展開では、初期構成にはグループポリシーを使用します（Controller または Cloud Connector が少なくとも2つある場合）。VDA を、そのゾーン内のローカルな Controller または Cloud Connector に向けます。自動更新を使用して、それらを最新の状態に保ちます。自動更新は、サテライトゾーンの VDA の `ListofDDCs` を自動的に最適化します。
- Controller が利用できない場合の登録問題を回避するために、`ListOfDDCs` レジストリキーに複数の Controller をスペースで区切ってリストします。例:

```
DDC7x.xd.local DDC7xHA.xd.local



32-bit: HKEY_LOCAL_MACHINE
\Software\Citrix\VirtualDesktopAgent\ListOfDDCs



HKEY_LOCAL_MACHINE \Software\Citrix\VirtualDesktopAgent\ListOfDDCs
(REG_SZ)
```

- `ListofDDCs` の下にリストされているすべての値が有効な完全修飾ドメイン名にマッピングされていることを確認し、起動時の登録遅延を防ぎます。

自動更新

自動更新（XenApp および XenDesktop 7.6 で導入）は、デフォルトで有効になっています。これは、VDA 登録を最新の状態に保つための最も効率的な方法です。初期登録には使用されませんが、初期登録時に自動更新ソフトウェアが `ListofDDCs` をダウンロードし、VDA 上の永続キャッシュに保存します。このプロセスは、各 VDA に対して実行されます。キャッシュにはマシンポリシー情報も保持され、ポリシー設定が再起動後も維持されるようにします。

自動更新は、MCS または Citrix Provisioning™ を使用してマシンをプロビジョニングする場合にサポートされます。ただし、Citrix Provisioning のサーバー側キャッシュは除きます。サーバー側キャッシュは、自動更新キャッシュ用の永続ストレージがないため、一般的なシナリオではありません。

この方法を指定するには:

- 設定 `Virtual Delivery Agent Settings > Enable auto update of Controllers` を含む Citrix ポリシーを通じて、自動更新を有効または無効にします。この設定はデフォルトで有効になっています。

仕組み:

- VDA が再登録されるたびに（たとえば、マシンの再起動後）、キャッシュが更新されます。各 Controller または Cloud Connector も、90分ごとにサイトデータベースをチェックします。前回のチェック以降に Controller または Cloud Connector が追加または削除された場合、あるいは VDA 登録に影響するポリシー変更が発生した場合、Controller または Cloud Connector は登録済みの VDA に更新されたリストを送信し、キャッシュが更新されます。VDA は、最新の

キャッシュされたリストにあるすべての Controller または Cloud Connector からの接続を受け入れます。

- VDA が、登録されている Controller または Cloud Connector を含まないリストを受け取った場合（つまり、その Controller または Cloud Connector がサイトから削除された場合）、VDA は、`ListofDDCs` 内の Controller または Cloud Connector の中から選択して再登録します。

例:

- 展開には、A、B、C の3つの Controller があります。VDA は Controller B に登録されます（これは VDA のインストール中に指定されました）。
- その後、2つの Controller（D と E）がサイトに追加されます。90分以内に、VDA は更新されたリストを受け取り、Controller A、B、C、D、E からの接続を受け入れます。（VDA が再起動されるまで、負荷はすべての Controller に均等に分散されません。）
- さらにその後、Controller B が別のサイトに移動されます。90分以内に、元のサイトの VDA は、前回のチェック以降に Controller の変更があったため、更新されたリストを受け取ります。元々 Controller B に登録されていた VDA（リストにはもうありません）は、現在のリスト（A、C、D、E）にある Controller の中から選択して再登録します。

マルチゾーン展開では、サテライトゾーンの自動更新は、まずすべてのローカル Controller を自動的にキャッシュします。プライマリゾーンのすべての Controller は、バックアップグループにキャッシュされます。サテライトゾーンにローカル Controller が利用できない場合、プライマリゾーンの Controller で登録が試行されます。

次の例に示すように、キャッシュファイルにはホスト名とセキュリティIDのリスト（`ListofSIDs`）が含まれています。VDAはSIDを照会しないため、Active Directoryの負荷が軽減されます。

VDAの登録キャッシュファイルの例(/en-us/citrix-virtual-apps-desktops/current-release/media/vda-registration-cache-file.png)

キャッシュファイルはWMI呼び出しで取得できます。ただし、SYSTEMアカウントのみが読み取り可能な場所に保存されています。

> **重要:**
>
> この情報は情報提供のみを目的としています。このファイルを変更しないでください。このファイルまたはフォルダーへの変更は、サポートされていない構成になります。

```
Get-WmiObject -Namespace "Root\Citrix\DesktopInformation" -Class
"Citrix_VirtualDesktopInfo" -Property "PersistentDataLocation"
```

セキュリティ上の理由から (Active Directoryの負荷軽減とは別に) `ListofSIDs` を手動で構成する必要がある場合、自動更新機能は使用できません。詳細については、ListOfSIDs を参照してください。

自動更新の優先順位の例外

自動更新は通常、すべてのVDA登録方法の中で最も高い優先順位を持ち、他の方法の設定を上書きしますが、例外があります。キャッシュ内の `NonAutoListOfDDCs` 要素は、初期VDA構成方法を指定します。自動更新はこの情報を監視します。初期登録方法が変更された場合、登録プロセスは自動更新をスキップし、次に高い優先順位で構成された方法を使用します。このプロセスは、VDAを別のサイトに移動する場合 (たとえば、ディザスターリカバリー中) に役立ちます。

構成に関する考慮事項

一般的なVDA登録構成を表示します。

<iframe src="https://www.youtube.com/embed/MgGMZp4SnZgEq9ieibQc9j" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
VDA登録手順を表示します。

<iframe src="https://www.youtube.com/embed/iwsbajSVY5QvoUTh6m7AjG" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
VDA登録に影響を与える可能性のある項目を構成する際は、次の点を考慮してください。

ControllerまたはCloud Connectorのアドレス

ControllerまたはCloud Connectorを指定するためにどの方法を使用するかにかかわらず、CitrixはFQDNアドレスを使用することを推奨します。IPアドレスはDNSレコードよりも侵害されやすいため、信頼できる構成とは見なされません。`ListofSIDs` を手動で入力する場合、`ListofDDCs` でIPを使用できます。ただし、FQDNが引き続き推奨されます。

負荷分散

前述のとおり、VDAは `ListofDDCs` 内のすべてのControllerまたはCloud Connectorに接続を自動的に分散します。フェールオーバーと負荷分散機能は、Citrix Brokering Protocol (CBP) に組み込まれています。構成で複数のControllerまたはCloud Connectorを指定した場合、必要に応じて登録はそれらの間で自動的にフェールオーバーします。自動更新により、すべてのVDAで自動フェールオーバーが自動的に発生します。

セキュリティ上の理由から、Citrix ADCなどのネットワークロードバランサーを使用することはできません。VDA登録はKerberos相互認証を使用します。この認証では、クライアント (VDA) がサービス (Controller) に対して自身のIDを証明する必要があります。ただし、ControllerまたはCloud ConnectorもVDAに対して自身のIDを証明する必要があります。これは、VDAとControllerまたはCloud Connectorが同時にサーバーとクライアントとして機能することを意味します。この記事の冒頭で述べたように、VDAからController/Cloud Connectorへ、およびController/Cloud ConnectorからVDAへの2つの通信チャネルがあります。

このプロセスにおけるコンポーネントは、サービスプリンシパル名 (SPN) と呼ばれ、Active Directoryコンピューターオブジェクトのプロパティとして保存されます。VDAがControllerまたはCloud Connectorに接続するときは、通信相手を指定する必要があります。このアドレスがSPNです。負荷分散されたIPを使用する場合、相互Kerberos認証は、そのIPが予期されたControllerまたはCloud Connectorに属していないことを正しく認識します。

詳細については、以下を参照してください。

- Kerberosの概要
- Kerberosを使用した相互認証

自動更新によるCNAMEの置き換え

自動更新機能は、XenAppおよびXenDesktop 7.xより前のバージョンにおけるCNAME (DNSエイリアス) 機能を置き換えます。CNAME機能は、XenAppおよびXenDesktop 7以降では無効になっています。CNAMEの代わりに自動更新を使用してください。(CNAMEを使用する必要がある場合は、CTX137960を参照してください。DNSエイリアスを常に機能させるには、自動更新とCNAMEを同時に使用しないでください。)

Controller/Cloud Connectorグループ

特定のシナリオでは、ControllerまたはCloud Connectorをグループで処理し、一方のグループを優先し、すべてのController/Cloud Connectorが失敗した場合に他方のグループをフェールオーバーに使用したい場合があります。ControllerまたはCloud Connectorはリストからランダムに選択されるため、グループ化することで優先的な使用を強制するのに役立ちます。

これらのグループは、単一のサイト内での使用を目的としています（複数のサイトではありません）。

Controller/Cloud Connectorのグループを指定するには、かっこを使用します。たとえば、4つのController（プライマリ2つとバックアップ2つ）がある場合、グループ化は次のようになります。

```
(XDC-001.cdz.lan XDC-002.cdz.lan) (XDC-003.cdz.lan XDC-004.cdz.lan)
```

この例では、最初のグループのController（001と002）が最初に処理されます。両方が失敗した場合、2番目のグループのController（003と004）が処理されます。

XenDesktop 7.0以降の場合、**登録グループ**機能を使用するには、追加の手順を実行する必要があります。Studioから**Controllerの自動更新を有効にする**ポリシーを**禁止**する必要があります。

ListOfSIDs

VDAが登録のために連絡できるControllerのリストは`ListofDDCs`です。VDAは、`ListofDDCs`内のControllerを自動的に信頼しないため、どのControllerを信頼すべきかも知る必要があります。`ListofSIDs`（セキュリティID）は、信頼されたControllerを識別します。VDAは、信頼されたControllerとのみ登録を試みます。

ほとんどの環境では、`ListofSIDs`は`ListofDDCs`から自動的に生成されます。CDFトレースを使用して`ListofSIDs`を読み取ることができます。

一般的に、`ListofSIDs`を手動で変更する必要はありません。いくつかの例外があります。最初の2つの例外は、新しいテクノロジーが利用可能になったため、もはや有効ではありません。

- **Controller の役割の分離:** XenApp および XenDesktop 7.7 でゾーンが導入される前は、Controller の一部のみが登録に使用される場合、`ListofSIDs` は手動で構成されていました。たとえば、XDC-001 と XDC-002 を XML ブローカーとして使用し、XDC-003 と XDC-004 を VDA 登録に使用する場合、すべての Controller を `ListofSIDs` に、XDC-003 と XDC-004 を `ListofDDCs` に指定していました。これは一般的または推奨される構成ではありません。新しい環境では使用しないでください。代わりにゾーンを使用してください。
- **Active Directory の負荷軽減:** XenApp および XenDesktop 7.6 で自動更新機能が導入される前は、ドメインコントローラーの負荷を軽減するために `ListofSIDs` が使用されていました。`ListofSIDs` を事前に入力することで、DNS 名から SID への解決をスキップできます。ただし、この永続キャッシュには SID が含まれているため、自動更新機能によりこの作業は不要になります。Citrix は自動更新機能を有効にしておくことを推奨します。
- **セキュリティ:** 一部の高度に保護された環境では、侵害された DNS サーバーからの潜在的なセキュリティ脅威を回避するために、信頼された Controller の SID が手動で構成されていました。ただし、これを行う場合は、自動更新機能も無効にする必要があります。そうしないと、永続キャッシュからの構成が使用されます。

したがって、特別な理由がない限り、`ListofSIDs` を変更しないでください。

`ListofSIDs` を変更する必要がある場合は、`HKLM\Software\Citrix\VirtualDesktopAgent` の下に `ListOfSIDs (REG_SZ)` という名前のレジストリキーを作成します。値は信頼された SID のリストで、複数ある場合はスペースで区切ります。

次の例では、1 つの Controller が VDA 登録 (`ListofDDCs`) に使用されていますが、2 つの Controller がブローカー処理 (List OfSIDs) に使用されています。

登録とブローカー処理に使用される異なる Controller の例(/en-us/citrix-virtual-apps-desktops/current-release/media/vda-registration-listofsids.png)

VDA 登録中の Controller 検索

VDA が登録を試行すると、Broker Agent はまずローカルドメインで DNS ルックアップを実行し、指定された Controller に到達できることを確認します。

最初のルックアップで Controller が見つからない場合、Broker Agent は AD でフォールバックのトップダウンクエリを開始できます。このクエリはすべてのドメインを検索し、頻繁に繰り返されます。Controller アドレスが無効な場合 (たとえば、管理者が VDA のインストール時に誤った FQDN を入力した場合)、そのクエリのアクティビティがドメインコントローラーで分散型サービス拒否 (DDoS) 状態を引き起こす可能性があります。

次のレジストリキーは、Broker Agent が最初の検索中に Controller を見つけられない場合に、フォールバックのトップダウンクエリを使用するかどうかを制御します。

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent`

- 名前: `DisableDdcWildcardNameLookup`
- 種類: `DWORD`
- 値: `0` (デフォルト) または任意のゼロ以外の値

`0` に設定すると、フォールバック検索が有効になります。Controller の最初の検索が失敗した場合、フォールバックのトップダウン検索が開始されます。これはデフォルトの動作です。ただし、ゼロ以外の値に設定すると、フォールバック検索は無効になります。Controller の最初の検索が失敗した場合、Broker Agent は検索を停止します。

読み取り専用ドメインコントローラーを使用した VDA 登録中の LDAP バインディングシーケンス

VDA が読み取り専用ドメインコントローラー (RODC) に登録する場合、Broker Agent は無視する Light Directory Access Protocol (LDAP) バインディングを選択する必要があります。この選択を行うには、Broker Agent に適切なレジストリキーが必要です。

レジストリキーが指定されていない場合、またはレジストリキーフィールドが空の場合、RODCへのVDA登録は、元のLDAPバインディングシーケンスを経由する必要があるため、時間がかかります。

LDAPバインディングシーケンスを変更するために、レジストリキー`ListofIgnoredBindings`が`HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent`に追加されました。`ListofIgnoredBindings`を使用すると、必要に応じてLDAPバインディングシーケンスを変更でき、RODCへのVDA登録を高速化できます。

- 名前: `ListofIgnoredBindings`
- 種類: `REG_SZ`
- 値: `DefaultPath`、`DomainPath`、`PDCPath`

この値は、コンマで区切られたバインディングパスオプションのリストです。レジストリキーは、有効と認識しない値を無視します。

VDA登録の問題のトラブルシューティング

前述のとおり、仲介されたセッションを起動する際に考慮されるには、VDAがDelivery ControllerまたはCloud Connectorに登録されている必要があります。未登録のVDAは、利用可能なリソースの利用率低下につながる可能性があります。VDAが登録されない理由はさまざまあり、その多くは管理者がトラブルシューティングできます。Studioは、カタログ作成ウィザードと、デリバリーグループ作成後にトラブルシューティング情報を提供します。

- **マシンカタログ作成中の問題の特定:** カタログ作成ウィザードで、既存のマシンを追加した後、コンピューターアカウント名のリストは、各マシンがカタログに追加するのに適しているかどうかを示します。各マシンの横にあるアイコンにカーソルを合わせると、そのマシンに関する情報メッセージが表示されます。

  メッセージで問題のあるマシンが特定された場合、そのマシンを削除する（**削除**ボタンを使用）か、マシンを追加することができます。たとえば、マシンに関する情報が取得されなかった（おそらく一度も登録されなかったため）ことを示すメッセージが表示された場合でも、そのマシンを追加することを選択できます。

  カタログの機能レベルは、カタログ内のマシンで利用できる製品機能を制御します。新しい製品バージョンで導入された機能を使用するには、新しいVDAが必要になる場合があります。機能レベルを設定すると、そのバージョンで導入されたすべての機能（および機能レベルが変更されない場合はそれ以降のバージョン）がカタログ内のマシンで利用可能になります。ただし、以前のVDAバージョンを持つカタログ内のマシンは登録できません。
- **デリバリーグループ作成後の問題の特定:** デリバリーグループを作成すると、Studioはそのグループに関連付けられているマシンに関する詳細を表示します。

  デリバリーグループの詳細ペインには、登録が必要だが登録されていないマシンの数が表示されます。つまり、電源がオンになっていてメンテナンスモードではないが、現在Controllerに登

録されていないマシンが1台以上存在する可能性があります。「未登録だが登録が必要」なマシンを表示する場合は、詳細ペインの**トラブルシューティング**タブで考えられる原因と推奨される是正措置を確認してください。

VDA登録のトラブルシューティングに関する詳細情報

- 機能レベルの詳細については、「VDAのバージョンと機能レベル」を参照してください。
- VDA登録のトラブルシューティングについて詳しくは、「CTX136668」を参照してください。
- VDA登録とセッション起動のトラブルシューティングには、Citrix Scoutのヘルスチェックも使用できます。詳細については、「ヘルスチェックについて」を参照してください。

仮想IPおよび仮想ループバック

重要:

- Windows 10 Enterprise multi-session は Remote Desktop IP Virtualization (Virtual IP) をサポートしていません。また、Windows 10 Enterprise multi-session では Remote Desktop IP Virtualization または仮想ループバックをサポートしていません。
- Remote Desktop IP Virtualization (Virtual IP) は、クラウドホスト型マシンではサポートされていません。 詳細については、Microsoft のドキュメントを参照してください。

Remote Desktop IP Virtualization および仮想ループバック機能は、Windows Server 2016、Windows Server 2019、および Windows Server 2022 マシンでサポートされています。これらの機能は、Windows デスクトップ OS マシンには適用されません。

Microsoft Remote Desktop IP Virtualization アドレス機能は、公開アプリケーションにセッションごとに一意の動的に割り当てられた IP アドレスを提供します。Citrix 仮想ループバック機能を使用すると、localhost (デフォルトでは 127.0.0.1) との通信に依存するアプリケーションを、localhost 範囲 (127.*) 内の一意の仮想ループバックアドレスを使用するように構成できます。

CRMやCTI（Computer Telephony Integration）などの特定のアプリケーションは、アドレス指定、ライセンス、識別、または一意のIPアドレスやループバックアドレスを必要とするその他の目的でIPアドレスを使用します。他のアプリケーションは静的ポートにバインドする可能性があるため、マルチユーザー環境でアプリケーションの追加インスタンスを起動しようとすると、ポート

が使用中であるために失敗します。このようなアプリケーションがCitrix Virtual Apps™環境で正しく機能するには、デバイスごとに一意のIPアドレスが必要です。

Remote Desktop IP Virtualization と仮想ループバックは、互いに独立した機能です。どちらか一方、または両方を使用できます。

管理者アクションの概要:

- Microsoft Remote Desktop IP Virtualization を使用するには、Windows サーバーでこれを有効にして構成します。(Citrix® ポリシー設定は不要です。)
- Citrix仮想ループバックを使用するには、Citrixポリシーで2つの設定を構成します。

リモートデスクトップIP仮想化 (仮想IP)

Windows サーバーで Remote Desktop IP Virtualization が有効になり構成されると、セッションで実行されている構成済みの各アプリケーションは、一意のアドレスを持っているように見えます。ユーザーは、Citrix Virtual Apps サーバー上のこれらのアプリケーションに、他の公開アプリケーションと同じ方法でアクセスします。プロセスが Remote Desktop IP Virtualization を必要とするのは、次のいずれかのケースです。

- プロセスがハードコードされたTCPポート番号を使用している
- プロセスがWindowsソケットを使用しており、一意のIPアドレスまたは指定されたTCPポート番号を必要としている

アプリケーションが Remote Desktop IP Virtualization アドレスを使用する必要があるかどうかを判断するには：

1. Microsoft から **TCPView** ツールを入手します。このツールは、特定の IP アドレスとポートをバインドするすべてのアプリケーションを一覧表示します。TCPView の詳細については、Microsoft ドキュメント を参照してください。
2. **IP アドレスの解決**機能を無効にして、ホスト名ではなくアドレスが表示されるようにします。
3. アプリケーションを起動し、**TCPView** を使用して、アプリケーションが開いている IP アドレスとポート、およびこれらのポートを開いているプロセス名を確認します。
4. サーバーのIPアドレス、0.0.0.0、または127.0.0.1を開くプロセスを構成します。
5. アプリケーションが異なるポートで同じ IP アドレスを開かないようにするには、アプリケーションの別のインスタンスを起動します。

Microsoft Remote Desktop (RD) IP仮想化の仕組み

- Microsoftサーバーで仮想IPアドレス指定を有効にする必要があります。

たとえば、Windows Server 2016 環境では、サーバーマネージャーから **Remote Desktop Services > RD Session Host Connections** を展開して、RD IP Virtualization 機能を有効にし、セッションごとまたはプログラムごとに動的ホスト構成プロトコル (DHCP) サーバーを使用して IP アドレスを動的に割り当てる設定を構成します。Remote Desktop IP Virtualization の構成の詳細については、Microsoft ドキュメント を参照してください。

- 機能を有効にすると、セッションの起動時に、サーバーはDHCPサーバーから動的に割り当てられたIPアドレスを要求します。
- The **RD IP Virtualization**機能は、リモートデスクトップ接続にセッションごとまたはプログラムごとにIPアドレスを割り当てます。複数のプログラムにIPアドレスを割り当てる場合、それらはセッションごとのIPアドレスを共有します。
- セッションにアドレスが割り当てられると、以下の呼び出しが行われるたびに、システムプライマリIPアドレスではなく仮想アドレスがセッションで使用されます:
  `bind`, `closesocket`, `connect`, `WSAConnect`, `WSAAccept`, `getpeername`, `getsockname`, `sendto`, `WSASendTo`, `WSASocketW`, `gethostbyaddr`, `getnameinfo`, `getaddrinfo`。

リモートデスクトップセッションホスティング構成内でMicrosoft IP仮想化機能を使用する場合、アプリケーションとWinsock関数呼び出しの間に「フィルター」コンポーネントを挿入することで、アプリケーションは特定のIPアドレスにバインドされます。これにより、アプリケーションは使用すべき正しいIPアドレスのみを認識します。アプリケーションがTCPまたはUDP通信をリッスンしようとすると、自動的に割り当てられた仮想IPアドレス（またはループバックアドレス）にバインドされます。アプリケーションによって開かれた発信接続はすべて、アプリケーションにバインドされたIPアドレスから発信されます。

アドレスを返す関数（Windowsポリシーが制御する`GetAddrInfo()`など）でローカルホストIPアドレスが要求された場合、リモートデスクトップIP仮想化は返されたIPアドレスを調べ、それをセッションのリモートデスクトップIP仮想化アドレスに変更します。このような名前関数を介してローカルサーバーのIPアドレスを取得しようとするアプリケーションは、そのセッションに割り当てられた一意のリモートデスクトップIP仮想化アドレスのみを認識します。このIPアドレスは、bindやconnectなどの後続のソケット呼び出しでよく使用されます。Windowsポリシーの詳細については、「RDS IP Virtualization in Windows Server」を参照してください。

多くの場合、アプリケーションはアドレス0.0.0.0でリッスンするためにポートへのバインドを要求します。アプリケーションがこれを行い、静的ポートを使用する場合、アプリケーションの複数のインスタンスを起動することはできません。リモートデスクトップIP仮想化アドレス機能は、これらの呼び出しタイプでも0.0.0.0を探します。特定の仮想IPアドレスでリッスンするように呼び出しを変更するため、複数のアプリケーションが同じコンピューター上の同じポートでリッスンできるようになります。これは、すべて異なるアドレスでリッスンしているためです。この呼び出しは、ICAセッション内であり、リモートデスクトップIP仮想化アドレス機能が有効に

なっている場合にのみ変更されます。たとえば、異なるセッションで実行されているアプリケーションの2つのインスタンスが、両方ともすべてのインターフェイス（0.0.0.0）と特定のポート（9000など）にバインドしようとした場合、それらはVIPAddress1:9000とVIPAddress2:9000にバインドされ、競合は発生しません。

仮想ループバック

Citrix Remote Desktop IP Virtualization loopback policy設定を有効にすると、各セッションが通信用に独自のループバックアドレスを持つことができます。アプリケーションがWinsock呼び出しでlocalhostアドレス（デフォルト = 127.0.0.1）を使用すると、仮想ループバック機能は127.0.0.1を127.X.X.Xに置き換えます。ここで、X.X.Xはセッション ID + 1を表します。たとえば、セッションIDが7の場合、127.0.0.8になります。セッションIDが第4オクテット（255を超える）を超過する可能性は低いですが、その場合はアドレスは次のオクテット（127.0.1.0）にロールオーバーし、最大127.255.255.255までとなります。

プロセスが仮想ループバックを必要とするのは、次のいずれかのケースです。

- プロセスがWindowsソケットループバック（localhost）アドレス（127.0.0.1）を使用している場合
- プロセスがハードコードされたTCPポート番号を使用している場合

プロセス間通信にループバックアドレスを使用するアプリケーションには、仮想ループバックポリシー設定を使用します。追加の構成は不要です。仮想ループバックは仮想IPに依存しないため、Microsoftサーバーを構成する必要はありません。

- 仮想IPループバックサポート。有効にすると、このポリシー設定により、各セッションが独自の仮想ループバックアドレスを持つことができます。この設定はデフォルトで無効になっています。この機能は、仮想IP仮想ループバックプログラムリストポリシー設定で指定されたアプリケーションにのみ適用されます。
- 仮想IP仮想ループバックプログラムリスト。このポリシー設定は、仮想IPループバック機能を使用するアプリケーションを指定します。この設定は、仮想IPループバックサポートポリシー設定が有効になっている場合にのみ適用されます。
- 仮想IPループバックポートの除外。アプリケーションがこの設定で指定されたポートでループバックアドレスを呼び出す場合、仮想ループバックは呼び出しをセッション固有のループバックアドレスに変更しません。

関連機能

仮想IPよりも仮想ループバックが優先されるように、以下のレジストリ設定を使用できます。この機能は「優先ループバック」と呼ばれます。ただし、注意して進めてください。

- 優先ループバックは、仮想IPと仮想ループバックの両方が有効になっている場合にのみ使用してください。そうしないと、予期しない結果が生じる可能性があります。
- レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrixは、レジストリエディターの誤った使用によって生じる問題が解決できることを保証できません。レジストリエディターは自己責任で使用してください。編集する前に必ずレジストリをバックアップしてください。

アプリケーションが常駐するサーバーでregeditを実行します。

- `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP`
- 名前: PreferLoopback, 種類: REG_DWORD, データ: 1
- 名前: PreferLoopbackProcesses, 種類: REG_MULTI_SZ, データ: \<プロセスのリスト\>

ゾーン

> **注:**
>
> バージョン2511以降、Citrix Web Studio（Webベース）はCitrix Virtual Apps and Desktops™の唯一の管理コンソールです。Citrix Studio（MMCベース）はインストーラーから削除されました。この記事はWeb Studioにのみ適用されます。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

WANで接続された広範囲に分散した場所にまたがる展開では、ネットワークの遅延と信頼性により課題が生じる可能性があります。これらの課題を軽減する2つのオプションがあります。

- 複数のサイトを展開し、それぞれに独自のSQL Serverサイトデータベースを持たせる。

  このオプションは、大規模なエンタープライズ展開に推奨されます。複数のサイトは個別に管理され、それぞれに独自のSQL Serverサイトデータベースが必要です。各サイトは独立したCitrix Virtual Apps™展開です。

- 単一サイト内に複数のゾーンを構成する。

  ゾーンを構成することで、リモート地域のユーザーがWANの大部分を通過することなくリソースに接続できるようになります。ゾーンを使用すると、単一のWeb Studioコンソール、Citrix Director、およびサイトデータベースから効果的なサイト管理が可能になります。これによ

り、リモートロケーションに個別のデータベースを含むより多くのサイトを展開、人員配置、ライセンス供与、および運用するコストを節約できます。

ゾーンは、あらゆる規模の展開で役立ちます。ゾーンを使用して、アプリケーションとデスクトップをエンドユーザーの近くに配置することで、パフォーマンスを向上させることができます。ゾーンには、冗長性と回復性のために1つ以上のControllerをローカルにインストールできますが、必須ではありません。

サイトに構成されているControllerの数は、サイト自体に新しいControllerを追加するなどの一部の操作のパフォーマンスに影響を与える可能性があります。これを避けるため、Citrix Virtual AppsまたはCitrix Virtual Desktops™サイトのゾーン数を50以下に制限することをお勧めします。

ゾーンのネットワーク遅延が250ミリ秒RTTを超える場合は、ゾーンではなく複数のサイトを展開することをお勧めします。

この記事全体を通して、「ローカル」という用語は、議論されているゾーンを指します。たとえば、「VDAがローカルControllerに登録する」とは、VDAがVDAが配置されているゾーン内のControllerに登録することを意味します。

このリリースでのゾーンは、XenAppバージョン6.5以前のゾーンと似ていますが、同一ではありません。たとえば、このゾーンの実装では、データコレクターはありません。サイト内のすべてのControllerは、プライマリゾーンの1つのサイトデータベースと通信します。また、このリリースではフェールオーバーゾーンと優先ゾーンの動作が異なります。

ゾーンの種類

サイトには常に1つのプライマリゾーンがあります。オプションで1つ以上のサテライトゾーンを持つこともできます。サテライトゾーンは、災害復旧、地理的に離れたデータセンター、支店、クラウド、またはクラウド内のアベイラビリティゾーンに使用できます。

プライマリゾーン:

プライマリゾーンのデフォルト名は「Primary」です。このゾーンには、SQL Serverサイトデータベース（および使用されている場合は高可用性SQLサーバー）、Web Studio、Director、Citrix StoreFront™、Citrix License Server、およびCitrix Gatewayが含まれます。サイトデータベースは常にプライマリゾーンに保持してください。

プライマリゾーンには、冗長性のために少なくとも2つのControllerが必要です。プライマリゾーンには、データベースおよびインフラストラクチャと密接に連携するアプリケーションを持つVDAを配置できます。

サテライトゾーン:

サテライトゾーンには、1つ以上のVDA、Controller、StoreFrontサーバー、およびCitrix Gatewayサーバーが含まれます。通常の運用では、サテライトゾーンのControllerはプライマリゾーンのデータベースと直接通信します。

サテライトゾーン、特に大規模なゾーンには、そのゾーンのマシンをプロビジョニングおよび保存するために使用されるハイパーバイザーが含まれる場合もあります。サテライトゾーンを構成する際、ハイパーバイザーまたはその他のサービス接続を関連付けることができます。（その接続を使用するカタログがすべて同じゾーンにあることを確認してください。）

サイトには、独自のニーズと環境に基づいて、さまざまな構成のサテライトゾーンを含めることができます。次の図は、プライマリゾーンとサテライトゾーンの例を示しています。

プライマリゾーンとサテライトゾーンの図(/en-us/citrix-virtual-apps-desktops/current-release/media/zones1.png)

図では、次のようになります。

- **プライマリゾーン:** 2つのController、Web Studio、Director、StoreFront、License Server、およびサイトデータベース（高可用性SQL Server展開を含む）が含まれます。プライマリゾーンには、複数のVDAとCitrix Gatewayも含まれます。
- **サテライトゾーン1: Controllerを持つVDA:** サテライトゾーン1には、Controller、VDA、およびStoreFrontサーバーが含まれます。このサテライトゾーンのVDAは、ローカルのControllerに登録されます。ローカルのControllerは、プライマリゾーンのサイトデータベースおよびライセンスサーバーと通信します。

  WANが失敗した場合、ローカルホストキャッシュ機能により、サテライトゾーンのControllerは、そのゾーンのVDAへの接続の仲介を続行できます。このような展開は、従業員がローカルのStoreFrontサイトとローカルのControllerを使用してローカルリソースにアクセスするオフィスで効果的です。
- **サテライトゾーン2: 冗長Controllerを持つVDA:** サテライトゾーン2には、2つのController、VDA、およびStoreFrontサーバーが含まれます。これは最も回復力のあるゾーンタイプであり、WANとローカルControllerの1つが同時に障害を起こした場合でも保護を提供します。

VDAの登録先とControllerのフェールオーバー先

プライマリゾーンとサテライトゾーンを含むサイトで、VDAの最小バージョンが7.7の場合:

- プライマリゾーンのVDAは、プライマリゾーンのControllerに登録されます。プライマリゾーンのVDAは、サテライトゾーンのControllerに登録しようとすることはありません。

- サテライトゾーンのVDAは、可能であればローカルのControllerに登録されます。（これは優先Controllerと見なされます。）ローカルのControllerが利用できない場合（たとえば、VDAの登録をこれ以上受け入れられない、または障害が発生した場合など）、VDAはプライマリゾーンのControllerに登録しようとします。この場合、サテライトゾーンのControllerが再び利用可能になったとしても、VDAはプライマリゾーンに登録されたままになります。サテライトゾーンのVDAは、別のサテライトゾーンのControllerに登録しようとすることはありません。
- VDAのController検出で自動更新が有効になっており、VDAのインストール中にControllerアドレスのリストを指定した場合、初期登録のためにそのリストからControllerがランダムに選択されます（Controllerがどのゾーンにあるかに関わらず）。そのVDAを持つマシンが再起動されると、VDAはローカルゾーンのControllerへの登録を優先し始めます。
- サテライトゾーンのControllerが故障した場合、可能であれば別のローカルControllerにフェールオーバーします。ローカルControllerが利用できない場合は、プライマリゾーンのControllerにフェールオーバーします。
- Controllerをゾーンの内外に移動し、自動更新が有効になっている場合、両方のゾーンのVDAは、どのControllerがローカルで、どのControllerがプライマリゾーンにあるかを示す更新されたリストを受け取り、どのControllerに登録し、どのControllerから接続を受け入れることができるかを知ることができます。
- カタログを別のゾーンに移動すると、そのカタログ内のVDAは、カタログを移動したゾーンのControllerに再登録します。（カタログを別のゾーンに移動する際は、このゾーンと関連するホスト接続があるゾーンが適切に接続されていることを確認してください。帯域幅が制限されているか、待ち時間が長い場合は、ホスト接続を関連するマシンカタログを含む同じゾーンに移動してください。）

プライマリゾーンのすべてのControllerが故障した場合：

- Web Studioはサイトに接続できません。
- プライマリゾーンのVDAへの接続はできません。
- プライマリゾーンのControllerが利用可能になるまで、サイトのパフォーマンスが低下します。

VDAバージョン7.7より前のバージョンを含むサイトの場合：

- サテライトゾーンのVDAは、ローカルゾーンおよびプライマリゾーンのControllerからの要求を受け入れます。（最小バージョン7.7のVDAは、他のサテライトゾーンのController要求を受け入れることができます。）
- サテライトゾーンのVDAは、プライマリゾーンまたはローカルゾーンのControllerにランダムに登録します。（最小バージョン7.7のVDAはローカルゾーンを優先します。）

ゾーンの優先順位

ゾーン優先機能を使用するには、最小限StoreFront 3.7およびCitrix Gateway 11.0-65.xを使用している必要があります。

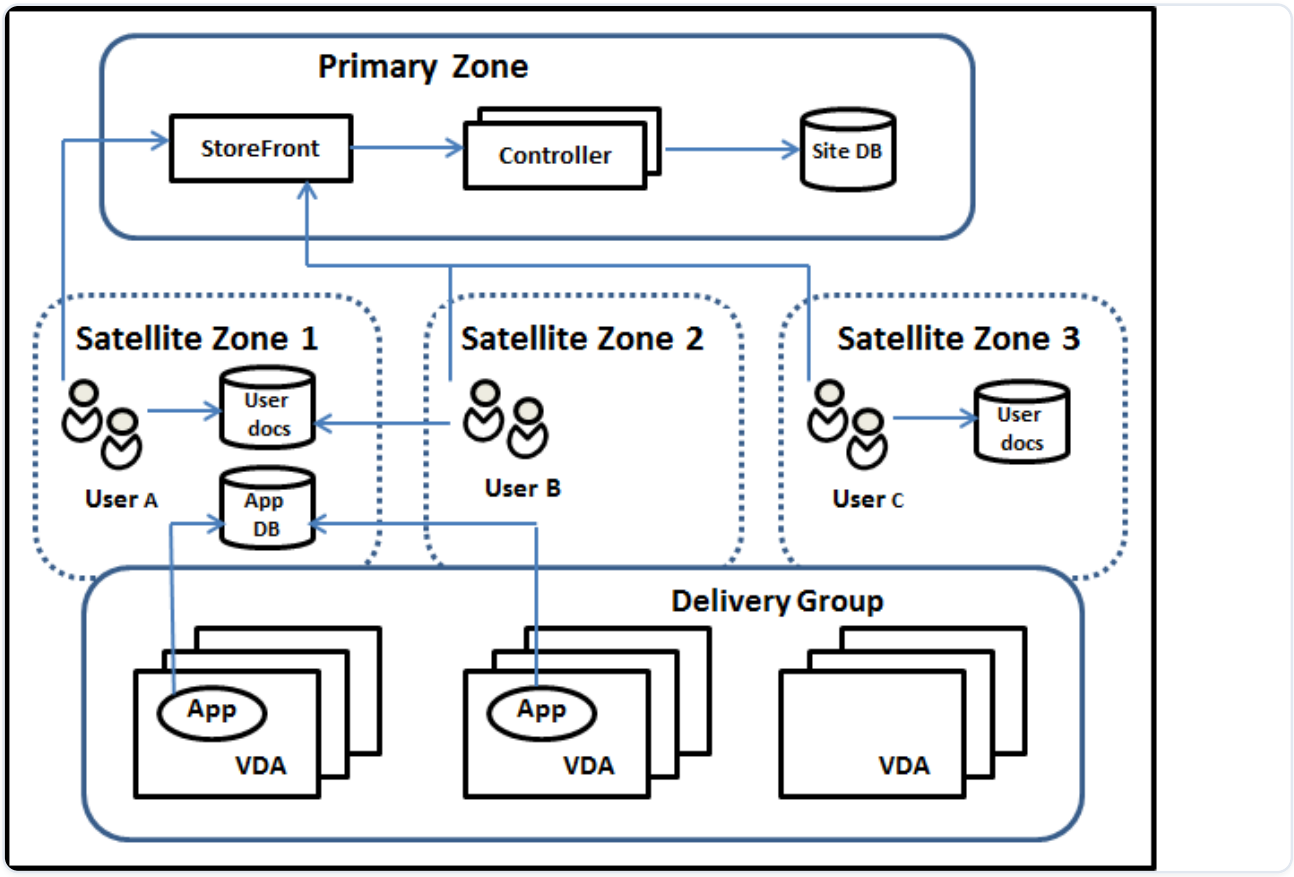
マルチゾーンサイトでは、ゾーン優先機能により、管理者はアプリケーションまたはデスクトップの起動に使用されるVDAをより柔軟に制御できます。

ゾーンの優先順位の仕組み

ゾーンの優先順位には3つの形式があります。特定のゾーンのVDAを使用することを優先する場合があります。その理由は次のとおりです。

- アプリケーションのデータが保存されている場所。これはアプリケーションホームと呼ばれます。
- ユーザーのホームデータ（プロファイルやホーム共有など）の場所。これはユーザーホームと呼ばれます。
- ユーザーの現在の場所（Citrix Workspace™アプリが実行されている場所）。これはユーザーの場所と呼ばれます。

次の図は、マルチゾーン構成の例を示しています。



この例では、VDAは3つのサテライトゾーンに分散していますが、すべて同じデリバリーグループに属しています。そのため、ブローカーはユーザーの起動リクエストに対してどのVDAを使用するかを選択する可能性があります。この例は、ユーザーがCitrix Workspaceアプリのエンドポイントを実行できる場所がいくつかあることを示しています。

- ユーザーAは、サテライトゾーン1でCitrix Workspaceアプリがインストールされたデバイスを使用しています。
- ユーザーBは、サテライトゾーン2でデバイスを使用しています。
- ユーザーのドキュメントはさまざまな場所に保存できます。
    - ユーザーAとBは、サテライトゾーン1にある共有を使用します。
    - ユーザーCは、サテライトゾーンCの共有を使用します。
    - 公開されているアプリケーションの1つは、サテライトゾーン1にあるデータベースを使用します。

ユーザーまたはアプリケーションのホームゾーンを構成することで、ユーザーまたはアプリケーションをゾーンに関連付けます。Delivery Controller™のブローカーは、リソースが利用可能な場合、これらの関連付けを使用してセッションが起動されるゾーンの選択を支援します。次のことができます。

- ユーザーをゾーンに追加して、ユーザーのホームゾーンを構成します。
- アプリケーションのプロパティを編集して、アプリケーションのホームゾーンを構成します。

ユーザーまたはアプリケーションは、一度に1つのホームゾーンしか持つことができません。（ユーザーグループのメンバーシップにより複数のゾーンメンバーシップが発生する場合、ユーザーには例外が発生する可能性があります。「その他の考慮事項」セクションを参照してください。ただし、この場合でも、ブローカーは1つのホームゾーンのみを使用します。）

ユーザーとアプリケーションのゾーン設定を構成できますが、ブローカーは起動に対して1つの優先ゾーンのみを選択します。優先ゾーンを選択するためのデフォルトの優先順位は、アプリケーションホーム \> ユーザーホーム \> ユーザーロケーションです。この順序を制限できます。詳細については、ゾーン設定の調整を参照してください。ユーザーがアプリケーションを起動すると：

- そのアプリケーションにゾーン関連付け（アプリケーションホーム）が構成されている場合、優先ゾーンはそのアプリケーションのホームゾーンになります。
- アプリケーションにゾーン関連付けが構成されていないが、ユーザーにゾーン関連付け（ユーザーホーム）が構成されている場合、優先ゾーンはそのユーザーのホームゾーンになります。
- アプリケーションにもユーザーにもゾーン関連付けが構成されていない場合、優先ゾーンはユーザーがCitrix Workspaceアプリインスタンスを実行しているゾーン（ユーザーロケーショ

ン）になります。そのゾーンが定義されていない場合、ランダムなVDAとゾーンの選択が使用されます。優先ゾーン内のすべてのVDAに負荷分散が適用されます。優先ゾーンがない場合、デリバリーグループ内のすべてのVDAに負荷分散が適用されます。

ゾーンの優先順位の調整

ユーザーまたはアプリケーションのホームゾーンを構成（または削除）する際、ゾーン設定の使用方法をさらに制限することもできます。

- **必須のユーザーホームゾーンの使用：** デリバリーグループでは、セッションがユーザーのホームゾーン（構成されている場合）で起動し、ホームゾーンに利用可能なリソースがない場合に他のゾーンへのフェイルオーバーを行わないように指定できます。この制限は、ゾーン間で大きなプロファイルやデータファイルをコピーするリスクを回避する必要がある場合に役立ちます。言い換えれば、別のゾーンでセッションを起動するよりも、セッションの起動を拒否する方が望ましいということです。
- **アプリケーションのホームゾーンの強制使用:** 同様に、アプリケーションのホームゾーンを構成する場合、そのアプリケーションは、アプリケーションのホームゾーンでリソースが利用できない場合に別のゾーンにフェールオーバーすることなく、そのゾーンでのみ起動されるように指定できます。
- **アプリケーションのホームゾーンなし、および構成されたユーザーホームゾーンを無視:** アプリケーションのホームゾーンを指定しない場合、そのアプリケーションを起動するときに、構成されたユーザーゾーンを考慮しないように指定することもできます。たとえば、一部のユーザーが異なるホームゾーンを持っている場合でも、ユーザーロケーションゾーンの優先設定を使用して、ユーザーがデバイスの近くのVDAでアプリケーションを実行することを好む場合があります。

優先ゾーンがセッションの使用に与える影響

ユーザーがアプリケーションまたはデスクトップを起動すると、ブローカーは既存のセッションを使用するよりも優先ゾーンを使用することを優先します。

アプリケーションまたはデスクトップを起動するユーザーが、起動されるリソースに適したセッション（たとえば、アプリケーションのセッション共有を使用できるセッション、または起動されるリソースがすでに実行されているセッション）をすでに持っているが、そのセッションがユーザー/アプリケーションの優先ゾーン以外のゾーンのVDAで実行されている場合、システムは新しいセッションを作成する可能性があります。これにより、そのユーザーのセッション要件にとって優先度の低いゾーンのセッションに再接続するよりも前に、正しいゾーンでの起動（利用可能な容量がある場合）が満たされます。

到達不能になる可能性のある孤立したセッションを防ぐため、既存の切断されたセッションへの再接続は、それらが非優先ゾーンにある場合でも許可されます。

起動を満たすためのセッションの望ましさの順序は次のとおりです。

1. 優先ゾーン内の既存のセッションに再接続する。
2. 優先ゾーン以外のゾーンで、既存の切断されたセッションに再接続する。
3. 優先ゾーンで新しいセッションを開始します。
4. 優先ゾーン以外のゾーンで、接続されている既存のセッションに再接続する。
5. 優先ゾーン以外のゾーンで、新しいセッションを開始する。

その他のゾーン優先度に関する考慮事項

- ユーザーグループ（セキュリティグループなど）にホームゾーンを構成すると、そのグループのユーザー（直接的または間接的なメンバーシップを通じて）は指定されたゾーンに関連付けられます。ただし、ユーザーは複数のセキュリティグループのメンバーになることができ、そのため、他のグループメンバーシップを通じて異なるホームゾーンが構成されている場合があります。このような場合、そのユーザーのホームゾーンの決定は曖昧になる可能性があります。

ユーザーがグループメンバーシップを通じて取得したものではない構成済みのホームゾーンを持っている場合、そのゾーンがゾーン優先度に使用されます。グループメンバーシップを通じて取得されたゾーン関連付けはすべて無視されます。

ユーザーがグループメンバーシップのみを通じて取得した複数の異なるゾーン関連付けを持っている場合、ブローカーはゾーンの中からランダムに選択します。ブローカーがこの選択を行うと、そのゾーンは、ユーザーのグループメンバーシップが変更されるまで、その後のセッション起動に使用されます。

- ユーザーロケーションゾーンの優先設定では、デバイスが接続するCitrix Gatewayによって、エンドポイントデバイス上のCitrix Workspaceアプリが検出される必要があります。Citrix Gatewayは、IPアドレスの範囲を特定のゾーンに関連付けるように構成する必要があり、検出されたゾーンIDはStoreFrontを介してControllerに渡される必要があります。

ゾーンの優先設定の詳細については、「ゾーンの優先設定の内部」を参照してください。

考慮事項、要件、およびベストプラクティス

- ゾーンには、Controller、マシンカタログ、ホスト接続、ユーザー、およびアプリケーションを配置できます。カタログがホスト接続を使用する場合、カタログと接続が同じゾーンにあるこ

とを確認してください。（ただし、低遅延で高帯域幅の接続が利用可能な場合は、異なるゾーンに配置することもできます。）」

- サテライトゾーンにアイテムを配置すると、サイトがそれらやそれらに関連する他のオブジェクトとどのようにやり取りするかに影響します。
  - Controllerがサテライトゾーンに配置されると、それらのマシンは同じゾーン内のハイパーバイザーおよびVDAに対して良好な（ローカル）接続性を持っていると見なされます。そのサテライトゾーンのControllerは、それらのハイパーバイザーおよびVDAマシンを処理するために、プライマリゾーンのControllerよりも優先して使用されます。
  - ハイパーバイザー接続がサテライトゾーンに配置されると、そのハイパーバイザー接続を介して管理されるすべてのハイパーバイザーもそのサテライトゾーンに存在すると見なされます。そのサテライトゾーンのControllerは、そのハイパーバイザー接続と通信する際に、プライマリゾーンのControllerよりも優先して使用されます。
  - マシンカタログがサテライトゾーンに配置されると、そのカタログ内のすべてのVDAマシンがサテライトゾーンにあると見なされます。各VDAの最初の登録後にControllerリストの自動更新メカニズムがアクティブになった後、サイトへの登録を試みる際には、プライマリゾーンのControllerよりもローカルのControllerが優先して使用されます。
  - Citrix Gatewayインスタンスもゾーンに関連付けることができます。これは、ここで説明されている他の要素の場合のようにサイト構成の一部としてではなく、StoreFront Optimal HDX™ルーティング構成の一部として行われます。Citrix Gatewayがゾーンに関連付けられている場合、そのゾーン内のVDAマシンへのHDX接続が使用されるときに、そのCitrix Gatewayが優先的に使用されます。
- 実稼働サイトを作成し、最初のカタログとデリバリーグループを作成すると、すべての項目はプライマリゾーンに配置されます。この初期設定が完了するまで、サテライトゾーンを作成することはできません。（空のサイトを作成した場合、プライマリゾーンには最初はコントローラーのみが含まれます。カタログとデリバリーグループを作成する前または後にサテライトゾーンを作成できます。）
- 1つ以上の項目を含む最初のサテライトゾーンを作成すると、サイト内の他のすべての項目はプライマリゾーンに残ります。
- プライマリゾーンはデフォルトで「Primary」という名前ですが、この名前は変更できます。Web Studioはどのゾーンがプライマリゾーンであるかを示しますが、プライマリゾーンには識別しやすい名前を使用するのがベストプラクティスです。プライマリゾーンを再割り当て（つまり、別のゾーンをプライマリゾーンにする）できますが、常にサイトデータベースと高可用性サーバーが含まれている必要があります。
- サイトデータベースは常にプライマリゾーンに保持してください。

- ゾーンを作成した後、後で項目をあるゾーンから別のゾーンに移動できます。この柔軟性により、近接して最適に機能する項目を分離できる可能性があります。たとえば、カタログ内のマシンを作成する接続（ホスト）とは異なるゾーンにカタログを移動すると、パフォーマンスに影響を与える可能性があります。項目をゾーン間で移動する前に、潜在的な意図しない影響を考慮してください。カタログとそれが使用するホスト接続は同じゾーンに、または適切に接続されたゾーン（たとえば、低遅延で高帯域幅のネットワーク経由）に保持してください。
- 最適なパフォーマンスを得るには、Web StudioとDirectorはプライマリゾーンにのみインストールしてください。Web StudioとDirectorはWebアプリケーションであるため、サテライトゾーン（たとえば、プライマリゾーンがアクセス不能になった場合のフェイルオーバーとして使用するコントローラーを含むサテライトゾーン）からアクセスできます。
- 理想的には、サテライトゾーンのCitrix Gatewayは、他のゾーンまたは外部の場所からそのゾーンに入ってくるユーザー接続に使用されますが、ゾーン内の接続にも使用できます。
- 注意: ゾーン優先機能を使用するには、StoreFront 3.7およびCitrix Gateway 11.0-65.x以降を使用している必要があります。

接続品質の制限

サテライトゾーンのコントローラーは、サイトデータベースと直接SQL対話を行います。これにより、サテライトゾーンとサイトデータベースを含むプライマリゾーン間のリンクの品質にいくつかの制限が課せられます。具体的な制限は、サテライトゾーンに展開されているVDAの数と、それらのVDA上のユーザーセッションの数に比例します。したがって、VDAとセッションが少ないサテライトゾーンは、VDAとセッションが多いサテライトゾーンよりも、データベースへの接続品質が低い場合でも機能できます。

詳細については、「Latency and SQL Blocking Query Improvements」を参照してください。

遅延がブローカリングパフォーマンスに与える影響

ゾーンによってユーザーは高遅延リンク上にいることができますが、ローカルブローカーが存在する場合でも、追加の遅延は必然的にエンドユーザーエクスペリエンスに影響を与えます。ユーザーが行うほとんどの作業において、サテライトゾーンのコントローラーとサイトデータベース間のラウンドトリップによって引き起こされる遅延を経験します。

アプリケーションを起動する場合、セッションブローカリングプロセスがセッション起動要求を送信するのに適したVDAを特定する際に、追加の遅延が発生します。

ゾーンの作成と管理

フル管理者であれば、すべてのゾーン作成および管理タスクを実行できます。ただし、ゾーンの作成、編集、削除を許可するカスタムロールを作成することもできます。ゾーン間でアイテムを移動

する場合、ゾーン関連の権限（ゾーン読み取り権限を除く）は必要ありませんが、移動するアイテムに対する編集権限が必要です。たとえば、カタログをあるゾーンから別のゾーンに移動するには、そのカタログに対する編集権限が必要です。詳しくは、「委任管理」を参照してください。

Citrix Provisioning™を使用している場合： Citrix Provisioningコンソールはゾーンを認識しないため、サテライトゾーンのカタログを作成するにはWeb Studioを使用することをお勧めします。Web Studioでカタログを作成し、正しいサテライトゾーンを指定します。その後、Citrix Provisioningコンソールを使用して、そのカタログ内のマシンをプロビジョニングします。（Citrix Provisioningウィザードを使用してカタログを作成した場合、カタログはプライマリゾーンに配置されます。後でWeb Studioを使用してサテライトゾーンに移動する必要があります。）

ゾーンの作成

1. Web Studioにサインインします。
2. 左側のペインで を選択します。
3. アクションバーで を選択します。
4. ゾーンの名前と説明（オプション）を入力します。名前はサイト内で一意である必要があります。
5. 新しいゾーンに配置するアイテムを選択します。選択可能なアイテムのリストをフィルター処理したり、検索したりできます。空のゾーンを作成することもできます。その場合は、どのアイテムも選択しないでください。
6. 「**保存**」をクリックします。

この方法の代わりに、Web Studioで1つ以上のアイテムを選択し、アクションバーで を選択することもできます。

ゾーン名または説明の変更

1. Web Studioにサインインします。
2. 左側のペインで を選択します。
3. 中央のペインでゾーンを選択し、アクションバーで**ゾーンの編集**を選択します。
4. ゾーン名、説明、またはその両方を変更します。プライマリゾーンの名前を変更する場合は、そのゾーンがプライマリゾーンとして容易に識別できることを確認してください。
5. または をクリックします。

ゾーン間でアイテムを移動する

1. Web Studioにサインインします。

2. 左側のペインで を選択します。
3. 中央ペインでゾーンを選択し、1つ以上の項目を選択します。
4. アイテムを移動先のゾーンにドラッグするか、アクションバーで を選択し、移動先のゾーンを指定します。

確認メッセージには、選択したアイテムが一覧表示され、それらすべてを移動してもよろしいかどうかが尋ねられます。

注意: カタログがハイパーバイザーまたはその他のサービスへのホスト接続を使用する場合、カタログと接続の両方を同じゾーンに配置してください。そうしないと、パフォーマンスに影響が出る可能性があります。一方を移動する場合は、もう一方も移動してください。

ゾーンを削除する

ゾーンは、削除する前に空である必要があります。プライマリゾーンは削除できません。

1. Web Studioにサインインします。
2. 左側のペインで を選択します。
3. 中央のペインでゾーンを選択します。
4. アクションバーから を選択します。ゾーンが空でない場合（アイテムが含まれている場合）、それらのアイテムを移動するゾーンを選択するよう求められます。
5. 削除を確認します。

ユーザーのホームゾーンを追加する

ユーザーのホームゾーンを構成することは、*ユーザーをゾーンに追加する*とも呼ばれます。

1. Web Studioにサインインします。
2. 左側のペインで を選択し、中央のペインでゾーンを選択します。
3. アクションバーで**Add Users to Zone**を選択します。
4. **Add Users to Zone**ダイアログボックスで、**Add**をクリックし、ゾーンに追加するユーザーとユーザーグループを選択します。すでにホームゾーンを持つユーザーを指定した場合、メッセージに2つの選択肢が表示されます。**Yes** = ホームゾーンを持たない指定したユーザーのみを追加します。**No** = ユーザー選択ダイアログに戻ります。
5. **OK**をクリックします。

ホームゾーンが構成されているユーザーの場合、セッションをそのホームゾーンからのみ起動するように要求できます。

1. デリバリーグループを作成または編集します。
2. **ユーザー**ページで、**セッションをユーザーのホームゾーンで起動することを要求する（構成されている場合）**チェックボックスをオンにします。

そのデリバリーグループのユーザーが起動するすべてのセッションは、そのユーザーのホームゾーン内のマシンから起動する必要があります。デリバリーグループ内のユーザーにホームゾーンが構成されていない場合、この設定は無効です。

ユーザーのホームゾーンを削除する

この手順は、ゾーンからユーザーを削除することとも呼ばれます。

1. Web Studioにサインインします。
2. 左ペインで**Zones**を選択し、中央ペインでゾーンを選択します。
3. アクションバーで**Remove Users from Zone**を選択します。
4. **Add Users to Zone**ダイアログボックスで、**Remove**をクリックし、ゾーンから削除するユーザーとグループを選択します。この操作では、ユーザーはゾーンからのみ削除されます。それらのユーザーは、所属するデリバリーグループおよびアプリケーショングループに残ります。
5. プロンプトが表示されたら削除を確定します。

アプリケーションのホームゾーンを管理する

アプリケーションのホームゾーンを構成することは、アプリケーションをゾーンに追加することとも呼ばれます。デフォルトでは、マルチゾーン環境では、アプリケーションにホームゾーンはありません。

アプリケーションのホームゾーンは、アプリケーションのプロパティで指定されます。アプリケーションをグループに追加するとき、または後でアプリケーションのプロパティを構成できます。

- デリバリーグループを作成するとき、アプリケーショングループを作成するとき、または既存のグループにアプリケーションを追加するときに、ウィザードの**Applications**ページで**Properties**を選択します。
- アプリケーションの追加後にアプリケーションのプロパティを変更するには、左ペインで**Applications**を選択します。アプリケーションを選択し、アクションバーで**Edit Application Properties**を選択します。

アプリケーションのプロパティ/設定の ページで、次の操作を行います。

- アプリケーションにホームゾーンを設定する場合：
    - **Use the selected zone to decide**ラジオボタンを選択し、ゾーンを選択します。

    - アプリケーションを、選択したゾーンからのみ（他のゾーンからは起動しないように）起動する場合は、ゾーン選択の下にあるチェックボックスをオンにします。

- アプリケーションにホームゾーンを設定しない場合：

    - ラジオボタンを選択します。
    - このアプリケーションを起動する際に、ブローカーが構成済みのユーザーゾーンを考慮しないようにする場合は、ラジオボタンの下にあるチェックボックスを選択します。この場合、アプリケーションまたはユーザーのホームゾーンのいずれも、このアプリケーションを起動する場所を決定するために使用されません。

ゾーンの指定を含むその他のアクション

少なくとも1つのサテライトゾーンを作成した後、ホスト接続を追加するか、カタログを作成する際にゾーンを指定できます。

通常、プライマリゾーンがデフォルトです。Machine Creation Services™を使用してカタログを作成する場合、ホスト接続用に構成されたゾーンが自動的に選択されます。

サイトにサテライトゾーンが含まれていない場合、プライマリゾーンが想定され、ゾーン選択ボックスは表示されません。

キャッシュからブローカーユーザーを削除する

管理者がキャッシュからブローカーユーザーを削除できない場合や、`Get-BrokerUser` の実行時にユーザーが AD から誤った SID を表示する場合があります。

これは、ユーザーがADから削除され、再作成されたにもかかわらず、ブローカーキャッシュに以前のユーザーSIDが残っている場合に発生します。

これを解決するには、次の手順を実行します。

1. Active Directory からユーザーを削除します。
2. 削除された各アカウントに対して `Get-BrokerUser` を実行します。どこからも参照されていないアカウントは、結果を返しません。参照されているユーザーの場合、`Get-BrokerUser` を実行すると値が返されます。次に、ユーザーが割り当てられているリソースを特定し、それらのリソースからユーザーを手動で削除する必要があります。

   例:

    - ユーザーがアプリケーションに割り当てられているかを確認します: `Get-BrokerApplication`

- ユーザーがアプリケーショングループに割り当てられているかを確認します: `Get-BrokerApplicationGroup`
- ユーザーがアクセスポリシーに割り当てられているかを確認します: `Get-BrokerAccessPolicyRule`
- ユーザーがアプリケーションエンタイトルメントポリシーに割り当てられているかを確認します: `Get-BrokerAppEntitlementPolicyRule`
- ユーザーがデスクトップエンタイトルメントポリシーに割り当てられているかを確認します: `Get-BrokerEntitlementPolicyRule`
- ユーザーがデスクトップグループセッションの残存に割り当てられているかを確認します: `Get-BrokerSessionLinger`
- ユーザーが VDA 上でセッションを実行しているかを確認します: `Get-BrokerSession`
- ユーザーがマージされたグループのリソースに割り当てられているかを確認します: `Get-BrokerMergedResource`
- ユーザーがリソースグループに割り当てられているかを確認します: `Get-BrokerMergeGroup`
- ユーザーに対してコマンドがキューに入っているか確認します: `Get-BrokerMachineCommand`
- ユーザーがプライベートデスクトップに割り当てられているか確認します: `Get-BrokerMachineV2`
- ユーザーがゾーン設定に割り当てられているか確認します: `Get-BrokerUserZonePreference`

3. リソースからユーザーを手動で削除します。
4. `Get-BrokerUser` コマンドを実行して、ユーザーがすべてのリソースから削除されたことを確認します。
5. ユーザーがすべてのリソースから削除されたら、キャッシュからユーザーを削除するために、以下を実行します。

```
Update-BrokerNameCache -Users -Purge -UnusedFor 0
```

Citrix Assistantアプリケーション

Citrix Virtual Desktop Assistantアプリは、エンドユーザーがCPU、メモリ、ネットワーク、HDX™、およびその他のパフォーマンス要因全体でセッションを最適化できるように設計されたGUIツールです。シンプルで便利なエクスペリエンスを提供し、多くの場合、ワンクリックでセッションパフォーマンスを大幅に向上させたり、トラブルシューティングを行ったりできます。

現在、セッションは以下の領域で最適化できます。

- システムリソース：CPUとメモリの最適化。
- ネットワーク：ネットワークステータスの確認とパーソナライズされた推奨事項。
- アプリケーション：応答しないアプリケーションを表示し、それらを終了するオプション。
- ストレージ：一時ファイルをクリーンアップし、100 MBを超えるファイルをユーザーインターフェイスから直接削除するために特定します。
- ハードウェアの診断とトラブルシューティング：
  - オーディオの診断とトラブルシューティング。
  - カメラデバイスのテスト。
  - キーボード診断
  - USB診断

  VDAに問題がある場合は、Always On Tracing (AOT) 機能も使用できます。

インストールと実行

ワークステーションおよびサーバーVDAの場合: Citrix Virtual Desktop Assistantアプリはデフォルトでダウンロードされ、最小限の操作モードで実行されます。インストール後、VDAを再起動して、システムトレイにCitrix Virtual Desktop Assistantアプリのアイコンを表示します。次に、システムトレイのCitrix Virtual Desktop Assistantアプリのアイコンをクリックして、グラフィカルユーザーインターフェイス (GUI) を起動します。

Citrix Virtual Desktop Assistant Studioポリシー設定を通じてアプリケーションを無効にできます。無効にすると、システムトレイからアイコンが削除され、ユーザーはアプリケーションを起動できなくなります。これを行うには：

1. Studioから、**ポリシー**に移動します。
2. Assistantアプリを右クリックし、**設定の編集**を選択して**無効**をクリックします。

ログファイル

Citrix Virtual Desktop Assistantアプリのログファイルは`USERPROFILE%\AppData\Local\Temp\citrix\AssistantApp\ctxasst.log`に保存されます。トラブルシューティングにはログファイルを使用してください。

これらのログを手動で添付し、`CitrixVDAssistantFeedback@citrix.com`にメールで送信していただくことで、Citrix Virtual Desktop Assistantアプリケーションの改善にご協力いただけます。

UIを探索する

アプリはオペレーティングシステムの言語バリアントを自動的に検出し、その言語でアプリを表示します。

アプリには、左ペインからアクセスできる3つの主要なページがあります。

- ホーム
- アプリ
- ファイル
- ツール
- 概要

カメラ、サウンド、キーボード、USBの設定は右下隅にあります。

ホーム

ホームページでは、次の機能が提供されます。

Citrix Assistantアプリのホーム画面(/en-us/citrix-virtual-apps-desktops/current-release/media/assistant-home-page-1.png)

- *デスクトップの最適化*: 最適化機能は、CPU使用率が高い期間中にリソースを大量に消費するアプリケーションのCPU優先度を調整することで、システム全体のパフォーマンスを向上させます。また、非アクティブなアプリケーションからメモリを解放し、システムリソースの効率的な使用を保証します。**デスクトップの最適化**をクリックすると、システムパフォーマンスの向上や、メモリ解放によって最適化されたアプリケーションに気づくかもしれません。
- *ネットワークステータス*: このタイルには、VDAネットワーク接続ステータスが表示されます。帯域幅と遅延データに基づいて、ネットワーク接続結果が表示されます。接続ステータスは、良好、普通、または不良に分類されます。ステータスが普通または不良の場合、**どうすればよいですか？**をクリックすると、改善のための推奨事項が提供されます。

> **注:**
>
> 接続が不良の場合、ファイルをクリーンアップするオプションは利用できません。

- *クリーンアップ*: このオプションは、ユーザープロファイルに関する情報を提供し、一時ファイルや大きなファイル（100 MBを超えるファイル）のクリーンアップに役立ちます。この操作により、マシンのログオン時間を大幅に改善できます。一時ファイルには、クラッシュダンプレポート、アプリケーションキャッシュ、肥大化したプロファイルの原因となる隠しファイルが含まれます。左ペインの ページにアクセスして、ファイルをクリーンアップすることもできます。詳細については、「 ページ」(#files-page)を参照してください。
- *セッションを記録*: このオプションは、トラブルシューティング、共同作業、セッションレビューのために、アクティブな仮想デスクトップセッションをMP4ビデオクリップとして記録するのに役立ちます。詳細については、ツールページを参照してください。
- *スクリーンショットを撮る*: このオプションは、Windows Snipping Toolが見逃したり、黒く表示されたりする可能性のある領域を含め、セッション全体をキャプチャするのに役立ちます。詳細については、ツールページを参照してください。
- *その他のツール*: このオプションは、仮想デスクトップエクスペリエンスを向上させるためのさまざまなツールが提供される**ツール**ページに移動します。詳細については、ツールページを参照してください。

アプリページ

アプリページには、VDAセッション内の応答しないすべてのアプリケーションと、それらを終了するオプションが表示されます。このインターフェイスから単一または複数のアプリケーションを終了できます。また、アプリケーションが最適化されたリストにある場合、アプリケーション名の横に**最適化済み**タグが表示されます。

Citrix Assistantアプリのアプリページ(/en-us/citrix-virtual-apps-desktops/current-release/media/new-assistant-apps-page.png)

- 単一のアプリを終了する: アプリの行にカーソルを合わせると**終了**ボタンが表示されるか、チェックボックスを選択して**選択したアプリを終了**をクリックします。プロンプトが表示されたらアクションを確認します。
- 複数のアプリを終了する: 複数のアプリケーションを一度に選択し、 をクリックします。プロンプトが表示されたら、操作を確定します。

Citrix Assistantアプリの「アプリ」ページ - 選択したアプリを終了(/en-us/citrix-virtual-apps-desktops/current-release/media/new-assisstant-apps-multiple-apps.png)

ファイルページ

「**ファイル**」ページには、ユーザープロファイルに関する情報が表示され、一時ファイルまたはサイズの大きいファイル（100 MBを超えるファイル）のクリーンアップに役立ちます。この操作により、マシンのログオン時間を大幅に短縮できます。一時ファイルには、クラッシュダンプレポート、アプリケーションキャッシュ、および肥大化したプロファイルの原因となる隠しファイルが含まれます。

Citrix Assistantアプリの「ファイル」ページ(/en-us/citrix-virtual-apps-desktops/current-release/media/new-assistant-files-page.png)

- 一時ファイル: をクリックして一時ファイルをクリーンアップします。
- 大きいファイル: をクリックして大きなファイルを削除するか、 をクリックしてその場所に移動し、適切な操作を決定できます。**Ctrl** キーを使用して、複数のファイルを同時に選択できます。
- ダウンロードとごみ箱フォルダー: をクリックしてその場所に移動し、適切な操作を決定します。

コンテナタイプのプロファイルの場合、容量の使用状況も確認できます。

Citrix Assistantアプリの「ファイル」ページ - 容量の使用状況(/en-us/citrix-virtual-apps-desktops/current-release/media/assistant-files-page-container-profile.png)

ページのデータを再計算するには、アプリの右上隅にある アイコンをクリックします。

ツールページ

「**ツール**」ページには、仮想デスクトップエクスペリエンスを向上させる次のツールが表示されます。

Citrix Assistantアプリの「ツール」ページ(/en-us/citrix-virtual-apps-desktops/current-release/media/assistant-tools-page.png)

- Snipping Tool: Citrix Snipping Toolを使用すると、ユーザーはCitrix Virtual Apps and Desktopsセッション内で、オーバーレイおよびリダイレクトされたコンテンツのスクリーンショットをシームレスにキャプチャできます。これには、Browser Content Redirection (BCR)、Microsoft Teams Optimization、その他のユニファイドコミュニケーションプラットフォームなどの最適化されたメディアが含まれます。詳細については、Citrix Snipping Toolのドキュメントを参照してください。

  セッション内のスクリーンショットをキャプチャするには:

a. **Snipping tool**をクリックします。

b. **New**をクリックして新しい切り取りを開始し、キャプチャする領域を選択します。

c. 切り取りがキャプチャされたら、`.PNG`または`.BMP`ファイル形式でファイルに保存するか、クリップボードに保存します。

> **注:**
>
> - デフォルトでは、Snipping toolはVDAセッションのユーザー定義領域をキャプチャできます。または、Snipping toolを使用して、画面全体のセッション内スクリーンショット（単一画面）をキャプチャしたり、複数の画面が使用されている場合（すべての画面）にキャプチャしたりすることもできます。
> - Snipping toolは、遅延スクリーンショットでも使用できます。遅延ボタンを使用して、目的の遅延を選択します。設定された遅延時間が経過すると、スクリーンショットが撮影されます。

> オーバーレイコンテンツがキャプチャされない場合は、以下を確認してください。

- Web Studioで**Screenshot Redirected Content**ポリシーが有効になっていることを確認します。
- VDAおよびCitrix Workspaceアプリのバージョンが最小要件を満たしていることを確認します。
  - VDA: 2603 以降
  - Windows 用 Citrix Workspace アプリ (CWA): 2603 以降
  - サポートされているクライアント: Windowsのみ
- App Protectionがスクリーンショット機能をブロックしていないか確認します。

- セッション記録: アクティブな仮想デスクトップセッションをMP4ビデオクリップとして記録し、トラブルシューティング、コラボレーション、セッションレビューに役立てます。

  Session recordingページでは、以下のオプションを使用してキャプチャを管理できます。

  - **録画を開始**: 現在のデスクトップセッションのキャプチャを開始します。録画が進行中であることを確認するために、録画インジケーターが表示されます。
  - **録画を停止**: キャプチャを終了し、ビデオをMP4ファイルとして自動的に保存します。

Citrix Assistantアプリの録画開始ページ(/en-us/citrix-virtual-apps-desktops/current-release/media/assistant-start-recording-page.png)

セッション録画ページには、キャプチャされたコンテンツを管理するための次のオプションがあります。

- **フォルダーを開く**: 録画されたMP4ファイルが保存されている設定済みのディレクトリを開きます。デフォルトでは、録画は`%userprofile%\Videos\SessionRecordings`に保存されます。
- **録画場所の変更**: セッション録画の保存パスを変更できます。サポートされている場所は次のとおりです。
  - ローカルストレージ: 仮想マシンのローカルドライブ上のフォルダー。
  - ネットワークパス: 書き込み権限がある場合、アクセス可能なマップされたネットワークドライブまたはUNCパス（例: `\\Server\Share\Recordings`）。

サウンドページ

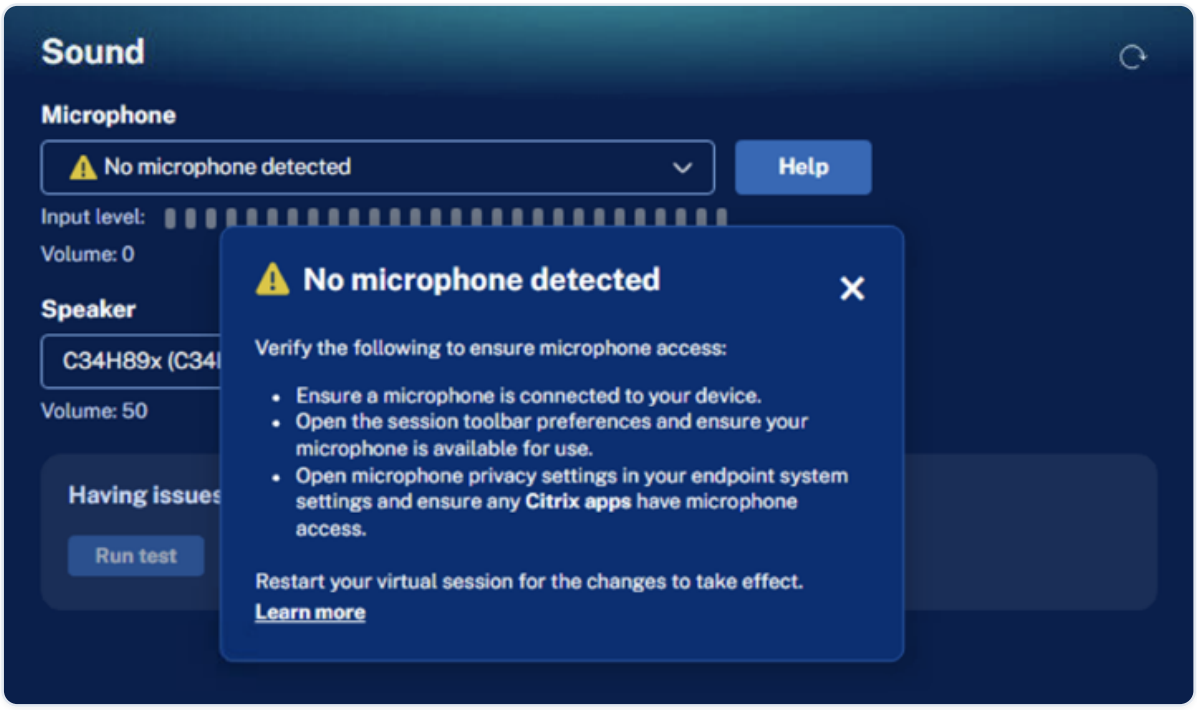
Citrix Virtual Desktop Assistantアプリのサウンドページは、VDAセッション内のオーディオ設定の診断とトラブルシューティングに役立ちます。

Citrix Assistantアプリのサウンドページ(/en-us/citrix-virtual-apps-desktops/current-release/media/new-assistant-sounds-page.png)

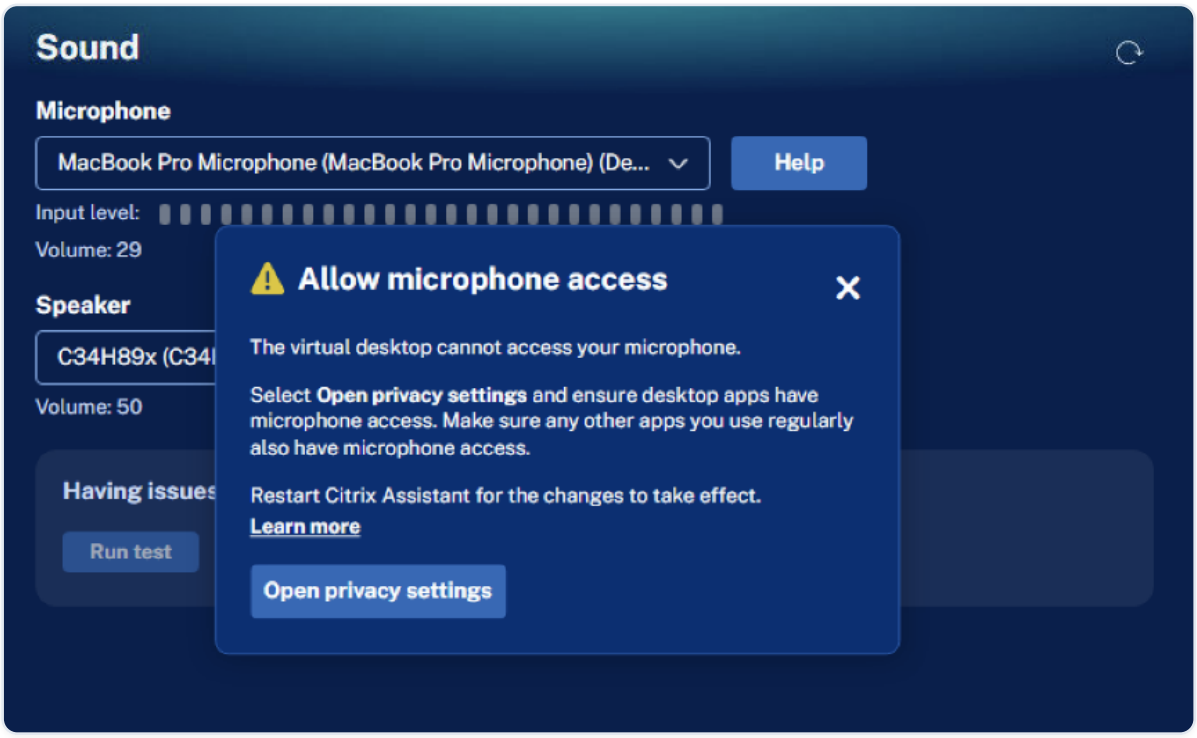
- 複数のオーディオデバイスが接続されている場合は、ドロップダウンリストからマイクとスピーカーを選択できます。

  Citrix Virtual Desktop Assistantがマイクを使用できない場合、次のいずれかの警告メッセージが表示されることがあります。

  - **マイクが検出されません**: これは、Citrix Workspaceアプリのマイクプライバシー設定が無効になっていることが原因である可能性が最も高いです。ダイアログに表示されるヒントに従って、マイクのプライバシー設定を確認し、Citrix Workspaceアプリへのアクセスを有効にしてください。

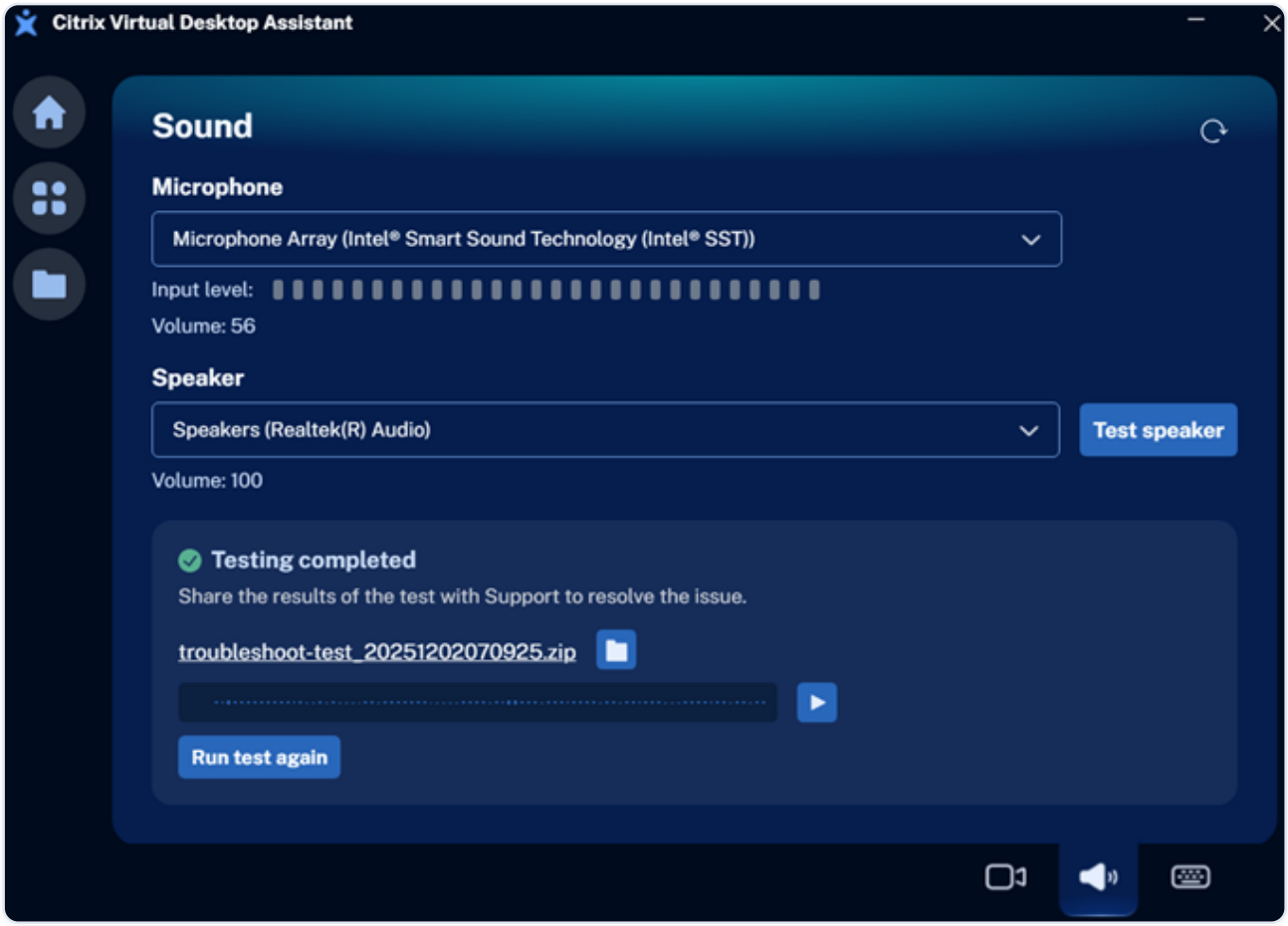


- **マイクへのアクセスを許可**：これは、Citrix Virtual Desktop Assistant が現在の Citrix 仮想デスクトップでマイクへのアクセス権を持っていない場合に発生します。ダイアログに表示されるヒントに従って、この問題を解決してください。



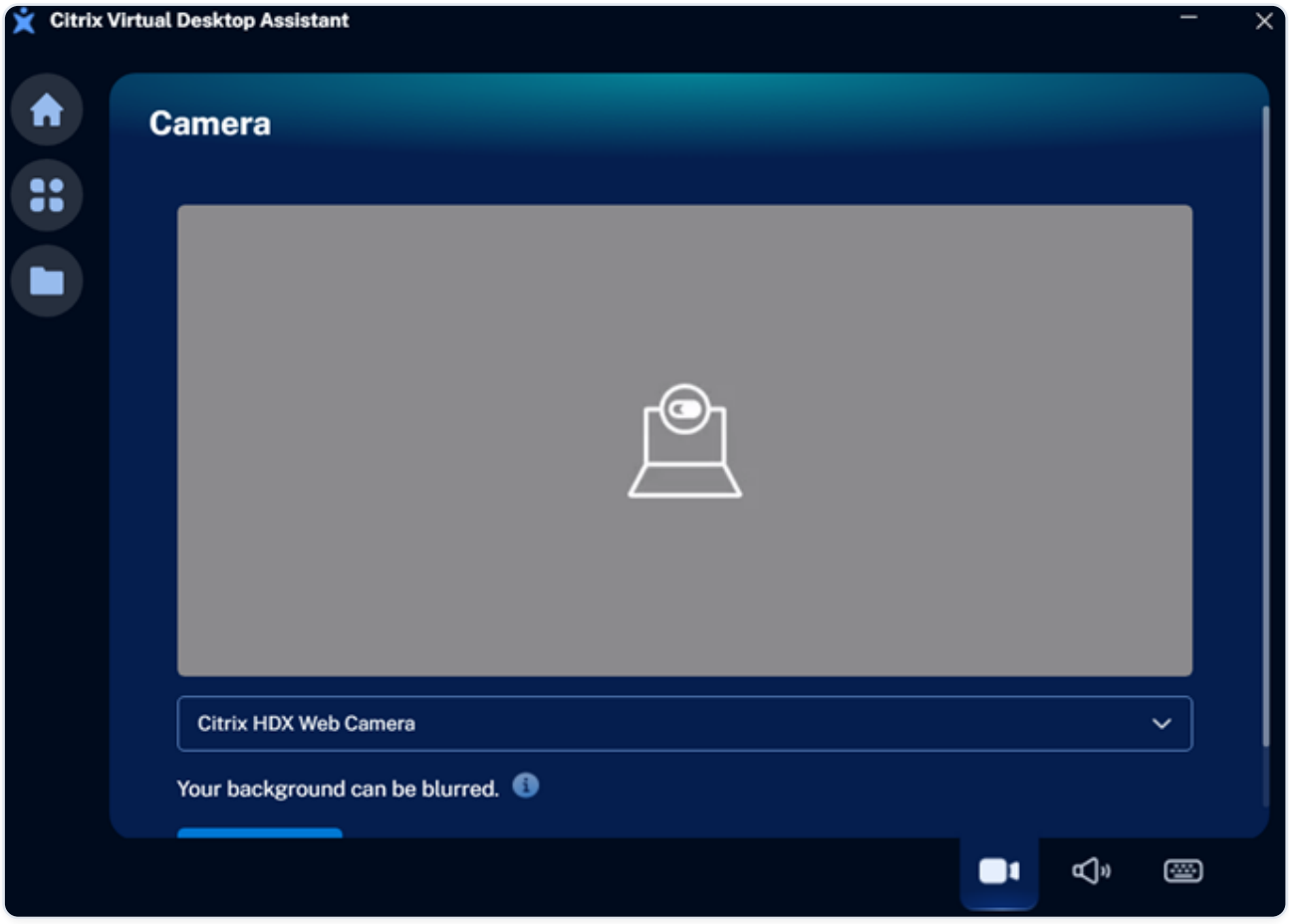
- **Test speaker** をクリックして、デモオーディオを再生して選択したスピーカーデバイスをテストします。
- VDAセッション内でオーディオデバイスの問題をトラブルシューティングする際は、**Run test** をクリックすると、アプリケーションがサウンド入力を記録します。この記録はzipファイルにエクスポートされます。このzipファイルをITまたはCitrix管理者チームと共有してサポートを

受けることができます。また、オーディオを再生してサウンドの再生を確認することもできます。



カメラページ

Citrix Virtual Desktop Assistant アプリのカメラページは、VDAセッション内のビデオ設定を構成するのに役立ちます。



- 複数のカメラが接続されている場合は、ドロップダウンリストからカメラを選択できます。

> **注:**
>
> **Citrix HDX Web Camera**のみが表示され、CWAクライアントに複数のカメラデバイスが接続されている場合は、VDAマシンを再起動して、接続されているすべてのカメラデバイスのリストを表示してください。Citrix Virtual Desktop Assistantアプリをインストールした後にのみ再起動するようにしてください。

- 背景をぼかすことができます。背景をぼかすには、**Citrix Workspace™ app > Preferences > Default webcam > Enable background blur** に移動します。
- カメラ設定を調整するには、**Retry Camera** をクリックします。ただし、カメラが他のビデオ会議ツールで使用されていないことを確認してください。

キーボードページ

キーボードページには、ローカルデバイスのキーボードレイアウト、仮想デスクトップのキーボードレイアウト、同期設定、およびキーボードショートカット設定が1つのビューに表示されま

す。これらの設定は、Citrix Workspaceアプリ（CWA）の環境設定ツールバーから更新でき、変更はAssistantアプリに反映されます。

VDAセッション内のキーボードまたはIMEの問題をトラブルシューティングするには、ページ下部の**診断レポートの収集**をクリックします。

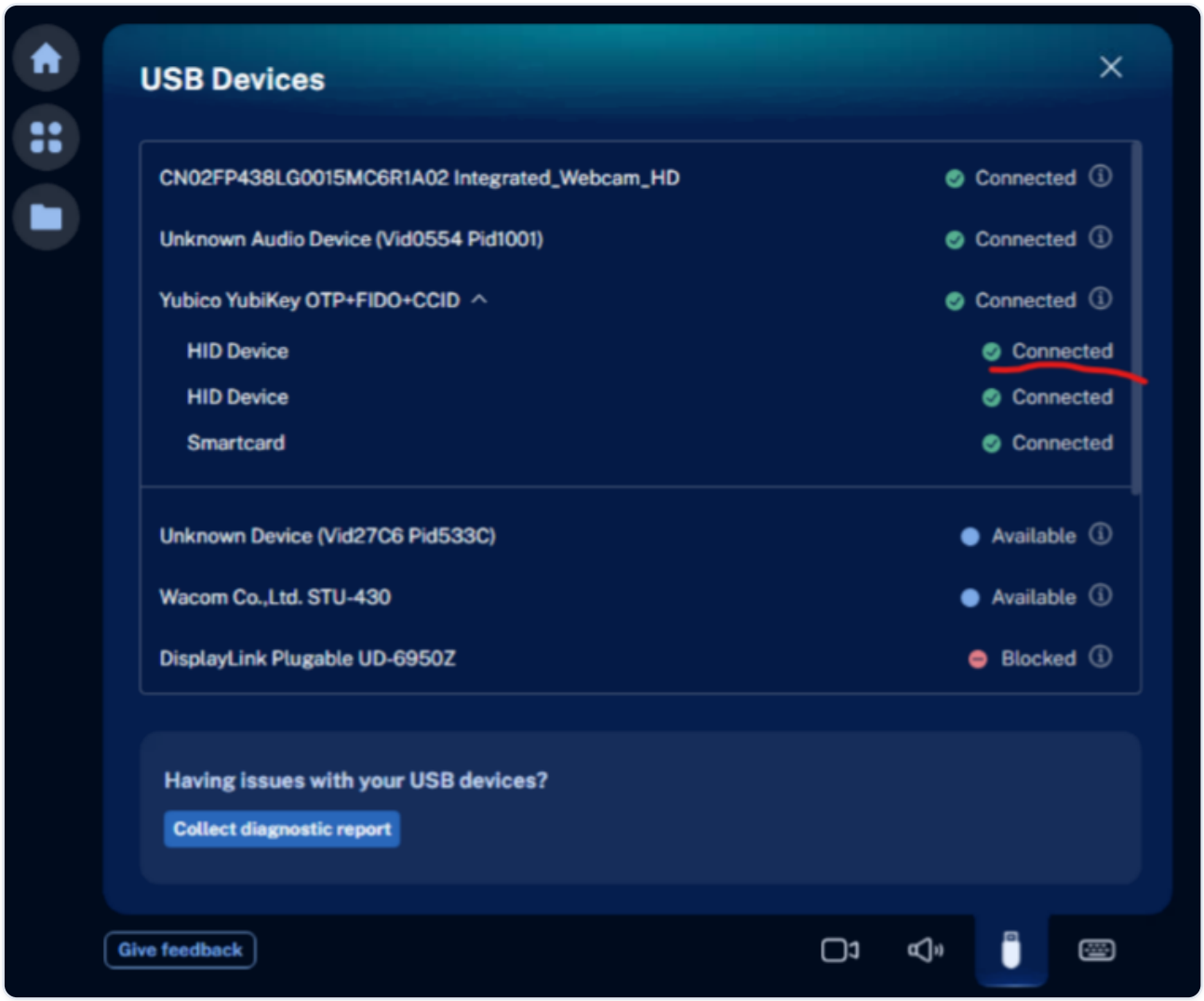


注:

情報アイコンにカーソルを合わせると、キーボード設定値について学習できます。

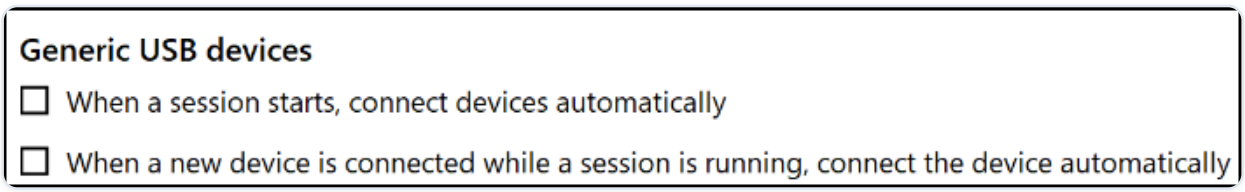
USBページ

USBページでは、USBデバイスを表示できます。



Citrix AssistantでUSB画面が表示されない場合は、以下を確認してください。

- Citrix Workspaceアプリ (CWA) のバージョンが2511以降であること。
- USBリダイレクトポリシーが無効になっていること。
- 設定ツールバーで以下のチェックボックスが選択されていること。



USBデバイスには、5つの異なるステータス値があります。

- **接続済み**: これらのデバイスは正常にリダイレクトされ、仮想チャネルを使用しており、クライアントとVDAの両方で使用できます。
- **情報付きで接続済み**: これらのUSBデバイスは正常にリダイレクトされ、VDAで使用できます。Citrix Workspaceアプリ (CWA) ツールバーから**デバイス**ツールバーにアクセスして、これらを無効にできます。

- **ドライバーが見つかりません**: これらのデバイスはVDAにドライバーをインストールする必要がありますが、現在そのドライバーが見つかりません。
- **ブロック済み**: これらのデバイスは、デバイスルールによって管理者がブロックしています。これらのデバイスを使用するには、管理者に連絡してください。
- **利用可能**: **デバイス**ツールバーからこれらのデバイスを有効にします。有効にすると、VDAに接続され、使用できるようになります。

VDAセッション内でUSBの問題をトラブルシューティングするには、ページ下部の**診断レポートの収集**をクリックします。

AOTログ

管理者がAlways On Tracing (AOT)機能を設定しており、VDAで問題が発生している場合は、**サポートバンドルのダウンロード**をクリックしてセッションのログをエクスポートし、管理者に共有してください。ログには、管理者またはサポートがバージョンに基づいて問題を特定できるように、Citrixソフトウェアのソフトウェアバージョンも記録されます。

Citrix Assistantアプリ AOT(/en-us/citrix-virtual-apps-desktops/current-release/media/assistant-aot-log.png)

バージョン情報ページ

左ペインで、**バージョン情報**アイコンを右クリックして、**バージョン情報**ページを開きます。

Citrix Assistantアプリ AOT(/en-us/citrix-virtual-apps-desktops/current-release/media/assistant-app-about-page_1.png)

Citrix Virtual Desktop Assistantアプリのバージョン情報とサードパーティライセンスエントリは、**バージョン情報**ページに表示されます。

サポートファイルをダウンロードしたり、Citrix Virtual Desktop Assistantのログとともにフィードバックを送信したりすることもできます。

Citrix Assistantアプリ AOT(/en-us/citrix-virtual-apps-desktops/current-release/media/assistant-send-feedback-page.png)

制限事項

- **一時ファイルのクリーンアップの制限**: 読み取り専用、破損している、または現在使用中のため、一時ファイルをクリーンアップできません。

- **大きなファイルの表示時間**: 「**大きなファイル**」セクションでファイルが表示されるまでにかなりの時間がかかる場合があります。これらのファイルの表示時間を短縮するための取り組みが進められています。
- **録画場所の制限**: セッション録画の保存パスは現在、英字のみをサポートしています。

モニター

管理者とヘルプデスク担当者は、さまざまな機能とツールを使用してCitrix Virtual Apps and Desktops™サイトを監視できます。これらのツールを使用すると、以下を監視できます。

- ユーザーセッションとセッションの使用状況
- ログオンパフォーマンス
- 接続とマシン（障害を含む）
- 負荷評価
- 履歴トレンド
- インフラストラクチャ

Citrix Director (シトリックス ディレクター)

Directorは、監視とトラブルシューティング、およびエンドユーザーのサポートタスクの実行に使用できるリアルタイムのWebツールです。

詳細については、Director の記事を参照してください。

構成ログ

構成ログを使用すると、管理者はサイトへの管理変更を追跡できます。構成ログは、構成変更が行われた後の問題の診断とトラブルシューティング、変更管理と構成の追跡を支援し、管理アクティビティを報告するのに役立ちます。

Studioからログに記録された情報のレポートを表示および生成できます。また、Directorでトレンドビューを使用してログに記録された項目を表示し、構成変更の通知を提供することもできます。この機能は、Studioにアクセスできない管理者にとって役立ちます。

トレンドビューは、一定期間にわたる構成変更の履歴データを提供するため、管理者は、サイトに対してどのような変更がいつ誰によって行われたかを評価し、問題の原因を特定できます。このビューは、構成情報を次の3つのカテゴリに分類します。

- 接続障害
- 失敗したシングルセッションマシン

- 失敗したマルチセッションマシン

構成ログを有効にして構成する方法の詳細については、構成ログを参照してください。Directorの記事では、そのツールからログに記録された情報を表示する方法について説明しています。

イベントログ

Citrix Virtual Apps and Desktops™内のサービスは、発生したイベントをログに記録します。イベントログは、操作の監視とトラブルシューティングに使用されます。

詳細については、イベントログを参照してください。個々の機能の記事にもイベント情報が含まれている場合があります。

構成ログ

構成ログは、サイト構成の変更と管理アクティビティをデータベースにキャプチャする機能です。この機能はデフォルトで有効になっています。ログに記録されたコンテンツは、次の目的で使用できます。

- 構成変更後、問題の診断とトラブルシューティングを行います。ログは追跡記録を提供します。
- 変更管理の支援と構成の追跡。
- 管理アクティビティを報告します。

Citrix Studioから、構成ログ設定の指定、構成ログの表示、HTMLおよびCSVレポートの生成を行うことができます。構成ログの表示は、日付範囲や全文検索結果でフィルタリングできます。強制ログが有効になっている場合、ログに記録できない構成変更は行えません。適切な権限があれば、構成ログからエントリを削除できます。構成ログ機能を使用してログコンテンツを編集することはできません。

構成ログは、PowerShell SDKと構成ログサービスを使用します。構成ログサービスは、サイト内のすべてのControllerで実行されます。いずれかのControllerが失敗した場合、別のControllerのサービスが自動的にログ要求を処理します。

デフォルトでは、構成ログ機能は有効になっており、サイト作成時に作成されるデータベース（サイト構成データベース）を使用します。データベースの別の場所を指定できます。構成ログデータベースは、サイト構成データベースと同じ高可用性機能をサポートします。

構成ログへのアクセスは、委任管理を通じて、「ログ設定の編集」および「構成ログの表示」の権限で制御されます。

構成ログは作成時にローカライズされます。たとえば、英語で作成されたログは、リーダーのロケールに関係なく、英語で読み取られます。

記録される内容

Studio、Director、およびPowerShellスクリプトから開始された構成変更と管理アクティビティがログに記録されます。ログに記録される構成変更の例には、以下に関する作業（作成、編集、削除、割り当て）が含まれます。

- マシンカタログ
- デリバリーグループ（電源管理設定の変更を含む）
- 管理者ロールとスコープ
- ホストリソースと接続
- Studioを介したCitrixポリシー

ログに記録される管理変更の例には、以下が含まれます。

- 仮想マシンまたはユーザーデスクトップの電源管理
- StudioまたはDirectorがユーザーにメッセージを送信する

次の操作はログに記録されません。

- プール管理による仮想マシンの電源投入などの自律的な操作。
- グループポリシー管理コンソール (GPMC) を介して実装されたポリシーアクション。これらのアクションのログを表示するには、Microsoftツールを使用してください。
- レジストリ、データベースへの直接アクセス、またはStudio、Director、PowerShell以外のソースを通じて行われた変更。
- 展開が初期化されると、最初の構成ログサービスインスタンスが構成サービスに登録されたときに、構成ログが利用可能になります。したがって、構成の初期段階（たとえば、データベーススキーマが取得および適用されるとき、ハイパーバイザーが初期化されるとき）はログに記録されません。

構成ログの管理

デフォルトでは、構成ログはサイトの作成時に作成されるデータベース（サイト構成データベースとも呼ばれます）を使用します。Citrixは、次の理由により、構成ログデータベース（および監視データベース）に別の場所を使用することを推奨します。

- 構成ログデータベースのバックアップ戦略は、サイト構成データベースのバックアップ戦略とは異なる可能性があります。
- 構成ログ（および監視サービス）のために収集されるデータ量によって、サイト構成データベースで利用可能な領域に悪影響が及ぶ可能性があります。
- これにより、3つのデータベースの単一障害点が分割されます。

構成ログをサポートしない製品エディションには、Studioにログノードがありません。

構成ログと強制ログの有効化と無効化

デフォルトでは、構成ログは有効になっており、強制ログは無効になっています。

1. Web Studio にサインインし、左側のペインで **Logging** を選択します。
2. アクションバーで **Preferences** を選択します。構成ログのダイアログボックスには、データベース情報が含まれており、構成ログと強制ログが有効か無効かを示します。
3. 希望するアクションを選択します。

   構成ログを有効にするには、**Enable** を選択します。これはデフォルト設定です。データベースに書き込みができない場合、ログ情報は破棄されますが、操作は続行されます。

   構成ログを無効にするには、**Disable** を選択します。以前にログが有効になっていた場合、既存のログはPowerShell SDKで読み取り可能です。

   強制ログを有効にするには、**Prevent changes to the site configuration when the database is not available** を選択します。通常ログに記録される構成変更や管理アクティビティは、構成ログデータベースに書き込みが可能な場合にのみ許可されます。強制ログは、構成ログが有効になっている場合（**Enable** が選択されている場合）にのみ有効にできます。構成ログサービスが失敗し、高可用性が使用されていない場合、強制ログが有効であると見なされます。そのような場合、通常ログに記録される操作は実行されません。

   強制ログを無効にするには、**Allow changes when to the site configuration when the database is not available** を選択します。構成ログデータベースにアクセスできない場合でも、構成変更と管理アクティビティが許可されます。これはデフォルト設定です。

構成ログデータベースの場所を変更する

強制ログが有効になっている場合、データベースの場所を変更することはできません。場所の変更には、ログに記録できない短い切断間隔が含まれるためです。

1. サポートされているSQL Serverバージョンを使用して、データベースサーバーを作成します。
2. Web Studio にサインインし、左側のペインで **Logging** を選択します。

3. アクションバーで **Preferences** を選択します。
4. ログ設定ダイアログボックスで、**Change logging database** を選択します。
5. ログデータベースの変更ダイアログボックスで、新しいデータベースサーバーを含むサーバーの場所を指定します。有効な形式については、データベースアドレス形式を参照してください。
6. Studio がデータベースを作成できるようにするには、**OK** をクリックします。プロンプトが表示されたら **OK** をクリックすると、データベースが自動的に作成されます。Studio は、現在のStudioユーザーの資格情報を使用してデータベースにアクセスしようとします。それが失敗した場合、データベースユーザーの資格情報の入力を求められます。その後、Studio はデータベーススキーマをデータベースにアップロードします。（資格情報はデータベース作成中のみ保持されます。）
7. データベースを手動で作成するには、**データベーススクリプトの生成**をクリックします。生成されたスクリプトには、データベースを手動で作成するための手順が含まれています。スキーマをアップロードする前に、データベースが空であり、少なくとも1人のユーザーがデータベースにアクセスして変更する権限を持っていることを確認してください。

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

構成ログコンテンツの表示

構成ログコンテンツを表示するには、左ペインで**ログ**を選択し、次に**イベント**タブを選択します。

デフォルトでは、イベントログは管理者名で一覧表示されます。必要に応じて、次のタスクを実行できます。

- **ログの詳細を表示します。** 高レベルの操作は、1つ以上のサービスおよびSDK呼び出し（低レベルの操作）をもたらします。上部ペインで高レベルの操作を選択すると、下部ペインに低レベルの操作が表示されます。
- **表示を並べ替えます。** 列ヘッダーをクリックして表示を並べ替えます。
- **ログをフィルターします。** 日間隔やカスタム期間などのフィルター条件を設定するか、検索ボックスにメインタスクの完全または部分的な名前を入力して、表示を絞り込みます。検索を使用した後に標準表示に戻るには、検索ボックスのテキストをクリアします。
- **ログをエクスポートします。** 選択したログまたはすべてのログをCSVファイルにエクスポートして、アーカイブまたは詳細な分析を行います。

- **列をカスタマイズします。** クライアントIPやラベルなどのデフォルト以外の列を追加して、表示をニーズに合わせて調整します。
- **ラベルを管理します。** イベントログのラベルを追加、編集、削除して、ログの整理と追跡を強化します。

表示の特性：

- 操作が完了する前に失敗した場合、ログ操作がデータベースで完了しない可能性があります。たとえば、開始レコードに対応する停止レコードがない場合などです。このような場合、ログには情報が不足していることが示されます。時間範囲に基づいてログを表示すると、データが基準に一致する場合、不完全なログが表示されます。

  たとえば、過去5日間のログを要求し、過去5日間に開始時刻があるログに終了時刻がない場合、それも含まれます。
- PowerShellコマンドレットを呼び出すスクリプトを使用する場合、親の高レベル操作を指定せずに低レベル操作を作成すると、構成ログは代理の高レベル操作を作成します。

レポートを生成する

構成ログデータを含むCSVおよびHTMLレポートを生成できます。

- CSVレポートには、指定された時間間隔のすべてのログデータが含まれます。データベース内の階層データは、単一のCSVテーブルにフラット化されます。データのどの側面もファイル内で優先されません。書式設定は使用されず、人間が読み取れることは想定されていません。ファイル（MyReportという名前）には、普遍的に利用可能な形式でデータが含まれています。CSVファイルは、データのアーカイブや、Microsoft Excelなどのレポート作成ツールまたはデータ操作ツールのデータソースとしてよく使用されます。
- HTMLレポートは、指定された時間間隔のログデータを人間が読み取れる形式で提供します。変更を確認するための構造化されたナビゲート可能なビューを提供します。HTMLレポートは、SummaryとDetailsという名前の2つのファイルで構成されます。Summaryには、各操作がいつ、誰によって、どのような結果になったかなど、高レベルの操作が一覧表示されます。各操作の横にある**Details**リンクをクリックすると、Detailsファイル内の低レベルの操作に移動し、追加情報が表示されます。

構成ログレポートを生成するには、Studioナビゲーションペインで**Logging**を選択し、アクションバーで**Create custom report**を選択します。

- レポートの日付範囲を選択します。
- レポート形式（CSV、HTML、またはその両方）を選択します。

- レポートを保存する場所を参照します。

構成ログコンテンツを削除する

構成ログを削除するには、特定の委任管理権限とSQL Serverデータベース権限が必要です。

- **委任管理:** 展開構成の読み取りを許可する委任管理ロールが必要です。完全管理者ロールにはこの権限があります。カスタムロールには、カテゴリでまたはが選択されている必要があります。

  構成ログデータを削除する前にバックアップを作成するには、カスタムロールのカテゴリでまたはが選択されている必要もあります。

- **SQL Serverデータベース:** データベースからレコードを削除する権限を持つSQL Serverログインが必要です。これを行うには2つの方法があります。

  - データベースサーバー上のあらゆるアクティビティを実行できるsysadminサーバーロールを持つSQL Serverデータベースログインを使用します。または、`serveradmin`または`setupadmin`サーバーロールを使用すると、削除操作を実行できます。
  - 展開でより高いセキュリティが必要な場合は、データベースからレコードを削除する権限を持つデータベースユーザーにマッピングされた非sysadminデータベースログインを使用します。

    a. SQL Server Management Studioで、「sysadmin」以外のサーバーロールを持つSQL Serverログインを作成します。

    b. ログインをデータベース内のユーザーにマッピングします。SQL Serverは、ログインと同じ名前のユーザーをデータベース内に自動的に作成します。

    c. データベースロールメンバーシップで、データベースユーザーのロールメンバーのうち少なくとも1つを指定します: `ConfigurationLoggingSchema_ROLE` または `dbowner`。

    詳細については、SQL Server Management Studioのドキュメントを参照してください。

構成ログを削除するには:

1. Web Studioにサインインし、左ペインで**ログ**を選択します。
2. アクションバーで**ログの削除**を選択します。
3. ログを削除する前にバックアップを作成するかどうかを尋ねられます。バックアップを作成することを選択した場合、バックアップアーカイブが保存される場所を参照します。バックアップはCSVファイルとして作成されます。

構成ログがクリアされた後、ログの削除は空のログに投稿される最初のアクティビティです。そのエントリには、誰がいつログを削除したかに関する詳細が記載されています。

APIおよびPowerShellログの表示

現在のセッション中に作成されたAPIリクエストを監視するには、**API**タブをクリックします。APIログは、Web Studioからサインアウトするとクリアされます。

その日に行ったUIアクションに対応するPowerShellコマンドを表示するには、**PowerShell**タブをクリックします。

構成ログにメタデータを関連付ける

ログレコードに`MetadataMap`と呼ばれる`name-value`ペアを関連付けることで、構成ログにメタデータを添付できます。

> **注:**
>
> - メタデータは、高レベルの操作オブジェクトにのみ添付できます。
> - メタデータは、実行時に既存のレコードに関連付けられます。

メタデータを設定する

ログレコードを`MetadataMap`に関連付けるには、PowerShellコマンド`Set-LogHighLevelOperationMetadata`を実行します。 `Set-LogHighLevelOperationMetadata`は次のパラメーターを受け取ります。

- **Id**: 上位レベルの操作のID。
- **InputObject**: メタデータを追加する上位レベルの操作。これは、上位レベルの操作オブジェクトまたはオブジェクトのリストがPowerShellコマンドに渡される`Id`パラメーターの代替です。
- **Name**: 追加するメタデータのプロパティ名。このプロパティは、指定された上位レベルの操作に対して一意である必要があります。このプロパティには、次の文字を含めることはできません: ()\/;:#.*?=<>|'"。
- **Value**: プロパティの値。
- **Map**: プロパティの(名前、値)ペアの辞書。これは、`-Name`および`-Value`パラメーターを使用してメタデータを設定する代替手段です。

たとえば、Id 40を持つすべての高レベルログレコードにメタデータを添付するには、次のPowerShellコマンドを実行します。

```
Get-LogHighLevelOperation – Id 40 | Set-LogHighLevelOperationMetadata -Name A -Value B
```

ユーザー`abc@example.com`を持つ上位レベルのレコードにメタデータを添付するには、次のPowerShellコマンドを実行します。

```
Get-LogHighLevelOperation – User `abc@example.com` | Set-LogHighLevelOperationMetadata -Name C -Value D
```

メタデータを使用して取得する

関連付けられたメタデータを使用してログレコードを取得するには、次のPowerShellコマンドを実行します。

- キーと値で検索:

  ```
  Get-LogHighLevelOperation -Metadata "Key:Value"
  ```

- 値で任意のキーを検索:

  ```
  Get-LogHighLevelOperation -Metadata "*:Value"
  ```

- キーと任意の値で検索:

  ```
  Get-LogHighLevelOperation -Metadata "Key:*"
  ```

メタデータを削除する

関連付けられたメタデータを削除するには、PowerShell コマンド `Remove-LogHighLevelOperationMetadata` を実行します。 `Remove-LogHighLevelOperationMetadata` は次のパラメーターを受け入れます。

- **Id**: 高レベル操作のID。
- **InputObject**: メタデータを追加する高レベル操作。これは、高レベル操作オブジェクトまたはオブジェクトのリストがPowerShellコマンドに渡される `Id`` パラメーターの代替です。
- **Name**: 削除するメタデータのプロパティ名。指定されたオブジェクトのすべてのメタデータを削除するには、$null に設定します。
- **Map**: プロパティの (名前、値) ペアの辞書。これはハッシュテーブル (@{"name1" = "val1"; "name2" = "val2"} で作成) または文字列辞書 (new-object

"System.Collections.Generic.Dictionary" で作成) のいずれかです。マップ内のキーと名前が一致するプロパティは削除されます。

ベストプラクティス

1. **まず直接パラメーターを使用します。**アクションについてわかっていることを、対応するパラメーター (`-User`、`-OperationType`、`-TargetType`、`-Source`、または `-IsSuccessful`) と一致させます。
2. **常に時間範囲を含めます。**`-StartTime` と `-EndTime` は、あらゆるクエリで最も効果的な最初のフィルターです。
3. **高レベルから低レベルへドリルダウンします。**特定のアクションを調査するときは、まず高レベル操作を取得し、そのIDを `-HighLevelOperationId` とともに使用します。
4. **エクスポートを対象期間に限定します。**`-StartDateRange` と `-EndDateRange` を使用して、関連する時間枠をターゲットにします。
5. **表示名が不要な場合は、エクスポートで `-RawReport` を使用します。**これにより、処理時間と出力サイズが削減されます。

イベントログ

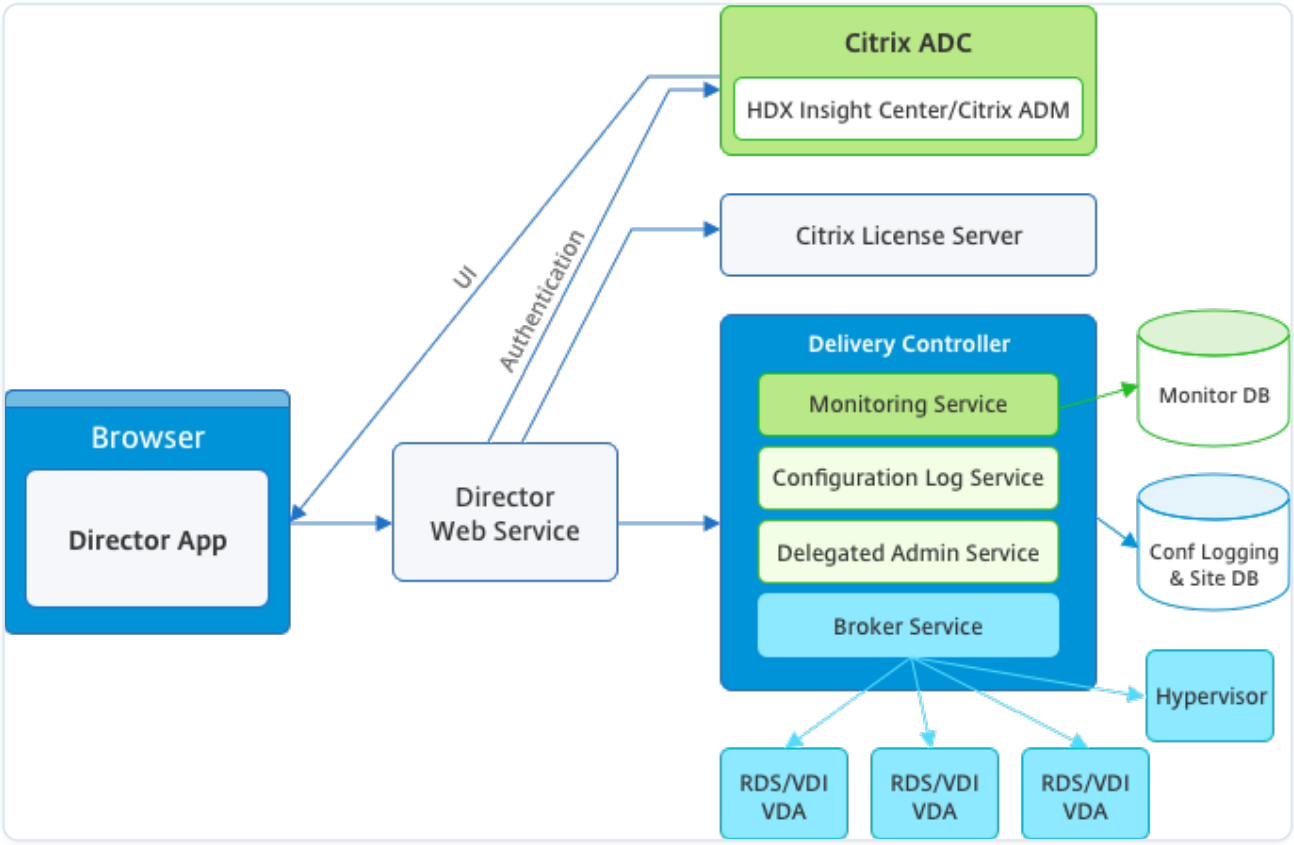
以下の記事では、Citrix Virtual Apps and Desktops 内のサービスによってログに記録される可能性のあるイベントを一覧表示し、説明します。

この情報は網羅的ではありません。読者は、追加のイベント情報について、個々の機能記事を確認してください。

- Citrix Broker Service イベント
- Citrix FMA Service SDK イベント
- シトリックス コンフィギュレーションサービス イベント
- シトリックス デリゲート管理サービス イベント

ディレクター

ディレクターは、Citrix Virtual Apps and Desktops 用の監視およびトラブルシューティングコンソールです。



ディレクターは以下にアクセスできます:

- Analytics、Performance Manager、および Network Inspector と統合された統合コンソールを使用して、Broker Agent からリアルタイムデータにアクセスします。以下の分析はCitrix ADMによって提供され、Citrix Virtual Apps™ または Desktops 環境におけるネットワークに起因するボトルネックを特定します:
  - 健全性と容量の保証のためのパフォーマンス管理
  - 履歴トレンドとネットワーク分析
- Configuration Loggingデータベースにアクセスするためにモニターデータベースに保存されている履歴データ。
- Citrix ADM を使用してCitrix Gateway からのICA®データ。

- Citrix Virtual Apps または Desktops の仮想アプリケーション、デスクトップ、およびユーザーのエンドユーザーエクスペリエンスの可視性を得る。
- 効果的なトラブルシューティングのために、ネットワークデータをアプリケーションデータおよびリアルタイムメトリックと関連付ける。
- Citrix Virtual Desktop 7 Director監視ツールと統合する。

ディレクターは、Citrix Virtual Apps または Desktops Site のリアルタイムおよび履歴の健全性監視を提供するトラブルシューティングダッシュボードを使用します。この機能により、リアルタイムで障害を確認でき、エンドユーザーが何を経験しているかをよりよく把握できます。

Director機能とDelivery Controller (DC)、VDA、およびその他の依存コンポーネントとの互換性に関する詳細については、「機能互換性マトリックス」を参照してください。

> **注:**
>
> MeltdownおよびSpectreの投機的実行サイドチャネル脆弱性の開示に伴い、Citrixは、関連する緩和パッチをインストールすることを推奨します。これらのパッチはSQL Serverのパフォーマンスに影響を与える可能性があります。詳細については、Microsoftサポート記事「SpectreおよびMeltdownサイドチャネル脆弱性からのSQL Serverの保護」を参照してください。Citrixは、本番環境にパッチを展開する前に、規模をテストし、ワークロードを計画することを推奨します。

> Director は、デフォルトで Delivery Controller 上の Web サイトとしてインストールされます。前提条件およびその他の詳細については、このリリースの システム要件 ドキュメントを参照してください。Director のインストールと構成に関する具体的な情報については、Director のインストールと構成 を参照してください。

Director へのログオン

Director の Web サイトは、https または `http://<Server FQDN>/Director` にあります。

マルチサイト展開でいずれかのサイトがダウンしている場合、ダウンしているサイトへの接続を試行するため、ログオンに少し時間がかかります。

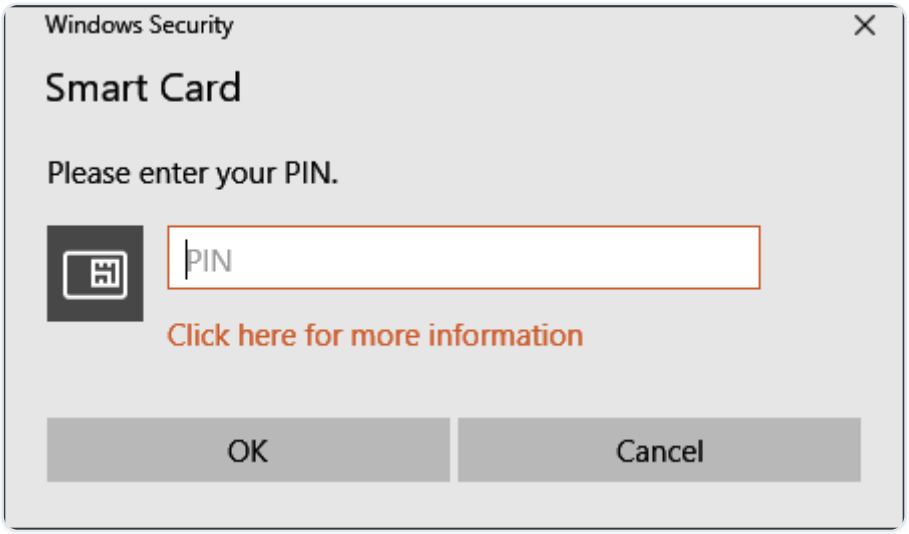
PIV スマートカード認証での Director の使用

Director は、Personal Identity Verification (PIV) ベースのスマートカード認証によるログオンをサポートするようになりました。この機能は、アクセス制御にスマートカードベースの認証を使用する組織や政府機関にとって有用です。 スマートカード認証には、Director サーバーおよび Active Directory での特定の構成が必要です。構成手順については、PIV スマートカード認証の構成 で詳しく説明されています。

> **注:**
>
> スマートカード認証は、同じ Active Directory ドメインのユーザーのみがサポートされます。

必要な構成を実行した後、スマートカードを使用して Director にログオンできます。

1. スマートカードをスマートカードリーダーに挿入します。
2. ブラウザーを開き、Director の URL `https://<directorfqdn>/Director` にアクセスします。
3. 表示されたリストから有効なユーザー証明書を選択します。
4. スマートカードトークンを入力します。



5. 認証されると、Director ログオンページで追加の資格情報を入力することなく Director にアクセスできます。

統合 Windows 認証での Director の使用

統合Windows認証（IWA）を使用すると、ドメイン参加ユーザーはDirectorログオンページで資格情報を再入力することなく、Directorに直接アクセスできます。統合Windows認証とDirectorを使用するための前提条件は次のとおりです。

- DirectorをホストするIIS Webサイトで統合Windows認証を有効にします。Directorをインストールすると、匿名認証とフォーム認証が有効になります。統合Windows認証とDirectorをサポートするには、匿名認証を無効にし、Windows認証を有効にします。ドメイン外のユーザーの認証のために、フォーム認証は有効のままにしておく必要があります。

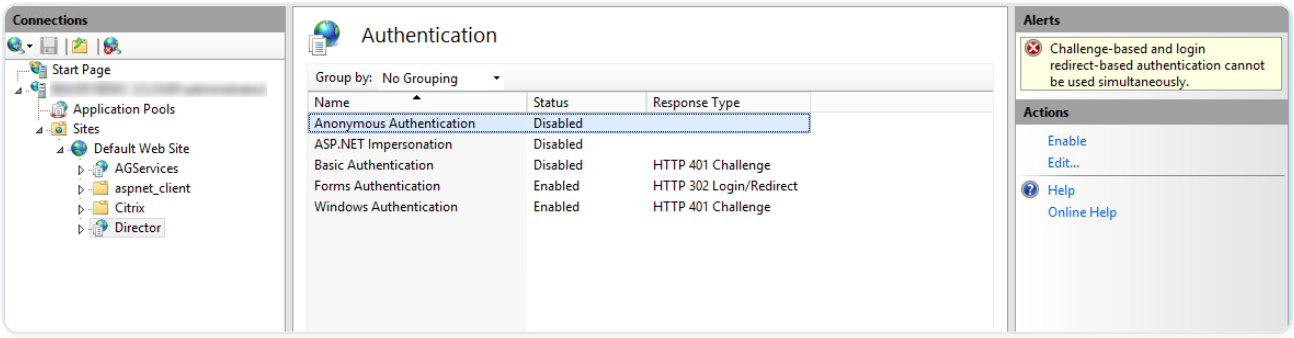
  a. IISマネージャーを起動します。

  b. **サイト** \> **既定のWebサイト** \> **Director**に移動します。

  c. **認証**を選択します。

  d. **匿名認証**を右クリックし、**無効**を選択します。

  e. **Windows認証**を右クリックし、**有効**を選択します。



- Directorマシンに対してActive Directoryの委任権限を構成します。構成が必要となるのは、DirectorとDelivery Controller™が別々のマシンにインストールされている場合のみです。

  a. Active Directoryマシンで、Active Directory管理コンソールを開きます。

  b. Active Directory管理コンソールで、**ドメイン名** \> **コンピューター**に移動します。Directorマシンを選択します。

  c. 右クリックして**プロパティ**を選択します。

  d. プロパティで、**委任**タブを選択します。

  e. **このコンピューターを、任意のサービスへの委任のために信頼する（Kerberosのみ）**オプションを選択します。

- Directorへのアクセスに使用するブラウザーは、統合Windows認証をサポートしている必要があります。FirefoxおよびChromeでは、追加の構成手順が必要になる場合があります。詳細については、ブラウザーのドキュメントを参照してください。

- 監視サービスは、Microsoft .NET Framework 4.5.1 以降の、Director のシステム要件に記載されているサポート対象バージョンを実行している必要があります。詳しくは、「」(/ja-jp/citrix-virtual-apps-desktops/current-release/system-requirements.html#citrix-director)を参照してください。

ユーザーがDirectorからログオフするか、セッションがタイムアウトすると、ログオンページが表示されます。ログオンページから、ユーザーは認証の種類を**自動ログオン**または**ユーザー資格情報**に設定できます。

インターフェイスビュー

Directorは、特定の管理者向けに調整されたさまざまなインターフェイスビューを提供します。製品の権限によって、表示される内容と利用可能なコマンドが決まります。

たとえば、ヘルプデスク管理者は、ヘルプデスクタスクに合わせて調整されたインターフェイスを表示します。Directorを使用すると、ヘルプデスク管理者は問題を報告しているユーザーを検索し、そのユーザーに関連付けられたアクティビティを表示できます。たとえば、ユーザーのアプリケーションとプロセスのステータスなどです。応答しないアプリケーションやプロセスを終了する、ユーザーのマシンでシャドウ操作を実行する、マシンを再起動する、ユーザープロファイルをリセットするなどのアクションを実行することで、問題を迅速に解決できます。

対照的に、完全な管理者はサイト全体を表示および管理し、複数のユーザーおよびマシンに対してコマンドを実行できます。ダッシュボードは、セッションのステータス、ユーザーログオン、サイトインフラストラクチャなど、展開の主要な側面を概観できます。情報は毎分更新されます。問題が発生した場合、発生した障害の数と種類に関する詳細が自動的に表示されます。

Directorにおけるさまざまな役割とその権限について詳しくは、「」(/ja-jp/citrix-virtual-apps-desktops/current-release/director/install-and-configure/permissions.html)を参照してください。

Pendoによる使用状況データの収集

Directorのインストール後、DirectorサービスはPendoを使用して使用状況データの収集を開始します。トレンドページの利用状況に関する統計とOData API呼び出しの分析が収集されます。分析の収集は、Citrixプライバシーポリシーに準拠しています。Directorをインストールすると、データ収集はデフォルトで有効になります。

Pendoのデータ収集をオプトアウトするには、Directorがインストールされているマシンのレジストリキーを編集します。レジストリキーが存在しない場合は、作成して目的の値に設定します。レジストリキーの値を変更した後、Directorインスタンスを更新します。

注意：レジストリエディターを誤って使用すると、オペレーティングシステムの再インストールが必要になる深刻な問題が発生する可能性があります。Citrixは、レジストリエディターの誤用によって発生した問題が解決されることを保証できません。レジストリエディターは、ご自身の責任において使用してください。Citrixは、Windowsレジストリを変更する前にバックアップすることをお勧めします。

場所：HKEY_LOCAL_MACHINE\Software\Citrix\Director

名前：DisableGoogleAnalytics

> **注:**

> 以前は、DirectorサービスはGoogle Analyticsを使用してデータを収集していました。同じレジストリキーがPendoでも使用されるようになりました。

> 値：0 = 有効（デフォルト）、1 = 無効

Pendoによるデータ収集を無効にするには、次のPowerShellコマンドレットを使用できます。

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director



New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name
DisableGoogleAnalytics -PropertyType DWORD -Value 1
```

新機能ガイド

Directorには、Pendoを使用して、現在のバージョンのDirectorでリリースされた新機能に関する洞察を提供する製品内ガイドがあります。適切な製品内メッセージと組み合わせた簡単な概要は、製品の新機能を理解するのに役立ちます。

この機能をオプトアウトするには、Directorがインストールされているマシンで、以下に説明するようにレジストリキーを編集します。レジストリキーが存在しない場合は、作成して目的の値に設定します。レジストリキーの値を変更した後、Directorインスタンスを更新してください。

> **注意:**

> レジストリエディターを誤って使用すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrixは、レジストリエディターの誤った使用に起因する問題が解決できることを保証できません。レジストリエディターは自己責任で使用してください。Citrixは、変更を加える前にWindowsレジストリをバックアップすることをお勧めします。

> 場所: HKEY_LOCAL_MACHINE\Software\Citrix\Director

名前: DisableGuidedHelp

値: 0 = 有効（デフォルト）、1 = 無効

製品内ガイドを無効にするには、次のPowerShellコマンドレットを使用できます。

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director



New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name DisableGuidedHelp
-PropertyType DWORD -Value 1
```

参照記事

- Citrix DirectorからのMTTRの削減
- Citrix Director - PowerShellによるアラートと通知の管理と構成
- Citrix Virtual Apps and Desktops開発者向けドキュメント

関連製品の新機能

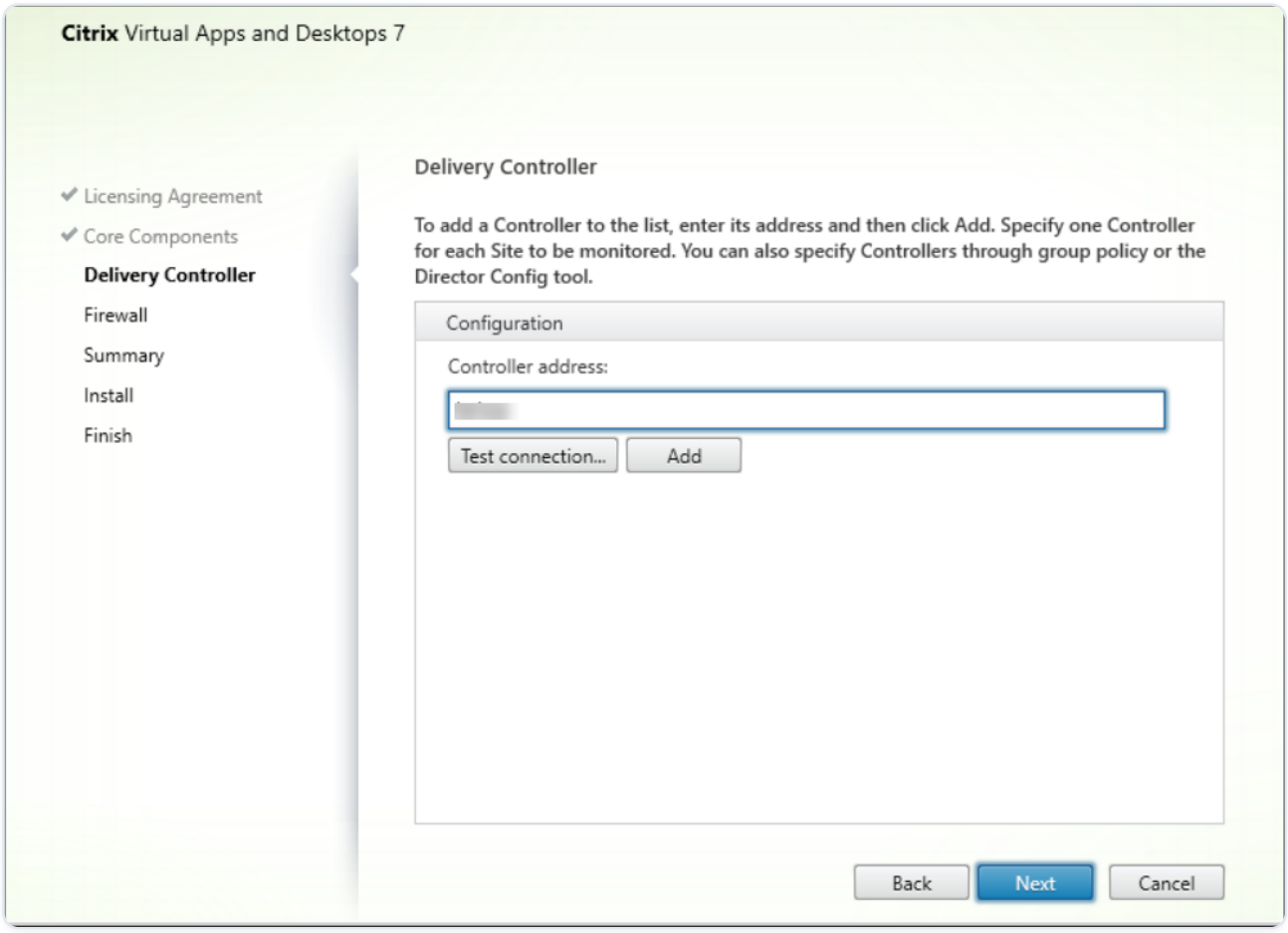
- シトリックス DaaS
- StoreFront
- セキュアプライベートアクセス
- シトリックス エンタープライズ ブラウザ
- Citrix Workspace (シトリックス ワークスペース)
- プロビジョニング

インストールと構成

Directorのインストール

Citrix Virtual Apps and Desktopsのフル製品ISOインストーラーを使用してDirectorをインストールします。これにより、前提条件の確認、不足しているコンポーネントのインストール、Director Webサイトのセットアップ、および基本的な構成が実行されます。前提条件およびその他の詳細については、このリリースのシステム要件ドキュメントを参照してください。このリリースのDirectorは、Virtual Apps 6.5より前の展開、またはVirtual Desktops 7より前の展開とは互換性がありません。 ISOインストーラーによって提供されるデフォルト構成は、一般的な展開に対応します。インストール時にDirectorが含まれていなかった場合は、ISOインストーラーを使用してDirectorを追加します。追加のコンポーネントを追加するには、ISOインストーラーを再実行し、インストールするコンポーネントを選択します。ISOインストーラーの使用方法については、インストールドキュメントのコアコンポーネントのインストールを参照してください。Citrixでは、.MSIファイルではなく、フル製品ISOインストーラーのみを使用してインストールすることをお勧めします。

DirectorがControllerにインストールされている場合、サーバーアドレスとしてlocalhostが自動的に構成され、Directorはデフォルトでローカルのcontrollerと通信します。Controllerから離れた専用サーバーにDirectorをインストールする場合は、ControllerのFQDNまたはIPアドレスを入力するよう求められます。



注:

追加をクリックして、監視するControllerを追加します。

Directorはデフォルトで、指定されたControllerと通信します。監視するサイトごとにControllerアドレスを1つだけ指定してください。Directorは、同じサイト内の他のすべてのControllerを自動的に検出し、指定したControllerが失敗した場合は、それらの他のControllerにフォールバックします。

注:

DirectorはController間で負荷分散を行いません。

ブラウザーとWebサーバー間の通信を保護するために、Citrix®は、DirectorをホストするIIS WebサイトでTLSを実装することをお勧めします。手順については、Microsoft IISのドキュメントを参照してください。TLSを有効にするためにDirectorの構成は必要ありません。

Directorの展開と構成

Directorが複数のサイトを含む環境で使用される場合、Controller、Director、およびその他のコアコンポーネントがインストールされているすべてのサーバーでシステムクロックを同期してください。そうしないと、Directorでサイトが正しく表示されない可能性があります。

> **重要:**
>
> ネットワーク経由でプレーンテキストで送信されるユーザー名とパスワードのセキュリティを保護するため、Director接続にはHTTPではなくHTTPSのみを使用してください。特定のツールは、HTTP（暗号化されていない）ネットワークパケット内のプレーンテキストのユーザー名とパスワードを読み取ることができ、ユーザーにとって潜在的なセキュリティリスクを生み出す可能性があります。

権限の構成

Directorにログオンするには、Directorの権限を持つ管理者はActive Directoryドメインユーザーであり、以下の権限を持っている必要があります。

- 検索対象となるすべてのActive Directoryフォレストにおける読み取り権限（高度な構成を参照）。
- 構成された委任管理者ロール ((/ja-jp/citrix-virtual-apps-desktops/current-release/director/install-and-configure/permissions.html)の「委任管理とDirector」を参照)。
- ユーザーをシャドウするには、管理者はWindowsリモートアシスタンス用のMicrosoftグループポリシーを使用して構成する必要があります。さらに：
  - VDAをインストールする際、すべてのユーザーデバイスでWindowsリモートアシスタンス機能が有効になっていることを確認してください（デフォルトで選択されています）。
  - Directorをサーバーにインストールする場合、Windowsリモートアシスタンスがインストールされていることを確認してください（デフォルトで選択されています）。ただし、サーバーではデフォルトで無効になっています。Directorがエンドユーザーにアシスタンスを提供するために、この機能を有効にする必要はありません。Citrixは、サーバーのセキュリティを向上させるために、この機能を無効のままにしておくことを推奨します。
  - 管理者がWindowsリモートアシスタンスを開始できるようにするには、リモートアシスタンスの適切なMicrosoftグループポリシー設定を使用して、必要な権限を付与します。詳しくは、CTX239706: How to configure Shadow feature in latest Director versionsを参照してください。

DirectorとのCitrix uberAgent®統合

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

Citrix Virtual Apps and Desktopsのインストールの一部としてuberAgentをインストールする方法の詳細については、uberAgentのドキュメントを参照してください。

主な機能：

ローカルアプリケーション使用状況の監視: Citrix uberAgentを使用すると、仮想デスクトップセッション内で起動されたアプリケーション（ローカルアプリケーションとも呼ばれます）の使用状況を監視でき、Directorとの統合により、データはDirectorダッシュボードで直接利用できます（Platinumライセンスで利用可能）。

DirectorとのCitrix uberAgent統合の構成

Citrix uberAgentのインストール後、DirectorとuberAgentを完全に統合して使用するために、Citrix Web Studio™で次のポリシーを構成します。

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

構成が完了すると、データはCitrix Directorのアプリケーション使用状況の監視セクションで利用可能になります。

> **注:**
>
> uberAgentのローカルアプリケーション使用状況データがDirectorで集計され表示されるまでには、少なくとも1日かかります。

高度な構成

Director は、ユーザー、Delivery Controller (DC)、VDA、および Director が異なるフォレストに配置されているフォレスト構成にまたがるマルチフォレスト環境をサポートできます。これには、フォレスト間の信頼関係と構成設定の適切なセットアップが必要です。

マルチフォレスト環境での推奨構成

推奨される構成では、ドメイン全体の認証を使用して、フォレスト間で送信および受信フォレスト信頼関係を作成する必要があります。

マルチフォレストサイト構成(/en-us/citrix-virtual-apps-desktops/current-release/media/multiforest-config.png)

Director からの信頼関係により、異なるフォレストにあるユーザーセッション、VDA、および Delivery Controller の問題をトラブルシューティングできます。

Director が複数のフォレストをサポートするために必要な高度な構成は、インターネットインフォメーションサービス (IIS) マネージャーで定義された設定によって制御されます。

> **重要:**

> IIS で設定を変更すると、Director サービスは自動的に再起動し、ユーザーをログオフします。

> IIS を使用して高度な設定を構成するには:

1. インターネットインフォメーションサービス (IIS) マネージャーコンソールを開きます。
2. デフォルトの Web サイトの下にある Director Web サイトに移動します。
3. をダブルクリックします。
4. 設定をダブルクリックして編集します。
5. をクリックして新しい設定を追加します。

Director は Active Directory を使用してユーザーを検索し、より多くのユーザーおよびマシン情報を参照します。デフォルトでは、Director は次のドメインまたはフォレストを検索します。

- 管理者アカウントがメンバーです。
- Director Webサーバーがメンバーです（異なる場合）。

Directorは、Active Directoryグローバルカタログを使用してフォレストレベルで検索を実行しようとします。フォレストレベルで検索する権限がない場合、ドメインのみが検索されます。

別のActive Directoryドメインまたはフォレストからデータを検索または参照するには、検索するドメインまたはフォレストを明示的に設定する必要があります。IISマネージャーで、Director Webサイトに次のアプリケーション設定を構成します。

```
Connector.ActiveDirectory.Domains = (user),(server)
```

値属性のuserとserverは、それぞれDirectorユーザー（管理者）とDirectorサーバーのドメインを表します。

追加のドメインまたはフォレストからの検索を有効にするには、この例に示すように、ドメイン名をリストに追加します。

```
Connector.ActiveDirectory.Domains = (user),(server),\&lt;domain1\>,
\&lt;domain2\>
```

リスト内の各ドメインについて、Directorはフォレストレベルで検索を実行しようとします。フォレストレベルで検索する権限がない場合、ドメインのみが検索されます。

ドメインローカルグループの構成

ほとんどのCitrix Service Provider（CSP）は、インフラストラクチャフォレストにVDA、DC、およびDirectorで構成される同様の環境設定を持っています。ユーザーまたはユーザーグループのレコードはカスタマーフォレストに属します。インフラストラクチャフォレストからカスタマーフォレストへの一方向の送信信頼が存在します。

CSP管理者は通常、インフラストラクチャフォレストにドメインローカルグループを作成し、カスタマーフォレストのユーザーまたはユーザーグループをこのドメインローカルグループに追加します。

推奨されるマルチフォレストサイト構成(/en-us/citrix-virtual-apps-desktops/current-release/media/domainlocalgroup-config.png)

Directorはこのようなマルチフォレスト設定をサポートし、ドメインローカルグループを使用して構成されたユーザーのセッションを監視できます。

1. IISマネージャーで、Director Webサイトに次のアプリケーション設定を追加します。

```
Connector.ActiveDirectory.DomainLocalGroupSearch= true



DomainLocalGroupSearchDomains= \&lt;domain1\>,\&lt;domain2\>
```

\<domain1\>\<domain2\> は、ドメインローカルグループが存在するフォレストの名前です。

2. Web Studioでドメインローカルグループをデリバリーグループに割り当てます。
3. IISを再起動し、変更を有効にするためにDirectorに再度ログオンします。これで、Directorはこれらのユーザーのセッションを監視し、表示できるようになります。

Directorにサイトを追加する

Directorがすでにインストールされている場合は、複数のサイトで動作するように構成します。構成するには、各DirectorサーバーでIISマネージャーコンソールを使用して、アプリケーション設定のサーバーアドレスリストを更新します。

各サイトのControllerのアドレスを次の設定に追加します。

```
Service.AutoDiscoveryAddresses = SiteAController,SiteBController
```

SiteAControllerとSiteBControllerは、2つの異なるサイトのDelivery Controllerのアドレスです。

アクティビティマネージャーで実行中のアプリケーションの可視性を無効にする

デフォルトでは、DirectorのActivity Managerは、ユーザーセッションで実行されているすべてのアプリケーションのリストを表示します。この情報は、DirectorのActivity Manager機能にアクセスできるすべての管理者によって表示されます。委任された管理者ロールの場合、これにはフル管理者、デリバリーグループ管理者、およびヘルプデスク管理者が含まれます。

ユーザーのプライバシーと実行中のアプリケーションを保護するために、実行中のアプリケーションを一覧表示する**アプリケーション**タブを無効にすることができます。

警告:

レジストリを誤って編集すると、オペレーティングシステムを再インストールする必要があるような深刻な問題が発生する可能性があります。Citrix® は、レジストリエディターの誤っ

> た使用によって生じる問題が解決されることを保証しません。レジストリエディターは自己責任で使用してください。編集する前に必ずレジストリをバックアップしてください。

1. VDAで、`HKEY_LOCAL_MACHINE\Software\Citrix\Director\TaskManagerDataDisplayed`にあるレジストリキーを変更します。デフォルトでは、キーは1に設定されています。値を0に変更すると、VDAから情報が収集されず、Activity Managerに表示されなくなります。
2. Directorがインストールされているサーバーで、実行中のアプリケーションの可視性を制御する設定を変更します。デフォルトでは、値は「true」であり、アプリケーションタブで実行中のアプリケーションの可視性を許可します。値を「false」に変更すると、可視性が無効になります。このオプションは、DirectorのActivity Managerのみに影響し、VDAには影響しません。次の設定の値を変更します。 UI.TaskManager.EnableApplications = false

> **重要:**
>
> 実行中のアプリケーションの表示を無効にするには、Activity Managerにデータが表示されないように両方の変更を行います。

PIVスマートカード認証を構成する

この記事では、スマートカード認証機能を有効にするためにDirectorサーバーとActive Directoryで必要な構成を一覧表示します。

> **注:**
>
> スマートカード認証は、同じActive Directoryドメインのユーザーのみがサポートされます。

Directorサーバーの構成

Directorサーバーで以下の構成手順を実行します。

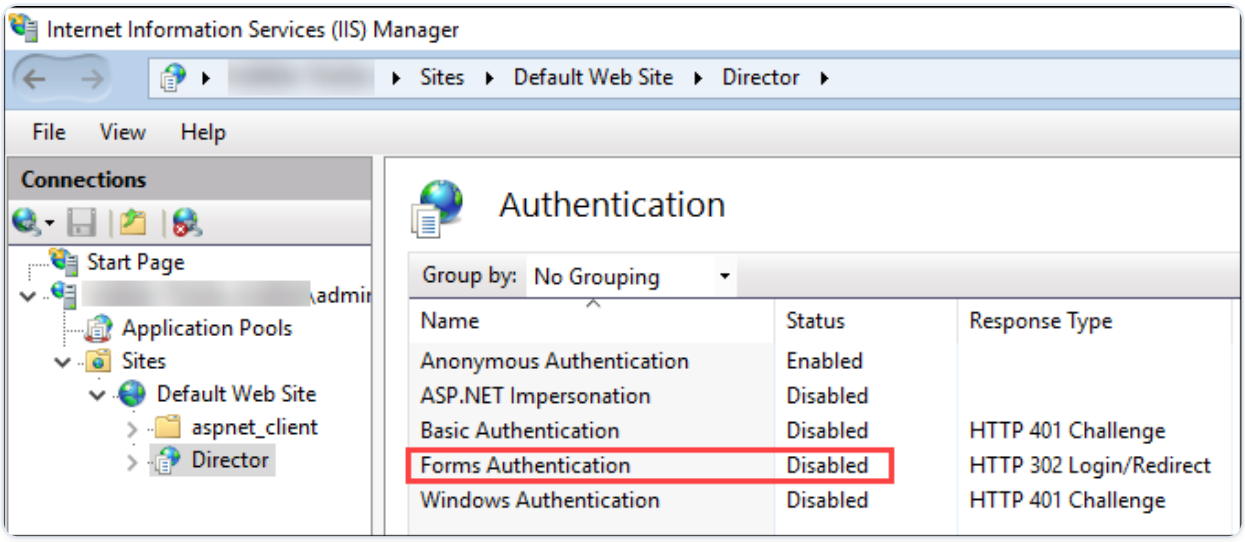
1. クライアント証明書マッピング認証をインストールして有効にします。Microsoftドキュメントのクライアント証明書マッピング認証にある**Active Directoryを使用したクライアント証明書マッピング認証**の手順に従います。
2. Directorサイトでフォーム認証を無効にします。

   IISマネージャーを起動します。

サイト \> **既定のWebサイト** \> **Director** に移動します。

認証 を選択します。

フォーム認証 を右クリックして、**無効** を選択します。



3. クライアント証明書認証のために、DirectorのURLをより安全なhttpsプロトコル (HTTPではなく) に構成します。

   a. IISマネージャーを起動します。

   b. **サイト** \> **既定のWebサイト** \> **Director** に移動します。

   c. 「**SSL Settings**」を選択します。

   d. 「**SSLを必須にする**」と「**クライアント証明書**」\>「**必須**」を選択します。

   SSL設定(/en-us/citrix-virtual-apps-desktops/current-release/media/dir-smartcard-config2.png)

4. web.config を更新します。テキストエディターを使用して、web.config ファイル（`c:\inetpub\wwwroot\Director` にあります）を開きます。

`<system.webServer>` 親要素の下に、次のスニペットを最初の子要素として追加します。

```
&lt;defaultDocument>

   &lt;files>

       &lt;add value="LogOn.aspx"/>

   &lt;/files>
```

```
&lt;/defaultDocument>
```

Active Directory の構成

デフォルトでは、Directorアプリケーションは**アプリケーションプール**のIDプロパティで実行されます。スマートカード認証には委任が必要であり、そのためにはDirectorアプリケーションのIDがサービスホスト上でTrusted Computing Base（TCB）権限を持っている必要があります。

Citrixでは、アプリケーションプールID用に個別のサービスアカウントを作成することをお勧めします。Microsoft MSDNの記事「Protocol Transition with Constrained Delegation Technical Supplement」の手順に従って、サービスアカウントを作成し、TCB権限を割り当ててください。

新しく作成したサービスアカウントを Director アプリケーションプールに割り当てます。次の図は、サンプルサービスアカウント「Domain Pool」のプロパティダイアログを示しています。

サンプルサービスアカウント(/en-us/citrix-virtual-apps-desktops/current-release/media/dir-smartcard-config3.png)

このアカウントに対して、次のサービスを構成します:

- デリバリーコントローラー™: ホスト、HTTP
- Director: ホスト、HTTP
- Active Directory のプロトコル: GC、LDAP

構成するには、,

1. 「ユーザーアカウントのプロパティ」ダイアログで、「**追加**」をクリックします。
2. 「**サービスの追加**」ダイアログで、「ユーザー」または「コンピューター」をクリックします。
3. Delivery Controllerのホスト名を選択します。
4. 「**利用可能なサービス**」リストから、HOSTとHTTPの「**サービスの種類**」を選択します。

サービスを構成する(/en-us/citrix-virtual-apps-desktops/current-release/media/dir-smartcard-config4.png)

同様に、**Director**および**Active Directory**ホストのサービスの種類を追加します。

サービスプリンシパル名レコードを作成する

各Directorサーバーと、Directorサーバーのプールへのアクセスに使用される負荷分散された仮想IP（VIP）ごとにサービスアカウントを作成する必要があります。新しく作成されたサービスアカウントへの委任を構成するには、サービスプリンシパル名（SPN）レコードを作成する必要があります。

- DirectorサーバーのSPNレコードを作成するには、次のコマンドを使用します。

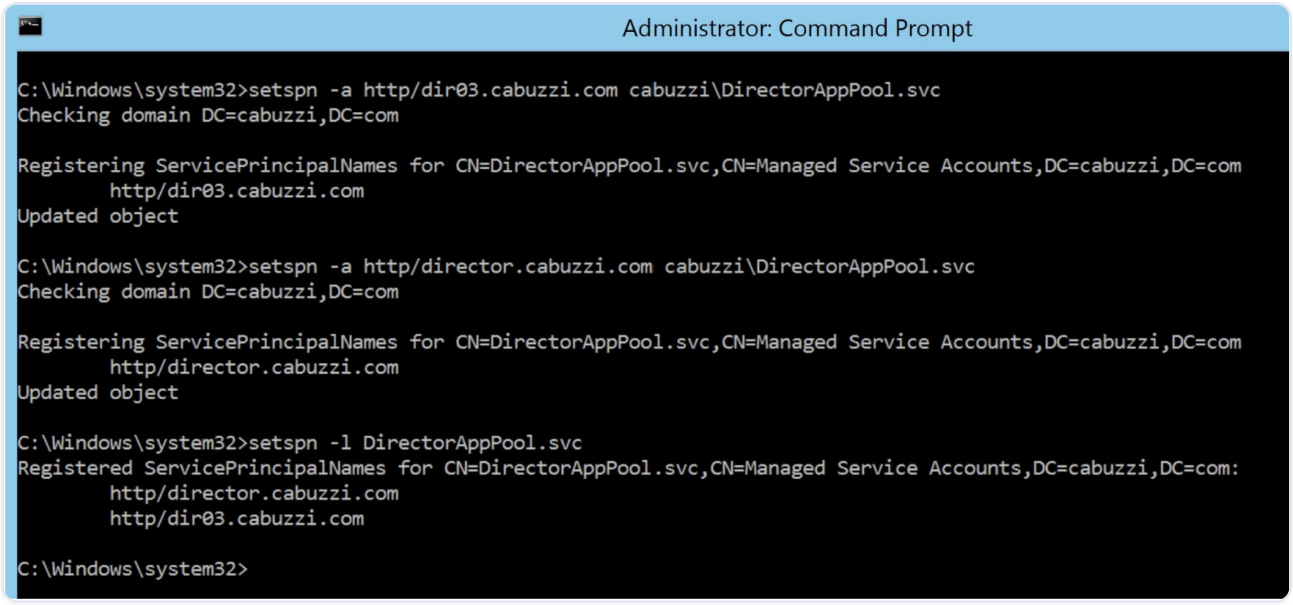
```
  setspn -a http/<directorServer>.<domain_fqdn>
<domain>\<DirectorAppPoolServiceAcct>
```

- 負荷分散されたVIPのSPNレコードを作成するには、次のコマンドを使用します。

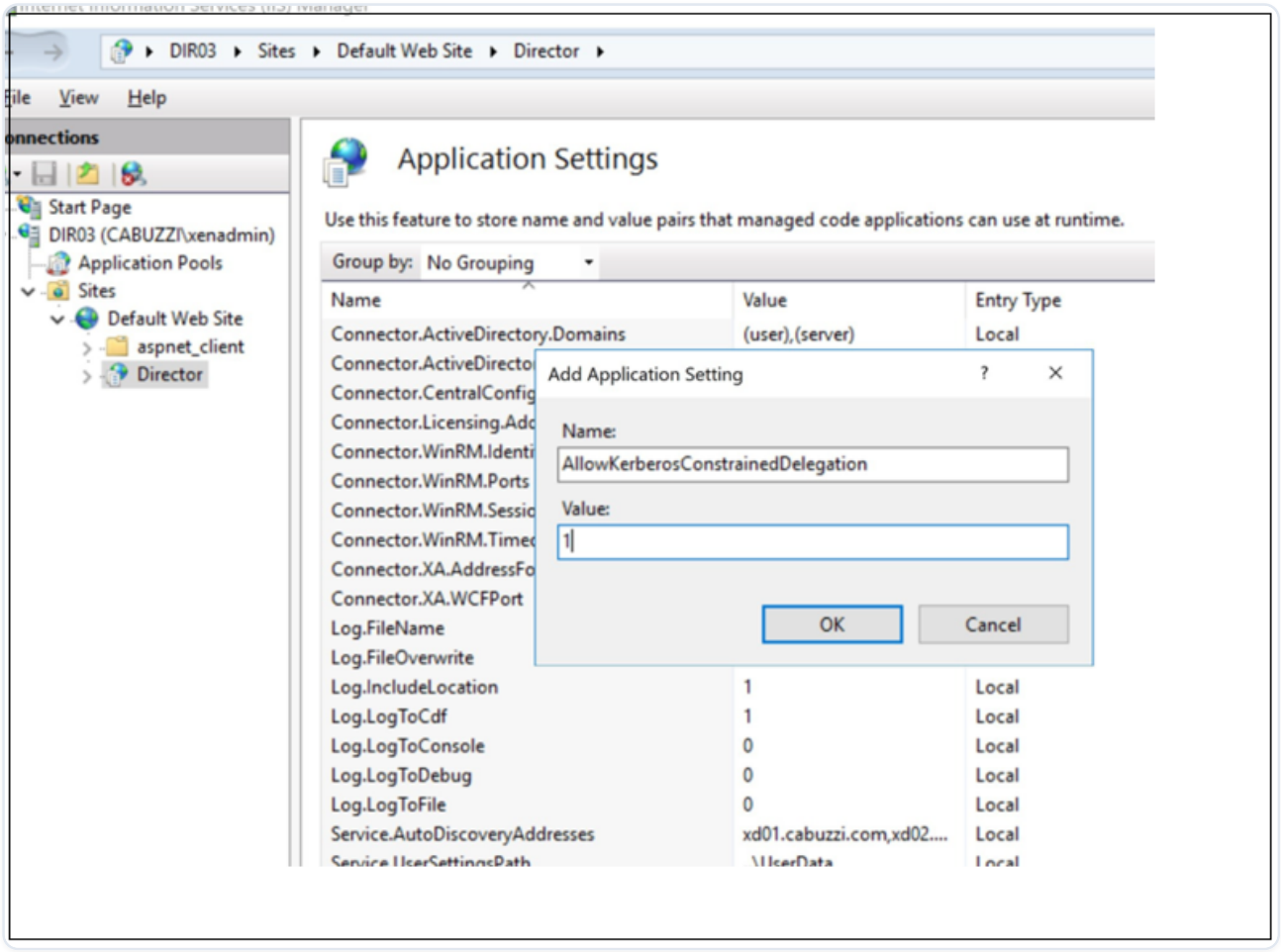
```
  setspn -S http/<DirectorFQDN> <domain>\<DirectorAppPoolServiceAcct>
```

- 作成されたSPNを表示またはテストするには、次のコマンドを使用します。

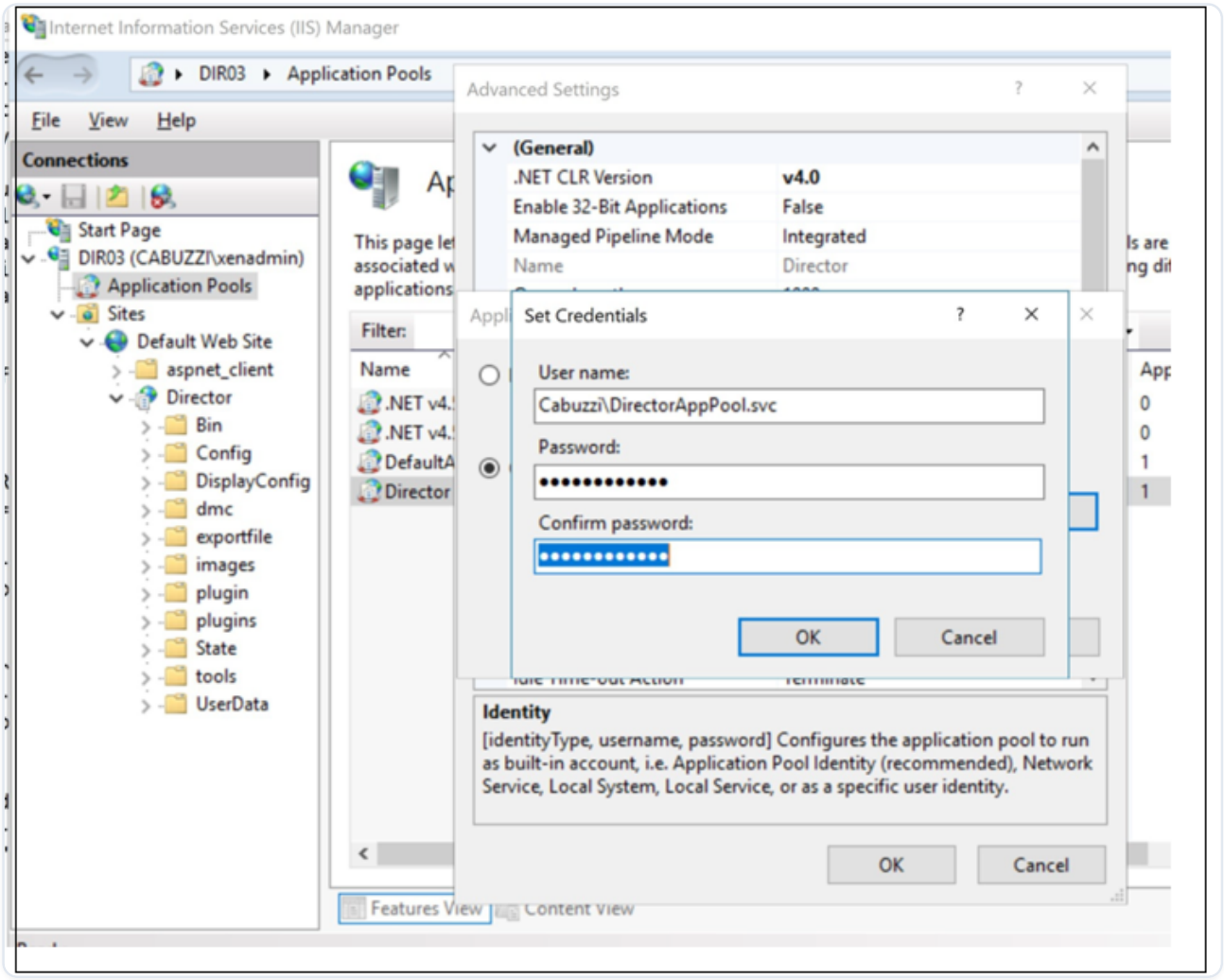
```
  setspn –l <DirectorAppPoolServiceAcct>
```



- 左ペインでDirector仮想ディレクトリを選択し、 をダブルクリックします。 ウィンドウで をクリックし、**AllowKerberosConstrainedDelegation** が1に設定されていることを確認します。



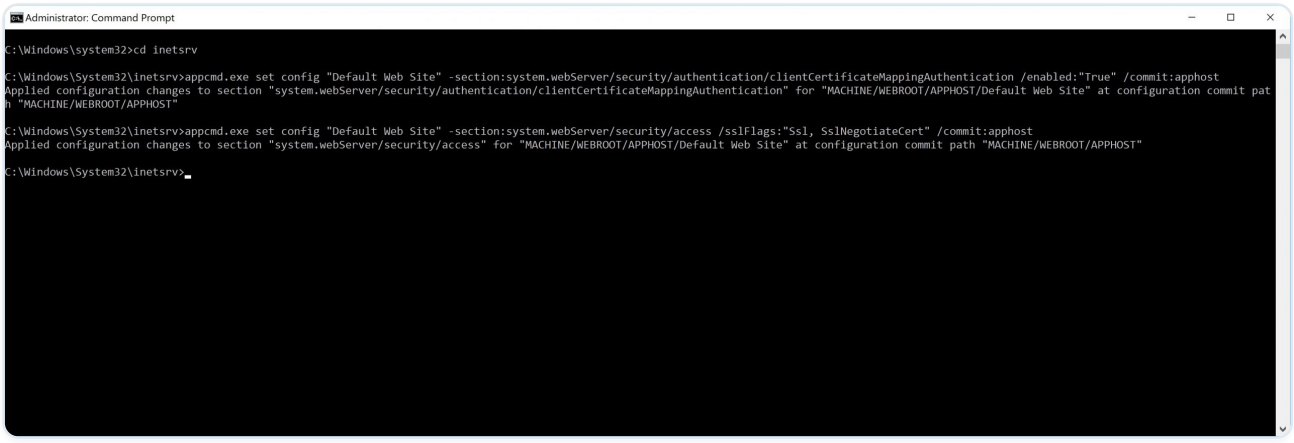
- 左側のペインで を選択し、Directorアプリケーションプールを右クリックして を選択します。
- 「**Identity**」を選択し、省略記号（「…」）をクリックしてサービスアカウントのドメイン\ログオンとパスワードの資格情報を入力します。IISコンソールを閉じます。



- 管理者として実行したコマンドプロンプトから、ディレクトリを C:\Windows\System32\inetsrv に変更し、次のコマンドを入力します。

```
   appcmd.exe set config “Default Web Site” -section:system.webServer/
security/authentication/clientCertificateMappingAuthentication /
enabled:”True” /commit:apphost
```

```
    appcmd.exe set config “Default Web Site” -section:system.webServer/
security/access /sslFlags:”Ssl, SslNegotiateCert” /commit:apphost
```



Firefoxブラウザーの構成

Firefoxブラウザーを使用するには、OpenSC 0.17.0で入手可能なPIVドライバーをインストールします。インストールと構成の手順については、Installing OpenSC PKCS#11 Module in Firefox, Step by Stepを参照してください。 Directorでのスマートカード認証機能の使用方法については、Directorの記事のUse Director with PIV based smart card authenticationセクションを参照してください。

ネットワーク分析の構成

> **注:**
>
> この機能の利用可否は、組織のライセンスと管理者権限によって異なります。

> DirectorはCitrix ADMと統合され、ネットワーク分析とパフォーマンス管理を提供します。

- ネットワーク分析は、Citrix ADMのHDX™ Insightレポートを使用して、ネットワークのアプリケーションおよびデスクトップのコンテキストビューを提供します。この機能により、Directorは展開環境におけるICAトラフィックの詳細な分析を提供します。
- パフォーマンス管理は、履歴保持と傾向レポートを提供します。リアルタイム評価ではなくデータの履歴保持により、キャパシティと健全性の傾向を含む傾向レポートを作成できます。

Directorでこの機能を有効にすると、HDX InsightレポートはDirectorに追加情報を提供します。

- ［傾向］ページの［ネットワーク］タブには、展開環境全体におけるアプリケーション、デスクトップ、およびユーザーの遅延と帯域幅の影響が表示されます。
- ［ユーザー詳細］ページには、特定のユーザーセッションに固有の遅延と帯域幅の情報が表示されます。

制限事項:

- ビューでは、バージョン7より前のVDAのHDX接続ログオンデータは収集されません。それ以前のVDAの場合、グラフデータは0として表示されます。

ネットワーク分析を有効にするには、DirectorにCitrix ADMをインストールして構成する必要があります。Directorには、Citrix ADMバージョン11.1ビルド49.16以降が必要です。MASはXenServer上で動作する仮想アプライアンスです。ネットワーク分析を使用すると、Directorは展開環境に関連する情報を通信および収集します。

詳しくは、Citrix ADMドキュメントを参照してください。

> **注:**
>
> Citrix NetScaler Insight Centerは、15 May 2018をもってメンテナンス終了日を迎えました。Citrix製品マトリックス を参照してください。ネットワーク分析のためにDirectorをCitrix ADMと統合してください。NetScaler Insight CenterをCitrix ADMに移行するには、「NetScaler Insight CenterからCitrix ADMへの移行」を参照してください。

1. Directorがインストールされているサーバーで、`C:\inetpub\wwwroot\Director\tools`にあるDirectorConfigコマンドラインツールを見つけ、コマンドプロンプトからパラメーター/confignetscalerを指定して実行します。
2. プロンプトが表示されたら、Citrix ADMマシン名（FQDNまたはIPアドレス）、ユーザー名、パスワード、HTTPS接続タイプ（HTTPよりも推奨）、およびCitrix ADM統合を選択します。
3. 変更を確認するには、ログオフして再度ログオンします。

> **注:**
>
> セキュリティ上の理由から、HDX Insightのみにアクセスするのに十分な権限を持つ、DirectorとのADM統合のためのカスタムロールを作成することをお勧めします。

> ADM Director統合のユーザーロール(/en-us/citrix-virtual-apps-desktops/current-release/media/dir-adm-user-role.png)

> 詳細については、アクセスポリシーの構成を参照してください。

委任管理とDirector

委任管理では、管理者、役割、スコープという3つの概念を使用します。権限は、管理者の役割と、その役割のスコープに基づいています。たとえば、管理者は、スコープが1つのサイトのエンドユーザーに対する責任を含むヘルプデスク管理者ロールを割り当てられる場合があります。

委任管理者の作成については、メインの委任管理の記事を参照してください。

管理権限によって、管理者に表示されるDirectorインターフェイスと、実行できるタスクが決まります。権限によって以下が決定されます。

- 管理者がアクセスできるビュー（総称してビューと呼ばれます）。
- 管理者が表示および操作できるデスクトップ、マシン、セッション。
- 管理者が実行できるコマンド（ユーザーセッションのシャドウイングやメンテナンスモードの有効化など）。

組み込みの役割と権限は、管理者がDirectorをどのように使用するかを決定します。

管理者ロール	DIRECTORでの権限
フル管理者	すべてのビューへのフルアクセス、およびすべてのコマンド（ユーザーセッションのシャドウイング、メンテナンスモードの有効化、トレンドデータのエクスポートなど）を実行できます。
デリバリーグループ管理者	すべてのビューへのフルアクセスが可能で、ユーザーセッションのシャドウイング、電源管理とセッション管理、メンテナンスモードの有効化、トレンドデータのエクスポートを含むすべてのコマンドを実行できます。
読み取り専用管理者	指定されたスコープ内のすべてのビューにアクセスし、すべてのオブジェクトとグローバル情報を表示できます。HDX™チャネルからレポートをダウンロードでき、トレンドビューの「エクスポート」オプションを使用してトレンドデータをエクスポートできます。その他のコマンドを実行したり、ビュー内の何かを変更したりすることはできません。
ヘルプデスク管理者	ヘルプデスクビューとユーザー詳細ビューのみにアクセスでき、管理者が管理を委任されて

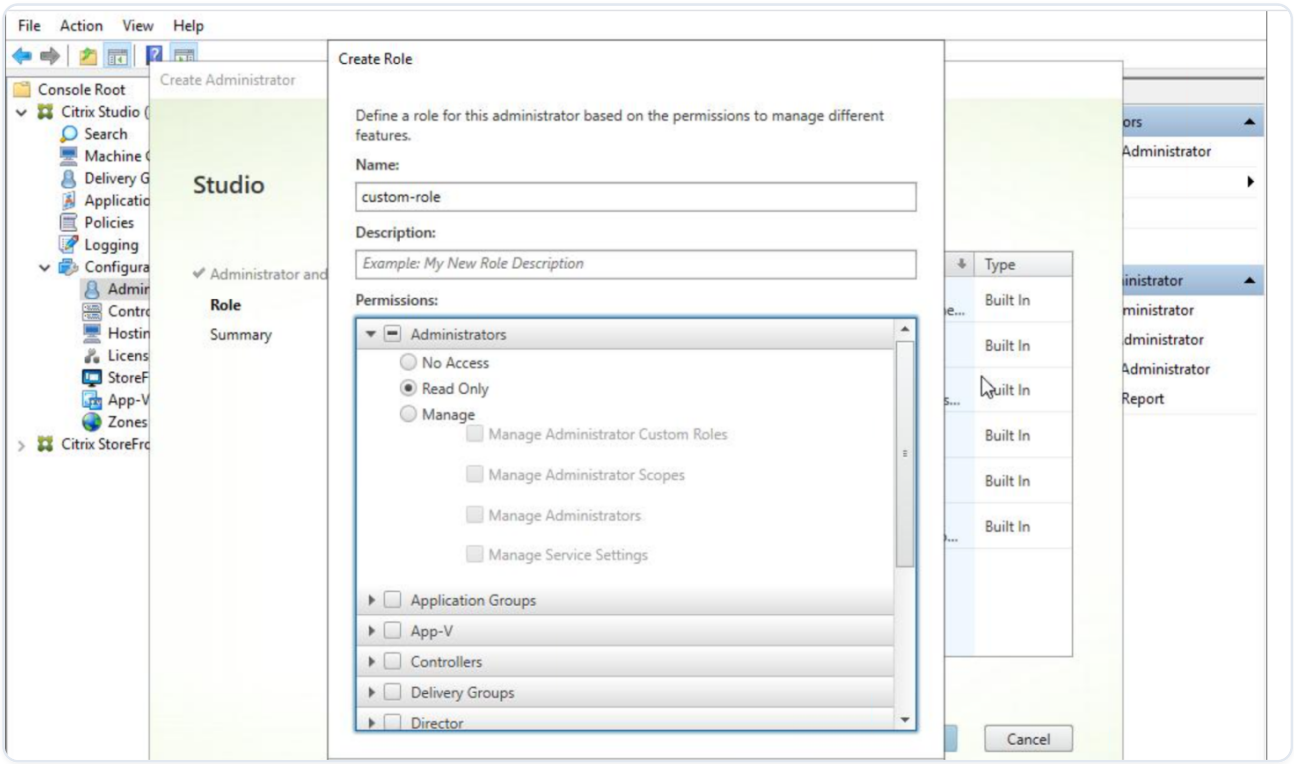
管理者ロール	DIRECTORでの権限
	いるオブジェクトのみを表示できます。ユーザーセッションのシャドウイングを行い、そのユーザーのコマンドを実行できます。メンテナンスモード操作を実行できます。シングルセッションOSマシンに対して電源制御オプションを使用できます。ダッシュボード、トレンド、アラート、またはフィルタービューにはアクセスできません。マルチセッションOSマシンに対して電源制御オプションを使用することはできません。
マシンカタログ管理者	マシン詳細ページ（マシンベース検索）のみにアクセスできます。
ホスト管理者	アクセスなし。この管理者はDirectorではサポートされておらず、データを表示できません。

Director管理者用のカスタム役割を構成する

Studioでは、組織の要件により厳密に一致させ、権限をより柔軟に委任するために、Director固有のカスタム役割を構成することもできます。たとえば、組み込みのヘルプデスク管理者役割を制限して、この管理者がセッションをログオフできないようにすることができます。

Director権限を持つカスタム役割を作成する場合、その役割に他の一般的な権限も付与する必要があります。

- Delivery Controller™ にログオンするための権限 - 管理者ノードで少なくとも読み取り専用アクセス
- Directorでそれらのデリバリーグループに関連するデータを表示するためのデリバリーグループへの権限 - 少なくとも読み取り専用アクセス

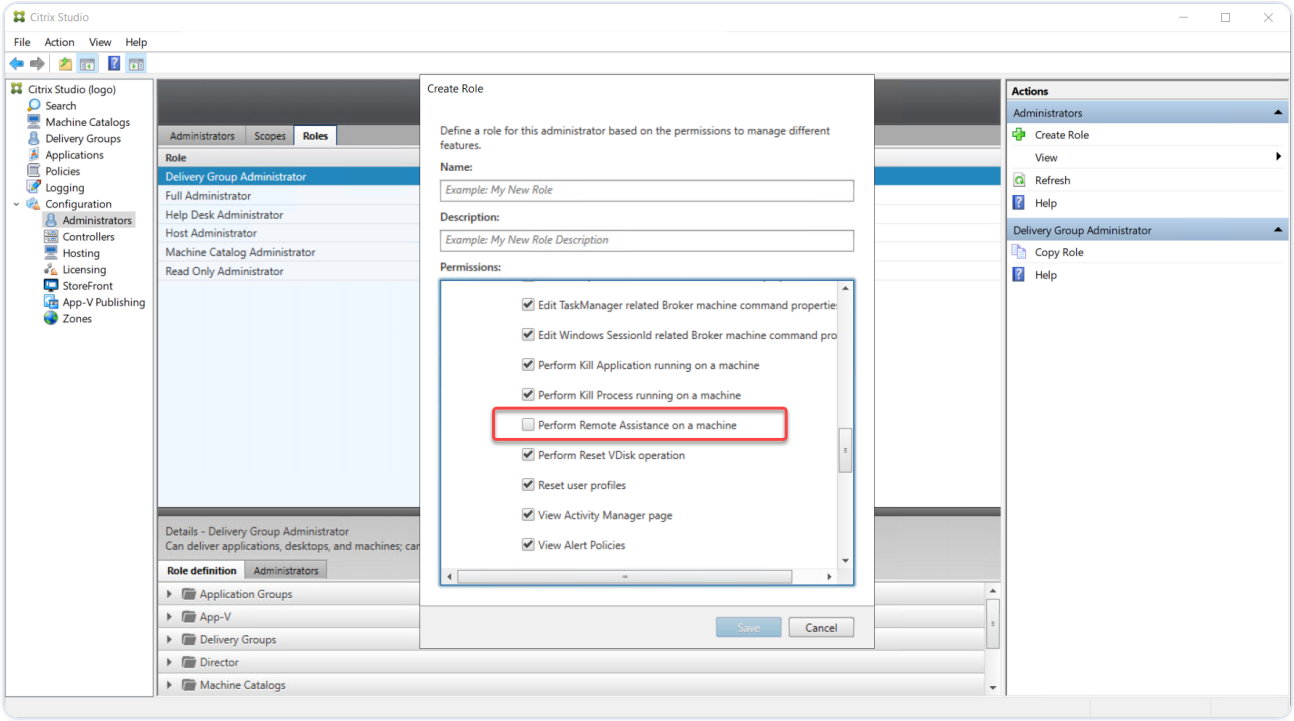


または、既存のロールをコピーして、さまざまなビューの追加の権限を含めることで、カスタムロールを作成できます。たとえば、ヘルプデスクロールをコピーして、ダッシュボードまたはフィルターページを表示する権限を含めることができます。

カスタムロールのDirector権限を選択します。これには以下が含まれます。

- マシン上で実行中のアプリケーションの強制終了を実行する
- マシン上で実行中のプロセスの強制終了を実行する
- マシン上でリモートアシスタンスを実行する
- ユーザープロファイルをリセットする
- クライアント詳細ページを表示
- ダッシュボードページの表示
- フィルターページを表示する
- マシン詳細ページを表示
- トレンドページの表示
- ユーザー詳細ページを表示

この例では、シャドウイング（マシン上でリモートアシスタンスを実行する）が無効になっています。



権限は、UIで適用可能になるために他の権限に依存する場合があります。たとえば、**マシン上で実行中のアプリケーションの強制終了を実行する**権限を選択すると、ロールに権限があるパネルでのみ**アプリケーションの終了**機能が有効になります。次のパネル権限を選択できます。

- フィルターページを表示する
- ユーザー詳細ページを表示
- マシン詳細ページを表示
- クライアント詳細ページを表示

さらに、他のコンポーネントの権限リストから、デリバリーグループの以下の権限を検討してください。

- デリバリーグループのメンバーシップを使用して、マシンのメンテナンスモードを有効/無効にする。
- デリバリーグループのメンバーシップを使用して、Windowsデスクトップマシンで電源操作を実行する。
- デリバリーグループのメンバーシップを使用して、マシンでセッション管理を実行する。

Directorの展開を保護する

この記事では、Directorの展開および構成時にシステムセキュリティに影響を与える可能性のある領域について説明します。

Directorの通信

実稼働環境では、Directorとサーバー間でやり取りされるデータを保護するためにHTTPSプロトコルを使用します。HTTPSは、Transport Layer Security（TLS）プロトコルを使用して強力なデータ暗号化を提供します。

> **注:**
>
> - Citrix®は、イントラネットネットワーク内でのDirectorコンソールへのアクセスを制限することを強くお勧めします。
> - Citrixは、実稼働環境でDirectorへの保護されていない接続を有効にしないことを強くお勧めします。
> - TLS 1.2以降を使用してください。レガシーTLSまたはSSLは使用しないでください。

> ユーザーのWebブラウザーとDirector間の通信を保護するには、「Web StudioおよびDirectorでTLSを有効にする」を参照してください。

DirectorとCitrix Virtual Apps and Desktopsサーバー間の通信（監視およびレポート用）を保護するには、「オンプレミスMonitor OData APIアクセスを保護する」を参照してください。

DirectorとCitrix ADC間の通信（Citrix Insight用）を保護するには、「ネットワーク分析を構成する」ときに、接続の種類としてHTTPSを選択します。

Microsoft インターネット インフォメーション サービス (IIS) の構成

制限されたIIS構成でDirectorを構成できます。

アプリケーションプールのリサイクル制限

Directorは、**Director**という名前のアプリケーションプールを使用します。アプリケーションプールで次のアプリケーションプールのリサイクル制限を設定できます。

- 仮想メモリ制限: 4,294,967,295
- プライベートメモリ制限: StoreFront™サーバーの物理メモリのサイズ
- 要求制限: 4,000,000,000

ファイル名拡張子

インストール中、Directorは次の拡張子のみを許可するように要求フィルタリングを構成します。

- .

