シトリックス バーチャル アプリ アンド デスクトップ™ 7 2203 LTSR

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

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

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

累積更新プログラム 6 (CU6) は、2203 LTSRの最新の更新プログラムです。LTSRは、Citrix Virtual Apps and Desktops 1912およびXenApp and XenDesktopバージョン7.15でも利用可能です。

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

以前のリリース

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

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

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

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

役立つリンク

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

新機能

累積更新プログラム 7 (CU7)

リリース日: Aug 28, 2025

このリリースについて

Citrix Virtual Apps and Desktops™ 7 2203 LTSR Cumulative Update 7 (CU7) は、2203 LTSR CU5 のリリース以降に報告された 25 を超える問題を修正します。

2203 LTSR (一般情報)

2203 LTSR (機能とアップグレード情報)

このリリースの新機能

Citrix Virtual Apps and Desktops 7 2203 LTSR CU5 で修正された問題

このリリースの既知の問題

非推奨と削除

Citrix 製品サブスクリプションアドバンテージの対象期間

ダウンロード

Citrix Virtual Apps and Desktops 7 2203 LTSR CU7 のダウンロード

新規展開

CU7 をゼロから展開するにはどうすればよいですか?

CU7 メタインストーラーを使用して、CU7 に基づく新しい Citrix Virtual Apps and Desktops 環境をセットアップできます。その前に、製品についてよく理解しておくことをお勧めします。

展開計画を開始する前に、Citrix Virtual Apps and Desktops 7 2203 LTSR (初期リリース) セクションを熟読し、技術概要、インストールと構成、および セキュリティ の各セクションに特に注意してください。セットアップがすべてのコンポーネントの システム要件 を満たしていることを確認してください。

既存の展開

何を更新しますか?

CU7 は、2203 LTSR の 15 の ベースラインコンポーネント に更新を提供します。注意: Citrix は、展開のすべての LTSR コンポーネントを CU7 に更新することを推奨しています。例: Citrix Provisioning が LTSR 展開の一部である場合、Citrix Provisioning コンポーネントを CU4 に更新してください。Citrix Provisioning が展開の一部でない場合、インストールまたは更新する必要はありません。

2203 LTSR CU7 ベースラインコンポーネント

2203 CU7 ベースラインコンポーネント	プログラムと機能に表示されるバージョン	ドキュメント
シングルセッションVDA	2203.0.7000.7522	シングルセッションVDA
マルチセッションVDA	2203.0.7000.7522	マルチセッションVDA
デリバリーコントローラー	2203.0.7000.7522	デリバリーコントローラー
シトリックス スタジオ	7.33.7000.57	シトリックス スタジオ
Citrix Director (シトリックス ディレクター)	7.33.7000.26	シトリックス ディレクター
Citrixグループポリシー管理	7.33.7000.20	Citrixグループポリシー管理
Citrixグループポリシー クライアント側拡張	7.33.7000.16	
シトリックス ストアフロント	2203.0.7000.7	Citrix ストアフロント
シトリックス プロビジョニング	7.33.40	Citrix プロビジョニング
ユニバーサル プリント サーバー	7.33.7000.18	「ユニバーサルプリントサーバー」(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/printing/printing-provision-printers.html)
セッション録画	22.3.7000	セッションレコーディング

2203 CU7 ベースラインコンポーネント	プログラムと機能に表示されるバージョン	ドキュメント
リナックス ブイディーエー	22.03.6000	Linux 仮想配信エージェント(/ja-jp/linux-virtual-delivery-agent.html)
プロファイル管理	22.3.7000.10	プロファイル管理
Citrix フェデレーション認証サービス	10.9.700.16	Citrix フェデレーション認証サービス (FAS)(/ja-jp/federated-authentication-service/2203-ltsr.html)
ブラウザコンテンツリダイレクション	15.32.7000.10	「ブラウザコンテンツリダイレクション」(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/multimedia/browser-content-redirection.html)
シトリックス プローブエージェント 2305	2305.1.0.0	ダウンロード

2203 LTSR CU7 互換コンポーネント

以下のコンポーネント（以下のバージョン）はLTSR環境と互換性があります。これらはLTSRのメリット（延長されたライフサイクルと修正のみの累積更新プログラム）の対象ではありません。Citrix®は、2203環境内でこれらのコンポーネントを新しいバージョンにアップグレードするよう求める場合があります。

互換性のあるコンポーネントと機能	プログラムと機能に表示されるバージョン	ドキュメント
アプリレイヤリング	2309	Citrix App Layering (Citrixアプリケーションレイヤリング)
HDX リアルタイム最適化パック	2.9.600	HDX RealTime Optimization Pack (HDX RealTime最適化パック)

互換性のあるコンポーネントと機能	プログラムと機能に表示されるバージョン	ドキュメント
ライセンスサーバー	11.17.2.0_BUILD_53100	ライセンスサーバー(/ja-jp/licensing/current-release.html)
ユーザーパーソナライゼーションレイヤー	25.3.3	ユーザーパーソナライゼーションレイヤー(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/install-configure/user-personalization-layer.html)
セッションレコーディングウェブプレーヤー	22.3.7000.6	セッションレコーディングWebプレーヤー(/ja-jp/session-recording/2203-ltsr/view-recordings/session-recording-web-player.html)
Microsoft Teamsの最適化	15.32.3000.9	Microsoft Teamsの最適化(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/multimedia/opt-ms-teams.html)
ワークスペース環境管理	22.12.0	ワークスペース環境管理
XenApp & XenDesktop 7.15 LTSR VDA (最新リリース)*	最新の累積更新プログラムのみ	ドキュメント

2203 LTSR CU7 の主な除外事項

以下の機能、コンポーネント、およびプラットフォームは、2203ライフサイクルマイルストーンおよび特典の対象ではありません。具体的には、累積更新プログラムと拡張ライフサイクル特典は除外されます。除外された機能およびコンポーネントの更新は、通常の現在のリリースを通じて利用できます。

除外されるコンポーネントと機能
AppDisks™
AppDNA®

除外されるコンポーネントと機能
Citrix SCOM 管理パック
フレームホーク
パーソナル vDisk
StoreFront Citrix オンライン統合
ライセンスアクティベーションサービス

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

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

新機能

Citrix Virtual Apps and Desktops™ 7 2203 LTSR Cumulative Update 7 (CU7) で利用可能な新機能と機能強化は次のとおりです。

> **注：**
>
> 2203 LTSR CU7 をご利用の場合は、次のいずれかのアップグレードパスに従うことをお勧めします。
>
> - 2402 LTSR CU3 以降の累積更新プログラムにアップグレードします。
> - 2507 以降のリリースにアップグレードします。
> - 一般的に、将来のリリースにアップグレードすることをお勧めします。

ファイルベースのライセンスシステムのEOL通知

従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されてきたファイルベースのライセンスシステムは、April 15, 2026 にサポート終了 (EOL) となります。License Activation Service (LAS) は、Citrix製品スイート全体での製品アクティベーションのための次世代

テクノロジーです。April 15, 2026 以降、LASがCitrixオンプレミスコンポーネントをアクティベートおよびライセンス供与する唯一の方法となります。サポートを継続するには、Citrix Virtual Apps and Desktops展開がLAS互換バージョンである必要があります。LAS互換の最小要件となるCVADバージョンは次のとおりです。

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

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

デリバリーコントローラー

Citrix Virtual Apps and Desktops サイトとのライセンスサーバーバージョンの互換性

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

修正された問題

Citrix Virtual Apps and Desktops™ 7 2203 LTSR CU6以降で修正された問題は次のとおりです。

デリバリーコントローラー™

- タスク定義内の無効な変数名が原因で、モニターサービスのグルーミングが失敗する可能性があります。この問題は`GroomResourceUtilization`タスクに影響を与え、他のグルーミングタスクにも影響を与える可能性があります。
- 数か月分のデータを保持している大規模なMonitorDBで、CPU使用率が高くなることがあります。インデックスを追加すると、CPU使用率を約10〜15%削減できます。
- 「,」のような非標準の小数点記号を使用している場合、1912 CU8から2203 CU4にアップグレードした後、新しいマシンカタログを作成したり、既存のVDAの電源をオンにしたりできなくなることがあります。
- Delivery Controllerを2203 CU5から2402 CU1にアップグレードすると、Citrix Studioでの自動サイトアップグレード中に失敗する可能性があります。Delivery Controllerのアップグレードは完了しますが、サイトの更新は正常に終了しません。

グラフィック

- VDA 2402にアップグレードした後、再起動後の最初のICA®セッションでグレースクリーンが表示されることがありますが、これは、切断して再接続するか、最初にアプリケーションセッションを起動することで解決します。
- Citrix Virtual Apps and Desktops (CVAD) 2203 CU5または2402にアップグレードした後、WMIインスタンス `Citrix_Client_Enum` へのアクセスが「Provider Load Failure」エラーで失敗する可能性があります。

メタインストーラー

- VDA 2203にアップグレードした後、再起動後の最初のICAセッションが起動しません。これは、セッションを2回目に起動することで解決できます。
- VDAを2203 CU3からCU5にアップグレードすると、`HKLM\SYSTEM\CurrentControlSet\Services\picadm` の下のすべてのレジストリ設定がリセットされ、`DisableFullStreamWrite` エントリの削除も含まれます。これらの設定が保持されることを期待する場合は、アップグレード後に再適用する必要がある場合があります。

ユニバーサル プリント サーバー

印刷

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

シングルセッションOS用VDA

セッション/接続

- セッションを起動した後、オーディオデバイスを複数回抜き差しすると、セッションがオーディオデバイスを認識しなくなります。
- シャットダウン中に、ストップコードを伴うブルースクリーンエラーが発生する可能性があります。

システム例外

- Windows 11 24H2を使用すると、セッションが起動中にハングし、ブラックスクリーンが表示されます。
- VDA 2203 CU5またはCU6にアップグレードした後、サーバーにログインできなくなることがあります。ログオンまたはログオフ中にセッションが応答しなくなります。

- picadm.sysモジュールの問題により、PAGE_FAULT_IN_NONPAGED_AREA (0x50) というコードのブルースクリーンエラーが断続的に発生する場合があります。
- CVAD 2203 CU5では、picadm.sysの新しい問題により、デバイスでブルースクリーンエラーが表示される場合があります。
- picadm.sysモジュールの問題により、PAGE_FAULT_IN_NONPAGED_AREA (0x50) というコードのブルースクリーンエラーが断続的に発生する場合があります。

マルチセッションOS用VDA

クリップボード

- Citrix Workspace™ for HTML5を使用しているときに、Excelで大量のデータをコピー＆ペーストすると、セッションがクラッシュします。
- マルチセッション環境で、約2,493文字を超える文字をコピーすると、コピー＆ペースト機能が動作しなくなる場合があります。
- Clipboard DLLの問題により、クリップボード操作中にCtxSvcHost.exeがクラッシュする場合があります。

セッション/接続

- ホストからクライアントへのURLリダイレクトは、大文字と小文字を区別するURLパラメーターを大文字から小文字に変換するため、特定の文字の大文字/小文字を区別する必要があるアプリケーションにアクセスする際に障害が発生する可能性があります。
- クライアントユーザーでランダムなUSBリダイレクトの失敗が発生し、セッション中にPinpad、TCR、プリンターなどのUSBデバイスが認識されなくなることがあります。
- シャットダウン中にストップコードを伴うブルースクリーンエラーが発生する場合があります。
- Citrix Workspace App for Linuxからセッションを起動すると、セッションは開いたように見えますが、エラーを表示せずにすぐに閉じます。

システム例外

- VDA 2203 CU5またはCU6にアップグレードした後、サーバーにログインできなくなり、ログオンまたはログオフ中にセッションが応答しなくなる場合があります。
- picadm.sysモジュールの問題により、PAGE_FAULT_IN_NONPAGED_AREA (0x50) というコードのブルースクリーンエラーが断続的に発生する場合があります。
- CVAD 2203 CU5では、picadm.sysの新しい問題により、デバイスでブルースクリーンエラーが表示される場合があります。

- picadm.sysモジュールの問題により、PAGE_FAULT_IN_NONPAGED_AREA (0x50) というコードのブルースクリーンエラーが断続的に発生する場合があります。
- 2203 CU5 VDAにアップデートした後、アプリケーションを終了してもセッションが閉じません。
- 2203 CU5では、レジストリ内のLastPingTimeが更新されず、接続が切断される可能性があります。
- ドライバーの問題を示すバグチェックコードとともに、不定期なクラッシュが発生する可能性があります。
- ホストからクライアントへのURLリダイレクトは、大文字を小文字に変換することで、大文字と小文字を区別するURLパラメータを変更します。これにより、特定の文字の大文字/小文字の区別を必要とするアプリケーションにアクセスする際に障害が発生する可能性があります。

シトリックス プロビジョニング™

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

リナックス ブイディーエー

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

プロファイル管理

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

セッション録画

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

StoreFront™

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

累積更新プログラム 6 (CU6)

リリース日: Jan 08, 2025

このリリースについて

Citrix Virtual Apps and Desktops™ 7 2203 LTSR Cumulative Update 6 (CU6) は、2203 LTSR CU5 のリリース以降に報告された25以上の問題を修正しています。

2203 LTSR (一般情報)

2203 LTSR (機能とアップグレード情報)

このリリースの新機能

Citrix Virtual Apps and Desktops 7 2203 LTSR CU5 で修正された問題

このリリースの既知の問題

非推奨と削除

Citrix 製品サブスクリプションアドバンテージの対象期間

ダウンロード

Citrix Virtual Apps and Desktops 7 2203 LTSR 累積更新プログラム 6 (CU6)

新規展開

CU6 を新規展開するには?

CU6 メタインストーラーを使用して、CU6 に基づく新しい Citrix Virtual Apps and Desktops 環境をセットアップできます。その前に、製品についてよく理解しておくことをお勧めします。

展開の計画を開始する前に、Citrix Virtual Apps and Desktops 7 2203 LTSR (初期リリース) セクションを熟読し、技術概要、インストールと構成、および セキュリティ の各セクションに特に注意してください。セットアップがすべてのコンポーネントのシステム要件を満たしていることを確認してください。

既存の展開

何を更新しますか?

CU6 は、2203 LTSR の15のベースラインコンポーネントを更新します。Citrix は、展開のすべての LTSR コンポーネントを CU6 に更新することを推奨しています。例: Citrix Provisioning が LTSR 展開の一部である場合、Citrix Provisioning コンポーネントを CU4 に更新します。Citrix Provisioning が展開の一部でない場合、インストールまたは更新する必要はありません。

2203 LTSR CU6 ベースラインコンポーネント

2203 CU6 ベースラインコンポーネント	プログラムと機能に表示されるバージョン	ドキュメント
シングルセッションVDA	2203.0.6000.6286	シングルセッションVDA
マルチセッションVDA	2203.0.6000.6286	マルチセッションVDA
デリバリーコントローラー	2203.0.6000.6286	デリバリーコントローラー
シトリックス スタジオ	7.33.6000.29	シトリックス スタジオ
Citrix Director (シトリックス ディレクター)	7.33.6000.20	シトリックス ディレクター
Citrixグループポリシー管理	7.33.6000.9	Citrixグループポリシー管理
Citrixグループポリシー クライアント側拡張	7.33.6000.9	
シトリックス ストアフロント	2203.0.6000.11	Citrix ストアフロント
シトリックス プロビジョニング	7.33.40	Citrix プロビジョニング
ユニバーサル プリント サーバー	7.33.6000.23	「ユニバーサルプリントサーバー」(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/printing/printing-provision-printers.html)
セッション録画	22.3.6000	セッションレコーディング
リナックス ブイディーエー	22.03.6000	Linux 仮想配信エージェント(/ja-jp/linux-virtual-delivery-agent.html)
プロファイル管理	22.3.6000.7	プロファイル管理
Citrix フェデレーション認証サービス	10.9.6000.9	Citrix フェデレーション認証サービス (FAS)(/ja-jp/federated-authentication-service/2203-ltsr.html)

2203 CU6 ベースラインコンポーネント	プログラムと機能に表示されるバージョン	ドキュメント
ブラウザコンテンツリダイレクション	15.32.6000.9	「ブラウザコンテンツリダイレクション」(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/multimedia/browser-content-redirection.html)
シトリックス プローブ エージェント 2305	2305.1.0.0	ダウンロード

2203 LTSR CU6 互換コンポーネント

以下のコンポーネント（下記バージョン）は、LTSR環境と互換性があります。これらはLTSRのメリット（延長されたライフサイクルと修正のみの累積更新プログラム）の対象ではありません。Citrix®は、2203環境内でこれらのコンポーネントを新しいバージョンにアップグレードするよう求める場合があります。

互換性のあるコンポーネントと機能	プログラムと機能に表示されるバージョン	ドキュメント
アプリレイヤリング	2309	Citrix App Layering (Citrixアプリケーションレイヤリング)
HDX リアルタイム最適化パック	2.9.600	HDX RealTime Optimization Pack (HDX RealTime最適化パック)
ライセンスサーバー	11.17.2.0_Build 51000	ライセンスサーバー(/ja-jp/licensing/current-release.html)
ユーザーパーソナライゼーションレイヤー	24.9.0	ユーザーパーソナライゼーションレイヤー(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/install-configure/user-personalization-layer.html)
セッションレコーディングウェブプレーヤー	22.3.6000.11	セッションレコーディングWebプレーヤー(/ja-jp/session-recording/2203-ltsr/

互換性のあるコンポーネントと機能	プログラムと機能に表示されるバージョン	ドキュメント
		view-recordings/session-recording-web-player.html)
Microsoft Teamsの最適化	15.32.3000.9	Microsoft Teamsの最適化(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/multimedia/opt-ms-teams.html)
ワークスペース環境管理	22.12.0	ワークスペース環境管理
XenApp & XenDesktop 7.15 LTSR VDA (最新リリース)*	最新の累積更新プログラムのみ	ドキュメント

2203 LTSR CU6 の主な除外事項

以下の機能、コンポーネント、およびプラットフォームは、2203のライフサイクルマイルストーンおよびメリットの対象ではありません。具体的には、累積更新プログラムと延長されたライフサイクルメリットは除外されます。除外された機能およびコンポーネントの更新は、通常の最新リリースを通じて利用できます。

除外されるコンポーネントと機能
AppDisks™
AppDNA®
Citrix SCOM 管理パック
フレームホーク
パーソナル vDisk
StoreFront Citrix オンライン統合
ライセンスアクティベーションサービス

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

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

新機能

以下の新機能と機能強化は、Citrix Virtual Apps and Desktops™ 7 2203 LTSR Cumulative Update 6 (CU6) で利用可能です。

WBCディスクをOSディスクと同じストレージ場所に配置するサポート

2203 LTSR CU6リリース以降、XenServer®、VMware、SCVMM仮想化環境において、ホスト接続の作成時に利用可能なOSストレージリストを利用可能な一時ストレージリストと同じように構成した場合、MCSはライトバックキャッシュ (WBC) ディスクをOSディスクと同じストレージ場所に配置するようになりました。

この実装により、OSディスクとWBCディスクの管理の複雑さを軽減できます。ホスト接続の作成については、接続とリソースを参照してください。

修正された問題

Citrix Virtual Apps and Desktops™ 7 2203 LTSR CU5 以降、以下の問題が修正されています。

Citrix Director (シトリックス ディレクター)

- マルチフォレストサイトでマルチセッションまたはシングルセッションのデスクトップVDAを使用すると、ユーザー中心の検索機能が動作しません。
- Director 2203では、無効なスコープターゲットが原因で、ユーザーはデフォルトのスマートアラートポリシーを編集および保存できません。ターゲットIDがnullまたは無効な場合、ポリシーは正しく機能しますが、検証に失敗し、エラーメッセージが表示されます。
- カスタムレポートにアクセスできないという問題が発生する可能性があります。
- Enum値の欠落が原因で、Directorの > でマシンリストが表示されない場合があります。

Citrixポリシー

- CseEngine.exeプロセスで高いメモリ使用率が発生し、マシンの登録に関する問題を引き起こす可能性があります。

シトリックス スタジオ

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

- ブローカーアプリケーションの名前と公開名の両方が変更された場合、App-Vアプリケーションの詳細で「配信元」フィールドが空白になる場合があります。

デリバリーコントローラー™

- 組織名または必須名を使用する更新された証明書が原因で、VDAアップグレード中にVUA検証が失敗するという問題が発生する可能性があります。
- 監視SQLデータベースで頻繁なデッドロックが発生し、Citrixモニターサービスで高いCPUおよびメモリ使用率が観測される可能性があります。
- Citrix 2203 CU2でMachine Creation Services™ (MCS)に関する断続的な問題が発生する可能性があります。既存のカタログに追加しようとしたマシンの半分しか成功しません。マシンはActive Directoryに表示されますが、成功したマシンのみがStudioに表示され、失敗したマシンはActive Directoryから手動でインポートされるまでNutanixハイパーバイザーに表示されません。
- 数か月分のデータを保持する大規模なMonitorDBで高いCPU使用率が発生する可能性があります。インデックスを追加すると、CPU使用率を約10～15%削減できます。

グラフィック

- 作業中に約10秒間続く断続的な画面のブラックアウトが発生する可能性があり、その間、Citrixソフトウェアグラフィックプロセス (Ctxgfx.exe) がリセットされます。twencodeスレッドでアクセス違反例外が発生し、これによりctxExceptionHandlerがミニダンプを記録してこの問題を引き起こします。ctxExceptionHandlerは、調査のために完全なダンプを生成するように設定されています。
- オンプレミス版Director for CVAD 2203 LTSR CU2では、ブローカリングと「VM起動」のメトリックが常にN/Aと表示される場合があります。これは、起動を開始したときにのみVDAが起動するように構成されている場合に発生します。ログオンパフォーマンスデータをレビューしているときに、この問題に遭遇する可能性があります。
- 作業中に約10秒間続く断続的な画面のブラックアウトが発生する可能性があり、その間、Citrixソフトウェアグラフィックプロセス (Ctxgfx.exe) がリセットされます。twencodeスレッドでアクセス違反例外が発生し、これによりctxExceptionHandlerがミニダンプを記録してこの問題を引き起こします。ctxExceptionHandlerは、調査のために完全なダンプを生成するように設定されています。

メタインストーラー

- マネージドインスタンス（MI）の状態が欠落しているために再起動または再開が必要になる問題が発生する場合があります。これはVUAの機能に影響を与える可能性があります。

- CVAD 2203 CU5からアップグレードした後、Citrix Virtual Desktop Agentのインストールディレクトリからファイル`Microsoft.IdentityModel.Abstractions.dll`がありません。

ユニバーサル プリント サーバー

印刷

- Citrixセッションでプリンターが動作せず、印刷スプーラーのクラッシュにより複数のイベントID 1102および1106エラーが発生する問題が発生する場合があります。
- Citrix Print Management Serviceが断続的に終了し、リダイレクトされたプリンターが機能しなくなることがあります。

シングルセッションOS用VDA

- CVAD 2203にアップグレードした後、デスクトップを開く際に約10秒の遅延が発生する場合があります。
- Citrix Cloud™ VDAでCitrix Audio Redirectionサービスが失敗し、セッション中のオーディオ機能に影響を与える問題が発生する場合があります。

クリップボード

- VDA 2203 LTSR Cu4を使用しているときに、WebP形式のコンテンツをコピーして貼り付けると、`WfShell`が動作を停止します。
- VDAで大きな画像やExcelグラフのセッションクリップボードリダイレクトが失敗し、これらのアイテムをクライアント側にコピー＆ペーストできない問題が発生する場合があります。

セッション/接続

- 2203 CU4にアップグレードした後、セッションからログオフしたり、公開アプリケーションウィンドウを終了したりしても、VDAからクリアされるまでに2〜3分かかる問題が発生する場合があります。
- 初期セッション中にスプーラーサービスが再起動された場合、再接続後にクライアントマップされたプリンターが消えることがあります。同じクライアントから再接続すると、プリンターは表示されたままになります。

スマートカード

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

システム例外

- ショートカット「Windows + Print Screen」を使用すると、Virtual Delivery Agent (VDA) で「explorer.exe」プロセスがクラッシュする場合があります。
- CitrixセッションでWebRTCベースのアプリケーションでリダイレクトされたWebカメラからストリームを録画すると、画像の歪みが発生する場合があります。
- アクティブなセッションがない状態で、停止期間への移行中または停止期間からの移行中に、シングルセッションのランダムなマシンの電源オフが発生する場合があります。
- このリリースでは、32ビットWebアプリケーションでFIDO2サポートは利用できません。

マルチセッションOS用VDA

- Machine Creation Services (MCS) でプロビジョニングされたVirtual Delivery Agent (VDA) に再接続すると、アイドル状態の切断により登録解除され、DirectorでVDAが未登録として表示される場合があります。この問題は、非MCS VDAにも影響し、VDAがRDP経由で切断された場合や、RDPセッションでアイドル状態のままになった場合に発生します。
- Citrix Cloud VDAでCitrix Audio Redirectionサービスが失敗し、セッション中のオーディオ機能に影響を与える問題が発生する場合があります。
- ローミング中にオーディオアプリケーションでクラッシュが発生する場合があります。これは、icaendpoint.dllモジュールでのハングが原因です。
- VDA 2402またはVDA 2402 CU1を搭載したWindows 2022 OSで、公開された新しいMicrosoft Teamsアプリのシステムトレイアイコンがシームレスアプリケーションとして実行されているときに左クリックに応答しない問題が発生する場合があります。これはアプリが最小化されている場合にのみ発生し、フルデスクトップセッションでは正常に動作します。

クリップボード

- VDA 2203 LTSR Cu4を使用している場合、WebP形式のコンテンツをコピーして貼り付けると、`WfShell` が動作を停止します。
- VDAで、大きな画像やExcelグラフのセッションクリップボードリダイレクトが失敗し、これらの項目をクライアント側にコピー＆ペーストできない問題が発生する場合があります。

セッション/接続

- Auto Client Reconnect (ACR) が無効になっている場合、再接続するたびに「MetaFrame 9006」イベントがログに記録され、不要なエラーメッセージが多数生成されることに気づく場合があります。
- VDAがランダムに応答しなくなり、未登録状態になる問題が発生し、ユーザーがICAセッションから強制的に切断される場合があります。

- 2203 CU4にアップグレードした後、セッションからログオフしたり、公開されたアプリケーションウィンドウを終了したりすると、VDAからクリアされるまでに2〜3分かかる問題が発生する場合があります。
- ICAセッションではバッテリーアイコンが1つしか表示されないにもかかわらず、その他のシステムトレイアイコンリストにCitrix WinFrame Shell項目が増加していることに気づく場合があります。この蓄積は、システム設定の「個人用設定」>「タスクバー」>「その他のシステムトレイアイコン」で発生します。
- 初期セッション中にスプーラーサービスが再起動された場合、再接続後にクライアントマップされたプリンターが消えることがあります。同じクライアントから再接続した場合は、プリンターは表示されたままになります。

スマートカード

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

システム例外

- マルチセッション環境でビデオを再生する際に、Windows Mediaリダイレクトで問題が発生する可能性があります。
- Citrix VDAでTermServiceがクラッシュする可能性があります。
- VDAがバッテリーの状態を受信しているにもかかわらず、Windows 11マルチセッションVDAでバッテリーの状態が表示されない問題が発生する可能性があります。
- ライセンスの状態を読み取る際に、wdica32.exeでバグチェック0x50が発生する可能性があります。

シトリックス プロビジョニング™

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

リナックス ブイディーエー

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

プロファイル管理

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

セッション録画

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

StoreFront™

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

累積更新プログラム 5 (CU5)

リリース日: Jun 04, 2024

このリリースについて

Citrix Virtual Apps and Desktops™ 7 2203 LTSR Cumulative Update 5 (CU5) は、2203 LTSR CU4のリリース以降に報告された25を超える問題を修正しました。

2203 LTSR (一般情報)

2203 LTSR (機能とアップグレード情報)

このリリースの新機能

Citrix Virtual Apps and Desktops 7 2203 LTSR CU4で修正された問題

このリリースの既知の問題

非推奨と削除

Citrix 製品サブスクリプションアドバンテージの対象期間

ダウンロード

シトリックス バーチャル アプリケーションズ アンド デスクトップ 7 2203 LTSR CU5

新規展開

CU5をゼロから展開する方法?

CU5メタインストーラーを使用して、CU5に基づいて新しいCitrix Virtual Apps and Desktops環境をセットアップできます。その前に、製品についてよく理解しておくことをお勧めします:

Citrix Virtual Apps and Desktops 7 2203 LTSR (初期リリース)セクションを熟読し、展開を計画し始める前に、技術概要、インストールと構成、およびセキュリティセクションに細心の注意を払ってください。セットアップがすべてのコンポーネントのシステム要件を満たしていることを確認してください。

既存の展開

何を更新しますか?

CU5は、2203 LTSRの15のベースラインコンポーネントに更新を提供します。注意: Citrixは、展開のすべてのLTSRコンポーネントをCU5に更新することを推奨しています。例: Citrix ProvisioningがLTSR展開の一部である場合、Citrix Provisioningコンポーネントを CU4に更新してください。Citrix Provisioningが展開の一部でない場合、インストールまたは更新する必要はありません。

2203 LTSR CU5 ベースラインコンポーネント

2203 CU5 ベースラインコンポーネント	プログラムと機能に表示されるバージョン	ドキュメント
シングルセッションVDA	2203.0.5000.5310	シングルセッションVDA
マルチセッションVDA	2203.0.5000.5310	マルチセッションVDA
デリバリーコントローラー	2203.0.5000.5310	デリバリーコントローラー
シトリックス スタジオ	7.33.5000.17	シトリックス スタジオ
Citrix Director (シトリックス ディレクター)	7.33.5000.16	シトリックス ディレクター
Citrixグループポリシー管理	7.33.5000.10	Citrixグループポリシー管理
Citrixグループポリシー クライアント側拡張	7.33.5000.9	
シトリックス ストアフロント	2203.0.5000.6	Citrix ストアフロント
シトリックス プロビジョニング	7.33.40	Citrix プロビジョニング
ユニバーサル プリント サーバー	7.33.5000.8	「ユニバーサルプリントサーバー」(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/

2203 CU5 ベースラインコンポーネント	プログラムと機能に表示されるバージョン	ドキュメント
		printing/printing-provision-printers.html)
セッション録画	22.3.5000	セッションレコーディング
リナックス ブイディーエー	22.03.5000	Linux 仮想配信エージェント(/ja-jp/linux-virtual-delivery-agent.html)
プロファイル管理	22.3.5000.2	プロファイル管理
Citrix フェデレーション認証サービス	10.9.5000.8	Citrix フェデレーション認証サービス (FAS)(/ja-jp/federated-authentication-service/2203-ltsr.html)
ブラウザコンテンツリダイレクション	15.32.5000.7	「ブラウザコンテンツリダイレクション」(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/multimedia/browser-content-redirection.html)
シトリックス プローブエージェント 2305	2305.1.0.0	ダウンロード

2203 LTSR CU5 互換コンポーネント

以下のコンポーネント（下記バージョン）は、LTSR環境と互換性があります。これらはLTSRのメリット（延長されたライフサイクルと修正のみの累積更新プログラム）の対象ではありません。Citrix®は、2203環境内でこれらのコンポーネントを新しいバージョンにアップグレードするよう求める場合があります。

互換性のあるコンポーネントと機能	プログラムと機能に表示されるバージョン	ドキュメント
アプリレイヤリング	2309	Citrix App Layering (Citrixアプリケーションレイヤリング)

互換性のあるコンポーネントと機能	プログラムと機能に表示されるバージョン	ドキュメント
HDX リアルタイム最適化パック	2.9.600	HDX RealTime Optimization Pack (HDX RealTime最適化パック)
ライセンスサーバー	11.17.2.0_BUILD_47000	ライセンスサーバー(/ja-jp/licensing/current-release.html)
ユーザーパーソナライゼーションレイヤー	24.3.2	ユーザーパーソナライゼーションレイヤー(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/install-configure/user-personalization-layer.html)
セッションレコーディングウェブプレーヤー	22.3.5000.2	セッションレコーディングWebプレーヤー(/ja-jp/session-recording/2203-ltsr/view-recordings/session-recording-web-player.html)
Microsoft Teamsの最適化	15.32.3000.9	Microsoft Teamsの最適化(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/multimedia/opt-ms-teams.html)
ワークスペース環境管理	22.12.0	ワークスペース環境管理
XenApp & XenDesktop 7.15 LTSR VDA (最新リリース)*	最新の累積更新プログラムのみ	ドキュメント

2203 LTSR CU5 主な除外事項

以下の機能、コンポーネント、およびプラットフォームは、2203ライフサイクルマイルストーンおよび特典の対象外です。具体的には、累積更新プログラムと拡張ライフサイクル特典は除外されます。除外された機能およびコンポーネントの更新は、通常の現在のリリースを通じて利用できます。

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

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

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

新機能

Citrix Virtual Apps and Desktops™ 7 2203 LTSR Cumulative Update 5 (CU5) には、新機能および機能強化はありません。

修正された問題

Citrix Virtual Apps and Desktops™ 7 2203 LTSR CU4 以降、以下の問題が修正されました:

Citrix Director (シトリックス ディレクター)

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

Citrixポリシー

- Windows 11マルチセッションマシンにStudioをインストールし、グループポリシー管理コンソールを開くと、Citrixグループポリシーモジュールをロードする際に以下のエラーメッセージが表示されます。 `ERROR_CODE: (NTSTATUS) 0xc0000005 - The instruction at 0x%p referenced memory at 0x%p. The memory could not be %s.`

- Citrix Studioは、**ポリシー**タブの「割り当て先」の名前ではなく、デリバリーグループ`uuid`を誤って表示します。

シトリックス スタジオ

- Studioを公開アプリケーションとして使用する場合、またはICA®セッション下の公開VDAで使用する場合、Studioコンソールがフリーズすることがあります。
- Citrix Studioを介してStoreFront™サーバーアドレスを追加し、それをデリバリーグループに割り当てると、ストアはデフォルトでオフに設定されます。

デリバリーコントローラー™

- アベイラビリティゾーンBではマシンカタログの作成/更新タスクが失敗しますが、アベイラビリティゾーンAおよびCでは正常に動作します。これは、クラウド接続でボリュームサービスインスタンスを起動できなかったためです。SQLサーバーで新しいVolumeWorkerTemplateを使用するようにサイトデータベーステーブルを更新するには、以下のコマンドを実行してください。`UPDATE HostingUnitServiceSchema.VolumeServiceConfigurationBaseTemplate SET TemplateId = 'ami-09b42976632b27e9b' WHERE RegionName = 'ap-southeast-2'`

> **注：**
>
> アベイラビリティゾーンは、お客様によって異なる場合があります。

- ハイパーバイザーの再起動後、ピーク時の電源管理が構成されているため、VMが起動しません。
- パスワードフィールドが空の場合、公開リソースの列挙に失敗することがあります。

グラフィック

- Citrix Virtual Apps and Desktops 2203を使用している場合、切断されたセッションに再接続する際にブラックスクリーンが表示されることがあります。

メタインストーラー

- Windows 10でVDAバージョン2203 CU3を使用する場合、Rendezvous Proxyが構成されていると、VDAインストーラーはカスタムWCFポートをホストしません。
- Citrix Virtual Apps and Desktopsをバージョン1912 LTSRからバージョン2305または2203 LTSRにアップグレードしようとすると、「サポートされていない構成が検出されました」というエラーメッセージが表示されて失敗することがあります。

Microsoft Teamsの最適化

- Microsoft Teams 2.1 は、VDA 上でデフォルトでは最適化されていません。

モニター

- 監視データベースの `MonitorData.ResourceUtilization` テーブルの更新が遅延します。

ユニバーサル プリント サーバー

印刷

- プリンターのセキュリティ権限からEveryoneグループを削除すると、Citrix Universal™ Print Serverが期待どおりに動作しない場合があります。
- Knowledge Centerの記事CTX140208に記載されているとおりにインストールされたHP Color LaserJet 2800 Series PSドライバーが、VDAのアップグレード中にアンインストールされる場合があります。
- VDAバージョン1912 CU5とOSバージョン2012 R2を使用している場合、本番環境のCitrix UPSプリントサーバーからさまざまな印刷ジョブが次のエラーメッセージとともに失敗します: `CCgpStream::Open: WaitForMultipleObjects time out.` `InternalUpcRemoteOpenStream: Failed to Open Stream. Abort Job.`
- Citrix Virtual Apps and DesktopsバージョンまたはでUPSバージョンまたはをWindows 10 VDAとともに使用すると、CUPSを使用するプリンターに次のメッセージが表示されます:

  `Access Denied, cannot connect message`

シングルセッションOS用VDA

キーボード

- VDA LTSR 2203のCitrixセッションにローカルワークステーションからファイルをコピー＆ペーストすると、`Wfshell.exe` プロセスがクラッシュする場合があります。
- 公開されたリモートアプリのクリップボードへのコピーオプションが、CU3およびCU4バージョンで機能しません。

セッション/接続

- うるう日にVDAを再起動した後、`WebSocketService.exe` プロセスが起動に失敗します。
- Windows 10 VDAバージョン2308を使用すると、`ctxappvservice.exe` プロセスがクラッシュする場合があります。

- Citrix VDAバージョンLTSR 1912 CU3以降を使用し、システムに接続された接続があり、接続されているユーザー数が多いほど発生する可能性が高い場合、Citrix HDX™ HTML5 Videoがクラッシュする場合があります。
- ICAセッションの再接続中に、サードパーティ製メッセージングアプリケーションのチャットウィンドウが自動的にフォアグラウンドに表示される場合があります。
- マシンを使用すると、ユーザーセッションの起動が断続的に失敗します。
- Citrix Workspace™ Appバージョン2210または2303がインストールされたWindows 10エンドポイントから、VDA 2203 CU3がインストールされたWindows 10に接続すると、WebRTCアプリケーションでカメラを選択しようとしたときにセッションが切断されます。
- IPv6が有効になっている場合、VDAが断続的に登録解除されることがあります。
- スマートカードを使用してCitrix Virtual Apps and Desktopsバージョン2203 LTSR CU2のVDAセッションに再接続しようとすると、ようこそ画面で停止する場合があります。
- 仮想デスクトップ（Windows 10マルチセッション）を起動し、イヤホンを接続すると、システムオーディオの音量を調整している間にUACサウンドに大幅な遅延が発生します。
- 公開されたMicrosoft Visioまたはデスクトップ上のVisioアプリからユーザーデバイス上のアプリにコンテンツをコピーすると、失敗する場合があります。
- 英語以外のオペレーティングシステムでCitrix HDX 3D Pro警告ダイアログに表示されるメッセージが破損して表示される場合があります。
- バージョン2203 LTSR CU2を実行し、Microsoft Defender Application Controlがインストールされているに接続するセッションを開始すると、数秒間グレースクリーンが表示される場合があります。
- リモートPCアクセスでは、「Citrix-HostCore-ICA Service/Admin」に一部のイベントがログに記録されます。**Ctrl+Alt+Del**を使用してセッションが切断された場合、イベントID 43と46がログに記録されました。英語OSのVDAでは期待どおりに動作しましたが、日本語OSのVDAではイベントID 37から50が「Citrix-HostCore-ICA Service」にログに記録されませんでした。
- ブラウザサービスは、エンドポイントで`ctxcsb`が利用可能かどうかを確認し、利用できない場合はGVCHを介したBCR機能交換を尊重し、その機能をオフにします。
- ExcelまたはWordでMicrosoftアカウントを使用してサインインし、特殊フォルダーリダイレクトが有効になっている場合、ExcelまたはWord 365は`sfrhook.dll`で、開いて数文字入力した後にクラッシュします。特殊フォルダーリダイレクトが無効になっている場合、この問題は発生しません。
- ACR再接続後、ターミナルサービスプロセスがクラッシュする場合があります。
- SFCRモードでブラウザコンテンツリダイレクトを設定すると、BCRウェブページがページ全体を読み込めない場合があります。

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

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

- Virtual Apps and Desktops 2203 LTSR、Citrix Workspace app 2203 LTSR CU3 (2303または2205)、およびWindows 11 22h2を搭載したVDA 2203 LTSRを使用している場合、再接続後に左モニターの左半分に設定されたアプリケーションが画面中央に誤って表示されます。
- プリンターまたはプリントサーバーに到達できない場合、セッションのログオンとログオフに時間がかかることがあります。

システム例外

- VDAを使用すると、picadd.sysで致命的な例外が発生し、バグチェックコード0x96のブルースクリーンが表示されることがあります。これはすべてのオペレーティングシステムに適用されます。
- VDAバージョンLTSR 2203 CU 4.1を使用している場合、セッションの開始時またはセッション中にいつでも、VDAがメッセージ`Error "StopCode: SYSTEM THREAD EXCEPTION NOT HANDLED: Tdica.sys`とともにバグチェックを実行する可能性があります。

マルチセッションOS用VDA

キーボード/マウス

- Windows Server 2022では、アプリまたはOSによってマウスが特定の場所に移動された場合、アプリまたはOSによってマウスが別の場所に移動されるまで、その場所にマウスを再度移動することはできません。
- 公開されたリモートアプリのクリップボードへのコピーオプションが、CU3およびCU4バージョンで機能しません。

セッション/接続

- うるう日にVDAを再起動した後、`WebSocketService.exe`プロセスが起動に失敗します。
- セッションアイドル時間制限が有効になっているにもかかわらず、2022 OS VDAのICAセッションで「Warning Idle Time Expired Message」ダイアログボックスが表示されません。
- Server 2019 VDAバージョンLTSR 2203 CU3で、`WmiPrvSE.exe`がクラッシュします。
- Citrix VDAバージョンLTSR 1912 CU3以降を使用し、システムに接続があり、接続されているユーザー数が多いほど発生する可能性が高い場合、Citrix HDX HTML5 Videoがクラッシュする可能性があります。

- 公開されたアプリケーションセッションで実行されている場合、Citrix Workspaceアプリの一部のプロセスが期待どおりに終了しないことがあります。
- ACR再接続後、ターミナルサービスプロセスがクラッシュする可能性があります。
- SFCRモードでブラウザコンテンツリダイレクトを設定すると、BCRウェブページがページ全体を読み込めない場合があります。
- **OpenTEXT ETX**アプリケーションは、以下のモジュールでアクセス違反が発生するため、開くことができません。

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

- プリンターまたはプリントサーバーに到達できない場合、セッションのログオンとログオフの応答に時間がかかることがあります。
- WebSocketService (HTML5 Video Redirection WebSocker Service) がクラッシュする可能性があります。

システム例外

- VDAを使用すると、picadd.sysで致命的な例外が発生し、バグチェックコード0x96のブルースクリーンが表示されることがあります。これはすべてのオペレーティングシステムに適用されます。
- VDAバージョンLTSR 2203 CU 4.1を使用すると、セッションの開始時またはセッション中にいつでも、VDAがメッセージ `Error "StopCode: SYSTEM THREAD EXCEPTION NOT HANDLED: Tdica.sys` でバグチェックを実行する可能性があります。

シトリックス プロビジョニング™

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

リナックス ブイディーエー

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

プロファイル管理

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

セッション録画

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

StoreFront

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

累積更新プログラム 4 (CU4)

リリース日: November 16, 2023

このリリースについて

Citrix Virtual Apps and Desktops™ 7 2203 LTSR Cumulative Update 4 (CU4) は、2203 LTSR CU3 のリリース以降に報告された 60 を超える問題を修正します。

2203 LTSR (一般情報)

2203 LTSR (機能とアップグレード情報)

このリリースの新機能

Citrix Virtual Apps and Desktops 7 2203 LTSR CU3 で修正された問題

このリリースの既知の問題

非推奨と削除

Citrix 製品サブスクリプションアドバンテージの対象期間

ダウンロード

シトリックス バーチャル アプリケーションズ アンド デスクトップス 7 2203 LTSR CU4

新規展開

CU4 をゼロから展開するにはどうすればよいですか?

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

展開を計画する前に、Citrix Virtual Apps and Desktops 7 2203 LTSR (初期リリース) セクションを熟読し、技術概要、インストールと構成、および セキュリティ の各セクションに細心の注意を払ってください。セットアップがすべてのコンポーネントのシステム要件を満たしていることを確認してください。

既存の展開

何を更新しますか?

CU4 は、2203 LTSR の 15 のベースラインコンポーネントに更新を提供します。注意: Citrix は、展開のすべての LTSR コンポーネントを CU4 に更新することを推奨しています。例: Citrix Provisioning が LTSR 展開の一部である場合、Citrix Provisioning コンポーネントを CU4 に更新してください。Citrix Provisioning が展開の一部でない場合、インストールまたは更新する必要はありません。

2203 LTSR CU4 ベースラインコンポーネント

2203 CU4 ベースラインコンポーネント	プログラムと機能に表示されるバージョン	ドキュメント
シングルセッションVDA	2203.0.4000.4310	シングルセッションVDA
マルチセッションVDA	2203.0.4000.4310	マルチセッションVDA
デリバリーコントローラー	2203.0.4000.4310	デリバリーコントローラー
シトリックス スタジオ	7.33.4000.15	シトリックス スタジオ
Citrix Director (シトリックス ディレクター)	7.33.4000.26	シトリックス ディレクター
Citrixグループポリシー管理	7.33.4000.2	Citrixグループポリシー管理
Citrixグループポリシー クライアント側拡張	7.33.4000.5	
シトリックス ストアフロント	2203.0.4000.13	Citrix ストアフロント
シトリックス プロビジョニング	7.33.40	Citrix プロビジョニング
ユニバーサル プリント サーバー	7.33.4000.11	「ユニバーサルプリントサーバー」(/ja-jp/citrix-virtual-

2203 CU4 ベースラインコンポーネント	プログラムと機能に表示されるバージョン	ドキュメント
		apps-desktops/2203-ltsr/printing/printing-provision-printers.html)
セッション録画	22.3.4000	セッションレコーディング
リナックス ブイディーエー	22.03.3000.6	Linux 仮想配信エージェント(/ja-jp/linux-virtual-delivery-agent.html)
プロファイル管理	22.3.4000.7	プロファイル管理
Citrix フェデレーション認証サービス	10.9.4000.6	Citrix フェデレーション認証サービス (FAS)(/ja-jp/federated-authentication-service/2203-ltsr.html)
ブラウザコンテンツリダイレクション	15.32.4000.12	「ブラウザコンテンツリダイレクション」(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/multimedia/browser-content-redirection.html)
Citrix プローブエージェント 2305	2305.1.0.0	ダウンロード

2203 LTSR CU4 互換コンポーネント

以下のコンポーネントは、以下のバージョンでLTSR環境と互換性があります。これらはLTSRのメリット（延長されたライフサイクルと修正のみの累積更新プログラム）の対象ではありません。Citrix®は、2203環境内でこれらのコンポーネントを新しいバージョンにアップグレードするよう求める場合があります。

互換性のあるコンポーネントと機能	プログラムと機能に表示されるバージョン	ドキュメント
アプリレイヤリング	2309	Citrix App Layering (Citrixアプリケーションレイヤリング)

互換性のあるコンポーネントと機能	プログラムと機能に表示されるバージョン	ドキュメント
HDX リアルタイム最適化パック	2.9.600	HDX RealTime Optimization Pack (HDX RealTime最適化パック)
ライセンスサーバー	11.17.2.0_BUILD_44000	ライセンスサーバー(/ja-jp/licensing/current-release.html)
ユーザーパーソナライゼーションレイヤー	23.9.1	ユーザーパーソナライゼーションレイヤー(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/install-configure/user-personalization-layer.html)
セッションレコーディングウェブプレーヤー	22.3.4000.4	セッションレコーディングWebプレーヤー(/ja-jp/session-recording/2203-ltsr/view-recordings/session-recording-web-player.html)
Microsoft Teamsの最適化	15.32.3000.9	Microsoft Teamsの最適化(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/multimedia/opt-ms-teams.html)
ワークスペース環境管理	22.12.0	ワークスペース環境管理
XenApp & XenDesktop 7.15 LTSR VDA (最新リリース)*	最新の累積更新プログラムのみ	ドキュメント

2203 LTSR CU4 の主な除外事項

以下の機能、コンポーネント、およびプラットフォームは、2203 ライフサイクルマイルストーンおよび特典の対象ではありません。具体的には、累積更新プログラムと拡張ライフサイクル特典は除外されます。除外された機能およびコンポーネントの更新プログラムは、通常の最新リリースを通じて利用できます。

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

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

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

新機能

Citrix Virtual Apps and Desktops 7 2203 LTSR Cumulative Update 4 (CU4) には、新機能や機能強化はありません。

修正された問題

2203 LTSR Cumulative Update 4 (CU4) Update 1 の修正された問題

シングルセッションおよびマルチセッションOS用VDA

システム例外

- VDAでpicadd.sysに致命的な例外が発生し、以下のエラーメッセージとともにブルースクリーンが表示されることがあります。

  エラー: バグチェック 0x96 INVALID_WORK_QUEUE_IT

> **注：**

> この修正は、CU4 Update 1 Minimalインストーラーでのみ利用可能です。

2203 LTSR Cumulative Update 4 (CU4) で修正された問題

Citrix Virtual Apps and Desktops™ 7 2203 LTSR CU3 以降、以下の問題が修正されました。

Citrix Director (シトリックス ディレクター)

- **Citrix Director コンソール > トレンド > ロード評価インデックス** にメモリ使用量が表示されない場合があります。
- Citrix Directorで、**Director コンソール > トレンド > マシン使用状況 > マルチセッションOSマシン** のマシン使用量が、すべてのデリバリーグループの「使用中」列に0（ゼロ）と表示されます。

Citrixポリシー

- HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\VCPolicies 設定の仮想チャネルポリシー値 **VirtualChannelWhiteList** が破損し、再起動後にVDAに適用されない場合があります。この問題は、C:\ProgramData\Citrix\GroupPolicy フォルダーからファイルを削除したり、フォルダー内のコンテンツを切り取って別の場所に貼り付けたりすると発生します。
- グループポリシーモデリング値が、実際の値ではなく無効な値として表示されます。たとえば、**メモリ単位の表示** の値が、実際の値である65536 KBではなく、無効として表示されます。
- VDAをLTSR CU7バージョンにアップグレードすると、異なるドメインにCitrixユーザーポリシーを適用しようとすると失敗する場合があります。
- **Citrix グループポリシーモデリングウィザード** からユーザーを選択し、**追加データを収集せずにウィザードの最終ページにスキップする** オプションを選択すると、**概要** ページに次のエラーメッセージが表示されることがあります。

  値はnullにできません。

  パラメーター名キー

- プロファイルのリセット後、フォルダーのリダイレクトが断続的に失敗する場合があります。

シトリックス スタジオ

- Citrix Studioのログビューにデータが表示されない場合があります。

デリバリーコントローラー™

- 特定のCitrix XMLパフォーマンスカウンターが、パフォーマンスモニターグラフに追加されない場合があります。
- XenServer®プールマスターで新しいホスティング接続を作成しようとすると、次のエラーメッセージが表示されて失敗する場合があります。

  ホストサーバーに接続できません。接続に有効なホストアドレスがあり、ホストサーバーの電源がオンになっていて正常に動作していることを確認してください。

  XenServerホストリストの取得に失敗しました。

- VDAが登録に失敗し、セッション数が-1と表示されたまま初期化状態から抜け出せなくなる場合があります。
- Microsoft Windows 11を実行している永続VDAがパスワードをリセットすると、VDAにログオンできない場合があります。イベントログにドメイントラスト関係の失敗エラーメッセージが30日ごとに表示される場合があります。
- AWSマシンカタログの作成中に、対応する準備仮想マシンが終了および削除された後でも、prepare-identityボリュームが自動的に削除されない場合があります。
- この修正により、Machine Creation Services™はvSAN 8をサポートします。

メタインストーラー

- **Enable connections to a server machine**オプションを有効にしてマルチセッションOS用VDAをインストールし、VDAをアップグレードすると、アップグレードウィザードに**Additional Components for Enable Brokered Connections to a Server**ではなく**Additional Components for Master MCS Image**というテキストが表示されます。

  > **注：**
  >
  > この修正は、Citrix Virtual Apps and Desktops 1912 LTSR CU8以降に適用され、1912 LTSR CUから1912 LTSR CU8以降へのアップグレードに適用されます。ただし、この修正はXenApp and XenDesktop 7.15 LTSR CUおよびXenApp and XenDesktop 7.15 LTSRからCitrix Virtual Apps and Desktops 1912 LTSR CUへのアップグレードには適用されません。

ユニバーサル プリント サーバー

クライアント

- Citrix Universal™ Print Serverを使用してファイルを印刷中に、印刷スプーラーサービスが予期せず終了する場合があります。

シングルセッションOS用VDA

インストール、アンインストール、アップグレード

- Citrix Virtual Apps and Desktops 2203 LTSRをCU1からCU2にアップグレードすると、以下のレジストリキーの下に手動で作成された値 **EnableVistaMousePointers**、**EnforceUserPolicyEvaluationSuccess**、**Flag**、および **CitrixDoD** が消える可能性があります。
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

    名前: `EnableVistaMousePointers`

    種類: DWORD

    値: 1
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Ica\GroupPolicy`

    名前: `EnforceUserPolicyEvaluationSuccess`

    種類: DWORD

    データ: 0
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\Smart Card Hook`

    名前: `Flag`

    種類: DWORD

    値: 0
  - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits

    名前: `CitrixDoD`

    種類: DWORD

    値: 0

- VDAを1912 LTSR CUxまたは2203 LTSR CUxにアップグレードした後、レジストリキーHKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI の下の**ApplicationLaunchWaitTimeoutMS** の値が復元されない可能性があります。

キーボード

- 英国や米国などのキーボードレイアウトを切り替えると、セッション内のキーボードで断続的な言語の問題が発生する可能性があります。
- VDAバージョン2203 LTSR CU3以前のUbuntuでCitrix Workspace™アプリを使用すると、キーボードレイアウトの同期が正しく機能しない可能性があります。たとえば、ユーザーがローカルおよびサーバー側のキーボードレイアウトを英語からドイツ語に変更した場合、両方のキーボードがドイツ語レイアウトであっても、キーボードが誤った文字出力を表示する可能性があります。

印刷

- Universal Print Serverポリシーが有効なVDAを再起動すると、Universal Print Serverの負荷分散が開始に失敗する可能性があります。
- 初回起動時にローカルプリンターがセッションにリダイレクトされない可能性があります。ただし、その後の起動時にはローカルプリンターがリダイレクトされます。

セッション/接続

- `servervdi` コマンドラインパラメーターを使用してVirtual Delivery Agentをインストールすると、Windowsオーディオサービスが自動的に開始されない可能性があります。このエラーメッセージが通知領域に表示されます。

  オーディオサービスが実行されていません。

- システムが起動するまで、Cloud StudioまたはMonitorでセッションが**ログオフ**状態のままになる可能性があります。この問題は、RemotePC内からRemotePC VDAがシャットダウンされたときに発生します。
- クリップボードマッピングを使用してセッション1からコンテンツをコピーし、セッション2に貼り付けようとすると、セッション2のクリップボードにコンテンツが表示されない可能性があります。この問題は、セッション1からコンテンツがコピーされた後にセッション2が起動されたときに発生します。
- VDAをバージョン2203にアップグレードした後、Skype for Businessアプリが起動時にスプラッシュ画面を表示し、応答しなくなる可能性があります。

- Citrix Print Manager Serviceが無効になっている場合、Microsoft Windows Serverで実行されている新規インストールされたVDAバージョン2203 LTSR CU2では、クライアントドライブマッピング（CDM）が機能しない可能性があります。
- VDAでShellbridge機能が有効になっている場合、HTML5およびAndroidからのシームレスアプリケーションセッションで、ユーザー入力をブロックする可能性のある予期しないUIウィンドウが表示されることがあります。
- レジストリキー HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy の下の値 **SaveRsopToFile**、**SaveRsopToMemory**、および **SaveRsopToRegistry** が復元されない可能性があります。
- Citrix Audio Redirection は、ユーザーデバイスに 8 台を超えるオーディオデバイスが接続されている場合、VDA バージョン 2203 LTSR CU3 で動作しないことがあります。
- macOS Ventura を実行している Mac 用 Citrix Workspace アプリで、Web カメラのリダイレクトが失敗する場合があります。
- VDA をバージョン 2203 LTSR CU3 にアップグレードした後、カスタム ICA® ファイルでアプリケーションを起動しようとすると失敗する場合があります。
- VDA に Session Recording エージェントがインストールされておらず、**Get-BrokerSessionRecordingStatus**、**Start-BrokerSessionRecording**、**Stop-BrokerSessionRecording** の PowerShell コマンドを実行すると、VDA は数秒以内に Delivery Controller から登録解除され、再度登録されます。この操作は既存のセッションには影響しません。Session Recording エージェントが VDA にインストールされている場合、PowerShell コマンドは問題なく動作します。

スマートカード

- スマートカードを使用してセッションを開始し、ロックされたセッションのロックを解除しようとすると、スマートカードの PIN の代わりにパスワードの入力を求めるプロンプトが表示される場合があります。この問題は、Microsoft のパッチ KB5018410 をインストールしている場合に発生します。
- VDA からログオフすると、CtxSvcHost (CtxSmartCardSvc) が予期せず終了する場合があります。

システム例外

- VDA がインストールされている特定のサードパーティアプリケーションの内部 Web サイトでは、プロンプトなしでアクセスが許可されない場合があります。
- Citrix PDF Universal Printer ドライバーは、障害のある acfpdfuamd64.dll モジュールが原因で予期せず終了する場合があります。
- wfica32.exe プロセスが予期せず終了する場合があります。

- VDA は Wdica.sys で致命的な例外を経験し、ブルースクリーンを表示する場合があります。
- Citrix ソフトウェアグラフィックプロセス (Ctxgfx.exe) は、セッション内の利用可能なすべてのメモリを常に消費し、最終的にセッションが切断される原因となる場合があります。
- グラフィックステータスインジケータープロセス GfxStatusIndicator.exe が繰り返し終了する場合があります。
- VDA をバージョン 2203 LTSR CU2 から CU3 にアップグレードした後、VDA は picadm.sys で致命的な例外を経験し、ブルースクリーンを表示する場合があります。

ユーザーエクスペリエンス

- Microsoft Excel で大量のデータをコピー＆ペーストしている間、wfshell.exe プロセスが応答しなくなる場合があります。

マルチセッションOS用VDA

キーボード

- VDAをバージョン2305またはバージョン2203 LTSR CU3にアップグレードした後、ショートカットキーの組み合わせが正しく機能しない場合があります。たとえば、Word文書で選択した単語に対して**Ctrl+Shift+K**キーを押すと、大文字になります。しかし、**K**キーを離してもう一度押しても、変更は元に戻りません。
- UbuntuでVDAバージョン2203 LTSR CU3以前のCitrix Workspaceアプリを使用すると、キーボードレイアウトの同期が正しく機能しない場合があります。たとえば、ユーザーがローカルおよびサーバー側のキーボードレイアウトを英語からドイツ語に変更した場合、両方のキーボードがドイツ語レイアウトであっても、キーボードが誤った文字出力を表示する可能性があります。

印刷

- Universal Print Serverポリシーが有効なVDAを再起動すると、Universal Print Serverの負荷分散が開始に失敗する場合があります。
- 初回起動時にローカルプリンターがセッションにリダイレクトされない場合があります。ただし、それ以降の起動時にはローカルプリンターはリダイレクトされます。

セッション/接続

- システムが起動するまで、セッションがCloud StudioまたはMonitorで「ログオフ中」の状態のままになる場合があります。この問題は、RemotePC VDAがRemotePC内からシャットダウンされたときに発生します。
- CitrixサーバーでAdobe Acrobat Reader DCを使用してPDFファイルを開こうとすると、次のエラーメッセージが表示されて失敗する場合があります。

Werfault.exe - アプリケーションエラー

アプリケーションを正しく起動できませんでした (0xc0000142)。をクリックしてアプリケーションを閉じてください。

- セッションからログオフした後や、セッションが切断された後でも、セッションレコーディングが記録を継続する場合があります。
- セッションを切断せずにエンドポイントを切り替えると、スケジュールされた再起動通知が有効になっている場合、複数の再起動通知が表示される場合があります。
- アプリケーションの2つのインスタンスを開き、**DisableToggler**設定を5秒に設定すると、2番目のアプリケーションで入力できるようになるまで、約30秒待つ必要がある場合があります。
- クリップボードマッピングを使用してセッション1からコンテンツをコピーし、セッション2に貼り付けようとすると、セッション2のクリップボードにコンテンツが表示されない場合があります。この問題は、セッション1からコンテンツがコピーされた後にセッション2が起動されたときに発生します。
- VDAをバージョン2203にアップグレードした後、Skype for Businessアプリが起動時にスプラッシュ画面を表示し、応答しなくなる場合があります。
- クライアントのDPI値を変更した後でセッションに再接続すると、新しい値がセッションに適用されない場合があります。
- VDAをバージョン2203 LTSR CU2にアップグレードした後、VDAが登録解除される場合があります。
- VDAをバージョン2203 LTSR CU3にアップグレードした後、カスタムICAファイルでアプリケーションを起動しようとすると失敗する可能性があります。
- macOS Venturaを実行しているCitrix Workspaceアプリ for Macで、Webカメラのリダイレクトが失敗する可能性があります。
- shellbridgeが有効になっている場合、ウィンドウの**X**アイコンをクリックしてセッションからログオフできない可能性があります。
- この修正により、シームレスセッションでトースト通知が正しく表示される可能性があります。この修正を機能させるには、shellbridgeを有効にする必要があります。ただし、この修正には以下の視覚的な制限があります。
  - 黒い背景がトースト通知を囲みます。
  - トースト通知がローカルタスクバーの一部を覆います。

スマートカード

- スマートカードを使用してセッションを開始し、ロックされたセッションのロックを解除しようとすると、スマートカードのPINの代わりにパスワードの入力を求めるプロンプトが表示されることがあります。この問題は、MicrosoftパッチKB5018410をインストールしている場合に発生します。
- VDAからログオフするときに、CtxSvcHost (CtxSmartCardSvc) が予期せず終了する可能性があります。

システム例外

- 障害のあるacfpdfuamd64.dllモジュールが原因で、Citrix PDFユニバーサルプリンタードライバーが予期せず終了する可能性があります。
- wfica32.exeプロセスが予期せず終了する可能性があります。
- VDAでWdica.sysに致命的な例外が発生し、ブルースクリーンが表示される可能性があります。
- Microsoft Teamsの使用中に、Citrix HDX HTML5ビデオリダイレクトサービス (WebSocketService.exe) が予期せず終了する可能性があります。
- VDAをバージョン2203 LTSR CU2からCU3にアップグレードした後、VDAでpicadm.sysに致命的な例外が発生し、ブルースクリーンが表示される可能性があります。

ユーザーエクスペリエンス

- Microsoft Excelで大量のデータをコピーアンドペーストしているときに、wfshell.exeプロセスが応答しなくなる可能性があります。

ユーザーインターフェイス

- Windows Serverバージョン2019以前では、VDAがマウスイベントをエンドポイントに送信できず、アプリケーションでグラフィックまたはマウスの問題が発生する可能性があります。

シトリックス プロビジョニング™

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

リナックス ブイディーエー

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

プロファイル管理

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

セッション録画

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

StoreFront™

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

累積更新プログラム 3 (CU3)

リリース日: June 1, 2023

このリリースについて

Citrix Virtual Apps and Desktops™ 7 2203 LTSR Cumulative Update 3 (CU3) は、2203 LTSR CU2 のリリース以降に報告された 60 を超える問題を修正します。

2203 LTSR (一般情報)

2203 LTSR (機能とアップグレード情報)

このリリースの新機能

Citrix Virtual Apps and Desktops 7 2203 LTSR CU2 で修正された問題

このリリースの既知の問題

非推奨と削除

Citrix 製品の Subscription Advantage 資格日

ダウンロード

Citrix Virtual Apps and Desktops 7 2203 LTSR 累積更新プログラム 3

新規展開

CU3 をゼロから展開するにはどうすればよいですか?

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

展開を計画する前に、Citrix Virtual Apps and Desktops 7 2203 LTSR (初期リリース) セクションを熟読し、技術概要、インストールと構成、および セキュリティ の各セクションに細心の注意を払ってください。すべてのコンポーネントについて、セットアップがシステム要件を満たしていることを確認してください。

既存の展開

何を更新しますか?

CU3 は、2203 LTSR の 15 のベースラインコンポーネントに更新を提供します。注意: Citrix は、展開のすべての LTSR コンポーネントを CU3 に更新することを推奨しています。例: Citrix Provisioning が LTSR 展開の一部である場合、Citrix Provisioning コンポーネントを CU3 に更新してください。Citrix Provisioning が展開の一部ではない場合、インストールまたは更新する必要はありません。

2203 LTSR CU3 ベースラインコンポーネント

2203 CU3 ベースラインコンポーネント	プログラムと機能に表示されるバージョン	ドキュメント
シングルセッションVDA	2203.0.3000.3300	シングルセッションVDA
マルチセッションVDA	2203.0.3000.3300	マルチセッションVDA
デリバリーコントローラー	2203.0.3000.3300	デリバリーコントローラー
シトリックス スタジオ	7.33.3000.18	シトリックス スタジオ
Citrix Director (シトリックス ディレクター)	7.33.3000.24	シトリックス ディレクター
Citrixグループポリシー管理	7.33.3000.10	Citrixグループポリシー管理
Citrixグループポリシー クライアント側拡張	7.33.3000.17	

2203 CU3 ベースラインコンポーネント	プログラムと機能に表示されるバージョン	ドキュメント
シトリックス ストアフロント	2203.0.3000.14	Citrix ストアフロント
シトリックス プロビジョニング	2203.0.17	Citrix プロビジョニング
ユニバーサル プリント サーバー	2203.0.3000.9	「ユニバーサルプリントサーバー」(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/printing/printing-provision-printers.html)
セッション録画	22.3.3000	セッションレコーディング
リナックス ブイディーエー	22.03.3000.6	Linux 仮想配信エージェント(/ja-jp/linux-virtual-delivery-agent.html)
プロファイル管理	22.3.3000.3	プロファイル管理
Citrix フェデレーション認証サービス	10.9.3000.10	Citrix フェデレーション認証サービス (FAS)(/ja-jp/federated-authentication-service/2203-ltsr.html)
ブラウザコンテンツリダイレクション	15.32.3000.7	「ブラウザコンテンツリダイレクション」(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/multimedia/browser-content-redirection.html)
シトリックス プローブ エージェント 2305	2305.1.0.0	ダウンロード

2203 LTSR CU3 互換コンポーネント

以下のコンポーネント（下記バージョン）はLTSR環境と互換性があります。これらはLTSRのメリット（延長されたライフサイクルと修正のみの累積更新プログラム）の対象ではありません。Citrix®は、2203環境内でこれらのコンポーネントを新しいバージョンにアップグレードするよう求める場合があります。

互換性のあるコンポーネントと機能	プログラムと機能に表示されるバージョン	ドキュメント
アプリレイヤリング	23.4.0	Citrix App Layering (Citrixアプリケーションレイヤリング)
HDX リアルタイム最適化パック	2.9.600	HDX RealTime Optimization Pack (HDX RealTime最適化パック)
ライセンスサーバー	11.17.2.0 ビルド 42000	ライセンスサーバー(/ja-jp/licensing/11-17-2-42000.html)
ユーザーパーソナライゼーションレイヤー	23.4.0	ユーザーパーソナライゼーションレイヤー(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/install-configure/user-personalization-layer.html)
セッションレコーディングウェブプレーヤー	22.3.3000.4	セッションレコーディングWebプレーヤー(/ja-jp/session-recording/2203-ltsr/view-recordings/session-recording-web-player.html)
Microsoft Teamsの最適化	15.32.3000.9	Microsoft Teamsの最適化(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/multimedia/opt-ms-teams.html)
ワークスペース環境管理	22.12.0	ワークスペース環境管理
XenApp & XenDesktop 7.15 LTSR VDA (最新リリース)*	最新の累積更新プログラムのみ	ドキュメント

2203 LTSR CU3の主な除外事項

以下の機能、コンポーネント、およびプラットフォームは、2203のライフサイクルマイルストーンおよび特典の対象ではありません。具体的には、累積更新プログラムおよび拡張ライフサイクル特典は除外されます。除外された機能およびコンポーネントの更新プログラムは、通常の現在のリリースを通じて利用可能です。

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

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

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

新機能

Citrix Virtual Apps and Desktops™ 7 2203 LTSR Cumulative Update 3 (CU3) で、以下の新機能と機能強化が利用可能です。

Citrix VDAセッションからクライアントエンドポイントへのワイルドカードリダイレクト

CU3リリース以降、双方向コンテンツリダイレクトは、リダイレクトするURLを定義する際にワイルドカードの使用をサポートします。詳細については、Citrix VDAからクライアントへのワイルドカードリダイレクトを参照してください。

修正された問題

Citrix Virtual Apps and Desktops™ 7 2203 LTSR CU2 以降、以下の問題が修正されました。

Citrix Director (シトリックス ディレクター)

- セッションが確立されると、Citrix Director の ページのコンピューターの表示名がデリバリーグループ名に戻ります。

Citrixポリシー

- この修正により、複数のメモリの問題が修正されました。
- ポリシー設定値が **Kbps** ではなく **Kpbs** と表示されることがあります。

デリバリーコントローラー™

- サイト集約または特定のブローカーポリシーを持つデリバリーグループが有効になっている場合、アプリケーションまたはデスクトップを起動すると、既存のセッションに再接続する代わりに新しいセッションが作成されます。
- HTTPS ポート 443 が使用中の場合、MCS マシンカタログの作成が失敗することがあります。
- 予約済みメモリが構成済みメモリよりも少ない場合、仮想マシンの電源投入が次のエラーメッセージで失敗することがあります。

  無効なメモリ設定: メモリ予約 (sched.mem.min) は memsize (94208) と同じである必要があります。仮想マシンの起動に失敗しました。MemSched モジュールの起動に失敗しました。スケジューラ固有の構成パラメータの解析エラー。

- Citrix Broker Service (Brokerservice.exe) がライセンスサーバーから切断された後、予期せず終了することがあります。
- この修正により、Citrix Virtual Apps and Desktops 2203 LTSR の全体的なパフォーマンスが向上します。
- この修正により、次のようなシナリオで NT5DS がデフォルトの時刻同期プロトコルになります。

  a. マスターイメージがドメインに参加していない (NDJ) 場合、および
  b. MCS プロビジョニング中に、VM を Active Directory (AD) またはハイブリッド Azure Active Directory (HAAD) に選択した場合

- この修正により、既存のプロビジョニングスキームのネットワーク設定を変更して、新しい VM が新しいサブネットワーク上に作成されるようにすることができます。ネットワーク設定を変更するには、`Set-ProvScheme` コマンドで `parameter -NetworkMapping` を使用します。詳細については、「既存のプロビジョニングスキームのネットワーク設定を変更する」を参照してください。

フェデレーション認証サービス

- Windows 11 デスクトップに VDA をインストールできません。次のエラーが表示されます。

Citrix Authentication Identity Assertion VDA Plug-in のインストールがエラーコード 1603 で失敗しました。

ライセンス

- 強力な暗号スイートが許可されている場合にのみ、Citrix Studio (Licensing Admin PowerShell スナップイン) がライセンスサーバーとの通信に失敗する可能性があります。

Microsoft Teams の最適化

- HTML5 Video Redirection Service (CtxHdxWebSocketService) が予期せず終了する可能性があります。

メタインストーラー

- Delivery Controller インストーラーには、1912 バージョンで利用可能だったコマンドラインオプション **/No_Pending_Reboot_Check** が 2203 LTSR バージョンで欠落しています。
- VDA をアップグレードすると、レジストリキー設定 HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\SetDisplayRequiredMode が削除される可能性があります。
- VDA をバージョン 2203 LTSR CU2 にアップグレードしようとすると、失敗する可能性があります。

セキュリティの問題

- この修正はセキュリティの問題に対処します。詳細については、Knowledge Center の記事 CTX559370 を参照してください。

ユニバーサル プリント サーバー

サーバー

- Universal Print Server で Citrix XTE Service が予期せず終了し、印刷ジョブがキューにスタックしたままになる可能性があります。
- Citrix Universal Print Server 2203 で EMFPrint.exe プロセスが予期せず終了する可能性があります。

シングルセッションOS用VDA

インストール、アンインストール、アップグレード

- VDA をバージョン 1912 LTSR CU3 からバージョン 2203 LTSR CU2 にアップグレードしようとすると、失敗する可能性があります。
- この修正により、コアコンポーネントのインストールまたはアップグレード時に、マシン上の以前のWindowsインストールからの保留中の再起動のチェックを防止するコマンドラインオプション **/no_pending_reboot_check** が導入されます。
- この修正により、VUAツールはアップグレードの実行中にメジャーバージョンを比較し、CUリリースアップグレードを可能にします。これにより、2203.0.0.xから2203.0.1000.x（CU1）のようなLTSRアップグレードを実行できるようになりました。
- 「Enable restore on failure」機能が有効になっている場合、VDAのアップグレードまたはインストール中に復元ポイントが作成されないことがあります。

キーボード

- 編集可能なフィールドにカーソルを置いても、公開アプリケーションで仮想キーボードが自動的に表示されないことがあります。

セッション/接続

- Citrix Universal™ Print Serverから共有セッションプリンターへのドキュメントの印刷が失敗することがあります。この問題は、Citrix Virtual Apps and Desktops 1912 LTSR CU4にアップグレードした後に発生します。
- ユーザーセッションを介してユーザーデバイスに再接続すると、レジストリHKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStreamの下にあるMicrosoft Teamsリダイレクトキー **MSTeamsRedirSupport** が見つからない場合があります。この問題は、RDPセッションがまだ存在する場合に発生します。
- セッションへの再接続が失敗することがあります。
- 物理VDAのローカルコンソールから現在接続されているユーザーセッションを引き継ぐと、物理VDAに接続されているディスプレイの一部またはすべてが省電力モードのままになることがあります。
- WindowsシステムにCドライブがない場合、VDAバージョン2203のインストールが失敗することがあります。
- VDAをバージョン2203にアップグレードした後、Skype for Businessアプリがスプラッシュ画面で応答しなくなることがあります。
- モニターを接続すると、シームレスウィンドウが消えることがあります。

- ダブルホップシナリオでは、最初のホップ中に2つの余分な未使用のWebカメラが表示されることがあります。
- Microsoft Windows 10バージョン21H2で実行されているVDAバージョン2203では、Windowsのスタートメニューに **Power > Disconnect** オプションの代わりに空のボックスが表示されることがあります。
- ドメインに参加していない、英語以外のWindows 10 H2 VDAでは、ICA®サービスが開かないことがあります。
- この修正により、双方向コンテンツリダイレクトは、リダイレクトするURLを定義する際にワイルドカードの使用をサポートします。詳細については、「Wildcard redirection from Citrix VDA to client」を参照してください。
- 最適化されたMicrosoft Teamsを使用して特定のカスタムアプリケーションを共有しようとすると、失敗する場合があります。
- shellbridgeが有効になっている場合、すべてのスタートアッププログラムはHDX™公開アプリケーションセッションで起動されます。アプリケーションからサインアウトすると、正常なログオフが妨げられる場合があります。問題が解決しない場合は、以下のレジストリで値を0に設定してください。

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Citrix Virtual Desktop Agent

  名前: Shellbridge

  種類: REG_DWORD

  値: 0

- **ON**になっているプールされたマシンが自動的に電源オフになり、登録解除される場合があります。[
- ユーザーセッションにオーディオデバイスが追加されると、Skype for Businessのサウンドを除き、どのデバイスからもサウンドが聞こえなくなります。このエラーメッセージが表示されます。

  エラー - デバイススロットがこれ以上利用できません - デバイスの追加に失敗しました。

  この問題は、8つ以上の再生デバイスまたは録音デバイスがエンドポイントに接続されている場合に発生します。

システム例外

- CseEngine.exeサービスがVDA上で予想よりも多くのメモリを消費する場合があります。

- Citrix HDX RAVEサービス (CtxSvcHost.exe) が予期せず終了する場合があります。
- 公開デスクトップを起動し、**ファイルエクスプローラー**を開いて、**ネットワーク > \Client**の下にあるリダイレクトされたローカルCドライブをクリックすると、**ファイルエクスプローラー**が予期せず終了する場合があります。
- Citrix Virtual Apps and Desktopsバージョン2203 LTSRまたは2203 LTSR CU1にアップグレードした後、VDAセッションへの再接続が断続的に失敗する場合があります。
- VDAでtdica.sysに致命的な例外が発生し、ブルースクリーンが表示される場合があります。この問題は、セッションに再接続しようとしたときに発生します。
- USBデバイスが素早く挿入および取り外しされた場合、VDAでバグチェックコード **000000CA** が発生する場合があります。
- 証明書テンプレートが**暗号化**プロバイダーとして**Key Storage Provider**を使用して作成されている場合、VDAでSSLを有効にしようとすると失敗する場合があります。
- DllHost.exe プロセスが予期せず終了し、次のエラーメッセージが表示されることがあります。

  COM サロゲートは動作していません

- セッション起動中に、VDA が ControlUP Custom Virtual Channel Initialization で致命的な例外を経験し、ブルースクリーンが表示されることがあります。
- HTML5 ビデオリダイレクトサービス (CtxHdxWebSocketService) が予期せず終了することがあります。
- Citrix ソフトウェアグラフィックプロセス (Ctxgfx.exe) が VDA 上で過剰な非ページメモリを消費し、仮想マシンが応答しなくなることがあります。
- 公開アプリケーションを最小化モードまたは全画面モードで開くと、黒い画面が表示されることがあります。この問題は、VDA を 1912 LTSR から 2203 LTSR バージョン CU1 または CU2 にアップグレードしたときに発生します。

ユーザーエクスペリエンス

- Microsoft Access アプリケーションからコンテンツを複数回コピーしようとすると、アプリケーション内の貼り付けボタンが無効になるため、失敗することがあります。
- Citrix Gateway からサインインし、**LDAP SSO Name Attribute** が **UserPrincipalName** に設定されている場合、Citrix ウォーターマークがサインイン名を誤って表示することがあります。

マルチセッションOS用VDA

インストール、アンインストール、アップグレード

- この修正により、VUA ツールはアップグレード実行時にメジャーバージョンを比較し、CU リリースアップグレードを可能にします。これにより、2203.0.0.x から 2203.0.1000.x (CU1) などの LTSR アップグレードを実行できるようになります。

キーボード

- 編集可能なフィールドにカーソルを置いても、公開アプリケーションで仮想キーボードが自動的に表示されないことがあります。
- アプリケーションの2つのインスタンスを開き、**DisableToggler** 設定を5秒に設定すると、2番目のアプリケーションで入力するまでに約30秒待つ必要がある場合があります。

印刷

- Mac クライアントでは、ログオフして再度ログインした後、プリンターのデフォルトの用紙サイズが保持されないことがあります。

セッション/接続

- CseEngine.exe サービスが VDA 上で予想よりも多くのメモリを消費することがあります。
- 共有セッションプリンターで Citrix Universal Print Server からドキュメントを印刷しようとすると失敗することがあります。この問題は、Citrix Virtual Apps and Desktops 1912 LTSR CU4 にアップグレードした後に発生します。
- 匿名ユーザーとしてVDAからアプリケーションを起動すると、次のエラーメッセージが表示されることがあります。

  ユーザー名またはパスワードが正しくありません。

- WindowsシステムにCドライブがない場合、VDAバージョン2203のインストールが失敗することがあります。
- 公開デスクトップを起動し、**ファイルエクスプローラー**を開いて、**ネットワーク > \Client**の下にあるリダイレクトされたローカルCドライブをクリックすると、**ファイルエクスプローラー**が予期せず終了することがあります。
- 証明書テンプレートが**暗号化**プロバイダーとして**キー記憶域プロバイダー**を使用して作成されている場合、VDAでSSLを有効にしようとすると失敗することがあります。
- Citrix Directorバージョン2203では、公開アプリ起動の対話型セッションの詳細（**Userinit**や**Shell**など）が、個別の行ではなく単一の行に表示されることがあります。

- あるシームレスウィンドウから別のシームレスウィンドウにマウスカーソルを移動すると、ドラッグアンドドロップ操作が失敗することがあります。
- 最適化されたMicrosoft Teamsを使用して特定のカスタムアプリケーションを共有しようとすると、失敗することがあります。
- CtxRaveSvc.exeサービスが応答しなくなり、リモートデスクトップサービスからのセッション変更通知を受信しないことがあります。
- WebSocketService.exeプロセスがVDA上で予想よりも多くのメモリを消費することがあります。
- 公開アプリケーションを最小化モードまたは全画面モードで開くと、黒い画面が表示されることがあります。この問題は、VDAを1912 LTSRから2203 LTSRバージョンCU1またはCU2にアップグレードしたときに発生します。
- 電源がオンになっているプールされたマシンが自動的にシャットダウンされ、登録解除されることがあります。[

システム例外

- セッションの信頼性機能により再接続が発生し、その間にVDAが致命的な例外を経験し、ブルースクリーンが表示されることがあります。
- Citrix HDX RAVEサービス (CtxSvcHost.exe) が予期せず終了することがあります。
- Microsoft Windowsのwinlogon.exeプロセスが予期せず終了し、セッションが閉じることがあります。この問題は、VDAをバージョン1912 LTSR CU4から2203 LTSRにアップグレードしたときに、icagfxstack.dllモジュールの障害が原因で発生します。
- 障害のあるモジュールRPM.dllが原因で、ターミナルサービスプロセスが予期せず終了する場合があります。
- USBデバイスをすばやく挿入および取り外しすると、VDAでバグチェックコード000000CAが発生する場合があります。
- DllHost.exeプロセスが、次のエラーメッセージとともに予期せず終了する場合があります。

  COM Surrogateは動作していません

- UiPath Remote Runtimeコンポーネントがインストールされている場合、マルチセッションOS用VDAでService Host (svchost.exe) プロセスが予想よりも多くのメモリを消費する場合があります。
- セッション起動中に、VDAでControlUP Custom Virtual Channel Initializationに致命的な例外が発生し、ブルースクリーンが表示される場合があります。

- ブラウザーコンテンツリダイレクトが有効な状態でYouTubeビデオを再生しようとすると、WebSocketAgent.exeサービスが予期せず終了する場合があります。
- HTML5ビデオリダイレクトサービス (CtxHdxWebSocketService) が予期せず終了する場合があります。
- Citrixソフトウェアグラフィックプロセス (Ctxgfx.exe) がVDAで過剰な非ページメモリを消費し、仮想マシンが応答しなくなる場合があります。

ユーザーエクスペリエンス

- Microsoft Accessアプリケーションからコンテンツを複数回コピーしようとすると、アプリケーションの貼り付けボタンが無効になるため、失敗する場合があります。
- Citrix Gatewayからサインインし、**LDAP SSO Name Attribute**が**UserPrincipalName**に設定されている場合、Citrixウォーターマークにサインイン名が誤って表示される場合があります。

仮想デスクトップコンポーネント – その他

- デュアル管理者モードを使用しているときに、公開されたApp-Vアプリケーションの起動が失敗する場合があります。
- App-Vキャッシュが永続ドライブにリダイレクトされている場合、非永続マシンでのApp-Vアプリケーションの起動が失敗する場合があります。

シトリックス プロビジョニング™

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

リナックス ブイディーエー

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

プロファイル管理

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

セッション録画

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

StoreFront™

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

累積更新プログラム 2 (CU2)

リリース日: December 08, 2022

このリリースについて

Citrix Virtual Apps and Desktops™ 7 2203 LTSR Cumulative Update 2 (CU2) は、2203 LTSR CU1 のリリース以降に報告された 50 を超える問題を修正しました。

2203 LTSR (一般情報)

2203 LTSR (機能とアップグレード情報)

このリリースの新機能

Citrix Virtual Apps and Desktops 7 2203 LTSR CU1 で修正された問題

このリリースの既知の問題

非推奨と削除

Citrix製品のサブスクリプション特典の対象日

ダウンロード

シトリックス バーチャル アプリケーションズ アンド デスクトップ 7 2203 LTSR CU2

新しい展開

CU2 をゼロから展開するにはどうすればよいですか?

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

展開を計画し始める前に、Citrix Virtual Apps and Desktops 7 2203 LTSR (初期リリース) セクションを参照し、技術概要、インストールと構成、および セキュリティ の各セクションに細心の注意を払ってください。セットアップがすべてのコンポーネントの システム要件 を満たしていることを確認してください。

既存の展開

何を更新しますか?

CU2 は、2203 LTSR の 15 の ベースラインコンポーネント の更新を提供します。注意: Citrix は、展開のすべての LTSR コンポーネントを CU2 に更新することを推奨します。例: Citrix Provisioning が LTSR 展開の一部である場合は、Citrix Provisioning コンポーネントを CU2 に更新してください。Citrix Provisioning が展開の一部ではない場合は、インストールまたは更新する必要はありません。

2203 LTSR CU2 ベースラインコンポーネント

2203 CU2 ベースラインコンポーネント	プログラムと機能に表示されるバージョン	ドキュメント
シングルセッションVDA	2203.0.2000.2071	シングルセッションVDA
マルチセッションVDA	2203.0.2000.2071	マルチセッションVDA
デリバリーコントローラー	2203.0.2000.2071	デリバリーコントローラー
シトリックス スタジオ	7.33.2000.21	シトリックス スタジオ
Citrix Director (シトリックス ディレクター)	7.33.2000.21	シトリックス ディレクター
Citrixグループポリシー管理	7.33.2000.12	Citrixグループポリシー管理
Citrixグループポリシー クライアント側拡張	7.33.2000.11	
シトリックス ストアフロント	2203.0.2000.5	Citrix ストアフロント
シトリックス プロビジョニング	2203.0.11	Citrix プロビジョニング
ユニバーサル プリント サーバー	2203.0.2000.2066	「ユニバーサルプリントサーバー」(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/printing/printing-provision-printers.html)
セッション録画	22.3.2000	セッションレコーディング

2203 CU2 ベースラインコンポーネント	プログラムと機能に表示されるバージョン	ドキュメント
リナックス ブイディーエー	22.03.2000.5	Linux 仮想配信エージェント(/ja-jp/linux-virtual-delivery-agent.html)
プロファイル管理	22.3.2000.1	プロファイル管理
Citrix フェデレーション認証サービス	10.9.2000.9	Citrix フェデレーション認証サービス (FAS)(/ja-jp/federated-authentication-service/2203-ltsr.html)
ブラウザコンテンツリダイレクション	15.32.2000.1	「ブラウザコンテンツリダイレクション」(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/multimedia/browser-content-redirection.html)
Citrix プロブエージェント 2206	2209.1.0.0	ダウンロード

2203 LTSR CU2 互換コンポーネント

以下のコンポーネント（下記バージョン）は、LTSR環境と互換性があります。これらはLTSRのメリット（延長されたライフサイクルと修正のみの累積更新プログラム）の対象ではありません。Citrix®は、2203環境内でこれらのコンポーネントを新しいバージョンにアップグレードするよう求める場合があります。

互換性のあるコンポーネントと機能	プログラムと機能に表示されるバージョン	ドキュメント
アプリレイヤリング	2208.0.0	Citrix App Layering (Citrixアプリケーションレイヤリング)
HDX リアルタイム最適化パック	2.9.500	HDX RealTime Optimization Pack (HDX RealTime最適化パック)

互換性のあるコンポーネントと機能	プログラムと機能に表示されるバージョン	ドキュメント
ライセンスサーバー	11.17.2.0 ビルド 40000	ライセンスサーバー(/ja-jp/licensing/current-release.html)
ユーザーパーソナライゼーションレイヤー	22.6.3	ユーザーパーソナライゼーションレイヤー(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/install-configure/user-personalization-layer.html)
セッションレコーディングウェブプレーヤー	22.3.2000.8	セッションレコーディングWebプレーヤー(/ja-jp/session-recording/2203-ltsr/view-recordings/session-recording-web-player.html)
Microsoft Teamsの最適化	15.32.1000.9	Microsoft Teamsの最適化(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/multimedia/opt-ms-teams.html)
ワークスペース環境管理	2209	ワークスペース環境管理
XenApp & XenDesktop 7.15 LTSR VDA (最新リリース)*	最新の累積更新プログラムのみ	ドキュメント

2203 LTSR CU2 の主な除外事項

以下の機能、コンポーネント、およびプラットフォームは、2203 のライフサイクルマイルストーンと特典の対象ではありません。具体的には、累積更新プログラムと拡張ライフサイクル特典は除外されます。除外された機能およびコンポーネントの更新プログラムは、通常の最新リリースを通じて利用できます。

除外されるコンポーネントと機能
AppDisks™
AppDNA®

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

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

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

新機能

Citrix Virtual Apps and Desktops™ 7 2203 LTSR Cumulative Update 2 (CU2) には、新しい機能や機能強化はありません。

修正された問題

Citrix Virtual Apps and Desktops™ 7 2203 LTSR CU1 以降、以下の問題が修正されました。

Citrixポリシー

- CseEngine.exe がグループポリシーオブジェクト (GPO) をフェッチする際に、誤った DNS クエリが生成されることがあります。

シトリックス スタジオ

- Citrix Studio コンソールから **DBCreator**、**Securityadmin**、および **Public permissions** を使用して新しい Citrix Virtual Apps and Desktops サイトを作成しようとすると、失敗する場合があります。
- この修正により、マシンカタログの作成中にドメインを検索する機能が提供されます。詳細については、「マシンカタログの作成」を参照してください。
- **デリバリーグループ > 電源管理** に移動した後、ピーク時間バーを更新しようとすると失敗する場合があります。

デリバリーコントローラー™

- 一部のドメインコントローラーがシャットダウンされている場合、Citrix Studio はアカウント名の代わりにマシンのセキュリティ識別子 (SID) を表示することがあります。

グラフィック

- 一部のアプリケーションでは、デフォルトの最大 30 FPS ではなく、最大 22 フレーム/秒 (FPS) にフレームレートが制限されます。

シングルセッションOS用VDA

セッション/接続

- 1人のユーザーに1つではなく2つのVDAが割り当てられることがあります。
- セッションを終了すると、サーバーが応答しなくなることがあります。この問題は、icausbb.sys に存在する無限ループが原因で発生します。
- Citrix 公開アプリケーションを起動すると、シームレスモードが設定されず、公開アプリケーションの背景が黒くなることがあります。
- Citrix Workspace™ app for Windows バージョン 2203 を実行しているマルチセッション OS VDA を再構成しようとすると、失敗する場合があります。
- Universal Windows Platform (UWP) アプリを VM ホスト型アプリとして起動すると、「**Application not running**」というアプリケーションステータスが表示されます。
- **Virtualization Based Security** 機能がオンになっている場合、ユーザーデバイスを介してリモート PC アクセスを使用してワークステーションにアクセスし、その後切断すると、物理的にワークステーションに到達してシステムにログオンしたときに黒い画面が表示されることがあります。
- 公開アプリケーションに再接続すると、2つの公開アプリケーションが起動され、Delivery Controller にアプリケーションの状態が「Application not running」と表示されることがあります。
- セッションの再接続中に、電源コードが接続されている場合、バッテリーステータスインジケーターが消えることがあります。
- ブラウザーコンテンツリダイレクト拡張機能が最新バージョンの Chrome で動作せず、最適化された Microsoft Teams 通話が切断されることがあります。
- 最新バージョンの Chrome では、ブラウザーコンテンツリダイレクト拡張機能が動作せず、最適化された Microsoft Teams 通話が切断されることがあります。

システム例外

- デュアルモニターを備えた Ubuntu 18 クライアントを使用している場合、**ctxgfx** プロセスが Windows VDA バージョン 2112 で高い CPU 使用率を引き起こすことがあります。
- Citrix Audio Redirection Service が VDA バージョン 2203 で動作しないことがあります。
- wfshell.exe または PicaVcHost.exe プロセスが、例外コード 0xc0000374 で予期せず終了することがあります。この問題は、「Allowed URLs to be redirected to Client」ポリシー設定で長い文字列を設定した場合に発生します。
- wfshell.exe プロセスが、障害のある CtxUiMon.dll モジュールが原因で予期せず終了することがあります。
- Microsoft Azure Information Protection (AIP) がインストールされており、Citrix Hook が有効になっている場合、Microsoft 365 アプリケーションが予期せず終了することがあります。

ユーザーエクスペリエンス

- Windows 11 マシンに VDA バージョン 2203 をインストールしている間、**スタート**メニューで右クリックが機能しないことがあります。

マルチセッションOS用VDA

セッション/接続

- セッションを終了すると、サーバーが応答しなくなることがあります。この問題は、icausbb.sys に存在する無限ループが原因で発生します。
- Citrix Workspace app for Windows バージョン 2203 を実行しているマルチセッション OS VDA の再構成を試みると、失敗する場合があります。
- クライアントプリンター名の下にリストされている「次の VDA バージョンに適用」ポリシーでは、利用可能なバージョンとして Virtual Delivery Agent 5.6 Feature Pack 1 のみが表示されます。
- この修正により、マルチセッション VDA のセッション、アイドル、および切断タイマーを構成するための新しいユーザー設定が利用可能になります。詳細については、セッション制限ポリシー設定 のドキュメントを参照してください。
- スクリーンセーバーが有効になっている VDA を介してシームレスな公開アプリから再接続されたセッションで、スクリーンセーバーが表示される場合があります。
- 公開アプリケーションに再接続すると、2つの公開アプリケーションが起動され、Delivery Controller にアプリケーションの状態が「Application not running」と表示される場合があります。

- この修正により、仮想チャネルを許可リストに追加する際に、プロセスパスでワイルドカードを使用できるようになります。詳細については、仮想チャネルのセキュリティ のドキュメントを参照してください。
- セッションの再接続中に、電源コードが接続されている場合、バッテリーステータスインジケーターが消えることがあります。
- RPM が期待どおりにロックを解放せず、ログオフプロセスを保留している場合、VDA が応答しなくなることがあります。
- ブラウザーコンテンツリダイレクト拡張機能が最新バージョンの Chrome で動作せず、Optimized Microsoft Teams 通話が切断される場合があります。
- 最新バージョンの Chrome では、ブラウザーコンテンツリダイレクト拡張機能が失敗し、Optimized Microsoft Teams 通話が切断される場合があります。

システム例外

- VDA で tdica.sys に致命的な例外が発生し、バグチェックコード 0x0000007E を伴うブルースクリーンが表示される場合があります。
- VDA で picavc.sys または picadm.sys に致命的な例外が発生し、ブルースクリーンが表示される場合があります。
- デュアルモニターを備えた Ubuntu 18 クライアントを使用している場合、Windows VDA バージョン 2112 で **ctxgfx** プロセスが CPU 使用率を高くする可能性があります。
- 仮想チャネルが切断されると、wfshell.exe プロセスが予期せず終了する場合があります。
- wfshell.exe または PicaVcHost.exe プロセスが、例外コード 0xc0000374 で予期せず終了する場合があります。この問題は、Allowed URLs to be redirected to Client ポリシー設定で長い文字列を設定すると発生します。
- wfshell.exe プロセスが、障害のある CtxUiMon.dll モジュールが原因で予期せず終了する場合があります。
- マルチセッション OS でバージョン 2203 を実行している VDA に接続しようとすると、logonui.exe プロセスが応答しなくなり、黒い画面が表示されたり、終了したりする場合があります。ただし、イベントログは表示される可能性があります。
- マルチセッション OS VDA で実行されているターミナルサービスが、断続的に登録解除され、終了する場合があります。

シトリックス プロビジョニング™

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

リナックス ブイディーエー

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

プロファイル管理

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

セッション録画

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

StoreFront™

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

累積更新プログラム 1 (CU1)

リリース日: August 03, 2022

このリリースについて

Cumulative Update 1 は、August 24, 2022 に Cumulative Update 1100 として再リリースされました。この再リリースは、一部のケースでシングルセッション VDA の 2203 Cumulative Update 1 へのアップグレードを妨げていた問題 LCM-11719 に対処します。

Citrix Virtual Apps and Desktops™ 7 2203 LTSR Cumulative Update 1 (CU1) は、2203 LTSR の初回リリース以降に報告された 30 を超える問題を修正します。

2203 LTSR (一般情報)

2203 LTSR (機能とアップグレード情報)

このリリースの新機能

Citrix Virtual Apps and Desktops 7 2203 LTSR (初回リリース) で修正された問題

このリリースの既知の問題

非推奨と削除

Citrix製品のSubscription Advantage資格日

ダウンロード

シトリックス バーチャルアプリおよびデスクトップ 7 2203 LTSR CU1

新規展開

CU1をゼロから展開するにはどうすればよいですか?

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

展開計画を開始する前に、Citrix Virtual Apps and Desktops 7 2203 LTSR (初回リリース) セクションを熟読し、技術概要、インストールと構成、および セキュリティ の各セクションに細心の注意を払ってください。セットアップがすべてのコンポーネントの システム要件 を満たしていることを確認してください。

既存の展開

何を更新しますか?

CU1 は、2203 LTSR の 15 のベースラインコンポーネント(#2203-ltsr-cu1-baseline-components)に更新を提供します。注意: Citrix は、展開のすべての LTSR コンポーネントを CU1 に更新することを推奨しています。たとえば、Citrix Provisioning が LTSR 展開の一部である場合、Citrix Provisioning コンポーネントを CU1 に更新してください。Citrix Provisioning が展開の一部でない場合、インストールまたは更新する必要はありません。

2203 LTSR CU1 ベースラインコンポーネント

2203 CU1 ベースラインコンポーネント	プログラムと機能に表示されるバージョン	ドキュメント
シングルセッションVDA	2203.0.1100.1178	シングルセッションVDA
マルチセッションVDA	2203.0.1100.1178	マルチセッションVDA
デリバリーコントローラー	2203.0.1100.1178	デリバリーコントローラー
シトリックス スタジオ	7.33.1100.27	シトリックス スタジオ
Citrix Director (シトリックス ディレクター)	7.33.1100.40	シトリックス ディレクター

2203 CU1 ベースラインコンポーネント	プログラムと機能に表示されるバージョン	ドキュメント
Citrixグループポリシー管理	7.33.1100.18	Citrixグループポリシー管理
Citrixグループポリシー クライアント側拡張	7.33.1100.16	
シトリックス ストアフロント	2203.0.1000.10	Citrix ストアフロント
シトリックス プロビジョニング	7.33.5	Citrix プロビジョニング
ユニバーサル プリント サーバー	7.33.1100.18	「ユニバーサルプリントサーバー」(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/printing/printing-provision-printers.html)
セッション録画	22.3.1100.1178	セッションレコーディング
リナックス ブイディーエー	22.03.1000.7	Linux 仮想配信エージェント(/ja-jp/linux-virtual-delivery-agent.html)
プロファイル管理	22.3.1000.4	プロファイル管理
Citrix フェデレーション認証サービス	10.9.1100.18	Citrix フェデレーション認証サービス (FAS)(/ja-jp/federated-authentication-service/2203-ltsr.html)
ブラウザコンテンツリダイレクション	15.32.1100.9	「ブラウザコンテンツリダイレクション」(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/multimedia/browser-content-redirection.html)
Citrix プロブエージェント 2206	2206.1.0.0	ダウンロード

2203 LTSR CU1 互換コンポーネント

以下のコンポーネント（下記バージョン）は、LTSR環境と互換性があります。これらはLTSRのメリット（延長されたライフサイクルと修正のみの累積更新プログラム）の対象ではありません。Citrix®は、2203環境内でこれらのコンポーネントを新しいバージョンにアップグレードするよう求める場合があります。

互換性のあるコンポーネントと機能	プログラムと機能に表示されるバージョン	ドキュメント
アプリレイヤリング	2206.0.0	Citrix App Layering (Citrixアプリケーションレイヤリング)
HDX リアルタイム最適化パック	2.9.400.2702	HDX RealTime Optimization Pack (HDX RealTime最適化パック)
ライセンスサーバー	11.17.2.0 ビルド 39000	ライセンスサーバー(/ja-jp/licensing/current-release.html)
ユーザーパーソナライゼーションレイヤー	22.6.1	ユーザーパーソナライゼーションレイヤー(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/install-configure/user-personalization-layer.html)
セッションレコーディングウェブプレーヤー	22.3.1000.5	セッションレコーディングWebプレーヤー(/ja-jp/session-recording/2203-ltsr/view-recordings/session-recording-web-player.html)
Microsoft Teamsの最適化	15.32.1000.9	Microsoft Teamsの最適化(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/multimedia/opt-ms-teams.html)
ワークスペース環境管理	2203.1.0.1	ワークスペース環境管理
XenApp & XenDesktop 7.15 LTSR VDA (最新リリース)*	最新の累積更新プログラムのみ	ドキュメント

2203 LTSR CU1 の主な除外事項

以下の機能、コンポーネント、およびプラットフォームは、2203 のライフサイクルマイルストーンと特典の対象ではありません。具体的には、累積更新プログラムと拡張ライフサイクル特典は除外されます。除外された機能およびコンポーネントの更新プログラムは、通常の現在のリリースを通じて利用できます。

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

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

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

修正された問題

以下の問題は、Citrix Virtual Apps and Desktops™ 7 2203 LTSR (初期リリース) 以降で修正されています。

Citrix Director (シトリックス ディレクター)

- VDAをアンインストールした後も、Citrix Windows Management Instrumentation (WMI) の名前空間が残る場合があります。
- Citrix StudioおよびCitrix Directorのアクティブセッション数が一致しない場合があります。

Citrixポリシー

- VDAがDelivery Controller™に登録されず、未登録のままになる場合があります。

- Citrix Studioでポリシーを割り当てるために使用されるタグまたはデリバリーグループは、250の制限を超えて列挙できません。

シトリックス スタジオ

- Citrix Studioでのマシンカタログに関する操作（カタログへのアクセス、作成、削除、列挙など）が遅くなる場合があります。この問題は、Nutanixハイパーバイザーが接続のホストに使用されている場合に発生します。

デリバリーコントローラー

- Citrix Virtual Apps and Desktopsをバージョン1912 LTSRにアップグレードしても、Citrix.AzureRmPlugin.dll.config構成ファイルが更新されず、Microsoft Azure Resource Managerへの接続が失敗する場合があります。
- Machine Creation Services™カタログを更新する際に、仮想マシンを選択してから関連するスナップショットを選択すると、次のエラーメッセージが表示される場合があります。

  予期せぬエラーが発生しました。Citrixテクニカルサポートにお問い合わせください。

- System Center Virtual Machine Manager (SCVMM) への接続が復元された後、マシンの電源をオンにしようとすると失敗する場合があります。
- マスターイメージからVDAバージョン2203 LTSRマシンを作成するために静的IPアドレスを使用すると、イメージ準備中にMachine Creation Services (MCS) がDHCPを有効にしない場合があります。

シングルセッションOS用VDA

キーボード

- Citrix Workspace™ app for Linuxを使用して開かれたセッションで、キーボードショートカットの**Ctrl+Break**が機能しない場合があります。

セッション/接続

- モニターを接続または切断すると、シームレスウィンドウの位置が正しくない場合があります。
- Microsoft Teamsの画面共有機能を使用して特定のサードパーティ製アプリを共有すると、失敗する場合があります。
- Microsoft Teamsで共有されているアプリのウィンドウのサイズを変更しようとすると、アプリが共有されていることを示す赤い枠が、アプリの実際のサイズと一致しない場合があります。

- VDAバージョン2112でConnection Quality Indicatorを実行すると、不正なラウンドトリップタイム (RTT) と遅延値が報告される場合があります。

  この修正により、HDX Adaptive Scaling機能が無効になっている場合に、従来のNetScaler® L7遅延測定を使用できるようになります。NetScaler L7遅延とVDA HDX Adaptive Scaling機能は同時に有効にできません。

  この修正の機能が有効になるには、VDAレジストリでHDX™ Adaptive Scaling機能を次のように無効にする必要があります。

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd

  名前: AdaptiveScalingEnabled

  種類: DWORD

  値: 0

- グラフィックステータスインジケーターポリシーが有効な状態でDesktop Viewerウィンドウのサイズを変更すると、失敗して一時的にグレースクリーンが表示されることがあります。グレースクリーンは、VDAを再起動するまで消えない場合があります。
- Microsoft Teamsの画面共有機能を使用して特定の公開アプリケーションを共有すると、失敗する場合があります。
- Citrix HDX最適化されたMicrosoft Teamsを使用しているときに、Citrix HDX HTML5 Video Redirection Service (WebSocketService.exe) がセッションリークを引き起こす可能性があります。
- 構成情報なしでCitrix WEM AgentがVDAマシンにインストールされている場合、VDAのアップグレードが失敗する可能性があります。
- シングルセッションVDAを2203 Cumulative Update 1にアップグレードすると失敗し、次のエラーメッセージが表示されることがあります。

  `IcaConfigConsole.exe failed with error code -4`

  回避策として、アップグレードする前にターゲットマシンに次のレジストリキーを作成してください。

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI

  詳細については、Knowledge Centerの記事CTX463588を参照してください。

注：この問題は、Cumulative Update 1の再スピンであるCumulative Update 1100で対処されました。

システム例外

- wfshell.exeプロセスが予期せず終了し、公開アプリケーションからの新しいアプリケーション起動が失敗する可能性があります。
- CTXCDFのエラーにより、Windows Management Instrumentation Provider Service (WMIPRVSE.exe) が停止し、イベントログにイベントID 5612が生成されることがあります。
- WebSocketService.exeプロセスが予期せず終了し、Microsoft Teamsの通話が以下のエラーメッセージで失敗することがあります。

  リモートデバイスに接続中です。通話はまだ利用できません。

- PicaVcHost.exeプロセスでアクセス違反が発生し、予期せず終了することがあります。

ユーザーエクスペリエンス

- ユーザーデバイスとVDAでプライマリボタンが**左**に設定されている左利き用マウスが、期待どおりに動作しないことがあります。

ユーザーインターフェイス

- 画面共有機能の使用中に他のユーザーに画面制御を提供すると、`<xxx>` **wants to control your desktop の代わりに** `<xxx>` **wants to view your desktop が表示される**という誤った中国語翻訳プロンプトが表示されることがあります。

マルチセッションOS用VDA

セッション/接続

- 以下のHDX公開アプリケーションの問題が解決されました。
  - Microsoft Officeのパスワードプロンプトが表示されないことがあります。
  - **プリンターとスキャナー**などのデバイスが、**設定**メニューに表示されないことがあります。
  - 新しく作成されたフォルダーが、**ファイルエクスプローラー**アプリケーションに表示されないことがあります。
  - **ファイルエクスプローラー**メニューの**設定を開く**が機能しません。

- Microsoft WordやMicrosoft Excelなどのアプリケーションで、**保存**または**開く**オプションを使用してフォルダーの名前変更、作成、または削除を行うと、ウィンドウが自動的に更新されません。ただし、ウィンドウは手動で更新できます。
- Universal Windows Platform (UWP) アプリの起動中、Citrix Workspaceアプリのセッション完了プログレスバーが消えてから8〜13秒後にアプリが画面に表示されます。その結果、ユーザーは複数回起動を試みる可能性があります。
- Windows 11バージョン22H2のHDXシームレスセッションで、印刷ダイアログボックスが開いている場合、印刷ウィンドウが部分的に表示されることがあります。
- 「**ファイルエクスプローラー**」の検索バーが機能しません。
- 非UWPアプリが以前に起動されている場合、ユニバーサルWindowsプラットフォーム (UWP) アプリを正常に起動できません。
- Microsoft Office 365ビルド16.0.7967以降のアプリケーションがWindows Server 2019ホストからのアプリケーションとして公開されている場合、Officeライセンスのアクティベーションが失敗します。

この修正を有効にするには、次の手順を実行します。

- 次のレジストリの詳細を追加します。

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Citrix Virtual Desktop Agent

  名前: Shellbridge

  種類: REG_DWORD

  値: 1
- 次のOSアップデートがインストールされていることを確認してください。

  Windows 11: KB5014019

  Windows Server 2022 の修正プログラム: KB5014021

  Windows 10 の修正プログラム: KB5014023

  Windows サーバー 2019: KB5014022

- Citrix Virtual Apps and Desktops 1912 CU に VDA をインストールする際に、レジストリキー HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Ica\Session の TermService 権限が復元されず、セッション障害が発生する可能性があります。

- VDAバージョン2112でConnection Quality Indicatorを実行すると、誤ったラウンドトリップタイム (RTT) および遅延値が報告される可能性があります。

  この修正により、HDXアダプティブスケーリング機能が無効になっている場合でも、従来のNetScaler L7遅延測定を使用できるようになります。NetScaler L7遅延とVDA HDXアダプティブスケーリング機能は同時に有効にできません。

  この修正の機能が有効になるようにするには、VDAレジストリでHDXアダプティブスケーリング機能を次のように無効にする必要があります。

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd

  名前: AdaptiveScalingEnabled

  種類: DWORD

  値: 0

- **クライアントプリンター名**の下にリストされている**次のVDAバージョンに適用**ポリシーでは、利用可能なバージョンとしてVirtual Delivery Agent 5.6 Feature Pack 1のみが表示されます。
- セッションへの再接続が失敗し、Citrix Directorからセッションが消えることがあります。既存のセッションに再接続する代わりに、新しいセッションが起動されます。この修正を有効にするには、次のレジストリキーを設定します。

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Ica\GroupPolicy

  名前: EnforceUserPolicyEvaluationSuccess

  種類: REG_DWORD

  値: 0

- 構成情報なしでCitrix WEM AgentがVDAマシンにインストールされている場合、VDAのアップグレードが失敗することがあります。

システム例外

- wfshell.exeプロセスが予期せず終了し、公開アプリケーションからの新しいアプリケーション起動が失敗することがあります。
- CTXCDFのエラーにより、Windows Management Instrumentation Provider Service (WMIPRVSE.exe) が停止し、イベントログにイベントID 5612が生成されることがあります。
- 仮想チャネルが切断されると、wfshell.exe プロセスが予期せず終了する場合があります。

- **設定を開く**ウィンドウを閉じると、ファイルエクスプローラーが予期せず終了することがあります。
- マルチセッションOS用VDAでターミナルサービスが断続的に終了することがあります。システムイベントログにイベントID 7011が次のメッセージとともに記録されます。

  TermServiceサービスからのトランザクション応答を待機中にタイムアウト (30000ミリ秒) に達しました。

ユーザーエクスペリエンス

- ユーザーデバイスとVDAでプライマリボタンが**左**に設定されている左利き用マウスが、期待どおりに動作しないことがあります。

ユーザーインターフェイス

- Citrixセッションとローカルエンドポイント間でファイルをドラッグアンドドロップすると、「**ドラッグアンドドロップ**」ポリシーが有効になっていても失敗する場合があります。「**CtxDnDSourceProxy**」というポップアップエラーが表示されます。

仮想デスクトップコンポーネント – その他

- App-Vキャッシュが永続ドライブにリダイレクトされている場合、非永続マシンでApp-Vアプリケーションの起動が失敗する場合があります。

シトリックス プロビジョニング™

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

リナックス ブイディーエー

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

プロファイル管理

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

セッション録画

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

StoreFront™

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

2203 LTSR (初回リリース)

このリリースについて

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

LTSRは、Citrix Virtual Apps and Desktops 1912およびXenApp and XenDesktop Version 7.15でも利用できます。

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

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

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

インストールとアップグレードの手順については、以下を参照してください。

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

2203 LTSR 初回リリースベースラインコンポーネント

2203 ベースラインコンポーネント	プログラムと機能に表示されるバージョン	ドキュメント
シングルセッションVDA	2203.0.0.33220	シングルセッションVDA
マルチセッションVDA	2203.0.0.33220	マルチセッションVDA
デリバリーコントローラー	2203.0.0.33220	デリバリーコントローラー
シトリックス スタジオ	7.33.0.70	シトリックス スタジオ
Citrix Director (シトリックス ディレクター)	7.33.0.67	シトリックス ディレクター
Citrixグループポリシー管理	7.33.0.33	Citrixグループポリシー管理
Citrixグループポリシー クライアント側拡張	7.33.0.22	
シトリックス ストアフロント	2203.0.0.36	Citrix ストアフロント
シトリックス プロビジョニング	2203.0.0	Citrix プロビジョニング
ユニバーサル プリント サーバー	7.33.0.12	「ユニバーサルプリントサーバー」(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/printing/printing-provision-printers.html)
セッション録画	22.3.0	セッションレコーディング
リナックス ブイディーエー	22.03.0.16	Linux 仮想配信エージェント(/ja-jp/linux-virtual-delivery-agent.html)
プロファイル管理	22.3.0.7	プロファイル管理
Citrix フェデレーション認証サービス	10.9.0.23	Citrix フェデレーション認証サービス (FAS)(/ja-jp/federated-authentication-service/2203-ltsr.html)

2203 ベースラインコンポーネント	プログラムと機能に表示されるバージョン	ドキュメント
ブラウザコンテンツリダイレクション	15.32.0.17	「ブラウザコンテンツリダイレクション」(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/multimedia/browser-content-redirection.html)
Citrixプローブエージェント	2103.1.0.0	ダウンロード

2203 LTSR初期リリース互換コンポーネント

以下のコンポーネント（記載されているバージョン）は、LTSR環境と互換性があります。これらのコンポーネントは、LTSRのメリット（延長されたライフサイクルと修正のみの累積更新プログラム）の対象ではありません。Citrixは、2203環境内でこれらのコンポーネントを新しいバージョンにアップグレードするよう求める場合があります。

互換性のあるコンポーネントと機能	プログラムと機能に表示されるバージョン	ドキュメント
アプリレイヤリング	2202.0.0	Citrix App Layering (Citrixアプリケーションレイヤリング)
HDX リアルタイム最適化パック	2.9.400	HDX RealTime Optimization Pack (HDX RealTime最適化パック)
ライセンスサーバー	11.17.2.0 ビルド 37000	ライセンスサーバー(/ja-jp/licensing/11-17-2-37000.html)
ユーザーパーソナライゼーションレイヤー	21.12.5.7	ユーザーパーソナライゼーションレイヤー(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/install-configure/user-personalization-layer.html)
セッションレコーディングウェブプレーヤー	22.3.0.24	セッションレコーディングWebプレーヤー(/ja-jp/session-recording/2203-ltsr/

互換性のあるコンポーネントと機能	プログラムと機能に表示されるバージョン	ドキュメント
		view-recordings/session-recording-web-player.html)
Microsoft Teamsの最適化	15.32	Microsoft Teamsの最適化(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/multimedia/opt-ms-teams.html)
ワークスペース環境管理	2203.1.0.1	ワークスペース環境管理
XenApp & XenDesktop 7.15 LTSR VDA (最新リリース)*	最新の累積更新プログラムのみ	ドキュメント

2203 LTSR 初回リリースにおける主な除外事項

以下の機能、コンポーネント、およびプラットフォームは、2203ライフサイクルマイルストーンおよび特典の対象ではありません。具体的には、累積更新プログラムと拡張ライフサイクル特典は除外されます。除外された機能およびコンポーネントの更新プログラムは、通常の現在のリリースを通じて利用できます。

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

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

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

新機能

この記事では、Citrix Virtual Apps and Desktops™ 7 2203 LTSR (初期リリース) の新機能と強化された機能について説明します。更新はコンポーネントごとに整理されています。

ローカルホストキャッシュ (LHC) を管理するためのPowerShellコマンド

Delivery ControllerでLHCを管理するためにPowerShellコマンドを使用できるようになりました。詳細については、「ローカルホストキャッシュのPowerShellコマンド」を参照してください。

ハイブリッド権限ライセンス

2203 LTSRの初期リリース以降、これまでサポートされていなかったパブリッククラウドホスト接続を、新しい**ハイブリッド権限ライセンス**を使用して展開できるようになりました。これにより、オンプレミス展開とクラウド展開を併用できます。サポートされているパブリッククラウドホスト接続は、AWS、Azure、Google Cloudです。展開にパブリッククラウドホスト接続が含まれている場合、ハイブリッド権限ライセンスなしでは現在のバージョンにアップグレードできません。詳細については、以下を参照してください。

- ハイブリッド権限による移行とアップグレード (TTU)
- 展開のアップグレード
- Citrix プロビジョニング
- システム要件(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/system-requirements.html)

仮想配信エージェント (VDA) 2203

WindowsシングルセッションOSおよびマルチセッションOS VDAのバージョン2203には、以下の機能強化が含まれています。これらの項目は、この記事で前述したVDAのインストールおよびアップグレード項目に追加されるものです。

Windowsログオン画面のキーボードレイアウトの強化

2203 LTSRの初期リリースでは、シングルサインオンが不可能な場合（たとえば、サービス継続性を使用している間の接続リースベースの起動時など）にVDAによって表示されるWindowsサインイン画面で発生するキーボードレイアウトの問題に対処しています。このリリース以前は、Windowsサインイン画面でVDAのキーボードレイアウトが使用されていました。

2203 LTSRの初期リリース以降、VDA上の仮想セッションにサインインする際、ローカルクライアントのキーボードレイアウトを使用して資格情報を入力できるようになりました。

アダプティブオーディオの更新

アダプティブオーディオとUDPオーディオに新しい実装が追加されました。詳細については、「UDPリアルタイムトランスポート経由のオーディオとオーディオUDPポート範囲」を参照してください。

Citrix Director (シトリックス ディレクター)

TLS 1.3 のサポート

Citrix DirectorはTLSバージョン1.3をサポートするようになりました。

シトリックス スタジオ

現在のリリースにおけるホストサポートの変更点

2203 LTSRの初回リリース以降、製品の現在のリリースは、以下のパブリッククラウドホスト上のVDA（アプリとデスクトップを提供するマシン）をサポートします。

- アマゾン ウェブ サービス
- グーグル クラウド プラットフォーム
- マイクロソフト Azure リソース マネージャー

> **重要:**
>
> 展開にパブリッククラウドホスト接続を追加する場合は、ハイブリッドライツライセンスが必要です。ハイブリッドライツライセンスの詳細については、「ハイブリッドライツによる移行とアップグレード (TTU)」を参照してください。

> サポートされているホストおよび仮想化リソースの完全なリストについては、「システム要件」を参照してください。

ライセンスの有効性チェック

Citrix Studioは、ホスト接続で使用されているライセンスの有効性を自動的にチェックするようになりました。ライセンスが無効な場合、ホスト接続はメンテナンスモードになります。その結果、接続の編集やメンテナンスモードの解除など、特定の操作を実行できなくなります。ライセンスが無効になるのは、たとえば次のような場合です。

- ライセンスの有効期限が切れています。この場合、Citrix営業担当者に連絡して、ライセンスを更新するか、新しいライセンスを購入してください。

- ライセンスがライセンスサーバーから削除されました。

Citrix Provisioning™ 2203 LTSR初回リリース

Citrix Provisioning 2203 LTSR初回リリースには、新機能と修正が含まれています。

Linux Virtual Delivery Agent 2203 LTSR 初回リリース

Linux Virtual Delivery Agent 2203 LTSR初回リリースには、新機能と修正が含まれています。

Profile Management 2203 LTSR初回リリース

Profile Management 2203 LTSR初回リリースには、新機能と修正が含まれています。

Session Recording 2203 LTSR 初期リリース

Session Recording 2203 LTSR 初期リリースには、新機能が含まれており、修正はありません。

StoreFront™ 2203 LTSR 初期リリース

StoreFront 2203 LTSR 初期リリースには、新機能と修正が含まれています。

ワークスペース環境管理™ 2203

Workspace Environment Management 2203 には、新機能と修正が含まれています。

修正された問題

Citrix Virtual Apps and Desktops™ 7 2112 以降、以下の問題が修正されました。

Microsoft Teams の最適化

- 1000を超えるアプリケーションウィンドウが開いている場合、アプリケーション共有の列挙に失敗し、共有トレイにアプリケーションが表示されません。

シングルセッションOS用VDA

キーボード

- バージョン1912 LTSR CU3を実行しているVDAに接続されたAndroidデバイスで、テキスト入力フィールドをアクティブにすると、画面キーボードが自動的に表示されない場合があります。
- ユーザーセッションを起動すると、汎用クライアントのInput Method Editor (IME) が自動的に設定されない場合があります。その結果、キーボードがエンドポイントと自動的に同期されません。

- この修正により、HTML5、Mac、およびLinuxクライアント向けのCitrix Workspace™アプリで発生するロシア語キーボードのマッピングの問題が解決されます。

印刷

- 公開デスクトップでクライアントプリンターリダイレクトが有効になっている場合、一部のクライアントプリンター設定がVDA上のプリンター設定と同期されない場合があります。
- セッションの再接続中にセッションプリンターが消えることがあり、その結果、リモートデスクトップ (RDP) からVDAにアクセスできなくなる場合があります。

セッション/接続

- セッションを終了すると、サーバーが応答しなくなる場合があります。この問題は、汎用USBリダイレクトを使用している場合に発生します。
- ローカルIMEが有効な公開されたMicrosoft Outlookアプリで以下の手順を実行すると、メールウィンドウにランダムな文字列が入力される可能性があります。
  - メールウィンドウを開きます。
  - Escキーを押して「**変更を保存しますか？**」ダイアログを表示し、ランダムなテキストを入力します。
  - Escキーを押してダイアログを閉じます。
- Citrix IMEが有効になっている場合、特定のサードパーティ製アプリケーションが応答しなくなり、ユーザーセッションでのアプリケーションの起動が失敗する場合があります。この問題は、CtxImeモジュールの障害が原因で発生します。

システム例外

- VDAで致命的な例外が発生し、バグチェックコード0x0000010D (WDF_VIOLATION) のブルースクリーンが表示される場合があります。
- VDAをバージョン2009以降にアップグレードすると、イベントログにKernelbaseクラッシュエラー（KERNELBASE.dll）が表示されることがあります。この問題は、Google ChromeおよびMicrosoft Edgeブラウザで発生します。

ユーザーインターフェイス

- マルチモニター環境で、メインモニターを縦向きモードに設定すると、SAS通知が90度回転して表示されることがあります。

ユーザーエクスペリエンス

- ユーザーデバイスとVDAでプライマリボタンが**左**に設定されている左利き用マウスが、期待どおりに動作しない場合があります。

マルチセッションOS用VDA

キーボード

- バージョン1912 LTSR CU3を実行しているVDAに接続されたAndroidデバイスで、テキスト入力フィールドをアクティブにすると、オンスクリーンキーボードが自動的に表示されない場合があります。

印刷

- 公開デスクトップでクライアントプリンターリダイレクトが有効になっている場合、一部のクライアントプリンター設定がVDA上のプリンター設定と同期しない場合があります。
- セッションの再接続中にセッションプリンターが消え、リモートデスクトップ（RDP）からVDAにアクセスできなくなることがあります。

セッション/接続

- 起動バーを非表示にするために**HideStatusMessages**の値を1に設定すると、レジストリキーHKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\が期待どおりに機能しない場合があります。
- シームレスセッションで、特定のサードパーティ製アプリケーションが応答しなくなることがあります。
- セッションを終了すると、サーバーが応答しなくなることがあります。この問題は、汎用USBリダイレクトを使用している場合に発生します。
- Citrix IMEが有効になっている場合、特定のサードパーティ製アプリケーションが応答しなくなり、ユーザーセッションでのアプリケーション起動が失敗することがあります。この問題は、CtxImeモジュールの障害が原因で発生します。
- ライセンスサーバーのライセンスが枯渇し、**ライセンスバーストモード**機能が無効になっている場合、「**アクセス拒否**」エラーメッセージでフリーズした黒い画面が表示されることがあります。
- トランスポートプロトコルとしてEDTを使用している場合、ネットワークの不安定性によりユーザーデバイスがVDAから切断されることがあります。ネットワークが復旧すると、VDAへの再接続に時間がかかります。
- Citrix仮想セッションを終了すると、次のいずれかまたは複数の問題が発生する可能性があります。

- VDAには、終了したセッションとlogonui.exeプロセスが引き続き表示されます。logonui.exeプロセスは強制終了できます。
- セッションがCitrix Studioで空白のユーザー名で表示されます。
- それ以上のセッションを起動できない場合があります。

システム例外

- 公開アプリケーションとしてリモートデスクトップ接続 (mstsc.exe) を起動すると、CredentialUIBroker.exe プロセスが予期せず終了する場合があります。
- Citrix Stack Control Service (SCService64.exe) が予期せず終了する場合があります。
- VDAをバージョン2009以降にアップグレードすると、イベントログにKernelbaseクラッシュエラー (KERNELBASE.dll) が表示される場合があります。この問題は、Google ChromeおよびMicrosoft Edgeブラウザで発生します。

シトリックス プロビジョニング™

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

リナックス ブイディーエー

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

プロファイル管理

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

セッション録画

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

StoreFront™

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

既知の問題

注

- この記事の2203初期リリース、CU1、CU2、CU3、CU4のセクションで説明されている既知の問題は、修正された問題のリストに含まれていない限り、CU5にも引き続き存在します。
- 既知の問題に回避策がある場合は、問題の説明の後に記載されています。
- レジストリエントリの変更を推奨する回避策には、以下の警告が適用されます。

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

2203 CU7の既知の問題

- 2203 LTSR CU7から2402 LTSR CU1またはCU2（2411以前のバージョンを含む）にアップグレードすると、アップグレードが失敗する可能性があります。回避策として、2402 LTSR CU3/CVAD 2503以降のような新しいバージョンに直接アップグレードできます。
- 部分的にアップグレードされたサイトで新しいAWS/Azureホスト接続を作成すると、失敗する可能性があります。完全にアップグレードされたサイトで新しいホスト接続を作成することをお勧めします。
- 複数のタブでブラウザコンテンツリダイレクトを全画面で使用している場合、タブをゆっくりドラッグアウトしているときに、ブラウザのビューポートが飛び出すことがあります。ドラッグが停止すると、ブラウザのビューポートはブラウザ画面に調整されます。
- HTML5ビデオリダイレクトを使用している場合、自動再生されないビデオのビデオコントロールが表示されない場合がありますが、それらは利用可能です。

2203 CU6の既知の問題

- このリリースでは、32ビット版FirefoxブラウザでFIDO2はサポートされていません。

2203 CU5の既知の問題

- Citrix Workspaceアプリバージョン22.03.5000（Citrix Virtual Apps and Desktops 2203 CU4 VDAおよびCU4 Update 1で利用可能）が既にインストールされている状態で、最新バージョンにアップグレードしようとすると、自動更新ポップアップが原因でアップグレードが失敗する可能性があります。 VDAをCU5に更新する前に、以下の回避策を使用してください。

  a. Citrix Workspaceアプリバージョン2203.1 LTSR CU6またはCitrix Workspaceアプリ2402 LTSRにアップグレードします。

  b. 自動更新を無効にします。詳細については、「グループポリシーオブジェクト管理用テンプレートを使用したCitrix Workspaceの更新の構成」を参照してください。

  c. Citrix Workspace™アプリの更新プロンプトで、**後で通知する**を選択します。

2203 CU4の既知の問題

- Windows、IIS、およびCitrix DirectorをC:\以外のドライブにインストールし、Citrix Directorをリリース2203 LTSR CU4にアップグレードすると、Citrix Directorのアイコンが空白で表示される場合があります。ただし、アイコンをクリックしてCitrix Directorを起動することはできます。

  アイコンを正しく表示するには、以下の回避策を使用できます。

1. コマンドプロンプトを開き、コマンド echo **%systemdrive%** を実行します。
2. コマンドの出力をコピーします。
3. Citrix Directorアイコンを右クリック > その他 > ファイルの場所を開く。
4. メモ帳を開き、ファイルエクスプローラーからアイコンをメモ帳にドラッグします。
5. 内容の「C:」を手順2でコピーした出力に置き換えて保存します。
6. Citrix Directorアイコンが正しく表示されるようになります。

- StoreFront™をバージョン2203 LTSR CU4にアップグレードすると、リソースまたはアプリの列挙の開始が失敗する場合があります。

> **注：**
>
> この問題は、2203 LTSR CU4 Update 1 で修正されています。

- VDAでpicadd.sysに致命的な例外が発生し、バグチェックコード0x96のブルースクリーンが表示されることがあります。

> **注：**
>
> この問題は、2203 LTSR CU4 Update 1 で修正されています。

2203 CU3の既知の問題

- 一部のオーディオデバイスが、デバイスリストに誤った名前で表示されることがあります。
- インターネットアクセスがない場合、VDAのインストールと同時にCitrix Workspaceアプリをインストールしようとすると失敗する場合があります。回避策として、Citrix Workspaceアプリのインストールをスキップするか、VDAをインストールする前にMicrosoft WebView（Citrix Workspaceアプリの前提条件）をインストールする必要があります。

2203 CU2の既知の問題

- インターネットアクセスがない場合、VDAのインストールと同時にCitrix Workspaceアプリをインストールしようとすると失敗する場合があります。回避策として、Citrix Workspaceアプリのインストールをスキップするか、VDAをインストールする前にMicrosoft WebView（Citrix Workspaceアプリの前提条件）をインストールする必要があります。
- Citrix Virtual Apps and Desktops™ 2203 LTSR CU1からCU2へのSession Recordingのアップグレードが失敗する場合があります。次のエラーメッセージが表示されます。

  インストールを完了できません。

  初期化中に問題が発生したため、インストールが完了しませんでした。製品は動作しますが、パフォーマンスが低下する可能性があります。

- ログオン中に、Profile ManagementがカスタマイズされたOutlook OSTパスをリセットする場合があります。

2203 CU1の既知の問題

- インターネットアクセスがない場合、VDAのインストールと同時にCitrix Workspaceアプリをインストールしようとすると失敗する可能性があります。回避策として、Citrix Workspaceアプリのインストールをスキップするか、VDAをインストールする前にMicrosoft WebView（Citrix Workspaceアプリの前提条件）をインストールする必要があります。

- VDA で tdica.sys に致命的な例外が発生し、バグチェックコード 0x0000007E を伴うブルースクリーンが表示される場合があります。

2203初期リリースの既知の問題

全般

- アプリバーを起動してから、Windows向けCitrix WorkspaceアプリでConnection Centerメニューを開くと、アプリバーがホストサーバーの下に表示されません。
- Windows 向け Citrix Workspace アプリを使用し、アプリバーを垂直位置で起動すると、バーがスタートメニューまたはシステムクロックトレイを覆います。
- Skype for Business Web App Plug-inをインストールした後、Webカメラが列挙されなかったり、Firefoxの会議ページが自動的に更新されなかったりする場合があります。
- StoreFrontからアプリケーションを起動すると、アプリケーションがフォアグラウンドで起動しないか、フォアグラウンドにはあるもののフォーカスがない場合があります。回避策として、タスクバーのアイコンをクリックしてアプリケーションを前面に表示するか、アプリケーション画面をクリックしてフォーカスを合わせます。
- Windows 10 1809 LTSCを使用している場合、`VCLibs`の依存関係のインストールに失敗します。
- ユーザーがホスト上で既にフォーカスされているコンボボックスを選択すると、コンボボックスが正しく表示されない場合があります。回避策として、別の UI 要素を選択してからコンボボックスを選択してください。
- ローカルアプリアクセスを有効にしている場合、Windows 2012 R2 VDAセッションを開始し、セッションを切断して再接続し、ローカルアプリケーションを開始して最大化すると、VDAタスクバーによってアプリケーションが切り詰められることがあります。
- Azure環境で、ICA®セッションを使用してVDAにログオンする際に、同じデスクトップのシームレスアプリを起動すると、約5分間黒い画面が表示される場合があります。
- Citrix Hypervisor™は、GFS2 SRを使用したMCSフルクローンVMをサポートしていません。
- Citrix Hypervisor 8.2でVMがホストされているCitrix Virtual Apps and Desktops展開で、単一のMCSカタログに複数のGFS2 SRを使用している場合、展開中にカタログ内のVMがVDIにアクセスできません。「VDI is currently in use」というエラーが報告されます。
- Microsoft Office 365ビルド16.0.7967以降のアプリケーションがWindows Server 2019ホストからアプリケーションとして公開されている場合、Officeライセンスのアクティベーションが失敗します。Citrixは、このMicrosoftの制限に対処するためMicrosoftと協力しています。サポートされている回避策は、問題のあるWeb Authentication Managerコンポーネントがないwindows Server 2016 VDAをインストールすることです。

- グループポリシーの評価が失敗すると、Session Managerはセッションの起動を終了します。これは、グループポリシーによって制限されているリソースへのユーザーアクセスを防ぐためです。以下のユーザーが実装した修正は、管理者が強制を解除するためのレジストリトグルを提供し、グループポリシーの評価が失敗した場合でもエンドユーザーがセッションに接続できるようにします。

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Ica\GroupPolicy

  名前: EnforceUserPolicyEvaluationSuccess

  種類: REG_DWORD

  値: 0 (現在の修正を有効にします)

- マルチセッションOS VDAで実行されているターミナルサービスが断続的に終了する場合があります。システムイベントログにイベントID 7011が次のメッセージとともに記録されます:

  TermServiceサービスからのトランザクション応答を待機中にタイムアウト (30000ミリ秒) に達しました。

- 8つ以上のHDXオーディオデバイスを有効にしているクライアントからシングルセッションのRemotePCまたはワークステーションVirtual Delivery Agent (VDA) に接続すると、High Definition Experience (HDX) オーディオデバイスが無効になります。回避策として、次のいずれかを選択してください:

  - 8つ未満のHDXオーディオデバイスを有効にしているクライアントから、シングルセッションのRemotePCまたはワークステーションVDAに接続します。
  - シングルセッションのRemotePCまたはワークステーションVDAが起動した後で、HDXオーディオデバイスを有効にします。
  - マルチセッションのRemotePCまたはワークステーションVDAに接続します。

- VDA で tdica.sys に致命的な例外が発生し、バグチェックコード 0x0000007E を伴うブルースクリーンが表示される場合があります。
- 一部のシナリオでは、クライアントIPポリシーフィルターを使用すると、ポリシーの評価に使用されるIPアドレスが正しくありません。

スタジオ

- サイト作成中に、ハイブリッドライセンスを有効にするライセンスを追加した後、サイト作成が完了するまで、パブリッククラウドホスト (Microsoft Azure、Google Cloud Platform、Amazon Web Servicesなど) は接続タイプリストに表示されません。

ディレクター

- **Citrix Director > Machine Details** の **Console** リンクは、Microsoft Edge 44およびFirefox 68 ESRブラウザではマシンコンソールを起動しません。

グラフィック

- 最小化されたアプリを共有すると、アプリのタイトルバーも共有される場合があります。
- ポリシー **ドラッグ中のウィンドウコンテンツの表示** を **禁止** に設定しても、ESXiおよびHyper-Vでは機能しません。
- Theora圧縮を使用して64ビットのWebカメラアプリでビデオプレビューを開始すると、セッションがクラッシュする可能性があります。
- 一部のアプリケーションは、デフォルトの最大30 FPSではなく、最大22フレーム/秒 (FPS) に制限されます。修正は2203 LTSR CU2で利用可能になります。回避策として、VDAで次のレジストリ値を設定してください:

  - キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
  - 値: EnableTimerPeriod = 1

  設定を有効にするには、セッションを切断して再起動する必要があります。

印刷

- 仮想デスクトップで選択されたUniversal Print Serverプリンターは、コントロールパネルの**デバイスとプリンター**ウィンドウに表示されません。ただし、ユーザーがアプリケーションで作業している場合、それらのプリンターを使用できます。この問題は、Windows Server 2012、Windows 10、およびWindows 8でのみ発生します。詳細については、CTX213540を参照してください。
- 印刷ダイアログウィンドウでデフォルトプリンターが正しくマークされない場合があります。この問題は、デフォルトプリンターに送信される印刷ジョブには影響しません。

マシンクリエーションサービス™ (MCS)

- GCP環境では、プロビジョニングスキームのカスタムプロパティを更新しても、カタログに新しく追加されたマシンには変更が適用されません。この問題を解決するには、プロビジョニングスキームのカスタムプロパティを更新した後、カタログ用に新しい更新済みイメージを作成します。
- カスタムプロパティを持つカタログを作成し、`Set-ProvScheme`を使用してカタログ作成時に設定されたカスタムプロパティと同じものを更新せずにプロビジョニングスキームを変更すると、`Set-ProvScheme`に記載されていないプロパティはデフォルト値に設定されます。ま

た、カタログ作成時にカスタムプロパティをデフォルト以外の値に設定した場合でも、`Set-ProvScheme`を実行するとデフォルト値に上書きされます。

サードパーティの問題

- Chromeは、ウェブページ周辺のツールバー、タブ、メニュー、ボタンに対してのみUIオートメーションをサポートします。このChromeの問題により、タッチデバイス上のChromeブラウザでは、自動キーボード表示機能が動作しない場合があります。回避策として、`chrome --force-renderer-accessibility`を実行するか、新しいブラウザタブを開いて`chrome://accessibility`と入力し、特定のページまたはすべてのページで**Native accessibility API**のサポートを有効にすることができます。さらに、シームレスアプリを公開する際、`--force-renderer-accessibility`スイッチを使用してChromeを公開できます。
- ブラウザコンテンツリダイレクトで、YouTube HTML5ビデオプレーヤーを使用してYouTubeビデオを開始した後、全画面表示モードが機能しない場合があります。ビデオの右下隅にあるアイコンをクリックしても、ビデオのサイズが変更されず、ページ全体に黒い背景が残ります。回避策として、全画面ボタンをクリックしてからシアターモードを選択してください。

廃止予定と削除

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

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

非推奨

非推奨の項目はすぐに削除されません。Citrixは引き続きそれらをサポートしますが、将来のリリースで削除されます。

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
ファイルベースのライセンス	2507	---	License Activation Service (LAS)は、Citrix製品スイート全体での製品アクティベーションのための次世代テクノロジーです。ファイルベースのライセンスを使用しているお客様は、April 15, 2026までに互換性のあるリリースにアップグレードし、このテクノロジー移行を実行する必要があります。April 15, 2026以降、LASがCitrixオンプレミスコンポーネントをアクティベートおよびライセンス供与する唯一の方法となります。
WebRTC SDP形式 (Plan B) のサポート	2308	---	Citrix Workspace™ Appをサポートされているバージョンにアップグレードしてください。
Microsoft Teams最適化におけるシングルウィンドウモードのサポート	2308	---	Citrix WorkspaceアプリをMultiWindowモードをサポートするバージョンにアップグレードします。詳しくは、「機能マトリックスとバージョンサポート」を参照してください。

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
Citrix Provisioningターゲットデバイスを管理のためにCitrix Virtual Apps and Desktops™カタログにインポートする	1912 LTSR	-	Citrix Provisioningデバイスのエクスポートウィザードを使用します。
ホストからクライアントへの（URL）リダイレクト	2203	---	---
クラウドおよびオンプレミス環境で使用される4つのAWS固有のコマンド（`Revoke-HypSecurityGroupIngress`、`Revoke-HypSecurityGroupEgress`、`Grant-HypSecuritygroupegress`、および`Grant-HypSecurityGroupIngress`）のサポート。	2203		
VDAメタインストーラーからのCitrix Files for WindowsおよびCitrix Files for Outlook。	2203		スタンドアロンインストーラーを使用します。
VDAメタインストーラーからのWEMエージェントコンポーネント。	2203		

項目	非推奨が発表されたバージョン	削除されたバージョン	代替
リモートPCアクセス用のSCCM統合Wake on LANオプション。	2012		スタンドアロンのWake on LAN機能を使用します。
XenAppおよびXenDesktop、Provisioning Services、StoreFront用のCitrix SCOM管理パック。監視できる製品バージョンについては、「Citrix SCOM管理パックのドキュメント」を参照してください。	1912		Directorを使用して展開を監視および管理します。SCOM EOLと代替の詳細については、(https://support.citrix.com/article/CTX266943)を参照してください。
モビリティ SDK / モバイル SDK (旧シトリックスラボ製)	7.16		モバイルエクスペリエンスポリシー設定、およびホスト型デスクトップ/アプリのネイティブエクスペリエンスに置き換えられました。

削除された機能

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

項目	廃止が発表されたバージョン	削除されたバージョン	代替
Citrix License Administration Console (Windows License Server 11.16.3 build 30000に最後に含まれ、	2003	2006	Citrix Licensing Managerを使用してください。

項目	廃止が発表されたバージョン	削除されたバージョン	代替
Windows License Server v11.16.6 build 31000で削除されました)。			
Windows 10バージョン1709以前でのCitrix Indirect Display Driver (IDD) グラフィックアダプターのサポート。	2003	2003	Citrix Virtual Apps and Desktops 7 1912 LTSR VDAを使用します。
GRID 9以前のディスプレイドライバーを使用するNvidia GPU (NVENC) によるハードウェアエンコード。	2003	2003	Citrix Virtual Apps and Desktops 7 2003以降のVDAでGRID 10ディスプレイドライバーを使用するか、Citrix Virtual Apps and Desktops 7 1912 LTSR VDAを使用します。
セルフサービスパスワードリセット (SSPR) 機能。	2003	2006	
VDAおよびコアサーバーコンポーネントのバージョン4.8より前のMicrosoft .NET Frameworkバージョンのサポート。Delivery Controller、Studio、Director、StoreFrontが含まれます。	1912	2003	.NET Framework バージョン4.8にアップグレードします。
Windows Server 2012 R2 で動作するVDA。	1912	2003	サポートされているオペレーティングシ

項目	廃止が発表されたバージョン	削除されたバージョン	代替
			ステムにVDAをインストールします。
Citrix Virtual Apps and Desktops Premium edition の AppDNA® アプリケーション移行コンポーネント。	1909	2003	
32ビット (x86) マシンへのStudioのインストール。	1909	2003	サポートされているx64オペレーティングシステムにインストールします。
シームレスアプリケーションでのExcelフックのサポート。これは、Microsoft Excel 2010の各ワークブックに個別のタスクバーアイコンを作成するために使用されていました。	1909	1909	
Windows Server 2012 R2 (Service Packを含む) 上のコアサーバーコンポーネント。以下が含まれます: Delivery Controller™、Studio、Director。	1906	2003	より新しいサポート対象のオペレーティングシステムにインストールしてください。
Microsoft SQL Server 2008 R2、2012、2014の各バージョン (すべての Service Packおよびエディションを含む) におけるサイト構	1906	2003	サポートされている Microsoft SQL Serverバージョンにデータベースをインストールします。

項目	廃止が発表されたバージョン	削除されたバージョン	代替
成、構成ログ、および監視データベースのサポート。			
x86プラットフォーム上のWindows 10でのVDAのサポート。	1906	1909*	サポートされているx64オペレーティングシステムにVDAをインストールします。*この機能は、Citrix Virtual Apps and Desktops 7 1912 LTSRで引き続きサポートされています。
Citrix Virtual Apps and Desktopsインストールメディアからのの削除。	1903	1906	
StoreFront内の以下のサポート終了製品（VDI-in-a-Box、XenMobile（9.0以前））に対するDelivery Controllerオプションの削除。	1903	1903	
Red Hat Enterprise Linux/CentOS 7.5でのLinux VDAのサポート。	1903	1903	Red Hat Enterprise Linux の以降のバージョンに Linux VDA をインストールします。
Citrix Virtual Apps and Desktops（旧XenAppおよびXenDesktop）とCitrix Receiver、およびWorkspace Hub	7.17	2203	Citrix Receiver を TLS 1.2 プロトコルをサポートする Citrix Workspace アプリにアップグレードしてください。

項目	廃止が発表されたバージョン	削除されたバージョン	代替
間のTLS 1.0およびTLS 1.1プロトコルに対するStoreFrontのサポート。			Citrix Workspace アプリの詳細については、https://docs.citrix.com/ja-jp/citrix-workspace-app を参照してください。
Desktop Appliance サイト上のデスクトップにユーザーがアクセスするためのStoreFront サポート	1811	1912	ドメインに参加していないユースケースには、Desktop Lock を使用してください。
Framehawk ディスプレイリモートテクノロジーのサポート	1811	1903	adaptive transport を有効にして Thinwire を使用してください。
すべての Citrix Virtual Apps and Desktops (および XenApp and XenDesktop) バージョンにおける Citrix Smart Scale のサポート。この機能は、31 May 2019 にサポート終了となります。	1808	1906	電源管理機能の向上のため、Citrix Cloud 上の Virtual Apps and Desktops Service の使用を検討してください。
Citrix StoreFront、Citrix VDA、Citrix Studio、Citrix Director、および Citrix Delivery Controller による Microsoft .NET Framework バージョン 4.5.1、4.5.2、4.6、4.6.1、4.6.2、	7.18	1808	.NET Framework バージョン 4.7.1 以降にアップグレードします。(インストーラーは、.NET Framework 4.7.1 がまだインストールされていない場合、自

項目	廃止が発表されたバージョン	削除されたバージョン	代替
および 4.7 のサポート。			動的にインストールします。)
Red Hat Enterprise Linux 7.3 上の Linux VDA のサポート。	7.18	1808	Red Hat Enterprise Linux の以降のバージョンに Linux VDA をインストールします。
ポリシー設定「インボックスプリンタードライバーの自動インストール」に対する VDA サポート。	7.16	7.16	なし。このポリシー設定は、以前の OS (Windows 7、Windows Server 2012 R2 以前) 上の VDA でのみサポートされます。
SUSE Linux Enterprise Server 11 Service Pack 4 上での Linux VDA のサポート。	7.16	7.16	サポートされている SUSE バージョンに Linux VDA をインストールします。
VDA での Citrix WDDM ドライバーのサポート	7.16	7.16	Citrix WDDMドライバーは、VDAとともにインストールされなくなりました。
Windows 10バージョン1511（Threshold 2）およびそれ以前のWindowsシングルセッションOSリリース（Windows 8.xおよびWindows 7を含む）上のVDA（`<https://www.citrix.com/blogs/2018/01/08/the-citrix-strategy-for-`	7.15 LTSR（および7.12）	7.16	Windows 10の最小バージョン1607（Redstone 1）以降の半期チャネルにシングルセッションOS VDAをインストールします。1607 LTSBを使用している場合は、7.15 VDAをお勧めします。CTX224843を参照してください。

項目	廃止が発表されたバージョン	削除されたバージョン	代替
`windows-7-virtual-desktop-users/>` を参照）。			
Windows Server 2008 R2およびWindows Server 2012（Service Packを含む）上のVDA	7.15 LTSR（および7.12）	7.16	サポートされているオペレーティングシステムにVDAをインストールします。
デスクトップコンポジションリダイレクト（以前はDirectX Command Remotingとして知られていた）（DCR）	7.15 LTSR	7.16	Thinwireを使用します。
Citrix Receiver for Webクラシックエクスペリエンス（「グリーンバブル」ユーザーインターフェイス）	7.15 LTSR (およびStoreFront 3.12)	1903	Citrix Receiver for Web の統合エクスペリエンス。
Windows Server 2012 およびWindows Server 2008 R2 (Service Pack を含む) 上のコアコンポーネント。含まれるもの: Delivery Controller、Studio、Director、StoreFront、License Server、Universal Print Server。	7.15 LTSR	7.18	サポートされているオペレーティングシステムにコンポーネントをインストールします。
Windows Server 2012 およびWindows Server 2008 R2 (Service	7.15 LTSR	7.18	より新しいサポート対象のオペレーティングシステムにイン

項目	廃止が発表されたバージョン	削除されたバージョン	代替
Pack を含む) 上のセルフサービスパスワードリセット (SSPR) 機能			ストールしてください。
Windows 7、Windows 8、および Windows 8.1 (Service Pack を含む) 上の Studio	7.15 LTSR	7.18	サポートされているオペレーティングシステムに Studio をインストールします。
Flashリダイレクト	7.15 LTSR	1912	ビデオコンテンツをHTML5ビデオとして作成します。管理対象コンテンツにはHTML5ビデオリダイレクトを使用し、公開Webサイトにはブラウザコンテンツリダイレクトを使用します。詳細については、Flash Redirection End of Lifeの注記を参照してください。
StoreFrontとのCitrix Online統合 (Goto製品)	7.14 (および StoreFront 3.11)	StoreFront 3.12	
VDAのインストール中に作成され、VDAマシンのローカル管理者グループに追加されたユーザーアカウント CtxAppVCOMAdmin は、作成されなくなりました。基盤となる「COM」メカニズ	7.14	7.14	Windowsサービス CtxAppVServiceは同じ機能を実行します。これは自動的にインストールおよび構成され、ユーザーによる操作は不要です。

項目	廃止が発表されたバージョン	削除されたバージョン	代替
ムも削除されました。			
Windows Server 2008 32ビット版でのUniversal Print Server UpsServerコンポーネントのサポート	7.14	7.14	より新しいサポート対象のオペレーティングシステムにインストールしてください。
インターネットエクスプローラー 8 でのストアフロント および レシーバー・フォー・ウェブ	7.13	7.13	
Citrix App-Vコンポーネントのインストールを防止するためのVDAコマンドラインインストールオプション /no_appv	7.13	7.13	コマンドラインインストールオプション /exclude "Citrix Personalization for App-V – VDA" を使用します。
フルプロダクトインストーラーは、新規インストール時にCitrix.Common.Commandsスナップインをインストールしなくなり、既存のインストールをアップグレードする際に自動的に削除します。	7.13	7.13	Citrix.Common.Commandsスナップインによって提供されていた一部のPowerShellコマンドは、XenApp 6.5 SDKで引き続き利用可能です。
*-CtxIconコマンドレットによって提供されていた、アイコンデータを操作する部分的な機能。	7.13	7.13	現在はBroker Serviceの*-BrokerIconコマンドレットによって提供されています。

項目	廃止が発表されたバージョン	削除されたバージョン	代替
レガシーThinwireモード	7.12	7.16	Thinwireを使用してください。Windows Server 2008 R2でレガシーThinwireモードを使用している場合は、Windows Server 2012 R2またはWindows Server 2016に移行し、Thinwireを使用してください。
StoreFront 2.0、2.1、2.5、および2.5.2からのインプレースアップグレード	7.13	7.16	これらのバージョンのいずれかから、サポートされている新しいバージョンにアップグレードし、その後XenAppおよびXenDesktop 7.16にアップグレードします。
XenDesktop 5.6または5.6 FP1からのインプレースアップグレード	7.12	7.16	XenDesktop 5.6または5.6 FP1の展開を現在のXenDesktopバージョンに移行します。これを行うには、まずXenDesktop 7.6 LTSR（最新のCUを含む）にアップグレードし、その後、最新のCitrix Virtual Desktops（旧XenDesktop）リリースまたはLTSRバージョンにアップグレードします。
32ビット（x86）マシンへのDelivery	7.12	7.16	サポートされているx64オペレーティン

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

項目	廃止が発表されたバージョン	削除されたバージョン	代替
			を使用してください。

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

システム要件

はじめに

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

インストールを開始する前に、インストールの準備を確認してください。

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

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

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

ハードウェア要件

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

次の表に、コアコンポーネントの最小要件を示します。

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

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

デスクトップとアプリケーションを提供するVMのサイジング

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

詳細については、以下を参照してください。

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

マイクロソフト ビジュアル C++

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

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

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

デリバリーコントローラー

サポートされているオペレーティングシステム:

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

要件:

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

データベース

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

- SQL Server 2019、Express、Standard、およびEnterprise エディション。
- SQL Server 2017、Express、Standard、およびEnterprise エディション。
  - 新規インストールの場合: 既存のサポートされているSQL Serverインストールが検出されない場合、デフォルトで、Controllerのインストール時に累積更新プログラム16を含むSQL Server Express 2017がインストールされます。
  - アップグレードの場合、既存のSQL Server Expressバージョンはアップグレードされません。
- SQL Server 2016 SP2、Express、Standard、およびEnterprise エディション。

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

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

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

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

- Controllerをインストールすると、ローカルホストキャッシュ機能で使用するために、累積更新プログラム20を含むMicrosoft SQL Server Express LocalDB 2019がインストールされます。(このインストールは、サイトデータベース用のデフォルトのSQL Server Expressインストールとは別です。)
- コントローラーをアップグレードする際、既存のMicrosoft SQL Server Express LocalDBのバージョンは自動的にアップグレードされません。交換要件と手順については、「SQL Server Express LocalDBの交換」を参照してください。

その他のデータベース情報:

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

シトリックス スタジオ

サポートされているオペレーティングシステム:

- ウィンドウズ サーバー 2022
- Windows Server 2019、StandardおよびDatacenterエディション
- Windows Server 2016、Standard、およびDatacenter エディション。
- ウィンドウズ 11
- Windows 10 (64ビットのみ)

要件:

- Microsoft .NET Framework 4.8（またはそれ以降のバージョン）がまだインストールされていない場合、自動的にインストールされます。
- Microsoft Management Console 3.0 (サポートされているすべてのオペレーティングシステムに含まれています)。
- Windows PowerShell 3.0、4.0、または5.0。

Citrix Director (シトリックス ディレクター)

サポートされているオペレーティングシステム:

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

要件:

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

シトリックス プロファイル マネージメント:

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

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

- ウィンドウズ サーバー 2012 R2
- System Center 2012 R2 オペレーションズマネージャー

Directorの表示でサポートされているブラウザー:

- Internet Explorer 11。Internet Explorerの互換モードはサポートされていません。Directorにアクセスするには、推奨されるブラウザ設定を使用してください。Internet Explorerをインストールする際は、推奨されるセキュリティおよび互換性設定を使用するためにデフォルトを受け入れてください。すでにブラウザをインストールしていて、推奨設定を使用しないことを選択した場合は、**ツール > インターネットオプション > 詳細設定 > リセット**に移動し、指示に従ってください。
- マイクロソフト エッジ。
- Firefox ESR (延長サポート版)。
- クローム。

Directorを表示するための推奨される最適な画面解像度は1366 x 1024です。

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

サポートされているオペレーティングシステム:

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

要件:

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

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

複数のマルチメディアアクセラレーション機能（HDX MediaStream Windows Media Redirectionなど）を使用するには、VDAをインストールするマシンにMicrosoft Media Foundationがインストールされている必要があります。マシンにMedia Foundationがインストールされていない場合、マルチメディアアクセラレーション機能はインストールされず、動作しません。Citrixソフトウェアのインストール後にマシンからMedia Foundationを削除しないでください。削除すると、ユーザーはマシンにログオンできなくなります。ほとんどのサポートされているWindowsシングルセッションOSエディションでは、Media Foundationのサポートはすでにインストールされてお

り、削除できません。ただし、Nエディションには特定のメディア関連テクノロジーが含まれていません。そのソフトウェアはMicrosoftまたはサードパーティから入手できます。詳細については、インストール準備を参照してください。

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

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

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

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

サポートされているオペレーティングシステム:

- Windows 11 (Citrix DaaS™でのみサポート)
- Windows 10 (x64のみ、Citrix DaaSでのみサポート)、現在メインストリームサポート中の任意のバージョン。
- Windows Server 2022、StandardおよびDatacenterエディション
- Windows Server 2019、StandardおよびDatacenterエディション
- Windows Server 2016、StandardおよびDatacenterエディション

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

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

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

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

Foundation機能はサーバーマネージャーを通じてインストールされます。詳細については、インストール準備を参照してください。

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

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

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

サポート対象外のWindowsオペレーティングシステムにVDAをインストールする方法については、「以前のオペレーティングシステム」(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/upgrade-migrate/upgrade.html#earlier-operating-systems)を参照してください。

ホスト / 仮想化リソース

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

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

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

サポートされているハイパーバイザー:

- **シトリックス ハイパーバイザー™ (旧称 XenServer (XenServer))**

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

  詳しくは、Citrix Hypervisor仮想化環境を参照してください。
- **マイクロソフト システム センター バーチャル マシン マネージャー**

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

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

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

- **Nutanix アクロポリス**

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

  詳細については、Nutanix仮想化環境を参照してください。

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

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

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

  詳細については、VMware仮想化環境を参照してください。

サポートされているパブリッククラウドホスト:

- **アマゾン ウェブ サービス (AWS)**

  AWSを使用して仮想マシンをプロビジョニングする方法については、Citrix DaaSドキュメントのAmazon Web Services仮想化環境セクションを参照してください。

- **グーグル クラウド プラットフォーム**

  Google Cloudを使用して仮想マシンをプロビジョニングする方法については、Citrix DaaSドキュメントのGoogle Cloud環境セクションと展開ガイドを参照してください。

- **マイクロソフト アジュール リソース マネージャー**

  Microsoft Azure Resource Managerを使用して仮想マシンをプロビジョニングする方法については、Citrix DaaSドキュメントのMicrosoft Azure Resource Manager仮想化環境セクションを参照してください。

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

- ハイブリッド権限ライセンスが必要です。ハイブリッド権限ライセンスについては、「ハイブリッド権限による移行とアップグレード (TTU)」を参照してください。ライセンスの追加については、「サイトの作成」を参照してください。
- 情報源は Citrix DaaS のドキュメントを参照しています。Citrix DaaS 製品のパブリッククラウドホストに精通している場合でも、オンプレミスバージョンとはいくつかの違いがあります。
  - Citrix DaaSでは、管理インターフェイスは「完全な構成」として知られています。オンプレミスのCitrix Virtual Apps and Desktops™では、管理インターフェイスは「Citrix Studio」として知られています。

- Citrix DaaS への更新は、約4週間ごとに展開されます。そのため、Citrix DaaS で利用できる特定の機能がオンプレミスバージョンでは利用できない場合があります。

Active Directoryの機能レベル

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

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

> **注：**

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

HDX

オーディオ

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

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

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

HDX Windows Media の配信

Windows Mediaクライアント側コンテンツフェッチ、Windows Mediaリダイレクト、およびリアルタイムWindows Mediaマルチメディアトランスコーディングには、Windows向けCitrix

Workspaceアプリ、iOS向けCitrix Workspaceアプリ、およびLinux向けCitrix Workspaceアプリがサポートされています。

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

HDX 3D Pro 機能

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

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

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

`<https://www.citrix.com/products/xenapp-xendesktop/hdx-3d-pro.html>`を参照してください。

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

グラフィック処理ユニット (GPU):

- CPUベースの圧縮（ロスレス圧縮を含む）の場合、HDX 3D Proは、提供されるアプリケーションと互換性のあるホストコンピューター上の任意のディスプレイアダプターをサポートします。
- NVIDIA GRID APIを使用した仮想グラフィックアクセラレーションの場合、GRID 10ドライバーでサポートされているすべてのNVIDIA GRID GPUでHDX 3D Proを使用できます（NVIDIA GRIDを参照）。NVIDIA GRIDは高いフレームレートを提供し、非常にインタラクティブなユーザーエクスペリエンスを実現します。
- 仮想グラフィックアクセラレーションは、Intel Xeon Processor E3ファミリーのデータセンターグラフィックプラットフォームでサポートされています。詳細については、`<https://www.citrix.com/intel>` および `<https://www.intel.com/content/www/us/en/servers/data-center-graphics.html>` を参照してください。
- 仮想グラフィックアクセラレーションは、AMD FirePro Sシリーズサーバーカード上のAMD RapidFireでサポートされています。AMD Virtualization Solution) を参照してください。

ユーザーデバイス:

- HDX 3D Proは、ホストコンピューターのGPUでサポートされているすべてのモニター解像度をサポートしています。最小推奨ユーザーデバイスおよびGPU仕様で最適なパフォーマンスを得るには、CitrixはLAN接続で最大1920 x 1200ピクセル、WAN接続で1280 x 1024ピクセルのモニター解像度を推奨しています。
- Citrixは、ユーザーデバイスに少なくとも1 GBのRAMと1.6 GHz以上のクロック速度を持つCPUを搭載することを推奨しています。低帯域幅接続で必須となるデフォルトのディープ圧縮コーデックを使用する場合、ハードウェアでデコードが行われない限り、より強力なCPUが必要です。最適なパフォーマンスを得るには、Citrixはユーザーデバイスに少なくとも2 GBのRAMと3 GHz以上のクロック速度を持つデュアルコアCPUを搭載することを推奨しています。
- マルチモニターアクセスの場合、Citrixはクアッドコアcpuを搭載したユーザーデバイスを推奨します。
- ユーザーデバイスは、HDX 3D Proで配信されるデスクトップまたはアプリケーションにアクセスするためにGPUを必要としません。
- Citrix Workspaceアプリがインストールされている必要があります。

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

ユニバーサル プリント サーバー

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

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

UpsServerコンポーネントは以下でサポートされています。

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

要件:

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

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

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

詳しくは、「プリンターのプロビジョニング」を参照してください。

その他

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

このリリースでCitrix Provisioning（旧Provisioning Services）を使用する場合、バージョン7.xは、XenAppおよびXenDesktop 7.xのライフサイクルとCitrix Virtual Apps and Desktopsのライフサイクルによってカバーされます。バージョンの互換性に関する詳細については、製品マトリックス を参照してください。

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

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

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

複数のNICがサポートされています。

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

Microsoft App-Vのサポートされているバージョンについては、App-V を参照してください。

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

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

この製品はPowerShellバージョン3から5をサポートしています。

技術概要

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

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

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

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

主要コンポーネント

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

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

一般的な展開における主要コンポーネント(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/components-new-op.png)

デリバリーコントローラー™

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

- アプリケーションとデスクトップを配信する

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

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

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

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

Controllerはデスクトップの状態を管理し、需要と管理構成に基づいてそれらを起動および停止します。一部のエディションでは、ControllerはProfile Managementをインストールして、仮想化または物理Windows環境でのユーザーのパーソナライズ設定を管理できます。

データベース

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

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

仮想配信エージェント (VDA)

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

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

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

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

シトリックス ストアフロント™

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

シトリックス ワークスペース™ アプリ

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

シトリックス スタジオ

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

Studioは、コントローラー内のブローカーサービスから表示する情報を取得し、TCPポート80を介して通信します。

Citrix Director (シトリックス ディレクター)

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

Directorは以下を表示します。

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

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

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

Citrix ライセンスサーバー

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

ハイパーバイザーまたはその他のサービス

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

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

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

追加コンポーネント

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

シトリックス プロビジョニング™

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

シトリックス ゲートウェイ

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

シトリックス SD-WAN™

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

一般的な展開の仕組み

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

展開におけるコンポーネント間の通信(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/deployment-overview.png)

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

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

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

ユーザー接続の処理方法

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

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

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

ユーザー接続フロー(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/user-connections.png)

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

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

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

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

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

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

データアクセスが機能する仕組み

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

展開におけるデータアクセス(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/data-access.png)

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

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

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

デスクトップとアプリケーションの配信

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

マシンカタログ

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

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

有効なマシンタイプは次のとおりです。

- **マルチセッションOS：** マルチセッションオペレーティングシステムを搭載した仮想マシンまたは物理マシン。Citrix Virtual Apps公開アプリ（サーバーベースのホスト型アプリケーションとも呼ばれる）およびCitrix Virtual Apps公開デスクトップ（サーバーホスト型デスクトップとも呼ばれる）の配信に使用されます。これらのマシンでは、複数のユーザーが同時に接続できます。
- **シングルセッションOS：** シングルセッションオペレーティングシステムを搭載した仮想マシンまたは物理マシン。VDIデスクトップ（オプションでパーソナライズできるシングルセッションOSを実行するデスクトップ）、VMホスト型アプリ（シングルセッションOSからのアプリケーション）、およびホスト型物理デスクトップの配信に使用されます。これらのデスクトップには、一度に1人のユーザーしか接続できません。

- **Remote PC Access：** リモートユーザーがCitrix Workspaceアプリを実行している任意のデバイスから物理オフィスPCにアクセスできるようにします。オフィスPCはCitrix Virtual Desktops展開を通じて管理され、ユーザーデバイスは許可リストで指定する必要があります。

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

デリバリーグループ

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

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

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

詳細については、「デリバリーグループの作成」を参照してください。

アプリケーショングループ

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

詳細については、「」(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/install-configure/application-groups-create.html)を参照してください。

詳細情報

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

アクティブディレクトリ

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

「システム要件」の記事には、フォレストとドメインでサポートされている機能レベルが記載されています。ポリシーモデリングを使用するには、ドメインコントローラーがWindows Server 2003からWindows Server 2012 R2で実行されている必要があります。これは、ドメインの機能レベルには影響しません。

この製品は以下をサポートします。

- **ユーザーアカウントとコンピューターアカウントが単一のActive Directoryフォレスト内のドメインに存在する展開。** ユーザーアカウントとコンピューターアカウントは、単一フォレスト内の任意のドメインに存在できます。この種類の展開では、すべてのドメイン機能レベルとフォレスト機能レベルがサポートされます。
- **ユーザーアカウントが、Controllerおよび仮想デスクトップのコンピューターアカウントを含むActive Directoryフォレストとは異なるActive Directoryフォレストに存在する展開。** この種類の展開では、Controllerおよび仮想デスクトップのコンピューターアカウントを含むドメインは、ユーザーアカウントを含むドメインを信頼する必要があります。フォレストの信頼または外部の信頼を使用できます。この種類の展開では、すべてのドメイン機能レベルとフォレスト機能レベルがサポートされます。
- **Controllerのコンピューターアカウントが、仮想デスクトップのコンピューターアカウントを含む1つ以上の追加のActive Directoryフォレストとは異なるActive Directoryフォレストに存在する展開。** この種類の展開では、Controllerのコンピューターアカウントを含むドメインと、仮想デスクトップのコンピューターアカウントを含むすべてのドメインとの間に双方向の信頼が存在する必要があります。この種類の展開では、Controllerまたは仮想デスクトップのコンピューターアカウントを含むすべてのドメインが「Windows 2000ネイティブ」機能レベル以上である必要があります。すべてのフォレスト機能レベルがサポートされます。

- **書き込み可能なドメインコントローラー。** 読み取り専用ドメインコントローラーはサポートされていません。

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

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

複数のActive Directoryフォレスト環境での展開

この情報は、最小バージョンXenDesktop 7.1およびXenApp 7.5に適用されます。XenDesktopまたはXenAppの以前のバージョンには適用されません。

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

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

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

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

> は、お客様ご自身の責任において行ってください。編集する前にレジストリをバックアップしてください。

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

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

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

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

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

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

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

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

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

セットアップ中に外部信頼が設定されている場合、`ListOfSIDs` レジストリキーが必要です。Active Directory FQDNがDNS FQDNと異なる場合、またはドメインコントローラーを含むドメイ

ンのNetBIOS名がActive Directory FQDNと異なる場合、`ListOfSIDs`レジストリキーも必要です。レジストリキーを追加するには、以下の情報を使用します:

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

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

外部信頼が設定されている場合、VDAで次の変更を行います:

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

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

次の表に、サポートされている信頼の種類を示します。

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

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

データベース

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

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

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

データベースサーバーに障害が発生した場合にバックアップから復元できるように、Citrixではデータベースを定期的にバックアップすることをお勧めします。各データベースのバックアップ戦略は異なる場合があります。手順については、CTX135207を参照してください。

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

高可用性

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

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

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

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

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

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

データベースソフトウェアのインストール

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

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

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

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

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

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

サイト作成ウィザードからデータベースをセットアップする

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

データベースページでは、データベースを設定するための2つのオプション（自動とスクリプトの使用）が提供されます。通常、必要なデータベース権限がある場合（StudioユーザーおよびCitrix®管理者）は、自動オプションを使用できます。（データベースを設定するために必要な権限を参照してください。）

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

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

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

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

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

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

自動セットアップ

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

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

スクリプトによるセットアップ

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

1. サイト作成ウィザードの ページで、 を選択します。この操作により、サイト、監視、ログの各データベースについて、プライマリデータベースとレプリカデータベースごとに次の3種類のスクリプトが生成されます。
    - *名前に「SysAdmin」を含むスクリプト*。データベースとDelivery Controllerのログインを作成するスクリプト。これらのタスクにはsecurityadmin権限が必要です。
    - *名前に「DbOwner」を含むスクリプト*。データベースにユーザーロールを作成し、ログインを追加し、データベーススキーマを作成するスクリプト。これらのタスクには `db_owner` 権限が必要です。
    - *名前に「Mixed」を含むスクリプト*。必要な権限に関係なく、すべてのタスクを1つのスクリプトにまとめたもの。

スクリプトの保存場所を指定できます。

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

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

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

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

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

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

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

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

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

データベースのセットアップに必要な権限

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

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

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

** Studioを介して、またはStudioやSDKによって生成されたスクリプトを使用してコントローラーがサイトから削除されても、データベースサーバーへのコントローラーのログオンは削除されません。これは、同じマシン上でこのCitrix製品以外のサービスによって使用されているログオンを誤って削除することを避けるためです。ログオンが不要になった場合は、手動で削除する必要があります。この操作には`securityadmin`サーバーロールのメンバーシップが必要です。

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

優先データベース権限スクリプト

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

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

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

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

詳細については、コマンドレットのヘルプを参照してください。

データベースアドレスの形式

データベースアドレスは、次のいずれかの形式で指定できます。

- `ServerName`

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

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

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

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

データベースの場所を変更する

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

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

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

データベースの場所を変更するには：

1. データベースを配置するサーバーに、サポートされているバージョンのMicrosoft SQL Serverがインストールされていることを確認してください。必要に応じて、高可用性機能をセットアップします。
2. Studioナビゲーションペインで、**構成**を選択します。
3. 新しい場所を指定するデータベースを選択し、**アクション**ペインで**データベースの変更**を選択します。
4. 新しい場所とデータベース名を指定します。
5. Studioにデータベースを作成させたい場合で、適切な権限がある場合は、**OK**をクリックします。プロンプトが表示されたら**OK**をクリックすると、Studioが自動的にデータベースを作成します。Studioは、あなたの資格情報を使用してデータベースへのアクセスを試みます。それが失敗した場合、データベースユーザーの資格情報の入力を求められます。その後、Studioはデータベーススキーマをデータベースにアップロードします。資格情報は、データベース作成期間中のみ保持されます。

6. Studioにデータベースを作成させたくない場合、または十分な権限がない場合は、**スクリプトの生成**をクリックします。生成されたスクリプトには、必要に応じてデータベースとミラーデータベースを手動で作成するための手順が含まれています。スキーマをアップロードする前に、データベースが空であり、少なくとも1人のユーザーがデータベースにアクセスして変更する権限を持っていることを確認してください。

詳細情報

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

配信方法

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

はじめに

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

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

- **ホスト型Windowsアプリ:** マルチユーザーのCitrix Virtual Appsホストにインストールされ、デスクトップではなくアプリケーションとして展開されるアプリケーションです。ユーザーはVDIデスクトップまたはエンドポイントデバイスからホスト型Windowsアプリにシームレスにアクセスでき、アプリがリモートで実行されているという事実を意識することはありません。詳細については、「デリバリーグループの作成」を参照してください。
- **ローカルアプリ:** エンドポイントデバイスに展開されるアプリケーションです。アプリケーションインターフェイスは、エンドポイントで実行されているにもかかわらず、ユーザーのホスト型VDIセッション内に表示されます。詳細については、「ローカルアプリアクセスとURLリダイレクト」を参照してください。

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

Citrix Virtual Apps™公開アプリとデスクトップ

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

ユースケース:

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

利点と考慮事項:

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

ユーザーエクスペリエンス:

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

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

アプリケーションの処理、ホスト、および配信:

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

セッション管理と割り当て:

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

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

VMホスト型アプリ

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

ユースケース:

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

利点と考慮事項:

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

ユーザーエクスペリエンス：

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

アプリケーションの処理、ホスト、および配信：

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

セッション管理と割り当て：

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

VDIデスクトップ

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

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

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

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

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

リモートPCアクセス

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

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

詳細については、リモートPCアクセス。

ネットワークポート

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

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

ポート情報が必要になる場合があります。

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

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

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

HDX™

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

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

仮想チャネル(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/hdx-vir-channels.png)

HDXは、次の3つの技術原則に基づいて設計されています。

- インテリジェントリダイレクト
- 適応型圧縮
- データ重複排除

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

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

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

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

  適応型圧縮(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/hdx-adaptive-compression.png)

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

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

デバイス上での動作

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

ネットワーク上

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

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

データセンター内

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

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

HDX インサイト

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

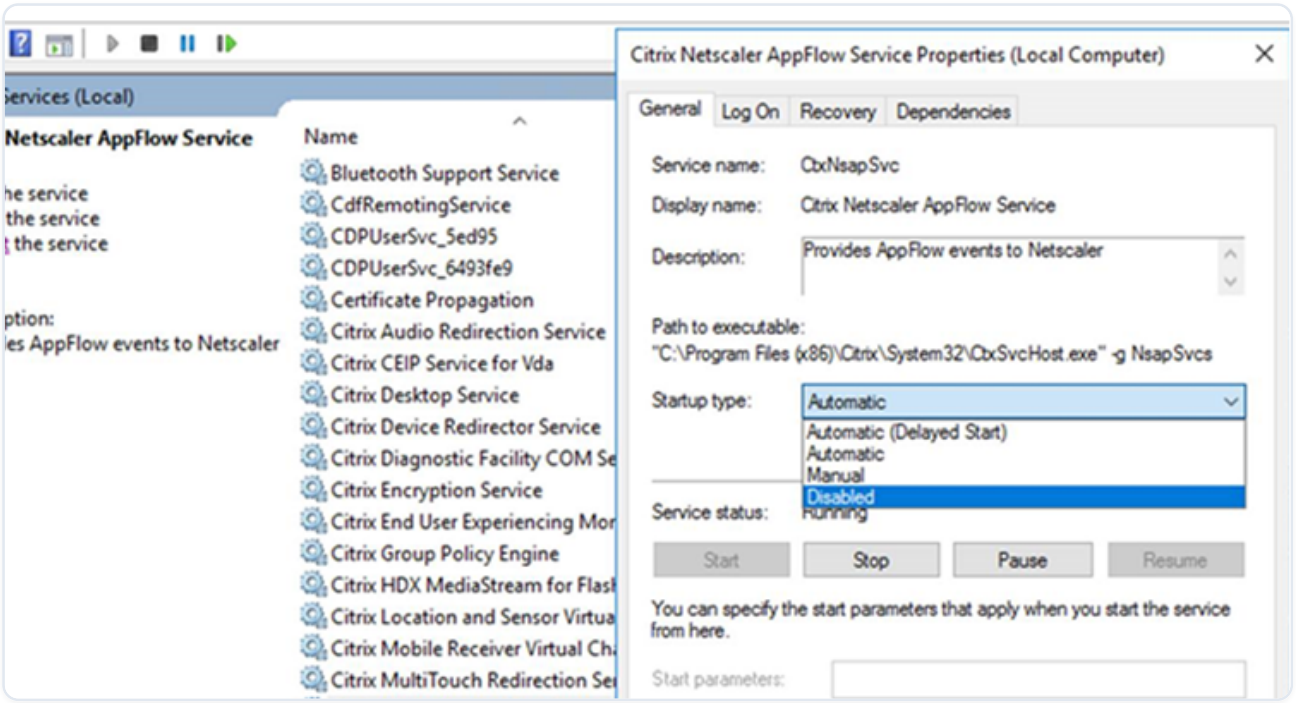
NetScalerでHDX Insight仮想チャネルを使用して、必要なすべてのデータポイントを非圧縮形式で移動させることができます。この機能を無効にすると、NetScalerデバイスは、さまざまな仮想チャネルに分散されたICA®トラフィックを復号化および解凍します。単一の仮想チャネルを使用することで、複雑さが軽減され、スケーラビリティが向上し、費用対効果が高まります。

最小要件:

- シトリックス バーチャルアップス アンド デスクトップス™ 7 v1808
- ゼンアップ アンド ゼンデスクトップ 7.17
- NetScalerバージョン 12.0 Build 57.x
- Windows用Citrix Workspace™アプリ 1808
- Windows用 シトリックス レシーバー 4.10
- Mac用Citrix Workspaceアプリ 1808
- Mac用 シトリックス レシーバー 12.8

HDX Insight仮想チャネルの有効化または無効化

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



仮想デスクトップからHDX機能を利用する

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

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

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

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

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

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

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

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

知っておくと良いこと:

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

自動クライアント再接続とセッションの信頼性

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

自動クライアント再接続:

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

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

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

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

自動クライアント再接続のデフォルト設定：

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

詳細については、(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/policies/reference/ica-policy-settings/auto-client-reconnect-policy-settings.html)のを参照してください。

セッションの信頼性:

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

- **デスクトップ。** セッションウィンドウは半透明になり、再接続までの時間がカウントダウンタイマーで表示されます。

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

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

再接続すると、クライアントとサーバーはプロトコル交換を行っていた同じポイントで再開します。セッションウィンドウは半透明ではなくなり、アプリケーションには適切な通知領域のポップアップが表示されます。

デフォルトのセッションの信頼性設定

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

詳細については、(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/policies/reference/ica-policy-settings/session-reliability-policy-settings.html)のを参照してください。

NetScalerと自動クライアント再接続およびセッションの信頼性:

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

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

HDX アダプティブスループット

HDX アダプティブスループットは、出力バッファを調整することで、ICA セッションのピークスループットをインテリジェントに微調整します。出力バッファの数は、最初は高い値に設定されています。この高い値により、特に高遅延ネットワークにおいて、データがクライアントに迅速かつ効率的に送信されます。これにより、より優れた対話性、高速なファイル転送、スムーズなビデオ再生、高いフレームレートと解像度が提供され、ユーザーエクスペリエンスが向上します。

ICA セッション内のデータストリームがインタラクティブ性に悪影響を与えていないかを判断するために、セッションのインタラクティブ性が常に測定されます。そのような状況が発生した場合、

セッションへの大量データストリームの影響を軽減し、インタラクティブ性を回復させるためにスループットが低下します。

> **重要:**

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

> この機能には、以下の要件があります。

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

ユーザーデバイスに送信される画質の向上

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

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

ビデオ会議のパフォーマンスを向上させる

複数の一般的なビデオ会議アプリケーションは、マルチメディアリダイレクトを介したCitrix Virtual Apps and Desktopsからの配信向けに最適化されています（例: HDX RealTime Optimization Pack）。最適化されていないアプリケーションの場合、HDXウェブカメラビデオ圧縮は、セッション中のビデオ会議におけるウェブカメラの帯域幅効率と遅延耐性を向上させます。このテクノロジーは、専用のマルチメディア仮想チャネルを介してウェブカメラトラフィックをストリー

ミングします。このテクノロジーは、アイソクロナスHDX Plug-n-Play USBリダイレクトサポートと比較して帯域幅の使用量が少なく、WAN接続でもうまく機能します。

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

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

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

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

ネットワークトラフィックの優先順位

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

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

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

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

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

警告:

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

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

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

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

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

リモート言語バーの表示/非表示

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

VDAから言語バー機能のクライアント制御を無効にするには：

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

Unicodeキーボードマッピング

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

Unicode キーボードレイアウトマッピングを有効または無効にする

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

KEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

名前: EnableKlMap

種類: DWORD

値: 1

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

Unicode キーボードレイアウトマッピング互換モードを有効にする

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

HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

名前: DisableWindowHook

種類: DWORD

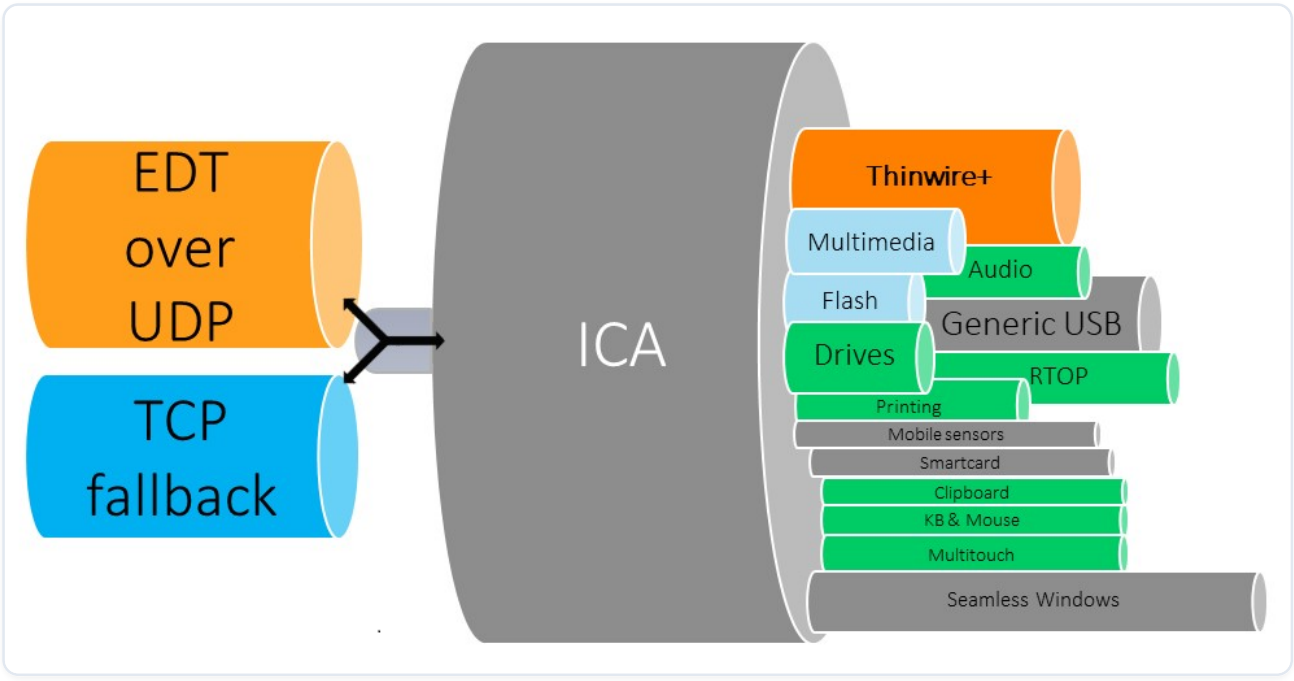
値: 1

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

アダプティブトランスポート

アダプティブトランスポートは、Citrix Virtual Apps and Desktops™のメカニズムであり、ICA接続のトランスポートプロトコルとしてEnlightened Data Transport (EDT)を使用する機能を提供します。EDTが利用できない場合、アダプティブトランスポートはTCPに切り替わります。

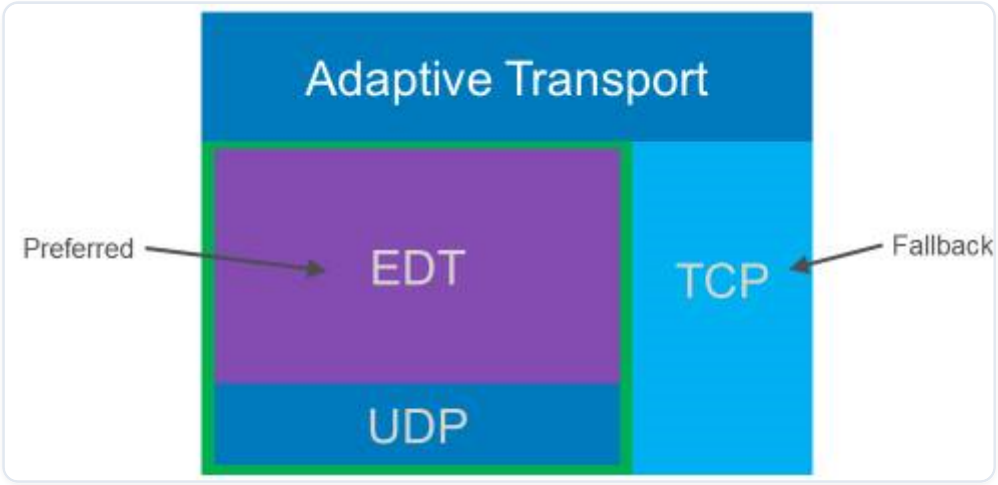
EDTは、User Datagram Protocol (UDP)上に構築されたCitrix独自のトランスポートプロトコルです。サーバーのスケーラビリティを維持しながら、困難な長距離接続で優れたユーザーエクスペリエンスを提供します。EDTは、信頼性の低いネットワーク上のすべてのICA®仮想チャネルのデータスループットを向上させ、より良く、より一貫したユーザーエクスペリエンスを提供します。



アダプティブトランスポートが**優先**に設定されている場合、EDTがプライマリトランスポートプロトコルとして使用され、TCPはフォールバックに使用されます。デフォルトでは、アダプティブトランスポートは**優先**に設定されています。テスト目的でアダプティブトランスポートを**診断モード**に設定できます。これによりEDTのみが許可され、TCPへのフォールバックは無効になります。

Windows、Mac、iOS版のCitrix Workspace™アプリでは、初期接続、セッションの信頼性の再接続、および自動クライアント再接続中に、EDTとTCP接続が並行して試行されます。これにより、基盤となるUDPトランスポートが利用できず、代わりにTCPを使用する必要がある場合、接続時間が短縮されます。アダプティブトランスポートが**優先**に設定されており、TCPを使用して接続が確立された場合、アダプティブトランスポートは5分ごとにEDTへの切り替えを試行し続けます。

LinuxおよびAndroid版のCitrix Workspaceアプリでは、EDT接続が最初に試行されます。接続が失敗した場合、EDT要求がタイムアウトした後、Citrix WorkspaceアプリはTCPを使用して接続を試みます。



システム要件

アダプティブトランスポートとEDTを使用するための要件は次のとおりです。

- コントロールプレーン
  - シトリックス DaaS (旧称: シトリックス バーチャル アプリケーションズ アンド デスクトップ サービス)
  - シトリックス バーチャル アプリケーションズ アンド デスクトップス 1912 以降
- バーチャル デリバリー エージェント
  - バージョン1912以降 (2103以降推奨)
  - バージョン2012は、Citrix Gateway ServiceでEDTを使用するために最低限必要なバージョンです
- StoreFront™
  - バージョン3.12.x
  - バージョン1912.0.x
- シトリックス ワークスペース アプリ
  - Windows: バージョン1912以降 (2105以降推奨)
  - Linux: バージョン1912以降 (2109以降推奨)
  - Mac: バージョン1912以降 (2108以降推奨)
  - iOS: Apple App Storeで入手可能な最新バージョン
  - Android: Google Playで入手可能な最新バージョン
- シトリックス ゲートウェイ (ADC)
  - 13.0.52.24以降
  - 12.1.56.22 以降
- ファイアウォール (VDA の観点から)
  - UDP 1494 インバウンド – セッションの信頼性が無効になっている場合
  - UDP 2598 インバウンド – セッションの信頼性が有効になっている場合
  - UDP 443 インバウンド – ICA 暗号化 (DTLS) 用に VDA SSL が有効になっている場合
  - UDP 443 アウトバウンド – Citrix Gateway Service を使用している場合。詳細については、Citrix Gateway service のドキュメントを参照してください。

考慮事項

- EDT MTU Discovery を使用し、Citrix Gateway および Citrix Gateway Service で EDT を使用するには、セッションの信頼性を有効にします。
- EDT MTU が適切に設定され、フラグメンテーションを回避していることを確認してください。そうしないと、パフォーマンスに影響が出たり、状況によってはセッションが起動しなくなる可能性があります。詳細については、EDT MTU Discover セクションを参照してください。
- Citrix Gateway Service で EDT を使用するための要件と考慮事項の詳細については、HDX Adaptive Transport with EDT support for Citrix Gateway service を参照してください。
- EDT をサポートするための Citrix Gateway の構成の詳細については、Configure Citrix Gateway to support Enlightened Data Transport and HDX Insight を参照してください。
- IPv6 は現在サポートされていません。

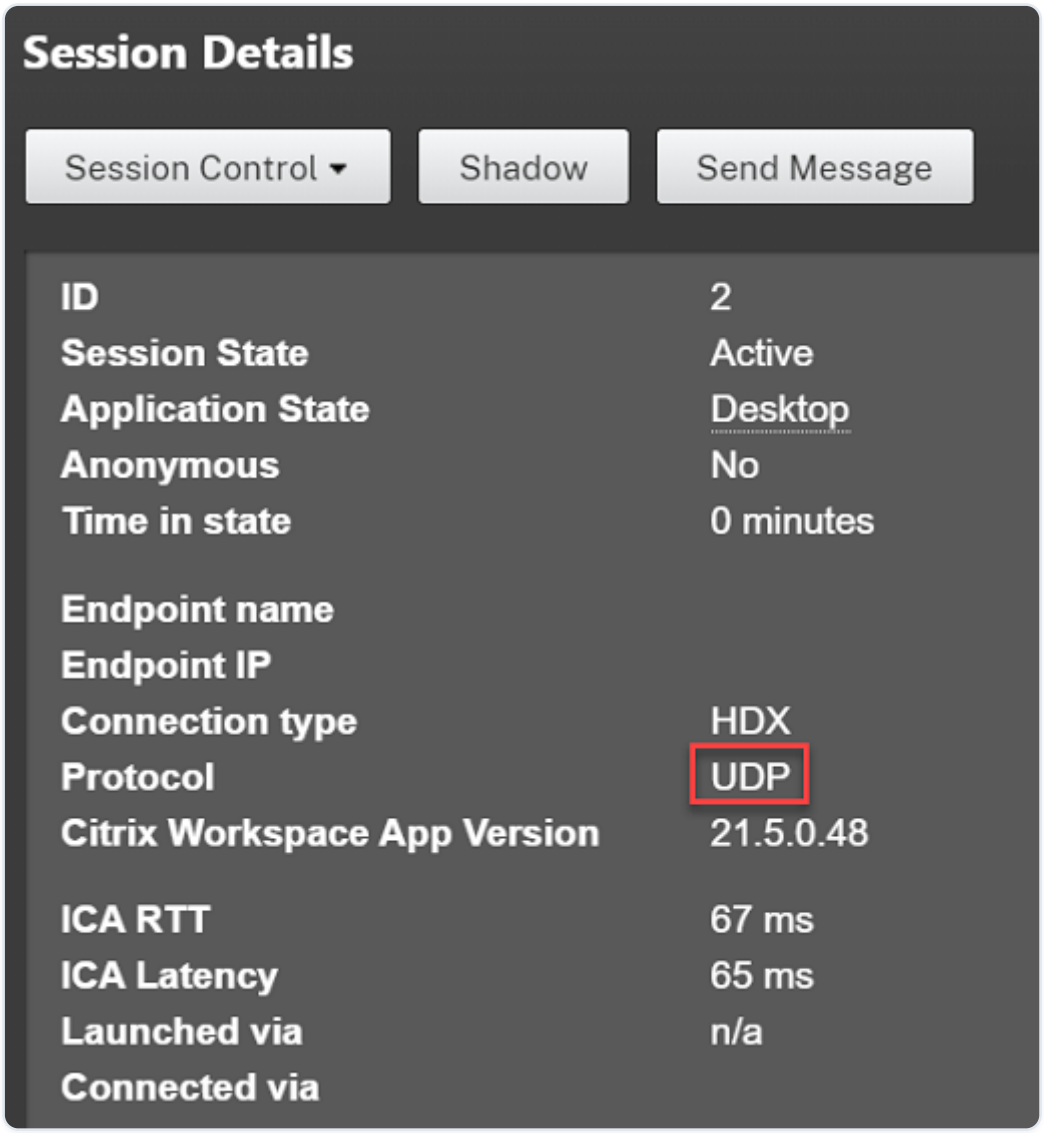
構成

アダプティブトランスポートはデフォルトで有効になっています。Citrix ポリシーの **HDX™ Adaptive Transport** 設定を使用して、次のオプションを構成できます。

- **優先**。これはデフォルト設定です。アダプティブトランスポートが有効になり、EDT を優先トランスポートプロトコルとして使用し、TCP へのフォールバックが行われます。
- **診断モード**。アダプティブトランスポートが有効になり、EDT の使用が強制されます。TCP へのフォールバックは無効になります。この設定は、テストとトラブルシューティングのみに推奨されます。
- **オフ**。アダプティブトランスポートは無効になり、トランスポートには TCP のみが使用されます。

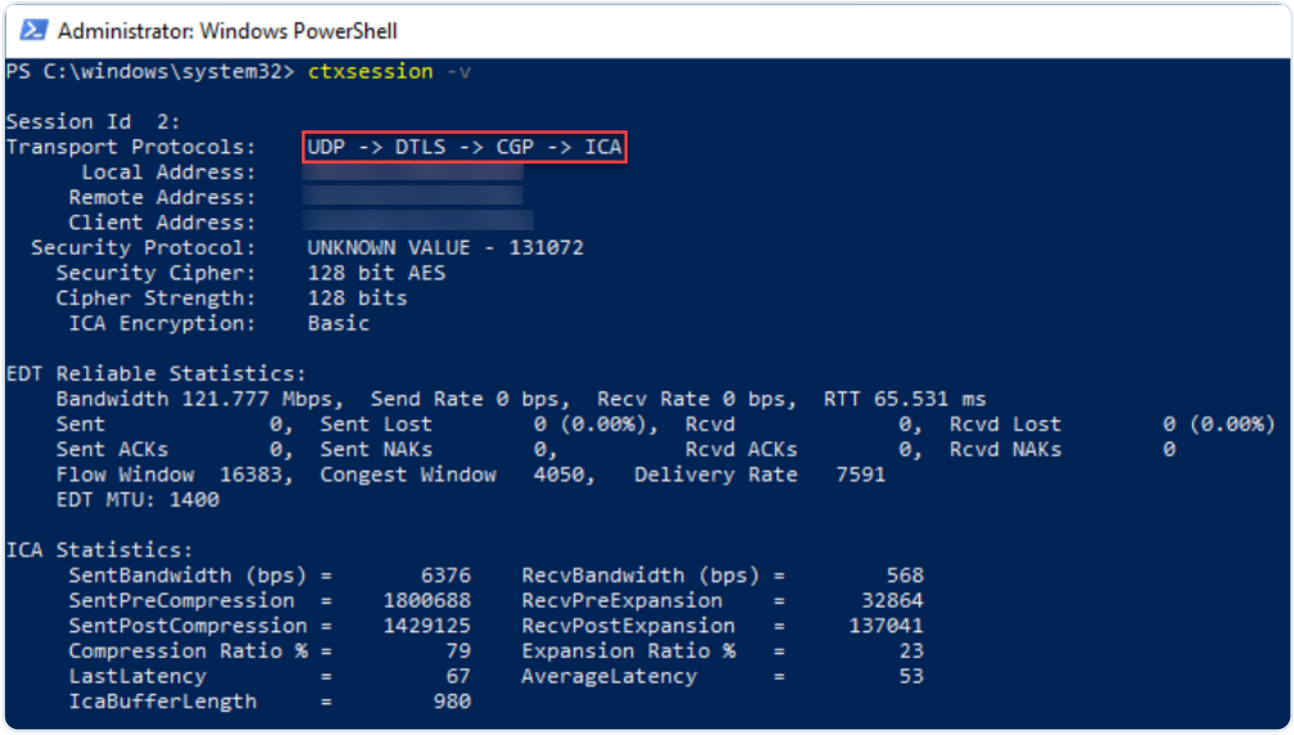
セッションのトランスポートプロトコルとしてEDTが使用されていることを確認するには、DirectorまたはVDA上のCtxSession.exeコマンドラインユーティリティを使用できます。

Directorでセッションを検索し、**詳細**を選択します。**接続の種類**が**HDX**で、**プロトコル**が**UDP**の場合、EDTがセッションのトランスポートプロトコルとして使用されています。**接続の種類**が**RDP**の場合、ICAは使用されておらず、**プロトコル**はN/Aと表示されます。詳細については、「セッションの監視」を参照してください。



CtxSession.exeユーティリティを使用するには、セッション内でコマンドプロンプトまたはPowerShellを起動し、`ctxsession.exe`を実行します。詳細な統計情報を表示するには、`ctxsession.exe -v`を実行します。EDTが使用されている場合、トランスポートプロトコルは次のいずれかを表示します。

- **UDP > ICA** (セッションの信頼性が無効)
- **UDP > CGP > ICA** (セッションの信頼性が有効)
- **UDP > DTLS > CGP > ICA** (ICAはDTLSでエンドツーエンド暗号化されています)



EDT MTU検出

MTU検出により、EDTはセッション確立時に最大転送単位（MTU）を自動的に決定できます。これにより、パフォーマンスの低下やセッション確立の失敗につながる可能性のあるEDTパケットの断片化を防ぎます。

システム要件

- VDAの最小バージョン1912 (2103以降を推奨)
- シトリックス ワークスペース アプリ
  - Windows: バージョン1912以降 (2105以降を推奨)
  - Mac: バージョン2108以降
  - Linux: バージョン2109以降
  - Android: バージョン21.5以降
- シトリックス ADC:
  - 13.0.52.24
  - 12.1.56.22
- セッションの信頼性を有効にする必要があります

この機能をサポートしないクライアントプラットフォームまたはバージョンを使用している場合は、環境に適したカスタムEDT MTUの構成の詳細について、「CTX231821」を参照してください。

> **重要:**
>
> MTU検出は、マルチストリームICAではサポートされていません。

VDAでEDT MTU検出を制御するには

MTU Discovery はデフォルトで有効になっています。この機能を無効にするには、**EDT MTU Discovery** レジストリ値を削除し、VDA を再起動します。詳細については、レジストリで管理される HDX 機能のリストにある EDT MTU Discovery 設定を参照してください。

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

ロス許容モード

> **重要:**
>
> - この機能には、Windows 用 Citrix Workspace アプリ 2002 以降が必要です。
> - 損失許容モードは、Citrix Gateway または Citrix Gateway Service ではサポートされていません。このモードは、直接接続でのみ利用可能です。

> 損失許容モードは、EDT Lossy トランスポートプロトコルを使用して、高遅延およびパケット損失のあるネットワーク経由で接続するユーザーのユーザーエクスペリエンスを向上させます。

当初、セッションは EDT を使用して確立されます。遅延とパケット損失のしきい値に達するか、それを超えると、該当する仮想チャネルは EDT から EDT Lossy に切り替わり、他の仮想チャネルは EDT のままになります。遅延とパケット損失がしきい値を下回ると、該当する仮想チャネルは EDT に戻ります。

デフォルトのしきい値は次のとおりです。

- パケット損失: 5%
- 遅延: 300 ms (RTT)

損失許容モードはデフォルトで有効になっています。このモードを無効にするか、損失許容モードのしきい値設定を使用してパケット損失と遅延のしきい値を調整できます。

システム要件

- シトリックス バーチャル デリバリー エージェント (VDA) 2003
- Windows 用 Citrix Workspace アプリ 2002
- セッションの信頼性が有効になっています。セッションの信頼性の詳細については、セッションの信頼性ポリシー設定 を参照してください。

既知の問題

アダプティブトランスポートとEDTには、以下の問題があります。

- パケットの断片化により、パフォーマンスの低下やセッションの起動失敗が発生する可能性があります。これを回避するために、EDT MTU を調整できます。MTU Discovery または CTX231821 に記載されている回避策を使用してください。
- MTU Discovery が有効になっている場合、Windows クライアントからセッションを起動すると、グレースクリーンまたはブラックスクリーンが表示されることがあります。この問題に対処するには、Windows 用 Workspace アプリ 2105 以降、または Windows 用 Workspace アプリ 1912 CU4 以降にアップグレードしてください。
- Citrix Gateway または Citrix Gateway Service 経由で接続する場合、Linux および Android クライアントで TCP へのフォールバックが失敗することがあります。これは、クライアントと Gateway 間で EDT ネゴシエーションが成功し、Gateway と VDA 間で EDT ネゴシエーションが失敗した場合に発生します。この問題に対処するには、Linux 用 Workspace アプリ 2104 以降、および Android 用 Workspace アプリ 21.5 以降にアップグレードしてください。
- 非対称ネットワークパスは、Citrix Gateway または Citrix Gateway Service を経由しない接続で MTU Discovery の失敗を引き起こす可能性があります。この問題に対処するには、VDA バージョン 2103 以降にアップグレードしてください。

- Citrix Gateway または Citrix Gateway Service を使用している場合、非対称ネットワークパスが原因で MTU Discovery が失敗することがあります。これは、Gateway の問題により、EDT パケットヘッダー内の Don't Fragment (DF) ビットが伝播されないためです。この問題に対する修正はまだ利用できません。
- MTU DiscoveryがDS-Liteネットワーク経由で接続するユーザーに対して失敗する可能性があります。一部のモデムは、パケット処理が有効になっているときにDFビットを尊重せず、MTU Discoveryがフラグメンテーションを検出するのを妨げます。この状況では、以下のオプションが利用可能です。
  - ユーザーのモデムでパケット処理を無効にします。
  - MTU Discoveryを無効にし、CTX231821に記載されているようにハードコードされたMTUを使用します。
  - Adaptive Transportを無効にして、セッションがTCPを使用するように強制します。ユーザーの一部のみが影響を受ける場合は、他のユーザーがEDTを引き続き使用できるように、クライアント側で無効にすることを検討してください。
- VPN経由で接続している一部のユーザーに対して、公開アプリケーションが起動しません。エラーは表示されません。詳細については、CTX280797を参照してください。

トラブルシューティング

Adaptive TransportとEDTのトラブルシューティングを行うには、以下をお勧めします。

1. 要件、考慮事項、および既知の問題を徹底的に確認し、検証してください。
2. StudioまたはGPOに、目的の**HDX Adaptive Transport**設定を上書きするCitrixポリシーがないか確認してください。
3. クライアントに、目的のHDX Adaptive Transport設定を上書きする設定がないか確認します。これは、GPO設定、オプションのWorkspace app管理テンプレートを使用して構成された設定、またはレジストリまたはクライアントの構成ファイルにおける**HDXoverUDP**設定の手動構成である可能性があります。
4. マルチセッションVDAマシンで、UDPリスナーがアクティブであることを確認します。VDAマシンでコマンドプロンプトを開き、`netstat -a -p udp`を実行します。詳細については、「HDX Enlightened Data Transportプロトコルを確認する方法」を参照してください。
5. Citrix Gatewayをバイパスして内部で直接セッションを起動し、使用されているプロトコルを確認します。セッションがEDTを使用している場合、VDAはCitrix Gateway経由の外部接続でEDTを使用する準備ができています。
6. EDTが直接内部接続では機能するが、Citrix Gatewayを介するセッションでは機能しない場合：

- セッションの信頼性が有効になっていることを確認します。
- GatewayでDTLSが有効になっていることを確認します。

7. ネットワークファイアウォールとVDAマシンで実行されているファイアウォールの両方で、適切なファイアウォールルールが構成されているか確認します。
8. ユーザーの接続が非標準のMTUを必要とするかどうかを確認します。実効MTUが1500バイト未満の接続は、EDTパケットのフラグメンテーションを引き起こし、それがパフォーマンスに影響を与えたり、セッション起動の失敗を引き起こしたりする可能性があります。この問題は、VPN、一部のWi-Fiアクセスポイント、および4Gや5Gなどのモバイルネットワークを使用している場合に一般的です。この問題に対処する方法については、MTU Discoveryセクションを参照してください。

Citrix SD-WAN™との相互運用性

Citrix SD-WAN WAN最適化 (WANOP) は、URLベースのビデオキャッシュを含むセッション間トークン化圧縮 (データ重複排除) を提供し、大幅な帯域幅削減を実現します。この削減は、オフィス拠点で2人以上のユーザーが同じクライアントフェッチビデオを視聴したり、同じファイルやドキュメントの大部分を転送または印刷したりする場合に発生します。さらに、WANOPは、ICAデータ削減および印刷ジョブ圧縮のプロセスを支店アプライアンスで実行することにより、VDAサーバーのCPUオフロードを提供し、Citrix Virtual Apps and Desktopsサーバーのスケーラビリティを向上させます。

現在、SD-WAN WANOPはEDTをサポートしていません。ただし、SD-WAN WANOPが使用されている場合でも、アダプティブトランスポートを無効にする必要はありません。ユーザーがWANOPが有効なSD-WANを経由するセッションを起動すると、セッションは自動的にトランスポートプロトコルとしてTCPを使用するように設定されます。WANOPを使用しないセッションは、可能な限りEDTを引き続き使用します。

Citrix ICA® 仮想チャネル

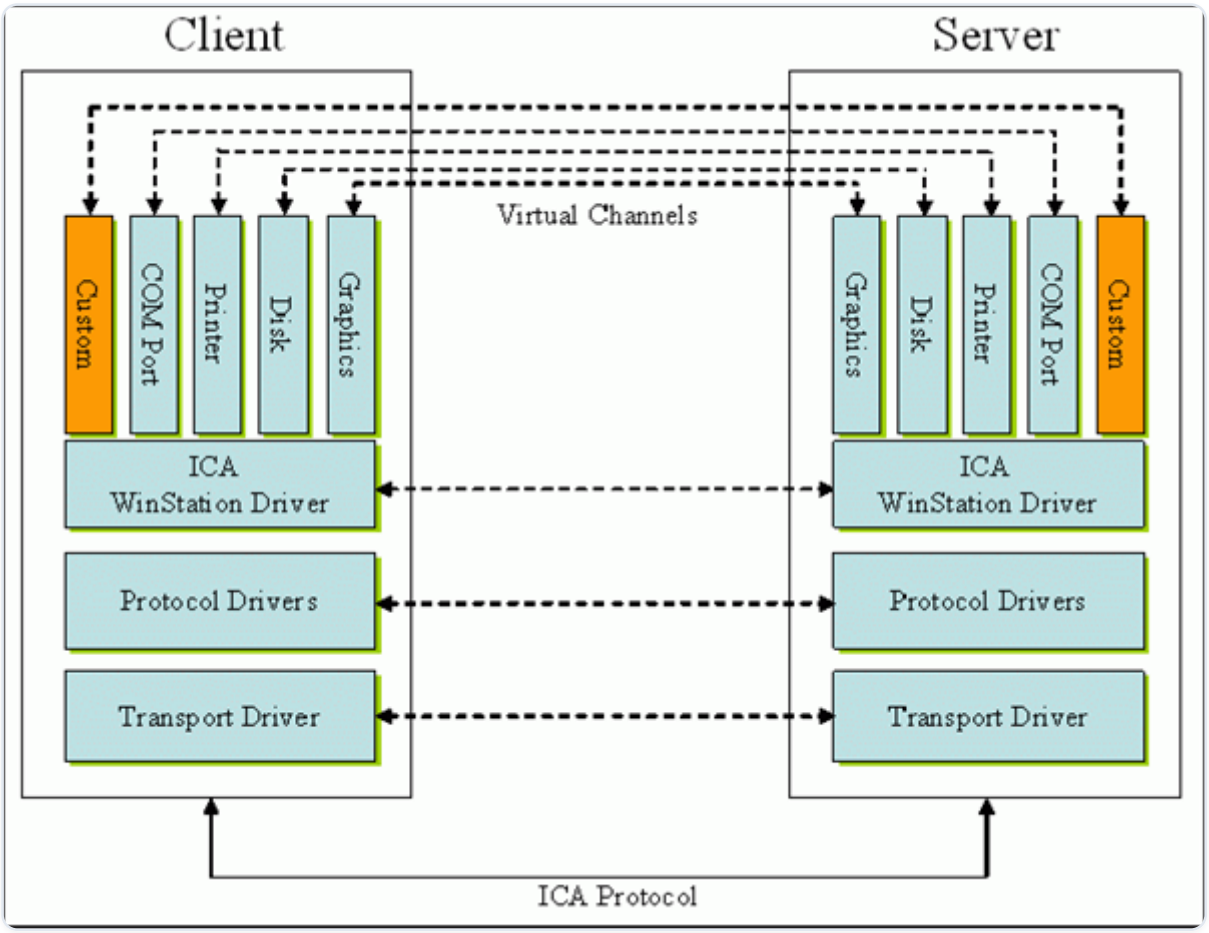
> **警告:**
>
> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrixは、レジストリエディターの誤った使用によって生じる問題が解決できることを保証できません。レジストリエディターは、ご自身の責任において使用してください。編集する前に、必ずレジストリをバックアップしてください。

ICA仮想チャネルとは?