- .aspx ファイル
- ．css
- ．eot
- .html ファイル
- ．ico
- .js
- ．png
- ．svc
- ．svg
- ．gif
- ドットジェイソン
- ドットウォフ
- ドットウォフ2
- ドットティーティーエフ

HTTP動詞

インストール中、Directorは以下の動詞のみを許可するようにリクエストフィルタリングを設定します。

- GET
- POST
- HEAD

IIS機能

Directorは以下のIISコンポーネントを必要としません。

- ISAPI拡張機能
- CGIプログラム
- FastCGIプログラム

これらのコンポーネントは削除できます。

.NET 信頼レベル

Director では、**.NET 信頼レベル**を**完全信頼**に設定する必要があります。.NET 信頼レベルを他の値に設定しないでください。

ユーザー権限の構成

Director のインストール時に、そのアプリケーションプールには次の権限が付与されます。

- **サービスとしてログオン**のログオン権限
- **プロセスに対するメモリクォータの調整**、**セキュリティ監査の生成**、および**プロセスレベルトークンの置き換え**の特権

言及されている権限と特権は、アプリケーションプールが作成される際の通常のインストール動作です。

これらのユーザー権限を変更する必要はありません。これらの特権は Director では使用されず、自動的に無効になります。

Director のセキュリティ分離

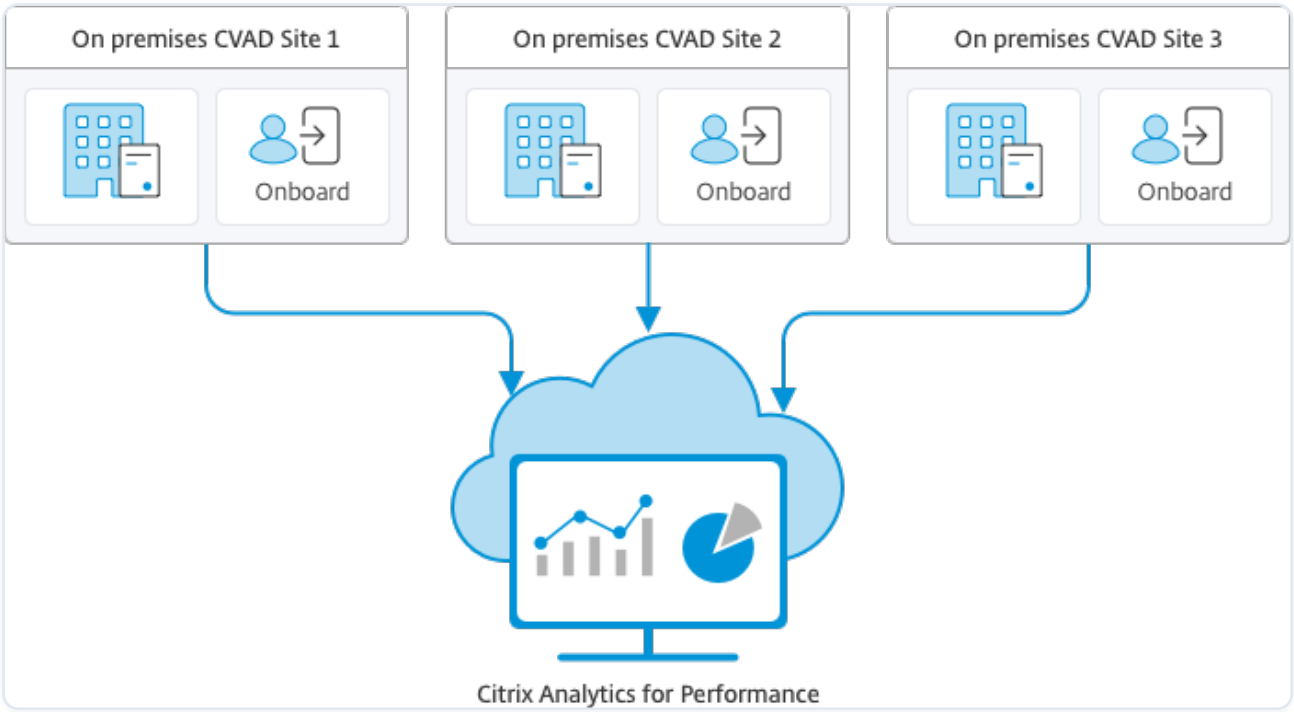
Director と同じ Web ドメイン（ドメイン名とポート）に任意の Web アプリケーションを展開できます。ただし、それらの Web アプリケーションのセキュリティリスクは、Director 展開のセキュリティを低下させる可能性があります。より高度なセキュリティ分離が必要な場合は、Citrix では Director を別の Web ドメインに展開することをお勧めします。

Citrix Analytics for Performance™ を使用したオンプレミスサイトの構成

Citrix Analytics for Performance (Performance Analytics) は、Citrix Analytics Cloud Serviceが提供する包括的なパフォーマンス監視ソリューションです。Performance Analyticsは、パフォーマンスメトリックに基づいて構築された高度なインサイトと分析を提供します。Performance Analytics は、組織内の1つ以上のCitrix Virtual Apps and Desktops™サイトの使用状況とパフォーマンスメトリックを監視および表示するのに役立ちます。

Performance Analyticsの詳細については、Performance Analyticsの記事を参照してください。

サイトからCitrix Cloud™上のCitrix Analytics for Performanceにパフォーマンスデータを送信して、その高度なパフォーマンス分析機能を活用できます。Performance Analyticsを表示および使用するには、まず**Director**の**Analytics**タブからCitrix Analytics for Performanceを使用してオンプレミスサイトを構成する必要があります。



Performance Analyticsは安全な方法でデータにアクセスし、Citrix Cloudからオンプレミス環境にデータが転送されることはありません。

前提条件

DirectorからCitrix Analytics for Performanceを構成するために、新しいコンポーネントをインストールする必要はありません。次の要件が満たされていることを確認してください。

- Delivery ControllerとDirectorがバージョン1912 CU2以降であること。詳細については、機能互換性マトリックスを参照してください。

注:

- Delivery ControllerがMicrosoft .NET Frameworkバージョン4.8より前のバージョンを実行している場合、DirectorからCitrix Analytics for Performanceを使用してオンプレミスサイトを構成すると、失敗する可能性があります。回避策として、Delivery ControllerのNET Frameworkをバージョン4.8にアップグレードしてください。LCM-9255。
- DirectorからCitrix Analytics for Performanceを使用してCitrix Virtual Apps and Desktopsバージョン2012を実行しているオンプレミスサイトを構成すると、構成が数時間後、またはDelivery ControllerでCitrix Monitor Serviceを再起動した後に失敗する可能性があります。この場合、Analyticsタブには「未接続」ステータスが表示されます。回避策として、Delivery Controllerのレジストリにencryptionフォルダーを作成します。場所: HKEY_LOCAL_MACHINE\Software\Citrix\XDservices\Monitor、フォルダー名:

> Encryption。CitrixMonitorアカウントがEncryptionフォルダーに対してフルコントロールアクセス権を持っていることを確認してください。Citrix Monitor Serviceを再起動します。DIR-14324。

- この構成を実行するための**Analytics**タブへのアクセスは、フル管理者のみが利用できます。
- Performance Analyticsがパフォーマンスメトリックにアクセスできるようにするには、すべてのDelivery ControllerとDirectorがインストールされているマシンで、アウトバウンドインターネットアクセスが利用可能である必要があります。具体的には、次のURLへのアクセス可能性を確認してください。
  - Citrixキー登録: `https://*.citrixnetworkapi.net/`
  - シトリックス クラウド: `https://*.citrixworkspacesapi.net/`
  - シトリックス アナリティクス: `https://*.cloud.com/`
  - Microsoft Azure: `https://*.windows.net/` Delivery ControllerとDirectorマシンがイントラネット内にあり、アウトバウンドインターネットアクセスがプロキシサーバー経由である場合、以下を確認してください。
- プロキシサーバーは、上記のURLリストを許可する必要があります。
- Director web.config および citrix.monitor.exe.config ファイルに次の構成を追加します。この構成は **configuration** タグ内に追加してください。

```
&lt;system.net>

    &lt;defaultProxy>

        &lt;proxy  usesystemdefault = "false"  proxyaddress = "http://
&lt;your_proxyserver_address>:80" bypassonlocal = "true"  />

    &lt;/defaultProxy>

&lt;/system.net>
```

  - Director web.config は、Director がインストールされているマシンの `C:\inetpub\wwwroot\Director\web.config` にあります。
  - citrix.monitor.exe.config は、Delivery Controller がインストールされているマシンの `C:\Program Files\Citrix\Monitor\Service\Citrix.Monitor.exe.Config` にあります。

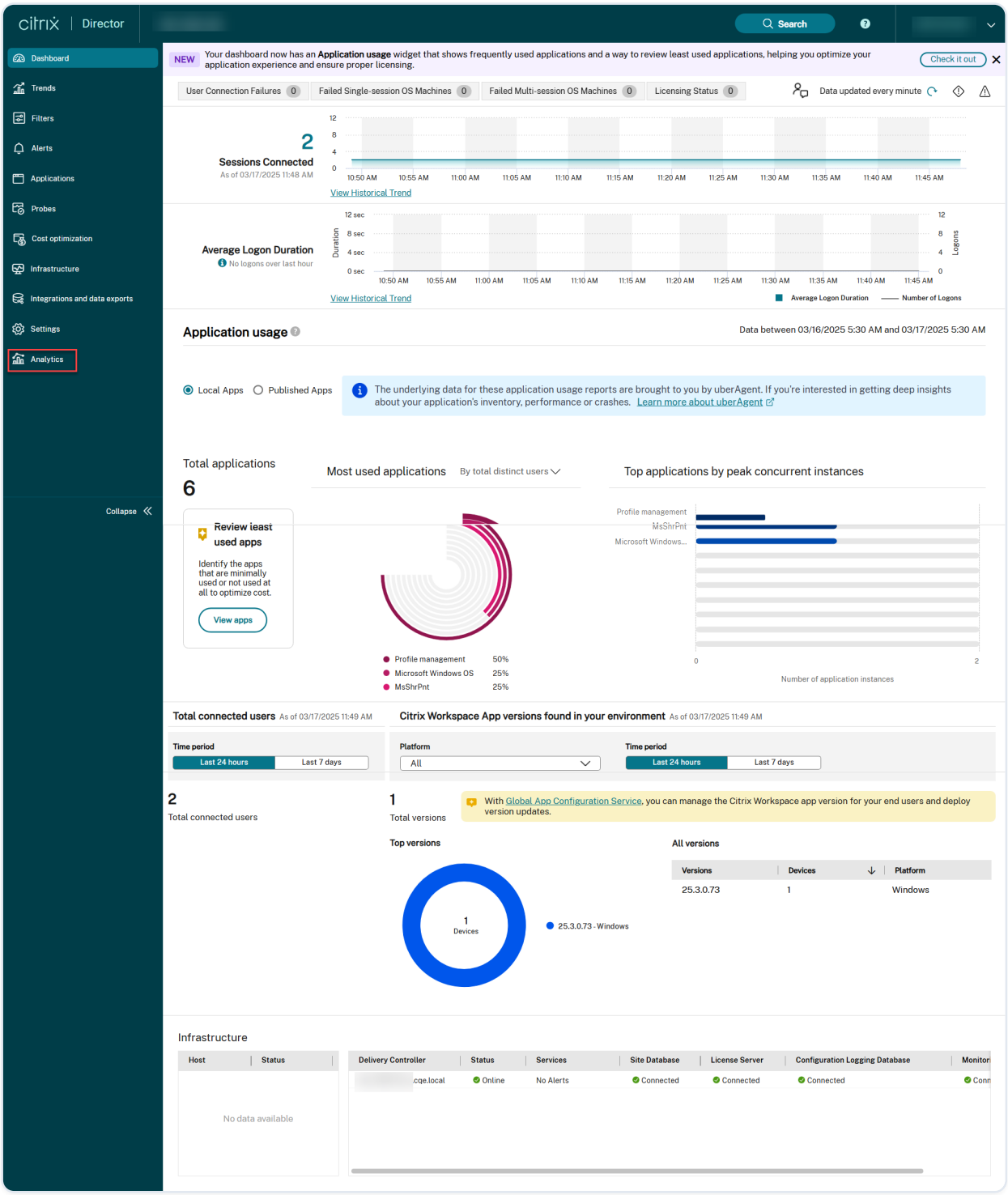
この設定は、IIS 上で Microsoft によって提供されます。詳細については、`https://docs.microsoft.com/ja-jp/dotnet/framework/network-programming/proxy-configuration` を参照してください。 構成ファイルの **defaultproxy** フィールドは、Director および Monitor Service のアウトバウンドアクセスを制御します。Performance Analytics との構成および通信には、**defaultproxy** フィールドを **true** に設定する必要があります。有効なポリシーによってこのフィールドが false に設定されている可能性があります。この場合、フィールドを手動で true に設定する必要があります。変更を行う前に構成ファイルのバックアップを取ってください。変更を有効にするには、Delivery Controller™ 上の監視サービスを再起動してください。

- Citrix Analytics for Performance の有効な Citrix Cloud エンタイトルメントをお持ちであること。
- Citrix Cloudアカウントは、製品登録エクスペリエンスに対する権限を持つ管理者アカウントである必要があります。管理者権限の詳細については、「管理者権限の変更」を参照してください。

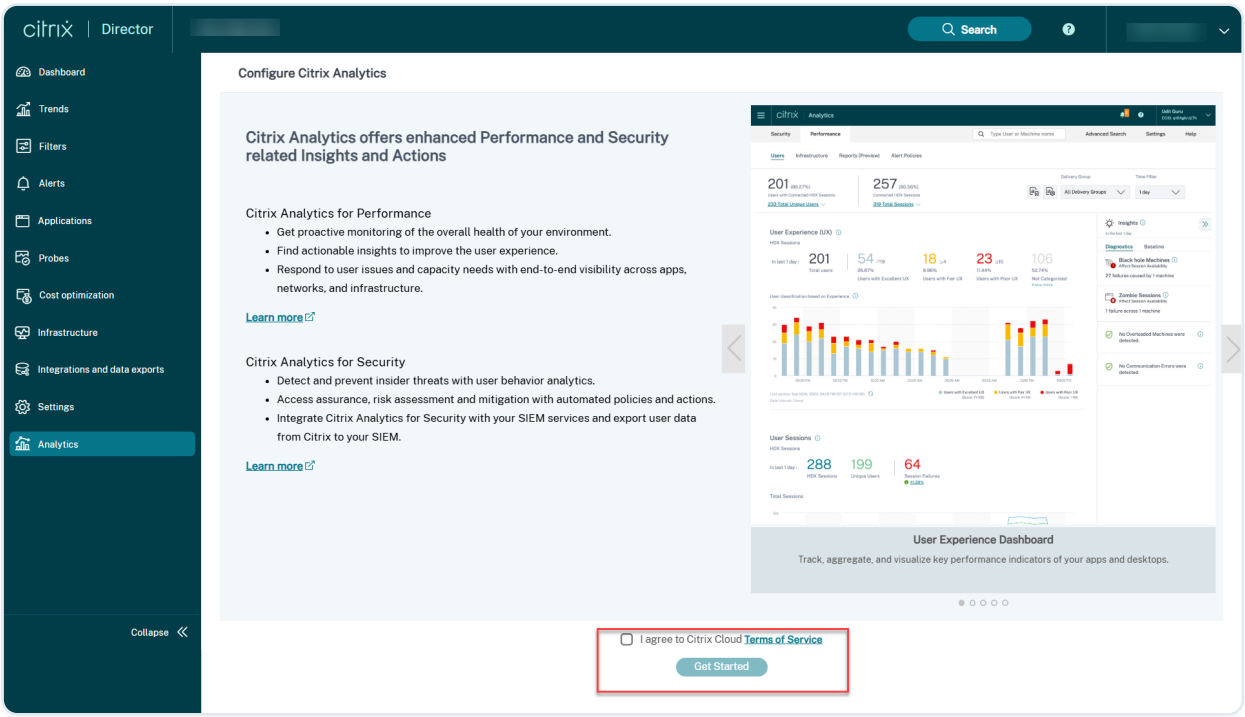
構成手順

前提条件を確認したら、次の手順を実行します。

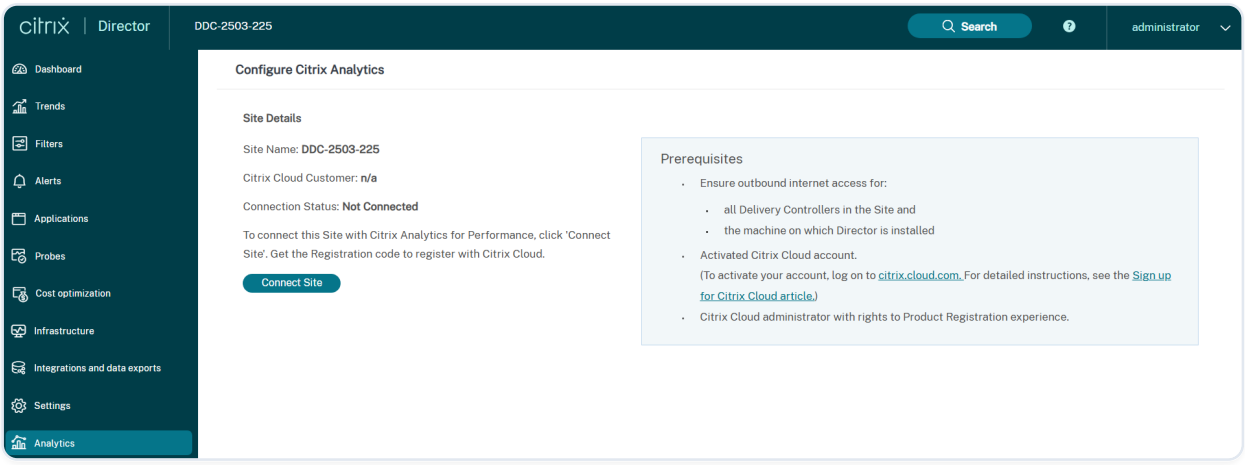
1. Director にフル管理者としてサインインし、Performance Analytics で構成するサイトを選択します。Director ダッシュボードページが表示されます。



2. **Analytics** タブをクリックします。**Citrix Analytics の構成**ページが表示されます。

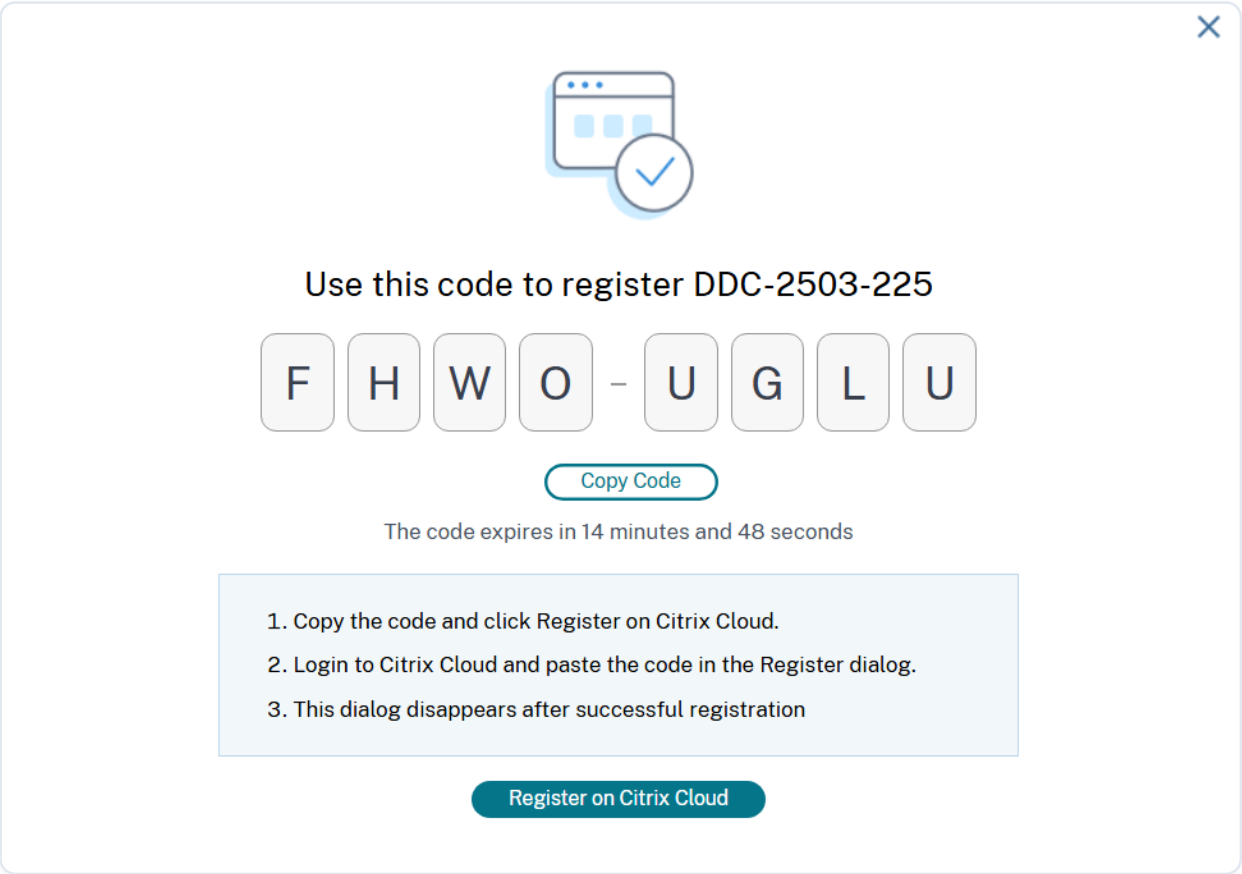


3. 手順を確認し、サービス利用規約を選択してから、**開始**をクリックします。**サイトの詳細**ページが表示されます。



4. 前提条件を確認し、満たされていることを確認します。サイトの詳細を確認します。
5. 構成プロセスを開始するには、**サイトの接続**をクリックします。

   このサイトを Citrix Cloud に登録するために使用する、一意の8桁の登録コードが生成されます。



6. **Copy Code** をクリックしてコードをコピーし、**Register on Citrix Cloud** をクリックします。Citrix Cloudの登録URLにリダイレクトされます。
7. Citrix Cloudの資格情報でサインインし、顧客を選択します。
8. Citrix Cloudの「製品登録」ページに、コピーした登録コードを貼り付けます。登録するには、**［続行］**をクリックします。登録の詳細を確認し、［登録］**をクリックします。

   Citrix Cloudでの登録(/en-us/citrix-virtual-apps-desktops/current-release/media/dir-onboarding6.png)

   オンプレミスサイトがCitrix Cloudに登録されます。
9. **Director**から、**［Analytics］タブの［Analyticsに移動］**をクリックします。

   Analyticsに移動(/en-us/citrix-virtual-apps-desktops/current-release/media/dir-onboarding7.png)

   Performance Analyticsがブラウザーの新しいタブで開きます。 Performance Analyticsダッシュボード(/en-us/citrix-virtual-apps-desktops/current-release/media/dir-onboarding-pa-dashboard.png)

   Citrix Cloudセッションの有効期限が切れている場合、Citrix.comまたはMy Citrixアカウントのログオンページにリダイレクトされることがあります。

10. 複数のサイトをPerformance Analyticsに登録するには、Directorから各サイトについて前述の構成手順を繰り返します。構成されているすべてのサイトのメトリックがPerformance Analyticsダッシュボードに表示されます。

    サイトごとに複数のDirectorインスタンスが実行されている場合は、いずれか1つのDirectorインスタンスから構成します。サイトに接続されている他のすべてのDirectorインスタンスは、構成プロセス後の次回の更新時に更新されます。

11. サイトをCitrix Cloudから切断するには、**［サイトの切断］**をクリックします。このオプションは、既存の構成を削除します。

> **注:**
>
> サイトを初めて構成するとき、サイトからのイベントの処理には時間がかかる場合があり（約1時間）、Performance Analyticsダッシュボードにメトリックが表示されるまでに遅延が生じます。その後、イベントは定期的に更新されます。
>
> 切断後、新しいアカウントからのイベントが送信されるまで、古いアカウントからのデータ送信はしばらく継続されます。データ送信が停止してから約1時間、古いアカウントに関連する分析はPerformance Analyticsダッシュボードに表示されたままになります。
>
> Citrix Analyticsサービスへのエンタイトルメントの有効期限が切れると、サイトメトリックがPerformance Analyticsに送信されなくなるまでに最大1日かかります。

LTSR展開用Directorの独立リリース

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

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

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

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

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

利点

- **新機能へのアクセス**: 2402 LTSR発表後にリリースされたDirector機能（Citrix Virtual Apps and Desktops™ 2407および2411累積リリース（CR）の機能を含む）にアクセスできます。
- **ターゲットを絞ったアップグレード**: LTSRインフラストラクチャの残りの部分に影響を与えることなく、Directorおよび監視サービスコンポーネントのみをアップグレードします。
- **LTSR互換性**: 最新のDirector機能強化の恩恵を受けながら、LTSR環境を維持します。
- **ロールバックオプション:** 必要に応じて、以前のDirectorバージョンにロールバックする柔軟性があります。

重要な考慮事項

アップグレードされたDirectorコンポーネントはLTSR互換ですが、LTSRコアコンポーネントのサポート対象ではありません。ただし、LTSRインフラストラクチャの残りの部分は、既存のサポートを維持します。

前提条件

1. Citrixダウンロードページから`Director2411.zip`ファイルをダウンロードします。
2. インストーラーファイルを解凍すると、次のインストーラーが見つかります。
    - DesktopDirector.msi
    - Monitor_PowerShellSnapIn.msi
    - Monitor_Service_x64.msi
3. Citrix Virtual Apps and Desktops™ 2402 LTSR または 2402 LTSR CU1 サイトを使用していることを確認してください。

概要

Citrix Virtual Apps and Desktops 2402 LTSR CU1サイトをCurrent Releaseの最新機能でアップグレードするには、次の手順に従います。

1. **データベースをバックアップする**: アップグレードする前に、監視データベースをバックアップしてください。アップグレードプロセスではデータベースも更新されるため、この手順は非常に重要です。
2. **サイトをアップグレードする**: 現在のリリースで新しい機能を取り込むために、サイトのアップグレードを進めます。
3. **ロールバックオプション**: アップグレードされたサイトの使用を継続しないと決定した場合、ロールバック手順を使用して以前のサイトに戻すことができます。

アップグレード手順

1. 監視データベースのバックアップを取ります。
2. Citrix downloads ページから `Director2411.zip` ファイルをダウンロードします。
3. インストーラーファイルを解凍すると、次のインストーラーが見つかります。
   - DesktopDirector.msi
   - Monitor_PowerShellSnapIn.msi
   - Monitor_Service_x64.msi
4. .msi ファイルの場所に移動します。
5. コマンドラインを使用してモニターサービスをインストールします。

```
msiexec /i Monitor_service_x64 REINSTALLMODE=amus /l*v <logfile path
and name>
```

6. 画面の指示に従ってウィザードを完了します。
7. コマンドラインを使用してDirectorサービスをインストールします。

```
msiexec /i DesktopDirector /l*v <logfile path and name>
```

8. 画面の指示に従ってウィザードを完了します。
9. コマンドラインを使用して次のコマンドを実行します。

```
DirectorConfig.exe /UPGRADE
```

10. コマンドラインを使用してモニター スナップインをインストールします。

```
msiexec /i Monitor_PowershellSnapin_x64.msi
```

11. すべての.msiインストールが完了したら、Program Files内のモニターサービスに移動し、コマンドを実行します。

```
Citrix.Monitor.exe /upgrade /enablefeatures
```

12. Citrix Site Managerを開き、**自動サイトアップグレード**オプションを選択して、アップグレードワークフローを完了します。
13. Directorにサインインして、新機能が利用可能であることを確認します。

ロールバック手順

1. Monitoring データベースのバックアップを必ず取得してください。
2. データベースロールバックスクリプト dbollback.zip をダウンロードして実行します。
3. コントロールパネルから以下をアンインストールします。
   - **Citrix Monitor Service PowerShell Snap-in- x64** を選択し、**アンインストール**をクリックします。
   - **Citrix Monitor Service - x64** を選択し、**アンインストール**をクリックします。
   - **Citrix Director** を選択し、**アンインストール**をクリックします。
4. すでに取得済みのバックアップから監視データベースを復元します。詳細については、ナレッジ共有記事 CTX135207 を参照してください。
5. Citrix Virtual Apps and Desktops インストーラーを使用して、Delivery Controller と Director を再インストールします。詳細については、「コアコンポーネントのインストール」を参照してください。

   または、,

次のコマンドを使用してコンポーネントを再インストールすることもできます。

```
XenDesktopServerSetup.exe /components controller,director /
configure_firewall /quiet
```

1. インストールが完了したら、**Open Citrix Site Manager** チェックボックスを選択します。
2. Citrix Site Manager で推奨されている場合は、サイトのアップグレードを実行します。

サポートとコンプライアンス

サポート

- Director の累積リリース (CR) バージョンは LTSR と互換性がありますが、LTSR に準拠していません。
- アップグレード後、必要なすべてのサポートチケットとバグ修正は、Director の次の累積リリース (CR) に追加されます。
- 変更または修正を含む CR は、次の累積更新プログラム (CU) で利用可能になります。

508/WCAG 2.1

- 508/WCAG 2.1 準拠の義務があるお客様には、すべてのコアコンポーネントの LTSR バージョンを継続して使用することをお勧めします。

サイト分析

Director を使用して、展開の健全性を監視できます。オンボードされたすべてのサイトでユーザー、エンドポイント、またはマシンを検索することで、パフォーマンスの問題をトラブルシューティングできます。

Director ダッシュボードの概要 1(/en-us/citrix-virtual-apps-desktops/current-release/media/dir-summary1.png)

完全な管理者権限があれば、Directorを開くと、ダッシュボードは、サイトの健全性と使用状況を監視するための一元的な場所を提供します。

Director ダッシュボードの概要 2(/en-us/citrix-virtual-apps-desktops/current-release/media/dir-summary2.png)

現在障害がなく、過去60分間に障害が発生していない場合、パネルは折りたたまれたままになります。障害が発生すると、特定の障害パネルが自動的に表示されます。

> **注:**
>
> 組織のライセンスと管理者権限によっては、一部のオプションまたは機能が利用できない場合があります。

Director ダッシュボードのパネル

ユーザー接続障害

過去60分間の接続障害。合計数の横にあるカテゴリをクリックすると、その種類の障害のメトリックが表示されます。隣接するテーブルでは、その数がデリバリーグループ別に分類されています。接続障害には、アプリケーション制限に達したことによる障害が含まれます。アプリケーション制限の詳細については、「アプリケーション」を参照してください。

Director ダッシュボードの概要 3(/en-us/citrix-virtual-apps-desktops/current-release/media/dir-summary3.png)

失敗したシングルセッションOSマシンまたは失敗したマルチセッションOSマシン

過去60分間の合計障害数（デリバリーグループ別）。障害は、起動失敗、起動中に停止、未登録などの種類別に分類されます。マルチセッションOSマシンでは、障害には最大負荷に達したマシンも含まれます。

ライセンスステータス

ライセンスサーバーアラートには、ライセンスサーバーから送信されたアラートと、アラートを解決するために必要なアクションが表示されます。ライセンスサーバーバージョン11.12.1以降が必要です。デリバリーコントローラーアラートには、コントローラーから見たライセンス状態の詳細が表示され、コントローラーによって送信されます。XenApp 7.6またはXenDesktop 7.6以降のコントローラーが必要です。Studioでアラートのしきい値を設定できます。**Delivery Controllers** > **Details** > **Product Editions** > **PLT** に表示されるライセンスステータスは、**Premium** を示し、**Platinum** ではありません。

猶予状態

Directorには、次のいずれかの猶予状態が表示されます。この情報はデリバリーコントローラーから取得されます。

1. **非アクティブ:** いずれの種類のライセンスキャッシュモードでもありません。通常のライセンス制限が適用されます。
2. **緊急猶予:** ライセンスサーバーに到達できない場合、または接続を仲介している間にライセンス情報を取得できない場合に有効になります。ユーザーには影響ありません。Directorに表示されるエラーは、ライセンスサーバーに到達可能になるまで閉じることができません。
3. **猶予期間の期限切れ:** 緊急ライセンスキャッシュモードの有効期限が切れました。

詳細については、ライセンスの超過 および ライセンスバーストモード を参照してください。

接続されたセッション

過去60分間のすべてのデリバリーグループにわたる接続セッション。

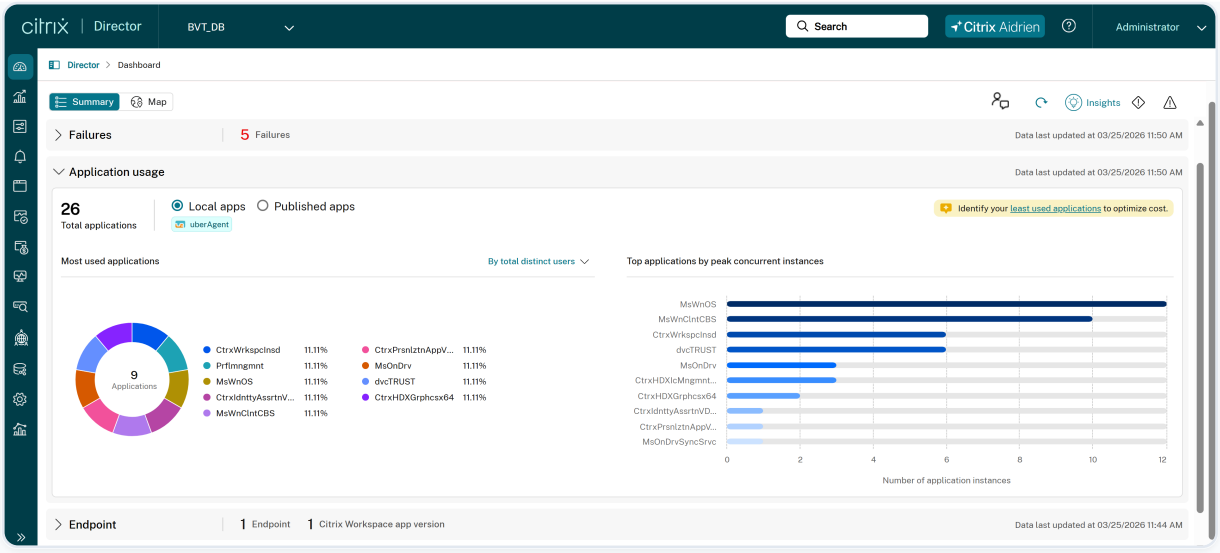
平均ログオン時間

過去60分間のログオンデータ。左側の大きな数字は、1時間あたりの平均ログオン時間です。XenDesktop 7.0より前のVDAのログオンデータは、この平均には含まれません。詳細については、ユーザーログオンの問題の診断 を参照してください。

インフラストラクチャ

サイトのインフラストラクチャ（ホストとコントローラー）を一覧表示します。XenServerまたはVMwareのインフラストラクチャの場合、パフォーマンスアラートを表示できます。たとえば、管理対象サーバーまたは仮想マシンでCPU、ネットワークI/O、またはディスクI/Oの使用率が指定されたしきい値を超えたときに、XenCenterがパフォーマンスアラートを生成するように構成できます。デフォルトでは、アラートの繰り返し間隔は60分ですが、これも構成できます。詳細については、XenServer製品ドキュメント のXenCenterパフォーマンスアラートのセクションを参照してください。

> **注:**
>
> 特定のメトリックにアイコンが表示されない場合、そのメトリックは使用しているホストの種類でサポートされていないことを示します。たとえば、System Center Virtual Machine Manager（SCVMM）ホスト、AWS、CloudStackでは、正常性情報は利用できません。



以下のオプションを使用して問題のトラブルシューティングを続行します（以下のセクションで説明されています）。

- ユーザーマシンの電源を制御する
- マシンへの接続を防止する

接続ユーザーの合計数

過去24時間または過去7日間に少なくとも1つの接続があったユーザーの数を表示します。このパネルは、管理者が導入傾向を役員に提示するのに役立ちます。

環境内で検出されたCitrix Workspace™アプリのバージョン

組織全体で使用されているCitrix Workspaceアプリのバージョン概要を提供します。これにより、異なるバージョンを使用しているデバイスの数を示すことで、バージョンを統一するのに役立ちます。デフォルトでは、すべてのOSプラットフォームのCitrix Workspaceアプリのバージョンデータが表示されます。特定のOSプラットフォームのバージョンデータは、**プラットフォームドロップダウン**リストから対応するOSを選択することで表示できます。

セッションの監視

セッションが切断されても、セッションはアクティブなままでアプリケーションは実行され続けますが、ユーザーデバイスはサーバーと通信しなくなります。

アクション	説明
ユーザーの現在接続されているマシンまたはセッションを表示する	アクティビティマネージャーとユーザー詳細ビューから、ユーザーが現在接続しているマシンまたはセッション、およびこのユーザーがアクセスできるすべてのマシンとセッションのリストを表示します。このリストにアクセスするには、ユーザータイトルバーのセッションスイッチャーアイコンをクリックします。詳細については、セッションの復元 を参照してください。
すべてのデリバリーグループにおける接続済みセッションの総数を表示する	ダッシュボードの**接続済みセッション**ペインで、過去60分間のすべてのデリバリーグループにおける接続済みセッションの合計数を表示します。次に、大きな合計数をクリックすると、フィルタービューが開き、選択したデリバリーグループと範囲、およびデリバリーグループ全体の使用状況に基づいてグラフィカルなセッションデータを表示できます。

アクション	説明
アイドルセッションを終了する	セッションフィルタービューには、すべてのアクティブなセッションに関連するデータが表示されます。関連ユーザー、デリバリーグループ、セッション状態、およびしきい値期間を超えるアイドル時間に基づいてセッションをフィルター処理します。フィルター処理されたリストから、ログオフまたは切断するセッションを選択します。詳細については、アプリケーションのトラブルシューティング を参照してください。
より長い期間のデータを表示する	トレンドビューで、**セッション**タブを選択すると、より長い期間（つまり、過去60分より前のセッション合計）の接続済みセッションと切断済みセッションに関するより具体的な使用状況データをドリルダウンして表示できます。この情報を表示するには、**履歴トレンドの表示**をクリックします。

注:

ユーザーデバイスがレガシーVirtual Delivery Agent（VDA）（バージョン7より前のVDAやLinux VDAなど）を実行している場合、Directorはセッションに関する完全な情報を表示できません。代わりに、情報が利用できないことを示すメッセージが表示されます。

デスクトップ割り当て規則の制限: Web Studioでは、異なるユーザーまたはユーザーグループに対して複数のデスクトップ割り当て規則（DAR）をデリバリーグループ内の単一のVDAに割り当てることができます。StoreFront™は、ログインユーザーのDARに従って、対応する**表示名**で割り当てられたデスクトップを表示します。ただし、DirectorはDARをサポートしておらず、ログインユーザーに関係なく、デリバリーグループ名を使用して割り当てられたデスクトップを表示します。その結果、Directorで特定のデスクトップをマシンにマッピングすることはできません。 StoreFrontに表示される割り当てられたデスクトップを、Directorに表示されるデリバリーグループ名にマッピングするには、次のPowerShellコマンドを使用します。

```
Get-BrokerDesktopGroup | Where-Object { $\_.Uid -eq (Get-
BrokerAssignmentPolicyRule | Where-Object { $\_.PublishedName -eq
"\&lt;Name on StoreFront\>" }).DesktopGroupUid } | Select-Object -Property
Name, Uid
```

セッション転送プロトコル

セッションの詳細パネルで、現在のセッションのHDX接続タイプで使用されている転送プロトコルを表示します。この情報は、VDAバージョン7.13以降で起動されたセッションで利用できます。

- **HDX™** 接続タイプの場合、,
  - HDX接続にEDTが使用されている場合、プロトコルは **UDP** と表示されます。
  - HDX接続にTCPが使用されている場合、プロトコルは **TCP** と表示されます。
- **RDP**接続タイプの場合、プロトコルは**n/a**と表示されます。

アダプティブトランスポートが構成されている場合、セッション転送プロトコルは、ネットワークの状態に基づいてEDT（UDP経由）とTCPの間で動的に切り替わります。EDTを使用してHDXセッションを確立できない場合、TCPプロトコルにフォールバックします。

アダプティブトランスポートの構成の詳細については、「アダプティブトランスポート」を参照してください。

レポートのエクスポート

定期的な使用状況および容量管理レポートを生成するために、トレンドデータをエクスポートできます。エクスポートは、PDF、Excel、CSVのレポート形式をサポートしています。PDFおよびExcel形式のレポートには、グラフと表で表されたトレンドが含まれます。CSV形式のレポートには、ビューを生成するために処理できる、またはアーカイブできる表形式のデータが含まれます。

レポートをエクスポートするには：

1. **トレンド**タブに移動します。
2. フィルター条件と期間を設定し、**適用**をクリックします。傾向グラフと表にデータが入力されます。
3. **エクスポート**をクリックし、レポートの名前と形式を入力します。

Directorは、選択したフィルター条件に基づいてレポートを生成します。フィルター条件を変更した場合は、**エクスポート**をクリックする前に**適用**をクリックしてください。

注:

大量のデータをエクスポートすると、Directorサーバー、Delivery Controller、およびSQL サーバーのメモリとCPUの使用量が大幅に増加します。最適なエクスポートパフォーマンスを実現するために、サポートされる同時エクスポート操作の数とエクスポートできるデータ量は、デフォルトの制限に設定されています。

サポートされるエクスポート制限

エクスポートされたPDFおよびExcelレポートには、選択されたフィルター条件に対する完全なグラフが含まれます。ただし、すべてのレポート形式の表形式データは、テーブル内の行数またはレコード数のデフォルト制限を超えると切り捨てられます。サポートされるデフォルトのレコード数は、レポート形式に基づいて定義されます。

Internet Information Services (IIS) のDirectorアプリケーション設定を構成することで、デフォルトの制限を変更できます。

レポート形式	サポートされるレコードのデフォルト数	DIRECTORアプリケーション設定のフィールド	サポートされるレコードの最大数
PDF	500	UI.ExportPdfDrilldownLimit	5000
エクセル	100,000	UI.ExportExcelDrilldownLimit	100,000
CSV	100,000 (「**セッション**」タブでは 10,000,000)	UI.ExportCsvDrilldownLimit	100,000

エクスポートできるレコード数の制限を変更するには：

1. IISマネージャーコンソールを開きます。
2. デフォルトのWebサイトの下にあるDirector Webサイトに移動します。
3. 「**アプリケーション設定**」をダブルクリックします。
4. 必要に応じて、UI.ExportPdfDrilldownLimit、UI.ExportExcelDrilldownLimit、または UI.ExportCsvDrilldownLimitフィールドの設定を編集または追加します。

アプリケーション設定でこれらのフィールド値を追加すると、デフォルト値が上書きされます。

警告:

サポートされている最大レコード数を超えるフィールド値を設定すると、エクスポートのパフォーマンスに影響を与える可能性があり、サポートされていません。

エラー処理

このセクションでは、エクスポート操作中に発生する可能性のあるエラーの対処方法について説明します。

- **Directorがタイムアウトしました**

このエラーは、ネットワークの問題、DirectorサーバーまたはMonitor Serviceでの高いリソース使用率が原因で発生する可能性があります。

デフォルトのタイムアウト期間は100秒です。Director Serviceのタイムアウト期間を長くするには、Internet Information Services (IIS) のDirectorアプリケーション設定で、**Connector.DataServiceContext.Timeoutフィールド**の値を設定します。

1. IISマネージャーコンソールを開きます。
2. デフォルトのWebサイトの下にあるDirector Webサイトに移動します。
3. **アプリケーション設定**をダブルクリックします。
4. **Connector.DataServiceContext.Timeout**の値を編集します。

- **Monitorがタイムアウトしました**

このエラーは、ネットワークの問題、Monitor ServiceまたはSQLサーバーでの高いリソース使用率が原因で発生する可能性があります。

Monitor Serviceのタイムアウト期間を長くするには、Delivery Controllerで次のPowerShellコマンドを実行します。

```
asnp Citrix.*

Get-MonitorConfiguration

Set-MonitorConfiguration -MonitorQueryTimeoutSeconds &lt;timeout value>
```

- **同時実行中のエクスポートまたはプレビュー操作の最大数**

Directorは、エクスポートまたはプレビューのインスタンスを1つサポートしています。「**同時実行中のエクスポートまたはプレビュー操作の最大数**」エラーが発生した場合は、次のエクスポート操作を後でもう一度試してください。

同時実行できるエクスポートまたはプレビュー操作の数を増やすことは可能ですが、Directorのパフォーマンスに影響を与える可能性があり、サポートされていません。

1. IISマネージャーコンソールを開きます。
2. デフォルトのWebサイトの下にあるDirector Webサイトに移動します。
3. **アプリケーション設定**をダブルクリックします。
4. 値**UI.ConcurrentExportLimit**を編集します。

- **Directorのディスク容量不足**

各エクスポート操作には、Windows Tempフォルダーに最大2 GBのハードディスク容量が必要です。空き容量を確保するか、Directorサーバーにハードディスク容量を追加してから、エクスポートを再試行してください。

Monitorのホットフィックス

特定のVDAマシン（物理またはVM）にインストールされているホットフィックスを表示するには、「**マシンの詳細**」ビューを選択します。

ユーザーマシンの電源状態を制御する

Directorで選択したマシンの状態を制御するには、電源制御オプションを使用します。これらのオプションは、シングルセッションOSマシンで利用できますが、マルチセッションOSマシンでは利用できない場合があります。

> **注:**
>
> この機能は、物理マシンまたはリモートPCアクセスを使用するマシンでは利用できません。

コマンド	機能
再起動	VMの順序だった（ソフト）シャットダウンを実行し、VMを再起動する前に実行中のすべてのプロセスを個別に停止します。たと

コマンド	機能
	えば、Directorで「起動に失敗しました」と表示されるマシンを選択し、このコマンドを使用して再起動します。
強制再起動	シャットダウン手順を最初に実行せずにVMを再起動します。このコマンドは、物理サーバーのプラグを抜き、再度差し込んで電源を入れ直すのと同じように機能します。
シャットダウン	VMの正常な（ソフト）シャットダウンを実行します。すべての実行中のプロセスは個別に停止されます。
強制シャットダウン	シャットダウン手順を最初に実行せずにVMをシャットダウンします。このコマンドは、物理サーバーのプラグを抜くのと同じように機能します。常にすべての実行中のプロセスをシャットダウンするとは限らず、この方法でVMをシャットダウンするとデータが失われるリスクがあります。
一時停止	実行中のVMを現在の状態で一時停止し、その状態をデフォルトのストレージリポジトリ上のファイルに保存します。このオプションを使用すると、VMのホストサーバーをシャットダウンし、後で再起動した後、VMを再開して元の実行状態に戻すことができます。
再開	一時停止されたVMを再開し、元の実行状態に戻します。
開始	VMがオフのときに起動します（コールドスタートとも呼ばれます）。

電源制御アクションが失敗した場合、アラートにマウスを重ねると、失敗の詳細を示すポップアップメッセージが表示されます。

マシンへの接続を防止する

適切な管理者がイメージのメンテナンス作業を実行している間、メンテナンスモードを使用して新しい接続を一時的に防止します。

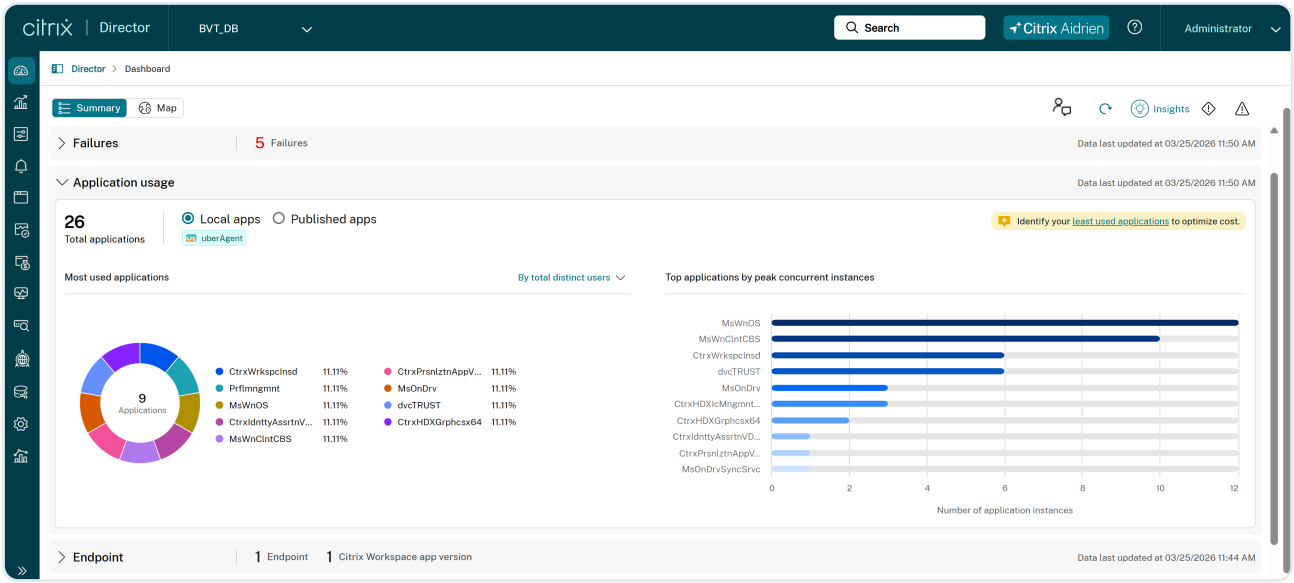
マシンでメンテナンスモードを有効にすると、無効にするまで新しい接続は許可されません。ユーザーが現在ログオンしている場合、すべてのユーザーがログオフするとすぐにメンテナンスモードが有効になります。ログオフしないユーザーには、マシンが特定の時間にシャットダウンされることを通知するメッセージを送信し、電源制御を使用してマシンを強制的にシャットダウンします。

1. ユーザー詳細ビューから、またはフィルタービューでマシンのグループから、マシンを選択します。
2. **メンテナンスモード**を選択し、オプションをオンにします。

ユーザーが割り当てられたデスクトップにメンテナンスモード中に接続しようとすると、デスクトップが利用できないことを示すメッセージが表示されます。メンテナンスモードを無効にするまで、新しい接続はできません。

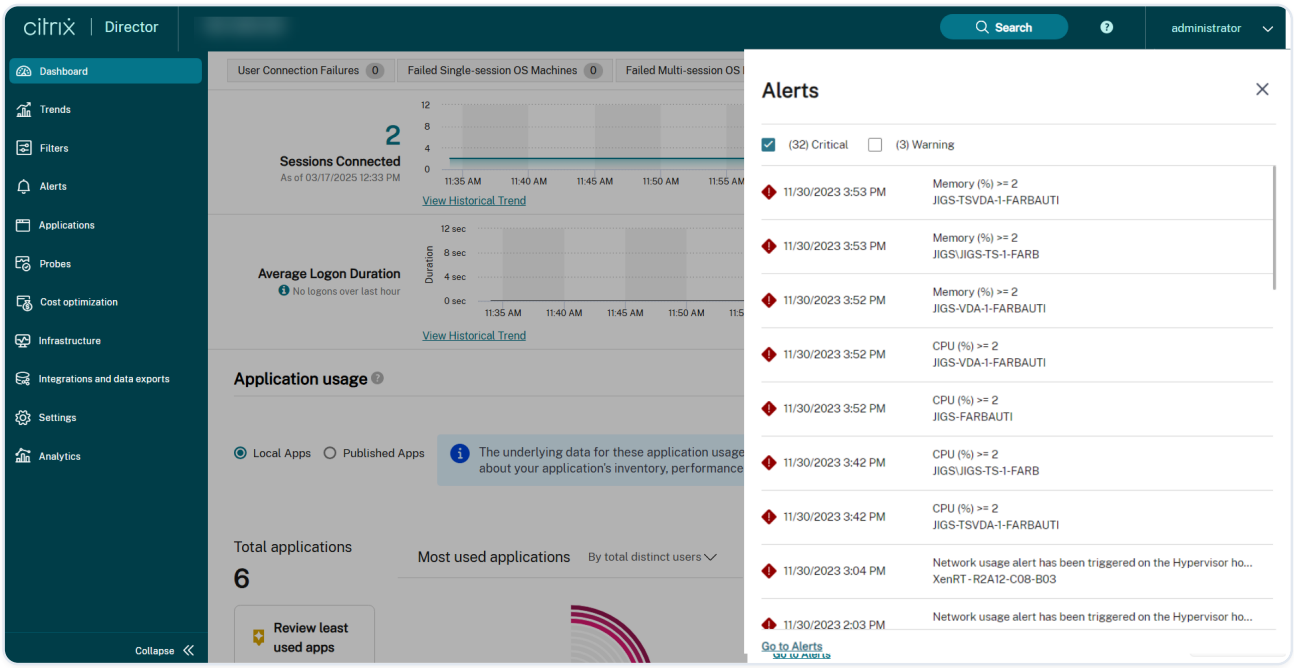
アプリケーション分析

アプリケーションタブには、アプリケーションベースの分析が単一の統合ビューで表示され、アプリケーションのパフォーマンスを効率的に分析および管理するのに役立ちます。サイトで公開されているすべてのアプリケーションの健全性と使用状況に関する貴重な洞察を得ることができます。プローブ結果、アプリケーションごとのインスタンス数、公開されているアプリケーションに関連する障害やエラーなどのメトリックが表示されます。詳細については、**アプリケーションのトラブルシューティング**のアプリケーション分析セクションを参照してください。



アラートと通知

アラートは、Directorのダッシュボードやその他の高レベルビューに、警告および重大なアラートシンボルとともに表示されます。アラートは、**Premium**ライセンスサイトで利用できます。アラートは1分ごとに自動的に更新されます。オンデマンドでアラートを更新することもできます。

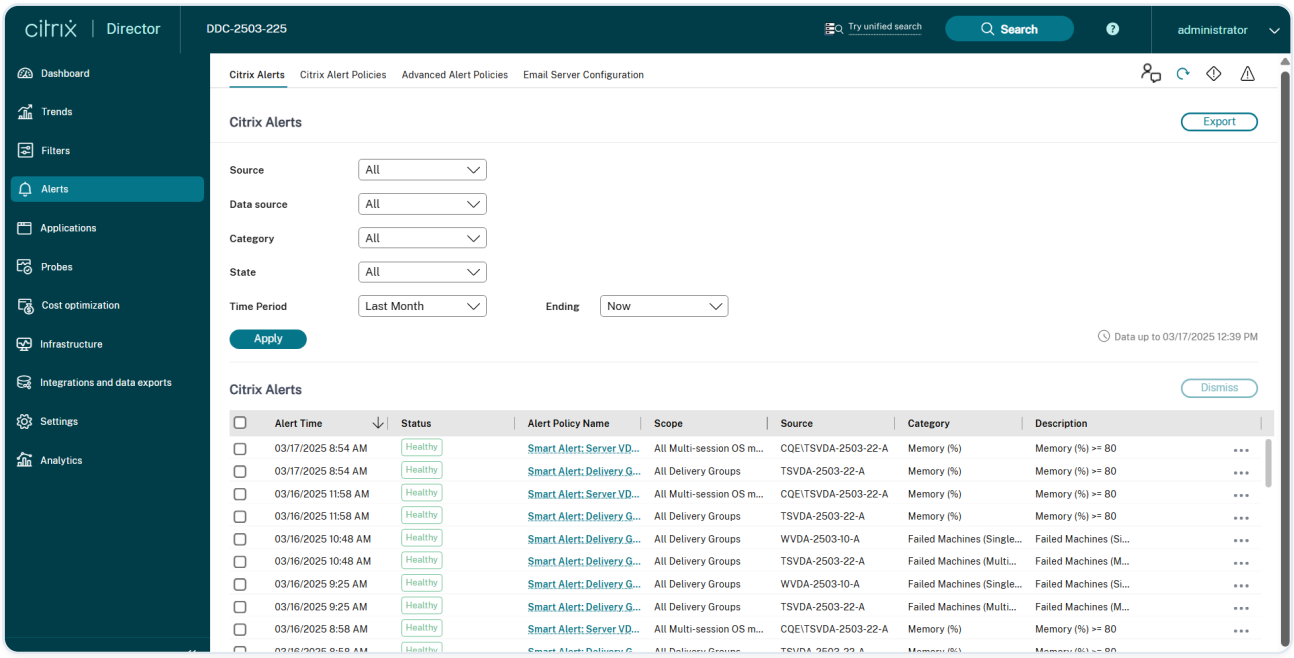


警告アラート（琥珀色の三角形）は、条件の警告しきい値に達したか、それを超えたことを示します。

重大なアラート（赤い円）は、条件の重大なしきい値に達したか、それを超えたことを示します。

アラートの詳細情報を表示するには、サイドバーからアラートを選択するか、サイドバーの下部にある**Go to Alerts**リンクをクリックするか、Directorページの上部から**Alerts**を選択します。

アラートビューでは、アラートをフィルター処理してエクスポートできます。たとえば、特定のデリバリーグループの過去1か月間の失敗したマルチセッションOSマシン、または特定のユーザーのすべてのアラートなどです。詳細については、「レポートのエクスポート」を参照してください。



Citrix®アラート

Citrixアラートは、Citrixコンポーネントから発生し、Directorで監視されるアラートです。Citrixアラートは、Directorの**Alerts** \> **Citrix Alerts Policy**で構成できます。構成の一部として、アラートが設定したしきい値を超えたときに、個人やグループにメールで通知を送信するように設定できます。Citrixアラートの設定の詳細については、「アラートポリシーの作成」を参照してください。

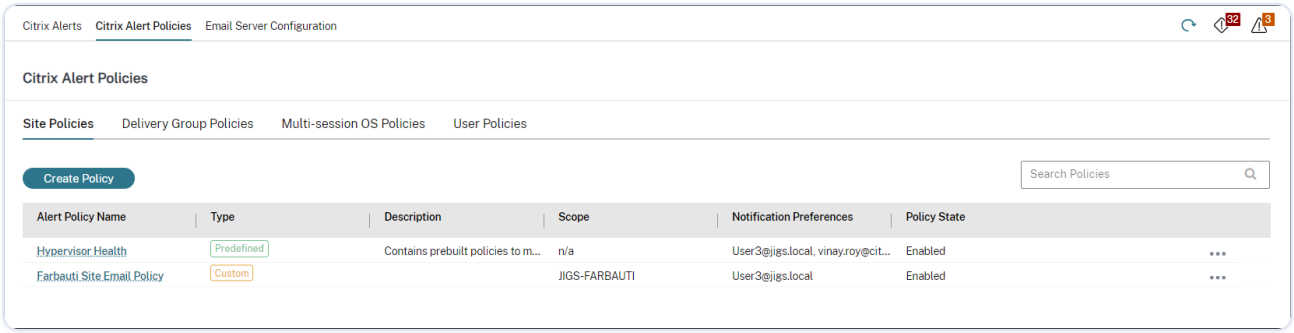
> **注:**
>
> ファイアウォール、プロキシ、またはMicrosoft Exchange Serverがメールアラートをブロックしないようにしてください。

スマートアラートポリシー

事前定義されたしきい値を持つ一連の組み込みアラートポリシーは、デリバリーグループおよびマルチセッションOS VDAスコープで利用できます。この機能には、Delivery Controllerバージョン7.18以降が必要です。組み込みアラートポリシーのしきい値パラメーターは、**Alerts** \> **Citrix Alerts Policy**で変更できます。 これらのポリシーは、サイトに少なくとも1つのアラートターゲット（デリバリーグループまたはマルチセッションOS VDA）が定義されている場合に作成されます。さらに、これらの組み込みアラートは、新しいデリバリーグループまたはマルチセッションOS VDAに自動的に追加されます。

Directorとサイトをアップグレードする場合、以前のDirectorインスタンスのアラートポリシーが引き継がれます。組み込みアラートポリシーは、Monitorデータベースに対応するアラートルールが存在しない場合にのみ作成されます。

組み込みアラートポリシーのしきい値については、「アラートポリシーの条件」セクションを参照してください。



高度なアラートポリシー

Directorのプロアクティブ通知およびアラート機能は、**高度なアラートポリシー**という新しいアラートフレームワークを含むように強化されました。この機能を使用すると、各要素または条件のきめ細かな詳細を含めてアラートを作成できるため、アラートのスコープに対する制御が強化されます。現在、これらのポリシーには、コスト削減とインフラストラクチャに関するアラートが含まれています。

データソース駆動型アラートである高度なアラートポリシーの導入により、複数条件のスコープフィルタリングを使用できます。

この機能は、重要な問題への対応の迅速性や有効性の低下につながる可能性のある過剰なアラートを減らすのに役立ちます。このポリシーは、アラートポリシーの有効性と管理者からのエンゲージメントを測定するのに役立ちます。

> > ****セクションから高度なアラートポリシーを作成できます。

次のデータソースのいずれかを選択できます。

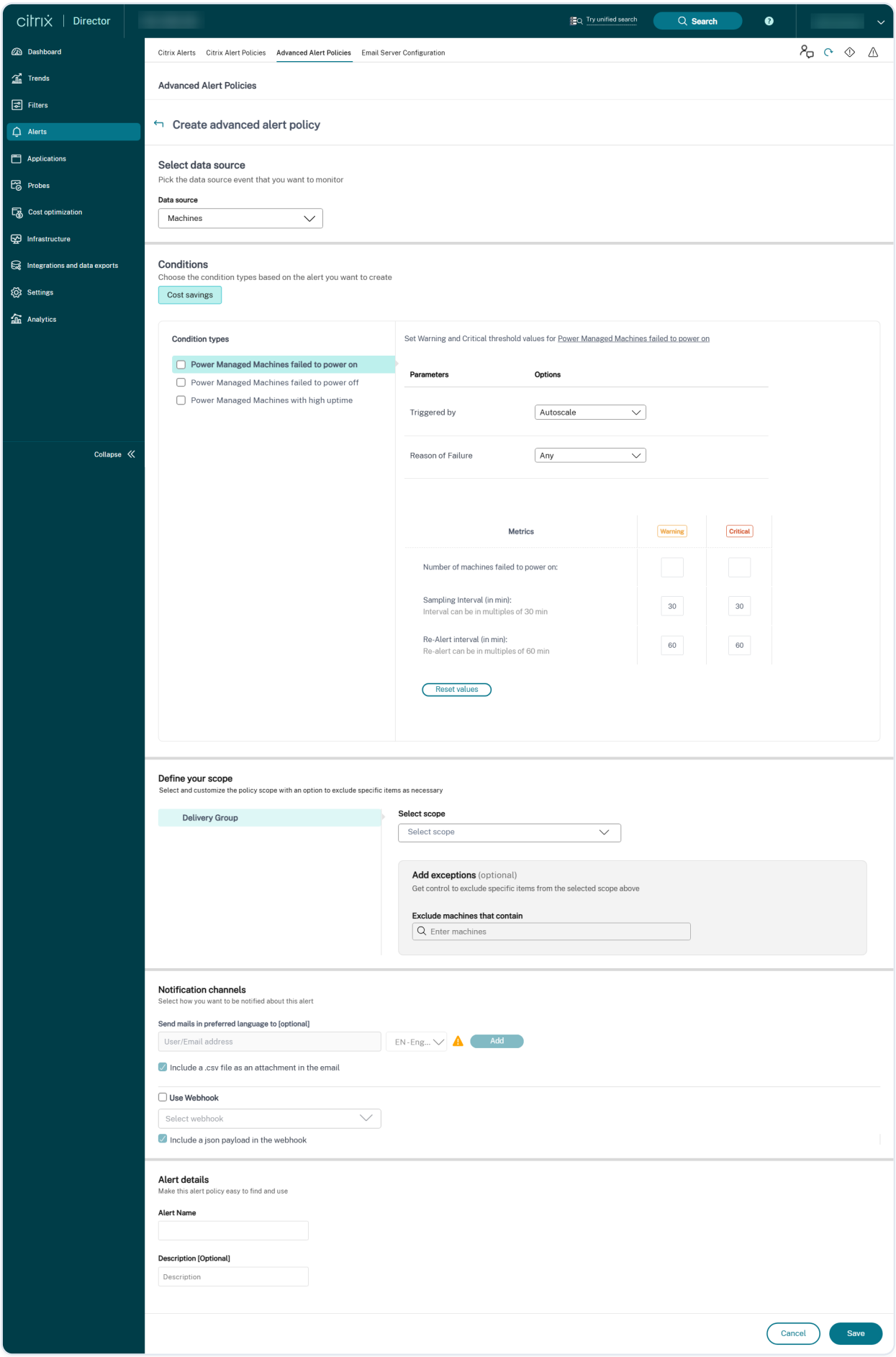
- マシン
- プロビジョニングサービス
- StoreFront™
- デリバリーコントローラー™

コスト削減に関するアラート

コストを最適化するのに役立つコスト削減のアラートを作成できます。現在、マシンに関するアラートを作成できます。

マシンに関するアラートを作成するには、次の手順を実行します。

1. ****タブ > **をクリックします。**ページが表示されます。
2. **ポリシーの作成**をクリックします。**高度なアラートポリシーの作成**セクションが表示されます。
3. データソースドロップダウンリストから**マシン**を選択します。コスト削減条件と対応する条件タイプが表示されます。


citrix | Director
Try unified search
Search
Dashboard
Trends
Filters
Alerts
Applications
Probes
Cost optimization
Infrastructure
Integrations and data exports
Settings
Analytics
Collapse
Citrix Alerts
Citrix Alert Policies
Advanced Alert Policies
Email Server Configuration
Advanced Alert Policies
Create advanced alert policy
Select data source
Pick the data source event that you want to monitor
Data source
Machines
Conditions
Choose the condition types based on the alert you want to create
Cost savings
Condition types
Power Managed Machines failed to power on
Power Managed Machines failed to power off
Power Managed Machines with high uptime
Set Warning and Critical threshold values for Power Managed Machines failed to power on
Parameters
Options
Triggered by
Autoscale
Reason of Failure
Any
Metrics
Warning
Critical
Number of machines failed to power on:
Sampling Interval (in min):
Interval can be in multiples of 30 min
30
30
Re-Alert interval (in min):
Re-alert can be in multiples of 60 min
60
60
Reset values
Define your scope
Select and customize the policy scope with an option to exclude specific items as necessary
Delivery Group
Select scope
Select scope
Add exceptions (optional)
Get control to exclude specific items from the selected scope above
Exclude machines that contain
Enter machines
Notification channels
Select how you want to be notified about this alert
Send mails in preferred language to [optional]
User/Email address
EN - Eng...
Add
Include a .csv file as an attachment in the email
Use Webhook
Select webhook
Include a json payload in the webhook
Alert details
Make this alert policy easy to find and use
Alert Name
Description [Optional]
Description
Cancel
Save

4. 必要な条件タイプを以下から選択します。
    - 電源管理されたマシンの電源オンに失敗しました
    - 電源管理されたマシンの電源オフに失敗しました
    - 高い稼働時間の電源管理マシン
5. 選択した各条件について、特定のパラメーターと対応するオプションを選択します。
6. 選択した条件タイプに対して、警告およびクリティカルのメトリックを設定します。
    - 高い稼働時間の電源管理マシンについて:
        - 稼働時間しきい値を超過したマシンの数
        - 再アラート間隔（分）は最低60分です。
    - 電源オンに失敗した電源管理マシンおよび電源オフに失敗した電源管理マシンについて:
        - 稼働時間しきい値を超過したマシンの数
        - サンプリング間隔（分）：間隔は30分の倍数にできます
        - 再アラート間隔（分）：再アラートは60分の倍数にできます
7. 必要に応じて、選択したアラートの再アラート間隔をスケジュールします。
8. アラートのスコープを定義します。
9. 通知チャネルを設定します。これはメールまたはWebhookにすることができます。
    a. 次のチェックボックスを選択できます。
        - WebhookにJSONペイロードを添付として含める
        - メールにCSVファイルを添付として含める

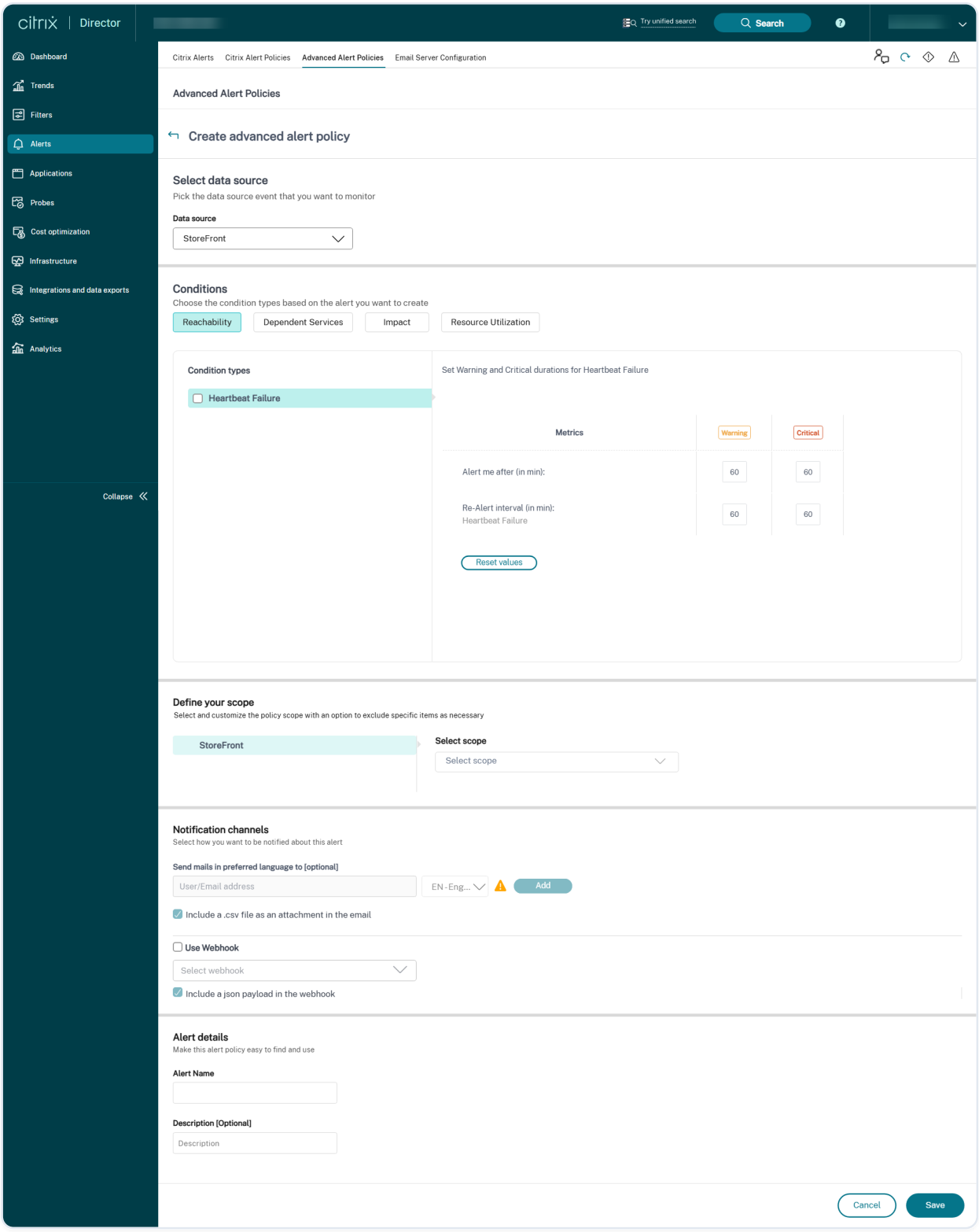
    詳細については、アラートコンテンツの強化を参照してください。
10. **アラート名**や**説明**（オプション）などの**アラートの詳細**を入力します。
11. **保存**をクリックします。アラートが作成されます。

インフラストラクチャ監視のアラート

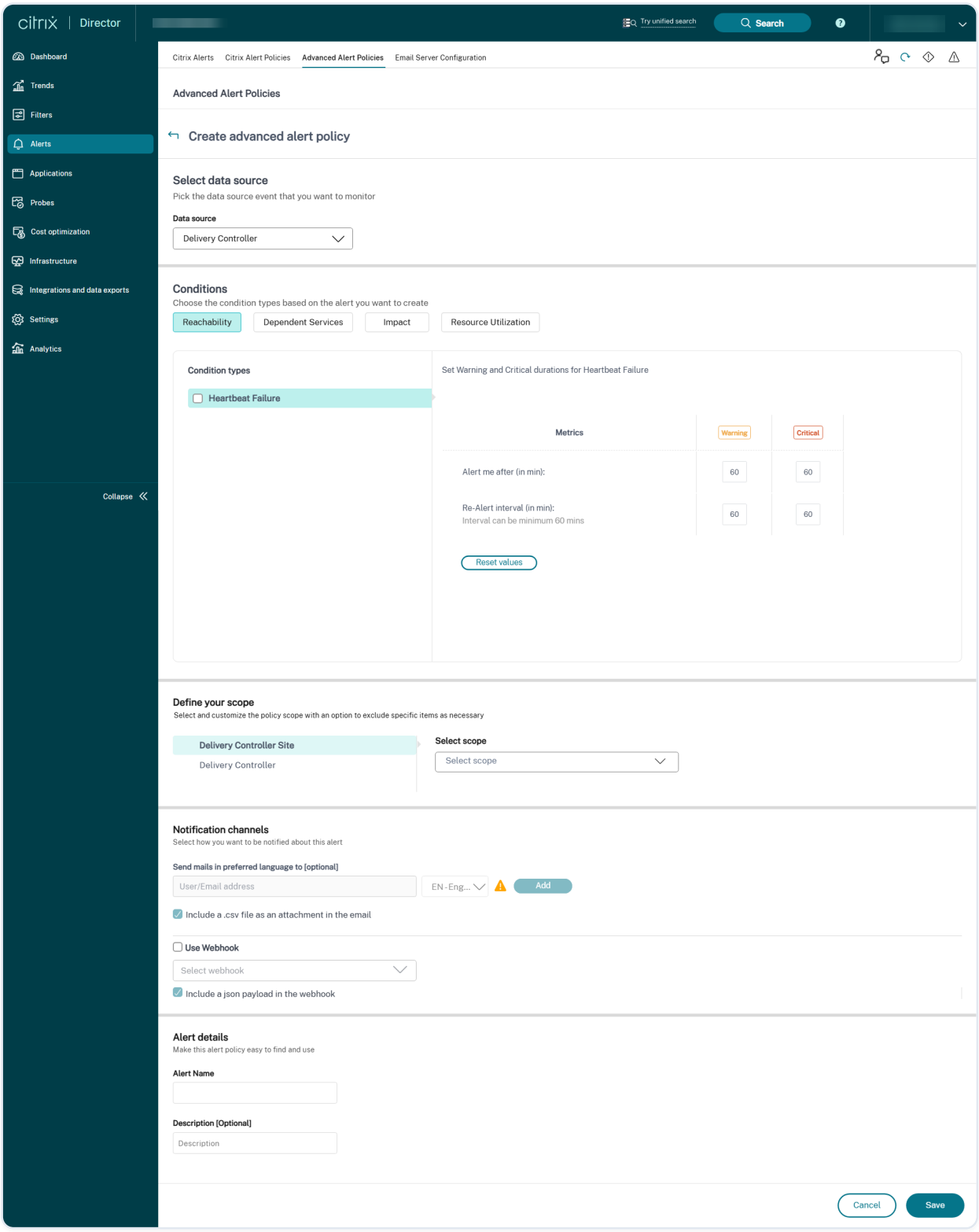
次のサポートされているCitrix Virtual Apps and Desktops™コンポーネントの健全性を監視するためにアラートを作成できます。

- プロビジョニングサービス

- StoreFront



- デリバリーコントローラー



インフラストラクチャ監視 の設定が完了すると、Directorで利用可能な健全性データを使用して、必要なコンポーネントのアラートを構成できます。管理者は、条件、スコープ、および通知媒体を設定して、電子メールまたはWebhookを介したJSONペイロードで重要なアラートを受信できます。Provisioning ServiceとDelivery Controllerの場合、アラートのスコープをサイトレベルまたは個々のサーバーレベルのいずれかとして選択できます。たとえば、Provisioning Serviceの場合、「すべてのProvisioning Service」を選択すると、サイトに2つのサーバーがある場合でも、サイト

全体に対して単一のアラートのみを受信します。これはサイトレベルのアラートと見なされます。発生したアラートは、分析と管理のために**Citrix Alerts**セクションでも利用できます。

新しく導入されたインフラストラクチャポリシーの一部として、アラート条件は次の4つのセクションに分類されます。

- 到達可能性
- 依存サービス
- 影響
- リソース使用率

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

アラート > **Citrixアラートポリシー**セクションからインフラストラクチャポリシーを作成できます。必要なカテゴリを選択し、ポリシーに必要な条件を選択できます。ポリシーの作成方法の詳細については、「アラートポリシーの作成」を参照してください。ポリシーが作成された後、Citrix Alerts ページでポリシーを編集、削除、または無効にできます。

各カテゴリとコンポーネントでサポートされている条件の詳細については、以下を参照してください。

- Provisioning Serviceの健全性メトリック
- StoreFront の正常性メトリック
- Delivery Controllerの健全性メトリック

次のデータは、電子メールまたは Citrix Alert ページでアラートとして受信されます。

フィールド	説明
顧客ID	サイトの顧客ID。
アラートレベル	指定可能な値は、Critical と Warning です。
ターゲット	アラートがトリガーされたマシンの名前。
時間	アラートがトリガーされた時刻。
スコープ	ポリシーのスコープ。
ポリシー	ポリシーの名前。

フィールド	説明
説明	アラートがトリガーされる問題の説明。

ポリシーのスコープを定義する

アラートのスコープを定義し、例外を追加できます。アラートは選択したスコープに対してのみ生成され、例外の追加を使用して除外されたサブスコープはアラート生成に含まれません。この機能は、詳細なレベルでアラートを作成するのに役立ちます。

メールまたはWebhook URLを介して通知を作成できます。アラートを受信する希望の言語を選択することもできます。また、アラートパラメータをメールの.CSVファイル添付として、またはWebhook URLを介したJSONペイロードとして受信するオプションを選択することもできます。添付ファイルには、必要なパラメータの詳細が含まれています。詳細については、「アラートコンテンツの機能強化」を参照してください。

次のデータは、メールまたは**Citrix Alerts**ページでアラートとして受信されます。

フィールド	説明
顧客ID	サイトの顧客ID。
アラートレベル	この値は、各アラート条件に設定された事前定義値です。可能な値は「Critical」と「Warning」です。
条件	この値は、ポリシー作成時に設定された条件です。たとえば、未登録のマシンの数が20以上である場合などです。
ターゲット	アラートがトリガーされるデリバリーグループまたはサイトの名前。
サイト	サイトの名前。
スコープ	ポリシーのスコープ。この値にはサブスコープも含まれます。
ポリシー	ポリシーの名前。
説明	アラートがトリガーされる問題の説明。

PowerShellスクリプトを使用して高度なアラートポリシーを作成する方法?

アラートポリシーを作成するためのPowerShellスクリプト:

```
asnp Citrix.Monitor.*

# Add Parameters

$timeSpan = New-TimeSpan -Seconds 30

$alertThreshold = 1

$alarmThreshold = 2

# Add Target UID's

$targetIds = @()

$targetIds += "e9a211b4-a1f3-4f74-b6c7-85225902e997"

# Add email addresses

$emailaddress = @()

$emailaddress += "loki@abc.com"

# Create new policy

$policy = New-MonitorNotificationPolicy -Name
"FailedMachinePercentageAlertCreationViaPowershell" -Description "Policy
created to test urm" -Enabled $true
```

次の行をFAILEDMACHINEPERCENTAGEの正しい条件に置き換えます

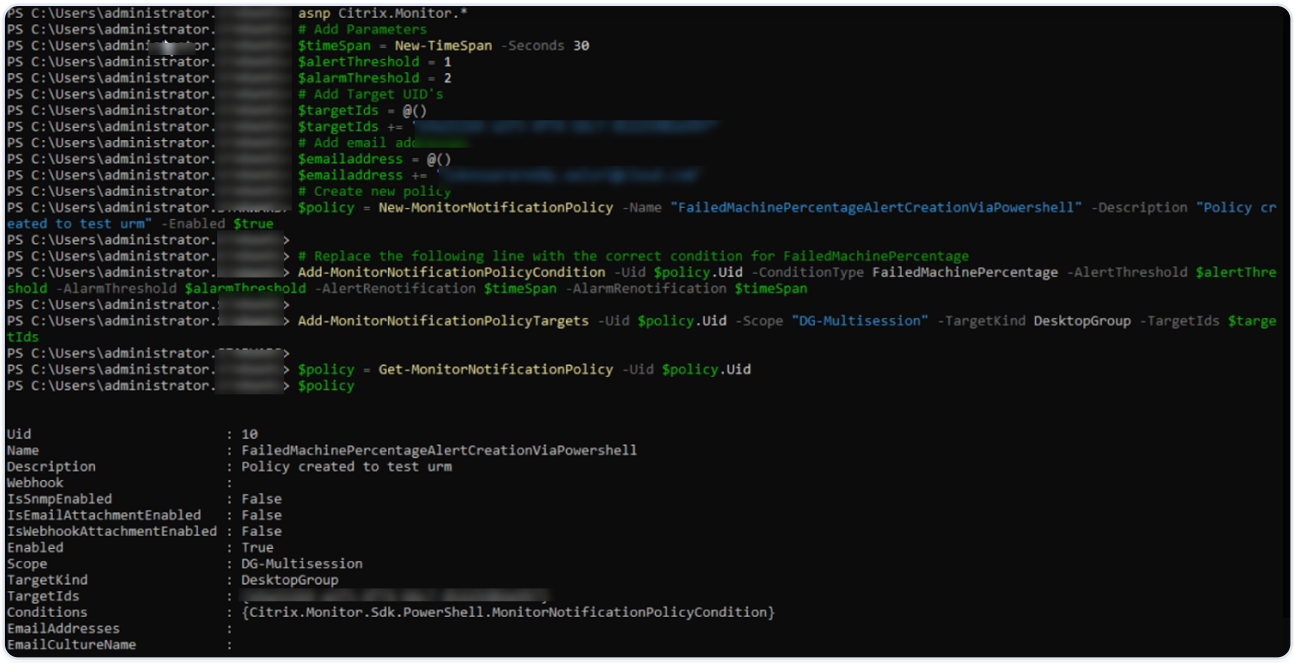
```
Add-MonitorNotificationPolicyCondition -Uid $policy.Uid -ConditionType
FailedMachinePercentage -AlertThreshold $alertThreshold -AlarmThreshold
$alarmThreshold -AlertRenotification $timeSpan -AlarmRenotification
$timeSpan



Add-MonitorNotificationPolicyTargets -Uid $policy.Uid -Scope "DG-
Multisession" -TargetKind DesktopGroup -TargetIds $targetIds
```

```
$policy = Get-MonitorNotificationPolicy -Uid $policy.Uid

$policy
```



上記の画像から、ポリシーが作成され、Uidが10であることがわかります。

構成にメールを追加するには

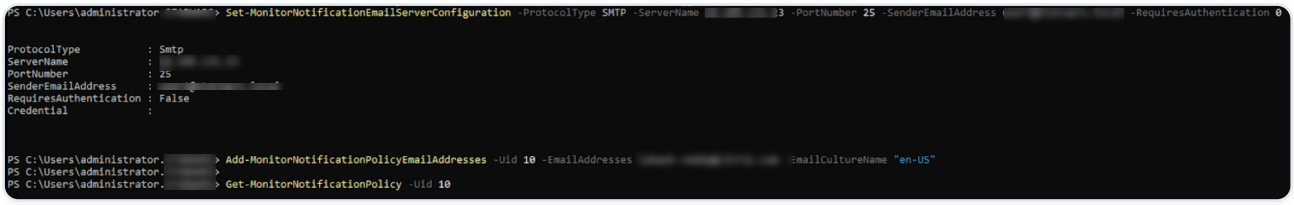
```
Set-MonitorNotificationEmailServerConfiguration -ProtocolType SMTP
-ServerName NameOfTheSMTPServerOrIPAddress -PortNumber 80
-SenderEmailAddress loki@abc.com -RequiresAuthentication 0
```

ポリシーにメールを追加するには

```
Add-MonitorNotificationPolicyEmailAddresses -Uid $policy.Uid
-EmailAddresses $emailaddress -EmailCultureName "en-US"
```

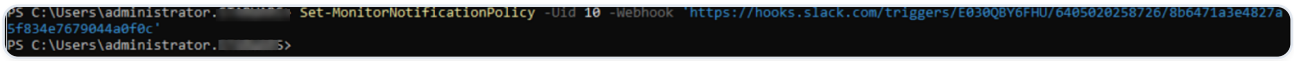
メールを追加するためのサンプルスクリプト:

```
Add-MonitorNotificationPolicyEmailAddresses -Uid 10 -EmailAddresses
$emailaddress -EmailCultureName "en-US"
```



ポリシーにWEBHOOK URLを追加するには

```
Set-MonitorNotificationPolicy –Uid $polcy.Uid –Webhook 'URL'
```

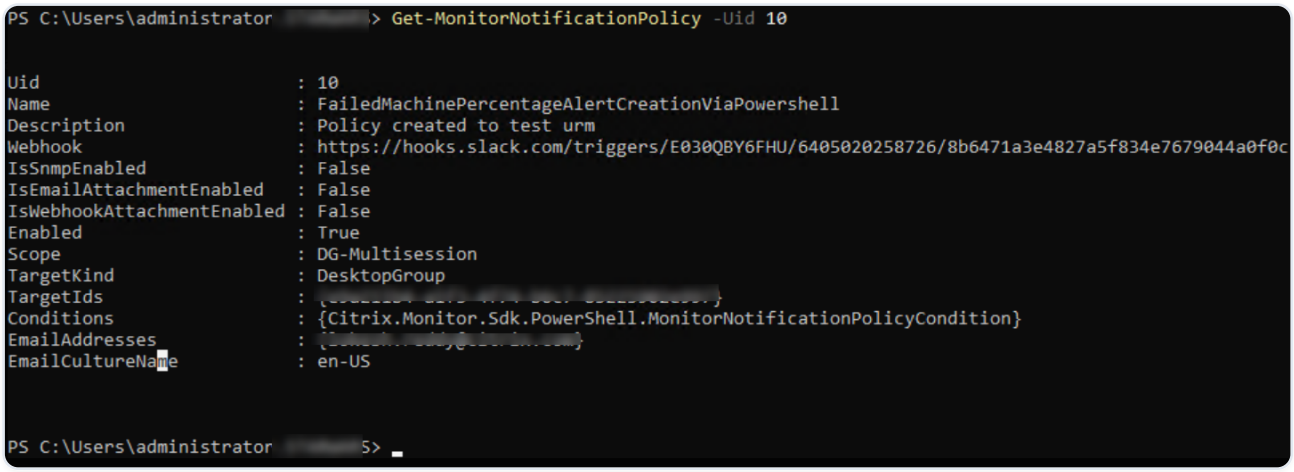


Webhook URLを追加するためのサンプルスクリプト:

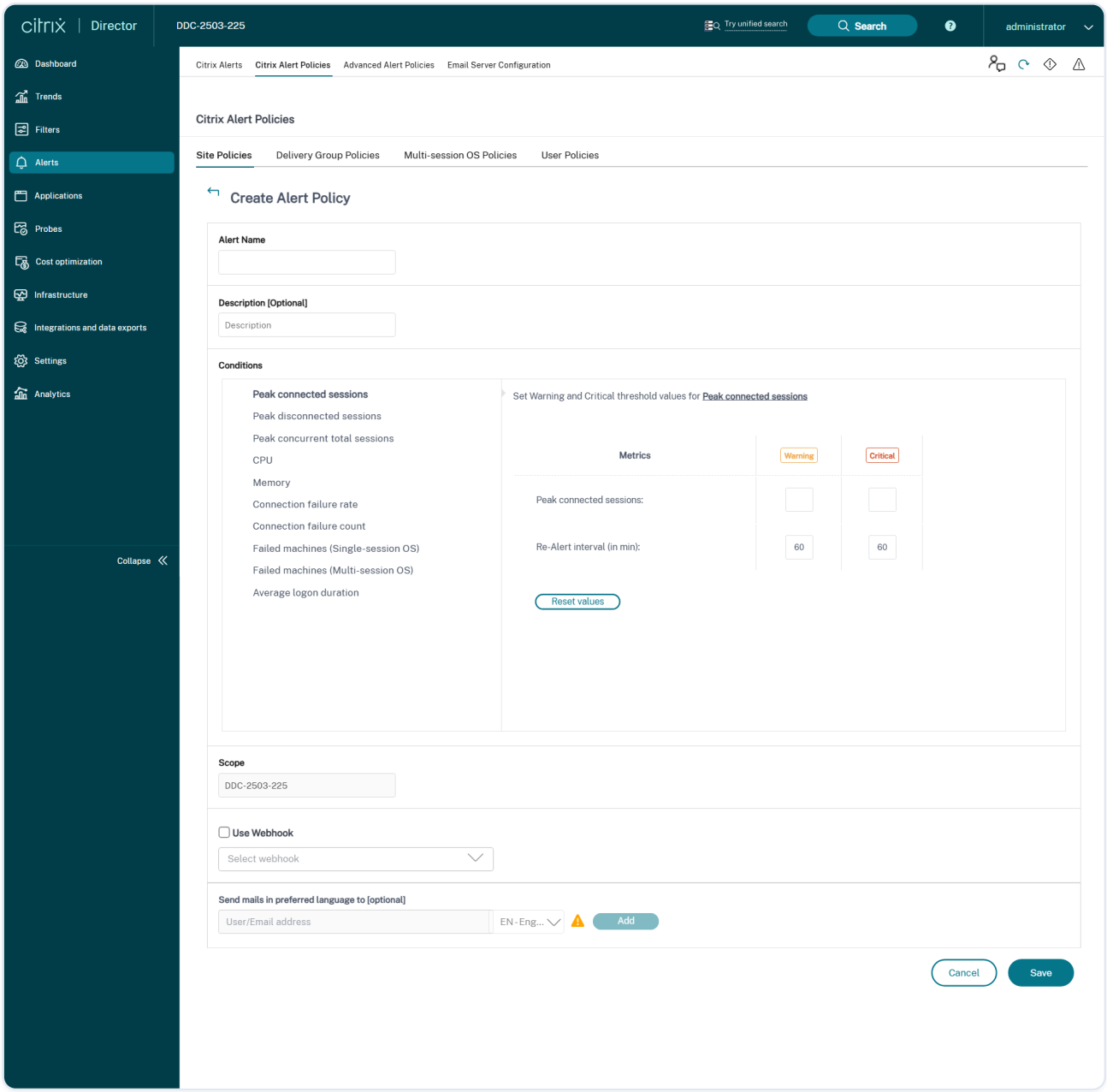
```
Set-MonitorNotificationPolicy –Uid 10  –Webhook  'https://hooks.slack.com/
triggers/E030QBY6FHU/6405020258726/8b6471a3e4827a5f834e7679022a1f1c'
```

作成されたポリシーの詳細を取得

```
Get-MonitorNotificationPolicy -Uid 10
```



アラートポリシーを作成する



アラートポリシーを作成するには、たとえば、特定のセッション数条件が満たされたときにアラートを生成するには、次の手順を実行します。

1. **アラート** > **Citrixアラートポリシー**に移動し、たとえば、マルチセッションOSポリシーを選択します。
2. **作成**をクリックします。
3. ポリシーに名前を付けて説明し、アラートがトリガーされるために満たす必要がある条件を設定します。たとえば、ピーク接続セッション、ピーク切断セッション、およびピーク同時合計セッションの警告値と危険値を指定します。警告値は危険値より大きくしてはいけません。詳細については、アラートポリシーの条件を参照してください。

4. 再アラート間隔を設定します。アラートの条件が引き続き満たされている場合、この時間間隔でアラートが再度トリガーされ、アラートポリシーで設定されている場合は、メール通知が生成されます。却下されたアラートは、再アラート間隔でメール通知を生成しません。
5. スコープを設定します。たとえば、特定のデリバリーグループに設定します。
6. 通知設定で、アラートがトリガーされたときにメールで通知する必要があるユーザーを指定します。アラートポリシーでメール通知設定を行うには、**メールサーバー構成**タブでメールサーバーを指定する必要があります。

    a. .CSV添付ファイルまたはJSONペイロードを介してアラートコンテンツを受信することもできます。これには、次のチェックボックスをオンにします。

    - **Webhookにjsonペイロードを添付として含める**
    - **メールにcsvファイルを添付として含める**

> **注:**
>
> .CSV添付ファイルおよびJSONペイロードを介してアラートコンテンツを受信するオプションは、現在、一部のアラートでのみ利用可能です。詳細については、「アラートコンテンツの機能強化」を参照してください。

7. 「**保存**」をクリックします。

スコープで20以上のデリバリーグループが定義されたポリシーを作成すると、構成の完了に約30秒かかる場合があります。この間、スピナーが表示されます。

最大20の固有のデリバリーグループ（合計1000のデリバリーグループターゲット）に対して50を超えるポリシーを作成すると、応答時間が増加する可能性があります（5秒以上）。

アクティブなセッションを含むマシンをあるデリバリーグループから別のデリバリーグループに移動すると、マシンパラメーターを使用して定義された誤ったデリバリーグループアラートがトリガーされる可能性があります。

> **注:**
>
> アラートポリシーを削除した後、そのポリシーによって生成されたアラート通知が停止するまでに最大30分かかる場合があります。

アラートコンテンツの機能強化

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

現在、この機能強化は次のアラートでのみ利用可能です。

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

この機能を使用するには、アラートに移動し、次のチェックボックスを選択します。

- **Webhookにjsonペイロードを添付として含める**
- **メールにcsvファイルを添付として含める**

以下は、**Citrix Alert Policies**セクションのスクリーンショットです。

強化されたアラート(/en-us/citrix-virtual-apps-desktops/current-release/media/csv-and-webhook.png)

以下は、**Advanced Alert Policies**セクションのスクリーンショットです。

強化されたアラート（詳細）(/en-us/citrix-virtual-apps-desktops/current-release/media/csv-and-webhook-advanced.png)

CSV添付ファイル

次の表は、サポートされているすべてのアラートの.CSV添付ファイルの列を示しています。

列	適用されるアラート
マシン名、IPアドレス、およびデリバリーグループ名	マシンの稼働時間、電源オフ失敗アクションと電源オン失敗アクション、および未登録マシン（%）
現在の登録状態、失敗日、障害状態、およびライフサイクル状態	未登録マシン（%）

列	適用されるアラート
最終電源アクション失敗理由、最終電源アクショントリガー元、最終電源アクションタイプ、および最終電源アクション完了日	電源オフ失敗アクションと電源オン失敗アクション
電源状態、電源オン日時、総稼働時間（分）	マシンの稼働時間

WEBHOOKペイロード

未登録マシンの割合アラート

```
{

  "text": "{\"Address\":\"<Webhook URL>\",\"NotificationId\":
\"<NotificationGUID>\",\"NotificationState\":\"NotificationActive\",
\"Priority\":\"<Critical/Warning>\",\"Target\":\"<DeliveryGroupName>\",
\"Condition\":\"Unregistered machines (in %)\",\"Value\":\"<Value Set as
Threshold>\",\"Timestamp\":\"<Timestamp string Eg: April 25, 2024 9:33 PM
(UTC +5)>\",\"PolicyName\":\"<Alert Policy Name>\",\"Description\":
\"<Alert Policy Description>\",\"Scope\":\"DeliveryGroup\",\"Site\":
\"<Name of the Site>\",\"AttachmentData\":[{\"MachineName\":\"<Name of the
Machine>\",\"IPAddress\":\"<IP Address>\",\"DeliveryGroupName\":\"<Name of
the DeliveryGroup>\",\"CurrentRegistrationState\":\"Unregistered\",
\"FailureDate\":\"<Date of Failure>\",\"FaultState\":\"<Fault State of the
Machine>\",\"LifecycleState\":\"<Lifecycle state of the Machine>\"},
{\"MachineName\":\"<Name of the Machine>\",\"IPAddress\":\"<IP Address>\",
\"DeliveryGroupName\":\"<Name of the DeliveryGroup>\",
\"CurrentRegistrationState\":\"Unregistered\",\"FailureDate\":\"<Date of
Failure>\",\"FaultState\":\"<Fault State of the Machine>\",
\"LifecycleState\":\"<Lifecycle state of the Machine>\"}]}"

}
```

電源オン失敗アクションアラート

```
{

  "text": "{\"Address\":\"<Webhook URL>\",\"NotificationId\":
\"<NotificationGUID>\",\"NotificationState\":\"NotificationActive\",
\"Priority\":\"<Critical/Warning>\",\"Target\":\"<DeliveryGroupName>\",
\"Condition\":\"Failure To PowerOn Action\",\"Value\":\"<Value Set as
Threshold>\",\"Timestamp\":\"<Timestamp string Eg: April 25, 2024 9:33 PM
(UTC +5)>\",\"PolicyName\":\"<Alert Policy Name>\",\"Description\":
```

```
\"<Alert Policy Description>\",\"Scope\":\"DeliveryGroup\",\"Site\":
\"<Name of the Site>\",\"AttachmentData\":[{\"MachineName\":\"<Name of the
Machine>\",\"IPAddress\":\"<IP Address>\",\"DeliveryGroupName\":\"<Name of
the DeliveryGroup>\",\"LastPowerActionFailureReason\":
\"<HypervisorReportedFailure, HypervisorRateLimitExceeded, UnknownError,
Power Action Type>\",\"LastPowerActionTriggeredBy\":\"<End-User,
Administrator, Auto-Scale, Schedule>\",\"LastPowerActionType\":\"<PowerOn/
PowerOff>\",\"LastPowerActionCompletedDate\":\"<Time string Eg:
2024-05-15T15:04:27.723>\"},{\"MachineName\":\"<Name of the Machine>\",
\"IPAddress\":\"<IP Address>\",\"DeliveryGroupName\":\"<Name of the
DeliveryGroup>\",\"LastPowerActionFailureReason\":
\"<HypervisorReportedFailure, HypervisorRateLimitExceeded, UnknownError,
Power Action Type>\",\"LastPowerActionTriggeredBy\":\"<End-User,
Administrator, Auto-Scale, Schedule>\",\"LastPowerActionType\":\"<PowerOn/
PowerOff>\",\"LastPowerActionCompletedDate\":\"<Time string Eg:
2024-05-15T15:04:27.723>\"}]}"

}
```

電源オフ失敗アクションアラート

```
{

  "text": "{\"Address\":\"<Webhook URL>\",\"NotificationId\":
\"<NotificationGUID>\",\"NotificationState\":\"NotificationActive\",
\"Priority\":\"<Critical/Warning>\",\"Target\":\"<DeliveryGroupName>\",
\"Condition\":\"Failure To PowerOff Action\",\"Value\":\"<Value Set as
Threshold>\",\"Timestamp\":\"<Timestamp string Eg: April 25, 2024 9:33 PM
(UTC +5)>\",\"PolicyName\":\"<Alert Policy Name>\",\"Description\":
\"<Alert Policy Description>\",\"Scope\":\"DeliveryGroup\",\"Site\":
\"<Name of the Site>\",\"AttachmentData\":[{\"MachineName\":\"<Name of the
Machine>\",\"IPAddress\":\"<IPV4 Address of the Machine>\",
\"DeliveryGroupName\":\"<Name of the DeliveryGroup>\",
\"LastPowerActionFailureReason\":
\"<HypervisorReportedFailure,HypervisorRateLimitExceeded,UnknownError,Powe
r Action Type>\",\"LastPowerActionTriggeredBy\":\"<End-
User,Administrator,Auto-Scale,Schedule>\",\"LastPowerActionType\":
\"<PowerOn/PowerOff>\",\"LastPowerActionCompletedDate\":\"<Time string Eg:
2024-05-15T15:04:27.723>\"},{\"MachineName\":\"<Name of the Machine>\",
\"IPAddress\":\"<IPV4 Address of the Machine>\",\"DeliveryGroupName\":
\"<Name of the DeliveryGroup>\",\"LastPowerActionFailureReason\":
\"<HypervisorReportedFailure,HypervisorRateLimitExceeded,UnknownError,Powe
r Action Type>\",\"LastPowerActionTriggeredBy\":\"<End-
User,Administrator,Auto-Scale,Schedule>\",\"LastPowerActionType\":
```

```
\"<PowerOn/PowerOff>\",\"LastPowerActionCompletedDate\":\"<Time string Eg:
2024-05-15T15:04:27.723>\"}]}"

}
```

マシンの稼働時間アラート

```
{

  "text": "{\"Address\":\"<Webhook URL>\",\"NotificationId\":
\"<NotificationGUID>\",\"NotificationState\":\"NotificationActive\",
\"Priority\":\"<Critical/Warning>\",\"Target\":\"<DeliveryGroupName>\",
\"Condition\":\"Machine Uptime Alert\",\"Value\":\"<Value Set as
Threshold>\",\"Timestamp\":\"<Timestamp string Eg: April 25, 2024 9:33 PM
(UTC +5)>\",\"PolicyName\":\"<Alert Policy Name>\",\"Description\":
\"<Alert Policy Description>\",\"Scope\":\"DeliveryGroup\",\"Site\":
\"<Name of the Site>\",\"AttachmentData\":[{\"MachineName\":\"<Name of the
Machine>\",\"IPAddress\":\"<IP Address>\",\"DeliveryGroupName\":\"<Name of
the DeliveryGroup>\",\"PowerState\":\"<On/Off>\",\"PoweredOnDate\":
\"2024-05-15T15:04:27.723\",\"TotalUptimeInMinutes\":180},
{\"MachineName\":\"<Name of the Machine>\",\"IPAddress\":\"<IP Address>\",
\"DeliveryGroupName\":\"<Name of the DeliveryGroup>\",\"PowerState\":
\"<ON/OFF>\",\"PoweredOnDate\":\"2024-05-15T15:04:27.723\",
\"TotalUptimeInMinutes\":\"<Uptime Duration>\"}]}"

}
```

アラートポリシーの条件

以下に、アラートカテゴリ、アラートを軽減するための推奨アクション、および定義されている場合は組み込みポリシー条件を示します。組み込みのアラートポリシーは、アラートおよび再アラートの間隔が60分に設定されています。

ピーク接続セッション

- Directorのセッショントレンドビューで、接続済みセッションのピークを確認します。
- セッション負荷に対応する十分な容量があることを確認してください。
- 必要に応じて新しいマシンを追加する

ピーク切断セッション

- Directorのセッショントレンドビューで、切断済みセッションのピークを確認します。
- セッション負荷に対応できる十分な容量があることを確認します。
- 必要に応じて、新しいマシンを追加します。
- 必要に応じて、切断されたセッションをログオフします。

ピーク時の同時合計セッション数

- Directorのセッショントレンドビューで、同時セッションのピークを確認します。
- セッション負荷に対応できる十分な容量があることを確認します。
- 必要に応じて、新しいマシンを追加します。
- 必要に応じて、切断されたセッションをログオフします。

CPU

CPU 使用率の割合は、プロセスを含む VDA 上の全体的な CPU 消費量を示します。個々のプロセスによる CPU 使用率の詳細については、対応する VDA の ページで確認できます。

- **> >** に移動し、CPU を消費しているプロセスを特定します。プロセスレベルのリソース使用状況統計の収集を開始するには、プロセス監視ポリシーが有効になっていることを確認してください。
- 必要に応じてプロセスを終了します。
- プロセスを終了すると、保存されていないデータが失われます。
- すべてが期待どおりに機能している場合は、将来的に追加のCPUリソースを追加します。

> **注:**
>
> **リソース監視を有効にする**ポリシー設定は、VDAがインストールされているマシンでのCPUおよびメモリのパフォーマンスカウンターの監視に対して、デフォルトで許可されています。このポリシー設定が無効になっている場合、CPUおよびメモリの状態に関するアラートはトリガーされません。詳しくは、「監視ポリシー設定」を参照してください。
>
> **スマートポリシー条件:**

- **スコープ：** デリバリーグループ、マルチセッションOSスコープ
- **しきい値:** 警告 - 80%、危険 - 90%

メモリ

メモリ使用率は、VDA上の全体的なメモリ消費量（プロセスによるものを含む）を示します。
個々のプロセスによるメモリ使用量に関する詳細な情報は、対応するVDAの**マシン詳細**ページから取得できます。

- **［マシン詳細］>［履歴使用率の表示］>［上位10プロセス］** に移動し、メモリを消費しているプロセスを特定します。プロセスレベルのリソース使用状況統計の収集を開始するには、プロセス監視ポリシーが有効になっていることを確認してください。
- 必要に応じてプロセスを終了します。
- プロセスを終了すると、保存されていないデータが失われます。
- すべてが期待どおりに機能している場合は、将来的に追加のメモリを追加します。

> **注:**
>
> **リソース監視を有効にする**ポリシー設定は、VDAがインストールされているマシンでのCPUおよびメモリのパフォーマンスカウンターの監視に対して、デフォルトで許可されています。このポリシー設定が無効になっている場合、CPUおよびメモリの状態に関するアラートはトリガーされません。詳しくは、「監視ポリシー設定」を参照してください。
>
> **スマートポリシー条件:**
>
> - **スコープ：** デリバリーグループ、マルチセッションOSスコープ
> - **閾値:** 警告 - 80%、危機的 - 90%

接続失敗率

過去1時間の接続失敗の割合。

- 試行された総接続数に対する総失敗数に基づいて計算されます。
- Directorの接続失敗トレンドビューで、構成ログから記録されたイベントを確認します。
- アプリケーションまたはデスクトップが到達可能であるかどうかを判断します。

接続失敗数

過去1時間の接続失敗数。

- Director Connection Failures Trendsビューで、構成ログから記録されたイベントを確認します。

- アプリケーションまたはデスクトップが到達可能であるかどうかを判断します。

ICA® RTT (平均)

平均ICAラウンドトリップ時間。

- ICA RTTの内訳についてCitrix ADMを確認し、根本原因を特定します。詳細については、Citrix ADMドキュメントを参照してください。
- Citrix ADMが利用できない場合は、DirectorのユーザーDetailビューでICA RTTと遅延を確認し、ネットワークの問題か、アプリケーションまたはデスクトップの問題かを判断します。

ICA RTT (セッション数)

閾値のICAラウンドトリップ時間を超えるセッションの数。

- ICA RTTが高いセッション数についてCitrix ADMを確認します。詳細については、Citrix ADMドキュメントを参照してください。
- Citrix ADMが利用できない場合は、ネットワークチームと協力して根本原因を特定します。

  スマートポリシーの条件:

  - **スコープ:** デリバリーグループ、マルチセッションOSスコープ
  - **しきい値:** 警告 - 5セッション以上で300ミリ秒、重大 - 10セッション以上で400ミリ秒

ICA RTT (セッションの割合)

平均ICAラウンドトリップ時間を超えるセッションの割合。

- ICA RTTが高いセッション数についてCitrix ADMを確認します。詳細については、Citrix ADMドキュメントを参照してください。
- Citrix ADMが利用できない場合は、ネットワークチームと協力して根本原因を特定します。

ICA RTT (ユーザー)

指定されたユーザーによって起動されたセッションに適用されるICAラウンドトリップ時間。ICA RTTが少なくとも1つのセッションでしきい値を超えた場合、アラートがトリガーされます。

失敗したマシン（シングルセッションOS）

失敗したシングルセッションOSマシンの数。失敗は、Directorのダッシュボードおよびフィルタービューに示されているように、さまざまな理由で発生する可能性があります。

- Citrix Scout診断を実行して、根本原因を特定します。

  スマートポリシー条件:

- **スコープ:** デリバリーグループ、マルチセッションOSスコープ
- **しきい値:** 警告 - 1、重大 - 2

失敗したマシン (マルチセッションOS)

失敗したマルチセッションOSマシンの数。失敗は、Directorのダッシュボードおよびフィルタービューに示されているように、さまざまな理由で発生する可能性があります。

- Citrix Scout診断を実行して、根本原因を特定します。

  スマートポリシー条件:

  - **スコープ:** デリバリーグループ、マルチセッションOSスコープ
  - **しきい値:** 警告 - 1、重大 - 2

失敗したマシン (割合)

デリバリーグループ内の失敗したシングルセッションおよびマルチセッションOSマシンの割合。これは、失敗したマシンの数に基づいて計算されます。このアラート条件では、デリバリーグループ内の失敗したマシンの割合としてアラートしきい値を構成でき、30秒ごとに計算されます。失敗は、Directorのダッシュボードおよびフィルタービューに示されているように、さまざまな理由で発生する可能性があります。Citrix Scout診断を実行して、根本原因を特定します。詳細については、「ユーザーの問題のトラブルシューティング」を参照してください。

電源オンアクションの失敗と電源オフアクションの失敗

デリバリーグループ内の電源オンアクションの失敗数と電源オフアクションの失敗数。これは、電源オンまたはオフに失敗した**電源管理マシン**の数に基づいて計算されます。このアラート条件では、デリバリーグループ内で電源オンまたはオフに失敗した**電源管理マシン**の数としてアラートしきい値を構成でき、30分ごとに計算されます。

管理者は、高度なアラートポリシーでこれらのアラートに対して次のパラメーターを構成できます。

- トリガー元: 電源アクションをトリガーしたもの
- 失敗の理由: なぜアクションが失敗したのか
- しきい値: ポリシーをトリガーするために電源アクションが失敗したマシンのしきい値の数
- サンプリング間隔: 失敗した電源アクションをチェックする必要がある間隔
- 再アラート間隔: アラートを再送信するまでの時間

失敗は、Directorのダッシュボードおよびフィルタービューに示されているように、さまざまな理由で発生する可能性があります。Citrix Scout診断を実行して、根本原因を特定します。詳細については、「ユーザーの問題のトラブルシューティング」を参照してください。

未登録マシン（%）

マシンが再起動によって不安定になった場合、またはデリバリーコントローラーと仮想マシン間の通信に問題がある場合、マシンは未登録と見なされます。**未登録マシン（%）**は、デリバリーグループ内の未登録のシングルセッションおよびマルチセッションOSマシンの割合であり、未登録マシンの数に基づいて計算されます。このアラート条件では、デリバリーグループ内の未登録マシンの割合として、警告およびクリティカルなしきい値を構成できます。再アラートの間隔を設定できます。**未登録マシン（%）の条件が満たされたときに通知を受け取るために、メールを追加することもできます。クリティカルまたは警告のしきい値を超えると、アラートとメールが生成されます。アラートはCitrix Alerts**で確認できます。**未登録マシン（%）**カテゴリ、および必要な状態と時間でフィルターできます。

メールがある場合はCSV添付ファイルで、Webhookがある場合はJSONペイロードで、アラートの詳細を受け取ることもできます。

> **注:**
>
> クリティカル値は警告値よりも大きくする必要があります。

> **ポリシー条件:**

- **スコープ**: シングルセッションOS、およびマルチセッションOSデリバリーグループ
- **しきい値**: 警告とクリティカル

マシン稼働時間アラート

デリバリーグループ内のマシンの稼働時間は、デリバリーグループ内で電源がオンになっているマシンの1日あたりの時間数、1週間あたりの時間数、または1か月あたりの時間数に基づいて計算されます。このアラート条件を使用すると、デリバリーグループ内でマシンが電源オンになっている時間としてアラートしきい値を構成できます。マシンの稼働時間アラートは、次の場合に次のように機能します。

- 1日あたりの時間数 - マシンが1日あたり電源オンになっている時間数を指定でき、30分ごとに計算されます。設定できる1日あたりの最大時間数は24時間です。
- 週あたりの時間 - マシンが1週間に稼働する時間を指定でき、6時間ごとに計算されます。設定できる週あたりの最大時間は168時間です。

- 月あたりの時間 - マシンが1ヶ月に稼働する時間を指定でき、毎日1回計算されます。月あたりの最大時間は720時間です。 設定できる再アラート間隔の最小値は60分です。警告および重大アラートセクションで、マシンの稼働時間しきい値を超過するマシンの数を入力できます。また、任意のマシンに対して例外を追加することもできます。

たとえば、このアラートに5つのデリバリーグループが追加されており、最初のデリバリーグループと4番目のデリバリーグループでマシンの数が警告または重大なしきい値を超えた場合、アラートは最初のデリバリーグループと4番目のデリバリーグループに対して個別にトリガーされます。

このアラートは、管理者がマシンの稼働時間を分析するのに役立ち、この分析に基づいて管理者はコストの最適化に貢献できます。メールがある場合はCSV添付ファイルで、Webhookがある場合はJSONペイロードで、アラートの詳細を受け取ることもできます。

平均ログオン時間

過去1時間に発生したログオンの平均ログオン時間。

- Directorダッシュボードでログオン期間に関する最新のメトリックを確認します。短期間に多くのユーザーがログオンすると、ログオン期間が長くなる可能性があります。
- ログオンのベースラインと内訳を確認して、原因を絞り込みます。詳細については、「ユーザーログオンの問題の診断」を参照してください。

  スマートポリシー条件:

  - **スコープ:** デリバリーグループ、マルチセッションOSスコープ
  - **しきい値:** 警告 - 45秒、重大 - 60秒

ログオン時間（ユーザー）

過去1時間に発生した、指定されたユーザーのログオンのログオン時間。

負荷評価インデックス

過去5分間の負荷評価インデックスの値。

- ピーク負荷（最大負荷）が発生している可能性のあるマルチセッションOSマシンについて、Directorで確認します。ダッシュボード（障害）とトレンドの負荷評価インデックスレポートの両方を確認します。

  スマートポリシーの条件:

  - **スコープ:** デリバリーグループ、マルチセッションOSスコープ
  - **しきい値:** 警告 - 80%、重大 - 90%

Webhook を使用してアラートポリシーを構成する

電子メール通知とは別に、Webhook を使用してアラートポリシーを構成できます。

注: この機能には、Delivery Controller バージョン 7.11 以降が必要です。

PowerShell コマンドレットを使用して、HTTP コールバックまたは HTTP POST でアラートポリシーを構成できます。これらは Webhook をサポートするように拡張されています。

新しい Octoblu ワークフローの作成と、対応する Webhook URL の取得については、Octoblu Developer Hub を参照してください。

新しいアラートポリシーまたは既存のポリシーの Webhook URL を構成するには、次の PowerShell コマンドレットを使用します。

Webhook URLを使用して新しいアラートポリシーを作成します:

```
$policy = New-MonitorNotificationPolicy -Name <Policy name> -Description
<Policy description> -Enabled $true -Webhook <Webhook URL>
```

既存のアラートポリシーに Webhook URL を追加する:

```
Set-MonitorNotificationPolicy - Uid <Policy id> -Webhook <Webhook URL>
```

PowerShellコマンドのヘルプについては、PowerShellヘルプを使用してください。例:

```
Get-Help  <Set-MonitorNotificationPolicy>
```

アラートポリシーから生成された通知は、Webhook URL への POST 呼び出しで Webhook をトリガーします。POST メッセージには、JSON 形式の通知情報が含まれています。

```
{"NotificationId" : \<Notification Id\>,



"Target" : \<Notification Target Id\>,



"Condition" : \<Condition that was violated\>,
```

```
"Value" : \<Threshold value for the Condition\>,

"Timestamp": \<Time in UTC when notification was generated\>,

"PolicyName": \<Name of the Alert policy\>,

"Description": \<Description of the Alert policy\>,

"Scope" : \<Scope of the Alert policy\>,

"NotificationState": \<Notification state critical, warning, healthy or dismissed\>,

"Site" : \<Site name\>}
```

アラートの一括解除

この機能は、管理者のアラート管理プロセスを最適化し、柔軟性を提供し、アラート疲労を軽減します。管理者は、時間、種類、またはカテゴリに基づいてアラートを一括解除でき、メンテナンス中やハイパーバイザーおよびその他の環境を扱う際のアラート管理を簡素化します。

アラートの一括解除は、管理者がワークロードを効率的に管理し、大量のアラートに圧倒されるのを防ぐのに役立ちます。

アラートを一括解除する手順

1. **アラート** > **Citrixアラート**タブに移動します。アラートが表示されます。

   「一括アラート」(/en-us/citrix-virtual-apps-desktops/current-release/media/bulk-alert.png)

2. **ソース**、**カテゴリ**、**状態**、または**期間**からオプションを選択して、解除したいアラートをフィルタリングします。特定のアラートが表示されます。
3. 特定のアラートの横にあるチェックボックスを選択するか、上部にあるチェックボックスを選択してすべてのアラートを選択します。
4. **解除**をクリックします。アラートの解除を確認する通知が表示されます。
5. **はい**をクリックします。選択されたアラートは*解除済み*としてマークされ、アラートのステータスがそれに応じて更新されます。

PowerShell SDKを使用したWebhook構成

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

> **注:**
>
> サポートされているペイロード形式はテキストであり、エンドユーザーはWebhookでテキストを有効にする必要があります。
>
> 最新のペイロード形式は次のとおりです。

```
{"text": "This is a message from a Webex incoming webhook."}
```

Webhookを作成する

次のPowerShellサンプルコマンドを使用して、Webhookプロファイルを作成できます。

認証ヘッダーなしでWebhookを作成するには:

```
$headers = [System.Collections.Generic.Dictionary[string,string]]::new()



$headers.Add("Content-Type", "application/json")



$payloads = '{ "text": "$PAYLOAD" }'
```

```
$url = "<Fill this field with the required URL>"


Add-MonitorWebhookProfile -Name "profile_slack" -Description "webhook
profile for slack" -Url $url -Headers $headers -PayloadFormat $payloads
```

認証ヘッダーを使用してWebhookを作成するには:

```
$headers = [System.Collections.Generic.Dictionary[string,string]]::new()


$headers.Add("Content-Type", "application/json")

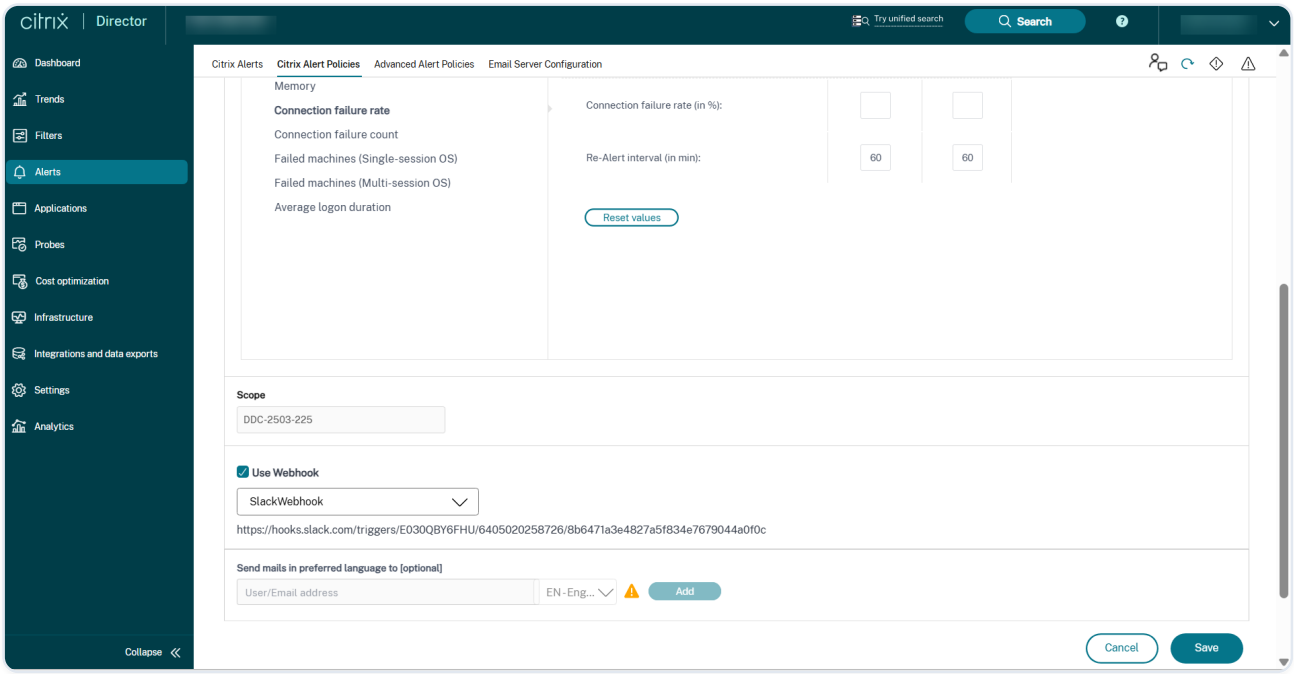

$headers.Add("Authorization", "Basic <Fill this field with the
authorization token>")


$payloads = '{ "text": "$PAYLOAD" }'


$url = "<Fill this field with the required URL>"


Add-MonitorWebhookProfile -Name "profile_azure" -Description "webhook
profile for azure function with Authentication" -Url $url -Headers
$headers -PayloadFormat $payloads
```

プロファイルが作成されたら、データベースで確認できます。また、新しく作成されたWebhookプロファイルは、**Citrix Alerts**ページで見つけることができます。



Webhookプロファイルを更新する

次のPowerShellサンプルコマンドを使用して、Webhookプロファイルを更新できます。

```
$headers = [System.Collections.Generic.Dictionary[string,string]]::new()


$headers.Add("Content-Type", "application/json")


$payloads = '{ "text": "$PAYLOAD" }'


$url =  "<Fill this field with the required URL>"


Set-MonitorWebhookProfile -Uid 1  -Name "profile_slack_citrix"
-Description "webhook profile for citrix slack" -Url $url -Headers
$headers -PayloadFormat $payloads
```

すべてのWebhookプロファイルの一覧を取得する

利用可能なすべてのWebhookプロファイルの一覧を取得するには、次のPowerShellコマンドのサンプルを使用できます。

```
Get-MonitorWebhookProfile



Get-MonitorWebhookProfile -Name 'profile_msteams'



Get-MonitorWebhookProfile -Uid 1
```

Webhookプロファイルを削除する

Webhookプロファイルを削除するには、次のPowerShellコマンドのサンプルを使用できます。

```
Remove-MonitorWebhookProfile -Uid 1
```

注:

Webhookプロファイルがいずれかのポリシーにマッピングされている場合、削除できません。回避策として、まずポリシーからWebhookマッピングを削除する必要があります。

Webhookプロファイルを使用してポリシーを作成する

Webhookプロファイルを使用してポリシーを作成するには、次のPowerShellコマンドのサンプルを使用できます。

```
New-MonitorNotificationPolicy -Name "Policy1" -Description "Policy
Description" -Enabled $true -WebhookProfileId 1
```

Webhookプロファイルを使用してポリシーを更新する

Webhookプロファイルを使用してポリシーを更新するには、次のPowerShellコマンドのサンプルを使用できます。

```
$Policy = Set-MonitorNotificationPolicy -Uid 1 -WebhookProfileId 1
```

ポリシーからWebhookマッピングを削除する

ポリシーからWebhookプロファイルを削除するには、次のPowerShellコマンドのサンプルを使用できます。

```
$Policy = Set-MonitorNotificationPolicy -Uid 1 -WebhookProfileId 0
```

Webhookプロファイルをテストする

Webhookプロファイルをテストするには、次のPowerShellコマンドのサンプルを使用できます。

```
$headers = [System.Collections.Generic.Dictionary[string,string]]::new()



$headers.Add("Content-Type", "application/json")



$headers.Add("Authorization", "Basic <Fill this with authorization
token>")



$payloads = '{ "text": "$PAYLOAD" }'



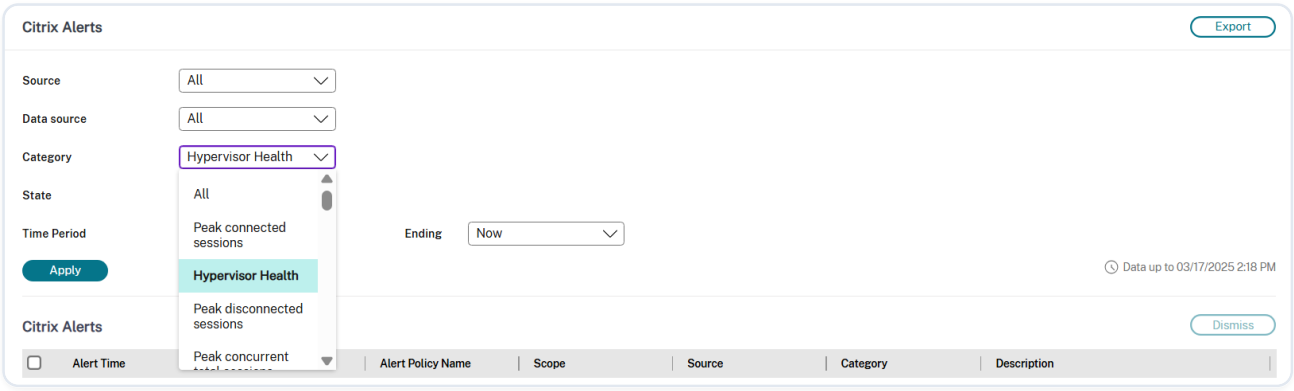
$url ="<Fill this field with the required URL>"



Test-MonitorWebhookProfile -Url $url -Headers $headers -PayloadFormat
$payloads
```

ハイパーバイザーアラートの監視

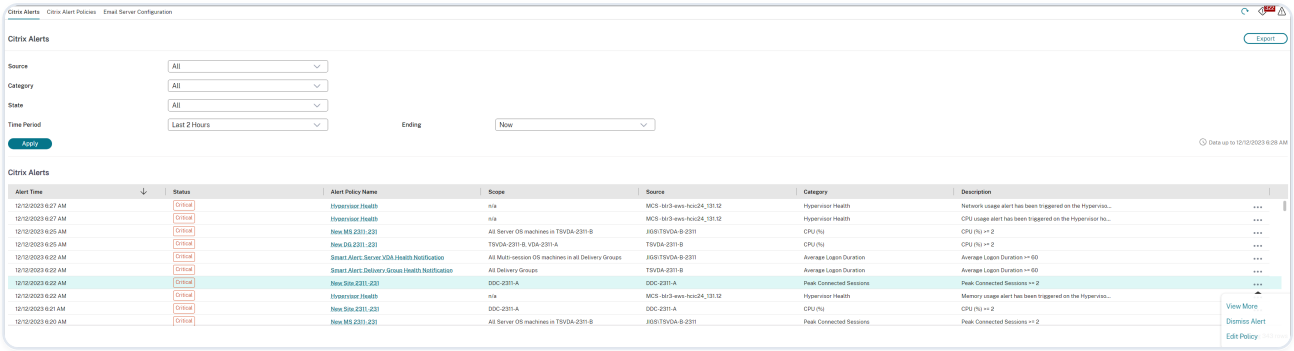
Directorは、ハイパーバイザーの健全性を監視するためのアラートを表示します。XenServer®およびVMware vSphereからのアラートは、ハイパーバイザーのパラメーターと状態の監視に役立ちます。ハイパーバイザーへの接続ステータスも監視され、ホストのクラスターまたはプールが再起動されたり、利用できなくなったりした場合にアラートが提供されます。



ハイパーバイザーアラートを受信するには、Web Studioでホスティング接続が作成されていることを確認してください。詳細については、「接続とリソース」を参照してください。ハイパーバイザーアラートの監視対象となるのは、これらの接続のみです。

これらのアラートは、しきい値に達するか、それを超えると表示されます。ハイパーバイザーアラートには次のものがあります。

- 重大 — ハイパーバイザーアラームポリシーの重大なしきい値に達したか、超えた場合
- 警告 — ハイパーバイザーアラームポリシーの警告しきい値に達したか、超えた場合
- 却下済み — アクティブなアラートとして表示されなくなったアラート



この機能には、Delivery Controllerバージョン7 1811以降が必要です。サイト7 1811以降で古いバージョンのDirectorを使用している場合、ハイパーバイザーアラートの数のみが表示されます。アラートを表示するには、Directorをアップグレードする必要があります。

次の表は、ハイパーバイザーアラートのさまざまなパラメーターと状態について説明しています。

アラート	サポートされているハイパーバイザー	トリガー元	条件	構成
CPU使用率	ゼノサーバー、ヴイエムウェア ブイスフィア	ハイパーバイザー	CPU使用率アラートのしきい値に達したか、超えた場合	アラートのしきい値はハイパーバイザーで構成

アラート	サポートされているハイパーバイザー	トリガー元	条件	構成
				する必要があります。
メモリ使用量	ゼノサーバー、ヴイエムウェア ブイスフィア	ハイパーバイザー	メモリ使用量アラートしきい値に達したか、超過しました	アラートのしきい値はハイパーバイザーで構成する必要があります。
ネットワーク使用量	ゼノサーバー、ヴイエムウェア ブイスフィア	ハイパーバイザー	ネットワーク使用量アラートしきい値に達したか、超過しました	アラートのしきい値はハイパーバイザーで構成する必要があります。
ディスク使用量	ヴイエムウェア ブイスフィア	ハイパーバイザー	ディスク使用量アラートしきい値に達したか、超過しました	アラートのしきい値はハイパーバイザーで構成する必要があります。
ホスト接続または電源状態	ヴイエムウェア ブイスフィア	ハイパーバイザー	ハイパーバイザーホストが再起動されたか、利用できません	アラートはVMware vSphereにプリビルドされています。追加の構成は不要です。
ハイパーバイザー接続が利用できません	ゼノサーバー、ヴイエムウェア ブイスフィア	デリバリーコントローラー	ハイパーバイザー（プールまたはクラスター）への接続が失われたか、電源がオフになったか、再起動されました。このアラートは、接続が利用できない間、1	アラートはDelivery Controllerにプリビルドされています。追加の構成は不要です。

アラート	サポートされているハイパーバイザー	トリガー元	条件	構成
			時間ごとに生成されます。	

注:

アラートの構成の詳細については、Citrix XenCenter Alerts を参照するか、VMware vCenter Alertsのドキュメントを確認してください。

メール通知設定は、**Citrix Alerts Policy > Site Policy > Hypervisor Health**で構成できます。ハイパーバイザーアラートポリシーのしきい値条件は、Directorからではなく、ハイパーバイザーからのみ構成、編集、無効化、または削除できます。ただし、メール設定の変更やアラートの解除はDirectorで行うことができます。インフラストラクチャの監視が役割に含まれていない場合は、アラートを無効にできます。

重要:

- ハイパーバイザーによってトリガーされたアラートは、Directorで取得および表示されます。ただし、ハイパーバイザーアラートのライフサイクル/状態の変更はDirectorには反映されません。
- ハイパーバイザーコンソールで正常、解除済み、または無効になっているアラートは、Directorに表示され続け、明示的に解除する必要があります。
- Directorで解除されたアラートは、ハイパーバイザーコンソールでは自動的に解除されません。

垂直および水平ロードバランシングアラートの処理の改善

以前は、`UseVerticalScalingForRdsLaunches`をtrueに設定し、Studioで「最大セッション数」ポリシーを構成すると、マシンは「最大容量」状態に移行しました。Directorは、制限が垂直ロードバランシングまたは水平ロードバランシングのいずれかによって達したかどうかにかかわらず、「最大容量」のアラートをトリガーしました。「最大負荷に達しました」などの特定のエラーが発生した場合、垂直ロードバランシングと水平ロードバランシングを区別する方法はありません

でした。これにより、垂直スケーリングシナリオにおける予期される動作に対して不要なアラートが発生し、時間と混乱を招いていました。

現在、垂直ロードバランシングがアクティブでマシンがセッション制限に達すると、「垂直スケーリングの最大容量」という新しい状態に移行します。Directorはこの新しい状態に対してアラートを生成しなくなりました。アラートは、水平スケーリングシナリオにおける「最大容量」に対してのみトリガーされます。新しい状態は、フィルターおよびカスタムレポートページで表示でき、これにより、予期される状態と例外的な状態を区別しやすくなります。この機能強化により、不要なアラートを回避し、実際の問題に集中できるようになり、監視とトラブルシューティングが効率化されます。これは、Set-BrokerSiteを使用して`UseVerticalScalingForRdsLaunches`を構成し、Studioで「最大セッション数」ポリシーを設定した場合に適用されます。

アプリケーション使用状況の監視

Citrix Directorは、以下の使用状況を監視するのに役立ちます。

- 仮想デスクトップセッション内で起動されたアプリケーション（ローカルアプリケーションとも呼ばれます）
- Citrix Workspace™アプリセッションから直接起動されたアプリケーション（公開アプリケーションとも呼ばれます）

アプリケーション使用状況レポートは、最も使用されているアプリケーション、ほとんど使用されていないアプリケーション、および使用されていないアプリケーションを可視化します。最も使用されているアプリケーションはダッシュボードに表示され、厳選されたグラフが含まれています。これらのグラフは、IT管理者またはアプリケーション管理者が、どのアプリケーションが頻繁に使用されているか、およびその使用状況の程度を把握するのに役立ちます。

> **注:**
>
> - この機能は、プラチナライセンスサイトでのみ利用できます。
> - ローカルアプリケーションの使用状況を監視するには、uberAgentをDirectorと統合する必要があります。詳細については、「Citrix uberAgentとDirectorの統合」を参照してください。
> - 環境で同じアプリケーションが公開アプリとデスクトップ内にインストールされたアプリ（ローカルアプリ）の両方として提供されている場合、そのアプリが公開アプリレポートとローカルアプリレポートの両方に表示されることがあります。

> この機能を使用すると、管理者はどのローカルアプリケーションと公開アプリケーションが最も使用されているかを確認できます。このデータを使用して、管理者は使用状況の程度をさらに深く掘り下げることができます。管理者は、過去24時間の人気アプリの詳細を次のデータポイントで分析できます。

- アプリケーションの総数 - 企業のサイト内のすべてのユーザーが使用しているアプリケーションの総数を特定します。
- ユニークユーザー数による最も使用されているアプリケーション - ユニークユーザーの総数に基づいて上位10のアプリを特定します。
- アプリケーション起動回数による最も使用されているアプリケーション - アプリケーション起動の総数に基づいて上位10のアプリを特定します。
- ピーク時の同時実行アプリインスタンス数 - 各アプリケーションの使用状況における同時インスタンスの最大数に基づいて上位10のアプリを特定します。この情報は、リストされているアプリケーションの最大需要を示します。

このグラフはダッシュボードページの下部に表示されます。ただし、画面上部の をクリックすると、グラフに直接アクセスできます。

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

をクリックして、単一のアプリの詳細を表示することもできます。このリンクをクリックすると、> > ページが開きます。

このグラフは、アプリの使用状況を視覚的に表現します。また、グラフにカーソルを合わせると、選択したデータポイントの絶対数が表示されます。グラフ上の任意のデータポイントをクリックすると、特定のアプリ名が選択された状態で > > ページが開きます。このデータは、企業システム内のすべてのアプリに対する比較値を示すものです。データポイントの絶対値も、同じホバー内に別途記載されます。

使用頻度の低いアプリと未使用アプリのレポート

大規模なCitrix Virtual Apps and Desktops™環境では、多くの利用率の低いアプリケーションが存在することがよくあります。環境を最適化するために、**アプリケーション**ページでは、組織内のアプリケーション使用パターンを理解し、リソース割り当てとコスト削減を改善するためのデータに基づいた意思決定を行うのに役立つ追加のメトリックが提供されるようになりました。

主な機能

- **詳細な使用状況情報:** 個別のユーザー数（過去30日間）、合計起動回数、ピーク時の同時実行インスタンス数、および各アプリケーションの経時的な個別のユーザー数の傾向グラフを表示します。
- **データに焦点を当てる:** アプリケーションの必要性を評価するために、過去7日間、30日間、または90日間のアプリケーション使用パターンを分析します。90日間のデータを表示することをお勧めします。これは四半期分のデータを提供し、アプリケーションの使用状況が変動するか、一貫しているかを観察できるためです。X軸上の日付は、組織のイベントと使用傾向を関連付け、使用量の減少が予測されたものかどうかを判断するのに役立ちます。このデータにより、管理者は不要なアプリケーションを排除することで、効率的な環境を維持できます。
- **最適化:** 公開されているアプリケーションの総数、使用頻度の低いアプリケーション、および未使用のアプリケーションを特定し、Citrix展開を最適化します。
- **実用的なデータ:** アプリケーション管理を支援するデータに基づいた意思決定を行い、リソース割り当てとライセンス管理を最適化します。
- **データのエクスポート:** 詳細な分析のために、データをPDFまたはCSV形式でエクスポートします。アプリケーションの使用状況を使用して、Power BI統合またはODATAクエリを使用してデータをエクスポートすることもできます。