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

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

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



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

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

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

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

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

または

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

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

> **注：**

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

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

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

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

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

64ビット互換性

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

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

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

汎用USB仮想チャネル

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

- ctxusbm.sys
- ctxusbr.sys

ICA仮想チャネルの仕組み

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

シェルによってロードされる仮想チャネルモジュール（例）：

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

一部はカーネルモードとしてロードされます。例:

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

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

サーバー側のグラフィック仮想チャネル

XenApp 7.0およびXenDesktop 7.0以降、`ctxgfx.exe` は、ワークステーションとターミナルサーバーの両方のセッションでグラフィック仮想チャネルをホストします。`Ctxgfx` は、対応するドライバー（RDSHの場合は`Icardd.dll`、ワークステーションの場合は`vdod.dll`および`vidd.dll`）と対話するプラットフォーム固有のモジュールをホストします。

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

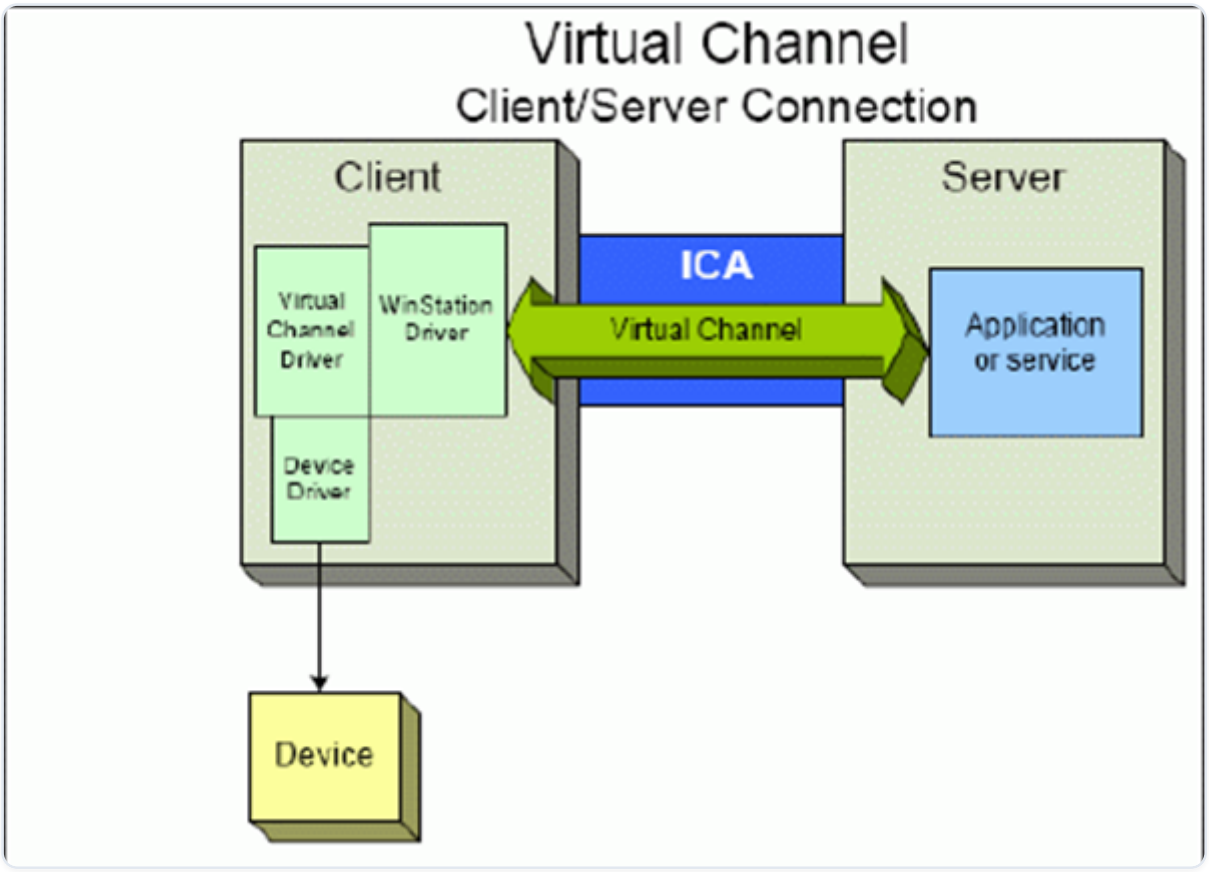
Windowsサービスでの特殊チャネルのホスティング

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

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

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

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



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

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

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

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

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

注：

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

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

注：

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

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

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

重要:

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

仮想チャネルのパススルー機能

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

次の機能は、シングルホップまたはマルチホップで同じように動作します。

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

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

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

> **重要:**

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

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

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

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

以下の従来の仮想チャネルとその機能をサポートしています。

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

セキュリティとICA仮想チャネル

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

ベストプラクティス

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

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

仮想チャネルの命名:

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

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

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

ダブルホップサポート:

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

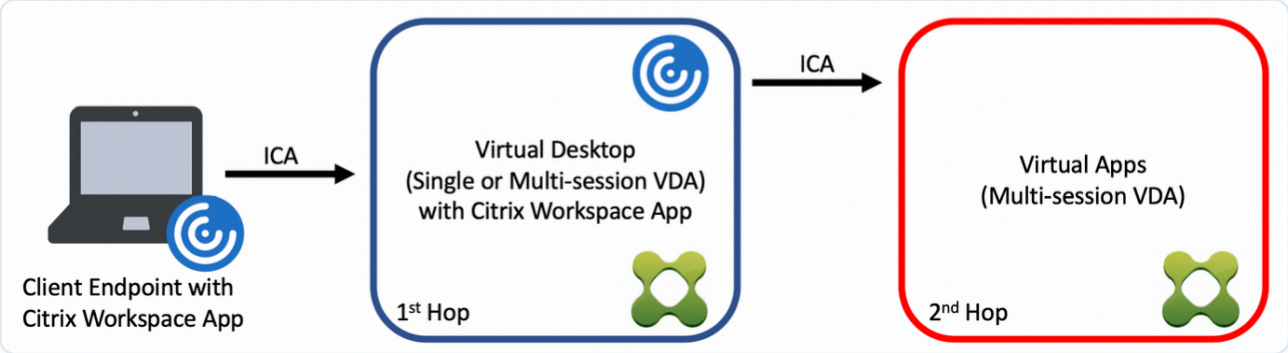
仮想チャネル	ダブルホップはサポートされていますか？
ツイン	はい
USB VC	はい
WAYCOM デバイス - K2M (USB VC を使用)	はい
Webカメラビデオ圧縮	はい
Windows Mediaリダイレクト	はい

参照

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

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

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



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

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

システム要件

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

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

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

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

ダブルホップにおけるHDX™の展開に関する考慮事項

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

グラフィック

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

遅延

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

マルチメディア

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

USBデバイスリダイレクト

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

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

注：

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

サポートの例外

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

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

インストールと構成

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

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

準備

インストール準備 を確認し、必要なタスクをすべて完了します。

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

コアコンポーネントのインストール

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

サイトの作成

コアコンポーネントをインストールしてStudioを起動すると、自動的にサイトの作成に誘導されます。

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

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

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

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

オプションコンポーネントのインストール

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

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

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

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

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

マシンカタログを作成する

Studioでサイトを作成した後、マシンカタログの作成に誘導されます。

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

デリバリーグループを作成する

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

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

アプリケーショングループの作成（オプション）

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

インストール準備

Citrix Virtual Apps and Desktops™ の展開は、以下のコンポーネントのインストールから始まります。このプロセスにより、ファイアウォール内のユーザーへのアプリケーションとデスクトップの配信が準備されます。

- 1つ以上のDelivery Controller
- シトリックス スタジオ
- Citrix Director (シトリックス ディレクター)
- Citrix StoreFront™ (シトリックス ストアフロント™)
- Citrix License Server (シトリックス ライセンス サーバー)
- 1つ以上のCitrix Virtual Delivery Agent (VDA) (シトリックス バーチャル デリバリー エージェント)
- Universal Print Server、Federated Authentication Service、Self-Service Password Resetなどのオプションコンポーネントおよびテクノロジー

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

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

製品ISOに含まれるフルプロダクトインストーラーを使用して、多くのコンポーネントとテクノロジーを展開できます。VDAのインストールには、スタンドアロンVDAインストーラーを使用できます。スタンドアロンVDAインストーラーは、Citrixダウンロードサイトで入手できます。すべてのインストーラーには、グラフィカルインターフェイスとコマンドラインインターフェイスが用意されています。「インストーラー」を参照してください。

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

インストール前に確認する情報

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

コンポーネントのインストール場所

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

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

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

  他のサーバーに他のコンポーネントをインストールする前に、Citrix License Serverとライセンスをインストールします。
- Server CoreOS（Delivery Controllerなど）にサポートされているコンポーネントをインストールするには、(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/install-configure/install-command.html) 必要があります。このOSタイプにはグラフィカルインターフェイスがないため、Studioやその他のツールは別の場所にインストールし、それらをControllerサーバーにポイントしてください。

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

各オペレーティングシステムに最新の更新プログラムが適用されていることを確認してください。

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

Citrix Hypervisorでは、仮想マシンが登録済みと表示されていても、電源状態が不明と表示される場合があります。この問題を解決するには、レジストリキー `HostTime` の値を編集して、ホストとの時刻同期を無効にします。

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

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

> **ヒント:**
>
> デフォルト値は`HostTime="UTC"`です。この値をUTC以外のもの（例: `Local`）に変更します。この変更により、ホストとの時刻同期が実質的に無効になります。
>
> Windows 10シングルセッションマシン向けの最適化ガイダンスは、CTX216252で入手できます。

コンポーネントをインストールしない場所:

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

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

権限とActive Directoryの要件

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

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

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

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

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

詳細については、以下を参照してください。

- (/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/secure/best-practices.html)
- (/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/secure/delegated-administration.html)
- Active Directory 構成に関する Microsoft ドキュメント

インストールのガイダンス、考慮事項、およびベストプラクティス

いずれかのコンポーネントのインストール中

- フルプロダクトメディアから Delivery Controller、Studio、License Server、または Director をインストールまたはアップグレードする際に、Citrix インストーラーがマシン上の以前の Windows インストールからの再起動が保留中であることを検出すると、インストーラーは終了/リターンコード 9 で停止します。マシンの再起動を促されます。

  これは Citrix による強制的な再起動ではありません。マシンに以前インストールされた他のコンポーネントが原因です。この状況が発生した場合は、マシンを再起動してから、Citrix インストーラーを再度起動してください。

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

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

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

VDAのインストール中

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

  制限を承諾するか、VDAのインストールを終了して、Media Foundationのインストール後に再開することができます。グラフィカルインターフェイスでは、この選択肢はメッセージで表示されます。コマンドラインでは、`/no_mediafoundation_ack` オプションを使用して制限を承諾できます。

- VDAをインストールすると、**Direct Access Users**という新しいローカルユーザーグループが自動的に作成されます。シングルセッションOS用VDAでは、このグループはRDP接続にのみ適用されます。マルチセッションOS用VDAでは、このグループはICA®およびRDP接続に適用されます。
- VDAは、通信するための有効なControllerアドレスを持っている必要があります。そうでない場合、セッションを確立できません。Controllerアドレスは、VDAのインストール時または後で指定できます。必ず実行してください。詳細については、「VDA登録」を参照してください。

VDAサポートツール

各VDAインストーラーには、VDAの全体的な健全性や接続品質など、VDAのパフォーマンスをチェックするためのCitrixツールを含むサポート性MSIが含まれています。このMSIのインストールは、VDAインストーラーのグラフィカルインターフェイスの **［追加コンポーネント］** ページで有効または無効にできます。コマンドラインからは、`/exclude "Citrix Supportability Tools"` オプションを使用してインストールを無効にできます。

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

サポート性MSIに含まれる現在のツール：

- Citrix Health Assistant：詳細については、「CTX207624」を参照してください。
- VDA Cleanup Utility：詳細については、「CTX209255」を参照してください。

VDAをインストールする際にツールをインストールしない場合、CTX記事に現在のダウンロードパッケージへのリンクが含まれています。

VDAインストール後およびインストール中の再起動

VDAインストールの最後に再起動が必要です。その再起動は、デフォルトで自動的に行われます。

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

VDAインストール中に必要な再起動の回数を最小限に抑えるには：

- VDAのインストールを開始する前に、サポートされている.NET Frameworkバージョンがインストールされていることを確認してください。

- WindowsマルチセッションOSマシンでは、VDAをインストールする前にRDSロールサービスをインストールして有効にしてください。

VDAをインストールする前にこれらの前提条件をインストールしない場合：

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

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

インストールまたはアップグレードの失敗時の復元

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

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

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

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

この機能を有効にしてマルチセッションVDAのインストールまたはアップグレードを開始すると、インストーラーは実際のインストールまたはアップグレードを開始する前にサーバーバックアップを作成します。VDAのインストールまたはアップグレードが失敗した場合、マシンはバックアップ状態に戻されます。`%temp%/Citrix`フォルダーには、展開ログと復元に関するその他の情報が含まれています。サーバーバックアップの作成にかかる時間は、必要なバックアップのサ

イズとサーバーで利用可能なリソースの量に基づきます。バックアップは *C:\WindowsImageBackup\servername* に保存されます。

デフォルトでは、この機能は無効になっています。

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

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

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

- VDAインストーラーのグラフィカルインターフェイス（**Autostart**や、復元またはサイレントオプションなしの `XenDesktopVDASetup.exe` コマンドなど）を使用する場合は、**Summary** ページで**Enable automatic restore if update fails**チェックボックスをオンにします。

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

インストーラー

フルプロダクトインストーラー

ISOで提供されているフルプロダクトインストーラーを使用すると、次のことができます。

- コアコンポーネント（Delivery Controller、Studio、Director、License Server）のインストール、アップグレード、または削除。
- StoreFront をインストールまたはアップグレードします。

- シングルセッションまたはマルチセッションオペレーティングシステム用の Windows VDA をインストールまたはアップグレードします。
- プリントサーバーに Universal Print Server `UpsServer` コンポーネントをインストールします。
- フェデレーション認証サービス をインストールします。
- Session Recording をインストールします。

1 人のユーザー (Web 開発など) 向けにマルチセッション OS からデスクトップを配信するには、製品版インストーラーのコマンドラインインターフェイスを使用します。詳細については、Server VDI を参照してください。

スタンドアロン VDA インストーラー

スタンドアロン VDA インストーラーは、Citrix ダウンロードページで入手できます。(製品のインストールメディアからは入手できません。) スタンドアロン VDA インストーラーは、製品版 ISO よりもはるかに小さく、次のような展開に容易に対応できます。

- ローカルにステージングまたはコピーされた電子ソフトウェア配布 (ESD) パッケージを使用する
- 物理マシンを使用する
- リモートオフィスを持つ

デフォルトでは、自己解凍型スタンドアロン VDA のファイルは **Temp** フォルダーに抽出されます。**Temp** フォルダーに抽出する場合、製品版インストーラーを使用する場合よりも多くのディスク容量がマシンに必要です。ただし、**Temp** フォルダーに抽出されたファイルは、インストール完了後に自動的に削除されます。または、絶対パスを指定して `/extract` コマンドを使用することもできます。

3つのスタンドアロンVDAインストーラーをダウンロードできます。

VDAServerSetup.exe:

マルチセッションOS用VDAをインストールします。フルプロダクトインストーラーで利用可能なマルチセッションOS用VDAのすべてのオプションをサポートします。

VDAWorkstationSetup.exe:

シングルセッションOS用VDAをインストールします。フルプロダクトインストーラーで利用可能なシングルセッションOS用VDAのすべてのオプションをサポートします。

VDAWorkstationCoreSetup.exe:

Remote PC Access展開またはコアVDIインストール用に最適化されたシングルセッションOS用VDAをインストールします。Remote PC Accessは物理マシンを使用します。コアVDIインストールは、イメージとして使用されていないVMです。このような展開のVDA接続に必要なコアサービスのみをインストールします。そのため、フルプロダクトインストーラーまたは `VDAWorkstationSetup.exe` インストーラーで有効なオプションのサブセットのみをサポートします。

このインストーラーは、以下の目的で使用されるコンポーネントをインストールまたは含みません。

- アップブイ。
- Profile Management。Citrix Profile Managementをインストールから除外すると、Citrix Directorの表示に影響します。詳細については、「VDAのインストール」を参照してください。
- マシンIDサービス。
- Citrix サポートツール。
- シトリックス ファイル for Windows。
- シトリックス ファイル for Outlook。
- Citrix WEM エージェント。

`VDAWorkstationCoreSetup.exe` インストーラーは、Windows向けCitrix Workspaceアプリをインストールまたは含みません。

`VDAWorkstationCoreSetup.exe` を使用することは、フルプロダクトインストーラーまたは `VDAWorkstationSetup` インストーラーを使用してシングルセッションOS VDAをインストールし、以下のいずれかを実行することと同じです。

- グラフィカルインターフェイスで、 ページでRemote PC Accessオプションを選択します。
- コマンドラインインターフェイスで: `/remotepc` オプションを指定する。
- コマンドラインインターフェイスで: `/components vda` と、有効な追加コンポーネント名をすべてリストする `/exclude` オプションを指定する。

省略されたコンポーネント/機能は、後でフルプロダクトインストーラーを実行してインストールできます。この操作により、不足しているすべてのコンポーネントをインストールできます。

`VDAWorkstationCoreSetup.exe` インストーラーは、Browser Content Redirection MSI を自動的にインストールします。この自動インストールは、VDA リリース 2003 以降のサポート対象リリースに適用されます。

Citrix インストールリターンコード

インストールログには、コンポーネントインストールの結果が Microsoft の値ではなく、Citrix のリターンコードとして含まれています。

- 0 = 成功
- 1 = 失敗
- 2 = 部分的な成功
- 3 = 部分的な成功と再起動が必要
- 4 = 失敗と再起動が必要
- 5 = ユーザーによってキャンセルされました
- 6 = コマンドライン引数が不足しています
- 7 = 新しいバージョンが見つかりました
- 8 = 成功と再起動が必要
- 9 = ファイルロック再起動
- 10 = 中止
- 11 = メディア失敗
- 12 = ライセンス失敗
- 13 = 事前チェック失敗
- 14 = 再起動保留チェック中止
- -1 = 終了

例えば、Microsoft System Center Configuration Managerなどのツールを使用する場合、インストールログにリターンコード3が含まれていると、スクリプトによるVDAインストールが失敗したように見えることがあります。これは、VDAインストーラーがユーザーが開始する必要のある再起動を待機している場合に発生する可能性があります (例えば、サーバーへのRDSロールの前提条件のインストール後など)。VDAインストールは、すべての前提条件と選択されたコンポーネントがインストールされ、インストール後にマシンが再起動されて初めて成功と見なされます。

あるいは、インストールをCMDスクリプト (Microsoftの終了コードを返します) でラップするか、Configuration Managerパッケージの成功コードを変更できます。

Windows Serverワークロード向けにMicrosoft RDSライセンスサーバーを構成する

この製品は、Windows 2016などのWindows Serverワークロードを提供する場合に、Windows Serverリモートセッション機能にアクセスします。これには通常、リモートデスクトップサービスクライアントアクセスライセンス (RDS CAL) が必要です。VDAは、RDS CALを要求するためにRDSライセンスサーバーに接続できる必要があります。ライセンスサーバーをインストールしてアクティブ化します。詳細については、Microsoftドキュメント「リモートデスクトップサービスライセンスサーバーをアクティブ化する」を参照してください。概念実証環境では、Microsoftが提供する猶予期間を使用できます。

この方法を使用すると、このサービスにライセンスサーバー設定を適用させることができます。イメージ上のRDSコンソールで、ライセンスサーバーとユーザーごとのモードを構成できます。Microsoftグループポリシー設定を使用してライセンスサーバーを構成することもできます。詳細については、Microsoftドキュメント「クライアントアクセスライセンス (CAL) を使用してRDS展開をライセンスする」を参照してください。

グループポリシー設定を使用してRDSライセンスサーバーを構成するには:

1. 利用可能なマシンにリモートデスクトップサービスライセンスサーバーをインストールします。そのマシンは常に利用可能である必要があります。Citrix製品のワークロードは、このライセンスサーバーに到達できる必要があります。
2. Microsoftグループポリシーを使用して、ライセンスサーバーのアドレスとユーザーごとのライセンスモードを指定します。詳細については、Microsoftドキュメント「RDセッションホストサーバーのリモートデスクトップライセンスモードを指定する」を参照してください。

Windows 10ワークロードには、適切なWindows 10ライセンスのアクティベーションが必要です。Windows 10ワークロードをアクティベートするには、Microsoftのドキュメントに従うことをお勧めします。

Microsoft Azure Resource Manager クラウド環境

Microsoft Azure Resource Manager を使用して Citrix Virtual Apps and Desktops™ 展開環境に仮想マシンをプロビジョニングする際は、この記事のガイダンスに従ってください。

以下の事項に精通していることを前提としています。

- アジュール アクティブ ディレクトリ: `<https://docs.microsoft.com/en-in/azure/active-directory/fundamentals/active-directory-whatis/>`
- 同意フレームワーク: `<https://docs.microsoft.com/ja-jp/azure/active-directory/manage-apps/plan-an-application-integration>`

- サービスプリンシパル: `<https://docs.microsoft.com/ja-jp/azure/active-directory/develop/app-objects-and-service-principals/>`

Azure オンデマンドプロビジョニング

Azure のオンデマンドプロビジョニングでは、プロビジョニングが完了した後、Citrix Virtual Apps and Desktops が電源オンアクションを開始したときにのみ VM が作成されます。

MCS を使用して Azure Resource Manager でマシンカタログを作成する場合、Azure オンデマンドプロビジョニング機能は次のとおりです。

- ストレージコストを削減します
- カタログ作成を高速化します

MCS カタログを作成すると、Azure portal にリソースグループ内のネットワークセキュリティグループ、ネットワークインターフェイス、ベースイメージ、およびIDディスクが表示されます。

Azureポータルには、Citrix Virtual Apps and DesktopsがVMの電源オンアクションを開始するまでVMは表示されません。マシンには次の違いを持つ2つのタイプがあります。

- プールされたマシンでは、オペレーティングシステムディスクとライトバックキャッシュはVMが存在する場合にのみ存在します。コンソールでプールされたマシンをシャットダウンすると、Azure portal にはVMが表示されません。マシンを定期的にシャットダウンする（たとえば、勤務時間外に）場合、ストレージコストを大幅に節約できます。
- 専用マシンでは、オペレーティングシステムディスクは VM が最初に電源オンになったときに作成されます。Azure portal の VM は、マシンIDが削除されるまでストレージに残ります。コンソールで専用マシンをシャットダウンしても、Azure portal に VM は表示されたままです。

Azure Resource Manager への接続

接続とリソース は、接続を作成するウィザードについて説明しています。以下の情報は、Azure Resource Manager 接続に固有の詳細をカバーしています。

考慮事項:

- Citrix® は、共同作成者ロールを持つサービスプリンシパルの使用を推奨しています。ただし、最小限の権限のリストについては、「最小限の権限」セクションを参照してください。
- 最初の接続を作成するとき、Azure は必要な権限を付与するよう求めます。今後の接続では、引き続き認証が必要ですが、Azure は以前の同意を記憶しており、プロンプトを再度表示することはありません。

- 認証に使用されるアカウントは、Azure RBAC を使用してサブスクリプション内でロールを割り当てる権限を持っている必要があります。例として、サブスクリプションの所有者、ロールベースのアクセス制御管理者、またはユーザーアクセス管理者などです。
- 認証に使用されるアカウントは、サブスクリプションのディレクトリのメンバーである必要があります。注意すべきアカウントの種類は、「職場または学校」と「個人用 Microsoft アカウント」の2種類です。詳細については、CTX219211 を参照してください。
- 既存の Microsoft アカウントをサブスクリプションのディレクトリのメンバーとして追加して使用することはできますが、ユーザーが以前にディレクトリのリソースのいずれかへのゲストアクセスを許可されていた場合、問題が発生する可能性があります。この場合、ディレクトリ内に必要な権限を付与しないプレースホルダーエントリが存在し、エラーが返される可能性があります。

  ディレクトリからリソースを削除し、明示的に再度追加することでこれを修正します。ただし、このオプションは、アカウントがアクセスできる他のリソースに意図しない影響を与える可能性があるため、慎重に実行してください。
- 特定のアカウントが実際にはメンバーであるにもかかわらず、ディレクトリゲストとして検出される既知の問題があります。このような構成は、通常、古くから確立されたディレクトリアカウントで発生します。回避策: ディレクトリにアカウントを追加し、適切なメンバーシップ値を取得します。
- リソースグループは単にリソースのコンテナであり、自身のリージョン以外のリージョンからのリソースを含むことができます。これは、リソースグループのリージョンに表示されるリソースが利用可能であると期待している場合、混乱を招く可能性があります。
- 必要な数のマシンをホストするのに十分な大きさのネットワークとサブネットがあることを確認してください。これにはある程度の先見性が必要ですが、Microsoft はアドレス空間の容量に関するガイダンスを提供し、適切な値を指定するのに役立ちます。

Azure へのホスト接続は、次の2つの方法で確立できます。

- Azure に認証してサービスプリンシパルを作成します。
- 以前に作成したサービスプリンシパルの詳細を使用して Azure に接続します。

サービスプリンシパルの作成

> **重要:**

> この機能は、Azure China および Azure Germany のサブスクリプションではまだ利用できません。

開始する前に、Azure に認証します。以下を確認してください。

- サブスクリプションのAzure Active Directoryテナントにユーザーアカウントがあること。
- 認証に使用されるアカウントは、Azure RBAC を使用してサブスクリプション内でロールを割り当てる権限を持っている必要があります。例として、サブスクリプションの所有者、ロールベースのアクセス制御管理者、またはユーザーアクセス管理者などです。
- 認証のためのグローバル管理者、アプリケーション管理者、またはアプリケーション開発者の権限があること。これらの権限は、ホスト接続の作成後に取り消すことができます。ロールの詳細については、「Azure AD の組み込みロール」を参照してください。

サービスプリンシパルを作成するためにAzureに認証すると、アプリケーションがAzureに登録されます。登録されたアプリケーションにはシークレットキー（クライアントシークレット）が作成されます。登録されたアプリケーションは、クライアントシークレットを使用してAzure ADに認証します。クライアントシークレットの有効期限が切れる前に必ず変更してください。シークレットキーの有効期限が切れる前に、コンソールにアラートが表示されます。

サービスプリンシパルを作成するためにAzureに認証するには、**接続とリソースの追加**ウィザードで次の手順を完了します。

1. **接続**ページで、**新しい接続の作成**、**Microsoft Azure**接続タイプ、およびAzure環境を選択します。
2. 仮想マシンを作成するために使用するツールを選択し、**次へ**を選択します。
3. ページで、Azure サブスクリプション ID と接続の名前を入力します。サブスクリプション ID を入力すると、 ボタンが有効になります。

   注：

   接続名には 1〜64 文字を含めることができ、空白のみ、または文字 `\/;:#.*?=<>|[]{}"'()'` を含めることはできません。

4. を選択し、Azure Active Directory アカウントのユーザー名とパスワードを入力します。
5. **サインイン**を選択します。
6. **承諾**を選択して、Citrix Virtual Apps and Desktopsに一覧表示された権限を付与します。Citrix Virtual Apps and Desktopsは、指定されたユーザーに代わってAzureリソースを管理できるサービスプリンシパルを作成します。

7. 「**Accept**」を選択すると、ウィザードの「**Connection**」ページに戻ります。

> **注：**
>
> Azure への認証が正常に完了すると、「**Create new**」ボタンと「**Use existing**」ボタンが消えます。「**Connection successful**」というテキストが緑色のチェックマークとともに表示され、Azure サブスクリプションへの接続が成功したことを示します。

8. 「**Connection Details**」ページで、「**Next**」を選択します。

> **注：**
>
> Azure への認証が正常に完了し、必要な権限の付与に同意するまで、次のページに進むことはできません。

9. 接続のリソースを構成します。リソースには、リージョンとネットワークが含まれます。
   - 「**地域**」ページで、地域を選択します。
   - 「**ネットワーク**」ページで、次の操作を行います。
     - リージョンとネットワークの組み合わせを識別しやすくするために、1〜64文字のリソース名を入力します。リソース名には、空白のみを含めることや、文字 `\/;:#.*?=<>|[]{}"'()'` を含めることはできません。
     - 仮想ネットワーク/リソースグループのペアを選択します。（同じ名前の仮想ネットワークが複数ある場合、ネットワーク名とリソースグループをペアにすることで、一意の組み合わせが提供されます。）前のページで選択した地域に仮想ネットワークがない場合は、そのページに戻り、仮想ネットワークがある地域を選択してください。
10. 「**概要**」ページで、設定の概要を確認し、「**完了**」を選択してセットアップを完了します。

以前に作成したサービスプリンシパルの詳細を使用してAzureに接続する

サービスプリンシパルを手動で作成するには、Azure Resource Managerサブスクリプションに接続し、以下のセクションで提供されているPowerShellコマンドレットを使用します。

前提条件:

- **SubscriptionId:** VDAをプロビジョニングするサブスクリプションのAzure Resource Manager `SubscriptionID`。
- 「**ActiveDirectoryID**」: Azure AD に登録したアプリケーションのテナントID。
- 「**ApplicationName**」: Azure AD で作成するアプリケーションの名前。

サービスプリンシパルを作成するには：

1. Azure Resource Manager サブスクリプションに接続します。

   ```
   Connect-AzAccount
   ```

2. サービスプリンシパルを作成する Azure Resource Manager サブスクリプションを選択します。

   ```
   Get-AzSubscription -SubscriptionId $subscriptionId | Select-AzSubscription
   ```

3. AD テナントにアプリケーションを作成します。

   ```
   $AzureADApplication = New-AzADApplication -DisplayName $ApplicationName
   ```

4. サービスプリンシパルを作成します。

   ```
   New-AzADServicePrincipal -ApplicationId $AzureADApplication.AppId
   ```

5. サービスプリンシパルにロールを割り当てます。

   ```
   New-AzRoleAssignment -RoleDefinitionName Contributor -ServicePrincipalName
   $AzureADApplication.AppId –scope /subscriptions/$SubscriptionId
   ```

6. PowerShell コンソールの出力ウィンドウから ApplicationId をメモします。ホスト接続を作成する際に、その ID を指定します。

接続とリソースの追加ウィザードで、次の手順を実行します。

1. **接続**ページで、**新しい接続の作成**、**Microsoft Azure**接続タイプ、およびAzure環境を選択します。
2. 仮想マシンを作成するために使用するツールを選択し、**次へ**を選択します。
3. 「**接続の詳細**」ページで、Azure サブスクリプション ID と接続の名前を入力します。

> **注：**
>
> 接続名には 1～64 文字を含めることができ、空白のみ、または文字 `\/;:#.*?=<>|[]{}"'()'` を含めることはできません。

4. **既存を使用**を選択します。**既存のサービスプリンシパルの詳細**ウィンドウで、既存のサービスプリンシパルに対して次の設定を入力します。詳細を入力すると、**保存**ボタンが有効になります。**保存**を選択します。有効な詳細情報を提供するまで、このページから先に進むことはできません。

   - **サブスクリプションID**。AzureサブスクリプションIDを入力します。サブスクリプションIDを取得するには、Azureポータルにサインインし、**サブスクリプション > 概要**に移動します。
   - **Active Directory ID** (テナント ID)。Azure AD に登録したアプリケーションのディレクトリ (テナント) ID を入力します。
   - **アプリケーション ID**。Azure AD に登録したアプリケーションのアプリケーション (クライアント) ID を入力します。
   - **アプリケーションシークレット**。シークレットキー (クライアントシークレット) を作成します。登録済みアプリケーションは、このキーを使用して Azure AD に対して認証を行います。セキュリティ上の理由から、キーを定期的に変更することをお勧めします。キーは後で取得できないため、必ず保存してください。
   - **シークレットの有効期限**。アプリケーションシークレットの有効期限が切れる日付を入力します。シークレットキーの有効期限が切れる前に、コンソールにアラートが表示されます。ただし、シークレットキーの有効期限が切れると、エラーが発生します。

     > **注：**
     >
     > セキュリティ上の理由から、有効期限は現在から2年を超えることはできません。

   - **認証 URL**。このフィールドは自動的に入力され、編集できません。
   - **管理 URL**。このフィールドは自動的に入力され、編集できません。
   - **ストレージサフィックス**。このフィールドは自動的に入力され、編集できません。

     AzureでMCSカタログを作成するには、以下のエンドポイントへのアクセスが必要です。これらのエンドポイントへのアクセスにより、ネットワークとAzureポータルおよびそのサービス間の接続が最適化されます。

     - 認証URL: `<https://login.microsoftonline.com/>`
     - 管理URL: `<https://management.azure.com/>`。これはAzure Resource Managerプロバイダー APIのリクエストURLです。管理のエンドポイントは環境によって異なりま

す。たとえば、Azure Globalの場合は`<https://management.azure.com/>`、Azure US Governmentの場合は`<https://management.usgovcloudapi.net/>`です。

- ストレージサフィックス: `<https://*.core.windows.net./>`。これはストレージサフィックスのワイルドカード文字(*)です。例: `<https://demo.table.core.windows.net/>`。

5. **保存**を選択すると、**接続の詳細**ページに戻ります。**次へ**を選択して次のページに進みます。
6. 接続のリソースを構成します。リソースには、リージョンとネットワークが含まれます。
   - 「**地域**」ページで、地域を選択します。
   - 「**ネットワーク**」ページで、次の操作を行います。
     - リージョンとネットワークの組み合わせを識別しやすくするために、1〜64文字のリソース名を入力します。リソース名には、空白のみを含めることや、文字`\/;:#.*?=<>|[]{}"'()'`を含めることはできません。
     - 仮想ネットワーク/リソースグループのペアを選択します。（同じ名前の仮想ネットワークが複数ある場合、ネットワーク名とリソースグループをペアにすることで、一意の組み合わせが提供されます。）前のページで選択した地域に仮想ネットワークがない場合は、そのページに戻り、仮想ネットワークがある地域を選択してください。
7. 「**概要**」ページで、設定の概要を確認し、「**完了**」を選択してセットアップを完了します。

Azure Resource Managerイメージを使用してマシンカタログを作成する

イメージは、ディスク、スナップショット、またはAzure Compute Gallery内のイメージ定義のイメージバージョンであり、マシンカタログ内のVMを作成するために使用されます。イメージに関する一般情報については、「マシンカタログの作成」を参照してください。

Azureスロットリング

Azure Resource Manager は、サブスクリプションとテナントの要求をスロットルし、プロバイダーの特定のニーズに合わせて調整された定義済みの制限に基づいてトラフィックをルーティングします。詳細については、Microsoft サイトの「Resource Manager の要求のスロットリング」を参照してください。サブスクリプションとテナントには制限があり、多数のマシンを管理すると問題が発生する可能性があります。たとえば、多数のマシンを含むサブスクリプションでは、電源操作に関連するパフォーマンスの問題が発生する可能性があります。

> **ヒント:**

> 詳細については、「Machine Creation Services を使用した Azure パフォーマンスの向上」を参照してください。

> これらの問題を軽減するために、MCS の内部スロットリングを削除して、Azure から利用可能な要求クォータをより多く使用できます。

たとえば、1,000 台の VM を含む大規模なサブスクリプションで VM の電源をオンまたはオフにする場合は、次の最適な設定をお勧めします。

- 絶対同時操作数: 500
- 1 分あたりの最大新規操作数: 2000
- 操作の最大同時実行数: 500

MCS はデフォルトで最大 500 の同時操作をサポートします。または、Remote PowerShell SDK を使用して、同時操作の最大数を設定することもできます。

PowerShell プロパティ `MaximumConcurrentProvisioningOperations` を使用して、Azure プロビジョニングの同時操作の最大数を指定します。このプロパティを使用する際は、以下を考慮してください。

- `MaximumConcurrentProvisioningOperations` のデフォルト値は 500 です。
- PowerShell コマンド `Set-item` を使用して、`MaximumConcurrentProvisioningOperations` パラメーターを構成します。

Azureリソースグループ

Azureプロビジョニングリソースグループは、ユーザーにアプリケーションとデスクトップを提供するVMをプロビジョニングする方法を提供します。MCSマシンカタログを作成する際に、既存の空のAzureリソースグループを追加することも、新しいリソースグループを作成することもできます。Azureリソースグループの詳細については、Microsoftドキュメントを参照してください。

Azureリソースグループの使用法

Azureリソースグループあたりの仮想マシン、マネージドディスク、スナップショット、およびイメージの数に制限はありません。（Azureリソースグループあたり240個のVM、800個のマネージドディスクという制限は削除されました。）

- フルスコープのサービスプリンシパルを使用してマシンカタログを作成する場合、MCSはAzureリソースグループを1つだけ作成し、そのグループをカタログに使用します。

- ナロースコープのサービスプリンシパルを使用してマシンカタログを作成する場合、カタログ用に空の、事前に作成されたAzureリソースグループを提供する必要があります。

Azureエフェメラルディスク

Azureエフェメラルディスクを使用すると、キャッシュディスクまたは一時ディスクを再利用して、Azure対応仮想マシンのOSディスクを保存できます。この機能は、標準のHDDディスクよりも高性能なSSDディスクを必要とするAzure環境で役立ちます。エフェメラルディスクを使用するには、`New-ProvScheme`の実行時にカスタムプロパティ`UseEphemeralOsDisk`を**true**に設定する必要があります。

> **注：**
>
> カスタムプロパティ `UseEphemeralOsDisk` が **false** に設定されているか、値が指定されていない場合、プロビジョニングされたすべてのVDAはプロビジョニングされたOSディスクを引き続き使用します。

> 以下は、プロビジョニングスキームで使用するカスタムプロパティのセットの例です。

```
"CustomProperties": [

            {

                "Name": "UseManagedDisks",

                "Value": "true"

            },

            {

                "Name": "StorageType",

                "Value": "Standard_LRS"

            },

            {

                "Name": "UseSharedImageGallery",
```

```
                "Value": "true"
            },
            {
                "Name": "SharedImageGalleryReplicaRatio",
                "Value": "40"
            },
            {
                "Name": "SharedImageGalleryReplicaMaximum",
                "Value": "10"
            },
            {
                "Name": "LicenseType",
                "Value": "Windows_Server"
            },
            {
                "Name": "UseEphemeralOsDisk",
                "Value": "true"
            }
        ],
```

エフェメラルOSディスクを使用してマシンを作成する方法

エフェメラルOSディスクは、`CustomProperties`パラメーターの`UseEphemeralOsDisk`プロパティに基づいて制御されます。

エフェメラルディスクに関する重要な考慮事項

`New-ProvScheme` を使用してエフェメラルOSディスクをプロビジョニングするには、次の制約を考慮してください。

- カタログに使用されるVMサイズは、エフェメラルOSディスクをサポートしている必要があります。
- VMサイズに関連付けられているキャッシュまたは一時ディスクのサイズは、OSディスクのサイズ以上である必要があります。
- 一時ディスクのサイズは、キャッシュディスクのサイズよりも大きくする必要があります。

以下の際にもこれらの問題を考慮してください:

- プロビジョニングスキームを作成する際。
- プロビジョニングスキームを変更する際。
- イメージを更新する際。

AZUREエフェメラルディスクとMACHINE CREATION SERVICES (MCS) ストレージ最適化 (MCS I/O)

Azure エフェメラル OS ディスクと MCS I/O は同時に有効にできません。

重要な考慮事項は次のとおりです。

- エフェメラルOSディスクとMCS I/Oの両方を同時に有効にしてマシンカタログを作成することはできません。
- `New-ProvScheme` または `Set-ProvScheme` で**true**に設定されたPowerShellパラメーター(`UseWriteBackCache` および `UseEphemeralOsDisk`) は、適切なエラーメッセージとともに失敗します。
- 両方の機能が有効になっている既存のマシンカタログについては、引き続き以下を行うことができます。
  - マシンカタログを更新する。
  - VMを追加または削除する。
  - マシンカタログを削除する。

Azureサーバー側暗号化

Citrix Virtual Apps and DesktopsおよびCitrix DaaSは、Azure Key Vaultを介したAzureマネージドディスクの顧客管理暗号化キーをサポートしています。このサポートにより、独自の暗号化キーを使用してマシンカタログのマネージドディスクを暗号化することで、組織およびコンプライアンス

要件を管理できます。詳しくは、「Azure Disk Storage のサーバー側暗号化」を参照してください。

マネージドディスクでこの機能を使用する場合：

- ディスクの暗号化に使用するキーを変更するには、`DiskEncryptionSet` で現在のキーを変更します。その `DiskEncryptionSet` に関連付けられているすべてのリソースは、新しいキーで暗号化されるように変更されます。
- キーを無効にするか削除すると、そのキーを使用しているディスクを持つVMは自動的にシャットダウンします。シャットダウン後、キーが再度有効になるか、新しいキーを割り当てない限り、VMは使用できません。そのキーを使用しているカタログは電源をオンにできず、VMを追加することもできません。

顧客管理暗号化キーを使用する際の重要な考慮事項

この機能を使用する際は、以下を考慮してください。

- 顧客管理キーに関連するすべてのリソース（Azure Key Vault、ディスク暗号化セット、VM、ディスク、スナップショット）は、同じサブスクリプションとリージョンに存在する必要があります。
- 顧客管理暗号化キーを有効にすると、後で無効にすることはできません。顧客管理暗号化キーを無効にするか削除する場合は、すべてのデータを顧客管理暗号化キーを使用していない別のマネージドディスクにコピーしてください。
- サーバー側暗号化と顧客管理キーを使用して暗号化されたカスタムイメージから作成されたディスクは、同じ顧客管理キーを使用して暗号化する必要があります。これらのディスクは同じサブスクリプション内にある必要があります。
- サーバー側暗号化と顧客管理キーで暗号化されたディスクから作成されたスナップショットは、同じ顧客管理キーで暗号化する必要があります。
- 顧客管理キーで暗号化されたディスク、スナップショット、およびイメージは、別のリソースグループやサブスクリプションに移動できません。
- 現在または以前にAzure Disk Encryptionを使用して暗号化されたマネージドディスクは、顧客管理キーを使用して暗号化することはできません。
- ディスク暗号化セットのリージョンごとの制限については、Microsoft サイトを参照してください。

> **注：**

> Azureサーバー側暗号化の構成については、「クイックスタート: Azure portal を使用して Key Vault を作成する」を参照してください。

Azureカスタマーマネージド暗号化キー

マシンカタログを作成する際、カタログにプロビジョニングされたマシン上のデータを暗号化するかどうかを選択できます。カスタマーマネージド暗号化キーによるサーバー側暗号化を使用すると、マネージドディスクレベルで暗号化を管理し、カタログ内のマシン上のデータを保護できます。ディスク暗号化セット（DES）は、カスタマーマネージドキーを表します。この機能を使用するには、まずAzureでDESを作成する必要があります。DESは次の形式です。

- `/subscriptions/12345678-1234-1234-1234-123456789012/resourceGroups/Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/SampleEncryptionSet`

リストからDESを選択します。選択するDESは、リソースと同じサブスクリプションおよびリージョンにある必要があります。イメージがDESで暗号化されている場合は、マシンカタログの作成時に同じDESを使用します。カタログ作成後にDESを変更することはできません。

暗号化キーを使用してカタログを作成し、後でAzureで対応するDESを無効にした場合、カタログ内のマシンの電源をオンにしたり、マシンを追加したりすることはできなくなります。

Azure専用ホスト

MCSを使用して、Azure専用ホストにVMをプロビジョニングできます。Azure専用ホストにVMをプロビジョニングする前に:

- ホストグループを作成します。
- そのホストグループにホストを作成します。
- カタログと仮想マシンを作成するために十分なホスト容量が予約されていることを確認します。

次のPowerShellスクリプトを使用して、ホストテナンシーが定義されたマシンのカタログを作成できます。

```
New-ProvScheme <otherParameters> -CustomProperties '<CustomProperties
xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <Property xsi:type="StringProperty" Name="HostGroupId"
Value="myResourceGroup/myHostGroup" />
```

```
...other Custom Properties...

</CustomProperties>
```

MCSを使用してAzure専用ホストに仮想マシンをプロビジョニングする場合、以下を考慮してください。

- *専用ホスト*はカタログのプロパティであり、カタログ作成後に変更することはできません。専用テナンシーは現在、Azureではサポートされていません。
- ホスティングユニットのリージョンにある、事前に構成されたAzureホストグループが、`HostGroupId` パラメーターを使用する際に必要です。
- Azureの自動配置が必要です。この機能は、ホストグループに関連付けられたサブスクリプションをオンボードするための要求を行います。詳細については、VM Scale Set on Azure Dedicated Hosts - Public Preview を参照してください。自動配置が有効になっていない場合、MCSはカタログ作成中にエラーをスローします。

Azure共有イメージギャラリー

Azure Shared Image Galleryを、AzureでMCSプロビジョニングされたマシンの公開イメージリポジトリとして使用します。公開イメージをギャラリーに保存することで、OSディスクの作成とハイドレーションを高速化し、非永続VMの起動時間とアプリケーション起動時間を改善できます。共有イメージギャラリーには、次の3つの要素が含まれています。

- *ギャラリー*: イメージはここに保存されます。MCSは、マシンカタログごとに1つのギャラリーを作成します。
- *ギャラリーイメージ定義*: この定義には、公開イメージに関する情報（オペレーティングシステムの種類と状態、Azureリージョン）が含まれます。MCSは、カタログ用に作成されたイメージごとに1つのイメージ定義を作成します。
- *ギャラリーイメージバージョン*: 共有イメージギャラリー内の各イメージは複数のバージョンを持つことができ、各バージョンは異なるリージョンに複数のレプリカを持つことができます。各レプリカは、公開イメージの完全なコピーです。

注：

共有イメージギャラリー機能は、マネージドディスクでのみ動作します。レガシーマシンカタログでは利用できません。

> 詳細については、Azure Shared Image Gallery の概要 を参照してください。

共有イメージギャラリーの構成

`New-ProvScheme` コマンドを使用して、Shared Image Gallery をサポートするプロビジョニングスキームを作成します。`Set-ProvScheme` コマンドを使用して、プロビジョニングスキームのこの機能を有効または無効にし、レプリカ比率とレプリカの最大値を変更します。

Shared Image Gallery 機能をサポートするために、プロビジョニングスキームに3つのカスタムプロパティが追加されました。

`UseSharedImageGallery`

- 公開されたイメージの保存に Shared Image Gallery を使用するかどうかを定義します。**True** に設定すると、イメージは Shared Image Gallery イメージとして保存され、それ以外の場合はスナップショットとして保存されます。
- 有効な値は**True**と**False**です。
- プロパティが定義されていない場合、デフォルト値は**False**です。

`SharedImageGalleryReplicaRatio`

- マシンとギャラリーイメージバージョンレプリカの比率を定義します。
- 有効な値は0より大きい整数です。
- プロパティが定義されていない場合、デフォルト値が使用されます。永続OSディスクのデフォルト値は1000、非永続OSディスクのデフォルト値は40です。

`SharedImageGalleryReplicaMaximum`

- 各ギャラリーイメージバージョンに対するレプリカの最大数を定義します。
- 有効な値は0より大きい整数です。
- プロパティが定義されていない場合、デフォルト値は10です。
- Azure は現在、ギャラリーイメージの単一バージョンに対して最大10個のレプリカをサポートしています。プロパティが Azure でサポートされている値よりも大きい値に設定されている場合、MCS は指定された値を使用しようとします。Azure はエラーを生成し、MCS はそれをログに記録し、現在のレプリカ数は変更されません。

> **ヒント:**

> MCS プロビジョニングカタログの公開イメージを保存するために Shared Image Gallery を使用する場合、MCS はカタログ内のマシンの数、レプリカ比率、およびレプリカの最大値に基づいて、ギャラリーイメージバージョンのレプリカ数を設定します。レプリカ数は、カタログ内のマシンの数をレプリカ比率で除算し（最も近い整数に切り上げ）、その値を最大レプリカ数で制限することによって計算されます。たとえば、レプリカ比率が20、最大値が5の場合、0〜20台のマシンには1つのレプリカが作成され、21〜40台には2つのレプリカ、41〜60台には3つのレプリカ、61〜80台には4つのレプリカ、81台以上には5つのレプリカが作成されます。

ユースケース：SHARED IMAGE GALLERY のレプリカ比率とレプリカの最大値の更新

既存のマシンカタログは Shared Image Gallery を使用しています。`Set-ProvScheme` コマンドを使用して、カタログ内のすべての既存マシンおよび将来のマシンのカスタムプロパティを更新します。

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="True"/> <Property
xsi:type="IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/>
<Property xsi:type="IntProperty" Name="SharedImageGalleryReplicaMaximum"
Value="20"/></CustomProperties>'
```

ユースケース：スナップショットカタログを SHARED IMAGE GALLERY カタログに変換する

このユースケースの場合：

1. `UseSharedImageGallery` フラグを**True**に設定して `Set-ProvScheme` を実行します。オプションで `SharedImageGalleryReplicaRatio` および `SharedImageGalleryReplicaMaximum` プロパティを含めます。
2. カタログを更新します。
3. マシンをパワーサイクルして、強制的に更新します。

例:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="True"/> <Property
xsi:type="IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/>
<Property xsi:type="IntProperty" Name="SharedImageGalleryReplicaMaximum"
Value="20"/></CustomProperties>'
```

ヒント:

パラメーター `SharedImageGalleryReplicaRatio` と `SharedImageGalleryReplicaMaximum` は必須ではありません。`Set-ProvScheme` コマンドが完了しても、共有イメージギャラリーのイメージはまだ作成されていません。カタログがギャラリーを使用するように構成されると、次回のカタログ更新操作で公開されたイメージがギャラリーに保存されます。カタログ更新コマンドは、ギャラリー、ギャラリーイメージ、およびイメージバージョンを作成します。マシンを再起動すると更新され、必要に応じてレプリカ数が更新されます。その時点から、既存のすべての非永続マシンは共有イメージギャラリーのイメージを使用してリセットされ、新しくプロビジョニングされたすべてのマシンはそのイメージを使用して作成されます。古いスナップショットは数時間以内に自動的にクリーンアップされます。

ユースケース: 共有イメージギャラリーカタログをスナップショットカタログに変換する

このユースケースの場合：

1. `UseSharedImageGallery` フラグを **False** に設定するか、未定義のままにして `Set-ProvScheme` を実行します。
2. カタログを更新します。
3. マシンをパワーサイクルして、強制的に更新します。

例:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

```
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="False"/></CustomProperties>'
```

ヒント:

スナップショットから共有イメージギャラリーカタログへの更新とは異なり、各マシンのカスタムデータは新しいカスタムプロパティを反映するようにまだ更新されていません。元の共有イメージギャラリーのカスタムプロパティを表示するには、次のコマンドを実行します: `Get-ProvVm -ProvisioningSchemeName catalog-name`。`Set-ProvScheme` コマンドが完了しても、イメージスナップショットはまだ作成されていません。カタログがギャラリーを使用しないように構成されると、次回のカタログ更新操作で公開されたイメージがスナップショットとして保存されます。その時点から、既存のすべての非永続マシンはスナップショットを使用してリセットされ、新しくプロビジョニングされたすべてのマシンはスナップショットから作成されます。マシンを再起動すると更新され、その時点でカスタムマシンデータが更新され、`UseSharedImageGallery` が **False** に設定されていることが反映されます。古い共有イメージギャラリーのアセット（ギャラリー、イメージ、バージョン）は数時間以内に自動的にクリーンアップされます。

指定された可用性ゾーンにマシンをプロビジョニングする

Azure環境では、特定の可用性ゾーンにマシンをプロビジョニングできます。これはPowerShellを使用して実現できます。

注：

ゾーンが指定されていない場合、MCSはAzureにそのリージョン内にマシンを配置させます。複数のゾーンが指定されている場合、MCSはそれらのゾーンにマシンをランダムに分散させます。

PowerShellによる可用性ゾーンの構成

PowerShellを使用して、`Get-Item` で提供されるインベントリアイテムを表示できます。たとえば、*米国東部リージョン*の `Standard_B1ls` サービス提供を表示するには:

```
$serviceOffering = Get-Item -path "XDHyp:\Connections\my-connection-name\East US.region\serviceoffering.folder\Standard_B1ls.serviceoffering"
```

ゾーンを表示するには、アイテムの`AdditionalData`パラメーターを使用します:

`$serviceOffering.AdditionalData`

可用性ゾーンが指定されていない場合、マシンのプロビジョニング方法に変更はありません。

PowerShellを介して可用性ゾーンを構成するには、`New-ProvScheme`操作で利用可能な**Zones**カスタムプロパティを使用します。**Zones**プロパティは、マシンをプロビジョニングする可用性ゾーンのリストを定義します。これらのゾーンには、1つ以上の可用性ゾーンを含めることができます。たとえば、ゾーン1および3の`<Property xsi:type="StringProperty" Name="Zones" Value="1, 3"/>`です。

プロビジョニングスキームのゾーンを更新するには、`Set-ProvScheme`コマンドを使用します。

無効なゾーンが提供された場合、プロビジョニングスキームは更新されず、無効なコマンドを修正する方法に関する指示を提供するエラーメッセージが表示されます。

ヒント:

無効なカスタムプロパティを指定すると、プロビジョニングスキームは更新されず、関連するエラーメッセージが表示されます。

Azureエフェメラルディスク

Azureエフェメラルディスクを使用すると、キャッシュまたは一時ディスクを再利用して、Azure対応仮想マシンのOSディスクを保存できます。この機能は、標準のHDDディスクよりも高性能なSSDディスクを必要とするAzure環境で役立ちます。

注：

永続カタログはエフェメラルOSディスクをサポートしていません。

エフェメラルOSディスクでは、プロビジョニングスキームでマネージドディスクと共有イメージギャラリーを使用する必要があります。詳しくは、「Azure共有イメージギャラリー」を参照してください。

PowerShellを使用してエフェメラルディスクを構成する

カタログのAzureエフェメラルOSディスクを構成するには、`Set-ProvScheme`で`UseEphemeralOsDisk`パラメーターを使用します。`UseEphemeralOsDisk`パラメーターの値を**true**に設定します。

> **注：**
>
> この機能を使用するには、`UseManagedDisks`と`UseSharedImageGallery`のパラメーターも有効にする必要があります。

例:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

<Property xsi:type="StringProperty" Name="UseEphemeralOsDisk"
Value="true" />

</CustomProperties>'
```

エフェメラルOS一時ディスクの保存

エフェメラルOSディスクをVMの一時ディスクまたはリソースディスクに保存するオプションがあります。この機能により、キャッシュがない、またはキャッシュが不十分なVMでエフェメラルOSディスクを使用できます。このようなVMには、`Ddv4`などのエフェメラルOSディスクを保存するための一時ディスクまたはリソースディスクがあります。

次の点を考慮してください。

- エフェメラルディスクは、VMキャッシュディスクまたはVMの一時（リソース）ディスクのいずれかに保存されます。キャッシュディスクがOSディスクの内容を保持するのに十分な大きさでない限り、一時ディスクよりもキャッシュディスクが優先されます。

- 更新の場合、キャッシュディスクより大きく、一時ディスクより小さい新しいイメージは、エフェメラルOSディスクをVMの一時ディスクに置き換える結果となります。

電源サイクル時にプロビジョニングされた仮想マシンを保持する

電源サイクル時にプロビジョニングされた仮想マシンを保持するかどうかを選択します。PowerShell パラメーター `New-ProvScheme CustomProperties` を使用します。このパラメーターは、電源サイクル時にプロビジョニングされた仮想マシンが保持されるかどうかを決定するために使用される追加のプロパティ `PersistVm` をサポートします。電源オフ時に仮想マシンを保持するには `PersistVm` プロパティを **true** に設定し、電源オフ時に仮想マシンが保持されないようにするにはプロパティを **false** に設定します。

> **注：**
>
> `PersistVm`プロパティは、`CleanOnBoot`と`UseWriteBackCache`のプロパティが有効になっているプロビジョニングスキームにのみ適用されます。非永続仮想マシンに対して`PersistVm`プロパティが指定されていない場合、それらは電源オフ時にAzure環境から削除されます。

「次の例では、`New-ProvScheme CustomProperties` パラメーターは `PersistVm` プロパティを **true** に設定します。」:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

<Property xsi:type="StringProperty" Name="PersistVm" Value="true" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="demo-
resourcegroup" />

<Property xsi:type="StringProperty" Name="LicenseType"
```

```
Value="Windows_Client" />

</CustomProperties>
```

次の例では、`New-ProvScheme CustomProperties`パラメーターは`PersistVM`を**true**に設定することでライトバックキャッシュを保持します。

```
 New-ProvScheme

 -AzureAdJoinType "None"

 -CleanOnBoot

 -CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageType`" Value=`"Standard_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"false`" /
><Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`"
Value=`"true`" /><Property xsi:type=`"StringProperty`" Name=`"PersistVm`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"ResourceGroups`" Value=`"demo-resourcegroup`" /><Property
xsi:type=`"StringProperty`" Name=`"LicenseType`"
Value=`"Windows_Client`" /></CustomProperties>"

 -HostingUnitName "demo"

 -IdentityPoolName "NonPersistent-MCSIO-PersistVM"

 -MasterImageVM "XDHyp:\HostingUnits\demo\image.folder\scale-
test.resourcegroup\demo-snapshot.snapshot"

 -NetworkMapping @ {"0"="XDHyp:\HostingUnits\demo\
\virtualprivatecloud.folder\East US.region\virtualprivatecloud.folder\ji-
test.resourcegroup\jitest-vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName "NonPersistent-MCSIO-PersistVM"

 -ServiceOffering "XDHyp:
\HostingUnits\demo\serviceoffering.folder\Standard_B2ms.serviceoffering"
-UseWriteBackCache
```

```
-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

ヒント:

「`PersistVm` プロパティは、プロビジョニングされた仮想マシンを保持するかどうかを決定します。`PersistOsdisk` プロパティは、OSディスクを永続化するかどうかを決定します。プロビジョニングされた仮想マシンを保持するには、まずOSディスクを保持します。仮想マシンを削除せずにOSディスクを削除することはできません。`PersistVm` パラメーターを指定せずに `PersistOsdisk` プロパティを使用できます。」.

ストレージの種類

MCSを使用するAzure環境の仮想マシンに対して、異なるストレージの種類を選択します。ターゲットVMの場合、MCSは以下をサポートします。

- OSディスク: プレミアムSSD、SSD、またはHDD
- ライトバックキャッシュディスク: プレミアムSSD、SSD、またはHDD

これらのストレージの種類を使用する場合、以下を考慮してください。

- 選択したストレージの種類をVMがサポートしていることを確認してください。
- 構成でAzureエフェメラルディスクを使用している場合、ライトバックキャッシュディスク設定のオプションは表示されません。

ヒント:

`StorageType` はOSタイプとストレージアカウント用に構成されます。`WBCDiskStorageType` はライトバックキャッシュストレージタイプ用に構成されます。通常のカタログの場合、`StorageType` が必要です。`WBCDiskStorageType` が構成されていない場合、`StorageType` が `WBCDiskStorageType` のデフォルトとして使用されます。

WBCDiskStorageType が構成されていない場合、StorageType が WBCDiskStorageType のデフォルトとして使用されます。

ストレージタイプの構成

VMのストレージタイプを構成するには、`New-ProvScheme` の `StorageType` パラメーターを使用します。`StorageType` パラメーターの値をサポートされているストレージタイプのいずれかに設定します。

以下は、プロビジョニングスキームにおける `CustomProperties` パラメーターの設定例です。

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

</CustomProperties>'
```

Azure VM、スナップショット、OS ディスク、およびギャラリーイメージ定義の情報を取得する

OSディスクと種類、スナップショット、ギャラリーイメージ定義を含むAzure VMの情報を表示できます。この情報は、マシンカタログが割り当てられている場合、マスターイメージ上のリソースに対して表示されます。この機能を使用して、LinuxまたはWindowsイメージを表示および選択します。PowerShellプロパティ `TemplateIsWindowsTemplate` が `AdditionDatafield` パラメーターに追加されました。このフィールドには、VMタイプ、OSディスク、ギャラリーイメージ情報、OSタイプ情報など、Azure固有の情報が含まれています。`TemplateIsWindowsTemplate` を **True**に設定するとOSタイプがWindowsであることを示し、`TemplateIsWindowsTemplate` を **False**に設定するとOSタイプがLinuxであることを示します。

> **ヒント:**
>
> `TemplateIsWindowsTemplate` PowerShell プロパティによって表示される情報は、Azure API から取得されます。場合によっては、このフィールドが空になることがあります。たとえば、データディスクからのスナップショットには、OS タイプをスナップショットから取得できないため、`TemplateIsWindowsTemplate` フィールドは含まれません。

たとえば、PowerShell を使用して、Windows OS の種類に対して Azure VM `AdditionData` パラメーターを **True** に設定します。

```
PS C:\Users\username> (get-item XDHyp:
\HostingUnits\mynetwork\image.folder\username-dev-testing-
rg.resourcegroup\username-dev-tsvda.vm).AdditionalData

Key Value

ServiceOfferingDescription Standard_B2ms

HardDiskSizeGB 127

ResourceGroupName FENGHUAJ-DEV-TESTING-RG

ServiceOfferingMemory 8192

ServiceOfferingCores 2

TemplateIsWindowsTemplate True

ServiceOfferingWithTemporaryDiskSizeInMb 16384

SupportedMachineGenerations Gen1,Gen2
```

Azure Marketplace (アジュール マーケットプレイス)

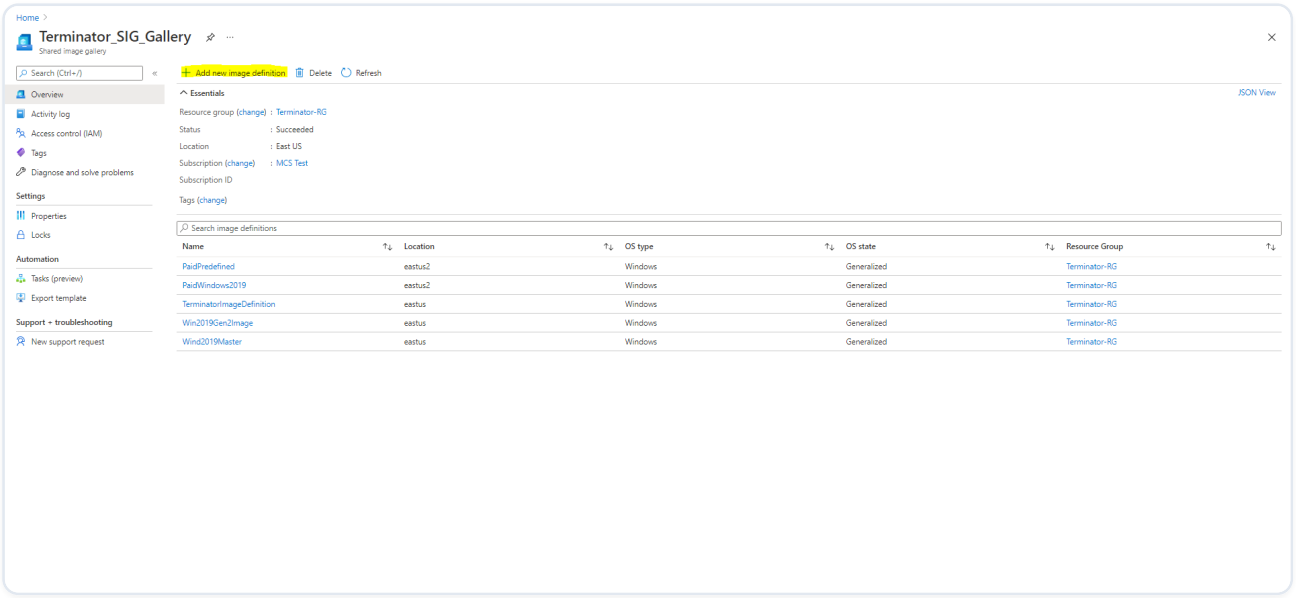
Citrix Virtual Apps and Desktops および Citrix DaaS は、プラン情報を含む Azure 上のマスターイメージを使用してマシンカタログを作成することをサポートしています。詳細については、「Microsoft Azure Marketplace」を参照してください。

ヒント:

標準の Windows Server イメージなど、Azure Marketplace で見つかる一部のイメージには、プラン情報が付加されていません。Citrix DaaS™ 機能は、有料イメージ向けです。

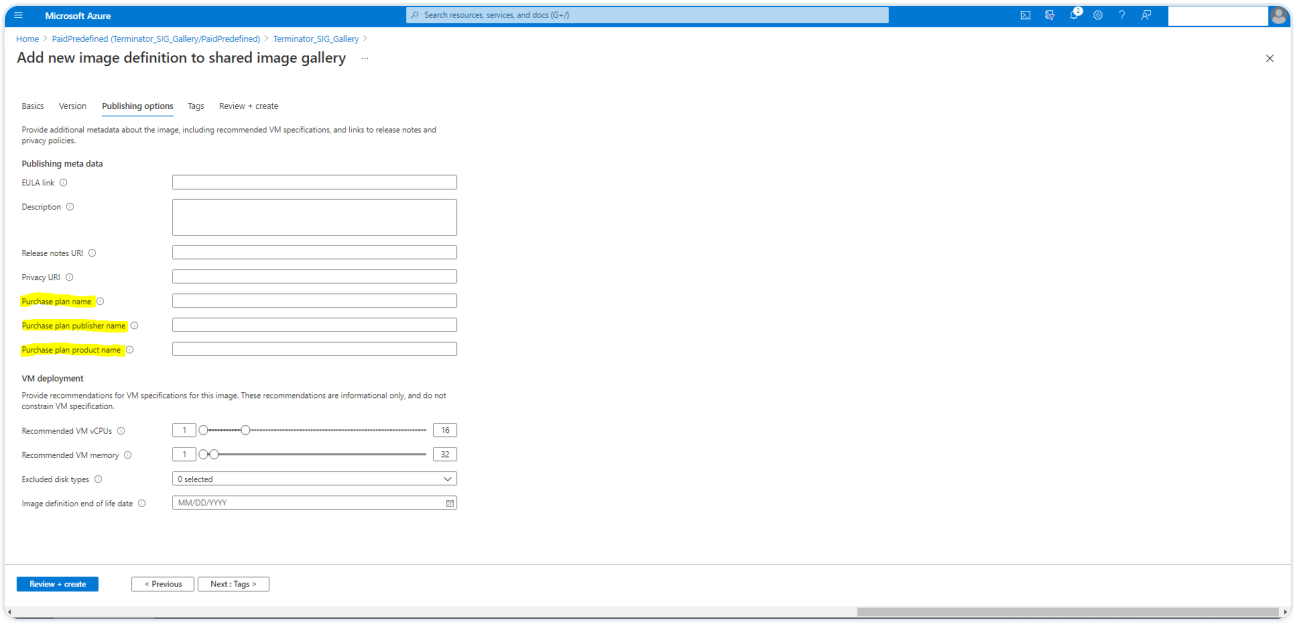
Shared Image Gallery で作成されたイメージに Azure プラン情報が含まれていることを確認します

このセクションの手順を使用して、Citrix Studio で共有イメージギャラリーのイメージを表示します。これらのイメージは、オプションでマスターイメージとして使用できます。イメージを共有イメージギャラリーに配置するには、ギャラリーでイメージ定義を作成します。

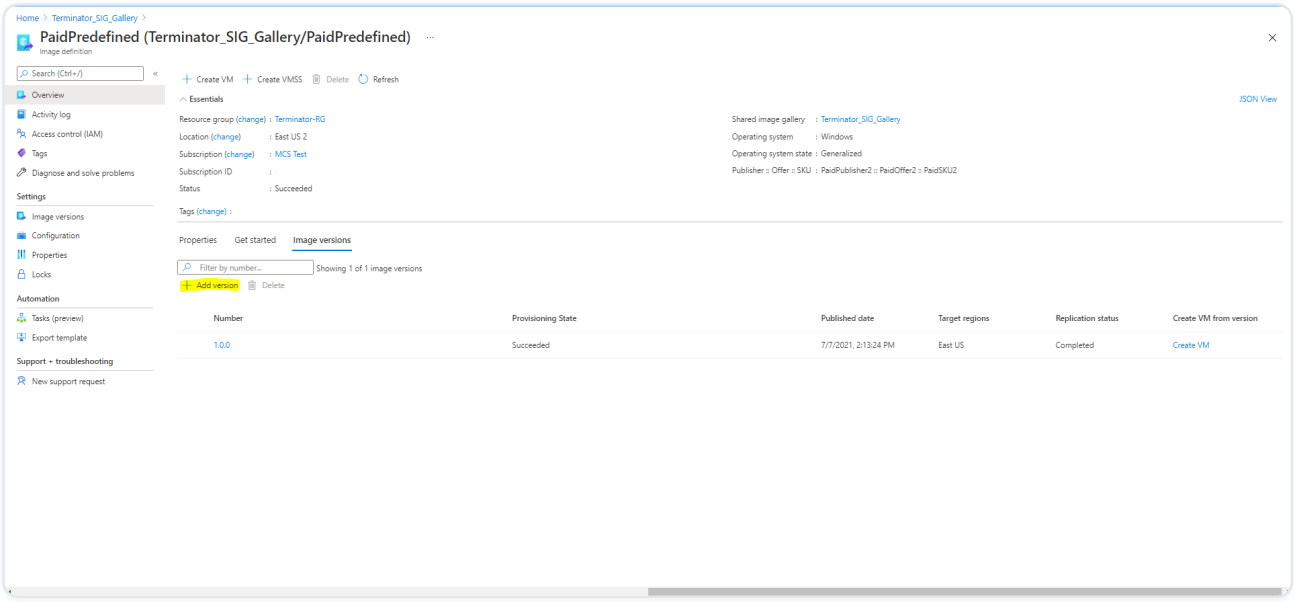


公開オプションページで、購入プラン情報を確認します。

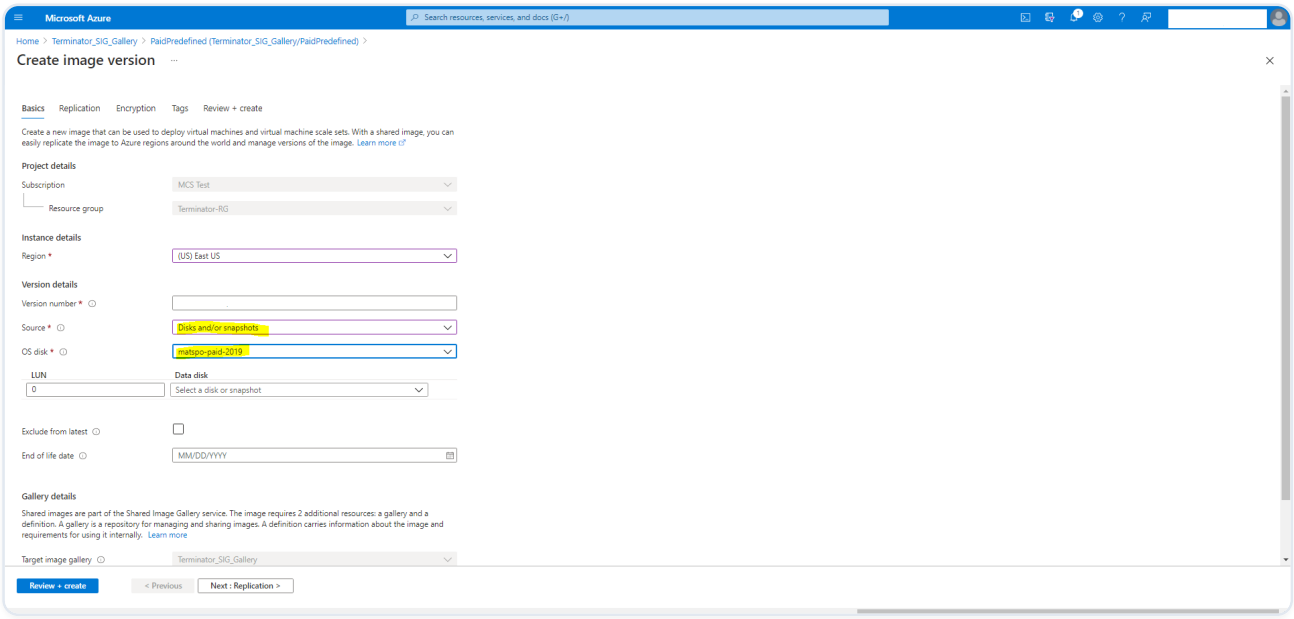
購入プラン情報フィールドは最初は空です。これらのフィールドに、イメージに使用された購入プラン情報を入力します。購入プラン情報を入力しないと、マシンカタログのプロセスが失敗する可能性があります。



購入プラン情報を確認した後、定義内にイメージバージョンを作成します。これはマスターイメージとして使用されます。**バージョンの追加**をクリックします。



バージョン詳細セクションで、イメージスナップショットまたはマネージドディスクをソースとして選択します。



Azure のアクセス許可について

このセクションには、Azure に必要な最小限の一般的なアクセス許可が含まれています。

最小限の権限

最小限のアクセス許可は、より優れたセキュリティ制御を提供します。ただし、追加のアクセス許可を必要とする新機能は、最小限のアクセス許可のみを使用しているため、失敗します。

ホスト接続の作成

Azure から取得した情報を使用して、新しいホスト接続を追加します。

```
"Microsoft.Network/virtualNetworks/read",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/disks/read",
```

VM の電源管理

マシンインスタンスの電源をオンまたはオフにします。

```
"Microsoft.Compute/virtualMachines/read",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/virtualMachines/start/action",

"Microsoft.Compute/virtualMachines/restart/action",
```

仮想マシンの作成、更新、または削除

マシンカタログを作成し、マシンを追加、削除、更新し、マシンカタログを削除します。

以下は、マスターイメージがマネージドディスクである場合、またはスナップショットがホスティング接続と同じリージョンにある場合に必要となる最小限の権限のリストです。

```
"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/deployments/validate/action",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/virtualMachines/write",

"Microsoft.Compute/virtualMachines/delete",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/snapshots/read",

"Microsoft.Compute/snapshots/write",
```

```
"Microsoft.Compute/snapshots/delete",

"Microsoft.Compute/snapshots/beginGetAccess/action",

"Microsoft.Compute/snapshots/endGetAccess/action",

"Microsoft.Compute/disks/read",

"Microsoft.Compute/disks/write",

"Microsoft.Compute/disks/delete",

"Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.Compute/disks/endGetAccess/action",

"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",

"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/networkSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkInterfaces/read",

"Microsoft.Network/networkInterfaces/write",

"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkInterfaces/join/action",
```

以下の機能については、最小限の権限に加えて、以下の追加権限が必要です。

- マスターイメージがホスティング接続と同じリージョンにあるストレージアカウント内の VHD である場合：

```
"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/listKeys/action",
```

- マスターイメージが共有イメージギャラリーのImageVersionである場合:

```
"Microsoft.Compute/galleries/read",

"Microsoft.Compute/galleries/images/read",

"Microsoft.Compute/galleries/images/versions/read",
```

- マスターイメージがマネージドディスクである場合。スナップショットまたはVHDがホスティング接続のリージョンとは異なるリージョンにある場合:

```
"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/listKeys/action",

"Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/delete",
```

- Citrix管理のリソースグループを使用する場合:

```
"Microsoft.Resources/subscriptions/resourceGroups/write",

"Microsoft.Resources/subscriptions/resourceGroups/delete",
```

- マスターイメージを共有イメージギャラリーに配置する場合:

```
"Microsoft.Compute/galleries/write",

"Microsoft.Compute/galleries/images/write",

"Microsoft.Compute/galleries/images/versions/write",

"Microsoft.Compute/galleries/read",

"Microsoft.Compute/galleries/images/read",
```

```
"Microsoft.Compute/galleries/images/versions/read",
"Microsoft.Compute/galleries/delete",
"Microsoft.Compute/galleries/images/delete",
"Microsoft.Compute/galleries/images/versions/delete",
```

- Azure専用ホストサポートを使用する場合:

```
"Microsoft.Compute/hostGroups/read",
"Microsoft.Compute/hostGroups/write",
"Microsoft.Compute/hostGroups/hosts/read",
```

- カスタマーマネージドキー (CMK) を使用してサーバー側暗号化 (SSE) を使用する場合:

```
"Microsoft.Compute/diskEncryptionSets/read",
```

- ARM テンプレート (マシンプロファイル) を使用して VM を展開する場合:

```
"Microsoft.Resources/deployments/write",
"Microsoft.Resources/deployments/operationstatuses/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/delete",
```

- Azure テンプレート仕様をマシンプロファイルとして使用する場合:

```
"Microsoft.Resources/templateSpecs/read",
"Microsoft.Resources/templateSpecs/versions/read",
```

アンマネージドディスクを使用したマシンの作成、更新、削除

マスターイメージが VHD であり、管理者が提供するリソースグループを使用する場合に必要となる最小限の権限のリストは次のとおりです。

```
"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Storage/storageAccounts/delete",

"Microsoft.Storage/storageAccounts/listKeys/action",

"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/write",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/virtualMachines/delete",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/virtualMachines/write",

"Microsoft.Resources/deployments/validate/action",

"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkInterfaces/join/action",

"Microsoft.Network/networkInterfaces/read",

"Microsoft.Network/networkInterfaces/write",

"Microsoft.Network/networkSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/subnets/join/action"
```

一般権限

共同作成者ロールは、すべてのリソースを管理するためのフルアクセス権を持っています。この権限セットは、新機能の取得を妨げるものではありません。

以下の権限セットは、現在の機能セットで必要とされる以上の権限が含まれていますが、今後も最高の互換性を提供します。

```
"Microsoft.Compute/diskEncryptionSets/read",

"Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.Compute/disks/delete",

"Microsoft.Compute/disks/endGetAccess/action",

"Microsoft.Compute/disks/read",

"Microsoft.Compute/disks/write",

"Microsoft.Compute/galleries/delete",

"Microsoft.Compute/galleries/images/delete",

"Microsoft.Compute/galleries/images/read",

"Microsoft.Compute/galleries/images/versions/delete",

"Microsoft.Compute/galleries/images/versions/read",

"Microsoft.Compute/galleries/images/versions/write",

"Microsoft.Compute/galleries/images/write",

"Microsoft.Compute/galleries/read",

"Microsoft.Compute/galleries/write",

"Microsoft.Compute/hostGroups/hosts/read",

"Microsoft.Compute/hostGroups/read",

"Microsoft.Compute/hostGroups/write",
```

```
"Microsoft.Compute/snapshots/beginGetAccess/action",
"Microsoft.Compute/snapshots/delete",
"Microsoft.Compute/snapshots/endGetAccess/action",
"Microsoft.Compute/snapshots/read",
"Microsoft.Compute/snapshots/write",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/restart/action",
"Microsoft.Compute/virtualMachines/start/action",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
```

```
"Microsoft.Resources/deployments/operationstatuses/read",

"Microsoft.Resources/deployments/read",

"Microsoft.Resources/deployments/validate/action",

"Microsoft.Resources/deployments/write",

"Microsoft.Resources/deployments/delete",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourceGroups/write",

"Microsoft.Resources/subscriptions/resourceGroups/delete",

"Microsoft.Storage/storageAccounts/delete",

"Microsoft.Storage/storageAccounts/listKeys/action",

"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/write",

"Microsoft.Resources/templateSpecs/read",

"Microsoft.Resources/templateSpecs/versions/read",
```

詳細情報

- 接続とリソース
- マシンカタログの作成
- CTX219211: Microsoft Azure Active Directory アカウントを設定する
- CTX219243: Azure サブスクリプションへの XenApp および XenDesktop アクセスを許可する
- CTX219271: サイト間 VPN を使用してハイブリッドクラウドを展開する

Microsoft System Center 仮想マシンマネージャー仮想化環境

Hyper-V と Microsoft System Center Virtual Machine Manager (VMM) を使用して仮想マシンを提供する場合は、このガイダンスに従ってください。

このリリースでは、システム要件に記載されているVMMバージョンがサポートされています。

> **注：**
>
> 混在するHyper-Vクラスター（異なるHyper-Vバージョンを実行しているサーバーを含む）はサポートされていません。
>
> Citrix Provisioning（旧Provisioning Services）およびMachine Creation Services™を使用して、以下をプロビジョニングできます。

- 第1世代でサポートされているデスクトップまたはサーバーOSのVM。
- セキュアブートのサポートを含む、第2世代でサポートされているデスクトップまたはサーバーOSのVM。

ハイパーバイザーのインストールと構成

> **重要:**
>
> すべてのDelivery Controllerは、VMMサーバーと同じフォレスト内にある必要があります。

1. サーバーにMicrosoft Hyper-VサーバーとVMMをインストールします。
2. すべてのControllerにSystem Center Virtual Machine Managerコンソールをインストールします。コンソールのバージョンは管理サーバーのバージョンと一致している必要があります。以前のコンソールでも管理サーバーに接続できますが、バージョンが異なる場合、VDAのプロビジョニングは失敗します。
3. 次のアカウント情報を確認してください。

   Studioでホストを指定するために使用するアカウントは、関連するHyper-Vマシンに対するVMM管理者またはVMM委任管理者である必要があります。このアカウントがVMMで委任管理者ロールのみを持っている場合、ホスト作成プロセス中にStudioにストレージデータが表示されません。

   > **ヒント:**

> VMM委任管理者を使用する場合、トップレベルのホストグループを定義し、その委任管理者にこのグループのみに対するフルアクセス権限を付与します。複数のホストグループには、複数のVMM委任管理者が必要です。ホストグループごとに1人の委任管理者を構成します。

> Studio統合に使用されるユーザーアカウントは、各Hyper-Vサーバーのadministrators ローカルセキュリティグループのメンバーである必要もあります。この構成は、VMの作成、更新、削除などのVMライフサイクル管理をサポートします。

Hyper-Vを実行しているサーバーにControllerをインストールすることはサポートされていません。

マスターVMを作成する

1. マスターVMにVDAをインストールし、パフォーマンスを向上させるためにデスクトップを最適化するオプションを選択します。
2. バックアップとして使用するために、マスターVMのスナップショットを作成します。

仮想デスクトップを作成する

MCSを使用してVMを作成する場合、サイトまたは接続を作成するときは、次の手順を実行します。

1. Microsoft仮想化ホストの種類を選択します。
2. アドレスをホストサーバーの完全修飾ドメイン名として入力します。
3. VMを作成する権限を持つ、以前に設定した管理者アカウントの資格情報を入力します。
4. **ホストの詳細**で、VMを作成するときに使用するクラスターまたはスタンドアロンホストを選択します。

   単一のHyper-Vホスト展開を使用している場合でも、クラスターまたはスタンドアロンホストを参照して選択します。

SMB 3ファイル共有上のMCS

VMストレージ用のSMB 3ファイル共有でMCSを使用して作成されたマシンカタログの場合、資格情報が次の要件を満たしていることを確認してください。これらの要件により、ControllerのHypervisor Communications Library（HCL）からの呼び出しがSMBストレージに正常に接続されます。

- VMMユーザーの資格情報には、SMBストレージへの完全な読み取り/書き込みアクセス権が含まれている必要があります。
- VMライフサイクルイベント中のストレージ仮想ディスク操作は、VMMユーザー資格情報を使用してHyper-Vサーバー経由で実行されます。

SMBストレージを使用する場合は、Controllerから個々のHyper-Vマシンへの認証資格情報セキュリティサポートプロバイダー（CredSSP）を有効にします。このプロセスは、Windows Server 2012上のHyper-VとVMM 2012 SP1で使用します。詳細については、CTX137465を参照してください。

HCLは`CredSSP`を使用してHyper-Vマシンへの接続を開きます。この機能は、Kerberosで暗号化されたユーザー資格情報をHyper-Vマシンに渡します。リモートHyper-Vマシン上のセッションでの**PowerShell**コマンドは、提供された資格情報で実行されます。この場合、ストレージへの通信コマンドが正しく機能するように、VMMユーザーの資格情報が使用されます。

次のタスクでは、HCLで生成され、SMB 3.0ストレージに対して動作するためにHyper-Vマシンに送信されるPowerShellスクリプトを使用します。

- **マスターイメージの統合**: マスターイメージは、MCSプロビジョニングスキーム（マシンカタログ）を作成します。マスターVMをクローンしてフラット化し、新しく作成されたディスクからVMを作成できるようにします（元のマスターVMへの依存関係を削除します）。

  root\\virtualization\\v2名前空間のConvertVirtualHardDisk

  例:

```
$ims = Get-WmiObject -class $class -namespace "root\\virtualization\\v2";

$result = $ims.ConvertVirtualHardDisk($diskName, $vhdastext)

$result
```

- **差分ディスクの作成:** マスターイメージを統合して生成されたマスターイメージから差分ディスクを作成します。その後、差分ディスクは新しいVMに接続されます。

  root\\virtualization\\v2名前空間のCreateVirtualHardDisk

  例:

```
$ims = Get-WmiObject -class $class -namespace "root\\virtualization\\v2";

$result = $ims.CreateVirtualHardDisk($vhdastext);

$result
```

- **IDディスクのアップロード:** HCLはIDディスクをSMBストレージに直接アップロードできません。そのため、Hyper-VマシンがIDディスクをストレージにアップロードしてコピーする必要があります。Hyper-VマシンはControllerからディスクを読み取ることができないため、HCLはまず次のようにHyper-Vマシン経由でIDディスクをコピーする必要があります。

  HCLは、管理者共有を介してIDをHyper-Vマシンにアップロードします。

  Hyper-Vマシンは、PowerShellリモートセッションで実行されているPowerShellスクリプトを介して、ディスクをSMBストレージにコピーします。Hyper-Vマシン上にフォルダーが作成され、そのフォルダーのアクセス許可はVMMユーザーのみにロックされます（リモートPowerShell接続を介して）。

  HCLは、管理者共有からファイルを削除します。

  HCLがIDディスクのHyper-Vマシンへのアップロードを完了すると、リモートPowerShellセッションはIDディスクをSMBストレージにコピーします。その後、Hyper-Vマシンから削除します。

  IDディスクフォルダーは、削除された場合でも再利用できるように再作成されます。

- **IDディスクのダウンロード:** アップロードと同様に、IDディスクはHyper-Vマシンを経由してHCLに渡されます。次のプロセスでは、Hyper-Vサーバー上にVMMユーザー権限のみを持つフォルダーが存在しない場合に作成します。

  Hyper-Vマシンは、PowerShellスクリプトを介してSMBストレージからローカルのHyper-Vストレージにディスクをコピーします。このスクリプトは、PowerShell V3リモートセッションで実行されます。

  HCL は、Hyper-V マシンの管理者共有からディスクをメモリに読み込みます。

  HCL は、管理者共有からファイルを削除します。

Citrix Hypervisor™ 仮想化環境

Citrix Hypervisor への接続を作成する

Citrix Hypervisor (旧 XenServer®) への接続を作成する場合、VM Power Admin またはそれ以上のレベルのユーザーの資格情報を指定する必要があります。

Citrix は、Citrix Hypervisor との通信を保護するために HTTPS を使用することを推奨しています。HTTPS を使用するには、Citrix Hypervisor にインストールされているデフォルトの SSL 証明書を置き換える必要があります。詳細については、CTX128656 を参照してください。

Citrix Hypervisor サーバーで高可用性が有効になっている場合、高可用性を構成できます。Citrix は、プールマスターに障害が発生した場合に Citrix Hypervisor サーバーとの通信を可能にするため、プール内のすべてのサーバー (高可用性の編集から) を選択することを推奨しています。

Citrix Hypervisor が vGPU をサポートしている場合、GPU の種類とグループを選択するか、パススルーすることができます。表示は、選択に専用の GPU リソースがあるかどうかを示します。

一つ以上の Citrix Hypervisor ホストで一時的なデータストレージにローカルストレージを使用する場合、プール内の各ストレージの場所に一意の名前があることを確認してください。(XenCenter® で名前を変更するには、ストレージを右クリックして名前プロパティを編集します。)

Citrix Provisioning（旧Provisioning Services）およびMachine Creation Services™（MCS）を使用して、以下をプロビジョニングできます。

- サポートされているデスクトップまたはサーバーOS VM用のレガシーBIOS。
- セキュアブートを含む、サポートされているデスクトップまたはサーバーOS VM用のUEFI。

> **注：**
>
> MCSを構成する際には、プールオペレーター以上の権限が必要です。

Citrix Hypervisor 接続に IntelliCache™ を使用する

IntelliCacheを使用すると、共有ストレージとローカルストレージの組み合わせを使用できるため、ホスト型VDI展開の費用対効果が高まります。これにより、パフォーマンスが向上し、ネットワークトラフィックが削減されます。ローカルストレージは共有ストレージからマスターイメージをキャッシュするため、共有ストレージへの読み取り回数が減少します。共有デスクトップの場

合、差分ディスクへの書き込みは、共有ストレージではなくホスト上のローカルストレージに書き込まれます。

- IntelliCacheを使用する場合、共有ストレージはNFSである必要があります。
- Citrix® は、可能な限り最速のデータ転送を確保するために、高性能なローカルストレージデバイスを使用することを推奨しています。

IntelliCache を使用するには、この製品と Citrix Hypervisor の両方で有効にする必要があります。

- Citrix Hypervisor をインストールする際、**シンプロビジョニングを有効にする (仮想デスクトップ向けに最適化されたストレージ)** を選択します。Citrix は、IntelliCache が有効なサーバーと無効なサーバーが混在するプールをサポートしていません。詳細については、Citrix Hypervisor のドキュメントを参照してください。
- Citrix Virtual Apps and Desktops™ では、IntelliCache はデフォルトで無効になっています。この設定は、Citrix Hypervisor 接続を作成するときにのみ変更できます。後で IntelliCache を無効にすることはできません。Citrix Hypervisor 接続を追加する場合：
  - ストレージの種類として**「Shared」**を選択します。
  - **「Use IntelliCache」**チェックボックスをオンにします。

必要な Citrix Hypervisor の権限

Citrix Hypervisor の権限はロールベース (RBAC) です。

詳細については、「Role-based access control」を参照してください。

権限が増加する順序でのロール階層は、次のとおりです。Read-Only → VM Operator → VM Admin → VM Power Admin → Pool Operator → Pool Admin。

次のセクションでは、各プロビジョニングタスクに必要な最小ロールをまとめます。

ホスト接続の作成

タスク	必要な最小ロール
XenServerから取得した情報を使用してホスト接続を追加する	読み取り専用
ユーザーとその割り当てられた役割を表示する	読み取り専用

VM の電源管理

タスク	必要な最小ロール
VMの電源をオンまたはオフにする	VMオペレーター

仮想マシンの作成、更新、または削除

タスク	必要な最小ロール
既存のスナップショットスケジュールにVMを追加または削除する	VM電源管理者
スナップショットスケジュールの追加、変更、削除	プールオペレーター
マスターイメージの公開	プールオペレーター（スイッチポートロックが必要）
マシンカタログを作成する	プールオペレーター: スイッチポートロックが必要
VMの追加または削除（GPU対応VMではない）	VM管理者
VMの追加または削除（GPU対応VM）	プールオペレーター
仮想ディスクまたはCDデバイスの追加、削除、または構成	VM管理者
タグの管理	VMオペレーター

RBACの役割と権限の詳細については、「RBACの役割と権限」を参照してください。

スイッチポートロックの詳細については、「スイッチポートロックの使用」を参照してください。

Citrix Hypervisor 接続を使用してマシンカタログを作成する

GPU対応マシンには、専用のマスターイメージが必要です。これらのVMには、GPUをサポートするビデオカードドライバーが必要です。GPU対応マシンを構成して、VMがGPUを操作に使用するソフトウェアで動作できるようにします。

1. XenCenterで、標準VGA、ネットワーク、およびvCPUを使用してVMを作成します。

2. VM構成を更新して、GPUの使用（パススルーまたはvGPUのいずれか）を有効にします。
3. サポートされているオペレーティングシステムをインストールし、RDPを有効にします。
4. Citrix VM ToolsとNVIDIAドライバーをインストールします。
5. パフォーマンスを最適化するために、Virtual Network Computing (VNC) 管理コンソールをクリアし、VMを再起動します。
6. RDPを使用するように求められます。RDPを使用してVDAをインストールし、VMを再起動します。
7. 必要に応じて、他のGPUマスターイメージのベースラインテンプレートとしてVMのスナップショットを作成します。
8. RDPを使用して、XenCenterで構成され、GPU機能を使用する顧客固有のアプリケーションをインストールします。

詳細情報

- 接続とリソース
- マシンカタログの作成

マイクロソフト システムセンター コンフィギュレーションマネージャー 環境

アプリケーションとデスクトップへのアクセスを管理するために Microsoft System Center Configuration Manager (Configuration Manager) を使用しているサイトは、以下のオプションを使用してその利用を Citrix Virtual Apps and Desktops™ に拡張できます。

- SCCM を使用した VDA のインストール。
- **Configuration Manager Wake Proxy 機能:** Remote PC Access の Wake on LAN 機能は Configuration Manager でサポートされています。詳細については、「Wake on LAN - SCCM 統合」を参照してください。
- **Citrix Virtual Apps and Desktops のプロパティ:** プロパティ を使用すると、Configuration Manager を介して管理する Citrix Virtual Desktops™ を識別できます。（一部のバージョンでは、Configuration Manager は Citrix Virtual Apps and Desktops の旧名である XenApp および XenDesktop を使用します。）

プロパティ

仮想デスクトップを管理するために、Microsoft System Center Configuration Manager でプロパティを利用できます。

Configuration Manager に表示されるブール型プロパティは、true または false ではなく、`1` または `0` として表示されます。

これらのプロパティは、`Root\Citrix\DesktopInformation` 名前空間の `Citrix_virtualDesktopInfo` クラスで利用できます。プロパティ名は Windows Management Instrumentation (WMI) プロバイダーから取得されます。

プロパティ	説明
`AssignmentType`	IsAssigned の値を設定します。有効な値は、`ClientIP`、`ClientName`、`None`、および `User` です (`IsAssigned` を `True` に設定します)。
`BrokerSiteName`	`HostIdentifier` と同じ値を返します。
`DesktopCatalogName`	デスクトップに関連付けられているマシンカタログ。
`DesktopGroupName`	デスクトップに関連付けられているデリバリーグループ。
`HostIdentifier`	`BrokerSiteName` と同じ値を返します。
`IsAssigned`	デスクトップをユーザーに割り当てるには `True`、ランダムなデスクトップの場合は `False` に設定します。
`IsMasterImage`	環境に関する決定を可能にします。たとえば、プロビジョニングされたマシンではなく、イメージにアプリケーションをインストールします。有効な値は次のとおりです。イメージとして使用されるVMでは `True`。この値は、インストール時に選択に基づいて設定されるか、そのイメージからプロビジョニングされたVMではクリアされます。
`IsVirtualMachine`	仮想マシンの場合は `True`、物理マシンの場合は `false`。
`OSChangesPersist`	デスクトップオペレーティングシステムイメージが再起動のたびにクリーンな状態にリ

プロパティ	説明
	セットされる場合は `False`。それ以外の場合は `true`。
`PersistentDataLocation`	Configuration Manager が永続データを保存する場所。これはユーザーにはアクセスできません。
`BrokerSiteName`、`DesktopCatalogName`、`DesktopGroupName`、`HostIdentifier`	デスクトップがControllerに登録されるときに決定されます。完全に登録されていないデスクトップの場合はnullです。

プロパティを収集するには、Configuration Manager でハードウェアインベントリを実行します。プロパティを表示するには、Configuration Manager Resource Explorer を使用します。これらの場合、名前にはスペースが含まれるか、プロパティ名とわずかに異なります。たとえば、`BrokerSiteName` は `Broker Site Name` として表示されます。

- Citrix VDA から Citrix WMI プロパティを収集するように Configuration Manager を構成する
- Citrix WMI プロパティを使用してクエリベースのデバイスコレクションを作成する
- Citrix WMI プロパティに基づいてグローバル条件を作成する
- グローバル条件を使用してアプリケーション展開タイプの要件を定義する

`Root\ccm_vdi` 名前空間の Microsoft クラス `CCM_DesktopMachine` で Microsoft プロパティを使用することもできます。詳細については、Microsoft のドキュメントを参照してください。

VMware 仮想化環境

仮想マシンを提供するのにVMwareを使用する場合は、このガイダンスに従ってください。

vCenter Serverと適切な管理ツールをインストールします。(vSphere vCenter Linked Mode操作はサポートされていません。)

MCSを使用する予定がある場合は、vCenter ServerのDatastore Browser機能（`<https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2101567>`で説明）を無効にしないでください。この機能を無効にすると、MCSは正しく動作しません。

Citrix Provisioning（旧Provisioning Services）およびMachine Creation Services™を使用して、以下をプロビジョニングできます。

- サポートされているデスクトップまたはサーバーOS VM用のレガシーBIOS。
- セキュアブートを含む、サポートされているデスクトップまたはサーバーOS VM用のUEFI。

必要な権限

VMwareユーザーアカウントと、この記事に記載されている権限のセットまたはすべての権限を持つ1つ以上のVMwareロールを作成します。ロールの作成は、Citrix DaaS™のさまざまな操作をいつでも要求するためにユーザーの権限に必要とされる特定の粒度レベルに基づいて行います。ユーザー固有の権限をいつでも付与するには、**子に伝播**オプションを選択した状態で、少なくともデータセンターレベルで、それらをそれぞれのロールに関連付けます。ただし、`StorageProfile`権限と特定の`Tags`権限については、**子に伝播**なしで、Root vCenter Serverレベルで権限を適用します。各テーブルの注記を参照してください。

次の表は、Citrix Virtual Apps and Desktops™の操作と、必要な最小限のVMware権限とのマッピングを示しています。

> **注：**
>
> 権限リストの表示名、特に*ユーザーインターフェイス*は、一部のvSphereバージョンで異なります。たとえば、vSphere 6.7では、*ユーザーインターフェイス*権限は、このページに記載されている必要な権限で説明されている**Settings**および**Memory**ではなく、**Change Memory**および**Change Settings**です。

接続とリソースを追加する

SDK	ユーザーインターフェイス
System.Anonymous、System.Read、およびSystem.View	自動的に追加されます。組み込みの読み取り専用ロールを使用できます。

電源管理

SDK	ユーザーインターフェイス
VirtualMachine.Interact.PowerOff	仮想マシン > インタラクション > 電源オフ
VirtualMachine.Interact.PowerOn	仮想マシン > インタラクション > 電源オン
VirtualMachine.Interact.Reset	仮想マシン > インタラクション > リセット

SDK	ユーザーインターフェイス
VirtualMachine.Interact.Suspend	仮想マシン > インタラクション > サスペンド
Datastore.Browse	Datastore > データストアの参照

マシンのプロビジョニング (Machine Creation Services)

MCS を使用してマシンをプロビジョニングするには、次の権限が必要です。

SDK	ユーザーインターフェイス
Datastore.AllocateSpace	Datastore > スペースの割り当て
Datastore.Browse	Datastore > データストアの参照
Datastore.FileManagement	Datastore > 低レベルファイル操作
Network.Assign	Network > ネットワークの割り当て
Resource.AssignVMToPool	リソース > 仮想マシンをリソースプールに割り当てる
VirtualMachine.Config.AddExistingDisk	仮想マシン > 構成 > 既存のディスクを追加
VirtualMachine.Config.AddNewDisk	仮想マシン > 構成 > 新しいディスクを追加
仮想マシン.構成.デバイスの追加または削除	仮想マシン > 構成 > デバイスの追加または削除
VirtualMachine.Config.AdvancedConfig	仮想マシン > 構成 > 詳細設定
VirtualMachine.Config.RemoveDisk	仮想マシン > 構成 > ディスクの削除
VirtualMachine.Config.CPUCount	仮想マシン > 構成 > CPU数の変更
VirtualMachine.Config.Memory	仮想マシン > 構成 > メモリの変更
VirtualMachine.Config.Settings	仮想マシン > 構成 > 設定の変更
VirtualMachine.Interact.PowerOff	仮想マシン > インタラクション > 電源オフ
VirtualMachine.Interact.PowerOn	仮想マシン > インタラクション > 電源オン

SDK	ユーザーインターフェイス
VirtualMachine.Interact.Reset	仮想マシン > インタラクション > リセット
VirtualMachine.Interact.Suspend	仮想マシン > インタラクション > サスペンド
VirtualMachine.Inventory.CreateFromExisting	仮想マシン > インベントリ > 既存から作成
VirtualMachine.Inventory.Create	仮想マシン > インベントリ > 新規作成
VirtualMachine.Inventory.Delete	仮想マシン > インベントリ > 削除
VirtualMachine.Provisioning.Clone	仮想マシン > プロビジョニング > 仮想マシンのクローン作成
VirtualMachine.State.CreateSnapshot	vSphere 5.0、Update 2、vSphere 5.1、Update 1、および vSphere 6.x、Update 1: 仮想マシン > 状態 > スナップショットの作成; vSphere 5.5: 仮想マシン > スナップショット管理 > スナップショットの作成

イメージの更新とロールバック

SDK	ユーザーインターフェイス
Datastore.AllocateSpace	Datastore > スペースの割り当て
Datastore.Browse	Datastore > データストアの参照
Datastore.FileManagement	Datastore > 低レベルファイル操作
Network.Assign	Network > ネットワークの割り当て
Resource.AssignVMToPool	リソース > 仮想マシンをリソースプールに割り当てる
VirtualMachine.Config.AddExistingDisk	仮想マシン > 構成 > 既存のディスクを追加
VirtualMachine.Config.AddNewDisk	仮想マシン > 構成 > 新しいディスクを追加
VirtualMachine.Config.AdvancedConfig	仮想マシン > 構成 > 詳細設定
VirtualMachine.Config.RemoveDisk	仮想マシン > 構成 > ディスクの削除

SDK	ユーザーインターフェイス
VirtualMachine.Interact.PowerOff	仮想マシン > インタラクション > 電源オフ
VirtualMachine.Interact.PowerOn	仮想マシン > インタラクション > 電源オン
VirtualMachine.Interact.Reset	仮想マシン > インタラクション > リセット
VirtualMachine.Inventory.CreateFromExisting	仮想マシン > インベントリ > 既存から作成
VirtualMachine.Inventory.Create	仮想マシン > インベントリ > 新規作成
VirtualMachine.Inventory.Delete	仮想マシン > インベントリ > 削除
VirtualMachine.Provisioning.Clone	仮想マシン > プロビジョニング > 仮想マシンのクローン作成

プロビジョニングされたマシンの削除

SDK	ユーザーインターフェイス
Datastore.Browse	Datastore > データストアの参照
Datastore.FileManagement	Datastore > 低レベルファイル操作
VirtualMachine.Config.RemoveDisk	仮想マシン > 構成 > ディスクの削除
VirtualMachine.Interact.PowerOff	仮想マシン > インタラクション > 電源オフ
VirtualMachine.Inventory.Delete	仮想マシン > インベントリ > 削除

ストレージプロファイル (vSAN)

vSANデータストアでカタログ作成中にストレージポリシーを表示、作成、または削除するには、以下の権限が必要です。

SDK	ユーザーインターフェイス
StorageProfile.Update	プロファイル駆動型ストレージ > プロファイル駆動型ストレージの更新。vSphere 8 の場合: VMストレージポリシー > VMストレージポリシーの更新

SDK	ユーザーインターフェイス
StorageProfile.View	PROFILE-DRIVEN STORAGE > プロファイル駆動型ストレージビュー。vSphere 8 の場合: VM ストレージポリシー > VM ストレージポリシーの表示

注：

ストレージプロファイルの権限は、**子に伝播**せずに、ルートvCenter Serverレベルで適用します。

タグとカスタム属性

タグとカスタム属性を使用すると、vSphereインベントリで作成されたVMにメタデータを添付でき、これらのオブジェクトの検索とフィルタリングが容易になります。タグまたはカテゴリを作成、編集、割り当て、削除するには、次の権限が必須です。

SDK	ユーザーインターフェイス
InventoryService.Tagging.CreateTag	vSphere タグ付け > vSphere タグの作成
InventoryService.Tagging.CreateCategory	vSphere タグ付け > vSphere タグカテゴリの作成
InventoryService.Tagging.EditTag	vSphere タグ付け > vSphere タグの編集
InventoryService.Tagging.EditCategory	vSphere タグ付け > vSphere タグカテゴリの編集
InventoryService.Tagging.DeleteTag	vSphere タグ付け > vSphere タグの削除
InventoryService.Tagging.DeleteCategory	vSphere タグ付け > vSphere タグカテゴリの削除
InventoryService.Tagging.AttachTag	vSphere タグ付け > vSphere タグの割り当てまたは割り当て解除
InventoryService.Tagging.ObjectAttachable	vSphere タグ付け > オブジェクトへの vSphere タグの割り当てまたは割り当て解除

SDK	ユーザーインターフェイス
Global.ManageCustomFields	グローバル > カスタム属性の管理
Global.SetCustomField	グローバル > カスタム属性の設定

注：

- MCS がマシンカタログを作成すると、ターゲット VM に特別な名前タグを付けます。これらのタグは、マスターイメージを MCS によって作成された VM と区別し、MCS によって作成された VM がイメージ準備に使用されるのを防ぎます。vCenter の `XdProvisioned` 属性の値によって違いを識別できます。MCS が VM を作成する場合、この属性は **True** に設定されます。
- ルート vCenter Server レベルで `InventoryService.Tagging.AttachTag` 権限を、**子への伝播**なしで適用します。

暗号化操作

暗号化操作の特権は、誰がどの種類のオブジェクトに対してどの種類の暗号化操作を実行できるかを制御します。vSphere Native Key Provider は `Cryptographer.*` 特権を使用します。暗号化操作には、以下の最小限の権限が必要です。

SDK	ユーザーインターフェイス
Cryptographer.Access	特権 > すべての特権 > 暗号化操作 > 直接アクセス
Cryptographer.AddDisk	特権 > すべての特権 > 暗号化操作 > ディスクの追加
Cryptographer.Clone	特権 > すべての特権 > 暗号化操作 > クローン
Cryptographer.Encrypt	特権 > すべての特権 > 暗号化操作 > 暗号化
Cryptographer.EncryptNew	特権 > すべての特権 > 暗号化操作 > 新規暗号化
Cryptographer.Decrypt	特権 > すべての特権 > 暗号化操作 > 復号化

SDK	ユーザーインターフェイス
Cryptographer.Migrate	特権 > すべての特権 > 暗号化操作 > 移行
Cryptographer.ReadKeyServersInfo	特権 > すべての特権 > 暗号化操作 > KMS情報の読み取り

マシンのプロビジョニング (Citrix Provisioning™)

Citrix Provisioningコンソールを介してCitrix Virtual Apps and Desktopsセットアップウィザードおよびデバイスのエクスポートウィザードを使用してVMをプロビジョニングするには、テンプレートをクローンおよび展開するためのこれらの権限が必要です。ホスティング接続の作成時に権限を設定します。マシンのプロビジョニング（Machine Creation Services）のすべての権限と、以下の権限が必要です。

SDK	ユーザーインターフェイス
VirtualMachine.Config.AddRemoveDevice	仮想マシン > 構成 > デバイスの追加または削除
VirtualMachine.Config.CPUCount	仮想マシン > 構成 > CPU数の変更
VirtualMachine.Config.Memory	仮想マシン > 構成 > メモリ
VirtualMachine.Config.Settings	仮想マシン > 構成 > 設定
VirtualMachine.Provisioning.CloneTemplate	仮想マシン > プロビジョニング > テンプレートのクローン作成
VirtualMachine.Provisioning.DeployTemplate	仮想マシン > プロビジョニング > テンプレートの展開
VApp.Export	vApp > エクスポート

注：

マシンプロファイルを使用してMCSマシンカタログを作成するには、`VApp.Export`が必要です。

証明書を取得してインポートする

vSphere通信を保護するため、Citrix®はHTTPではなくHTTPSを使用することを推奨します。

HTTPSにはデジタル証明書が必要です。組織のセキュリティポリシーに準拠した認証局から発行されたデジタル証明書を使用してください。

認証局から発行されたデジタル証明書を使用できない場合は、VMwareがインストールした自己署名証明書を使用できます。この方法は、組織のセキュリティポリシーで許可されている場合にのみ使用してください。VMware vCenter証明書を各Delivery Controllerに追加します。

1. vCenter Serverを実行しているコンピューターの完全修飾ドメイン名（FQDN）を、そのサーバーのhostsファイル（`%SystemRoot%/WINDOWS/system32/Drivers/etc/`）に追加します。この手順は、vCenter Serverを実行しているコンピューターのFQDNがドメインネームシステムにまだ存在しない場合にのみ必要です。
2. 以下の3つの方法のいずれかを使用してvCenter証明書を取得します。

   vCenterサーバーから。

   a. rui.crt ファイルを vCenter サーバーから Delivery Controllers でアクセス可能な場所にコピーします。
   b. Controller で、エクスポートされた証明書の場所に移動し、rui.crt ファイルを開きます。

   Web ブラウザーを使用して証明書をダウンロードします。 Internet Explorer を使用している場合は、Internet Explorer を右クリックし、**管理者として実行**を選択して証明書をダウンロードまたはインストールします。

   a. Web ブラウザーを開き、vCenter サーバーへの安全な Web 接続を行います (例: `<https://server1.domain1.com)>`)。
   b. セキュリティ警告を受け入れます。
   c. 証明書エラーが表示されているアドレスバーをクリックします。
   d. 証明書を表示し、 タブをクリックします。
   e. プロンプトが表示されたら名前を指定して、**ファイルにコピーして .CER 形式でエクスポート**を選択します。
   f. エクスポートされた証明書を保存します。
   g. エクスポートされた証明書の場所に移動し、.CER ファイルを開きます。

   管理者として実行している Internet Explorer から直接インポートします。

- Web ブラウザーを開き、vCenter サーバーへの安全な Web 接続を行います (例: `<https://server1.domain1.com)>`)。
- セキュリティ警告を受け入れます。
- 証明書エラーが表示されているアドレスバーをクリックします。
- 証明書を表示します。

3. 各Controllerの証明書ストアに証明書をインポートします。

   a. **証明書のインストール**オプションをクリックし、**ローカルコンピューター**を選択して、**次へ**をクリックします。

   b. **証明書をすべて次のストアに配置する**を選択し、**参照**をクリックします。**信頼されたユーザー**を選択し、**OK**をクリックします。**次へ**をクリックし、**完了**をクリックします。

   インストール後にvSphereサーバーの名前を変更した場合は、新しい証明書をインポートする前に、そのサーバーで新しい自己署名証明書を生成する必要があります。

構成に関する考慮事項

マスターVMを作成する:

マスターVMを使用して、マシンカタログでユーザーデスクトップとアプリケーションを提供します。ハイパーバイザーで、次の操作を行います。

1. マスターVMにVDAをインストールし、パフォーマンスを向上させるデスクトップの最適化オプションを選択します。
2. バックアップとして使用するために、マスターVMのスナップショットを作成します。

接続を作成する:

接続作成ウィザードで：

- VMware接続の種類を選択します。
- vCenter SDKのアクセスポイントのアドレスを指定します。
- 以前に設定した、VMを作成する権限を持つVMwareユーザーアカウントの資格情報を指定します。ユーザー名はdomain/usernameの形式で指定します。

VMware SSLサムプリント

VMware SSLサムプリント機能により、VMware vSphereハイパーバイザーへのホスト接続を手動で作成する必要がなくなります。接続を作成する前に、サイト内のDelivery Controllerとハイパーバイザーの証明書との間に信頼関係を手動で作成する必要はなくなりました。

VMware SSLサムプリント機能は、信頼されていない証明書のサムプリントをサイトデータベースに保存します。この構成により、ハイパーバイザーは、コントローラーによってではないにしても、Citrix Virtual Apps and Desktopsによって継続的に信頼できるものとして識別されることが保証されます。

StudioでvSphereホスト接続を作成する際、接続先のマシンの証明書を表示できるダイアログボックスが表示されます。その後、それを信頼するかどうかを選択できます。

トラブルシューティング

カタログの作成に失敗した場合は、CTX294978を参照してください。

VMware クラウドおよびパートナーソリューション

Citrix Virtual Apps and Desktops™ は、以下の VMware クラウドおよびパートナーソリューションをサポートしています。

- Azure VMware ソリューション (AVS)(#azure-vmware-solution-avs-integration)
- Google Cloud VMware エンジン(#google-cloud-vmware-engine)
- VMware クラウド オン Amazon Web Services (AWS)(#vmware-cloud-on-amazon-web-services-aws)

Azure VMware ソリューション (AVS) の統合

Citrix Virtual Apps and Desktop サービスは AVS をサポートしています。AVS は、Azure インフラストラクチャによって作成された vSphere クラスターを含むクラウドインフラストラクチャを提供します。Citrix Virtual Apps and Desktop サービスを活用して、オンプレミス環境で vSphere を使用する場合と同じ方法で、AVS を使用して VDA ワークロードをプロビジョニングします。

AVS クラスターのセットアップ

Citrix Virtual Apps™ and Desktop サービスで AVS を使用できるようにするには、Azure で次の手順を実行します。

- ホストクォータを要求する
- Microsoft.AVS リソース プロバイダーを登録する
- ネットワークチェックリスト
- Azure VMware Solution プライベートクラウドを作成する
- Azure VMware Solution プライベートクラウドにアクセスする
- AzureでVMwareプライベートクラウドのネットワークを構成する

- Azure VMware Solution の DHCP を構成する
- Azure VMware Solution にネットワークセグメントを追加する
- Azure VMware Solution 環境を確認する

AZURE ENTERPRISE AGREEMENTのお客様のホストクォータを要求する

Azureポータルの**ヘルプとサポート**ページで、**新しいサポートリクエスト**を選択し、次の情報を含めます。

- 問題の種類: 技術
- サブスクリプション: サブスクリプションを選択してください
- サービス: すべてのサービス > Azure VMware Solution
- リソース: 一般的な質問
- 概要: 容量が必要
- 問題の種類: 容量管理の問題
- 問題のサブタイプ: 追加のホストクォータ/容量に関する顧客からの要求

サポートチケットの に、 タブで次の情報を含めます。

- POC または本番環境
- リージョン名
- ホスト数
- その他の詳細

> **注：**

> AVS には最低 3 つのホストが必要であり、N+1 ホストの冗長性を使用することをお勧めします。

> サポート チケットの詳細を指定したら、 を選択して Azure にリクエストを送信します。

MICROSOFT.AVS リソース プロバイダーを登録する

ホスト クォータを要求した後、リソース プロバイダーを登録します。

1. Azureポータルにサインインします。
2. Azure portal メニューで、 を選択します。
3. メニューで、サブスクリプションを入力し、 を選択します。

4. サブスクリプション リストからサブスクリプションを選択します。
5. を選択し、検索バーに **Microsoft.AVS** と入力します。
6. リソース プロバイダーが登録されていない場合は、 を選択します。

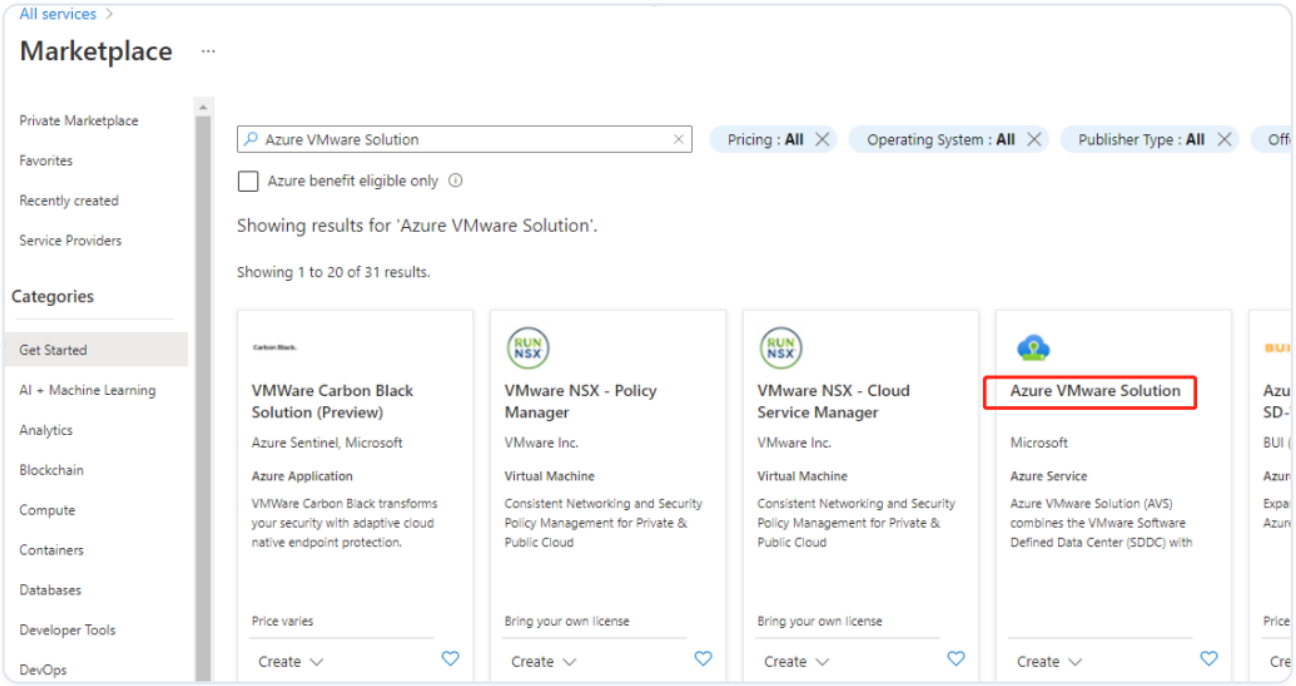
ネットワークに関する考慮事項

AVSは、特定のネットワークアドレス範囲とファイアウォールポートを必要とするネットワークサービスを提供します。詳細については、Azure VMware Solution のネットワーク計画チェックリストを参照してください。

AZURE VMWARE SOLUTION プライベートクラウドを作成する

環境のネットワーク要件を考慮した後、AVS プライベートクラウドを作成します。

1. Azureポータルにサインインします。
2. **新しいリソースの作成**を選択します。
3. **Marketplace の検索**テキストボックスに、*Azure VMware Solution*と入力し、リストから**Azure VMware Solution**を選択します。



image

Azure VMware Solutionウィンドウで、:

1. **作成**を選択します。
2. タブをクリックします。
3. 以下の表の情報を使用して、フィールドに値を入力します。

フィールド	値
サブスクリプション	展開に使用するサブスクリプションを選択します。Azure サブスクリプション内のすべてのリソースはまとめて請求されます。
リソースグループ	プライベートクラウドのリソースグループを選択します。Azure リソースグループは、Azure リソースがデプロイおよび管理される論理コンテナです。または、プライベートクラウド用に新しいリソースグループを作成することもできます。
場所	east us などの場所を選択します。これは、計画フェーズで定義したリージョンです。
リソース名	Azure VMware Solution プライベートクラウドの名前を指定します。
SKU	AV36 を選択します。
ホスト	プライベートクラウドクラスターに割り当てられたホストの数を示します。デフォルト値は 3で、デプロイ後に増減できます。
アドレスブロック	プライベートクラウドの IP アドレスブロックを指定します。CIDR はプライベートクラウド管理ネットワークを表し、vCenter Server や NSX-T Manager などのクラスター管理サービスに使用されます。/22 アドレス空間を使用します（例: 10.175.0.0/22）。アドレスは一意であり、他の Azure 仮想ネットワークやオンプレミスネットワークと重複しないようにしてください。
仮想ネットワーク	Azure VMware Solution ExpressRoute 回線は展開後の手順で確立されるため、ここは空白のままにします。

プライベートクラウドの作成画面で：

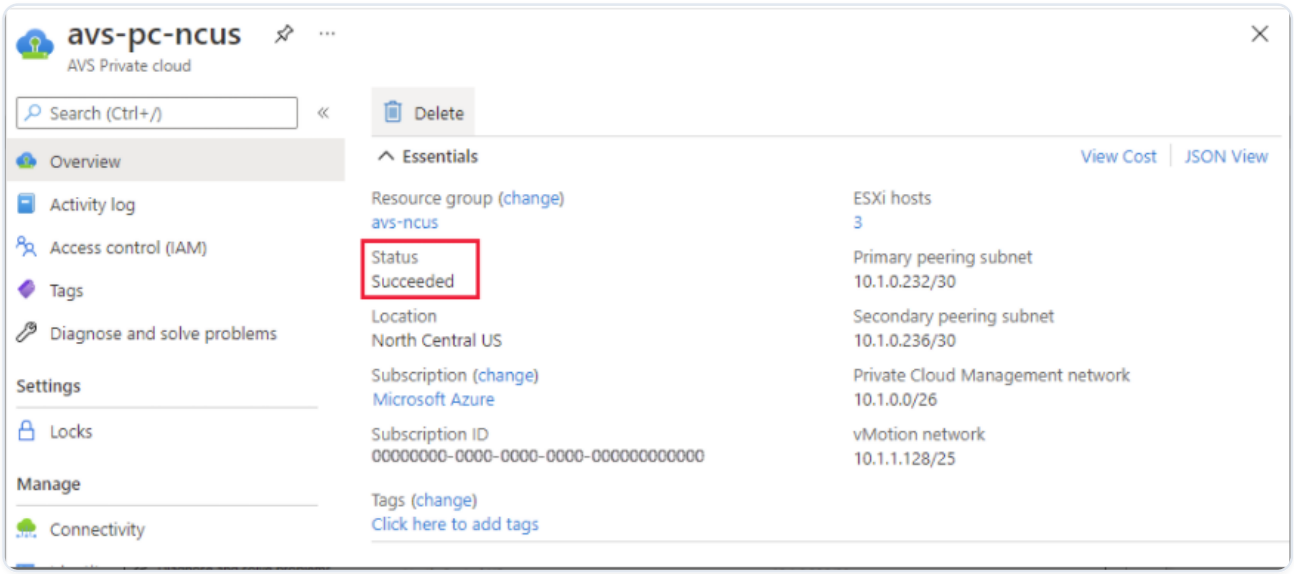
1. フィールドで、AVS が存在するリージョンを選択します。リソースグループのリージョンは AVS リージョンと同じです。

2. フィールドで、 を選択します。
3. 「**アドレスブロック**」フィールドにIPアドレスを指定します。例: 10.15.0.0/22。
4. 「**確認 + 作成**」を選択します。
5. 情報を確認したら、「**作成**」をクリックします。

Azure ASV プライベートクラウドの作成(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/azure-avs-create-private-cloud.png)

> **ヒント:**
>
> プライベートクラウドの作成には3〜4時間かかる場合があります。クラスターに単一のホストを追加するには30〜45分かかる場合があります。

> 展開が成功したことを確認します。作成したリソースグループに移動し、プライベートクラウドを選択します。**ステータス**が**成功**になったら、展開は完了です。



AZURE VMWARE SOLUTION プライベートクラウドにアクセスする

プライベートクラウドを作成したら、Windows VMを作成し、プライベートクラウドのローカルvCenterに接続します。
新しいWindows仮想マシンの作成

1. リソースグループで、**+ 追加**を選択し、**Microsoft Windows 10/2016/2019**を検索して選択します。
2. **Create** をクリックします。
3. 必要な情報を入力し、「**確認 + 作成**」を選択します。

4. 検証が完了したら、「**作成**」を選択して仮想マシンの作成プロセスを開始します。

プライベートクラウドのローカルvCenterに接続する

1. クラウド管理者として **vSphere Client with VMware vCenter SSO** にサインインします。

   Azure ASV vSphere ログイン(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/azure-avs-vsphere-login.png)

2. Azure portal でプライベートクラウドを選択し、 **>** を選択します。

プライベートクラウドのvCenterおよびNSX-T ManagerのURLとユーザー資格情報が表示されます。

Azure ASV セットアップ vCenter(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/azure-avs-setup-vcenter.png)

URLとユーザー資格情報を確認した後:

1. 前の手順で作成したVMに移動し、仮想マシンに接続します。
2. Windows VMでブラウザを開き、vCenterとNSX-T ManagerのURLを2つのブラウザタブで開きます。vCenterタブで、前の手順で取得した*cloudadmin@vmcp.local*ユーザーの資格情報を入力します。

AZUREでVMWAREプライベートクラウドのネットワークを構成する

ASVプライベートクラウドにアクセスした後、仮想ネットワークとゲートウェイを作成してネットワークを構成します。
仮想ネットワークを作成する

1. Azureポータルにサインインします。
2. 以前に作成したリソースグループに移動します。
3. 新しいリソースを定義するには、 を選択します。
4. テキストボックスに「*仮想ネットワーク*」と入力します。仮想ネットワークリソースを見つけて選択します。
5. 「**仮想ネットワーク**」ページで、「**作成**」を選択してプライベートクラウドの仮想ネットワークを設定します。
6. 「**仮想ネットワークの作成**」ページで、仮想ネットワークの詳細を入力します。
7. 「**基本**」タブで、仮想ネットワークの名前を入力し、適切なリージョンを選択して、「**次へ：IPアドレス**」をクリックします。
8. 「**IPアドレス**」タブのIPv4アドレス空間で、以前に作成したアドレスを入力します。

> **重要:**
>
> プライベートクラウドを作成したときに使用したアドレス空間と重複しないアドレスを使用してください。
>
> アドレス空間を入力した後:

1. 「**+ サブネットの追加**」を選択します。
2. 「**サブネットの追加**」ページで、サブネットに名前と適切なアドレス範囲を割り当てます。
3. 「**追加**」をクリックします。
4. 「**確認 + 作成**」を選択します。
5. 情報を確認し、「**作成**」をクリックします。デプロイが完了すると、仮想ネットワークがリソースグループに表示されます。

仮想ネットワークゲートウェイを作成する
仮想ネットワークを作成した後、仮想ネットワークゲートウェイを作成します。

1. リソースグループで、「**+ 追加**」を選択して新しいリソースを追加します。
2. 「**Search the Marketplace**」テキストボックスに「*virtual network gateway*」と入力します。仮想ネットワークリソースを見つけて選択します。
3. 「**Virtual Network gateway**」ページで、「**Create**」をクリックします。
4. 「**Create virtual network gateway**」ページの「**Basics**」タブで、フィールドに値を入力します。
5. 「**Review + create**」をクリックします。

Azure ASV セットアップ vCenter(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/azure-avs-create-virtual-gateway.png)

仮想ネットワークゲートウェイの構成を確認したら、**作成**をクリックして仮想ネットワークゲートウェイを展開します。 展開が完了したら、**ExpressRoute**接続をAzure AVSプライベートクラウドを含む仮想ネットワークゲートウェイに接続します。

EXPRESSROUTEを仮想ネットワークゲートウェイに接続する

仮想ネットワークゲートウェイを展開した後、それとAzure AVSプライベートクラウドの間に接続を追加します。

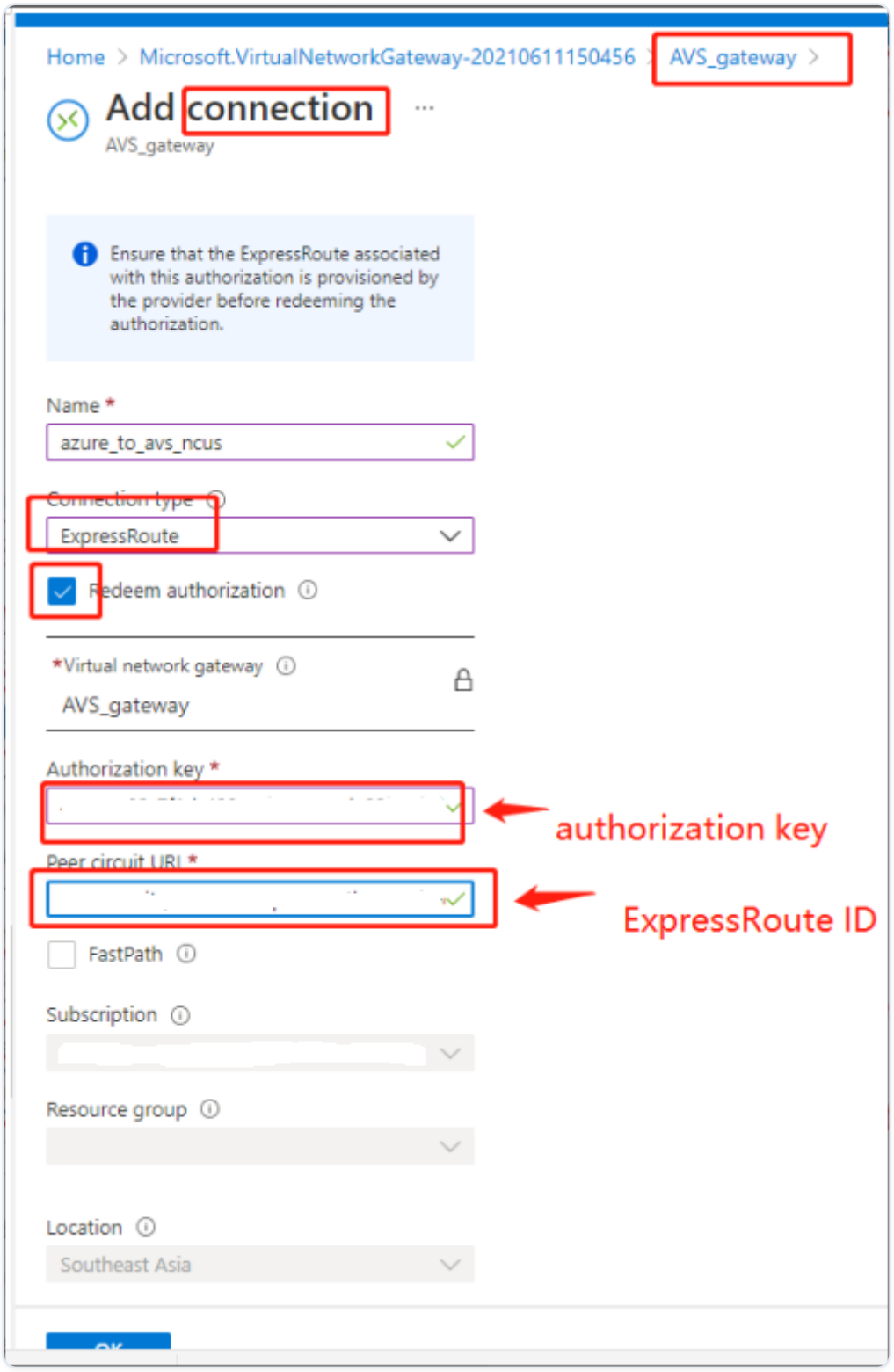
1. ExpressRoute承認キーを要求します。

2. Azureポータルで、**Azure VMware Solution private cloud**に移動します。「**Manage> Connectivity > ExpressRoute**」を選択し、次に「**+ Request an authorization key**」を選択します。

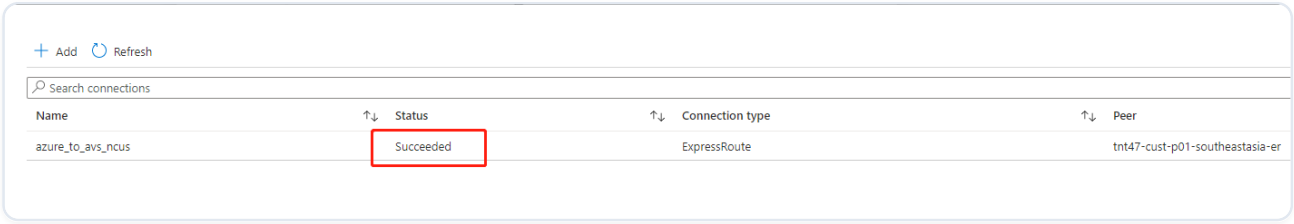
Azure ASV 承認キーの要求(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/azure-avs-expressroute.png)

承認キーを要求した後：

1. キーの名前を入力し、「**Create**」をクリックします。キーの作成には約30秒かかる場合があります。作成されると、新しいキーはプライベートクラウドの承認キーのリストに表示されます。
2. **承認キー**と**ExpressRoute ID**をコピーします。これらはピアリングプロセスを完了するために必要です。承認キーはしばらくすると消えるため、表示されたらすぐにコピーしてください。
3. 使用する**仮想ネットワークゲートウェイ**に移動し、「**Connections> + Add**」を選択します。
4. 「**接続の追加**」ページで、フィールドの値を入力し、「**OK**」を選択します。



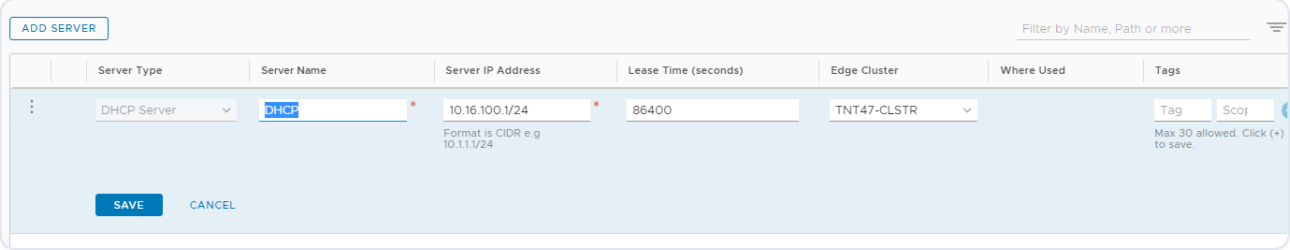
ExpressRoute回線と仮想ネットワーク間の接続が確立されます。



AZURE VMWARE SOLUTION の DHCP を構成する

ExpressRouteを仮想ゲートウェイに接続した後、DHCPを構成します。
NSX-T を使用して DHCP サーバーをホストする
NSX-T Manager で、次の手順を実行します。

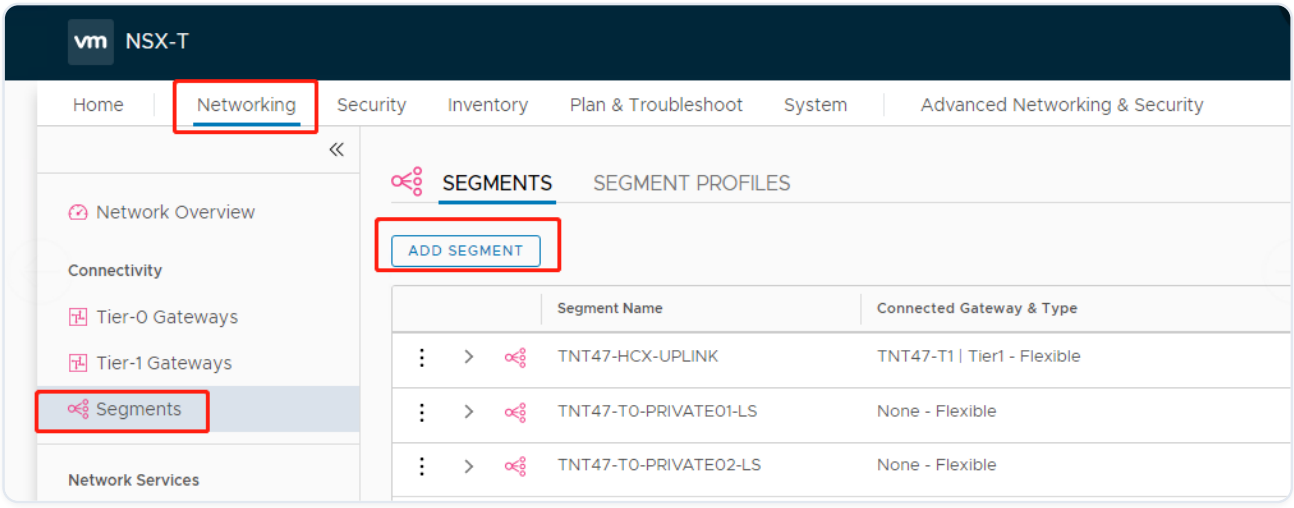
1. **「ネットワーク」>「DHCP」の順に選択し、「サーバーの追加」**を選択します。
2. **「サーバーの種類」で「DHCP」**を選択し、サーバー名とIPアドレスを入力します。
3. 「**保存**」をクリックします。
4. **「Tier 1 ゲートウェイ」を選択し、Tier-1 ゲートウェイの縦の省略記号を選択して、「編集」**を選択します。
5. サブネットを追加するには、**「IP割り当てなし」**を選択します。
6. **「種類」で「DHCPローカルサーバー」**を選択します。
7. **「DHCPサーバー」で「Default DHCP」を選択し、「保存」**をクリックします。
8. もう一度**Save**をクリックし、**Close Editing**を選択します。



AZURE VMWARE SOLUTION にネットワークセグメントを追加する

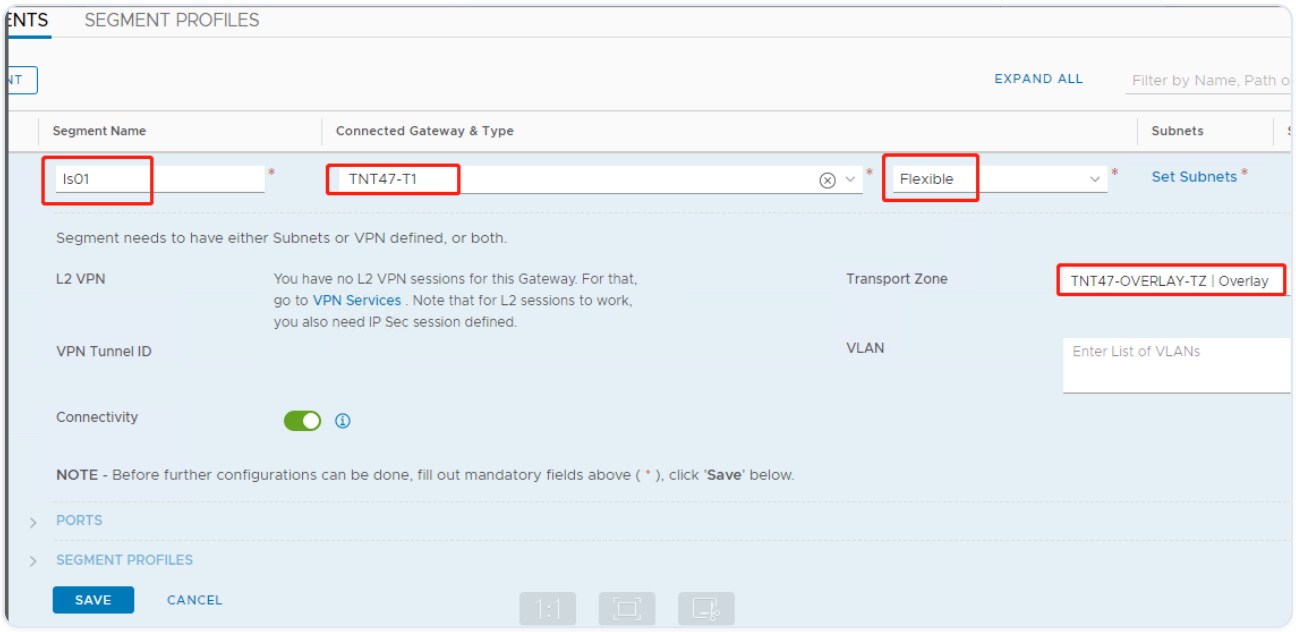
DHCPを設定した後、ネットワークセグメントを追加します。

ネットワークセグメントを追加するには、NSX-T Managerで**Networking> Segments**を選択し、**Add Segment**をクリックします。



Segments profile画面で：

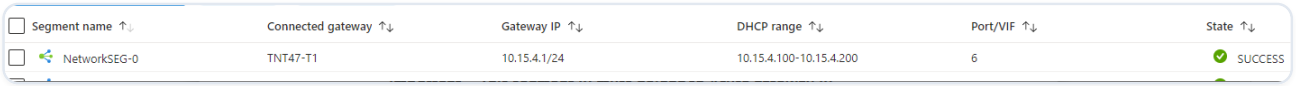
1. セグメントの**name**を入力します。
2. **Tier-1 Gateway (TNTxx-T1)**を**Connected Gateway**として選択し、**Type**は**Flexible**のままにします。
3. 事前設定されたオーバーレイ**Transport Zone(TNTxx-OVERLAY-TZ)**を選択します。
4. **Set Subnets**をクリックします。



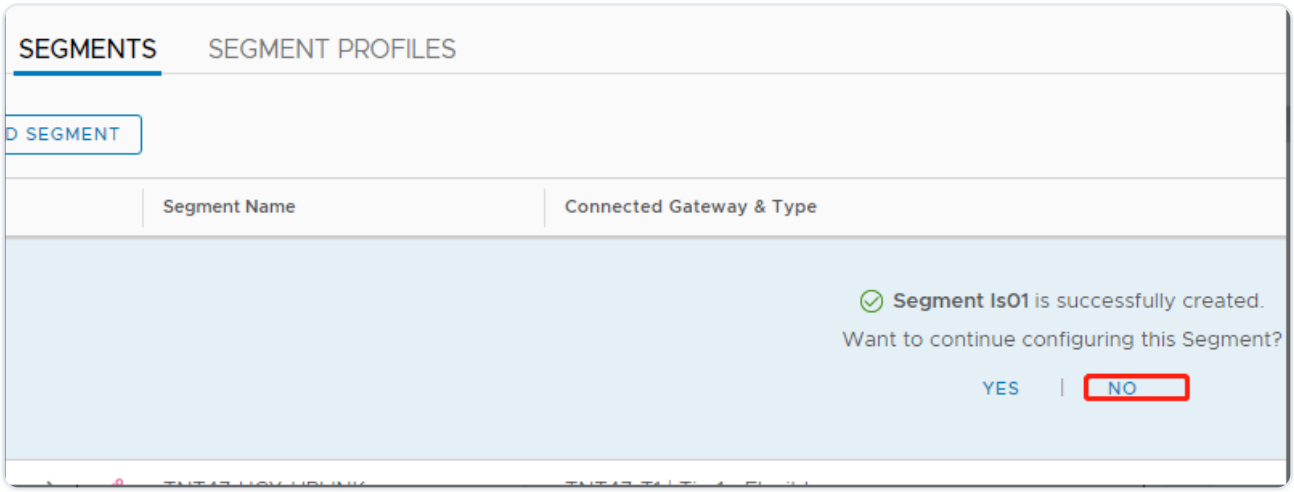
Subnetsセクションで：

1. ゲートウェイIPアドレスを入力します。
2. **Add**を選択します。

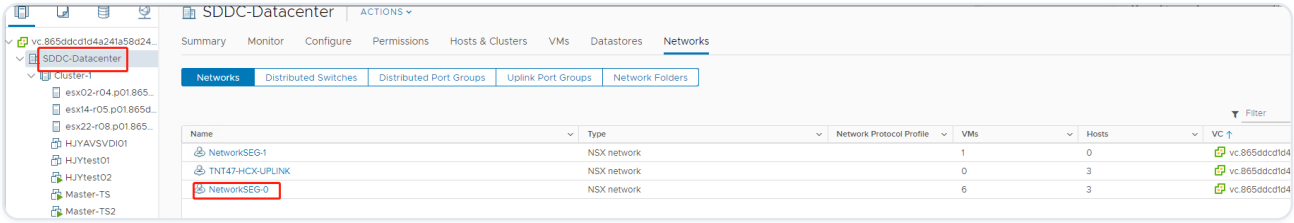
> **重要:**
>
> このセグメントのIPアドレスは、Azureゲートウェイの IPアドレス (10.15.0.0/22) に属している必要があります。
>
> DHCP範囲はセグメントIPアドレスに属している必要があります。



セグメントの構成を続行するオプションを拒否するには、 を選択します:

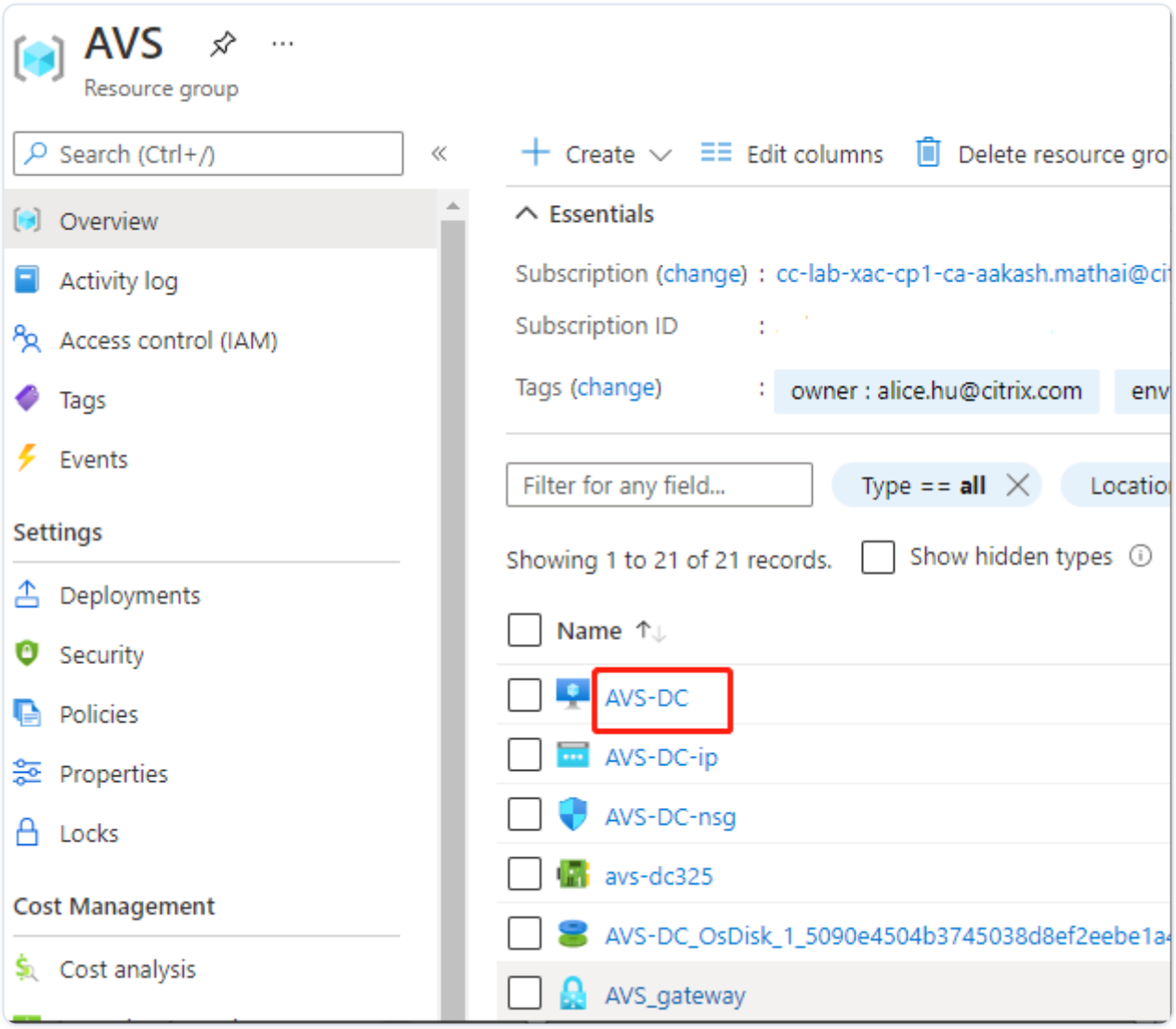


vCenterで、 > を選択します:

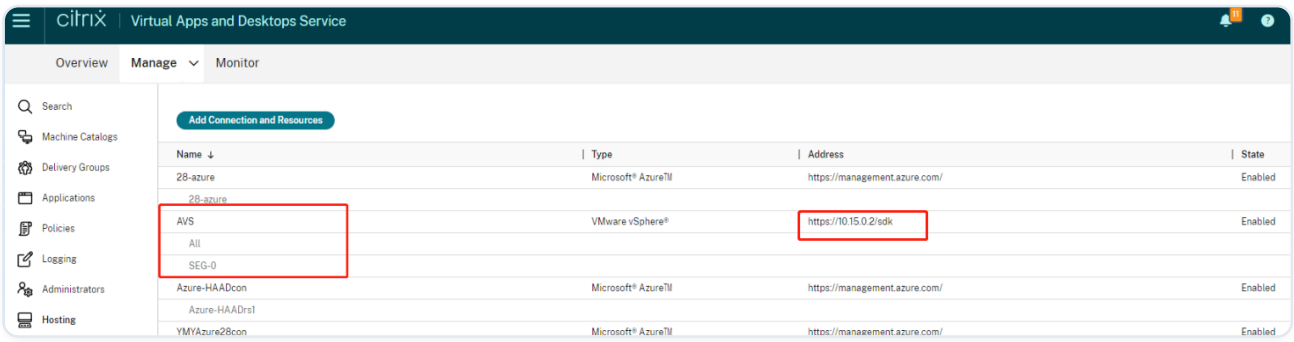


AZURE AVS環境の検証

Azureリソースグループで直接接続とコネクタを設定します。



vCenterの資格情報で接続を確認します。



グーグル クラウド ヴイエムウェア エンジン

Citrix Virtual Apps and Desktopsを使用すると、VMwareベースのオンプレミスCitrixワークロードをGoogle Cloud VMware Engineに移行できます。

グーグル クラウド VMware エンジン の構成

以下の手順では、Google Cloud VMware Engineでクラスターを取得してセットアップする方法について説明します。

VMWARE ENGINEポータルにアクセスする

1. **Google Cloud Console**で、ナビゲーションメニューをクリックします。
2. **Compute**セクションで、**VMware Engine**をクリックして、新しいブラウザータブでVMware Engineを開きます。

最初のプライベートクラウドを作成するための要件

Google Cloud VMware Engineへのアクセス、利用可能なVMware Engineノードクォータ、および適切なIAMロールが必要です。プライベートクラウドの作成を続行する前に、以下の要件を準備してください。

1. APIアクセスとノードクォータをリクエストします。詳細については、「APIアクセスとクォータのリクエスト」を参照してください。
2. VMware管理アプライアンスおよびHCX展開ネットワークに使用するアドレス範囲をメモします。詳細については、「ネットワーク要件」を参照してください。
3. VMware Engine Service Admin IAMロールを取得します。

最初のプライベートクラウドを作成する

1. VMware Engineポータルにアクセスします。
2. VMware Engineのホーム画面で、 をクリックします。ホスティング場所とハードウェアノードの種類が一覧表示されます。
3. プライベートクラウドのノード数を選択します。少なくとも3つのノードが必要です。
4. VMware管理ネットワークのクラスレスドメイン間ルーティング（CIDR）範囲を入力します。
5. HCX展開ネットワークのCIDR範囲を入力します。

> **重要:**
>
> CIDR範囲は、オンプレミスまたはクラウドのサブネットと重複してはなりません。
> CIDR範囲は/27以上である必要があります。

6. を選択します。
7. 設定を確認します。設定を変更するには、 をクリックします。
8. プライベートクラウドの作成を開始するには、 をクリックします。

VMware Engineが新しいプライベートクラウドを作成すると、いくつかのVMwareコンポーネントが展開され、プライベートクラウド内のクラスターの初期Autoscale™ポリシーが設定されます。

プライベートクラウドの作成には30分から2時間かかる場合があります。プロビジョニングが完了すると、メールが届きます。

GOOGLE CLOUD VMWARE ENGINE VPNゲートウェイをセットアップする

Google Cloud VMware Engineへの初期接続を確立するには、VPNゲートウェイを使用できます。これはOpenVPNベースのクライアントVPNであり、これを使用してVMware Software Defined Data Center (SDDC) vCenterに接続し、必要な初期構成を行うことができます。

VPNゲートウェイを展開する前に、SDDCが展開されているリージョンの**Edge Services**範囲を構成します。これを行うには：

1. **Google Cloud VMware Engine**ポータルにログオンし、 **>** に移動します。 をクリックします。
2. SDDCが展開されているリージョンを選択し、 と を有効にします。
3. 計画中にメモしたEdge Servicesの範囲を入力し、 をクリックします。これらのサービスを有効にするには10～15分かかります。

   完了すると、リージョン設定ページでEdge Servicesが**** と表示されます。これらの設定を有効にすると、SDDCにパブリックIPを割り当てることができ、これはVPNゲートウェイを展開するための要件です。

VPNゲートウェイを展開するには：

1. **Google Cloud VMware Engine**ポータルで、 **>** に移動します。 をクリックします。
2. VPNゲートウェイの名前と、計画中に予約したクライアントサブネットを指定します。**次へ**をクリックします。
3. VPNアクセスを許可するユーザーを選択します。「**次へ**」をクリックします。
4. VPN経由でアクセス可能にする必要があるネットワークを指定します。「**次へ**」をクリックします。
5. 概要画面が表示されます。選択内容を確認し、「**送信**」をクリックしてVPNゲートウェイを作成します。VPNゲートウェイページに、新しいVPNゲートウェイのステータスが「**作成中**」と表示されます。
6. ステータスが「**稼働中**」に変わったら、新しいVPNゲートウェイをクリックします。
7. 「**VPN構成をダウンロード**」をクリックして、VPNゲートウェイ用に事前設定されたOpenVPNプロファイルを含むZIPファイルをダウンロードします。UDP/1194およびTCP/443経由で接続するためのプロファイルが利用可能です。好みのプロファイルを選択してOpenVPNにインポートし、接続します。
8. 「**リソース**」に移動し、SDDCを選択します。

VPNを接続する

1. VPNゲートウェイの設定を通じて、オンプレミスネットワークとプライベートクラウド間のポイントツーサイト接続を確立します。Google Cloud VMware Engine VPNゲートウェイのセットアップを参照してください。
2. Google Cloud VMware Engine VPNゲートウェイのセットアップでダウンロードしたVPN構成をアップロードします。
3. VPNクライアント（例: OpenVPN Connect）にインポートします。

詳細については、VPNを使用した接続を参照してください。

最初のサブネットを作成する

VMware EngineポータルからNSX-T Managerにアクセスする
サブネットの作成プロセスはNSX-Tで行われ、VMware Engineを介してアクセスします。NSX-T Managerにアクセスするには、次の手順を実行します。

1. **Google Cloud VMware Engine**ポータルにログオンします。
2. メインナビゲーションから、**リソース**に移動します。
3. サブネットを作成するプライベートクラウドに対応する**プライベートクラウド名**をクリックします。
4. プライベートクラウドの詳細ページで、**vSphere Management Network**タブをクリックします。
5. NSX-T Managerに対応する**FQDN**をクリックします。
6. プロンプトが表示されたら、サインイン資格情報を入力します。vIDMを設定し、Active DirectoryなどのIDソースに接続している場合は、代わりにIDソースの資格情報を使用します。

> **注意:**
>
> 生成された資格情報は、プライベートクラウドの詳細ページから取得できます。

サブネットのDHCPサービスを設定する
サブネットを作成する前に、DHCPサービスを設定します。

NSX-T Manager で、次の手順を実行します。

1. **ネットワーキング > DHCP**に移動します。ネットワーキングダッシュボードには、DHCPサービスが1つのTier-0と1つのTier-1ゲートウェイを作成することが示されます。

2. DHCPサーバーのプロビジョニングを開始するには、**サーバーの追加**をクリックします。
3. **「サーバーの種類」で「DHCP」**を選択し、サーバー名とIPアドレスを入力します。
4. **保存**をクリックしてDHCPサービスを作成します。

このDHCPサービスを関連するTier-1ゲートウェイにアタッチするには、次の手順を実行します。デフォルトのTier-1ゲートウェイは、DHCPサービスによってすでにプロビジョニングされています。

1. **「Tier 1 ゲートウェイ」を選択し、Tier-1 ゲートウェイの縦の省略記号を選択して、「編集」**を選択します。
2. 「**IP Address Management**」フィールドで、「**No IP Allocation Set**」を選択します。
3. **「種類」で「DHCPローカルサーバー」**を選択します。
4. 「**DHCP Server**」には、作成した DHCP サーバーを選択します。
5. 「**保存**」をクリックします。
6. 「**Close Editing**」をクリックします。

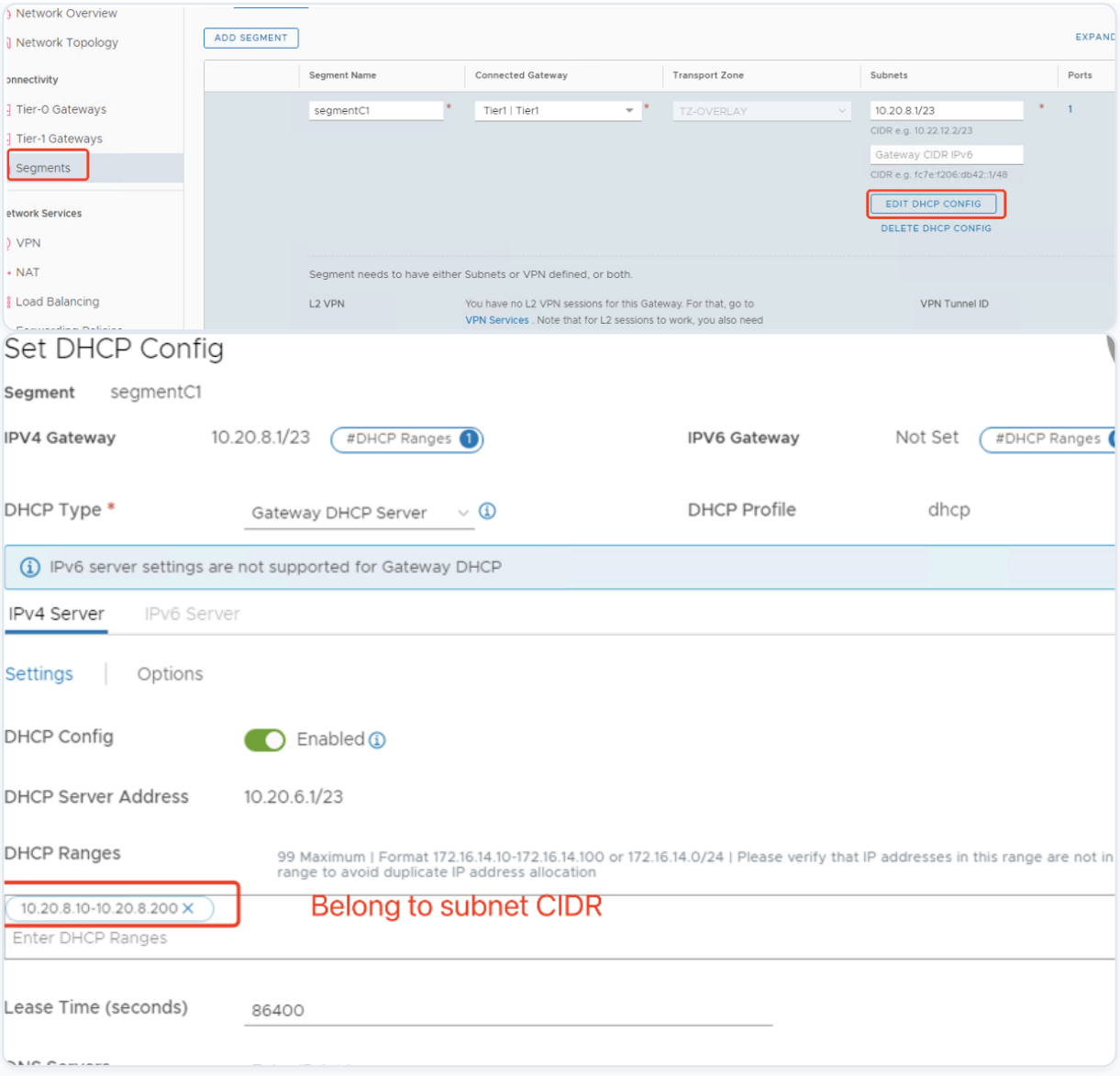
これで、NSX-T でネットワークセグメントを作成できます。NSX-T の DHCP の詳細については、DHCP に関する VMware ドキュメントを参照してください。
NSX-T でネットワークセグメントを作成する
ワークロード VM の場合、プライベートクラウドの NSX-T ネットワークセグメントとしてサブネットを作成します。

1. NSX-T Manager で、「**Networking > Segments**」に移動します。
2. 「**Add Segment**」をクリックします。
3. セグメントの名前を入力します。
4. 「**Connected Gateway**」として「**Tier-1**」を選択し、「Type」は「**Flexible**」のままにします。
5. **Set Subnets**をクリックします。
6. 「**Add Subnets**」をクリックします。
7. 「**Gateway IP/Prefix Length**」にサブネット範囲を入力します。最後のオクテットが「**.1**」となるようにサブネット範囲を指定します。例: **10.12.2.1/24**。
8. DHCP範囲を指定し、**ADD**をクリックします。
9. 「**Transport Zone**」で、ドロップダウンリストから「**TZ-OVERLAY**」を選択します。
10. **Save**をクリックします。これで、VMの作成時にvCenterでこのネットワークセグメントを選択できるようになります。

特定のリージョンでは、VMware EngineからVPC networkへのプライベートサービスアクセスを使用して、最大100個の一意のルートを設定できます。これには、たとえば、プライベートクラウド管理IPアドレス範囲、NSX-Tワークロードネットワークセグメント、HCXネットワークIPアドレス範囲が含まれます。この制限には、リージョン内のすべてのプライベートクラウドが含まれます。

注：

Google Cloudの構成の問題により、DHCP範囲設定を複数回構成する必要があります。したがって、Google Cloudの構成後にDHCP範囲設定を構成するようにしてください。DHCP範囲を構成するには、**EDIT DHCP CONFIG**をクリックします。



CITRIX STUDIOでGOOGLE CLOUD VMWARE接続を作成する

1. vCenterでマシンを作成します。
2. Citrix Studioを起動します。
3. ホスティングノードを選択し、 をクリックします。
4. 画面で、 と以下の詳細を選択します:

   「接続とリソースの追加」(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/gcp-vmware-add-connection.png)

   a. **接続タイプ**として**VMware vSphere**を選択します。
   b. **接続アドレス**に、vCenterプライベートIPアドレスを入力します。
   c. vCenterの資格情報を入力します。
   d. 接続名を入力します。
   e. 仮想マシンを作成するツールを選択します。
5. **ネットワーク**画面で、NSX-Tサーバーで作成されたサブネットを選択します。
6. ウィザードを完了します。

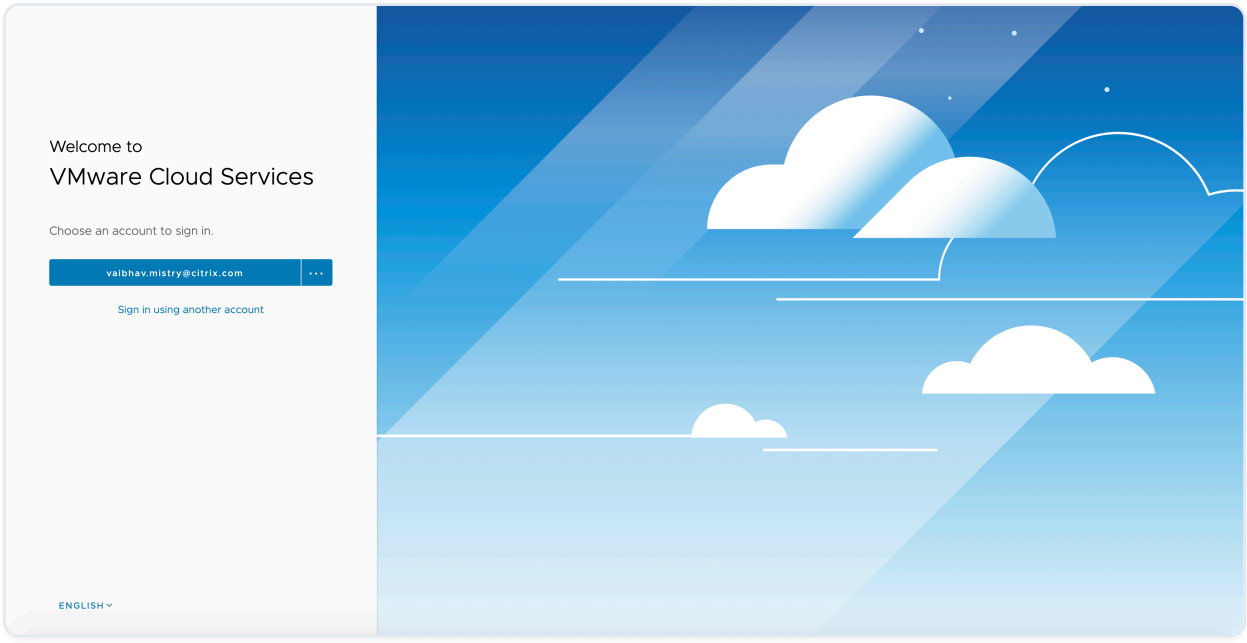
アマゾン ウェブ サービス (AWS) 上の ヴイエムウェア クラウド

Amazon Web Services (AWS) 上のVMware Cloudを使用すると、VMwareベースのオンプレミスCitrixワークロードをAWS Cloudに移行できます。

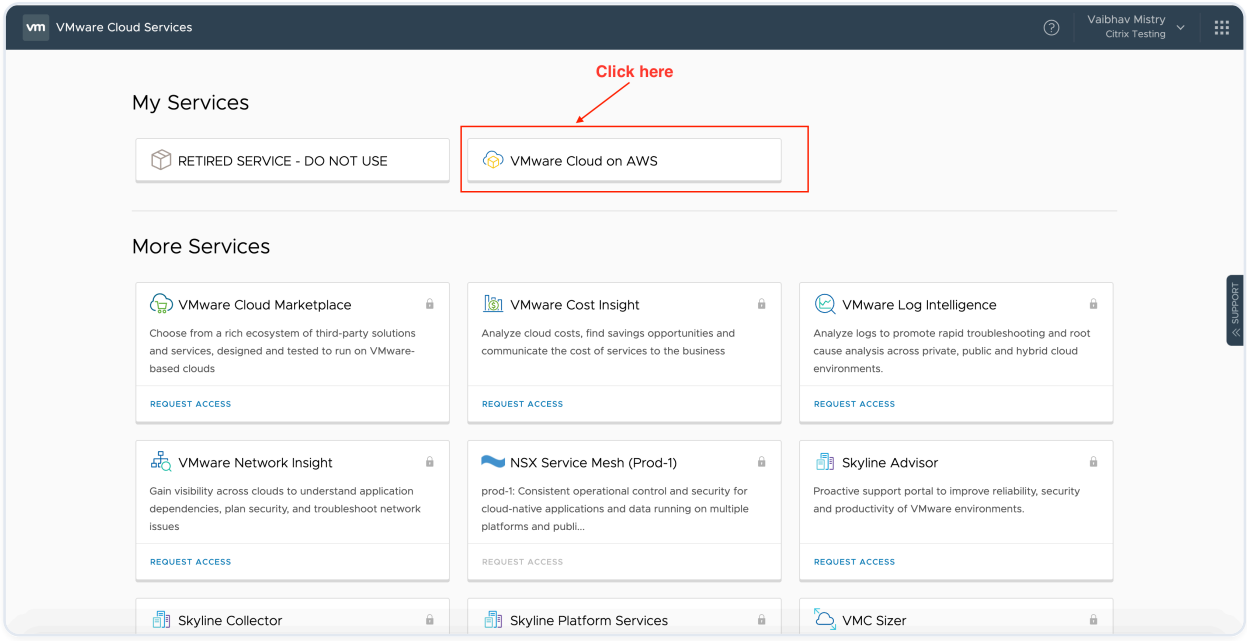
この記事では、AWS上にVMware Cloudをセットアップする手順について説明します。

VMware Cloud環境にアクセスする

1. URL `<https://console.cloud.vmware.com/>` を使用してVMware Cloudサービスにログインします。



2. 「**VMware Cloud on AWS**」をクリックします。「Software-Defined Data Centers (SDDC)」ページが表示されます。



3. 「**OPEN VCENTER**」をクリックし、次に「**SHOW CREDENTIALS**」をクリックします。後で使用するために資格情報を控えておきます。

「vCenterを開く」(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/vmc-sddc.png)

「資格情報を表示」(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/show-credentials-vmc.png)

4. Webブラウザを開き、vSphere Web ClientのURLを入力します。
5. 記載されている資格情報を入力し、**ログイン**をクリックします。vSphereクライアントのWebページは、オンプレミス環境のものと似ています。

「vSphereクライアントのWebページ」(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/vcenter-page.png)

VMwareクラウド環境について

vSphereクライアントのWebページには4つのビューがあります。

- ホストおよびクラスタービュー: 新しいクラスターを作成することはできませんが、クラウド管理者は複数のリソースプールを作成できます。

  「ホストおよびクラスタービュー」(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/host-cluster-view.png)
- VMおよびテンプレートビュー: クラウド管理者は多くのフォルダーを作成できます。

  「VMおよびテンプレートビュー」(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/vm-template-view.png)
- ストレージビュー: Citrix Studioでホスティングユニットを追加する際は、**WorkloadDatastore**ストレージを選択してください。Workload Datastoreにのみアクセスできるためです。

  「ストレージビュー」(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/storage-view.png)
- ネットワークビュー: VMwareクラウドネットワークと不透明なネットワークでは、アイコンが異なります。

  「ネットワークビュー」(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/network-view.png)

クラスターを設定した後、接続とリソースを追加するには、VMware virtualization environmentsを参照してください。

AWSクラウド環境

この記事では、Citrix Virtual Apps and Desktopsで使用できるリソースの場所としてAWSアカウントを設定する方法について説明します。このリソースの場所には、概念実証（PoC）や、複数のアベイラビリティゾーンにリソースを分散させる必要のないその他の展開に最適な、基本的なコンポーネントセットが含まれています。これらのタスクを完了すると、VDAのインストール、マシンのプロビジョニング、マシンカタログの作成、およびデリバリーグループの作成を行うことができます。

この記事のタスクを完了すると、リソースロケーションには次のコンポーネントが含まれます。

- 単一のアベイラビリティゾーン内にパブリックサブネットとプライベートサブネットを持つ仮想プライベートクラウド (VPC)。

- VPCのプライベートサブネットに配置され、Active Directoryドメインコントローラーと DNSサーバーの両方として実行されるインスタンス。
- VPCのパブリックサブネットで踏み台ホストとして機能するインスタンス。このインスタンスは、管理目的でプライベートサブネット内のインスタンスへのRDP接続を開始するために使用されます。リソースの場所の設定が完了したら、このインスタンスをシャットダウンして、容易にアクセスできないようにすることができます。VDAインスタンスなど、プライベートサブネット内の他のインスタンスを管理する必要がある場合は、踏み台ホストインスタンスを再起動できます。

制限事項

Citrix Virtual Apps and Desktops 2203 LTSR以降では、MCS AWSプラグインは `DescribeInstanceTypes` AWS APIコールを実行し、それが成功すると、MCSはAPI応答から作成されたインベントリ名を使用します。

したがって、CVAD 1912から2203以降にアップグレードする場合は、AWSで `DefineInstanceType` 権限を無効にし、その後、 `Set-ProvScheme` コマンドを使用して既存のカタログを更新し、AWSの命名スキームに合わせます。その後、カタログの更新が完了し、サービス提供がAWSの命名スキームと一致したら、 `DescribeInstanceType` 権限を再度追加します。

タスクの概要

パブリックサブネットとプライベートサブネットを持つ仮想プライベートクラウド（VPC）を設定します。このタスクを完了すると、AWSはパブリックサブネットにElastic IPアドレスを持つNATゲートウェイを展開します。このアクションにより、プライベートサブネット内のインスタンスがインターネットにアクセスできるようになります。パブリックサブネット内のインスタンスはインバウンドのパブリックトラフィックにアクセスできますが、プライベートサブネット内のインスタンスはアクセスできません。

セキュリティグループを構成します。 セキュリティグループは、VPC内のインスタンスのトラフィックを制御する仮想ファイアウォールとして機能します。パブリックサブネット内のインスタンスがプライベートサブネット内のインスタンスと通信できるようにするルールをセキュリティグループに追加します。また、これらのセキュリティグループをVPC内の各インスタンスに関連付けます。

DHCPオプションセットを作成します。Amazon VPCでは、DHCPおよびDNSサービスがデフォルトで提供されており、Active Directoryドメインコントローラーでの DNSの構成方法に影響します。AmazonのDHCPは無効にできず、AmazonのDNSはパブリックDNS解決にのみ使用でき、Active Directory名解決には使用できません。DHCPを介してインスタンスに渡されるドメインとネームサーバーを指定するには、DHCPオプションセットを作成します。このセットは、Active

Directoryドメインサフィックスを割り当て、VPC内のすべてのインスタンスのDNSサーバーを指定します。インスタンスがドメインに参加したときにホスト（A）および逆引き（PTR）レコードが自動的に登録されるようにするには、プライベートサブネットに追加する各インスタンスのネットワークアダプタープロパティを構成します。

踏み台ホストとドメインコントローラーをVPCに追加します。踏み台ホストを介して、プライベートサブネット内のインスタンスにログオンし、ドメインを設定してインスタンスをドメインに参加させることができます。

タスク1：VPCをセットアップする

1. AWSマネジメントコンソールから、**VPC**を選択します。
2. VPCダッシュボードから、**Create VPC**を選択します。
3. 「**VPC and more**」を選択します。
4. NAT ゲートウェイ ($) の下で、「**In 1 AZ**」または「**1 per AZ**」を選択します。
5. DNS オプションの下で、「**Enable DNS hostnames**」が選択されたままにします。
6. 「**Create VPC**」を選択します。AWS は、パブリックサブネットとプライベートサブネット、インターネットゲートウェイ、ルートテーブル、およびデフォルトのセキュリティグループを作成します。

タスク 2: セキュリティグループの構成

このタスクでは、VPC 用に次のセキュリティグループを作成および構成します:

- パブリックサブネット内のインスタンスに関連付けるためのパブリックセキュリティグループ。
- プライベートサブネット内のインスタンスに関連付けるためのプライベートセキュリティグループ。

セキュリティグループを作成するには:

1. VPC ダッシュボードで、「**Security Groups**」を選択します。
2. パブリックセキュリティグループ用のセキュリティグループを作成します。「**Create Security Group**」を選択し、グループの名前タグと説明を入力します。VPC で、以前に作成した VPC を選択します。「**Yes, Create**」を選択します。

パブリックセキュリティグループの構成

1. セキュリティグループのリストから、パブリックセキュリティグループを選択します。
2. **［Inbound Rules］**タブを選択し、［Edit］**を選択して、次のルールを作成します。

タイプ	送信元
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	パブリックセキュリティグループを選択します。
ICMP	0.0.0.0/0
22 (SSH)	0.0.0.0/0
80 (HTTP)	0.0.0.0/0
443 (HTTPS)	0.0.0.0/0
1494 (ICA/HDX)	0.0.0.0/0
2598 (セッションの信頼性)	0.0.0.0/0
3389 (RDP)	0.0.0.0/0

3. 完了したら、**保存**を選択します。
4. **［Outbound Rules］タブを選択し、［Edit］**を選択して、次のルールを作成します。

タイプ	宛先
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	0.0.0.0/0
ICMP	0.0.0.0/0

5. 完了したら、**保存**を選択します。

プライベートセキュリティグループを構成する

1. セキュリティグループリストから、プライベートセキュリティグループを選択します。
2. パブリックセキュリティグループからのトラフィックを設定していない場合は、TCPポートを設定する必要があります。**［Inbound Rules］タブを選択し、［Edit］**を選択して、次のルールを作成します。

タイプ	送信元
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	パブリックセキュリティグループを選択します。
ICMP	パブリックセキュリティグループを選択します。
TCP 53 (DNS)	パブリックセキュリティグループを選択します。
UDP 53 (DNS)	パブリックセキュリティグループを選択します。
80 (HTTP)	パブリックセキュリティグループを選択します。
TCP 135	パブリックセキュリティグループを選択します。
TCP 389	パブリックセキュリティグループを選択します。
UDP 389	パブリックセキュリティグループを選択します。
443 (HTTPS)	パブリックセキュリティグループを選択します。
TCP 1494 (ICA/HDX)	パブリックセキュリティグループを選択します。
TCP 2598 (セッションの信頼性)	パブリックセキュリティグループを選択します。
3389 (RDP)	パブリックセキュリティグループを選択します。
TCP 49152–65535	パブリックセキュリティグループを選択します。

3. 完了したら、**保存**を選択します。
4. **［Outbound Rules］**タブを選択し、**［Edit］**を選択して、次のルールを作成します。

タイプ	宛先
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	0.0.0.0/0
ICMP	0.0.0.0/0
UDP 53 (DNS)	0.0.0.0/0

5. 完了したら、**保存**を選択します。

タスク3：インスタンスの起動

次の手順を実行して、2つのEC2インスタンスを作成し、Amazonが生成するデフォルトの管理者パスワードを復号します。

1. AWS管理コンソールから、**EC2**を選択します。
2. EC2ダッシュボードから、**インスタンスの起動**を選択します。
3. Windows Serverマシンイメージとインスタンスタイプを選択します。
4. **［Configure Instance Details］**ページで、インスタンスの名前を入力し、以前に設定したVPCを選択します。
5. **サブネット**で、各インスタンスについて次の選択を行います。
   - Bastionホスト：パブリックサブネットを選択します
   - ドメインコントローラー：プライベートサブネットを選択します
6. **「パブリック IP アドレスの自動割り当て」**で、各インスタンスについて次の選択を行います。
   - 踏み台ホスト：**［Enable］**を選択します。
   - ドメインコントローラー：**［Use default setting］または［Disable］**を選択します。
7. **「ネットワークインターフェース」**で、ドメインコントローラーのプライベートサブネットのIP範囲内のプライマリIPアドレスを入力します。
8. 必要に応じて、**「ストレージの追加」**ページでディスクサイズを変更します。

9. 「**インスタンスのタグ付け**」ページで、各インスタンスにわかりやすい名前を入力します。
10. 「**セキュリティグループの設定**」ページで、「**既存のセキュリティグループを選択**」を選択し、各インスタンスについて次の選択を行います。
    - バスティオンホスト: パブリックセキュリティグループを選択します。
    - ドメインコントローラー: プライベートセキュリティグループを選択します。
11. 選択内容を確認し、「**起動**」を選択します。
12. 新しいキーペアを作成するか、既存のキーペアを選択します。新しいキーペアを作成する場合は、秘密鍵（.pem）ファイルをダウンロードして安全な場所に保管してください。インスタンスのデフォルトの管理者パスワードを取得する際に、秘密鍵を提供する必要があります。
13. 「**インスタンスの起動**」を選択します。「**インスタンスの表示**」を選択して、インスタンスのリストを表示します。新しく起動したインスタンスがすべてのステータスチェックに合格するまで待ってからアクセスしてください。
14. 各インスタンスのデフォルトの管理者パスワードを取得します。
    a. インスタンスリストから、インスタンスを選択し、「**接続**」を選択します。
    b. 「**RDP クライアント**」タブに移動し、「**パスワードの取得**」を選択し、プロンプトが表示されたら秘密鍵 (`.pem`) ファイルをアップロードします。
    c. 「**パスワードの復号**」を選択して、人間が読めるパスワードを取得します。AWSはデフォルトのパスワードを表示します。
15. 手順2から繰り返して、2つのインスタンスを作成します。
    - パブリックサブネットに1つの踏み台ホストインスタンス
    - ドメインコントローラーとして使用するプライベートサブネット内のインスタンスを1つ。

タスク4：DHCPオプションセットを作成する

1. VPCダッシュボードから、「**DHCPオプションセット**」を選択します。
2. 次の情報を入力します。
    - 名前タグ：セットのわかりやすい名前を入力します。
    - ドメイン名：ドメインコントローラーインスタンスを設定するときに使用する完全修飾ドメイン名を入力します。
    - ドメインネームサーバー：ドメインコントローラーインスタンスに割り当てたプライベートIPアドレスと、カンマで区切られた文字列「**AmazonProvidedDNS**」を入力します。
    - NTPサーバー：このフィールドは空白のままにします。

- NetBIOSネームサーバー：ドメインコントローラーインスタンスのプライベートIPアドレスを入力します。
- NetBIOSノードタイプ：「**2**」と入力します。

3. **はい、作成**を選択します。
4. 新しいセットをVPCに関連付けます。

   a. VPCダッシュボードから、**Your VPCs**を選択し、以前に設定したVPCを選択します。

   b. **アクション > DHCPオプションセットの編集**を選択します。

   c. プロンプトが表示されたら、作成した新しいセットを選択し、「**保存**」を選択します。

タスク5：インスタンスを構成する

1. RDPクライアントを使用して、踏み台ホストインスタンスのパブリックIPアドレスに接続します。プロンプトが表示されたら、管理者アカウントの資格情報を入力します。
2. 踏み台ホストインスタンスから、リモートデスクトップ接続を起動し、構成するインスタンスのプライベートIPアドレスに接続します。プロンプトが表示されたら、インスタンスの管理者資格情報を入力します。
3. プライベートサブネット内のすべてのインスタンスについて、DNS設定を構成します。

   a. **スタート > コントロールパネル > ネットワークとインターネット > ネットワークと共有センター > アダプターの設定の変更**を選択します。表示されているネットワーク接続をダブルクリックします。

   b. **プロパティ > インターネットプロトコルバージョン4 (TCP/IPv4) > プロパティ**を選択します。

   c. 「**詳細設定 > DNS**」を選択します。次の設定が有効になっていることを確認し、「**OK**」を選択します。

      - この接続のアドレスをDNSに登録する
      - この接続のDNSサフィックスをDNS登録で使用する

4. ドメインコントローラーを構成するには:

   a. Server Manager を使用して、Active Directory ドメインサービス の役割をすべてのデフォルト機能とともに追加します。

   b. インスタンスをドメインコントローラーに昇格させます。昇格中にDNSを有効にし、DHCPオプションセットを作成したときに指定したドメイン名を使用します。プロンプトが表示されたらインスタンスを再起動します。

接続を作成する

Studioから接続を作成する場合：

- APIキーとシークレットキーの値を指定する必要があります。これらの値を含むキーファイルをAWSからエクスポートし、インポートできます。また、リージョン、アベイラビリティゾーン、VPC名、サブネットアドレス、ドメイン名、セキュリティグループ名、および資格情報も指定する必要があります。
- ルートAWSアカウントの資格情報ファイル（AWSコンソールから取得）は、標準のAWSユーザー用にダウンロードされた資格情報ファイルと同じ形式ではありません。したがって、Citrix Virtual Apps and Desktops管理では、このファイルを使用してAPIキーとシークレットキーのフィールドに入力することはできません。AWS Identity Access Management (IAM) の資格情報ファイルを使用していることを確認してください。

> **注：**
>
> 接続を作成した後、APIキーとシークレットキーの更新が失敗する場合があります。この問題を解決するには、プロキシサーバーまたはファイアウォールの制限を確認し、次のアドレスにアクセスできることを確認してください: `https://*.amazonaws.com`。

ホスト接続のデフォルト値

AWSクラウド環境でホスト接続を作成すると、次のデフォルト値が表示されます。

オプション	絶対値	パーセンテージ
同時実行アクション（すべての種類）	125	100
1分あたりの新規アクションの最大数	125	

MCS は、デフォルトで最大 100 の同時プロビジョニング操作をサポートしています。

サービスエンドポイントURL

標準ゾーンサービスエンドポイントURL

MCSを使用すると、APIキーとAPIシークレットを持つ新しいAWS接続が追加されます。この情報と認証済みアカウントを使用して、MCSはAWS DescribeRegions EC2 API呼び出しを使用して、サポートされているゾーンをAWSに照会します。クエリは、汎用EC2サービスエンドポイント

URL `https://ec2.amazonaws.com/`を使用して行われます。MCSを使用して、サポートされているゾーンのリストから接続のゾーンを選択します。優先されるAWSサービスエンドポイントURLは、そのゾーンに対して自動的に選択されます。ただし、サービスエンドポイントURLを作成した後、そのURLを設定または変更することはできません。

AWSテナンシー

AWSは、共有テナンシー（デフォルトタイプ）と専用テナンシーという、以下のテナンシーオプションを提供します。共有テナンシーとは、異なる顧客の複数のAmazon EC2インスタンスが同じ物理ハードウェア上に存在する可能性があることを意味します。専用テナンシーとは、デプロイした他のインスタンスと同じハードウェア上でのみEC2インスタンスが実行されることを意味します。他の顧客は同じハードウェアを使用しません。

PowerShellを使用して、MCSでAWS専用ホストをプロビジョニングできます。

PowerShellを使用してAWS専用ホストのテナンシーを構成する

PowerShellを介してホストテナンシーが定義されたマシンカタログを作成できます。

Amazon 専用ホストは、インスタンス容量を持つ完全に専用の物理サーバーであり、既存のソケットごと、またはVMごとのソフトウェアライセンスを使用できます。

専用ホストには、インスタンスタイプに基づいて事前に設定された利用率があります。たとえば、C4 Largeインスタンスタイプの単一の割り当て済み専用ホストは、16インスタンスの実行に制限されています。詳細については、AWSサイトを参照してください。

AWSホストへのプロビジョニングの要件は次のとおりです。

- インポートされたBYOL（bring your own license）イメージ（AMI）。専用ホストでは、既存のライセンスを使用および管理します。
- プロビジョニング要求を満たすのに十分な利用率を持つ専用ホストの割り当て。
- **自動配置**を有効にする。

PowerShellを使用してAWSの専用ホストにプロビジョニングするには、パラメーターTenancyTypeを*Host*に設定して**New-ProvScheme**コマンドレットを使用します。

詳細については、Citrix開発者向けドキュメントを参照してください。

AWS インスタンスプロパティのキャプチャ

AWS で Machine Creation Services (MCS) を使用してマシンをプロビジョニングするためのカタログを作成するときは、そのカタログのマスター/ゴールデンイメージを表す AMI を選択します。その AMI から、MCS はディスクのスナップショットを使用します。以前のリリースでは、マシン

にロールまたはタグを付けたい場合、AWS コンソールを使用して個別に設定していました。この機能はデフォルトで有効になっています。

> **ヒント:**

> AWS インスタンスプロパティのキャプチャを使用するには、AMI に関連付けられた VM が必要です。

> このプロセスを改善するために、**MCS は** AMI が取得されたインスタンスからプロパティを読み取り、そのマシンの Identity Access Management (IAM) ロールとタグを、特定のカタログ用にプロビジョニングされたマシンに適用します。このオプション機能を使用すると、カタログ作成プロセスは選択された AMI ソースインスタンスを見つけ、限られたプロパティセットを読み取ります。これらのプロパティは AWS Launch Template に保存され、そのカタログのマシンをプロビジョニングするために使用されます。カタログ内のすべてのマシンは、キャプチャされたインスタンスプロパティを継承します。

キャプチャされるプロパティは次のとおりです。

- IAM ロール – プロビジョニングされたインスタンスに適用されます。
- タグ – プロビジョニングされたインスタンス、そのディスク、および NIC に適用されます。これらのタグは、S3 バケットとオブジェクト、ボリュームとワーカーリソース、AMI、スナップショット、起動テンプレートなど、一時的な Citrix® リソースに適用されます。

> **ヒント:**

> 一時的な Citrix リソースのタグ付けはオプションであり、カスタムプロパティ `AwsOperationalResourcesTagging` を使用して構成できます。

AWS インスタンスプロパティのキャプチャ

AWS ホスティング接続のプロビジョニングスキームを作成するときに、カスタムプロパティ `AwsCaptureInstanceProperties` を指定することで、この機能を使用できます。

`New-ProvScheme -CustomProperties “AwsCaptureInstanceProperties,true” …<standard provscheme parameters`

詳細については、Citrix Developer Documentation を参照してください。

AWS インスタンスプロパティの適用と運用リソースのタグ付け

MCS を使用して AWS でマシンをプロビジョニングするためのカタログを作成するときに、IAM ロールとタグプロパティをそれらのマシンに適用するかどうかを制御できます。また、マシンのタグを運用リソースに適用するかどうかも制御できます。

AWS 運用リソースのタグ付け

Amazon マシンイメージ (AMI) は、Amazon Cloud 環境内で仮想マシンを作成するために使用される仮想アプライアンスの一種であり、一般にEC2と呼ばれます。AMIを使用して、EC2環境を使用するサービスを展開します。AWS向けMCSを使用してマシンをプロビジョニングするカタログを作成するときは、そのカタログのゴールデンイメージとして機能する**AMI**を選択します。

> **重要:**
>
> 運用リソースのタグ付けを使用するには、インスタンスプロパティと起動テンプレートをキャプチャしてカタログを作成する必要があります。

> AWSカタログを作成するには、まずゴールデンイメージとするインスタンスのAMIを作成する必要があります。MCSはそのインスタンスからタグを読み取り、起動テンプレートに組み込みます。起動テンプレートのタグは、AWS環境で作成されたすべてのCitrixリソースに適用されます。これには以下が含まれます。

- 仮想マシン
- VMディスク
- VMネットワークインターフェイス
- S3 バケット
- S3 オブジェクト
- 起動テンプレート
- AMI

運用リソースのタグ付け

PowerShell を使用してリソースにタグを付けるには：

1. DDC ホストから PowerShell ウィンドウを開きます。
2. コマンド `asnp citrix` を実行して、Citrix固有のPowerShellモジュールをロードします。

プロビジョニングされたVMのリソースにタグを付けるには、新しいカスタムプロパティ`AwsOperationalResourcesTagging`を使用します。このプロパティの構文は次のとおりです。

```
New-ProvScheme -CustomProperties “AwsCaptureInstanceProperties,true;AwsOperationalResourcesTagging,true” …<standard provscheme parameters>
```

IAM権限の定義

このセクションの情報を使用して、AWS上のCitrix DaaSのIAM権限を定義します。AmazonのIAMサービスでは、複数のユーザーを持つアカウントが許可されており、それらのユーザーはさらにグループに編成できます。これらのユーザーは、アカウントに関連する操作を実行する能力を制御するために、異なる権限を持つことができます。IAM権限の詳細については、「IAM JSON policy reference」を参照してください。

新しいユーザーグループにIAM権限ポリシーを適用するには：

1. AWS管理コンソールにログインし、ドロップダウンリストから**IAMサービス**を選択します。
2. **新しいユーザーグループの作成**を選択します。
3. 新しいユーザーグループの名前を入力し、**続行**を選択します。
4. **Permissions**ページで、**Custom Policy**を選択します。**Select**を選択します。
5. **権限ポリシー**の名前を入力します。
6. **Policy Document**セクションで、関連する権限を入力します。

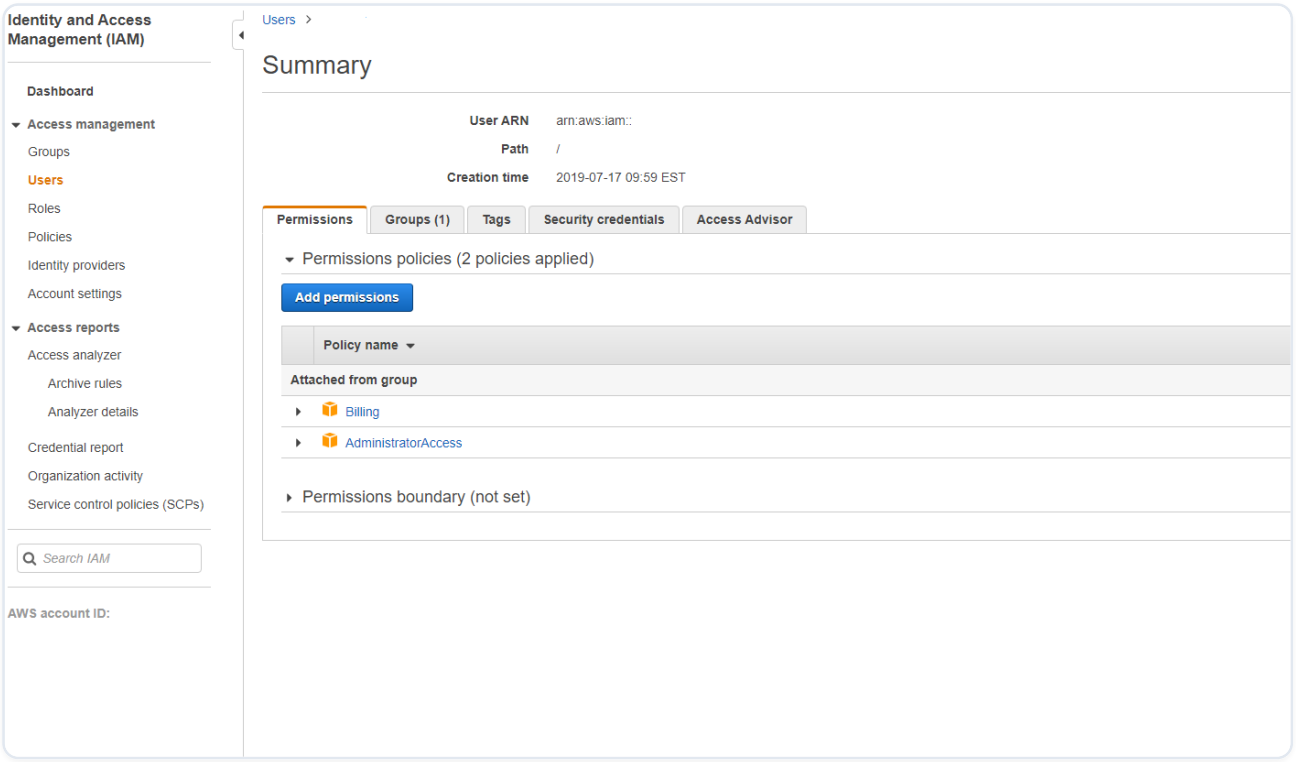
ポリシー情報を入力したら、**続行**を選択してユーザーグループを完了します。グループ内のユーザーには、Citrix DaaSに必要なアクションのみを実行する権限が付与されます。

> **重要:**
>
> 上記の例で提供されているポリシーテキストを使用して、Citrix DaaSがAWSアカウント内でアクションを実行するために使用するアクションを、特定のリソースに制限することなくリストします。Citrixは、テスト目的でこの例を使用することを推奨します。本番環境では、リソースにさらなる制限を追加することを選択できます。

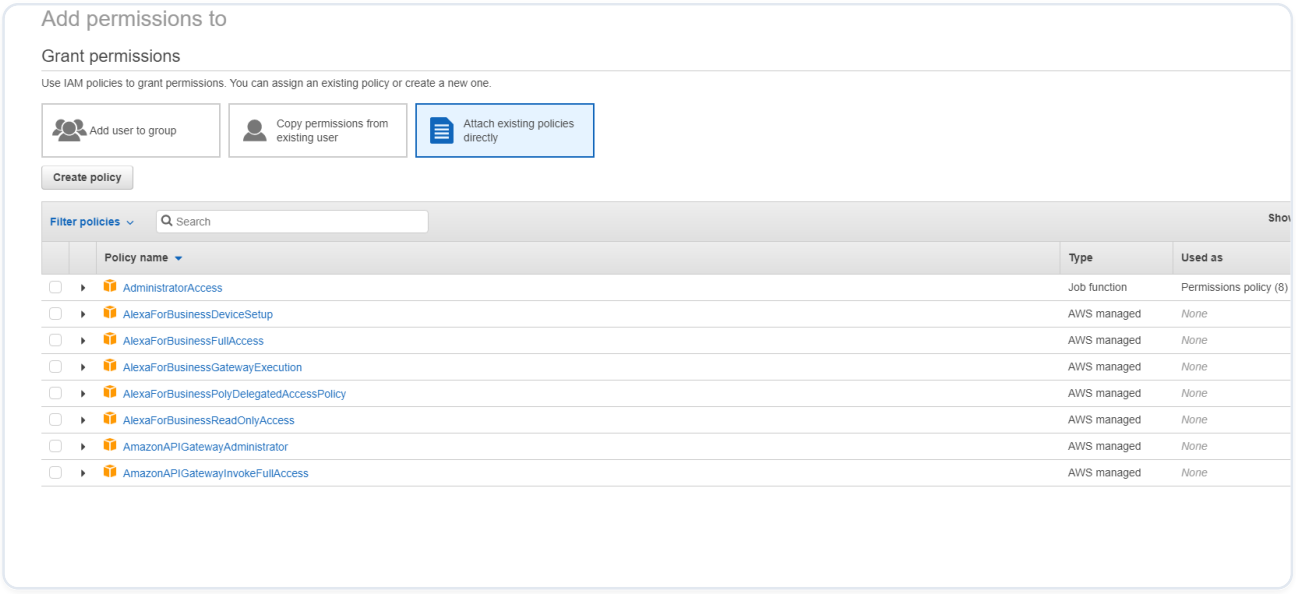
IAM権限の追加

AWSマネジメントコンソールの**IAM**セクションで権限を設定します。

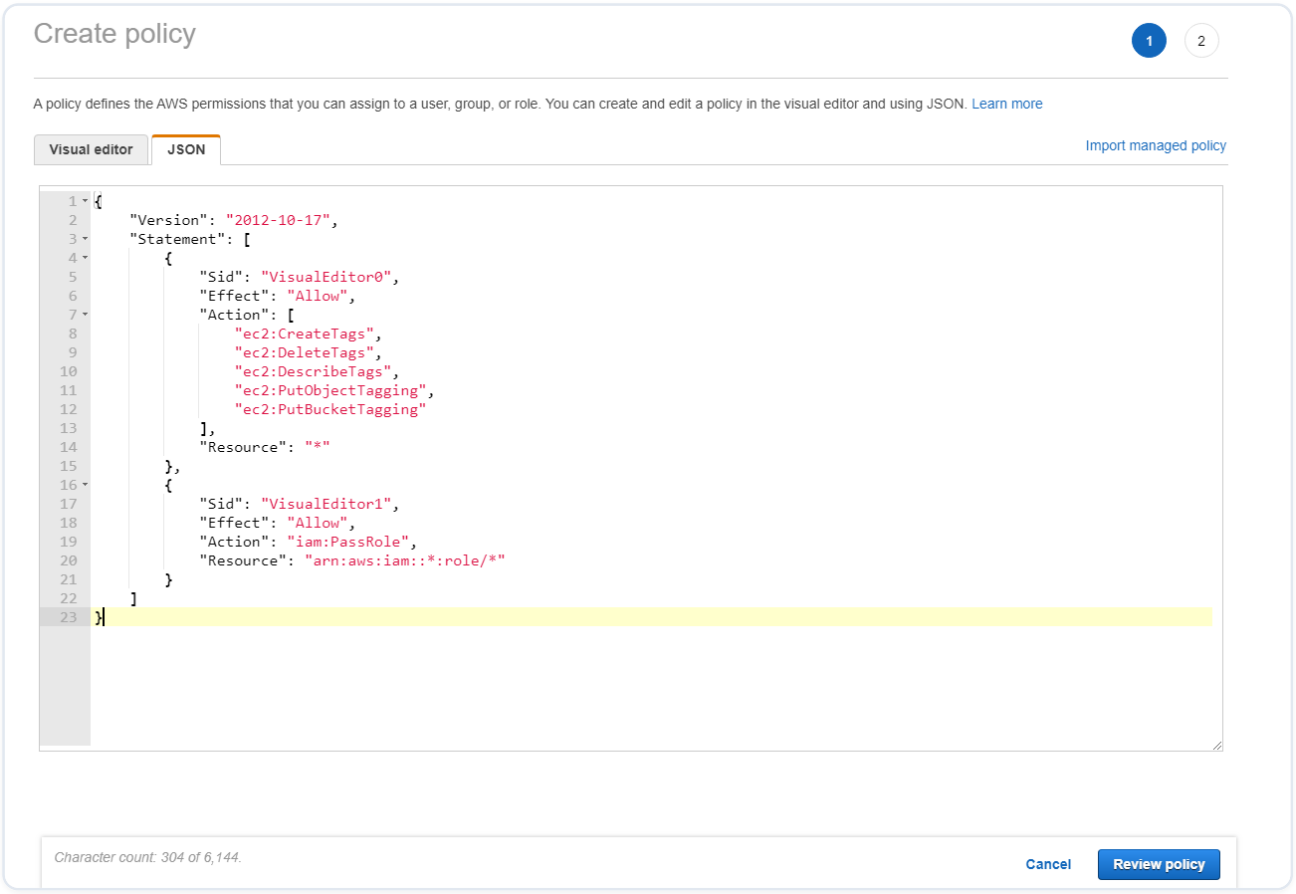
1. **概要**パネルで、**アクセス許可**タブを選択します。
2. **アクセス許可の追加**を選択します。



アクセス許可の追加先画面で、アクセス許可を付与します。



「**JSON**」タブで、以下を例として使用します。



ヒント:

記載されているJSONの例には、お使いの環境に必要なすべての権限が含まれていない場合があります。詳細については、「AWS で Citrix Virtual Apps and Desktops を実行するための ID およびアクセス管理権限を定義する方法」を参照してください。

AWS権限について

このセクションには、AWS権限の完全なリストが含まれています。

注：

iam:PassRole 権限は、**role_based_auth** の場合にのみ必要です。

ホスト接続の作成

AWSから取得した情報を使用して、新しいホスト接続が追加されます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "ec2:DescribeSnapshots",
                "ec2:DescribeLaunchTemplates"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

VM の電源管理

マシンインスタンスの電源がオンまたはオフになります。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:CreateVolume",
                "ec2:DeleteVolume",
                "ec2:DescribeInstances",
                "ec2:DescribeVolumes",
                "ec2:DetachVolume",
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

仮想マシンの作成、更新、または削除

AWSインスタンスとしてプロビジョニングされたVMを使用して、マシンカタログが作成、更新、または削除されます。

```
{

    "Version": "2012-10-17",

    "Statement": [

        {

            "Action": [

                "ec2:AttachVolume",

                "ec2:AssociateIamInstanceProfile",

                "ec2:AuthorizeSecurityGroupEgress",

                "ec2:AuthorizeSecurityGroupIngress",

                "ec2:CreateImage",

                "ec2:CreateLaunchTemplate",

                "ec2:CreateSecurityGroup",

                "ec2:CreateTags",

                "ec2:CreateVolume",

                "ec2:DeleteVolume",

                "ec2:DescribeAccountAttributes",

                "ec2:DescribeAvailabilityZones",

                “ec2:DescribeIamInstanceProfileAssociations”,

                "ec2:DescribeImages",

                "ec2:DescribeInstances",
```

```
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeLaunchTemplates",
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
```

```
            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:PutBucketAcl",
                "s3:PutBucketTagging",
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:PutObjectTagging"
            ],
```

```
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::citrix*"
        },
        {
            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

注：

> SecurityGroupsに関連するEC2セクションは、カタログ作成中に準備VM用に分離セキュリティグループを作成する必要がある場合にのみ必要です。これが完了すると、これらの権限は不要になります。

ディスクの直接アップロードとダウンロード

直接ディスクアップロードは、マシンカタログプロビジョニングにおけるボリュームワーカーの要件を排除し、代わりにAWSが提供するパブリックAPIを使用します。この機能により、追加のストレージアカウントに関連するコストと、ボリュームワーカー操作を維持する複雑さが軽減されます。

以下の権限をポリシーに追加する必要があります。

- `ebs:StartSnapshot`
- `ebs:GetSnapshotBlock`
- `ebs:PutSnapshotBlock`
- `ebs:CompleteSnapshot`
- `ebs:ListSnapshotBlocks`
- `ebs:ListChangedBlocks`
- `ec2:CreateSnapshot`
- `ec2:DeleteSnapshot`
- `ec2:DescribeLaunchTemplates`

> **重要:**
>
> - ボリュームワーカーAMIやボリュームワーカーVMなどのボリュームワーカー操作なしで、既存のマシンカタログに新しいVMを追加できます。
> - 以前にボリュームワーカーを使用していた既存のカタログを削除すると、ボリュームワーカー関連を含むすべてのアーティファクトが削除されます。

作成されたボリュームのEBS暗号化

AMIが暗号化されている場合、またはEBSがすべての新しいボリュームを暗号化するように構成されている場合、EBSは新しく作成されたボリュームを自動的に暗号化できます。ただし、この機能を実装するには、IAMポリシーに次の権限を含める必要があります。

```
{

     "Version": "2012-10-17",

     "Statement": [

        {

            "Effect": "Allow",

            "Action": [

                 "kms:CreateGrant",

                 "kms:Decrypt",

                 "kms:DescribeKey",

                 "kms:GenerateDataKeyWithoutPlainText",

                 "kms:ReEncryptTo",

                 "kms:ReEncryptFrom"

            ],

            "Resource": "*"

        }

    ]

}
```

注：

ユーザーの判断により、リソースと条件ブロックを含めることで、権限を特定のキーに限定できます。例：**条件付きKMS権限**：

```
{
     "Version": "2012-10-17",
     "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": [
                "arn:aws:kms:us-east-2:123456789012:key/abcd1234-
a123-456d-a12b-a123b4cd56ef"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
```

```
        }

    ]

}
```

次のキーポリシーステートメントは、アカウントがIAMポリシーを使用してKMSキーに対するすべてのアクション (kms:*) の権限を委任できるようにするために必要な、KMSキーのデフォルトのキーポリシー全体です。

```
{

"Sid": "Enable IAM policies",

"Effect": "Allow",

"Principal": {

"AWS": "arn:aws:iam::111122223333:root"

},

"Action": "kms:",

"Resource": ""

}
```

詳細については、「AWS Key Management Service 公式ドキュメント」を参照してください。

IAMロールベース認証

ロールベース認証をサポートするために、次の権限が追加されます。

```
{

     "Version": "2012-10-17",

     "Statement": [

        {
```

```
            "Effect": "Allow",

            "Action": "iam:PassRole",

            "Resource": "arn:aws:iam::*:role/*"

        }

    ]

}
```

最小限のIAM権限ポリシー

次のJSONは、現在サポートされているすべての機能に使用できます。このポリシーを使用すると、ホスト接続の作成、VMの作成、更新、削除、および電源管理を行うことができます。 このポリシーは、IAM権限の定義セクションで説明されているようにユーザーに適用することも、**role_based_auth**セキュリティキーとシークレットキーを使用してロールベース認証を使用することもできます。

> **重要:**
>
> **role_based_auth**を使用するには、まずクラウドコネクタのセットアップ時に、クラウドコネクタのEC2インスタンスで目的のIAMロールを構成します。Citrix Studioを使用して、ホスティング接続を追加し、認証キーとシークレットにrole_based_authを指定します。これらの設定を持つホスティング接続は、ロールベース認証を使用します。

```
{

    "Version": "2012-10-17",

    "Statement": [

        {

            "Action": [

                "ec2:AttachVolume",
```

```
                "ec2:AssociateIamInstanceProfile",

                "ec2:AuthorizeSecurityGroupEgress",

                "ec2:AuthorizeSecurityGroupIngress",

                "ec2:CreateImage",

                "ec2:CreateLaunchTemplate",

                "ec2:CreateNetworkInterface",

                "ec2:CreateTags",

                "ec2:CreateVolume",

                "ec2:DeleteLaunchTemplate",

                "ec2:DeleteNetworkInterface",

                "ec2:DeleteSecurityGroup",

                "ec2:DeleteSnapshot",

                "ec2:DeleteTags",

                "ec2:DeleteVolume",

                "ec2:DeregisterImage",

                "ec2:DescribeAccountAttributes",

                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeIamInstanceProfileAssociations",

                "ec2:DescribeImages",

                "ec2:DescribeInstances",

                "ec2:DescribeInstanceTypes",

                "ec2:DescribeLaunchTemplates",
```

```
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RebootInstances",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
```

```
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:DeleteObject",
                "s3:GetObject",
                "s3:PutBucketAcl",
                "s3:PutObject",
                "s3:PutBucketTagging",
                "s3:PutObjectTagging"
            ],
            "Effect": "Allow",
```

```
            "Resource": "arn:aws:s3:::citrix*"
        },
        {
            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
```

```
                "kms:ReEncryptTo",

                "kms:ReEncryptFrom"

            ],

            "Resource": "*"

        },

        {

            "Effect": "Allow",

            "Action": "iam:PassRole",

            "Resource": "arn:aws:iam::*:role/*"

        }

    ]

}
```

注：

- SecurityGroupsに関連するEC2セクションは、カタログ作成中に準備VM用に分離セキュリティグループを作成する必要がある場合にのみ必要です。これが完了すると、これらの権限は不要になります。
- KMSセクションは、EBSボリューム暗号化を使用する場合にのみ必要です。
- iam:PassRole 権限セクションは、**role_based_auth** の場合にのみ必要です。
- 要件と環境に基づいて、フルアクセスではなく特定のリソースレベルの権限を追加できます。詳細については、AWSドキュメントのDemystifying EC2 Resource-Level Permissions および Access management for AWS resources を参照してください。

詳細情報

- 接続とリソース

- マシンカタログの作成

Google Cloud環境

Citrix Virtual Apps and Desktops™では、Google Cloudでマシンをプロビジョニングおよび管理できます。この記事では、Machine Creation Services（MCS）を使用して、Citrix Virtual AppsまたはCitrix Virtual Desktopsサービス展開で仮想マシンをプロビジョニングする方法について説明します。

要件

- Citrix Cloud™アカウント。この記事で説明されている機能は、Citrix Cloudでのみ利用可能です。
- Citrix DaaSサブスクリプション。詳細については、「Get started」を参照してください。
- Google Cloudプロジェクト。このプロジェクトには、マシンカタログに関連付けられているすべてのコンピューティングリソースが保存されます。既存のプロジェクトでも新規のプロジェクトでもかまいません。
- Google Cloudプロジェクトで4つのAPIを有効にします。詳細については、「Enable Google Cloud APIs」を参照してください。
- Google Cloudサービスアカウント。サービスアカウントはGoogle Cloudに認証し、プロジェクトへのアクセスを有効にします。詳細については、「Configure the Google Cloud service account」を参照してください。
- Googleプライベートアクセスを有効にします。詳細については、「Enable-private-google-access」を参照してください。

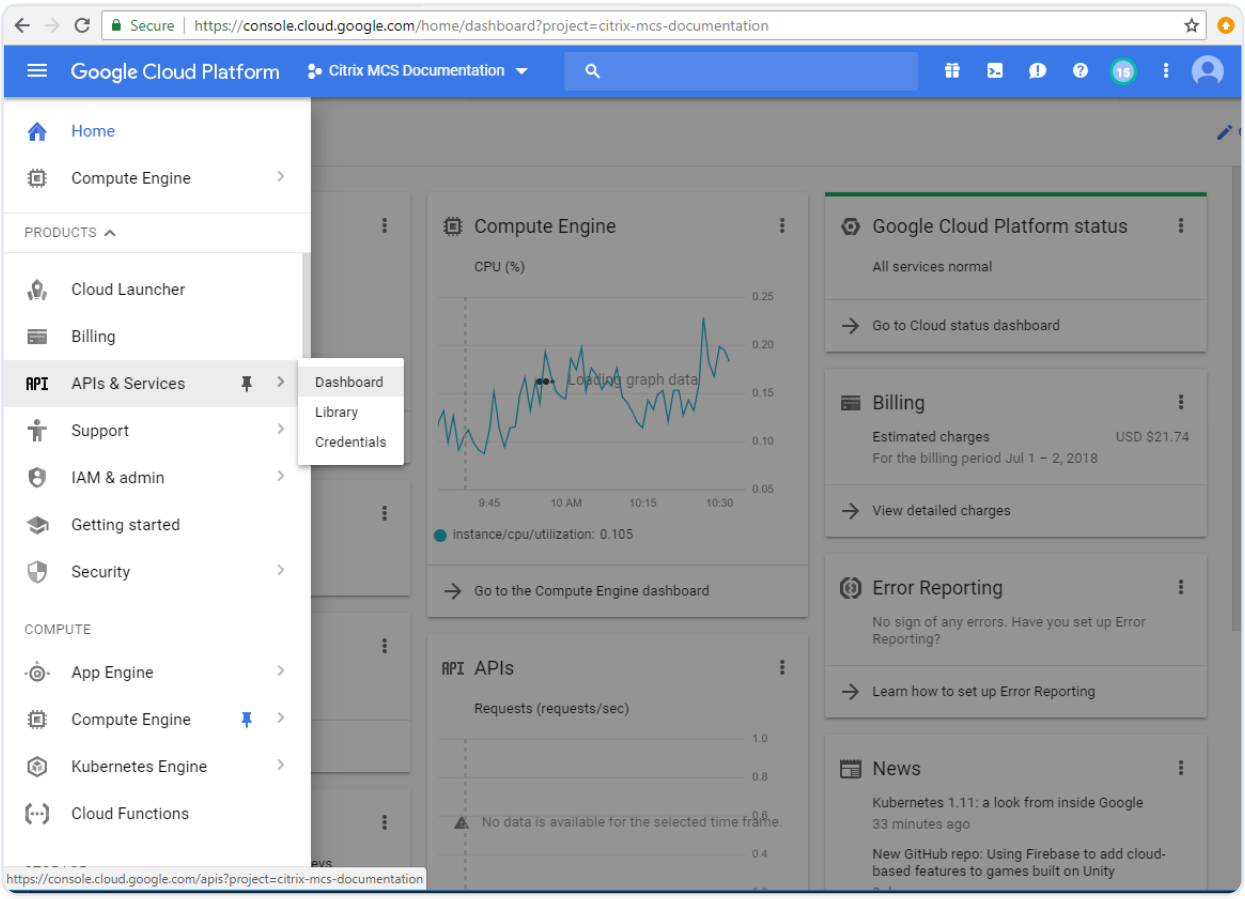
Google Cloud APIを有効にする

Web Studioを介してGoogle Cloudの機能を使用するには、Google Cloudプロジェクトで次のAPIを有効にします。

- コンピュート エンジン API
- クラウド リソース マネージャー API
- ID およびアクセス管理 (IAM) API
- クラウド ビルド API

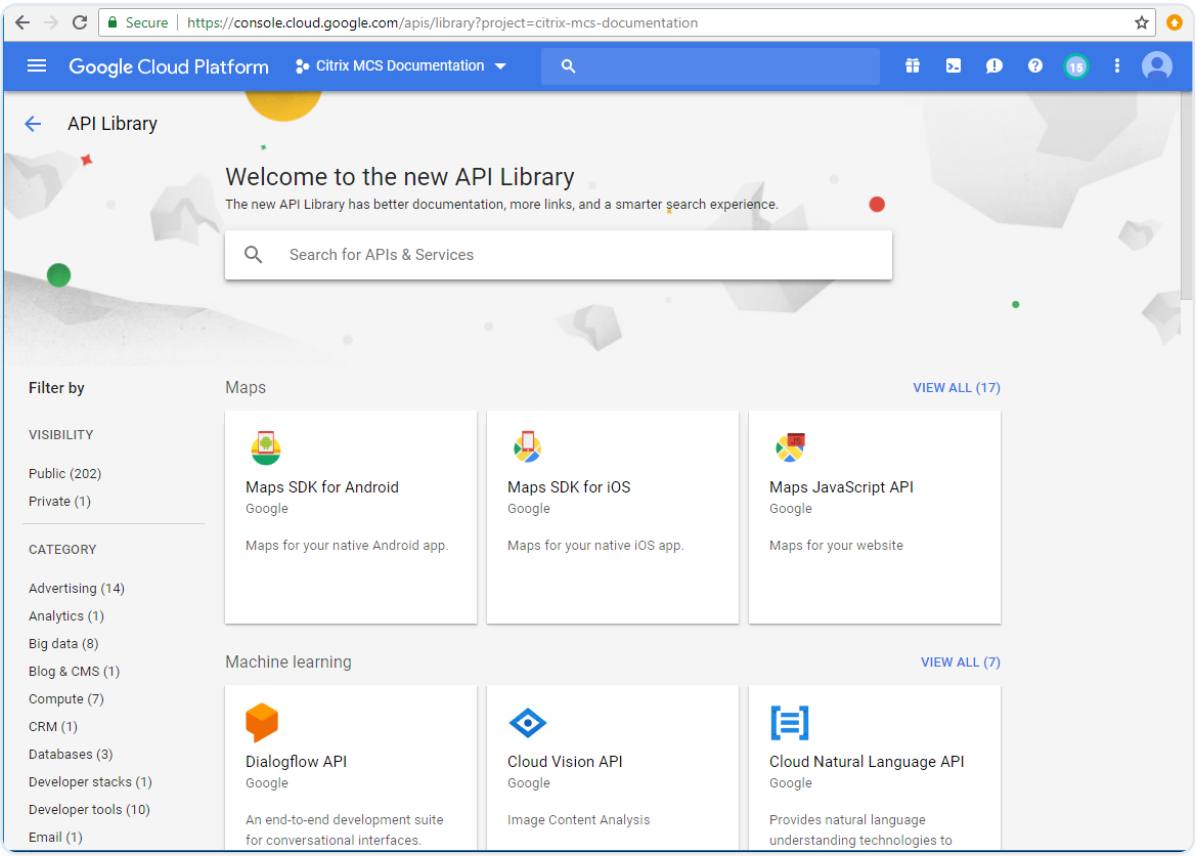
Google Cloudコンソールから、次の手順を実行します。

1. 左上のメニューで、**「APIとサービス」>「ダッシュボード」**を選択します。



2. **ダッシュボード**画面で、Compute Engine APIが有効になっていることを確認します。 有効になっていない場合は、次の手順に従ってください。

   a. 「**APIとサービス > ライブラリ**」に移動します。



b. 検索ボックスに「*Compute Engine*」と入力します。

c. 検索結果から「**Compute Engine API**」を選択します。

d. 「**Compute Engine API**」ページで、「**有効にする**」を選択します。

3. Cloud Resource Manager APIを有効にします。

a. 「**APIとサービス > ライブラリ**」に移動します。

b. 検索ボックスに「*Cloud Resource Manager*」と入力します。

c. 検索結果から「**Cloud Resource Manager API**」を選択します。

d. 「**Cloud Resource Manager API**」ページで、「**有効にする**」を選択します。APIのステータスが表示されます。

4. 同様に、**Identity and Access Management (IAM) API**と**Cloud Build API**を有効にします。

Google Cloud Shellを使用してAPIを有効にすることもできます。これを行うには：

1. Googleコンソールを開き、Cloud Shellをロードします。
2. Cloud Shellで次の4つのコマンドを実行します。

- gcloud services enable compute.googleapis.com を有効にします。
- gcloud services enable cloudresourcemanager.googleapis.com を有効にします。

- gcloud services enable iam.googleapis.com を有効にします。
- gcloud services enable cloudbuild.googleapis.com を有効にします。

3. Cloud Shellがプロンプトを表示した場合、「**承認**」をクリックします。

サービスアカウントの構成と更新

> **注：**
>
> CP は、Cloud Build Service のデフォルトの動作とサービスアカウントの使用に関して、April 29, 2024 以降に変更を導入します。詳細については、「Cloud Build Service Account Change」(https://cloud.google.com/build/docs/cloud-build-service-account-updates) を参照してください。April 29, 2024 より前に Cloud Build API が有効になっている既存の Google プロジェクトは、この変更の影響を受けません。ただし、April 29 以降も既存の Cloud Build Service の動作を維持したい場合は、Cloud Build API を有効にする前に、制約の適用を無効にする組織ポリシーを作成または適用できます。その結果、以下のコンテンツは「Before April 29, 2024」(#before-april-29-2024) と「After April 29, 2024」(#after-april-29-2024) の2つに分かれています。新しい組織ポリシーを設定した場合は、「Before April 29, 2024」(#before-april-29-2024) のセクションに従ってください。

April 29, 2024より前

Citrix Cloudは、Google Cloudプロジェクト内で3つの個別のサービスアカウントを使用します。

- *Citrix Cloudサービスアカウント*: このサービスアカウントにより、Citrix CloudはGoogleプロジェクトにアクセスし、マシンをプロビジョニングおよび管理できます。このサービスアカウントは、Google Cloudによって生成されたキーを使用してGoogle Cloudに認証します。

  ここに概説されているように、このサービスアカウントを手動で作成する必要があります。詳細については、Citrix Cloudサービスアカウントの作成を参照してください。

  このサービスアカウントは、メールアドレスで識別できます。例: `<my-service-account>@<project-id>.iam.gserviceaccount.com`。
- *Cloud Buildサービスアカウント*: このサービスアカウントは、Google Cloud APIの有効化で言及されているすべてのAPIを有効にすると自動的にプロビジョニングされます。自動的に作成されたすべてのサービスアカウントを表示するには、**Google Cloud**コンソールで**IAMと管理 > IAM**に移動し、**Googleが提供するロールの付与を含める**チェックボックスをオンにします。

このサービスアカウントは、**プロジェクトID**と**cloudbuild**という単語で始まるメールアドレスで識別できます。例: `<project-id>@cloudbuild.gserviceaccount.com`

サービスアカウントに以下のロールが付与されていることを確認します。ロールを追加する必要がある場合は、Cloud Build サービスアカウントにロールを追加するに記載されている手順に従ってください。

- Cloud Build サービスアカウント
- Compute Instance 管理者
- サービスアカウントユーザー

- *Cloud Compute サービスアカウント*: このサービスアカウントは、Compute API がアクティブ化されると、Google Cloud によって Google Cloud で作成されたインスタンスに追加されます。このアカウントには、操作を実行するための IAM 基本編集者ロールがあります。ただし、よりきめ細かな制御を行うためにデフォルトの権限を削除した場合は、次の権限を必要とする **Storage Admin** ロールを追加する必要があります。
  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

このサービスアカウントは、**プロジェクト ID** と **compute** という単語で始まるメールアドレスで識別できます。例: `<project-id>-compute@developer.gserviceaccount.com`。

CITRIX CLOUD サービスアカウントを作成する

Citrix Cloud サービスアカウントを作成するには、次の手順に従います。

1. Google Cloud コンソールで、**IAM と管理 > サービスアカウント**に移動します。
2. **サービスアカウント**ページで、**サービスアカウントを作成**を選択します。
3. **サービスアカウントの作成**ページで、必要な情報を入力し、**作成して続行**を選択します。
4. 「**このサービスアカウントにプロジェクトへのアクセスを許可する**」ページで、「**ロールを選択**」ドロップダウンメニューをクリックし、必要なロールを選択します。さらにロールを追加する場合は、「**+別のロールを追加**」をクリックします。

   各アカウント（個人またはサービス）には、プロジェクトの管理を定義するさまざまなロールがあります。このサービスアカウントには、以下のロールを付与してください。

   - Compute 管理者

- Storage管理者
- Cloud Build編集者
- サービスアカウントユーザー
- クラウド データストア ユーザー
- Cloud KMS 暗号オペレーター

Cloud KMS 暗号オペレーターには、以下の権限が必要です。

- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.get
- cloudkms.keyRings.list

> **注：**
>
> 新しいサービスアカウントを作成する際に利用可能なロールの完全なリストを取得するには、すべてのAPIを有効にしてください。

5. **CONTINUE**をクリックします。
6. **このサービスアカウントへのユーザーアクセスを許可**ページで、このサービスアカウントでアクションを実行するアクセス権を付与するために、ユーザーまたはグループを追加します。
7. **DONE**をクリックします。
8. IAMメインコンソールに移動します。
9. 作成されたサービスアカウントを特定します。
10. ロールが正常に割り当てられていることを検証します。

考慮事項:

サービスアカウントを作成する際は、以下を考慮してください。

- **このサービスアカウントにプロジェクトへのアクセスを許可**および**このサービスアカウントへのユーザーアクセスを許可**の手順はオプションです。これらのオプションの構成手順をスキップすることを選択した場合、新しく作成されたサービスアカウントは、**IAMと管理 > IAM**ページに表示されません。

- サービスアカウントに関連付けられたロールを表示するには、オプションの手順をスキップせずにロールを追加します。このプロセスにより、構成されたサービスアカウントにロールが表示されるようになります。

CITRIX CLOUDサービスアカウントキー

Citrix DaaSで接続を作成するには、Citrix Cloudサービスアカウントキーが必要です。キーは資格情報ファイル（.json）に含まれています。キーを作成すると、ファイルは自動的にダウンロードされ、**ダウンロード**フォルダーに保存されます。キーを作成するときは、キーの種類をJSONに設定してください。そうしないと、Web Studioはそれを解析できません。

サービスアカウントキーを作成するには、**IAMと管理 > サービスアカウント**に移動し、Citrix Cloudサービスアカウントのメールアドレスをクリックします。**キー**タブに切り替え、**キーを追加 > 新しいキーを作成**を選択します。キータイプとして**JSON**を選択していることを確認してください。

> **ヒント:**
>
> Google Cloud コンソールで、**サービスアカウント**ページを使用してキーを作成します。セキュリティ上の理由から、キーを定期的に変更することをお勧めします。既存の Google Cloud 接続を編集することで、Citrix Virtual Apps and Desktops アプリケーションに新しいキーを提供できます。

CITRIX CLOUD サービスアカウントにロールを追加する

Citrix Cloud サービスアカウントにロールを追加するには、次の手順を実行します。

1. Google Cloud コンソールで、**IAM と管理 > IAM** に移動します。
2. **IAM > 権限**ページで、作成したサービスアカウントを電子メールアドレスで特定し、見つけます。

   例: `<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. 鉛筆アイコンを選択して、サービスアカウントのプリンシパルへのアクセスを編集します。
4. 選択したプリンシパルオプションの**「project-id」へのアクセスを編集**ページで、**別のロールを追加**を選択して、必要なロールをサービスアカウントに1つずつ追加し、**保存**を選択します。

CLOUD BUILD サービスアカウントにロールを追加する

Cloud Build サービスアカウントにロールを追加するには、次の手順を実行します。

1. Google Cloud コンソールで、**IAM と管理 > IAM** に移動します。
2. **IAM**ページで、**プロジェクト ID**と**cloudbuild**という単語で始まる電子メールアドレスで識別できる Cloud Build サービスアカウントを見つけます。

   例: `<project-id>@cloudbuild.gserviceaccount.com`
3. 鉛筆アイコンを選択して、Cloud Build アカウントのロールを編集します。
4. 選択したプリンシパルオプションの**「"project-id"へのアクセスを編集」ページで、「別のロールを追加」を選択して、必要なロールをCloud Buildサービスアカウントに1つずつ追加し、「保存」**を選択します。

> **注：**
>
> すべてのAPIを有効にして、ロールの完全なリストを取得します。

April 29, 2024 以降

Citrix Cloudは、Google Cloudプロジェクト内で2つの異なるサービスアカウントを使用します。

- *Citrix Cloudサービスアカウント*: このサービスアカウントにより、Citrix CloudはGoogleプロジェクトにアクセスし、マシンをプロビジョニングおよび管理できます。このサービスアカウントは、Google Cloudによって生成されたキーを使用してGoogle Cloudに認証します。

  このサービスアカウントは手動で作成する必要があります。

  このサービスアカウントは、メールアドレスで識別できます。例: `<my-service-account>@<project-id>.iam.gserviceaccount.com`。
- *Cloud Computeサービスアカウント*：このサービスアカウントは、Google Cloud APIを有効にするで言及されているすべてのAPIを有効にした後に自動的にプロビジョニングされます。自動的に作成されたすべてのサービスアカウントを表示するには、**Google Cloud**コンソールで**「IAMと管理」>「IAM」に移動し、「Google提供のロール付与を含める」チェックボックスを選択します。このアカウントには、操作を実行するためのIAM基本編集者ロールがあります。ただし、より詳細な制御を行うためにデフォルトの権限を削除した場合、次の権限を必要とする**Storage Admin**ロールを追加する必要があります。
  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

このサービスアカウントは、**プロジェクトID**と**compute**という単語で始まるメールアドレスで識別できます。例：`<project-id>-compute@developer.gserviceaccount.com.`.

サービスアカウントに次のロールが付与されていることを確認します。

- Cloud Build サービスアカウント
- Compute Instance 管理者
- サービスアカウントユーザー

CITRIX CLOUD サービスアカウントを作成する

Citrix Cloud サービスアカウントを作成するには、次の手順に従います。

1. Google Cloud コンソールで、**IAM と管理 > サービスアカウント**に移動します。
2. **サービスアカウント**ページで、**サービスアカウントを作成**を選択します。
3. **サービスアカウントの作成**ページで、必要な情報を入力し、**作成して続行**を選択します。
4. 「**このサービスアカウントにプロジェクトへのアクセスを許可する**」ページで、「**ロールを選択**」ドロップダウンメニューをクリックし、必要なロールを選択します。さらにロールを追加する場合は、「**+別のロールを追加**」をクリックします。

   各アカウント（個人またはサービス）には、プロジェクトの管理を定義するさまざまなロールがあります。このサービスアカウントには、以下のロールを付与してください。

   - Compute 管理者
   - Storage管理者
   - Cloud Build編集者
   - サービスアカウントユーザー
   - クラウド データストア ユーザー
   - Cloud KMS 暗号オペレーター

   Cloud KMS 暗号オペレーターには、以下の権限が必要です。

   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.get
   - cloudkms.keyRings.list

> **注：**

> 新しいサービスアカウントを作成する際に利用可能なロールの完全なリストを取得するには、すべてのAPIを有効にしてください。

5. **CONTINUE**をクリックします。
6. **このサービスアカウントへのユーザーアクセスを許可**ページで、このサービスアカウントでアクションを実行するアクセス権を付与するために、ユーザーまたはグループを追加します。
7. **DONE**をクリックします。
8. IAMメインコンソールに移動します。
9. 作成されたサービスアカウントを特定します。
10. ロールが正常に割り当てられていることを検証します。

考慮事項:

サービスアカウントを作成する際は、以下を考慮してください。

- **このサービスアカウントにプロジェクトへのアクセスを許可**および**このサービスアカウントへのユーザーアクセスを許可**の手順はオプションです。これらのオプションの構成手順をスキップすることを選択した場合、新しく作成されたサービスアカウントは、**IAMと管理 > IAM**ページに表示されません。
- サービスアカウントに関連付けられたロールを表示するには、オプションの手順をスキップせずにロールを追加します。このプロセスにより、構成されたサービスアカウントにロールが表示されるようになります。

CITRIX CLOUDサービスアカウントキー

Citrix DaaSで接続を作成するには、Citrix Cloudサービスアカウントキーが必要です。キーは資格情報ファイル（.json）に含まれています。キーを作成すると、ファイルは自動的にダウンロードされ、**ダウンロード**フォルダーに保存されます。キーを作成するときは、キーの種類をJSONに設定してください。そうしないと、Web Studioはそれを解析できません。

サービスアカウントキーを作成するには、**IAMと管理 > サービスアカウント**に移動し、Citrix Cloudサービスアカウントのメールアドレスをクリックします。**キー**タブに切り替え、**キーを追加 > 新しいキーを作成**を選択します。キータイプとして**JSON**を選択していることを確認してください。

> **ヒント:**

> Google Cloud コンソールで、**サービスアカウント**ページを使用してキーを作成します。セキュリティ上の理由から、キーを定期的に変更することをお勧めします。既存の Google Cloud 接続を編集することで、Citrix Virtual Apps and Desktops アプリケーションに新しいキーを提供できます。

CITRIX CLOUD サービスアカウントにロールを追加する

Citrix Cloud サービスアカウントにロールを追加するには、次の手順を実行します。

1. Google Cloud コンソールで、**IAM と管理 > IAM** に移動します。
2. **IAM > 権限**ページで、作成したサービスアカウントを電子メールアドレスで特定し、見つけます。

   例: `<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. 鉛筆アイコンを選択して、サービスアカウントのプリンシパルへのアクセスを編集します。
4. 選択したプリンシパルオプションの**「project-id」へのアクセスを編集**ページで、**別のロールを追加**を選択して、必要なロールをサービスアカウントに1つずつ追加し、**保存**を選択します。

CLOUD COMPUTE SERVICE ACCOUNT にロールを追加する

Cloud Compute Service Account にロールを追加するには、次の手順を実行します。

1. Google Cloud コンソールで、**IAM と管理 > IAM** に移動します。
2. **IAM** ページで、**プロジェクト ID** と **compute** という単語で始まるメールアドレスで識別できる Cloud Compute Service Account を見つけます。

   例: `<project-id>-compute@developer.gserviceaccount.com`
3. 鉛筆アイコンを選択して、Cloud Build アカウントのロールを編集します。
4. 選択したプリンシパルオプションの**「"project-id"へのアクセスを編集」ページで、「別のロールを追加」を選択して、必要なロールをCloud Buildサービスアカウントに1つずつ追加し、「保存」**を選択します。

> **注：**
>
> すべてのAPIを有効にして、ロールの完全なリストを取得します。

ストレージの権限とバケット管理

Citrix DaaS は、Google Cloud サービス のクラウドビルド障害の報告プロセスを改善します。このサービスは Google Cloud でビルドを実行します。Citrix DaaS は、Google Cloud サービスがビルドログ情報をキャプチャする `citrix-mcs-cloud-build-logs-{region}-{5 random characters}` という名前のストレージバケットを作成します。このバケットには、30 日後にコンテンツを削除するオプションが設定されています。このプロセスでは、接続に使用されるサービスアカウントに Google Cloud の権限が `storage.buckets.update` に設定されている必要があります。サービスアカウントにこの権限がない場合、Citrix DaaS はエラーを無視し、カタログ作成プロセスを続行します。この権限がないと、ビルドログのサイズが増加し、手動でのクリーンアップが必要になります。

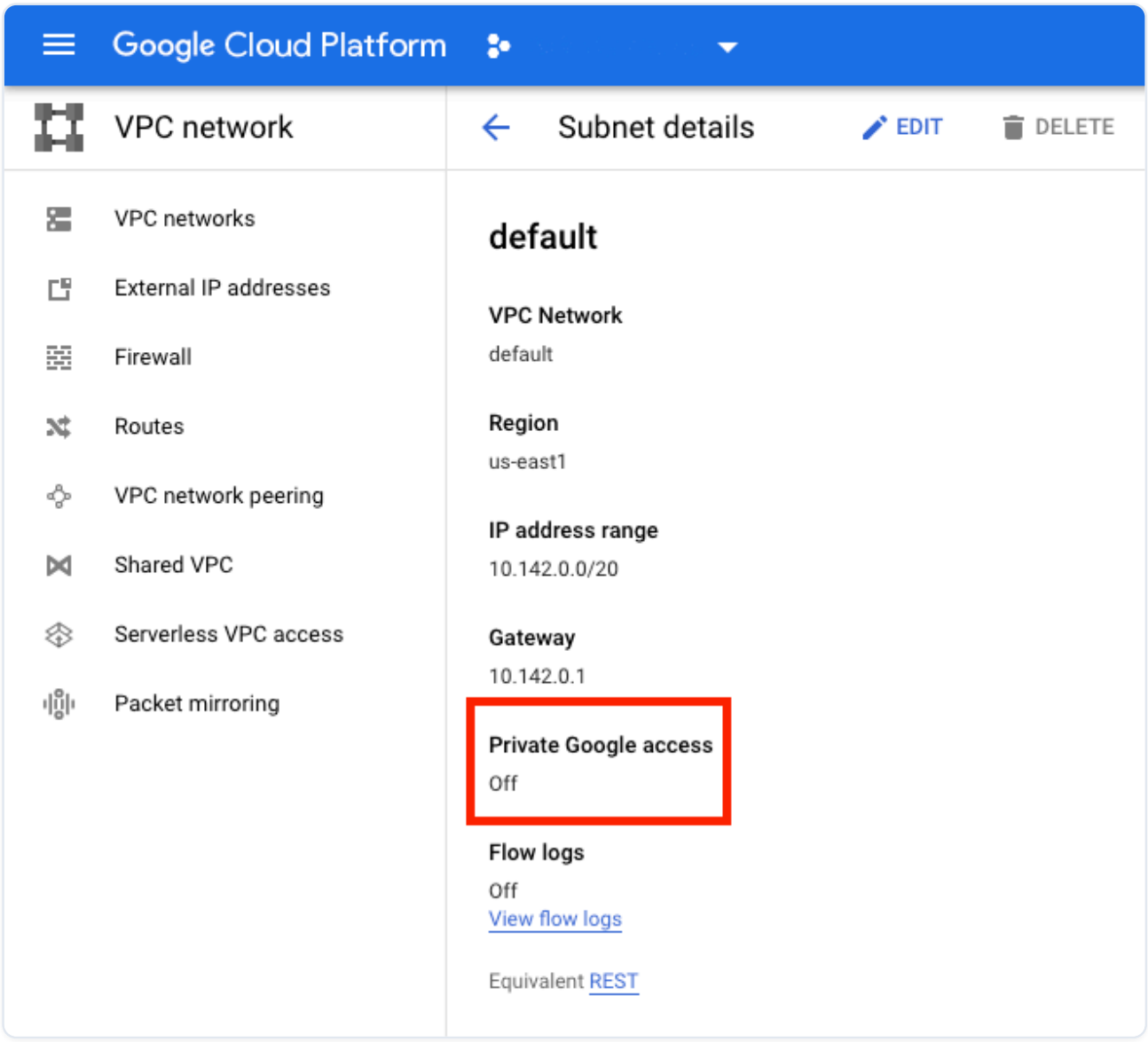
プライベート Google アクセスを有効にする

VM のネットワークインターフェイスに外部 IP アドレスが割り当てられていない場合、パケットは他の内部 IP アドレスの宛先にのみ送信されます。プライベートアクセスを有効にすると、VM は Google API および関連サービスで使用される外部 IP アドレスのセットに接続します。

> **注：**
>
> プライベート Google アクセスが有効になっているかどうかにかかわらず、パブリック IP アドレスを持つ VM と持たない VM の両方が、特にサードパーティのネットワークアプライアンスが環境にインストールされている場合、Google Public API にアクセスできる必要があります。

MCSプロビジョニングのために、サブネット内のVMがパブリックIPアドレスなしでGoogle APIにアクセスできるようにするには、次の手順を実行します。

1. Google Cloudで、**VPC network configuration**にアクセスします。
2. サブネットの詳細画面で、「**Private Googleアクセス**」をオンにします。



詳細については、「Configuring Private Google Access」を参照してください。

> **重要:**
>
> ネットワークがVMのインターネットアクセスを防止するように構成されている場合、VMが接続されているサブネットに対してPrivate Googleアクセスを有効にすることに関連するリスクを組織が負うことを確認してください。

接続の追加

「接続とリソースの作成」(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/manage-deployment/connections.html)のガイダンスに従ってください。次の説明は、ホスティング接続の設定について説明しています。

1. **管理 > 構成**から、左側のペインで**ホスティング**を選択します。

2. アクションバーで**「接続とリソースの追加」**を選択します。
3. **「接続」ページで、「新しい接続の作成」と「Citrix provisioning™ tools」を選択し、「次へ」**を選択します。
   - **接続の種類**。メニューから**Google Cloud**を選択します。
   - **接続名**。接続の名前を入力します。
4. 「**リージョン**」ページで、メニューからプロジェクト名を選択し、使用するリソースを含むリージョンを選択してから、「**次へ**」を選択します。
5. 「**ネットワーク**」ページで、リソースの名前を入力し、メニューから仮想ネットワークを選択し、サブセットを選択してから、「**次へ**」を選択します。リソース名は、リージョンとネットワークの組み合わせを識別するのに役立ちます。名前に「*(Shared)*」サフィックスが付いている仮想ネットワークは、共有VPCを表します。共有VPCのサブネットレベルのIAMロールを構成した場合、共有VPCの特定のサブネットのみがサブネットリストに表示されます。

   > **注：**
   >
   > - リソース名には1～64文字を含めることができ、空白のみ、または文字`\ / ; : # . * ? = < > | [ ] { } " ' ( ) ' )`を含めることはできません。

6. 「**概要**」ページで情報を確認し、「**完了**」を選択して「**接続とリソースの追加**」ウィンドウを終了します。

接続とリソースを作成すると、作成した接続とリソースが一覧表示されます。接続を構成するには、接続を選択し、アクションバーで該当するオプションを選択します。

同様に、接続の下に作成されたリソースを削除、名前変更、またはテストできます。これを行うには、接続の下のリソースを選択し、アクションバーで該当するオプションを選択します。

マスターVMインスタンスと永続ディスクを準備する

> **ヒント:**
>
> 永続ディスクは、仮想ディスクを指すGoogle Cloudの用語です。

> マスターVMインスタンスを準備するには、計画しているマシンカタログ内のクローンVDAインスタンスに必要な構成と一致するプロパティを持つVMインスタンスを作成および構成します。この構成は、インスタンスのサイズとタイプにのみ適用されるわけではありません。メタデータ、タグ、GPU割り当て、ネットワークタグ、サービスアカウントのプロパティなどのインスタンス属性も含まれます。

マスタリングプロセスの一環として、MCSはマスターVMインスタンスを使用してGoogle Cloudの*インスタンステンプレート*を作成します。このインスタンステンプレートは、マシンカタログを構成するクローンVDAインスタンスの作成に使用されます。クローンインスタンスは、インスタンステンプレートが作成されたマスターVMインスタンスのプロパティ（VPC、サブネット、永続ディスクのプロパティを除く）を継承します。

マスターVMインスタンスのプロパティを要件に合わせて構成したら、インスタンスを起動し、そのインスタンスの永続ディスクを準備します。

ディスクのスナップショットを手動で作成することをお勧めします。そうすることで、意味のある命名規則を使用してバージョンを追跡し、マスターイメージの以前のバージョンを管理するためのより多くのオプションが得られ、マシンカタログ作成の時間を節約できます。独自のスナップショットを作成しない場合、MCSは一時的なスナップショットを作成します（これはプロビジョニングプロセスの終了時に削除されます）。

マシンカタログを作成する

> **注：**
>
> マシンカタログを作成する前に、リソースを作成してください。マシンカタログを構成する際は、Google Cloud が定めた命名規則を使用してください。詳細については、バケットとオブジェクトの命名ガイドラインを参照してください。

> 「マシンカタログの作成」(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/install-configure/machine-catalogs-create.html)のガイダンスに従ってください。現在、StudioはGoogle Cloudカタログの作成をサポートしていません。代わりにPowerShellを使用してください。

マシンカタログの管理

カタログにマシンを追加したり、マシンを更新したり、更新をロールバックしたりするには、「マシンカタログの管理」を参照してください。

電源管理

Citrix DaaSでは、Google Cloudマシンの電源管理が可能です。ナビゲーションペインの**検索**ノードを使用して、電源管理したいマシンを見つけます。以下の電源操作が利用可能です。

- 削除
- 起動
- 再起動
- 強制再起動
- シャットダウン
- 強制シャットダウン
- デリバリーグループに追加
- タグの管理
- メンテナンスモードをオンにする

Autoscaleを使用してGoogle Cloudマシンを電源管理することもできます。これを行うには、Google Cloudマシンをデリバリーグループに追加し、そのデリバリーグループでAutoscaleを有効にします。Autoscaleの詳細については、「Autoscale」を参照してください。

偶発的なマシン削除からの保護

Citrix DaaSでは、偶発的な削除を防ぐために、Google Cloud上のMCSリソースを保護できます。プロビジョニングされたVMを構成するには、`deletionProtection`フラグをTRUEに設定します。

デフォルトでは、MCSまたはGoogle Cloudプラグインを介してプロビジョニングされたVMは、InstanceProtectionが有効な状態で作成されます。この実装は、永続カタログと非永続カタログの両方に適用されます。非永続カタログは、インスタンスがテンプレートから再作成されるときに更新されます。既存の永続マシンについては、Google Cloudコンソールでフラグを設定できます。フラグの設定の詳細については、「Googleドキュメントサイト」を参照してください。永続カタログに追加される新しいマシンは、`deletionProtection`が有効な状態で作成されます。

`deletionProtection`フラグを設定したVMインスタンスを削除しようとすると、リクエストは失敗します。ただし、`compute.instances.setDeletionProtection`権限が付与されているか、IAMの**Compute Admin**ロールが割り当てられている場合は、フラグをリセットしてリソースを削除できるようにすることができます。

手動で作成されたGoogle Cloudマシンをインポートする

Google Cloudへの*接続を作成*し、*その後Google Cloudマシンを含むカタログを作成*できます。その後、Citrix DaaSを介してGoogle Cloudマシンを手動で電源サイクルできます。この機能を使用すると、次のことが可能になります。

- 手動で作成されたGoogle CloudマルチセッションOSマシンをCitrix Virtual Apps and Desktopsマシンカタログにインポートします。
- 手動で作成されたGoogle CloudマルチセッションOSマシンをCitrix Virtual Apps and Desktopsカタログから削除します。
- 既存のCitrix Virtual Apps and Desktopsの電源管理機能を使用して、Google Cloud WindowsマルチセッションOSマシンの電源を管理します。たとえば、それらのマシンの再起動スケジュールを設定します。

この機能は、既存のCitrix Virtual Apps and Desktopsのプロビジョニングワークフローに変更を加える必要はなく、既存の機能を削除する必要もありません。手動で作成されたGoogle Cloudマシンをインポートする代わりに、Web StudioでMCSを使用してマシンをプロビジョニングすることをお勧めします。

共有仮想プライベートクラウド

共有仮想プライベートクラウド（VPC）は、共有サブネットが利用可能になるホストプロジェクトと、そのリソースを使用する1つ以上のサービスプロジェクトで構成されます。共有VPCは、共有企業Googleクラウド資産の一元的な制御、使用、管理を提供するため、大規模なインストールに適したオプションです。詳細については、Googleドキュメントサイトを参照してください。

この機能により、Machine Creation Services™ (MCS) は、共有VPCに展開されたマシンカタログのプロビジョニングと管理をサポートします。このサポートは、現在ローカルVPCで提供されているサポートと機能的に同等ですが、2つの点で異なります。

1. ホスト接続の作成に使用されるサービスアカウントに追加の権限を付与する必要があります。このプロセスにより、MCSは共有VPCリソースにアクセスして使用できるようになります。
2. 2つのファイアウォールルールを作成する必要があります。1つはイングレス用、もう1つはエグレス用です。これらのファイアウォールルールは、イメージマスタリングプロセス中に使用されます。

必要な新しい権限

ホスト接続を作成する際には、特定の権限を持つGoogle Cloudサービスアカウントが必要です。これらの追加権限は、共有VPCベースのホスト接続の作成に使用されるすべてのサービスアカウントに付与する必要があります。

ヒント:

これらの追加権限は、Citrix DaaSにとって新しいものではありません。これらはローカルVPCの実装を容易にするために使用されます。共有VPCでは、これらの追加権限により、他の共有VPCリソースへのアクセスが可能になります。

Shared VPCをサポートするために、ホスト接続に関連付けられたサービスアカウントに最大4つの追加権限を付与する必要があります。

1. **compute.firewalls.list** - この権限は必須です。MCSがShared VPCに存在するファイアウォールルールのリストを取得できるようにします。
2. **compute.networks.list** - この権限は必須です。MCSがサービスアカウントで利用可能なShared VPCネットワークを識別できるようにします。
3. **compute.subnetworks.list** – この権限は、VPCの使用方法によってオプションです。MCSが可視Shared VPC内のサブネットを識別できるようにします。この権限はローカルVPCを使用する際にはすでに必要ですが、Shared VPCホストプロジェクトでも割り当てる必要があります。
4. **compute.subnetworks.use** - この権限は、VPCの使用方法によってオプションです。プロビジョニングされたマシンカタログでサブネットリソースを使用するために必要です。この権限はローカルVPCを使用する際にはすでに必要ですが、Shared VPCホストプロジェクトでも割り当てる必要があります。

これらの権限を使用する際には、マシンカタログの作成に使用される権限の種類に基づいて異なるアプローチがあることを考慮してください。

- プロジェクトレベルの権限:
  - ホストプロジェクト内のすべてのShared VPCへのアクセスを許可します。
  - 権限 #3 と #4 をサービスアカウントに割り当てる必要があります。
- サブネットレベルの権限:
  - Shared VPC内の特定のサブネットへのアクセスを許可します。
  - 権限 #3 と #4 はサブネットレベルの割り当てに固有のものであるため、サービスアカウントに直接割り当てる必要はありません。

組織のニーズとセキュリティ基準に合ったアプローチを選択してください。

> **ヒント:**
>
> プロジェクトレベルとサブネットレベルの権限の違いの詳細については、Google Cloud ドキュメントを参照してください。

ファイアウォールルール

マシンカタログの準備中に、カタログのマスターイメージシステムディスクとして機能するマシンイメージが準備されます。このプロセスが発生すると、ディスクは一時的に仮想マシンに接続されます。このVMは、すべてのインバウンドおよびアウトバウンドネットワークトラフィックを防止する分離された環境で実行する必要があります。これは、イングレス用とエグレス用の2つのすべての拒否ファイアウォールルールによって実現されます。Google CloudローカルVCPを使用する場合、MCSはこのファイアウォールをローカルネットワークに作成し、マスタリング用のマシンに適用します。マスタリングが完了すると、ファイアウォールルールはイメージから削除されます。

共有VPCを使用するために必要な新しい権限の数を最小限に抑えることをお勧めします。共有VPCはより上位の企業リソースであり、通常、より厳格なセキュリティプロトコルが導入されています。このため、ホストプロジェクトの共有VPCリソースに、イングレス用とエグレス用の2つのファイアウォールルールを作成してください。それらに最高の優先順位を割り当てます。次の値を使用して、これらの各ルールに新しいターゲットタグを適用します。

`citrix-provisioning-quarantine-firewall`

MCSがマシンカタログを作成または更新するとき、このターゲットタグを含むファイアウォールルールを検索します。次に、ルールの正確性を確認し、カタログのマスターイメージを準備するために使用されるマシンに適用します。ファイアウォールルールが見つからない場合、またはルールは見つかったものの、ルールやその優先順位が正しくない場合は、次のようなメッセージが表示されます。