要件

- Delivery Controller バージョン 7.16 以降
- VDA バージョン 7.15 以降

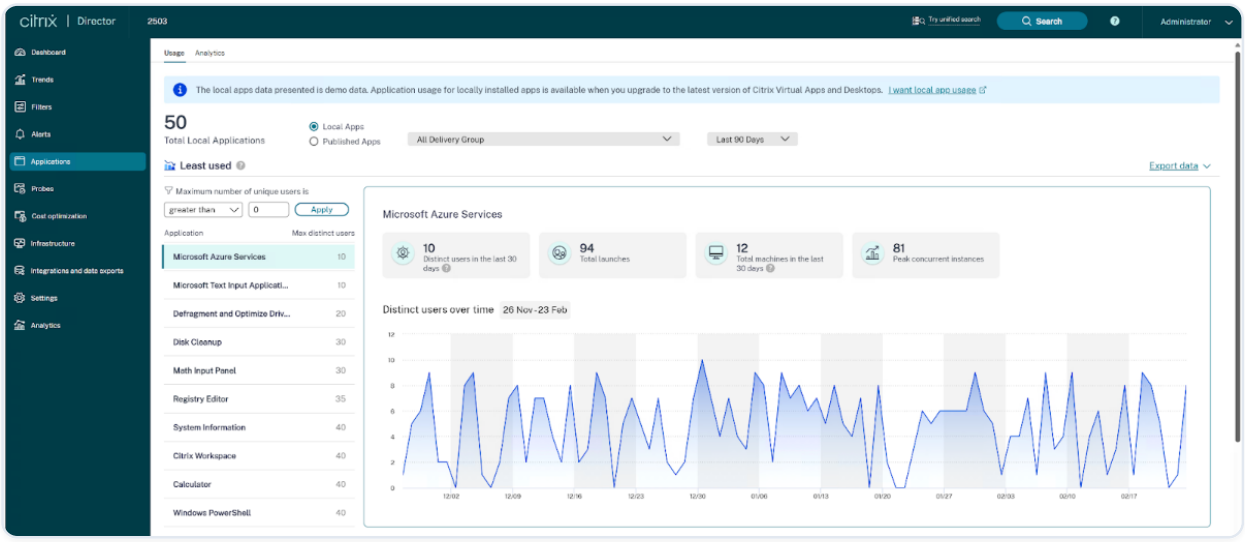
アプリケーション使用状況の詳細の表示

1. ダッシュボードの**使用頻度の低いアプリのレビュー**セクションにある**アプリの表示**リンクをクリックします。

   または、,

   アプリケーションタブをクリックします。次のページが表示されます。

   ローカルアプリオプションが選択されている場合:



公開済みアプリオプションが選択されている場合:

「アプリケーション」タブ(/en-us/citrix-virtual-apps-desktops/current-release/media/dir-app-analytics-published.png)

2. 目的のデリバリーグループを選択します。
3. 必要な期間を選択します。(注: 最適な分析のため、デフォルトは過去90日間です。)

次の情報が表示されます。

- **ローカルおよび公開アプリケーションの合計:** ローカルおよび公開アプリケーションの合計数が表示されます。
- **最も使用頻度の低い:** 選択した期間でユニークユーザーが最も少ないアプリが表示されます。計算は次のように行われます。

  a. **日次ユーザー数:** 各アプリのユニークユーザー数が毎日カウントされます。

  b. **日次ピーク使用量:** 各アプリの最も高い日次ユーザー数が特定されます。

  c. **全体で最も高い使用量:** 選択した期間全体で各アプリの最も高いユーザー数が決定されます。

  d. **昇順:** アプリは、全体で最も高いユーザー数に基づいて昇順でリストされ、最も低いユーザー数のアプリから始まります。

> **注:**
>
> 分析期間として過去90日間を選択することをお勧めします。この期間は四半期分のデータを提供し、アプリの使用パターンを包括的に把握できます。ただし、7日間および1か月でフィルタリングするオプションも利用できます。

- **未使用:** 過去90日間で一度も起動されていないアプリケーションがリストされます。配信されたデリバリーグループ、アプリのバージョン、および最終使用の正確なタイムスタンプが提供されます。この情報は、管理者が仮想デスクトップからアプリケーションを削除する前に、情報に基づいた意思決定を行うのに役立ちます。

  「アプリケーション」タブ - 未使用(/en-us/citrix-virtual-apps-desktops/current-release/media/dir-app-analytics-not-used.png)

4. **最も使用頻度の低い**カテゴリからアプリを選択して、以下を含む詳細な使用状況情報を表示します。

   - **過去30日間の個別ユーザー:** 過去30日間にアプリにアクセスした個別ユーザーの数が表示されます。7日間でフィルタリングした場合、このメトリックは、選択したアプリのその7日間の個別ユーザー数を表示します。

   > **注:**
   >
   > 90日を選択した場合でも、このメトリックは過去30日間のデータのみを表示します。

   - **合計起動回数:** アプリが起動された回数を表示します。
   - **過去30日間の合計マシン数**: 過去30日間にインストールされたマシンの数を表示します。このメトリックは、ローカルアプリの詳細を表示している場合にのみ表示されます。
   - **ピーク同時実行インスタンス数:** 同時に実行されているインスタンスの最大数を表示します。
   - **トレンドチャート:** 選択したアプリの経時的なユニークユーザー数を示すトレンドチャートを表示します。**詳細を表示**をクリックすると、**キャパシティ管理 > ホスト型アプリケーション使用状況**セクションで詳細情報が表示されます。

トレンドチャートの使用方法

トレンドチャートは使用パターンを示し、選択した期間における使用量の低い期間や高い期間の傾向を特定するのに役立ちます。X軸は日数を表し、Y軸は経時的なユニークユーザー数を表します。これらのメトリックと使用パターングラフを分析することで、管理者はCitrix Virtual Apps and Desktops™環境を自信を持って最適化できます。

トレンドチャートは以下の方法で使用できます。

- **データポイントにカーソルを合わせる:** 選択した期間のユニークユーザー数を表示します。

- **トレンドの表示:** 使用パターンを特定し、アプリの使用状況が一貫しているか、一時的な急増に過ぎないかを判断します。このチャートは、管理者が従業員の活動を監視し、潜在的な問題や改善領域を特定するのに役立ちます。たとえば、従業員が休暇を取ると、その期間はアプリケーションの使用がない場合があります。従業員が戻ると、アプリケーションの使用が増加します。期間のデフォルトフィルターは90日で、管理者がこれらの計算を行うのに役立ちます。
- **詳細を表示:** 日付と対応するユニークユーザー数を表示します。
- **フィルターオプション:** 異なる期間フィルターオプションを選択して、対応するデータを表示します。

障害のトラブルシューティングのためにデータをフィルタリングする

ダッシュボードの数値をクリックするか、フィルターメニューから事前定義されたフィルターを選択すると、選択したマシンまたは障害タイプに基づいてデータを表示するフィルタービューが開きます。

事前定義されたフィルターは編集できませんが、事前定義されたフィルターをカスタムフィルターとして保存し、後で変更できます。また、すべてのデリバリーグループにわたるマシン、接続、セッション、およびアプリケーションインスタンスのカスタムフィルタービューを作成できます。

1. ビューを選択します。

    - **マシン**。シングルセッションOSマシンまたはマルチセッションOSマシンを選択します。これらのビューには、構成されたマシンの数が表示されます。マルチセッションOSマシンのタブには、ロード評価インデックスも含まれており、これはパフォーマンスカウンターの分布と、リンクにカーソルを合わせると表示されるセッション数のツールヒントを示します。
    - **セッション**。セッションを、過去60分、過去24時間、過去7日間、またはカスタム期間を含む異なる期間でフィルターします。セッションビューからセッション数を確認することもできます。アイドル時間測定を使用して、しきい値期間を超えてアイドル状態のセッションを特定します。**関連ユーザー**をクリックすると、そのユーザーのアクティビティマネージャーが開きます。**エンドポイント**名をクリックすると、そのエンドポイントのアクティビティマネージャーが開きます。**詳細表示**をクリックすると、それぞれ**ユーザー詳細**または**エンドポイント詳細**ページが開きます。詳細については、「ユーザー詳細」を参照してください。
    - **接続**。接続を、過去60分、過去24時間、過去7日間、またはカスタム期間を含む異なる期間でフィルターします。
    - **アプリケーションインスタンス**。アプリケーションインスタンスを、過去60分、過去24時間、過去7日間、またはカスタム期間を含む異なる期間でフィルターします。このビューに

は、サーバーおよびシングルセッションOSのVDA上のすべてのアプリケーションインスタンスのプロパティが表示されます。セッションアイドル時間測定は、マルチセッションOSのVDA上のアプリケーションインスタンスで利用できます。

> **注:**
>
> Windows 10 1809コンピューターにインストールされたVDAでデスクトップセッションを起動した場合、Directorのアクティビティマネージャーでは、Microsoft EdgeとOfficeがアクティブに実行されているアプリケーションとして表示されることがありますが、実際にはバックグラウンドでのみ実行されています。

2. **フィルター条件**で、基準を選択します。
3. 必要に応じて、各ビューの追加タブを使用してフィルターを完了します。
4. 必要に応じて、追加の列を選択してさらにトラブルシューティングを行います。
5. フィルターを保存して名前を付けます。
6. 複数のDirectorサーバーからフィルターにアクセスするには、それらのサーバーからアクセス可能な共有フォルダーにフィルターを保存します。
   - 共有フォルダーには、Directorサーバー上のアカウントに対する変更権限が必要です。
   - Directorサーバーは、共有フォルダーにアクセスするように構成する必要があります。構成するには、**IIS Manager**を実行します。**サイト > Default Web Site > Director > アプリケーション設定**で、**Service.UserSettingsPath**設定を共有フォルダーのUNCパスを反映するように変更します。
7. 後でフィルターを開くには、**フィルター**メニューからフィルタータイプ（マシン、セッション、接続、またはアプリケーションインスタンス）を選択し、保存されたフィルターを選択します。
8. **エクスポート**をクリックして、データをCSV形式ファイルにエクスポートします。最大100,000レコードのデータをエクスポートできます。この機能は、Delivery Controller™バージョン1808以降で利用可能です。
9. 必要に応じて、**マシン**または**接続**ビューでは、フィルターされたリストで選択したすべてのマシンに対して電源コントロールを使用します。セッションビューでは、セッションコントロールまたはメッセージ送信オプションを使用します。
10. 必要に応じて、複数のアクションを使用できます。アクションの進行状況を示すプログレスバーが表示されます。また、アクションが完了するとメッセージが表示されます。

11. 「**マシン**」ビューと「**接続**」ビューで、失敗したマシンまたは接続の「**障害理由**」をクリックすると、障害の詳細な説明と、障害のトラブルシューティングに推奨されるアクションが表示されます。マシンおよび接続の障害理由と推奨されるアクションについては、Citrix Director の障害理由とトラブルシューティングを参照してください。
12. **マシン**ビューで、マシン名リンクをクリックすると、対応する**マシン詳細**ページに移動します。このページには、マシンの詳細が表示され、電源コントロールが提供され、CPU、メモリ、ディスク監視、および GPU 監視グラフが表示されます。また、**履歴使用率の表示**をクリックすると、マシンのリソース使用率の傾向を確認できます。詳細については、マシンのトラブルシューティングを参照してください。
13. 「**アプリケーションインスタンス**」ビューで、閾値期間より長い「**アイドル時間**」に基づいて並べ替えまたはフィルター処理を行います。終了するアイドル状態のアプリケーションインスタンスを選択します。アプリケーションインスタンスのログオフまたは切断により、同じセッション内のすべてのアクティブなアプリケーションインスタンスが終了します。詳細については、アプリケーションのトラブルシューティングを参照してください。「アプリケーションインスタンス」フィルターページと「セッション」フィルターページでのアイドル時間測定は、Director、Delivery Controller、およびVDAがバージョン7.13以降の場合に利用できます。

注:

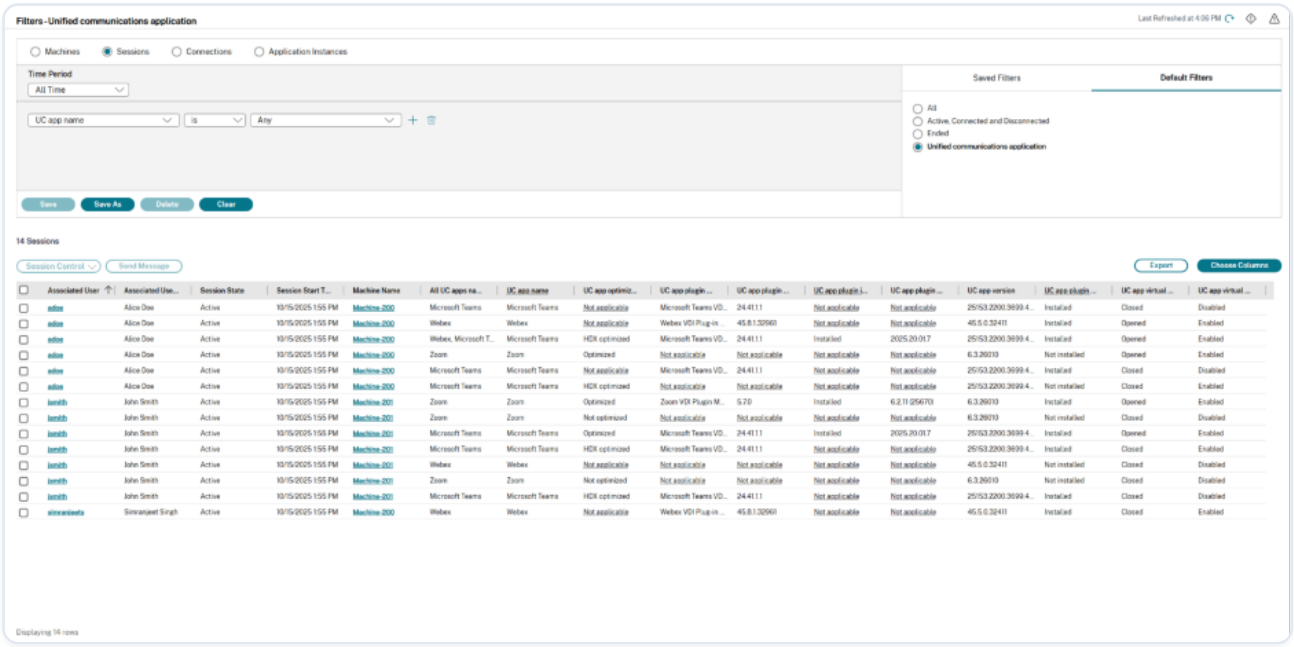
Web Studioでは、デリバリーグループ内の単一のVDAに、異なるユーザーまたはユーザーグループに対して複数のデスクトップ割り当てルール（DAR）を割り当てることができます。StoreFront™は、ログインしているユーザーに対して、DARに従って対応する表示名で割り当てられたデスクトップを表示します。しかし、DirectorはDARをサポートしておらず、ログインしているユーザーに関係なく、デリバリーグループ名を使用して割り当てられたデスクトップを表示します。その結果、Directorで特定のデスクトップをマシンにマッピングすることはできません。StoreFrontに表示される割り当てられたデスクトップをDirectorに表示されるデリバリーグループ名にマッピングするには、次のPowerShellコマンドを使用します。

```
Get-BrokerDesktopGroup | Where-Object { $_.Uid -eq (Get-
BrokerAssignmentPolicyRule | Where-Object { $_.PublishedName -eq "<Name on
StoreFront>" }).DesktopGroupUid } | Select-Object -Property Name, Uid
```

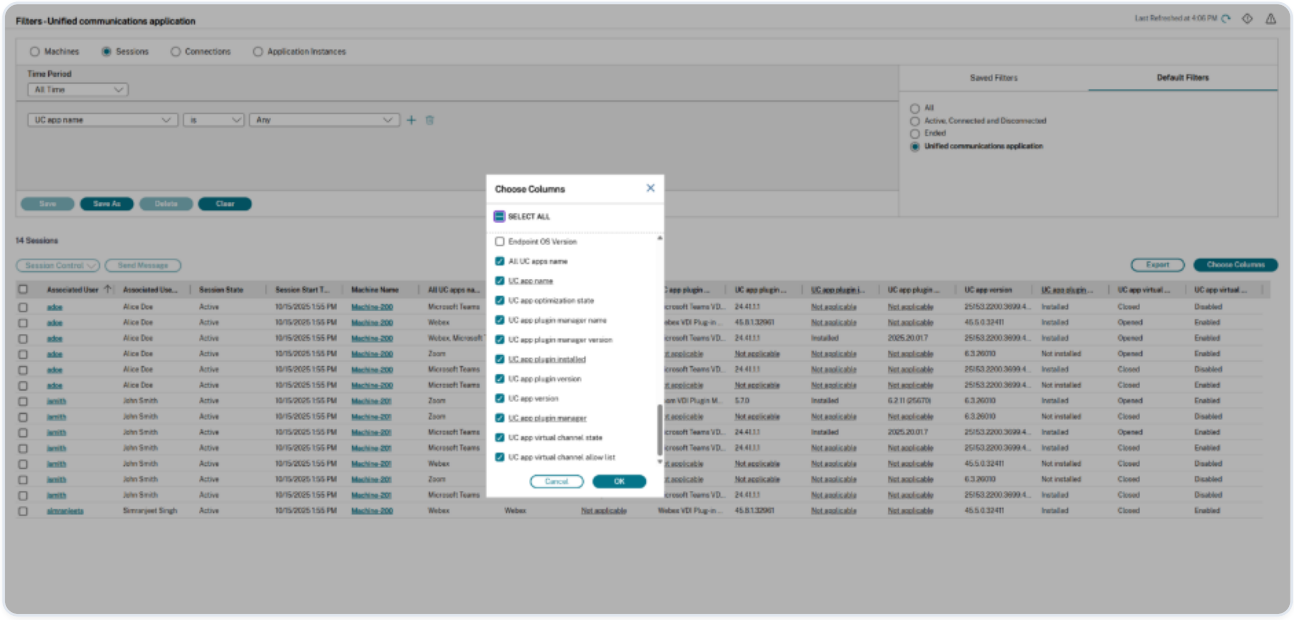
ユニファイドコミュニケーションアプリのメトリック

「セッション」ビューには、ユーザーセッションにおけるユニファイドコミュニケーション（UC）アプリケーションの使用状況に関する詳細な洞察を提供する、いくつかの新しい表示列が含まれるようになりました。これらのメトリックは、セッションのリストを絞り込むためのフィルターで利用でき、メインのセッションテーブルビューに表示するために、「**列の選択**」オプションを介して選択することもできます。

- **All UC apps name (Column Only):** セッションで同時に実行されていたすべての複数のUCアプリケーションのデータリストが含まれます。これは表示列であり、フィルターオプションではありません。
- **UC app name:** 特定のユニファイドコミュニケーションアプリケーションの名前（例：Microsoft Teams、Webex、Zoom）。
- **UC app optimization state:** セッション内のUCアプリケーションの最適化ステータス（例：最適化済み、HDX最適化済み、最適化されていません、該当なし）。
- **UC app plugin manager name:** UCアプリケーションに使用されるプラグインマネージャーの名前。
- **UC app plugin manager version:** 使用されているプラグインマネージャーのバージョン。
- **UC app plugin installed:** UCアプリケーションに必要なアプリケーションプラグインがインストールされているか、インストールされていないかを示します。
- **UC app plugin version:** 特定のUCアプリケーションプラグインのバージョン。
- **UC app version:** ユニファイドコミュニケーションアプリケーションの全体的なバージョン。
- **UC app plugin manager:** UCアプリケーションに必要なアプリケーションプラグインマネージャーがエンドポイントにインストールされているか、インストールされていないかを示します。
- **UC app virtual channel state:** UCアプリケーション用に確立された仮想チャネルのステータス（例：Opened、Closed）。
- **UC app virtual channel allow list:** アプリケーションの仮想チャネルが許可リストにあるかどうかを示します。



UCアプリメトリクス 2(/en-us/citrix-virtual-apps-desktops/current-release/media/uc-app-metrics-2.png)



サイト全体の履歴トレンドを監視する

トレンドビューは、以下のパラメータについて、各サイトの履歴トレンド情報にアクセスします。

- セッション
- 接続障害
- マシン障害
- ログオンパフォーマンス
- 負荷評価

- キャパシティ管理
- マシン使用状況
- リソース使用率
- 各サイトのネットワーク分析。

この情報を見つけるには、**トレンド**メニューをクリックします。

ズームイン ドリルダウン機能を使用すると、期間をズームイン（グラフのデータポイントをクリック）し、トレンドに関連する詳細を表示するためにドリルダウンすることで、トレンドグラフをナビゲートできます。この機能により、誰が、または何が影響を受けているかの詳細をよりよく理解できます。

各グラフのデフォルトのスコープを変更するには、データに別のフィルターを適用します。

履歴トレンド情報が必要な期間を選択してください。期間の利用可能性は、Directorの展開によって次のように異なります。

- Premiumライセンスサイトでは、最大1年間 (365日) のトレンドレポートを利用できます。
- Advancedライセンスサイトでは、最大1か月間 (31日) のトレンドレポートを利用できます。
- PremiumおよびAdvanced以外のライセンスサイトでは、最大7日間のトレンドレポートを利用できます。

注:

- すべてのDirector展開において、期間が「先月」（**現在まで**）以下に設定されている場合、セッション、障害、ログオンパフォーマンスのトレンド情報はグラフとテーブルとして利用できます。期間がカスタム終了日を指定した「先月」または「昨年」として選択されている場合、トレンド情報はグラフとして利用でき、テーブルとしては利用できません。
- Monitor Serviceのグルーミング保持値によって、トレンドデータの可用性が制御されます。デフォルト値は、データ粒度と保持で確認できます。Premiumライセンスサイトのお客様は、グルーミング保持を希望する保持日数に変更できます。
- IIS Managerの以下のパラメータは、選択可能なカスタム終了日の範囲を制御します。ただし、選択された日付のデータ可用性は、測定される特定のメトリックのグルーミング保持設定によって異なります。

パラメーター	デフォルト値
UI.TrendsLast2HoursRange	3
UI.TrendsLast24HoursRange	32
UI.TrendsLast7DaysRange	32
UI.TrendsLastMonthRange	365

利用可能なトレンド

セッションの傾向を表示: 「**セッション**」タブから、デリバリーグループと期間を選択して、同時セッション数に関する詳細情報を表示します。

「**セッションの自動再接続**」列には、セッション内の自動再接続の数が表示されます。自動再接続は、セッションの信頼性ポリシーまたはクライアント自動再接続ポリシーが有効な場合に有効になります。エンドポイントでネットワークの中断が発生した場合、次のポリシーが有効になります。

- セッションの信頼性が有効になり（デフォルトで3分間）、Citrix Receiver™またはCitrix Workspace™アプリがVDAへの接続を試行します。
- クライアント自動再接続が3分から5分の間に有効になり、クライアントがVDAへの接続を試行します。

両方の再接続がキャプチャされ、ユーザーに表示されます。この情報は、再接続が発生してからDirector UIに表示されるまでに最大5分かかる場合があります。

自動再接続情報は、中断のあるネットワーク接続の表示とトラブルシューティングに役立ちます。また、シームレスなエクスペリエンスを持つネットワークも分析します。フィルターで選択した特定のデリバリーグループまたは期間の再接続数を表示できます。ドリルダウンでは、セッションの信頼性やクライアント自動再接続、タイムスタンプ、エンドポイントIP、Workspaceアプリがインストールされているマシンのエンドポイント名などの追加情報が提供されます。

デフォルトでは、ログはイベントのタイムスタンプの降順でソートされます。この機能は、Windows用Citrix Workspaceアプリ、Mac用Citrix Workspaceアプリ、Windows用Citrix Receiver、およびMac用Citrix Receiverで利用できます。この機能には、Delivery Controller™バージョン7 1906以降、およびVDA 1906以降が必要です。

セッションの再接続の詳細については、「セッション」を参照してください。

ポリシーの詳細については、「クライアント自動再接続ポリシー設定」および「セッションの信頼性ポリシー設定」を参照してください。

自動再接続データがDirectorに表示されない場合があります。その理由は次のとおりです。

- WorkspaceアプリがVDAに自動再接続データを送信していません。
- VDAがモニターサービスにデータを送信していません。
- Delivery Controllerは、対応するセッションがない可能性があるため、VDAペイロードを破棄します。

> **注:**
>
> 特定のCitrix Gatewayポリシーが設定されている場合、クライアントIPアドレスが正しく取得されないことがあります。

> **接続障害の傾向を表示:** 「障害」タブから、接続、マシンタイプ、障害タイプ、デリバリーグループ、および期間を選択して、サイト全体のユーザー接続障害に関する詳細情報を含むグラフを表示します。

マシン障害の傾向を表示: Single-session OS Machine FailuresタブまたはMulti-session OS Machinesタブから、障害タイプ、デリバリーグループ、および期間を選択すると、サイト全体のマシン障害に関する詳細情報を含むグラフが表示されます。

ログオンと再接続のパフォーマンスの傾向を表示: Logon and Reconnect Performanceタブから、デリバリーグループと期間を選択すると、ユーザーのログオンと再接続の期間に関する詳細情報を含むグラフがサイト全体に表示されます。このビューは、ログオンまたは再接続の数と全体的なパフォーマンスを理解するのに役立ちます。

グラフには以下が含まれます。

- **ログオンイベント、ログオン期間、およびフェーズ**（ブローカー処理、対話型セッションなど）。新しいセッションを起動する際のユーザーエクスペリエンスに関する洞察を提供します。
- **再接続イベントと再接続期間**。切断されたセッションから再接続する際のユーザーエクスペリエンスに関する洞察を提供します。

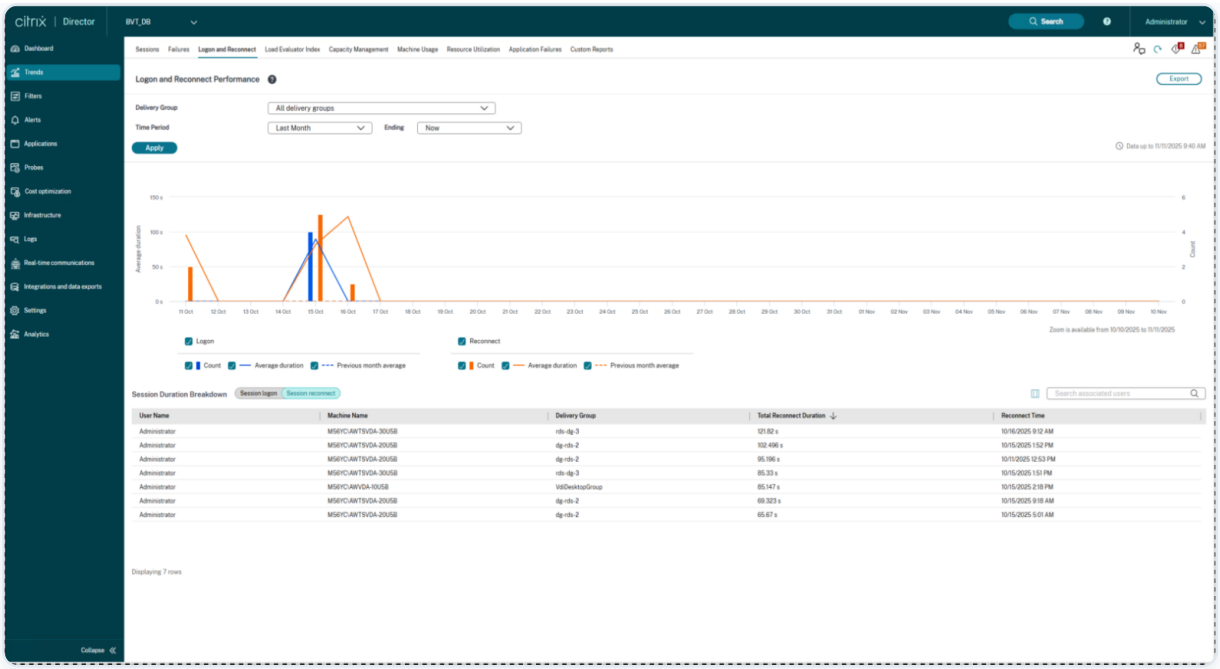
凡例を使用して、分析対象の傾向に基づいて必要なメトリックを選択します。

- カウント

- 平均期間
- 以前の（期間）平均

グラフの下の表には、ユーザーセッションまたは接続ごとの**セッションログオン**と**セッション再接続**の詳細が表示されます。表の上にある選択肢を使用してメトリックを切り替えたり、表示する列を選択したり、任意の列で並べ替えたり、レポートをPDF、Excel、またはCSV形式でエクスポートしたりできます。

> **注:**
>
> セッション再接続期間は、**DirectorおよびVDAバージョン2511 CR以降**でサポートされています。



負荷評価の傾向を表示: Load Evaluator Indexタブから、Multi-session OSマシン間で分散される負荷に関する詳細情報を含むグラフを表示します。このグラフのフィルターオプションには、デリバリーグループまたはデリバリーグループ内のMulti-session OSマシン、Multi-session OSマシン（デリバリーグループ内のMulti-session OSマシンが選択されている場合にのみ利用可能）、および範囲が含まれます。

ホストされたアプリケーションの使用状況を表示: この機能の利用可能性は、組織のライセンスによって異なります。 **Capacity Management**タブから、**Hosted Applications Usage**タブを選択します。デリバリーグループと期間を選択すると、ピーク時の同時使用状況を示すグラフと、アプリケーションベースの使用状況を示す表が表示されます。Application Based Usage表から、特定の

アプリケーションを選択して詳細と、そのアプリケーションを使用している、または使用したユーザーのリストを確認できます。

Single-sessionおよびMulti-session OSの使用状況を表示: トレンドビューには、サイト別およびデリバリーグループ別のSingle-session OSの使用状況が表示されます。**サイト**を選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、ユーザーごとの使用状況が表示されます。 トレンドビューには、サイト別、デリバリーグループ別、およびマシン別のMulti-session OSの使用状況も表示されます。**サイト**を選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、マシンごとおよびユーザーごとの使用状況が表示されます。マシンが選択されている場合は、ユーザーごとの使用状況が表示されます。

仮想マシンの使用状況を表示: マシン使用状況タブから、**シングルセッションOSマシンまたはマルチセッションOSマシン**を選択すると、VMの使用状況をリアルタイムで確認でき、サイトのキャパシティニーズを迅速に評価できます。 シングルセッションOSの可用性 - サイト全体または特定のデリバリーグループにおけるシングルセッションOSマシン（VDI）の可用性による現在の状態を表示します。 マルチセッションOSの可用性 - サイト全体または特定のデリバリーグループにおけるマルチセッションOSマシンの可用性による現在の状態を表示します。

コスト最適化によるマシン使用状況の可視性を高めるには、表示されるバナーの以下のリンクをクリックします。

- 推定節約額 - このリンクをクリックすると、**コスト最適化**ページの**推定節約額**セクションに移動し、すべてのデリバリーグループの詳細が表示されます。
- 節約レポート - このリンクをクリックすると、**コスト最適化**ページの**節約レポート**セクションに移動し、すべてのデリバリーグループの詳細が表示されます。

> **注:**
>
> 利用可能カウンターに表示されるマシンの数には、メンテナンスモードのマシンが含まれます。

> **リソース使用率の表示: リソース使用率**タブから、**シングルセッションOSマシンまたはマルチセッションOSマシン**を選択すると、CPUおよびメモリ使用量、IOPS、各VDIマシンのディスク待機時間に関する履歴トレンドデータを確認でき、より適切なキャパシティプランニングに役立ちます。 この機能には、Delivery ControllerおよびVDAの**バージョン7.11**以降が必要です。 グラフには、平均CPU、平均メモリ、平均IOPS、ディスク待機時間、ピーク時

の同時セッションのデータが表示されます。マシンにドリルダウンして、CPUを消費している上位10個のプロセスのデータとグラフを表示できます。

デリバリーグループと期間でフィルタリングします。CPU、メモリ使用量、およびピーク時の同時セッションのグラフは、過去2時間、24時間、7日間、1か月、1年間で利用できます。平均IOPSとディスク待機時間のグラフは、過去24時間、1か月、1年間で利用できます。バナーの**確認**リンクをクリックすると、コスト最適化によるマシン使用状況の可視性を高めることができます。このリンクをクリックすると、**コスト最適化**ページの**ワークロードの適正化**タブに移動し、**リソース使用率**タブから選択したデリバリーグループの詳細が表示されます。

注:

- 履歴マシン使用率ページの「上位10プロセス」テーブルでデータを収集して表示するには、監視ポリシー設定の**プロセス監視を有効にする**を**許可**に設定する必要があります。このポリシーは、デフォルトで**禁止**に設定されています。すべてのリソース使用率データはデフォルトで収集されます。これは、**リソース監視を有効にする**ポリシー設定を使用して無効にできます。グラフの下のテーブルには、マシンごとのリソース使用率データが表示されます。詳細については、「監視ポリシー設定」を参照してください。
- 平均IOPSは日次平均を示します。ピークIOPSは、選択した期間のIOPS平均の最高値として計算されます。（IOPS平均とは、VDAで1時間中に収集されたIOPSの時間平均です）。
- マシンのドリルダウンでは、平均CPUまたは平均メモリ使用量が1%を超えるプロセスが一覧表示されます。これは、場合によっては10個未満のプロセスしか表示されない可能性があることを意味します。

ネットワーク分析データの表示: この機能の可用性は、組織のライセンスと管理者権限によって異なります。この機能には、Delivery Controllerの**バージョン7.11**以降が必要です。

ネットワークタブから、ネットワーク分析を監視します。これにより、ネットワークのユーザー、アプリケーション、デスクトップのコンテキストビューが提供されます。この機能により、DirectorはCitrix ADMからのHDX Insightレポートを通じて、展開におけるICAトラフィックの高度な分析を提供します。詳細については、「ネットワーク分析の構成」を参照してください。

アプリケーション障害の表示: アプリケーション障害タブには、VDA上の公開アプリケーションに関連する障害が表示されます。

この機能には、Delivery ControllerおよびVDAの**バージョン7.15**以降が必要です。Windows Vista以降を実行するシングルセッションOS VDA、およびWindows Server 2008以降を実行するマルチセッションOS VDAがサポートされています。 詳細については、「履歴アプリケーション障害監視」を参照してください。

デフォルトでは、マルチセッションOS VDAからのアプリケーション障害のみが表示されます。監視ポリシーを使用して、アプリケーション障害の監視を設定できます。詳細については、「監視ポリシー設定」を参照してください。

プローブ結果の表示: プローブ結果タブには、構成ページでプローブ用に構成されたアプリケーションおよびデスクトップのプローブ結果が表示されます。ここでは、障害が発生した起動の段階が記録されます。

詳しくは、「アプリケーションおよびデスクトップのプローブ」を参照してください。

カスタマイズされたレポートの作成: カスタムレポートタブは、監視データベースからリアルタイムおよび履歴データを表形式で含むカスタムレポートを生成するためのユーザーインターフェイスを提供します。

この機能には、Delivery Controllers **バージョン7.12**以降が必要です。

以前に保存したカスタムレポートクエリのリストから、**実行してダウンロード**をクリックしてレポートをCSV形式でエクスポートしたり、**ODataをコピー**をクリックして対応するODataクエリをコピーして共有したり、**編集**をクリックしてクエリを編集したりできます。 マシン、接続、セッション、またはアプリケーションインスタンスに基づいてカスタムレポートクエリを作成できます。マシン、デリバリーグループ、期間などのフィールドに基づいてフィルター条件を指定します。カスタムレポートに必要な追加の列を指定します。プレビューには、レポートデータのサンプルが表示されます。カスタムレポートクエリを保存すると、保存されたクエリのリストに追加されます。

コピーしたODataクエリに基づいてカスタムレポートクエリを作成できます。これを行うには、ODataクエリオプションを選択し、コピーしたODataクエリを貼り付けます。結果のクエリは後で実行するために保存できます。

> **注:**
>
> ODataクエリを使用して生成されたプレビューおよびエクスポートレポートの列名はローカライズされておらず、英語で表示されます。

グラフ上のフラグアイコンは、特定の期間における重要なイベントまたはアクションを示します。フラグにマウスを合わせ、クリックしてイベントまたはアクションを一覧表示します。

注:

- HDX™接続ログオンデータは、7より前のVDAでは収集されません。それより前のVDAの場合、グラフデータは0と表示されます。
- Citrix Studioで削除されたデリバリーグループは、関連データが整理されるまで、Director Trendsフィルターで選択可能です。削除されたデリバリーグループを選択すると、保持期間までの利用可能なデータのグラフが表示されます。ただし、テーブルにはデータは表示されません。
- アクティブなセッションを含むマシンをあるデリバリーグループから別のデリバリーグループに移動すると、新しいデリバリーグループの**リソース使用率と負荷評価インデックス**テーブルに、古いデリバリーグループと新しいデリバリーグループから統合されたメトリックが表示されます。

Autoscaleで管理されているマシンの監視

Autoscaleは、デリバリーグループ内の登録済みすべてのマルチセッションおよびシングルセッションOSマシンに対するプロアクティブな電源管理を可能にする電源管理機能です。Web Studioで、選択したデリバリーグループに対してAutoscaleを構成できます。詳しくは、「Autoscale」(/ja-jp/citrix-virtual-apps-desktops/current-release/manage-deployment/autoscale.html)を参照してください。 Directorを使用して、Autoscaleが有効なマシンの主要なメトリックを監視できます。

マシン使用状況

マシン使用状況ページには、選択したデリバリーグループと期間について、電源がオンになっているAutoscaleが有効なマルチセッションおよびシングルセッションOSマシンの合計数が表示されます。このメトリックは、デリバリーグループ内のマシンの実際の使用状況を示します。 **シングルセッションOSマシン**タブまたは**マルチセッションOSマシン**タブから、デリバリーグループと期間を選択します。

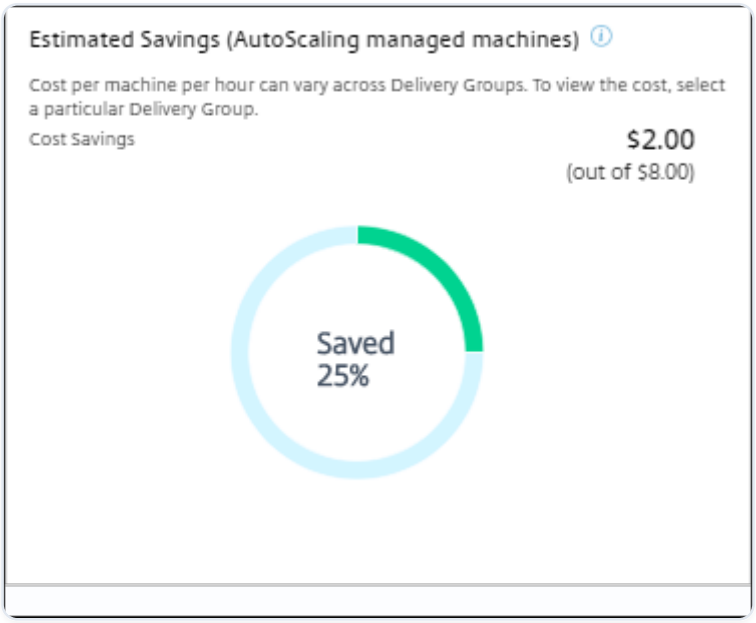
このグラフには、次のメトリックが表示されます:

- **電源オンのマシン** - 電源がオンになっているAutoscaleが有効なマシンの数
- **登録済みマシン** - 登録済みのマルチセッションまたはシングルセッションOSマシンの数

- **メンテナンス中のマシン** - メンテナンスモードがオンになっているマルチセッションまたはシングルセッションOSマシンの数

推定節約額

マシン使用状況ページには、選択したデリバリーグループでAutoscaleを有効にすることによって達成された推定コスト削減額も表示されます。



推定節約額は、**デリバリーグループの編集** > **Autoscale**で構成されている、1時間あたりのマシンごとの節約額（米ドル）の割合として計算されます。マシンごとの節約額の構成について詳しくは、「Autoscale」(/ja-jp/citrix-virtual-apps-desktops/current-release/manage-deployment/autoscale.html)を参照してください。

すべてのデリバリーグループを選択すると、すべてのデリバリーグループにおける推定節約額の平均値が表示されます。

推定節約額は、管理者が既存のインフラストラクチャを統合し、最大限の節約と利用率を達成するためのキャパシティを計画するのに役立ちます。

マシンとセッションのアラート通知

Directorダッシュボードには、アラート通知が表示されます。これらの通知はさらにドリルダウンできます。アラートの詳細は、**アラート**ページに表示されます。

- デリバリーグループでアラートポリシーを作成するには、**アラート** > **Citrixアラートポリシー** > **デリバリーグループポリシー**に移動します。
- ここでは、次の警告および重大なしきい値を設定できます。

    - 失敗したマシン（シングルセッションOS）および失敗したマシン（マルチセッションOS）、,
    - デリバリーグループ内のピーク接続セッション、ピーク切断セッション、およびピーク同時合計セッション。

- デリバリーグループ内の対応するメトリックがしきい値に達すると、アラートが生成されます。

アラートポリシーの条件と新しいアラートポリシーの作成に関する詳細については、「アラートと通知」を参照してください。

マシンのステータス

- **フィルター** > **マシン**には、すべてのマシンの電源状態が表形式で表示されます。特定のデリバリーグループでフィルターできます。
- **フィルター** > **セッション**には、マシン名でフィルターして、関連するセッションとそのリアルタイムステータスが表示されます。
- **トレンド** > **セッション**で、デリバリーグループと期間を選択すると、セッションとその関連メトリックのトレンドが表示されます。

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

負荷評価のトレンド

トレンド > **負荷評価インデックス**ページには、マルチセッションOSマシン間で分散される負荷に関する詳細情報を含むグラフが表示されます。このグラフのフィルターオプションには、デリバリーグループまたはデリバリーグループ内のマルチセッションOSマシン、マルチセッションOSマシン（デリバリーグループ内のマルチセッションOSマシンが選択されている場合にのみ利用可能）、および範囲が含まれます。負荷評価インデックスは、CPU合計、メモリ、ディスク、またはセッションの割合として表示され、最後の間隔での接続ユーザー数と比較して示されます。

リアルタイム通信ダッシュボード

監視とトラブルシューティングのための Microsoft 通話品質ダッシュボード

この機能は、Microsoft Graph API 統合を使用して、管理者に対し Microsoft Teams の通話パフォーマンスの統合ビューを提供することで、Citrix Director を強化します。これにより、集約さ

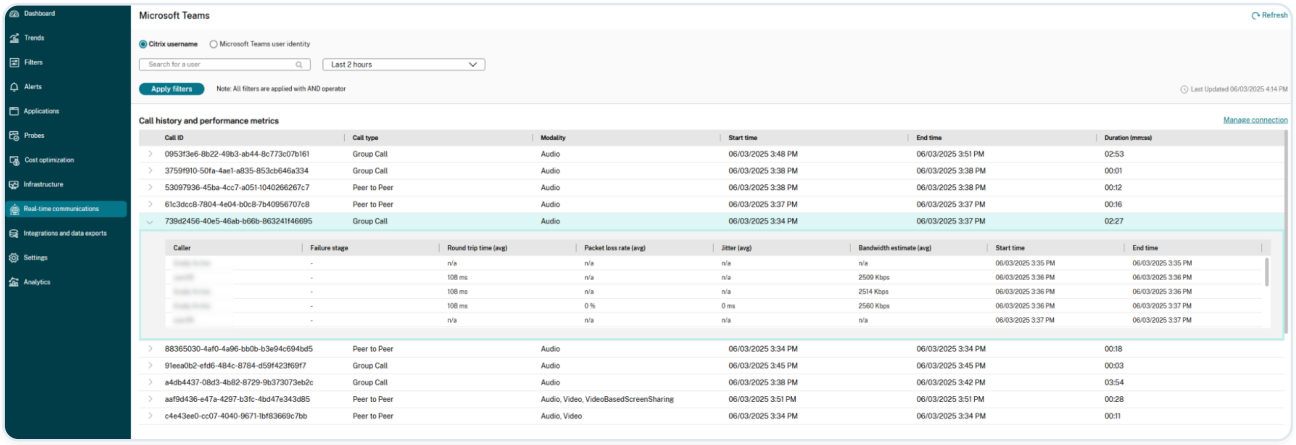
れた監視とトラブルシューティングが可能になり、Citrix 環境での Microsoft Teams の IT 運用を効率化することで、ユーザーエクスペリエンスが向上します。

ダッシュボードには、参加者セッションごとの通話の詳細と品質メトリックが表示されます。通常の通話、ビデオ会議、その他のコラボレーションセッションを区別できます。

マイクロソフト チームズ

Citrix Director の Microsoft Teams ダッシュボードは、ユーザー全体の Microsoft Teams 通話の可視性を提供し、参加者に関する詳細情報と通話パフォーマンスを示すメトリックを提供します。このダッシュボードは、次の機能を提供します。

- Microsoft Teams の使用状況の概要を評価する
- 選択した期間の Microsoft Teams 通話の詳細をフィルタリングして表示する
- パフォーマンスメトリックを使用して個々の通話を評価する



前提条件

Citrix Director の許可リストに Microsoft Graph アプリケーションプログラミングインターフェイス (API) を追加します。

- Directorが通話記録にアクセスできるように、Directorがインストールされているすべてのマシンでアウトバウンドインターネットアクセスが利用可能であることを確認してください。特に、`<https://graph.microsoft.com>` URLにアクセスできることを確認してください。
- プロキシサーバーを使用している場合は、Microsoft Graph API : `<https://graph.microsoft.com>` URLにアクセスできることを確認してください。

はじめに

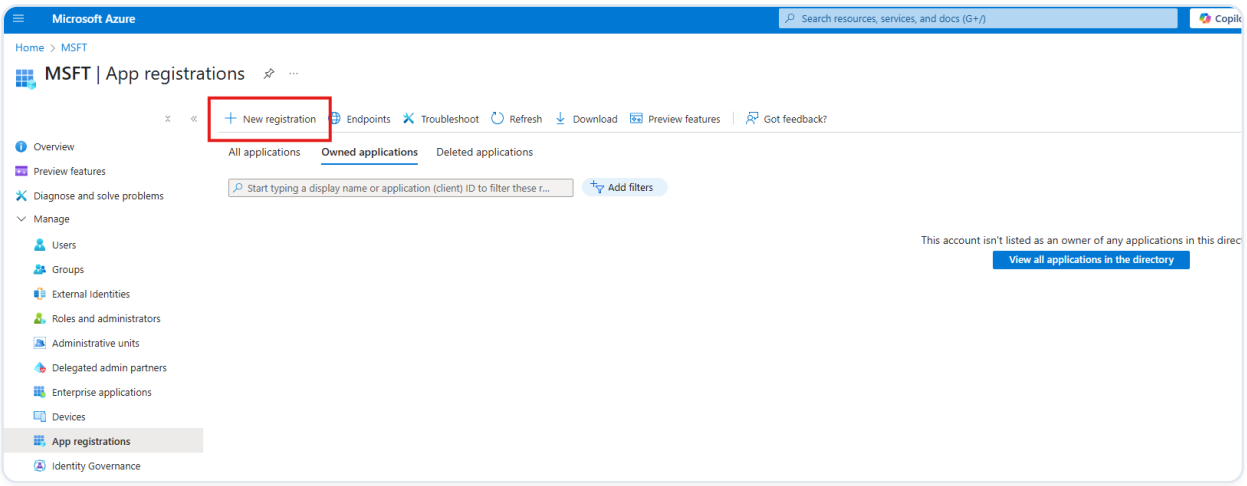
Microsoft Graph API への接続

Microsoft の通話詳細は Microsoft Graph API から取得されます。Citrix Director が API にアクセスするには、必要な権限を持つアプリを Microsoft Entra ID で作成する必要があります。Graph API の URL も Director の許可リストに追加する必要があります。

接続を完了するには、次の手順を実行します。

ステップ 1: Microsoft Entra ID でのアプリケーション登録

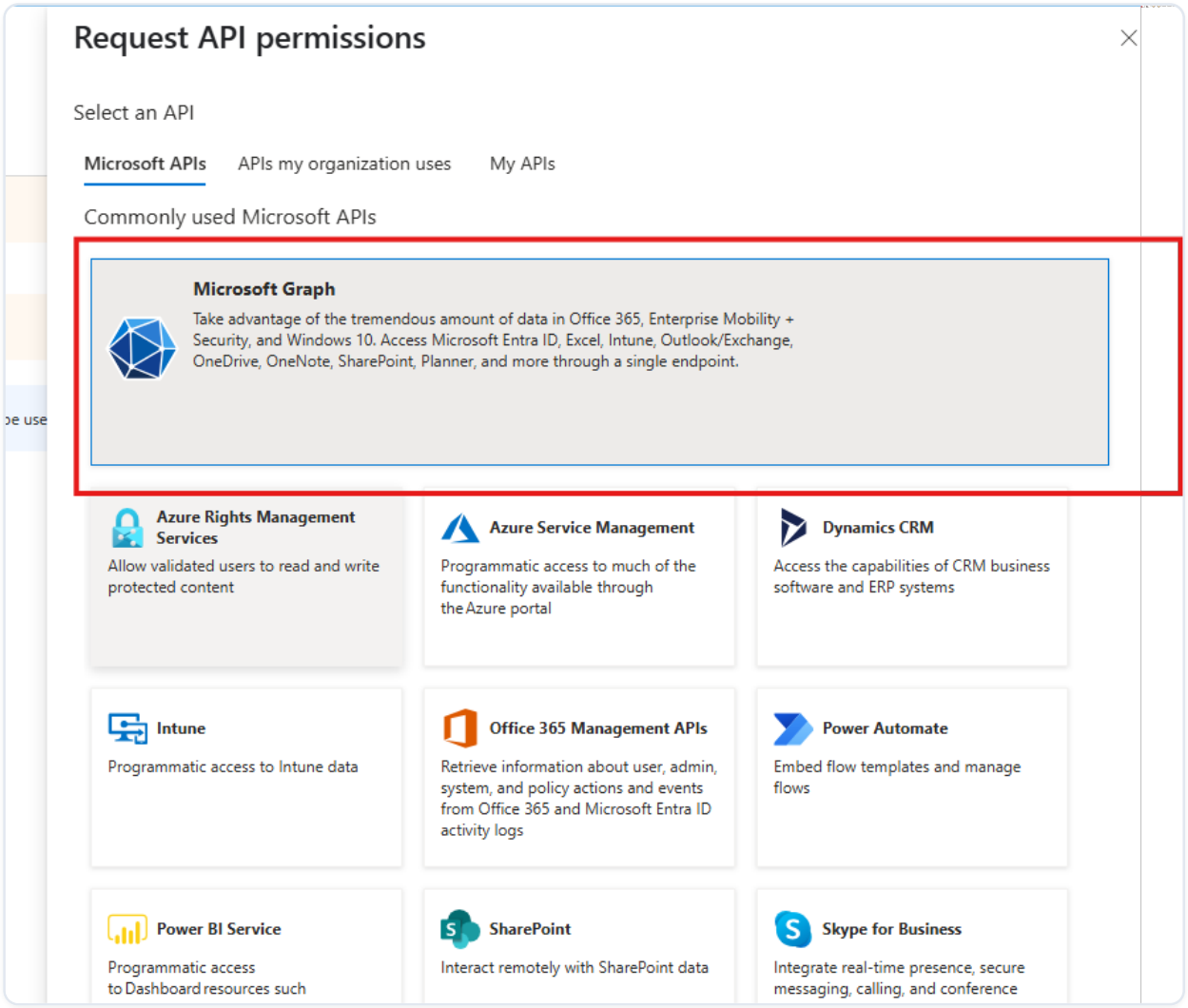
1. Microsoft Entra ID で **アプリの登録** -> **新規登録** に移動します。



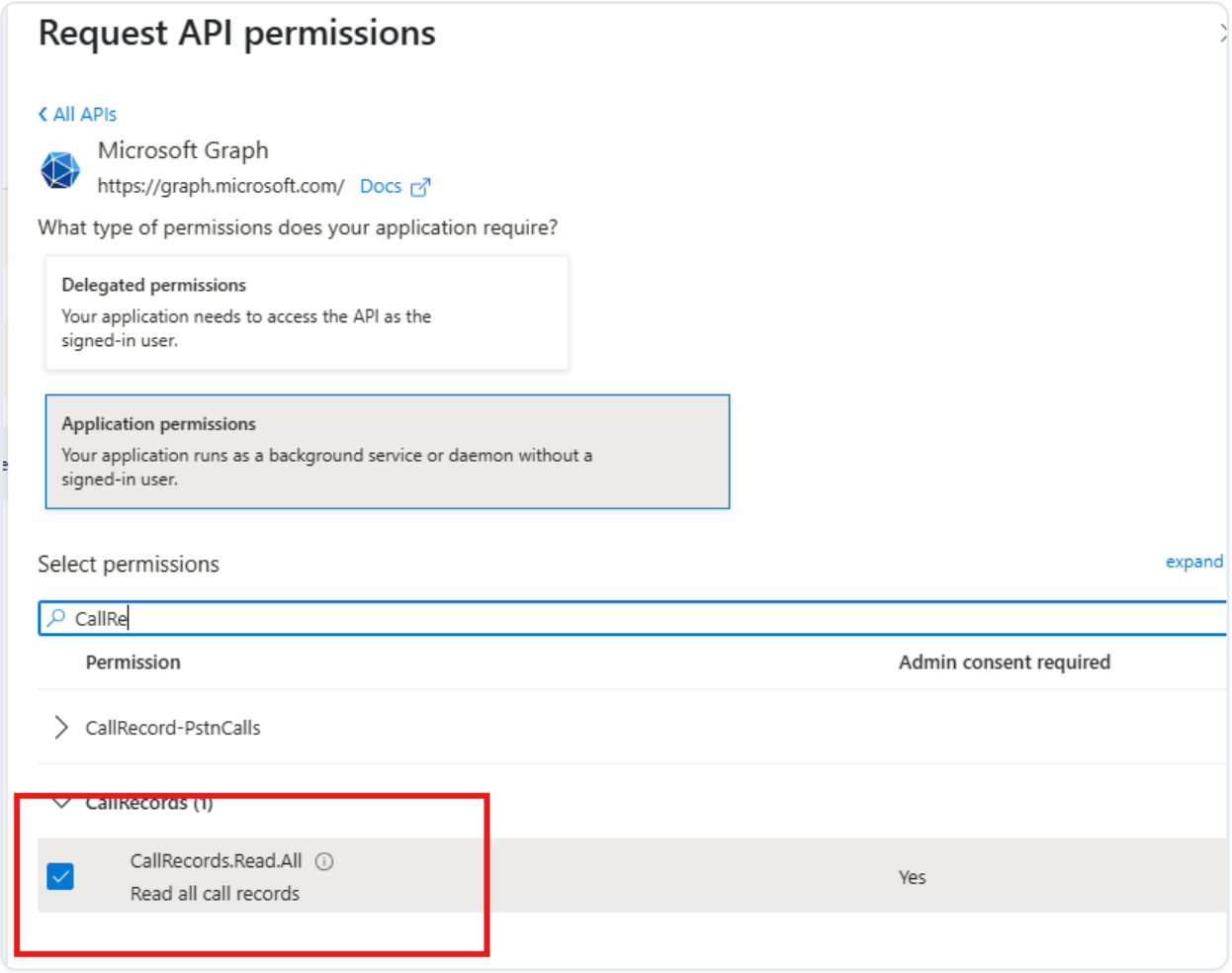
2. アプリ登録に必要な手順を実行します。
3. 登録後、アプリケーションのクライアントIDとテナントIDをコピーします。

ステップ2：Microsoft Entra IDでMicrosoft Graphのアクセス許可を追加する

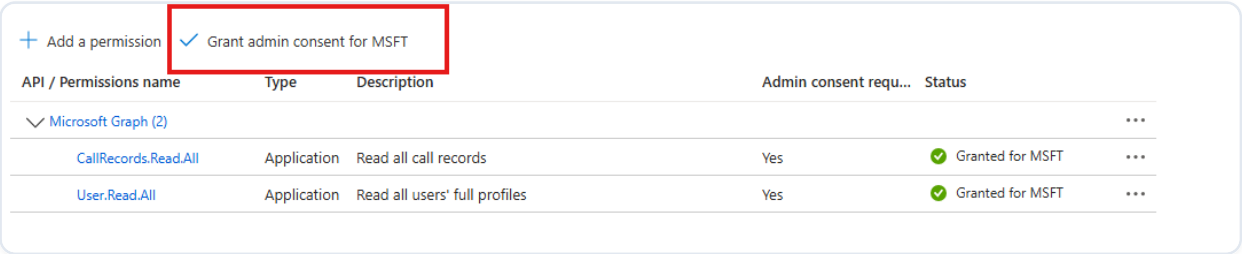
1. **API のアクセス許可** -> **アクセス許可の追加** に移動します。
2. **Microsoft Graph** を選択し、次に **アプリケーションのアクセス許可** を選択します。



3. **CallRecords.Read.All** と **User.Read.All** へのアクセス許可を追加します。

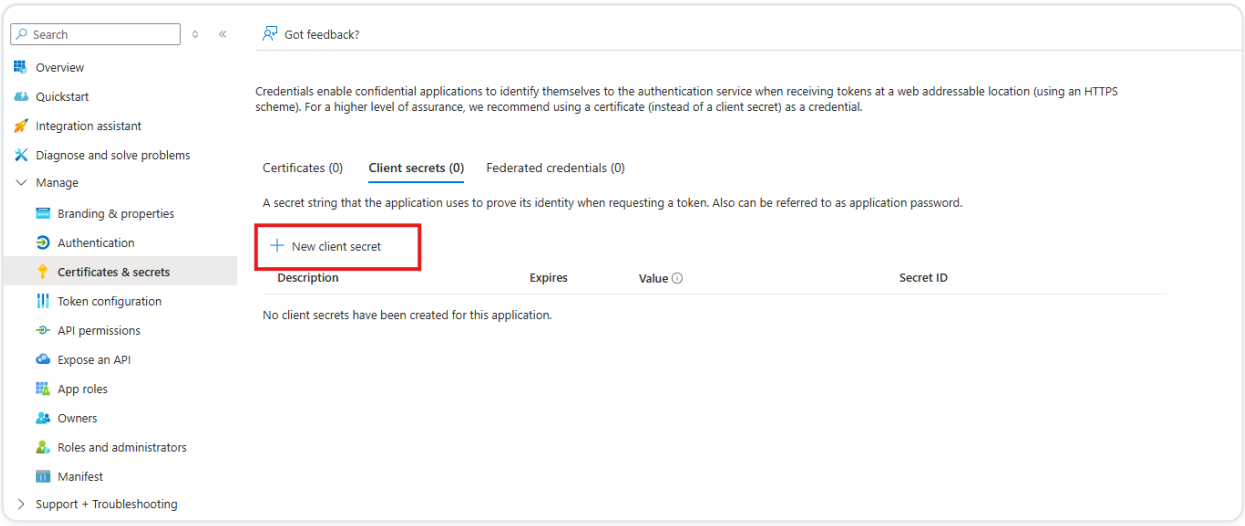


4. **MSFT の管理者の同意を付与** をクリックします。この操作には、Entra ID のグローバル管理者が必要です。



ステップ3：クライアントシークレットを作成する

1. Microsoft Entra ID で、**証明書とシークレット** -> **クライアントシークレット** -> **新しいクライアントシークレット** に移動します。既存のシークレットを再利用することもできます。

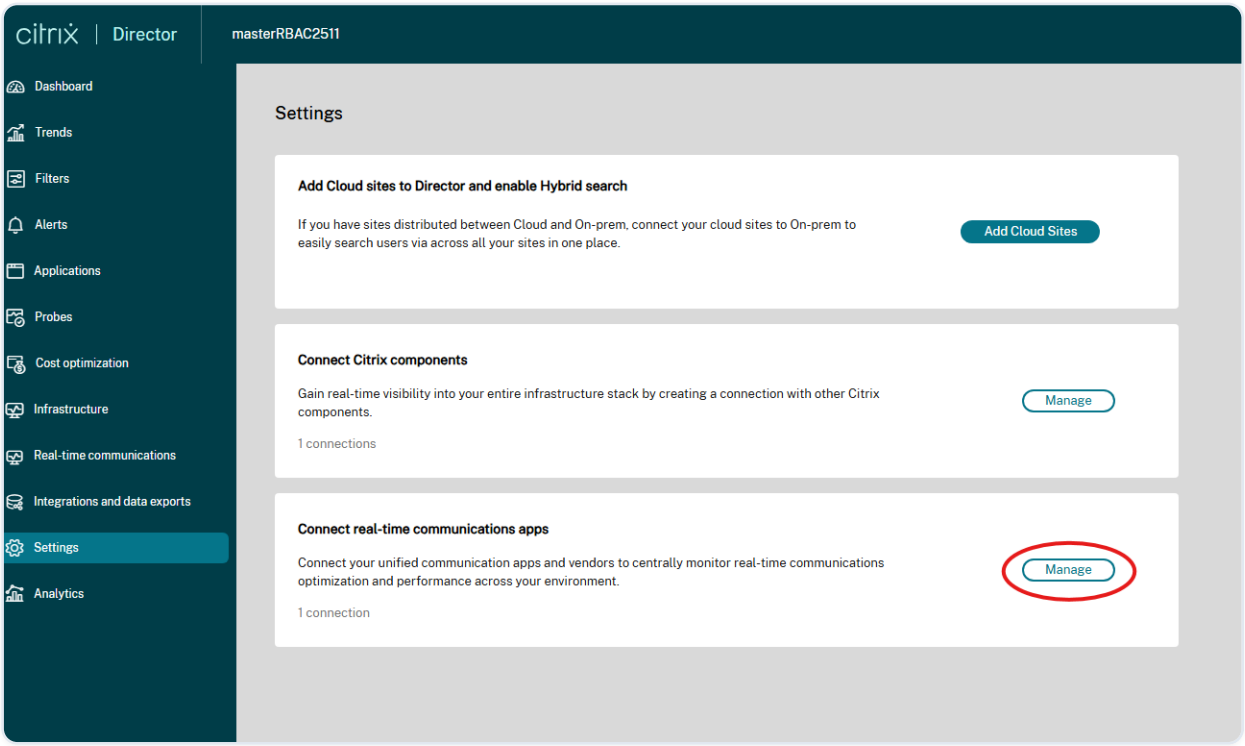


2. シークレットの名前と有効期限を指定します。接続を維持するために、有効期限が切れる前にシークレットを更新してください。
3. Director UI で使用するためにクライアントシークレットをコピーします。

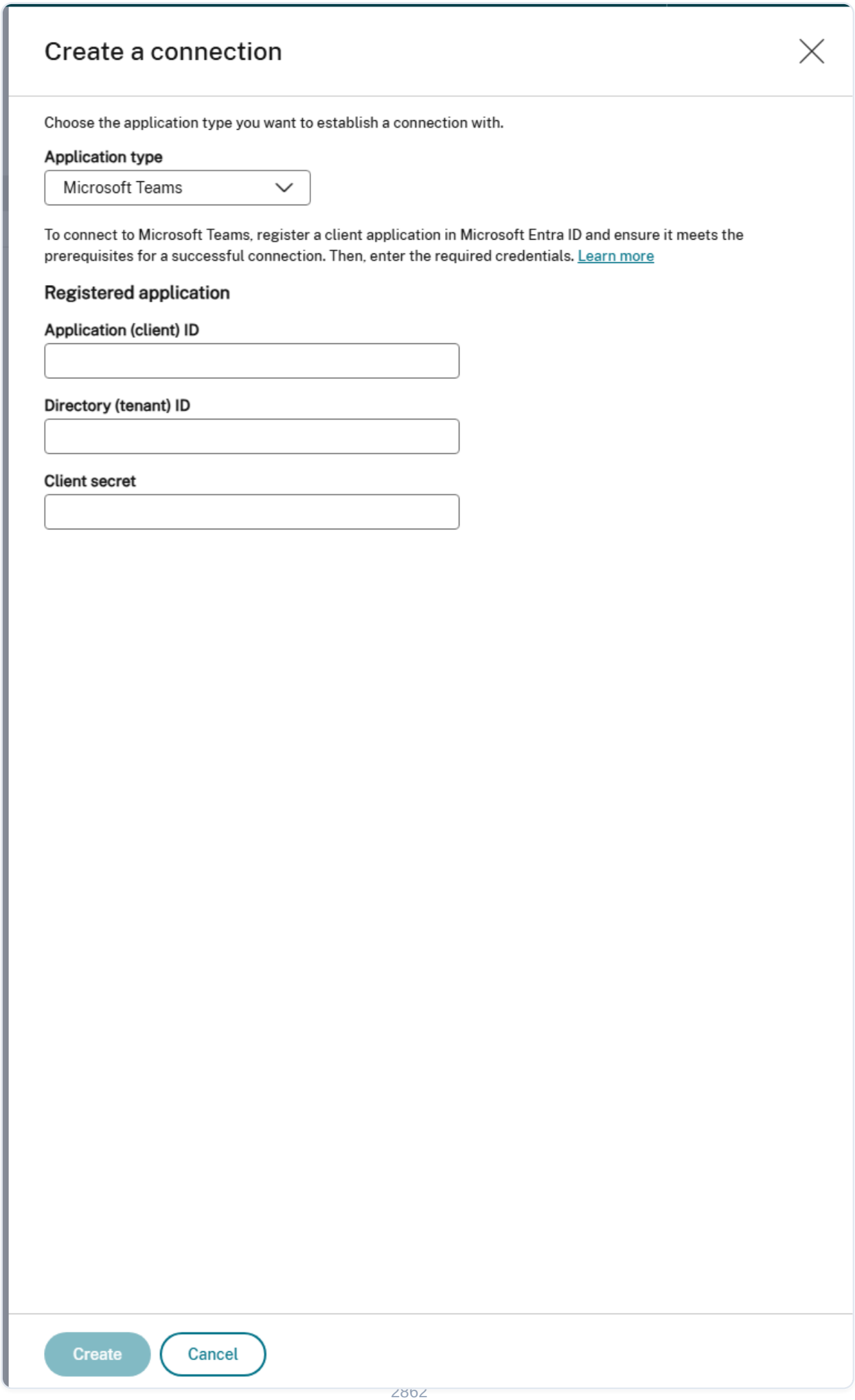
詳細については、問題が発生した場合に公式のAzure ドキュメントを参照してください。

ステップ4：Directorで接続を完了する

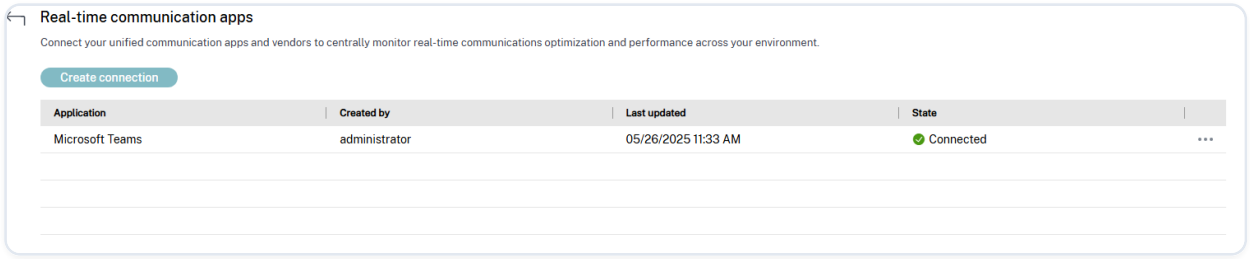
1. Directorで、**設定** -> **リアルタイム通信アプリを接続** に移動します。



2. **接続を作成** をクリックし、アプリ登録からコピーしたアプリケーションID、ディレクトリID、およびクライアントシークレットを入力します。


Create a connection
Choose the application type you want to establish a connection with.
Application type
Microsoft Teams
To connect to Microsoft Teams, register a client application in Microsoft Entra ID and ensure it meets the prerequisites for a successful connection. Then, enter the required credentials. Learn more
Registered application
Application (client) ID
Directory (tenant) ID
Client secret
Create
Cancel

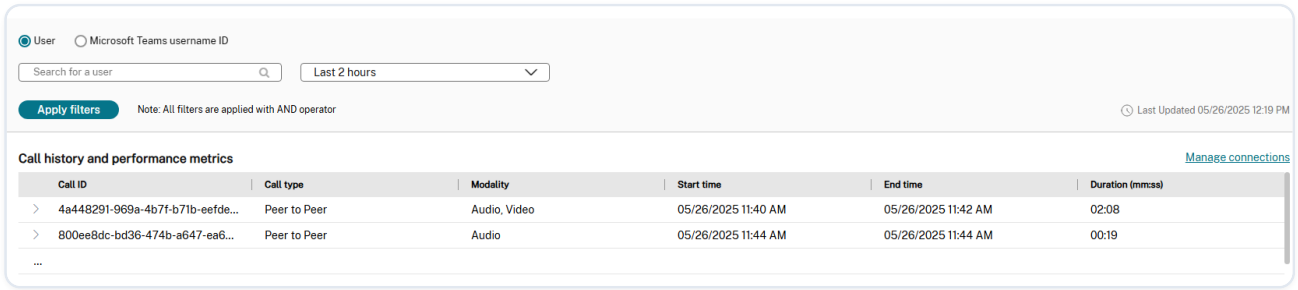
有効な資格情報と通話の詳細を取得するための権限が利用できる場合、接続は正常に確立されます。



3. 行の末尾にある省略記号をクリックすると、接続を**編集**および**削除**できます。

Microsoft Teams ダッシュボード

Director UIの**リアルタイム通信**タブに移動します。Microsoft Teamsダッシュボードには、確立されたMicrosoft Graph接続から収集されたデータが入力されます。通話の詳細情報は、通話終了後約15分で利用可能になります。



テーブルビューには、すべての通話について次の詳細が表示されます。

列名	説明
通話ID	各通話の一意の識別子。
通話の種類	通話がピアツーピアかグループ通話かを示します。
モダリティ	通話中に使用されるモード（オーディオ、ビデオ、画面共有など）を示します。
開始時刻	通話が開始された日時。
終了時刻	通話が終了した日時。
期間 (mm:ss)	通話の分数と秒数での期間。

テーブル内の個々の通話をクリックすると、ユーザーごとの障害とパフォーマンスの詳細が表示されます。

個別の通話(/en-us/citrix-virtual-apps-desktops/current-release/media/individual-calls.png)

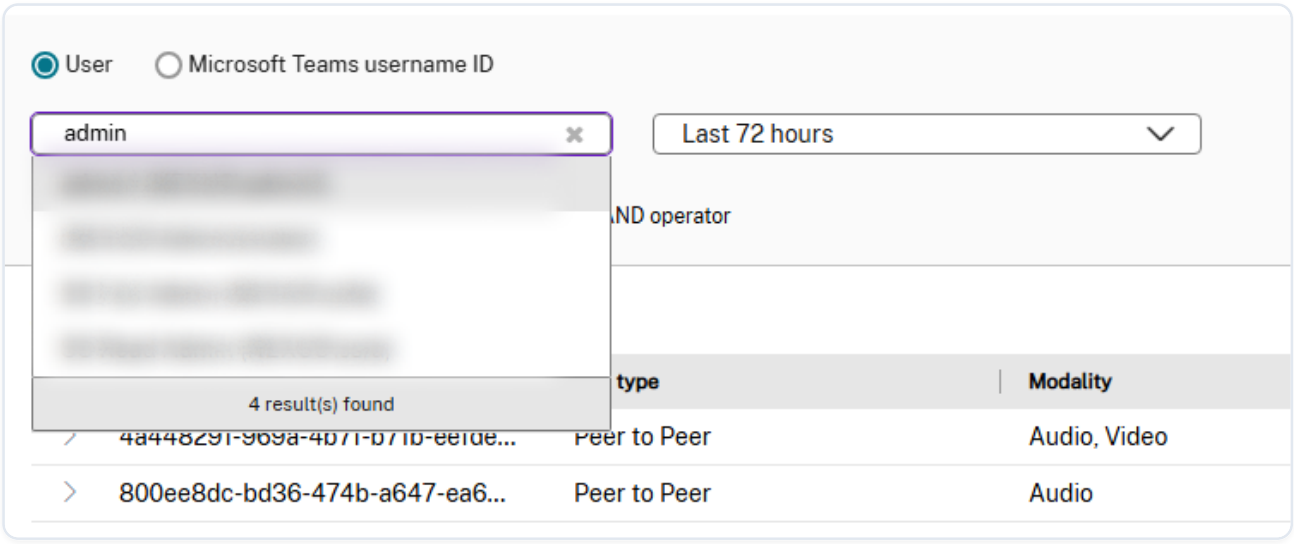
グループ通話でユーザーが切断して再参加した場合、それは別のセッションとして扱われます。この考慮事項は、特定のネットワークに接続した際のレイテンシーの増加など、特定の問題を特定するのに役立ちます。

通話詳細テーブルの各行には、次の情報が含まれています。

列名	説明
開始時刻	通話または参加者のセグメントが開始された日時。
ラウンドトリップ時間 (平均)	データパケットの平均往復時間。
パケット損失率（平均）	通話中に失われたパケットの平均割合。
ジッター（平均）	受信パケットの遅延の平均変動。
失敗ステージ	通話の失敗が発生した段階（セットアップ中や通話中など）を示します。
終了時刻	通話または参加者のセグメントが終了した日時。
発信者	通話の参加者の名前。
帯域幅の見積もり（平均）	通話中に使用された推定平均帯域幅。

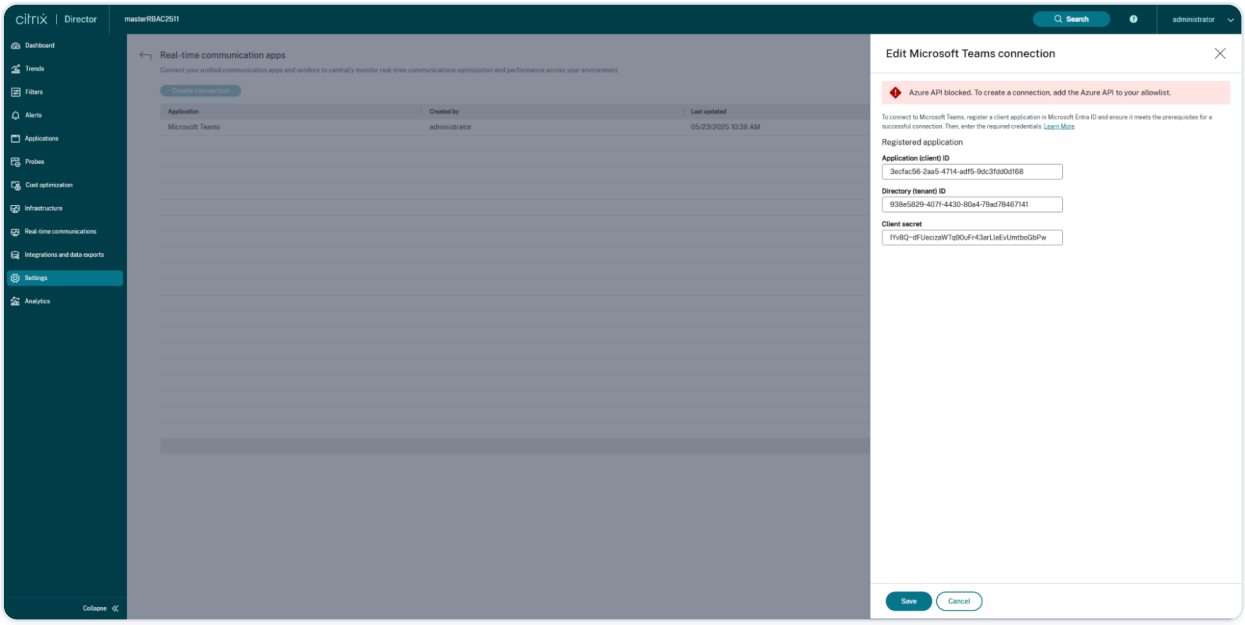
ユーザーは、Citrixユーザー名またはMicrosoft Teamsユーザー名の2つの方法でフィルタリングできます。ページ上部のラジオボタンを使用して、これらのオプションを切り替えることができます。

- Citrixユーザー名: ユーザー名の入力を開始すると、システムが一致するユーザーを提案します。その後、特定のアカウントを選択して詳細を表示できます。
- Microsoft Teamsユーザー名: Microsoft Teamsアカウントに関連付けられているメールアドレスまたはユーザープリンシパル名（UPN）がCitrixアカウントIDと異なる場合は、このオプションを使用します。この方法を使用する場合は、完全で有効なメールアドレスを入力する必要があります。



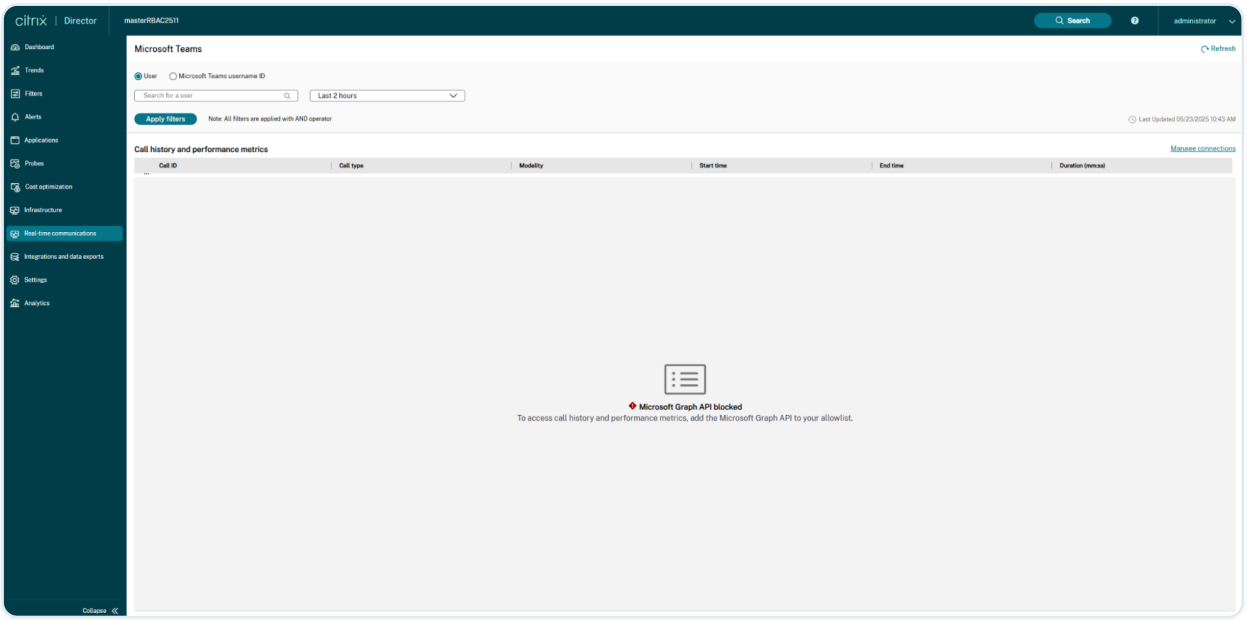
トラブルシューティング

- 「Azure API がブロックされました。接続を作成するには、Azure API を許可リストに追加してください」というエラーでオンボーディングが失敗したのはなぜですか？



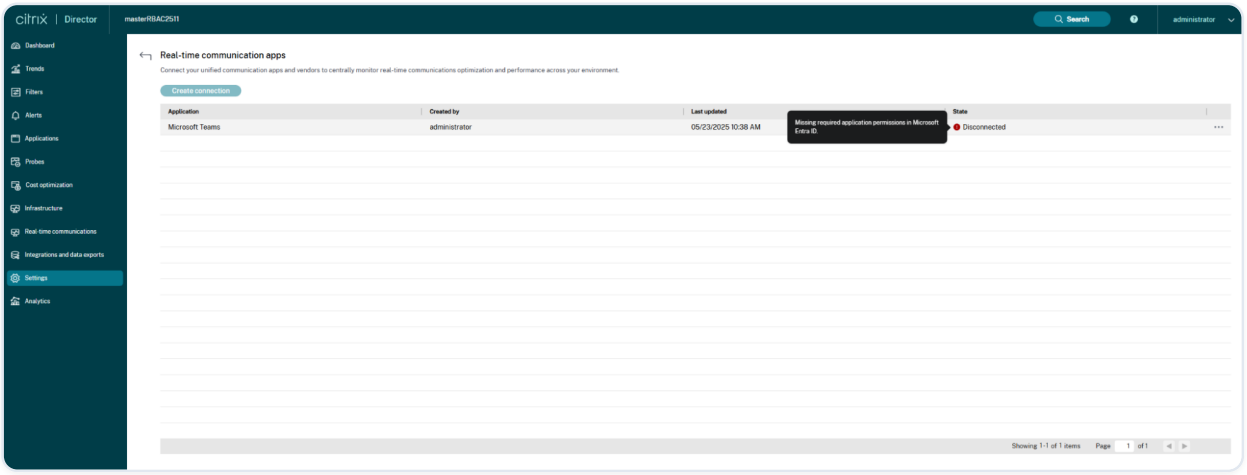
解決策: 前提条件に従い、Microsoft Graph API エンドポイントを許可リストに追加したことを確認してください。

- 通話を表示すると、「Microsoft Graph API がブロックされました」というエラーが表示されるのはなぜですか？



解決策: 前提条件に従い、Microsoft Graph API エンドポイントを許可リストに追加したことを確認してください。

- 接続画面に「Microsoft Entra ID で必要なアプリケーション権限が不足しています」と表示されるのはなぜですか？



解決策: アプリケーション権限の **CallRecords.Read.All** と **User.Read.All** が Entra ID アプリケーションに割り当てられていることを確認してください。

展開のトラブルシューティング

アプリケーションのトラブルシューティング

リアルタイムアプリケーション監視

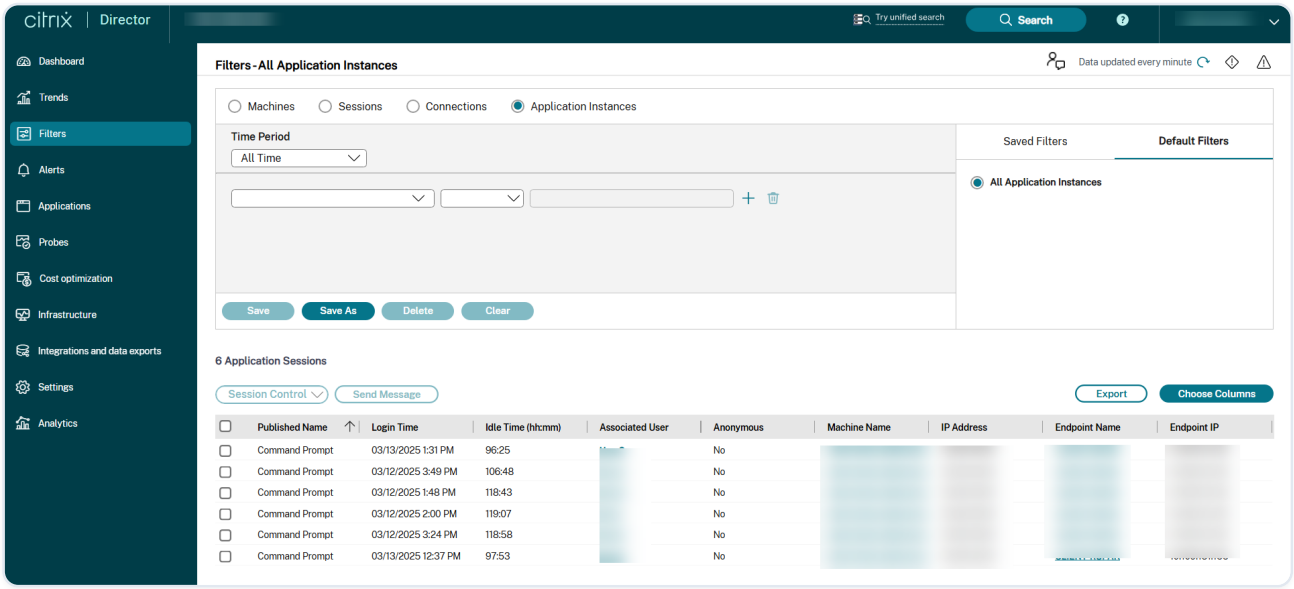
アイドル時間メトリックを使用して、特定の時間制限を超えてアイドル状態になっているインスタンスを特定することで、アプリケーションとセッションのトラブルシューティングを行うことができます。

アプリケーションベースのトラブルシューティングの典型的なユースケースは、従業員がアプリケーションライセンスを共有する医療分野にあります。そこでは、Citrix Virtual Apps and Desktops™環境をパージしたり、パフォーマンスの低いサーバーを再構成したり、アプリケーションを保守およびアップグレードしたりするために、アイドル状態のセッションとアプリケーションインスタンスを終了する必要があります。

アプリケーションインスタンスフィルターページには、サーバーおよびシングルセッションOSのVDA上のすべてのアプリケーションインスタンスが一覧表示されます。関連するアイドル時間測定値は、少なくとも10分間アイドル状態であったマルチセッションOSのVDA上のアプリケーションインスタンスに対して表示されます。

> **注:**
>
> アプリケーションインスタンスのメトリックは、すべてのライセンスエディションのサイトで利用できます。

この情報を使用して、特定の期間を超えてアイドル状態になっているアプリケーションインスタンスを特定し、必要に応じてログオフまたは切断します。これを行うには、**フィルター\> アプリケーションインスタンス**を選択し、事前に保存されたフィルターを選択するか、**すべてのアプリケーションインスタンス**を選択して独自のフィルターを作成します。

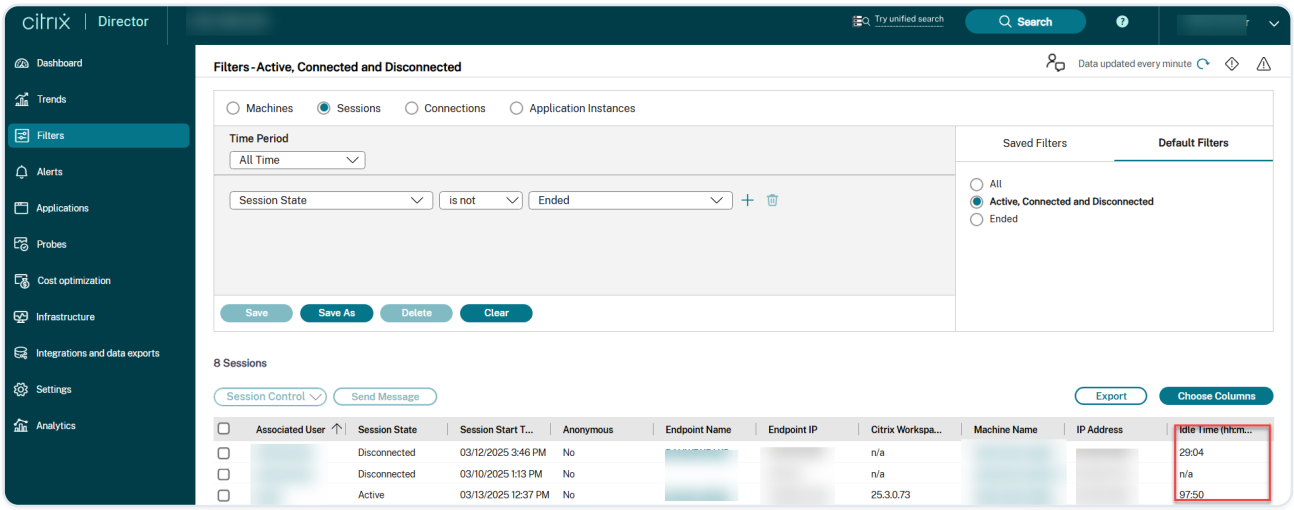


フィルターの例は次のとおりです。**フィルター条件**として、**公開名**（アプリケーションの）と**アイドル時間**を選択します。次に、**アイドル時間**を特定の時間制限**以上**に設定し、再利用のためにフィルターを保存します。フィルターされたリストから、アプリケーションインスタンスを選択しま

す。メッセージを送信するオプションを選択するか、**セッション制御**ドロップダウンから**ログオフ**または**切断**を選択してインスタンスを終了します。

> **注:**
>
> アプリケーションインスタンスをログオフまたは切断すると、現在のセッションがログオフまたは切断され、同じセッションに属するすべてのアプリケーションインスタンスが終了します。

セッションフィルターページから、セッションの状態とセッションアイドル時間メトリックを使用して、アイドル状態のセッションを特定できます。**アイドル時間**列で並べ替えるか、特定の時間制限を超えてアイドル状態になっているセッションを特定するためのフィルターを定義します。アイドル時間は、少なくとも10分間アイドル状態であったマルチセッションOSのVDA上のセッションに対して表示されます。



セッションまたはアプリケーションインスタンスが次の条件の場合、**アイドル時間**は**N/A**と表示されます。

- 10分以上アイドル状態になっていない場合、,
- シングルセッションOSのVDAで起動されている場合、または
- Version 7.12以前のVDAで起動されます。

アプリケーション障害の履歴監視

トレンド -\> **アプリケーション障害**タブには、VDA上の公開アプリケーションに関連する障害が表示されます。

アプリケーション障害の傾向は、PremiumおよびAdvancedライセンスサイトでは過去2時間、24時間、7日間、および1か月間利用できます。その他のライセンスタイプでは、過去2時間、24時間、および7日間利用できます。「Application Errors」をソースとしてイベントビューアにログ記録されたアプリケーション障害が監視されます。**エクスポート**をクリックすると、CSV、Excel、またはPDF形式でレポートを生成できます。

アプリケーション障害監視のグルーミング保持設定であるGroomApplicationErrorsRetentionDaysとGroomApplicationFaultsRetentionDaysは、Premiumおよび非Premiumライセンスサイトの両方で、デフォルトで1日に設定されています。この設定は、PowerShellコマンドを使用して変更できます。

```
Set-MonitorConfiguration -\<setting name\> \<value\>
```

アプリケーション障害の傾向(/en-us/citrix-virtual-apps-desktops/current-release/media/dir_application_faults.png)

障害は、その重大度に基づいて**アプリケーションフォールト**または**アプリケーションエラー**として表示されます。アプリケーションフォールトタブには、機能またはデータの損失に関連する障害が表示されます。アプリケーションエラーは、すぐには関連しない問題を示し、将来問題を引き起こす可能性のある状態を示します。

公開アプリケーション名、**プロセス名**、**デリバリーグループ**、および**期間**に基づいて障害をフィルタリングできます。テーブルには、フォールトまたはエラーコードと障害の簡単な説明が表示されます。詳細な障害の説明はツールチップとして表示されます。

注:

対応するアプリケーション名を導出できない場合、公開アプリケーション名は「Unknown」と表示されます。これは通常、起動されたアプリケーションがデスクトップセッションで失敗した場合、または依存する実行可能ファイルによって引き起こされた未処理の例外が原因で失敗した場合に発生します。

デフォルトでは、マルチセッションOS VDAでホストされているアプリケーションの障害のみが監視されます。監視グループポリシー（アプリケーション障害の監視を有効にする、シングルセッションOS VDAでのアプリケーション障害の監視を有効にする、障害監視から除外されるアプリケーションのリスト）を通じて監視設定を変更できます。詳細については、監視ポリシー設定のアプリケーション障害監視のポリシーを参照してください。

トレンド \> アプリケーションプローブ結果ページには、過去24時間および7日間にサイトで実行されたアプリケーションプローブの結果が表示されます。アプリケーションプローブの構成方法の詳細については、アプリケーションプローブを参照してください。

マシンの健全性監視

1. はじめに: 新機能?

Virtual Delivery Agent (VDA) マシンの健全性とパフォーマンスに関するより豊富なインサイトを提供するため、いくつかの主要な機能強化を導入しました。

- **新しい視覚化:**
  a. **概要、電源状態、登録状態**の3つのカテゴリを持つサマリーパネルが追加されました。
  b. マシンのステータスと履歴トレンドを即座にグラフィカルに表示するために、**マシン分布**と**経時的な平均パフォーマンス**という2つの新しいグラフが追加されました。
- **強化された表形式データ: シングルセッション**および**マルチセッションデスクトップ**マシンのテーブルに、重要なVDAサービスの詳細なステータス列が追加され、マシンの健全性問題の根本原因を迅速に特定するのに役立ちます。
- **新しい時間範囲フィルター:** 履歴トレンドをサポートするために、過去2時間と過去7日間という2つの新しい時間範囲フィルターが追加されました。

新しい時間フィルター(/en-us/citrix-virtual-apps-desktops/current-release/media/dir-new-time-filter.png)

2. 新しい視覚化の理解

2.1. サマリーパネル

- **概要:** 関連付けられているVDA（マシン）の総数を表示します。
- **電源状態:** マシンの電源状態（オン、オフ、中断、管理対象外、その他）に基づいてマシンの数を表示します。
- **登録状態:** マシンの登録状態（登録済み、未登録、その他）に基づいてマシンの数を表示します。

このサマリーは折りたたみ可能で、管理者が上記の分類に基づいて、オフ状態のマシンをオンにしたり、未登録状態のマシンを特定したりするなど、必要なアクションを実行するのに役立ちます。

概要パネル(/en-us/citrix-virtual-apps-desktops/current-release/media/dir-machine-summary.png)

2.2. マシン分布

- **目的:** この棒グラフは、現在のフィルターセットに含まれるVDAマシンの迅速な視覚的内訳を提供します。デフォルトのフィルターはVDAバージョンに設定されています。ただし、ユーザーはデリバリーグループ、マシンカタログ、登録状態、メンテナンスモード、デリバリーコントローラー、ハイパーバイザー接続名、障害タイプ、障害理由、および電源状態を使用してフィルター処理できます。
- **ユーティリティ:** これにより、管理者はフィルター条件に基づいてVDAの全体的な概要を把握できます。例えば、VDAバージョンごとのマシン分布は、VDAの大部分が古いまたは非標準のVDAバージョンで実行されているかどうかを管理者が迅速に特定するのに役立ちます。これは、トラブルシューティングやアップグレード計画の前提条件となる場合があります。

マシン分布(/en-us/citrix-virtual-apps-desktops/current-release/media/dir-machine-distribution.png)

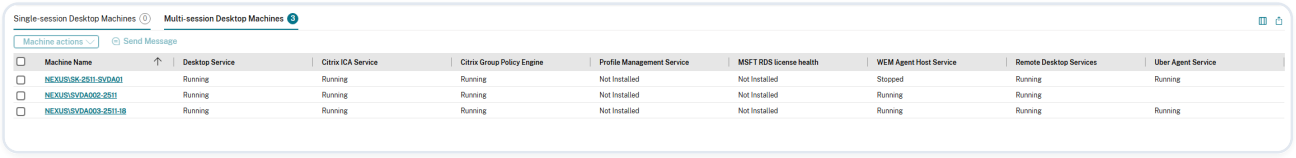
2.3. 時間経過に伴う平均パフォーマンス

平均パフォーマンス(/en-us/citrix-virtual-apps-desktops/current-release/media/dir-machine-avg-performance.png)

- **目的:** この時系列チャートは、選択された期間（例：過去24時間）における主要なパフォーマンスメトリックを追跡します。
- **追跡される主要メトリック:**
  - **CPU使用率 (%):** 使用されているCPUの平均パーセンテージ。
  - **メモリ使用率 (%):** 利用されているRAMの平均パーセンテージ。
  - **ディスクIOPS:** 1秒あたりの平均入出力操作数。
  - **ディスク遅延 (ミリ秒):** ディスクI/O要求の平均時間遅延（ミリ秒単位）。
  - **GPU使用率 (%):** 使用されているGPUの平均パーセンテージ（該当する場合）。
  - **ロード評価 (%):** VDAマシン上の計算されたロードインデックスのパーセンテージ。
- **ユーティリティ：** 履歴トレンド分析を可能にし、パフォーマンスの低下、リソースの競合、およびピーク負荷の発生時期を特定するのに役立ちます。

3. 強化された表形式データ

シングル/マルチセッションテーブル：新しい列の定義



列名	説明	可能な値
デスクトップサービス	デスクトップセッションの管理を担当する主要サービスの健全性ステータス（例：CtxSvcHost）。	実行中、停止済み、未インストール、一時停止、開始保留中、停止保留中、続行保留中、一時停止保留中、不明
Citrix ICAサービス	ユーザーセッション用のIndependent Computing Architecture (ICA) プロトコルを処理するコアサービスの健全性ステータス。	実行中、停止済み、未インストール、一時停止、開始保留中、停止保留中、続行保留中、一時停止保留中、不明
Citrixグループポリシーエンジン	Citrix固有のポリシーを処理および適用する責任を負うサービスの健全性ステータス。	実行中、停止済み、未インストール、一時停止、開始保留中、停止保留中、続行保留中、一時停止保留中、不明
プロファイル管理サービス	Citrix仮想環境でユーザープロファイルを管理するために使用されるCitrix Profile Managementのヘルスステータス。	実行中、停止、未インストール、一時停止、開始保留中、停止保留中、続行保留中、一時停止保留中、不明
MSFT RDSライセンスの健全性	Microsoft Remote Desktop Services (RDS) ライセンスチェックのステータスを示します。	実行中、停止、未インストール、一時停止、開始保留中、停止保留中、続行保留中、一時停止保留中、不明
WEMエージェントホストサービス	最適化と構成を担当するWorkspace Environment Management (WEM) エージェントのヘルスステータス。	実行中、停止、未インストール、一時停止、開始保留中、停止保留中、続行保留中、一時停止保留中、不明
リモートデスクトップサービス	基盤となるMicrosoft Remote Desktop Servicesのヘルスステータス（シングルセッションホスト機能とマルチセッションホスト機能の両方に必要）。	実行中、停止、未インストール、一時停止、開始保留中、停止保留中、続行保留中、一時停止保留中、不明

列名	説明	可能な値
Uber Agentサービス	サードパーティの監視エージェントサービスのヘルスステータス（該当する場合、およびインストールされている場合）。	実行中、停止、未インストール、一時停止、開始保留中、停止保留中、続行保留中、一時停止保留中、不明

4. 新しい時間範囲フィルターへの対応

新しい時間フィルター(/en-us/citrix-virtual-apps-desktops/current-release/media/dir-new-filter-time.png)

1. **過去2時間**
    - **目的:** 過去120分間のVDAリソース使用率を、高粒度で即座に表示します。
    - **用途:** この短い時間枠は、リアルタイムのトラブルシューティングに最適です。これを使用して、リソースの急増（高CPUや低ディスクIOPSなど）が発生した正確な時間を特定し、最近のユーザーアクティビティや管理操作と関連付けます。
2. 過去7日間
    - **目的:** 過去1週間のリソース使用状況とパフォーマンスの傾向を表示します。
    - **用途:** これは、週次パフォーマンスレビューの標準フィルターです。これにより、管理者は、VDAリソースに常に負荷をかける特定の日やピーク時間（例：月曜日の朝のログオン）など、繰り返し発生するパフォーマンスの問題を特定し、プロアクティブなキャパシティプランニングと最適化を可能にします。

VDAヘルス監視メトリック: サポートされているプラットフォームとバージョン

VDA列	ウィンドウズ	MAC	リナックス
デスクトップサービス	2511以降	2511 以上	2511 以上
Citrix ICAサービス	2511 以上	2511 以上	2511 以上
Citrixグループポリシーエンジン	2511 以上	2511 以上	2511 以上
プロファイル管理サービス	2511 以上	2511 以上	2511 以上

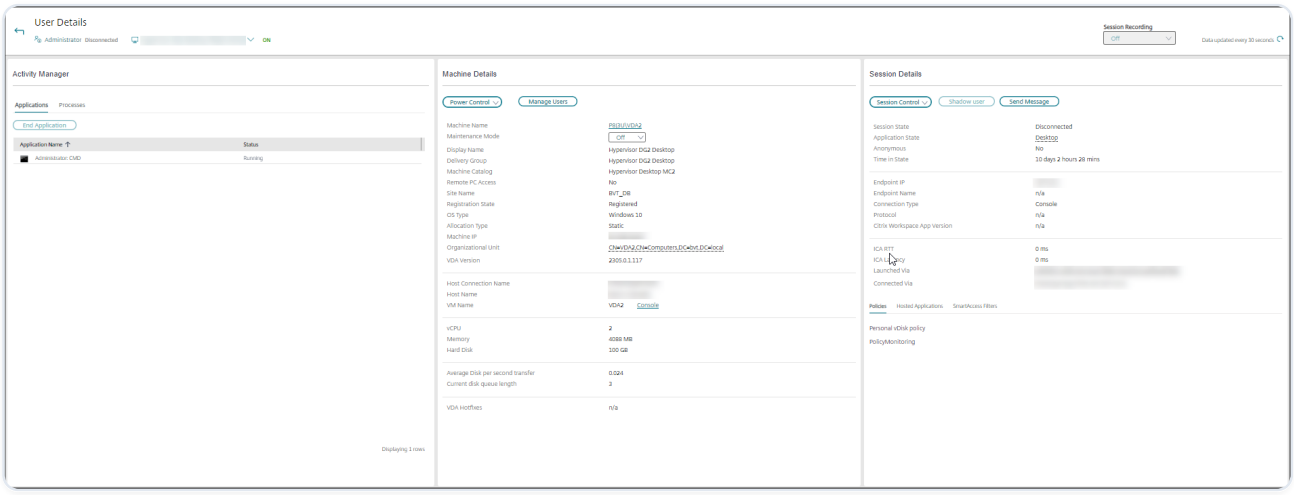
VDA列	ウィンドウズ	MAC	リナックス
MSFT RDSライセンスの健全性	2511以降	2511以降	2511以降
WEM エージェントホストサービス	2511以降	2511以降	2511以降
リモートデスクトップサービス	2511以降	2511以降	2511以降
UberAgent サービス	2511以降	2511以降	2511以降

ユーザーの問題のトラブルシューティング

Directorの**ヘルプデスク**ビュー（**アクティビティマネージャー**ページ）を使用して、ユーザーまたはセッションに関する情報を表示します。

ユーザーの詳細(/en-us/citrix-virtual-apps-desktops/current-release/media/dir-user-details-summary.png)

アクティビティマネージャーからユーザーに対して**詳細の表示**をクリックすると、**ユーザーの詳細**ページが開きます。 アクティビティマネージャーからエンドポイントに対して**詳細の表示**をクリックすると、**エンドポイントの詳細**ページが開きます。



セッションセレクター

ユーザーが複数のセッションを開始している場合、セッションセレクターはセッションの選択に役立ちます。

セッションセレクター(/en-us/citrix-virtual-apps-desktops/current-release/media/dir-session-selector.png)

詳細を表示するセッションを選択します。

- セッション、ユーザーのサインインエクスペリエンス、セッションの起動、接続、およびアプリケーションに関する詳細を確認します。
- ユーザーのマシンをシャドウできます。
- ICA®セッションを記録します。

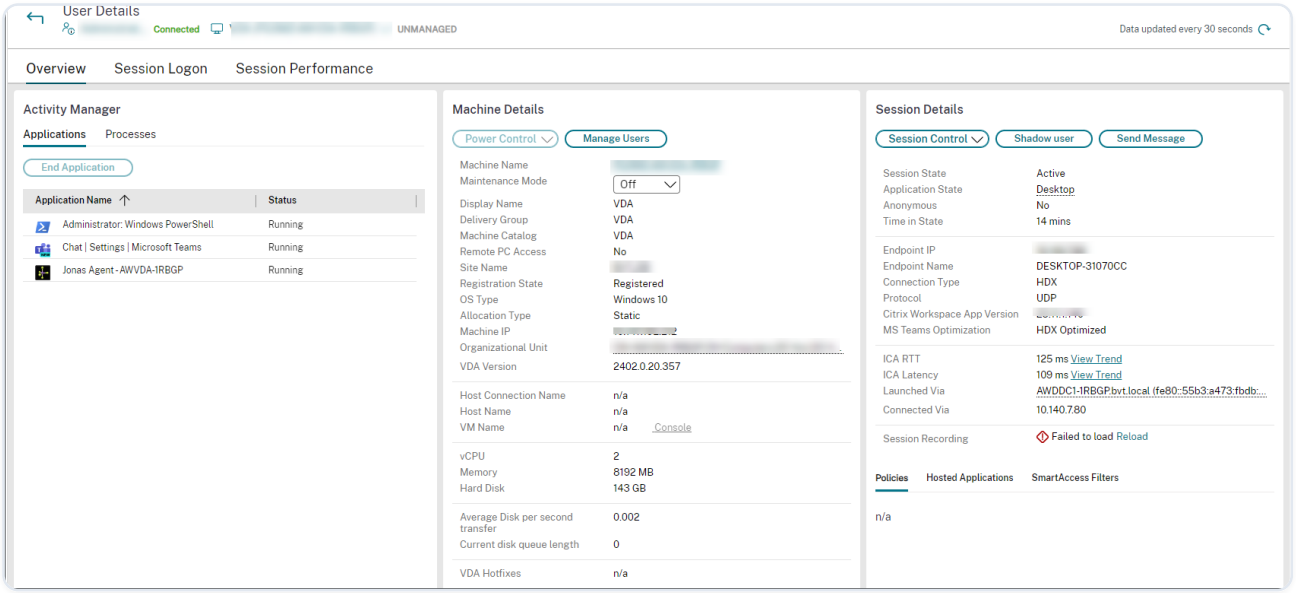
Microsoft Teamsの最適化ステータス

Directorは、HDX™セッションのMicrosoft Teamsの最適化ステータスを、**ユーザーの詳細**ページ > **セッションの詳細**パネル > **MS Teamsの最適化**フィールドに表示します。Microsoft Teamsが最適化されていることは、クリアなオーディオやビデオなど、より良いユーザーエクスペリエンスにとって重要です。Microsoft Teamsの最適化ステータスの可視性は、チケット解決にかかる時間を短縮し、トラブルシューティング中に管理者が重要なメトリックを特定するのに役立ちます。

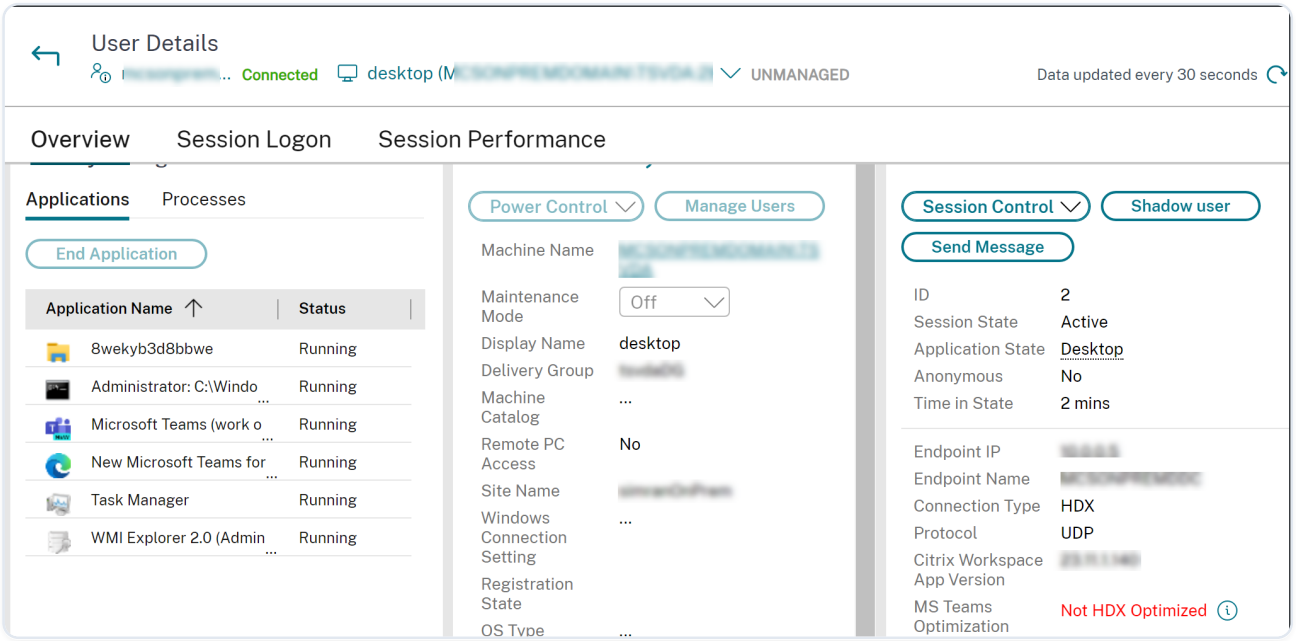
> **注:**
>
> Citrix Directorは、Microsoft Teamsバージョン2.1以前をサポートしています。

> 前提条件:

- VDAはバージョン2311以降を実行しています。
- Citrix Workspace app でサポートされているバージョンは、Microsoft Teams の最適化に記載されています。
- Microsoft Teams は、公開アプリケーションとして、または公開デスクトップ内で実行されます。
- Citrix HDX HTML5 Video Redirection Service などの重要なサービスが実行されています。



Microsoft Teams が最適化されていない場合、ツールヒントには、Microsoft Teams を最適化するためのヒントを含む、HDX からの外部トラブルシューティングライブ記事へのリンクが表示されます。HDX 最適化のトラブルシューティング。



トラブルシューティングのヒント

以下の表に記載されている推奨されるアクションで問題をトラブルシューティングし、必要に応じて適切な管理者に問題をエスカレートしてください。

ユーザーの問題	提案
ログオンに時間がかかる、または断続的または繰り返し失敗する	ユーザーログオンの問題を診断する

ユーザーの問題	提案
セッションの起動に時間がかかる、または断続的または繰り返し失敗する	セッション起動の問題を診断する
セッションの応答が遅い、または応答しない	セッションパフォーマンスの問題を診断する
アプリケーションが遅い、または応答しない	アプリケーション障害の解決
接続に失敗しました	デスクトップ接続の復元
セッションが遅い、または応答しない	セッションの復元
セッションを記録する	セッションの記録
ビデオが遅い、または品質が悪い	HDXチャネルシステムレポートの実行

注:

マシンがメンテナンスモードになっていないことを確認するには、［ユーザーの詳細］ビューから［マシンの詳細］パネルを確認します。

セッションログオン

［ユーザーの詳細］ ビュー > **［セッションログオン］** タブには、セッションログオンプロセスの包括的なビューが表示されます。このタブには、合計ログオン時間、クライアントとコントローラーの期間、およびVDAの期間が表示されます。**［セッションログオン］** タブには、さまざまなログオンフェーズがプロットされたログオン期間フェーズチャートが含まれています。このデータを使用して、ユーザーログオンの問題をトラブルシューティングします。詳しくは、「ユーザーログオンの問題の診断」を参照してください。

セッションパフォーマンス

セッションパフォーマンスタブには、ユーザーセッション内の問題を特定するためにリアルタイムメトリックを関連付ける機能から始まる、強化されたトラブルシューティングワークフローがあります。**セッショントポロジ**パネルは、接続されたHDXセッションのセッション内パスを視覚的に表現します。**パフォーマンスメトリック**パネルは、ICARTT、ICA遅延、1秒あたりのフレーム数、利用可能な出力帯域幅、消費された出力帯域幅などのセッションメトリックの傾向を提供し、これらのメトリックが時間の経過とともにどのようにパフォーマンスを発揮したかを示します。詳細については、セッションパフォーマンスの問題の診断を参照してください。

検索のヒント

検索フィールドにユーザー名を入力すると、Director は Director をサポートするように構成されているすべてのサイトのユーザーについて、Active Directory でユーザーを検索します。

検索フィールドにマルチユーザーマシンの名前を入力すると、Director は指定されたマシンのマシン詳細を表示します。

検索フィールドにエンドポイント名を入力すると、Director は特定のEndpointに接続されている認証されていない（匿名）セッションと認証済みセッションを使用します。この検索により、認証されていないセッションのトラブルシューティングが可能になります。認証されていないセッションのトラブルシューティングを可能にするには、エンドポイント名が一意であることを確認してください。

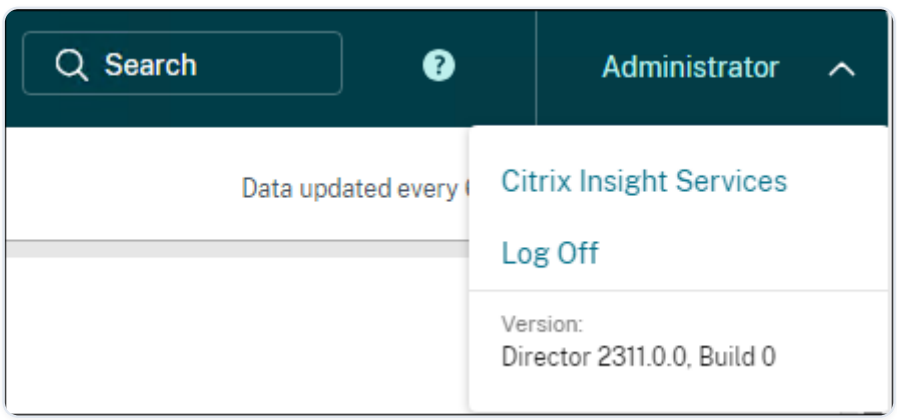
検索結果には、現在マシンを使用していない、またはマシンに割り当てられていないユーザーも含まれます。

- 検索では大文字と小文字は区別されません。
- 部分的な入力では、一致する可能性のあるリストが生成されます。
- スペースで区切られた2つの部分からなる名前の数文字を入力すると、両方の文字列に一致する結果が表示されます。2つの部分からなる名前の例としては、ユーザー名、姓と名、または表示名があります。たとえば、「jo rob」と入力すると、「John Robertson」や「Robert Jones」などの文字列が結果に含まれる場合があります。

ランディングページに戻るには、**Director ロゴ**をクリックします。

Citrix Insight Servicesへのアクセス

Director の ドロップダウンリストから Citrix Insight Services (CIS) にアクセスして、追加の診断情報を取得できます。CIS で利用できるデータは、Call Home や Citrix Scout などのソースから取得されます。



トラブルシューティング情報をCitrixテクニカルサポートにアップロードする

単一のDelivery Controller™またはVDAからCitrix Scoutを実行して、主要なデータポイントとCitrix Diagnostics Facility (CDF) トレースをキャプチャし、選択したコンピューターのトラブルシューティングを行います。Scoutは、データをCISプラットフォームに安全にアップロードして、Citrixテクニカルサポートのトラブルシューティングを支援する機能を提供します。Citrixテクニカルサポートは CISプラットフォームを使用して、顧客から報告された問題の解決時間を短縮します。

ScoutはCitrix Virtual Apps and Desktops™コンポーネントとともにインストールされます。Windowsのバージョンに応じて、Citrix Virtual Apps and Desktopsをインストールまたはアップグレードすると、Scoutは**Windowsのスタート**メニューまたはスタート画面に表示されます。

Scoutを起動するには、スタートメニューまたはスタート画面から **\>** を選択します。

Scoutの使用方法と構成、およびFAQについては、CTX130147を参照してください。

セッション起動の問題を診断する

ユーザーログオンの問題の診断セクションで述べられているログオンプロセスフェーズに加えて、Directorはセッション起動時間を表示します。これは、**ユーザーの詳細**ページと**マシンの詳細**ページで、Workspace Appセッション起動時間とVDAセッション起動時間に分けられます。これらの2つの期間は、さらに個々のフェーズを含み、その起動時間も表示されます。このデータは、セッション起動時間の長さの原因を理解し、トラブルシューティングするのに役立ちます。さらに、セッション起動に関わる各フェーズの期間は、個々のフェーズに関連する問題のトラブルシューティングに役立ちます。たとえば、ドライブマッピングの時間が長い場合、GPOまたはスクリプトですべての有効なドライブが正しくマッピングされているか確認できます。この機能は、Delivery Controllerバージョン7 1906以降およびVDA 1903以降で利用可能です。

前提条件

セッション起動時間のデータが表示されるには、以下の前提条件が満たされていることを確認してください。

- デリバリーコントローラー™ 7 1906 以降。
- VDA 1903以降。
- Citrix End User Experience Monitoring (EUEM)サービスがVDAで実行されている必要があります。

制限事項

Directorがセッション起動時間のデータを表示する際には、以下の制限が適用されます。

- セッション起動時間は、HDX™セッションでのみ利用可能です。

- iOSおよびAndroid OSからのセッション起動の場合、VDA起動時間のみが利用可能です。
- ICA®ファイルダウンロード時間 (IFDCD) は、ブラウザから起動する際にWorkspace Appが検出された場合にのみ利用可能です。
- Mac OSからのセッション起動の場合、IFDCDはWorkspace App 1902以降でのみ利用可能です。
- Windows OSからのセッション起動の場合、IFDCDはWorkspace app 1902以降で利用可能です。それ以前のバージョンでは、IFDCDはブラウザからWorkspace appが検出されたアプリ起動の場合にのみ表示されます。

注:

- 前提条件が満たされた後もセッション起動時間の表示に問題がある場合は、CTX130320に記載されているDirectorサーバーおよびVDAログを確認してください。 共有セッション（同じセッションで複数のアプリケーションが起動された場合）の場合、Workspace Appの起動メトリックは、最新の接続または最新のアプリケーション起動に対して表示されます。
- VDAセッション起動の一部のメトリックは、再接続時には適用されません。そのような場合、メッセージが表示されます。

セッション起動(/en-us/citrix-virtual-apps-desktops/current-release/media/session_startup.png)

Workspace App セッション起動フェーズ

セッション起動クライアント期間 (SSCD)

このメトリックが高い場合、起動時間が長くなるクライアント側の問題を示しています。問題の根本原因を特定するために、後続のメトリックを確認してください。SSCD は、要求 (マウスクリック) の時刻にできるだけ近い時点から開始されます。クライアントデバイスと VDA 間の ICA 接続が確立されたときに終了します。共有セッションの場合、サーバーへの新しい接続の作成に関連するセットアップコストの多くが発生しないため、この期間ははるかに短くなります。次のレベルでは、いくつかの詳細なメトリックが利用可能です。

ICA ファイルダウンロード期間

これは、クライアントがサーバーから ICA ファイルをダウンロードするのにかかる時間です。全体的なプロセスは次のとおりです。

1. ユーザーは Workspace Application でリソース (アプリケーションまたはデスクトップ) をクリックします。
2. ユーザーからの要求は、Citrix Gateway (構成されている場合) を介して StoreFront™ に送信され、StoreFront™ はその要求を Delivery Controller に送信します。
3. Delivery Controller は要求に利用可能なマシンを見つけ、マシン情報とその他の詳細を StoreFront に送信します。また、StoreFront は Secure Ticket Authority からワンタイムチケットを要求し、受け取ります。
4. StoreFront は ICA ファイルを生成し、Citrix Gateway (構成されている場合) を介してユーザーに送信します。

IFDCD は、完全なプロセス (ステップ 1〜4) にかかる時間を表します。IFDCD 期間は、クライアントが ICA ファイルを受信したときにカウントを停止します。

LPWD は、プロセスの StoreFront コンポーネントです。

IFDCD が高い (ただし LPWD が正常である) 場合、起動のサーバー側処理は成功しましたが、クライアントデバイスと StoreFront の間に通信の問題がありました。これは、2つのマシン間のネットワークの問題に起因します。したがって、まず潜在的なネットワークの問題をトラブルシューティングできます。

起動ページ WEB サーバー期間 (LPWD)

これは、StoreFront で起動ページ (launch.aspx) を処理するのにかかる時間です。LPWD が高い場合、StoreFront にボトルネックがある可能性があります。

考えられる原因は次のとおりです。

- StoreFrontの負荷が高い。Internet Information Services (IIS) のログや監視ツール、タスクマネージャー、パフォーマンスモニターなどを確認して、遅延の原因を特定してください。
- StoreFrontがDelivery Controllerなどの他のコンポーネントとの通信に問題がある。StoreFrontとDelivery Controller間のネットワーク接続が遅いか、一部のDelivery Controllerがダウンしているか、過負荷になっていないかを確認してください。

名前解決WEBサーバー期間 (NRWD)

これは、Delivery Controllerが公開アプリケーション/デスクトップの名前をVDAマシンのIPアドレスに解決するのにかかる時間です。

このメトリックが高い場合、Delivery Controllerが公開アプリケーションの名前をIPアドレスに解決するのに時間がかかっていることを示します。

可能性のある原因としては、クライアント側の問題、Delivery Controllerの過負荷などのDelivery Controllerの問題、またはそれらの間のネットワークリンクの問題が挙げられます。

チケット応答WEBサーバー期間 (TRWD)

この期間は、Secure Ticket Authority (STA) サーバーまたはDelivery Controllerからチケットを取得するのにかかる時間を示します（必要な場合）。この期間が長い場合、STAサーバーまたはDelivery Controllerが過負荷になっていることを示します。

セッション検索クライアント期間 (SLCD)

この期間は、要求された公開アプリケーションをホストするためにすべてのセッションを照会するのにかかる時間を表します。既存のセッションがアプリケーション起動要求を処理できるかどうかを判断するために、クライアントでチェックが実行されます。使用される方法は、セッションが新規か共有かによって異なります。

セッション作成クライアント期間 (SCCD)

この期間は、wfica32.exe（または同様の同等ファイル）が起動されてから接続が確立されるまでの、セッション作成にかかる時間を表します。

VDAセッション起動フェーズ

セッション起動VDA期間 (SSVD)

この期間は、VDAが起動操作全体を実行するのにかかる時間を含む、高レベルのサーバー側接続起動メトリックです。このメトリックが高い場合、セッション起動時間を増加させるVDAの問題があることを示します。これには、VDAで起動操作全体を実行するのに費やされた時間が含まれます。

資格情報取得VDA期間 (COVD)

VDAがユーザー資格情報を取得するのにかかる時間。

ユーザーが時間内に資格情報を提供できない場合、この期間は人為的に増加する可能性があります。そのため、VDA起動期間には含まれません。この時間は、手動ログインが使用され、サーバー側の資格情報ダイアログが表示される場合（またはログイン開始前に法的通知が表示される場合）にのみ重要となる可能性があります。

資格情報認証VDA期間 (CAVD)

これは、VDAが認証プロバイダーに対してユーザーの資格情報を認証するのにかかる時間です。認証プロバイダーは、Kerberos、Active Directory、またはセキュリティサポートプロバイダーインターフェイス (SSPI) のいずれかです。

グループポリシーVDA期間 (GPVD)

この期間は、ログオン中にグループポリシーオブジェクトを適用するのにかかる時間です。

ログオンスクリプト実行VDA期間 (LSVD)

これは、VDAがユーザーのログオンスクリプトを実行するのにかかる時間です。

ユーザーまたはグループのログオンスクリプトを非同期にすることを検討してください。アプリケーション互換性スクリプトを最適化するか、代わりに環境変数を使用することを検討してください。

プロファイルロードVDA期間 (PLVD)

これは、VDAがユーザープロファイルをロードするのにかかる時間です。

この期間が長い場合は、ユーザープロファイル構成を検討してください。ローミングプロファイルのサイズと場所は、セッションの起動が遅くなる原因となります。ユーザーがターミナルサービスローミングプロファイルとホームフォルダーが有効になっているセッションにログオンすると、ローミングプロファイルの内容と当該フォルダーへのアクセスがログオン中にマッピングされます。これには追加のリソースが必要です。場合によっては、CPU使用率を大幅に消費することがあります。この問題を軽減するために、リダイレクトされた個人フォルダーとともに**ターミナルサービスホーム**フォルダーを使用することを検討してください。一般に、Citrix環境でユーザープロファイルを管理するには、Citrix Profile Managementの使用を検討してください。Citrix Profile Managementを使用しており、ログオン時間が遅い場合は、アンチウイルスソフトウェアがCitrix Profile Managementツールをブロックしていないか確認してください。

プリンター作成VDA期間 (PCVD)

これは、VDAがユーザーのクライアントプリンターを同期的にマッピングするのにかかる時間です。プリンター作成が非同期で実行されるように構成されている場合、セッション起動の完了に影響しないため、PCVDの値は記録されません。

プリンターのマッピングに過剰な時間が費やされるのは、多くの場合、プリンターの自動作成ポリシー設定が原因です。ユーザーのクライアントデバイスにローカルで追加されたプリンターの数と、印刷構成がセッションの開始時間に直接影響を与える可能性があります。セッションが開始されると、Citrix Virtual Apps and Desktops™ は、クライアントデバイス上のローカルにマップされたすべてのプリンターを作成する必要があります。特にユーザーが多数のローカルプリンターを持っている場合は、作成されるプリンターの数を減らすために、印刷ポリシーを再構成することを検討してください。これを行うには、Delivery Controller および Citrix Virtual Apps and Desktops でプリンターの自動作成ポリシーを編集します。

ドライブマッピングVDA期間 (DMVD)

これは、VDAがユーザーのクライアントドライブ、デバイス、ポートをマッピングするのにかかる時間です。

ICAプロトコルを最適化し、セッション全体のパフォーマンスを向上させるために、ベースポリシーに未使用の仮想チャネル（オーディオやCOMポートのマッピングなど）を無効にする設定が含まれていることを確認してください。

アプリケーション/デスクトップ起動VDA期間 (ALVD/DLVD)

このフェーズは、UserinitとShellの期間の組み合わせです。ユーザーがWindowsマシンにログオンすると、winlogonがuserinit.exeを実行します。Userinit.exeはログオンスクリプトを実行し、ネットワーク接続を再確立してからExplorer.exeを開始します。Userinitは、userinit.exeの開始から仮想デスクトップまたはアプリケーションのユーザーインターフェイスの開始までの期間を表します。Shell期間は、ユーザーインターフェイスの初期化からユーザーがキーボードとマウスの制御を受け取るまでの時間です。

セッション作成VDA期間 (SCVD)

この時間には、VDAでのセッション作成時間におけるその他の遅延が含まれます。

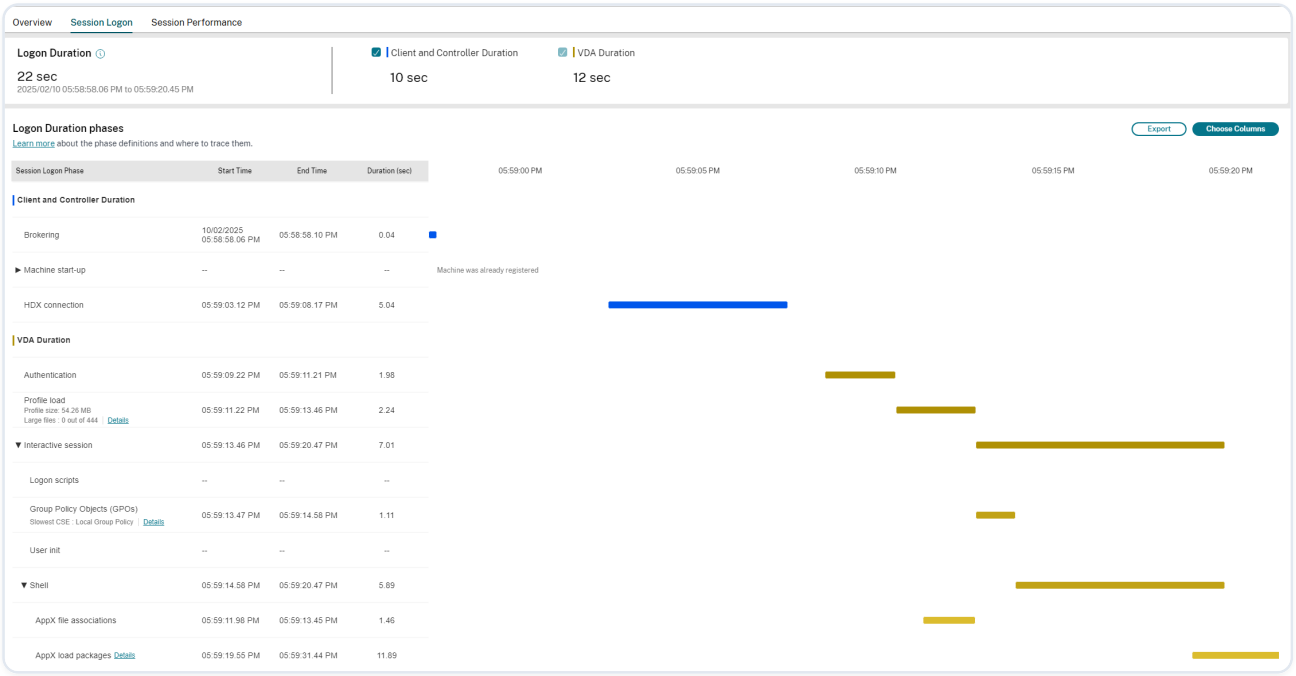
ユーザーログオンの問題を診断する

「**ユーザー詳細**」ビュー > 「**セッションログオン**」タブには、セッションログオンプロセスの包括的なビューが表示されます。このタブには、合計ログオン時間、クライアントとコントローラーの時間、およびVDAの時間が表示されます。このデータを使用して、ユーザーログオンの問題をトラブルシューティングします。

ログオン期間は、HDX を使用したデスクトップまたはアプリへの初回接続の場合にのみ測定されます。このデータには、リモートデスクトッププロトコルで接続しようとしているユーザーや、切断されたセッションから再接続しているユーザーは含まれません。具体的には、ユーザーが最初に非 HDX プロトコルを使用して接続し、HDX を使用して再接続する場合、ログオン期間は測定されません。

ユーザーがCitrix Virtual Apps and Desktops™にログオンすると、Monitor Serviceはログオンプロセスのフェーズを追跡します。フェーズは、ユーザーがCitrix Workspace™アプリから接続した時点から、アプリまたはデスクトップが使用可能になるまでの時間で始まります。

「**セッションログオン**」タブには、さまざまなログオンフェーズがプロットされたログオン時間フェーズチャートが含まれています。ログオン時間は、接続を確立し、Delivery Controller™からアプリまたはデスクトップを取得するのに費やされた時間と、仮想アプリまたはデスクトップに認証してログオンするのに費やされた時間を表します。時間の情報は秒（または秒の端数）で表示されます。



ログオン期間フェーズチャートは、さまざまなログオンフェーズとその開始時刻および終了時刻を明確に表示します。このチャートは、個々のログオンフェーズの重複を示します。合計ログオン時間は、個々のログオンフェーズの期間の合計ではない場合があります。これは、個々のフェーズが重複する可能性があり、すべてのログオンフェーズがこの表現の一部ではないためです。また、特定のフェーズは、ユーザーが仮想アプリまたはデスクトップとの対話を開始した後も延長される可能性があり、この期間は全体のログオン期間の一部として測定されません。

このビューを使用して、セッション起動の遅延を引き起こしている特定のログオンフェーズを特定します。各ログオンフェーズの定義と、情報を追跡できるイベントソースは、さらなるトラブルシューティングに役立ちます。チャートにカーソルを合わせると、現在のセッションのフェーズ期間、ユーザーの7日間平均、およびデリバリーグループの7日間平均を含むツールチップが表示されます。この情報は、現在のセッションログオン期間を7日間平均値と比較するのに役立ちます。GPOおよびプロファイルの詳細の場合、サブフェーズ測定にさらにドリルダウンできます。この視覚化は、ログオン期間関連の問題を簡単に理解し、トラブルシューティングするのに役立ちます。

前提条件

ログオン期間データとドリルダウンが表示されるように、次の前提条件が満たされていることを確認してください。

1. VDA に **Citrix User Profile Manager** と **Citrix User Profile Manager WMI Plugin** をインストールします。
2. Citrix Profile Management Service が実行されていることを確認します。
3. XenApp および XenDesktop サイト 7.15 以前の場合、GPO 設定 **レガシー実行リストを処理しない** を無効にします。

4. 対話型セッションのドリルダウンには、監査プロセス追跡を有効にする必要があります。
5. GPO ドリルダウンの場合、グループポリシーの運用ログのサイズを増やします。

> **注:**
>
> - ログオン時間は、デフォルトのWindowsシェル (explorer.exe) でのみサポートされ、カスタムシェルではサポートされません。
> - Remote PC Accessのログオン時間は、Remote PC Accessのインストール中に**Citrix User Profile Manager**と**Citrix User Profile Manager WMI Plugin**が追加コンポーネントとしてインストールされている場合にのみ利用可能です。詳細については、「Remote PC Accessの構成とシーケンスに関する考慮事項」のステップ4を参照してください。

ユーザーログオンの問題をトラブルシューティングする手順

1. 「**ユーザー詳細**」ビュー > 「**セッションログオン**」タブから、ログオン時間チャートを使用してログオン状態をトラブルシューティングします。
   - ユーザーがログオン中の場合、ビューにはログオンのプロセスが反映されます。
   - ユーザーがログオンしている場合、ログオン時間パネルには、ユーザーが現在のセッションにログオンするまでにかかった時間が表示されます。
2. ログオンプロセスのフェーズを検査します。

ログオンプロセスのフェーズ

クライアントとコントローラーの時間

ユーザーがアプリまたはデスクトップアイコンをクリックしてから、キーボードとマウスの制御がエンドユーザーに渡され、セッションと対話できるようになるまでの時間。
ブローカリング
ユーザーに割り当てるデスクトップを決定するまでにかかった時間。
マシンの起動
セッションでマシンの起動が必要だった場合、これは仮想マシンの起動にかかった時間です。以下のサブセクションでは、異なるフェーズで仮想マシンを起動するまでにかかった時間の内訳を示します。

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

折りたたみボタンを使用して、**マシンの起動**の下にあるオプションを折りたたんだり展開したりできます。

HDX接続

クライアントから仮想マシンへのHDX接続の設定に必要な手順を完了するのにかかった時間。

VDAの時間

VDAでセッションを作成するのにかかった時間。

認証

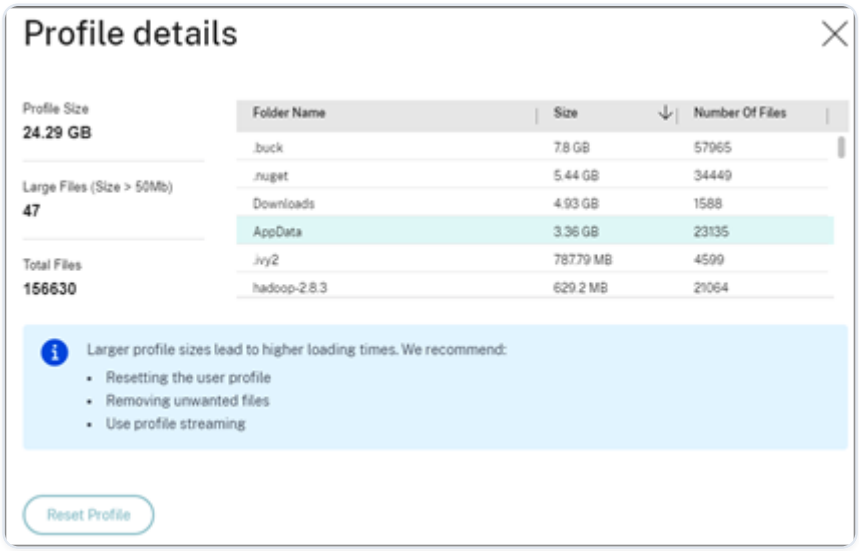
リモートセッションへの認証を完了するのにかかった時間。

プロファイル読み込み

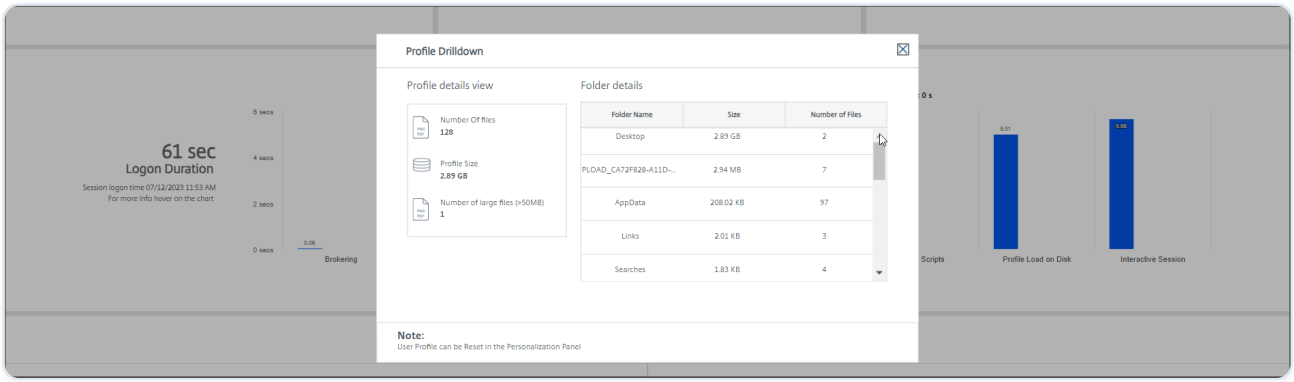
ユーザーまたは仮想マシンにプロファイル設定が構成されている場合、これはプロファイルの読み込みにかかる時間です。

Citrix Profile ManagementとFSLogixが構成されている場合、プロファイルロードバーには、Citrix Profile ManagementとFSLogixがユーザープロファイルを処理するのにかかった時間が含まれます。この情報は、管理者が高いプロファイル処理時間の問題をトラブルシューティングするのに役立ちます。Profile ManagementとFSLogixが構成されている場合、プロファイルロードバーは増加した時間を表示します。この増加はこの機能強化によって引き起こされるものであり、パフォーマンスの低下を反映するものではありません。この機能強化は、VDAバージョン2407以降で利用可能です。

プロファイルロードバーにカーソルを合わせると、現在のセッションのユーザープロファイルの詳細を示すツールチップが表示されます。



「**詳細**」をクリックして、プロファイルルートフォルダー（例：C:/Users/username）内の個々のフォルダー、そのサイズ、およびファイル数（ネストされたフォルダー内のファイルを含む）をさらにドリルダウンします。



プロファイルのドリルダウンは、Delivery Controllerバージョン7 1811以降およびVDA 1811以降で利用できます。プロファイルのドリルダウン情報を使用して、高いプロファイルロード時間に関連する問題を解決できます。次のことができます。

- ユーザープロファイルをリセットする
- 不要な大きなファイルを削除してプロファイルを最適化する
- ネットワーク負荷を軽減するためにファイル数を減らす
- プロファイルストリーミングを使用する

デフォルトでは、プロファイルルート内のすべてのフォルダーがドリルダウンに表示されます。フォルダーの表示を非表示にするには、VDAマシンで次のレジストリ値を編集します。

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

1. VDAで、HKEY_LOCAL_MACHINE\Software\Citrix\Director\ に新しいレジストリ値 **ProfileFoldersNameHidden** を追加します。
2. 値を1に設定します。この値はDWORD（32ビット）値である必要があります。これでフォルダー名の表示が無効になります。
3. フォルダー名を再度表示するには、値を0に設定します。

> **注:**

> GPOまたはPowerShellコマンドを使用して、複数のマシンにレジストリ値の変更を適用できます。GPOを使用してレジストリの変更を展開する方法の詳細については、ブログを参照してください。

追加情報

- プロファイルのドリルダウンでは、リダイレクトされたフォルダーは考慮されません。
- ルートフォルダー内のNTUser.datファイルは、エンドユーザーには表示されない場合があります。ただし、これらはプロファイルのドリルダウンに含まれ、**ルートフォルダー**のファイルリストに表示されます。
- AppDataフォルダー内の一部の隠しファイルは、プロファイルのドリルダウンに含まれません。
- ファイル数とプロファイルサイズデータは、特定のWindowsの制限により、パーソナライゼーションパネルのデータと一致しない場合があります。

対話型セッション

インタラクティブセッションとは、ユーザープロファイルがロードされた後、キーボードとマウスの制御をユーザーに「引き渡す」のにかかる時間です。これは通常、ログオンプロセスのすべてのフェーズの中で最も長い期間であり、**インタラクティブセッション期間 = デスクトップ準備完了イベントタイムスタンプ (VDA上のEventId 1000) - ユーザープロファイルロード済みイベントタイムスタンプ (VDA上のEventId 2)** として計算されます。インタラクティブセッションには、Pre-userinit、Userinit、Shellの3つのサブフェーズがあります。インタラクティブセッションにカーソルを合わせると、次のツールチップが表示されます。

- サブフェーズ
- 各サブフェーズにかかる時間
- これらのサブフェーズ間の累積合計時間遅延

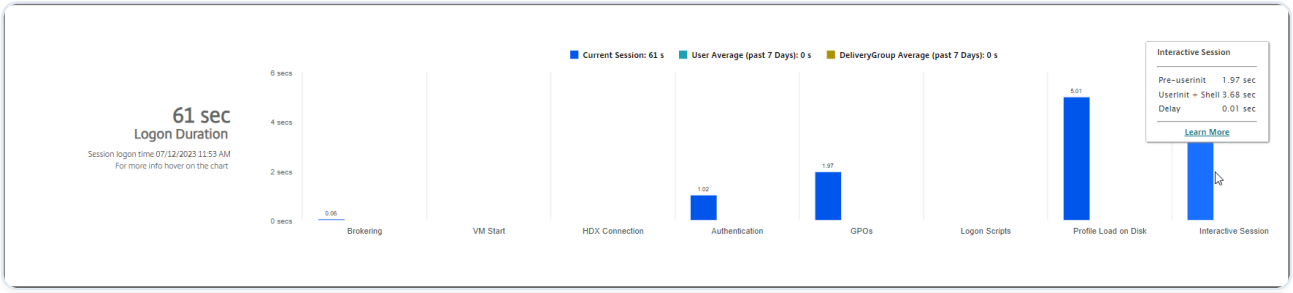
折りたたみ可能なボタンを使用して、**インタラクティブセッション**の下のオプションを折りたたんだり展開したりできます。

> **注:**
>
> この機能はVDA 1811以降で利用できます。7.18より前のサイトでセッションを起動し、その後7.18以降にアップグレードした場合、「サーバーエラーのためドリルダウンが利用できません」というメッセージが表示されます。ただし、アップグレード後にセッションを起動した場合は、エラーメッセージは表示されません。

各サブフェーズの期間を表示するには、VM (VDA) で監査プロセス追跡を有効にします。監査プロセス追跡が無効になっている場合 (デフォルト)、Pre-userinitの期間と、UserinitおよびShellの合計期間が表示されます。グループポリシーオブジェクト (GPO) を使用して監査プロセス追跡を有効にするには、次の手順を実行します。

1. GPOを作成し、GPOエディターを使用して編集します。
2. **コンピューターの構成 > Windows の設定 > セキュリティの設定 > ローカル ポリシー > 監査ポリシー**に移動します。
3. 右側のペインで、**監査プロセス追跡**をダブルクリックします。
4. **成功**を選択し、OKをクリックします。
5. このGPOを必要なVDAまたはグループに適用します。

監査プロセス追跡とその有効化または無効化の詳細については、Microsoftドキュメントの監査プロセス追跡を参照してください。



ユーザー詳細ビューのログオン期間パネル。

- **インタラクティブセッション – Pre-userinit:** グループポリシーオブジェクトとスクリプトと重複するインタラクティブセッションのセグメント。このサブフェーズは、GPOとスクリプトを最適化することで短縮できます。
- **インタラクティブセッション – Userinit:** ユーザーがWindowsマシンにログオンすると、Winlogonはuserinit.exeを実行します。Userinit.exeはログオンスクリプトを実行し、ネットワーク接続を再確立してから、Windowsユーザーインターフェイスであるexplorer.exeを起動します。インタラクティブセッションのこのサブフェーズは、Userinit.exeの開始から仮想デスクトップまたはアプリケーションのユーザーインターフェイスの開始までの期間を表します。
- **インタラクティブセッション – Shell:** 前のフェーズで、UserinitはWindowsユーザーインターフェイスの初期化を開始します。Shellサブフェーズは、ユーザーインターフェイスの初期化からユーザーがキーボードとマウスの制御を受け取るまでの期間を捕捉します。
- **遅延:** これは、**Pre-userinitとUserinit**サブフェーズ間、および**Userinitとシェル**サブフェーズ間の累積時間遅延です。

合計ログオン時間は、これらのフェーズの正確な合計ではありません。たとえば、一部のフェーズは並行して発生し、一部のフェーズでは、合計よりも長いログオン期間につながるより多くの処理が発生します。 合計ログオン時間には、ICAファイルのダウンロードとアプリケーションのICAファイル起動の間の時間であるICA®アイドル時間は含まれません。 アプリケーション起動時にICAファイルを自動的に開くには、ICAファイルのダウンロード時にブラウザがICAファイルを自動的に起動するように設定します。詳細については、CTX804493を参照してください。

> **注:**
>
> ログオン期間グラフは、ログオンフェーズを秒単位で表示します。1秒未満の期間値は、サブ秒値として表示されます。1秒を超える値は、最も近い0.5秒に丸められます。グラフは、Y軸の最大値が200秒になるように設計されています。200秒を超える値は、バーの上に実際の値が表示されます。

ログオンスクリプト
セッションにログオンスクリプトが構成されている場合、これはログオンスクリプトの実行にかかる時間です。
GPO
仮想マシンでグループポリシー設定が有効になっている場合、これはログオン中にグループポリシーオブジェクトを適用するのにかかる時間です。CSE（クライアント側拡張）ごとの各ポリシーの適用にかかる時間のドリルダウンは、GPOバーにカーソルを合わせるとツールチップとして表示されます。



詳細をクリックすると、ポリシーの状態と対応するGPO名を含むテーブルが表示されます。ドリルダウンの時間期間はCSE処理時間のみを表し、合計GPO時間には加算されません。ドリルダウンテーブルをコピーして、さらなるトラブルシューティングやレポートでの使用に役立てることが

できます。ポリシーのGPO時間は、イベントビューアログから取得されます。ログは、運用ログに割り当てられたメモリ（デフォルトサイズは4 MB））に応じて上書きされる可能性があります。運用ログのログサイズを増やす方法の詳細については、Microsoft TechNetの記事「イベントログの構成」を参照してください。

ユーザー初期化

ユーザーがWindowsマシンにログオンすると、Winlogonはuserinit.exeを実行します。Userinit.exeはログオンスクリプトを実行し、ネットワーク接続を再確立してから、Windowsユーザーインターフェイスであるexplorer.exeを起動します。インタラクティブセッションのこのサブフェーズは、Userinit.exeの開始から仮想デスクトップまたはアプリケーションのユーザーインターフェイスの開始までの期間を表します。

シェル

シェルサブフェーズは、ユーザーインターフェイスの初期化から、ユーザーがキーボードとマウスの制御を受け取るまでの期間を捕捉します。

AppXファイルの関連付け

新しいVDAセッション中にAppXファイルを関連付けるのにかかった時間。

AppXパッケージの読み込み

新しいVDAセッション中にAppXパッケージを読み込むのにかかった時間。

> **注:**
>
> 新しいVDAセッション中にAppXパッケージの読み込み時間を収集するには、uberAgentをDirectorと統合する必要があります。詳細については、Citrix uberAgentとDirectorの統合を参照してください。

データのエクスポート

デフォルトのログオン期間フェーズテーブルオプション（セッションログオンフェーズと期間）に加えて、セッションログオンページで以下の列を選択することもできます。

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

以前のデータを.CSVファイルにエクスポートすることもできます。

トラブルシューティングのヒント

グラフ内の異常な値や予期しない値を特定するには、現在のセッションの各フェーズにかかった時間と、このユーザーの過去7日間の平均所要時間、およびこのデリバリーグループ内のすべてのユーザーの過去7日間の平均所要時間を比較します。

必要に応じてエスカレートします。たとえば、**マシンの起動**が遅い場合、問題はハイパーバイザーにある可能性があるため、ハイパーバイザー管理者にエスカレートできます。

以下を含む異常な相違点を調べます。

- 欠落している（現在の）ログオンバー
- 現在の所要時間とこのユーザーの平均所要時間の間の大きな不一致。原因は次のとおりです。
  - 新しいアプリケーションがインストールされた。
  - オペレーティングシステムのアップデートが行われた。
  - 構成変更が行われた。
  - ユーザーのプロファイルサイズが大きい。この場合、プロファイルロードが高い。
- ユーザーのログオン数値（現在の期間と平均期間）とデリバリーグループの平均期間との間に大きな不一致がある場合。

必要に応じて、**再起動**をクリックしてユーザーのログオンプロセスを監視し、**マシンの起動**や**ブローカリング**などの問題をトラブルシューティングします。

セッションパフォーマンスの問題を診断する

ユーザー詳細ページにある**セッションパフォーマンス**タブには、HDX™ユーザーセッション内の問題を特定するのに役立つ、強化されたトラブルシューティングワークフローが用意されています。**セッションのトポロジとパフォーマンスメトリック**パネルは、セッションのコンポーネントビューと複数のパフォーマンスメトリックを単一のビューで関連付け、セッションエクスペリエンスの問題解決にかかる平均時間を短縮します。

セッションパフォーマンスビュー(/en-us/citrix-virtual-apps-desktops/current-release/media/dir-session-performance.png)

エンドツーエンドのネットワークホップビュー

エンドツーエンドのネットワークホップビューは、完全なセッションパスを視覚的に表現し、トラブルシューティングに大きく役立ちます。このビューには、**ユーザー詳細** > **セッションパフォーマンス** > **セッションのトポロジ**からアクセスできます。エンドツーエンドのネットワーク

ホップビューには、接続されたHDXセッションのコンポーネント、メタデータ、リンク、および公開アプリケーションが表示されます。

このビューは、管理者が次のことを行うのに役立ちます。

- セッションのデータフローを理解する。
- 特定のホップにおけるパフォーマンスのボトルネックを特定する。

セッションパフォーマンスメトリック

以下のメトリックは、管理者が特定のセッションのパフォーマンスを理解するのに役立つように、コンテキストに応じて利用できます。エンドツーエンドのネットワークホップビューに表示されるメトリックは、ほぼリアルタイムで利用でき、UIに表示される間隔に基づいて定期的に更新されます。

エンドポイントメトリック

エンドポイントメトリックは、ユーザーエクスペリエンスの「ラストマイル」に関する洞察を提供し、ユーザーの即時環境に関する詳細を明らかにするため、Citrix®セッションパフォーマンスのトラブルシューティングに不可欠です。これらのメトリックは、劣悪なWi-Fi、低いネットワークスループット、エンドポイントデバイスの制限などのローカルなボトルネックを特定し、サーバー側とクライアント側の問題を区別するのに役立ちます。セッションのトポロジ内のメトリックと組み合わせることで全体的なビューを提供することにより、エンドポイントデータはパフォーマンス問題の根本原因の特定を迅速化し、解決を早め、ユーザーエクスペリエンスを向上させます。

Citrix Studioのポリシーを使用して、要件に基づいてリストされたエンドポイントメトリックの収集を有効または無効にします。これらのポリシーは、Citrix管理者がコンプライアンス要件に準拠してメトリックを報告するための詳細な制御を提供します。

ポリシー名	ポリシーの説明	UIメトリック	デフォルト値	値のオプション	VIRTUAL DELIVERY AGENTバージョン
エンドポイント統計間隔	ユーザーエンドポイントからのエンドポイントネットワーク詳細の収集を許可します。このポリ	Wi-Fi信号強度、ネットワークインターフェースタイプ、送受信スループット、リンク速度、ワー	有効	有効または無効。頻度を60秒～3600秒の間で変更するオプション。60秒が推奨値です。	2407以降

ポリシー名	ポリシーの説明	UIメトリック	デフォルト値	値のオプション	VIRTUAL DELIVERY AGENTバージョン
	シーを有効にすることは、他のエンドポイント関連ポリシーが有効になるための前提条件です。	クスペースタイプ、エンドポイントCPU、エンドポイントメモリ、エンドポイントGPU			
エンドポイント位置情報収集	Locusサービスを使用して、ユーザーエンドポイントからエンドポイントの場所とISPの詳細の収集を可能にします - `<https://locus.analytics.cloud.com>`	パブリックIPアドレス、国、都市、およびインターネットサービスプロバイダー。	無効	有効または無効	2411 以降
エンドポイントネットワーク遅延測定間隔	エンドポイントとビーコンホスト間のネットワーク遅延の測定と収集を可能にします - `<https://downloadplugins.citrix.com>`	ネットワーク遅延 (エンドポイントネットワークの詳細内)	無効	有効または無効。頻度を60秒～3600秒の間で変更するオプション。60秒が推奨値です。	2411 以降

注:

Citrix Virtual Apps and Desktops™ 2507以降では、**エンドポイント位置情報収集**ポリシーと**エンドポイントネットワーク遅延測定間隔**ポリシーはデフォルトで無効になっています。そのため、これらのポリシーがStudioで手動で有効にされない限り、関連データはDirectorで利用できません。

すぐに利用できるエンドポイントメトリックは以下のとおりです。

- エンドポイント名
- エンドポイントIP
- エンドポイントOS
- Citrix Workspace™アプリのバージョン

次の表に、サポートされている製品バージョンに依存するメトリックを示します。

機能名	UIパラメーター	VDA WINDOWSバージョン	VDA MACバージョン	VDA LINUXバージョン	CITRIX WORKSPACE APP FOR WINDOWSのバージョン	CITRIX WORKSPACE APP FOR MACのバージョン	CITRIX WORKSPACE APP LINUX版バージョン	CITRIX WORKSPACE APP FOR HTML5バージョン	CITRIX WORKSPACE APP FOR CHROME OSバージョン
エンドポイントのネットワーク詳細	ネットワークインターフェイスの種類	2407以降	NA	NA	2405.10以降	2409以降	2408以降	2411以降	2411以降

機能名	UIパラメーター	VDA WINDOWSバージョン	VDA MACバージョン	VDA LINUXバージョン	CITRIX WORKSPACE APP FOR WINDOWSのバージョン	CITRIX WORKSPACE APP FOR MACのバージョン	CITRIX WORKSPACE APP LINUX版バージョン	CITRIX WORKSPACE APP FOR HTML5バージョン	CITRIX WORKSPACE APP FOR CHROME OSバージョン
	信号強度	2407以降	NA	NA	2405.10以降	2409以降	2408以降	該当なし	該当なし
	エンドポイントスループット(受信、送信)	2407以降	NA	NA	2405.10以降	2409以降	2408以降	該当なし	該当なし
	リンク速度	2407以降	NA	NA	2405.10以降	2409以降	2408以降	2411以降	2411以降
	エンドポイントのパブリックIPアドレス	2411以降	NA	NA	2409以降	2409以降	2408以降	2411以降	2411以降

機能名	UIパラメーター	VDA WINDOWSバージョン	VDA MACバージョン	VDA LINUXバージョン	CITRIX WORKSPACE APP FOR WINDOWSのバージョン	CITRIX WORKSPACE APP FOR MACのバージョン	CITRIX WORKSPACE APP LINUX版バージョン	CITRIX WORKSPACE APP FOR HTML5バージョン	CITRIX WORKSPACE APP FOR CHROME OSバージョン
	エンドポイントの都市、エンドポイントの国	2411以降	NA	NA	2409以降	2409以降	2408以降	2411以降	2411以降
	インターネットサービスプロバイダー	2411以降	NA	NA	2409以降	2409以降	2408以降	2411以降	2411以降
	ワークスペースの種類	2411以降	NA	NA	2409以降	2409以降	2408以降	2411以降	2411以降
	アクセス	2411以降	NA	NA	2409以降	2409以降	2408以降	2411以降	2411以降

機能名	UIパラメーター	VDA WINDOWS バージョン	VDA MAC バージョン	VDA LINUX バージョン	CITRIX WORKSPACE APP FOR WINDOWS のバージョン	CITRIX WORKSPACE APP FOR MAC のバージョン	CITRIX WORKSPACE APP LINUX版バージョン	CITRIX WORKSPACE APP FOR HTML5 バージョン	CITRIX WORKSPACE APP FOR CHROME OS バージョン
	タイプ (Workspace / StoreFront 経由)								
	エンドポイント CPU	2411 以降	NA	NA	2409 以降	2409 以降	2408 以降	該当なし	2411 以降
	エンドポイントメモリ	2411 以降	NA	NA	2409 以降	2409 以降	2408 以降	該当なし	2411 以降
	エンドポイント GPU	2411 以降	NA	NA	2409 以降	2409 以降	2408 以降	該当なし	該当なし
	ネットワー	2411 以降	NA	NA	2409 以降	2409 以降	2408 以降	2411 以降	2411 以降

機能名	UIパラメーター	VDA WINDOWSバージョン	VDA MACバージョン	VDA LINUXバージョン	CITRIX WORKSPACE APP FOR WINDOWSのバージョン	CITRIX WORKSPACE APP FOR MACのバージョン	CITRIX WORKSPACE APP LINUX版バージョン	CITRIX WORKSPACE APP FOR HTML5バージョン	CITRIX WORKSPACE APP FOR CHROME OSバージョン
	ク遅延								

データ定義:

UIパラメーター	説明
エンドポイント名	セッションに使用されるユーザーのエンドポイントデバイスの名前。
エンドポイントIP	Virtual Delivery Agent (VDA) で利用可能なエンドポイントのIPアドレス。エンドポイントデバイスのプライベートIPアドレスまたはパブリックIPアドレスが含まれる場合があります。
エンドポイントOS	エンドポイントデバイスのオペレーティングシステム
Citrix Workspaceアプリのバージョン	インストールされているCitrix Workspaceアプリのバージョン
信号強度	ワイヤレス信号の品質と強度を表示します。
エンドポイントスループット (受信、送信)	ネットワークインターフェイスへのデータ転送速度と、ネットワークインターフェイスからのデータ転送速度を示します。エンドポイントで観測されるアップロードおよびダウンロードのインターネット速度に類似しています。