```
"Unable to find valid INGRESS and EGRESS quarantine firewall rules for VPC <name> in project <project>. " Please ensure you have created 'deny all' firewall rules with the network tag 'citrix-provisioning-quarantine-firewall' and proper priority." "Refer to Citrix Documentation for details."
```

共有VPCの構成

Web Studioで共有VPCをホスト接続として追加する前に、プロビジョニングするプロジェクトからサービスアカウントを追加するために、次の手順を完了してください。

1. IAMロールを作成します。

2. CVADホスト接続の作成に使用されるサービスアカウントを、共有VPCホストプロジェクトのIAMロールに追加します。
3. プロビジョニングするプロジェクトのCloud Buildサービスアカウントを、共有VPCホストプロジェクトのIAMロールに追加します。
4. ファイアウォールルールを作成します。

IAMロールを作成する

ロールのアクセスレベルを決定します — *プロジェクトレベルアクセス*、または*サブネットレベルアクセス*を使用するより制限されたモデル。

IAMロールのプロジェクトレベルアクセス。プロジェクトレベルのIAMロールには、次の権限を含めます。

- compute.firewalls.list
- compute.networks.list
- compute.subnetworks.list
- compute.subnetworks.use

プロジェクトレベルのIAMロールを作成するには：

1. Google Cloudコンソールで、**IAMと管理 > ロール**に移動します。
2. 「**ロール**」ページで、「**ロールを作成**」を選択します。
3. 「**ロールを作成**」ページで、ロール名を指定します。「**権限を追加**」を選択します。
    a. **権限の追加**ページで、ロールに権限を個別に追加します。権限を追加するには、**テーブルをフィルタリング**フィールドに権限の名前を入力します。権限を選択し、**追加**を選択します。
    b. 「**作成**」を選択します。

サブネットレベルのIAMロール。このロールは、**ロールを作成**を選択した後に、権限`compute.subnetworks.list`と`compute.subnetworks.use`の追加を省略します。このIAMアクセスレベルの場合、権限`compute.firewalls.list`と`compute.networks.list`を新しいロールに適用する必要があります。

サブネットレベルのIAMロールを作成するには：

1. Google Cloudコンソールで、**VPCネットワーク** > **共有VPC**に移動します。**共有VPC**ページが表示され、ホストプロジェクトに含まれる共有VPCネットワークのサブネットが表示されます。

2. 「**共有VPC**」ページで、アクセスするサブネットを選択します。
3. 右上隅で「**メンバーを追加**」を選択して、サービスアカウントを追加します。
4. 「**メンバーを追加**」ページで、次の手順を実行します。
    a. 「**新しいメンバー**」フィールドにサービスアカウントの名前を入力し、メニューからサービスアカウントを選択します。
    b. 「**ロールを選択**」フィールドを選択し、次に「**Compute Network User**」を選択します。
    c. 「**保存**」を選択します。
5. Google Cloud コンソールで、「**IAM と管理**」>「**ロール**」に移動します。
6. 「**ロール**」ページで、「**ロールを作成**」を選択します。
7. 「**ロールを作成**」ページで、ロール名を指定します。「**権限を追加**」を選択します。
    a. 「**権限を追加**」ページで、ロールに個別に権限を追加します。権限を追加するには、「**テーブルをフィルタ**」フィールドに権限の名前を入力します。権限を選択し、「**追加**」を選択します。
    b. 「**作成**」を選択します。

ホストプロジェクトのIAMロールにサービスアカウントを追加する

IAMロールを作成したら、ホストプロジェクトのサービスアカウントを追加するために次の手順を実行します。

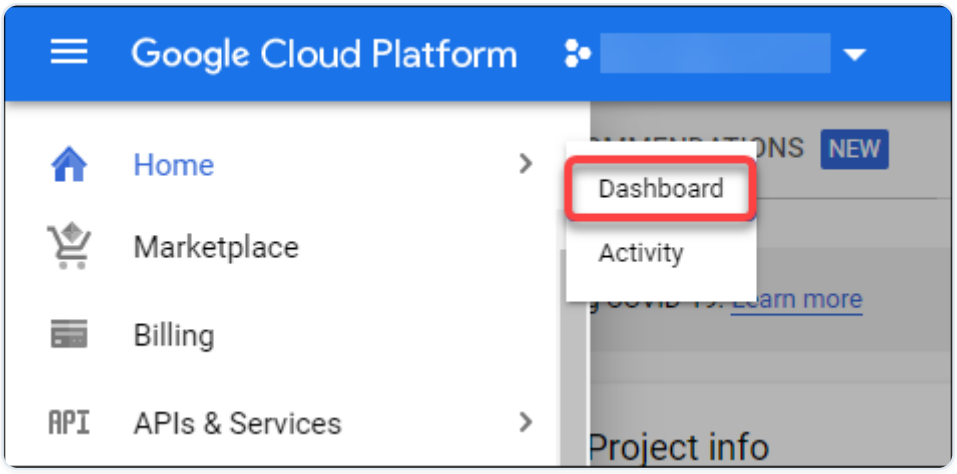
1. Google Cloud コンソールで、ホストプロジェクトに移動し、次に「**IAM と管理 > IAM**」に移動します。
2. 「**IAM**」ページで、「**追加**」を選択してサービスアカウントを追加します。
3. 「**メンバーを追加**」ページで、:
    a. 「**新しいメンバー**」フィールドにサービスアカウントの名前を入力し、メニューからサービスアカウントを選択します。
    b. ロールフィールドを選択し、作成したIAMロールを入力して、メニューからそのロールを選択します。
    c. 「**保存**」を選択します。

これで、サービスアカウントがホストプロジェクト用に構成されました。

クラウドビルドサービスアカウントを共有VPCに追加する

すべてのGoogle Cloudサブスクリプションには、プロジェクトID番号の後に `cloudbuild.gserviceaccount` が続くサービスアカウントがあります。例: `705794712345@cloudbuild.gserviceaccount`。

Google Cloudコンソールで**ホーム**と**ダッシュボード**を選択すると、プロジェクトのプロジェクトID番号を確認できます。



画面の**プロジェクト情報**領域の下にある**プロジェクト番号**を見つけます。

Cloud Buildサービスアカウントを共有VPCに追加するには、次の手順を実行します。

1. Google Cloudコンソールで、ホストプロジェクトに移動し、**IAMと管理** > **IAM**に移動します。
2. 「**権限**」ページで、「**追加**」を選択してアカウントを追加します。
3. 「**メンバーを追加**」ページで、次の手順を実行します。
    a. 「**新しいメンバー**」フィールドにCloud Buildサービスアカウントの名前を入力し、メニューからサービスアカウントを選択します。
    b. 「**ロールを選択**」フィールドを選択し、`Computer Network User` と入力して、メニューからロールを選択します。
    c. 「**保存**」を選択します。

ファイアウォールルールを作成する

マスタリングプロセスの一環として、MCS は選択したマシンイメージをコピーし、それを使用してカタログ用のマスターイメージシステムディスクを準備します。マスタリング中に、MCS はディスクを一時的な仮想マシンに接続し、その仮想マシンが準備スクリプトを実行します。この VM は、すべてのインバウンドおよびアウトバウンドネットワークトラフィックを禁止する分離された環境で実行する必要があります。分離された環境を作成するには、MCS は2つの *すべて拒否*

ファイアウォールルール（イングレスルールとエグレスルール）を必要とします。したがって、*ホストプロジェクト* に次の2つのファイアウォールルールを作成します。

1. Google Cloud コンソールで、ホストプロジェクトに移動し、次に **VPC ネットワーク > ファイアウォール** に移動します。
2. 「**ファイアウォール**」ページで、「**ファイアウォールルールを作成**」を選択します。
3. 「**ファイアウォールルールを作成**」ページで、以下を完了します。
   - **名前**。ルールの名前を入力します。
   - **ネットワーク**。イングレスファイアウォールルールが適用される共有 VPC ネットワークを選択します。
   - **優先度**。値が小さいほど、ルールの優先度が高くなります。小さい値（例: 10）をお勧めします。
   - **トラフィックの方向**。**イングレス** を選択します。
   - **一致時のアクション**。**拒否** を選択します。
   - **ターゲット**。デフォルトの **指定されたターゲットタグ** を使用します。
   - **ターゲットタグ**。`citrix-provisioning-quarantine-firewall` と入力します。
   - **ソースフィルター**。デフォルトの **IP 範囲** を使用します。
   - **ソース IP 範囲**。すべてのトラフィックに一致する範囲を入力します。`0.0.0.0/0` と入力します。
   - **プロトコルとポート**。「**すべて拒否**」を選択します。
4. 「**作成**」を選択してルールを作成します。
5. 手順1〜4を繰り返して、別のルールを作成します。**トラフィックの方向** には、**エグレス** を選択します。

接続の追加

Google Cloud環境への接続を追加します。「接続の追加」を参照してください。

ゾーン選択を有効にする

Citrix Virtual Apps and Desktops はゾーン選択をサポートしています。ゾーン選択を使用すると、VM を作成するゾーンを指定できます。ゾーン選択を使用すると、管理者は選択したゾーンに単一テナントノードを配置できます。単一テナンシーを構成するには、Google Cloud で以下を完了する必要があります。

- Google Cloud の単一テナントノードを予約する

- VDA マスターイメージを作成する

Google Cloud の単一テナントノードの予約

単一テナントノードを予約するには、Google Cloud のドキュメントを参照してください。

> **重要:**
>
> ノードテンプレートは、ノードグループに予約されているシステムのパフォーマンス特性を示すために使用されます。これらの特性には、vGPU の数、ノードに割り当てられるメモリ量、およびノード上に作成されるマシンに使用されるマシンタイプが含まれます。詳細については、Google Cloud のドキュメントを参照してください。

VDA マスターイメージの作成

単一テナントノードにマシンを正常に展開するには、マスター VM イメージを作成する際に追加の手順を実行する必要があります。Google Cloud のマシンインスタンスには、*ノードアフィニティラベル*と呼ばれるプロパティがあります。単一テナントノードに展開されるカタログのマスターイメージとして使用されるインスタンスには、**ターゲットノードグループ**の名前と一致する*ノードアフィニティラベル*が必要です。これを実現するには、次の点に留意してください。

- 新しいインスタンスの場合、インスタンスの作成時に Google Cloud コンソールでラベルを設定します。詳細については、「インスタンス作成時にノードアフィニティラベルを設定する」を参照してください。
- 既存のインスタンスの場合、**gcloud** コマンドラインを使用してラベルを設定します。詳細については、「既存のインスタンスにノードアフィニティラベルを設定する」を参照してください。

> **注：**
>
> 共有 VPC で単一テナンシーを使用する場合は、共有仮想プライベートクラウドを参照してください。

インスタンス作成時にノードアフィニティラベルを設定する

ノードアフィニティラベルを設定するには：

1. Google Cloud コンソールで、**Compute Engine > VM インスタンス** に移動します。
2. **VM インスタンス** ページで、**インスタンスを作成** を選択します。

3. **インスタンスの作成** ページで、必要な情報を入力または構成し、**管理、セキュリティ、ディスク、ネットワーク、単一テナンシー** を選択して設定パネルを開きます。
4. **単一テナンシー** タブで、**参照** を選択して現在のプロジェクトで利用可能なノードグループを表示します。**単一テナントノード** ページが表示され、利用可能なノードグループのリストが表示されます。
5. **単一テナントノード** ページで、リストから該当するノードグループを選択し、**選択** を選択して **単一テナンシー** タブに戻ります。ノードアフィニティラベルフィールドには、選択した情報が入力されます。この設定により、インスタンスから作成されたマシンカタログが選択したノードグループに展開されることが保証されます。
6. 「**作成**」を選択してインスタンスを作成します。

既存のインスタンスにノードアフィニティラベルを設定する

ノードアフィニティラベルを設定するには:

1. Google Cloud Shellターミナルウィンドウで、*gcloud compute instances*コマンドを使用してノードアフィニティラベルを設定します。**gcloud**コマンドに次の情報を含めます:

   - **VMの名前**。たとえば、`s*2019-vda-base`.*という既存のVMを使用します。
   - **ノードグループの名前**。以前に作成したノードグループ名を使用します。たとえば、`mh-sole-tenant-node-group-1`。
   - **インスタンスが存在するゾーン**。たとえば、VMは`*us-east-1b* zone`にあります。

   たとえば、ターミナルウィンドウで次のコマンドを入力します:

   - `gcloud compute instances set-scheduling "s2019-vda-base" --node-group="mh-sole-tenant-node-group-1" --zone="us-east1-b"`

   *gcloud compute instances*コマンドの詳細については、`<https://cloud.google.com/sdk/gcloud/reference/beta/compute/instances/set-scheduling>`にあるGoogle Developer Toolsのドキュメントを参照してください。
2. インスタンスの**VMインスタンスの詳細**ページに移動し、**ノードアフィニティ**フィールドにラベルが入力されていることを確認します。

マシンカタログを作成する

ノードアフィニティラベルを設定した後、マシンカタログを構成します。

プレビュー: 顧客管理の暗号化キー (CMEK) の使用

MCSカタログに顧客管理の暗号化キー (CMEK) を使用できます。この機能を使用する場合、Google Cloud Key Management Serviceの`CryptoKey Encrypter/Decrypter`ロールをCompute Engineサービスエージェントに割り当てます。Citrix DaaSアカウントは、キーが保存されているプロジェクトで適切な権限を持っている必要があります。詳細については、Cloud KMSキーを使用してリソースを保護するを参照してください。

Compute Engine サービスエージェントは次の形式です: `service-<Project_Number>@compute-system.iam.gserviceaccount.com`。この形式は、デフォルトの Compute Engine サービスアカウントとは異なります。

> **注：**
>
> この Compute Engine サービスアカウントは、Google Console の「**IAM 権限**」表示に表示されない場合があります。そのような場合は、Cloud KMS キーを使用してリソースを保護する で説明されているように、`gcloud` コマンドを使用してください。

Citrix DaaS アカウントに権限を割り当てる

Google Cloud KMS の権限はさまざまな方法で構成できます。*プロジェクトレベル*の KMS 権限または*リソースレベル*の KMS 権限のいずれかを付与できます。詳細については、権限とロール を参照してください。

プロジェクトレベルの権限

1つのオプションは、Citrix DaaS アカウントに Cloud KMS リソースを参照するためのプロジェクトレベルの権限を付与することです。これを行うには、カスタムロールを作成し、次の権限を追加します。

- `cloudkms.keyRings.list`
- `cloudkms.keyRings.get`
- `cloudkms.cryptokeys.list`
- `cloudkms.cryptokeys.get`

このカスタムロールをCitrix DaaSアカウントに割り当てます。これにより、インベントリ内の関連プロジェクトでリージョンキーを参照できるようになります。

リソースレベルの権限

もう1つのオプションであるリソースレベルの権限については、Google Cloudコンソールで、MCSプロビジョニングに使用する`cryptoKey`を参照します。カタログプロビジョニングに使用するキーリングまたはキーにCitrix DaaSアカウントを追加します。

> **ヒント:**
>
> このオプションでは、Citrix DaaSアカウントにCloud KMSリソースに対するプロジェクトレベルのリスト権限がないため、インベントリでプロジェクトのリージョンキーを参照できません。ただし、以下で説明するように、`ProvScheme`カスタムプロパティで正しい`cryptoKeyId`を指定することで、CMEKを使用してカタログをプロビジョニングすることは可能です。

カスタムプロパティを使用したCMEKによるプロビジョニング

PowerShellでプロビジョニングスキームを作成する際に、`ProvScheme CustomProperties`で`CryptoKeyId`プロパティを指定します。例:

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="CryptoKeyId"
Value="<yourCryptoKeyId>" />

</CustomProperties>'
```

`cryptoKeyId`は次の形式で指定する必要があります。

`projectId:location:keyRingName:cryptoKeyName`

たとえば、IDが`my-example-project-1`のプロジェクトで、`us-east1`リージョンのキーリング`my-example-key-ring`にあるキー`my-example-key`を使用したい場合、`ProvScheme`カスタム設定は次のようになります。

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-
example-project-1:us-east1:my-example-key-ring:my-example-key" />
```

```
</CustomProperties>'
```

このプロビジョニングスキームに関連するすべてのMCSプロビジョニング済みディスクとイメージは、この顧客管理暗号化キーを使用します。

ヒント:

グローバルキーを使用する場合、顧客プロパティの場所は**リージョン**名ではなく`global`と記述する必要があります。上記の例では**us-east1**です。例: `<Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-example-project-1:global:my-example-key-ring:my-example-key" />`。

顧客管理キーのローテーション

Google Cloudは、既存の永続ディスクまたはイメージでのキーのローテーションをサポートしていません。マシンがプロビジョニングされると、作成時に使用されていたキーのバージョンに紐付けられます。ただし、新しいバージョンのキーを作成でき、その新しいキーは、新しくプロビジョニングされたマシンや、新しいマスターイメージでカタログが更新されたときに作成されるリソースに使用されます。

キーリングに関する重要な考慮事項

キーリングの名前変更や削除はできません。また、キーリングを構成する際に予期せぬ料金が発生する可能性があります。キーリングを削除または削除すると、Google Cloudはエラーメッセージを表示します。

```
Sorry, you can't delete or rename keys or key rings. We were concerned
about the security implications of allowing multiple keys or key versions
over time to have the same resource name, so we decided to make names
immutable. (And you can't delete them, because we wouldn't be able to do a
true deletion--there would still have to be a tombstone tracking that this
name had been used and couldn't be reused).

We're aware that this can make things untidy, but we have no immediate
plans to change this.

If you want to avoid getting billed for a key or otherwise make it
unavailable, you can do so by deleting all the key versions; neither keys
```

```
nor key rings are billed for, just the active key versions within the
keys.
```

ヒント:

詳細については、「コンソールからキーリングを編集または削除する」を参照してください。

均一なバケットレベルのアクセス互換性

Citrix DaaS は、Google Cloud の uniform bucket-level access control policy と互換性があります。この機能は、ストレージバケットを含むリソースの操作を許可するために、サービスアカウントに権限を付与する IAM ポリシーの使用を強化します。uniform bucket level access control を使用すると、Citrix DaaS はアクセス制御リスト (ACL) を使用して、ストレージバケットまたはそこに保存されているオブジェクトへのアクセスを制御できます。Google Cloud の uniform bucket-level access の概要については、Uniform bucket-level access を参照してください。構成情報については、Require uniform bucket-level access を参照してください。

サービスエンドポイントURL

次のURLにアクセスできる必要があります。

- `https://oauth2.googleapis.com`
- `https://cloudresourcemanager.googleapis.com`
- `https://compute.googleapis.com`
- `https://storage.googleapis.com`
- `https://cloudbuild.googleapis.com`

Google Cloudプロジェクト

Google Cloudプロジェクトには基本的に2つのタイプがあります。

- プロビジョニングプロジェクト：この場合、現在の管理者アカウントがプロジェクト内のプロビジョニングされたマシンを所有します。このプロジェクトはローカルプロジェクトとも呼ばれます。
- 共有VPCプロジェクト: プロビジョニングプロジェクトで作成されたマシンが、共有VPCプロジェクトのVPCを使用するプロジェクト。プロビジョニングプロジェクトに使用される管理者

アカウントは、このプロジェクトで限られた権限、具体的にはVPCを使用する権限のみを持ちます。

必要なGCP権限

このセクションには、GCP権限の完全なリストが含まれています。機能が正しく動作するように、このセクションに記載されている権限の完全なセットを使用してください。

> **注：**
>
> GCPは、Cloud Build Servicesのデフォルトの動作とサービスアカウントの使用に関して、April 29, 2024以降に変更を導入します。詳細については、Cloud Build Service Account Changeを参照してください。April 29, 2024より前にCloud Build APIが有効になっている既存のGoogleプロジェクトは、この変更の影響を受けません。ただし、April 29以降も既存のCloud Build Serviceの動作を維持したい場合は、APIを有効にする前に、制約の適用を無効にする組織ポリシーを作成または適用できます。新しい組織ポリシーを設定した場合、このセクションの既存の権限と、**Cloud Build Service Account Change前**とマークされている項目を引き続き使用できます。そうでない場合は、既存の権限と、**Cloud Build Service Account Change後**とマークされている項目に従ってください。

ホスト接続の作成

- プロビジョニングプロジェクトのCitrix Cloudサービスアカウントに必要な最小限の権限：

```
compute.instanceTemplates.list

compute.instances.list

compute.networks.list

compute.projects.get

compute.regions.list

compute.subnetworks.list

compute.zones.list

resourcemanager.projects.get
```

次の Google 定義ロールには、上記にリストされている権限があります:

- Compute 管理者
- クラウド データストア ユーザー

- 共有 VPC プロジェクト内の Citrix Cloud サービスアカウントの共有 VPC に必要な追加の権限:

```
compute.networks.list

compute.subnetworks.list

resourcemanager.projects.get
```

次の Google 定義ロールには、上記にリストされている権限があります:

- コンピュート ネットワーク ユーザー

VM の電源管理

電源管理のみのカタログの場合に、プロビジョニングプロジェクト内のCitrix Cloudサービスアカウントに必要な最小限の権限:

```
compute.instanceTemplates.list

compute.instances.list

compute.instances.get

compute.instances.reset

compute.instances.resume

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.networks.list

compute.projects.get
```

```
compute.regions.list

compute.subnetworks.list

compute.zones.list

resourcemanager.projects.get

compute.zoneOperations.get
```

次の Google 定義ロールには、上記にリストされている権限があります:

- Compute 管理者
- クラウド データストア ユーザー

仮想マシンの作成、更新、または削除

- プロビジョニングプロジェクトのCitrix Cloudサービスアカウントに必要な最小限の権限：

```
cloudbuild.builds.create

cloudbuild.builds.get

cloudbuild.builds.list

compute.acceleratorTypes.list

compute.diskTypes.get

compute.diskTypes.list

compute.disks.create

compute.disks.createSnapshot

compute.disks.delete

compute.disks.get

compute.disks.list

compute.disks.setLabels
```

```
compute.disks.use

compute.disks.useReadOnly

compute.firewalls.create

compute.firewalls.delete

compute.firewalls.list

compute.globalOperations.get

compute.images.create

compute.images.delete

compute.images.get

compute.images.list

compute.images.setLabels

compute.images.useReadOnly

compute.instanceTemplates.create

compute.instanceTemplates.delete

compute.instanceTemplates.get

compute.instanceTemplates.list

compute.instanceTemplates.useReadOnly

compute.instances.attachDisk

compute.instances.create

compute.instances.delete

compute.instances.detachDisk

compute.instances.get
```

```
compute.instances.list

compute.instances.reset

compute.instances.resume

compute.instances.setDeletionProtection

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setServiceAccount

compute.instances.setTags

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.machineTypes.get

compute.machineTypes.list

compute.networks.list

compute.networks.updatePolicy

compute.nodeGroups.list

compute.nodeTemplates.get

compute.projects.get

compute.regions.list

compute.snapshots.create

compute.snapshots.delete

compute.snapshots.list
```

```
compute.snapshots.get

compute.snapshots.setLabels

compute.snapshots.useReadOnly

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.zoneOperations.get

compute.zoneOperations.list

compute.zones.get

compute.zones.list

iam.serviceAccounts.actAs

resourcemanager.projects.get

storage.buckets.create

storage.buckets.delete

storage.buckets.get

storage.buckets.list

storage.buckets.update

storage.objects.create

storage.objects.delete

storage.objects.get

storage.objects.list

compute.networks.get
```

```
compute.resourcePolicies.use
```

次の Google 定義ロールには、上記にリストされている権限があります:

- Compute 管理者
- Storage管理者
- Cloud Build編集者
- サービスアカウントユーザー
- クラウド データストア ユーザー

- 共有VPCプロジェクトのVPCとサブネットワークを使用してホスティングユニットを作成するために、共有VPCプロジェクト内のCitrix Cloudサービスアカウントの共有VPCに追加で必要な権限:

```
compute.firewalls.list

compute.networks.list

compute.projects.get

compute.regions.list

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.zones.list

resourcemanager.projects.get
```

次の Google 定義ロールには、上記にリストされている権限があります:

- コンピュート ネットワーク ユーザー
- クラウド データストア ユーザー

- (Cloud Buildサービスアカウント変更前): Google Cloud Buildサービスが準備指示ディスクをMCSにダウンロードする際に、プロビジョニングプロジェクトのCloud Buildサービスアカウントに必要となる最小限の権限:
- (Cloud Buildサービスアカウント変更後): Google Cloud Computeサービスが準備指示ディスクをMCSにダウンロードする際に、プロビジョニングプロジェクトのCloud Computeサービスアカウントに必要となる最小限の権限:

```
compute.disks.create

compute.disks.delete

compute.disks.get

compute.disks.list

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.images.get

compute.images.list

compute.images.useReadOnly

compute.instances.create

compute.instances.delete

compute.instances.get

compute.instances.getSerialPortOutput

compute.instances.list

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setServiceAccount
```

```
compute.machineTypes.list

compute.networks.get

compute.networks.list

compute.projects.get

compute.subnetworks.list

compute.subnetworks.use

compute.subnetworks.useExternalIp

compute.zoneOperations.get

compute.zones.list

iam.serviceAccounts.actAs

logging.logEntries.create

pubsub.topics.publish

resourcemanager.projects.get

source.repos.get

source.repos.list

storage.buckets.create

storage.buckets.get

storage.buckets.list

storage.objects.create

storage.objects.delete

storage.objects.get
```

```
storage.objects.list
```

次の Google 定義ロールには、上記にリストされている権限があります:

- Cloud Build サービスアカウント (Cloud Build サービスアカウント変更後はCloud Compute サービスアカウント)
- Compute Instance 管理者
- サービスアカウントユーザー

- MCSに準備指示ディスクをダウンロードする際に、Google Cloud Buildサービスによってプロビジョニングプロジェクトの Cloud Compute サービスアカウントに必要とされる最小限の権限:

```
resourcemanager.projects.get

storage.objects.create

storage.objects.get

storage.objects.list
```

次の Google 定義ロールには、上記にリストされている権限があります:

- コンピュート ネットワーク ユーザー
- ストレージアカウントユーザー
- クラウド データストア ユーザー

- (Cloud Buildサービスアカウント変更前): Google Cloud Buildサービスが準備指示ディスクをMCSにダウンロードする際に、プロビジョニングプロジェクトのCloud Buildサービスアカウントの共有VPCに必要となる追加の権限:
- (Cloud Buildサービスアカウント変更後): Google Cloud Computeサービスが準備指示ディスクをMCSにダウンロードする際に、プロビジョニングプロジェクトのCloud Computeサービスアカウントの共有VPCに必要となる追加の権限:

```
compute.firewalls.list

compute.networks.list
```

```
compute.subnetworks.list

compute.subnetworks.use

resourcemanager.projects.get
```

次の Google 定義ロールには、上記にリストされている権限があります:

- コンピュート ネットワーク ユーザー
- ストレージアカウントユーザー
- クラウド データストア ユーザー

- プロビジョニングプロジェクトのCitrix Cloudサービスアカウントの Cloud Key Management Service (KMS) に必要な追加権限:

```
cloudkms.cryptoKeys.get

cloudkms.cryptoKeys.list

cloudkms.keyRings.get

cloudkms.keyRings.list
```

次の Google 定義ロールには、上記にリストされている権限があります:

- Compute KMS 閲覧者

一般的な権限

以下は、MCSでサポートされているすべての機能について、プロビジョニングプロジェクトの Citrix Cloudサービスアカウントの権限です。これらの権限は、今後最高の互換性を提供します:

```
resourcemanager.projects.get

cloudbuild.builds.create

cloudbuild.builds.get

cloudbuild.builds.list

compute.acceleratorTypes.list
```

```
compute.diskTypes.get

compute.diskTypes.list

compute.disks.create

compute.disks.createSnapshot

compute.disks.delete

compute.disks.get

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.firewalls.create

compute.firewalls.delete

compute.firewalls.list

compute.globalOperations.get

compute.images.create

compute.images.delete

compute.images.get

compute.images.list

compute.images.setLabels

compute.images.useReadOnly

compute.instanceTemplates.create

compute.instanceTemplates.delete

compute.instanceTemplates.get
```

```
compute.instanceTemplates.list

compute.instanceTemplates.useReadOnly

compute.instances.attachDisk

compute.instances.create

compute.instances.delete

compute.instances.detachDisk

compute.instances.get

compute.instances.list

compute.instances.reset

compute.instances.resume

compute.instances.setDeletionProtection

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setTags

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.instances.update

compute.instances.updateAccessConfig

compute.instances.updateDisplayDevice

compute.instances.updateSecurity

compute.instances.updateShieldedInstanceConfig
```

```
compute.instances.updateShieldedVmConfig

compute.machineTypes.get

compute.machineTypes.list

compute.networks.list

compute.networks.updatePolicy

compute.nodeGroups.list

compute.nodeTemplates.get

compute.projects.get

compute.regions.list

compute.snapshots.create

compute.snapshots.delete

compute.snapshots.list

compute.snapshots.get

compute.snapshots.setLabels

compute.snapshots.useReadOnly

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.subnetworks.useExternalIp

compute.zoneOperations.get

compute.zoneOperations.list

compute.zones.get
```

```
compute.zones.list

resourcemanager.projects.get

storage.buckets.create

storage.buckets.delete

storage.buckets.get

storage.buckets.list

storage.buckets.update

storage.objects.create

storage.objects.delete

storage.objects.get

storage.objects.list

cloudkms.cryptoKeys.get

cloudkms.cryptoKeys.list

cloudkms.keyRings.get

cloudkms.keyRings.list

compute.disks.list

compute.instances.setServiceAccount

compute.networks.get

compute.networks.use

compute.networks.useExternalIp

iam.serviceAccounts.actAs
```

```
compute.resourcePolicies.use
```

詳細情報

- 接続とリソース
- マシンカタログの作成

Nutanix仮想化環境

Nutanix Acropolis を使用して Citrix Virtual Apps and Desktops™ 展開環境で仮想マシンを提供する場合は、このガイダンスに従ってください。セットアッププロセスには、次のタスクが含まれます。

- Citrix Virtual Apps and Desktops 環境に Nutanix プラグインをインストールして登録します。
- Nutanix Acropolis ハイパーバイザーへの接続を作成します。
- Nutanix ハイパーバイザーで作成したマスターイメージのスナップショットを使用するマシンカタログを作成します。

詳細については、Nutanix Support Portal で入手できる Nutanix Acropolis MCS プラグインインストールガイドを参照してください。

Nutanixプラグインのインストールと登録

すべての Delivery Controller に Nutanix プラグインをインストールして登録するには、次の手順を完了します。Citrix Studio を使用して Nutanix への接続を作成します。次に、Nutanix 環境で作成したマスターイメージのスナップショットを使用するマシンカタログを作成します。

> **ヒント:**
>
> Nutanix プラグインをインストールまたは更新する際は、Citrix Host Service、Citrix Broker Service、および Machine Creation Services™ を停止してから再起動することをお勧めします。
>
> Nutanix プラグインのインストールについては、Nutanix Documentation site を参照してください。

Nutanixへの接続を作成する

以下の情報は、接続とリソースのガイダンスを補足するものです。Nutanix接続を作成するには、その記事の一般的なガイダンスに従い、Nutanixに固有の詳細に注意してください。

接続とリソースの追加ウィザードで、**接続**ページでNutanix接続の種類を選択し、アドレスと資格情報、および接続の名前を指定します。**ネットワーク**ページで、ホスティングユニットのネットワークを選択します。

選択可能な接続タイプは次のとおりです: **Nutanix AHV**、**Nutanix AHV Xi**、および **Nutanix AHV PC**。

- **Nutanix AHV**の場合、Prism Element（PE）クラスターのアドレスと資格情報を指定します。
- **Nutanix AHV PC**の場合、Prism Central（PC）のアドレスと資格情報を指定します。

  > **注：**
  >
  > 現在、接続タイプNutanix AHV PCは、Azure上のNutanix Cloud Cluster（NC2）への接続を作成する場合にのみ使用されます。また、マシンカタログは、Azure接続上のNC2内の単一クラスターでのみホストできます。

- **Nutanix AHV DRaaS**の場合、DRaaSテナントのアドレスとユーザー名を指定します。プライベートおよびパブリックのNutanix DRaaS資格情報ファイル（`.pem`）をインポートします。

> **ヒント:**
>
> Nutanix AHV（Prism Element）をリソースとして使用してマシンを展開する場合は、VMのディスクが格納されているコンテナを選択します。

Nutanixスナップショットを使用してマシンカタログを作成する

次の情報は、マシンカタログの作成 のガイダンスを補足するものです。カタログを作成するには、その記事の一般的なガイダンスに従い、Nutanix に固有の詳細に注意してください。

選択したスナップショットは、カタログ内の VM を作成するために使用されるテンプレートです。カタログを作成する前に、Nutanix でイメージとスナップショットを作成してください。詳細については、Nutanix のドキュメントを参照してください。

カタログ作成ウィザードで：

- The **Operating System** および **Machine Management** ページには、Nutanix 固有の情報は含まれていません。
- **Container**または**Cluster and Container**ページはNutanix固有のものです。

  Nutanix AHV XI をリソースとして使用してマシンを展開する場合、**Container** ページが表示されます。VM の ID ディスクが配置されるコンテナを選択します。

  Nutanix AHV Prism Central (PC) をリソースとして使用してマシンを展開する場合、**Cluster and Container** ページが表示されます。VM の展開に使用するクラスターを選択し、次にコンテナを選択します。
- On the **Master Image** ページで、イメージスナップショットを選択します。Acropolis スナップショット名は、Citrix Virtual Apps and Desktops で使用するために「XD_」で始まる必要があります。必要に応じて、Acropolis コンソールを使用してスナップショットの名前を変更してください。スナップショットの名前を変更した場合は、カタログ作成ウィザードを再起動して、更新されたリストを表示します。
- **Virtual Machines**ページで、仮想CPUの数とvCPUあたりのコア数を指定します。
- 「**ネットワークカード**」ページで、関連するネットワークをフィルタリングするためにNICタイプを選択します。NICタイプは**VLAN**と**OVERLAY**の2種類です。マスターイメージに含まれるNICを1つ以上選択し、各NICに関連付けられた仮想ネットワークを選択します。
- **Machine Identities**、**Domain Credentials**、**Scopes**、および**Summary**ページには、Nutanix 固有の情報は含まれていません。

Nutanix クラウドおよびパートナーソリューション

Citrix Virtual Apps and Desktops™ は、以下の Nutanix クラウドおよびパートナーソリューションをサポートしています。

- AWS 上のニュータニックス クラウドクラスター

AWS 上のニュータニックス クラウドクラスター

Citrix Virtual Apps and Desktops は AWS 上の Nutanix Cloud Clusters をサポートしています。Nutanix クラスターは、プライベートクラウドまたは複数のパブリッククラウドでアプリケーションを実行する方法を簡素化します。AWS 上の Nutanix Cloud Clusters の詳細については、Nutanix Cloud Clusters on AWS Deployment and User Guide を参照してください。

> **ヒント:**

> このサポートは、Nutanix オンプレミス クラスターと同じ機能を提供します。サポートされるクラスターは、*Prism Element* の単一クラスターのみです。詳細については、こちら を参照してください。

要件

AWS で Nutanix クラスターを使用するには、以下が必要です。

- Nutanix アカウント。
- 次の権限を持つ AWS アカウント:
  - IAMFullAccess
  - AWSConfigRole
  - AWSCloudFormationFullAccess

Nutanix クラスターを作成する

Nutanix クラスターを作成するには:

1. Nutanix アカウントにログインします。
2. 「**Nutanix cluster**」オプションを見つけて、「**Launch**」をクリックします。「**Nutanix Console**」が開きます。詳細については、Get Started with Nutanix Cluster on AWS を参照してください。
3. **新しい VPC** を作成することを選択します。

クラスター作成プロセスは、以下のエラーで失敗する可能性があります:

- クラスターは指定された時間内に作成できませんでした。クラスターを削除しています。
- ホスト Nutanix クラスター - ノード `XXXXXXXXXX: Instance i-xxxxxxxxxxxx: disable network interface source/dest check error.`.
- ホスト Nutanix クラスター - ノード `XXXXXXXXXX: Unable to obtain instance i-xxxxxxxxxxxxx network interface info.`.

クラスターの作成に失敗した場合:

- 別のリージョンで再作成してみてください。
- 再試行する前に、Nutanix CloudFormation Stack (CFS) を必ず削除してください。

他のリソースに加えて、Nutanix CFS は以下を作成します。

- 1 つの VPC (*Nutanix Cluster xxxxxxxxxxxx* 10.0.0.0/16 という名前)

- 2つのサブネット 10.0.128.0/24 および 10.0.129.0/24
- 1つのインターネットゲートウェイ
- 1つのNATゲートウェイ

クラスターが作成されたら、**Nutanix Prism**のアドレスを取得します。

1. **Nutanix Console**に移動します。
2. コンソールの右上にあるリンク **Launch Prism Element** にマウスオーバーし、URLをコピーします。

Nutanix Prismへの接続

Nutanix クラスターを作成したら、Nutanix Prism に接続します。

Nutanix Prism に接続するには:

1. 10.0.129.0/24サブネットに踏み台VMを作成します。
2. 踏み台VMにRDP接続し、前のセクションでコピーした**Prism Element**のURLにアクセスします。
3. デフォルトの資格情報 `admin:nutanix/4u` を使用してログインします。パスワードを変更することを忘れないでください。

Nutanixクラスター上にVMを作成する

Nutanix Prismに接続した後、Nutanixクラスター上にVMを作成します。

VMにインターネットアクセスが必要な場合

1. AWS コンソールに移動します。
2. Nutanix CFS によって作成された VPC と同じ VPC に、新しいサブネット 10.0.130.0/24 を作成します。
3. このサブネットのルートテーブルに、すべての非ローカルトラフィックを上記のNATゲートウェイに転送するルートを追加します。
4. 踏み台VMにRDP接続し、前のセクションでコピーした**Prism Element**のURLにアクセスしてログインします。
5. 新しいネットワークを追加します。**Settings>Network Configuration>Create Subnet** に移動します。AWS で使用したのと同じサブネット 10.0.130.0/24 を使用します。
6. その新しいサブネットにすべての VM (AD、CC、VDA など) を作成します。

VM がインターネットアクセスを必要としない場合

1. 踏み台VMにRDP接続し、前のセクションでコピーした**Prism Element**のURLにアクセスしてログインします。
2. 新しいネットワークを追加します。**Settings>Network Configuration>Create Subnet** に移動します。サブネット 10.0.129.0/24 を使用します。
3. そのサブネットにすべての VM (AD、CC、VDA など) を作成します。

> **ヒント:**
>
> VM の時刻とタイムゾーン情報が正しく設定されていることを確認してください。これは特に AD に当てはまります。

ホスト接続を作成する

1. Web Studio を起動します。
2. ホスティングノードを選択し、 をクリックします。
3. **Connection** 画面で、**Create a new Connection** を選択し、**Connection address** に `https://xxx.xxx.xxx.xxx:9440` を入力します。
4. UI に従ってウィザードを完了します。

> **注：**
>
> Web Studio で Nutanix のオプションを表示するには、Nutanix ゾーンで使用されていない場合でも、すべてのコネクタ VM に nutanix プラグインがインストールされている必要があります。

コアコンポーネントをインストールする

> **重要:**
>
> Citrixは、ライセンスコンプライアンスを含む正当な利益のために、基本的なライセンスデータを収集します。詳細については、「Citrix Licensing Data」(/ja-jp/licensing/current-release/license-server/licensing-data-collection-programs.html)を参照してください。 ライセンス

> サーバーがバージョン11.17.2ビルド53100以降を実行していることを確認してください。この前提条件を満たさない場合、サイトのアップグレードや作成中にエラーや推奨事項が発生する可能性があります。

> コアコンポーネントは、Citrix Delivery Controller™、Citrix Studio、Citrix Director、および Citrix License Serverです。

(2003 より前のバージョンでは、コアコンポーネントに Citrix StoreFront が含まれていました。**Citrix StoreFront** タイルをクリックするか、インストールメディアで利用可能なコマンドを実行することで、StoreFront をインストールできます。)

インストールを開始する前に、この記事と「インストールの準備」を確認してください。

この記事では、コアコンポーネントのインストール時のインストールウィザードのシーケンスについて説明します。コマンドラインの同等機能も提供されています。詳細については、「コマンドラインを使用したインストール」を参照してください。

ステップ 1. 製品ソフトウェアをダウンロードしてウィザードを起動する

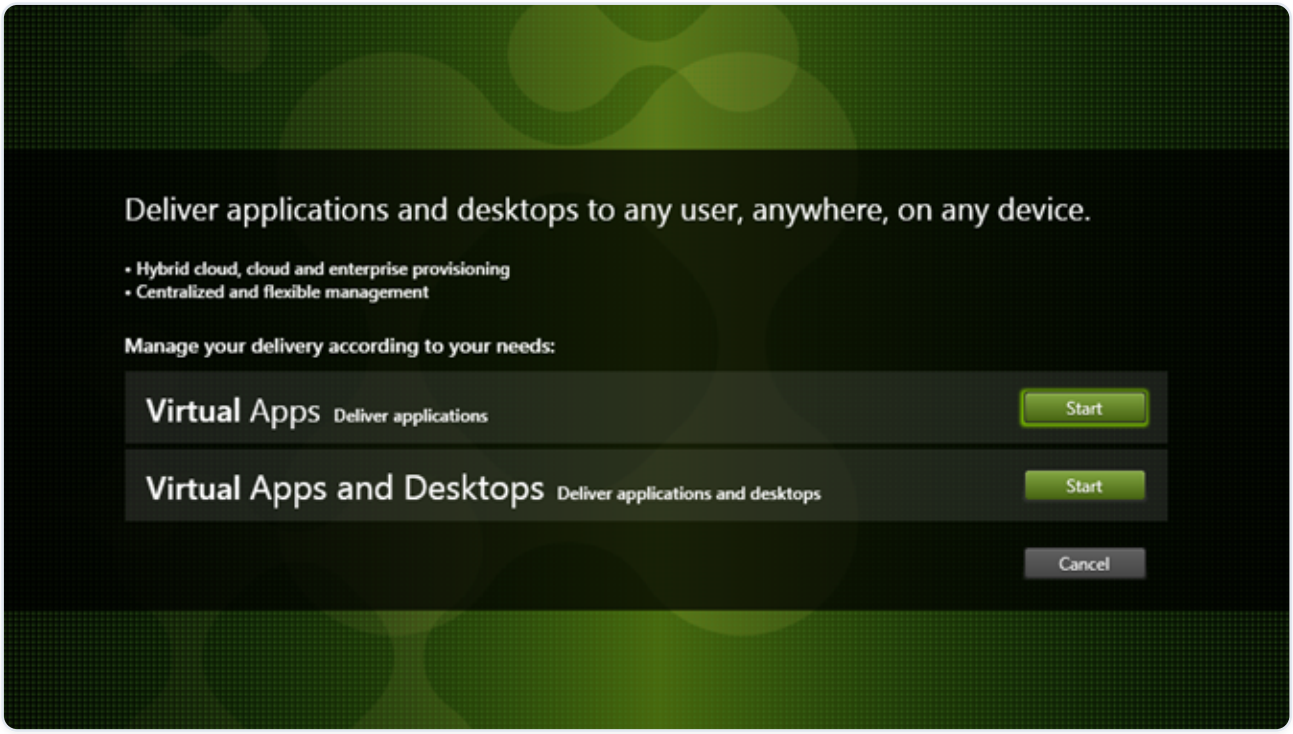
Citrix アカウントの資格情報を使用して、Citrix Virtual Apps and Desktops™ のダウンロードページにアクセスします。製品の ISO ファイルをダウンロードします。

ファイルを解凍します。必要に応じて、ISO ファイルを DVD に書き込みます。

コアコンポーネントをインストールするマシンに、ローカル管理者アカウントを使用してログオンします。

DVD をドライブに挿入するか、ISO ファイルをマウントします。インストーラーが自動的に起動しない場合は、**AutoSelect** アプリケーションまたはマウントされたドライブをダブルクリックします。

ステップ 2. インストールする製品を選択する



インストールする製品 (Virtual Apps または Virtual Apps and Desktops) の横にある **Start** をクリックします。

(マシンにCitrix Virtual Apps and Desktopsコンポーネントがすでにインストールされている場合、このページは表示されません。)

コマンドラインオプション: Citrix Virtual Apps をインストールするには `/xenapp` を使用します。このオプションを省略すると、Citrix Virtual Apps and Desktops がインストールされます。

ステップ 3. インストールするものを選択する

コンポーネントインストーラーのコンポーネント選択ページ(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/what-to-install-2.png)

初めて使用する場合は、**Delivery Controller** を選択します。(後のページで、このマシンにインストールする特定のコンポーネントを選択します。)

コントローラーをすでにインストールしている場合 (このマシンまたは別のマシンに)、別のコンポーネントをインストールするには、**展開の拡張**セクションからコンポーネントを選択します。

コマンドラインオプション: `/components`

ステップ 4. ライセンス契約を読んで同意する

コンポーネントインストーラーのライセンス契約ページ(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/core-license-75.png)

ライセンス契約ページで、ライセンス契約を読んだ後、内容を読んで同意したことを示します。次に、**次へ**をクリックします。

ステップ 5. インストールするコンポーネントとインストール場所を選択する

コンポーネントインストーラーのコアコンポーネントページ(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/core-components-75.png)

コアコンポーネントページで:

- **場所:** デフォルトでは、コンポーネントは`C:\Program Files\Citrix`にインストールされます。ほとんどの展開では、デフォルトで問題ありません。別の場所を指定する場合、その場所にはネットワークサービスに対する実行権限が必要です。
- **コンポーネント:** デフォルトでは、すべてのコアコンポーネントのチェックボックスが選択されています。すべてのコアコンポーネントを1つのサーバーにインストールすることは、概念実証、テスト、または小規模な本番展開には問題ありません。大規模な本番環境では、CitrixはDirector、StoreFront、およびLicense Serverを個別のサーバーにインストールすることを推奨します。

> **注：**
>
> 複数のサーバーにコンポーネントをインストールする場合は、他のサーバーに他のコンポーネントをインストールする前に、Citrix License Server とライセンスを最初にインストールしてください。ガイダンスについては、Citrix Virtual Apps and Desktops のライセンスガイド の「自動インストール」セクションを参照してください。

> このマシンに必須のコアコンポーネントをインストールしないことを選択すると、アイコンで警告が表示されます。この警告は、そのコンポーネントをインストールする必要があることを通知しますが、必ずしもこのマシンにインストールする必要があるわけではありません。

Nextをクリックします。

コマンドラインオプション: `/installdir`、`/components`、`/exclude`

ハードウェアチェック

Delivery Controller をインストールまたはアップグレードすると、ハードウェアがチェックされます。マシンに推奨される RAM 容量 (5 GB) より少ない場合、インストーラーは警告を表示します。これはサイトの安定性に影響を与える可能性があります。詳細については、「ハードウェア要件」を参照してください。

グラフィカルインターフェイス: ダイアログボックスが表示されます。

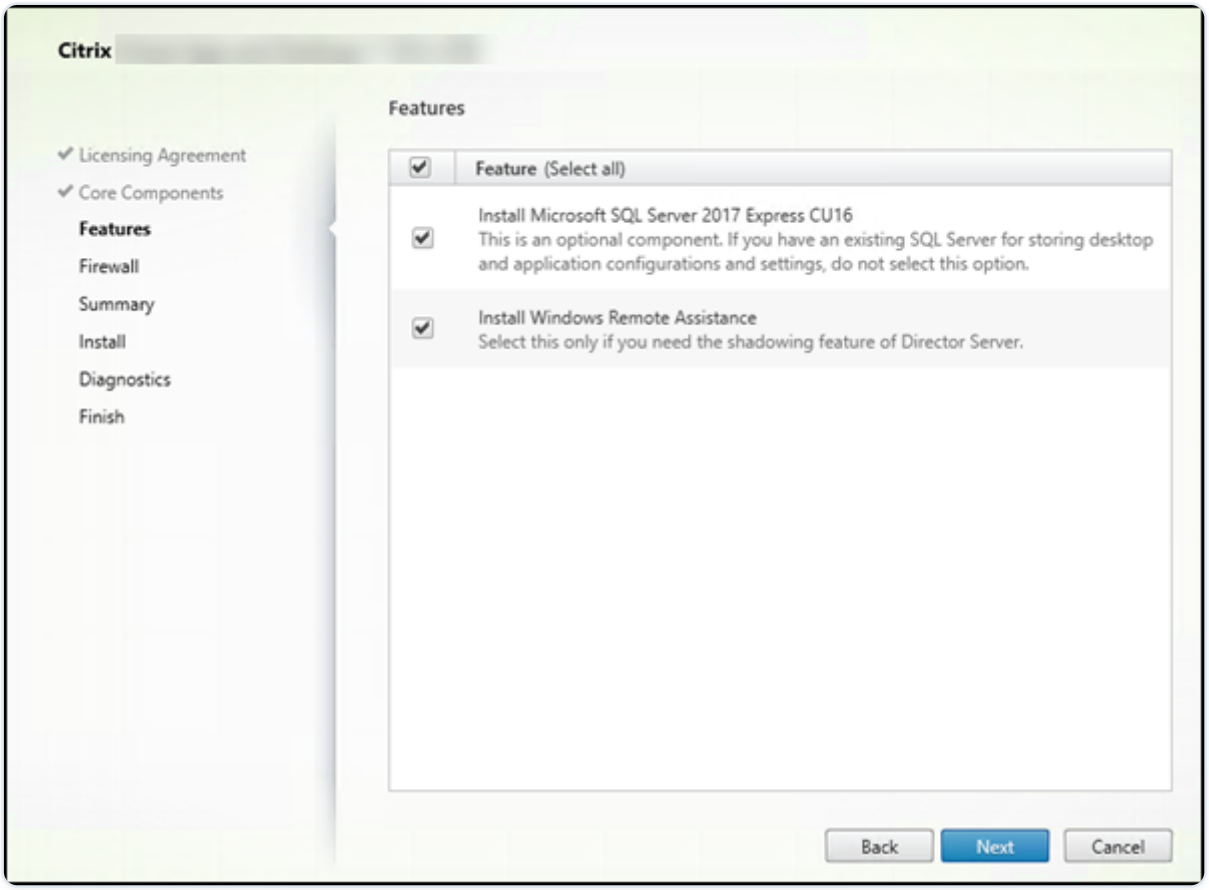
- 推奨: **キャンセル** をクリックしてインストールを停止します。マシンに RAM を追加してから、再度インストールを開始します。
- または、**次へ** をクリックしてインストールを続行します。サイトで安定性の問題が発生する可能性があります。

コマンドラインインターフェイス: インストール/アップグレードが終了します。インストールログには、検出された内容と利用可能なオプションを説明するメッセージが含まれています。

- 推奨: マシンに RAM を追加してから、再度コマンドを実行します。
- または、`/ignore_hw_check_failure` オプションを指定してコマンドを再度実行し、警告を上書きします。サイトで安定性の問題が発生する可能性があります。

アップグレード時には、OS または SQL Server のバージョンがサポートされなくなった場合にも通知されます。詳細については、「展開のアップグレード」を参照してください。

手順 6. 機能の有効化または無効化



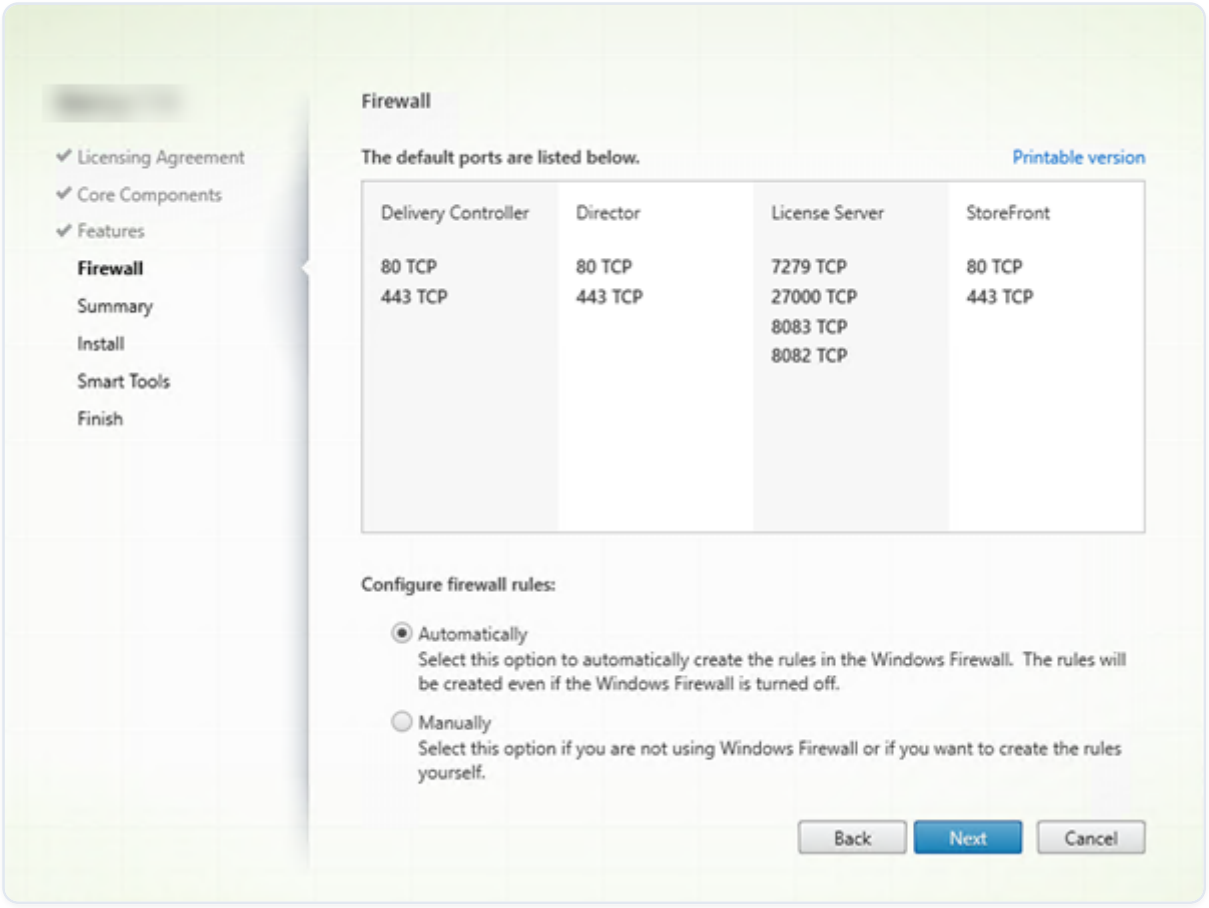
機能ページで:

- サイトデータベースとして使用するMicrosoft SQL Server Expressをインストールするかどうかを選択します。デフォルトでは、この選択は有効になっています。Citrix Virtual Apps and Desktopsデータベースに慣れていない場合は、データベースを確認してください。
- Directorをインストールすると、Windowsリモートアシスタンスが自動的にインストールされます。Directorのユーザーシャドウイングで使用するために、Windowsリモートアシストでシャドウイングを有効にするかどうかを選択します。シャドウイングを有効にすると、TCPポート3389が開きます。デフォルトでは、この機能は有効になっています。ほとんどの展開では、デフォルト設定で問題ありません。この機能は、Directorをインストールしている場合にのみ表示されます。

Nextをクリックします。

コマンドラインオプション: `/nosql` (インストールを防止するため)、`/no_remote_assistance` (有効化を防止するため)

手順7. Windowsファイアウォールポートを開く



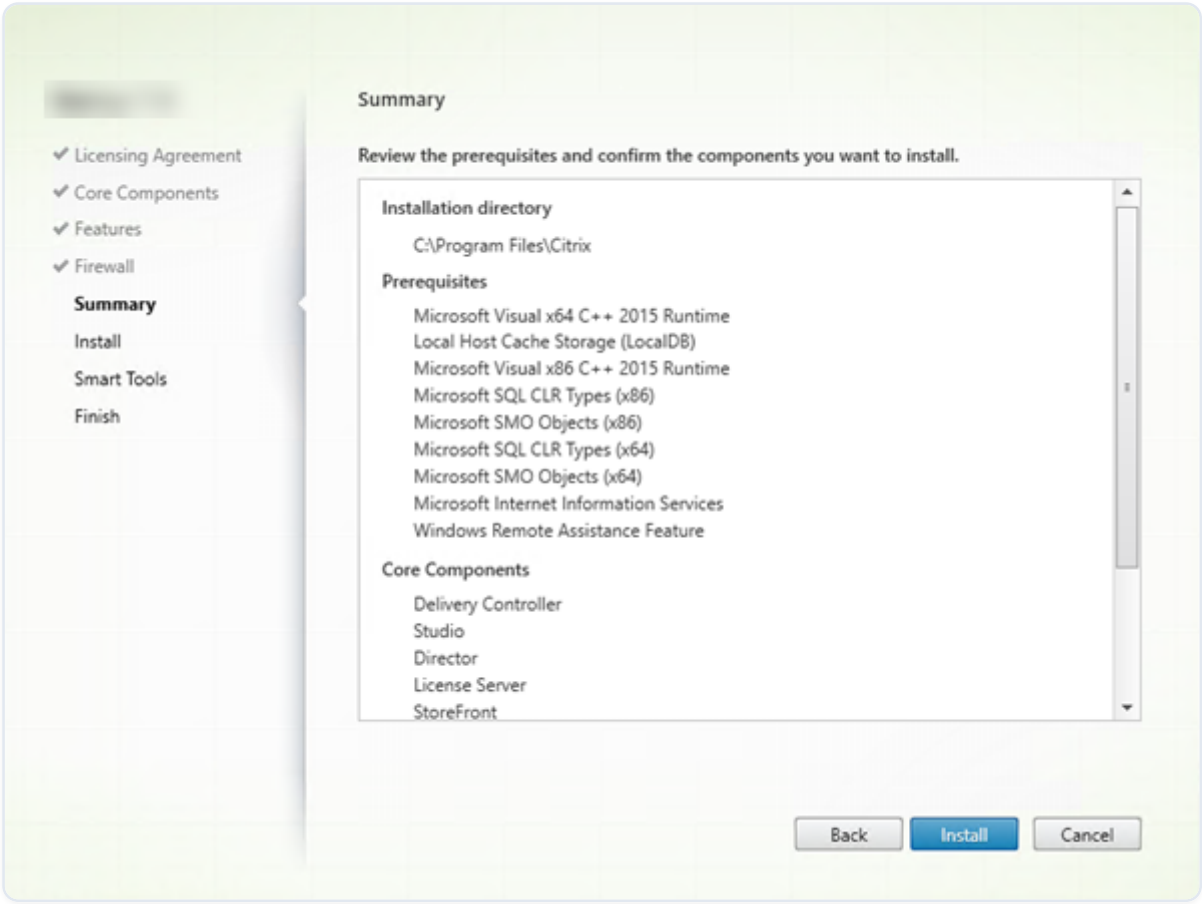
デフォルトでは、Windowsファイアウォールサービスが実行されている場合、ファイアウォールが有効になっていなくても、**ファイアウォール**ページ上のポートは自動的に開かれます。ほとんどの展開では、デフォルト設定で問題ありません。ポート情報については、ネットワークポートを参照してください。

Nextをクリックします。

(このグラフィックは、このマシンにすべてのコアコンポーネントをインストールしたときのポートリストを示しています。この種のインストールは、通常、テスト展開のみを対象としています。)

コマンドラインオプション: `/configure_firewall`

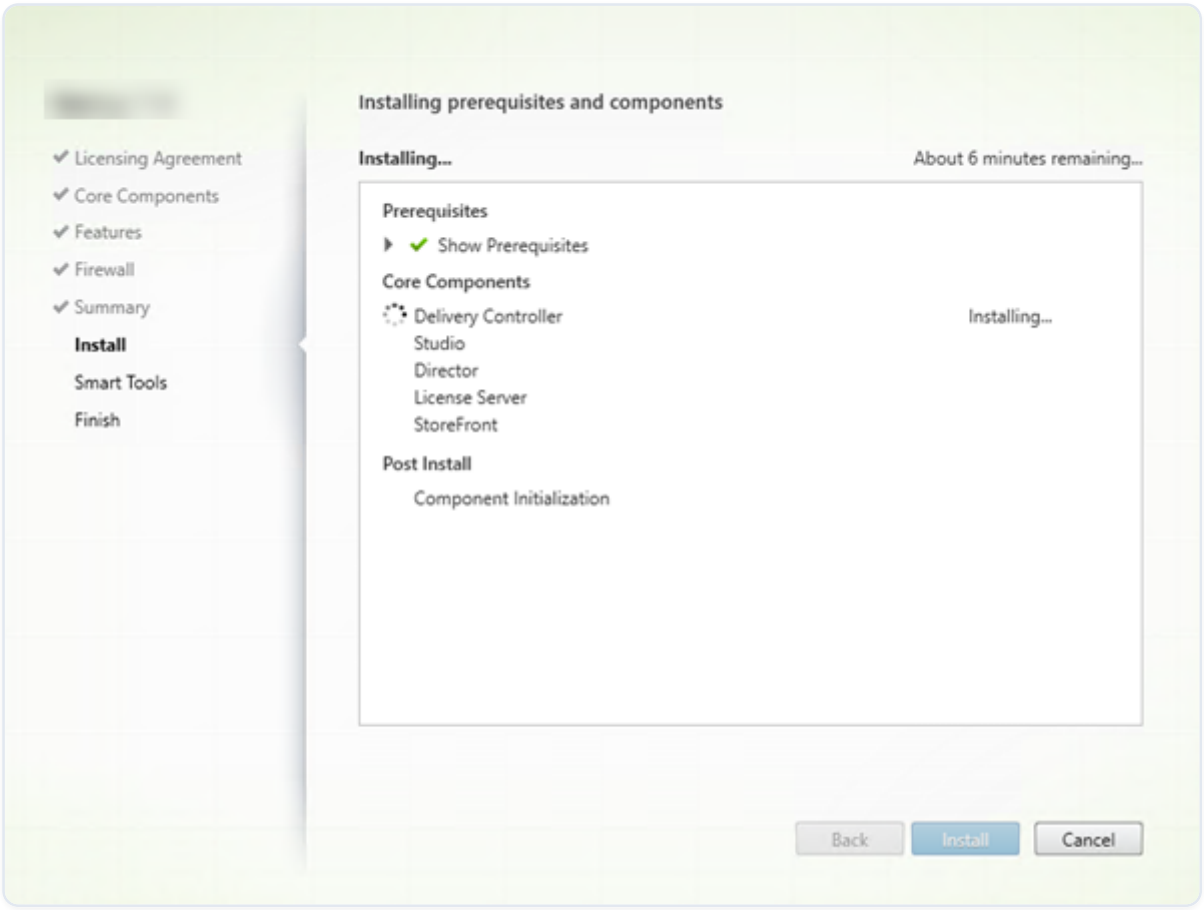
手順8. 前提条件を確認し、インストールを確定する



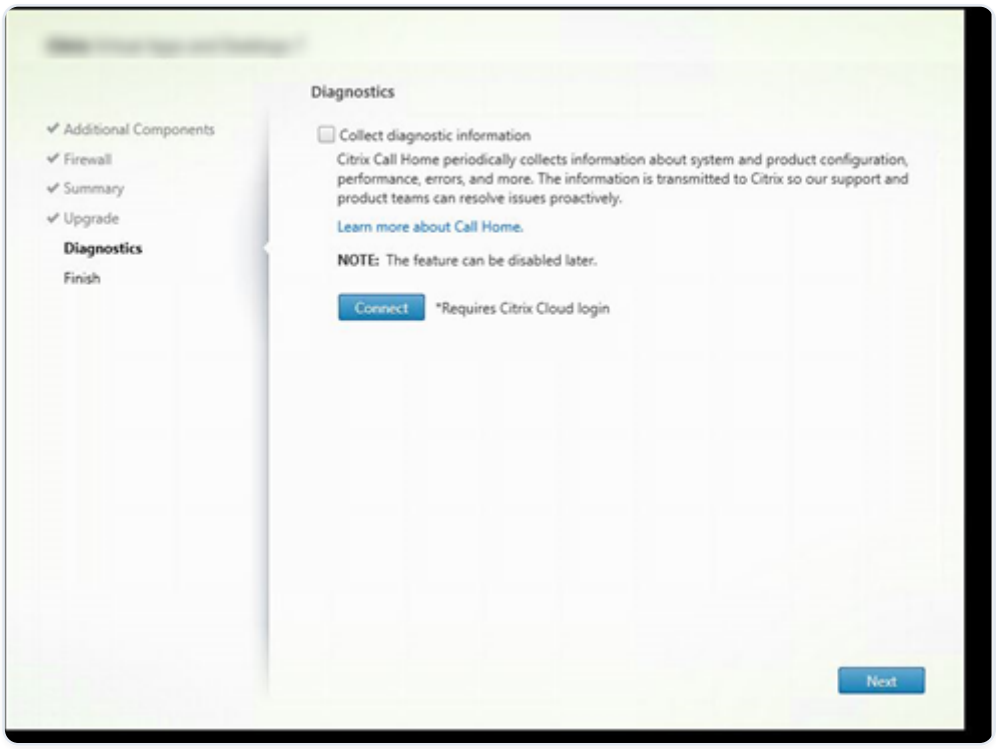
概要ページには、インストールされるものが一覧表示されます。必要に応じて、**戻る**ボタンを使用して以前のウィザードページに戻り、選択を変更します。

準備ができたら、**インストール**をクリックします。

ディスプレイにはインストールの進行状況が表示されます。



ステップ9. 診断



診断ページで、Citrix Call Homeに参加するかどうかを選択します。

このページは、グラフィカルインターフェイスを使用してDelivery Controllerをインストールするときに表示されます。StoreFrontをインストールする場合（ただしControllerではない場合）、ウィザードはこのページを表示します。その他のコアコンポーネントをインストールする場合（ただしControllerまたはStoreFrontではない場合）、ウィザードはこのページを表示しません。

アップグレード中に、Call Homeがすでに有効になっている場合、またはインストーラーがCitrix Telemetry Serviceに関連するエラーを検出した場合、このページは表示されません。

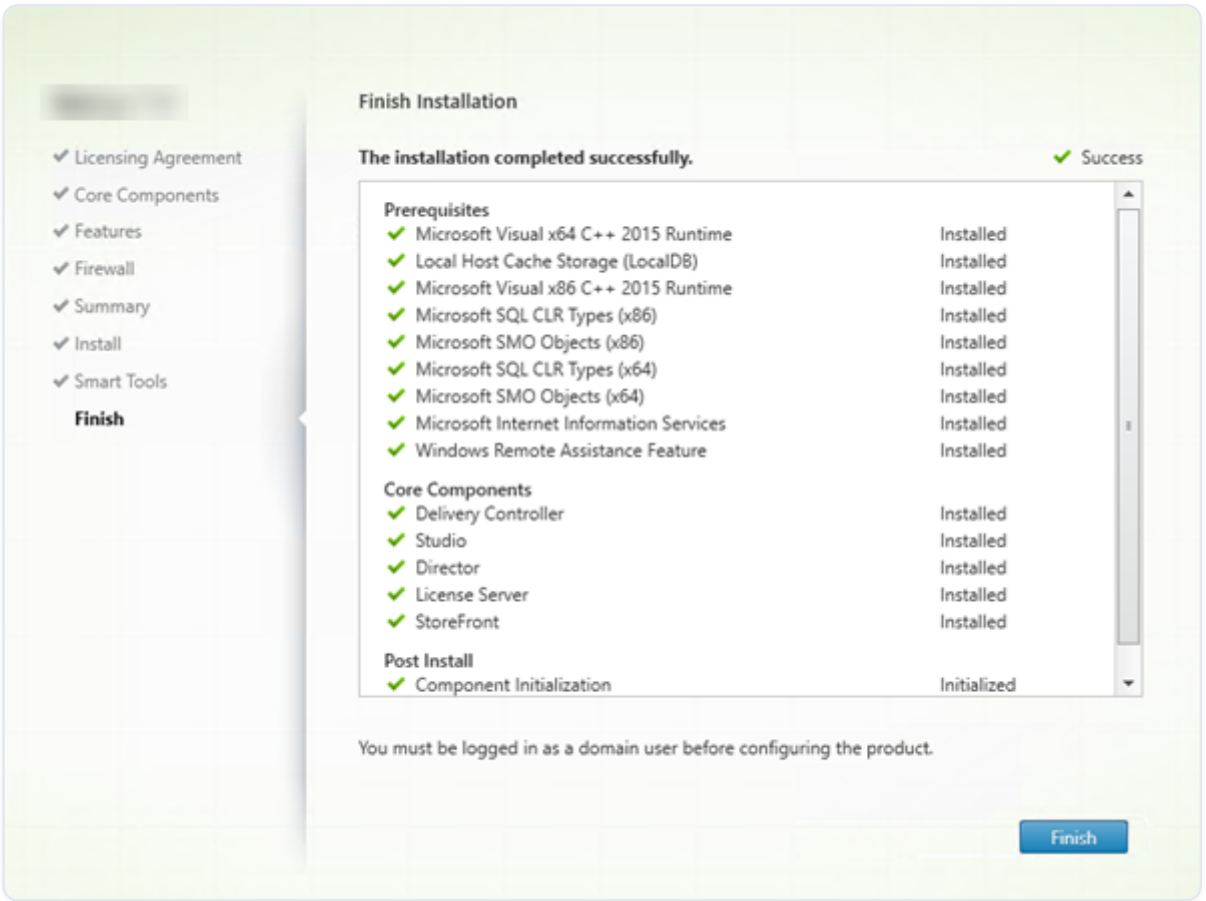
参加することを選択した場合（デフォルト）、**接続**をクリックします。プロンプトが表示されたら、Citrixアカウントの資格情報を入力します。登録の選択は、インストール後に変更できます。

資格情報が検証された後（または参加しないことを選択した場合）、**次へ**をクリックします。

診断ページで、最初に**診断情報の収集**を選択せずに**接続**をクリックした場合、**Citrix Insight Servicesに接続**ダイアログを閉じると**次へ**ボタンが無効になります。次のページに進むことはできません。**次へ**ボタンを再度有効にするには、**診断情報の収集**を選択してすぐに選択を解除します。

詳細については、Call Homeを参照してください。

ステップ10. このインストールを完了する



完了ページには、正常にインストールおよび初期化されたすべての前提条件とコンポーネントの緑色のチェックマークが表示されます。

完了をクリックします。

ステップ11. 残りのコアコンポーネントを他のマシンにインストールする

すべてのコアコンポーネントを1台のマシンにインストールした場合は、「次のステップ」に進みます。そうでない場合は、他のマシンでインストーラーを実行して他のコンポーネントをインストールします。他のサーバーにControllerを追加でインストールすることもできます。

次のステップ

必要なすべてのコンポーネントをインストールしたら、Studioを使用してサイトを作成します。

サイトを作成したら、VDAをインストールします。

いつでも、フルプロダクトインストーラーを使用して、以下のコンポーネントで展開を拡張できます。

- **Universal Print Serverサーバーコンポーネント:** プリントサーバーでインストーラーを起動します。

  a. **展開の拡張**セクションで**Universal Print Server**を選択します。

  b. ライセンス契約に同意します。

  c. 「**ファイアウォール**」ページでは、Windowsファイアウォールサービスが実行されている場合、ファイアウォールが有効になっていない場合でも、デフォルトでTCPポート7229および8080がファイアウォールで開かれます。ポートを手動で開きたい場合は、このデフォルトのアクションを無効にできます。

  このコンポーネントをコマンドラインからインストールするには、「Universal Print Serverをインストールするためのコマンドラインオプション」を参照してください。
- 「フェデレーション認証サービス」。
- 「セッション録画」。

VDAのインストール

> **重要:**

> アップグレード中で、現在のバージョンにPersonal vDiskまたはAppDisksソフトウェアがインストールされている場合は、PvD、AppDisks、およびサポートされていないホストの削除を参照してください。

> Windowsマシン用のVDAには、マルチセッションOS用VDAとシングルセッションOS用VDAの2種類があります。(Linuxマシン用VDAについては、Linux Virtual Delivery Agentドキュメントを参照してください。)

インストールを開始する前に、インストールの準備を確認し、すべての準備タスクを完了してください。

VDAをインストールする前に、コアコンポーネントをインストールします。VDAをインストールする前にサイトを作成することもできます。

この記事では、VDAをインストールする際のインストールウィザードのシーケンスについて説明します。コマンドラインでの同等の操作も提供されています。詳細については、コマンドラインを使用したインストールを参照してください。

ステップ1. 製品ソフトウェアをダウンロードしてウィザードを起動する

フル製品インストーラーを使用している場合:

1. 製品ISOをまだダウンロードしていない場合:
   - Citrixアカウントの資格情報を使用して、Citrix Virtual Apps and Desktops™ダウンロードページにアクセスします。製品ISOファイルをダウンロードします。
   - ファイルを解凍します。必要に応じて、ISOファイルをDVDに書き込みます。
2. VDAをインストールするイメージまたはマシンで、ローカル管理者アカウントを使用します。DVDをドライブに挿入するか、ISOファイルをマウントします。インストーラーが自動的に起動しない場合は、**AutoSelect**アプリケーションまたはマウントされたドライブをダブルクリックします。

   インストールウィザードが起動します。

スタンドアロンパッケージを使用している場合:

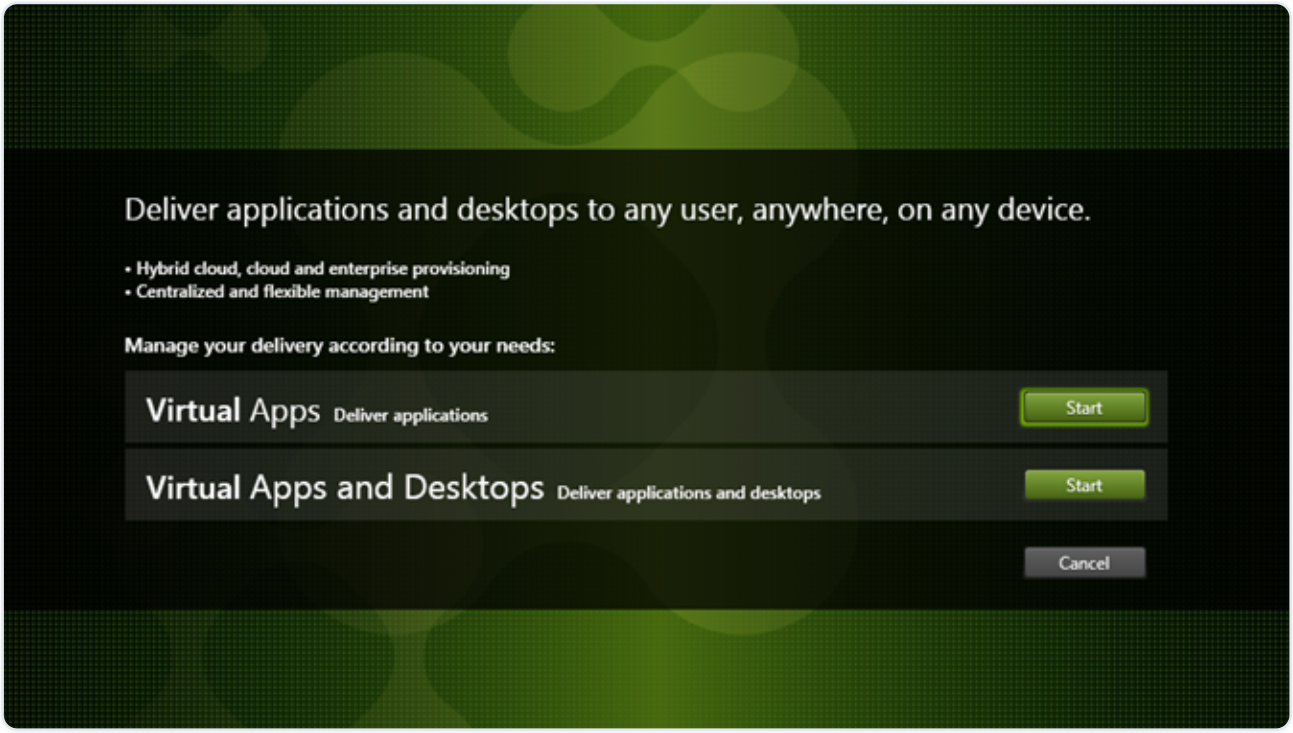
1. Citrixアカウントの資格情報を使用して、Citrix Virtual Apps and Desktopsダウンロードページにアクセスします。適切なパッケージをダウンロードします:
   - `VDAServerSetup.exe`: マルチセッションOS VDA バージョン

- `VDAWorkstationSetup.exe`: シングルセッションOS VDA バージョン
- `VDAWorkstationCoreSetup.exe`: シングルセッションOSコアサービスVDA バージョン

2. パッケージを右クリックし、**管理者として実行**を選択します。

   インストールウィザードが起動します。

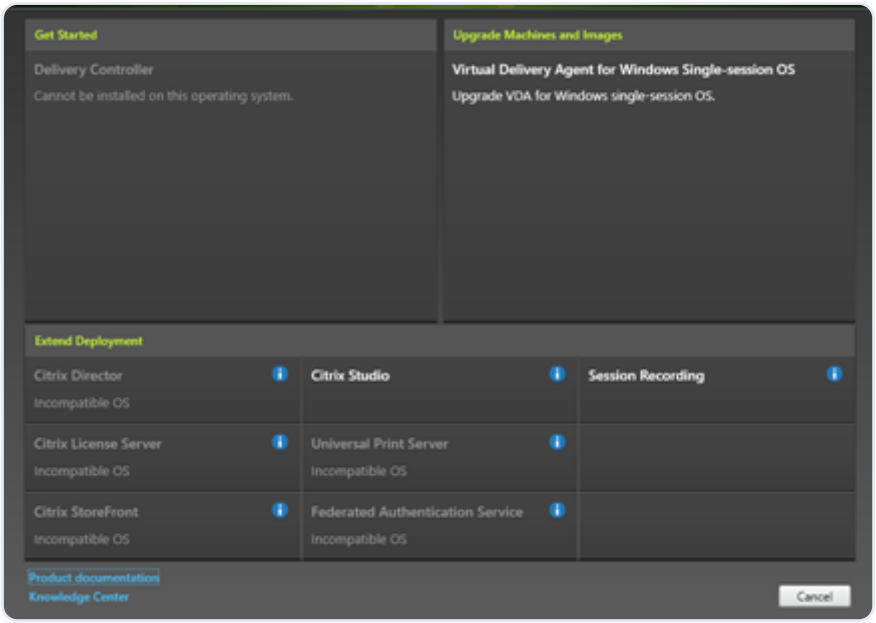
ステップ2. インストールする製品を選択する



インストールする製品（Citrix Virtual AppsまたはCitrix Virtual Desktops）の横にある**開始**をクリックします。（マシンにCitrix Virtual AppsまたはCitrix Virtual Desktopsコンポーネントがすでにインストールされている場合、このページは表示されません。）

コマンドラインオプション: Citrix Virtual Appsをインストールするための`/xenapp`。このオプションが省略された場合、Citrix Virtual Desktopsがインストールされます。

ステップ3. VDAを選択する



Virtual Delivery Agentエントリを選択します。インストーラーは、シングルセッションOSまたはマルチセッションOSのどちらで実行されているかを認識しているため、適切なVDAタイプのみを提供します。

たとえば、Windows Server 2016マシンでインストーラーを実行すると、マルチセッションOS用VDAオプションが利用可能になります。シングルセッションOS用VDAオプションは提供されません。

このCitrix Virtual Apps and Desktopsバージョンでサポートされていないオスに Windows VDAをインストール（またはアップグレード）しようとすると、オプションに関する情報を示すメッセージが表示されます。

ステップ4. VDAの使用方法を指定する

VDAインストーラーの環境ページ(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/vda-ss-environment.png)

環境ページで、VDAの使用方法を指定し、このマシンをより多くのマシンをプロビジョニングするためのイメージとして使用するかどうかを示します。

選択したオプションは、どのCitrix provisioning™ツールが自動的にインストールされるか（もしあれば）、およびVDAインストーラーの「追加コンポーネント」ページのデフォルト値に影響します。

VDAをインストールすると、複数のMSI（プロビジョニング用およびその他）が自動的にインストールされます。これらのインストールを防止する唯一の方法は、コマンドラインインストールで`/exclude`オプションを使用することです。

次のいずれかを選択してください。

- **マスターMCSイメージを作成する:** Machine Creation Services™を使用してVMをプロビジョニングする予定がある場合は、このオプションを選択してVDAをVMイメージにインストールします。このオプションは、Machine Identity Serviceをインストールします。これがデフォルトのオプションです。

  コマンドラインオプション: `/mastermcsimage` または `/masterimage`

> **重要:**
>
> インストールメディアまたはISOイメージはローカルにマウントする必要があります。ソフトウェアのインストールを目的として、ネットワークドライブからISOイメージをマウントすることはサポートされていません。

- **Citrix Provisioningまたはサードパーティのプロビジョニングツールを使用してマスターイメージを作成する:** Citrix Provisioningまたはサードパーティのプロビジョニングツール（Microsoft System Center Configuration Managerなど）を使用してVMをプロビジョニングする予定がある場合は、このオプションを選択してVDAをVMイメージにインストールします。

  コマンドラインオプション: `/masterpvsimage`

- （マルチセッションOSマシンでのみ表示）**サーバーへの仲介接続を有効にする:** このオプションを選択すると、他のマシンをプロビジョニングするためのイメージとして使用されない物理または仮想マシンにVDAがインストールされます。

  コマンドラインオプション: `/remotepc`

- （シングルセッションOSマシンでのみ表示）**Remote PC Accessを有効にする:** Remote PC Accessで使用する物理マシンにVDAをインストールするには、このオプションを選択します。

  コマンドラインオプション: `/remotepc`

Nextをクリックします。

このページは表示されません。

- VDAをアップグレードする場合
- `VDAWorkstationCoreSetup.exe` インストーラーを使用している場合

ステップ5. インストールするコンポーネントとインストール場所を選択します

VDAインストーラーのコアコンポーネントページ(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/vda-ss-core-components.png)

コアコンポーネントページで:

- **場所:** デフォルトでは、コンポーネントは`C:\Program Files\Citrix`にインストールされます。このデフォルトはほとんどの展開で問題ありません。別の場所を指定する場合、その場所にはネットワークサービスに対する実行権限が必要です。
- **コンポーネント:** デフォルトでは、Citrix Workspaceアプリ for WindowsはVDAと一緒にインストールされません。`VDAWorkstationCoreSetup.exe`インストーラーを使用している場合、Citrix Workspaceアプリ for Windowsはインストールされないため、このチェックボックスは表示されません。

Nextをクリックします。

コマンドラインオプション: VDAとCitrix Workspaceアプリ for Windowsをインストールするには、`/installdir`、`/components vda,plugin`

ステップ6. 追加コンポーネントをインストールします

VDAインストーラーの追加コンポーネントページ(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/vda-ss-addtnl-components.png)

追加コンポーネントページには、VDAとともに他の機能やテクノロジーのインストールを有効または無効にするためのチェックボックスが含まれています。コマンドラインインストールでは、`/exclude`または`/includeadditional`オプションを使用して、利用可能なコンポーネントを明示的に除外または含めることができます:

- **/includeadditional** "*コンポーネント*"\["*コンポーネント*"\] ...
- **/除外** "*コンポーネント*"\["*コンポーネント*"\] ...

次の表は、このページの項目のデフォルト設定を示しています。デフォルト設定は、「**環境**」ページで選択したオプションによって異なります。

追加コンポーネントページ	環境ページ：「MCS を使用したマスターイメージ」または「CITRIX PROVISIONING を使用したマスターイメージ」が選択されている場合	環境ページ：「サーバーへの仲介接続を有効にする」（マルチセッションOSの場合）または「リモートPCアクセス」（シングルセッションOSの場合）が選択されている場合
ワークスペース環境管理™	選択されていません	選択されていません
Citrix App-V 用パーソナライゼーション	選択されていません	選択されていません
ユーザーパーソナライゼーションレイヤー	選択されていません	このユースケースでは無効なため表示されません。
Citrixサポートツール	選択済み	選択されていません
Citrix プロファイル管理	選択済み	選択されていません
Citrix プロファイル管理 WMI プラグイン	選択済み	選択されていません
Citrix VDA アップグレードエージェント	選択されていません	選択されていません
ウィンドウズ版 Citrix Files	選択されていません	選択されていません
Citrix Outlook 用ファイル	選択されていません	選択されていません
ストレージ最適化のためのMCSIO書き込みキャッシュ	選択されていません	選択されていません
Rendezvousプロトコル構成	選択されていません	選択されていません

このページは、次の場合には表示されません。

- `VDAWorkstationCoreSetup.exe` インストーラーを使用している場合。また、追加コンポーネントのコマンドラインオプションは、そのインストーラーでは無効です。
- VDA をアップグレードしていて、すべての追加コンポーネントがすでにインストールされている場合。一部の追加コンポーネントがすでにインストールされている場合、そのページにはインストールされていないコンポーネントのみが表示されます。

次のチェックボックスをオンまたはオフにします。(コンポーネントはインストーラーで異なる順序で表示される場合があります。)

- **Workspace Environment Management:** 展開でCitrix Workspace Environment Managementを使用している場合は、このコンポーネントをインストールします。詳細については、Workspace Environment Managementを参照してください。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix WEM Agent"`、コンポーネントのインストールを防止するには `/exclude "Citrix WEM Agent"`

- **Citrix Personalization for App-V:** Microsoft App-Vパッケージのアプリケーションを使用する場合、このコンポーネントをインストールします。詳細については、「App-V」を参照してください。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Personalization for App-V – VDA"`、コンポーネントのインストールを無効にするには `/exclude "Citrix Personalization for App-V – VDA"`

- **Citrixユーザーパーソナライゼーションレイヤー:** ユーザーパーソナライゼーションレイヤー用のMSIをインストールします。詳細については、「ユーザーパーソナライゼーションレイヤー」を参照してください。

  このコンポーネントは、シングルセッションのWindows 10マシンにVDAをインストールする場合にのみ表示されます。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "User Personalization Layer"`、コンポーネントのインストールを無効にするには `/exclude "User Personalization Layer"`

- **Citrix Supportability Tools** Citrix Health AssistantなどのCitrixサポートツールを含むMSIをインストールします。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Supportability Tools"`、コンポーネントのインストールを無効にするには `/exclude "Citrix Supportability Tools"`

- **Citrix Profile Management:** このコンポーネントは、ユーザープロファイル内のユーザーパーソナライゼーション設定を管理します。詳細については、「Profile Management」を参照してください。

Citrix Profile Managementをインストールから除外すると、Citrix DirectorによるVDAの監視とトラブルシューティングに影響します。**ユーザーの詳細**ページと**エンドポイント**ページでは、**パーソナライゼーション**パネルと**ログオン期間**パネルが機能しません。**ダッシュボード**ページと**傾向**ページでは、**平均ログオン期間**パネルはProfile Managementがインストールされているマシンのみのデータを表示します。

サードパーティのユーザープロファイル管理ソリューションを使用している場合でも、Citrixは Citrix Profile Management Serviceをインストールして実行することをお勧めします。Citrix Profile Management Serviceを有効にする必要はありません。

コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Profile Management"`、コンポーネントのインストールを無効にするには `/exclude "Citrix Profile Management"`

- **Citrix Profile Management WMIプラグイン:** このプラグインは、WMI (Windows Management Instrumentation) オブジェクト (プロファイルプロバイダー、プロファイルの種類、サイズ、ディスク使用量など) でProfile Managementのランタイム情報を提供します。WMIオブジェクトは、Directorにセッション情報を提供します。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Profile Management WMI Plugin"`、コンポーネントのインストールを無効にするには `/exclude "Citrix Profile Management WMI Plugin"`

- **VDAアップグレードエージェント:** Citrix DaaS（旧Citrix Virtual Apps and Desktopsサービス）の展開にのみ適用されます。VDAがVDAアップグレード機能に参加できるようにします。この機能を使用して、管理コンソールからカタログのVDAを即座に、またはスケジュールされた時間にアップグレードできます。このエージェントがインストールされていない場合、マシン上でVDAインストーラーを実行することでVDAをアップグレードできます。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix VDA Upgrade Agent"`、コンポーネントのインストールを無効にするには `/exclude "Citrix VDA Upgrade Agent"`

- **Citrix Files for Windows:** このコンポーネントにより、ユーザーはCitrix Filesアカウントに接続できます。その後、Windowsファイルシステム内のマップされたドライブを介してCitrix Filesとやり取りできます（コンテンツの完全な同期は不要です）。詳細については、「Content Collaboration」を参照してください。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Files for Windows"`、コンポーネントのインストールを無効にするには `/exclude "Citrix Files for Windows"`

- **Citrix Files for Outlook:** Citrix Files for Outlookを使用すると、ファイルサイズの制限を回避し、Citrix Filesを介して添付ファイルやメールを送信することで、セキュリティを追加できます。同僚、顧客、パートナー向けに、メールで直接安全なファイルアップロードリクエストを提供できます。詳細については、「Content Collaboration」を参照してください。

  コマンドラインオプション: コンポーネントのインストールを有効にするには`/includeadditional "Citrix Files for Outlook"`、コンポーネントのインストールを無効にするには`/exclude "Citrix Files for Outlook"`

- **ストレージ最適化用MCSIOライトキャッシュ:** Citrix MCS IOドライバーをインストールします。詳細については、「ハイパーバイザーで共有されるストレージ」および「一時データ用のキャッシュの構成」を参照してください。

  コマンドラインオプション: コンポーネントのインストールを有効にするには`/includeadditional "Citrix MCS IODriver"`、コンポーネントのインストールを無効にするには`/exclude "Citrix MCS IODriver"`

- **Rendezvous Proxy Configuration:** このコンポーネントは、環境内でCitrix Gateway ServiceとRendezvousプロトコルを使用する予定があり、ネットワークにアウトバウンド接続用の非透過型プロキシがある場合にインストールします。HTTPプロキシのみがサポートされています。

  このコンポーネントをインストールする場合は、**Rendezvousプロキシ構成**ページでプロキシのアドレスまたはPACファイルのパスを指定します。機能の詳細については、「Rendezvousプロトコル」を参照してください。

  コマンドラインオプション: コンポーネントのインストールを有効にするには`/includeadditional "Citrix Rendezvous V2"`、コンポーネントのインストールを防止するには`/exclude "Citrix Rendezvous V2"`

ステップ7. ワークスペース環境管理

Workspace Environment Management (WEM) ページは、**追加コンポーネント**ページで対応するチェックボックスを有効にした場合にのみ表示されます。

1. WEMオンプレミス展開とWEMクラウド（サービス）展開のどちらを使用するかを選択します。
2. FQDNまたはIPアドレスを追加します。特殊文字は無視されます。
   - WEMオンプレミスの場合: WEMインフラストラクチャサーバーのアドレス

VDAインストーラーでWEMインフラストラクチャサーバーを指定する(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/vda-wem-infra-server.png)

> **注：**
>
> WEMサーバー接続をテストすると、次のエラーメッセージが表示されることがあります: `Unable to establish connection with "<the address you entered>"` 。アドレスが正しく、サーバーに接続できる場合は、このメッセージを無視できます。

- WEMサービスの場合: Cloud Connectorのアドレス

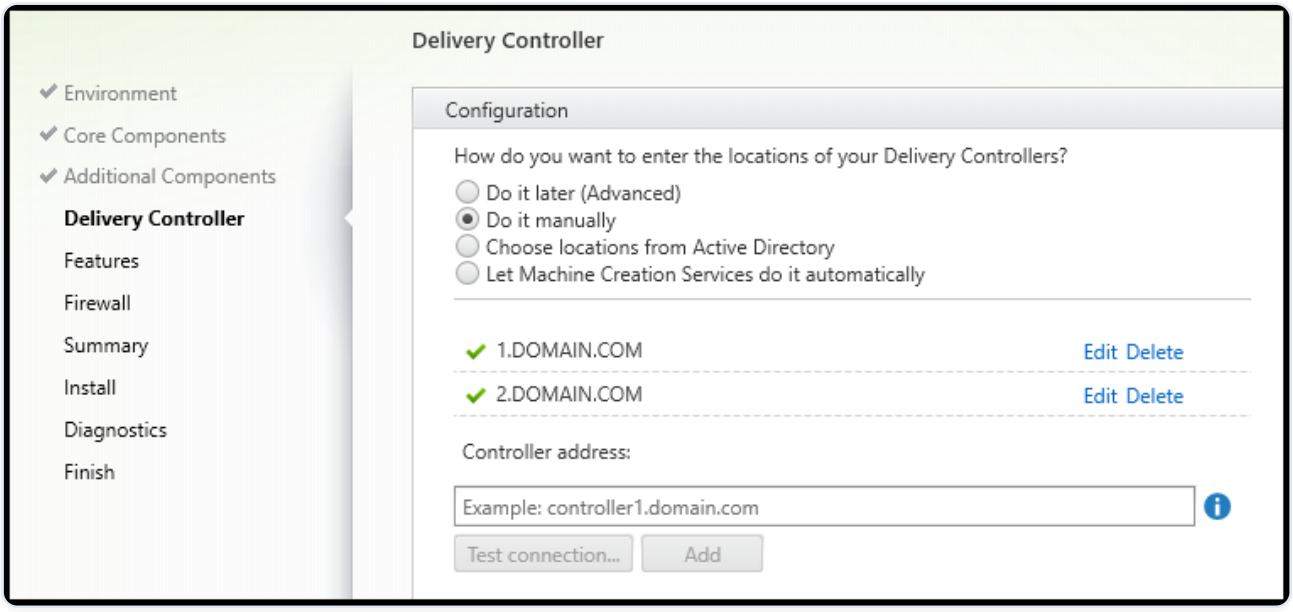
  VDAインストーラーでWEMのCloud Connectorを指定する(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/vda-wem-connectors.png)

3. **接続テスト**をクリックします。ポートはファイアウォールで開いている必要があります。
4. 接続テストが成功したら、**追加**をクリックします。
5. WEMサービス展開の場合、他のCloud Connectorについても手順2〜4を繰り返します。
6. **Next**をクリックします。

コマンドラインオプション: `/wem_server` 、 `/wem_cloud_connectors`

コマンドラインインターフェイスでは、WEMエージェントの構成オプションがさらに利用可能です。(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/install-configure/install-command.html#command-line-options-for-installing-a-vda)を参照してください。

手順8. Delivery Controller™のアドレス



Delivery Controllerページで、インストールされているControllerのアドレスを入力する方法を選択します。Citrixでは、VDAのインストール中にアドレスを指定することをお勧めします（**手動で実行**）。VDAは、この情報がないとControllerに登録できません。VDAが登録できない場合、ユーザーはそのVDA上のアプリケーションやデスクトップにアクセスできません。

- **手動で実行:**（デフォルト）インストールされているControllerのFQDNを入力し、**追加**をクリックします。複数のControllerをインストールしている場合は、それらのアドレスを追加します。
- **後で実行（詳細設定）：** このオプションを選択すると、ウィザードは続行する前にその操作を実行することを確認するよう求めます。アドレスを後で指定するには、インストーラーを再実行するか、Citrixグループポリシーを使用します。ウィザードは、**概要**ページでも通知します。
- **Active Directoryから場所を選択:** マシンがドメインに参加しており、ユーザーがドメインユーザーである場合にのみ有効です。
- **Machine Creation Servicesに自動的に実行させる:** MCSを使用してマシンをプロビジョニングする場合にのみ有効です。

次へをクリックします。**後で実行（詳細設定）**を選択した場合、Controllerアドレスを後で指定することを確認するプロンプトが表示されます。

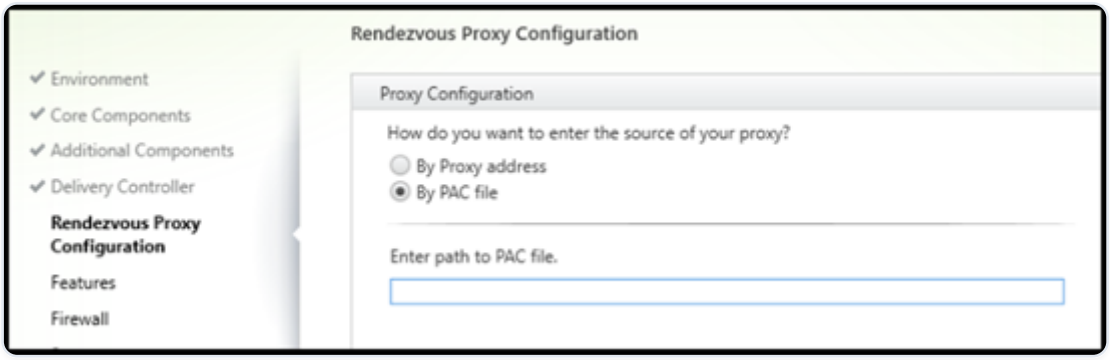
その他の考慮事項:

- アドレスには英数字以外の文字を含めることはできません。
- VDAのインストール中およびグループポリシーでアドレスを指定した場合、ポリシー設定はインストール中に提供された設定を上書きします。

- VDAの登録を成功させるには、Controllerとの通信に使用されるファイアウォールポートが開いている必要があります。このアクションは、ウィザードの**ファイアウォール**ページでデフォルトで有効になっています。
- Controllerの場所を指定した後（VDAのインストール中またはインストール後）、Controllerが追加または削除されたときに、自動更新機能を使用してVDAを更新できます。VDAがControllerを検出して登録する方法の詳細については、「VDA登録」を参照してください。

コマンドラインオプション：`/controllers`

ステップ9. Rendezvousプロキシ構成



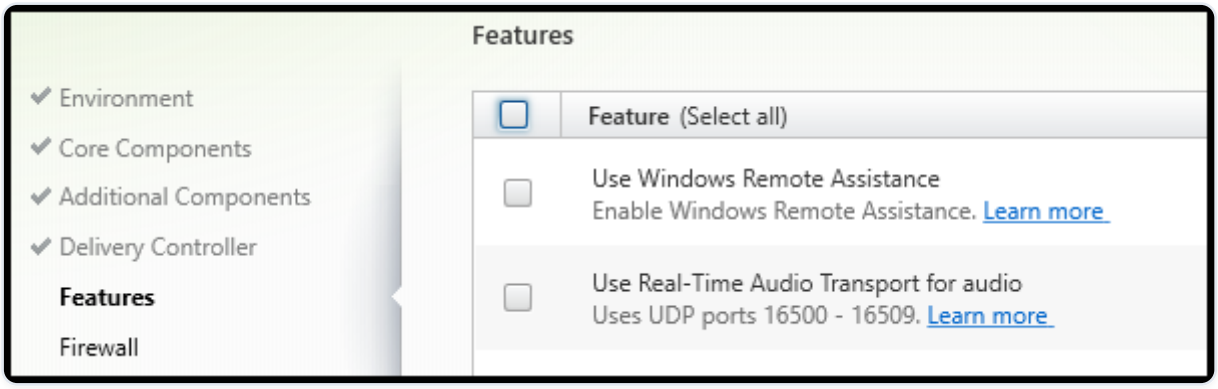
Rendezvousプロキシ構成ページは、**追加コンポーネント**ページで**Rendezvousプロキシ構成**チェックボックスを有効にした場合にのみ表示されます。

1. プロキシソースをプロキシアドレスで指定するか、PACファイルパスで指定するかを選択します。
2. プロキシアドレスまたはPACファイルパスを指定します。
   - プロキシアドレスの形式: `http://<url-or-ip>:<port>`
   - PACファイルの形式: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

接続テストを成功させるには、プロキシポートのファイアウォールが開いている必要があります。プロキシへの接続ができない場合でも、VDAのインストールを続行するかどうかを選択できます。

コマンドラインオプション: `/proxyconfig`

ステップ10. 機能の有効化または無効化



機能ページで、チェックボックスを使用して、使用する機能を有効または無効にします。

- **Windowsリモートアシスタンスの使用：** この機能を有効にすると、Directorのユーザーシャドウ機能でWindowsリモートアシスタンスが使用されます。Windowsリモートアシスタンスは、ファイアウォールで動的ポートを開きます。（デフォルト = 無効）

  コマンドラインオプション: `/enable_remote_assistance`

- **オーディオにリアルタイムオーディオトランスポートを使用:** ネットワークでVoIPが広く使用されている場合は、この機能を有効にします。この機能により、遅延が減少し、損失の多いネットワークでのオーディオの回復性が向上します。UDPトランスポート経由でRTPを使用してオーディオデータを送信できます。(デフォルト = 無効)

  コマンドラインオプション: `/enable_real_time_transport`

- **画面共有を使用:** 有効にすると、画面共有で使用されるポートがWindowsファイアウォールで開かれます。(デフォルト = 無効)

  コマンドラインオプション: `/enable_ss_ports`

- **このVDAはクラウドのVMにインストールされていますか:** この設定は、Citrixがテレメトリ目的でオンプレミスおよびサービス (Citrix Cloud™) VDA展開のリソースの場所を正しく識別するのに役立ちます。この機能は、顧客側の利用には影響しません。展開でCitrix DaaSを使用している場合は、この設定を有効にします (デフォルト = 無効)。

  コマンドラインオプション: `/xendesktopcloud`

このページに**MCS I/O**という機能が含まれている場合、それを使用しないでください。MCS IO機能は、**追加コンポーネント**ページで構成されます。

Nextをクリックします。

ステップ11. ファイアウォールポート

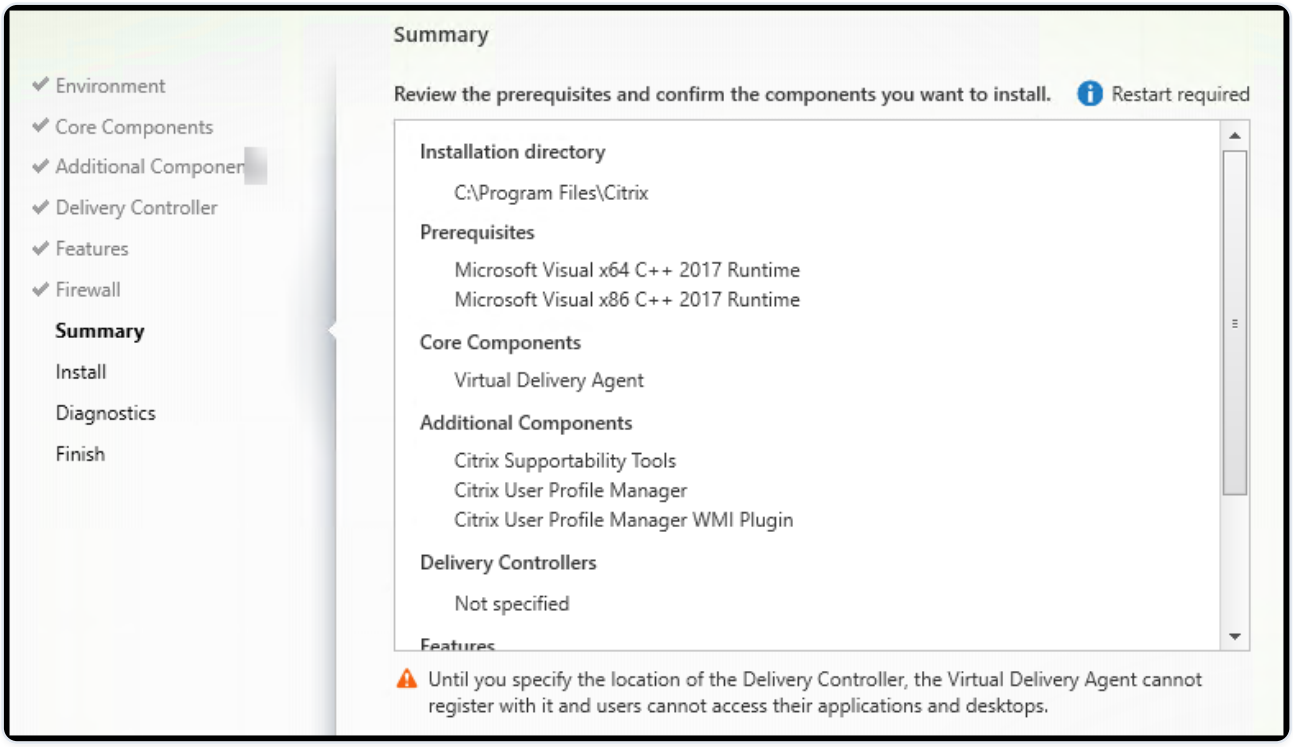


デフォルトでは、**ファイアウォール**ページでWindowsファイアウォールサービスが実行されている場合、ファイアウォールが有効になっていなくてもポートは自動的に開かれます。このデフォルト設定は、ほとんどの展開で問題ありません。ポート情報については、「ネットワークポート」を参照してください。

Nextをクリックします。

コマンドラインオプション: `/enable_hdx_ports`

ステップ12. 前提条件の確認とインストールの確定



概要ページには、インストールされるものが一覧表示されます。**戻る**ボタンを使用して、以前のウィザードページに戻り、選択を変更します。

（シングルセッションVDAのみ）**更新が失敗した場合に自動復元を有効にする**チェックボックスを選択して、障害発生時の復元機能を有効にします。詳細については、(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/install-configure/install-prepare.html#restore-on-install-or-upgrade-failure)を参照してください。

準備ができたら、**インストール**をクリックします。

前提条件がまだインストールまたは有効になっていない場合、マシンは1回以上再起動する可能性があります。(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/install-configure/install-prepare.html)を参照してください。

ステップ13. 診断

VDAインストーラーの診断ページ(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/vda-ss-diagnostics.png)

診断ページで、Citrix Call Homeに参加するかどうかを選択します。参加することを選択した場合（デフォルト）、**接続**をクリックします。プロンプトが表示されたら、Citrixアカウントの資格情報を入力します。

資格情報が検証された後（または参加しないことを選択した場合）、**次へ**をクリックします。

フル製品インストーラーを使用している場合、**診断**ページで最初に**診断情報の収集**を選択せずに**接続**をクリックすると、**Citrix Insight Servicesへの接続**ダイアログを閉じた後、**次へ**ボタンが無効になります。次のページに進むことはできません。**次へ**ボタンを再度有効にするには、**診断情報の収集**を選択し、すぐに選択を解除します。

詳細については、(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/manage-deployment/cis.html#citrix-call-home)を参照してください。

ステップ14. このインストールを完了する

VDAインストーラーのインストール完了ページ(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/vda-ss-finish.png)

完了ページには、正常にインストールおよび初期化されたすべての前提条件とコンポーネントの緑色のチェックマークが表示されます。

完了をクリックします。デフォルトでは、マシンは自動的に再起動します。この自動再起動を無効にすることはできますが、マシンが再起動するまでVDAは使用できません。

次のステップ

必要に応じて、上記のプロシージャを繰り返して、他のマシンまたはイメージにVDAをインストールします。

すべてのVDAをインストールしたら、Studioを起動します。まだサイトを作成していない場合、Studioはそのタスクに自動的に誘導します。それが完了すると、Studioはマシンカタログとデリバリーグループの作成に誘導します。参照：

- サイトの作成
- マシンカタログの作成
- 「デリバリーグループの作成」(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/install-configure/delivery-groups-create.html)

シトリックス オプティマイザー

Citrix Optimizerは、Citrix管理者がさまざまなコンポーネントを削除および最適化することでVDAを最適化するのに役立つWindows OS用のツールです。

VDAをインストールし、最終的な再起動を完了した後、Citrix Optimizerをダウンロードしてインストールします。「CTX224676」を参照してください。CTXの記事には、ダウンロードパッケージと、Citrix Optimizerのインストールおよび使用方法に関する手順が含まれています。

VDAをカスタマイズする

インストール済みのVDAをカスタマイズするには：

1. Windowsのプログラムの削除または変更機能から、「**Citrix Virtual Delivery Agent**」または「**Citrix Remote PC Access/VDI Core Services VDA**」を選択します。その後、右クリックして「**変更**」を選択します。
2. 「**Virtual Delivery Agent Settingsのカスタマイズ**」を選択します。インストーラーが起動したら、以下を変更できます。

   - Controllerアドレス
   - Controllerに登録するTCP/IPポート（デフォルト = 80）
   - Windowsファイアウォールポートを自動的に開くかどうか

トラブルシューティング

- Citrixがコンポーネントインストールの結果を報告する方法については、「Citrixインストールのリターンコード」を参照してください。
- デリバリーグループのStudio表示では、**詳細**ペインの**インストール済みVDAバージョン**エントリが、マシンにインストールされているバージョンと異なる場合があります。マシンのWindowsのプログラムと機能の表示には、実際のVDAバージョンが表示されます。
- VDAがインストールされても、Delivery Controllerに登録されるまでは、ユーザーにアプリやデスクトップを配信できません。

  VDA登録方法と登録問題のトラブルシューティング方法については、「VDA登録」(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/manage-deployment/vda-registration.html)を参照してください。

コマンドラインを使用したインストール

> **重要:**

> アップグレード中で、現在のバージョンでPersonal vDiskまたはAppDisksソフトウェアが使用されているかインストールされている場合は、「PvD、AppDisks、およびサポートされていないホストの削除」を参照してください。

はじめに

この記事は、Windowsオペレーティングシステムを搭載したマシンにコンポーネントをインストールする場合に適用されます。Linuxオペレーティングシステム用VDAについては、「Linux Virtual Delivery Agent」を参照してください。

この記事では、製品のインストールコマンドを発行する方法について説明します。インストールを開始する前に、「インストールの準備」を確認してください。この記事には、利用可能なインストーラーの説明が含まれています。

コマンドの実行の進行状況と戻り値を確認するには、元の管理者であるか、「**管理者として実行**」を使用する必要があります。詳しくは、Microsoftのコマンドに関するドキュメントを参照してください。

インストールコマンドを直接使用することに加えて、Active Directory内のマシンにVDAをインストール、アップグレード、または削除するサンプルスクリプトが製品ISOに用意されています。詳しくは、「スクリプトを使用したVDAのインストール」を参照してください。

このCitrix Virtual Apps and Desktopsのバージョンでサポートされていないバージョンにインストールまたはアップグレードしようとすると、オプションに関する情報を示すメッセージが表示されます。「以前のオペレーティングシステム」を参照してください。

Citrixがコンポーネントインストールの結果を報告する方法については、「Citrixインストールのリターンコード」を参照してください。

フル製品インストーラーを使用する

フル製品インストーラーのコマンドラインインターフェイスにアクセスするには：

1. Citrixから製品パッケージをダウンロードします。ダウンロードサイトにアクセスするには、Citrixアカウントの資格情報が必要です。
2. ファイルを解凍します。必要に応じて、ISOファイルをDVDに書き込みます。
3. コンポーネントをインストールするサーバーに、ローカル管理者アカウントを使用してログオンします。
4. DVDをドライブに挿入するか、ISOファイルをマウントします。
5. メディアの `\x64\XenDesktop Setup` ディレクトリから、適切なコマンドを実行します。

   コアコンポーネントをインストールするには: `XenDesktopServerSetup.exe` を実行します。オプションについては、コアコンポーネントのインストール用コマンドラインオプション を参照してください。

VDAをインストールするには: `XenDesktopVDASetup.exe` を実行します。オプションについては、VDAのインストール用コマンドラインオプション を参照してください。

StoreFrontをインストールするには: インストールメディアの `x64 > StoreFront` フォルダーで `CitrixStoreFront-x64.exe` を実行します。

Universal Print Serverをインストールするには: Universal Print Serverのインストール用コマンドラインオプション のガイダンスに従ってください。

Federated Authentication Serviceをインストールするには: Citrixでは、グラフィカルインターフェイスを使用することをお勧めします。

Session Recordingをインストールするには: Session Recording のガイダンスに従ってください。

コアコンポーネントのインストール用コマンドラインオプション

`XenDesktopServerSetup.exe` コマンドを使用してコアコンポーネントをインストールする場合、以下のオプションが有効です。オプションの詳細については、コアコンポーネントのインストール を参照してください。

> **注：**
>
> - コアコンポーネントのインストール用コマンドラインオプションを使用している間は、`/exclude` を使用しないでください。
> - `/components` を使用して1つのコンポーネントをアップグレードすると、他のコンポーネントもアップグレードされる場合があります。これは、異なるコンポーネント間の互換性の問題を回避するためです。
> - 1つのコンポーネントのみをアップグレードする場合は、そのコンポーネントの個別のインストーラーを使用してください。展開のアップグレード を参照してください。

- **/components** *コンポーネント ...*

  インストールまたは削除するコンポーネントのコンマ区切りリスト。有効な値は次のとおりです。

  - `CONTROLLER`: コントローラー
  - `DESKTOPSTUDIO`: スタジオ

- `DESKTOPDIRECTOR`: ディレクター
- `LICENSESERVER`: Citrix ライセンスサーバー

このオプションを省略すると、すべてのコンポーネントがインストールされます（`/remove` オプションも指定されている場合は削除されます）。

（2003より前のリリースでは、有効な値には `STOREFRONT` が含まれていました。バージョン2003以降では、Use the full-product installer で説明されている専用のStoreFrontインストールコマンドを使用してください）。

- **/configure_firewall**

  Windows ファイアウォールサービスが実行されている場合、ファイアウォールが有効になっていなくても、インストールされるコンポーネントが使用するWindows ファイアウォールのすべてのポートを開きます。サードパーティのファイアウォールを使用している場合、またはファイアウォールを使用していない場合は、手動でポートを開く必要があります。

- **/ディスエーブルエクスペリエンスメトリクス**

  インストール、アップグレード、または削除中に収集された分析データがCitrixに自動的にアップロードされるのを防ぎます。

- **/help** または **/h**

  コマンドのヘルプを表示します。

- **/ignore_hw_check_failure**

  ハードウェアチェックが失敗した場合（たとえば、RAM不足のため）でも、Delivery Controllerのインストールまたはアップグレードを続行できるようにします。詳細については、Hardware check を参照してください。

- **/ignore_site_test_failure**

  Controllerのアップグレード中にのみ有効です。通常、サイトテストの失敗は無視され、アップグレードは続行されます。省略された場合（またはfalseに設定された場合）、サイトテストの失敗があると、アップグレードを実行せずにインストーラーが失敗します。デフォルト = false

  アップグレード中に、サポートされていないSQL Serverバージョンが検出された場合、このオプションは無視されます。詳細については、SQL Server version check を参照してください。

- **/installdir** *ディレクトリ*

コンポーネントがインストールされる既存の空のディレクトリ。デフォルト = `c:\Program Files\Citrix`。

- **/logpath パス**

  ログファイルの場所。指定されたフォルダーは存在している必要があります。インストーラーは作成しません。デフォルト = `TEMP%\Citrix\XenDesktop Installer`

- **/no_pending_reboot_check**

  コアコンポーネントのインストールまたはアップグレード時に、マシン上の以前のWindowsインストールからの保留中の再起動のチェックを防止します。

- **/no_remote_assistance**

  Directorのインストール時にのみ有効です。Windowsリモートアシスタンスを使用するユーザーシャドウイング機能を無効にします。

- **再起動なし**

  インストール後の再起動を防止します。（ほとんどのコアコンポーネントでは、再起動はデフォルトで有効になっていません。）

- **再開しない**

  デフォルトでは、インストール中にマシンの再起動が必要な場合、再起動が完了するとインストーラーは自動的に再開します。デフォルトを上書きするには、`/noresume`を指定します。これは、メディアを再マウントする必要がある場合や、自動インストール中に情報を取得したい場合に役立ちます。

- **ノースキューエル**

  ControllerをインストールしているサーバーへのMicrosoft SQL Server Expressのインストールを防止します。このオプションを省略すると、サイトデータベースとして使用するためにSQL Server Expressがインストールされます。

  このオプションは、ローカルホストキャッシュに使用されるSQL Server Express LocalDBのインストールには影響しません。

- **サイレント** または **パッシブ**

  インストール中にユーザーインターフェイスは表示されません。インストールプロセスの唯一の証拠はWindowsタスクマネージャーにあります。このオプションを省略すると、グラフィカルインターフェイスが起動します。

- **/削除**

`/components`オプションで指定されたコアコンポーネントを削除します。

- **/すべて削除**

  インストールされているすべてのコアコンポーネントを削除します。

- **/エクスペリエンスメトリックを送信**

  インストール、アップグレード、または削除中に収集された分析データをCitrixに自動的に送信します。このオプションを省略した場合（または`/disableexperiencemetrics`が指定された場合）、分析データはローカルで収集されますが、自動的には送信されません。

- **一時ディレクトリ** *directory*

  インストール中に一時ファイルを保持するディレクトリ。デフォルト = `c:\Windows\Temp`。

- **ゼナップ**

  Citrix Virtual Apps をインストールします。このオプションを省略すると、Citrix Virtual Apps and Desktops™ がインストールされます。

コアコンポーネントのインストール例

次のコマンドは、サーバーにDelivery Controller™、Studio、Citrix Licensing、およびSQL Server Expressをインストールします。コンポーネント通信に必要なファイアウォールポートは自動的に開かれます。

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components controller,desktopstudio,licenseserver /configure_firewall
```

次のコマンドは、サーバーにCitrix Virtual Apps™ Controller、Studio、およびSQL Server Expressをインストールします。コンポーネント通信に必要なファイアウォールポートは自動的に開かれます。

```
\x64\XenDesktop Setup\\XenDesktopServerSetup.exe /xenapp /components controller,desktopstudio /configure_firewall
```

スタンドアロンVDAインストーラーを使用する

ダウンロードサイトにアクセスするには、Citrixアカウントの資格情報が必要です。インストールを開始する前に、管理者特権を昇格させるか、**管理者として実行**を使用する必要があります。

1. Citrixから適切なパッケージをダウンロードします。

   - マルチセッションOS Virtual Delivery Agent: `VDAServerSetup.exe`

- シングルセッションOS Virtual Delivery Agent: `VDAWorkstationSetup.exe`
- シングルセッションOS Core Services Virtual Delivery Agent: `VDAWorkstationCoreSetup.exe`

2. まず、パッケージから既存のディレクトリにファイルを抽出し、インストールコマンドを実行するか、単にパッケージを実行します。

   ファイルをインストールする前に抽出するには、絶対パスを指定して`/extract`を使用します（例: `.\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia`）。ディレクトリが存在している必要があります。存在しない場合、抽出は失敗します。その後、別のコマンドで、この記事に記載されている有効なオプションを使用して、適切なコマンドを実行します。

   - `VDAServerSetup_XXXX.exe` の場合は、`<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe` を実行します
   - `VDAWorkstationCoreSetup_XXXX.exe` の場合は、`<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopRemotePCSetup.exe` を実行します
   - `VDAWorkstationSetup_XXXX.exe` の場合は、`<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe` を実行します

   ダウンロードしたパッケージを実行するには、その名前（`VDAServerSetup.exe`、`VDAWorkstationSetup.exe`、または`VDAWorkstationCoreSetup.exe`）を実行します。この記事に記載されている有効なオプションを使用してください。

フル製品インストーラーに慣れている場合：

- スタンドアロンの`VDAServerSetup.exe`または`VDAWorkstationSetup.exe`インストーラーを、名前以外はすべて`XenDesktopVdaSetup.exe`コマンドであるかのように実行します。
- `VDAWorkstationCoreSetup.exe` インストーラーは、他のインストーラーで利用できるオプションのサブセットをサポートしているため、異なります。

VDA をインストールするためのコマンドラインオプション

以下のオプションは、次のコマンド（インストーラー）のいずれか、または複数で有効です: `VDAServerSetup_xxxx.exe`、`VDAWorkstationSetup_xxxx.exe`、および `VDAWorkstationCoreSetup_xxxx.exe`。

オプションの詳細については、「VDA のインストール」を参照してください。

- **/コンポーネント** *コンポーネント\[,コンポーネント\]*

  インストールまたは削除するコンポーネントのコンマ区切りリスト。有効な値は次のとおりです。

  - `VDA`: バーチャル デリバリー エージェント
  - `PLUGINS`: Citrix Workspace™ Windows 用アプリ

  VDA と Citrix Workspace app for Windows をインストールするには、`/components vda,plugins` を指定します。

  このオプションを省略すると、VDA のみがインストールされます（Citrix Workspace app はインストールされません）。

  このオプションは、`VDAWorkstationCoreSetup_xxxx.exe` インストーラーを使用する場合は無効です。そのインストーラーでは Citrix Workspace app をインストールできません。

- **/controllers** "*コントローラー\[コントローラー\]*"

  VDA が通信できるコントローラーのスペース区切りの FQDN を、引用符で囲んで指定します。`/site_guid` オプションと `/controllers` オプションの両方を指定しないでください。

- **/ディスエーブルエクスペリエンスメトリクス**

  インストール、アップグレード、または削除中に収集された分析がCitrixに自動的にアップロードされるのを防ぎます。

- **/enable_hdx_ports**

  Windows ファイアウォールサービスが検出された場合、ファイアウォールが有効になっていなくても、VDAおよび有効な機能（Windows リモートアシスタンスを除く）に必要なポートをWindows ファイアウォールで開きます。別のファイアウォールを使用している場合、またはファイアウォールを使用していない場合は、ファイアウォールを手動で構成する必要があります。ポート情報については、ネットワークポートを参照してください。

  HDX アダプティブトランスポートが使用する UDP ポートを開くには、この `/enable_hdx_ports` オプションに加えて、`/enable_hdx_udp_ports` オプションを指定します。

- **/enable_hdx_udp_ports**

  Windows ファイアウォールサービスが検出された場合、ファイアウォールが有効になっていなくても、HDX アダプティブトランスポートが使用する Windows ファイアウォールの UDP

ポートを開きます。別のファイアウォールを使用している場合、またはファイアウォールを使用していない場合は、ファイアウォールを手動で構成する必要があります。ポート情報については、「ネットワークポート」を参照してください。

VDAが使用する追加ポートを開くには、この`/enable_hdx_udp_ports`オプションに加えて、`/enable_hdx_ports`オプションを指定します。

- **/enable_real_time_transport**

  オーディオパケットにUDPを使用するかどうかを有効または無効にします（オーディオ用のリアルタイムオーディオトランスポート）。この機能を有効にすると、オーディオパフォーマンスが向上する可能性があります。Windows ファイアウォールサービスが検出されたときにUDPポートを自動的に開く場合は、`/enable_hdx_ports`オプションを含めます。

- **/enable_remote_assistance**

  Directorで使用するために、Windowsリモートアシスタンスのシャドウイング機能を有効にします。このオプションを指定すると、Windowsリモートアシスタンスはファイアウォールで動的ポートを開きます。

- **/enablerestore** または **/enablerestorecleanup**

  （シングルセッションVDAにのみ有効）VDAのインストールまたはアップグレードが失敗した場合に、復元ポイントへの自動復帰を有効にします。

  インストール/アップグレードが正常に完了した場合：

  - `/enablerestorecleanup`は、インストーラーに復元ポイントを削除するよう指示します。
  - `/enablerestore`は、使用されなかった場合でも、インストーラーに復元ポイントを保持するように指示します。

  詳細については、インストールまたはアップグレードの失敗時の復元を参照してください。

- **/enable_ss_ports**

  Windows ファイアウォールサービスが検出された場合、ファイアウォールが有効になっていなくても、画面共有に必要なポートをWindows ファイアウォールで開きます。別のファイアウォールを使用している場合、またはファイアウォールを使用していない場合は、手動でファイアウォールを構成する必要があります。

- **/exclude** "*コンポーネント*"\[,"*コンポーネント*"\]

コンマで区切られた1つ以上のオプションコンポーネントのインストールを防止します。各コンポーネントはストレート引用符で囲まれています。たとえば、MCSで管理されていないイメージにVDAをインストールまたはアップグレードする場合、マシンIDサービスコンポーネントは必要ありません。有効な値は次のとおりです。

マルチセッションOS	シングルセッションOS	シングルセッションOSコアサービス
`Citrix Authentication Identity Assertion VDA Plug-in`	`Citrix Authentication Identity Assertion VDA Plug-in`	`Citrix Authentication Identity Assertion VDA Plug-in`
`Citrix Backup and Restore`	`Citrix Backup and Restore`	`Citrix Browser Content Redirection`
`Citrix Browser Content Redirection`	`Citrix Browser Content Redirection`	`Citrix Personalization for App-V - VDA`
`Citrix MCS IODriver`	`Citrix MCS IODriver`	`Citrix Telemetry Service`
`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`	`Citrix Universal Print Client`
`Citrix Profile Management`	`Citrix Profile Management`	`Citrix Vda Log Capture Service`
`Citrix Profile Management WMI Plug-in`	`Citrix Profile Management WMI Plug-in`	`CSE Component`
`Citrix Rendezvous V2`	`Citrix Rendezvous V2`	`Director VDA Plug-in`
`Citrix Supportability Tools`	`Citrix Supportability Tools`	`Machine Management Provider`
`Citrix Telemetry Service`	`Citrix Telemetry Service`	`VDA Monitor Plug-in`
`Citrix Universal Print Client`	`Citrix Universal Print Client`	`VDA WMI Proxy Plug-in`
`Citrix Vda Log Capture Service`	`Citrix Vda Log Capture Service`	

マルチセッションOS	シングルセッションOS	シングルセッションOSコアサービス
`Citrix VDA Upgrade Agent`	`Citrix VDA Upgrade Agent`	
`Citrix WEM Agent`	`Citrix WEM Agent`	
`CSE Component`	`CSE Component`	
`Director VDA Plug-in`	`Director VDA Plug-in`	
`Machine Identity Service`	`Machine Identity Service`	
`Machine Management Provider`	`Machine Management Provider`	
`VDA Monitor Plug-in`	`User Personalization Layer`	
`VDA WMI Proxy Plug-in`	`VDA Monitor Plug-in`	
	`VDA WMI Proxy Plug-in`	

Citrix Profile Managementをインストールから除外する（`/exclude "Citrix Profile Management"`）と、Citrix DirectorでのVDAの監視とトラブルシューティングに影響します。**ユーザーの詳細**ページと**エンドポイント**ページでは、パーソナライゼーションパネルとログオン期間パネルが機能しません。**ダッシュボード**ページと**トレンド**ページでは、平均ログオン期間パネルはProfile Managementがインストールされているマシンのみのデータを表示します。

サードパーティのユーザープロファイル管理ソリューションを使用している場合でも、Citrixは Citrix Profile Management Serviceをインストールして実行することを推奨します。Citrix Profile Management Serviceを有効にする必要はありません。

同じコンポーネント名で`/exclude`と`/includeadditional`の両方を指定した場合、そのコンポーネントはインストールされません。

このオプションは、`VDAWorkstationCoreSetup.exe`インストーラーを使用している場合は無効です。このインストーラーは、これらの項目の多くを自動的に除外します。

- **/h** または **/help**

コマンドのヘルプを表示します。

- **/includeadditional** "*コンポーネント*"\[,"*コンポーネント*"\]

  コンマで区切られた1つ以上のオプションコンポーネントのインストールを含めます。各コンポーネントはストレート引用符で囲まれています。このオプションは、リモートPCアクセス展開を作成していて、デフォルトで含まれていない他のコンポーネントをインストールしたい場合に役立ちます。有効な値は次のとおりです。

マルチセッションOS	シングルセッションOS
`Citrix Backup and Restore`	`Citrix Backup and Restore`
`Citrix MCS IODriver`	`Citrix MCS IODriver`
`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`
`Citrix Profile Management`	`Citrix Profile Management`
`Citrix Profile Management WMI Plug-in`	`Citrix Profile Management WMI Plug-in`
`Citrix Rendezvous V2`	`Citrix Rendezvous V2`
`Citrix Supportability Tools`	`Citrix Supportability Tools`
`Citrix VDA Upgrade Agent`	`Citrix VDA Upgrade Agent`
`Citrix WEM Agent`	`Citrix WEM Agent`
`Machine Identity Service`	`Machine Identity Service`
	`User Personalization Layer`

  同じコンポーネント名で`/exclude`と`/includeadditional`の両方を指定した場合、そのコンポーネントはインストールされません。

- **/installdir** *ディレクトリ*

  コンポーネントがインストールされる既存の空のディレクトリ。デフォルト = `c:\Program Files\Citrix`。

- **/install_mcsio_driver**

使用しないでください。代わりに`/includeadditional "Citrix MCS IODriver"`または`/exclude "Citrix MCS IODriver"`を使用してください。

- **/logpath** パス

  ログファイルの場所。指定されたフォルダーは存在している必要があります。インストーラーは作成しません。デフォルト = 「`%TEMP%\Citrix\XenDesktop Installer`」

  このオプションはグラフィカルインターフェイスでは利用できません。

- **/マスターイメージ**

  VMにVDAをインストールする場合にのみ有効です。VDAを他のマシンを作成するために使用するイメージとして設定します。このオプションは`/mastermcsimage`と同等です。

  このオプションは、`VDAWorkstationCoreSetup_xxxx.exe`インストーラーを使用している場合は無効です。

- **/マスターMCSイメージ**

  このマシンがMachine Creation Servicesでイメージとして使用されることを指定します。このオプションは`/masterimage`と同等です。

- **/マスターPVSイメージ**

  このマシンが、Citrix Provisioning™ またはサードパーティのプロビジョニングツール (Microsoft System Center Configuration Manager など) を使用して、VM をプロビジョニングするためのイメージとして使用されることを指定します。

- **/no_mediafoundation_ack**

  Microsoft Media Foundation がインストールされていないこと、およびいくつかの HDX™ マルチメディア機能がインストールされず、動作しないことを承認します。このオプションを省略し、Media Foundation がインストールされていない場合、VDA のインストールは失敗します。ほとんどのサポートされている Windows エディションには、N エディションを除き、Media Foundation がすでにインストールされています。

- **デスクトップエクスペリエンスなし**

  拡張デスクトップエクスペリエンス機能は利用できなくなりました。このオプション（およびポリシー設定）は、指定されても無視されます。

  マルチセッションOS用VDAをインストールする場合にのみ有効です。拡張デスクトップエクスペリエンス機能の有効化を防止します。この機能は、拡張デスクトップエクスペリエンスCitrixポリシー設定でも制御されます。

- **再起動なし**

  インストール後の再起動を防止します。VDAは再起動するまで使用できません。

- **再開しない**

  デフォルトでは、インストール中にマシンの再起動が必要な場合、再起動が完了するとインストーラーは自動的に再開します。デフォルトを上書きするには、`/noresume`を指定します。これは、メディアを再マウントする必要がある場合や、自動インストール中に情報を取得したい場合に役立ちます。

- **ポート番号** *port*

  `/reconfig`オプションが指定されている場合にのみ有効です。VDAとController間の通信を有効にするポート番号。以前に構成されたポートは、ポート80でない限り無効になります。

- **/proxyconfig** "*アドレスまたはPACファイルのパス*"

  コマンドに`/includeadditional "Citrix Rendezvous V2"`が含まれている場合にのみ有効です。Rendezvousプロトコルで使用するプロキシのアドレスまたはPACファイルのパス。機能の詳細については、Rendezvous protocolを参照してください。

  - プロキシアドレスの形式: `http://<url-or-ip>:<port>`
  - PACファイルの形式: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

- **サイレント** または **パッシブ**

  インストール中にユーザーインターフェイスは表示されません。インストールと構成プロセスの唯一の証拠は、Windowsタスクマネージャーにあります。このオプションを省略すると、グラフィカルインターフェイスが起動します。

- **/再構成**

  `/portnumber`、`/controllers`、または`/enable_hdx_ports`オプションと組み合わせて使用すると、以前に構成されたVDA設定をカスタマイズします。このオプションを`/quiet`オプションも指定せずに指定すると、VDAをカスタマイズするためのグラフィカルインターフェイスが起動します。

- **/リモートPC**

  リモートPCアクセス展開（シングルセッションOS）またはブローカー接続（マルチセッションOS）の場合にのみ有効です。追加コンポーネントのインストールを除外します（`/exclude`および`/includeadditional`オプションのコンポーネントリストを参照）。

このオプションは、`VDAWorkstationCoreSetup.exe`インストーラーを使用する場合は無効です。そのインストーラーは、これらのコンポーネントのインストールを自動的に除外します。

`/remotepc` は `/servervdi` オプションと互換性がありません。

- **/削除**

  `/components`オプションで指定されたコンポーネントを削除します。

- **/remove_appdisk_ack**

  AppDisks™ VDAプラグインがインストールされている場合、VDAインストーラーがそれをアンインストールすることを承認します。

- **/remove_pvd_ack**

  Personal vDiskがインストールされている場合、VDAインストーラーがそれをアンインストールすることを承認します。

- **/すべて削除**

  VDAを削除します。Citrix Workspaceアプリ（インストールされている場合）は削除しません。

- **/エクスペリエンスメトリックを送信**

  インストール、アップグレード、または削除中に収集された分析データをCitrixに自動的に送信します。このオプションが省略された場合（または`/disableexperiencemetrics`オプションが指定された場合）、分析データはローカルで収集されますが、自動的には送信されません。

- **サーバーVDI**

  サポートされているWindowsマルチセッションマシンにシングルセッションOS用VDAをインストールします。Windowsマルチセッションマシンにマルチセッション OS用VDAをインストールする場合は、このオプションを省略してください。

  このオプションを使用する前に、サーバーVDI を参照してください。

  このオプションは、フルプロダクトVDAインストーラーでのみ使用してください。

- **サイトGUID** *guid*

  サイトのActive Directory組織単位（OU）のグローバル一意識別子。これは、検出にActive Directoryを使用している場合に、仮想デスクトップをサイトに関連付けます（自動更新が推奨

されるデフォルトの検出方法です）。サイトGUIDは、Studioに表示されるサイトプロパティです。`/site_guid`と`/controllers`の両方のオプションを指定しないでください。

- **一時ディレクトリ** *directory*

  インストール中に一時ファイルを保持するディレクトリ。デフォルト = `c:\Windows\Temp`。

  このオプションはグラフィカルインターフェイスでは利用できません。

- **仮想マシン**

  VDAをVMにインストールする場合にのみ有効です。BIOS情報がVMに渡されることで物理マシンとして表示される、インストーラーによる物理マシンの検出を上書きします。

  このオプションはグラフィカルインターフェイスでは利用できません。

- **/wem_add_firewall_rules**

  WEMエージェントのファイアウォールルールを追加します。

- **/wem_agent_cache_location**

  WEMエージェントの代替キャッシュの場所。

- **/wem_agent_port**

  WEMエージェントがWEMインフラストラクチャサーバーと通信するために使用するポート。

- **/wem_cached_data_sync_port**

  WEMエージェントがWEMインフラストラクチャサーバーとキャッシュを同期するために使用するポート。

- **/wem_cloud_connectors**

  WEM展開を含むリソースの場所にあるCitrix Cloud™ Connectorのコンマ区切りリスト。

- **/wem_server**

  WEMインフラストラクチャサーバーのFQDNまたはIPアドレス。

- **XenDesktopクラウド**

  VDAがCitrix DaaS™ (Citrix Cloud) 展開にインストールされていることを示します。

VDAのインストール例

フルプロダクトインストーラーでVDAをインストールする:

次のコマンドは、シングルセッションOSおよびCitrix Workspaceアプリ用のVDAを、VMのデフォルトの場所にインストールします。このVDAはイメージとして使用され、MCSを使用してVMをプロビジョニングします。VDAは、`mydomain`ドメイン内の`Contr-Main`という名前のサーバー上のControllerに最初に登録されます。VDAはユーザーパーソナライゼーションレイヤーとWindowsリモートアシスタンスを使用します。

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda,plugins /
controllers "Contr-Main.mydomain.local" /enable_hdx_ports /includeadditional
"user personalization layer" /mastermcsimage /enable_remote_assistance
```

VDAWorkstationCoreSetupスタンドアロンインストーラーでシングルセッションOS VDAをインストールする:

次のコマンドは、リモートPCアクセスまたはVDI展開で使用するために、シングルセッションOSにコアサービスVDAをインストールします。Citrix Workspaceアプリおよびその他の非コアサービスはインストールされません。Controllerのアドレスが指定され、Windowsファイアウォールサービス内のポートは自動的に開かれます。管理者が再起動を処理します。

```
VDAWorkstationCoreSetup .exe /quiet /controllers "Contr-East.domain.com" /
enable_hdx_ports /noreboot
```

VDAをカスタマイズする

VDAをインストールした後、いくつかの設定をカスタマイズできます。製品メディアの`\x64\XenDesktop Setup`ディレクトリから、VDAのインストール用コマンドラインオプションで説明されている以下のオプションを1つ以上使用して、`XenDesktopVdaSetup.exe`を実行します。

- `/reconfigure` (VDAをカスタマイズする際に必須)
- `/h` または `/help`
- `/quiet`
- `/noreboot`
- `/controllers`
- `/portnumber port`
- `/enable_hdx_ports`

VDAのトラブルシューティング

- デリバリーグループのStudio表示で、**詳細**ペインの**インストール済みVDAバージョン**エントリが、マシンにインストールされているバージョンと異なる場合があります。マシンのWindowsのプログラムと機能の表示には、実際のVDAバージョンが表示されます。
- VDAがインストールされても、Delivery Controllerに登録されるまでは、ユーザーにアプリやデスクトップを配信できません。

  VDAの登録方法と登録の問題のトラブルシューティングについては、VDAの登録を参照してください。

Universal Print Serverをインストールするためのコマンドラインオプション

次のオプションは、`XenDesktopPrintServerSetup.exe`コマンドで有効です。

- **/enable_upsserver_port**

ソフトウェア	フォルダ	ファイル名
Citrix診断機能	x64 > 仮想デスクトップコンポーネント	`cdf_x64.msi`
Universal Print Serverサーバーコンポーネント	x64 > ユニバーサルプリントサーバー	`UpsServer_x64.msi`

このオプションが指定されていない場合、インストーラーはグラフィカルインターフェイスから**ファイアウォール**ページを表示します。インストーラーにWindowsファイアウォール規則を自動的に追加させるには**自動**を選択し、管理者が手動でファイアウォールを構成する場合は**手動**を選択します。

印刷サーバーにソフトウェアをインストールした後、(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/printing/printing-provision-printers.html)のガイダンスを使用してUniversal Print Serverを構成します。

詳細情報

Citrixがコンポーネントのインストール結果を報告する方法については、(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/install-configure/install-prepare.html#citrix-installation-return-codes)を参照してください。

スクリプトを使用してVDAをインストールする

> **注：**
>
> Citrixは、お客様の運用環境に合わせて調整されたスクリプトによって引き起こされる問題について責任を負いません。インストール関連のCitrixの問題については、Citrixサポートポータルを使用して、関連するインストールログとともにテクニカルサポートケースをオープンしてください。

> この記事は、Windowsオペレーティングシステムを搭載したマシンへのVDAのインストールに適用されます。Linuxオペレーティングシステム用VDAの詳細については、Linux Virtual Delivery Agentのドキュメントを参照してください。

インストールメディアには、Active Directory内のマシンにVirtual Delivery Agent（VDA）をインストール、アップグレード、または削除するサンプルスクリプトが含まれています。これらのスクリプトは、Machine Creation Services™およびCitrix Provisioning（旧Provisioning Services）で使用されるマスターイメージの保守にも使用できます。

必要なアクセス権:

- スクリプトには、VDAインストールコマンドが配置されているネットワーク共有へのEveryone読み取りアクセス権が必要です。インストールコマンドは、製品版ISOでは `XenDesktopVdaSetup.exe`、スタンドアロンインストーラーでは `VDAWorkstationSetup.exe` または `VDAServerSetup.exe` です。
- ログの詳細は各ローカルマシンに保存されます。レビューと分析のために結果を集中してログに記録するには、スクリプトに適切なネットワーク共有へのEveryone読み取り/書き込みアクセス権が必要です。

スクリプトの実行結果を確認するには、中央ログ共有を調べます。キャプチャされたログには、スクリプトログ、インストーラーログ、MSIインストールログが含まれます。各インストールまたは削除の試行は、タイムスタンプ付きのフォルダーに記録されます。フォルダーのタイトルは、PASSまたはFAILのプレフィックスで操作結果を示します。標準のディレクトリ検索ツールを使用して、中央ログ共有で失敗したインストールまたは削除を見つけることができます。これらのツールは、ターゲットマシンでローカルに検索する代替手段を提供します。

インストールを開始する前に、インストールの準備のタスクを読み、完了してください。

スクリプトを使用してVDAをインストールまたはアップグレードする

1. インストールメディアの`\Support\AdDeploy\`からサンプルスクリプト **InstallVDA.bat** を入手します。Citrixは、元のスクリプトをカスタマイズする前にバックアップを作成することをお勧めします。
2. スクリプトを編集します:
   - インストールするVDAのバージョンを指定します: `SET DESIREDVERSION`。たとえば、バージョン7は7.0として指定できます。完全な値は、インストールメディアのProductVersion.txtファイルに記載されています。ただし、完全一致は必須ではありません。
   - インストーラーが呼び出されるネットワーク共有を指定します。レイアウトのルート（ツリーの最上位）を指します。スクリプトの実行時に、適切なバージョンのインストーラー（32ビットまたは64ビット）が自動的に呼び出されます。例: `SET DEPLOYSHARE=\\fileserver1\share1`。
   - オプションで、集中ログを保存するためのネットワーク共有の場所を指定します。例: `SET LOGSHARE=\\fileserver1\log1)`。
   - コマンドラインを使用したインストールで説明されているように、VDA構成オプションを指定します。`/quiet`および`/noreboot`オプションは、スクリプトにデフォルトで含まれており、必須です: `SET COMMANDLINEOPTIONS=/QUIET /NOREBOOT`。
3. グループポリシーのスタートアップスクリプトを使用して、スクリプトをマシンを含むOUに割り当てます。このOUには、VDAをインストールするマシンのみを含める必要があります。そのOU内のマシンが再起動されると、スクリプトはすべてのマシンで実行されます。サポートされているオペレーティングシステムを持つ各マシンにVDAがインストールされます。

スクリプトを使用してVDAを削除する

1. インストールメディアの`\Support\AdDeploy\`からサンプルスクリプトUninstallVDA.batを入手します。Citrixでは、スクリプトをカスタマイズする前に元のスクリプトのバックアップを作成することをお勧めします。
2. スクリプトを編集します。
   - 削除するVDAのバージョンを指定します: `SET CHECK\_VDA\_VERSION`。たとえば、バージョン7は7.0として指定できます。完全な値は、インストールメディアのProductVersion.txtファイル（7.0.0.3018など）で確認できます。ただし、完全一致は必要ありません。
   - オプションで、集中ログを保存するためのネットワーク共有の場所を指定します。

3. グループポリシーのスタートアップスクリプトを使用して、スクリプトをマシンを含むOUに割り当てます。このOUには、VDAを削除するマシンのみを含める必要があります。OU内のマシンが再起動されると、スクリプトはすべてのマシンで実行されます。各マシンからVDAが削除されます。

トラブルシューティング

- スクリプトは、スクリプトの実行の進行状況を記述する内部ログファイルを生成します。スクリプトは、展開の開始から数秒以内に`Kickoff_VDA_Startup_Script`ログを中央ログ共有にコピーします。全体的なプロセスが機能していることを確認できます。このログが期待どおりに中央ログ共有にコピーされない場合は、ローカルマシンを検査してさらにトラブルシューティングを行ってください。スクリプトは、各マシンの`%temp%`フォルダーに2つのデバッグログファイルを配置します。

  - `Kickoff_VDA_Startup_Script_<DateTimeStamp>.log`
  - `VDA_Install_ProcessLog_<DateTimeStamp>.log`

  スクリプトが次の状態であることを確認するために、これらのログを確認します。

  - 期待どおりに実行されている。
  - ターゲットオペレーティングシステムを適切に検出している。
  - `DEPLOYSHARE`共有の`ROOT`を指すように正しく構成されている（`AutoSelect.exe`という名前のファイルが含まれている）。
  - `DEPLOYSHARE`と`LOG`の両方の共有に対して認証できる。

- Citrixがコンポーネントインストールの結果を報告する方法については、Citrixインストールのリターンコードを参照してください。
- デリバリーグループのStudio表示では、**詳細**ペインの**インストール済みVDAバージョン**エントリが、マシンにインストールされているバージョンと異なる場合があります。マシンのプログラムと機能の表示には、実際のVDAバージョンが表示されます。
- VDAがインストールされた後、Delivery Controllerに登録されるまで、ユーザーにアプリやデスクトップを配信できません。

  VDA登録方法と登録の問題のトラブルシューティング方法については、「VDA登録」を参照してください。

SCCM を使用した VDA のインストール

> **注：**
>
> Citrixは、顧客の運用環境に合わせて調整されたMicrosoft System Center Configuration Manager (SCCM)などのソフトウェア配布ツールを使用してVirtual Delivery Agent (VDA)を展開することによって発生する問題について責任を負いません。インストール関連のCitrixの問題については、Citrixサポートポータルを使用して関連するインストールログを添えてテクニカルサポートケースをオープンしてください。

概要

Microsoft System Center Configuration Manager (SCCM)または類似のソフトウェア配布ツールを使用してVirtual Delivery Agent (VDA)を正常に展開するには、Citrix®はVDAインストーラーを段階的に使用することを推奨します。

Citrix は、VDA のインストールまたはアップグレードの一部として VDA Cleanup Utility を使用することを推奨しません。VDA インストーラーが以前に失敗した場合にのみ、VDA Cleanup Utility を使用してください。

再起動

VDA のインストール中に必要な再起動の回数は、環境によって異なります。例:

- 保留中の更新や以前のソフトウェアインストールからの再起動のために、再起動が必要になる場合があります。
- 他のプロセスによって以前にロックされていたファイルは更新が必要になる場合があり、追加の再起動を強制します。
- VDA インストーラーの一部のオプションコンポーネント (Citrix Profile Management や Citrix Files など) は、再起動が必要になる場合があります。

SCCMタスクシーケンサーは、必要なすべての再起動を管理します。

タスクシーケンスを定義する

すべての前提条件と再起動を特定したら、SCCMタスクシーケンサーを使用して以下を完了します。

- VDAは、インストールメディアのアクセス可能なコピーから、またはVDAスタンドアロンインストーラーのいずれかからインストールできます。
    - `VDAWorkstationSetup_XXXX.exe`

  - `VDAServerSetup_XXXX.exe`
  - `VDAWorkstationCoreSetup_XXXX.exe`

  VDAインストーラーの詳細については、「インストーラー」を参照してください。

- VDAをアップグレードする場合、インストールされているマシンはセッションがない状態でメンテナンスモードになっている必要があります。
- マシンでVDAのインストールが初めて実行されると、使用されているVDAインストーラーがそのマシンにコピーされます。
  - `VDAWorkstationCoreSetup_XXXX.exe` 以外のVDAインストーラーを使用する場合、VDAインストーラーは `%ProgramData%\Citrix\XenDesktopSetup\XenDesktopVdaSetup.exe` にコピーされます。
  - `VDAWorkstationCoreSetup_XXXX.exe` を使用する場合、VDAインストーラーは `%ProgramData%\Citrix\XenDesktopSetup\XenDesktopRemotePCSetup.exe` にコピーされます。 `
- VDAインストーラーのディレクトリの場所は、レジストリ `“HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaInstall” “MetaInstallerInstallLocation”` にも保存されます。
- コマンドラインオプションに `/NOREBOOT` 、 `/NORESUME` 、および `/QUIET` を追加します。
  - `/QUIET` : インストール中にユーザーインターフェイスを表示しないようにします。これにより、SCCMがインストールプロセスを制御できます。
  - `/NOREBOOT` : VDAインストーラーが自動的に再起動するのを抑制します。SCCMは必要に応じて再起動をトリガーします。
  - `/NORESUME` : 通常、インストール中に再起動が必要な場合、VDAインストーラーは `runonce` レジストリキー (`\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce`) を設定します。マシンが再起動すると、Windowsはこのキーを使用してVDAインストーラーを起動します。これはSCCMにとって問題となります。なぜなら、SCCMはインストールを監視して終了コードをキャプチャできないためです。

SCCM を使用したインストールシーケンスの例

次の例は、インストールシーケンスを示しています。

1. **SCCM TASK1:** マシンを再起動して準備します。
2. **SCCM TASK2:** VDAのインストールを開始します。

a. コマンドラインオプションに`/quiet`、`/noreboot`、および`/noresume`オプションを追加します。

b. 選択した VDA インストーラー (ローカルイメージまたは最小インストーラーのいずれか) を実行します。

c. SCCM はリターンコードをキャプチャする必要があります。

- リターンコードが 0 または 8 の場合、インストールは完了しており、再起動が必要です。
- 戻りコードが3の場合、マシンを再起動し、SCCM TASK3に制御を渡します。

3. **SCCM TASK3:** VDAのインストールを続行します。

a. SCCM TASK2が0または8を返さない場合、再起動が完了した後にインストールを続行する必要があります。

b. VDAインストーラーが0または8（インストールが成功したことを示す）または3（SCCM TASK3を繰り返す必要があることを示す）を返すまで、SCCM TASK3は繰り返されます。その他の戻りコードはエラーとして扱い、SCCM TASK3はエラーを報告して停止する必要があります。

c. コマンドラインパラメーターなしで、コピーされた場所（タスクシーケンスの定義で説明）から適切なVDAインストーラー（ほとんどの場合`XenDesktopVdaSetup.exe`、`VDAWorkstationCoreSetup_XXXX.exe`が使用された場合は`XenDesktopRemotePCSetup.exe`）を実行して、VDAのインストールを再開します。（VDAインストーラーは、インストーラーの初回実行時に保存したパラメーターを使用します。）

d. VDAインストーラーからのリターンコードを確認します。

- 0または8：成功、インストール完了、再起動が必要です。
- 3: インストールが完了していません。マシンを再起動し、0または8が返されるまでSCCM TASK3を繰り返します。その他の戻りコードはエラーとして扱い、SCCM TASK3はエラーを報告して終了する必要があります。

リターンコードの詳細については、Citrixインストールリターンコードを参照してください。

VDAインストールコマンドの例

利用可能なインストールオプションは、使用するインストーラーによって異なります。コマンドラインオプションの詳細については、以下の記事を参照してください。

- VDAのインストール

- コマンドラインを使用したインストール

Remote PC Access のインストールコマンド

- 次のコマンドは、シングルセッションコア VDA インストーラー（`VDAWorkstationCoreSetup.exe`）を使用します。

  ```
  VDAWorkstationCoreSetup.exe /quiet /controllers “control.domain.com” /enable_hdx_ports /noresume /noreboot
  ```

- 次のコマンドは、シングルセッションフル VDA インストーラー（`VDAWorkstationSetup.exe`）を使用します。

  ```
  VDAWorkstationSetup.exe /quiet /remotepc /controllers “control.domain.com” /enable_hdx_ports /noresume /noreboot
  ```

専用 VDI のインストールコマンド

- 次のコマンドは、シングルセッションフル VDA インストーラー（`VDAWorkstationSetup.exe`）を使用します。

  ```
  VDAWorkstationSetup.exe /quiet /components vda /controllers “control.domain.com” /enable_hdx_ports /enable_remote_assistance /noresume /noreboot
  ```

サイトを作成する

サイトとは、Citrix Virtual Apps and Desktops™展開に付ける名前です。これには、Delivery Controllerとその他のコアコンポーネント、Virtual Delivery Agent (VDA)、ホストへの接続、マシンカタログ、およびデリバリーグループが含まれます。サイトは、コアコンポーネントをインストールした後、最初のマシンカタログとデリバリーグループを作成する前に作成します。

ControllerがServer Coreにインストールされている場合は、Citrix Virtual Apps and Desktops SDKのPowerShellコマンドレットを使用してサイトを作成します。

サイトを作成すると、Citrix Customer Experience Improvement Program (CEIP) に自動的に登録されます。CEIP は匿名の統計情報と使用状況情報を収集し、Citrix に送信します。最初のデータパッケージは、サイト作成後約7日後に Citrix に送信されます。サイト作成後いつでも登録を変更できます。Studio ナビゲーションペインで **構成** を選択し、次に **製品サポート** タブを選択して、ガイダンスに従ってください。詳細については、`<http://more.citrix.com/XD-CEIP>` を参照してください。

サイトを作成したユーザーは、完全な管理者になります。詳細については、委任管理 を参照してください。

サイトを作成する前にこの記事を確認して、何が期待できるかを知っておいてください。

手順1. Studio を開き、サイト作成ウィザードを開始する

Studio がまだ開いていない場合は開きます。サイト作成ウィザードを開始するアクションに自動的に誘導されます。そのアクションを選択します。

手順2. サイトの種類と名前

はじめに ページで、サイトの種類を選択します。

- **アプリケーションおよびデスクトップ配信サイト**。アプリケーションおよびデスクトップ配信サイトを作成する際、完全な展開サイト（推奨）または空のサイトを作成するかをさらに選択できます。空のサイトは部分的にしか構成されておらず、通常は上級管理者が作成します。
- **Remote PC Access サイト**。Remote PC Access サイトでは、指定されたユーザーがセキュアな接続を介してオフィスPCにリモートでアクセスできます。

今すぐアプリケーションおよびデスクトップ配信展開を作成した場合でも、後で Remote PC Access 展開を追加できます。逆に、今すぐ Remote PC Access 展開を作成した場合でも、後で完全な展開を追加できます。

サイトの名前を入力します。サイトが作成されると、その名前が Studio ナビゲーションペインの上部に表示されます: **Citrix Studio** (*サイト名*)。

ステップ3. データベース

データベースページには、サイト、監視、および構成ログデータベースの設定に関する選択肢が含まれています。データベースの設定の選択肢と要件の詳細については、データベースを参照してください。

> **注：**
>
> SQL Server Always On ListenerがTLS暗号化用に構成されている場合、データベース作成権限を持つ資格情報の入力を求められることがあります。有効な管理者資格情報を入力しても、データベースの作成は失敗します。SQL Server証明書に、Subject Alternative Names (SAN) にリスナーのDNS名が含まれていることを確認してください。詳細については、`<https://docs.microsoft.com/ja-jp/sql/database-engine/availability-groups/`

> `windows/listeners-client-connectivity-application-failover#SSLcertificates>`を参照してください。

> サイトデータベースとして使用するためにSQL Server Expressをインストールすることを選択した場合（デフォルト）、そのソフトウェアのインストール後に再起動が発生します。サイトデータベースとして使用するためにSQL Server Expressソフトウェアをインストールしないことを選択した場合、その再起動は発生しません。

デフォルトのSQL Server Expressを使用しない場合は、サイトを作成する前に、SQL Serverソフトウェアがマシンにインストールされていることを確認してください。システム要件にサポートされているバージョンが記載されています。

サイトにDelivery Controllerを追加したい場合で、すでに他のサーバーにControllerソフトウェアをインストールしている場合は、このページからそれらのControllerを追加できます。データベースを設定するスクリプトを生成する予定がある場合は、スクリプトを生成する前にControllerを追加してください。

ステップ4. ライセンス

> **注：**

> ライセンスサーバーがバージョン11.17.2ビルド53100以降で実行されていることを確認してください。この前提条件を満たさない場合、サイトのアップグレードや作成中にエラーや推奨事項が発生する可能性があります。

> **ライセンス**ページで、ライセンスサーバーのアドレスを指定し、使用する（インストールする）ライセンスを示します。

- ライセンスサーバーのアドレスを`name:[port]`の形式で指定します。*名前*はFQDN、NetBIOS、またはIPアドレスである必要があります。FQDNを推奨します。ポート番号を省略した場合、デフォルトは27000です。**接続**をクリックします。ライセンスサーバーへの接続が成功するまで、次のページに進むことはできません。
- 接続が確立されると、デフォルトで**既存のライセンスを使用**が選択されます。表示には、現在インストールされているライセンスに基づいて、この製品が構成できる互換性のある製品が一覧表示されます。

- この製品をリストされている製品のいずれか（例：Citrix Virtual Apps PremiumまたはCitrix Virtual Desktops™ Premium）として、それらのライセンスのいずれかを使用して構成したい場合は、そのエントリを選択します。
- この製品で使用するために、すでにライセンスを割り当ててダウンロードしている（Citrix Manage Licenses Tool を使用して）が、まだライセンスをインストールしていない場合：
  - **ライセンスファイルを参照**をクリックします。
  - ファイルエクスプローラーで、ダウンロードしたライセンスを見つけて選択します。関連する製品がサイト作成ウィザードの**ライセンス**ページに表示されます。使用したいエントリを選択します。
- 目的の製品が表示されない場合、または割り当て済みでダウンロード済みのライセンスがない場合は、ライセンスを割り当て、ダウンロードしてインストールできます。これを行うには、ライセンスサーバーがインターネットにアクセスできる必要があります。目的の製品のライセンスアクセスコードが必要です。Citrixからそのコードがメールで送信されます。
  - **割り当ててダウンロード**をクリックします。
  - **ライセンスの割り当て**ダイアログで、Citrixから送信されたライセンスアクセスコードを入力します。**ライセンスを割り当てる**をクリックします。
  - 新しいライセンスに関連付けられている製品が、サイト作成ウィザードの**ライセンス**ページに表示されます。使用するエントリを選択します。

  または、**30日間の無料試用版を使用**を選択し、後でライセンスをインストールします。詳細については、ライセンスドキュメントを参照してください。

手順5. 電源管理（Remote PC Access のみ）

手順8. Remote PC Access を参照してください。

手順6. ホスト接続、ネットワーク、およびストレージ

ハイパーバイザーまたはその他のサービス上のVMを使用してアプリケーションとデスクトップを配信している場合、オプションでそのホストへの最初の接続を作成できます。その接続のストレージおよびネットワークリソースを指定することもできます。サイト作成後、この接続とリソースを変更したり、さらに接続を作成したりできます。詳細については、接続とリソースを参照してください。

- **接続**ページで指定する情報については、接続とリソースを参照してください。

- ハイパーバイザーまたはその他のサービスでVMを使用していない場合（または、Studio を使用して専用ブレードPC上のデスクトップを管理している場合）は、接続の種類として **なし** を選択します。
- Remote PC Accessサイトを構成し、Wake on LAN機能を使用する予定がある場合は、**Microsoft System Center Configuration Manager**タイプを選択します。

接続の種類に加えて、Citrixツール（Machine Creation Services™など）またはその他のツールを使用してVMを作成するかどうかを指定します。

- **ストレージ**ページと**ネットワーク**ページで指定する情報については、ホストストレージ、ストレージ管理、およびストレージの選択を参照してください。
- ハイブリッド権限ライセンスを所有しており、パブリッククラウドホスト接続（例：AWS）を追加している場合、それらの接続がここに表示されます。これらのパブリッククラウドホスト接続を表示するには、Citrix Studioを再起動してください。

ステップ7. 追加機能

追加機能ページで、サイトをカスタマイズするための機能を選択できます。情報が必要な項目のチェックボックスを選択すると、構成ボックスが表示されます。

- **App-V公開:** App-Vサーバー上のMicrosoft App-Vパッケージからアプリケーションを使用する場合は、この機能を選択します。App-V管理サーバーのURLと、App-V公開サーバーのURLおよびポート番号を指定します。

  ネットワーク共有場所にあるApp-Vパッケージからのみアプリケーションを使用する場合は、この機能を選択する必要はありません。

  この機能は、後でStudioで有効/無効にしたり、構成したりすることもできます。詳細については、App-Vを参照してください。

ステップ8. Remote PC Access

Remote PC Accessの展開については、Remote PC Accessを参照してください。

Wake on LAN機能を使用する場合は、サイトを作成する前にMicrosoft System Center Configuration Managerで構成手順を完了してください。詳細については、Configuration ManagerとRemote PC Access Wake on LANを参照してください。

Remote PC Accessサイトを作成する場合：

- Wake on LAN機能を使用している場合は、**電源管理**ページでMicrosoft System Center Configuration Managerのアドレス、資格情報、および接続情報を指定します。

- **ユーザー**ページでユーザーまたはユーザーグループを指定します。すべてのユーザーを自動的に追加するデフォルトのアクションはありません。また、**マシンアカウント**ページでマシンアカウント（ドメインとOU）情報を指定します。

  ユーザー情報を追加するには、**ユーザーの追加**をクリックします。ユーザーとユーザーグループを選択し、**ユーザーの追加**をクリックします。

  マシンアカウント情報を追加するには、**マシンアカウントの追加**をクリックします。マシンアカウントを選択し、**マシンアカウントの追加**をクリックします。**OUの追加**をクリックします。ドメインと組織単位を選択し、サブフォルダー内の項目を含めるかどうかを指定します。**OUの追加**をクリックします。

`Remote PC User Machine Accounts`という名前のマシンカタログが自動的に作成されます。このカタログには、サイト作成ウィザードで追加したすべてのマシンアカウントが含まれます。`Remote PC User Desktops`という名前のデリバリーグループが自動的に作成されます。このグループには、追加したすべてのユーザーとユーザーグループが含まれます。

ステップ9. 概要

「**概要**」ページには、指定した情報が一覧表示されます。変更したい場合は、「**戻る**」ボタンを使用してください。完了したら、「**作成**」をクリックすると、サイトの作成が開始されます。

サイト構成のテスト

サイト作成後にテストを実行するには、ナビゲーションペインの上部にある「**Citrix Studio (サイト *サイト名*)**」を選択します。次に、中央ペインで「**サイトのテスト**」をクリックします。サイトテスト結果のHTMLレポートを表示できます。

Windows Server 2016にインストールされたControllerでは、サイトテスト機能が失敗する場合があります。この失敗は、サイトデータベースにローカルのSQL Server Expressが使用されており、SQL Server Browserサービスが開始されていない場合に発生します。この失敗を回避するには、次のタスクを完了してください。

1. SQL Server Browserサービスを有効にし（必要に応じて）、開始します。
2. SQL Server (SQLEXPRESS) サービスを再起動します。

以前の展開をアップグレードすると、サイトテストは自動的に実行されます。詳細については、「サイトの事前テスト」を参照してください。

トラブルシューティング

サイトを構成した後、Studioをインストールし、MMCを介してリモートマシンにスナップインとして追加できます。後でそのスナップインを削除しようとすると、MMCが応答を停止する場合があります。回避策として、MMCを再起動してください。

マシンカタログを作成する

> **重要:**

> Citrix Virtual Apps and Desktops™ 7 2006以降、現在の展開で以下のいずれかのテクノロジーを使用している場合、それらのテクノロジーを使用するサポート終了（EOL）アイテムを削除した後にのみ、現在のリリースに展開をアップグレードできます。

> - パーソナルvDisk (PvDs)
> - AppDisks™
> - パブリッククラウドホストの種類：Citrix CloudPlatform、Microsoft Azure Classic

> 詳細については、「PvD、AppDisks、およびサポートされていないホストの削除」を参照してください。

> 展開にパブリッククラウドホスト接続を使用する場合は、新規インストールまたは現在のリリースへのアップグレードを完了するためにHybrid Rights Licenseが必要です。

インストーラーがサポートされていないテクノロジーの1つ以上、またはHybrid Rights Licenseなしのホスト接続を検出すると、アップグレードは一時停止または停止します。説明メッセージが表示されます。インストーラーログには詳細が含まれています。詳細については、「展開のアップグレード」を参照してください。

ホスト接続に対するHybrid Rights Licenseの影響

Hybrid Rights Licenseの資格に基づいて、パブリッククラウドホストへのホスト接続が影響を受ける3つのシナリオがあります。

- パブリッククラウドホストへのホスト接続を作成するには、Hybrid Rights Licenseが必要です。

- Hybrid Rights Licenseを所有しているがライセンスの有効期限が切れている場合、パブリッククラウドホストへの既存の接続は資格なしとマークされ、メンテナンスモードに入ります。既存のホスト接続がメンテナンスモードの場合、次の操作はできません。
  - ホスト接続の追加または変更
  - カタログの作成とイメージの更新
  - 電源操作の実行
- 資格なしのホスト接続が資格ありに変更されると、既存のホスティング接続が再度有効になります。

はじめに

物理マシンまたは仮想マシンのコレクションは、マシンカタログと呼ばれる単一のエンティティとして管理されます。カタログ内のマシンは、マルチセッションOSまたはシングルセッションOSのいずれかの同じ種類のオペレーティングシステムを持ちます。マルチセッションOSマシンを含むカタログには、WindowsマシンまたはLinuxマシンのいずれかを含めることができ、両方を含めることはできません。

サイトを作成した後、Citrix Studioは最初のマシンカタログを作成するようにガイドします。最初のカタログを作成した後、Studioは最初のデリバリーグループを作成するようにガイドします。後で、作成したカタログを変更したり、さらにカタログを作成したりできます。

> **ヒント:**
>
> 既存の展開をアップグレードすると、Machine Creation Services (MCS) ストレージ最適化 (MCS I/O) 機能が有効になり、追加の構成は不要です。Virtual Delivery Agent (VDA) と Delivery Controller のアップグレードが MCS I/O のアップグレードを処理します。

概要

VMのカタログを作成するときは、それらのVMをプロビジョニングする方法を指定します。Machine Creation Services™ (MCS) や Citrix Provisioning (旧Provisioning Services) などのCitrixツールを使用できます。または、独自のツールを使用してマシンを提供することもできます。

考慮事項:

- MCSは、仮想マシンイメージからの単一のシステムディスクをサポートします。そのイメージに接続されている残りのデータディスクは無視されます。

- Citrix Provisioningを使用してマシンを作成する場合は、手順についてCitrix Provisioningドキュメントを参照してください。
- MCSを使用してVMをプロビジョニングする場合、カタログ内に同一のVMを作成するためにマスターイメージ（またはイメージのスナップショット）を提供します。カタログを作成する前に、まずツールを使用してマスターイメージを作成および構成します。このプロセスには、イメージへのVirtual Delivery Agent (VDA) のインストールが含まれます。その後、Studioでマシンカタログを作成します。そのイメージ（またはスナップショット）を選択し、カタログに作成するVMの数を指定し、追加情報を構成します。
- マシンがすでに利用可能な場合でも、それらのマシン用に1つ以上のマシンカタログを作成する必要があります。
- PowerShell SDKを直接使用してカタログを作成する場合、イメージやスナップショットではなく、ハイパーバイザーテンプレート (VMTemplates) を指定できます。
- テンプレートを使用してカタログをプロビジョニングすることは、実験的な機能と見なされます。この方法を使用すると、仮想マシンの準備が失敗する可能性があります。その結果、テンプレートを使用してカタログを公開することはできません。

MCSまたはCitrix Provisioning™を使用して最初のカタログを作成する場合、サイトを作成したときに構成したホスト接続を使用します。後で（最初のカタログとデリバリーグループを作成した後）、その接続に関する情報を変更したり、さらに接続を作成したりできます。

カタログ作成ウィザードを完了すると、正しく構成されていることを確認するためにテストが自動的に実行されます。テストが完了すると、テストレポートを表示できます。Studioからいつでもテストを実行できます。

> **注：**
>
> MCSはWindows 10 IoT CoreおよびWindows 10 IoT Enterpriseをサポートしていません。詳細については、Microsoftサイトを参照してください。

> Citrix Provisioningツールの技術的な詳細については、Citrix Virtual Apps and Desktops Image Managementを参照してください。

RDS ライセンスチェック

Citrix Studioは現在、WindowsマルチセッションOSマシンを含むマシンカタログを作成する際に、有効なMicrosoft RDSライセンスのチェックを実行しません。Windows **マルチセッションOSマシン**のMicrosoft RDSライセンスのステータスを表示するには、Citrix Directorに移動します。**マ**

シン詳細パネルでMicrosoft RDSライセンスのステータスを表示します。このパネルは、**マシン詳細とユーザー詳細**ページにあります。詳細については、Microsoft RDS license healthを参照してください。

VDA登録

ブローカーセッションを起動する際、VDAはDelivery Controller™に登録されている必要があります。登録されていないVDAは、利用可能なリソースの活用不足につながる可能性があります。VDAが登録されない理由はさまざまあり、その多くは管理者がトラブルシューティングできます。Studioは、カタログ作成ウィザードおよびカタログからデリバリーグループにマシンを追加した後に、トラブルシューティング情報を提供します。

ウィザードを使用して既存のマシンを追加すると、コンピューターアカウント名の一覧に、各マシンがカタログへの追加に適しているかどうかが示されます。各マシンの横にあるアイコンにカーソルを合わせると、そのマシンに関する情報メッセージが表示されます。

メッセージで問題のあるマシンが特定された場合は、そのマシンを削除するか、追加します。たとえば、マシンに関する情報が取得できない可能性があることを示すメッセージが表示された場合でも、そのマシンを追加してください。

詳細については、以下を参照してください。

- VDA登録のトラブルシューティングガイダンスについては、CTX136668
- VDAのバージョンと機能レベル
- VDA登録方法

MCSカタログ作成の概要

カタログ作成ウィザードで情報を提供した後の、デフォルトのMCSアクションの概要を以下に示します。

- マスターイメージ（スナップショットではなく）を選択した場合、MCSはスナップショットを作成します。
- MCSはスナップショットの完全なコピーを作成し、そのコピーをホスト接続で定義されている各ストレージの場所に配置します。
- MCSはマシンをActive Directoryに追加し、一意のIDを作成します。
- MCSは、ウィザードで指定された数のVMを作成し、各VMに2つのディスクを定義します。VMごとの2つのディスクに加えて、マスターも同じストレージの場所に保存されます。複数のストレージの場所が定義されている場合、それぞれに次のディスクタイプが割り当てられます。

- 作成されたばかりのVM間で共有される、読み取り専用のスナップショットの完全なコピー。
- 各VMに一意のIDを付与する一意の16 MBのIDディスク。各VMはIDディスクを取得します。
- VMへの書き込みを保存するための固有の差分ディスク。このディスクはシンプロビジョニングされており（ホストストレージでサポートされている場合）、必要に応じてマスターイメージの最大サイズまで増加します。各VMには差分ディスクが割り当てられます。差分ディスクには、セッション中に加えられた変更が保持されます。専用デスクトップの場合は永続的です。プールされたデスクトップの場合、デリバリーコントローラーを介した再起動ごとに削除され、新しいものが作成されます。

あるいは、静的デスクトップを配信するためにVMを作成する際、カタログ作成ウィザードの**マシン**ページで、シック（完全コピー）VMクローンを指定できます。完全クローンは、すべてのデータストアにマスターイメージを保持する必要はありません。各VMは独自のファイルを持っています。

MCSストレージに関する考慮事項

MCSのストレージソリューション、構成、容量を決定する際には、多くの要因があります。以下の情報は、ストレージ容量に関する適切な考慮事項を提供します。

容量に関する考慮事項:

- ディスク

  DeltaまたはDifferencing (Diff) ディスクは、ほとんどのMCS展開において、各VMで最大のスペースを消費します。MCSによって作成される各VMには、作成時に最低2つのディスクが割り当てられます。

  - Disk0 = 差分ディスク：マスターベースイメージからコピーされたOSが含まれます。
  - Disk1 = IDディスク: 16 MB - 各VMのActive Directoryデータを格納します。

  製品の進化に伴い、特定のユースケースや機能の消費を満たすために、さらにディスクを追加する必要がある場合があります。例:

  - MCS Storage Optimizationは、各VMにライトキャッシュスタイルのディスクを作成します。XenServer、VMware、およびSCVMM仮想化環境では、ホスト接続の作成時に利用可能なOSストレージリストと利用可能な一時ストレージリストを同じように構成した場合、MCSはライトバックキャッシュ (WBC) ディスクをOSディスクと同じストレージ場所に配置します。

- MCSは、前のセクションで説明したDeltaディスクのシナリオとは対照的に、フルクローンを使用する機能を追加しました。

ハイパーバイザーの機能も考慮に入れる必要があるかもしれません。例:

- Citrix Hypervisor IntelliCacheは、各Citrix Hypervisorのローカルストレージに読み取りディスクを作成します。このオプションにより、共有ストレージの場所に保持されている可能性のあるマスターイメージに対するIOPSを節約できます。

- ハイパーバイザーのオーバーヘッド

  ハイパーバイザーは、VMのオーバーヘッドを発生させる特定のファイルを使用します。ハイパーバイザーは、管理および一般的なログ記録操作にもストレージを使用します。オーバーヘッドを含めるための領域を計算します。

  - ログファイル
  - ハイパーバイザー固有のファイル。例：
    - VMwareは、**VMストレージ**フォルダーにファイルを追加します。VMwareのベストプラクティスを参照してください。
    - 仮想マシンの合計サイズ要件を計算します。仮想ディスクに20 GB、スワップファイルに16 GB、ログファイルに100 MBを使用し、合計36.1 GBを消費する仮想マシンを考慮してください。
  - XenServerのスナップショット; VMwareのスナップショット。

- プロセスオーバーヘッド

  カタログの作成、マシンの追加、カタログの更新には、それぞれ固有のストレージへの影響があります。例：

  - 初期カタログ作成では、ベースディスクのコピーを各ストレージの場所にコピーする必要があります。
    - また、一時的に準備VMを作成する必要があります。
  - カタログにマシンを追加する場合、ベースディスクを各ストレージの場所にコピーする必要はありません。カタログの作成は、選択された機能によって異なります。
  - カタログを更新すると、各ストレージの場所に余分なベースディスクが作成されます。カタログの更新では、カタログ内の各VMが一定期間2つの差分ディスクを持つため、一時的なストレージのピークも発生します。

その他の考慮事項：

- **RAMサイジング：** I/O最適化ディスク、ライトキャッシュ、スナップショットファイルなど、特定のハイパーバイザーファイルとディスクのサイズに影響します。
- **シンプロビジョニング/シックプロビジョニング:** シンプロビジョニング機能があるため、NFSストレージが推奨されます。

Machine Creation Services (MCS) ストレージ最適化

MCS I/O と呼ばれる Machine Creation Services (MCS) ストレージ最適化機能では、次のようになります。

- ライトキャッシュコンテナは*ファイルベース*であり、Citrix Provisioning と同じ機能です。たとえば、Citrix Provisioning のライトキャッシュファイル名は `D:\vdiskdif.vhdx` で、MCS I/O のライトキャッシュファイル名は `D:\mcsdif.vhdx` です。
- ライトキャッシュディスクに書き込まれる Windows クラッシュダンプファイルのサポートを含めることで、診断機能の改善を実現します。
- MCS I/O は、最適な多層書き込みキャッシュソリューションを提供するために、*RAM 内キャッシュとハードディスクへのオーバーフロー*というテクノロジーを保持しています。この機能により、管理者は各層（RAM とディスク）のコストとパフォーマンスのバランスを取り、目的のワークロード要件を満たすことができます。

書き込みキャッシュ方式を*ディスクベース*から*ファイルベース*に更新するには、次の変更が必要です。

1. MCS I/O は、RAM のみのキャッシュをサポートしなくなりました。マシンカタログ作成時に Citrix Studio でディスクサイズを指定してください。
2. VM の書き込みキャッシュディスクは、VM を初めて起動するときに自動的に作成およびフォーマットされます。VM が起動すると、書き込みキャッシュファイル `mcsdif.vhdx` がフォーマットされたボリューム `MCSWCDisk` に書き込まれます。
3. ページファイルはこのフォーマットされたボリューム `MCSWCDisk` にリダイレクトされます。その結果、このディスクサイズはディスク領域の合計量を考慮します。これには、ディスクサイズと生成されたワークロードの差分に加えて、ページファイルサイズが含まれます。これは通常、VM の RAM サイズに関連付けられます。

MCS ストレージ最適化の更新の有効化

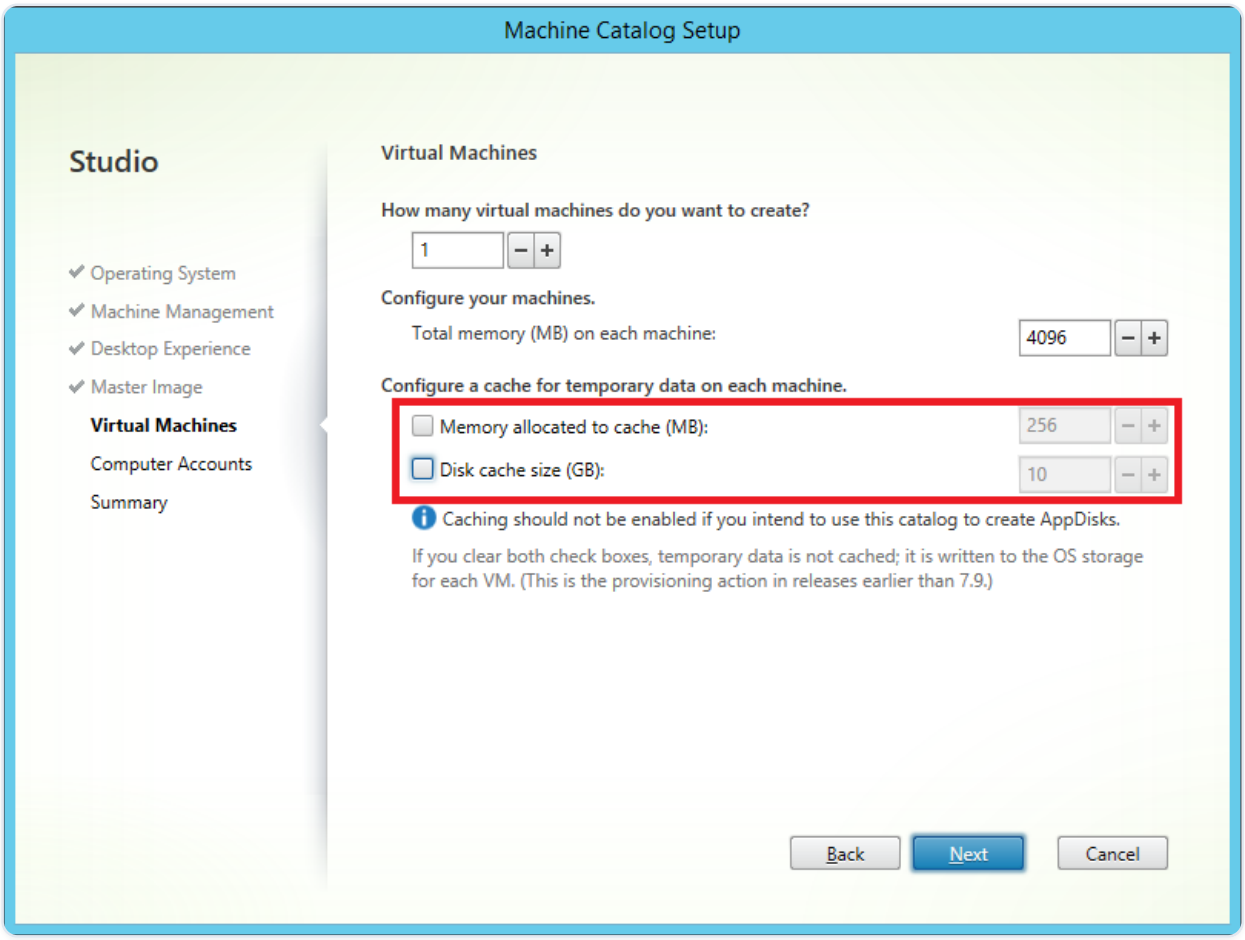
MCS I/O ストレージ最適化機能を有効にするには、Delivery Controller と VDA を Citrix Virtual Apps and Desktops の最新バージョンにアップグレードしてください。

注：

MCS I/O が有効になっている既存の展開をアップグレードする場合、追加の構成は不要です。VDA と Delivery Controller のアップグレードによって MCS I/O のアップグレードが処理されます。

MCS ストレージ最適化の更新を有効にする際は、次の点を考慮してください。

- マシンカタログを作成する際、管理者は RAM とディスクサイズを構成できます。



- バージョン 1903 用に構成された VDA を含む新しい VM スナップショットに既存のマシンカタログを更新すると、次の動作になります。新しいスナップショットは、既存のカタログの RAM およびディスクサイズに対する MCS I/O 設定を引き続き使用します。既存の生ディスクはフォーマットされます。

重要:

> Citrix Virtual Apps and Desktops バージョン 1903 で MCS ストレージ最適化が変更されました。このリリースでは、ファイルベースのライトキャッシュテクノロジがサポートされ、パフォーマンスと安定性が向上しています。MCS I/O によって提供される新しい機能では、以前の Citrix Virtual Apps and Desktops リリースと比較して、より高いライトキャッシュストレージ要件が必要になる場合があります。Citrix は、割り当てられたワークフローと追加のページファイルサイズに対して十分なディスク容量があることを確認するために、ディスクサイズを再評価することをお勧めします。ページファイルサイズは通常、システム RAM の量に関連しています。既存のカタログディスクサイズが不十分な場合は、マシンカタログを作成し、より大きなライトキャッシュディスクを割り当ててください。

永続的なライトバックキャッシュディスクを持つカタログを PowerShell を使用して作成する

永続的なライトバックキャッシュディスクを持つカタログを構成するには、PowerShell パラメーター `New-ProvScheme CustomProperties` を使用します。このパラメーターは、MCS プロビジョニングされたマシンに対してライトバックキャッシュディスクがどのように永続化するかを決定するために使用される追加のプロパティ `PersistWBC` をサポートします。`PersistWBC` プロパティは、`UseWriteBackCache` パラメーターが指定され、`WriteBackCacheDiskSize` パラメーターがディスクが作成されることを示すように設定されている場合にのみ使用されます。

`PersistWBC`をサポートする前の`CustomProperties`パラメーターで見つかったプロパティの例は次のとおりです。

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

</CustomProperties>
```

これらのプロパティを使用する場合、`CustomProperties`パラメーターからプロパティが省略されていると、それらはデフォルト値を含むことに注意してください。`PersistWBC`プロパティには、**true**または**false**の2つの可能な値があります。

`PersistWBC` プロパティを **true** に設定すると、Citrix Virtual Apps and Desktops 管理者が Citrix Studio を使用してマシンをシャットダウンしても、ライトバックキャッシュディスクは削除されません。

`PersistWBC` プロパティを **false** に設定すると、Citrix Virtual Apps and Desktops 管理者が Citrix Studio を使用してマシンをシャットダウンしたときに、ライトバックキャッシュディスクが削除されます。

注：

`PersistWBC` プロパティが省略されている場合、このプロパティはデフォルトで **false** になり、Citrix Studio を使用してマシンがシャットダウンされると、ライトバックキャッシュは削除されます。

例えば、`CustomProperties` パラメーターを使用して `PersistWBC` をtrueに設定する場合：

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />

</CustomProperties>
```

重要:

`PersistWBC` プロパティは、`New-ProvScheme` PowerShellコマンドレットを使用してのみ設定できます。作成後にプロビジョニングスキームの `CustomProperties` を変更しようと

しても、マシンカタログや、マシンがシャットダウンされたときのライトバックキャッシュディスクの永続性には影響しません。

例えば、`New-ProvScheme`をライトバックキャッシュを使用するように設定し、同時に`PersistWBC`プロパティをtrueに設定する場合：

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistWBC`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127
```

```
-WriteBackCacheMemorySize 256
```

マスターイメージの準備

接続ホストの作成については、「接続とリソース」を参照してください。

マスターイメージには、オペレーティングシステム、仮想化されていないアプリケーション、VDA、およびその他のソフトウェアが含まれています。

知っておくと良いこと:

- マスターイメージは、クローンイメージ、ゴールデンイメージ、ベースVM、またはベースイメージとも呼ばれることがあります。ホストベンダーは異なる用語を使用します。
- Citrix Provisioning を使用する場合、マスターイメージまたは物理コンピューターをマスターターゲットデバイスとして使用できます。Citrix Provisioning は、イメージを参照するために MCS とは異なる用語を使用します。詳細については、Citrix Provisioning のドキュメントを参照してください。
- ホストに、作成されるマシンの数に対応できる十分なプロセッサ、メモリ、ストレージがあることを確認してください。
- デスクトップとアプリケーションに必要なハードディスク容量を正しく構成してください。この値は後で変更したり、マシンカタログで変更したりすることはできません。
- Remote PC Accessのマシンカタログはマスターイメージを使用しません。
- MCSを使用する際のMicrosoft KMSアクティベーションに関する考慮事項: 展開にXenServer 6.1または6.2、vSphere、またはMicrosoft System Center Virtual Machine Managerホストを備えた7.x VDAが含まれている場合、Microsoft WindowsまたはMicrosoft Officeを手動で再アクティブ化する必要はありません。

マスターイメージに以下のソフトウェアをインストールして構成します:

- ハイパーバイザー用の統合ツール（Citrix VM Tools、Hyper-V Integration Services、VMware toolsなど）。この手順を省略すると、アプリケーションやデスクトップが正しく機能しない可能性があります。
- VDA。Citrix は、最新機能にアクセスできるように、最新バージョンのインストールを推奨しています。マスターイメージに VDA をインストールしないと、カタログの作成が失敗します。

- 必要に応じて、アンチウイルスソフトウェアや電子ソフトウェア配布エージェントなどのサードパーティツール。ユーザーとマシンタイプに適した設定（更新機能など）でサービスを構成します。
- 仮想化しないサードパーティアプリケーション。Citrixはアプリケーションの仮想化を推奨します。仮想化により、アプリケーションの追加または再構成後にマスターイメージを更新する必要がなくなるため、コストが削減されます。また、インストールされるアプリケーションが少ないほど、マスターイメージのハードディスクサイズが小さくなり、ストレージコストが節約されます。
- App-Vアプリケーションを公開する予定がある場合は、推奨設定のApp-Vクライアント。App-VクライアントはMicrosoftから入手できます。
- MCSを使用する場合、Microsoft Windowsをローカライズする際は、ロケールと言語パックをインストールしてください。プロビジョニング中にスナップショットが作成されると、プロビジョニングされたVMはインストールされているロケールと言語パックを使用します。

重要:

Citrix Provisioning または MCS を使用している場合は、マスターイメージで Sysprep を実行しないでください。

マスターイメージを準備するには：

1. ハイパーバイザーの管理ツールを使用してマスターイメージを作成し、オペレーティングシステム、すべてのサービスパック、および更新プログラムをインストールします。vCPU の数を指定します。PowerShell を使用してマシンカタログを作成する場合も、vCPU の値を指定できます。Studio を使用してカタログを作成する場合、vCPU の数を指定することはできません。デスクトップとアプリケーションに必要なハードディスク容量を構成します。この値は、後で変更したり、カタログ内で変更したりすることはできません。
2. ハードディスクがデバイスロケーション0に接続されていることを確認します。ほとんどの標準マスターイメージテンプレートでは、この場所がデフォルトで構成されていますが、一部のカスタムテンプレートではそうでない場合があります。
3. 上記のソフトウェアをマスターイメージにインストールして構成します。
4. Citrix Provisioning を使用する場合、マスターターゲットデバイスをドメインに参加させる前に、マスターターゲットデバイスから仮想ディスク用の VHD ファイルを作成します。詳細については、Citrix Provisioning のドキュメントを参照してください。

5. MCSを使用していない場合は、アプリケーションとデスクトップがメンバーであるドメインにマスターイメージを参加させます。マシンが作成されるホストでマスターイメージが利用可能であることを確認します。MCSを使用している場合、マスターイメージをドメインに参加させる必要はありません。プロビジョニングされたマシンは、カタログ作成ウィザードで指定されたドメインに参加します。
6. Citrix は、マスターイメージのスナップショットを作成して名前を付けることを推奨しています。カタログ作成時にスナップショットではなくマスターイメージを指定した場合、Studio はスナップショットを作成します。そのスナップショットに名前を付けることはできません。

Studioを使用してマシンカタログを作成する

カタログ作成ウィザードを開始する前に、このセクションを確認してください。

マスターイメージを使用している場合は、カタログを作成する前に、イメージに VDA がインストールされていることを確認してください。

Studio から:

- サイトをすでに作成しているが、まだマシンカタログを作成していない場合、Studio はカタログを作成するための正しい開始場所に案内します。
- カタログを既に作成していて、別のカタログを作成する場合は、**Studio** ナビゲーションペインで **Machine Catalogs** を選択します。次に、**Actions** ペインで **Create Machine Catalog** を選択します。

ウィザードは、以下の項目について順を追って説明します。表示されるウィザードページは、選択内容によって異なります。

オペレーティングシステム

各カタログには、1種類のマシンのみが含まれます。1つ選択してください。

- **マルチセッションOS:** マルチセッションOSカタログは、ホストされた共有デスクトップを提供します。マシンはサポートされているバージョンのWindowsまたはLinuxオペレーティングシステムを実行できますが、カタログに両方を含めることはできません。（そのOSの詳細については、Linux VDAのドキュメントを参照してください。）
- **シングルセッションOS:** シングルセッションOSカタログは、さまざまなユーザーに割り当てることができるVDIデスクトップを提供します。
- **Remote PC Access:** Remote PC Accessカタログは、ユーザーに物理的なオフィスデスクトップマシンへのリモートアクセスを提供します。Remote PC Accessは、セキュリティを提供するためにVPNを必要としません。

マシン管理

このページは、リモートPCアクセスカタログを作成する際には表示されません。

マシン管理ページには、マシンの管理方法と、マシンの展開に使用するツールが表示されます。

カタログ内のマシンをStudio経由で電源管理するかどうかを選択します。

- マシンはStudio経由で電源管理されます（例：VMまたはブレードPC）。このオプションは、ホストへの接続を既に構成している場合にのみ利用可能です。
- マシンはStudio経由で電源管理されません（例：物理マシン）。

マシンがStudio経由で電源管理されることを指定した場合、VMの作成に使用するツールを選択します。

- **Citrix Machine Creation Services (MCS):** マスターイメージを使用して仮想マシンを作成および管理します。MCSは物理マシンでは利用できません。
- **Citrix Provisioning:** （旧Provisioning Services。）ターゲットデバイスをデバイスコレクションとして管理します。マスターターゲットデバイスからイメージ化されたCitrix Provisioning仮想ディスクが、デスクトップとアプリケーションを提供します。

  > **注：**
  >
  > このオプションはサポートされなくなりました。Citrix Provisioningターゲットデバイスをを Citrix Virtual Apps and Desktopsカタログにインポートするには、**Citrix Provisioning Export Devices Wizard**を使用します。

- **その他:** データセンターに既に存在するマシンを管理するツールです。Citrixでは、カタログ内のマシンの一貫性を確保するために、Microsoft System Center Configuration Managerまたはその他のサードパーティ製アプリケーションを使用することをお勧めします。

デスクトップの種類（デスクトップエクスペリエンス）

このページは、シングルセッションOSマシンを含むカタログを作成している場合にのみ表示されます。

デスクトップエクスペリエンスページでは、ユーザーがログオンするたびに何が起こるかを決定します。次のいずれかを選択します。

- ユーザーはログオンするたびに新しい（ランダムな）デスクトップに接続します。

- ユーザーはログオンするたびに同じ（静的な）デスクトップに接続します。

2番目のオプションを選択し、MCSを使用してマシンをプロビジョニングしている場合は、デスクトップに対するユーザーの変更がどのように処理されるかを構成できます。

- ユーザーの変更をローカルディスク上のデスクトップに保存します。
- ユーザーがログオフしたときに、ユーザーの変更を破棄し、仮想デスクトップをクリアします。ユーザーパーソナライゼーションレイヤーを使用している場合は、このオプションを選択します。

マスターイメージ

このページは、MCSを使用してVMを作成している場合にのみ表示されます。

マスターイメージページで、ホストへの接続を選択し、以前に作成したスナップショットまたはVMを選択します。最初のカタログを作成している場合、利用可能な接続は、サイトを作成したときに構成した接続のみです。

注意：

- MCSまたはCitrix Provisioningを使用している場合、マスターイメージでSysprepを実行しないでください。
- スナップショットではなくマスターイメージを指定した場合、Studioはスナップショットを作成しますが、名前を付けることはできません。

最新の製品機能を使用できるようにするには、マスターイメージに最新のVDAバージョンがインストールされていることを確認してください。デフォルトの最小VDA選択を変更しないでください。ただし、以前のVDAバージョンを使用する必要がある場合は、「VDAバージョンと機能レベル」を参照してください。

ウィザードで以前に選択したマシン管理テクノロジーと互換性のないスナップショットまたはVMを選択すると、エラーメッセージが表示されます。

デバイスコレクション

このページは、Citrix Provisioning を使用してVMを作成する場合にのみ表示されます。

デバイスコレクションページには、デバイスコレクションと、まだカタログに追加されていないデバイスが表示されます。

使用するデバイスコレクションを選択します。

マシン

リモートPCアクセス カタログを作成している場合、このページは表示されません。

このページのタイトルは、**マシン管理**ページで選択した内容（**マシン**、**仮想マシン**、または**VMとユーザー**）によって異なります。

MCSを使用する場合：

- 作成する仮想マシンの数を指定します。
- 各 VM が持つメモリ量 (MB 単位) を選択します。
- 作成された各VMにはハードディスクがあります。そのサイズはマスターイメージで設定されます。カタログでハードディスクのサイズを変更することはできません。
- 展開に複数のゾーンが含まれている場合、カタログのゾーンを選択できます。
- 静的デスクトップVMを作成する場合は、仮想マシンコピーモードを選択します。「仮想マシンコピーモード」を参照してください。
- vDiskを使用しないランダムデスクトップVMを作成する場合は、各マシンの一時データに使用するキャッシュを構成できます。「一時データ用のキャッシュの構成」を参照してください。

Citrix Provisioningを使用する場合：

デバイスページには、前のウィザードページで選択したデバイスコレクション内のマシンが一覧表示されます。このページでマシンを追加または削除することはできません。

その他のツールを使用する場合：

Active Directoryマシンアカウント名を追加（またはリストをインポート）します。VMを追加/インポートした後、そのVMのActive Directoryアカウント名を変更できます。「**デスクトップエクスペリエンス**」ページで静的マシンを指定した場合、追加する各VMのActive Directoryユーザー名をオプションで指定できます。

名前を追加またはインポートした後、このページにいる間は「**削除**」ボタンを使用してリストから名前を削除できます。

Citrix Provisioningまたはその他のツールを使用する場合（MCS以外）：

追加された（またはインポートされた、あるいはCitrix Provisioningデバイスコレクションからの）各マシンに表示されるアイコンとツールヒントは、カタログに追加できない可能性のあるマシンや、Delivery Controllerに登録できないマシンを特定するのに役立ちます。詳細については、「VDAのバージョンと機能レベル」を参照してください。

仮想マシンのコピーモード

「**マシン**」ページで指定するコピーモードによって、MCSがマスターイメージからシン（高速コピー）クローンを作成するか、シック（完全コピー）クローンを作成するかが決まります。（デフォルト = シンクローン）

- ストレージをより効率的に使用し、マシンの作成を高速化するには、高速コピーのクローンを使用します。
- マシン作成後のIOPSを削減できる可能性があり、より優れたデータ回復と移行サポートのために、完全コピーのクローンを使用します。

VDAのバージョンと機能レベル

カタログの機能レベルは、カタログ内のマシンで利用できる製品機能を制御します。新しい製品バージョンで導入された機能を使用するには、新しいVDAが必要です。機能レベルを設定すると、そのバージョンで導入されたすべての機能（および機能レベルが変更されない場合はそれ以降のバージョンで導入された機能）がカタログ内のマシンで利用可能になります。ただし、そのカタログ内の以前のVDAバージョンのマシンは登録できません。

「**マシン**」（または「**デバイス**」）ページの下部にあるメニューで、最小VDAレベルを選択できます。これにより、カタログの最小機能レベルが設定されます。デフォルトでは、オンプレミス展開の場合、最新の機能レベルが選択されています。Citrixの推奨に従って、常にVDAとコアコンポーネントを最新バージョンにインストールおよびアップグレードする場合は、この選択を変更する必要はありません。ただし、古いVDAバージョンを使い続ける必要がある場合は、正しい値を選択してください。

Citrix Virtual Apps and Desktopsのリリースには、新しいVDAバージョンが含まれていない場合や、新しいVDAが機能レベルに影響を与えない場合があります。そのような場合、機能レベルは、インストールまたはアップグレードされたコンポーネントよりも古いVDAバージョンを示すことがあります。たとえば、バージョン7.17には7.17 VDAが含まれていますが、デフォルトの機能レベル（「7.9以降」）は最新のままです。したがって、コンポーネント7.9～7.16を7.17にインストールまたはアップグレードした後も、デフォルトの機能レベルを変更する必要はありません。各リリースの「新機能」の記事には、デフォルトの機能レベルの変更が示されています。

選択された機能レベルは、その上にあるマシンのリストに影響します。リストでは、各エントリの横にあるツールヒントが、その機能レベルでマシンのVDAがカタログと互換性があるかどうかを示します。

各マシンのVDAが選択された最小機能レベルを満たしていないか、超えていない場合、ページにメッセージが表示されます。ウィザードを続行できます。それらのマシンは、後でControllerに登録できない可能性があります。または、次のことができます。

- 古いVDAを含むマシンをリストから削除し、VDAをアップグレードしてから、カタログに再度追加します。
- 最新の製品機能へのアクセスを妨げる、より低い機能レベルを選択します。

マシンタイプが正しくないためにマシンがカタログに追加されなかった場合も、メッセージが表示されます。例としては、シングルセッションOSカタログにサーバーを追加しようとしたり、ランダム割り当て用に作成されたシングルセッションOSマシンを静的マシンのカタログに追加したりする場合があります。

> **重要:**

> リリース1811で、追加の機能レベル「**1811（またはそれ以降）**」が追加されました。このレベルは、将来のCitrix Virtual Apps and Desktops機能で使用することを目的としています。「**7.9（またはそれ以降）**」の選択はデフォルトのままです。このデフォルトは、現在すべての展開で有効です。

> **1811 (またはそれ以降)** を選択した場合、そのカタログ内の以前のVDAバージョンはControllerに登録できません。ただし、カタログにバージョン1811以降のサポートされているVDAのみが含まれている場合は、すべて登録可能です。これには、バージョン1903および現在のリリースより前のその他の19XXリリースを含む、後のCitrix Virtual Apps and Desktopsリリース用に構成されたVDAを含むカタログも含まれます。

一時データのキャッシュを構成する

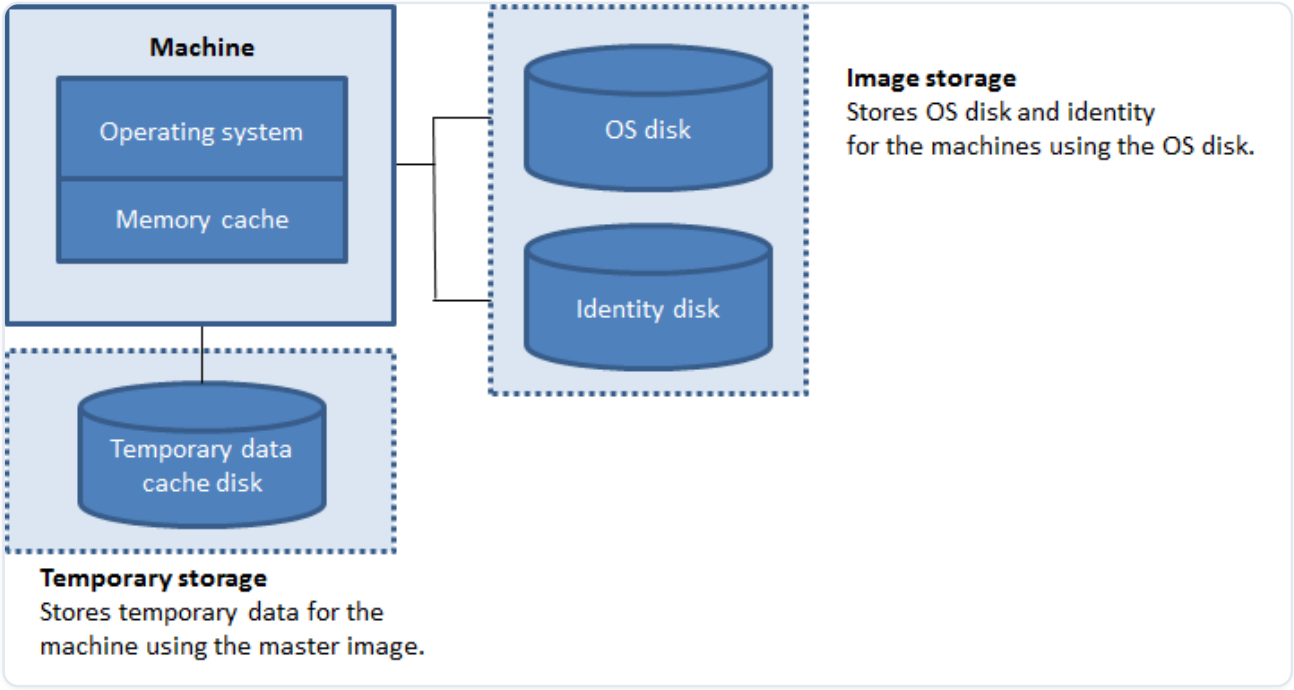
VMに一時データをローカルでキャッシュすることはオプションです。MCSを使用してカタログ内のプールされた（専用ではない）マシンを管理する場合、マシン上の一時データキャッシュの使用を有効にできます。カタログが一時データのストレージを指定する接続を使用している場合、カタログの作成時に一時データキャッシュ情報を有効にして構成できます。

> **重要:**

> この機能には、最新のMCS I/Oドライバーが必要です。このドライバーのインストールは、VDAをインストールまたはアップグレードする際のオプションです。デフォルトでは、このドライバーはインストールされていません。

カタログが使用する接続を作成するときに、一時データが共有ストレージとローカルストレージのどちらを使用するかを指定します。詳しくは、「接続とリソース」を参照してください。各マシンの一時データキャッシュを構成するには、次の2つのオプションを使用できます。**キャッシュに割り当てられるメモリ (MB)** と **ディスクキャッシュサイズ (GB)**。デフォルトでは、この2つのオプションはクリアされています。キャッシュに割り当てられるメモリ (MB) オプションを有効にするには、ディスクキャッシュサイズ (GB) チェックボックスをオンにします。**ディスクキャッシュサイズ** チェックボックスが選択されていない場合、キャッシュに割り当てられるメモリ オプションはグレー表示されます。接続の種類によっては、これらのオプションのデフォルト値が異なる場合があります。一般的に、デフォルト値はほとんどの場合に十分です。ただし、以下のために必要な領域を考慮してください。

- Windows自体によって作成される一時データファイル（Windowsページファイルを含む）。
- ユーザープロファイルデータ。
- ユーザーのセッションに同期されるShareFileデータ。
- セッションユーザーまたはユーザーがセッション内にインストールする可能性のあるアプリケーションによって作成またはコピーされる可能性のあるデータ。



各マシンの一時データキャッシュを構成するには、以下の3つのシナリオに注意してください。

- ディスクキャッシュサイズチェックボックスとメモリ割り当てキャッシュチェックボックスを選択しない場合、一時データはキャッシュされません。各VMの差分ディスク（OSストレージにあります）に直接書き込まれます。（これはバージョン7.8以前のプロビジョニングアクションです。）

- ディスクキャッシュサイズチェックボックスを選択し、メモリ割り当てキャッシュチェックボックスを選択しない場合、一時データは最小限のメモリキャッシュを使用して、キャッシュディスクに直接書き込まれます。
- ディスクキャッシュサイズチェックボックスとメモリ割り当てキャッシュチェックボックスを選択した場合、一時データは最初にメモリキャッシュに書き込まれます。メモリキャッシュが構成された制限（キャッシュに割り当てられるメモリ値）に達すると、最も古いデータは一時データキャッシュディスクに移動されます。

重要:

- ディスクキャッシュの容量が不足すると、ユーザーセッションは使用できなくなります。
- この機能は、Nutanixホスト接続を使用している場合は利用できません。
- マシン作成後、マシンカタログのキャッシュ値を変更することはできません。

注：

- メモリキャッシュは、各マシンの合計メモリ量の一部です。したがって、キャッシュに割り当てられるメモリ オプションを有効にする場合は、各マシンの合計メモリ量を増やすことを検討してください。
- ディスクキャッシュサイズをデフォルト値から変更すると、パフォーマンスに影響を与える可能性があります。サイズは、ユーザー要件とマシンにかかる負荷に合わせる必要があります。

NIC

リモートPCアクセス カタログを作成している場合、このページは表示されません。

「**ネットワークインターフェイスカード**」ページで、複数のNICを使用する予定がある場合は、各カードに仮想ネットワークを関連付けます。たとえば、1つのカードを特定のセキュアネットワークへのアクセスに割り当て、別のカードをより一般的に使用されるネットワークへのアクセスに割り当てることができます。このページからNICを追加または削除することもできます。

マシンアカウント

このページは、リモートPCアクセス カタログを作成する場合にのみ表示されます。

「**マシンアカウント**」ページで、ユーザーまたはユーザーグループに対応するActive Directoryマシンアカウントまたは組織単位（OU）を指定します。OU名にスラッシュ（/）を使用しないでください。

以前に構成した電源管理接続を選択するか、電源管理を使用しないことを選択できます。電源管理を使用したいが、適切な接続がまだ構成されていない場合は、後でその接続を作成し、マシンカタログを編集して電源管理設定を更新できます。

コンピューターアカウント

このページは、MCSを使用してVMを作成する場合にのみ表示されます。

カタログ内の各マシンには、対応するActive Directoryコンピューターアカウントが必要です。「**コンピューターアカウント**」ページで、アカウントを作成するか既存のアカウントを使用するか、およびそれらのアカウントの場所を指定します。

- アカウントを作成する場合、マシンが存在するOUでコンピューターアカウントを作成する権限が必要です。

  マシンのアカウント命名スキームを指定します。連続する数字または文字が表示される場所を示すには、ハッシュマークを使用します。OU名にスラッシュ（/）を使用しないでください。名前は数字で始めることはできません。たとえば、PC-Sales-##（0～9を選択）という命名スキームでは、PC-Sales-01、PC-Sales-02、PC-Sales-03などのコンピューターアカウントが作成されます。
- 既存のアカウントを使用する場合は、アカウントを参照するか、**インポート**をクリックしてアカウント名を含む.csvファイルを指定します。インポートするファイルの内容は、次の形式を使用する必要があります。

```
[ADComputerAccount]

ADcomputeraccountname.domain

...
```

追加するすべてのマシンに対して十分なアカウントがあることを確認してください。Studioがこれらのアカウントを管理するため、Studioがすべてのアカウントのパスワードをリセットすることを許可するか、すべてのアカウントで同じパスワードを指定してください。

物理マシンまたは既存のマシンを含むカタログの場合、既存のアカウントを選択またはインポートします。各マシンをActive Directoryコンピューターアカウントとユーザーアカウントの両方に割り当てます。

Citrix Provisioningで作成されたマシンの場合、ターゲットデバイスのコンピューターアカウントは異なる方法で管理されます。Citrix Provisioningのドキュメントを参照してください。

概要、名前、および説明

概要ページで、指定した設定を確認します。カタログの名前と説明を入力します。この情報はStudioに表示されます。

完了したら、**完了**をクリックしてカタログ作成を開始します。

トラブルシューティング

> **重要:**

> Citrix Studio を使用してマシンカタログを作成した後、`Get-ProvTask` PowerShell コマンドを使用して、マシンカタログ作成に関連するタスクを取得することはできません。この制限は、カタログが正常に作成されたかどうかにかかわらず、Studio がマシンカタログ作成後にそれらのタスクを削除するためです。

> Citrix では、サポートチームが解決策を提供できるよう、ログを収集することをお勧めします。Citrix Provisioning を使用している場合は、次の手順でログファイルを生成します。

1. マスターイメージで、値 1 (DWORD (32 ビット) 値として) を持つ次のレジストリキーを作成します: `HKLM\Software\Citrix\MachineIdentityServiceAgent\LOGGING`。
2. マスターイメージをシャットダウンし、スナップショットを作成します。
3. Delivery Controller で、次の PowerShell コマンドを実行します: `Set-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown -Value $True`。
4. そのスナップショットに基づいてカタログを作成します。
5. ハイパーバイザー上に準備 VM が作成されたら、ログインして `C:\` のルートから次のファイル (Image-prep.log および PvsVmAgentLog.txt) を抽出します。
6. マシンをシャットダウンすると、その時点で障害が報告されます。

7. イメージ準備マシンの自動シャットダウンを再度有効にするには、次の PowerShell コマンドを実行します: `Remove-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown`。

次のステップ

これが最初に作成されたカタログである場合、Studio は デリバリーグループの作成 に誘導します。

マシンカタログを管理する

はじめに

マシンカタログへのマシンの追加または削除、名前の変更、説明の変更、またはカタログのActive Directoryコンピューターアカウントの管理を行うことができます。

カタログの保守には、各マシンが最新のOSアップデートを適用していることを確認することも含まれます。これには、ウイルス対策の更新、オペレーティングシステムのアップグレード、または構成の変更が含まれます。

- Machine Creation Services™ (MCS) を使用して作成されたプールされたランダムマシンを含むカタログは、カタログで使用されるマスターイメージを更新し、その後マシンを更新することでマシンを保守します。この方法により、多数のユーザーマシンを効率的に更新できます。
- Citrix Provisioning™ を使用して作成されたマシンでは、マシンの更新は仮想ディスクを介して伝播されます。詳細については、Citrix Provisioning のドキュメントを参照してください。
- 静的で永続的に割り当てられたマシンを含むカタログ、およびリモートPCアクセス マシンカタログの場合、ユーザーのマシンへの更新はStudioの外部で管理します。このタスクは、個別に、またはサードパーティのソフトウェア配布ツールを使用してまとめて実行します。

ホストハイパーバイザーへの接続の作成と管理については、「接続とリソース」を参照してください。

> **注：**

> MCSはWindows 10 IoT CoreおよびWindows 10 IoT Enterpriseをサポートしていません。詳細については、Microsoftサイトを参照してください。

永続インスタンスについて

永続的または専用インスタンスを使用して作成されたMCSカタログを更新する場合、カタログ用に作成された新しいマシンはすべて更新されたイメージを使用します。既存のインスタンスは引き続き元のインスタンスを使用します。イメージの更新プロセスは、他の種類のカタログと同じ方法で行われます。以下を考慮してください。

- 永続ディスクカタログの場合、既存のマシンは新しいイメージに更新されませんが、カタログに追加される新しいマシンは新しいイメージを使用します。
- 非永続ディスクカタログの場合、マシンイメージはマシンがリセットされる次回のタイミングで更新されます。
- 永続マシンカタログの場合、イメージを更新すると、それを使用するカタログインスタンスも更新されます。
- 永続化しないカタログの場合、異なるマシンに異なるイメージを使用したい場合は、イメージは別々のカタログに存在する必要があります。

マシンをカタログに追加する

開始する前に:

- 仮想化ホストに、追加のマシンを収容するのに十分なプロセッサ、メモリ、ストレージがあることを確認してください。
- 未使用のActive Directoryコンピューターアカウントが十分にあることを確認してください。既存のアカウントを使用している場合、追加できるマシンの数は利用可能なアカウントの数によって制限されます。
- Studioを使用して追加のマシン用のActive Directoryコンピューターアカウントを作成する場合、適切なドメイン管理者権限が必要です。

カタログにマシンを追加するには:

1. **Studio** ナビゲーションペインで、**マシンカタログ** を選択します。
2. マシンカタログを選択し、**操作** ペインで **マシンの追加** を選択します。
3. 追加する仮想マシンの数を選択します。
4. 追加するVMの数に対して既存のActive Directoryアカウントが不足している場合は、アカウントが作成されるドメインと場所を選択します。連続する数字または文字が表示される場所を示すには、ハッシュマークを使用してアカウントの命名スキームを指定します。OU名にスラッシュ（/）を使用しないでください。名前は数字で始めることはできません。たとえば、PC-

Sales-##（0-9を選択）という命名スキームでは、PC-Sales-01、PC-Sales-02、PC-Sales-03などのコンピューターアカウントが作成されます。

5. 既存のActive Directoryアカウントを使用する場合は、アカウントを参照するか、**インポート**をクリックしてアカウント名を含む.csvファイルを指定します。追加するすべてのマシンに対して十分なアカウントがあることを確認してください。Studioはこれらのアカウントを管理します。Studioにすべてのアカウントのパスワードをリセットさせるか、すべてのアカウントで同じである必要があるアカウントパスワードを指定します。

マシンはバックグラウンドプロセスとして作成され、多数のマシンを作成する場合は時間がかかることがあります。Studioを閉じてもマシンの作成は続行されます。

カタログからマシンを削除する

マシンカタログからマシンを削除すると、ユーザーはそのマシンにアクセスできなくなるため、マシンを削除する前に、以下を確認してください。

- ユーザーデータがバックアップされているか、不要になっていること。
- すべてのユーザーがログオフしていること。メンテナンスモードをオンにすると、マシンへの新しい接続が停止します。
- マシンが電源オフになっていること。

カタログからマシンを削除するには：

1. **Studio** ナビゲーションペインで、**マシンカタログ** を選択します。
2. カタログを選択し、**操作** ペインで **マシンの表示** を選択します。
3. 1つ以上のマシンを選択し、**操作** ペインで **削除** を選択します。

削除するマシンを削除するかどうかを選択します。マシンを削除することを選択した場合は、それらのマシンのActive Directoryアカウントを保持するか、無効にするか、削除するかを指定します。

カタログの説明を変更するか、リモートPCアクセス設定を変更する

1. **Studio** ナビゲーションペインで、**マシンカタログ** を選択します。
2. カタログを選択し、**操作** ペインで **マシンカタログの編集** を選択します。
3. リモートPCアクセス カタログの場合、**電源管理** ページを使用して電源管理設定を変更し、電源管理接続を選択します。**組織単位** ページで、Active Directory OUを追加または削除します。
4. **説明**ページで、カタログの説明を変更します。

カタログの名前を変更する

1. **Studio** ナビゲーションペインで、**マシンカタログ** を選択します。
2. カタログを選択し、**操作** ペインで **マシンカタログの名前変更** を選択します。
3. 新しい名前を入力します。

カタログを別のゾーンに移動する

展開に複数のゾーンがある場合、カタログをあるゾーンから別のゾーンに移動できます。

カタログ内のVMを含むハイパーバイザーとは異なるゾーンにカタログを移動すると、パフォーマンスに影響します。

1. 「**Studio**」ナビゲーションペインで、**マシンカタログ**を選択します。
2. カタログを選択し、「**Actions**」ペインで**移動**を選択します。
3. カタログを移動するゾーンを選択します。

カタログを削除する

カタログを削除する前に、以下を確認してください。

- すべてのユーザーがログオフされ、切断されたセッションが実行されていないこと。
- カタログ内のすべてのマシンでメンテナンスモードがオンになっており、新しい接続が確立できないこと。
- カタログ内のすべてのマシンが電源オフになっていること。
- カタログはデリバリーグループに関連付けられていません。つまり、デリバリーグループにはそのカタログのマシンが含まれていません。

カタログを削除するには：

1. 「**Studio**」ナビゲーションペインで、**マシンカタログ**を選択します。
2. カタログを選択し、「**Actions**」ペインで**マシンカタログの削除**を選択します。
3. カタログ内のマシンを削除するかどうかを指定します。マシンを削除することを選択した場合、それらのマシンのActive Directoryコンピューターアカウントを保持するか、無効にするか、削除するかを指定します。

カタログ内のActive Directoryコンピューターアカウントを管理する

マシンカタログ内のActive Directoryアカウントを管理するには、次の操作を実行できます。

- シングルセッションOSおよびマルチセッションOSカタログからActive Directoryコンピューターアカウントを削除して、未使用のマシンアカウントを解放します。これらのアカウントは、他のマシンに使用できます。
- カタログにマシンが追加されたときにコンピューターアカウントがすでに存在するように、アカウントを追加します。OU名にスラッシュ（/）を使用しないでください。

Active Directoryアカウントを管理するには：

1. 「**Studio**」ナビゲーションペインで、**マシンカタログ**を選択します。
2. カタログを選択し、「**Actions**」ペインで**ADアカウントの管理**を選択します。
3. コンピューターアカウントを追加するか削除するかを選択します。アカウントを追加する場合は、アカウントのパスワードをどうするかを指定します。すべてリセットするか、すべてのアカウントに適用されるパスワードを入力します。

   現在のアカウントパスワードが不明な場合は、パスワードをリセットできます。パスワードのリセットを実行する権限が必要です。パスワードを入力すると、アカウントがインポートされるときにパスワードが変更されます。アカウントを削除するときは、Active Directory内のアカウントを保持するか、無効にするか、削除するかを選択します。

カタログからマシンを削除したり、カタログを削除したりする際に、Active Directoryアカウントを保持するか、無効にするか、削除するかを指定します。

カタログを更新する

カタログ内のマシンを更新する前に、マスターイメージのコピーまたはスナップショットを保存することをお勧めします。データベースは、各マシンカタログで使用されたマスターイメージの履歴レコードを保持します。カタログ内のマシンをロールバックまたは元に戻して、マスターイメージの以前のバージョンを使用します。ユーザーがデスクトップに展開した更新プログラムで問題が発生した場合に、このタスクを実行します。これにより、ユーザーのダウンタイムが最小限に抑えられます。マスターイメージを削除、移動、または名前変更しないでください。それらを使用してカタログを元に戻すことはできません。

Citrix Provisioning（旧Provisioning Services）を使用するカタログの場合、カタログに変更を適用するには、新しい仮想ディスクを公開する必要があります。詳しくは、Citrix Provisioningのドキュメントを参照してください。

マシンが更新されると、自動的に再起動します。

マスターイメージを更新または作成する

マシンカタログを更新する前に、既存のマスターイメージを更新するか、ホストハイパーバイザー上に新しいマスターイメージを作成します。

1. ハイパーバイザーで、現在のVMのスナップショットを取得し、そのスナップショットに意味のある名前を付けます。このスナップショットは、必要に応じてカタログ内のマシンを元に戻す（ロールバックする）ために使用できます。
2. 必要に応じて、マスターイメージの電源をオンにし、ログオンします。
3. 更新プログラムをインストールするか、マスターイメージに必要な変更を加えます。
4. VMの電源をオフにします。
5. VMのスナップショットを作成します。Studioでカタログが更新されたときに認識されるような、意味のある名前を付けます。Studioでスナップショットを作成できますが、Citrixではハイパーバイザー管理コンソールを使用して作成することをお勧めします。その後、Studioでそのスナップショットを選択します。このプロセスにより、自動生成された名前ではなく、意味のある名前と説明を提供できます。GPUマスターイメージの場合、マスターイメージはCitrix Hypervisor™コンソールからのみ変更できます。

カタログを更新する

カタログ内のすべてのマシンに更新プログラムを準備して展開するには：

1. 「**Studio**」ナビゲーションペインで、**マシンカタログ**を選択します。
2. カタログを選択し、「**Actions**」ペインで**マシンの更新**を選択します。
3. 「**Master Image**」ページで、展開するホストとイメージを選択します。
4. 「**展開戦略**」ページで、マシンカタログ内のマシンを新しいマスターイメージで更新するタイミング（次回のシャットダウン時または即時）を選択します。
5. 「**概要**」ページで情報を確認し、「**完了**」をクリックします。各マシンは更新後に自動的に再起動します。

StudioではなくPowerShell SDKを直接使用してカタログを更新する場合、ハイパーバイザーテンプレート（VMテンプレート）を指定します。これは、イメージまたはイメージのスナップショットの代替として使用します。

展開戦略：

次回のシャットダウン時にイメージを更新すると、現在使用されていないマシン、つまりアクティブなユーザーセッションがないマシンにすぐに影響します。使用中のシステムは、現在のアクティブセッションが終了したときに更新を受け取ります。以下を考慮してください。

- 該当するマシンでの更新が完了するまで、新しいセッションを起動することはできません。
- シングルセッションOSマシンでは、マシンが使用されていないとき、またはユーザーがログオンしていないときに、マシンはすぐに更新されます。
- 子マシンを持つマルチセッションOSの場合、再起動は自動的に行われません。更新されたマスターイメージを適用するには、Studio、PowerShell、またはWorkspaceを使用してマシンを再起動します。マシンまたはハイパーバイザーからの再起動では、更新は適用されません。

> **ヒント:**
>
> ホスト接続の詳細設定を使用して、再起動されるマシンの数を制限します。これらの設定を使用して、特定のカタログに対して実行されるアクションを変更します。詳細設定はハイパーバイザーによって異なります。

> イメージをすぐに更新することを選択した場合は、配布時間と通知を設定します。

- **配布時間:** すべてのマシンを同時に更新するか、カタログ内のすべてのマシンの更新を開始する合計時間を指定します。内部アルゴリズムにより、その間隔中に各マシンがいつ更新および再起動されるかが決定されます。
- **通知:** 左側の通知ドロップダウンメニューで、更新が開始される前にマシンに通知メッセージを表示するかどうかを選択します。デフォルトでは、メッセージは表示されません。更新が開始される15分前にメッセージを表示することを選択します。または、最初のメッセージの後に5分ごとにメッセージを繰り返すことを選択します。デフォルトでは、メッセージは繰り返されません。すべてのマシンを同時に更新することを選択しない限り、通知メッセージは更新が開始される前の適切なタイミングで各マシンに表示されます。

更新をロールバックする

更新された/新しいマスターイメージを展開した後、それをロールバックできます。このプロセスは、新しく更新されたマシンで問題が発生した場合に必要になることがあります。ロールバックすると、カタログ内のマシンは最後に機能していたイメージにロールバックされます。新しいイメージを必要とする新機能は利用できなくなります。展開と同様に、マシンのロールバックには再起動が含まれます。

1. **Studio** ナビゲーションペインで を選択します。
2. カタログを選択し、 ペインで を選択します。
3. 展開操作の前のセクションで説明されているように、以前のマスターイメージをマシンに適用するタイミングを指定します。

ロールバックは、元に戻す必要があるマシンにのみ適用されます。新しい/更新されたマスターイメージで更新されていないマシンは、通知メッセージを受信せず、強制的にログオフされることもありません。

カタログをアップグレードまたはアップグレードを元に戻す

マシンのVDAを新しいバージョンにアップグレードした後、マシンカタログをアップグレードします。Citrix®は、すべての最新機能にアクセスできるように、すべてのVDAを最新バージョンにアップグレードすることを推奨しています。

カタログをアップグレードする前に:

- Citrix Provisioningを使用している場合は、VDAバージョンをアップグレードします。プロビジョニングコンソールはVDAバージョンを保持しません。Citrix Provisioningは、Citrix Virtual Apps and Desktops™セットアップウィザードと直接通信して、作成されたカタログのVDAバージョンを設定します。
- アップグレードされたマシンを起動して、Controllerに登録させます。このプロセスにより、Studioはカタログ内のマシンがアップグレードを必要としていることを判断できます。

カタログをアップグレードするには:

1. **Studio**ナビゲーションペインで、**マシンカタログ**を選択します。
2. カタログを選択します。下ペインの**「詳細」**タブにバージョン情報が表示されます。
3. **カタログのアップグレード**を選択します。Studioがカタログのアップグレードが必要であると検出した場合、メッセージが表示されます。プロンプトに従います。1つ以上のマシンをアップグレードできない場合、その理由を説明するメッセージが表示されます。Citrixは、すべてのマシンが適切に機能するように、カタログをアップグレードする前にマシンの問題を解決することを推奨します。

カタログのアップグレードが完了したら、カタログを選択し、**操作**ペインで**元に戻す**を選択することで、マシンを以前のVDAバージョンに戻すことができます。

既存のプロビジョニングスキームのネットワーク設定を変更する

既存のプロビジョニングスキームのネットワーク設定を変更して、新しいVMが新しいサブネットワーク上に作成されるようにすることができます。ネットワーク設定を変更するには、`Set-ProvScheme`コマンドで`-NetworkMapping`パラメーターを使用します。

> **注：**

この機能は、Citrix Virtual Apps and Desktops 2203 LTSR CU3以降のバージョンでサポートされています。

既存のプロビジョニングスキームのネットワーク設定を変更するには、次の手順を実行します。

1. PowerShellウィンドウで、コマンド `asnp citrix*` を実行してPowerShellモジュールをロードします。
2. 変更するネットワークパスに移動するには、`(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` を実行します。
3. 新しいネットワーク設定に変数を割り当てます。例:

```
$NewNetworkMap = @{“0”= “XDHYP:\HostingUnits\MyNetworks\Network 0.network”}
```

4. `Set-ProvScheme -ProvisioningSchemeName "name" -NetworkMapping $NewNetworkMap` を実行します。
5. 既存のプロビジョニングスキームの新しいネットワーク設定を確認するには、`(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` を実行します。

トラブルシューティング

- 「Power State Unknown」ステータスのマシンについては、ガイダンスとしてCTX131267を参照してください。
- 不明な電源状態を継続的に表示するVMを修正するには、How to fix VMs that continuously show an unknown power stateを参照してください。

デリバリーグループの作成

デリバリーグループは、1つ以上のマシンカタログから選択されたマシンのコレクションです。デリバリーグループは、どのユーザーがそれらのマシンを使用できるか、およびそれらのユーザーが利用できるアプリケーションとデスクトップを指定します。

デリバリーグループの作成は、サイトの作成とマシンカタログの作成の後、展開を構成する次のステップです。後で、最初のデリバリーグループの初期設定を変更したり、他のデリバリーグループを作成したりできます。デリバリーグループの作成時ではなく、編集時にのみ構成できる機能と設定もあります。

Remote PC Accessの場合、サイトを作成すると、「Remote PC Access Desktops」という名前のデリバリーグループが自動的に作成されます。

デリバリーグループを作成するには：

1. サイトとマシンカタログを作成したが、デリバリーグループを作成していない場合、Studioはデリバリーグループを作成するための正しい開始場所に案内します。すでにデリバリーグループを作成していて、別のデリバリーグループを作成したい場合は、**Delivery Groups**を選択します。アクションペインで**Create Delivery Group**を選択します。
2. ウィザードは**Introduction**ページから起動します。このページは、今後のウィザードの起動時に表示しないように設定できます。
3. その後、ウィザードは次のセクションで説明されているページを案内します。各ページの作業が完了したら、**Next**をクリックして最後のページに進みます。

ステップ1. マシン

Machinesページで、カタログを選択し、そのカタログから使用するマシンの数を選択します。

知っておくと良いこと:

- 選択したカタログでは、少なくとも1台のマシンが未使用のまま残っている必要があります。
- カタログは複数のデリバリーグループで指定できます。マシンは1つのデリバリーグループでのみ使用できます。
- デリバリーグループは複数のカタログのマシンを使用できますが、それらのカタログには同じマシンタイプ（マルチセッションOS、シングルセッションOS、またはRemote PC Access）が含まれている必要があります。つまり、デリバリーグループ内でマシンタイプを混在させることはできません。同様に、展開にWindowsマシンのカタログとLinuxマシンのカタログがある場合、デリバリーグループにはどちらかのOSタイプのマシンを含めることができますが、両方を含めることはできません。
- Citrixは、すべてのマシンを最新のVDAバージョンでインストールまたはアップグレードすることを推奨します。必要に応じて、カタログとデリバリーグループをアップグレードしてください。デリバリーグループを作成する際に、異なるVDAバージョンがインストールされているマシンを選択した場合、デリバリーグループは最も古いVDAバージョンと互換性があります。これはグループの*機能レベル*と呼ばれます。たとえば、いずれかのマシンにVDAバージョン7.1がインストールされており、他のマシンに現在のバージョンがインストールされている場合、グループ内のすべてのマシンはVDA 7.1でサポートされていた機能のみを使用できます。これは、より新しいVDAバージョンを必要とする一部の機能がそのデリバリーグループでは利用できない可能性があることを意味します。

- Remote PC Accessカタログ内の各マシンは、自動的にデリバリーグループに関連付けられます。Remote PC Accessサイトを作成すると、「Remote PC Access Machines」という名前のカタログと「Remote PC Access Desktops」という名前のデリバリーグループが自動的に作成されます。
- 以下の互換性チェックが実行されます。
  - MinimumFunctionalLevelは互換性がある必要があります
  - SessionSupportは互換性がある必要があります
  - AllocationTypeはSingleSessionと互換性がある必要があります
  - ProvisioningType` は互換性がある必要があります
  - PersistChanges はMCSおよびCitrix Provisioning™と互換性がある必要があります
  - RemotePCカタログはRemotePCカタログとのみ互換性があります。
  - AppDisk関連の確認

ステップ2. 配信の種類

このページは、静的（割り当て済み）シングルセッションOSマシンを含むカタログを選択した場合にのみ表示されます。

配信の種類ページで、**アプリケーション**または**デスクトップ**のいずれかを選択します。両方を有効にすることはできません。

マルチセッションOSまたはシングルセッションOSのランダム（プールされた）カタログからマシンを選択した場合、配信の種類はアプリケーションとデスクトップであると見なされます。アプリケーション、デスクトップ、またはその両方を配信できます。

ステップ3. ユーザー

デリバリーグループ内のアプリケーションとデスクトップを使用できるユーザーとユーザーグループを指定します。

ユーザーリストが指定される場所

Active Directoryユーザーリストは、以下を作成または編集する際に指定されます。

- Studioを介して構成されていないサイトのユーザーアクセスリスト。デフォルトでは、アプリケーションエンタイトルメントポリシー規則には全員が含まれます。詳細については、PowerShell SDK `BrokerAppEntitlementPolicyRule` コマンドレットを参照してください。
- アプリケーショングループ（構成されている場合）。

- デリバリーグループ。
- アプリケーション。

StoreFront™を介してアプリケーションにアクセスできるユーザーのリストは、上記のユーザーリストの交差によって形成されます。たとえば、他のグループへのアクセスを不当に制限することなく、特定の部門にアプリケーションAの使用を構成するには、次の手順を実行します。

- 全員を含むデフォルトのアプリケーションエンタイトルメントポリシー規則を使用します。
- デリバリーグループのユーザーリストを構成して、すべての本社ユーザーがデリバリーグループで指定された任意のアプリケーションを使用できるようにします。
- (アプリケーショングループが構成されている場合) アプリケーショングループのユーザーリストを構成して、管理および財務ビジネスユニットのメンバーがアプリケーションAからLにアクセスできるようにします。
- アプリケーションAのプロパティを構成して、その可視性を管理および財務部門の経理担当者のみに制限します。

認証済みユーザーと未認証ユーザー

ユーザーには、認証済みユーザーと未認証ユーザーの2種類があります（未認証ユーザーは匿名ユーザーとも呼ばれます）。デリバリーグループでは、いずれか一方または両方の種類のユーザーを構成できます。

- **認証済み:** アプリケーションとデスクトップにアクセスするには、名前で指定したユーザーとグループメンバーが、StoreFrontまたはCitrix Workspace™ appにスマートカードやユーザー名とパスワードなどの資格情報を提示する必要があります。シングルセッションOSマシンを含むデリバリーグループの場合、後でデリバリーグループを編集してユーザーデータ（ユーザーのリスト）をインポートできます。
- **未認証（匿名）:** マルチセッションOSマシンを含むデリバリーグループの場合、ユーザーがStoreFrontまたはCitrix Workspace appに資格情報を提示せずにアプリケーションとデスクトップにアクセスできるようにすることができます。たとえば、キオスクではアプリケーションが資格情報を要求する場合がありますが、Citrixアクセス ポータルとツールは要求しません。最初のDelivery Controllerをインストールすると、匿名ユーザーグループが作成されます。

  未認証ユーザーにアクセスを許可するには、デリバリーグループ内の各マシンにWindows Server OS用VDA（最小バージョン7.6）がインストールされている必要があります。未認証ユーザーが有効になっている場合、未認証のStoreFrontストアが必要です。

  未認証ユーザーアカウントは、セッションが起動されるとオンデマンドで作成され、Anon*XYZ*という名前になります。ここで*XYZ*は一意の3桁の値です。

認証されていないユーザーセッションには、デフォルトで10分間のアイドルタイムアウトがあり、クライアントが切断されると自動的にログオフされます。再接続、クライアント間のローミング、およびWorkspace Controlはサポートされていません。

次の表は、**ユーザー**ページでの選択肢について説明しています。

アクセスを有効にする対象	ユーザーとユーザーグループを追加/割り当てますか？	「未認証ユーザーにアクセスを許可する」チェックボックスを有効にしますか？
認証済みユーザーのみ	はい	いいえ
認証されていないユーザーのみ	いいえ	はい
認証済みユーザーと未認証ユーザーの両方	はい	はい

ステップ4. アプリケーション

知っておくと良いこと:

- Remote PC Accessデリバリーグループにアプリケーションを追加することはできません。
- デフォルトでは、追加する新しいアプリケーションは「Applications」という名前のフォルダーに配置されます。別のフォルダーを指定することもできます。詳細については、「アプリケーションの管理」の記事を参照してください。
- アプリケーションをデリバリーグループに追加するとき、または後で、そのプロパティを変更できます。詳細については、「アプリケーションの管理」の記事を参照してください。
- アプリケーションを追加しようとして、そのフォルダーに同じ名前のアプリケーションが存在する場合、追加しようとしているアプリケーションの名前を変更するよう求められます。拒否した場合、そのアプリケーションは、そのアプリケーションフォルダー内で一意になる接尾辞を付けて追加されます。
- アプリケーションを複数のデリバリーグループに追加する場合、それらすべてのデリバリーグループでアプリケーションを表示するための十分な権限がないと、可視性の問題が発生する可能性があります。そのような場合は、より高い権限を持つ管理者に相談するか、アプリケーションが追加されたすべてのデリバリーグループを含むようにスコープを拡張してください。
- 同じ名前の2つのアプリケーションを同じユーザーに公開する場合、Studioでアプリケーション名（ユーザー向け）プロパティを変更してください。そうしないと、ユーザーはCitrix Workspaceアプリで重複した名前を目にすることになります。

追加をクリックして、アプリケーションソースを表示します。

- **スタートメニューから:** 選択したカタログのマスターイメージから作成されたマシンで検出されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストを含む新しいページが起動します。追加したいものを選択し、**OK**をクリックします。
- **手動で定義:** サイト内またはネットワーク内の他の場所にあるアプリケーション。このソースを選択すると、実行可能ファイルのパス、作業ディレクトリ、オプションのコマンドライン引数、管理者およびユーザー向けの表示名を入力する新しいページが起動します。この情報を入力したら、**OK**をクリックします。
- **既存:** 以前にサイトに追加されたアプリケーション（おそらく別のデリバリーグループ内）。このソースを選択すると、検出されたアプリケーションのリストを含む新しいページが起動します。アプリケーションを追加し、**OK**をクリックします。
- **App-V:** App-Vパッケージ内のアプリケーション。このソースを選択すると、App-Vサーバーまたはアプリケーションライブラリを選択する新しいページが起動します。表示されたリストから追加したいアプリケーションを選択し、**OK**をクリックします。詳細については、App-Vを参照してください。

アプリケーションソースまたはアプリケーションが利用できないか無効な場合、それは表示されないか、選択できません。たとえば、サイトにアプリケーションが追加されていない場合、**既存**ソースは利用できません。または、アプリケーションが選択したカタログ内のマシンのサポートされているセッションタイプと互換性がない場合があります。

ステップ5. デスクトップ

このページのタイトルは、**マシン**ページで選択したカタログによって異なります。

- プールされたマシンを含むカタログを選択した場合、このページは**デスクトップ**というタイトルになります。
- 割り当てられたマシンを含むカタログを選択し、**デリバリーの種類**ページで「デスクトップ」を指定した場合、このページは**デスクトップユーザー割り当て**というタイトルになります。
- 割り当てられたマシンを含むカタログを選択し、**デリバリーの種類**ページで「アプリケーション」を指定した場合、このページは**アプリケーションマシンユーザー割り当て**というタイトルになります。

追加をクリックします。ダイアログボックスで、:

- 表示名と説明のフィールドに、Citrix Workspaceアプリに表示する情報を入力します。

- デスクトップにタグ制限を追加するには、**このタグを持つマシンへの起動を制限する**を選択し、ドロップダウンリストからタグを選択します。詳細については、タグを参照してください。
- ラジオボタンを使用して、デスクトップを起動するか、デスクトップ起動時にマシンを割り当てます。ユーザーは、このデリバリーグループにアクセスできる全員、または特定のユーザーおよびユーザーグループのいずれかです。
- グループに割り当てられたマシンが含まれている場合、ユーザーあたりのデスクトップの最大数を指定します。これは1以上の値である必要があります。
- デスクトップ（プールされたマシン用）またはデスクトップ割り当てルール（割り当てられたマシン用）を有効または無効にします。デスクトップを無効にすると、デスクトップの配信が停止します。デスクトップ割り当てルールを無効にすると、ユーザーへのデスクトップの自動割り当てが停止します。
- ダイアログボックスでの作業が完了したら、**OK**をクリックします。

サイト内のデスクトップの最大インスタンス数（PowerShellのみ）

サイト内のデスクトップの最大インスタンス数を構成するには（PowerShellのみ）：

- PowerShellで、適切なBrokerEntitlementPolicyRuleコマンドレットをMaxPerEntitlementInstancesパラメーターとともに使用します。たとえば、次のコマンドレットは、`tsvda-desktop` ルールを変更して、サイトで許可されるデスクトップの同時インスタンスの最大数を2に設定します。2つのデスクトップインスタンスが実行されている場合、3番目のサブスクライバーがデスクトップを起動しようとするとエラーが発生します。

  ```
  Set-BrokerEntitlementPolicyRule -Name tsvda-desktop
  -MaxPerEntitlementInstances 2
  ```

- ガイダンスについては、Get-Help コマンドレットを使用してください。たとえば、`Get-Help Set-BrokerEntitlementPolicyRule-Parameter MaxPerEntitlementInstances`。

ステップ 6. 概要

デリバリーグループの名前を入力します。オプションで、Citrix WorkspaceアプリとStudioに表示される説明を入力することもできます。

概要情報を確認し、**「完了」**をクリックします。

デリバリーグループの管理

はじめに

この記事では、管理コンソールからデリバリーグループを管理する手順について説明します。グループ作成時に指定した設定を変更するだけでなく、デリバリーグループの作成時には利用できないその他の設定も構成できます。

手順のカテゴリには、全般、ユーザー、マシン、セッションがあります。一部のタスクは複数のカテゴリにまたがります。たとえば、「ユーザーがマシンに接続できないようにする」はマシンのカテゴリで説明されていますが、ユーザーにも影響します。あるカテゴリでタスクが見つからない場合は、関連するカテゴリを確認してください。

その他の関連情報については、以下の記事も参照してください。

- 「アプリケーション」(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/manage-deployment/applications-manage.html)には、デリバリーグループ内のアプリケーションの管理に関する情報が含まれています。
- デリバリーグループの管理には、Delivery Group Administratorの組み込みロール権限が必要です。詳細については、「委任管理」(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/secure/delegated-administration.html)を参照してください。

全般

- 配信タイプの変更(#change-the-delivery-type-of-a-delivery-group)
- StoreFront™アドレスの変更(#change-storefront-addresses)
- デリバリーグループをアップグレードする
- Remote PC Accessデリバリーグループの管理(#manage-remote-pc-access-delivery-groups)

デリバリーグループのデリバリーの種類を変更する

デリバリーの種類は、グループが提供できるもの（アプリケーション、デスクトップ、またはその両方）を示します。

アプリケーションのみまたは**デスクトップとアプリケーション**のタイプを**デスクトップのみ**のタイプに変更する前に、グループからすべてのアプリケーションを削除してください。

1. ナビゲーションペインで を選択します。
2. グループを選択し、アクションペインで をクリックします。
3. ページで、目的のデリバリーの種類を選択します。

4. をクリックして変更を適用し、ウィンドウを開いたままにします。または、 をクリックして変更を適用し、ウィンドウを閉じます。

StoreFrontアドレスを変更する

1. ナビゲーションペインで を選択します。
2. グループを選択し、アクションペインで をクリックします。
3. **［StoreFront］**ページで、StoreFrontのURLを選択または追加します。これらのURLは、デリバリーグループ内の各マシンにインストールされているCitrix Workspace™アプリによって使用されます。
4. をクリックして変更を適用し、ウィンドウを開いたままにします。または、 をクリックして変更を適用し、ウィンドウを閉じます。

ナビゲーションペインで **>** を選択して、StoreFrontサーバーアドレスを指定することもできます。

デリバリーグループをアップグレードまたはアップグレードを元に戻す

デリバリーグループのアップグレードは、そのマシン上のVirtual Delivery Agent (VDA) と、デリバリーグループで使用されているマシンを含むマシンカタログをアップグレードした後に行います。

デリバリーグループのアップグレードを開始する前に：

- Citrix Provisioning™（旧Provisioning Services）を使用している場合は、Citrix Provisioningコンソールで VDAバージョンをアップグレードします。
- アップグレードされたVDAを含むマシンを起動して、Delivery Controllerに登録できるようにします。このプロセスにより、デリバリーグループで何がアップグレードされる必要があるかがコンソールに通知されます。
- 以前のVDAバージョンを使い続ける場合、新しい製品機能は利用できません。詳しくは、アップグレードのドキュメントを参照してください。

デリバリーグループをアップグレードするには：

1. ナビゲーションペインで を選択します。
2. グループを選択し、アクションペインで をクリックします。 アクションは、アップグレードされたVDAが検出された場合にのみ表示されます。

表示には、アップグレードできないマシンがある場合、そのマシンと理由が示されます。その後、アップグレードをキャンセルし、マシンの問題を解決してから、再度アップグレードを開始できます。

アップグレードが完了した後、デリバリーグループを選択し、 ペインで をクリックすることで、マシンを以前の状態に戻すことができます。

Remote PC Accessデリバリーグループの管理

Remote PC Accessマシンカタログ内のマシンが割り当てられていない場合、そのマシンは一時的にそのカタログに関連付けられたデリバリーグループに割り当てられます。この一時的な割り当てにより、後でマシンをユーザーに割り当てることができます。

デリバリーグループとマシンカタログの関連付けには優先度値があります。優先度は、マシンがシステムに登録されるとき、またはユーザーがマシン割り当てを必要とするときに、マシンに割り当てられるデリバリーグループを決定します。値が小さいほど優先度が高くなります。Remote PC Accessマシンカタログに複数のデリバリーグループ割り当てがある場合、ソフトウェアは最も優先度の高い一致を選択します。この優先度値を設定するには、PowerShell SDKを使用します。

リモートPCアクセス マシンカタログは、最初に作成されたときにデリバリーグループに関連付けられます。後でカタログに追加されたマシンアカウントまたは組織単位は、デリバリーグループに追加できます。この関連付けは、オン/オフを切り替えることができます。

Remote PC Accessマシンカタログとデリバリーグループの関連付けを追加または削除するには：

1. ナビゲーションペインで を選択します。
2. Remote PC Accessグループを選択します。
3. **詳細**セクションで、**マシンカタログ**タブをクリックし、Remote PC Accessカタログを選択します。
4. 関連付けを追加または復元するには、**デスクトップの追加**をクリックします。関連付けを削除するには、**関連付けの削除**をクリックします。

ユーザー

- ユーザー設定の変更
- ユーザーの追加または削除

デリバリーグループのユーザー設定を変更する

このページの名前は、**ユーザー設定** または **基本設定** のいずれかで表示されます。

1. ナビゲーションペインで を選択します。
2. グループを選択し、アクションペインで をクリックします。
3. **ユーザー設定** (または **基本設定**) ページで、次の表の設定のいずれかを変更します。

4. 加えた変更を適用してウィンドウを開いたままにするには、「**適用**」をクリックします。または、変更を適用してウィンドウを閉じるには、「**OK**」をクリックします。

設定	説明
説明	Citrix Workspace（またはStoreFront）が使用し、ユーザーに表示されるテキスト。
デリバリーグループを有効にする	デリバリーグループが有効になっているかどうか。
タイムゾーン	このデリバリーグループの仮想マシンが存在する必要があるタイムゾーン。このオプションには、サイトでサポートされているタイムゾーンが一覧表示されます。
Secure ICA® を有効にする	SecureICA を使用してデリバリーグループ内のマシンとの通信を保護します。SecureICA は ICA プロトコルを暗号化します。デフォルトのレベルは 128 ビットです。このレベルは SDK を使用して変更できます。Citrix® は、パブリックネットワークを通過する際に TLS 暗号化などのより多くの暗号化方法を使用することを推奨しています。また、SecureICA はデータ整合性をチェックしません。

デリバリーグループでのユーザーの追加または削除

ユーザーに関する詳細については、「ユーザー」を参照してください。

1. ナビゲーションペインで を選択します。
2. グループを選択し、アクションペインで「**デリバリーグループの編集**」をクリックします。
3. **ユーザー**ページで:
   - ユーザーを追加するには、**追加**をクリックし、追加するユーザーを指定します。
   - ユーザーを削除するには、1人以上のユーザーを選択し、**削除**をクリックします。
   - 認証されていないユーザーによるアクセスを許可するには、チェックボックスをオンまたはオフにします。
4. 加えた変更を適用してウィンドウを開いたままにするには、「**適用**」をクリックします。または、変更を適用してウィンドウを閉じるには、「**OK**」をクリックします。

ユーザーリストのインポートまたはエクスポート

物理的なシングルセッションOSマシンを含むデリバリーグループの場合、デリバリーグループの作成後に.csvファイルからユーザー情報をインポートできます。ユーザー情報を.csvファイルにエクスポートすることもできます。.csvファイルには、以前の製品バージョンのデータを含めることができます。

CSVファイルの最初の行には、コンマで区切られた2つの列ヘッダーが含まれている必要があります。最初のヘッダーが`Machine Account`で、2番目のヘッダーが`User Names`であることを確認してください。（追加のヘッダーを含めることはできますが、サポートされていません。）ファイルの以降の行には、コンマで区切られたデータが含まれます。`Machine Account`エントリは、コンピューターSID、FQDN、またはドメインとコンピューター名のペアにすることができます。

ユーザー情報をインポートまたはエクスポートするには：

1. ナビゲーションペインで を選択します。
2. グループを選択し、アクションペインで「**デリバリーグループの編集**」をクリックします。
3. **マシン割り当て**ページで、**リストのインポート**または**リストのエクスポート**を選択し、ファイルの場所を参照します。
4. 加えた変更を適用してウィンドウを開いたままにするには、「**適用**」をクリックします。または、変更を適用してウィンドウを閉じるには、「**OK**」をクリックします。

マシン

- マシンからユーザーへの割り当てを変更する
- ユーザーあたりの最大マシン数を変更する
- マシンを更新する
- デスクトップのタグ制限を追加、変更、または削除する
- マシンを削除する
- マシンへのアクセスを制限する
- ユーザーがマシンに接続するのを防ぐ（メンテナンスモード）
- マシンをシャットダウンして再起動する
- マシンの再起動スケジュールを作成および管理する
- 管理対象マシンをロードする
- 管理対象マシンの電源を管理する

デリバリーグループ内のマシンからユーザーへの割り当てを変更する

MCSでプロビジョニングされたシングルセッションOSマシンの割り当てを変更できます。マルチセッションOSマシンまたはCitrix Provisioningでプロビジョニングされたマシンの割り当ては変更できません。

1. ナビゲーションペインで を選択します。
2. グループを選択し、アクションペインで「**デリバリーグループの編集**」をクリックします。
3. 「**デスクトップ**」ページまたは「**デスクトップ割り当て規則**」ページ（ページタイトルは、デリバリーグループが使用するマシンカタログの種類によって異なります）で、新しいユーザーを指定します。
4. 加えた変更を適用してウィンドウを開いたままにするには、「**適用**」をクリックします。または、変更を適用してウィンドウを閉じるには、「**OK**」をクリックします。

デリバリーグループ内のユーザーあたりの最大マシン数を変更する

1. ナビゲーションペインで を選択します。
2. グループを選択し、アクションペインで「**デリバリーグループの編集**」をクリックします。
3. **デスクトップ割り当てルール**ページで、ユーザーあたりの最大デスクトップ数を設定します。
4. 加えた変更を適用してウィンドウを開いたままにするには、「**適用**」をクリックします。または、変更を適用してウィンドウを閉じるには、「**OK**」をクリックします。

デリバリーグループ内のマシンを更新する

1. ナビゲーションペインで を選択します。
2. グループを選択し、アクションペインで「**マシンの表示**」をクリックします。
3. マシンを選択し、アクションペインで「**マシンの更新**」をクリックします。

別のイメージを選択するには、「**マスターイメージ**」を選択し、スナップショットを選択します。

変更を適用してマシンユーザーに通知するには、**「エンドユーザーへのロールアウト通知」**を選択します。次に、以下を指定します。

- マスターイメージを更新するタイミング: 今すぐ、または次回の再起動時
- 再起動の配布時間（グループ内のすべてのマシンの更新を開始するまでの合計時間）
- ユーザーに再起動が通知されるかどうか
- ユーザーが受信するメッセージ

デスクトップのタグ制限を追加、変更、または削除する

タグ制限の追加、変更、削除は、起動対象となるデスクトップに予期せぬ影響を与える可能性があります。「タグ」の考慮事項と注意点を確認してください。

1. ナビゲーションペインで を選択します。
2. グループを選択し、アクションペインで「**デリバリーグループの編集**」をクリックします。
3. **デスクトップ**ページで、デスクトップを選択し、**編集**をクリックします。
4. タグ制限を追加するには、**タグを持つマシンへの起動を制限する**を選択し、タグを選択します。
5. タグ制限を変更または削除するには、次のいずれかを実行します。
   - 別のタグを選択します。
   - **このタグを持つマシンへの起動を制限する**のチェックを外して、タグ制限を削除します。
6. 「**適用**」をクリックして変更を適用し、ウィンドウを開いたままにします。または、「**OK**」をクリックして変更を適用し、ウィンドウを閉じます。

デリバリーグループからマシンを削除する

マシンを削除すると、デリバリーグループから削除されます。デリバリーグループが使用するマシンカタログからは削除されません。したがって、そのマシンは別のデリバリーグループに割り当てることができます。

マシンは、削除する前にシャットダウンする必要があります。削除中にユーザーがマシンに接続するのを一時的に停止するには、シャットダウンする前にマシンをメンテナンスモードにします。

マシンには個人データが含まれている可能性があるため、別のユーザーにマシンを割り当てる前に注意してください。マシンの再イメージングを検討してください。

1. ナビゲーションペインで を選択します。
2. グループを選択し、アクションペインで「**マシンの表示**」をクリックします。
3. マシンがシャットダウンされていることを確認します。
4. マシンを選択し、アクションペインで「**デリバリーグループから削除**」をクリックします。

マシンが使用する接続を介して、デリバリーグループからマシンを削除することもできます。

デリバリーグループ内のマシンへのアクセスを制限する

デリバリーグループ内のマシンへのアクセスを制限するために行った変更は、使用する方法に関係なく、以前の設定に優先します。次のことができます。

- **委任管理スコープを使用して管理者へのアクセスを制限する:** 管理者がすべてのアプリケーションにアクセスできるスコープと、特定のアプリケーションのみにアクセスできる別のスコープを作成して割り当てます。詳細については、「委任管理」を参照してください。
- **SmartAccessポリシー式を使用してユーザーアクセスを制限する：** ポリシー式を使用して、Citrix Gateway経由のユーザー接続をフィルタリングします。

  a. ナビゲーションペインで を選択します。

  b. グループを選択し、アクションペインで「**デリバリーグループの編集**」をクリックします。

  c. ****ページで、****を選択します。

  d. これらの接続のサブセットを選択するには、****を選択します。次に、Citrix Gatewayサイトを定義し、許可されるユーザーアクセスシナリオのSmartAccessポリシー式を追加、編集、または削除します。詳細については、Citrix Gatewayのドキュメントを参照してください。

  e. 「**適用**」をクリックして変更を適用し、ウィンドウを開いたままにします。または、「**OK**」をクリックして変更を適用し、ウィンドウを閉じます。

- **除外フィルターを使用してユーザーアクセスを制限する：** SDKで設定したアクセスポリシーに除外フィルターを使用します。アクセスポリシーは、接続を絞り込むためにデリバリーグループに適用されます。たとえば、マシンアクセスをユーザーのサブセットに制限したり、許可されるユーザーデバイスを指定したりできます。除外フィルターは、アクセスポリシーをさらに絞り込みます。たとえば、セキュリティのために、ユーザーまたはデバイスのサブセットへのアクセスを拒否できます。デフォルトでは、除外フィルターは無効になっています。

  たとえば、企業ネットワークサブネット上の教育ラボで、そのラボから特定のデリバリーグループへのアクセスを防止する場合などです。ラボ内のマシンを誰が使用しているかに関係なく、次のコマンドを使用します: `Set-BrokerAccessPolicy -Name VPDesktops_Direct -ExcludedClientIPFilterEnabled $True -`。

  アスタリスク (*) ワイルドカードを使用して、同じポリシー式で始まるすべてのタグに一致させます。たとえば、あるマシンにタグ `VPDesktops_Direct` を追加し、別のマシンに `VPDesktops_Test` を追加した場合、`Set-BrokerAccessPolicy` スクリプトでタグを `VPDesktops_*` に設定すると、両方のマシンにフィルターが適用されます。

Webブラウザーを使用している場合、またはストアでCitrix Workspaceアプリのユーザーエクスペリエンス機能が有効になっている場合は、クライアント名除外フィルターを使用できません。

デリバリーグループ内のマシンへのユーザー接続を防止する（メンテナンスモード）

マシンへの新しい接続を一時的に停止する必要がある場合は、デリバリーグループ内の1台またはすべてのマシンでメンテナンスモードをオンにできます。これは、パッチを適用したり、管理ツールを使用したりする前に行うことがあります。

- マルチセッションOSマシンがメンテナンスモードの場合、ユーザーは既存のセッションに接続できますが、新しいセッションを開始することはできません。
- シングルセッションOSマシン（またはリモートPCアクセスを使用するPC）がメンテナンスモードの場合、ユーザーは接続または再接続できません。現在の接続は、切断またはログオフするまで接続されたままになります。

メンテナンスモードをオンまたはオフにするには：

1. ナビゲーションペインで を選択します。
2. グループを選択します。
3. デリバリーグループ内のすべてのマシンでメンテナンスモードを有効にするには、アクションペインで「**メンテナンスモードを有効にする**」をクリックします。

   1台のマシンでメンテナンスモードを有効にするには、アクションペインで「**マシンの表示**」をクリックします。マシンを選択し、アクションペインで「**メンテナンスモードを有効にする**」をクリックします。
4. デリバリーグループ内の1台またはすべてのマシンでメンテナンスモードを無効にするには、上記の手順に従い、アクションペインで「**メンテナンスモードを無効にする**」をクリックします。

Windowsリモートデスクトップ接続（RDC）の設定も、マルチセッションOSマシンがメンテナンスモードであるかどうかに影響します。メンテナンスモードは、次のいずれかが発生した場合にオンになります。

- 前述のとおり、メンテナンスモードがオンに設定されています。
- RDCは「**このコンピューターへの接続を許可しない**」に設定されています。
- RDCは「**このコンピューターへの接続を許可しない**」に設定されていません。「**リモートホスト構成ユーザーログオンモード**」設定は、「**再接続を許可するが、新しいログオンは禁止する**

」または「**再接続を許可するが、サーバーが再起動されるまで新しいログオンは禁止する**」のいずれかです。

以下のメンテナンスモードをオンまたはオフにすることもできます。

- 接続。その接続を使用しているマシンに影響します。
- マシンカタログ。そのカタログ内のマシンに影響します。

デリバリーグループ内のマシンをシャットダウンして再起動する

この手順は、Remote PC Accessマシンではサポートされていません。

1. ナビゲーションペインで を選択します。
2. グループを選択し、アクションペインで「**マシンの表示**」をクリックします。
3. マシンを選択し、アクションペインで次のいずれかのエントリをクリックします。
    - **強制シャットダウン：** マシンの電源を強制的にオフにし、マシンリストを更新します。
    - **再起動：** オペレーティングシステムにシャットダウンを要求し、その後マシンを再起動します。オペレーティングシステムがこれに応じられない場合、マシンは現在の状態のままになります。
    - **強制再起動：** オペレーティングシステムを強制的にシャットダウンし、その後マシンを再起動します。
    - **一時停止:** マシンをシャットダウンせずに一時停止し、マシンの一覧を更新します。
    - **シャットダウン:** オペレーティングシステムにシャットダウンを要求します。

強制ではないアクションの場合、マシンが10分以内にシャットダウンしないと、電源がオフになります。シャットダウン中にWindowsが更新プログラムのインストールを試みると、更新が完了する前にマシンの電源がオフになるリスクがあります。

Citrixでは、シングルセッションOSマシンのユーザーがセッション内で**シャットダウン**を選択できないようにすることをお勧めします。詳細については、Microsoftのポリシーに関するドキュメントを参照してください。

接続でマシンをシャットダウンおよび再起動することもできます。

デリバリーグループ内のマシンの再起動スケジュールを作成および管理する

再起動スケジュールは、デリバリーグループ内のマシンが定期的に再起動されるタイミングを指定します。デリバリーグループに対して1つ以上のスケジュールを作成できます。スケジュールは、次のいずれかに影響します。

- グループ内のすべてのマシン。
- グループ内の1つまたは複数（ただしすべてではない）のマシン。マシンは、マシンに適用するタグによって識別されます。これはタグ制限と呼ばれます。タグがアクションをそのタグを持つアイテムのみに制限するためです。

たとえば、すべてのマシンが1つのデリバリーグループにあるとします。すべてのマシンを週に1回再起動し、経理チームが使用するマシンを毎日再起動したいとします。これを実現するには、すべてのマシンに対して1つのスケジュールを設定し、経理のマシンのみに対して別のスケジュールを設定します。

スケジュールには、再起動が開始される日時と期間が含まれます。

スケジュールを有効または無効にできます。スケジュールを無効にすることは、テスト中、特別な期間中、またはスケジュールが必要になる前に準備する際に役立ちます。

管理コンソールから自動電源オンまたはシャットダウンにスケジュールを使用することはできません。再起動のみに使用できます。

> **注：**
>
> Citrix Studioは、デスクトップOSの再起動スケジュールの構成をサポートしていません。

スケジュールの重複

複数のスケジュールが重複する可能性があります。上記の例では、両方のスケジュールが経理部門の仮想マシンに影響を与えます。これらのマシンは日曜日に2回再起動される可能性があります。スケジューリングコードは、意図したよりも頻繁に同じマシンを再起動しないように設計されていますが、保証はできません。

- スケジュールの開始時刻と期間が正確に一致する場合、マシンが再起動されるのは1回だけである可能性が高くなります。
- スケジュールの開始時刻と期間が異なるほど、複数回の再起動が発生する可能性が高くなります。
- スケジュールによって影響を受けるマシンの数も、重複の可能性に影響します。この例では、すべてのマシンに影響する週次スケジュールは、それぞれに指定された期間に応じて、経理部門の仮想マシンに対する日次スケジュールよりも早く再起動を開始する可能性があります。

再起動スケジュールの詳細については、「再起動スケジュールの内部」を参照してください。

再起動スケジュールの表示

1. ナビゲーションペインで を選択します。
2. グループを選択し、アクションペインで「**デリバリーグループの編集**」をクリックします。
3. **Restart Schedule**ページを選択します。

Restart Scheduleページには、構成された各スケジュールについて次の情報が含まれています。

- スケジュール名。
- 使用されているタグ制限（ある場合）。
- マシンの再起動がどのくらいの頻度で発生するか。
- マシンユーザーが通知を受け取るかどうか。
- スケジュールが有効になっているかどうか。

タグの追加（適用）

タグ制限を使用する再起動スケジュールを構成する場合は、スケジュールが影響するマシンにタグが追加されていることを確認してください。上記の例では、経理チームが使用する各マシンにタグが適用されています。詳細については、「タグ」を参照してください。

1台のマシンに複数のタグを適用できますが、再起動スケジュールで指定できるタグは1つだけです。

1. ナビゲーションペインで を選択します。
2. スケジュールによって制御されるマシンを含むグループを選択します。
3. 「**マシンの表示**」をクリックし、タグを追加するマシンを選択します。
4. 「アクション」ペインで**「タグの管理」**をクリックします。
5. タグが存在する場合は、タグ名の横にあるチェックボックスをオンにします。タグが存在しない場合は、「**作成**」をクリックし、タグの名前を指定します。タグが作成されたら、新しく作成されたタグ名の横にあるチェックボックスをオンにします。
6. 「**タグの管理**」ダイアログで「**保存**」をクリックします。

再起動スケジュールの作成

> **注：**

> 再起動スケジュールは、電源管理されているすべてのマルチセッションマシンと、電源管理されていないマルチセッションマシンに適用できます。

1. ナビゲーションペインで を選択します。
2. グループを選択し、「アクション」ペインで**「デリバリーグループの編集」**をクリックします。
3. 「**再起動スケジュール**」ページで、「**追加**」をクリックします。
4. 「**再起動スケジュールの追加**」ページで、次のようにします。

   - スケジュール名と説明を入力します。
   - タグ制限を使用している場合は、タグを選択します。
   - **「再起動の頻度」**で、再起動の発生頻度（毎日、平日、週末、または毎週特定の曜日）を選択します。
   - 24時間形式を使用して、再起動を開始する時刻を指定します。
   - **「再起動期間」**で、すべてのマシンを同時に再起動するか、影響を受けるすべてのマシンの再起動を開始する合計時間を選択します。内部アルゴリズムにより、その間隔で各マシンが再起動されるタイミングが決定されます。

     > **注：**
     >
     > PowerShellを使用する場合、別の再起動期間の選択肢が利用可能です。「ドレイン後の再起動」を参照してください。

   - **「ユーザーへの通知の送信」**で、再起動が開始される前に影響を受けるマシンに通知メッセージを表示するかどうかを選択します。デフォルトでは、メッセージは表示されません。
   - 再起動が開始される15分前にメッセージを表示することを選択した場合、（通知頻度で）最初のメッセージの後に5分ごとにメッセージを繰り返すように選択できます。デフォルトでは、メッセージは繰り返されません。
   - 通知のタイトルとテキストを入力します。デフォルトのテキストはありません。

     メッセージに再起動までの分数を含める場合は、変数**%m%**を含めます。例：「警告: コンピューターは%m%分後に自動的に再起動されます。」この値は、繰り返される各メッセージで5分ずつ減少します。すべてのマシンを同時に再起動することを選択しない限り、メッセージは内部アルゴリズムによって計算された再起動前の適切なタイミングで各マシンに表示されます。

- スケジュールを有効にするには、チェックボックスをオンにします。スケジュールを無効にするには、チェックボックスをオフにします。

5. **「適用」をクリックして変更を適用し、ウィンドウを開いたままにします。または、「OK」**をクリックして変更を適用し、ウィンドウを閉じます。

ドレイン後の再起動

PowerShell を使用してマシンの再起動スケジュールを作成または更新する場合 (`New-BrokerRebootSchedulev2` または `Set-BrokerRebootSchedulev2`)、別の再起動期間値を使用できます。

`-UseNaturalReboot <Boolean>` パラメーターでドレイン後の再起動機能を有効にすると、すべてのセッションがドレインされた後にすべてのマシンが再起動されます。再起動時刻になると、マシンはドレイン状態になり、すべてのセッションがログオフされると再起動されます。

この機能は、シングルセッションまたはマルチセッションのマシンを含むデリバリーグループでサポートされています。マシンは電源管理されている必要があります。

オンプレミス環境では、この機能はPowerShellを使用している場合にのみサポートされます。この機能はStudioでは利用できません。

再起動スケジュールの編集、削除、有効化、または無効化

1. ナビゲーションペインで を選択します。
2. グループを選択し、「アクション」ペインで**「デリバリーグループの編集」**をクリックします。
3. **再起動スケジュール**ページで、スケジュールのチェックボックスを選択します。

   - スケジュールを編集するには、 をクリックします。再起動スケジュールの作成 のガイダンスに従って、スケジュール構成を更新します。
   - スケジュールを有効または無効にするには、 をクリックします。 チェックボックスをオンまたはオフにします。
   - スケジュールを削除するには、 をクリックします。削除を確認します。スケジュールを削除しても、影響を受けるマシンに適用されているタグには影響しません。

データベース障害により遅延したスケジュールされた再起動

> **注：**

> この機能はPowerShellでのみ利用可能です。

> デリバリーグループ内のマシン (VDA) のスケジュールされた再起動が開始される前にサイトデータベースの停止が発生した場合、停止が終了すると再起動が開始されます。これにより、予期しない結果が生じる可能性があります。

たとえば、デリバリーグループの再起動を非稼働時間中 (03:00 から) に発生するようにスケジュールしたとします。スケジュールされた再起動が開始される1時間前 (02:00) にサイトデータベースの停止が発生しました。停止は6時間 (08:00 まで) 続きました。Delivery Controller とサイトデータベース間の接続が復元されると、再起動スケジュールが開始されます。VDA の再起動は元のスケジュールから5時間後に開始され、稼働時間中に VDA が再起動されることになります。

この状況を回避するために、`New-BrokerRebootScheduleV2` および `Set-BrokerRebootScheduleV2` コマンドレットで `MaxOvertimeStartMins` パラメーターを使用できます。この値は、再起動スケジュールが開始できる、スケジュールされた開始時刻を超える最大分数を示します。

- その時間内 (スケジュールされた時間 + `MaxOvertimeStartMins`) にデータベース接続が復元された場合、VDAの再起動が開始されます。
- その時間内にデータベース接続が復元されない場合、VDAの再起動は開始されません。
- このパラメーターが省略されているか、値がゼロの場合、停止期間に関係なく、データベースへの接続が復元されたときにスケジュールされた再起動が開始されます。

詳細については、cmdlet ヘルプを参照してください。この機能は PowerShell でのみ利用可能です。Studio で再起動スケジュールを構成する際には、この値を設定できません。

メンテナンスモードのマシンのスケジュールされた再起動

> **注：**

> この機能はPowerShellでのみ利用可能です。

> 再起動スケジュールがメンテナンスモードのマシンに影響するかどうかを示すには、`BrokerRebootScheduleV2` コマンドレットで `IgnoreMaintenanceMode` オプションを使用します。

たとえば、次のコマンドレットは、メンテナンスモードのマシン (メンテナンスモードではないマシンに加えて) を再起動するスケジュールを作成します。

`New-Brokerrebootschedulev2 rebootSchedule1 -DesktopGroupName <myDesktopGroup> -IgnoreMaintenanceMode $true`

次のコマンドレットは、既存の再起動スケジュールを変更します。

`Set-Brokerrebootschedulev2 rebootSchedule1 -IgnoreMaintenanceMode $true`

詳細については、コマンドレットのヘルプを参照してください。この機能はPowerShellでのみ利用可能です。

デリバリーグループ内の負荷管理されたマシン

負荷管理できるのはマルチセッションOSマシンのみです。

負荷管理は、サーバーの負荷を測定し、現在の環境条件でどのサーバーを選択するかを決定します。この選択は、以下に基づいています。

- **サーバーメンテナンスモードのステータス:** マルチセッションOSマシンは、メンテナンスモードがオフの場合にのみ負荷分散の対象となります。
- **サーバー負荷インデックス:** マルチセッションOSマシンを提供するサーバーが接続を受け入れる可能性を決定します。このインデックスは、セッション数やCPU、ディスク、メモリ使用量などのパフォーマンスメトリックの設定といった負荷評価子の組み合わせです。負荷評価子は、負荷管理ポリシー設定で指定されます。

  サーバー負荷インデックスが10000の場合、サーバーが完全に負荷されていることを示します。他に利用可能なサーバーがない場合、ユーザーはセッションを起動したときに、デスクトップまたはアプリケーションが利用できないというメッセージを受け取る可能性があります。

  ロードインデックスは、Director (監視)、Studio (管理) 検索、および SDK で監視できます。

  コンソール表示で、**Server Load Index** 列 (デフォルトでは非表示) を表示するには、マシンを選択し、列ヘッダーを右クリックして、**Select Column** を選択します。**Machine category** で、**Load Index** を選択します。

  SDKでは、`Get-BrokerMachine` コマンドレットを使用します。詳細については、「CTX202150」を参照してください。
- **同時ログオン許容ポリシー設定**: サーバーへの同時ログオン要求の最大数。（この設定は、XenApp 6.xバージョンでの負荷調整に相当します。）

すべてのサーバーが同時ログオン許容設定以上の場合、次のログオン要求は、保留中のログオンが最も少ないサーバーに割り当てられます。複数のサーバーがこれらの条件を満たす場合、ロードインデックスが最も低いサーバーが選択されます。

デリバリーグループ内の電源管理されたマシン

電源管理できるのは、仮想シングルセッションOSマシンのみであり、物理マシン（リモートPCアクセス マシンを含む）はできません。GPU機能を備えたシングルセッションOSマシンは一時停止できないため、電源オフ操作は失敗します。マルチセッションOSマシンでは、再起動スケジュールを作成できます。

プールされたマシンを含むデリバリーグループでは、仮想シングルセッションOSマシンは次のいずれかの状態になります。

- ランダムに割り当てられ、使用中
- 割り当てられておらず、未接続

静的マシンを含むデリバリーグループでは、仮想シングルセッションOSマシンは次のようになります。

- 永続的に割り当てられ、使用中
- 永続的に割り当てられ、未接続（ただし準備完了）
- 割り当てられておらず、未接続

通常の使用では、静的デリバリーグループには通常、永続的に割り当てられたマシンと割り当てられていないマシンの両方が含まれます。最初は、デリバリーグループの作成時に手動で割り当てられたマシンを除き、すべてのマシンが割り当てられていません。ユーザーが接続すると、マシンは永続的に割り当てられます。これらのデリバリーグループ内の割り当てられていないマシンは完全に電源管理できますが、永続的に割り当てられたマシンは部分的にしか管理できません。

- **プールとバッファー:** プールされたデリバリーグループと、割り当てられていないマシンを持つ静的デリバリーグループの場合、プール（この場合）とは、電源オン状態に保たれ、ユーザーが接続できる状態になっている、割り当てられていない、または一時的に割り当てられたマシンのセットです。ユーザーはログオン後すぐにマシンを取得します。プールサイズ（電源オン状態に保たれるマシンの数）は、時間帯によって構成可能です。静的デリバリーグループの場合は、SDKを使用してプールを構成します。

  バッファーとは、プール内のマシンの数がしきい値を下回ったときに電源がオンになる、割り当てられていないマシンの追加のスタンバイセットです。しきい値は、デリバリーグループサイズのパーセンテージです。大規模なデリバリーグループの場合、しきい値を超えるとかなり

の数のマシンがオンになる可能性があります。そのため、デリバリーグループのサイズを慎重に計画するか、SDKを使用してデフォルトのバッファーサイズを調整してください。

- **電源状態タイマー:** 電源状態タイマーを使用すると、ユーザーが指定された時間切断された後にマシンを一時停止できます。たとえば、ユーザーが10分以上切断された場合、勤務時間外にマシンは自動的に一時停止します。

  タイマーは、平日と週末、およびピーク時と非ピーク時の間隔で構成できます。

- **永続的に割り当てられたマシンの部分的な電源管理:** 永続的に割り当てられたマシンについては、電源状態タイマーを設定できますが、プールやバッファーは設定できません。マシンは各ピーク期間の開始時にオンになり、各非ピーク期間の開始時にオフになります。消費されたマシンを補うために利用可能になるマシンの数について、割り当てられていないマシンで得られるようなきめ細かな制御はできません。

仮想シングルセッションOSマシンの電源管理

1. ナビゲーションペインで を選択します。
2. グループを選択し、アクションペインで **Edit Delivery Group** をクリックします。
3. **Power Management**ページで、**Power manage machines**の**Weekdays**を選択します。デフォルトでは、平日は月曜日から金曜日です。
4. ランダムなデリバリーグループの場合、**Machines to be powered on**で**Edit**をクリックし、平日のプールサイズを指定します。次に、電源をオンにするマシンの数を選択します。
5. **Peak hours**で、各日のピーク時間と非ピーク時間を設定します。
6. 平日のピーク時間と非ピーク時間の電源状態タイマーを設定します。**During peak hours > When disconnected**で、デリバリーグループ内の切断されたマシンを一時停止するまでの遅延（分単位）を指定し、**Suspend**を選択します。**During off-peak hours > When disconnected**で、デリバリーグループ内のログオフされたマシンをシャットダウンするまでの遅延を指定し、**Shutdown**を選択します。このタイマーは、ランダムなマシンを持つデリバリーグループでは使用できません。
7. **Power manage machines**で**Weekend**を選択し、週末のピーク時間と電源状態タイマーを構成します。
8. 加えた変更を適用してウィンドウを開いたままにするには、**Apply** をクリックします。または、変更を適用してウィンドウを閉じるには、**OK** をクリックします。

SDKを使用して、次の操作を行います。

- 電源状態タイマーに応じてマシンを中断するのではなくシャットダウンするか、タイマーを接続解除ではなくログオフに基づいて設定したい場合。

- デフォルトの平日と週末の定義を変更する。
- 電源管理を無効にします。CTX217289を参照してください。

切断されたセッションを持つVDIマシンが異なる時間帯に移行する際の電源管理

> **重要:**

> この機能強化は、切断されたセッションを持つVDIマシンにのみ適用されます。ログオフされたセッションを持つVDIマシンには適用されません。

> 以前のリリースでは、アクション (切断アクション = 「**Suspend**」または「**Shutdown**」) が必要な時間帯に移行する VDI マシンは、電源が入ったままでした。このシナリオは、アクション (切断アクション = 「**Nothing**」) が不要な時間帯 (ピーク時またはオフピーク時) にマシンが切断された場合に発生しました。

Citrix Virtual Apps and Desktops™ 7 1909 以降、指定された切断時間が経過すると、宛先時間帯に構成されている切断アクションに応じて、マシンは一時停止または電源オフになります。

たとえば、VDIデリバリーグループに対して次の電源ポリシーを構成します。

- `PeakDisconnectAction` を「Nothing」に設定します
- `OffPeakDisconnectAction` を「Shutdown」に設定します
- `OffPeakDisconnectTimeout` を「10」に設定します

電源ポリシーの切断アクションに関する詳細については、`<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policy>` および `<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/>` を参照してください。

以前のリリースでは、ピーク時にセッションが切断されたVDIマシンは、ピークからオフピークに移行しても電源がオンのままでした。Citrix Virtual Apps and Desktops 7 1909以降、期間移行時に `OffPeakDisconnectAction` および `OffPeakDisconnectTimeout` ポリシーアクションがVDIマシンに適用されます。その結果、マシンはオフピークに移行してから10分後に電源がオフになります。

以前の動作に戻したい場合（つまり、切断されたセッションを持つマシンがピークからオフピークへ、またはオフピークからピークへ移行しても何もアクションを実行しない場合）、次のいずれかを実行します:

- `LegacyPeakTransitionDisconnectedBehaviour`レジストリ値を`1`に設定します。これは以前の動作を有効にする*true*に相当します。デフォルトでは、値は`0`、つまり*false*であり、これは期間移行時に切断電源ポリシーアクションをトリガーします。
  - パス: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer`
  - 名前: `LegacyPeakTransitionDisconnectedBehaviour`
  - 種類: `REG_DWORD`
  - データ: `0x00000001 (1)`
- `Set-BrokerServiceConfigurationData` PowerShellコマンドを使用して設定を構成します。例:
  - `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

期間移行時に電源ポリシーアクションを適用する前に、マシンは次の基準を満たす必要があります。

- 切断されたセッションがあること。
- 保留中の電源アクションがないこと。
- 異なる時間帯に移行するVDI（シングルセッション）デリバリーグループに属していること。
- 特定の時間帯（ピーク時またはオフピーク時）にセッションが切断され、電源アクションが割り当てられている期間に移行すること。

カタログの電源オン状態のVDAの割合を変更する

1. デリバリーグループの**電源管理**セクションから、デリバリーグループのピーク時間を調整します。
2. デスクトップグループ名をメモします。
3. 管理者権限でPowerShellを起動し、次のコマンドを実行します。「Desktop Group Name」を、実行中のVDAの割合が変更されたデスクトップグループの名前に置き換えます。

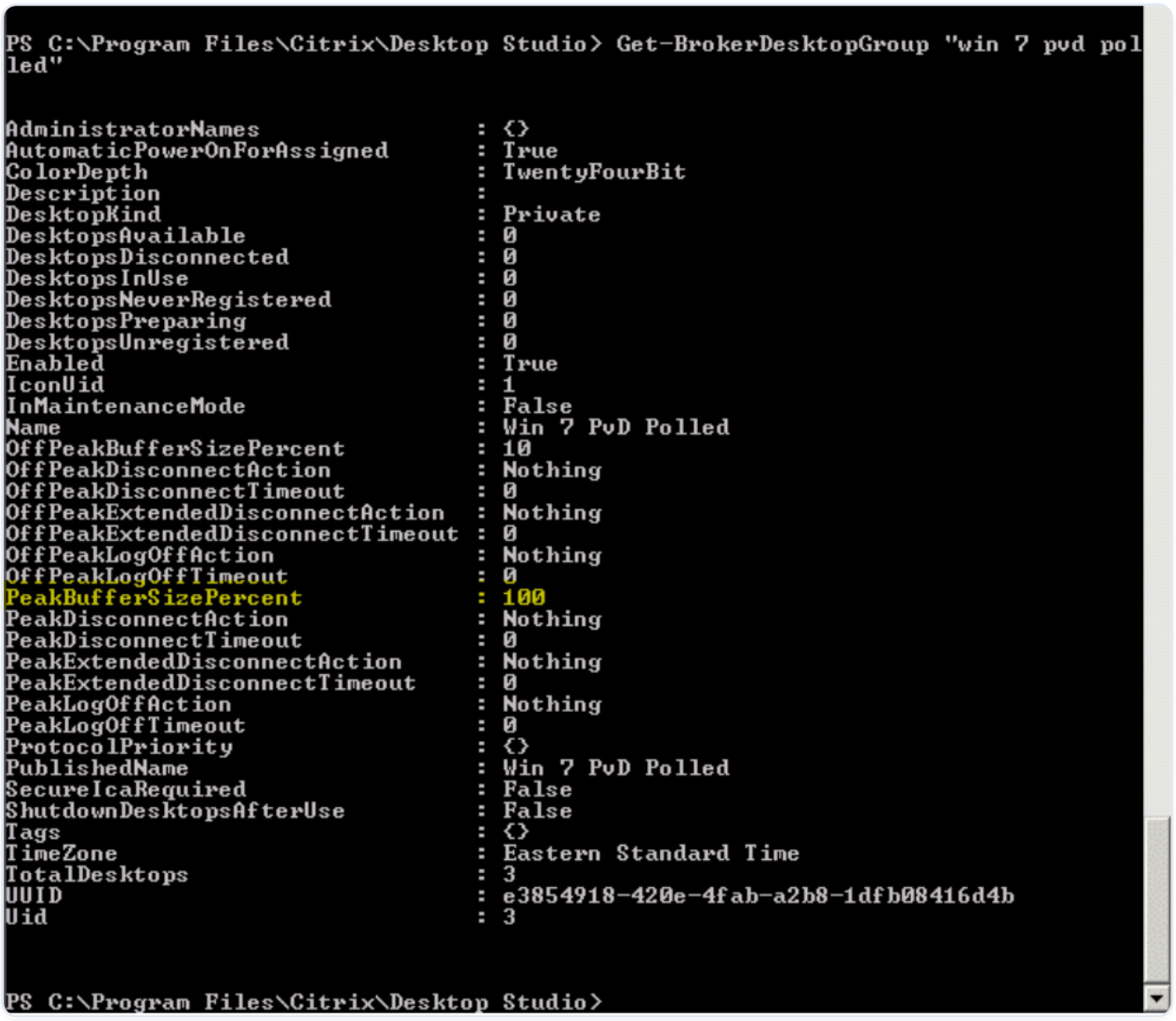
   `asnp Citrix*`

   `# Set-BrokerDesktopGroup "Desktop Group Name" -PeakBufferSizePercent 100`

値が100の場合、VDAの100%が準備完了状態であることを意味します。

4. 次のコマンドを実行してソリューションを確認します。

```
#Get-BrokerDesktopGroup "Desktop Group Name"
```



変更が有効になるまで最大1時間かかる場合があります。

ユーザーがログオフした後にVDAをシャットダウンするには、次のように入力します。

```
# Set-BrokerDesktopGroup "Desktop Group Name" -ShutDownDesktopsAfterUse $True
```

ピーク時にVDAを再起動して、ユーザーがログオフした後にすぐに使用できるようにするには、次のように入力します。

```
# Set-BrokerDesktopGroup "Desktop Group Name"
-AutomaticPowerOnForAssignedDuringPeak $True
```

セッション

- セッションのログオフまたは切断、またはユーザーへのメッセージ送信
- セッションのプレ起動とセッションの維持を構成する
- メンテナンスモードのマシンから切断された場合のセッション再接続を制御する

セッションのログオフまたは切断

1. Studio ナビゲーションペインで、**Delivery Groups** を選択します。
2. デリバリーグループを選択し、**Actions** ペインで **View Machines** を選択します。
3. 中央ペインでマシンを選択し、**Actions** ペインで **View Sessions** を選択してから、セッションを選択します。
    - または、中央ペインで**Session**タブを選択し、セッションを選択します。
4. セッションからログオフするには、**Actions** ペインで **Log off** を選択します。セッションが閉じられ、ユーザーはログアウトされます。マシンが特定のユーザーに割り当てられていない限り、他のユーザーが利用できるようになります。
5. セッションを切断するには、**Actions** ペインで **Disconnect** を選択します。アプリケーションはセッション内で実行を継続し、マシンはそのユーザーに割り当てられたままになります。ユーザーは同じマシンに再接続できます。

シングルセッションOSマシンでは、未使用のセッションを自動的に処理するように電源状態タイマーを構成できます。詳細については、「電源管理されたマシン」を参照してください。

デリバリーグループにメッセージを送信する

1. Studioナビゲーションペインで、**デリバリーグループ**を選択します。
2. デリバリーグループを選択し、**操作**ペインで**マシンの表示**を選択します。
3. 中央ペインで、メッセージを送信するマシンを選択します。
4. **操作**ペインで、**セッションの表示**を選択します。
5. 中央ペインで、すべてのセッションを選択し、**操作**ペインで**メッセージの送信**を選択します。
6. メッセージを入力し、**OK**をクリックします。必要に応じて、重大度レベルを指定できます。オプションには、**重大**、**質問**、**警告**、**情報**があります。

または、Citrix Directorを使用してメッセージを送信することもできます。詳しくは、「ユーザーへのメッセージの送信」を参照してください。

デリバリーグループでセッションの事前起動とセッションの維持を構成する

これらの機能は、マルチセッションOSマシンでのみサポートされています。

セッションの事前起動とセッションの維持機能は、要求される前にセッションを開始すること（セッションの事前起動）と、ユーザーがすべてのアプリケーションを閉じた後もアプリケーションセッションをアクティブに保つこと（セッションの維持）により、指定されたユーザーがアプリケーションにすばやくアクセスできるようにします。

デフォルトでは、セッションの事前起動とセッションの維持は使用されません。セッションは、ユーザーがアプリケーションを起動したときに開始（起動）され、セッション内の最後に開いたアプリケーションが閉じるまでアクティブなままになります。

考慮事項:

- デリバリーグループはアプリケーションをサポートしている必要があり、マシンはマルチセッションOS用のVDA（最小バージョン7.6）を実行している必要があります。
- これらの機能は、Windows向けCitrix Workspaceアプリを使用している場合にのみサポートされ、追加のCitrix Workspaceアプリ構成も必要です。手順については、お使いのWindows向けCitrix Workspaceアプリバージョンの製品ドキュメントで「session prelaunch」を検索してください。
- Citrix Workspace app for HTML5はサポートされていません。
- セッションの事前起動を使用している場合、ユーザーのマシンがサスペンドまたは休止状態になると、事前起動は機能しません（セッションの事前起動設定にかかわらず）。ユーザーはマシン/セッションをロックできます。ただし、ユーザーがCitrix Workspaceアプリからログオフすると、セッションは終了し、事前起動は適用されなくなります。
- セッションの事前起動を使用している場合、物理クライアントマシンはサスペンドまたは休止状態の電源管理機能を使用できません。クライアントマシンのユーザーはセッションをロックできますが、ログオフしないでください。
- 事前起動および維持されているセッションは同時接続ライセンスを消費しますが、これは接続されている場合に限ります。ユーザー/デバイスライセンスを使用している場合、ライセンスは90日間有効です。未使用の事前起動および維持されているセッションは、デフォルトで15分後に切断されます。この値はPowerShellで構成できます（`New/Set-BrokerSessionPreLaunch` コマンドレット）。
- これらの機能が互いに補完し合うように調整するには、ユーザーのアクティビティパターンを慎重に計画し、監視することが不可欠です。最適な構成とは、ユーザーがアプリケーションをより早く利用できるというメリットと、ライセンスの使用とリソースの割り当てにかかるコストとのバランスが取れているものです。

- Citrix Workspaceアプリで、スケジュールされた時刻にセッションの事前起動を構成することもできます。

未使用の事前起動セッションと残存セッションがアクティブなままになる期間

ユーザーがアプリケーションを起動しない場合に、未使用のセッションがアクティブなままになる期間を指定する方法はいくつかあります。構成されたタイムアウトとサーバー負荷のしきい値です。これらすべてを構成できます。最初に発生したイベントにより、未使用のセッションが終了します。

- **タイムアウト:** 構成されたタイムアウトは、未使用の事前起動セッションまたは残存セッションがアクティブなままになる分、時間、または日数を指定します。タイムアウトを短く設定しすぎると、事前起動セッションは、ユーザーにアプリケーションへのより迅速なアクセスという利点を提供する前に終了します。タイムアウトを長く設定しすぎると、サーバーに十分なリソースがないため、受信ユーザー接続が拒否される可能性があります。

  このタイムアウトは、管理コンソールからではなく、SDKからのみ有効にできます (`New/Set-BrokerSessionPreLaunch` コマンドレット)。タイムアウトを無効にすると、そのデリバリーグループのコンソール表示や**デリバリーグループの編集**ページには表示されません。

- **しきい値:** サーバー負荷に基づいて事前起動セッションと残存セッションを自動的に終了することで、サーバーリソースが利用可能であると仮定して、セッションが可能な限り開いたままになることを保証します。未使用の事前起動セッションと残存セッションは、新しいユーザーセッションにリソースが必要なときに自動的に終了されるため、接続拒否を引き起こしません。

  2つのしきい値を構成できます。デリバリーグループ内のすべてのサーバーの平均負荷率と、グループ内の単一サーバーの最大負荷率です。しきい値を超えると、事前起動または残存状態にあった時間が最も長いセッションが終了されます。負荷がしきい値を下回るまで、セッションは1分間隔で1つずつ終了されます。しきい値を超えている間は、新しい事前起動セッションは開始されません。

Controllerに登録されていないVDAを持つサーバーと、メンテナンスモードのサーバーは、完全にロードされていると見なされます。計画外の停止により、容量を解放するために事前起動セッションと残存セッションが自動的に終了します。

セッションの事前起動を有効にするには

1. ナビゲーションペインで を選択します。
2. グループを選択し、操作ペインで**デリバリーグループの編集**をクリックします。
3. **アプリケーションの事前起動**ページで、セッションを起動するタイミングを選択して、セッションの事前起動を有効にします。

- ユーザーがアプリケーションを起動したとき。これはデフォルト設定です。セッションの事前起動は無効になっています。
- デリバリーグループ内の任意のユーザーがCitrix Workspaceアプリ for Windowsにログオンしたとき。
- ユーザーおよびユーザーグループのリスト内のいずれかのユーザーがCitrix Workspaceアプリ for Windowsにログオンしたとき。このオプションを選択する場合は、ユーザーまたはユーザーグループも指定してください。

アプリケーションの事前起動セッションページ(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/dws-session-2.png)

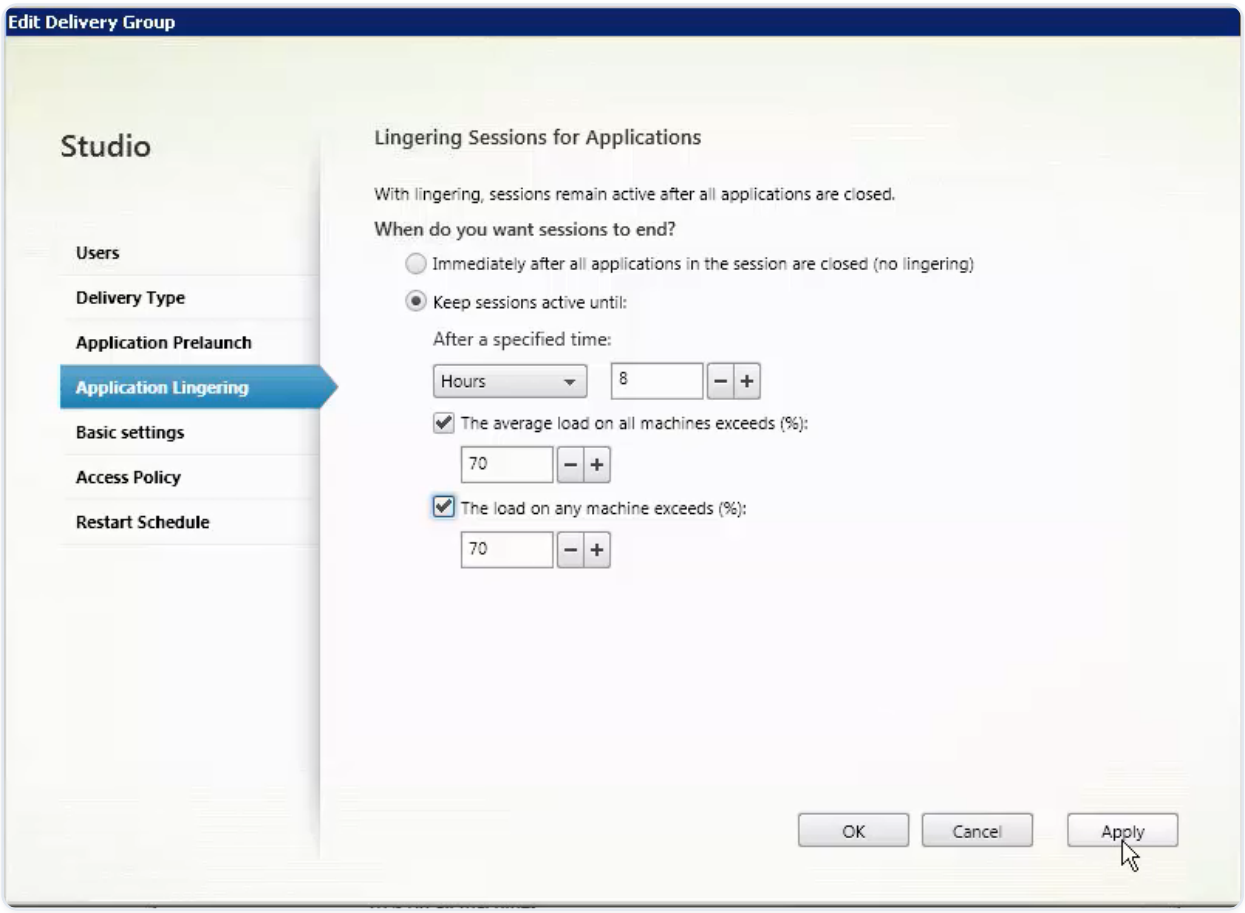
4. ユーザーがアプリケーションを起動すると、事前起動されたセッションは通常のセッションに置き換えられます。ユーザーがアプリケーションを起動しない場合（事前起動されたセッションが未使用の場合）、以下の設定がそのセッションがアクティブなままになる期間に影響します。

   - 指定された時間間隔が経過したとき。時間間隔は変更できます（1〜99日、1〜2376時間、または1〜142,560分）。
   - デリバリーグループ内のすべてのマシンの平均負荷が指定された割合（1〜99%）を超えたとき。
   - デリバリーグループ内のいずれかのマシンの負荷が指定された割合（1〜99%）を超えたとき。

   まとめ：事前起動されたセッションは、ユーザーがアプリケーションを起動する、指定された時間が経過する、または指定された負荷しきい値を超える、のいずれかのイベントが発生するまでアクティブなままです。

セッションの維持を有効にするには

1. ナビゲーションペインで を選択します。
2. グループを選択し、操作ペインで**デリバリーグループの編集**をクリックします。
3. **アプリケーションの維持**ページで、**セッションをアクティブなままにする期間**を選択して、セッションの維持を有効にします。



4. ユーザーが別のアプリケーションを起動しない場合、残存セッションがアクティブなままになる期間に影響する設定がいくつかあります。

   - 指定された時間間隔が経過した場合。時間間隔は、1～99日、1～2376時間、または1～142,560分に変更できます。
   - デリバリーグループ内のすべてのマシンの平均負荷が指定された割合（1～99%）を超えた場合。
   - デリバリーグループ内のいずれかのマシンの負荷が指定された割合（1～99%）を超えた場合。

   まとめ：残存セッションは、ユーザーがアプリケーションを起動する、指定された時間が経過する、または指定された負荷しきい値を超える、のいずれかのイベントが発生するまでアクティブなままです。

メンテナンスモードのマシンから切断された場合のセッション再接続を制御する

> **注：**
>
> この機能はPowerShellでのみ利用可能です。

> メンテナンスモードのマシンで切断されたセッションが、デリバリーグループ内のマシンに再接続できるかどうかを制御できます。

バージョン2106より前は、メンテナンスモードのマシンから切断されたシングルセッションのプールされたデスクトップセッションの再接続は許可されていませんでした。バージョン2106以降では、メンテナンスモードのマシンから切断された後の再接続（セッションの種類に関係なく）を許可または禁止するようにデリバリーグループを構成できます。

デリバリーグループを作成または編集する際（`New-BrokerDesktopGroup`、`Set-BrokerDesktopGroup`）、`-AllowReconnectInMaintenanceMode <boolean>`パラメーターを使用して、メンテナンスモードのマシンから切断されたマシンへの再接続を許可または禁止します。

- trueに設定すると、セッションはグループ内のマシンに再接続できます。
- 「false」に設定されている場合、セッションはグループ内のマシンに再接続できません。

デフォルト値:

- シングルセッション: 無効
- マルチセッション: 有効

トラブルシューティング

- デリバリーコントローラーに登録されていないVDAは、仲介されたセッションの起動時には考慮されません。これにより、利用可能なリソースが十分に活用されない結果となります。VDAが登録されない理由はさまざまあり、その多くは管理者がトラブルシューティングできます。詳細表示には、カタログ作成ウィザードおよびデリバリーグループにカタログを追加した後のトラブルシューティング情報が提供されます。

  デリバリーグループを作成した後、デリバリーグループの詳細ペインには、登録可能だが登録されていないマシンの数が表示されます。たとえば、1台以上のマシンが電源オンでメンテナンスモードではないが、現在Controllerに登録されていない場合などです。「登録されていないが、登録されるべき」マシンを表示するときは、詳細ペインの**トラブルシューティング**タブで考えられる原因と推奨される是正措置を確認してください。

  機能レベルに関するメッセージについては、「VDAのバージョンと機能レベル」を参照してください。

  VDA登録のトラブルシューティングについては、「CTX136668」を参照してください。
- デリバリーグループの表示では、詳細ペインの**インストール済みVDAバージョン**が、マシンに実際にインストールされているバージョンと異なる場合があります。マシンのWindowsのプログラムと機能の表示には、実際のVDAバージョンが表示されます。

- **電源状態不明**のステータスのマシンについては、ガイダンスとしてCTX131267を参照してください。

アプリケーショングループの作成

はじめに

アプリケーショングループを使用すると、アプリケーションのコレクションを管理できます。異なるデリバリーグループ間で共有されるアプリケーション、またはデリバリーグループ内のユーザーのサブセットによって使用されるアプリケーションに対してアプリケーショングループを作成します。アプリケーショングループはオプションであり、同じアプリケーションを複数のデリバリーグループに追加する代替手段を提供します。デリバリーグループを複数のアプリケーショングループに関連付けたり、アプリケーショングループを複数のデリバリーグループに関連付けたりできます。

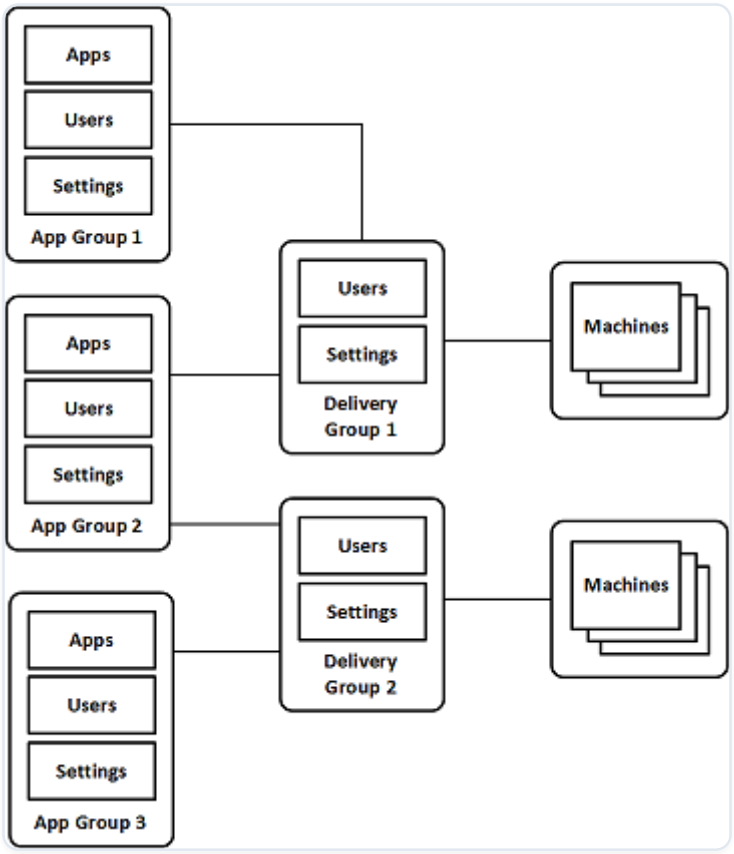
アプリケーショングループを使用すると、より多くのデリバリーグループを使用する場合と比較して、アプリケーション管理とリソース制御の利点が得られます。

- アプリケーションとその設定を論理的にグループ化することで、それらのアプリケーションを単一の単位として管理できます。たとえば、同じアプリケーションを個々のデリバリーグループに1つずつ追加（公開）する必要はありません。
- アプリケーショングループ間のセッション共有は、リソース消費を節約できます。それ以外の場合、アプリケーショングループ間のセッション共有を無効にすることが有益な場合もあります。
- タグ制限機能を使用すると、選択したデリバリーグループ内のマシンのサブセットのみを考慮して、アプリケーショングループからアプリケーションを公開できます。タグ制限を使用すると、既存のマシンを複数の公開タスクに使用できるため、追加のマシンの展開と管理に関連するコストを節約できます。タグ制限は、デリバリーグループ内のマシンを細分化（またはパーティション分割）するものと考えることができます。タグ制限付きのアプリケーショングループまたはデスクトップを使用すると、デリバリーグループ内のマシンのサブセットを分離してトラブルシューティングする際に役立ちます。

構成例

例 1:

次のグラフィックは、アプリケーショングループを含むCitrix Virtual Apps and Desktops™展開を示しています。



この構成では、アプリケーションはデリバリーグループではなくアプリケーショングループに追加されます。デリバリーグループは、どのマシンが使用されるかを指定します。（図には示されていませんが、マシンはマシンカタログ内にあります。）

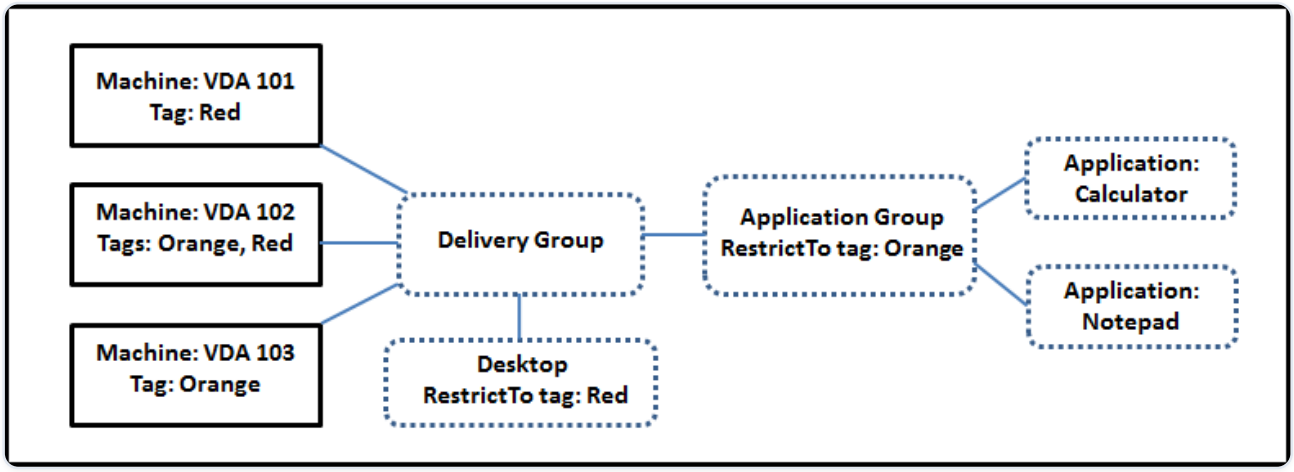
アプリケーショングループ1はデリバリーグループ1に関連付けられています。アプリケーショングループ1で指定されたユーザーがアプリケーショングループ1のアプリケーションにアクセスします。これらのグループは、デリバリーグループ1のユーザーリストにも含まれている場合にのみ表示されます。この構成は、アプリケーショングループのユーザーリストが、関連付けられたデリバリーグループのユーザーリストのサブセット（制限）であるというガイダンスに従います。アプリケーショングループ1の設定（アプリケーショングループ間のアプリケーションセッション共有、関連付けられたデリバリーグループなど）は、そのグループ内のアプリケーションとユーザーに適用されます。デリバリーグループ1の設定は、アプリケーショングループ1と2のユーザーに適用されます。これは、これらのアプリケーショングループがそのデリバリーグループに関連付けられているためです。

アプリケーショングループ2は、2つのデリバリーグループ（1と2）に関連付けられています。これらの各デリバリーグループには、アプリケーショングループ2で優先度が割り当てられ、アプリケーションが起動されるときにデリバリーグループがチェックされる順序を示します。優先度が等しいデリバリーグループはロードバランスされます。アプリケーショングループ2で指定されたユーザーがアプリケーショングループ2のアプリケーションにアクセスします。ただし、それらの

ユーザーはデリバリーグループ1とデリバリーグループ2のユーザーリストにも含まれている必要があります。

例 2:

このシンプルなレイアウトでは、タグ制限を使用して、特定のデスクトップおよびアプリケーションの起動に考慮されるマシンを制限します。このサイトには、1つの共有デリバリーグループ、1つの公開デスクトップ、および2つのアプリケーションで構成された1つのアプリケーショングループがあります。



3台のマシン（VDA 101～103）のそれぞれにタグが追加されています。

アプリケーショングループは「Orange」タグ制限付きで作成されました。その各アプリケーションは、そのデリバリーグループ内で「Orange」タグを持つマシン（VDA 102および103）でのみ起動されます。

アプリケーショングループ（およびデスクトップ）でタグ制限を使用するためのより包括的な例とガイダンスについては、「タグ」を参照してください。

ガイダンスと考慮事項

Citrix®は、アプリケーションをアプリケーショングループまたはデリバリーグループのいずれかに追加することを推奨しており、両方に追加することは推奨していません。そうしないと、2種類のグループにアプリケーションが存在することによる複雑さが増し、管理がより困難になる可能性があります。

デフォルトでは、アプリケーショングループは有効になっています。アプリケーショングループを作成した後、グループを編集してこの設定を変更できます。「アプリケーショングループの管理」を参照してください。

デフォルトでは、アプリケーショングループ間のアプリケーションセッション共有は有効になっています。「アプリケーショングループ間のセッション共有」を参照してください。

Citrixでは、デリバリーグループを現在のバージョンにアップグレードすることをお勧めします。このプロセスには、次のものが必要です。

1. デリバリーグループで使用されているマシン上のVDAをアップグレードする。
2. それらのマシンを含むマシンカタログのアップグレード。
3. デリバリーグループのアップグレード。

詳細については、「デリバリーグループの管理」を参照してください。

アプリケーショングループを使用するには、コアコンポーネントが最小バージョン7.9である必要があります。

アプリケーショングループを作成するには、Delivery Group Administrator の組み込みロールの委任管理権限が必要です。詳細については、「委任管理」(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/secure/delegated-administration.html) を参照してください。

この記事では、アプリケーションを複数のアプリケーショングループに「関連付ける」ことについて言及しています。これは、利用可能なソースからそのアプリケーションのインスタンスを追加する操作とは区別されます。同様に、デリバリーグループは、互いの追加やコンポーネントではなく、アプリケーショングループに関連付けられます。

アプリケーショングループとのセッション共有

アプリケーションセッション共有が有効になっている場合、すべてのアプリケーションは同じアプリケーションセッションで起動します。これにより、より多くのアプリケーションセッションを起動するコストが削減され、コピー＆ペースト操作など、クリップボードを使用するアプリケーション機能の使用が可能になります。ただし、状況によってはセッション共有をクリアできます。

アプリケーショングループを使用する場合、デリバリーグループのみを使用する場合に利用できる標準のセッション共有動作を拡張する、次の3つの方法でアプリケーションセッション共有を構成できます。

- アプリケーショングループ間でセッション共有が有効。
- 同じアプリケーショングループ内のアプリケーション間でのみセッション共有が有効。
- セッション共有が無効。

アプリケーショングループ間のセッション共有

アプリケーショングループ間でアプリケーションセッション共有を有効にすることも、または、同じアプリケーショングループ内のアプリケーションにのみアプリケーションセッション共有を制限するために無効にすることもできます。

- **アプリケーショングループ間のセッション共有を有効にすることが役立つ例:**

  アプリケーショングループ1にはWordやExcelなどのMicrosoft Officeアプリケーションが含まれています。アプリケーショングループ2にはメモ帳や電卓などの他のアプリケーションが含まれており、両方のアプリケーショングループは同じデリバリーグループにアタッチされています。両方のアプリケーショングループにアクセスできるユーザーは、Wordを起動してアプリケーションセッションを開始し、次にメモ帳を起動します。コントローラーが、Wordを実行しているユーザーの既存のセッションがメモ帳の実行に適していると判断した場合、メモ帳は既存のセッション内で開始されます。メモ帳が既存のセッションから実行できない場合（たとえば、タグ制限によってセッションが実行されているマシンが除外される場合など）、セッション共有を使用するのではなく、適切なマシン上に新しいセッションが作成されます。

- **アプリケーショングループ間のセッション共有を無効にすることが役立つ例:**

  同じマシンにインストールされている他のアプリケーションとうまく相互運用できない一連のアプリケーションの構成。たとえば、同じソフトウェアスイートの2つの異なるバージョンや、同じWebブラウザーの2つの異なるバージョンなどです。ユーザーが同じセッションで両方のバージョンを起動することを許可しないようにしたい場合。

  ソフトウェアスイートのバージョンごとにアプリケーショングループを作成し、各バージョンのソフトウェアスイートのアプリケーションを対応するアプリケーショングループに追加します。これらのアプリケーショングループのそれぞれでグループ間のセッション共有が無効になっている場合、それらのグループで指定されたユーザーは、同じバージョンのアプリケーションを同じセッションで実行できます。ユーザーは同時に他のアプリケーションを実行できますが、同じセッションでは実行できません。異なるバージョンのアプリケーション、またはアプリケーショングループに含まれていないアプリケーションを起動すると、そのアプリケーションは新しいセッションで起動されます。

このアプリケーショングループ間のセッション共有機能は、セキュリティサンドボックス機能ではありません。これは完璧ではなく、ユーザーが他の手段（例えば、Windows Explorer経由など）でセッションにアプリケーションを起動するのを防ぐことはできません。

マシンが容量に達している場合、新しいセッションはそのマシンでは開始されません。必要に応じて、セッション共有を使用して、新しいアプリケーションがそのマシンの既存のセッションで開始されます。

アプリケーションセッション共有が許可されているアプリケーショングループに対してのみ、事前起動セッションを利用可能にできます。（セッションリンガー機能を使用するセッションは、すべてのアプリケーショングループで利用可能です。）これらの機能は、アプリケーショングルー

プに関連付けられている各デリバリーグループで有効にして構成する必要があります。アプリケーショングループ内でこれらを構成することはできません。

デフォルトでは、アプリケーショングループを作成する際に、アプリケーショングループ間のアプリケーションセッション共有が有効になります。グループ作成時にこれを変更することはできません。アプリケーショングループを作成した後、グループを編集してこの設定を変更できます。アプリケーショングループの管理を参照してください。

アプリケーショングループ内でのセッション共有を無効にする

同じアプリケーショングループ内のアプリケーション間でのアプリケーションセッション共有を防ぐことができます。

- **アプリケーショングループ内でのセッション共有を無効にすることが役立つ例:**

  ユーザーに、別々のモニターでアプリケーションの複数の同時フルスクリーンセッションにアクセスさせたい場合。

  アプリケーショングループを作成し、そこにアプリケーションを追加します。

デフォルトでは、アプリケーショングループを作成すると、アプリケーションセッション共有が有効になります。グループの作成時にこの設定を変更することはできません。アプリケーショングループを作成した後、グループを編集してこの設定を変更できます。「アプリケーショングループの管理」を参照してください。

アプリケーショングループを作成する

アプリケーショングループを作成するには：

1. Studioナビゲーションペインで を選択し、アクションペインで を選択します。
2. ウィザードは ページから起動します。このページは、今後のウィザード起動時に表示しないように設定できます。
3. ウィザードは、次のセクションで説明するページを順に案内します。各ページの作業が完了したら、概要ページに到達するまで をクリックします。

手順1. デリバリーグループ

デリバリーグループページには、すべてのデリバリーグループと、各グループに含まれるマシンの数が一覧表示されます。

- リストには、選択できるデリバリーグループが表示されます。互換性のあるデリバリーグループには、ランダム（永続的または静的に割り当てられていない）なマルチセッションまたはシングルセッションOSマシンが含まれています。

- リストには、選択できないデリバリーグループが表示されます。各エントリには、静的に割り当てられたマシンが含まれているなど、互換性がない理由が説明されています。

アプリケーショングループは、アプリケーションを配信できる共有（プライベートではない）マシンを含むデリバリーグループに関連付けることができます。

以下の両方の条件が満たされている場合、デスクトップのみを配信する共有マシンを含むデリバリーグループを選択することもできます。

- デリバリーグループに共有マシンが含まれており、XenDesktopバージョン7.9より前のバージョンで作成されていること。
- デリバリーグループの編集権限があること。

アプリケーショングループ作成ウィザードがコミットされると、デリバリーグループの種類は自動的に「デスクトップとアプリケーション」に変換されます。

関連付けられたデリバリーグループがないアプリケーショングループを作成することはできますが（アプリケーションを整理するため、または現在使用されていないアプリケーションのストレージとして機能させるためなど）、少なくとも1つのデリバリーグループが指定されるまで、そのアプリケーショングループをアプリケーションの配信に使用することはできません。また、デリバリーグループが指定されていない場合、「**スタートから**」メニューソースからアプリケーショングループにアプリケーションを追加することはできません。

選択したデリバリーグループは、アプリケーションの配信に使用されるマシンを指定します。アプリケーショングループに関連付けるデリバリーグループの横にあるチェックボックスをオンにします。

タグ制限を追加するには、「**タグを持つマシンへの起動を制限する**」を選択し、ドロップダウンリストからタグを選択します。

手順2. ユーザー

アプリケーショングループでアプリケーションユーザーを指定します。前のページで選択したデリバリーグループ内のすべてのユーザーとユーザーグループを許可するか、それらのデリバリーグループから特定のユーザーとユーザーグループを選択します。使用を特定のユーザーに制限する場合、デリバリーグループ、アプリケーショングループで指定されたユーザーのみがこのグループのアプリケーションにアクセスできます。基本的に、アプリケーショングループのユーザーリストは、デリバリーグループのユーザーリストに対するフィルターとして機能します。

認証されていないユーザーによるアプリケーションの使用の有効化または無効化は、アプリケーショングループではなく、デリバリーグループでのみ利用できます。

展開でユーザーリストが指定される場所については、「ユーザーリストが指定される場所」を参照してください。

ステップ3. アプリケーション

知っておくと良いこと:

- デフォルトでは、追加する新しいアプリケーションは「**Applications**」という名前のフォルダーに配置されます。別のフォルダーを指定できます。アプリケーションを追加しようとしたときに、そのフォルダーに同じ名前のアプリケーションが存在する場合、追加しようとしているアプリケーションの名前を変更するよう求められます。提案された一意の名前に同意すると、その新しい名前でアプリケーションが追加されます。そうでない場合は、追加する前に自分で名前を変更する必要があります。詳細については、「アプリケーションフォルダーの管理」を参照してください。
- アプリケーションのプロパティ（設定）は、追加時または後で変更できます。「アプリケーションプロパティの変更」を参照してください。同じ名前の2つのアプリケーションを同じユーザーに公開する場合は、Studioで プロパティを変更してください。そうしないと、Citrix Workspaceアプリでユーザーに重複する名前が表示されます。
- アプリケーションを複数のアプリケーショングループに追加する場合、それらのすべてのグループでアプリケーションを表示するのに十分な権限がないと、表示の問題が発生する可能性があります。そのような場合は、より高い権限を持つ管理者に相談するか、アプリケーションが追加されたすべてのグループを含むようにスコープを拡張してください。

アプリケーションソースを表示するには、ドロップダウンメニューから「**追加**」をクリックします。

- **スタートメニューから**：選択したデリバリーグループ内のマシンで検出されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストが表示された新しいページが起動します。追加するアプリケーションのチェックボックスをオンにして、「**OK**」をクリックします。

  以下のいずれかを選択した場合、このソースは選択できません。

  - 関連付けられたデリバリーグループがないアプリケーショングループ。
  - 関連付けられたデリバリーグループにマシンが含まれていないアプリケーショングループ。
  - マシンが含まれていないデリバリーグループ。
- **手動で定義**：サイト内またはネットワーク内の別の場所にあるアプリケーション。このソースを選択すると、実行可能ファイルへのパス、作業ディレクトリ、オプションのコマンドライン

引数、管理者とユーザーの表示名を入力する新しいページが起動します。この情報を入力したら、「**OK**」をクリックします。

- **既存**：以前にサイトに追加されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストが表示された新しいページが起動します。追加するアプリケーションのチェックボックスをオンにして、「**OK**」をクリックします。サイトにアプリケーションがない場合、このソースは選択できません。
- **App-V**: App-Vパッケージ内のアプリケーション。このソースを選択すると、新しいページが起動し、そこで または を選択します。表示された画面から、追加するアプリケーションのチェックボックスをオンにして、 をクリックします。詳しくは、「App-V」を参照してください。App-Vがサイト用に構成されていない場合、このソースは選択できません（または表示されない場合があります）。

記載されているように、「**追加**」ドロップダウンメニューの一部のエントリは、その種類の有効なソースがない場合、選択できません。互換性のないソースはまったく表示されません（たとえば、アプリケーショングループにアプリケーショングループを追加することはできないため、アプリケーショングループを作成するときにそのソースは表示されません）。

ステップ4. スコープ

このページは、以前にカスタムスコープを作成した場合にのみ表示されます。デフォルトでは、**すべて**のスコープが選択されています。詳細については、委任管理を参照してください。

ステップ5. 概要

アプリケーショングループの名前を入力します。説明を（オプションで）入力することもできます。

概要情報を確認し、**「完了」**をクリックします。

アプリケーショングループの管理

はじめに

この記事では、作成したアプリケーショングループを管理する方法について説明します。

アプリケーショングループまたはデリバリーグループ内のアプリケーションの管理方法については、アプリケーションを参照してください。これには、以下の方法が含まれます。

- アプリケーショングループ内のアプリケーションを追加または削除する。
- アプリケーショングループの関連付けを変更する。

アプリケーショングループの管理には、Delivery Group Administratorの組み込みロールの委任管理権限が必要です。詳細については、委任管理を参照してください。

アプリケーショングループを有効または無効にする

アプリケーショングループが有効になっている場合、そのグループに追加されたアプリケーションを配信できます。アプリケーショングループを無効にすると、そのグループ内の各アプリケーションが無効になります。ただし、それらのアプリケーションが他の有効なアプリケーショングループにも関連付けられている場合、それらの他のグループから配信できます。アプリケーションがアプリケーショングループに関連付けられたデリバリーグループに明示的に追加された場合、アプリケーショングループを無効にしても、それらのデリバリーグループ内のアプリケーションには影響しません。

アプリケーショングループは作成時に有効になります。グループ作成時にこの設定を変更することはできません。

1. Studioナビゲーションペインで「**アプリケーション**」を選択します。
2. 中央ペインでアプリケーショングループを選択し、操作ペインで「**アプリケーショングループの編集**」を選択します。
3. **設定**ページで、**アプリケーショングループを有効にする**チェックボックスをオンまたはオフにします。
4. ウィンドウを開いたままにするには、**適用**をクリックするか、変更を適用してウィンドウを閉じるには、**OK**をクリックします。

アプリケーショングループ間のアプリケーションセッション共有を有効または無効にする

アプリケーションセッション共有は、アプリケーショングループの作成時に有効になります。この構成は、グループの作成時に変更できません。詳細については、「アプリケーショングループとのセッション共有」を参照してください。

1. Studioナビゲーションペインで「**アプリケーション**」を選択します。
2. 中央ペインでアプリケーショングループを選択し、操作ペインで「**アプリケーショングループの編集**」を選択します。
3. ページで、 チェックボックスをオンまたはオフにします。
4. ウィンドウを開いたままにするには、**適用**をクリックするか、変更を適用してウィンドウを閉じるには、**OK**をクリックします。

アプリケーショングループ内でのアプリケーションセッション共有を無効にする

同じアプリケーショングループ内のアプリケーション間でのセッション共有は、アプリケーショングループの作成時にデフォルトで有効になります。アプリケーショングループ間でのアプリケーションセッション共有を無効にしても、同じアプリケーショングループ内のアプリケーション間でのセッション共有は有効のままです。

PowerShell SDKを使用して、アプリケーションセッション共有を無効にしたアプリケーショングループを構成できます。場合によっては、このオプションが望ましいことがあります。たとえば、ユーザーに非シームレスアプリケーションを別のモニターの全画面表示アプリケーションウィンドウで起動させたい場合があります。

アプリケーショングループ内でアプリケーションセッション共有を無効にすると、そのグループ内の各アプリケーションは新しいアプリケーションセッションで起動します。同じアプリケーションを実行している適切な切断されたセッションが利用可能な場合、そのセッションが再接続されます。たとえば、メモ帳を実行している切断されたセッションがある状態でメモ帳を起動すると、新しいセッションを作成する代わりにそのセッションが再接続されます。複数の適切な切断されたセッションが利用可能な場合、ランダムではあるものの決定論的な方法で、いずれかのセッションが再接続のために選択されます。同じ状況が再発した場合、同じセッションが選択されますが、それ以外の場合にセッションが予測可能であるとは限りません。

PowerShell SDKを使用して、既存のアプリケーショングループ内のすべてのアプリケーションのアプリケーションセッション共有を無効にするか、アプリケーションセッション共有を無効にしたグループを作成します。

PowerShellコマンドレットの例

セッション共有を無効にするには、Broker PowerShellコマンドレット `New-BrokerApplicationGroup` または `Set-BrokerApplicationGroup` を使用し、パラメーター `SessionSharingEnabled` を `False` に、パラメーター `SingleAppPerSession` を `True` に設定します。

- たとえば、グループ内のすべてのアプリケーションでアプリケーションセッション共有を無効にしたアプリケーショングループを作成するには、次のようにします。

  ```
  New-BrokerApplicationGroup AppGr1 -SessionSharingEnabled $False
  -SingleAppPerSession $True
  ```

- たとえば、既存のアプリケーショングループ内のすべてのアプリケーション間でアプリケーションセッション共有を無効にするには、次のようにします。

```
Set-BrokerApplicationGroup AppGR1 -SessionSharingEnabled $False
-SingleAppPerSession $True
```

考慮事項

- `SingleAppPerSession` プロパティを有効にするには、`SessionSharingEnabled` プロパティを False に設定する必要があります。両方のプロパティを同時に有効にすることはできません。`SessionSharingEnabled` パラメーターは、アプリケーショングループ間のセッション共有を指します。
- アプリケーションセッション共有は、アプリケーショングループに関連付けられているがデリバリーグループには関連付けられていないアプリケーションでのみ機能します。デリバリーグループに直接関連付けられているすべてのアプリケーションは、デフォルトでセッションを共有します。
- アプリケーションが複数のアプリケーショングループに割り当てられている場合は、グループの設定が競合しないようにしてください。たとえば、一方のグループのオプションが `True` に設定され、もう一方のグループのオプションが `False` に設定されている場合、予期しない動作が発生します。

アプリケーショングループの名前を変更する

1. Studioナビゲーションペインで「**アプリケーション**」を選択します。
2. 中央ペインでアプリケーショングループを選択し、操作ペインで「**アプリケーショングループ名の変更**」を選択します。
3. 新しい一意の名前を指定し、 をクリックします。

アプリケーショングループとのデリバリーグループの関連付けを追加、削除、または優先度を変更する

アプリケーショングループは、アプリケーションを配信できる共有（プライベートではない）マシンを含むデリバリーグループに関連付けることができます。

以下の両方の条件が満たされている場合、デスクトップのみを配信する共有マシンを含むデリバリーグループを選択することもできます。

- デリバリーグループには共有マシンが含まれており、バージョン7.9より前のバージョンで作成されました。
- デリバリーグループの編集権限があること。

ダイアログがコミットされると、デリバリーグループの種類は自動的に「デスクトップとアプリケーション」に変換されます。

1. Studioナビゲーションペインで「**アプリケーション**」を選択します。
2. 中央ペインでアプリケーショングループを選択し、操作ペインで「**アプリケーショングループの編集**」を選択します。
3. ページを選択します。
4. デリバリーグループを追加するには、 をクリックします。利用可能なデリバリーグループのチェックボックスをオンにします。（互換性のないデリバリーグループは選択できません。）選択が完了したら、 をクリックします。
5. デリバリーグループを削除するには、削除するグループのチェックボックスをオンにして、 をクリックします。確認を求められたら削除を確定します。
6. デリバリーグループの優先度を変更するには、デリバリーグループのチェックボックスをオンにして、 をクリックします。優先度（0 = 最高）を入力し、 をクリックします。
7. 変更を適用してウィンドウを開いたままにするには、**適用**をクリックするか、変更を適用してウィンドウを閉じるには、**OK**をクリックします。

アプリケーショングループのタグ制限を追加、変更、または削除する

タグ制限の追加、変更、削除は、アプリケーション起動の対象となるマシンに予期せぬ影響を与える可能性があります。タグの考慮事項と注意事項を確認してください。

1. Studioナビゲーションペインで「**アプリケーション**」を選択します。
2. 中央ペインでアプリケーショングループを選択し、操作ペインで「**アプリケーショングループの編集**」を選択します。
3. **デリバリーグループ**ページを選択します。
4. タグ制限を追加するには、**タグを持つマシンへの起動を制限する**を選択し、ドロップダウンリストからタグを選択します。
5. タグ制限を変更または削除するには、別のタグを選択するか、**このタグを持つマシンへの起動を制限する**のチェックを外してタグ制限を完全に削除します。
6. 変更を適用してウィンドウを開いたままにするには、**適用**をクリックするか、変更を適用してウィンドウを閉じるには、**OK**をクリックします。

アプリケーショングループのユーザーを追加または削除する

ユーザーの詳細については、「アプリケーショングループの作成」を参照してください。

1. Studioナビゲーションペインで「**アプリケーション**」を選択します。
2. 中央ペインでアプリケーショングループを選択し、操作ペインで「**アプリケーショングループの編集**」を選択します。

3. **ユーザー**ページを選択します。関連付けられたデリバリーグループのすべてのユーザーにアプリケーショングループ内のアプリケーションの使用を許可するか、特定のユーザーとグループのみに許可するかを指定します。ユーザーを追加するには、**追加**をクリックし、追加するユーザーを指定します。ユーザーを削除するには、1人以上のユーザーを選択し、**削除**をクリックします。
4. 変更を適用してウィンドウを開いたままにするには、**適用**をクリックするか、変更を適用してウィンドウを閉じるには、**OK**をクリックします。

アプリケーショングループのスコープを変更する

スコープは、作成した場合にのみ変更できます (すべてのスコープは編集できません)。詳細については、「委任管理」を参照してください。

1. Studioナビゲーションペインで、 を選択します。
2. 中央ペインでアプリケーショングループを選択し、操作ペインで を選択します。
3. ページを選択します。スコープの横にあるチェックボックスをオンまたはオフにします。
4. 変更を適用してウィンドウを開いたままにするには、**適用**をクリックするか、変更を適用してウィンドウを閉じるには、**OK**をクリックします。

アプリケーショングループを削除する

アプリケーションは、少なくとも1つのデリバリーグループまたはアプリケーショングループに関連付けられている必要があります。アプリケーショングループを削除した結果、1つ以上のアプリケーションがどのグループにも属さなくなった場合、そのグループを削除するとそれらのアプリケーションも削除されるという警告が表示されます。その後、削除を確定またはキャンセルできます。

アプリケーションを削除しても、元のソースから削除されるわけではありません。ただし、再度利用可能にする場合は、もう一度追加する必要があります。

1. Studioナビゲーションペインで、 を選択します。
2. 中央ペインでアプリケーショングループを選択し、操作ペインで を選択します。
3. プロンプトが表示されたら、削除を確定します。

リモートPCアクセス

Remote PC Accessは、Citrix Virtual Apps and Desktops™の機能であり、組織が従業員に企業リソースへのリモートアクセスを安全な方法で簡単に許可できるようにします。Citrixプラットフォームは、ユーザーが物理的なオフィスPCにアクセスできるようにすることで、この安全なア

クセスを可能にします。ユーザーがオフィスPCにアクセスできれば、仕事に必要なすべてのアプリケーション、データ、およびリソースにアクセスできます。Remote PC Accessは、テレワークに対応するための他のツール（たとえば、仮想デスクトップやアプリケーション、およびそれらに関連するインフラストラクチャ）を導入および提供する必要性を排除します。

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

この機能は、**Remote PC Access**タイプのマシンカタログで構成されており、次の機能を提供します。

- OUを指定してマシンを追加する機能。この機能により、PCの一括追加が容易になります。
- オフィスWindows PCにログインするユーザーに基づいた自動ユーザー割り当て。シングルユーザーおよび複数ユーザーの割り当てをサポートしています。

Citrix Virtual Apps and Desktopsは、他の種類のマシンカタログを使用することで、物理PCのより多くのユースケースに対応できます。これらのユースケースには、次のものが含まれます。

- 物理Linux PC
- プールされた物理PC（つまり、ランダムに割り当てられ、専用ではないもの）

注:

サポートされているOSバージョンの詳細については、シングルセッションOSおよびLinux VDAのVDAのシステム要件を参照してください。

オンプレミス展開の場合、Remote PC AccessはCitrix Virtual Apps and Desktops AdvancedまたはPremiumライセンスでのみ有効です。セッションは、他のCitrix Virtual Desktops™セッションと同じ方法でライセンスを消費します。Citrix Cloudの場合、Remote PC AccessはCitrix DaaS（旧Citrix Virtual Apps and Desktopsサービス）およびWorkspace Premium Plusで有効です。

考慮事項

Citrix Virtual Apps and Desktops全般に適用されるすべての技術要件と考慮事項はRemote PC Accessにも適用されますが、物理PCの使用事例により関連性が高い、または排他的なものもあります。

重要:

Windows 11物理システム（および一部のWindows 10を実行しているシステム）には、仮想化ベースのセキュリティ機能が含まれており、その結果、VDAソフトウェアがそれらを仮想マシンとして誤って検出します。この問題を軽減するには、以下のオプションがあります。

- VDAコマンドラインインストールの一部として、「/remotepc」オプションとともに「/physicalmachine」オプションを使用する
- 上記のオプションを使用しなかった場合は、VDAのインストール後に以下のレジストリ値を追加します `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`
  - 名前: ForceEnableRemotePC
  - 種類: DWORD
  - データ: 1

展開に関する考慮事項

Remote PC Accessの展開を計画する際には、いくつかの一般的な決定を下します。

- 既存のCitrix Virtual Apps and Desktops展開にRemote PC Accessを追加できます。このオプションを選択する前に、次の点を考慮してください。
  - 現在のDelivery ControllerまたはCloud Connectorは、Remote PC Access VDAに関連する追加の負荷をサポートするために適切にサイジングされていますか？
  - オンプレミスサイトのデータベースおよびデータベースサーバーは、Remote PC Access VDAに関連する追加の負荷をサポートするために適切にサイジングされていますか？
  - 既存のVDAと新しいRemote PC Access VDAは、サイトあたりの最大サポートVDA数を超えますか？
- VDAは自動プロセスを通じてオフィスPCに展開する必要があります。利用可能なオプションは次のとおりです。

  - SCCMなどの電子ソフトウェア配布 (ESD) ツール: SCCMを使用してVDAをインストールする。
  - 展開スクリプト: スクリプトを使用してVDAをインストールする。
- Remote PC Accessのセキュリティに関する考慮事項を確認してください。

マシンカタログに関する考慮事項

必要なマシンカタログの種類は、ユースケースによって異なります。

- Remote PC Accessマシンカタログ
  - Windows専用PC
  - Windows専用マルチユーザーPC。このユースケースは、複数のユーザーが異なるシフトでリモートからアクセスできる物理的なオフィスPCに適用されます。
  - プールされたWindows PC。このユースケースは、コンピューターラボのように、複数のランダムなユーザーがアクセスできる物理PCに適用されます。
- シングルセッションOSマシンカタログ
  - 静的 - 専用Linux PC
  - ランダム - プールされたLinux PC

マシンカタログの種類を特定したら、次の点を考慮してください。

- 1台のマシンは、一度に1つのマシンカタログにのみ割り当てることができます。
- 委任された管理を容易にするために、地理的な場所、部門、または各カタログの管理を適切な管理者に委任しやすくするその他のグループに基づいてマシンカタログを作成することを検討してください。
- マシンアカウントが存在するOUを選択する際は、より詳細な粒度を得るために下位レベルのOUを選択します。そのような粒度が必要ない場合は、上位レベルのOUを選択できます。たとえば、Bank/Officers/Tellersの場合、より詳細な粒度を得るには**Tellers**を選択します。それ以外の場合は、要件に基づいて**Officers**または**Bank**を選択できます。
- Remote PC Accessマシンカタログに割り当てられた後にOUを移動または削除すると、VDAの関連付けに影響を与え、今後の割り当てで問題が発生します。したがって、マシンカタログのOU割り当ての更新がActive Directoryの変更計画で考慮されるように、適切に計画してください。
- OU構造のためにマシンカタログにマシンを追加するOUを選択するのが容易でない場合、OUを選択する必要はありません。後でPowerShellを使用してカタログにマシンを追加できます。

デスクトップ割り当てがデリバリーグループで正しく構成されていれば、ユーザーの自動割り当ては引き続き機能します。ユーザー割り当てとともにマシンカタログにマシンを追加するサンプルスクリプトは、GitHubで入手できます。

- 統合されたWake on LANは、**Remote PC Access**タイプのマシンカタログでのみ利用可能です。

Linux VDAに関する考慮事項

以下の考慮事項は、Linux VDAに固有のものです。

- 物理マシンでは、Linux VDAを非3Dモードでのみ使用してください。NVIDIAドライバーの制限により、HDX™ 3Dモードが有効になっている場合、PCのローカル画面はブラックアウトされず、セッションのアクティビティが表示されます。この画面を表示することはセキュリティリスクです。
- 物理Linuxマシンには、シングルセッションOSタイプのマシンカタログを使用します。
- 自動ユーザー割り当てはLinuxマシンでは利用できません。
- ユーザーがすでにローカルでPCにログオンしている場合、StoreFront™からPCを起動しようとすると失敗します。
- 省電力オプションはLinuxマシンでは利用できません。

技術要件と考慮事項

このセクションでは、物理PCの技術要件と考慮事項について説明します。

- 以下はサポートされていません。
  - KVMスイッチ、またはセッションを切断できるその他のコンポーネント。
  - ハイブリッドPC（オールインワンPC、NVIDIA Optimus搭載ノートPC、PCを含む）。
  - デュアルブートマシン。
- キーボードとマウスはPCに直接接続してください。モニターや、電源を切ったり切断したりできるその他のコンポーネントに接続すると、これらの周辺機器が利用できなくなる可能性があります。入力デバイスをモニターなどのコンポーネントに接続する必要がある場合は、それらのコンポーネントの電源を切らないでください。
- PCはActive Directory Domain Servicesドメインに参加している必要があります。
- セキュアブートはWindows 10およびWindows 11でのみサポートされています。
- PCにはアクティブなネットワーク接続が必要です。信頼性と帯域幅を向上させるには、有線接続が推奨されます。

- Wi-Fiを使用する場合は、次の操作を行います。

  a. 電源設定でワイヤレスアダプターをオンのままにするように設定します。

  b. ユーザーがログオンする前にワイヤレスネットワークに自動的に接続できるように、ワイヤレスアダプターとネットワークプロファイルを構成します。そうしないと、ユーザーがログオンするまでVDAは登録されません。ユーザーがログオンするまで、PCはリモートアクセスに利用できません。

  c. Delivery ControllerまたはCloud ConnectorがWi-Fiネットワークから到達可能であることを確認します。

- ラップトップコンピューターでRemote PC Accessを使用できます。ラップトップがバッテリーで動作するのではなく、電源に接続されていることを確認してください。ラップトップの電源オプションをデスクトップPCのオプションと一致するように構成します。例：

  a. 休止状態機能を無効にします。

  b. スリープ機能を無効にします。

  c. 蓋を閉じたときの動作を**何もしない**に設定します。

  d. 「電源ボタンを押したときの動作」を**シャットダウン**に設定します。

  e. ビデオカードとNICの省電力機能を無効にします。

- Remote PC Accessは、Windows 10を搭載したSurface Proデバイスでサポートされています。前述のラップトップと同じガイドラインに従ってください。
- ドッキングステーションを使用している場合、ラップトップのドッキング解除と再ドッキングが可能です。ラップトップをドッキング解除すると、VDAはWi-Fi経由でDelivery ControllerまたはCloud Connectorに再登録されます。ただし、ラップトップを再ドッキングしても、ワイヤレスアダプターを切断しない限り、VDAは有線接続に切り替わりません。一部のデバイスには、有線接続が確立されたときにワイヤレスアダプターを切断する組み込み機能が提供されています。その他のデバイスでは、ワイヤレスアダプターを切断するためにカスタムソリューションまたはサードパーティ製ユーティリティが必要です。前述のWi-Fiに関する考慮事項を確認してください。

  Remote PC Accessデバイスのドッキングとドッキング解除を有効にするには、次の操作を行います。

  a. **スタート**メニューで、**設定 > システム > 電源とスリープ**を選択し、**スリープ**を**なし**に設定します。

  b. 「**デバイスマネージャー > ネットワークアダプター > イーサネットアダプター**」で「**電源の管理**」に移動し、「**電力節約のために、コンピューターでこのデバイスの電源をオフに**

できるようにする」のチェックを外します。「**このデバイスで、コンピューターのスタンバイ状態を解除できるようにする**」がオンになっていることを確認してください。

- 同じオフィスPCにアクセスする複数のユーザーには、Citrix Workspaceで同じアイコンが表示されます。ユーザーがCitrix Workspaceにログオンすると、そのリソースが他のユーザーによってすでに使用されている場合、利用不可として表示されます。
- オフィスPCにアクセスする各クライアントデバイス（たとえば、自宅のPC）にCitrix Workspaceアプリをインストールします。

構成シーケンス

このセクションでは、**Remote PC Access**タイプのマシンカタログを使用する場合にRemote PC Accessを構成する方法の概要を説明します。その他の種類のマシンカタログの作成方法については、マシンカタログの作成を参照してください。

1. オンプレミスサイトのみ - 統合されたWake on LAN機能を使用するには、Wake on LANに記載されている前提条件を構成してください。
2. Remote PC Access用に新しいCitrix Virtual Apps and Desktopsサイトが作成された場合：

   a. **Remote PC Access**サイトタイプを選択します。

   b. **電源の管理**ページで、デフォルトのRemote PC Accessマシンカタログの電源管理を有効または無効にするかを選択します。この設定は、後でマシンカタログのプロパティを編集して変更できます。Wake on LANの構成の詳細については、Wake on LANを参照してください。

   c. **ユーザー**ページと**マシンアカウント**ページで情報を入力します。

   これらの手順を完了すると、**Remote PC Access Machines**という名前のマシンカタログと、**Remote PC Access Desktops**という名前のデリバリーグループが作成されます。
3. 既存のCitrix Virtual Apps and Desktopsサイトに追加する場合：

   a. **Remote PC Access**タイプのマシンカタログを作成します（ウィザードの「オペレーティングシステム」ページ）。マシンカタログの作成方法の詳細については、マシンカタログの作成を参照してください。ターゲットPCがRemote PC Accessで使用できるよう、適切なOUを割り当ててください。

   b. マシンカタログ内のPCへのユーザーアクセスを提供するために、デリバリーグループを作成します。デリバリーグループの作成方法の詳細については、デリバリーグループの作成を参照してください。デリバリーグループを、PCへのアクセスを必要とするユーザーを含むActive Directoryグループに割り当ててください。

4. オフィスPCにVDAを展開します。

   - シングルセッションOSコアVDAインストーラー（VDAWorkstationCoreSetup.exe）を使用することをお勧めします。
   - シングルセッションフルVDAインストーラー（VDAWorkstationSetup.exe）を`/remotepc`オプションとともに使用することもできます。これは、コアVDAインストーラーを使用した場合と同じ結果になります。
   - ヘルプデスクチームがCitrix Directorを介してリモートサポートを提供できるように、Windowsリモートアシスタンスを有効にすることを検討してください。これを行うには、`/enable_remote_assistance`オプションを使用します。詳細については、「コマンドラインを使用したインストール」を参照してください。
   - Directorでログオン期間情報を表示するには、シングルセッションのフルVDAインストーラーを使用し、**Citrix User Profile Management WMI Plugin** コンポーネントを含める必要があります。このコンポーネントを含めるには、`/includeadditional`オプションを使用します。詳細については、「コマンドラインを使用したインストール」を参照してください。
   - SCCMを使用してVDAを展開する方法については、「SCCMを使用したVDAのインストール」を参照してください。
   - 展開スクリプトを使用してVDAを展開する方法については、「スクリプトを使用したVDAのインストール」を参照してください。

   手順2～4を正常に完了すると、ユーザーがPCにローカルでログオンしたときに、自分のマシンに自動的に割り当てられます。

5. ユーザーに、オフィスPCにリモートでアクセスするために使用する各クライアントデバイスにCitrix Workspaceアプリをダウンロードしてインストールするよう指示します。Citrix Workspaceアプリは、`https://www.citrix.com/downloads/`またはサポートされているモバイルデバイスのアプリケーションストアから入手できます。

レジストリを介して管理される機能

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

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

複数ユーザーの自動割り当てを無効にする

各Delivery Controller™で、次のレジストリ設定を追加します。

`HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer`

- 名前: AllowMultipleRemotePCAssignments
- 種類: DWORD
- データ: 0

スリープモード (最小バージョン 7.16)

Remote PC Accessマシンをスリープ状態にするには、VDAにこのレジストリ設定を追加し、マシンを再起動します。再起動後、オペレーティングシステムの省電力設定が適用されます。事前設定されたアイドルタイマーが経過すると、マシンはスリープモードに入ります。マシンがウェイクアップすると、Delivery Controllerに再登録されます。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 名前: DisableRemotePCSleepPreventer
- 種類: DWORD
- データ: 1

セッション管理

デフォルトでは、ローカルユーザーがそのマシンでセッションを開始すると（CTRL+ALT+DELを押すことで）、リモートユーザーのセッションは自動的に切断されます。この自動動作を防ぐには、オフィスPCに次のレジストリエントリを追加し、マシンを再起動します。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- 名前: SasNotification
- 種類: DWORD
- データ: 1

デフォルトでは、接続メッセージがタイムアウト期間内に確認されない場合、リモートユーザーがローカルユーザーよりも優先されます。この動作を設定するには、以下の設定を使用します。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- 名前: RpcaMode
- 種類: DWORD
- データ:
  - 1 - 指定されたタイムアウト期間内にメッセージングUIに応答しない場合、リモートユーザーが常に優先されます。この設定が構成されていない場合、この動作がデフォルトです。
  - 2 - ローカルユーザーが優先されます。

Remote PC Accessモードを適用するためのタイムアウトは、デフォルトで30秒です。このタイムアウトは構成できますが、30秒未満に設定しないでください。タイムアウトを構成するには、このレジストリ設定を使用します。

`HKLM\SOFTWARE\Citrix\PortICA\RemotePC`

- 名前: RpcaTimeout
- 種類: DWORD
- データ: タイムアウトの秒数（10進値）

ユーザーが強制的にコンソールアクセスを取得したい場合: ローカルユーザーは、10秒の間にCtrl+Alt+Delを2回押すことで、リモートセッションのローカル制御を取得し、切断イベントを強制できます。

レジストリ変更とマシンの再起動後、リモートユーザーが使用中にローカルユーザーがCtrl+Alt+Delを押してそのPCにログオンしようとすると、リモートユーザーにプロンプトが表示されます。このプロンプトは、ローカルユーザーの接続を許可するか拒否するかを尋ねます。接続を許可すると、リモートユーザーのセッションは切断されます。

セッション管理のログ記録

Remote PC Accessには、アクティブなICA®セッションを持つPCに誰かがアクセスしようとしたときにログを記録する機能が追加されました。これにより、不要なアクティビティや予期しないアクティビティがないか環境を監視し、インシデントを調査する必要がある場合にそのようなイベントを監査できます。

イベントはWindowsイベントビューアーを使用してログに記録され、**Applications and Services > Citrix > HostCore > ICA Service > Admin**にあります。

Remote PC Accessを使用すると、3つの異なるイベントがログに記録されます。

Ctrl+Alt+Delイベント

このイベントは、アクティブなリモートセッション中にローカルユーザーがコンソールキーボードでCtrl+Alt+Delを押したときに表示されます。

イベントの詳細

- ログ名: アプリケーションとサービス
- イベントID: 43, 44, 45
- ソース: ICA サービス

イベント ID 43

このイベント ID は、SasNotification レジストリ値が存在しない場合、または SasNotification レジストリ値が 0 の場合に表示されます。

- メッセージ:

```
Ctrl+Alt+Del has been pressed on the endpoint.

The session management behavior is set to automatically disconnect the
remote session.
```

イベント ID 44

このイベント ID は、SasNotification レジストリ値が 1 で、RpcaMode レジストリ値が 1 の場合、または RpcaMode レジストリ値が存在しない場合に表示されます。

- メッセージ:

```
Ctrl+Alt+Del has been pressed on the endpoint.

The session management behavior is set to notify the remote user. The
user preference is set to remote user.
```

イベント ID 45

このイベント ID は、SasNotification レジストリ値が 1 で、RpcaMode レジストリ値が 2 の場合に表示されます。

- メッセージ:

```
Ctrl+Alt+Del has been pressed on the endpoint.

The session management behavior is set to notify the remote user.

The user preference is set to local user.
```

リモートセッション切断イベント

このイベントは、さまざまな理由でリモートセッションが切断された場合に表示されます。

イベントの詳細

- ログ名: アプリケーションとサービス
- イベント ID: 46, 47, 48
- ソース: ICA Service

イベントID 46

このイベントIDは、リモートセッションが切断され、SasNotification レジストリ値が存在しないか、SasNotification レジストリ値が0である場合に表示されます。

- メッセージ:

```
The remote session for &lt;remoteUserName> has been disconnected.
```

イベントID 47

このイベントIDは、リモートユーザーがセッションの切断に同意し、SasNotification レジストリ値が1であり、RpcaMode レジストリ値が1であるか、RpcaMode レジストリ値が2であるか、または RpcaMode レジストリ値が存在しない場合に表示されます。

- メッセージ:

```
The remote session for &lt;remoteUserName> has been disconnected
because the user accepted the request to disconnect the session.
```

イベントID 48

このイベントIDは、リモートユーザーが指定されたタイムアウト期間内に切断要求を拒否せず、SasNotification レジストリ値が1であり、RpcaMode レジストリ値が2である場合に表示されます。

- メッセージ:

```
The remote session for &lt;remoteUserName> has been disconnected
because the user did not decline the disconnection request within the
configured timeout period (&lt;timeout period>).
```

Ctrl+Alt+Del 2回押しイベント

このイベントは、10秒以内にCtrl+Alt+Delが2回押された場合に表示されます。

イベントの詳細

- ログ名: アプリケーションとサービス
- イベントID: 49
- ソース: ICA Service

イベントID 49

このイベントIDは、Ctrl+Alt+Delが10秒以内に2回押されたときに表示されます。

- メッセージ:

```
The remote session for &lt;remoteUserName> has been forcibly
disconnected.
```

Wake on LAN (ウェイク・オン・ラン)

Remote PC AccessはWake on LANをサポートしており、ユーザーは物理PCをリモートで起動できます。この機能により、ユーザーは使用していないときにオフィスPCの電源を切ったままにして、エネルギーコストを節約できます。また、誤ってマシンの電源が切れてしまった場合でも、リモートアクセスを可能にします。

Wake on LAN機能を使用すると、デリバリーコントローラーからの指示があった場合、PC上で実行されているVDAから、そのPCが存在するサブネットにマジックパケットが直接送信されます。これにより、追加のインフラストラクチャコンポーネントやマジックパケット配信のためのサードパーティソリューションに依存することなく、この機能が動作します。

Wake on LAN機能は、レガシーなSCCMベースのWake on LAN機能とは異なります。SCCMベースのWake on LANの詳細については、「Wake on LAN – SCCM統合」を参照してください。

制限事項

Wake on LAN機能を使用するRemote PC Accessは、ピーク時の自動電源オンをサポートしていません。

システム要件

Wake on LAN機能を使用するためのシステム要件は次のとおりです。

- コントロールプレーン:
  - シトリックス DaaS™
  - シトリックス バーチャルアプリおよびデスクトップ 2009以降
- 物理PC:
  - VDAバージョン2009以降
  - Windows 10またはWindows 11。サポートの詳細については、VDAシステム要件を参照してください。
  - BIOS/UEFIでWake on LANが有効になっていること
  - Windows構成内のネットワークアダプターのプロパティでWake on LANが有効になっていること

Wake on LANの構成

オンプレミスのCitrix Virtual Apps and Desktopsを使用している場合、統合Wake on LANの構成はPowerShellを使用してのみサポートされます。

Wake on LANを構成するには:

1. まだ Remote PC Access マシンカタログがない場合は、作成します。
2. まだ Wake on LAN ホスト接続がない場合は、作成します。

> **注：**
>
> Wake on LAN機能を使用するには、「Microsoft Configuration Manager Wake on LAN」タイプのホスト接続がある場合、新しいホスト接続を作成します。

3. Wake on LANホスト接続の一意の識別子を取得します。
4. Wake on LAN ホスト接続をマシンカタログに関連付けます。

Wake on LAN ホスト接続を作成するには：

```
# Load Citrix SnapIns

Add-PSSnapIn -Name "*citrix*"



# Provide the name of the Wake on LAN host connection

[string]$connectionName = "Remote PC Access Wake on LAN"



# Create the hypervisor connection

$hypHc = New-Item -Path xdhyp:\Connections `

                -Name $connectionName `

                -HypervisorAddress "N/A" `

                -UserName "woluser" `

                -Password "wolpwd" `

                -ConnectionType Custom `

                -PluginId VdaWOLMachineManagerFactory `

                -CustomProperties "<CustomProperties></CustomProperties>"
`

                -Persist



$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid



# Wait for the connection to be ready before trying to use it
```

```
while (-not $bhc.IsReady)

{

    Start-Sleep -s 5

    $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid

}
```

ホスト接続の準備ができたら、次のコマンドを実行してホスト接続の一意の識別子を取得します。

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"

$hypUid = $bhc.Uid
```

接続の一意の識別子を取得したら、次のコマンドを実行して、その接続をRemote PC Accessマシンカタログに関連付けます。

```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog
-RemotePCHypervisorConnectionUid $hypUid
```

設計上の考慮事項

Remote PC Access で Wake on LAN を使用する予定がある場合は、次の点を考慮してください。

- 複数のマシンカタログで同じ Wake on LAN ホスト接続を使用できます。
- ある PC が別の PC を起動するには、両方の PC が同じサブネット内にあり、同じ Wake on LAN ホスト接続を使用している必要があります。PC が同じマシンカタログ内にあるか、異なるマシンカタログ内にあるかは関係ありません。
- ホスト接続は特定のゾーンに割り当てられます。展開に複数のゾーンが含まれている場合は、各ゾーンに Wake on LAN ホスト接続が必要です。これはマシンカタログにも当てはまります。
- マジックパケットはグローバルブロードキャストアドレス255.255.255.255を使用してブロードキャストされます。このアドレスがブロックされていないことを確認してください。

- そのサブネット内のマシンを起動できるようにするには、Wake on LAN接続ごとに、サブネット内に少なくとも1台のPCが電源オンになっている必要があります。

運用上の考慮事項

Wake on LAN機能を使用する際の考慮事項は次のとおりです。

- 統合されたWake on LAN機能を使用してPCを起動できるようにするには、VDAが少なくとも1回登録されている必要があります。
- Wake on LANはPCを起動するためにのみ使用できます。再起動やシャットダウンなどの他の電源操作はサポートしていません。
- Wake on LAN接続が作成されると、Studioに表示されます。ただし、Citrix Virtual Apps and Desktopsオンプレミスを使用している場合、Studio内でそのプロパティを編集することはサポートされていません。
- マジックパケットは次の2つの方法のいずれかで送信されます。

  a. ユーザーが自分のPCへのセッションを起動しようとし、VDAが未登録の場合

  b. 管理者がStudioまたはPowerShellから手動で電源オンコマンドを送信した場合

- デリバリーコントローラーはPCの電源状態を認識しないため、Studioでは電源状態の下に**サポートされていません**と表示されます。デリバリーコントローラーはVDA登録状態を使用して、PCがオンかオフかを判断します。

Wake on LAN – SCCM統合

SCCM統合Wake on LANは、Remote PC Accessの代替Wake on LANオプションであり、オンプレミスのCitrix Virtual Apps and Desktopsでのみ利用可能です。

システム要件

SCCM統合Wake on LAN機能を使用するためのシステム要件は次のとおりです。

- シトリックス バーチャル アプリケーションズ アンド デスクトップ 1912 以降
- 物理PC:
  - VDA バージョン 1912 以降
  - Windows 10。サポートの詳細については、VDA システム要件を参照してください。
  - BIOS/UEFIでWake on LANが有効になっていること
  - Windows構成内のネットワークアダプターのプロパティでWake on LANが有効になっていること

- システムセンターコンフィギュレーションマネージャー (SCCM) 2012 R2 以降

SCCM 統合型 Wake on LAN の構成

以下の前提条件を完了してください。

1. 組織内で SCCM 2012 R2、2016、または 2019 を構成します。次に、すべての Remote PC Access マシンに SCCM クライアントを展開し、スケジュールされた SCCM インベントリサイクルが実行されるのを待つか、必要に応じて手動で強制実行します。
2. Wake Proxy のサポートについては、SCCM でオプションを有効にします。Remote PC Access Wake on LAN 機能を使用する PC を含む組織内の各サブネットについて、3 台以上のマシンがセンチネルマシンとして機能できることを確認してください。
3. マジックパケットのサポートについては、サブネット指向ブロードキャストまたはユニキャストのいずれかを使用してマジックパケットを送信できるように、ネットワークルーターとファイアウォールを構成します。
4. 各PCのBIOS/UEFI設定でWake on LANを構成します。
5. まだ行っていない場合は、VDAを物理PCに展開します。

前提条件に対処した後、Delivery Controller が SCCM と通信できるように、次の手順を完了します。

1. SCCM のホスト接続を作成します。詳細については、接続とリソースを参照してください。
    - 接続の種類として **Microsoft Configuration Manager Wake on LAN** を選択します。
    - 入力された資格情報には、スコープ内のコレクションへのアクセス権があり、**Remote Tools Operator** ロールが必要です。
2. Studioで接続を選択し、**接続の編集**を選択して、**詳細設定**をクリックします。
3. Wake on LANの処理に適したオプションを選択します。
    - Wake-upプロキシを使用している場合は、最初のオプションである**Microsoft System Center Configuration Manager Wake-upプロキシ**を選択します。
    - マジックパケットを使用している場合は、2番目のオプションである**Delivery Controllerによって送信されるWake on LANパケット**を選択します。
        - 適切な送信方法（**サブネット指向ブロードキャスト**または**ユニキャスト**）を選択します。

ホスト接続を作成したら、その接続をRemote PC Accessカタログに関連付けます。

- 新しいRemote PC Accessカタログを作成する場合は、カタログ作成ウィザードの**オペレーティングシステム**ページで、カタログの種類として**Remote PC Access**を選択し、ドロップダウンリストから適切な接続を選択します。
- 既存のRemote PC AccessカタログにWake on LANを追加するには：

  a. Studioの**マシンカタログ**ノードに移動し、マシンカタログを選択してから、**マシンカタログの編集**を選択します。

  b. **電源管理**タブを選択し、マシンカタログの電源管理を有効にするには**はい**を選択します。

  c. ドロップダウンリストから適切な接続を選択し、**OK**をクリックします。

トラブルシューティング

モニターのブランキングが機能しない

アクティブなHDXセッション中にWindows PCのローカルモニターが空白にならず（ローカルモニターにセッションで何が起こっているかが表示される）GPUベンダーのドライバーに問題がある場合、以下のレジストリ値を設定することで、Citrix Indirect Displayドライバー（IDD）にグラフィックカードのベンダードライバーよりも高い優先順位を与え、問題を解決できます。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits`

- 名前: CitrixIDD
- 種類: DWORD
- データ: 3

ディスプレイアダプターの優先順位とモニターの作成の詳細については、Knowledge Centerの記事CTX237608を参照してください。

セッション管理通知が有効になっているマシンでCtrl+Alt+Delを選択すると、セッションが切断されます

SasNotificationレジストリ値によって制御されるセッション管理通知は、VDAでRemote PC Accessモードが有効になっている場合にのみ機能します。物理PCでHyper-Vの役割または仮想化ベースのセキュリティ機能が有効になっている場合、そのPCは仮想マシンとして報告されます。VDAが仮想マシン上で実行されていることを検出すると、Remote PC Accessモードを自動的に無効にします。Remote PC Accessモードを有効にするには、次のレジストリ値を追加します。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 名前: ForceEnableRemotePC

- 種類: DWORD
- データ: 1

設定を有効にするには、PCを再起動します。

診断情報

Remote PC Accessに関する診断情報は、Windowsアプリケーションイベントログに書き込まれます。情報メッセージはスロットリングされません。エラーメッセージは、重複するメッセージを破棄することでスロットリングされます。

- 3300（情報）: マシンがカタログに追加されました
- 3301（情報）: マシンがデリバリーグループに追加されました
- 3302（情報）: マシンがユーザーに割り当てられました
- 3303 (エラー): 例外

電源管理

Remote PC Accessの電源管理が有効になっている場合、サブネット指向ブロードキャストでは、Controllerとは異なるサブネットにあるマシンを起動できないことがあります。サブネット指向ブロードキャストを使用してサブネット間で電源管理が必要で、AMTサポートが利用できない場合は、Wake-upプロキシまたはユニキャスト方式を試してください。これらの設定が電源管理接続の詳細プロパティで有効になっていることを確認してください。

アクティブなリモートセッションはローカルのタッチスクリーン入力を記録します

VDA が Remote PC Access モードを有効にすると、マシンはアクティブなセッション中にローカルのタッチスクリーン入力を無視します。物理 PC で Hyper-V ロールまたは仮想化ベースのセキュリティ機能が有効になっている場合、その PC は仮想マシンとして報告されます。VDA が仮想マシン上で実行されていることを検出すると、Remote PC Access モードを自動的に無効にします。Remote PC Access モードを有効にするには、次のレジストリ設定を追加します。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 名前: ForceEnableRemotePC
- 種類: DWORD
- データ: 1

設定を有効にするには、PC を再起動してください。

その他のリソース

以下は Remote PC Access に関するその他のリソースです。

- ソリューション設計ガイダンス: Remote PC Access Design Decisions。
- Remote PC Access アーキテクチャの例: Citrix Remote PC Access ソリューションのリファレンスアーキテクチャ。

アプリブイ

Citrix Virtual Apps and Desktops™ で App-V を使用する

Microsoft Application Virtualization (App-V) を使用すると、アプリケーションをサービスとして展開、更新、サポートできます。ユーザーは、自分のデバイスにアプリケーションをインストールすることなく、アプリケーションにアクセスできます。App-V と Microsoft User State Virtualization (USV) は、場所やインターネット接続に関係なく、アプリケーションとデータへのアクセスを提供します。 次の表に、サポートされているバージョンを示します。

アプリブイ	CITRIX VIRTUAL APPS AND DESKTOPS デリバリーコントローラー	シトリックス バーチャルアプリおよびデスクトップ VDA
5.0 および 5.0 SP1	XenDesktop 7 以降、XenApp 7.5 以降	7.0 以降
5.0 SP2	XenDesktop 7 以降、XenApp 7.5 以降	7.1 以降
5.0 SP3 および 5.1	XenDesktop 7.6 以降、XenApp 7.6 以降	7.6.300 以降
Windows Server 2016 における App-V	XenDesktop 7.12 以降、XenApp 7.12 以降	7.12 以降

App-V クライアントは、アプリケーションへのオフラインアクセスをサポートしていません。App-V 統合サポートには、アプリケーション用の SMB 共有の使用が含まれます。HTTP プロトコルはサポートされていません。 App-V に詳しくない場合は、Microsoft のドキュメントを参照してください。この記事で言及されている App-V コンポーネントの概要を以下に示します。

- **管理サーバー**。App-V インフラストラクチャを管理するための一元化されたコンソールを提供し、App-V デスクトップクライアントとリモートデスクトップサービスクライアントの両方に

仮想アプリケーションを配信します。App-V 管理サーバーは、管理者に必要なセキュリティ、測定、監視、およびデータ収集を認証、要求、提供します。このサーバーは、Active Directory とサポートツールを使用してユーザーとアプリケーションを管理します。

- **公開サーバー**。特定のユーザー向けにアプリケーションを App-V クライアントに提供し、ストリーミング用の仮想アプリケーションパッケージをホストします。管理サーバーからパッケージを取得します。
- **クライアント**。仮想アプリケーションを取得し、クライアント上でアプリケーションを公開し、Windows デバイス上で実行時に仮想環境を自動的にセットアップおよび管理します。App-V クライアントは VDA にインストールされ、各ユーザーのプロファイルにレジストリやファイルの変更などのユーザー固有の仮想アプリケーション設定を保存します。

アプリケーションは、事前の構成やオペレーティングシステム設定の変更なしにシームレスに利用できます。App-V アプリケーションは、サーバー OS およびデスクトップ OS のデリバリーグループから起動できます。

- Citrix Workspace™ アプリ経由で
- App-V クライアントと Citrix Workspace アプリ経由で
- 複数のユーザーが複数のデバイスで同時に
- Citrix StoreFront™ 経由で

変更された App-V アプリケーションプロパティは、アプリケーションが起動されたときに実装されます。たとえば、表示名が変更されたアプリケーションやカスタマイズされたアイコンを持つアプリケーションの場合、ユーザーがアプリケーションを起動すると変更が反映されます。動的構成ファイルに保存されたアプリケーションのカスタマイズも、アプリケーションの起動時に適用されます。

管理方法

App-V シーケンサーで作成され、App-V サーバーまたはネットワーク共有に配置されている App-V パッケージと動的構成ファイルを使用できます。

- **App-Vサーバー:** App-Vサーバー上のパッケージからアプリケーションを使用するには、StudioとApp-Vサーバー間で、検出、構成、VDAへのダウンロードのために継続的な通信が必要です。これにより、ハードウェア、インフラストラクチャ、および管理のオーバーヘッドが発生します。特にユーザー権限については、StudioとApp-Vサーバーを同期させておく必要があります。

  App-Vパッケージとアプリケーションへのアクセスには StudioとApp-Vサーバーの両方のコンソールが必要なため、これは*デュアル管理者*管理方法と呼ばれます。この方法は、App-Vと

Citrixの緊密に連携した展開で最も効果的です。この方法では、管理サーバーが動的構成ファイルを処理します。デュアル管理者管理方法を使用する場合、Citrix App-Vコンポーネントは、アプリケーションの起動に必要な適切な公開サーバーの登録を管理します。これにより、適切なタイミングでユーザーに対して公開サーバーが同期されます。公開サーバーは、構成された設定を使用して、パッケージのライフサイクル（ログオン時の更新や接続グループなど）の他の側面を維持します。

- **ネットワーク共有:** ネットワーク共有に配置されたパッケージとXML展開構成ファイルは、StudioのApp-Vサーバーおよびデータベースインフラストラクチャへの依存をなくし、オーバーヘッドを削減します。（各VDAにMicrosoft App-Vクライアントをインストールする必要があります。）

  App-Vパッケージとアプリケーションの使用にはStudioコンソールのみが必要なため、これは*シングル管理者*管理方法と呼ばれます。ネットワーク共有を参照し、その場所から1つ以上のApp-Vパッケージをサイトレベルのアプリケーションライブラリに追加します。この方法では、アプリケーションが起動されると、Citrix App-Vコンポーネントが展開構成ファイルを処理します。（ユーザー構成ファイルはサポートされていません。）シングル管理者管理方法を使用する場合、Citrix App-Vコンポーネントはホストマシン上のパッケージのライフサイクルのすべての側面を管理します。パッケージは、ブローカーの起動時、または構成変更が検出されたとき（セッション起動時でも可能）にマシンに追加されます。パッケージは、Citrix Workspaceアプリから起動要求が受信されたときに、「ジャストインタイム」でオンデマンドで個々のユーザーに初めて公開されます。

  シングル管理者は、Studioで作成された分離グループ構成定義を満たすために必要な接続グループのライフサイクルも管理します。

  *アプリケーションライブラリ*は、App-Vパッケージに関する情報を格納するキャッシュリポジトリを指すCitrix用語です。アプリケーションライブラリには、他のCitrixアプリケーション配信テクノロジーに関する情報も格納されます。

どちらの管理方法でも、VDAがユーザーデータを破棄するように構成されている場合、公開（または同期）は次回のセッション起動時に再実行する必要があります。

1つまたは両方の管理方法を同時に使用できます。つまり、アプリケーションをデリバリーグループに追加すると、アプリケーションはApp-Vサーバーまたはネットワーク共有にあるApp-Vパッケージから取得できます。

> **注：**

両方の管理方法を同時に使用しており、App-Vパッケージが両方の場所に動的構成ファイルを持っている場合、App-Vサーバー内のファイル（デュアル管理）が使用されます。

Studioナビゲーションペインで**構成 > App-V公開**を選択すると、App-Vパッケージ名とソースが表示されます。ソース列は、パッケージがApp-Vサーバー上にあるか、アプリケーションライブラリにキャッシュされているかを示します。パッケージを選択すると、詳細ペインにパッケージ内のアプリケーションとショートカットが一覧表示されます。

動的構成ファイル

概要

App-Vパッケージは、動的構成ファイルを使用してカスタマイズできます。これらのファイルはパッケージに適用されると、その特性を変更するために使用できます。たとえば、追加のアプリケーションショートカットや動作を定義するために使用できます。Citrix App-Vは両方のタイプの動的構成ファイルをサポートしています。ファイル設定はアプリケーションの起動時に適用されます。

- 展開構成ファイルは、すべてのユーザーに対してマシン全体の構成を提供します。これらのファイルは、\<*packageFileName*>_DeploymentConfig.xmlという名前で、適用されるApp-Vパッケージと同じフォルダーに配置されている必要があります。シングル管理者およびデュアル管理者管理でサポートされています。
- ユーザー構成ファイルは、パッケージに対するユーザーごとのカスタマイズをサポートするユーザー固有の構成を提供します。シングル管理者は、次の形式で命名されたユーザー構成ファイルをサポートします: \<*packageFileName*>_UserConfig.xml で、適用されるApp-Vパッケージと同じフォルダーに配置されている必要があります。

特定のパッケージに対して複数のユーザー構成ファイルが存在する場合、それらは次の優先順位で適用されます。

1. ユーザーSID
2. ユーザー名
3. ADグループSID (最初に見つかったものが優先)
4. ADグループ名 (最初に見つかったものが優先)
5. デフォルト

例

```
MyAppVPackage_S-1-5-21-000000001-0000000001-000000001-001_UserConfig.xml

MyAppVPackage_joeblogs_UserConfig.xml

MyAppVPackage_S-1-5-32-547_UserConfig.xml

MyAppVPackage_Power Users_UserConfig.xml

MyAppVPackage_UserConfig.xml
```

注：

ファイル名のユーザー固有の部分は、オプションで末尾に配置することもできます（例: MyAppVPackage_UserConfig_**joeblogs**.xml）。

動的構成ファイルの場所

シングル管理者管理では、Citrix App-Vコンポーネントは、App-Vパッケージと同じフォルダーにある動的構成ファイルのみを処理します。パッケージ内のアプリケーションが起動されると、対応する動的構成ファイルへの変更が再適用されます。動的構成ファイルがパッケージとは異なる場所にある場合は、マッピングファイルを使用してパッケージを展開構成ファイルにマッピングします。

マッピングファイルを作成するには

1. 新しいテキストファイルを開きます。
2. 各動的構成ファイルについて、パッケージへのパスを「\<PackageGuid> : path」の形式で指定する行を追加します。

   例:

   F1f4fd78ef044176aad9082073a0c780 : c:\widows\file\packagedeploy.xml
3. ファイルをパッケージと同じフォルダーに ctxAppVDynamicConfigurations.cfg として保存します。パッケージ内のアプリケーションが起動されるたびに、App-V パッケージと同じ UNC 共有上のディレクトリ階層全体が、このファイルを求めて再帰的に上位検索されます。

注：

> パッケージ内のアプリケーションが開いているユーザーセッションがある場合、動的展開構成に変更を適用することはできません。他のユーザー（*現在のユーザーではない*）がパッケージ内のアプリケーションを開いている場合は、動的ユーザー構成ファイルに変更を適用できます。

動的構成ファイルを使用するように IIS を構成する

VDA 上の Citrix App-V コンポーネントは、UNC ホスト型パッケージが使用するのと同じ規則に従って、パッケージの隣に配置された App-V 展開構成ファイルおよびユーザー構成ファイルを利用できます。 これを行うには、VDA コンポーネントが IIS ディレクトリ構造を参照して、使用するファイルを決定する権限が必要です。UNC ホスト型パッケージとは異なり、VDA は公開で使用する前に、まずサーバーからホストマシン上の一時的な場所に構成ファイルをダウンロードする必要があります。これはオプション機能であり、ディレクトリブラウジングが有効になっていない場合、動的構成ファイルは無視されます。

サイトのディレクトリブラウジングを有効にするには、次の手順を実行します。

1. IIS マネージャーコンソールで、Web サイトノードを選択し、中央のペインで をダブルクリックします。
2. 右側のペインで をクリックし、*時間*、*サイズ*、*拡張子*、*日付* を選択します。（長い日付は選択しないでください。）これにより、VDA 上の Citrix App-V コンポーネントは、構成ファイルの最新バージョンが適用されているかどうか、または更新が必要かどうかを判断できます。

分離グループ

App-V シングル管理者方式を使用する場合、分離グループを作成すると、サンドボックス内で実行する必要がある相互依存アプリケーションのグループを指定できます。この機能は App-V 接続グループに似ていますが、同じではありません。App-V 管理サーバーで使用される必須およびオプションのパッケージ用語の代わりに、Citrix はパッケージ展開オプションに自動および明示を使用します。

- ユーザーが App-V アプリケーション（プライマリアプリケーション）を起動すると、自動的に含めるようにマークされた他のアプリケーションパッケージが分離グループで検索されます。これらのパッケージは自動的にダウンロードされ、分離グループに含まれます。プライマリアプリケーションを含むデリバリーグループにそれらを追加する必要はありません。
- 明示的に含めるようにマークされた分離グループ内のアプリケーションパッケージは、そのアプリケーションをプライマリアプリケーションを含む同じデリバリーグループに明示的に追加した場合にのみダウンロードされます。

これにより、すべてのユーザーにグローバルに利用可能な自動的に含まれるアプリケーションが混在する分離グループを作成できます。さらに、このグループには、特定のライセンス制約を持つ可能性のあるプラグインやその他のアプリケーションのセットを含めることができ、追加の分離グループを作成することなく、特定のユーザーセット（デリバリーグループを通じて識別される）に制限できます。

たとえば、アプリケーション「app-a」の実行には JRE 1.7 が必要です。app-a（明示的な展開タイプ）と JRE 1.7（自動展開タイプ）を含む分離グループを作成できます。次に、これらの App-V パッケージを1つ以上のデリバリーグループに追加します。ユーザーが app-a を起動すると、JRE 1.7 が自動的に展開されます。

アプリケーションを複数のApp-V分離グループに追加できます。ただし、ユーザーがそのアプリケーションを起動すると、そのアプリケーションが最初に追加された分離グループが常に使用されます。そのアプリケーションを含む他の分離グループの順序付けや優先順位付けはできません。

App-Vサーバーの負荷分散

デュアル管理者管理方式を使用している場合、DNSラウンドロビンを使用した管理サーバーと公開サーバーの負荷分散がサポートされます。NetScaler、F5（または類似の）仮想IPの背後にある管理サーバーの負荷分散は、StudioがリモートPowerShellを介して管理サーバーと通信する必要があるため、サポートされていません。詳細については、Citrixのブログ記事を参照してください。

App-Vパッケージをホストおよびストリーミングするための IISの構成

IISサーバーでApp-Vパッケージをホストおよびストリーミングできるようにするには、次の手順を実行します。

1. IISマネージャーコンソールを開きます。手順については、`<https://docs.microsoft.com/ja-jp/previous-versions/iis/6.0-sdk/ms525920(v%3Dvs.90)>`を参照してください。
2. 使用するWebサイトインスタンスを右クリックし、 を選択します。
3. エイリアス名と、パッケージがネットワーク上に物理的に保存されているパスを入力します。
4. 中央ペインで をダブルクリックし、ウィンドウ内の任意の場所を右クリックして を選択します。
5. ファイル名拡張子に`.appv`と入力し、MIMEの種類に`application/app-v`を選択して、 をクリックします。

HTTPストリーミングApp-VパッケージをCitrix DaaS™（旧Citrix Virtual Apps and Desktops service）にインポートする

> **注：**
>
> この機能は、バージョン2009以降のVirtual Delivery Agents (VDAs)でのみサポートされています。HTTP(S)パスを持つApp-Vパッケージ内のアプリケーションが、機能レベル2003以降のデリバリーグループに追加された場合、それらはCitrix DaaSに公開されますが、VDAがバージョン2009以降でない限り、ユーザーはCitrix Cloudからそれらを起動できません。デリバリーグループの機能レベルについては、Create delivery groupsで説明されています。

1. *CVAD Remote PowerShell SDK* と *Citrix App-V Package Discovery module* の最新バージョンをダウンロードしてインストール/解凍します。Citrix DaaS SDKとAPIを参照してください。
2. パッケージ検出モジュールを使用して、App-VパッケージをIISサーバーからCitrix DaaSにインポートします。例：

```
Import-Module <Download
Directory>\Citrix.Cloud.AppLibrary.Admin.v1.psm1

Import-AppVPackageToCloud

–PackagePath "https://My.AppVServer.net/Packages/Notepad++.appv"
```

3. Citrix Cloud™アカウントにログインします。
4. パッケージは、お使いのマシン上の一時的な場所にダウンロードされ、そこから関連情報が抽出され、Citrix DaaSインスタンスのアプリケーションライブラリにアップロードされます。

セットアップ

次の表は、シングル管理者およびデュアル管理者管理方法を使用してCitrix Virtual Apps and DesktopsでApp-Vを使用するためのセットアップタスクの順序をまとめたものです。

シングル管理者	デュアル管理者	タスク
X	X	App-Vの展開
X	X	パッケージングと配置

シングル管理者	デュアル管理者	タスク
	X	StudioでApp-Vサーバーアドレスを構成する
X	X	VDAマシンにソフトウェアをインストールする
X		アプリケーションライブラリにApp-Vパッケージを追加する
X		App-V分離グループを追加する（オプション）
X	X	デリバリーグループにApp-Vアプリケーションを追加する

Microsoft App-Vの展開

App-Vの展開手順については、`<https://docs.microsoft.com/ja-jp/microsoft-desktop-optimization-pack/>`を参照してください。

任意でApp-V公開サーバーの設定を変更します。Citrixは、ControllerでSDKコマンドレットを使用することを推奨します。詳細については、SDKドキュメントを参照してください。

- 公開サーバーの設定を表示するには、「**Get-CtxAppvServerSetting -AppVPublishingServer \<*pubServer*>**」と入力します。
- App-Vアプリケーションが適切に起動するようにするには、「**Set-CtxAppvServerSetting –UserRefreshonLogon 0**」と入力します。

以前にGPOポリシー設定を使用して公開サーバー設定を管理していた場合、GPO設定はコマンドレット設定を含むすべてのApp-V統合設定を上書きします。これにより、App-Vアプリケーションの起動に失敗する可能性があります。Citrixは、すべてのGPOポリシー設定を削除し、SDKを使用してそれらの設定を構成することを推奨します。

パッケージングと配置

どちらの管理方法でも、App-Vシーケンサーを使用してアプリケーションパッケージを作成します。詳細については、Microsoftドキュメントを参照してください。

- シングル管理者管理の場合、パッケージとその対応する動的構成ファイルをUNCまたはSMB共有ネットワークの場所に配置します。Delivery Groupにアプリケーションを追加するStudio

管理者が、その場所に対して少なくとも読み取りアクセス権を持っていることを確認してください。

- デュアル管理者管理の場合、UNCパスからApp-V管理サーバーにパッケージを公開します。（HTTP URLからの公開はサポートされていません。）

パッケージがApp-Vサーバー上にあるかネットワーク共有上にあるかにかかわらず、Studio管理者がアクセスできるように、パッケージに適切なセキュリティ権限があることを確認してください。VDAとStudioの両方がデフォルトで読み取りアクセス権を持つように、ネットワーク共有は「Authenticated users」と共有されている必要があります。

StudioでApp-Vサーバーアドレスを構成する

> **重要:**
>
> Citrixは、App-Vサーバーが非デフォルトのプロパティ値を使用している場合、ControllerでPowerShellコマンドレットを使用してApp-Vサーバーアドレスを指定することを推奨します。詳細については、SDKドキュメントを参照してください。StudioでApp-Vサーバーアドレスを変更すると、指定した一部のサーバー接続プロパティがデフォルト値にリセットされる可能性があります。これらのプロパティは、VDAがApp-V公開サーバーに接続するために使用されます。この場合、リセットされたプロパティの非デフォルト値をサーバー上で再構成してください。

> この手順は、デュアル管理者管理方法にのみ有効です。

デュアル管理者管理方法の場合、App-V管理サーバーと公開サーバーのアドレスは、サイト作成中またはサイト作成後に指定します。これは、サイト作成中またはサイト作成後に行うことができます。

サイト作成中:

- ウィザードの**App-V**ページで、Microsoft App-V管理サーバーのURL、およびApp-V公開サーバーのURLとポート番号を入力します。
- ウィザードを続行する前に接続をテストします。テストが失敗した場合は、以下の「トラブルシューティング」セクションを参照してください。

サイト作成後:

1. Studioナビゲーションペインで、**構成 > App-V公開**を選択します。

2. 以前にApp-Vサーバーアドレスを指定していない場合は、操作ペインで**Microsoftサーバーの追加**を選択します。
3. App-Vサーバーアドレスを変更するには、操作ペインで**Microsoftサーバーの編集**を選択します。
4. Microsoft App-V管理サーバーのURL、およびApp-V公開サーバーのURLとポート番号を入力します。
5. ダイアログボックスを閉じる前に、それらのサーバーへの接続をテストします。テストが失敗した場合は、以下の「トラブルシューティング」セクションを参照してください。

後で、App-V管理サーバーおよび公開サーバーへのすべてのリンクを削除し、Studioがそれらのサーバーから App-Vパッケージを検出しないようにする場合は、操作ペインで**Microsoftサーバーの削除**を選択します。この操作は、それらのサーバー上のパッケージ内のアプリケーションが現在どのデリバリーグループにも公開されていない場合にのみ許可されます。公開されている場合は、App-Vサーバーを削除する前に、それらのアプリケーションをデリバリーグループから削除する必要があります。

VDAマシンにソフトウェアをインストールする

App-Vをサポートするには、VDAを含むマシンに2種類のソフトウェアをインストールする必要があります。1つはMicrosoft製、もう1つはCitrix製です。

Microsoft App-Vクライアント

このソフトウェアは、仮想アプリケーションを取得し、クライアント上でアプリケーションを公開し、Windowsデバイス上で実行時に仮想環境を自動的にセットアップおよび管理します。App-Vクライアントは、各ユーザーのプロファイルにレジストリやファイルの変更などのユーザー固有の仮想アプリケーション設定を保存します。

App-VクライアントはMicrosoftから入手できます。VDAを含む各マシン、またはマシンカタログでVMを作成するために使用されるマスターイメージにクライアントをインストールします。**注**: Windows 10 (1607以降) およびWindows Server 2016には、すでにApp-Vクライアントが含まれています。これらのOSでのみ、PowerShellの**Enable-AppV**コマンドレット (パラメーターなし) を実行してApp-Vクライアントを有効にします。**Get-AppVStatus**コマンドレットは、現在の有効化ステータスを取得します。

> **ヒント:**

> App-Vクライアントをインストールした後、管理者権限でPowerShellの**Get-AppvClientConfiguration**コマンドレットを実行し、EnablePackageScriptsが1に設定され

ていることを確認します。1に設定されていない場合は、**Set-AppvClientConfiguration -EnablePackageScripts $true**を実行します。

Citrix App-Vコンポーネント

Citrix App-V コンポーネントソフトウェアは、VDA のインストール時にデフォルトで除外されます。

VDA のインストール中に、このデフォルトの動作を制御できます。グラフィカルインターフェイスでは、**追加コンポーネント**ページで**Citrix Personalization for App-V - VDA**チェックボックスを選択します。コマンドラインインターフェイスでは、**/includeadditional "Citrix Personalization for App-V – VDA"**オプションを使用します。

VDA のインストール中に Citrix App-V コンポーネントを含めなかったが、後で App-V アプリケーションを使用したい場合は、Windows マシンのプログラムと機能の一覧で、**Citrix Virtual Delivery Agent**エントリを右クリックし、**変更**を選択します。ウィザードが起動します。ウィザードで、App-V 公開コンポーネントをインストールして有効にするオプションを有効にします。

アプリケーションライブラリで App-V パッケージを追加または削除する

これらの手順は、単一管理者管理方法にのみ有効です。

App-V パッケージを含むネットワーク共有への読み取りアクセス権が少なくとも必要です。

アプリケーションライブラリに App-V パッケージを追加する

1. Studio ナビゲーションペインで、**構成 > App-V 公開**を選択します。
2. 操作ペインで、**パッケージの追加**を選択します。
3. App-V パッケージを含む共有を参照し、1つまたは複数のパッケージを選択します。
4. **追加**をクリックします。

アプリケーションライブラリから App-V パッケージを削除する

アプリケーションライブラリから App-V パッケージを削除すると、Studio の App-V 公開ノードの表示から削除されます。ただし、デリバリーグループからそのアプリケーションが削除されるわけではなく、それらのアプリケーションは引き続き起動できます。パッケージは物理的なネットワークの場所に残ります。（この効果は、デリバリーグループから App-V アプリケーションを削除する場合とは異なります。）

1. Studio ナビゲーションペインで、**構成 > App-V 公開**を選択します。
2. 削除する1つまたは複数のパッケージを選択します。
3. 操作ペインで、**パッケージの削除**を選択します。

App-V分離グループの追加、編集、または削除

App-V分離グループの追加

1. Studioナビゲーションペインで、**App-V Publishing**を選択します。
2. アクションペインで、**Add Isolation Group**を選択します。
3. **Add Isolation Group Settings**ダイアログボックスで、分離グループの名前と説明を入力します。
4. 利用可能なパッケージリストから、分離グループに追加するアプリケーションを選択し、右矢印をクリックします。選択したアプリケーションは、分離グループ内のパッケージリストに表示されます。各アプリケーションの横にある**Deployment**ドロップダウンで、**Explicit**または**Automatic**のいずれかを選択します。上下の矢印を使用して、リスト内のアプリケーションの順序を変更することもできます。
5. 完了したら、**OK**をクリックします。

App-V分離グループの編集

1. Studioナビゲーションペインから、**App-V Publishing**を選択します。
2. 中央ペインで**Isolation Groups**タブを選択し、編集する分離グループを選択します。
3. アクションペインで、**Edit Isolation Group**を選択します。
4. **Edit Isolation Group Settings**ダイアログボックスで、分離グループの名前または説明を変更したり、アプリケーションを追加または削除したり、展開の種類を変更したり、アプリケーションの順序を変更したりします。
5. 完了したら、**OK**をクリックします。

App-V分離グループの削除

分離グループを削除しても、アプリケーションパッケージは削除されません。グループ化のみが削除されます。

1. Studioナビゲーションペインで**App-V公開**を選択します。
2. 中央ペインで**分離グループ**タブを選択し、削除する分離グループを選択します。
3. 操作ペインで**分離グループの削除**を選択します。
4. 削除を確認します。

App-Vアプリケーションをデリバリーグループに追加する

以下の手順では、App-Vアプリケーションをデリバリーグループに追加する方法について説明します。デリバリーグループの作成に関する詳細については、「デリバリーグループの作成」を参照してください。

手順1： 新しいデリバリーグループを作成するか、既存のデリバリーグループにApp-Vアプリケーションを追加するかを選択します。

App-Vアプリケーションを含むデリバリーグループを作成するには：

1. Studioのナビゲーションペインで**［デリバリーグループ］**を選択します。
2. 操作ペインで**デリバリーグループの作成**を選択します。
3. ウィザードの次のページで、マシンカタログとユーザーを指定します。

既存のデリバリーグループにApp-Vアプリケーションを追加するには：

1. Studioナビゲーションペインで**アプリケーション**を選択します。
2. 操作ペインで**アプリケーションの追加**を選択します。
3. App-Vアプリケーションを追加するデリバリーグループを1つ以上選択します。

手順2： ウィザードの**アプリケーション**ページで、**追加**ドロップダウンをクリックしてアプリケーションソースを表示します。**App-V**を選択します。

手順3： **App-Vアプリケーションの追加**ページで、App-Vソース（App-Vサーバーまたはアプリケーションライブラリ）を選択します。結果の表示には、アプリケーション名とパッケージ名、パッケージバージョンが含まれます。追加するアプリケーションまたはアプリケーションショートカットの横にあるチェックボックスをオンにします。次に、**OK**をクリックします。

ステップ4: ウィザードを完了します。

知っておくと良いこと:

- App-Vアプリケーションをデリバリーグループに追加する際にそのプロパティを変更した場合、変更はアプリケーションの起動時に適用されます。たとえば、アプリケーションをグループに追加する際に表示名やアイコンを変更した場合、その変更はユーザーがアプリケーションを起動したときに表示されます。
- 動的構成ファイルを使用してApp-Vアプリケーションのプロパティをカスタマイズした場合、それらのプロパティは、デリバリーグループに追加する際に行った変更を上書きします。

- App-Vアプリケーションを含むデリバリーグループを後で編集する場合、グループの配信タイプをデスクトップとアプリケーションからアプリケーションのみに変更しても、App-Vアプリケーションのパフォーマンスに変化はありません。
- 以前に公開された（単一管理者）App-Vパッケージをデリバリーグループから削除すると、Citrix App-Vクライアントコンポーネントは、単一管理者管理方法で不要になったパッケージのクリーンアップ、公開解除、および削除を試行します。
- ハイブリッド展開を使用している場合（単一管理者管理方法とApp-V公開サーバーによって配信されるパッケージがあり、デュアル管理者または別のメカニズム（グループポリシーなど）によって管理されている場合）、どの（現在冗長である可能性のある）パッケージがどのソースから来たのかを判断することはできません。この場合、クリーンアップは試行されません。
- 単一のデリバリーグループで100を超えるApp-Vアプリケーションを公開すると、アプリケーションが起動しない場合があります。その場合は、適切なバインディング要素のMaxReceivedMessageSizeプロパティを使用して、デリバリーコントローラーおよび/またはVDA上のブローカーエージェントの構成で受信可能な最大メッセージサイズを増やしてください。

トラブルシューティング

デュアル管理者方式を使用している場合にのみ発生する問題は、(DUAL)とマークされています。

(DUAL) Studioのナビゲーションペインで**構成 > App-V公開**を選択すると、PowerShell接続エラーが発生します。

- Studio管理者はApp-Vサーバー管理者でもありますか？Studio管理者は、App-V管理サーバーと通信できるように、そのサーバーの「administrators」グループに属している必要があります。

(DUAL) StudioでApp-Vサーバーアドレスを指定すると、接続テスト操作がエラーを返します。

- App-Vサーバーの電源はオンになっていますか？Pingコマンドを送信するか、IISマネージャーを確認してください。各App-Vサーバーは「Started」および「Running」状態である必要があります。
- App-VサーバーでPowerShellリモート処理が有効になっていますか？有効になっていない場合は、`<https://docs.microsoft.com/ja-jp/previous-versions/technet-magazine/ff700227(v=msdn.10)>`を参照してください。
- Studio管理者はApp-Vサーバー管理者でもありますか？Studio管理者は、App-V管理サーバーと通信できるように、そのサーバーの*administrators*グループに属している必要があります。

- App-Vサーバーでファイル共有が有効になっていますか？Windowsエクスプローラーまたは「ファイル名を指定して実行」コマンドで `\\<App-V server FQDN>` と入力してください。
- App-Vサーバーは、App-V管理者と同じファイル共有権限を持っていますか？App-Vサーバーで、 `\\<App-V server FQDN>` のエントリを に追加し、App-Vサーバーで管理者権限を持つユーザーの資格情報を指定します。ガイダンスについては、 `<http://support.microsoft.com/kb/306541>` を参照してください。
- App-VサーバーはActive Directoryにありますか？

  StudioマシンとApp-Vサーバーが信頼関係のない異なるActive Directoryドメインにある場合は、StudioマシンのPowerShellコンソールから **winrm s winrm/Config/client '@(TrustedHosts="\<*App-V server FQDN*>")'** を実行します。

  TrustedHostsがGPOによって管理されている場合、「*The config setting TrustedHosts cannot be changed because use is controlled by policies. The policy would need to be set to Not Configured to change the config setting*」というエラーメッセージが表示されます。この場合、GPOのTrustedHostsポリシー（管理用テンプレート > Windowsコンポーネント > Windowsリモート管理 (WinRM) > WinRMクライアント）にApp-Vサーバー名のエントリを追加します。

(DUAL) デリバリーグループにApp-Vアプリケーションを追加すると、検出に失敗します。

- Studio管理者はApp-V管理サーバーの管理者でもありますか？Studio管理者は、App-V管理サーバーと通信できるように、そのサーバーの *administrators* グループに属している必要があります。
- App-V管理サーバーは実行中ですか？Pingコマンドを送信するか、IISマネージャーを確認してください。各App-Vサーバーは「Started」および「Running」状態である必要があります。
- 両方のApp-VサーバーでPowerShellリモート処理が有効になっていますか？有効になっていない場合は、 `<https://docs.microsoft.com/ja-jp/previous-versions/technet-magazine/ff700227(v=msdn.10)>` を参照してください。
- パッケージはStudio管理者がアクセスするための適切なセキュリティ権限を持っていますか？

App-Vアプリケーションは1つのブラウザーバージョンでのみ起動します。

- 同じブラウザーアプリの複数のシーケンスバージョンを公開した場合、VDA上のユーザーごとに一度に起動できるアプリのバージョンは1つだけです。Citrixコンポーネントが関与しておらず、ユーザーが異なるパスを指すデスクトップショートカットからシーケンスされたアプリを起動した場合でも、同じことが発生します。

ユーザーが最初に起動したブラウザーバージョンによって、その後に実行されるブラウザーバージョンが決まります。Firefoxは、2回目の起動を検出すると、新しいプロセスを作成するのではなく、すでに実行中のプロセスのインスタンスを作成することを優先します。他のブラウザーも同様の動作をする可能性があります。

ショートカットの起動コマンドにコマンドラインパラメーター **-no-remote** を追加することで、意図したFirefoxブラウザーバージョンでアプリケーションを起動できます。他のブラウザーも同様の機能を提供しています。

> **注：**
>
> ショートカット列挙機能を利用するには、XenApp 7.17以降を使用している必要があります。また、この双方向の動作を実現するには、アプリの両方のバージョンでパッケージを変更する必要があります。

App-Vアプリケーションが起動しません。

- (DUAL) パブリッシングサーバーは実行中ですか？
- (DUAL) App-Vパッケージには、ユーザーがアクセスできるように適切なセキュリティ権限が設定されていますか？
- (DUAL) VDAで、Tempが正しい場所を指していること、およびTempディレクトリに十分な空き容量があることを確認してください。
- (DUAL) App-Vパブリッシングサーバーで、`Get-AppvPublishingServer *`を実行してパブリッシングサーバーのリストを表示します。
- (DUAL) App-Vパブリッシングサーバーで、UserRefreshonLogonがFalseに設定されていることを確認してください。
- (DUAL) App-Vパブリッシングサーバーで、管理者として**Set-AppvPublishingServer**を実行し、UserRefreshonLogonをFalseに設定します。
- VDAにサポートされているバージョンのApp-Vクライアントがインストールされていますか？VDAで**enable package scripts**設定が有効になっていますか？
- App-VクライアントとVDAを含むマシンで、レジストリエディター (regedit) から、HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\AppV に移動します。AppVServers キーが次の値形式であることを確認してください: AppVManagementServer+metadata;PublishingServer (例: `http://xmas-demo-appv.blrstrm.com+0+0+0+1+1+1+0+1;http://xmas-demo-appv.blrstrm.com:8082)`)。

- App-VクライアントとVDAを含むマシンまたはマスターイメージで、PowerShellのExecutionPolicyがRemoteSignedに設定されていることを確認します。Microsoftが提供するApp-Vクライアントは署名されておらず、このExecutionPolicyによりPowerShellは署名されていないローカルスクリプトとコマンドレットを実行できます。ExecutionPolicyを設定するには、次の2つの方法のいずれかを使用します。(1) 管理者として、コマンドレット「**Set-ExecutionPolicy RemoteSigned**」を入力する、または (2) グループポリシー設定から、 > > > > > に移動します。
- 「RegistrationManager.AttemptRegistrationWithSingleDdc: Failed to register」というエラーが表示される場合は、適切なバインディング要素のMaxReceivedMessageSizeプロパティを使用して、Delivery ControllerおよびVDA上のBroker Agentの構成で受信可能なメッセージの最大サイズを増やしてください。

これらの手順で問題が解決しない場合は、ログを有効にして確認してください。

ログ

App-V構成関連のログはC:\CtxAppvLogsにあります。アプリケーション起動ログは%LOCALAPPDATA%\Citrix\CtxAppvLogsにあります。LOCALAPPDATAはログオンしているユーザーのローカルフォルダーに解決されます。アプリケーションの起動に失敗したユーザーのローカルフォルダーを確認してください。

App-Vで使用されるStudioおよびVDAログを有効にするには、管理者権限が必要です。また、メモ帳などのテキストエディターも必要になります。

Studioログを有効にするには：

1. C:\CtxAppvLogsフォルダーを作成します。
2. C:\Program Files\Citrix\StudioAppVIntegration\SnapIn\Citrix.Appv.Admin.V1 に移動します。テキストエディターで CtxAppvCommon.dll.config を開き、次の行のコメントを解除します: \<add key ="LogFileName" value="C:\CtxAppvLogs\log.txt"/>
3. ログ記録を開始するには、Broker サービスを再起動します。

VDA ログを有効にするには:

1. C:\CtxAppvLogs フォルダーを作成します。
2. C:\Program Files\Citrix\ Virtual Desktop Agent に移動します。テキストエディターで CtxAppvCommon.dll.config を開き、次の行のコメントを解除します: \<add key ="LogFileName" value="C:\CtxAppvLogs\log.txt"/>
3. その行のコメントを解除し、value フィールドを 1 に設定します: \<add key ="EnableLauncherLogs" value="1"/>

4. ログ記録を開始するには、マシンを再起動します。

コンテンツの公開

Microsoft WordドキュメントやWebリンクなど、リソースへのURLまたはUNCパスであるアプリケーションを公開できます。この機能は「公開コンテンツ」として知られています。コンテンツを公開する機能により、ユーザーへのコンテンツ配信方法に柔軟性が加わります。既存のアクセス制御とアプリケーション管理の恩恵を受けることができます。また、コンテンツを開くためにローカルアプリケーションを使用するか、公開アプリケーションを使用するかを指定することもできます。

公開されたコンテンツは、StoreFront™およびCitrix Workspace™アプリの他のアプリケーションと同様に表示されます。ユーザーはアプリケーションにアクセスするのと同じ方法でアクセスします。クライアントでは、リソースは通常どおり開きます。

- ローカルにインストールされたアプリケーションが適切な場合、そのアプリケーションが起動されてリソースが開かれます。
- ファイルの種類に関連付けが定義されている場合、公開されたアプリケーションが起動されてリソースが開かれます。

PowerShell SDKを使用してコンテンツを公開します。Studioを使用してコンテンツを公開することはできません。ただし、公開後にStudioを使用してアプリケーションプロパティを編集することはできます。

構成の概要と準備

コンテンツの公開には、次の主要なプロパティを持つ `New-BrokerApplication` コマンドレットを使用します。（すべてのコマンドレットプロパティの説明については、コマンドレットのヘルプを参照してください。）

```
New-BrokerApplication –ApplicationType PublishedContent
-CommandLineExecutable location -Name app-name -DesktopGroup delivery-
group-name
```

`ApplicationType` プロパティは `PublishedContent` である必要があります。

`CommandLineExecutable` プロパティは、公開コンテンツの場所を指定します。以下の形式がサポートされており、255文字の制限があります。

- HTMLウェブサイトアドレス（例: `<http://www.citrix.com>`）

- ウェブサーバー上のドキュメントファイル（例: `https://www.citrix.com/press/pressrelease.doc`）
- FTPサーバー上のディレクトリ（例: `ftp://ftp.citrix.com/code`）
- FTPサーバー上のドキュメントファイル（例: `ftp://ftp.citrix.com/code/Readme.txt` >）
- UNC ディレクトリパス (例: `file://myServer/myShare or \\\\myServer\\myShare`)
- UNC ファイルパス (例: `file://myServer/myShare/myFile.asf` または `\\myServer\myShare\myFile.asf`)

正しいSDKがあることを確認してください。

- Citrix DaaS (旧Citrix Virtual Apps and Desktopsサービス) の展開の場合、ダウンロード して、Citrix Virtual Apps and Desktops Remote PowerShell SDKをインストールします。
- オンプレミスのCitrix Virtual Apps and Desktops展開の場合、Delivery Controllerとともにインストールされているの PowerShell SDKを使用します。公開コンテンツアプリケーションを追加するには、最低バージョン7.11のDelivery Controllerが必要です。

以下の手順では例を使用します。例では、次のようになります:

- マシンカタログが作成されています。
- `PublishedContentApps` という名前のデリバリーグループが作成されています。このグループは、カタログからマルチセッションOSマシンを使用します。WordPadアプリケーションがグループに追加されています。
- デリバリーグループ名、`CommandLineExecutable` の場所、およびアプリケーション名が割り当てられます。

はじめに

PowerShell SDKを含むマシンで、PowerShellを開きます。

次のコマンドレットは、適切なPowerShell SDKスナップインを追加し、返されたデリバリーグループレコードを割り当てます。

```
Add-PsSnapin Citrix&ast; $dg = Get-BrokerDesktopGroup –Name PublishedContentApps
```

Citrix DaaSを使用している場合は、Citrix Cloud™の資格情報を入力して認証します。複数の顧客がいる場合は、1つを選択します。

URLを公開する

場所とアプリケーション名を割り当てた後、次のコマンドレットはCitrix®ホームページをアプリケーションとして公開します。

```
$citrixUrl = "https://www.citrix.com/"

$appName = "Citrix Home Page"



New-BrokerApplication –ApplicationType PublishedContent –
CommandLineExecutable $citrixURL –Name $appName –DesktopGroup $dg.Uid
```

成功を確認します:

- StoreFrontを開き、PublishedContentAppsデリバリーグループ内のアプリケーションにアクセスできるユーザーとしてログオンします。デフォルトのアイコンを持つ新しく作成されたアプリケーションが表示されます。アイコンのカスタマイズについては、`<https://www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-xd7/>`を参照してください。
- **Citrix Home Page**アプリケーションをクリックします。URLは、ローカルで実行されているデフォルトブラウザの新しいタブで起動します。

UNCパスにあるリソースを公開する

この例では、管理者は`PublishedResources`という名前の共有をすでに作成しています。場所とアプリケーション名を割り当てた後、以下のコマンドレットはその共有内のRTFファイルとDOCXファイルをリソースとして公開します。

```
$rtfUNC = "\\GMSXJ-EDGE0.xd.local\\PublishedResources\\PublishedRTF.rtf"

$rtfAppName = "PublishedRTF"



New-BrokerApplication –ApplicationType PublishedContent

–CommandLineExecutable $rtfUNC -Name $rtfAppName

-DesktopGroup $dg.Uid
```

```
$docxUNC = "\\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedDOCX.docx"

$docxAppName = "PublishedDOCX"