UIパラメーター	説明
リンク速度	イーサネット、Wi-Fi、セルラーなどのネットワーク接続の種類を指定します。
ネットワークインターフェイスの種類	ネットワーク接続の最大データ転送速度を表します。
エンドポイントのパブリックIPアドレス	インターネットサービスプロバイダーによってデバイスに割り当てられた外部IPアドレス。
エンドポイントの都市、エンドポイントの国	デバイスの地理的な場所（国と都市を含む）。
インターネットサービスプロバイダー	エンドユーザーデバイスにインターネットアクセスを提供する会社の名前。
ワークスペースの種類	使用されているワークスペースの種類（Citrix WorkspaceアプリまたはWebブラウザ）。
アクセスタイプ (Workspace / StoreFront経由)	Citrix WorkspaceまたはStoreFrontのいずれかを通じてリソースにアクセスする方法。
エンドポイントCPU	現在使用されているCPUリソースの割合。
エンドポイントメモリ	現在使用されているメモリリソースの割合。
エンドポイントGPU	現在使用されているGPUリソースの割合。
ネットワーク遅延テスト	ネットワークで発生する時間遅延（ミリ秒単位で測定）。

ネットワークメトリック

Citrixセッションのパフォーマンスと安定性は基盤となるネットワークの状態に大きく依存するため、ネットワークメトリックはCitrixセッションのトラブルシューティングにとって重要です。ローカルアプリケーションとは異なり、Citrixセッションはネットワークを介してインタラクティブなデスクトップまたはアプリケーションエクスペリエンスをストリーミングするため、ネットワークの不安定性やボトルネックはユーザーのパフォーマンス認識に直接影響します。

Citrix Studioのポリシーを使用して、要件に基づいてリストされているネットワークメトリックの収集を有効または無効にします。これらのポリシーは、Citrix管理者に、コンプライアンス要件に従ってメトリックを報告するためのきめ細かな制御を提供します。

ポリシー名	ポリシーの説明	UIメトリック	デフォルト値	値のオプション	VIRTUAL DELIVERY AGENTバージョン
ネットワーク テレメトリ	ユーザーエンドポイントとバックエンドコンポーネント間のネットワーク詳細の収集を許可します。	Citrix Gateway および Citrix Gateway サービスに関するすべての HDX Insights メトリック	無効	有効または無効。頻度を60秒～3600秒の間で変更するオプション。60秒が推奨値です。	Gateway サービスの場合は 2411 以降。Citrix Gateway の場合は 2503 以降。

シトリックス ゲートウェイ サービス

次の表に、サポートされている製品バージョンに依存するメトリックを示します。

機能名	UIパラメーター	WINDOWS VDA のバージョン	MAC VDA のバージョン	LINUX VDA バージョン	CITRIX WORKSPACE APP FOR WINDOWS のバージョン	CITRIX WORKSPACE APP FOR MAC のバージョン	CITRIX WORKSPACE APP LINUX版バージョン	CITRIX WORKSPACE APP FOR HTML5 バージョン	CITRIX WORKSPACE APP FOR CHROME OS バージョン
ネットワークメトリック	L7 サーバー遅延	2411 以降	2507 以降	2507 以降	2409 以降	2505 以降	2505 以降	NA	NA
	L7 クライアント遅延	2411 以降	2507 以降	2507 以降	2409 以降	2505 以降	2505 以降	NA	NA

機能名	UIパラメーター	WINDOWS VDAのバージョン	MAC VDAのバージョン	LINUX VDAバージョン	CITRIX WORKSPACE APP FOR WINDOWSのバージョン	CITRIX WORKSPACE APP FOR MACのバージョン	CITRIX WORKSPACE APP LINUX版バージョン	CITRIX WORKSPACE APP FOR HTML5バージョン	CITRIX WORKSPACE APP FOR CHROME OSバージョン
	クライアント側の再送信 注: TCPセッションでのみ利用可能	2411以降	2507以降	2507以降	2409以降	2505以降	2505以降	NA	NA
	スループット	2411以降	NA	NA	2409以降	2505以降	2505以降	NA	NA

シトリックス ゲートウェイ

次の表に、サポートされている製品バージョンに依存するメトリックを示します。

機能名	UIパラメーター	CITRIX GATEWAYのバージョン	WINDOWS VDAのバージョン	MACのバージョン	LINUXのバージョン	CITRIX WORKSPACE APP FOR WINDOWSのバージョン	CITRIX WORKSPACE APP FOR MACのバージョン	CITRIX WORKSPACE APP LINUX版バージョン	CITRIX WORKSPACE APP FOR HTML5バージョン	CITRIX WORKSPACE APP FOR CHROME OSバージョン
ネットワークメトリック	WAN遅延	Netscaler 14.1-47.46以降	2503以降	2507以降	2507以降	2503以降	2505以降	2505以降	NA	NA
	DC遅延	Netscaler 14.1-47.46以降	2503以降	2507以降	2507以降	2503以降	2505以降	2505以降	NA	NA
	サーバー側再送信	Netscaler 14.1-47.46以降	2503以降	2507以降	2507以降	2503以降	2505以降	2505以降	NA	NA
	クライアント	Netscaler 14.1	2503以降	2507以降	2507以降	2503以降	2505以降	2505以降	NA	NA

機能名	UIパラメーター	CITRIX GATEWAYのバージョン	WINDOWS VDAのバージョン	MACのバージョン	LINUXのバージョン	CITRIX WORKSPACE APP FOR WINDOWSのバージョン	CITRIX WORKSPACE APP FOR MACのバージョン	CITRIX WORKSPACE APP LINUX版バージョン	CITRIX WORKSPACE APP FOR HTML5バージョン	CITRIX WORKSPACE APP FOR CHROME OSバージョン
	側再送信	-47.46以降								
	L7サーバー遅延	Netscaler 14.1-47.46以降	2503以降	2507以降	2507以降	2503以降	2505以降	2505以降	NA	NA
	L7クライアント遅延	Netscaler 14.1-47.46以降	2503以降	2507以降	2507以降	2503以降	2505以降	2505以降	NA	NA
	クライアント側のゼロウィンドウサイズ	Netscaler 14.1-47.46以降	2503以降	2507以降	2507以降	2503以降	2505以降	2505以降	NA	NA

機能名	UIパラメーター	CITRIX GATEWAYのバージョン	WINDOWS VDAのバージョン	MACのバージョン	LINUXのバージョン	CITRIX WORKSPACE APP FOR WINDOWSのバージョン	CITRIX WORKSPACE APP FOR MACのバージョン	CITRIX WORKSPACE APP LINUX版バージョン	CITRIX WORKSPACE APP FOR HTML5バージョン	CITRIX WORKSPACE APP FOR CHROME OSバージョン
	イベント									
	クライアント側の高速RTO	Netscaler 14.1-47.46以降	2503以降	2507以降	2507以降	2503以降	2505以降	2505以降	NA	NA
	サーバー側のゼロウィンドウサイズイベント	Netscaler 14.1-47.46以降	2503以降	2507以降	2507以降	2503以降	2505以降	2505以降	NA	NA
	サーバー側高速RTO	Netscaler 14.1-47.	2503以降	2507以降	2507以降	2503以降	2505以降	2505以降	NA	NA

機能名	UIパラメーター	CITRIX GATEWAY のバージョン	WINDOWS VDA のバージョン	MAC のバージョン	LINUX のバージョン	CITRIX WORKSPACE APP FOR WINDOWS のバージョン	CITRIX WORKSPACE APP FOR MAC のバージョン	CITRIX WORKSPACE APP LINUX 版バージョン	CITRIX WORKSPACE APP FOR HTML5 バージョン	CITRIX WORKSPACE APP FOR CHROMEOS バージョン
		46 以降								

データ定義:

UIパラメーター	説明
WAN 遅延	NetScaler® からエンドユーザーまでの、ネットワークのクライアント側によって引き起こされる遅延。
DC 遅延	NetScaler からバックエンドサーバーまでの、ネットワークのサーバー側によって引き起こされる遅延。
L7 クライアント遅延	ICA® クライアントと NetScaler インスタンス間で観測される平均 L7 遅延。このメトリックは、配信パスに存在する非 Citrix デバイスで役立ちます。
L7 サーバー遅延	NetScaler デバイスと Citrix Virtual App 間で観測される平均 L7 遅延。このメトリックは、配信パスに非 Citrix デバイスが存在する場合に役立ちます。
クライアントの再送信	NetScalerとエンドユーザー間の接続で再送信されたパケットの数。このメトリックの値が高い場合、再送信による帯域幅の使用率が高

UIパラメーター	説明
	いことを示しますが、必ずしもユーザーエクスペリエンスが悪いことを意味するわけではありません。注：Gatewayサービスを使用するセッションの場合、クライアントの再送信はTCPセッションでのみ利用可能です。
サーバー側の再送信	NetScalerとバックエンドサーバー間の接続で再送信されたパケットの数。
クライアント側のゼロウィンドウ数	クライアントがゼロTCPウィンドウをアドバタイズした回数。
サーバー側のゼロウィンドウ数	サーバーがゼロTCPウィンドウをアドバタイズした回数。

VDAメトリック

機能名	UIパラメーター	WINDOWS VDAのバージョン	MACのバージョン	LINUXのバージョン	CITRIX WORKSPACE APP FOR WINDOWSのバージョン	CITRIX WORKSPACE APP FOR MACのバージョン	CITRIX WORKSPACE APP LINUX版バージョン	CITRIX WORKSPACE APP FOR HTML5バージョン	CITRIX WORKSPACE APP FOR CHROME OSバージョン
VDAメトリック	VDA CPU	2511以降	NA	NA	2503以降	2503以降	2503以降	NA	NA
	VDAメモリ	2511以降	NA	NA	2503以降	2503以降	2503以降	NA	NA
	VDAディスクIOPS	2511以降	NA	NA	2503以降	2503以降	2503以降	NA	NA

機能名	UIパラメーター	WINDOWS VDAのバージョン	MACのバージョン	LINUXのバージョン	CITRIX WORKSPACE APP FOR WINDOWSのバージョン	CITRIX WORKSPACE APP FOR MACのバージョン	CITRIX WORKSPACE APP LINUX版バージョン	CITRIX WORKSPACE APP FOR HTML5バージョン	CITRIX WORKSPACE APP FOR CHROME OSバージョン
	VDAディスク遅延	2511以降	NA	NA	2503以降	2503以降	2503以降	NA	NA

HDXメトリック

HDXメトリックは、ユーザーの仮想エクスペリエンスの品質を理解し、トラブルシューティングを行う上で不可欠です。これらのメトリックは、仮想セッションを提供するICA/HDXプロトコルのパフォーマンスを直接測定します。

注:

ICAメトリックは、Citrix Workspace app for Windowsバージョン2405.10以降、およびCitrix Virtual Apps and Desktops 2407以降で利用可能です。ただし、データの更新と修正は最新バージョンで提供されています。各データポイントの推奨バージョンについては、以下の表を参照してください。

機能名	UIパラメーター	WINDOWS VDA のバージョン	MAC VDA のバージョン	LINUX VDA バージョン	CITRIX WORKSPACE APP FOR WINDOWS のバージョン	CITRIX WORKSPACE APP FOR MAC のバージョン	CITRIX WORKSPACE APP LINUX版 バージョン	CITRIX WORKSPACE APP FOR HTML5 バージョン
ICA メトリック	ICA RTT	2507 以降	NA	NA	2503 以降	2503 以降	2503 以降	2503 以降
	ネットワーク遅延	2507 以降	NA	NA	2503 以降	2503 以降	2503 以降	2503 以降
	HDX 接続タイプ	2411 以降	NA	NA	2411 以降	2411 以降	2411 以降	2411 以降
	プロトコル	2411 以降	NA	NA	2411 以降	2411 以降	2411 以降	2411 以降
	EDT MTU	2411 以降	NA	NA	2411 以降	2411 以降	2411 以降	2411 以降

データ定義:

UIパラメーター	説明
ICA RTT	ユーザーのアクションから画面の応答までの時間を測定します。Citrix Virtual Apps and Desktops バージョン 2507 以降では、Thinwire RTT カウンターがこのメトリックを表します。以前のバージョンでは、引き続き EUEM RTT を使用します。

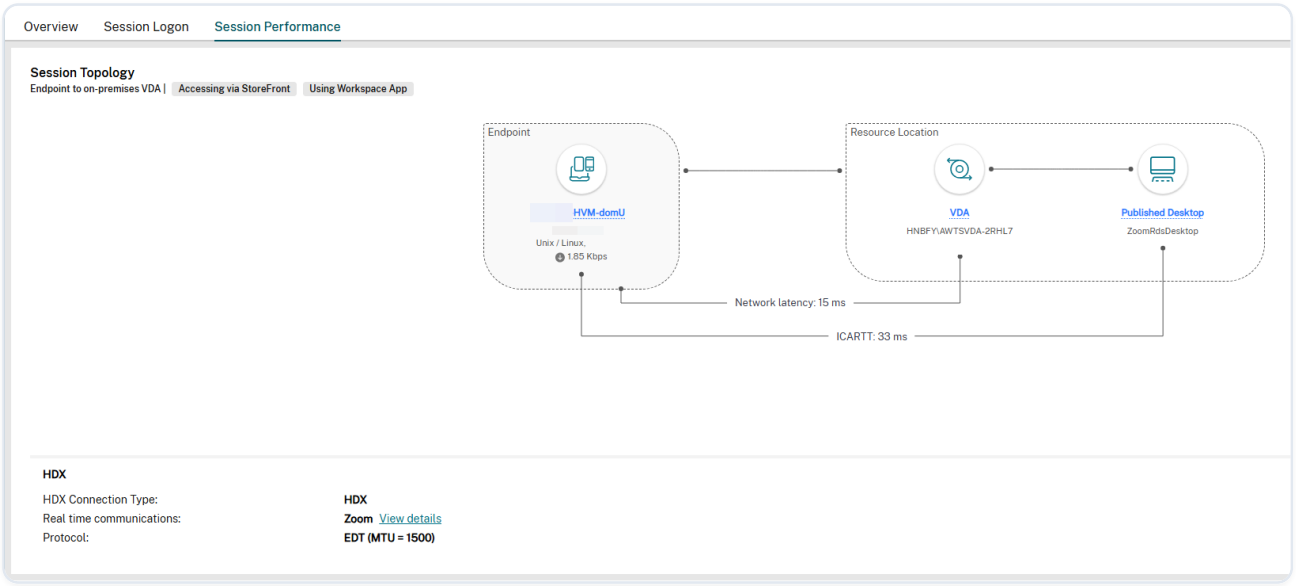
UIパラメーター	説明
ネットワーク遅延	ネットワーク遅延と潜在的な速度低下を示します。Citrix Virtual Apps and Desktops バージョン 2503 以降では、クライアント側とサーバー側の遅延の合計として定義されます。以前のバージョンでは、VDA で報告される HDX 遅延を引き続き使用します。
HDX 接続タイプ	ユーザーセッションの HDX 接続タイプ。
プロトコル	ユーザーセッションに使用される基盤となるプロトコル。値は*TCP*または*EDT*です。
EDT MTU	MTU（最大伝送単位）は、ネットワークインターフェイスがフラグメント化することなく送信できるパケットの最大サイズ（バイト単位）です。EDT MTUは、ユーザーのEDTセッション用に確立されたMTUを表します。

リアルタイム通信の最適化の可視性
セッショントポロジは、Citrixセッション内のMicrosoft Teams、Zoom、WebExなどのリアルタイム通信（RTC）アプリケーションの最適化ステータスに関する包括的な可視性を提供します。アプリケーションが最適化されているかどうかを特定し、最適なパフォーマンスを妨げる不足しているコンポーネント（必要なプラグイン、プラグイン管理、プラットフォーム固有の制限など）を識別します。

利点:

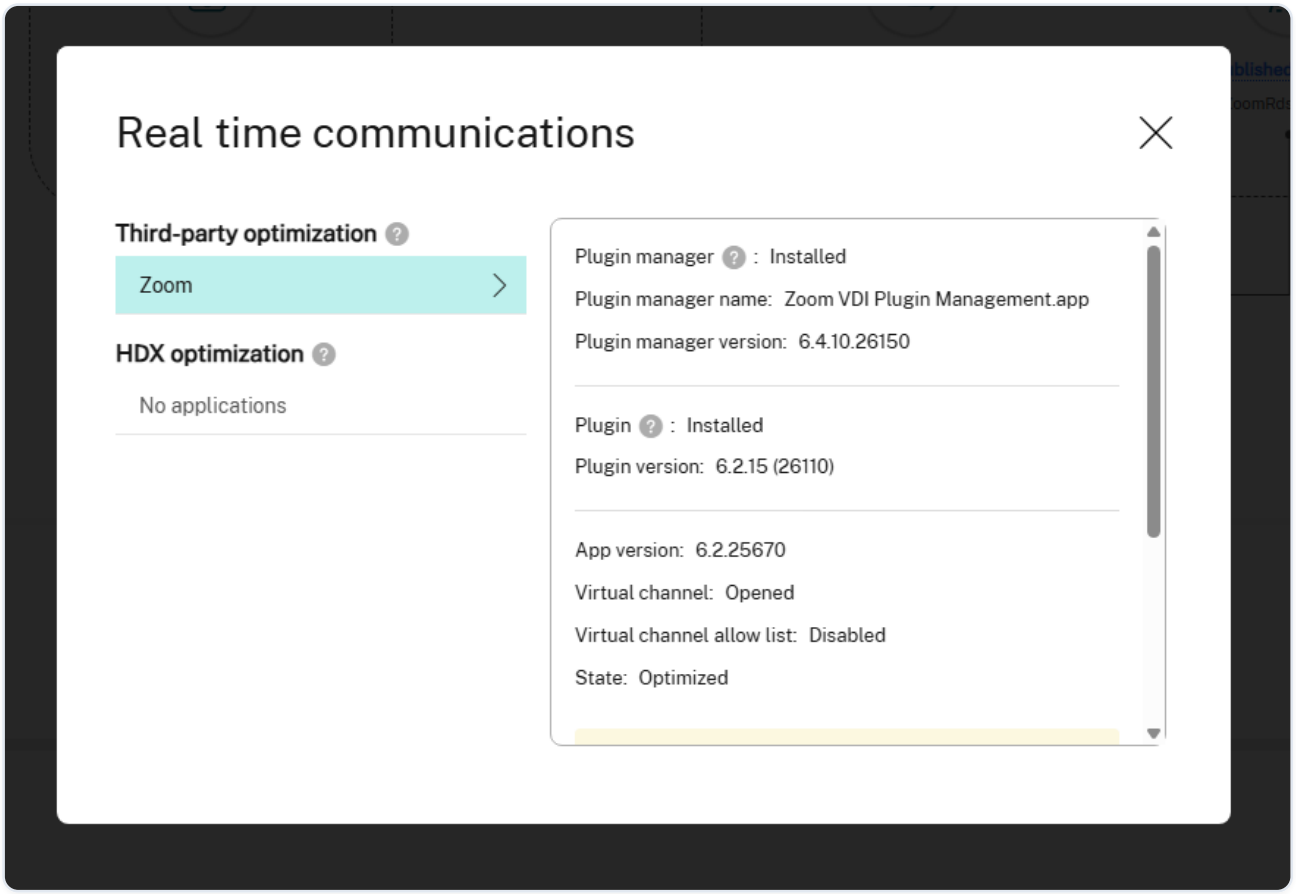
- 顧客はRTCアプリケーションの最適化に関して明確な保証を得られ、セッションが本当に最適化されているかどうかの推測を排除できます。
- 不足しているコンポーネントに関する直接的な洞察により、問題を事前に解決し、完全な最適化を実現できます。
- トラブルシューティングの高速化により、重要な通信ツールのユーザーエクスペリエンスが向上します。

セッショントポロジの**リアルタイム通信**フィールドを使用して、各アプリケーションの最適化の詳細を表示します。



サードパーティ製の最適化されたアプリケーションは、Citrixテクノロジを使用して仮想チャネルを作成しますが、その他の構成と設定はアプリケーションベンダーが管理します。最適化はベンダーが所有するソリューションに依存します。

セッショントポロジ画面の**リアルタイム通信**フィールドの横にある**詳細の表示**リンクをクリックします。次の画面が表示されます。



HDX最適化アプリケーションはCitrix仮想チャネルを使用し、Citrixの構成と設定によって直接影響を受けます。

「**リアルタイム通信**」画面で「**HDX最適化**」セクションをクリックします。次の画像が表示されます。

MS Teamsリアルタイム通信(/en-us/citrix-daas/media/msteams-real-time-opt.png)

リアルタイム通信の詳細は5分ごとに更新されます。次の表は、サードパーティの最適化に依存するアプリケーションで利用可能な詳細を示しています。完全な可視性を得るには、サポートされている製品バージョンを使用していることを確認してください。

注:

- Microsoft Teams Slimcore最適化は、公開されたデスクトップと、ベンダーサポートに従ってNew Teamsでのみ利用可能です。
- Zoomの場合、プラグインの詳細と最適化の状態を取得するためのベンダー変更はバージョン6.3.10以降で利用可能です。詳細については、Zoomドキュメントを参照してください。

次の表に、Citrix HDX最適化に依存するアプリケーションで利用可能な詳細を示します。完全な可視性を得るには、サポートされている製品バージョンを使用していることを確認してください。

機能名	UIパラメーター	VIRTUAL DELIVERY AGENTバージョン	CITRIX WORKSPACE APP FOR WINDOWS のバージョン	CITRIX WORKSPACE APP FOR MAC のバージョン	CITRIX WORKSPACE APP LINUX版 バージョン
Microsoft Teams スリムコア	プラグインマネージャー、プラグインマネージャー名、プラグインマネージャーバージョン	2503	2503	ベンダーによってサポートされていません	ベンダーによってサポートされていません
	アプリバージョン、仮想チャネ	2503	2402	ベンダーによってサ	ベンダーによってサ

機能名	UIパラメーター	VIRTUAL DELIVERY AGENTバージョン	CITRIX WORKSPACE APP FOR WINDOWS のバージョン	CITRIX WORKSPACE APP FOR MAC のバージョン	CITRIX WORKSPACE APP LINUX版 バージョン
	ル、仮想チャネル許可リスト			ポートされていません	ポートされていません
	プラグイン、プラグインバージョン、状態	2507	2503	ベンダーによってサポートされていません	ベンダーによってサポートされていません
ズーム	プラグインマネージャー、プラグインマネージャー名、プラグインマネージャーバージョン	2507	2503	2505	プラグインが利用できません
	アプリバージョン、仮想チャネル、仮想チャネル許可リスト	2507	2402	2402	2402
	プラグイン、プラグインバージョン、状態	2507	2503	2505	プラグイン利用不可
ウェブエックス	プラグインマネージャー、プラグインマネージャー	2507	2503	プラグイン利用不可	プラグイン利用不可

機能名	UIパラメーター	VIRTUAL DELIVERY AGENTバージョン	CITRIX WORKSPACE APP FOR WINDOWS のバージョン	CITRIX WORKSPACE APP FOR MAC のバージョン	CITRIX WORKSPACE APP LINUX版 バージョン
	名、プラグインマネージャーバージョン				
	アプリバージョン、仮想チャネル、仮想チャネル許可リスト	2507	2402	2402	2402

次の表に、Citrix HDX最適化に依存するアプリケーションで利用可能な詳細を示します。完全な可視性を得るには、サポートされている製品バージョンを使用していることを確認してください。

機能名	UIパラメーター	VIRTUAL DELIVERY AGENTバージョン	CITRIX WORKSPACE APP FOR WINDOWS のバージョン	CITRIX WORKSPACE APP FOR MAC のバージョン	CITRIX WORKSPACE APP LINUX版 バージョン
マイクロソフト チームズ	状態	1906.2	2112	2203	2203

データ定義:

UIパラメーター	説明
プラグインマネージャー	プラグインマネージャーがインストールされているかどうかを示します。プラグインマネージャーは、仮想チャネルを開き、最適化に必要なメディアエンジン（プラグイン）をダウンロードする小さな管理コンポーネントです。注：機能はベンダーによって異なる場合があります。

UIパラメーター	説明
プラグインマネージャー名	インストールされているプラグインマネージャーの名前です。
プラグインマネージャーのバージョン	インストールされているプラグインマネージャーのバージョンです。
プラグイン	プラグインがインストールされているかどうかを示します。プラグインは、最適化に必要なメディアエンジンです。注：機能はベンダーによって異なる場合があります。
プラグインのバージョン	エンドポイントにインストールされているプラグインのバージョンです。
アプリのバージョン	仮想配信エージェント（VDA）上のアプリケーションのバージョンを表します。
仮想チャネル	リアルタイム通信アプリの仮想チャネルが開いているか閉じているかを表します。
仮想チャネル許可リスト	仮想チャネルのステータスを表示します。値は *Enabled* または *Disabled* です。
状態	特定のユーザーセッションにおけるアプリケーションの最適化状態を表示します

セッショントポロジのシナリオ

セッショントポロジはアクティブなセッションで利用可能で、リアルタイムで更新されます。切断されたセッションと終了したセッションは、包括的なセッション後分析のために、最後に認識された状態のトポロジを表示します。

サイトの展開シナリオに応じて、セッションに関与するコンポーネントは次のすべてまたは一部です。

- エンドポイント上のCitrix Workspaceアプリ
- Gatewayサービス/オンプレミスGateway
- Cloud Connector – ハイブリッド接続の場合、GatewayはCloud Connectorを介してDaaSに接続されます。
- VDA

したがって、可能なネットワークトポロジは次のとおりです。

- エンドポイント上のCitrix Workspaceアプリは、Citrix WorkspaceおよびGateway Serviceを介してオンプレミスのVDAに接続します。VDAへの接続にCloud Connectorは使用されません。

セッショントポロジビュー(/en-us/citrix-virtual-apps-desktops/current-release/media/dir-session-topology1.png)

- エンドポイント上のCitrix Workspaceアプリは、Citrix WorkspaceおよびGateway Serviceを介して、Cloud Connector経由でオンプレミスのVDAに接続します。

セッショントポロジビュー(/en-us/citrix-virtual-apps-desktops/current-release/media/dir-session-topology2.png)

- エンドポイント上のCitrix Workspaceアプリは、StoreFront™およびオンプレミスGatewayを介してオンプレミスVDAに接続します。

セッショントポロジビュー(/en-us/citrix-virtual-apps-desktops/current-release/media/dir-session-topology3.png)

- エンドポイント上のCitrix Workspaceアプリは、StoreFrontを介してオンプレミスVDAに接続します。

セッショントポロジビュー(/en-us/citrix-virtual-apps-desktops/current-release/media/dir-session-topology4.png)

パフォーマンスメトリック

パフォーマンスメトリックパネルでは、ユーザーセッション内の問題を特定するためにリアルタイムメトリックを関連付けることができます。セッションメトリックの傾向は、これらのメトリックが時間の経過とともにどのようにパフォーマンスを発揮したかを示すのに役立ちます。**セッションパフォーマンス**タブをクリックすると、リアルタイムデータとともに、過去15分間および48時間分のデータを表示できます。プロットは、複数のコンポーネントのパフォーマンスメトリックを単一のビューで関連付けるのに役立ちます。

セッションパフォーマンスメトリック(/en-us/citrix-virtual-apps-desktops/current-release/media/dir-session-performance-trends.png)

> **注:**

- 過去15分間のメトリックサポートにより、グラフはセッションが接続および切断された期間にわたってプロットされます。切断されたセッションのメトリックはゼロの値で表示されます。
- 過去48時間のメトリックサポートにより、ICARTT、ICA Latency、およびセッション再接続のプロットは履歴データメトリックで更新されます。セッション再接続情報は、中断のあるネットワーク接続を表示およびトラブルシューティングするのに役立ちます。また、シームレスなエクスペリエンスを持つネットワークも分析します。セッション再接続数、合計セッション再接続数、自動クライアント再接続、およびセッション信頼性再接続の数を確認するためのグラフ。

ICARTTとICA Latencyの他に、リアルタイムおよび過去15分間のメトリックとして以下のメトリックが利用可能です。

- フレーム/秒 - フレーム/秒は、セッションの応答性を示す重要なメトリックです。
- 出力帯域幅の利用可能量 - 出力帯域幅の利用可能量は、VDAからエンドポイントへデータを送信するために利用可能な総帯域幅の測定値です。
- 出力帯域幅の消費量 - 出力帯域幅の消費量は、ユーザーにセッションを表示するためにVDAからエンドポイントへ送信された実際のデータ量を示します。

出力帯域幅の利用可能量と出力帯域幅の消費量を分析することで、セッションを提供するために十分な帯域幅が利用可能であるかを確認し、セッションが帯域幅不足の影響を受けているかどうかを検出するのに役立ちます。

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

以前は、EUEMサービスまたはプロファイル管理サービスが実行に失敗した場合、ICA RTTまたはセッションログオン期間に関連するデータ取得の失敗理由が表示されませんでした。この新機能により、失敗の理由とその失敗に対する対応する解決策を取得できます。**詳細**リンクには、以下の表に示すように、ICA RTTおよびセッションログオン期間のエラー、失敗の理由、および解決策が記載されています。

エラーの種類	エラー	エラーメッセージ	解決策
ICA RTTエラー	ICA RTT値が表示されません。	**Citrix End User Experience Monitoringが実行されていません。**	1. サービスコンソールを開きます。このコンソールを開くには、**スタート**を

エラーの種類	エラー	エラーメッセージ	解決策
			クリックし、**サービス**と入力します。
			2. Citrix End User Experience Monitoring Serviceが実行されていることを確認します。
			3. デスクトップセッションを再度開き、試してください。ICA RTT値が表示されるはずです。
			4. 問題が解決しない場合は、Citrix管理者に連絡してください。
ICA RTTエラー	ICA RTT値が表示されません。	**Citrix End User Experience Monitoring がインストールされていません。**	1. VDAを再インストールしてください。
			2. サービスコンソールを開きます。このコンソールを開くには、**スタート**をクリックし、「サービス」と入力します。
			3. Citrix End User Experience Monitoring Serviceが実行されていることを確認します。
			4. デスクトップセッションを再度開き、試してくださ

エラーの種類	エラー	エラーメッセージ	解決策
			い。ICA RTT値が表示されるはずです。
			5. 問題が解決しない場合は、Citrix管理者に連絡してください。
ICA RTTエラー	ICA RTT値が表示されません。	**データの取得エラー。**	1. 「サービス」コンソールを開きます。このコンソールを開くには、**スタート**をクリックし、「サービス」と入力します。
			2. **Windows Management Instrumentation サービス**が実行されていることを確認します。
			3. また、**アクティビティマネージャー** > **プロセス**タブで WfShell.exe/ PicaShell.exe プロセスが実行されていることを確認します。実行されていない場合は、デスクトップセッションを再度開きます。
			4. 前の手順が機能しない場合は、Citrix_Euem_RoundTrip インスタンスが存在することを確認するために、次のコ

エラーの種類	エラー	エラーメッセージ	解決策
			マンドを実行します: `Get-CimInstance -Namespace 'ROOT\Citrix\Euem' -Query "select * from Citrix_Euem_RoundTrip"`
			`5.` Citrix_Euem_RoundTrip インスタンスが存在する場合は、デスクトップセッションを再度開きます。
			`6.` 問題が解決しない場合は、Citrix管理者に連絡してください。
セッションログオン期間エラー	グラフが読み込まれていません。	**Citrix Profile Management が実行されていません**	`1.` 「サービス」コンソールを開きます。このコンソールを開くには、**スタート**をクリックし、「サービス」と入力します。
			`2.` **Citrix Profile Management Service**が実行されていることを確認します。
			`3.` デスクトップセッションを再度開き、試してください。グラフが表示されるはずです。

エラーの種類	エラー	エラーメッセージ	解決策
			4. 問題が解決しない場合は、Citrix管理者に連絡してください。
セッションログオン期間エラー	グラフが読み込まれていません。	**Citrix Profile Management**がインストールされていません。	1. Citrix Profile Management Serviceをインストールしてください。
			2. 「サービス」コンソールを開きます。このコンソールを開くには、**スタート**をクリックし、「サービス」と入力します。
			3. **Citrix Profile Management Service**が実行されていることを確認します。
			4. デスクトップセッションを再度開き、試してください。グラフが表示されるはずです。
			5. 問題が解決しない場合は、Citrix管理者に連絡してください。
セッションログオン期間エラー	グラフが読み込まれていません。	**データの取得エラー。**	1. **「サービス」**コンソールを開きます。このコンソールを開くには、**スタート**をクリックし、

エラーの種類	エラー	エラーメッセージ	解決策
			「サービス」と入力します。
			`2.` **Windows Management Instrumentation サービス**が実行されていることを確認します。
			`3.` 前述のサービスがすでに実行されている場合は、`LogonTimings instance is present`を確認するために、次のコマンドを実行します: `Get-CimInstance -Namespace 'ROOT\Citrix\Profile\Metrics' -Query "select * from LogonTimings"`
			`4.` 問題が解決しない場合は、Citrix管理者に連絡してください。
ICA RTTエラー	ICA RTT値が表示されません。	コンソールはサポートされていません。	HDXを使用してセッションを開始します。
ICA RTTエラー	ICA RTT値が表示されません。	リモートデスクトッププロトコル (RDP) はサポートされていません。	HDXを使用してセッションを開始します。

エラーの種類	エラー	エラーメッセージ	解決策
ICA RTTエラー	ICA RTT値が表示されません。	詳細なエラー検出とすべての機能へのアクセスを得るには、VDAをバージョン2402以降にアップグレードしてください。	VDAを2402以降にアップグレードしてください。
セッションログオン期間エラー	グラフが読み込まれていません。	Citrix Profile Management WMI プラグインがインストールされていません。	Citrix Profile Management WMI プラグインをインストールしてください。

アプリケーションのパフォーマンスの問題を診断する

Citrix Director (uberAgentと統合) におけるアプリケーションパフォーマンス監視は、公開されているアプリケーションとローカルアプリケーションの両方を含む個々のアプリケーションがどのように動作しているかについて、管理者に詳細な洞察を提供します。このデータは、問題がアプリケーションのリソース消費、ネットワーク依存関係、またはUIの応答性の低さによって引き起こされているかどうかを特定するのに役立ちます。

前提条件

- VDA Windowsのバージョンは2603以上である必要があります
- uberAgentがVDAにインストールされている必要があります
- 「アプリケーションパフォーマンスのためにuberAgentデータでDirectorを強化する」ポリシーは、Studioで有効にする必要があります。

ポリシー名	ポリシーの説明	UIメトリック	デフォルト値	値のオプション	VDA WINDOWSのバージョン	VDA (リナックス、マック)
アプリケーションパフォーマンスのために	アプリケーションパフォーマンスのために	アプリケーション名, 公開済み, プロセス名, CPU	有効	有効または無効	2603以降	利用できません

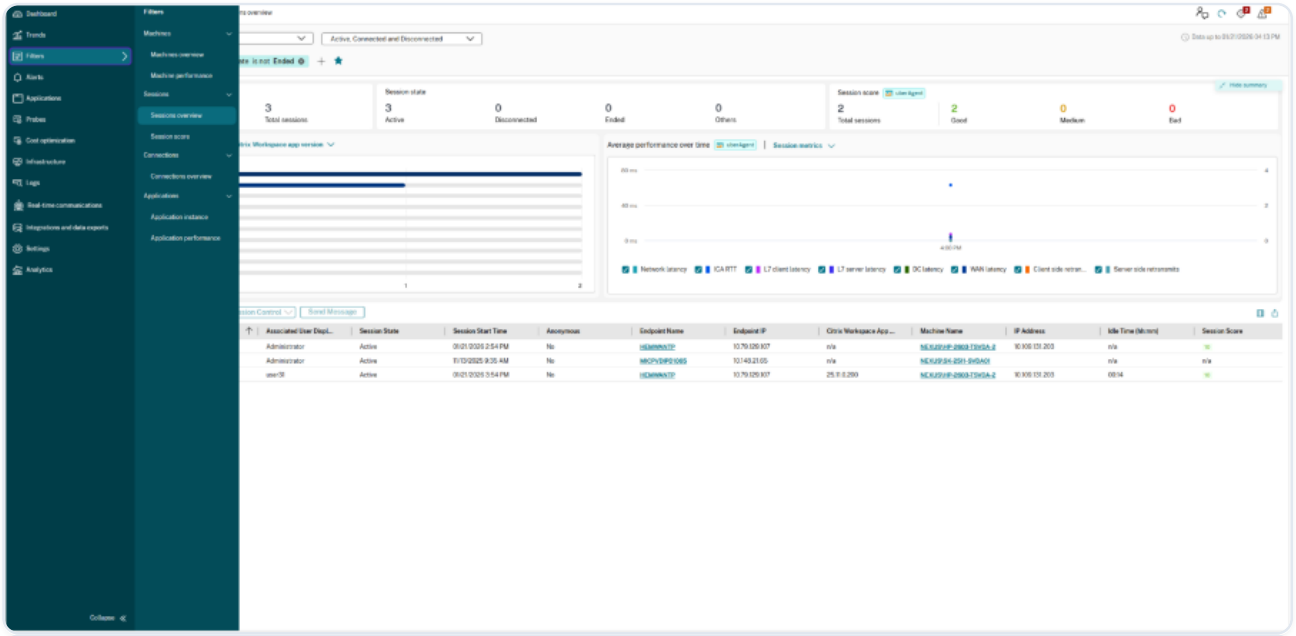
ポリシー名	ポリシーの説明	UIメトリック	デフォルト値	値のオプション	VDA WINDOWSのバージョン	VDA (リナックス、マック)
uberAgentデータでDirectorを強化	uberAgentが提供するマシンメトリックデータを使用するようにDirectorを有効にする	使用率 %, メモリ使用率 %, ワーキングセットメモリ (MB), ディスクIOPS, ディスク待機時間 (ms), ネットワーク待機時間 (ms), 入力遅延 (ms), CPU使用率 % (P95), メモリ使用率 % (P95), 入力遅延 (P95) (ms), 1秒あたりのページフォールト				

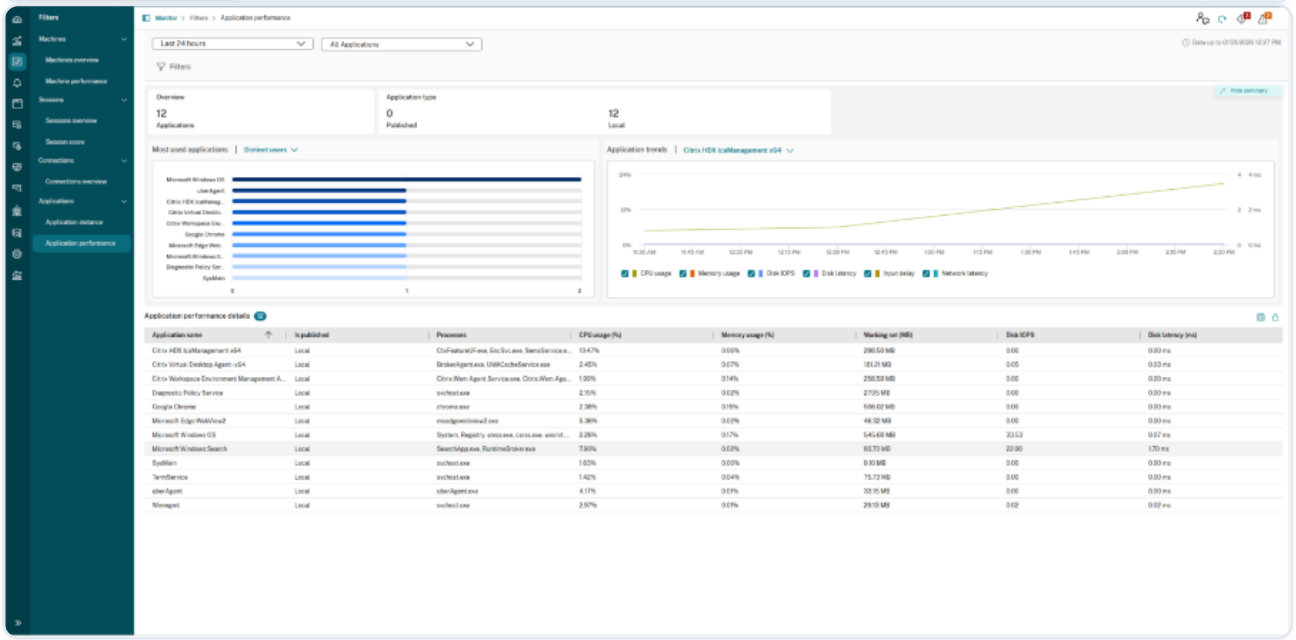
概要と主要機能

このページでは、公開アプリケーションとローカルアプリケーションの両方のリアルタイムおよび履歴監視に焦点を当てた新しい**アプリケーションパフォーマンス**タブのドキュメントについて詳しく説明します。

主要機能は次のとおりです。

- 時間範囲フィルター: 時間範囲オプションにより監視精度が向上しました。
- 効率化されたフィルター管理: フィルター管理のための直感的なドロップダウン。
- 直感的なフィルター作成: メインページで直接フィルターを作成および変更するための柔軟なワークフロー。
- 視覚化: アプリケーションのパフォーマンス傾向を即座に把握するためのアプリケーション分布チャートと経時的パフォーマンスチャートの導入。

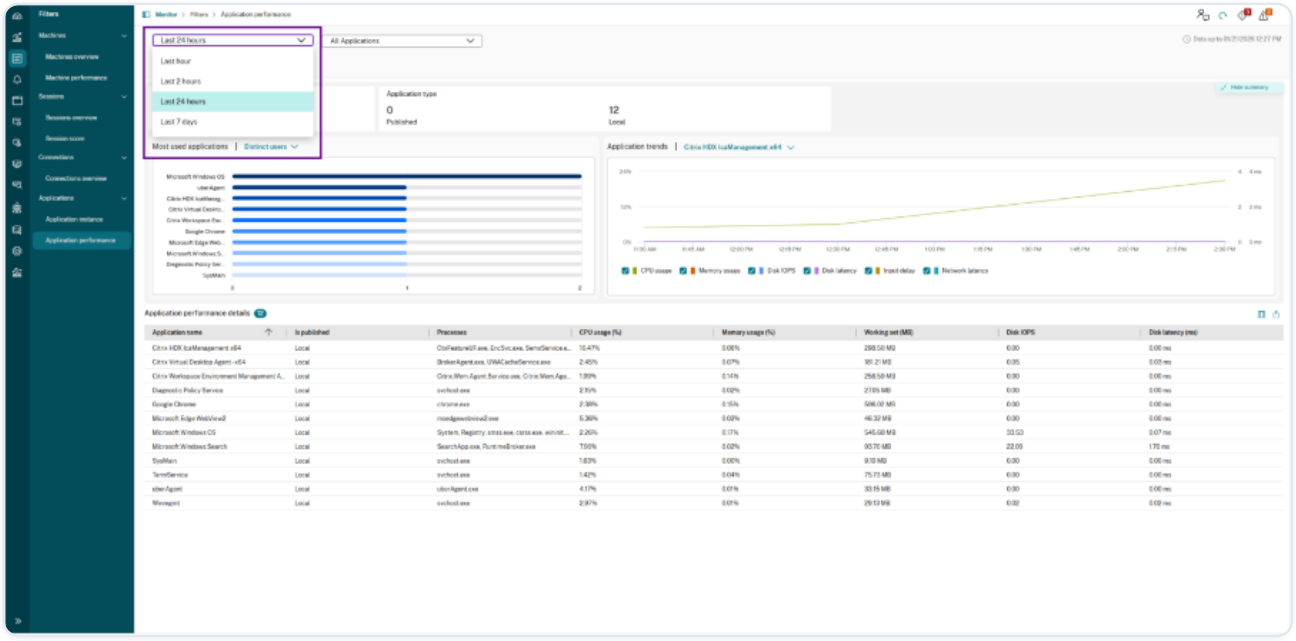




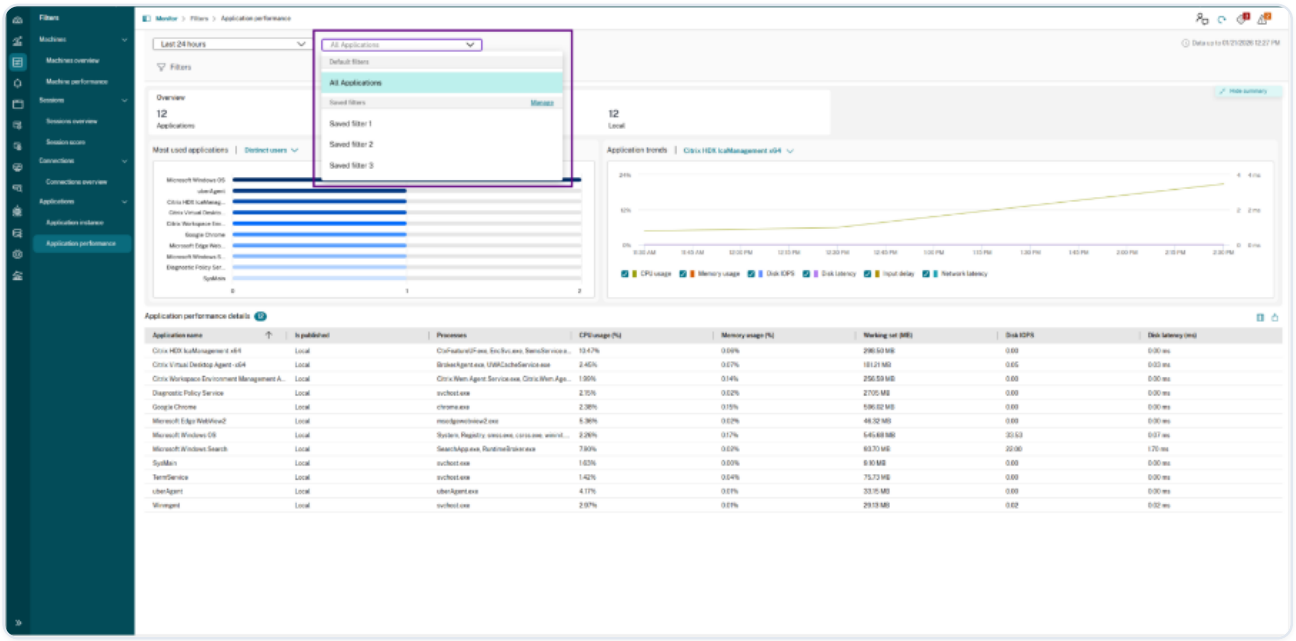
データのフィルタリング

ページ上部で、表示されるデータの範囲を定義できます。

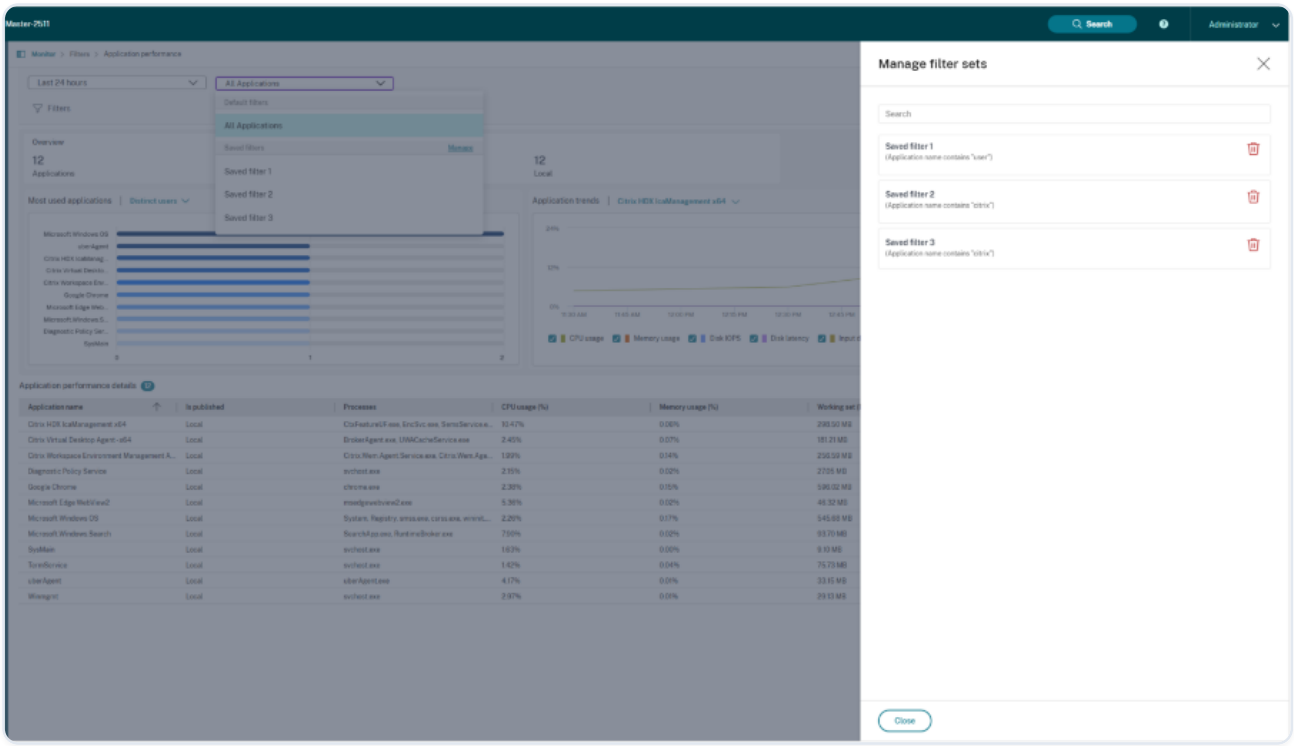
- **期間:** 時間範囲を選択します。時間範囲フィルターには、1時間、2時間、1日、または7日が含まれます。



- **アプリケーションスコープ:** アプリケーションドロップダウンを使用して、ダッシュボード全体を特定のフィルターで絞り込むか、**すべてのアプリケーション**を表示します。



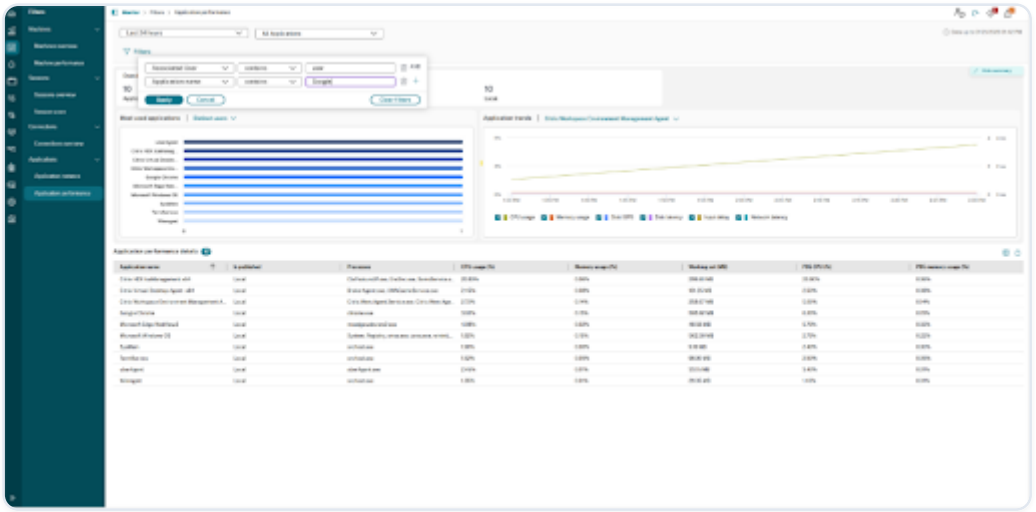
- **フィルター:** フィルターアイコンを使用して、データをさらに絞り込みます。
- **管理:** をクリックすると、既存の保存済みフィルターを検索、表示、または削除できるサイドパネルが開きます。

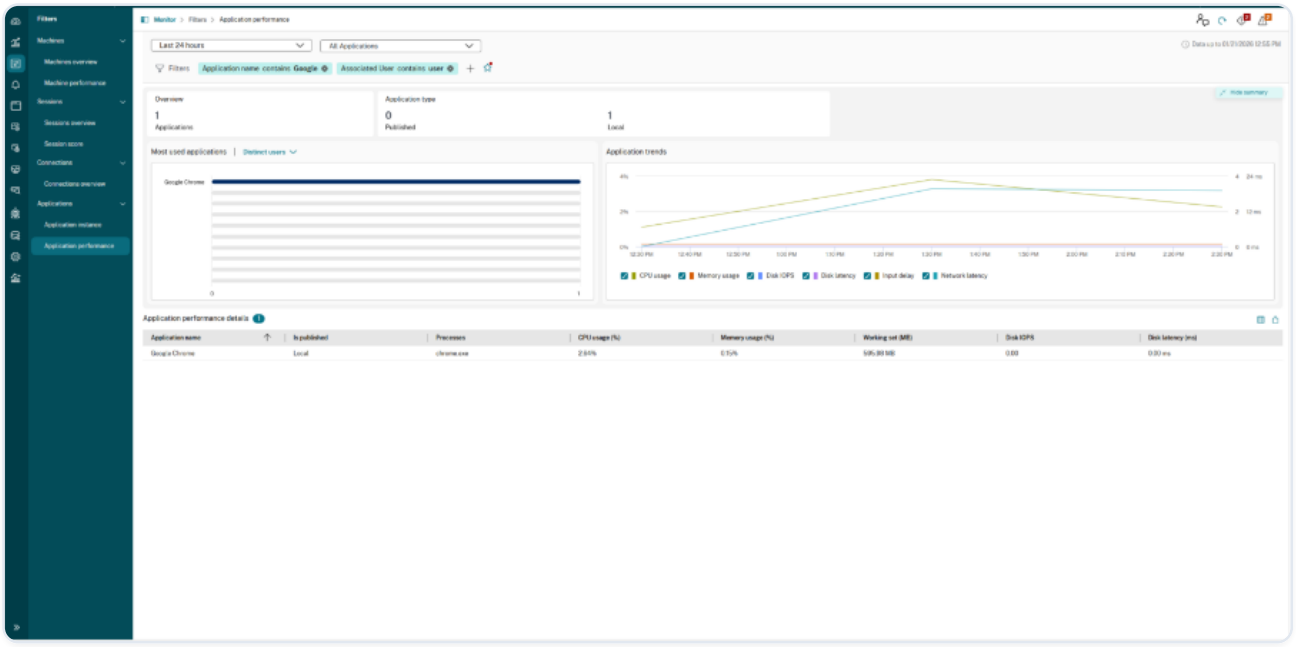


フィルターの作成と適用

アプリケーションの概要ページで、複雑なフィルターセットを直接作成できるようになりました。

- フィルターアイコンまたは既存のフィルターの横にある + ボタンをクリックします。
- 条件（例: アプリケーション名）、演算子（例: 含む）、および値（例: Google）を選択します。





フィルターの保存ステータスとワークフロー

アクティブなフィルターの横にある星のアイコン (⋆) は、現在のフィルターセットのステータスを視覚的に示します。これにより、管理者はカスタムフィルターの保存、適用、管理を行うことができます。

フィルターステータス	アイコンの外観	意味	必要な操作
未保存のフィルター	 (赤い点が付いた空のアウトライン)	現在のフィルター条件の組み合わせは**保存されていません**。	**空の星**をクリックしてダイアログボックスを開き、フィルターセットに名前を付けて保存します。
保存済みフィルター	 (塗りつぶし / 実線)	現在アクティブなフィルターセットは、以前に保存されたフィルターと**完全に一致**しています。	アクションは不要です。定義済みのテンプレートに基づいてデータを表示しています。
変更が加えられた保存済みフィルター		**保存済みフィルター**を使用しているときに、他のフィルターが追加または削除された場合、あるいは列がソートされた場合、変更が**まだ保存されていない**ことを	既存の保存済みフィルターを更新するには**赤い点が付いた星**をクリックするか、ドロップダウンを使用して**フィルターセットとして保存**を

フィルターステータス	アイコンの外観	意味	必要な操作
	(赤い点で塗りつぶし)	示す赤い点が表示されます。	選択して新しいものを作成します。

フィルターアクションボタン

新しいフィルターを追加したり、保存済みのフィルターを変更したりすると、以下のコントロールとステータスインジケーターが利用可能になります。

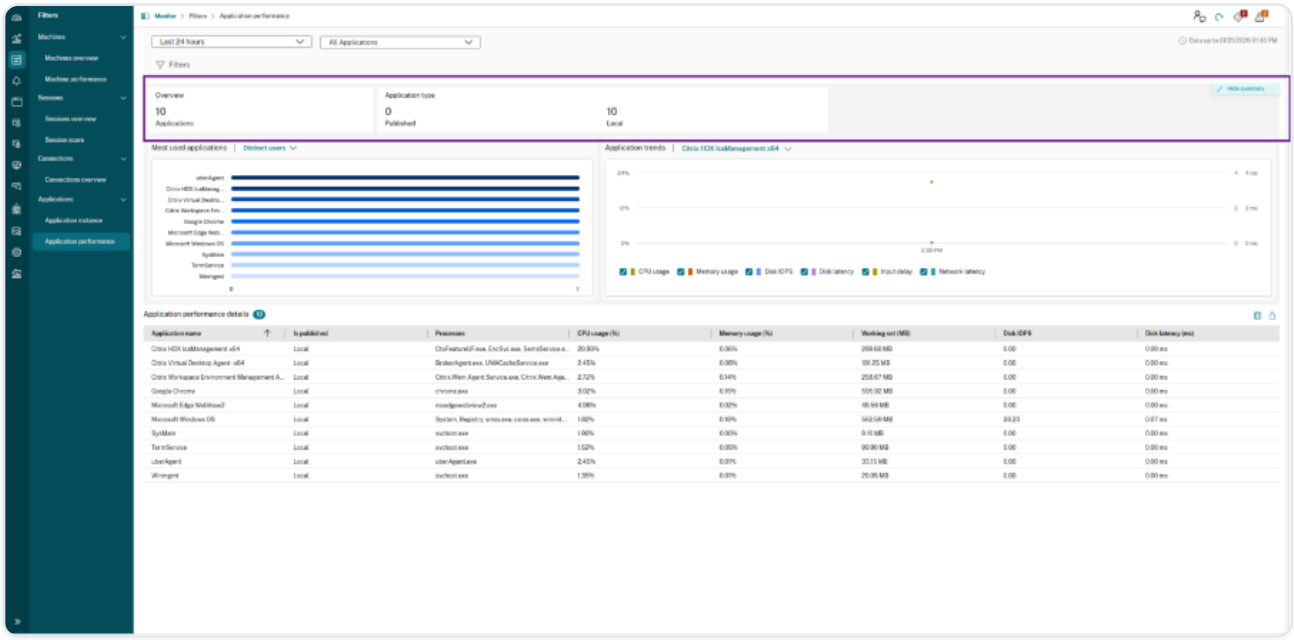
ボタン	意味と操作
更新	現在アクティブなすべてのフィルター条件をグラフとアプリケーションパフォーマンスデータテーブルに適用します。
キャンセル	現在のフィルターセットに加えられた変更を破棄し、最後に適用されたフィルターに戻します。
フィルターをクリア	新しく追加されたすべてのフィルター条件を削除します。
 **アイコン**	このアイコンがクリックされた、選択されたフィルター条件を削除します。

視覚化

概要サマリー

サマリーペインには、現在監視されているアプリケーションの即時カウントが表示されます。

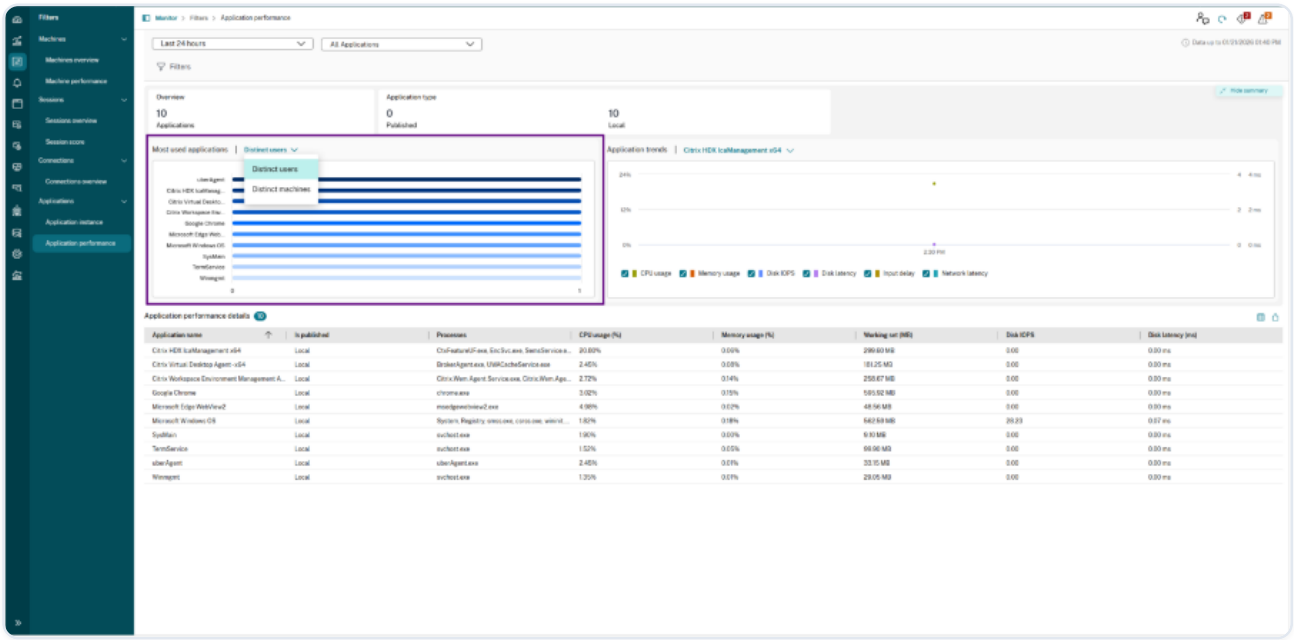
- **アプリケーション:** 環境内で検出された一意のアプリケーション名の総数。
- **アプリケーションの種類:** VDAで実行されている**公開**アプリケーションと**ローカル**アプリケーションの数を内訳で示します。



分布グラフ

分布グラフは、特定のパフォーマンスバケットに基づいてアプリケーションインスタンスの数を分類するヒストグラムとして機能します。これは、環境全体でのユーザーエクスペリエンスの「広がり」を理解するのに役立つように設計されています。

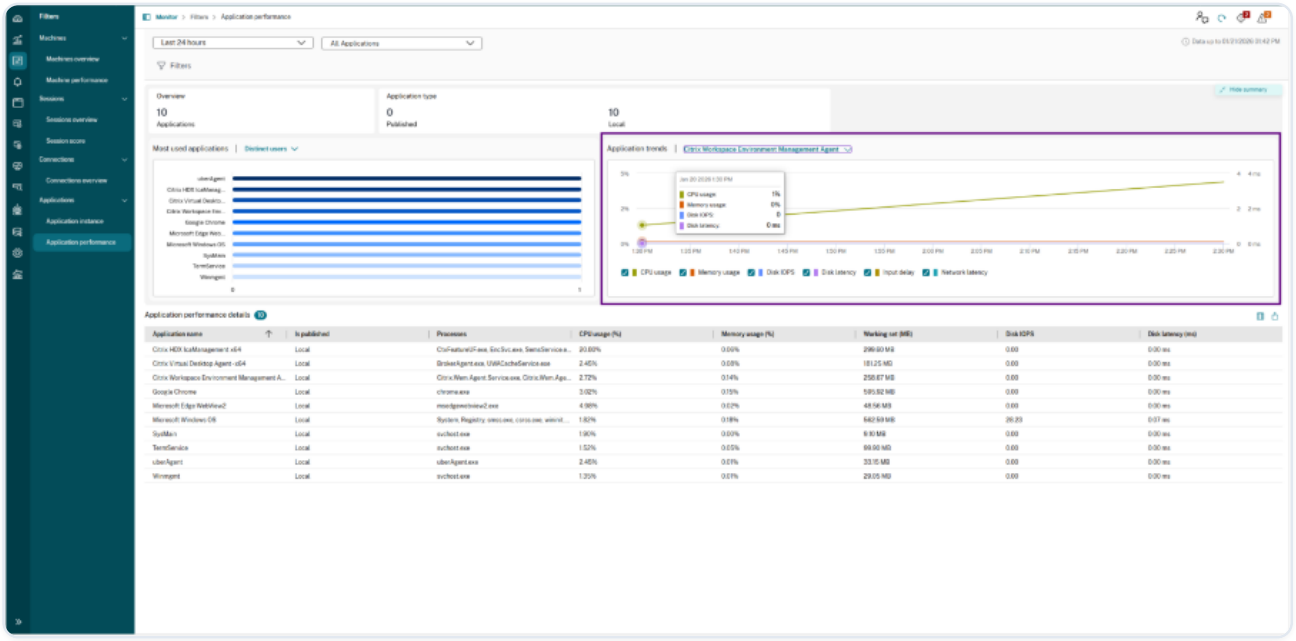
- **メトリックのグループ化:** X軸は選択されたメトリック（**UI遅延**や**起動時間**など）の範囲を表し、Y軸はそれらの範囲内での発生回数を表します。
- **表示の視点:** ドロップダウンメニューを使用すると、2つのビュー間でデータの表示を切り替えることができます。
  - **個別ユーザー:** 一意のユーザー数に基づいたパフォーマンスの分布を表示します。
  - **個別マシン:** VDAの数に基づいた分布を表示します。



パフォーマンスグラフ

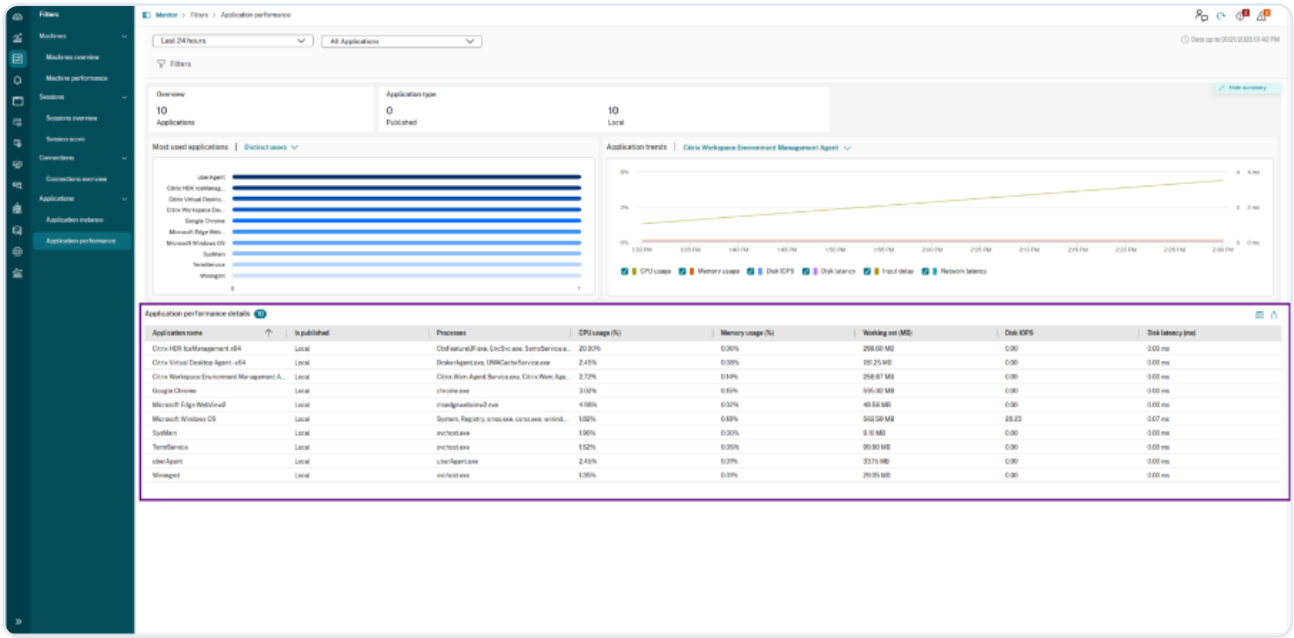
パフォーマンスグラフは、選択した期間にわたるアプリケーションの健全性を追跡する時系列の視覚化です。これにより、パフォーマンスの変化を特定の時間間隔やリソース消費と関連付けることができます。

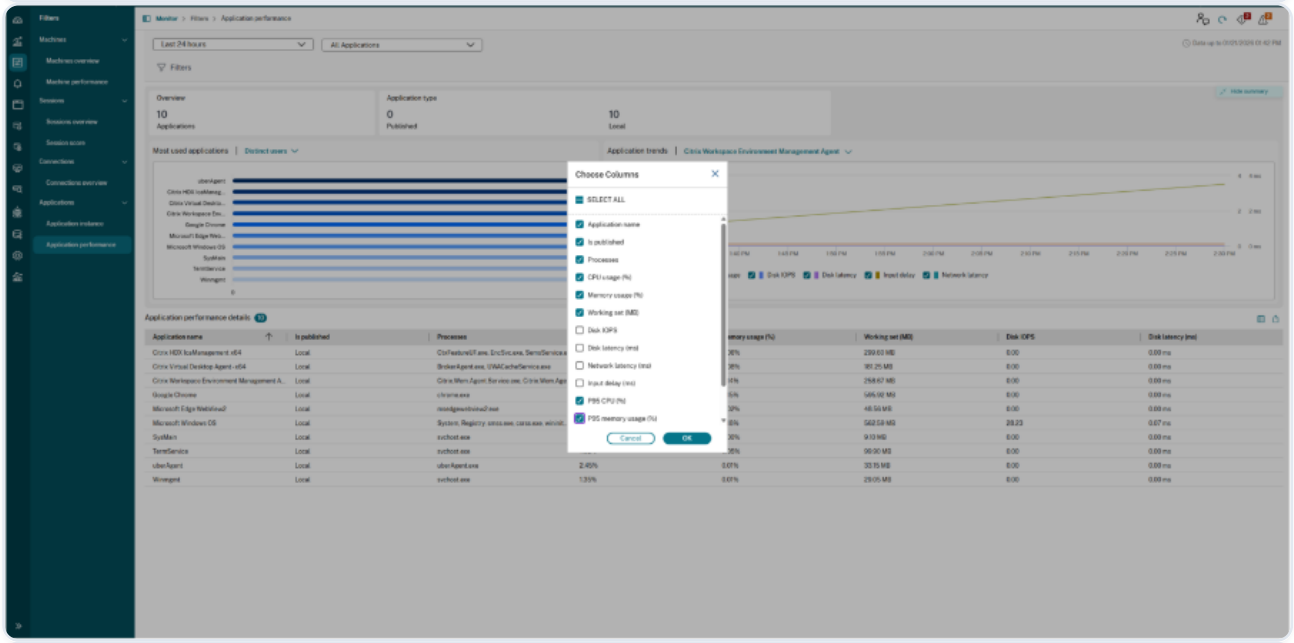
- **アプリケーションの選択:** グラフ上部のドロップダウンメニューを使用して、分析する特定のアプリケーションを選択します。
- **複数メトリックの相関関係:** このグラフでは、複数の主要業績評価指標（KPI）を同時に重ねて表示し、応答性とリソース使用量の相関関係を見つけることができます。
  - **CPUとメモリの使用量**: アプリケーションによるリソース消費の割合を表示します。
  - **ディスクIOPSとディスク遅延**: ストレージのボトルネックがアプリケーションのパフォーマンスに影響を与えているかどうかを特定します。
  - **入力遅延**：ユーザーのアクションとアプリケーションの応答の間の時間を測定します。
  - **ネットワーク遅延**：アプリケーションの通信に関連するネットワーク遅延を追跡します。

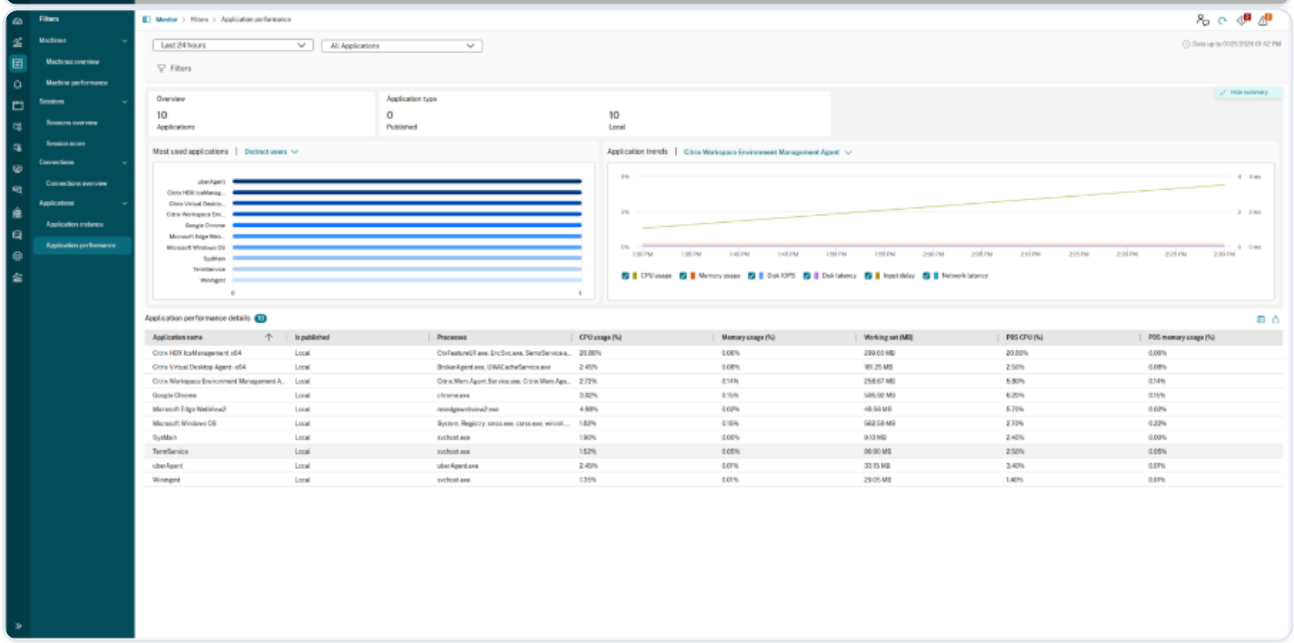


アプリケーションパフォーマンスの詳細（表）

下部のペインには、すべてのアプリケーションインスタンスの生データと実用的なデータが表示されます。データはエクスポートでき、表示する列を選択できます。




Choose Columns
SELECT ALL
Application name
Is published
Processes
CPU usage (%)
Memory usage (%)
Working set (MB)
Disk IOPS
Disk latency (ms)
Network latency (ms)
Input delay (ms)
PBS CPU (%)
PBS memory usage (%)
Cancel
OK



過去のユーザーセッションを診断する

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

- マシン詳細パネル - 選択したセッションが起動されたマシンの利用可能な詳細を表示します。
- セッション詳細パネル - 選択したセッションの利用可能な詳細を表示します。
- セッションログオン期間 - 選択したセッションにかかったログオン期間に関する情報を表示します。以下の項目にかかった時間のチャートを表示できます。
    - ブローカリング
    - マシンの起動
    - HDX™接続
    - 認証
    - GPO
    - ログオンスクリプト
    - ディスクへのプロファイル読み込み
    - 対話型セッション

過去のユーザーセッションを表示するには、次の手順を実行します。

1. **フィルター** > **セッション**ビューをクリックします。
2. 「**関連ユーザー**」をクリックして、ユーザーのActivity Managerを開きます。

    履歴ユーザーセッションのActivity Manager(/en-us/citrix-virtual-apps-desktops/current-release/media/dir-his-user-sessions-am.png)
3. 「**終了したセッション**」セクションから必要なセッションを選択します。
4. 「**マシン詳細**」パネルと「**セッション詳細**」パネルを表示します。

    履歴ユーザーセッションの詳細(/en-us/citrix-virtual-apps-desktops/current-release/media/dir-his-user-sessions-details.png)
5. 下にスクロールして、終了したセッションの「**セッションログオン期間**」を表示します。

    履歴ユーザーセッションの期間(/en-us/citrix-virtual-apps-desktops/current-release/media/dir-his-user-sessions-duration.png)

6. 「**セッションログオン**」タブをクリックして、詳細を表示します。

   終了したユーザーセッションのログオン期間(/en-us/citrix-virtual-apps-desktops/current-release/media/session-logon-ended.png)

7. 「**セッションパフォーマンス**」タブをクリックして、詳細を表示します。

   終了したユーザーセッションのパフォーマンス(/en-us/citrix-virtual-apps-desktops/current-release/media/session-performance-ended.png)

シャドウユーザー

Directorから、シャドウユーザー機能を使用して、ユーザーの仮想マシンまたはセッションを直接表示したり操作したりできます。Windows VDAとLinux VDAの両方をシャドウできます。シャドウするマシンにユーザーが接続している必要があります。これは、ユーザーのタイトルバーに表示されているマシン名を確認することで検証できます。

Directorは新しいタブでシャドウを開始します。DirectorのURLからのポップアップを許可するようにブラウザ設定を更新してください。

シャドウ機能は、**ユーザーの詳細**ビューからアクセスします。ユーザーセッションを選択し、アクティビティマネージャービューまたはセッション詳細パネルで**シャドウ**をクリックします。

リモートアシストの使用

LINUX VDAのシャドウ

シャドウは、RHEL7.3またはUbuntuバージョン16.04のLinuxディストリビューションを実行している、バージョン7.16以降のLinux VDAで利用できます。

> **注:**
>
> - シャドウが機能するには、VDAがDirector UIからアクセス可能である必要があります。したがって、シャドウはDirectorクライアントと同じイントラネット内のLinux VDAでのみ可能です。
> - DirectorはFQDNを使用してターゲットLinux VDAに接続します。Directorクライアントが Linux VDAのFQDNを解決できることを確認してください。
> - VDAには、python websockifyおよびx11vncパッケージがインストールされている必要があります。

- VDAへのnoVNC接続はWebSocketプロトコルを使用します。デフォルトでは、**ws://** WebSocketプロトコルが使用されます。セキュリティ上の理由から、Citrixは安全な **wss://** プロトコルを使用することを推奨します。各DirectorクライアントとLinux VDAにSSL証明書をインストールしてください。

セッションシャドウ の手順に従って、シャドウ用にVDAを構成してください。

1. **シャドウ**をクリックすると、シャドウ接続が初期化され、ユーザーデバイスに確認プロンプトが表示されます。
2. ユーザーに**はい**をクリックするよう指示して、マシンまたはセッションの共有を開始します。
3. 管理者はシャドウされたセッションを表示することのみ可能です。

WINDOWS VDA のシャドウイング

Windows VDA セッションは、Windows リモートアシスタンスを使用してシャドウイングされます。VDA のインストール中に、**ユーザー Windows リモートアシスタンス**機能を有効にします。詳細については、「機能の有効化または無効化」を参照してください。

1. **シャドウ**をクリックすると、シャドウイング接続が初期化され、.msrc インシデントファイルを開くか保存するかを求めるダイアログボックスが表示されます。
2. デフォルトで選択されていない場合は、リモートアシスタンスビューアーでインシデントファイルを開きます。ユーザーデバイスに確認プロンプトが表示されます。
3. マシンまたはセッションの共有を開始するには、ユーザーに**はい**をクリックするよう指示します。
4. より詳細な制御を行うには、ユーザーにキーボードとマウスの制御を共有するよう依頼します。

シャドウイング用に MICROSOFT INTERNET EXPLORER ブラウザーを合理化する

ダウンロードした Microsoft Remote Assistance (.msra) ファイルをリモートアシスタンスクライアントで自動的に開くように、Microsoft Internet Explorer ブラウザーを構成します。

これを行うには、グループポリシーエディターで 設定を有効にする必要があります。

コンピューターの構成 \> 管理用テンプレート \> Windows コンポーネント \> Internet Explorer \> インターネットコントロールパネル \> セキュリティページ \> インターネットゾーン \> ファイルのダウンロード時に自動的に確認する。

デフォルトでは、このオプションはローカルイントラネットゾーンのサイトで有効になっています。Director サイトがローカルイントラネットゾーンにない場合は、このゾーンにサイトを手動で追加することを検討してください。

HDX Screen Share の使用

Director は、IT 管理者とヘルプデスク担当者が HDX 画面共有テクノロジーを通じてエンドユーザーにリモートサポートを提供できるリモートアシスタンスをサポートしています。この機能は、Citrix のネイティブ HDX プロトコルを活用して、トラブルシューティングとユーザー支援のシナリオ向けに、安全で高性能な画面共有機能を提供します。

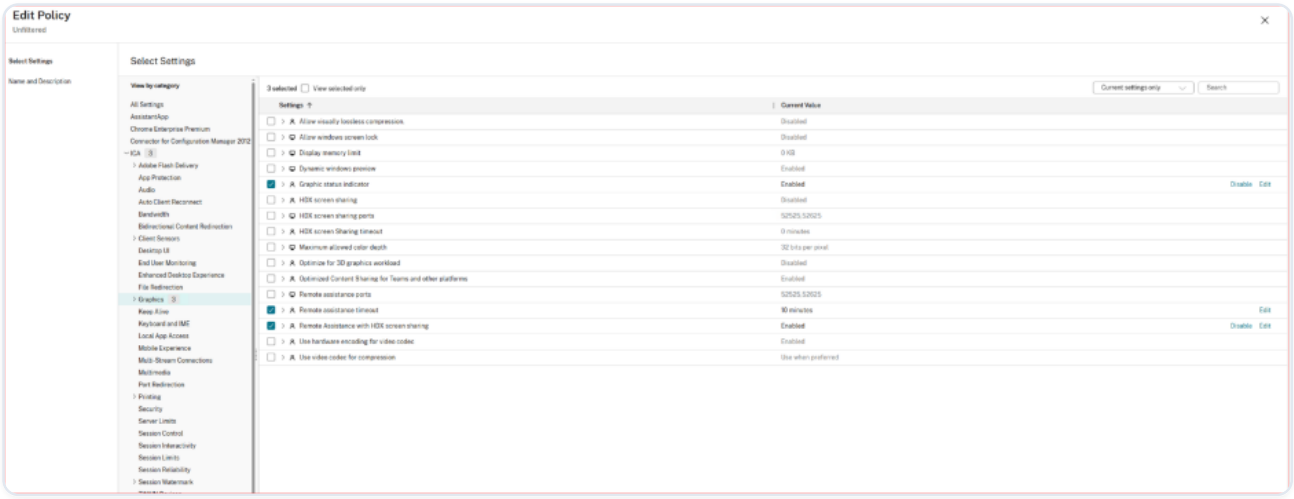
前提条件

コンポーネント	サポートされる環境またはバージョン
オペレーティングシステム	シングルセッションOSまたは**マルチセッションOS**用のWindows、Linux
仮想配信エージェント (VDA)	CR 2511以降
ディレクター	CR 2511以降
デリバリーコントローラー	CR 2511以降
TWPlayer (シンワイヤー プレイヤー)	シャドウセッションを開始する際に、プレーヤーをダウンロードするためのリンクがDirector UIで利用可能です

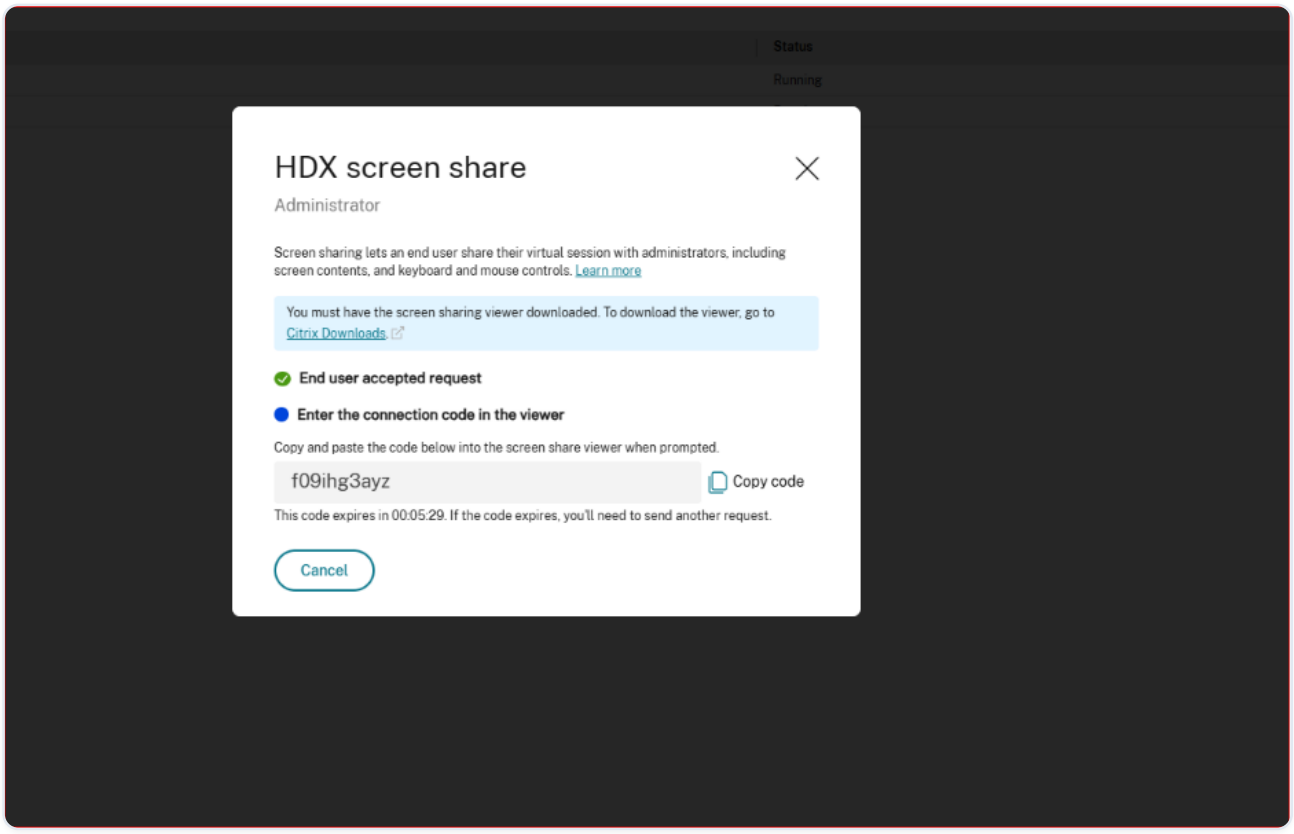
グループポリシーの構成

DirectorとHDX Screen Shareを使用してリモートアシスタンスを有効にするには、VDA上で次のグループポリシーを構成します。

- HDX画面共有によるリモートアシスタンス
- リモートアシスタンスのタイムアウト
- グラフィックステータスインジケーター



TWPlayer (ThinWire Player) は、HDX画面共有機能を有効にするために1回ダウンロードする必要がある必須コンポーネントです。シャドウセッションを開始する際に、プレーヤーをダウンロードするためのリンクがDirector UIで利用可能です。



制限事項

- 公開アプリケーション（アプリセッション）はシャドウできません。デスクトップセッションのみです。

Director と HDX Screen Share を使用したワークフロー
管理者が HDX 画面共有セッションを開始する手順を以下に示します。

1. **シャドウセッションの開始**

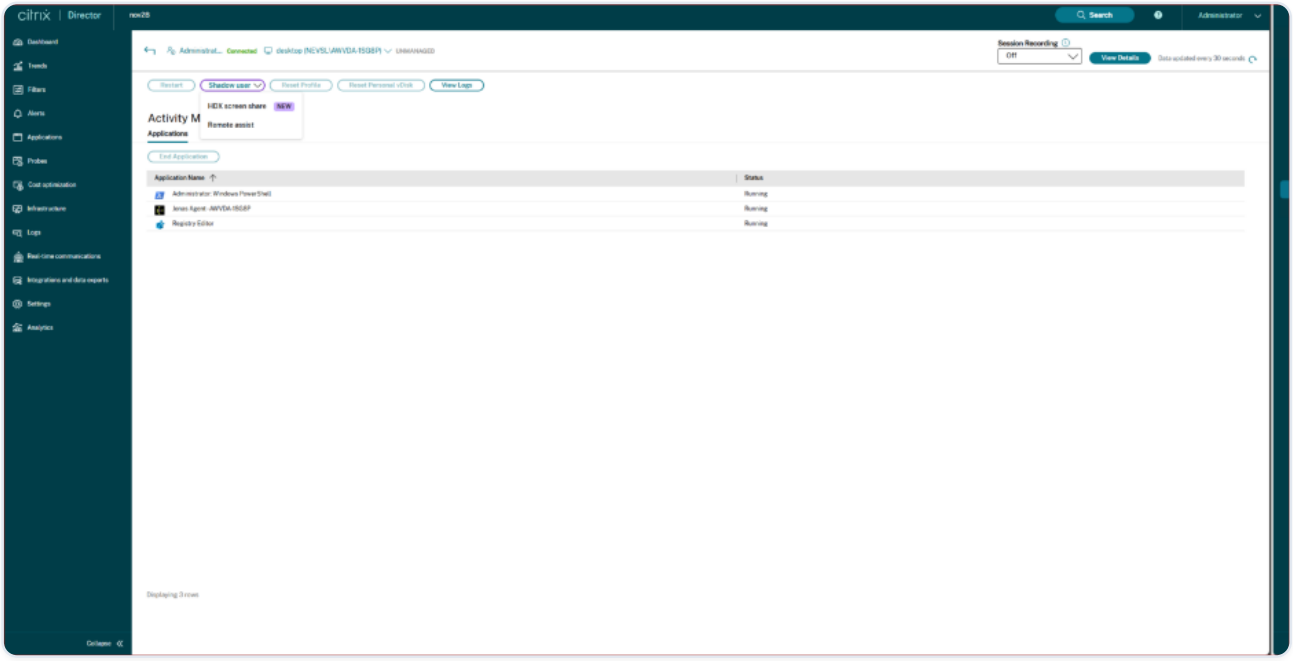
a. Citrix Director にログインします
b. サポートが必要なユーザーセッションに移動します
c. 「シャドウ」ボタンをクリックします
d. HDX 画面共有を選択します

2. **ビューアーの起動**

a. 生成されたインシデントファイルを TWPlayer/リモートアシスタンスビューアーで開きます
b. ユーザーが接続要求を承諾するのを待ちます

3. **セッションの表示**

a. セッション画面がビューアーウィンドウに表示されます
b. 管理者はユーザーの操作をリアルタイムで監視できます



ユーザーにメッセージを送信する

Directorから、1台以上のマシンに接続しているユーザーにメッセージを送信します。この機能を使用して、デスクトップのメンテナンス、マシンのログオフと再起動、プロファイルのリセットなど、差し迫った管理操作に関する即時通知を送信します。

1. アクティビティマネージャービューで、ユーザーを選択し、 をクリックします。
2. ユーザー詳細ビューで、セッション詳細パネルを見つけ、 をクリックします。
3. および フィールドにメッセージ情報を入力し、 をクリックします。

メッセージが正常に送信されると、Directorに確認メッセージが表示されます。メッセージはユーザーのマシンに表示されます。

メッセージが正常に送信されなかった場合、Directorにエラーメッセージが表示されます。エラーメッセージに従って問題をトラブルシューティングします。完了したら、件名とメッセージテキストを再度入力し、もう一度 をクリックします。

ユーザーアクションの一括アクションオプションを制限するカスタムロール

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

次の手順で、ロールを編集して一括アクションの権限を制限できるようになりました。

1. Citrix Cloudにサインインします。
2. **ロール**に移動し、「**一括アクションは有効になっていません**」ロールを選択します。
3. 3つの点をクリックし、「**編集**」を選択します。
4. **Director > 管理**に移動し、「**マシンの電源アクション、メンテナンスモード操作、およびセッション管理の一括アクションを実行する**」チェックボックスを選択します。
5. 次のロールも選択されていることを確認してください。
    - **マシンカタログメンバーシップを介してマシンのメンテナンスモードを有効/無効にする**
    - **マシンカタログメンバーシップを介してデスクトップのメンテナンスモードを有効/無効にする**
    - **マシンカタログメンバーシップを介してWindowsデスクトップマシンで電源操作を実行する**
    - **マシンカタログメンバーシップを介してWindowsサーバーマシンで電源操作を実行する**

ステップ5のオプションが選択されている場合、ユーザーは単一のアクションを実行できます。一括アクションを実行するには、ステップ4のオプションとステップ5のオプションを選択する必要があります。

アプリケーションの障害を解決する

「**アクティビティマネージャー**」ビューで、タブをクリックします。このユーザーがアクセスできるすべてのマシン上のすべてのアプリケーション（現在接続されているマシンのローカルアプリケーションとホスト型アプリケーションを含む）と、それぞれのステータスを表示できます。

注:

タブがグレー表示されている場合は、タブを有効にする権限を持つ管理者に連絡してください。

このリストには、セッション内で起動されたアプリケーションのみが含まれます。

マルチセッションOSマシンおよびシングルセッションOSマシンでは、切断されたセッションごとにアプリケーションが一覧表示されます。ユーザーが接続されていない場合、アプリケーションは表示されません。

アクション	説明
応答しないアプリケーションを終了する	応答しないアプリケーションを選択し、[アプリケーションの終了]をクリックします。アプリケーションが終了したら、ユーザーに再度起動するよう依頼します。
応答しないプロセスを終了する	必要な権限がある場合は、[プロセス]タブをクリックします。アプリケーションに関連する、または大量のCPUリソースやメモリを使用しているプロセスを選択し、[プロセスの終了]をクリックします。ただし、プロセスを終了するのに必要な権限がない場合、プロセスを終了しようとしても失敗します。
ユーザーのマシンを再起動する	シングルセッションOSマシンのみの場合、選択したセッションで[再起動]をクリックします。または、[マシン詳細]ビューから、電源コントロールを使用してマシンを再起動またはシャットダウンします。アプリケーションを再確認できるように、ユーザーに再度ログオンするよう指示します。マルチセッションOSマシンでは、再起動オプションは利用できません。代わりに、ユーザーからログオフし、ユーザーに再度ログオンさせます。
マシンをメンテナンスモードにする	マシンのイメージにパッチやその他の更新などのメンテナンスが必要な場合は、マシンをメンテナンスモードにします。[マシン詳細]ビューから[詳細]をクリックし、メンテナンス

アクション	説明
	モードオプションをオンにします。適切な管理者にエスカレートしてください。

デスクトップ接続を復元する

Directorから、ユーザーのタイトルバーで現在のマシンに対するユーザーの接続ステータスを確認します。

デスクトップ接続が失敗した場合、失敗の原因となったエラーが表示され、トラブルシューティングの方法を決定するのに役立ちます。

アクション	説明
マシンがメンテナンスモードではないことを確認します	ユーザー詳細ページで、メンテナンスモードがオフになっていることを確認します。
ユーザーのマシンを再起動する	マシンを選択し、**再起動**をクリックします。ユーザーのマシンが応答しない、または接続できない場合にこのオプションを使用します。たとえば、マシンが異常に高いCPUリソースを使用しており、CPUが使用不能になっている場合などです。

セッションを復元する

セッションが切断されても、セッションはアクティブなままでアプリケーションは実行され続けますが、ユーザーデバイスはサーバーと通信しなくなります。

ユーザー詳細ビューで、**セッションの詳細**パネルのセッション障害をトラブルシューティングします。セッションIDで示される現在のセッションの詳細を表示できます。

アクション	説明
応答しないアプリケーションまたはプロセスを終了する	**アプリケーション**タブをクリックします。応答しないアプリケーションを選択し、**アプリケーションの終了**をクリックします。同様に、応答しない対応するプロセスを選択し、**プロセスの終了**をクリックします。また、異常に大量のメモリまたはCPUリソースを消費しているプロセスを終了します。これにより、CPUが使用不能になる可能性があります。

アクション	説明
Windowsセッションを切断する	**セッション制御**をクリックし、**切断**を選択します。このオプションは、ブローカーされたマルチセッションOSマシンでのみ利用可能です。ブローカーされていないセッションの場合、このオプションは無効になります。
ユーザーのセッションからログオフする	**セッション制御**をクリックし、**ログオフ**を選択します。

セッションをテストするには、ユーザーはセッションに再度ログオンを試みることができます。また、ユーザーをシャドウして、このセッションをより詳細に監視することもできます。

HDX™ チャネルシステムレポートを実行する

ユーザーの詳細ビューで、**HDX**パネルにあるユーザーのマシン上のHDXチャネルのステータスを確認します。このパネルは、ユーザーのマシンがHDXを使用して接続されている場合にのみ利用可能です。

情報が現在利用できないことを示すメッセージが表示された場合は、ページが更新されるまで1分間待つか、**更新**ボタンを選択します。HDXデータの更新には、他のデータよりも少し時間がかかります。

詳細については、エラーまたは警告アイコンをクリックしてください。

> ヒント:
>
> タイトルバーの左隅にある左右の矢印をクリックすると、同じダイアログボックスで他のチャネルに関する情報を表示できます。

> HDXチャネルシステムレポートは、主にCitrixサポートがさらなるトラブルシューティングのために使用します。

1. HDXパネルで、をクリックします。
2. .xmlレポートファイルを表示または保存できます。
    - .xmlファイルを表示するには、をクリックします。.xmlファイルは、Directorアプリケーションと同じウィンドウに表示されます。

- .xmlファイルを保存するには、をクリックします。ウィンドウが表示され、Directorマシン上のファイルのダウンロード先を尋ねられます。

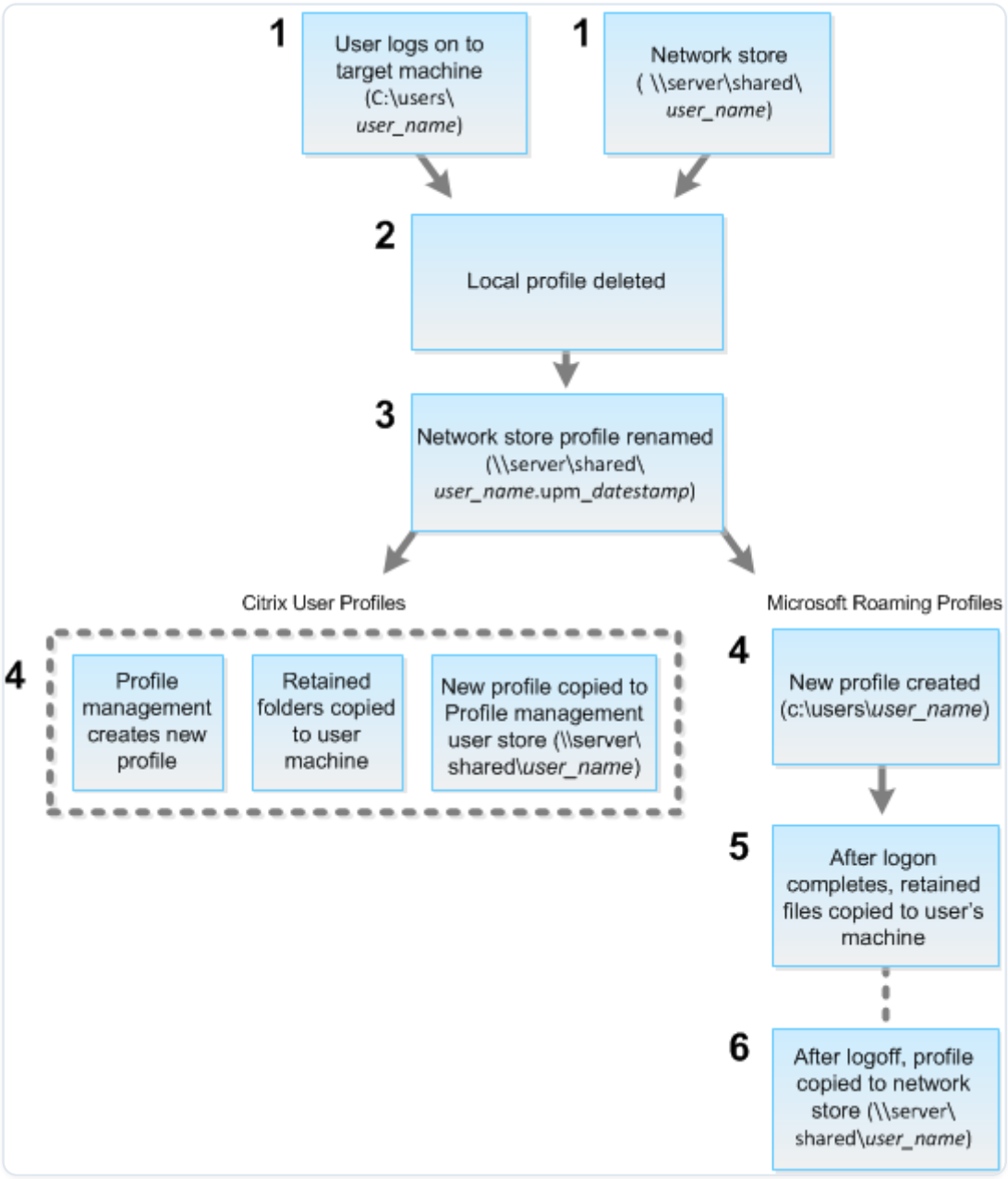
ユーザープロファイルをリセットする

> **注意:**
>
> プロファイルがリセットされると、ユーザーのフォルダーとファイルは保存され、新しいプロファイルにコピーされます。ただし、ほとんどのユーザープロファイルデータは失われます（たとえば、レジストリがリセットされ、アプリケーション設定が削除される可能性があります）。
>
> リセット機能は、ファイルベースとコンテナベースの両方のプロファイルソリューションに適用されます。

リセットされたプロファイルの処理方法

Citrix®ユーザープロファイルまたはMicrosoftローミングプロファイルのいずれもリセットできます。ユーザーがログオフし、リセットコマンド（DirectorまたはPowerShell SDKを使用して）を選択すると、Directorはまず使用中のユーザープロファイルを識別し、適切なリセットコマンドを発行します。Directorは、プロファイルサイズ、種類、ログオン時間などの情報をProfile Managementを通じて受け取ります。

この図は、ユーザープロファイルがリセットされた場合の、ユーザーログオン後のプロセスを示しています。



Directorによって発行されるリセットコマンドは、プロファイルの種類を指定します。その後、Profile Managementサービスはその種類のプロファイルをリセットしようとし、適切なネットワーク共有（ユーザーストア）を探します。ユーザーがProfile Managementによって処理されているにもかかわらず、ローミングプロファイルコマンドを受け取った場合、それは拒否されます（またはその逆も同様です）。

1. ローカルプロファイルが存在する場合、それは削除されます。
2. ネットワークプロファイルの名前が変更されます。
3. 次のアクションは、リセットされるプロファイルがCitrixユーザープロファイルかMicrosoftローミングプロファイルかによって異なります。

Citrixユーザープロファイルの場合、新しいプロファイルはProfile Managementのインポートルールを使用して作成されます。フォルダーはネットワークプロファイルにコピーされ、ユーザーは通常どおりログオンできます。リセットにローミングプロファイルが使用される場合、ローミングプロファイル内のレジストリ設定はリセットされたプロファイルに保持されます。必要に応じて、テンプレートプロファイルがローミングプロファイルを上書きするようにProfile Managementを構成できます。

Microsoftローミングプロファイルの場合、Windowsはプロファイルを作成し、ユーザーがログオンすると、フォルダーはユーザーデバイスにコピーされます。ユーザーが再度ログオフすると、新しいプロファイルはネットワークストアにコピーされます。

Directorでユーザープロファイルをリセットするには

Citrix Virtual Desktops™ (Desktop VDA) を使用している場合は、次の操作を行います。

1. **Director** で、プロファイルをリセットするユーザーを検索し、そのユーザーのセッションを選択します。
2. をクリックします。
3. ユーザーにすべてのセッションからログオフするよう指示します。
4. ユーザーに再度ログオンするよう指示します。 ユーザーのプロファイルから保存されたフォルダーとファイルは、新しいプロファイルにコピーされます。

Citrix Virtual Desktops (Server VDA) を使用している場合、プロファイルのリセットを実行するにはログオンしている必要があります。その後、ユーザーはログオフし、再度ログオンしてプロファイルのリセットを完了する必要があります。

重要:

ユーザーが複数のプラットフォーム (Windows 8 や Windows 7 など) でプロファイルを持っている場合、ユーザーが問題として報告したのと同じデスクトップまたはアプリに最初に再度ログオンするよう指示します。このログオン操作により、正しいプロファイルがリセットされます。プロファイルがCitrixユーザープロファイルの場合、ユーザーのデスクトップが表示されるまでにプロファイルはすでにリセットされています。プロファイルがMicrosoftローミングプロファイルの場合、フォルダーの復元が短時間進行中の可能性があります。ユーザーは復元が完了するまでログオンしたままにする必要があります。

> プロファイルが正常にリセットされない場合 (たとえば、ユーザーがマシンに正常にログオンできない、または一部のファイルが欠落している場合) は、元のプロファイルを手動で復元する必要があります。

次の点に注意してください。

- ユーザープロファイルソリューションとしてユーザーストアが有効になっている場合、新しいプロファイルには元のユーザープロファイルから次の個人用フォルダーが含まれます。
  - デスクトップ
  - クッキー
  - お気に入り
  - ドキュメント
  - ピクチャ
  - ミュージック
  - ビデオ
- Citrix Profile Managementバージョン2407以降では、プロファイルコンテナがユーザープロファイルソリューション全体として有効になっている場合、新しいプロファイルは上記の個人用フォルダーを保持します。
- Windows 8以降では、プロファイルがリセットされると、Cookieは新しいプロファイルにコピーされません。

リセットに失敗したプロファイルを手動で復元するには

1. ユーザーにすべてのセッションからログオフするよう指示します。
2. ローカルプロファイルが存在する場合は削除します。
3. ネットワーク共有上で、フォルダー名に日付と時刻が付加されたアーカイブフォルダー（.upm_datestamp拡張子を持つフォルダー）を見つけます。
4. 現在のプロファイル名、つまりupm_datestamp拡張子がない方を削除します。
5. アーカイブされたフォルダーを元のプロファイル名にリネームします。つまり、日付と時刻の拡張子を削除します。これにより、プロファイルはリセット前の元の状態に戻ります。

PowerShell SDKを使用してプロファイルをリセットするには

Broker PowerShell SDKを使用してプロファイルをリセットできます。

NEW-BROKERMACHINECOMMAND

特定のユーザー、セッション、またはマシンへの配信のためにキューに入れられたコマンドを作成します。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerMachineCommand/>`を参照してください。

例

プロファイルをリセットするためのPowerShellコマンドレットの使用方法の詳細については、以下の例を参照してください。

Profile Managementプロファイルをリセットする

- user1のプロファイルをリセットしたいとします。New-BrokerMachineCommand PowerShellコマンドを使用します。例：
  - `New-BrokerMachineCommand -Category UserProfileManager -CommandName "ResetUpmProfile" -DesktopGroups 1 -CommandData $byteArray -SendTrigger logon -user domain1\user1`

> **重要:**
>
> `CommandData $byteArray`は次の形式である必要があります: `<SID>[,<backup path>]`。バックアップパスを指定しない場合、Profile Managementは現在の日時で名前が付けられたバックアップフォルダーを生成します。

Windowsローミングプロファイルをリセットする

- user1 のローミングプロファイルをリセットしたいとします。New-BrokerMachineCommand PowerShell コマンドを使用します。例:
  - `New-BrokerMachineCommand -Category UserProfileManager -CommandName "ResetRoamingProfile" -DesktopGroups 1 -CommandData $byteArray -SendTrigger logon -user domain1\user1`

セッションを記録する

Directorの**ユーザー詳細**画面と**マシン詳細**画面にあるセッション記録コントロールを使用して、ICA®セッションを記録できます。この機能は、**Premium**サイトのお客様にご利用いただけます。

動的セッション記録

ユーザー詳細画面のセッション記録コントロールを使用して、現在アクティブなセッションを記録できます。動的セッション記録について詳しくは、(/ja-jp/session-recording/service.html)の記事を参照してください。

ポリシーベースのセッション記録

DirectorConfigツールを使用してDirectorでポリシーベースのセッション記録を構成するには、(/ja-jp/session-recording/current-release/configure/policies/session-recording-policies.html#configure-the-director-to-use-the-session-recording-serverording-server)の「**セッション記録サーバーを使用するようにDirectorを構成する**」セクションを参照してください。 セッション記録コントロールは、ログオンしているユーザーがセッション記録ポリシーを変更する権限を持っている場合にのみDirectorで利用できます。この権限は、(/ja-jp/session-recording/current-release/configure/settings-on-session-recording-server/grant-access-rights.html)で説明されているように、セッション記録承認コンソールで設定できます。

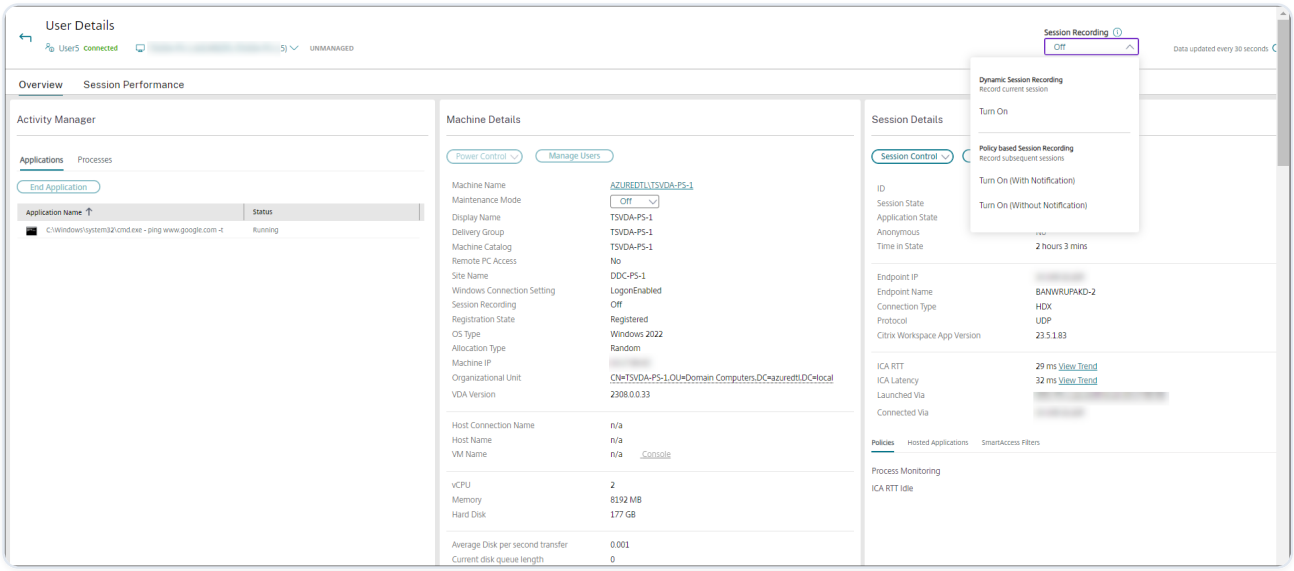
> **注:**
>
> Directorまたはセッション記録ポリシーコンソールを通じてセッション記録設定に加えられた変更は、以降のICAセッションから有効になります。

Directorのセッション記録コントロール

ユーザー詳細 > **セッション記録**アクションを使用して、現在または以降のセッションを記録できます。

- 動的セッション記録をオンにする - 現在のセッションが記録されます。
- オンにする（通知あり） - 以降のセッションが記録され、ICAセッションにログオンする際に、セッションが記録されていることがユーザーに通知されます。
- オンにする（通知なし） - 以降のセッションが記録され、ユーザーに通知することなく、セッションはサイレントに記録されます。
- オフにする - ユーザーのセッション記録を無効にする。

ポリシーパネルには、アクティブなセッション記録ポリシーの名前が表示されます。



マシン詳細パネルには、マシンのセッション記録ポリシーのステータスが表示されます。

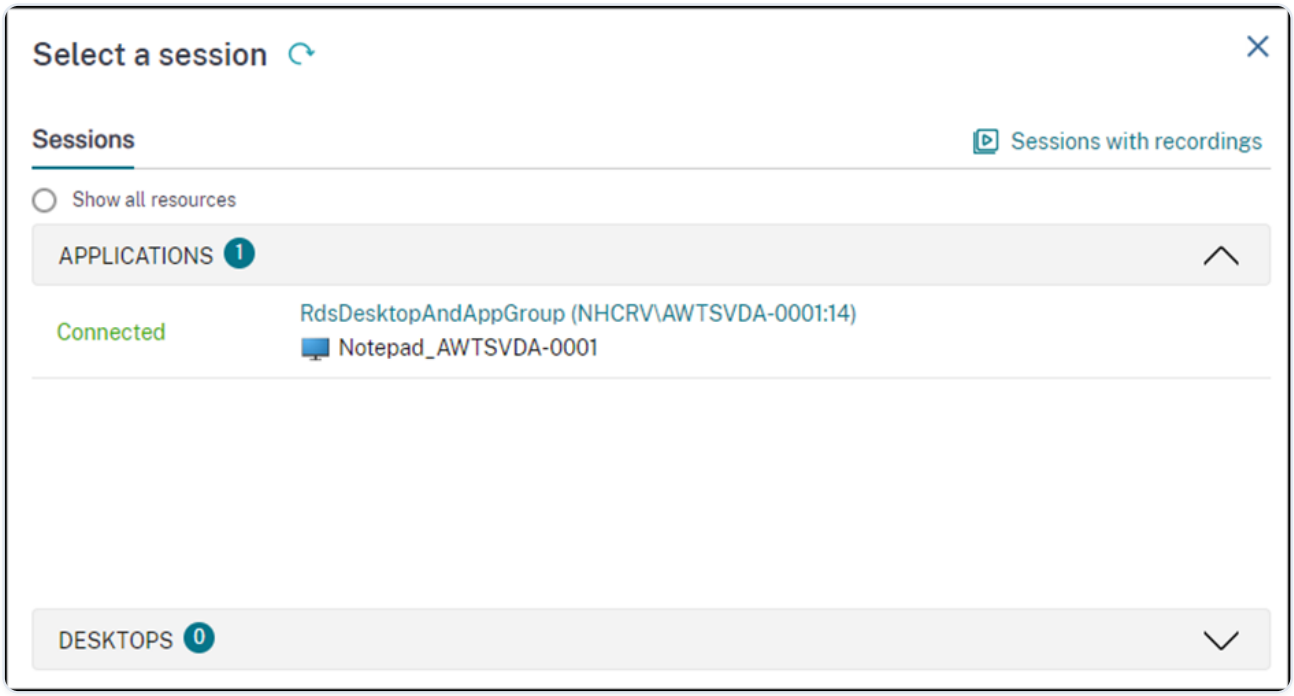
ライブセッションと録画セッションを再生する

ユーザーが遭遇した問題を理解するために、録画されたユーザーセッションとライブユーザーセッションを再生できます。Directorコンソール内で録画とセッション関連のメトリックにすぐにアクセスできるため、複数のセッション録画サーバーで録画を検索したり、録画を表示するためのサードパーティ製アプリを探したりする必要がなくなります。これにより、録画で発見された問題とパフォーマンスメトリックを関連付けるのに役立ちます。

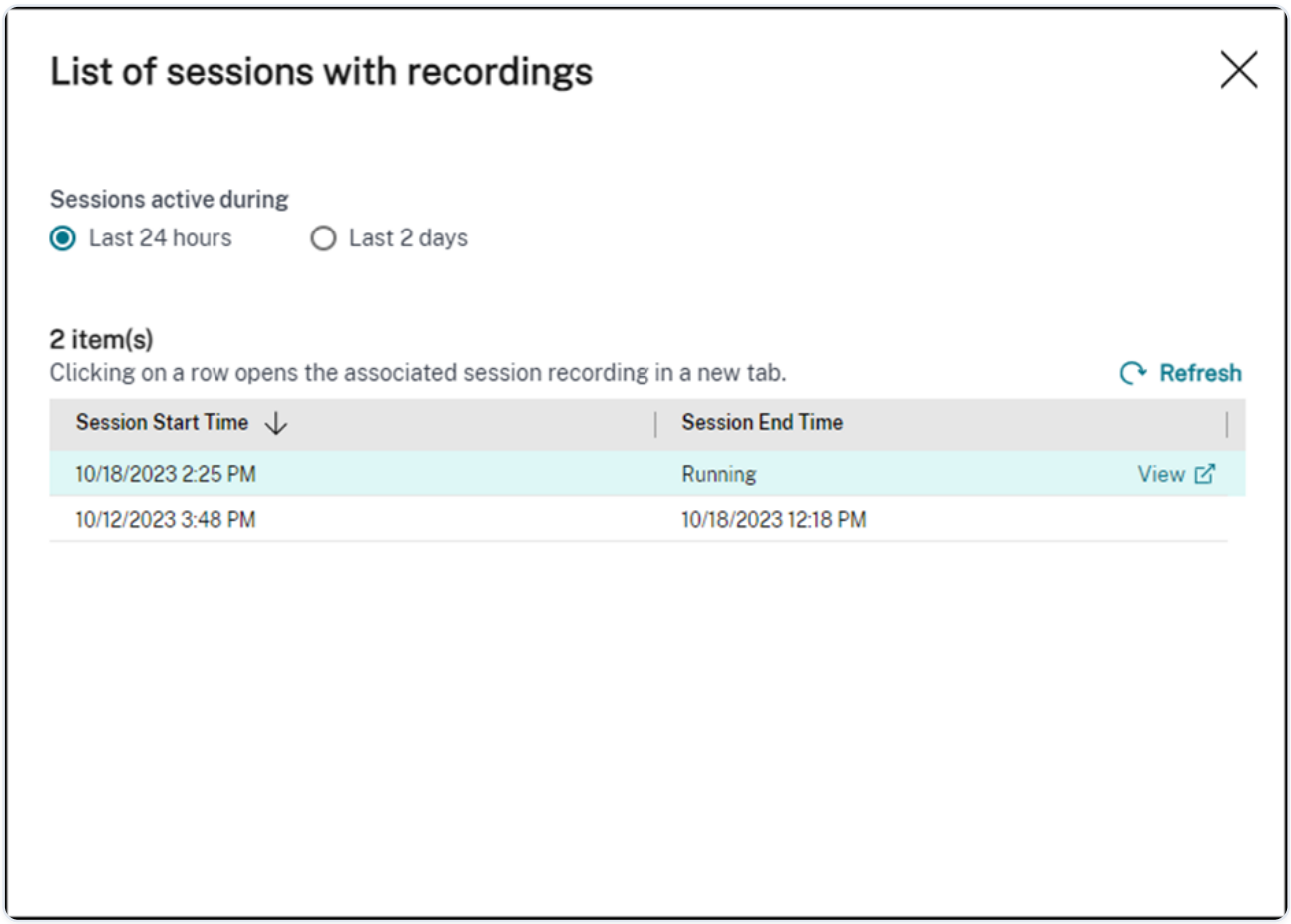
この機能には、以下が必要です。

- VDAとセッション録画サーバーはバージョン2308以降であること。
- Delivery Controller™とDirectorはバージョン2311以降であること。

Directorはセッション録画を一元的なリポジトリに保存します。「**Session Selector**」モーダル > 「**Sessions with recordings**」リンクをクリックすると、ユーザーに属する録画のリストが表示されます。



過去24時間または過去2日間にアクティブだったセッションの録画を表示することを選択できます。現在アクティブなセッションのライブ録画は、「**Session End Time**」が「**Running**」と表示されます。



「**View**」リンクをクリックすると、Citrix Session Recording再生サーバーを使用して新しいタブで録画を再生できます。

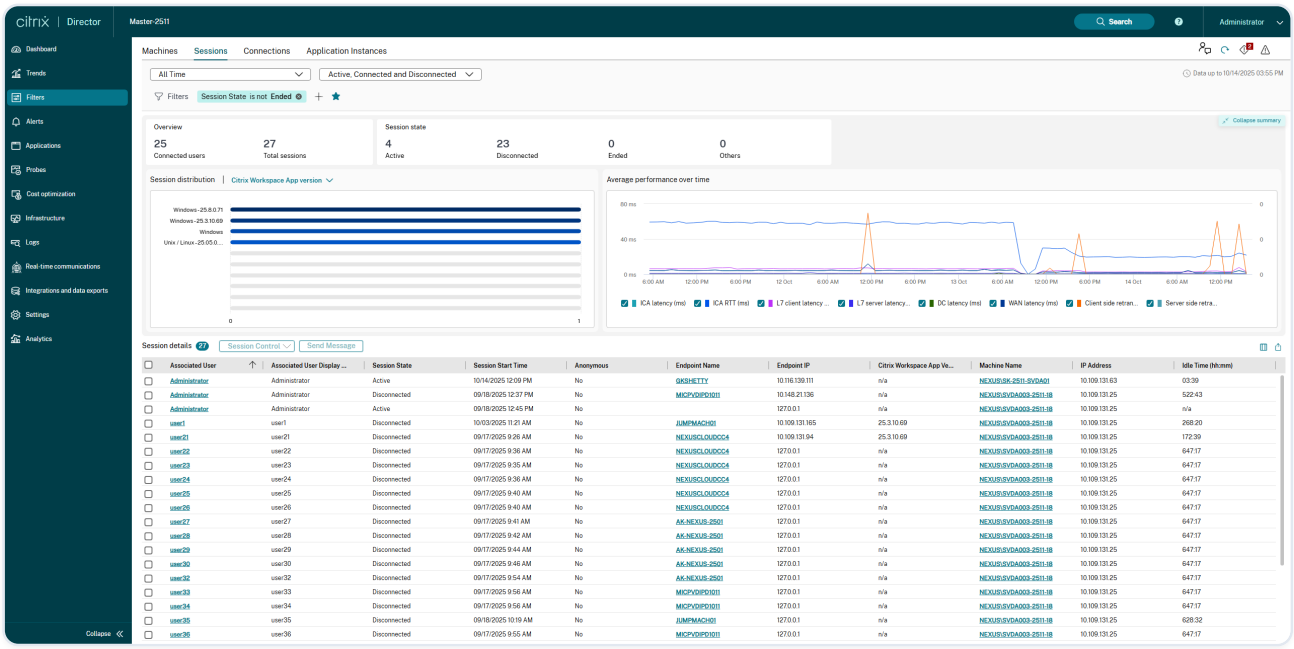
セッションビューの強化されたフィルター

1. 概要と主な機能強化

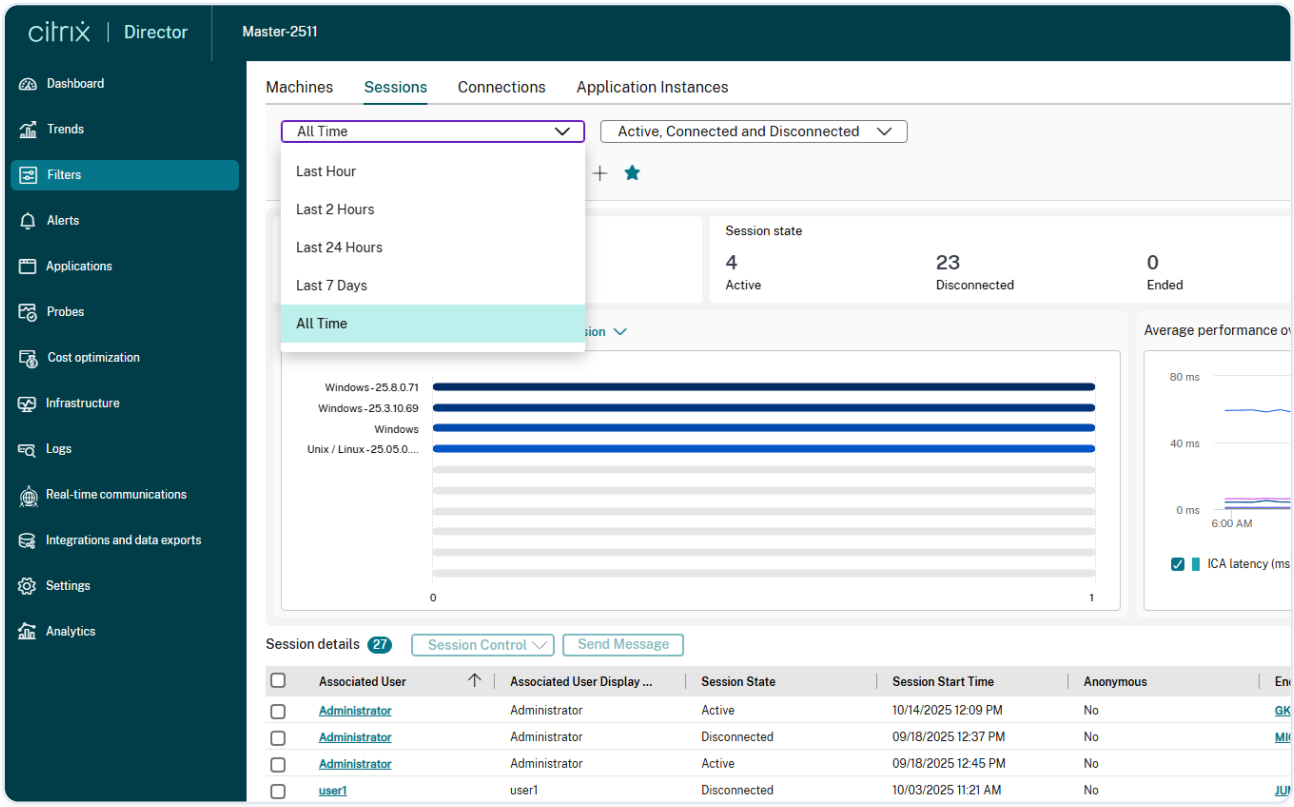
このページでは、リアルタイムおよび履歴ユーザーセッションの監視に焦点を当てたセッションビューへの主要な更新について詳しく説明します。

主な機能強化は次のとおりです。

- **新しい時間範囲フィルター**: 新しい時間範囲オプションにより、監視の精度が向上しました。
- **合理化されたフィルター管理**: デフォルトフィルターと保存済みフィルターを管理するための、新しい直感的なドロップダウン。
- **直感的なフィルター作成**: メインページで直接フィルターを作成および変更するための、新しい柔軟なワークフロー。
- **新しい視覚化**: セッションの状態とパフォーマンスの傾向に関する即座の洞察を得るための、**セッション分布**チャートと**時間の経過に伴う平均パフォーマンス**チャートの導入。



2. 新しい時間範囲フィルター



選択された時間範囲は、チャートとテーブルのデータセットを決定します。既存のオプションに加えて、新しい、きめ細かな時間フィルターを導入しました。

時間フィルター	目的	ユースケース
過去1時間	**即時アクション**。セッションアクティビティとパフォーマンスメトリックの最新ビューを提供します。	**リアルタイム監視**や、サービス再起動、ポリシー適用といった管理アクションの即時効果を観察するのに最適です。
過去2時間 (新規)	**迅速なトラブルシューティング**。急激なスパイクや低下を分析するために、直近のデータを取得します。	**インシデント後の分析**に最適で、過去2時間以内に高遅延や低IOPSなどの問題がいつ発生したかを正確に特定できます。
過去24時間	**日次概要**。1日分の集計されたパフォーマンスデータを表示します。	日々の運用チェックのデフォルト設定であり、ビジネスサイクル全体におけるピーク使用時間とリソース競合の特定に役立ちます。

時間フィルター	目的	ユースケース
過去7日間 (新規)	**週次トレンド分析**。1週間のセッション動作をより広範かつ継続的に表示します。	**キャパシティプランニング**、毎週発生するボトルネックの特定、および環境全体の安定性の評価に不可欠です。
全期間	**アクティブステータスチェック**。開始日に関係なく、**現在接続中、アクティブ、または切断されているすべてのセッション** (つまり、終了していない) を表示します。	現在の環境における**実行中のセッション**の完全な数を取得するために不可欠です。

3. 新しいフィルター管理エクスペリエンス

フィルターの選択、作成、変更のプロセスが合理化され、データテーブルのすぐ上に移動されました。

フィルター管理(/en-us/citrix-virtual-apps-desktops/current-release/media/dir-filter-management.png)

3.1. フィルターへのアクセス

フィルター管理パネルは、サイドタブから中央のドロップダウンに移動しました。

1. **デフォルトフィルター**: 標準の既製フィルター（例: アクティブ、接続済み、切断済み）が含まれています。
2. **保存済みフィルター**: 管理者が作成したすべてのカスタムフィルターセットを一覧表示します。
3. **管理**: **管理**をクリックすると、既存の保存済みフィルターを**検索**、**表示**、または**削除**できるサイドパネルが開きます。

フィルターにアクセス 1(/en-us/citrix-virtual-apps-desktops/current-release/media/dir-access-filter1.png)

フィルターにアクセス 2(/en-us/citrix-virtual-apps-desktops/current-release/media/dir-access-filter2.png)

3.2. フィルターの構築と適用

セッション概要ページで直接、複雑なフィルターセットを構築できるようになりました。

1. **フィルター**アイコンまたは既存のフィルターの横にある**+**ボタンをクリックします。

条件（例: **ワークスペースの種類**）、演算子（例: 次と等しい）、および値（例: Windows、Mac、Linux、HTML5、Chrome、不明）を選択します。

フィルターを構築 1(/en-us/citrix-virtual-apps-desktops/current-release/media/dir-build-filter1.png)

フィルターを構築 2(/en-us/citrix-virtual-apps-desktops/current-release/media/dir-build-filter2.png)

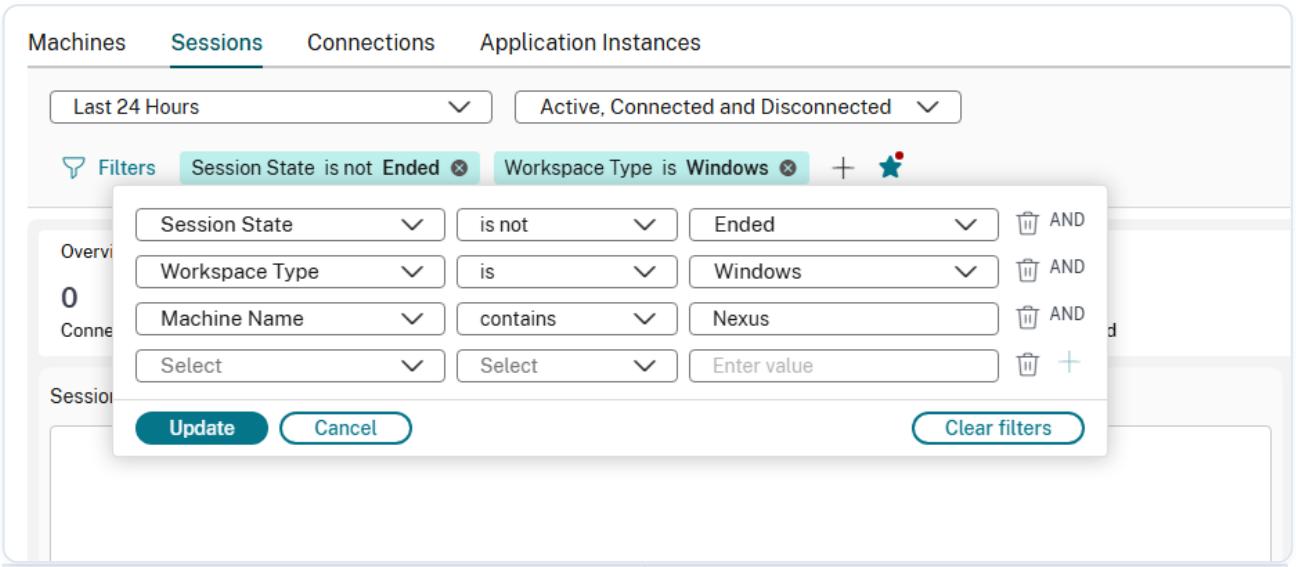
3.3. フィルター保存ステータスとワークフロー

アクティブなフィルターの横にある星のアイコン (⋆) は、現在のフィルターセットのステータスを視覚的に示します。これにより、管理者はカスタムフィルターの保存、適用、管理を行うことができます。

フィルターステータス	アイコンの外観	意味	必要な操作
未保存のフィルター	 (赤い点が付いた空のアウトライン)	現在のフィルター条件の組み合わせは**保存されていません**。	**空の星**をクリックしてダイアログボックスを開き、フィルターセットに名前を付けて保存します。
保存済みフィルター	 (塗りつぶし / 実線)	現在アクティブなフィルターセットは、以前に保存されたフィルターと**完全に一致**しています。	アクションは不要です。定義済みのテンプレートに基づいてデータを表示しています。
変更が加えられた保存済みフィルター	 (赤い点で塗りつぶし)	**保存済みフィルター**を使用しているときに、他のフィルターが追加または削除された場合、あるいは列がソートされた場合、変更が**まだ保存されていない**ことを示す赤い点が表示されます。	既存の保存済みフィルターを更新するには**赤い点が付いた星**をクリックするか、ドロップダウンを使用して**フィルターセットとして保存**を選択して新しいものを作成します。
デフォルトフィルター			

3.4. フィルターアクションボタン

新しいフィルターを追加したり、保存済みのフィルターを変更したりすると、以下のコントロールとステータスインジケーターが利用可能になります。

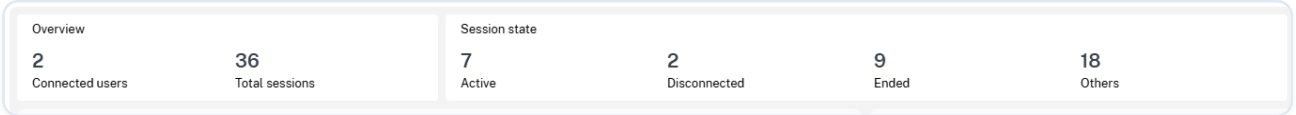


ボタン	意味と操作
更新	現在アクティブなすべてのフィルター条件をグラフとアプリケーションパフォーマンスデータテーブルに適用します。
キャンセル	現在のフィルターセットに加えられた変更を破棄し、最後に適用されたフィルターに戻します。
フィルターをクリア	新しく追加されたすべてのフィルター条件を削除します。
アイコン	このアイコンがクリックされた、選択されたフィルター条件を削除します。

4. 新しい視覚化: セッション分析

セッションの動作とパフォーマンスに関する即時かつグラフィカルな洞察を提供するために、2つの新しいグラフが追加されました。

4.1. サマリーパネル

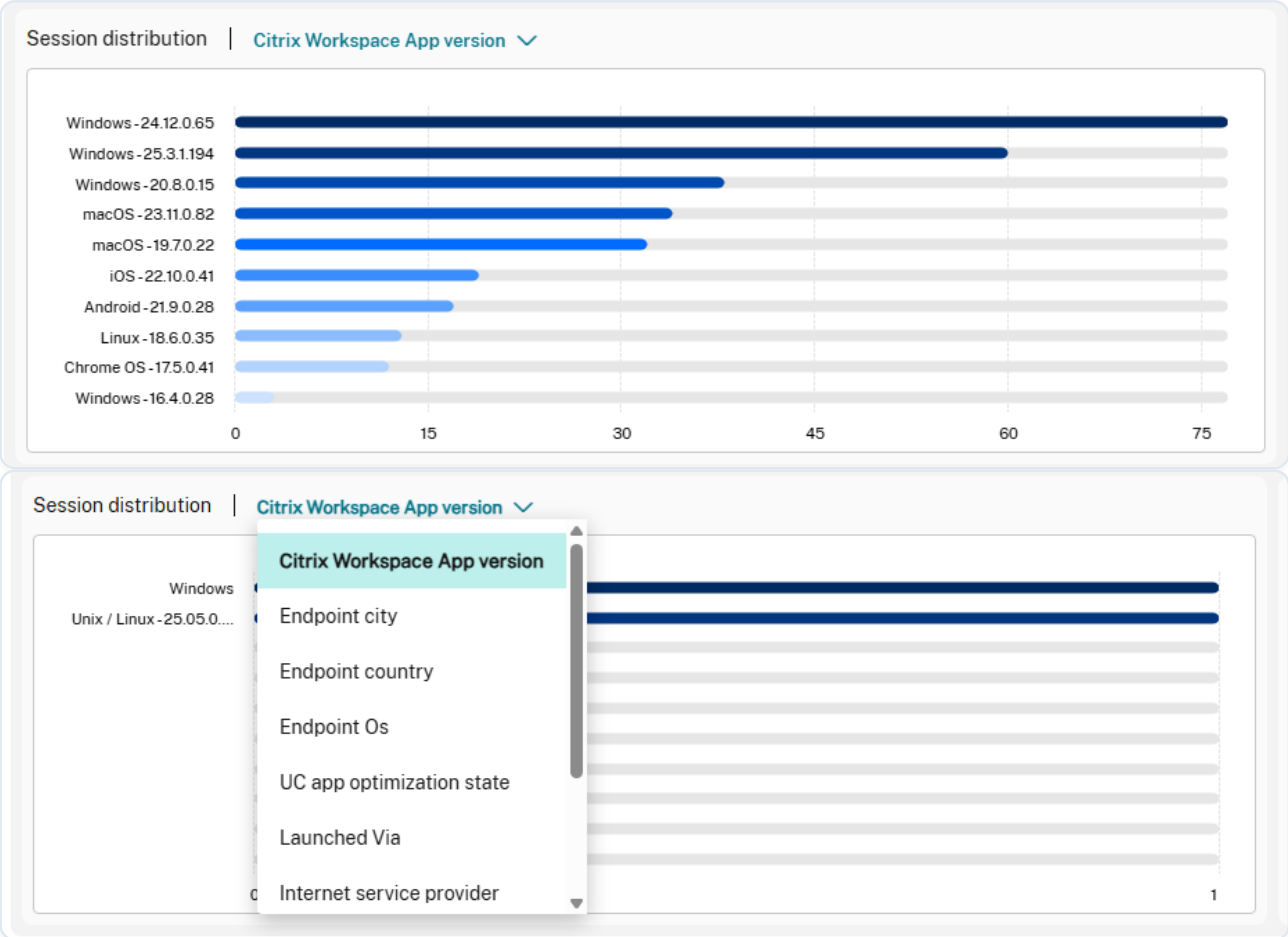


- **概要**: 接続ユーザーの総数と、それらに関連付けられたセッションの総数を表示します。

- **セッションの状態**: アクティブ、切断、終了、その他といった状態に基づいてセッション数を表示します。

このサマリーは折りたたみ可能で、管理者が上記の分類に基づいて必要なアクションを実行するのに役立ちます。たとえば、長時間実行されているセッションを把握して必要に応じて終了したり、切断されたセッションに基づいてネットワーク障害を特定したりできます。

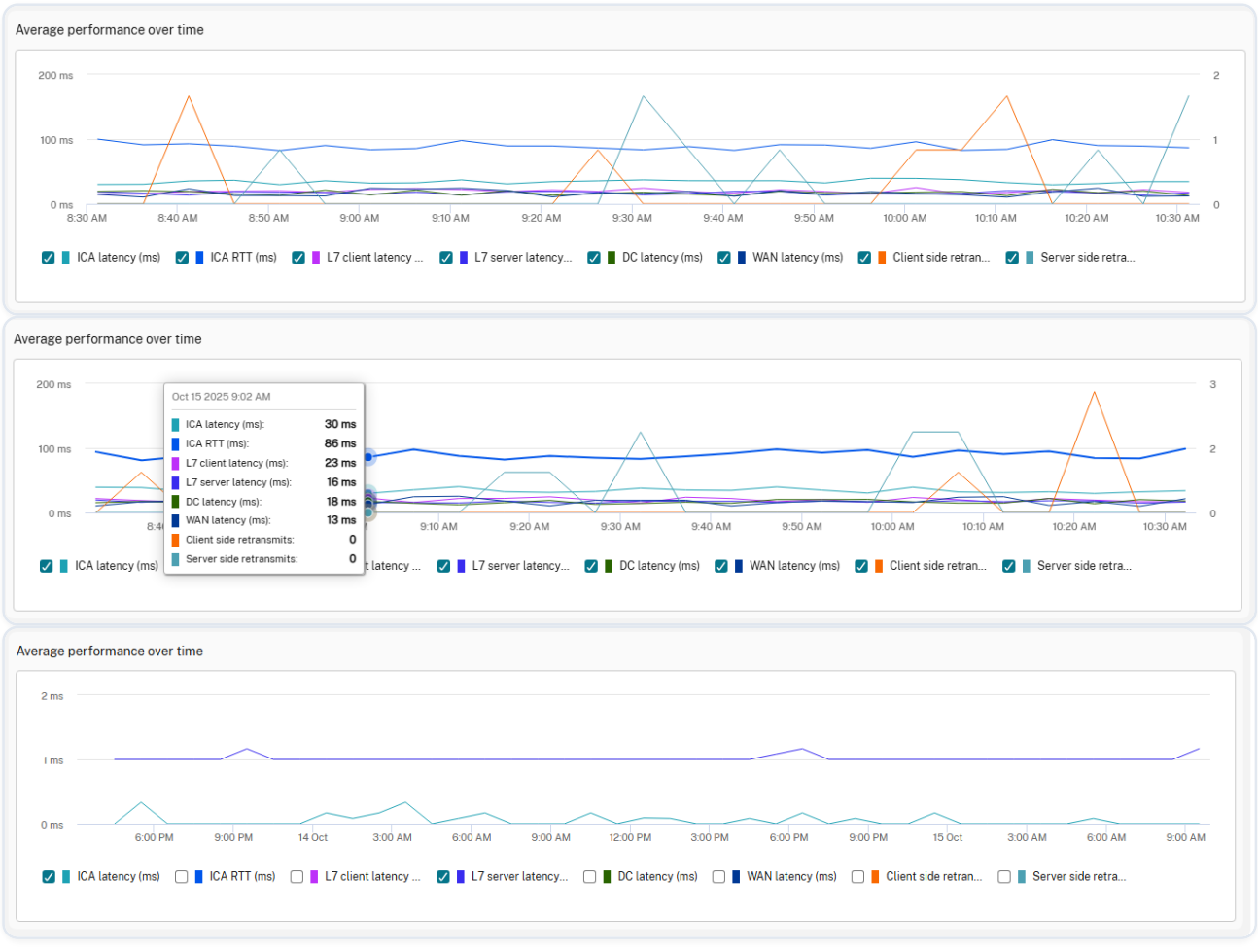
4.2. セッション分布



- **目的:** このグラフは、現在フィルターされているセッションを、選択されたカテゴリメトリック（デフォルトは**Citrix Workspace Appバージョン**）で分類します。
- **ユーティリティ:** 管理者がユーザー環境、クライアントバージョン、接続設定に基づいてセッションの傾向を迅速に特定するのに役立ちます。たとえば、**ワークスペースの種類**でフィルタリングすると、Mac、Windows、またはHTML5クライアント経由で接続しているユーザーの数を確認できます。
- **サポートされるフィルターの種類:** 分布は以下によってセグメント化できます。
  - Citrix Workspaceアプリのバージョン
  - エンドポイントの都市
  - エンドポイントの国

- UCアプリの最適化状態
- 起動元
- インターネットサービスプロバイダー
- マシン名
- プロトコル
- ワークスペースの種類

4.3. 時間経過に伴う平均パフォーマンス



- **目的:** 現在のフィルターと時間範囲に含まれるセッションの主要なセッションパフォーマンスメトリックを追跡します。
- **追跡される主要なメトリック:** このグラフは、ユーザーエクスペリエンスに不可欠なメトリックに焦点を当てています。
  - ICA遅延 (ms)
  - ICA RTT (ms)
  - L7クライアント遅延 (ms)
  - L7サーバー遅延 (ms)

  - DC遅延 (ms)
  - WAN遅延 (ms)
  - クライアント側の再送信
  - サーバー側の再送信

- **用途**: ユーザーの苦情を過去のパフォーマンスデータと迅速に相関させるために不可欠です。このグラフにおける遅延または再送信の急激な上昇は、ユーザーエクスペリエンスに影響を与える可能性のあるネットワークまたはVDAのパフォーマンス問題を示しています。

マシンのトラブルシューティング

> **注:**
>
> **Citrix Health Assistant** は、未登録のVDAにおける構成の問題をトラブルシューティングするためのツールです。このツールは、VDA登録の失敗、セッション起動の問題、タイムゾーンリダイレクト構成の問題の根本原因を特定するために、いくつかのヘルスチェックを自動化します。Knowledge Centerの記事「Citrix Health Assistant - Troubleshoot VDA Registration and Session Launch」には、**Citrix Health Assistant** ツールのダウンロードと使用方法が記載されています。

> Directorコンソールの **フィルター > マシン** ビューには、サイトで構成されているマシンが表示されます。「マルチセッションOSマシン」タブには、パフォーマンスカウンターの分布を示すロード評価インデックスと、リンクにカーソルを合わせるとセッション数のツールヒントが表示されます。

失敗したマシンの **失敗理由** 列をクリックすると、失敗の詳細な説明と、その失敗をトラブルシューティングするために推奨されるアクションが表示されます。マシンおよび接続の失敗の理由と推奨されるアクションは、「Citrix Director の失敗理由とトラブルシューティング」で確認できます。

マシン名のリンクをクリックすると、**マシン詳細** ページに移動します。

マシン詳細ページには、マシンの詳細、インフラストラクチャの詳細、およびマシンに適用されたホットフィックスの詳細が一覧表示されます。

前提条件

- uberAgentはVDAにインストールされている必要があります

- **Windows VDAバージョン**: 2511以降

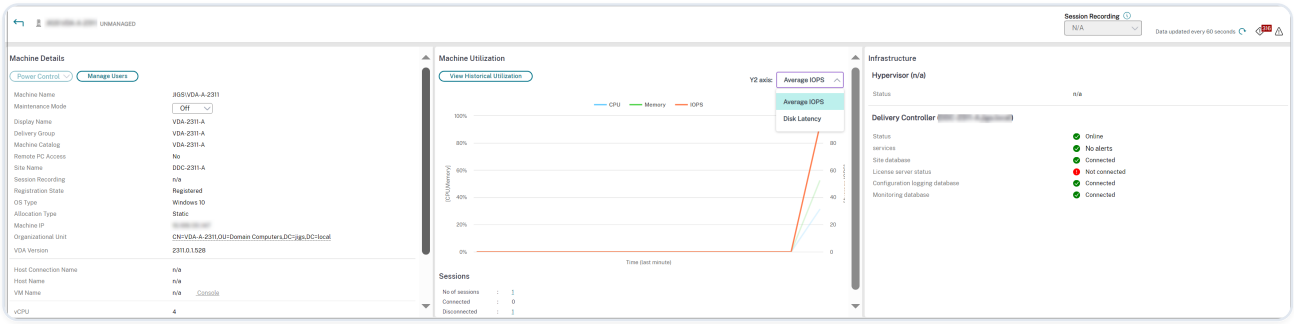
メトリック

メトリック	説明
平均CPU使用率 (%)	
平均RAM使用率 (%)	
平均ディスクIOPS	
平均ディスク待機時間 (ms)	
平均GPU使用率 (%)	
平均ネットワーク使用率 (%)	
平均負荷インデックス	
平均ディスク使用率 (%)	
平均プロファイルディスク使用率 (%)	
平均CPUアイドル率 (%)	
平均ページファイル使用率 (%)	
平均CPU相対周波数 (%)	

マシンベースのリアルタイムリソース使用率

マシン使用率パネルには、CPUとメモリのリアルタイム使用率を示すグラフが表示されます。さらに、Delivery ControllerとVDAのバージョンが**7.14**以降のサイトでは、ディスクおよびGPU監視グラフも利用できます。

ディスク監視グラフ、平均IOPS、およびディスク遅延は、VDAディスクに関連する問題を監視およびトラブルシューティングするのに役立つ重要なパフォーマンス測定値です。平均IOPSグラフは、ディスクへの読み取りおよび書き込みの平均数を表示します。**ディスク遅延**を選択すると、データ要求からディスクからの応答までの遅延（ミリ秒単位で測定）を示すグラフが表示されます。



GPU使用率

マルチセッションおよびシングルセッションOS VDAでのGPU関連の問題をトラブルシューティングするには、**GPU使用率**を選択して、GPU、GPUメモリ、エンコーダー、およびデコーダーの利用率（パーセンテージ）を確認します。

サポートされているGPUバージョン:

- ディスプレイドライバーバージョン369.17以降を実行しているNVIDIA Tesla M60 GPU。詳細については、「NVIDIA vGPU Software」を参照してください。
- AMD Radeon Instinct MI25 GPUおよびAMD EPYC 7V12(Rome) CPU。詳細については、「AMD Drivers and Support」を参照してください。

ドライバー:

適切なドライバーまたは拡張機能をVDAにインストールする必要があります。

- NVIDIA GPUの場合、GRIDドライバーを手動または拡張機能経由でインストールします。詳細については、NVIDIA vGPU Softwareを参照してください。
  - NVIDIAの場合、GRIDドライバーのみがサポートされています。CUDAドライバーはNVadsA10 v5シリーズでは動作せず、サポートされていません。
  - Azureベースのマシンに拡張機能経由でNVIDIA Grid GPUドライバーをインストールする手順の例については、NVIDIA GRID drivers. NVIDIA GPU Driver Extension - Azure Windows VMs - Azure Virtual Machinesを参照してください。
  - NVIDIA Grid GPUドライバーを手動でインストールする手順の例については、Azure N-series NVIDIA GPU driver setup for Windows - Azure Virtual Machinesを参照してください。
- AMD GPUの場合、AMDグラフィックドライバーを手動または拡張機能経由でインストールします。詳細については、AMD Drivers and Supportを参照してください。

- Azureベースのマシンに拡張機能経由でAMD GPUドライバーをインストールする手順の例については、AMD GPU Driver Extension - Azure Windows VMs - Azure Virtual Machinesを参照してください。
- AzureマシンにAMD GPUドライバーを手動でインストールする手順の例については、Install AMD GPU drivers on N-series VMs running Windowsを参照してください。

使用上の注意:

- GPU使用率グラフは、64ビットWindowsを実行しているVDAでのみ利用可能です。
- GPUアクセラレーションを提供するには、VDAでHDX 3D Proが有効になっている必要があります。詳細については、GPU acceleration for Windows Single-session OSおよびGPU acceleration for Windows Multi-session OSを参照してください。
- VDAが複数のGPUにアクセスする場合、使用率グラフには個々のGPUから収集されたGPUメトリックの平均が表示されます。GPUメトリックはVDA全体に対して収集され、個々のプロセスに対しては収集されません。
- AMDの場合、エンコーダーとデコーダーの使用状況は個別にサポートされていません。GPUを使用するエンコード/デコードのワークロードは、GPU使用率における一般的な3D負荷として報告されます。
- インストール中にNVIDIA WMIをインストールしてください。このウィンドウは手動インストール時にのみ利用可能です。
- ドライバーがインストールされているが、DirectorがGPUを検出しない場合
  - タスクマネージャーを確認します。ドライバーが適切にインストールされていれば、GPUはタスクマネージャーに表示されるはずです。
  - マシンが登録されているか確認します。マシンがオンラインとして検出されるまでに時間がかかる場合があります。
- DirectorでGPU使用率にアクティビティが表示されない場合は、実行しているワークロードがGPUを使用していることを確認してください。グラフィックワークロードの場合、これは > > > > から有効にできます。「高パフォーマンス」をオンにしてください。場合によっては、他の設定に基づいて、これがシステムデフォルトまたは省電力に設定されていると、Windowsはグラフィックワークロードに CPUを使用するようデフォルトで設定されます。
- データは1分ごとに更新され、**GPU使用率**を選択してから1分以内にデータの視覚化が開始されます。

マシンベースの履歴リソース使用率

マシン使用率パネルで、**履歴使用率の表示**をクリックして、選択したマシンのリソースの履歴使用率を表示します。 使用率グラフには、CPU、メモリ、ピーク時の同時セッション、平均IOPS、ディスク遅延の重要なパフォーマンスカウンターが含まれます。

> **注:**
>
> 監視ポリシー設定の**プロセス監視を有効にする**は、履歴マシン使用率ページの「上位10プロセス」テーブルでデータを収集および表示するために、「許可」に設定する必要があります。収集はデフォルトで禁止されています。

> CPUとメモリの使用率、平均IOPS、ディスク遅延のデータはデフォルトで収集されます。**リソース監視を有効にする**ポリシー設定を使用して、収集を無効にできます。



1. **マシン詳細**ビューの**マシン使用率**パネルから、**履歴使用率の表示**を選択します。
2. **履歴マシン使用率**ページで、**期間**を「過去2時間」、「過去24時間」、「過去7日間」、「月」、「年」に設定して使用状況を表示します。

> **注:**
>
> 平均IOPSとディスク遅延の使用状況データは、現在までの過去24時間、月、年についてのみ利用可能です。カスタム終了時刻はサポートされていません。

3. **適用**をクリックし、必要なグラフを選択します。
4. グラフの異なるセクションにカーソルを合わせると、選択した期間の詳細情報が表示されます。



例えば、**過去2時間**を選択した場合、ベースライン期間は選択した時間範囲の前の2時間です。過去2時間およびベースライン期間のCPU、メモリ、セッションの傾向を表示します。**先月**を選択した場合、ベースライン期間は前月です。先月およびベースライン期間の平均IOPSとディスク遅延を表示するように選択します。

1. 選択した期間のリソース使用率データをエクスポートするには、**エクスポート**をクリックします。詳細については、「展開の監視」のレポートのエクスポートセクションを参照してください。
2. グラフの下の表には、CPUまたはメモリ使用率に基づいて上位10個のプロセスが一覧表示されます。選択した時間範囲におけるアプリケーション名、ユーザー名、セッションID、平均CPU、ピークCPU、平均メモリ、ピークメモリを表示する任意の列で並べ替えることができます。IOPSとディスク遅延の列は並べ替えることができません。

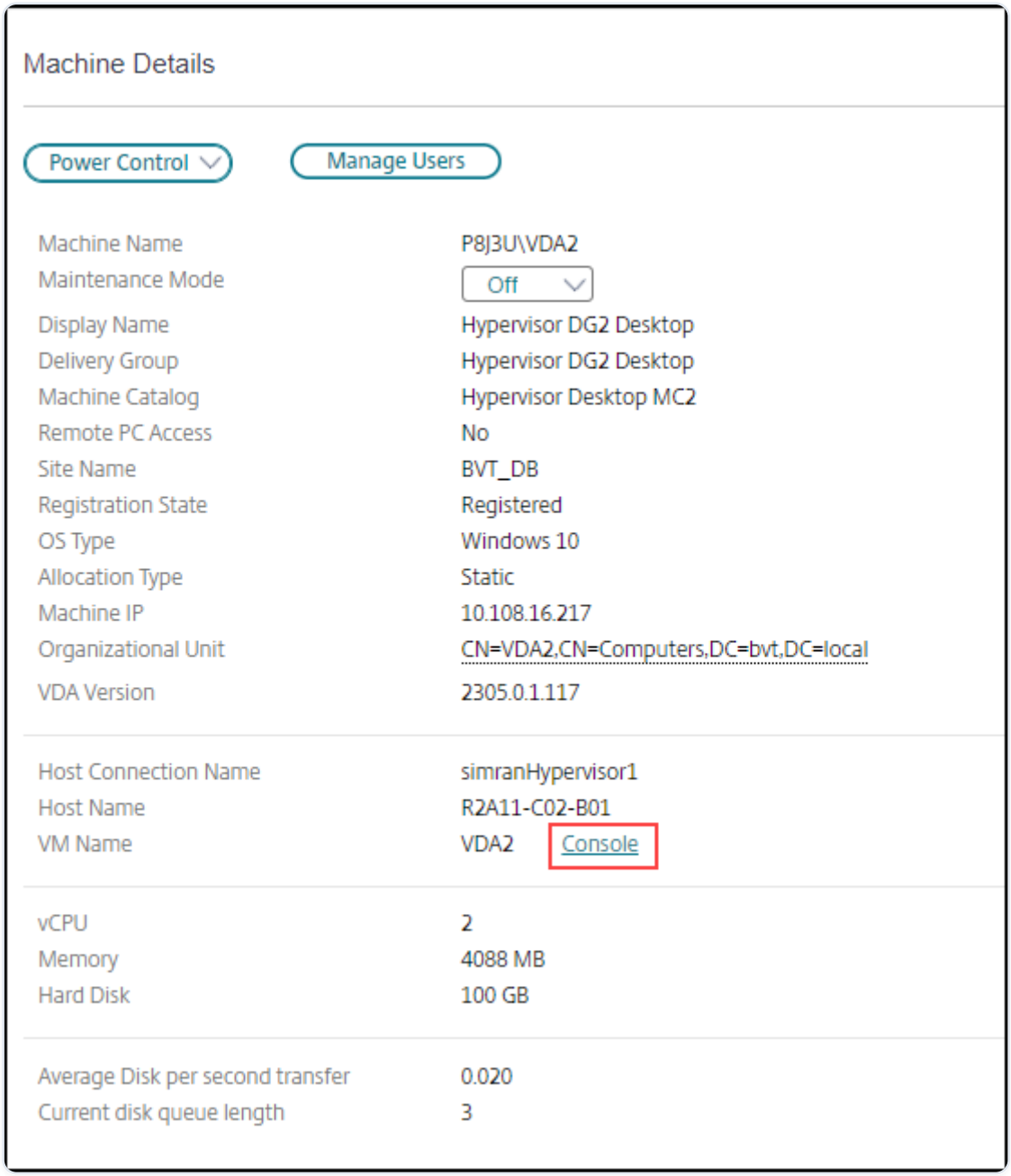
> **注:**
>
> システムプロセスのセッションIDは「0000」と表示されます。

3. 特定のプロセスのリソース消費の履歴傾向を表示するには、上位10個のプロセスのいずれかをドリルダウンします。

マシンコンソールへのアクセス

XenServerバージョン7.3以降でホストされているシングルセッションおよびマルチセッションOSマシンのコンソールには、Directorから直接アクセスできます。これにより、XenServerでホストされているVDAの問題をトラブルシューティングするためにXenCenterは必要ありません。この機能を利用するには：