New-BrokerApplication –ApplicationType PublishedContent

–CommandLineExecutable $docxUNC -Name $docxAppName

-DesktopGroup $dg.Uid
```

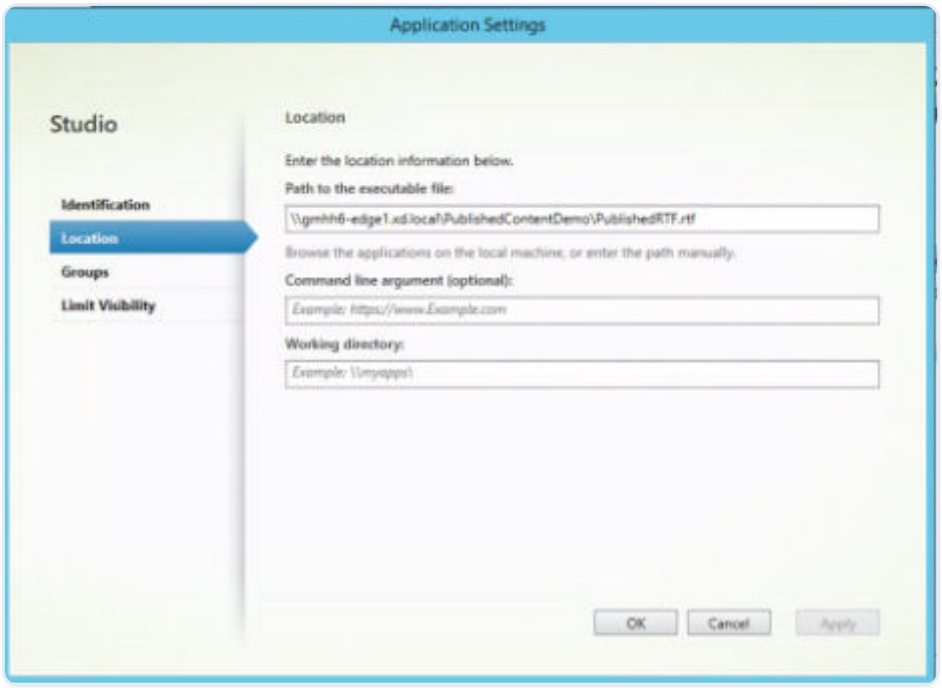
成功を確認する:

- StoreFrontウィンドウを更新して、新しく公開されたドキュメントを表示します。
- **PublishedRTF**および**PublishedDOCX**アプリケーションをクリックします。各ドキュメントは、ローカルで実行されているWordPadで開きます。

PublishedContentアプリケーションの表示と編集

公開されたコンテンツは、他のアプリケーションタイプと同じ方法で管理します。公開されたコンテンツ項目は、Studioの**アプリケーション**リストに表示され、Studioで編集できます。

アプリケーションプロパティ（ユーザーの可視性、グループ関連付け、ショートカットなど）は、公開されたコンテンツに適用されます。ただし、**場所**ページでコマンドライン引数または作業ディレクトリのプロパティを変更することはできません。リソースを変更するには、そのページの**実行可能ファイルへのパス**フィールドを変更します。

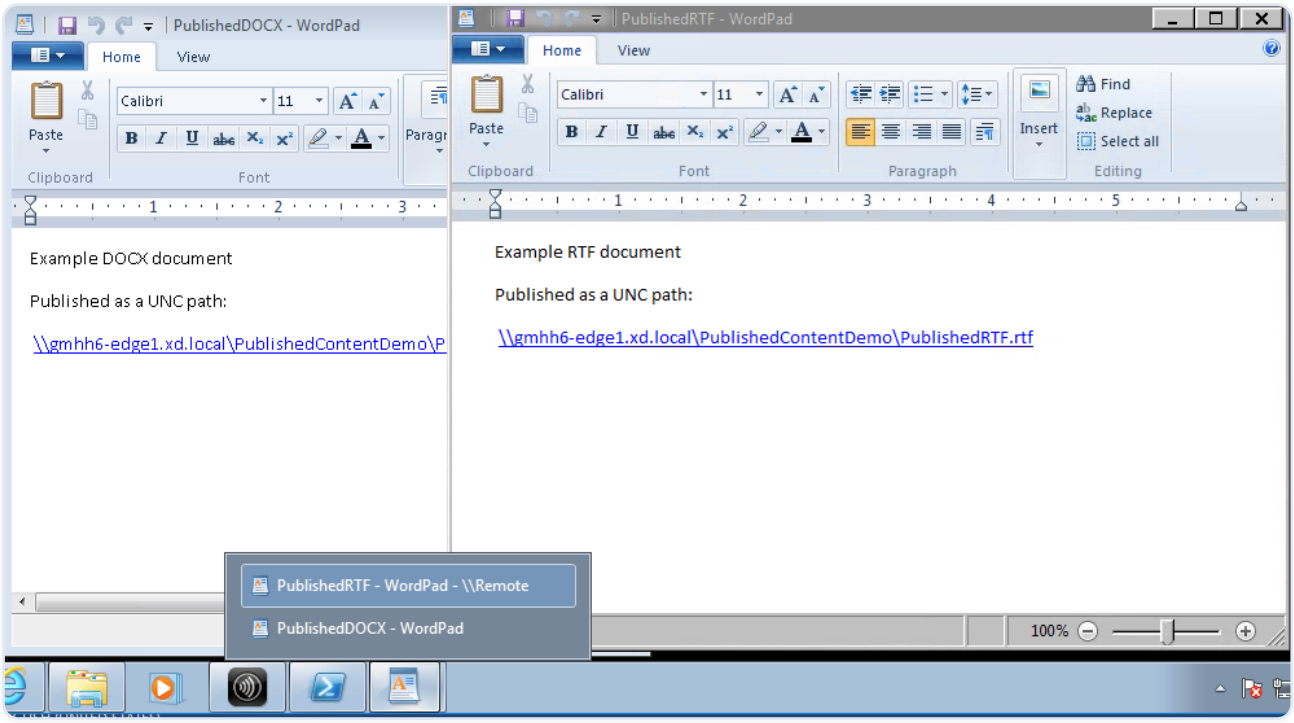


公開されたアプリケーションを使用して`PublishedContent`アプリケーション（ローカルアプリケーションではなく）を開くには、公開されたアプリケーションの**ファイルタイプ関連付け**プロパティを編集します。この例では、公開されたWordPadアプリケーションが編集され、.rtfファイルのファイルタイプ関連付けが作成されました。

ファイルタイプ関連付けを編集する前に、デリバリーグループのメンテナンスモードをオンにします。完了したら、メンテナンスモードをオフにすることを忘れないでください。

Studioのファイルタイプ関連付けアプリケーション設定(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/pub-content-props-fta.png)

StoreFrontを更新してファイルタイプ関連付けの変更を読み込み、**PublishedRTF**および**PublishedDOCX**アプリケーションをクリックします。違いに注目してください。**PublishedDOCX**は引き続きローカルのWordPadで開きます。しかし、**PublishedRTF**はファイルタイプ関連付けにより、公開されたWordPadで開くようになりました。



詳細情報

- マシンカタログの作成
- デリバリーグループの作成
- アプリケーションプロパティの変更

サーバー VDI

Server VDI (Virtual Desktop Infrastructure) 機能を使用して、単一ユーザー向けにサーバーオペレーティングシステムからデスクトップを配信します。

- エンタープライズ管理者は、サーバーオペレーティングシステムをVDIデスクトップとして配信できます。これは、エンジニアやデザイナーなどのユーザーにとって価値があります。
- サービスプロバイダーは、クラウドからデスクトップを提供できます。これらのデスクトップは、Microsoft Services Provider License Agreement (SPLA) に準拠しています。

サポート:

- Citrix Virtual Apps and Desktops™ および Citrix DaaS (旧称 Citrix Virtual Apps and Desktops service) の展開環境では、Server VDI は Windows Server 2022、Windows Server 2019、および Windows Server 2016 でサポートされています。
- すべてのServer VDI展開は、ユーザーパーソナライゼーションレイヤーテクノロジーをサポートしています。

- Server VDIがスキャナーなどのTWAINデバイスで動作するには、Windows Serverのデスクトップエクスペリエンス機能がインストールされている必要があります。
- 以下の機能はServer VDIでは使用できません:
  - ホスト型アプリケーション
  - ローカルアプリアクセス
  - 直接（ブローカーなし）デスクトップ接続
  - リモートPCアクセス

Server VDIのインストールと構成

1. Windowsサーバーをインストール用に準備します。
   - Windows Server Managerを使用して、リモートデスクトップサービスロールサービスがインストールされていないことを確認します。以前にインストールされていた場合は、削除してください。これらのロールサービスがインストールされていると、VDAのインストールは失敗します。
   - 「**各ユーザーを単一セッションに制限する**」プロパティが有効になっていることを確認します。Windowsサーバーで、ターミナルサーバー設定のレジストリを編集します。

     `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server`

     `DWORD fSingleSessionPerUser = 1`
2. Citrix Virtual Apps and Desktopsインストーラーのコマンドラインインターフェイスを使用して、サポートされているサーバーまたはサーバーマスターイメージにVDAをインストールし、`/servervdi`オプションを指定します。(デフォルトでは、インストーラーのグラフィカルインターフェイスは、サーバーオペレーティングシステム上のWindowsシングルセッションOS VDAをブロックします。コマンドラインを使用すると、この動作が上書きされます。)次のいずれかのコマンドを使用します。
   - Citrix Virtual Apps and Desktops展開の場合:
     - `XenDesktopVdaSetup.exe /servervdi`
     - `VDAWorkstationSetup.exe /servervdi`
   - Citrix DaaS™展開の場合:
     - `VDAWorkstationSetup.exe /servervdi`

   その他のオプション:

- Delivery ControllerまたはCloud Connectorを指定するには、`/controllers`を使用します。
- ファイアウォールを手動で構成する場合を除き、ファイアウォールでポートを開くには、`/enable_hdx_ports`を使用します。
- イメージにVDAをインストールし、そのイメージからMCSを使用してサーバーVMを作成する場合は、`/mastermcsimage` (または`/masterimage`) を使用します。
- すべてのオプションの詳細については、「コマンドラインを使用したインストール」を参照してください。

3. Server VDI用のマシンカタログを作成します。カタログ作成ウィザードで:
   - **オペレーティングシステム**ページで、**シングルセッションOS**を選択します。
   - **概要**ページで、Server VDIであることを明確に識別できるマシンカタログ名と管理者向けの記述を指定します。これは、カタログがServer VDIをサポートしていることをStudioで示す唯一のインジケーターです。

   Studioで検索を使用すると、VDAがマルチセッションマシンにインストールされている場合でも、Server VDIカタログは**シングルセッションOSマシン**タブに表示されます。
4. デリバリーグループを作成し、作成したServer VDIカタログを選択します。

VDAのインストール中にDelivery ControllerまたはCloud Connectorを指定しなかった場合は、後で指定することを忘れないでください。詳細については、「VDA登録」を参照してください。

ユーザーパーソナライゼーションレイヤー

Citrix Virtual Apps and Desktops™ のユーザーパーソナライゼーションレイヤー機能は、非永続マシンカタログの機能を拡張し、セッション間でユーザーのデータとローカルにインストールされたアプリケーションを保持します。基盤となるCitrix App Layeringテクノロジーを搭載したユーザーパーソナライゼーションレイヤー機能は、非永続マシンカタログにおけるCitrix ProvisioningおよびMachine Creation Services (MCS) をサポートします。

マスターイメージ内にVirtual Delivery Agentと併せてユーザーパーソナライゼーションレイヤーコンポーネントをインストールします。VHDファイルは、ユーザーがローカルにインストールしたアプリケーションを保存します。イメージにマウントされたVHDは、ユーザー自身の仮想ハードドライブとして機能します。

> **重要:**

> Citrix Virtual Apps and Desktopsでユーザーパーソナライゼーションレイヤーを展開するか、イメージテンプレートで有効になっているApp Layeringユーザーレイヤーを展開できますが、両方はできません。App Layering内のレイヤーにユーザーパーソナライゼーションレイヤー機能をインストールしないでください。

> この機能はPersonal vDisk (PvD) に代わるものであり、非永続的なプールされたデスクトップ環境でユーザーに永続的なワークスペースエクスペリエンスも提供します。

ユーザーパーソナライゼーションレイヤー機能を展開するには、記事に記載されている手順を使用してインストールおよび構成します。それまでは、この機能は利用できません。

アプリケーションのサポート

以下の例外を除き、ユーザーがデスクトップにローカルでインストールするすべてのアプリケーションは、ユーザーパーソナライゼーションレイヤーでサポートされます。

例外

以下のアプリケーションは例外であり、ユーザーパーソナライゼーションレイヤーではサポートされません。

- MS OfficeやVisual Studioなどのエンタープライズアプリケーション。
- ネットワークスタックまたはハードウェアを変更するアプリケーション。例：VPNクライアント。
- ブートレベルドライバーを持つアプリケーション。例：ウイルススキャナー。
- ドライバーストアを使用するドライバーを持つアプリケーション。例：プリンタードライバー。

> **注：**
>
> Windowsグループポリシーオブジェクト (GPO) を使用してプリンターを利用可能にできます。

サポートされていないアプリケーションをローカルにインストールすることをユーザーに許可しないでください。代わりに、これらのアプリケーションはマスターイメージに直接インストールしてください。

ローカルユーザーまたは管理者アカウントを必要とするアプリケーション

ユーザーがアプリケーションをローカルにインストールすると、そのアプリはユーザーレイヤーに格納されます。その後、ユーザーがローカルユーザーまたはグループを追加または編集しても、その変更はセッションを超えて保持されません。

> **重要:**
>
> 必要なローカルユーザーまたはグループは、マスターイメージに追加してください。

要件

ユーザーパーソナライゼーションレイヤー機能には、以下のコンポーネントが必要です。

- シトリックス バーチャル アプリケーションズ アンド デスクトップ 7 1909 以降
- Virtual Delivery Agent (VDA) バージョン1912
- Citrix Provisioning™、バージョン1909以降
- Windowsファイル共有 (SMB)、またはオンプレミスAD認証が有効なAzure Files

OSがシングルセッションとして展開されている場合、ユーザーパーソナライゼーションレイヤー機能を次のWindowsバージョンに展開できます。サポートは、シングルセッションの単一ユーザーに限定されます。

- Windows 10 Enterprise x64、バージョン1607以降
- Windows 10 マルチセッション (Azure Files対応)
- Windows Server 2016 (Azure Files サポート対象)
- Windows Server 2019 (Azure Files がサポートされています)

Citrix Virtual Apps and Desktops 7の場合、ユーザーパーソナライゼーションレイヤーでのAzure Filesの使用は、Windows Server 2019、Windows Server 2016v、およびWindows 10クライアントでサポートされています。

> **注：**
>
> ユーザーパーソナライゼーションレイヤーは、Server VDI展開としてのみサポートされます。展開の詳細については、Server VDI の記事を参照してください。

> ユーザーパーソナライゼーションレイヤーは、マシンごとに一度に1人のユーザーのみをサポートし、その後、ディスクをリセットするためにマシンを再起動する必要があります。マルチセッションサーバーオペレーティングシステムではユーザーパーソナライゼーションレイヤーを使用できません。シングルセッションサーバーシステムでのみ使用できます。ユーザーパーソナライゼーションレイヤーは、非永続デスクトップでのみ機能します。

> ユーザーパーソナライゼーションレイヤー機能がインストールされている場合は、アンインストールします。最新リリースをインストールする前に、マスターイメージを再起動します。

ファイル共有を設定する

ユーザーパーソナライゼーションレイヤー機能には、Windows Server Message Block (SMB) ストレージが必要です。Windowsファイル共有を作成するには、使用しているWindowsオペレーティングシステムの通常の手順に従ってください。

Azureベースのカタログでは Azure Filesを使用する方法の詳細については、「ユーザーパーソナライゼーションレイヤー用のAzure Filesストレージを設定する」を参照してください。

推奨事項

ユーザーパーソナライゼーションレイヤーの展開を成功させるには、このセクションの推奨事項に従ってください。

プロファイル管理ソリューション

ユーザーパーソナライゼーションレイヤーは、単一のマシンカタログイメージに対してユーザーが行うすべての変更を保存します。複数のカタログイメージ間でローミングプロファイルデータなどの拡張機能を追加するには、CitrixはProfile Managementも使用することを推奨します。詳細については、Profile Managementのドキュメント を参照してください。

ユーザーパーソナライゼーションレイヤー機能でProfile Managementを使用する場合、ログオフ時にユーザー情報を削除します。Group Policy Object (GPO) またはDelivery Controller™ (DDC) のポリシーを使用して削除をクリアできます。

利用可能なプロファイル管理ポリシーの詳細については、プロファイル管理ポリシーの説明とデフォルトを参照してください。

マイクロソフト システムセンター コンフィグレーションマネージャー (SCCM)

ユーザーパーソナライゼーションレイヤー機能でSCCMを使用している場合は、VDI環境でイメージを準備するためのMicrosoftのガイドラインに従ってください。詳細については、このMicrosoft TechNet記事を参照してください。

ユーザーレイヤーのサイズ

ユーザーレイヤーは、ディスク上のスペースが使用されるにつれて拡張するシンプロビジョニングディスクです。ユーザーレイヤーに許可されるデフォルトサイズは10 GBで、これは推奨される最小値です。

> **注：**
>
> インストール中に値がゼロ (0) に設定されている場合、デフォルトのユーザーレイヤーサイズは10 GBに設定されます。

> ユーザーレイヤーのサイズを変更したい場合は、**ユーザーレイヤーサイズ** Studioポリシーに別の値を入力できます。「**オプション: GB単位のユーザーレイヤーサイズの横にあるをクリックします。**」の下にある「**ステップ5: デリバリーグループのカスタムポリシーを作成する**」を参照してください。

ユーザーレイヤーのサイズを上書きするためのツール (オプション)

Windowsツールを使用してユーザーレイヤーファイル共有にクォータを定義することで、ユーザーレイヤーのサイズを上書きできます。

以下のMicrosoftクォータツールのいずれかを使用して、**Users**という名前のユーザーレイヤーディレクトリにハードクォータを設定します。

- ファイルサーバーリソースマネージャー (FSRM)
- クォータマネージャー

> **注：**
>
> クォータを増やすと、新しいユーザーレイヤーに影響し、既存のユーザーレイヤーが拡張されます。クォータを減らすと、新しいユーザーレイヤーのみに影響します。既存のユーザーレイヤーのサイズが小さくなることはありません。

ユーザーパーソナライゼーションレイヤーを展開する

ユーザーパーソナライゼーション機能を展開する際は、Studio内でポリシーを定義します。その後、その機能が展開されるマシンカタログにバインドされたデリバリーグループにポリシーを割り当てます。

マスターイメージにユーザーパーソナライゼーションレイヤーの設定がない場合、サービスはアイドル状態のままであり、オーサリングアクティビティを妨げません。

マスターイメージでポリシーを設定すると、サービスはマスターイメージ内でユーザーレイヤーを実行およびマウントしようとします。その結果、マスターイメージは予期しない動作や不安定性を示す可能性があります。

ユーザーパーソナライゼーションレイヤー機能を展開するには、以下の手順をこの順序で完了します。

- ステップ1: Citrix Virtual Apps and Desktops環境の可用性を確認します。
- ステップ2：マスターイメージを準備します。
- ステップ3：マシンカタログを作成します。
- ステップ4：デリバリーグループを作成します。
- ステップ5：デリバリーグループのカスタムポリシーを作成します。

ステップ 1: Citrix Virtual Apps and Desktops 環境が利用可能であることを確認する

この新機能を使用できるように、Citrix Virtual Apps and Desktops環境が利用可能であることを確認してください。セットアップの詳細については、「Citrix Virtual Apps and Desktopsのインストールと構成」を参照してください。

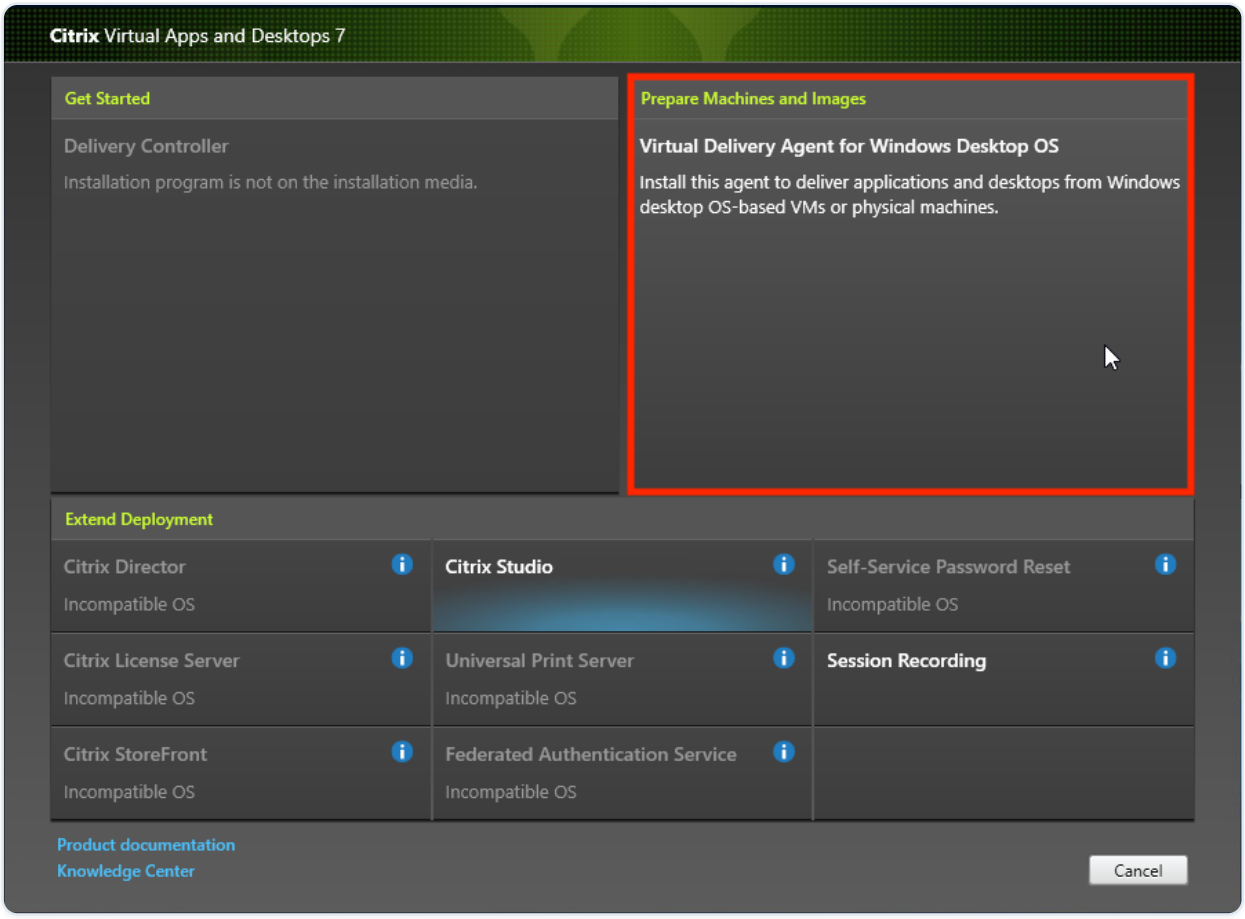
ステップ 2: マスターイメージを準備する

マスターイメージを準備するには:

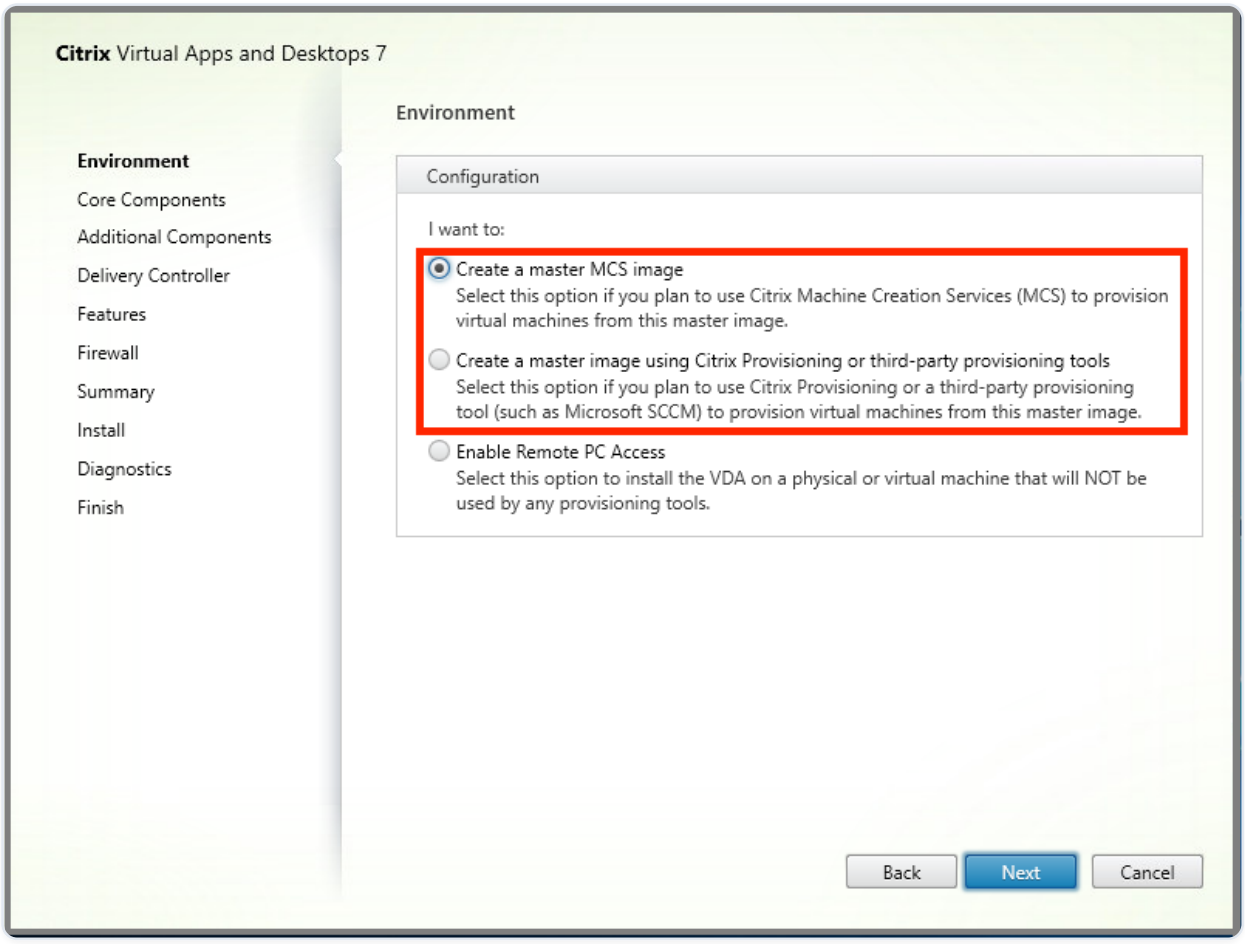
1. マスターイメージを見つけます。組織のエンタープライズアプリケーションや、ユーザーが一般的に役立つと考えるその他のアプリをインストールします。
2. Server VDI を展開する場合は、Server VDI の記事の手順に従ってください。オプションコンポーネントである**ユーザーパーソナライゼーションレイヤー**を必ず含めてください。詳細については、「VDA をインストールするためのコマンドラインオプション」を参照してください。
3. Windows 10を使用している場合は、Virtual Delivery Agent (VDA) 1912をインストールします。以前のバージョンのVDAがすでにインストールされている場合は、まず古いバージョンをアンインストールしてください。新しいバージョンをインストールする際は、オプションコン

ポーネントである**Citrix User Personalization Layer**を必ず選択してインストールしてください。手順は次のとおりです。

a. タイル「**Virtual Delivery Agent for Windows Desktop OS**」をクリックします。

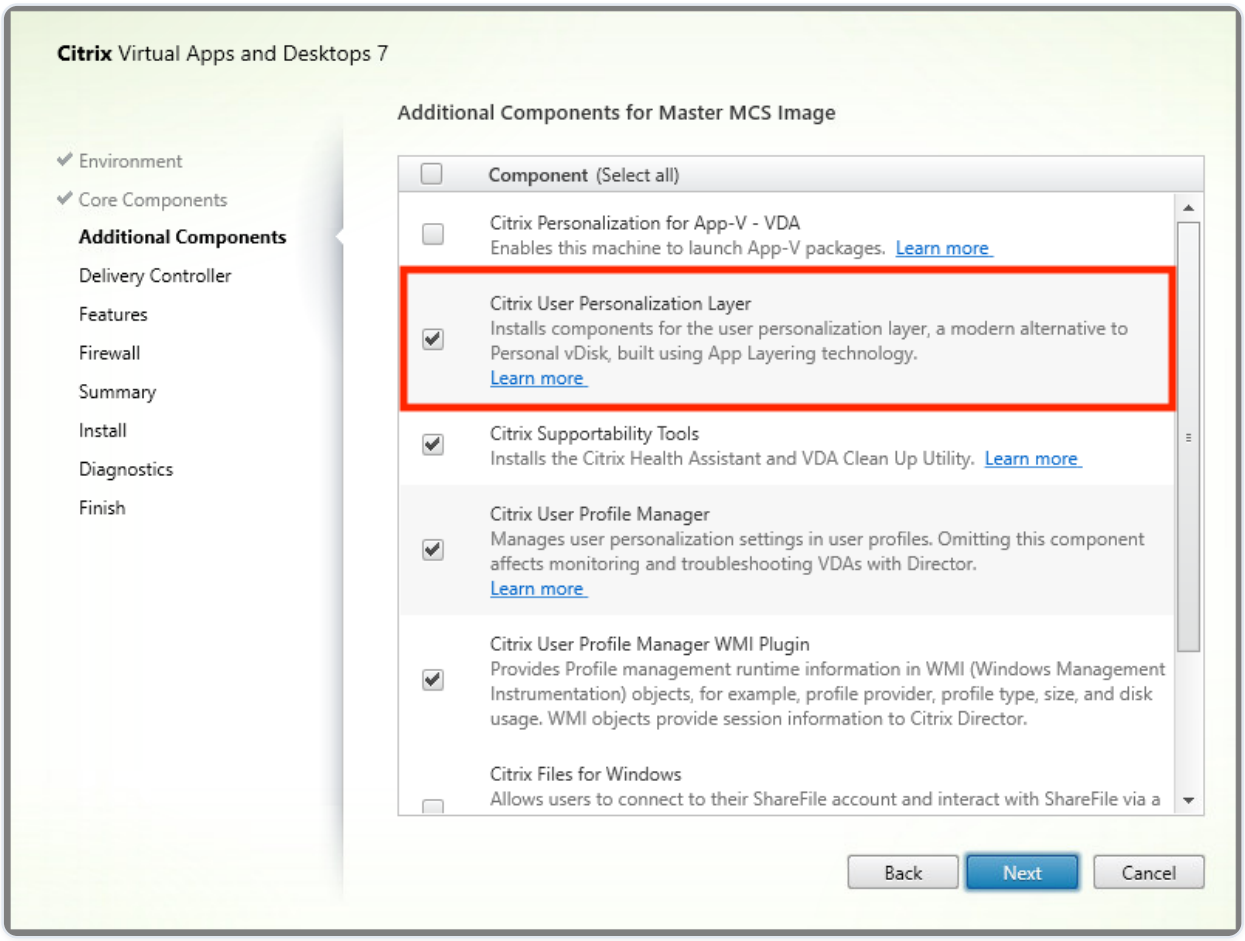


a. **環境:** 「マスターMCSイメージを作成する」または「Citrix Provisioningまたはサードパーティのプロビジョニングツールを使用してマスターイメージを作成する」のいずれかを選択します。



a. **コアコンポーネント:** 「次へ」をクリックします。

b. **追加コンポーネント:** 「**Citrix User Personalization Layer**」をチェックします。



a. 残りのインストール画面を進み、必要に応じてVDAを構成し、をクリックします。インストール中にイメージが1回以上再起動します。

4. **Windows Update**は無効のままにしてください。ユーザーパーソナライゼーションレイヤーインストーラーは、イメージ上のWindows Updateを無効にします。更新は無効のままにしてください。

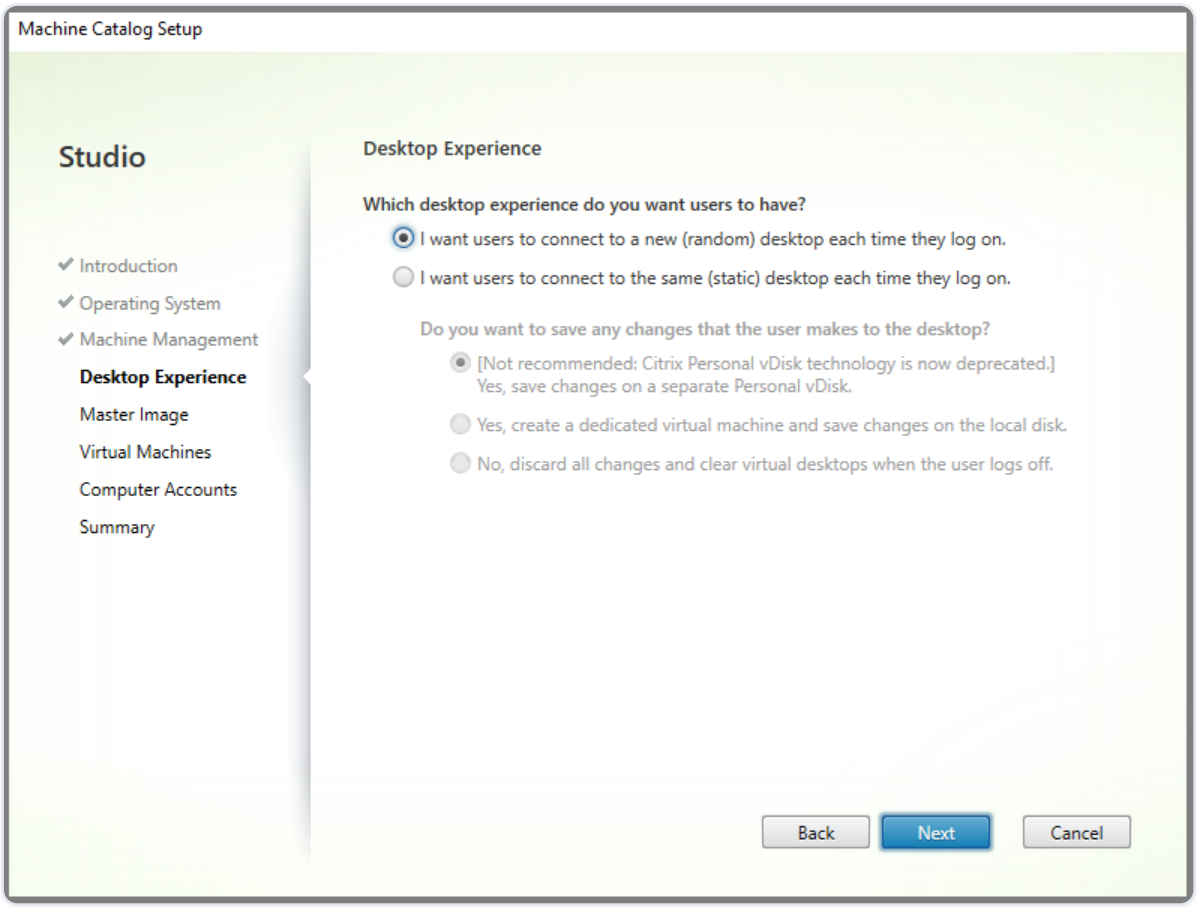
イメージをStudioにアップロードする準備ができました。

ステップ3：マシンカタログを作成する

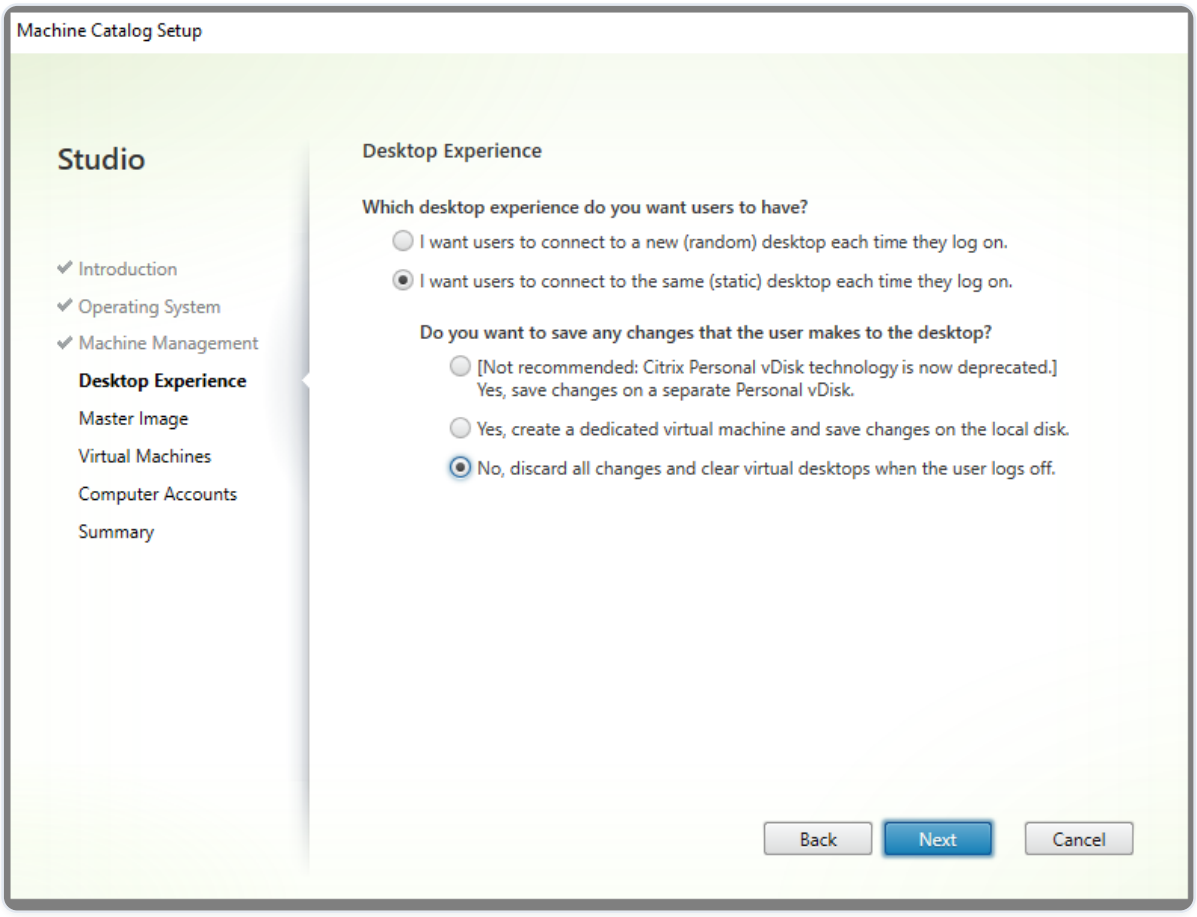
Studioで、マシンカタログを作成する手順に従います。カタログ作成時に以下のオプションを使用します。

1. **オペレーティングシステム**を選択し、**シングルセッションOS**に設定します。
2. **マシン管理**を選択し、**電源管理されているマシン**に設定します。たとえば、仮想マシンやブレードPCなどです。
3. **デスクトップエクスペリエンス**を選択し、以下の例のように、**プールされたランダム**または**プールされた静的**カタログタイプに設定します。

   - **プールされたランダム:**



- **プールされた静的:** プールされた静的を選択した場合、次のスクリーンショットに示すように、ユーザーがログオフするときにすべての変更を破棄し、仮想デスクトップをクリアするようにデスクトップを構成します。



> **注：**
>
> ユーザーパーソナライゼーションレイヤーは、Citrix Personal vDiskを使用するように構成されている、または専用仮想マシンとして割り当てられているプールされた静的カタログをサポートしていません。

4. MCSを使用している場合は、**マスターイメージ**と、前のセクションで作成したイメージのスナップショットを選択します。
5. 環境の必要に応じて、残りのカタログプロパティを構成します。

ステップ 4: デリバリーグループを作成する

作成したマシンカタログのマシンを含め、**デリバリーグループ**を作成して構成します。詳細については、「デリバリーグループの作成」を参照してください。

ステップ 5: デリバリーグループのカスタムポリシーを作成する

Virtual Delivery Agents 内でユーザーレイヤーのマウントを有効にするには、構成パラメーターを使用して以下を指定します。

- ネットワーク上のどこでユーザーレイヤーにアクセスするか。
- ユーザーレイヤーディスクの最大許容サイズ。

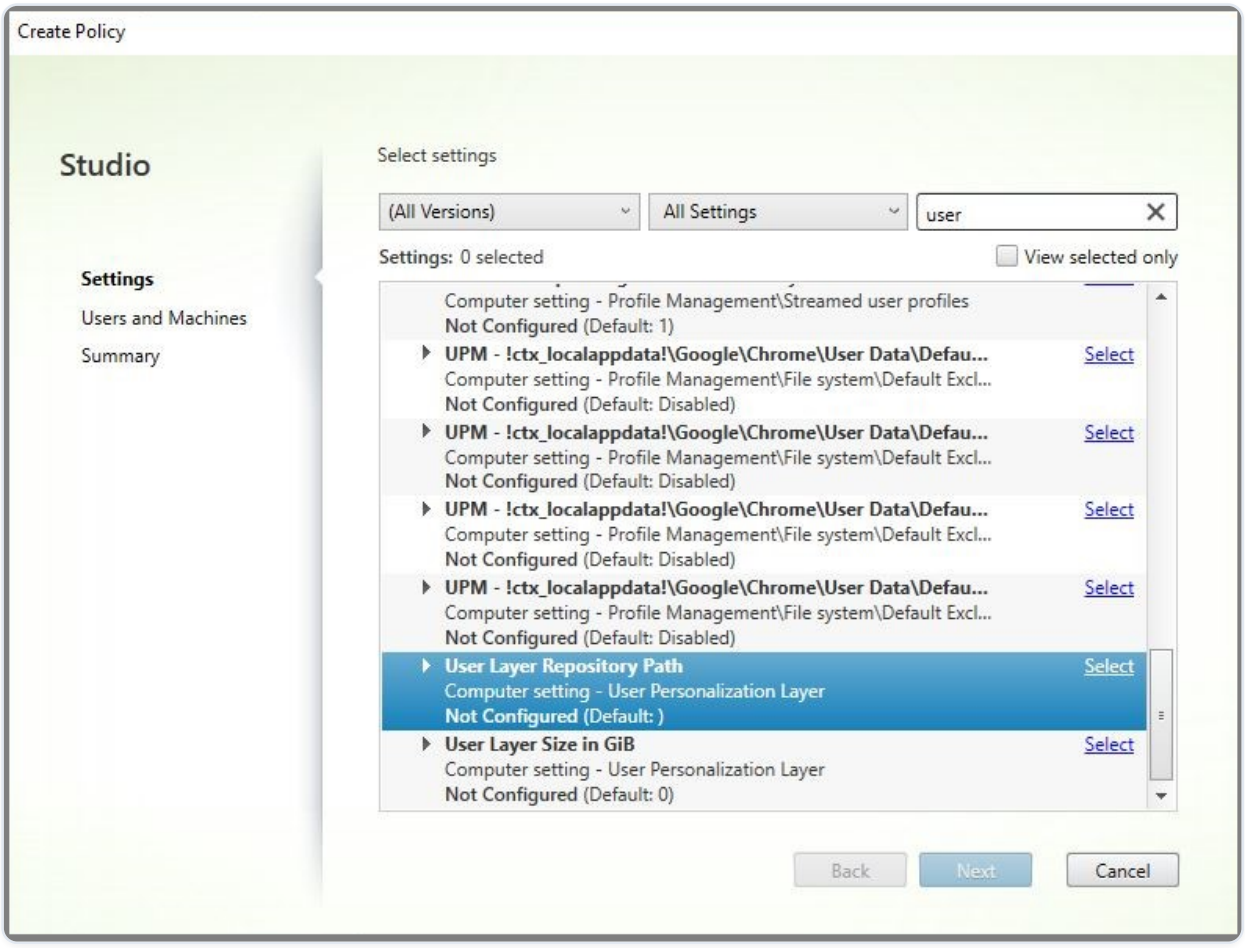
Studio でパラメーターをカスタム Citrix ポリシーとして定義し、それらをデリバリーグループに割り当てます。

1. Studio で、ナビゲーションペインの を選択します。

   Studio でポリシーを選択(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/upl-studio-select-policies.png)
2. ペインで を選択します。 ウィンドウが表示されます。
3. 検索フィールドに「user layer」と入力します。利用可能なポリシーのリストに次の2つのポリシーが表示されます。

   - ユーザーレイヤーリポジトリパス
   - ユーザーレイヤーサイズ (GB)

   > **注：**
   >
   > サイズを増やすと、新しいユーザーレイヤーに影響し、既存のユーザーレイヤーが拡張されます。サイズを減らすと、新しいユーザーレイヤーにのみ影響します。既存のユーザーレイヤーのサイズが小さくなることはありません。
4. の横にある をクリックします。 ウィンドウが表示されます。



5. フィールドにパスを入力し、 をクリックします。

   - **パス形式:** `\\server-name-or-address\share-name\folder`
   - **パスの例:** `\\Server\Share\UPLUsers`
   - **結果のパスの例: CoolCompanyDomain** の **Alex** という名前のユーザーの場合、パスは次のようになります。`\\Server\Share\UPLUsers\Users\CoolCompanyDomain_Alex\A_OK`

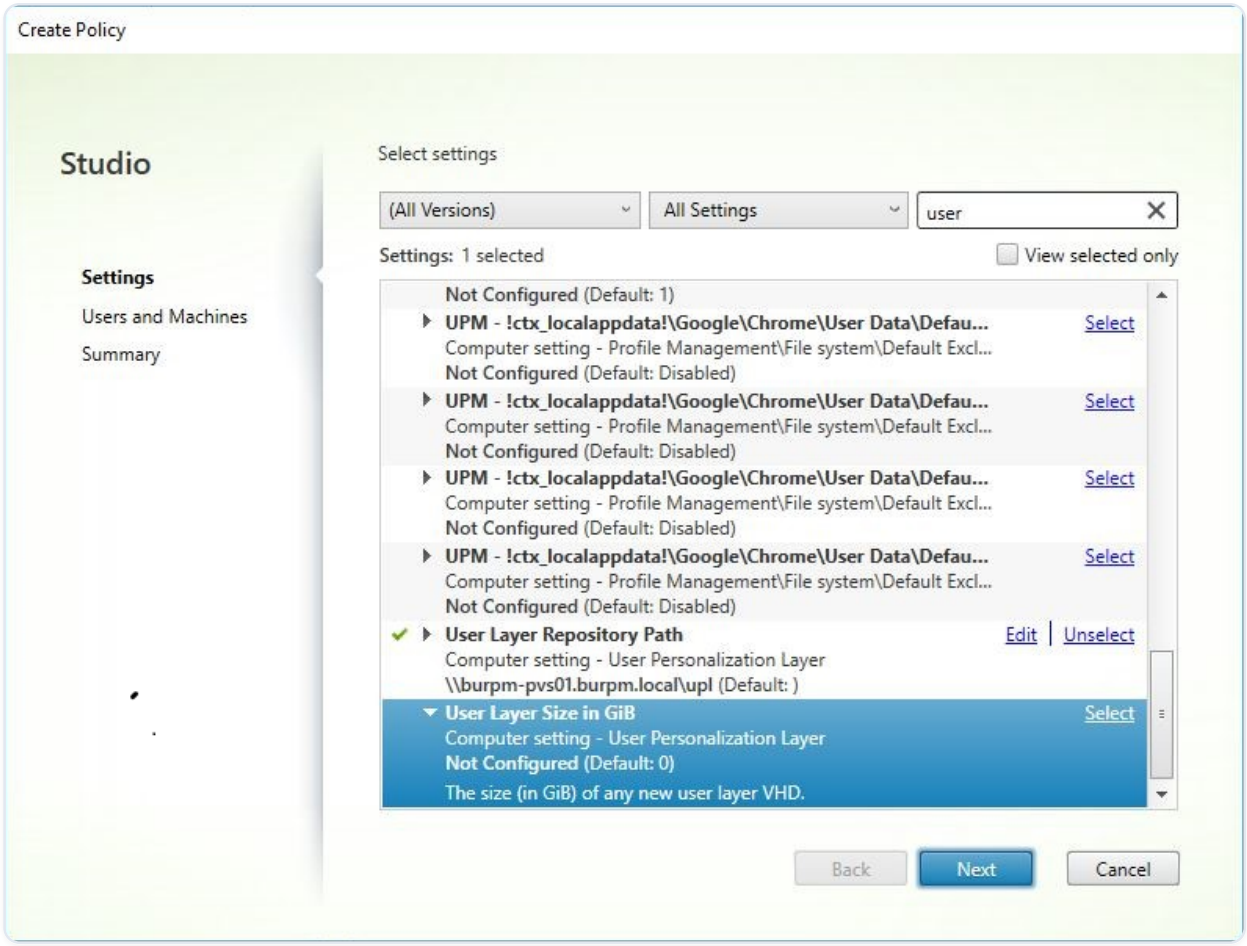
   リポジトリパス(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/upl-user-layer-repo-enter-path-no-variables.png)

   変数 `%USERNAME%`、`%USERDOMAIN%`、およびマシン環境変数を使用してパスをカスタマイズできます。これらの変数を展開すると、明示的なパスになります。

   - **パス形式:** `\\Server-name-or-address\share-name\folder-with-environment-variables`
   - **パスの例:** `\\Server\Share\UPLUserLayers\%USERNAME%\%USERDOMAIN%`
   - **結果のパスの例: CoolCompanyDomain** の **Alex** という名前のユーザーの場合、パスは次のようになります。`\\Server\Share\UPLUserLayers\Alex\CoolCompanyDomain\A_OK`

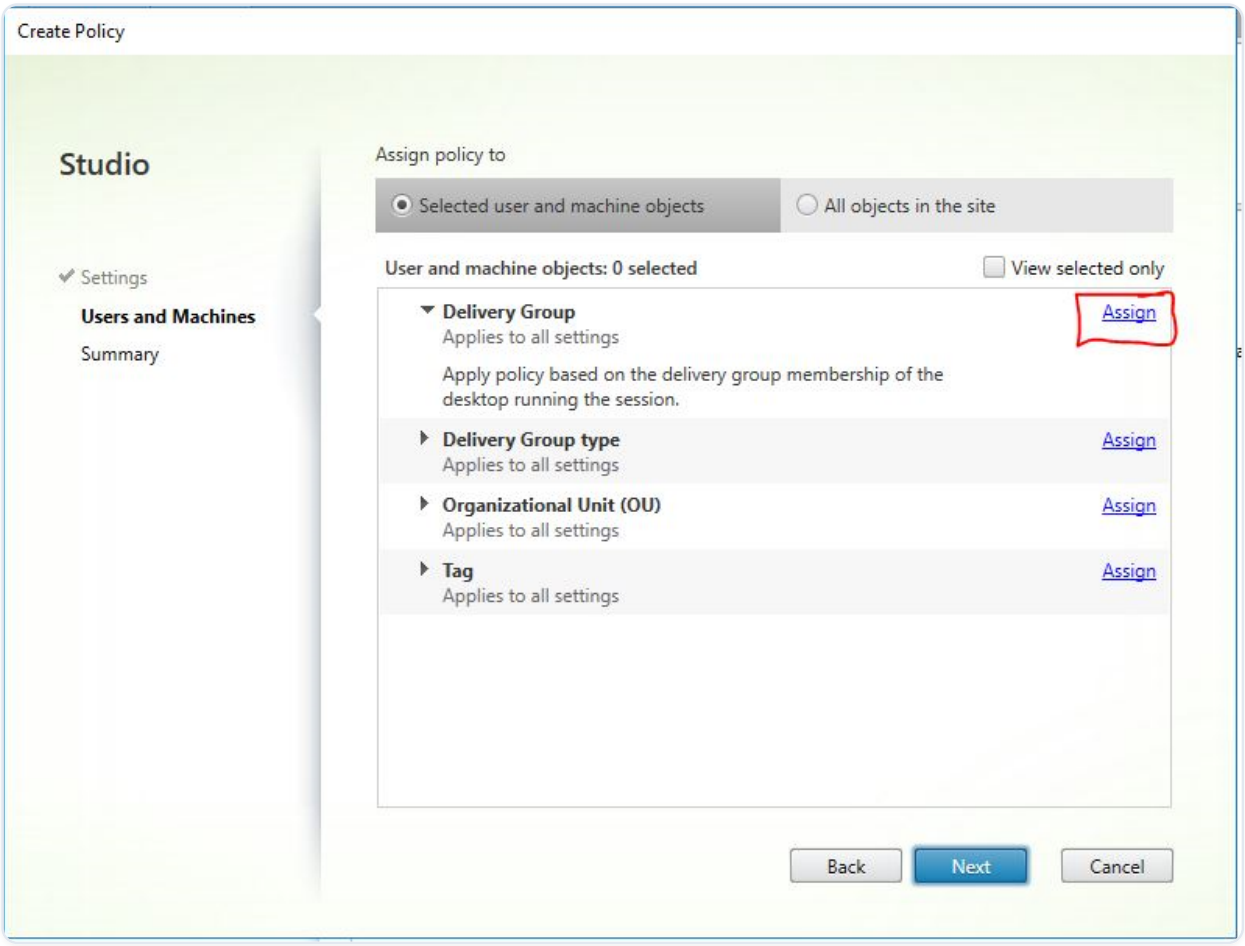
環境変数を含むリポジトリパス(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/upl-user-layer-repo-enter-path-variables.png)

6. オプション：「User Layer Size in GB」の横にある「**選択**」をクリックします。

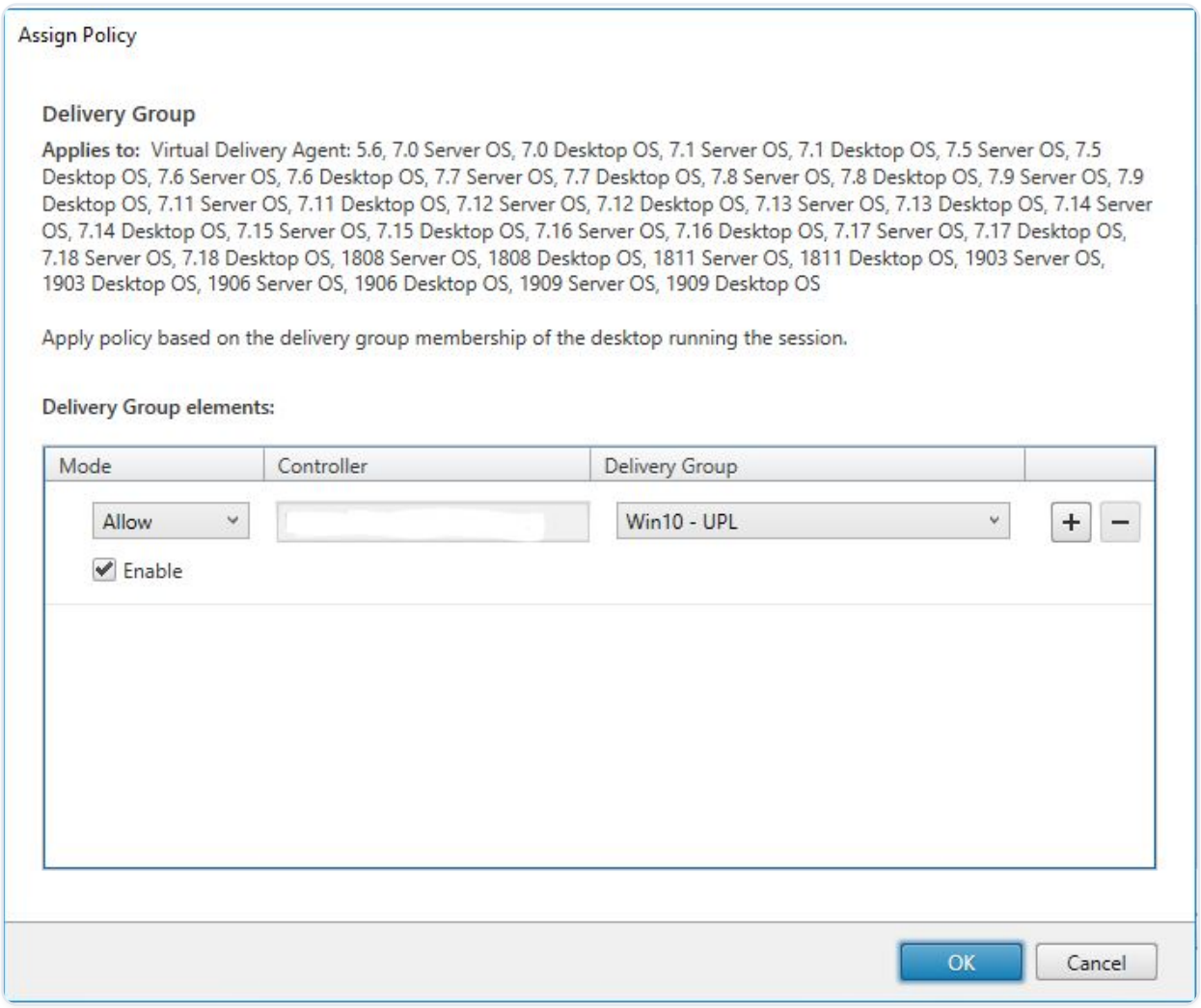


設定の編集ウィンドウが表示されます。

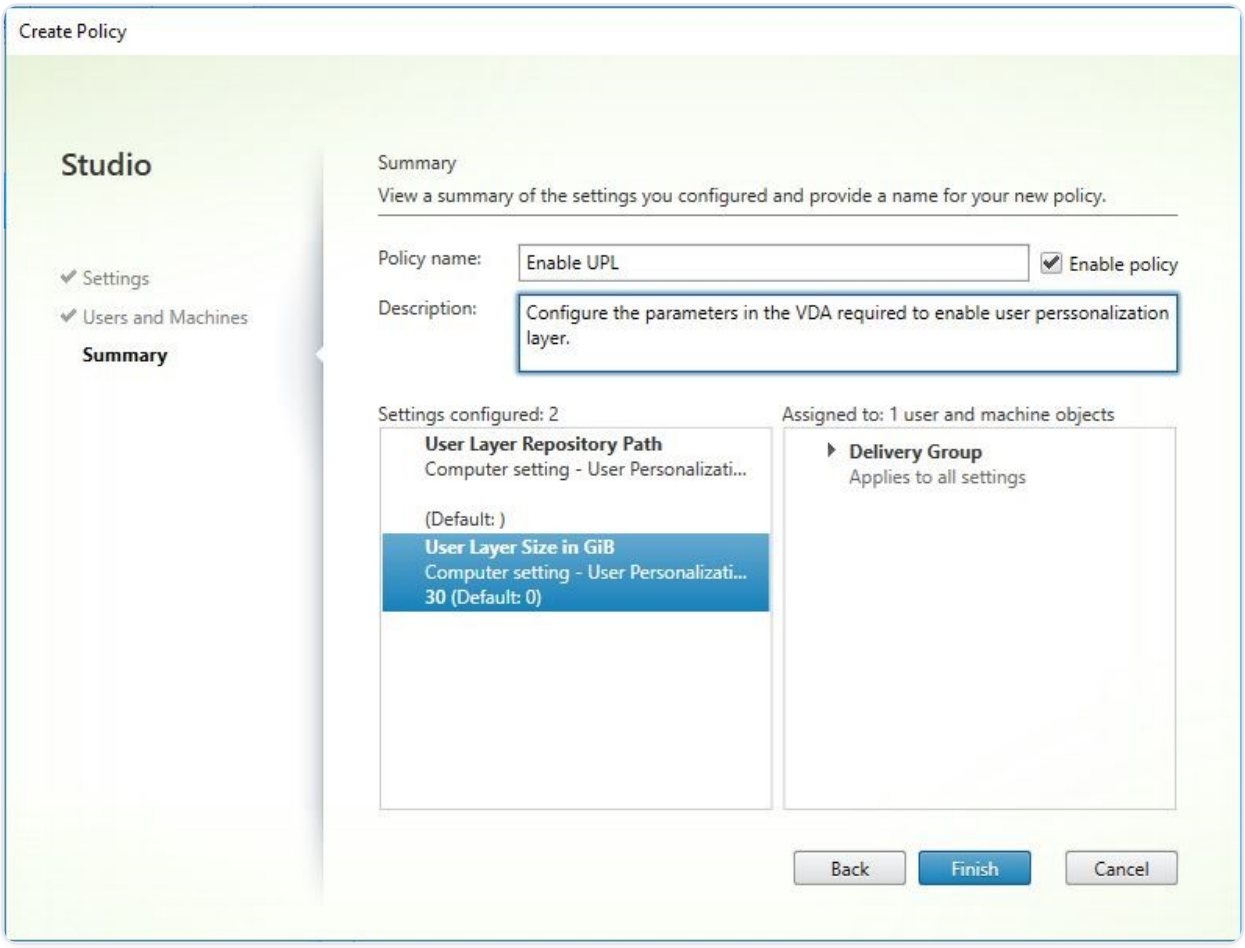
7. オプション: デフォルト値の **10 GB** を、各ユーザーレイヤーが拡張できる最大サイズに変更します。 をクリックします。
8. をクリックして、ユーザーとマシンを構成します。この画像で強調表示されている リンクをクリックします。



9. デリバリーグループメニューで、前のセクションで作成したデリバリーグループを選択します。「OK」をクリックします。



10. ポリシーの名前を入力します。ポリシーを有効にするには、チェックボックスをオンにして、**Finish** をクリックします。



ユーザーレイヤーフォルダーのセキュリティ設定を構成する

ドメイン管理者として、ユーザーレイヤーのストレージ場所を複数指定できます。ストレージ場所ごとに（デフォルトの場所を含め）、`\Users` サブフォルダーを作成します。次の設定を使用して、各場所を保護します。

設定名	値	適用先	
作成者/所有者	変更	サブフォルダーとファイルのみ	
所有者の権限	変更	サブフォルダーとファイルのみ	
ユーザーまたはグループ	フォルダーの作成/データの追加、フォルダーの横断/ファイルの実行、フォルダーの一覧表示/データの読み取り、属性の読み取り	選択したフォルダーのみ	

設定名	値	適用先	
システム	フルコントロール	選択されたフォルダー、サブフォルダー、およびファイル	
ドメイン管理者、および選択された管理者グループ	フルコントロール	選択されたフォルダー、サブフォルダー、およびファイル	

ユーザーレイヤーメッセージ

ユーザーがユーザーレイヤーにアクセスできない場合、次のいずれかの通知メッセージが表示されます。

- **ユーザーレイヤーが使用中です**

  `We were unable to attach your user layer because it is in use. Any changes you make to application settings or data will not be saved. Be sure to save any work to a shared network location.`.

- **ユーザーレイヤーが利用できません**

  `We were unable to attach your user layer. Any changes you make to application settings or data will not be saved. Be sure to save any work to a shared network location.`.

- **ユーザーサインアウト後にシステムがリセットされませんでした**

  `This system was not shut down properly. Please log off immediately and contact your system administrator.`.

トラブルシューティング時に使用するログファイル

ログファイル ulayersvc.log には、変更がログに記録されるユーザーパーソナライゼーションレイヤーソフトウェアの出力が含まれています。

```
C:\ProgramData\Unidesk\Logs\ulayersvc.log
```

制限事項

ユーザーパーソナライゼーションレイヤー機能をインストールして使用する際は、以下の制限事項に注意してください。

- App Layering 内のレイヤーにユーザーパーソナライゼーションレイヤーソフトウェアを展開しようと *しないでください*。ユーザーパーソナライゼーションレイヤーは Citrix Virtual Apps and Desktops に展開するか、App Layering イメージテンプレートでユーザーレイヤーを有効にするかのいずれかにしてください。両方を行うことはできません。どちらのプロセスでも、必要なユーザーレイヤーが生成されます。
- 永続的なマシンカタログでユーザーパーソナライゼーションレイヤー機能を構成*しないでください*。
- 「セッションホスト」は使用*しないでください*。
- 新しい OS インストールを実行しているイメージ (Windows 10 の同じバージョンであっても) でマシンカタログを更新 *しないでください*。ベストプラクティスは、マシンカタログの作成時に使用したのと同じマスターイメージ内で OS の更新を適用することです。
- ブート時ドライバーやその他の早期ブートパーソナライゼーションを *使用しないでください*。
- PvDデータをユーザーパーソナライゼーションレイヤー機能に移行*しないでください*。
- 既存のユーザーレイヤーを完全なApp Layering製品からユーザーパーソナライゼーションレイヤー機能に移行*しないでください*。
- 異なるマスターOSイメージを使用して作成されたユーザーレイヤーにアクセスするために、ユーザーレイヤーのSMBパスを変更*しないでください*。
- ユーザーがセッションからログアウトして再度ログインすると、新しいセッションはプール内の別のマシンで実行されます。VDI 環境では、Microsoft Software Center は最初のマシンではアプリケーションを と表示しますが、2番目のマシンでは と表示します。

  アプリケーションの実際のステータスを確認するには、ユーザーにSoftware Centerでアプリケーションを選択し、**インストール**をクリックするよう指示します。すると、SCCMがステータスを実際の値に更新します。
- ユーザーパーソナライゼーションレイヤー機能が有効になっているVDA内で、Software Centerが起動直後に停止することがあります。この問題を回避するには、XenDesktop VDI環境でのSCCMの実装に関するMicrosoftの推奨事項に従ってください。また、Software Centerを起動する前に、`ccmexec`サービスが実行されていることを確認してください。

- グループポリシー (コンピューター設定) では、ユーザーレイヤー設定がマスターイメージに適用された設定を上書きします。したがって、GPO を使用してコンピューター設定で行った変更は、次回のセッションログイン時にユーザーに常に適用されるとは限りません。

  この問題を回避するには、次のコマンドを発行するユーザーログオンスクリプトを作成します。

  ```
  gpupdate /force
  ```

  たとえば、あるお客様は、ユーザーがログインするたびに次のコマンドを実行するように設定しました。

  ```
  gpudate /Target:Computer /force
  ```

  最良の結果を得るには、ユーザーがログインした後で、コンピューター設定への変更をユーザーレイヤーに直接適用します。
- ドメインユーザーアカウントがマスターイメージに最後にログインしたユーザーであってはなりません。そうしないと、そのイメージからプロビジョニングされたマシンで問題が発生します。

コンポーネントの削除

コンポーネントを削除するには、プログラムの削除または変更を行うWindows機能を使用することをお勧めします。または、コマンドラインまたはインストールメディア上のスクリプトを使用してコンポーネントを削除することもできます。

コンポーネントを削除しても、前提条件は削除されず、ファイアウォール設定も変更されません。たとえば、Delivery Controller™を削除しても、SQL Serverソフトウェアとデータベースは削除されません。

Web Interfaceを含む以前の展開からControllerをアップグレードした場合は、Web Interfaceコンポーネントを個別に削除する必要があります。インストーラーを使用してWeb Interfaceを削除することはできません。

以下に記載されていない機能の削除については、その機能のドキュメントを参照してください。

準備

Controllerを削除する前に、サイトから削除してください。詳しくは、「Controllerを削除する」を参照してください。

StudioとDirectorを削除する前に、それらを閉じます。

Windowsのプログラムの削除または変更機能を使用してコンポーネントを削除する

Windowsのプログラムの削除または変更機能から：

- Controller、Studio、Director、License Server、またはStoreFrontを削除するには、**Citrix Virtual Apps *version*** または **Citrix Virtual Apps and Desktops™ *version*** を右クリックして、**アンインストール**を選択します。インストーラーが起動します。削除するコンポーネントを選択します。

  または、**Citrix StoreFront**を右クリックして**アンインストール**を選択することで、StoreFront™を削除できます。
- VDAを削除するには、**Citrix Virtual Delivery Agent *version*** を右クリックして、**アンインストール**を選択します。インストーラーが起動し、削除するコンポーネントを選択できます。デフォルトでは、削除後にマシンは自動的に再起動します。
- Universal Print Serverを削除するには、**Citrix Universal™ Print Server**を右クリックして、**アンインストール**を選択します。

コマンドラインを使用してコアコンポーネントを削除する

`\x64\XenDesktop Setup`ディレクトリから、`XenDesktopServerSetup.exe`コマンドを実行します。

- 1つ以上のコンポーネントを削除するには、`/remove`および`/components`オプションを指定します。
- すべてのコンポーネントを削除するには、`/removeall`オプションを指定します。

コマンドとパラメーターの詳細については、「コマンドラインを使用したインストール」を参照してください。

例えば、次のコマンドはStudioを削除します。

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components studio
```

コマンドラインを使用してVDAを削除する

`\x64\XenDesktop Setup`ディレクトリから、`XenDesktopVdaSetup.exe`コマンドを実行します。

- 1つ以上のコンポーネントを削除するには、`/remove`オプションと`/components`オプションを使用します。例えば、VDAとCitrix Workspaceアプリを削除するには、`/remove /components vda,plugin`を使用します。

- `/removeall`オプションはVDAのみを削除します。Citrix Workspaceアプリは削除しません。

コマンドとパラメーターの詳細については、コマンドラインを使用したインストールを参照してください。

デフォルトでは、削除後にマシンは自動的に再起動します。

Active Directoryでスクリプトを使用してVDAを削除するには、スクリプトを使用したVDAのインストールまたは削除を参照してください。

アップグレードと移行

注:

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

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

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

注:

- **「バージョン交差」の警告**

  異なるLTSRバージョンは、そのメンテナンスサイクルが重複することがよくありますのでご注意ください。アップグレードを開始する前に、現在の累積更新プログラム (CU) とターゲットLTSR (またはその後のCU) の両方の**リリース日**を確認する必要があります。

> 現在の環境のリリース日がターゲットLTSRまたはLTSR CUのリリース日よりも**新しい**場合、Citrixは新しいLTSRの次のCUを待つことを強く推奨します。そうしない場合、古いコードが既存のセキュリティ更新プログラム、安定性パッチ、および機能強化を上書きする可能性があります。
>
> - **「サポート対象外の状態」条項**
>
>   リリース日が古いバージョンにアップグレードしようとすると、技術的には**コアコンポーネントのダウングレード**と見なされます。この特定の構成は、**「部分的な成功」**ステータスになる可能性があります。

はじめに

アップグレードすると、新しいマシンやサイトをセットアップすることなく、展開がCitrix Virtual Apps and Desktops 7 Current Release (CR) に変更されます。このアップグレードはインプレースアップグレードとして知られています。

アップグレードにより、対象となる最新の機能とテクノロジーにアクセスできるようになります。アップグレードには、以前のバージョンからの修正、明確化、および機能強化も含まれる場合があります。

アップグレードの概要

1. アップグレードを開始する前に、(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/upgrade-migrate/upgrade.html) の記事を確認してください。この記事は、アップグレードの準備方法と実装方法を学ぶための主要な情報源です。
2. 準備ガイダンスを完了します。
3. インストーラーを実行してコアコンポーネントをアップグレードします。
4. システムデータベースとサイトをアップグレードします。
5. イメージ上のVDA（またはマシンに直接）をアップグレードします。
6. その他のコンポーネントをアップグレードします。

各準備およびアップグレードの手順については、展開のアップグレードで詳しく説明しています。

アップグレード可能なバージョン

Citrix Virtual Apps and Desktops™ 2203 LTSRには、以下からアップグレードできます。

- XenApp and XenDesktop 7.15 LTSR CU5から最新のCUまで

- Virtual Apps and Desktops 1912（CUの有無にかかわらず、最新のCUまでを含む）
- Citrix Virtual Apps and Desktopsの現在サポートされているCRバージョン

Citrix Virtual Apps and DesktopsのCurrent Releaseバージョンのサポートについては、展開のアップグレードで確認できます。

よくある質問

このセクションでは、Citrix Virtual Apps and Desktopsのアップグレードに関するよくある質問に回答します。

- **Virtual Apps and Desktops環境をアップグレードする正しい順序は何ですか？**

  推奨されるアップグレードシーケンスの図と説明については、アップグレードシーケンスおよびアップグレード手順を参照してください。

- **私のサイトには複数のDelivery Controller（異なるゾーンにあります）があります。一部のみをアップグレードした場合、どうなりますか？同じメンテナンス期間中にサイト内のすべてのControllerをアップグレードする必要がありますか？**

  各Controller上のさまざまなサービスが相互に通信するため、すべてのDelivery Controllerを同じメンテナンス期間中にアップグレードすることがベストプラクティスです。異なるバージョンを維持すると問題が発生する可能性があります。メンテナンス期間中には、Controllerの半分をアップグレードし、サイトをアップグレードしてから、残りのControllerをアップグレードすることをお勧めします。(詳細については、アップグレード手順を参照してください。)

- **最新バージョンに直接アップグレードできますか、それとも段階的なアップグレードを行う必要がありますか？**

  アップグレードするバージョンの**新機能**の記事で明示的に記載されていない限り、ほとんどの場合、最新バージョンにアップグレードし、中間リリースをスキップできます。アップグレードガイドを参照してください。

- **お客様はLong Term Service Release (LTSR) 環境からCurrent Releaseにアップグレードできますか？**

  はい。お客様は長期間にわたってLong Term Service Releaseにとどまる必要はありません。お客様は、ビジネス要件と機能に基づいて、LTSR環境をCurrent Releaseに移行できます。

- **コンポーネントの混在バージョンは許可されていますか？**

  各サイト内で、Citrixはすべてのコンポーネントを同じバージョンにアップグレードすることを推奨しています。一部のコンポーネントで以前のバージョンを使用することはできますが、最

新バージョンのすべての機能が利用できない場合があります。詳細については、混在環境に関する考慮事項を参照してください。

- **Current Releaseはどのくらいの頻度でアップグレードする必要がありますか？**

  Current Releaseはリリース日から6か月後にメンテナンス終了 (EOM) に達します。Citrixは、お客様が最新のCurrent Releaseを採用することを推奨しています。Current Releaseはリリース日から18か月後にサポート終了 (EOL) に達します。詳細については、Current Releaseのライフサイクルを参照してください。

- **推奨されるのは、LTSRへのアップグレードですか、それともCRへのアップグレードですか？**

  Current Release (CR) は、最新かつ最も革新的なアプリ、デスクトップ、およびサーバー仮想化の機能を提供します。これにより、最先端のテクノロジーを維持し、競合他社の一歩先を行くことができます。

  Long Term Service Release (LTSR) は、長期間にわたって同じベースバージョンを維持することを好む大規模なエンタープライズ本番環境に最適です。

  詳細については、サービスオプションを参照してください。

- **ライセンスをアップグレードする必要がありますか？**

  現在のライセンスの有効期限が切れておらず、アップグレード先のリリースで有効であることを確認してください。CTX111618を参照してください。更新については、Customer Success Services renewal licensesを参照してください。

- **アップグレードにはどのくらい時間がかかりますか？**

  展開のアップグレードにかかる時間は、インフラストラクチャとネットワークによって異なります。そのため、正確な時間をお伝えすることはできません。

- **ベストプラクティスは何ですか？**

  準備ガイダンスを理解し、それに従ってください。

- **サポートされているオペレーティングシステムは何ですか？**

  アップグレード先のバージョンのシステム要件の記事に、サポートされているOSが記載されています。

  現在の展開でサポートされなくなったオペレーティングシステムを使用している場合は、以前のオペレーティングシステムを参照してください。

- **サポートされているVMware vSphere (vCenter + ESXi) のバージョンは何ですか？**

CTX131239には、サポートされているホストとバージョン、および既知の問題へのリンクが記載されています。

- **私のバージョンはいつEOLになりますか？**

  製品マトリックスを確認してください。

- **最新リリースにおける既知の問題は何ですか？**

  - シトリックス仮想アプリおよびデスクトップ
  - StoreFront
  - シトリックス プロビジョニング
  - シトリックス ライセンス サーバー
  - Windows向けCitrix Workspaceアプリ

詳細情報

Long Term Service Release (LTSR)の展開の更新には、累積更新プログラム（CU）が使用されます。CUはLTSRのベースラインコンポーネントを更新し、各CUには独自のメタインストーラーが含まれています。

各CUには専用のドキュメントがあります。たとえば、7.15 LTSRの場合、そのLTSRの**「新機能」**ページで最新のCUへのリンクを確認してください。各CUページには、サポートされているバージョン情報、手順、およびCUダウンロードパッケージへのリンクが含まれています。

移行

クラウドへの移行

Citrix Virtual Apps and Desktopsの自動構成ツールを使用して、オンプレミス展開をクラウドに移行できます。詳しくは、「クラウドへの移行」を参照してください。

レガシー移行

移行とは、以前の展開から新しいバージョンにデータを移動することです。このプロセスには、新しいコンポーネントのインストールと新しいサイトの作成、古いファームからのデータのエクスポート、そして新しいサイトへのデータのインポートが含まれます。

XenAppおよびXenDesktop®のバージョン、または以前のCitrix Virtual Apps and Desktopsのバージョンを移行するためのサポートされているツールやスクリプトはありません。

以前のXenApp 6.xの移行コンテンツについては、以下を参照してください。スクリプトはサポートも保守もされていません。

- XenApp 6.xバージョンのオープンソース移行スクリプトは`<https://github.com/citrix/xa65migrationtool>`で入手できます。Citrixはこれらの移行スクリプトをサポートまたは保守していません。
- **7.xでの変更点、XenApp 6.5ワーカーを新しいVDAにアップグレードする**、および**XenApp 6.xを移行する**については、`<https://docs.citrix.com/ja-jp/legacy-archive/citrix-virtual-apps-and-desktops.html>`のCitrix Virtual Apps and Desktopsレガシーアーカイブを参照してください。

デプロイをアップグレードする

注：

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

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

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

はじめに

新しいマシンやサイトを最初にセットアップすることなく、特定の展開を新しいバージョンにアップグレードできます。これはインプレースアップグレードと呼ばれます。

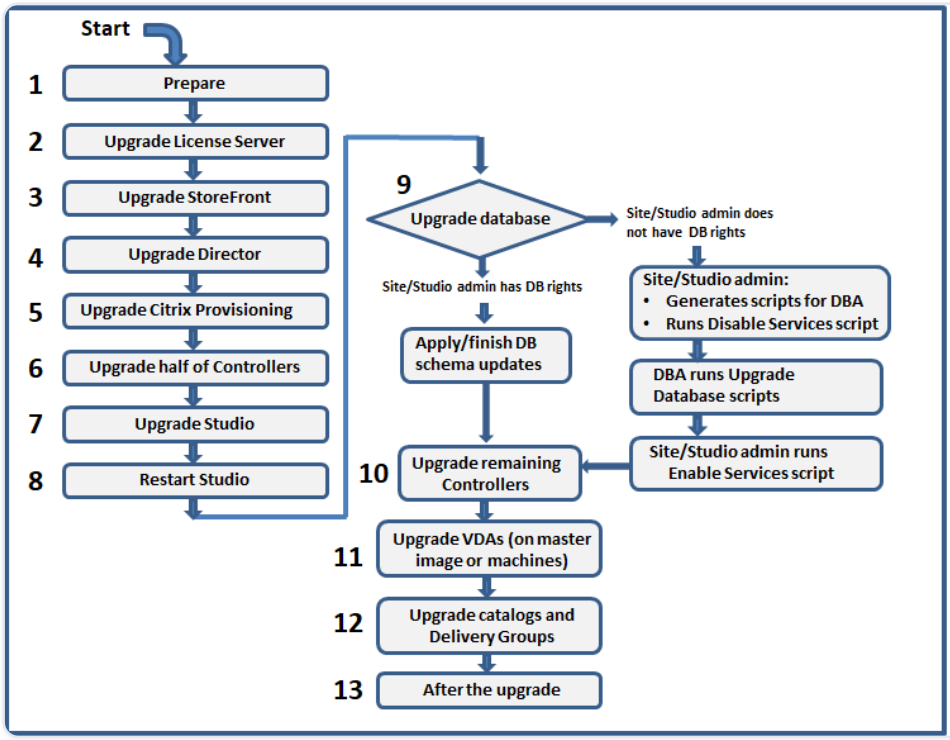
アップグレードを開始するには、新しいバージョンのインストーラーを実行して、以前にインストールされたコアコンポーネント、VDA、および特定のその他のコンポーネントをアップグレードします。次に、データベースとサイトをアップグレードします。

新しいバージョンが提供されている場合、フルプロダクトインストーラー（およびスタンドアロンVDAインストーラー）でインストールできる任意のコンポーネントをアップグレードできます。フルプロダクトインストーラーでインストールされないその他のコンポーネント（Citrix Provisioning™やProfile Managementなど）については、そのコンポーネントのドキュメントを参照してください。ホストのアップグレードについては、適切なドキュメントを参照してください。

アップグレードを開始する前に、この記事のすべての情報を確認してください。

アップグレードシーケンス

次の図は、アップグレードシーケンスのステップを示しています。Upgrade procedure には、図の各ステップの詳細が含まれています。



> **注：**

障害を回避するため、新しいマシンカタログの作成、マシンカタログの削除、デリバリーグループ内のマシンの更新など、プロビジョニングおよびデリバリーグループ関連のタスクを実行する前に、すべてのDelivery Controllerとデータベースをアップグレードする必要があります。

ハイブリッド権限ライセンス

ハイブリッド権限ライセンスは、顧客が永続ライセンスからクラウドサービスサブスクリプションに移行またはアップグレードする際に、クラウドサービスサブスクリプションに加えて提供される期間ベースのサブスクリプションライセンスです。DaaSサブスクリプションでハイブリッド権限アドオンを購入することもできます。

SaaS属性を持つハイブリッド権限ライセンスをお持ちの場合、Citrix Virtual Apps and Desktops™ LTSR 2203以降にアップグレードすると、Citrix Virtual Apps and Desktops LTSR 1912では利用できなかった機能にアクセスできるようになります。これらの機能には、Microsoft Azure、AWS EC2、Google Cloudなどのパブリッククラウドでのワークロードのプロビジョニングとホスティングが含まれます。新しいライセンスファイルを展開する前に、ライセンスサーバーを最新バージョンに更新してください。この前提条件を満たさない場合、サイトのアップグレードおよび作成中にエラーや推奨事項が発生する可能性があります。

Citrix Virtual Apps and Desktops LTSR 1912からLTSR 2203にアップグレードし、Azure、AWS、またはGoogle Cloud接続を含む新しいハイブリッド権限ライセンスの資格がある場合は、次の手順に従ってください。そうしないと、2203メタインストーラーによってアップグレードがブロックされます。

注：

- 新しいライセンスコードが記載されたメールが届きます。詳しくは、「ライセンスアクセスコードの使用」を参照してください。
- 既存のライセンスは取り消されます。取り消されたライセンスはライセンスサーバーから削除し、その後新しいライセンスをインストールする必要があります。詳しくは、「ライセンスファイルの削除」を参照してください。

1. citrix.comのライセンス管理ポータルにアクセスし、クラウドプロビジョニング権限が有効になっている（SaaS属性を持つ）新しいハイブリッド権限ライセンスファイルをダウンロード

します。詳しくは、「ライセンスのダウンロード」を参照してください。次の図は、増分セクションにSaaS属性を持つハイブリッド権限ライセンスファイルを示しています。

```
INCREMENT XDT_PLT_CCS CITRIX 2022.1201 01-dec-2022 5 \
    VENDOR_STRING=;LT=RetailS;GP=720;PSL=10;CL=VDS,VDA,VDE,VDP,SaaS-SA=0;ODP=0;NUDURMIN=2880;NUDURMAX=525600;AP=ADMIN/INT/14
    OVERDRAFT=1 DUP_GROUP=V ISSUED=18-dec-2005 NOTICE="Citrix \
    Systems Inc." SN=RetailSSaaS SIGN="..."
```

2. ライセンスサーバーにハイブリッド権限ライセンスファイルをインストールします。詳しくは、「ライセンスのインストール」を参照してください。
3. ライセンスのエディションまたはモデルに変更がある場合は、ブローカーコマンドを実行してエディションとモデルを設定し、インプレースアップグレードを開始してください。ブローカーコマンドの詳細については、「Broker PowerShell SDK」セクションを参照してください。

Citrix Virtual Apps and DesktopsのCurrent ReleasesおよびLong Term Service Releasesでのパブリッククラウドサポートの詳細については、CTX270373を参照してください。

アップグレード手順

主要な製品コンポーネントのほとんどは、コンポーネントを含むマシンで製品インストーラーを実行することでアップグレードできます。

1台のマシンに複数のコンポーネント（Studioやライセンスサーバーなど）が含まれている場合、製品メディアにそれらのソフトウェアの新しいバージョンが含まれていれば、そのマシン上のすべてのコンポーネントがアップグレードされます。

インストーラーを使用するには：

- フル製品インストーラーのグラフィカルインターフェイスを実行するには、マシンにログオンし、メディアを挿入するか、新しいリリースのISOドライブをマウントします。**AutoSelect** をダブルクリックします。
- コマンドラインインターフェイスを使用するには、適切なコマンドを発行します。「コマンドラインを使用したインストール」を参照してください。

ステップ1：準備

アップグレードを開始する前に、準備が整っていることを確認してください。必要なタスクを読み、完了してください。

- PVD、AppDisks™、およびサポートされていないホストの削除
- PvDまたはAppDiskコンポーネントを持つVDA

- 制限事項
- 混在環境に関する考慮事項
- 以前のオペレーティングシステム
- 準備
- サイトの事前テスト
- SQL Serverのバージョンチェック

ステップ2：ライセンスサーバーのアップグレード

インストールに新しいバージョンのCitrix License Serverソフトウェアが含まれている場合は、他のコンポーネントよりも先にこのコンポーネントをアップグレードしてください。

まだライセンスサーバーが新しいバージョンと互換性があるかどうかを判断していない場合は、他のコアコンポーネントをアップグレードする前に、ライセンスサーバーでインストーラーを実行することが不可欠です。

ステップ3：StoreFront™のアップグレード

インストールメディアに新しいバージョンのStoreFrontソフトウェアが含まれている場合は、StoreFrontサーバーを含むマシンでインストーラーを実行します。

- グラフィカルインターフェイスで、 セクションから を選択します。
- コマンドラインから、Citrix Virtual Apps and Desktopsインストールメディアの`x64`フォルダーにある`CitrixStoreFront-x64.exe`を実行します。

ステップ4：Directorのアップグレード

インストールメディアに新しいバージョンのDirectorソフトウェアが含まれている場合は、Directorを含むマシンでインストーラーを実行します。

ステップ5：Citrix Provisioningのアップグレード

Citrix Provisioningのインストールメディアは、Citrix Virtual Apps and Desktopsのインストールメディアとは別に提供されています。Citrix Provisioningサーバーおよびターゲットデバイスソフトウェアのインストールとアップグレードの方法については、Citrix Provisioning製品ドキュメントを参照してください。

ステップ6：Delivery Controllerの半分をアップグレードする

たとえば、サイトに4つのControllerがある場合、そのうちの2つでインストーラーを実行します。

Controllerの半分をアクティブなままにしておくことで、ユーザーはサイトにアクセスできます。VDAは残りのControllerに登録できます。Controllerの数が少ないため、サイトの容量が低下する場合があります。アップグレードによって、最終的なデータベースアップグレード手順中に新しいクライアント接続の確立が一時的に中断されるだけです。アップグレードされたControllerは、サイト全体がアップグレードされるまで要求を処理できません。

サイトにControllerが1つしかない場合、アップグレード中は動作しません。

実際のアップグレードが開始される前に、最初のControllerでサイトの事前テストが実行されます。詳細については、「サイトの事前テスト」を参照してください。

ステップ7：Studioのアップグレード

Studioをまだアップグレードしていない場合（別のコンポーネントと同じマシンにあったため）、Studioを含むマシンでインストーラーを実行します。

ステップ8：Studioの再起動

アップグレードされたStudioを再起動します。アップグレードプロセスは自動的に再開されます。

ステップ9：データベースとサイトのアップグレード

> **注：**
>
> 障害を避けるため、新しいマシンカタログの作成、マシンカタログの削除、デリバリーグループ内のマシンの更新など、プロビジョニングおよびデリバリーグループ関連のタスクを実行する前に、すべてのDelivery Controllerとデータベースをアップグレードする必要があります。

> SQL Serverデータベースのスキーマを更新するために必要な権限については、準備を確認してください。

- SQL Serverデータベーススキーマを更新する十分な権限がある場合は、自動データベースアップグレードを開始できます。データベースとサイトを自動的にアップグレードするに進みます。
- データベースの十分な権限がない場合は、スクリプトを使用する手動アップグレードを開始し、データベース管理者（必要な権限を持つ人）の助けを借りて進めることができます。手動アップグレードの場合、Studioユーザーはスクリプトを生成し、サービスを有効/無効にするスクリプトを実行します。データベース管理者は、SQLCMDユーティリティまたはSQLCMD

モードのSQL Server Management Studioを使用して、データベーススキーマを更新する他のスクリプトを実行します。データベースとサイトを手動でアップグレードするに進みます。

- マルチゾーン展開があり、データベースとサイトを自動的にアップグレードしたい場合は、サイトのSQL Serverデータベースをホストするのと同じゾーンでdbschemaアップグレードを実行することをCitrixは推奨します。そうしないと、データベースとサイトの自動アップグレードが失敗する可能性があります。

Citrixは、アップグレード前にデータベースをバックアップすることを強く推奨します。CTX135207を参照してください。データベースのアップグレード中は、製品サービスが無効になります。その間、Controllerはサイトの新しい接続を仲介できないため、慎重に計画してください。

データベースとサイトを自動的にアップグレードする

1. 新しくアップグレードされたStudioを起動します。
2. サイトのアップグレードを自動的に開始することを示し、準備ができたことを確認します。

データベースとサイトのアップグレードが進行します。

データベースとサイトを手動でアップグレードする

1. 新しくアップグレードされたStudioを起動します。
2. サイトを手動でアップグレードすることを示します。ウィザードはライセンスサーバーの互換性を確認し、確認を求めます。
3. データベースをバックアップしたことを確認します。

   ウィザードは、スクリプトとアップグレード手順のチェックリストを生成して表示します。アップグレード対象の製品バージョン以降、データベースのスキーマが変更されていない場合、そのスクリプトは生成されません。たとえば、ログデータベースのスキーマが変更されない場合、`UpgradeLoggingDatabase.sql` スクリプトは生成されません。
4. 以下のスクリプトを記載されている順序で実行します。

   - `DisableServices.ps1`: Studioユーザーは、製品サービスを無効にするために、ControllerでこのPowerShellスクリプトを実行します。
   - `UpgradeSiteDatabase.sql`: データベース管理者は、サイトデータベースを含むサーバーでこのSQLスクリプトを実行します。
   - `UpgradeMonitorDatabase.sql`: データベース管理者は、監視データベースを含むサーバーでこのSQLスクリプトを実行します。

- `UpgradeLoggingDatabase.sql`: データベース管理者は、構成ログデータベースを含むサーバーでこのSQLスクリプトを実行します。このスクリプトは、このデータベースが変更された場合（たとえば、ホットフィックスを適用した後など）にのみ実行してください。
- `EnableServices.ps1`: Studioユーザーは、製品サービスを有効にするために、Controllerでこのpowershellスクリプトを実行します。

データベースのアップグレードが完了し、製品サービスが有効になると、Studioは環境と構成を自動的にテストし、HTMLレポートを生成します。問題が特定された場合は、データベースのバックアップを復元できます。問題を解決した後、データベースを再度アップグレードできます。

5. チェックリストのタスクを完了したら、**Finish upgrade** をクリックします。

手順10: 残りのDelivery Controllerをアップグレードする

新しくアップグレードされたStudioから、ナビゲーションペインで **Citrix Studio** *サイト名* を選択します。**Common Tasks** タブで、**Upgrade remaining Delivery Controllers** を選択します。

アップグレードを完了し、完了を確認したら、Studioを閉じてから再度開きます。Studioは、Controllerのサービスをサイトに登録するため、またはゾーンIDが存在しない場合にゾーンIDを作成するために、追加のサイトアップグレードを促すことがあります。

手順11: VDAをアップグレードする

> **重要:**

> VDAをバージョン1912以降にアップグレードする場合は、「VDAを1912以降にアップグレードする」を参照してください。

> VDAを含むマシンで製品インストーラーを実行します。

Machine Creation Services™とマスターイメージを使用してマシンを作成した場合、ホストに移動し、マスターイメージ上のVDAをアップグレードします。利用可能なVDAインストーラーのいずれかを使用できます。

- グラフィックインターフェイスのガイダンスについては、VDAのインストールを参照してください。

- コマンドラインのガイダンスについては、コマンドラインを使用したインストールを参照してください。

Citrix Provisioningを使用してマシンを作成した場合は、アップグレードに関するガイダンスについてCitrix Provisioning製品ドキュメントを参照してください。

ステップ12：マシンカタログとデリバリーグループを更新する

- アップグレードされたVDAを持つマシンを使用するカタログを更新する。
- アップグレードされたVDAを持つマシンを使用するカタログをアップグレードする。
- アップグレードされたVDAを持つマシンを使用するデリバリーグループをアップグレードする。

ステップ13：アップグレード後

アップグレードが完了したら、新しくアップグレードされたサイトをテストできます。Studioで、ナビゲーションペインの**Citrix Studio site-name**を選択します。**Common Tasks**タブで、**Test Site**を選択します。これらのテストはデータベースのアップグレード後に自動的に実行されますが、いつでも再度実行できます。

サイトデータベースにローカルのMicrosoft SQL Server Expressが使用されている場合、SQL Server Browserサービスが開始されていないと、Windows Server 2016上のControllerでテストが失敗する可能性があります。これを回避するには：

- SQL Server Browserサービスを有効にし（必要に応じて）、開始します。
- SQL Server (SQLEXPRESS) サービスを再起動します。

展開内の他のコンポーネントをアップグレードします。ガイダンスについては、以下の製品ドキュメントを参照してください。

- StoreFront
- AppDNA
- Citrix App Layering (Citrixアプリケーションレイヤリング)
- HDX RealTime Optimization Pack (HDX RealTime最適化パック)
- プロファイル管理
- Citrix プロビジョニング
- セッションレコーディング
- ワークスペース環境管理

Microsoft SQL Server Express LocalDBソフトウェアを新しいバージョンに置き換える必要がある場合は、「SQL Server Express LocalDBの置き換え」を参照してください。

Dbschemaのアップグレード

展開を更新すると、複数のデータベーススキーマをアップグレードできます。次の表に、そのプロセスでアップグレードされるデータベーススキーマを示します。

From/To	1912 CU1	1912 CU2	1912 CU3	1912 CU4	1912 CU5	2203 RTM	2203 CU1	2203 CU2	2203 CU3
7.15 RTM/CU	Site; Monitor; config	Site; Monitor; config	Site; Monitor; config	Site; Monitor; config	Site; Monitor; config	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging
1912 RTM	Config	Site; Config	Site; Config	Site; Monitor; config	Site; Monitor; config	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging
1912 CU1		Site	Site; Config	Site; Monitor; config	Site; Monitor; config	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging
1912 CU2			Site; Config	Site; Monitor; config	Site; Monitor; config	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging
1912 CU3				Site; Monitor; config	Site; Monitor; config	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging
1912 CU4					Site; Config	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging
1912 CU5						Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging
1912 CU6						Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging
1912 CU7						Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging	Site; Monitor; config;logging
2203 RTM							Config	Config	Config
2203 CU1								Config	Config
2203 CU2									Config

用語の定義:

- サイト: サイトデータストア。Dbschemaの更新はサイトデータストアに対して行われます。
- モニター: モニターデータストア。Dbschemaの更新はモニターデータストアに対して行われます。
- 構成: 構成テーブル。構成テーブルでは、Desktop Studioのバージョン、ライセンス情報、またはその両方が更新されます。
- ロギング: ロギングデータストア。Dbschemaの更新はロギングデータストアに対して行われます。

VDAを2203以降にアップグレードする

Personal vDisk (PvD) コンポーネントがVDAにインストールされていた場合、そのVDAはバージョン2203以降にアップグレードできません。新しいVDAを使用するには、現在のVDAをアンインストールしてから、新しいVDAをインストールする必要があります。

この指示は、PvDを一度も使用したことがない場合でも適用されます。

以前のバージョンでPvDコンポーネントがインストールされた可能性のある方法は次のとおりです。

- VDAインストーラーのグラフィカルインターフェイスでは、PvDは**追加コンポーネント**ページでオプションとして提供されていました。7.15 LTSRおよびそれ以前の7.xリリースでは、このオプションがデフォルトで有効になっていました。したがって、デフォルトを受け入れた場合（または、いずれかのリリースでこのオプションを明示的に有効にした場合）、PvDがインストールされました。

- コマンドラインでは、`/baseimage` オプションによってPvDがインストールされました。このオプションを指定した場合、またはこのオプションを含むスクリプトを使用した場合は、PvDがインストールされました。

VDAにPvDがインストールされているかどうかわからない場合は、マシンまたはイメージで新しいVDA（2203以降）のインストーラーを実行してください。

- PvDがインストールされている場合、互換性のないコンポーネントがあることを示すメッセージが表示されます。
  - グラフィカルインターフェイスから、メッセージが表示されているページで**キャンセル**をクリックし、インストーラーを閉じたいことを確認します。
  - CLIからは、コマンドは表示されたメッセージとともに失敗します。
- PvDがインストールされていない場合、アップグレードが続行されます。

対処法

VDAにPvDがインストールされていない場合は、通常のアップグレード手順に従ってください。

VDAにPvDがインストールされている場合：

1. 現在のVDAをアンインストールします。
2. 新しいVDAをインストールします。

Windows 10 (1607以前、更新なし) マシンでPvDを継続して使用する場合は、VDA 7.15 LTSRが最新のサポート対象バージョンです。

> **注：**

> *XenAppおよびXenDesktop 7.15 LTSRでWindows 7デスクトップとPersonal vDiskを使用できますか？*

> Citrixは、2016年1月に発表されたXenAppおよびXenDesktop 7.6 LTSRからPersonal vDisk (PvD) を除外しました。さらに、CitrixはPvDテクノロジーの非推奨を発表し、今後Citrix App Layeringの使用を開始するよう顧客に推奨しています。Citrix App Layering (バージョン4.4以降) は、XenAppおよびXenDesktop 7.15 LTSRの互換コンポーネントです。しかし、Windows 7上の既存のPvD展開を持つ顧客がCitrix App Layeringテクノロジーに移行するのを支援するため、CitrixはJan 14, 2020まで、XenAppおよびXenDesktop 7.15 LTSR累積更新プログラム (CU) を通じてWindows 7デスクトップ用のPvD展開に対する期間限定のサポート

> を提供することを決定しました。PvDコンポーネントはLTSR CUから削除され、Jan 14, 2020以降はサポートされません。さらに、Jan 14, 2020以降にWindows 7でPvDを使用すると、LTSRサイトは非準拠になります。また、Windows 10用のPvDは引き続き7.15 LTSRから除外されます。したがって、顧客は7.15 LTSRサイトでこれを使用すべきではありません。

PvD、AppDisks、およびサポートされていないホストを削除する

Citrix Virtual Apps and Desktops 7 Current Release展開では、以下のテクノロジーとホストタイプはサポートされていません。

- カタログ内のユーザーのVMの隣にデータを保存するための**Personal vDisks (PvD)**。ユーザーパーソナライゼーションレイヤー機能がユーザーの永続性を処理するようになりました。
- デリバリーグループで使用されるアプリケーションを管理するための**AppDisks**。
- **ホストタイプ:** Azure Classic、CloudPlatform (元のCitrix製品)。
    - このリリースでサポートされているホストタイプについては、システム要件を参照してください。
    - ARMおよびAWSを継続して使用できる代替方法については、CTX270373を参照してください。

現在の展開でPvDまたはAppDisksを使用している場合、あるいはサポートされていないホストタイプ (例: Microsoft Azure Classic) への接続がある場合、それらのテクノロジーを使用する項目を削除した後にのみ、バージョン2006 (またはそれ以降のサポートされているバージョン) にアップグレードできます。現在の展開でパブリッククラウドホスト接続 (例: AWS) を使用している場合は、アップグレードする前にハイブリッドライツライセンスがあることを確認してください。インストーラーがサポートされていないテクノロジーまたはハイブリッドライツライセンスのないホスト接続を1つ以上検出すると、アップグレードは一時停止または停止し、説明メッセージが表示されます。インストーラーログには詳細が含まれています。

アップグレードを確実に成功させるために、サポートされていない項目を削除するための該当するガイダンスを確認し、それに従ってください。

- PvDを削除
- AppDisk を削除する
- サポートされていないホスト項目を削除する

展開でPvDまたはAppDiskを使用していなかった場合でも、関連するMSIが以前のVDAのインストールまたはアップグレードに含まれていた可能性があります。VDAをバージョン2006（または

それ以降のサポートされているバージョン）にアップグレードする前に、そのソフトウェアを一度も使用していなかったとしても、削除する必要があります。グラフィカルインターフェイスを使用する場合、その削除は自動的に行われるか、CLIを使用する際に削除オプションを含めることができます。詳細については、「PvDまたはAppDiskコンポーネントを持つVDAのアップグレード」(#vdas-that-have-pvd-or-appdisks-components)を参照してください。

PvDを削除する

PvDを使用するように構成されているすべてのマシンを削除するまで、展開のアップグレードは成功しません。これはカタログとデリバリーグループに影響します。

グループとカタログからPvDを削除するには：

1. Studioで、デリバリーグループにPvDを使用するカタログのマシンが含まれている場合、「それらのマシンをグループから削除」(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/install-configure/delivery-groups-manage.html#remove-a-machine-from-a-delivery-group)します。
2. Studioで、PvDを使用するマシンを含む「すべてのカタログを削除」(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/install-configure/machine-catalogs-manage.html#delete-a-catalog)します。

VDAのアップグレード： 展開のアップグレードでは、VDAにAppDiskまたはPvDコンポーネントがインストールされているかどうかは検出されません。ただし、VDAインストーラーは検出します。詳細については、「PvDまたはAppDiskコンポーネントを持つVDA」(#vdas-that-have-pvd-or-appdisks-components)を参照してください。

AppDiskを削除する

AppDiskを使用するすべてのデリバリーグループからAppDiskを削除し、その後AppDisk自体を削除するまで、展開のアップグレードは続行できません。

1. Studioのナビゲーションペインで**［デリバリーグループ］**を選択します。
2. グループを選択し、アクションペインで**［AppDiskの管理］**をクリックします。
3. グループからAppDiskを削除するアクションをクリックします。
4. AppDiskを使用する各デリバリーグループに対して、手順2と3を繰り返します。
5. Studioナビゲーションペインで**AppDisks**を選択します。
6. AppDiskを選択し、AppDiskを削除するアクションをクリックします。
7. 各AppDiskについて、手順5と6を繰り返します。

VDAのアップグレード: 展開のアップグレードでは、VDAにAppDiskまたはPvDコンポーネントがインストールされているかどうかは検出されません。ただし、VDAインストーラーは検出します。

詳細については、「PvDまたはAppDisksコンポーネントがインストールされているVDA」を参照してください。

サポートされていないホストアイテムを削除する

サイトがCitrix CloudPlatformやMicrosoft Azure Classicなどのサポートされていないホストタイプへの接続を持っている場合、バージョン2006（またはそれ以降のサポートされているバージョン）への展開のアップグレードは続行できません。アップグレードを試みる前に、次のタスクを完了してください。

Studioから：

- サポートされていないホストへのすべての接続を削除します。
- デリバリーグループに、サポートされていないホストのマスターイメージで作成されたカタログのマシンが含まれている場合は、それらのマシンをグループから削除します。
- サポートされていないホストのマスターイメージを使用して作成されたすべてのカタログを削除します。

PvDまたはAppDisksコンポーネントがインストールされているVDA

PvDおよびAppDisksテクノロジーを有効にするコンポーネントがVDAにインストールされている場合、それらのコンポーネントが削除されるまで、そのVDAはアップグレードできません。

> **注：**
>
> バージョン1912にアップグレードする場合、現在のVDAをアンインストールしてから新しいVDAをインストールする必要がありました。このバージョンでは、Citrixがコンポーネントを削除してアップグレードを続行するかどうかを尋ねられます。

> AppDiskおよびPvDコンポーネントは、それらのテクノロジーを一度も使用していなくても、以前のVDAバージョンでインストールされている可能性があります。

- グラフィカルインターフェイス：VDAインストーラーの**追加コンポーネント**ページには、**Citrix AppDisk / Personal vDisk**オプションが含まれていました。7.15 LTSRおよびそれ以前の7.xリリースでは、このオプションがデフォルトで有効になっていました。したがって、デフォルトを受け入れた場合（または、このオプションが提供されたリリースで明示的に有効にした場合）、そのコンポーネントがインストールされました。
- CLI: `/baseimage`オプションを指定すると、コンポーネントがインストールされました。

対処法

VDAインストーラーが現在インストールされているVDAでAppDisksまたはPvDコンポーネントを検出しない場合、アップグレードは通常どおり続行されます。

インストーラーが現在インストールされているVDAでAppDisksまたはPvDコンポーネントを検出した場合：

- グラフィックインターフェイス：アップグレードが一時停止します。サポートされていないコンポーネントを自動的に削除するかどうかを尋ねるメッセージが表示されます。**OK**をクリックすると、コンポーネントは自動的に削除され、アップグレードが続行されます。
- CLI：コマンドの失敗を避けるには、コマンドに次のオプションを含めます。
  - `/remove_appdisk_ack`
  - `/remove_pvd_ack`

制限事項

アップグレードには次の制限が適用されます。

- **選択的なコンポーネントのインストール：** 新しいバージョンにコンポーネントをインストールまたはアップグレードしても、アップグレードが必要な他のコンポーネント（別のマシン上）をアップグレードしないことを選択した場合、Studioから通知されます。たとえば、アップグレードにControllerとStudioの新しいバージョンが含まれているとします。Controllerはアップグレードしましたが、Studioがインストールされているマシンでインストーラーを実行しませんでした。Studioは、Studioをアップグレードするまでサイトの管理を続行できません。

  VDAをアップグレードする必要はありませんが、利用可能なすべての機能を使用できるように、すべてのVDAをアップグレードすることをお勧めします。
- **早期リリースまたはテクノロジプレビューバージョン：** 早期リリース、テクノロジプレビュー、またはプレビューバージョンからアップグレードすることはできません。
- **以前のオペレーティングシステム上のコンポーネント：** MicrosoftまたはCitrixでサポートされなくなったオペレーティングシステムに現在のVDAをインストールすることはできません。詳しくは、「以前のオペレーティングシステム」を参照してください。
- **混在環境/サイト：** 以前のバージョンのサイトと現在のバージョンのサイトを継続して実行する必要がある場合は、「混在環境に関する考慮事項」を参照してください。

- **製品の選択：** 以前のバージョンからアップグレードする場合、インストール時に設定された製品（Citrix Virtual AppsまたはCitrix Virtual Apps and Desktops）を選択または指定することはありません。

混在環境に関する考慮事項

アップグレード時には、エディションとバージョンで利用可能なすべての新機能と強化された機能にアクセスできるように、すべてのコンポーネントとVDAをアップグレードすることをお勧めします。

例えば、以前のControllerバージョンを含む展開で現在のVDAを使用することはできますが、現在のリリースで追加された新機能は利用できない場合があります。最新ではないバージョンを使用している場合、VDA登録の問題も発生する可能性があります。

一部の環境では、すべてのVDAを最新バージョンにアップグレードできない場合があります。その場合、マシンカタログを作成する際に、マシンにインストールされているVDAバージョンを指定できます。(これは機能レベルと呼ばれます。)デフォルトでは、この設定は推奨される最小VDAバージョンを指定します。ほとんどの展開では、デフォルト値で十分です。カタログにデフォルトよりも古いVDAが含まれている場合にのみ、設定を以前のバージョンに変更することを検討してください。マシンカタログ内でVDAバージョンを混在させることは推奨されません。

カタログがデフォルトの最小VDAバージョン設定で作成され、1つ以上のマシンがデフォルトバージョンよりも古いVDAを持っている場合、それらのマシンはControllerに登録できず、機能しません。

詳細については、VDAバージョンと機能レベルを参照してください。

異なるバージョンを持つ複数のサイト

環境に異なる製品バージョンを持つサイト（例えば、XenDesktop 7.18サイトとCitrix Virtual Apps and Desktops 1909サイト）が含まれている場合、CitrixはStoreFrontを使用して異なる製品バージョンからのアプリケーションとデスクトップを集約することを推奨します。詳細については、StoreFrontのドキュメントを参照してください。

混在環境では、各リリースに対応するStudioおよびDirectorのバージョンを引き続き使用しますが、異なるバージョンは別々のマシンにインストールされていることを確認してください。

以前のオペレーティングシステム

サポートされているオペレーティングシステム（OS）バージョンを実行しているマシンに、コンポーネントの以前のバージョンをインストールしたとします。現在、より新しいコンポーネント

バージョンを使用したいと考えていますが、そのOSは現在のコンポーネントバージョンではサポートされていません。

例えば、Windows Server 2008 R2マシンにサーバーVDAをインストールしたとします。現在、そのVDAを現在のリリースにアップグレードしたいと考えていますが、アップグレード先の現在のリリースではWindows Server 2008 R2はサポートされていません。

許可されていないオペレーティングシステムにコンポーネントをインストールまたはアップグレードしようとすると、「このオペレーティングシステムにはインストールできません」などのエラーメッセージが表示されます。

これらの考慮事項は、Current ReleaseおよびLong Term Service Releaseバージョンのアップグレードに適用されます。（LTSRバージョンにCUを適用することには影響しません。）

サポートされているOSについては、以下のリンクを参照してください。

- Citrix Virtual Apps and Desktops (現在のリリース):
  - デリバリーコントローラー、スタジオ、ディレクター、VDA、ユニバーサルプリントサーバー
  - フェデレーション認証サービス
  - StoreFront、セルフサービスパスワードリセット、およびセッションレコーディングについては、現在のリリースのシステム要件の記事を参照してください。
- LTSRについては、お使いのLTSRバージョンとCUのコンポーネントリストを参照してください。(メインのCitrix Virtual Apps and Desktops製品ドキュメントページからお使いのLTSRバージョンを選択してください。)

無効なオペレーティングシステム

以下の表に、現在のリリースでコンポーネントのインストール/アップグレードに無効な以前のオペレーティングシステムを示します。各OSでサポートされる最新の有効なコンポーネントバージョンと、インストールおよびアップグレードが無効になったコンポーネントバージョンを示します。

表中のオペレーティングシステムにはサービスパックと更新プログラムが含まれます。

オペレーティングシステム	コンポーネント/機能	最新の有効なバージョン	インストール/アップグレードが不可能になったバージョン
Windows 7およびWindows 8	VDA	7.15 LTSR	7.16
Windows 7およびWindows 8	その他のインストーラーコンポーネント	7.17	7.18
Windows 10 バージョン 1607 より前のもの	VDA	7.15 LTSR	7.16
Windows 10 x86 バージョン	VDA	1906.2.0	1909
Windows サーバー 2008 R2	VDA	7.15 LTSR	7.16
Windows サーバー 2008 R2	その他のインストーラーコンポーネント	7.17	7.18
Windows サーバー 2012	VDA	7.15 LTSR	7.16
Windows サーバー 2012	その他のインストーラーコンポーネント	7.17	7.18
ウィンドウズ サーバー 2012 R2	その他のインストーラーコンポーネント *	1912 LTSR	2003
ウィンドウズ サーバー 2012 R2	サーバーVDI	7.15 LTSR	7.16

Windows XPおよびWindows Vistaは、7.xのコンポーネントまたはテクノロジーでは無効です。

* Delivery Controller、Studio、Director、およびVDAに適用されます。

実行できること

選択肢があります。次のことができます。

- 現在のOSを継続して使用する(#continue-with-the-current-os)
- マシンの再イメージ化またはアップグレード(#reimage-or-upgrade-the-machine)
- 新しいマシンを追加してから古いマシンを削除する(#add-new-machines-and-then-remove-old-machines)

現在のOSを継続して使用する

これらの方法はVDAで実行可能です。以前のOSを搭載したマシンの使用を継続する場合は、次のいずれかを選択できます。

- インストールされているコンポーネントバージョンを継続して使用する。
- 最新の有効なコンポーネントバージョンをダウンロードし、そのバージョンにコンポーネントをアップグレードする。（これは、最新の有効なコンポーネントバージョンがまだインストールされていないことを前提としています。）

たとえば、Windows 7 SP1マシンに7.14 VDAがインストールされているとします。Windows 7 OSマシンで有効な最新のVDAバージョンは、XenApp and XenDesktop 7.15 LTSRです。7.14を継続して使用するか、7.15 LTSR VDAをダウンロードしてVDAをそのバージョンにアップグレードすることができます。これらの以前のVDAバージョンは、新しいバージョンのDelivery Controllerを含む展開で動作します。たとえば、7.15 LTSR VDAはCitrix Virtual Apps and Desktops 7 1808 Controllerに接続できます。

マシンの再イメージ化またはアップグレード

これらの方法は、VDAおよびコアコンポーネント（Delivery Controllerなど）がインストールされていないその他のマシンで実行可能です。次のいずれかを選択してください。

- マシンをサービスから外し（メンテナンスモードをオンにしてすべてのセッションを閉じさせてから）、サポートされているWindows OSバージョンに再イメージ化し、コンポーネントの最新バージョンをインストールできます。
- 再イメージ化せずにVDAマシンでOSをアップグレードするには、まずアップグレード先のOSでサポートされているVDAバージョンをインストールするか、OSのアップグレード後にVDAをアップグレードする必要があります。そうしないと、Citrixソフトウェアはサポートされません。VDAをアンインストールせずにインプレースアップグレードを実行する場合、次の最小OSバージョンにアップグレードできます。
  - 2023-07 Cumulative Update for Windows 11 (KB5028185)以降がインストールされているWindows 11（ビルド22621.1992以降）。
  - 2023-07 Dynamic Update for Windows 10 (KB5028311)がインストールされているWindows 10。

- アップグレードを計画しているWindowsのバージョンが上記のガイドラインに合致しない場合は、OSをアップグレードする前にVDAをアンインストールし、OSのアップグレードが完了した後にサポートされているVDAバージョンをインストールする必要があります。

新しいマシンを追加し、古いマシンを削除する

この方法は、Delivery Controller™ またはその他のコアコンポーネントを含むマシンの OS をアップグレードする必要がある場合に実行可能です。

Citrix は、サイト内のすべてのコントローラーが同じ OS を持つことを推奨しています。以下のアップグレードシーケンスは、異なるコントローラーが異なる OS を持つ期間を最小限に抑えます。

1. サイト内のすべての Delivery Controller のスナップショットを取得し、サイトデータベースをバックアップします。
2. サポートされているオペレーティングシステムを搭載したクリーンなサーバーに新しい Delivery Controller をインストールします。たとえば、2 台の Windows Server 2016 マシンにコントローラーをインストールします。
3. 新しいコントローラーをサイトに追加します。
4. 現在のリリースで有効ではないオペレーティングシステムで実行されているコントローラーを削除します。たとえば、2 台の Windows Server 2008 R2 マシン上の 2 つのコントローラーを削除します。Delivery Controllers のコントローラー削除に関する推奨事項に従ってください。

準備

アップグレードを開始する前に、以下の情報を確認し、必要なタスクを完了してください。

> **注：**
>
> VDA のアップグレードは アップグレードシーケンス の後半で行われますが、アップグレードを開始する前にインストーラーを選択し、手順を確認して、何が予想されるかを知っておくことをお勧めします。

インストーラーとインターフェイスを選択する

コンポーネントをアップグレードするには、製品 ISO からフルプロダクトインストーラーを使用します。VDA は、フルプロダクトインストーラーまたはスタンドアロン VDA インストーラーのいずれかを使用してアップグレードできます。すべてのインストーラーは、グラフィカルインターフェイスとコマンドラインインターフェイスを提供します。

詳細については、インストーラー を参照してください。

インストールの詳細: 準備作業を完了し、インストーラーを起動する準備ができたら、インストール記事には、表示される内容 (グラフィカルインターフェイスを使用している場合) または入力する内容 (コマンドラインインターフェイスを使用している場合) が示されています。

- グラフィカルインターフェイスを使用してコアコンポーネントをインストール/アップグレードする
- コマンドラインを使用してコアコンポーネントをインストール/アップグレードする
- グラフィカルインターフェイスを使用したVDAのインストール/アップグレード
- コマンドラインを使用したVDAのインストール/アップグレード

シングルセッションVDAを`VDAWorkstationCoreSetup.exe`インストーラーで最初にインストールした場合、そのインストーラーを使用してアップグレードすることをお勧めします。フルプロダクトVDAインストーラーまたは`VDAWorkstationSetup.exe`インストーラーを使用してVDAをアップグレードすると、明示的にアップグレードから除外しない限り、元々除外されていたコンポーネントがインストールされる可能性があります。

VDAを現在のリリースにアップグレードする際、アップグレードプロセス中にマシンの再起動が発生します（この要件は7.17リリースから始まりました）。これは回避できません。再起動後、アップグレードは自動的に再開されます（コマンドラインで`/noresume`を指定しない限り）。

データベース操作

サイト、監視、および構成ログデータベースをバックアップします。CTX135207の手順に従ってください。アップグレード後に問題が発見された場合、バックアップを復元できます。

サポートされなくなったSQL Serverバージョンのアップグレードについては、SQL Serverバージョンチェックを参照してください。（これは、サイト、モニター、および構成ログデータベースに使用されるSQL Serverを指します。）

Microsoft SQL Server Express LocalDBは、ローカルホストキャッシュで使用するために自動的にインストールされます。以前のバージョンを置き換える必要がある場合、新しいバージョンはSQL Server Express LocalDB 2019である必要があります。コンポーネントとサイトをアップグレードした後にSQL Server Express LocalDBを新しいバージョンに置き換える方法の詳細については、SQL Server Express LocalDBの置き換えを参照してください。

Citrixライセンスが最新であることを確認する

Citrixライセンスの管理に関する包括的な情報については、Citrixライセンスのアクティブ化、アップグレード、および管理を参照してください。

フルプロダクトインストーラーを使用してライセンスサーバーをアップグレードできます。または、ライセンスコンポーネントを個別にダウンロードしてアップグレードすることもできます。アップグレードを参照してください。

アップグレードする前に、Customer Success Services / Software Maintenance / Subscription Advantageの有効期限が新しい製品バージョンに対応していることを確認してください。日付は2021年11月15日以降である必要があります。

Citrixライセンスサーバーの互換性を確認する

Citrixライセンスサーバーが新しいバージョンと互換性があることを確認してください。これには2つの方法があります。

- 他のCitrixコンポーネントをアップグレードする前に、Delivery Controllerを含むマシンでISOレイアウトから`XenDesktopServerSetup.exe`インストーラーを実行します。互換性の問題がある場合、インストーラーは推奨される解決手順とともにそれを報告します。
- インストールメディアの`XenDesktop Setup`ディレクトリから、コマンド`.\LicServVerify.exe -h <license-server-fqdn> -p 27000 -v`を実行します。表示でライセンスサーバーが互換性があるかどうかが示されます。ライセンスサーバーに互換性がない場合は、ライセンスサーバーをアップグレードしてください。

StoreFrontの変更をバックアップする

アップグレードを開始する前に、`C:\inetpub\wwwroot\Citrix\<StoreName>\App_Data`内のファイル（*default.ica*や*usernamepassword.tfrm*など）に変更を加えている場合は、各ストアのファイルをバックアップしてください。アップグレード後にそれらを復元して、変更を元に戻すことができます。

アプリケーションとコンソールを閉じる

アップグレードを開始する前に、管理コンソールやPowerShellセッションなど、ファイルロックを引き起こす可能性のあるすべてのプログラムを閉じます。

マシンを再起動すると、ファイルロックがすべて解除され、保留中のWindowsアップデートがないことが保証されます。

アップグレードを開始する前に、サードパーティの監視エージェントサービスをすべて停止して無効にします。

適切な権限があることを確認する

ドメインユーザーであることに加えて、製品コンポーネントをアップグレードするマシンではローカル管理者である必要があります。

サイトデータベースとサイトは、自動または手動でアップグレードできます。データベースの自動アップグレードの場合、Studioユーザーの権限には、SQL Serverデータベーススキーマを更新する機能（たとえば、`db_securityadmin`または`db_owner`データベースロール）が含まれている必要があります。詳細については、「データベース」を参照してください。

Studioユーザーがこれらの権限を持っていない場合、手動データベースアップグレードを開始すると、スクリプトが生成されます。Studioユーザーは、Studioから一部のスクリプトを実行します。データベース管理者は、SQL Server Management Studioなどのツールを使用して、他のスクリプトを実行します。

その他の準備タスク

- 必要に応じて、テンプレートをバックアップし、ハイパーバイザーをアップグレードします
- 事業継続計画で定められているその他の準備タスクを完了します。

サイトの事前テスト

Delivery Controllerとサイトをアップグレードすると、実際のアップグレードが始まる前に予備サイトテストが実行されます。これらのテストでは、以下が検証されます。

- サイトデータベースにアクセスでき、バックアップされていること
- 重要なCitrixサービスへの接続が正しく機能していること
- Citrixライセンスサーバーのアドレスが利用可能であること
- 構成ログデータベースにアクセスできること
- パブリッククラウドホスト接続（例：AWS）を追加する場合は、ハイブリッド権限ライセンスがあることを確認してください。そうしないと、予備サイトテストが一時停止または停止し、説明メッセージが表示されます。

テストの実行後、結果のレポートを表示できます。検出された問題を修正し、テストを再度実行できます。予備サイトテストを実行せず、問題を解決しないと、サイトの動作に影響を与える可能性があります。

テスト結果を含むレポートは、インストールログと同じディレクトリにあるHTMLファイル（`PreliminarySiteTestResult.html`）です。そのファイルが存在しない場合は作成されます。ファイルが存在する場合は、その内容が上書きされます。

テストを実行する

- インストーラーのグラフィカルインターフェイスを使用してアップグレードする場合、ウィザードにはテストを開始してレポートを表示できるページが含まれています。テストが実行さ

れ、レポートを確認し、見つかった問題を解決した後、テストを再実行できます。テストが正常に完了したら、 をクリックしてウィザードを続行します。

- コマンドラインインターフェイスを使用してアップグレードする場合、テストは自動的に実行されます。デフォルトでは、テストが失敗した場合、アップグレードは実行されません。レポートを確認し、問題を解決した後、コマンドを再実行してください。

Citrixは、Controllerとサイトのアップグレードを続行する前に、常に予備サイトテストを実行し、問題を解決することを推奨しています。テストを実行するのにかかるわずかな時間で得られる潜在的なメリットは十分にあります。ただし、この推奨されるアクションを上書きすることもできます。

- グラフィカルインターフェイスでアップグレードする場合、テストをスキップしてアップグレードを続行することを選択できます。
- コマンドラインからアップグレードする場合、テストをスキップすることはできません。デフォルトでは、サイトテストが失敗すると、アップグレードを実行せずにインストーラーが失敗します。ほとんどの場合、`/ignore_site_test_failure` オプションを含めると、テストの失敗は無視され、アップグレードが続行されます。（例外については、SQL Serverのバージョンチェック を参照してください。）

複数のControllerをアップグレードする場合

1つのControllerでアップグレードを開始し、その後、同じサイト内の別のControllerでアップグレードを開始した場合（最初のアップグレードが完了する前）：

- 最初のControllerで予備サイトテストが完了している場合、他のControllerのウィザードには予備サイトテストページは表示されません。
- 他のControllerでアップグレードを開始したときに最初のControllerでのテストが進行中の場合、他のControllerのウィザードにサイトテストページが表示されます。ただし、最初のControllerでのテストが完了すると、最初のControllerからのテスト結果のみが保持されます。

サイトの健全性に関連しないテストの失敗

- 予備サイトテストがメモリ不足で失敗した場合は、より多くのメモリを確保してからテストを再実行してください。
- アップグレードの権限はあるがサイトテストを実行する権限がない場合、予備サイトテストは失敗します。これを解決するには、テストを実行する権限を持つユーザーアカウントでインストーラーを再実行してください。

SQL Serverバージョンの確認

Citrix Virtual Apps and Desktopsの展開を成功させるには、サイト、モニター、および構成ログデータベース用にサポートされているバージョンのMicrosoft SQL Serverが必要です。サポートされなくなったSQL ServerバージョンでCitrix展開をアップグレードすると、機能上の問題が発生する可能性があり、サイトはサポート対象外となります。

アップグレード先のCitrixリリースでサポートされているSQL Serverのバージョンについては、そのリリースのシステム要件の記事を参照してください。

Controllerをアップグレードする際、Citrixインストーラーは、サイト、モニター、および構成ログデータベースに使用されている現在インストールされているSQL Serverのバージョンを確認します。

- チェックの結果、現在インストールされているSQL Serverのバージョンが、アップグレード先のCitrixリリースでサポートされているバージョンではないと判断された場合：
  - グラフィカルインターフェイス：アップグレードはメッセージとともに停止します。「**了解**」をクリックし、次に「**キャンセル**」をクリックしてCitrixインストーラーを閉じます。（アップグレードを続行することはできません。）
  - コマンドラインインターフェイス：コマンドは失敗します（コマンドに`/ignore_db_check_failure`オプションを含めた場合でも）。

  SQL Serverのバージョンをアップグレードしてから、Citrixのアップグレードを再度開始してください。
- チェックで現在インストールされているSQL Serverのバージョンを特定できない場合は、現在インストールされているバージョンがアップグレード先のバージョンでサポートされているかどうかを確認してください（システム要件）。
  - グラフィカルインターフェイス: アップグレードがメッセージとともに停止します。
    - 現在インストールされているSQL Serverのバージョンがサポートされている場合は、**I understand**をクリックしてメッセージを閉じ、**Next**をクリックしてCitrixのアップグレードを続行します。
    - 現在インストールされているSQL Serverのバージョンがサポートされていない場合は、**I understand**をクリックしてメッセージを閉じ、**Cancel**をクリックしてCitrixのアップグレードを終了します。SQL Serverをサポートされているバージョンにアップグレードしてから、Citrixのアップグレードを再度開始してください。
  - コマンドラインインターフェイス: コマンドがメッセージとともに失敗します。メッセージを閉じた後:

- 現在インストールされているSQL Serverのバージョンがサポートされている場合は、`/ignore_db_check_failure`オプションを指定してコマンドを再度実行します。
- 現在インストールされているSQL Serverのバージョンがサポートされていない場合は、SQL Serverをサポートされているバージョンにアップグレードします。コマンドを再度実行してCitrixのアップグレードを開始します。

SQL Serverのアップグレード

新しいSQL Serverサーバーを立ち上げてサイトデータベースを移行する場合、接続文字列を更新する必要があります。

サイトが現在、サイトデータベースにSQL Server Expressを使用している場合（Citrixがサイト作成時に自動的にインストールしたもの）：

1. 最新のSQL Server Expressバージョンをインストールします。
2. データベースをデタッチします。
3. データベースを新しいSQL Server Expressにアタッチします。
4. 接続文字列を移行します。

詳細については、接続文字列の構成およびMicrosoft SQL Serverの製品ドキュメントを参照してください。

SQL Server Express LocalDBの置き換え

Microsoft SQL Server Express LocalDB は、Local Host Cache がスタンドアロンで使用する SQL Server Express の機能です。Local Host Cache は、SQL Server Express LocalDB 以外の SQL Server Express のコンポーネントを必要としません。

Citrix は SQL Server Express LocalDB を自動的に更新しません。SQL Server Express LocalDB のバージョンを更新するには、このセクションのガイダンスに従ってください。

- Delivery Controller を Citrix Virtual Apps and Desktops バージョン 2203 LTSR 以降のバージョンにアップグレードする場合、サポートされるバージョンは SQL Server Express LocalDB 2019 または SQL Server Express LocalDB 2022 です。

> **注：**
>
> SQL Server Express LocalDB 2022 は、Citrix Virtual Apps and Desktops バージョン 2203 LTSR CU5 以降でサポートされています。

> 必要なもの:

- Citrix Virtual Apps and Desktops のインストールメディア。
- Windows Sysinternals ツールボックスの PsExec ツール。

手順:

1. Citrix Virtual Apps and Desktops のコンポーネント、データベース、およびサイトのアップグレードを完了します。（これらのデータベースアップグレードは、サイト、監視、および構成ログデータベースに影響します。SQL Server Express LocalDB を使用する Local Host Cache データベースには影響しません。）
2. SQL Server Express LocalDB を更新する Delivery Controller にログオンします。
3. Microsoft から PsExec をダウンロードし、その Delivery Controller 上のアクセスしやすい場所（例: C:\Temp）に配置します。
4. Windowsシステムサービスから、Delivery Controller上のCitrix High Availability Serviceを停止します。
5. Delivery Controller でコマンドプロンプトを開き、PsExec がある場所（例: `C:\Temp`）に移動してから、次のコマンドを実行して、Network Service アカウントでコマンドプロンプトを昇格させます。

   ```
   psexec -i -u "NT AUTHORITY\NETWORKSERVICE" cmd
   ```

6. `whoami` を実行して、コマンドプロンプトが Network Service アカウントとして実行されていることを確認します。次の出力が得られるはずです: `nt authority\networkservice`。
7. コマンドプロンプトを使用して、SQL LocalDB インスタンスに移動します。

   - SQL LocalDB 2014からアップグレードする場合:

     ```
     cd "C:\Program Files\Microsoft SQL Server\120\Tools\Binn"
     ```

   - SQL LocalDB 2017からアップグレードする場合:

     ```
     cd "C:\Program Files\Microsoft SQL Server\140\Tools\Binn"
     ```

   - SQL LocalDB 2019からアップグレードする場合:

```
cd "C:\Program Files\Microsoft SQL Server\150\Tools\Binn"
```

8. SQL LocalDBインスタンスを停止して削除します: `CitrixHA`。

```
SqlLocalDB stop CitrixHA



SqlLocalDB delete CitrixHA
```

9. Delivery Controllerから以下のファイルを削除します:

```
C:\Windows\ServiceProfiles\NetworkService\HADatabaseName.*

C:\Windows\ServiceProfiles\NetworkService\HADatabaseName_log.*

C:\Windows\ServiceProfiles\NetworkService\HAImportDatabaseName.* (if
exists)

C:\Windows\ServiceProfiles\NetworkService\HAImportDatabaseName_log.*
(if exists)
```

10. プログラムを削除するためのWindowsのネイティブ機能を使用して、Delivery Controllerから既存のSQL LocalDB SQL Server Expressをアンインストールします。
11. アンインストールが完了したら、Delivery Controllerを再起動します。
12. Windowsシステムサービスから、Delivery Controller上のCitrix High Availability Serviceを停止します。
13. Citrix Virtual Apps and Desktopsのインストールメディアを Delivery Controllerにマウントします。
14. Delivery Controllerに管理者としてSQL Server Express LocalDB 2019をインストールします。
    a. Citrix Virtual Apps and Desktopsインストールメディアの `Support > SQLLocalDB` フォルダーにある `sqllocaldb.msi` ファイルを使用します。たとえば、インストールメディアが `E drive` ドライブにマウントされている場合、ファイルは `E:\Support\SQLLocalDB\sqllocaldb.msi` にあります。インストールを完了するには再起動が必要です。

   b. 新しいSQL LocalDBは`C:\Program Files\Microsoft SQL Server\160\Tools\Binn`にある必要があります。

15. Windowsシステムサービスから、Delivery Controller上のCitrix High Availability Serviceを開始します。
16. Delivery Controllerのコマンドプロンプトで、`C:\Program Files\Microsoft SQL Server\160\Tools\Binn`に移動し、`SqlLocalDB i`を実行してCitrixHAインスタンスが作成されたことを確認します。返されたインスタンスのリストに`CitrixHA`が含まれている必要があります。

> **注：**
>
> Citrix High Availability Serviceの開始後、CitrixHAデータベースが作成されるまでに最大15分かかる場合があります。

17. ローカルホストキャッシュデータベースファイルが作成されていることを確認し、必要に応じて高可用性サービス（セカンダリブローカー）が引き継ぐことができることを確認します。
   a. Delivery Controllerで、`C:\Windows\ServiceProfiles\NetworkService`を参照します。
   b. `HaDatabaseName.mdf`と`HaDatabaseName_log.ldf`が作成されていることを確認します。
18. 残りのDelivery Controllerで手順を繰り返します。

セキュリティ

Citrix Virtual Apps and Desktops™ は、セキュリティニーズに合わせて環境を調整できる、設計段階から安全なソリューションを提供します。

モバイルワーカーが直面するセキュリティ上の懸念の1つは、データの紛失または盗難です。Citrix Virtual Apps and Desktopsは、アプリケーションとデスクトップをホストすることで、すべてのデータをデータセンターに保持し、機密データと知的財産をエンドポイントデバイスから安全に分離します。データ転送を許可するポリシーが有効になっている場合、すべてのデータは暗号化されます。

Citrix Virtual Apps and Desktops のデータセンターは、一元化された監視および管理サービスにより、インシデント対応も容易にします。Director を使用すると、IT部門はネットワーク全体でアクセスされているデータを監視および分析でき、Studio を使用すると、IT部門は各エンドユーザーデバイスでローカルに問題を修正する代わりに、データセンター内のほとんどの脆弱性をパッチ適用して修復できます。

Citrix Virtual Apps and Desktops は、監査と規制コンプライアンスも簡素化します。調査官は、一元化された監査証跡を使用して、誰がどのアプリケーションとデータにアクセスしたかを判断できるためです。Director は、構成ログと OData API にアクセスすることで、システムへの更新とユーザーデータ使用量に関する履歴データを収集します。

委任管理により、Citrix Virtual Apps and Desktops へのアクセスをきめ細かく制御するための管理者ロールを設定できます。これにより、組織内で特定の管理者にタスク、操作、スコープへのフルアクセスを許可し、他の管理者には制限されたアクセスを許可する柔軟性が得られます。

シトリックス バーチャルアプリ＆デスクトップは、ローカルレベルから組織単位レベルまで、ネットワークのさまざまなレベルでポリシーを適用することにより、管理者にユーザーに対するきめ細かな制御を提供します。このポリシーの制御により、ユーザー、デバイス、またはユーザーとデバイスのグループが接続、印刷、コピー/貼り付け、またはローカルドライブのマッピングができるかどうかが決定され、サードパーティの臨時作業者に関するセキュリティ上の懸念を最小限に抑えることができます。管理者は、デスクトップロック機能も使用でき、エンドユーザーが仮想デスクトップのみを使用できるようにし、エンドユーザーデバイスのローカルオペレーティングシステムへのアクセスを防止します。

管理者は、サイトを構成して、Controller の、またはエンドユーザーと Virtual Delivery Agents (VDA) 間の Transport Layer Security (TLS) プロトコルを使用するようにすることで、Citrix Virtual Apps または Citrix Virtual Desktops のセキュリティを強化できます。このプロトコルは、TCP/IP 接続のサーバー認証、データストリーム暗号化、およびメッセージ整合性チェックを提供するために、サイトで有効にすることもできます。

Citrix Virtual Apps and Desktops は、Windows または特定のアプリケーションの多要素認証もサポートしています。多要素認証は、Citrix Virtual Apps and Desktops によって提供されるすべてのリソースを管理するためにも使用できます。これらの方法には以下が含まれます。

- トークン
- スマートカード
- RADIUS
- ケルベロス
- 生体認証

Citrix Virtual Desktops は、ID管理からウイルス対策ソフトウェアまで、多くのサードパーティ製セキュリティソリューションと統合できます。サポートされている製品のリストは `<http://www.citrix.com/ready>` で確認できます。

Citrix Virtual Apps and Desktops の一部のリリースは、Common Criteria 標準の認定を受けています。これらの標準のリストについては、`<https://www.commoncriteriaportal.org/cc/>` にアクセスしてください。

セキュリティに関する考慮事項とベストプラクティス

> **注：**
>
> 組織は規制要件を満たすために特定のセキュリティ標準に準拠する必要がある場合があります。このようなセキュリティ標準は時間とともに変化するため、このドキュメントではこの主題を扱いません。セキュリティ標準とCitrix製品に関する最新情報については、`<http://www.citrix.com/security/>` を参照してください。

セキュリティのベストプラクティス

環境内のすべてのマシンをセキュリティパッチで最新の状態に保ちます。利点の1つは、シンクライアントをターミナルとして使用できるため、このタスクが簡素化されることです。

環境内のすべてのマシンをアンチウイルスソフトウェアで保護します。

プラットフォーム固有のマルウェア対策ソフトウェアの使用を検討してください。

ソフトウェアをインストールする際は、提供されているデフォルトのパスにインストールしてください。

- 提供されているデフォルトのパス以外のファイル場所にソフトウェアをインストールする場合は、そのファイル場所に制限付きアクセス許可などの追加のセキュリティ対策を追加することを検討してください。

すべてのネットワーク通信は、セキュリティポリシーに合わせて適切に保護および暗号化する必要があります。Microsoft Windowsコンピューター間のすべての通信はIPSecを使用して保護できます。これを行う方法の詳細については、オペレーティングシステムのドキュメントを参照してください。さらに、ユーザーデバイスとデスクトップ間の通信は、Citrix SecureICAによって保護されます。SecureICAは、デフォルトで128ビット暗号化に設定されています。SecureICAは、デリバリーグループの作成または更新時に構成できます。

> **注：**
>
> Citrix SecureICAはICA/HDXプロトコルの一部ですが、Transport Layer Security (TLS) のような標準準拠のネットワークセキュリティプロトコルではありません。ユーザーデバイスとデスクトップ間のネットワーク通信はTLSを使用して保護することもできます。TLSを構成するには、「Transport Layer Security (TLS)」を参照してください。

> アカウント管理にはWindowsのベストプラクティスを適用してください。Machine Creation ServicesまたはProvisioning Servicesによって複製される前に、テンプレートまたはイメージ上にアカウントを作成しないでください。保存された特権ドメインアカウントを使用してタスクをスケジュールしないでください。共有Active Directoryマシンアカウントを手動で作成しないでください。これらの慣行は、マシン攻撃がローカルの永続的なアカウントパスワードを取得し、それらを使用して他のユーザーに属するMCS/PVS共有イメージにログオンするのを防ぐのに役立ちます。

ファイアウォール

環境内のすべてのマシンを、必要に応じてエンクレーブ境界を含め、境界ファイアウォールで保護します。

環境内のすべてのマシンは、パーソナルファイアウォールによって保護されている必要があります。コアコンポーネントとVDAをインストールする際、Windowsファイアウォールサービスが検出された場合（ファイアウォールが有効になっていない場合でも）、コンポーネントおよび機能通信に必要なポートを自動的に開くように選択できます。これらのファイアウォールポートを手動で構成することもできます。別のファイアウォールを使用する場合は、手動で構成する必要があります。

従来の環境をこのリリースに移行する場合、既存の境界ファイアウォールの再配置や新しい境界ファイアウォールの追加が必要になる場合があります。たとえば、データセンター内の従来のクライアントとデータベースサーバーの間に境界ファイアウォールがあるとします。このリリースを使用する場合、その境界ファイアウォールは、仮想デスクトップとユーザーデバイスが一方にあり、データセンター内のデータベースサーバーとDelivery Controllerがもう一方にあるように配置する必要があります。したがって、データベースサーバーとControllerを格納するために、データセンター内にエンクレーブを作成することを検討してください。また、ユーザーデバイスと仮想デスクトップの間に保護を設けることも検討してください。

> **注：**
>
> TCPポート1494と2598はICAとCGPに使用されるため、データセンター外のユーザーがアクセスできるようにファイアウォールで開かれている可能性が高いです。Citrixは、管理インターフェイスが意図せず攻撃にさらされる可能性を避けるため、これらのポートを他の目的で使用しないことを推奨します。ポート1494と2598は、Internet Assigned Number Authority (http://www.iana.org/) に正式に登録されています。

アプリケーションセキュリティ

非管理者ユーザーが悪意のある操作を実行するのを防ぐため、VDAホストおよびローカルのWindowsクライアントで、インストーラー、アプリケーション、実行可能ファイル、およびスクリプトに対してWindows AppLockerルールを構成することをお勧めします。

ユーザー権限の管理

ユーザーには必要な機能のみを付与します。Microsoft Windowsの特権は、通常の方法でデスクトップに適用され続けます。特権はユーザー権利の割り当てを通じて、グループメンバーシップはグループポリシーを通じて構成します。このリリースの利点の1つは、デスクトップが保存されているコンピューターに対する物理的な制御を付与することなく、ユーザーにデスクトップへの管理者権限を付与できることです。

デスクトップの特権を計画する際は、以下に注意してください。

- デフォルトでは、非特権ユーザーがデスクトップに接続すると、自身のユーザーデバイスのタイムゾーンではなく、デスクトップを実行しているシステムのタイムゾーンが表示されます。ユーザーがデスクトップを使用する際にローカルタイムを表示できるようにする方法については、「デリバリーグループの管理」の記事を参照してください。
- デスクトップの管理者であるユーザーは、そのデスクトップを完全に制御できます。デスクトップが専用デスクトップではなくプールされたデスクトップである場合、そのユーザーは、将来のユーザーを含む、そのデスクトップの他のすべてのユーザーに関して信頼できる必要があります。デスクトップのすべてのユーザーは、この状況によってデータセキュリティに潜在的に永続的なリスクがあることを認識する必要があります。この考慮事項は、単一ユーザーのみが使用する専用デスクトップには適用されません。そのユーザーは、他のどのデスクトップの管理者であってもなりません。
- デスクトップの管理者であるユーザーは、一般的に、悪意のあるソフトウェアを含むソフトウェアをそのデスクトップにインストールできます。また、そのユーザーは、デスクトップに接続されているネットワーク上のトラフィックを監視または制御できる可能性もあります。

ログオン権限の管理

ログオン権限は、ユーザーアカウントとコンピューターアカウントの両方に必要です。Microsoft Windowsの特権と同様に、ログオン権限は通常の方法でデスクトップに適用され続けます。ログオン権限はユーザー権利の割り当てを通じて、グループメンバーシップはグループポリシーを通じて構成します。

Windowsのログオン権限は、ローカルログオン、リモートデスクトップサービス経由のログオン、ネットワーク経由のログオン（ネットワークからこのコンピューターにアクセス）、バッチジョブとしてログオン、サービスとしてログオンです。

コンピューターアカウントの場合、コンピューターに必要なログオン権限のみを付与します。「ネットワークからこのコンピューターにアクセス」のログオン権限は、以下の場合に必要です。

- VDAで、デリバリーコントローラーのコンピューターアカウントに対して
- デリバリーコントローラーで、VDAのコンピューターアカウントに対して。「Active Directory OUベースのコントローラー検出」を参照してください。
- StoreFront™ サーバーで、同じ StoreFront サーバーグループ内の他のサーバーのコンピューターアカウントに対して

ユーザーアカウントの場合、ユーザーには必要なログオン権限のみを付与します。

Microsoftによると、デフォルトでは、Remote Desktop Usersグループには「リモートデスクトップサービス経由でのログオンを許可」のログオン権限が付与されています（ドメインコントローラーを除く）。

組織のセキュリティポリシーによっては、このグループをそのログオン権限から削除するよう明示的に規定している場合があります。次のアプローチを検討してください。

- マルチセッションOS用Virtual Delivery Agent (VDA) は、Microsoft Remote Desktop Servicesを使用します。Remote Desktop Usersグループを制限付きグループとして構成し、Active Directoryグループポリシーを介してグループのメンバーシップを制御できます。詳細については、Microsoftのドキュメントを参照してください。
- シングルセッションOS用VDAを含むCitrix Virtual Apps and Desktops™のその他のコンポーネントでは、Remote Desktop Usersグループは不要です。したがって、これらのコンポーネントの場合、Remote Desktop Usersグループには「リモートデスクトップサービスによるログオンを許可」のログオン権限は不要であり、削除できます。さらに：
  - リモートデスクトップサービスを介してそれらのコンピューターを管理する場合、そのようなすべての管理者がすでにAdministratorsグループのメンバーであることを確認してください。
  - それらのコンピューターをリモートデスクトップサービス経由で管理しない場合は、それらのコンピューターでリモートデスクトップサービス自体を無効にすることを検討してください。

ログイン権限「リモートデスクトップサービス経由でのログオンを拒否」にユーザーとグループを追加することは可能ですが、ログオン拒否権限の使用は一般的に推奨されません。詳細については、Microsoftのドキュメントを参照してください。

ユーザー権限の構成

Delivery Controller™ のインストールにより、次の Windows サービスが作成されます。

- Citrix AD Identity Service (NT SERVICE\CitrixADIdentityService): VMのMicrosoft Active Directoryコンピューターアカウントを管理します。
- Citrix Analytics (NT SERVICE\CitrixAnalytics): サイト管理者が承認した場合、Citrixが使用するためのサイト構成の使用状況情報を収集します。その後、この情報をCitrixに送信し、製品の改善に役立てます。
- Citrix App Library (NT SERVICE\CitrixAppLibrary): AppDiskの管理とプロビジョニング、AppDNA統合、およびApp-Vの管理をサポートします。

- Citrix Broker Service (NT SERVICE\CitrixBrokerService): ユーザーが利用できる仮想デスクトップまたはアプリケーションを選択します。
- Citrix Configuration Logging Service (NT SERVICE\CitrixConfigurationLogging): 管理者がサイトに対して行ったすべての構成変更およびその他の状態変更を記録します。
- Citrix Configuration Service (NT SERVICE\CitrixConfigurationService): 共有構成のためのサイト全体のリポジトリ。
- Citrix Delegated Administration Service (NT SERVICE\CitrixDelegatedAdmin): 管理者に付与された権限を管理します。
- Citrix Environment Test Service (NT SERVICE\CitrixEnvTest): 他のDelivery Controllerサービスのセルフテストを管理します。
- Citrix Host Service (NT SERVICE\CitrixHostService): Citrix Virtual AppsまたはCitrix Virtual Desktops展開で使用されるハイパーバイザーインフラストラクチャに関する情報を保存し、コンソールがハイパーバイザープール内のリソースを列挙するために使用する機能も提供します。
- Citrix Machine Creation Services (NT SERVICE\CitrixMachineCreationService): デスクトップVMの作成をオーケストレーションします。
- Citrix Monitor Service (NT SERVICE\CitrixMonitor): Citrix Virtual AppsまたはCitrix Virtual Desktopsのメトリックを収集し、履歴情報を保存し、トラブルシューティングおよびレポートツール用のクエリインターフェイスを提供します。
- Citrix Storefront Service (NT SERVICE\ CitrixStorefront): StoreFront の管理をサポートします。(StoreFront コンポーネント自体の一部ではありません。)
- Citrix Storefront Privileged Administration Service (NT SERVICE\CitrixPrivilegedService): StoreFront の特権管理操作をサポートします。(StoreFront コンポーネント自体の一部ではありません。)
- Citrix Config Synchronizer Service (NT SERVICE\CitrixConfigSyncService): メインサイトデータベースからローカルホストキャッシュに構成データを伝播します。
- Citrix High Availability Service (NT SERVICE\CitrixHighAvailabilityService): メインサイトデータベースが利用できない場合に、ユーザーが利用できる仮想デスクトップまたはアプリケーションを選択します。

Delivery Controllerのインストールでは、以下のWindowsサービスも作成されます。これらは、他のCitrixコンポーネントと一緒にインストールされた場合にも作成されます。

- Citrix Diagnostic Facility COM Server (NT SERVICE\CdfSvc): Citrixサポートが使用するための診断情報の収集をサポートします。

- Citrix Telemetry Service (NT SERVICE\CitrixTelemetryService): Citrixによる分析のために診断情報を収集し、管理者が分析結果と推奨事項を表示してサイトの問題の診断に役立てられるようにします。

Delivery Controllerのインストールでは、以下のWindowsサービスも作成されます。これは現在使用されていません。有効になっている場合は、無効にしてください。

- Citrix リモート ブローカー プロバイダー (NT SERVICE\XaXdCloudProxy)

Delivery Controllerのインストールでは、以下のWindowsサービスも作成されます。これらは現在使用されていませんが、有効にする必要があります。無効にしないでください。

- Citrix オーケストレーション サービス (NT SERVICE\CitrixOrchestration)
- Citrix トラスト サービス (NT SERVICE\CitrixTrust)

Citrix Storefront Privileged Administration Service を除き、これらのサービスには「サービスとしてログオン」のログオン権限と、「プロセスのメモリクォータの調整」、「セキュリティ監査の生成」、「プロセスレベルトークンの置き換え」の特権が付与されます。これらのユーザー権限を変更する必要はありません。これらの特権は Delivery Controller では使用されず、自動的に無効になります。

サービス設定の構成

Citrix Storefront Privileged Administration サービスと Citrix Telemetry Service を除き、上記の ユーザー権限の構成 セクションに記載されている Delivery Controller の Windows サービスは、NETWORK SERVICE ID としてログオンするように構成されています。これらのサービス設定を変更しないでください。

Citrix Config Synchronizer Service は、Delivery Controller 上のローカル管理者グループに NETWORK SERVICE アカウントが属している必要があります。これにより、ローカルホストキャッシュが正しく機能します。

Citrix Storefront Privileged Administration サービスは、ローカルシステム (NT AUTHORITY\SYSTEM) としてログオンするように構成されています。これは、通常サービスでは利用できない Delivery Controller の StoreFront 操作 (Microsoft IIS サイトの作成を含む) に必要です。そのサービス設定を変更しないでください。

Citrix Telemetry Service は、サービス固有の ID としてログオンするように構成されています。

Citrix Telemetry Service は無効にできます。このサービスと、すでに無効になっているサービスを除き、これらの Delivery Controller Windows サービスの他のサービスを無効にしないでください。

レジストリ設定の構成

VDA ファイルシステムで 8.3 形式のファイル名とフォルダーの作成を有効にする必要はなくなりました。レジストリキー **NtfsDisable8dot3NameCreation** を構成して、8.3 形式のファイル名とフォルダーの作成を無効にできます。これは、**fsutil.exe behavior set disable8dot3** コマンドを使用しても構成できます。

展開シナリオのセキュリティへの影響

ユーザー環境には、組織によって管理されておらず、完全にユーザーの制御下にあるユーザーデバイス、または組織によって管理および運用されているユーザーデバイスのいずれかを含めることができます。これら2つの環境のセキュリティに関する考慮事項は、一般的に異なります。

管理対象ユーザーデバイス

管理対象ユーザーデバイスは管理制御下にあります。それらは、お客様自身の制御下にあるか、信頼する別の組織の制御下にあります。ユーザーデバイスを直接ユーザーに構成して提供することも、単一のデスクトップが全画面表示モードでのみ実行されるターミナルを提供することもできます。すべての管理対象ユーザーデバイスについて、上記の一般的なセキュリティのベストプラクティスに従ってください。このリリースには、ユーザーデバイスに必要なソフトウェアが最小限であるという利点があります。

管理対象のユーザーデバイスは、全画面専用モードまたはウィンドウモードで使用するように構成できます。

- 全画面専用モード: ユーザーは通常のWindowsログオン画面でログオンします。その後、同じユーザー資格情報を使用して、このリリースに自動的にログオンします。
- ユーザーはデスクトップをウィンドウで表示します: ユーザーはまずユーザーデバイスにログオンし、次にこのリリースに付属のWebサイトを通じてこのリリースにログオンします。

管理対象外のユーザーデバイス

信頼できる組織によって管理および運用されていないユーザーデバイスは、管理制御下にあるとは見なされません。たとえば、ユーザーが自分のデバイスを入手して構成することを許可する場合がありますが、ユーザーは上記の一般的なセキュリティのベストプラクティスに従わない可能性があります。このリリースには、管理対象外のユーザーデバイスにデスクトップを安全に配信できるという利点があります。これらのデバイスには、キーロガーや同様の入力攻撃を防ぐための基本的なウイルス対策保護が引き続き必要です。

データストレージに関する考慮事項

このリリースを使用する場合、ユーザーが物理的に制御しているユーザーデバイスにデータを保存することを防ぐことができます。ただし、ユーザーがデスクトップにデータを保存することの影響を考慮する必要があります。ユーザーがデスクトップにデータを保存することは良い習慣ではありません。データは、適切に保護できるファイルサーバー、データベースサーバー、またはその他のリポジトリに保持する必要があります。

デスクトップ環境は、プールされたデスクトップや専用デスクトップなど、さまざまな種類のデスクトップで構成される場合があります。ユーザーは、プールされたデスクトップなど、ユーザー間で共有されるデスクトップにデータを保存してはなりません。ユーザーが専用デスクトップにデータを保存する場合、そのデスクトップが後で他のユーザーに利用可能になった場合は、そのデータを削除する必要があります。

混在バージョン環境

一部のアップグレードでは、混在バージョン環境は避けられません。ベストプラクティスに従い、異なるバージョンのCitrixコンポーネントが共存する時間を最小限に抑えてください。混在バージョン環境では、たとえばセキュリティポリシーが均一に適用されない場合があります。

注：

これは他のソフトウェア製品にも共通しています。以前のバージョンのActive Directoryを使用すると、後のバージョンのWindowsではグループポリシーが部分的にしか適用されません。

以下のシナリオでは、特定の混在バージョンCitrix環境で発生する可能性のあるセキュリティ問題について説明します。Citrix Receiver 1.7を使用してXenAppおよびXenDesktop 7.6 Feature Pack 2のVDAを実行している仮想デスクトップに接続すると、サイトでポリシー設定 が有効になりますが、XenAppおよびXenDesktop 7.1を実行しているDelivery Controllerでは無効にできません。これは、製品の後のバージョンでリリースされたポリシー設定を認識しないためです。このポリシー設定により、ユーザーはファイルを仮想デスクトップにアップロードおよびダウンロードできるようになり、これがセキュリティ問題となります。この問題を回避するには、Delivery Controller（またはStudioのスタンドアロンインスタンス）をバージョン7.6 Feature Pack 2にアップグレードし、グループポリシーを使用してポリシー設定を無効にします。または、影響を受けるすべての仮想デスクトップでローカルポリシーを使用します。

Remote PC Accessのセキュリティに関する考慮事項

Remote PC Accessは、次のセキュリティ機能を実装しています。

- スマートカードの使用がサポートされています。
- リモートセッションが接続されると、オフィスPCのモニターは空白で表示されます。
- Remote PC Accessは、CTRL+ALT+DEL、USB対応スマートカード、生体認証デバイスを除くすべてのキーボードおよびマウス入力をリモートセッションにリダイレクトします。
- SmoothRoamingは、単一ユーザーのみがサポートされます。
- ユーザーがオフィスPCにリモートセッションを接続している場合、そのユーザーのみがオフィスPCへのローカルアクセスを再開できます。ローカルアクセスを再開するには、ユーザーはローカルPCでCtrl-Alt-Delを押し、リモートセッションで使用したのと同じ資格情報でログオンします。システムに適切なサードパーティの資格情報プロバイダー統合がある場合、ユーザーはスマートカードを挿入するか、生体認証を利用してローカルアクセスを再開することもできます。このデフォルトの動作は、グループポリシーオブジェクト（GPO）を介して高速ユーザー切り替えを有効にするか、レジストリを編集することで上書きできます。

> **注：**
>
> Citrixでは、VDA管理者権限を一般セッションユーザーに割り当てないことをお勧めします。

自動割り当て

デフォルトでは、Remote PC Accessは複数のユーザーをVDAに自動的に割り当てることをサポートしています。XenDesktop 5.6 Feature Pack 1では、管理者はRemotePCAccess.ps1 PowerShellスクリプトを使用してこの動作を上書きできました。このリリースでは、複数の自動リモートPC割り当てを許可または禁止するためにレジストリエントリを使用します。この設定はサイト全体に適用されます。

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

> 自動割り当てを単一ユーザーに制限するには：

サイト内の各Controllerで、次のレジストリエントリを設定します。

```
HKEY_LOCAL_MACHINE\Software\Citrix|DesktopServer

Name: AllowMultipleRemotePCAssignments

Type: REG_DWORD

Data: 0 = Disable multiple user assignment, 1 = (Default) Enable multiple
user assignment.
```

既存のユーザー割り当てがある場合は、SDKコマンドを使用してそれらを削除し、VDAが単一の自動割り当ての対象となるようにします。

- VDAから割り当てられているすべてのユーザーを削除します: `$machine.AssociatedUserNames | %{ Remove-BrokerUser-Name $_ -Machine $machine`
- デリバリーグループからVDAを削除します: `$machine | Remove-BrokerMachine -DesktopGroup $desktopGroup`

物理的なオフィスPCを再起動します。

XML信頼

XML信頼設定は、以下を使用する展開に適用されます。

- オンプレミスのStoreFront。
- パスワードを必要としないサブスクライバー（ユーザー）認証技術。このような技術の例としては、ドメインパススルー、スマートカード、SAML、Veridiumソリューションなどがあります。

XML信頼設定を有効にすると、ユーザーは正常に認証され、アプリケーションを起動できるようになります。Delivery Controllerは、StoreFrontから送信された資格情報を信頼します。この設定は、Delivery ControllerとStoreFront間の通信が保護されている場合（ファイアウォール、IPsec、またはその他のセキュリティ推奨事項を使用している場合）にのみ有効にしてください。

この設定はデフォルトで無効になっています。

XML信頼設定の確認、有効化、または無効化には、Citrix Virtual Apps and Desktops PowerShell SDKを使用します。

- XML信頼設定の現在の値を確認するには、`Get-BrokerSite` を実行し、`TrustRequestsSentToTheXMLServicePort` の値を調べます。
- XML信頼を有効にするには、`Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true` を実行します。
- XML信頼を無効にするには、`Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $false` を実行します。

シトリックス Virtual Apps and Desktops™ と シトリックス ゲートウェイ の統合

StoreFront™ サーバーは、公開されたリソースとデータへのアクセスを管理するために展開および構成されます。リモートアクセスの場合、StoreFront の前に Citrix Gateway を追加することをお勧めします。

> **注：**

> Citrix Virtual Apps and Desktops と Citrix Gateway を統合する方法の詳細な構成手順については、StoreFront のドキュメントを参照してください。

> The following diagram illustrates an example of a simplified Citrix deployment that includes Citrix Gateway. Citrix Gateway communicates with StoreFront to protect apps and data delivered by Citrix Virtual Apps and Desktops. The user devices run Citrix Workspace™ app to create a secure connection and access their apps, desktops, and files.

Citrix Gateway を含む簡素化された Citrix 展開(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/sample-deployment-overview.png)

ユーザーは Citrix Gateway を使用してログオンし、認証します。Citrix Gateway は DMZ に展開され、保護されています。2 要素認証が構成されています。ユーザー資格情報に基づいて、ユーザーには関連するリソースとアプリケーションが提供されます。アプリケーションとデータは適切なサーバー上にあります（図には示されていません）。セキュリティ上機密性の高いアプリケーションとデータには、個別のサーバーが使用されます。

委任管理

委任管理モデルは、ロールベースおよびオブジェクトベースの制御を使用して、組織が管理アクティビティを委任する方法に合わせる柔軟性を提供します。委任管理は、あらゆる規模の展開に対応し、展開の複雑さが増すにつれて、より詳細な権限の粒度を構成できるようにします。委任管理では、管理者、ロール、スコープという3つの概念を使用します。

- **管理者:** 管理者は、Active Directoryアカウントによって識別される個人またはグループを表します。各管理者は、1つ以上の役割とスコープのペアに関連付けられています。
- **ロール:** ロールは職務を表し、それに関連付けられた定義済みの権限を持ちます。たとえば、Delivery Group Administratorロールには、「Delivery Groupの作成」や「Delivery Groupからのデスクトップの削除」などの権限があります。管理者はサイトに対して複数のロールを持つことができるため、ある人物がDelivery Group AdministratorとMachine Catalog Administratorの両方になることができます。ロールは組み込みまたはカスタムにすることができます。

  組み込みロールは次のとおりです。

ロール	権限
フル管理者	すべてのタスクと操作を実行できます。フル管理者 (Full Administrator) は常に「すべて」のスコープと組み合わされます。
読み取り専用管理者	グローバル情報に加えて、指定されたスコープ内のすべてのオブジェクトを表示できますが、何も変更することはできません。たとえば、Scope=Londonの読み取り専用管理者 (Read Only Administrator) は、すべてのグローバルオブジェクト（構成ログなど）と、ロンドンにスコープが設定されたオブジェクト（ロンドンデリバリーグループなど）を表示できます。ただし、その管理者はニューヨークのスコープ内のオブジェクトを表示できません（ロンドンとニューヨークのスコープが重複しないと仮定した場合）。
ヘルプデスク管理者	デリバリーグループを表示し、それらのグループに関連付けられたセッションとマシンを管理できます。監視対象のデリバリーグループの「マシンカタログ」とホスト情報を表示できます。また、それらのデリバリーグ

ロール	権限
	ループ内のマシンのセッション管理およびマシン電源管理操作を実行できます。
マシンカタログ管理者	マシンカタログを作成および管理し、それらにマシンをプロビジョニングできます。仮想化インフラストラクチャ、Provisioning Services、および物理マシンからマシンカタログを構築できます。このロールはベースイメージを管理し、ソフトウェアをインストールできますが、アプリケーションやデスクトップをユーザーに割り当てることはできません。
デリバリーグループ管理者	アプリケーション、デスクトップ、およびマシンを配信できます。また、関連するセッションを管理できます。ポリシーや電源管理設定などのアプリケーションおよびデスクトップ構成も管理できます。
ホスト管理者	ホスト接続とその関連リソース設定を管理できます。ユーザーにマシン、アプリケーション、またはデスクトップを配信することはできません。

特定の製品エディションでは、組織の要件に合わせてカスタムロールを作成し、より詳細な権限を委任できます。カスタムロールを使用すると、コンソールでのアクションまたはタスクの粒度で権限を割り当てることができます。

- **スコープ:** スコープはオブジェクトの集合を表します。スコープは、組織に関連する方法でオブジェクトをグループ化するために使用されます（たとえば、営業チームが使用するデリバリーグループのセットなど）。オブジェクトは複数のスコープに属することができます。オブジェクトには1つ以上のスコープがラベル付けされていると考えることができます。組み込みスコープは1つだけあり、「すべて」という名前で、すべてのオブジェクトを含みます。フル管理者ロールは常に「すべて」スコープとペアになっています。

例

XYZ社は、部門（経理、営業、倉庫）とデスクトップオペレーティングシステム（Windows 7またはWindows 8）に基づいてアプリケーションとデスクトップを管理することにしました。管理者

は5つのスコープを作成し、各デリバリーグループに2つのスコープをラベル付けしました。1つは使用される部門用、もう1つは使用されるオペレーティングシステム用です。

次の管理者が作成されました。

管理者	ロール	スコープ
domain/fred	フル管理者	すべて (フル管理者ロールは常に「すべて」スコープを持ちます)
domain/rob	読み取り専用管理者	すべて
domain/heidi	読み取り専用管理者、ヘルプデスク管理者	すべての営業
domain/warehouseadmin	ヘルプデスク管理者	倉庫
domain/peter	デリバリーグループ管理者、マシンカタログ管理者	Win7

- Fredはフル管理者であり、システム内のすべてのオブジェクトを表示、編集、削除できます。
- Robはサイト内のすべてのオブジェクトを表示できますが、それらを編集または削除することはできません。
- Heidiはすべてのオブジェクトを表示でき、Salesスコープ内のデリバリーグループに対してヘルプデスクタスクを実行できます。これにより、彼女はそれらのグループに関連付けられたセッションとマシンを管理できます。ただし、マシンの追加や削除など、デリバリーグループに変更を加えることはできません。
- warehouseadmin Active Directoryセキュリティグループのメンバーである人は誰でも、Warehouseスコープ内のマシンを表示し、ヘルプデスクタスクを実行できます。
- PeterはWindows 7のスペシャリストであり、すべてのWindows 7マシンカタログを管理でき、どの部署スコープに属していても、Windows 7アプリケーション、デスクトップ、およびマシンを提供できます。管理者は、PeterをWin7スコープのフル管理者にすることを検討しました。しかし、フル管理者は「サイト」や「管理者」など、スコープが設定されていないすべてのオブジェクトに対しても完全な権限を持つため、彼女はこれに反対しました。

委任管理の使用方法

一般的に、管理者の数と権限の粒度は、展開の規模と複雑さによって異なります。

- 小規模な展開や概念実証の展開では、1人または数人の管理者がすべての作業を行います。委任はありません。この場合、各管理者を、すべてのスコープを持つ組み込みのフル管理者ロールで作成します。
- マシン、アプリケーション、デスクトップが多い大規模な展開では、より多くの委任が必要です。複数の管理者が、より具体的な機能的責任（ロール）を持つ場合があります。たとえば、2人がフル管理者で、他の管理者がヘルプデスク管理者である場合があります。また、管理者がマシンカタログなど、特定のオブジェクトグループ（スコープ）のみを管理する場合もあります。この場合、新しいスコープを作成し、組み込みロールのいずれかと適切なスコープを持つ管理者を作成します。
- さらに大規模な展開では、より多くの（またはより具体的な）スコープと、型にはまらないロールを持つ異なる管理者が必要になる場合があります。この場合、より多くのスコープを編集または作成し、カスタムロールを作成し、既存および新規のスコープに加えて、組み込みまたはカスタムロールを持つ各管理者を作成します。

柔軟性と構成の容易さのために、管理者を作成するときにスコープを作成できます。マシンカタログまたは接続を作成または編集するときにスコープを指定することもできます。

管理者の作成と管理

ローカル管理者としてサイトを作成すると、ユーザーアカウントは自動的に、すべてのオブジェクトに対する完全な権限を持つフル管理者になります。サイトが作成された後、ローカル管理者には特別な権限はありません。

フル管理者ロールには常にすべてのスコープが割り当てられます。これは変更できません。

既定では、管理者は有効になっています。管理者を今作成しても、その人が後で管理業務を開始しない場合は、管理者を無効にする必要があるかもしれません。既存の有効な管理者については、オブジェクト/スコープを再編成している間に複数人を無効にし、更新された構成で稼働準備が整ったときに再度有効にしたい場合があります。有効なフル管理者がいなくなる場合、フル管理者を無効にすることはできません。管理者の作成、コピー、または編集時に、有効/無効チェックボックスが利用可能です。

管理者をコピー、編集、または削除する際にロール/スコープのペアを削除すると、その管理者に対するロールとスコープ間の関連付けのみが削除されます。ロールまたはスコープ自体は削除されません。また、そのロール/スコープのペアで構成されている他の管理者には影響しません。

管理者を管理するには、Studioナビゲーションペインで **>** をクリックし、上部中央ペインで タブをクリックします。

- **管理者の作成:** ペインで をクリックします。ユーザーアカウント名を入力または参照し、スコープを選択または作成し、役割を選択します。新しい管理者はデフォルトで有効になっています。これは変更できます。
- **管理者のコピー:** 中央ペインで管理者を選択し、 ペインで をクリックします。ユーザーアカウント名を入力または参照します。役割/スコープのペアを選択して編集または削除したり、新しいペアを追加したりできます。新しい管理者はデフォルトで有効になっています。これは変更できます。
- **管理者の編集:** 中央ペインで管理者を選択し、 ペインで をクリックします。役割/スコープのペアを編集または削除したり、新しいペアを追加したりできます。
- **管理者の削除:** 中央ペインで管理者を選択し、 ペインで をクリックします。有効なフル管理者がいなくなる場合、フル管理者を削除することはできません。

上部のペインには、作成した管理者が表示されます。管理者を選択すると、下部のペインにその詳細が表示されます。**警告**列は、管理者に関連付けられているロールとスコープのペアに、使用できないロールまたはスコープが含まれているかどうかを示します。関連付けられているロールとスコープのペアに、使用できないロールまたはスコープが含まれている場合、次の警告メッセージが表示されます。

- 関連付けられているロールまたはスコープが使用できません
    - 管理者から役割とスコープのペアを削除します。

> **重要:**

> 警告メッセージは、関連付けられているロールとスコープのペアに、使用できないロール、スコープ、またはその両方が含まれている場合にのみ表示されます。

> 管理者からロールとスコープのペアを削除するには、次のいずれかの手順を実行します。

- ロールとスコープのペアを削除します。
    a. ペインで をクリックします。
    b. ウィンドウで、役割とスコープのペアを選択し、 をクリックします。
    c. **OK**をクリックして終了します。
- 管理者を削除します。
    a. ペインで をクリックします。

b. ウィンドウで をクリックします。

役割の作成と管理

管理者が役割を作成または編集する場合、自分自身が持っている権限のみを有効にできます。これにより、管理者が現在持っている権限よりも多くの権限を持つ役割を作成し、それを自分自身に割り当てたり（または既に割り当てられている役割を編集したりする）ことを防ぎます。

役割名には最大64個のUnicode文字を含めることができます。ただし、バックスラッシュ、スラッシュ、セミコロン、コロン、ポンド記号、コンマ、アスタリスク、疑問符、等号、左右の矢印、パイプ、左右の角括弧、左右の丸括弧、引用符、アポストロフィは含めることができません。説明には最大256個のUnicode文字を含めることができます。

組み込みの役割を編集または削除することはできません。カスタム役割が管理者によって使用されている場合、その役割を削除することはできません。

> **注：**
>
> 特定の製品エディションのみがカスタムロールをサポートしています。カスタムロールをサポートするエディションのみが、 ペインに関連エントリを持っています。

> 役割を管理するには、Studioナビゲーションペインで**構成 > 管理者**をクリックし、上部中央ペインで**役割**タブをクリックします。

- **役割の詳細を表示:** 中央ペインで役割を選択します。中央ペインの下部には、役割のオブジェクトタイプと関連する権限が一覧表示されます。下部ペインのタブをクリックすると、現在この役割を持つ管理者の一覧が表示されます。
- **カスタム役割を作成:** ペインで**新しい役割の作成**をクリックします。名前と説明を入力します。オブジェクトタイプと権限を選択します。
- **役割をコピー:** 中央ペインで役割を選択し、ペインで**役割のコピー**をクリックします。必要に応じて、名前、説明、オブジェクトタイプ、および権限を変更します。
- **カスタム役割を編集:** 中央ペインで役割を選択し、ペインで**役割の編集**をクリックします。必要に応じて、名前、説明、オブジェクトタイプ、および権限を変更します。
- **カスタム役割を削除:** 中央ペインで役割を選択し、ペインで**役割の削除**をクリックします。プロンプトが表示されたら、削除を確認します。

スコープの作成と管理

サイトを作成するときに利用できるスコープは「すべて」スコープのみであり、これは削除できません。

次の手順でスコープを作成できます。管理者を作成するときにもスコープを作成できます。各管理者は、少なくとも1つのロールとスコープのペアに関連付けられている必要があります。デスクトップ、マシンカタログ、アプリケーション、またはホストを作成または編集するときに、それらを既存のスコープに追加できます。スコープに追加しない場合、それらは「すべて」スコープの一部として残ります。

サイトの作成はスコープ化できません。また、委任管理オブジェクト（スコープと役割）もスコープ化できません。ただし、スコープ化できないオブジェクトは「すべて」のスコープに含まれます。（完全な管理者は常に「すべて」のスコープを持ちます。）マシン、電源操作、デスクトップ、およびセッションは直接スコープ化されません。管理者は、関連するマシンカタログまたはデリバリーグループを通じて、これらのオブジェクトに対する権限を割り当てることができます。

スコープ名には最大64個のUnicode文字を含めることができます。スコープ名には、バックスラッシュ、スラッシュ、セミコロン、コロン、ポンド記号、コンマ、アスタリスク、疑問符、等号、左矢印、右矢印、パイプ、左右の角かっこ、左右の丸かっこ、引用符、またはアポストロフィを含めることはできません。説明には最大256個のUnicode文字を含めることができます。

スコープをコピーまたは編集する際は、スコープからオブジェクトを削除すると、それらのオブジェクトに管理者がアクセスできなくなる可能性があることに留意してください。編集されたスコープが1つ以上のロールとペアになっている場合、スコープの更新によってどのロール/スコープのペアも使用できなくならないようにしてください。

スコープを管理するには、Studioナビゲーションペインで**構成 > 管理者**をクリックし、上部中央ペインで**スコープ**タブをクリックします。

- **スコープを作成:** ペインで**新しいスコープの作成**をクリックします。名前と説明を入力します。特定のタイプのすべてのオブジェクト（例：デリバリーグループ）を含めるには、オブジェクトタイプを選択します。特定のオブジェクトを含めるには、タイプを展開し、個々のオブジェクト（例：営業チームが使用するデリバリーグループ）を選択します。
- **スコープをコピー:** 中央ペインでスコープを選択し、ペインで**スコープのコピー**をクリックします。名前と説明を入力します。必要に応じて、オブジェクトタイプとオブジェクトを変更します。
- **スコープを編集:** 中央ペインでスコープを選択し、ペインで**スコープの編集**をクリックします。必要に応じて、名前、説明、オブジェクトタイプ、およびオブジェクトを変更します。

- **スコープを削除:** 中央ペインでスコープを選択し、ペインで**スコープの削除**をクリックします。プロンプトが表示されたら、削除を確認します。

レポートの作成

委任管理レポートには、次の2種類を作成できます。

- 管理者に関連付けられた役割/スコープのペア、および各オブジェクトタイプ（例：デリバリーグループとマシンカタログ）の個別の権限を一覧表示するHTMLレポート。このレポートはStudioから生成します。

  このレポートを作成するには、Studioナビゲーションペインで**構成 > 管理者**をクリックします。中央ペインで管理者を選択し、ペインで**レポートの作成**をクリックします。

  管理者の作成、コピー、または編集時に、このレポートを要求することもできます。

- すべての組み込み役割とカスタム役割を権限にマッピングするHTMLまたはCSVレポート。このレポートは、OutputPermissionMapping.ps1という名前のPowerShellスクリプトを実行して生成します。

  このスクリプトを実行するには、フル管理者、読み取り専用管理者、または役割を読み取る権限を持つカスタム管理者である必要があります。スクリプトは、Program Files\Citrix\DelegatedAdmin\SnapIn\Citrix.DelegatedAdmin.Admin.V1\Scriptsにあります。

  構文：

  `OutputPermissionMapping.ps1 [-Help] [-Csv] [-Path string] [-AdminAddress string] [-Show] [CommonParameters]`

パラメーター	説明
`-Help`	スクリプトのヘルプを表示します。
`-Csv`	CSV出力を指定します。デフォルト = HTML
`-Path string`	出力の書き込み先。デフォルト = stdout
`-AdminAddress string`	接続先のDelivery Controller™のIPアドレスまたはホスト名。デフォルト = localhost
`-Show`	(`-Path` パラメーターも指定されている場合にのみ有効) 出力をファイルに書き込む

パラメーター	説明
	と、`-Show` によって出力がWebブラウザーなどの適切なプログラムで開かれます。
共通パラメーター	`Verbose`、`Debug`、`ErrorAction`、`ErrorVariable`、`WarningAction`、`WarningVariable`、`OutBuffer`、および `OutVariable`。詳細については、Microsoftのドキュメントを参照してください。

次の例では、HTMLテーブルをRoles.htmlという名前のファイルに書き込み、そのテーブルをWebブラウザーで開きます。

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"

-Path Roles.html –Show
```

次の例では、CSVテーブルをRoles.csvという名前のファイルに書き込みます。テーブルは表示されません。

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"

–CSV -Path Roles.csv
```

Windowsのコマンドプロンプトから、上記の例のコマンドは次のとおりです。

```
powershell -command "& '%ProgramFiles%\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1'

-CSV -Path Roles.csv"
```

セキュリティキーの管理

注:

- この機能は、StoreFront™ 1912 LTSR CU2以降と組み合わせて使用する必要があります。
- Secure XML機能は、Citrix ADCおよびCitrix Gatewayリリース12.1以降でのみサポートされています。

この機能を使用すると、承認されたStoreFrontおよびCitrix Gatewayマシンのみがcitrix Delivery Controllerと通信できるようになります。この機能を有効にすると、キーを含まないすべての要求はブロックされます。この機能を使用して、内部ネットワークから発生する攻撃から保護するための追加のセキュリティ層を追加します。

この機能を使用するための一般的なワークフローは次のとおりです。

1. Studioで機能設定を表示できるようにします。
2. サイトの設定を構成します。
3. StoreFrontで設定を構成します。
4. Citrix ADCで設定を構成します。

Studioで機能設定を表示できるようにする

デフォルトでは、セキュリティキーの設定はStudioから非表示になっています。Studioでそれらを表示できるようにするには、PowerShell SDKを次のように使用します。

1. Citrix Virtual Apps and Desktops™ PowerShell SDKを実行します。
2. コマンドウィンドウで、次のコマンドを実行します。
   - `Add-PSSnapIn Citrix*`。このコマンドはCitrixスナップインを追加します。
   - `Set-ConfigSiteMetadata -Name "Citrix_DesktopStudio_SecurityKeyManagementEnabled" -Value "True"`

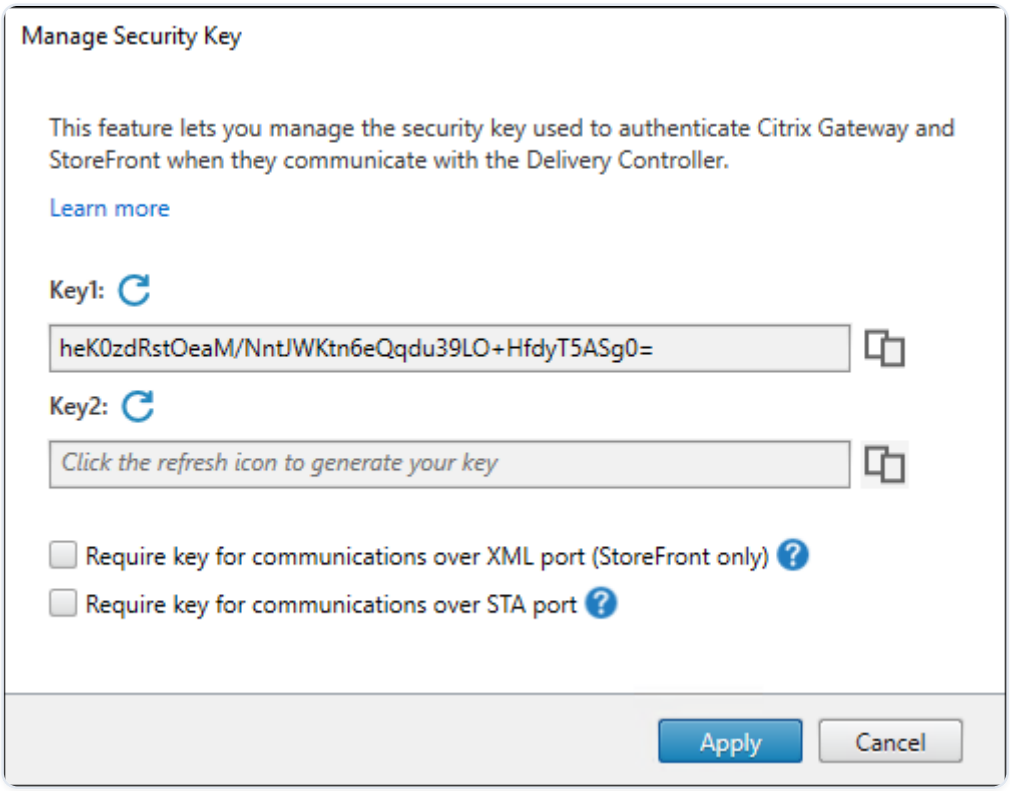
PowerShell SDKの詳細については、SDKとAPIを参照してください。

サイトの設定を構成する

StudioまたはPowerShellを使用して、サイトのセキュリティキー設定を構成できます。

Studioコンソールを使用する

1. **Studio > 設定 > セキュリティキーの管理**に移動し、**編集**をクリックします。**セキュリティキーの管理**ウィンドウが表示されます。



重要:

- 使用できるキーは2つあります。XMLポートおよびSTAポートを介した通信には、同じキーまたは異なるキーを使用できます。一度に1つのキーのみを使用することをお勧めします。未使用のキーは、キーローテーションにのみ使用されます。
- 使用中のキーを更新するために更新アイコンをクリックしないでください。クリックすると、サービスが中断されます。

2. 更新アイコンをクリックして、新しいキーを生成します。
3. キーが必要な場所を選択します。

- **XMLポートを介した通信にキーを要求する（StoreFrontのみ）**。選択した場合、XMLポートを介した通信を認証するためにキーが必要になります。StoreFrontはこのポートを介してCitrix Cloudと通信します。XMLポートの変更については、Knowledge Centerの記事CTX127945を参照してください。

- **STAポートを介した通信にキーを要求する。**選択した場合、STAポートを介した通信を認証するためにキーが必要になります。Citrix GatewayとStoreFrontはこのポートを介してCitrix Cloudと通信します。STAポートの変更については、Knowledge Centerの記事CTX101988を参照してください。

4. 変更を適用してウィンドウを終了するには、**保存**をクリックします。

PowerShell を使用する

以下は、Studio操作に相当するPowerShellの手順です。

1. Citrix Virtual Apps and Desktops Remote PowerShell SDK を実行します。
2. コマンドウィンドウで、次のコマンドを実行します。
   - `Add-PSSnapIn Citrix*`
3. キーを生成し、Key1を設定するには、次のコマンドを実行します。
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey1 <the key you generated>`
4. 以下のコマンドを実行してキーを生成し、Key2 をセットアップします。
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey2 <the key you generated>`
5. 通信の認証でキーの使用を有効にするには、以下のコマンドのいずれか、または両方を実行します。
   - XMLポート経由の通信を認証するには:
     - `Set-BrokerSite -RequireXmlServiceKeyForNFuse $true`
   - STAポート経由の通信を認証するには:
     - `Set-BrokerSite -RequireXmlServiceKeyForSta $true`

ガイダンスと構文については、PowerShellコマンドのヘルプを参照してください。

StoreFront で設定を構成する

サイトの構成が完了したら、PowerShellを使用してStoreFrontで関連する設定を構成する必要があります。

StoreFront サーバーで、以下の PowerShell コマンドを実行します。

XMLポートを介した通信用のキーを構成するには、コマンドを使用します。例:

```
$store = Get-STFStoreService -VirtualPath [Path to store]

$farm = Get-STFStoreFarm -StoreService $store -FarmName [Resource feed
name]

Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true
-XMLValidationSecret [secret]
```

次のパラメータに適切な値を入力します。

- `Path to store`
- `Resource feed name`
- `secret`

STAポート経由の通信用にキーを構成するには、`New-STFSecureTicketAuthority`および`Set-STFRoamingGateway`コマンドを使用します。例:

```
$gateway = Get-STFRoamingGateway -Name [Gateway name]

$sta1 = New-STFSecureTicketAuthority -StaUrl [STA1 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

$sta2 = New-STFSecureTicketAuthority -StaUrl [STA2 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

Set-STFRoamingGateway -Gateway $gateway -SecureTicketAuthorityObjs
$sta1,$sta2
```

次のパラメータに適切な値を入力します。

- `Gateway name`
- `STA URL`
- `Secret`

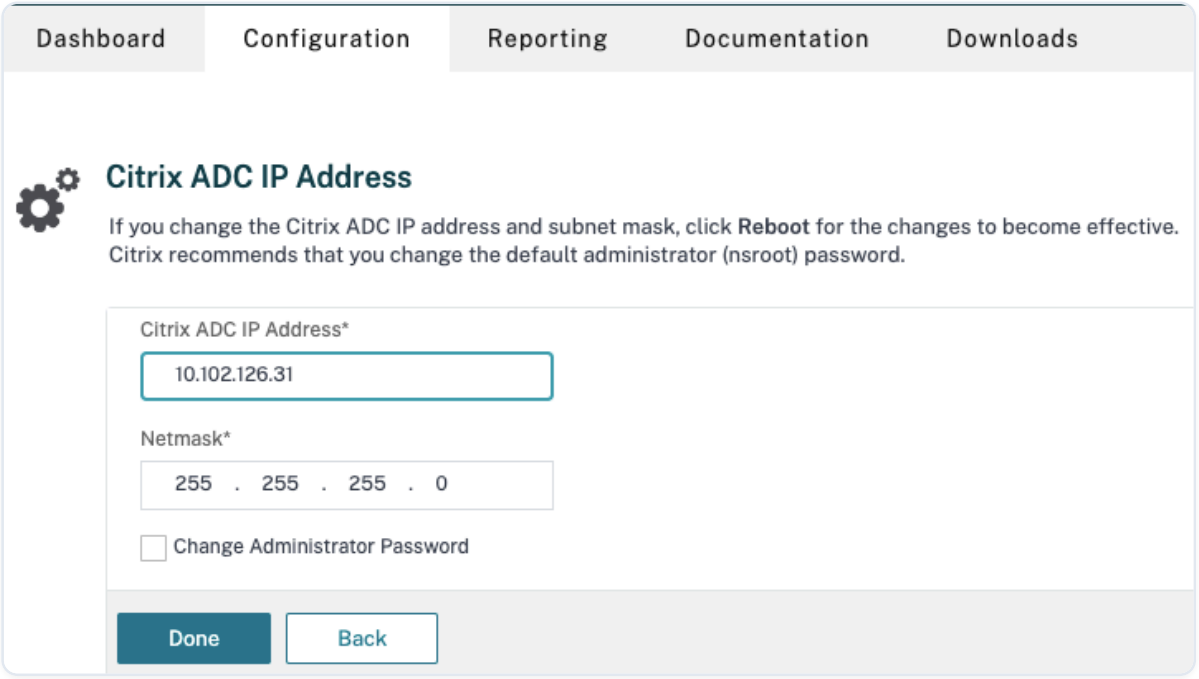
ガイダンスと構文については、PowerShellコマンドのヘルプを参照してください。

Citrix ADCでの設定

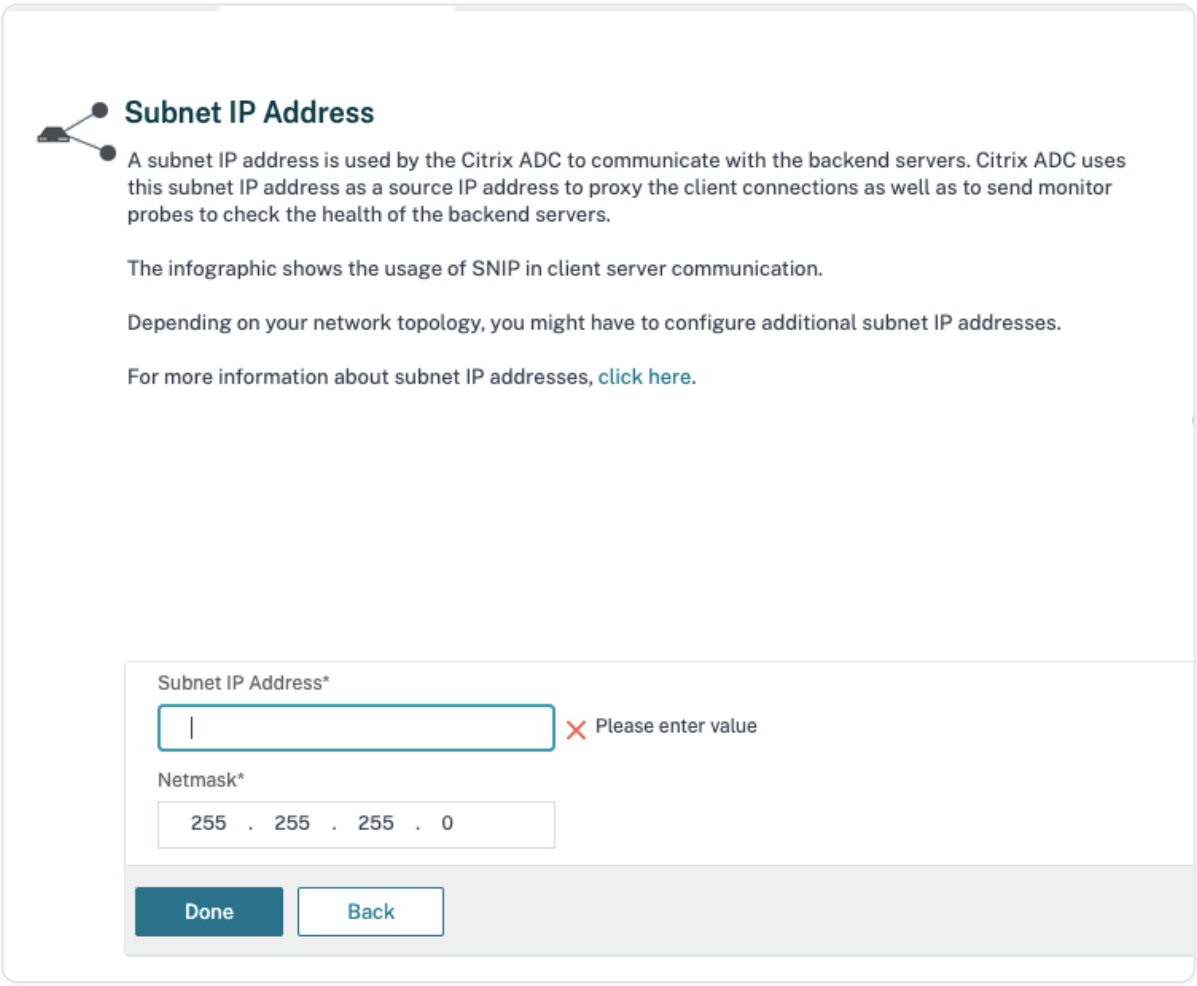
注:

Citrix ADCをゲートウェイとして使用しない限り、Citrix ADCでこの機能を構成する必要はありません。Citrix ADCを使用する場合は、以下の手順に従ってください。

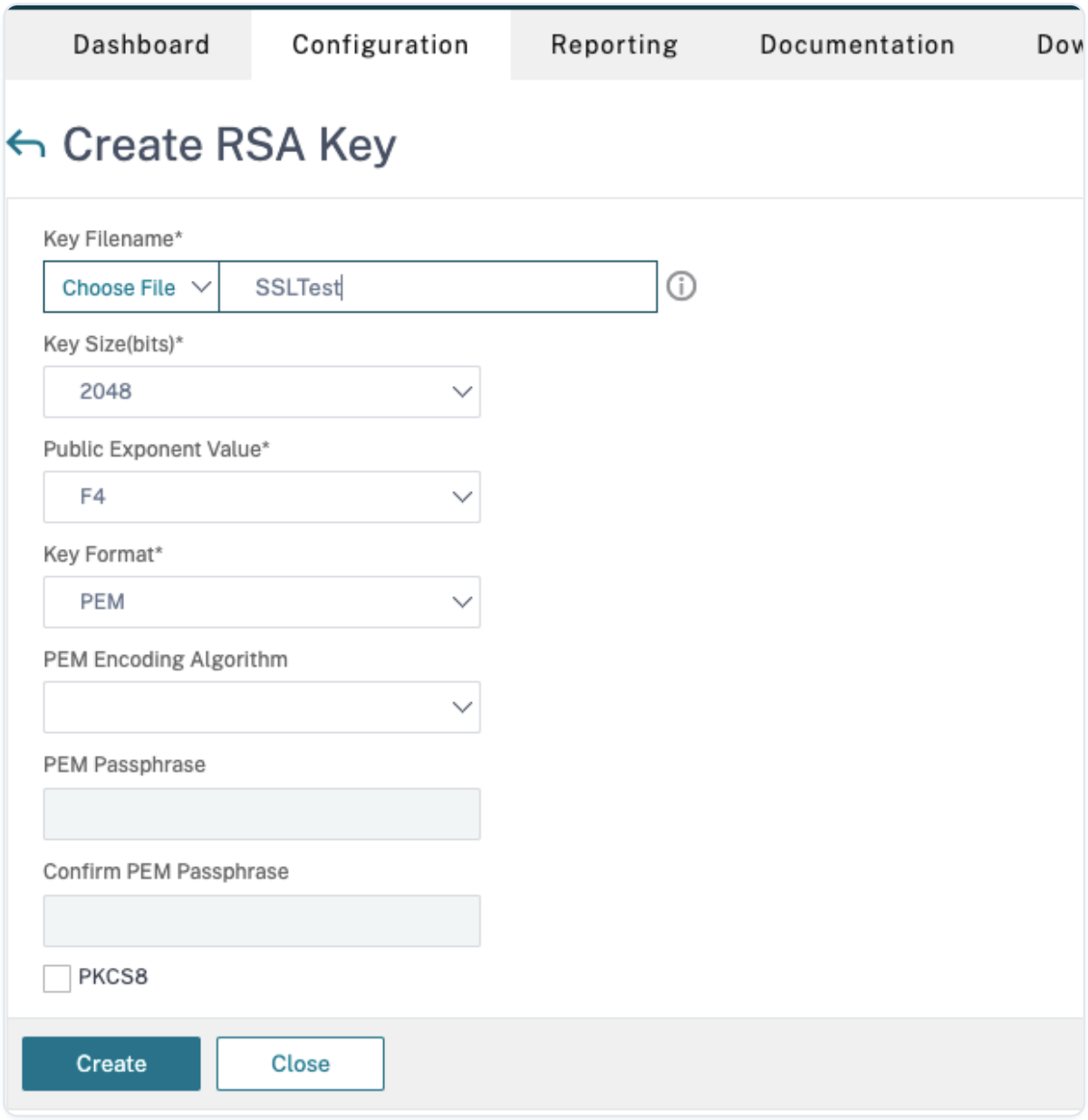
1. 次の前提条件となる構成がすでに設定されていることを確認してください。
   - 次のCitrix ADC関連のIPアドレスが構成されています。
     - Citrix ADCコンソールにアクセスするための Citrix ADC管理IP (NSIP) アドレス。詳細については、「NSIPアドレスの構成」を参照してください。



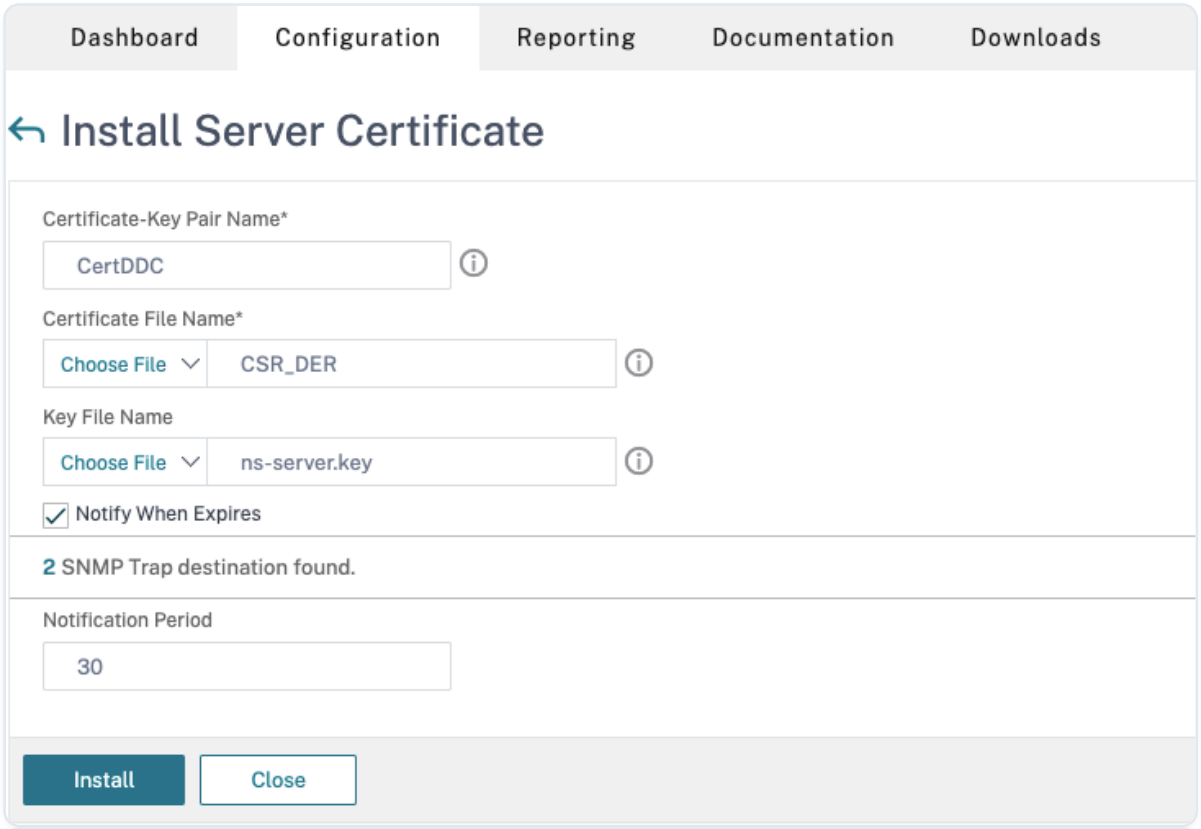
     - Citrix ADCアプライアンスとバックエンドサーバー間の通信を有効にするためのサブネットIP（SNIP）アドレス。詳細については、「サブネットIPアドレスの構成」を参照してください。
     - セッション起動のためにADCアプライアンスにログインするためのCitrix Gateway仮想IPアドレスとロードバランサー仮想IPアドレス。詳細については、「仮想サーバーの作成」を参照してください。

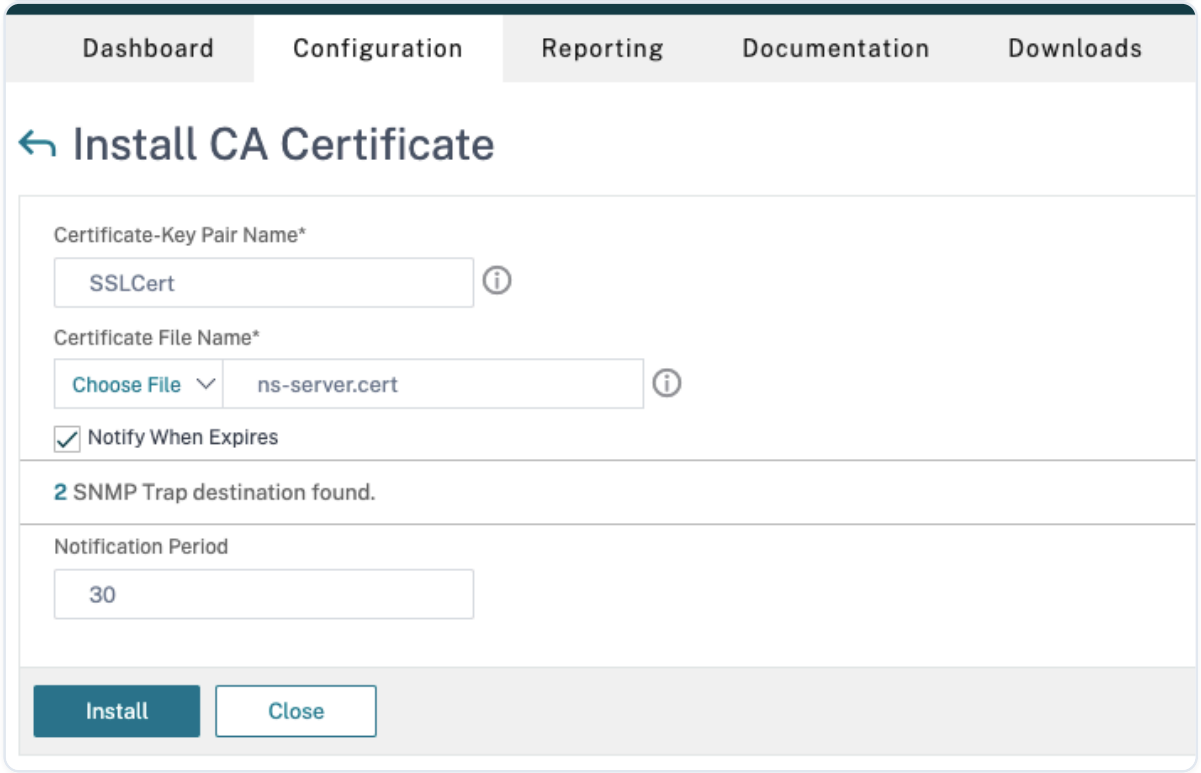


- Citrix ADCアプライアンスで必要なモードと機能が有効になっています。
  - モードを有効にするには、Citrix ADC GUIで**System > Settings > Configure Mode**に移動します。
  - 機能を有効にするには、Citrix ADC GUIで**System > Settings > Configure Basic Features**に移動します。
- 証明書関連の構成が完了しています。
  - 証明書署名要求（CSR）が作成されます。詳細については、「証明書の作成」を参照してください。

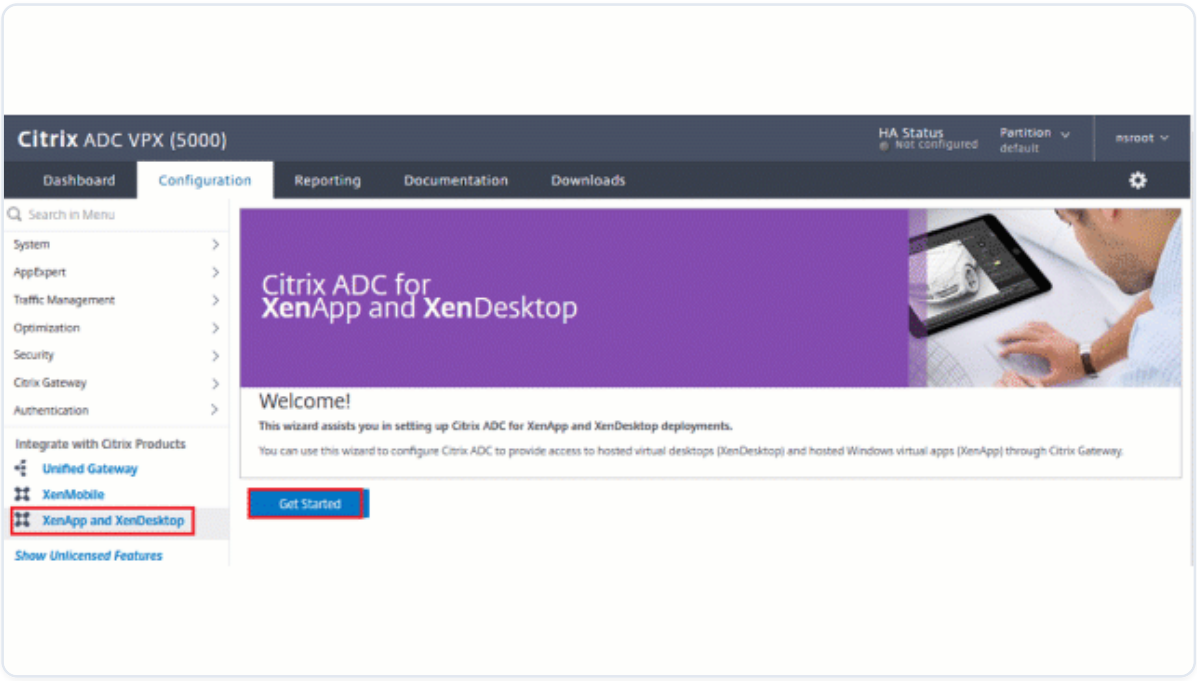


- サーバー証明書、CA証明書、およびルート証明書がインストールされます。詳細については、「インストール、リンク、および更新」を参照してください。





- Citrix Virtual Desktops用にCitrix Gatewayが作成されました。仮想サーバーがオンラインであることを確認するには、**Test STA Connectivity**ボタンをクリックして接続をテストします。詳細については、「Setting up Citrix ADC for Citrix Virtual Apps and Desktops」を参照してください。



2. リライトアクションを追加します。詳細については、「リライトアクションの構成」を参照してください。

   a. **AppExpert > Rewrite > Actions**に移動します。

   b. 新しい書き換えアクションを追加するには、**追加**をクリックします。アクションの名前は「set Type to INSERT_HTTP_HEADER」にすることができます。

   書き換えアクションの追加(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/adc-appexpert-rewrite-action.png)

   a. **タイプ**で、**INSERT_HTTP_HEADER**を選択します。

   b. **ヘッダー名**に「X-Citrix-XmlServiceKey」と入力します。

   c. **式**に、引用符付きで`<XmlServiceKey1 value>`を追加します。XmlServiceKey1 の値は、Desktop Delivery Controller™ の構成からコピーできます。

   XMLサービスキーの値(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/xml-service-key-values.png)

3. 書き換えポリシーを追加します。詳細については、「書き換えポリシーの構成」を参照してください。

   a. **AppExpert > Rewrite > Policies**に移動します。

   b. 新しいポリシーを追加するには、**追加**をクリックします。

   書き換えポリシーの追加(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/adc-appexpert-rewrite-policy.png)

a. **アクション**で、前の手順で作成したアクションを選択します。

b. **式**に「HTTP.REQ.IS_VALID」を追加します。

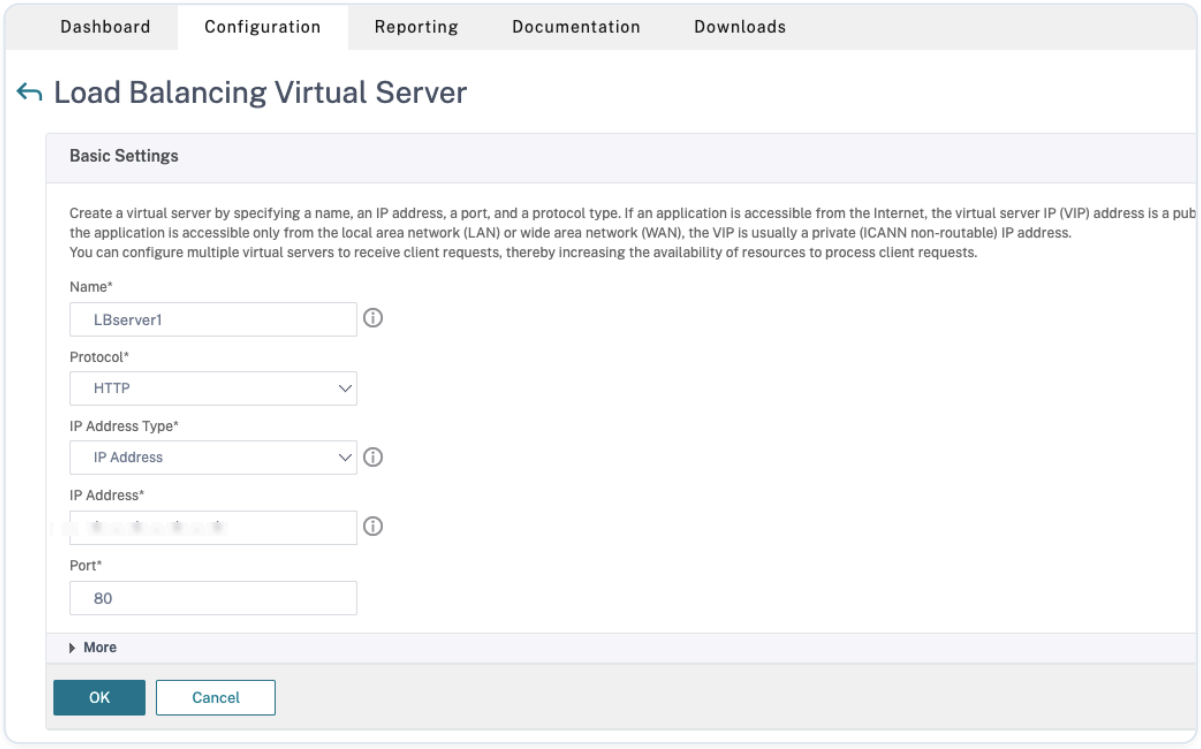
c. **OK**をクリックします。

4. 負荷分散を設定します。STAサーバーごとに1つの負荷分散仮想サーバーを構成する必要があります。構成しない場合、セッションの起動に失敗します。

   詳細については、基本的な負荷分散のセットアップを参照してください。

   a. 負荷分散仮想サーバーを作成します。

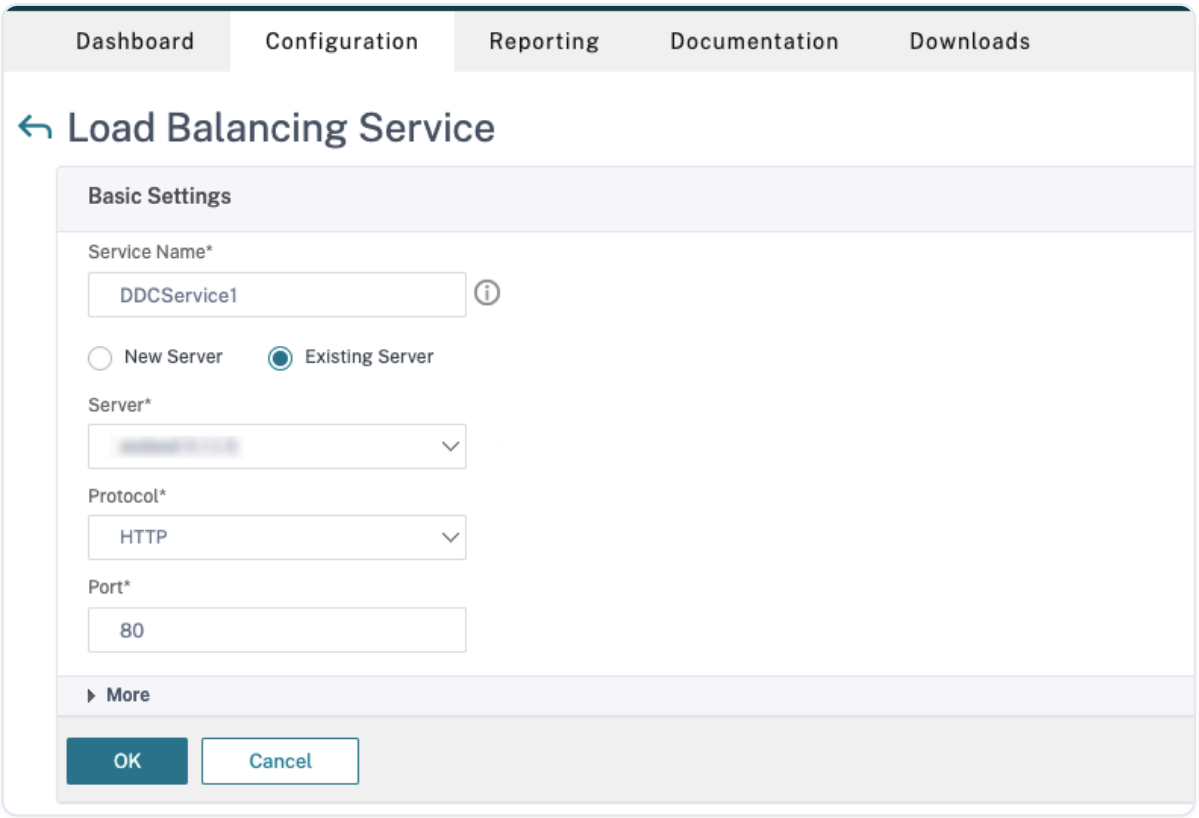
      - 「**トラフィック管理 > 負荷分散 > サーバー**」に移動します。
      - **Virtual Servers**ページで、**Add**をクリックします。



      - **Protocol**で、**HTTP**を選択します。
      - 負荷分散仮想IPアドレスを追加し、**Port**で**80**を選択します。
      - **OK**をクリックします。

   b. 負荷分散サービスを作成します。

      - 「**トラフィック管理 > 負荷分散 > サービス**」に移動します。



- **Existing Server**で、前のステップで作成した仮想サーバーを選択します。
- **Protocol**で**HTTP**を選択し、**Port**で**80**を選択します。
- **OK**をクリックし、その後**Done**をクリックします。

c. サービスを仮想サーバーにバインドします。

- 以前に作成した仮想サーバーを選択し、**編集**をクリックします。
- **サービスとサービスグループ**で、**ロードバランシング仮想サーバーサービスバインディングなし**をクリックします。

仮想サーバーにサービスをバインド(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/adc-bind-service-to-lbvserver.png)

- **Service Binding**で、以前に作成したサービスを選択します。
- **バインド**をクリックします。

d. 以前に作成した書き換えポリシーを仮想サーバーにバインドします。

- 以前に作成した仮想サーバーを選択し、**編集**をクリックします。
- **詳細設定**で、**ポリシー**をクリックし、次に**ポリシー**セクションで**+**をクリックします。

書き換えポリシーをバインド(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/adc-bind-rewrite-policy.png)

- **ポリシーの選択**で**書き換え**を選択し、**タイプの選択**で**要求**を選択します。
- **続行**をクリックします。
- **ポリシーの選択**で、以前に作成した書き換えポリシーを選択します。
- **バインド**をクリックします。
- **完了**をクリックします。

e. 必要に応じて、仮想サーバーの永続性を設定します。

- 以前に作成した仮想サーバーを選択し、**編集**をクリックします。
- **詳細設定**で、**永続性**をクリックします。

永続性の設定(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/adc-lb-vserver-persistence.png)

- 永続性の種類として**その他**を選択します。
- 仮想サーバーによって選択されたサービスのIPアドレス（宛先IPアドレス）に基づいて永続性セッションを作成するには、**DESTIP**を選択します。
- 「**IPv4ネットマスク**」で、DDCと同じネットワークマスクを追加します。
- **OK**をクリックします。

f. 他の仮想サーバーについても、これらの手順を繰り返します。

Citrix ADCアプライアンスがCitrix Virtual Desktops™で既に構成されている場合の構成の変更点

Citrix ADCアプライアンスをCitrix Virtual Desktopsで既に構成している場合、Secure XML機能を使用するには、以下の構成変更を行う必要があります。

- セッション起動前に、ゲートウェイの**セキュリティチケット機関URL**を、負荷分散仮想サーバーのFQDNを使用するように変更します。
- `TrustRequestsSentToTheXmlServicePort`パラメーターがFalseに設定されていることを確認します。デフォルトでは、`TrustRequestsSentToTheXmlServicePort`パラメーターはFalseに設定されています。ただし、顧客がCitrix Virtual Desktops用にCitrix ADCを既に構成している場合、`TrustRequestsSentToTheXmlServicePort`はTrueに設定されます。

1. Citrix ADC GUIで、**構成 > Citrix製品との統合**に移動し、**XenApp and XenDesktop®**をクリックします。
2. ゲートウェイインスタンスを選択し、編集アイコンをクリックします。

   既存のゲートウェイ構成を編集(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/edit-gateway-instance.png)
3. StoreFrontペインで、編集アイコンをクリックします。

   StoreFrontの詳細を編集(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/edit-storefront-details.png)
4. **Secure Ticket Authority URL**を追加します。

   - Secure XML機能が有効になっている場合、STA URLはロードバランシングサービスのURLである必要があります。
   - Secure XML機能が無効になっている場合、STA URLはSTAのURL（DDCのアドレス）である必要があり、DDC上のTrustRequestsSentToTheXmlServicePortパラメーターはTrueに設定する必要があります。

   STA URLを追加(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/add-sta-urls.png)

スマートカード

スマートカードおよび同等のテクノロジーは、この記事で説明されているガイドライン内でサポートされています。Citrix Virtual AppsまたはCitrix Virtual Desktops™でスマートカードを使用するには、次の手順を実行します。

- スマートカードの使用に関する組織のセキュリティポリシーを理解します。これらのポリシーには、たとえば、スマートカードの発行方法やユーザーがスマートカードを保護する方法が記載されている場合があります。これらのポリシーの一部は、Citrix Virtual Apps™またはCitrix Virtual Desktops環境で再評価する必要がある場合があります。
- スマートカードで使用するユーザーデバイスの種類、オペレーティングシステム、および公開アプリケーションを決定します。
- スマートカードテクノロジーと、選択したスマートカードベンダーのハードウェアおよびソフトウェアに精通してください。
- 分散環境でデジタル証明書を展開する方法を理解します。

> **注：**

(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/secure/smart-cards.html#fast-smart-card)ではスマートカードの登録はサポートされていません。スマートカードの登録は、高速スマートカードが無効になっている場合に機能する可能性がありますが、スマートカードとミドルウェアの種類によって異なります。Citrix Virtual Apps and Desktopsとの統合および仮想セッションを介したスマートカード登録のサポートについては、スマートカードおよびミドルウェアベンダーにお問い合わせください。

スマートカードの種類

企業向けスマートカードと消費者向けスマートカードは、同じ寸法、電気コネクタを持ち、同じスマートカードリーダーに適合します。

企業向けスマートカードにはデジタル証明書が含まれています。これらのスマートカードはWindowsログオンをサポートし、ドキュメントやメールのデジタル署名および暗号化のためのアプリケーションでも使用できます。Citrix Virtual Apps and Desktops™はこれらの用途をサポートしています。

消費者向けスマートカードにはデジタル証明書は含まれていません。共有シークレットが含まれています。これらのスマートカードは、支払い（チップアンドサインまたはチップアンドPINクレジットカードなど）をサポートできます。Windowsログオンや一般的なWindowsアプリケーションはサポートしていません。これらのスマートカードを使用するには、特殊なWindowsアプリケーションと適切なソフトウェアインフラストラクチャ（たとえば、決済カードネットワークへの接続を含む）が必要です。これらの特殊なアプリケーションをCitrix Virtual AppsまたはCitrix Virtual Desktopsでサポートする方法については、Citrixの担当者にお問い合わせください。

企業向けスマートカードには、同様の方法で使用できる互換性のある同等品があります。

- スマートカードと同等のUSBトークンは、USBポートに直接接続します。これらのUSBトークンは通常、USBフラッシュドライブと同じサイズですが、携帯電話で使用されるSIMカードと同じくらい小さい場合もあります。これらはスマートカードとUSBスマートカードリーダーの組み合わせとして表示されます。
- Windows Trusted Platform Module (TPM)を使用する仮想スマートカードは、スマートカードとして表示されます。これらの仮想スマートカードは、Citrix Workspace app（最小バージョンCitrix Receiver 4.3）を使用するWindows 8およびWindows 10でサポートされています。
    - XenApp and XenDesktop 7.6 FP3より前のバージョンのCitrix Virtual Apps and Desktops（旧XenApp and XenDesktop）は、仮想スマートカードをサポートしていません。
    - 仮想スマートカードの詳細については、仮想スマートカードの概要を参照してください。

> **注記:** 「仮想スマートカード」という用語は、ユーザーコンピューターに保存されているデジタル証明書を指すためにも使用されます。これらのデジタル証明書は、厳密にはスマートカードと同等ではありません。

Citrix Virtual Apps and Desktopsのスマートカードサポートは、Microsoft Personal Computer/Smart Card (PC/SC) 標準仕様に基づいています。最低要件として、スマートカードおよびスマートカードデバイスは、基盤となるWindowsオペレーティングシステムによってサポートされ、対象となるWindowsオペレーティングシステムを実行するコンピューターで使用するために、Microsoft Windows Hardware Quality Labs (WHQL) によって承認されている必要があります。ハードウェアのPC/SC準拠に関する追加情報については、Microsoftのドキュメントを参照してください。他の種類のユーザーデバイスもPS/SC標準に準拠している場合があります。詳細については、Citrix Readyプログラムを参照してください。

通常、各ベンダーのスマートカードまたは同等のものには、個別のデバイスドライバーが必要です。ただし、スマートカードがNIST個人識別検証（PIV）標準などの標準に準拠している場合、さまざまなスマートカードに単一のデバイスドライバーを使用できる可能性があります。デバイスドライバーは、ユーザーデバイスとVirtual Delivery Agent (VDA) の両方にインストールする必要があります。デバイスドライバーは、Citrixパートナーから入手できるスマートカードミドルウェアパッケージの一部として提供されることが多く、スマートカードミドルウェアパッケージは高度な機能を提供します。デバイスドライバーは、暗号化サービスプロバイダー（CSP）、キーストレージプロバイダー（KSP）、またはミニドライバーとも呼ばれる場合があります。

Windowsシステム用の以下のスマートカードとミドルウェアの組み合わせは、Citrixによってそのタイプの代表的な例としてテストされています。ただし、他のスマートカードとミドルウェアも使用できます。Citrix互換のスマートカードとミドルウェアに関する詳細については、`<http://www.citrix.com/ready>`を参照してください。

ミドルウェア	対応カード
Gemalto .NETカード用ミニドライバー	ジェムアルト ドットネット v2以降

他の種類のデバイスでのスマートカードの使用に関する情報については、そのデバイスのCitrix Workspace™アプリのドキュメントを参照してください。

リモートPCアクセス

スマートカードは、Windows 10、Windows 8、またはWindows 7を実行している物理的なオフィスPCへのリモートアクセスでのみサポートされています。

Remote PC Accessでテストされたスマートカードは次のとおりです。

ミドルウェア	対応カード
Gemalto .NETミニドライバー	ジェムアルト ドットネット v2以降

高速スマートカード

高速スマートカードは、既存のHDX PC/SCベースのスマートカードリダイレクトを改善したものです。高遅延のWAN環境でスマートカードを使用する場合にパフォーマンスが向上します。遅延が大きい場合、パフォーマンスの向上は大幅なものになります（例えば、Windowsの高速スマートカードログオンでは15秒、PC/SCベースのスマートカードリダイレクトでは1分以上）。

高速スマートカードは、現在サポートされているWindows VDAを搭載したホストマシンでデフォルトで有効になっています。ホスト側で高速スマートカードを無効にするには（例えば診断目的で）、'Disable Cryptographic Redirection' レジストリ設定をゼロ以外の値に設定します。

```
HKLM\SOFTWARE\Citrix\SmartCard

CryptographicRedirectionDisable (DWORD)
```

クライアント側で高速スマートカードを有効にするには、関連するStoreFrontサイトの*default.ica*ファイルにSmartCardCryptographicRedirection ICAパラメーターを含めます。

```
[WFClient]

SmartCardCryptographicRedirection=On
```

さらに、クライアント側では、以下のレジストリ設定を使用して、高速スマートカードを強制的に有効または無効にできます（例えば診断目的で）。

- HKLM\SOFTWARE\Citrix\ICA Client\SmartCard\ForceEnableCryptographicRedirection (ゼロ以外のDWORDとして)

または

- HKLM\SOFTWARE\Citrix\ICA Client\SmartCard\ForceDisableCryptographicRedirection (ゼロ以外のDWORDとして)

クライアントマシンが64ビットの場合、32ビットレジストリハイブを指定する必要があります（`WOW6432Node`を使用）。

制限事項:

- Windows版Citrix Workspaceアプリのみが高速スマートカードをサポートしています。default.icaファイルで高速スマートカードを設定した場合、Windows版ではないCitrix Workspaceアプリは、既存のPC/SCリダイレクトを依然として使用します。
- 高速スマートカードがサポートする唯一のダブルホップシナリオは、両方のホップで高速スマートカードが有効になっているICA® > ICAです。高速スマートカードはICA > RDPダブルホップシナリオをサポートしていないため、これらのシナリオは機能しません。
- 高速スマートカードはCryptography Next Generationをサポートしていません。したがって、高速スマートカードは楕円曲線暗号 (ECC) スマートカードをサポートしていません。
- 高速スマートカードは読み取り専用のキーコンテナ操作のみをサポートしています。
- 高速スマートカードはスマートカードPINの変更をサポートしていません。

VDAバージョン2203およびWindows版Citrix Workspaceアプリバージョン2202（またはそれ以降）以降、高速スマートカードはCryptography Next Generation (CNG) と互換性があります。さらに、楕円曲線暗号 (ECC) スマートカードは、ECDSAとECDHの両方で、P-256、P-384、P-521ビットの以下の曲線に対応しています。

VDAバージョン2203以降、高速スマートカードは、同じユーザーのログオンセッション内のアプリケーション間でスマートカードPINをキャッシュする機能を追加します。例えば、**セッションPINキャッシュ**が有効になっており、エンドユーザーが以前にOutlookにスマートカードPINを提供している場合、その後Wordを使用してドキュメントに署名すると、Wordはすでにキャッシュされているスマートカードpin（Outlookに送信されたもの）を使用します。**セッションPINキャッシュ**は、ユーザーがスマートカードPINを入力する回数を減らすことで、ユーザーエクスペリエンスを向上させます。さらに、スマートカードがVDAへのログオンに使用される場合、Windowsスマートカードログオンpinをオプションで**セッションPINキャッシュ**に保存できます。これにより、ユーザーエクスペリエンスがさらに向上します。

セッションPINキャッシュはデフォルトで無効になっています。VDA上の以下のレジストリ設定で有効化および制御できます。

HKLM\SOFTWARE\Citrix\SmartCard: で:

- `EnablePinSessionCache` をDWORDとして (有効にするにはゼロ以外)
- `EnableLogonPinSessionCache` をDWORDとして (有効にするにはゼロ以外)
- `PinSessionCacheEntryStaleTimeout` をDWORDとして (エントリが古くなるまでの秒数、デフォルトは1時間)

スマートカードリーダーの種類

スマートカードリーダーは、ユーザーデバイスに内蔵されている場合や、ユーザーデバイスに別途接続されている場合 (通常はUSBまたはBluetooth経由) があります。USB Chip/Smart Card Interface Devices (CCID) 仕様に準拠した接触型カードリーダーがサポートされています。これらには、ユーザーがスマートカードを挿入するスロットまたはスワイプ部分があります。Deutsche Kreditwirtschaft (DK) 規格では、接触型カードリーダーの4つのクラスが定義されています。

- クラス1スマートカードリーダーは最も一般的で、通常はスロットを備えています。クラス1スマートカードリーダーは、通常、オペレーティングシステムに付属の標準CCIDデバイスドライバーでサポートされます。
- クラス2スマートカードリーダーには、ユーザーデバイスからアクセスできないセキュアキーパッドも搭載されています。クラス2スマートカードリーダーは、セキュアキーパッドが統合されたキーボードに組み込まれている場合があります。クラス2スマートカードリーダーについては、Citrixの担当者にお問い合わせください。セキュアキーパッド機能を有効にするには、リーダー固有のデバイスドライバーが必要になる場合があります。
- クラス3スマートカードリーダーには、セキュアディスプレイも搭載されています。クラス3スマートカードリーダーはサポートされていません。
- クラス4スマートカードリーダーには、セキュアトランザクションモジュールも搭載されています。クラス4スマートカードリーダーはサポートされていません。

> **注：**
>
> スマートカードリーダーのクラスは、USBデバイスクラスとは関係ありません。

> スマートカードリーダーは、対応するデバイスドライバーをインストールしてユーザーデバイスにインストールする必要があります。

サポートされているスマートカードリーダーについては、使用しているCitrix Workspaceアプリのドキュメントを参照してください。Citrix Workspaceアプリのドキュメントでは、サポートされているバージョンは、スマートカードに関する記事またはシステム要件に関する記事に記載されています。

ユーザーエクスペリエンス

スマートカードのサポートは、Citrix Virtual Apps and Desktopsに統合されており、特定のICA/HDXスマートカード仮想チャネルを使用します。これはデフォルトで有効になっています。

重要: スマートカードリーダーに汎用USBリダイレクトを使用しないでください。これはスマートカードリーダーではデフォルトで無効になっており、有効にしてもサポートされません。

同じユーザーデバイス上で複数のスマートカードと複数のリーダーを使用できますが、パススルー認証が使用されている場合は、ユーザーが仮想デスクトップまたはアプリケーションを起動するときに、スマートカードを1枚だけ挿入する必要があります。アプリケーション内でスマートカードを使用する場合（たとえば、デジタル署名や暗号化機能の場合）、スマートカードの挿入やPINの入力に関する追加のプロンプトが表示されることがあります。これは、複数のスマートカードが同時に挿入されている場合に発生する可能性があります。

- スマートカードがすでにリーダーに挿入されているにもかかわらず、スマートカードの挿入を促すプロンプトが表示された場合は、ユーザーはキャンセルを選択する必要があります。
- PINの入力を求められた場合は、ユーザーはPINを再度入力する必要があります。

カード管理システムまたはベンダーユーティリティを使用してPINをリセットできます。

> **重要:**
>
> Citrix Virtual AppsまたはCitrix Virtual Desktopsセッション内で、Microsoft Remote Desktop Connectionアプリケーションとスマートカードを併用することはサポートされていません。これは「ダブルホップ」使用と呼ばれることがあります。

スマートカードを展開する前に

- スマートカードリーダー用のデバイスドライバーを入手し、ユーザーデバイスにインストールします。多くのスマートカードリーダーは、Microsoftが提供するCCIDデバイスドライバーを使用できます。
- スマートカードベンダーからデバイスドライバーと暗号化サービスプロバイダー（CSP）ソフトウェアを入手し、ユーザーデバイスと仮想デスクトップの両方にインストールします。ドライバーとCSPソフトウェアはCitrix Virtual Apps and Desktopsと互換性がある必要があります。互換性についてはベンダーのドキュメントを確認してください。ミニドライバーモデルをサポートおよび使用するスマートカードを使用する仮想デスクトップの場合、スマートカードミニドライバーは自動的にダウンロードされますが、http://catalog.update.microsoft.comまたはベンダーから入手することもできます。また、PKCS#11ミドルウェアが必要な場合は、カードベンダーから入手してください。
- 重要: Citrixは、Citrixソフトウェアをインストールする前に、物理コンピューターにドライバーとCSPソフトウェアをインストールしてテストすることを推奨します。

- Windows 10でInternet Explorerを使用してスマートカードを使用するユーザーのために、Citrix Receiver™ for WebのURLを信頼済みサイトリストに追加します。Windows 10では、信頼済みサイトの場合、Internet Explorerはデフォルトで保護モードで実行されません。
- 公開鍵インフラストラクチャ（PKI）が適切に構成されていることを確認してください。これには、Active Directory環境向けに証明書とアカウントのマッピングが正しく構成されており、ユーザー証明書の検証が正常に実行できることを確認することが含まれます。
- 展開が、Citrix WorkspaceアプリやStoreFrontなど、スマートカードで使用される他のCitrixコンポーネントのシステム要件を満たしていることを確認してください。
- サイト内の以下のサーバーへのアクセスを確保してください。
    - スマートカード上のログオン証明書に関連付けられているユーザーアカウントのActive Directoryドメインコントローラー
    - デリバリーコントローラー™
    - シトリックス ストアフロント
    - シトリックス ゲートウェイ/シトリックス アクセス ゲートウェイ 10.x
    - VDA
    - (Remote PC Access の場合、オプション): Microsoft Exchange Server

スマートカードの使用を有効にする

ステップ 1. カード発行ポリシーに従って、ユーザーにスマートカードを発行します。

ステップ 2. (オプション) ユーザーがRemote PC Access を利用できるようにスマートカードを設定します。

ステップ 3. スマートカードのリモート処理のために、Delivery Controller と StoreFront (まだインストールされていない場合) をインストールして構成します。

ステップ 4. スマートカードの使用のためにStoreFront を有効にします。詳細については、StoreFront ドキュメントの「スマートカード認証の構成」を参照してください。

ステップ 5. スマートカードの使用のためにCitrix Gateway/Access Gateway を有効にします。詳細については、NetScaler ドキュメントの「認証と承認の構成」および「Web Interface を使用したスマートカードアクセスの構成」を参照してください。

ステップ 6. スマートカードの使用のためにVDA を有効にします。

- VDA に必要なアプリケーションと更新プログラムがあることを確認します。
- ミドルウェアをインストールします。

- スマートカードのリモート処理を設定し、ユーザーデバイス上のCitrix Workspace アプリと仮想デスクトップセッション間のスマートカードデータの通信を有効にします。

ステップ 7. ユーザーデバイス (ドメイン参加済みまたは非ドメイン参加済みマシンを含む) でスマートカードの使用を有効にします。詳細については、StoreFront ドキュメントの「スマートカード認証の構成」を参照してください。

- 証明機関のルート証明書と発行証明機関の証明書をデバイスのキーストアにインポートします。
- ベンダーのスマートカードミドルウェアをインストールします。
- Windows 用Citrix Workspace アプリをインストールして構成します。その際、グループポリシー管理コンソールを使用してicaclient.adm をインポートし、スマートカード認証を有効にしてください。

ステップ 8. 展開をテストします。テストユーザーのスマートカードを使用して仮想デスクトップを起動し、展開が正しく構成されていることを確認します。可能なすべてのアクセスメカニズム（たとえば、Internet Explorer および Citrix Workspace アプリを介したデスクトップへのアクセス）をテストします。

スマートカードリーダーの挿入回数を追跡する

スマートカードのリモート処理を使用すると、SCardGetStatusChange 関数を使用して、スマートカードがリーダーに挿入または取り外された回数を追跡できます。この関数は、監視するリーダーごとに 1 つの SCARD_READERSTATE データ構造の配列を更新します。各 SCARD_READERSTATE の dwEventState フィールドのハイワード（16 ビット）には、リーダーのカウントが含まれています。詳細については、Microsoft の記事 SCardGetStatusChangeA function および SCARD_READERSTATEA structure を参照してください。

リーダー挿入回数レポート設定は、デフォルトで無効になっています。追跡を有効にするには、次のレジストリキーを追加します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard

名前: EnableReaderInsertCountReporting

種類: DWORD

値: ゼロ以外の任意の値

セッションが切断されると、カウントはゼロにリセットされます。

リーダー挿入回数レポートは、サードパーティのスマートカードミドルウェアと互換性があります。

スマートカードの展開

この製品バージョンおよびこのバージョンを含む混在環境では、以下の種類のスマートカード展開がサポートされています。その他の構成も動作する可能性がありますが、サポートされていません。

タイプ	STOREFRONT™ 接続
ローカルのドメイン参加済みコンピューター	直接接続
ドメイン参加済みコンピューターからのリモートアクセス	Citrix Gateway 経由で接続
ドメインに参加していないコンピューター	直接接続
ドメインに参加していないコンピューターからのリモートアクセス	Citrix Gateway 経由で接続
ドメインに参加していないコンピューターおよびシンクライアントがDesktop Applianceサイトにアクセス	Desktop Applianceサイト経由で接続
XenApp® Services URL を介してStoreFrontにアクセスするドメイン参加済みコンピューターおよびシンクライアント	XenApp Services URL 経由で接続

展開タイプは、スマートカードリーダーが接続されているユーザーデバイスの特性によって定義されます。

- デバイスがドメイン参加済みか、非ドメイン参加済みか。
- デバイスがStoreFrontにどのように接続されているか。
- 仮想デスクトップとアプリケーションを表示するためにどのソフトウェアが使用されているか。

さらに、Microsoft WordやMicrosoft Excelなどのスマートカード対応アプリケーションをこれらの展開で使用できます。これらのアプリケーションを使用すると、ユーザーはドキュメントにデジタル署名したり、暗号化したりできます。

バイモーダル認証

これらの展開のそれぞれにおいて可能な場合、Receiverはスマートカードの使用とユーザー名およびパスワードの入力の選択肢をユーザーに提供することで、バイモーダル認証をサポートします。これは、スマートカードが使用できない場合（たとえば、ユーザーが自宅に忘れた場合やログオン証明書が期限切れになった場合）に役立ちます。

非ドメイン参加デバイスのユーザーはReceiver for Windowsに直接ログオンするため、ユーザーが明示的な認証にフォールバックできるようにすることができます。バイモーダル認証を構成すると、ユーザーは最初にスマートカードとPINを使用してログオンするように求められますが、スマートカードに問題が発生した場合は明示的な認証を選択するオプションがあります。

Citrix Gatewayを展開する場合、ユーザーはデバイスにログオンし、Receiver for WindowsによってCitrix Gatewayへの認証を求められます。これは、ドメイン参加済みデバイスと非ドメイン参加済みデバイスの両方に適用されます。ユーザーは、スマートカードとPIN、または明示的な資格情報を使用してCitrix Gatewayにログオンできます。これにより、Citrix Gatewayログオンに対してバイモーダル認証をユーザーに提供できます。Citrix GatewayからStoreFrontへのパススルー認証を構成し、スマートカードユーザーの資格情報検証をCitrix Gatewayに委任することで、ユーザーはStoreFrontにサイレント認証されます。

複数のActive Directoryフォレストに関する考慮事項

Citrix環境では、スマートカードは単一のフォレスト内でサポートされます。フォレストをまたがるスマートカードログオンには、すべてのユーザーアカウントへの直接的な双方向フォレスト信頼が必要です。スマートカードを含むより複雑なマルチフォレスト展開（つまり、信頼が一方通行であるか、異なるタイプである場合）はサポートされていません。

リモートデスクトップを含むCitrix環境でスマートカードを使用できます。この機能は、ローカル（スマートカードが接続されているユーザーデバイス上）またはリモート（ユーザーデバイスが接続するリモートデスクトップ上）にインストールできます。

スマートカード取り外しポリシー

製品に設定されているスマートカード取り外しポリシーは、セッション中にリーダーからスマートカードを取り外した場合に何が起こるかを決定します。スマートカード取り外しポリシーは、Windowsオペレーティングシステムを介して構成および処理されます。

ポリシー設定	デスクトップの動作
何もしない	何もしない。

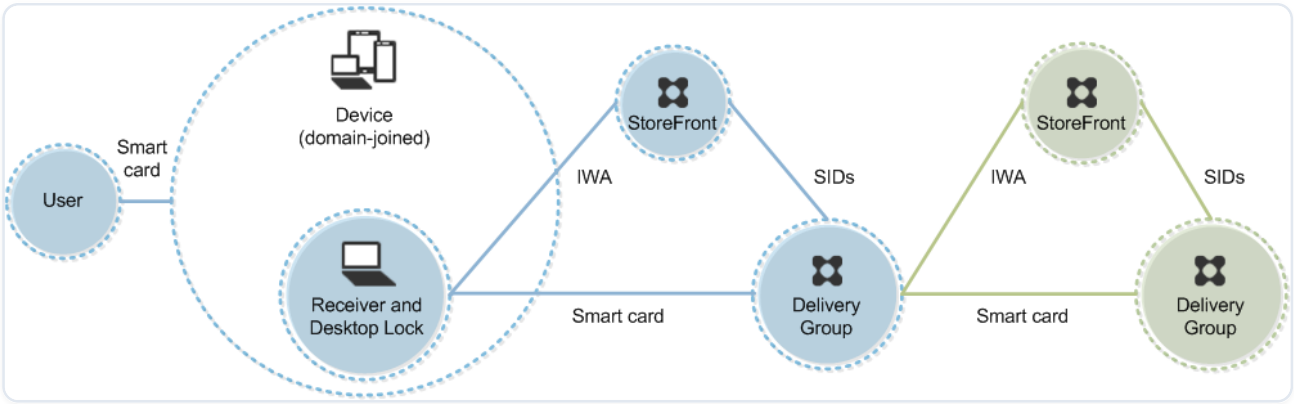
ポリシー設定	デスクトップの動作
ワークステーションをロックする	デスクトップセッションが切断され、仮想デスクトップがロックされます。
強制ログオフ	ユーザーは強制的にログオフされます。ネットワーク接続が失われ、この設定が有効になっている場合、セッションがログオフされ、ユーザーはデータを失う可能性があります。
リモートターミナルサービスセッションの場合に切断する	セッションが切断され、仮想デスクトップがロックされます。

証明書失効チェック

証明書失効チェックが有効になっていて、ユーザーが無効な証明書を含むスマートカードをカードリーダーに挿入した場合、ユーザーは認証できず、その証明書に関連するデスクトップまたはアプリケーションにアクセスできません。たとえば、無効な証明書がメールの復号化に使用されている場合、メールは暗号化されたままになります。認証に使用されるものなど、カード上の他の証明書がまだ有効な場合、それらの機能はアクティブなままです。

展開例：ドメイン参加済みコンピューター

この展開では、Desktop Viewer を実行し、StoreFront に直接接続するドメイン参加済みユーザーデバイスを使用します。



ユーザーはスマートカードとPINを使用してデバイスにログオンします。Receiver は、統合Windows認証 (IWA) を使用してユーザーをStoreFrontサーバーに認証します。StoreFront は、ユーザーセキュリティ識別子 (SID) を Citrix Virtual Apps または Citrix Virtual Desktops に渡します。ユーザーが仮想デスクトップまたはアプリケーションを起動すると、Receiver でシングルサインオン機能が構成されているため、PIN の再入力を求められることはありません。

この展開は、2番目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiver は、2番目のStoreFrontサーバーに認証します。この2番目の接続には、任意の認証方法を使用できます。最初のホップで示された構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例: ドメイン参加済みコンピューターからのリモートアクセス

この展開では、Desktop Viewer を実行し、Citrix Gateway/Access Gateway を介して StoreFront に接続するドメイン参加済みユーザーデバイスが関与します。

展開例: ドメイン参加済みコンピューターからのリモートアクセス(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/smartcard2_1.png)

ユーザーはスマートカードとPINを使用してデバイスにログオンし、その後Citrix Gateway/Access Gatewayに再度ログオンします。この2回目のログオンは、Receiverがこの展開でバイモーダル認証を許可しているため、スマートカードとPIN、またはユーザー名とパスワードのいずれかで行うことができます。

ユーザーはStoreFrontに自動的にログオンし、StoreFrontはユーザーセキュリティ識別子（SID）をCitrix Virtual Apps™またはCitrix Virtual Desktopsに渡します。ユーザーが仮想デスクトップまたはアプリケーションを起動しても、Receiverでシングルサインオン機能が構成されているため、PINの再入力を求められることはありません。

この展開は、2台目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2台目のStoreFrontサーバーに対して認証を行います。この2番目の接続には、任意の認証方法を使用できます。最初のホップで示された構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例: ドメイン非参加コンピューター

この展開では、Desktop Viewer を実行し、StoreFront に直接接続するドメイン非参加ユーザーデバイスが関与します。

展開例: ドメイン非参加コンピューター(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/smartcard3_1.png)

ユーザーはデバイスにログオンします。通常、ユーザーはユーザー名とパスワードを入力しますが、デバイスがドメインに参加していないため、このログオンの資格情報はオプションです。この展開ではバイモーダル認証が可能であるため、Receiverはユーザーにスマートカードと PIN、また

はユーザー名とパスワードのいずれかを要求します。その後、ReceiverはStorefrontに対して認証を行います。

StoreFrontはユーザーセキュリティ識別子（SID）をCitrix Virtual AppsまたはCitrix Virtual Desktopsに渡します。ユーザーが仮想デスクトップまたはアプリケーションを起動すると、この展開ではシングルサインオン機能が利用できないため、PINの再入力を求められます。

この展開は、2台目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2台目のStoreFrontサーバーに対して認証を行います。この2番目の接続には、任意の認証方法を使用できます。最初のホップで示された構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例: ドメイン非参加コンピューターからのリモートアクセス

この展開では、Desktop Viewer を実行し、StoreFront に直接接続するドメイン非参加ユーザーデバイスが関与します。

展開例: ドメイン非参加コンピューターからのリモートアクセス(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/smartcard4_1.png)

ユーザーがデバイスにログオンします。通常、ユーザーはユーザー名とパスワードを入力しますが、デバイスがドメインに参加していないため、このログオンの資格情報はオプションです。この展開ではバイモーダル認証が可能なため、Receiverはスマートカードと PIN、またはユーザー名とパスワードのいずれかをユーザーに要求します。その後、ReceiverはStorefrontに対して認証を行います。

StoreFrontはユーザーセキュリティ識別子（SID）をCitrix Virtual AppsまたはCitrix Virtual Desktopsに渡します。ユーザーが仮想デスクトップまたはアプリケーションを起動すると、この展開ではシングルサインオン機能が利用できないため、ユーザーは再度PINを要求されます。