- バージョン7.16以降のDelivery Controllerが必要です。
- マシンをホストしているXenServerはバージョン7.3以降である必要があり、Director UIからアクセスできる必要があります。



マシンのトラブルシューティングを行うには、対応するマシン詳細パネルの**コンソール**リンクをクリックします。提供されたホスト資格情報が認証されると、WebベースのVNCクライアントで

あるnoVNCを使用して、マシンコンソールが別のタブで開きます。これで、コンソールにキーボードとマウスでアクセスできるようになります。

注:

- この機能はInternet Explorer 11ではサポートされていません。
- マシンコンソールのマウスカーソルがずれている場合は、問題を解決する手順についてCTX230727を参照してください。
- Directorは新しいタブでコンソールアクセスを起動します。ブラウザの設定でポップアップが許可されていることを確認してください。
- セキュリティ上の理由から、Citrix®はブラウザにSSL証明書をインストールすることを推奨しています。

最近の電源操作があるマシンを検査する

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

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

注:

データは電源管理されているマシンでのみ利用可能です。この機能がサポートされる前に実行された電源操作のデータは利用できません。

以下の方法で、マシンの電源操作ステータスを表示できます。

フィルター -> **マシン** タブから。この場合、デフォルトで**電源操作時刻**と**電源操作結果**の列が表示されます。表示したい列を選択することもできます。

コスト最適化タブから。この場合、デフォルトのフィルターは**電源操作のトリガー元**が*Autoscale™*に設定され、**電源操作結果**が*失敗*に設定されています。

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

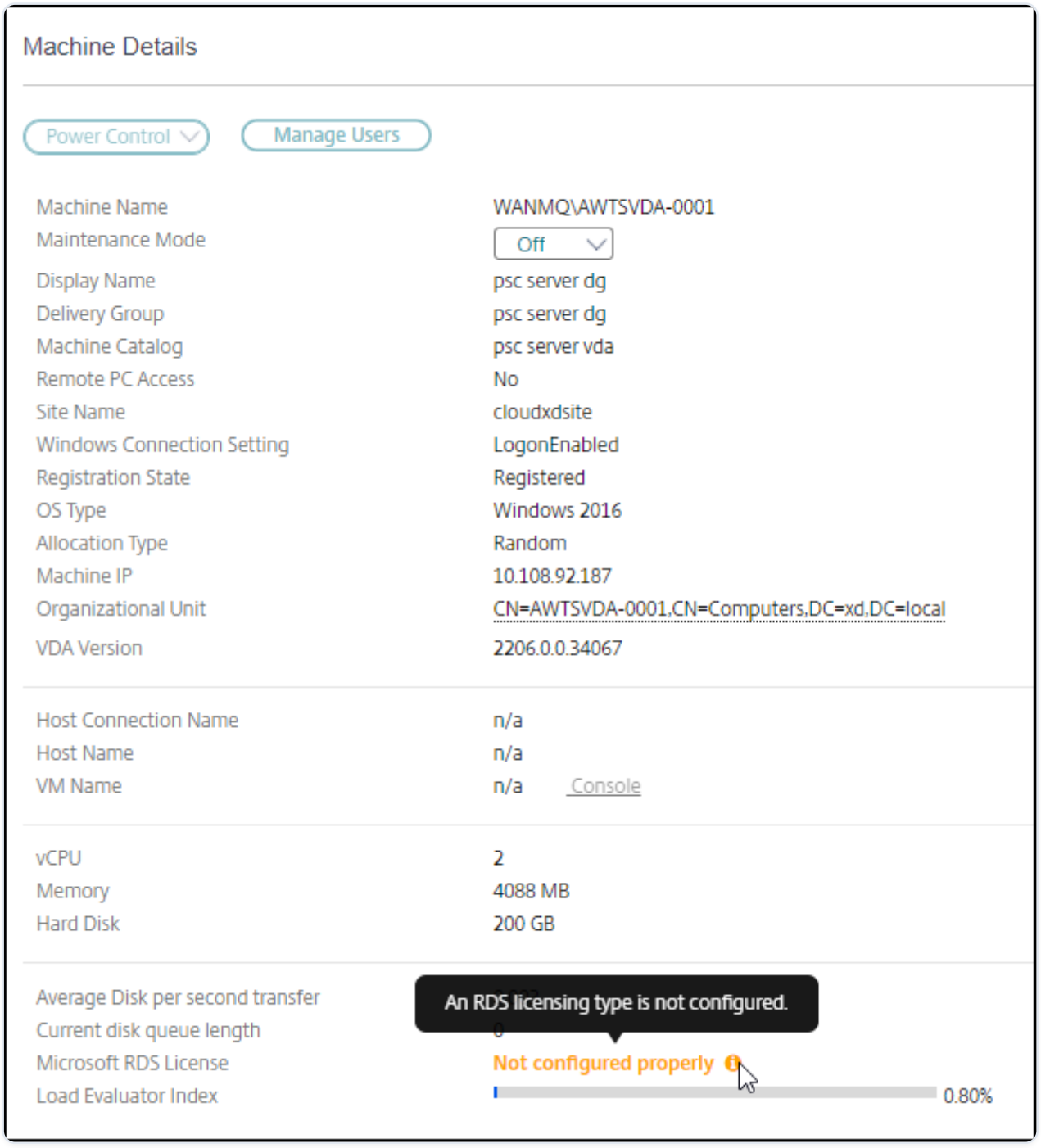
電源操作ステータスを表示するために、以下のフィルターが追加されました。

フィルター	説明
電源操作結果	電源操作の結果を表示します。可能なフィルター値は「成功」と「失敗」です。
電源操作のトリガー元	電源操作をトリガーしたユーザーまたは内容を表示します。可能なフィルター値は次のとおりです。 • オートスケール - この値は、電源操作が次によってトリガーされた場合に表示されます。 • 管理者がVMのOSディスクを初期状態に戻すためにVMをシャットダウンした場合 • 設定されたポリシーに基づいてVMがシャットダウンまたは一時停止された場合 • プールサイズまたはバッファサイズの設定に基づいてVMが利用可能になった場合 • 管理者 - この値は、電源操作が管理者によってトリガーされた場合に表示されます。考えられる例としては、管理者がVMの電源オフ、電源オン、一時停止、

フィルター	説明
	再開、再起動、またはリブートを要求した場合などがあります。
	• ユーザー - この値は、電源操作がユーザーによってトリガーされた場合に表示されます。例としては、ユーザーがVMをリセット、電源オン、または作業を再開した場合などがあります。
	• その他 - この値は、電源アクションがスケジュールされた理由と不明な理由によってトリガーされた場合に表示されます。
最終電源アクション	マシンで発生した正確な電源操作（電源オン、電源オフ、シャットダウン、再起動、リセット、再開など）を表示します。
電源アクション時刻	電源アクションが完了した時刻。可能なフィルター値は、過去1分、過去5分、過去30分、過去1時間、今日、過去24時間、昨日です。
電源アクション失敗理由	失敗の理由を表示します。可能なフィルター値は、ハイパーバイザー報告の失敗、ハイパーバイザーのレート制限超過、不明なエラー、なしです。アクションが成功した場合は、「なし」と表示されます。

Microsoft RDSライセンスの健全性

マルチセッションOSマシンでは、**マシン詳細**ページと**ユーザー詳細**ページの**マシン詳細**パネルでMicrosoft RDSライセンスのステータスを表示できます。



次のいずれかのメッセージが表示されます。

- ライセンス利用可能
- 適切に構成されていません（警告）
- ライセンスエラー（エラー）
- 互換性のないVDAバージョン（エラー）

> **注:**

有効なライセンスを持つ猶予期間中のマシンのMicrosoft RDSライセンスの健全性ステータスは、緑色で**ライセンス利用可能**メッセージを表示します。ライセンスの有効期限が切れる前に更新してください。

警告メッセージとエラーメッセージについては、情報アイコンにカーソルを合わせると、次の表に示す追加情報が表示されます。

メッセージの種類	DIRECTOR内のメッセージ
エラー	VDAバージョン7.16以降で利用可能です。
エラー	新しいRDS接続は許可されていません。
エラー	Microsoft RDSライセンスの猶予期間が過ぎました。
エラー	必要なOSレベルに対して、デバイスごとのクライアントアクセスライセンスの種類でライセンスサーバーが構成されていません。
エラー	構成されているライセンスサーバーは、デバイスごとのクライアントアクセスライセンスの種類でRDSホストOSレベルと互換性がありません。
警告	Personal Terminal Serverは、Citrix Virtual Apps and Desktops™展開において有効なRDSライセンスの種類ではありません。
警告	管理用リモートデスクトップは、Citrix Virtual Apps and Desktops™展開では有効なライセンスの種類ではありません。
警告	RDSライセンスの種類が構成されていません。
警告	ユーザーごとのクライアントアクセスRDSライセンスの種類では、ドメインコントローラーまたはライセンスサーバーに到達できません。

メッセージの種類	DIRECTOR内のメッセージ
警告	デバイスごとのクライアントアクセスライセンスの種類では、必要なOSレベルのライセンスサーバーに到達できないため、クライアントデバイスライセンスを判別できません。

注:

この機能は、Microsoft RDS CAL (クライアントアクセスライセンス) にのみ適用されます。

ハイブリッドマルチクラウド展開のための統合検索

以前は、トリアージ中にDirectorでユーザーを検索すると、そのユーザーがオンプレミスサイトのユーザーである場合にのみ、ユーザーの詳細が表示されました。ユーザーがクラウドサイトのユーザーである場合は、Monitorに移動して再度検索する必要がありました。

この強化された検索機能により、Directorの**検索**オプションを使用して、クラウドサイトまたはオンプレミスサイトのユーザーを検索できます。この機能は、ハイブリッド展開（クラウドサイトとオンプレミスサイトの両方）を使用している場合や、トリアージ目的でDirectorを使用している場合に利用できます。オンプレミスサイトかクラウドサイトかに関わらず、ユーザーの詳細を取得できます。サイトがDirectorに存在する場合は、選択したセッションのActivity ManagerにDirector内で直接移動できます。サイトがDirectorに存在しない場合は、選択したセッションのActivity ManagerにMonitor内で直接移動できます。その後、トリアージを続行できます。

注:

Citrix Directorを介して統合検索コンソールを使用できます。

この機能により、問題解決までの平均時間が短縮され、クラウドユーザーとオンプレミスユーザーの両方に単一のコンソールでシームレスなエクスペリエンスを提供します。追加の利点として、クラウドサイトの詳細のみがDirectorに追加されるため、データベースのサイズが急速に増大することはありません。ユーザーの詳細はクラウド自体に保存されます。

注:

> 最大6つ以下のクラウドサイトの場合、検索結果を3秒以内に取得できます。

> この機能を有効にするには、クラウドサイトをDirectorに接続する必要があります。

Directorへのクラウドサイトの接続

前提条件

Citrix Directorで統合検索を構成するために、新しいコンポーネントをインストールする必要はありません。次の要件が満たされていることを確認してください。

- 統合検索の場合、すべてのDelivery ControllerおよびDirectorがインストールされているマシンで、アウトバウンドインターネットアクセスが利用可能である必要があります。具体的には、次のURLへのアクセスが可能であることを確認してください。
  - Citrix キー登録: `<https://*.citrixnetworkapi.net/>`
  - シトリックス クラウド：`<https://*.citrixworkspacesapi.net/>`
  - シトリックス DaaS：`<https://*.cloud.com/>`
  - マイクロソフト Azure：`<https://*.windows.net/>`
- Delivery ControllerおよびDirectorマシンがイントラネット内にあり、アウトバウンドインターネットアクセスがプロキシサーバーを介している場合は、次のことを確認してください。
  - プロキシサーバーは、上記のURLリストを許可する必要があります。
  - Directorの**web.config**ファイルと**citrix.monitor.exe.config**ファイルに次の構成を追加します。この構成は**configuration**タグ内に必ず追加してください。

```
<system.net>

    <defaultProxy>

        <proxy usesystemdefault="false" proxyaddress="http://
<your_proxyserver_address>:80" bypassonlocal="true" />

    </defaultProxy>

</system.net>
```

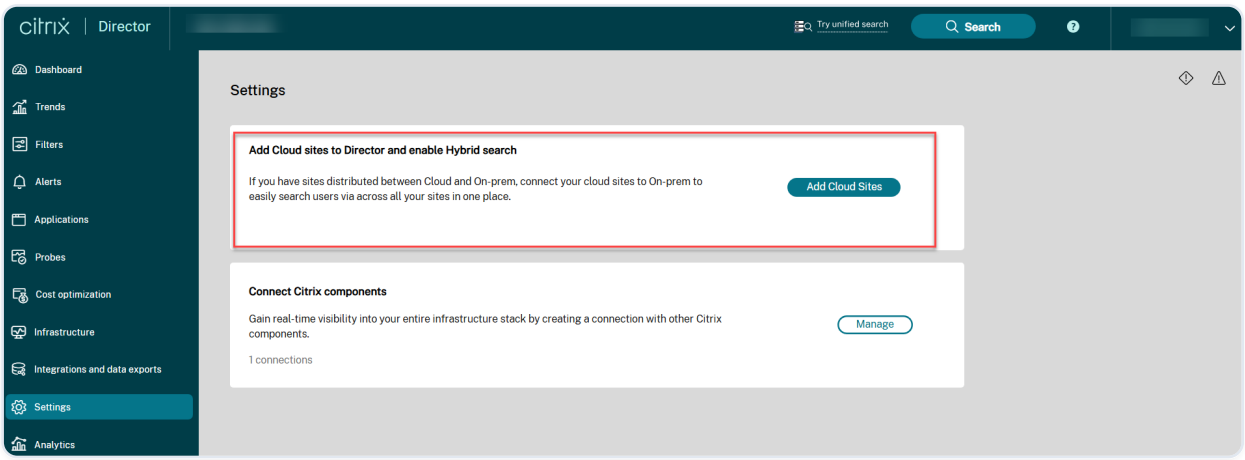
- Directorの**web.config**は、Directorがインストールされているマシンの`C:\inetpub\wwwroot\Director\web.config`にあります。
- **citrix.monitor.exe.config**は、Delivery Controllerがインストールされているマシンの`C:\Program Files\Citrix\Monitor\Service\Citrix.Monitor.exe.Config`にあります。

この設定は、IIS上のMicrosoftによって提供されます。詳細については、「プロキシ構成」を参照してください。構成ファイルの**defaultproxy**フィールドは、DirectorおよびMonitor Serviceのアウトバウンドアクセスを制御します。Citrix DaaSとの構成および通信には、**defaultproxy**フィールドをtrueに設定する必要があります。有効なポリシーによってこのフィールドがfalseに設定されている可能性があります。この場合、手動でフィールドをtrueに設定する必要があります。変更を行う前に、構成ファイルのバックアップを取ってください。変更を反映するには、Delivery Controllerで監視サービスを再起動します。

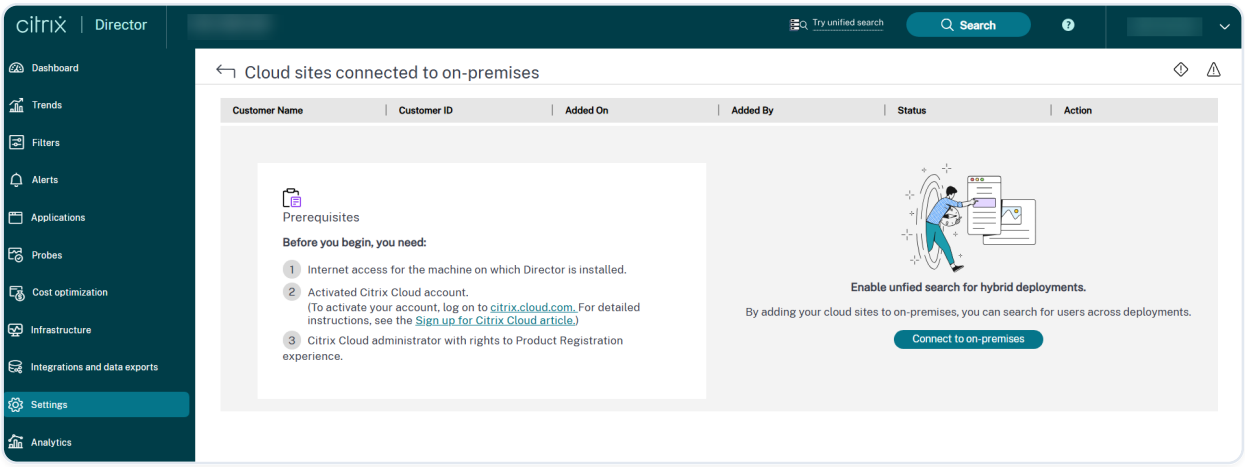
- DaaSのCitrix Cloud™アクティブエンタイトルメントが必要です。
- Citrix Cloudアカウントは、製品登録エクスペリエンスに対する権限を持つ管理者アカウントである必要があります。管理者権限の詳細については、「管理者権限の変更」を参照してください。
- Citrix Directorがインストールされているマシンにインターネットアクセスがあることを確認してください。
- Citrix Cloudサービスを使用するには、HTTPSポート443を介して必要なCitrixアドレスに接続できる必要があります。詳細については、「インターネット接続要件」を参照してください。
- 製品登録を実行するための完全な管理者アクセス権があることを確認してください。

構成手順

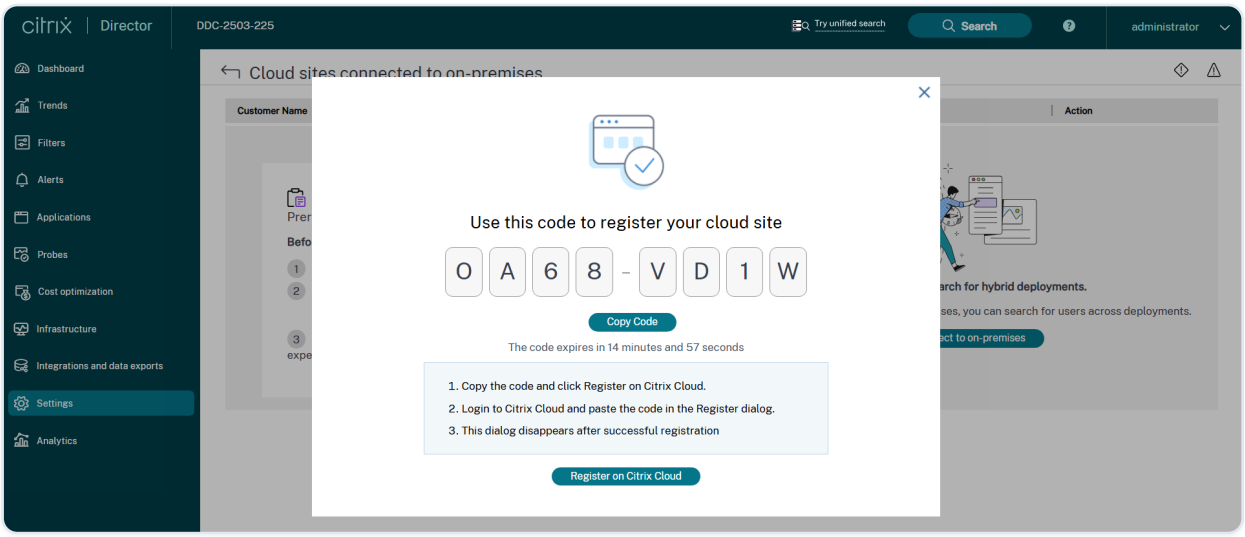
1. フル管理者としてDirectorにサインインします。Directorダッシュボードページが表示されます。
2. **設定**タブをクリックします。**設定**ページが表示されます。



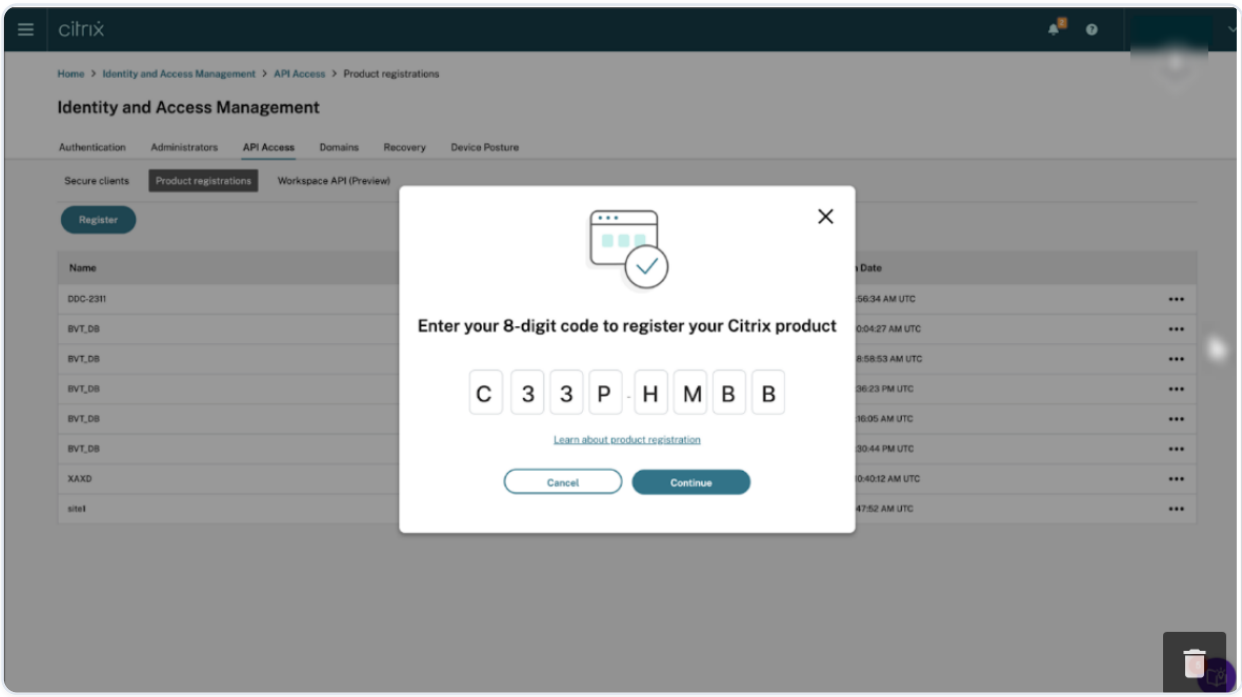
3. **クラウドサイトの追加**をクリックします。次のページが表示されます。



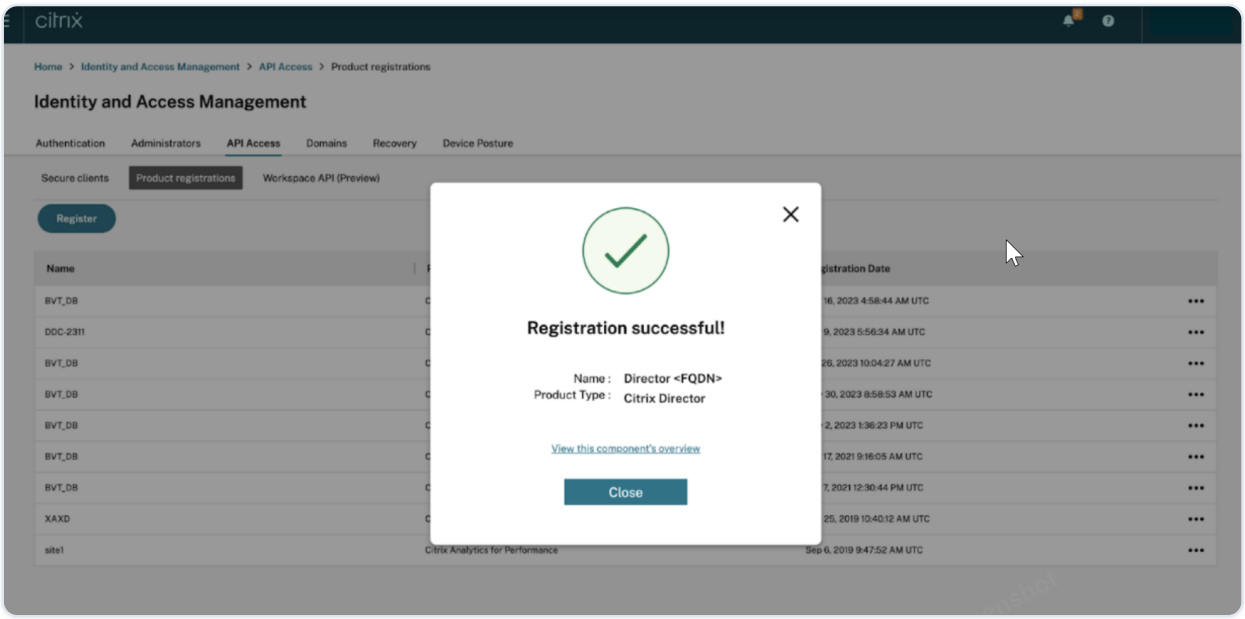
4. 前提条件を確認し、**Connect cloud sites** をクリックして構成プロセスを開始します。このサイトをCitrix Cloudに登録するために使用する、一意の8桁の登録コードが生成されます。



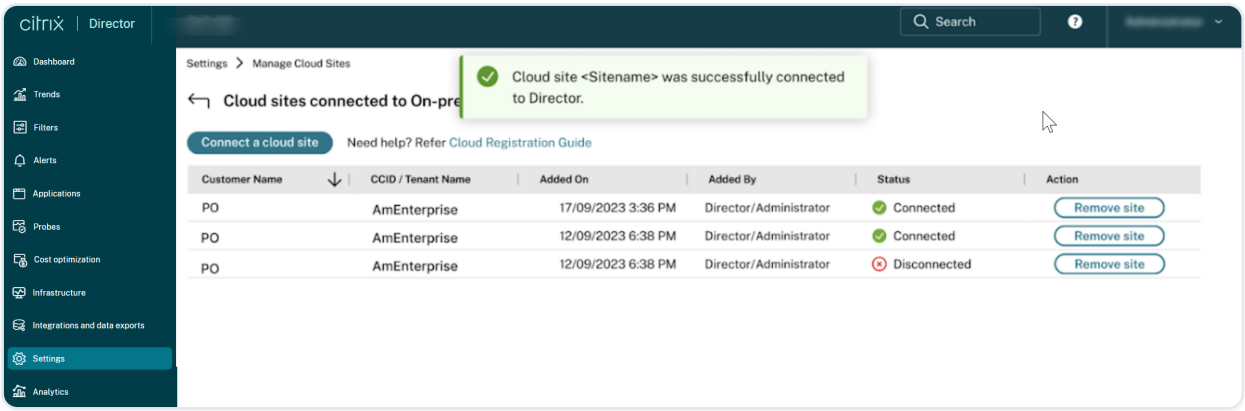
5. **Copy Code** をクリックしてコードをコピーし、**Register on Citrix Cloud** をクリックします。Citrix Cloudの登録URLにリダイレクトされます。
6. Citrix Cloudの資格情報でサインインし、顧客を選択します。
7. コピーした登録コードをCitrix Cloudの **Product Registrations** ページに貼り付けます。**Continue** をクリックしてサイトを登録します。



8. **Continue** をクリックします。クラウドサイトがCitrix Directorに登録され、次のメッセージが表示されます。



9. **Close** をクリックします。次の画面が表示されます。



10. Directorで複数のクラウドサイトを構成するには、Directorから各サイトに対して前述の構成手順を繰り返します。

    サイトごとに複数のDirectorインスタンスが実行されている場合は、いずれか1つのDirectorインスタンスから構成します。サイトに接続されている他のすべてのDirectorインスタンスは、構成プロセス後の次回の更新時に更新されます。

> **注:**
>
> サイトをCitrix Directorから切断するには、**Remove site** をクリックします。このオプションは既存の構成を削除します。

ハイブリッド展開からのユーザー検索

ユーザーを検索するには、次の手順を実行します。

1. 上部のナビゲーションバーで「**検索**」をクリックします。「**展開の監視とトラブルシューティング**」ページが表示されます。

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

2. ドロップダウンリストから「**ユーザー**」を選択し、ユーザー名を入力します。オンプレミスおよびクラウド展開からのアクティブなセッションと失敗したセッションのリストが表示されます。

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

3. 検査するセッションを選択します。

- クラウド展開を使用しているセッションの場合、ユーザーコンテキストを含む関連するDaaS Monitor URLが「**アクティビティマネージャー**」ページに開き、すばやくトラブルシューティングを開始できます。
- オンプレミス展開を使用しているセッションの場合、アクティビティマネージャーページがすぐに開き、トラブルシューティングを開始できます。

インフラストラクチャ監視

Director は現在、Citrix Virtual Apps and Desktops™ コンポーネントの運用状況を可視化します。この機能は、インフラストラクチャに関連する問題を簡単に特定、トラブルシューティング、解決するのに役立ちます。現在、以下のコンポーネントの健全性が監視されています。

- デリバリーコントローラー™
- シトリックス プロビジョニング™ サービス
- StoreFront™

この機能をサポートするために、Citrix コンポーネント向けに `citrixinframonitor.msi` という新しい Windows 実行可能ファイルが導入されました。これにより、Provisioning Service または StoreFront サーバーから Director への関連する健全性メトリックの収集と送信が容易になります。ただし、Delivery Controller の監視には `CitrixInfraMonitor.msi` は必要ありません。Delivery Controller コンポーネントは、Citrix Virtual Apps and Desktops サイトに接続されると、監視のために自動的にオンボーディングされます。

この機能により、Director の単一ダッシュボードで、Delivery Controller、Provisioning Service、および StoreFront サーバーに関する重要な監視データセットとプロアクティブなアラートを取得できます。最新の情報を確保するため、監視対象コンポーネントから5分ごとにデータが収集されます。

この機能は、プロアクティブな監視、詳細なメトリック、および自動化されたアラートを提供することで運用効率の向上を目指し、Citrix® インフラストラクチャがスムーズかつ効率的に稼働することを保証します。

主な機能

リアルタイム監視:

- Delivery Controller、Citrix Provisioning (Provisioning Service) サーバー、StoreFront などの Citrix インフラストラクチャコンポーネントの継続的な監視。

- システムの健全性、リソース使用率、および関連するパフォーマンスメトリックを表示するダッシュボードビュー。

詳細な分析:

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

自動アラートと通知:

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

ユースケース

運用効率:

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

チケット解決の高速化:

サーバーの健全性とパフォーマンスに関する主要なメトリックを監視し、仮想アプリケーションとデスクトップのユーザーへの最適な配信を評価します。これらのメトリックを使用して、関連するコンポーネントを分析することで、パフォーマンスに関連するユーザーの苦情を診断し、解決します。

前提条件

- Citrix Virtual Apps and Desktops™ バージョン 2407 以降
- Provisioning Serviceの前提条件またはStoreFrontの前提条件が満たされていることを確認してください。
- Citrix Provisioningを監視する場合:
  - **DB Connectivity** および **License Server Reachability** を監視するために必要な最小バージョンは Citrix Provisioning 2407 です。
  - **PXE Service**、**TFTP Service**、および **Total Reconnect Count** を監視するために必要な最小バージョンは Citrix Infra Monitor 2411 です。

- Citrix Infrastructure Monitorを実行するために必要なユーザーアカウントまたは権限:
  - エンドポイントマシンにCitrix Infrastructure Monitorをインストールするための Windows管理者権限を持つユーザーアカウント。
  - フル管理者ユーザーアカウント、または以下の Director 権限を持つカスタムロール:
    - アラートポリシーの作成\編集\有効化\削除
    - アラートメールサーバー構成の作成\編集\削除
    - Citrix コンポーネントへの接続の作成\編集\管理 (インフラ監視)
    - アラートの無視
    - アラートポリシーの表示
    - アラートの表示
    - ダッシュボードページの表示
    - インフラストラクチャモニターページの表示

注:

- 前述の前提条件は、Provisioning ServiceおよびStoreFrontコンポーネントの監視にのみ有効です。
- **アラート**ページにアクセスする権限がない場合、**インフラストラクチャ監視**ページで**アラートの管理**オプションが無効になります。

詳細については、以下を参照してください。

- インフラストラクチャ監視の概要
- 接続の管理
- インフラストラクチャダッシュボード
- 高度なアラートポリシー
- インフラストラクチャポリシー

インフラストラクチャ監視の概要

Citrix Infrastructure Monitorには、次の方法で接続できます。

- 手動接続 - Citrix Infrastructure Monitorサービスを手動でダウンロードしてインストールします。
- 自動接続 - UIがダウンロードとインストールを自動的に処理します。

手動接続と自動接続の両方を行った後、Citrix Infrastructure MonitorのHTTPSをオプションで構成できます。

詳細については、以下を参照してください。

- 手動接続
- 自動接続
- Citrix Infrastructure MonitorのHTTPSを構成する

Citrix Infrastructure Monitor の手動接続

> **注:**
>
> 以下の2つの手順は、Provisioning ServiceおよびStoreFront™コンポーネントの監視にのみ有効です。

ステップ1：Citrix Infrastructure Monitorのインストール

安全なデータ収集のための接続を確立するため、ターゲットコンポーネントへのインストールを完了するには、以下の手順を実行します。

> **注:**
>
> Citrix Infrastructure Monitor をインストールするマシンには、Provisioning Service または StoreFront のいずれかがすでにインストールされている必要があります。

ステップ1.1：ターゲットコンポーネントの特定

監視が必要なProvisioning ServiceやStoreFrontサーバーなどのターゲットコンポーネントを特定します。

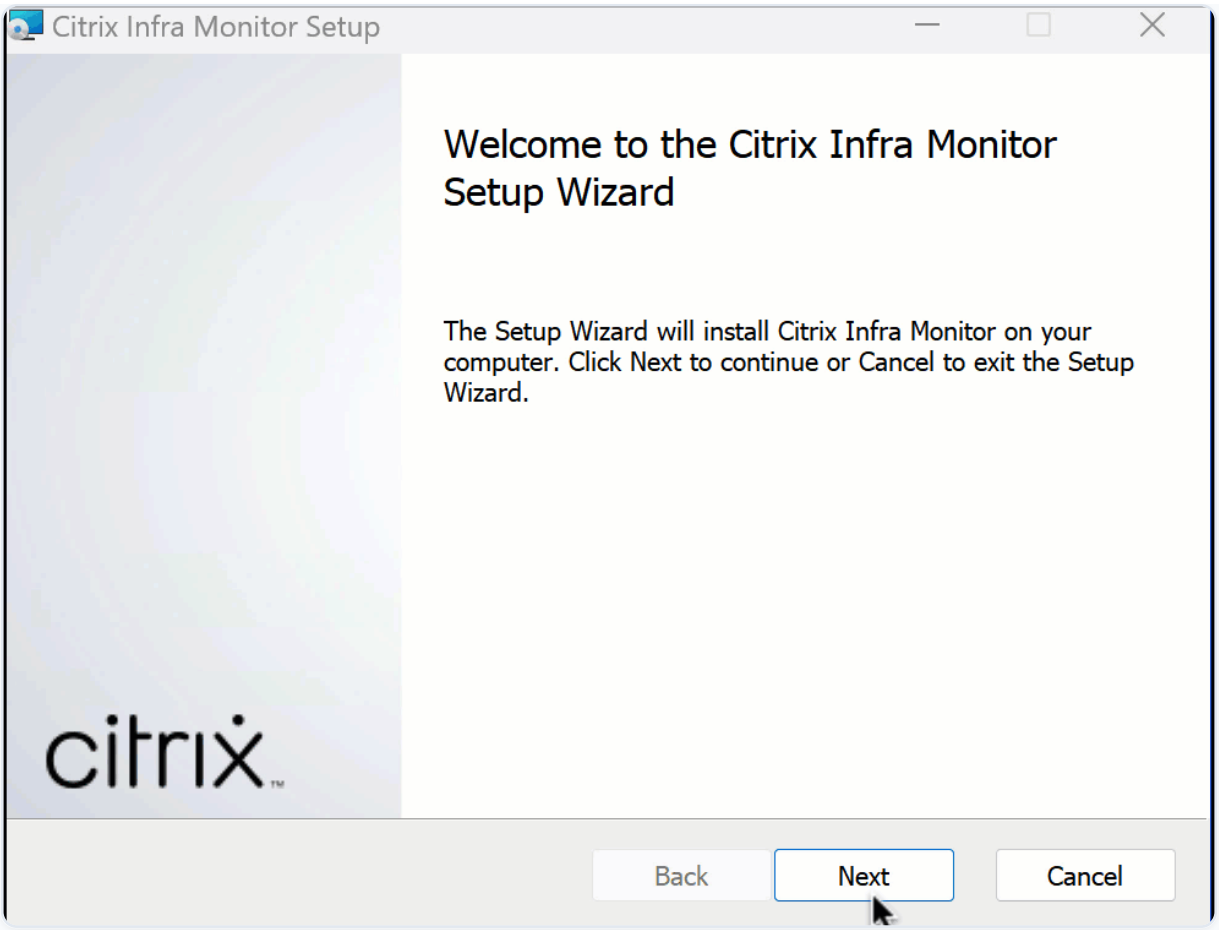
ステップ1.2：Citrix Infrastructure Monitorのダウンロード

ステップ1.1で特定されたターゲットサーバーのCitrixダウンロードページから `CitrixInfraMonitor.msi` をダウンロードできます。

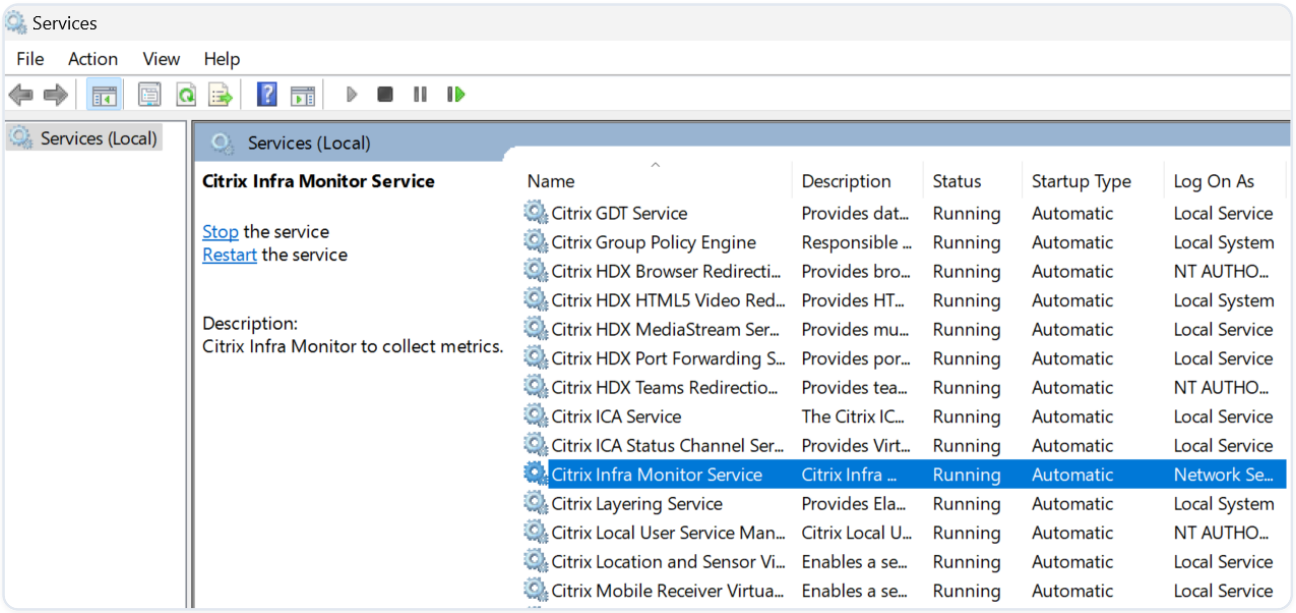
ステップ 1.3: Citrix Infrastructure Monitor を実行する

インストールウィザードの指示に従って、ターゲットコンポーネントで `CitrixInfraMonitor.msi` インストーラーを実行します。

> **注:**
>
> 管理者権限を持つユーザーは、ターゲットコンポーネントにCitrix Infrastructure Monitorをインストールおよび構成できます。



インストールが正常に完了すると、「**サービス**」セクションでCitrix Infrastructure Monitorサービスを表示できます。



ステップ 1.4: 登録トークンを取得する

シトリックス インフラストラクチャ モニターがインストールされているシステムで、`C:\ProgramData\Citrix\InfraMonitor\RegistrationToken.txt` にある `RegistrationToken.txt` ファイルに記載されているトークンを取得し、ステップ 2: シトリックス インフラストラクチャ モニターを登録するで使用できるように準備してください。

ポート要件

`CitrixInfraMonitor.msi` を正常にインストールすると、インストーラーは9595ポートの例外を作成します。サードパーティのファイアウォールを使用している場合は、Citrix Infrastructure Monitoringサービスを使用するために、このポートのTCP通信を手動で許可する必要がある場合があります。

次の表は、Provisioning ServiceおよびStoreFrontマシンに対するインバウンドポート要件の詳細を示しています。

送信元	ターゲット	タイプ	ポート	プロトコル	目的
DDC	Provisioning Serviceまたは StoreFront マシン	TCP	9595	HTTPまたは HTTPS	Provisioning Serviceまたは StoreFront マシンからメトリックを収集するための呼び出し。

注:

Provisioning ServiceおよびStoreFrontマシンは、Infrastructure Monitoringサービスに対してアウトバウンド呼び出しを行いません。

ステップ2：Citrix Infrastructure Monitorを登録する

Citrix Infrastructure Monitorは、以下の方法で登録できます。

- ディレクターユーザーインターフェース
- PowerShell SDK

Director UI から

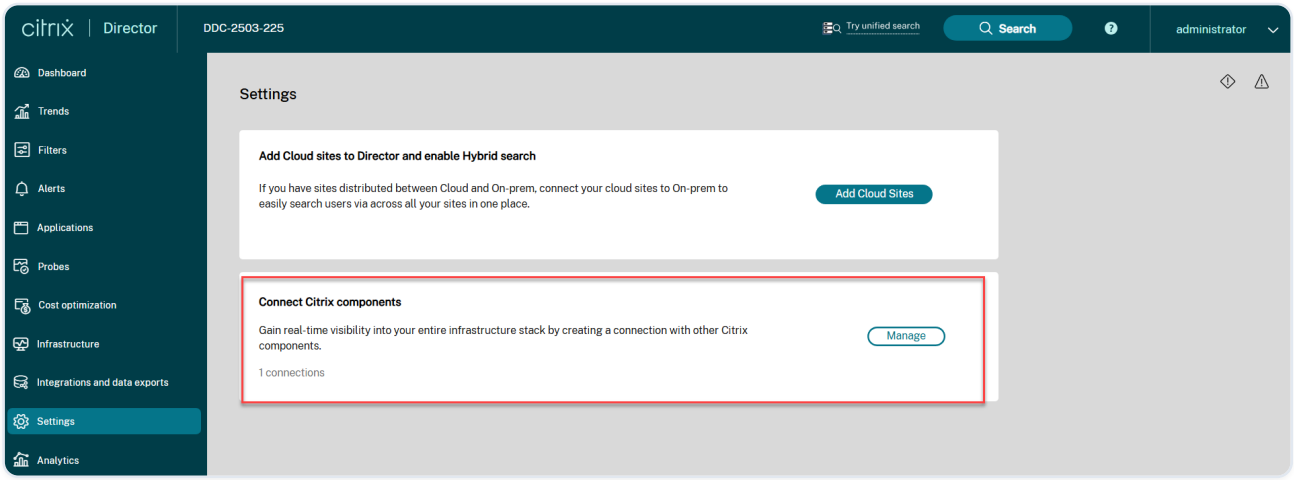
次の手順で Director UI で登録を完了します。

ステップ 2.1: CITRIX コンポーネントの接続ページに移動する

［設定］ > ［Citrix コンポーネントの接続］ > ［管理］ の順にクリックします。

または、,

インフラストラクチャ > **管理**をクリックします。



](/en-us/citrix-virtual-apps-desktops/current-release/media/connect-citrix-components.png)

ステップ2.2：コンポーネントの詳細を入力する

［Citrix コンポーネントの接続］ 画面で、 ［接続の作成］ をクリックします。 ［接続の作成］ ウィンドウが表示されます。

](/en-us/citrix-virtual-apps-desktops/current-release/media/create-a-connectiOn.png)

`CitrixInfraMonitor.msi`がターゲットにダウンロードされ、インストールされていることを確認してください。詳細については、このドキュメントのステップ1を参照してください。画面の指示に従い、安全な接続を確立するために必要なコンポーネントの詳細を入力してください。

- ドロップダウンリストからコンポーネントの種類を選択します。コンポーネントは Provisioning Service または StoreFront のいずれかです。
- ホスト名を入力します。
- ドメイン名を入力します。
- Provisioning Service または StoreFront マシンのユーザー名を入力します。
- Provisioning Service または StoreFront マシンのパスワードを入力します。

ステップ2.3：接続を承認する

Citrix Infrastructure Monitorがインストールされているシステムで、`C:\ProgramData\Citrix\InfraMonitor\RegistrationToken.txt`にある`RegistrationToken.txt`ファイルからCitrix Infrastructure Monitorトークンを取得します。

取得したトークンの詳細を Director UI に入力します。このトークンは、サイトとコンポーネント間の接続を認証します。

`RegistrationToken.txt`ファイルに存在するトークンテキストは、Citrix Infrastructure Monitor サービスを再起動すると再生成されます。登録が成功すると、トークンファイルはマシンから削除されます。何らかの理由で新しいトークンファイルを再作成する必要がある場合は、Citrix Infrastructure Monitorサービスを再起動してください。セキュリティ上の理由から、無効なトークンによる登録試行が3回失敗すると、トークンファイルは削除されます。

ステップ 2.4: 接続を作成する

詳細が入力されたら、**作成**をクリックします。作成された接続は、**Citrix コンポーネントの接続**ページの接続リストに表示されます。

Citrix コンポーネントの接続](/en-us/citrix-virtual-apps-desktops/current-release/media/connect-citrix-components.png)

リモート PowerShell SDK の使用

前提条件：

- Citrix Infrastructure Monitor が StoreFront または PVS マシンにインストールされていることを確認します。

PVS または StoreFront マシンと通信するために、Citrix Infrastructure Monitor を DDC に登録します。この登録は、PVS または StoreFront マシンで収集されたインフラストラクチャの正常性メトリックを DDC に送信するためのものです。

Citrix Infrastructure Monitor に登録するには、Delivery Controller™ で次の PowerShell コマンドを実行します。

```
Add-MonitorDirectorAgent -Fqdn <FQDN of component> -Component <component>
-Domain <domain> -Username <username> -Password <password> -Token <token>
```

注:

ユーザー名とパスワードはオプションのパラメーターです。ただし、これらのパラメーターを指定しない場合、一部のメトリックは利用できません。

上記のコマンドのパラメーターは次のとおりです。

パラメーター	説明
`Fqdn`	PVS または StoreFront サーバーの FQDN。
`Component`	オンボーディングするコンポーネント。例: PVS または SF。PVS は Citrix Provisioning™ を表し、SF は StoreFront を表します。
`Domain`	すべてのコンポーネントが属するドメイン。
`Username`	管理者ユーザーのユーザー名。
`Password`	管理者ユーザーのパスワード。
`Token`	Citrix Infrastructure Monitorがインストールされているシステムで、`C:\ProgramData\Citrix\InfraMonitor\RegistrationToken.txt` にある `RegistrationToken.txt` ファイルからCitrix Infrastructure Monitorトークンを取得します。

注:

- Citrix Infrastructure Monitorサービスを再起動すると、`RegistrationToken.txt`ファイルに存在するトークンテキストが再生成されます。登録が成功すると、トークンファイルはマシンから削除されます。再登録する必要がある場合は、Citrix Infrastructure Monitorサービスを再起動してください。
- セキュリティ上の理由から、無効なトークンによる登録試行が3回失敗すると、トークンファイルは削除されます。

PVS または StoreFront マシンの登録が正常に完了すると、マシン名の詳細が **Director** > **インフラストラクチャ**タブに表示されます。

Citrix Infrastructure Monitorに登録するためのコマンド例は次のとおりです。

```
Add-MonitorDirectorAgent -Component PVS -Fqdn NX-PVS-
-Domain  -Username  -Password  -Token
```

Citrix Infrastructure Monitor の自動接続

新しい自動接続機能は、以下の手順を自動的に実行することで、オンボーディングプロセスを簡素化します。

- Citrix Infrastructure Monitor のダウンロードとインストール
- 接続の検証

自動接続では、コンポーネントの詳細を手動で追加するだけで済みます。手動接続プロセスは変更されておらず、ユーザーはエージェントをダウンロードし、ターゲットマシンにインストールして、必要な詳細情報を提供する必要があります。

この変更に対応するため、UI には以下の2つのタブが追加されました。

- 自動接続
- 手動接続

自動接続プロセスには、資格情報を入力する前にすべての前提条件が満たされていることを確認するためのチェックボックスが含まれています。

自動接続の目的は、ユーザーにとってオンボーディングプロセスを可能な限りシームレスにすることです。

前提条件

Director UI からマシンに Citrix Infrastructure Monitor サービスをリモートでインストールできます。Director UI からのリモートインストールには、Provisioning Service および StoreFront™ マシンに対して以下が必要です。

- Citrix Infrastructure Monitor がインストールされるターゲットマシンで、ローカル管理者権限を持っている必要があります。
- ターゲットマシンで WMI が利用可能である必要があります。ファイアウォールで WMI が許可されていることを確認してください。詳細については、「リモート WMI 接続のセットアップ」を参照してください。
- ターゲットマシンで RPC が利用可能である必要があります。管理共有 (Admin$ および C$) は、Delivery Controller™ マシンからアクセスできる必要があります。
- ターゲットマシンは、解決可能な DNS ホスト名を持っている必要があります。

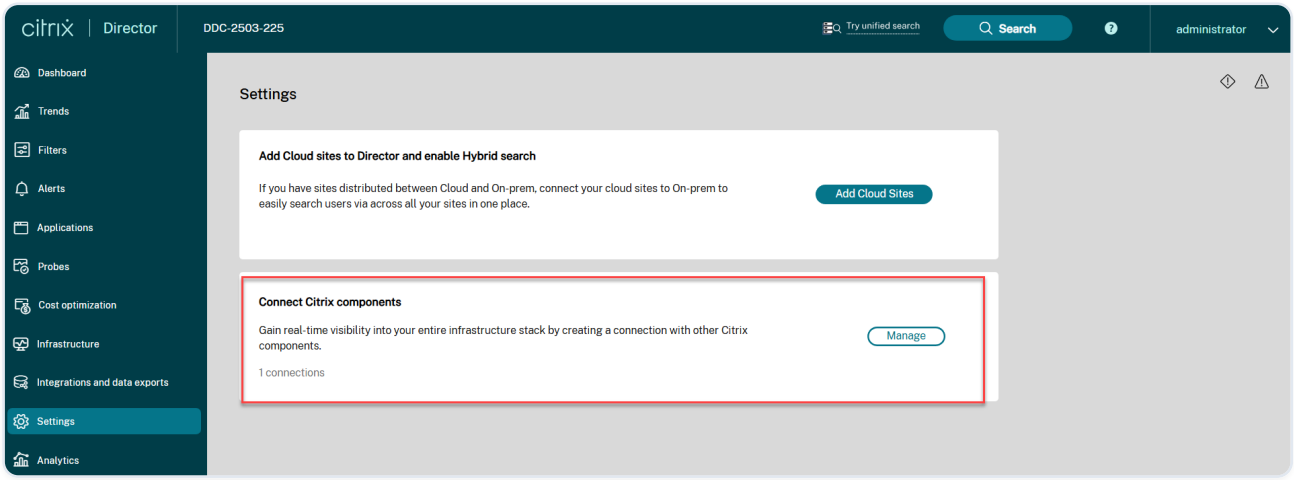
これらの要件が環境で満たせない場合は、「Citrix Infrastructure Monitor の手動オンボーディング」を参照してください。

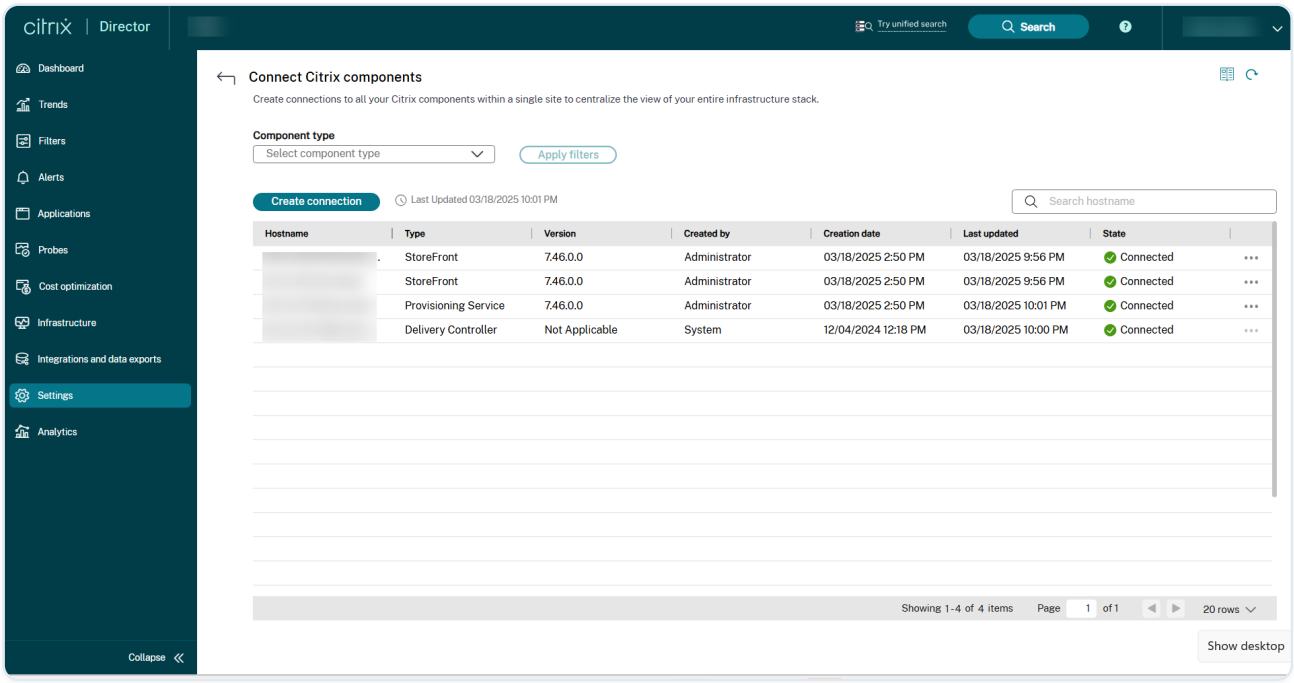
Citrix Infrastructure Monitor を自動的に登録する

Director UI を使用して Citrix Infrastructure Monitor を登録できます。次の手順で Director UI で登録を完了します。

ステップ 1：Citrix コンポーネントの接続ページに移動する

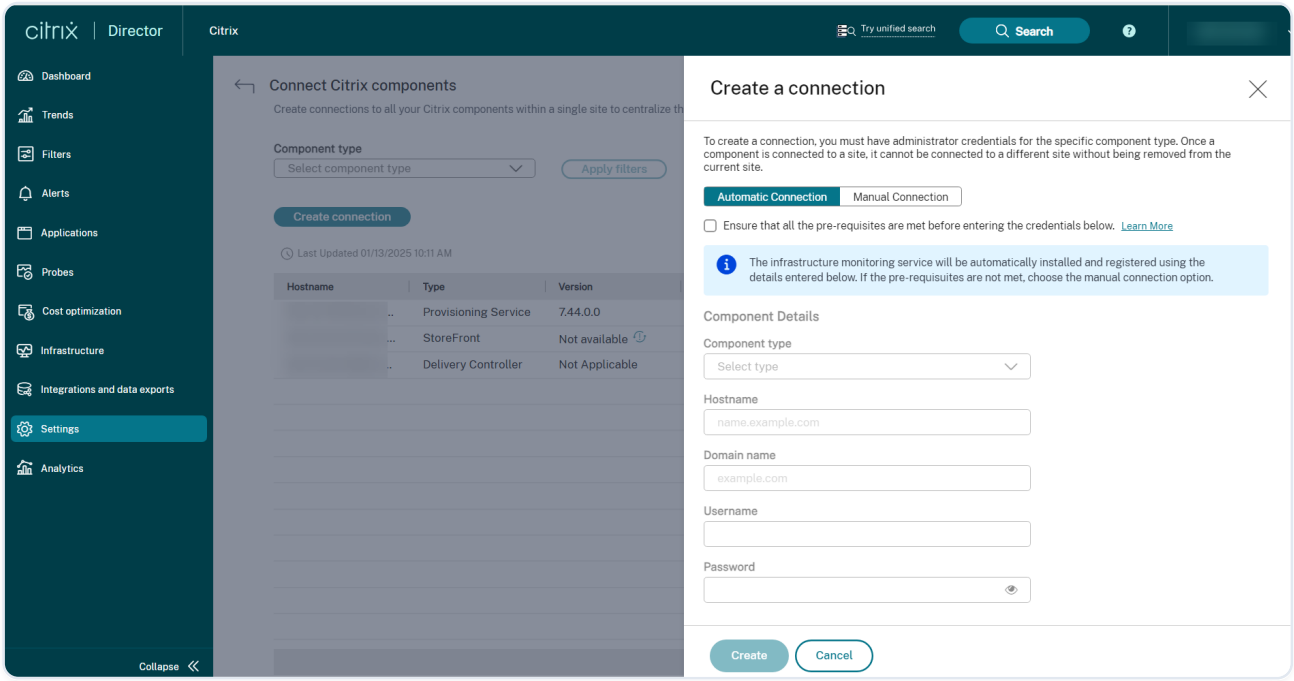
［設定］ > ［Citrix コンポーネントの接続］ > ［管理］ の順にクリックします。





ステップ 2：コンポーネントの詳細を入力する

［Citrix コンポーネントの接続］画面で、**［接続の作成］** をクリックします。**［接続の作成］** ウィンドウが表示されます。デフォルトでは、**［自動接続］** タブが強調表示されています。



セキュリティで保護された接続を確立するために必要なコンポーネントの詳細を入力します。

- ドロップダウンリストからコンポーネントの種類を選択します。コンポーネントは Provisioning Service または StoreFront です。
- ホスト名を入力します。
- ドメイン名を入力します。

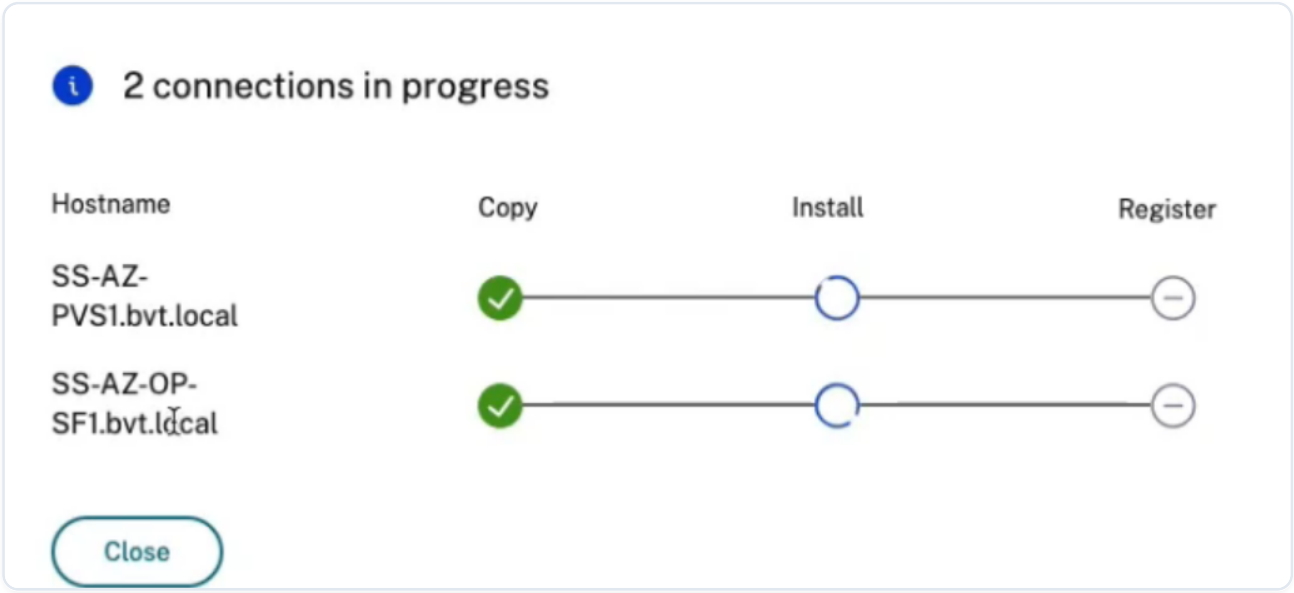
- Provisioning Service または StoreFront マシンのユーザー名を入力します。
- Provisioning Service または StoreFront マシンのパスワードを入力します。

インフラストラクチャ監視サービスは、上記の詳細を使用して自動的にインストールおよび登録されます。

ステップ 3: 接続を作成する

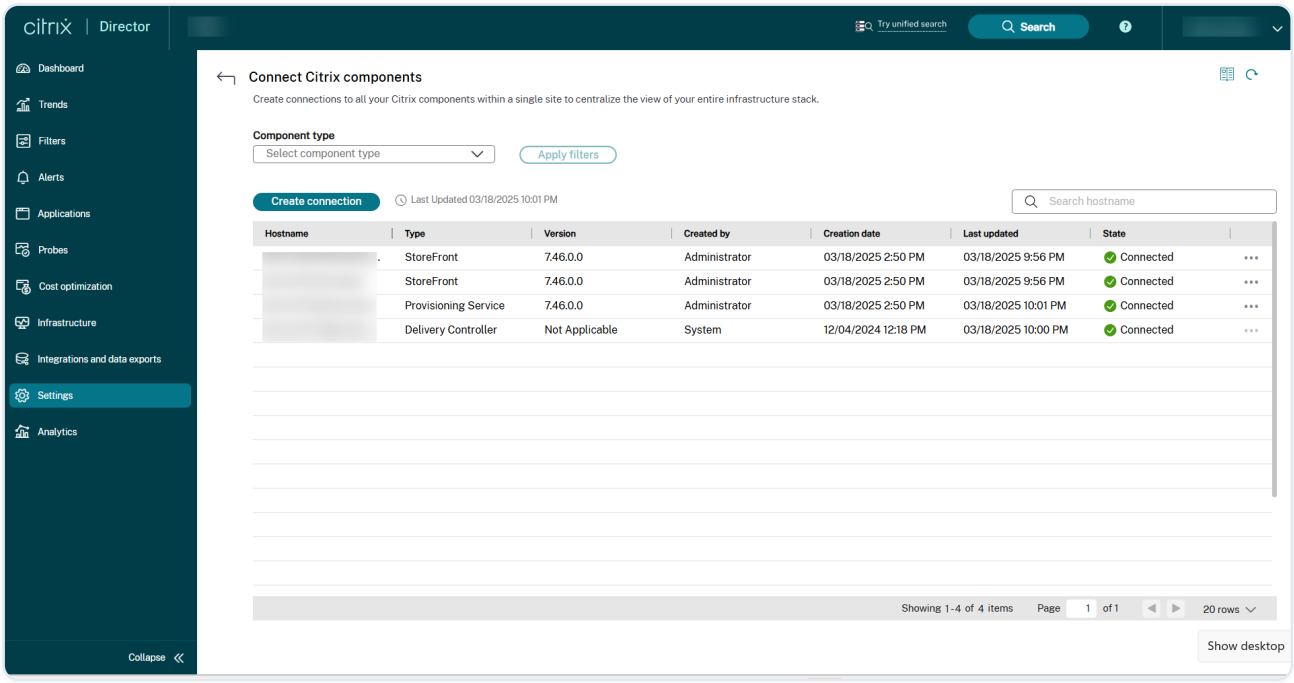
詳細が入力されたら、**作成**をクリックします。リクエストが承認される前に、特定の事前チェックが実行されます。これらのチェックは、続行する前に前提条件が満たされていることを検証します。前提条件が満たされると、自動接続プロセスは、コピー、インストール、登録の各ステップを示す進行状況バーを表示します。いずれかのステップが失敗した場合、ユーザーには再試行オプションが表示されます。

自動接続プロセスの詳細を表示するには、**詳細の表示**をクリックします。



MSI ファイルがダウンロードされ、インストール場所にコピーされた後、インストールおよび登録されます。完了すると、作成された接続は ページの接続リストで利用可能になります。

接続が失敗した場合は、接続を再試行できます。再試行するには、管理者資格情報を提供する必要があります。



エラー処理

システムは前提条件の事前チェックを実行し、いずれかのチェックが失敗した場合はエラーメッセージを表示します。

注:

事前チェックは特定の順序で実行されます。たとえば、WMI エラーをチェックするには、資格情報が正しい必要があります。

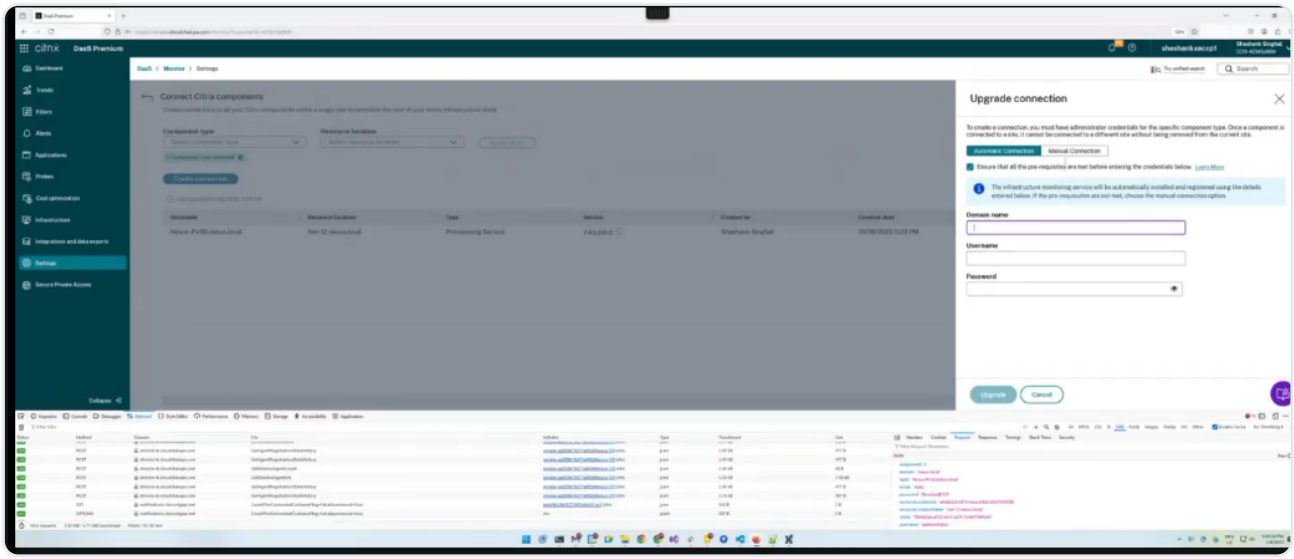
次の表に、エラーメッセージと対応する解決策を示します。

エラーシナリオ	説明
無効な FQDN 形式	FQDN形式が無効です。この問題を解決するには、FQDN形式を修正してください。
到達不能なFQDN	FQDNマシンに到達できません。
無効な資格情報	ユーザー名またはパスワードが無効です。
リモートマシンでHTTPSが設定されていません。	Monitor構成でHTTPSが有効になっているにもかかわらず、リモートマシンでHTTPSを有効にするための環境変数が設定されていません。この問題を解決するには、**System**

エラーシナリオ	説明
	Properties > **Advanced** > **Environment Variables** > **Edit system variable** で値を設定してください。
リモートマシンでHTTPSが誤って設定されています	Monitor構成でHTTPSが無効になっているにもかかわらず、リモートマシンでHTTPSを有効にするための環境変数が設定されています。この問題を解決するには、**System Properties** > **Advanced** > **Environment Variables** > **Edit system variable** で値を削除してください。
リモートマシンでWindows Management Instrumentation (WMI) がブロックされています。	Windowsファイアウォールディフェンダーの**許可されたアプリと機能**セクションにあるWMIのチェックボックスが選択されていません。この問題を解決するには、WMIがファイアウォールを介してアクセスできることを確認してください。
リモートマシンでSMBポートがブロックされています。	Delivery Controllerからの受信TCP接続には、ポート445を有効にする必要があります。
リモートマシンでAdmin Shareが無効になっています	自動接続の前提条件が満たされていません。

アップグレードプロセス

Citrix Infrastructure Monitor の以前のバージョンを使用している場合、アップグレードするオプションがあります。これは、Provisioning Service と StoreFront にのみ適用されます。自動アップグレードでは、進行状況バーが表示され、管理者資格情報が必要です。



自動または手動でアップグレードを選択できます。

アップグレードのプロンプトは、新しいバージョンが利用可能な場合にのみ表示されます。アップグレードに登録は不要です。アップグレード後、最新バージョンが反映されるまでに約5分かかります。

Citrix Infrastructure MonitorのHTTPSを構成する手順

> **注:**
>
> Citrix Infrastructure MonitorサービスはHTTPモードでも動作するため、この場合、以下の設定は不要です。ただし、HTTPSモードでの使用を推奨します。Citrix Infrastructure MonitorでHTTPSを設定する必要がある場合にのみ、以下の手順を実行してください。

ステップ1：証明書をマシンにアップロードする

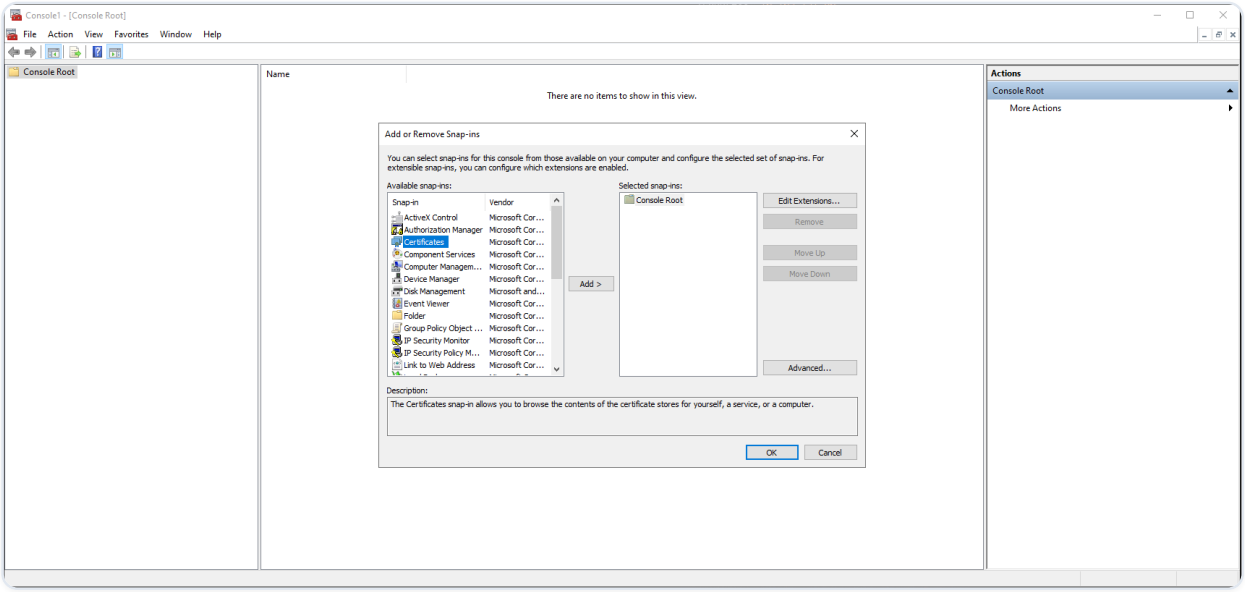
1. Citrix Infrastructure Monitorがインストールされているマシン用に`PFX`証明書を取得します。PFXファイルの生成に関する詳細については、「PFXファイルの作成方法」を参照してください。

   > **注:**
   >
   > パスワードで保護されたPFXファイルも使用できます。

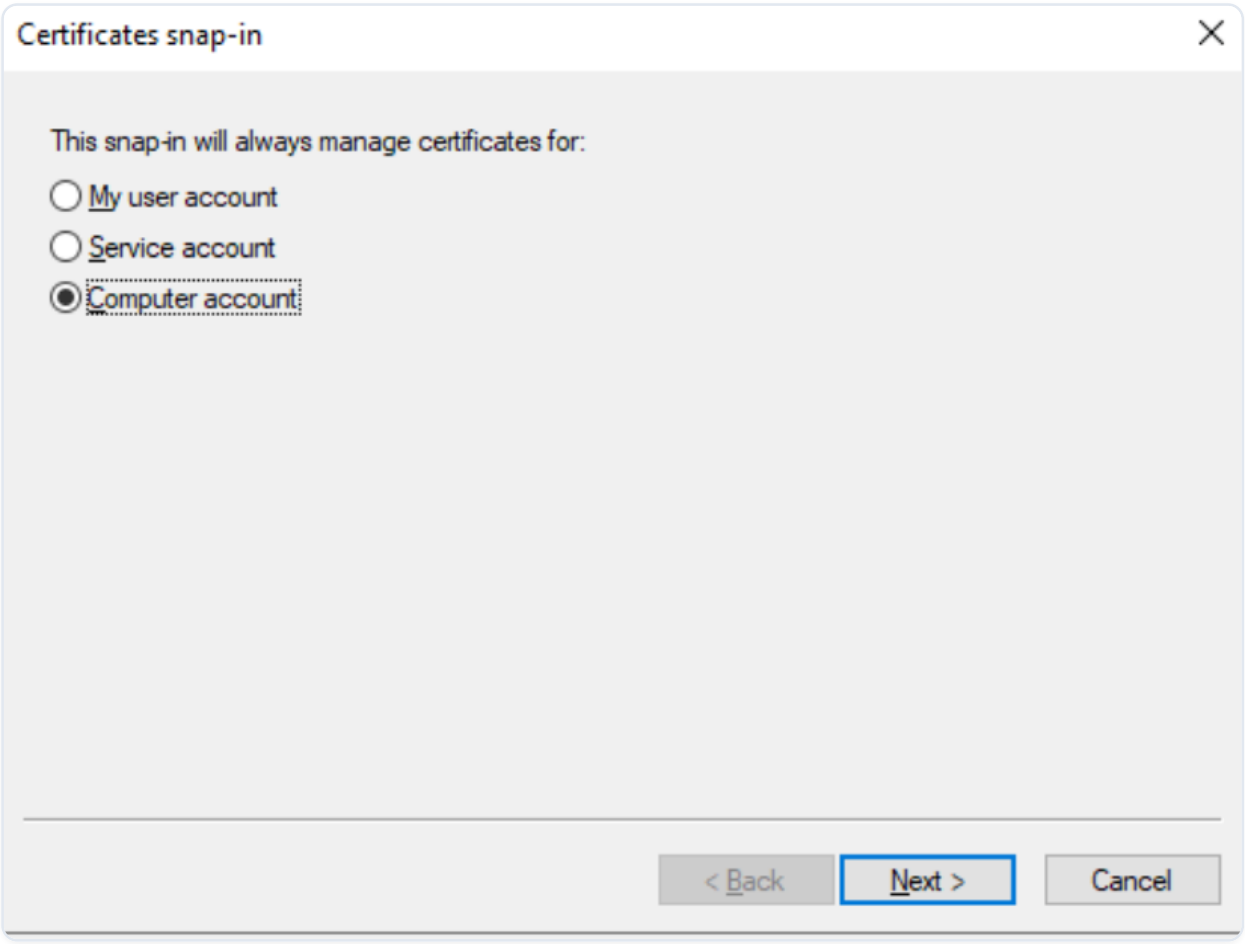
2. 証明書をマシンの任意の場所にアップロードします。

ステップ2：証明書をコンピューター証明書にインポートする

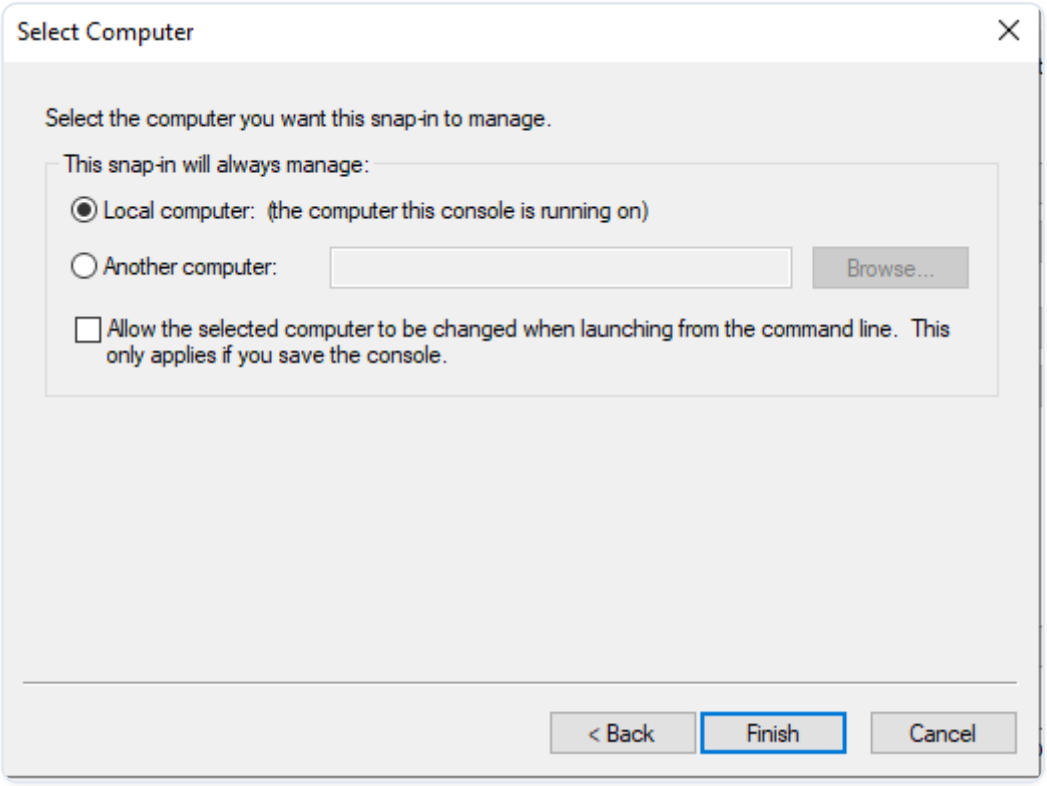
1. **スタート** > **ファイル名を指定して実行**をクリックし、`mmc`と入力して**OK**をクリックします。**コンソール1 - **ウィンドウが表示されます。
2. **ファイル**メニューで、**スナップインの追加と削除**をクリックします。**スナップインの追加と削除**ウィンドウが表示されます。



3. 「**スナップイン**」の下で、「**証明書**」をダブルクリックします。「**証明書スナップイン**」ウィンドウが表示されます。

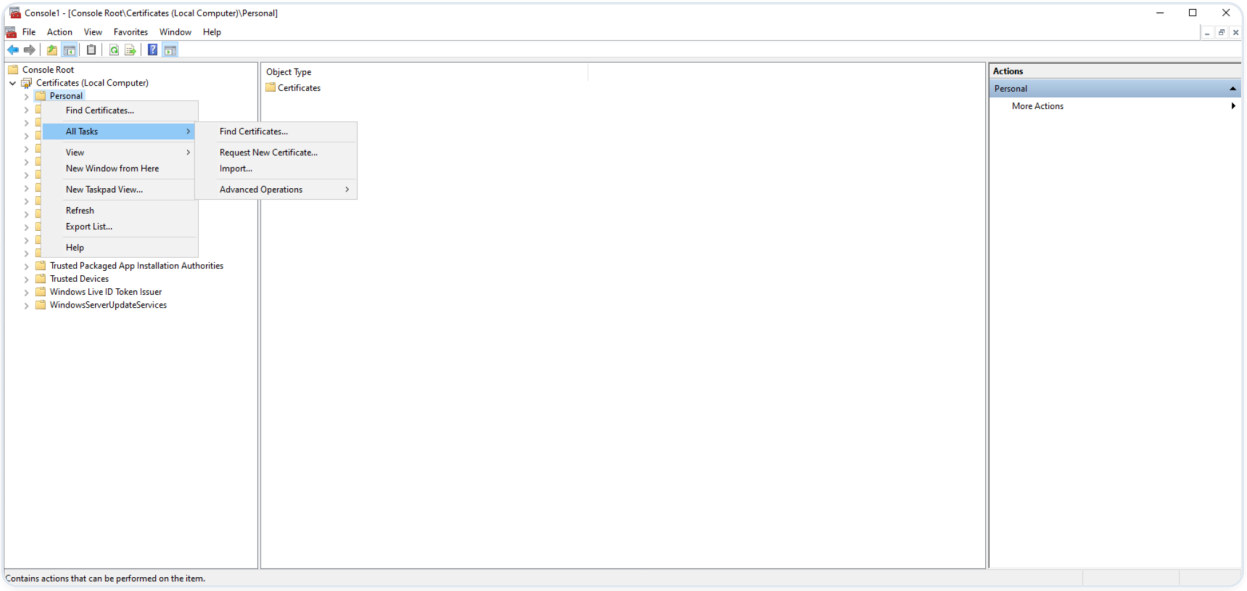


4. 「**コンピューターアカウント**」を選択し、「**次へ**」をクリックします。「**コンピューターの選択**」ウィンドウが表示されます。

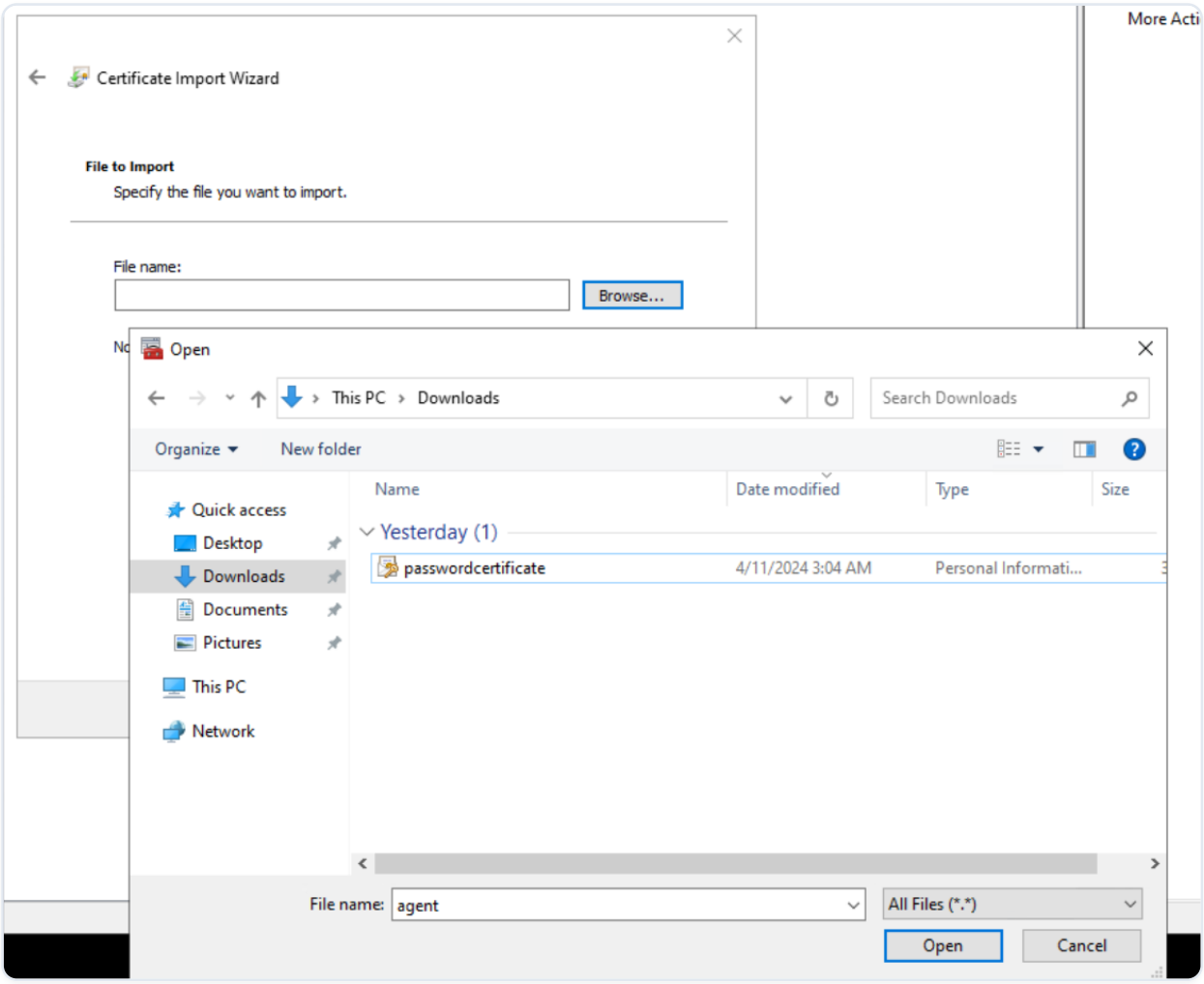


5. 「**ローカルコンピューター**」を選択します。

6. 「**完了**」をクリックします。新しいコンソールの選択されたスナップインのリストに、「**証明書 (ローカルコンピューター)**」セクションが表示されます。
7. **OK**をクリックします。
8. 「**証明書**」を展開し、「**個人**」を右クリックして「**すべてのタスク**」>「**インポート**」を選択します。「**証明書のインポートウィザードへようこそ**」が表示されます。



9. 「**次へ**」>「**ファイルの参照**」を選択します。PFXファイルをアップロードした場所に移動し、ファイルの種類を「**すべてのファイル**」に変更して、該当するPFX証明書を選択します。



10. PFXパスワードを入力します。パスワードがない場合は空白のままにできます。
11. **Next**をクリックします。
12. 証明書ストアについては、「**証明書をすべて次のストアに配置する**」オプションが選択されており、「**証明書ストア**」が「**個人**」として選択されていることを確認します。

    証明書ストア(/en-us/citrix-virtual-apps-desktops/current-release/media/sm-certificate-store.png)
13. **Next**をクリックします。
14. 詳細を確認し、**完了**をクリックします。
15. 確認を待ちます。「*インポートは正常に完了しました*」というメッセージが表示されます。
16. **証明書** > **個人**に移動し、証明書が存在することを確認します。
17. マシンからPFX証明書ファイルを削除します。

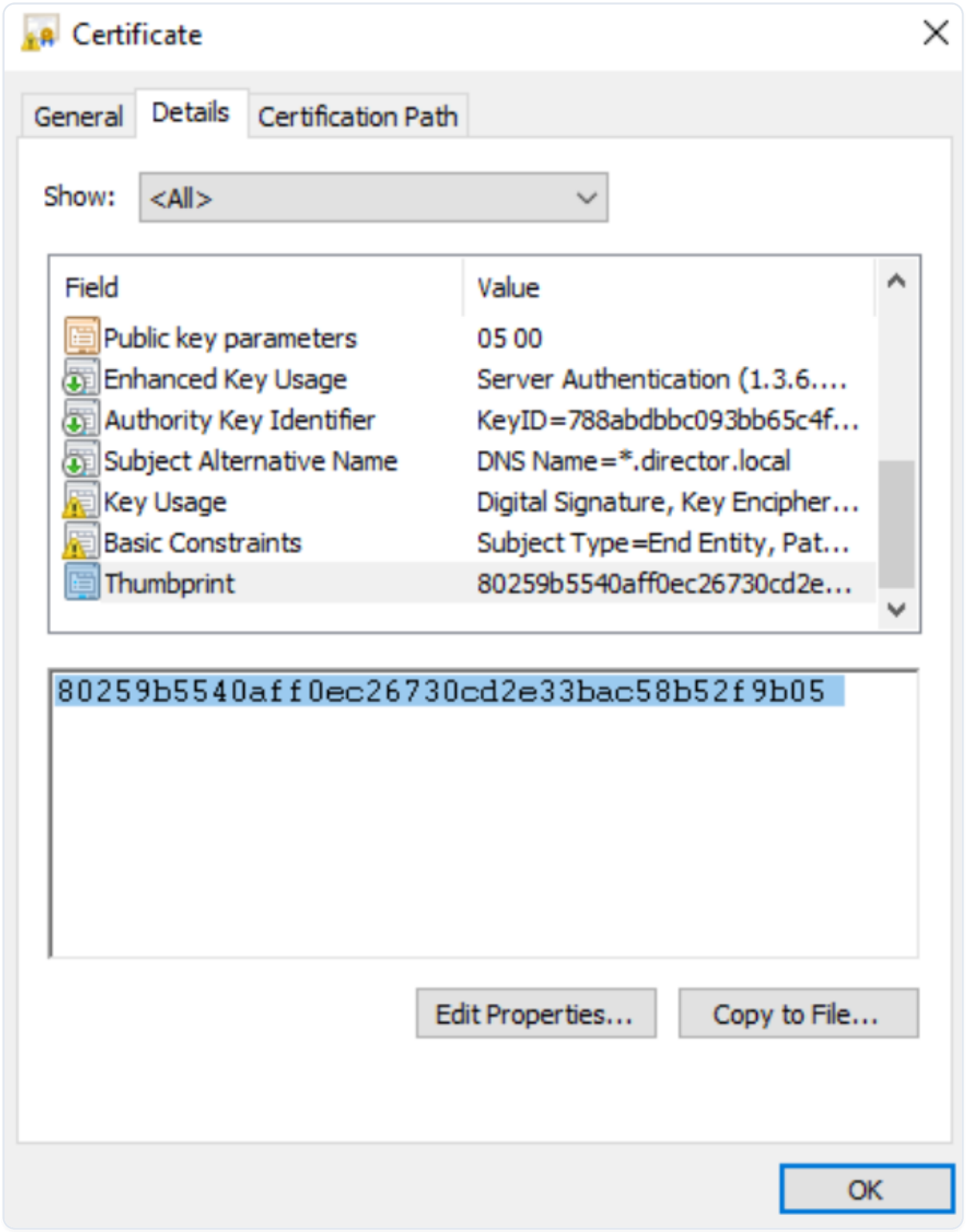
ステップ3：証明書に読み取りアクセス権を付与する

1. インポートした証明書を右クリックし、**すべてのタスク** > **秘密キーの管理**を選択します。

2. 開いたダイアログで、**追加**を選択し、**Network Service**を検索します。 **OK**をクリックします。
3. **グループ**または**ユーザー名**の下にある**NETWORK SERVICE**を選択します。
4. **NETWORK SERVICEのアクセス許可**の下で*読み取り*アクセスを許可します。
5. **OK**をクリックします。

ステップ4：サムプリントを取得する

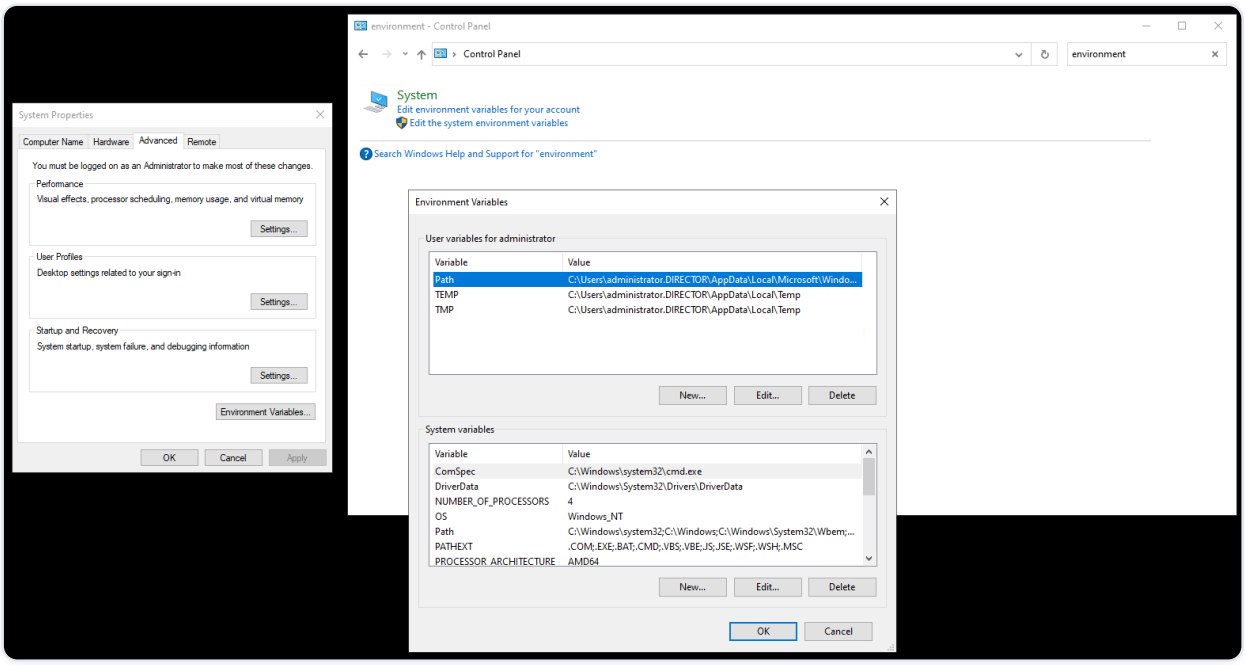
1. インポートした証明書をダブルクリックします。
2. 開いたダイアログで、**詳細**タブに移動し、一番下までスクロールします。
3. **Thumbprint**をクリックします。



4. 値をコピーし、次のステップのために準備しておきます。

ステップ5：環境変数の設定

1. コントロールパネルを開きます。
2. 「環境」を検索し、**システム環境変数の編集**を選択します。
3. **システム変数（すべてのユーザー）の下にある新規**をクリックします。



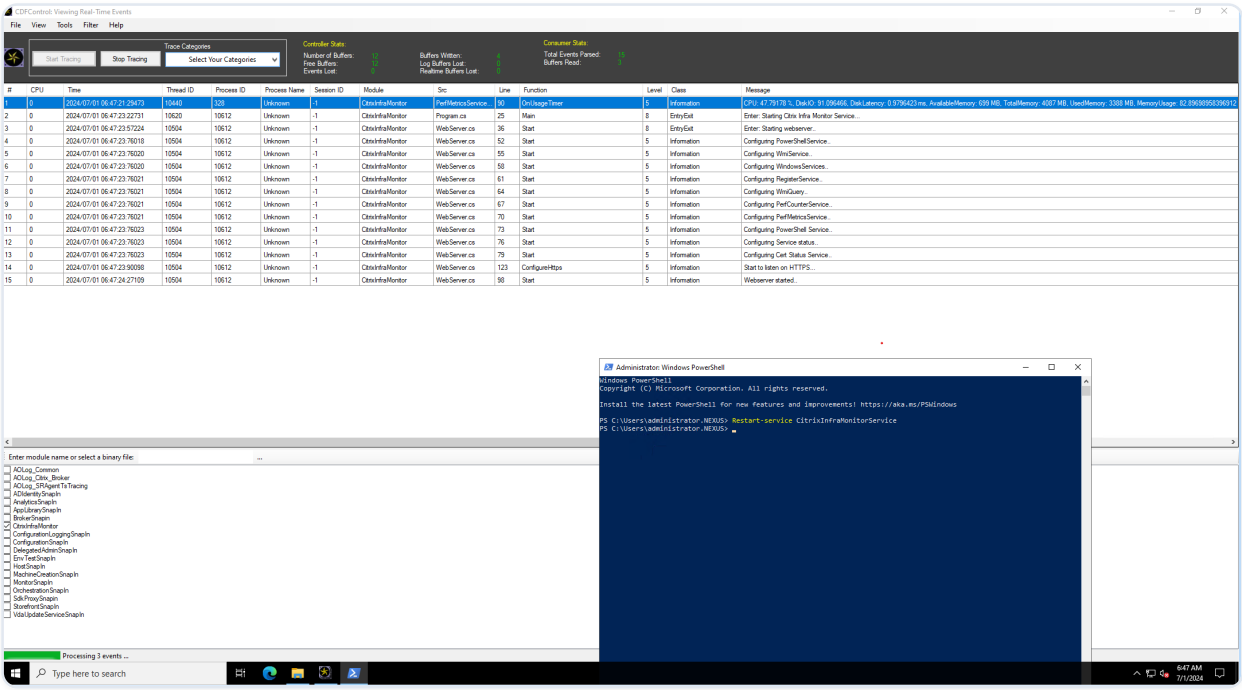
4. **変数**名として*DIRECTOR_AGENT_HTTPS_CERTIFICATE_THUMBPRINT*を指定します。
5. **変数値**に、前のステップで取得したサムプリントを指定します。
6. **OK**をクリックします。

ステップ6：CitrixInfraMonitorServiceの再起動

1. PowerShellを開き、次のコマンドを実行します。

```
Restart-Service CitrixInfraMonitorService
```

2. **CitrixInfraMonitorService**モジュールをキャプチャし、ログ行**Start to listen on HTTPS...**を探して、HTTPSが有効になっていることを確認します。



ステップ 7: モニター構成で HTTPS を有効にする

Delivery Controller™マシンで次のコマンドを実行します。

```
Set-MonitorConfiguration -DirectorAgentEnableHttps $true
```

接続の管理

「**Citrixコンポーネントの接続**」ページで、接続の表示、削除、または編集ができます。

接続の表示

このビューで使用可能な、接続済みおよび切断済みのすべてのコンポーネントの詳細を表示できます。次の表は、「**接続の作成**」ページのさまざまな列について説明しています。

列	説明
ホスト名	サーバーの名前。
種類	接続の種類。Delivery Controller™、Provisioning Service、およびStoreFrontがあります。
バージョン	コンポーネントにインストールされている `CitrixInfraMonitor.msi` のバージョン。このフィールドはDelivery Controllerには適用されません。

列	説明
作成者	接続を作成したユーザーの名前。
作成日	接続が確立された日付。
最終更新日	接続が最後に更新された日付。
状態	状態には、接続中、接続済み、切断済みがあります。
	接続中: この状態は、新しいコンポーネントのデータが表示されるまでに約5分、リソース使用率のデータが利用可能になるまでに約10分かかることを示します。
	接続済み: この状態は、コンポーネントとサイト間の接続が稼働中であることを示します。
	切断済み: この状態は、コンポーネントとサイト間の接続が切断されていることを示します。切断状態の考えられる理由としては、サーバーのダウンタイムや、サイトがCitrix Infrastructure Monitorに接続できないことなどが挙げられます。

> **注:**
>
> オンプレミスのCitrix Virtual Apps and Desktops™サイトに接続されている場合、Delivery Controllerの接続はこのビューに自動的に入力されます。

接続の編集

Provisioning ServiceまたはStoreFront™接続を確立するために使用される管理者資格情報を更新するには、接続の編集が必要になる場合があります。

既存の接続を編集するには、次の手順を実行します。

1. **設定**タブまたは**インフラストラクチャ**タブから「**Citrixコンポーネントの接続**」ページに移動します。
2. 接続リストテーブルで、目的のコンポーネントの行の末尾にある3つの点をクリックします。

3. **編集**をクリックし、必要に応じて詳細を更新します。

コンポーネントを削除する

Director UIまたはPowerShellコマンドを使用して、コンポーネントを削除できます。

Director UIの使用

コンポーネントの削除とは、DirectorからProvisioning ServiceまたはStoreFront接続を登録解除するプロセスです。登録解除プロセスが完了すると、選択したコンポーネントの新しいデータ収集は停止します。既存の接続を削除するには：

1. **設定**タブまたは**インフラストラクチャ**タブから「**Citrixコンポーネントの接続**」ページに移動します。
2. 接続リストテーブルで、目的のコンポーネントの行の末尾にある3つの点をクリックします。
3. 「**削除**」をクリックします。接続は登録解除され、Director から削除されます。

PowerShell SDK の使用

特定のコンポーネントの登録を解除する必要がある場合は、Delivery Controller で次の PowerShell コマンドを実行します。

```
Remove-MonitorDirectorAgent -Fqdn <FQDN of component> -Component
<component>
```

Citrix Infrastructure Monitorの登録を解除するコマンドの例は次のとおりです。

```
Remove-MonitorDirectorAgent -Component PVS -Fqdn [redacted]
```

注:

コンポーネントの登録解除は、特定のコンポーネントからDirectorへのデータフローを停止するだけです。Citrix Infrastructure Monitor をアンインストールする必要がある場合は、「**コントロールパネル**」からアンインストールしてください。

インフラストラクチャダッシュボード

「**インフラストラクチャ監視**」ページで、コンポーネントの健全性値を確認できます。これらの結果は、インフラストラクチャに関する問題を事前に分析し、トラブルシューティングするのに役立ちます。

「**インフラストラクチャ監視**」ページは、以下でフィルタリングできます。

- ホスト名 - ホスト名を選択します
- 到達可能性 - **稼働中**（サーバーに到達可能）または**停止中**（サーバーに到達不能）チェックボックスを選択します
- エラー - 「エラーのある行のみ表示」チェックボックスを選択します。

「**列の管理**」オプションを使用して、ダッシュボードに表示するデータを選択します。

Provisioning Serviceの健全性メトリック

「**インフラストラクチャ**」タブをクリックし、「**Provisioning Service**」を選択します。Provisioning Serviceのインフラストラクチャダッシュボードが表示されます。

Provisioning Serviceダッシュボード(/en-us/citrix-virtual-apps-desktops/current-release/media/sm-pvs-dashboard.png)

Provisioning Serviceサーバーについては、以下の詳細が監視されます。

カテゴリ	メトリック	説明
到達可能性	ホスト名	Citrix Infrastructure Monitorがインストールされている Provisioning Serviceマシンの名前です。このメトリックは文字列値です。
	Provisioning Serviceサイト名	Provisioning Serviceサイトの名前です。このメトリックは文字列値です。
	Provisioning Serviceファーム名	Provisioning Serviceファームの名前です。このメトリックは文字列値です。
	プロビジョニングサービス サイトID	Provisioning Serviceサーバーのサイトidを表示します。このメトリックは文字列値です。
	プロビジョニングサービス ファームID	Provisioning Serviceサーバーのファームidを表示します。

カテゴリ	メトリック	説明
		このメトリックは文字列値です。
	サーバーの状態	指定されたサーバーの到達可能性の状態を表示します。可能な値は、*Up*、*Down*、*Unknown* です。
	最終起動時刻	Provisioning Serviceサーバーが最後に起動された時刻を表示します。
	最終更新日時	Provisioning Serviceサーバーからデータが収集された時刻を表示します。
依存サービス	ストリーミングサービス	ストリーミングサービスのステータスを表示します。このメトリックは、Windowsサービスのステータスを示します。可能な値は、*Not running*、*Running*、*Not Installed*、および *n/a* (ヘルプアイコン付き) です。
	SOAPサービス	Simple Object Access Protocol (SOAP) サービスのステータスを表示します。このメトリックは、Windowsサービスのステータスを示します。可能な値は、*Not running*、*Running*、*Not Installed*、および *n/a* (ヘルプアイコン付き) です。
	DB接続	データベース接続のステータスを表示します。Citrix Provisioningサーバーバージョン2402以前を使用している場合、不明なエラーが発生する可能性があります。可能な値は、*未接続*、*接続済み*、

カテゴリ	メトリック	説明
		不明、および*該当なし*（ヘルプアイコン付き）です。
	ライセンスサーバー到達可能性	ライセンスサーバーに到達可能かどうかを表示します。Citrix Provisioningサーバーバージョン2402以前を使用している場合、不明なエラーが発生する可能性があります。可能な値は、*未接続*、*接続済み*、*不明*、および*該当なし*（ヘルプアイコン付き）です。
	合計再接続数	セッションが再接続された回数を表示します。
	PXEサービス	プリブート実行環境サービスのステータスを表示します。このメトリックは、Windowsサービスのステータスを示します。可能な値は、*実行中ではない*、*実行中*、*インストールされていません*、および*n/a*（ヘルプアイコン付き）です。
	TFTPサービス	トリビアルファイル転送プロトコルサービスのステータスを表示します。このメトリックは、Windowsサービスのステータスを示します。可能な値は、*実行中ではない*、*実行中*、*インストールされていません*、および*n/a*（ヘルプアイコン付き）です。
リソース使用率	CPU使用率 %	CPU使用率を折れ線グラフでパーセンテージ表示します。表示される値は、過去5分間

カテゴリ	メトリック	説明
		の終わりにおける最新の値です。
	平均CPU使用率 %	過去10分間に集計されたProvisioning Serviceサーバーの平均CPUパーセンテージを表示します。
	ピークCPU %	過去5分間のProvisioning Serviceサーバーのピーク CPUパーセンテージを表示します。
	メモリ使用率 %	スタックチャートを使用して、メモリの使用率をパーセンテージで表示します。表示される値は、過去5分間の終わり時点での最新の値です。
	平均メモリ使用率 %	過去10分間にわたって集計されたProvisioning Serviceサーバーの平均メモリ使用率をパーセンテージで表示します。
	ピークメモリ使用率 %	過去5分間のProvisioning Serviceサーバーのピークメモリ使用率をパーセンテージで表示します。
	ディスクIOPS	折れ線グラフを使用して、ディスクの入出力値を表示します。
	平均ディスクIOPS (%)	過去10分間にわたって集計されたProvisioning Serviceサーバーの平均ディスクIOPSを表示します。
	ピークディスクIOPS %	過去10分間のProvisioning Serviceサーバーのピークディ

カテゴリ	メトリック	説明
		スクIOPSの割合を表示します。
	ディスク遅延 (ミリ秒)	折れ線グラフを使用してディスクの遅延値を表示します。
	平均ディスク遅延 %	過去10分間にわたって集計されたProvisioning Serviceサーバーの平均ディスク遅延を表示します。
	ピークディスク遅延 %	過去5分間のProvisioning Serviceサーバーのピークディスク遅延の割合を表示します。
影響	拒否されたログインの合計	失敗したログインの合計数を、ログイン試行の合計数で割ったものです。
	アクティブなデバイス数	Provisioning Serviceサーバー内のアクティブなデバイスの総数を表示します。このメトリックは整数値です。

StoreFront™の健全性メトリック

インフラストラクチャタブをクリックし、**StoreFront**を選択します。StoreFrontのインフラストラクチャダッシュボードが表示されます。

Provisioning Serviceダッシュボード(/en-us/citrix-virtual-apps-desktops/current-release/media/sm-storefront-dashboard.png)

StoreFrontサーバーでは、以下の詳細が監視されます。

カテゴリ	メトリック	説明
到達可能性	ホスト名	StoreFrontサーバーの名前を表示します。このメトリックは文字列値です。

カテゴリ	メトリック	説明
	サーバーのステータス	StoreFrontサーバーのステータスを表示します。このメトリックはWindowsサービスのステータスを示します。可能な値は、*実行中ではない*、*実行中*、*インストールされていない*、および*n/a*（ヘルプアイコン付き）です。
	ベースURLステータス	ベースURLの正常性を表示します。HTTPステータスコードが200の場合、ステータスはUPです。それ以外の場合、値はDownです。
	最終起動時間	StoreFrontサーバーが最後に起動された時間を表示します。
	最終更新	StoreFrontサーバーからデータが収集された時間を表示します。
依存サービス	ドメインサービス	ドメインサービスという名前のWindowsサービスの正常性。このメトリックは、Windowsサービスのステータスを示します。可能な値は、*実行していません*、*実行中*、*インストールされていません*、および*該当なし*（ヘルプアイコン付き）です。
	資格情報ウォレットサービス	このサービスは、暗号化されたパスワードを保存するために使用されるWindowsサービスです。可能な値は、*実行していません*、*実行中*、*インストールされていません*、および*該当なし*（ヘルプアイコン付き）です。

カテゴリ	メトリック	説明
	ピア解決サービス	このサービスは、StoreFrontサーバーのピアメッシュを形成するサーバー間グループネットワーク通信を担当するWindowsサービスです。可能な値は、*実行していません*、*実行中*、*インストールされていません*、および*n/a*（ヘルプアイコン付き）です。
	WWWサービス	このメトリックは、StoreFrontサーバーのWebサービスです。このメトリックは、Windowsサービスのステータスを示します。可能な値は、*実行していません*、*実行中*、*インストールされていません*、および*n/a*（ヘルプアイコン付き）です。
リソース使用率	CPU使用率 %	CPUの使用率を折れ線グラフでパーセンテージ表示します。表示される値は、過去5分間の終わり時点での最新の値です。
	平均CPU使用率 %	過去10分間にわたって集計されたStoreFrontサーバーの平均CPU使用率をパーセンテージで表示します。
	ピークCPU %	過去5分間のStoreFrontサーバーのピークCPU使用率をパーセンテージで表示します。この値は、CPUに必要な最大容量を決定するのに役立ちます。
	メモリ使用率 %	スタックチャートを使用して、メモリの使用率をパーセンテージで表示します。表示

カテゴリ	メトリック	説明
		される値は、過去5分間の終わり時点での最新の値です。
	平均メモリ使用率 %	過去10分間にわたって集計されたStoreFrontサーバーの平均メモリ使用率をパーセンテージで表示します。
	ピークメモリ %	過去5分間のStoreFrontサーバーのピークメモリ使用率をパーセンテージで表示します。
	ディスクIOPS	ラインチャートを使用して、ディスクの入出力値を表示します。
	平均ディスクIOPS (%)	フロートを使用して、StoreFrontサーバーの平均ディスクIOPSを表示します。
	ピークディスクIOPS %	過去10分間のStoreFrontサーバーのピークディスクIOPSパーセンテージを表示します。
	ディスク遅延 (ミリ秒)	折れ線グラフを使用してディスクの遅延値を表示します。
	平均ディスク遅延 %	過去10分間のStoreFrontサーバーの平均ディスク遅延を表示します。
	ピークディスク遅延 %	過去5分間のStoreFrontサーバーのピークディスク遅延パーセンテージを表示します。
影響	ICA®証明書の有効性	ICA証明書の有効性を表示します。可能な値は、*期限切れ*、*期限切れ間近*、*有効*、*見つかりません*です。

カテゴリ	メトリック	説明
	ICA証明書チェーンの有効性	StoreFront ICA証明書チェーンが有効かどうかを表示します。可能な値は、*Yes*または*No*です。
	IIS証明書の有効性	IIS証明書の有効性を表示します。可能な値は、*Expired*、*Expiring*、*Valid*、*Not Found*です。
	IIS証明書チェーンの有効性	StoreFront IIS証明書チェーンが有効かどうかを表示します。可能な値は、*Yes*または*No*です。

Delivery Controller™の健全性メトリック

Delivery Controllerコンポーネントは、インフラストラクチャ監視の一部としてデフォルトで追加されます。Citrix Virtual Apps and Desktops™サイトに接続されているDelivery Controllerコンポーネントは、監視のために自動的にオンボーディングされます。

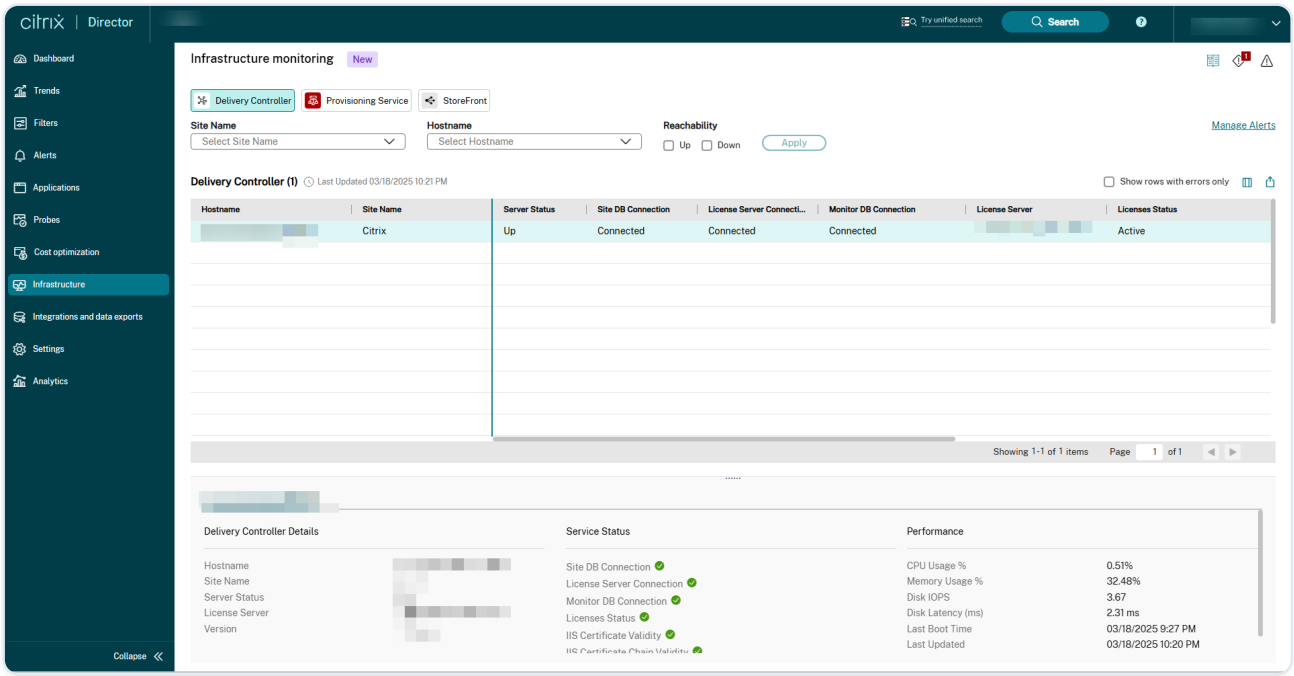
この機能により、お客様はインフラストラクチャ監視ダッシュボードでコントローラーの健全性を監視し、アラートを設定できます。アラート機能により、デリバリーコントローラー用に作成されたポリシーのいずれかがクリティカルまたは警告段階にある場合、顧客管理者にアラートが通知されます。

必要なサイト名を選択すると、選択したサイト名に応じて詳細が表示されます。また、*Up* または *Down* などの**到達可能性ステータス**を選択することもできます。

注： Delivery Controllerの監視には、`CitrixInfraMonitor.msi`ファイルは必要ありません。

インフラストラクチャの詳細について、シングルサイトとマルチサイトの両方の詳細を監視できます。

インフラストラクチャタブをクリックし、**Delivery Controller**を選択します。Delivery Controllerのインフラストラクチャダッシュボードが表示されます。



Delivery Controllerでは、以下の詳細が監視されます。

カテゴリ	メトリック	説明
到達可能性	サーバーの状態	指定されたDelivery Controllerの到達可能性状態を表示します。可能な値は、*Up* と *Down* です。
	バージョン	Delivery Controller のバージョン。
	最終起動時刻	Delivery Controller が最後に起動された時刻を表示します。
	最終更新日時	Delivery Controller からデータが収集された時刻を表示します。
依存サービス	サイトDB接続	サイトデータベース接続のステータスを表示します。可能な値は、*未接続*、*接続済み*、*不明*、および *n/a* (ヘルプアイコン付き) です。**不明:** この値は、メトリックが収集されていないか、利用できない場合に表示されます。**n/a:** 該当な

カテゴリ	メトリック	説明
		し。この値は、サーバーのステータスがダウンしている場合に表示されます。
	ライセンスサーバー接続	ライセンスサーバー接続のステータスを表示します。可能な値は、*未接続*、*接続済み*、*不明*、および *n/a* (ヘルプアイコン付き) です。
	モニターDB接続	モニターデータベース接続のステータスを表示します。可能な値は、*未接続*、*接続済み*、*不明*、および *n/a* (ヘルプアイコン付き) です。
	ライセンスサーバー	ライセンスサーバーに到達可能かどうかを表示します。
	ライセンスステータス	ライセンスのステータスを表示します。
リソース使用率	CPU使用率 %	CPU使用率を折れ線グラフでパーセンテージ表示します。表示される値は、過去5分間の終わりにおける最新の値です。
	平均CPU使用率 %	過去10分間に集計されたDelivery Controllerサーバーの平均CPU使用率を表示します。
	ピークCPU %	過去5分間のDelivery Controllerサーバーのピーク CPU使用率を表示します。
	メモリ使用率 %	スタックチャートを使用して、メモリの使用率をパーセンテージで表示します。表示

カテゴリ	メトリック	説明
		される値は、過去5分間の終わり時点での最新の値です。
	平均メモリ使用率 %	過去10分間の集計における Delivery Controllerサーバーの平均メモリ使用率を表示します。
	ピークメモリ使用率 %	過去5分間のDelivery Controllerサーバーのピークメモリ使用率を表示します。
	ディスクIOPS	折れ線グラフを使用して、ディスクの入出力値を表示します。
	平均ディスクIOPS (%)	過去10分間の集計における Delivery Controllerサーバーの平均ディスクIOPSを表示します。
	ピークディスクIOPS %	過去10分間のDelivery Controllerサーバーのピークディスクの割合を表示します。
	ディスク遅延 (ミリ秒)	折れ線グラフを使用してディスクの遅延値を表示します。
	平均ディスク遅延 %	過去10分間の集計における Delivery Controllerサーバーの平均ディスク待機時間を表示します。
	ピークディスク遅延 %	過去5分間のDelivery Controllerサーバーのピークディスク待機時間の割合を表示します。
影響	IIS証明書の有効性	IIS証明書の有効性を表示します。可能な値は、*Expired*、

カテゴリ	メトリック	説明
		Expiring、*Valid*、*Not Found* です。
	IIS証明書チェーンの有効性	StoreFront IIS証明書チェーンが有効であるかどうかを表示します。指定できる値は *Yes*または*No*です。

アラートの作成と管理

関心のある条件と範囲をプロアクティブに監視し、アラート疲れを軽減するためにアラートを設定できます。アラートは、重大度、再アラート間隔、通知媒体で構成でき、製品でサポートされているアラートライフサイクルに従います。インフラストラクチャに関連するアラートは、**Advanced Alert Policies**セクションから作成できます。

詳細については、Advanced alert policiesページを参照してください。

アプリケーションおよびデスクトップのプロービング

アプリケーションとデスクトップのプロービングは、StoreFront を使用してサイトに公開されているアプリとデスクトップをテスト起動することで、それらの正常性をチェックするプロセスを自動化します。プロービングの結果は Director で確認できます。

要件

- アプリケーションプロービングには Delivery Controller バージョン 7.18 以降、デスクトッププロービングにはバージョン 1906 以降が必要です。
- プローブエージェントを実行するエンドポイントマシンは、アプリケーションプロービングにはCitrix Workspace™ app for Windowsバージョン1808以降、デスクトッププロービングにはバージョン1906以降を搭載したWindowsマシンです。Unified Windows Platform (UWP) 用のWorkspaceアプリはサポートされていません。
- Citrix Probe Agent は、Active Directory 資格情報を使用した StoreFront および Citrix Workspace 経由の認証をサポートしています。エンドポイントデバイスが Citrix Gateway 経由で StoreFront / Workspace に接続されている場合、Citrix Gateway ドメイン資格情報または多要素認証 (MFA) を使用して認証できます。Citrix Probe Agent は、シングルサインオン (SSO) などの他の認証方法をサポートしていません。

> **注:**

- ユーザーがCitrix Cloud™でサインインポリシーまたは条件付き認証を有効にしている場合、プローブエージェントはStoreFrontまたはCitrix Workspaceアプリにサインインできません。
- Probe Agentは、Citrix Workspaceアプリへの認証にActive Directory認証のみをサポートしています。

- Citrix Probe Agentは、プロキシサーバーやCitrix GatewayまたはCitrix ADCのようなロードバランサーが展開されていない場合にのみ機能します。
- プローブエージェントをインストールするエンドポイントマシンに、Microsoft .NET Frameworkバージョン4.7.2以降がインストールされていることを確認してください。

プローブの実行に必要なユーザーアカウントまたは権限:

- 各エンドポイントマシンでプローブする一意の StoreFront ユーザー。StoreFront ユーザーは管理者である必要はありません。プローブは非管理者コンテキストで実行できます。
- エンドポイントマシンにCitrix Probe Agentをインストールおよび構成するためのWindows管理者権限を持つユーザーアカウント。
- ユーザーは、アプリケーションまたはデスクトップの起動に使用されるVDAと同じドメインのメンバーである必要があります。Probe Agentは現在、複数のドメインをサポートしていません。
- 既存のユーザーアカウントをプロービングに再利用すると、ユーザーのアクティブなセッションからログオフする可能性があります。フル管理者ユーザーアカウント、または以下の権限を持つカスタムロールが必要です。
  - デリバリーグループの権限:
    - 読み取り専用
  - Directorの権限:
    - アラートメールサーバー構成の作成\\編集\\削除 - (メールサーバーがまだ構成されていない場合)
    - プローブ構成の作成\\編集\\削除
    - 構成ページの表示
    - トレンドページの表示

構成

複数の地域で、ピーク時間外にプローブを実行するようにスケジュールできます。包括的なプローブ結果は、ユーザーが問題に遭遇する前に、アプリケーション、ホストマシン、または接続に関連する問題をトラブルシューティングするのに役立ちます。

Citrix Probe Agent バージョン 2103 以降は、サイト集約をサポートしています。Citrix Probe Agent を構成するときは、集約されたサイトからのアプリケーションとデスクトップの列挙を有効にするために、Workspace (StoreFront) Site Aggregation Enabled オプションを選択します。以下のサイトの組み合わせがサポートされています。

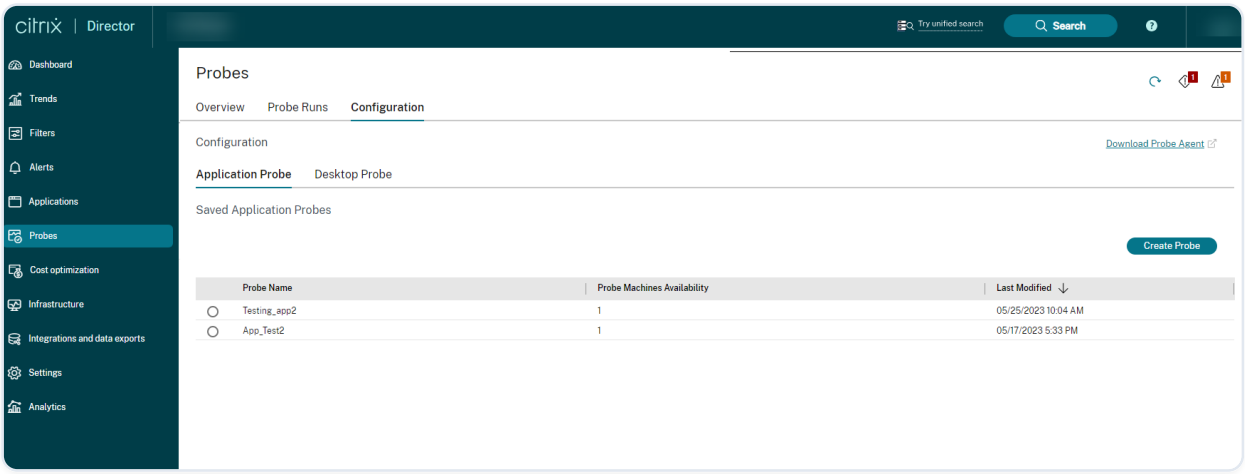
- 1つの StoreFront URL を持つ複数のオンプレミスサイト。
- StoreFront または Workspace URL のいずれかを持つオンプレミスサイトとクラウドサイト。
- 1つの Workspace URL を持つ複数のクラウドサイト。
- Citrix Gateway 経由で StoreFront または Workspace に接続されているオンプレミスサイト。

> **注:**
>
> 1つのサイトにのみアクセスできるプローブを構成するには、個別の管理者またはユーザーを作成する必要があります。

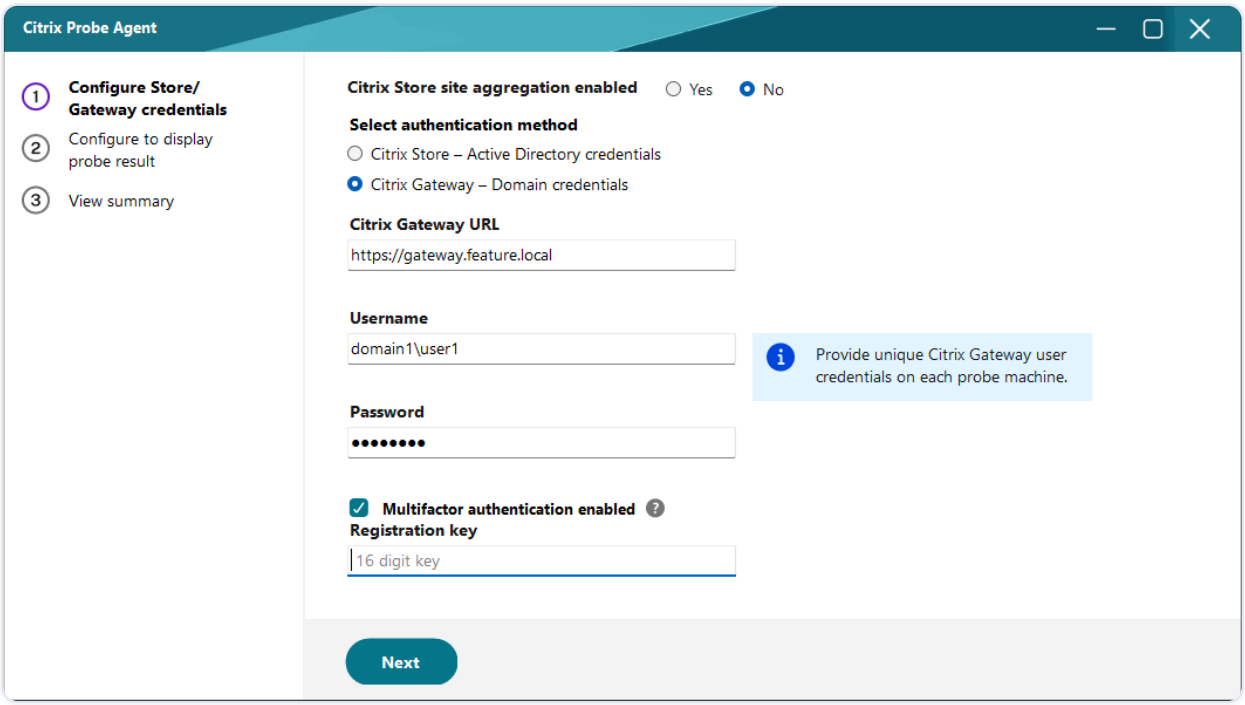
ステップ1：Citrix Probe Agentをインストールして構成する

Citrix Probe Agent は、ユーザーが StoreFront を介して実際のアプリケーションまたはデスクトップを起動するのをシミュレートする Windows 実行可能ファイルです。Director で構成された起動をテストし、その結果を Director に報告します。

1. プロービングを実行するエンドポイントマシンを特定します。
2. 管理者権限を持つユーザーは、エンドポイントマシンにCitrix Probe Agentをインストールおよび構成できます。Citrixダウンロードページで入手可能なCitrix Probe Agent実行可能ファイルをダウンロードしてください。ダウンロードリンクは、Directorの**プローブ**タブでも利用できます。

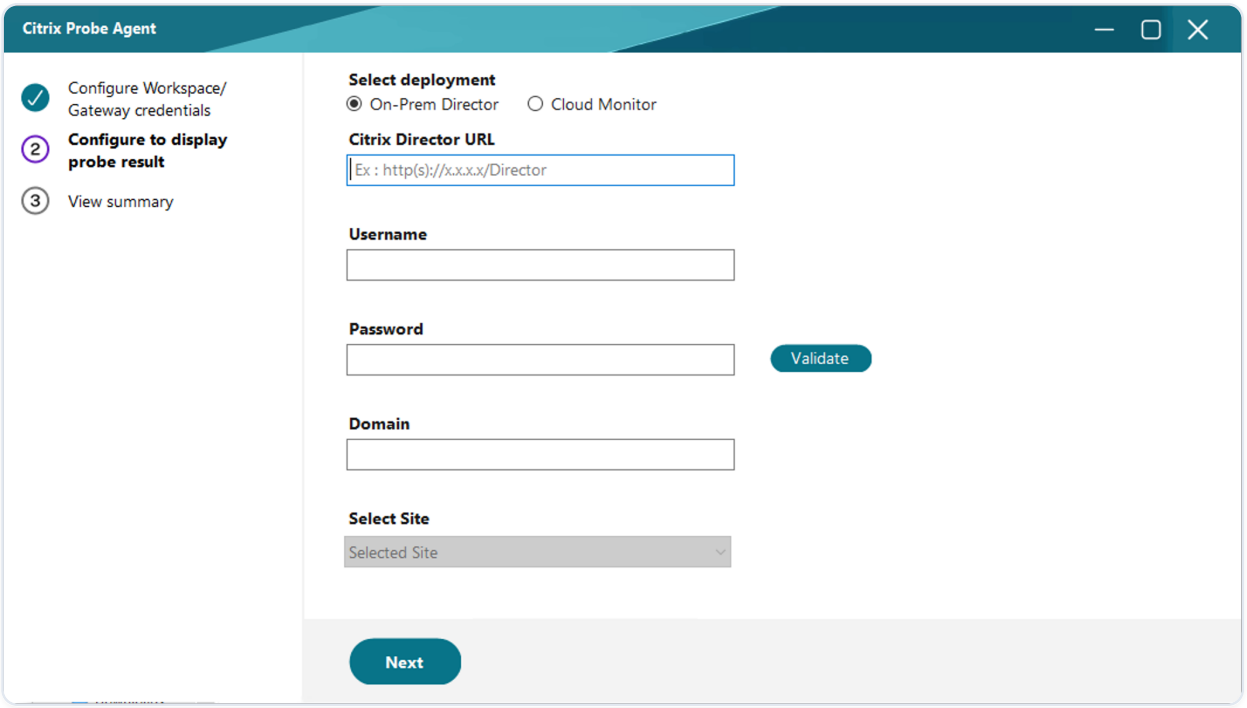


3. 集約されたサイトがある場合は、集約されたサイトからのアプリケーションとデスクトップの列挙を有効にするために、Workspace (StoreFront) Site Aggregation Enabled オプションを選択します。
4. 認証方法を選択し、関連する資格情報を入力します。資格情報は暗号化され、安全に保存されます。
5. StoreFront の Active Directory 資格情報で構成します。各エンドポイントマシンで一意の Workspace (StoreFront) ユーザーを構成します。
6. エンドポイントがCitrix Gatewayを介してStoreFrontに接続されている場合は、Citrix Gatewayオプションを選択し、Citrix Gatewayドメインの資格情報で構成します。



7. Gatewayがサポートしている場合は、多要素認証オプションを選択し、16桁の認証キーを入力します。これは、LDAPとシングルログインスキーマを使用したネイティブOTPで構成されたCitrix Gatewayでのみ利用可能です。

8. タブで、Director の資格情報を入力し、 をクリックします。



9. サイトを選択し、**次へ**をクリックします。
10. 「**概要の表示**」タブで、構成された詳細が正確であることを確認します。変更が必要な場合は、該当するタブに移動して更新します。

> **注:**
>
> Automating Citrix Probe Agent Installation and Configuration に含まれるPowerShellスクリプトを使用して、Citrix Probe Agentのインストールと構成を自動化できます。

ステップ2：Directorでプロービングを構成する

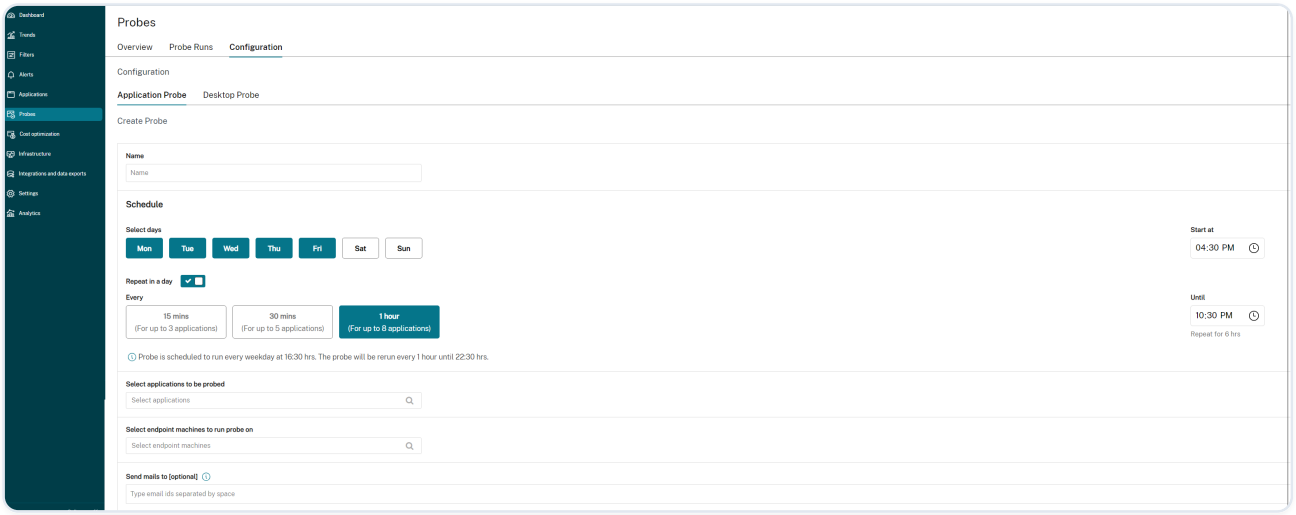
> **制限事項:**
>
> 対話型ログオンメッセージバナーが有効になっているWindows VDAからアプリケーションまたはデスクトップがテスト起動されると、プロービングは失敗します。これは、対話型ログオンメッセージの承認を待機しているためにタイムアウトが発生するためです。 サーバーVDAでログオンメッセージを無効にするには、 > > > > に移動します。
>
> 以下のフィールドのテキストを削除し、Microsoftポリシーを更新します。

- 対話型ログオン: ログオンしようとしているユーザーへのメッセージテキスト
- 対話型ログオン: ログオンしようとしているユーザーへのメッセージタイトル

プローブがアプリケーションまたはデスクトップの起動状態を通過できるように、対話型ログオンメッセージバナーを無効にして、この特定のサーバーVDAにプローブユーザーを割り当てます。

詳細については、`<https://learn.microsoft.com/ja-jp/windows/security/threat-protection/security-policy-settings/interactive-logon-message-text-for-users-attempting-to-log-on>`を参照してください。

1. **プローブ** \> **アプリケーションプローブ**または**デスクトッププローブ**に移動し、**プローブの作成**をクリックします。
2. 「**プローブの作成**」ページで、プローブの名前を入力します。
3. スケジュールを選択します。
   a. プローブを実行する曜日を選択します。
   b. プローブを実行する開始時刻を入力します。
   c. さらに、「**1日あたりの繰り返し**」オプションを選択できます。プローブを1日の中で繰り返す終了時刻と間隔を入力します。たとえば、以下の構成では、毎週月曜日、水曜日、木曜日、日曜日に、12:08から16:34まで30分ごとにアプリケーションプローブが実行されます。
4. 間隔に応じて、プローブするアプリケーションまたはデスクトップの推奨数を選択します。
5. プローブを実行する必要があるエンドポイントマシンを選択します。
6. 失敗したプローブの結果を送信する管理者のメールアドレスを入力します。メールサーバーは、**アラート** > **メールサーバーの構成**で構成します。



この構成では、毎週月曜日、水曜日、木曜日、日曜日に、アプリケーションセッションが12:08、12:38、13:08といった具合に16:08まで起動します。

注:

- 構成後、エージェントは次の時間から構成されたプローブを実行します。
- 「**1日あたりの繰り返し**」オプションが導入される前に設定されたプローブは、スケジュールされた時刻に引き続き実行されます。これらのプローブでは、「**1日あたりの繰り返し**」オプションはデフォルトで無効になっています。
- 重複を防ぐため、各実行に5分の期間があるようにプローブを構成することをお勧めします。

ステップ3：プローブの実行

エージェントは、Directorから定期的に取得するプローブ構成に従ってプロービングを実行します。

StoreFrontを使用して、選択されたアプリケーションを順次起動します。エージェントは、Monitorデータベースを介して結果をDirectorに報告します。障害は5つの特定の段階で報告されます。

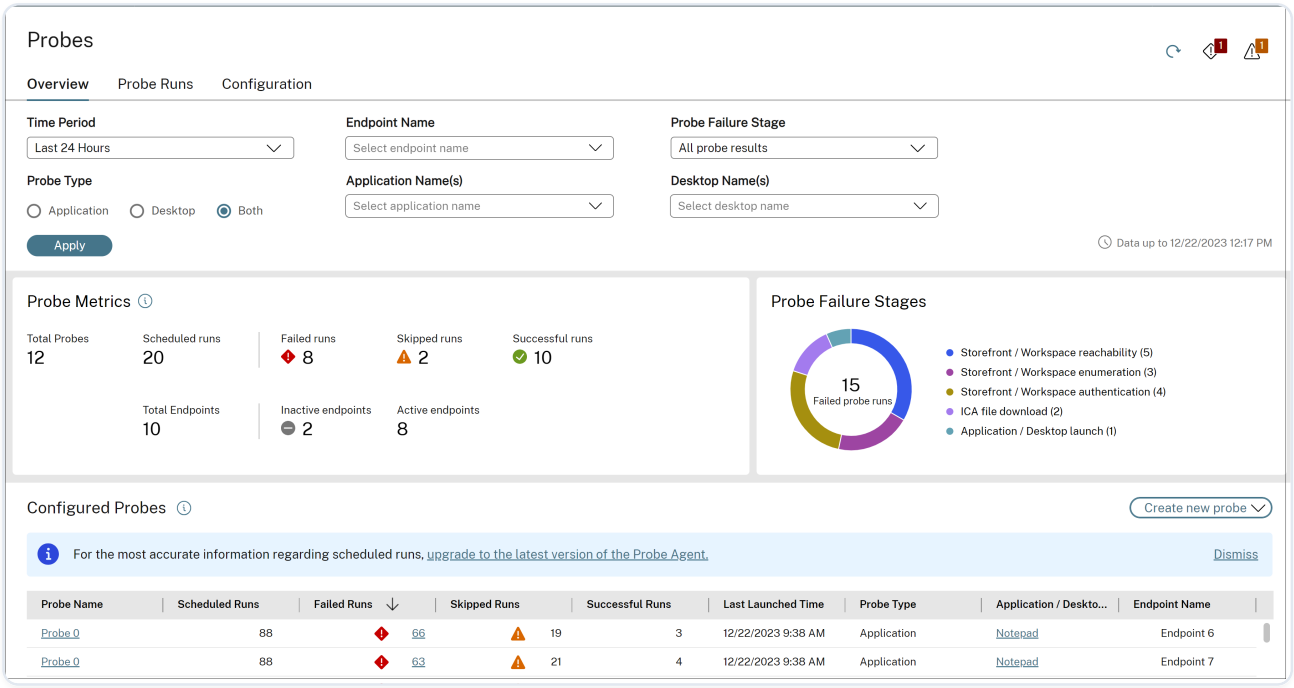
- **StoreFront到達可能性** - 構成されたStoreFront URLに到達できません。
- **StoreFront認証** - 構成されたStoreFront資格情報が無効です。
- **StoreFront列挙** - StoreFrontのアプリケーション列挙リストに、プローブ対象のアプリケーションまたはデスクトップが含まれていません。
- **ICA®ダウンロード** - ICAファイルが利用できません。

- **アプリケーション/デスクトップの起動** – アプリケーションまたはデスクトップを起動できませんでした。

ステップ4：プローブ結果の表示

プローブでプローブ結果を確認できます。プローブビューでは、プローブ結果の包括的な概要が示されます。これらの結果は、問題をプロアクティブに分析およびトラブルシューティングし、ユーザーのセッション起動エクスペリエンスをよりスムーズにするのに役立ちます。

概要タブには、構成されているすべてのプローブの概要が1つのビューに表示されます。



プローブは、期間、プローブタイプ、エンドポイント名、アプリケーション名、デスクトップ名、およびプローブ結果タイプに基づいてフィルターできます。フィルター条件に一致するプローブは、プローブ、アプリケーション/デスクトップ、およびエンドポイントごとに次の詳細とともに表示されます。

プローブメトリックには、スケジュール済み、計画済み、スキップ済み、成功、失敗した実行の数が表示されます。

- 完了した実行 – 完了まで実行されたプローブ実行の数。
- 失敗した実行 – 失敗したプローブ実行の数。
- スキップされた実行 – エンドポイントが非アクティブであるか、サービスが利用できないために完了しなかった実行の数。
- 成功した実行 – アプリ/デスクトップの起動中に、どの段階でも失敗することなく正常に完了したプローブの数。

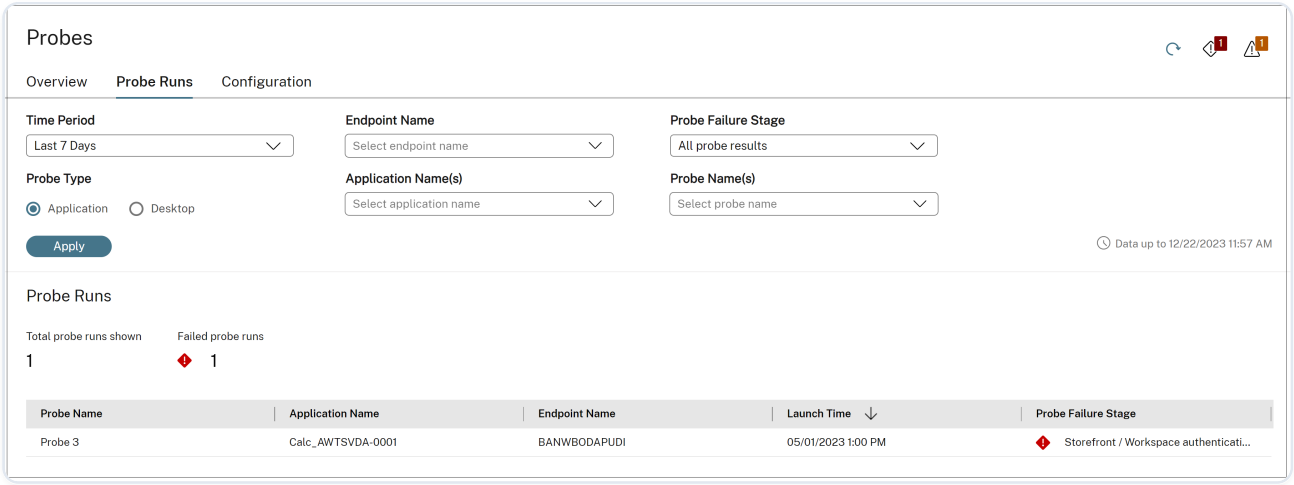
エンドポイントマシンの総数も、アクティブなマシンと非アクティブなマシンの数とともに表示されます。

プローブ失敗ステージは、各失敗グループの失敗分布を視覚的に内訳表示します。ほとんどの失敗が発生したステージを分析することで、プローブ結果の解釈と問題のトラブルシューティングが容易になります。グラフィカル表示では、アプリケーション/デスクトップの起動、ICAファイルのダウンロード、Storefront/Workspaceの列挙、Storefront/Workspaceの到達可能性、Storefront/Workspaceの認証における失敗したプローブ実行の数が示されます。

ほとんどの失敗が発生したステージを分析するのに役立ちます。この情報は、プローブ結果を迅速に理解し、トラブルシューティングを行うのに役立ちます。

エンドポイントが非アクティブであるか、サービスが利用できないために、一部のプローブ実行が完了しない場合があります。

プローブ実行タブには、完了したプローブ実行の結果が詳細に表示されます。選択したプローブの個々の実行の詳細を確認するためにドリルダウンできます。重要なピボットポイントに基づいて、さらにフィルタリングおよび分析できます。



プローブ実行は、期間、プローブタイプ、エンドポイント名、アプリケーション名、デスクトップ名、プローブ失敗ステージに基づいてフィルタリングできます。プローブ失敗ステージは、プローブが失敗したステージを表示します。プローブ名、スケジュールされた実行、失敗した実行、アプリケーション/デスクトップ名のリンクをクリックすると、フィルタ条件に一致するプローブ実行のリストが表示されたプローブ実行ページに移動します。

コスト最適化

Citrix Director には、仮想マシンとセッションの使用状況を効果的に分析するのに役立つ、コスト最適化と呼ばれる新機能が導入されました。この機能は、コストを最適化する方法について洞察

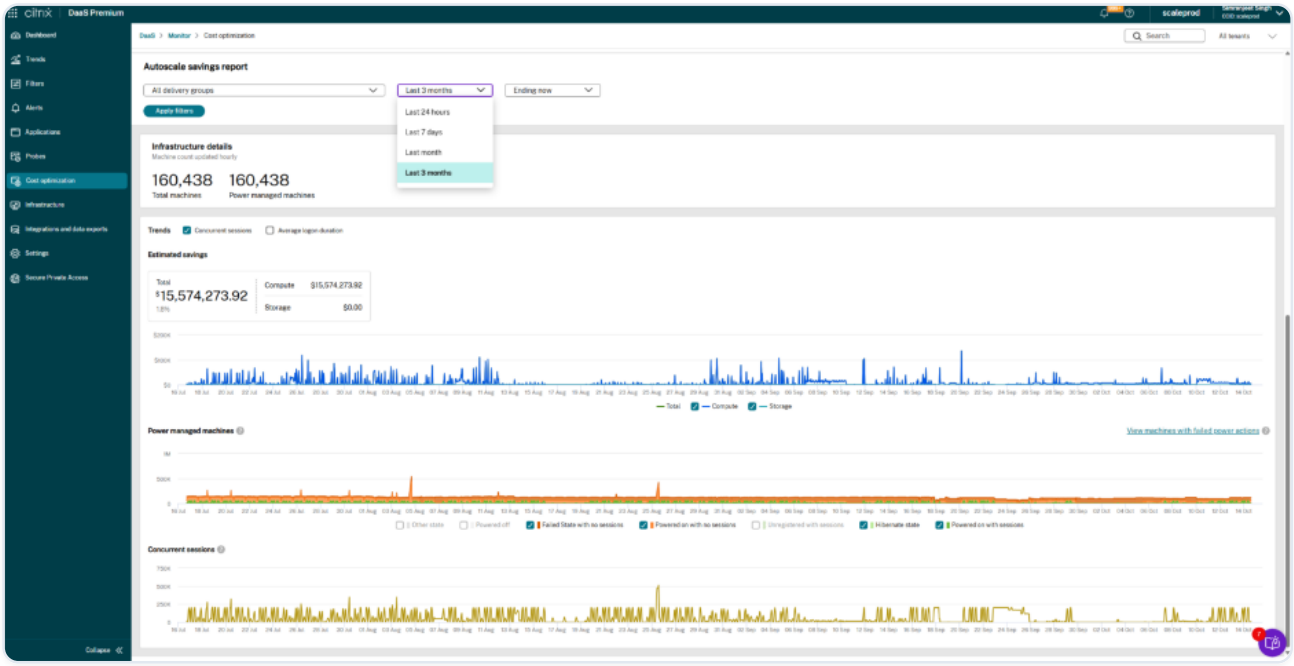
に満ちた視覚的な表現を提供します。また、不要なマシンを排除し、それによってコストを削減するのにも役立ちます。

コスト最適化をサポートするために、次のアラートも導入されました。

- 起動失敗アクションとシャットダウン失敗アクション
- マシンの稼働時間アラート

最近の電源操作を行ったマシンを検査して、ユーザーの問題を引き起こす電源オンの失敗や、コストを増加させる電源オフの失敗を分析することもできます。詳細については、最近の電源操作を行ったマシンの検査セクションを参照してください。

ホームページの左メニューから**コスト最適化**タブをクリックして、**コスト最適化**ページにアクセスします。



コスト最適化ホームでは、次のことができます。

- 開始リンク - このリンクにアクセスして、コスト最適化機能の詳細を確認してください。
- コスト最適化ページを確認する - **コスト最適化**ページに関するフィードバックを提供できます
- データを更新します。
- アラートを表示する - 重大なアラートと警告アラートの両方を表示できます。

コスト最適化ページには、次の機能が含まれています。

- コスト削減
- ワークロードの適正化

コスト最適化のコストはどのように計算されますか?

マシンあたりの時間コストは、ハイパーバイザーがサポートする通貨で表示されます。このセクションでは、Azureマシンおよびその他のマシンのコストがどのように計算されるかについて説明します。

Azureマシンのコスト

コスト計算の優先順位は次のとおりです:

1. 'Microsoft.Consumption/pricesheets/read権限が利用可能な場合、Azureサブスクリプションで構成されている通貨で実効価格が表示されます。
2. 権限が利用できない場合、Azureの小売価格が表示されます。詳細については、Azure Retail Prices overviewを参照してください。
3. 実効価格または小売価格が利用できない場合、Web Studioで管理者が入力したコストに基づいてコストが表示されます。
4. Web Studioでコストが指定されていない場合、デフォルトのコストである1ドルが考慮されます。

Azureのアカウント詳細を確認し、実効価格を見つけるために必要な権限を追加するには、次の手順を実行します:

1. Citrix DaaSに移動します。
2. **Hosting**タブをクリックして、ホスティング接続アカウントを見つけます。
3. 「**ホスティング**」タブに記載されている「**アプリケーション ID**」を探します。

   ホスティングタブ(/en-us/citrix-virtual-apps-desktops/current-release/media/daas-azure-hosting.png)
4. Microsoft Entra ID に移動し、手順 3 でメモした「**アプリケーション ID**」を探します。
5. **サブスクリプション** > **アクセス制御 (IAM)** に移動し、ホスティング接続 SPN 用に構成されたカスタマイズされたロールを選択します。

   Azure ポータル(/en-us/citrix-virtual-apps-desktops/current-release/media/azure-portal.png)

   Azure ポータルのサブスクリプション(/en-us/citrix-virtual-apps-desktops/current-release/media/azure-portal-subscriptions.png)
6. ロールに *Microsoft.Consumption/pricesheets/read* 権限を追加します。

Azureの小売価格を確認する方法?

`Microsoft.Consumption/pricesheets/read` が利用できない場合、Azure の小売価格が表示されます。これで、Retail Rates Prices API を使用して、すべての Azure サービスの小売価格を取得できます。以前は、Azure サービスの価格を取得する唯一の方法は、Azure 料金計算ツールを使用するか、Azure ポータルを使用することでした。詳細については、「Azure 小売価格の概要」を参照してください。

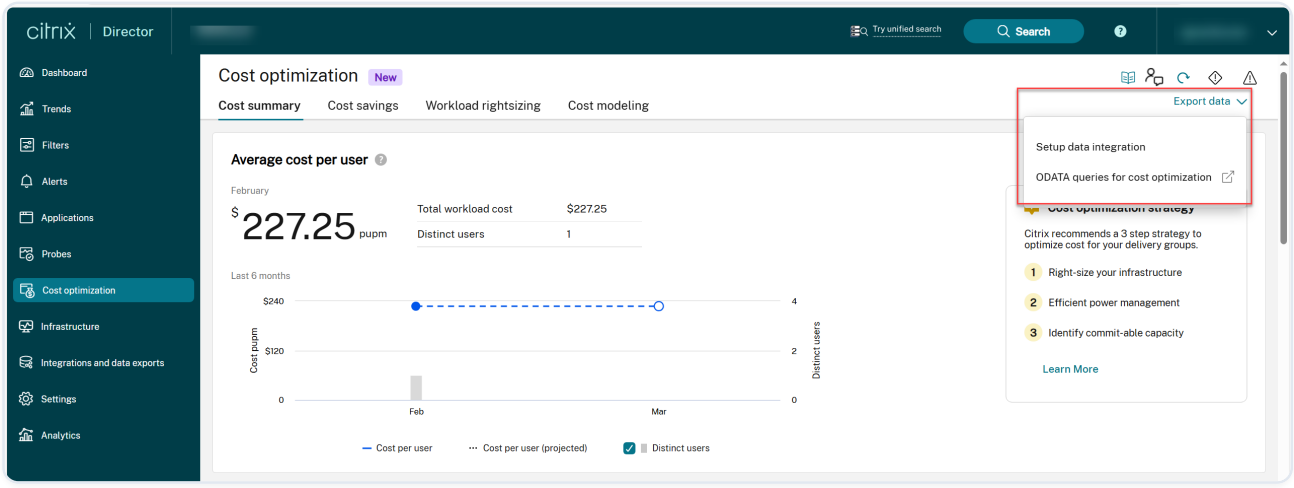
Azure 以外のマシンのコスト計算

その他のマシンについては、Web Studio で管理者が入力したコストに基づいてコストが表示されます。Web Studio でコストが指定されていない場合、デフォルトのコスト $1 が考慮されます。

データのエクスポート

データ統合と ODATA クエリを使用して、「**コスト最適化**」ページのデータをエクスポートできます。データをエクスポートするには、「**コスト最適化**」ページで「**データのエクスポート**」をクリックすると、次のオプションが表示されます。

- データ統合のセットアップ
- コスト最適化のための ODATA クエリ



データ統合のセットアップ

Monitor Service API を使用してコスト最適化データを統合し、トラブルシューティングや問題のトリアージのためにデータを収集できます。詳細については、統合とデータエクスポートページを参照してください。

コスト最適化のためのODATAクエリ

コスト最適化ページで利用可能なサンプルODATAクエリを使用して、データをエクスポートできます。

ODATAの利用を開始する

以下のリンクは、ODATAの利用を開始するのに役立ちます。

- ODATAの概要
- Citrix CloudのOData v4エンドポイントを使用してCitrix Monitor Serviceデータにアクセスするためのさまざまな方法
- Citrix Monitor ServiceデータでOData V4集計クエリを使用する
- ODataとAPIクライアントを使用してPowerBIをDaaS Monitorに接続する方法
- Postmanを使用してログオン時間が長いユーザーの詳細を取得する
- Monitor Serviceデータにアクセスする方法
- データアクセスプロトコル
- モニターモデル
- モニター通知

サンプルODATAクエリ

未使用のVDAを検索する

未使用のVDAを検索するには、デスクトップグループID、VDAの開始日、および終了日を指定する必要があります。

未使用のリソースへの支出を削減する方法の詳細については、「ワークロードの適切なサイジング」を参照してください。

クエリの例:

```
https://<DDC URL>/monitorodata/ResourceUtilizationSummary?
$apply=filter(DesktopGroupId eq desktop-group-id and granularity eq 1440
and SummaryDate ge startdate and SummaryDate lt enddate)/
groupby((MachineId), aggregate(cast(TotalSessionCount, Edm.Int32) with
average as AvgTotalSessionCount))/filter(AvgTotalSessionCount eq 0.0)/
aggregate($count as UnusedVDACount)
```

1日の平均稼働時間（分）を検索する

1日の平均稼働時間（分）を検索するには、以下を指定する必要があります。

- デスクトップグループID
- 開始日

- 終了日
- 終了日と開始日の間の日数。

未使用のリソースへの支出を削減する方法の詳細については、「ワークロードの適切なサイジング」を参照してください。

クエリの例:

```
https://[<DDC URL>|https://api-us.cloud.com/monitorodata/
ResourceUtilizationSummary?$apply=filter(DesktopGroupId] /monitorodata/
ResourceUtilizationSummary?$apply=filter(desktopGroupId eq desktop-group-
id and granularity eq 1440 and SummaryDate ge startdate and SummaryDate lt
enddate)/groupby((MachineId), aggregate(cast(UptimeInMinutes, Edm.Int32)
div day-difference with sum as TotalUptimeInMinutes))/
aggregate(TotalUptimeInMinutes with average as
DailyAverageUptimeInMinutes)
```

失敗したマシンの電源アクションを検索する

失敗したマシンの電源アクションの詳細については、「電源オンアクションの失敗と電源オフアクションの失敗」を参照してください。

クエリの例:

```
https:// <DDC URL> /monitorodata/Machines?$filter=LifecycleState eq 0 and
DesktopGroup/SessionSupport eq 1 and
(cast(LastPowerActionReason,'Edm.Int32') eq 6 or
cast(LastPowerActionReason,'Edm.Int32') eq 7 or
cast(LastPowerActionReason,'Edm.Int32') eq 8) and
(cast(LastPowerActionFailureReason,'Edm.Int32') eq 300 or
cast(LastPowerActionFailureReason,'Edm.Int32') eq 402 or
cast(LastPowerActionFailureReason,'Edm.Int32') eq 401) and MachineRole eq
0&$orderby=Name&$skip=0&$top=50&$expand=DesktopGroup($select=Name)&$select
=Sid,Id,Name,IsAssigned,IPAddress,FaultState,LastDeregisteredCode,FailureD
ate,CurrentPowerState,CurrentSessionCount,IsInMaintenanceMode,LastPowerAct
ionFailureReason,LastPowerActionCompletedDate
```

合計節約額を確認する

コスト削減の詳細については、コスト削減ページを参照してください。

サンプルクエリ:

```
https://[<DDC URL>|https://api-us.cloud.com/monitorodata/
ResourceUtilizationSummary?$apply=filter(DesktopGroupId] /monitorodata/
MachineCostSavingsSummaries?$apply=aggregate(TotalAmountSaved with sum as
TotalAmountSavedSum)
```

マシンの状態を確認する

コスト削減の詳細については、コスト削減ページを参照してください。

サンプルクエリ:

```
https:// <DDC URL> /monitorodata/MachineCostSavingsSummaries?
$filter=SummaryDate eq
2024-08-09T06:00:00Z&$select=TotalMachinesCount,PowerManagedMachinesOff,Po
werManagedMachinesInHibernate,PowerManagedMachinesOnWithSessions,PowerMana
gedMachinesOnWithoutSessions
```

コスト削減

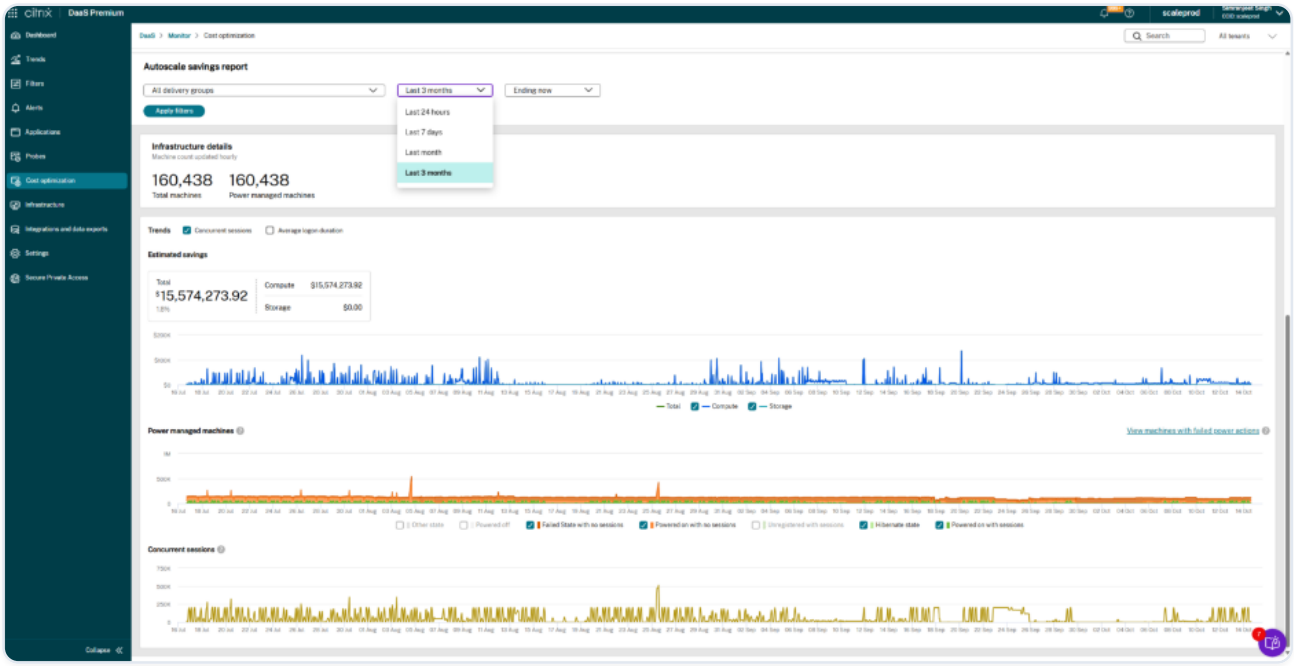
「**コスト削減**」ページには、選択した期間に発生したインフラストラクチャの節約額の視覚的な表示と、残りの日数で予想される節約額の予測が表示されます。このページでは、マシンの使用状況とセッションを分析することで、達成された節約とコスト削減の機会を特定するのに役立ちます。このページでは以下を提供します。

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

マシンの使用量は通常、ピーク時に増加し、より多くのリソースを必要とします。Autoscale™ 機能は、需要の少ない期間に未使用のマシンを自動的に電源オフすることで、コスト削減に役立ちます。予測される節約額は、この使用パターンによって異なります。ただし、未使用のマシンが存在する場合や、Autoscale の電源アクションに障害が発生した場合など、特定の状況下ではコストが予想を超える可能性があります。これらの発生の背後にある理由を特定することは、これまで困難でした。

「**コスト最適化**」ページには、予想されるコストを超える可能性のあるさまざまなシナリオに関する詳細情報が表示されます。同様に、たとえば、セッションのないマシンがある場合、さらなるコスト削減の機会が表示されます。

「**コスト最適化**」ページにアクセスするには、「**ホーム**」ページの左メニューから「**コスト最適化**」タブをクリックします。



上部のドロップダウンリストから、サイトにクラウドプロバイダーとオンプレミスプロバイダーの両方がある場合、すべてのクラウドプロバイダー、すべてのオンプレミスプロバイダー、または個々のプロバイダーでフィルタリングできるようになりました。

注:

> フィルターは、適用ボタンなしで選択するとすぐに適用されます。

> 「**コスト最適化**」ページには、「**推定節約額**」と「**Autoscale節約レポート**」が含まれています。コスト削減は、ハイパーバイザーの通貨または発生したコストの割合として表示できます。

推定節約額: このグラフィカルな表示は、インフラストラクチャリソースの効率的な利用を評価するのに役立ちます。コスト削減は、ハイパーバイザーの通貨または発生したコストの割合として表示されます。このグラフは、コンピューティング関連の節約とストレージの節約から達成された節約を示しています。

注:

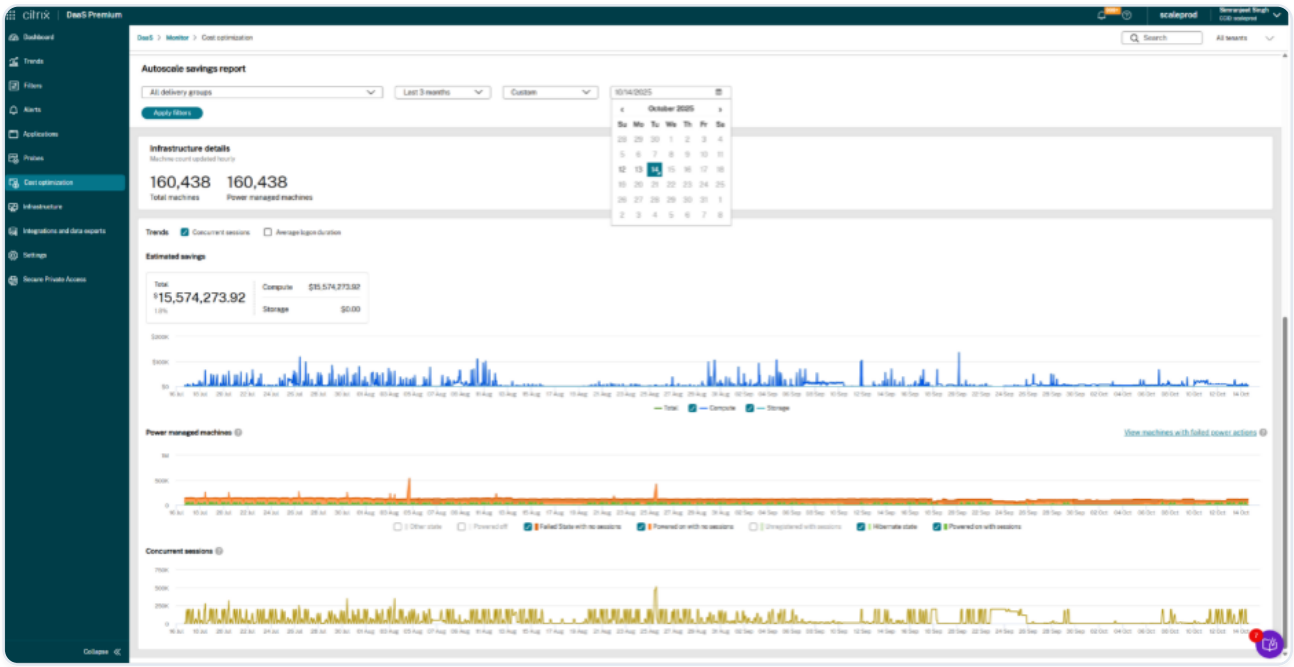
> ストレージからの節約を表示するには:

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

以下の期間の結果を表示できます。

- 7日間
- 30日間
- 3か月
- 6か月
- 12か月

次の図は、「推定インフラストラクチャ節約」セクションを示しています。



次の表は、「推定インフラストラクチャ節約」グラフの要素を示しています。

要素	説明
合計節約額	選択した期間にインフラストラクチャで達成された合計節約額を表示します。節約額はさら

要素	説明
	にストレージコストとコンピューティングコストに分類され、表形式で利用できます。
推定節約額	選択した期間にインフラストラクチャで達成された節約額を表示します。
電源管理されたマシン	電源管理されたマシンの総数を表示します。
予測節約額	残りの期間でどれだけのインフラストラクチャ節約が可能かを表示します。
コンピューティング - 合計	コンピューティング関連の節約から達成された合計節約額を表示します。
コンピューティング - Autoscale	Autoscale機能を使用しているコンピューティング関連の節約から達成された合計節約額を表示します。
コンピューティング - ユーザーアクション	ユーザーアクションによるコンピューティング関連の節約から達成された合計節約額を表示します。
ストレージ - 合計	ストレージの節約から達成された合計節約額を表示します。
ストレージ - Autoscale	Autoscale機能を使用しているストレージの節約から達成された合計節約額を表示します。
ストレージ - ユーザーアクション	ユーザーアクションによるストレージ節約から達成された合計節約額を表示します。

オートスケール節約レポート: このグラフィカルな表現は、オートスケール機能が構成および有効化されているデリバリーグループの節約レポートを提供します。このレポートは、電源管理されているマシンにのみ適用されます。デリバリーグループを選択し、今日、昨日、先週、来週、今月、または来月のデータを選択できます。グラフにカーソルを合わせると、特定のグラフ値を取得できます。

> **注:**

> デリバリーグループが削除された場合、オートスケール節約レポートでデータは取得できません。

> デリバリーグループのドロップダウンリストから、以下のオプションにドリルダウンできます。

- **すべてのデリバリーグループ**: インフラストラクチャの詳細には、すべてのデリバリーグループ情報が表示されます。
- **すべてのシングルセッション**: シングルセッションマシンであるすべてのデリバリーグループのインフラストラクチャの詳細が、チャートにカーソルを合わせたときの、マシンの電源状態、成功したオートスケール電源アクション、およびセッションのグラフィカルな表現とともに表示されます。
- **すべてのマルチセッション**: マルチセッションマシンであるすべてのデリバリーグループのインフラストラクチャの詳細が、グラフィカルな表現とともに表示されます。
- **最大15個を選択** - インフラストラクチャの詳細には、選択されたすべてのデリバリーグループ（最大15個）が、グラフィカルな表現とともに表示されます。
- **最大15個を除外** - インフラストラクチャの詳細には、選択されたデリバリーグループ（最大15個）を除外したすべてのデリバリーグループが、グラフィカルな表現とともに表示されます。

選択した期間のデータが表示されます。**推定節約額**のグラフ表示は、ドロップダウンメニューから選択された実際の節約額です。ピークポイントにカーソルを合わせると、マシンの電源状態、Autoscaleの電源アクションの成功、およびセッションに関する情報が表示されます。

選択したデリバリーグループに基づいて、次の詳細を表示できます。

- **インフラストラクチャの詳細**
  - 総マシン数と電源管理対象マシン数 - 総マシン数と、そのうち電源管理されているマシンの数を表示します。このデータは、残りの電源管理対象外のマシンを電源管理対象マシンに変換し、Autoscale機能を有効にしてより包括的なカバレッジを実現するさらなる機会を提供します。インフラストラクチャの詳細セクションのデータは、1時間ごとに更新される最新の既知の情報を表示します。
- **カタログの詳細**

  ハイパーバイザー（サービスプロバイダー）の名前を表示します。詳細については、「サポートされているVDAホスティングプラットフォーム」を参照してください。カタログの詳細のデータは、現在の時点で利用可能な最新のデータ（ライブデータ）を表示します。

次の詳細を取得できます。

- **ハイパーバイザー名** - サイトが接続されているハイパーバイザーの名前を表示します。複数のハイパーバイザーが存在する場合は、利用可能なすべてのハイパーバイザーを表示します。
- **インスタンス** - インスタンスの名前を表示します。
- **1時間あたりの合計コスト** - ハイパーバイザーがサポートする通貨で、マシンごとの1時間あたりのコストを表示します。Azureマシンでは、Microsoft.Consumption/pricesheets/read権限が利用可能な場合、Azureサブスクリプションで構成されている通貨で実効価格が表示されます。権限が利用できない場合、Azureの小売価格が表示されます。詳細については、Azure Retail Prices overviewを参照してください。その他のマシンでは、Web Studioで管理者が入力したコストに基づいてコストが表示されます。Web Studioでコストが指定されていない場合、デフォルトのコストは1ドルです。詳細については、[コスト最適化のコストはどのように計算されますか？
- **1時間あたりのコンピューティングコスト** - コンピューティング関連の節約によるコスト削減額を表示します。
- **1時間あたりのストレージコスト** - ストレージの節約によるコスト削減額を表示します。
- **マシン** - 選択したインスタンスのマシン数を表示します。

- **Autoscale構成（最新の既知）**

  使用中のタグ - WebStudioのAutoscale設定で構成されているマシンのタグを表示します。タグ付けされたマシンに基づいてデータをフィルタリングすることもできます。この場合、タグ付けされたマシンの概要のみが表示されます。

  キャパシティバッファ（ピーク時）」と「キャパシティバッファ（オフピーク時）

  ピーク時およびオフピーク時のデリバリーグループの最大要件に基づいて、電源がオンになっているマシンのバッファの割合を表示します。

- **推定節約額**

  選択した期間にインフラストラクチャで達成された節約額を表示します。Autoscale機能が有効なAzureマシンについて、コンピューティング関連の節約とストレージ関連の節約による節約額を表示できます。

- **電源管理対象マシン**

  Autoscaleを有効にすると、コストを最適化するために、電源管理対象マシンは使用されていないときに電源がオフになります。以下の詳細情報を取得できます。

- 電源がオフになったマシンの数 - このデータは、電源がオフになり、コスト削減に貢献したマシンの数を分析するのに役立ちます。
- 休止状態 - このデータは、休止状態にあるマシンの数を分析するのに役立ちます。
- セッションなしで稼働中のマシン - このデータは、なぜマシンがセッションなしでアクティブであったかを分析する機会を提供します。このデータは、より効果的なインフラストラクチャ節約戦略を計画する機会を提供します。
- セッションありで稼働中のマシン - このデータは、電源がオンになり、アクティブなセッションがあったマシンの数を分析するのに役立ちます。
- 電源オフ - このデータは、電源がオフまたは中断されたマシンの数と、このアクションがいつ実行されたかを分析するのに役立ちます。このデータを確認し、さらに変更を加えることで、コスト削減に貢献できます。
- 電源オン - このデータは、電源がオンになったマシンの数と、このアクションがいつ実行されたかを分析するのに役立ちます。このデータを確認し、さらに変更を加えることで、コスト削減に貢献できます。
- セッションなしの失敗状態: このフィールドには、失敗状態にあり、アクティブなセッションがないマシンの数が表示されます。
- セッションありで未登録: このフィールドには、未登録状態にあるが、セッションを提供しているマシンの数が表示されます。

> **注:**
>
> セッションなしで失敗状態のマシンと、電源操作が失敗した状態のマシンの数を表示し、失敗の理由、時間、デリバリーグループに基づいてアクションを実行できます。これらの数はクリック可能なリンクであり、さらなるアクションのためにフィルターページに移動します。この数には、シングルセッションマシンとマルチセッションマシンの両方が含まれます。

- **同時セッション**

  選択した時点でのセッションの合計数を表示します。このデータは、コスト最適化のためにマシンをいつ電源オフにするかを決定するのに役立ちます。

- **平均ログオン時間**

  選択した期間におけるユーザーの平均ログオン時間を表示します。

ワークロードの適正化

強化されたワークロードの適正化ページは、デリバリーグループの使用状況とサイジングの側面を分析するのに役立ちます。これにより、デリバリーグループはマシンまたはユーザーのアクティビティに基づいて分析できます。

マシンベースの分析では、次のことが可能です。

- 使用状況に基づいて仮想デスクトップを分類し、アクティビティがない、または低いマシンを特定して、未使用のリソースへの支出を削減します。使用状況分析
- 仮想デスクトップのリソース使用率を分析し、コストを削減したり、ユーザーエクスペリエンスを向上させたりするために適正化する必要があるマシンを特定します。サイジング分析

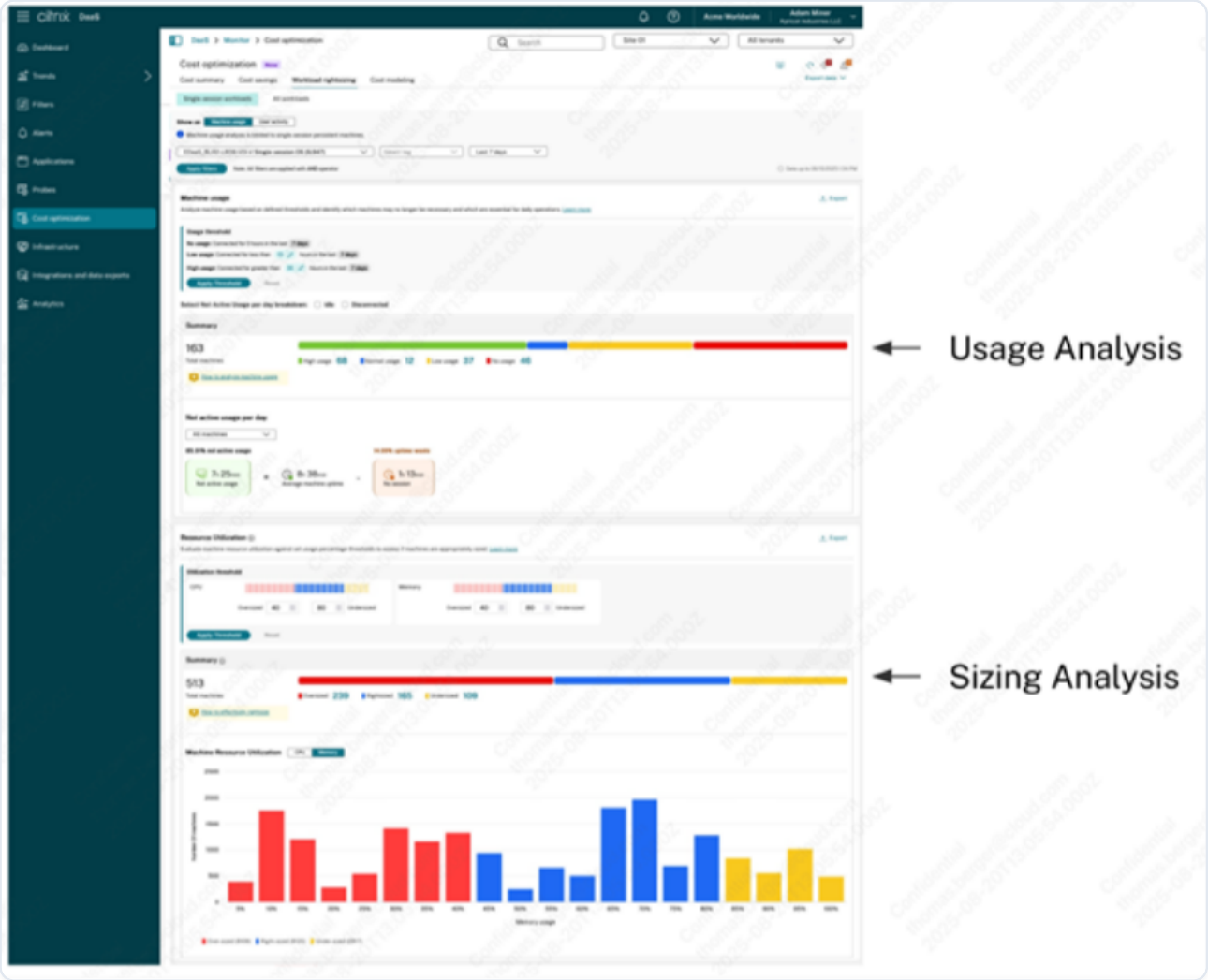
ユーザーベースの分析では、次のことが可能です。

- アクティビティに基づいてユーザーを分類します。IT衛生上の理由から、アクティビティのないユーザーのアクセス権限を削除することを検討してください。使用率の低いユーザーは、より効率的なリソース使用のために共有リソースに移動できます。
- ユーザーのリソース消費量を分析して、平均よりも高いまたは低いリソース消費量を持つコホートを特定し、ユーザーをより効果的に分散させます。

ホーム画面の左メニューから**コスト最適化**タブをクリックします。次に、**ワークロードの適正化**タブをクリックして、**ワークロードの適正化**ページにアクセスします。

> **注:**
>
> ページの上部で、マシンベースとユーザーベースの分析を切り替えることができます。

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



マシン分析は、Windows 365 EnterpriseやFrontline専用など、ユーザーに静的に割り当てられた仮想デスクトップのシナリオに最適です。ユーザー分析は、ランダムに割り当てられた仮想デスクトップを持つデリバリーグループの分析に役立ちます。現在、どちらの分析もシングルセッションマシンに限定されています。

> **注:**
>
> ページ上部の「すべてのワークロード」ボタンからアクセスできる従来のライトサイジング分析は、今後のリリースで非推奨になります。

使用状況分析

使用状況分析では、仮想デスクトップをアクティビティレベルに基づいて次のように分類できます。

- **使用率が低いまたは使用されていないマシン (専用マシン)**: このカテゴリのマシンは不要になっている可能性があり、コスト削減のために削除できる場合があります。

- **使用率が高いマシン (専用マシン)**: このカテゴリは日常業務に不可欠であり、追加のサービス継続性対策が必要になる場合があります。
- **使用率が低いまたは使用されていないユーザー (プールされたマシン)**: 選択した期間内にアクティビティがないユーザーは、デリバリーグループに割り当てる必要がなくなる場合があります。それらを削除すると、環境のコスト削減に役立ちます。アクティビティの低いユーザーは、再割り当ての恩恵を受ける可能性があります。使用状況を統合し、コストを削減するには、専用デスクトップを持つアクティビティの低いユーザーをプールされたデスクトップに移動することを検討してください。

使用状況分析を実行するには：

1. デリバリーグループまたはタグに基づいてマシンを選択します
2. 分析の期間を選択します。
3. 低使用率および高使用率のパターンを定義するしきい値を確認および構成します。
4. 構成されたしきい値に基づいて仮想デスクトップの分類を示す概要セクションを調べます。
5. 各マシンの使用状況の詳細を表示する正味アクティブ使用状況セクションを確認します。アイドル時間と切断時間は、正味アクティブ使用状況分析に含めることも除外することもできます。
6. ドロップダウンを使用して、特定のカテゴリに焦点を当てます。
7. エクスポート機能を使用してマシン名と関連ユーザーをエクスポートし、マシン名と関連ユーザーを確認します。

> **注:**
>
> 提供された例はマシンベースの使用状況分析を示していますが、ユーザーベースの分析の手順も同等であり、個別に説明されていません。

> マシンの使用状況(/en-us/citrix-daas/media/machine-usage.png)

サイジング分析

サイジング分析は、リソース使用率に基づいて仮想デスクトップまたはユーザーを以下のように分類します。

- オーバーサイズのマシン: 必要以上のリソースを持っています。リソース割り当てを減らすことで、ユーザーエクスペリエンスに影響を与えることなくコストを削減できます。

- アンダーサイズのマシン: 十分なリソースがありません。より多くのリソースを割り当てることで、ユーザーエクスペリエンスを向上させることができます。
- 適切なサイズのマシン: オーバーサイズとアンダーサイズのしきい値の間に位置します。
- ライトユーザー: これらのユーザーは再割り当ての恩恵を受ける可能性があります。統合してコストを削減するために、専用デスクトップを持つライトユーザーを共有プールデスクトップに移動することを検討してください。
- 中程度のユーザー: 中程度のユーザーは、デリバリーグループ内のマシンに適切に割り当てられており、最適なユーザーエクスペリエンスを期待できます。
- パワーユーザー: パワーユーザーは大量のリソースを消費し、プールされたデスクトップを共有している場合、その高い使用率が、そのマシン上の他のユーザーの全体的なエクスペリエンスに悪影響を与える可能性があります。すべてのユーザーのエクスペリエンスを向上させ、パワーユーザーがデスクトップに一貫してアクセスできるようにするために、これらのユーザーを専用デスクトップに移動するか、個別のデリバリーグループに割り当てることを検討してください。

サイジング分析を実行するには:

1. デリバリーグループまたはタグに基づいてマシンを選択します
2. 分析の期間を選択します。
3. CPUとメモリ使用率に個別のしきい値を構成します。
4. 仮想デスクトップの分類を示す概要セクションを確認します
5. CPUとメモリの分布を示すマシンリソース使用率チャートを分析します。
6. リソースタイプに基づいてマシン構成を微調整し、外れ値を特定します。
7. エクスポート機能を使用してマシン名と関連ユーザーをエクスポートし、マシン名と関連ユーザーを確認します。

> **注:**

> 提示された例はマシンベースのリソース消費分析を示していますが、ユーザーベースの分析の手順も同等であり、別途説明はしません。

> リソース使用率(/en-us/citrix-daas/media/resource-utilization.png)

> **注:**

> 使用率分析では、選択した期間におけるデリバリーグループの95パーセンタイル使用率を使用します。これは、CPUまたはメモリ使用率の95%が設定値以下であることを示します。

ベストプラクティス

- 使用状況分析を使用して、利用率の低いマシンを削除することでコスト削減の機会を特定します。
- サイジング分析を適用して、リソース割り当てを最適化し、ユーザーエクスペリエンスを向上させます。
- 静的に割り当てられた仮想デスクトップのシナリオでは、正確な分析のためにマシン分析を使用します。
- プールされた仮想デスクトップのシナリオでは、正確な分析のためにユーザーアクティビティを使用します。
- ランダムに割り当てられた仮想デスクトップを分析する際は、ローミングパターンを考慮します。
- 詳細なレポートをエクスポートして、さらなる分析とドキュメント作成に役立てます。

主要な用語とグラフ

マシンの正味アクティブ使用量: 正味アクティブ使用量は、平均マシン稼働時間から合計稼働時間の無駄を差し引いて計算されます。すべての時間は分単位です。

正味アクティブ使用量の割合: ユーザーがマシンをアクティブに使用した実際の時間。これは、マシンが電源オンの状態で、少なくとも1つのセッションがアクティブだった期間です。

平均マシン稼働時間: マシンが電源オンだった合計時間。

セッションなし: アクティブなセッションがないことによる稼働時間の無駄。

アイドル時間: アイドル状態のセッションによる稼働時間の無駄。これは、マシン上のすべてのセッションがアイドル状態である時間です。

切断時間: 切断されたセッションによる稼働時間の無駄。これは、マシン上のすべてのセッションが切断されている時間です。

合計マシン数 - マシンの総数を表示します。これには、選択した期間中に電源がオンになっていたすべてのマシンが含まれます。

平均セッション密度 - これは、マシン数と選択した期間にわたる平均です。セッションに利用可能なリソースに影響を与える、マシン上のセッション負荷の量を指します。

未使用のマシン - 選択した期間中にセッションがなかったが、電源がオンのままだったマシンの数を表示します。

CPU使用率:

マシンコホート - CPU使用率に基づいて、上位、中位、下位に分類されたマシングループに関する情報を提供します。しきい値の制限は管理者が構成できます。

CPUピークの範囲 - マシンコホートに対応するCPU使用率に基づいて、CPUピークの範囲を表示します。

マシン - マシンコホートに対応するマシンの数を表示します。

セッション密度 - マシンコホートに対応するセッション密度を表示します。

リソース使用率の傾向:

CPUピークの範囲 - バンド内のCPUピークの範囲を表示します。バンド内の任意のポイントにカーソルを合わせると、バンドの上下の値が表示されます。

メモリ使用率のピーク - 選択したマシンと選択した期間のメモリ使用率の最高値をグラフで表示します。

平均セッション密度 - 選択したマシンと選択した期間の平均セッション密度をグラフで表示します。

平均ICA RTT - セッションの平均ラウンドトリップ時間を表示します。このグラフは、アクティブなセッションがない場合やセッションが切断されている場合に中断を示します。

平均ログオン時間 - 選択したマシンと選択した期間の平均ログオン時間をグラフで表示します。このグラフは、選択した期間中に新しいログオンが開始された場合にデータを表示します。

コスト概要

コスト概要ページでは、Citrix®環境の実行に関連する費用の包括的な概要が提供されます。この機能強化により、以下の情報を把握できます。

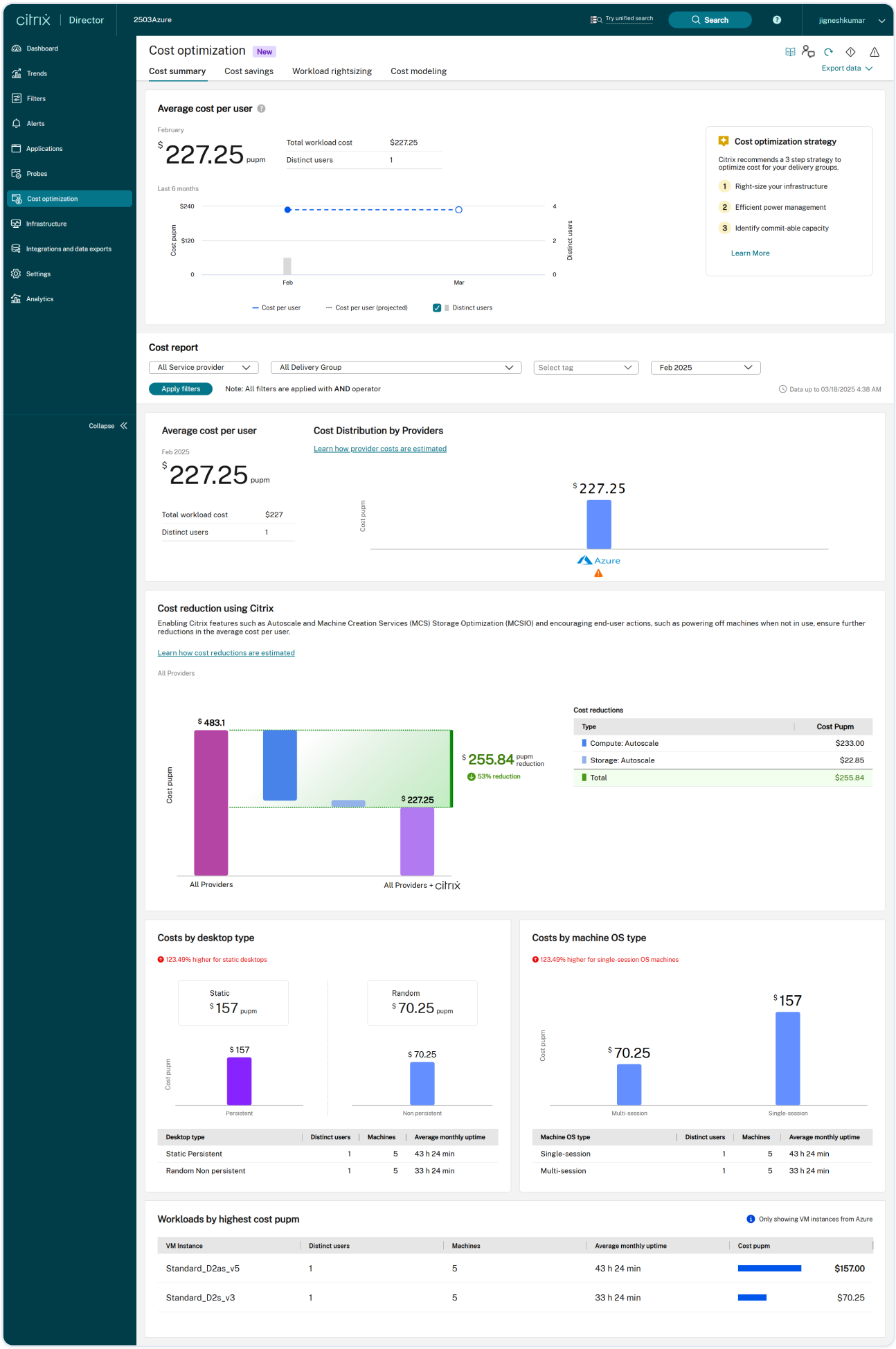
- ユーザーあたりの総コスト
- 選択されたワークロードプロバイダー、デスクトップの種類、およびVMシリーズセットによる仮想化提供のコスト

このページでは、以下を提供します。

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

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

「**コスト概要**」ページにアクセスするには、「**Director**」>「**コスト最適化**」>「**コスト概要**」をクリックします。「**コスト概要**」ページが表示されます。


citrix | Director
2503Azure
Try unified search
Search
jigneshkumar
Dashboard
Trends
Filters
Alerts
Applications
Probes
Cost optimization
Infrastructure
Integrations and data exports
Settings
Analytics
Collapse
Cost optimization
New
Cost summary
Cost savings
Workload rightsizing
Cost modeling
Export data
Average cost per user
February
$ 227.25 pupm
Total workload cost $227.25
Distinct users 1
Last 6 months
$240
$120
0
Cost pupm
4
2
0
Distinct users
Feb
Mar
Cost per user
Cost per user (projected)
Distinct users
Cost optimization strategy
Citrix recommends a 3 step strategy to optimize cost for your delivery groups.
1 Right-size your infrastructure
2 Efficient power management
3 Identify commit-able capacity
Learn More
Cost report
All Service provider
All Delivery Group
Select tag
Feb 2025
Apply filters
Note: All filters are applied with AND operator
Data up to 03/18/2025 4:38 AM
Average cost per user
Feb 2025
$ 227.25 pupm
Total workload cost $227
Distinct users 1
Cost Distribution by Providers
Learn how provider costs are estimated
$ 227.25
Cost pupm
Azure
Cost reduction using Citrix
Enabling Citrix features such as Autoscale and Machine Creation Services (MCS) Storage Optimization (MCSIO) and encouraging end-user actions, such as powering off machines when not in use, ensure further reductions in the average cost per user.
Learn how cost reductions are estimated
All Providers
$ 483.1
$ 255.84 pupm reduction
53% reduction
$ 227.25
Cost pupm
All Providers
All Providers + citrix
Cost reductions
Type
Cost Pupm
Compute: Autoscale $233.00
Storage: Autoscale $22.85
Total $255.84
Costs by desktop type
123.49% higher for static desktops
Static
$ 157 pupm
Random
$ 70.25 pupm
$ 157
$ 70.25
Cost pupm
Persistent
Non persistent
Desktop type
Distinct users
Machines
Average monthly uptime
Static Persistent 1 5 43 h 24 min
Random Non persistent 1 5 33 h 24 min
Costs by machine OS type
123.49% higher for single-session OS machines
$ 157
$ 70.25
Cost pupm
Multi-session
Single-session
Machine OS type
Distinct users
Machines
Average monthly uptime
Single-session 1 5 43 h 24 min
Multi-session 1 5 33 h 24 min
Workloads by highest cost pupm
Only showing VM instances from Azure
VM Instance
Distinct users
Machines
Average monthly uptime
Cost pupm
Standard_D2as_v5 1 5 43 h 24 min $157.00
Standard_D2s_v3 1 5 33 h 24 min $70.25

コスト概要ページには、以下が含まれます。

- **ユーザーあたりの平均コスト**

  過去6か月間の月ごとのユーザーあたりの実際のコストと、現在の月の予測コストを表示できます。さらに、ワークロードの総コストとサイト上のユニークユーザー数を確認できます。複数の通貨が関係する場合、USDがそのうちの1つであれば、コストはUSDで表示されます。それ以外の場合は、リストからランダムに選択された通貨でコストが表示されます。先月および先々月と比較したコスト削減額がパーセンテージで表示されます。また、ユニークユーザー数の変化も表示されます。グラフィカル表示では、毎月の傾向が示されます。

  ユーザーあたりの平均コストを使用して、使用状況を最適化できます。

- **コストレポート**

  選択したサービスプロバイダー、選択したデリバリーグループ、および選択したタグのコストレポートを表示できます。過去3か月分のレポートを個別に表示することも、過去3か月分のデータを統合して表示することもできます。

- **Citrix を使用したコスト削減**

  Autoscale や Machine Creation Services™ (MCS)、Storage Optimization (MCSIO) などのCitrix機能を有効にすることで、ユーザーあたりの平均コストをさらに削減できます。また、使用していないときにマシンをシャットダウンするなど、エンドユーザーの行動を促すこともできます。

  このデータは、Citrix 機能が適用された場合の総削減額を表示します。また、エンドユーザーの行動による削減額も表示します。

- **デスクトップタイプ別のコスト**

  次の種類のデスクトップのコストを表示できます。

  - **静的永続:** ユーザーは毎回同じ仮想デスクトップにサインオンし、デスクトップに加えられた変更は保存されます。
  - **静的非永続:** ユーザーは毎回同じ仮想デスクトップにサインオンしますが、デスクトップに加えられた変更は保存されません。
  - **ランダム永続:** ユーザーにはデスクトッププールから仮想デスクトップが割り当てられ、デスクトップに加えられた変更は保存されます。
  - **ランダム非永続型:** ユーザーにはデスクトッププールから仮想デスクトップが割り当てられ、デスクトップに加えられた変更は保存されません。

各マシンタイプについて、個別のユーザー数、マシン数、および月間平均稼働時間を表示できます。

このデータを使用して、ユーザーを異なる種類のデスクトップに移動することでコストを節約する計画を立てることができます。たとえば、静的永続型デスクトップタイプは、ランダム非永続型デスクトップと比較して、より多くのリソース使用量を必要とします。したがって、一部のユーザーを静的永続型デスクトップタイプからランダム非永続型デスクトップタイプに移動する計画を立てることができます。

- **OSタイプ別のコスト**

  シングルセッションおよびマルチセッションOSタイプのコストを表示できます。マシンのOSタイプ、個別のユーザー数、マシン数、および月間平均稼働時間を表示できます。このデータを使用して、ユーザーを異なる種類のOSに移動することでコストを節約する計画を立てることができます。

- **ユーザーあたりの月間最高コストによるワークロード**

  仮想マシンインスタンス、個別のユーザー数、マシンの平均稼働時間など、ユーザーあたりの月間最高コストの詳細を表示できます。また、マシン数とユーザーあたりのコストも確認できます。

  このデータを使用して、各VM構成タイプのコストを表示し、どの構成をユーザーに割り当てるかを決定します。

Azureワークロードのコストモデリング

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

> **注:**
>
> 最適な推定を得るには、過去28日間の安定した環境からのデータを使用することをお勧めします。休暇や急な使用量の急増など、異常なアクティビティ期間のデータは使用しないでください。使用量がベースラインレベルに戻るまで待ってから、これらの推奨事項に従ってください。

利点:

- カスタマイズされたコスト削減の推奨事項を提供します。
- 予約プランとSavings Planの両方をサポートします。
- 正確な洞察のために最近の使用状況データを分析します。
- リソース割り当てを最適化し、費用を削減するのに役立ちます。
- デリバリーグループ、タグ、VMシリーズ、およびリージョンの選択において柔軟性を提供します。

注:

コストモデリングはAzureワークロードのみでサポートされています。

プランの種類

Azureには、コストを節約するための2種類のプランがあります。

- **Azure Reservations**: 顧客は、事前に予約するマシンの数を決定します。予約は、従量課金制のコストと比較して、割引料金で異なる定額コストがかかります。
- **Savings Plan**: 顧客は、マシンの数ではなく、特定の金額をコミットします。その金額が消費されるまでは、割引料金が請求されます。その後は、従量課金制の料金を支払います。

「**コストモデリング**」ページには、各プランの推奨事項が個別に表示され、潜在的な節約額が示されます。

コスト最適化 > コストモデリングをクリックします。「**コストモデルとクラウドワークロード**」ページが表示されます。

citrix | DaaS Premium | 0 - Production

DaaS > Monitor > Cost optimization

Try unified search | Search | 1 - Production

Cost optimization New

Cost summary | Cost savings | Workload rightsizing | Cost modeling

Export data

Cost model cloud workloads

We recommend that you filter only by long-term-use machines and production workloads. Delivery groups and machines used for testing or short-term use may skew the cost model results.

All delivery groups | Select tag | All VM series | All regions

Apply filters | Note: All filters are applied with **AND** operator

Data up to 04/03/2025 9:56 AM | Download report

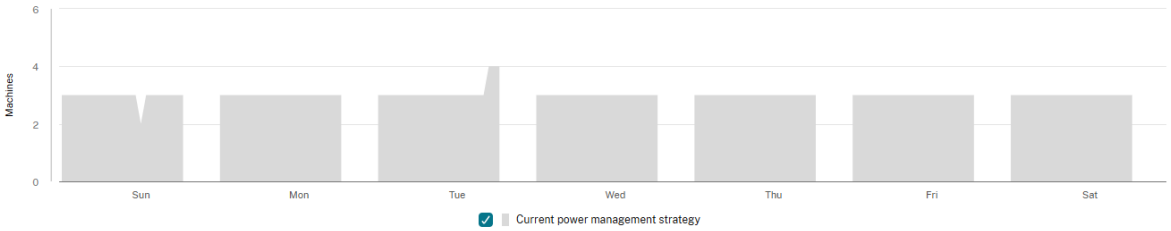
Cost model based on power management strategy

Choose from various Autoscale power management strategies to visualize concurrent machine consumption and savings opportunities.

No changes to Autoscale	Potential changes to Autoscale	
Current power management strategy Analyze potential savings opportunities by utilizing the existing Autoscale configuration.	**Deallocate machines at session end** Analyze potential savings opportunities if Autoscale is configured to deallocate machines at the end of a user's session. **95.45% reduced machine consumption**	**Deallocate machines for inactive session** Analyze potential savings opportunities if Autoscale is configured to deallocate machines when a session is inactive. **99.01% reduced machine consumption**

Concurrent machine consumption

Concurrent machine consumption is analyzed based on the last 28 days of historical consumption.



Savings opportunity

Determine the best commitment strategy and term length based on the selected power management strategy. View cost analysis

	Reserved instances		Savings plan	
	1 year	3 year	1 year	3 year
Potential savings opportunity	**40 %** Save up to $2,717.07 / yr	**61 %** Save up to $4,142.95 / yr	**31 %** Save up to $2,074.39 / yr	**53 %** Save up to $3,570.76 / yr
Commitment	$3,978.07 / yr	$2,552.20 / yr	$4,620.75 / yr	$3,124.39 / yr
Pay as you go	$72.58 / yr	$72.58 / yr	$72.58 / yr	$72.58 / yr
Total	**$4,050.65 / yr**	**$2,624.78 / yr**	**$4,693.33 / yr**	**$3,196.97 / yr**

Recommendations

Review the recommended changes to your commitment strategy based on the term length.

			Machines to be reserved		Savings plan hourly commitment (USD)	
Virtual machine series	Region	Current machines	1 year	3 year	1 year	3 year
Standard_D4s_v3	eastus	727	2	2	$0.26 / hr	$0.18 / hr
Standard_D8as_v4	eastus	21	1	1	$0.26 / hr	$0.18 / hr

Analyze per virtual machine series

Validate the optimum number of machines required per series by correlating with respective cost per user.

Virtual machine series

Standard_D4s_v3 in eastus

Export analysis



必要に応じて、すべてのデリバリーグループ、最大15個（または実際の数）のデリバリーグループを選択し、最大15個（または実際の数）のデリバリーグループを除外できます。ドロップダウンリストから**すべてのシングルセッション**または**すべてのマルチセッション**を選択できます。また、**タグ**、**VMシリーズ**、**リージョン**でフィルタリングすることもできます。オプションを選択しない場合、分析はデフォルトで適用可能なデータセット全体に対して実行され、過去28日間のデータが考慮されます。

> **注:**
>
> コストモデリングの推奨事項は、過去28日間のデータに基づいており、この期間中の動作が一貫していることを前提としています。

電源管理戦略

データ分析は、選択した電源管理戦略によって異なります。同時実行マシンの消費量と節約の機会を視覚化するために、次のAutoscale™電源管理戦略のいずれかを選択できます。

- **現在の電源管理戦略**: 既存のAutoscale構成を使用して潜在的な節約を分析するには、この戦略を選択します。Autoscale構成に変更はありません。推奨されるコストモデリングは、現在のAutoscale設定に基づいて生成され、稼働中のすべてのマシンのコストを計算します。
- **セッション終了時にマシンの割り当てを解除**: ユーザーセッションの終了時にマシンの割り当てを解除するようにAutoscale構成を変更して潜在的な節約を分析する場合は、この戦略を選択します。推奨されるコストモデリングは、更新されたAutoscale構成に基づいて生成され、アクティブなセッション時間のみのコストを計算し、切断時間は無視します。
- **非アクティブセッションのマシンの割り当てを解除**: セッションが非アクティブなときにマシンの割り当てを解除するようにAutoscale構成を変更して潜在的な節約を分析する場合は、この戦略を選択します。推奨されるコストモデリングは、更新されたAutoscale構成に基づいて生成され、セッションがアクティブでアイドル状態ではない時間のみのコストを計算します。

たとえば、マシンが60分間稼働し、セッションが20分間切断された場合、残りの40分がアクティブセッション時間です。アクティブセッション中にユーザーが10分間アイドル状態だった場合、正味使用時間は30分のみです。

- **現在の電源管理戦略**では、正味使用時間は60分です。
- 「**セッション終了時にマシンを割り当て解除する戦略**」では、切断時間を除いた正味使用量は40分です。

- 「**非アクティブセッションのマシンを割り当て解除する戦略**」では、アイドル時間を含めた正味使用量は30分です。

これらの基準は分析のベースラインとして機能します。これらの戦略は、マシンの正味使用量をより正確に判断するのに役立ちます。

マシンの消費と推奨事項

「**コストモデリング**」ページには、マシンの消費と推奨事項に関する以下の詳細が記載されています。

- **同時マシン消費グラフ**: このグラフは、過去28日間のベースライン使用量を表示し、各バーは週の1日を表します。ベースラインは、平均または中央値と同様の集計メトリックである使用量の75パーセンタイル (p75) を使用して計算されます。たとえば、火曜日の午前10時など、各曜日と時間について、ベースラインは過去4回の火曜日の午前10時のデータのp75を分析することによって決定されます。このプロセスは、週のすべての時間と曜日について繰り返されます。グラフにカーソルを合わせると、現在の電源管理戦略と、Autoscaleへの潜在的な変更が適用された場合の選択された戦略の下で消費されたマシンの数を確認できます。
- **節約の機会**: Azure ReservationsとSavings Plansの両方について、1年間および3年間の潜在的な節約の機会を表示します。「**コミットメント**」と「**従量課金制**」オプションの節約の機会が表示されます。
- **推奨事項**: Azure ReservationsとSavings Plansの両方に対する推奨される変更を表示します。推奨事項には、仮想マシンシリーズ、タイプ、およびリージョンのすべての該当する組み合わせに対する各プランのコミットメントが含まれます。データは1年間および3年間の期間で利用できます。

仮想マシンシリーズごとの分析

ドロップダウンリストから仮想マシンシリーズを選択して、ユーザーあたりのコストに関して最適なマシン数を検証します。月あたりのユーザーあたりのコストは、予測される月あたりのユーザーあたりのコストの見積もりです。この見積もりは、お客様がAzure Reservationsで特定の数のマシンを予約した場合、または「**Savings Plan**」で特定の時間あたりのドル額をコミットした場合の、予測される月あたりのユーザーあたりのコストを理解するのに役立ちます。Azure Reserved InstancesとSavings Planの時間あたりのコミットメントのユーザーあたりのコストを表示します。グラフには、さまざまな予約レベル（「**予約なし**」から「**完全予約**」まで、「**最適な予約**」を含む）と時間あたりのコストコミットメントレベル（「**コミットメントなし**」から「**最大コミットメント**」まで、「**最適なコミットメント**」を含む）のデータポイントが表示されます。

「**コストモデリング**」ページは、お客様がAzureワークロードを最適化し、コストを節約するのに役立つ貴重な洞察と推奨事項を提供します。使用パターンを分析し、適切なプランを選択することで、お客様は大幅な節約を実現できます。

機能互換性マトリックス

Citrix Director 7 2503 は以下と互換性があります:

- Citrix Virtual AppsおよびDesktops™ 7 2112 以降
- シトリックス バーチャル アプリケーションズ アンド デスクトップス™ 7 1912 LTSR

各サイト内で、Director を以前のバージョンの Delivery Controller™ とともに使用することはできますが、Director の最新バージョンのすべての機能が利用できるとは限りません。Citrix は、Director、Delivery Controller、および VDA を同じバージョンにすることを推奨しています。

注:

Delivery Controller をアップグレードした後、Studio を開くとサイトのアップグレードを促されます。詳細については、展開のアップグレード の「**アップグレードシーケンス**」セクションを参照してください。

Director のアップグレード後に初めてログインすると、構成済みのサイトでバージョンチェックが実行されます。いずれかのサイトが Director より古いバージョンの Controller を実行している場合、Director コンソールにサイトのアップグレードを推奨するメッセージが表示されます。さらに、サイトのバージョンが Director より古い間は、この不一致を示すメモが Director ダッシュボードに表示され続けます。

注:

以前のバージョンの Citrix Director では、最近の VDA バージョンで実行されているユーザーセッションに適用されたポリシーは表示されません。Citrix Director 1912 およびそれ以前のバージョンでは、VDA バージョン 2003 以降で実行されているユーザーセッションに適用されたポリシーは表示されません。これらのポリシーを表示するには、Citrix Director バージョン 2003 以降を使用してください。

Director の特定の機能と、必要な Delivery Controller (DC)、VDA、その他の依存コンポーネントの最小バージョン、およびライセンスエディションを以下に示します。

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
2507	監視とトラブルシューティングのための Microsoft 通話品質ダッシュボード	なし	すべて
2507	垂直および水平ロードバランシングアラートの処理の改善	なし	すべて
2507	セッション トポロジで使用されるエンドポイント データ収集のデフォルト ポリシー動作の変更	なし	すべて
2507	DirectorにおけるICA RTTおよびネットワーク遅延測定の強化された定義(/ja-jp/citrix-virtual-apps-desktops/current-release/director/troubleshoot-deployments/user-issues/session-performance.html#hdx-metrics)	なし	すべて
2507	リアルタイム通信アプリケーション向けのプラグインマネージャーと最適化状態の視認性の向上(/ja-jp/citrix-virtual-apps-desktops/current-release/director/troubleshoot-	なし	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
	deployments/user-issues/session-performance.html#real-time-communications-optimization-visibility)		
2503	Azureワークロードのコストモデリング	なし	すべて
2503	コスト削減ページへの機能強化(/ja-jp/citrix-virtual-apps-desktops/current-release/director/cost-optimization/cost-savings.html)	なし	すべて
2503	uberAgentとのDirector統合(/ja-jp/citrix-virtual-apps-desktops/current-release/director/install-and-configure.html#citrix-uberagent-integration-with-director)	VDA 2503 (uberAgentがインストール済み)	すべて
2503	ローカルアプリケーション使用状況レポート(/ja-jp/citrix-virtual-apps-desktops/current-release/director/site-analytics/application-usage-monitoring.html)	VDA 2503	Platinumライセンスサイト

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
2503	VDAログオン期間の詳細の監視	VDA 2503	すべて
2503	Provisioning Service向けの追加のメトリック収集(/ja-jp/citrix-virtual-apps-desktops/current-release/director/infrastructure-monitoring/infrastructure-dashboard.html#provisioning-service-health-metrics)	VDA 2503	すべて
2503	Microsoft Teams以外のHDX最適化の監視を拡張するオプション	VDA 2503	すべて
2503	フィルタービューおよびセッションパフォーマンスタブでのセッション自動再接続の詳細(/ja-jp/citrix-virtual-apps-desktops/current-release/director/site-analytics/trends.html)	VDA 2503	すべて
2503	Citrix Director向けの統合されたプラットフォームエクスペリエンス	なし	すべて
2503	ユーザーアクションの一括操作オプションを制限するカスタムロール(/ja-jp/citrix-	なし	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
	virtual-apps-desktops/current-release/director/troubleshoot-deployments/user-issues/custom-role-to-limit-bulk-action.html)		
2503	Provisioning ServiceおよびDelivery Controller向けにサイトレベルのアラートを設定する機能(/ja-jp/citrix-virtual-apps-desktops/current-release/director/site-analytics/alerts-notifications.html#alerts-for-infrastructure-monitoring)	VDA 2503	すべて
2503	Webhookとの統合(/ja-jp/citrix-virtual-apps-desktops/current-release/director/integrations-and-data-exports.html#integrations-with-alerting-and-itsm-tools)	なし	すべて
2411	アプリケーションページでの、最も使用されていない公開済みアプリと未使用の公開済みアプリのレポート(/ja-jp/citrix-virtual-apps-desktops/current-	DDC 7.16、VDA 7.15	Platinumライセンスサイト

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
	release/director/site-analytics/application-usage-monitoring.html#least-used-and-unused-published-apps-report)		
2411	PowerShell SDK を使用した Webhook 構成	VDA 2411および DDC 2411	すべて
2411	一括アラート解除	VDA 2411および DDC 2411	すべて
2411	ワークロードの適正化ページでのマシンの正味アクティブ使用量(/ja-jp/citrix-virtual-apps-desktops/current-release/director/cost-optimization/workload-rightsizing.html)	なし	すべて
2411	ストレージ使用量を最適化することによるコスト削減 (プレビュー)(/ja-jp/citrix-virtual-apps-desktops/current-release/director/cost-optimization/cost-savings.html)	なし	すべて
2411	コストの概要 (プレビュー)(/ja-jp/citrix-virtual-apps-desktops/current-release/director/cost-	なし	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
	optimization/cost-summary.html)		
2411	Delivery Controllerの監視 (プレビュー)(/ja-jp/citrix-virtual-apps-desktops/current-release/director/infrastructure-monitoring/infrastructure-dashboard.html#delivery-controller-health-metrics)	VDA 2411	すべて
2411	UIからのCitrixコンポーネントの接続 (プレビュー)(/ja-jp/citrix-virtual-apps-desktops/current-release/director/infrastructure-monitoring/manage-connections.html)	VDA 2411	すべて
2407	コスト最適化	なし	すべて
2407	統合とデータのエクスポート	VDA 2407	すべて
2407	過去のユーザーセッションの診断（プレビュー）	VDA 2407	すべて
2407	Secure Private Accessセッション用アクティビティマネージャー (プレビュー)	VDA 2407	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
2407	DirectorとのTCPおよびUDPアプリ向けSecure Private Access統合 (プレビュー)	VDA 2407	すべて
2407	インフラストラクチャ監視 (プレビュー)	VDA 2407	すべて
2407	未登録マシンアラート(/ja-jp/citrix-virtual-apps-desktops/current-release/director/site-analytics/alerts-notifications.html#unregistered-machines-in-)	VDA 2407およびDDC 2407	すべて
2407	マシンの稼働時間アラート	VDA 2407およびDDC 2407	すべて
2407	電源オンアクションの失敗および電源オフアクションの失敗アラート	VDA 2407およびDDC 2407	すべて
2407	アラートメールにCSV添付ファイルを含め、アラートWebhookにJSONペイロードを含める機能(/ja-jp/citrix-virtual-apps-desktops/current-release/director/site-analytics/alerts-notifications.html#en	VDA 2407およびDDC 2407	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
	hancements-on-alert-content)		
2407	最近の電源操作があるマシンを検査	VDA 2407	すべて
2407	高度なアラートポリシー(/ja-jp/citrix-virtual-apps-desktops/current-release/director/site-analytics/alerts-notifications.html#advanced-alert-policies)	VDA 2407およびDDC 2407	すべて
2407	クラウドおよびオンプレミスユーザー向け統合検索(/ja-jp/citrix-virtual-apps-desktops/current-release/director/unified-search.html)	DDC 2407	すべて
2407	ダッシュボード上の公開アプリケーション使用状況監視チャート	VDA 2407およびDDC 2407	Platinumライセンスサイト
2402 LTSR	DirectorによるWebおよびSaaSアプリのSecure Private Access統合（プレビュー）	VDA 2402 LTSR	すべて
2402 LTSR	Microsoft Teamsバージョン2.1以前のサポート](/ja-jp/citrix-virtual-apps-desktops/current-release/director/	VDA 2402 LTSR	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
	troubleshoot-deployments/user-issues.html#microsoft-teams-optimization-status)		
2311	ライブおよび録画セッションの再生	VDA 2308 および DDC 2311	すべて
2311	セッショントポロジとパフォーマンスメトリック	複数バージョン - リンク	すべて
2311	最適な画面解像度	なし	すべて
2311	MS Teams の最適化	VDA 2311 および DDC 最新版	すべて
2311	プローブの概要の機能強化	なし	すべて
2311	刷新されたセッションログオン期間ビュー	なし	すべて
2308	「プローブの概要とドリルダウン」(/ja-jp/citrix-virtual-apps-desktops/current-release/director/probes.html#step-4-view-probe-results)	なし	すべて
2308	「Citrix Gateway 多要素認証の Citrix Probe Agent サポート」(/ja-jp/citrix-virtual-apps-desktops/current-release/director/probes.html#step-1-	シトリックス ゲートウェイ	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
	install-and-configure-the-citrix-probe-agent)		
2308	「ハイパーバイザーアラートの無効化」(/ja-jp/citrix-virtual-apps-desktops/current-release/director/site-analytics/alerts-notifications.html#hypervisor-alerts-monitoring)	なし	すべて
2308	「セッションエクスペリエンスメトリックの傾向」(/ja-jp/citrix-virtual-apps-desktops/current-release/director/troubleshoot-deployments/user-issues.html#trends-for-session-performance-metrics)	なし	すべて
2305	「Citrix Gateway を介した認証のサポート」(/ja-jp/citrix-virtual-apps-desktops/current-release/director/probes.html)	なし	すべて
2305	「Director での Autoscale 管理」(/ja-jp/citrix-virtual-apps-desktops/current-release/director/site-	なし	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
	analytics/autoscale-managed-machines.html)		
2303	失敗したマシンアラート(/ja-jp/citrix-virtual-apps-desktops/current-release/director/site-analytics/alerts-notifications.html#failed-machines-in-)	DC 7 2303	プレミアム
2203	TLS 1.3 のサポート	-	すべて
2212	AMD GPUでリアルタイムGPU使用率が利用可能	64ビットWindowsおよびHDX 3D Proが有効なDC 7.14およびVDA 7.14	すべて
2212	高度なプローブスケジューリング(/ja-jp/citrix-virtual-apps-desktops/current-release/director/probes.html)	DC 7 1906 と シトリックス プローブ エージェント 2209	プレミアム
1909	Citrix Analytics for Performance を使用してオンプレミスサイトを構成する(/ja-jp/citrix-virtual-apps-desktops/current-release/director/install-and-configure/onboarding.html)	DC 7 1906およびVDA 1906	すべて
1906	セッションの自動再接続	DC 7 1906およびVDA 1906	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
1906	セッション起動時間	DC 7 1906およびVDA 1903	すべて
1906	デスクトッププロービング	DC 7 1906 と シトリックス プローブ エージェント 1903	プレミアム
7.9以降	プロファイルロードにおけるCitrix Profile Managementの期間	VDA 1903	すべて
1811	プロファイルドリルダウン	DC 7 1811およびVDA 1811	すべて
1811	ハイパーバイザーアラート監視	DC 7 1811	プレミアム
1811	アプリケーションプロービング	DC 7 1811 および Citrix アプリケーション プローブ エージェント 1811	プレミアム
1811	Microsoft RDS ライセンスの健全性	DC 7 1811 および VDA 7.16	すべて
1811	主要なRTOPデータ表示	DC 7 1811 および VDA 1808	プレミアム
1808	フィルターデータの書き出し	DC 7 1808	すべて
1808	インタラクティブセッションのドリルダウン	DC 7 1808およびVDA 1808	すべて
1808	GPOのドリルダウン	DC 7 1808およびVDA 1808	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
1808	OData APIを使用したマシンの履歴データ利用可能	DC 7 1808	すべて
7.18	アプリケーションプロービング	DC 7.18	プレミアム (旧 Platinum)
7.18	スマートアラートポリシー	DC 7.18	プレミアム (旧 Platinum)
7.18	Health Assistant リンク	なし	すべて
7.18	インタラクティブセッションのドリルダウン	なし	すべて
7.17	PIV スマートカード認証	なし	すべて
7.16	アプリケーション分析	DC 7.16およびVDA 7.15	すべて
7.16	OData API バージョン4	DC 7.16	すべて
7.16	Shadow Linux VDA ユーザー	VDA 7.16	すべて
7.16	ドメインローカルグループのサポート	なし	すべて
7.16	マシンコンソールアクセス	DC 7.16	すべて
7.15	アプリケーション障害監視	DC 7.15およびVDA 7.15	すべて
7.14	アプリケーション中心のトラブルシューティング	DC 7.13およびVDA 7.13	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
7.14	ディスク監視	DC 7.14およびVDA 7.14	すべて
7.14	GPU監視	DC 7.14およびVDA 7.14	すべて
7.13	セッション詳細パネルのトランスポートプロトコル	DC 7.x および VDA 7.13	すべて
7.12	ユーザーフレンドリーな接続およびマシン障害の説明	DC 7.12 および VDA 7.x	すべて
7.12	Enterpriseエディションでの履歴データ可用性の向上	DC 7.12 および VDA 7.x	エンタープライズ
7.12	カスタムレポート	DC 7.12 および VDA 7.x	プレミアム (旧 Platinum)
7.11	リソース使用率レポート	DC 7.11およびVDA 7.11	すべて
7.11	CPU、メモリ、ICA RTT条件に対するアラート機能の拡張	DC 7.11およびVDA 7.11	プレミアム (旧 Platinum)
7.11	レポートのエクスポート機能の改善	DC 7.11およびVDA 7.x	すべて
7.11	Citrix ADMとの統合	DC 7.11、VDA 7.x、およびMASバージョン11.1ビルド49.16	プレミアム (旧 Platinum)
7.9	ログオン期間の内訳	DC 7.9 および VDA 7.x	すべて
7.7	プロアクティブな監視とアラート	DC 7.7 および VDA 7.x	プレミアム (旧 Platinum)

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
7.7	Windows認証統合	DC 7.x および VDA 7.x	すべて
7.7	シングルセッションおよびマルチセッションOSの使用状況	DC 7.7 および VDA 7.x	プレミアム (旧 Platinum)
7.6.300	Framehawk仮想チャネルのサポート(/ja-jp/citrix-virtual-apps-desktops/current-release/director/troubleshoot-deployments/user-issues/hdx-channel-reports.html)	DC 7.6 および VDA 7.6	すべて
7.6.200	セッション記録の統合(/ja-jp/citrix-virtual-apps-desktops/current-release/director/troubleshoot-deployments/user-issues/record-sessions.html)	DC 7.6 および VDA 7.x	プレミアム (旧 Platinum)
7	HDX Insightの統合(/ja-jp/citrix-virtual-apps-desktops/current-release/director/install-and-configure/hdx-insight.html)	DC 7.6、VDA 7.x、およびCitrix ADM	プレミアム (旧 Platinum)

データ粒度と保持

データ値の集計

Monitor Serviceは、ユーザーセッションの使用状況、ユーザーログオンパフォーマンスの詳細、セッション負荷分散の詳細、接続およびマシン障害情報など、さまざまなデータを収集します。データはカテゴリに応じて異なる方法で集計されます。OData Method APIを使用して提示されるデータ値の集計を理解することは、データを解釈するために不可欠です。例:

- 接続されたセッションとマシン障害は一定期間に発生します。したがって、それらは期間中の最大値として公開されます。
- ログオン期間は時間の長さを測定するものであるため、期間中の平均値として公開されます。
- ログオン数と接続障害は一定期間に発生した回数であるため、期間中の合計値として公開されます。

同時データ評価

セッションは、同時と見なされるためには重複している必要があります。ただし、時間間隔が1分の場合、その1分間のすべてのセッション（重複しているかどうかにかかわらず）は同時と見なされます。間隔のサイズが非常に小さいため、精度を計算するのに伴うパフォーマンスオーバーヘッドは、追加される価値に見合いません。セッションが同じ時間内に発生しても、同じ分内に発生しない場合、それらは重複しているとは見なされません。

サマリーテーブルと生データの相関

データモデルは、メトリックを2つの異なる方法で表します。

- サマリーテーブルは、分、時間、日ごとの時間粒度でメトリックの集計ビューを表します。
- 生データは、セッション、接続、アプリケーション、およびその他のオブジェクトで追跡される個々のイベントまたは現在の状態を表します。

API呼び出し間またはデータモデル自体内でデータを相関させようとするときは、以下の概念と制限を理解することが重要です。

- **部分的な間隔のサマリーデータはありません。** メトリックのサマリーは、長期間にわたる履歴トレンドのニーズを満たすように設計されています。これらのメトリックは、完全な間隔でサマリーテーブルに集計されます。データ収集の開始時（利用可能な最も古いデータ）または終了時の部分的な間隔には、サマリーデータはありません。1日の集計（Interval=1440）を表示する場合、これは最初と最新の不完全な日にはデータがないことを意味します。これらの部分的な間隔には生データが存在する可能性がありますが、それは決して要約されません。特定

のデータ粒度について、特定のサマリーテーブルから最小および最大のSummaryDateを抽出することで、最も早い集計間隔と最も遅い集計間隔を決定できます。SummaryDate列は間隔の開始を表します。Granularity列は、集計データの期間の長さを表します。

- **時間による相関。** メトリックは、前述のセクションで説明されているように、完全な間隔でサマリーテーブルに集計されます。これらは履歴トレンドに使用できますが、生イベントはトレンド分析のために要約されたものよりも現在の状態をより正確に反映している可能性があります。サマリーと生データの時間ベースの比較では、発生する可能性のある部分的な間隔、または期間の開始と終了にはサマリーデータがないことを考慮する必要があります。
- **見逃されたイベントと潜在的なイベント。** 集計テーブルに集計されるメトリックは、イベントが見逃されたり、集計期間に対して潜在的であったりする場合、わずかに不正確になる可能性があります。モニターサービスは正確な現在の状態を維持しようとしますが、見逃されたイベントや潜在的なイベントのために、集計テーブルの集計を再計算するために過去に遡ることはありません。
- **接続の高可用性。** 接続の高可用性中、現在の接続のサマリーデータカウントにギャップが生じますが、セッションインスタンスは引き続き生データで実行されます。
- **データ保持期間。** サマリーテーブルのデータは、生イベントデータのスケジュールとは異なるグルーミングスケジュールで保持されます。サマリーテーブルまたは生テーブルからグルーミングによってデータが削除されたため、データが欠落している可能性があります。保持期間は、サマリーデータの異なる粒度によっても異なる場合があります。粒度の低いデータ（分単位）は、粒度の高いデータ（日単位）よりも早くグルーミングされます。グルーミングによってある粒度からデータが欠落している場合でも、より高い粒度で見つかる可能性があります。API呼び出しは要求された特定の粒度のみを返すため、ある粒度でデータが受信されないからといって、同じ期間のより高い粒度でデータが存在しないという意味ではありません。
- **タイムゾーン。** メトリックはUTCタイムスタンプで保存されます。サマリーテーブルは、時間単位のタイムゾーン境界で集計されます。時間単位の境界に該当しないタイムゾーンの場合、データが集計される場所に関して多少の不一致が生じる可能性があります。

粒度と保持

Directorによって取得される集計データの粒度は、要求された時間 (T) スパンの関数です。ルールは次のとおりです。

- 0 \< T \<= 1時間 - 分単位の粒度を使用
- 0 \< T \<= 30日 - 時間単位の粒度を使用
- T \> 31日 - 日単位の粒度を使用

集計データから取得されない要求データは、生のセッションおよび接続情報から取得されます。このデータは急速に増加する傾向があるため、独自のグルーミング設定があります。グルーミングは、関連データのみが長期的に保持されることを保証します。グルーミングは、レポートに必要な粒度を維持しながら、より良いパフォーマンスを保証します。Premiumライセンスサイトのお客様は、グルーミング保持を希望する保持日数に変更できます。変更しない場合はデフォルトが使用されます。サイトデータベースとの接続が失われた場合、モニターサービスは以下の表で指定されているPremiumエンタイトルメントのデフォルトの保持日数を使用します。

設定にアクセスするには、Delivery Controller™ で次のPowerShellコマンドを実行します。

```
asnp Citrix.*

 Get-MonitorConfiguration

 Set-MonitorConfiguration -<setting name> <value>
```

#	設定名	影響を受けるスキーマテーブル	モニターページで影響を受けるテーブルとグラフ	PREMIUMの保持日数	ADVANCEDの保持日数
1	GroomSessionsRetentionDays	MonitorData.Session および Monitordata.Connection テーブル	この設定は、トレンドページのセッションの詳細、ユーザーセッションごとのログオン期間、アプリケーションベースの使用状況テーブルに影響します。	90	31
2	GroomFailuresRetentionDays	MonitorData.MachineFailureLog および MonitorData	トレンドページ：この設定は、障害タブのグラフと	90	31

#	設定名	影響を受けるスキーマテーブル	モニターページで影響を受けるテーブルとグラフ	PREMIUMの保持日数	ADVANCEDの保持日数
		.ConnectionFailureLog	テーブルに影響します。		
3	GroomLoadIndexesRetentionDays	MonitorData.LoadIndex	この設定は、トレンドページの「ロードエバリュエーターインデックス」タブに表示されるデータに影響します。	3	3
4	GroomDeletedRetentionDays	LifecycleStateが「Deleted」であるMonitorData.Machine、MonitorData.Catalog、MonitorData.DesktopGroup、およびMonitorData.Hypervisorエンティティ。この設定は、関連するSession、SessionDetail、Summary、Failure、または	LifecycleStateが「Deleted」であるMachine、Catalog、DesktopGroup、およびHypervisorエンティティ。この設定は、関連するSession、SessionDetail、Summary、Failure、またはLoadIndexレコードも	90	31

#	設定名	影響を受けるスキーマテーブル	モニターページで影響を受けるテーブルとグラフ	PREMIUMの保持日数	ADVANCEDの保持日数
		LoadIndexレコードも削除します。	削除します。		
5	GroomSummariesRetentionDays	MonitorData.DesktopGroupSummary、MonitorData.FailureLogSummary、およびMonitorData.LoadIndexSummary	この設定は、トレンドページ上のすべてのグラフデータに影響します。	365	31
6	GroomMachineHotfixLogRetentionDays	MonitorData.Hotfix	この設定は、マシン詳細ページに表示されるVDAホットフィックスデータに影響します。	90	31
7	GroomMinuteRetentionDays	すべてのサマリーテーブル	この設定は、トレンドページに表示される「過去2時間」の時間期間のグラフに影響します。	3	3

#	設定名	影響を受けるスキーマテーブル	モニターページで影響を受けるテーブルとグラフ	PREMIUMの保持日数	ADVANCEDの保持日数
8	GroomHourlyRetentionDays	すべてのサマリーテーブル	これは、トレンドページに表示される週次グラフに影響します。	32	31
9	GroomApplicationInstanceRetentionDays	MonitorData.ApplicationInstance	この設定は、キャパシティ管理タブのグラフとテーブル、およびトレンドページのアプリケーション使用状況テーブルに影響します。	90	該当なし
10	GroomNotificationLogRetentionDays	MonitorData.NotificationLog	この設定は、Monitorに表示されるアラートに影響します。	90	該当なし
11	GroomResourceUsageRawDataRetentionDays	MonitorData.Resourceutilization	この設定は、「履歴マシン使用率」のマシン詳細ページに表示される CPU およびメモリのグラフと、コスト	3	3

#	設定名	影響を受けるスキーマテーブル	モニターページで影響を受けるテーブルとグラフ	PREMIUMの保持日数	ADVANCEDの保持日数
			最適化領域の「ワークロードの適正化」タブでのデータ計算に影響します。		
12	GroomResourceUsageMinuteDataRetentionDays	MonitorData.ResourceUtilizationSummary	この設定は、「履歴マシン使用率」のマシン詳細ページに表示される「過去 2 時間」の期間の CPU およびメモリのグラフと、コスト最適化領域の「ワークロードの適正化」タブでのデータ計算に影響します。	7	7
13	GroomResourceUsageHourDataRetentionDays	MonitorData.Resourceutilizationsummary	この設定は、「履歴マシン使用率」のマシン詳細ページに表示されるCPUとメモリのグラフ、およびコスト最適化領域の	30	30

#	設定名	影響を受けるスキーマテーブル	モニターページで影響を受けるテーブルとグラフ	PREMIUMの保持日数	ADVANCEDの保持日数
			「ワークロード適正化タブ」でのデータ計算に影響します。		
14	GroomResourceUsageDayDataRetentionDays	MonitorData.Resourceutilizationsummary	この設定は、トレンドページの「リソース使用率」のマシンに表示されるCPUとメモリのグラフ、および特定の「マシン使用率」ページに影響します。	365	31
15	GroomProcessUsageRawDataRetentionDays	MonitorData.ProcessUtilization	この設定は、マシンの履歴使用状況ページに表示されるプロセスごとのリソース傾向情報に影響します。	1	1
16	GroomProcessUsageMinuteDataRetentionDays	MonitorData.ProcessUtilizationMinuteSummary	この設定は、履歴マシン使用率ページに表示される	3	3

#	設定名	影響を受けるスキーマテーブル	モニターページで影響を受けるテーブルとグラフ	PREMIUMの保持日数	ADVANCEDの保持日数
			「過去2時間」のプロセスごとのCPUとメモリ使用量グラフに影響します。		
17	GroomProcessUsageHourDataRetentionDays	MonitorData.ProcessUtilizationHourSummary	この設定は、マシンの履歴使用状況ページに表示されるプロセスごとのCPUおよびメモリ使用量の傾向に影響します。	7	7
18	GroomProcessUsageDayDataRetentionDays	MonitorData.ProcessUtilizationDaySummary	この設定は、マシンの履歴使用状況ページに表示されるプロセスごとのCPUおよびメモリ使用量の傾向に影響します。	30	30
19	GroomSessionMetricsDataRetentionDays	MonitorData.Sessionmetrics	この設定は、ユーザー詳細ページの「セッションパフォーマンス」タ		

#	設定名	影響を受けるスキーマテーブル	モニターページで影響を受けるテーブルとグラフ	PREMIUMの保持日数	ADVANCEDの保持日数
			ブに表示されるすべてのグラフに影響します。		
20	GroomMachineMetricDataRetentionDays	MonitorData.Machinemetrics	この設定は、トレンドページの「リソース使用率」タブにあるグラフとテーブルに影響します。	3	3
21	GroomMachineMetricDaySummaryDataRetentionDays	MonitorData.MachineMetricDaySummary	この設定は、トレンドページの「リソース使用率」タブにあるグラフと表に影響します。	365	31
22	GroomApplicationErrorsRetentionDays	MonitorData.ApplicationError	この設定は、アプリケーションページの「アプリケーションエラー」列に表示されるエラー詳細に影響します。	1	1

#	設定名	影響を受けるスキーマテーブル	モニターページで影響を受けるテーブルとグラフ	PREMIUMの保持日数	ADVANCEDの保持日数
23	GroomApplicationFaultsRetentionDays	MonitorData.Applicationfailure	この設定は、アプリケーションページの「アプリケーション障害」列に影響します。	1	1

注意:

Monitor Serviceデータベースの値を変更した場合、新しい値を有効にするにはサービスを再起動する必要があります。Monitor Serviceデータベースへの変更は、Citrixサポートの指示の下でのみ行うことをお勧めします。

設定GroomProcessUsageRawDataRetentionDays、GroomResourceUsageRawDataRetentionDays、およびGroomSessionMetricsDataRetentionDaysはデフォルト値の1に制限されており、GroomProcessUsageMinuteDataRetentionDaysはデフォルト値の3に制限されています。プロセス使用状況データは急速に増加する傾向があるため、これらの値を設定するPowerShellコマンドは無効になっています。 また、ライセンスベースの保持設定は次のとおりです。

- **Premiumライセンスサイト -** すべての設定のグルーミング保持期間は1000日（Citrixは365日を推奨）に制限されています。
- **Advancedライセンスサイト -** すべての設定のグルーミング保持期間は31日に制限されています。
- **その他のすべてのサイト -** すべての設定のグルーミング保持期間は7日に制限されています。

例外:

- GroomApplicationInstanceRetentionDays は、Premiumライセンスサイトでのみ設定できます。

- GroomApplicationErrorsRetentionDays および GroomApplicationFaultsRetentionDays は、Premiumライセンスサイトでは31日間に制限されます。

長期間データを保持すると、テーブルサイズに以下の影響があります:

- **時間単位のデータ。** 時間単位のデータが最大2年間データベースに残ることを許可すると、1000のデリバリーグループを持つサイトでは、データベースが次のように増加する可能性があります:

  1000のデリバリーグループ x 24時間/日 x 365日/年 x 2年 = 17,520,000行のデータ。集計テーブル内のこれほど大量のデータがパフォーマンスに与える影響は甚大です。ダッシュボードデータはこのテーブルから取得されるため、データベースサーバーへの要件は大きくなる可能性があります。過度に大量のデータは、パフォーマンスに劇的な影響を与える可能性があります。

- **セッションおよびイベントデータ。** セッションが開始され、接続/再接続が行われるたびに収集されるデータです。大規模なサイト（10万ユーザー）の場合、このデータは急速に増加します。たとえば、これらのテーブルの2年分のデータは1TBを超えるデータとなり、ハイエンドのエンタープライズレベルのデータベースが必要になります。

統合とデータのエクスポート

Citrix Director は、統合とデータエクスポートのための新しいUIを提供するようになりました。この機能は、Citrix Directorで利用可能なさまざまなインターフェイスとサードパーティ統合の認識を高めるのに役立ちます。新しく導入された**統合とデータエクスポート**ページには、以下がリストされています。

- 利用可能な統合
- サポートされている開発者ツール

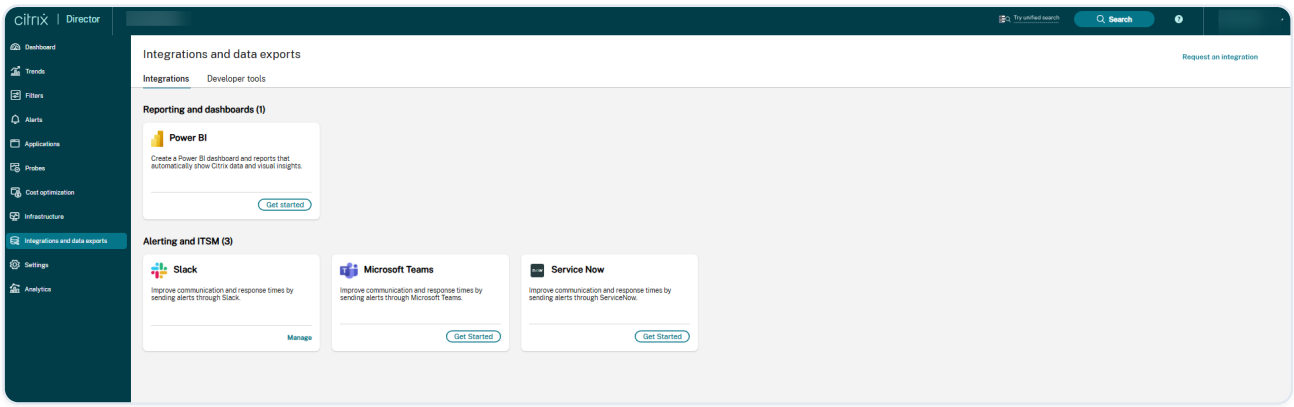
このページでは、データのエクスポートのための REST API の設定についても説明しています。また、統合と開発者ツールの使用を開始するためのガイドとドキュメントへの参照リンクも提供しています。

Citrix 監視メトリックを収集するために、次の統合オプションが提供されています。

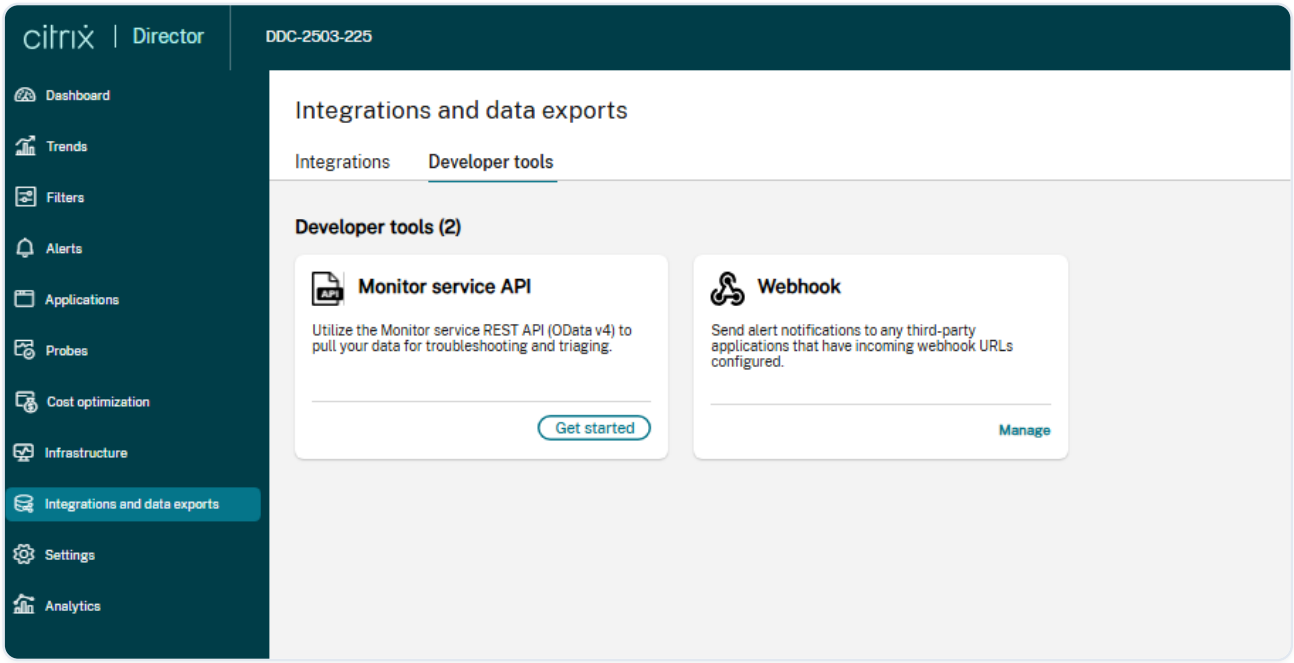
- Citrix Monitor Service API - Citrix Monitor サービス API を使用して、Citrix Monitor からパフォーマンスデータとイベントを収集し、Power BI にエクスポートできます。
- アラートと ITSM - 受信 Webhook URL が構成されている次のサードパーティアプリケーションにアラート通知を送信できます。

- スラック
- マイクロソフト Teams
- ServiceNow

左側のナビゲーションメニューから をクリックします。 ページが表示されます。



開発者ツール:



利用可能な統合を表示

統合タブには、Citrix Directorで利用可能な統合が表示されます。利用可能な統合は、以下のように分類されます。

- レポートとダッシュボード
- アラートとITSM

レポートとダッシュボード

Power BIは、Citrix Director APIを通じて収集されたメトリックを視覚化するために使用できます。**開始**をクリックします。**REST API**開発者ツール詳細ページが表示されます。

Monitor サービス API をクリックすると、PowerBI との統合に関するリソースやブログへの参照リンクが表示されます。

このページには、リソースやブログへの参照リンクが記載されています。

アラートおよびITSMツールとの統合

アラートおよびITSMツールには、次のものが含まれます。

- スラック
- マイクロソフト チームズ
- ServiceNow

アラートおよびITSMツールをWebhookと統合するには、ツールの横にある「**開始する**」リンクをクリックします。このリンクをクリックすると、特定のアラートおよびITSMツールの統合ページが開き、前提条件とアラートを送信するための具体的な手順の詳細が表示されます。ツールとWebhook URLを設定できます。たとえば、Slackを統合するには、Slackのドキュメントに従ってチャネルとWebhook URLを作成する必要があります。

それが完了したら、2番目のステップに進み、Webhookプロファイルを作成します。

参照リソースも確認できます。例えば、Slackとの統合の前提条件と手順は以下のとおりです。

Slack統合(/en-us/citrix-virtual-apps-desktops/current-release/media/slack-integration.png)

Webhookとの統合

1. **Integrations**タブ > **Alerting and ITSM**セクション > 選択したツールの横にある**Get started**をクリックします。そのツールの**Integration**ページが開きます。
2. リソースやブログへの参照リンクにアクセスできます。
3. ステップ1に従います。
4. ステップ2の一部として**Create webhook**プロファイルをクリックします。`<name of the tool>` **Create Webhook profile**ページが表示されます。
5. Webhookプロファイルの**Name**を入力します。
6. Webhookプロファイルの**Description**を入力します。
7. **Webhook configuration**セクションで、希望する**Method**を選択します。

8. 前のステップで選択したメソッドに従って、**API/Webhook** URLを入力します。
9. **Message**形式を表示します。
10. **Headers**セクションにキーと値を追加します。
11. 作成したWebhookを検証するには、**Test**をクリックします。
12. Webhookが正常に検証されたら、**Create Webhook**をクリックします。Webhookが作成されます。
13. 作成されたWebhookプロファイルは、**開発者ツール** > **Webhook** > **管理**で表示できます。**Webhookプロファイル開発者ツール詳細**ページが開きます。

Webhookプロファイルは、**開発者ツール** > **Webhook** > **Webhookプロファイルの作成**でも作成できます。

WebhookプロファイルをCitrixアラートと統合する

作成されたWebhookプロファイルは、**アラート** > **高度なアラートポリシー** > **ポリシーの作成**セクションで表示し、Citrixアラートの一部として使用できます。

Webhookプロファイルを新しいCitrixアラートポリシーと統合するには、次の手順を実行します。

1. **アラート** > **高度なアラートポリシー** > **ポリシーの作成**をクリックします。**高度なアラートポリシーの作成**ページが表示されます。
2. **通知チャネル** > **Webhookの使用**セクションに移動します。
3. Webhookプロファイルを選択します。
4. アラートポリシーを保存します。

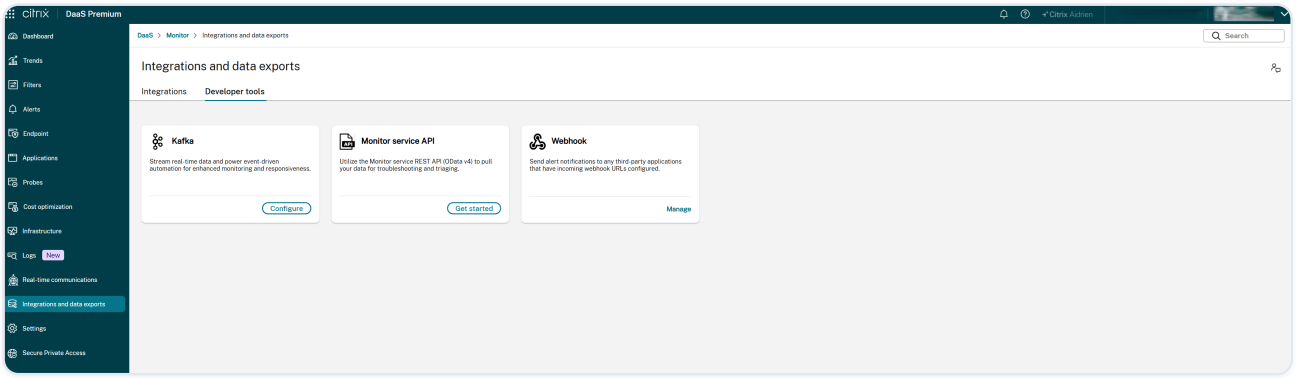
Webhookプロファイルを既存のアラートポリシーと統合するには、次の手順を実行します。

1. **アラート** > **高度なアラートポリシー** > **ポリシーの編集**をクリックします。**高度なアラートポリシーの編集**ページが表示されます。
2. **通知チャネル** > **Webhookの使用**セクションに移動します。
3. Webhookプロファイルを選択または変更します。
4. アラートポリシーを更新して保存します。

サポートされている開発者ツールを表示する

利用可能な開発者ツールを表示するには、**Developer tools**タブをクリックします。

利用可能な開発者ツールは、Monitor service APIとWebhookです。



モニターサービス API

「**開始する**」をクリックします。「**Monitor Service API**」開発者ツール詳細ページが開きます。リソースやブログへの参照リンクにアクセスできます。

ウェブフック

Webhookプロファイルは、「**開発者ツール**」>「**Webhook**」>「**Webhookプロファイルの作成**」で表示および作成できます。

Citrix Director の障害理由とトラブルシューティング

以下の表は、さまざまな障害カテゴリ、その理由、および問題を解決するために必要なアクションについて説明しています。詳細については、「列挙型、エラーコード、および説明」を参照してください。

接続障害エラー

カテゴリ	理由	問題	アクション
該当なし	[0] 不明。このエラーコードはマッピングされていません。	監視サービスは、ブローカリングサービスから共有された情報から、報告された起動または接続障害の理由を判断できません。	コントローラーでCDFログを収集し、Citrixサポートに連絡してください。
[0] なし	[1] なし	なし	該当なし
[2] MachineFailure	[2] SessionPreparation	デリバリーコントローラーからVDAへのセッション準備要求が失敗しました。	コントローラーとVDA間の通信問題を引き起こす一般的な問題については、ナ

カテゴリ	理由	問題	アクション
		考えられる原因：コントローラーとVDA間の通信の問題、Broker Serviceが準備要求を作成する際に発生した問題、またはVDAが要求を受け入れない原因となるネットワークの問題。	レッジセンターの記事「Citrix Virtual Apps and Desktopsにおけるデリバリーコントローラーへの Virtual Delivery Agent登録のトラブルシューティング」に記載されているトラブルシューティング手順を参照してください。
[2] MachineFailure	[3] RegistrationTimeout	VDAは電源がオンになっていましたが、デリバリーコントローラーへの登録中にタイムアウトが発生しました。	Citrix Broker Serviceがデリバリーコントローラーで実行されていること、およびDesktopサービスがVDAで実行されていることを確認します。停止している場合は、それぞれを開始します。
[1] ClientConnectionFailure	[4] ConnectionTimeout	セッション起動のためにVDAが準備された後、クライアントがVDAに接続しませんでした。セッションは正常に仲介されましたが、クライアントがVDAに接続するのを待っている間にタイムアウトが発生しました。考えられる原因：ファイアウォール設定、ネットワーク中断、またはリモート接続を妨げる設定。	Directorコンソールで、クライアントが現在アクティブな接続を持っているかどうかを確認します。アクティブな接続がある場合、ユーザーは影響を受けていません。セッションが存在しない場合は、クライアントとVDAのイベントログでエラーを確認します。クライアントとVDA間のネットワーク接続に関する問題を解決します。

カテゴリ	理由	問題	アクション
[4] NoLicensesAvailable	[5] ライセンス	ライセンス要求が失敗しました。考えられる原因：ライセンス数が不足しているか、ライセンスサーバーが30日以上ダウンしている。	ライセンスサーバーがオンラインで到達可能であることを確認します。ライセンスサーバーへのネットワーク接続の問題を解決するか、ライセンスサーバーが誤動作しているように見える場合は再起動します。環境内に十分なライセンスがあることを確認し、必要に応じて追加で割り当てます。
[1] ClientConnectionFailure	[6] チケット	チケット発行中に障害が発生しました。これは、VDAへのクライアント接続が仲介された要求と一致しないことを示しています。起動要求チケットはBrokerによって準備され、ICA®ファイルで配信されます。ユーザーがセッションを起動しようとすると、VDAはICAファイル内の起動チケットをBrokerで検証します。考えられる原因：ICAファイルが破損しているか、ユーザーが不正な接続を試みている。	デリバリーグループで定義されたユーザーグループに基づいて、ユーザーがアプリケーションまたはデスクトップにアクセスできることを確認します。ユーザーにアプリケーションまたはデスクトップを再起動するよう指示し、これが一時的な問題であるかどうかを判断します。問題が再度発生する場合は、クライアントデバイスのイベントログでエラーを確認します。ユーザーが接続しようとしているVDAが登録されていることを確認します。登録されていない場合は、VDAのイベントログ

カテゴリ	理由	問題	アクション
			を確認し、登録に関する問題を解決します。
[1] ClientConnectionFailure	[7] その他	クライアントがVDAに最初に接続した後、接続シーケンスを完了する前に、セッションがVDAから終了したと報告されました。	起動前にユーザーによってセッションが終了されなかったことを確認します。セッションを再起動してみてください。問題が解決しない場合は、CDFログを収集してCitrixサポートに連絡してください。
[1] クライアント接続失敗	[8] 一般的な失敗	セッションの起動に失敗しました。考えられる原因：ブローカーが起動中または初期化中にブローカーによる起動が要求されたか、起動のブローカー処理フェーズ中に内部エラーが発生しました。	Citrix Broker Serviceが実行されていることを確認し、セッションの起動を再試行してください。
[5] 構成	[9] メンテナンスモード	VDA、またはVDAが属するデリバリーグループがメンテナンスモードに設定されています。	メンテナンスモードが必要かどうかを判断します。不要な場合は、該当するデリバリーグループまたはマシンでメンテナンスモードを無効にし、ユーザーに再接続を試みるよう指示してください。
[5] 構成	[10] アプリケーション無効	アプリケーションは管理者によって無効	アプリケーションが本番環境で使用され

カテゴリ	理由	問題	アクション
		にされているため、エンドユーザーはアクセスできません。	ることを意図している場合は、アプリケーションを有効にし、ユーザーに再接続するよう指示してください。
[4] 利用可能なライセンスなし	[11] ライセンス機能が拒否されました	使用されている機能は、既存のライセンスではカバーされていません。	既存のCitrix Virtual Apps and Desktops™ライセンスのエディションとタイプでカバーされている機能を確認するには、Citrixの営業担当者にお問い合わせください。
[3] 利用可能な容量がありません	[13] セッション制限に達しました	すべてのVDAが使用中で、これ以上セッションをホストする容量がありません。考えられる原因: すべてのVDAが使用中である（シングルセッションOS VDAの場合）、またはすべてのVDAが構成された最大同時セッション数に達している（マルチセッションOS VDAの場合）。	メンテナンスモードのVDAがないか確認してください。より多くの容量を解放するために不要な場合は、メンテナンスモードを無効にしてください。サーバーVDAあたりのセッション数を増やすには、Citrixポリシー設定の**最大セッション数**の値を増やすことを検討してください。マルチセッションOS VDAを追加することを検討してください。シングルセッションOS VDAを追加することを検討してください。

カテゴリ	理由	問題	アクション
[5] 構成	[14] 許可されていないプロトコル	ICAおよびRDPプロトコルは許可されていません。	デリバリーコントローラーで**Get-BrokerAccessPolicyRule** PowerShellコマンドを実行し、**AllowedProtocols**の値に目的のプロトコルがすべてリストされていることを確認してください。この問題は、構成ミスがある場合にのみ発生します。
[5] 構成	[15] リソースが利用できません	ユーザーが接続しようとしているアプリケーションまたはデスクトップが利用できません。このアプリケーションまたはデスクトップが存在しないか、実行できるVDAがありません。考えられる原因: アプリケーションまたはデスクトップが非公開になっている、アプリケーションまたはデスクトップをホストしているVDAが最大負荷に達している、またはアプリケーションまたはデスクトップがメンテナンスモードに設定されている。	アプリケーションまたはデスクトップがまだ公開されており、VDAがメンテナンスモードではないことを確認してください。マルチセッションOS VDAがフルロード状態であるかどうかを判断してください。もしそうであれば、より多くのマルチセッションOS VDAをプロビジョニングしてください。接続に利用可能なシングルセッションOS VDAがあることを確認してください。必要に応じて、より多くのシングルセッションOS VDAをプロビジョニングしてください。

カテゴリ	理由	問題	アクション
[5] 構成	[16] ActiveSessionReconnectDisabled	ICAセッションはアクティブで、別のエンドポイントに接続されています。ただし、**アクティブセッションの再接続**が無効になっているため、クライアントはアクティブなセッションに接続できません。	デリバリーコントローラーで、**アクティブセッションの再接続**が有効になっていることを確認します。レジストリの **HKEY_LOCAL_MACHINE\Software\Citrix\Desktop\Server** にある **DisableActiveSessionReconnect**の値が0に設定されていることを確認します。
[2] MachineFailure	[17] NoSessionToReconnect	クライアントは特定のセッションへの再接続を試みましたが、セッションは終了しました。	ワークスペースコントロールの再接続を再試行してください。
[2] MachineFailure	[18] SpinUpFailed	セッション起動のためにVDAの電源をオンにできません。これはハイパーバイザーによって報告された問題です。	マシンがまだ電源オフの状態である場合は、Citrix Studioからマシンの起動を試行します。これが失敗する場合は、ハイパーバイザーの接続と権限を確認します。VDAがPVSプロビジョニングされたマシンの場合は、PVSコンソールでマシンが実行されていることを確認します。実行されていない場合は、マシンにパーソナルvDiskが割り当てられていることを確認し、ハイパーバイザーにログ

カテゴリ	理由	問題	アクション
			インしてVMをリセットします。
[2] MachineFailure	[19] 拒否	デリバリーコントローラーは、エンドユーザーからの接続に備えるようVDAに要求を送信しますが、VDAはこの要求を積極的に拒否します。	pingで、デリバリーコントローラーとVDAが正常に通信できることを確認します。できない場合は、ファイアウォールまたはネットワークルーティングの問題を解決してください。
[2] マシン障害	[20] 構成セットの失敗	セッション起動中に、デリバリーコントローラーがポリシー設定やセッション情報などの必要な構成データをVDAに送信しませんでした。考えられる原因としては、コントローラーとVDA間の通信の問題、構成セット要求の作成中にBroker Serviceで発生した問題、またはVDAが要求を受け入れない原因となるネットワークの問題が挙げられます。	-
[3] 利用可能な容量なし	[21] 最大インスタンス数を超過	アプリケーションの最大インスタンス数に達しました。VDA上でアプリケーションの追加インスタンスを開くことはできません。この問題は、アプリケーショ	ライセンスが許す場合、アプリケーション設定の「**同時に実行するインスタンス数を制限する**」をより高い値に増やすことを検討してください。

カテゴリ	理由	問題	アクション
		ン制限機能に関連しています。	
[3] 利用可能な容量なし	[22] ユーザーごとの最大インスタンス数を超過	ユーザーがアプリケーションの複数のインスタンスを開こうとしていますが、アプリケーションはユーザーごとに1つのインスタンスのみを許可するように構成されています。この問題は、アプリケーション制限機能に関連しています。	デフォルトでは、ユーザーごとにアプリケーションのインスタンスは1つのみ許可されています。ユーザーごとに複数のインスタンスが必要な場合は、アプリケーション設定で「**ユーザーごとに1つのインスタンスに制限する**」設定をクリアすることを検討してください。
[1] クライアント接続の失敗	[23] 通信エラー	デリバリーコントローラーは、接続の準備を要求するなどの情報をVDAに送信しようとしましたが、通信中にエラーが発生しました。これはネットワークの中断が原因である可能性があります。	すでに開始されている場合は、VDA上のデスクトップサービスを再起動して登録プロセスを再開し、VDAが正常に登録されていることを確認します。アプリケーションイベントログの詳細を通じて、VDA用に構成されているデリバリーコントローラーが正確であることを確認します。
[3] NoCapacityAvailable	[100] NoMachineAvailable 監視サービスは、[12] NoDesktopAvailable をこのエラーコードに変換します。	セッションを起動するために割り当てられたVDAが無効な状態であるか、利用できません。考えられる原因：VDAの電源状態が不明または利	VDAがデリバリーグループ内にあることを確認します。ない場合は、適切なデリバリーグループに追加します。公開された共有デスクトップ

カテゴリ	理由	問題	アクション
		用できない、前回のユーザーセッション以降VDAが再起動されていない、現在のセッションでセッション共有が必要なのに無効になっている、またはVDAがデリバリーグループまたはサイトから削除された。	またはユーザーが要求したアプリケーションを起動できるように、十分なVDAが登録され、準備状態にあることを確認します。VDAをホストしているハイパーバイザーがメンテナンスモードではないことを確認します。
[2] MachineFailure	[101] MachineNotFunctional。監視サービスは、[12] NoDesktopAvailableをこのエラーコードに変換します。	VDAが動作していません。考えられる原因：VDAがデリバリーグループから削除された、VDAが未登録である、VDAの電源状態が利用できない、またはVDAが内部的な問題を抱えている。	VDAがデリバリーグループ内にあることを確認します。ない場合は、適切なデリバリーグループに追加します。VDAがCitrix Studioで電源オンとして表示されていることを確認します。複数のマシンの電源状態が不明な場合は、ハイパーバイザーへの接続に関する問題またはホストの障害を解決します。VDAをホストしているハイパーバイザーがメンテナンスモードではないことを確認します。これらの問題が解決されたら、VDAを再起動します。

マシン障害の種類

エラーコード	エラーコードID	問題	アクション
不明	-	-	-
未登録	3	-	-
最大容量（Directorでは最大負荷として表示）	4	マシンが最大容量、つまり最大負荷インデックスを報告しています	すべてのハイパーバイザーの電源がオンになっていることを確認します。ハイパーバイザーの容量を増やすか、ハイパーバイザーを追加することで、影響を受けるデリバリーグループにマシンを追加します。
StuckOnBoot	2	VMが起動シーケンスを完了せず、ハイパーバイザーと通信していません。	VMがハイパーバイザー上で正常に起動したことを確認します。OSの問題など、VM上の他のメッセージを確認します。ハイパーバイザーツールがVMにインストールされていることを確認します。VDAがVMにインストールされていることを確認します。
FailedToStart	1	VMがハイパーバイザー上で起動しようとしたときに問題が発生しました。	ハイパーバイザーのログを確認します。
なし	0	-	-

マシンの登録解除理由 (障害の種類が「未登録」または「不明」の場合に適用)

エラーコード	エラーコードID	問題	アクション
AgentShutdown	0	VDAは正常にシャットダウンされました。	既存の電源管理ポリシーに基づいてVDAがオフになっていると想定されない場合は、VDAの電源をオンにします。イベントログのエラーを確認します。
AgentSuspended	1	VDAは休止状態またはスリープモードです。	VDAを休止状態から復帰させます。電源設定を介してCitrix Virtual Apps and Desktops™ VDAの休止状態を無効にすることを検討してください。
IncompatibleVersion	100	Citrixプロトコルバージョンの不一致により、VDAはデリバリーコントローラーと通信できません。	VDAとデリバリーコントローラーのバージョンを合わせます。
AgentAddressResolutionFailed	101	デリバリーコントローラーはVDAのIPアドレスを解決できませんでした。	VDAマシンアカウントがADに存在することを確認します。存在しない場合は、作成します。DNS内のVDAの名前とIPアドレスが正確であることを確認します。正確でない場合は、修正します。広範囲にわたる場合は、デリバリーコントローラーのDNS設定を検証します。コント

エラーコード	エラーコードID	問題	アクション
			ローラーから `nslookup` コマンドを実行してDNS解決を確認します。
[Cloud]:AgentAddressResolutionFailed	101	デリバリーコントローラーはVDAのIPアドレスを解決できませんでした。	VDAマシンアカウントがADに存在することを確認します。存在しない場合は、作成します。DNS内のVDAの名前とIPアドレスが正確であることを確認します。正確でない場合は、修正します。
AgentNotContactable	102	デリバリーコントローラーとVDAの間で通信の問題が発生しました。	pingを使用して、デリバリーコントローラーとVDAが正常に通信できることを確認します。通信できない場合は、ファイアウォールまたはネットワークの問題を解決してください。コントローラーとVDA間の通信問題を引き起こす一般的な問題については、Knowledge Centerの記事「Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668)」に記載されているトラブルシューティング手

エラーコード	エラーコードID	問題	アクション
			順を参照してください。
[Cloud]: AgentNotContactable	102	デリバリーコントローラーとVDA間で通信の問題が発生しました。	コントローラーとVDA間の通信問題を引き起こす一般的な問題については、Knowledge Centerの記事「Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668)」に記載されているトラブルシューティング手順を参照してください。Citrixサポートに連絡してください。
AgentWrongActiveDirectoryOU	103	Active Directoryの検出設定が誤っています。VDAレジストリで構成されているサイト固有のOU（サイトコントローラー情報がADに保存されている場所）が、別のサイト用です。	Active Directoryの設定が正しいことを確認するか、レジストリ設定を確認してください。
EmptyRegistrationRequest	104	VDAからデリバリーコントローラーに送信された登録要求が空でした。これは、VDAソフトウェアのインストールが破損していることが原因	VDA上のDesktopサービスを再起動して、登録プロセスを再開し、アプリケーションイベントログを介してVDAが正しく登録されているこ

エラーコード	エラーコードID	問題	アクション
		である可能性があります。	とを確認してください。
MissingRegistrationCapabilities	105	VDAのバージョンがデリバリーコントローラーと互換性がありません。	VDAをアップグレードするか、VDAを削除してから再インストールしてください。
MissingAgentVersion	106	VDAのバージョンがデリバリーコントローラーと互換性がありません。	問題がすべてのマシンに影響している場合は、VDAソフトウェアを再インストールしてください。
InconsistentRegistrationCapabilities	107	VDAはBrokerにその機能を通知できません。これは、VDAとデリバリーコントローラーのバージョン間の非互換性が原因である可能性があります。バージョンごとに変更される登録機能は、登録要求と一致しない形式で表現されています。	VDAとデリバリーコントローラーのバージョンを合わせてください。
NotLicensedForFeature	108	使用しようとしている機能はライセンスされていません。	Citrixライセンスエディションを確認するか、VDAを削除してから再インストールしてください。
[Cloud]: NotLicensedForFeature	108	使用しようとしている機能はライセンスされていません。	Citrixサポートにお問い合わせください。

エラーコード	エラーコードID	問題	アクション
サポートされていないCredentialSecurityバージョン	109	VDAとデリバリーコントローラーが同じ暗号化メカニズムを使用していません。	VDAとデリバリーコントローラーのバージョンを合わせてください。
無効な登録リクエスト	110	VDAがブローカーに登録リクエストを行いましたが、リクエストの内容が破損しているか無効です。	コントローラーとVDA間の通信問題を引き起こす一般的な問題については、Knowledge Centerの記事「Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668)」に記載されているトラブルシューティング手順を参照してください。
シングル/マルチセッションの不一致	111	VDAのオペレーティングシステムタイプは、マシンカタログまたはデリバリーグループと互換性がありません。	VDAを、適切なマシンカタログタイプまたは同じオペレーティングシステムを持つマシンを含むデリバリーグループに追加してください。
FunctionalLevelTooLowForCatalog	112	マシンカタログは、インストールされているVDAバージョンよりも高いVDA機能レベルに設定されています。	VDAのマシンカタログ機能レベルがVDAの機能レベルと一致していることを確認してください。マシンカタログをVDAの機能レベルに合わせてアップグレードま

エラーコード	エラーコードID	問題	アクション
			たはダウングレードしてください。
FunctionalLevelTooLowForDesktopGroup	113	デリバリーグループは、インストールされているVDAバージョンよりも高いVDA機能レベルに設定されています。	VDAのデリバリーグループ機能レベルがVDAの機能レベルと一致していることを確認してください。マシンカタログをVDAの機能レベルに合わせてアップグレードまたはダウングレードしてください。
PowerOff	200	VDAが正常にシャットダウンされませんでした。	VDAが電源オン状態であるべき場合は、Citrix StudioからVDAの起動を試み、VDAが正常に起動して登録されることを確認してください。起動または登録に関する問題があればトラブルシューティングを行ってください。VDAが再び稼働したら、イベントログを確認してシャットダウンの根本原因を特定するのに役立ててください。
AgentRejectedSettingsUpdate	203	Citrixポリシーなどの設定が変更または更新されましたが、VDAへの更新の送信中にエラーが発生しました。これは、更新がインストールされているVDAバー	必要に応じてVDAをアップグレードしてください。適用された更新がVDAバージョンでサポートされているかどうかを確認してください。

エラーコード	エラーコードID	問題	アクション
		ジョンと互換性がない場合に発生する可能性があります。	
SessionPrepareFailure	206	ブローカーは、VDAで実行されているセッションの監査を完了しませんでした。	広範囲にわたる場合は、デリバリーコントローラーでCitrix Broker Serviceを再起動してください。
[Cloud]: SessionPrepareFailure	206	ブローカーは、VDAで実行されているセッションの監査を完了しませんでした。	Citrixサポートにお問い合わせください。
ContactLost	207	デリバリーコントローラーがVDAとの接続を失いました。これはネットワーク障害が原因である可能性があります。	デリバリーコントローラーでCitrix Broker Serviceが実行されており、VDAでDesktop Serviceが実行されていることを確認します。停止している場合は、それぞれを開始します。すでに開始されている場合は、VDAでDesktop Serviceを再起動して登録プロセスを再開し、VDAが正常に登録されることを確認します。アプリケーションイベントログの詳細を通じて、VDA用に構成されているデリバリーコントローラーが正確であることを確認します。pingを使用して、デリバリーコントローラー

エラーコード	エラーコードID	問題	アクション
			とVDAが正常に通信できることを確認します。通信できない場合は、ファイアウォールまたはネットワークの問題を解決します。
[Cloud]: ContactLost	207	デリバリーコントローラーがVDAとの接続を失いました。これはネットワーク障害が原因である可能性があります。	VDAでDesktop Serviceが実行されていることを確認します。停止している場合は開始します。
BrokerRegistrationLimitReached	301	デリバリーコントローラーが、同時に登録できるVDAの構成済み最大数に達しました。デフォルトでは、デリバリーコントローラーは10,000の同時VDA登録を許可します。	サイトにデリバリーコントローラーを追加するか、サイトを作成することを検討してください。また、**HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer\MaxWorkers** レジストリキーを使用して、デリバリーコントローラーに同時に登録できるVDAの数を増やすこともできます。詳細については、Knowledge Centerの記事「Citrix Virtual Apps and Desktops で使用されるレジストリキーエントリ (CTX117446)」を参照してください。この数を増やすと、コントローラーにより多くのCPUお

エラーコード	エラーコードID	問題	アクション
			よびメモリリソースが必要になる場合があります。
SettingsCreationFailure	208	ブローカーがVDAに送信する設定と構成のセットを構築しませんでした。ブローカーがデータを収集できない場合、登録は失敗し、VDAは登録解除されます。	デリバリーコントローラーのイベントログでエラーを確認してください。ログに特定の問題が明らかでない場合は、ブローカーサービスを再起動してください。ブローカーサービスが再起動されたら、影響を受けるVDAでデスクトップサービスを再起動し、それらが正常に登録されることを確認してください。
[Cloud]: SettingsCreationFailure	208	ブローカーがVDAに送信する設定と構成のセットを構築しませんでした。ブローカーがデータを収集できない場合、登録は失敗し、VDAは登録解除されます。	影響を受けるVDAでデスクトップサービスを再起動し、それらが正常に登録されることを確認してください。Citrixサポートに連絡してください。
SendSettingsFailure	204	ブローカーが設定および構成データをVDAに送信しませんでした。ブローカーがデータを収集できるが送信できない場合、登録は失敗します。	単一のVDAに限定される場合は、VDA上のデスクトップサービスを再起動して再登録を強制し、アプリケーションイベントログを介してVDAが正常に登録されることを検証してください。発生したエラーをトラブル

エラーコード	エラーコードID	問題	アクション
			シューティングしてください。コントローラーとVDA間の通信問題を引き起こす一般的な問題については、Knowledge Centerの記事「Citrix Virtual Apps and Desktops でのデリバリーコントローラーとのVirtual Delivery Agent登録のトラブルシューティング (CTX136668)」に記載されているトラブルシューティング手順を参照してください。
エージェント要求	2	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
デスクトップの再起動	201	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
デスクトップが削除されました	202	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
セッション監査の失敗	205	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
UnknownError	300	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
RegistrationStateMismatch	302	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
不明	-	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。

ログ

Citrix Director/Monitor の新しいログビューは、Always On Tracing (AOT) を活用して、管理者が Citrix Virtual Apps and Desktops (CVAD) 環境における顧客の問題を診断および解決する能力を大幅に向上させるように設計されています。この機能は、集中ログサーバーと統合することで、Virtual Delivery Agents、Delivery Controllers、StoreFront、その他の Citrix コンポーネントを含むさまざまなコアコンポーネントにわたる AOT ログの統合された検索可能なビューを提供します。この一元化されたアクセスにより、単一のコンソールからログを迅速に取得および分析できるため、トラブルシューティングが効率化されます。

Director ログ(/en-us/citrix-virtual-apps-desktops/current-release/media/dir-logs.png)

製品ドキュメントで Always On Tracing (AOT) のアーキテクチャと利点の詳細をご覧ください。

前提条件と構成

Director の「ログ」ビューを効果的に使用するには、環境が正しく構成され、必要な前提条件を満たしている必要があります。

- **CVAD バージョン要件**: CVAD 2507 CU1 または CVAD 2511 (またはそれ以降のバージョン) を実行している必要があります。
- 集中ログサーバー: お客様が管理するリソースロケーションで集中ログサーバーをホストする必要があります。ログサーバーのインストールと構成 の詳細をご覧ください。
- ログサーバーが HTTPS モード (例: `https://<LogServerFQDN>:port`) で構成されている場合、Director マシンと DDC マシンの両方に必要な証明書をインストールして信頼することが不可欠です。この証明書は、各マシンのコンピューターアカウントによって管理される必要があります。

はじめに

前提条件の構成が完了すると、Director UI の新しいログタブにより、集中化された AOT ログへの統合された可視性が提供されます。

ログビューへのアクセス

ログビューには、Director 内の専用タブとして直接アクセスすることも、他の主要なトラブルシューティング領域からコンテキストで移動することもできます。

- **専用の「ログ」タブ**: ナビゲーションパネルを使用して、Director/Monitor インターフェイスで新しい「ログ」ページに直接アクセスします。

- **アクティビティマネージャー**」: オプションをクリックして、セッションをホストしているマシンに関連するログを表示します。
- **マシンフィルター**」: オプションをクリックして、マシン名が事前入力された関連ログを表示します。

ログビューの使用

ログビューは、柔軟で強力なログ検索ができるように設計されており、管理者は関連するイベントをすばやく特定できます。

ログビュー(/en-us/citrix-virtual-apps-desktops/current-release/media/dir-logs-view.png)

メインの検索インターフェイスには、次のものが含まれます。

- **検索バー**」: あらゆるキーワードで検索できる強力なテキストボックスです。一般的な検索語には、トランザクションID、セッションID、ユーザー名、または特定のエラーメッセージなどがあります。
- **フィルターセレクター**」: 次のドロップダウンフィルターを使用して、検索範囲を絞り込みます。
- **時間間隔**」: 特定の時間範囲でログをフィルターします。
- **カテゴリ**」: ログカテゴリでフィルターします。
- **ログクラス**」: ログメッセージのクラス（例: AOT_INFO）でフィルターします。
- **マシン名**」: 特定のマシン名から発信されたログをフィルターします。

検索結果は、時間、メッセージ、ホスト名、レベル、モジュール、プロセスIDなどの主要な属性を含む包括的なテーブル形式で表示されます。個々のログエントリを展開して、詳細を表示できます。Directorは、ログデータに関連するカスタム列の構成と表示をサポートしています。さらに、結果はページ分割されており、大規模なデータセットの表示とナビゲーションが容易です。

すべてのAOTログに即座にコンテキストを意識したアクセスを提供することで、この機能はツール間の切り替えやログの手動での関連付けに費やす時間を削減し、問題解決の高速化を目指します。

インサイト

インサイトパネルは、環境内のセッション障害または遅延に関する情報を提供します。これらのインサイトで特定のメトリックを深く掘り下げることで、セッション障害や遅延のトラブルシューティングと解決をより迅速に行うことができます。障害インサイトは、特に管理者がセッションの可用性を向上させるのに役立ちます。これは、ユーザーエクスペリエンスを決定する重要

な要素です。これらのインサイトは、ユーザーエクスペリエンスのプロアクティブな監視を支援するように設計されています。したがって、システム内の現在の障害に対してインサイトが表示されます（15分ごとに更新されます）。

Directorインサイト(/en-us/citrix-daas/media/dir-insights.png)

ダッシュボードからインサイトアイコンをクリックすると、インサイトの詳細と、マシンビューまたは接続ビューにドリルダウンするオプションを含むインサイトペインが表示されます。管理者は、パネルからアラート設定に移動することもできます。

このパネルでは、ブラックホールマシン、ゾンビセッション、過負荷マシン、およびセッション障害インサイトが利用可能です。各インサイトを展開すると、失敗したセッションまたはそれらをホストしているマシンへのリンクが表示されます。これにより、失敗したマシンまたはセッションを含むフィルタービューに移動します。ここから、特定の仮想マシンまたはセッションをクリックして詳細なメトリックを表示することで、さらにドリルダウンできます。

各インサイトの展開ビューには、サイト、デリバリーグループ、シングルまたはマルチOSセッションマシンに関して検出された上位の障害パターンが表示されます。これらのパターンは、管理者が特定の一群のユーザーが問題を経験しているかどうかを特定するのに役立つことを目的としています。システムが分散したコホートのためにパターンを強調表示できない場合は、自己分析のためにドリルダウンすることをお勧めします。また、問題のトラブルシューティングと解決のために推奨されるアクションも表示されます。

ブラックホールマシン

環境内の一部のマシンは、登録されており正常に見えても、それらに仲介されたセッションを処理しない場合があり、その結果、障害が発生します。4つ以上の連続したセッション要求を処理できなかったマシンは、ブラックホールマシンと呼ばれます。これらの障害の原因は、RDSライセンスの不足、断続的なネットワークの問題、マシンへの瞬間的な負荷など、マシンに影響を与える可能性のあるさまざまな要因に関連しています。これらの障害には、容量またはライセンスの可用性による障害は含まれません。環境内にブラックホールマシンが存在すると、セッション障害が増加し、セッションの可用性が低下します。ブラックホールマシンインサイトは、環境内で識別されたブラックホールマシンの数を示します。

ブラックホール(/en-us/citrix-daas/media/dir-black-hole.png)

ブラックホールマシンに推奨されるアクション:

- マシンのRDSライセンスを確認する
- マシンをメンテナンスモードにする
- 再起動する

「検出されたパターン」セクションには、以下の基準に関してブラックホールマシンで確認された上位のパターンが表示されます。

- シングルセッションまたはマルチセッションOSを実行しているブラックホールマシンの数
- 影響を受けたマシンが最も多いデリバリーグループ

ゾンビセッション

ゾンビセッションサブペインには、環境内でゾンビセッションが原因で発生したセッション障害に関する情報が表示されます。ゾンビセッションとは、シングルセッションOSマシン上で放棄されたセッションのことで、そのマシン上での新しいセッション起動が失敗する原因となります。このマシンでセッションを起動しようとすると、「利用可能な容量がありません」というエラーで失敗します。放棄されたセッションが終了するまで、以降のすべてのセッション起動試行は失敗します。ゾンビセッションのインサイトは、放棄されたセッションを持つこれらのマシンを特定し、これらの障害をプロアクティブに軽減するのに役立つことを目的としています。

ゾンビセッション(/en-us/citrix-daas/media/dir-zombie.png)

ゾンビセッションの推奨されるアクション:

- Citrix DaaSサイトのMonitorを使用して、ゾンビセッションからユーザーをログアウトさせることができます。
- ゾンビセッションを含むマシンを再起動できます。

「検出されたパターン」セクションには、以下の基準に関してゾンビセッションで確認された上位のパターンが表示されます。

- 影響を受けたマシンが最も多いデリバリーグループ
- 影響を受けたセッションが最も多いデリバリーグループ

過負荷のマシン

過負荷のマシンインサイトは、エクスペリエンスの低下を引き起こす過負荷のリソースを可視化します。5分以上継続するCPUスパイク、または高いメモリ使用量、あるいはその両方を経験し、ユーザーエクスペリエンスの低下につながる可能性のあるマシンは、過負荷と見なされます。

過負荷のマシン(/en-us/citrix-daas/media/dir-overload-machines.png)

「検出されたパターン」セクションには、以下の基準に関して過負荷のマシンで確認された上位のパターンが表示されます。

- シングルセッションまたはマルチセッションOSを実行している過負荷マシンの数

- 影響を受けるマシンが最も多いデリバリーグループ
- 持続的なメモリまたはCPUスパイクが発生している過負荷マシンの数

接続障害

接続障害インサイトには、エンドポイント（ユーザーがセッションを起動する場所）からマシン（セッションが仲介される場所）までの問題によるセッション障害の数が表示されます。これらの障害は、ファイアウォールの設定ミス、ネットワーク通信の問題、マシンの利用不可など、さまざまな理由で発生する可能性があります。

接続障害(/en-us/citrix-daas/media/dir-connection-failures.png)

接続障害の2つのカテゴリは次のとおりです。

- クライアント接続障害 — エンドポイントで通信エラーが発生したセッションを一覧表示します。
- マシン障害 — マシンでエラーが発生したセッションを一覧表示します。

さらに、接続障害サブパネルには、エラーを解決するための次の推奨事項が表示されます。

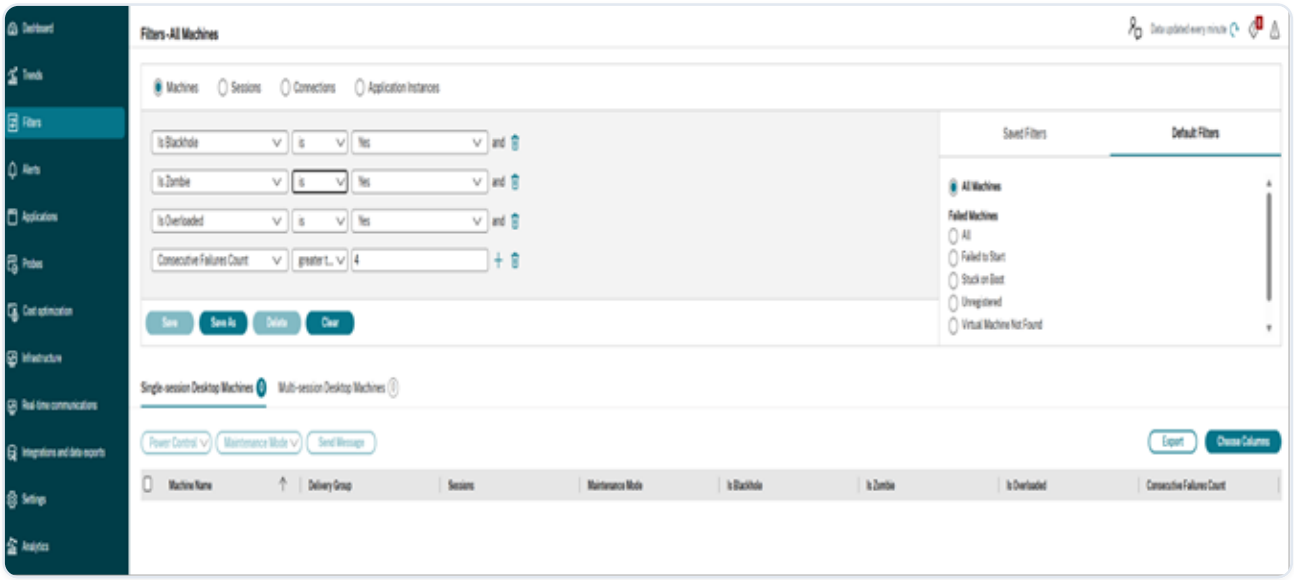
- マシンとゲートウェイのファイアウォール設定を確認します。
- コンポーネント間のネットワーク接続を確認します。
- マシンの電源がオンになっており、登録済み状態であることを確認します。

障害は、ブロックされたユーザー、つまり選択した期間中に接続障害が発生した後、成功したセッションが一度もなかったユーザーを特定するためにグループ化されます。両方のカテゴリの障害パターンが強調表示されます。詳細をクリックすると、選択した期間中に環境内のエラーが原因で失敗したすべてのセッションを表示するようにフィルター処理された接続ビューが開きます。このビューは、失敗した個々のセッションを分析し、考えられる根本原因を特定するのに役立ちます。

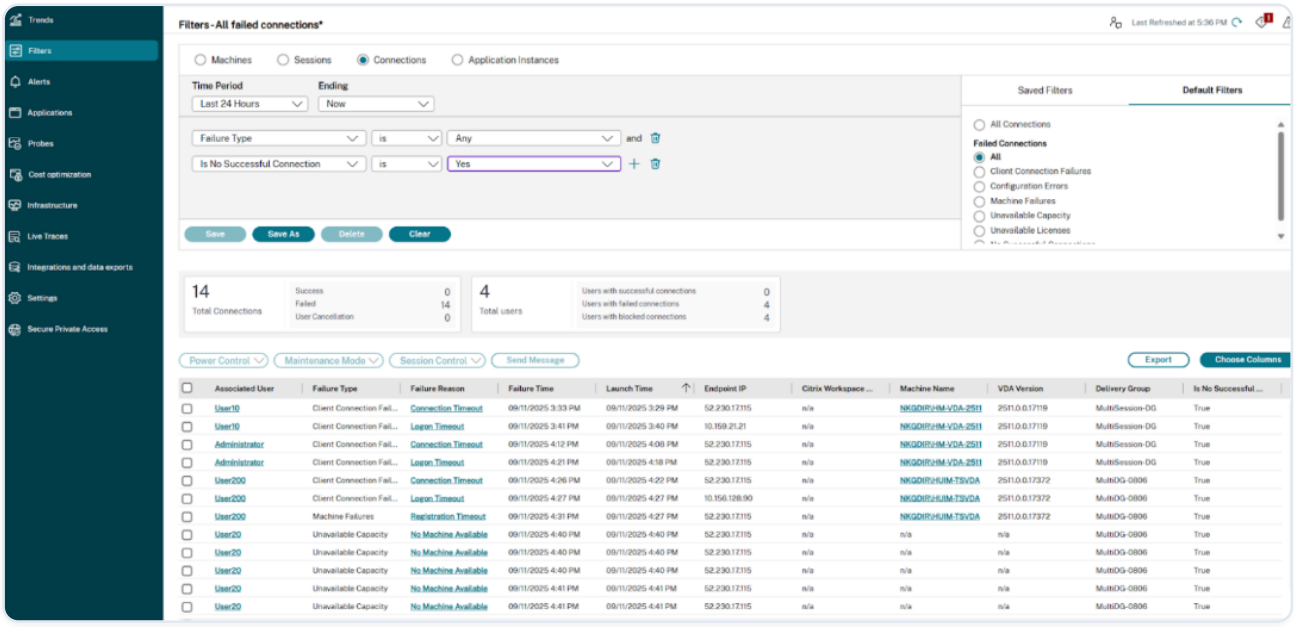
フィルタービュー

以下は、 -> の下の ビューに追加された新しいフィルターと列です。

- 連続失敗回数: マシンが報告した連続セッション起動失敗の回数
- ブラックホールか: マシンがブラックホールマシンとして識別されたかどうか
- ゾンビか: マシンがゾンビマシンとして識別されたかどうか
- 過負荷か: マシンが過負荷マシンとして識別されたかどうか



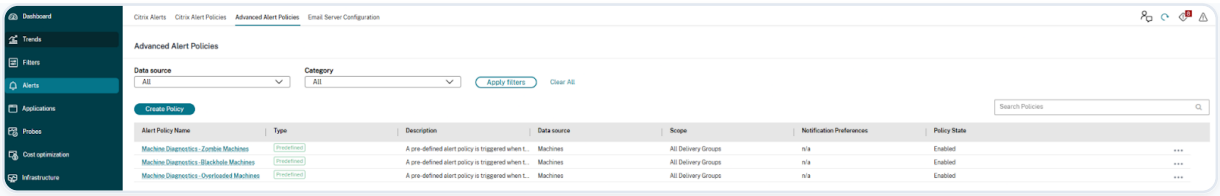
以下は、 -> の ビューに追加された新しいフィルタと列です。



アラート

システム内でブラックホール、ゾンビ、または過負荷のマシン（すべてのデリバリーグループにわたる）が識別された場合に、管理者がプロアクティブにアラートを発生させるのに役立つ、3つの新しい「高度なアラートポリシー」が利用可能で、デフォルトで有効になっています。

> **注:**
>
> 現在のリリースでは、高度なアラートポリシーで接続障害はサポートされていません。



デフォルトポリシーの管理

診断インサイトの価値を最大化するために、デフォルトのアラートポリシーに関するいくつかの重要なポイントを以下に示します。

- **カスタマイズ:** 管理者は、これらのデフォルトポリシーの**アラートポリシーパラメータ、スコープ、または通知アクション**をカスタマイズできます。
- **制限事項:** デフォルトポリシーの**条件を変更したり、削除したりする**ことはできません。
- **有効化/無効化:** ポリシーは必要に応じて**無効化または有効化**できます。
- **通知:** デフォルトポリシーは、既定では**通知が構成されていません。UIアラート**のみが発生します。管理者には、これらのポリシーの**通知設定を更新することを強くお勧めします。**

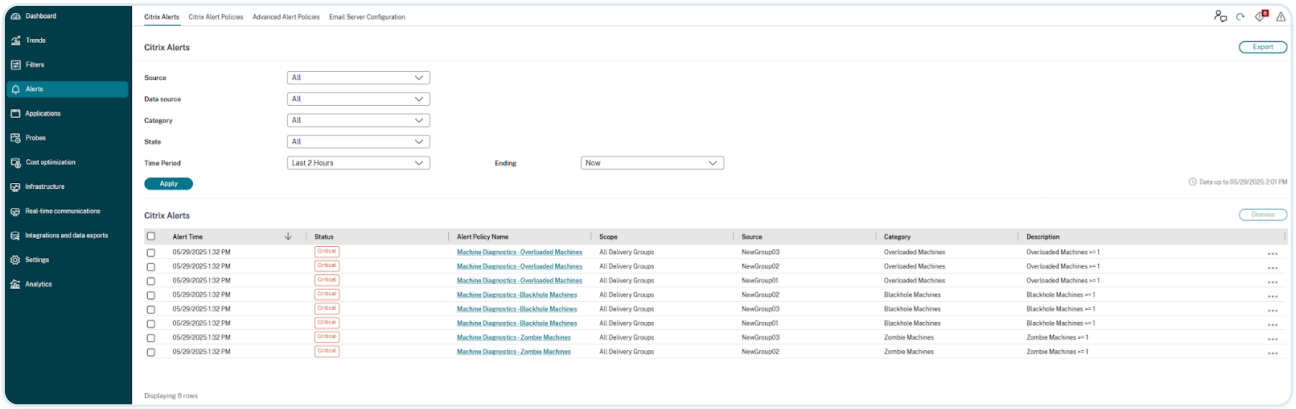
> **注:**
>
> - Insights Panel自体は、有効なポリシーに依存しています。デフォルトポリシーを無効にし、有効なカスタムポリシーがない場合、Insights Panelは更新を停止します。
> - アラートパラメータを更新すると、ダッシュボード上の対応するインサイトの計算も変更されます。

カスタムポリシーの作成

これらのインサイトに対して、追加の**カスタムポリシー**を作成できます。カスタムポリシーを作成する場合は、カスタムポリシーの対象となる**Delivery Groupを除外する**ように、**デフォルトポリシーのスコープを変更する**ことをお勧めします。これにより、重複や潜在的な重複アラートを防ぐことができます。

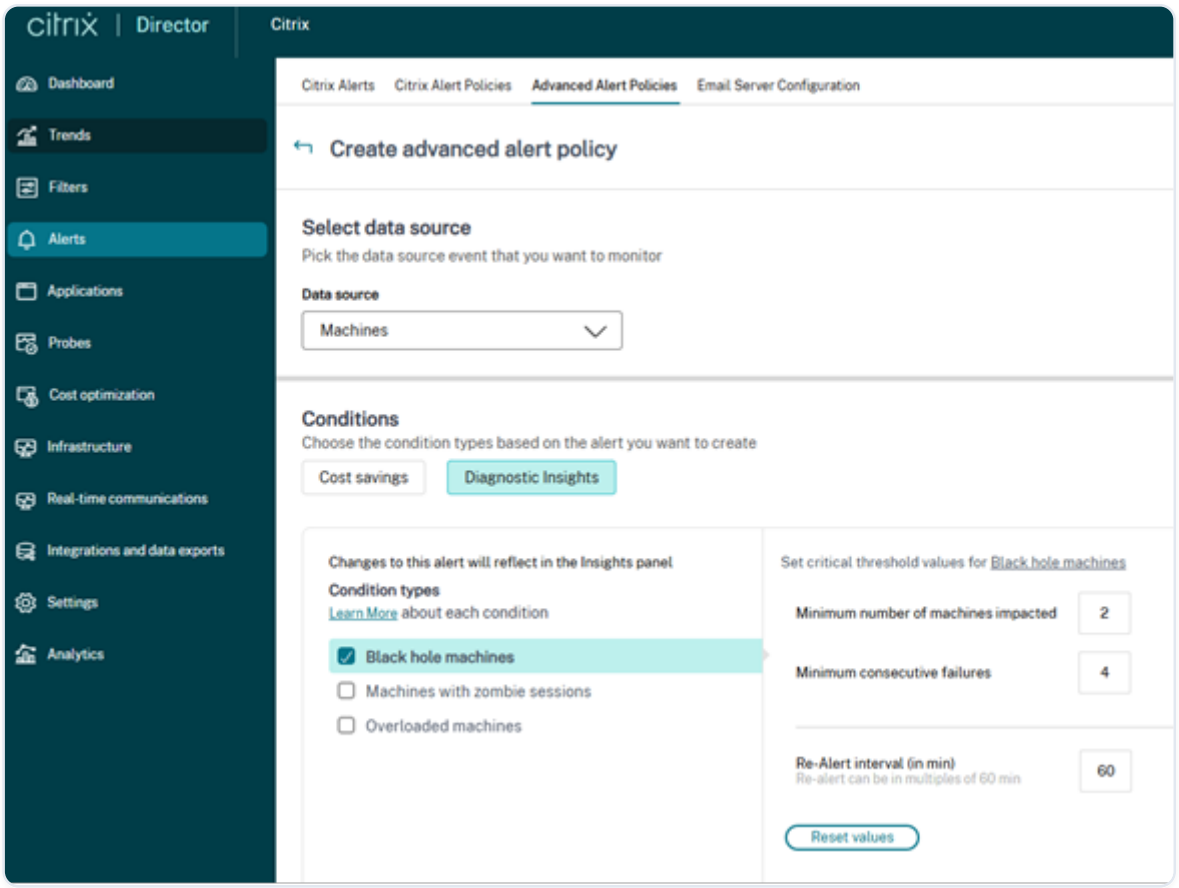
アラート通知

以下は、インサイトに対して発生した「Citrixアラート」のクイックビューです。



ブラックホールマシンに関するアラート

Monitorは15分ごとにブラックホールマシンをスキャンし、ユーザーが直面するセッション障害をプロアクティブに軽減するために管理者へアラートを送信します。4回以上の連続したセッション要求に応答できなかったマシンは、デフォルトでブラックホールマシンと呼ばれます。選択したアラートのアラート条件と再アラート間隔はカスタマイズできます。



セッション障害を引き起こしたマシンの詳細は、アラートメールまたはWebhookペイロードで送信されます。これらの通知を受信するには、ブラックホールマシンアラートポリシーを有効にする必要があります。

ゾンビセッションを持つマシンに関するアラート

ゾンビセッションを持つマシンに関するアラートは、15分間隔で環境内にゾンビセッションを持つ新しいマシンが検出されたときに生成されます。

管理者は、ゾンビセッションを持つマシンに関するアラートのアラート条件をカスタマイズできます。

高度なアラート ゾンビセッション(/en-us/citrix-daas/media/dir-alert-zombie.png)

ゾンビセッションと障害の原因となったマシンの詳細は、アラートメールまたはWebhookペイロードで送信されます。

過負荷状態のマシンに関するアラート

設定されたサンプリング間隔で、CPUスパイクの継続、高いメモリ使用量、またはその両方を経験したマシンは、過負荷と見なされます。

管理者は、過負荷のマシンに関するアラートのアラート条件と再アラート設定をカスタマイズできます。

過負荷のマシン(/en-us/citrix-daas/media/dir-alert-overloaded-machines.png)

再アラート

特定のインサイトアラートの場合、設定された**再アラート間隔**内の通知動作は増分です。この間隔中に新しい問題のあるマシンが特定された場合、再アラートメールまたはWebhookには**それらの新しいマシンのみ**が含まれます。特定のデリバリーグループのすべての問題のあるマシンをリストした完全なアラートは、**再アラート間隔**ごとに1回送信されます（これは**デフォルトで24時間**です）。

セッション起動成功のマップビュー

概要

Citrix Directorのマップビューは、管理者にCitrix環境全体でのセッション起動の成功に関する包括的な地理的視覚化を提供します。この機能は、ユーザー接続をグローバル規模で視覚的にマッピングし、ITチームが地域のパフォーマンスパターンを迅速に特定し、地理的な接続の問題をトラブルシューティングし、位置データに基づいてエンドユーザーエクスペリエンスを最適化するのに役立ちます。マップには、さまざまな地理的場所でのログオンパフォーマンスを示す色分けされた接続ポイントが表示されます。

前提条件

次の表に、機能、エンドポイントメトリック、およびサポートされている製品バージョンを示します。

VDA

VDA WINDOWSバージョン	VDA MACバージョン	VDA LINUXバージョン
2411 以降	NA	NA

VIRTUAL DELIVERY AGENTバージョン	CITRIX WORKSPACE APP FOR WINDOWS のバージョン	CITRIX WORKSPACE APP FOR MAC のバージョン	CITRIX WORKSPACE APP LINUX版 バージョン	CITRIX WORKSPACE APP FOR HTML5 バージョン	CITRIX WORKSPACE APP FOR CHROMEOS バージョン
2411 以降	2409 以降	2409 以降	2408 以降	2411 以降	2411 以降

> **注:**
>
> マップ上の位置データにアクセスして表示するには、スタジオポリシー「Endpoint Location Data Collection」を有効にする必要があります。続行する前に、このポリシーが構成されていることを確認してください。

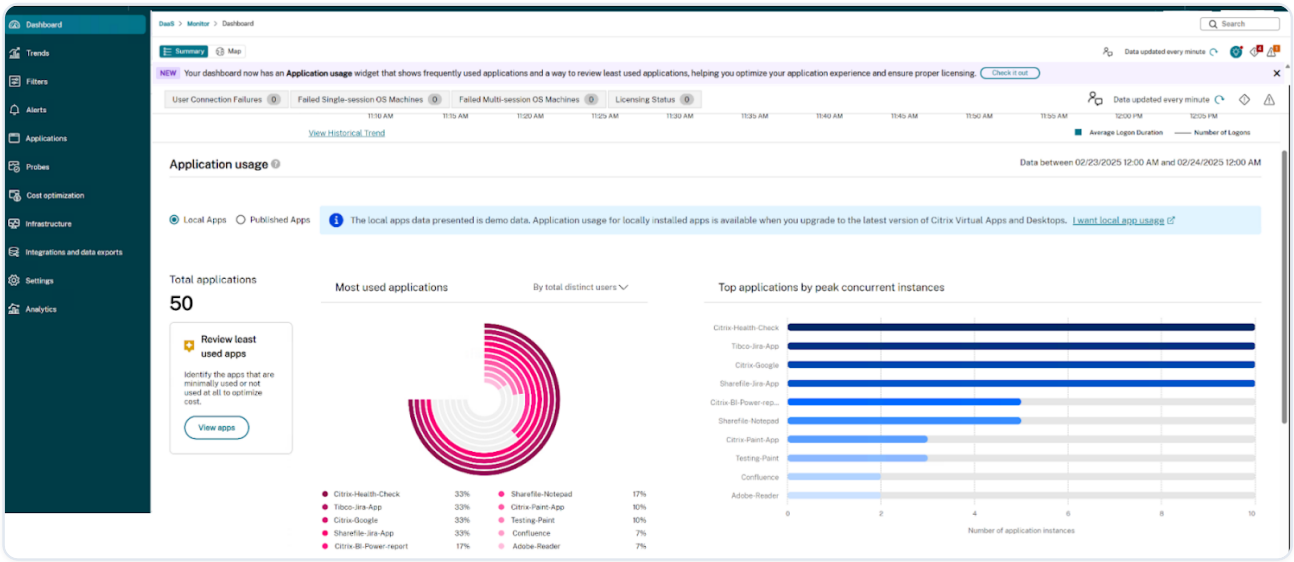
主な利点

- **地理的パフォーマンスのインサイト:** さまざまな国や地域における接続パフォーマンスメトリックを即座に視覚化します。
- **カスタマイズ可能なパフォーマンスしきい値:** 低、中、高（不良）のログオン期間について、独自の標準を定義します。
- **接続密度の視覚化:** 色分けされたインジケーターとさまざまな円のサイズを通じて、トラフィックの多い地理的領域を特定します。
- **グローバル展開の概要:** 環境全体の重要な概要メトリックにアクセスします。
- **地域別のトラブルシューティング:** 地理的領域別にパフォーマンスの問題を迅速に特定し、対処します。
- **リアルタイム監視:** 5分ごとに自動的に更新されるデータを表示します。

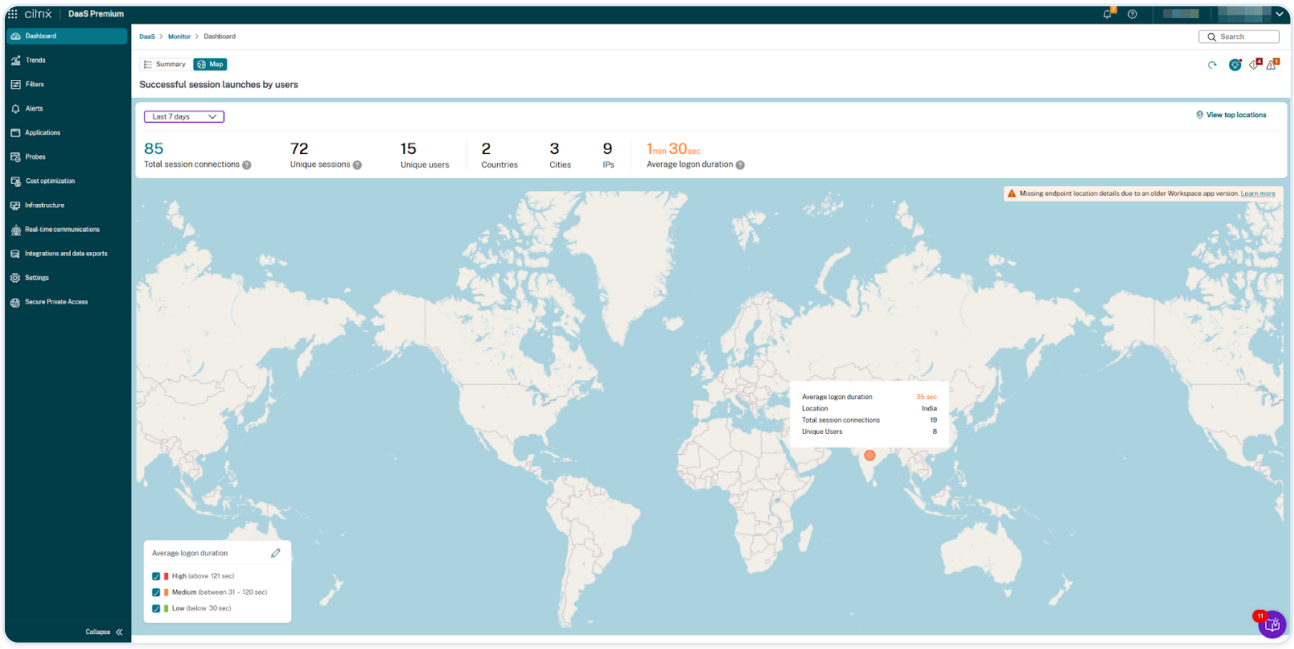
完全な管理者権限があれば、Directorを開くと、ダッシュボードは、サイトの健全性と使用状況を監視するための一元的な場所を提供します。

ダッシュボードには、概要ビューとマップビューが含まれています。

概要ビュー:



マップビュー:



ユーザーインターフェイスコンポーネント

ナビゲーションと表示オプション

- **概要/マップ切り替え:** 概要統計と地理的マップの視覚化を切り替えます
- **時間範囲セレクター:** 期間でデータをフィルターします (デフォルト: 「過去1時間」)

- **上位の場所を表示:** 接続密度が最も高い領域に焦点を当てるオプション
- **データ更新インジケーター:** データが最後に更新された日時を表示します (5分ごとに更新)
- **通知アイコン:** 展開に関連するシステムアラートとメッセージ

概要ダッシュボードメトリック

マップビューの上部で、管理者は次の重要な展開全体のメトリックを表示できます。

メトリック	説明
合計セッション接続数	すべての場所におけるセッション接続の総数
ユニークセッション数	重複を除外して確立された個々のセッション数
ユニークユーザー数	接続を確立した個別のユーザーの総数
国	接続が発信された異なる国の数
都市	接続が発信された個別の都市の数
IPアドレス	接続を確立した一意のIPアドレスの総数
平均ログオン時間	展開全体でセッション確立にかかった平均時間

パフォーマンス分類

接続パフォーマンスは、カスタマイズ可能なしきい値を持つ次の3つの階層に分類されます。

パフォーマンスレベル	色コード	デフォルトのしきい値	説明
低 (良好)	緑	60秒未満	遅延が最小限に抑えられた高速ログオンエクスペリエンス
中	オレンジ	61〜120秒*	許容可能なログオン時間
高 (不良)	赤	120秒以上	注意が必要な最適とは言えないログオンエクスペリエンス

> **注:**

> このインターフェイスでは、管理者は凡例パネルの入力フィールドを通じてこれらのしきい値をカスタマイズできます。

マップ凡例と閾値コントロール

インタラクティブな凡例パネルには、次のものが表示されます。

- **色分けされたパフォーマンスインジケーター**と対応するしきい値
- 中程度のパフォーマンス範囲 (最小値と最大値) をカスタマイズするための**編集可能なしきい値フィールド**
- 最大しきい値が最小しきい値を超え、ゼロでも負でもないことを保証する**検証メッセージ**
- 特定のパフォーマンスカテゴリに焦点を当てるための**選択/フィルターコントロール**

システム要件と通知

Citrix Workspaceアプリのバージョン互換性

マップには、Citrix Workspaceアプリのバージョンが古いためにエンドポイントの位置情報が不足している場合に警告バナーが表示されます。

- **警告メッセージ:** 「古いWorkspaceアプリのバージョンのため、エンドポイントの位置情報が不足しています。」
- **解決策:** 最新のWorkspaceアプリバージョンにアップグレードすると、完全な地理的データ収集が保証されます。
- **詳細情報:** バナーには、バージョン要件に関する追加情報が記載されたドキュメントへのリンクが含まれています。

構成オプション

パフォーマンスしきい値の設定

- マップビューの左下にある凡例パネルを見つけます。
- 中程度のパフォーマンスカテゴリにカスタム値を入力します。
    - 最小しきい値 (デフォルト: 61秒)
    - 最大しきい値 (デフォルト: 120秒)

- 低カテゴリは「未満」に自動的に調整されます。
- 高カテゴリは「超」に自動的に調整されます。
- 検証により、最大しきい値が最小しきい値を超え、どちらもゼロまたは負ではないことが保証されます。
- 変更されたしきい値はブラウザのキャッシュ（ローカルストレージ）に保存され、ブラウザ固有のものです。

時間範囲の設定

1. メトリックセクションの左上隅にあるドロップダウンメニューを使用します。
2. 希望する期間を選択します（デフォルト：「過去1時間」）。

マップとメトリックは、選択された期間のデータを反映するように自動的に更新されます。

マップビューの使用方法

マップビューは以下の目的で使用できます。

地域ごとのパフォーマンスのトラブルシューティング

1. 主に赤色（高）のログオン期間インジケーターが表示されている地域を特定します。
2. それらの地域にサービスを提供するインフラストラクチャコンポーネントと関連付けます。
3. 影響を受ける地理的領域に対して、ターゲットを絞った最適化を実装します。

キャパシティプランニング

1. さまざまな地域の円のサイズを観察して、接続密度パターンを確認します。
2. 追加のリソースを必要とするトラフィックの多い地理的領域（より大きな円）を特定します。
3. 地域ごとの使用パターンに基づいてインフラストラクチャのスケーリングを計画します。

グローバル展開の評価

1. メトリックパネルを使用して、展開の規模（合計接続数、ユニークユーザー数）を把握します。
2. 異なる地理的地域間でのログオンパフォーマンスを比較します。
3. 異なる場所のベースラインパフォーマンスの期待値を設定します。

しきい値の最適化

1. マップ上の緑、オレンジ、赤のインジケーターの分布を確認します。

2. 特定の環境で許容されるパフォーマンスをより適切に反映するようにしきい値を調整します。
3. 実際のユーザーエクスペリエンスに基づいて、より意味のあるパフォーマンス分類を作成します。

トラブルシューティング

不足している地理データ

警告バナー「古いWorkspaceアプリのバージョンが原因でエンドポイントの位置情報の詳細がありません」が表示された場合：

1. 古いバージョンのCitrix Workspaceアプリを使用しているユーザーを特定します。
2. 最新のCitrix Workspaceアプリバージョンへの段階的なアップグレードを計画します。
3. 地理データが最も重要となる地域でのアップグレードを優先します。

パフォーマンス分類の問題

パフォーマンスカテゴリが不正確に表示されているように見える場合：

1. 凡例パネルで現在のしきい値設定を確認します
2. 必要に応じて、中カテゴリの最小値と最大値を調整します
3. しきい値が、お使いの環境の実際のパフォーマンス特性と期待値に合致していることを確認します

データ更新の問題

データが古いように見える場合：

1. 「Data updated every 5 minutes」インジケーターで最終更新時刻を確認します。

> **注:**
>
> 過去1週間、自動更新は無効になっています。最新のデータを取得するには、手動で更新してください。

1. 選択した時間範囲がトラブルシューティング期間と一致していることを確認します。
2. 利用可能な場合は、 ボタンを使用してデータを手動で更新します。

ベストプラクティス

- インフラストラクチャの改善に基づいて、パフォーマンスしきい値を定期的に確認および調整します。
- **View top locations** オプションを使用して、接続ボリュームが最も多い領域に焦点を当てます。
- インフラストラクチャの変更前と変更後の地理的なパフォーマンスパターンを比較します。
- 最適な運用期間中に、地域ごとのパフォーマンスのベースラインレポートを作成します。
- パフォーマンスの期待値を設定する際には、地域ごとのネットワーク状況を考慮してください。
- 完全なデータ収集のために、最新のCitrix Workspaceアプリバージョンへのアップグレードについてユーザーに周知してください。
- セッションパフォーマンスにおける新たな傾向を特定するために、定期的に**マップビュー**を確認してください。

シトリックス エイドリアン

Director向けCitrix Aidrien統合は、オンプレミスDirector環境とCitrix Cloud間の合理化されたブリッジを提供します。(/ja-jp/citrix-aidrien.html)は、Citrix Cloud内で利用可能なAI搭載サービスで、CitrixおよびNetScalerソリューションの製品内サポートと支援を提供するように設計されています。

Citrix Aidrienを使用すると、管理者は自然言語で質問し、CitrixおよびNetScalerソリューションに関するCitrix公開ドキュメントで強化された即時応答を受け取ることができます。

管理者がDirectorで**Citrix Aidrien**ボタンをクリックすると、Citrix Cloudインターフェイスにリダイレクトされます。管理者はCitrix Cloudユーザー資格情報を使用して認証し、Citrix Aidrienでの作業を続行できます。

Citrix AidrienおよびCitrix Directorでサポートされているユースケースの詳細については、(/ja-jp/citrix-aidrien.html)を参照してください。

前提条件

DirectorでCitrix Aidrien統合を使用する前に、次の要件が満たされていることを確認してください。

- 管理者は、Citrix Aidrienにアクセスするための適切な権限を持つ有効な**Citrix Cloudアカウント**を所有している必要があります。

- **Citrix Aidrienが有効になっている**こと、および管理者にアクセス権が付与されていること。詳細については、(/ja-jp/citrix-aidrien.html#manage-access-to-citrix-aidrien)を参照してください。

> **注:**

> オンプレミスDirector向けのCitrix Aidrien統合は、**Citrix公開ドキュメントのみ**を使用し、環境固有のコンテキストはサポートしていません。

> DirectorでCitrix Aidrien統合を使用する前に、次の要件が満たされていることを確認してください。

- 管理者は有効なCitrix Cloudアカウントを所有している必要があります。詳細については、(/ja-jp/citrix-cloud/citrix-cloud-management/identity-access-management/add-admins.html)を参照してください。
- Citrix CloudでCitrix Aidrienが有効になっていることを確認してください。詳細については、(/ja-jp/citrix-aidrien.html#enable-citrix-aidrien-in-citrix-cloud)を参照してください。
- 管理者はCitrix Aidrienにアクセスするための有効な権限を持っている必要があります。詳細については、(/ja-jp/citrix-aidrien.html#administrator-access-to-citrix-aidrien)を参照してください。

> **注:**

> 1. オンプレミスDirector向けのCitrix Aidrien統合は、Citrix公開ドキュメントのみを使用し、環境コンテキストはサポートしていません。
> 2. Citrix Directorは、Directorコンソールを使用するすべての管理者に対してAidrienボタンを表示します。

はじめに

Director から Citrix Aidrien を使い始めるのは簡単です。

1. 管理者として Citrix Director にサインインします。
2. Director UI の右上隅にある Citrix Aidrien ボタンを見つけてクリックします。
3. Citrix Cloud サインインページにリダイレクトされます。
4. Citrix Cloud のユーザー資格情報を使用して認証します。

5. サインインが成功すると、Citrix Aidrien が Citrix Cloud で開き、ワークフローを続行できます。
6. 前提条件を満たしていれば、Director で追加のセットアップや構成は必要ありません。

セッションスコアのメトリック

前提条件

uberAgent lite を介したセッションスコアは、VDA バージョン 2511 以降で利用可能です。この機能は、CU2 を介して LTSR 2507 にもバックポートされています。

概要

セッションの詳細には、セッションのパフォーマンスをトラブルシューティングし、全体的なセッションの健全性を分析するための追加のデータポイントが含まれるようになりました。追加データは、個々のセッションの全体的なユーザーエクスペリエンスに関する洞察を提供し、管理者がパフォーマンスの低いセッションの原因を理解するのに役立ちます。

1. セッションエクスペリエンスの概要 – これはセッションエクスペリエンスを素早く確認するのに役立ちます。選択した期間中に環境内で起動されたすべてのセッションにおけるユーザーエクスペリエンスの概要を表示します。分析されたセッションは、良好、中程度、不良に分類されます。管理者はエクスペリエンスカテゴリをクリックして、自動的にフィルターが適用された詳細なセッションビュー（フィルターページ）を開くことができます。
2. セッションとコンポーネントのスコア – セッションの概要には、分析されたセッションの平均セッションスコアとコンポーネントスコアも表示されます。単独の平均スコアは非常に有用な指標ではないかもしれませんが、ほとんどのセッションのセッションエクスペリエンスの良好な指標として機能します。同様に、管理者は平均コンポーネントスコアを使用して、不良セッションの潜在的な根本原因を理解できます。
3. セッション分布 – フィルターページにセッション分布チャートが追加されました。管理者は、エンドポイントの国、都市、エンドポイントOS、CWAバージョン、ISPなどでセッション分布を表示できます。
4. パフォーマンストレンド – フィルターページには、セッションパフォーマンストレンドチャートも追加されました。パフォーマンスチャートは、セッションとコンポーネントのパフォーマンストレンドを分析し、時刻、国などに基づいて繰り返されるパターンを特定するのに役立ちます。
5. 個々のセッションデータ – セッション詳細テーブルの各セッションに、以下のデータポイントが追加されました。

a. セッションスコア

b. CPUスコア

c. RAMスコア

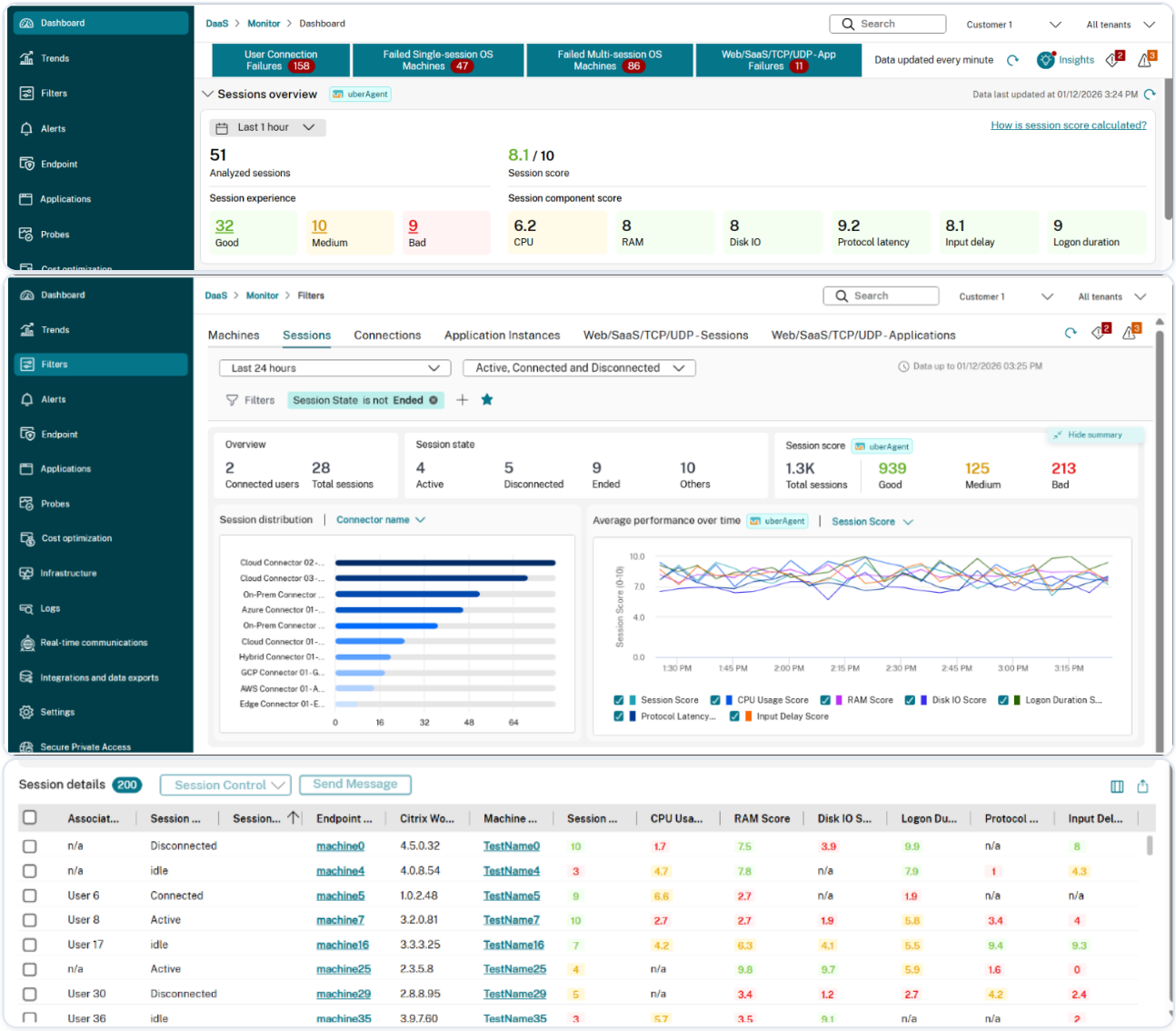
d. ディスクIOスコア

e. プロトコル遅延スコア

f. 入力遅延スコア

g. ログオン期間スコア

エクスペリエンススコアの計算の詳細については、エクスペリエンススコアを参照してください。



Directorでのエンドポイントセキュリティポリシーの有効化と脅威検出レポート

Citrix Workspaceアプリは、手動設定なしでエンドポイントで有効になっているMicrosoft Recallなどの高リスクな状態を自動的に検出する組み込みのセキュリティチェックを導入しています。このような検出のリアルタイムな可視性は、Citrix DirectorおよびMonitorで利用可能になります。このレポート機能により、管理者はリスクを迅速に評価し、より安全な環境を確保するために保護ポリシーを設定できるようになります。Recallのような特定のイベントの検出は自動ですが、イベントからの保護には、管理者によるアプリ保護ポリシーの手動設定が必要です。有効になっているすべてのポリシーのアクティベーションイベントも、DirectorおよびMonitorで報告されます。プロアクティブなリスク管理とポリシーの再構成を利用することで、管理者は環境内のエンドポイントセキュリティを強化し、新たな脅威への露出を減らすことができます。