この展開は、2番目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2番目のStoreFrontサーバーに対して認証を行います。この2番目の接続には、任意の認証方法を使用できます。最初のホップに示されている構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例：ドメインに参加していないコンピューターとシンクライアントがDesktop Applianceサイトにアクセスする場合

この展開には、Desktop Lockを実行し、Desktop Applianceサイトを介してStoreFrontに接続する可能性のある、ドメインに参加していないユーザーデバイスが含まれます。

Desktop Lockは、Citrix Virtual Apps、Citrix Virtual Desktops、およびVDI-in-a-Boxとともにリリースされる個別のコンポーネントです。これはDesktop Viewerの代替であり、主に再利用されたWindowsコンピューターとWindowsシンクライアント向けに設計されています。Desktop Lockは、これらのユーザーデバイスのWindowsシェルとタスクマネージャーを置き換え、ユーザーが基盤となるデバイスにアクセスするのを防ぎます。Desktop Lockを使用すると、ユーザーはWindows Server MachineデスクトップとWindows Desktop Machineデスクトップにアクセスできます。Desktop Lockのインストールはオプションです。

展開例：ドメインに参加していないコンピューターとシンクライアントがDesktop Applianceサイトにアクセスする場合(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/smartcard5_1.png)

ユーザーはスマートカードを使用してデバイスにログオンします。デバイスでDesktop Lockが実行されている場合、デバイスはキオスクモードで実行されているInternet Explorerを介してDesktop Applianceサイトを起動するように構成されています。サイト上のActiveXコントロールがユーザーにPINを要求し、それをStoreFrontに送信します。StoreFrontはユーザーセキュリティ識別子（SID）をCitrix Virtual AppsまたはCitrix Virtual Desktopsに渡します。割り当てられたデスクトップグループのアルファベット順リストで最初に利用可能なデスクトップが起動します。

この展開は、2番目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2番目のStoreFrontサーバーに対して認証を行います。この2番目の接続には、任意の認証方法を使用できます。最初のホップに示されている構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例：ドメインに参加しているコンピューターとシンクライアントがXenApp Services URLを介してStoreFrontにアクセスする場合

この展開には、Desktop Lockを実行し、XenApp Services URLを介してStoreFrontに接続するドメインに参加しているユーザーデバイスが含まれます。

Desktop Lockは、Citrix Virtual Apps、Citrix Virtual Desktops、およびVDI-in-a-Boxとともにリリースされる個別のコンポーネントです。これはDesktop Viewerの代替であり、主に再利用されたWindowsコンピューターとWindowsシンクライアント向けに設計されています。Desktop Lockは、これらのユーザーデバイスのWindowsシェルとタスクマネージャーを置き換え、ユーザーが基盤となるデバイスにアクセスするのを防ぎます。Desktop Lockを使用すると、ユーザーはWindows Server MachineデスクトップとWindows Desktop Machineデスクトップにアクセスできます。Desktop Lockのインストールはオプションです。

展開例：ドメインに参加しているコンピューターとシンクライアントがXenApp Services URLを介してStoreFrontにアクセスする場合(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/smartcard6.png)

ユーザーはスマートカードとPINを使用してデバイスにログオンします。デバイスでDesktop Lockが実行されている場合、統合Windows認証（IWA）を使用してユーザーをStorefrontサーバーに認証します。StoreFrontはユーザーセキュリティ識別子（SID）をCitrix Virtual AppsまたはCitrix Virtual Desktopsに渡します。ユーザーが仮想デスクトップを起動すると、Receiverでシングルサインオン機能が構成されているため、ユーザーは再度PINを要求されません。

この展開は、2番目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2番目のStoreFrontサーバーに対して認証を行います。この2番目の接続には、任意の認証方法を使用できます。最初のホップに示されている構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

スマートカードによるパススルー認証とシングルサインオン

パススルー認証

スマートカードによる仮想デスクトップへのパススルー認証は、Windows 10、Windows 8、Windows 7 SP1 EnterpriseおよびProfessional Editionを実行しているユーザーデバイスでサポートされています。

スマートカードを使用したホストされたアプリケーションへのパススルー認証は、Windows Server 2016、Windows Server 2012 R2、Windows Server 2012、および Windows Server 2008 R2 SP1 を実行しているサーバーでサポートされています。

スマートカードホスト型アプリケーションでパススルー認証を使用するには、サイトの認証方法としてスマートカードによるパススルーを構成する際に、Kerberosの使用を有効にしてください。

注：スマートカードによるパススルー認証の利用可能性は、以下を含む（ただしこれらに限定されない）多くの要因に依存します。

- パススルー認証に関する組織のセキュリティポリシー。
- ミドルウェアの種類と構成。
- スマートカードリーダーの種類。
- ミドルウェアのPINキャッシュポリシー。

スマートカードによるパススルー認証はCitrix StoreFrontで構成されます。詳細については、StoreFrontのドキュメントを参照してください。

シングルサインオン

シングルサインオンは、仮想デスクトップおよびアプリケーションの起動時にパススルー認証を実装するCitrixの機能です。この機能は、ドメイン参加済み、StoreFrontへの直接接続、およびドメイン参加済み、NetScalerからStoreFrontへのスマートカード展開で使用でき、ユーザーがPINを入力する回数を減らすことができます。これらの展開タイプでシングルサインオンを使用するには、StoreFrontサーバーにあるdefault.icaファイルで以下のパラメーターを編集します。

- ドメイン参加済み、StoreFrontへの直接接続スマートカード展開 — DisableCtrlAltDelをOffに設定
- ドメイン参加済み、NetScalerからStoreFrontへのスマートカード展開 — UseLocalUserAndPasswordをOnに設定

これらのパラメーターの設定に関する詳細な手順については、StoreFrontまたはCitrix Gatewayのドキュメントを参照してください。

シングルサインオン機能の利用可否は、以下を含む多くの要因に依存します（ただし、これらに限定されません）。

- シングルサインオンに関する組織のセキュリティポリシー。
- ミドルウェアの種類と構成。
- スマートカードリーダーの種類。
- ミドルウェアのPINキャッシュポリシー。

注：

ユーザーがスマートカードリーダーが接続されたマシン上のVirtual Delivery Agent (VDA) にログオンすると、スマートカードやパスワードなど、以前に成功した認証モードを表すWindowsタイルが表示されることがあります。その結果、シングルサインオンが有効になっている場合、シングルサインオンタイルが表示されることがあります。ログオンするには、シングルサインオンタイルは機能しないため、ユーザーは別のタイルを選択するために**ユーザーの切り替え**を選択する必要があります。

FIDO2およびWebAuthn認証

FIDO2およびWebAuthnを使用したローカル認証と仮想認証

ユーザーは、FIDO2セキュリティキーと、TPM 2.0およびWindows Helloを搭載した統合生体認証デバイスを使用して、仮想セッション内でFIDO2またはWebAuthnを活用するアプリケーションに認証できます。

FIDO2の詳細については、「FIDO2: WebAuthn & CTAP」を参照してください。

この機能の使用方法については、「FIDO2 redirection」を参照してください。

> **注**
>
> この機能は、WebAuthnまたはFIDO2を使用した仮想セッションへのログオンをサポートしていません。この機能は、仮想セッション内のアプリケーションでこれらの認証方法を使用することのみを許可します。

> この機能は、ダブルホップシナリオではサポートされていません。

サポートマトリックス

セッションホストオペレーティングシステム	WEBアプリケーション認証	UWPアプリケーション認証
Windows サーバー 2016	USBリダイレクト経由でサポート	サポートされていません
Windows サーバー 2019	サポート対象	サポートされていません
ウィンドウズ サーバー 2022	サポート対象	サポート対象
ウィンドウズ 10	サポート対象	サポート対象
ウィンドウズ 11	サポート対象	サポート対象

詳細については、以下の要件を確認してください。

Webアプリケーション認証

要件

WebアプリケーションでFIDO2およびWebAuthn認証を使用するための要件は次のとおりです。

Citrix® コントロールプレーン

- シトリックス バーチャル アプリケーションズ アンド デスクトップ™ 2009以降

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - Windows Server 2019 以降のバージョン
- VDA
  - Windows: バージョン2009以降

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - Linux: Workspace app for Linuxのシステム要件を参照してください。
- Workspaceアプリ
  - Windows: バージョン2009.1以降
  - Linux: 2303以降

Webブラウザーの要件

- 64ビットブラウザーのみ

サポートされる認証方法

- FIDO2セキュリティキー
- ウィンドウズ ハロー
  - TPM 2.0
  - 統合生体認証
    - 顔認識

    - 指紋スキャナー
  - WebAuthn

UWPアプリケーション認証

Citrix Virtual Apps and Desktops 2112のリリースにより、CitrixはUWPアプリケーションでのWebAuthnおよびFIDO2認証をサポートします。

Microsoft Teams、Office 365向けMicrosoft Outlook、OneDriveなどのアプリケーションは、Azure Active Directoryへのリンクとして UWPアプリケーションを認証に使用します。Citrixは現在、これらのアプリケーションの認証にFIDO2を使用することをサポートしています。

要件

UWPアプリケーションでFIDO2およびWebAuthn認証を使用するための要件は次のとおりです。

Citrixコントロールプレーン

- シトリックス バーチャル アプリ アンド デスクトップ 2112 以降

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - ウィンドウズ サーバー 2022 以降
- VDA
  - Windows: バージョン2112以降

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - Linux: Linux向けWorkspaceアプリのシステム要件を参照してください
- Workspaceアプリ
  - Windows: バージョン2009.1以降
  - Linux: 2303以降

サポートされる認証方法

- FIDO2セキュリティキー
- ウィンドウズ ハロー
  - TPM 2.0
  - 統合生体認証
    - 顔認識
    - 指紋スキャナー
  - WebAuthn

トランスポート層セキュリティ (TLS)

Citrix Virtual Apps and Desktopsは、コンポーネント間のTCPベースの接続にトランスポート層セキュリティ (TLS) プロトコルをサポートしています。Citrix Virtual Apps and Desktopsは、(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/technical-overview/hdx/adaptive-transport.html)を使用して、UDPベースのICA/HDX接続にデータグラムトランスポート層セキュリティ (DTLS) プロトコルもサポートしています。

TLSとDTLSは類似しており、同じデジタル証明書をサポートしています。Citrix Virtual AppsまたはCitrix Virtual Desktops™サイトをTLSを使用するように構成すると、DTLSを使用するように構成されます。次の手順を使用してください。記載されている箇所を除き、手順はTLSとDTLSの両方に共通です。

- すべてのDelivery Controllerにサーバー証明書を取得、インストール、登録し、TLS証明書でポートを構成します。詳細については、(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/secure/tls.html#install-tls-server-certificates-on-controllers)を参照してください。

  必要に応じて、ControllerがHTTPおよびHTTPSトラフィックをリッスンするために使用するポートを変更できます。
- Citrix Workspace™アプリとVirtual Delivery Agent (VDA) 間でTLS接続を有効にするには、次のタスクを完了します。
  - VDAがインストールされているマシンでTLSを構成します。(便宜上、VDAがインストールされているマシンは、以降「VDA」と表記します。) 一般情報については、(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/secure/tls.html#tls-settings-on-vdas)を参照してください。TLS/DTLSの構成には、Citrixが提供するPowerShellスクリプトを使用することを強くお勧めします。詳細については、(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/secure/

tls.html#configure-tls-on-a-vda-using-the-powershell-script)を参照してください。ただし、TLS/DTLSを手動で構成する場合は、(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/secure/tls.html#manually-configure-tls-on-a-vda)を参照してください。

- Studioで一連のPowerShellコマンドレットを実行して、VDAを含むデリバリーグループでTLSを構成します。詳細については、(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/secure/tls.html#configure-tls-on-delivery-groups)を参照してください。

  要件と考慮事項:

  - ユーザーとVDA間のTLS接続を有効にすることは、XenApp 7.6およびXenDesktop 7.6サイト、およびそれ以降のサポート対象リリースでのみ有効です。
  - コンポーネントをインストールし、サイトを作成し、マシンカタログを作成し、デリバリーグループを作成した後で、デリバリーグループとVDAでTLSを構成します。
  - デリバリーグループでTLSを構成するには、Controllerのアクセスルールを変更する権限が必要です。フル管理者にはこの権限があります。
  - VDAでTLSを構成するには、VDAがインストールされているマシンでWindows管理者である必要があります。
  - Machine Creation Services™またはProvisioning Servicesによってプロビジョニングされたプールされ たVDAでは、VDAマシンイメージは再起動時にリセットされ、以前のTLS設定が失われます。VDAが再起動されるたびにPowerShellスクリプトを実行して、TLS設定を再構成してください。

警告:

Windowsレジストリでの作業を含むタスクの場合—レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になる深刻な問題が発生する可能性があります。Citrix®は、レジストリエディターの誤った使用によって発生した問題が解決されることを保証できません。レジストリエディターは自己責任で使用してください。編集する前に必ずレジストリをバックアップしてください。

サイトデータベースへのTLSを有効にする方法については、CTX137556を参照してください。

Controller に TLS サーバー証明書をインストールする

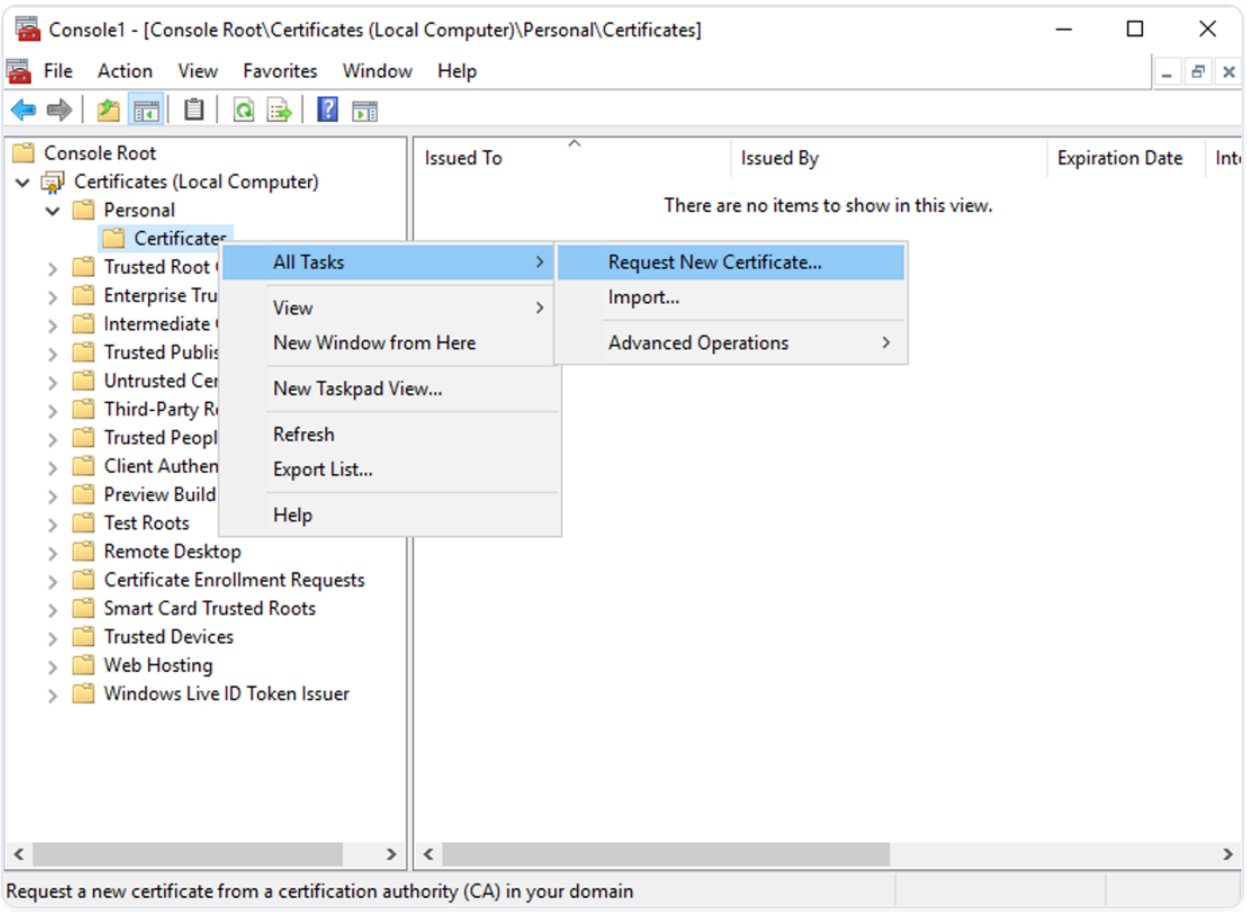
HTTPS の場合、XML Service はクライアント証明書ではなくサーバー証明書を使用して TLS 機能をサポートします。このセクションでは、Delivery Controller で TLS 証明書を取得してインストールする方法について説明します。同じ手順を Cloud Connector に適用して、STA および XML トラフィックを暗号化できます。

証明機関にはさまざまな種類があり、そこから証明書を要求する方法もさまざまですが、この記事では Microsoft 証明機関について説明します。Microsoft 証明機関には、サーバー認証の目的で公開された証明書テンプレートが必要です。

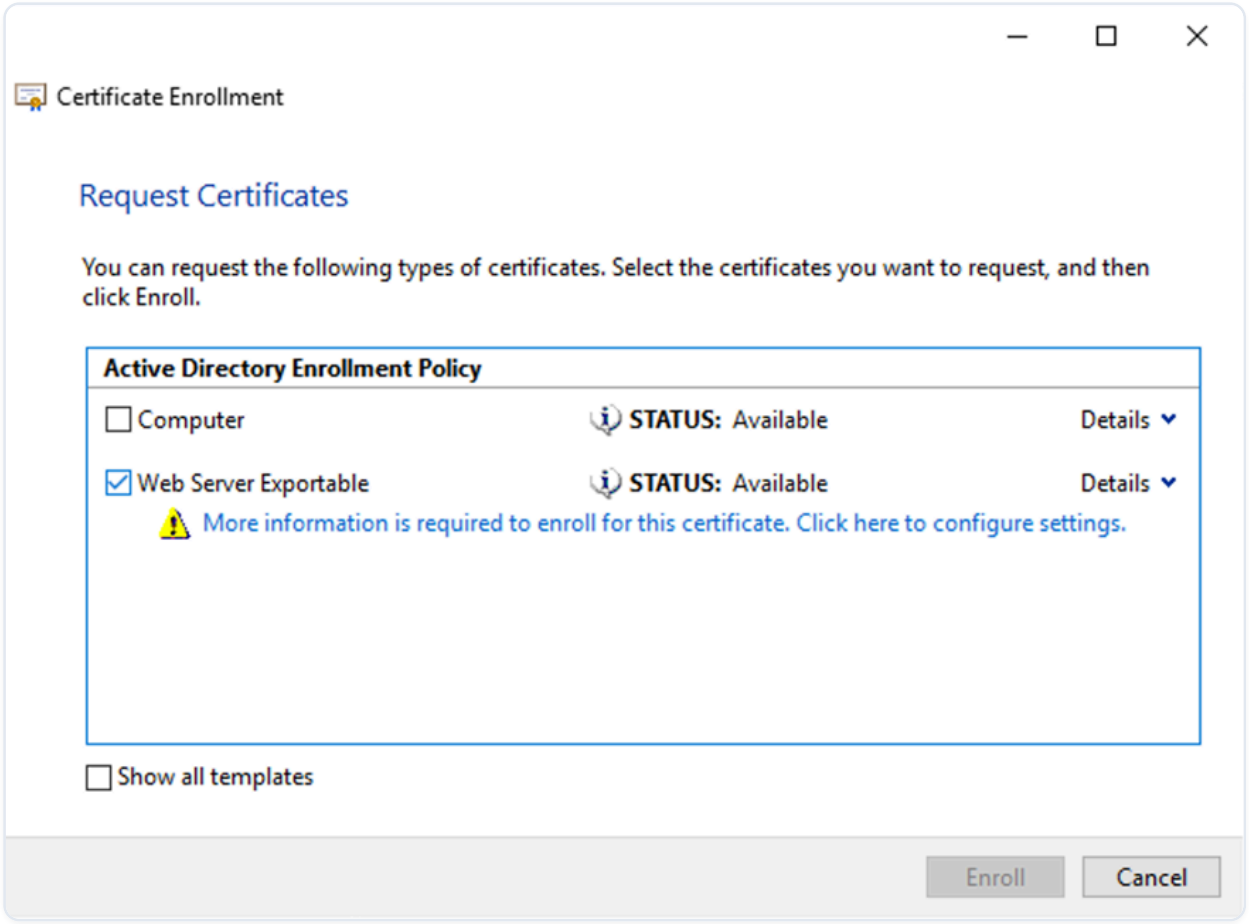
Microsoft 証明機関が Active Directory ドメインまたは Delivery Controller が参加している信頼されたフォレストに統合されている場合、証明書 MMC スナップインの証明書登録ウィザードから証明書を取得できます。

証明書の要求とインストール

1. Delivery Controller™ で、MMC コンソールを開き、証明書スナップインを追加します。プロンプトが表示されたら、 を選択します。
2. **個人 > 証明書**を展開し、**すべてのタスク > 新しい証明書の要求**コンテキストメニューコマンドを使用します。



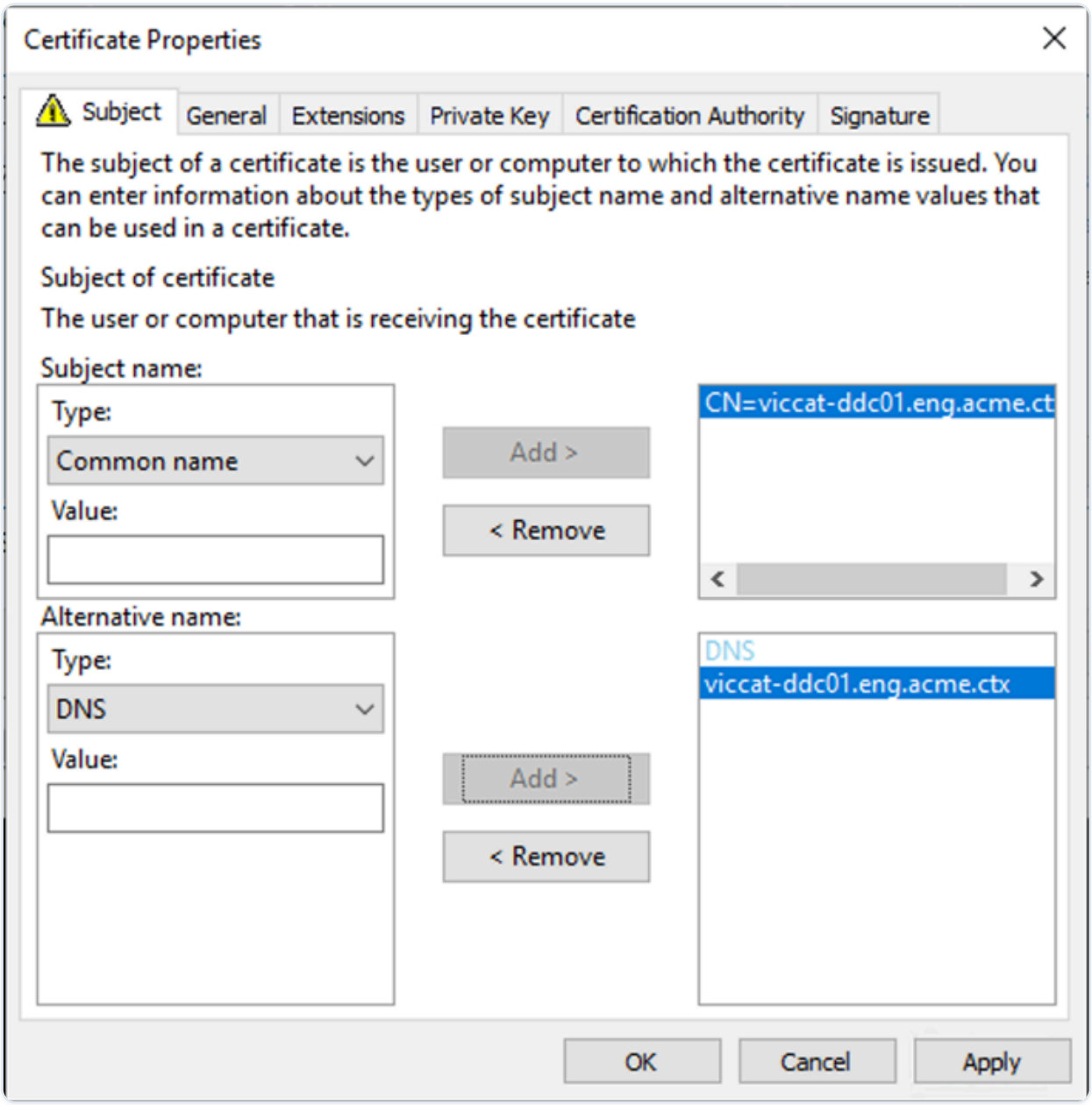
3. **次へ**をクリックして開始し、**次へ**をクリックして Active Directory 登録から証明書を取得することを確認します。
4. サーバー認証証明書のテンプレートを選択します。テンプレートがサブジェクトの値を自動的に提供するように設定されている場合は、詳細を指定せずに**登録**をクリックできます。



5. 証明書テンプレートの詳細を指定するには、**詳細**の矢印ボタンをクリックして、以下を構成します。

   サブジェクト名: 共通名を選択し、Delivery Controller の FQDN を追加します。

   代替名: DNS を選択し、Delivery Controller の FQDN を追加します。



SSL/TLSリスナーポートの構成

Web StudioおよびDirectorの一部としてインストールされているIIS Windowsコンポーネントが同じサーバーにインストールされている場合、IISを使用してTLSを構成できます。詳細については、「Web StudioおよびDirectorでTLSを有効にする」(/ja-jp/citrix-virtual-apps-desktops/2507-ltsr/secure/tls-studio.html)を参照してください。それ以外の場合は、PowerShellを使用して証明書を構成するには：

1. 既存の証明書がバインドされているかを確認するには、コマンドプロンプトを開き、`netsh http show sslcert`を実行します。

   ```
   netsh http show sslcert
   ```

2. 既存のバインドがある場合は、それを削除します。

```
netsh http delete sslcert ipport=0.0.0.0:443
```

既存のバインドで特定のIPアドレスとポートが指定されていた場合は、`0.0.0.0:443`をそのIPアドレスとポートに置き換えます。

3. 以前にインストールした証明書のサムプリントを見つけます。サムプリントを表示するには、**コンピューター証明書の管理**を開き、証明書を参照して開き、**詳細**タブに移動します。

証明書のプロパティでサムプリントが表示されているスクリーンショット(/en-us/citrix-virtual-apps-desktops/2507-ltsr/media/certificate-thumbprint.png)

または、PowerShellを使用することもできます。たとえば、次のスクリプトは、共通名がサーバーのホスト名と一致する証明書を検索し、サムネイルを出力します。

```
$HostName =
([System.Net.Dns]::GetHostByName(($env:computerName))).Hostname

$Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object
{$_.Subject -match ("CN=" + $HostName)}).Thumbprint -join ';'

Write-Host -Object "Certificate Thumbprint for $($HostName): $
($Thumbprint)" -Foreground Yellow
```

証明書の共通名がホスト名と一致しない場合、これは失敗します。ホスト名に対して複数の証明書がある場合、これは連結された複数のサムプリントを返し、適切なサムプリントを選択する必要があります。

次の例は、フレンドリ名で証明書を検索します。

```
$friendlyName = "My certificate name"

$Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object
{$_.FriendlyName -eq $friendlyNam}).Thumbprint -join ';'

Write-Host -Object "Certificate Thumbprint for $friendlyName: $
($Thumbprint)" -Foreground Yellow
```

指定されたフレンドリ名を持つ証明書が複数ある場合、これは連結された複数のサムプリントを返し、適切なサムプリントを選択する必要があります。

4. 証明書をポートにバインドするには、`netsh http add sslcert`コマンドを使用します。

```
netsh http add sslcert ipport=[IP address]:443 certhash=[certificate
hash] appid=[application GUID] disablelegacytls=enable
```

- `ipport`: IPアドレスとポート。0.0.0.0:443を使用すると、すべてのIPアドレスに適用されます。代わりに、特定のIPアドレスを指定することもできます。
- `certhash`: 前のステップで特定した証明書のサムプリント。
- `appid`: シトリックスブローカーサービスの GUID。

> **注：**
>
> 証明書を更新または再バインドする際は、任意のGUIDではなく、Broker Serviceに関連付けられた特定の`appid`を使用してください。
>
> Citrix Broker Serviceの正しい`appid`を見つけるには、次の手順を実行します。

a. 管理者としてPowerShellコマンドウィンドウを開き、次のコマンドを実行します。

```
Get-WmiObject -Class Win32_Product | Select-String -Pattern
"broker"
```

b. 出力でCitrix Broker ServiceのIdentifyingNumber (GUID) を見つけます (例: `{D333C884-187F-447C-8C67-463F33989C8F}`)。このGUIDを`appid`パラメーターに使用します。

- `disablelegacytls=enable`: レガシーバージョンのTLSを無効にします。このパラメーターはWindows 2022以降で利用可能です。Windows 2022ではTLS 1.0および1.1を無効にします。Windows 2025では、TLS 1.0および1.1がデフォルトで無効になっているため、これは不要です。

たとえば、すべてのIPアドレスで、サムプリント`bc96f958848639fd101a793b87915d5f2829b0b6`の証明書をポート`443`にバインドするには、次のコマンドを実行します。

```
netsh http add sslcert ipport=0.0.0.0:443
certhash=bc96f958848639fd101a793b87915d5f2829b0b6 appid={91fe7386-
e0c2-471b-a252-1e0a805febac} disablelegacytls=enable
```

HTTPSが有効になったら、StoreFront展開とNetscaler Gatewayを、デリバリーコントローラーへの接続にHTTPではなくHTTPSを使用するように構成する必要があります。

注：

ControllerがWindows Server 2016にインストールされ、StoreFrontがWindows Server 2012 R2にインストールされている場合、TLS暗号スイートの順序を変更するために、Controllerで構成変更が必要です。この構成変更は、他のWindows Serverバージョンの組み合わせのControllerとStoreFrontでは必要ありません。

暗号スイートの順序リストには、`TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384`または`TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256`暗号スイート（またはその両方）を含める必要があります。また、これらの暗号スイートは、`TLS_DHE_`暗号スイートよりも前に配置する必要があります。

1. Microsoftグループポリシーエディターを使用して、**コンピューターの構成 > 管理用テンプレート > ネットワーク > SSL構成設定**に移動します。
2. 「SSL暗号スイートの順序」ポリシーを編集します。デフォルトでは、このポリシーは「未構成」に設定されています。このポリシーを「有効」に設定します。
3. スイートを正しい順序に並べ替えます。使用したくない暗号スイートスイートは削除します。

`TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384`または`TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256`のいずれかが、`TLS_DHE_`暗号スイートよりも前に来るようにしてください。

Microsoft MSDNで、Schannel暗号スイートの優先順位付けも参照してください。

HTTPまたはHTTPSポートを変更する

デフォルトでは、Controller の XML Service は、HTTP トラフィックにはポート 80 を、HTTPS トラフィックにはポート 443 をリッスンします。デフォルト以外のポートを使用することもできますが、Controller を信頼できないネットワークに公開することによるセキュリティリスクに注意

してください。デフォルトを変更するよりも、スタンドアロンの StoreFront サーバーを展開する方が推奨されます。

Controller で使用されるデフォルトの HTTP または HTTPS ポートを変更するには、Studio から次のコマンドを実行します。

```
BrokerService.exe -WIPORT \<http-port> -WISSLPORT \<https-port>
```

ここで、`<http-port>` は HTTP トラフィックのポート番号、`<https-port>` は HTTPS トラフィックのポート番号です。

> **注：**
>
> ポートを変更した後、Studio にライセンスの互換性とアップグレードに関するメッセージが表示されることがあります。この問題を解決するには、次の PowerShell コマンドレットシーケンスを使用してサービスインスタンスを再登録します。

```
Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding XML_HTTPS
|

Unregister-ConfigRegisteredServiceInstance

Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" |

Register-ConfigServiceInstance
```

HTTPS トラフィックのみを強制する

XML Service で HTTP トラフィックを無視させる場合は、Controller の HKLM\Software\Citrix\DesktopServer\ に次のレジストリ設定を作成し、Broker Service を再起動します。

HTTP トラフィックを無視するには、DWORD XmlServicesEnableNonSsl を作成し、値を 0 に設定します。

HTTPS トラフィックを無視するために作成できる対応するレジストリ DWORD 値があります: DWORD XmlServicesEnableSsl。これが 0 に設定されていないことを確認してください。

VDA の TLS 設定

デリバリーグループには、TLS が構成されている VDA と TLS が構成されていない VDA を混在させることはできません。デリバリーグループの TLS を構成する前に、そのデリバリーグループ内のすべての VDA に対して TLS がすでに構成されていることを確認してください。

VDA で TLS を構成すると、インストールされている TLS 証明書のアクセス許可が変更され、ICA® Service に証明書の秘密キーへの読み取りアクセス権が付与され、ICA Service に次の情報が通知されます。

- **TLS に使用する証明書ストア内の証明書。**
- **TLS 接続に使用する TCP ポート番号。**

  Windows ファイアウォール（有効な場合）は、この TCP ポートでの受信接続を許可するように構成する必要があります。この構成は、PowerShell スクリプトを使用すると自動的に行われます。
- **許可する TLS プロトコルのバージョン。**

  > **重要:**
  >
  > Citrixでは、SSLv3の使用状況を確認し、必要に応じてSSLv3のサポートを削除するように展開を再構成することをお勧めします。CTX200238を参照してください。

  > サポートされているTLSプロトコルバージョンは、階層（最低から最高）に従います：SSL 3.0、TLS 1.0、TLS 1.1、TLS 1.2。許可される最小バージョンを指定します。そのバージョンまたはそれ以降のバージョンを使用するすべてのプロトコル接続が許可されます。

  たとえば、最小バージョンとしてTLS 1.1を指定した場合、TLS 1.1およびTLS 1.2プロトコル接続が許可されます。最小バージョンとしてSSL 3.0を指定した場合、サポートされているすべてのバージョンの接続が許可されます。最小バージョンとしてTLS 1.2を指定した場合、TLS 1.2接続のみが許可されます。

  DTLS 1.0はTLS 1.1に対応し、DTLS 1.2はTLS 1.2に対応します。
- **許可するTLS暗号スイート。**

  暗号スイートは、接続に使用される暗号化を選択します。クライアントとVDAは、異なる暗号スイートのセットをサポートできます。クライアント（Citrix Workspaceアプリまたは StoreFront）が接続し、サポートされているTLS暗号スイートのリストを送信すると、VDAは

クライアントの暗号スイートの1つを、自身の構成済み暗号スイートのリストにある暗号スイートの1つと照合し、接続を受け入れます。一致する暗号スイートがない場合、VDAは接続を拒否します。

VDAは、3つの暗号スイートセット（コンプライアンスモードとも呼ばれます）をサポートしています：GOV（政府）、COM（商用）、およびALL。許容される暗号スイートは、Windows FIPSモードにも依存します。Windows FIPSモードの詳細については、`<http://support.microsoft.com/kb/811833>`を参照してください。次の表に、各セットの暗号スイートを示します。

TLS/DTLS暗号スイート	すべて	COM	GOV	すべて	COM	GOV
FIPSモード	オフ	オフ	オフ	オン	オン	オン
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384*	X		X	X		X
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	X		X	X		X
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	X	X		X	X	

* Windows Server 2012 R2ではサポートされていません。

注：

> VDAはDHE暗号スイート（例：TLS_DHE_RSA_WITH_AES_256_GCM_SHA384、TLS_DHE_RSA_WITH_AES_256_CBC_SHA、TLS_DHE_RSA_WITH_AES_128_GCM_SHA256、TLS_DHE_RSA_WITH_AES_128_CBC_SHA）をサポートしていません。Windowsによって選択された場合でも、Receiverでは使用されないことがあります。

> Citrix Gatewayを使用している場合は、バックエンド通信の暗号スイートサポートに関する情報についてCitrix ADCのドキュメントを参照してください。TLS暗号スイートのサポートについては、Citrix ADCアプライアンスで利用可能な暗号を参照してください。DTLS暗号スイートのサポートについては、DTLS暗号のサポートを参照してください。

証明書を要求してインストールする

1. VDAで、MMCコンソールを開き、証明書スナップインを追加します。プロンプトが表示されたら、コンピューターアカウントを選択します。
2. **個人 > 証明書**を展開し、コンテキストメニューコマンド**すべてのタスク > 新しい証明書の要求**を使用します。
3. 開始するには **次へ** をクリックし、Active Directory 登録から証明書を取得することを確認するには **次へ** をクリックします。
4. サーバー認証証明書のテンプレートを選択します。デフォルトの Windows **コンピューター** または **Web サーバー (エクスポート可能)** の両方を使用できます。テンプレートが Subject の値を自動的に提供するように設定されている場合は、詳細を指定せずに **登録** をクリックできます。

   「証明書要求」ダイアログ(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/tls-request-certificates.png)
5. 証明書テンプレートの詳細を指定するには、**詳細** をクリックして以下を構成します。

   サブジェクト名 — タイプ **共通名** を選択し、VDA の FQDN を追加します。

   代替名 — タイプ **DNS** を選択し、VDA の FQDN を追加します。

   証明書のプロパティ(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/tls-certificate-properties.png)

   > **注：**

> Active Directory 証明書サービス証明書の自動登録を使用して、VDA への証明書の発行と展開を自動化します。これについては、`<https://support.citrix.com/article/CTX205473>` で説明されています。

> ワイルドカード証明書を使用して、単一の証明書で複数の VDA を保護できます。

サブジェクト名 — タイプ **共通名** を選択し、VDA の *.primary.domain を入力します。

代替名 — タイプ **DNS** を選択し、VDA の *.primary.domain を追加します。

ワイルドカード証明書要求ダイアログ(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/tls-request-certificates-wildcard.png)

SAN 証明書を使用して、単一の証明書で複数の特定の VDA を保護できます。

サブジェクト名 — タイプ **共通名** を選択し、証明書の使用状況を識別するのに役立つ文字列を入力します。

代替名 — タイプ **DNS** を選択し、各 VDA の FQDN のエントリを追加します。最適な TLS ネゴシエーションを確保するために、代替名の数を最小限に抑えてください。

「証明書要求」ダイアログ(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/tls-request-certificates-san.png)

> **注：**
>
> ワイルドカード証明書とSAN証明書の両方で、［秘密キー］タブの**［秘密キーをエクスポート可能にする］**が選択されている必要があります。

> 「証明書要求」ダイアログ(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/tls-certificate-properties-private-key.png)

PowerShellスクリプトを使用してVDAでTLSを構成する

証明書ストアの［ローカルコンピューター］>［個人］>［証明書］領域にTLS証明書をインストールします。その場所に複数の証明書がある場合は、証明書のサムプリントをPowerShellスクリプトに指定します。

> **注：**

> XenAppおよびXenDesktop 7.16 LTSR以降、PowerShellスクリプトはVDAのFQDNに基づいて正しい証明書を検索します。VDAのFQDNに対して証明書が1つしかない場合は、サムプリントを指定する必要はありません。

> Enable-VdaSSL.ps1スクリプトは、VDAでTLSリスナーを有効または無効にします。このスクリプトは、インストールメディアの*Support* > *Tools* > *SslSupport*フォルダーにあります。

TLSを有効にすると、DHE暗号スイートは無効になります。ECDHE暗号スイートは影響を受けません。

TLSを有効にすると、スクリプトは指定されたTCPポートの既存のWindowsファイアウォール規則をすべて無効にします。次に、ICAサービスがTLS TCPポートとUDPポートでのみ受信接続を受け入れることを許可する新しい規則を追加します。また、次のWindowsファイアウォール規則も無効にします。

- Citrix ICA（デフォルト：1494）
- Citrix CGP（デフォルト：2598）
- Citrix WebSocket（デフォルト：8008）

その結果、ユーザーはTLSまたはDTLSを使用してのみ接続できます。TLSまたはDTLSなしでは、ICA/HDX、セッションの信頼性を備えたICA/HDX、またはWebSocket経由のHDXを使用できません。

> **注：**

> DTLSは、UDPリアルタイムトランスポート経由のICA/HDXオーディオ、またはICA/HDX Framehawkではサポートされていません。

> 「ネットワークポート」を参照してください。(/ja-jp/tech-zone/build/tech-papers/citrix-communication-ports.html#citrix-virtual-apps-and-desktops).

スクリプトには以下の構文説明と追加の例が含まれています。この情報はNotepad++などのツールを使用して確認できます。

> **重要:**

EnableまたはDisableパラメーターと、CertificateThumbPrintパラメーターを指定します。その他のパラメーターはオプションです。

構文

```
Enable-VdaSSL {-Enable | -Disable} -CertificateThumbPrint "<thumbprint>" [-SSLPort <port>] [-SSLMinVersion "<min-ssl-version>"] [-SSLCipherSuite"\<suite>"]
```

パラメーター	説明
有効	VDAにTLSリスナーをインストールして有効にします。このパラメーターまたはDisableパラメーターのいずれかが必要です。
無効	VDA上のTLSリスナーを無効にします。このパラメーターまたはEnableパラメーターのいずれかが必要です。このパラメーターを指定した場合、他のパラメーターは無効になります。
証明書サムプリント "<thumbprint>"	引用符で囲まれた、証明書ストア内のTLS証明書のサムプリント。スクリプトは指定されたサムプリントを使用して、使用する証明書を選択します。このパラメーターを省略すると、誤った証明書が選択されます。
SSLポート <port>	TLSポート。デフォルト: 443
SSL最小バージョン "<version>"	引用符で囲まれた、最小TLSプロトコルバージョン。有効な値: 「TLS_1.0」（デフォルト）、「TLS_1.1」、および「TLS_1.2」。
SSL暗号スイート "<suite>"	TLS暗号スイート。引用符で囲みます。有効な値: "GOV"、"COM"、および "ALL" (デフォルト)。

例

次のスクリプトは、TLSプロトコルバージョン値をインストールして有効にします。サムプリント (この例では「12345678987654321」と表記) は、使用する証明書を選択するために使用されます。

```
Enable-VdaSSL -Enable -CertificateThumbPrint "12345678987654321"
```

次のスクリプトは、TLSリスナーをインストールして有効にし、TLSポート400、GOV暗号スイート、および最小TLS 1.2プロトコル値を指定します。サムプリント (この例では「12345678987654321」と表記) は、使用する証明書を選択するために使用されます。

```
Enable-VdaSSL -Enable

-CertificateThumbPrint "12345678987654321"

-SSLPort 400 -SSLMinVersion "TLS_1.2"

-SSLCipherSuite "All"
```

次のスクリプトは、VDA上のTLSリスナーを無効にします。

```
Enable-VdaSSL -Disable
```

VDAでTLSを手動で構成する

VDAでTLSを手動で構成する場合、各VDA上の適切なサービスに対して、TLS証明書の秘密キーへの一般的な読み取りアクセスを許可します。WindowsシングルセッションOS用VDAの場合はNT SERVICE\PorticaService、またはWindowsマルチセッションOS用VDAの場合はNT SERVICE\TermServiceです。VDAがインストールされているマシンで:

手順 1. Microsoft管理コンソール (MMC) を起動します。 > > mmc.exe。

手順 2. MMCに証明書スナップインを追加します。

1. > を選択します。
2. を選択し、 をクリックします。
3. 「このスナップインは常に次の証明書を管理します:」というプロンプトが表示されたら、「コンピューターアカウント」を選択し、 をクリックします。
4. 「このスナップインで管理するコンピューターを選択してください」というプロンプトが表示されたら、「ローカルコンピューター」を選択し、 をクリックします。

手順 3. > > で、証明書を右クリックし、 > を選択します。

手順 4. アクセス制御リストエディターに「(FriendlyName) の秘密キーのアクセス許可」が表示されます。ここで(FriendlyName)はTLS証明書の名前です。次のいずれかのサービスを追加し、読み取りアクセス権を付与します。

- WindowsシングルセッションOS用VDAの場合、「PORTICASERVICE」
- Windows Multi-session OS 用 VDA の場合、「TERMSERVICE」

手順 5. インストールされている TLS 証明書をダブルクリックします。証明書ダイアログで、 タブを選択し、一番下までスクロールします。 をクリックします。

手順 6. regedit を実行し、HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd に移動します。

1. SSL Thumbprint キーを編集し、TLS 証明書の拇印の値をこのバイナリ値にコピーします。 ダイアログボックスの不明な項目（「0000」や特殊文字など）は無視しても問題ありません。
2. SSLEnabled キーを編集し、DWORD 値を 1 に変更します。（後で SSL を無効にするには、DWORD 値を 0 に変更します。）
3. デフォルト設定を変更する場合（オプション）は、同じレジストリパスで以下を使用します。

   SSLPort DWORD – SSL ポート番号。デフォルト: 443。

   SSLMinVersion DWORD – 1 = SSL 3.0、2 = TLS 1.0、3 = TLS 1.1、4 = TLS 1.2。デフォルト: 2 (TLS 1.0)。

   SSLCipherSuite DWORD – 1 = GOV、2 = COM、3 = ALL。デフォルト: 3 (ALL)。

手順 7. TLS の TCP および UDP ポートがデフォルトの 443 でない場合、Windows ファイアウォールで開いていることを確認します。（Windows ファイアウォールで受信規則を作成する際は、そのプロパティで「接続を許可する」と「有効」が選択されていることを確認してください。）

手順 8. 他のアプリケーションやサービス（IIS など）が TLS TCP ポートを使用していないことを確認します。

手順 9. Windows Multi-session OS 用 VDA の場合、変更を有効にするためにマシンを再起動します。（Windows Single-session OS 用 VDA を含むマシンを再起動する必要はありません。）

> **重要:**

> VDA が Windows Server 2012 R2、Windows Server 2016、または Windows 10 Anniversary Edition 以降のサポート対象リリースである場合、追加の手順が必要です。これは、Citrix Receiver for Windows（バージョン 4.6～4.9）、Citrix Workspace app for HTML5、および Citrix Workspace app for Chrome からの接続に影響します。Citrix Gateway を使用する接続も含まれます。

Citrix Gateway と VDA 間の TLS が構成されている場合、すべての VDA バージョンにおいて、Citrix Gateway を使用するすべての接続でこの手順も必要です。これは、すべての Citrix Receiver™ バージョンに影響します。

VDA（Windows Server 2012 R2、Windows Server 2016、または Windows 10 Anniversary Edition 以降）で、グループポリシーエディターを使用して、 > > > > > に移動します。次の順序を選択します。

```
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
```

注：

最初の6つの項目では、楕円曲線（P384またはP256）も指定します。「curve25519」が選択されていないことを確認してください。FIPSモードは「curve25519」の使用を妨げません。

このグループポリシー設定が構成されている場合、VDAは、グループポリシーリストと、選択されたコンプライアンスモード（COM、GOV、またはALL）のリストの両方に表示される場合にのみ、暗号スイートを選択します。暗号スイートは、クライアント（Citrix WorkspaceアプリまたはStoreFront）から送信されたリストにも表示されている必要があります。

このグループポリシー構成は、VDA上の他のTLSアプリケーションおよびサービスにも影響します。アプリケーションが特定の暗号スイートを必要とする場合、それらをこのグループポリシーリストに追加する必要がある場合があります。

> **重要:**

> グループポリシーの変更は適用時に表示されますが、TLS構成のグループポリシーの変更はオペレーティングシステムの再起動後にのみ有効になります。したがって、プールされたデスクトップの場合、TLS構成のグループポリシーの変更をベースイメージに適用してください。

デリバリーグループでTLSを構成する

TLS接続用に構成したVDAを含む各デリバリーグループに対して、この手順を完了してください。

1. StudioからPowerShellコンソールを開きます。
2. Citrix製品のコマンドレットをロードするには、**asnp Citrix.*** を実行します。
3. **Get-BrokerAccessPolicyRule -DesktopGroupName '\<*delivery-group-name*>' \| Set-BrokerAccessPolicyRule -HdxSslEnabled $true** を実行します。
4. **Set-BrokerSite -DnsResolutionEnabled $true** を実行します。

トラブルシューティング

接続エラーが発生した場合は、VDAのシステムイベントログを確認してください。

Windows版Citrix Workspaceアプリを使用しているときに、TLSエラーを示す接続エラーが発生した場合は、Desktop Viewerを無効にしてから、再度接続を試みてください。接続は引き続き失敗しますが、根本的なTLS問題の説明が提供される場合があります。（たとえば、証明機関から証明書を要求する際に誤ったテンプレートを指定したなど。）

HDX™ Adaptive Transportを使用するほとんどの構成は、Citrix Workspaceアプリ、Citrix Gateway、およびVDAの最新バージョンを使用するものを含め、DTLSで正常に動作します。Citrix WorkspaceアプリとCitrix Gatewayの間でDTLSを使用し、Citrix GatewayとVDAの間でDTLSを使用する一部の構成では、追加の操作が必要です。

次の場合、追加の操作が必要です。

- Citrix ReceiverのバージョンがHDX Adaptive TransportおよびDTLSをサポートしている場合：Receiver for Windows (4.7, 4.8, 4.9)、Receiver for Mac (12.5, 12.6, 12.7)、Receiver for iOS (7.2, 7.3.x) またはReceiver for Linux (13.7)

以下のいずれかに該当する場合も同様です。

- Citrix GatewayのバージョンはVDAへのDTLSをサポートしているが、VDAのバージョンはDTLSをサポートしていない（バージョン7.15以前）。
- VDAのバージョンはDTLSをサポートしている（バージョン7.16以降）が、Citrix GatewayのバージョンはVDAへのDTLSをサポートしていない。

Citrix Receiverからの接続が失敗するのを避けるには、以下のいずれかを実行してください。

- Citrix Receiverを、Receiver for Windowsバージョン4.10以降、Receiver for Mac 12.8以降、またはReceiver for iOSバージョン7.5以降に更新する。
- Citrix Gatewayを、VDAへのDTLSをサポートするバージョンに更新する。
- VDAをバージョン7.16以降に更新する。
- VDAでDTLSを無効にする。
- HDX Adaptive Transportを無効にする。

> **注：**
>
> Receiver for Linuxの適切なアップデートはまだ利用できません。Receiver for Android（バージョン3.12.3）は、Citrix Gateway経由のHDX Adaptive TransportおよびDTLSをサポートしていないため、影響を受けません。

> VDAでDTLSを無効にするには、VDAファイアウォール構成を変更してUDPポート443を無効にします。(/ja-jp/tech-zone/build/tech-papers/citrix-communication-ports.html#citrix-virtual-apps-and-desktops)を参照してください。

ControllerとVDA間の通信

Windows Communication Framework (WCF) のメッセージレベル保護により、ControllerとVDA間の通信が保護されます。TLSを使用した追加のトランスポートレベル保護は必要ありません。WCF構成では、ControllerとVDA間の相互認証にKerberosを使用します。暗号化には256ビットキーのCBCモードAESを使用します。メッセージの整合性にはSHA-1を使用します。

Microsoftによると、WCFで使用されるセキュリティ プロトコル は、WS-SecurityPolicy 1.2を含むOASIS（Organization for the Advancement of Structured Information Standards）の標準に準拠しています。さらに、Microsoftは、WCFが Security Policy 1.2 に記載されているすべてのアルゴリズムスイートをサポートしていると述べています。

ControllerとVDA間の通信では、上記で述べたアルゴリズムを使用するbasic256アルゴリズムスイートが使用されます。

TLS と HTML5 ビデオリダイレクト、およびブラウザコンテンツリダイレクト

HTML5 ビデオリダイレクトとブラウザコンテンツリダイレクトを使用して、HTTPS Web サイトをリダイレクトできます。これらの Web サイトに挿入された JavaScript は、VDA で実行されている Citrix HDX HTML5 ビデオリダイレクトサービスへの TLS 接続を確立する必要があります。これを実現するために、HTML5 ビデオリダイレクトサービスは、VDA の証明書ストアに 2 つのカスタム証明書を生成します。サービスを停止すると、証明書は削除されます。

HTML5 ビデオリダイレクトポリシーは、デフォルトで無効になっています。

ブラウザコンテンツリダイレクトは、デフォルトで有効になっています。

HTML5 ビデオリダイレクトの詳細については、「マルチメディアポリシー設定」を参照してください。

ユニバーサルプリントサーバーでのトランスポート層セキュリティ (TLS)

Virtual Delivery Agent (VDA) とユニバーサルプリントサーバー間のTCPベースの接続では、トランスポート層セキュリティ (TLS) プロトコルがサポートされています。

> **警告:**
>
> Windowsレジストリでの作業を含むタスクの場合—レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になる深刻な問題が発生する可能性があります。Citrix®は、レジストリエディターの誤った使用によって発生した問題が解決されることを保証できません。レジストリエディターは自己責任で使用してください。編集する前に必ずレジストリをバックアップしてください。

VDAとユニバーサルプリントサーバー間の印刷接続の種類

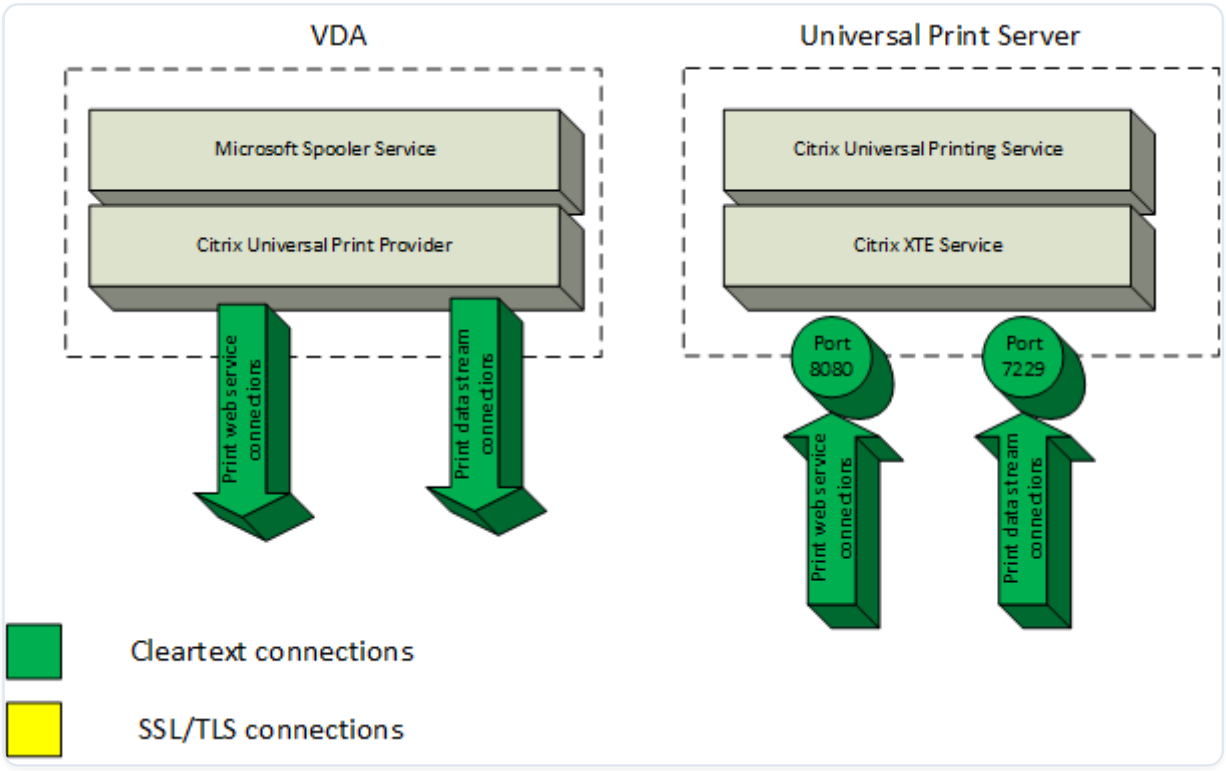
クリアテキスト接続

印刷に関連する以下の接続は、VDAから発信され、ユニバーサルプリントサーバーのポートに接続します。これらの接続は、**SSL enabled** ポリシー設定が **Disabled** (デフォルト) に設定されている場合にのみ行われます。

- クリアテキスト印刷Webサービス接続 (TCPポート 8080)

- クリアテキスト印刷データストリーム (CGP) 接続 (TCPポート 7229)

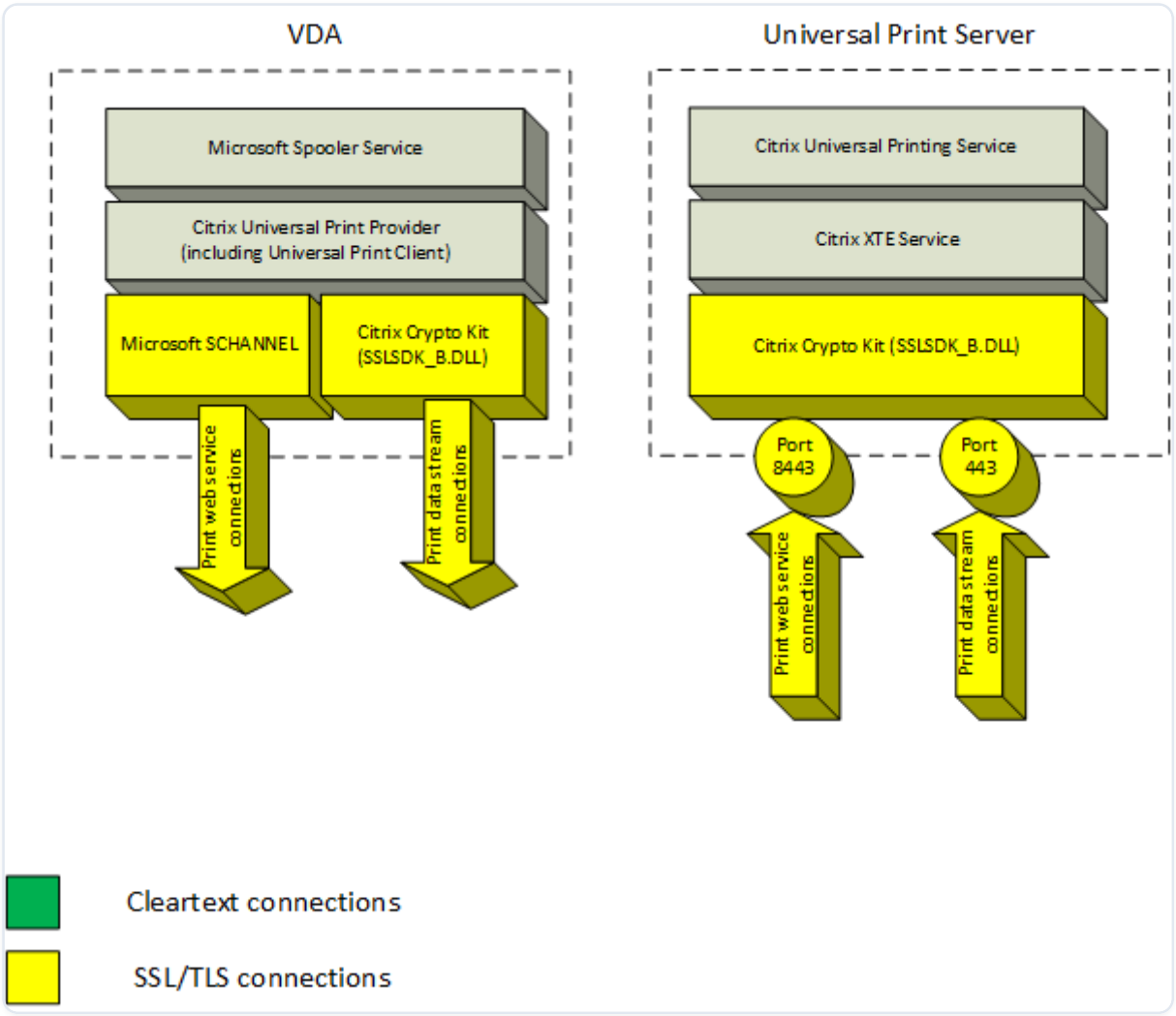
Microsoft サポート技術情報「Windows のサービス概要とネットワークポート要件」には、Microsoft Windows Print Spooler サービスが使用するポートについて記載されています。このドキュメントの SSL/TLS 設定は、Windows Print Spooler サービスによって行われる NETBIOS および RPC 接続には適用されません。「**Universal Print Server の有効化**」ポリシー設定が「**Windows のネイティブなリモート印刷へのフォールバックを有効にする**」に設定されている場合、VDA は Windows ネットワーク印刷プロバイダー (win32spl.dll) をフォールバックとして使用します。



暗号化された接続

印刷に関連するこれらのSSL/TLS接続は、VDAから発信され、ユニバーサルプリントサーバーのポートに接続します。これらの接続は、**SSL enabled** ポリシー設定が **Enabled** に設定されている場合にのみ行われます。

- 暗号化された印刷Webサービス接続 (TCPポート 8443)
- 暗号化された印刷データストリーム (CGP) 接続 (TCPポート 443)



SSL/TLS クライアント構成

VDA は SSL/TLS クライアントとして機能します。

Microsoft Group Policy とレジストリを使用して、暗号化された印刷 Web サービス接続 (TCP ポート 8443) 用に Microsoft SCHANNEL SSP を構成します。Microsoft サポート記事の TLS Registry Settings には、Microsoft SCHANNEL SSP のレジストリ設定が記載されています。

VDA (Windows Server 2016 または Windows 10) でグループポリシーエディターを使用して、**［コンピューターの構成］>［管理用テンプレート］>［ネットワーク］>［SSL 構成設定］>［SSL 暗号スイートの順序］**の順に移動します。次の順序を選択します。

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256

> **注：**

> このグループポリシー設定が構成されている場合、VDA は、暗号化された印刷 Web サービス接続 (デフォルトポート: 8443) の暗号スイートを、その接続が両方の SSL 暗号スイートリストに表示されている場合にのみ選択します。

> - グループポリシー SSL 暗号スイート順序リスト
> - 選択した SSL 暗号スイートポリシー設定 (COM、GOV、または ALL) に対応するリスト

> このグループポリシー構成は、VDA 上の他の TLS アプリケーションおよびサービスにも影響します。アプリケーションが特定の暗号スイートを必要とする場合、それらをこのグループポリシー暗号スイート順序リストに追加する必要がある場合があります。

> **重要:**

> TLS 構成のグループポリシーの変更は、オペレーティングシステムの再起動後にのみ有効になります。

> Citrix ポリシーを使用して、暗号化された印刷データストリーム (CGP) 接続 (TCP ポート 443) の SSL/TLS 設定を構成します。

SSL/TLS サーバー構成

Universal Print Server は SSL/TLS サーバーとして機能します。

`Enable-UpsSsl.ps1` PowerShellスクリプトを使用して、SSL/TLS設定を構成します。

Universal Print ServerにTLSサーバー証明書をインストールする

HTTPS の場合、Universal Print Server はサーバー証明書を使用して TLS 機能をサポートします。クライアント証明書は使用されません。Microsoft Active Directory 証明書サービスまたは別の証明機関を使用して、Universal Print Server の証明書を要求します。

マイクロソフト アクティブ ディレクトリ証明書サービスを使用して証明書を登録/要求する際は、以下の考慮事項に留意してください。

1. 証明書をローカルコンピューターの**個人**証明書ストアに配置します。

2. 証明書のサブジェクト識別名（Subject DN）の**共通名**属性を、Universal Print Serverの完全修飾ドメイン名（FQDN）に設定します。これは証明書テンプレートで指定します。
3. 証明書要求と秘密鍵の生成に使用される暗号化サービスプロバイダー（CSP）を**Microsoft Enhanced RSA and AES Cryptographic Provider (Encryption)**に設定します。これは証明書テンプレートで指定します。
4. キーサイズを2048ビット以上に設定します。これは証明書テンプレートで指定します。

Universal Print ServerでのSSLの構成

Universal Print Server上のXTEサービスは、受信接続をリッスンします。SSLが有効な場合、SSLサーバーとして機能します。受信接続には、印刷コマンドを含む印刷Webサービス接続と、印刷ジョブを含む印刷データストリーム接続の2種類があります。これらの接続でSSLを有効にできます。SSLは、これらの接続の機密性と整合性を保護します。デフォルトでは、SSLは無効になっています。

SSLの構成に使用されるPowerShellスクリプトはインストールメディアにあり、ファイル名は次のとおりです: `\Support\Tools\SslSupport\Enable-UpsSsl.ps1.`.

Universal Print Serverでのリスニングポート番号の構成

これらは XTE サービスのデフォルトポートです。

- クリアテキスト印刷Webサービス（HTTP）TCPポート: 8080
- クリアテキスト印刷データストリーム (CGP) TCPポート: 7229
- 暗号化された印刷Webサービス (HTTPS) TCPポート: 8443
- 暗号化された印刷データストリーム (CGP) TCPポート: 443

Universal Print ServerでXTEサービスが使用するポートを変更するには、管理者としてPowerShellで次のコマンドを実行します (Enable-UpsSsl.ps1 PowerShellスクリプトの使用に関する注意点については、後のセクションを参照してください):

1. `Stop-Service CitrixXTEServer, UpSvc`
2. `Enable-UpsSsl.ps1 -Enable -HTTPSPort <port> -CGPSSLPort <port>` または `Enable-UpsSsl.ps1 -Disable -HTTPPort <port> -CGPPort <port>`
3. `Start-Service CitrixXTEServer`

ユニバーサルプリントサーバーでのTLS設定

負荷分散構成で複数の Universal Print Server を使用している場合は、すべての Universal Print Server で TLS 設定が一貫して構成されていることを確認してください。

Universal Print Server で TLS を構成すると、インストールされている TLS 証明書のアクセス許可が変更され、Universal Printing Service に証明書の秘密キーへの読み取りアクセス権が付与され、Universal Printing Service に次の情報が通知されます。

- TLSに使用する証明書ストア内の証明書。
- TLS接続に使用するTCPポート番号。

Windowsファイアウォール (有効な場合) は、これらのTCPポートでの受信接続を許可するように構成する必要があります。この構成は、Enable-UpsSsl.ps1 PowerShellスクリプトを使用すると自動的に行われます。

- 許可するTLSプロトコルのバージョン。

Universal Print Server は、TLS プロトコルバージョン 1.2、1.1、1.0 をサポートしています。許可される最小バージョンを指定します。

デフォルトのTLSプロトコルバージョンは1.2です。

- 許可するTLS暗号スイート。

暗号スイートは、接続に使用される暗号化アルゴリズムを選択します。VDA と Universal Print Server は、異なる暗号スイートのセットをサポートできます。VDA が接続してサポートされている TLS 暗号スイートのリストを送信すると、Universal Print Server はクライアントの暗号スイートの 1 つを、構成されている暗号スイートの独自のリスト内の暗号スイートの 1 つと照合し、接続を受け入れます。一致する暗号スイートがない場合、Universal Print Server は接続を拒否します。

Universal Print Server は、OPEN、FIPS、および SP800-52 ネイティブ Crypto Kit モード用に、GOV (政府機関向け)、COM (商用)、ALL と名付けられた次の暗号スイートのセットをサポートしています。許容される暗号スイートは、「**SSL FIPS モード**」ポリシー設定と Windows FIPS モードにも依存します。Windows FIPS モードの詳細については、この Microsoft サポート技術情報 を参照してください。

暗号スイート（優先順位の降順）	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
TLS_ECDHE_RSA_AES256_GCM_SHA384	X		X	X		X	X		X
TLS_ECDHE_RSA_AES256_CBC_SHA384	X		X	X		X	X		X
TLS_ECDHE_RSA_AES256_CBC_SHA	X	X		X	X		X	X	

PowerShellスクリプトを使用してUniversal Print ServerでTLSを構成する

証明書ストアの**ローカルコンピューター > 個人 > 証明書**領域にTLS証明書をインストールします。その場所に複数の証明書がある場合は、証明書のサムプリントを`Enable-UpsSsl.ps1` PowerShellスクリプトに指定します。

> **注：**
>
> PowerShellスクリプトは、Universal Print ServerのFQDNに基づいて正しい証明書を見つけます。Universal Print ServerのFQDNに対して単一の証明書のみが存在する場合、証明書のサムプリントを指定する必要はありません。

> `Enable-UpsSsl.ps1`スクリプトは、VDAからUniversal Print ServerへのTLS接続を有効または無効にします。このスクリプトは、インストールメディアの**Support > Tools > SslSupport**フォルダーにあります。

TLS を有効にすると、スクリプトは Universal Print Server の TCP ポートに対する既存の Windows ファイアウォール規則をすべて無効にします。次に、XTE サービスが TLS TCP および UDP ポートでのみ受信接続を受け入れることを許可する新しい規則を追加します。また、次の Windows ファイアウォール規則も無効にします。

- クリアテキスト印刷Webサービス接続 (デフォルト: 8080)
- クリアテキスト印刷データストリーム (CGP) 接続 (デフォルト: 7229)

その結果、VDAはTLSを使用している場合にのみこれらの接続を行うことができます。

> **注：**
>
> TLSを有効にしても、VDAからUniversal Print ServerへのWindows Print Spooler RPC/SMB接続には影響しません。

> **重要:**
>
> 最初のパラメーターとして「**Enable**」または「**Disable**」を指定します。ローカルコンピューターの個人証明書ストアに Universal Print Server の FQDN を持つ証明書が 1 つしかない場合、CertificateThumbprint パラメーターはオプションです。その他のパラメーターはオプションです。

構文

```
Enable-UpsSSL.ps1 -Enable [-HTTPPort &lt;port&gt;] [-CGPPort &lt;port&gt;] [-HTTPSPort &lt;port&gt;] [-CGPSSLPort &lt;port&gt;] [-SSLMinVersion &lt;version&gt;] [-SSLCipherSuite &lt;name&gt;] [-CertificateThumbprint &lt;thumbprint&gt;] [-FIPSMode &lt;Boolean&gt;] [-ComplianceMode &lt;mode&gt;]

Enable-UpsSSL.ps1 -Disable [-HTTPPort &lt;portnum&gt;] [-CGPPort &lt;portnum&gt;]
```

パラメーター	説明
有効にする	XTEサーバーでSSL/TLSを有効にします。このパラメーターまたはDisableパラメーターのいずれかが必要です。
無効にする	XTEサーバーでSSL/TLSを無効にします。このパラメーターまたはEnableパラメーターのいずれかが必要です。
CertificateThumbprint `"<thumbprint>"`	ローカルコンピューターの個人証明書ストアにあるTLS証明書のサムプリント。引用符で囲みます。スクリプトは、指定されたサムプリントを使用して、使用する証明書を選択します。
HTTPポート `<port>`	クリアテキスト印刷Webサービス (HTTP/SOAP) ポート。デフォルト: 8080
CGPポート `<port>`	クリアテキスト印刷データストリーム (CGP) ポート。デフォルト: 7229
HTTPSポート `<port>`	暗号化された印刷Webサービス (HTTPS/SOAP) ポート。デフォルト: 8443
CGP SSL ポート `<port>`	暗号化された印刷データストリーム (CGP) ポート。デフォルト: 443
SSLMinVersion `"<version>"`	最小 TLS プロトコルバージョン。引用符で囲みます。有効な値: 「TLS_1.0」、「TLS_1.1」、「TLS_1.2」。デフォルト: TLS_1.2。

パラメーター	説明
SSLCipherSuite `“<name>”`	TLS 暗号スイートパッケージの名前。引用符で囲みます。有効な値: 「GOV」、「COM」、「ALL」（デフォルト）。
FIPS モード `<Boolean>`	XTEサーバーでFIPS 140モードを有効または無効にします。有効な値: FIPS 140モードを有効にする場合は$true、FIPS 140モードを無効にする場合は$false。

例

次のスクリプトは TLS を有効にします。サムプリント（この例では「12345678987654321」として表されます）は、使用する証明書を選択するために使用されます。

```
Enable-UpsSsl.ps1 –Enable -CertificateThumbprint "12345678987654321"
```

次のスクリプトはTLSを無効にします。

```
Enable-UpsSsl.ps1 –Disable
```

FIPSモードの構成

米国連邦情報処理標準（FIPS）モードを有効にすると、Universal Print Serverの暗号化された接続にはFIPS 140準拠の暗号化のみが使用されるようになります。

クライアントでFIPSモードを構成する前に、サーバーでFIPSモードを構成してください。

Windows FIPS モードの有効化/無効化については、Microsoft のドキュメントサイトを参照してください。

クライアントでのFIPSモードの有効化

Delivery Controller™ で Citrix Studio を実行し、Citrix ポリシー設定の **SSL FIPS モード** を **有効** に設定します。Citrix ポリシーを有効にします。

各VDAで以下を実行します。

1. Windows FIPSモードを有効にします。
2. VDAを再起動します。

サーバーでのFIPSモードの有効化

各Universal Print Serverで以下を実行します。

1. Windows FIPSモードを有効にします。
2. 管理者としてこのPowerShellコマンドを実行します: `stop-service CitrixXTEServer, UpSvc`
3. `-Enable -FIPSMode $true` パラメーターを指定して、`Enable-UpsSsl.ps1` スクリプトを実行します。
4. Universal Print Serverを再起動します。

クライアントでのFIPSモードの無効化

Delivery Controller で Citrix Studio を実行し、Citrix ポリシー設定の **SSL FIPS モード** を **無効** に設定します。Citrix ポリシーを有効にします。**SSL FIPS モード** の Citrix ポリシー設定を削除することもできます。

各VDAで以下を実行します:

1. Windows FIPSモードを無効にします。
2. VDAを再起動します。

サーバーでのFIPSモードの無効化

各Universal Print Serverで以下を実行します:

1. Windows FIPSモードを無効にします。
2. 管理者としてこのPowerShellコマンドを実行します: `stop-service CitrixXTEServer, UpSvc`
3. `-Enable -FIPSMode $false` パラメーターを指定して、`Enable-UpsSsl.ps1` スクリプトを実行します。
4. Universal Print Serverを再起動します。

SSL/TLSプロトコルバージョンの構成

デフォルトの SSL/TLS プロトコルバージョンは TLS 1.2 です。TLS 1.2 は、本番環境での使用が推奨される唯一の SSL/TLS プロトコルバージョンです。トラブルシューティングのために、非本番環境で SSL/TLS プロトコルバージョンを一時的に変更する必要がある場合があります。

SSL 2.0およびSSL 3.0は、Universal Print Serverではサポートされていません。

サーバーでのSSL/TLSプロトコルバージョンの設定

各Universal Print Serverで以下を実行します。

1. 管理者としてこのPowerShellコマンドを実行します: `stop-service CitrixXTEServer, UpSvc`
2. `-Enable -SSLMinVersion` バージョンパラメーターを指定して `Enable-UpsSsl.ps1` スクリプトを実行します。テストが完了したら、これを TLS 1.2 に戻すことを忘れないでください。
3. Universal Print Serverを再起動します。

クライアントでのSSL/TLSプロトコルバージョンの設定

各VDAで以下を実行します。

1. Delivery Controllerで、**SSLプロトコルバージョン**ポリシー設定を目的のプロトコルバージョンに設定し、ポリシーを有効にします。
2. Microsoft サポート記事の TLS Registry Settings には、Microsoft SCHANNEL SSP のレジストリ設定が記載されています。レジストリ設定を使用して、クライアント側の **TLS 1.0、TLS 1.1、または TLS 1.2** を有効にします。

   > **重要:**
   >
   > テストが完了したら、レジストリ設定を元の値に戻すことを忘れないでください。

3. VDAを再起動します。

トラブルシューティング

接続エラーが発生した場合は、Universal Print Server の C:\Program Files (x86)\Citrix\XTE\logs\error.log ログファイルを確認してください。

SSL/TLSハンドシェイクが失敗した場合、このログファイルにエラーメッセージ**SSL handshake from client failed**が表示されます。このような失敗は、VDAとUniversal Print ServerのSSL/TLSプロトコルバージョンが一致しない場合に発生する可能性があります。

Universal Print Serverのホスト名を含む以下のポリシー設定で、Universal Print ServerのFQDNを使用します。

- セッションプリンター
- プリンターの割り当て
- 負荷分散用のUniversal Print Server

Universal Print ServerとVDAでシステムクロック（日付、時刻、タイムゾーン）が正しいことを確認してください。

仮想チャネルのセキュリティ

デフォルトでは、仮想チャネル許可リスト機能が有効になっています。その結果、Citrix®仮想チャネルのみが仮想アプリおよびデスクトップセッションで開くことが許可されます。自社製またはサードパーティ製のカスタム仮想チャネルを使用する必要がある場合は、それらを明示的に許可リストに追加する必要があります。

仮想チャネルを許可リストに追加する

仮想チャネルを許可リストに追加するには、次のものが必要です。

1. コードで定義されている仮想チャネル名。最大7文字です。例: `CTXCVC1`。
2. VDAマシン上で仮想チャネルを開くプロセスのパス。例: `C:\Program Files\Application\run.exe`。

必要な情報が揃ったら、仮想チャネル許可リストポリシー設定を使用して、仮想チャネルを許可リストに追加する必要があります。仮想チャネルをリストに追加するには、仮想チャネル名の後にコンマを入力し、次に仮想チャネルにアクセスするプロセスのパスを入力します。複数のプロセスがある場合は、コンマで区切って追加できます。

> **注：**
>
> ポリシーを変更した後、変更を有効にするためにVDAを再起動してください。

> 前の例を使用して、次をリストに追加します。

```
CTXCVC1,C:\Program Files\Application\run.exe
```

複数のプロセスがある場合は、次をリストに追加します。

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application\run2.exe
```

Citrix仮想チャネルに関する考慮事項

すべての組み込みCitrix仮想チャネルは信頼されており、追加の設定なしで開くことが許可されています。ただし、外部依存関係のため、許可リストに明示的なエントリを必要とする2つの機能があります。

- マルチメディアリダイレクト
- ビジネス向け Skype 用 HDX™ リアルタイム最適化パック

マルチメディアリダイレクト

許可リストのエントリには、次の情報が必要です。

- 仮想チャネル名: CTXMM
- プロセス: VDAマシンで使用されるメディアプレーヤーへのパス。例: C:\Program Files (x86)\Windows Media Player\wmplayer.exe
- 許可リストエントリ: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

スカイプ フォー ビジネス 用 HDX RealTime Optimization Pack

許可リストのエントリには、次の情報が必要です。

- 仮想チャネル名: CTXRMEP
- プロセス: VDAマシン上のSkype for Business実行可能ファイルへのパス。これはSkype for Businessのバージョンや、カスタムインストールパスを使用したかどうかによって異なる場合があります。例: C:\Program Files\Microsoft Office\root\Office16\lync.exe。
- 許可リストエントリ: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

仮想チャネル名とプロセスの取得

VDAマシン上で仮想チャネル名とその仮想チャネルを開くプロセスを取得する最も簡単な方法は、その仮想チャネルを提供した開発者またはサードパーティベンダーから情報を入手することです。

または、この情報は、機能のログを適用し、以下の手順に従うことで取得できます。

1. カスタム仮想チャネルのクライアントおよびサーバーコンポーネントが配置されたら、仮想アプリケーションまたは仮想デスクトップを起動します。

2. VDAマシンのシステムイベントログで、次のイベントからカスタム仮想チャネル名を探します。
   - シングルセッションVDAでは、ソースPicaddからのイベントID 2004。
   - マルチセッションVDAでは、ソースRpmからのイベントID 16。
3. セッションからログオフします。
4. 識別された仮想チャネルに対して、仮想チャネル名のみで仮想チャネル許可リストポリシー設定にエントリを追加します。
5. VDAを再起動します。
6. 仮想アプリケーションまたは仮想デスクトップを再度起動します。
7. VDAマシンのシステムイベントログで、次のイベントから仮想チャネルを開こうとしたプロセスを探します。
   - シングルセッションVDAでは、ソースPicaddからのイベントID 2002。
   - マルチセッションVDAでは、ソースRpmからのイベントID 14。
8. セッションからログオフします。
9. 識別されたプロセスを含めるように、仮想チャネル許可リストポリシー設定のエントリを編集します。
10. VDAを再起動します。
11. カスタム仮想チャネルが正常に開くことを検証するために、仮想アプリケーションまたは仮想デスクトップを起動します。

仮想チャネル許可リストのログ記録

シングルセッションVDAマシンのイベントログには、次のイベントが記録されます。

ログ名	システム
ID	2001
送信元	ピックアップド
レベル	情報
説明	カスタム仮想チャネル `<vcName>` はプロセス `<processName>` によって開かれました

ログ名	システム
ID	2002
送信元	ピックアッド
レベル	警告
説明	カスタム仮想チャネル `<vcName>` はプロセス `<processName>` によって開くことができません

ログ名	システム
ID	2003
送信元	ピックアッド
レベル	情報
説明	`<username>` がカスタム仮想チャネル `<vcName>` を開きました

ログ名	システム
ID	2004
送信元	ピックアッド
レベル	警告
説明	`<username>` がカスタム仮想チャネル `<vcName>` を開こうとしました

マルチセッションVDAマシンのイベントログには、次のイベントが記録されます。

ログ名	システム
ID	13
送信元	Rpm

レベル	情報
説明	カスタム仮想チャネル `<vcName>` はプロセス `<processName>` によって開かれました

ログ名	システム
ID	14
送信元	Rpm
レベル	警告
説明	カスタム仮想チャネル `<vcName>` はプロセス `<processName>` によって開くことができません

ログ名	システム
ID	15
送信元	Rpm
レベル	情報
説明	`<username>` がカスタム仮想チャネル `<vcName>` を開きました

ログ名	システム
ID	16
送信元	Rpm
レベル	警告
説明	`<username>` がカスタム仮想チャネル `<vcName>` を開こうとしました

既知のサードパーティ仮想チャネル

以下は、カスタムCitrix仮想チャネルを使用する既知のサードパーティソリューションです。このリストには、カスタムCitrix仮想チャネルを使用するすべてのソリューションが含まれているわけではありません。

- カーナー
- シスコ Webex Teams
- シスコ ウェブエックス ミーティングス バーチャルデスクトップ ソフトウェア
- エピック ワープドライブ
- ミッドマーク IQPath クライアント拡張機能
- ニュアンス PowerMic クライアント拡張機能
- ニュアンス ドラゴン メディカル ネットワーク エディション 360 vSync
- VDI向けZoomミーティング

関連する仮想チャネルを許可リストに追加するための詳細については、ソリューションのベンダーにお問い合わせください。または、仮想チャネル名とプロセスの取得セクションに記載されている手順に従ってください。

フェデレーション認証サービス

Citrix Federated Authentication Service (FAS) は、SAML や OpenID Connect (OIDC) などの最新のIDプロバイダーを介してユーザーが認証し、Windowsパスワードを提供しない環境において、Citrix仮想デスクトップおよびアプリケーションへのシングルサインオン (SSO) を可能にし、Active Directoryドメインに参加しているセッションホストへのシームレスなアクセスを保証します。

フェデレーション認証サービスを使用して展開を保護する方法の詳細については、フェデレーション認証サービス ドキュメントを参照してください。

デバイス

HDX™は、あらゆる場所のあらゆるデバイスで高精細なユーザーエクスペリエンスを提供します。デバイスセクションの記事では、以下のデバイスについて説明します。

- 汎用USBデバイス
- モバイルおよびタッチスクリーンデバイス
- シリアルデバイス
- 特殊キーボード
- TWAINデバイス
- Webカメラ
- WIAデバイス

最適化されたUSBデバイスと汎用USBデバイス

最適化されたUSBデバイスとは、Citrix Workspace™アプリが特定のサポートを提供しているデバイスです。たとえば、HDXマルチメディア仮想チャネルを使用してWebカメラをリダイレクトする機能などです。汎用デバイスとは、Citrix Workspaceアプリで特定のサポートがないUSBデバイスです。

デフォルトでは、汎用USBリダイレクトは、汎用モードに設定しない限り、最適化された仮想チャネルサポートを持つUSBデバイスをリダイレクトできません。

一般的に、USBデバイスは汎用モードよりも最適化モードの方が優れたパフォーマンスを発揮します。ただし、最適化モードではUSBデバイスが完全な機能を持たない場合があります。その機能に完全にアクセスするには、汎用モードに切り替える必要があるかもしれません。

USB大容量記憶装置では、Citrix®ポリシーによって制御されるクライアントドライブマッピングまたは汎用USBリダイレクト、あるいはその両方を使用できます。主な違いは次のとおりです。

汎用USBリダイレクトとクライアントドライブマッピングポリシーの両方が有効になっていて、セッション開始前または開始後にマスストレージデバイスが挿入された場合、そのデバイスはクライアントドライブマッピングを使用してリダイレクトされます。

これらの条件が真の場合、マスストレージデバイスは汎用USBリダイレクトを使用してリダイレクトされます。

- 汎用USBリダイレクトとクライアントドライブマッピングポリシーの両方が有効になっている。
- デバイスが自動リダイレクト用に構成されている。
- セッション開始前または開始後にマスストレージデバイスが挿入される。

詳細については、`<http://support.citrix.com/article/CTX123015>`を参照してください。

機能	クライアントドライブマッピング	汎用USBリダイレクト
デフォルトで有効	はい	いいえ
読み取り専用アクセスを構成可能	はい	いいえ
暗号化されたデバイスアクセス	はい、仮想セッションでデバイスにアクセスする前に暗号化が解除されている場合。	シトリックス バーチャル デスクトップ™ のみ

マルチモニターでのDPIの混在

Citrix Virtual Apps and Desktops環境では、モニター間で異なるDPIを使用することはサポートされていません。DPI（%スケーリング）は、Windowsのコントロールパネル > ディスプレイオプションで確認できます。Windows 8.1またはWindows 10のクライアントデバイスを使用している場合、Windowsのコントロールパネル > ディスプレイオプションで**「すべてのディスプレイで1つの拡大/縮小レベルを選択する」オプション**を有効にすると、モニターが適切に構成されます。詳しくは、Knowledge Centerの記事CTX201696を参照してください。

マップされたクライアントドライブ

セキュリティ上の予防措置として、ユーザーがCitrix Virtual Apps and Desktopsにログオンすると、デフォルトで、サーバーはユーザーの実行権限なしでクライアントドライブをマップします。マップされたクライアントドライブにある実行可能ファイルをユーザーが実行できるようにするには、サーバーのレジストリを編集してこのデフォルト設定を上書きします。レジストリ設定の詳細については、レジストリを介して管理される機能のリストにあるマップされたクライアントドライブを参照してください。

Citrix Virtual Apps and Desktops™ 7 2006は、このレジストリの場所を含む最初のバージョンです。以前のバージョンのCitrix Virtual Apps and Desktopsでは、異なるレジストリの場所が使用されていました。

汎用USBデバイス

HDX™テクノロジーは、ほとんどの一般的なUSBデバイスに**最適化されたサポート**を提供します。これらのデバイスには以下が含まれます。

- モニター
- マウス
- キーボード
- VoIP電話
- ヘッドセット
- Webカメラ
- スキャナー
- カメラ
- プリンタ
- ドライブ
- スマートカードリーダー
- ペンタブレット
- 署名パッド

最適化されたサポートは、WAN経由でパフォーマンスと帯域幅の効率を向上させ、ユーザーエクスペリエンスを改善します。最適化されたサポートは、特に高遅延またはセキュリティに敏感な環境において、通常は最良の選択肢です。

HDXテクノロジーは、最適化されたサポートがない、または不適切な特殊デバイス向けに**汎用USBリダイレクト**を提供します。汎用USBリダイレクトの詳細については、「汎用USBリダイレクト」を参照してください。

USBデバイスとCitrix Workspaceアプリ for Windowsの詳細については、複合USBデバイスリダイレクトの構成およびUSBサポートの構成を参照してください。

モバイルおよびタッチスクリーンクライアントデバイスのサポート

Citrix Virtual Apps and Desktops™ を使用すると、ユーザーは公開されたアプリケーションやデスクトップにモバイルおよびタッチスクリーンクライアントデバイスからアクセスできます。

要件

Citrix® コントロールプレーン

- シトリックス バーチャル アプリケーションズ アンド デスクトップ 7.15 以降
- シトリックス DaaS™

セッションホスト

- オペレーティングシステム
  - Windows 10 1903 以降
  - ウィンドウズ サーバー 2016 以降
- VDA
  - Windows: バージョン 7.15 以降

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
- Windows版 Citrix Workspace™ アプリ バージョン1808以降

Windows Continuum を使用するタッチスクリーンデバイスのタブレットモード

Continuum は、クライアントデバイスの使用方法に適応する Windows 10 の機能です。VDA は、タッチ対応クライアントでキーボードまたはマウスの存在を検出すると、クライアントをデスクトップモードにします。キーボードまたはマウスが存在しない場合、VDA はクライアントをタブレット/モバイルモードにします。この検出は、セッションの接続時および再接続時、ならびにセッション中にキーボードまたはマウスが接続または切断されたときに発生します。

この機能はデフォルトで有効になっています。この機能を無効にするには、ポリシー設定タブレットモード切り替えポリシー設定を構成します。

上記のタッチスクリーンデバイスの要件に加えて、Windows Continuumには以下が必要です。

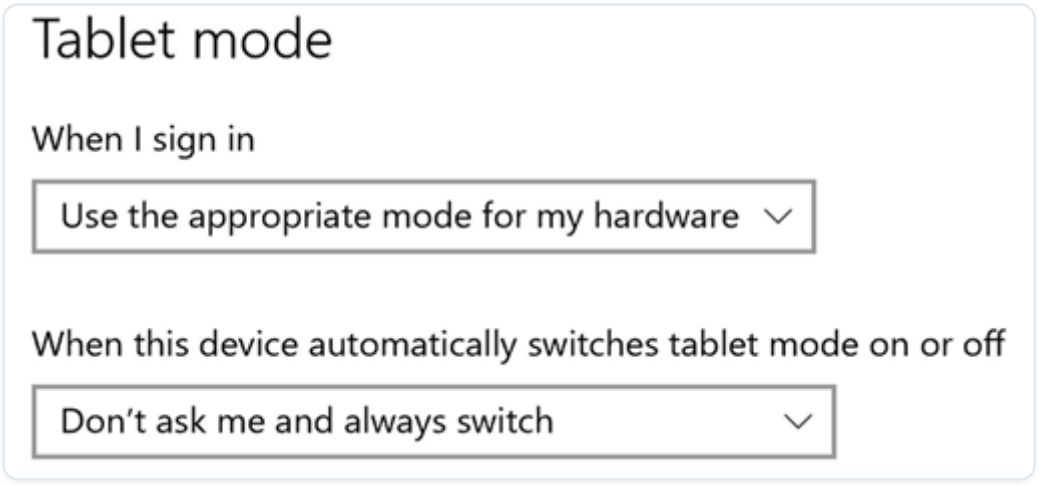
シトリックス ハイパーバイザー™

- シトリックス ハイパーバイザー 8.2 以降
- ラップトップ/タブレットの切り替えを許可するには、XenServer CLIコマンドを実行します。
  xe vm-param-set uuid=\<VM_UUID\> platform:acpi_laptop_slate=1

> **重要:**
>
> メタデータ設定を変更した後に既存のマシンカタログのベースイメージを更新しても、以前にプロビジョニングされたVMには影響しません。XenServer VMのベースイメージを変更した後、カタログを作成し、ベースイメージを選択して、新しいMachine Creation Services™ (MCS) マシンをプロビジョニングします。

セッションホスト

- オペレーティングシステム
  - Windows 10 1903 以降
  - ウィンドウズ 11
- VDA
  - Windows: バージョン 7.16 以降
  - **現在のオペレーティングシステム構成の制限により、ユーザーは最初のICA®セッションを開始してVDAを再起動した後、ドロップダウンメニューから以下のオプションを設定する必要があります。**
    - **設定 > システム > タブレットモード**
      - ハードウェアに適したモードを使用する
      - 常に切り替える（確認しない）



タブレットモードは、タッチスクリーンにより適したユーザーインターフェイスを提供します。

- ボタンが少し大きくなります。
- スタート画面と起動するすべてのアプリが全画面で開きます。
- タスクバーに「戻る」ボタンが含まれます。
- タスクバーからアイコンが削除されます。

ファイルエクスプローラーにアクセスできます。



Windows 10 は、この更新された BIOS に基づいて、ターゲット仮想マシンに GPIO ドライバーをロードします。これは、仮想マシン内でタブレットモードとデスクトップモードを切り替えるために使用されます。

HTML5 用 Citrix Workspace アプリは、Windows Continuum 機能をサポートしていません。

デスクトップモードは、PCとキーボード、マウスを使用するのと同じ方法で操作する従来のユーザーインターフェイスを提供します。

マイクロソフト Surface Pro および Surface Book ペン

Windows Inkベースのアプリケーションで標準のペン機能をサポートしています。サポートには、ポインティング、消去、ペン圧、Bluetooth信号、およびオペレーティングシステムのファームウェアとペンモデルに応じたその他の機能が含まれます。例えば、ペン圧は最大4096レベルまで可能です。この機能はデフォルトで有効になっています。

ペン機能のサポートに関する要件は次のとおりです。

Citrixコントロールプレーン

- Citrix Virtual Apps and Desktops のバージョン1903以降
- シトリックス DaaS

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - ウィンドウズ サーバー 2016 以降
  - ウィンドウズ 11
- VDA
  - Windows: バージョン1903以降

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
- Windows 用 Citrix Workspace アプリ バージョン 1902 以降

Windows Ink とペンの機能のデモンストレーションについては、このグラフィックをクリックしてください。



この機能を無効または有効にするには、レジストリを介して管理される機能のリストにある Microsoft Surface Pro および Surface Book のペン を参照してください。

既知の問題

ペンサポートに関する既知の問題は次のとおりです。

- Windows Server 2k22 の OS 制限により、2k22 サーバーアプリケーションまたはデスクトップに接続している場合、ユーザーはペンのショートカットを設定したり、コントロールパネルでペン/インクの設定を調整したりすることはできません。
- OS の制限により、ペン対応の Windows 11 クライアントからのペンのショートカットは認識されません。

シリアルポート

ほとんどの新しいPCには、内蔵のシリアル（COM）ポートがありません。USBコンバーターを使用すれば、これらのポートを簡単に追加できます。シリアルポートに適したアプリケーションには、センサー、コントローラー、古いチェックリーダー、パッドなどがよく含まれます。一部のUSB仮想COMポートデバイスは、Windowsが提供するドライバー（usbser.sys）の代わりに、ベンダー固有のドライバーを使用します。これらのドライバーを使用すると、USBデバイスの仮想COMポートを、異なるUSBソケットに接続しても変更されないように強制できます。これは、**デバイスマネージャー > ポート (COM と LPT) > プロパティ**から、またはデバイスを制御するアプリケーションから実行できます。

クライアントCOMポートマッピングを使用すると、ユーザーのエンドポイントのCOMポートに接続されたデバイスを仮想セッション中に使用できます。これらのマッピングは、他のネットワークマッピングと同様に使用できます。

各COMポートに対して、オペレーティングシステムのドライバーはCOM1やCOM2などのシンボリックリンク名を割り当てます。アプリケーションは、そのリンクを使用してポートにアクセスします。

> **重要:**

> デバイスがUSBを直接使用してエンドポイントに接続できるからといって、汎用USBリダイレクトを使用してリダイレクトできるとは限りません。一部のUSBデバイスは仮想COMポートとして機能し、アプリケーションは物理シリアルポートと同じ方法でアクセスできます。オペレーティングシステムはCOMポートを抽象化し、ファイル共有のように扱うことができます。仮想COMの一般的なプロトコルは、CDC ACMまたはMCTの2つです。RS-485ポートを介して接続した場合、アプリケーションがまったく機能しない可能性があります。RS-485をCOMポートとして使用するには、RS-485-to-RS232コンバーターを入手してください。
> **重要:**

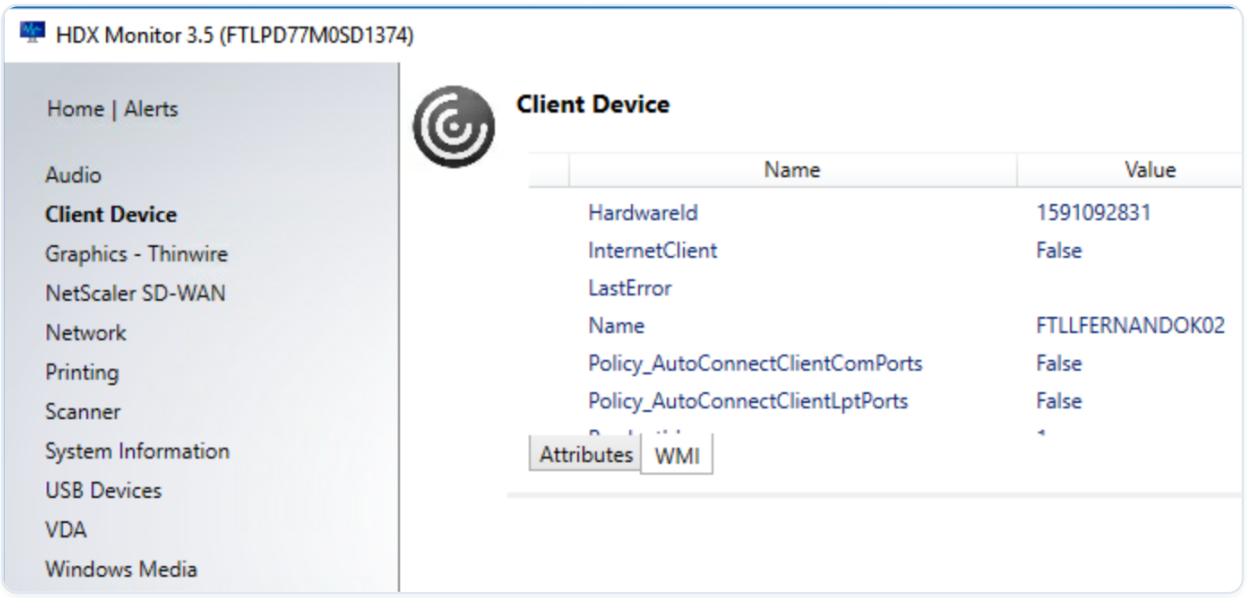
> 一部のアプリケーションは、デバイス（署名パッドなど）がクライアントワークステーションのCOM1またはCOM2に接続されている場合にのみ、一貫して認識します。

クライアントCOMポートをサーバーCOMポートにマッピングする

クライアントCOMポートをCitrix®セッションにマッピングするには、次の3つの方法があります。

- Studioポリシー。ポリシーの詳細については、「ポートリダイレクトポリシー設定」を参照してください。
- VDAコマンドプロンプト。
- リモートデスクトップ（ターミナルサービス）構成ツール。

1. **クライアントCOMポートリダイレクト**ポリシーと**クライアントCOMポートの自動接続Studio**ポリシーを有効にします。適用後、一部の情報はHDX™ Monitorで利用できます。



2. **クライアントCOMポートの自動接続**でポートのマッピングに失敗した場合は、手動でポートをマッピングするか、ログオンスクリプトを使用できます。VDAにログオンし、コマンドプロンプトウィンドウで次のように入力します。

   NET USE COMX: `\\CLIENT\COMZ`:

   または

   NET USE COMX: `\\CLIENT\CLIENTPORT:COMZ`:

   X はVDA上のCOMポートの番号です（ポート1～9がマッピングに利用可能です）。**Z** はマッピングするクライアントCOMポートの番号です。

操作が成功したことを確認するには、VDAのコマンドプロンプトで **NET USE** と入力します。表示されるリストには、マップされたドライブ、LPTポート、およびマップされたCOMポートが含まれます。



3. このCOMポートを仮想デスクトップまたはアプリケーションで使用するには、ユーザーデバイスアプリケーションをインストールし、マップされたCOMポート名を指定します。たとえば、クライアント上のCOM1をサーバー上のCOM3にマップする場合、VDAにCOMポートデバイスアプリケーションをインストールし、セッション中にCOM3を指定します。このマップされたCOMポートは、ユーザーデバイス上のCOMポートと同様に使用します。

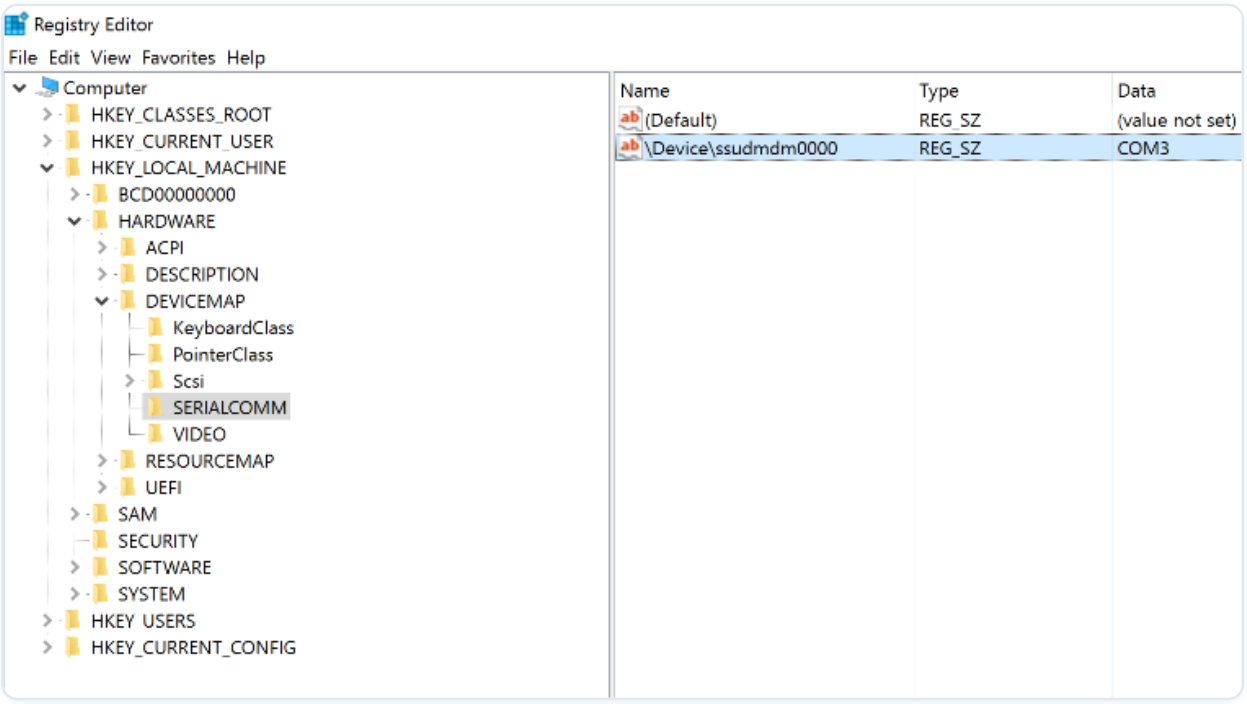
重要:

COMポートマッピングはTAPI互換ではありません。Windows Telephony Application Programming Interface (TAPI) デバイスをクライアントCOMポートにマップすることはできません。TAPIは、アプリケーションがデータ、FAX、音声通話の電話機能を制御するための標準的な方法を定義します。TAPIは、ダイヤル、応答、通話終了などのシグナリングを管理します。また、保留、転送、会議通話などの付加サービスも管理します。

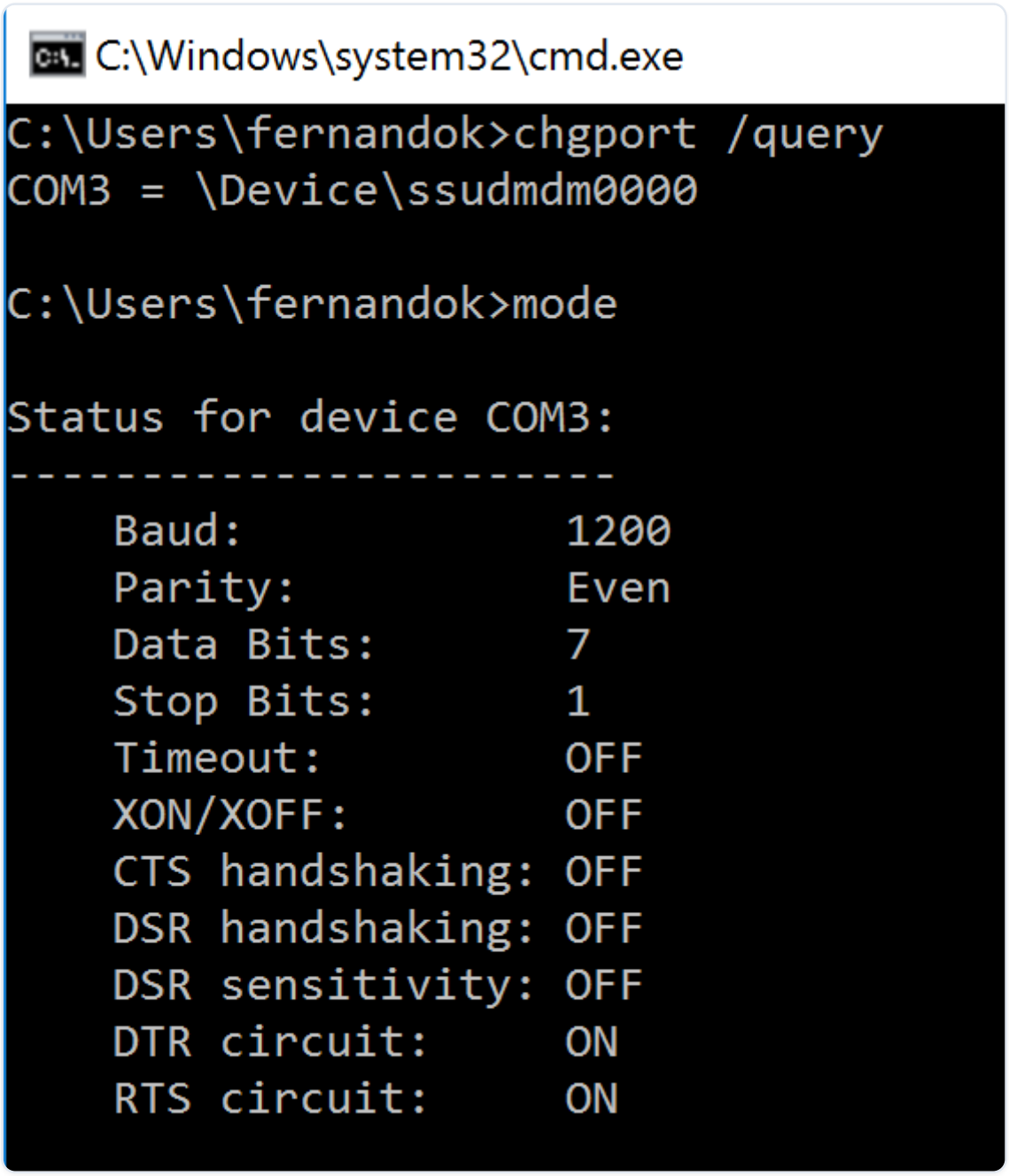
トラブルシューティング

1. Citrixをバイパスして、エンドポイントからデバイスに直接アクセスできることを確認してください。ポートがVDAにマップされていない間は、Citrixセッションに接続されていません。デバイスに付属のトラブルシューティング手順に従い、まずローカルで動作することを確認してください。 シリアルCOMポートにデバイスが接続されると、ここに示されているハイブにレ

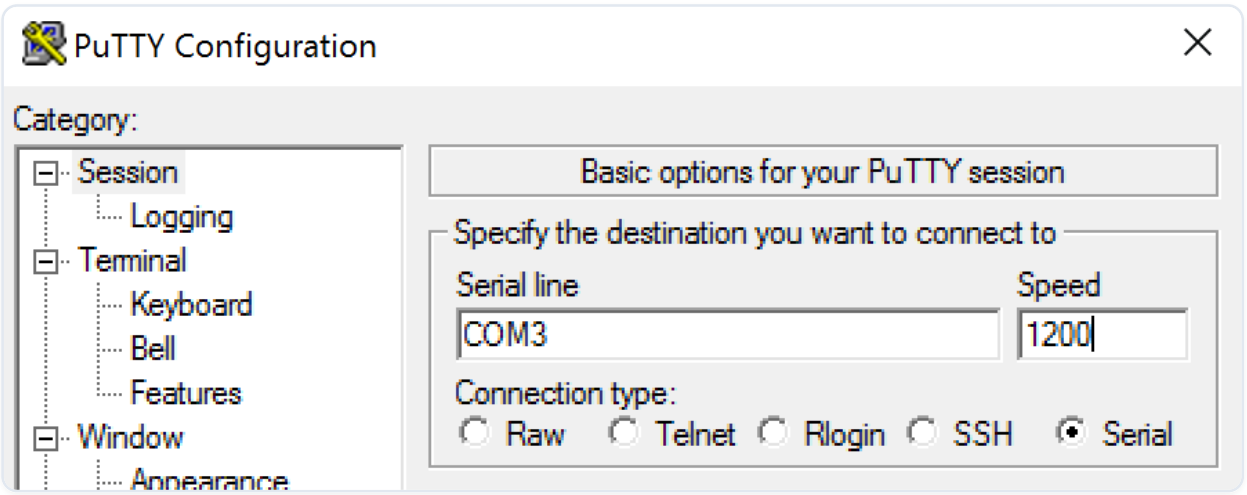
ジストリキーが作成されます。



この情報は、コマンドプロンプトで **chgport /query** を実行することでも確認できます。



デバイスのトラブルシューティング手順が利用できない場合は、PuTTYセッションを開いてみてください。**Session** を選択し、**Serial line** でCOMポートを指定します。



ローカルコマンドウィンドウで**MODE**を実行できます。出力には、使用中のCOMポートと、PuTTYセッションで必要となるボーレート/パリティ/データビット/ストップビットが表示される場合があります。PuTTY接続が成功した場合、**Enter**キーを押してデバイスからのフィードバックを確認します。入力した文字が画面に繰り返されたり、応答されたりする場合があります。この手順が失敗した場合、仮想セッションからデバイスにアクセスすることはできません。

2. ローカルのCOMポートをVDAにマップし (ポリシーまたは**NET USE COMX: `\\CLIENT\COMZ`:**を使用して)、前の手順と同じPuTTYの手順を繰り返しますが、今回はVDAのPuTTYから実行します。PuTTYがエラー「**Unable to open connection to COM1. Unable to open serial port**」を表示する場合、別のデバイスがCOM1を使用している可能性があります。

3. **chgport /query**を実行します。VDA上の組み込みWindowsシリアルドライバーが \Device\Serial0をVDAのCOM1ポートに自動割り当てしている場合、次の手順を実行します。
   A. VDAでCMDを開き、**NET USE**と入力します。

   B. VDA上の既存のマッピング（例：COM1）を削除します。

   NET USE COM1 /DELETE

   C. デバイスをVDAにマッピングします。

   NET USE COM1: `\\CLIENT\COM3`:

   D. VDA上のアプリケーションをCOM3にポイントします。

   最後に、ローカルのCOMポート (例: COM3) をVDA上の別のCOMポート (COM1以外、例: COM3) にマップしてみてください。アプリケーションがそれを指していることを確認してください: **NET USE COM3: `\\CLIENT\COM3`**

4. ポートがマッピングされていることが確認でき、PuTTYは動作しているもののデータが通過しない場合、それは競合状態である可能性があります。アプリケーションがマッピングされる前にポートに接続して開いてしまい、マッピングをロックしている可能性があります。次のいずれかを試してください。

   - 同じサーバーで公開されている2番目のアプリケーションを開きます。ポートがマッピングされるまで数秒待ち、その後、ポートを使用しようとする実際のアプリケーションを開きます。
   - Studioではなく、Active Directoryのグループポリシーエディターから COMポートリダイレクトポリシーを有効にします。これらのポリシーは「**Client COM port redirection**」と「**Auto connect client COM ports**」です。このように適用されたポリシーは、Studioポリ

シーよりも前に処理され、COMポートが確実にマッピングされるようにする可能性があります。CitrixポリシーはVDAにプッシュされ、次の場所に保存されます。
`HKLN\SOFTWARE\Policies\Citrix \<user session ID\>`

- ユーザーにこのログオンスクリプトを使用するか、アプリケーションを公開する代わりに、まずVDA上のマッピングを削除し、仮想COMポートを再マッピングしてからアプリケーションを起動する.batスクリプトを公開します。

@echo off NET USE COM1 /delete NET USE COM2 /delete NET USE COM1: `\\CLIENT\COM1`: NET USE COM2: `\\CLIENT\COM2`: MODE COM1: BAUD=1200 (または必要な値) MODE COM2: BAUD=9600 PARITY=N Data=8 Stop=1 (または必要な値) START C:\Program Files\\\<Your Software Path>\\\<your_software.exe>

5. SysinternalsのProcess Monitorは、最後の手段となるツールです。VDAでこのツールを実行する際、COM3、picaser.sys、CdmRedirectorなどのオブジェクト、特に\<your_app\>.exeを見つけてフィルターします。エラーは「アクセス拒否」またはそれに類するものとして表示される場合があります。

特殊キーボード

Bloombergキーボード

> **警告:**

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

> Citrix Virtual Apps and Desktops™は、Bloombergモデル5、モデル4 Starboardキーボード（およびそれ以前のモデル3）をサポートしています。このキーボードにより、金融業界のお客様は、キーボードの特殊機能を使用して金融市場データにアクセスし、迅速な取引を実行できます。

> **重要:**

> Bloombergキーボードは1つのセッションでのみ使用することをお勧めします。複数の同時セッション（1つのクライアントから複数のセッションへ）でキーボードを使用することはお勧めしません。

> Bloombergキーボードは、1つの物理シェルに複数のUSBデバイスを搭載したUSB複合デバイスです。

- キーボード。
- 指紋リーダー。
- 音量を上げ下げするキー、およびスピーカーとマイクをミュートするキーを備えたオーディオデバイス。このデバイスには、オンボードスピーカー、マイク、およびマイクとヘッドセット用のジャックが含まれています。
- これらすべてのデバイスをシステムに接続するためのUSBハブ。

要件:

- Citrix Workspace™ app for Windowsが接続するセッションは、USBデバイスをサポートしている必要があります。
- Bloombergキーボードモデル5をサポートするには、Citrix Workspace app 2207 for Linux以降が必要です。
- Bloombergキーボードモデル5をサポートするには、Citrix Workspace app 2109 for Windows以降が必要です。
- Bloombergキーボードモデル3および4をサポートするには、Citrix Workspace app 1808 for WindowsまたはCitrix Receiver for Windows 4.8以降が必要です。
- モデル4でKVMモード（2本のUSBケーブルのうち1本がKVMを介してルーティングされる）を使用するには、Citrix Workspace app 1808 for WindowsまたはCitrix Receiver for Windows 4.12以降が必要です。

Citrix Workspace app for WindowsでのBloombergキーボードの構成については、Bloombergキーボードの構成を参照してください。

Bloombergキーボードのサポートを有効にするには、レジストリを介して管理される機能のリストでBloombergキーボードを参照してください。

サポートを確認する:

Citrix WorkspaceアプリでBloombergキーボードのサポートが有効になっているかを確認するには、Desktop ViewerがBloombergキーボードのデバイスを正しく報告しているかを確認します。

デスクトップシナリオ:

Desktop Viewerを開きます。Bloombergキーボードのサポートが有効になっている場合、Desktop ViewerにはUSBアイコンの下に3つのデバイスが表示されます。

Bloomberg 5キーボードの場合:

- ブルームバーグLP ブルームバーグ生体認証モジュール
- Bloomberg LP Keyboard (2つのインターフェイスを持つ複合デバイス)
- Bloomberg LP Keyboard Audio (3つのインターフェイスを持つ複合デバイス)

Bloomberg 3および4キーボードの場合:

- ブルームバーグ指紋スキャナー
- ブルームバーグキーボード機能
- ブルームバーグLP キーボード 2013

シームレスアプリケーションのみのシナリオ:

Citrix Workspaceアプリの通知領域アイコンから**接続センター**メニューを開きます。Bloombergキーボードのサポートが有効になっている場合、3つのデバイスが**デバイス**メニューに表示されます。

これらの各デバイスのチェックマークは、それらがセッションにリモート接続されていることを示します。

TWAIN デバイス

要件

- スキャナーはTWAIN準拠である必要があります。
- TWAINドライバーをローカルデバイスにインストールします。サーバー上では必要ありません。
- スキャナーをローカルに接続します（例：USB経由）。
- スキャナーがWindowsイメージ取得サービスではなく、ローカルのTWAINドライバーを使用していることを確認してください。
- テストに使用されるユーザーアカウントに、ICA®セッション内の帯域幅を制限するポリシーが適用されていないことを確認してください。たとえば、クライアントUSBリダイレクト帯域幅制限などです。

ポリシー設定については、TWAINデバイスのポリシー設定を参照してください。

Webカメラ

高解像度Webカメラストリーミング

Webカメラは、仮想セッション内で実行されているビデオ会議アプリケーションで使用できます。サーバー上のアプリケーションは、サポートされているフォーマットタイプに基づいてWebカメラのフォーマットと解像度を選択します。セッションが開始されると、クライアントはWebカメラ情報をサーバーに送信します。ビデオ会議アプリケーションからWebカメラを選択します。Webカメラとアプリケーションの両方が高解像度レンダリングをサポートしている場合、アプリケーションは高解像度を使用します。Webカメラの解像度は最大1920x1080までサポートしています。

この機能には、Citrix Receiver for Windowsバージョン4.10以降が必要です。HDX Webカメラリダイレクトをサポートするアプリプラットフォームのリストについては、「Citrix Workspace app feature matrix」を参照してください。

高解像度Webカメラストリーミングの詳細については、「HDX video conferencing and webcam video compression」を参照してください。

レジストリキーを使用してこの機能を無効または有効にし、特定の解像度を構成できます。詳細については、レジストリで管理される機能のリストにある「High-definition webcam streaming and High-definition webcam resolution」を参照してください。

WIA デバイス

要件

- スキャナーはWIA準拠である必要があります。
- WIAドライバーをローカルデバイスにインストールします。サーバーには必要ありません。
- スキャナーをローカルに接続します（例：USB経由）。
- スキャナーがローカルのWindows Image Acquisitionサービスを使用しており、TWAINドライバーを使用していないことを確認してください。
- テストに使用されるユーザーアカウントに、ICA®セッション内の帯域幅を制限するポリシーが適用されていないことを確認してください。たとえば、クライアントUSBリダイレクト帯域幅制限などです。

Windows Image Acquisitionアプリケーションの許可リスト

許可リストを使用すると、VDA上のどのアプリケーションがWindows Image Acquisitionスキャナーリダイレクトにアクセスできるかを制御できます。レジストリエディターは、Windows Image Acquisitionを含む各VDAの許可リスト設定からの入力を使用します。デフォルトでは、どのアプリケーションもWindows Image Acquisitionにアクセスできません。

VDA上のアプリケーション向けにWindows Image Acquisitionを調整するには、レジストリで管理される機能のリストにあるWindows Image Acquisitionアプリケーション許可リスト設定を参照してください。

ポリシー設定については、「WIAデバイスポリシー設定」を参照してください。

グラフィックス

Citrix HDXグラフィックスには、Citrix Virtual Apps and Desktopsからのリッチグラフィックスアプリケーションの配信を最適化する、広範なグラフィックスアクセラレーションおよびエンコーディングテクノロジーが含まれています。これらのグラフィックテクノロジーは、グラフィックスを多用する仮想アプリケーションをリモートで操作する際に、物理デスクトップを使用するのと同じエクスペリエンスを提供します。

グラフィックスレンダリングには、ソフトウェアまたはハードウェアを使用できます。ソフトウェアレンダリングには、ソフトウェアラスタライザーと呼ばれるサードパーティライブラリが必要です。たとえば、WindowsにはDirectXベースのグラフィックス用のWARPラスタライザーが含まれています。場合によっては、代替のソフトウェアレンダラーを使用したいと思うかもしれません。ハードウェアレンダリング（ハードウェアアクセラレーション）には、グラフィックスプロセッサ（GPU）が必要です。

HDX™ Graphicsは、最も一般的なユースケース向けに最適化されたデフォルトのエンコーディング構成を提供します。Citrixポリシーを使用することで、IT管理者はさまざまなグラフィックス関連設定を構成して、さまざまな要件を満たし、望ましいユーザーエクスペリエンスを提供することもできます。

シンワイヤー

Thinwireは、Citrix Virtual Apps and Desktopsで使用されるCitrixのデフォルトのディスプレイリモートテクノロジーです。

ディスプレイリモートテクノロジーにより、あるマシンで生成されたグラフィックスを、通常はネットワーク経由で別のマシンに送信して表示できます。グラフィックスは、キーボード入力やマウス操作などのユーザー入力の結果として生成されます。

エイチディーエックス スリーディー プロ

Citrix Virtual Apps and DesktopsのHDX 3D Pro機能を使用すると、ハードウェアアクセラレーションにグラフィックス処理ユニット（GPU）を使用して最高のパフォーマンスを発揮するデスクトップとアプリケーションを配信できます。これらのアプリケーションには、OpenGLおよびDirectXベースの3Dプロフェッショナルグラフィックスアプリケーションが含まれます。標準VDAはDirectXのGPUアクセラレーションのみをサポートします。

WindowsシングルセッションOS向けGPUアクセラレーション

HDX 3D Proを使用すると、グラフィックスを多用するアプリケーションを、ホストされたデスクトップまたはシングルセッションOSマシン上のアプリケーションの一部として配信できます。HDX 3D Proは、物理ホストコンピューター（デスクトップ、ブレード、ラックワークステーションを含む）と、XenServer®、vSphere、Hyper-V（パススルーのみ）ハイパーバイザーが提供するGPUパススルーおよびGPU仮想化テクノロジーをサポートします。

GPUパススルーを使用すると、専用のグラフィックス処理ハードウェアに排他的にアクセスできるVMを作成できます。ハイパーバイザーに複数のGPUをインストールし、これらのGPUのそれぞれにVMを1対1で割り当てることができます。

GPU仮想化を使用すると、複数の仮想マシンが単一の物理GPUのグラフィックス処理能力に直接アクセスできます。

WindowsマルチセッションOS向けGPUアクセラレーション

HDX 3D Proを使用すると、WindowsマルチセッションOSセッションで実行されているグラフィックス負荷の高いアプリケーションを、サーバーのグラフィックス処理ユニット（GPU）でレンダリングできます。OpenGL、DirectX、Direct3D、およびWindows Presentation Foundation（WPF）のレンダリングをサーバーGPUに移行することで、グラフィックスレンダリングがサーバーCPUの速度を低下させることはありません。また、ワークロードがCPUとGPUに分割されるため、サーバーはより多くのグラフィックスを処理できます。

フレームホーク

> **重要:**
>
> Citrix Virtual Apps and Desktops 7 1903以降、Framehawkはサポートされなくなりました。代わりに、Thinwireをアダプティブトランスポートを有効にして使用してください。

> Framehawkは、ブロードバンドワイヤレス接続（Wi-Fiおよび4G/LTEセルラーネットワーク）を使用するモバイルワーカー向けのディスプレイリモートテクノロジーです。Framehawkは、スペクトル干渉やマルチパス伝播の課題を克服し、仮想アプリおよびデスクトップのユーザーにスムーズでインタラクティブなユーザーエクスペリエンスを提供します。

テキストベースのセッションウォーターマーク

テキストベースのセッションウォーターマークは、データ盗難を抑止し、追跡を可能にするのに役立ちます。この追跡可能な情報は、写真やスクリーンキャプチャを使用してデータを盗む者への抑止力として、セッションデスクトップに表示されます。テキストのレイヤーであるウォーターマークを指定できます。ウォーターマークは、元のドキュメントの内容を変更することなく、セッション画面全体に表示できます。テキストベースのセッションウォーターマークにはVDAのサポートが必要です。

関連情報

- HDX 3D プロ
- WindowsシングルセッションOSのGPUアクセラレーション
- WindowsマルチセッションOSのGPUアクセラレーション
- フレームホーク
- シンワイヤー
- テキストベースのセッションウォーターマーク(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/graphics/session-watermark.html)

HDX™ 3D プロ

Citrix Virtual Apps and Desktops™のHDX 3D Pro機能を使用すると、ハードウェアアクセラレーションのためにグラフィック処理ユニット（GPU）を使用すると最高のパフォーマンスを発揮するデスクトップとアプリケーションを提供できます。これらのアプリケーションには、OpenGLおよびDirectXベースの3Dプロフェッショナルグラフィックアプリケーションが含まれます。標準VDAは、DirectXのGPUアクセラレーションのみをサポートします。

HDX 3D Proポリシー設定については、「3Dグラフィックワークロードの最適化」(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/policies/reference/ica-policy-settings/graphics-policy-settings.html#optimize-for-3d-graphics-workload)を参照してください。

サポートされているすべてのCitrix Workspaceアプリは、3Dグラフィックで使用できます。複雑な3Dワークロード、高解像度モニター、マルチモニター構成、高フレームレートアプリケーションで最高のパフォーマンスを得るには、Citrix Workspace app for WindowsおよびCitrix Workspace app for Linuxの最新バージョンをお勧めします。Citrix Workspaceアプリのサポートされているバージョンに関する詳細については、Citrix Workspaceアプリのライフサイクルマイルストーンを参照してください。

3Dプロフェッショナルアプリケーションの例は次のとおりです。

- コンピューター支援設計、製造、エンジニアリング (CAD/CAM/CAE) アプリケーション
- 地理情報システム (GIS) ソフトウェア
- 医用画像処理通信システム (PACS)
- 最新のOpenGL、DirectX、NVIDIA CUDA、OpenCL、およびWebGLバージョンを使用するアプリケーション
- 並列コンピューティングにNVIDIA Compute Unified Device Architecture (CUDA) GPUを使用する計算集約型の非グラフィックアプリケーション

HDX 3D Proは、あらゆる帯域幅で最高のユーザーエクスペリエンスを提供します。

- WAN接続の場合：1.5 Mbpsという低い帯域幅のWAN接続でも、インタラクティブなユーザーエクスペリエンスを提供します。
- LAN接続の場合：LAN接続でローカルデスクトップと同等のユーザーエクスペリエンスを提供します。

  複雑で高価なワークステーションを、グラフィック処理をデータセンターに移動して一元管理することで、よりシンプルなユーザーデバイスに置き換えることができます。

HDX 3D Pro は、Windows シングルセッション OS マシンおよび Windows マルチセッション OS マシンに GPU アクセラレーションを提供します。詳細については、「GPU acceleration for Windows single-session OS」および「GPU acceleration for Windows multi-session OS」を参照してください。

HDX 3D Pro は、ベアメタルに加えて、以下のハイパーバイザーが提供する GPU パススルーおよび GPU 仮想化テクノロジーと互換性があります。

- シトリックス ハイパーバイザー™
  - NVIDIA GRID、AMD、および Intel GVT-d を使用した GPU パススルー
  - NVIDIA GRID、AMD、および Intel GVT-g を使用した GPU 仮想化
  - ハードウェアの互換性については、「Hypervisor Hardware Compatibility List」を参照してください。

HDX Monitor ツールを使用して、HDX 視覚化テクノロジーの動作と構成を検証し、HDX の問題を診断およびトラブルシューティングします。ツールのダウンロードと詳細については、`<https://taas.citrix.com/hdx/download/>` を参照してください。

WindowsマルチセッションOSのGPUアクセラレーション

HDX™ 3D Proを使用すると、WindowsマルチセッションOSセッションで実行されているグラフィックを多用するアプリケーションを、サーバーのグラフィック処理ユニット（GPU）でレンダリングできます。OpenGL、DirectX、Direct3D、およびWindows Presentation Foundation（WPF）のレンダリングをサーバーのGPUに移行することで、グラフィックレンダリングがサーバーのCPUを遅くすることはありません。また、ワークロードがCPUとGPUの間で分割されるため、サーバーはより多くのグラフィックを処理できます。

Windows Server はマルチユーザーオペレーティングシステムであるため、複数のユーザーが GPU 仮想化 (vGPU) を必要とせずに Citrix Virtual Apps™ によってアクセスされる GPU を共有できます。

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

GPU 共有

GPU 共有により、リモートデスクトップセッションで OpenGL および DirectX アプリケーションの GPU ハードウェアレンダリングが可能になります。次の特性があります。

- アプリケーションのスケーラビリティとパフォーマンスを向上させるために、ベアメタルまたは仮想マシンで使用できます。
- 複数の同時セッションで GPU リソースを共有できます (ほとんどのユーザーは専用 GPU のレンダリングパフォーマンスを必要としません)。
- 特別な設定は必要ありません。

GPU は、ハイパーバイザーおよび GPU ベンダーの要件に従って、フルパススルーモードまたは仮想 GPU (vGPU) モードのいずれかで Windows Server 仮想マシンに割り当てることができます。物理 Windows Server マシンへのベアメタル展開もサポートされています。

GPU 共有は、特定のグラフィックカードに依存しません。

- 仮想マシンの場合、使用しているハイパーバイザーと互換性のあるグラフィックカードを選択してください。Citrix Hypervisorのハードウェア互換性リストについては、「Hypervisor Hardware Compatibility List」を参照してください。

- ベアメタルで実行する場合、オペレーティングシステムによって単一のディスプレイアダプターが有効になっていることを推奨します。複数の GPU がハードウェアにインストールされている場合は、デバイスマネージャーを使用して、1 つを除くすべてを無効にしてください。

GPU Sharing を使用したスケーラビリティは、いくつかの要因によって異なります。

- 実行されているアプリケーション
- 消費するビデオ RAM の量
- グラフィックカードの処理能力

一部のアプリケーションは、他のアプリケーションよりもビデオ RAM の不足をうまく処理します。ハードウェアが過負荷になると、グラフィックカードドライバーの不安定化やクラッシュが発生する可能性があります。このような問題を回避するには、同時ユーザー数を制限してください。

GPUアクセラレーションが機能していることを確認するには、GPU-Zなどのサードパーティツールを使用します。GPU-Zは`<http://www.techpowerup.com/gpuz/>`で入手できます。

- NVIDIA GPUおよびIntel Iris Proグラフィックプロセッサ用の高性能ビデオエンコーダーへのアクセス。ポリシー設定（デフォルトで有効）がこの機能を制御し、H.264エンコーディング（利用可能な場合）にハードウェアエンコーディングの使用を許可します。このようなハードウェアが利用できない場合、VDAはソフトウェアビデオコーデックを使用したCPUベースのエンコーディングにフォールバックします。詳しくは、「グラフィックポリシー設定」を参照してください。

DirectX、Direct3D、および WPF レンダリング

DirectX、Direct3D、および WPF レンダリングは、ディスプレイドライバーインターフェイス（DDI）バージョン 9ex、10、または 11 をサポートする GPU を搭載したサーバーでのみ利用できます。

- Windows Server 2008 R2では、DirectXおよびDirect3Dで単一のGPUを使用するために特別な設定は必要ありません。
- Windows Server 2012以降では、RDセッションホストサーバー上のRemote Desktop Services（RDS）セッションは、Microsoft Basic Render Driverをデフォルトのアダプターとして使用します。Windows Server 2012以降のRDSセッションでGPUを使用するには、グループポリシーの**ローカルコンピューターポリシー** \> **コンピューターの構成** \> **管理用テンプレート** \> **Windowsコンポーネント** \> **Remote Desktop Services** \> **リモートデスクトップセッションホスト** \> **リモートセッション環境**で、**すべてのRemote Desktop Servicesセッションにハードウェアのデフォルトグラフィックアダプターを使用する**設定を有効にします。

- WPF アプリケーションがサーバーの GPU を使用してレンダリングできるようにするには、Windows マルチセッション OS セッションを実行しているサーバーのレジストリに設定を作成します。レジストリ設定の詳細については、レジストリで管理される機能のリストにある「Windows Presentation Foundation (WPF) レンダリング」を参照してください。

CUDAまたはOpenCLアプリケーションのGPUアクセラレーション

ユーザーセッションで実行されているCUDAおよびOpenCLアプリケーションのGPUアクセラレーションは、デフォルトで無効になっています。

CUDAアクセラレーションPOC機能を使用するには、レジストリ設定を有効にします。詳細については、レジストリで管理される機能のリストにある「CUDAまたはOpenCLアプリケーションのGPUアクセラレーション」を参照してください。

Windowsシングルセッション OS向けGPUアクセラレーション

HDX 3D Pro を使用すると、グラフィックを多用するアプリケーションを、ホストされたデスクトップまたはシングルセッションOSマシン上のアプリケーションの一部として配信できます。HDX 3D Pro は、物理ホストコンピューター（デスクトップ、ブレード、ラックワークステーションを含む）と、Citrix Hypervisor™、vSphere、Nutanix、および Hyper-V（パススルーのみ）ハイパーバイザーが提供する GPU パススルーおよび GPU 仮想化テクノロジーをサポートします。

HDX™ 3D Proは以下の機能を提供します。

- WANおよびワイヤレスパフォーマンスを最適化するための、適応型H.264ベースまたはH.265ベースのディープ圧縮。HDX 3D Proは、エンコードのデフォルト圧縮技術としてCPUベースの全画面H.264圧縮を使用します。H.264によるハードウェアエンコードは、NVENCをサポートするNVIDIA、Intel、およびAMDのカードで使用されます。H.265によるハードウェアエンコードは、NVENCをサポートするNVIDIAのカードで使用されます。
- 特殊なユースケース向けのロスレス圧縮オプション。HDX 3D Proは、医療画像処理など、ピクセルパーフェクトなグラフィックが必要なアプリケーションをサポートするために、CPUベースのロスレスコーデックも提供します。真のロスレス圧縮は、より多くのネットワークリソースと処理リソースを消費するため、特殊なユースケースでのみ推奨されます。

  ロスレス圧縮を使用する場合：

  - 通知領域アイコンであるロスレスインジケーターは、表示されている画面がロッシーフレームかロスレスフレームかをユーザーに通知します。このアイコンは、**Visual Quality**ポリシー設定で**Build to lossless**が指定されている場合に役立ちます。送信されるフレームがロスレスの場合、ロスレスインジケーターは緑色に変わります。

- ロスレススイッチを使用すると、ユーザーはセッション中にいつでも常にロスレスモードに変更できます。**セッション中にいつでもロスレス**を選択または選択解除するには、アイコンを右クリックして**Switch to pixel perfect**をクリックするか、ショートカットALT+SHIFT+1を使用します。

  ロスレス圧縮の場合：HDX 3D Proは、ポリシーで選択されたコーデックに関係なく、ロスレスコーデックを圧縮に使用します。

  ロッシー圧縮の場合：HDX 3D Proは、デフォルトまたはポリシーで選択された元のコーデックを使用します。

  ロスレススイッチの設定は、以降のセッションでは保持されません。すべての接続でロスレスコーデックを使用するには、**Visual quality**ポリシー設定で**Always lossless**を選択します。

- セッション内でロスレスを選択または選択解除するためのデフォルトのショートカットALT+SHIFT+1を上書きできます。
  `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\LLIndicator`で新しいレジストリ設定を構成します。

  - 名前: HKEY_LOCAL_MACHINE_HotKey, 種類: String
  - ショートカットの組み合わせを構成する形式は、C=0`|`1、A=0`|`1、S=0`|`1、W=0`|`1、K=valです。キーはコンマ「,」で区切る必要があります。キーの順序は関係ありません。
  - A、C、S、W、Kはキーであり、C=Control、A=ALT、S=SHIFT、W=Win、K=有効なキーです。Kに許可される値は、0〜9、a〜z、および任意の仮想キーコードです。
  - 例:
    - F10の場合、K=0x79を設定
    - Ctrl + F10の場合、C=1、K=0x79を設定
    - Alt + Aの場合、A=1、K=aまたはA=1、K=AまたはK=A、A=1を設定
    - Ctrl + Alt + 5の場合、C=1、A=1、K=5またはA=1、K=5、C=1を設定
    - Ctrl + Shift + F5の場合、A=1、S=1、K=0x74を設定

> **注意:**

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

- 複数および高解像度モニターのサポート。シングルセッションOSマシンでは、HDX 3D Proは最大4台のモニターを備えたユーザーデバイスをサポートします。ユーザーはモニターを任意の構成で配置でき、異なる解像度や向きのモニターを混在させることもできます。モニターの数は、ホストコンピューターのGPU、ユーザーデバイス、および利用可能な帯域幅の機能によって制限されます。HDX 3D Proはすべてのモニター解像度をサポートしており、ホストコンピューターのGPUの機能によってのみ制限されます。
- 動的解像度。仮想デスクトップまたはアプリケーションウィンドウを任意の解像度にサイズ変更できます。**注**: 解像度を変更する唯一のサポートされている方法は、VDAセッションウィンドウのサイズを変更することです。VDAセッション内から解像度を変更すること（**コントロールパネル > デザイン**と**個人設定 > ディスプレイ > 画面の解像度**を使用）はサポートされていません。
- NVIDIA vGPUアーキテクチャのサポート。HDX 3D ProはNVIDIA vGPUカードをサポートしています。詳細については、GPUパススルーおよびGPU共有に関するNVIDIA vGPUを参照してください。NVIDIA vGPUを使用すると、複数のVMが単一の物理GPUに同時に直接アクセスできるようになり、非仮想化オペレーティングシステムに展開されているものと同じNVIDIAグラフィックドライバーが使用されます。
- Virtual Direct Graphics Acceleration (vDGA) を使用したVMware vSphereおよびVMware ESXのサポート - HDX 3D ProをvDGAと組み合わせて、RDSおよびVDIワークロードの両方で使用できます。
- NVIDIA vGPUおよびAMD MxGPUを使用したVMware vSphere/ESXのサポート。
- Windows Server 2016のDiscrete Device Assignmentを使用したMicrosoft HyperVのサポート。
- Intel Xeon Processor E3ファミリーによるデータセンターグラフィックスのサポート。HDX 3D Pro は、サポートされているIntelプロセッサーファミリーで、マルチモニター（最大3台）、コンソールブランキング、カスタム解像度、高フレームレートをサポートします。詳細については、`<http://www.citrix.com/intel>` および `<http://www.intel.com/content/www/us/en/servers/data-center-graphics.html>` を参照してください。
- AMD FirePro Sシリーズサーバーカードでの AMD RapidFireのサポート。HDX 3D Pro は、マルチモニター（最大6台）、コンソールブランキング、カスタム解像度、高フレームレートをサポートします。注：AMD MxGPU（GPU仮想化）に対するHDX 3D Proのサポートは、

VMware vSphere vGPUでのみ機能します。Citrix Hypervisor および Hyper-V は、GPUパススルーでサポートされます。詳細については、AMD Virtualization Solution を参照してください。

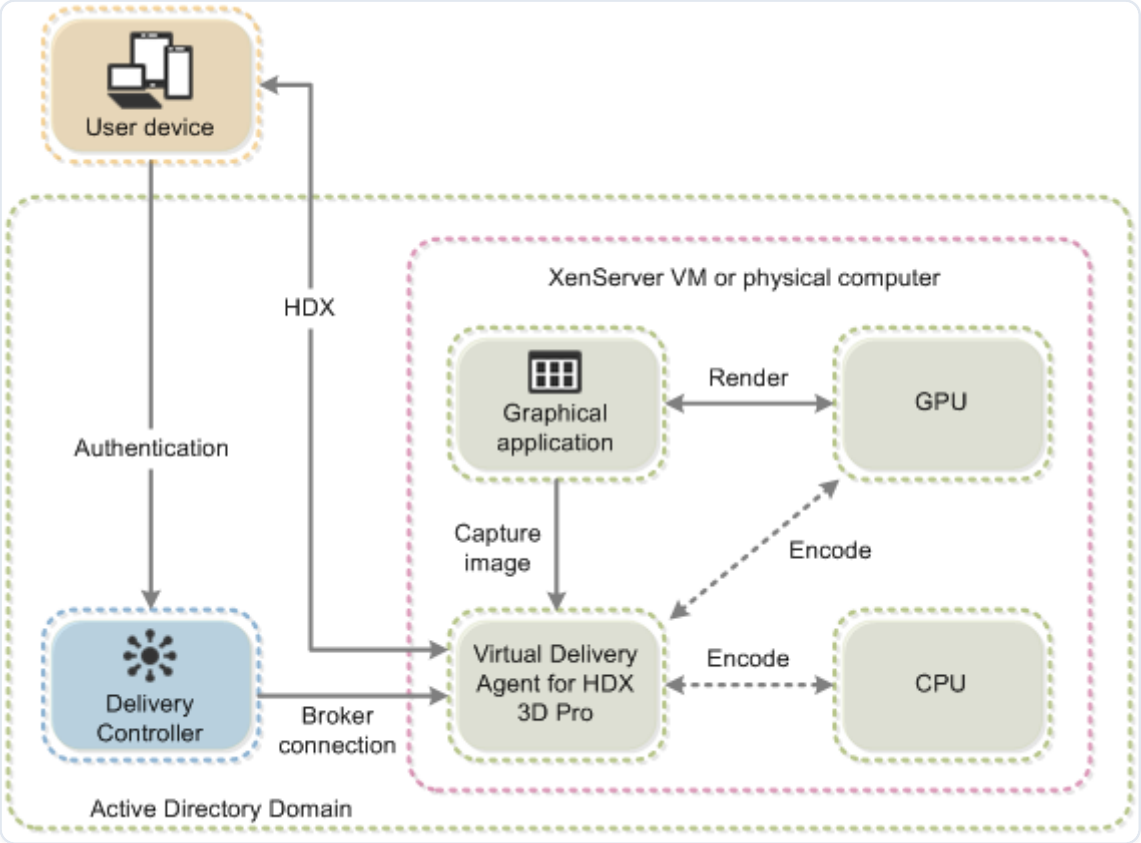
- NVIDIA GPU、AMD GPU、Intel Iris Proグラフィックプロセッサ用の高性能ビデオエンコーダーへのアクセス。ポリシー設定（デフォルトで有効）がこの機能を制御します。この機能により、H.264エンコーディングにハードウェアエンコーディング（利用可能な場合）を使用できます。このようなハードウェアが利用できない場合、VDAはソフトウェアビデオコーデックを使用したCPUベースのエンコーディングにフォールバックします。詳細については、「グラフィックポリシー設定」(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/policies/reference/ica-policy-settings/graphics-policy-settings.html)を参照してください。

次の図に示すように：

- ユーザーがCitrix Workspace™アプリにログオンし、仮想アプリケーションまたはデスクトップにアクセスすると、Controllerがユーザーを認証します。その後、ControllerはHDX 3D Pro用VDAに接続し、グラフィックアプリケーションをホストするコンピューターへの接続を仲介します。

HDX 3D Pro用VDAは、ホスト上の適切なハードウェアを使用して、デスクトップ全体またはグラフィックアプリケーションのみのビューを圧縮します。

- デスクトップまたはアプリケーションのビューと、それらに対するユーザーの操作は、ホストコンピューターとユーザーデバイス間で送信されます。この送信は、Citrix WorkspaceアプリとHDX 3D Pro用VDA間の直接HDX接続を介して行われます。



HDX 3D Proのユーザーエクスペリエンスを最適化する

複数のユーザーが帯域幅が制限された接続（たとえば、支店など）を共有している場合、各ユーザーが利用できる帯域幅を制限するために、**セッション全体の帯域幅制限**ポリシー設定を使用することをお勧めします。この設定を使用すると、ユーザーがログオンおよびログオフしても、利用可能な帯域幅が大きく変動しないようにできます。HDX 3D Proは利用可能なすべての帯域幅を使用するように自動的に調整するため、ユーザーセッション中に利用可能な帯域幅が大きく変動すると、パフォーマンスに悪影響を及ぼす可能性があります。

たとえば、20人のユーザーが60 Mbpsの接続を共有している場合、各ユーザーが利用できる帯域幅は、同時ユーザー数に応じて3 Mbpsから60 Mbpsの間で変動する可能性があります。このシナリオでユーザーエクスペリエンスを最適化するには、ピーク時のユーザーあたりの必要な帯域幅を決定し、常にこの量にユーザーを制限します。

3Dマウスのユーザーの場合、汎用USBリダイレクト仮想チャネルの優先度を0に上げることをお勧めします。仮想チャネルの優先度を変更する方法については、Knowledge Centerの記事CTX128190を参照してください。

フレームホーク

> **重要:**

> Citrix Virtual Apps and Desktops 7 1903以降、Framehawk はサポートされなくなりました。代わりに、Thinwireをアダプティブトランスポートを有効にして使用してください。

> Framehawkは、高いパケット損失が発生しやすいブロードバンドワイヤレス接続（Wi-Fiおよび4G/LTEセルラーネットワーク）を使用するモバイルワーカー向けの特殊なディスプレイリモートテクノロジーです。Framehawkは、スペクトル干渉とマルチパス伝播の課題を克服します。Framehawkは、ラップトップやタブレットなどのWindowsおよびiOSモバイルデバイスで仮想アプリやデスクトップを使用するユーザーに、流動的でインタラクティブなユーザーエクスペリエンスを提供します。サーバーのスケーラビリティを最大化し、ネットワーク帯域幅の消費を最小限に抑えるため、Framehawkは上記の特定のユースケースでのみ使用することをお勧めします。その他のすべてのユースケースでは、データスループットを最大化するために多くのFramehawkの概念を取り入れたアダプティブトランスポートをお勧めします。

Citrix®ポリシーテンプレートを使用して、組織に適した方法で、特定のユーザーセットとアクセスシナリオに対してFramehawkを実装できます。Framehawkは、ラップトップやタブレットなどのシングルスクリーンモバイルユースケースを対象としています。リアルタイムのインタラクティブパフォーマンスのビジネス価値が、サーバーリソースの追加コストとブロードバンド接続の要件を正当化する場合に、Framehawkを使用してください。

Framehawkがスムーズなユーザーエクスペリエンスを維持する方法

Framehawkは、フレームバッファの内容を見て、画面上のさまざまな種類のコンテンツを識別する、人間の目のソフトウェア実装だと考えてください。ユーザーにとって何が重要でしょうか？ビデオや動くグラフィックのように画面の領域が急速に変化する場合、一部のピクセルが失われても人間の目には問題ありません。それらの領域は新しいデータで迅速に上書きされます。

しかし、画面の静的な領域に関しては、人間の目は非常にうるさいです。たとえば、通知領域やツールバーのアイコン、またはユーザーが読み始めたい場所までスクロールした後のテキストなどです。ユーザーはこれらの領域がピクセルパーフェクトであることを期待します。**0と1**の観点から技術的に正確であることを目指すプロトコルとは異なり、Framehawkはテクノロジーを使用している人間にとって関連性があることを目指しています。

Framehawkには、次世代のQuality of Service信号増幅器と、よりきめ細かく効率的なワークロード識別のための時間ベースのヒートマップが含まれています。データ圧縮に加えて、自律的な自己修復変換を使用し、データの再送信を回避して、クリック応答、線形性、および一貫したケイデンスを維持します。損失の多いネットワーク接続では、Framehawkは補間によって損失を隠すことができ、ユーザーはより流動的なエクスペリエンスを楽しみながら、良好な画質を認識できます。さらに、Framehawkアルゴリズムは、異なる種類のパケット損失をインテリジェントに区別

します。たとえば、ランダムな損失（補償のためにより多くのデータを送信する）と輻輳による損失（チャネルがすでに詰まっているため、より多くのデータを送信しない）などです。

Citrix Workspace™アプリのFramehawk Intent Engineは、上下のスクロール、ズーム、左右への移動、読み取り、入力、その他の一般的なアクションを区別します。このエンジンは、共有辞書を使用してVirtual Delivery Agent (VDA)への通信も管理します。ユーザーが読もうとしている場合、テキストの視覚的な品質は優れている必要があります。ユーザーがスクロールしている場合、それは迅速かつスムーズでなければなりません。そして、中断可能である必要があり、ユーザーが常にアプリケーションまたはデスクトップとのインタラクションを制御できるようにします。

ネットワーク接続のケイデンス（自転車のチェーンの張力に例えられる**ギアリング**）を測定することで、Framehawkロジックはより迅速に反応し、高遅延接続で優れたエクスペリエンスを提供します。このユニークで特許取得済みのギアリングシステムは、ネットワーク状態に関する常に最新のフィードバックを提供し、Framehawkが帯域幅、遅延、損失の変化に即座に反応できるようにします。

ThinwireとFramehawkを使用する際の設計上の考慮事項

Framehawkは、User Datagram Protocol (UDP) の上に構築されたデータ転送層を使用します。Framehawkのパフォーマンスを他のUDPベースのプロトコルと比較するとわかるように、UDPはFramehawkが損失を克服する方法の小さな部分です。UDPは、Framehawkを際立たせる人間中心の技術にとって重要な基盤を提供します。

Framehawkにはどのくらいの帯域幅が必要ですか？

ブロードバンドワイヤレスの意味は、接続を共有するユーザー数、接続の品質、使用されているアプリなど、いくつかの要因によって異なります。最適なパフォーマンスを得るには、Citrixはベースとして4 Mbpsまたは5 Mbpsに加えて、同時ユーザーあたり約150 Kbpsを推奨しています。

Thinwireの帯域幅推奨は、通常、ベースとして1.5 Mbpsに加えてユーザーあたり150 Kbpsです。詳細については、Citrix Virtual Apps and Desktopsの帯域幅に関するブログを参照してください。パケット損失が3%の場合、TCP上のThinwireは、良好なユーザーエクスペリエンスを維持するためにFramehawkよりもはるかに多くの帯域幅が必要であることがわかります。

Thinwireは、ICA®プロトコルにおける主要なディスプレイリモートチャネルであり続けます。Framehawkはデフォルトで無効になっています。Citrixは、組織内のブロードバンドワイヤレスアクセスシナリオに対応するために、選択的に有効にすることを推奨しています。FramehawkはThinwireよりもかなり多くのサーバーリソース（CPUとメモリ）を必要とすることに注意してください。

要件と考慮事項

Framehawkには、VDA 7.6.300およびGroup Policy Management 7.6.300が最低限必要です。

エンドポイントには、Workspace app for Windows 1808、またはCitrix Receiver for Windows 4.3.100、Workspace app for iOS 1808、またはCitrix Receiver for iOS 6.0.1が最低限必要です。

デフォルトでは、Framehawkは双方向のUser Datagram Protocol (UDP) ポート範囲（3224～3324）を使用して、Citrix WorkspaceアプリとFramehawkディスプレイチャネルデータを交換します。この範囲は、**Framehawk display channel port range**というポリシー設定でカスタマイズできます。クライアントと仮想デスクトップ間の同時接続ごとに一意のポートが必要です。Citrix Virtual Apps™サーバーなどのマルチユーザーOS環境では、同時ユーザーセッションの最大数をサポートするのに十分なポートを定義してください。VDIデスクトップなどのシングルユーザーOSの場合、単一のUDPポートを定義するだけで十分です。Framehawkは、最初に定義されたポートから、範囲で指定された最後のポートまでを順に試行します。これは、Citrix Gatewayを介する場合と、StoreFrontサーバーへの直接内部接続の両方に適用されます。

リモートアクセスには、Citrix Gatewayを展開する必要があります。デフォルトでは、Citrix GatewayはクライアントのCitrix WorkspaceアプリとGateway間の暗号化された通信にUDPポート443を使用します。このポートは、双方向の安全な通信を許可するために、すべての外部ファイアウォールで開いている必要があります。この機能はDatagram Transport Security (DTLS)として知られています。

> **注：**
>
> Framehawk/DTLS接続はFIPSアプライアンスではサポートされていません。
>
> 暗号化されたFramehawk接続は、NetScaler Gatewayバージョン11.0.62およびNetScaler Unified Gatewayバージョン11.0.64.34以降でサポートされています。

NetScaler High Availabilityは、XenAppおよびXenDesktop 7.12以降でサポートされています。

Framehawkを実装する前に、以下の推奨事項を考慮してください。

- Framehawk用に定義されたUDPポートがファイアウォールで開いていることを確認するために、セキュリティ管理者に連絡してください。インストールプロセスでは、ファイアウォールは自動的に構成されません。
- 多くの場合、Citrix GatewayはDMZにインストールされ、外部と内部の両側にファイアウォールが配置されていることがあります。外部ファイアウォールでUDPポート443が開いているこ

とを確認してください。環境がデフォルトのポート範囲を使用している場合は、内部ファイアウォールでUDPポート3224から3324が開いていることを確認してください。

構成

> **注意:**

> Citrixは、高いパケット損失が発生する可能性のあるユーザーに対してのみFramehawkを有効にすることを推奨しています。また、サイト内のすべてのオブジェクトに対してFramehawkをユニバーサルポリシーとして有効にしないことを推奨します。

> Framehawkはデフォルトで無効になっています。有効にすると、サーバーはユーザーグラフィックと入力にFramehawkを使用しようとします。何らかの理由で前提条件が満たされない場合、接続はデフォルトモード（Thinwire）を使用して確立されます。

以下のポリシー設定がFramehawkに影響します。

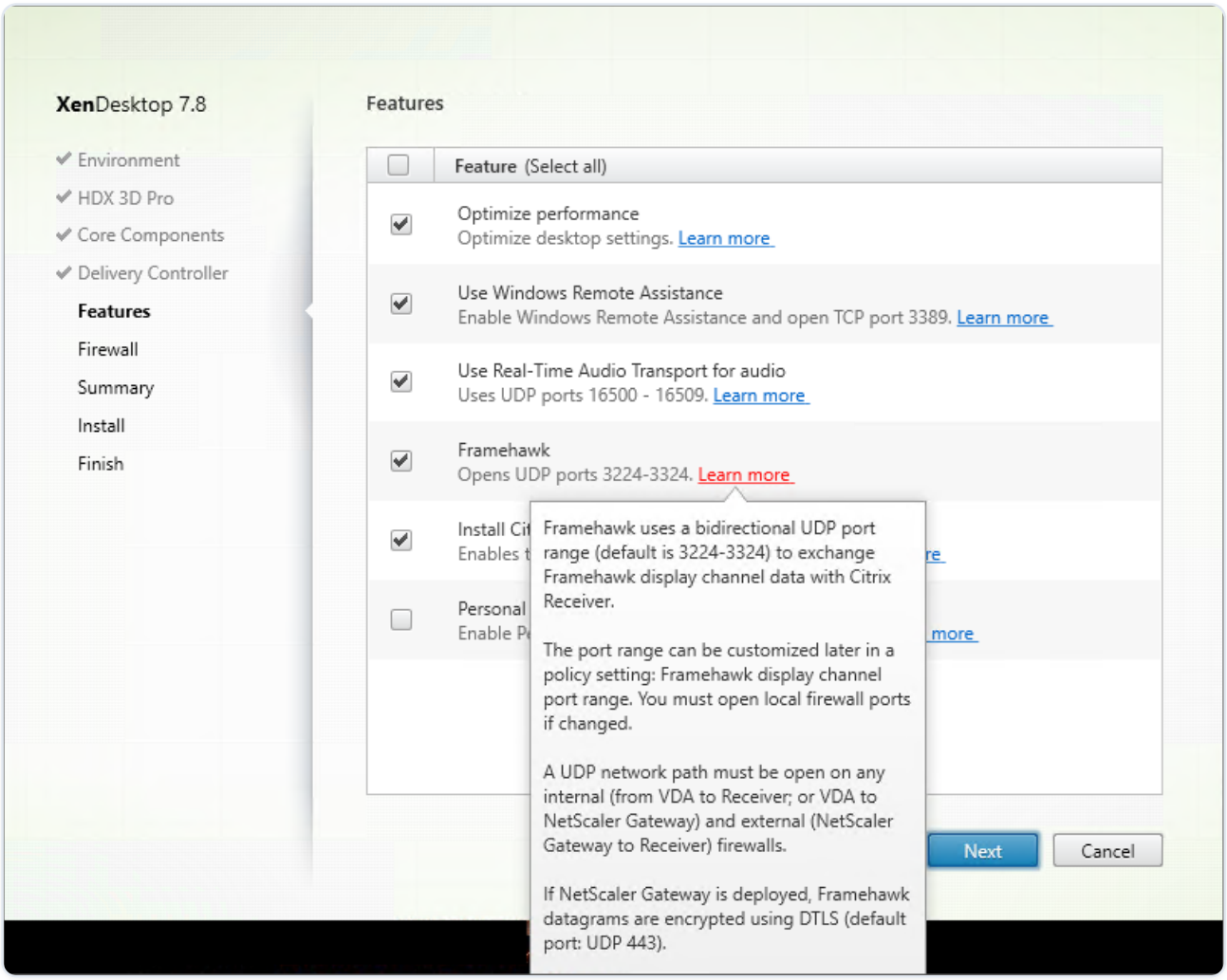
- Framehawk ディスプレイチャネル: この機能を有効または無効にします。
- Framehawk ディスプレイチャネルポート範囲: VDA がユーザーデバイスと Framehawk ディスプレイチャネルデータを交換するために使用する UDP ポート番号の範囲（最小ポート番号から最大ポート番号まで）を指定します。VDA は、最小ポート番号から開始し、その後の試行ごとにインクリメントしながら、各ポートの使用を試みます。このポートは、インバウンドおよびアウトバウンドトラフィックを処理します。

Framehawk ディスプレイチャネルのポートを開く

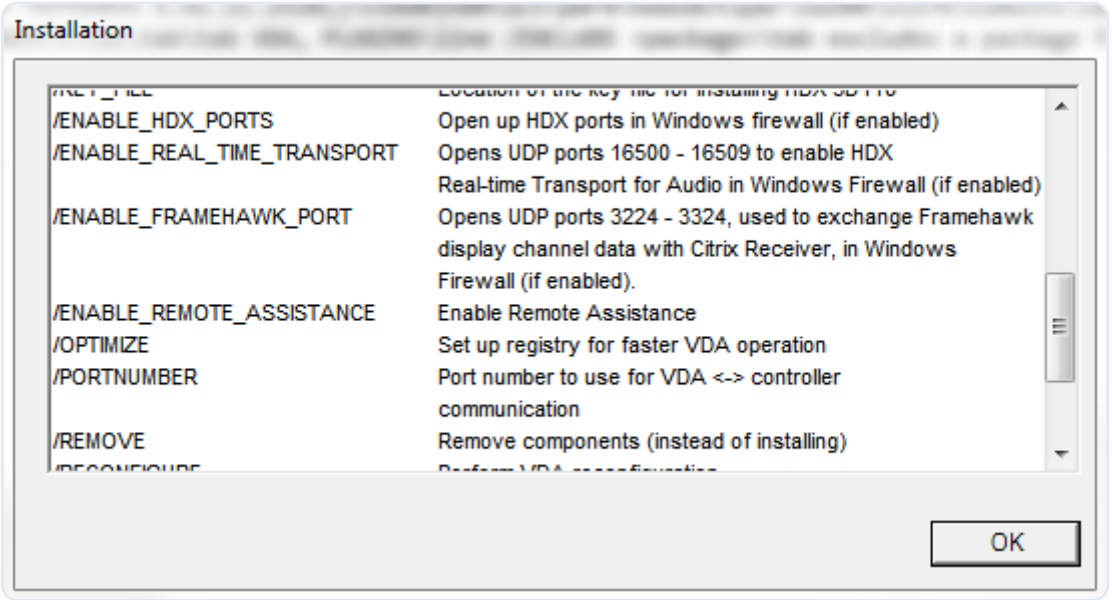
XenApp および XenDesktop 7.8 以降では、VDA インストーラーの ステップでファイアウォールを再構成するオプションが利用できます。このチェックボックスをオンにすると、Windows ファイアウォールで UDP ポート 3224 から 3324 が開きます。次のような状況では、手動でのファイアウォール構成が必要です。

- 任意のネットワークファイアウォールの場合。 または
- デフォルトのポート範囲がカスタマイズされている場合。

これらの UDP ポートを開くには、 チェックボックスをオンにします。

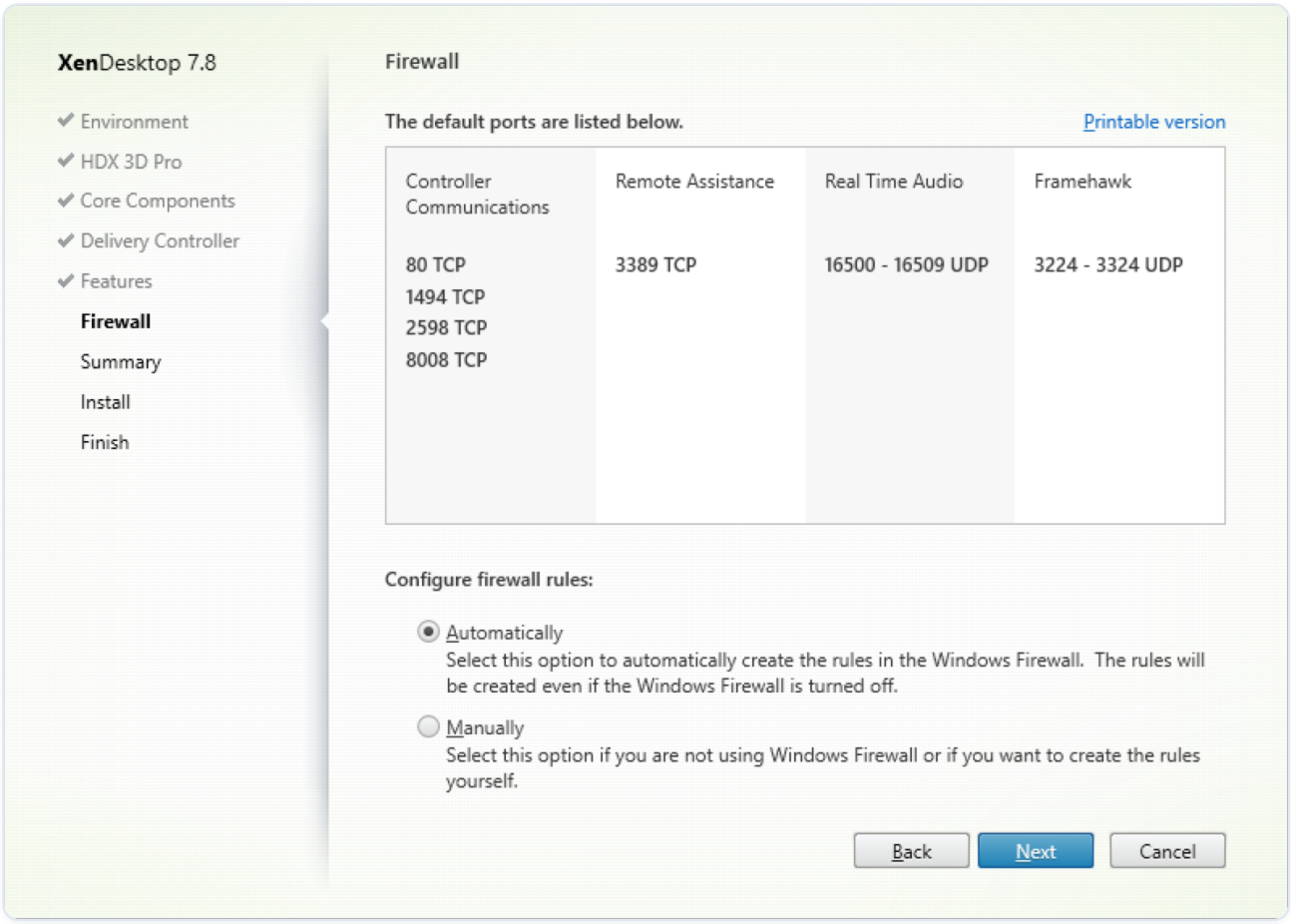


コマンドラインを使用して、**/ENABLE_FRAMEHAWK_PORT** で Framehawk 用の UDP ポートを開くこともできます。

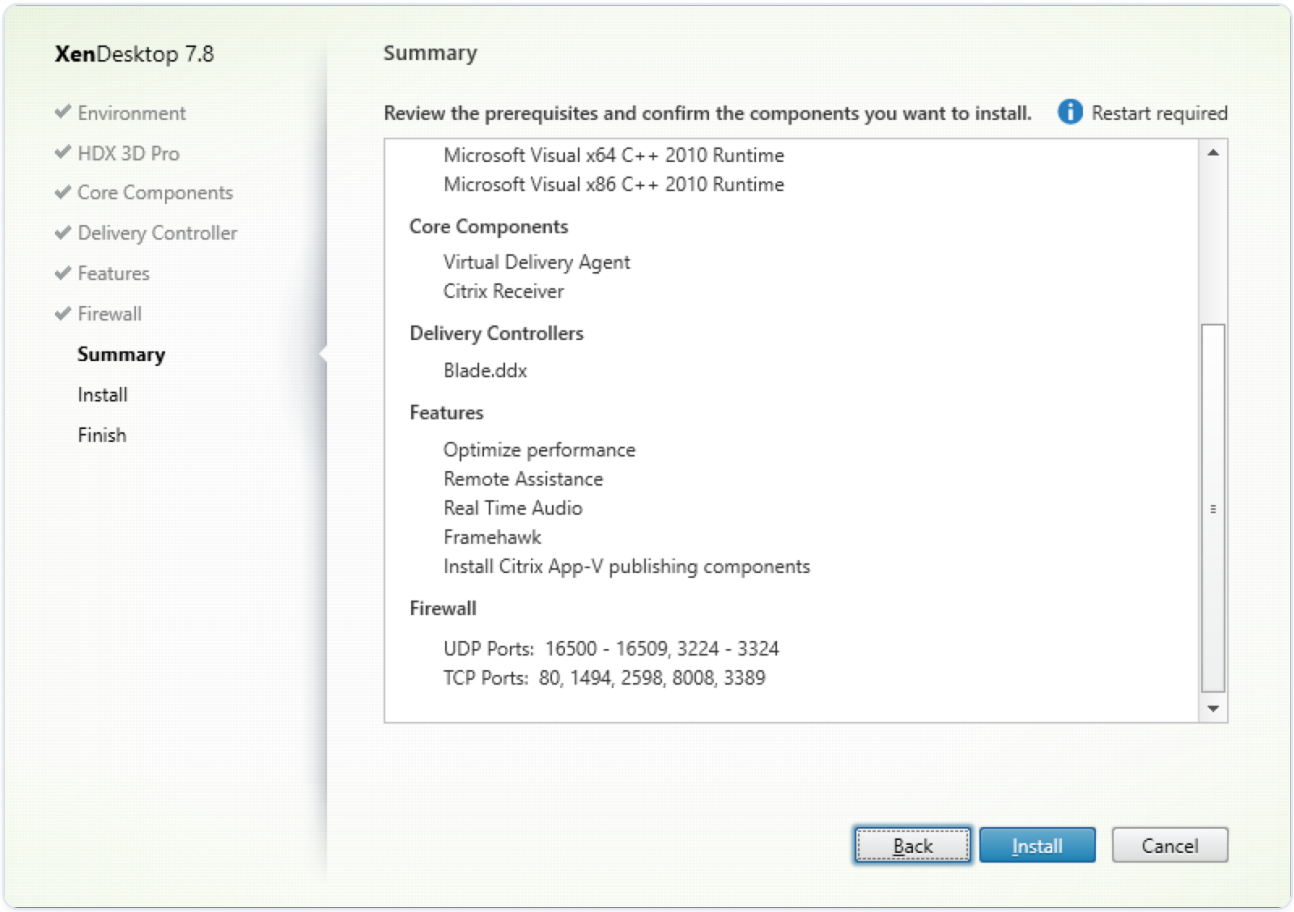


Framehawk UDP ポートの割り当ての確認

インストール中に、 画面で Framehawk に割り当てられている UDP ポートを確認できます。



画面には、Framehawk 機能が有効になっているかどうかが表示されます。



Framehawk の Citrix Gateway サポート

暗号化された Framehawk トラフィックは、Citrix Gateway 1808 以降、NetScaler Gateway 11.0.62.10 以降、Citrix Unified Gateway 1808、および NetScaler Unified Gateway 11.0.64.34 以降でサポートされています。

- Citrix Gateway は、Gateway VPN 仮想サーバーがエンドユーザーデバイスから直接アクセスできる展開アーキテクチャを指します。つまり、VPN 仮想サーバーにはパブリック IP アドレスが割り当てられており、ユーザーはこの IP アドレスに直接接続します。
- Unified Gateway を使用する Citrix Gateway は、Gateway VPN 仮想サーバーがコンテンツスイッチング仮想サーバー (CS) のターゲットとしてバインドされている展開を指します。この展開では、CS 仮想サーバーがパブリックインターネットプロトコルアドレスを持ち、Gateway VPN 仮想サーバーがダミーのインターネットプロトコルアドレスを持ちます。

Citrix Gateway で Framehawk サポートを有効にするには、Gateway VPN 仮想サーバーレベルの DTLS パラメーターを有効にする必要があります。パラメーターが有効になり、Citrix Virtual Apps または Citrix Virtual Desktops™ のコンポーネントが正しく更新されると、Framehawk のオーディオ、ビデオ、およびインタラクティブトラフィックは Gateway VPN 仮想サーバーとユーザーデバイス間で暗号化されます。

Citrix Gateway、Unified Gateway、および Citrix Gateway + グローバルサーバー負荷分散は Framehawk でサポートされています。

以下のシナリオは Framehawk でサポートされていません。

- HDX™ インサイト
- IPv6 モードの Citrix Gateway
- Citrix Gateway ダブルホップ
- クラスター設定の Citrix Gateway

シナリオ	FRAMEHAWK のサポート
シトリックス ゲートウェイ	はい
Citrix Gateway + グローバルサーバー負荷分散	はい
Unified Gateway を使用する Citrix Gateway	はい。**注:** Unified Gateway バージョン 11.0.64.34 以降がサポートされています。
HDX インサイト	いいえ

シナリオ	FRAMEHAWK のサポート
IPv6 モードの Citrix Gateway	いいえ
Citrix Gateway ダブルホップ	いいえ
Citrix Gateway 上の複数のセキュア チケット オーソリティ	はい
Citrix Gateway と高可用性	はい
Citrix Gateway とクラスター設定	いいえ

Framehawk サポートのための Citrix Gateway の構成

Citrix Gateway で Framehawk サポートを有効にするには、Gateway VPN の *仮想サーバー* レベルで DTLS パラメーターを有効にします。パラメーターが有効になり、Citrix Virtual Apps and Desktops™ のコンポーネントが正しく更新されると、Framehawk のオーディオ、ビデオ、およびインタラクティブトラフィックは、Gateway VPN 仮想サーバーとユーザーデバイス間で暗号化されます。

この構成は、リモートアクセス用に Citrix Gateway で UDP 暗号化を有効にする場合に必要です。

Framehawk サポートのために Citrix Gateway を構成する場合：

- 外部ファイアウォールで UDP ポート 443 が開いていることを確認します
- 外部ファイアウォールで CGP ポート（デフォルト 2598）が開いていることを確認します
- VPN 仮想サーバーの設定で DTLS を有効にします
- SSL 証明書とキーのペアをバインド解除して再バインドします。Citrix Gateway 1808 以降、または NetScaler バージョン 11.0.64.34 以降を使用している場合、この手順は不要です。

Framehawk サポートのために Citrix Gateway を構成するには：

1. Citrix Gateway を展開および構成して、StoreFront™ と通信し、Citrix Virtual Apps and Desktops のユーザーを認証します。
2. Citrix Gateway の構成タブで、Citrix Gateway を展開し、**Virtual Servers** を選択します。
3. VPN 仮想サーバーの基本設定を表示するには、**Edit** を選択します。DTLS 設定の状態を確認します。
4. その他の構成オプションを表示するには、**More** を選択します。

5. Framehawk などのデータグラムプロトコルに通信セキュリティを提供するには、**DTLS** を選択します。**OK** をクリックします。VPN 仮想サーバーの基本設定領域に、DTLS フラグが **True** に設定されていることが表示されます。
6. サーバー証明書バインド画面を再度開き、**+** をクリックして証明書キーペアをバインドします。
7. 以前の証明書キーペアを選択し、**Select** をクリックします。
8. サーバー証明書バインドへの変更を保存します。
9. 保存後、証明書キーペアが表示されます。**Bind** をクリックします。
10. 警告メッセージ「**No usable ciphers configured on the SSL vserver/service**」が表示された場合は無視してください。

以前の NetScaler® Gateway バージョンの手順

NetScaler Gateway のバージョンが 11.0.64.34 より古い場合：

1. サーバー証明書バインド画面を再度開き、+ をクリックして証明書キーペアをバインドします。
2. 以前の証明書キーペアを選択し、**Select** をクリックします。
3. サーバー証明書バインドへの変更を保存します。
4. 保存後、証明書キーペアが表示されます。［**バインド**］ をクリックします。
5. **No usable ciphers configured on the SSL vserver/service** という警告メッセージが表示された場合は、無視してください。

FramehawkをサポートするようにUnified Gatewayを構成するには：

1. Unified Gatewayがインストールされ、適切に構成されていることを確認します。詳しくは、Citrix製品ドキュメントサイトのUnified Gatewayを参照してください。
2. ターゲット*仮想サーバー*としてCS *仮想サーバー*にバインドされているVPN *仮想サーバー*でDTLSパラメーターを有効にします。

制限事項

クライアントデバイスにCitrix Gateway仮想サーバーの古いDNSエントリがある場合、アダプティブトランスポートとFramehawkはUDPトランスポートではなくTCPトランスポートにフォールバックする可能性があります。TCPトランスポートへのフォールバックが発生した場合は、クライアントのDNSキャッシュをフラッシュし、再接続してUDPトランスポートを使用してセッションを確立してください。

Framehawkは、PTC Creoなどのアプリケーションに見られる32ビットのマウスポインターをサポートしていません。

Framehawkは、シングルモニターを使用するラップトップやタブレットなどのモバイルデバイス向けに設計されており、デュアル/マルチモニター構成ではThinwireに戻ります。

その他のVPN製品のサポート

Citrix Gatewayは、Framehawkで必要とされるUDP暗号化をサポートする唯一のSSL VPN製品です。別のSSL VPNまたは誤ったバージョンのCitrix Gatewayが使用されている場合、Framehawkポリシーが適用されないことがあります。従来のIPsec VPN製品は、変更なしでFramehawkをサポートします。

Framehawkの監視

Citrix DirectorからFramehawkの使用状況とパフォーマンスを監視できます。HDX仮想チャネルの詳細ビューには、任意のセッションでFramehawkのトラブルシューティングと監視に役立つ情報が含まれています。Framehawk関連のメトリックを表示するには、［**Graphics-Framehawk**］ を選択します。

Framehawk接続が確立されている場合、詳細ページに **Provider = VD3D** および **Connected = True** と表示されます。仮想チャネルの状態がアイドルであるのは正常です。これは、初期ハンドシェイク中にのみ使用されるシグナリングチャネルを監視するためです。このページには、接続に関するその他の有用な統計も表示されます。

問題が発生した場合は、Framehawkトラブルシューティングブログを参照してください。

シンワイヤー

はじめに

Thinwireは、Citrix HDXテクノロジーの一部であり、Citrix Virtual Apps and Desktopsで使用されるCitrixのデフォルトのディスプレイリモートテクノロジーです。

ディスプレイリモートテクノロジーにより、あるマシンで生成されたグラフィックを、通常はネットワーク経由で別のマシンに送信して表示できます。

成功したディスプレイリモートソリューションは、ローカルPCと同様の高度にインタラクティブなユーザーエクスペリエンスを提供します。Thinwireは、複雑で効率的な画像分析および圧縮技術を幅広く使用することで、このエクスペリエンスを実現します。Thinwireは、サーバーのスケーラビリティを最大化し、他のディスプレイリモートテクノロジーよりも少ない帯域幅を消費します。

このバランスにより、Thinwireはほとんどの一般的なビジネスユースケースに対応し、Citrix Virtual Apps and Desktopsのデフォルトのディスプレイリモートテクノロジーとして使用されています。

HDX™ 3D プロ

デフォルト構成では、Thinwireは3Dグラフィックまたは高度にインタラクティブなグラフィックを提供し、存在する場合はグラフィック処理ユニット（GPU）を使用できます。ただし、GPUが存在するシナリオでは、**3Dグラフィックワークロード向けに最適化**または**視覚品質 > ロスレスビルド**ポリシーを使用してHDX 3D Proモードを有効にすることをお勧めします。これらのポリシーは、GPUが存在する場合に、Thinwireがビデオコーデック（H.264またはH.265）を使用してハードウェアアクセラレーションで画面全体をエンコードするように構成します。これにより、3Dプロフェッショナルグラフィックのよりスムーズなエクスペリエンスが提供されます。詳細については、H.264 ロスレスビルド、HDX 3D Pro、およびWindowsシングルセッションOSのGPUアクセラレーションを参照してください。

要件

Thinwireは、Windows Server 2022、Windows Server 2019、Windows Server 2016、Windows Server 2012 R2、Windows 10、Windows 7などの最新のオペレーティングシステム向けに最適化されています。Windows Server 2008 R2の場合は、レガシーグラフィックモードが推奨されます。これらのユースケースに対してCitrixが推奨するポリシー設定の組み合わせを提供するには、組み込みのCitrixポリシーテンプレート、High Server Scalability-Legacy OS、およびOptimized for WAN-Legacy OSを使用します。

> **注：**
>
> このリリースでは、レガシーグラフィックモードはサポートされていません。これは、XenApp 7.15 LTSR、XenDesktop 7.15 LTSR、およびWindows 7とWindows 2008 R2を使用する以前のVDAリリースとの下位互換性のために含まれています。

- Thinwireの動作を制御するポリシー設定である**圧縮にビデオコーデックを使用**は、Citrix Virtual Apps and Desktops 7 1808以降およびXenApp and XenDesktop 7.6 FP3以降のVDAバージョンで利用できます。**優先時にビデオコーデックを使用**オプションは、Citrix Virtual Apps and Desktops 7 1808以降およびXenApp and XenDesktop 7.9以降のVDAバージョンでのデフォルト設定です。
- すべてのCitrix Workspace™アプリはThinwireをサポートしています。一部のCitrix Workspaceアプリは、帯域幅使用量を削減するための8ビットまたは16ビットグラフィックなど、他のア

プリがサポートしないThinwireの機能をサポートする場合があります。このような機能のサポートは、Citrix Workspaceアプリによって自動的にネゴシエートされます。

- Thinwireは、マルチモニターおよび高解像度のシナリオで、より多くのサーバーリソース（CPU、メモリ）を使用します。Thinwireが使用するリソースの量を調整することは可能ですが、その結果、帯域幅の使用量が増加する可能性があります。
- 低帯域幅または高遅延のシナリオでは、インタラクティブ性を向上させるために8ビットまたは16ビットグラフィックを有効にすることを検討してください。特に8ビットの色深度では、視覚品質が影響を受ける可能性があります。

エンコード方法

Thinwireは、ポリシーとクライアントの機能に応じて、2つの異なるエンコードモードで動作できます。

- ThinwireフルスクリーンH.264またはH.265
- 選択的H.264またはH.265を使用したThinwire

従来のGDIリモート処理では、XPDMリモート処理ドライバーを使用しており、Thinwireビットマップエンコーダーは使用していません。

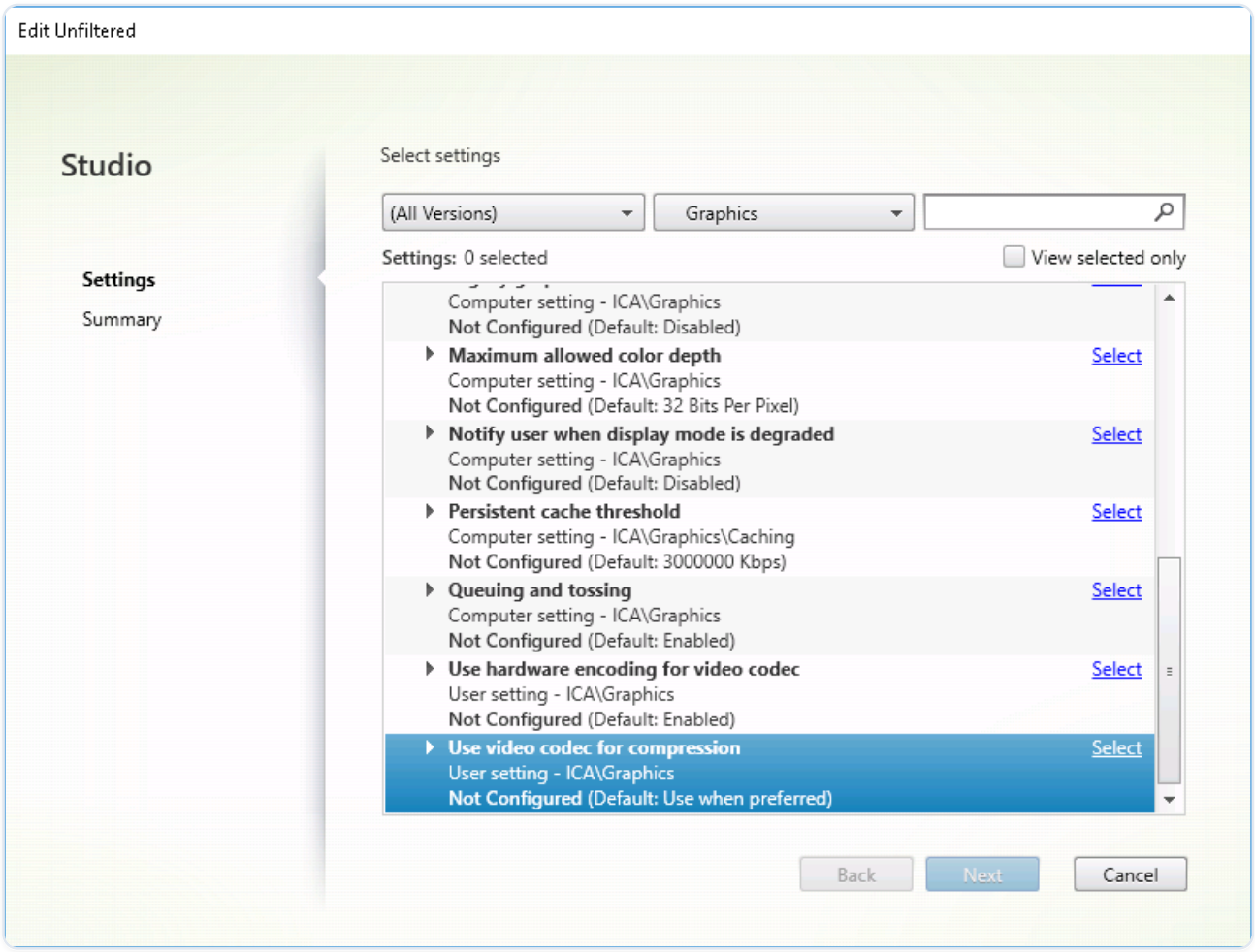
構成

Thinwireは、デフォルトのディスプレイリモート処理テクノロジーです。

以下のグラフィックポリシー設定は、デフォルトを設定し、さまざまなユースケースに対応する代替手段を提供します。

- 圧縮にビデオコーデックを使用
  - **ビデオコーデックを優先する場合にビデオコーデックを使用する**。これがデフォルト設定です。追加の構成は必要ありません。この設定をデフォルトのままにすることで、すべてのCitrix接続でThinwireが選択され、一般的なデスクトップワークロードのスケーラビリティ、帯域幅、優れた画質のために最適化されます。これは、**アクティブに変更される領域の場合**と機能的に同等です。
- このポリシー設定のその他のオプションは、さまざまなユースケースで他のテクノロジーとThinwireを引き続き使用します。例：
  - **アクティブに変更される領域の場合**。Thinwireのアダプティブディスプレイテクノロジーは、動いている画像（ビデオ、移動中の3D）を識別し、画像が動いている画面の一部でのみH.264またはH.265を使用します。

- **画面全体の場合**。3Dグラフィックを多用するケースで、ユーザーエクスペリエンスと帯域幅を向上させるために、フルスクリーンH.264またはH.265でThinwireを提供します。H.264 4:2:0の場合（**視覚的にロスレス**ポリシーが無効になっている場合）、最終的な画像はピクセルパーフェクト（ロスレス）ではなく、特定のシナリオには適さない場合があります。そのような場合は、代わりにH.264ビルドトゥロスレスの使用を検討してください。



以下の視覚表示ポリシー設定を含む、さまざまなその他のポリシー設定を使用して、ディスプレイリモート処理テクノロジーのパフォーマンスを微調整できます。Thinwireはそれらすべてをサポートしています。

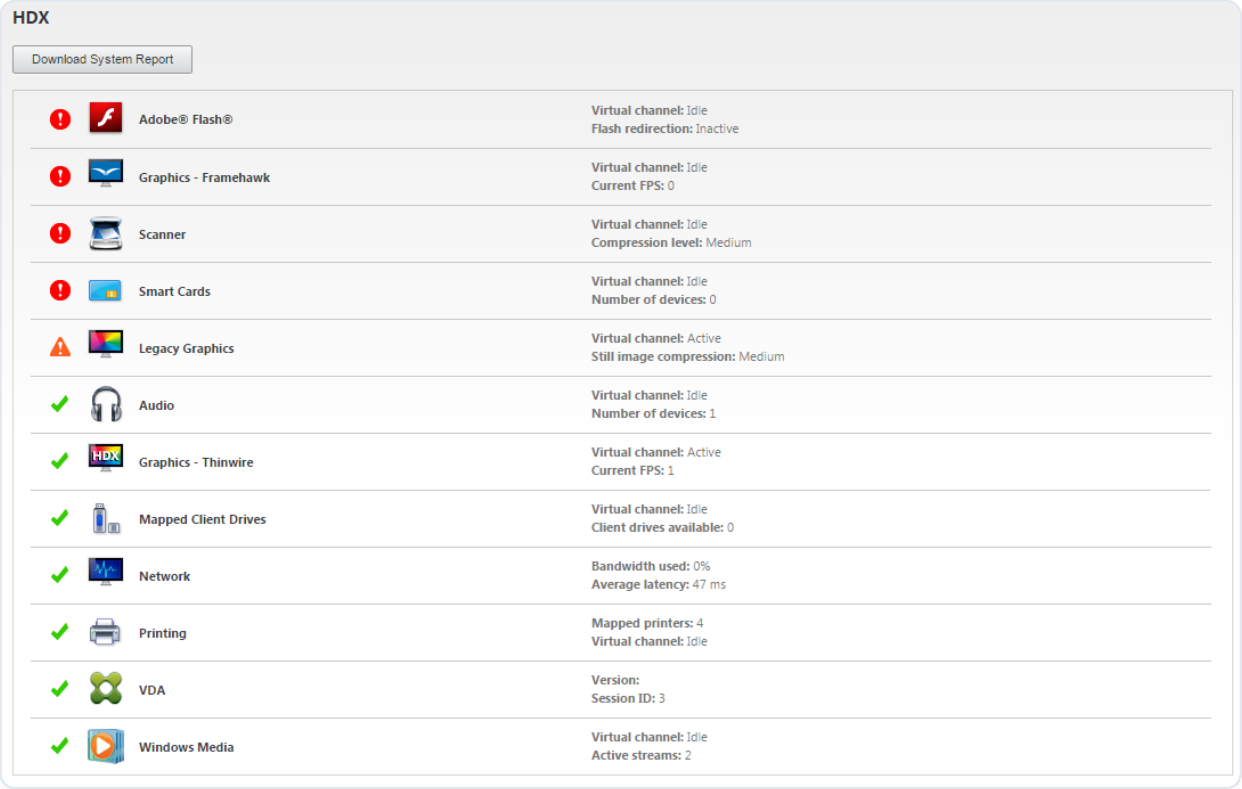
- シンプルなグラフィックの優先色深度
- ターゲットフレームレート
- 視覚品質

さまざまなビジネスユースケースに対応するCitrix推奨のポリシー設定の組み合わせを取得するには、組み込みのCitrixポリシーテンプレートを使用します。**高サーバー拡張性**および**超高精細ユーザーエクスペリエンス**テンプレートはどちらも、組織の優先順位とユーザーの期待に最適なポリシー設定の組み合わせでThinwireを使用します。

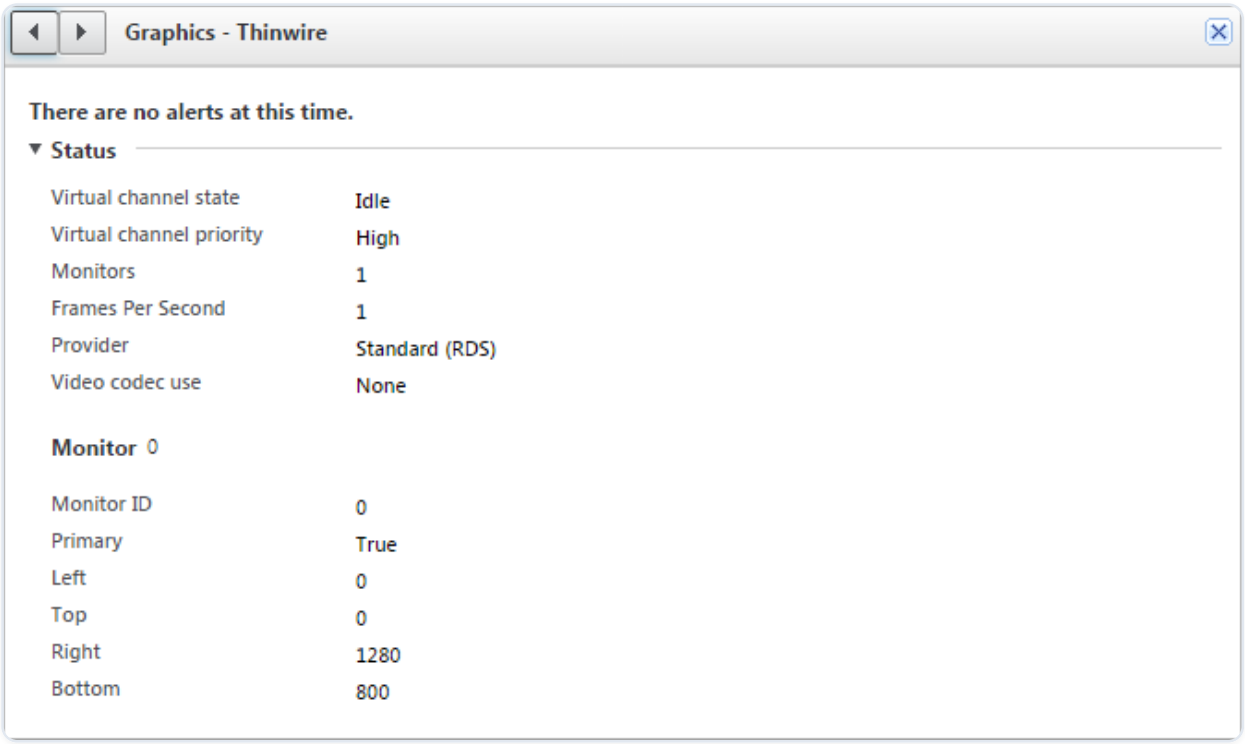
Thinwireの監視

Citrix Director から Thinwire の使用状況とパフォーマンスを監視できます。HDX 仮想チャネルの詳細ビューには、任意のセッションで Thinwire のトラブルシューティングと監視を行うための有用な情報が含まれています。Thinwire 関連のメトリックを表示するには：

1. Director で、ユーザー、マシン、またはエンドポイントを検索し、アクティブなセッションを開いて をクリックします。または、 > > を選択し、アクティブなセッションを開いて をクリックします。
2. パネルまでスクロールします。



3. を選択します。



ロスレス圧縮コーデック (MDRLE)

一般的なデスクトップセッションでは、ほとんどの画像は単純なグラフィックまたはテキスト領域です。Thinwire はこれらの領域がどこにあるかを判断し、2DRLE コーデックを使用してロスレスエンコードのためにこれらの領域を選択します。Citrix Workspace アプリクライアント側では、これらの要素はセッション表示のために Citrix Workspace アプリ側の 2DRLE デコーダーを使用してデコードされます。

XenApp および XenDesktop 7.17 では、2DRLE コーデックよりも一般的なデスクトップセッションで消費帯域幅が少ない、より高い圧縮率の MDRLE コーデックが追加されました。この新しいコーデックは、サーバーのスケーラビリティには影響しません。

帯域幅が低いということは、通常、セッションの対話性が向上し（特に共有リンクや制約のあるリンクの場合）、コストが削減されることを意味します。たとえば、MDRLE コーデックを使用した場合の予想帯域幅消費量は、一般的な Office のようなワークロードの場合、XenApp および XenDesktop 7.15 LTSR と比較して約 10〜15% 少なくなります。

MDRLE コーデックの構成は不要です。Citrix Workspace アプリが MDRLE デコードをサポートしている場合、VDA は VDA MDRLE エンコードと Citrix Workspace アプリ MDRLE デコードを使用します。Citrix Workspace アプリが MDRLE デコードをサポートしていない場合、VDA は自動的に 2DRLE エンコードにフォールバックします。

MDRLE の要件:

- Citrix Virtual Apps and Desktops の最小バージョン 7 1808 VDA

- XenApp および XenDesktop の最小バージョン 7.17 VDA
- Citrix Workspace アプリ for Windows の最小バージョン 1808
- Citrix Receiver for Windows の最小バージョン 4.11

プログレッシブモード

Citrix Virtual Apps and Desktops 1808 では、プログレッシブモードが導入され、デフォルトで有効になりました。ネットワークの状態が制限されている場合（デフォルト：帯域幅 < 2 Mbps、または遅延 > 200 ms）、Thinwire は画面アクティビティ中のインタラクティブ性を向上させるために、テキストと静止画像の圧縮を強化しました。その後、画面アクティビティが停止すると、高度に圧縮されたテキストと画像は、ランダムなブロック方式で段階的にシャープ化されます。このように圧縮とシャープ化を行うことで、全体的なインタラクティブ性は向上しますが、キャッシュ効率が低下し、帯域幅の使用量が増加します。

Citrix Virtual Apps and Desktops 1906 以降、プログレッシブモードはデフォルトで無効になっています。現在、私たちは異なるアプローチを使用しています。静止画の品質は、ネットワークの状態に基づいており、各**視覚品質**設定の事前定義された最小値と最大値の間で変動します。明示的なシャープ化ステップがないため、Thinwire は画像配信を最適化し、キャッシュ効率を維持しながら、プログレッシブモードのほぼすべての利点を提供します。

プログレッシブモードの動作の変更

レジストリキーを使用してプログレッシブモードの状態を変更できます。詳しくは、レジストリで管理される機能のリストにあるプログレッシブモードを参照してください。

H.264 ロスレスビルド

ロスレスビルドは、インタラクティブ性と最終的な画質のためにグラフィック配信を最適化する特別なThinwire構成です。この設定は、**視覚品質**ポリシーを**ロスレスビルド**に設定することで有効にできます。

ロスレスビルドは、画面アクティビティ中にH.264（またはH.265）を使用して画面を圧縮し、アクティビティが停止するとピクセルパーフェクト（ロスレス）にシャープ化します。H.264（またはH.265）の画質は、利用可能なリソースに適応して、可能な限り最高のフレームレートを維持します。シャープ化ステップは段階的に実行され、シャープ化開始直後にユーザーが画面アクティビティを開始した場合でも即座に反応します。たとえば、モデルを選択して回転させる場合などです。

H.264 **ロスレスビルド**は、ハードウェアアクセラレーションを含むフルスクリーンH.264またはH.265のすべての利点を提供しますが、最終的に保証されたロスレス画面という追加の利点があります。これは、最終的なピクセルパーフェクトな画像を必要とする3Dタイプのワークロードに

とって重要です。たとえば、医療画像の操作などです。また、H.264 **ロスレスビルド**は、フルスクリーンH.264 4:4:4よりも少ないリソースを使用します。その結果、**ロスレスビルド**を使用すると、通常、視覚的にロスレスなH.264 4:4:4よりも高いフレームレートが得られます。

注：

視覚品質ポリシーに加えて、**ビデオコーデックの使用**ポリシーを**推奨時に使用**（デフォルト）または**アクティブに変更される領域の場合**に設定します。**ビデオコーデックの使用**ポリシーを**ビデオコーデックを使用しない**に設定することで、H.264以外のロスレスビルドに戻すことができます。これにより、動画はH.264（またはH.265）ではなくJPEGでエンコードされます。

テキストベースのセッションウォーターマーク

テキストベースのセッションウォーターマークは、データ盗難を抑止し、追跡を可能にするのに役立ちます。この追跡可能な情報は、写真やスクリーンキャプチャを使用してデータを盗む者への抑止力として、セッションデスクトップに表示されます。元のドキュメントの内容を変更することなく、セッション画面全体に表示されるテキストのレイヤーであるウォーターマークを指定できます。テキストベースのセッションウォーターマークにはVDAのサポートが必要です。

重要:

テキストベースのセッションウォーターマークは、セキュリティ機能ではありません。このソリューションはデータ盗難を完全に防ぐものではありませんが、ある程度の抑止力と追跡可能性を提供します。この機能を使用した場合の完全な情報追跡可能性は保証しませんが、必要に応じて他のセキュリティソリューションと組み合わせて使用することをお勧めします。

セッションウォーターマークはテキストであり、ユーザーに配信されるセッションに適用されます。セッションウォーターマークには、データ盗難を追跡するための情報が含まれています。最も重要なデータは、スクリーンイメージが取得された現在のセッションのログオンユーザーのIDです。データ漏洩をより効果的に追跡するために、サーバーまたはクライアントのインターネットプロトコルアドレスや接続時間などの他の情報を含めます。

ユーザーエクスペリエンスを調整するには、セッションウォーターマークポリシー設定 を使用して、画面上の配置とウォーターマークの外観を構成します。

要件:

仮想配信エージェント:

マルチセッションOS 7.17 シングルセッションOS 7.17

制限事項:

- セッションウォーターマークは、ローカルアプリアクセス、Windowsメディアリダイレクト、MediaStream、ブラウザコンテンツリダイレクト、およびHTML5ビデオリダイレクトが使用されているセッションではサポートされていません。セッションウォーターマークを使用するには、これらの機能が無効になっていることを確認してください。
- セッションが全画面ハードウェアアクセラレーションモード（全画面H.264またはH.265エンコーディング）で実行されている場合、セッションウォーターマークはサポートされず、表示されません。
- これらのHDX™ポリシーを設定すると、ウォーターマーク設定は有効にならず、セッション表示にウォーターマークは表示されません。

ビデオコーデックにハードウェアエンコーディングを使用 を **有効** **圧縮にビデオコーデックを使用** を **画面全体**

- これらのHDXポリシーを設定すると、動作は未定義となり、ウォーターマークが表示されない場合があります。

  ビデオコーデックにハードウェアエンコーディングを使用 を **有効** **圧縮にビデオコーデックを使用** を **優先する場合にビデオコーデックを使用**

  ウォーターマークが表示されるようにするには、**ビデオコーデックにハードウェアエンコーディングを使用** を **無効** に設定するか、**圧縮にビデオコーデックを使用** を **アクティブに変更される領域** または **ビデオコーデックを使用しない** に設定します。
- セッションウォーターマークは、Thinwireグラフィックモードのみをサポートします。
- セッションレコーディングを使用している場合、記録されたセッションにはウォーターマークは含まれません。
- Windowsリモートアシスタンスを使用している場合、ウォーターマークは表示されません。
- ユーザーが画面をキャプチャするために **Print Screen** キーを押した場合、VDA側でキャプチャされた画面にはウォーターマークは含まれません。キャプチャされた画像がコピーされるのを防ぐための対策を講じることをお勧めします。

画面共有

画面共有により、ユーザーはCitrix Virtual Desktopセッションを、画面コンテンツ、キーボード、マウスコントロールを含めて他のユーザーと共有できます。

システム要件

- Windows: シングルセッションまたはマルチセッションOS VDA
- Linux: Linuxセッションの共有に関する詳細については、Linux VDAドキュメントを参照してください。
- デスクトップセッションのみ共有できます。
- セッションをホストするVDAと、共有セッションに接続するマシンとの間にネットワーク接続が必要です。ネットワークポート要件は、使用中のICAポート（TCP/UDP 1494または2598）と、画面共有ポリシーの構成（デフォルトではTCP 52525〜52625）に基づいています。

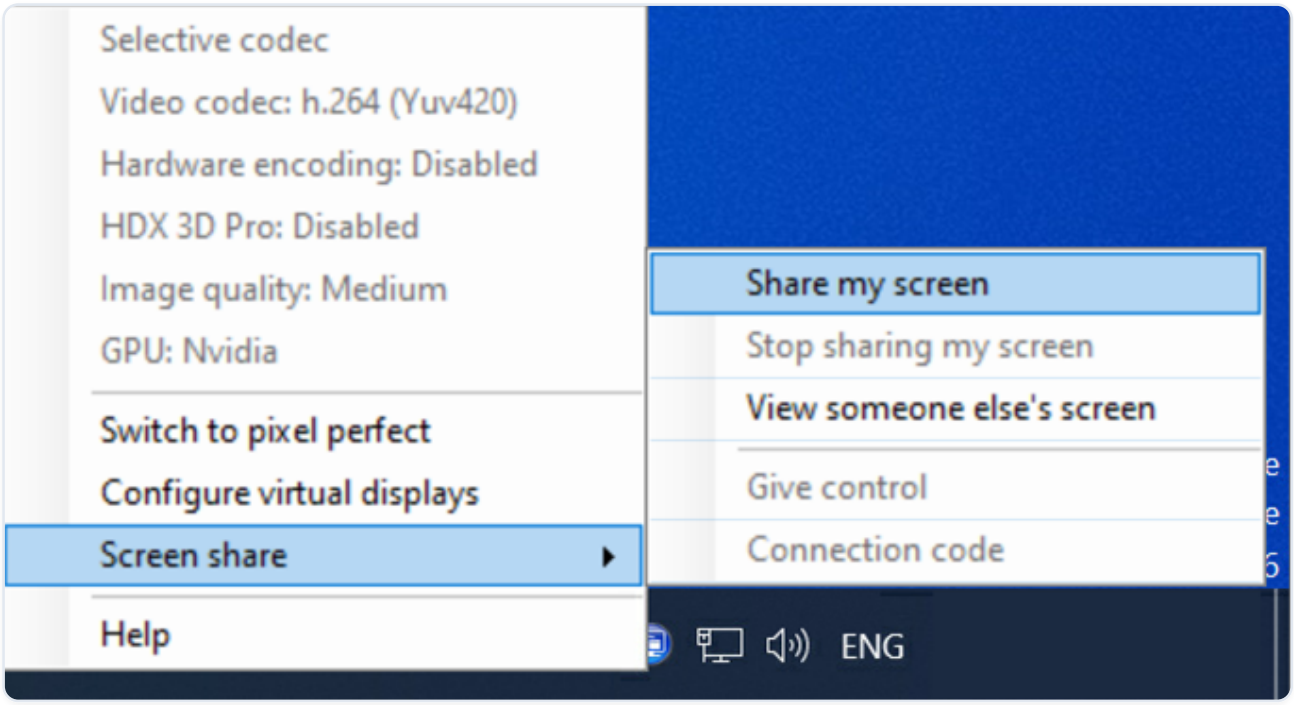
構成

画面共有はCitrixポリシーを使用して有効にする必要があります。画面共有はデフォルトで無効になっています。画面共有ポリシーを構成して、この機能を有効または無効にし、使用可能なネットワークポート範囲を割り当てます。

セッションの共有と接続のコントロールを含むユーザーインターフェイスを表示するには、グラフィックステータスインジケーターポリシーを有効にします。

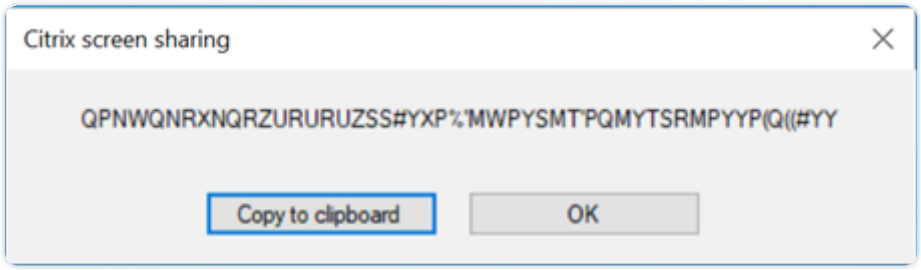
セッションの共有

セッションを共有するには、Windowsの通知領域にあるHDX™グラフィックステータスインジケーターアイコンを探します。アイコンを右クリックしてメニューを表示し、**画面共有 > 自分の画面を共有**を選択します。



クリップボードにコピーをクリックするか、ダイアログボックスに表示されている文字列全体を手動で選択してコピーします。この文字列は、電子メールやIMクライアントなど、任意のアプリケーションに貼り付けて他のユーザーに配布できます。

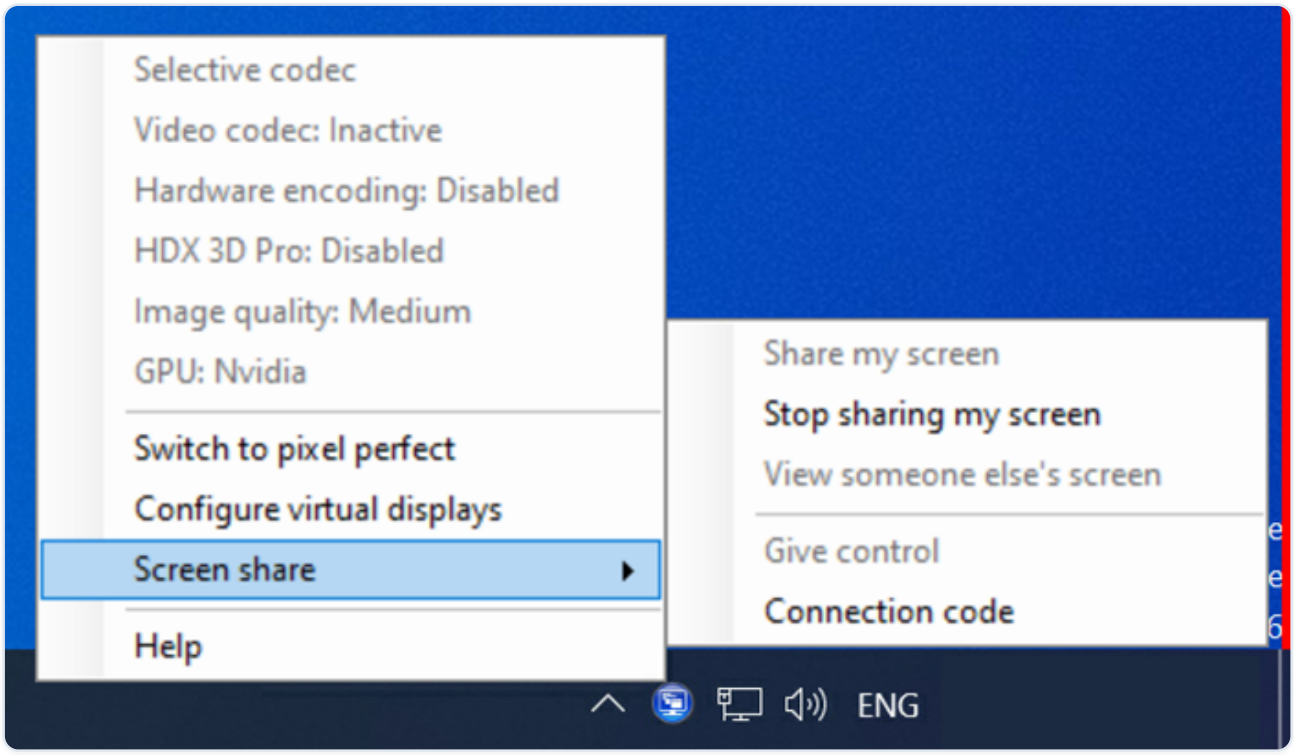
OKまたは**x**をクリックしてダイアログボックスを閉じます。セッションが共有されている間はいつでも、**画面共有 > 接続コード**メニューオプションから接続コードを取得できます。



セッションが共有されており、他のユーザーから見えることを示すために、画面の周囲に赤い枠線が表示されます。

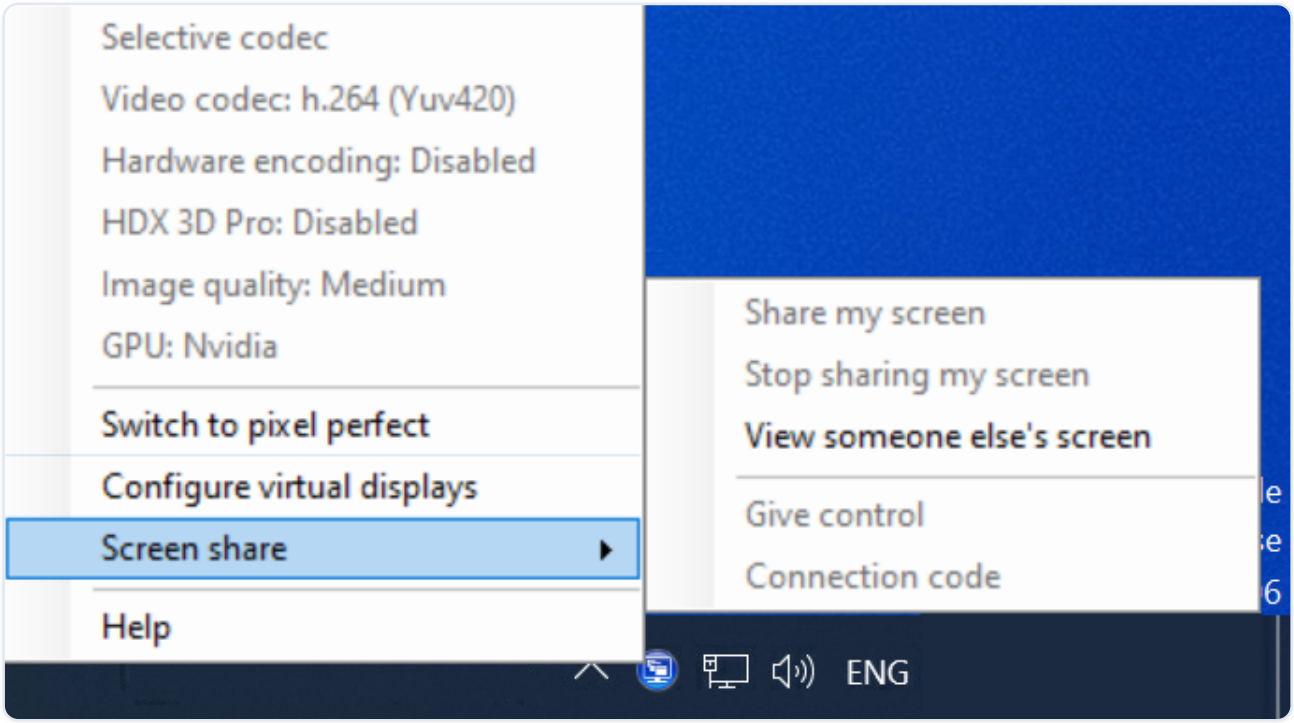
キーボードとマウスのコントロールも、**画面共有 > 制御を付与**メニューオプションを使用して他のユーザーと共有できます。

画面共有 > 自分の画面の共有を停止メニューオプションを使用して、セッションの共有を停止し、すべてのユーザーを切断します。

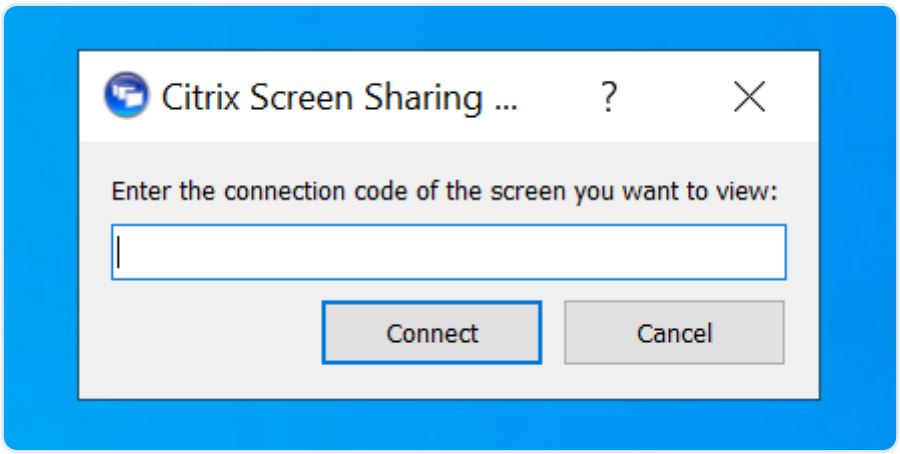


共有セッションへの接続

他のユーザーのセッションに接続するには、Windowsの通知領域にあるHDXグラフィックステータスインジケーターアイコンを探します。それを右クリックしてメニューを表示し、**画面共有 > 他のユーザーの画面を表示**を選択します。

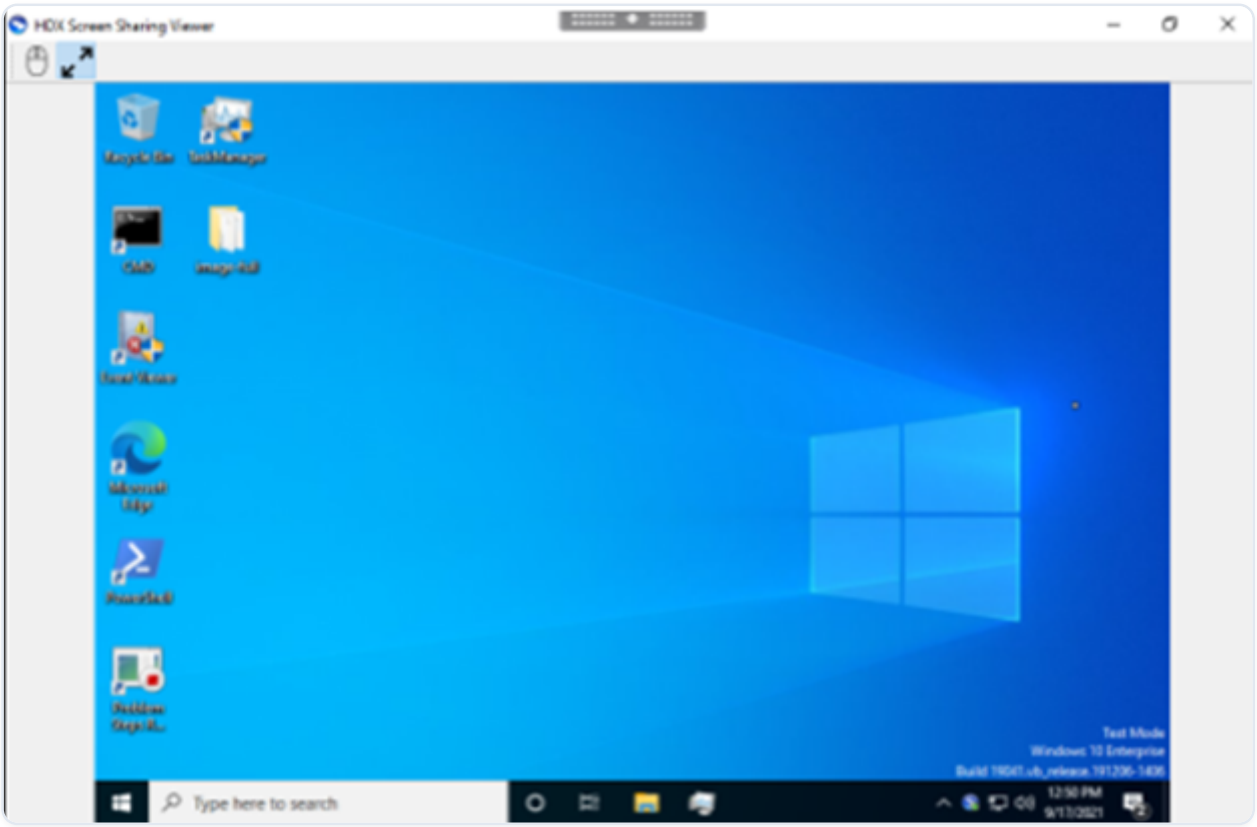


セッションを共有しているユーザーから提供された接続文字列をテキストボックスに入力または貼り付けます。**接続**をクリックして接続を確立します。



HDX画面共有ビューアウィンドウの左上隅にあるマウスアイコンをクリックすると、キーボードとマウスの制御を要求できます。

HDX画面共有ビューアウィンドウを閉じると、いつでも共有セッションから切断できます。



その他の考慮事項

- 画面共有ビューアアプリケーションは、VDAに*C:\Program Files\Citrix\HDX\bin\TwPlayer.exe*として含まれており、Virtual Apps Serverを使用して公開アプリケーションとして展開される場合があります。この代替展開モデルにより、仮想デスクトップにアクセスできないユーザーとのコラボレーションが可能になります。

- 共有セッションに接続できるユーザー数は、画面共有ポリシーのネットワークポート範囲を使用して制限できます。ユーザーごとに1つのポートが必要です。デフォルトの範囲では最大100ユーザーが許可されます。
- セッションに接続されているすべてのモニターが共有されます。個々のモニターを選択することはできません。
- H.265ビデオコーデックはサポートされていません。

マルチメディア

HDX™ テクノロジースタックは、2つの補完的なアプローチを通じてマルチメディアアプリケーションの配信をサポートします。

- サーバー側レンダリングによるマルチメディア配信
- クライアント側レンダリングによるマルチメディアリダイレクト

この戦略により、優れたユーザーエクスペリエンスで幅広いマルチメディア形式を配信できると同時に、サーバーのスケーラビリティを最大化してユーザーあたりのコストを削減できます。

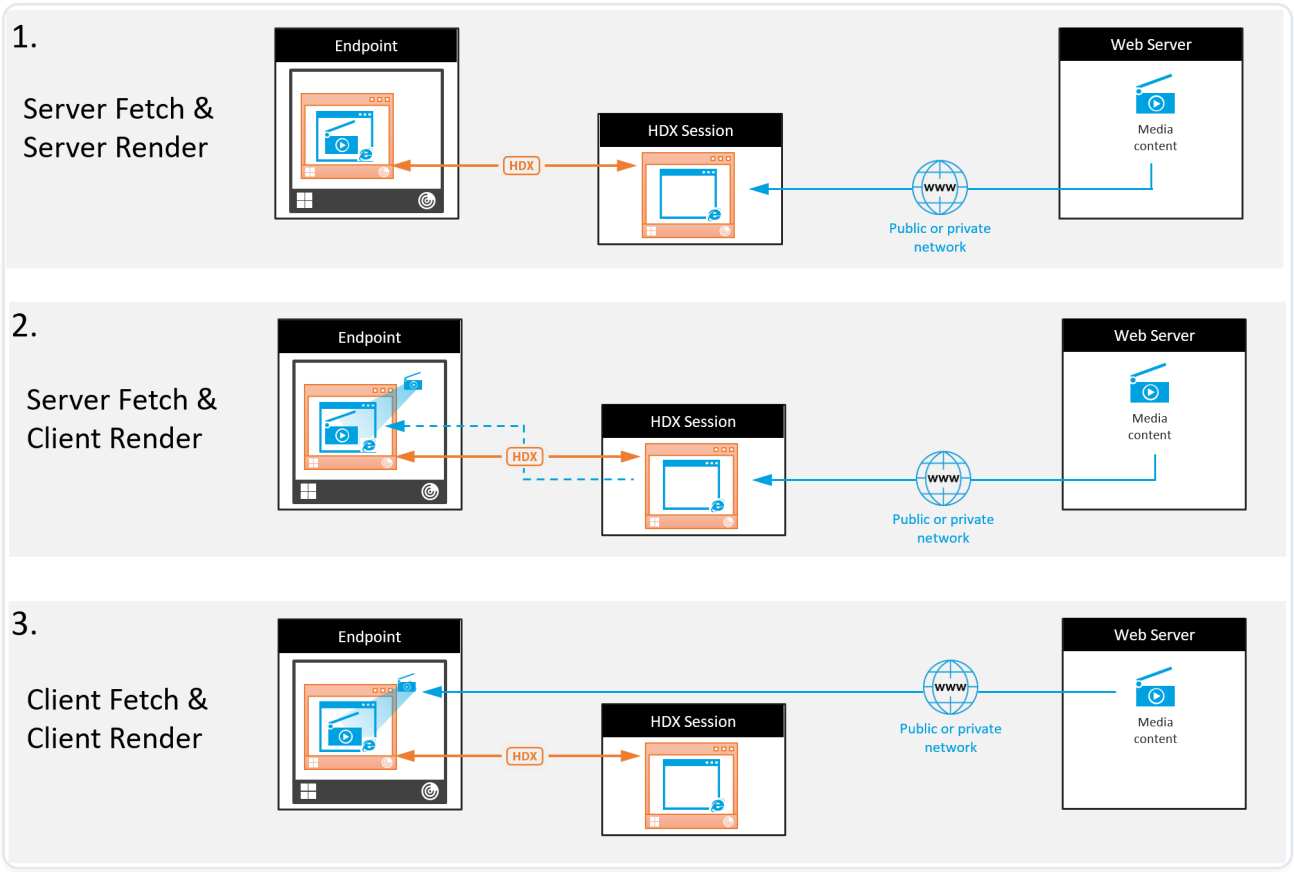
サーバー側でレンダリングされるマルチメディア配信では、オーディオおよびビデオコンテンツはアプリケーションによってCitrix Virtual Apps and Desktopsサーバー上でデコードおよびレンダリングされます。その後、コンテンツは圧縮され、ICAプロトコルを使用してユーザーデバイス上のCitrix Workspaceアプリに配信されます。この方法は、さまざまなアプリケーションおよびメディア形式との互換性を最大限に高めます。ビデオ処理は計算負荷が高いため、サーバー側でレンダリングされるマルチメディア配信は、オンボードのハードウェアアクセラレーションから大きな恩恵を受けます。たとえば、DirectX Video Acceleration (DXVA) のサポートにより、H.264デコードを個別のハードウェアで実行することでCPUの負荷を軽減します。Intel Quick Sync、AMD RapidFire、NVIDIA NVENCテクノロジーは、ハードウェアアクセラレーションによるH.264エンコーディングを提供します。

ほとんどのサーバーはビデオ圧縮のためのハードウェアアクセラレーションを提供しないため、すべてのビデオ処理がサーバーCPUで行われる場合、サーバーのスケーラビリティは悪影響を受けます。多くのマルチメディア形式をローカルレンダリングのためにユーザーデバイスにリダイレクトすることで、高いサーバーのスケーラビリティを維持できます。

- Windows Mediaリダイレクトは、通常Windows Media Playerに関連付けられているさまざまなメディア形式について、サーバーの負荷を軽減します。
- HTML5ビデオは普及しており、Citrix®はこの種のコンテンツ向けにリダイレクトテクノロジーを導入しました。HTML5、HLS、DASH、またはWebRTCを使用するWebサイトには、ブラウザコンテンツリダイレクトをお勧めします。
- 一般的なコンテンツリダイレクトテクノロジーであるホストからクライアントへのリダイレクトとローカルアプリアクセスをマルチメディアコンテンツに適用できます。

これらのテクノロジーを組み合わせると、リダイレクトを設定しない場合、HDXはサーバー側レンダリングを実行します。 リダイレクトを設定した場合、HDXはサーバーフェッチとクライアントレンダリング、またはクライアントフェッチとクライアントレンダリングのいずれかを使用します。これらの方法が失敗した場合、HDXは必要に応じてサーバー側レンダリングにフォールバックし、フォールバック防止ポリシーの対象となります。

シナリオ例



シナリオ1. (サーバーフェッチとサーバーレンダリング):

1. サーバーはソースからメディアファイルを取得し、デコードしてから、オーディオデバイスまたはディスプレイデバイスにコンテンツを提示します。
2. サーバーは、提示された画像またはサウンドをそれぞれディスプレイデバイスまたはオーディオデバイスから抽出します。
3. サーバーはオプションでそれを圧縮し、その後クライアントに送信します。

このアプローチでは、高いCPUコスト、高い帯域幅コスト（抽出された画像/音声が効率的に圧縮されていない場合）、および低いサーバー拡張性が発生します。

Thinwireおよびオーディオ仮想チャネルがこのアプローチを処理します。このアプローチの利点は、クライアントのハードウェアおよびソフトウェア要件を削減できることです。このアプローチ

を使用すると、デコードはサーバーで行われ、より幅広い種類のデバイスとフォーマットで動作します。

シナリオ2。（サーバーフェッチとクライアントレンダリング）：

このアプローチは、メディアコンテンツがデコードされ、オーディオまたはディスプレイデバイスに提示される前に傍受できることに依存しています。圧縮されたオーディオ/ビデオコンテンツは代わりにクライアントに送信され、そこでローカルでデコードおよび提示されます。このアプローチの利点は、クライアントデバイスにオフロードされ、サーバーのCPUサイクルを節約できることです。

しかし、これはクライアントに追加のハードウェアおよびソフトウェア要件ももたらします。クライアントは、受信する可能性のある各フォーマットをデコードできる必要があります。

シナリオ3。（クライアントフェッチとクライアントレンダリング）：

このアプローチは、メディアコンテンツのURLがソースからフェッチされる前に傍受できることに依存しています。URLはクライアントに送信され、そこでメディアコンテンツがフェッチ、デコード、およびローカルで提示されます。このアプローチは概念的にシンプルです。その利点は、サーバーが制御コマンドのみを送信するため、サーバーのCPUサイクルと帯域幅の両方を節約できることです。ただし、メディアコンテンツが常にクライアントからアクセスできるとは限りません。

フレームワークとプラットフォーム：

シングルセッションオペレーティングシステム（Windows、Mac OS X、Linux）は、マルチメディアアプリケーションのより迅速な開発を可能にするマルチメディアフレームワークを提供します。この表は、より一般的なマルチメディアフレームワークの一部をリストしています。各フレームワークは、メディア処理をいくつかの段階に分け、パイプラインベースのアーキテクチャを使用します。

フレームワーク	プラットフォーム
DirectShow	Windows (98以降)
メディア ファンデーション	ウィンドウズ (ビスタ以降)
Gストリーマー	リナックス
クイックタイム	マック オーエス テン

メディアリダイレクト技術によるダブルホップサポート

オーディオリダイレクト	いいえ
ブラウザコンテンツリダイレクト	いいえ
HDX Webカメラリダイレクト	はい
HTML5ビデオのリダイレクト	はい
Windows Mediaリダイレクト	はい

オーディオ機能

HDXオーディオ機能を最適化するポリシーに、以下のCitrixポリシー設定を構成して追加できます。使用方法の詳細、および他のポリシー設定との関係と依存関係については、「オーディオポリシー設定」、「帯域幅ポリシー設定」、および「マルチストリーム接続ポリシー設定」を参照してください。

アダプティブオーディオ

アダプティブオーディオを使用すると、VDAでオーディオ品質ポリシーを手動で構成する必要がありません。アダプティブオーディオは、環境に合わせて設定を最適化し、古いオーディオ圧縮形式を置き換えて、優れたユーザーエクスペリエンスを提供します。

アダプティブオーディオはデフォルトで有効になっています。アダプティブオーディオを無効にするには、「オーディオポリシー設定」を参照してください。

重要:

リアルタイムオーディオアプリケーションが必要な場合は、TCPではなくUser Datagram Protocol (UDP) を使用してオーディオを配信することをお勧めします。Windows Virtual Delivery Agent (VDA) のみがUDP経由のオーディオをサポートします。

DTLSを使用したUDPオーディオ暗号化は、Citrix GatewayとCitrix Workspace™ appの間でのみ利用可能です。そのため、TCPトランスポートを使用する方が望ましい場合があります。TCPは、VDAからCitrix Workspace appへのエンドツーエンドのTLS暗号化をサポートします。

> アダプティブオーディオとUDPオーディオの詳細については、「UDPリアルタイムトランスポート経由のオーディオとオーディオUDPポート範囲」を参照してください。

オーディオ品質

一般的に、音質が高いほど、より多くのオーディオデータをユーザーデバイスに送信するため、より多くの帯域幅とサーバーCPU使用率を消費します。サウンド圧縮を使用すると、音質とセッション全体のパフォーマンスのバランスを取ることができます。Citrixポリシー設定を使用して、サウンドファイルに適用する圧縮レベルを構成します。

デフォルトでは、**Audio quality policy**設定は、TCPトランスポートが使用されている場合、High - high definition audioに設定されています。UDPトランスポート（推奨）が使用されている場合、このポリシーはMedium - optimized-for-speechに設定されます。**High Definition audio**設定は、高忠実度のステレオオーディオを提供しますが、他の品質設定よりも多くの帯域幅を消費します。最適化されていない音声チャットやビデオチャットアプリケーション（ソフトフォンなど）には、このオーディオ品質を使用しないでください。これは、リアルタイム通信に適さない遅延をオーディオパスに導入する可能性があるためです。選択したトランスポートプロトコルに関係なく、リアルタイムオーディオにはoptimized for speechポリシー設定を推奨します。

帯域幅が制限されている場合（衛星接続やダイヤルアップ接続など）は、オーディオ品質を**Low**に下げると、消費される帯域幅が最小限になります。この状況では、低帯域幅接続のユーザー向けに個別のポリシーを作成し、高帯域幅接続のユーザーが悪影響を受けないようにします。

設定の詳細については、「オーディオポリシー設定」を参照してください。ユーザーデバイスでClient audio settingsを有効にすることを忘れないでください。

オーディオ再生と録音の帯域幅ガイドライン：

- アダプティブオーディオ（デフォルト）
  - ビットレート: 可変アダプティブ
  - チャンネル数: 再生用2（ステレオ）、マイクキャプチャ用1（モノラル）
  - 周波数: 48000 Hz
  - ビット深度: 16ビット
- 高音質
  - ビットレート：再生で約100 kbps（最小75、最大175 kbps）/マイクキャプチャで約70 kbps
  - チャンネル数：再生で2（ステレオ）、マイクキャプチャで1（モノラル）

    - 周波数：44100 Hz
    - ビット深度: 16ビット

- 中品質 (VoIPに推奨)
    - ビットレート: 再生時 ~16 kbps (最小20 kbps、最大40 kbps)、マイクキャプチャ時 ~16 kbps
    - チャンネル数: 再生とキャプチャの両方で1 (モノラル)
    - 周波数: 16000 Hz (広帯域)
    - ビット深度: 16ビット
- 低品質
    - ビットレート: 再生時 ~11 kbps (最小10 kbps、最大25 kbps)、マイクキャプチャ時 ~11 kbps
    - チャンネル数: 再生とキャプチャの両方で1 (モノラル)
    - 周波数: 8000 Hz (狭帯域)
    - ビット深度: 16ビット

クライアントオーディオリダイレクト

ユーザーデバイス上のスピーカーまたはその他のサウンドデバイスを介して、サーバー上のアプリケーションからオーディオを受信できるようにするには、**クライアントオーディオリダイレクト**設定を**許可**のままにします。これはデフォルトです。

クライアントオーディオマッピングは、サーバーとネットワークに余分な負荷をかけます。ただし、クライアントオーディオリダイレクトを禁止すると、すべてのHDX™オーディオ機能が無効になります。

設定の詳細については、「オーディオポリシー設定」を参照してください。ユーザーデバイスでクライアントオーディオ設定を有効にすることを忘れないでください。

クライアントマイクのリダイレクト

ユーザーデバイス上のマイクなどの入力デバイスを使用してユーザーがオーディオを録音できるようにするには、**クライアントマイクのリダイレクト**設定をデフォルト（許可）のままにします。

セキュリティのため、ユーザーデバイスは、信頼できないサーバーがマイクにアクセスしようとすると、ユーザーに警告します。ユーザーはマイクを使用する前に、アクセスを許可するか拒否するかを選択できます。ユーザーはCitrix Workspaceアプリでこの警告を無効にできます。

設定の詳細については、「オーディオポリシー設定」を参照してください。ユーザーデバイスでClient audio settingsを有効にすることを忘れないでください。

オーディオプラグアンドプレイ

オーディオプラグアンドプレイポリシー設定は、複数のオーディオデバイスを使用してサウンドを録音および再生することを許可または禁止します。この設定は、デフォルトで**有効**になっています。オーディオプラグアンドプレイにより、オーディオデバイスが認識されるようになります。ユーザーセッションが開始されるまで接続されていなくても、デバイスは認識されます。

この設定は、WindowsマルチセッションOSマシンにのみ適用されます。

設定の詳細については、「オーディオポリシー設定」を参照してください。

オーディオリダイレクト帯域幅制限とオーディオリダイレクト帯域幅制限の割合

オーディオリダイレクト帯域幅制限ポリシー設定は、セッションでのオーディオの再生と録音の最大帯域幅（キロビット/秒）を指定します。

オーディオリダイレクト帯域幅制限の割合設定は、オーディオリダイレクトの最大帯域幅を、利用可能な総帯域幅の割合として指定します。

デフォルトでは、両方の設定でゼロ（最大なし）が指定されています。両方の設定が構成されている場合、帯域幅制限が最も低い方が使用されます。

設定の詳細については、「帯域幅ポリシー設定」を参照してください。ユーザーデバイスでクライアントオーディオ設定を有効にすることを忘れないでください。

UDPリアルタイムトランスポート経由のオーディオとオーディオUDPポート範囲

デフォルトでは、ユーザーデータグラムプロトコル（UDP）リアルタイムトランスポート経由のオーディオは許可されています（インストール時に選択した場合）。これは、UDPリアルタイムトランスポート経由のオーディオを使用する接続のために、サーバー上にUDPポートを開きます。ネットワークの輻輳やパケット損失がある場合は、可能な限り最高のユーザーエクスペリエンスを確保するために、オーディオにUDP/RTPを構成することをお勧めします。ソフトフォンアプリケーションなどのリアルタイムオーディオの場合、EDTよりもUDPオーディオが推奨されます。UDPは再送信なしでパケット損失を許容するため、パケット損失が多い接続で遅延が追加されることはありません。

重要:

Citrix Gatewayが経路にない場合、UDPで送信されるオーディオデータは暗号化されません。Citrix GatewayがCitrix Virtual Apps and Desktops™リソースにアクセスするように構成されている場合、エンドポイントデバイスとCitrix Gateway間のオーディオトラフィックはDTLSプロトコルを使用して保護されます。

オーディオUDPポート範囲は、Windows VDAがユーザーデバイスとオーディオパケットデータを交換するために使用するポート番号の範囲を指定します。

デフォルトでは、範囲は16500から16509です。

注：

適応型オーディオにUDPリアルタイムトランスポート経由のオーディオが必要ない場合、Citrixはポリシー設定を「無効」に構成することを推奨します。これにより、Citrix Workspaceアプリクライアントが UDP接続のオープンを要求したり、不要なCitrix Workspaceアプリクライアントのファイアウォール構成ダイアログウィンドウが表示されたりするのを防ぐことができます。

UDPリアルタイムトランスポート経由のオーディオに関する設定の詳細については、オーディオポリシー設定を参照してください。オーディオUDPポート範囲の詳細については、マルチストリーム接続ポリシー設定を参照してください。ユーザーデバイスでクライアントオーディオ設定を有効にすることを忘れないでください。

UDP経由のオーディオにはWindows VDAが必要です。Linux VDAでサポートされているポリシーについては、ポリシーサポートリストを参照してください。

ユーザーデバイスのオーディオ設定ポリシー

1. グループポリシーオブジェクト管理用テンプレートの構成に従って、グループポリシーテンプレートをロードします。
2. グループポリシーエディターで、**管理用テンプレート > Citrixコンポーネント > Citrix Workspace > ユーザーエクスペリエンス**を展開します。
3. **クライアントオーディオ設定**で、**未構成**、**有効**、または**無効**を選択します。

- **未構成**。デフォルトでは、オーディオリダイレクトは高品質オーディオまたは以前に構成されたカスタムオーディオ設定を使用して有効になっています。
- **有効**。選択したオプションを使用してオーディオリダイレクトを有効にします。
- **無効**。オーディオリダイレクトを無効にします。

4. **有効**を選択した場合、音質を選択します。UDPオーディオの場合は、**中**（デフォルト）を使用します。
5. UDPオーディオの場合のみ、**リアルタイムトランスポートを有効にする**を選択し、ローカルのWindowsファイアウォールで開く受信ポートの範囲を設定します。
6. Citrix Gateway で UDP Audio を使用するには、**Allow Real-Time Transport Through gateway** を選択します。Citrix Gateway を DTLS で構成します。詳細については、こちらの記事を参照してください。

管理者として、これらの変更を行うためのエンドポイントデバイスを制御できない場合は、StoreFront の default.ica 属性を使用して UDP Audio を有効にします。たとえば、BYOD (個人所有デバイス) や自宅のコンピューターの場合などです。

1. StoreFront マシンで、メモ帳などのエディターを使用して C:\inetpub\wwwroot\Citrix\\\<Store Name>\App_Data\default.ica を開きます。
2. セクションに以下のエントリを作成します。

   ; このテキストはリアルタイムトランスポートを有効にします

   RTPオーディオを有効にする=true

   ; このテキストはゲートウェイ経由のリアルタイムトランスポートを許可します

   ゲートウェイ経由のUDPを有効にする=true

   ; このテキストはオーディオ品質を「中」に設定します

   AudioBandwidthLimit=1

   ; UDP ポート範囲

   RtpAudioLowestPort=16500

   RtpAudioHighestPort=16509

default.ica を編集してユーザーデータグラムプロトコル (UDP) オーディオを有効にすると、そのストアを使用しているすべてのユーザーに対して UDP オーディオが有効になります。

マルチメディア会議中のエコーを回避する

オーディオまたはビデオ会議のユーザーはエコーを聞くことがあります。エコーは通常、スピーカーとマイクが互いに近すぎるときに発生します。そのため、オーディオおよびビデオ会議にはヘッドセットの使用をお勧めします。

HDXは、エコーを最小限に抑えるエコーキャンセレーションオプション（デフォルトで有効）を提供します。エコーキャンセレーションの有効性は、スピーカーとマイクの間の距離に影響されます。デバイスが互いに近すぎたり遠すぎたりしないようにしてください。

レジストリ設定を変更して、エコーキャンセレーションを無効にできます。詳細については、レジストリを介して管理される機能のリストにあるマルチメディア会議中のエコーを回避するを参照してください。

ソフトフォン

ソフトフォンは、電話インターフェースとして機能するソフトウェアです。ソフトフォンを使用して、コンピューターやその他のスマートデバイスからインターネット経由で電話をかけます。ソフトフォンを使用すると、画面を使って電話番号をダイヤルしたり、その他の電話関連機能を実行したりできます。

Citrix Virtual Apps and Desktopsは、ソフトフォンを配信するためのいくつかの代替手段をサポートしています。

- **制御モード**。ホストされているソフトフォンが物理的な電話機を制御します。このモードでは、Citrix Virtual Apps and Desktopsサーバーを介してオーディオトラフィックは流れません。
- **HDX RealTime最適化ソフトフォンサポート（推奨）**。メディアエンジンはユーザーデバイス上で実行され、Voice over Internet Protocolトラフィックはピアツーピアで流れます。例については、以下を参照してください。
  - Microsoft Teams向けHDX最適化
  - HDX RealTime Optimization Pack（Microsoft Skype for Businessの配信を最適化します）
  - Cisco Jabber Softphone for VDI (シスコ ジャバー ソフトフォン フォー VDI)（旧称VXME）
  - VDI向け シスコ Webex ミーティング
  - Avaya VDI Equinox（以前はVDI Communicatorという名称でした）
  - Zoom VDI Plugin (ズーム VDI プラグイン)
  - Genesys PureEngage クラウド
  - Nuance Dragon PowerMic ディクテーションデバイス

- **ローカルアプリアクセス**。Citrix Virtual Apps and Desktopsの機能で、ソフトフォンなどのアプリケーションをWindowsユーザーデバイス上でローカルに実行しながら、仮想/公開デスクトップとシームレスに統合されているように見せることができます。この機能は、すべてのオーディオ処理をユーザーデバイスにオフロードします。詳細については、「ローカルアプリアクセスとURLリダイレクト」を参照してください。
- **HDX RealTime汎用ソフトフォンサポート**。ICA経由のVoice over Internet Protocol。

汎用ソフトフォンサポート

汎用ソフトフォンサポートにより、データセンターのXenAppまたはXenDesktopで未変更のソフトフォンをホストできます。オーディオトラフィックは、Citrix ICAプロトコル（できればUDP/RTPを使用）を介して、Citrix Workspaceアプリを実行しているユーザーデバイスに送信されます。

汎用ソフトフォンサポートは、HDX RealTimeの機能です。このソフトフォン配信アプローチは、特に次の場合に役立ちます。

- ソフトフォンを配信するための最適化されたソリューションが利用できず、ユーザーがLocal App Accessを使用できるWindowsデバイスを使用していない場合。
- ソフトフォンの最適化された配信に必要なメディアエンジンがユーザーデバイスにインストールされていないか、ユーザーデバイスで実行されているオペレーティングシステムのバージョンで利用できない場合。このシナリオでは、汎用HDX RealTimeが貴重なフォールバックソリューションを提供します。

Citrix Virtual Apps and Desktopsを使用する際のソフトフォン配信には、次の2つの考慮事項があります。

- ソフトフォンアプリケーションが仮想/公開デスクトップにどのように配信されるか。
- ユーザーのヘッドセット、マイク、スピーカー、またはUSB電話機にオーディオがどのように配信されるか。

Citrix Virtual Apps and Desktopsには、汎用ソフトフォン配信をサポートするための多数のテクノロジーが含まれています。

- リアルタイムオーディオの高速エンコードと帯域幅効率のためのOptimized-for-Speechコーデック。
- 低遅延オーディオスタック。
- ネットワーク遅延が変動したときにオーディオをスムーズにするサーバー側ジッターバッファ。

- サービス品質のためのパケットタグ付け (DSCP および WMM)。
  - RTPパケットのDSCPタグ付け (レイヤー3)
  - Wi-FiのWMMタグ付け

Windows、Linux、Chrome、Mac版のCitrix Workspaceアプリも、Voice over Internet Protocolに対応しています。Windows版Citrix Workspaceアプリは、以下の機能を提供します。

- クライアント側のジッターバッファ - ネットワーク遅延が変動しても、スムーズなオーディオを保証します。
- エコーキャンセル - ヘッドセットを使用しない作業者向けに、マイクとスピーカー間の距離の変動を大きく許容します。
- オーディオプラグアンドプレイ - オーディオデバイスは、セッションを開始する前に接続する必要はありません。いつでも接続できます。
- オーディオデバイスルーティング - ユーザーは着信音をスピーカーに、音声パスをヘッドセットにルーティングできます。
- マルチストリームICA - ネットワーク上で柔軟なサービス品質ベースのルーティングを可能にします。
- ICAは4つのTCPストリームと2つのUDPストリームをサポートします。UDPストリームの1つは、RTPを介したリアルタイムオーディオをサポートします。

Citrix Workspaceアプリの機能の概要については、Citrix Receiver Feature Matrixを参照してください。

システム構成の推奨事項

クライアントハードウェアとソフトウェア: 最適なオーディオ品質を得るには、最新バージョンのCitrix Workspaceアプリと、音響エコーキャンセル (AEC) 機能を備えた高品質のヘッドセットをお勧めします。Windows、Linux、Mac版のCitrix Workspaceアプリは、Voice over Internet Protocolをサポートしています。また、Dell WyseはThinOS (WTOS) 向けにVoice over Internet Protocolをサポートしています。

CPUに関する考慮事項: VDAのCPU使用率を監視して、各仮想マシンに2つの仮想CPUを割り当てる必要があるかどうかを判断します。リアルタイムの音声とビデオはデータ集約型です。2つの仮想CPUを構成すると、スレッド切り替えの遅延が減少します。したがって、Citrix Virtual Desktops™ VDI環境では2つのvCPUを構成することをお勧めします。

2つの仮想CPUを持つことは、物理CPUの数を2倍にすることを必ずしも意味しません。物理CPUはセッション間で共有できるためです。

Citrix Gateway Protocol (CGP) は、セッション信頼性機能に使用され、CPU 消費も増加させます。高品質のネットワーク接続では、VDA の CPU 消費を削減するためにこの機能を無効にできます。強力なサーバーでは、上記のいずれのステップも不要な場合があります。

UDPオーディオ: UDP経由のオーディオは、ネットワークの輻輳とパケット損失に対して優れた耐性を提供します。利用可能な場合は、TCPの代わりにこれをお勧めします。

LAN/WAN構成: 良好なリアルタイムオーディオ品質のためには、ネットワークの適切な構成が不可欠です。通常、過剰なブロードキャストパケットはジッターを引き起こす可能性があるため、仮想LAN (VLAN) を構成する必要があります。IPv6対応デバイスは多くのブロードキャストパケットを生成する可能性があります。IPv6サポートが不要な場合は、それらのデバイスでIPv6を無効にできます。Quality of Serviceをサポートするように構成してください。

WAN接続の使用設定: LANおよびWAN接続を介してボイスチャットを使用できます。WAN接続では、オーディオ品質は接続の遅延、パケット損失、およびジッターに依存します。WAN接続のユーザーにソフトフォンを配信する場合、データセンターとリモートオフィス間でNetScaler® SD-WANを使用することをお勧めします。これにより、高いQuality of Serviceが維持されます。NetScaler SD-WANは、UDPを含むMulti-Stream ICAをサポートしています。また、単一のTCPストリームの場合、さまざまなICA仮想チャネルの優先順位を区別して、高優先度のリアルタイムオーディオデータが優先的に処理されるようにすることが可能です。

DirectorまたはHDX Monitorを使用して、HDX構成を検証します。

リモートユーザー接続: Citrix Gatewayは、UDP/RTPトラフィックをネイティブに（TCPでのカプセル化なしで）配信するためにDTLSをサポートしています。 ポート443経由のUDPトラフィックに対してファイアウォールを双方向に開きます。

コーデックの選択と帯域幅の消費: ユーザーデバイスとデータセンター内のVDAの間では、**Optimized-for-Speech**コーデック設定（中品質オーディオとも呼ばれます）を使用することをお勧めします。VDAプラットフォームとIP-PBXの間では、ソフトフォンは構成またはネゴシエートされたコーデックを使用します。例：

- G711は良好な音声品質を提供しますが、1コールあたり80キロビット/秒から100キロビット/秒の帯域幅要件があります（ネットワークレイヤー2のオーバーヘッドに依存）。
- G729は良好な音声品質を提供し、1コールあたり30キロビット/秒から40キロビット/秒の低い帯域幅要件があります（ネットワークレイヤー2のオーバーヘッドに依存）。

仮想デスクトップへのソフトフォンアプリケーションの配信

XenDesktop®仮想デスクトップにソフトフォンを配信するには、2つの方法があります。

- アプリケーションは仮想デスクトップイメージにインストールできます。
- アプリケーションはMicrosoft App-Vを使用して仮想デスクトップにストリーミングできます。このアプローチには、仮想デスクトップイメージが整理された状態に保たれるため、管理上の利点があります。仮想デスクトップにストリーミングされた後、アプリケーションは通常の方法でインストールされたかのようにその環境で実行されます。すべてのアプリケーションがApp-Vと互換性があるわけではありません。

ユーザーデバイスとの間のオーディオ配信

汎用HDX RealTimeは、ユーザーデバイスとの間でオーディオを配信する2つの方法をサポートしています。

- **Citrix Audio Virtual Channel**。Citrix Audio Virtual Channelはオーディオ転送専用に設計されているため、一般的に推奨されます。
- **Generic USB Redirection**。ユーザーデバイスがCitrix Virtual Apps and Desktopsサーバーへの LANまたはLANに似た接続上にある場合、ボタンまたはディスプレイ（あるいはその両方）を備えたオーディオデバイス、ヒューマンインターフェースデバイス（HID）をサポートします。

Citrix オーディオ仮想チャネル

双方向のCitrixオーディオ仮想チャネル（CTXCAM）により、オーディオをネットワーク経由で効率的に配信できます。汎用HDX RealTimeは、ユーザーのヘッドセットまたはマイクからのオーディオを取得して圧縮します。その後、ICAを介して仮想デスクトップ上のソフトフォンアプリケーションに送信します。同様に、ソフトフォンのオーディオ出力は圧縮され、逆方向にユーザーのヘッドセットまたはスピーカーに送信されます。この圧縮は、ソフトフォン自体が使用する圧縮（G.729やG.711など）とは独立しています。これは、Optimized-for-Speechコーデック（中品質）を使用して行われます。その特性は、Voice over Internet Protocolに最適です。エンコード時間が短く、ネットワーク帯域幅はピーク時で約56キロビット/秒（各方向28 Kbps）しか消費しません。このコーデックは、デフォルトのオーディオコーデックではないため、Studioコンソールで明示的に選択する必要があります。デフォルトはHDオーディオコーデック（高品質）です。このコーデックは高忠実度のステレオサウンドトラックに優れていますが、Optimized-for-Speechコーデックと比較してエンコードが遅いです。

汎用 USB リダイレクト

Citrix Generic USB Redirectionテクノロジー（CTXGUSB仮想チャネル）は、複合デバイス（オーディオとHID）およびアイソクロナスUSBデバイスを含むUSBデバイスをリモートで利用するための汎用的な手段を提供します。このアプローチは、LAN接続されたユーザーに限定されます。その理由は、USBプロトコルがネットワーク遅延に敏感であり、かなりのネットワーク帯域幅を必要

とする傾向があるためです。アイソクロナスUSBリダイレクトは、一部のソフトフォンを使用する場合にうまく機能します。このリダイレクトは、優れた音声品質と低遅延を提供します。ただし、Citrix Audio Virtual Channelはオーディオトラフィックに最適化されているため、こちらが推奨されます。主な例外は、ボタン付きのオーディオデバイスを使用している場合です。たとえば、データセンターにLAN接続されたユーザーデバイスに接続されたUSB電話などです。この場合、Generic USB Redirectionは、ソフトフォンに信号を送り返すことで機能を制御する、電話機またはヘッドセットのボタンをサポートします。デバイス上でローカルに機能するボタンには問題ありません。

制限事項

クライアントにオーディオデバイスをインストールし、オーディオリダイレクトを有効にして、RDSセッションを開始します。オーディオファイルが再生に失敗し、エラーメッセージが表示されることがあります。

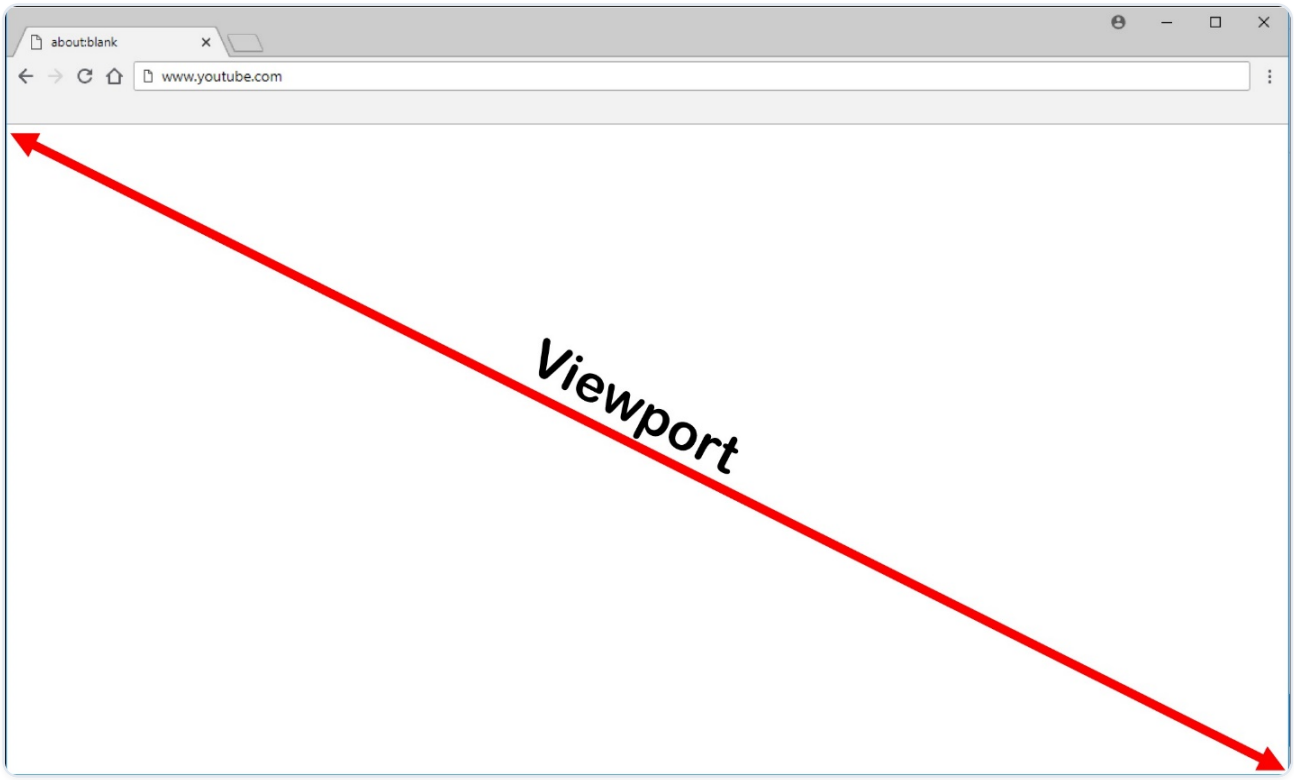
回避策として、RDSマシンにレジストリキーを追加し、マシンを再起動します。詳細については、レジストリで管理される機能のリストにあるオーディオの制限を参照してください。

ブラウザコンテンツリダイレクト

ブラウザコンテンツリダイレクトは、許可リストにあるWebページのVDA側でのレンダリングを防ぎます。この機能は、Citrix Workspace™ app for Windows または Citrix Workspace app for Linux を使用して、クライアント側で対応するレンダリングエンジンをインスタンス化し、URLからHTTPおよびHTTPSコンテンツを取得します。

> **注：**
>
> ブロックリストを使用すると、WebページをVDA側にリダイレクトする（クライアント側ではリダイレクトしない）ように指定できます。
>
> このオーバーレイWebレイアウトエンジンは、VDA上ではなくエンドポイントデバイス上で実行され、エンドポイントのCPU、GPU、RAM、およびネットワークを使用します。

リダイレクトされるのはブラウザのビューポートのみです。ビューポートとは、コンテンツが表示されるブラウザの長方形の領域です。ビューポートには、アドレスバー、**お気に入り**ツールバー、ステータスバーなどは含まれません。これらの項目はユーザーインターフェイスにあり、VDAのブラウザで引き続き実行されています。



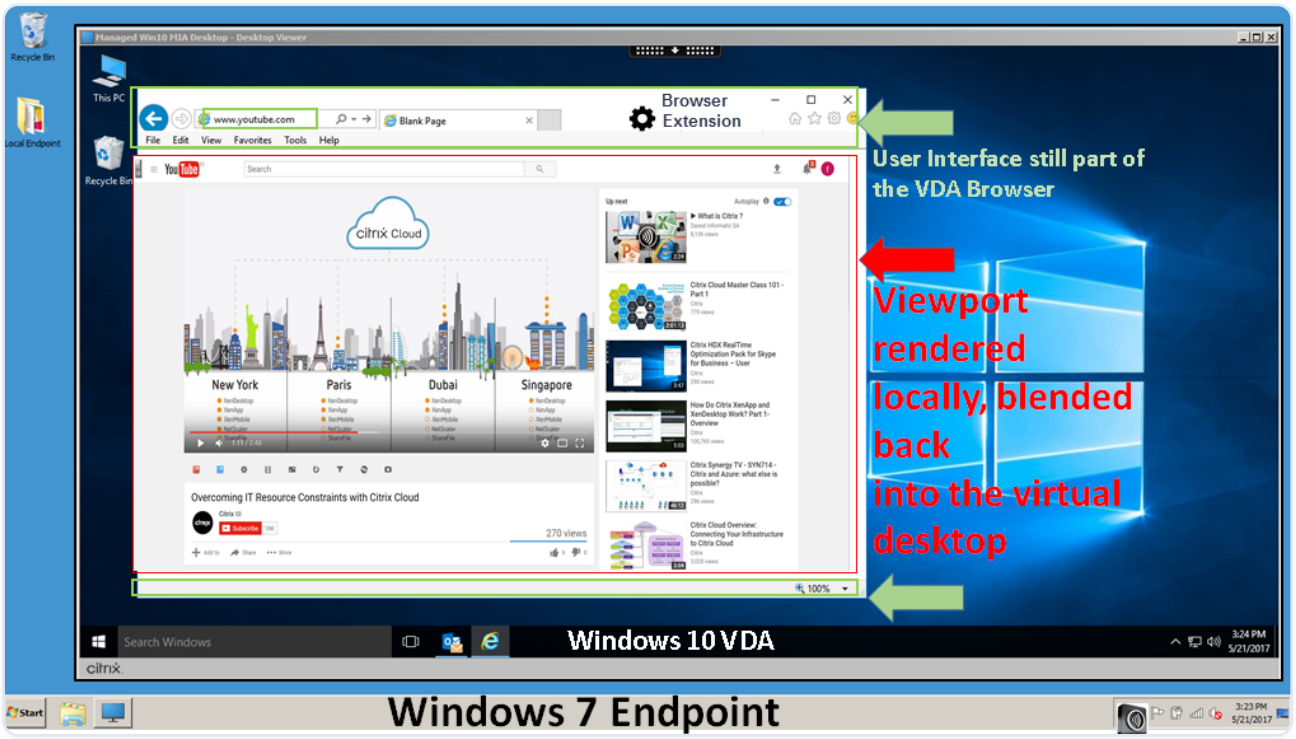
1. リダイレクトの許可リストに含まれるURL、または特定のURLパスのリダイレクトを無効にするブロックリストを含むアクセス制御リストを指定するStudioポリシーを構成します。VDA上のブラウザが、ユーザーがアクセスしているURLが許可リストと一致するか、ブロックリストと一致しないことを検出するには、ブラウザ拡張機能が比較を実行します。Internet Explorer 11のブラウザ拡張機能はインストールメディアに含まれており、自動的にインストールされます。Chromeの場合、ブラウザ拡張機能はChromeウェブストアで入手でき、グループポリシーとADMXファイルを使用して展開できます。Chrome拡張機能はユーザーごとにインストールされます。拡張機能を追加または削除するためにゴールデンイメージを更新する必要はありません。
2. 許可リストに一致するものが見つかり（例: `https://www.mycompany.com/`）、ブロックリストのURLに一致するものがない場合（例: `https://www.mycompany.com/engineering`）、仮想チャネル（CTXCSB）がCitrix Workspace appにリダイレクトが必要であることを指示し、URLを中継します。その後、Citrix Workspace appはローカルレンダリングエンジンをインスタンス化し、Webサイトを表示します。
3. その後、Citrix Workspace appはWebサイトを仮想デスクトップのブラウザコンテンツ領域にシームレスにブレンドして戻します。

> **注：**
>
> ブラウザコンテンツリダイレクト拡張機能の新機能と修正の詳細については、Chromeウェブストアにアクセスし、「citrix® bcr」を検索して拡張機能を見つけてください。

> ロゴの色はChrome拡張機能のステータスを示します。以下の3色のいずれかです。

- 緑：アクティブで接続済み。
- 灰色：現在のタブで非アクティブ/アイドル状態。
- 赤：破損/動作していません。

拡張機能メニューの**オプション**を使用して、ログのデバッグが可能です。



Citrix Workspaceアプリがコンテンツを取得するシナリオを次に示します。

- **サーバーフェッチとサーバーレンダリング**: サイトを許可リストに追加しなかったか、リダイレクトが失敗したため、リダイレクトは行われません。VDAでWebページをレンダリングし、Thinwireを使用してグラフィックをリモート処理します。フォールバック動作を制御するにはポリシーを使用します。VDAでのCPU、RAM、および帯域幅の消費量が高くなります。
- **サーバーフェッチとクライアントレンダリング**: Citrix Workspaceアプリは、仮想チャネル (CTXPFWD) を使用してVDAを介してWebサーバーに接続し、コンテンツを取得します。このオプションは、クライアントがインターネットアクセスを持たない場合 (シンクライアントなど) に役立ちます。VDAでのCPUとRAMの消費量は低いですが、ICA®仮想チャネルで帯域幅が消費されます。

  このシナリオには3つの動作モードがあります。「プロキシ」という用語は、VDAがインターネットアクセスを得るためにアクセスするプロキシデバイスを指します。

  選択するポリシーオプション:

- 明示的プロキシ - データセンターに単一の明示的プロキシがある場合。
- 直接または透過的 - プロキシがない場合、または透過的プロキシを使用している場合。
- PACファイル - VDA内のブラウザが指定されたURLを取得するために適切なプロキシサーバーを自動的に選択できるように、PACファイルに依存している場合。

PACファイル(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/browser-content-redirection-direct-pac.png)

- **クライアントフェッチとクライアントレンダリング**: Citrix WorkspaceアプリがWebサーバーに直接接続するため、インターネットアクセスが必要です。このシナリオでは、XenAppおよびXenDesktop®サイトからすべてのネットワーク、CPU、およびRAMの使用量をオフロードします。

  利点:

  - より良いエンドユーザーエクスペリエンス (アダプティブビットレート (ABR))
  - VDAリソース使用量の削減 (CPU/RAM/IO)
  - 帯域幅消費量の削減

ブラウザビューポートリダイレクトシナリオの画像(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/browser-viewport-redirection-scenarios.png)

フォールバックメカニズム:

クライアントリダイレクトが失敗する場合があります。たとえば、クライアントマシンがインターネットに直接アクセスできない場合、エラー応答がVDAに戻されることがあります。そのような場合、VDA上のブラウザはページを再読み込みし、サーバー上でレンダリングできます。

既存の**Windows Media フォールバック防止**ポリシーを使用すると、ビデオ要素のサーバーレンダリングを抑制できます。このポリシーを**すべてのコンテンツをクライアントでのみ再生**または**クライアントでアクセス可能なコンテンツのみをクライアントで再生**に設定します。これらの設定は、クライアントリダイレクトで障害が発生した場合に、ビデオ要素がサーバーで再生されるのをブロックします。このポリシーは、ブラウザコンテンツリダイレクトを有効にし、**アクセス制御リスト**ポリシーにフォールバックするURLが含まれている場合にのみ有効になります。URLはブロックリストポリシーに含めることはできません。

システム要件:

Windowsエンドポイント:

- ウィンドウズ 10

- Citrix Workspaceアプリ 1809 for Windows以降

> **注：**
>
> ブラウザコンテンツリダイレクトは、Citrix Workspaceアプリ for WindowsのCurrent Releaseでのみサポートされており、Citrix WorkspaceアプリLTSRリリース（1912および2203.1）ではサポートされていません。

> Linuxエンドポイント:

- Citrix Workspaceアプリ 1808 for Linux以降
- シンクライアント端末にはWebKitGTK+が含まれている必要があります

Citrix Virtual Apps and Desktops 7 1808以降およびXenApp and XenDesktop 7.15 CU5以降:

- VDAオペレーティングシステム: Windows 10（最小バージョン1607）、Windows Server 2012 R2、Windows Server 2016、Windows Server 2019
- VDA上のブラウザ:
  - Google Chrome v66以降（Chromeには、ユーザーエンドポイントにCitrix Workspaceアプリ 1809 for Windows以降、Citrix Virtual Apps and Desktops™ 7 1808 VDA以降、およびブラウザコンテンツリダイレクト拡張機能が必要です）
  - Internet Explorer 11と以下のオプションを構成します:
    - **インターネットオプション** > **詳細設定** > **セキュリティ**で**拡張保護モード**をオフにします
    - **インターネットオプション** > **詳細設定** > **閲覧**で**サードパーティ製のブラウザ拡張機能を有効にする**をオンにします

トラブルシューティング

トラブルシューティング情報については、Knowledge Centerの記事https://support.citrix.com/article/CTX230052を参照してください。

ブラウザコンテンツリダイレクトChrome拡張機能

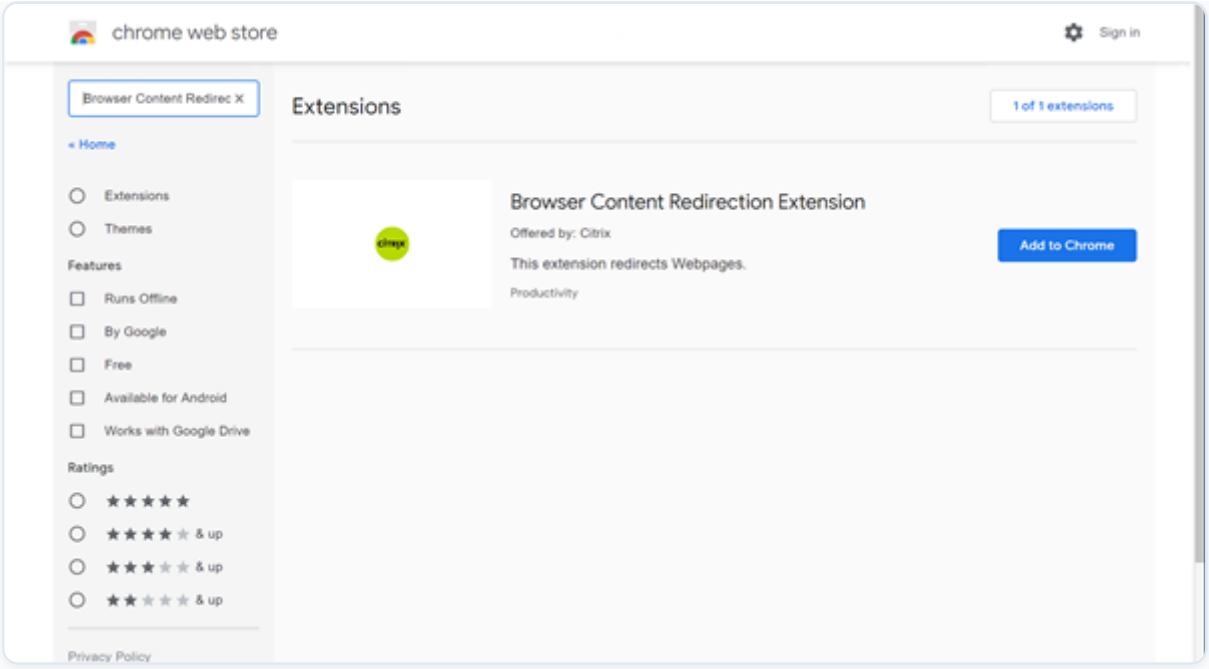
Chromeでブラウザコンテンツリダイレクトを使用するには、Chromeウェブストアからブラウザコンテンツリダイレクト拡張機能を追加します。Citrix Virtual Apps and Desktops環境で**Chromeに追加**をクリックします。

この拡張機能は、ユーザーのクライアントマシンには**不要**です。VDAにのみ必要です。

システム要件

- Chrome v66以降
- ブラウザコンテンツリダイレクト拡張機能
- シトリックス バーチャル アプリケーションズ アンド デスクトップス 7 1808以降
- Windows向けCitrix Workspaceアプリ1809以降

> **注：**
>
> ブラウザコンテンツリダイレクトは、Windows向けCitrix WorkspaceアプリのCurrent Releaseでのみサポートされており、Citrix WorkspaceアプリのLTSRリリース（1912および2203.1）ではサポートされていません。

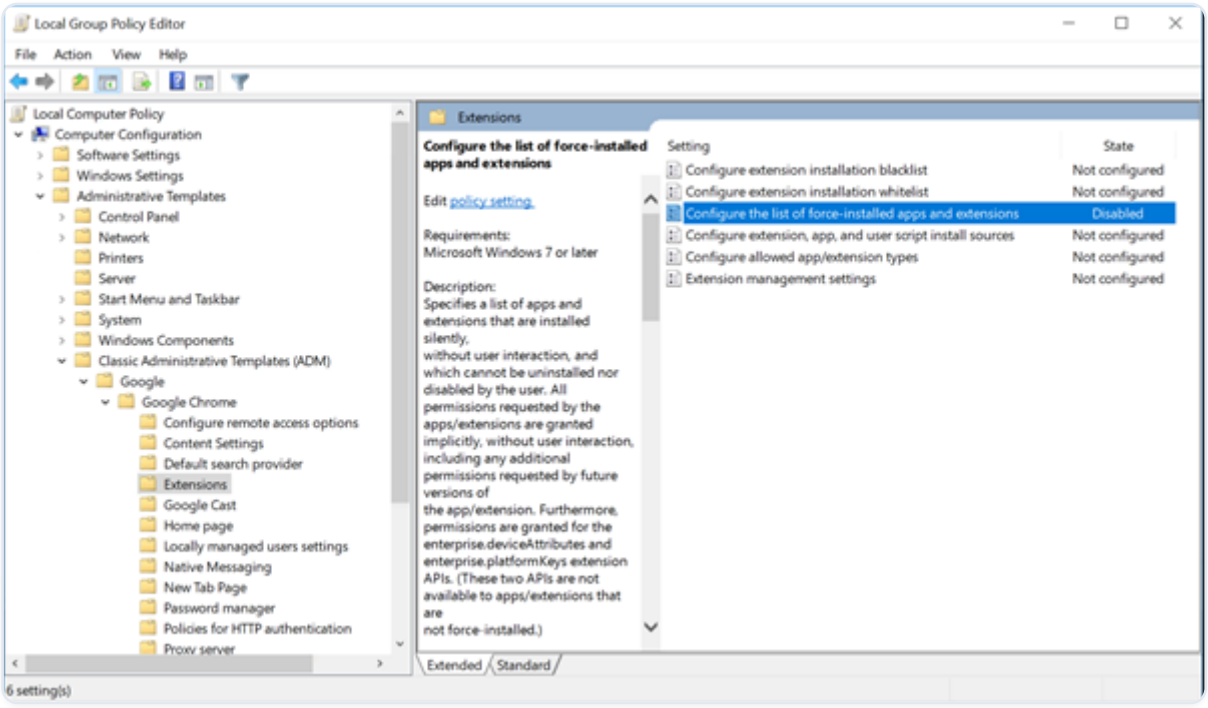


この方法は個々のユーザーに有効です。組織内の大規模なユーザーグループに拡張機能を展開するには、グループポリシーを使用して拡張機能を展開します。

グループポリシーを使用して拡張機能を展開する

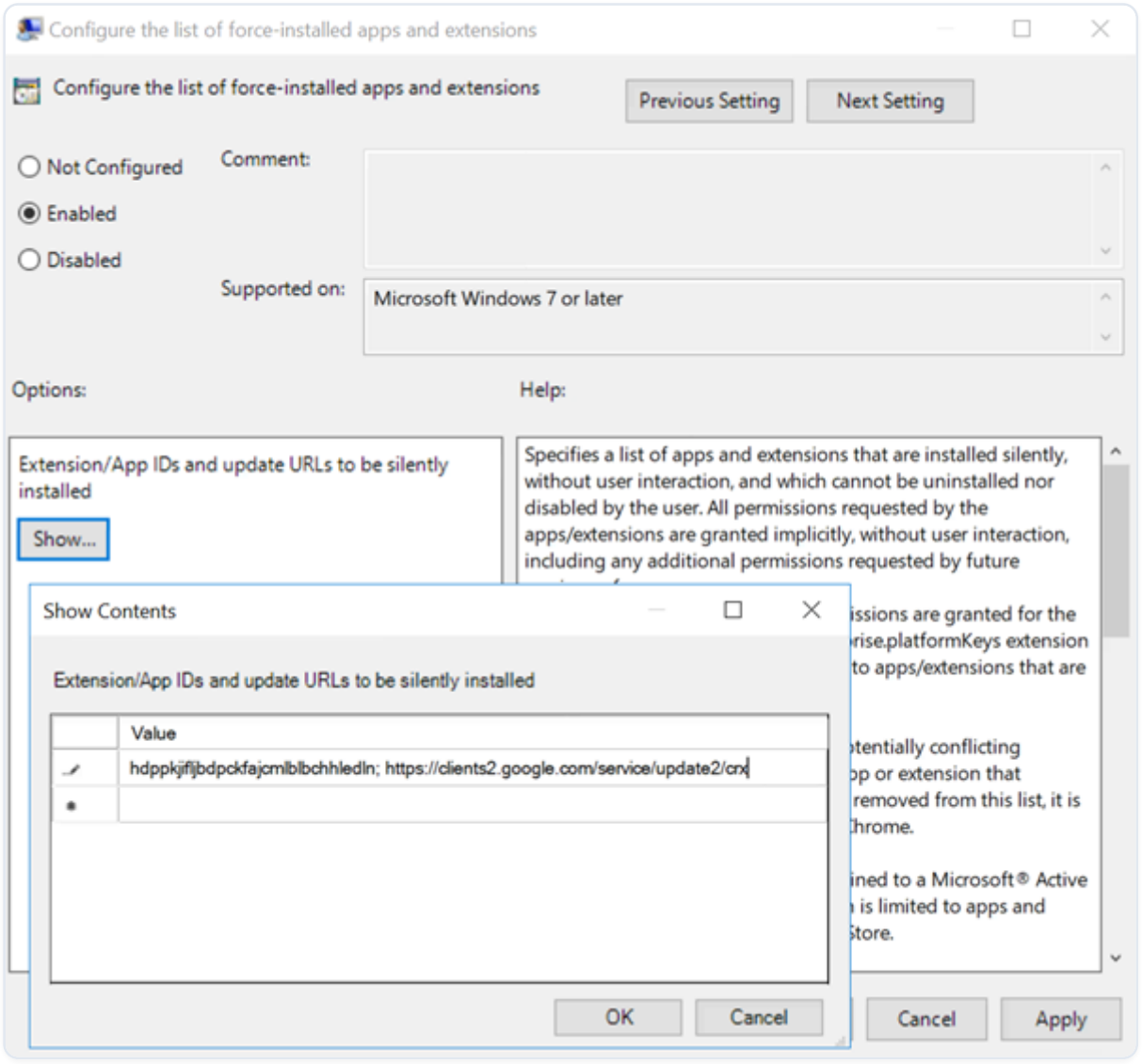
1. Google Chrome ADMXファイルを環境にインポートします。ポリシーテンプレートのダウンロード、およびテンプレートをグループポリシーエディターにインストールして構成する方法については、「管理対象PCでChromeブラウザポリシーを設定する」を参照してください。

2. グループポリシー管理コンソールを開き、**ユーザーの構成 \ 管理用テンプレート\従来の管理用テンプレート (ADM) \ Google\ Google Chrome \ 拡張機能**に移動します。「**強制インストールするアプリと拡張機能のリストを構成する**」設定を有効にします。



3. 「**表示**」をクリックし、拡張機能IDに対応する次の文字列を入力します。ブラウザコンテンツリダイレクト拡張機能のURLを更新します。