Directorでは、以下のレポート機能が利用可能になります。

- **監査証跡**
    - **自動検出** – デフォルトのスキャン中に、CWAはエンドポイント上のWindows Recallのような様々な脅威を検出します。脅威が検出された場合、CWAはDirectorにイベントを送信します。各イベントについて、以下のデータが報告されます。
        - タイムスタンプ
        - ユーザー名
        - エンドポイント名
        - エンドポイントOS
        - CWAバージョン
        - イベント名
        - イベントタイプ – 検出または保護
- **構成済みポリシーの保護** – 管理者は、スクリーンキャプチャ、DLLインジェクション、キーロギングなどの特定のイベントを防ぐために保護ポリシーを構成できます。スクリーンキャプチャ防止ポリシーは、Recallによるスクリーンキャプチャの試行も防ぐために使用できます。Directorで報告される保護イベントには、上記のすべてのデータポイントが含まれます。
- **集約されたインサイトと傾向** – イベントデータは集約され、以下の情報が報告されます。
    - 環境の検出/保護の概要、,
    - 上位の保護/検出イベント、および
    - 時間経過に伴う保護および検出イベントの傾向

この機能は、組織が新たな脅威を特定し、リアルタイムで対応できるよう支援することで、アプリケーションを安全に提供するというCitrixのコミットメントをさらに強化するように設計されています。

管理者は、上記のインサイトを使用して、環境内のセキュリティ「脅威」をよりよく理解し、機密データを保護し、セキュリティリスクを最小限に抑え、そのようなリスクを軽減するために設計された関連する企業レベルのポリシーの確立をサポートするための保護ポリシーを設定できます。(例: リコール、キーロガーなどのツールの使用を推奨しない)

Citrix DaaS™ MCP サーバー ローカル

Citrix DaaS MCPサーバーは、MCP対応のAIエージェントがオンプレミスのCitrix Virtual Apps and Desktops™ Delivery Controller™ (DDC) に接続できるようにします。接続後、管理者は互換性のあるAIクライアントを介して、自然言語を使用してサイト情報のクエリ、セッションとマシンの問題の調査、およびパフォーマンスメトリックの取得を行うことができます。

このサーバーは、デリバリーグループ、マシンカタログ、VDAマシン、セッション、ユーザー、エンドポイント、およびサイト全体の概要をカバーする20個の読み取り専用ツールを公開しています。すべてのツールは読み取り専用であり、DDCまたはサイトに対して書き込み操作は実行されません。

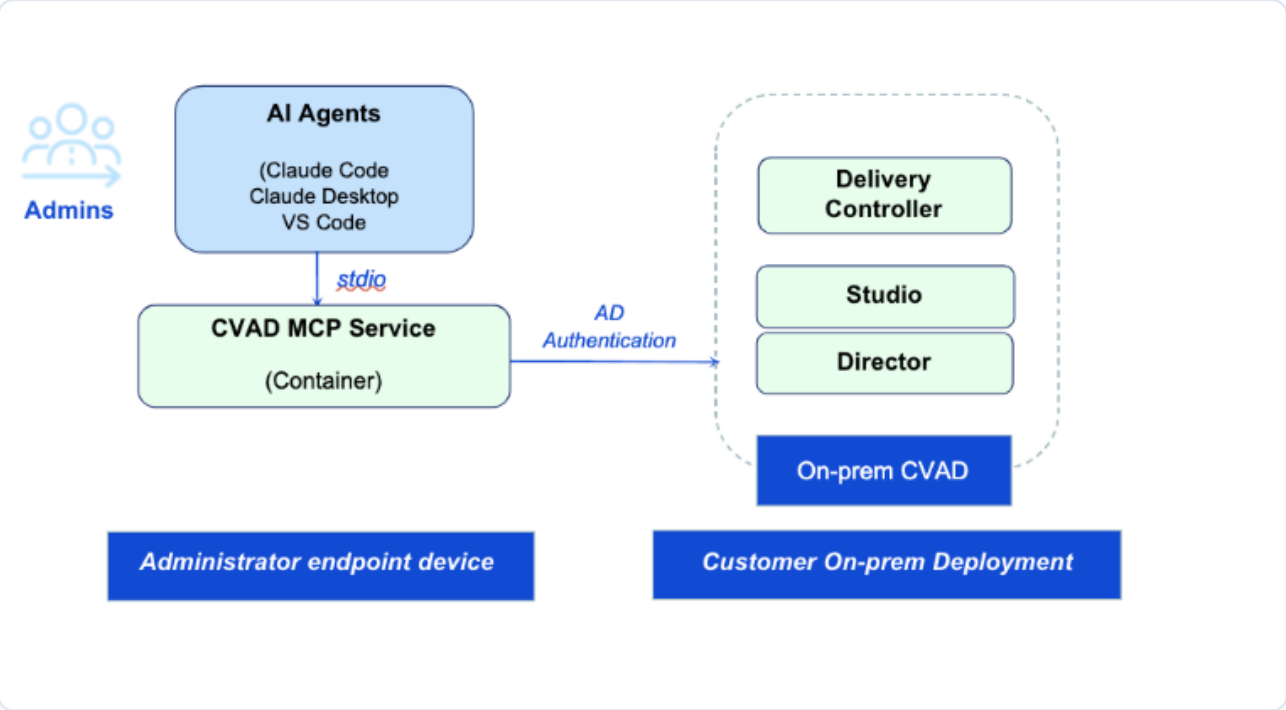
Citrix DaaS MCPサーバーが接続された後、次のような自然言語クエリを使用します。

- 「このサイトのすべてのデリバリーグループを一覧表示」
- 「メンテナンスモードのマシンを表示」
- 「ユーザーjohn.smithが現在持っているセッションは何ですか？」
- 「過去24時間のユーザーjane.doeの接続失敗を表示」
- 「マシンVDA-01のリソース使用状況と健全性はどうなっていますか？」
- 「最も負荷の高いマルチセッションマシンはどれですか？」
- 「ユーザーjohn.smithのログオンの内訳を表示」
- 「すべてのグループポリシーとその設定を一覧表示」
- 「どのようなハイパーバイザー接続が構成されていますか？」
- 「接続失敗とセッション数の時間ごとの概要を表示」

動作の仕組み

Citrix DaaS MCP Server Localは、AIエージェントが外部ツールやデータソースとどのように連携するかを定義するオープンプロトコルであるModel Context Protocol (MCP)を使用します。このプロトコルはクライアント/サーバーアーキテクチャに従います。

- **ホスト** - AIエージェントを実行するアプリケーション (例: Claude Code、MCP拡張機能付きのVS Code)。
- **クライアント** - ホスト内でMCPサーバーに接続し、ツールを呼び出すコンポーネント。
- **サーバー** - Delivery Controllerを照会するためのツールを公開するCitrix DaaS MCP Server Local。



サーバーはWindowsマシン上のPodman/Dockerコンテナ内で起動され、ネットワーク経由でDDCと通信します。管理者が自然言語クエリを発行すると、AIクライアントはそれをツール呼び出しに変換し、Citrix DaaS MCP ServerはDDC内のデータソース (StudioまたはDirector) に対してクエリを実行し、結果は表示のためにAIクライアントに返されます。

セキュリティと認証

Citrix DaaS MCP Server Localは、ドメイン管理者資格情報を使用してDelivery Controllerで認証します。これらの資格情報は初期構成設定中に提供され、サーバーがインストールされているマシンにローカルに保存されます。

主なセキュリティ特性:

- **暗号化された資格情報ストレージ** - 管理者資格情報はWindows資格情報マネージャー (OS資格情報チェーン) に保存され、ログインしているユーザーのWindowsアカウントによって保護されます。サーバーを構成したユーザーのみが、保存された資格情報にアクセスできます。
- **読み取り専用アクセス** - すべてのツールは読み取り専用ツールです。サーバーは、Delivery Controller上またはCitrix Virtual Apps and Desktopsサイト内でリソースを作成、変更、または削除しません。
- **ローカル実行** - サーバーは管理者のマシン上でローカルに実行されます。ネットワークエンドポイントを公開したり、インバウンド接続を受け入れたりすることはありません。
- **資格情報のスコープ** - サーバーは、構成されたDDC管理者資格情報をすべてのクエリに使用します。ツール結果は、構成されたアカウントの権限を反映します。
- **データ流出なし** - クエリ結果はローカルのAIクライアントにのみ返されます。MCPサーバーは外部サービスにデータを送信しません。

> **注:**
>
> Citrix DaaS MCP Server Localは、組織内の管理者による使用を目的としています。マシンまたはAIクライアントが不正なユーザーにアクセス可能な環境では使用しないでください。

> **注:**
>
> 物理マシン上、またはネストされた仮想化が有効になっている仮想マシン内でWindows 11を使用することを強くお勧めします。

サポートされているAIクライアント

以下のAIクライアントは、Citrix DaaS MCP Server Localで検証済みです。

AIクライアント	注
Claudeコード	CLIベースのAIエージェントです。Claude Codeの設定で、`citrix-daas-mcp-local`をMCPサーバーとして追加します。

上記にリストされていないクライアントから接続するには、クライアントがstdioトランスポートを備えたModel Context Protocol (MCP)をサポートしている必要があります。MCPサーバーの追加手順については、クライアントのドキュメントを参照してください。

前提条件

- Windows 11 オペレーティングシステム
- Node.js 18以降 (20 LTSを推奨)
- 同じマシンにインストールされているMCP対応AIクライアント
- マシンからCitrix® Delivery Controllerへのネットワーク接続
- サイトでCitrix管理者ロールを持つドメインユーザーアカウント
- シトリックス バーチャル アプリケーションズ アンド デスクトップ 2402 LTSR 以降

> **注:**
>
> Citrix DaaS MCP Server Localは、Citrix DirectorおよびStudioと同じ基盤となるソースからデータを取得します。DirectorまたはStudioの機能に適用される最小要件または前提条件は、MCPサーバーを通じて利用可能な対応するデータにも適用されます。Directorでデータを表示するために特定のVDAバージョン、Citrix Virtual Apps and Desktopsリリース、または構成が必要な機能の場合、サポートされているツールでMCPを通じてそのデータを利用できるようにするには、同じ要件を満たす必要があります。

はじめに

Node.jsのインストール

`node -v`がすでにv18以上を報告している場合は、このセクションをスキップしてください。NVM for Windowsを使用してNode.jsをインストールします。すべてのコマンドはPowerShellで実行してください。

ステップ1: NVMがインストールされているか確認する

次のコマンドを実行します。

```
nvm version
```

バージョン番号が表示された場合、NVMはすでにインストールされています。ステップ2に進んでください。コマンドが認識されない場合は、NVM for Windowsをインストールしてください:

```
winget install -e --id CoreyButler.NVMforWindows
```

インストール後にPowerShellを再起動し、`nvm`がPATHで利用できるようにします。

ステップ2: Node.js 20をインストールして選択する

```
nvm install 20

nvm use <exact_version>
```

> **注:**
>
> `<exact_version>`を、インストールされている実際のバージョン（例: 20.15.1）に置き換えてください。

ステップ3: インストールを確認する

次のコマンドを実行し、それぞれがバージョン番号を返すことを確認してください:

```
nvm version

node -v

npx -v
```

> **注:**
>
> `node -v`はv18以上を報告する必要があります。

Citrix DaaS MCP Server Localをインストールして構成する

ステップ1: バンドルファイルを入手する

Citrixダウンロードページから Citrix DaaS MCP Server Localバンドルファイルをダウンロードします。

ステップ2: 構成コマンドを実行する

PowerShellを管理者として開きます。バンドルファイルを含むフォルダに移動し、以下を実行します:

```
npx -y .\citrix-daas-mcp-local-bundle-<version>.tgz config
```

`<version>`を、ダウンロードしたバンドルファイルのバージョン番号に置き換えてください。

ステップ 3: 対話型プロンプトを完了する

config コマンドは、以下の環境詳細を要求します:

プロンプト	説明
Citrix DDC ホスト	Delivery Controller のホスト名。
シトリックス DDC IPアドレス	Delivery Controller の IP アドレス。
管理者ユーザー	DDC 上で権限を持つドメイン管理者アカウント (例: `domain\username`)。
パスワード	管理者アカウントのパスワード。

注:

コンテナランタイムがインストールされていないマシンでは、config コマンドが自動的にインストールします。インストール中に再起動を求められた場合は、マシンを再起動し、config コマンドを再実行してください。

ステップ 4: インストールを確認する

config コマンドは、構成が完了すると組み込みのセルフテストを実行します。セルフテストがエラーなしで完了した場合、サーバーは使用準備ができています。

MCP サーバーを AI クライアントに接続する

インストール後、MCP対応AIクライアントを`citrix-daas-mcp-local`サーバーに接続するように構成します。MCPサーバーの追加手順については、AIクライアントのドキュメントを参照してください。

> **注:**
>
> Claude Code はステップ 3 で自動的に構成されます。他の AI クライアントでは手動構成が必要になる場合があります。

その他のAIクライアントの場合（手動セットアップ）

別のMCP対応クライアントを使用している場合は、インストーラーが提供する出力を使用して、サーバー構成を手動で追加する必要があります。

1. **構成の特定** - インストールプロセスの最後に、ターミナルで****というタイトルのセクションを探します。
2. **JSONのコピー** - セットアップスクリプトは、お使いのマシン用の正確なファイルパスを含むカスタムJSONスニペットを自動的に生成します。このJSONブロック全体をコピーします。
3. **クライアントの更新** - コピーしたJSONをAIクライアントのMCP構成ファイルに貼り付けます（正確なファイルの場所については、お使いのクライアントのドキュメントを参照してください）。
4. **再起動** - AIクライアントを再起動するか、新しいチャットセッションを開始して、新しいMCPサーバー構成をロードします。

コピーする生成された構成ブロックの例：

```
{

  "citrix-daas-mcp-local": {

    "command": "C:\\path\\to\\node.exe",

    "args": [

      "C:\\path\\to\\daas-mcp-local\\cli.js",

      "run"

    ],

    "env": {

      "DAAS_MCP_LOCAL_CONFIG": "C:\\path\\to\\config.json"
```

```
    }
  }
}
```

接続したら、サーバーがロードされ、そのツールが利用可能であることを確認します。「このサイトのデリバリーグループを一覧表示してください」のような自然言語クエリを発行してテストできます。

共通のツールパラメーター

いくつかのツールは共通の入力パラメーターを共有しています。次の表は、ツール間で受け入れられる入力形式について説明しています。

マシン名の形式

マシン名を受け入れるツールは、次の形式をサポートしています。

形式	例
正規 (DOMAIN\HOSTNAME)	`CTXCO\TestVDA1`
ホスト名のみ	`TestVDA1`
完全修飾ドメイン名 (FQDN)	`TestVDA1.ctxco.local`

指定された名前が単一のマシンと完全に一致しない場合、ツールはあいまい検索を試みます。複数のマシンが一致する場合、明確化応答に候補が一覧表示されます。

ユーザー名形式

ユーザー名を受け入れるツールは、`domain\username` 形式を使用します (例: `nkgdir\john.smith`)。検索ツールでは部分一致がサポートされています。

時間枠パラメーター

いくつかのツールは、データをどのくらい遡って取得するかを制御するために時間枠を受け入れます。

パラメーター	デフォルト	最大	使用元
`latest_hours`	2時間	2時間	`get_session_metrics`, `get_endpoint_metrics`
`offset_hours`	2時間	7日間	`get_connection_failures` (ユーザー別)

利用可能なツール

Citrix DaaS MCP Server Local は、20個のツールを領域別に公開しています。すべてのツールは読み取り専用であり、Delivery Controllerにクエリを実行し、リソースを変更することなくデータを返します。

サイトの概要

ツール	説明
`get_hourly_summaries`	タイプ別の現在の接続失敗数、タイプ別の失敗したVDIおよびRDSマシンの数、および過去1時間の接続セッションアクティビティを取得します。
`get_hypervisors_info`	すべてのハイパーバイザー接続を一覧表示するか、特定のハイパーバイザーの詳細構成を取得します。
`get_group_policy_list`	サイトグループポリシーリスト（ポリシー名、優先度、有効状態、設定、およびフィルターを含む）を取得します。

デリバリー グループ

ツール	説明
`search_delivery_groups`	名前、メンテナンスモード、有効状態、共有の種類、およびセッションサポートでフィルターを適用して、デリバリーグループを検索して一覧表示します。

ツール	説明
`get_delivery_group_details`	名前またはIDで特定のデリバリーグループの詳細情報を取得します。

マシンカタログ

ツール	説明
`search_machine_catalogs`	名前、物理マシン、割り当てタイプ、プロビジョニングタイプ、およびセッションサポートでフィルターを適用して、マシンカタログを検索して一覧表示します。
`get_machine_catalog_details`	名前またはIDで特定のマシンカタログの詳細情報を取得します。

VDAマシン

ツール	説明
`search_vda_machines`	デリバリーグループ、マシンカタログ、エージェントバージョン、OSタイプ、タグ、メンテナンスモード、電源状態、登録状態、セッション状態、および障害状態でフィルターを適用して、マシンを検索します。
`get_vda_machine_details`	特定のVDAマシンに関する詳細情報を名前またはIDで取得します。
`get_vda_machine_resource_usage`	異常検出、飽和パターン検出、および実用的な推奨事項のために、統計プロファイリング（平均、P95、最大）を含むヘルスアセスメントでマシンリソース使用率メトリックを分析します。
`list_top_vda_machines_by_load_index`	有効な負荷インデックスでランク付けされた、最も負荷の高いマルチセッションOS VDAマシンを一覧表示します。

セッション

ツール	説明
`search_sessions`	ユーザー、マシン、デリバリーグループ、マシンカタログ、エージェントバージョン、OSタイプ、セッション状態、セッションサポート、および使用中のアプリケーションでフィルターを使用してセッションを検索します。
`get_session_details`	セッションIDで特定のセッションの完全な詳細を取得します。
`get_session_metrics`	過去2時間以内のユーザーまたはセッションのセッションパフォーマンスメトリックを取得します。時間間隔内のメトリックのギャップは、その期間中のセッション切断を示している可能性があります。
`get_session_logon_breakdown_metrics`	ユーザーのログオン期間の内訳メトリックを取得し、各ログオンステップの期間、開始時刻、終了時刻を表示します。

ユーザーとエンドポイント

ツール	説明
`get_active_machines_by_user`	ユーザーが現在アクティブなセッションを持っているVDAマシンを、マシン名、DNS名、IPアドレス、エージェントバージョンを含めて一覧表示します。
`get_active_users_by_machine`	特定のマシンでアクティブなセッションを持つユーザーを、ユーザー名、UPN、フルネーム、ドメインを含めて一覧表示します。
`get_endpoint_metrics`	過去2時間以内のユーザーまたはセッションのエンドポイント（クライアント）デバイスメトリックを取得します。
`get_connection_failures`	ユーザーの失敗した接続試行（過去7日まで）またはトランザクションIDによる失敗した接

ツール	説明
	続試行（90日まで）を、失敗理由と失敗時のマシンステータスを含めて取得します。

高度なクエリ

ツール	説明
`run_dynamic_odata`	CVAD Monitor ODataサービスに対してカスタムODataクエリを実行します。最大10,000行までの自動ページネーションをサポートします。
`get_odata_reference`	AIクライアントにCitrix Monitor ODataドキュメントを取得するよう指示します。オンラインドキュメントが利用できない場合、ツールはイメージにバンドルされている参照ドキュメントにフォールバックします。

構成を更新する

設定（DDCホスト、管理者資格情報など）を変更するには、configコマンドを再実行します。

```
npx -y .\citrix-daas-mcp-local-bundle-<version>.tgz config
```

既知の制限事項

制限事項	詳細
セッションとエンドポイントのメトリックウィンドウ	`get_session_metrics`と`get_endpoint_metrics`は、過去2時間分のデータのみを返します。
接続失敗の遡及期間	`get_connection_failures`は、ユーザー名ごとに最大7日間をサポートします。
OData行数制限	`run_dynamic_odata`は、クエリごとに最大10,000行を返します。
オーケストレーションツールの制限	構成の詳細を取得するツールには最大500の制限があります。マシンおよびセッションのリストは切り捨てられる場合があります。

制限事項	詳細
シングルサイト接続	サーバーは一度に1つのCitrixサイトに接続します。別のサイトを照会するには、configコマンドを再実行し、そのサイトのDelivery Controllerを指定してください。
ローカル実行のみ	サーバーはAIクライアントと同じマシンで実行する必要があります。リモートまたはホストされたMCPサーバーの展開はサポートされていません。

トラブルシューティング

Citrix DaaS MCP Server Localには、問題診断用のdoctorコマンドが含まれています。サーバーが期待どおりに動作しない場合は、これを実行してください。

```
npx -y .\citrix-daas-mcp-local-bundle-<version>.tgz doctor
```

doctorコマンドは、サーバー操作の各段階を検査し、失敗した段階と修復手順を報告します。

configコマンドの成功後、Citrixツールまたはcitrix-daas-mcp-local MCPサーバーが見つからない、またはブロックされている?

解決策:

- Claude Code以外のAIクライアントの場合、MCPサーバーを手動で構成します。詳細については、その他のAIクライアント向け（手動セットアップ）を参照してください。
- AIクライアントがMCP許可リストを適用している場合、`citrix-daas-mcp-local`が許可されていることを確認してください。詳細については、AIクライアントのドキュメントを参照してください。
- AIクライアントを再起動するか、新しいセッションを開始してください。

インストール後にNVMが認識されない?

解決策:

- PowerShellを閉じて再度開いてください。
- NVMがPATH上にあることを確認するには、`nvm version`を実行してください。
- それでも認識されない場合は、マシンを再起動して再度試してください。

Node.jsのバージョンが18未満?

解決策:

- Node.js 20をインストールするには、`nvm install 20`を実行してください。
- インストールされているバージョンに切り替えるには、`nvm use <exact_version>` を実行します。
- `node -v` で確認します。

コンテナランタイムのインストールが構成中に失敗?

解決策:

- マシンにDocker DesktopまたはPodmanを手動でインストールします。
- コンテナランタイムが利用可能になったら、構成コマンドを再実行します。

システム起動後にコンテナランタイムが準備できていません?

解決策:

- コンテナランタイムの起動が完了したら、MCPサーバーに再接続します。

複数のコンテナが実行されています?

解決策:

- 不要になったAIクライアントセッションをすべて閉じます。対応するコンテナは自動的に停止されます。

サーバーが応答しない、またはエラーを返す?

解決策:

- doctorコマンドを実行し、報告された修復に従います。
- DDCへのネットワーク接続を確認します（このマシンからDDCのホスト名とIPに到達可能であることを確認します）。
- 管理者資格情報が正しく、必要な権限を持っていることを確認します。

AIクライアントでツールが読み込まれない?

解決策:

- サーバーがAIクライアントのMCPサーバーリストに接続済みとして表示されていることを確認します。

- サーバーを追加した後、AIクライアントセッションを再起動します。
- サーバー構成が有効であることを確認するために、doctorコマンドを実行します。
- Node.js 18以降がインストールされており、PATHで利用可能であることを確認します。

クエリが空の結果を返す、または予期しないエラーが発生する?

解決策:

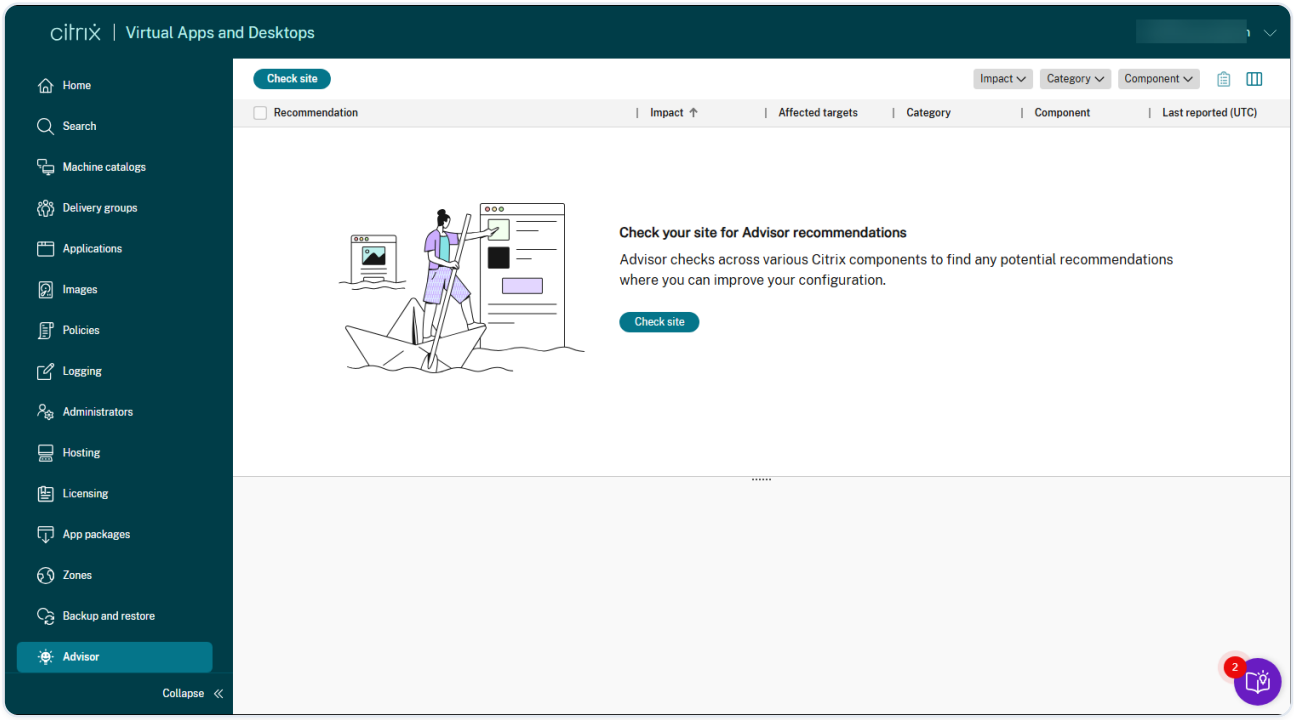
- このマシンからDDCに到達可能であることを確認します。
- 構成された管理者アカウントがDDCに必要な権限を持っていることを確認します。
- Delivery Controllerサービスが実行されていることを確認します。
- 完全な診断のためにdoctorコマンドを実行します。

コマンドリファレンス

コマンド	目的
`npx -y .\citrix-daas-mcp-local-bundle-<version>.tgz config`	サーバーとコンテナランタイムをインストールまたは再構成します。初回インストール時にセルフテストを実行します。
`npx -y .\citrix-daas-mcp-local-bundle-<version>.tgz doctor`	サーバー構成または接続の問題を診断します。

アドバイザー

Citrix Advisor は、Citrix Virtual Apps and Desktops の展開を最適化し、その全体的な健全性と準備状況を向上させるのに役立つサービスです。環境チェックを自動化し、実用的な推奨事項を提供することで、構成の問題、非効率性、リソースの無駄、ベストプラクティスからの逸脱などをプロアクティブに特定できるようにします。



注:

- このサービスは、**フル管理者**のみが利用できます。
- ページの右上隅にあるフィードバックアイコンを使用して、フィードバックを送信することをお勧めします。

利点

Advisorを使用すると、次のことができます。

- **問題をプロアクティブに特定して解決する**: 潜在的な問題、構成のずれ、ベストプラクティスからの逸脱がユーザーに影響を与えたり、ビジネス運用を妨げたり、セキュリティを侵害したりする前に検出します。
- **環境のパフォーマンスと安定性を最適化する**: 構成を微調整し、リソース割り当てを最適化し、ベストプラクティスを実装して、Citrix展開の安定性、セキュリティ、およびパフォーマンスを向上させます。
- **運用を合理化し、オーバーヘッドを削減する**: 定期的なチェックを自動化し、複雑な修復タスクを簡素化し、ガイダンス付きの支援を受けることで、運用オーバーヘッドを削減し、管理リソースを解放します。
- **コストとリソース利用率を最適化する**: 過剰支出の領域を特定し、リソース最適化の機会を発見し、Citrixテクノロジーの効率的な利用を確保して、総所有コストを最小限に抑えます。
- **コンプライアンスとベストプラクティスへの準拠を維持する**: Citrix展開がCitrixのベストプラクティス、セキュリティ標準、および業界規制に準拠していることを確認し、リスクを軽減し、全体的なガバナンスを向上させます。
- **複雑なタスクを簡素化する**: 健全で最適化された環境をサポートするために、管理タスクを簡素化します。

推奨事項を確認する

Advisor の推奨事項についてサイトを確認するには、次の手順に従います。

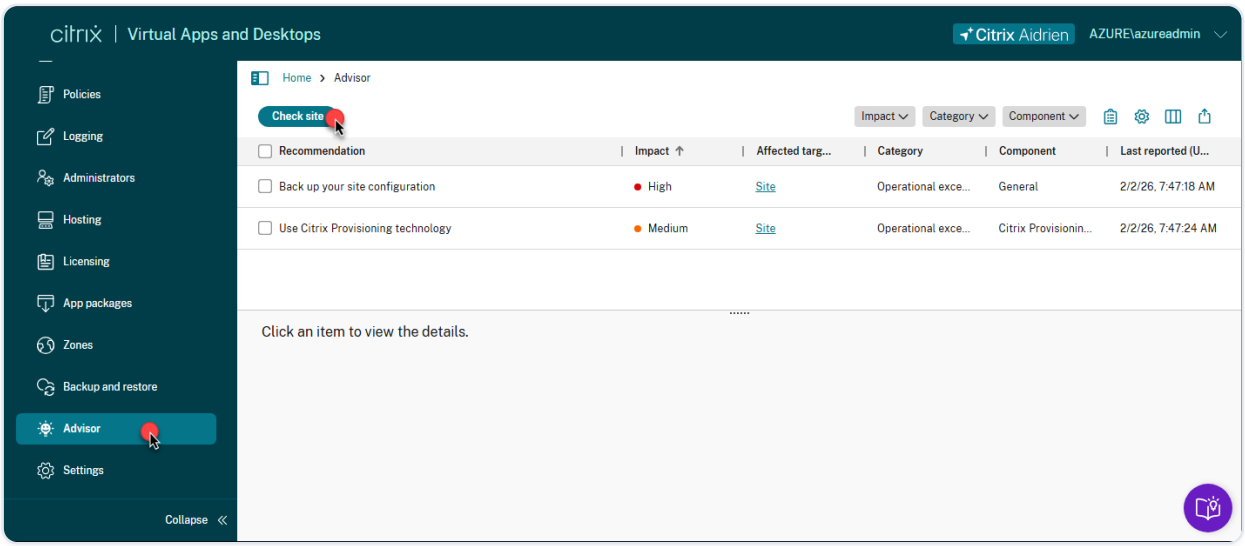
1. **フル管理者**ロールを持つアカウントを使用して Web Studio にサインインします。
2. 左側のペインで、**Advisor** を選択します。
3. **Check site** をクリックします。
4. **Check site** ページで、Advisor にチェックさせたいカテゴリを選択します。

カテゴリ	説明	参照
セキュリティ	セキュリティ侵害につながる可能性のある脅威や脆弱性を検出するための推奨事項。	セキュリティに関する推奨事項
信頼性	ビジネスに不可欠なアプリケーションの継続性を確保し、向上させるための推奨事項。	信頼性に関する推奨事項

カテゴリ	説明	参照
パフォーマンス	アプリケーションとデスクトップ全体のパフォーマンスを向上させ、エンドユーザーにより高速で応答性の高いエクスペリエンスを提供するための推奨事項。	パフォーマンスに関する推奨事項
運用上の卓越性	プロセスとワークフローの効率性、リソース管理性、および展開のベストプラクティスを達成するための推奨事項。	運用上の卓越性に関する推奨事項
コスト最適化	リソースの適正化、無駄の最小化、および実際の使用ニーズに合わせたキャパシティの調整により、全体的な支出を削減するための推奨事項。	コスト最適化に関する推奨事項

5. **チェックを実行**をクリックしてサイトチェックを実行し、現在の構成に基づいて更新された推奨事項を生成します。

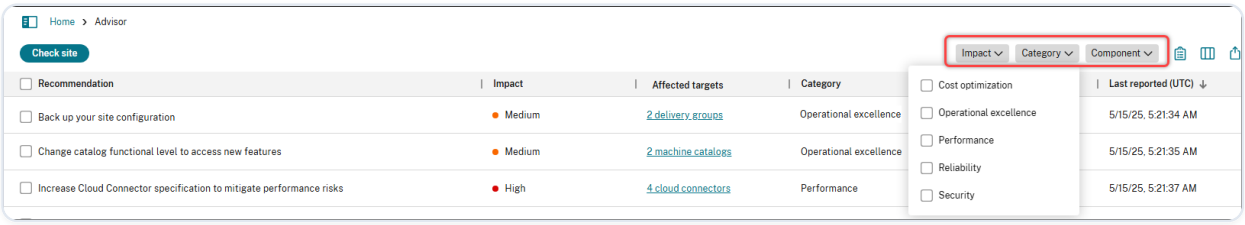
   すべての推奨事項がリストに表示されます。



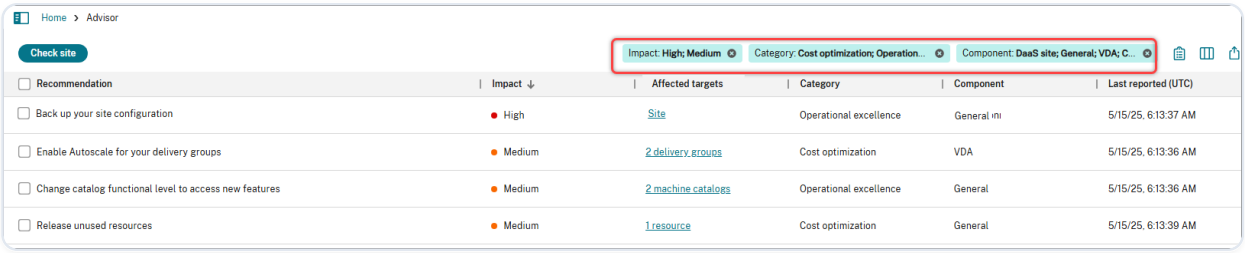
推奨事項のフィルタリング

デプロイメントに最も関連性の高い情報に焦点を当てるために、**影響**、**カテゴリ**、または**コンポーネント**で推奨事項をフィルタリングできます。

1. **Advisor**で、推奨事項リストの右上にあるフィルターを見つけます。



2. フィルター（例：**カテゴリ**）をクリックして、利用可能なオプションを表示します。
3. 1つ以上のチェックボックスを選択してフィルターを適用します。リストは自動的に更新され、選択内容に一致する推奨事項のみが表示されます。
4. 複数のフィルターを組み合わせて使用し、リストを絞り込みます。



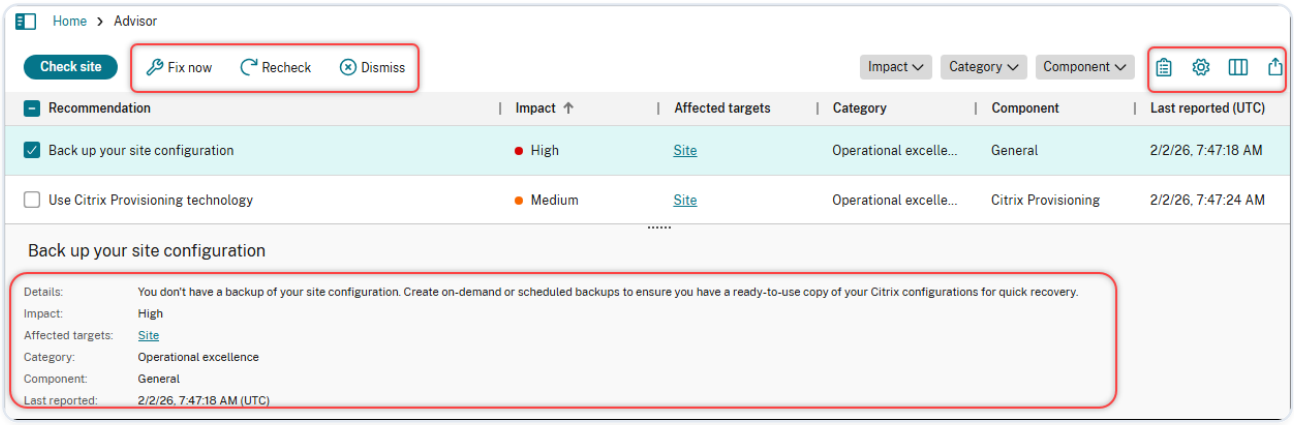
推奨事項を確認して対応する

推奨事項リストを使用して、デプロイメントにおける構成の問題と改善の機会を理解します。推奨事項に対して、次のアクションを実行できます。

- 推奨事項の詳細を表示する
- 推奨されるアクションを実装する
- 推奨事項を却下する
- 推奨事項内の特定の対象ターゲットを却下する
- チェックルールをカスタマイズする
- サイトチェックレポート全体を表示する

推奨事項の詳細を表示

推奨事項を確認するには、推奨事項を選択して下部ペインでその詳細を表示します。

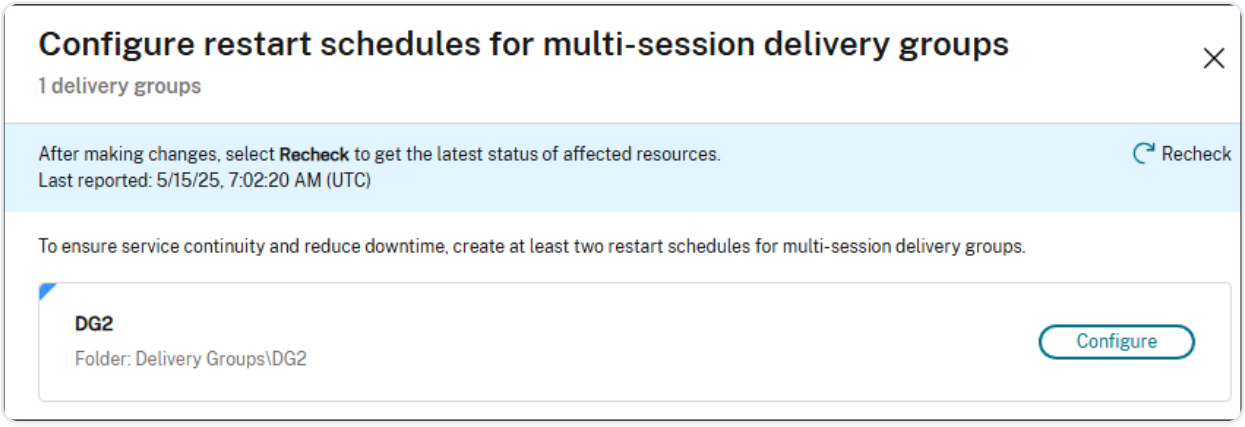


推奨されるアクションを実装する

推奨事項に対して推奨されるアクションを実装するには、次の手順に従います。

1. 推奨事項を選択します。
2. アクションバーで をクリックします。
3. 必要な更新を行うには、推奨される手順に従います。

   自動構成がサポートされていない、または実現不可能な場合、サポートドキュメントに誘導されることがあります。Advisor は、可能な限り UI 内で直接自動アクションを提供するように設計されており、手動設定の必要性を最小限に抑えることを目指しています。
4. 更新後、 をクリックして、影響を受けるターゲットのステータスを更新します。



注:

UI と手順は推奨事項によって異なります。表示されているスクリーンショットは説明のみを目的としています。

推奨事項を却下する

推奨事項が展開に関連しない場合、またはアクションを必要としない場合は、現在のリストおよび今後のチェック結果から削除できます。

1. レコメンデーションを選択します。
2. アクションバーの「**却下**」をクリックします。

> **ヒント:**
>
> 推奨事項を復元するには、推奨事項リストの右上隅にある**歯車**アイコンをクリックし、**却下されたアイテムの管理**を選択します。

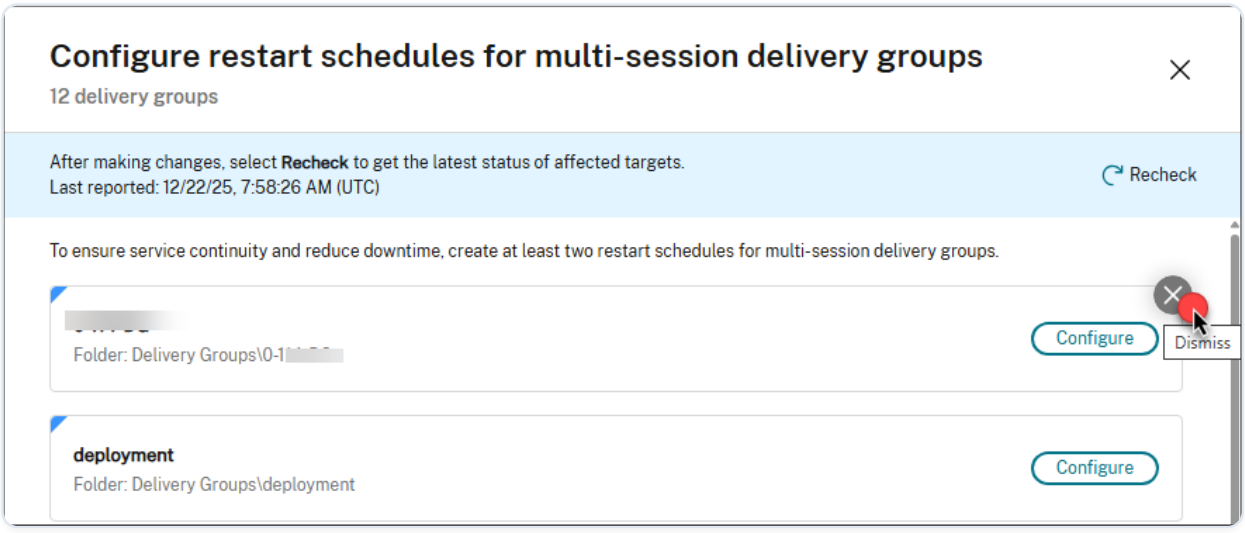
レコメンデーション内の特定の対象ターゲットを却下する

推奨事項に、意図的にベストプラクティスに準拠していない影響を受けるターゲット（*たとえば*、テスト、検証、または一時的なリソース）が含まれている場合、それらをこの推奨事項から削除できます（`granular dismissal` とも呼ばれます）。

> **注:**
>
> 詳細な却下は、マシンカタログ、デリバリーグループ、アプリケーショングループ、ゾーンのターゲットでのみサポートされています。

> 詳細な手順は次のとおりです。

1. レコメンデーションを選択します。
2. レコメンデーションの「**対象ターゲット**」フィールドをクリックします。レコメンデーションページにすべての対象ターゲットが表示されます。
3. 却下したい対象ターゲットにカーソルを合わせます。ターゲットの右上隅に「**却下**」アイコンが表示されます。



4. 「**却下**」アイコンをクリックします。却下確認ダイアログボックスが表示されます。
5. 必要に応じて却下のメモを入力し、「**却下**」をクリックします。対象ターゲットはレコメンデーションページから削除されます。

> **ヒント:**
>
> 推奨事項で却下されたターゲットを復元するには、推奨事項リストの右上隅にある歯車アイコンをクリックし、「**却下された項目を管理**」を選択します。

チェックルールをカスタマイズする

次の推奨事項について、Advisorチェックルールをカスタマイズできます。

- **Cloud Connectorハードウェアを強化する:** CPU、メモリ、ディスク使用量のしきい値を調整し、特定のディスクを除外します。
- **未使用のリソースを解放する:** マシンとアプリケーションのカスタムの未使用時間しきい値を定義します。
- **VDAのGPO構成を最適化する:** GPO処理時間のしきい値を変更します。

単一の推奨事項のチェックルールをカスタマイズするには、次の手順に従います。

1. 推奨事項を選択し、アクションバーで「**カスタマイズ**」をクリックします。



2. 「**カスタマイズ**」ページで、必要に応じてチェック設定を更新します。

3. **保存**をクリックします。変更は、次回チェックを実行したときに有効になります。

3つの推奨事項すべてのチェックルールを一元的な場所からカスタマイズするには、次の手順に従います。

1. 推奨事項リストの右上隅にある「**歯車**」アイコンをクリックし、「**ルールをカスタマイズ**」を選択します。3つの推奨事項が表示されます。
2. 推奨事項の横にある「**編集**」アイコンをクリックします。
3. 必要に応じてチェック設定を更新します。
4. 残りの推奨事項のチェックルールを更新するには、手順2〜3を繰り返します。
5. **保存**をクリックします。変更は、次回チェックを実行したときに有効になります。

サイトチェックの完全なレポートを表示する

完全なレポートには、最新のサイトチェックからのすべてのAdvisor推奨事項の概要が示されます。これには、合格、却下、未解決のチェックポイントが含まれており、DaaSサイトの全体的な健全性と最適化の機会を評価するのに役立ちます。

完全なレポートを表示するには、推奨事項リストの右上にある**完全なレポートを表示**アイコンをクリックします。

Advisorの完全なレポート(/en-us/citrix-virtual-apps-desktops/current-release/media/advisor-full-report.png)

Advisor チェックのために StoreFront™ をセットアップする

Citrix AdvisorのStoreFront関連の推奨事項には、追加のセットアップが必要です。Advisorチェックのために StoreFrontをセットアップするには、次の手順を実行します。

1. 対応する接続を作成して、StoreFront サーバーをインフラストラクチャ監視に追加します。詳細については、「インフラストラクチャ監視」を参照してください。
2. **手動接続**モードでStoreFront接続を構成する場合は、Citrix Infrastructure Monitoringバージョン2603以降がダウンロードおよびインストールされていることを確認してください。必要なバージョンがインストールされていることを確認するには：
    a. **Director > 設定**に移動します。
    b. **種類**が`StoreFront`である接続を見つけます。
    c. **バージョン**フィールドに`7.47`以上が表示されていることを確認します。

重要:

Advisorの推奨事項に基づいてStoreFront展開に変更を適用した後、同じ推奨事項を再確認する前に少なくとも6時間待ってください。この遅延により、Infrastructure Monitoringは更新されたテレメトリを収集および処理し、Advisorが最新のデータを評価できるようになります。

参照

このセクションでは、Citrix Advisorのすべての推奨事項をカテゴリ別に一覧表示し、その目的と影響を理解するのに役立てます。

セキュリティに関する推奨事項

推奨事項	ID	影響	コンポーネント	説明
サポート終了に達したVDAをアップグレードする	REC_001	高	VDA	一部のマシンは、サポート終了に達し、Citrixによってサポートされなくなったバージョンを使用しています。影響を受けるマシンを最新のLTSRまたはCR VDAバージョンにアップグレードしてください。
セキュリティグループにリソースを割り当てる	REC_016	中	全般	一部のリソースが個々のユーザーに割り当てられています。管理を効率化し、セキュリティを強化するために、セキュリティグループを介してのみ

推奨事項	ID	影響	コンポーネント	説明
				ユーザーアクセスを割り当てるのがCitrixのベストプラクティスです。デリバリーグループとアプリケーショングループのユーザー割り当てを再構成し、セキュリティグループのみを含めるようにしてください。
サポート終了に達したCitrix Workspaceアプリのバージョンをアップグレードする	REC_017	高	Workspace アプリ	一部のエンドポイントデバイスは、サポート終了に達したCitrix Workspaceアプリのバージョンを使用しています。サポート性とセキュリティのリスクを軽減するために、デバイスを最新のWorkspaceアプリバージョンにアップグレードしてください。バージョン管理の簡素化と自動更新の制御には、Global App Configuration Serviceを使用してください。さらに、ストアへのアクセスに

推奨事項	ID	影響	コンポーネント	説明
				最低限のWorkspaceアプリバージョンを強制するために、エンドポイント分析ソリューションの使用も検討してください。
ホスト接続にHTTPSを使用する	REC_039	中	全般	一部のホスト接続は現在、HTTPS ではなく HTTP で構成されています。ハイパーバイザーとの安全な通信を確保するには、これらの接続を HTTPS を使用するように更新してください。これには、ハイパーバイザーで HTTPS を有効にし、有効な TLS 証明書が配置されていることを確認する必要があります。
サポート終了に達したStoreFrontサーバーバージョンをアップグレードする	REC_043	高	StoreFront	一部のStoreFrontサーバーは、サポート終了（EOL）に達し、Citrixによってサポートされなくなったバージョンを実行していま

推奨事項	ID	影響	コンポーネント	説明
				す。安全でサポート可能な環境を維持するために、影響を受けるすべてのStoreFrontサーバーを最新のLTSRまたはCRバージョンにアップグレードしてください。
StoreFrontベースURLにHTTPSを使用する	REC_044	高	StoreFront	一部のStoreFrontベースURLは現在、HTTPSではなくHTTPで構成されています。ユーザーの資格情報と機密データを保護するために、StoreFrontサーバーと関連するロードバランサーをHTTPSを使用するように構成してください。ベースURLが「https://」で始まることを確認してください。これにより、すべての通信が暗号化され、中間者攻撃などのセキュリティ脅威を防ぐのに役立ちます。

推奨事項	ID	影響	コンポーネント	説明
StoreFront と Delivery Controller 間の通信に HTTPS を使用する	REC_045	高	StoreFront	StoreFront と Delivery Controller 間のトラフィックは現在、暗号化されていない HTTP 経由で送信されており、ユーザー資格情報がセキュリティ上の脅威にさらされる可能性があります。環境を保護するには、Delivery Controller で HTTPS を有効にし、StoreFront を構成して安全な接続を使用するようにします。

注:

StoreFront関連の推奨事項には追加のセットアップが必要です。詳細については、Advisor チェックのためのStoreFrontのセットアップを参照してください。

信頼性に関する推奨事項

推奨事項	ID	影響	コンポーネント	説明
マルチセッションデリバリーグループの再起動スケジュールを構成する	REC_004	高	VDA	一部のマルチセッションデリバリーグループでは、再起動スケジュールが構成されていませ

推奨事項	ID	影響	コンポーネント	説明
				ん。スケジュールされた再起動は、マルチセッションOS VDA全体の最適なパフォーマンス、安定性、およびリソースの可用性を維持するのに役立ちます。サービス継続性を確保し、ダウンタイムを削減するために、少なくとも2つの再起動スケジュールを作成してください。VDAを「偶数」と「奇数」などのグループにタグ付けすることで、タグ制限付きの再起動スケジュールを交互に設定します。
複数のVDAでアプリケーションをホストする	REC_006	高	VDA	一部の公開アプリケーションは単一のVDAでのみホストされており、サービス継続性に影響を与え、ダウンタイムのリスクにつながる可能性があります。可用性と信頼性を維持するために、各アプリケーションがデ

推奨事項	ID	影響	コンポーネント	説明
				リバリーグループ内の複数のVDAでホストされていることを確認してください。
カタログの機能レベルに合わせてVDAをアップグレードする	REC_008	高	VDA	一部のマシンは、最小カタログ機能レベルでサポートされていない以前のVDAバージョンを使用しており、登録できない可能性があります。登録の問題を回避するには、以前のVDAバージョンをカタログ機能レベルに合わせてアップグレードしてください。
StoreFrontストアの高度なヘルスチェックを有効にする	REC_036	中	StoreFront	一部のStoreFrontサーバー上の一部のストアで、高度なヘルスチェックが有効になっていません。StoreFrontは、高度なヘルスチェックの結果から得られる追加情報を使用して、ローカルホストキャッシュ (LHC) モードで起動要求が適切

推奨事項	ID	影響	コンポーネント	説明
				なリソースロケーション (ゾーン) に送信されるようにします。高度なヘルスチェックがないと、LHC モードで起動が失敗する可能性があります。Citrix環境の回復性を向上させるには、StoreFrontサーバー上のすべてのストアで高度なヘルスチェックを有効にしてください。
StoreFrontサーバーの冗長性を確保する	REC_042	高	StoreFront	一部の StoreFrontサーバーグループにはサーバーが1台しか含まれておらず、障害発生時に単一障害点となり、冗長性が不足しています。回復力を高めるには、サーバーグループに少なくとも2台の StoreFrontサーバーを展開し、ロードバランサーでそれらを前面に配置して、シームレスなフェイルオー

推奨事項	ID	影響	コンポーネント	説明
				バーと中断のないアクセスを確保してください。

注:

StoreFront関連の推奨事項には追加のセットアップが必要です。詳細については、Advisorチェックのための StoreFrontのセットアップを参照してください。

パフォーマンスに関する推奨事項

推奨事項	ID	影響	コンポーネント	説明
高リソース消費マシンの適切なサイジング	REC_023	中	VDA	一部のマシンは、高いCPUまたはメモリ使用率、あるいは高いセッション数など、パフォーマンスの負荷の兆候を示しています。これは、マシンがサポートするワークロードを処理するにはサイズが不足していることを示しており、ユーザーエクスペリエンスの低下やパフォーマンスの低下につながる可能性があります。マシンのサイズを変更して割り当てられた

推奨事項	ID	影響	コンポーネント	説明
				リソースを増やすか、パワーユーザーを高性能マシンを持つデリバリーグループに再配置することを検討してください。
PVSサーバーのリソース割り当てを評価する	REC_031	中	プロビジョニング	一部のCitrix Provisioning (PVS) サーバーは、高いCPUまたはメモリ使用率など、パフォーマンスの負荷の兆候を示しています。サーバーリソースの割り当てが不十分な場合、パフォーマンスの低下や起動時間の延長につながる可能性があります。必要に応じて、これらのPVSサーバーのCPUとメモリ割り当てを増やすことを検討してください。
PVSサーバーのリソース割り当てを増やす	REC_032	高	プロビジョニング	一部のCitrix Provisioning (PVS) サーバーは、CPUまたはメモリ使用率が危機的なレベルに達するなど、パフォーマンス

推奨事項	ID	影響	コンポーネント	説明
				の負荷の兆候を示しています。サーバーのリソース割り当てが不十分な場合、パフォーマンスの低下や起動時間の延長につながる可能性があります。必要に応じて、これらのPVSサーバーのCPUとメモリの割り当てを増やすことを検討してください。
PVSターゲットデバイスのライトキャッシュディスクサイズを評価する	REC_033	中	VDA	一部のCitrix Provisioning (PVS) ターゲットデバイスのライトキャッシュディスク使用量がしきい値に近づいています。パフォーマンスの問題やユーザーセッションの障害を回避するために、現在のライトキャッシュディスクサイズを評価し、必要に応じて増やしてください。
VDAのGPO構成を最適化する	REC_035	中	VDA	一部のユーザーセッションでは、ログオン中

推奨事項	ID	影響	コンポーネント	説明
				にGPO処理が長時間にわたり、パフォーマンスに影響を与えました。環境設定の制御を強化するには、VDA組織単位のグループポリシーの継承をブロックし、関連するポリシーとセキュリティ構成のみを適用してください。さらに、Citrix Workspace Environment Managementを活用して設定を非同期で処理し、セッションログオンを高速化することを検討してください。
StoreFrontストアのソケットプーリングを有効にする	REC_046	中	StoreFront	一部のStoreFrontストアでは、ソケットプーリングが有効になっていません。ソケットプーリングは、Delivery ControllerまたはCloud Connectorとの通信のために、すぐに利用できるネットワーク

推奨事項	ID	影響	コンポーネント	説明
				接続（ソケット）のプールを維持することで効率を高めます。StoreFrontは、リクエストごとに新しいソケットを作成して閉じる（高オーバーヘッドのプロセス）のではなく、プールから既存の接続を再利用します。環境全体のパフォーマンスと効率を向上させるには、すべてのストア、特にトランスポート層セキュリティ（TLS）接続でソケットプーリングを有効にしてください。

注:

StoreFront関連の推奨事項には追加の設定が必要です。詳細については、Advisorチェックのための StoreFrontのセットアップを参照してください。

運用エクセレンスの推奨事項

推奨事項	ID	影響	コンポーネント	説明
VDAを最新バージョンにアップグレードする	REC_002	低	VDA	一部のマシンは古いVDAバージョンを使用しています。最新のLTSRまたはCR VDAバージョンにアップグレードして、新機能、改善、セキュリティ強化にアクセスしてください。
Citrixプロビジョニングテクノロジーを使用する	REC_003	中	プロビジョニング	サイト内のすべてのマシンは手動でプロビジョニングされており、Machine Creation Services (MCS) や Citrix Provisioning Services (PVS) などのCitrixプロビジョニングテクノロジーを使用していません。VDAの一貫性を確保し、手動タスクを最小限に抑え、環境のスケーリング操作を効率化するために、MCSまたはPVSを使用してください。

推奨事項	ID	影響	コンポーネント	説明
サイト構成をバックアップする	REC_011	高	全般	サイト構成のバックアップがありません。迅速な回復のためにCitrix構成のすぐに使用できるコピーを確保するには、オンデマンドまたはスケジュールされたバックアップを作成してください。
汚染されたActive Directoryアカウントをリセットする	REC_049	中	プロビジョニング	一部のマシンカタログには、AD Identity Service で「汚染済み」とマークされた AD アカウントが含まれています。これらのアカウントは、その後のプロビジョニング操作で利用できるようにリセットする必要があります。

注:

StoreFront 関連の推奨事項には追加の設定が必要です。詳細については、Advisor チェックのためのStoreFront の設定 を参照してください。

コスト最適化の推奨事項

推奨事項	ID	影響	コンポーネント	説明
デリバリーグループでAutoscaleを有効にする	REC_010	中	VDA	一部の対象となるデリバリーグループでAutoscaleが使用されていません。Autoscaleを有効にすることで、一貫したマシンの電源管理が可能になり、可用性を維持しながらコストとユーザーエクスペリエンスのバランスを効果的に取ることができます。
未使用のリソースを解放する	REC_013	中	全般	マシンやアプリケーションなどの一部の専用ワークロードが30日以上使用されていません。不要な支出を削減し、コストを最適化するために、未使用のマシンを利用可能なプールに戻し、未使用のアプリケーションを管理してください。

VDA アップグレードサービス (VUS)

テクニカルプレビューの機能

テクニカルプレビューの機能は、非本番環境または限定的な本番環境で使用でき、お客様がフィードバックを共有する機会を提供します。Citrix はテクニカルプレビューの機能に関するサポートケースを受け付けていませんが、改善のためのフィードバックを歓迎します。Citrix は、フィードバックの重大度、重要度、および重要性に基づいて対応する場合があります。

これは、いかなる資料、コード、または機能を提供するというコミットメント、約束、または法的義務ではなく、Citrix 製品の購入決定を行う際に依拠すべきではありません。機能の開発、リリース、およびタイミングは、当社の単独の裁量に委ねられており、通知や協議なしに変更される場合があります。

Citrix VDA アップグレードサービスの概要

Citrix VDA アップグレードサービス (VUS) は、Citrix Virtual Apps and Desktops™ (CVAD) のコンポーネントであり、Citrix 環境内の永続的な Virtual Delivery Agent (VDA) のアップグレードプロセスを効率化します。このサービスは、環境を最新の VDA バージョンに保ち、パフォーマンスとセキュリティを強化し、新しい Citrix DaaS 機能を有効にするのに役立ちます。

> **注:**
>
> アップグレードをスケジュールする前に、VDA Upgrade Service は、各VDAの現在のオペレーティングシステムが選択されたターゲットバージョンでサポートされていることを確認します。ターゲットバージョンがサポートしなくなったオペレーティングシステムでVDAが実行されている場合、そのターゲットはVDAに提供されず、VDAは「最新」として報告されます。

> 管理者はVUSを活用して、更新の確認、アップグレードのスケジュール設定、アップグレードの進行状況の監視を行うことができます。アップグレードはすぐに開始することも、特定の日時にスケジュールすることもでき、これにより、アップグレードに最適な時間を選択できます。

VDA のアップグレードがこれまでになく簡単になりました。VDA またはイメージに VDA アップグレードエージェントをインストールし、Web Studio でマシンまたはマシンカタログを右クリックして「Upgrade VDAs」を選択し、環境に最適なオプションを選択します。

アップグレードする前に、アップグレードサイクルオプションを確認してください。VDAには2つのアップグレードトラックがあります。Long-Term Service Release (LTSR) と Current Release (CR) です。LTSRはサポートライフサイクルが長く、より高い安定性とアップグレード頻度の低減を提供します。CRバージョンはより頻繁にリリースされ、最新かつ最高の機能を提供します。詳細については、 ライフサイクルマイルストーンを参照してください。

VUS を使用した VDA アップグレードの前提条件

VUS を使用して VDA アップグレードを実行するには、次の前提条件を満たす必要があります。

サイトで VDA アップグレードサービスを有効にする

2503 サイトで VUS を有効にするには、次の PowerShell コマンドレットを実行します。

```
Set-VusSite -Enabled $true
```

有効にしたら、次の PowerShell コマンドレットを実行して、最新の VDA バージョンを CVAD サイトにインポートします。

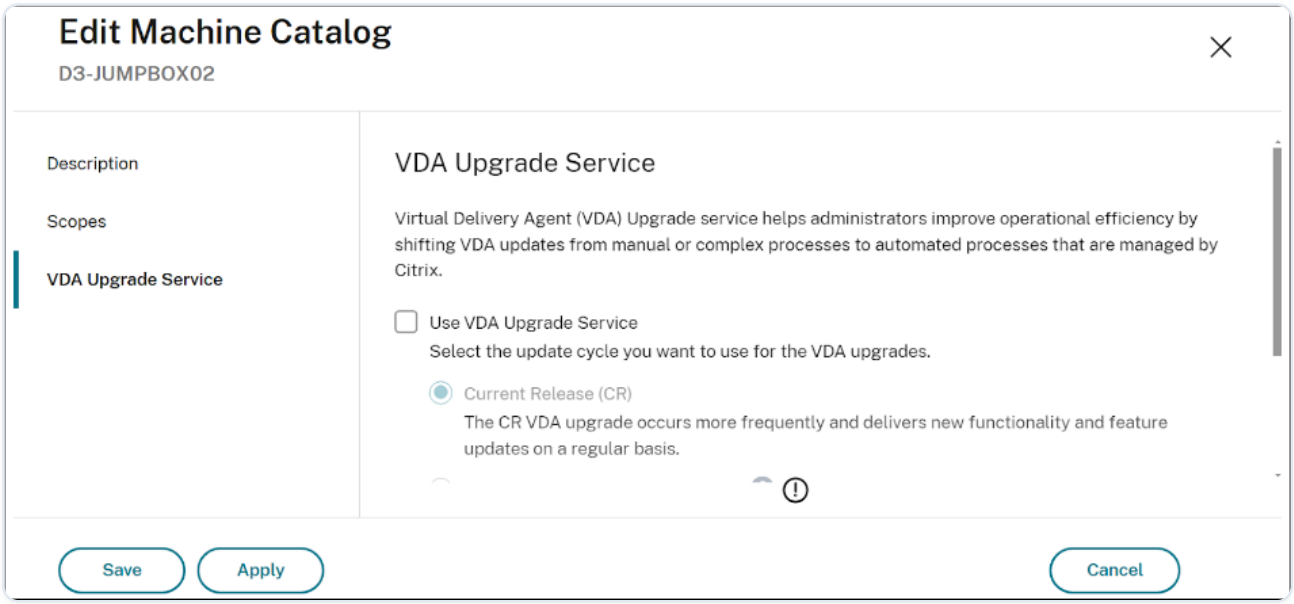
```
Import-VusVdaReleasesMetadata -Path '[<CVAD-2503-ISO>\Support\VdaUpdateServiceMetadata\vda_releases.xml]'
```

VDA アップグレードサービスを有効にする

VDA アップグレードサービス機能を有効にするには、マシンカタログの作成または編集時に VDA アップグレードオプションを使用します。管理者は、VUS を有効にする際に、次のアップグレードサイクルから選択する必要があります。

- LTSR
- CR
- LTSR 早期アクセスリリース (EAR)
- CR EAR

Web Studio からマシンカタログの VDA アップグレードサービスを有効にするには、カタログを右クリックし、 をクリックし、 タブを選択し、 チェックボックスをオンにして、アップグレードトラックを選択します。



PowerShell を使用してマシンカタログの VDA アップグレードサービスを有効にするには、`Set-VusCatalogUpgradeType` コマンドレットを使用します。

アップグレードの種類は、「LTSR」、「CR」、「EAR_CR」、または「EAR_LTSR」に設定できます。

例: `Set-VusCatalogUpgradeType -CatalogName "Workstation catalog" -UpgradeType LTSR`

> **注:**
>
> VDA アップグレードオプションを有効にしても、VDA が自動的にアップグレードされることはありません。VUS を介したすべての VDA アップグレードは、管理者によって明示的に実行される個別のタスクとして開始する必要があります。

VDAの要件

VDAのバージョン

- MCS を使用して作成されたマシンの場合:
  - 2311 以降
- Websocket VDA Enrollment を使用して追加されたマシンの場合
  - 2311 以降
- 手動でプロビジョニングされたマシンの場合

- 2411 以降

ソースVDAのオペレーティングシステム

VDAアップグレードサービスは、VDAの現在のオペレーティングシステムをシステム要件に含むターゲットバージョンのみを提供します。ターゲットバージョンでサポート対象外となったオペレーティングシステム（たとえば、CVAD 2407以降VDA OSとしてサポートされていないWindows Server 2016など）でVDAが実行されている場合、そのターゲットは提供されず、VDAは「最新の状態であり、利用可能なアップグレードはありません」と報告されます。そのようなVDAをアップグレードするには、サポートされているオペレーティングシステムに再イメージングしてください。各バージョンがサポートするオペレーティングシステムについては、そのバージョンのシステム要件とCTX224843を参照してください。

プロビジョニングの種類

- Citrix 以外のプロビジョニング™サービスまたは を使用してプロビジョニングされた、シングルセッションまたはマルチセッションの永続マシン。
- シングルセッションのMCSプロビジョニング済み永続マシン（AD参加済み、Microsoft Entra参加済み、およびドメイン非参加）。
- Remote PC Accessマシン。

VDAアップグレードエージェント

- VDA アップグレードエージェントバージョン 7.44 以降が VDA にインストールされ、アクティブになっている必要があります。エージェントは次のようにインストールできます。
  - VDAのアップグレード時、またはVDAのインストール変更時に、追加コンポーネントとして。
  - Citrix Virtual Apps and Desktops™ ISOで利用可能なスタンドアロンMSIを使用します。
    - MSI名：CitrixUpgradeAgent_x64.msi
    - パス: x64\仮想デスクトップコンポーネント

権限

CVAD でフル管理者またはマシンカタログ管理者ロールを持っている必要があります。

VDAの状態

VUSを介してスケジュールされたアップグレードが意図どおりに進行するには、アップグレード対象のVDAは次の前提条件を満たしている必要があります。

- VDAは手動でメンテナンスモードに設定されていない必要があります。
- VDAのアップグレードを正常に実行するには、ユーザーがログオンしていない必要があります。
  - アップグレードプロセスがアップグレードウィンドウ全体でユーザーセッションのドレインを開始すると、VDAはメンテナンスモードになります。アップグレードが正常に完了すると、メンテナンスモードから解除されます。
  - アップグレードウィンドウの期間中、ユーザーがアクティブまたは切断されたセッションを持っている場合、アップグレードはアップグレードウィンドウの終了時にキャンセルされます。

    注:

    アクティブおよび切断されたセッションは、VUSの強制ログオフオプションを使用して終了できます。
- MCSを介してプロビジョニングされていないVDA（手動でプロビジョニングされたVDA）は、VUSを介してアップグレードを実行する前にデリバリーグループに追加する必要があります。
- VDAは電源が入っている必要があります。

  注:

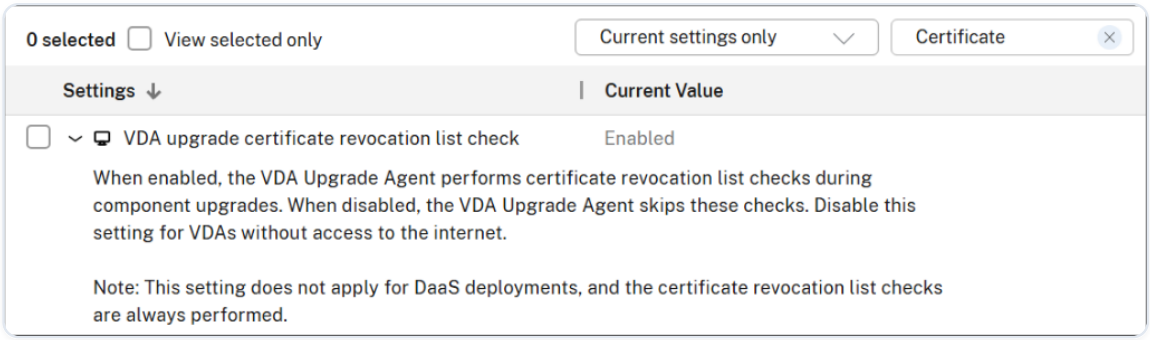
  VDAアップグレードがスケジュールされている場合でも、AutoScale™はマシンの電源管理を停止しません。アップグレードの進行中は、デリバリーグループのAutoScaleスケジュールを無効にすることを検討してください。

接続

- VDA アップグレードの場合、VDA は HTTPS 経由で Delivery Controller と通信できる必要があります。
  - VDAインストーラーが有効な証明書によって署名されていることを確認するには、VDAは以下のURLと通信する必要があります。
    - `<http://crl3.digicert.com/>`*

- `<http://crl4.digicert.com/>`*
- `<http://ocsp.digicert.com/>`*
- `<http://cacerts.digicert.com/>`*

- VDAがインターネットにアクセスできない場合、証明書失効リスト (CRL) をバイパスするようにVDAを構成します。
  - 「VDAアップグレード証明書失効リストチェック」Citrix®ポリシー設定を無効にし、デリバリーグループに割り当てます。
    - ポリシーの説明:
      - 有効にすると、VDAアップグレードエージェントはコンポーネントのアップグレード中に証明書失効リストチェックを実行します。
      - 無効にすると、VDAアップグレードエージェントはこれらのチェックをスキップします。インターネットにアクセスできないVDAの場合は、この設定を無効にします。



プロキシ構成を持つVDA

- ホスト名:ポート (IP:ポート) 形式のプロキシとPACファイルのみがサポートされています。SOCKS5プロキシはサポートされていません。
- VDAアップグレードエージェントは、Web Studioまたはレジストリを使用してプロキシを使用するように構成する必要があります。
  - Web Studioを使用したVDAアップグレードエージェントのプロキシ構成。
    - プロキシを使用するVDAに対して、VDAアップグレードプロキシ構成のCitrixポリシー設定を有効にします。
    - 設定でプロキシアドレスまたはPACファイルへのパスを入力します。
  - レジストリを使用したVDAアップグレードエージェントのプロキシ構成

- **キー:** `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent`
  - **値の型:** `String`
  - **値の名前:** `ProxySettings`
  - **値のデータ:** プロキシアドレスまたはPACファイルへのパス。
    - 例:
      - **プロキシアドレス:** `http://<URL or IP>:\<port>`
      - **PACファイル:** `http://<URL or IP>/\<path/\<filename>.pac`

VDAWorkstationCoreSetup.exe を使用してインストールされたVDA

VDAがVDAWorkstationCoreSetup.exeを使用して最初にインストールされた場合でも、`VDAWorkstationSetup.exe`を利用するVUSを使用してアップグレードできます。

VUSを使用して`VDAWorkstationCoreSetup.exe`でインストールされたVDAをアップグレードする場合、特に最小限のコアインストールから移行する場合は、必要な機能のみが有効になっていることを確認するために、インストールオプションを確認する必要があります。

VUS を使用して VDA をアップグレードする

ターゲットのマシンカタログ、個々のマシン、またはマシンのグループを選択し、「VDA のアップグレード」を選択することで、VDA アップグレードサービスを通じて VDA のアップグレードを開始できます。

> **注:**
>
> Citrix® は、可能な場合はアップグレードを実行する前に VDA をバックアップすることを推奨します。

アップグレードのスケジュール設定

Citrix の VDA アップグレードプロセスは、要件に応じて、カタログレベル、マシンのグループレベル、または個々のマシンレベルで実行できます。アップグレードはすぐに開始するように設定することも、最大 7 日前までに日時を指定してスケジュールすることもできます。

考慮事項

- **カタログ vs. マシンのグループ vs. マシンのスコープ:** カタログのアップグレードは一括更新に最適ですが、個別にまたはグループでマシンをアップグレードすると、よりきめ細かな制御が可能になります。
- **スケジュール設定:** アップグレードは最大 7 日前までにスケジュールできます。マシンカタログレベルのアップグレードを使用する場合、アップグレードがスケジュールされた後にカタログに追加されたマシンは、既存のスケジュールされたアップグレードの一部として含まれません。

主な違い

機能	カタログごとのアップグレード	マシンごとのアップグレード	マシンのグループ
アップグレードの範囲	カタログ全体	個々のマシン	マシンカタログ内のマシンのグループ
スケジュール制御	単一のスケジュールがマシンカタログ内のすべてのVDAに適用され、大規模なアップグレード操作に最適です	VDAは個別にスケジュールされ、主にテストや1回限りのアップグレードに使用されます	VDAはグループでスケジュールされ、異なるVDAグループを異なる時間にアップグレードする柔軟性を提供します
管理	Web Studioの「マシンカタログ」ノードまたは`New-VusCatalogSchedule`コマンドレットで管理されます	Web Studioの「検索」ノードまたは`New-VusMachineUpgrade`コマンドレットで管理されます	Web Studioの「検索」ノード、またはマシンのリストを`New-VusMachineUpgrade`コマンドレットに渡すことで管理されます
ユースケース	マシンカタログ全体のバルクアップグレード	ターゲットを絞ったアップグレードとテストシナリオのためのきめ細かい制御	VDAのサブセットを対象とした制御。カタログ内のアップグレードを段階的に実行するために使用できます

機能	カタログごとのアップグレード	マシンごとのアップグレード	マシンのグループ
利用可能なVDAバージョン	CRおよび現在サポートされているすべてのLTSR VDAバージョンでは、最新バージョンと2つ前のバージョン (N-2) にアップグレードできます。詳細については、利用可能なVDAバージョンを参照してください。	CRおよび現在サポートされているすべてのLTSR VDAバージョンでは、最新バージョンと2つ前のバージョン (N-2) にアップグレードできます。詳細については、利用可能なVDAバージョンを参照してください。	最新のLTSRまたはCR VDAバージョンのみがアップグレード可能です。
追加コンポーネント	各VDAにVDAコンポーネントをインストールまたはアップグレードします。コンポーネントのチェックを外しても機能はアンインストールされませんが、コンポーネントはアップグレードされません。	VDAにVDAコンポーネントをインストールまたはアップグレードします。コンポーネントのチェックを外しても機能はアンインストールされませんが、コンポーネントはアップグレードされません。	マシンのグループをアップグレードする場合、VDAアップグレードサービスでは追加コンポーネントを管理できません。注: 「復元クリーンアップを有効にする」などの追加機能は、マシンのグループのアップグレードで利用できます。
追加機能	追加機能を有効またはアップグレードできます。	追加機能を有効またはアップグレードできます。	追加機能を有効またはアップグレードできます。
同時実行数	アップグレードをスケジュールする際の構成として制御されます。詳細については、同時実行数を参照してください。	単一のVDAがアップグレードされます。	アップグレードスケジュールの一部として選択されたVDAの数に基づいて、自動的に負荷分散されます
失敗しきい値	指定された数のVDAのアップグレードが失敗した場合に、それ以降のアップグ	失敗しきい値は、マシンごとのアップグレードには適用されません。	失敗しきい値は、マシンのグループのアップグレードには使用できません。

機能	カタログごとのアップグレード	マシンごとのアップグレード	マシンのグループ
	レードを防止するために、失敗しきい値を設定できます。詳細については、失敗しきい値を参照してください。		アップグレードするマシンのグループのサイズを、許容できる失敗数となるVDAの最大数に設定することを検討してください。

スケジュールされたアップグレードの仕組み

VDA上のVDAアップグレードエージェントは、VDAをアップグレードする必要があるかどうかを判断するために、定期的にDelivery Controllerと通信します。 VDAは、すぐにアップグレードするように、または最大7日前にアップグレードするようにスケジュールできます。事前にアップグレードをスケジュールする場合、アップグレードが開始される日付と時刻（UTC）を設定できます。

アップグレード期間は、スケジュールされたアップグレード開始時刻からアップグレードが実行されるまでの時間を設定します。デフォルトでは、マシンカタログおよびマシンのグループのアップグレードの場合、Citrixはパフォーマンスを向上させ、ボトルネックを回避するために、アップグレード期間全体にわたってVDAアップグレードの負荷分散を行います。

アップグレードが開始されると、VDAはアップグレードが完了するまでメンテナンスモードになります。VDAでセッションが実行されている場合、セッションがなくなるまでVDAはアップグレードされません。メンテナンスモードの間は、新しいセッションをVDAに仲介することはできません。アップグレード期間中にユーザーがセッションから切断した場合、アップグレードが完了するまで再接続できません。

VDAは、スケジュールされたアップグレード期間が完了するまでアップグレードを試行し続けます。アップグレード期間全体にわたってセッションが存在する場合、アップグレードはキャンセルされ、VDAのメンテナンスモードはオフになります。VDAアップグレードの成功率を向上させるために、より長いアップグレード期間を検討してください。

注:

スケジュールされたアップグレードの前に手動でメンテナンスモードに設定されたVDAは、アップグレードに失敗します。

利用可能なVDAバージョン

VDAアップグレードサービスは、CRバージョンではVDAのN-2バージョンを、現在サポートされているすべてのLTSRバージョンではN-2 CUバージョンを維持します。

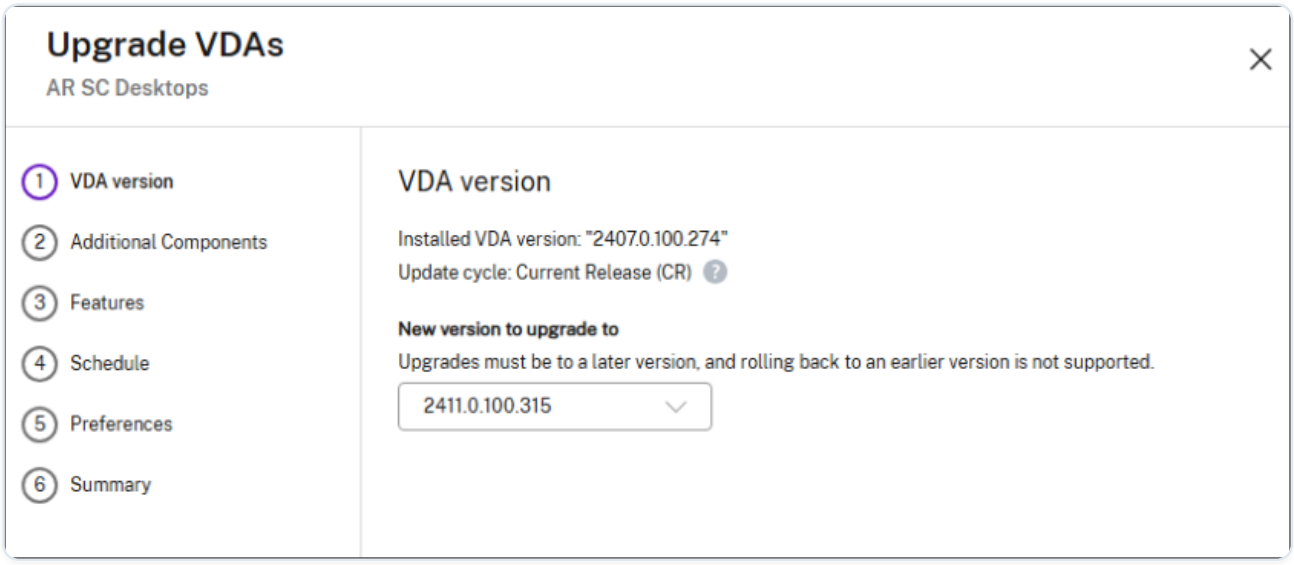
VDAのアップグレードウィザードには、選択した各VDAの現在のオペレーティングシステムと互換性のあるターゲットバージョンのみが表示されます。VDAのオペレーティングシステムのサポートを削除したターゲットは、そのVDAには表示されません。

新しいCVADバージョンがリリースされた場合、サイト全体を更新することなく、VUSを更新してより新しいVDAバージョンを含めることができます。VUSは**vda_releases.xml**ファイルを使用して、利用可能なVDAバージョンを投入します。**vda_releases.xmld**ファイルは、CVADメタインストーラーの次の場所にあります。

<CVAD-ISO\>\Support\VdaUpdateServiceMetadata\vda_releases.xml

新しいvda_releases.xmlファイルをVUSにインポートするには、次のコマンドレットを実行します。 `Import-VusVdaReleasesMetadata -Path '[Path to vda_releases.xml]'`

Web Studioで、カタログまたは個々のマシンをアップグレードする際、UIはVDAをどのバージョンにアップグレードするかを尋ねます。

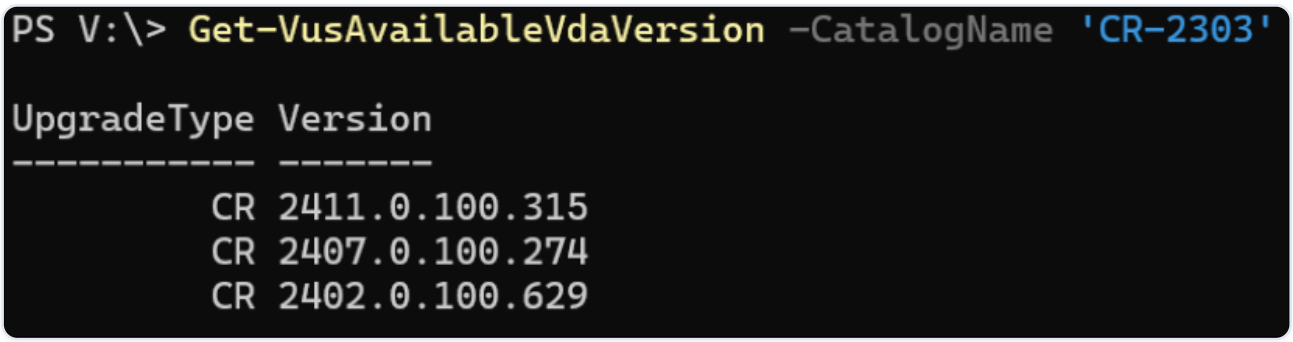


PowerShell を使用して利用可能なVDAバージョンを特定するには、`Get-VusAvailableVdaVersion` コマンドレットを使用します。

コマンドレットにマシンまたはカタログを渡さない場合、コマンドレットはすべてのアップグレードトラックで利用可能な最新バージョンを返します。

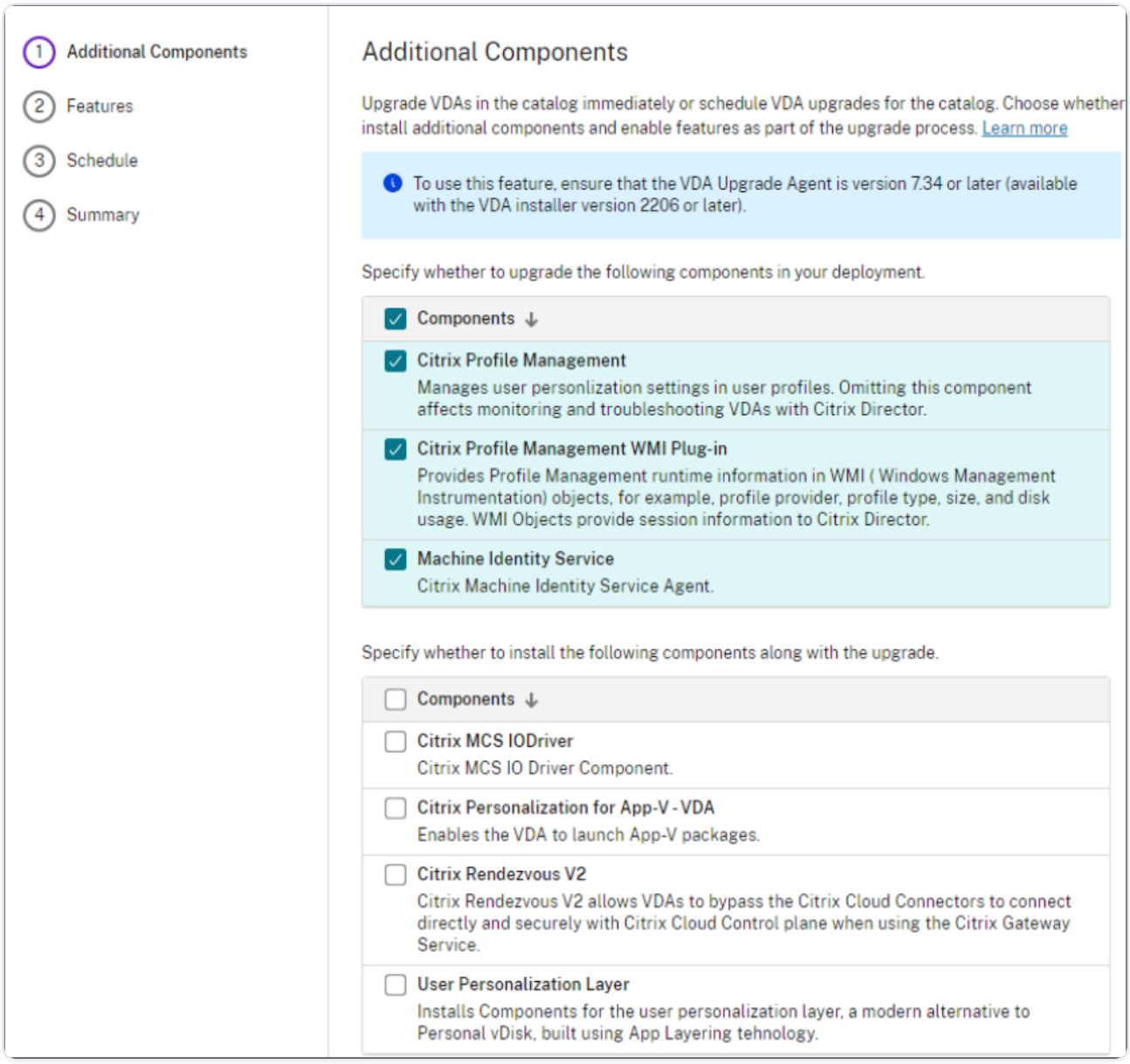
リソースで利用可能な特定のバージョンを取得するには、VDA (-MachineName, -MachineUid または -MachineUuid) またはカタログ (-CatalogName, -CatalogUid, または -CatalogUuid) を `Get-VusAvailableVdaVersion` コマンドレットに渡します。

例: `Get-VusAvailableVdaVersion -CatalogName '[Name of your Machine Catalog]'`



追加コンポーネント

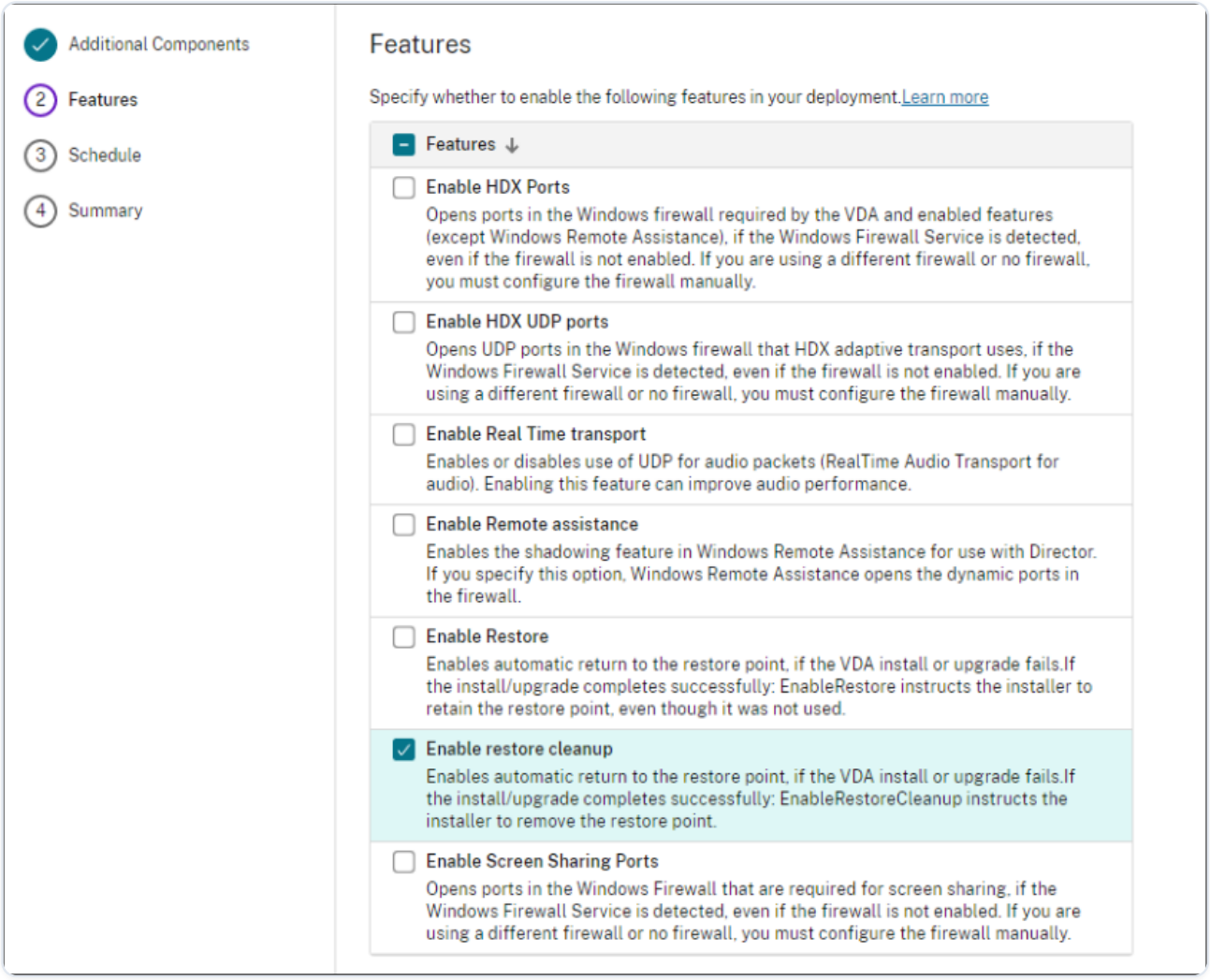
マシンカタログまたは個々のマシンでVDAをアップグレードする際に、追加コンポーネントをインストールまたはアップグレードできます。コンポーネントをチェックしない場合、そのコンポーネントはアンインストールされませんが、VDA全体のアップグレードの一部としてアップグレードされることはありません。



機能

VDAアップグレードサービスを通じて、VDAの機能を有効化またはアップグレードできます。機能をチェックしない場合、その機能は無効化されませんが、VDA全体のアップグレードの一部としてアップグレードされることはありません。

デフォルトでは、**復元クリーンアップを有効にする** チェックボックスが選択されています。Citrixは、管理を容易にし、失敗したアップグレードからの回復を改善するために、復元クリーンアップ機能を有効にすることを推奨しています。この機能が有効になっている場合、アップグレードが開始される前にシステム復元ポイントが作成されます。アップグレードが失敗した場合、VDAはシステム復元ポイントに復元されます。復元ポイントは、VDAのインストールが成功した後に削除されます。詳細については、インストールまたはアップグレードの失敗時の復元 を参照してください。



注:

Windows システムの復元は、シングルセッションオペレーティングシステム (例: Windows 10および11) でのみサポートされています。「復元のクリーンアップを有効にする」機能が動作するためには、VDAでWindows システムの復元機能が有効になっている必要があります。「復元を有効にする」または「復元のクリーンアップを有効にする」が選択されているにもかかわらず、VDAでWindows システムの復元が構成されていない場合、アップグレードが失敗する可能性があります。

同時実行性

マシンカタログをアップグレードする際、VUSを使用すると、同時にアップグレードされるVDAの最大数を定義できます。これにより、インターネット接続やファイルサーバーへの負荷を軽減でき、失敗しきい値と組み合わせて使用することで、多数のVDAのアップグレードが失敗した場合にアップグレードを停止できます。

スケジュールされたアップグレードが開始されるとすぐに、カタログ内のすべてのVDAがメンテナンスモードになります。定義された最大同時実行設定に一致する数のVDAでアップグレードが開始されます。VDAのアップグレードが完了するとすぐに、別のVDAがアップグレードを開始し、同時にアップグレードされるVDAの同時実行数を維持します。

マシンカタログのスケジュールされたアップグレードで同時実行性が指定されていない場合、Citrixはカタログ内のVDAの総数とアップグレード期間に基づいてデフォルトの同時実行値を使用します。

アップグレードの完了には平均約30分かかりますが、これは環境条件によって大きく異なる場合があります。指定されたアップグレード期間内にすべてのVDAがアップグレードできるような同時実行数を設定することを検討してください。例えば、4時間かけてアップグレードするように設定された20台のVDAがある場合、1時間あたり5台のVDAをアップグレードする必要があります。平均アップグレード期間30分を使用すると、同時実行値を3に設定することで、1時間あたり5台のVDAアップグレード要件を満たすことができます（30分あたり3回のアップグレードで、1時間あたり6回の更新になります）。

失敗しきい値

マシンカタログをアップグレードする際、失敗しきい値を使用して、特定の数のVDAが失敗した場合にそれ以上のVDAがアップグレードされるのを防ぎます。失敗しきい値は、アップグレードの失敗を引き起こす問題の影響範囲を縮小し、管理者のトラブルシューティング作業を軽減できます。

失敗しきい値は、今後のVDAがアップグレードを開始するのを防ぎますが、すでにアップグレードを開始したVDAは停止しません。例えば、マシンカタログに100台のVDAがあり、同時実行数が10台のVDAに設定され、失敗しきい値が3に設定されている場合、すべてのVDAアップグレードが失敗すると、少なくとも13台のVDAがアップグレードを試行したことになり、残りの87台は開始されず、アップグレードはキャンセルされます。

スケジュールされたアップグレードの開始時に10台の同時実行VDAがアップグレードを開始します。最初のアップグレードが失敗した場合、10台の同時実行アップグレードを維持するために別のVDAがアップグレードを開始します。2番目のアップグレードが失敗した場合、別のVDAがアップグレードを開始します。3番目のアップグレードが失敗した場合、現在アップグレードプロセス中のすべてのVDAは続行され、アップグレードスケジュール内の残りのVDAはアップグレードがキャンセルされます。

VDAインストーラーの場所

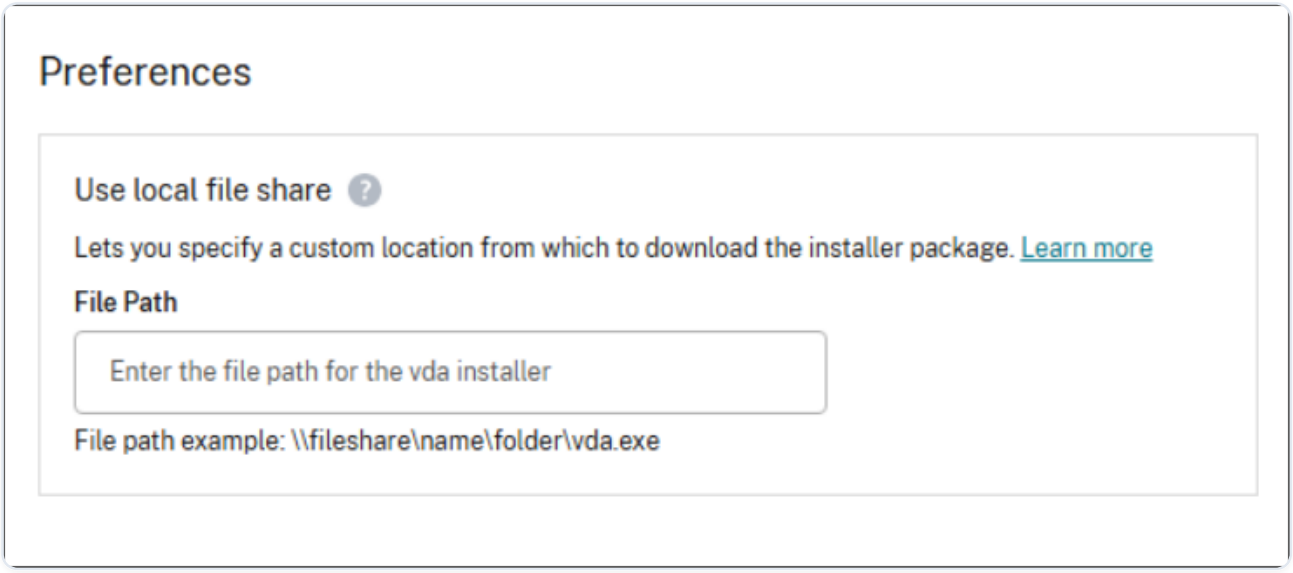
VDAインストーラーは、環境内のローカルファイル共有でホストする必要があります。ファイル共有とVDAインストーラーの要件を以下に示します。

ファイル共有には、次の前提条件が必要です。

- ファイル共有のアクセス許可
  - VDAインストーラーパッケージを含むネットワーク共有には、Local System (NT AUTHORITY\SYSTEMプリンシパル) として実行されるVDAアップグレードエージェントサービスに対する読み取りアクセス権が必要です。
  - ドメイン参加済みVDA:
    - ローカルシステムアカウント (VUAはローカルシステムとして実行されます) は、ネットワーク共有にアクセスする際にコンピューターの資格情報を使用します。
    - ファイル共有には、ドメインコンピューターへの読み取りアクセス権を付与する必要があります。
    - 詳細共有設定で、**ファイルとプリンターの共有**を有効にする必要があります。
  - ドメイン非参加VDA:
    - ローカルシステムアカウント (VUAはローカルシステムとして実行されます) は、ネットワーク共有にアクセスする際に**ANONYMOUS LOGON**を使用します。
    - **ネットワークと共有センターのパスワード保護共有**は無効にする必要があります。
    - フォルダーのアクセス許可の**セキュリティ**タブで、**ANONYMOUS LOGON**に読み取りアクセス許可を付与する必要があります。
    - 詳細共有設定で、**ファイルとプリンターの共有**を有効にする必要があります。
    - 共有フォルダー名は、**ネットワークアクセスセキュリティポリシー**に追加する必要があります。
- VDAインストーラー
  - VDAインストーラーは、Citrix Downloads Webサイトからダウンロードし、ファイル共有に配置する必要があります。
  - マシンカタログに関連するVDAインストーラーをダウンロードする必要があります。
    - カタログタイプがマルチセッションの場合は、**Multi-session OS VDA installer**を使用します。
    - カタログタイプがシングルセッションの場合は、**Single-session OS VDA installer**を使用します。
  - 特定のアップグレードの場合、ファイル共有上のインストーラーのバージョンは、VUSによって公開されているバージョンと完全に一致している必要があります。利用可能なバー

ジョンを確認するには、`Get-VusAvailableVersion` PowerShellコマンドレットを使用します。

インストーラーへのパスは、実行可能ファイルを含むファイルパスである必要があります。例: `\\hostname\VDA-Packages\VDAWorkstationSetup_2308.exe`。



PowerShellを介してVUSを使用する場合、アップグレードをスケジュールする際に、`-VdaWorkstationPackageUri`（シングルセッションOS）または`-VdaServerPackageUri`（マルチセッションOS）パラメーターを使用します。

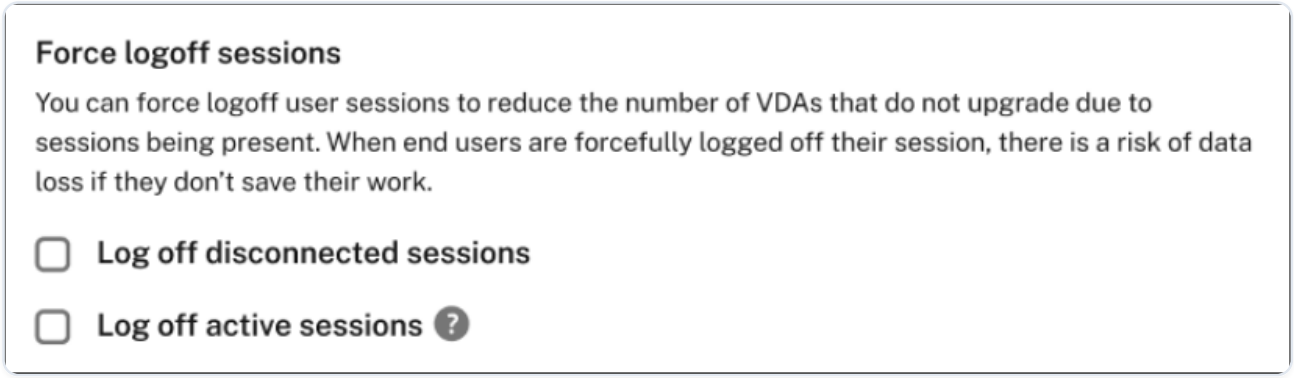
セッションの強制ログオフ

スケジュールされたアップグレード中にアップグレード可能なVDAの数を増やすには、アップグレード中にユーザーセッションを強制的にログオフすることを検討してください。強制ログオフは、個々のVDAのアップグレードが開始されるときに発生し、全体のスケジュールされたアップグレード期間の開始時ではありません。

スケジュールされた期間内で異なるVDAが異なる時間にアップグレードを開始するため、ユーザーは自身の特定のVDAのアップグレードが開始されたときにのみログオフされます。

Web Studioを使用してスケジュールされたアップグレード中に切断されたセッションを強制的にログオフするには、 オプションを選択します。

Web Studioを使用してスケジュールされたアップグレード中にアクティブなセッションを強制的にログオフするには、「**アクティブなセッションをログオフする**」オプションを選択します。アクティブなセッションをログオフする場合、ユーザーはアップグレード開始の10分前にセッション内で通知を受け取り、自動的にログオフされる前に作業を保存するよう促されます。



PowerShell を使用してスケジュールされたアップグレード中に切断されたセッションを強制的にログオフするには、アップグレードをスケジュールするときに `-LogoffOption` パラメーターを使用します。`-LogoffOption` の利用可能なオプションは次のとおりです。

- **ActiveSessionsOnly:** スケジュールされたアップグレード期間中に VDA でアクティブなセッションがある場合、ユーザーはログオフされます。ユーザーがログオフされる10分前に警告バナーが表示されます。切断されたセッションを持つ VDA は、アップグレード期間中にログオフされません。切断されたセッションがアップグレード期間中ずっと残っている場合、その VDA のアップグレードはキャンセルされます。
- **DisconnectedSessionsOnly:** スケジュールされたアップグレード期間中に VDA で切断されたセッションがある場合、ユーザーはログオフされます。ユーザーには、切断されたセッションがログオフされることは通知されません。アクティブなセッションを持つ VDA は、アップグレード期間中にログオフされません。アクティブなセッションがアップグレード期間中ずっと残っている場合、その VDA のアップグレードはキャンセルされます。
- **ActiveAndDisconnectedSessions:** スケジュールされたアップグレード期間中に VDA で切断されたセッションまたはアクティブなセッションがある場合、ユーザーはログオフされます。アクティブなセッションの場合、ユーザーがログオフされる10分前に警告バナーが表示されます。
- **DoNotLogoff:** アクティブなセッションと切断されたセッションはログオフされません。アップグレードスケジュールの期間中ずっと VDA にセッションが存在する場合、スケジュールされたアップグレード期間の終了時にアップグレードはキャンセルされます。

可能な場合は、Citrix はセッションを強制的にログオフして、正常にアップグレードされる VDA の数を増やすことを推奨します。

> **重要:**
>
> セッションを強制的にログオフすると、ユーザーはセッション内の保存されていない作業を失う可能性があります。

VDAワークフローの編集またはキャンセル

カタログのアップグレードをスケジュールした後、アップグレードの開始時刻と期間を編集したり、または完全にキャンセルしたりできます。

マシンカタログレベルでUIを使用してアップグレードを編集またはキャンセルするには、既存のスケジュールされたアップグレードがあるマシンカタログを右クリックし、「**スケジュールされたVDAアップグレードの編集**」をクリックします。PowerShellを使用して既存のマシンカタログレベルのアップグレードを編集するには、`Set-VusCatalogUpgrade`および`Remove-VusCatalogUpgrade`コマンドレットを使用します。

マシンレベルでアップグレードを編集またはキャンセルするには、検索ノードで、既存のスケジュールされたアップグレードがあるマシンを右クリックし、「**スケジュールされたVDAアップグレードの編集**」をクリックします。複数のマシンに対して同時にスケジュールされたVDAアップグレードを編集することはできません。PowerShellを使用して既存のマシンレベルのアップグレードを編集するには、`Set-VusMachineUpgrade`および`Remove-VusMachineUpgrade`コマンドレットを使用します。

VUSの監視とトラブルシューティング

スケジュールされたVDAアップグレードの監視

VDAとマシンカタログには、VDAアップグレードの準備状況と現在のステータスを監視するのに役立つ2つの属性があります。これらは、StudioまたはVDAやカタログの詳細ペインでフィルタリングに使用できる列として表示されます。

- VDAアップグレード
- VDAアップグレードの状態

VDAアップグレード

VDAアップグレードは、VDAまたはマシンカタログにVDAアップグレードエージェントが構成されているかどうか、およびVDAが最新であるか、またはアップグレードが利用可能であるかに関する情報を提供します。利用可能なステータスは次のとおりです。

VDAアップグレード (STUDIO)	VDAアップグレード (POWERSHELL)	説明
カタログレベル		

VDAアップグレード (STUDIO)	VDAアップグレード (POWERSHELL)	説明
未構成	MissingUpgradeType	マシンカタログに対して、アップグレードトラック (CR、LTSR、CR EAR、またはLTSR EAR) が選択されていません。
スケジュール済み	UpgradeScheduled	マシンカタログのアップグレードがスケジュールされています。
利用可能	UpgradeAvailable	カタログ内のVDAは、アップグレードトラックの最新バージョンではありません。アップグレードが推奨されます。
最新	UpToDate	カタログ内のVDAは、アップグレードトラックの最新バージョンです。アクションは不要です。または、VDAの現在のオペレーティングシステムをサポートする利用可能なアップグレードターゲットがありません。
不明	不明	最新のVDAアップグレード状態を取得しています。
マシンレベル		
未構成	MissingUpgradeType	VDAのマシンカタログに対して、アップグレードトラック（CR、LTSR、CR EAR、またはLTSR EAR）が選択されていません。
スケジュール済み	UpgradeScheduled	VDAのアップグレードがスケジュールされています。
利用可能	UpgradeAvailable	VDAはアップグレードトラックの最新バージョンではあり

VDAアップグレード (STUDIO)	VDAアップグレード (POWERSHELL)	説明
		ません。アップグレードが推奨されます。
最新	UpToDate	VDAはアップグレードトラックの最新バージョンです。アクションは不要です。または、VDAの現在のオペレーティングシステムをサポートする利用可能なアップグレードターゲットがありません。
状態を確認中	不明	最新のVDAアップグレード状態を取得しています。

注:

- LTSRトラックを使用しているVDAの場合、カタログは、VDAが最新の長期サービス (LTSR) バージョンの最新の累積更新プログラム (CU) にある場合にのみ「最新」と表示されます。VDAが以前のLTSRバージョンの最新のCUにある場合でも、VDAアップグレードは**利用可能**と表示されます。
- 利用可能なアップグレードターゲットが現在のオペレーティングシステム（例えば、CVAD 2407以降のWindows Server 2016）をサポートしていない場合、VDAも「最新の状態」と表示されます。この場合、VDAアップグレードウィザードはVDAのターゲットを提供しません。アップグレードするには、マシンをサポートされているオペレーティングシステムに再イメージングしてから、アップグレードをスケジュールします。ターゲットバージョンのシステム要件とCTX224843を参照してください。

VDAアップグレードの状態

VDAアップグレードの状態は、スケジュールされたアップグレードのステータスに関する情報を提供します。VDAアップグレードの状態のステータスは次のとおりです。

VDAアップグレードの状態 (STUDIO)	VDAアップグレードの状態 (POWERSHELL)	説明
カタログレベル		

VDAアップグレードの状態 (STUDIO)	VDAアップグレードの状態 (POWERSHELL)	説明
スケジュールされていません	NotScheduled	カタログのアップグレードはスケジュールされていません。
スケジュール済み	UpgradeScheduled	カタログのアップグレードがスケジュールされています。
進行中	UpgradeInProgress	カタログのアップグレードが進行中です。
キャンセル済み	UpgradeCancelled	カタログのアップグレードがキャンセルされました。これは、手動によるキャンセル、または失敗しきい値に達したことが原因である可能性があります。
失敗	UpgradeFailed	カタログのスケジュールされたアップグレードが失敗しました。
成功	UpgradeSuccessful	カタログのスケジュールされたアップグレードが正常に完了しました。注: アップグレードが成功したからといって、カタログ内のすべてのVDAが正常にアップグレードされたわけではありません。
-	空	カタログのアップグレードはスケジュールされていません。
マシンレベル		
スケジュール済み	UpgradeScheduled	VDAのアップグレードがスケジュールされています。
アップグレード待機中	UpgradeInUpgradeWindow	スケジュールされたアップグレードはアクティブですが、VDAはまだアップグレードを

VDAアップグレードの状態 (STUDIO)	VDAアップグレードの状態 (POWERSHELL)	説明
		開始していません。VDAアップグレードの負荷分散方法の詳細については、「同時実行」を参照してください。
進行中	UpgradeInProgress	VDAは現在アップグレード中です。
キャンセル済み	UpgradeCancelled	アップグレードが開始される前に、VDAのスケジュールされたアップグレードがキャンセルされました。
アップグレード失敗	UpgradeFailed	VDAはアップグレードを開始しましたが、アップグレードは正常に完了しませんでした。詳細については、「トラブルシューティング」を参照してください。
成功	UpgradeSuccess	VDAは正常にアップグレードされました。
検証に失敗しました	UpgradeValidationFailed	VDAインストーラーのメタデータをダウンロード中に、証明書の検証に失敗しました。
-	空	VDAのアップグレードはスケジュールされていません。

スケジュールされたVDAアップグレードのトラブルシューティング

アップグレードの失敗が発生した場合、以下のログは問題の特定とトラブルシューティングに役立ちます。これらのログをCitrixテクニカルサポートと共有することで、サポートプロセスを迅速化することもできます。

VDAインストールログ

アップグレードの失敗をトラブルシューティングする際は、VDAの初期インストールと失敗したアップグレードの両方のログを収集して確認してください。インストールおよびアップグレードのログは、以下の場所にあります。

- VDAインストールのインストールログは、次の場所にあります。
  - %temp%/Citrix/XenDesktop インストーラー
- VDAインストールのアップグレードログは、次のいずれかの場所にあります。
  - C:\Windows\Temp\Citrix\XenDesktop Installer **または**
  - C:\Windows\SystemTemp\Citrix\XenDesktop インストーラー

VDA アップグレードエージェントのバージョン

VUS を介してアップグレードの失敗をトラブルシューティングするためにデータを収集する際、VDA 上のアップグレードエージェントのバージョンを知ることが重要です。VDA アップグレードエージェントのバージョンを確認するには、次のコマンドレットを使用します: `Get-VusComponentVersion -ComponentType VUS`。これにより、すべての VDA とその VDA アップグレードエージェントのバージョンが一覧表示されます。

カタログレベルで VDA アップグレードエージェントのバージョンを確認するには、次のスクリプトを使用できます。

> **注:**

> このスクリプトは例として提供されており、特定の環境に合わせて調整する必要がある場合があります。本番環境で使用する前に、スクリプトを十分にテストすることをお勧めします。

```
Param( [Parameter (Mandatory=$true)] [string] $CatalogName ) try { $Uuids = Get-BrokerMachine -CatalogName $CatalogName | Select-Object -Property UUID
```

```
if($Uuids -eq $null) { throw "Cannot find CatalogName " +$CatalogName } Write-Output("Catalog Name passed is "+$CatalogName)
```

```
foreach($Uuid in $Uuids) { $compVersion = Get-VusComponentVersion -MachineId $machine.UUID -ComponentType VUS $Machine = Get-BrokerMachine -UUID $compVersion.MachineId Write-Output("MachineName: "+ $Machine.MachineName+", Machine UUID:"+$machine.MachineId+", VUA Version:"+ $compVersion.Version) } } catch { Write-Output("Exception Occured") Write-Host $_ }
```

VDA アップグレードエージェントに関連するログ

VDA アップグレードエージェント (VUA) のログは、アップグレードの失敗や VUA と VDA アップグレードサービスとの通信に関する問題のトラブルシューティングに不可欠な情報を提供できます。収集できるログには次のものがあります。

- Citrix Diagnostic Facility (CDF) トレース。CDFモジュール名は`VdaUpgradeAgent`です。
- Windowsイベントログ。ログは**イベントビューアー > Windowsログ > アプリケーション > Citrix VDA Upgrade Agent Service**で表示します。

管理者が、ログファイルが大きくなりすぎるのを防ぎながら、トラブルシューティングに重要な情報をキャプチャするローテーションログファイルを有効にできるレジストリ設定が利用可能です。ログファイルの合計サイズは20 MBに制限されています。ファイルへのログ記録を有効にするには、次のレジストリキーを作成します。

- **キー:** `HKLM:\SOFTWARE\Citrix\UpdateServices\UpdateAgent`
- **値の名前:** `LogToFile`
- **値の型:** `REG_DWORD`
- **値のデータ:**
  - `0` - ファイルトレース無効
  - `1` - ファイルトレース有効

PowerShell を使用して VDA 上に LogToFile レジストリキーを作成するには、次のコマンドレットを使用します:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\UpdateServices\UpdateAgent -Name LogToFile -Value 1 -PropertyType DWord -Force
```

大規模なマシン群に対して LogToFile を有効にするには、グループポリシー設定を使用してすべての VDA 組織単位 (OU) に LogToFile レジストリを作成することを検討してください。

> **注:**
>
> - `LogToFile=1` が設定されている場合、ログはファイルにのみ書き込まれます。CDF トレースには表示されません。
> - レジストリの変更を有効にするには、VDA Upgrade Agent サービスの再起動が必要です
> - ログファイルは C:\ProgramData\Citrix\Update Services\Logs フォルダーに作成されます

VDAアップグレードのダウンロード失敗のトラブルシューティング

VDAアップグレード機能に関連するダウンロードの失敗をトラブルシューティングし、解決するには、以下の手順に従ってください。

1. URLフィルタリングが有効な場合は、関連するURLが許可リストに追加されていることを確認してください。接続性を参照してください。
2. 必要なURLを許可リストに追加した後、VDAアップグレードの再スケジュールを試してください。

CDFトレースを有効にするか、`LogToFile`を`1`に設定して、分析用の詳細なログをキャプチャできます。ダウンロードの失敗の問題が解決しない場合は、エラーを確認してください。次のエラーメッセージ「Download Failed: This access control list is not in canonical form and therefore cannot be modified」が表示される場合、それは`C:\ProgramData\Citrix\UpgradeServices\Downloads\VDA`フォルダーのアクセス許可が正しくないことを示しています。

この問題に対処するには、次のいずれかを実行します。

- **オプション1：** 次のコマンドを使用して、フォルダーのアクセス制御リスト（ACL）をリセットします。（このコマンドは、一致するすべてのファイルに対して、デフォルトで継承されたACLでACLをリセットします。）
  - icacls.exe "C:\ProgramData\Citrix\UpgradeServices\Downloads\VDA" /reset /T /C /L /Q
- **オプション2：** Downloadsの下にあるVDAフォルダーを削除し、VDAアップグレードをスケジュールします。

VDAアップグレード検証の失敗のトラブルシューティング

VDAアップグレード機能に関連するダウンロードの失敗をトラブルシューティングし、解決するには、以下の手順に従ってください。

1. URLフィルタリングが有効な場合は、関連するURL、特に失効チェックに必要な証明書失効リスト (CRL) またはオンライン証明書ステータスプロトコル (OCSP) のURLが許可リストに追加されていることを確認してください。VDAアップグレード要件を参照してください。
2. 必要なURLを許可リストに追加した後、VDAアップグレードの再スケジュールを試してください。

分析のために詳細なログをキャプチャするには、CDFトレースを有効にするか、`LogToFile`を`1`に設定することをお勧めします。ログには次のエラーが含まれる場合があります。

- RevocationStatusUnknown
- 失効機能は、証明書の失効ステータスを確認できませんでした。
- 失効サーバーがオフラインだったため、失効機能は失効を確認できませんでした。

VDAアップグレードエージェントは、Windowsシステムコールに依存して証明書を検証し、失効チェックを実行します。上記のエラーは、エージェントがCRLまたはOCSPのURLへの接続を確立できないことを示しています。

Windows CryptoAPIは現在、プロキシ設定をサポートしていません。送信CRL呼び出しを容易にするためにVDAプロキシを構成するには、「プロキシ構成を持つVDA」セクションを確認してください。

Citrix Always On トレース

Always On Tracing (AOT) は、Citrix Virtual Apps and Desktops (CVAD) 環境全体で関連するログデータを継続的にキャプチャするように設計された、Citrix の最新の診断フレームワークです。AOT は Citrix Diagnostic Facility (CDF) トレースのサブセットであり、他のコンポーネントからの追加ログも含まれており、一般的な障害 (VDA 登録、アプリケーション/デスクトップの起動など) のトラブルシューティングに役立ちます。

手動での介入が必要な従来のツールとは異なり、AOT はデフォルトでバックグラウンドで実行され、問題が再現できない場合でも、問題発生時に重要な情報が利用可能であることを保証します。

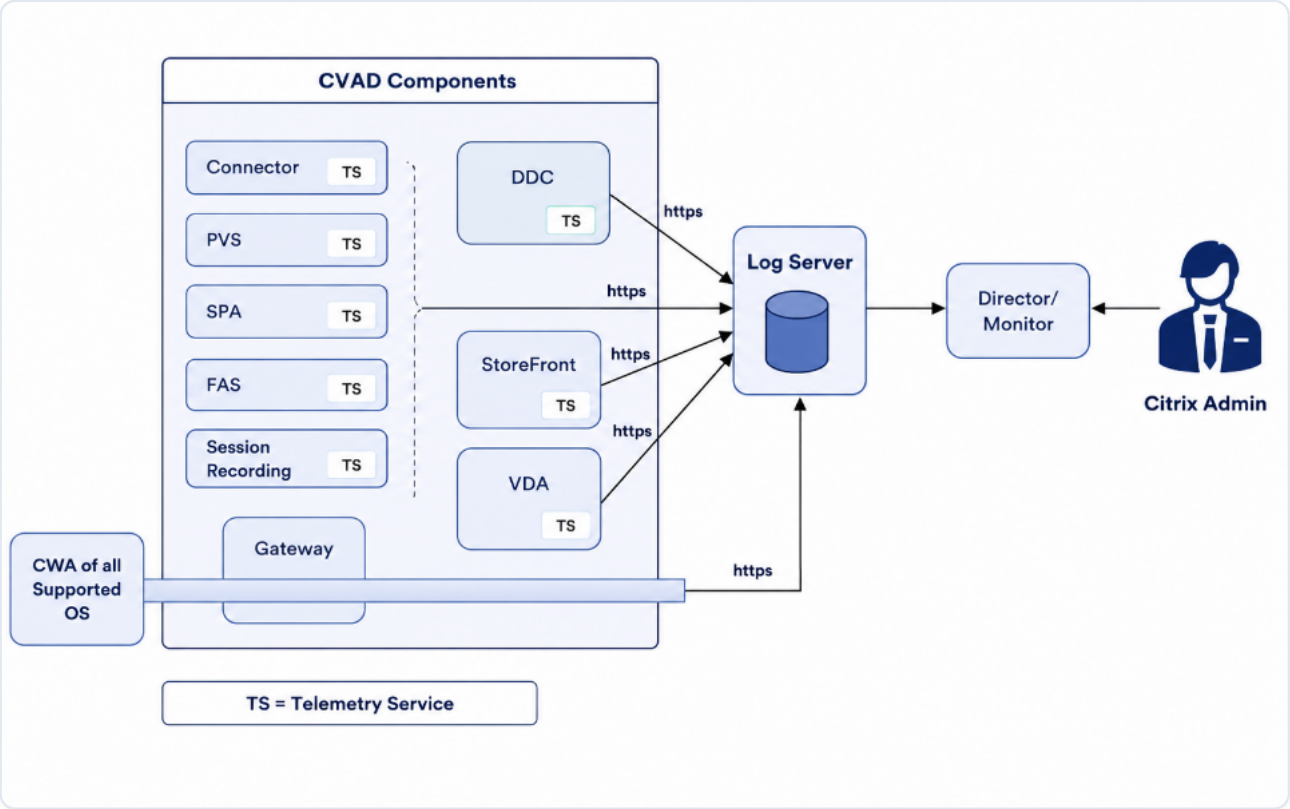
AOT は、IT 管理者と Citrix サポートチームのトラブルシューティングを簡素化し、平均解決時間 (MTTR) を改善するために構築されています。具体的には、次のことを行います。

- ユーザーセッションとシステムイベントのログデータを自動的にキャプチャします。
- 問題を再現する必要がなくなります。
- エンジニアリングレベルの専門知識がなくても、ログに簡単にアクセスして読み取れるようにします。
- セルフサービスログデータを有効にして、Citrix サポートへの依存を減らします。

主な利点

- MTTR (平均解決時間) の短縮
- 常時稼働、手動でのトレース開始は不要
- 一般的な問題の自己診断
- 完全なコンテキストで Citrix サポートへのエスカレーションを合理化
- 機密データの編集による、安全でコンプライアンスに準拠したログ処理

コアコンセプト



Always on Tracing (AOT) アーキテクチャは、Citrix Virtual Apps and Desktops (CVAD) および DaaS 環境全体で継続的なリアルタイムログ収集を提供するように設計されています。これにより、IT管理者とCitrixサポートは、手動でのログ開始や問題の再現を必要とせずに、ユーザーおよびインフラストラクチャの問題をトラブルシューティングできます。

AOTシステムは、複数のCitrixインフラストラクチャ層からのログをキャプチャ、転送、保存するために、順序立てて連携するいくつかの統合されたコンポーネントに基づいて構築され、一元化されたリポジトリに格納します。

主要コンポーネントとワークフロー

1. **AOTログジェネレーター (Citrixコアコンポーネント)**: Virtual Delivery Agent (VDA)、Delivery Controller (DDC)、StoreFrontなどのCitrixコンポーネントは、ログジェネレーターとして機能します。これらのコンポーネントには、テレメトリサービスまたは同様のサービスが搭載されており、AOT APIを使用して、トレースデータをキャプチャし、事前定義されたステップトレースを記録し、ユーザーセッションおよびトランザクションに関連するエラーイベントをログに記録します。
2. **ログ収集の有効化**: 管理者がログ収集要求を開始すると (通常はWeb Studioの設定を通じて)、指示はサイトデータベースに保存され、ブローカーに送信されます。ブローカーは、ブローカー、StoreFront、VDAなどの関連コンポーネント全体でログ収集プロセスを調整します。管

理者は、Session Recording、PVS、FASなどの他のコンポーネントからPowerShellコマンドを通じて個別にログ収集要求を開始します。

3. **テレメトリサービス**: Citrix Web Studioでログサーバーアドレスを設定し、設定が伝播されると、各コンポーネントのテレメトリサービスは新しいリアルタイムAOTリスナーをアクティブ化します。これにより、事前定義されたイベント、障害、またはトリガーポイントに基づいてログが収集されます。
4. **集中ログサーバーへのログ転送**: ログが収集されると、テレメトリサービスまたは独立したサービスが、それらを直接、集中ログサーバーに安全に転送します。エンドポイントがCitrix Gatewayを介して外部ネットワークから接続されている環境では、安全でシームレスな転送を確保するために、通常SOCKSトンネルを介して転送が行われます。
5. **ログの保存と整理**: 集中ログサーバーは、AOTログを受信、解析し、インデックス付きデータベースバックエンド (デフォルトではOpenSearch) を使用して、構造化された検索可能な形式で保存します。ログはセッション、コンポーネント、およびタイムスタンプによってタグ付けされ、容易なアクセスと効率的なトラブルシューティングを可能にします。

Citrix AOTシステム内のログは、容易なアクセスと効率的なトラブルシューティングを可能にするために、さまざまなフィールドでタグ付けされた、構造化された検索可能な形式で保存されます。これらのタグには以下が含まれます。

- **MachineName**: ログが生成されたマシンの名前。
- **MachineIP**: マシンのIPアドレス。
- **Role**: Citrixコンポーネントの役割 (例: VDA、DDC、StoreFront)。
- **TimeStamp**: ログイベントが発生したUTCタイムスタンプ。
- **メッセージ**：実際のログメッセージの内容。単語で検索/フィルタリングできます。
- **レベル**：ログの重大度レベル（例：情報、警告、エラー）。
- **モジュール**：ログを生成した特定のソフトウェアモジュール。
- **プロセス名**：ログを生成したプロセスの名前。
- **プロセスID**：プロセスのID。
- **スレッド**：プロセス内のスレッドID。
- **CPU**：ログ記録時のCPU IDに関する情報。
- **セッションID**：ログに関連付けられたユーザーセッションのID。
- **クラス**：モジュール内のクラスまたはコンポーネント。

これらの詳細なタグにより、管理者は特定の基準に基づいてログを迅速にフィルタリング、検索、分析し、問題の特定と解決を容易にすることができます。

要約すると、AOTワークフローはCitrixコンポーネントがログを生成することから始まります。これらのログを収集するために一元的なリクエストが開始され、テレメトリサービスが関連コンポーネントからログを収集します。収集されたログは、インデックス作成、保存、およびその後の分析のために、一元化されたログサーバーに安全に転送されます。

AOTの仕組み

Citrix Always on Tracing (AOT) は、環境内の主要コンポーネントからログデータを継続的に取得します。トリガーされると、ログは自動的に収集され、一元化されたログサーバーに安全に転送され、分析のために保持されます。これにより、手動でのトレースが不要になり、トラブルシューティングが簡素化されます。

トレースのトリガーとログ収集：VDA、DDC、StoreFrontなどのCitrixコンポーネントは、重要な手順とエラーを追跡するためのAOT APIを搭載しています。これらのコンポーネントはAOTログジェネレーターとして機能します。管理者がDelivery Controllerからログ収集リクエストを開始すると、次のようになります。

- DDCは関連するCitrixコンポーネントに指示を送信します。各コンポーネントは、そのリクエストをローカルのテレメトリサービスに転送します。
- テレメトリーサービスは、AOTログを収集するためにリアルタイムAOTリスニングプログラムを開始し、ログを一元ログサーバーに転送します。

ログの保存と保持: AOTログを受信すると、一元ログサーバーはそれらをフォーマットし、構造化された検索可能なデータベースにインデックス化します。ログは、ストレージ使用量を最適化するために、定義された保持ポリシーに基づいて保持されます。デフォルトでは、AOTログは7日間保持され、その後、スペースを節約するために自動的にパージされます。

AOTと従来のログ記録の比較

側面	AOT	従来のCDFトレース
アクティベーション	自動、継続的	手動、問題の再現が必要
複雑さ	ユーザーフレンドリーで読みやすいログ	エンジニアリングレベルの解析
診断速度	即座にログが利用可能	再現作業により遅延
リソース使用量	最適化されたバッファによる低オーバーヘッド	誤って使用すると中程度から高程度

従来のトレースツールは手作業が必要で、問題が発生している最中に捕捉した場合にのみ機能します。AOTを使用すると、ログはバックグラウンドで継続的に実行されるため、監視していなくても問題が発生したときに捕捉されます。これにより時間が節約され、トラブルシューティングがはるかに簡単になります。

AOTのハイライト

- **常時稼働**: トレースは常に実行され、手動でオンにする必要はありません。
- **自動キャプチャ**: 問題が発生すると常にログが収集されます。
- **中央ログサーバー**: すべてのログは、簡単にアクセスできるように一箇所に保存されます。
- **トラブルシューティングの簡素化**: 一般的な障害を迅速に特定するのに役立ちます。
- **再現不要**: 問題を再現する必要はありません。すでに捕捉されています。

中央集中型 AOT ログサーバー

AOTログサーバーは、さまざまなCitrixコンポーネントからのAlways on Tracing (AOT) ログを収集および保存するための中央集中型宛先として機能します。Dockerテクノロジーを使用してコンテナ化されており、Linuxへの展開が推奨されますが、Docker Desktopを介したWindows環境やCitrix Connectorアプライアンス上でもサポートされています。

AOTログサーバーの主な機能

- **中央集中型ログストレージ**: 複数のCitrixコンポーネントからのログを、統合された検索可能な場所に集約します。
- **保持ポリシー**: ストレージ使用量とパフォーマンスを最適化するために、構成可能なポリシー（デフォルト：7日間）に基づいてログが保持されます。
- **展開**: ログサーバーは、パッケージ化されたインストーラースクリプトとDockerコンテナを使用して展開されます。セットアップには、互換性のあるハードウェアとDockerランタイム環境、またはCloud Connectorアプライアンス（選択した場合）が必要です。
- **セキュアなログアクセス**: ログは、ログサーバーに含まれるCLIツールを使用して取得できます。すべてのアクセスには、セキュリティとコンプライアンスを確保するために適切な認証が必要です。
- **Citrixコアコンポーネントとの統合**: AOTテレメトリーサービスはCitrixコアコンポーネントに組み込まれており、それらがログジェネレーターとして機能できるようにします。テレメトリーサービスは、これらのコンポーネント全体でシームレスかつ自動化されたログキャプチャを保証し、Citrixインフラストラクチャ全体で一貫したログの可視性を可能にします。

AOTログサーバーの展開と構成

AOTの前提条件

AOTログサーバーは、機能するためにDockerコンテナテクノロジーに依存しています。Linuxが推奨されるホストオペレーティングシステムですが、Docker Desktopを使用すればWindowsへのインストールも可能です。あるいは、Citrix Connector Applianceを使用すると、ホストとDockerインフラストラクチャを管理する必要がなくなるパッケージソリューションが提供されます。

1つのログサーバーは、常に**最大128,000のアクティブなコンポーネント接続**をサポートでき、**毎秒最大10,000のログイベント**を処理できます。サイジングまたは展開の推奨事項は、次の2つの要因に基づいている必要があります。

- **接続容量**は、同時に接続できるコンポーネントの数を決定します。
- **ログスループット**は、パフォーマンスに影響を与えることなくシステムが取り込み、インデックス化できるログの数を決定します。

環境がこれらの制限内に収まっている限り、単一のログサーバーで十分です。

シトリックス コネクタアプライアンス

- Citrix Connector Appliance の最新バージョンを実行していることを確認してください。
- お持ちでない場合は、Citrix Cloud から最新バージョンをダウンロードしてインストールしてください。

リナックス

- **サポートされているOS**: Ubuntu 24.04 および RHEL 8.10、9.4
- **ハードウェア要件**: 4コアCPU、16 GB RAM、500 GBの空きディスク容量。
- **ソフトウェア要件**: Linux 用 Docker Engine または Linux 用 Docker Desktop をインストールします。
- **ユーザー権限**: ユーザーが root 権限を必要とせずに Docker を起動できることを確認してください。

ウィンドウズ

- **サポートされているOS**: Windows 11、Windows 10、Windows Server 2022、Windows Server 2025。Azure VM については、こちらで推奨事項 を参照してください。
- **ハードウェア要件**: 8コアCPU、24 GB RAM、500 GBの空きディスク容量。
- **ソフトウェア要件**: Windows 用 Docker Desktop をインストールします (サブスクリプションが必要な場合があります)。

- **WSL バージョン 2.1.5** 以降が必要です。
- **Hyper-V** と **Containers** の Windows 機能を有効にします。
- Docker Desktopの設定でメモリ制限を12 GB以上に設定します。

ログサーバーの推奨事項

1日のログ量 (ストレージ)

項目	マシンの数	1日あたりのセッション数/マシン	セッションあたりの平均ログサイズ	1日あたりの合計ログ数
永続VDA	1000	2	2 MB	4,000 MB (約4 GB)
プールされたVDA	1000	50	2 MB	100,000 MB (約100 GB)
CWAエンドポイント	8000	4	1-1.5 MB	48,000 メガバイト (≈48 ギガバイト)
デリバリーコントローラー	4	—	DDCあたり300 MB	1,200 メガバイト (≈1.2 ギガバイト)
StoreFrontサーバー	4	—	サーバーあたり300 MB	1,200 MB (約1.2 GB)
NetScaler Gateway /PVS/ Session Recording/ FSAおよびその他のサーバー	4	—	サーバーあたり300 MB	1,200 MB (約1.2 GB)
1日の合計ログサイズ（圧縮後）	—	—	—	**圧縮前は約156 GB/日**
				圧縮後は80 GB～125 GB/日

サイジングの前提条件

- この例は、約10,000の管理対象エンドポイントとインフラストラクチャコンポーネントのリファレンス展開を表しています。
- サイジングの目的では、Delivery Controllers、StoreFrontサーバー、Gateway、PVS、FAS、Session Recording、およびその他のインフラストラクチャコンポーネントは、サーバーあたり1日300 MBと見積もられています。
- サーバーあたり300 MBという値は、ストレージ計画と容量計算に使用される控えめな見積もりです。

注:

1. これらの値はおおよそのものであり、展開によって大きく異なる場合があります。ログの量は、サイトの規模、ユーザーアクティビティ、コンポーネントの組み合わせ、および保持の必要性によって異なります。これらの数値は、計画を開始するためのベースラインとしてのみ使用し、環境の実際の使用状況、成長傾向、およびパフォーマンス テストに基づいてストレージ割り当てを調整してください。
2. ログサーバーはデフォルトでLZ4圧縮アルゴリズムを使用します。圧縮率は20%から50%の間になる可能性があります。これは、最大圧縮時にはLogServerがディスクスペースの半分を占め、最小圧縮時には80%を占めることを意味します。
3. 単一のAOTログサーバーは、最大**128,000のアクティブなコンポーネント接続**をサポートし、**毎秒最大10,000のログイベント**を処理できます。ログサーバーは、環境がこれらの接続およびスループットのしきい値内にある限り、AOTログを24時間体制で継続的に収集および保存するように設計されています。
4. これらの推奨事項は、仮想マシンのサイズではなく、受信AOTログを取り込み、処理し、保存する基盤となる**検索およびインデックス作成エンジン**の容量によって決定されます。この検索レイヤーは、インデックス作成、クエリ、および保持操作を処理するため、最終的に最大規模を決定します。環境が成長するにつれて、このレイヤーはパフォーマンスを維持するために水平方向にスケーリングする必要があります。
5. 現在、ログサーバーは、ログサーバーサービスと検索/インデックスエンジンを両方含む単一の結合ノードとして提供されています。これにより展開は簡素化されますが、検索層を独立してスケーリングする能力が制限されます。
6. 今後のリリースでは、Citrixは**分離されたアーキテクチャ**に移行し、取り込みとストレージ/インデックス作成が独立したノードで実行されるようになります。これにより、顧客は環境の成長に合わせて検索層をスケーリングし、大規模またはマルチサイト展開での

パフォーマンスを向上させ、現在のシングルノード設計によって課せられるスケーラビリティの制限を取り除くことができます。

7. AOTログサーバーをSSD対応ストレージに展開します。特に大容量環境では、信頼性の高いログ取り込み、高速な検索パフォーマンス、効率的な相関関係を確保するために、SSDが強く推奨されます。

AOTログサーバーのストレージサイジング

ストレージを適切にサイジングすることは、AOTログサーバーを計画する上で最も重要なステップの1つです。必要なストレージの総量は、AOTログを送信するマシンの数、1日に生成されるデータ量、およびログを保持する必要がある期間によって異なります。

各Citrix環境の動作は異なるため、お客様はまず、VDA、Citrix Workspaceアプリのエンドポイント、Delivery Controller、StoreFrontサーバーのログ生成パターンを使用して、1日のログ量を推定することから始める必要があります。1日の量がわかれば、以下の式を使用して総ストレージを計算できます。

ストレージ計算式 総ストレージ (GB) = 1日のログ量 (GB) × 保持日数

AOTログサーバーのストレージサイジングガイダンス

展開規模に基づいた1日のログ量とストレージ要件の推定には、以下の表を参照してください。これらの推定値は容量計画を目的としており、ユーザーアクティビティ、セッション密度、有効なコンポーネント、および展開アーキテクチャによって異なる場合があります。

1日のログ量推定

展開規模	圧縮前の1日のログ量	圧縮後の1日のログ量 (LZ4)	推奨カテゴリ
5,000台のマシン	約78 GB/日	約40〜63 GB/日	小規模
10,000台のマシン	~156 GB/日	~80〜125 GB/日	中
50,000台のマシン	~780 GB/日	~400〜625 GB/日	大規模
100,000台のマシン	~1.56 TB/日	~800 GB〜1.25 TB/日	エンタープライズ

保持期間に基づくストレージの見積もり

展開サイズ	7日間の保持	10日間の保持
5,000台のマシン	~300〜450 GB	約400〜630 GB
10,000台のマシン	約600 GB〜1 TB	約800 GB〜1.25 TB
50,000台のマシン	約3〜5 TB	約4〜6.3 TB
100,000台のマシン	約6〜10 TB	約8〜12.5 TB

注:

- これらの値は、キャパシティプランニングを目的としたおおよその見積もりです。実際のストレージ要件は、展開アーキテクチャ、ユーザーアクティビティ、有効なコンポーネント、保持期間、および圧縮効率によって異なります。
- 見積もりは、10,000台のマシンリファレンス展開モデルに基づいており、線形にスケーリングされています。

Always on Tracing (AOT) の最小サポートバージョン

この表は、Always On Tracing (AOT) のログ収集を有効にするために必要なCitrixコンポーネントの最小サポートバージョンを示しています。バージョン要件は、ユーザーがリソースにアクセスする方法（**直接アクセス** (例: StoreFrontへの直接アクセス) または **ゲートウェイ経由のアクセス** (Citrix Gateway または Cloud Gateway Services)）によって異なる場合があります。

コンポーネント / プラットフォーム	タイプ	最小バージョン (直接アクセス)	最小バージョン (ゲートウェイ経由のアクセス)
シトリックス ワークスペース アプリ ウィンドウズ	クライアント	2511.10 および 2507 CU1 以降	2603 および 2507 CU2 以降
シトリックス ワークスペース アプリ マック	クライアント	2603以降	2603以降

コンポーネント / プラットフォーム	タイプ	最小バージョン (直接アクセス)	最小バージョン (ゲートウェイ経由のアクセス)
シトリックス ワークスペース アプリ リナックス	クライアント	近日公開予定	近日公開予定
Citrix Workspace アプリ HTML5	クライアント	2511以降	2603以降
Citrix Workspace アプリ ChromeOS	クライアント	2511以降	2603以降
シトリックス ワークスペース アプリ アンドロイド	クライアント	2603以降	2603以降
Citrix Workspaceアプリ iOS	クライアント	2603以降	2603以降
Citrix Virtual Apps and Desktops (Windows VDA、DDC、PVS、FAS、セッションレコーディング、STF、Linux VDA、Mac VDA、WEM、UPM)	プラットフォーム	2402 CU4、2507 CU1、2511以降	2402 CU4、2507 CU1、2511以降
シトリックス ダース *	サービス	2026年2月以降	2026年2月以降
シトリックス ネットスケーラー	インフラストラクチャ	14.1.60.57	14.1.60.57
Citrix ライセンスサーバー		540000以降	54000以降

*Citrix DaaS展開の場合、AOTログ収集は同じプロセスに従います。ログをAOTログサーバーに転送するようにDaaS設定を構成する必要があります。リソースの場所に展開されたすべてのコンポーネントは、構成されるとログをログサーバーに転送できます。Citrix DaaSコントロールプレーンコンポーネントは、顧客管理のログサーバーにログを送信せず、代わりにCitrix管理のクラ

ウドテレメトリ（Splunk）にログを転送し続けます。この動作は、これらのクラウドコントロールプレーンコンポーネントが、該当する場合にWorkspace Platformの代わりにStoreFrontを使用したり、Cloud Gateway Servicesの代わりにCitrix Gatewayを使用したりするなど、顧客管理のCVADコンポーネントに置き換えられたり補完されたりしない限り適用されます。異なる展開モデルでのログの可用性の詳細については、「AOT Logs Availability Across Deployment Scenarios」セクションを参照してください。

注:

ダイレクトアクセスとは、Gatewayが関与しないシナリオ（例：StoreFrontへの直接アクセス）を指します。

Access via Gateway には、Citrix Gateway および Cloud Gateway Services (CGS) が含まれます。

「Coming soon」は、今後のリリースでサポートが予定されていることを示します。

ログサーバーのインストールと構成

ログサーバーは、個別のLinuxまたはWindowsサーバーにセットアップすることも、Citrix Connector Applianceでホストして常時更新を利用することもできます。各オプションのインストールおよび構成手順については、関連セクションを参照してください。

インストールに関する注意

- セキュリティを強化するため、展開ではHTTPSの使用を推奨します。
- 選択したポートが既に使用されていないことを確認してください。
- 管理者またはシステムレベルの権限が必要なため、特権ポート（0〜1023）の使用は避けてください。
- ファイアウォールルールが選択したポートでのトラフィックを許可していることを確認してください。
- 有効な範囲（0〜65535）内のポート番号を使用しますが、競合を避けるため、システムサービスで一般的に使用されるポートは避けてください。

- Citrix Connector Applianceを使用してログサーバーを展開する場合は、ポート443のみが構成されていることを確認してください。
- 例で使用されているポート番号（HTTPの場合は8080、HTTPSの場合は8443）は参照用です。これらのポートを厳密に使用する必要はありません。環境に基づいて適切なポート番号を選択し、AOTログサーバーを構成する際には、上記のインストールガイドラインに従ってください。

Citrix Connector Applianceを介したログサーバーのインストール

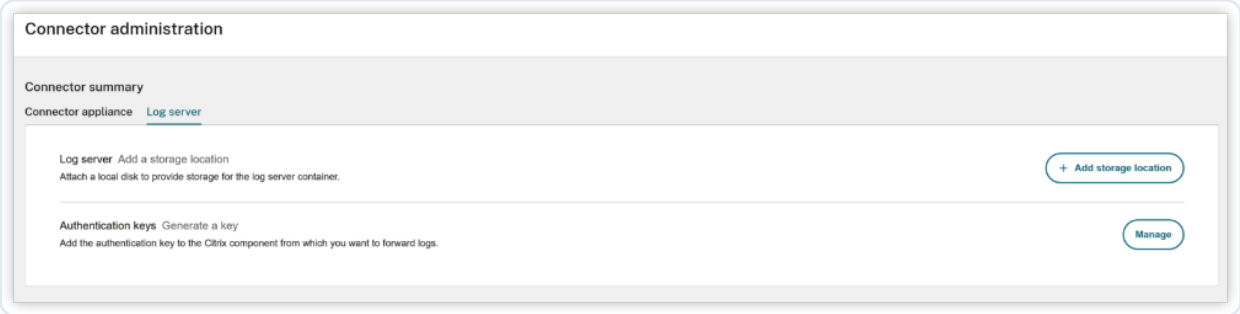
ログサーバーはCitrix Connector Appliance内に展開できます。このアプローチにより、ホストVMの展開と管理、イメージの手動ダウンロード、またはコンテナコマンドの実行が不要になります。ログサーバーは、Connector Applianceのアップグレード中に自動的にオンボーディングされ、継続的なコネクタの更新を通じて最新の状態に保たれるため、常に最新バージョンを使用できます。詳細については、「コネクタアプライアンスの更新」を参照してください。

Citrix Connector Applianceを介してログサーバーを展開する手順

1. 環境にConnector Applianceがまだない場合は、ハイパーバイザーまたはパブリッククラウドマーケットプレイスからアプライアンスを展開します。必要なCitrix Connector Applianceの最小バージョンは11.4.1.444です。インポート後、アプライアンスをCitrix Cloudに登録します。詳細については、「コネクタアプライアンスの入手」を参照してください。
2. デフォルトでは、Connector Applianceには2つのvCPUと4GBのメモリが搭載されています。ログサーバーの要求を処理するために、リソースを少なくとも4つのvCPUと16GBのメモリに増やしてください。
3. サポートされているコンポーネントがLog Serverのホスト名を解決できるように、Connector Appliance FQDNのDNS「A」レコードを作成します。Connector ApplianceをActive Directoryドメインに参加させることはオプションです。
4. Cloud Monitorは、リソースの場所にある**サポートされているWindows Cloud Connectorで実行されているMonitor Connectorサービス**を介してAOTログを取得します。Log ServerがCitrix Connector Applianceに展開されている場合、サポートされているWindows Cloud Connectorも同じリソースの場所に存在する必要があります。Connector Applianceだけでは、Cloud MonitorがAOTトレースを取得するには不十分です。Cloud Connectorは、バージョン **6.141.0.13739** (または**4.420.0.13739**) 以降を実行している必要があります。以前のバージョンでは、`GetAotTraces` API呼び出しが失敗し、MonitorでHTTP 500エラーが発生します。
5. Connector Applianceは、Connector Appliance管理ページに接続するブラウザに提供される自己署名証明書を提供します。HTTPS経由でログサーバーに接続できるようにするには、この自

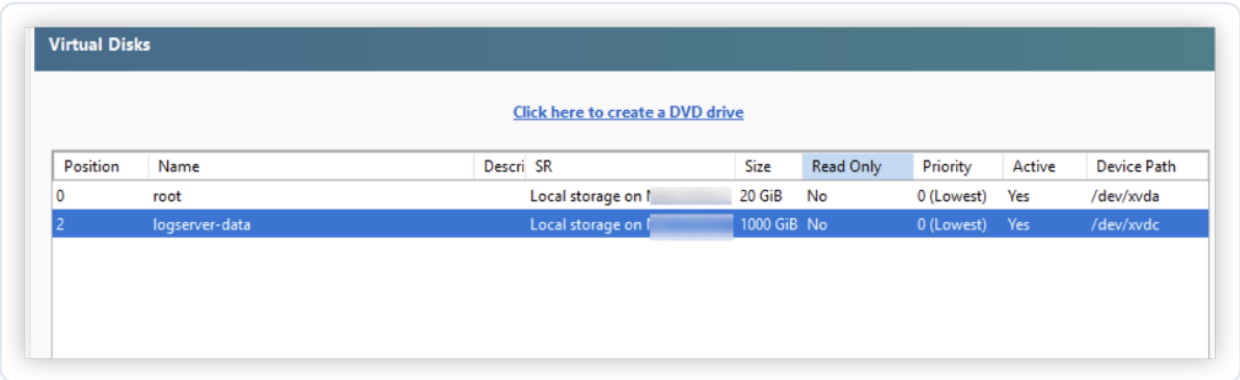
己署名証明書を、組織によって署名された、または組織の信頼チェーンを使用して生成された独自の証明書に置き換える必要があります。詳細については、証明書の管理 または サーバー証明書の置き換え を参照してください。

6. アップグレードが完了したら、`https://<connector-appliance-FQDN>/?enable=logserver` のConnector Appliance UIにログインし、「?enable=logserver」があることを確認して、ログサーバーUIを表示できるようにします。新しいLog Serverタブには、ストレージと認証キー管理オプションが表示されます。



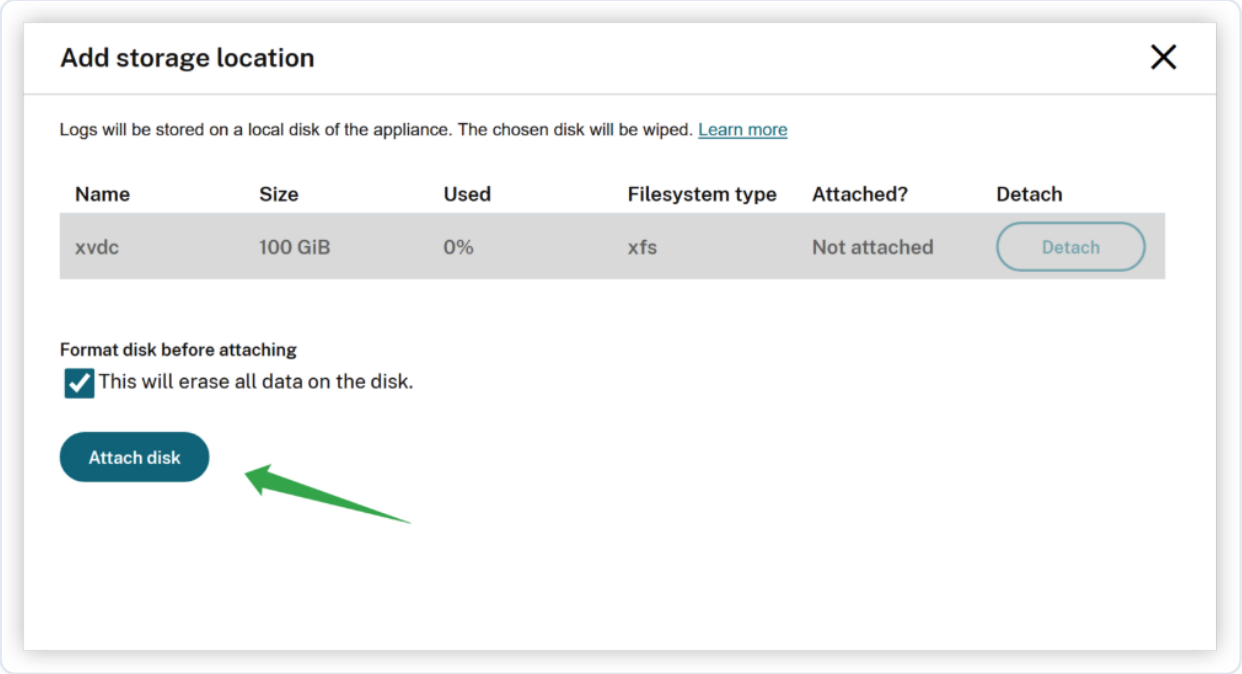
7. コネクタアプライアンスのブートディスクの容量は20GBです。ログサーバーで効率的なログストレージをサポートするには、ハイパーバイザーまたはクラウド管理プラットフォームを使用して、コネクタアプライアンスに別の仮想ディスクを追加する必要があります。この追加ディスクには、ログストレージのニーズを満たすのに十分なスペースが必要です（前のセクションで説明したとおり）。

   以下のXenServerのスクリーンショットは、追加ディスクが構成されたコネクタアプライアンスの例を示しています。

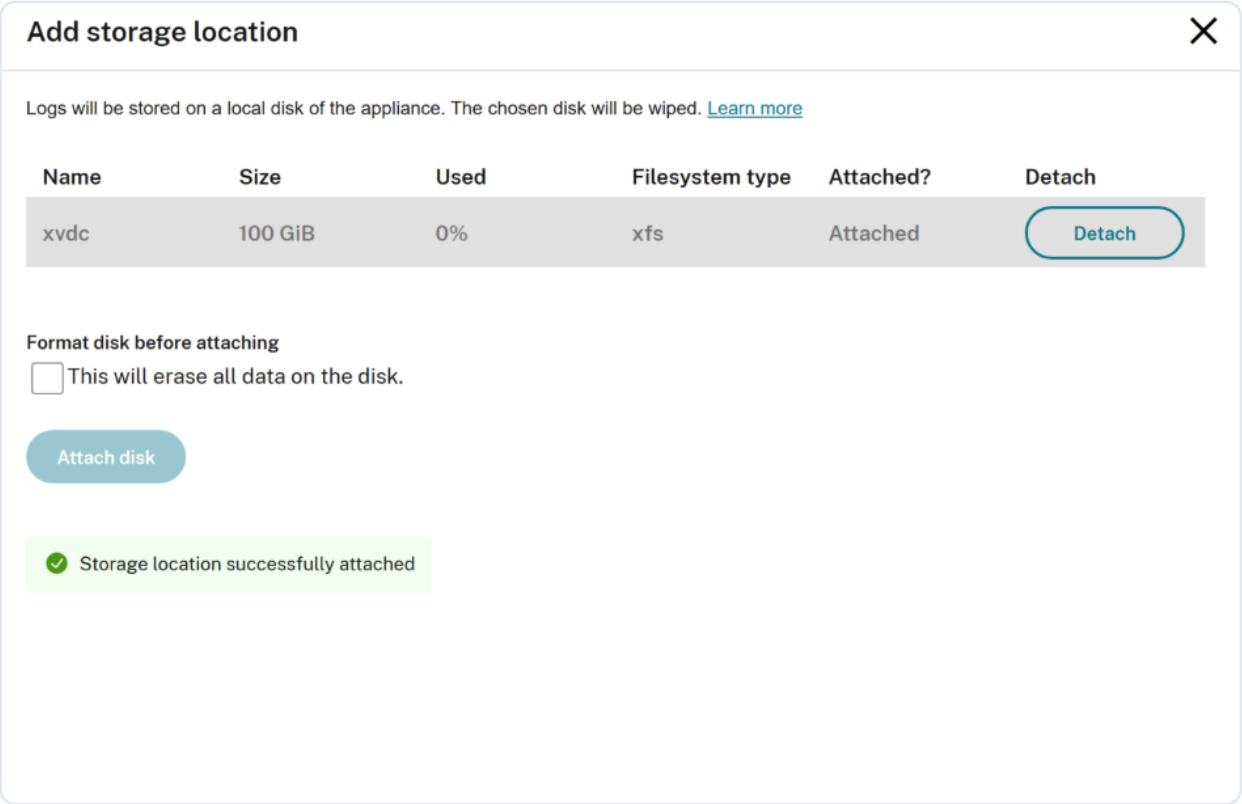


> **注:**
>
> **VMware ESXi の既知の要件:** ユーザーは、追加のデータディスクをルートディスクが使用する SCSI コントローラーとは異なる SCSI コントローラーに接続する必要があります。

8. キーディスクを追加すると、ログサーバーUIが自動的にそれを検出し、Connector Appliance上のログサーバーコンテナにフォーマットしてマウントできるようになります。



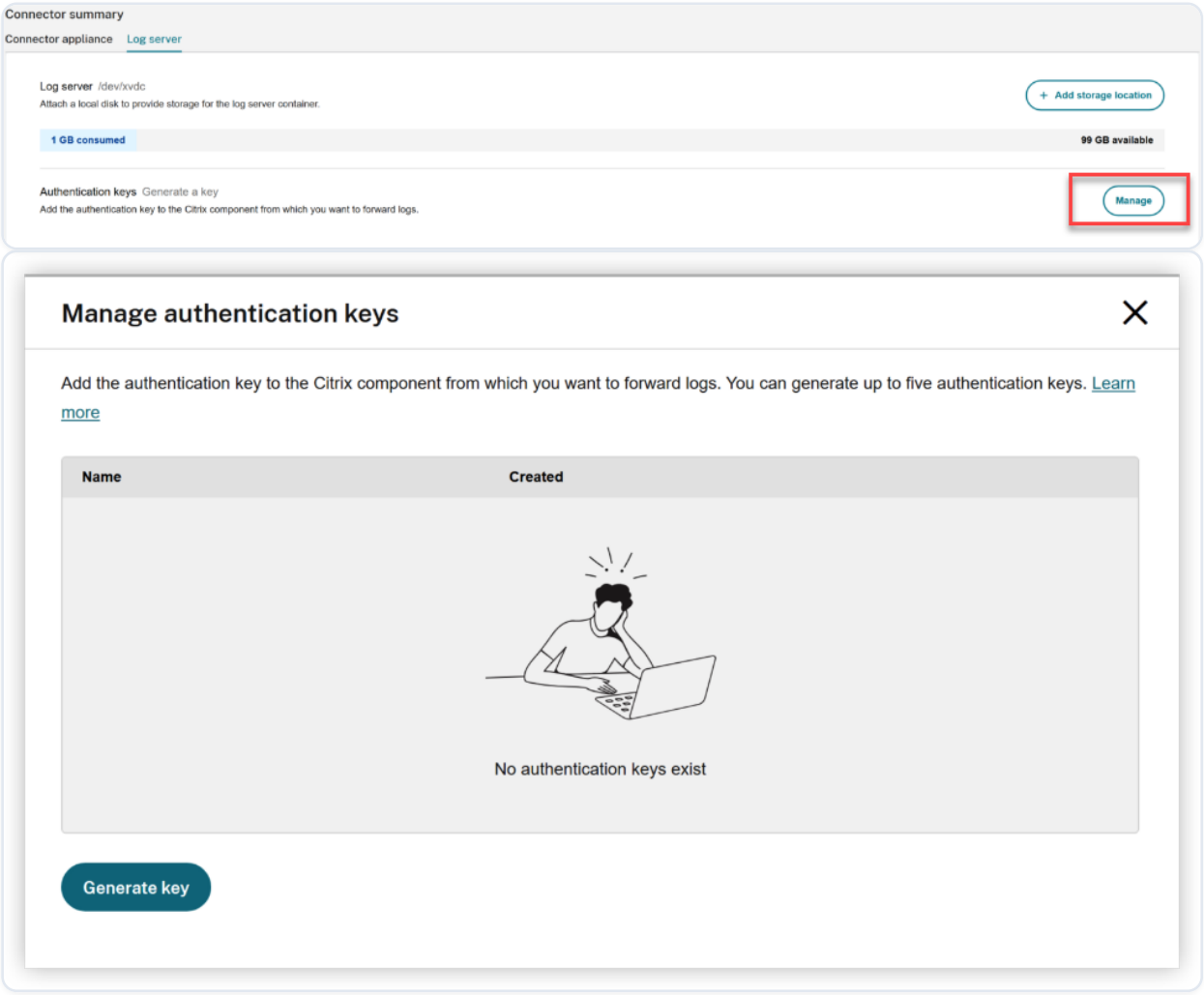
9. 「ディスクの接続」ボタンをクリックすると、ディスクはログサーバーコンテナにマウントされます。

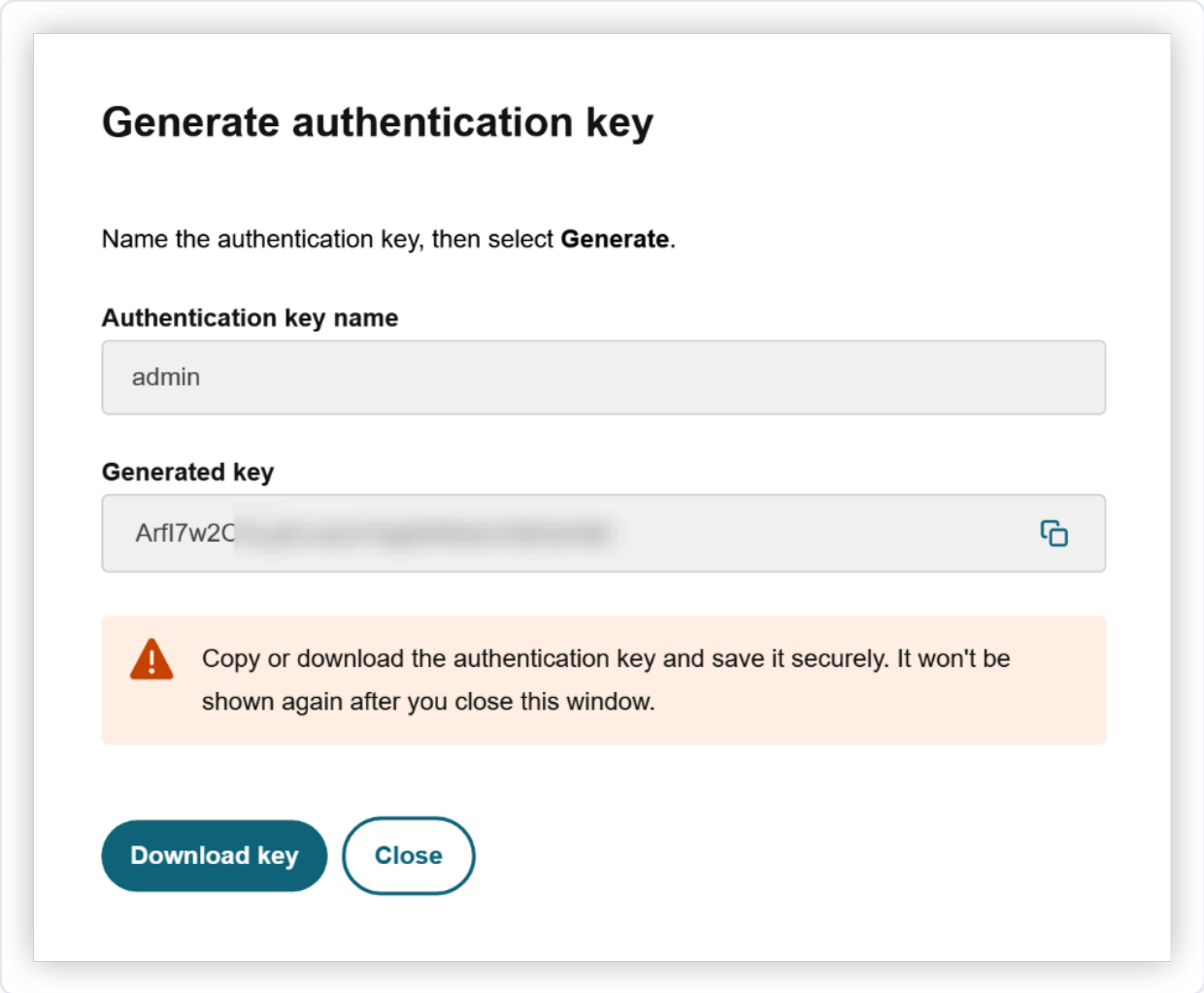


10. メインページには、ディスクサイズと、使用済みスペースおよび残りのスペースに関する情報が表示されます。



11. ディスクが接続されたら、ping エンドポイント `https://<connector-appliance-FQDN>/ctxlogserver/Ping` を呼び出して、Log Server が実行されていることを確認します。pong 応答は、Log Server が正常に起動したことを確認します。
12. 「管理」ボタンをクリックし、「キーを生成」をクリックします。次に、ロール名を入力し、認証キーをコピーまたはダウンロードします。ウィンドウを閉じると、キーは再度表示されません。





Linuxへのインストール

1. ログサーバーのDockerコンテナイメージを(https://www.citrix.com/downloads/citrix-tools/citrixtoolspage/CitrixAlwaysOnTracing-LogServer-2507CU1.html)からダウンロードします。
2. ダウンロードしたファイルを同じディレクトリに配置します。
3. ターミナル (Linux) またはコマンドプロンプト (Windows) を使用して、そのディレクトリでインストーラーを実行し、指示に従います。

```
chmod +x ./InstallLogServer



#Install with https mode with port 8443 with default path

./InstallLogServer --https --cert </path/your_private_cert_key.pfx> --port
8443
```

```
#Install with http mode, with port 8080 with default path

./InstallLogServer --port 8080



#Command to change the config path and data path of your choice with https
mode

./InstallLogServer --https --cert </path/your_private_cert_key.pfx> --port
8443 --config /Path/LogServer/Config --database /Path/LogServer/Data



#Command to change the config path and data path of your choice with http
mode

./InstallLogServer --port 8080 --config /Path/LogServer/Config --
database /Path/LogServer/Data



#To support CWA client uploading AOT logs, some additional parameters need
to be added after the install log server command.