```
hdppkjifljbdpckfajcmlblbchhledln; https://clients2.google.com/service/update2/crx
```



4. 設定を適用し、**gpupdate**で更新すると、ユーザーは自動的に拡張機能を受け取ります。ユーザーのセッションでChromeブラウザを起動すると、拡張機能はすでに適用されており、ユーザーはそれを削除できません。

   拡張機能への更新は、設定で指定した更新URLを通じて、ユーザーのマシンに自動的にインストールされます。

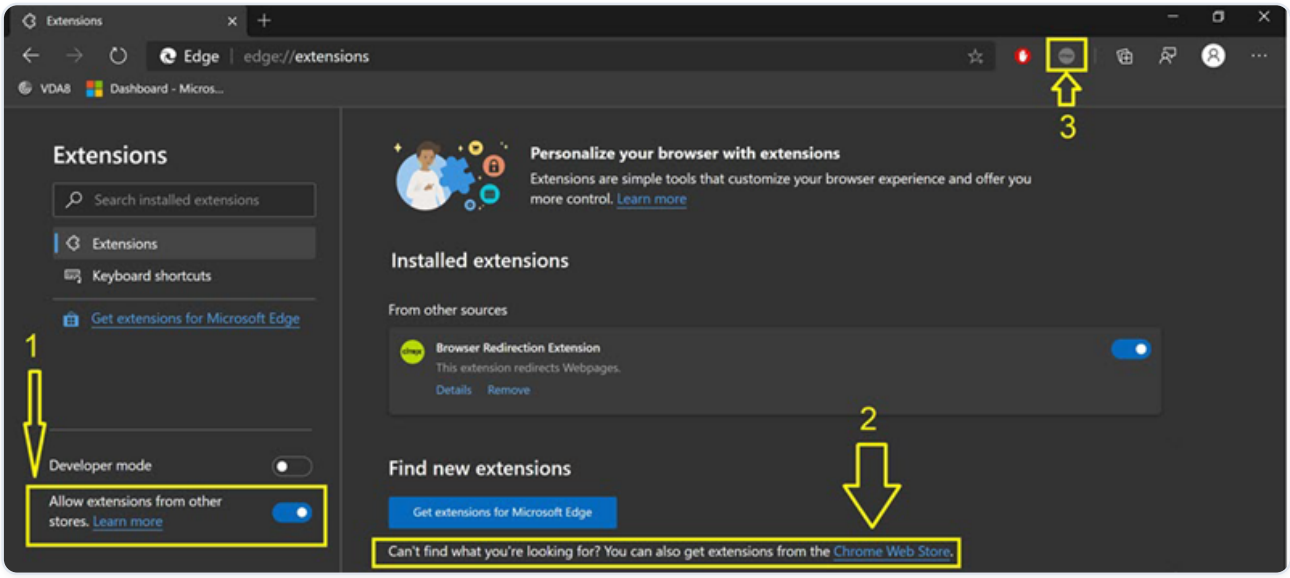
   「**強制インストールされるアプリと拡張機能のリストを構成する**」設定が「**無効**」に設定されている場合、拡張機能はすべてのユーザーのChromeから自動的に削除されます。

ブラウザコンテンツリダイレクトEdge Chromium拡張機能

Edgeにブラウザコンテンツリダイレクト拡張機能をインストールするには、Edgeブラウザのバージョン**83.0.478.37**以降がインストールされていることを確認してください。

1. 「**拡張機能**」オプションをクリックします。「**拡張機能の管理**」を選択します。「**他のストアからの拡張機能を許可する**」をオンにします。

2. 「**Chromeウェブストア**」リンクをクリックすると、拡張機能が右上のバーに表示されます。Microsoft Edge拡張機能の詳細については、「拡張機能」を参照してください。



ブラウザコンテンツリダイレクトとDPI

ユーザーのマシンでDPI（スケーリング）が100%を超えて設定されている状態でブラウザコンテンツリダイレクトを使用すると、リダイレクトされたブラウザコンテンツ画面が正しく表示されません。この問題を回避するには、ブラウザコンテンツリダイレクトを使用する際にDPIを設定しないでください。この問題を回避するもう1つの方法は、ユーザーのマシンにレジストリキーを作成して、Chromeのブラウザコンテンツリダイレクト GPUアクセラレーションを無効にすることです。詳細については、レジストリで管理される機能のリストにある「ブラウザコンテンツリダイレクトとDPI」を参照してください。

統合Windows認証によるシングルサインオン

ブラウザコンテンツリダイレクトは、VDAと同じドメイン内で統合Windows認証（IWA）が構成されたWebサーバーへの認証にNegotiateスキームを使用するようにオーバーレイを強化します。

デフォルトでは、ブラウザコンテンツリダイレクトは、ユーザーがWebサーバーにアクセスするたびにVDA資格情報で認証することを要求する基本認証スキームを使用します。シングルサインオンの場合、「**ブラウザコンテンツリダイレクト統合Windows認証サポート**」ポリシー設定を有効にするか、VDAにレジストリキーを作成することができます。

シングルサインオンを有効にする前に、以下を完了してください。

- Kerberosインフラストラクチャを構成して、ホスト名から構築されたサービスプリンシパル名（SPN）のチケットを発行します。例えば、`HTTP/serverhostname.com`。

- サーバーフェッチの場合：サーバーフェッチモードでブラウザコンテンツリダイレクトを使用する場合、VDAでDNSが適切に構成されていることを確認してください。
- クライアントフェッチの場合：クライアントフェッチモードでブラウザコンテンツリダイレクトを使用する場合、クライアントデバイスでDNSが適切に構成されており、オーバーレイからWebサーバーのIPアドレスへのTCP接続を許可していることを確認してください。

ブラウザコンテンツリダイレクトポリシーを使用してシングルサインオンを構成するには、「ブラウザコンテンツリダイレクトの統合Windows認証サポート」設定を参照してください。

または、VDAにレジストリキーを追加することで、Webサーバーへのシングルサインオンを有効にできます。詳細については、レジストリで管理される機能のリストにある「ブラウザコンテンツリダイレクトの統合Windows認証によるシングルサインオン」を参照してください。

User-agentリクエストヘッダー

User-agentヘッダーは、ブラウザコンテンツリダイレクトから送信されるHTTPリクエストを識別するのに役立ちます。この設定は、プロキシおよびファイアウォールルールを構成する際に役立ちます。例えば、サーバーがブラウザコンテンツリダイレクトから送信されるリクエストをブロックする場合、user-agentヘッダーを含むルールを作成して、特定の要件をバイパスできます。

Windowsデバイスのみがuser-agentリクエストヘッダーをサポートしています。

デフォルトでは、user-agentリクエストヘッダー文字列は無効になっています。クライアントでレンダリングされるコンテンツに対してuser-agentヘッダーを有効にするには、レジストリエディターを使用します。詳細については、レジストリで管理される機能のリストにある「User-agentリクエストヘッoper」を参照してください。

ブラウザコンテンツリダイレクトクライアントの互換性

WMIを使用して、クライアントがブラウザコンテンツリダイレクトと互換性があるかどうかを確認できます。WMIにアクセスするための任意の方法を使用できます。以下はPowerShellを使用した例です。

1. PowerShell を開きます。
2. `Get-WmiObject -Class CTXBCRStatus` を実行します。
3. `BCR_Capable` パラメーターを確認します。
    - `True` の場合、クライアントはブラウザコンテンツリダイレクトと互換性があります。
    - `False` の場合、クライアントはブラウザコンテンツリダイレクトと互換性がありません。

追加情報

- `CtxBrowserSvc`が利用できない場合、コマンド実行時に結果は表示されません。
- `CtxBrowserSvc`が一度も実行されていない場合、結果は無効なクラスエラーを返します。

HDX™ ビデオ会議とウェブカメラのビデオ圧縮

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

> 仮想セッション内で実行されているアプリケーションは、HDXウェブカメラビデオ圧縮またはHDXプラグアンドプレイ汎用USBリダイレクトを使用してウェブカメラを利用できます。モードを切り替えるには、**Citrix Workspace™アプリ > 環境設定 > デバイス**を使用します。可能であれば、常にHDXウェブカメラビデオ圧縮を使用することをお勧めします。HDX汎用USBリダイレクトは、HDXビデオ圧縮とのアプリケーション互換性の問題がある場合、またはウェブカメラの高度なネイティブ機能が必要な場合にのみ推奨されます。パフォーマンスを向上させるため、CitrixはVirtual Delivery Agentに少なくとも2つの仮想CPUを搭載することを推奨します。

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

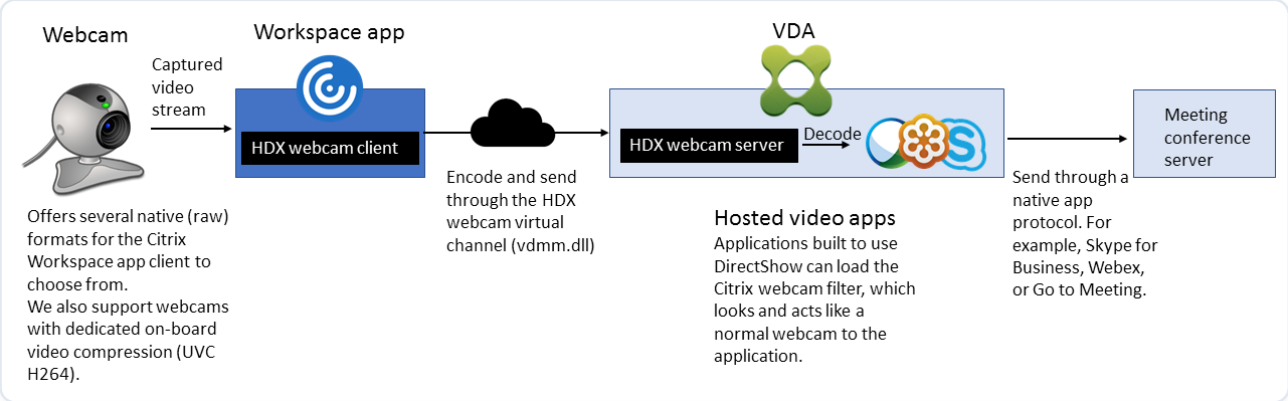
HDXウェブカメラビデオ圧縮

HDXウェブカメラビデオ圧縮は、**最適化された**ウェブカメラモードとも呼ばれます。この種類のウェブカメラビデオ圧縮は、H.264ビデオを仮想セッションで実行されているビデオ会議アプリケーションに直接送信します。VDAリソースを最適化するため、HDXウェブカメラ圧縮はウェブカメラビデオのエンコード、トランスコード、デコードを行いません。この機能はデフォルトで有効になっています。

サーバーからビデオ会議アプリへの直接ビデオストリーミングを無効にするには、VDAでレジストリキーを0に設定します。詳しくは、レジストリで管理される機能の一覧にあるウェブカメラビデオ圧縮を参照してください。

ビデオリソースをストリーミングするためのデフォルト機能を無効にすると、HDXウェブカメラビデオ圧縮は、クライアントオペレーティングシステムの一部であるマルチメディアフレームワークテクノロジーを使用して、キャプチャデバイスからのビデオをインターセプトし、トランスコードして圧縮します。キャプチャデバイスの製造元は、OSカーネルストリーミングアーキテクチャに接続するドライバーを提供します。

クライアントはウェブカメラとの通信を処理します。その後、クライアントはビデオを適切に表示できるサーバーにのみ送信します。サーバーはウェブカメラを直接処理しませんが、その統合によりデスクトップで同じエクスペリエンスが得られます。Workspaceアプリは、帯域幅を節約し、WANシナリオでの回復性を向上させるためにビデオを圧縮します。



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

- マルチメディア会議
- Windows Mediaリダイレクト

ウェブカメラがハードウェアエンコードをサポートしている場合、HDXビデオ圧縮はデフォルトでハードウェアエンコードを使用します。ハードウェアエンコードは、ソフトウェアエンコードよりも多くの帯域幅を消費する可能性があります。ソフトウェア圧縮を強制するには、クライアントでレジストリキーを編集します。詳しくは、レジストリで管理される機能の一覧にあるウェブカメラソフトウェア圧縮を参照してください。

HDXウェブカメラビデオ圧縮の要件

HDXウェブカメラビデオ圧縮は、Citrix Workspaceアプリの次のバージョンをサポートしています。

プラットフォーム	プロセッサ
Windows版 Citrix Workspaceアプリ	Windows向けCitrix Workspaceアプリは、XenAppおよびXenDesktop 7.17以降で32ビットおよび64ビットアプリのWebカメラビデオ圧縮をサポートしています。それ以前のバージョンでは、Windows向けCitrix Workspaceアプリは32ビットアプリのみをサポートしています。
Mac向けCitrix Workspaceアプリ	Mac向けCitrix Workspaceアプリ2006以降は、XenAppおよびXenDesktop 7.17以降で64ビットアプリのWebカメラビデオ圧縮をサポートしています。それ以前のバージョンでは、Mac向けCitrix Workspaceアプリは32ビットアプリのみをサポートしています。
Linux向け Citrix Workspace アプリ	Linux 版 Citrix Workspace アプリは、仮想デスクトップ上の 32 ビットアプリのみをサポートします。
Chrome向けCitrix Workspaceアプリ	一部のARM ChromebookはH.264エンコーディングをサポートしていないため、32ビットアプリのみが最適化されたHDX Webカメラビデオ圧縮を使用できます。

Media Foundation ベースのビデオアプリケーションは、Windows 8.x 以降および Windows Server 2012 R2 以降で HDX ウェブカメラビデオ圧縮をサポートします。詳細については、Knowledge Center の記事 CTX132764 を参照してください。

その他のユーザーデバイス要件:

- サウンドを生成するための適切なハードウェア。
- DirectShow互換のWebカメラ（Webカメラのデフォルト設定を使用してください）。ハードウェアエンコーディング対応のWebカメラは、クライアント側のCPU使用率を低減します。
- HDX Webカメラビデオ圧縮の場合、可能であれば、カメラメーカーから入手したWebカメラドライバーをクライアントにインストールしてください。デバイスドライバーのインストールはサーバー上では不要です。

Webカメラによってフレームレート、明るさ、コントラストのレベルが異なります。Webカメラのコントラストを調整すると、アップストリームトラフィックを大幅に削減できます。Citrixは、初期機能検証のために以下のWebカメラを使用しています:

- Microsoft LifeCam VXモデル（2000、3000、5000、7000）
- クリエイティブ ライブ！カム オプティア プロ
- ロジクール クイックカム メッセンジャー
- ロジクール C600、C920
- HP デラックス ウェブカメラ

優先ビデオフレームレートを調整するには、クライアントでレジストリキーを編集します。詳細については、レジストリで管理される機能のリストにあるWebcam video compression frame rateを参照してください。

高解像度Webカメラストリーミング

サーバー上のビデオ会議アプリケーションは、サポートされているフォーマットタイプに基づいてウェブカメラのフォーマットと解像度を選択します。セッションが開始されると、クライアントはウェブカメラ情報をサーバーに送信します。アプリケーションからウェブカメラを選択します。ウェブカメラとビデオ会議アプリケーションが高解像度レンダリングをサポートしている場合、アプリケーションは高解像度を使用します。ウェブカメラの解像度は最大 1920x1080 までサポートしています。

この機能には、Citrix Workspaceアプリ for Windows バージョン1808以降、またはCitrix Receiver for Windows バージョン4.10以降が必要です。

レジストリキーを使用して、この機能を無効または有効にできます。詳細については、レジストリで管理される機能のリストにあるHigh-definition webcam streamingを参照してください。

メディアタイプのネゴシエーションが失敗した場合、HDX はデフォルトの解像度である 352x288 CIF にフォールバックします。クライアント上のレジストリキーを使用して、デフォルトの解像度を構成できます。カメラが指定された解像度をサポートしていることを確認してください。詳細については、レジストリを通じて管理される機能のリストにある 高解像度ウェブカメラの解像度 を参照してください。

HDX Webカメラビデオ圧縮は、プラグアンドプレイの汎用USBリダイレクトと比較して帯域幅を大幅に削減し、WAN接続でも良好に機能します。帯域幅を調整するには、クライアントでレジストリキーを設定します。詳細については、レジストリで管理される機能のリストにあるHigh-definition webcam bandwidthを参照してください。

ビット/秒単位で値を入力します。帯域幅を指定しない場合、ビデオ会議アプリケーションはデフォルトで350000 bpsを使用します。

HDXプラグアンドプレイ汎用USBリダイレクト

HDXプラグアンドプレイ汎用USBリダイレクト（アイソクロナス）は、**汎用**Webカメラモードとも呼ばれます。HDXプラグアンドプレイ汎用USBリダイレクトの利点は、シンクライアント/エンドポイントにドライバーをインストールする必要がないことです。USBスタックは仮想化されており、ローカルクライアントに接続したものはすべてリモートVMに送信されます。リモートデスクトップは、ネイティブに接続したかのように動作します。Windowsデスクトップは、ハードウェアとのすべてのやり取りを処理し、プラグアンドプレイロジックを実行して正しいドライバーを見つけます。ほとんどのWebカメラは、ドライバーがサーバーに存在し、ICA経由で動作する場合に機能します。汎用Webカメラモードは、USBプロトコルで非圧縮ビデオをネットワーク経由で送信するため、大幅に多くの帯域幅（毎秒数メガビット）を使用します。

HTML5 マルチメディアリダイレクト

HTML5 マルチメディアリダイレクトは、HDX™ MediaStream のマルチメディアリダイレクト機能を拡張し、HTML5 オーディオとビデオを含みます。特にモバイルデバイスへのマルチメディアコンテンツのオンライン配信の増加により、ブラウザ業界はオーディオとビデオを提示するためのより効率的な方法を開発しました。

Flash は標準でしたが、プラグインが必要で、すべてのデバイスで動作せず、モバイルデバイスではバッテリー消費量が多くなります。YouTube、Netflix、および Mozilla、Google、Microsoft の新しいブラウザバージョンなどの企業は、HTML5 に移行しており、これが新しい標準となっています。

HTML5 ベースのマルチメディアには、独自のプラグインに比べて多くの利点があります。

- 企業に依存しない標準 (W3C)
- 簡素化されたデジタル著作権管理 (DRM) ワークフロー
- プラグインによって引き起こされるセキュリティ問題なしにパフォーマンスの向上

HTTP プログレッシブダウンロード

HTTP プログレッシブダウンロードは、HTML5 をサポートする HTTP ベースの疑似ストリーミング方式です。プログレッシブダウンロードでは、ブラウザは HTTP Web サーバーからダウンロード中に単一のファイル（単一の品質でエンコードされたもの）を再生します。ビデオは受信時に

ドライブに保存され、ドライブから再生されます。ビデオを再視聴する場合、ブラウザはキャッシュからビデオを読み込むことができます。

プログレッシブダウンロードの例については、HTML5 ビデオ リダイレクト テスト ページ を参照してください。ウェブページ内のビデオ要素を検査し、HTML5 ビデオタグ内のソース (mp4 コンテナ形式) を見つけるには、ブラウザの開発者ツールを使用します。

HTML5 と Flash の比較

機能	HTML5	フラッシュ
独自のプレーヤーが必要	いいえ	はい
モバイルデバイスで実行	はい	一部
さまざまなプラットフォームでの実行速度	高	低速
iOSでサポート	はい	いいえ
リソース使用量	少ない	多い
より速くロード	はい	いいえ

要件

mp4形式のプログレッシブダウンロードのリダイレクトのみをサポートしています。WebMおよびDASH/HLSのようなアダプティブビットレートストリーミング技術はサポートしていません。

以下をサポートしており、ポリシーを使用してこれらを制御します。詳細については、「マルチメディアポリシー設定」を参照してください。

- サーバー側レンダリング
- サーバーフェッチクライアントレンダリング
- クライアント側フェッチとレンダリング

Citrix Workspace™アプリおよびCitrix Receiver™の最小バージョン:

- Windows向けCitrix Workspaceアプリ1808
- シトリックス レシーバー for Windows 4.5
- シトリックス ワークスペース アプリ 1808 for Linux

- シトリックス レシーバー for Linux 13.5

最小VDAブラウザバージョン	WINDOWS オペレーティングシステム バージョン/ビルド/サービスパック
インターネット エクスプローラー 11.0	ウィンドウズ 10 x86 (1607 RS1) および x64 (1607 RS1); ウィンドウズ 7 x86 および x64; ウィンドウズ サーバー 2016 RTM 14393 (1607); ウィンドウズ サーバー 2012 R2
Firefox 47 証明書を手動でFirefoxの証明書ストアに追加するか、Windowsの信頼された証明書ストアから証明書を検索するようにFirefoxを構成します。詳細については、`https://wiki.mozilla.org/CA:AddRootToFirefox`を参照してください。	ウィンドウズ 10 x86 (1607 RS1) および x64 (1607 RS1); ウィンドウズ 7 x86 および x64; ウィンドウズ サーバー 2016 RTM 14393 (1607); ウィンドウズ サーバー 2012 R2
クローム 51	ウィンドウズ 10 x86 (1607 RS1) および x64 (1607 RS1); ウィンドウズ 7 x86 および x64; ウィンドウズ サーバー 2016 RTM 14393 (1607); ウィンドウズ サーバー 2012 R2

HTML5ビデオリダイレクトソリューションのコンポーネント

- **HdxVideo.js** - Webサイト上のビデオコマンドをインターセプトするJavaScriptフック。HdxVideo.jsは、セキュアWebSocket (SSL/TLS) を使用してWebSocketServiceと通信します。
- **WebSocket SSL証明書**
  - CA (ルート) の場合: **Citrix XenApp/XenDesktop HDX In-Product CA** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp and XenDesktop Engineering; CN = Citrix XenApp and XenDesktop HDX In-Product CA) 場所: **証明書 (ローカルコンピューター) > 信頼されたルート証明機関 > 証明書**。
  - エンドエンティティ (リーフ) の場合: **Citrix XenApp/XenDesktop HDX Service** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp and XenDesktop Engineering; CN = Citrix XenApp and XenDesktop HDX Service) 場所: **証明書 (ローカルコンピューター) > 個人 > 証明書**。
- **WebSocketService.exe** - ローカルシステムで実行され、SSL終端とユーザーセッションマッピングを実行します。TLS Secure WebSocketは127.0.0.1ポート9001でリッスンしています。
- **WebSocketAgent.exe** - ユーザーセッションで実行され、WebSocketServiceコマンドの指示に従ってビデオをレンダリングします。

HTML5ビデオのリダイレクトを有効にするにはどうすればよいですか?

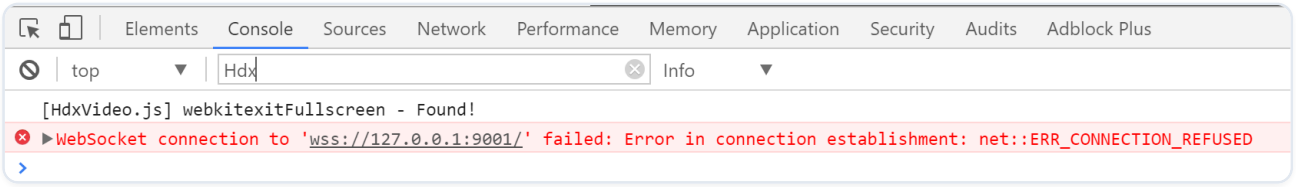
このリリースでは、この機能は制御されたWebページでのみ利用可能です。HTML5マルチメディアコンテンツが利用可能なWebページに、HdxVideo.js JavaScript（Citrix Virtual Apps and Desktopsインストールメディアに含まれています）を追加する必要があります。たとえば、社内トレーニングサイトのビデオなどです。

youtube.comのような、アダプティブビットレート技術（例: HTTP Live Streaming (HLS) および Dynamic Adaptive Streaming over HTTP (DASH)）に基づいたウェブサイトはサポートされていません。

詳細については、「*マルチメディアポリシー設定*」を参照してください。

トラブルシューティングのヒント

WebページがHdxVideo.jsを実行しようとすると、エラーが発生する可能性があります。JavaScriptの読み込みに失敗すると、HTML5リダイレクトメカニズムも失敗します。ブラウザの開発者ツールウィンドウでコンソールを検査し、HdxVideo.jsに関連するエラーがないことを確認してください。例:



Microsoft Teams (Classic) の最適化

Citrixは、Citrix Virtual Apps and Desktops™およびCitrix Workspace™アプリを使用して、デスクトップベースのMicrosoft Teams向けに最適化を提供します。デフォルトでは、必要なすべてのコンポーネントをCitrix WorkspaceアプリとVirtual Delivery Agent (VDA) にバンドルしています。

Microsoft Teams向けのCitrixの最適化には、VDA側のHDX™サービスと、Microsoft Teamsホスト型アプリと連携してコマンドを受信するAPIが含まれています。これらのコンポーネントは、Citrix Workspaceアプリ側のメディアエンジンへの制御仮想チャネル (CTXMTOP) を開きます。エンドポイントはマルチメディアをローカルでデコードして提供し、Citrix Workspaceアプリのウィンドウをホスト型Microsoft Teamsアプリに戻します。

認証とシグナリングは、他のMicrosoft Teamsサービス (チャットやコラボレーションなど) と同様に、Microsoft Teamsホスト型アプリでネイティブに発生します。オーディオ/ビデオのリダイレクトはこれらに影響しません。

`CTXMTOP`はコマンドおよび制御仮想チャネルです。これは、Citrix WorkspaceアプリとVDAの間でメディアが交換されないことを意味します。

クライアントフェッチ/クライアントレンダリングのみが利用可能です。

このビデオデモでは、Citrix仮想環境でMicrosoft Teamsがどのように機能するかを理解できます。



Microsoft Teamsのインストール

CitrixとMicrosoftは、Microsoft Teamsの最新バージョンを使用し、常に最新の状態に保つことを推奨しています。 現在のバージョンのリリース日から90日以上古いリリース日のMicrosoft Teamsデスクトップアプリのバージョンはサポートされていません。 サポートされていないMicrosoft Teamsデスクトップアプリのバージョンでは、ユーザーにブロックページが表示され、アプリの更新が要求されます。

最新の利用可能なバージョンについては、「Teamsアプリの更新履歴（デスクトップおよびMac）」を参照してください。

> **注：**
>
> ゴールデンイメージにMicrosoft Teamsをインストールする前に、VDAをインストールすることをお勧めします。このインストール順序は、**ALLUSER=1**フラグを有効にするために必要です。VDAをインストールする前に仮想マシンにMicrosoft Teamsをインストールした場合は、Microsoft Teamsをアンインストールして再インストールしてください。App Layeringを使用している場合は、詳細についてApp Layeringの場合を参照してください。
>
> Microsoft Teamsのコンピューター全体へのインストールガイドラインに従うことをお勧めします。また、Microsoft Teamsを`AppData`にインストールする.exeインストーラーの使用は避けてください。代わりに、コマンドラインから**ALLUSER=1**フラグを使用して`C:\Program Files (x86)\Microsoft\Teams`にインストールしてください。

```
msiexec /i <path_to_msi> /l*v <install_logfile_name> ALLUSER=1 ALLUSERS=1
```

この例では、**ALLUSERS=1**パラメーターも使用します。このパラメーターを設定すると、Microsoft Teams Machine-Wide Installerが**コントロールパネル**の**プログラムと機能**に表示されます。また、コンピューターのすべてのユーザーのWindows設定の**アプリと機能**にも表示されます。

すべてのユーザーは、管理者資格情報を持っている場合、Microsoft Teamsをアンインストールできます。

ALLUSERS=1と**ALLUSER=1**の違いを理解することが重要です。**ALLUSERS=1**パラメーターは、非VDI環境とVDI環境の両方で使用できます。**ALLUSER=1**パラメーターは、VDI環境でのみ使用して、マシンごとのインストールを指定します。

ALLUSER=1モードでは、新しいバージョンがあるたびにMicrosoft Teamsアプリケーションは自動更新されません。このモードは、Windows ServerまたはWindows 10のランダム/プールされたカタログからのホストされた共有アプリやデスクトップなどの非永続環境に推奨されます。詳細については、MSIを使用してMicrosoft Teamsをインストールする（VDIインストールセクション）を参照してください。

Windows 10専用の永続VDI環境があるとします。Microsoft Teamsアプリケーションを自動更新し、Microsoft Teamsを`Appdata/Local`の下にユーザーごとにインストールすることを希望する場合、この場合は、`.exe`インストーラーまたは**ALLUSER=1**なしのMSIを使用してください。

Remote PC Accessの場合

VDAのインストール後にMicrosoft Teamsバージョン1.4.00.22472以降をインストールすることをお勧めします。そうしないと、Microsoft TeamsがVDAを期待どおりに検出するために、サインアウトして再度サインインする必要があります。バージョン1.4.00.22472以降には、Microsoft Teamsの起動時およびサインイン時にVDA検出のために実行される拡張ロジックが含まれています。これらのバージョンには、アクティブなセッションタイプ識別（HDX、RDP、またはクライアントマシンにローカル接続）も含まれています。ローカル接続の場合、以前のバージョンのMicrosoft Teamsでは、特定の機能やUI要素（ブレイクアウトルーム、会議やチャットのポップアップウィンドウ、会議のリアクションなど）の検出と無効化に失敗する可能性があります。

一部のRemote PC Accessシナリオでは、HDX最適化をサポートする新しいエンドポイントから以前に最適化されていないセッションに再接続する場合、HDX最適化をサポートするためにMicrosoft Teamsを再起動する必要がある場合があります。

App Layeringの場合

Citrix App Layeringを使用してVDAとMicrosoft Teamsのインストールを異なるレイヤーで管理している場合は、**ALLUSER=1**でMicrosoft Teamsをインストールする前に、このレジストリキーをWindows VDAに展開してください。詳細については、レジストリを介して管理される機能のリストにあるCitrix App LayeringによるMicrosoft Teamsの最適化を参照してください。

プロファイル管理の推奨事項

Windows ServerおよびプールされたVDI Windows 10環境には、マシン全体のインストーラーを使用することをお勧めします。

コマンドラインからMSIに**ALLUSER=1**フラグが渡されると（マシン全体のインストーラー）、Microsoft Teamsアプリは`C:\Program Files (x86)`（約300 MB）にインストールされます。アプリは、ログに`AppData\Local\Microsoft\TeamsMeetingAddin`を、ユーザー固有の構成、ユーザーインターフェイスの要素のキャッシュなどに`AppData\Roaming\Microsoft\Teams`（約600～700 MB）を使用します。

> **重要:**

> **ALLUSER=1**フラグを渡さない場合、MSIはTeams.exeインストーラーと`setup.json`を`C:\Program Files (x86)\Teams Installer`に配置します。レジストリキー（TeamsMachineInstaller）は`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`の下に追加されます。

> その後のユーザーログオンにより、代わりに**AppData**に最終インストールがトリガーされます。

マシン全体のインストーラー

以下は、Windows Server 2016 64ビットVMにMicrosoft Teamsマシン全体のインストーラーをインストールすることによって作成されるフォルダー、デスクトップショートカット、およびレジストリの例です。

フォルダー:

- `C:\Program Files (x86)\Microsoft\Teams`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

デスクトップショートカット:

`C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

レジストリ:

- `HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- 名前: `Teams`
- 種類: `REG_SZ`
- 値: `C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

> **注：**
>
> レジストリの場所は、基盤となるオペレーティングシステムとビット数によって異なります。

推奨事項

- Microsoft Teams のレジストリキーを削除して自動起動を無効にすることをお勧めします。これにより、同時に発生する多数のログオン（たとえば、勤務開始時など）によって VM の CPU 使用率が急上昇するのを防ぎます。
- 仮想デスクトップに GPU/vGPU がない場合は、パフォーマンスを向上させるために、Microsoft Teams の で を設定することをお勧めします。この設定 (`"disableGpu":true`) は `desktop-config.json` の `%Appdata%\Microsoft\Teams` に保存されています。ログオンスクリプトを使用してそのファイルを編集し、値を **true** に設定できます。
- Citrix Workspace Environment Management™ (WEM) を使用している場合は、Microsoft Teams のプロセッサ消費を管理するために **CPU スパイク保護**を有効にしてください。

ユーザーごとのインストーラー

`.exe`インストーラーを使用する場合、インストールプロセスは異なります。すべてのファイルはAppDataに配置されます。

フォルダー:

- `C:\Users\<username>\AppData\Local\Microsoft\Teams`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsPresenceAddin`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsMeetingAddin`
- `C:\Users\<username>\AppData\Local\SquirrelTemp`

- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

デスクトップショートカット:

`C:\Users\<username>\AppData\Local\Microsoft\Teams\Update.exe --processStart "Teams.exe"`

レジストリ:

`HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

ベストプラクティス

ベストプラクティスの推奨事項は、ユースケースシナリオに基づいています。 非永続的なセットアップでMicrosoft Teamsを使用する場合、効率的なMicrosoft Teamsランタイムデータ同期のためにプロファイルキャッシュマネージャーが必要です。プロファイルキャッシュマネージャーを使用すると、ユーザーセッション中に適切なユーザー固有の情報がキャッシュされます。たとえば、ユーザー固有の情報には、ユーザーデータ、プロファイル、設定が含まれます。これら2つのフォルダーのデータを同期します。

- `C:\Users\<username>\AppData\Local\Microsoft\IdentityCache`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

非永続的セットアップ向けの Microsoft Teams キャッシュコンテンツ除外リスト

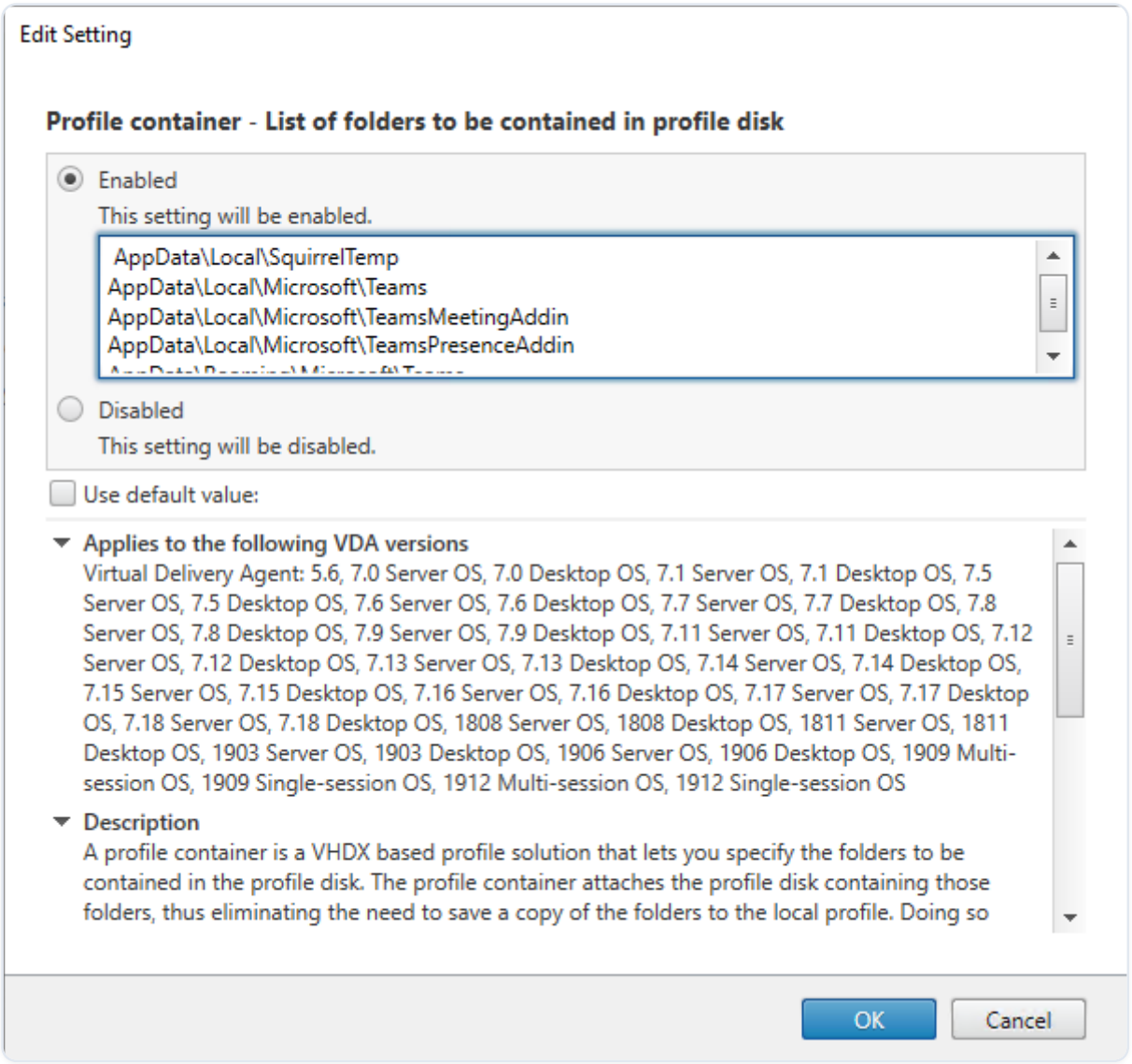
Microsoft ドキュメントに記載されているように、Microsoft Teams のキャッシュフォルダーからファイルとディレクトリを除外します。この操作により、ユーザーのキャッシュサイズを削減し、非永続的セットアップをさらに最適化できます。

ユースケース: シングルセッションシナリオ

このシナリオでは、エンドユーザーは一度に1つの場所でMicrosoft Teamsを使用します。同時に2つのWindowsセッションでMicrosoft Teamsを実行する必要はありません。一般的な仮想デスクトップ展開では、各ユーザーに1つのデスクトップが割り当てられ、Microsoft Teamsは仮想デスクトップに1つのアプリケーションとして展開されます。 Citrix Profileコンテナを有効にし、ユーザーごとのインストーラーにリストされているユーザーごとのディレクトリをコンテナにリダイレクトすることをお勧めします。

1. ゴールデンイメージにMicrosoft Teamsのコンピューター全体インストーラー (**ALLUSER=1**) を展開します。
2. Citrix Profile Managementを有効にし、適切な権限でユーザープロファイルストアを設定します。

3. 次のProfile Managementポリシー設定を有効にします: **ファイルシステム > 同期 > プロファイルコンテナ – プロファイルディスクに含めるフォルダーのリスト。**



この構成にすべてのユーザーごとのディレクトリをリストします。これらの設定は、Citrix Workspace Environment Management (WEM) サービスを使用して構成することもできます。

4. 設定を適切なデリバリーグループに適用します。
5. ログインして展開を検証します。

システム要件

推奨される最小バージョン - Delivery Controller (DDCs) 1906.2

以前のバージョンを使用している場合は、Microsoft Teamsの最適化を有効にするを参照してください:

サポートされているオペレーティングシステム:

- Windows Server 2022、2019、2016、2012R2 StandardおよびDatacenterエディション、ならびにServer Coreオプション

最小バージョン - Virtual Delivery Agents (VDA) 1906.2

サポートされているオペレーティングシステム:

- ウィンドウズ 11。
- Windows 10 64ビット、バージョン1607以降。VMホスト型アプリは、Citrix Workspaceアプリ for Windows 2109.1以降でサポートされています。
- Windows Server 2022、2019、2016、および2012 R2 (StandardおよびDatacenterエディション)。

要件:

- BCR_x64.msi - Microsoft Teamsの最適化コードを含み、GUIから自動的に起動するMSI。VDAインストールにコマンドラインインターフェイスを使用している場合は、除外しないでください。

推奨バージョン – Citrix Workspaceアプリ for Windows最新CRおよび最小バージョン - Citrix Workspaceアプリ 1907 for Windows

- ウィンドウズ 11。
- Windows 10 (32ビットおよび64ビットエディション、Embeddedエディションを含む) (Windows 7のサポートはバージョン2006で終了しました) (Windows 8.1のサポートはバージョン2204.1で終了しました)。
- Windows 10 IoT Enterprise 2016 LTSB (v1607) および 2019 LTSC (v1809) に対応しています。
- サポートされているプロセッサ（CPU）アーキテクチャ: x86およびx64（ARMはサポートされていません）。
- エンドポイント要件: ピアツーピアビデオ会議中に720p HD解像度をサポートできる約2.2〜2.4 GHzデュアルコアCPU。
- デュアルコアまたはクアッドコアCPUで、ベース速度が低く（約1.5 GHz）、Intel Turbo BoostまたはAMD Turbo Coreを搭載し、少なくとも2.4 GHzまでブーストできるもの。
- 動作確認済みHPシンクライアント: t630/t640、t730/t740、mt44/mt45。
- 動作確認済みDellシンクライアント: 5070、5470 Mobile TCおよびAIO。
- 動作確認済み10ZiGシンクライアント: 4510および5810q。

- 動作確認済みエンドポイントの完全なリストについては、「シンクライアント」を参照してください。
- Citrix Workspaceアプリには、少なくとも600 MBの空きディスク容量と1 GBのRAMが必要です。
- Microsoft .NET Frameworkの最小要件はバージョン4.8です。Citrix Workspaceアプリは、システムに.NET Frameworkが存在しない場合、自動的にダウンロードしてインストールします。

管理者は、Teams最適化ポリシーを変更することで、最適化モードでMicrosoft Teamsを有効/無効にできます。Citrix Workspaceアプリで最適化モードを開始するユーザーは、Microsoft Teamsを無効にできません。

最小バージョン - Linux用Citrix Workspaceアプリ2006

詳しくは、Citrix WorkspaceアプリfoLinuxのドキュメントにあるMicrosoft Teamsの最適化を参照してください。

ソフトウェア:

- `GStreamer` 1.0以降またはCairo 2
- libc++-9.0以降
- `libgdk` 3.22 以降
- OpenSSL 1.1.1d
- x64 Linuxディストリビューション

ハードウェア:

- ピアツーピアのビデオ会議通話中に720p HD解像度をサポートできる最小1.8 GHzデュアルコアCPU
- ベース速度1.8 GHz、Intel Turbo Boostの高速化が少なくとも2.9 GHzのデュアルコアまたはクアッドコアCPU

検証済みエンドポイントの完全なリストについては、Thin Clientsを参照してください。

詳細については、Citrix Workspaceアプリをインストールするための前提条件を参照してください。

`/opt/Citrix/ICAClient/config/module.ini`ファイルで**VDWEBRTC**フィールドの値をOffに更新すると、Microsoft Teamsの最適化を無効にできます。デフォルトはVDWEBRTC=Onです。更新が完了したら、セッションを再起動してください。(ルート権限が必要です)。

最小バージョン - Mac用Citrix Workspaceアプリ2012

サポートされているオペレーティングシステム:

- macOS カタリナ (10.15)。
- macOS Big Sur 11.0.1以降。
- macOS モントレー。

サポートされている機能:

- オーディオ
- ビデオ
- 画面共有の最適化 (送受信)

> **注：**
>
> 画面共有が機能するには、Citrix Viewerアプリがmacosの「セキュリティとプライバシー」設定へのアクセスを必要とします。ユーザーは、この設定を**Appleメニュー > システム環境設定 > セキュリティとプライバシー > プライバシー > 画面収録**で構成し、**Citrix Viewer**を選択します。

> Microsoft Teamsの最適化は、Citrix Workspaceアプリ2012以降およびmacOS 10.15でデフォルトで機能します。

Microsoft Teamsの最適化を無効にするには、ターミナルでこのコマンドを実行し、Citrix Workspaceアプリを再起動します。

```
defaults write com.citrix.receiver.nomas mtopEnabled -bool NO
```

最小バージョン - 最新バージョンのChrome OSで実行されているChrome OS用Citrix Workspaceアプリの最新バージョン

ハードウェア:

- Intel i3、クアッドコア2.4 GHzと同等以上の性能を持つプロセッサ。

サポートされる機能:

- オーディオ
- ビデオ

- 画面共有の最適化（送受信） - デフォルトでは無効になっています。有効にする方法については、これらの設定を参照してください。

シングルサーバーのスケーラビリティ

このセクションでは、単一の物理ホストでサポートできるユーザー数または仮想マシン（VM）数を推定するための推奨事項とガイダンスを提供します。これは一般にCitrix Virtual Apps and Desktopsのシングルサーバーのスケーラビリティ（SSS）と呼ばれます。Citrix Virtual Apps（CVA）またはセッション仮想化のコンテキストでは、ユーザー密度とも呼ばれます。その目的は、主要なハイパーバイザーを実行している単一のハードウェアで、いくつのユーザーまたはVMを実行できるかを明らかにすることです。

> **注：**
>
> このセクションには、SSS を推定するためのガイダンスが含まれています。このガイダンスは一般的なものであり、お客様固有の状況や環境に必ずしも特化したものではないことに注意してください。Citrix Virtual Apps and Desktops の SSS を真に理解する唯一の方法は、Login VSI などのスケーラビリティまたはロードテストツールを使用することです。Citrix は、SSS を迅速に推定するためだけに、このガイダンスとこれらの簡単なルールを使用することを推奨します。ただし、Citrix は、特にハードウェアを購入したり、財務上の決定を下したりする前に、Login VSI または選択したロードテストツールを使用して結果を検証することを推奨します。

ハードウェア (テスト対象システム)

- デル パワーエッジ R740
- Intel Xeon (Gold) 6126 @ 2.60 GHz (最大ターボ 3.70 GHz)、ソケットあたり 12 コア、ハイパースレッディング有効のデュアルソケット
- 382 GB の RAM
- ローカル SSD RAID 0 ストレージ (11 ディスク) 6 TB

ソフトウェア

Citrix Virtual Apps and Desktops 2106 を実行する Windows 2019 (TSVDA) を搭載した単一の仮想マシン (40 論理プロセッサ) VMware ESXi 6.7

用語

- ナレッジワーカーのワークロード: Acrobat Reader、Freemind/Java、フォトビューアー、Edge、および Excel、Outlook、PowerPoint、Word などの MS Office アプリが含まれます。
- ベースライン: ナレッジワーカーのワークロード (Microsoft Teams なし) で実行されるサーバーのスケーラビリティテスト。
- Microsoft Teams ワークロード: ナレッジワーカーの一般的なワークロード + Microsoft Teams。

Microsoft Teams のストレステスト方法

- Microsoft Teams は HDX で最適化されています。そのため、すべてのマルチメディア処理はエンドポイントまたはクライアントにオフロードされ、測定には含まれません。
- ワークロードが開始される前に、すべての Microsoft Teams プロセスが停止または強制終了されます。
- Microsoft Teams を開く（コールドスタート）。
- Microsoft Teams がロードされ、Microsoft Teams のプライマリウィンドウがフォーカスを取得するまでにかかる時間を測定します。
- キーボードショートカットを使用してチャットウィンドウに切り替えます。
- キーボードショートカットを使用してカレンダーウィンドウに切り替えます。
- キーボードショートカットを使用して、特定のユーザーにチャットメッセージを送信します。
- キーボードショートカットを使用して Microsoft Teams ウィンドウに切り替えます。

結果

- ベースライン（137ユーザー）と比較して、Microsoft Teams ワークロード（81ユーザー）ではスケーラビリティに40%の影響があります。
- サーバー容量を約40%（CPU）増やすと、ベースラインワークロードの場合と同様のユーザー数に戻ります。
- ベースラインと比較して、Microsoft Teams ワークロードでは20%の追加メモリが必要です。
- ユーザーあたりのストレージサイズを512〜1024 MB増やします。
- IOPS 書き込みが約50%増加し、IOPS 読み取りが約100%増加します。Microsoft Teams は、ストレージが遅い環境では大きな影響を与える可能性があります。

機能マトリックスとバージョンサポート

機能	MICROSOFT TEAMS (最小バージョン)	VDA (最小バージョン)	WINDOWS 向け CITRIX WORKSPACE アプリ CR	CITRIX WORKSPACE アプリ FOR WINDOWS 1912 LTSR (および CU1-CU4)	WINDOWS 向け CITRIX WORKSPACE アプリ 1912 CU5	CITRIX WORKSPACE アプリ FOR WINDOWS 1912 CU6 (以降)	MAC 向け CITRIX WORKSPACE アプリ	LINUX向け CITRIX WORKSPACE アプリ	CHROMEOS 向け CITRIX WORKSPACE アプリ
画面共有	現在のバージョンから90日遡ったもの	1906	1907	はい	はい	はい	2012	2006	2105.5 (1)
i. 画面インジケーターの赤い枠線	現在のバージョンから90日遡ったもの	1906	2002	はい	はい	はい	2012	2006	いいえ

ii. キャプチャをDesktop Viewerに制限	現在のバージョンから90日遡ったもの	1906	2009.5	いいえ	はい	はい	2012	2006	いいえ
iii. マルチモニター	現在のバージョンから90日遡ったもの	1906	2106 (2)	いいえ	いいえ	はい (2)	2106	2106	いいえ
DTMF	現在のバージョンから90日遡ったもの	該当なし	2102	いいえ	はい (5)	はい (5)	2101	2101	2111.1
プロキシサーバーのサポート	現在のバージョンから90日遡っ	該当なし	2012 (3)	いいえ	はい (3) (5)	はい (3) (5)	2104 (4)	2101 (4)	いいえ

	たもの								
アプリ共有	現在のバージョンから90日遡ったもの	2109	2109.1	いいえ	いいえ	いいえ	2203.1	いいえ	いいえ
マルチウィンドウ	1.5.0.0.11865	2112	2112.1	いいえ	いいえ	いいえ	2203.1	2203	いいえ
制御を付与	現在のバージョンから90日遡ったもの	該当なし	2112.1	いいえ	いいえ	いいえ	2203.1	いいえ	いいえ
制御を要求	現在のバージョンから90日遡ったもの	該当なし	2112.1	いいえ	いいえ	いいえ	2203.1	いいえ	いいえ

ライブキャプション	現在のバージョンから90日遡ったもの	該当なし	2109.1	いいえ	いいえ	いいえ	2109	2109	いいえ
動的e911	現在のバージョンから90日遡ったもの	該当なし	2112.1	いいえ	いいえ	いいえ	2112	2112	2112

1. デフォルトで無効になっており、管理者が有効にする必要があります。
2. CDビューアは全画面モードのみ。SHIFT+F2はサポートされていません。
3. Negotiate/Kerberos、NTLM、Basic、およびDigest。`Pac`ファイルもサポートされています。
4. 匿名のみ。
5. Windows 10、Windows IoT Client OSでのみ利用可能です。
6. 現在、Microsoft Teamsでは利用できない機能です。ETAについては、Microsoftのページを参照してください。

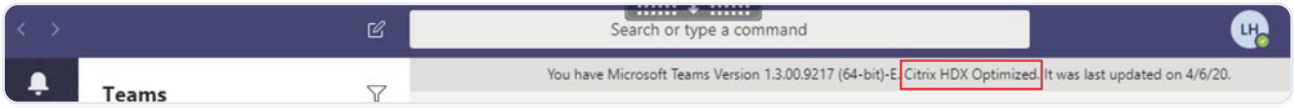
Microsoft Teamsの最適化を有効にする

Microsoft Teamsの最適化を有効にするには、Microsoft Teams redirectionポリシーで説明されている管理コンソールポリシーを使用します。このポリシーはデフォルトで**ON**になっています。このポリシーが有効になっていることに加えて、HDXはCitrix Workspaceアプリのバージョンが最低要件を満たしていることを確認します。ポリシーを有効にし、Citrix Workspaceアプリのバージョンがサポートされている場合、VDA上で

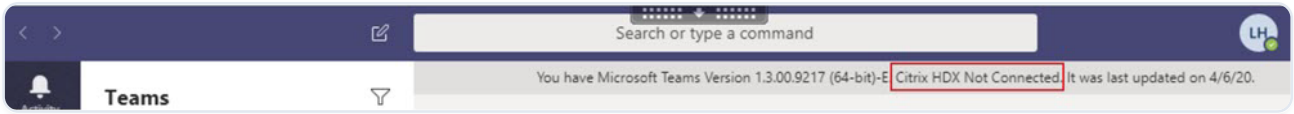
HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream\MSTeamsRedirSupportが自動的に**1**に設定されます。Microsoft Teamsはこのキーを読み取り、VDIモードでロードします。

> **注：**
>
> バージョン1906.2以降のVDA、またはManageコンソール（Studio）でポリシーが利用できない古いコントローラーバージョン（バージョン7.15など）を使用している場合でも、VDAを最適化できます。Microsoft TeamsのHDX最適化は、VDAでデフォルトで有効になっています。

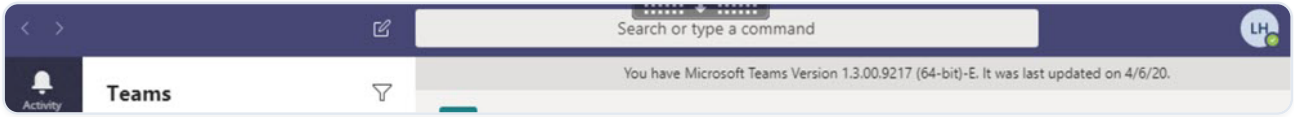
> **About > Version**をクリックすると、**Citrix HDX Optimized**の凡例が表示されます。



Citrix HDX Not Connectedと表示される場合、Citrix APIはMicrosoft Teamsにロードされています。APIのロードはリダイレクトへの最初のステップです。しかし、スタックの後続の部分でエラーが発生しています。このエラーは、VDAサービスまたはCitrix Workspaceアプリにある可能性が最も高いです。



凡例が表示されない場合、Microsoft TeamsはCitrix APIのロードに失敗しています。通知領域のアイコンを右クリックしてMicrosoft Teamsを終了し、再起動してください。管理コンソールポリシーが**禁止**に設定されておらず、Citrix Workspaceアプリのバージョンがサポートされていることを確認してください。



> **重要: セッションの再接続**
>
> - 接続性が変更された場合、HDX最適化セッションを取得するためにMicrosoft Teamsを再起動する必要がある場合があります。たとえば、サポートされていないエンドポイント（iOS、Android、またはWindows/Linux/Macの古いバージョンのWorkspaceアプリ）からサポートされているエンドポイント（Windows/Linux/Mac/ChromeOS/HTML5のWorkspaceアプリ）にローミングする場合、またはその逆の場合です。

- VDAにMicrosoft Teamsの.exeインストーラーを使用してアプリをインストールした場合も、Microsoft Teamsの再起動が必要です。.exeインストーラーは、永続的なVDI展開に推奨されます。このような場合、HDXセッションが切断状態にある間にMicrosoft Teamsが自動更新されることがあります。そのため、HDXセッションに再接続するユーザーは、Microsoft Teamsが最適化されて実行されていないことに気づくでしょう。
- ローカルセッションからHDXセッションにローミングする場合、HDXで最適化するためにMicrosoft Teamsを再起動する必要があります。この操作は、Remote PC Accessシナリオで必要です。

ネットワーク要件

Microsoft Teamsは、会議や多人数通話のためにMicrosoft 365のメディアプロセッササーバーに依存しています。また、Microsoft Teamsは、以下のシナリオでMicrosoft 365トランスポートリレーに依存しています。

- ポイントツーポイント通話の2つのピアが直接接続されていない
- 参加者がメディアプロセッサに直接接続されていない。

そのため、ピアとMicrosoft 365クラウド間のネットワークの状態が通話のパフォーマンスを決定します。ネットワーク計画に関する詳細なガイドラインについては、Microsoft 365 network connectivity principlesを参照してください。

クラウド音声およびビデオの全体的な展開に影響を与える可能性のあるリスクと要件を特定するために、環境を評価することをお勧めします。 ネットワークがMicrosoft Teamsに対応しているかテストするには、Skype for Business Network Assessment Toolを使用してください。サポート情報については、Supportを参照してください。

Real Time Protocol (RTP) トラフィックに関する主要なネットワーク推奨事項の概要

- 支社からMicrosoft 365ネットワークにできるだけ直接接続します。
- 支社で十分な帯域幅を計画し、提供します。
- 各支社のネットワーク接続と品質を確認します。
- 支店で以下のいずれかを使用する必要がある場合は、RTP/UDPトラフィック (Citrix WorkspaceアプリのHdxRtcEngine.exeによって処理されます) が妨げられないことを確認してください。
    - プロキシサーバーをバイパスする
    - ネットワークSSLインターセプト

- ディープパケットインスペクションデバイス
- VPNヘアピン（可能であればスプリットトンネリングを使用）

重要: VPNスプリットトンネル構成

HdxRtcEngine.exeのトラフィックはVPNトンネルから迂回させ、ユーザーのローカルインターネット接続を使用してサービスに直接接続できるようにする必要があります。これを実現する方法は、使用するVPN製品とマシンプラットフォームによって異なりますが、ほとんどのVPNソリューションでは、このロジックを適用するための簡単なポリシー構成が可能です。VPNプラットフォーム固有のスプリットトンネルガイダンスの詳細については、this Microsoft articleを参照してください。

WorkspaceアプリのWebRTCメディアエンジン（HdxRtcEngine.exe）は、クライアントにオフロードされるマルチメディアストリームにSecure Real-time Transport Protocol (SRTP) を使用します。SRTPはRTPに機密性と認証を提供します。この機能では、AES暗号化方式を使用してメディアおよび制御メッセージを暗号化するために、対称鍵（DTLSとネゴシエートされる）が使用されます。

良好なユーザーエクスペリエンスのために、以下のメトリックが推奨されます。

メトリック	エンドポイントからMICROSOFT 365まで
遅延 (片道)	< 50 ミリ秒
遅延 (RTT)	< 100 ミリ秒
パケット損失	15秒間隔で1%未満
パケット到着間隔ジッター	15秒間隔で30ミリ秒未満

詳細については、Microsoft Teams 用に組織のネットワークを準備するを参照してください。

帯域幅要件については、Microsoft Teams の最適化では、オーディオ (OPUS/G.722/PCM G711) およびビデオ (H264) 用にさまざまなコーデックを使用できます。

ピアは、セッション記述プロトコル (SDP) Offer/Answer を使用して、通話確立プロセス中にこれらのコーデックをネゴシエートします。 Citrix のユーザーあたりの最小推奨事項は次のとおりです。

タイプ	帯域幅	コーデック
音声 (双方向)	約 90 kbps	G.722
音声 (双方向)	約 60 kbps	オーパス*
ビデオ (双方向)	約 700 kbps	H264 360p で 30 fps 16:9
画面共有	約 300 kbps	H264 1080p、15フレーム/秒

* Opusは、6 kbpsから510 kbpsまでの定ビットレートおよび可変ビットレートエンコーディングをサポートしています。

OpusとH264は、ピアツーピアおよび電話会議に推奨されるコーデックです。

重要:

パフォーマンスについてですが、クライアントマシンでのCPU使用量に関して、エンコードはデコードよりもコストがかかります。LinuxおよびWindows版Citrix Workspaceアプリで、最大エンコード解像度をハードコードできます。「エンコーダーパフォーマンス見積もり」および「Microsoft Teamsの最適化」を参照してください。

シトリックス ゲートウェイ

オンプレミスのCitrix GatewayまたはCitrix Gatewayサービスが HDXプロキシとして存在しても、Microsoft Teamsの最適化には影響しません。これは、WorkspaceアプリとVDAの間にはコマンドアンドコントロール仮想チャネルのみが確立されているためです。

すべてのオーディオまたはビデオストリームは、ローカル処理のためにクライアントにオフロードされます。その結果、サーバー側でのレンダリングは行われません。

環境内の構成に応じて、コマンドアンドコントロール仮想チャネルは、以下のいずれかを使用してCitrix Gatewayを介して流れます。

- TCP 用の TLS
- EDT 用の DTLS

VPN に Citrix Gateway も使用している場合は、クライアントマシンが O365 Microsoft Teams サーバーに直接アクセスできるようにしてください。これは、スプリットトンネリングまたはその他の方法で実現できます。

プロキシサーバー

プロキシの場所に応じて、以下を考慮してください。

- VDAでのプロキシ構成:

  VDA で明示的なプロキシサーバーを構成し、localhost への接続をプロキシ経由でルーティングすると、リダイレクトは失敗します。プロキシを正しく構成するには、**Internet Options > Connections > LAN Settings > Proxy Servers** で **Bypass proxy servers for local address** 設定を選択し、`127.0.0.1:9002` がバイパスされるようにする必要があります。

  PACファイルを使用する場合、PACファイルからのVDAプロキシ構成スクリプトは、`wss://127.0.0.1:9002` に対して **DIRECT** を返す必要があります。そうでない場合、最適化は失敗します。スクリプトが **DIRECT** を返すことを確認するには、`shExpMatch(url, "wss://127.0.0.1:9002/*")` を使用します。

- Citrix Workspaceアプリでのプロキシ構成:

  支社がプロキシ経由でインターネットにアクセスするように構成されている場合、以下のバージョンがプロキシサーバーをサポートします。

  - Citrix Workspaceアプリ for Windowsバージョン2012 (Negotiate/Kerberos、NTLM、Basic、Digest。`Pac` ファイルもサポートされています)
  - Citrix Workspaceアプリ for Windowsバージョン1912 CU5 (Negotiate/Kerberos、NTLM、Basic、Digest。`Pac` ファイルもサポートされています)
  - Citrix Workspaceアプリ for Linuxバージョン2101 (匿名認証)
  - Citrix Workspaceアプリ for Macバージョン2104 (匿名認証)

以前のバージョンのCitrix Workspaceアプリを搭載したクライアントデバイスは、プロキシ構成を読み取ることができません。これらのデバイスは、Microsoft 365 TURNサーバーに直接トラフィックを送信します。

> **重要:**

> - クライアントデバイスがDNS解決を行うためにDNSサーバーに接続できることを確認してください。クライアントデバイスは、以下のMicrosoft Teamsリレーサーバーの FQDN を解決できる必要があります。
>
>   - `worldaz.relay.teams.microsoft.com`

- `inaz.relay.teams.microsoft.com`
- `uaeaz.relay.teams.microsoft.com`
- `euaz.relay.teams.microsoft.com`
- `usaz.relay.teams.microsoft.com`
- `turn.dod.teams.microsoft.us`
- `turn.gov.teams.microsoft.us`

DNS要求が失敗した場合、外部ユーザーとのP2P通話および会議通話のメディア確立は失敗します。

- 会議サーバーの場所は、最初の参加者の仮想デスクトップの場所に基づいて選択されます（クライアントではありません）。

通話の確立とメディアフローパス

可能な場合、Citrix WorkspaceアプリのHDX WebRTCメディアエンジン（HdxRtcEngine.exe）は、ピアツーピア通話でユーザーデータグラムプロトコル（UDP）を介した直接ネットワークのセキュアリアルタイムトランスポートプロトコル（SRTP）接続を確立しようとします。UDPハイポートがブロックされている場合、メディアエンジンはTCP/TLS 443にフォールバックします。

HDXメディアエンジンは、候補の検出と接続の確立のために、ICE、NAT用セッショントラバーサルユーティリティ（STUN）、およびNAT周辺リレーを使用したトラバーサル（TURN）をサポートしています。このサポートは、エンドポイントがDNS解決を実行できる必要があることを意味します。

2つのピア間、またはピアと会議サーバー間に直接パスがなく、多人数通話または会議に参加しているシナリオを考えてみましょう。HdxRtcEngine.exeは、Microsoft 365のMicrosoft Teamsトランスポートリレーサーバーを使用して、他のピアまたは会議がホストされているメディアプロセッサに到達します。クライアントマシンは、3つのMicrosoft 365サブネットIPアドレス範囲と4つのUDPポート（UDPがブロックされている場合はフォールバックとしてTCP/TLS 443）にアクセスできる必要があります。詳細については、通話設定 および Office 365 URLとIPアドレス範囲 ID 11 のアーキテクチャ図を参照してください。

ID	カテゴリ	アドレス	宛先ポート
11	最適化が必要	13.107.64.0/18, 52.112.0.0/14, 52.120.0.0/14	**UDP:** 3478, 3479, 3480, 3481, **TCP:** 443 (フォールバック)

これらの範囲には、トランスポートリレーとメディアプロセッサの両方が含まれており、Azure Load Balancerによってフロントエンドされています。 Microsoft Teamsトランスポートリレーは STUNおよびTURN機能を提供しますが、ICEエンドポイントではありません。また、Microsoft Teamsトランスポートリレーはメディア、TLSを終端したり、トランスコーディングを行ったりしません。他のピアまたはメディアプロセッサにトラフィックを転送する際に、TCP（HdxRtcEngine.exeがTCPを使用する場合）をUDPにブリッジできます。

WorkspaceアプリのWebRTCメディアエンジンは、Microsoft 365クラウド内で最も近いMicrosoft Teamsトランスポートリレーに接続します。メディアエンジンは、エニーキャストIPとポート3478～3481 UDP（ワークロードごとに異なるUDPポートですが、多重化が発生する可能性があります）、またはフォールバックとして443 TCP/TLSを使用します。通話品質は基盤となるネットワークプロトコルに依存します。UDPは常にTCPよりも推奨されるため、ブランチオフィスでUDPトラフィックに対応できるようにネットワークを設計することをお勧めします。

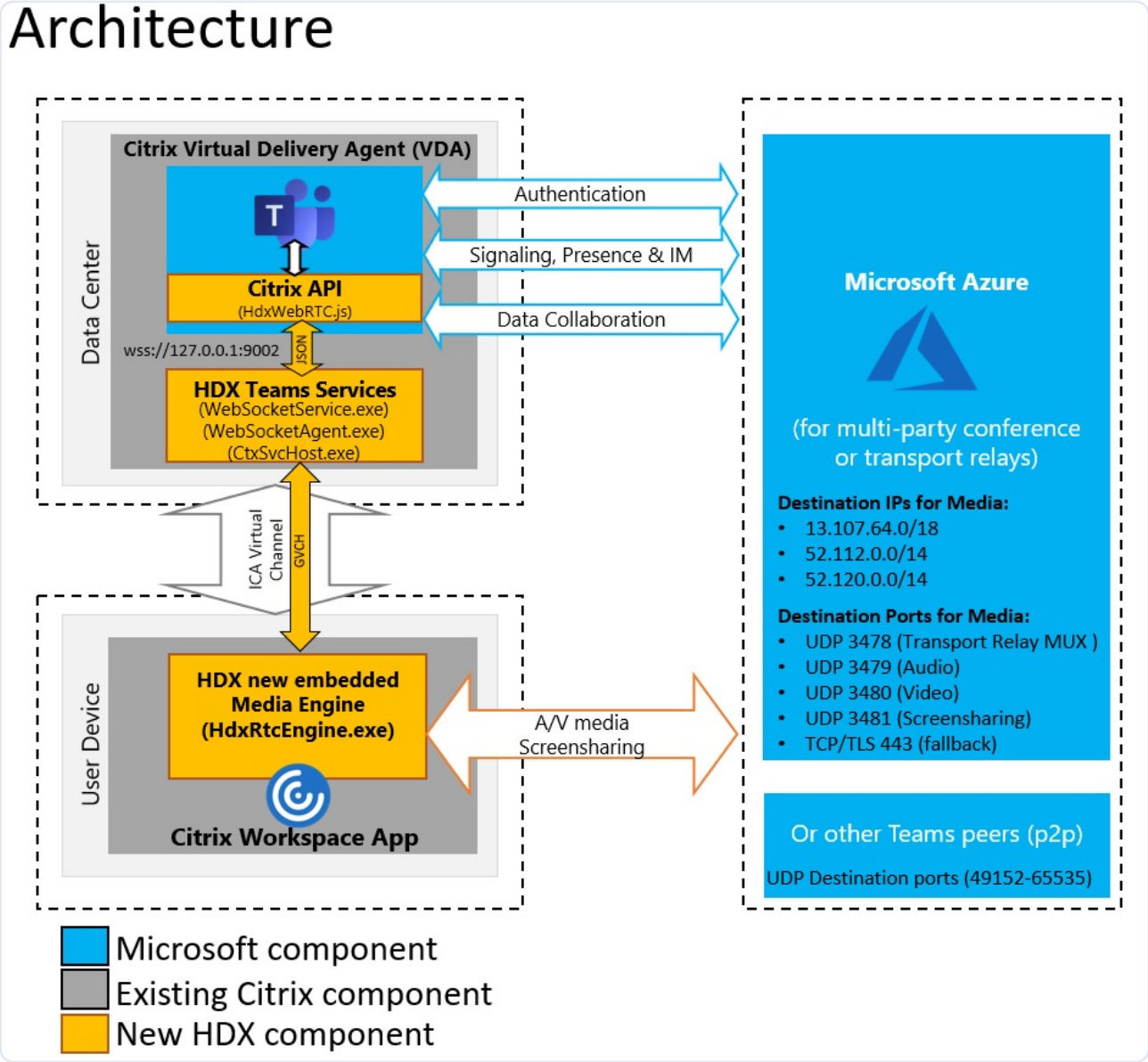
Microsoft Teamsが最適化モードでロードされ、HdxRtcEngine.exeがエンドポイントで実行されている場合、ICEの障害により通話設定の失敗や、音声/ビデオが片方向のみになる可能性があります。通話が完了できない場合やメディアストリームが全二重でない場合は、まずエンドポイントの**Wiresharkトレース**を確認してください。ICE候補収集プロセスに関する詳細については、サポートセクションの「ログの収集」を参照してください。

> **注：**
>
> エンドポイントにインターネットアクセスがない場合でも、両方のユーザーが同じLAN上にいれば、ピアツーピア通話を行うことができる場合があります。会議は失敗します。この場合、通話設定が開始されるまでに30秒のタイムアウトが発生します。

通話設定

このアーキテクチャ図を、通話フローシーケンスの視覚的な参照として使用してください。対応する手順は図に示されています。

アーキテクチャ



1. Microsoft Teams を起動します。
2. Microsoft Teams は O365 に対して認証を行います。テナントポリシーは Microsoft Teams クライアントにプッシュされ、関連する TURN およびシグナリングチャネル情報がアプリに中継されます。
3. Microsoft Teams は VDA で実行されていることを検出し、Citrix JavaScript API に API 呼び出しを行います。
4. Microsoft Teams 内の Citrix JavaScript は、VDA で実行されている WebSocketService.exe に対してセキュアな WebSocket 接続を開き、これによりユーザーセッション内で WebSocketAgent.exe が生成されます。
5. WebSocketAgent.exe は、Citrix HDX Microsoft Teams Redirection Service (CtxSvcHost.exe) を呼び出すことによって、汎用仮想チャネルをインスタンス化します。

6. Citrix Workspace アプリの wfica32.exe (HDX エンジン) は、HdxRtcEngine.exe と呼ばれる新しいプロセスを生成します。これは、Microsoft Teams の最適化に使用される新しい WebRTC エンジンです。
7. Citrix メディアエンジンと Teams.exe は双方向仮想チャネルパスを持ち、マルチメディア要求の処理を開始できます。

   -----ユーザー通話------

8. **ピア A** が **通話** ボタンをクリックします。Teams.exe は Microsoft 365 の Microsoft Teams サービスと通信し、**ピア B** とのエンドツーエンドのシグナリングパスを確立します。Microsoft Teams は HdxRtcEngine に、サポートされている一連の通話パラメーター (コーデック、解像度など。これはセッション記述プロトコル (SDP) オファーとして知られています) を要求します。これらの通話パラメーターは、シグナリングパスを使用して Microsoft 365 の Microsoft Teams サービスに中継され、そこからもう一方のピアに中継されます。
9. SDPオファー/アンサー（シングルパスネゴシエーション）はシグナリングチャネルを介して行われ、ICE接続チェック（STUNバインド要求を使用したNATおよびファイアウォールトラバーサル）が完了します。その後、Secure Real-time Transport Protocol (SRTP)メディアは、HdxRtcEngine.exeと他のピア間（会議の場合はMicrosoft 365会議サーバー）で直接流れます。

マイクロソフト 電話システム

Phone System は、Microsoft Teams を使用して Microsoft 365 クラウドで通話制御と PBX を可能にする Microsoft のテクノロジーです。Microsoft Teams の最適化は、Microsoft 365 Calling Plans または Direct Routing を使用して Phone System をサポートします。Direct Routing を使用すると、追加のオンプレミスソフトウェアなしで、サポートされている独自のセッションボーダーコントローラーを Microsoft Phone System に直接接続できます。 通話キュー、転送、フォワード、保留、ミュート、通話の再開がサポートされています。

DTMF

デュアルトーン多周波 (DTMF) 機能は、Citrix Workspace アプリの以下のバージョン (およびそれ以降) でサポートされています。

- Citrix Workspace アプリ for Windows バージョン 2102
- Citrix Workspaceアプリ Windows版 LTSR 1912 CU5 (Windows 10 OSのみ)
- Citrix Workspaceアプリ for Linux バージョン 2101
- Citrix Workspaceアプリ for Mac バージョン 2101
- Citrix Workspaceアプリ for Chrome OS バージョン 2111.1

動的e911のサポート

バージョン 2112 以降、Citrix Workspaceアプリは動的な緊急通報をサポートします。Microsoft Calling Plans、Operator Connect、およびDirect Routingで使用する場合、次のことが可能になります。

- 緊急通報の設定とルーティング。
- セキュリティ担当者への通知。

通知は、VDAで実行されているMicrosoft Teamsクライアントではなく、エンドポイントで実行されているCitrix Workspaceアプリの現在の場所に基づいて提供されます。

Ray Baum法では、911通報者の派遣可能な位置情報を適切な公共安全応答拠点（PSAP）に送信することが義務付けられています。HDXによるMicrosoft Teamsの最適化は、以下のバージョンのCitrix Workspaceアプリで使用する場合、Ray Baum法に準拠しています。

- Citrix Workspaceアプリ for Windows バージョン 2112.1 以降
- Citrix Workspaceアプリ for Linux バージョン 2112 以降
- Citrix Workspaceアプリ for Mac バージョン 2112 以降
- Citrix Workspaceアプリ for Chrome OS バージョン 2112 以降

動的な緊急通報を有効にするには、管理者はMicrosoft Teams管理センターを使用して、ネットワークまたは緊急ロケーションマップを作成するために以下を構成する必要があります。

- ネットワーク設定
- ロケーション情報サービス (LIS)

動的緊急通報の詳細については、Microsoft のドキュメントを参照してください。

Citrix WorkspaceアプリがMicrosoft Teamsに中継するディスパッチ可能な位置情報は次のとおりです。

- イーサネット/スイッチ接続用のリンク層検出プロトコル (LLDP) を使用したシャーシ ID / ポート ID。イーサネット/スイッチ (LLDP) は以下でサポートされています。
  - Windows バージョン 8.1 および 10
  - macOS。これにはLLDP有効化ソフトウェアが必要です。
  - Linux。シンクライアントのオペレーティングシステム (OS) ディストリビューションに LLDP ライブラリを含める必要があります。

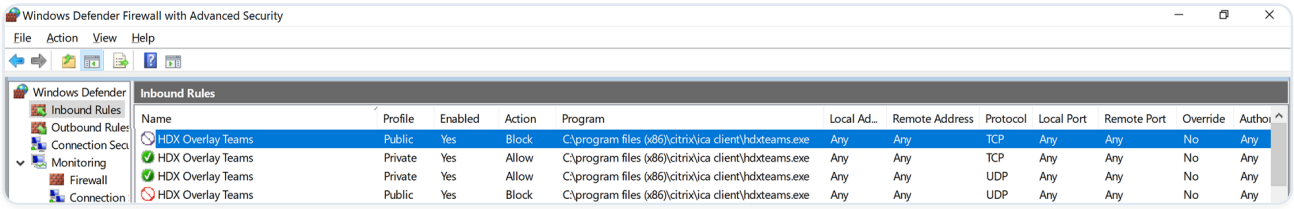
- Citrix Workspace アプリがインストールされているエンドポイントの WLAN BBSID および {IPv4-IPv6; サブネット; MAC アドレス}。
    - サブネットおよび WiFi ベースのロケーションは、Windows、Linux、Mac 用 Workspace アプリでサポートされています。
- 緯度と経度（Citrix Workspaceアプリがインストールされ ているOSレベルでユーザー権限が付与されている場合（権限はHDX RTC Engineに設定されています））。
    - すべてのWorkspaceアプリプラットフォームでサポートされています。ただし、Citrix Workspace for Linux の場合、シンクライアントの OS ディストリビューションに `libgps` ライブラリを含める必要があります (>sudo apt-get install libgps-dev gpsd lldpd)。

ファイアウォールの考慮事項

ユーザーが Microsoft Teams クライアントを使用して最適化された通話を初めて開始すると、**Windows ファイアウォール**設定に関する警告が表示されることがあります。この警告は、HdxTeams.exe または HdxRtcEngine.exe (HDX Overlay Microsoft Teams) の通信を許可するようユーザーに求めます。

ファイアウォールの警告](/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/firewall1.png)

「**Windows Defender ファイアウォール > セキュリティが強化されたWindows Defender ファイアウォール**」コンソールの**受信の規則**に、次の4つのエントリが追加されます。必要に応じて、より制限の厳しい規則を適用できます。



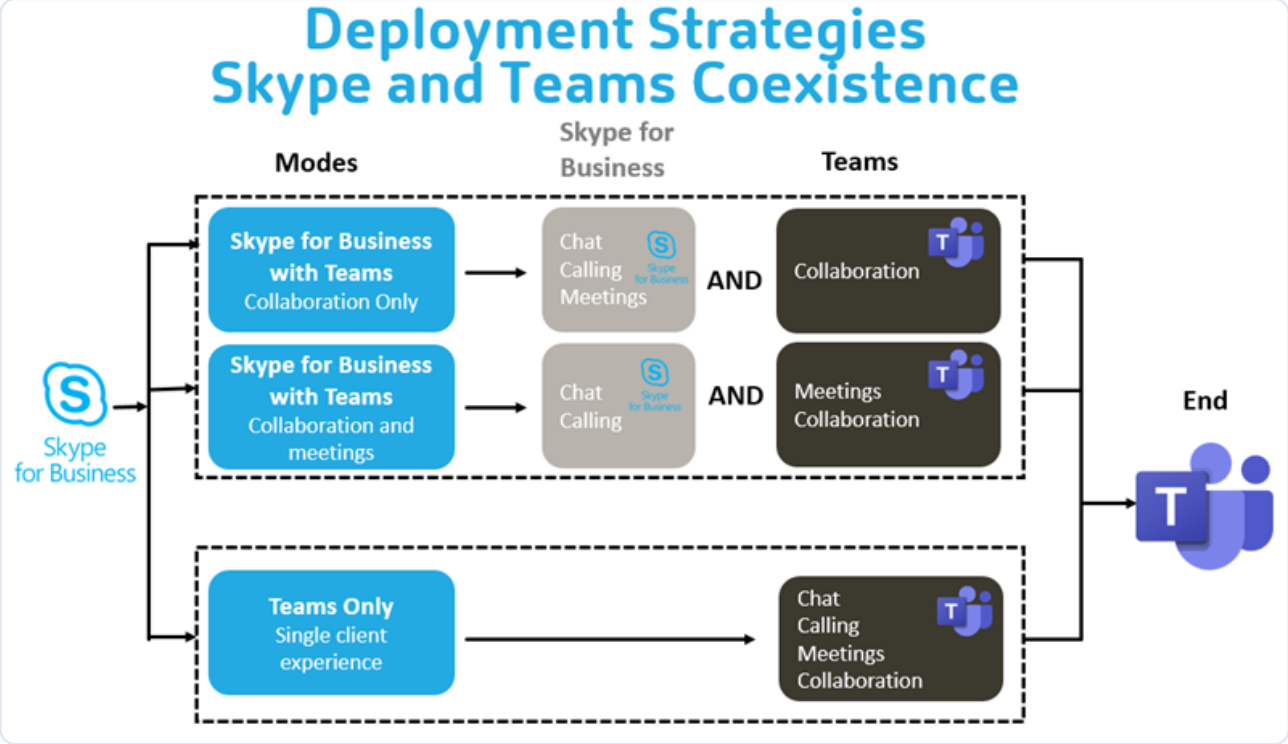
Microsoft Teams と Skype for Business の共存について

Microsoft TeamsとSkype for Businessは、機能が重複する2つの個別のソリューションとして並行して展開できます。 詳細については、「Microsoft TeamsとSkype for Businessの共存と相互運用性を理解する」を参照してください。

Citrix RealTime Optimization PackとMicrosoft Teamsマルチメディアエンジン用のHDX最適化は、環境で設定された構成を尊重します。例としては、アイランドモードや、Microsoft Teamsとの

Skype for Businessコラボレーションなどがあります。また、Microsoft TeamsとのSkype for Businessコラボレーションと会議も含まれます。

周辺機器へのアクセスは、一度に1つのアプリケーションにのみ許可されます。たとえば、通話中にRealTime Media EngineがWebカメラにアクセスすると、通話中はイメージングデバイスがロックされます。デバイスが解放されると、Microsoft Teamsで利用できるようになります。



Citrix SD-WAN™: Microsoft Teams向けに最適化されたネットワーク接続

最適なオーディオおよびビデオ品質には、低遅延、低ジッター、低パケット損失のMicrosoft 365クラウドへのネットワーク接続が必要です。支社のCitrix Workspaceアプリユーザーからデータセンターを経由してインターネットに接続する前に、Microsoft Teamsのオーディオ/ビデオRTPトラフィックをバックホールすると、過剰な遅延が発生する可能性があります。また、WANリンクで輻輳を引き起こす可能性もあります。Citrix SD-WANは、Microsoft 365のネットワーク接続原則に従って、Microsoft Teamsの接続を最適化します。Citrix SD-WANは、Microsoft RESTベースのMicrosoft 365 IPアドレスとWebサービス、および近接DNSを使用します。これは、Microsoft Teamsトラフィックを識別、分類、および誘導するために使用されます。

多くの地域で、ビジネスブロードバンドインターネット接続は、断続的なパケット損失、過剰なジッター期間、および停止に悩まされています。

Citrix SD-WANは、ネットワークの状態が不安定または劣化している場合に、Microsoft Teamsのオーディオ/ビデオ品質を維持するための2つのソリューションを提供します。

- Microsoft Azureを使用している場合、Azure VNETに展開されたCitrix SD-WAN仮想アプライアンス（VPX）は、高度な接続最適化を提供します。これらの最適化には、シームレスなリンクフェイルオーバーとオーディオパケットレーシングが含まれます。
- Citrix SD-WANのお客様は、Citrix Cloud™ Directサービスを介してMicrosoft 365に接続できます。このサービスは、すべてのインターネット向けトラフィックに対して信頼性の高い安全な配信を提供します。

支社のインターネット接続の品質が問題にならない場合は、遅延を最小限に抑えるだけで十分かもしれません。遅延を最小限に抑えるために、Microsoft TeamsトラフィックをCitrix SD-WANブランチアプライアンスから最寄りのMicrosoft 365フロントドアに直接誘導します。詳細については、「Citrix SD-WAN Office 365の最適化」を参照してください。

シトリックス SD-WAN](/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/sd-wan.png)

マルチウィンドウ会議とチャット

Windows版Microsoft Teamsでは、複数の会議またはチャットウィンドウを使用できます。ポップアウト機能の詳細については、Microsoft 365サイトのMicrosoft Teams Pop-Out Windows for Chats and Meetingsを参照してください。

> **注：**
>
> この機能は、Citrix Workspaceアプリ for Windows 2112.1、Mac 2203、Linux 2203、およびVDA 2112でサポートされています。

Microsoft Teamsのギャラリービューとアクティブスピーカー

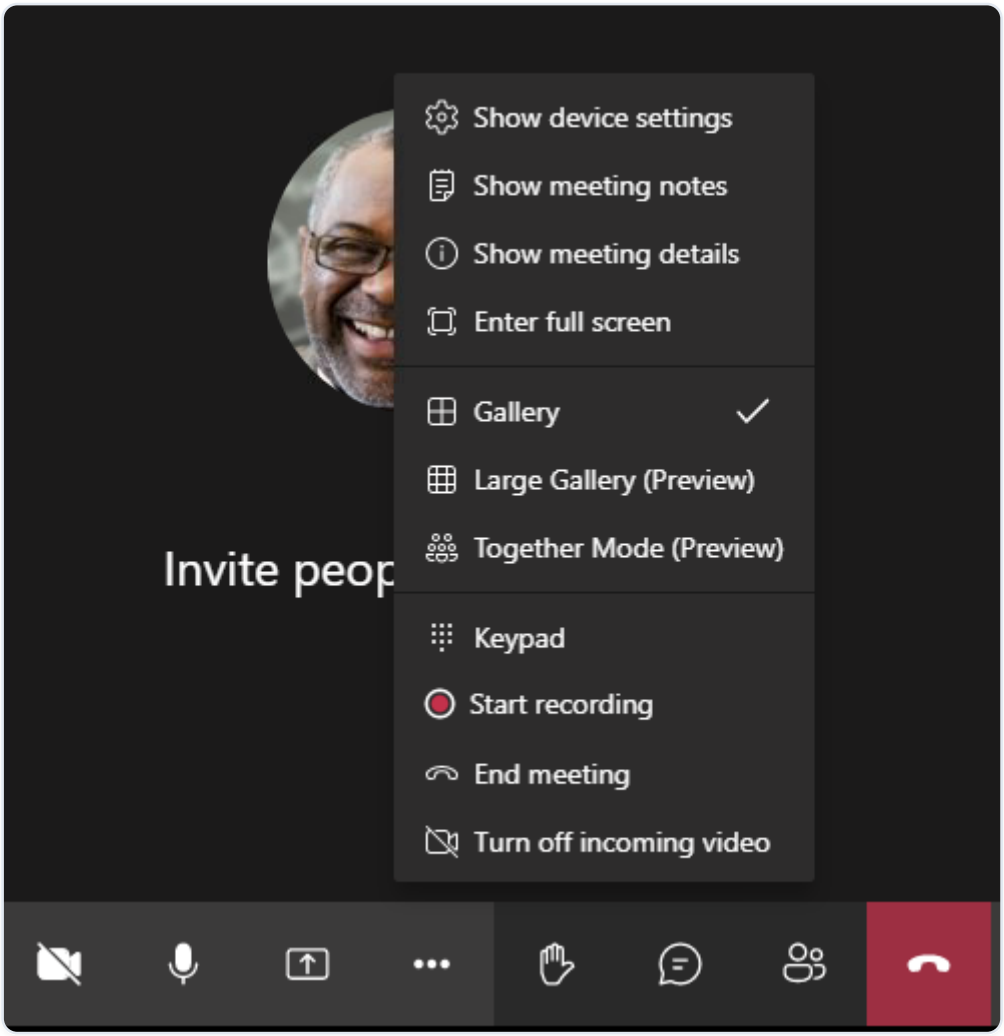
Microsoft Teamsは、**ギャラリー**、**大規模ギャラリー**、および**Together**モードのレイアウトをサポートしています。

Microsoft Teamsは、4人の参加者のビデオストリームを2x2のグリッドで表示します（**ギャラリー**として知られています）。この場合、Microsoft Teamsはデコードのために4つのビデオストリームをクライアントデバイスに送信します。4人以上の参加者がビデオを共有している場合、画面には最もアクティブな最後の4人のスピーカーのみが表示されます。

Microsoft Teamsは、最大7x7のグリッドを持つ大規模ギャラリービューも提供します。その結果、Microsoft Teams会議サーバーは単一のビデオフィードを合成し、デコードのためにクライアントデバイスに送信するため、CPU消費量が削減されます。この単一のマトリックス形式のフィードには、ユーザーのセルフプレビュービデオも含まれる場合があります。

最後に、Microsoft Teamsは新しい会議エクスペリエンスの一部である**Together**モードをサポートしています。AIセグメンテーション技術を使用して参加者を共有背景にデジタル配置することで、Microsoft Teamsはすべての参加者を同じ講堂に配置します。

ユーザーは、会議中に省略記号メニューで**ギャラリー**、**大規模ギャラリー**、または**Together**モードのレイアウトを選択することで、これらのモードを制御できます。



ビデオアスペクト比の制約のサポート（CWA for Windows 2102、CWA for Linux 2106、CWA for MAC 2106以降）：

- **フレームに合わせる**オプションは、ギャラリー/大規模ギャラリービューで利用できます。このオプションは、サブウィンドウに収まるようにビデオサイズをトリミングします。一方、**フレームにフィット**は、ビデオの側面に黒いバー（レターボックス）を表示するため、トリミングは行われません。

次の表は、ギャラリーレイアウトと大規模ギャラリーレイアウトの比較を示しています。

	ギャラリービュー 2X2 (デフォルト)	ラージギャラリービュー
レイアウト/グリッド	4人の参加者のビデオストリームを含む2x2のグリッドを表示します。画面には直近の最もアクティブな4人のスピーカーのみが表示され、他の参加者はグリッドに表示されません。	49人の参加者のビデオストリームを含む7x7のグリッドを表示します。
ミキシング技術	メディアルーターは、各参加者からの個々のストリームをすべてのユーザーに転送します。	中央の会議サーバーがすべてのオーディオまたはビデオをミキシングおよびトランスコードし、各参加者向けにカスタマイズされた複合レイアウトを作成します。この処理により、追加の遅延が発生します。
アクティブスピーカー	新しいアクティブスピーカーは、グリッド内で最もアクティブでないスピーカーと置き換わります。	アクティブか非アクティブかに関わらず、すべての参加者を表示します。
エンドポイントでのエンコード	単一品質のビデオストリーム。クライアントでエンコード解像度値を設定できます。詳細については、エンコーダーパフォーマンスエスティメーターおよびMicrosoft Teamsの最適化を参照してください。品質は解像度と1秒あたりのフレーム数として定義されます。現在、サイマルキャストビデオはサポートされていません。	単一品質のビデオストリーム。クライアントでエンコード解像度値を設定できます。詳細については、エンコーダーパフォーマンスエスティメーターおよびMicrosoft Teamsの最適化を参照してください。
エンドポイントでのデコード	各参加者は最大4つの個別のメディアストリームを受信します。これにより、HdxRtcEngine.exeによるエンドポイントでのCPU消費量が	各参加者は、オーディオとビデオの単一ストリームのみを取得します。この設定により、エンドポイントでのCPU消費が削減されます。

	ギャラリービュー 2X2 (デフォルト)	ラージギャラリービュー
	増加します（デコード/レンダリングのため）。	
最大解像度	720p。4人の参加者がビデオを共有している場合、ビデオフィードあたりの最大解像度は360pです。4人未満の参加者がビデオを共有している場合、ビデオフィードあたりの解像度は高くなる可能性があります。	複合レイアウトまたはミキシングの場合は720p。複合レイアウトでは、参加者ごとに高品質のビデオストリームは必要ありません。この条件のため、各送信者は解像度またはアップロードビットレートを削減します。
「低速ユーザー」の問題	送信者は、各モダリティ（オーディオ/ビデオ/画面共有）の品質を、参加者間の最低共通ネットワーク品質に調整します。このマルチメディアストリームは、他のすべての参加者に転送されます。その結果、ネットワーク状態の悪い参加者が、通話中の他の全員の品質に影響を与えます。	最低共通ネットワーク品質のシナリオの影響を受けにくい。会議サーバーは、個々の参加者のネットワーク状態に基づいて異なる品質を提供します。
セルフプレビュー	自分自身を小さなサムネイルでリアルタイムに表示します。	自分自身をサムネイルで表示し、他のビデオフィードと混合します。その結果、メインのビデオレイアウトに自分自身が追加の遅延とともに含まれて表示されることがあります。

Microsoft Teamsでの画面共有

Microsoft Teamsは、ビデオベースの画面共有（VBSS）に依存しており、共有されているデスクトップをH264などのビデオコーデックで効率的にエンコードし、高精細ストリームを作成します。HDX最適化を使用すると、受信する画面共有はビデオストリームとして扱われます。

Windows、Linux、またはMac用のCitrix Workspaceアプリ2109以降では、ユーザーは画面とビデオカメラを同時に共有できます。

以前のバージョンでは、ビデオ通話中に相手がデスクトップの共有を開始すると、元のカメラビデオフィードは一時停止されます。代わりに、画面共有ビデオフィードが表示されます。その後、相手は手動でカメラ共有を再開する必要があります。

PowerPoint Liveに関する注意

PowerPoint Liveからコンテンツを共有している場合、この制限はありません。その場合、他のピアは引き続きあなたのウェブカメラとコンテンツを見ることができ、他のスライドを確認するために前後に移動できます。このシナリオでは、スライドはVDAでレンダリングされます。PowerPoint Liveのスライドデッキにアクセスするには、「共有トレイ」ボタンをクリックし、提案されたPowerPointスライドのいずれかを選択するか、「参照」をクリックして、コンピューターまたはOneDrive上のPowerPointファイルを見つけます。

送信画面共有も最適化され、Citrix Workspaceアプリにオフロードされます。この場合、メディアエンジンはCitrix Desktop Viewer (CDViewer.exe) ウィンドウのみをキャプチャして送信し、その周囲には赤い枠線が描画されます。Desktop Viewerと重なるローカルアプリケーションはキャプチャされません。

注

Mac版Citrix Workspaceアプリで画面共有を有効にするには、特定の権限を設定してください。詳細については、システム要件を参照してください。

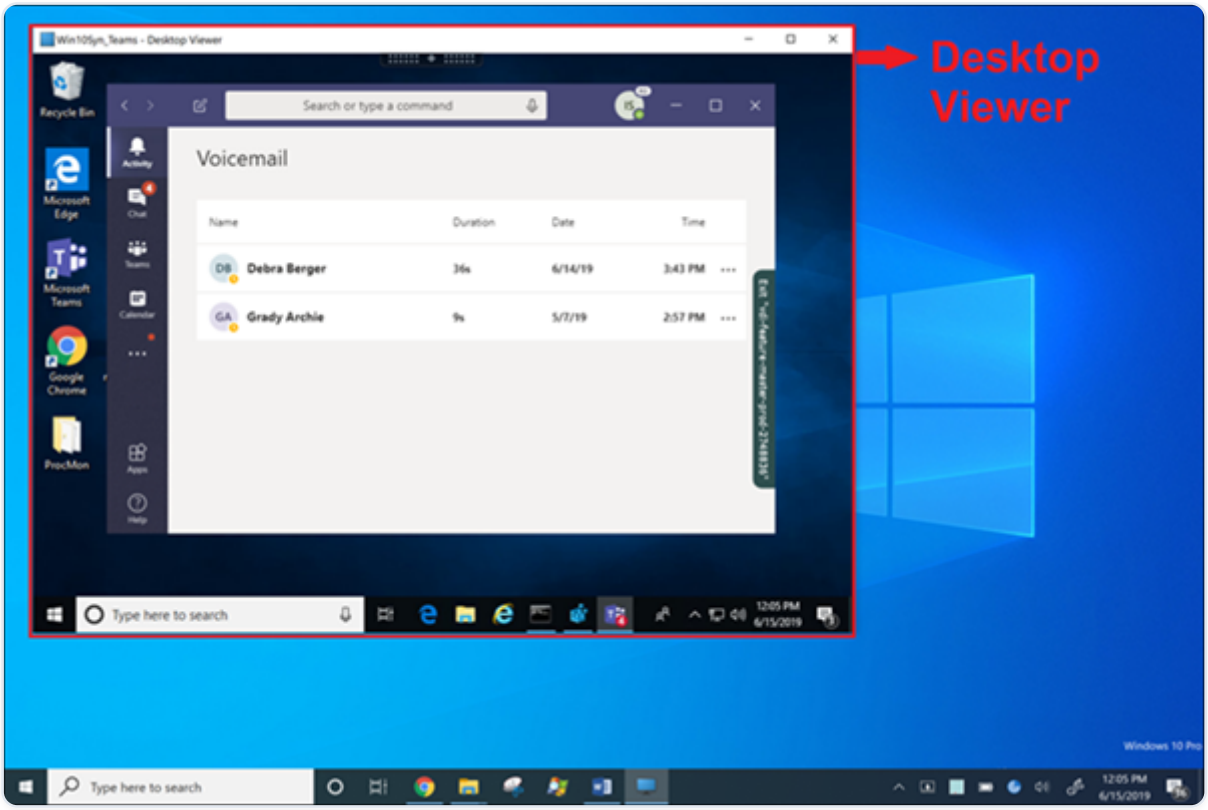
マルチモニター

Desktop Viewer (CDViewer.exe) がフルスクリーンモードでマルチモニター設定にまたがっている場合、Citrix Workspaceアプリ2106以降 (Windows/Linux/Mac) では、画面ピッカーで共有するモニターを選択できます。

既知の制限:

- Desktop Viewerが無効になっている場合、またはDesktop Lockが使用されている場合、Microsoft Teamsの画面ピッカーではマルチモニター選択は利用できません。Desktop Viewerは、`.ICA`ファイルテンプレートを編集するか、`StoreFront web.config`によって無効にすることができます。SHIFT+F2ホットキーはマルチモニター画面共有と互換性がありません。

- Workspaceアプリのバージョン2106より古い場合、プライマリモニターのみが共有されます。通話中の他のピアに見せるには、仮想デスクトップ内のアプリケーションをプライマリモニターにドラッグしてください。
- Citrix Workspaceアプリを仮想モニターレイアウト機能（単一の物理モニターの論理パーティション）で構成した場合、マルチモニター画面共有が機能しない可能性があります。この場合、すべての仮想モニターは複合画像として共有されます。
- Windows版Citrix Workspaceアプリの古いバージョン（1907から2008まで）では、クライアントマシンで実行されているローカルアプリケーションも共有されます。この共有は、ローカルアプリがDesktop Viewerの上にオーバーレイされている場合にのみ可能です。この動作は、2009.6以降および1912 CU5以降で削除されました。



シームレスアプリケーションからの画面共有:

Microsoft Teamsをスタンドアロンのシームレスアプリケーションとして公開している場合、画面共有は物理エンドポイントのローカルデスクトップをキャプチャします。Citrix Workspaceアプリの最小バージョン1909が必要です。

アプリ共有

Citrix Workspaceアプリ for Windows 2112.1およびVDA 2112以降、Microsoft TeamsはHDX 3D Proを使用したアプリ共有をサポートしています。

Citrix Workspace app for Windows 2109、Mac 2203、およびVDA 2109以降、Microsoft Teamsは仮想セッションで実行されている特定のアプリの画面共有をサポートします。特定のアプリを共有するには:

1. リモートセッション内でMicrosoft Teamsアプリに移動します。
2. Microsoft Teams UIで**コンテンツを共有**をクリックします。
3. 会議で共有するアプリを選択します。選択したアプリの周囲に赤い枠が表示され、通話中の参加者は共有されたアプリを見ることができます。

別のアプリを共有するには、もう一度**コンテンツを共有**をクリックして、新しいアプリを選択します。

アプリ共有を無効にする場合は、VDAの`HKLM\SOFTWARE\Citrix\Graphics`に次のレジストリキーを作成します。 名前: `UseWsProvider` 種類: `DWORD` 値: 0

> **注：**
>
> - アプリを最小化すると、Microsoft Teamsは共有アプリの最後の画像を表示します。画面共有を再開するには、ウィンドウを最大化できます。
> - 画面共有は、VDA側でのウィンドウのキャプチャに依存します。コンテンツは最大レートでCitrix Workspaceアプリに中継されます。最大レートは1秒あたり30フレームです。Citrix Workspaceアプリは、コンテンツをピアまたは会議サーバーに転送します。

> Microsoft Teamsのアプリ共有](/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/ms-teams-app-sharing.png)

特定のアプリの画面共有に関する既知の制限：

- アプリを画面共有している場合、マウスカーソルは表示されません。
- アプリを共有中に最小化すると、スクリーンピッカーにはアプリのアイコンのみが表示されます。アプリのサムネイルはスクリーンピッカーでプレビューされません。アプリを最大化するまで、コンテンツを共有できず、赤い枠も表示されません。

アプリ保護との互換性 特定のアプリの画面共有は、HDX最適化されたMicrosoft Teamsのアプリ保護機能と互換性があります。アプリ保護が有効になっているデリバリーグループからアプリまたはデスクトップを起動した場合、特定のアプリを画面共有できます。

Microsoft Teams UIで**コンテンツを共有**をクリックすると、スクリーンピッカーから**デスクトップ**オプションが削除されます。開いているアプリを共有するには、**ウィンドウ**オプションのみを選択できます。

> **注：**
>
> アプリ保護が有効になっているデリバリーグループからアプリまたはデスクトップを起動する場合、Workspace app for Windows 2202以前を使用していると、受信ビデオまたは画面共有を表示できません。この制限は、Workspace app for Windows 2203 LTSR以降にはありません。

Microsoft Teamsで制御を付与および要求する

この機能は、Citrix Workspaceアプリの以下のバージョンでサポートされています（VDAバージョンやオペレーティングシステム、シングルセッションまたはマルチセッションには依存しません）。

- Windows版Citrix Workspaceアプリ バージョン2112.1以降
- Mac版Citrix Workspaceアプリ バージョン2203.1以降

Microsoft Teams通話中に参加者が画面を共有している場合、制御を要求できます。制御を取得すると、共有画面に対して選択、編集、その他のキーボードおよびマウス操作を行うことができます。

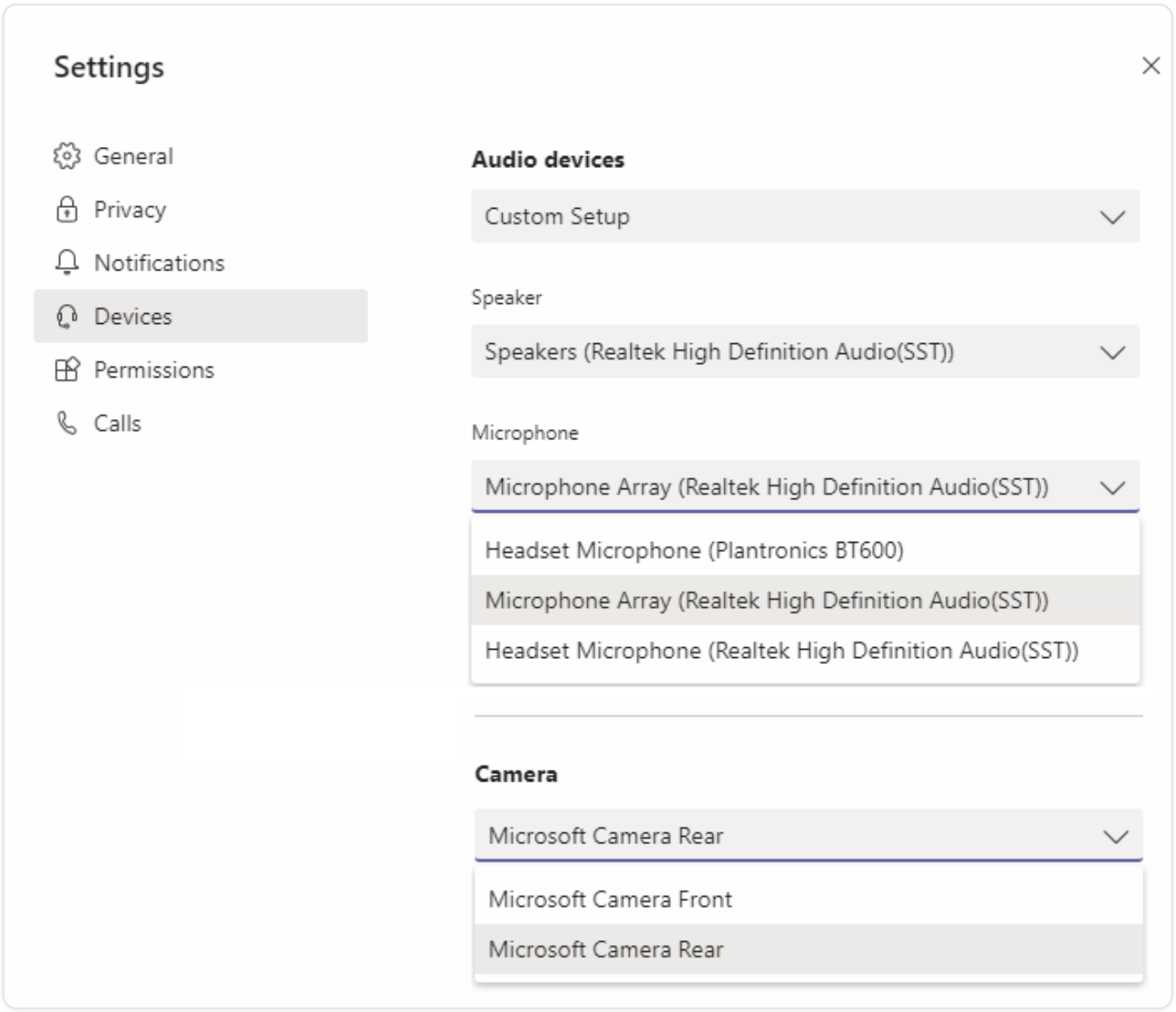
画面が共有されているときに制御を取得するには、Microsoft Teams UIの**制御を要求**ボタンをクリックします。画面を共有している会議参加者は、あなたの要求を許可または拒否できます。

制御中は、共有画面に対して選択、編集、その他の変更を行うことができます。これらの操作には、キーボードとマウスの両方を使用します。完了したら、**制御を要求**をクリックします。

> **制限事項:**
>
> - ユーザーが単一のアプリ（アプリ共有とも呼ばれます）を共有している場合、制御の付与と要求は利用できません。デスクトップ全体またはモニターを共有する必要があります。
> - コントロールバーを特定の場所に固定する機能は利用できません。

Microsoft Teamsでの周辺機器

Microsoft Teamsの最適化が有効な場合、Citrix Workspaceアプリは周辺機器（ヘッドセット、マイク、カメラ、スピーカーなど）にアクセスします。その後、周辺機器はMicrosoft Teams UIの（**設定 > デバイス**）に適切に一覧表示されます。



Microsoft Teamsはデバイスに直接アクセスしません。代わりに、メディアの取得、キャプチャ、処理のためにWorkspaceアプリのWebRTCメディアエンジンに依存します。Microsoft Teamsは、ユーザーが選択できるようにデバイスを一覧表示します。

Microsoft Teamsがアクティブなときに挿入された周辺機器は、デフォルトでは選択されません。Microsoft Teams UIの**設定** > **デバイス**画面から周辺機器を手動で選択する必要があります。周辺機器が選択されると、Microsoft Teamsは周辺機器の情報をキャッシュします。その結果、同じエンドポイントからセッションに再接続すると、周辺機器が自動的に選択されます。

推奨事項:

- エコーキャンセレーション内蔵のMicrosoft Teams認定ヘッドセット。マイクとスピーカーが別々のデバイスにある追加の周辺機器を使用するセットアップでは、エコーが発生する可能性があります。例としては、マイク内蔵のWebカメラとスピーカー付きのモニターがあります。外部スピーカーを使用する場合は、マイクからできるだけ離して配置してください。また、音をマイクに屈折させる可能性のある表面から離して配置してください。
- Microsoft Teams認定カメラ。ただし、Skype for Business認定周辺機器もMicrosoft Teamsと互換性があります。
- Citrix Workspaceアプリのメディアエンジンは、オンボードH.264エンコーディング（UVC 1.1および1.5）を実行するWebカメラではCPUオフロードを利用できません。

注：

Windows用Workspaceアプリ2009.6は、24ビットまたは96 kHzを超える周波数のオーディオ形式に対応した周辺機器を取得できるようになりました。

HdxTeams.exe（Windows用Citrix Workspaceアプリ2009以前の場合）は、これらの特定のオーディオデバイス形式（チャンネル、ビット深度、サンプルレート）のみをサポートします。

- 再生デバイス: 最大2チャンネル、16ビット、最大96,000 Hzの周波数
- 録音デバイス: 最大4チャンネル、16ビット、最大96,000 Hzの周波数

スピーカーまたはマイクのいずれかが予期される設定と一致しない場合でも、Microsoft Teamsでのデバイス列挙は失敗し、**設定 > デバイス**の下に**なし**と表示されます。

HdxTeams.exeの**Webrpc**ログには、この種類の情報が表示されます。

`Mar 27 20:58:22.885 webrtcapi.WebRTCEngine Info: init. initializing...`.

`Mar 27 20:58:23.190 webrtcapi.WebRTCEngine Error: init. couldn't create audio module!`!

回避策として、特定のデバイスを無効にするか、次のいずれかを実行します。

1. **サウンドコントロールパネル** (mmsys.cpl) を開きます。
2. 再生デバイスまたは録音デバイスを選択します。
3. **プロパティ > 詳細設定**に移動し、設定をサポートされているモードに変更します。

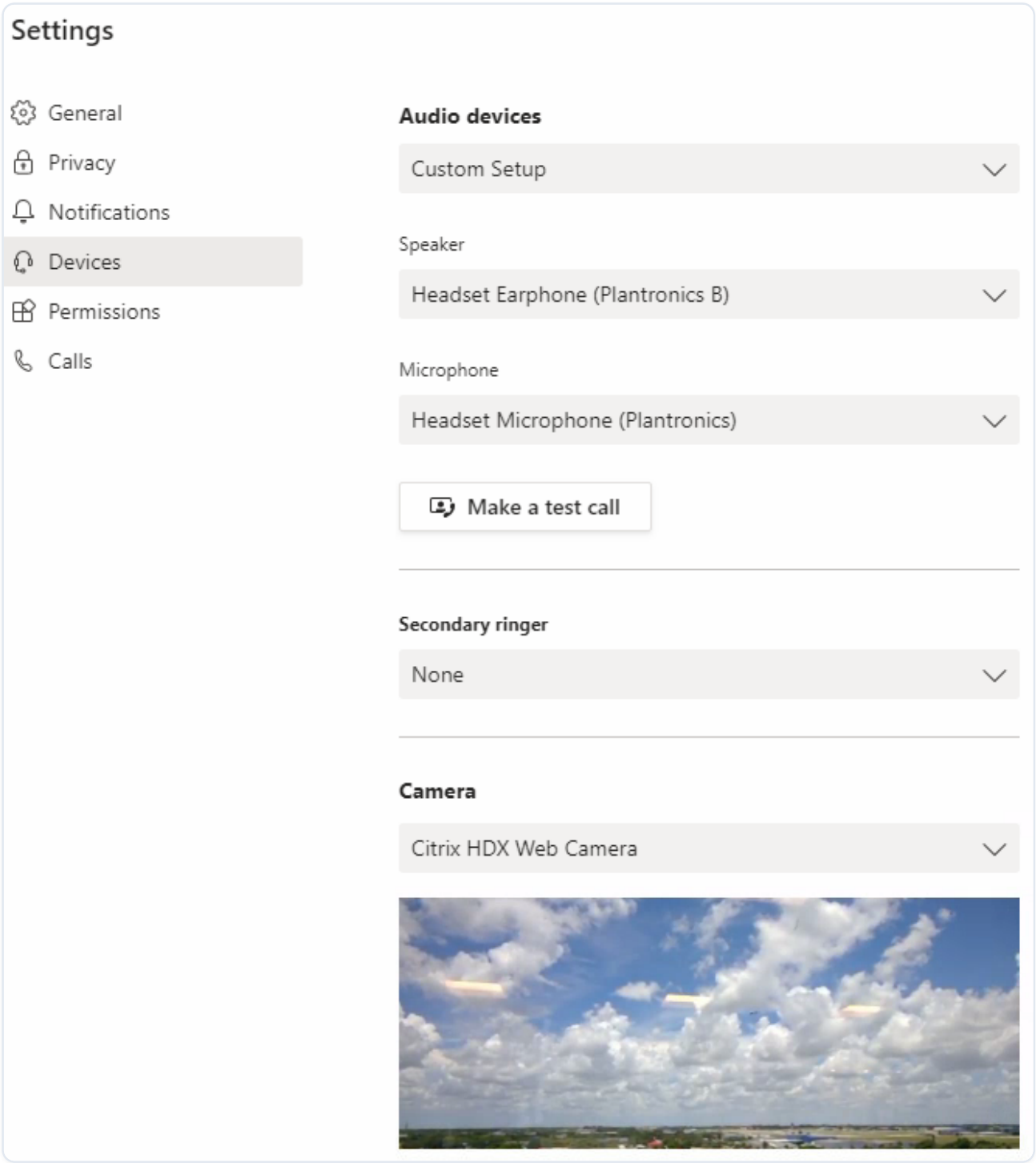
フォールバックモード

Microsoft Teamsが最適化されたVDIモード（Teams/バージョン情報/バージョンで「Citrix HDX Not Connected」と表示される）でロードに失敗した場合、VDAはレガシーHDXテクノロジーにフォールバックします。レガシーHDXテクノロジーには、Webカメラのリダイレクト、クライアントオーディオ、マイクのリダイレクトが含まれる場合があります。Microsoft Teamsの最適化をサポートしないWorkspaceアプリのバージョン/プラットフォームOSを使用している場合、フォールバックレジストリキーは適用されません。 フォールバックモードでは、周辺機器はVDAにマッピングされます。周辺機器は、仮想デスクトップにローカルで接続されているかのようにMicrosoft Teamsアプリに表示されます。

VDAでレジストリキーを設定することにより、フォールバックメカニズムをきめ細かく制御できるようになりました。詳細については、レジストリを介して管理される機能のリストにある Microsoft Teamsフォールバックモードを参照してください。

この機能には、Microsoft Teamsバージョン1.3.0.13565以降が必要です。

Microsoft Teamsアプリの**設定 > デバイス**タブで、最適化モードか非最適化モードかを確認するには、カメラ名が主な違いとなります。Microsoft Teamsが非最適化モードでロードされた場合、レガシーHDXテクノロジーが起動します。Webカメラ名には、次の図に示すように**Citrix HDX**サフィックスが付いています。スピーカーとマイクのデバイス名は、最適化モードと比較してわずかに異なる（または切り詰められている）場合があります。



従来のHDXテクノロジーを使用する場合、Microsoft Teamsはオーディオ、ビデオ、画面共有の処理をエンドポイントのCitrix WorkspaceアプリWebRTCメディアエンジンにオフロードしません。代わりに、HDXテクノロジーはサーバー側レンダリングを使用します。ビデオをオンにすると、VDAで高いCPU消費が予想されます。リアルタイムオーディオのパフォーマンスは最適ではない可能性があります。

既知の制限事項

Citrixの制限事項

Citrix Workspaceアプリの制限事項：

- HIDボタン - 通話応答と通話終了はサポートされていません。音量アップとダウンはサポートされています。
- Microsoft Teamsの管理センターでのQoS設定は、VDIユーザーには適用されません。
- VDAでスニッピングツールを使用している場合、ユーザーはTeamsコンテンツのスクリーンショットを撮ることができません。クライアント側で使用した場合のみ、コンテンツをキャプチャできます。

VDAの制限事項：

- Citrix WorkspaceアプリのDPI設定を**はい**に構成すると、リダイレクトされたビデオウィンドウがずれて表示されます。この制限は、モニターのDPIスケーリング係数が100%を超えて設定されている場合に発生します。

Citrix WorkspaceアプリとVDAの制限事項：

- 最適化された通話の音量は、VDAではなく、クライアントマシンの音量バーを使用してのみ制御できます。

Microsoftの制限事項

- 3x3ギャラリービューはサポートされていません。Microsoft Teamsの依存関係 – 3x3グリッドがいつ提供されるかについてはMicrosoftにお問い合わせください。
- Skype for Businessとの相互運用性は音声通話に限定されており、ビデオモダリティはありません。
- 送受信ビデオストリームの最大解像度は720pです。
- PSTN通話の呼び出し音はサポートされていません。
- ダイレクトルーティングのメディアバイパスはサポートされていません。
- ブロードキャストおよびライブイベントのプロデューサーおよびプレゼンターの役割はサポートされていません。出席者の役割はサポートされていますが、最適化されていません（代わりにVDAでレンダリングされます）。
- Microsoft Teamsのズームインおよびズームアウト機能はサポートされていません。
- ロケーションベースルーティングとメディアバイパスはサポートされていません。
- 通話の健全性は利用できません。

- ブレイクアウトルームはVDI参加者でサポートされています。主催者がVDIユーザーの場合、Microsoft Teamsはブレイクアウトルームをサポートしません。
- 通話のマージはサポートされていません（ユーザーインターフェイスにオプションが表示されません）。

CitrixとMicrosoftの制限事項

- 画面共有を行う際、「**システムオーディオを含める**」オプションは利用できません。
- サイマルキャストは利用できません。
- **セカンダリリンガー** (**Teams** > **設定** > **デバイス**) はサポートされていません。
- 背景をぼかしたりカスタマイズしたりするオプションはサポートされていません。

今後のMicrosoft Teamsシングルウィンドウの EOL

January 31, 2024に、MicrosoftはVDI Microsoft Teams最適化を使用する際のシングルウィンドウUIに対するMicrosoft Teamsのサポートを終了し、マルチウィンドウエクスペリエンスのみをサポートします。Microsoftは、9/8/2023にM365管理者センター（投稿ID: MC674419）でこの非推奨化について通知しました。 マルチウィンドウ機能に関する公開されている詳細は、Tech Communityの記事「New Meeting and Calling Experience in Microsoft Teams」で確認できます。

ビデオおよび画面共有のためにMicrosoft Teamsを最適化モードで引き続き使用するには、VDAとCitrix Workspaceアプリをサポートされているバージョンにアップグレードする必要があります。インフラストラクチャとエンドポイントをマルチウィンドウをサポートするようにアップグレードしない場合、音声通話のみ確立できます。最適化されたビデオおよび画面共有機能を使用できなくなります。

次の表は、Citrix VDIでMicrosoft Teamsの最適化された通話を継続して使用するために必要なVDAおよびCitrix Workspaceアプリの最小バージョン、LTSRバージョン、推奨バージョンを示しています。

コンポーネント	最小バージョン	LTSRサポートバージョン	推奨バージョン
マイクロソフト チームズ	1.5.00.11865	該当なし	最新
VDA	1912 CU6 LTSR, 2112 CR	1912 CU7+、2203 CU2+	2308 CR+

コンポーネント	最小バージョン	LTSRサポートバージョン	推奨バージョン
Windows版 Citrix Workspaceアプリ	2205 CR	2203 CU2+	2309 CR以降
Mac版 Citrix Workspaceアプリ	2209 CR	該当なし	2308 CR+
Linux向け Citrix Workspace アプリ	2209 CR	該当なし	2308 CR+
ChromeOSまたはHTML5版 Citrix Workspaceアプリ	2303 CR	該当なし	2309 CR以降

WebRTCからのSDP形式（プランB）の非推奨のお知らせ

Citrixは、将来のリリースでWebRTCからの現在のSDP形式 (プランB) のサポートを廃止する予定です。最適化されたMicrosoft Teamsの機能に対応するには、WebRTCでUnified Planを使用する必要があります。

影響を受ける製品

Citrix Workspaceアプリケーションの将来のリリースにおいて、Citrix Workspaceアプリの今後のリリースを使用するエンドポイントと、Citrix Workspaceアプリ2108以前のバージョンを使用するエンドポイント間の通話はサポートされません。この通話の非互換性には、1912 LTSR Citrix Workspaceアプリクライアント (CWA) が含まれます。以下のCWAクライアントが影響を受けます。

- Windows向けCitrix Workspaceアプリ
- Linux向け Citrix Workspace アプリ
- Mac向けCitrix Workspaceアプリ
- Chrome向けCitrix Workspaceアプリ

プランBの代替

Citrix Workspaceアプリのバージョン2109より古いバージョンを実行している場合は、サポートされているバージョン（できれば最新のCRリリース）にアップグレードする必要があります。そうしないと、将来のリリースまたは新しいエンドポイントとの通話は接続に失敗します。将来のリ

リースとフェデレーション通信パートナー間の通話も、フェデレーションパートナーがCitrix Workspaceをアップグレードしていない場合、完了に失敗する可能性があります。

Citrix Workspaceアプリバージョン2108は2023年3月にサポート期限を終了しました。より新しいバージョンにアップグレードする必要があります。詳細については、Citrix Workspaceアプリのバージョンサポートに関するWorkspace Appを参照してください。

プランBの廃止に関する詳細については、WebRTCドキュメントを参照してください。

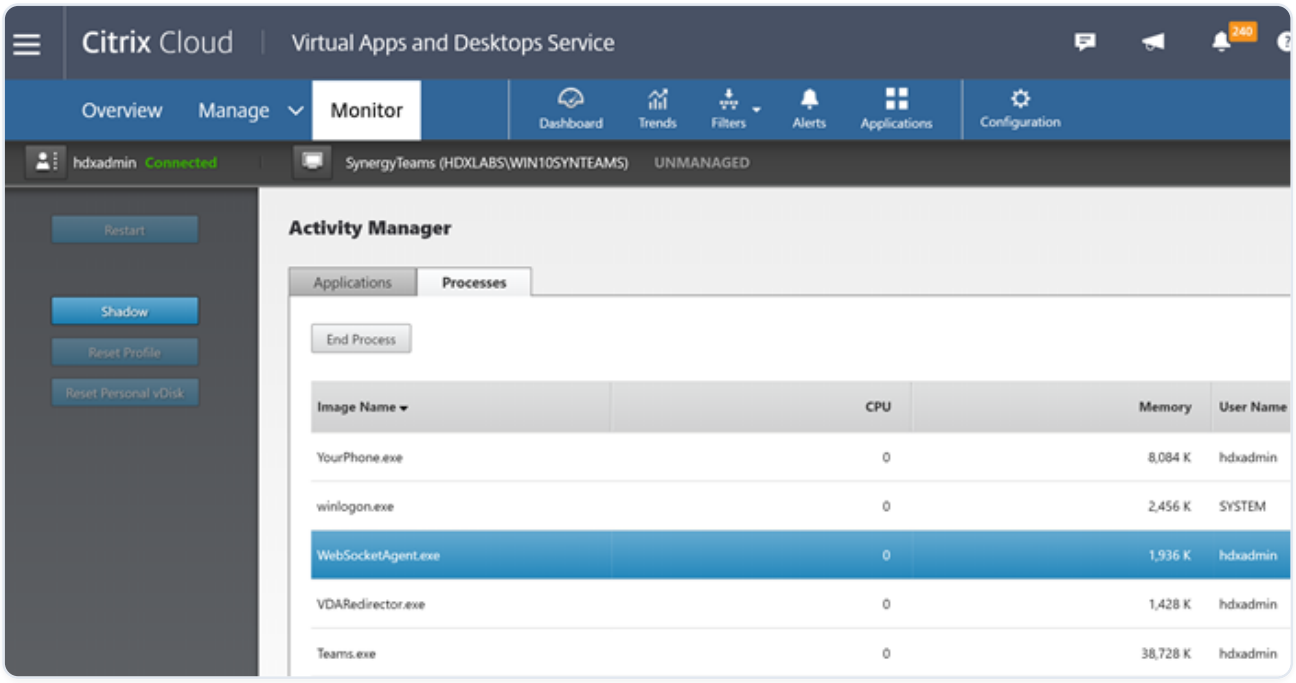
追加情報

- Microsoft Teams の監視、トラブルシューティング、サポート
- VM への Microsoft Teams デスクトップアプリの展開
- MSI を使用した Microsoft Teams のインストール (VDI インストールセクション)
- シンクライアント
- Skype for Business ネットワーク評価ツール
- Microsoft Teams と Skype for Business の共存と相互運用性を理解する

Microsoft Teamsの監視、トラブルシューティング、サポート

Teamsの監視

このセクションでは、HDXによるMicrosoft Teamsの最適化を監視するためのガイドラインを提供します。 最適化モードで実行中で、`HdxRtcEngine.exe`がクライアントマシンで実行されている場合、VDA上の`WebSocketAgent.exe`というプロセスがセッションで実行されています。Directorの**アクティビティマネージャー**を使用してアプリケーションを確認します。



VDAバージョン1912以降では、Citrix HDX Monitor（バージョン3.11以降）を使用してアクティブなTeams通話を監視できます。Citrix Virtual Apps and Desktops製品ISOには、フォルダー `layout\image-full\Support\HDX Monitor` に最新の `hdxmonitor.msi` が含まれています。

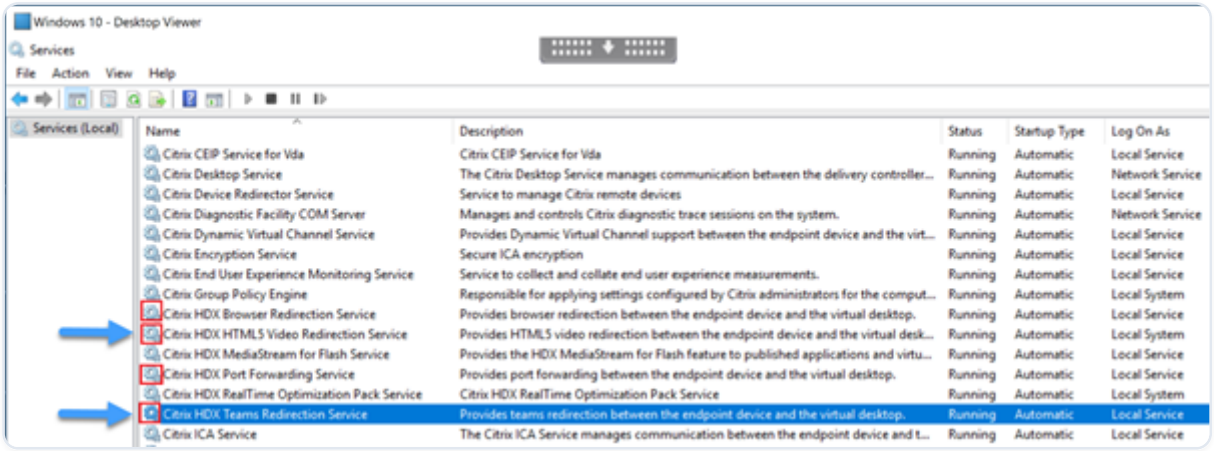
詳しくは、Knowledge Centerの記事「CTX253754」の「*監視*」を参照してください。

トラブルシューティング

このセクションでは、Microsoft Teamsの最適化を使用する際に発生する可能性のある問題のトラブルシューティングのヒントを提供します。詳しくは、「CTX253754」を参照してください。

バーチャル デリバリー エージェント上で

BCR_x64.msiによって4つのサービスがインストールされます。このうち2つだけがVDAでのMicrosoft Teamsリダイレクトを担当します。



- **Citrix HDX Teams Redirection Service**は、Microsoft Teamsで使用される仮想チャネルを確立します。このサービスはCtxSvcHost.exeに依存しています。

- **Citrix HDX HTML5 Video Redirection Service**は、WebSocketService.exeとして実行され、127.0.0.1:9002 TCPでリッスンします。WebSocketService.exeは主に2つの機能を実行します。

  i. **セキュアWebSocketのTLS終端**は、Microsoft Teamsアプリ内のコンポーネントであるvdiCitrixPeerConnection.jsからセキュアWebSocket接続を受信します。これはProcess Monitorで追跡できます。証明書について詳しくは、「ControllerとVDA間の通信」の「TLSとHTML5ビデオのリダイレクト、およびブラウザコンテンツのリダイレクト」セクションを参照してください。

  一部のアンチウイルスソフトウェアやデスクトップセキュリティソフトウェアは、`WebSocketService.exe`とその証明書の適切な機能に干渉します。Citrix HDX HTML5 Video Redirectionサービスが`services.msc`コンソールで実行されている場合でも、netstatで確認すると、localhost `127.0.0.1:9002` TCPソケットはリッスンモードになりません。サービスを再起動しようとすると、ハングアップします（「停止中...」）。`WebSocketService.exe`プロセスに適切な除外を適用してください。

  「プロセスモニター」(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/team-process-monitor.png)

  ii. **ユーザーセッションマッピング。** Microsoft Teamsアプリケーションが起動すると、WebSocketService.exeはVDAのユーザーセッションでWebSocketAgent.exeプロセスを開始します。WebSocketService.exeはLocalSystemアカウントとしてセッション0で実行されます。

  「WebSocketAgent.exeサービス」(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/websocketservice-websocketagent.png)

  VDAでWebSocketService.exeサービスがアクティブなリッスン状態にあるかどうかを確認するには、`netstat`を使用できます。

  昇格されたコマンドプロンプトウィンドウから`netstat -anob -p tcp`を実行します。

  「netstatの例を実行」(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/teams-netstat.png)

  接続が成功すると、状態はESTABLISHEDに変わります。

  「netstatの成功例」(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/teams-netstat-success.png)

> **重要:**

WebSocketService.exeは、2つのTCPソケット（127.0.0.1:9001と127.0.0.1:9002）でリッスンします。ポート9001は、ブラウザコンテンツリダイレクトとHTML5ビデオのリダイレクトに使用されます。ポート9002は、Microsoft Teamsのリダイレクトに使用されます。Teams.exeとWebSocketService.exe間の直接通信を妨げる可能性のあるプロキシ構成がVDAのWindows OSにないことを確認してください。Internet Explorer 11で明示的なプロキシ（**インターネットオプション > 接続 > LANの設定 > プロキシサーバー**）を構成すると、接続が割り当てられたプロキシサーバーを経由する場合があります。手動および明示的なプロキシ設定を使用する場合は、**ローカルアドレスにはプロキシサーバーを使用しない**がチェックされていることを確認してください。

サービスの位置と説明

サービス	WINDOWS SERVER OSの実行可能ファイルへのパス	ログオンアカウント	説明
Citrix HTML5ビデオリダイレクトサービス	"C:\Program Files (x86)\Citrix\System32\WebSocketService.exe" /service	ローカルシステムアカウント	仮想デスクトップとエンドポイントデバイス間でメディアリダイレクトを実行するために必要な初期フレームワークを、複数のHDXマルチメディアサービスに提供します。
Citrix HDXブラウザリダイレクトサービス	"C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g BrowserRedirSvcs	このアカウント（ローカルサービス）	エンドポイントデバイスと仮想デスクトップ間でブラウザコンテンツリダイレクトを提供します。
Citrixポート転送サービス	"C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g PortFwdSvcs	このアカウント（ローカルサービス）	ブラウザコンテンツリダイレクトのために、エンドポイントデバイスと仮想デスクトップ間でポート転送を提供します。
Citrix HDX Teamsリダイレクトサービス	"C:\Program Files (x86)\Citrix\System3	ローカルシステムアカウント	エンドポイントデバイスと仮想デスクトップ間でMicrosoft

サービス	WINDOWS SERVER OSの実行可能ファイルへのパス	ログオンアカウント	説明
	2\CtxSvcHost.exe" -g TeamsSvcs		Teamsリダイレクトを提供します。

シトリックス ワークスペース™ アプリ

ユーザーのエンドポイントでは、Windows用Citrix WorkspaceアプリがHdxTeams.exeまたはHdxRtcEngine.exeという新しいサービスをインスタンス化します。これは、VDAでMicrosoft Teamsが起動し、ユーザーがセルフプレビューで通話しようとしたり、周辺機器にアクセスしようとしたりするときに行われます。このサービスが表示されない場合は、以下を確認してください。

1. Windows 用 Workspace アプリ バージョン 1905 以降がインストールされていることを確認します。Workspace アプリのインストールパスに HdxTeams.exe または HdxRtcEngine.exe と webrpc.dll バイナリが表示されますか？
2. 手順1を確認したら、HdxTeams.exe または HdxRtcEngine.exe が起動しているかどうかを確認するために、次の操作を行います。
    a. VDA 上の Microsoft Teams を終了します。
    b. VDA で services.msc を起動します。
    c. Citrix HDX Teams Redirection Service を停止します。
    d. ICA® セッションを切断します。
    e. ICA セッションを接続します。
    f. Citrix HDX Teams Redirection Service を開始します。
    g. Citrix HDX HTML5 Video Redirection Service を再起動します。
    h. VDA 上で Microsoft Teams を起動します。
3. クライアントエンドポイントで HdxTeams.exe または HdxRtcEngine.exe が起動しない場合は、次の操作を行います。
    a. VDA を再起動します。
    b. クライアントエンドポイントを再起動します。

サポート

Citrix と Microsoft は、Microsoft Teams の最適化を使用して、Citrix Virtual Apps and Desktops™ からの Microsoft Teams の配信を共同でサポートしています。この共同サポートは、両社の緊密な連携の成果です。有効なサポート契約があり、このソリューションで問題が発生した場合は、問

題の原因となっていると思われるコードのベンダーにサポートチケットをオープンしてください。つまり、Teams の場合は Microsoft、最適化コンポーネントの場合は Citrix です。 Citrix または Microsoft がチケットを受け取り、問題をトリアージし、必要に応じてエスカレートします。各社のサポートチームに連絡する必要はありません。

問題が発生した場合は、Teams UI で **>** をクリックすることをお勧めします。VDA 側のログは、技術的な問題をより迅速に解決するために、Citrix と Microsoft の間で自動的に共有されます。

ログの収集

HDXメディアエンジンログはユーザーのマシン上（VDA上ではない）にあります。問題が発生した場合は、サポートケースにログを添付してください。

Windowsログ：

Windowsログは、**HDXTeams**フォルダー内の%TEMP%にあります（AppData/Local/Temp/HDXTeamsまたはAppData/Local/Temp/HdxRtcEngine）。webrpc_Day_Month_timestamp_Year.txtという名前の.txtファイルを探してください。Citrix Workspaceアプリの新しいバージョン（Citrix Workspaceアプリ2009.5以降など）を使用している場合は、ログをAppData\Local\Temp\HdxRtcEngineに保存します。

各セッションはログ用の個別のフォルダーを作成します。

Macログ：

1. VDWEBRTCログ - 仮想チャネルの実行を記録します。

   場所：`/Users/<User Name>/Library/Logs/Citrix Workspace/CitrixViewer_<Y_M_D_H_M_S>.txt`

2. HdxRtcEngineログ - HdxRtcEngine上のプロセスの実行を記録します。

   場所: `$TMPDIR/hdxrtcengine/<W_M_D_H_M_S_Y>/hdxrtcengine.log`

   HdxRtcEngineログはデフォルトで有効になっています。

3. Webrpcログ - webrtcライブラリのラップアップの実行を記録する最も重要なログです。

   場所: `/Users/<USERNAME>/Library/Logs/HdxRtcEngine/<W_M_D_H_M_S_Y>/webrpc.log`

Linuxログ：

Linuxログは`/tmp/webrpc/<current date>/ and /tmp/hdxrtcengine/<current date>/`フォルダーにあります。 Webrtcログ：`/tmp/webrpc/<current date>/webrtc.log` カーネルログ：`/var/log/syslog`

ICE/STUN/TURN/ログ：

通話を確立する際には、次の4つのICEフェーズが必要です。

- 候補収集
- 候補交換
- 接続チェック (STUNバインド要求)
- 候補昇格

HdxRtcEngine.exeログでは、以下のエントリが関連するInteractive Connectivity Establishment (ICE) エントリです。これらのエントリは、通話設定が成功するために必要です。収集段階のサンプルスニペットを以下に示します。

```
RPCStubs Info: -> device id = \\?
\display#int3470#4&1835d135&0&uid13424#{65e8773d-8f56-11d0-
a3b9-00a0c9223196}\{bf89b5a5-61f7-4127-a279-e187013d7caf} label =
Microsoft Camera Front groupId =



webrtcapi.RTCPeerConnection Info: createOffer. audio = 1 video = 1

webrtcapi.RTCPeerConnection Info: setLocalDescription.

>>> begin:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
HaveLocalOffer



webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state = Gathering



[…]

>>> begin:sdp
```

```
candidate:840548147 1 udp 2122194687 10.108.124.215 56927 typ host
generation 0 ufrag oVk6 network-id 1

<<< end:sdp

[…]

>>> begin:sdp

candidate:1938109490 1 udp 24911871 52.114.xxx.xxx 52786 typ relay raddr
73.205.xxx.x rport 25651 generation 0 ufrag dDML network-id 1 network-cost
10

<<< end:sdp

[…]

>>> begin:sdp

candidate:4271145120 1 udp 1685987071 66.xxx.xxx.xxx 55839 typ srflx raddr
10.108.124.215 rport 55839 generation 0 ufrag uAVH network-id 1

<<< end:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state = Complete
webrtcapi.RTCPeerConnection Info: setRemoteDescription.