--sta-server http://STA_SERVER_FQDN:port --log-server LOG_SERVER_FQDN:PORT
```

ここで、,

- STA_SERVER_FQDNは、STAサーバーのホスト名またはIPアドレスです（オンプレミスインストールでは、STAサーバーは通常DDCとともにインストールされます）。
- LOG_SERVER_FQDNとPORTは、ログサーバー自体のホスト名と、指定されたポート（8080、8443、またはインストールパラメーターの–port値）です。
- ログサーバー証明書 your_private_cert_key.pfx は、AOTクライアントがTLS接続を使用してログをアップロードする他のCitrixコンポーネントによって信頼されている必要があります。

STA_SERVERアドレスを使用すると、セッションタイムアウト後など、StoreFrontが再接続STAチケットを提供できない場合に、ログサーバーがCitrix Workspaceアプリ (CWA) クライアントに再接続STAチケットを発行できます。これにより、接続が切断された場合でも、CWAクライアントはログサーバーと直接接続を再確立できます。

LOG_SERVERアドレスは、ログサーバーが構成済みのSTAサーバーからSTAチケットを要求するときに使用されます。STAサーバーは、ログサーバーエンドポイントへの接続を特別に承認するチケットを返します。

CWAクライアントが再接続STAチケットを必要としない場合、またはゲートウェイなしでLogServerに直接接続する場合は、これらのパラメーターはオプションです。

Linuxでのインストール後

インストール後、いくつかの便利なスクリプトファイルが生成されます。

```
# In Linux, sh scripts will be generated

DownloadLogsByTime.sh

DownloadLogsByWords.sh

GetAuthKey.sh

ListMachines.sh

StartLogServer.sh
```

LogServerが正常に起動したことを確認するには、`./StartLogServer.sh to start the server. Check your configpath/weblogs.txt`を使用します。

LogServerが正常に起動した場合、weblogsファイルに以下のメッセージが表示されます。ポート5000は、選択されたhttpまたはhttpsプロトコルで、LogServerによってDockerコンテナ内で内部的に使用されます。

```
Now listening on https://[::]:5000
```

ログサーバーがHTTPモードでインストールされた場合、成功したログには以下が表示されます。

```
Now listening on http://[::]:5000
```

LogServerがHTTPSを使用する場合、AOTログをアップロードするすべてのマシンでその証明書が信頼されていることを確認してください。

> **注:**

- インストール手順で構成されたポート（8080または8443、あるいは指定された任意のポート）は、DDC、Storefront、VDAなどでLogServerのURLを構成する際に使用する必要があります。
- 通常、Linuxでの起動には30秒から60秒かかります。

Windowsへのインストール

1. ログサーバーのDockerコンテナイメージをCitrix downloadsからダウンロードします。
2. ダウンロードしたファイルを同じディレクトリに配置します。
3. ターミナル（Linux）またはコマンドプロンプト（Windows）を使用して、そのディレクトリでインストーラーを実行し、指示に従います。

ステップ1

ログサーバーVMにWindows用Docker Desktop（サブスクリプションが必要な場合があります）をインストールします。WSL 2に依存するWindowsシステムでDocker Desktopが正しくインストールされ、起動することを確認するには、以下の手順に従ってください。

1. Docker Desktopの設定でメモリ制限を12 GB以上に設定します。
2. Docker Desktop には以下の Windows 機能が必要です。これらの機能が有効になっていることを確認してください。
   - ハイパーブイ
   - 仮想マシン プラットフォーム
   - Linux 用 Windows サブシステム (WSL)
3. 不足している機能がある場合は、それらをインストールし、VM を再起動して変更を適用してください。
4. システムの再起動後、**PowerShell** を管理者として実行し、コマンド `wsl --update` を実行して WSL を更新します。
5. Docker Desktop には WSL 2 が必要です。コマンド `wsl --set-default-version 2` を実行して、WSL 2 を既定として構成します。
6. WSL が更新され、必要な Windows 機能が有効になると、Docker Desktop Engine は正常に起動するはずです。

ステップ 2

インストールを続行するには、以下のコマンドを実行します。

> **注:**
>
> Config および Database (Data) フォルダーの既定の場所は C:\Users\<username>\LogServer の下に作成されます。以下のコマンドで変更できます。

```
#Install with https mode with port 8443 with default path

InstallLogServer.exe --https --cert <c:\path\cert.pfx> --port 8443



#Install with http mode, with port 8080 with default path

InstallLogServer.exe --port 8080



#Command to change the config path and data path of your choice with https mode

InstallLogServer.exe --https --cert <c:\path\cert.pfx> --port 8443 --config C:\LogServer\Config --database C:\LogServer\Datacmd



#Install with specific config path and data path

InstallLogServer.exe --port 8080 --config C:\LogServer\Config --database C:\LogServer\Datacmd



#To support CWA client uploading AOT logs, some additional parameters need to be added after the install log server command.
```

```
--sta-server http://STA_SERVER_FQDN:port --log-server LOG_SERVER_FQDN:PORT
```

ここで、,

- STA_SERVER_FQDN は STA サーバーのホスト名または IP アドレスです (オンプレミス インストールでは、STA サーバーは通常 DDC とともにインストールされます)。
- LOG_SERVER_FQDN と PORT は、ログサーバー自体のホスト名と、指定されたポート (8080、8443、またはインストールパラメーターの –port 値) です。
- ログサーバー証明書 your_private_cert_key.pfx は、AOT クライアントがログをアップロードするために TLS 接続を使用する他の Citrix コンポーネントによって信頼されている必要があります。

STA_SERVER アドレスにより、LogServer は、セッションタイムアウトのために StoreFront が再接続 STA チケットを提供できない場合に、CWA クライアントに再接続 STA チケットを供給できます。その結果、CWA クライアントは、接続障害が発生した場合に LogServer から直接再接続チケットを取得できます。

LOG_SERVERアドレスは、ログサーバーがSTA_SERVERからSTAチケットを要求する際に利用されます。STA_SERVERは、LOG_SERVERアドレスへの接続のみを承認するSTAチケットを発行します。

CWAクライアントが再接続STAチケットを必要としない場合、またはゲートウェイなしでLogServerに直接接続する場合は、これらのパラメータはオプションです。

Windowsでのインストール後

インストール後、インストーラーファイルを保存したのと同じディレクトリに、いくつかの便利なスクリプトファイルが生成されます。

注:

これらのファイルを別の場所に移動できます。ただし、ログサーバーを構成する際に再度必要となるため、新しい場所を覚えておいてください。

```
#In Windows, bat scripts will be generated in the same directory where you saved the installer files.

DownloadLogsByTime.bat
```

DownloadLogsByWords.bat

GetAuthKey.bat

ListMachines.bat

StartLogServer.bat

ログサーバーを起動するには、`StartLogServer.bat`を使用します。

LogServerが正常に起動したことを確認するには、`configpath\weblogs.txt`を確認してください。

ログに以下が表示された場合、ログサーバーが正常に起動したことを意味します。LogServerが正常に起動すると、weblogsファイルに以下のメッセージが表示されます。ポート5000は、選択されたhttpまたはhttpsプロトコルを使用するDockerコンテナ内でLogServerによって内部的に使用されます。

```
Now listening on: https://[::]:5000
```

ログサーバーがHTTPモードでインストールされた場合、成功したログには以下が表示されるはずです。

```
Now listening on: http://[::]:5000
```

LogServerがHTTPSを使用する場合、AOTログをアップロードするすべてのマシンでその証明書が信頼されていることを確認してください。

注:

- インストール手順で構成されたポート（8080または8443、あるいは指定された任意のポート）は、DDC、Storefront、VDAなどでログサーバーのURLを構成する際に使用する必要があります。
- 通常、Windowsではハードウェアによって1〜10分かかります。

相互TLS認証（オプション）

相互TLS (mTLS) は、ログサーバーとクライアント (VDA、DDC、StoreFront、CWA) の間にセキュリティの追加レイヤーを提供します。mTLSが有効になっている場合、クライアントとサーバーの両方が、エンタープライズPKIによって発行された証明書を使用して相互に認証します。

mTLSは、次のような環境で役立ちます。

- ネットワークセグメントが信頼されていないか、共有されている
- ログサーバーだけでなく、各AOTログクライアントも認証する必要がある
- 顧客が不正なシステムからのログデータ送信を防止したい
- 規制またはコンプライアンスポリシーにより、証明書ベースの認証が必要である。

mTLSはオプションですが、信頼されたCitrixコンポーネントのみがログサーバーと通信できるようにし、ログサーバーがテレメトリデータを受け入れる前にすべての着信接続を検証できるようにすることで、セキュリティを強化します。

証明書の要件

mTLSを構成するには、次の証明書を生成する必要があります。

- **aotclient.pfx** – AOTログクライアント（VDA、DDC、StoreFront、CWA）が使用する証明書
- **logserver.pfx** – ログサーバーが使用する証明書
- **enterprise-ca.cer** – 両方の.pfxファイルに署名するために使用されるルートまたは中間証明書

> **注**
>
> - Citrix Connector Applianceを使用している場合、この相互TLSセクションはサポートされていないためスキップしてください。
> - enterprise-ca.cerファイルは、ログサーバーとテレメトリクライアントの両方の信頼されたルート証明機関ストアにインポートする必要があります。
> - aotclient.pfxおよびlogserver.pfx証明書はパスワードで保護しないでください。
> - aotclient.pfxのサブジェクトはCitrixAOTClientである必要があります。これにより、テレメトリクライアントは実行時に証明書を自動的に見つけることができます。

> mTLSを有効にするには、ログサーバーのインストールコマンドに--caパラメーターを含めます。 このパラメーターは、enterprise-ca.cer証明書へのパスを指定します。

```
# with default path

./InstallLogServer --https --cert logserver.pfx --ca enterprise-ca.cer --
port 8443



# with customized path

./InstallLogServer --config /YourPath/LogServer/Config --database /
YourPath/LogServer/Data --cert /YourPath/logserver.pfx --ca /YourPath/
enterprise-ca.cer --port 8443



# delete temp certificate logserver.pfx in current install directory

sudo rm -rf /YourPath/logserver.pfx



# keep logserver.pfx accessed only by the container process user 'ubuntu'.

sudo chmod 400 LogServer/Config/logserver.pfx

sudo chown ubuntu:ubuntu LogServer/Config/logserver.pfx
```

相互TLS認証が必要な場合は、DDC、Storefront、VDA、およびその他のCVADコンポーネントで管理者権限を使用して、次のPowerShellコマンドを実行します。

```
# import client cert at the machine aot client

Import-PfxCertificate -CertStoreLocation Cert:\LocalMachine\My\ -FilePath
c:\aotclient.pfx



# Verify successful import

Get-ChildItem Cert:\LocalMachine\My | Where-Object { $_.Subject -like
"*AOTclient*" }
```

```
# delete temp certificate aotclient.pfx

Remove-Item -Path "C:\aotclient.pfx" -Force

# Ensure LogServer’s certificate is trusted on all machines uploading AOT
logs.
```

注:

テレメトリサービスは「ネットワークサービス」アカウントで実行されているため、certlm.mscグラフィカルインターフェイスを使用して、CitrixAOTClient証明書の秘密キーに対するNETWORK SERVICEのフルコントロールを手動で付与する必要があります。

1. Win + Rを押し、certlm.mscと入力してEnterキーを押し、証明書（ローカルコンピューター）コンソールを開きます。
2. 証明書（ローカルコンピューター） > 個人 > 証明書を展開します。
3. 右側のペインで、CitrixAOTClientに発行された証明書を見つけます。
4. 「秘密キーの管理」を開きます
5. 証明書を右クリックし、 > を選択します。
6. アクセス許可ダイアログで、 を選択し、「NETWORK SERVICE」と入力して、 をクリックします（NT AUTHORITY\NETWORK SERVICEに解決されるはずです）。
7. をクリックしてアクセス許可を適用します。

お客様が自己署名証明書を提供する場合、次のようにします。

- ログサーバー側では、logserver.pfxとaotclient.cerが前述のとおりインストールされます。aotclient.cerはenterprise-ca.cerの役割を果たします。
- クライアント側では、aotclient.pfxとlogserver.cerが前述のとおりインポートされます。logserver.cerはenterprise-ca.cerの役割を果たします。
- 詳細については、「新しい証明書の作成」を参照してください。

ログサーバーの確認

Log Server、VDA、またはDDCでブラウザを開き、`<http://YourLogServerFQDN:8080/Ping>` にアクセスします。

ブラウザに「Pong UTC:08/19/2025 01:03:29 Version: 2511.1.6」という応答文字列が表示されます。UTC時刻はLogServerのUTC時刻である必要があります。バージョン文字列には、リリース名とビルダー番号が含まれます。

> **注:**
>
> デフォルトポートを使用していない場合は、ポート8080を構成済みのポートに変更し、HTTPSモードでインストールされている場合はhttpをhttpsに変更します。

> ログサーバーの検証に失敗した場合は、以下のログを確認してください。

- docker logs logserver を実行して、dockerログを確認します。
- Linuxの場合 - `$HOME/LogServer/Config/weblogs.txt` (デフォルトを使用していない場合は、$HOME/LogServer を実際のインストールパスに変更してください)
- Windowsの場合 - `C:\Users\YourUserName\LogServer\Config\weblogs.txt` (YourUserName を実際のユーザー名に変更してください。デフォルトを使用していない場合は、C:\Users\YourUserName\LogServer を実際のインストールパスに変更してください)

ログサーバーの詳細設定

LinuxまたはWindowsの場合

`docker stop logserver` を実行してログサーバーを停止します

デフォルトでは、ログサーバーは以下の値で構成されています。変更を行うには、`StartLogServer.sh` を編集するか、Windowsにインストールされている場合は `StartLogServer.bat` を編集します。

```
-e MAX_RESERVE_DAYS=7

-e MAX_DISK_USAGE_PERCENTAGE=85

-e LOCAL_DOWN_ONLY=true
```

```
-e OPENSEARCH_JAVA_OPTS="-Xms2G -Xmx2G"
```

LOGSERVER構成オプション	デフォルト値	値の範囲	説明
LOG_LEVEL	2	0-4	0=トレース, 1=デバッグ, 2=情報, 3=警告, 4=エラー
CORS_ORIGINS		"Url" または "url1;url2;url3"	CWA H5/ChromeクライアントがAOTログをアップロードできるように、この値を変更します。複数のURLを「;」で区切って指定できます。
MAX_RESERVE_DAYS	7	1~30	ログサーバーは、タイムスタンプフィールドに基づいてログエントリを最大日数保存します。7日前に挿入されたログは削除されます。10分ごとに確認します。
MAX_DISK_USAGE_PERCENTAGE	85	10~90	ログサーバーはデータストレージの使用率を監視します。使用率が90%を超えると、ログサーバーは使用率が90%未満になるまで古いログを毎日削除します。10分ごとに確認します。
LOCAL_DOWN_ONLY	真	true/false	trueの場合、ログサーバーがインストールされているマシンのみが/

LOGSERVER構成オプション	デフォルト値	値の範囲	説明
			Download/*APIにアクセスできます。falseの場合、AuthKeyを持つ他のマシンが/Download/*APIにアクセスできます。
OPENSEARCH_JAVA_OPTS	"-Xms2G -Xmx2G"	2G ~ MaxMem/2	Opensearch メモリ構成。ログをLog Serverに送信するマシンが多い場合は、より多くのメモリを提供してください。例: 0〜999台のマシン: 2GB、1000〜1999台のマシン: 4GB、2000〜9999台のマシン: 6GB

`./StartLogServer.sh`をLinuxで実行して、変更が更新されたかどうかを確認します。

`StartLogServer.bat`をWindowsで実行して、変更が更新されたかどうかを確認します。

シトリックス コネクタ アプライアンス上

以下は、ローカルAPIを介してCitrix Connector Appliance上のログサーバーの詳細設定を構成する手順です。

これはPostman、Curl、またはPowerShellのいずれかで実行できます。以下はPostmanで実行された指示の例です。

1. **認証: JWTの生成**

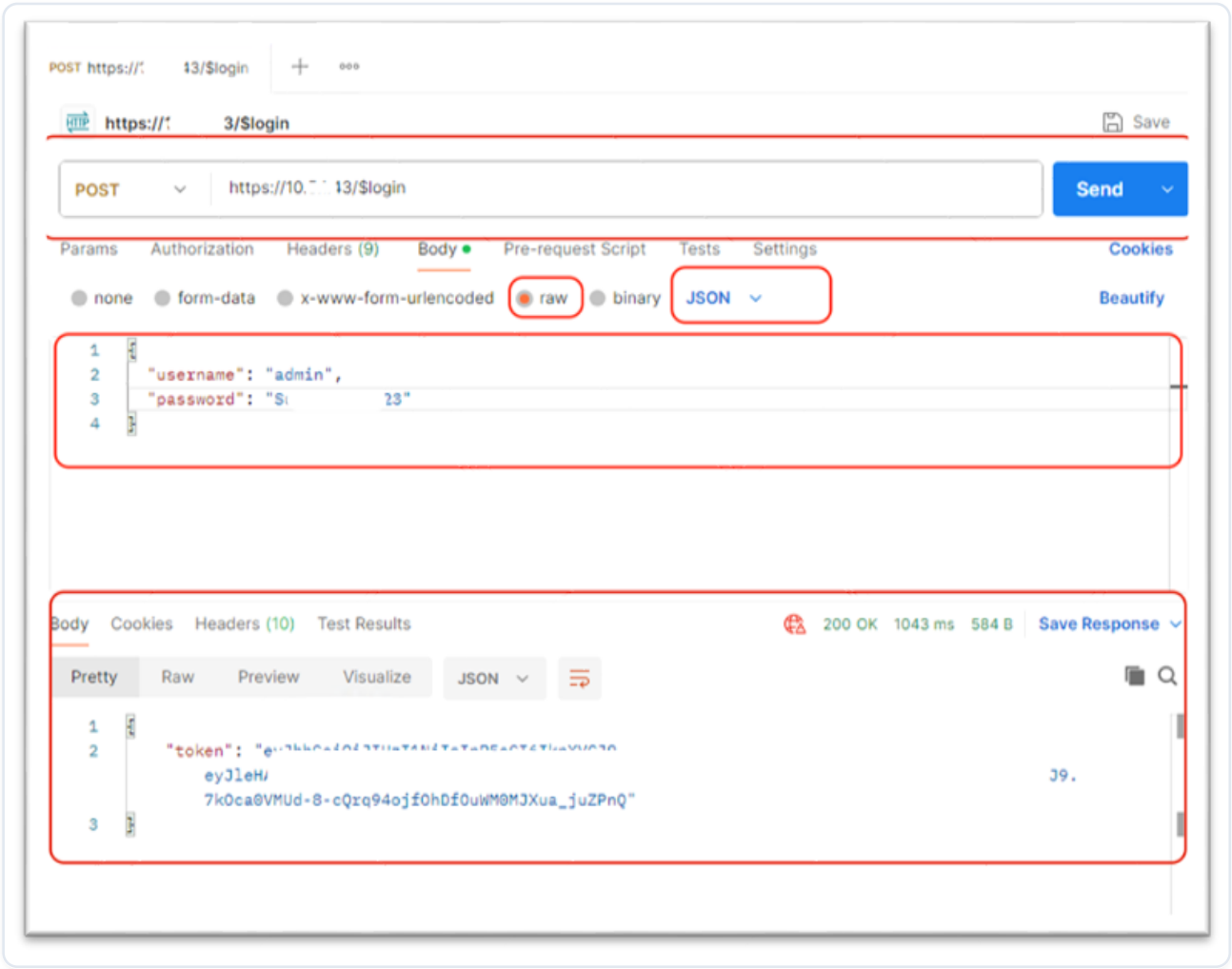
すべてのAPI呼び出しは、JSON Web Token (JWT) を使用して認証する必要があります。まずトークンを生成し、そのトークンを後続のリクエストのヘッダーに含める必要があります。

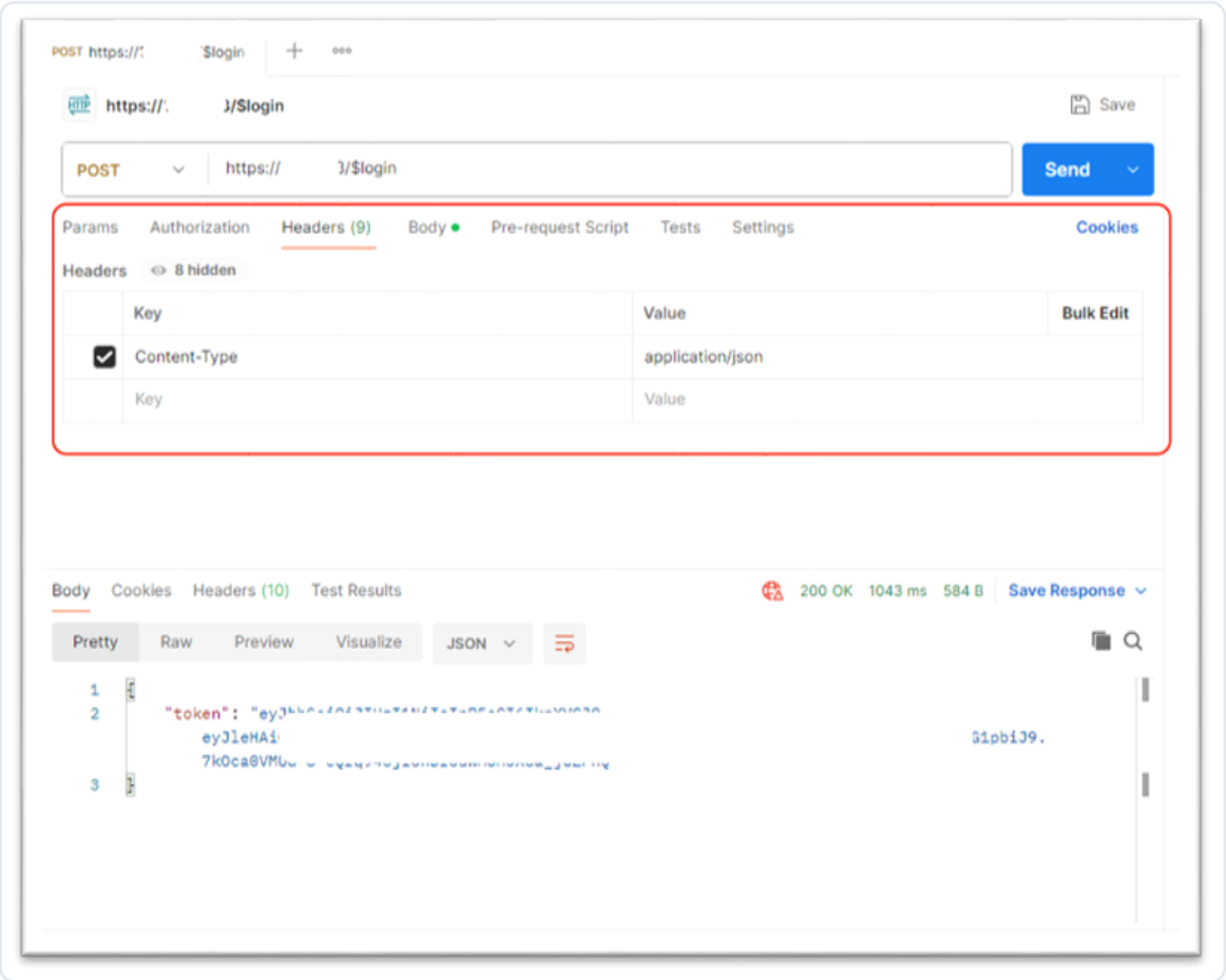
ステップ 1.1: トークンの生成

トークンを生成するには、$loginエンドポイントにPOSTリクエストを実行します。

- エンドポイント: POST https:///$login

- Body: 認証に必要なJSONペイロード (例: ユーザー名とパスワード) を含める必要があります。資格情報が正しい場合、APIはトークンを返します。



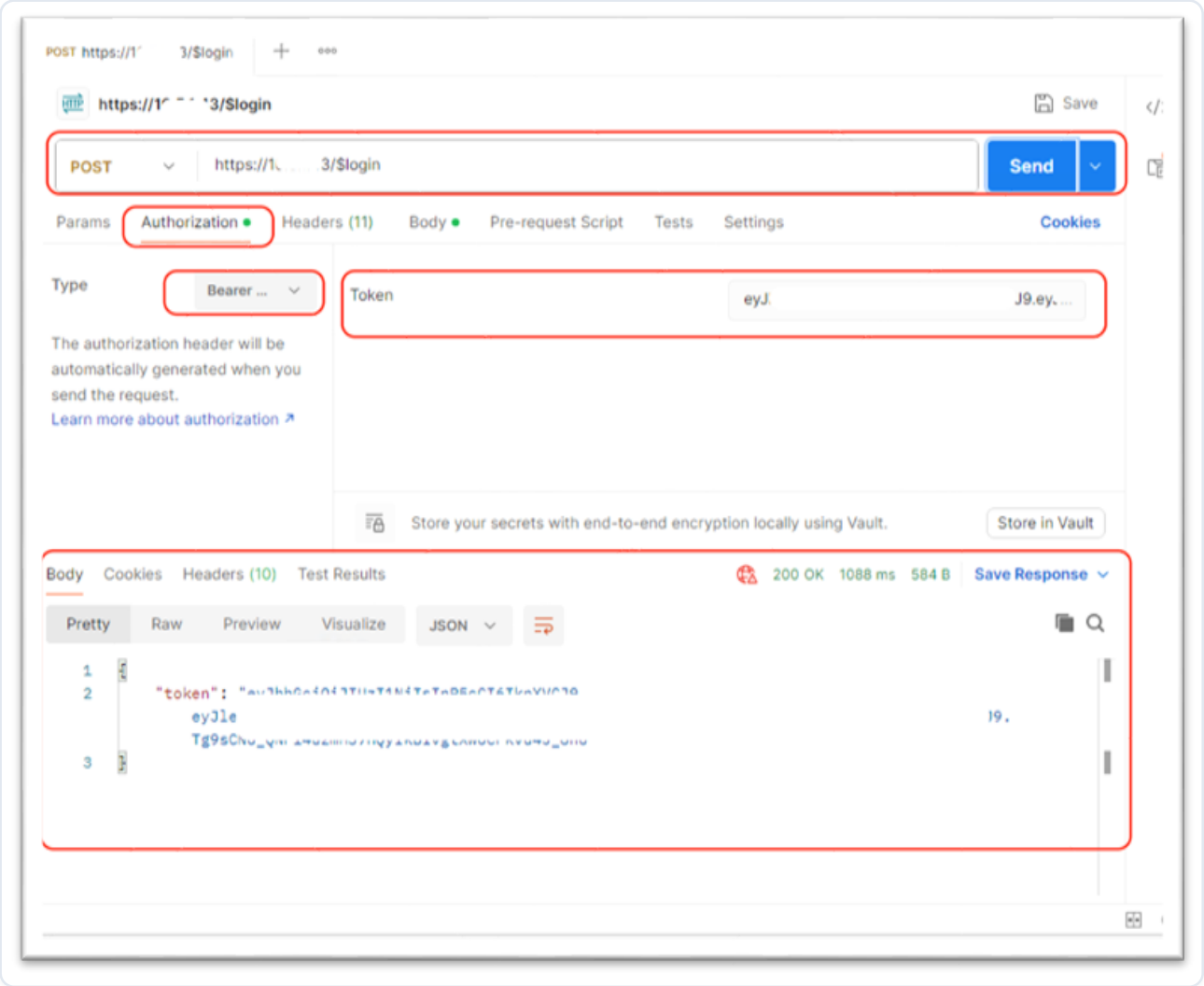


このトークン値をコピーして、次の手順で使用します。

ステップ1.2: API呼び出しを承認する

生成されたトークンを、以降のすべてのAPI呼び出しのAuthorizationヘッダーに含めます。トークンにはBearerをプレフィックスとして付ける必要があります。

認証: **Bearer abCD.efGH.ijKL**



有効なトークンはAPI呼び出しの続行を許可します。無効なトークンまたは期限切れのトークンは、エラーメッセージとともに拒否されます。

1. **詳細設定の追加**

認証後、ログサーバーのようなターゲットコンテナの設定を構成できます。
MAX_RESERVE_DAYSを構成する

このアクションは、ログサーバーのMAX_RESERVE_DAYSを構成します。

- エンドポイント: https:///providers/logserver-provider/environment
- メソッド: PATCH

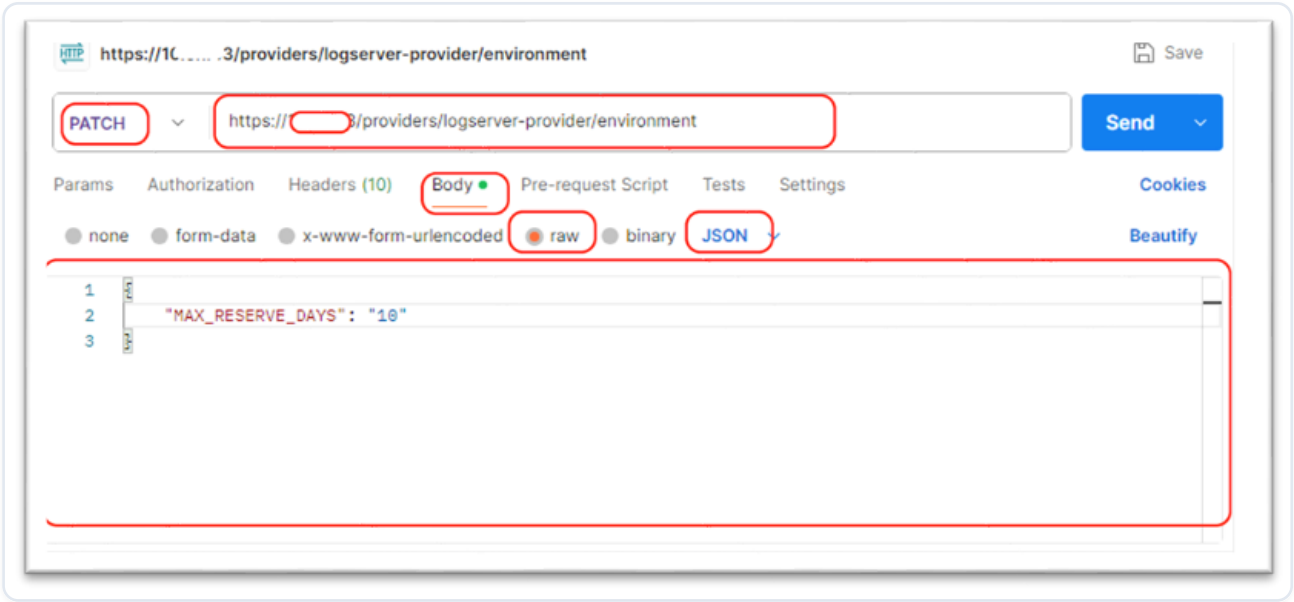
リクエストボディ

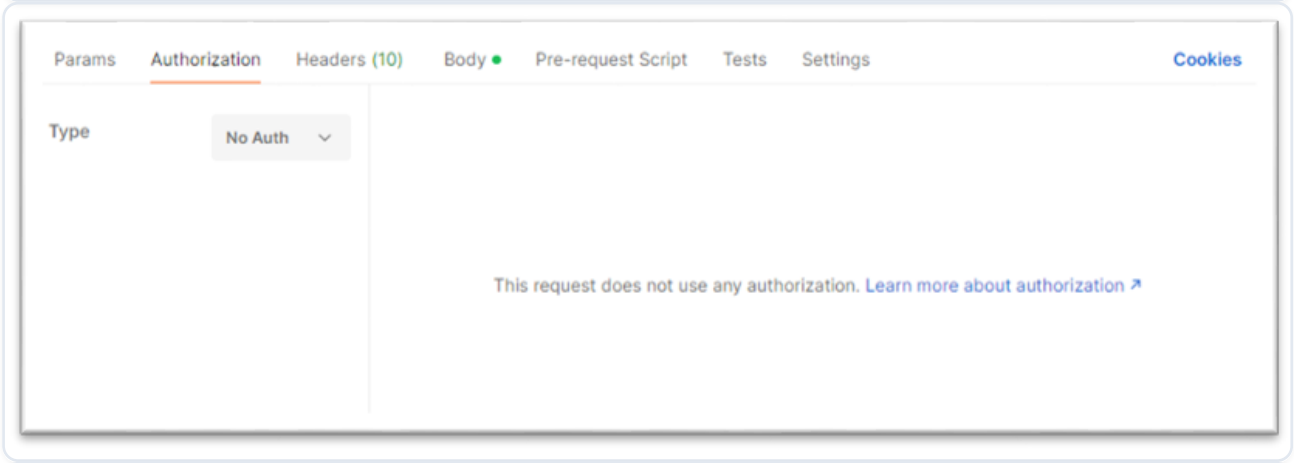
{ "MAX_RESERVE_DAYS": "7" }

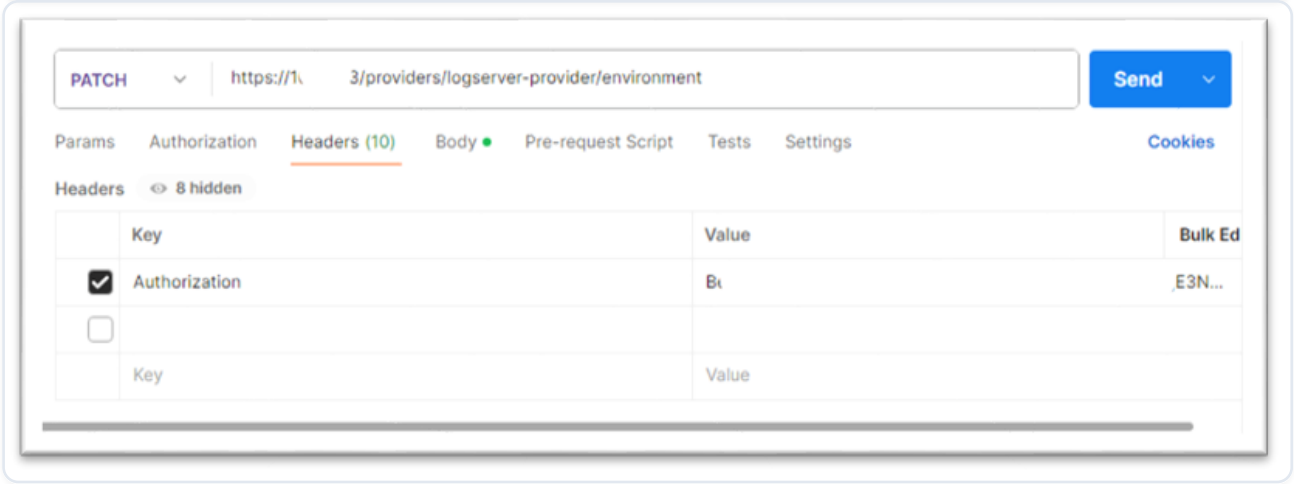
フィールド

- MAX_RESERVE_DAYS (文字列、必須): デフォルト値は7日です。ログサーバーは、TimeStampフィールドに基づいてログエントリを最大日数保存します。7日前に挿入されたログは削除されます。10分ごとにチェックします。

この例では、10日に変更しています。

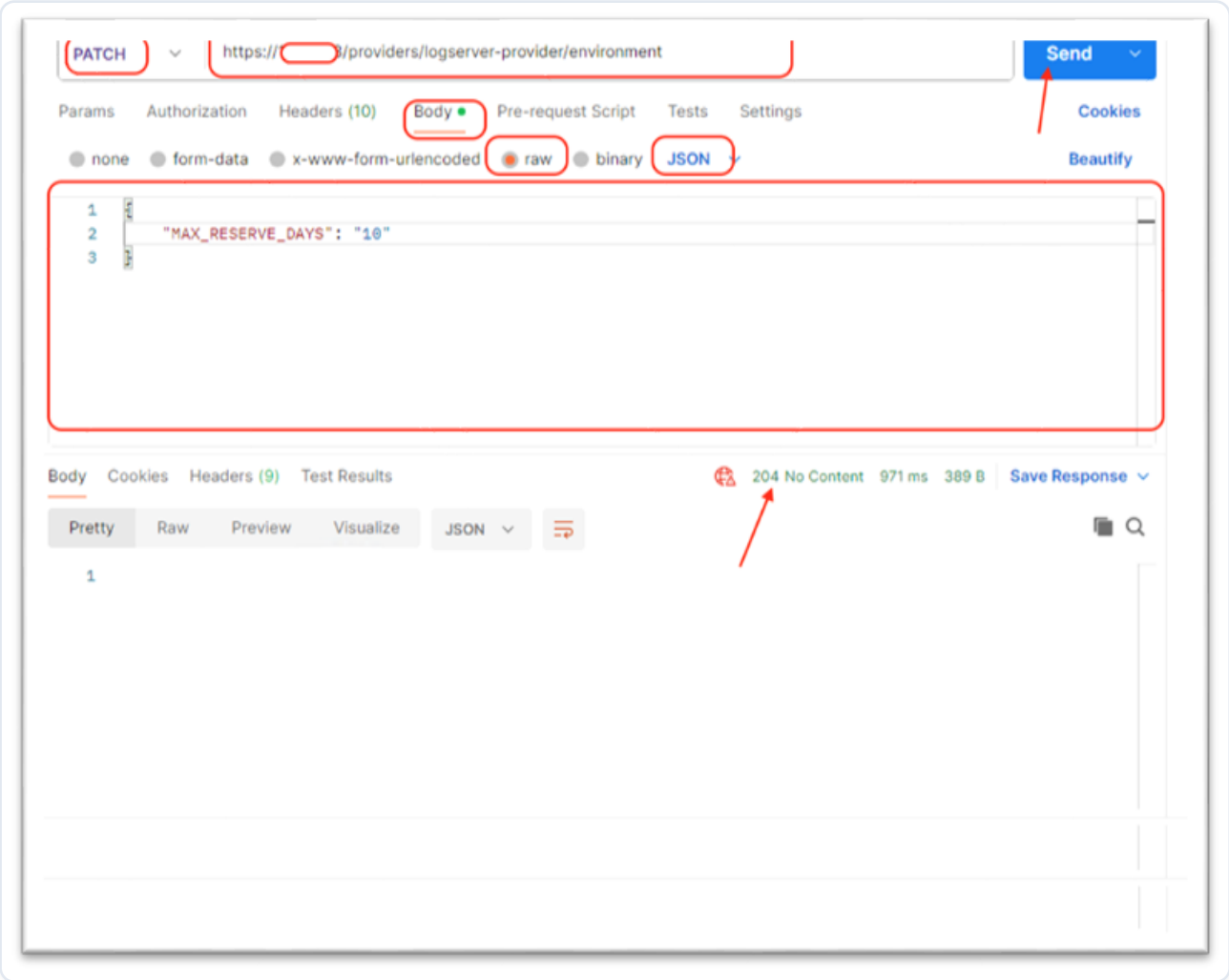




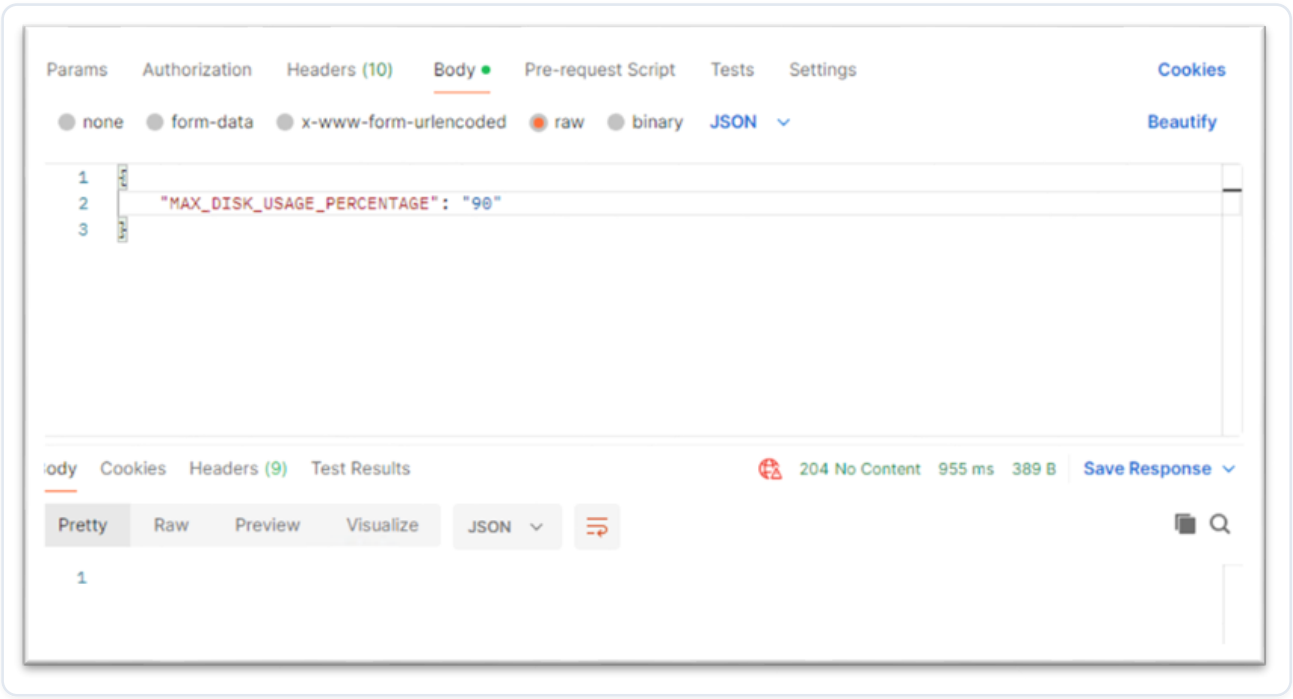


応答

✓ 成功 (204 OK) 設定が正しく構成されていることを示します



同様に、最大ディスク使用率もデフォルトの85から調整できます。ここでは90に変更します。ディスク使用率が90%に達すると、新しいログのためのスペースを確保するために古いログが削除されます。



応答

✓ 成功 (204 OK) 設定が正しく構成されていることを示します

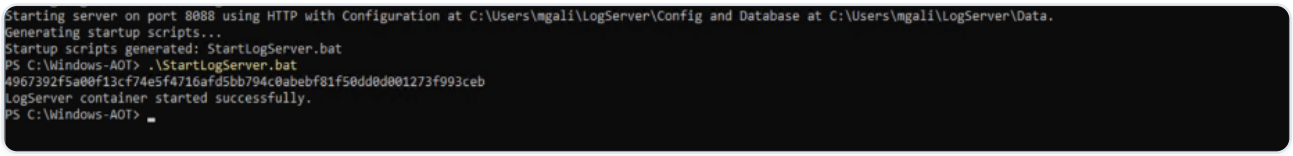
ログサーバーのアップグレード

アップグレードを成功させるには、`docker rm -f logserver`を実行して、既存のログサーバーコンテナを事前に削除することをお勧めします。

- ログサーバーをアップグレードするには、インストールイメージと新しい実行可能ログサーバーファイルをダウンロードし、同じ引数でInstallLogServerコマンドを実行します。
- InstallLogServerは、現在のログサーバーコンテナとイメージを削除するかどうかを尋ねます。ログデータと構成は個別に保存されるため、コンテナとイメージを削除しても安全です。

```
PS C:\Windows-AOT>
PS C:\Windows-AOT> .\InstallLogServer.exe
Checking if Docker is available...
Checking for existing logserver container...
Existing logserver container found.
Select action: [R]ename container or [D]elete container:
```

- 古いコンテナを保持する必要がある場合は、アップグレードプロセスの前にコンテナの名前を変更して停止する必要があります (docker stop logserver)。
- 古いコンテナと新しいコンテナを同じ--dataパスで同時に起動しないでください。そうしないと、ログデータが破損します。
- アップグレード後、新しく生成されたスクリプトを使用してログサーバーを起動する必要があります。



> **注:**
>
> この手順は、Citrixによって更新が自動的に管理されるため、Connector Applianceには必要ありません。

ログサーバーのアンインストール

1. Linux でログサーバーをアンインストールする

ターミナルで以下のコマンドを実行します。

```
docker rm -f logserver

docker rmi logserver



# List containers and images to make sure



docker ps -a

docker images



# Delete Log Server config and data files if not needed any more, change $HOME/LogServer to real installed path if not installed with the default one



rm -r $HOME/LogServer
```

2. Windows でログサーバーをアンインストールする

PowerShell で以下のコマンドを実行します。

```
docker rm -f logserver

docker rmi logserver



# List containers and images to make sure



docker ps -a

docker images



# Delete Log Server config and data files if not needed any more, change
~/LogServer to real installed path if not installed with the default one



Remove-Item -Recurse -Force ~/LogServer
```

CVADコアコンポーネントからのAOTログのアップロード

CVAD 2507 CU1およびCVAD 2511以降、AOTログはすべての該当するコンポーネントから収集されます。サポートされているコンポーネントには、DDC、StoreFront、Citrix Director、Windows VDA、Linux VDA、Mac VDA、License Server、FAS、Cloud Connector、PVS、WEM、Session Recording、Citrix Workspace UI、およびCitrix Gatewayが含まれます。

CVADオンプレミス向けCitrix Web Studioを介した集中型ログ転送構成

Citrix Web Studioは、サイト全体のAlways-on Tracing (AOT) ログ転送を構成するための集中管理された場所を提供します。この設定は、AOTログの送信先を定義し、構成を環境内の関連コンポーネントに自動的に伝播します。

Web Studioでログサーバーを構成すると、次のようになります。

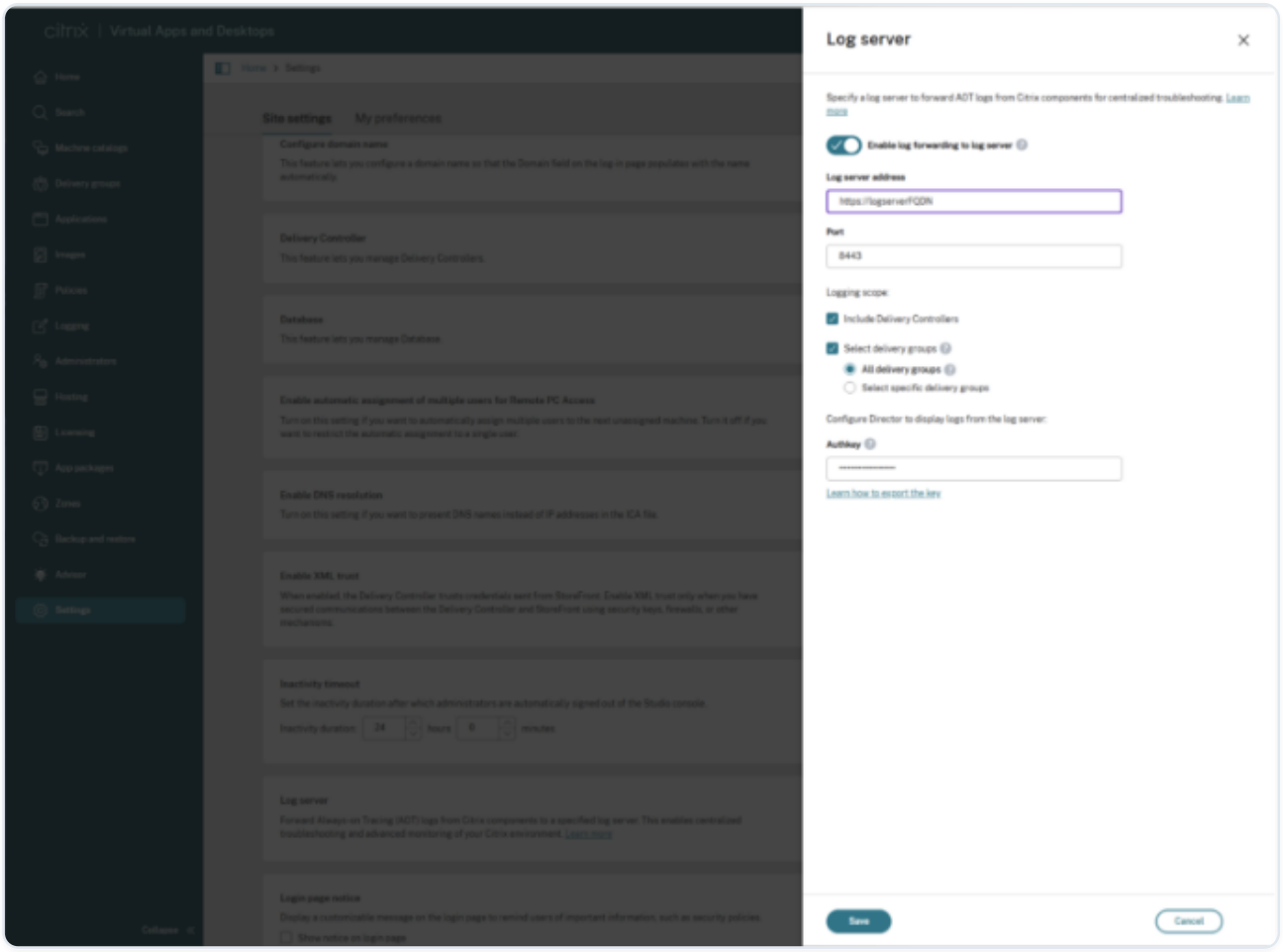
- **サイトデータベース**に構成が書き込まれます。
- **Delivery Controller**は更新された設定を取得し、選択されたデリバリーグループ内のVDAに配布します。
- **VDA**は受信した構成を使用して、AOTログを指定されたログサーバーに転送します。
- AOTログ記録に参加する**StoreFront**は、同じ集中管理メカニズムを通じて必要な詳細情報を受け取ります。
- **Director**は、提供されたAuthKeyとログサーバーの詳細を使用して、監視およびトラブルシューティングのためにAOTログをクエリおよび表示します。

この集中管理アプローチにより、各コンポーネントを個別に構成する必要がなくなります。Web Studioでログサーバーの詳細を一度設定するだけで、Citrixは構成をサイト全体に自動的に伝播します。

以下は、Web Studioで設定されるとログサーバーの詳細を取得するコンポーネントのリストです。

- シトリックス ディレクター/モニター
- シトリックス デリバリー コントローラー
- ウィンドウズ ブイディーエー
- リナックス ブイディーエー
- Mac VDA
- StoreFront
- セッション録画エージェント
- CWA

オンプレミス環境のログサーバー設定を構成するには



1. **Web Studio**にサインインし、左側のペインで**設定**を選択します。
2. 「**ログサーバー**」タイルで、ログサーバーが構成されていない場合は、「**追加**」を選択します。
3. 「**ログサーバー**」ページで、「**ログサーバーへのログ転送を有効にする**」をオンにします。
4. 「**ログサーバーアドレス**」と「**ポート**」を入力します。VDAとDelivery Controllerは、この情報を使用してAOTログを転送します。

> **注:**
>
> a. Citrix Connector Applianceを使用してログサーバーを展開する場合は、ポート443のみが構成されていることを確認してください。
>
> b. Citrix Studioでログサーバーのアドレスとポートを更新すると、最初は機能しますが、設定を再確認し、認証キーを再入力せずにログサーバーの詳細を変更すると、操作が成功したように見えても、保存後に認証キーのプレースホルダーが空になります。これにより、DirectorとMonitorで構成が欠落したり無効になったりします。回避

> 策として、この問題が解決されるまで、ログサーバー設定を変更する際は常に認証キーを再入力して検証してください。

5. ログを転送するコンポーネントを選択します。
    a. **Delivery Controllerを含める**: すべてのDelivery ControllerからAOTログを送信します。
    b. **デリバリーグループを選択**: 選択したデリバリーグループ内のVDAからログを送信します。
    - **すべてのデリバリーグループ**: すべてのVDAからログを送信します。
    - **特定のデリバリーグループを選択**: 含める個々のデリバリーグループを選択します。
6. ログサーバーで生成されたAuthKeyを入力します。Directorは、このキーを使用してログを認証および取得します。
7. 構成を適用するには、「**保存**」を選択します。

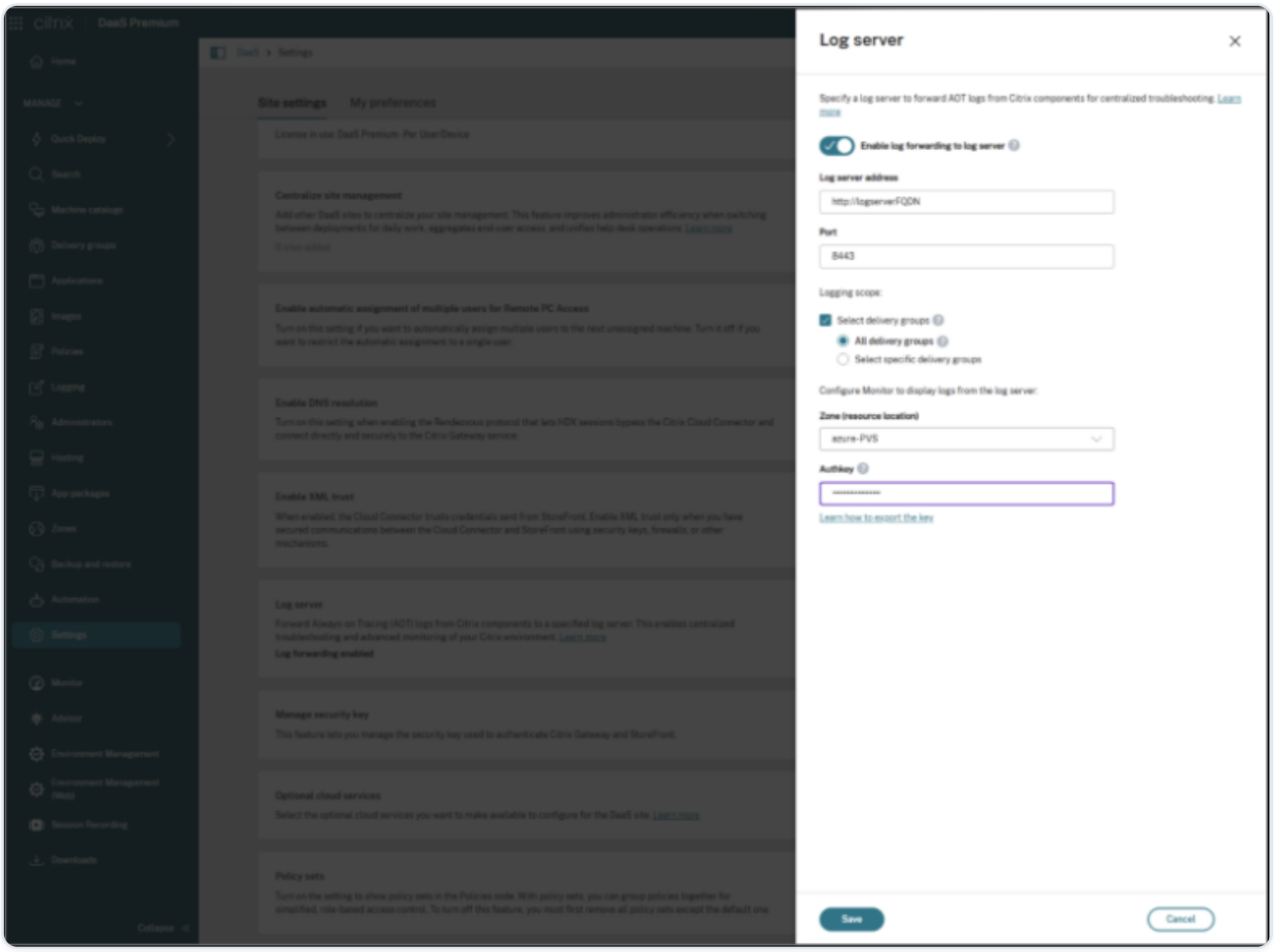
既存の構成を編集するには

ログサーバーを更新するか、ログ記録スコープを変更するには、**設定 > ログサーバー**に移動し、**編集**を選択します。

DaaS設定を介してCitrix DaaS/Cloud環境のログサーバー設定を構成する

Always On Tracing (AOT) は、オンプレミス (CVAD) と Citrix DaaS (クラウド) の両方の展開でサポートされています。ただし、ログ収集の動作は、コンポーネントがホストされている場所によって異なります。

AOTログサーバー (Linux、Windows、またはコネクタアプライアンス上) をインストールして構成した後、クラウド展開用のCitrix DaaS設定でログサーバーへのログ転送を有効にするには、以下を完了します。



DaaS 用 Citrix Web Studio (DaaS 設定) は、クラウド管理サイトの Always-on Tracing (AOT) ログ転送を構成するための一元的な場所を提供します。この構成により、AOT ログの送信先が決定され、どの VDA がログ転送に参加するかが制御されます。Monitor はこれらの設定を使用して、トラブルシューティングのためにログを取得および表示します。

1. DaaS 用 **Web Studio** (DaaS 設定) にサインインし、左ペインで **設定** を選択します。
2. **ログサーバー** タイルで、現在ログサーバーが構成されていない場合は、**追加** を選択します。
3. **ログサーバー** ページで、**ログサーバーアドレス** と **ポート** を入力します。VDA はこの情報を使用して、AOT ログをサーバーに転送します。
4. ログを転送するVDAを定義します。
   a. スコープを制御するには、**デリバリーグループの選択** を選択します。
   b. **すべてのデリバリーグループ** (デフォルト) は、サイト内のすべてのVDAからログを転送します。
   c. 特定のVDAをターゲットにするには、**特定のデリバリーグループの選択** を選択し、含めるデリバリーグループを選択します。

> **注:**

> Citrix Connector Applianceを使用してログサーバーを展開する場合は、ポート443のみが構成されていることを確認してください。

5. ログサーバーが展開されているゾーン (リソースの場所) を選択します。
6. ログサーバーによって生成された認証キーを入力します。モニターはこのキーを使用して、ログを認証し、表示のために取得します。
7. 構成を適用するには、 を選択します。

その他のコンポーネントのログ転送構成

Citrix Cloud展開におけるStoreFrontのAOTログアップロードの構成

Citrix Cloud (ハイブリッド) 展開で、Cloud DDC とともにオンプレミスのStoreFront (Citrix Workspaceの代わりに) が使用されている場合、StoreFrontはCloud ConnectorからAOTログサーバー構成を自動的に受信しません。StoreFrontサーバーで次のPowerShellコマンドを実行して、AOTログサーバーエンドポイントを手動で構成します。

```
# Enable - Run the following command in StoreFront PowerShell



Enable-CitrixAOTUpload -AoTDataStoreEndpoint https://
<FQDNofLogServer>:<server_port> -Role StoreFront



# Disable - Run the following command in StoreFront PowerShell

Disable-CitrixAOTUpload
```

注:

> このコマンドは、Cloud DDCを使用するCitrix Cloud (ハイブリッド) 展開でのみ実行してください。StoreFrontがオンプレミスのDelivery Controllerとペアになっているオンプレミスの CVAD展開では、ログサーバー構成が自動的に同期され、手動構成は不要なため、このコマンドを実行しないでください。

セッションレコーディングサーバーのAOTログアップロードの構成

セッションレコーディングサーバーマシンで次のPowerShellコマンドを実行することにより、セッションレコーディングサーバーがAOTログを中央ログサーバーにアップロードするように構成できます。

```
#Enable - run following command in Session Recording Server PowerShell

Enable-CitrixAOTUpload -AotDataStoreEndpoint <https://
FQDNofServer>:<server port> -Role SessionRecording



#Disable - run following command in Session Recording Server PowerShell

Disable-CitrixAOTUpload
```

FASのAOTログアップロードの構成

FASサーバーで次のPowerShellコマンドを実行することにより、FASがAOTログを中央ログサーバーにアップロードするように構成できます。

```
#Enable - run following command in FAS PowerShell

Enable-CitrixAOTUpload -AotDataStoreEndpoint <https://
FQDNofServer>:<server port> -Role FAS



#Disable - run following command in FAS PowerShell

Disable-CitrixAOTUpload
```

注:

FASインストーラーMSIファイル - FederatedAuthenticationService_x64.msi を使用してインストールまたはアップグレードした場合、常時オンのトレースは利用できません。

FASは常にCVAD MetaInstallerまたはXenDesktopFasSetup.exeまたはFasSetup_xxxx.exeからインストールしてください。

PVSのAOTログアップロードの構成

PVSサーバーで次のPowerShellコマンドを実行することにより、PVSがAOTログを中央ログサーバーにアップロードするように構成できます。

```
#Enable - run following command in PVS PowerShell

Enable-CitrixAOTUpload -AotDataStoreEndpoint <https://
FQDNofServer>:<server port> -Role PVS



#Disable - run following command in PVS PowerShell

Disable-CitrixAOTUpload
```

注:

複数のPVSサーバーがある場合は、それぞれのサーバーでAOTログのアップロードを有効または無効にするコマンドを実行してください。

License Server の AOT ログのアップロード

- Logserver URL は、場所「C:\Program Files (x86)\Citrix\Licensing\WebServicesForLicensing\SimpleLicenseServiceConfig.xml」にあるSLS設定ファイル内で、XML タグ「AotServerURL」を使用して更新する必要があります。

例:

```
<AotServerURL>https://<FQDNofLogServer:443>//ctxlogserver/
UploadCitrixLogStream</AotServerURL>
```

注:

> **License Server でログはいつ生成されますか？**

> License Server AOT ログは、License Server のインストールまたはアップグレード、WSL (Citrix Web Services for Licensing) サービスの再起動、ライセンスアクティベーションの失敗、ダークサイトアクティベーションの失敗、クロック関連のライセンス問題など、特定のイベント中にのみ生成されます。

> これらのイベントのいずれも最近発生していない場合、ログがないことは必ずしも問題を示しているわけではありません。

クイックチェック

1. 最近、対象となるイベント（再起動、アップグレード、アクティベーションの問題など）が発生したかどうかを確認します。
2. Citrix Web Services for Licensing サービスを再起動し、アップロード処理に最大1時間かかります。
3. AOT Log Server URL が正しく構成されていることを確認します。
4. Citrix Web Services for Licensing サービスが実行中であることを確認します。
5. 確認: `C:\Program Files (x86)\Citrix\Licensing\LS\resource\aot` ファイルにデータが含まれている場合、ログはアップロードを待機している可能性があります。

> **注:**

> License Server AOT ロギングはイベント駆動型であり、継続的ではありません。対象となるイベントが発生していない場合にログが表示されないのは正常です。

- License Server は、定期的にログを AOT サーバーに自動的にアップロードします。

Citrix Connector の AOT ログアップロードを構成する

AOT Log Server で Cloud Connector ログを収集するには、次の要件が適用されます。

- Cloud Connector は **バージョン 6.169.0.22492 以降**である必要があります。
- **Cloud DDC 展開**では、ログサーバーの構成詳細は**5月リリース**でレジストリに自動的に同期され、手動での構成は不要です。

- **ハイブリッド展開 (オンプレミス DDC)** では、ログ収集を有効にするために手動でのレジストリ構成が必要です。Cloud Connector マシンに以下のレジストリエントリを作成してください。

パス: `HKLM\Software\Citrix\ConfigSyncService`

エントリ：

- `LogServerEnabled (REG_DWORD) = 1`
- `LogServerEndpoint (REG_SZ) =` https://<logserver-fqdn `:<port>>`

Citrix Workspace アプリの AOT ログアップロードを構成する

Citrix は、Citrix Workspace アプリクライアントが診断ログを集中ログサーバーに自動的にアップロードできるようにします。この機能により、管理者は手動でのログ収集を必要とせずに、クライアント側の診断情報に即座にアクセスできるため、トラブルシューティングの効率が向上します。クライアント側の AOT は自動的にアップロードされ、AOT 機能が CVAD 環境全体で有効になっている場合、およびユーザーがリソースを起動したときにトリガーされます。

システム要件

- Citrix Virtual Apps and Desktops 2511 または CVAD 2507 CU1 以降のバージョン
- Citrix Workspace アプリ 2511 または CWA 2507.1 CU1 以降のバージョン
- 選択した Citrix Workspace アプリ (CWA) の必要なバージョンがインストールされていることを確認してください。詳細については、サポートされているバージョンを参照してください。

前提条件

CITRIX WORKSPACE アプリの WEB 起動

Citrix Workspace アプリの Web 起動 (WebHelper、直接 ICA ファイルダウンロード、Web ブラウザ拡張機能起動方法を含む) の場合、StoreFront は最新のユーザーインターフェイス (UI エクスペリエンス) を使用するように構成する必要があります。 最新の UI エクスペリエンスを有効にする手順については、StoreFront ドキュメントを参照してください。

> **注:**
>
> この前提条件は Web ベースの起動にのみ適用され、ネイティブの Citrix Workspace アプリの起動には必要ありません。

NetScaler の AOT ログアップロードを構成する

- NetScaler CLI に SSH で接続し、「shell」コマンドを実行して NetScaler シェルに入ります。
- /var/analytics_conf ディレクトリに移動します

```
cd /var/analytics_conf
```

- インタラクティブなPythonスクリプト「python {auditlog_schema_generator_for_hec_export.py}」を実行して、スキーマファイルを生成します。スキーマファイルは、HTTPヘッダー（Auth-token、User-Agentなど）とペイロード属性（Role、Machine IPなど）を定義します。

このスクリプトによって生成された出力のスニペット

```
root@Raju-adc2# python auditlog_schema_generator_for_hec_export.py

Schema Builder: Follow the prompts to define your schema.

Include 'Auth-Token'? (Y/n):

Enter the display name (alias) for 'Auth-Token' (press Enter to keep as
is): Authkey

'Auth-Token' can only go in 'header'. Automatically selected.

Include 'HostName'? (Y/n): n

Include 'Content-type'? (Y/n): y

Enter the display name (alias) for 'Content-type' (press Enter to keep as
is):

'Content-type' can only go in 'header'. Automatically selected.

Default value for 'Content-type' is 'application/json'.

Do you want to change it? (y/N):

Include 'User-agent'? (Y/n):

Enter the display name (alias) for 'User-agent' (press Enter to keep as
is):
```

```
'User-agent' can only go in 'header'. Automatically selected.

Default value for 'User-agent' is 'AUDITLOGS/1.0'.

Do you want to change it? (y/N):

Include 'Role'? (Y/n): y

Enter the display name (alias) for 'Role' (press Enter to keep as is):

Where should 'Role' be included? (HEADER/payload): HEADER

Default value for 'Role' is 'GW'.

Do you want to change it? (y/N): y

Enter new default value for 'Role': Gateway
```

生成されたスキーマファイルのサンプル

```
{

     "Header": {

         "Auth-Token": {

             "name": "AuthKey"

         },

         "Content-type": {

             "name": "Content-type",

             "value": "application/json"

         },

         "User-agent": {

             "name": "User-agent",
```

```
            "value": "AUDITLOGS/1.0"
        },
        "Role": {
            "name": "Role",
            "value": "Gateway"
        },
        "MachineIP": {
            "name": "MachineIP"
        },
        "MachineName": {
            "name": "MachineName"
        }
    },
    "Payload": {
        "LogLevel": "Level",
        "MessageContent": "Message",
        "ModuleName": "Module",
        "Time": "TimeStamp"
    },
    "Format": {
        "delimiter": ""
    }
```

```
}
```

- シェルを終了し、NetScaler CLIに戻ります
- Syslogサーバー、ポート、およびスキーマファイル（前の手順で作成したもの）などを定義するsyslogアクションを作成します

```
add audit syslogAction {Action Name} {AOT Server IP/FQDN} -serverPort
{Destination Port} -logLevel {Log Level} -transport HTTP -httpAuthToken
{Authentication Token generated on the AOT sever} -httpEndpointUrl {AOT
Server URL where logs will be sent} -httpSchemaFile {Schema File created
in Previous Step}
```

例:

```
add audit syslogAction act1 10.102.154.196 -serverPort 8088 -logLevel ALL
-transport HTTP -httpAuthToken
fbb94d5b234d86a6cb155e3f808dd33c9698a0d1a866e814573b1909e4c9e56896f433da10
71e3276bd133269fd69203d8f29166816f4d427e709773ceb9d41d531043331f7f76
-httpEndpointUrl "/services/collector/event" -httpSchemaFile sample.json
```

- syslogActionを監査Syslogポリシーにバインドします

```
add audit syslogPolicy {PolicyName} True {Name of the Syslog Action}
```

例:

```
add audit syslogPolicy pol1 true act1
```

AOTログの表示と使用

Director UI経由でのログへのアクセス

ステップ1

`StartLogServer.bat`ファイルを編集する

`StartLogServer.bat`ファイルには、AOTログサーバーコンテナの起動に使用されるすべての構成パラメーターが含まれており、ログアクセスと動作を制御するいくつかの環境変数も含まれています。主要な設定の1つは、**LOCAL_DOWN_ONLY**です。

- **LOCAL_DOWN_ONLY=false**の場合、ログサーバーはリモートログ表示要求を受け入れます。これにより、**Citrix Director/Monitor**がログサーバーに接続し、AOTログをMonitor UIに直接表示できます。
- **LOCAL_DOWN_ONLY=true**の場合、ログサーバーはログアクセスをローカル接続のみに制限します。このモードでは、ログを表示するにはログサーバーマシンに直接接続する必要があり、**Citrix Director Monitorはログを取得または表示できません。**



ステップ 2

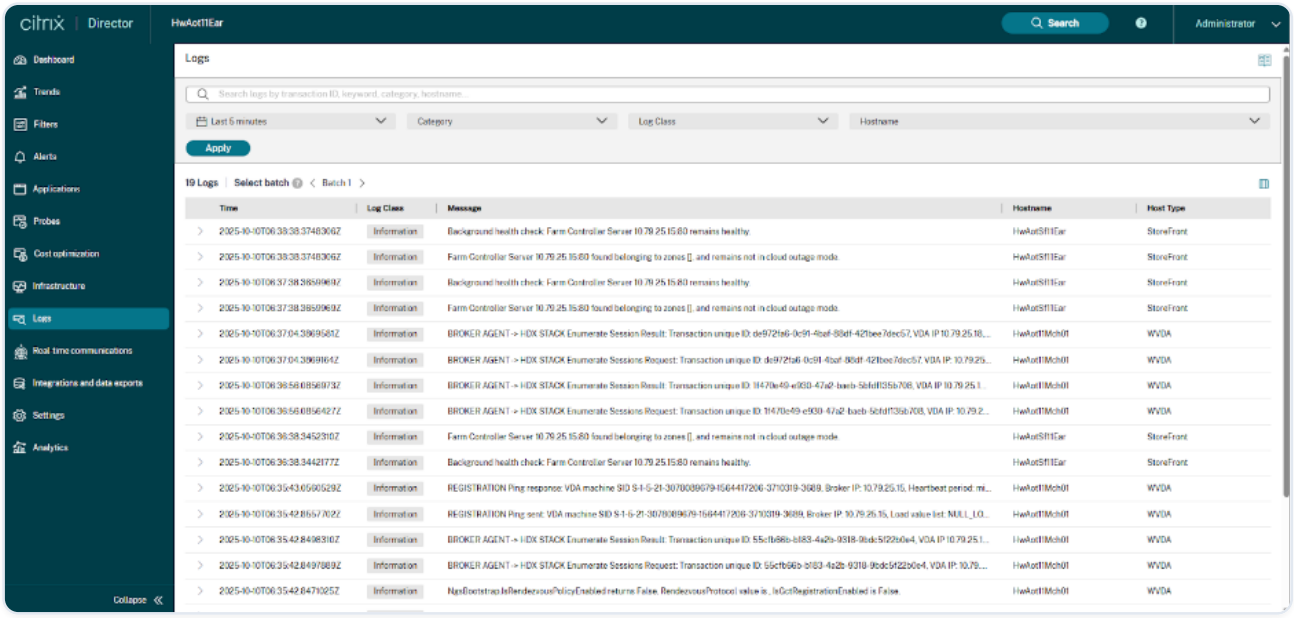
Web Studioには、**Citrix Director**がAOTログサーバーに接続し、Monitorコンソールにログを表示できるようにする専用の設定が用意されています。Web Studioの設定が保存されると、デリバリーコントローラーはサイト構成を更新し、Directorはログサーバーのアドレス、ポート、認証キーを含むログサーバーの詳細を受け取ります。Directorはこれらの設定を使用して、ログサーバーへの安全な接続を確立します。

ステップ3

構成後：

1. **Citrix Director**を開きます。
2. 左側のナビゲーションパネルに新しい**ログ**オプションが表示されます。

3. **ログ**を選択すると、ページが表示されます。これらの設定は以前に完了しているため、**閉じる**をクリックしてスキップしてください。
4. Directorがログサーバーから直接AOTログを取得して表示するようになります。



Directorの**ログ**ページでは、Delivery Controller、VDA、StoreFrontサーバー、およびその他のCitrixコンポーネントからのAOTイベントを統合的に表示できます。ログをリアルタイムで検索、フィルター処理、検査して、問題を迅速にトラブルシューティングできます。

フリーテキスト検索: ログページの上部には、フリーテキスト検索バーがあります。キーワードを入力して結果を絞り込むことができます。フィルターを適用すると、検索結果は即座に更新されます。例を次に示します。

- ユーザー名
- マシン名
- イベントキーワード（例：登録、認証、STA）
- トランザクションID
- エラーメッセージまたは部分文字列

時間フィルター: 時間セレクター（例：過去5分、過去1時間、過去24時間）を使用して、特定の期間内に生成されたログを表示します。これにより、問題が発生した正確な時刻周辺のイベントを迅速に特定できます。

カテゴリフィルター: カテゴリフィールドを使用すると、イベントまたはサブシステムのタイプに基づいてログをフィルター処理できます。これにより、アプリケーション起動、登録、VDA構成、グラフィックス、HDX Direct、ICA接続などに関連するログに焦点を当てることができます。

ログクラスフィルター: ログクラスフィルターは、ログを重大度またはイベントタイプでグループ化します。これにより、トラブルシューティング時にエラーや重要なイベントのみに焦点を当てることができます。一般的なクラスには次のものがあります。

- 情報
- 警告
- エラー
- 失敗

ホスト名フィルター: ホスト名フィルターを使用すると、VDA、Delivery Controller、CWA、StoreFrontサーバーなどの特定のコンピューターを選択できます。これは、展開全体を検索するのではなく、単一のエンドポイントまたはVMのログを詳細に調べたい場合に役立ちます。

この集中アクセスにより、単一のコンソールから迅速なログの取得と分析が可能になり、トラブルシューティングが効率化されます。前提条件と開始方法の詳細については、Director - Logsを参照してください。

ログサーバー経由でのログへのアクセス

以下の内容はAuthKeyの生成です。ログへのアクセスを有効にするには、ユーザーは以下を行う必要があります。

1. `StartLogServer.bat` スクリプトの **LOCAL_DOWN_ONLY=false** を変更する
2. AuthKeyを生成する

ログを安全に保つため、ダウンロードする前に**AuthKey**が必要です。手順は次のとおりです。

1. **AuthKeyを取得する** – 自身のロール名/名前を使用して生成します。
2. **ローカルで実行する** – スクリプトは、Dockerコンテナがインストールされているマシンでのみ実行できます。
3. **Windowsユーザー** – シェルスクリプトの代わりに`GetAuthKey.bat`スクリプトを使用してください。
4. **ログをダウンロードする** – 認証が完了すると、安全にログを取得できます。

AOTログサーバーの認証キーの生成と管理

提供されている.sh (Linux) または .bat (Windows) スクリプトを使用すると、特定のロールまたはユーザーの新しい認証キーを迅速に生成できます。これらのスクリプトは、生成されたキーと関連するロールを返すことでプロセスを簡素化します。

Linuxの場合

```
./GetAuthKey.sh role-name
```

Windowsの場合

```
GetAuthKey.bat role-name
```

AOTログサーバーは、異なるロールまたはユーザーに関連付けられた認証キーを管理するためのコマンドを提供します。これらのコマンドにより、管理者はコンテナから直接認証キーを**追加、一覧表示、検証**し、**削除**できます。利用可能なdocker execコマンドをログサーバーコンテナで直接使用してください。

- **新しい認証キーを追加する**: 指定されたロールまたはユーザーの新しい認証キーを作成します。

`docker exec logserver /app/authkey add <RoleName>`

- **すべての認証キーを一覧表示**: 認証キーが作成されている既存のすべてのロール/ユーザーを表示します。

`docker exec logserver /app/authkey list`

- **認証キーを検証**: 指定された認証キーが有効であるかどうかを確認し、関連付けられているロールを識別します。

`docker exec logserver /app/authkey validate <key>`

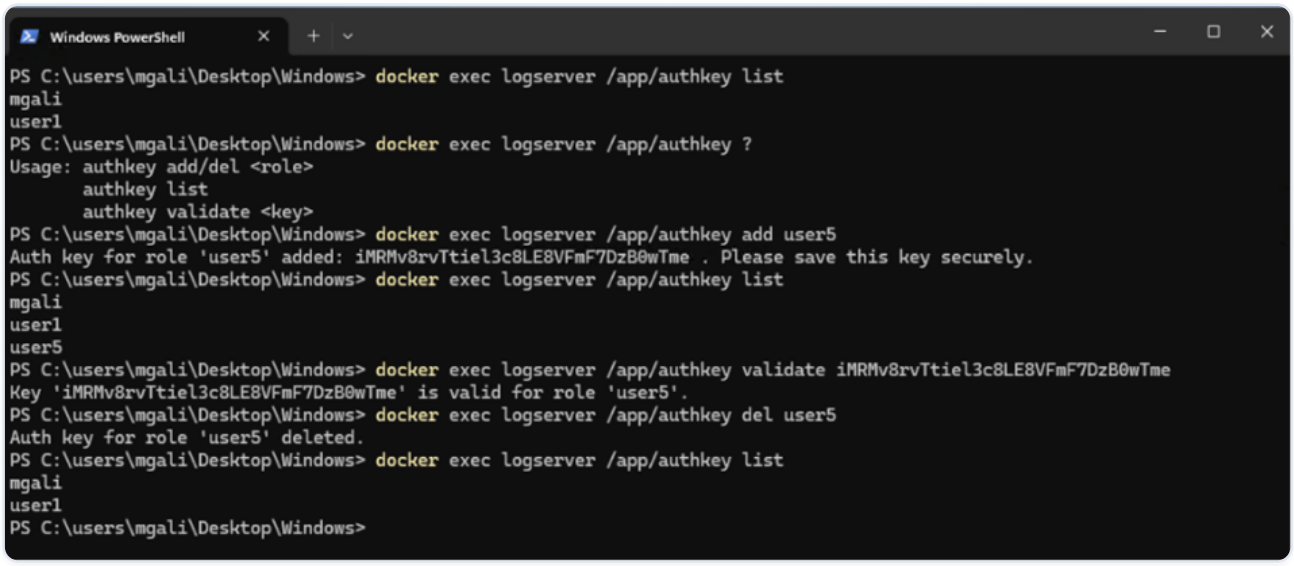
- **認証キーを削除**: 特定のロールに関連付けられている認証キーを削除します。

`docker exec logserver /app/authkey del <RoleName>`

- **コマンドの使用法を表示**: 認証キー管理で利用可能なオプションを表示します。

`docker exec logserver /app/authkey ??`?

次の例は、認証キーを管理する方法を示しています。



AOTログをログサーバーにすでに送信したマシン名を一覧表示

このパラメーターは、GetAuthKey.sh から取得したキーです。

Linuxの場合

```
./ListMachines.sh ebac9b7726cb4be597c92c6769134d25

{"machines":["MachineName"]}
```

空のマシンは、ログがないことを意味します。

Windowsの場合

```
ListMachines.bat ebac9b7726cb4be597c92c6769134d25

{"machines":["MachineName"]}
```

LogServerが「-e LOCAL_DOWN_ONLY=false」で起動する場合のWindows PowerShell:

```
Invoke-WebRequest -Uri "https://logserver_fqdn:8443/ctxlogserver/Download/
ListMachine" -Headers @{ AuthKey = "ebac9b7726cb4be597c92c6769134d25" }
```

logserver_fqdn をログサーバーの実際のFQDNに、8443 をログサーバーの実際のポートに置き換えます。HTTPモードでインストールされている場合は、https を http に置き換えます。

空のマシンは、ログがないことを意味します。

マシン名と時間範囲でログをダウンロードします。

時間はUTC形式です:YYYY-mm-ddTHH:MM:SSZ。

```
#Usage: ./DownloadLogsByTime.sh [AuthKey] [MachineName] [StartTime|YYYY-mm-ddTHH:MM:SSZ] [EndTime|YYYY-mm-ddTHH:MM:SSZ] [OutputFile]

#Example:
```

Linuxの場合

```
./DownloadLogsByTime.sh ebac9b7726cb4be597c92c6769134d25 MachineName 2025-01-01T00:00:00Z 2025-01-02T00:00:00Z logs.csv
```

Windowsの場合

```
DownloadLogsByTime.bat ebac9b7726cb4be597c92c6769134d25 MachineName 2025-01-01T00:00:00Z 2025-01-02T00:00:00Z logs.csv
```

LogServerが「-e LOCAL_DOWN_ONLY=false」で起動する場合のWindows PowerShell:

```
Invoke-WebRequest -Uri "https://logserver_fqdn:8443/ctxlogserver/Download/TimeRange?start=2025-01-01T00:00:00Z&end=2025-01-02T00:00:00Z" -Headers @{ AuthKey = "ebac9b7726cb4be597c92c6769134d25" } -OutFile logs.csv
```

キーワードフィルターでログをダウンロードします。時間はUTC形式です

注:

- キーワードは単一の単語でも、複数の単語の組み合わせでも構いません。
- キーワードはログメッセージ内のどこにでも一致させることができます。
- **トランザクションID**もキーワードとして使用できます。

```
#Usage: ./DownloadLogsByWords.sh [AuthKey] [StartTime|YYYY-mm-ddTHH:MM:SSZ] [EndTime|YYYY-mm-ddTHH:MM:SSZ] [SearchWords] [OutputFile]

#Example:
```

Linuxの場合

```
./DownloadLogsByWords.sh authkey 2025-01-01T00:00:00.000Z
2025-12-31T23:59:59.999Z "session launch" logs.csv
```

Windowsの場合

```
DownloadLogsByWords.bat authkey 2025-01-01T00:00:00.000Z
2025-12-31T23:59:59.999Z "failed vda" logs.csv
```

LogServerが「-e LOCAL_DOWN_ONLY=false」で起動する場合のWindows PowerShell:

```
Invoke-WebRequest -Uri "https://logserver_fqdn:8443/ctxlogserver/Download/
SearchLog?start=2025-01-01T00:00:00Z&end=2025-01-02T00:00:00Z&words=failed
vda" -Headers @{ AuthKey = "ebac9b7726cb4be597c92c6769134d25" } -OutFile
logs.csv
```

単語はスペースで区切られます

展開シナリオ全体でのAOTログの可用性

この表は、AOT (Always On Tracing) のログ収集がさまざまな展開シナリオでどのように行われるかを示しています。使用されるアーキテクチャ（**オンプレミス、Gatewayベース、クラウド、ハイブリッド展開**など）に基づいて、どのコンポーネントがAOTログサーバーにログを送信できるかを強調しています。

ユースケース	展開シナリオ	CWA	STOREFRONT (オンプレミス)	CITRIX WORKSPACE (クラウド)	GATEWAY (オンプレミス)	CITRIX GATEWAY サービス	DDC (オンプレミス)	クラウド DDC	クラウドコネクタ	VDA	FAS	PVS	その他のコンポーネント
1	オンプレミス直接アクセス (StoreFront + オンプレミス DDC)	はい	はい	該当なし	該当なし	該当なし	はい	該当なし	該当なし	はい	はい	はい	はい

ユースケース	展開シナリオ	CWA	STOREFRONT (オンプレミス)	CITRIX WORKSPACE (クラウド)	GATEWAY (オンプレミス)	CITRIX GATEWAY サービス	DDC (オンプレミス)	クラウド DDC	クラウドコネクタ	VDA	FAS	PVS	その他のコンポーネント
2	Gateway 経由のオンプレミス (StoreFront + オンプレミス D	はい	はい	該当なし	はい	該当なし	はい	該当なし	該当なし	はい	はい	はい	はい

ユースケース	展開シナリオ	CWA	STOREFRONT (オンプレミス)	CITRIX WORKSPACE (クラウド)	GATEWAY (オンプレミス)	CITRIX GATEWAY サービス	DDC (オンプレミス)	クラウド DDC	クラウドコネクタ	VDA	FAS	PVS	その他のコンポーネント
	DC + Gateway)												
3	完全なクラウド (Citrix Workspace + クラ	近日公開	該当なし	はい *	該当なし	はい *	該当なし	はい *	はい	はい	はい	はい	はい

ユースケース	展開シナリオ	CWA	STOREFRONT (オンプレミス)	CITRIX WORKSPACE (クラウド)	GATEWAY (オンプレミス)	CITRIX GATEWAY サービス	DDC (オンプレミス)	クラウド DDC	クラウドコネクタ	VDA	FAS	PVS	その他のコンポーネント
	ウド DDC + Citrix Gateway サービス)												
4	ハイブリッドクラウ	近日公開	該当なし	はい *	はい	該当なし	該当なし	はい *	はい	はい	はい	はい	はい

ユースケース	展開シナリオ	CWA	STOREFRONT (オンプレミス)	CITRIX WORKSPACE (クラウド)	GATEWAY (オンプレミス)	CITRIX GATEWAY サービス	DDC (オンプレミス)	クラウド DDC	クラウドコネクタ	VDA	FAS	PVS	その他のコンポーネント
	ド (Citrix Workspace + Cloud DDC + Gateway)												
5	ハイブリ	近日	はい (手	該当	はい	該当	該当	はい *	はい	はい	はい	はい	はい

ユースケース	展開シナリオ	CWA	STOREFRONT (オンプレミス)	CITRIX WORKSPACE (クラウド)	GATEWAY (オンプレミス)	CITRIX GATEWAY サービス	DDC (オンプレミス)	クラウド DDC	クラウドコネクタ	VDA	FAS	PVS	その他のコンポーネント
	ッドクラウド (StoreFront + Cloud DDC + Gateway)	公開	動設定が必要)	なし		なし	なし						

注:

- **はい** → コンポーネントはログをAOTログサーバーにアップロードするのをサポートしています
- **はい*** → ログは利用可能ですが、顧客が管理するAOTログサーバーではなく、Citrixが管理するサービスを通じて処理および保存されます
- **手動設定が必要** → ログサーバーへのログアップロードには手動設定が必要です
- **近日公開 (CWA)** → Citrix Workspaceアプリからの直接ログアップロードにおける現在のギャップを示します (現在開発中)

ログサーバーAPIの一般的な応答コード

この表は、ログサーバーのAPIがクライアント要求の結果を伝えるために使用する標準HTTP応答コードの概要を示しています。これらのコードは、クライアントが要求が成功したか、エラーが発生したか、どのような種類のエラーが発生したかを理解するのに役立ちます。これらの応答コードを理解することは、問題の診断、API呼び出しのデバッグ、およびログサーバーとのスムーズな統合を確保するために不可欠です。

エラーコード	ステータス	説明
200	OK	要求は正常に処理されました。
400	不正なリクエスト。	サーバーは、パラメータの不足、構文の誤り、または必須HTTPヘッダーの欠如により、要求を処理できませんでした。たとえば、要求ヘッダーにMachineNameやRoleのようなフィールドがない場合、この応答がトリガーされます。
401	認証されていません。	クライアントが認証されていないため、要求は拒否されました。これは通常、使用されているIPアドレスまたは認証キー（AuthKey）がログサー

エラーコード	ステータス	説明
		バーへのアクセスを許可されていない場合に発生します。
404	見つかりません。	要求されたAPIパスが存在しません。この応答は、エンドポイントが無効であるか、誤って入力された場合に返されます。
500	内部エラー。	ログサーバーが予期せぬ状態に遭遇し、リクエストの処理を妨げられたことを示します。これは通常、リソース枯渇（例：メモリやディスク容量）などのサーバー側の問題によって引き起こされます。

Always On Tracing の一般的な問題のトラブルシューティング

適用対象: Citrix Virtual Apps and Desktops 2402 CU4、2507 CU1、2511、2603 以降、DaaS

要件: AOT Log Server が展開されていること。AuthKey が Director または Monitor の設定で構成されていること。

Always On Tracing (AOT) は、VDA、Delivery Controller、StoreFront、License Server、Citrix Workspace App など、すべての Citrix コンポーネントでログを継続的にキャプチャします。問題が報告された場合でも、データはすでに存在します。この記事では、Citrix Director または Monitor の **ログ** ノードを使用して問題の原因を特定する方法と、Citrix テクニカルサポートに提出するために Director または Monitor からログをエクスポートする方法について説明します。

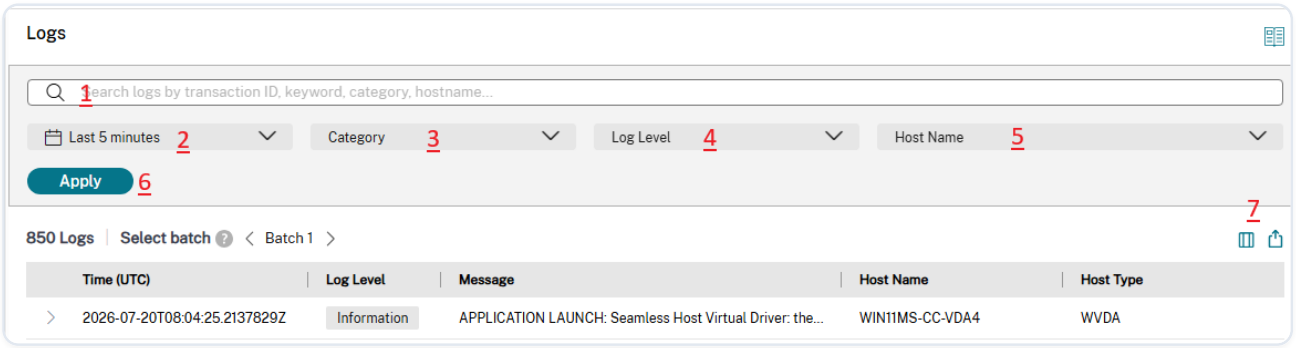
開始する前に — すべてのシナリオでこれを収集してください

- **影響を受けるユーザーまたはマシン** — 特定のユーザー名、VDA ホスト名、またはデリバリーグループ名
- **障害発生時刻** — おおよその時間枠でも、デフォルトの時間フィルターを絞り込むのに役立ちます。報告された障害発生前の期間をカバーするように時間範囲を調整してください。
- **範囲** — 1人のユーザー、1台のマシン、それとも環境全体か？ログを開く前に、範囲だけで正しい障害パターンを特定できることがよくあります。

- **最近の変更** — 関連する期間における CVAD の更新、グループポリシーの変更、電源管理の変更、またはネットワークの変更

Director および Monitor のログノード

ログノードは、**Citrix Director** (オンプレミス CVAD) と **Citrix Monitor** (DaaS) の両方で利用できます。アクセスするには、左側のナビゲーションパネルから **ログ** を選択します。インターフェイスはどちらの環境でも同じです。



1. **検索バー** — キーワード、トランザクション ID、カテゴリ、またはホスト名
2. **時間フィルター** — 障害をカバーする時間枠を選択します
3. **カテゴリフィルター** — イベントタイプでフィルターします
4. **ログレベルフィルター** — 重大度でフィルター
5. **ホスト名フィルター** — 1つ以上のマシンを選択
6. **適用ボタン** — すべてのアクティブなフィルター選択を適用します
7. **エクスポートアイコン** — ログをダウンロードしてCitrixテクニカルサポートに提出

フィルターバー

フィルターバーには4つのフィルターと、独立した**適用**ボタンがあります。まずフィルターを設定し、次に**適用**をクリックしてログビューを更新します。現在のログ数はフィルターバーの下に表示されます（例：*バッチ1に850個のログ*）。バッチナビゲーション矢印を使用して、大規模な結果セットをページ移動します。

フィルター	機能	オプション
時間	ログ取得の時間枠を設定します。報告された障害の前に開始する時間枠に設定して、障害に至ったイベントをキャプチャします。	過去5分 · 過去1時間 · 過去24時間 · 過去48時間 · 過去7日間 · カスタム (UTC) *(CVAD 2603以降のクラウドリリースのみ)*

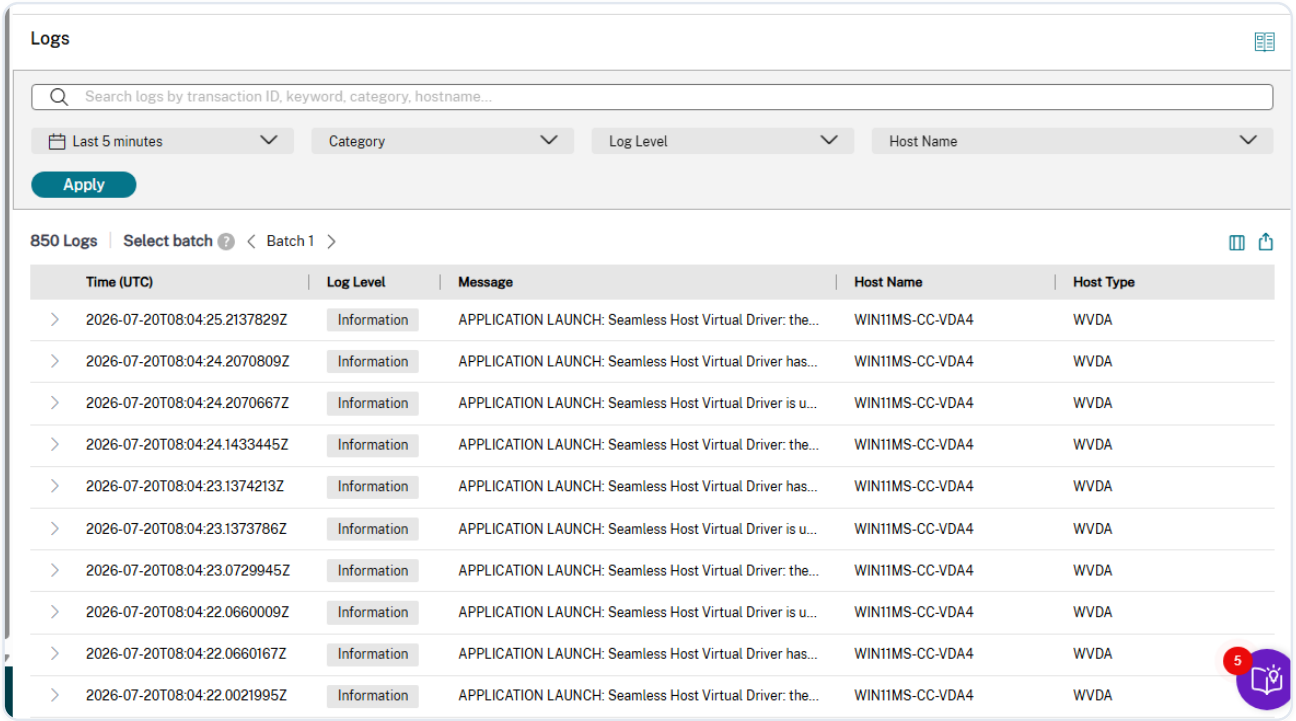
フィルター	機能	オプション
カテゴリ	イベントタイプでフィルターします。各カテゴリは、Citrixコンポーネントのライフサイクルの特定の部分に対応しています。名前でカテゴリをすばやく見つけるためのカテゴリ検索フィールドが含まれています。	アプリケーション起動 · クリップボード · CWA-PostLaunch · CWA-PreLaunch · データベース · デバイス · など
ログレベル	重大度でフィルターします。1つ以上選択します。選択がアクティブな場合、ボタンのラベルには選択された数が表示されます（例：*1つのログレベルが選択済み*）。	情報 · 警告 · エラー · 重大
ホスト名	1つまたは複数の特定のコンピューターにフィルターを適用します。検索ホストフィールドと、現在ログサーバーにログを送信しているすべてのコンピューターのチェックボックスリストが含まれます。アクティブな場合、*N ホスト名が選択されました*と表示されます。	ログサーバーに登録されているすべてのコンピューター

ログレベル	使用するタイミング
情報	標準コンポーネントイベント — セッション開始、VDA登録、ライセンスチェックアウト。完全なライフサイクルシーケンスを確認するために使用します。
警告	問題を示す可能性のある重要ではない問題 — セッション切断、アイドルタイムアウト、ハートビート警告。**切断シナリオの場合はここから開始します。**

ログレベル	使用するタイミング
エラー	調査が必要な障害 — 起動エラー、登録失敗、ライセンス枯渇。**ほとんどのシナリオの場合はここから開始します。**
重大	サービスに影響を与える重大な障害 — 通常、コンポーネントのクラッシュまたは回復不能な状態

ログテーブル — 列

ログテーブルには、各エントリに対してデフォルトで5つの列が表示されます。列ボタンをクリックすると、新しい列を追加できます。いずれかの行にある > 展開矢印をクリックすると、完全なログメッセージと追加フィールドが表示されます。



アプリケーション起動カテゴリがアクティブなログテーブル。ログ数とバッチナビゲーションはテーブルの上に表示されます。> 矢印で任意の行を展開して、完全なメッセージを読みます。

列	表示される内容
時刻 (UTC)	イベントのUTCタイムスタンプ。ミリ秒単位の精度。発生順にイベントのシーケンスを読み取るには、昇順でソートします。

列	表示される内容
ログレベル	重大度バッジ: 情報、警告、エラー、または致命的
メッセージ	コンポーネントからのログメッセージ。テーブルでは切り詰められています。行の **>** 展開矢印をクリックして、完全なメッセージを読み取ります。完全なメッセージは主要な診断テキストです。
ホスト名	ログエントリを生成したマシン
ホストの種類	コンポーネントの種類: DDC、StoreFront、WVDA (Windows VDA)、CWAWindows、およびログサーバーに登録されているものに応じてその他の種類。

Citrixテクニカルサポート向けログのエクスポート

エクスポートアイコン (上記の注釈付きスクリーンショットの **7**) は、ログセクションの右上隅に表示されます。これを使用して、現在フィルターされているログビューをファイルとしてダウンロードします。エクスポートする前に:

> **バージョン提供状況:**

> エクスポートアイコンは、Cloud 129 (2026年4月〜5月) リリース以降のDaaSで利用でき、CVAD 2603以降のCitrix Virtual Apps and Desktopsでも利用できます。それ以前のバージョンではこのオプションは利用できません。

> **AuthKeyが必要です:**

> 「ログ」ノードは、AuthKeyがDirectorまたはMonitorの設定で構成されている場合にのみデータを表示します。AuthKeyはログサーバーのセットアップ中に生成されます。AuthKeyがない場合、「ログ」ノードにはエントリが表示されません。

シナリオ1：セッション起動の失敗

ユーザーが公開されたデスクトップまたはアプリケーションをクリックすると、起動エラーが発生します。セッションは開かれません。エラーはCitrix Workspaceアプリの画面に表示されるか、進行状況バーが停止してタイムアウトし、セッションが接続されない場合があります。

「ログ」ノードで、**カテゴリ**を**アプリケーション起動**に、**ログレベル**を**エラー**に設定し、**時間**を障害発生期間をカバーするように調整します。**適用**をクリックします。**時間 (UTC)** で昇順に並べ替え、**メッセージ**と**ホストタイプ**の列を一緒に読み取ります。これらは、起動パスのどのコンポーネントが失敗し、それが何を報告したかを示します。

> **参照のみ：**

> 以下のログメッセージは例示的なものです。実際の環境でのメッセージは、同じ形式と列構造に従いますが、正確な文言は異なる場合があります。

例：デリバリーグループで利用可能なVDAがない

DDCは起動要求を受信しましたが、デスクトップを割り当てることができませんでした。デリバリーグループ内のすべてのVDAが登録解除されているか、セッション容量に達していました。

時間 (UTC)	ログレベル	メッセージ	ホスト名	ホストタイプ
2026-07-20T09:14:22.1034Z	情報	APPLICATION LAUNCH: ユーザー DOMAIN\jsmith がデリバリーグループ 'Windows 11 VDAs' からデスクトップを要求しました	DDC-01	DDC
2026-07-20T09:14:22.3841Z	エラー	APPLICATION LAUNCH: 適切なデスクトップが見つかりませんでした — デリバリーグループ 'Windows 11	DDC-01	DDC

時間 (UTC)	ログレベル	メッセージ	ホスト名	ホストタイプ
		VDAs' 内のすべての VDA が未登録であるか、セッション容量に達しています		
2026-07-20T09:14:22.4102Z	エラー	APPLICATION LAUNCH: ユーザー DOMAIN\jsmith の起動に失敗しました — 利用可能なリソースがありません	STF-01	StoreFront

DDC からのエラーは、ブローカーが利用可能な VDA を見つけられなかったことを示しています。Web Studio → で VDA の登録を確認してください。VDA 登録のトラブルシューティングについては、シナリオ 2: VDA 登録の失敗 を参照してください。

例: VDA は割り当てられたが、セッションの初期化に失敗した

DDC は VDA を割り当てましたが、VDA はセッションを開始できませんでした。一般的な原因としては、FSLogix またはローミングプロファイルコンテナの障害、グループポリシー処理エラー、または VDA リソースの枯渇が挙げられます。

時刻 (UTC)	ログレベル	メッセージ	ホスト名	ホストの種類
2026-07-20T09:22:11.0234Z	情報	アプリケーション起動: ユーザー DOMAIN\jsmith の VDA WIN11MS-CC-VDA4 が選択されました	DDC-01	DDC
2026-07-20T09:22:11.8820Z	エラー	アプリケーション起動: ユーザー DOMAIN\jsmith のセッション初	WIN11MS-CC-VDA4	WVDA

時刻 (UTC)	ログレベル	メッセージ	ホスト名	ホストの種類
		期化に失敗しました — FSLogix プロファイルコンテナを `\\fileserver\profiles\jsmith.vhdx` にマウントできませんでした		
2026-07-20T09:22:12.0011Z	エラー	アプリケーション起動: 起動要求が失敗しました — VDA WIN11MS-CC-VDA4 がユーザー DOMAIN\jsmith のセッション準備エラーを報告しました	DDC-01	DDC

ホストタイプWVDAからのエラーは、VDAを障害点として特定し、メッセージには正確な原因が表示されます。その行の**>**展開矢印をクリックして、完全なプロファイルコンテナパスとエラーコードを含む完全なメッセージを読みます。

例: CWA起動中の仮想チャネルエラー

セッションはVDA側で作成されましたが、CWAクライアントはICA仮想チャネル接続を確立できませんでした。**ホスト名**をCWAマシンでフィルタリングして、クライアント側のエラーを確認します。

時刻 (UTC)	ログレベル	メッセージ	ホスト名	ホストタイプ
2026-07-20T09:31:04.5521Z	情報	アプリケーション起動: シームレスホスト仮想ドライバーが正	WIN11MS-CC-VDA4	WVDA

時刻 (UTC)	ログレベル	メッセージ	ホスト名	ホストタイプ
		常に初期化されました		
2026-07-20T09:31:05.1204Z	エラー	CWA-POSTLAUNCH::VIRTUAL CHANNEL: 仮想ドライバーのロードに失敗しました — チャネルネゴシエーションがタイムアウトしました。ポート1494および2598のファイアウォールルールを確認してください。	ウィン22-CC-01	CWA (ウィンドウズ版)

ホストタイプCWAWindowsでCWA-POSTLAUNCHエラーが発生した場合、VDAは準備ができていたものの、クライアントとVDA間のICAデータパスがブロックされていたことを意味します。クライアントマシンからVDAへのポート1494および2598が開いていることを確認してください。

シナリオ2：VDA登録の失敗

VDAはDirectorまたはWeb Studio → Search Machinesで**未登録**と表示されます。ユーザーには「現在、利用可能なデスクトップはありません。」と表示されます。公開されたデスクトップはStoreFrontまたはCitrix Workspaceでグレー表示されます。

ログノードで、**カテゴリ**を**VDA登録**に、**ログレベル**を**エラー**に設定し、**ホスト名**を影響を受けるVDAとDDCの両方に設定します。**適用**をクリックします。登録ハンドシェイクの両側（同じタイムスタンプのVDA行とDDC行）を一緒に読むことで、障害がどこで発生したかを正確に示します。

> **参照のみ：**

> 以下のログメッセージは例示です。お使いの環境での実際のメッセージは、同じ形式と列構造に従いますが、正確な文言は異なる場合があります。

例：VDAがDelivery Controllerに到達できない

VDAは登録を試みていますが、DDCはリクエストを受信しません。VDA側のエラーのみが表示され、同じタイムスタンプで一致するDDC行はありません。

時刻 (UTC)	ログレベル	メッセージ	ホスト名	ホストタイプ
2026-07-20T08:30:11.2341Z	エラー	登録: ポート443でDelivery Controller DDC-01.domain.comに接続できませんでした — 接続がタイムアウトしました	WIN11MS-CC-VDA4	WVDA
2026-07-20T08:30:41.2341Z	エラー	登録: ポート443でDelivery Controller DDC-01.domain.comに接続できませんでした — 接続がタイムアウトしました	WIN11MS-CC-VDA4	WVDA
2026-07-20T08:31:11.2341Z	エラー	登録: ポート443でDelivery Controller DDC-01.domain.comに接続できませんでした — 接続がタイムアウトしました	WIN11MS-CC-VDA4	WVDA

同じエラーが一定の間隔で繰り返されるのは再試行ループです。VDAは稼働していますがブロックされています。VDAからDDCへのポート80と443が開いていることを確認し、VDAの `ListOfDDCs` レジストリキーで古いまたは誤ったDDCアドレスをチェックしてください。

例: DDCが登録要求を拒否する

VDAはDDCに到達しましたが、DDCはVDAの登録を拒否しました。VDAとDDCの両方の行が表示されます。拒否理由についてはDDCメッセージを読んでください。

時刻 (UTC)	ログレベル	メッセージ	ホスト名	ホストタイプ
2026-07-20T08:30:11.2341Z	情報	REGISTRATION: VDA WIN11MS-CC-VDA4 が DDC-01.domain.com への登録を試行しています	WIN11MS-CC-VDA4	WVDA
2026-07-20T08:30:11.8820Z	エラー	REGISTRATION: 登録が拒否されました — マシンアカウント WIN11MS-CC-VDA4$ が無効になっているか、Active Directory に見つかりません	DDC-01	DDC

エラー行はホストタイプDDCから来ています。DDCが障害点であり、VDAではありません。DDC行の**>**展開矢印をクリックして、拒否理由の全文を読んでください。一般的な理由としては、Active Directoryでのマシンアカウントの無効化、VDA/DDCのバージョン不一致、ライセンスプールの枯渇などがあります。

例：VDAが登録された後、すぐに登録解除される

登録は成功しますが、DDCが数秒以内に登録解除を開始します。これがループで繰り返されます。電源管理ドレインポリシーにより、VDAがセッションを受け入れる前にシャットダウンされています。

時刻 (UTC)	ログレベル	メッセージ	ホスト名	ホストタイプ
2026-07-20T09:01:33.1240Z	情報	登録：VDA WIN11MS-CC-VDA4が	WIN11MS-CC-VDA4	WVDA

時刻 (UTC)	ログレベル	メッセージ	ホスト名	ホストタイプ
		DDC-01.domain.comに正常に登録されました		
2026-07-20T09:01:47.4421Z	エラー	電源管理：PowerManagementDrainが開始されました — デリバリーグループの電源ポリシーにより、マシンはシャットダウンがスケジュールされています	WIN11MS-CC-VDA4	WVDA
2026-07-20T09:01:47.6830Z	エラー	REGISTRATION: VDA WIN11MS-CC-VDA4 の登録が解除されました — 理由: 電源管理によるドレイン	DDC-01	DDC

登録と登録解除の間の14秒のギャップが原因です。Web Studio → デリバリーグループ → 電源管理 を確認し、営業時間中に適用されているドレインまたはシャットダウンのスケジュールがないか確認してください。

> **注:**
>
> この記事のシナリオは、Citrix Director または Monitor でログを検索および調査する方法の例です。同じ方法論は、セッション障害、認証エラー、接続の問題、VDA の不安定性、またはその他のコンポーネントレベルの問題など、遭遇するあらゆる Citrix 関連の問題に適用されます。適切な **カテゴリ**、**ログレベル**、および **ホスト名** フィルターを設定し、**時間 (UTC)** 順にログシーケンスを読み取り、個々の行を展開して完全な **メッセージ** を読み取ります。最初にエラーをログに記録したコンポーネントとメッセージの内容が、シナリオに関係なく根本原因を示します。

ヒント — Citrix Aidrien アクセス権を持つ DaaS のお客様へ: AOT ログからエラーメッセージをコピーし、Citrix Aidrien に直接貼り付けます。Aidrien がエラーを説明し、推奨されるトラブルシューティング手順を提供します。これだけであらゆる問題が解決するわけではありませんが、根本原因を絞り込み、多くの場合、Citrix テクニカルサポートに連絡する前に解決策へと導きます。

Citrix テクニカルサポートへのエスカレーション

セルフサービスによる調査で問題が解決しない場合は、サポートチケットを開く際に以下を含めてください。

- **障害発生期間をカバーするエクスポートされたログファイル** — 上記のオプション 7 で説明されているエクスポートアイコンを使用します。状況に応じて、2つの方法でエクスポートできます。
  - **ターゲットを絞ったエクスポート** — 時間、カテゴリ、ホスト名のフィルターを適用してからエクスポートします。これにより、サポートは障害に絞り込んだログセットを得ることができます。
  - **広範囲なエクスポート** — 時間フィルターのみを適用し、他のフィルターなしでエクスポートします。これにより、サポートは障害発生期間のログ全体像を得ることができ、範囲が不明確な場合に役立ちます。

  ファイルがダウンロードされると、ファイル名には **AOT** がプレフィックスとして付加されます。このプレフィックスを削除したり、名前を変更したりしないでください。その後のファイル名の部分は編集できますが、常に先頭に **AOT** を保持してください。
- 上記のセクションで特定された障害パターン
- CVADバージョン、コンポーネントバージョン（VDA、DDC、StoreFront）、およびログサーバーバージョン
- 失敗したイベントのトランザクションIDまたはセッションID — プレースホルダー「*"Search logs by transaction ID, keyword, category, hostname"*」を使用してログノードの検索バーで検索可能

AOTはログを継続的にキャプチャし、すべてのエントリにホスト名、ホストタイプ、タイムスタンプが含まれているため、Citrixテクニカルサポートは、問題の再現や新しいトレースの収集を依頼することなく、すぐに分析を開始できます。

よくある質問

1. **MAX_RESERVE_DAYSのような、実行中のログサーバー設定を確認するにはどうすればよいですか？**

   以下のいずれかのコマンドを使用して、コンテナ環境の値を確認できます。

   `docker inspect logserver |findstr MAX_RESERVE_DAYS` または、コンテナ環境を確認する： `docker exec -it logserver env |grep MAX_RESERVE_DAYS`

   何も返されない場合、ログサーバーはデフォルト値を使用していることを意味します。MAX_RESERVE_DAYS=7

2. **Windowsにログサーバーコンテナイメージをインストールする際、Docker Desktopライセンスを購入する必要がありますか？**

   はい。有効なDocker Desktopライセンスが必要です。

3. **ログサーバーのインストールには新しいサーバーを使用すべきですか？**

   はい。パフォーマンスと分離を確保するため、ログサーバーのインストールには専用サーバーを使用することをお勧めします。

4. **単一のAOTログサーバーの持続的な取り込み容量はどのくらいですか？最大および安全な1秒あたりのイベント数（EPS）の制限は何ですか？**

   単一のAOTログサーバーは、**1秒あたり10,000イベント（EPS）の持続的な取り込み容量をサポートします。この値は、継続的な取り込みにおける最大値**と**安全な運用しきい値**の両方を表します。

5. **単一のAOTログサーバーはいくつのコンポーネントを処理できますか？最大制限はありますか？**

   単一のログサーバーは最大128,000のコンポーネントに接続できますが、1秒あたり約10,000ログしか処理できません。したがって、マシンの数が問題になることはめったにありません。実際のサイジング要因は、ピークアクティビティ中にユーザーが生成するログの数です。

6. **AOTログサーバーのバースト耐性とは何ですか？損失やバックログの超過なしに、どれくらいの突然のログスパイクを処理できますか？**

   AOTログサーバーは、ログを失うことなく、**通常のイベントレートの2倍**までの短期間のバーストを処理できます。ログ量がこれを超えて急増した場合（例えば5倍）、システムはイベントを確実に永続化できなくなり、十分に速くインデックスを作成できないため、**OpenSearchはログのドロップを開始します。**

7. **AOTログサーバーはログを圧縮できますか？どのくらいの圧縮率を期待できますか？**

はい。AOTログサーバーは、OpenSearchにログを保存するためにデフォルトの**LZ4圧縮アルゴリズム**を使用します。標準的な圧縮率は約**2:1**で、ログデータは元のサイズの半分以下に削減され、高速な読み書きパフォーマンスを維持します。

8. **各インフラストラクチャタイプ（シングルサイトオンプレミス、マルチサイトオンプレミス、シングルリージョンクラウド、マルチリージョンクラウド、ハイブリッド、MSP/テナント）において、AOTログサーバーはどこにデプロイすべきですか？また、その理由は何ですか？**

   AOTログサーバーは、常に**VDAと同じ視線上に**デプロイする必要があります。これにより、安定した接続が確保され、ログを生成するコンポーネントとそれを取り込むログサーバー間の低遅延が維持されます。すべてのコンポーネント（VDA、DDC、StoreFront、Gatewayなど）がログサーバーに確実に到達できる限り、環境は正常に機能します。

9. **リージョンごとに1つのログサーバーが必要ですか、それともすべてを集中化できますか？遅延とエグレスについてはどうですか？**

   ログサーバーを集中化することは可能ですが、お客様はご自身の環境における**遅延**と**エグレスコスト**の影響を評価する必要があります。**リージョン間の遅延はログの取り込みに影響を与える可能性があり**、特に大量の期間中に顕著です。ラウンドトリップ遅延が高い場合、ログの急増やバーストにより、ピーク負荷時に遅延、バックログの蓄積、または潜在的な損失が発生する可能性があります。ログがリージョンまたはクラウドの境界を越える場合、エグレス料金が発生する可能性があります。

10. **AOTは大量のネットワーク帯域幅やシステムリソースを消費しますか？**

    いいえ。AOTは、エンドポイント、VDA、その他のコンポーネント、およびネットワークパフォーマンスへの影響を最小限に抑えるように設計されています。

    AOTはログを継続的に収集し、HTTPS経由でほぼリアルタイムにAOTログサーバーにアップロードします。個々のログレコードは通常非常に小さく（多くの場合わずか数キロバイト）、これにより通常の運用中のネットワークオーバーヘッドを最小限に抑えることができます。

    消費される全体的な帯域幅は、アクティブセッションの数、有効なコンポーネント、および環境のアクティビティによって異なります。ほとんどのデプロイメントにおいて、AOTのログトラフィックは全体のネットワーク利用率のごく一部を占めるにすぎません。

    AOTは、ストレージ要件を削減し、ログサーバーへのデータ転送を最適化するために圧縮も使用します。

11. **AOTログサーバーで1,000台のマシンをサポートするための最小ハードウェア仕様は何ですか？**

1,000台のマシンまでの環境では、**1ノード**（ログサーバー + OpenSearch結合）、**4 vCPU、8 GB RAM、2,000 IOPS**以上（SSDまたはNVMe推奨）、**1 Gbps NIC**が必要です。このセットアップは、ログ量が中程度の小規模またはシングルサイトのデプロイメントに適しています。

12. **ログサーバーに問題がある場合、どのようにトラブルシューティングできますか？**

    LogServerはDockerコンテナとして実行されているため、すべてのDockerコマンドを使用して問題を見つけることができます。

    ```
    docker logs logserver

    docker inspect logserver
    ```

    また、ユーザーは実行中のコンテナにアタッチして、ログサーバー自体のログを表示することもできます。

    ```
    docker exec –it logserver bash
    ```

    logserver docker コンテナのbashシェルで、ユーザーはlogserverとopensearchの健全性を確認できます。

    ```
    curl http://localhost:5000/Ping

    curl http://localhost:9200/_cluster/health?pretty
    ```

    そして、コンテナ内のログを確認します。

    ```
    tail Config/applogs.txt

    tail Config/weblogs.txt
    ```

    さらにログが必要な場合は、ユーザーはStartLogServer.sh/StartLogServer.batでLOG_LEVEL=0を変更し、これらのスクリプトファイルでlogserverを再起動できます。そうすると、詳細なログにはTRACE、DEBUG、INFO、WARN、ERRORのすべてのレベルが含まれるようになります。

13. **不適切にデタッチされたログサーバーのストレージディスクからの回復**

    Citrix Connector Applianceの管理UIからログサーバーのストレージディスクを最初にデタッチせずに、**ハイパーバイザー**または**クラウドプロバイダー**から直接削除またはデタッチした場

合、Connector Applianceはストレージ構成を保持し、ディスクがまだ接続されていると見なします。その結果、以前に接続されていたディスクはConnector Applianceに構成されたままになり、新しいディスクの接続は失敗し、次のようなエラーが表示されることがあります: **A local disk is already mounted to the provider**。

オプション1（推奨）： 元のディスクがまだ利用可能な場合：

a. ハイパーバイザーまたはクラウドプロバイダーから、元のディスクをConnector Appliance VMに再接続します。
b. Connector Applianceを再起動します。
c. アプライアンスが正常に起動した後、Connector Applianceの管理UIを使用してディスクをデタッチします。
d. 必要に応じて、新しいディスクを接続できるようになります。

オプション2： 元のディスクが利用できなくなった場合は、以下のAPIリクエストを実行して、古いストレージ構成を手動で削除します。認証トークンを取得し、適切なコマンドを実行します。

リナックス:

```
curl -X POST "https://<connector-fqdn>/storage/$detach" \

-H "Content-Type: application/json" \

-H "Authorization: Bearer <token>" \

-d '{"targetProvider":"logserver-provider","storageType":"local"}'
```

ウィンドウズ:

```
curl -X POST "https://<connector-fqdn>/storage/$detach" ^

-H "Content-Type: application/json" ^

-H "Authorization: Bearer <token>" ^

-d "{\"targetProvider\":\"logserver-provider\",\"storageType\":
\"local\"}"
```

> **注:**
>
> 古いストレージ構成が正常に削除された場合でも、APIがエラーを返すことがあります。ディスクの接続を再試行する前に、ストレージ構成を確認してください。

> ベストプラクティスとして、ハイパーバイザーまたはクラウドプロバイダーからディスクを削除またはデタッチする前に、必ずConnector Applianceの管理UIからログサーバーのストレージディスクをデタッチしてください。これにより、Connector Applianceはストレージ構成をクリーンアップし、古いストレージ参照が残るのを防ぎます。

修正された問題

- **大規模な展開でOpenSearchのサーキットブレーカーがHTTP 429エラーを引き起こす** (XASUP-8128)

多数のDDC、StoreFrontサーバー、VDAが同時にAOTログを送信する大規模な展開において、親サーキットブレーカーが作動したため、OpenSearchが断続的にHTTP 429でリクエストを拒否していました。この問題は解決されました。

- **StudioでAOTログサーバーを有効にした後、Directorがログにアクセスできない** (XASUP-7776)

AOTログサーバーがHTTPを使用して構成されている場合、LOCAL_DOWN_ONLYフラグはデフォルトで有効になります。これにより、Directorはログを表示できなくなり、アクセスエラーが発生する可能性があります。この問題は、Log Serverバージョン2603以降で修正されています。HTTPSモードで構成されている場合、LOCAL_DOWN_ONLYフラグは自動的に無効になり、Directorは追加設定なしでログを表示できます。

ただし、HTTPモードで運用する場合、セキュリティ上の理由からLOCAL_DOWN_ONLYフラグは有効のままであり、ログアクセスを許可するにはユーザーが手動で更新する必要があります。

- **Log Serverのアップグレード時にポート競合エラーが発生する** (XASUP-7658)

Log Serverのアップグレード中に、インストーラーがシステムキャッシュの競合により、構成されたポートがすでに使用中であると誤って報告し、最初の試行でアップグレードが失敗していました。この問題は解決され、アップグレードは再試行を必要とせずに正常に完了します。

- **Citrix Studioで設定を更新すると、Log Serverの認証キーがクリアされる** (STUD-40505)

Citrix StudioでLog Serverのアドレスとポートを更新する操作は最初は機能しますが、設定を再確認し、認証キーを再入力せずにLog Serverの詳細を変更すると、操作が成功したように見えても、保存後に認証キーのプレースホルダーが空になります。これにより、DirectorおよびMonitorで構成が欠落したり無効になったりします。回避策として、Log Serverの設定を変更する際は常に認証キーを再入力して検証してください。この問題は、2603およびWeb Studioリリース73で解決されました。

既知の問題と制限事項

- **環境ごとにサポートされるログサーバーは1つのみ**

  現在のアーキテクチャでは、環境ごとに単一のAOTログサーバーのみがサポートされており、Web StudioとDirector/Monitorの両方が単一のログサーバー構成でのみ動作するように設計されています。すべてのコンポーネントは、この同じログサーバーを指す必要があります。複数のログサーバーにわたるワークロードの構成または分散は、現在サポートされていません。この単一のログサーバーは、最大128,000のアクティブなコンポーネント接続を処理し、1秒あたり最大10,000のログイベントを処理できます。これはほとんどの展開で十分です。これらの制限は、コンポーネントの数ではなく、接続容量とログスループットに基づいているため、非常に大規模な環境でも、スループットのしきい値内に収まっている限り、1つのログサーバーで運用できます。

  ただし、ピーク時のアクティビティ中にログ量が非常に多いお客様は、水平スケーリングがないため、取り込みまたはインデックス作成の制限に達する可能性があります。複数のログサーバーのサポートとより広範なスケーリングオプションは、進化するアーキテクチャの一部として、将来のリリースで導入される予定です。

- **XenServerでホストされているWindows VM**でAOTログサーバーを実行することは**サポートされていません**。 XenServerはネストされた仮想化をサポートしていないため、Dockerがゲスト VM内で実行できません。その結果、この構成ではログサーバーコンテナをデプロイできません。

- **Windows上のDocker Desktopは、AOTログサーバーにアクティブなユーザーセッションを必要とします**

  Docker Desktopを使用してWindows VMにAOTログサーバーをデプロイすると、コンテナは Docker Desktopを起動したユーザーセッションのコンテキスト内で実行されます。Docker Desktopはユーザーセッションベースのアプリケーションとして設計されており、Windows上でシステムレベルのサービスとして実行されません。その結果、ユーザーがログアウトすると Docker Desktopが停止し、AOTログサーバーコンテナも停止します。この動作のため、展開が

特定のユーザーセッションに依存しているため、ユーザーがログアウトするとAOTログサーバーが停止します。他の管理者は実行中のコンテナにアクセスしたり管理したりできません。

回避策: Docker DesktopとAOTログサーバーコンテナが継続して実行されるように、ユーザーセッションをアクティブな状態または切断された状態に保ちます（ログアウトしないでください）。

推奨事項 本番環境での展開には、次のいずれかを使用してください。

- Docker Engineを使用してLinux VMにAOTログサーバーをデプロイする
- サポートされている場合は、Citrix Connector Appliance (CCA) ベースの展開を使用する

これらのオプションにより、ログサーバーはユーザーセッションから独立して実行され、より信頼性の高い常時稼働の展開モデルが提供されます。

> **注:**
>
> このアプローチは、セッションタイムアウトや厳格なセキュリティポリシーが適用される環境では信頼できない場合があります。
>
> この動作は、Windows上のDocker Desktopの既知の制限であり、AOTログサーバーに固有のものではありません。

- **ライセンスサーバーログがDirector/Monitorで不正なホストタイプで表示される**

  Directorでライセンスサーバーから AOTログを表示すると、ホスト名は正しいにもかかわらず、**ホストタイプ**列に値が**DDC**ではなく**License Server**と誤って表示される場合があります。

  この問題は、Directorでのホストタイプの表示方法に限定されており、ログ収集や機能には影響しません。この問題は、最新のライセンスサーバーリリースで解決されており、**License Server version: 55000 以降**で修正されています。

- **MonitorでAOTログを表示するにはCitrix Cloud Connectorが必要です**

  AOTログを表示するために**Citrix Monitor**を使用するお客様は、環境内に少なくとも1つの**Citrix Cloud Connector**を導入している必要があります。この要件は、AOTログサーバーがLinux VM、Windows VM、Citrix Connector Applianceのどこでホストされているかに関わらず適用されます。

Citrix Monitorは、**Cloud Connectorで実行されているMonitorサービス**に依存して、構成されたログサーバーからログを取得し、UIに表示します。

Windows Cloud Connectorがない場合、MonitorでAOTログを取得または表示することはできません。

- **Citrix DirectorでADC Gatewayログが正しく表示されない**

  症状: Citrix DirectorでCitrix ADC GatewayのAlways On Tracing (AOT)ログを表示すると、次の現象が見られる場合があります:

  - ログレベルが**Debug**または**Info**ではなく**Error**と表示される。
  - **Message**列に生のログエントリ全体が表示される。
  - 表示されるタイムスタンプが元のイベントタイムスタンプと異なる。
  - 影響を受けるのは、形式が不正なJSONログレコードのみです。有効なログレコードは正しく表示されます。

  影響を受けるバージョン: Citrix ADC **14.1-73.x**より前のバージョンおよびCitrix ADC **15.1-8.x**より前のバージョン。

  原因: Citrix ADC Gatewayが、AOTログサーバーで解析できない不正な形式のJSONログレコードをアップロードします。その結果、ログサーバーは生のログエントリを保存し、エラーとして分類します。

  解決策: Citrix ADCを次のいずれかのバージョン以降にアップグレードしてください。

  - 14.1-73.x
  - 15.1-8.x

  修正済み: Citrix ADC **14.1-73.x** および Citrix ADC **15.1-8.x**。

  - AOTログサーバーは現在、**FIPS準拠の展開**をサポートしていません。FIPS要件が必須のお客様は、FIPSサポートが利用可能になるまで本番環境への展開を延期する必要があります。

    FIPS準拠を必要としないお客様は、サポートされている環境でAOTログサーバーの展開と評価を継続できます。

サードパーティ通知

Citrix Virtual Apps and Desktops™ のこのリリースには、以下のドキュメントに定義されている条件に基づいてライセンスされたサードパーティ製ソフトウェアが含まれている場合があります。

- Citrix Virtual Apps and Desktops サードパーティ通知(/ja-jp/citrix-virtual-apps-desktops/current-release/downloads/third-party-notices-apps-and-desktops-2603.pdf) (PDFダウンロード)
- Citrix Assistant App サードパーティ通知 - プレビュー(/ja-jp/citrix-virtual-apps-desktops/current-release/downloads/thirdpartynotices_citrix_assistant_app.pdf) (PDFダウンロード)
- FlexNet Publisher 2017 (11.15.0.0) の非商用ソフトウェア開示(/ja-jp/citrix-virtual-apps-desktops/current-release/downloads/fnp-licensing-11-15-0-ncsd-summary.pdf) (PDFダウンロード)
- FlexNet Publisher 11.15.0 で使用されている FlexNet Publisher ドキュメント補足 サードパーティおよびオープンソースソフトウェア(/ja-jp/citrix-virtual-apps-desktops/current-release/downloads/fnp-licensing-11-15-0-opensource.pdf) (PDFダウンロード)

SDKおよびAPI

このリリースでは、いくつかのSDKとAPIが利用可能です。SDKとAPIにアクセスするには、Build anything with Citrixにアクセスしてください。そこから、**Citrix Workspace**を選択して、Citrix Virtual Apps and Desktopsおよび関連コンポーネントのプログラミング情報にアクセスします。

> **注:**
>
> Citrix Virtual Apps and Desktops™ SDKとCitrix Group Policy SDKは、モジュールまたはスナップインとしてインストールできます。いくつかのコンポーネントSDK（Citrix Licensing、Citrix Provisioning、StoreFrontなど）は、スナップインのみを使用してインストールされます。

> この製品はPowerShellバージョン3から5をサポートしています。

シトリックス バーチャルアップス アンド デスクトップス™ SDK

このSDKは、Delivery Controller™またはStudioをインストールすると、PowerShellモジュールとして自動的にインストールされます。これにより、スナップインを追加することなく、このSDKのコマンドレットを使用できます。（このSDKをスナップインとしてインストールすることを選択した場合の指示は以下に記載されています。）

権限

Citrix管理権限を持つIDを使用してシェルまたはスクリプトを実行する必要があります。Controller上のローカル管理者グループのメンバーは、Citrix Virtual AppsまたはCitrix Virtual Desktops™をインストールするための完全な管理権限を自動的に持っていますが、Citrixは、通常の操作では、ローカル管理者アカウントを使用するのではなく、適切な権限を持つCitrix管理者を作成することを推奨します。

コマンドレットにアクセスして実行する

1. PowerShellでシェルを起動します。Studioを開き、**PowerShell**タブを選択し、**Launch PowerShell**をクリックします。
2. スクリプト内でSDKコマンドレットを使用するには、PowerShellで実行ポリシーを設定します。PowerShellの実行ポリシーについては、Microsoftのドキュメントを参照してください。
3. (モジュールではなく) スナップインを使用する場合は、`Add-PSSnapin` (または`asnp`) コマンドレットを使用してスナップインを追加します。

   V1とV2はスナップインのバージョンを示します。XenDesktop 5のスナップインはバージョン1です。Citrix Virtual Apps and Desktops、およびそれ以前のXenDesktop 7バージョンのスナップインはバージョン2です。例えば、Citrix Virtual Apps and Desktopsスナップインをインストールするには、`Add-PSSnapin Citrix.ADIdentity.Admin.V2`と入力します。すべてのコマンドレットをインポートするには、次のように入力します: `Add-PSSnapin Citrix.*.Admin.V*`

これで、コマンドレットとヘルプファイルを使用できます。

- このSDKのヘルプファイルにアクセスするには、Categoriesリストで製品またはコンポーネントを選択し、次に**Citrix Virtual Apps and Desktops SDK**を選択します。
- PowerShellのガイダンスについては、Windows PowerShell Integrated Scripting Environment (ISE)を参照してください。

グループポリシーSDK

Citrix Group Policy SDKを使用すると、グループポリシーの設定とフィルターを表示および構成できます。このSDKは、PowerShellプロバイダーを使用して、マシンおよびユーザーの設定とフィルターに対応する仮想ドライブを作成します。このプロバイダーは、`New-PSDrive`の拡張機能として表示されます。

Group Policy SDKを使用するには、StudioまたはCitrix Virtual Apps and Desktops SDKのいずれかがインストールされている必要があります。

Citrix Group Policy PowerShell プロバイダーは、モジュールまたはスナップインとして利用できます。

- モジュールを使用する場合、追加の作業は不要です。
- スナップインを追加するには、`Add-PSSnapin citrix.common.grouppolicy` と入力します。

ヘルプにアクセスするには、`help New-PSDrive -path localgpo:/` と入力します。

仮想ドライブを作成し、設定をロードするには、`New-PSDrive <Standard Parameters> [-PSProvider] CitrixGroupPolicy -Controller <string>` と入力します。ここで、Controller 文字列は、接続して設定をロードしたいサイト内の Controller の完全修飾ドメイン名です。

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

Citrix Virtual Apps and Desktops REST API を使用すると、Citrix Virtual Apps and Desktops 展開内のリソースの管理を自動化できます。

Citrix Virtual Apps and Desktops REST API は `<https://developer.cloud.com/citrixworkspace/citrix-daas-rest-apis/docs/citrix-virtual-apps-and-desktops-apis>` で利用できます。Citrix Virtual Apps and Desktops に適用されない API は、そのようにマークされています。そこにあるガイダンスに従って、API サービスへのアクセスを設定し、API を使用してリソースを管理および最適化してください。

モニターサービス OData

Monitor API を使用すると、OData API のバージョン 3 または 4 を使用して Monitor Service データにアクセスできます。Monitor Service データからクエリされたデータに基づいて、カスタマイズされた監視およびレポートダッシュボードを作成できます。OData V.4 は ASP.NET Web API に基づいており、集計クエリをサポートしています。

詳細については、Monitor Service OData API を参照してください。

__index__

サイト全体の履歴トレンドを監視する

トレンドビューは、以下のパラメータについて、各サイトの履歴トレンド情報にアクセスします。

- セッション
- 接続障害
- マシン障害
- ログオンパフォーマンス
- 負荷評価
- キャパシティ管理
- マシン使用状況
- リソース使用率
- 各サイトのネットワーク分析。

この情報を見つけるには、**トレンド**メニューをクリックします。

ズームイン ドリルダウン機能を使用すると、期間をズームイン（グラフのデータポイントをクリック）し、トレンドに関連する詳細を表示するためにドリルダウンすることで、トレンドグラフをナビゲートできます。この機能により、誰が、または何が影響を受けているかの詳細をよりよく理解できます。

各グラフのデフォルトのスコープを変更するには、データに別のフィルターを適用します。

履歴トレンド情報が必要な期間を選択してください。期間の利用可能性は、Directorの展開によって次のように異なります。

- Premiumライセンスサイトでは、最大1年間 (365日) のトレンドレポートを利用できます。
- Advancedライセンスサイトでは、最大1か月間 (31日) のトレンドレポートを利用できます。
- PremiumおよびAdvanced以外のライセンスサイトでは、最大7日間のトレンドレポートを利用できます。

> **注:**

- すべてのDirector展開において、期間が「先月」（**現在まで**）以下に設定されている場合、セッション、障害、ログオンパフォーマンスのトレンド情報はグラフとテーブルとして利用できます。期間がカスタム終了日を指定した「先月」または「昨年」として選択されている場合、トレンド情報はグラフとして利用でき、テーブルとしては利用できません。
- Monitor Serviceのグルーミング保持値によって、トレンドデータの可用性が制御されます。デフォルト値は、データ粒度と保持で確認できます。Premiumライセンスサイトのお客様は、グルーミング保持を希望する保持日数に変更できます。
- IIS Managerの以下のパラメータは、選択可能なカスタム終了日の範囲を制御します。ただし、選択された日付のデータ可用性は、測定される特定のメトリックのグルーミング保持設定によって異なります。

パラメーター	デフォルト値
UI.TrendsLast2HoursRange	3
UI.TrendsLast24HoursRange	32
UI.TrendsLast7DaysRange	32
UI.TrendsLastMonthRange	365

利用可能なトレンド

セッションの傾向を表示: 「**セッション**」タブから、デリバリーグループと期間を選択して、同時セッション数に関する詳細情報を表示します。

「**セッションの自動再接続**」列には、セッション内の自動再接続の数が表示されます。自動再接続は、セッションの信頼性ポリシーまたはクライアント自動再接続ポリシーが有効な場合に有効になります。エンドポイントでネットワークの中断が発生した場合、次のポリシーが有効になります。

- セッションの信頼性が有効になり（デフォルトで3分間）、Citrix Receiver™またはCitrix Workspace™アプリがVDAへの接続を試行します。
- クライアント自動再接続が3分から5分の間に有効になり、クライアントがVDAへの接続を試行します。

両方の再接続がキャプチャされ、ユーザーに表示されます。この情報は、再接続が発生してからDirector UIに表示されるまでに最大5分かかる場合があります。

自動再接続情報は、中断のあるネットワーク接続の表示とトラブルシューティングに役立ちます。また、シームレスなエクスペリエンスを持つネットワークも分析します。フィルターで選択した特定のデリバリーグループまたは期間の再接続数を表示できます。ドリルダウンでは、セッションの信頼性やクライアント自動再接続、タイムスタンプ、エンドポイントIP、Workspaceアプリがインストールされているマシンのエンドポイント名などの追加情報が提供されます。

デフォルトでは、ログはイベントのタイムスタンプの降順でソートされます。この機能は、Windows用Citrix Workspaceアプリ、Mac用Citrix Workspaceアプリ、Windows用Citrix Receiver、およびMac用Citrix Receiverで利用できます。この機能には、Delivery Controller™バージョン7 1906以降、およびVDA 1906以降が必要です。

セッションの再接続の詳細については、「セッション」を参照してください。

ポリシーの詳細については、「クライアント自動再接続ポリシー設定」および「セッションの信頼性ポリシー設定」を参照してください。

自動再接続データがDirectorに表示されない場合があります。その理由は次のとおりです。

- WorkspaceアプリがVDAに自動再接続データを送信していません。
- VDAがモニターサービスにデータを送信していません。
- Delivery Controllerは、対応するセッションがない可能性があるため、VDAペイロードを破棄します。

> **注:**
>
> 特定のCitrix Gatewayポリシーが設定されている場合、クライアントIPアドレスが正しく取得されないことがあります。

> **接続障害の傾向を表示:** 「障害」タブから、接続、マシンタイプ、障害タイプ、デリバリーグループ、および期間を選択して、サイト全体のユーザー接続障害に関する詳細情報を含むグラフを表示します。

マシン障害の傾向を表示: Single-session OS Machine FailuresタブまたはMulti-session OS Machinesタブから、障害タイプ、デリバリーグループ、および期間を選択すると、サイト全体のマシン障害に関する詳細情報を含むグラフが表示されます。

ログオンと再接続のパフォーマンスの傾向を表示: Logon and Reconnect Performanceタブから、デリバリーグループと期間を選択すると、ユーザーのログオンと再接続の期間に関する詳細情報を含むグラフがサイト全体に表示されます。このビューは、ログオンまたは再接続の数と全体的なパフォーマンスを理解するのに役立ちます。

グラフには以下が含まれます。

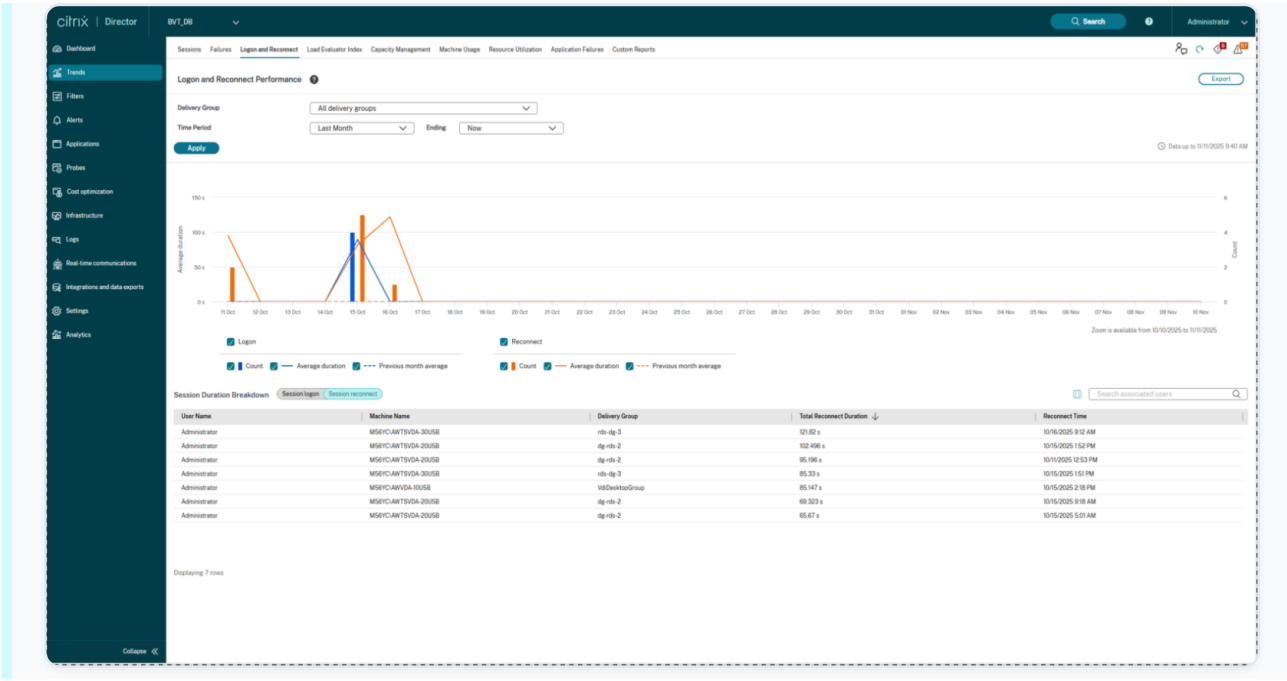
- **ログオンイベント、ログオン期間、およびフェーズ**（ブローカー処理、対話型セッションなど）。新しいセッションを起動する際のユーザーエクスペリエンスに関する洞察を提供します。
- **再接続イベントと再接続期間**。切断されたセッションから再接続する際のユーザーエクスペリエンスに関する洞察を提供します。

凡例を使用して、分析対象の傾向に基づいて必要なメトリックを選択します。

- カウント
- 平均期間
- 以前の（期間）平均

グラフの下の表には、ユーザーセッションまたは接続ごとの**セッションログオン**と**セッション再接続**の詳細が表示されます。表の上にある選択肢を使用してメトリックを切り替えたり、表示する列を選択したり、任意の列で並べ替えたり、レポートをPDF、Excel、またはCSV形式でエクスポートしたりできます。

> **注:**
>
> セッション再接続期間は、**DirectorおよびVDAバージョン2511 CR以降**でサポートされています。



負荷評価の傾向を表示: Load Evaluator Indexタブから、Multi-session OSマシン間で分散される負荷に関する詳細情報を含むグラフを表示します。このグラフのフィルターオプションには、デリバリーグループまたはデリバリーグループ内のMulti-session OSマシン、Multi-session OSマシン（デリバリーグループ内のMulti-session OSマシンが選択されている場合にのみ利用可能）、および範囲が含まれます。

ホストされたアプリケーションの使用状況を表示: この機能の利用可能性は、組織のライセンスによって異なります。 **Capacity Management**タブから、**Hosted Applications Usage**タブを選択します。デリバリーグループと期間を選択すると、ピーク時の同時使用状況を示すグラフと、アプリケーションベースの使用状況を示す表が表示されます。Application Based Usage表から、特定のアプリケーションを選択して詳細と、そのアプリケーションを使用している、または使用したユーザーのリストを確認できます。

Single-sessionおよびMulti-session OSの使用状況を表示: トレンドビューには、サイト別およびデリバリーグループ別のSingle-session OSの使用状況が表示されます。**サイト**を選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、ユーザーごとの使用状況が表示されます。 トレンドビューには、サイト別、デリバリーグループ別、およびマシン別のMulti-session OSの使用状況も表示されます。**サイト**を選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、マシンごとおよびユーザーごとの使用状況が表示されます。マシンが選択されている場合は、ユーザーごとの使用状況が表示されます。

仮想マシンの使用状況を表示: マシン使用状況タブから、**シングルセッションOSマシンまたはマルチセッションOSマシン**を選択すると、VMの使用状況をリアルタイムで確認でき、サイトのキャパシティニーズを迅速に評価できます。 シングルセッションOSの可用性 - サイト全体または特定

のデリバリーグループにおけるシングルセッションOSマシン（VDI）の可用性による現在の状態を表示します。 マルチセッションOSの可用性 - サイト全体または特定のデリバリーグループにおけるマルチセッションOSマシンの可用性による現在の状態を表示します。

コスト最適化によるマシン使用状況の可視性を高めるには、表示されるバナーの以下のリンクをクリックします。

- 推定節約額 - このリンクをクリックすると、**コスト最適化**ページの**推定節約額**セクションに移動し、すべてのデリバリーグループの詳細が表示されます。
- 節約レポート - このリンクをクリックすると、**コスト最適化**ページの**節約レポート**セクションに移動し、すべてのデリバリーグループの詳細が表示されます。

> **注:**
>
> 利用可能カウンターに表示されるマシンの数には、メンテナンスモードのマシンが含まれます。

> **リソース使用率の表示: リソース使用率**タブから、**シングルセッションOSマシンまたはマルチセッションOSマシン**を選択すると、CPUおよびメモリ使用量、IOPS、各VDIマシンのディスク待機時間に関する履歴トレンドデータを確認でき、より適切なキャパシティプランニングに役立ちます。 この機能には、Delivery ControllerおよびVDAの**バージョン7.11**以降が必要です。 グラフには、平均CPU、平均メモリ、平均IOPS、ディスク待機時間、ピーク時の同時セッションのデータが表示されます。マシンにドリルダウンして、CPUを消費している上位10個のプロセスのデータとグラフを表示できます。

デリバリーグループと期間でフィルタリングします。CPU、メモリ使用量、およびピーク時の同時セッションのグラフは、過去2時間、24時間、7日間、1か月、1年間で利用できます。平均IOPSとディスク待機時間のグラフは、過去24時間、1か月、1年間で利用できます。バナーの**確認**リンクをクリックすると、コスト最適化によるマシン使用状況の可視性を高めることができます。このリンクをクリックすると、**コスト最適化**ページの**ワークロードの適正化**タブに移動し、**リソース使用率**タブから選択したデリバリーグループの詳細が表示されます。

> **注:**
>
> - 履歴マシン使用率ページの「上位10プロセス」テーブルでデータを収集して表示するには、監視ポリシー設定の**プロセス監視を有効にする**を**許可**に設定する必要があります。

このポリシーは、デフォルトで**禁止**に設定されています。すべてのリソース使用率データはデフォルトで収集されます。これは、**リソース監視を有効にする**ポリシー設定を使用して無効にできます。グラフの下のテーブルには、マシンごとのリソース使用率データが表示されます。詳細については、「監視ポリシー設定」を参照してください。

- 平均IOPSは日次平均を示します。ピークIOPSは、選択した期間のIOPS平均の最高値として計算されます。（IOPS平均とは、VDAで1時間中に収集されたIOPSの時間平均です）。
- マシンのドリルダウンでは、平均CPUまたは平均メモリ使用量が1%を超えるプロセスが一覧表示されます。これは、場合によっては10個未満のプロセスしか表示されない可能性があることを意味します。

ネットワーク分析データの表示: この機能の可用性は、組織のライセンスと管理者権限によって異なります。この機能には、Delivery Controllerの**バージョン7.11**以降が必要です。

ネットワークタブから、ネットワーク分析を監視します。これにより、ネットワークのユーザー、アプリケーション、デスクトップのコンテキストビューが提供されます。この機能により、DirectorはCitrix ADMからのHDX Insightレポートを通じて、展開におけるICAトラフィックの高度な分析を提供します。詳細については、「ネットワーク分析の構成」を参照してください。

アプリケーション障害の表示: アプリケーション障害タブには、VDA上の公開アプリケーションに関連する障害が表示されます。

この機能には、Delivery ControllerおよびVDAの**バージョン7.15**以降が必要です。Windows Vista以降を実行するシングルセッションOS VDA、およびWindows Server 2008以降を実行するマルチセッションOS VDAがサポートされています。 詳細については、「履歴アプリケーション障害監視」を参照してください。

デフォルトでは、マルチセッションOS VDAからのアプリケーション障害のみが表示されます。監視ポリシーを使用して、アプリケーション障害の監視を設定できます。詳細については、「監視ポリシー設定」を参照してください。

プローブ結果の表示: プローブ結果タブには、構成ページでプローブ用に構成されたアプリケーションおよびデスクトップのプローブ結果が表示されます。ここでは、障害が発生した起動の段階が記録されます。

詳しくは、「アプリケーションおよびデスクトップのプローブ」を参照してください。

カスタマイズされたレポートの作成: カスタムレポートタブは、監視データベースからリアルタイムおよび履歴データを表形式で含むカスタムレポートを生成するためのユーザーインターフェイスを提供します。

この機能には、Delivery Controllers **バージョン7.12**以降が必要です。

以前に保存したカスタムレポートクエリのリストから、**実行してダウンロード**をクリックしてレポートをCSV形式でエクスポートしたり、**ODataをコピー**をクリックして対応するODataクエリをコピーして共有したり、**編集**をクリックしてクエリを編集したりできます。 マシン、接続、セッション、またはアプリケーションインスタンスに基づいてカスタムレポートクエリを作成できます。マシン、デリバリーグループ、期間などのフィールドに基づいてフィルター条件を指定します。カスタムレポートに必要な追加の列を指定します。プレビューには、レポートデータのサンプルが表示されます。カスタムレポートクエリを保存すると、保存されたクエリのリストに追加されます。

コピーしたODataクエリに基づいてカスタムレポートクエリを作成できます。これを行うには、ODataクエリオプションを選択し、コピーしたODataクエリを貼り付けます。結果のクエリは後で実行するために保存できます。

> **注:**
>
> ODataクエリを使用して生成されたプレビューおよびエクスポートレポートの列名はローカライズされておらず、英語で表示されます。
>
> グラフ上のフラグアイコンは、特定の期間における重要なイベントまたはアクションを示します。フラグにマウスを合わせ、クリックしてイベントまたはアクションを一覧表示します。

> **注:**
>
> - HDX™接続ログオンデータは、7より前のVDAでは収集されません。それより前のVDAの場合、グラフデータは0と表示されます。
> - Citrix Studioで削除されたデリバリーグループは、関連データが整理されるまで、Director Trendsフィルターで選択可能です。削除されたデリバリーグループを選択する

と、保持期間までの利用可能なデータのグラフが表示されます。ただし、テーブルにはデータは表示されません。

- アクティブなセッションを含むマシンをあるデリバリーグループから別のデリバリーグループに移動すると、新しいデリバリーグループの**リソース使用率と負荷評価インデックス**テーブルに、古いデリバリーグループと新しいデリバリーグループから統合されたメトリックが表示されます。