>>> begin:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
HaveRemotelOffer
```

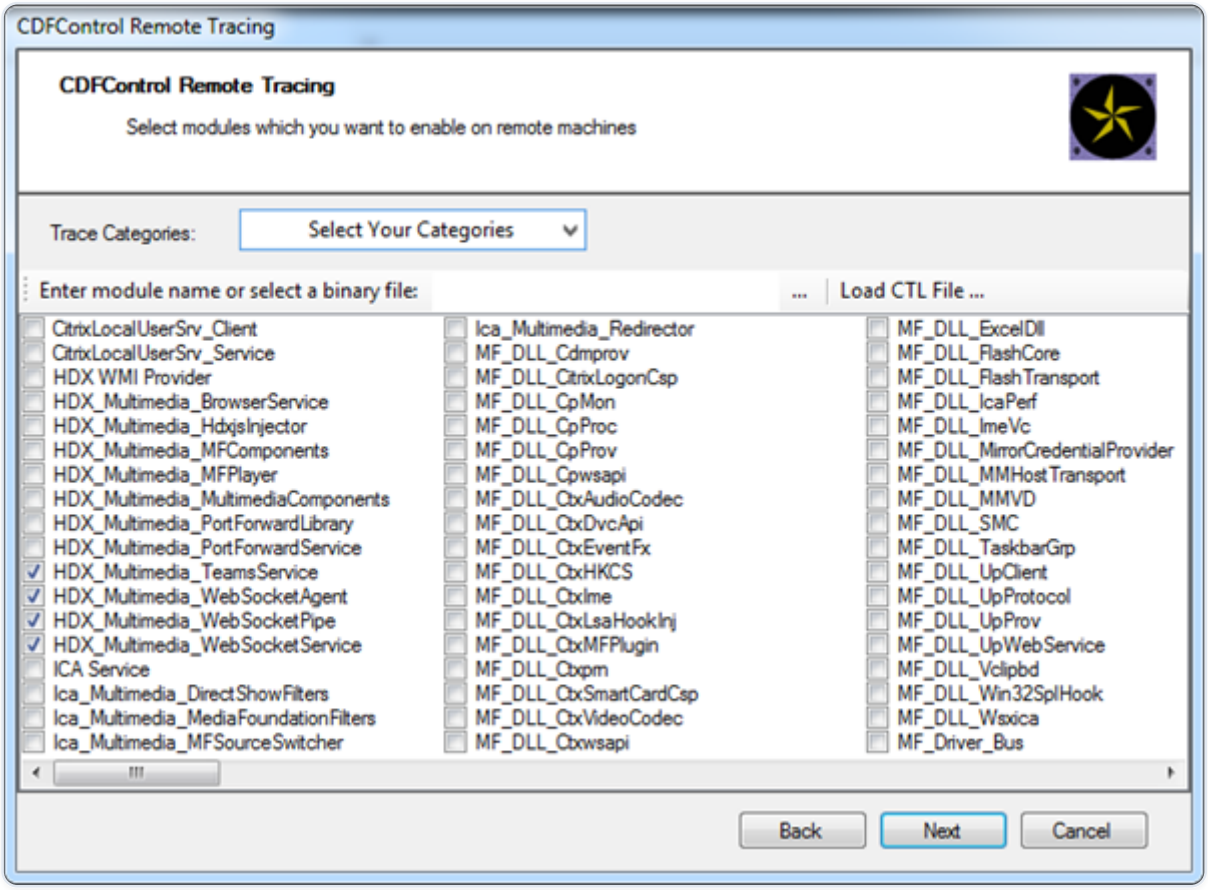
複数のICE候補がある場合、優先順位は次のとおりです。

1. ホスト
2. ピア反射型
3. サーバー反射型
4. トランスポートリレー

一貫して再現可能な問題が発生した場合は、Teamsで**ヘルプ > 問題の報告**をクリックすることをお勧めします。Microsoftでケースをオープンした場合、技術的な問題を解決するために、ログはCitrixとMicrosoftの間で共有されます。 Citrixサポートに連絡する前にCDFトレースをキャプチャすることも有益です。詳細については、Knowledge Centerの記事CDFcontrolを参照してください。

CDFトレース収集の推奨事項については、Knowledge Centerの記事Recommendations for Collecting the CDF Tracesを参照してください。

VDA側CDFトレース - 次のCDFトレースプロバイダーを有効にします。



Workspaceアプリ側CDFトレース - 次のCDFトレースプロバイダーを有効にします。

Workspace App 側の CDF トレース(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/team-cwa-cdf-traces.png)

- IcaClient_DriversVd_TeamsRedir (オプション)
- IcaClient_Multimedia_HdxTeams (Citrix Workspace app 2012 以降が必要)

Windows Media リダイレクト

Windows Media リダイレクトは、サーバーがストリーミングオーディオとビデオをユーザーに配信する方法を制御し、最適化します。メディアのランタイムファイルをサーバーではなくクライアントデバイスで再生することで、Windows Media リダイレクトは、マルチメディアファイルの再生に必要な帯域幅を削減します。Windows Media リダイレクトは、仮想Windowsデスクトップで実行されているWindows Media Playerおよび互換性のあるプレーヤーのパフォーマンスを向上させます。

Windows Media クライアント側コンテンツフェッチの要件が満たされない場合、メディア配信は自動的にサーバー側フェッチを使用します。この方法はユーザーには透過的です。使用されている方法を特定するには、Citrix Scoutを使用してHostMMTransport.dllからCitrix Diagnosis Facility (CDF) トレースを実行できます。詳しくは、「Citrix Scout」(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/manage-deployment/cis/scout.html)を参照してください。

Windows Media リダイレクトは、ホストサーバーでメディアパイプラインをインターセプトし、メディアデータをネイティブの圧縮形式でキャプチャし、コンテンツをクライアントデバイスにリダイレクトします。クライアントデバイスは、ホストサーバーから受信したメディアデータを解凍してレンダリングするために、メディアパイプラインを再構築します。Windows Media リダイレクトは、Windowsオペレーティングシステムを実行しているクライアントデバイスでうまく機能します。これらのデバイスには、ホストサーバーに存在していたメディアパイプラインを再構築するために必要なマルチメディアフレームワークがあります。Linuxクライアントは、同様のオープンソースメディアフレームワークを使用してメディアパイプラインを再構築します。

ポリシー設定の**Windows Media リダイレクト**は、この機能を制御し、デフォルトで**許可**されています。通常、この設定により、サーバーからレンダリングされるオーディオおよびビデオの品質が、クライアントデバイスでローカルに再生されるコンテンツに匹敵するレベルに向上します。まれに、Windows Media リダイレクトを使用して再生されるメディアが、基本的なICA®圧縮と通常のオーディオを使用してレンダリングされるメディアよりも悪く見えることがあります。この機能を無効にするには、**Windows Media リダイレクト**設定をポリシーに追加し、その値を**禁止**に設定します。

ポリシー設定について詳しくは、「マルチメディアポリシー設定」(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/policies/reference/ica-policy-settings/multimedia-policy-settings.html)を参照してください。

制限事項:

セッション内でWindows Media PlayerとRemote Audio & Video Extensions (RAVE) を有効にしている場合、黒い画面が表示されることがあります。この黒い画面は、ビデオコンテンツを右クリックして**常に「再生中」を最前面に表示**を選択した場合に表示されることがあります。

一般的なコンテンツリダイレクト

コンテンツリダイレクトを使用すると、ユーザーがサーバーで公開されているアプリケーションを使用するか、ユーザーデバイスでローカルに実行されているアプリケーションを使用するかによって、情報にアクセスする方法を制御できます。

クライアントフォルダーリダイレクト(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/general-content-redirection/client-folder-redirection.html)

クライアントフォルダーリダイレクトは、クライアント側のファイルがホスト側のセッションでアクセス可能になる方法を変更します。

- サーバーでクライアントドライブマッピングのみを有効にすると、クライアント側のフルボリュームは、Universal Naming Convention (UNC) リンクとしてセッションに自動的にマッピングされます。
- サーバーでクライアントフォルダーリダイレクトを有効にし、ユーザーがWindowsデスクトップデバイスでそれを構成すると、ユーザーが指定したローカルボリュームの一部がリダイレクトされます。

ホストからクライアントへのリダイレクト(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/general-content-redirection/host-to-client-redirection.html)

特定のまれなユースケースでは、ホストからクライアントへのリダイレクトの使用を検討してください。通常、他の形式のコンテンツリダイレクトの方が優れている場合があります。このタイプのリダイレクトは、マルチセッションOS VDAでのみサポートされており、シングルセッションOS VDAではサポートされていません。

ローカルアプリアクセスとURLリダイレクト(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/general-content-redirection/laa-url-redirect.html)

ローカルアプリアクセスは、ローカルにインストールされたWindowsアプリケーションをホストされたデスクトップ環境にシームレスに統合します。これは、あるコンピューターから別のコンピューターに切り替えることなく行われます。

HDX™テクノロジーは、最適化されたサポートがない、または不適切な特殊デバイス向けに**汎用USBリダイレクト**を提供します。

クライアントフォルダーリダイレクト

クライアントフォルダーリダイレクトは、クライアント側のファイルがホスト側のセッションでアクセスされる方法を変更します。サーバーでクライアントドライブマッピングのみを有効にすると、クライアント側の完全なボリュームは、Universal Naming Convention (UNC) リンクとしてセッションに自動的にマッピングされます。サーバーでクライアントフォルダーリダイレクトを有効にし、ユーザーがユーザーデバイスでそれを構成すると、ユーザーが指定したローカルボリュームの一部がリダイレクトされます。

ユーザーが指定したフォルダーのみが、セッション内でUNCリンクとして表示されます。つまり、ユーザーデバイス上の完全なファイルシステムではなく、指定されたフォルダーのみが表示されます。レジストリを介してUNCリンクを無効にすると、クライアントフォルダーはセッション内でマップされたドライブとして表示されます。

クライアントフォルダーリダイレクトは、WindowsシングルセッションOSマシンでのみサポートされています。

外部USBドライブのクライアントフォルダーリダイレクトは、デバイスの取り外しと再接続時に保存されません。

サーバーでクライアントフォルダーリダイレクトを有効にします。次に、クライアントデバイスで、リダイレクトするフォルダーを指定します。クライアントフォルダーオプションを指定するために使用するアプリケーションは、このリリースで提供されるCitrix Workspace™アプリに含まれています。

要件:

サーバーの場合:

- ウィンドウズ サーバー 2022
- Windows Server 2019、StandardおよびDatacenterエディション
- Windows Server 2016、StandardおよびDatacenterエディション
- Windows Server 2012 R2、StandardおよびDatacenterエディション

クライアントの場合:

- Windows 10、32ビットおよび64ビットエディション (最小バージョン1607)
- Windows 8.1、32ビットおよび64ビットエディション (Embeddedエディションを含む)
- Windows 7、32ビットおよび64ビットエディション (Embeddedエディションを含む)

サーバーでクライアントフォルダーリダイレクトを有効にするには、レジストリを介して管理される機能のリストにあるクライアントフォルダーリダイレクトを参照してください。

ユーザーデバイスで、リダイレクトするフォルダーを指定します:

1. 最新バージョンのCitrix Workspaceアプリがインストールされていることを確認してください。
2. Citrix Workspaceアプリのインストールディレクトリから、CtxCFRUI.exeを起動します。
3. **Custom** ラジオボタンを選択し、フォルダーを追加、編集、または削除します。
4. 設定を有効にするには、セッションを切断して再接続します。

ホストからクライアントへのリダイレクト

ホストからクライアントへのリダイレクトを使用すると、Citrix®セッションで実行されているアプリケーションにハイパーリンクとして埋め込まれたURLを、ユーザーエンドポイントデバイス上の対応するアプリケーションを使用して開くことができます。ホストからクライアントへのリダイレクトの一般的なユースケースには、次のようなものがあります。

- Citrixサーバーがソースへのインターネットまたはネットワークアクセスを持たない場合のWebサイトのリダイレクト。
- セキュリティ、パフォーマンス、互換性、またはスケーラビリティの理由から、Citrixセッション内でWebブラウザを実行することが望ましくない場合のWebサイトのリダイレクト。
- URLを開くために必要なアプリケーションがCitrixサーバーにインストールされていない場合の特定のURLタイプのリダイレクト。

ホストからクライアントへのリダイレクトは、Citrixセッションで実行されているWebブラウザーのアドレスバーでアクセスまたは入力するURLを対象としていません。WebブラウザーでのURLのリダイレクトについては、「双方向URLリダイレクト」または「ブラウザーコンテンツリダイレクト」を参照してください。

システム要件

- マルチセッションOS VDA
- サポートされているクライアント：
  - Windows向けCitrix Workspace™アプリ
  - Mac向けCitrix Workspaceアプリ
  - Linux向け Citrix Workspace アプリ

- HTML5向けCitrix Workspaceアプリ
- Chrome向けCitrix Workspaceアプリ

クライアントデバイスには、URLタイプのリダイレクトを処理するためのアプリケーションがインストールされ、構成されている必要があります。

構成

この機能を有効にするには、ホストからクライアントへのリダイレクト Citrixポリシーを使用します。**ホストからクライアントへのリダイレクト**は、デフォルトで無効になっています。ホストからクライアントへのリダイレクトポリシーを有効にすると、Citrix Launcherアプリケーションが Windowsサーバーに登録され、URLをインターセプトしてクライアントデバイスに送信できるようになります。

次に、必要なURLタイプのデフォルトアプリケーションとしてCitrix Launcherを使用するように Windowsグループポリシーを構成する必要があります。CitrixサーバーVDAで、 ServerFTAdefaultPolicy.xmlファイルを作成し、次のXMLコードを挿入します。

```
<?xml version="1.0" encoding="UTF-8"?>



<DefaultAssociations>



<Association Identifier="http" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />



<Association Identifier="https" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />



</DefaultAssociations>
```

グループポリシー管理コンソールから、**コンピューターの構成 > 管理用テンプレート > Windows コンポーネント > エクスプローラー > 既定の関連付け構成ファイルを設定する** に移動し、 ServerFTAdefaultPolicy.xmlファイルを保存します。

> **注：**

> Citrixサーバーにグループポリシー設定がない場合、WindowsはURLを開くためのアプリケーションを選択するようユーザーに促します。

> デフォルトでは、次のURLタイプのリダイレクトをサポートしています。

- HTTP
- HTTPS
- RTSP
- RTSPU
- PNM
- MMS

リダイレクト用のリストに、追加の標準またはカスタムURLタイプを含めるには、以前に参照したServerFTAdefaultPolicy.xmlファイルに新しい**Association Identifier**行を作成します。例：

```
<Association Identifier="ftp" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

```
<Association Identifier="mailto" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

```
<Association Identifier="customtype1" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

```
<Association Identifier="customtype2" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

リストにURLタイプを追加するには、クライアント構成も必要です。Windowsクライアントで以下のレジストリキーと値を作成します。

> **注：**

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

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

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA
- 値の名前: ExtraURLProtocols
- 値の型: REG_SZ
- 値のデータ: 必要なURLタイプをセミコロンで区切って指定します。URLのオーソリティ部分より前のすべてを含めます。例： `ftp://;mailto:;customtype1://;custometype2://`

URLタイプはWindowsクライアントにのみ追加できます。上記のレジストリ設定がないクライアントは、Citrixセッションへのリダイレクトを拒否します。クライアントには、指定されたURLタイプを処理するようにインストールおよび構成されたアプリケーションが必要です。

デフォルトのリダイレクトリストからURLタイプを削除するには、サーバーVDAで以下のレジストリキーと値を作成します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- 値の名前: DisableServerFTA
- 値の型: DWORD
- 値のデータ: 1
- 値の名前: NoRedirectClasses
- 値の型: REG_MULTI_SZ
- 値のデータ: 次の値の任意の組み合わせを指定します: `http`、`https`、`rtsp`、`rtspu`、`pnm`、または `mms`。複数の値を別々の行に入力します。例:

`http`

`https`

`rtsp`

特定のWebサイトでホストからクライアントへのリダイレクトを有効にするには、サーバーVDAにレジストリキーと値を作成します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- 値の名前: ValidSites
- 値の型: REG_MULTI_SZ

- 値のデータ: 完全修飾ドメイン名 (FQDN) の任意の組み合わせを指定します。複数のFQDNを別々の行に入力します。プロトコル (`http://` または `https://`) を含めず、FQDNのみを含めます。FQDNには、アスタリスク (`*`) をワイルドカード文字として左端の位置にのみ含めることができます。このワイルドカードは、RFC 6125のルールに準拠した単一レベルのドメインに一致します。例:

`www.exmaple.com`

`*.example.com`

> **注：**
>
> **ValidSites** キーを **DisableServerFTA** および **NoRedirectClasses** キーと組み合わせて使用することはできません。

サーバーVDAのデフォルトブラウザ構成

このセクションで参照されているホストからクライアントへのリダイレクトを有効にすると、サーバーVDA上の以前のデフォルトブラウザー構成がすべて上書きされます。Web URLがリダイレクトされない場合、Citrix LauncherはURLを `command_backup` レジストリキーで構成されたブラウザーに渡します。このキーはデフォルトでInternet Explorerを指していますが、別のブラウザーへのパスを含むように変更できます。詳しくは、レジストリで管理される機能のリストにある「サーバーVDAのデフォルトブラウザー構成」を参照してください。

双方向コンテンツリダイレクト

双方向コンテンツリダイレクトにより、Webブラウザー内のHTTPまたはHTTPS URL、あるいはアプリケーションに埋め込まれたURLを、Citrix VDAセッションとクライアントエンドポイント間で双方向に転送できます。Citrixセッションで実行されているブラウザーに入力されたURLは、クライアントのデフォルトブラウザーを使用して開くことができます。逆に、クライアントで実行されているブラウザーに入力されたURLは、公開アプリケーションまたはデスクトップのいずれかを使用して、Citrixセッションで開くことができます。双方向コンテンツリダイレクトの一般的なユースケースには、次のようなものがあります。

- 開始ブラウザーがソースへのネットワークアクセスを持たない場合のWeb URLのリダイレクト。
- ブラウザーの互換性およびセキュリティ上の理由によるWeb URLのリダイレクト。

- Citrixセッションまたはクライアントでwebブラウザーを実行したくない場合に、アプリケーションに埋め込まれたWeb URLのリダイレクト。

システム要件

- シングルセッションまたはマルチセッションOS VDA
- Windows向けCitrix Workspace™アプリ

ブラウザー：

- インターネット エクスプローラー 11
- Citrix Browser Redirection Extension が組み込まれた Google Chrome (Google Chrome Web Store で入手できます)
- Citrix Browser Redirection Extension が組み込まれた Microsoft Edge (Chromium) (Google Chrome Web Store で入手できます)

構成

リダイレクトを機能させるには、VDAとクライアントの両方でCitrixポリシーを使用して双方向コンテンツリダイレクトを有効にする必要があります。双方向コンテンツリダイレクトはデフォルトで無効になっています。

VDA構成については、ICAポリシー設定の双方向コンテンツリダイレクトを参照してください。

クライアント構成については、Citrix Workspaceアプリ for Windowsドキュメントの双方向コンテンツリダイレクトを参照してください。

ブラウザ拡張機能は、表示されているコマンドを使用して登録する必要があります。使用しているブラウザに基づいて、VDAおよびクライアントで必要に応じてコマンドを実行してください。

VDAにブラウザ拡張機能を登録するには、コマンドプロンプトを開きます。次に、表示されている例のように、必要なブラウザオプションを指定して`%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe`を実行します。

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regIE
```

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regChrome
```

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regEdge
```

すべての利用可能なブラウザに拡張機能を登録するには、以下を実行します。

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regall
```

ブラウザ拡張機能を登録解除するには、表示されている例のように`/unreg<browser>`オプションを使用します。

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /unregIE
```

クライアントにブラウザ拡張機能を登録するには、コマンドプロンプトを開き、表示されている例と同じオプションで`%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe`を実行します。

> **注：**
>
> 登録コマンドを実行すると、ChromeおよびEdgeブラウザは初回起動時にCitrix Browser Redirection Extensionを有効にするようユーザーに促します。ブラウザ拡張機能は、Google Chrome Web Storeから手動でインストールすることもできます。

Citrix VDAからクライアントへのワイルドカードリダイレクト

双方向コンテンツリダイレクトは、リダイレクトするURLを定義する際にワイルドカードの使用をサポートします。双方向コンテンツリダイレクトを構成するには、構成の手順を参照してください。

Citrix Studioで、**Allowed URLs to be redirected to Client** にワイルドカードURLを設定します。アスタリスク (*) がワイルドカード文字です。

> **注：**
>
> - クライアントポリシーで **Allowed URLs to be redirected to VDA** を設定しないでください。無限リダイレクトループを避けるために、サイトが **Allowed URLs to be redirected to VDA** を設定していることを確認してください。
> - トップレベルドメインはサポートされていません。たとえば、`https://www.citrix.*` や `http://www.citrix.co*` はリダイレクトされません。

その他の考慮事項

- ブラウザーの要件と構成は、リダイレクトを開始するブラウザーにのみ適用されます。リダイレクトが成功した後にURLが開かれる宛先ブラウザーは、サポートの対象とはなりません。VDAからクライアントにURLをリダイレクトする場合、サポートされるブラウザー構成はVDA

上でのみ必要です。逆に、クライアントからVDAにURLをリダイレクトする場合、サポートされるブラウザー構成はクライアント上でのみ必要です。リダイレクトされたURLは、方向に応じて、クライアントまたはVDAのいずれかの宛先マシンで構成されたデフォルトのブラウザーに渡されます。VDAとクライアントで同じブラウザータイプを使用する必要はありません。

- リダイレクトルールがループ構成にならないことを確認してください。たとえば、VDAポリシーが `https://www.citrix.com` をリダイレクトするように設定され、クライアントポリシーが同じURLをリダイレクトするように設定されている場合、無限ループが発生します。
- HTTP/HTTPSプロトコルのURLのみがサポートされています。URL短縮サービスはサポートされていません。
- クライアントからVDAへのリダイレクトには、Windowsクライアントを管理者権限でインストールする必要があります。
- 宛先ブラウザがすでに開いている場合、リダイレクトされたURLは新しいタブで開きます。そうでない場合、URLは新しいブラウザウィンドウで開きます。
- 双方向コンテンツリダイレクトは、ローカルアプリアクセス (LAA) が有効になっている場合は機能しません。

ローカルアプリアクセスとURLリダイレクト

はじめに

Local App Accessは、ローカルにインストールされたWindowsアプリケーションを、デスクトップを切り替えることなくホストされたデスクトップ環境にシームレスに統合します。Local App Accessを使用すると、次のことが可能になります。

- 物理的なラップトップ、PC、またはその他のデバイスにローカルにインストールされているアプリケーションに、仮想デスクトップから直接アクセスできます。
- 柔軟なアプリケーション配信ソリューションを提供します。仮想化できない、またはIT部門が保守していないローカルアプリケーションをユーザーが持っている場合でも、それらのアプリケーションは仮想デスクトップにインストールされているかのように動作します。
- アプリケーションが仮想デスクトップとは別にホストされている場合のダブルホップの遅延を解消します。これを行うには、公開されたアプリケーションへのショートカットをユーザーのWindowsデバイスに配置します。
- 次のようなアプリケーションを使用します。
  - GoToMeetingなどのビデオ会議ソフトウェア。
  - まだ仮想化されていない特殊なアプリケーションまたはニッチなアプリケーション。

    - そうでなければ、ユーザーデバイスからサーバーへ、そしてサーバーからユーザーデバイスへと大量のデータを転送するようなアプリケーションと周辺機器。たとえば、DVDバーナーやTVチューナーなど。

Citrix Virtual Apps and Desktops™では、ホストされたデスクトップセッションは、URLリダイレクトを使用してLocal App Accessアプリケーションを起動します。URLリダイレクトにより、アプリケーションは複数のURLアドレスで利用可能になります。デスクトップセッション内のブラウザで埋め込みリンクを選択することにより、ローカルブラウザ（ブラウザのURLブロックリストに基づく）を起動します。ブロックリストにないURLに移動すると、そのURLはデスクトップセッションで再度開かれます。

URLリダイレクトはデスクトップセッションでのみ機能し、アプリケーションセッションでは機能しません。アプリケーションセッションで使用できる唯一のリダイレクト機能は、ホストからクライアントへのコンテンツリダイレクトです。これは、サーバーFTA（ファイルタイプ関連付け）リダイレクトの一種です。このFTAは、HTTP、HTTPS、RTSP、MMSなどの特定のプロトコルをクライアントにリダイレクトします。たとえば、HTTPで埋め込みリンクのみを開く場合、リンクはクライアントアプリケーションで直接開かれます。URLブロックリストまたは許可リストのサポートはありません。

Local App Accessが有効になっている場合、ローカルで実行されているアプリケーション、ユーザーがホストするアプリケーションからのリンクとして、またはデスクトップ上のショートカットとしてユーザーに表示されるURLは、次のいずれかの方法でリダイレクトされます。

- ユーザーのコンピューターからホストされたデスクトップへ
- Citrix Virtual Apps and Desktopsサーバーからユーザーのコンピューターへ
- 起動された環境でレンダリングされる（リダイレクトされない）

特定のWebサイトからのコンテンツのリダイレクトパスを指定するには、Virtual Delivery AgentでURL許可リストとURLブロックリストを構成します。これらのリストには、URLリダイレクトポリシー設定を指定する複数文字列のレジストリキーが含まれています。詳細については、「ローカルアプリアクセス ポリシー設定」を参照してください。

URLは、以下の例外を除き、VDAでレンダリングできます。

- 地域/ロケール情報 — msn.comやnews.google.comなど、ロケール情報を必要とするWebサイト（地域に基づいて国固有のページを開きます）。たとえば、VDAが英国のデータセンターからプロビジョニングされ、クライアントがインドから接続している場合、ユーザーはin.msn.comが表示されることを期待しますが、実際にはuk.msn.comが表示されます。
- マルチメディアコンテンツ — リッチメディアコンテンツを含むWebサイトは、クライアントデバイスでレンダリングされると、エンドユーザーにネイティブなエクスペリエンスを提供

し、高遅延ネットワークでも帯域幅を節約します。この機能は、Silverlightなどの他のメディアタイプを含むサイトをリダイレクトします。このプロセスは安全な環境で行われます。つまり、管理者が承認したURLはクライアントで実行され、残りのURLはVDAにリダイレクトされます。

URLリダイレクトに加えて、FTAリダイレクトを使用できます。FTAは、セッション内でファイルが検出されたときにローカルアプリケーションを起動します。ローカルアプリが起動された場合、そのローカルアプリはファイルを開くためにファイルへのアクセス権を持っている必要があります。したがって、ローカルアプリケーションを使用して開くことができるファイルは、ネットワーク共有上またはクライアントドライブ上（クライアントドライブマッピングを使用）にあるファイルのみです。たとえば、PDFファイルを開く際に、PDFリーダーがローカルアプリである場合、そのPDFリーダーを使用してファイルが開かれます。ローカルアプリはファイルに直接アクセスできるため、ファイルを開くためのICA®を介したネットワーク転送は発生しません。

要件、考慮事項、および制限事項

WindowsマルチセッションOS用VDAおよびWindowsシングルセッションOS用VDAの有効なオペレーティングシステムで、ローカルアプリアクセスをサポートしています。ローカルアプリアクセスには、Citrix Workspaceアプリ for Windowsバージョン4.1（最小）が必要です。以下のブラウザーがサポートされています。

- Edge、最新バージョン
- Firefox、最新バージョンおよび延長サポートリリース
- Chrome、最新バージョン

ローカルアプリアクセスとURLリダイレクトを使用する際の以下の考慮事項と制限事項を確認してください。

- ローカルアプリアクセスは、すべてのモニターにまたがる全画面の仮想デスクトップ向けに設計されています。
    - ウィンドウモードで実行される仮想デスクトップや、すべてのモニターをカバーしない仮想デスクトップでローカルアプリアクセスを使用すると、ユーザーエクスペリエンスが混乱する可能性があります。
    - 複数モニター — 1つのモニターが最大化されると、そのセッションで起動されたすべてのアプリケーションのデフォルトデスクトップになります。このデフォルトは、後続のアプリケーションが通常別のモニターで起動される場合でも発生します。
    - この機能は1つのVDAをサポートします。複数の同時VDAとの統合はありません。
- 一部のアプリケーションは予期しない動作をし、ユーザーに影響を与える可能性があります。

- ドライブ文字は、仮想デスクトップのC:ドライブではなくローカルのC:ドライブのように表示されるため、ユーザーを混乱させる可能性があります。
- 仮想デスクトップで利用可能なプリンターは、ローカルアプリケーションでは利用できません。
- 昇格された権限を必要とするアプリケーションは、クライアントホスト型アプリケーションとして起動できません。
- シングルインスタンスアプリケーション（Windows Media Playerなど）に対する特別な処理はありません。
- ローカルアプリケーションは、ローカルマシンのWindowsテーマで表示されます。
- 全画面表示アプリケーションはサポートされていません。これには、PowerPointのスライドショーやデスクトップ全体を覆うフォトビューアーなど、全画面で開くアプリケーションが含まれます。
- ローカルアプリアクセスは、ローカルアプリケーションのプロパティ（クライアントのデスクトップやスタートメニューのショートカットなど）をVDAにコピーします。ただし、ショートカットキーや読み取り専用属性などの他のプロパティはコピーしません。
- 重なり合うウィンドウの順序の処理方法をカスタマイズするアプリケーションは、予期しない結果をもたらす可能性があります。たとえば、一部のウィンドウが非表示になることがあります。
- マイコンピューター、ごみ箱、コントロールパネル、ネットワークドライブのショートカット、フォルダーのショートカットなど、ショートカットはサポートされていません。
- 次のファイルの種類とファイルはサポートされていません：カスタムファイルの種類、関連付けられたプログラムがないファイル、zipファイル、隠しファイル。
- 32ビットと64ビットのクライアントホスト型またはVDAアプリケーションが混在している場合、タスクバーのグループ化はサポートされていません。つまり、32ビットのローカルアプリケーションと64ビットのVDAアプリケーションをグループ化することはできません。
- COMを使用してアプリケーションを起動することはできません。たとえば、Officeアプリケーション内から埋め込みOfficeドキュメントをクリックした場合、プロセスの起動が検出されず、ローカルアプリケーションの統合は失敗します。

- ユーザーが別の仮想デスクトップセッション内から仮想デスクトップを起動するダブルホップシナリオはサポートされていません。
- URLリダイレクトは明示的なURL（つまり、ブラウザのアドレスバーに表示されるURL、またはブラウザに応じてブラウザ内ナビゲーションを使用して見つかるURL）のみをサポートします。

- URLリダイレクトはデスクトップセッションでのみ機能し、アプリケーションセッションでは機能しません。
- VDAセッションのローカルデスクトップフォルダーでは、ユーザーはファイルを作成できません。
- ローカルで実行されているアプリケーションの複数のインスタンスは、仮想デスクトップ用に設定されたタスクバー設定に従って動作します。ただし、ローカルで実行されているアプリケーションへのショートカットは、それらのアプリケーションの実行中のインスタンスとグループ化されません。また、ホストされたアプリケーションの実行中のインスタンスや、ホストされたアプリケーションへのピン留めされたショートカットともグループ化されません。ユーザーは、タスクバーからローカルで実行されているアプリケーションのウィンドウのみを閉じることができます。ユーザーはローカルアプリケーションウィンドウをデスクトップのタスクバーやスタートメニューにピン留めできますが、これらのショートカットを使用するとアプリケーションが常に起動するとは限りません。
- **ローカルアプリアクセスを許可**ポリシー設定を**有効**に設定した場合、ブラウザーコンテンツリダイレクトはサポートされません。デフォルトでは、ローカルアプリアクセスは禁止されています。

Windowsとの連携

ローカルアプリアクセスとWindowsとの連携には、次の動作が含まれます。

- Windows 8およびWindows Server 2012のショートカットの動作
  - クライアントにインストールされているWindowsストアアプリケーションは、ローカルアプリアクセスのショートカットの一部として列挙されません。
  - 画像ファイルとビデオファイルは、デフォルトでWindowsストアアプリケーションを使用して開かれます。ただし、ローカルアプリアクセスはWindowsストアアプリケーションを列挙し、デスクトップアプリケーションでショートカットを開きます。
- ローカルプログラム
  - Windows 7の場合、フォルダーはスタートメニューで利用できます。
  - Windows 8の場合、ローカルプログラムは、ユーザーがスタート画面からカテゴリとして**すべてのアプリ**を選択した場合にのみ利用できます。すべてのサブフォルダーがローカルプログラムに表示されるわけではありません。
- アプリケーション向けのWindows 8グラフィック機能

  - デスクトップアプリケーションはデスクトップ領域に制限されており、スタート画面およびWindows 8スタイルのアプリケーションによって覆われます。
  - ローカルアプリアクセスアプリケーションは、マルチモニターモードではデスクトップアプリケーションのように動作しません。マルチモニターモードでは、スタート画面とデスクトップが異なるモニターに表示されます。

- Windows 8とローカルアプリアクセスURLリダイレクト
  - Windows 8のInternet Explorerではアドオンが有効になっていないため、URLリダイレクトを有効にするにはデスクトップ版Internet Explorerを使用してください。
  - Windows Server 2012では、Internet Explorerはデフォルトでアドオンを無効にします。URLリダイレクトを実装するには、Internet Explorerの拡張構成を無効にします。その後、Internet Explorerのオプションをリセットして再起動し、標準ユーザー向けにアドオンが有効になっていることを確認します。

ローカルアプリアクセスとURLリダイレクトの構成

Citrix Workspace™アプリでローカルアプリアクセスとURLリダイレクトを使用するには：

- ローカルクライアントマシンにCitrix Workspaceアプリをインストールします。Citrix Workspaceアプリのインストール中に両方の機能を有効にするか、グループポリシーエディターを使用してローカルアプリアクセステンプレートを有効にすることができます。
- **ローカルアプリアクセスを許可**ポリシー設定を**有効**に設定します。URLリダイレクトのURL許可リストおよびブロックリストポリシー設定も構成できます。詳しくは、「ローカルアプリアクセス ポリシー設定」を参照してください。

ローカルアプリアクセスとURLリダイレクトを有効にする

すべてのローカルアプリケーションでローカルアプリアクセスを有効にするには、次の手順に従います。

1. Citrix Studio を起動します。
   - オンプレミス展開の場合、**スタートメニュー**から**Citrix Studio**を開きます。
   - クラウドサービス展開の場合、**Citrix Cloud™ > Virtual Apps and Desktops service > 管理**タブに移動します。
2. Studio ナビゲーションペインで、**ポリシー**をクリックします。
3. 操作ペインで、**ポリシーの作成**をクリックします。

4. ポリシーの作成ウィンドウで、検索ボックスに「Allow Local App Access」と入力し、**選択**をクリックします。
5. 設定の編集ウィンドウで、**許可**を選択します。デフォルトでは、**ローカルアプリアクセスを許可**ポリシーは禁止されています。この設定が許可されている場合、VDAは、公開アプリケーションとローカルアプリアクセスのショートカットをセッションで有効にするかどうかをエンドユーザーが決定できるようにします。（この設定が禁止されている場合、公開アプリケーションとローカルアプリアクセスのショートカットの両方がVDAで機能しません。）このポリシー設定は、マシン全体とURLリダイレクトポリシーに適用されます。
6. ポリシーの作成ウィンドウで、検索ボックスに「URL redirection allow list」と入力し、**選択**をクリックします。URLリダイレクト許可リストは、リモートセッションのデフォルトブラウザーで開くURLを指定します。
7. 「設定の編集」ウィンドウで、「**追加**」をクリックしてURLを追加し、「**OK**」をクリックします。
8. 「ポリシーの作成」ウィンドウで、検索ボックスに「URL redirection block list」と入力し、「**選択**」をクリックします。URLリダイレクトブロックリストは、エンドポイントで実行されているデフォルトのブラウザーにリダイレクトされるURLを指定します。
9. 「設定の編集」ウィンドウで、「**追加**」をクリックしてURLを追加し、「**OK**」をクリックします。
10. 「設定」ページで、「**次へ**」をクリックします。
11. 「ユーザーとマシン」ページで、該当するデリバリーグループにポリシーを割り当て、「**次へ**」をクリックします。
12. 「概要」ページで設定を確認し、「**完了**」をクリックします。

Citrix Workspaceアプリのインストール中にすべてのローカルアプリケーションでURLリダイレクトを有効にするには、次の手順に従います。

1. マシン上のすべてのユーザーに対してCitrix Workspaceアプリをインストールするときに、URLリダイレクトを有効にします。これにより、URLリダイレクトに必要なブラウザーアドオンも登録されます。
2. コマンドプロンプトから、以下のいずれかのオプションを使用してCitrix Workspaceアプリをインストールするための適切なコマンドを実行します。

   - CitrixReceiver.exeの場合は、`/ALLOW_CLIENTHOSTEDAPPSURL=1`を使用します。
   - CitrixReceiverWeb.exeの場合は、`/ALLOW_CLIENTHOSTEDAPPSURL=1`を使用します。

グループポリシーエディターを使用してローカルアプリアクセス テンプレートを有効にする

注：

- グループポリシーエディターを使用してローカルアプリアクセステンプレートを有効にする前に、receiver.admx/adml テンプレートファイルをローカル GPO に追加します。詳細については、「グループポリシーオブジェクト管理用テンプレートの構成」を参照してください。
- Windows向けCitrix Workspaceアプリのテンプレートファイルは、CitrixBase.admx/CitrixBase.admlを%systemroot%\policyDefinitionsフォルダーに追加した場合にのみ、ローカルGPOの**管理用テンプレート > Citrixコンポーネント > Citrix Workspace**フォルダーで利用できます。

グループポリシーエディターを使用してローカルアプリアクセス テンプレートを有効にするには、次の手順に従います。

1. **gpedit.msc**を実行します。
2. **コンピューターの構成 > 管理用テンプレート > クラシック管理用テンプレート (ADM) > Citrix Components > Citrix Workspace > ユーザーエクスペリエンス**に移動します。
3. **ローカルアプリアクセス設定**をクリックします。
4. **有効**を選択し、**URLリダイレクトを許可**を選択します。URLリダイレクトの場合、この記事の後半にある「*ブラウザーアドオンの登録*」セクションで説明されているコマンドラインを使用して、ブラウザーアドオンを登録します。

公開アプリケーションのみにアクセスを提供する

レジストリエディターまたはPowerShell SDKを使用して、公開アプリケーションへのアクセスを提供できます。

レジストリエディターについては、レジストリを介して管理される機能のリストにある「公開アプリケーションのローカルアプリアクセス」を参照してください。

PowerShell SDKを使用するには：

1. Delivery Controller™が実行されているマシンでPowerShellを開きます。

2. 次のコマンドを入力します: `set-configsitemetadata -name "studio_clientHostedAppsEnabled" -value "true"`。

クラウドサービス展開で**ローカルアプリアクセスアプリケーションの追加**にアクセスするには、Citrix DaaS Remote PowerShell SDKを使用します。詳しくは、「Citrix DaaS Remote PowerShell SDK」を参照してください。

1. インストーラーをダウンロードします:

   `<https://download.apps.cloud.com/CitrixPoshSdk.exe>`

2. 次のコマンドを実行します:

   a. `asnp citrix.*`.

   b. `Get-XdAuthentication`

3. 次のコマンドを入力します: `set-configsitemetadata -name “studio_clientHostedAppsEnabled” -value “true”`。

該当する前の手順を完了したら、以下の手順に従って続行します。

1. **スタート**メニューから**Citrix Studio**を開きます。
2. Studio ナビゲーションペインで、**アプリケーション**をクリックします。
3. 上部中央のペインで、空白の領域を右クリックし、コンテキストメニューから**ローカルアプリアクセスアプリケーションの追加**を選択します。操作ペインで**ローカルアプリアクセスアプリケーションの追加**をクリックすることもできます。操作ペインにローカルアプリアクセスアプリケーションの追加オプションを表示するには、**更新**をクリックします。
4. ローカルアプリアクセスアプリケーションを公開します。

   - ローカルアプリケーションアクセスウィザードが起動し、紹介ページが表示されます。このページは、今後のウィザードの起動時に表示しないように設定できます。
   - ウィザードは、以下で説明するグループ、場所、識別、配信、および概要の各ページを案内します。各ページの作業が完了したら、概要ページに到達するまで**次へ**をクリックします。
   - グループページで、新しいアプリケーションを追加するデリバリーグループを1つ以上選択し、**次へ**をクリックします。
   - 場所ページで、ユーザーのローカルマシン上のアプリケーションの完全な実行可能パスと、アプリケーションが配置されているフォルダーへのパスを入力します。Citrixでは、システム環境変数パスを使用することをお勧めします。例: %ProgramFiles(x86)%\Internet Explorer\iexplore.exe。

- 識別ページで、デフォルト値を受け入れるか、必要な情報を入力してから**次へ**をクリックします。
- ページで、このアプリケーションをユーザーに配信する方法を構成し、**次へ**をクリックします。選択したアプリケーションのアイコンを指定できます。また、仮想デスクトップ上のローカルアプリケーションへのショートカットを、スタートメニュー、デスクトップ、またはその両方に表示するかどうかを指定できます。
- 概要ページで設定を確認し、**完了**をクリックしてローカルアプリケーションアクセスウィザードを終了します。

ブラウザアドオンを登録する

> **注：**
>
> URLリダイレクトに必要なブラウザーアドオンは、コマンドラインから /ALLOW_CLIENTHOSTEDAPPSURL=1 オプションを使用してCitrix Workspaceアプリをインストールすると、自動的に登録されます。

> 1つまたはすべてのアドオンを登録および登録解除するには、次のコマンドを使用します。

- クライアントデバイスにアドオンを登録するには: \<*client-installation-folder*>\redirector.exe /reg\<*browser*>
- クライアントデバイスのアドオンを登録解除するには: \<*client-installation-folder*>\redirector.exe /unreg\<*browser*>
- VDAにアドオンを登録するには: \<*VDAinstallation-folder*>\VDARedirector.exe /reg\<*browser*>
- VDAのアドオンを登録解除するには: \<*VDAinstallation-folder*>\VDARedirector.exe /unreg\<*browser*>

ここで、\<*browser*>はInternet Explorer、Firefox、Chrome、またはAllです。

たとえば、次のコマンドは、Citrix Workspaceアプリを実行しているデバイスにInternet Explorerアドオンを登録します。

C:\Program Files\Citrix\ICA Client\redirector.exe/regIE

次のコマンドは、WindowsマルチセッションOS VDA上のすべてのアドオンを登録します。

C:\Program Files (x86)\Citrix\HDX\bin\VDARedirector.exe /regAll

ブラウザ間のURLインターセプト

- デフォルトでは、Internet Explorerは指定されたURLをリダイレクトします。URLがブロックリストにないが、ブラウザまたはWebサイトが別のURLにリダイレクトする場合、最終的なURLはリダイレクトされません。ブロックリストにある場合でもリダイレクトされません。

URLリダイレクトが正しく機能するように、ブラウザからプロンプトが表示されたらアドオンを有効にしてください。インターネットオプションを使用しているアドオン、またはプロンプト内のアドオンが無効になっている場合、URLリダイレクトは正しく機能しません。

- Firefoxのアドオンは常にURLをリダイレクトします。

アドオンがインストールされると、Firefoxは新しいタブページにアドオンのインストールを許可するか、または防止するかを促します。機能が動作するようにアドオンを許可してください。

- Chromeのアドオンは、入力されたURLではなく、常にナビゲートされた最終URLをリダイレクトします。

拡張機能は外部からインストールされています。拡張機能を無効にすると、ChromeでURLリダイレクト機能が動作しません。シークレットモードでURLリダイレクトが必要な場合は、ブラウザの設定でそのモードでの拡張機能の実行を許可してください。

ログオフ時および切断時のローカルアプリケーションの動作を構成する

> **注：**

> これらの手順に従って設定を構成しない場合、デフォルトでは、ユーザーが仮想デスクトップからログオフまたは切断しても、ローカルアプリケーションは実行を継続します。再接続後、ローカルアプリケーションが仮想デスクトップで利用可能な場合、それらは再統合されます。

> ログオフ時および切断時のローカルアプリケーションの動作を構成するには、レジストリを介して管理される機能のリストにあるログオフ時および切断時のローカルアプリケーションの動作を参照してください。

汎用USBリダイレクトとクライアントドライブに関する考慮事項

HDX™テクノロジーは、ほとんどの一般的なUSBデバイスに対して**最適化されたサポート**を提供します。最適化されたサポートは、WAN経由でパフォーマンスと帯域幅の効率を向上させ、ユーザーエクスペリエンスを改善します。特に高遅延またはセキュリティに敏感な環境では、最適化されたサポートが通常最良の選択肢です。

HDXテクノロジーは、最適化されたサポートがない、または不適切な特殊なデバイスに対して**汎用USBリダイレクト**を提供します。例を次に示します。

- USBデバイスに、マウスやWebカメラのボタンの増加など、最適化されたサポートに含まれない高度な機能がある場合。
- ユーザーが最適化されたサポートに含まれない機能を必要とする場合。
- USBデバイスが、テストおよび測定機器や産業用コントローラーなどの特殊なデバイスである場合。
- アプリケーションがUSBデバイスとしてデバイスに直接アクセスする必要がある場合。
- USBデバイスにWindowsドライバーしか利用できない場合。たとえば、スマートカードリーダーには、Citrix Workspace™ app for Android用のドライバーが利用できない場合があります。
- Citrix Workspace appのバージョンが、この種類のUSBデバイスに対して最適化されたサポートを提供していない場合。

汎用USBリダイレクトでは、次のようになります。

- ユーザーはユーザーデバイスにデバイスドライバーをインストールする必要がありません。
- USBクライアントドライバーはVDAマシンにインストールされます。

重要:

- 汎用USBリダイレクトは、最適化されたサポートと組み合わせて使用できます。汎用USBリダイレクトを有効にする場合は、汎用USBリダイレクトと最適化されたサポートの両方について、CitrixのUSBデバイスポリシー設定を構成してください。
- クライアントUSBデバイスの最適化ルールのCitrixポリシー設定は、特定のUSBデバイスに対する汎用USBリダイレクトの特定のポリシー設定です。ここで説明する最適化されたサポートには適用されません。

USBデバイスのパフォーマンスに関する考慮事項

ネットワークの遅延と帯域幅は、一部の種類のUSBデバイスで汎用USBリダイレクトを使用する場合、ユーザーエクスペリエンスとUSBデバイスの動作に影響を与える可能性があります。たとえば、タイミングに敏感なデバイスは、高遅延で低帯域幅のリンクでは正しく動作しない場合があります。可能な場合は、代わりに最適化されたサポートを使用してください。

一部のUSBデバイスは、使用可能にするために高帯域幅を必要とします。たとえば、3Dマウス（通常、高帯域幅を必要とする3Dアプリで使用）などです。帯域幅を増やすことができない場合は、帯域幅ポリシー設定を使用して他のコンポーネントの帯域幅使用量を調整することで、問題を軽減できる場合があります。詳細については、「クライアントUSBデバイスリダイレクトの帯域幅ポリシー設定」および「マルチストリーム接続ポリシー設定」を参照してください。

USBデバイスのセキュリティに関する考慮事項

一部のUSBデバイスは、スマートカードリーダー、指紋リーダー、署名パッドなど、本質的にセキュリティに敏感です。USBストレージデバイスなどの他のUSBデバイスは、機密データである可能性のあるデータを送信するために使用できます。

重要:

スマートカードリーダーには汎用USBリダイレクトを使用しないでください。この機能はスマートカードリーダーではデフォルトで無効になっており、有効にしてもサポートされません。

USBデバイスは、マルウェアを配布するためによく使用されます。Citrix Workspace appとCitrix Virtual Apps and Desktops™の設定により、これらのUSBデバイスからのリスクを軽減できますが、排除することはできません。この状況は、汎用USBリダイレクトを使用する場合でも、最適化されたサポートを使用する場合でも当てはまります。

重要:

セキュリティに敏感なデバイスやデータについては、常にTLSまたはIPsecを使用してHDX接続を保護してください。

必要なUSBデバイスのサポートのみを有効にしてください。このニーズを満たすように、汎用USBリダイレクトと最適化されたサポートの両方を構成してください。

USBデバイスを安全に使用するためのガイダンスをユーザーに提供してください。

- 信頼できる情報源から入手したUSBデバイスのみを使用してください。
- インターネットカフェなど、開かれた環境でUSBデバイスを放置しないでください。
- 複数のコンピューターでUSBデバイスを使用するリスクを説明してください。

汎用USBリダイレクトとの互換性

汎用USBリダイレクトは、USB 2.0以前のデバイスでサポートされています。汎用USBリダイレクトは、USB 2.0またはUSB 3.0ポートに接続されたUSB 3.0デバイスでもサポートされています。汎用USBリダイレクトは、スーパースピードなど、USB 3.0で導入されたUSB機能をサポートしていません。

以下のCitrix Workspaceアプリは、汎用USBリダイレクトをサポートしています。

- Windows向けCitrix Workspaceアプリ。詳しくはアプリケーション配信の構成を参照してください。
- Citrix Workspaceアプリ for Mac。詳しくは、Citrix Workspaceアプリ for Macを参照してください。
- Linux向けCitrix Workspaceアプリ。詳しくは最適化を参照してください。
- Chrome OS 向け Citrix Workspace アプリについては、Citrix Workspace app for Chromeを参照してください。

Citrix Workspace アプリのバージョンについては、Citrix Workspace app feature matrixを参照してください。

以前のバージョンのCitrix Workspaceアプリを使用している場合は、Citrix Workspaceアプリのドキュメントを参照して、汎用USBリダイレクトがサポートされていることを確認してください。サポートされているUSBデバイスの種類に関する制限については、Citrix Workspaceアプリのドキュメントを参照してください。

汎用USBリダイレクトは、VDA for Single-session OSバージョン7.6以降のデスクトップセッションでサポートされています。

汎用USBリダイレクトは、VDA for Multi-session OSバージョン7.6以降のデスクトップセッションでサポートされていますが、以下の制限があります。

- VDAは、Windows Server 2012 R2、Windows Server 2016、Windows Server 2019、またはWindows Server 2022を実行している必要があります。
- USBデバイスドライバーは、VDA OS（Windows 2012 R2）のRemote Desktop Session Host（RDSH）と完全に互換性があり、完全な仮想化サポートを含む必要があります。

一部の種類のUSBデバイスは、リダイレクトしても有用ではないため、汎用USBリダイレクトではサポートされていません。

- USBモデム。
- USBネットワークアダプター。
- USBハブ。USBハブに接続されたUSBデバイスは個別に処理されます。
- USB仮想COMポート。汎用USBリダイレクトではなく、COMポートリダイレクトを使用してください。

汎用USBリダイレクトでテスト済みのUSBデバイスについては、Citrix Ready Marketplaceを参照してください。一部のUSBデバイスは、汎用USBリダイレクトでは正しく動作しません。

汎用USBリダイレクトを構成する

汎用USBリダイレクトを使用するUSBデバイスの種類は、個別に制御および構成できます。

- VDA上で、Citrixポリシー設定を使用します。詳しくは、ポリシー設定リファレンスのクライアントドライブとユーザーデバイスのリダイレクトおよびUSBデバイスポリシー設定を参照してください。
- Citrix Workspaceアプリで、Citrix Workspaceアプリに依存するメカニズムを使用します。たとえば、管理用テンプレートは、Windows向けCitrix Workspaceアプリを構成するレジストリ設定を制御します。デフォルトでは、USBリダイレクトは特定のクラスのUSBデバイスで許可され、他のデバイスでは拒否されます。詳しくは、Windows向けCitrix Workspaceアプリのドキュメントの構成を参照してください。

この個別の構成により、柔軟性が向上します。例：

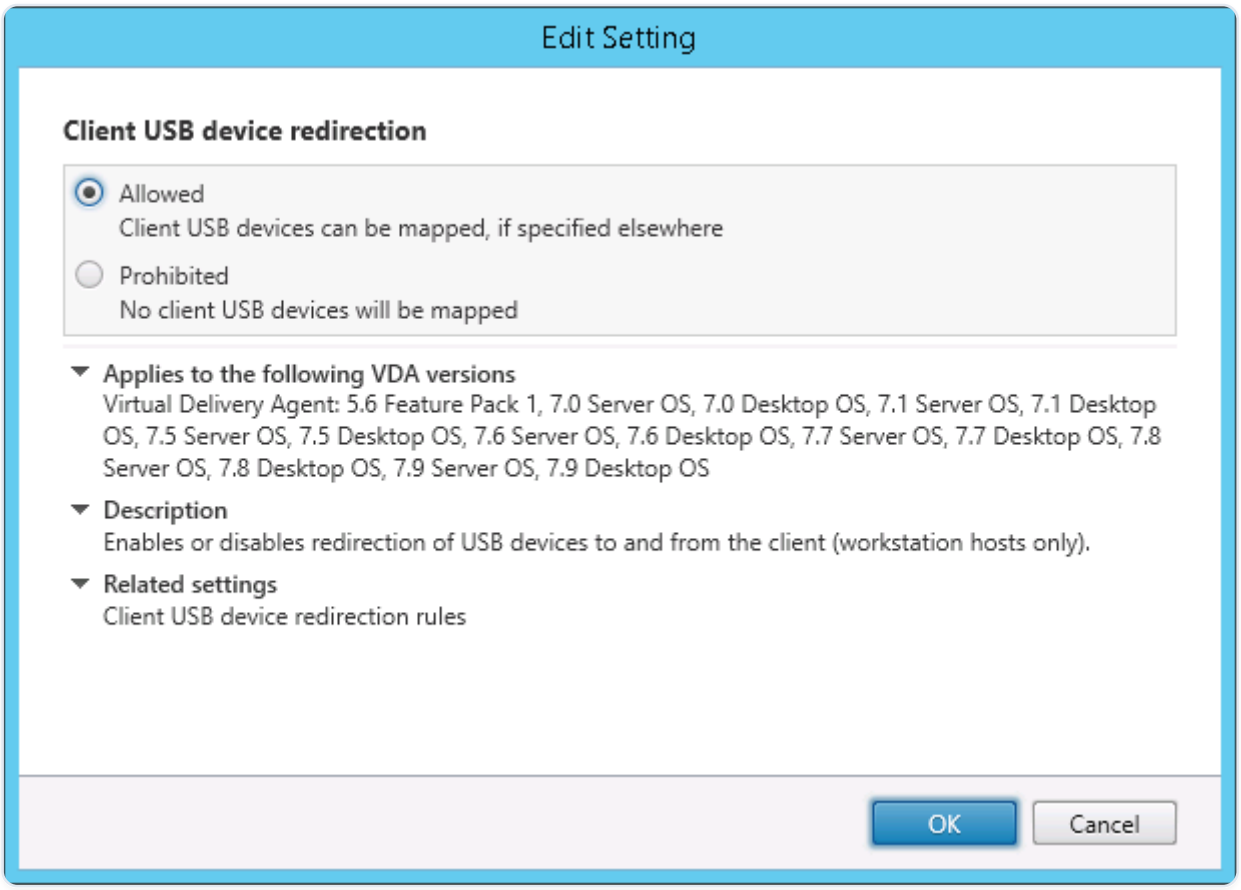
- 2つの異なる組織または部門がCitrix WorkspaceアプリとVDAを担当している場合、それぞれが個別に制御を適用できます。この構成は、ある組織のユーザーが別の組織のアプリケーションにアクセスする場合に適用されます。
- Citrixポリシー設定は、特定のユーザーのみに許可されるUSBデバイス、またはLAN経由でのみ接続するユーザー（Citrix Gatewayを使用しない場合）に許可されるUSBデバイスを制御できます。

汎用USBリダイレクトを有効にする

汎用USBリダイレクトを有効にし、ユーザーによる手動リダイレクトを不要にするには、Citrixポリシー設定とCitrix Workspaceアプリの接続設定の両方を構成します。

Citrixポリシー設定で：

1. クライアントUSBデバイスリダイレクトをポリシーに追加し、その値を**許可**に設定します。



2. （オプション）リダイレクトに利用可能なUSBデバイスのリストを更新するには、クライアントUSBデバイスリダイレクト規則設定をポリシーに追加し、USBポリシー規則を指定します。

ポリシー設定が完了したら、Citrix Workspaceアプリで:

3. デバイスが手動リダイレクトなしで自動的に接続されるように指定します。これは、管理用テンプレートを使用するか、Citrix Workspaceアプリの **Windows > Preferences > Connections** で行うことができます。

接続イメージ(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/connections-generic-usb-devices-receiver.png)

前のステップでVDAのUSBポリシー規則を指定した場合は、Citrix Workspaceアプリにも同じポリシー規則を指定します。

シンクライアントの場合、USBサポートの詳細と必要な構成については、製造元にお問い合わせください。

汎用USBリダイレクトで利用可能なUSBデバイスの種類を構成する

USBサポートが有効になっており、USBユーザー設定でUSBデバイスを自動的に接続するように設定されている場合、USBデバイスは自動的にリダイレクトされます。接続バーがない場合も、USBデバイスは自動的にリダイレクトされます。

ユーザーは、USBデバイスリストからデバイスを選択することで、自動的にリダイレクトされないデバイスを明示的にリダイレクトできます。詳細については、Citrix Workspaceアプリ for Windowsのユーザーヘルプ記事「Display your devices in the Desktop Viewer」を参照してください。

デバイスイメージ(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/usb-device-list-receiver.png)

最適化されたサポートではなく、汎用USBリダイレクトを使用するには、次のいずれかの方法があります。

- Citrix Workspaceアプリで、汎用USBリダイレクトを使用するUSBデバイスを手動で選択し、環境設定ダイアログボックスの［デバイス］タブから **［汎用に切り替える］** を選択します。
- USBデバイスの種類（例: AutoRedirectStorage=1）の自動リダイレクトを構成し、USBユーザー設定でUSBデバイスを自動的に接続するように設定することで、汎用USBリダイレクトを使用するUSBデバイスを自動的に選択します。詳細については、「Configure automatic redirection of USB devices」を参照してください。

> **注：**
>
> ウェブカメラがHDXマルチメディアリダイレクトと互換性がないと判明した場合にのみ、ウェブカメラで使用する汎用USBリダイレクトを構成してください。

> USBデバイスが一覧表示されたりリダイレクトされたりするのを完全に防ぐには、Citrix WorkspaceアプリとVDAのデバイス規則を指定できます。

汎用USBリダイレクトの場合、少なくともUSBデバイスクラスとサブクラスを知る必要があります。すべてのUSBデバイスが、その明白なUSBデバイスクラスとサブクラスを使用するわけではありません。例:

- ペンはマウスデバイスクラスを使用します。

- スマートカードリーダーは、ベンダー定義またはHIDデバイスクラスを使用できます。

より正確な制御を行うには、ベンダーID、製品ID、およびリリースIDを知る必要があります。この情報はデバイスベンダーから入手できます。

> **重要:**

> 悪意のあるUSBデバイスは、意図された用途と一致しないUSBデバイスの特性を提示する可能性があります。デバイスルールは、この動作を防ぐことを意図していません。

> デフォルトのUSBポリシー規則を上書きするために、USBデバイスリダイレクトルールを指定することで、汎用USBリダイレクトで利用可能なUSBデバイスを制御します。

Citrix DaaS（以前の名称：Citrix Virtual Apps and Desktopsサービス）：

- ほとんどの場合、Citrix Group Policy Management Console MSI (`CitrixGroupPolicyManagement_x64.msi`) を ダウンロード し、Active Directoryシステムにインストールしてから、ADグループポリシーを管理します。（MSIをVDAにインストールしないでください。）
- Windows向けCitrix Workspaceアプリの場合、ユーザーデバイスのレジストリを編集します。インストールメディアには管理用テンプレート（ADMファイル）が含まれているため、Active Directoryグループポリシーを通じてユーザーデバイスを変更できます: dvd root `\os\lang\Support\Configuration\icaclient_usb.adm`

オンプレミスCitrix Virtual Apps and Desktops:

- VDAの場合、グループポリシー規則を通じて、マルチセッションOSマシンの管理者上書き規則を編集します。Group Policy Management Consoleはインストールメディアに含まれています:
  - x64: DVDルート `\os\lang\x64\Citrix Policy\CitrixGroupPolicyManagement_x64.msi`
  - x86: DVD ルート `\os\lang\x86\Citrix Policy\CitrixGroupPolicyManagement_x86.msi`
- Windows向けCitrix Workspaceアプリの場合、ユーザーデバイスのレジストリを編集します。インストールメディアには管理用テンプレート（ADMファイル）が含まれているため、Active Directoryグループポリシーを通じてユーザーデバイスを変更できます: dvd root `\os\lang\Support\Configuration\icaclient_usb.adm`

警告:

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

製品のデフォルト規則はHKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\GenericUSBに保存されています。これらの製品のデフォルト規則を編集しないでください。代わりに、管理者上書き規則を作成するためのガイドとして使用してください。これはこの記事の後半で説明します。GPO上書きは、製品のデフォルト規則よりも前に評価されます。

管理者上書き規則はHKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\PortICA\GenericUSB\DeviceRulesに保存されています。GPOポリシー規則は**{Allow:`|`Deny:}**の形式を取り、その後に空白で区切られた*tag=value*式のセットが続きます。

以下のタグがサポートされています:

タグ	説明
VID	デバイス記述子からのベンダーID
PID	デバイス記述子からの製品ID
REL	デバイス記述子からのリリースID
クラス	デバイス記述子またはインターフェイス記述子のいずれかからのクラス。利用可能なUSBクラスコードについては、`<http://www.usb.org/>`のUSBウェブサイトを参照してください。
サブクラス	デバイス記述子またはインターフェース記述子のいずれかからのサブクラス

タグ	説明
保護	デバイス記述子またはインターフェイス記述子のいずれかからのプロトコル

ポリシー規則を作成する際は、以下に注意してください:

- 規則では大文字と小文字は区別されません。
- 規則の末尾には、`#` で始まるオプションのコメントを付けることができます。区切り文字は不要で、コメントは照合目的では無視されます。
- 空行と純粋なコメント行は無視されます。
- 空白は区切り文字として使用されますが、数値または識別子の中央に表示することはできません。たとえば、Deny: Class = 08 SubClass=05 は有効な規則ですが、Deny: Class=0 Sub Class=05 は無効です。
- タグは一致演算子 = を使用する必要があります。例: VID=1230。
- 各ルールは新しい行で開始するか、セミコロンで区切られたリストの一部である必要があります。

> **注：**
>
> ADMテンプレートファイルを使用している場合、規則はセミコロンで区切られたリストとして、1行で作成する必要があります。

例:

- 次の例は、ベンダーおよび製品識別子に対する管理者定義のUSBポリシー規則を示しています:

  `Allow: VID=046D PID=C626 # Allow Logitech SpaceNavigator 3D Mouse Deny: VID=046D # Deny all Logitech products`

- 次の例は、定義されたクラス、サブクラス、およびプロトコルに対する管理者定義のUSBポリシー規則を示しています:

  `Deny: Class=EF SubClass=01 Prot=01 # Deny MS Active Sync devices Allow: Class=EF SubClass=01 # Allow Sync devices Allow: Class=EF # Allow all USB-Miscellaneous devices`

USBデバイスの使用と取り外し

ユーザーは、仮想セッションを開始する前または後にUSBデバイスを接続できます。

Windows版Citrix Workspaceアプリを使用する場合、以下が適用されます:

- セッション開始後に接続されたデバイスは、Desktop ViewerのUSBメニューにすぐに表示されます。
- USBデバイスが適切にリダイレクトされない場合は、仮想セッションが開始されるまでデバイスの接続を待つことで、問題を解決できる場合があります。
- データ損失を避けるため、USBデバイスを取り外す前にWindowsの「ハードウェアを安全に取り外す」アイコンを使用してください。

USBマスストレージデバイスのセキュリティ制御

USBマスストレージデバイスには、最適化されたサポートが提供されます。このサポートは、Citrix Virtual Apps and Desktopsのクライアントドライブマッピングの一部です。ユーザーがログオンすると、ユーザーデバイス上のドライブが仮想デスクトップ上のドライブ文字に自動的にマッピングされます。ドライブは、マッピングされたドライブ文字を持つ共有フォルダーとして表示されます。クライアントドライブマッピングを構成するには、**クライアントリムーバブルドライブ**設定を使用します。この設定は、ICAポリシー設定のファイルリダイレクトポリシー設定セクションにあります。

USB大容量記憶装置では、クライアントドライブマッピング、汎用USBリダイレクト、またはその両方を使用できます。これらはCitrixポリシーを使用して制御します。主な違いは次のとおりです。

機能	クライアントドライブマッピング	汎用USBリダイレクト
デフォルトで有効	はい	いいえ
読み取り専用アクセスを構成可能	はい	いいえ
暗号化されたデバイスアクセス	はい、デバイスにアクセスする前に暗号化が解除されている場合	はい
BitLocker To Goデバイス	いいえ	いいえ

機能	クライアントドライブマッピング	汎用USBリダイレクト
セッション中にデバイスを削除しても安全	いいえ	はい、ユーザーが安全な取り外しに関するオペレーティングシステムの推奨事項に従う場合

汎用USBリダイレクトとクライアントドライブマッピングの両方のポリシーが有効になっており、セッションの開始前または開始後に大容量記憶装置が挿入されると、クライアントドライブマッピングを使用してリダイレクトされます。汎用USBリダイレクトとクライアントドライブマッピングの両方のポリシーが有効になっており、デバイスが自動リダイレクト用に構成されている場合、セッションの開始前または開始後に大容量記憶装置が挿入されると、汎用USBリダイレクトを使用してリダイレクトされます。詳しくは、Knowledge Centerの記事CTX123015を参照してください。

> **注：**
>
> USBリダイレクトは、50 Kbpsなどの低帯域幅接続でもサポートされます。ただし、大きなファイルのコピーは機能しません。

クライアントドライブマッピングでファイルアクセスを制御する

ユーザーが仮想環境からユーザーデバイスにファイルをコピーできるかどうかを制御できます。デフォルトでは、マップされたクライアントドライブ上のファイルとフォルダーは、セッション内から読み取り/書き込みモードで利用できます。

ユーザーがマップされたクライアントデバイス上のファイルやフォルダーを追加または変更できないようにするには、**読み取り専用クライアントドライブアクセス**ポリシー設定を有効にします。この設定をポリシーに追加するときは、クライアントドライブリダイレクト設定が**許可**に設定されており、ポリシーにも追加されていることを確認してください。

印刷

環境でのプリンターの管理は、多段階のプロセスです。

1. まだ慣れていない場合は、印刷の概念に慣れてください。
2. 印刷アーキテクチャを計画します。これには、ビジネスニーズ、既存の印刷インフラストラクチャ、ユーザーとアプリケーションが現在印刷とどのようにやり取りしているか、およびどの印刷管理モデルが環境に最適であるかを分析することが含まれます。
3. プリンターのプロビジョニング方法を選択し、印刷設計を展開するためのポリシーを作成して、印刷環境を構成します。新しい従業員やサーバーが追加されたときにポリシーを更新します。
4. ユーザーに展開する前に、パイロット印刷構成をテストします。
5. プリンタードライバーを管理し、印刷パフォーマンスを最適化することで、Citrix® 印刷環境を維持します。
6. 発生する可能性のある問題をトラブルシューティングします。

印刷の概念

展開の計画を開始する前に、印刷に関する以下の主要な概念を理解していることを確認してください。

- 利用可能なプリンタープロビジョニングの種類
- 印刷ジョブのルーティング方法
- プリンタードライバー管理の基本

印刷の概念は、Windowsの印刷の概念に基づいています。環境で印刷を構成し、正常に管理するには、Windowsネットワークとクライアント印刷がどのように機能するか、そしてそれがこの環境での印刷動作にどのように変換されるかを理解する必要があります。

印刷プロセス

この環境では、すべての印刷はアプリケーションをホストするマシン上で（ユーザーによって）開始されます。印刷ジョブは、ネットワークプリントサーバーまたはユーザーデバイスを介して印刷デバイスにリダイレクトされます。

仮想デスクトップおよびアプリケーションのユーザーには、永続的なワークスペースはありません。セッションが終了するとユーザーのワークスペースは削除されるため、各セッションの開始時にすべての設定を再構築する必要があります。その結果、ユーザーが新しいセッションを開始するたびに、システムはユーザーのワークスペースを再構築する必要があります。

ユーザーが印刷する場合：

- ユーザーに提供するプリンターを決定します。これはプリンタープロビジョニングとして知られています。
- ユーザーの印刷設定を復元します。
- セッションのデフォルトプリンターを決定します。

プリンタープロビジョニング、印刷ジョブルーティング、プリンタープロパティ保持、およびドライバー管理のオプションを構成することで、これらのタスクを実行する方法をカスタマイズできます。さまざまなオプション設定が、環境での印刷パフォーマンスとユーザーエクスペリエンスにどのように影響するかを評価するようにしてください。

プリンタープロビジョニング

セッションでプリンターを利用可能にするプロセスは、プロビジョニングとして知られています。プリンタープロビジョニングは通常、動的に処理されます。つまり、セッションに表示されるプリンターは事前に決定されて保存されるわけではありません。代わりに、プリンターはログオン時および再接続時にセッションが構築される際に、ポリシーに基づいて組み立てられます。その結果、プリンターはポリシーに反映されていれば、ポリシー、ユーザーの場所、およびネットワークの変更に応じて変化する可能性があります。したがって、異なる場所にローミングするユーザーは、ワークスペースの変更を目にする可能性があります。

システムは、クライアント側のプリンターも監視し、クライアント側のプリンターへの追加、削除、変更に基づいて、セッション内で自動作成されるプリンターを動的に調整します。この動的なプリンター検出は、さまざまなデバイスから接続するモバイルユーザーにメリットをもたらします。

プリンタープロビジョニングの最も一般的な方法は次のとおりです。

- **Universal Print Server** - Citrix ユニバーサルプリントサーバーは、ネットワークプリンターのユニバーサル印刷をサポートします。ユニバーサルプリントサーバーは、ユニバーサルプリントドライバーを使用します。このソリューションにより、マルチセッションOSマシンで単一のドライバーを使用して、任意のデバイスからネットワーク印刷を行うことができます。

Citrixは、リモートプリントサーバーのシナリオにCitrix Universal™ Print Serverを推奨します。ユニバーサルプリントサーバーは、最適化され圧縮された形式で印刷ジョブをネットワーク経由で転送するため、ネットワークの使用を最小限に抑え、ユーザーエクスペリエンスを向上させます。

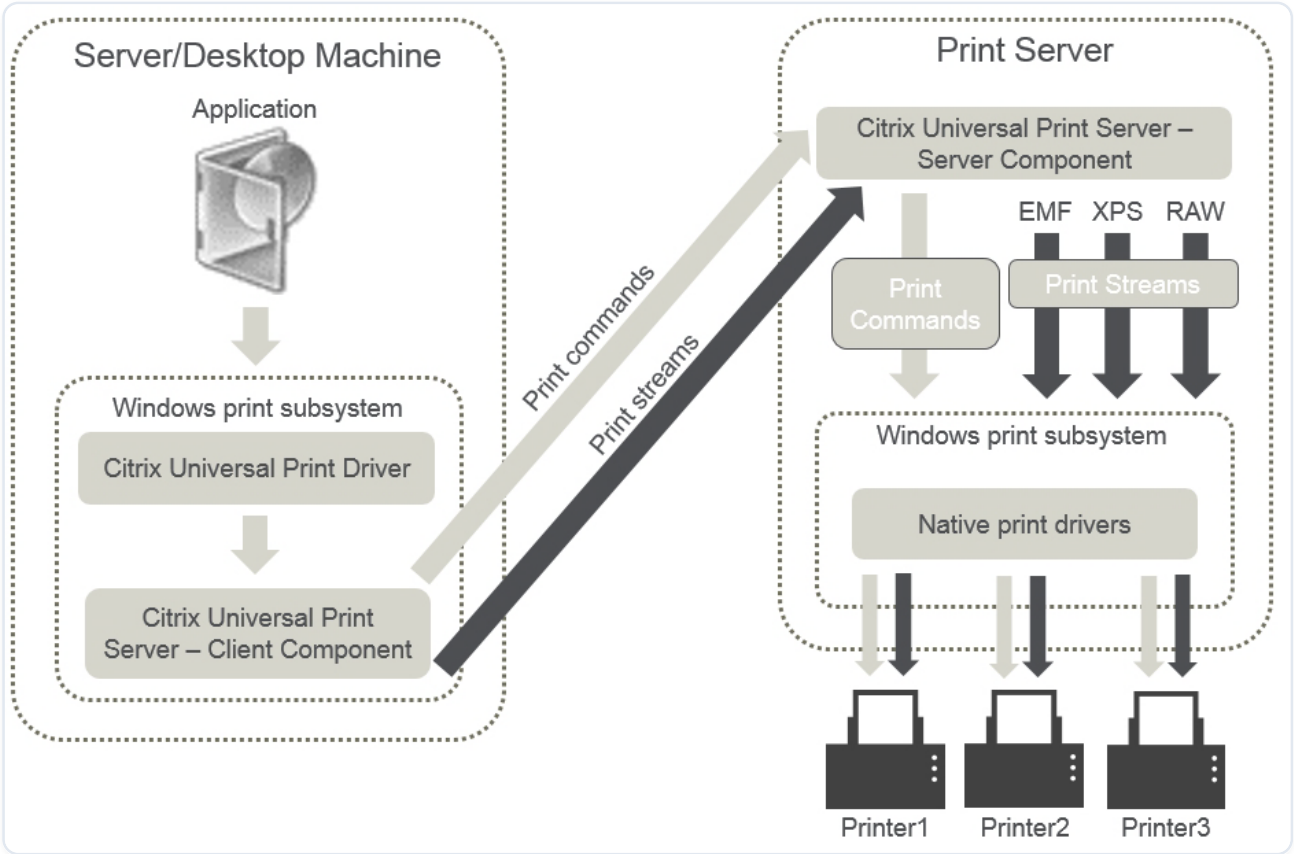
ユニバーサルプリントサーバーの機能は次のとおりです。

クライアントコンポーネント、**UPClient** - セッションネットワークプリンターをプロビジョニングし、ユニバーサルプリントドライバーを使用する各マルチセッションOSマシンでUPClientを有効にします。

サーバーコンポーネント、**UPServer** - セッションネットワークプリンターをプロビジョニングし、セッションプリンターにユニバーサルプリントドライバーを使用する（セッションプリンターが集中管理されているかどうかにかかわらず）各プリントサーバーにUPServerをインストールします。

Universal Print Serverの要件とセットアップの詳細については、システム要件とインストールの記事を参照してください。

次の図は、Universal Print Serverを使用する環境におけるネットワークベースのプリンターの一般的なワークフローを示しています。



Citrix Universal Print Serverを有効にすると、接続されているすべてのネットワークプリンターが自動検出によって自動的にそれを利用します。

- **自動作成** - *自動作成*とは、各セッションの開始時に自動的に作成されるプリンターを指します。リモートネットワークプリンターとローカルに接続されたクライアントプリンターの両方を自動作成できます。ユーザーあたりのプリンター数が多い環境では、デフォルトのクライアントプリンターのみを自動作成することを検討してください。自動作成するプリンターの数を減らすと、マルチセッションOSマシンでのオーバーヘッド（メモリとCPU）が少なくなります。自動作成されるプリンターを最小限に抑えることで、ユーザーのログオン時間を短縮することもできます。

  自動作成されたプリンターは、以下に基づいています。

  - ユーザーデバイスにインストールされているプリンター。
  - セッションに適用されるポリシー。

    自動作成ポリシー設定を使用すると、自動作成されるプリンターの数または種類を制限できます。デフォルトでは、ローカルに接続されたプリンターとネットワークプリンターを含む、ユーザーデバイス上のすべてのプリンターを自動的に構成すると、プリンターはセッションで利用可能になります。

  ユーザーがセッションを終了すると、そのセッションのプリンターは削除されます。

  クライアントおよびネットワークプリンターの自動作成には、関連するメンテナンスが必要です。たとえば、プリンターを追加するには、次の操作が必要です。

  - セッションプリンターポリシー設定を更新します。
  - プリンタードライバーマッピングと互換性ポリシー設定を使用して、すべてのマルチセッションOSマシンにドライバーを追加します。

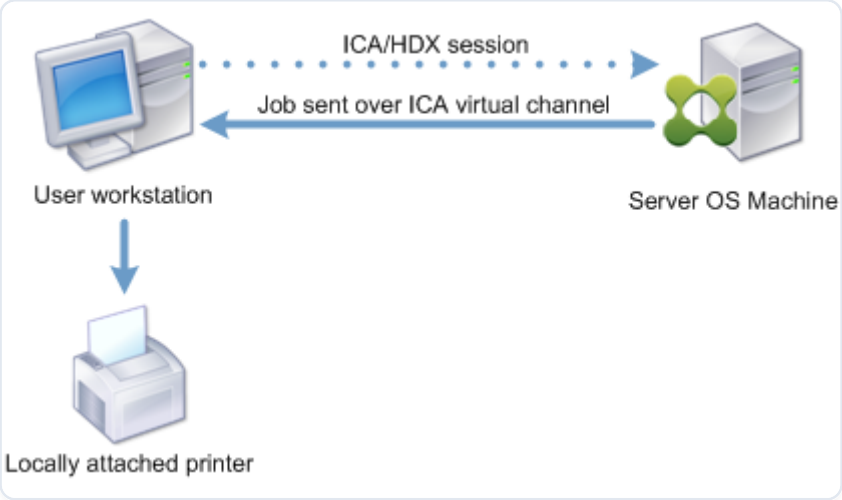
印刷ジョブのルーティング

印刷経路という用語は、印刷ジョブがルーティングされるパスと、印刷ジョブがスプールされる場所の両方を包含します。この概念の両方の側面が重要です。ルーティングはネットワークトラフィックに影響を与えます。スプーリングは、ジョブを処理するデバイス上のローカルリソースの利用に影響を与えます。

この環境では、印刷ジョブは印刷デバイスへの2つの経路を取ることができます。クライアントを介するか、ネットワークプリントサーバーを介するかです。これらの経路は、クライアント印刷経路およびネットワーク印刷経路と呼ばれます。デフォルトでどちらの経路が選択されるかは、使用されるプリンターの種類によって異なります。

ローカル接続されたプリンター

システムは、マルチセッションOSマシンからクライアントを介して印刷デバイスにジョブをルーティングします。ICA®プロトコルは、印刷ジョブのトラフィックを最適化および圧縮します。印刷デバイスがユーザーデバイスにローカルに接続されている場合、印刷ジョブはICA仮想チャネルを介してルーティングされます。



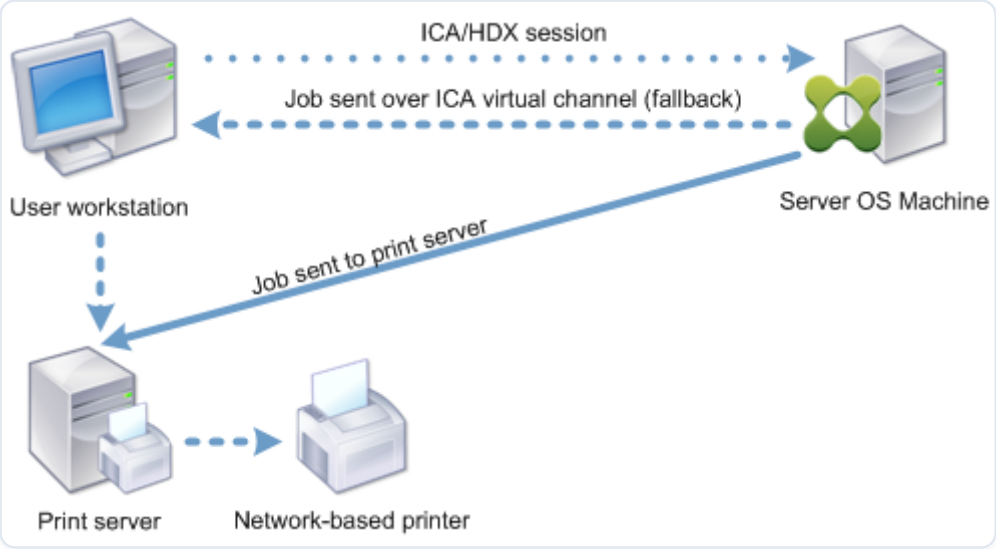
ネットワークベースのプリンター

デフォルトでは、ネットワークプリンター宛てのすべての印刷ジョブは、マルチセッションOSマシンからネットワーク経由で直接印刷サーバーにルーティングされます。ただし、次の状況では、印刷ジョブはICA接続を介して自動的にルーティングされます。

- 仮想デスクトップまたはアプリケーションが印刷サーバーに接続できない場合。
- ネイティブプリンタードライバーがマルチセッションOSマシンで利用できない場合。

Universal Print Serverが有効になっていない場合、ネットワーク印刷用のクライアント印刷経路を構成することは、ICA接続を介してジョブを送信することによって得られる最適化とトラフィック圧縮の恩恵を受けることができる、広域ネットワークなどの低帯域幅接続に役立ちます。

クライアント印刷経路を使用すると、トラフィックを制限したり、印刷ジョブに割り当てられる帯域幅を制限したりすることもできます。印刷機能のないシンクライアントなど、ユーザーデバイスを介したジョブのルーティングが不可能な場合は、ICA/HDXトラフィックを優先し、良好なセッション内ユーザーエクスペリエンスを確保するために、Quality of Serviceを構成する必要があります。



印刷ドライバーの管理

Citrix Universal Printer Driver (UPD)は、ほとんどのプリンターと互換性のあるデバイスに依存しない印刷ドライバーです。Citrix UPDは、次の2つのコンポーネントで構成されています。

サーバーコンポーネント。Citrix UPDは、Citrix Virtual Apps and Desktops™ VDAのインストールの一部としてインストールされます。VDAは、Citrix UPDとともに次のドライバーをインストールします。「Citrix Universal Printer」（EMFドライバー）および「Citrix XPS Universal Printer」（XPSドライバー）。

Name	Processor	Type
Citrix Universal Printer	x64	Type 3 - User Mode
Citrix XPS Universal Printer	x64	Type 3 - User Mode

VDAインストーラーは、Universal Print Server PDFプリンタードライバーのインストールを制御するオプションを提供しなくなりました。PDFプリンタードライバーは、常に自動的にインストールされます。7.17 VDA（またはそれ以降のサポートされるバージョン）にアップグレードすると、以前にインストールされていたCitrix PDFプリンタードライバーは自動的に削除され、最新バージョンに置き換えられます。

印刷ジョブが開始されると、ドライバーはアプリケーションの出力を記録し、変更を加えることなくエンドポイントデバイスに送信します。

クライアントコンポーネント。Citrix UPDは、Citrix Workspace™アプリのインストールの一部としてインストールされます。これは、Citrix Virtual Apps and Desktopsセッションの受信印刷ストリームを取得します。その後、印刷ストリームをローカル印刷サブシステムに転送し、そこでデバイス固有のプリンタードライバーを使用して印刷ジョブがレンダリングされます。

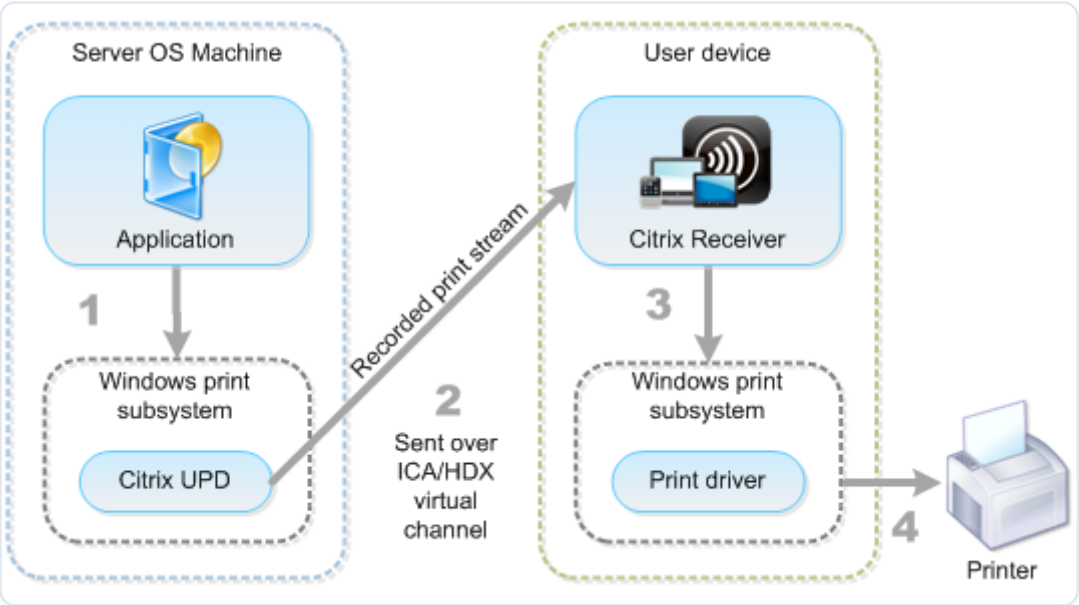
Citrix UPDは、以下の印刷形式をサポートしています。

- 拡張メタファイル形式（**EMF**）、デフォルト。EMFは、Windowsメタファイル（WMF）形式の32ビットバージョンです。EMFドライバーは、Windowsベースのクライアントでのみ使用できます。
- XML Paper Specification（**XPS**）。XPSドライバーはXMLを使用して、Adobe PDF形式に似たプラットフォームに依存しない「電子ペーパー」を作成します。
- プリンターコマンド言語（**PCL5c**および**PCL4**）。PCLは、元々ヒューレット・パッカードがインクジェットプリンター向けに開発した印刷プロトコルです。基本的なテキストとグラフィックの印刷に使用され、HP LaserJetおよび多機能周辺機器で広くサポートされています。
- PostScript（**PS**）。PostScriptは、テキストやベクターグラフィックの印刷に使用できるコンピューター言語です。このドライバーは、低コストのプリンターや多機能周辺機器で広く使用されています。

PCLおよびPSドライバーは、MacやUNIXクライアントなどのWindows以外のデバイスを使用する場合に最適です。Citrix UPDがドライバーを使用しようとする順序は、Universal driver preferenceポリシー設定を使用して変更できます。

Citrix UPD（EMFおよびXPSドライバー）は、ステープルや給紙元選択などの高度な印刷機能をサポートしています。これらの機能は、ネイティブドライバーがMicrosoft Print Capabilityテクノロジーを使用して利用可能にしている場合に利用できます。ネイティブドライバーは、Print Capabilities XMLで標準化されたPrint Schema Keywordsを使用する必要があります。非標準のキーワードが使用されている場合、Citrix Universal Print Driverを使用しても高度な印刷機能は利用できません。

次の図は、Universal Print Driverのコンポーネントと、デバイスにローカル接続されたプリンターの一般的なワークフローを示しています。



ドライバー管理戦略を計画する際には、Universal Print Driver、デバイス固有のドライバー、またはその両方をサポートするかどうかを決定します。標準ドライバーをサポートする場合は、以下を決定する必要があります。

プリンターの自動作成中に、システムがユーザーデバイスに接続された新しいローカルプリンターを検出した場合、必要なプリンタードライバーをMulti-session OSマシンで確認します。デフォルトでは、Windowsネイティブドライバーが利用できない場合、システムはUniversal Print Driverを使用します。

印刷を成功させるには、Multi-session OSマシン上のプリンタードライバーとユーザーデバイス上のドライバーが一致している必要があります。次の図は、クライアント印刷でプリンタードライバーが2か所でどのように使用されるかを示しています。

クライアントがローカルプリンターに印刷する図(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/cds-print-client-routing.png)

- サポートするドライバーの種類。
- マルチセッションOSマシンにプリンタードライバーがない場合に、自動的にインストールするかどうか。
- ドライバー互換性リストを作成するかどうか。

関連コンテンツ

- 印刷構成の例(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/printing/printing-configuration-example.html)
- ベストプラクティス、セキュリティに関する考慮事項、およびデフォルトの操作(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/printing/printing-best-practices.html)
- 印刷ポリシーと設定(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/printing/printing-policies-preferences.html)
- プリンターのプロビジョニング(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/printing/printing-provision-printers.html)
- 印刷環境の維持(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/printing/printing-maintain-environment.html)

印刷構成の例

ニーズと環境に最も適した印刷構成オプションを選択することで、管理を簡素化できます。デフォルトの印刷構成はほとんどの環境でユーザーが印刷できるようにしますが、そのデフォルト設定では、期待されるユーザーエクスペリエンスや、環境にとって最適なネットワーク使用量および管理オーバーヘッドが得られない場合があります。

印刷構成は以下に依存します。

- ビジネスニーズと既存の印刷インフラストラクチャ。

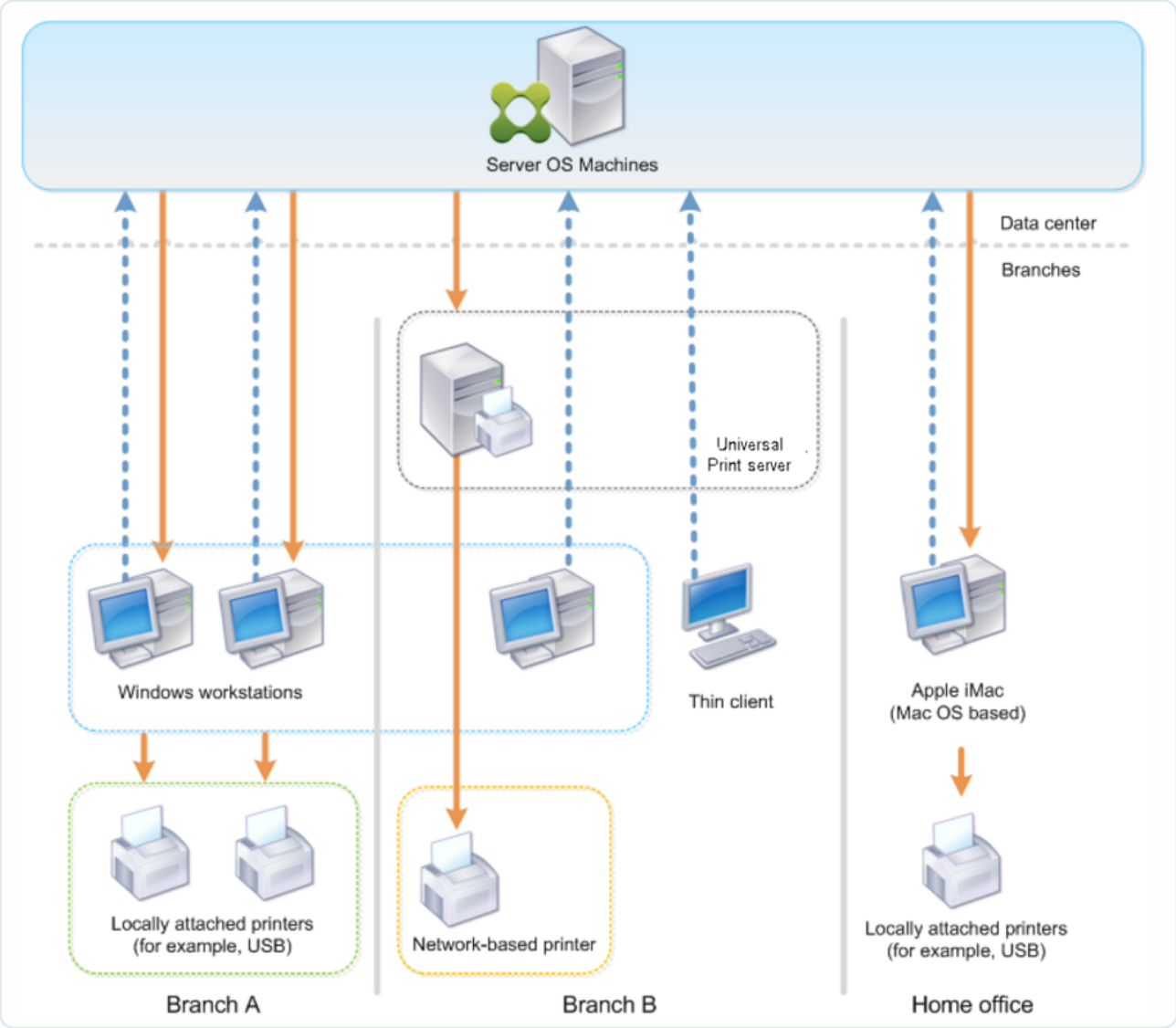
  組織のニーズに合わせて印刷構成を設計します。既存の印刷実装（ユーザーがプリンターを追加できるかどうか、どのユーザーがどのプリンターにアクセスできるかなど）は、印刷構成を定義する際に役立つガイドとなる場合があります。
- 組織に、特定のユーザー（人事部や給与計算部門のプリンターなど）のためにプリンターを予約するセキュリティポリシーがあるかどうか。
- ユーザーが、ワークステーション間を移動する従業員や出張中の従業員のように、主要な勤務地を離れて印刷する必要があるかどうか。

印刷構成を設計する際は、ユーザーがローカルユーザーデバイスから印刷する場合と同じエクスペリエンスをセッション内で得られるように努めてください。

印刷展開の例

次の図は、これらのユースケースの印刷展開を示しています。

- **支店A** - 数台のWindowsワークステーションを持つ小規模な海外支店。各ユーザーワークステーションには、ローカルに接続されたプライベートプリンターがあります。
- **支店B** - シンクライアントとWindowsベースのワークステーションを持つ大規模な支店。効率を高めるため、この支店のユーザーはネットワークベースのプリンター（フロアごとに1台）を共有しています。支店内に設置されたWindowsベースのプリントサーバーが印刷キューを管理します。
- **ホームオフィス** - 会社のCitrix®インフラストラクチャにアクセスするMac OSベースのユーザーデバイスを備えたホームオフィス。ユーザーデバイスにはローカルに接続されたプリンターがあります。



以下のセクションでは、環境の複雑さを最小限に抑え、その管理を簡素化する構成について説明します。

自動作成されたクライアントプリンターとCitrix Universal™ プリンタードライバー

支店Aでは、すべてのユーザーがWindowsベースのワークステーションで作業しているため、自動作成されたクライアントプリンターとユニバーサルプリンタードライバーが使用されます。これらのテクノロジーは以下の利点を提供します。

- パフォーマンス - 印刷ジョブはICA®印刷チャネルを介して配信されるため、印刷データを圧縮して帯域幅を節約できます。

  大容量のドキュメントを印刷する単一のユーザーが他のユーザーのセッションパフォーマンスを低下させないようにするため、最大印刷帯域幅を指定するようにCitrixポリシーが構成されています。

代替ソリューションは、印刷トラフィックが別の低優先度TCP接続内で転送されるマルチストリームICA接続を活用することです。マルチストリームICAは、WAN接続でQuality of Service (QoS) が実装されていない場合のオプションです。

- 柔軟性 - Citrix Universalプリンタードライバーを使用することで、クライアントに接続されたすべてのプリンターを、データセンターに新しいプリンタードライバーを統合することなく、仮想デスクトップまたはアプリケーションセッションから使用できるようになります。

Citrix ユニバーサルプリントサーバー

支店Bでは、すべてのプリンターがネットワークベースであり、そのキューはWindowsプリントサーバーで管理されているため、Citrix Universal Print Serverが最も効率的な構成となります。

必要なすべてのプリンタードライバーは、ローカル管理者によってプリントサーバーにインストールおよび管理されます。プリンターを仮想デスクトップまたはアプリケーションセッションにマッピングする方法は次のとおりです。

- Windowsベースのワークステーションの場合 - ローカルITチームは、ユーザーが適切なネットワークベースのプリンターをWindowsワークステーションに接続するのを支援します。これにより、ユーザーはローカルにインストールされたアプリケーションから印刷できるようになります。

  仮想デスクトップまたはアプリケーションセッション中に、ローカルで構成されたプリンターは自動作成によって列挙されます。その後、仮想デスクトップまたはアプリケーションは、可能であれば直接ネットワーク接続としてプリントサーバーに接続します。

  Citrix Universal Print Serverコンポーネントがインストールされ、有効になっているため、ネイティブプリンタードライバーは不要です。ドライバーが更新されたり、プリンターキューが変更されたりしても、データセンターでの追加構成は不要です。
- シンクライアントの場合 - シンクライアントユーザーの場合、プリンターは仮想デスクトップまたはアプリケーションセッション内で接続されている必要があります。ユーザーに最もシンプルな印刷エクスペリエンスを提供するために、管理者は、フロアのプリンターをデフォルトプリンターとして接続するために、フロアごとに単一のCitrixセッションプリンターポリシーを構成します。

  ユーザーがフロア間を移動しても正しいプリンターが接続されるようにするため、ポリシーはサブネットまたはシンクライアントの名前に基づいてフィルタリングされます。この構成は近接印刷と呼ばれ、ローカルプリンタードライバーのメンテナンスを可能にします（委任された管理モデルに従って）。

プリンターキューを変更または追加する必要がある場合、Citrix管理者は、環境内でそれぞれのセッションプリンターポリシーを変更する必要があります。

ネットワーク印刷トラフィックはICA仮想チャネル外で送信されるため、QoSが実装されます。ICA/HDXトラフィックで使用されるポートでのインバウンドおよびアウトバウンドネットワークトラフィックは、他のすべてのネットワークトラフィックよりも優先されます。この構成により、ユーザーセッションが大規模な印刷ジョブによって影響を受けることはありません。

自動作成されたクライアントプリンターとCitrixユニバーサルプリンタードライバー

ユーザーが非標準のワークステーションで作業し、管理されていない印刷デバイスを使用するホームオフィスの場合、最も簡単なアプローチは、自動作成されたクライアントプリンターとユニバーサルプリンタードライバーを使用することです。

展開の概要

要約すると、サンプルの展開は次のように構成されています。

- マルチセッションOSマシンにはプリンタードライバーはインストールされていません。Citrixユニバーサルプリンタードライバーのみが使用されます。ネイティブ印刷へのフォールバックとプリンタードライバーの自動インストールは無効になっています。
- すべてのユーザーに対してすべてのクライアントプリンターを自動作成するポリシーが構成されています。マルチセッションOSマシンは、デフォルトで印刷サーバーに直接接続します。必要な構成は、ユニバーサルプリントサーバーコンポーネントを有効にすることだけです。
- 支店Bの各フロアに対してセッションプリンターポリシーが構成され、各フロアのすべてのシンクライアントに適用されます。
- 優れたユーザーエクスペリエンスを保証するために、支店BにはQoSが実装されています。

ベストプラクティス、セキュリティに関する考慮事項、およびデフォルトの操作

ベストプラクティス

特定の環境に最適な印刷ソリューションを決定する要因は多数あります。これらのベストプラクティスの一部は、お客様のサイトには適用されない場合があります。

- Citrix Universal™ Print Serverを使用します。
- UniversalプリンタードライバーまたはWindowsネイティブドライバーを使用します。

- マルチセッションOSマシンにインストールされているプリンタードライバーの数を最小限に抑えます。
- ネイティブドライバーへのドライバーマッピングを使用します。
- テストされていないプリンタードライバーを本番サイトにインストールしないでください。
- ドライバーの更新は避けてください。常にドライバーをアンインストールし、プリントサーバーを再起動してから、交換用ドライバーをインストールするようにしてください。
- 使用されていないドライバーをアンインストールするか、プリンタードライバーマッピングおよび互換性ポリシーを使用して、そのドライバーでプリンターが作成されないようにします。
- バージョン2のカーネルモードドライバーの使用は避けるようにしてください。
- プリンターモデルがサポートされているかどうかを確認するには、製造元に問い合わせるか、Citrix Ready製品ガイド（www.citrix.com/ready）を参照してください。

  一般に、Microsoftが提供するすべてのプリンタードライバーは、ターミナルサービスでテストされており、Citrixで動作することが保証されています。ただし、サードパーティのプリンタードライバーを使用する前に、Windows Hardware Quality Labs（WHQL）プログラムによってドライバーがターミナルサービス向けに認定されていることをプリンタードライバーベンダーに確認してください。Citrixはプリンタードライバーを認定していません。

セキュリティに関する考慮事項

Citrixの印刷ソリューションは、設計上安全です。

- Citrix Print Manager Serviceは、ログオンとログオフ、切断、再接続、セッション終了などのセッションイベントを常に監視し、それらに応答します。実際のセッションユーザーを偽装することで、サービス要求を処理します。
- Citrix印刷は、各プリンターにセッション内で一意の名前空間を割り当てます。
- Citrix印刷は、自動作成されたプリンターのデフォルトのセキュリティ記述子を設定し、あるセッションで自動作成されたクライアントプリンターが、他のセッションで実行されているユーザーからアクセスできないようにします。デフォルトでは、管理ユーザーは、任意のクライアントプリンターの権限を表示および手動で調整できる場合でも、誤って別のセッションのクライアントプリンターに印刷することはできません。

デフォルトの印刷操作

デフォルトでは、ポリシー規則を構成しない場合、印刷動作は次のとおりです。

- ユニバーサルプリントサーバーは無効になっています。

- ユーザーデバイスで構成されているすべてのプリンターは、各セッションの開始時に自動的に作成されます。

  この動作は、Citrixポリシー設定「クライアントプリンターの自動作成」を「すべてのクライアントプリンターを自動作成」オプションで構成することと同じです。
- システムは、ユーザーデバイスにローカルに接続されたプリンターにキューイングされたすべての印刷ジョブを、クライアント印刷ジョブとして（つまり、ICA®チャネルを介してユーザーデバイス経由で）ルーティングします。
- システムは、ネットワークプリンターにキューイングされたすべての印刷ジョブを、マルチセッションOSマシンから直接ルーティングします。システムがネットワーク経由でジョブをルーティングできない場合、リダイレクトされたクライアント印刷ジョブとしてユーザーデバイス経由でルーティングします。

  この動作は、Citrixポリシー設定「プリントサーバーへの直接接続」を無効にすることと同じです。
- システムは、ユーザーの印刷設定と印刷デバイス固有の設定を組み合わせた印刷プロパティを、ユーザーデバイスに保存しようとします。クライアントがこの操作をサポートしない場合、システムは印刷プロパティをマルチセッションOSマシンのユーザープロファイルに保存します。

  この動作は、Citrixポリシー設定「プリンタープロパティの保持」を「クライアントに保存されていない場合のみプロファイルに保持」オプションで構成することと同じです。
- VDAバージョン7.16以降では、V3インボックスプリンタードライバーがオペレーティングシステムに含まれていないため、Citrixポリシー設定「インボックスプリンタードライバーの自動インストール」はWindows 8以降のWindowsオペレーティングシステムバージョンには影響しません。
- VDA 7.16より前のバージョンでは、マルチセッションOSマシンで利用可能な場合、システムはプリンタードライバーのWindowsバージョンを使用します。プリンタードライバーが利用できない場合、システムはWindowsオペレーティングシステムからドライバーをインストールしようとします。Windowsでドライバーが利用できない場合、Citrixユニバーサルプリントドライバーを使用します。

  この動作は、Citrixポリシー設定「インボックスプリンタードライバーの自動インストール」を有効にし、ユニバーサル印刷設定を「要求されたドライバーが利用できない場合のみユニバーサル印刷を使用する」で構成することと同じです。

  「インボックスプリンタードライバーの自動インストール」を有効にすると、多数のネイティブプリンタードライバーのインストールにつながる可能性があります。

> **注：**
>
> 印刷の出荷時のデフォルト設定が不明な場合は、新しいポリシーを作成し、すべての印刷ポリシー規則を「有効」に設定して表示します。表示されるオプションがデフォルトです。

常時オンロギング

VDA上の印刷サーバーと印刷サブシステムで、常時オンロギング機能が利用可能です。

ログをZIP形式でまとめてメールで送信するため、またはCitrix Insight Servicesにログを自動的にアップロードするため、**Start-TelemetryUpload** PowerShellコマンドレットを使用します。

印刷ポリシーと設定

ユーザーが公開アプリケーションからプリンターにアクセスする場合、Citrix®ポリシーを構成して以下を指定できます。

- プリンターがプロビジョニングされる方法（またはセッションに追加される方法）
- 印刷ジョブがルーティングされる方法
- プリンタードライバーが管理される方法

異なるユーザーデバイス、ユーザー、またはポリシーがフィルターされるその他のオブジェクトに対して、異なる印刷構成を設定できます。

ほとんどの印刷機能は、Citrixの印刷ポリシー設定を通じて構成されます。印刷設定は、標準のCitrixポリシー動作に従います。

ユーザーのネットワークアカウントに十分な権限がある場合、システムはセッションの終了時にプリンター設定をプリンターオブジェクトまたはクライアント印刷デバイスに書き込むことができます。デフォルトでは、Citrix Workspace™ appは、設定や環境設定を他の場所で探す前に、セッション内のプリンターオブジェクトに保存されている設定を使用します。

デフォルトでは、システムはプリンタープロパティをユーザーデバイス（デバイスがサポートしている場合）またはMulti-session OSマシンのユーザープロファイルに保存または保持します。ユーザーがセッション中にプリンタープロパティを変更すると、それらの変更はマシンのユーザープロファイルに更新されます。次回ユーザーがログオンまたは再接続すると、ユーザーデバイスは保持されているそれらの設定を継承します。つまり、ユーザーデバイスでのプリンタープロパティの変更は、ユーザーがログオフして再度ログオンするまで、現在のセッションには影響しません。

印刷設定の場所

Windowsの印刷環境では、印刷設定への変更はローカルコンピューターまたはドキュメントに保存できます。この環境では、ユーザーが印刷設定を変更すると、設定は次の場所に保存されます。

- **ユーザーデバイス自体** - Windowsユーザーは、コントロールパネルでプリンターを右クリックし、「印刷設定」を選択することで、ユーザーデバイスのデバイス設定を変更できます。たとえば、ページ方向として「横」が選択されている場合、「横」はそのプリンターのデフォルトのページ方向設定として保存されます。
- **ドキュメント内** - ワープロプログラムやデスクトップパブリッシングプログラムでは、ページ方向などのドキュメント設定は、多くの場合ドキュメント内に保存されます。たとえば、ドキュメントを印刷キューに入れると、Microsoft Wordは通常、指定した印刷設定（ページ方向やプリンター名など）をドキュメント内に保存します。これらの設定は、次回そのドキュメントを印刷するときにデフォルトで表示されます。
- **ユーザーがセッション中に行った変更から** - システムは、自動作成されたプリンターの印刷設定への変更がセッション内のコントロールパネル（つまり、Multi-session OSマシン上）で行われた場合にのみ、その変更を保持します。
- **Multi-session OSマシン上** - これらは、マシン上の特定のプリンタードライバーに関連付けられているデフォルト設定です。

Windowsベースの環境で保持される設定は、ユーザーが変更を行った場所によって異なります。これは、スプレッドシートプログラムなどのある場所で表示される印刷設定が、ドキュメントなどの他の場所での設定と異なる場合があることも意味します。結果として、特定のプリンターに適用される印刷設定は、セッション中に変更される可能性があります。

ユーザーの印刷設定の階層

印刷設定は複数の場所に保存できるため、システムは特定の優先順位に従ってそれらを処理します。また、デバイス設定はドキュメント設定とは明確に区別され、通常はドキュメント設定よりも優先されることに注意することが重要です。

デフォルトでは、システムは他の設定を考慮する前に、ユーザーがセッション中に変更した印刷設定（つまり、保持された設定）を常に適用します。ユーザーが印刷すると、システムはMulti-session OSマシンに保存されているデフォルトのプリンター設定と、保持されているクライアントプリンター設定を結合して適用します。

ユーザーの印刷設定の保存

Citrixは、プリンタープロパティの保存場所を変更しないことを推奨します。ユーザーデバイスにプリンタープロパティを保存するデフォルト設定は、一貫した印刷プロパティを確保する最も簡単な方法です。システムがユーザーデバイスにプロパティを保存できない場合、自動的にMulti-session OSマシンのユーザープロファイルにフォールバックします。

次のシナリオが当てはまる場合は、「プリンタープロパティの保持」ポリシー設定を確認してください。

- ユーザーがユーザーデバイスにプリンタープロパティを保存することを許可しないレガシープラグインを使用している場合。
- Windowsネットワークで強制プロファイルを使用しており、ユーザーのプリンタープロパティを保持したい場合。

プリンターのプロビジョニング

Citrix Universal™ プリントサーバー

環境に最適な印刷ソリューションを決定する際には、次の点を考慮してください。

- Universal Print Serverは、Windows Print Providerでは利用できない機能（イメージとフォントのキャッシュ、高度な圧縮、最適化、QoSサポート）を提供します。
- Universal Print Driverは、Microsoftが定義するパブリックなデバイス非依存設定をサポートします。ユーザーがプリンタードライバーメーカー固有のデバイス設定にアクセスする必要がある場合、Universal Print ServerとWindowsネイティブドライバーの組み合わせが最適なソリューションとなる可能性があります。この構成により、Universal Print Serverの利点を維持しつつ、ユーザーに特殊なプリンター機能へのアクセスを提供できます。考慮すべきトレードオフとして、Windowsネイティブドライバーにはメンテナンスが必要です。
- Citrix Universal Print Serverは、ネットワークプリンターのユニバーサル印刷をサポートします。Universal Print Serverは、Multi-session OSマシン上の単一ドライバーであるUniversal Print Driverを使用し、シンクライアントやタブレットを含むあらゆるデバイスからのローカルまたはネットワーク印刷を可能にします。

Universal Print ServerをWindowsネイティブドライバーとともに使用するには、Universal Print Serverを有効にします。デフォルトでは、Windowsネイティブドライバーが利用可能な場合はそれが使用されます。そうでない場合は、Universal Print Driverが使用されます。Windowsネイティブドライバーのみを使用するか、Universal Print Driverのみを使用するかなど、この動作の変更を指定するには、Universal Print Driverの使用ポリシー設定を更新します。

Universal Print Serverのインストール

Universal Print Serverを使用するには、インストールドキュメントに記載されているとおり、UpsServerコンポーネントをプリントサーバーにインストールして構成します。詳しくは、コアコンポーネントのインストールおよびコマンドラインを使用したインストールを参照してください。

たとえば、**XenApp 6.5**など、UPClientコンポーネントを個別に展開したい環境の場合：

1. WindowsシングルセッションOSまたはWindowsマルチセッションOS用のCitrix Virtual Apps and Desktops™ Virtual Delivery Agent (VDA) スタンドアロンパッケージをダウンロードします。
2. コマンドラインを使用したインストールに記載されているコマンドライン手順を使用してVDAを抽出します。
3. `\Image-Full\Support\VcRedist_2013_RTM`から前提条件をインストールします
   - Vcredist_x64 / vcredist_x86
     - 32ビットのみの場合はx86を実行し、64ビット展開の場合は両方を実行します
4. `\Image-Full\x64\Virtual Desktop Components`または`\Image-Full\x86\Virtual Desktop Components`からcdfの前提条件をインストールします。
   - Cdf_x64 / Cdf_x86
     - 32ビット版はx86、64ビット版はx64
5. `\Image-Full\x64\Virtual Desktop Components`または`\Image-Full\x86\Virtual Desktop Components`でUPClientコンポーネントを見つけます。
6. UPClientコンポーネントを抽出し、そのMSIを起動してインストールします。
7. UPClientコンポーネントのインストール後、再起動が必要です。

Universal Print ServerのCEIPをオプトアウトする

Universal Print Serverをインストールすると、Citrix Customer Experience Improvement Program (CEIP) に自動的に登録されます。最初のデータアップロードは、インストール日時から7日後に実行されます。

CEIPをオプトアウトするには、レジストリキー**`HKLM\Software\Citrix\Universal Print Server\CEIPEnabled`を編集し、DWORD値を**0**に設定します。

再度オプトインするには、DWORD値を1に設定します。

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

詳しくは、Citrix Insight Servicesを参照してください。

ユニバーサルプリントサーバーの構成

Universal Print Serverを構成するには、以下のCitrixポリシー設定を使用します。詳しくは、画面上のポリシー設定ヘルプを参照してください。

- **Universal Print Serverを有効にする**。Universal Print Serverはデフォルトで無効になっています。Universal Print Serverを有効にすると、Universal Print Serverが利用できない場合にWindows Print Providerを使用するかどうかを選択できます。Universal Print Serverを有効にすると、ユーザーはWindows Print ProviderおよびCitrix Providerインターフェイスを介してネットワークプリンターを追加および列挙できるようになります。
- **Universal Print Server印刷データストリーム (CGP) ポート**。Universal Print Server印刷データストリームCGP (Common Gateway Protocol) リスナーが使用するTCPポート番号を指定します。デフォルトは**7229**です。
- **Universal Print Server ウェブサービス (HTTP/SOAP) ポート**。Universal Print Serverリスナーが受信HTTP/SOAP要求に使用するTCPポート番号を指定します。デフォルトは**8080**です。

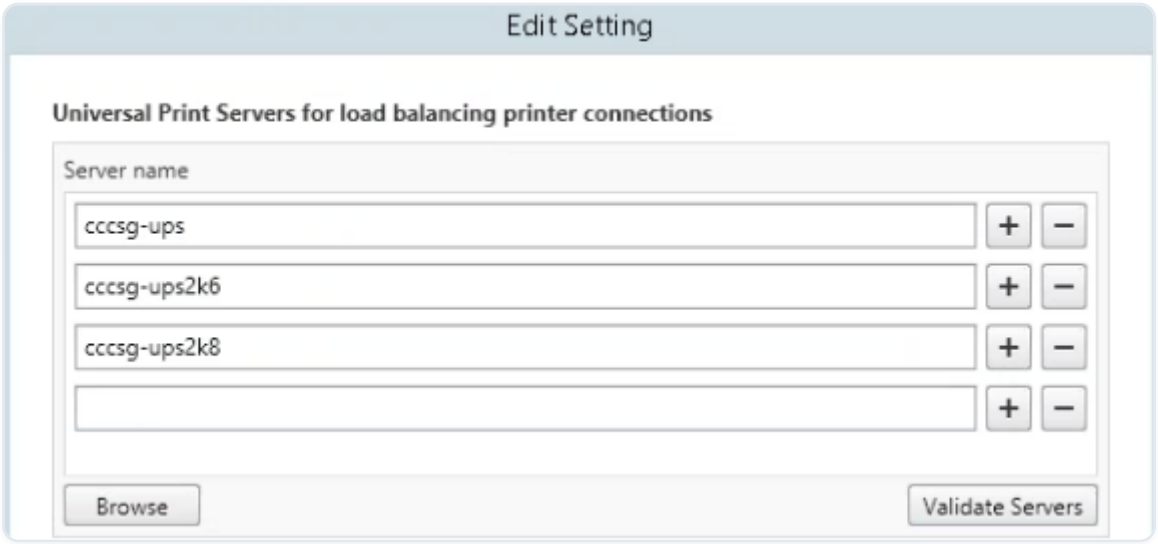
Citrix Virtual Apps and Desktops VDAへのUniversal Print Server通信のデフォルトポートであるHTTP 8080を変更するには、Universal Print Serverコンピューターで以下のレジストリを作成し、ポート番号の値を変更する必要があります。

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\PrintingPolicies`
"UpsHttpPort"=DWORD:\<portnumber\>

このポート番号は、StudioのHDXポリシー、Universal Print Server Webサービス (HTTP/SOAP) ポートと一致している必要があります。

- **Universal Print Server印刷ストリーム入力帯域幅制限 (kbps)**。各印刷ジョブからCGPを使用してUniversal Print Serverに配信される印刷データの転送速度の上限 (キロビット/秒) を指定します。デフォルトは0 (無制限) です。
- **負荷分散用のUniversal Print Server**。この設定では、他のCitrix印刷ポリシー設定を評価した後、セッション起動時に確立されたプリンター接続の負荷分散に使用するUniversal Print

Serverを一覧表示します。プリンター作成時間を最適化するために、Citrixはすべての印刷サーバーが同じ共有プリンターのセットを持つことを推奨します。



- **Universal Print Serverサービス停止しきい値**。ロードバランサーが、利用できない印刷サーバーが回復するまで待機する時間を指定します。この時間を過ぎると、サーバーが永続的にオフラインであると判断され、その負荷が他の利用可能な印刷サーバーに再分散されます。デフォルトは180 (秒) です。

Delivery Controller™で印刷ポリシーが変更されると、ポリシーの変更がVDAに適用されるまでに数分かかる場合があります。

他のポリシー設定との相互作用 - Universal Print Serverは、他のCitrix印刷ポリシー設定を尊重し、以下の表に示すようにそれらと相互作用します。提供される情報は、Universal Print Serverポリシー設定が有効になっており、Universal Print Serverコンポーネントがインストールされ、ポリシー設定が適用されていることを前提としています。

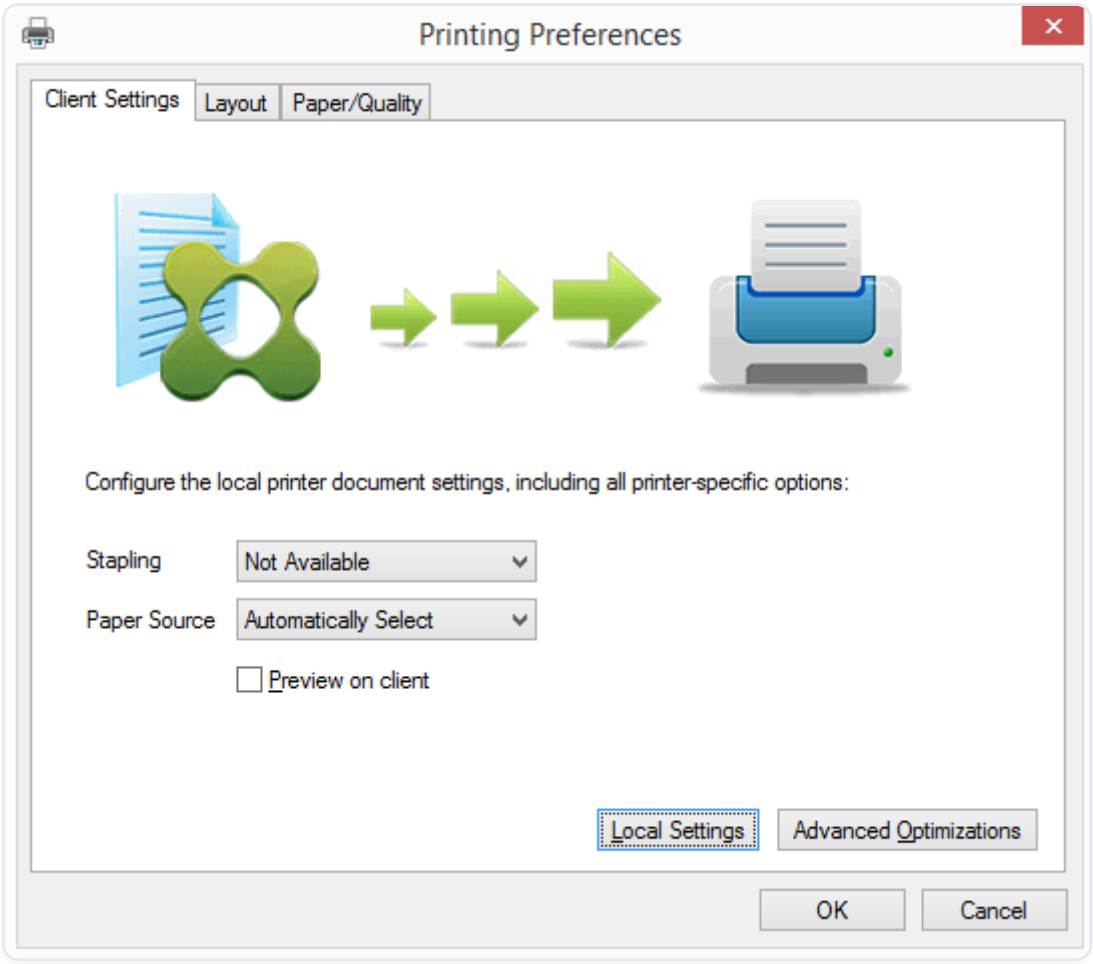
ポリシー設定	**相互作用**
クライアントプリンターリダイレクト、クライアントプリンターの自動作成	Universal Print Serverが有効になると、クライアントネットワークプリンターは、ネイティブドライバーではなくUniversal Print Driverを使用して作成されます。ユーザーには以前と同じプリンター名が表示されます。
セッションプリンター	Citrix Universal Print Serverソリューションを使用する場合、ユニバーサルプリントドライバーのポリシー設定が適用されます。

プリントサーバーへの直接接続	Universal Print Serverが有効で、ユニバーサルプリントドライバーの使用ポリシー設定がユニバーサル印刷のみを使用するように構成されている場合、ユニバーサルプリントドライバーを使用して、プリントサーバーへの直接ネットワークプリンター接続を作成できます。
UPDの優先設定	EMFおよびXPSドライバーをサポートします。

ユーザーインターフェイスへの影響 - Universal Print Serverで使用されるCitrix Universal Print Driverは、以下のユーザーインターフェイスコントロールを無効にします。

- プリンターのプロパティダイアログボックスの「ローカルプリンター設定」ボタン
- ドキュメントのプロパティダイアログボックスの「ローカルプリンター設定」および「クライアントでプレビュー」ボタン

Citrix Universal Print Driver（EMFおよびXPSドライバー）は、ステープルや給紙元などの高度な印刷機能をサポートしています。セッション内でUPDにマップされているクライアントまたはネットワークプリンターがこれらの機能をサポートしている場合、ユーザーはカスタムUPD印刷ダイアログからステープルまたは給紙元のオプションを選択できます。



ステープルやセキュアPINなどの非標準のプリンター設定を行うには、Citrix UPD EMFまたはXPSドライバーを使用するクライアントマッププリンターのカスタムUPD印刷ダイアログで、**ローカル設定**を選択します。マップされたプリンターの**印刷設定**ダイアログがセッション外のクライアントに表示され、ユーザーは任意のプリンターオプションを変更できます。変更されたプリンター設定は、そのドキュメントを印刷する際にアクティブなセッションで使用されます。

これらの機能は、ネイティブドライバーがMicrosoft Print Capabilityテクノロジーを使用して利用可能にしている場合に利用できます。ネイティブドライバーは、Print Capabilities XMLで標準化されたPrint Schema Keywordsを使用する必要があります。非標準のキーワードが使用されている場合、Citrix Universal Print Driverを使用しても高度な印刷機能は利用できません。

Universal Print Serverを使用する場合、Citrix Print Providerのプリンターの追加ウィザードは、Windows Print Providerのプリンターの追加ウィザードと同じですが、以下の例外があります。

- 名前またはアドレスでプリンターを追加する場合、プリントサーバーのHTTP/SOAPポート番号を指定できます。そのポート番号はプリンター名の一部となり、表示されます。
- Citrix Universal Print Driver使用ポリシー設定でユニバーサル印刷を使用する必要がある場合、プリンターを選択する際にユニバーサルプリントドライバー名が表示されます。Windows Print Providerはユニバーサルプリントドライバーを使用できません。

Citrix Print Providerはクライアント側レンダリングをサポートしていません。

Universal Print Serverの詳細については、CTX200328を参照してください。

自動作成されたクライアントプリンター

クライアントプリンターには、以下のユニバーサル印刷ソリューションが提供されます。

- **Citrix Universal Printer** - セッション開始時に作成される、印刷デバイスに紐付けられていない汎用プリンターです。Citrix Universal Printerは、ログオン時に利用可能なクライアントプリンターを列挙する必要がないため、リソース使用量を大幅に削減し、ユーザーのログオン時間を短縮できます。Universal Printerは、あらゆるクライアント側印刷デバイスに印刷できます。

  Citrix Universal Printerは、お使いの環境のすべてのユーザーデバイスまたはCitrix Workspace™アプリで動作しない場合があります。Citrix Universal PrinterはWindows環境を必要とし、Citrix Offline Plug-inやクライアントにストリーミングされるアプリケーションはサポートしていません。このような環境では、自動作成されたクライアントプリンターとユニバーサルプリントドライバーの使用を検討してください。

  Windows以外のCitrix Workspaceアプリでユニバーサル印刷ソリューションを使用するには、PostScript/PCLベースで自動的にインストールされる他のユニバーサルプリントドライバーのいずれかを使用してください。

- **Citrix Universal Print Driver** - デバイスに依存しないプリンタードライバーです。Citrix Universal Print Driverを構成すると、システムはデフォルトでEMFベースのUniversal Print Driverを使用します。

  Citrix Universal Print Driverは、古いまたは高度でないプリンタードライバーよりも小さい印刷ジョブを作成する可能性があります。ただし、特殊なプリンターの印刷ジョブを最適化するには、デバイス固有のドライバーが必要になる場合があります。

ユニバーサル印刷の構成 - ユニバーサル印刷を構成するには、以下のCitrixポリシー設定を使用します。詳細については、画面上のポリシー設定ヘルプを参照してください。

- ユニバーサルプリントドライバーの使用。ユニバーサル印刷を使用するタイミングを指定します。
- 汎用ユニバーサルプリンターの自動作成。ユニバーサル印刷と互換性のあるユーザーデバイスが使用されているセッションで、汎用Citrix Universal Printerオブジェクトの自動作成を有効または無効にします。デフォルトでは、汎用Universal Printerオブジェクトは自動作成されません。

- ユニバーサルドライバーの優先順位。システムがユニバーサルプリントドライバーを使用しようとする順序を、リストの最初のエントリから指定します。ドライバーの追加、編集、削除、およびリスト内のドライバーの順序変更が可能です。
- ユニバーサル印刷プレビューの優先順位。自動作成されたプリンターまたは汎用ユニバーサルプリンターに対して印刷プレビュー機能を使用するかどうかを指定します。
- ユニバーサル印刷EMF処理モード。Windowsユーザーデバイス上のEMFスプールファイルの処理方法を制御します。デフォルトでは、EMFレコードはプリンターに直接スプールされます。プリンターに直接スプールすることで、スプーラーはレコードをより速く処理し、CPUリソースの使用量を削減できます。

その他のポリシーについては、「印刷パフォーマンスの最適化」を参照してください。用紙サイズ、印刷品質、色、両面印刷、部数などの設定のデフォルトを変更するには、「CTX113148」を参照してください。

ユーザーデバイスからのプリンターの自動作成 - セッションの開始時に、システムはデフォルトでユーザーデバイス上のすべてのプリンターを自動作成します。ユーザーにプロビジョニングされるプリンターの種類を制御したり、自動作成を防止したりできます。

Citrixポリシー設定を使用します クライアントプリンターの自動作成を制御します。次のように指定できます。

- ネットワークプリンターやローカル接続プリンターを含む、ユーザーデバイスに表示されるすべてのプリンターが、各セッションの開始時に自動的に作成される（デフォルト）
- ユーザーデバイスに物理的に接続されているすべてのローカルプリンターが自動的に作成される
- ユーザーデバイスのデフォルトプリンターのみが自動的に作成される
- すべてのクライアントプリンターで自動作成が無効になる

「クライアントプリンターの自動作成」設定を使用するには、「クライアントプリンターのリダイレクト」設定が「許可」（デフォルト）になっている必要があります。

ユーザーへのネットワークプリンターの割り当て

デフォルトでは、ユーザーデバイス上のネットワークプリンターはセッションの開始時に自動的に作成されます。システムでは、各セッション内で作成するネットワークプリンターを指定することで、列挙およびマップされるネットワークプリンターの数を減らすことができます。このようなプリンターはセッションプリンターと呼ばれます。

IPアドレスでセッションプリンターポリシーをフィルターして、近接印刷を提供できます。近接印刷により、指定されたIPアドレス範囲内のユーザーは、その同じ範囲内に存在するネットワーク印刷デバイスに自動的にアクセスできます。近接印刷はCitrix Universal Print Serverによって提供され、このセクションで説明されている構成は必要ありません。

近接印刷には、次のシナリオが含まれる場合があります。

- 社内ネットワークは、ユーザーにIPアドレスを自動的に割り当てるDHCPサーバーで運用されています。
- 社内のすべての部門には、一意に指定されたIPアドレス範囲があります。
- ネットワークプリンターは、各部署のIPアドレス範囲内に存在します。

近接印刷が構成されており、従業員がある部署から別の部署に移動した場合、追加の印刷デバイス構成は不要です。ユーザーデバイスが新しい部署のIPアドレス範囲内で認識されると、その範囲内のすべてのネットワークプリンターにアクセスできるようになります。

セッションでリダイレクトする特定のプリンターを構成する - 管理者によって割り当てられたプリンターを作成するには、Citrixポリシー設定の「セッションプリンター」を構成します。次のいずれかの方法を使用して、そのポリシーにネットワークプリンターを追加します。

- `\\servername\printername`の形式を使用して、プリンターのUNCパスを入力します。
- ネットワーク上のプリンターの場所を参照します。
- 特定のサーバー上のプリンターを参照します。`\\servername`の形式を使用してサーバー名を入力し、「参照」をクリックします。

重要：サーバーは、適用されているすべてのポリシーの有効なセッションプリンター設定を、優先度の高いものから低いものへとマージします。プリンターが複数のポリシーオブジェクトで構成されている場合、カスタムのデフォルト設定は、そのプリンターが構成されている最も優先度の高いポリシーオブジェクトからのみ取得されます。

「セッションプリンター」設定で作成されたネットワークプリンターは、サブネットなどのオブジェクトでフィルタリングすることにより、セッションが開始された場所に応じて異なる場合があります。

セッションのデフォルトネットワークプリンターを指定する - デフォルトでは、ユーザーのメインプリンターがセッションのデフォルトプリンターとして使用されます。Citrixポリシー設定の「デフォルトプリンター」を使用して、セッションでユーザーデバイスのデフォルトプリンターがどのように確立されるかを変更します。

1. 「デフォルトプリンター設定」ページで、「クライアントのデフォルトプリンターを選択」の設定を選択します。

    - ネットワークプリンター名。「セッションプリンター」ポリシー設定で追加されたプリンターがこのメニューに表示されます。このポリシーのデフォルトとして使用するネットワークプリンターを選択します。
    - ユーザーのデフォルトプリンターを調整しない。デフォルトプリンターには、現在のターミナルサービスまたはWindowsユーザープロファイル設定を使用します。詳細については、画面上のポリシー設定ヘルプを参照してください。

2. 影響を与えたいユーザーグループ（またはその他のフィルターされたオブジェクト）にポリシーを適用します。

近接印刷を構成する - 近接印刷はCitrix Universal Print Serverによっても提供され、ここに記載されている構成は不要です。

1. 各サブネット（またはプリンターの場所に対応する）ごとに個別のポリシーを作成します。
2. 各ポリシーで、そのサブネットの地理的な場所にあるプリンターをSession printers設定に追加します。
3. Default printer設定を「ユーザーのデフォルトプリンターを調整しない」に設定します。
4. クライアントIPアドレスでポリシーをフィルターします。DHCP IPアドレス範囲の変更を反映するように、これらのポリシーを必ず更新してください。

印刷環境の維持

印刷環境の維持には、以下が含まれます。

- プリンタードライバーの管理
- 印刷パフォーマンスの最適化
- プリンターの表示と印刷キューの管理

プリンタードライバーの管理

管理オーバーヘッドとプリンタードライバーの問題の可能性を最小限に抑えるため、Citrixでは Citrix Universal™ Print Driverの使用を推奨しています。

自動作成が失敗した場合、デフォルトでは、システムはWindowsに付属のWindowsネイティブプリンタードライバーをインストールします。ドライバーが利用できない場合、システムは Universal Print Driverにフォールバックします。プリンタードライバーのデフォルト設定の詳細に

ついては、「ベストプラクティス、セキュリティに関する考慮事項、およびデフォルトの操作」を参照してください。

すべてのシナリオでCitrix Universal Print Driverが選択肢とならない場合、Multi-session OSマシンにインストールされるドライバーの数を最小限に抑えるために、プリンタードライバーをマップします。さらに、プリンタードライバーをマップすることで、次のことが可能になります。

- 指定されたプリンターがCitrix Universal Print Driverのみを使用できるようにする
- 指定されたドライバーでプリンターが作成されることを許可または防止する
- 古いドライバーや破損したドライバーを適切なプリンタードライバーに置き換える
- クライアントドライバー名に対して、Windowsサーバーで利用可能なドライバーを置き換える

プリンタードライバーの自動インストールを防止する - Multi-session OSマシン全体で一貫性を確保するために、プリンタードライバーの自動インストールを無効にする必要があります。これは、Citrix®ポリシー、Microsoftポリシー、またはその両方を通じて実現できます。Windowsネイティブプリンタードライバーの自動インストールを防止するには、Citrixポリシー設定「Automatic installation of in-box printer drivers」を無効にします。

クライアントプリンタードライバーをマップする - 各クライアントは、ログオン時にプリンタードライバー名を含むクライアント側プリンターに関する情報を提供します。クライアントプリンターの自動作成中に、クライアントから提供されたプリンターモデル名に対応するWindowsサーバープリンタードライバー名が選択されます。その後、自動作成プロセスは、識別された利用可能なプリンタードライバーを使用して、リダイレクトされたクライアント印刷キューを構築します。

マップされたクライアントプリンタードライバーのドライバー置換ルールを定義し、印刷設定を編集する一般的なプロセスは次のとおりです。

1. 自動作成されたクライアントプリンターのドライバー置換ルールを指定するには、Citrixポリシー設定の「プリンタードライバーのマッピングと互換性」を構成します。これには、クライアントプリンタードライバー名を追加し、「プリンタードライバーの検索」メニューから、クライアントプリンタードライバーの代わりに置換するサーバードライバーを選択します。この設定ではワイルドカードを使用できます。たとえば、すべてのHPプリンターに特定のドライバーを使用させるには、ポリシー設定で「HP*」と指定します。
2. プリンタードライバーを禁止するには、ドライバー名を選択し、「作成しない」設定を選択します。
3. 必要に応じて、既存のマッピングを編集したり、マッピングを削除したり、リスト内のドライバーエントリの順序を変更したりします。

4. マップされたクライアントプリンタードライバーの印刷設定を編集するには、プリンタードライバーを選択し、「設定」をクリックして、印刷品質、向き、色などの設定を指定します。プリンタードライバーがサポートしていない印刷オプションを指定した場合、そのオプションは無効になります。この設定は、ユーザーが以前のセッションで設定した保持されているプリンター設定を上書きします。
5. 特定のドライバーでのみ利用可能なプリンター機能があるため、Citrixはドライバーをマッピングした後、プリンターの動作を詳細にテストすることを推奨します。

ユーザーがログオンすると、システムはクライアントプリンターを設定する前に、クライアントプリンタードライバーの互換性リストをチェックします。

印刷パフォーマンスの最適化

印刷パフォーマンスを最適化するには、Universal Print ServerとUniversal Print Driverを使用します。以下のポリシーは、印刷の最適化と圧縮を制御します。

- ユニバーサル印刷の最適化のデフォルト。セッション用にユニバーサルプリンターが作成される際のデフォルト設定を指定します。
    - 希望する画質は、ユニバーサル印刷に適用されるデフォルトの画像圧縮制限を指定します。デフォルトでは、標準品質が有効になっており、ユーザーは標準または低品質の圧縮を使用してのみ画像を印刷できます。
    - ヘビーウェイト圧縮を有効にするは、希望する画質で設定された圧縮レベルを超えて帯域幅を削減するかどうかを有効または無効にします。画質は低下しません。デフォルトでは、ヘビーウェイト圧縮は無効になっています。
    - 画像とフォントのキャッシュ設定は、印刷ストリームに複数回出現する画像とフォントをキャッシュするかどうかを指定し、各固有の画像またはフォントがプリンターに一度だけ送信されるようにします。デフォルトでは、埋め込み画像とフォントはキャッシュされます。
    - 管理者以外のユーザーによるこれらの設定の変更を許可するかどうかは、ユーザーがセッション内でデフォルトの印刷最適化設定を変更できるかどうかを指定します。デフォルトでは、ユーザーはデフォルトの印刷最適化設定を変更できません。
- ユニバーサル印刷の画像圧縮制限。Universal Print Driverで印刷される画像に利用可能な最大品質と最小圧縮レベルを定義します。デフォルトでは、画像圧縮制限は「最高品質（ロスレス圧縮）」に設定されています。
- ユニバーサル印刷の印刷品質制限。セッションで印刷出力を生成するために利用可能な最大ドット/インチ（dpi）を指定します。デフォルトでは、制限は指定されていません。

デフォルトでは、ネットワークプリンター宛てのすべての印刷ジョブは、マルチセッションOSマシンからネットワーク経由で直接プリントサーバーにルーティングされます。ネットワークにかなりの遅延や帯域幅の制限がある場合は、ICA®接続経由で印刷ジョブをルーティングすることを検討してください。これを行うには、Citrixポリシー設定の「プリントサーバーへの直接接続」を無効にします。ICA接続経由で送信されるデータは圧縮されるため、WANを介してデータが転送される際の帯域幅消費が少なくなります。

印刷帯域幅を制限してセッションパフォーマンスを向上させる - マルチセッションOSマシンからユーザープリンターにファイルを印刷している間、特にユーザーが低速ネットワーク経由でサーバーにアクセスする場合、帯域幅の競合により、他の仮想チャネル（ビデオなど）のパフォーマンスが低下する可能性があります。このような劣化を防ぐために、ユーザー印刷で使用される帯域幅を制限できます。印刷のデータ転送速度を制限することで、HDX™データストリームでビデオ、キーストローク、マウスデータの転送により多くの帯域幅を利用できるようになります。

> **重要:**
>
> プリンターの帯域幅制限は、他のチャネルが使用されていない場合でも常に適用されます。
>
> 以下のCitrixポリシーの帯域幅プリンター設定を使用して、印刷帯域幅のセッション制限を構成します。サイトの制限を設定するには、Studioを使用してこのタスクを実行します。個々のサーバーの制限を設定するには、各マルチセッションOSマシンでWindowsのグループポリシー管理コンソールを使用してこのタスクを実行します。

- プリンターリダイレクト帯域幅制限設定は、印刷に利用可能な帯域幅をキロビット/秒 (kbps) で指定します。
- プリンターリダイレクト帯域幅制限パーセント設定は、印刷に利用可能な帯域幅を、利用可能な全体帯域幅のパーセンテージに制限します。

  注：プリンターリダイレクト帯域幅制限パーセント設定を使用して帯域幅をパーセンテージで指定するには、全体セッション帯域幅制限も有効にする必要があります。

  両方の設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

印刷帯域幅に関するリアルタイム情報を取得するには、Citrix Directorを使用します。

ユニバーサルプリントサーバーの負荷分散

ユニバーサルプリントサーバーソリューションは、負荷分散ソリューションにプリントサーバーを追加することで拡張できます。各VDAには独自のロードバランサーがあり、印刷負荷をすべてのプリントサーバーに分散するため、単一障害点はありません。

ポリシー設定の負荷分散用ユニバーサルプリントサーバーとユニバーサルプリントサーバーのサービス停止しきい値を使用して、負荷分散ソリューション内のすべてのプリントサーバーに印刷負荷を分散します。

プリントサーバーに予期せぬ障害が発生した場合、各VDAのロードバランサーのフェイルオーバーメカニズムは、障害が発生したプリントサーバーに割り当てられていたプリンター接続を他の利用可能なプリントサーバーに自動的に再分散します。これにより、既存および新規のすべてのセッションは、ユーザーエクスペリエンスに影響を与えることなく、また管理者の即時介入を必要とせずに正常に機能します。

管理者は、一連のパフォーマンスカウンターを使用して、負荷分散されたプリントサーバーのアクティビティを監視し、VDAで以下を追跡できます。

- VDA上の負荷分散されたプリントサーバーのリストとその状態（利用可能、利用不可）
- 各プリントサーバーが受け入れたプリンター接続の数
- 各プリントサーバーで失敗したプリンター接続の数
- 各プリントサーバーでのアクティブなプリンター接続の数
- 各プリントサーバーでの保留中のプリンター接続の数

印刷キューの表示と管理

次の表は、環境内でプリンターを表示し、印刷キューを管理できる場所をまとめたものです。

	印刷パス	場所
クライアントプリンター（ユーザーデバイスに接続されているプリンター）	クライアント印刷パス	UAC有効時: Microsoft Management Console にある印刷の管理スナップイン; UAC無効時: Windows 8より前: コントロールパネル、Windows 8: 印刷の管理スナップイン

	印刷パス	場所
ネットワークプリンター（ネットワークプリントサーバー上のプリンター）	ネットワーク印刷パス	UAC有効時: プリントサーバー \> Microsoft Management Console にある印刷の管理スナップイン; UAC無効時: プリントサーバー \> コントロールパネル
ネットワークプリンター（ネットワークプリントサーバー上のプリンター）	クライアント印刷パス	UAC有効時: プリントサーバー \> Microsoft Management Console にある印刷の管理スナップイン; UAC無効時: Windows 8より前: コントロールパネル、Windows 8: 印刷の管理スナップイン
ローカルネットワークサーバープリンター (ネットワークプリントサーバーからマルチセッションOSマシンに追加されたプリンター)	ネットワーク印刷経路	UAC有効時: 印刷サーバー \> コントロールパネル; UAC無効時: 印刷サーバー \> コントロールパネル

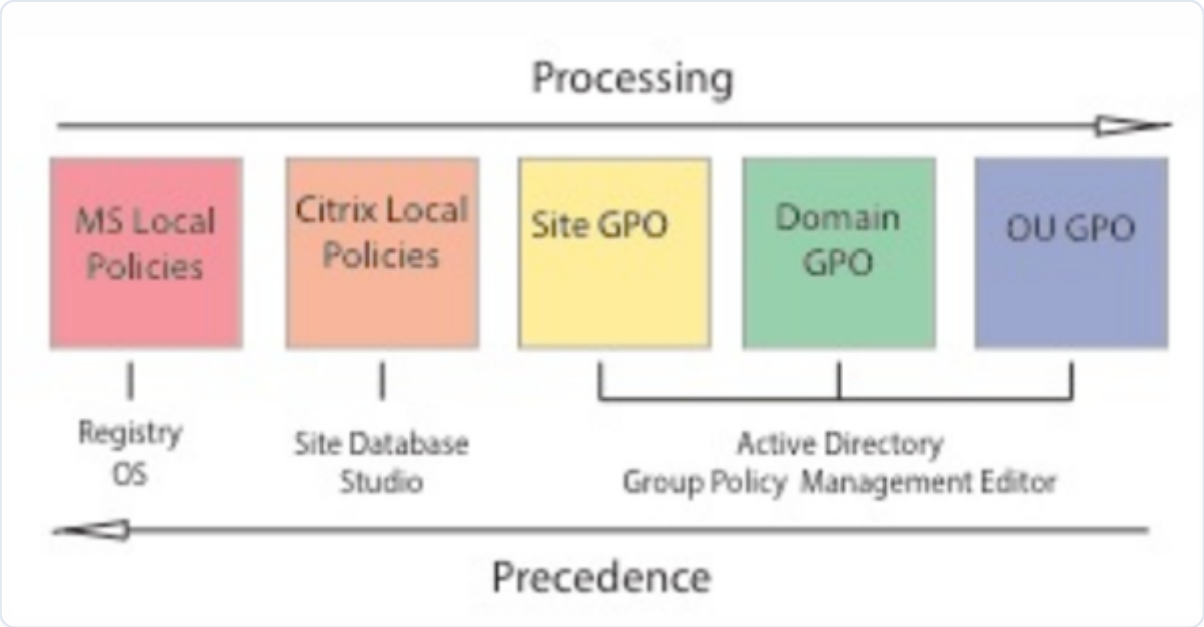
注：

ネットワーク印刷経路を使用するネットワークプリンターの印刷キューはプライベートであり、システムを通じて管理できません。

ポリシー

ポリシーは、ユーザー、デバイス、または接続タイプのグループに対して、セッション、帯域幅、およびセキュリティがどのように管理されるかを定義する設定の集合です。

ポリシー設定は、物理マシンおよび仮想マシン、またはユーザーに適用できます。設定は、ローカルレベルの個々のユーザー、またはActive Directoryのセキュリティグループに適用できます。構成は特定の基準とルールを定義します。ポリシーを明示的に割り当てない場合、設定はすべての接続に適用されます。



ポリシーはネットワークのさまざまなレベルに適用できます。組織単位GPOレベルに配置されたポリシー設定は、ネットワーク上で最も高い優先順位を持ちます。ドメインGPOレベルのポリシーは、サイトグループポリシーオブジェクトレベルのポリシーを上書きします。サイトグループポリシーオブジェクトレベルは、MicrosoftおよびCitrixローカルポリシーレベルの両方における競合するポリシーを上書きします。

すべてのCitrixローカルポリシーは、Citrix Studioコンソールで作成および管理され、サイトデータベースに保存されます。グループポリシーは、Microsoftグループポリシー管理コンソール (GPMC) を使用して作成および管理され、Active Directoryに保存されます。Microsoftローカルポリシーは、Windowsオペレーティングシステムで作成され、レジストリに保存されます。

Studioは、モデリングウィザードを使用して、管理者がテンプレートとポリシー内の構成設定を比較し、競合する設定や冗長な設定を排除するのに役立ちます。管理者はGPMCを使用してGPOを

設定し、設定を構成できます。また、それらをネットワークのさまざまなレベルのターゲットユーザーセットに適用することもできます。

これらのGPOはActive Directoryに保存されます。これらの設定の管理へのアクセスは、セキュリティ上の理由からほとんどのIT担当者に対して制限されています。

設定は、優先順位とその条件に従ってマージされます。無効な設定は、下位の有効な設定を上書きします。未構成のポリシー設定は無視され、下位の設定を上書きしません。

ローカルポリシーは、Active Directory内のグループポリシーと競合することもあり、状況によっては互いに上書きし合う可能性があります。

すべてのポリシーは次の順序で処理されます。

1. エンドユーザーはドメイン資格情報を使用してマシンにログオンします。
2. 資格情報はドメインコントローラーに送信されます。
3. Active Directoryはすべてのポリシー（エンドユーザー、エンドポイント、組織単位、およびドメイン）を適用します。
4. エンドユーザーはCitrix Workspace™アプリにログオンし、アプリケーションまたはデスクトップにアクセスします。
5. CitrixおよびMicrosoftのポリシーは、エンドユーザーとリソースをホストするマシンに対して処理されます。
6. Active Directoryはポリシー設定の優先順位を決定します。その後、それらをエンドポイントデバイスのレジストリと、リソースをホストするマシンに適用します。
7. エンドユーザーがリソースからログオフします。エンドユーザーおよびエンドポイントデバイスに対するCitrixポリシーは、アクティブではなくなります。
8. エンドユーザーがユーザーデバイスからログオフすると、GPOユーザーポリシーが解放されます。
9. エンドユーザーがデバイスの電源を切ると、GPOマシンポリシーが解放されます。

ユーザー、デバイス、マシンのグループに対してポリシーを作成する場合、一部のメンバーは異なる要件を持つ可能性があり、一部のポリシー設定に例外が必要になる場合があります。例外は、ポリシーが誰または何に影響するかを決定するStudioおよびGPMCのフィルターによって作成されます。

> **注:** 同じGPOでWindowsポリシーとCitrixポリシーを混在させることはサポートされていません。

ポリシーの操作

ユーザーアクセスとセッション環境を制御するためにCitrix®ポリシーを構成します。Citrixポリシーは、接続、セキュリティ、帯域幅の設定を制御する最も効率的な方法です。特定のユーザーグループ、デバイス、または接続の種類に対してポリシーを作成できます。各ポリシーには複数の設定を含めることができます。

Citrixポリシーを操作するためのツール

Citrixポリシーでは、次のツールを使用できます。

- **Studio** - グループポリシーを管理する権限のないCitrix管理者の場合は、Studioを使用してサイトのポリシーを作成します。Studioを使用して作成されたポリシーは、サイトデータベースに保存されます。更新は、仮想デスクトップがブローカーに登録されたとき、またはユーザーがその仮想デスクトップに接続したときに、仮想デスクトップにプッシュされます。
- **ローカルグループポリシーエディター**（Microsoft管理コンソールスナップイン） - ネットワーク環境でActive Directoryを使用しており、グループポリシーを管理する権限がある場合は、ローカルグループポリシーエディターを使用してサイトのポリシーを作成できます。構成する設定は、グループポリシー管理コンソールで指定するグループポリシーオブジェクト（GPO）に影響します。

> **重要:**
>
> ローカルグループポリシーエディターを使用して、一部のポリシー設定を構成します。これらのポリシー設定には、VDAをコントローラーに登録することに関連する設定が含まれます。また、Microsoft App-Vサーバーに関連する設定も含まれます。

ポリシーの処理順序と優先順位

グループポリシー設定は、次の順序で処理されます。

1. ローカルGPO
2. XenAppまたはXenDesktop®サイトGPO（サイトデータベースに保存）
3. サイトレベルのGPO
4. ドメインレベルのGPO
5. 組織単位

ただし、競合が発生した場合、最後に処理されたポリシー設定が、以前に処理された設定を上書きします。この構成は、ポリシー設定が次の順序で優先されることを意味します。

1. 組織単位
2. ドメインレベルのGPO
3. サイトレベルのGPO
4. XenApp®またはXenDesktopサイトGPO（サイトデータベースに保存）
5. ローカルGPO

たとえば、Citrix管理者はStudioを使用して、会社の営業担当者向けにクライアントファイルリダイレクトを有効にするポリシー（ポリシーA）を作成します。一方、別の管理者はグループポリシーエディターを使用して、営業担当者向けにクライアントファイルリダイレクトを無効にするポリシー（ポリシーB）を作成します。営業担当者が仮想デスクトップにログオンすると、ポリシーBが適用され、ポリシーAは無視されます。その理由は、ポリシーBがドメインレベルで処理され、ポリシーAがXenAppまたはXenDesktopサイトGPOレベルで処理されたためです。

ただし、ユーザーがICA®またはリモートデスクトッププロトコル（RDP）セッションを起動すると、Citrixセッション設定は、Active Directoryポリシーまたはリモートデスクトップセッションホスト構成を使用して構成された同じ設定を上書きします。この設定には、一般的なRDPクライアント接続設定に関連する設定が含まれます。RDPクライアント接続設定の例としては、デスクトップの壁紙、メニューアニメーション、ドラッグ中のウィンドウコンテンツの表示などがあります。

複数のポリシーを使用する場合、競合する設定を含むポリシーに優先順位を付けることができます。詳細については、「ポリシーの比較、優先順位付け、モデル化、およびトラブルシューティング」を参照してください。

Citrixポリシーのワークフロー

ポリシーを構成するプロセスは次のとおりです。

1. ポリシーを作成します。
2. ポリシー設定を構成します。
3. ポリシーをマシンオブジェクトとユーザーオブジェクトに割り当てます。
4. ポリシーに優先順位を付けます。
5. Citrixグループポリシーモデリングウィザードを実行して、有効なポリシーを確認します。

> **注：**

> Citrixグループポリシーモデリングウィザードを開くには、**［ポリシー］>［モデリング］タブに移動し、［操作］ペインで［モデリングウィザードの起動］をクリックします。**［モデリング］**タブは、Citrix Cloudでホストされ ているStudioでは使用できません。

Citrixポリシーと設定のナビゲート

ローカルグループポリシーエディターでは、ポリシーと設定は「コンピューターの構成」と「ユーザーの構成」の2つのカテゴリに表示されます。各カテゴリにはCitrixポリシーノードがあります。このスナップインのナビゲートと使用の詳細については、Microsoftのドキュメントを参照してください。

Studioでは、ポリシー設定は、影響を与える機能または特徴に基づいてカテゴリに分類されます。たとえば、**［プロファイル管理］**セクションには、プロファイル管理のポリシー設定が含まれています。

- コンピューター設定（マシンに適用されるポリシー設定）は、仮想デスクトップの動作を定義し、仮想デスクトップの起動時に適用されます。これらの設定は、仮想デスクトップでアクティブなユーザーセッションがない場合でも適用されます。ユーザー設定は、ICAを使用して接続する際のユーザーエクスペリエンスを定義します。ユーザーポリシーは、ユーザーがICAを使用して接続または再接続するときに適用されます。ユーザーがRDPを使用して接続したり、コンソールに直接ログオンしたりする場合、ユーザーポリシーは適用されません。

  ポリシー、設定、またはテンプレートにアクセスするには、Studioナビゲーションペインで を選択します。

  - タブには、すべてのポリシーが一覧表示されます。ポリシーを選択すると、右側に次のタブが表示されます。
    - 概要（名前、優先度、有効/無効の状態、説明）
    - 設定（構成された設定のリスト）
    - 割り当て先（ポリシーが割り当てられているユーザーおよびマシンオブジェクト）。詳しくは、「ポリシーの作成」を参照してください。
  - タブには、Citrixが提供するテンプレートと、作成したカスタムテンプレートが一覧表示されます。テンプレートを選択すると、右側に次のタブが表示されます。
    - 説明（テンプレートを使用する理由）

    - 設定（構成された設定のリスト）。 詳しくは、「ポリシーテンプレート」を参照してください。

  - タブでは、ポリシーまたはテンプレートの設定を、他のポリシーまたはテンプレートの設定と比較できます。たとえば、ベストプラクティスへの準拠を確実にするために、設定値を確認したい場合があります。詳しくは、「ポリシーの比較、優先順位付け、モデル化、およびトラブルシューティング」を参照してください。
  - タブから、Citrixポリシーを使用した接続シナリオをシミュレートできます。詳しくは、「ポリシーの比較、優先順位付け、モデル化、およびトラブルシューティング」を参照してください。

    > **注：**
    >
    > Citrix Cloudでホストされ ているStudioでは、 タブは使用できません。

  ポリシーまたはテンプレートで設定を検索するには：

  a. ポリシーまたはテンプレートを選択します。
  b. ペインで または を選択します。
  c. ［設定］ページで、設定の名前を入力し始めます。

  検索は、以下を選択して絞り込むことができます。

  - 特定の製品バージョン
  - カテゴリ（例：帯域幅）
  - ［選択済みのみ表示］チェックボックス
  - 選択したポリシーに追加された設定のみを検索する場合。

  フィルターなしで検索するには、**［すべての設定］**を選択します。

- ポリシー内で設定を検索するには：

  a. ポリシーを選択します。
  b. **［設定］**タブを選択し、設定の名前を入力します。

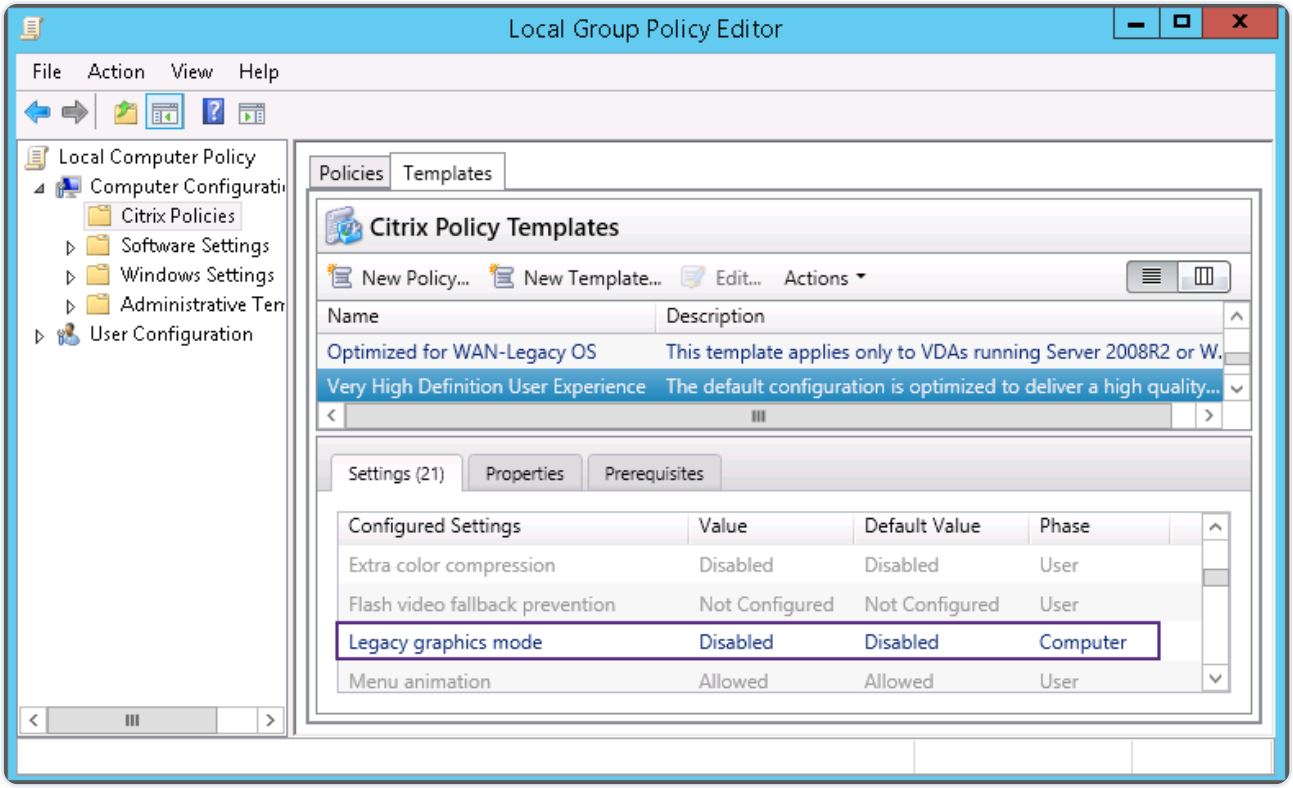
特定の製品バージョンを選択するか、カテゴリを選択して検索を絞り込むことができます。フィルターなしで検索するには、**［すべての設定］**を選択します。

ポリシーは、一度作成されると、使用されたテンプレートとは独立します。新しいポリシーの**［説明］**フィールドを使用して、使用されたソーステンプレートを追跡できます。

Studioでは、ポリシーとテンプレートは、ユーザー設定、コンピューター設定、またはその両方の種類のいずれが含まれているかに関係なく、単一のリストに表示されます。また、ポリシーとテンプレートの両方を、ユーザーフィルターとコンピューターフィルターの両方を使用して適用できます。

グループポリシーエディターでは、コンピューター設定とユーザー設定は、両方の種類の両方の設定を含むテンプレートから作成された場合でも、個別に適用する必要があります。この例では、コンピューターの構成で「非常に高精細なユーザーエクスペリエンス」を使用することを選択しています。

- レガシーグラフィックモードは、このテンプレートから作成されたポリシーで使用されるコンピューター設定です。
- グレー表示されているユーザー設定は、このテンプレートから作成されたポリシーでは使用されません。



ポリシーテンプレート

テンプレートは、事前定義された開始点からポリシーを作成するためのソースです。特定の環境やネットワーク条件に合わせて最適化されたCitrix®の組み込みテンプレートは、次のように使用できます。

- サイト間で共有する独自のポリシーとテンプレートを作成するためのソース。
- 展開間の結果をより簡単に比較するための参照。たとえば、「...Citrixテンプレートxまたはyを使用する場合...」のように結果を引用できます。
- テンプレートをインポートまたはエクスポートすることで、Citrixサポートまたは信頼できるサードパーティとポリシーを伝達する方法。

ポリシーテンプレートはインポートおよびエクスポートできます。

テンプレートを使用してポリシーを作成する際の考慮事項については、Knowledge Centerの記事CTX202330を参照してください。PDFをダウンロードするには、資格情報を使用してログインしてください。

組み込みのCitrixテンプレート

次のポリシーテンプレートが利用可能です。

- **非常に高精細なユーザーエクスペリエンス**。このテンプレートは、ユーザーエクスペリエンスを最大化するデフォルト設定を適用します。複数のポリシーが優先順位に従って処理されるシナリオでこのテンプレートを使用します。
- **高サーバー拡張性**。サーバーリソースを節約するためにこのテンプレートを適用します。このテンプレートは、ユーザーエクスペリエンスとサーバーの拡張性のバランスを取ります。単一サーバーでホストできるユーザー数を増やしながら、優れたユーザーエクスペリエンスを提供します。このテンプレートは、グラフィックの圧縮にビデオコーデックを使用せず、サーバー側のマルチメディアレンダリングを防止します。
- **高サーバー拡張性 - レガシーOS**。この高サーバー拡張性テンプレートは、Windows Server 2008 R2またはWindows 7以前を実行しているVDAにのみ適用されます。このテンプレートは、これらのオペレーティングシステムにより効率的なレガシーグラフィックモードに依存しています。
- **NetScaler SD-WANに最適化**。Citrix Virtual Desktopsの配信を最適化するためにNetScaler SD-WANを使用している支社のユーザーにこのテンプレートを適用します。(NetScaler SD-WANはCloudBridgeの新しい名称です)。
- **WAN向けに最適化**。このテンプレートは、共有WAN接続を使用する支社のタスクワーカー、またはグラフィックがシンプルなユーザーインターフェイスと少ないマルチメディアコンテンツのアプリケーションにアクセスする低帯域幅接続のリモートロケーション向けです。このテンプレートは、帯域幅効率を最適化するために、ビデオ再生エクスペリエンスと一部のサーバー拡張性を犠牲にします。
- **WAN向けに最適化 - レガシーOS**。この*WAN向けに最適化*テンプレートは、Windows Server 2008 R2またはWindows 7以前を実行しているVDAにのみ適用されます。このテンプレート

は、これらのオペレーティングシステムにより効率的なレガシーグラフィックモードに依存しています。

- **セキュリティと制御**。リスク許容度が低い環境でこのテンプレートを使用し、Citrix Virtual Apps and Desktopsでデフォルトで有効になっている機能を最小限に抑えます。このテンプレートには、ユーザーデバイスでの印刷、クリップボード、周辺機器、ドライブマッピング、ポートリダイレクト、Flashアクセラレーションへのアクセスを無効にする設定が含まれています。このテンプレートを適用すると、より多くの帯域幅を使用し、サーバーあたりのユーザー密度が減少する可能性があります。

組み込みのCitrixテンプレートをデフォルト設定で使用することをお勧めしますが、特定の推奨値がない設定もあります。たとえば、WAN向けに最適化テンプレートに含まれる**セッション全体の帯域幅制限**などです。この場合、テンプレートは設定を公開し、管理者がこの設定がシナリオに適用される可能性が高いことを理解できるようにします。

テンプレートのデフォルト設定画像(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/template-default-settings.png)

XenApp and XenDesktop 7.6 FP3より前の展開（ポリシー管理とVDA）を使用しており、High Server ScalabilityおよびOptimized for WANテンプレートが必要な場合は、該当するレガシーOSバージョンのこれらのテンプレートを使用してください。

> **注：**
>
> Citrixは組み込みテンプレートを作成および更新します。これらのテンプレートは変更または削除できません。

Studioを使用したテンプレートの作成と管理

テンプレートに基づいてテンプレートを作成するには：

1. Studioナビゲーションペインで**［ポリシー］**を選択します。
2. **［テンプレート］**タブを選択し、テンプレートを作成する元のテンプレートを選択します。
3. 操作ペインで**［テンプレートの作成］**を選択します。
4. テンプレートに含めるポリシー設定を選択して構成します。不要な既存の設定は削除します。テンプレートの名前を入力します。

［完了］をクリックすると、新しいテンプレートが［テンプレート］**タブに表示されます。

ポリシーに基づいてテンプレートを作成するには：

1. Studioナビゲーションペインで**［ポリシー］**を選択します。
2. **［ポリシー］**タブを選択し、テンプレートを作成する元のポリシーを選択します。
3. 操作ペインで**［テンプレートとして保存］**を選択します。
4. テンプレートに含める新しいポリシー設定を選択して構成します。不要な既存の設定は削除します。テンプレートの名前と説明を入力し、**［完了］**をクリックします。

テンプレートをインポートするには：

1. Studioナビゲーションペインで**［ポリシー］**を選択します。
2. 「**テンプレート**」タブを選択し、「**テンプレートのインポート**」を選択します。
3. インポートするテンプレートファイルを選択し、「**開く**」をクリックします。既存のテンプレートと同じ名前のテンプレートをインポートする場合、既存のテンプレートを上書きするか、自動的に生成される別の名前でテンプレートを保存するかを選択できます。

テンプレートをエクスポートするには：

1. Studioナビゲーションペインで「**ポリシー**」を選択します。
2. 「**テンプレート**」タブを選択し、「**テンプレートのエクスポート**」を選択します。
3. テンプレートを保存する場所を選択し、「**保存**」をクリックします。

指定した場所に`.gpt`ファイルが作成されます。

グループポリシーエディターを使用したテンプレートの作成と管理

グループポリシーエディターから、コンピューターの構成またはユーザーの構成を展開します。「**ポリシー**」ノードを展開し、「**Citrixポリシー**」を選択します。適切なアクションを選択します。

タスク	手順
既存のポリシーからテンプレートを作成する	「**ポリシー**」タブで、ポリシーを選択し、「**アクション > テンプレートとして保存**」を選択します。
既存のテンプレートからポリシーを作成する	**テンプレート**タブでテンプレートを選択し、**新しいポリシー**をクリックします。

タスク	手順
既存のテンプレートからテンプレートを作成する	「**テンプレート**」タブで、テンプレートを選択し、「**新しいテンプレート**」をクリックします。
テンプレートをインポートする	「**テンプレート**」タブで、「**アクション > インポート**」を選択します。
テンプレートをエクスポートする	**テンプレート**タブで、**アクション > エクスポート**を選択します。
テンプレート設定を表示する	**テンプレート**タブでテンプレートを選択し、**設定**タブをクリックします。
テンプレートプロパティの概要を表示する	**テンプレート**タブでテンプレートを選択し、**プロパティ**タブをクリックします。
テンプレートの前提条件を表示する	**テンプレート**タブでテンプレートを選択し、**前提条件**タブをクリックします。

テンプレートと委任管理

ポリシーテンプレートは、ポリシー管理パッケージがインストールされているマシンに保存されます。このマシンは、Delivery Controllerマシンまたはグループポリシーオブジェクト管理マシンのいずれかであり、Citrix Virtual Apps and Desktopsサイトのデータベースではありません。これは、サイトの委任管理ロールとスコープではなく、Windowsの管理権限がポリシーテンプレートファイルを制御することを意味します。

その結果、サイトで読み取り専用権限を持つ管理者は、たとえばテンプレートを作成できます。ただし、テンプレートはローカルファイルであるため、環境に変更は加えられません。

カスタムテンプレートは、それらを作成したユーザーアカウントにのみ表示され、ユーザーのWindowsプロファイルに保存されます。カスタムテンプレートをさらに公開するには、それからポリシーを作成するか、共有場所にエクスポートします。

ポリシーの作成

ポリシーを作成する前に、それが影響を与える可能性のあるユーザーまたはデバイスのグループを決定します。ユーザーの職務、接続タイプ、ユーザーデバイス、または地理的な場所に基づいてポ

リシーを作成することもできます。Windows Active Directoryグループポリシーで使用するのと同じ基準を使用することもできます。

すでにグループに適用されるポリシーを作成している場合は、別のポリシーを作成するのではなく、そのポリシーを編集することを検討してください。ポリシーを編集した後、適切な設定を構成します。特定の機能を有効にするためだけ、または特定のユーザーにポリシーが適用されないようにするためだけにポリシーを作成することは避けてください。

ポリシーを作成する際、ポリシーテンプレートの設定に基づいて作成し、必要に応じて設定をカスタマイズできます。テンプレートを使用せずに、必要なすべての設定を追加して作成することもできます。

Citrix Studioでは、**ポリシーを有効にする**チェックボックスが明示的にオンになっていない限り、新しく作成されたポリシーは無効に設定されます。

ポリシー設定

ポリシー設定は、有効、無効、または未構成にできます。デフォルトでは、ポリシー設定は構成されていません。つまり、ポリシーに追加されていません。設定は、ポリシーに追加された場合にのみ適用されます。

一部のポリシー設定は、次のいずれかの状態になります。

- 「許可」または「禁止」は、設定によって制御されるアクションを許可または防止します。セッション内でユーザーが設定のアクションを管理することを許可または防止する場合があります。たとえば、メニューアニメーション設定が「許可」に設定されている場合、ユーザーはクライアント環境でメニューアニメーションを制御できます。
- 「有効」または「無効」は、設定をオンまたはオフにします。設定を無効にすると、下位ランクのポリシーでは有効になりません。

さらに、一部の設定は、依存する設定の有効性を制御します。たとえば、クライアントドライブリダイレクトは、ユーザーがデバイス上のドライブにアクセスできるかどうかを制御します。ユーザーがネットワークドライブにアクセスできるようにするには、この設定と「**クライアントネットワークドライブ**」設定の両方をポリシーに追加する必要があります。「**クライアントドライブリダイレクト**」設定が無効になっている場合、「**クライアントネットワークドライブ**」設定が有効になっていても、ユーザーはネットワークドライブにアクセスできません。

一般に、マシンに影響を与えるポリシー設定の変更は、仮想デスクトップが再起動したとき、またはユーザーがログオンしたときに有効になります。ユーザーに影響を与えるポリシー設定の変更は、ユーザーが次回ログオンしたときに有効になります。Active Directoryを使用している場合、ポリシー設定はActive Directoryが90分間隔でポリシーを再評価するときに更新されます。そし

て、ポリシー設定は、仮想デスクトップが再起動したとき、またはユーザーがログオンしたときに適用されます。

一部のポリシー設定では、設定をポリシーに追加するときに値を入力または選択できます。「デフォルト値を使用」を選択することで、設定の構成を制限できます。この選択により、設定の構成が無効になり、ポリシーが適用されるときに設定のデフォルト値のみが使用されるようになります。この選択は、「デフォルト値を使用」を選択する前に入力された値とは関係ありません。

ベストプラクティスとして:

- ポリシーは個々のユーザーではなく、グループに割り当ててください。グループにポリシーを割り当てると、グループにユーザーを追加または削除したときに、割り当てが自動的に更新されます。
- リモートデスクトップセッションホスト構成で、競合する設定や重複する設定を有効にしないでください。リモートデスクトップセッションホスト構成は、Citrixポリシー設定と同様の機能を提供することがあります。トラブルシューティングを容易にするため、可能な限りすべての設定を一貫性のある状態（有効または無効）に保ってください。
- 使用されていないポリシーは無効にしてください。設定が追加されていないポリシーは、不要な処理を生成します。

ポリシーの割り当て

ポリシーを作成する際、特定のユーザーおよびマシンオブジェクトに割り当てます。そのポリシーは、特定の基準またはルールに従って接続に適用されます。一般に、基準の組み合わせに基づいて、ポリシーに任意の数の割り当てを追加できます。割り当てを指定しない場合、ポリシーはすべての接続に適用されます。

次の表に、利用可能な割り当てを示します。

割り当て名	ポリシーの適用基準
アクセスコントロール	クライアントが接続しているアクセス制御条件。*接続の種類* - NetScaler® Gatewayを使用する接続と使用しない接続のどちらにポリシーを適用するか。*NetScaler Gatewayファーム名* - NetScaler Gateway仮想サーバーの名前。*アクセス条件* - 使用するエンドポイント分析ポリシーまたはセッションポリシーの名前。

割り当て名	ポリシーの適用基準
NetScaler SD-WAN	ユーザーセッションがNetScaler SD-WANを介して起動されるかどうか。**注:** 1つのポリシーにNetScaler SD-WANの割り当てを1つだけ追加できます。
クライアントIPアドレス	セッションへの接続に使用されるユーザーデバイスのIPアドレス: IPv4の例: 12.0.0.0, 12.0.0.*, 12.0.0.1-12.0.0.70, 12.0.0.1/24; IPv6の例: 2001:0db8:3c4d:0015:0:0:abcd:ef12, 2001:0db8:3c4d:0015::/54
クライアント名	ユーザーデバイスの名前。完全一致: ClientABCName。ワイルドカードの使用: Client*Name。
デリバリーグループ	デリバリーグループのメンバーシップ。
デリバリーグループの種類	デスクトップまたはアプリケーションの種類: プライベートデスクトップ、共有デスクトップ、プライベートアプリケーション、または共有アプリケーション。**注:** プライベートデスクトップと共有デスクトップのフィルターオプションは、Citrix Virtual Apps and Desktops 7.xでのみ利用可能です。詳細については、CTX219153を参照してください。
組織単位 (OU)	組織単位。
タグ	タグ。**注:** このポリシーをすべてのタグ付きマシンに適用します。アプリケーションタグは含まれません。
ユーザーまたはグループ	ユーザーまたはグループ名。

ユーザーがログオンすると、接続の割り当てに一致するすべてのポリシーが特定されます。これらのポリシーは優先順位順に並べ替えられ、設定の複数のインスタンスが比較されます。各設定は、ポリシーの優先順位に従って適用されます。無効になっているポリシー設定は、有効になっている下位ランクの設定よりも優先されます。構成されていないポリシー設定は無視されます。

重要:

> Group Policy Management Console を使用して Active Directory ポリシーと Citrix ポリシーの両方を構成する場合、割り当てと設定が期待どおりに適用されないことがあります。詳細については、CTX127461を参照してください。

> 「Unfiltered」という名前のポリシーがデフォルトで提供されます。

- Studioを使用してCitrixポリシーを管理する場合、Unfilteredポリシーに追加した設定は、サイト内のすべてのサーバー、デスクトップ、および接続に適用されます。
- ローカルグループポリシーエディターを使用して Citrix ポリシーを管理する場合、Unfiltered ポリシーに追加した設定は、すべてのサイトと接続に適用されます。サイトと接続は、ポリシーを含むグループポリシーオブジェクト (GPO) のスコープ内にある必要があります。たとえば、Sales OU には、米国の営業チームのすべてのメンバーを含む Sales-US という GPO が含まれています。Sales-US GPO は、いくつかのユーザーポリシー設定を含む Unfiltered ポリシーで構成されています。米国の営業マネージャーがサイトにログオンすると、Unfiltered ポリシーの設定がセッションに自動的に適用されます。この構成は、ユーザーが Sales-US GPO のメンバーであるためです。

割り当てのモードは、ポリシーがすべての割り当て基準に一致する接続にのみ適用されるかどうかを決定します。モードが (デフォルト) に設定されている場合、ポリシーは割り当て基準に一致する接続にのみ適用されます。モードが に設定されている場合、接続が割り当て基準に一致しない場合にポリシーが適用されます。以下の例は、複数の割り当てが存在する場合に割り当てモードが Citrix ポリシーにどのように影響するかを示しています。

- **例: モードが異なる同種の割り当て** - 同じ種類の2つの割り当てがあり、一方が に設定され、もう一方が に設定されているポリシーでは、接続が両方の割り当てを満たす場合、 に設定された割り当てが優先されます。例:

  ポリシー 1 には次の割り当てが含まれます。

  - 割り当て A は Sales グループを指定します。モードは に設定されています。
  - 割り当て B は営業マネージャーのアカウントを指定します。モードは に設定されています。

  割り当て B のモードが に設定されているため、ユーザーが Sales グループのメンバーであっても、営業マネージャーがサイトにログオンしたときにポリシーは適用されません。
- **例: モードが同じでタイプが異なる割り当て** - タイプが異なる2つ以上の割り当てがあり、 に設定されているポリシーでは、ポリシーが適用されるためには、接続が各タイプの少なくとも1つの割り当てを満たす必要があります。例:

ポリシー 2 には次の割り当てが含まれます。

- 割り当て C は、Sales グループを指定するユーザー割り当てです。モードは に設定されています。
- 割り当て D は、10.8.169.* (企業ネットワーク) を指定するクライアント IP アドレス割り当てです。モードは に設定されています。

営業マネージャーがオフィスからサイトにログオンすると、接続が両方の割り当てを満たすため、ポリシーが適用されます。

ポリシー3には、次の割り当てが含まれます。

- 割り当てEは、営業グループを指定するユーザー割り当てです。モードは「許可」に設定されています。
- 割り当てFは、NetScaler Gatewayの接続条件を指定するアクセスコントロール割り当てです。モードは「許可」に設定されています。

営業マネージャーがオフィスからサイトにログオンしても、接続が割り当てFを満たさないため、ポリシーは適用されません。

Studioを使用してテンプレートに基づいてポリシーを作成する

1. Studioナビゲーションペインで、 を選択します。
2. **［テンプレート］**タブを選択し、テンプレートを選択します。
3. 「**操作**」ペインで、「**テンプレート**」から「**ポリシーの作成**」を選択します。
4. デフォルトでは、新しいポリシーはテンプレートのすべてのデフォルト設定を使用します。この場合、 が選択されています。設定を変更する場合は、 を選択し、設定を追加または削除します。
5. 次のいずれかを選択して、ポリシーの適用方法を指定します。
   - 選択したユーザーオブジェクトとマシンオブジェクトに割り当て、ポリシーを適用する必要があるユーザーオブジェクトとマシンオブジェクトを選択します。
   - サイト内のすべてのオブジェクトに割り当てて、サイト内のすべてのユーザーオブジェクトとマシンオブジェクトにポリシーを適用します。
6. ポリシーの名前を入力するか、デフォルト名を受け入れます。ポリシーの名前は、それが影響する対象（例: 経理部、リモートユーザーなど）に基づいて検討してください。必要に応じて、説明を追加します。

ポリシーはデフォルトで有効になっていますが、無効にすることもできます。ポリシーを有効にすると、ログオンするユーザーにすぐに適用されます。無効にすると、ポリシーは適用されません。ポリシーの優先順位を付けたり、後で設定を追加したりする必要がある場合は、適用する準備ができるまでポリシーを無効にしておくことを検討してください。

Studioを使用してポリシーを作成する

1. Studioナビゲーションペインで、 を選択します。
2. **ポリシー**タブを選択します。
3. ペインで、 を選択します。
4. ポリシー設定を追加および構成します。
5. 次のいずれかを選択して、ポリシーを適用する方法を指定します。
   - 選択したユーザーオブジェクトとマシンオブジェクトに割り当て、ポリシーを適用する必要があるユーザーオブジェクトとマシンオブジェクトを選択します。
   - サイト内のすべてのオブジェクトに割り当てて、サイト内のすべてのユーザーオブジェクトとマシンオブジェクトにポリシーを適用します。
6. ポリシーの名前を入力するか、デフォルトを受け入れます。ポリシーが影響する対象（例: 経理部、リモートユーザーなど）に基づいてポリシーに名前を付けることを検討してください。必要に応じて、説明を追加します。

   ポリシーはデフォルトで有効になっていますが、無効にすることもできます。ポリシーを有効にすると、ログオンするユーザーにすぐに適用されます。無効にすると、ポリシーは適用されません。ポリシーの優先順位を付けたり、後で設定を追加したりする必要がある場合は、適用する準備ができるまでポリシーを無効にしておくことを検討してください。

グループポリシーエディターを使用してポリシーを作成および管理する

グループポリシーエディターで、**コンピューターの構成またはユーザーの構成**を展開します。**ポリシー**ノードを展開し、**Citrixポリシー**を選択します。適切なアクションを選択します。

タスク	手順
ポリシーを作成する	**ポリシー**タブで、**新規**をクリックします。
既存のポリシーを編集する	**ポリシー**タブで、ポリシーを選択し、**編集**をクリックします。

タスク	手順
既存のポリシーの優先度を変更する	**ポリシー**タブでポリシーを選択し、**上位**または**下位**をクリックします。
ポリシーの概要情報を表示する	**ポリシー**タブでポリシーを選択し、**概要**タブをクリックします。
ポリシー設定を表示および修正する	**ポリシー**タブでポリシーを選択し、**設定**タブをクリックします。
ポリシーフィルターを表示および修正する	**ポリシー**タブでポリシーを選択し、**フィルター**タブをクリックします。ポリシーに複数のフィルターを追加する場合、ポリシーが適用されるには、すべてのフィルター条件が満たされている必要があります。
ポリシーを有効または無効にする	**ポリシー**タブでポリシーを選択し、**アクション > 有効**または**アクション > 無効**を選択します。
既存のテンプレートからポリシーを作成する	**テンプレート**タブでテンプレートを選択し、**新しいポリシー**をクリックします。

ポリシーの比較、優先順位付け、モデル化、トラブルシューティング

複数のポリシーを使用して、ユーザーの職務、地理的な場所、または接続の種類に基づいて、ユーザーのニーズを満たすように環境をカスタマイズできます。たとえば、セキュリティを強化するために、機密データを定期的に扱うユーザーグループに制限を設けることができます。

ユーザーが機密ファイルをローカルクライアントドライブに保存できないようにするポリシーを作成することもできます。ただし、ユーザーグループ内の一部のユーザーがローカルドライブへのアクセスを必要とする場合は、それらのユーザー専用の別のポリシーを作成できます。次に、どちらが優先されるかを制御するために、2つのポリシーをランク付けまたは優先順位付けします。複数のポリシーを使用する場合、次のことを決定する必要があります。

- ポリシーの優先順位付け方法
- 例外の作成方法
- ポリシーが競合する場合に有効なポリシーを表示する方法。

一般に、ポリシーは、サイト全体、特定のDelivery Controller、またはユーザーデバイス用に構成された同様の設定を上書きします。この原則の例外はセキュリティです。環境内の最高の暗号化設定は、常に他の設定とポリシーを上書きします。最高の暗号化設定には、オペレーティングシステムと最も制限の厳しいシャドウイング設定が含まれます。

Citrix®ポリシーは、オペレーティングシステムで設定したポリシーと相互作用します。Citrix環境では、Citrix設定は、Active Directoryポリシーで構成された設定、またはリモートデスクトップセッションホスト構成を使用して構成された設定と同じ設定を上書きします。この設定には、一般的なリモートデスクトッププロトコル (RDP) クライアント接続設定に関連する設定が含まれます。一般的なRDP設定には、デスクトップの壁紙、メニューアニメーション、ドラッグ中のウィンドウコンテンツの表示などの設定が含まれます。

Secure ICA®などの一部のポリシー設定は、オペレーティングシステムの設定と一致している必要があります。より高い優先度の暗号化レベルが他の場所で設定されている場合、ポリシーで指定した、またはアプリケーションとデスクトップを配信するときに指定した**Secure ICAポリシー**設定は上書きされる可能性があります。

たとえば、デリバリーグループを作成するときに指定する暗号化設定は、環境全体で指定した暗号化設定と同じレベルである必要があります。

> **注：**
>
> ダブルホップシナリオの2番目のホップでは、シングルセッションOS VDAがマルチセッションOS VDAに接続すると考えます。この場合、Citrixポリシーは、シングルセッションOS VDAをユーザーデバイスであるかのように扱います。たとえば、ポリシーがユーザーデバイスに画像をキャッシュするように設定されているとします。この例では、ダブルホップシナリオの2番目のホップ用にキャッシュされた画像は、シングルセッションOS VDAマシンにキャッシュされます。

ポリシーとテンプレートの比較

ポリシーまたはテンプレートの設定を、他のポリシーまたはテンプレートの設定と比較できます。たとえば、ベストプラクティスへの準拠を維持するために、設定値を確認する必要がある場合があります。また、ポリシーまたはテンプレートの設定を、Citrixが提供するデフォルト設定と比較することもできます。

1. Studioナビゲーションペインでポリシーを選択します。
2. 比較タブをクリックし、選択をクリックします。

3. 比較するポリシーまたはテンプレートを選択します。比較にデフォルト値を含めるには、デフォルト設定と比較チェックボックスをオンにします。
4. 「比較」をクリックすると、設定された設定が列に表示されます。
5. すべての設定を表示するには、「すべての設定を表示」を選択します。デフォルトのビューに戻るには、「共通設定を表示」を選択します。

ポリシーの優先順位付け

ポリシーに競合する設定が含まれている場合、ポリシーの優先順位を付けることで、その優先順位を定義できます。ユーザーがログオンすると、接続の割り当てに一致するすべてのポリシーが特定されます。これらのポリシーは優先順位順に並べ替えられ、任意の設定の複数のインスタンスが比較されます。各設定は、ポリシーの優先順位に従って適用されます。

Studioで異なる優先順位番号を割り当てることで、ポリシーの優先順位を付けます。デフォルトでは、新しいポリシーには最も低い優先順位が与えられます。ポリシー設定が競合する場合、優先順位が高いポリシー（優先順位番号1が最も高い）は、優先順位が低いポリシーを上書きします。設定は、優先順位と設定の条件（たとえば、設定が無効か有効か）に従ってマージされます。無効になっている設定は、有効になっている下位ランクの設定を上書きします。構成されていないポリシー設定は無視され、下位ランクの設定を上書きしません。

1. Studioナビゲーションペインで**ポリシー**を選択します。**ポリシー**タブが選択されていることを確認します。
2. ポリシーを選択します。
3. **アクション**ペインで**優先順位を下げる**または**優先順位を上げる**を選択します。

例外

ユーザー、ユーザーデバイス、またはマシンのグループに対してポリシーを作成する場合、グループの一部のメンバーが特定のポリシー設定の例外を必要とすることがあります。例外は、次の方法で作成できます。

- 例外が必要なグループメンバーのみにポリシーを作成し、そのポリシーをグループ全体のポリシーよりも上位にランク付けする
- ポリシーに追加された割り当てに拒否モードを使用する

モードが拒否に設定された割り当ては、割り当て条件に一致しない接続にのみポリシーを適用します。たとえば、ポリシーには次の割り当てが含まれます。

- 割り当てAは、範囲208.77.88.*を指定するクライアントIPアドレス割り当てです。モードは許可に設定されています。

- 割り当てBは、特定のユーザーアカウントを指定するユーザー割り当てです。モードは拒否に設定されています。

このポリシーは、割り当てAで指定された範囲のIPアドレスを使用してサイトにログオンするすべてのユーザーに適用されます。ただし、割り当てBで指定されたユーザーアカウントを使用してサイトにログオンするユーザーには適用されません。

接続に適用されるポリシーを決定する

複数のポリシーが適用されるため、接続が期待どおりに応答しない場合があります。優先度の高いポリシーが接続に適用されると、元のポリシーで構成した設定が上書きされる可能性があります。ポリシーの結果セットを計算し、接続に対して最終的なポリシー設定がどのようにマージされるかを判断できます。

ポリシーの結果セットは、次の方法で計算できます。

- Citrixグループポリシーモデリングウィザードを使用して接続シナリオをシミュレートし、Citrixポリシーがどのように適用されるかを判別します。接続シナリオの条件は、次のように指定できます。
  - ドメインコントローラー
  - ユーザー
  - Citrixポリシー割り当ての証拠値
  - 低速ネットワーク接続などのシミュレートされた環境設定 ウィザードが生成するレポートには、そのシナリオで有効になる可能性のあるCitrixポリシーが一覧表示されます。ドメインユーザーとしてControllerにログオンしているとします。この場合、ウィザードはサイトポリシー設定とActive Directoryグループポリシーオブジェクト（GPO）の両方を使用してポリシーの結果セットを計算します。
- グループポリシーの結果を使用して、特定のユーザーとコントローラーに適用されているCitrixポリシーを記述したレポートを作成します。グループポリシーの結果ツールは、環境内のGPOの現在の状態を評価するのに役立ち、レポートを生成します。生成されたレポートには、Citrixポリシーを含むこれらのオブジェクトが、特定のユーザーとコントローラーに現在どのように適用されているかが記述されています。

Citrixグループポリシーモデリングウィザードは、**Citrix Studio**の**アクション**ペインから起動できます。どちらのツールも、Windowsのグループポリシー管理コンソールから起動できます。

Studioを使用して作成されたサイトポリシー設定は、次の場合、ポリシーの結果セットに含まれません。

- グループポリシー管理コンソールからCitrixグループポリシーモデリングウィザードを実行する場合 または、
- グループポリシー管理コンソールからグループポリシーの結果ツールを実行する場合

最も包括的なポリシーの結果セットを取得していることを確認するには、グループポリシー管理コンソールのみを使用してポリシーを作成する場合を除き、CitrixはStudioからCitrixグループポリシーモデリングウィザードを起動することをお勧めします。

Citrixグループポリシーモデリングウィザードを使用する

次のいずれかの方法でCitrixグループポリシーモデリングウィザードを開きます。

- Studioナビゲーションペインでポリシーを選択し、モデリングタブを選択し、次に、アクションペインでモデリングウィザードの起動を選択します。
- グループポリシー管理コンソール (gpmc.msc) を起動し、ツリーペインで を右クリックし、を選択します。

ウィザードの指示に従って、以下を選択します。

- ドメインコントローラー
- ユーザー
- コンピューター
- 環境設定
- シミュレーションで使用するCitrix割り当て基準。

完了をクリックすると、ウィザードはモデリング結果のレポートを生成します。Studioでは、レポートは中央ペインの タブに表示されます。

レポートを表示するには、 を選択します。

> **注：**
>
> タブは、Citrix Cloudでホストされているstudioでは利用できません。

ポリシーのトラブルシューティング

ユーザー、IPアドレス、およびその他の割り当てられたオブジェクトには、同時に適用される複数のポリシーが存在する場合があります。このシナリオでは、ポリシーが予期したとおりに動作しない競合が発生する可能性があります。Citrix Group Policy Modeling Wizardまたはグループポ

リシー結果ツールを実行すると、ユーザー接続にポリシーが適用されていないことが判明する場合があります。このようなシナリオでは、ポリシー評価基準に一致する条件下でアプリケーションやデスクトップに接続するユーザーには、ポリシー設定が適用されません。この状況は、次の場合に発生します。

- ポリシー評価基準に一致する割り当てを持つポリシーがない。
- 割り当てに一致するポリシーに、設定が構成されていない。
- 割り当てに一致するポリシーが無効になっている。

指定された基準を満たす接続にポリシー設定を適用する場合は、以下を確認してください。

- それらの接続に適用するポリシーが有効になっている。
- 適用するポリシーに、適切な設定が構成されている。

デフォルトのポリシー設定

以下の表に、ポリシー設定、そのデフォルト値、およびそれらが適用されるVirtual Delivery Agent (VDA) のバージョンを示します。

ICA®

名前	デフォルト設定	VDA
アダプティブトランスポート	オフ。優先する場合に使用	VDA 7.13〜7.15、VDA 7.16以降
クライアントクリップボードリダイレクト	許可	すべてのVDAバージョン
クライアントクリップボード書き込み許可形式	形式は指定されていません	VDA 7.6 以降
デスクトップの起動	禁止	マルチセッションOS用VDA 7以降
ICAリスナーポート番号	1494	すべてのVDAバージョン
クライアント接続中の非公開プログラムの起動	禁止	マルチセッションOS用VDA 7以降

名前	デフォルト設定	VDA
クリップボードのクライアントからセッションへの転送サイズを制限する	無効	VDA 2009
クリップボードのセッションからクライアントへの転送サイズを制限する	無効	VDA 2009
ロス許容モード	許可	VDA 2003。注: 損失許容モードはまだ利用できません。VDA のこのバージョンは、利用可能になった時点でこれをサポートします。
ロス許容しきい値	損失許容モードが利用可能な場合: パケット損失: 5%、遅延: 300 ms (RTT)	VDA 2003 以降
Rendezvous プロトコル	無効	Citrix Cloud を介して確立された HDX セッションにのみ適用されます。
クライアントクリップボードへの書き込みを制限する	禁止	VDA 7.6 以降
セッションクリップボードへの書き込みを制限する	禁止	VDA 7.6 以降
セッションクリップボード書き込み許可形式	形式は指定されていません	VDA 7.6 以降
タブレットモードの切り替え	有効	VDA 7.16 以降; VDA 7.14 および 7.15 LTSR の場合、この設定はレジストリを使用して構成します。
仮想チャネル許可リスト	有効	VDA 2109

ICA/Adobe Flash 配信/Flash リダイレクト

名前	デフォルト設定	VDA
Flashビデオのフォールバック防止	未構成	VDA 7.6 FP3 から現在まで
Flashビデオのフォールバック防止エラー *.swf	VDA 7.6 FP3 から現在まで	

ICA/オーディオ

名前	デフォルト設定	VDA
アダプティブオーディオ	有効	Citrix Virtual Apps and Desktops™ 2109以降を使用するVDAの、シングルセッションOSおよびマルチセッションOSの両方のセッションに適用されます。
UDPリアルタイムトランスポート経由のオーディオ	許可	すべてのVDAバージョン
オーディオプラグアンドプレイ	許可	マルチセッションOS用VDA 7 から現在まで
オーディオ品質	高 - 高精細オーディオ	すべてのVDAバージョン
クライアントオーディオリダイレクト	許可	すべてのVDAバージョン
クライアントマイクのリダイレクト	許可	すべてのVDAバージョン

ICA/自動クライアント再接続

名前	デフォルト設定	VDA
自動クライアント再接続	許可	すべてのVDAバージョン
自動クライアント再接続認証	認証を要求しない	すべてのVDAバージョン

名前	デフォルト設定	VDA
自動クライアント再接続ログ	自動再接続イベントをログに記録しない	すべてのVDAバージョン
自動クライアント再接続タイムアウト	120秒	VDA 7.13 から現在まで
再接続UIの透過レベル	80%	VDA 7.13 から現在まで

ICA/帯域幅

名前	デフォルト設定	VDA
オーディオリダイレクトの帯域幅制限	0 キロビット/秒	すべてのVDAバージョン
オーディオリダイレクトの帯域幅制限（パーセント）	0	すべてのVDAバージョン
クライアントUSBデバイスリダイレクトの帯域幅制限	0 キロビット/秒	VDA 5.5、5.6 FP1、Multi-session OS 用 VDA 7 以降、Single-session OS 用 VDA 7 以降
クライアントUSBデバイスリダイレクトの帯域幅制限（パーセント）	0	VDA 5.5、5.6 FP1、Multi-session OS 用 VDA 7 以降、Single-session OS 用 VDA 7 以降
クリップボードリダイレクトの帯域幅制限	0 キロビット/秒	すべてのVDAバージョン
クリップボードリダイレクトの帯域幅制限（パーセント）	0	すべてのVDAバージョン
COMポートリダイレクトの帯域幅制限	0 キロビット/秒	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します。
COMポートリダイレクトの帯域幅制限（パーセント）	0	すべてのVDAバージョン。VDA 7.0から7.8までは、レジ

名前	デフォルト設定	VDA
		ストリを使用してこの設定を構成します。
ファイルリダイレクト帯域幅制限	0 キロビット/秒	すべてのVDAバージョン
ファイルリダイレクトの帯域幅制限（パーセント）	0	すべてのVDAバージョン
HDX MediaStreamマルチメディアアクセラレーション帯域幅制限	0 キロビット/秒	VDA 5.5、5.6 FP1、Multi-session OS用VDA 7およびSingle-session OS用VDA 7から現在のMulti-session OS用VDAおよびSingle-session OS用VDA
HDX MediaStreamマルチメディアアクセラレーション帯域幅制限パーセント	0	VDA 5.5、5.6 FP1、Multi-session OS 用 VDA 7 以降、Single-session OS 用 VDA 7 以降
LPTポートリダイレクト帯域幅制限	0 キロビット/秒	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します。
LPTポートリダイレクトの帯域幅制限（パーセント）	0	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します。
セッション全体の帯域幅制限	0 キロビット/秒	すべてのVDAバージョン
プリンターリダイレクト帯域幅制限	0 キロビット/秒	すべてのVDAバージョン
プリンターリダイレクトの帯域幅制限（パーセント）	0	すべてのVDAバージョン
TWAINデバイスリダイレクト帯域幅制限	0 キロビット/秒	VDA 5.5、5.6 FP1、Multi-session OS 用 VDA 7 以降、

名前	デフォルト設定	VDA
		Single-session OS 用 VDA 7 以降
TWAINデバイスリダイレクト帯域幅制限の割合	0	VDA 5.5、5.6 FP1、Multi-session OS 用 VDA 7 以降、Single-session OS 用 VDA 7 以降

ICA/双方向コンテンツリダイレクト

名前	デフォルト設定	VDA
双方向コンテンツリダイレクトを許可する	禁止	VDA 7.13 から現在まで
クライアントにリダイレクトを許可するURL	空	VDA 7.13 から現在まで
VDAにリダイレクトされる許可されたURL	空	VDA 7.13 から現在まで
クライアントからホスト (VDA) およびクライアント間双方向コンテンツリダイレクト	Citrix Workspace™ アプリのグループポリシーオブジェクト管理用テンプレートを使用します	

ICA/ブラウザコンテンツリダイレクト

名前	デフォルト設定	VDA
ブラウザコンテンツリダイレクト	許可	VDA 7.16 から現在まで
ブラウザコンテンツリダイレクトACL構成	`https://www.youtube.com/*`	VDA 7.16 から現在まで
ブラウザコンテンツリダイレクト統合Windows認証のサポート	禁止	VDA 2106 から現在まで

名前	デフォルト設定	VDA
ブラウザコンテンツリダイレクトプロキシ構成	空	VDA 7.16 から現在まで
ブラウザコンテンツリダイレクトサーバーフェッチWebプロキシ認証	禁止	VDA 2012から現在まで

ICA/クライアントセンサー

名前	デフォルト設定	VDA
アプリケーションによるクライアントデバイスの物理的な場所の使用を許可する	禁止	VDA 5.6 FP1、マルチセッションOS用VDA 7から現在まで、シングルセッションOS用VDA 7から現在まで

ICA/デスクトップUI

名前	デフォルト設定	VDA
デスクトップコンポジションリダイレクト	無効 (7.6 FP3から現在まで); 有効 (5.6から7.6 FP2まで)	VDA 5.6、シングルセッションOS用VDA 7から7.15まで
デスクトップコンポジションリダイレクトのグラフィック品質	中	VDA 5.6、シングルセッションOS用VDA 7から7.15まで
デスクトップの壁紙	許可	すべてのVDAバージョン
メニューアニメーション	許可	すべてのVDAバージョン
ドラッグ中にウィンドウの内容を表示	許可	すべてのVDAバージョン

ICA/エンドユーザー監視

名前	デフォルト設定	VDA
ICAラウンドトリップ計算	有効	すべてのVDAバージョン

名前	デフォルト設定	VDA
ICAラウンドトリップ計算間隔	15秒	すべてのVDAバージョン
アイドル接続のICAラウンドトリップ計算	無効	すべてのVDAバージョン

ICA/強化されたデスクトップエクスペリエンス

名前	デフォルト設定	VDA
強化されたデスクトップエクスペリエンス	許可	マルチセッションOS 7以降のVDA

ICA/ファイルリダイレクト

名前	デフォルト設定	VDA
クライアントドライブの自動接続	許可	すべてのVDAバージョン
クライアントドライブのリダイレクト	許可	すべてのVDAバージョン
クライアント固定ドライブ	許可	すべてのVDAバージョン
クライアントフロッピードライブ	許可	すべてのVDAバージョン
クライアントネットワークドライブ	許可	すべてのVDAバージョン
クライアント光学ドライブ	許可	すべてのVDAバージョン
クライアントリムーバブルドライブ	許可	すべてのVDAバージョン
ホストからクライアントへのリダイレクト	無効	マルチセッションOS向けVDA 7以降

名前	デフォルト設定	VDA
クライアントドライブ文字を保持する	無効	VDA 5、5.5、5.6 FP1、シングルセッションOS向けVDA 7以降
読み取り専用クライアントドライブアクセス	無効	VDA 5.5、5.6 FP1、マルチセッションOS向けVDA 7以降、シングルセッションOS向けVDA 7以降
特殊フォルダーのリダイレクト	許可	Web Interface展開のみ。マルチセッションOS向けVDA 7以降
非同期書き込みを使用する	無効	すべてのVDAバージョン

ICA/グラフィック

名前	デフォルト設定	VDA
視覚的にロスレスな圧縮を許可する	無効	VDA 7.6以降
表示メモリ制限	65,536 Kb	VDA 5、5.5、5.6 FP1、シングルセッションOS向けVDA 7以降
ディスプレイモードの劣化設定	最初に色深度を劣化させる	すべてのVDAバージョン
動的ウィンドウプレビュー	有効	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
グラフィックステータスインジケーター	無効	VDA 7.16以降
イメージキャッシュ	有効	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

名前	デフォルト設定	VDA
レガシーグラフィックモード	無効	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
許可される最大色深度	32ビット/ピクセル	すべてのVDAバージョン
ディスプレイモードが劣化した場合にユーザーに通知する	無効	マルチセッションOS用VDA 7以降
3Dグラフィックワークロード向けに最適化	無効	VDA 7.17から現在まで
キューイングとトッシング	有効	すべてのVDAバージョン
画面共有	無効	VDA 2112
圧縮にビデオコーデックを使用	優先される場合にビデオコーデックを使用	VDA 7.6 FP3から現在まで
ビデオコーデックにハードウェアエンコードを使用	有効	VDA 7.11から現在まで

ICA/グラフィック/キャッシュ

名前	デフォルト設定	VDA
永続キャッシュしきい値	3,000,000 ビット/秒	マルチセッションOS用VDA 7から現在まで

ICA/グラフィック/Framehawk

名前	デフォルト設定	VDA
Framehawkディスプレイチャネル	無効	VDA 7.6 FP2 以降
Framehawkディスプレイチャネルのポート範囲	3224,3324	VDA 7.6 FP2 以降

ICA/キープアライブ

名前	デフォルト設定	VDA
ICAキープアライブタイムアウト	60秒	すべてのVDAバージョン
ICAキープアライブ	ICAキープアライブメッセージを送信しない	すべてのVDAバージョン

ICA/ローカルアプリアクセス

名前	デフォルト設定	VDA
ローカルアプリアクセスを許可	禁止	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
URLリダイレクトブロックリスト	サイトは指定されていません	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
URLリダイレクト許可リスト	サイトは指定されていません	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ICA/モバイルエクスペリエンス

名前	デフォルト設定	VDA
自動キーボード表示	禁止	VDA 5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
タッチ最適化デスクトップの起動	許可	VDA 5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降。この設定は無効になっており、Windows 10およびWindows Server 2016マシンでは利用できません。

名前	デフォルト設定	VDA
コンボボックスのリモート処理	禁止	VDA 5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ICA/マルチメディア

名前	デフォルト設定	VDA
HTML5ビデオリダイレクト	禁止	VDA 7.12以降
ビデオ品質の制限	未構成	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
Microsoft Teamsリダイレクト	許可	マルチセッションOS用VDA 1906以降、シングルセッションOS用VDA 1906以降。
マルチメディア会議	許可	すべてのVDAバージョン
WAN経由のWindows Media マルチメディアリダイレクトの最適化	許可	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
WAN経由のWindows Media マルチメディアリダイレクトの最適化にGPUを使用	禁止	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
Windows Mediaフォールバックの防止	未構成	VDA 7.6 FP3以降
Windows Mediaクライアント側コンテンツフェッチ	許可	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
Windows Mediaリダイレクト	許可	すべてのVDAバージョン
Windows Mediaリダイレクトバッファサイズ	5秒	VDA 5、5.5、5.6 FP1から現在まで

名前	デフォルト設定	VDA
Windows Mediaリダイレクトバッファサイズの使用	無効	VDA 5、5.5、5.6 FP1から現在まで

ICA/マルチストリーム接続

名前	デフォルト設定	VDA
UDP経由のオーディオ	許可	VDA for Multi-session OS 7から現在まで
オーディオUDPポート範囲	16500、16509	VDA 5.5、5.6 FP1、VDA for Multi-session OS 7から現在まで、VDA for Single-session OS 7から現在まで
マルチポートポリシー	プライマリポート (2598) は高優先度	VDA 5.5、5.6 FP1、VDA for Multi-session OS 7から現在まで、VDA for Single-session OS 7から現在まで
マルチストリーム コンピューター設定	無効	VDA 5.5、5.6 FP1、VDA for Multi-session OS 7から現在まで、VDA for Single-session OS 7から現在まで
マルチストリーム ユーザー設定	無効	VDA 5.5、5.6 FP1、VDA for Multi-session OS 7から現在まで、VDA for Single-session OS 7から現在まで
マルチストリーム仮想チャネルストリーム割り当て設定	デフォルトのストリーム割り当てについては、マルチストリーム仮想チャネル割り当て設定を参照してください。	VDA 2003

ICA/ポートリダイレクト

名前	デフォルト設定	VDA
クライアントCOMポートの自動接続	無効	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します
クライアントLPTポートの自動接続	無効	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します
クライアントCOMポートリダイレクト	禁止	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します
クライアントLPTポートリダイレクト	禁止	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します

ICA/印刷

名前	デフォルト設定	VDA
クライアントプリンターリダイレクト	許可	すべてのVDAバージョン
デフォルトプリンター	デフォルトプリンターをクライアントのメインプリンターに設定する	すべてのVDAバージョン
プリンターの割り当て	ユーザーの現在のプリンターがセッションのデフォルトプリンターとして使用されます	すべてのVDAバージョン
プリンターの自動作成イベントログの優先順位	エラーと警告をログに記録	すべてのVDAバージョン

名前	デフォルト設定	VDA
セッションプリンター	プリンターが指定されていません	すべてのVDAバージョン
プリンターが作成されるまで待機する (デスクトップ)	無効	すべてのVDAバージョン

ICA/印刷/クライアントプリンター

名前	デフォルト設定	VDA
クライアントプリンターを自動作成	すべてのクライアントプリンターを自動作成	すべてのVDAバージョン
汎用ユニバーサルプリンターを自動作成	無効	すべてのVDAバージョン
クライアントプリンター名	標準プリンター名	VDA 5.6
印刷サーバーへの直接接続	有効	すべてのVDAバージョン
プリンタードライバーのマッピングと互換性	ルールは指定されていません	すべてのVDAバージョン
プリンタープロパティの保持	クライアントに保存されていない場合にのみプロファイルに保持	すべてのVDAバージョン
保持および復元されたクライアントプリンター	許可	VDA 5、5,5、5.6 FP1

ICA/Printing/Drivers

名前	デフォルト設定	VDA
インボックスプリンタードライバーの自動インストール	有効	すべてのVDAバージョン
ユニバーサルドライバーの優先順位	イーエムエフ; エックスピーエス; ピーシーエルファイブ	すべてのVDAバージョン

名前	デフォルト設定	VDA
	シー; ピーシーエルフォー; ピーエス	
ユニバーサル印刷ドライバーの使用	要求されたドライバーが利用できない場合にのみユニバーサル印刷を使用する	すべてのVDAバージョン

ICA/印刷/ユニバーサルプリントサーバー

名前	デフォルト設定	VDA
ユニバーサルプリントサーバーを有効にする	無効	すべてのVDAバージョン
ユニバーサルプリントサーバー印刷データストリーム (CGP) ポート	7229	すべてのVDAバージョン
ユニバーサルプリントサーバー印刷ストリーム入力帯域幅制限 (kbps)	0	すべてのVDAバージョン
ユニバーサルプリントサーバーWebサービス (HTTP/SOAP) ポート	8080	すべてのVDAバージョン
負荷分散用のUniversal Print Server	VDA バージョン 7.9 から現在まで	
ユニバーサルプリントサーバーのサービス停止しきい値	180 (秒)	VDA バージョン 7.9 から現在まで

ICA/印刷/ユニバーサル印刷

名前	デフォルト設定	VDA
ユニバーサル印刷 EMF 処理モード	プリンターに直接スプールする	すべてのVDAバージョン
ユニバーサル印刷画像圧縮制限	最高品質 (ロスレス圧縮)	すべてのVDAバージョン

名前	デフォルト設定	VDA
ユニバーサル印刷最適化のデフォルト	画像圧縮: 希望する画質 = 標準品質, ヘビーウェイト圧縮を有効にする = 無効; 画像とフォントのキャッシュ: 埋め込み画像のキャッシュを許可する = 有効; 管理者以外のユーザーがこれらの設定を変更することを許可する = 無効;	すべてのVDAバージョン
ユニバーサル印刷プレビュー設定	自動作成されたプリンターまたは汎用ユニバーサルプリンターには印刷プレビューを使用しない	すべてのVDAバージョン
ユニバーサル印刷の印刷品質制限	制限なし	すべてのVDAバージョン

ICA/セキュリティ

名前	デフォルト設定	VDA
SecureICAの最小暗号化レベル	基本	マルチセッションOS用VDA 7以降

ICA/サーバー制限

名前	デフォルト設定	VDA
サーバーアイドルタイマー間隔	0ミリ秒	マルチセッションOS用VDA 7以降

ICA/セッション制限

名前	デフォルト設定	VDA
切断されたセッションタイマー	無効	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降

名前	デフォルト設定	VDA
リモートPCアクセス切断セッションタイマー	無効	シングルセッションOS用VDA 7以降
切断セッションタイマー間隔	1,440分	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
セッション接続タイマー	無効	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
セッション接続タイマー間隔	1,440分	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
セッションアイドルタイマー	有効	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
セッションアイドルタイマー間隔	1,440分	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降

ICA/セッションの信頼性

名前	デフォルト設定	VDA
セッションの信頼性接続	許可	すべてのVDAバージョン
セッションの信頼性ポート番号	2598	すべてのVDAバージョン
セッションの信頼性タイムアウト	180秒	すべてのVDAバージョン

ICA/タイムゾーン制御

名前	デフォルト設定	VDA
レガシークライアントのローカル時刻を推定する	有効	マルチセッションOS 7以降のVDA
セッション切断またはログオフ時にシングルセッションOSのタイムゾーンを復元する	有効	現在のVDAバージョン
クライアントのローカル時刻を使用する	サーバーのタイムゾーンを使用する	すべてのVDAバージョン

ICA/TWAINデバイス

名前	デフォルト設定	VDA
クライアントTWAINデバイスリダイレクト	許可	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
TWAIN圧縮レベル	中	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ICA/USBデバイス

名前	デフォルト設定	VDA
クライアントUSBデバイス最適化ルール	有効 (VDA 7.6 FP3以降); 無効 (VDA 7.11以降); デフォルトでは、ルールは指定されていません	VDA 7.6 FP3以降
クライアントUSBデバイスのリダイレクト	禁止	すべてのVDAバージョン

名前	デフォルト設定	VDA
クライアントUSBデバイスリダイレクト規則	ルールは指定されていません	すべてのVDAバージョン
クライアントUSBプラグアンドプレイデバイスリダイレクト	許可	マルチセッションOS 用 VDA 7 以降、シングルセッション OS 用 VDA 7 以降

ICA/ビジュアルディスプレイ

名前	デフォルト設定	VDA
単純なグラフィックの優先色深度	24ビット/ピクセル	VDA 7.6 FP3 以降
ターゲットフレームレート	30 フレーム/秒	すべてのVDAバージョン
画質	中	マルチセッションOS 用 VDA 7 以降、シングルセッション OS 用 VDA 7 以降

ICA/ビジュアルディスプレイ/動画

名前	デフォルト設定	VDA
最小画質	標準	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
動画圧縮	有効	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
プログレッシブ圧縮レベル	なし	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

名前	デフォルト設定	VDA
プログレッシブ圧縮のしきい値	2,147,483,647 キロビット/秒	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
目標最小フレームレート	10 フレーム/秒	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ICA/視覚表示/静止画像

名前	デフォルト設定	VDA
追加の色圧縮	無効	すべてのVDAバージョン
追加の色圧縮のしきい値	8,192 キロビット/秒	すべてのVDAバージョン
高負荷圧縮	無効	すべてのVDAバージョン
非可逆圧縮レベル	中	すべてのVDAバージョン
非可逆圧縮しきい値	2,147,483,647 ケービーピーエス	すべてのVDAバージョン

ICA/WebSockets

名前	デフォルト設定	VDA
WebSockets接続	禁止	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
WebSocketsポート番号	8008	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
WebSockets信頼済みオリジンサーバーリスト	ワイルドカード「*」は、すべてのReceiver for Web URL	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

名前	デフォルト設定	VDA
	を信頼するために使用されます	

負荷管理

名前	デフォルト設定	VDA
同時ログオン許容数	2	マルチセッションOS用VDA 7以降
CPU使用率	無効	マルチセッションOS用VDA 7以降
CPU使用率から除外されるプロセスの優先度	標準以下または低	マルチセッションOS用VDA 7以降
ディスク使用量	無効	マルチセッションOS用VDA 7以降
最大セッション数	250	マルチセッションOS用VDA 7以降
メモリ使用量	無効	マルチセッションOS用VDA 7以降
メモリ使用量のベース負荷	ゼロ負荷: 768 MB	マルチセッションOS用VDA 7以降

プロファイル管理/詳細設定

名前	デフォルト設定	VDA
自動構成を無効にする	無効	すべてのVDAバージョン
問題が発生した場合にユーザーをログオフする	無効	すべてのVDAバージョン
ロックされたファイルへのアクセス時の再試行回数	5	すべてのVDAバージョン

名前	デフォルト設定	VDA
ログオフ時にインターネットCookieファイルを処理する	無効	すべてのVDAバージョン

プロファイル管理/基本設定

名前	デフォルト設定	VDA
アクティブライトバック	無効	すべてのVDAバージョン
Profile Management を有効にする	無効	すべてのVDAバージョン
除外されるグループ	無効。すべてのユーザーグループのメンバーが処理されます。	すべてのVDAバージョン
オフラインプロファイルのサポート	無効	すべてのVDAバージョン
ユーザーストアへのパス	ウィンドウズ	すべてのVDAバージョン
ローカル管理者によるログオンの処理	無効	すべてのVDAバージョン
処理されるグループ	無効。すべてのユーザーグループのメンバーが処理されます。	すべてのVDAバージョン

プロファイル管理/クロスプラットフォーム設定

名前	デフォルト設定	VDA
クロスプラットフォーム設定ユーザーグループ	無効。処理済みグループで指定されたすべてのユーザーグループが処理されます	すべてのVDAバージョン
クロスプラットフォーム設定を有効にする	無効	すべてのVDAバージョン

名前	デフォルト設定	VDA
クロスプラットフォーム定義へのパス	無効。パスは指定されていません。	すべてのVDAバージョン
クロスプラットフォーム設定ストアへのパス	無効。Windows\PM_CMが使用されます。	すべてのVDAバージョン
クロスプラットフォーム設定の作成元	無効	すべてのVDAバージョン

プロファイル管理/ファイルシステム/除外

名前	デフォルト設定	VDA
除外リスト - ディレクトリ	無効。ユーザープロファイル内のすべてのフォルダーが同期されます。	すべてのVDAバージョン
除外リスト - ファイル	無効。ユーザープロファイル内のすべてのファイルが同期されます。	すべてのVDAバージョン

プロファイル管理/ファイルシステム/同期

名前	デフォルト設定	VDA
同期するディレクトリ	無効。除外されていないフォルダーのみが同期されます。	すべてのVDAバージョン
同期するファイル	無効。除外されていないファイルのみが同期されます。	すべてのVDAバージョン
ミラーリングするフォルダー	無効。フォルダーはミラーリングされません。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト

名前	デフォルト設定	VDA
管理者アクセスを許可する	無効	すべてのVDAバージョン

名前	デフォルト設定	VDA
ドメイン名を含める	無効	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/AppData(Roaming)

名前	デフォルト設定	VDA
AppData(Roaming)パス	無効。場所は指定されていません。	すべてのVDAバージョン
AppData(Roaming)のリダイレクト設定	コンテンツは、AppData(Roaming)パスのポリシー設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/連絡先

名前	デフォルト設定	VDA
連絡先パス	無効。場所は指定されていません。	すべてのVDAバージョン
連絡先のリダイレクト設定	コンテンツは、**連絡先パスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/デスクトップ

名前	デフォルト設定	VDA
デスクトップパス	無効。場所は指定されていません。	すべてのVDAバージョン
デスクトップのリダイレクト設定	コンテンツは、**デスクトップパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ドキュメント

名前	デフォルト設定	VDA
ドキュメントパス	無効。場所は指定されていません。	すべてのVDAバージョン
ドキュメントのリダイレクト設定	コンテンツは、**ドキュメントパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ダウンロード

名前	デフォルト設定	VDA
ダウンロードパス	無効。場所は指定されていません。	すべてのVDAバージョン
ダウンロードのリダイレクト設定	コンテンツは、**ダウンロードパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/お気に入り

名前	デフォルト設定	VDA
お気に入りパス	無効。場所は指定されていません。	すべてのVDAバージョン
お気に入りのリダイレクト設定	コンテンツは、**お気に入りパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/リンク

名前	デフォルト設定	VDA
リンクパス	無効。場所は指定されていません。	すべてのVDAバージョン

名前	デフォルト設定	VDA
リンクのリダイレクト設定	コンテンツは、**リンクパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ミュージック

名前	デフォルト設定	VDA
ミュージックパス	無効。場所は指定されていません。	すべてのVDAバージョン
ミュージックのリダイレクト設定	コンテンツは、「**ミュージックパスポリシー**」設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ピクチャ

名前	デフォルト設定	VDA
ピクチャパス	無効。場所は指定されていません。	すべてのVDAバージョン
ピクチャのリダイレクト設定	コンテンツは、「**ピクチャパスポリシー**」設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/保存されたゲーム

名前	デフォルト設定	VDA
保存されたゲームパス	無効。場所は指定されていません。	すべてのVDAバージョン
保存されたゲームのリダイレクト設定	コンテンツは、「**保存されたゲームパスポリシー**」設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/検索

名前	デフォルト設定	VDA
検索パス	無効。場所は指定されていません。	すべてのVDAバージョン
検索のリダイレクト設定	コンテンツは、**検索パスポリシー**設定で指定されたUNCパスにリダイレクトされます。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/スタートメニュー

名前	デフォルト設定	VDA
スタートメニューパス	無効。場所は指定されていません。	すべてのVDAバージョン
スタートメニューのリダイレクト設定	コンテンツは、スタートメニューパスポリシー設定で指定されたUNCパスにリダイレクトされます。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ビデオ

名前	デフォルト設定	VDA
ビデオパス	無効。場所は指定されていません。	すべてのVDAバージョン
ビデオのリダイレクト設定	コンテンツは、**ビデオパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/ログ設定

名前	デフォルト設定	VDA
Active Directory のアクション	無効	すべてのVDAバージョン
一般情報	無効	すべてのVDAバージョン

名前	デフォルト設定	VDA
一般的な警告	無効	すべてのVDAバージョン
ログの有効化	無効	すべてのVDAバージョン
ファイルシステムのアクション	無効	すべてのVDAバージョン
ファイルシステム通知	無効	すべてのVDAバージョン
ログオフ	無効	すべてのVDAバージョン
ログオン	無効	すべてのVDAバージョン
ログファイルの最大サイズ	1048576	すべてのVDAバージョン
ログファイルへのパス	無効。ログファイルはデフォルトの場所 (%SystemRoot%\System32\Logfiles\UserProfileManager) に保存されます。	すべてのVDAバージョン
パーソナライズされたユーザー情報	無効	すべてのVDAバージョン
ログオン時とログオフ時のポリシー値	無効	すべてのVDAバージョン
レジストリアクション	無効	すべてのVDAバージョン
ログオフ時のレジストリの相違点	無効	すべてのVDAバージョン

プロファイル管理/プロファイルの処理

名前	デフォルト設定	VDA
キャッシュされたプロファイルを削除するまでの遅延	0	すべてのVDAバージョン
ログオフ時にローカルにキャッシュされたプロファイルを削除する	無効	すべてのVDAバージョン

名前	デフォルト設定	VDA
ローカルプロファイルの競合処理	ローカルプロファイルを使用する	すべてのVDAバージョン
既存プロファイルの移行	ローカルとローミング	すべてのVDAバージョン
テンプレートプロファイルへのパス	無効。新しいユーザープロファイルは、ユーザーが最初にログオンしたデバイスのデフォルトユーザープロファイルから作成されます。	すべてのVDAバージョン
テンプレートプロファイルがローカルプロファイルを上書きする	無効	すべてのVDAバージョン
テンプレートプロファイルが移動プロファイルを上書きする	無効	すべてのVDAバージョン
すべてのログオンでCitrix®必須プロファイルとして使用されるテンプレートプロファイル	無効	すべてのVDAバージョン

プロファイル管理/レジストリ

名前	デフォルト設定	VDA
除外リスト	無効。ユーザーがログオフすると、HKCUハイブ内のすべてのレジストリキーが処理されます。	すべてのVDAバージョン
包含リスト	無効。ユーザーがログオフすると、HKCUハイブ内のすべてのレジストリキーが処理されます。	すべてのVDAバージョン

プロファイル管理/ストリーム配信ユーザープロファイル

名前	デフォルト設定	VDA
常にキャッシュ	無効	すべてのVDAバージョン
常にキャッシュサイズ	0 MB	すべてのVDAバージョン
プロファイルストリーミング	無効	すべてのVDAバージョン
ストリーミングされたユーザープロファイルグループ	無効。OU内のすべてのユーザープロファイルは通常どおり処理されます。	すべてのVDAバージョン
保留中のエリアロックファイルのタイムアウト (日数)	1日	すべてのVDAバージョン

レシーバー

名前	デフォルト設定	VDA
StoreFront™アカウントリスト	ストアは指定されていません	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ユーザーパーソナライゼーションレイヤー

名前	デフォルト設定	VDA
ユーザーレイヤーリポジトリパス	無効。パスは指定されていません。	VDA 19.12以降のバージョン
ユーザーレイヤーサイズ (GB)	10 GB。ユーザーレイヤーは、設定されたサイズまで拡張するシンプロビジョニングディスクです。ユーザーレイヤーのサイズが小さくなることはありません。	VDA 19.12以降のバージョン

バーチャル デリバリー エージェント

名前	デフォルト設定	VDA
コントローラー登録IPv6ネットマスク	ネットマスクは指定されていません	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
コントローラー登録ポート	80	すべてのVDAバージョン
コントローラーSID	SIDは指定されていません	すべてのVDAバージョン
コントローラー	コントローラーは指定されていません	すべてのVDAバージョン
コントローラーの自動更新を有効にする	有効	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
IPv6コントローラー登録のみを使用する	無効	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
サイトGUID	GUIDは指定されていません	すべてのVDAバージョン

バーチャル デリバリー エージェント/HDX 3D Pro

名前	デフォルト設定	VDA
ロスレスを有効にする	有効	VDA 5.5、5.6 FP1
HDX 3D Pro品質設定	VDA 5.5、5.6 FP1	

バーチャル デリバリー エージェント/監視

名前	デフォルト設定	VDA
プロセス監視を有効にする	無効	VDA 7.11以降
リソース監視を有効にする	有効	VDA 7.11以降

仮想IP

名前	デフォルト設定	VDA
仮想IPループバックサポート	無効	VDA 7.6 以降
仮想IP仮想ループバックプログラムリスト	なし	VDA 7.6 以降

ポリシー設定リファレンス

ポリシーには、ポリシーが適用されるときに適用される設定が含まれます。このセクションの説明では、機能を有効にするためにより多くの設定が必要かどうか、または設定に類似しているかどうかも示します。

クイックリファレンス

以下の表に、ポリシー内で構成できる設定を示します。左の列で完了したいタスクを見つけ、右の列で対応する設定を見つけてください。

.CHM (コンパイル済みHTML) 形式および .CSV 形式で、すべてのポリシー設定の完全なリストが利用可能です。これらのファイルは、ブローカー (デリバリーコントローラー) がインストールされているサーバーの `\program files\citrix\grouppolicy` フォルダーにあります。ポリシー設定の最新バージョンは、こちらをクリックしてダウンロードすることもできます。

オーディオ

このタスクの場合	このポリシー設定を使用
複数のオーディオデバイスの使用を許可するかどうかを制御する	オーディオプラグアンドプレイ
ユーザーデバイスのマイクからのオーディオ入力を許可するかどうかを制御する	クライアントマイクのリダイレクト
ユーザーデバイスのオーディオ品質を制御する	オーディオ品質
ユーザーデバイスのスピーカーへのオーディオマッピングを制御する	クライアントオーディオリダイレクト

ユーザーデバイスの帯域幅

使用される帯域幅を制限するには	このポリシー設定を使用
クライアントオーディオマッピング	オーディオリダイレクト帯域幅制限またはオーディオリダイレクト帯域幅制限率
ローカルクリップボードを使用した切り取りと貼り付け	クリップボードリダイレクト帯域幅制限またはクリップボードリダイレクト帯域幅制限率
セッションでのローカルクライアントドライブへのアクセス	ファイルリダイレクト帯域幅制限またはファイルリダイレクト帯域幅制限率
HDX™ MediaStream マルチメディアアクセラレーション	HDX MediaStream マルチメディアアクセラレーション帯域幅制限またはHDX MediaStream マルチメディアアクセラレーション帯域幅制限率
クライアントセッション	セッション全体の帯域幅制限
印刷	プリンターリダイレクト帯域幅制限またはプリンターリダイレクト帯域幅制限率
TWAINデバイス（カメラやスキャナーなど）	TWAINデバイスリダイレクト帯域幅制限またはTWAINデバイスリダイレクト帯域幅制限率
USBデバイス	クライアントUSBデバイスリダイレクト帯域幅制限またはクライアントUSBデバイスリダイレクト帯域幅制限率

クライアントドライブとユーザーデバイスのリダイレクト

このタスクの場合	このポリシー設定を使用する
ユーザーがサーバーにログオンしたときに、ユーザーデバイス上のドライブを接続するかどうかを制御します	クライアントドライブの自動接続
サーバーとローカルクリップボード間のカットアンドペーストデータ転送を制御します	クライアントクリップボードリダイレクト
ユーザーデバイスからドライブがどのようにマップされるかを制御します	クライアントドライブのリダイレクト

このタスクの場合	このポリシー設定を使用する
ユーザーのローカルハードドライブがセッションで利用可能かどうかを制御します	クライアント固定ドライブとクライアントドライブのリダイレクト
ユーザーのローカルフロッピーディスクドライブがセッションで利用可能かどうかを制御します	クライアントフロッピーディスクドライブとクライアントドライブのリダイレクト
ユーザーのネットワークドライブがセッションで利用可能かどうかを制御します	クライアントネットワークドライブとクライアントドライブのリダイレクト
ユーザーのローカルCD、DVD、またはBlu-rayドライブがセッションで利用可能かどうかを制御します	クライアント光学ドライブとクライアントドライブのリダイレクト
ユーザーのローカルリムーバブルドライブがセッションで利用可能かどうかを制御します	クライアントリムーバブルドライブとクライアントドライブリダイレクト
スキャナーやカメラなどのユーザーのTWAINデバイスがセッションで利用可能かどうかを制御し、画像データ転送の圧縮を制御します	クライアントTWAINデバイスリダイレクト; TWAIN圧縮リダイレクト
USBデバイスがセッションで利用可能かどうかを制御します	クライアントUSBデバイスリダイレクトとクライアントUSBデバイスリダイレクト規則
WAN経由でクライアントディスクへのファイルの書き込みおよびコピーの速度を向上させます	非同期書き込みを使用する

コンテンツリダイレクト

このタスクの場合	このポリシー設定を使用する
サーバーからユーザーデバイスへのコンテンツリダイレクトを使用するかどうかを制御します	ホストからクライアントへのリダイレクト

デスクトップUI

このタスクの場合	このポリシー設定を使用する
ユーザーセッションでデスクトップの壁紙を使用するかどうかを制御します	デスクトップの壁紙
ウィンドウのドラッグ中にウィンドウの内容を表示します	ドラッグ中のウィンドウの内容を表示

グラフィックとマルチメディア

重要:

Flashポリシーは、古いVDAを使用している顧客が新しいコントローラー（たとえば、バージョン1912コントローラー）を使用し、引き続きFlashを使用できるようにするためにのみ残されています。このVDAバージョンはFlashをサポートしていません。

このタスクの場合	このポリシー設定を使用します
仮想デスクトップからユーザーデバイスに送信される1秒あたりの最大フレーム数を制御します。	ターゲットフレームレート
ユーザーデバイスに表示される画像の視覚的な品質を制御します。	視覚的な品質
セッションでアクセスされたときに、Webサイトがフラッシュコンテンツを表示できるかどうかを制御します。	Flashサーバー側コンテンツ取得URLリスト; Flash URL互換性リスト; Flashビデオフォールバック防止ポリシー設定; Flashビデオフォールバック防止エラー *.swf
サーバーでレンダリングされたビデオの圧縮を制御します。	圧縮にビデオコーデックを使用。ビデオコーデックにハードウェアエンコードを使用。
ユーザーへのHTML5マルチメディアWebコンテンツの配信を制御します。	HTML5ビデオリダイレクト

マルチストリームネットワークトラフィックの優先順位付け

このタスクの場合	このポリシー設定を使用
複数の接続にわたるICA®トラフィックのポートを指定し、ネットワークの優先順位を確立します。	マルチポートポリシー
サーバーとユーザーデバイス間のマルチストリーム接続のサポートを有効にします。	マルチストリーム (コンピューターとユーザーの設定)

印刷

このタスクの場合	このポリシー設定を使用
ユーザーデバイス上のクライアントプリンターの作成を制御します。	クライアントプリンターの自動作成とクライアントプリンターのリダイレクト
プリンタープロパティが保存される場所を制御します。	プリンタープロパティの保持
クライアントまたはサーバーが印刷要求を処理するかどうかを制御する	印刷サーバーへの直接接続
ユーザーが自分のユーザーデバイスに接続されているプリンターにアクセスできるかどうかを制御する	クライアントプリンターリダイレクト
クライアントおよびネットワークプリンターを自動的に作成する際のネイティブWindowsドライバーのインストールを制御する	インボックスプリンタードライバーの自動インストール
ユニバーサルプリンタードライバーをいつ使用するかを制御する	ユニバーサルプリンタードライバーの使用
ローミングユーザーセッション情報に基づいてプリンターを選択する	既定のプリンター
ユニバーサルプリントサーバーの負荷分散とフェールオーバースレッショルドの設定	負荷分散のためのユニバーサルプリントサーバー。サービス停止しきい値のユニバーサルプリントサーバー

> **注：**
>
> ポリシーを使用して、デスクトップまたはアプリケーションセッションでスクリーンセーバーを有効にすることはできません。スクリーンセーバーを必要とするユーザー向けには、ユーザーデバイス上でスクリーンセーバーを実装できます。

ICA® ポリシー設定

> **注：**
>
> このページでは、ICAポリシー設定の説明とサポートされている構成値を提供します。ポリシーの操作の詳細については、「ポリシーの操作」セクションを参照してください。

アダプティブトランスポート

この設定により、EDTをプライマリとして、TCPをフォールバックとして使用したデータ転送を許可または禁止します。

デフォルトでは、アダプティブトランスポートは有効になっており（**Preferred**）、可能な場合はEDTが使用され、TCPにフォールバックします。無効になっている場合に有効にするには、次の手順に従います。

1. Studioで、ポリシー設定「HDX™アダプティブトランスポート」を有効にします。また、この機能をサイト内のすべてのオブジェクトに対するユニバーサルポリシーとして有効にしないことをお勧めします。
2. ポリシー設定を有効にするには、値を**Preferred**に設定し、**OK**をクリックします。

優先。可能な場合はEDT経由のアダプティブトランスポートが使用され、TCPにフォールバックします。

診断モード。EDTが強制的にオンになり、TCPへのフォールバックは無効になります。この設定はトラブルシューティングの場合にのみ推奨されます。

オフ。TCPが強制的にオンになり、EDTは無効になります。

詳細については、「アダプティブトランスポート」を参照してください。

ドラッグアンドドロップ設定

この設定により、クライアントと仮想アプリケーションまたはデスクトップ間でのファイルのドラッグを許可または禁止します。デフォルトでは、ドラッグアンドドロップポリシーは無効になっています。このポリシーを有効にするには、次の手順を実行します。

1. Citrix Studioで、ポリシー設定「**ドラッグアンドドロップ**」を有効にします。
2. 値を**Enabled**に設定し、**OK**をクリックします。

アプリケーション起動待機タイムアウト

この設定は、セッションが最初のアプリケーションの起動を待機するミリ秒単位の待機タイムアウト値を指定します。アプリケーションの起動がこの期間を超えると、セッションは終了します。

デフォルトの時間（10,000ミリ秒）を選択するか、ミリ秒単位の数値を指定できます。

クライアントクリップボードリダイレクト

この設定は、ユーザーデバイスのクリップボードがサーバー上のクリップボードにマップされることを許可または禁止します。

デフォルトでは、クリップボードのリダイレクトは許可されています。

セッションとローカルクリップボード間のカットアンドペーストデータ転送を禁止するには、**Prohibit**を選択します。ユーザーは、セッションで実行されているアプリケーション間では引き続きデータをカットアンドペーストできます。

この設定を許可した後、クライアント接続でクリップボードが消費できる最大許容帯域幅を構成します。**クリップボードリダイレクト帯域幅制限**または**クリップボードリダイレクト帯域幅制限率**の設定を使用します。

クライアントクリップボード書き込み許可形式

クライアントクリップボード書き込みの制限設定が**有効**の場合、ホストクリップボードデータはクライアントエンドポイントと共有できません。この設定を使用して、特定のデータ形式をクライアントエンドポイントのクリップボードと共有することを許可できます。この設定を使用するには、有効にして、許可する特定の形式を追加します。

次のクリップボード形式はシステム定義です。

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT

- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

XenAppおよびXenDesktopとCitrix Virtual Apps and Desktops™には、以下のカスタム形式が事前定義されています。

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8
- CFX_FILE

HTML形式はデフォルトで無効になっています。この機能を有効にするには:

- **クライアントクリップボードリダイレクト**が**許可**に設定されていることを確認します。
- **クライアントクリップボード書き込みの制限**が**有効**に設定されていることを確認します。

- **クライアントクリップボード書き込み許可形式**に**CF_HTML**（およびサポートしたいその他の形式）のエントリを追加します。

カスタム形式をさらに追加できます。カスタム形式名は、システムに登録される形式と一致している必要があります。形式名は大文字と小文字を区別します。

この設定は、**クライアントクリップボードリダイレクト**ポリシーが**禁止**に設定されている場合、または**クライアントクリップボード書き込みの制限**ポリシーが**無効**に設定されている場合には適用されません。

> **注：**
>
> HTML形式のクリップボードコピーサポート（CF_HTML）を有効にすると、コピーされたコンテンツのソースから宛先にスクリプトがコピーされます。コピーを進める前に、ソースを信頼できることを確認してください。スクリプトを含むコンテンツをコピーした場合、それらは宛先ファイルをHTMLファイルとして保存して実行した場合にのみ有効になります。

クリップボードのクライアントからセッションへの転送サイズを制限する

この設定は、ユーザーが1回のカットアンドペースト操作でクライアントエンドポイントから仮想セッションに転送できるクリップボードデータの最大サイズを指定します。

クリップボードの転送サイズを制限するには、**クリップボードのクライアントからセッションへの転送サイズを制限する**設定を有効にします。次に、**サイズ制限**フィールドにキロバイト単位の値を入力して、ローカルクリップボードとセッション間のデータ転送サイズを定義します。

既定では、この設定は無効になっており、クライアントからセッションへの転送に制限はありません。

クリップボードのセッションからクライアントへの転送サイズを制限する

この設定は、ユーザーが1回のカットアンドペースト操作で仮想セッションからクライアントエンドポイントに転送できるクリップボードデータの最大サイズを指定します。

クリップボードの転送サイズを制限するには、**クリップボードのセッションからクライアントへの転送サイズを制限する**設定を有効にします。次に、**サイズ制限**フィールドにキロバイト単位の値を入力して、セッションとローカルクリップボード間のデータ転送サイズを定義します。

既定では、この設定は無効になっており、セッションからクライアントへの転送に制限はありません。

クライアントクリップボードへの書き込みを制限する

この設定が**有効**な場合、ホストのクリップボードデータはクライアントエンドポイントと共有できません。**クライアントクリップボード書き込み許可形式**設定を有効にすることで、特定の形式を許可できます。

デフォルトでは、この設定は**無効**です。

セッションクリップボードへの書き込みを制限する

この設定が**有効**な場合、クライアントのクリップボードデータはセッションアプリケーションと共有できません。**セッションクリップボード書き込み許可形式**設定を有効にすることで、特定の形式を許可できます。

デフォルトでは、この設定は**無効**です。

セッションクリップボード書き込み許可形式

セッションクリップボードへの書き込みを制限する設定が**有効**な場合、クライアントのクリップボードデータはセッションアプリケーションと共有できません。この設定を使用して、特定のデータ形式をセッションクリップボードと共有することを許可できます。

以下のクリップボード形式はシステム定義です。

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP

- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

XenApp and XenDesktopおよびCitrix Virtual Apps and Desktopsでは、以下のカスタム形式が事前定義されています。

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8

HTML形式はデフォルトで無効になっています。この機能を有効にするには：

- **クライアントクリップボードリダイレクト**が**許可**に設定されていることを確認します。
- **セッションクリップボード書き込みの制限**が**有効**に設定されていることを確認します。
- **セッションクリップボード書き込み許可形式**に**CF_HTML**（およびサポートしたいその他の形式）のエントリを追加します。

カスタム形式を追加できます。カスタム形式名は、システムに登録される形式と一致する必要があります。形式名は大文字と小文字を区別します。

この設定は、**クライアントクリップボードリダイレクト**ポリシーが**禁止**に設定されている場合、または**セッションクリップボード書き込みの制限**ポリシーが**無効**に設定されている場合には適用されません。

> **注：**
>
> HTML形式のクリップボードコピーサポート (CF_HTML) を有効にすると、コピーされたコンテンツのソースから宛先にスクリプトがコピーされます。コピーを進める前に、ソースを信頼できることを確認してください。スクリプトを含むコンテンツをコピーした場合、それらは宛先ファイルをHTMLファイルとして保存して実行した場合にのみ有効になります。

デスクトップの起動

この設定は、VDA Direct Access Usersグループの非管理者ユーザーがICA接続を使用してそのVDA上のセッションに接続することを許可または禁止します。

デフォルトでは、非管理者ユーザーはこれらのセッションに接続できません。

この設定は、RDP接続を使用しているVDAダイレクトアクセスユーザーグループ内の非管理者ユーザーには影響しません。これらのユーザーは、この設定が有効または無効になっている場合でもVDAに接続できます。この設定は、VDAダイレクトアクセスユーザーグループに属していない非管理者ユーザーには影響しません。これらのユーザーは、この設定が有効または無効になっている場合、VDAに接続できません。

FIDO2リダイレクト

この設定は、FIDO2リダイレクトを有効または無効にします。FIDO2リダイレクトにより、ユーザーは仮想マシン内のローカルエンドポイントFIDO2コンポーネントを活用できます。ユーザーは、TPM 2.0とWindows Helloを搭載したデバイスで、FIDO2セキュリティキーまたは統合生体認証を介して仮想セッションを認証できます。

この設定が**許可**されている場合、ユーザーはローカルエンドポイント機能を使用してFIDO2認証を行うことができます。デフォルトでは、この設定は**許可**されています。

FIDO2リダイレクトは、以下のレジストリキーを構成することで、クライアントエンドポイントで有効または無効にすることもできます。

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\

名前: FIDO2

種類: REG_DWORD

値: 1

機能を無効にするには値を0に、有効にするには1に設定します。デフォルトでは、この機能は有効になっています。

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

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

ICAリスナー接続タイムアウト

この設定は、ICAプロトコルを使用した接続が完了するまでの最大待機時間を指定します。

デフォルトでは、最大待機時間は120,000ミリ秒、つまり2分です。

ICAリスナーポート番号

この設定は、サーバー上のICAプロトコルによって使用されるTCP/IPポート番号を指定します。

デフォルトでは、ポート番号は1494に設定されています。

有効なポート番号は0～65535の範囲内である必要があり、他のよく知られているポート番号と競合してはなりません。ポート番号を変更した場合は、新しい値を有効にするためにサーバーを再起動してください。サーバーのポート番号を変更した場合は、サーバーに接続するすべてのCitrix Workspace™アプリまたはプラグインでも変更する必要があります。

キーボードと入力方式エディター (IME)

この設定は、次の項目を有効または無効にします。

- 動的キーボードレイアウト同期
- 入力方式エディター (IME)
- Unicode キーボードレイアウトマッピング
- キーボードレイアウト切り替え通知ダイアログメッセージを非表示または表示します

1. Studioで、**キーボードとIME**を選択します。
2. VDAでの動的なキーボードレイアウト同期と汎用クライアント入力方式エディター (IME) 機能を制御するには、**クライアントキーボードレイアウトの同期とIMEの改善**を選択します。設定できる項目は次のとおりです。

   無効 - 動的なキーボードレイアウト同期と汎用クライアント入力方式エディター (IME)。

   動的なクライアントキーボードレイアウト同期をサポート - 動的なキーボードレイアウト同期を有効にします。

   動的なクライアントキーボードレイアウト同期とIMEの改善をサポート - 動的なキーボードレイアウト同期と汎用クライアント入力方式エディター (IME) の両方を有効にします。

3. Unicodeキーボードマッピングを有効または無効にするには、**Unicodeキーボードレイアウトマッピングを有効にする**を選択します。
4. ユーザーがクライアントキーボードレイアウトを変更したときに、キーボードレイアウトが同期中であることを示すメッセージを表示するかどうかを制御するには、**キーボードレイアウト切り替えポップアップメッセージボックスを非表示にする**を選択します。メッセージが表示されないようにすると、ユーザーは誤った文字入力にならないように、入力する前に数秒待つ必要があります。

デフォルト設定：

- **クライアントキーボードレイアウトの同期とIMEの改善**
  - Windows Server 2016およびWindows Server 2019では無効。
  - Windows Server 2012およびWindows 2010では、動的なクライアントキーボードレイアウト同期とIMEの改善をサポート。
- **Unicodeキーボードレイアウトマッピングを無効にする**
- **キーボードレイアウト切り替えポップアップメッセージボックスを表示する**

このポリシーは、ポリシー設定の**説明**セクションに記載されているレジストリ設定を置き換えます。

ログオフチェッカーの起動遅延

この設定は、ログオフチェッカーの起動を遅延させる期間を指定します。このポリシーを使用して、クライアントセッションがセッションを切断するまでに待機する時間（秒単位）を設定します。

この設定は、ユーザーがサーバーからログオフするのにかかる時間も増加させます。

ロス許容モード

> **重要:**
>
> - この機能には、Windows 用 Citrix Workspace アプリ 2002 以降が必要です。VDA のこのバージョンは、利用可能になった時点でこれをサポートします。
> - ロス許容モードは、Citrix Gateway または Citrix Gateway Service ではサポートされていません。このモードは、直接接続でのみ利用可能です。

> この設定は、ロス許容モードを有効または無効にします。

デフォルトでは、ロス許容モードは**許可**されています。

許可されている場合、パケット損失と遅延がしきい値を超えると、このモードに入ります。しきい値は、ロス許容しきい値ポリシー を使用して設定できます。

詳細については、ロス許容モード を参照してください。

ロス許容しきい値

ロス許容モード が利用可能な場合、この設定は、セッションがロス許容モードに切り替わるネットワークメトリックのしきい値を指定します。

デフォルトのしきい値は次のとおりです。

- パケット損失: 5%
- 遅延: 300 ms (RTT)

詳細については、ロス許容モード を参照してください。

Rendezvous プロトコル

この設定は、Citrix Gateway Serviceを使用する際のHDXセッションのプロキシ方法を変更します。有効にすると、HDXトラフィックはCitrix Cloud Connectorを経由しなくなります。代わりに、VDAはCitrix Gateway Serviceに直接アウトバウンド接続を確立します（Cloud Connectorのスケーラビリティが向上します）。

> **重要:**
>
> Citrix Cloud™の機能トグルとHDXポリシー設定がこの機能を制御します。Citrix Cloudの機能トグルはデフォルトで有効になっていますが、HDX設定はデフォルトで無効になっています。HDX設定は、Citrix Gateway Serviceを介して確立されたHDXセッションにのみ影響します。この設定は、クライアントとVDA間で直接確立されたセッションや、オンプレミスのCitrix Gatewayを介して確立されたセッションには影響しません。

> 詳細については、Rendezvousプロトコルを参照してください。

Rendezvousプロキシ構成

この設定により、Rendezvousプロトコルで使用する明示的なプロキシを構成できます。透過型プロキシを使用している場合、この設定を有効にする必要はありません。

デフォルトでは、この設定は無効になっています。

無効にすると、VDAはGateway ServiceとのRendezvous接続を確立しようとするときに、非透過型プロキシを介してアウトバウンドトラフィックをルーティングしません。

有効にすると、VDAはこの設定で定義されたプロキシを介してGateway ServiceとのRendezvous接続を確立しようとします。

VDAは、Rendezvous接続にHTTPおよびSOCKS5プロキシの使用をサポートしています。Rendezvous接続にプロキシを使用するようにVDAを構成するには、この設定を有効にする必要があります。また、プロキシのアドレスまたはPACファイルへのパスを指定します。例：

- プロキシアドレス: `http://<URL or IP>:<port>` または `socks5://<URL or IP>:<port>`
- PACファイル: `http://<URL or IP>/<path>/<filename>.pac`

  VDAバージョン2103は、PACファイルを使用したプロキシ構成でサポートされる最小バージョンです。SOCKS5プロキシのPACファイルスキーマの詳細については、「プロキシ構成」を参照してください。

> **注：**
>
> SOCKS5プロキシのみがEDTを介したデータ転送をサポートします。HTTPプロキシの場合は、ICAのトランスポートプロトコルとしてTCPを使用してください。

> 詳細については、「Rendezvousプロトコル」を参照してください。

クライアント接続中の非公開プログラムの起動

この設定は、サーバー上でRDPを介して初期アプリケーションの起動を許可するかどうかを指定します。

デフォルトでは、サーバー上でRDPを介して初期アプリケーションの起動は許可されていません。

タブレットモード切り替えポリシー設定

タブレットモードの切り替えは、VDA上のストアアプリ、Win32アプリ、およびWindowsシェルを最適化します。これは、電話やタブレットなどの小型デバイス、またはタッチ対応デバイスから接続する際に、仮想デスクトップを自動的にタブレットモードに切り替えることで実現されます。

このポリシーが無効になっている場合、VDAはユーザーが設定したモードになり、クライアントの種類に関係なく、そのモードを維持します。

自動クライアント再接続ポリシー設定

自動クライアント再接続セクションには、セッションの自動再接続を制御するためのポリシー設定が含まれています。

自動クライアント再接続

この設定は、接続が中断された後に同じクライアントによる自動再接続を許可または禁止します。

Citrix Receiver for Windows 4.7以降およびCitrix Workspaceアプリ1808以降では、自動クライアント再接続はCitrix Studioからのポリシー設定のみを使用します。Studioでこれらのポリシーを更新すると、自動クライアント再接続がサーバーからクライアントに同期されます。以前のバージョンのCitrix Receiver for Windowsで自動クライアント再接続を構成するには、Studioポリシーを使用し、レジストリまたはdefault.icaファイルを変更します。

自動クライアント再接続を許可すると、接続が切断されたときに中断された場所からユーザーが作業を再開できるようになります。自動再接続は、切断された接続を検出し、ユーザーをセッションに再接続します。

セッションIDと資格情報へのキーを含むCitrix Workspace™アプリのCookieが使用されない場合、自動再接続によって新しいセッションが開始される可能性があります。つまり、既存のセッションに再接続するのではなく、新しいセッションが開始されます。Cookieは、有効期限が切れている場合は使用されません。たとえば、再接続の遅延や、資格情報の再入力が必要な場合などにCookieの有効期限が切れることがあります。ユーザーが意図的に切断した場合、自動クライアント再接続はトリガーされません。

再接続が進行中の場合、セッションウィンドウはグレー表示されます。カウントダウンタイマーは、セッションが再接続されるまでの残り時間を表示します。セッションがタイムアウトすると、切断されます。

アプリケーションセッションの場合、自動再接続が許可されていると、通知領域にカウントダウンタイマーが表示されます。このタイマーは、セッションが再接続されるまでの残り時間を指定

します。Citrix Workspaceアプリは、再接続が成功するか、ユーザーが再接続の試行をキャンセルするまで、セッションへの再接続を試みます。

ユーザーセッションの場合、自動再接続が許可されていると、Citrix Workspaceアプリは、再接続が成功するか、ユーザーが再接続の試行をキャンセルしない限り、指定された期間セッションへの再接続を試みます。デフォルトでは、この期間は2分です。この期間を変更するには、ポリシーを編集します。

デフォルトでは、自動クライアント再接続は許可されています。

自動クライアント再接続を無効にするには：

1. Citrix Studioを起動します。
2. **自動クライアント再接続**ポリシーを開きます。
3. ポリシーを**禁止**に設定します。

自動クライアント再接続画像

自動クライアント再接続認証

この設定は、自動クライアント再接続に認証を必要とします。

ユーザーが最初にログオンすると、資格情報は暗号化され、メモリに保存され、暗号化キーを含むCookieが作成されます。このCookieはCitrix Workspaceアプリに送信されます。この設定が構成されている場合、Cookieは使用されません。代わりに、Citrix Workspaceアプリが自動的に再接続を試みるときに、資格情報を要求するダイアログボックスがユーザーに表示されます。

デフォルトでは、認証は不要です。

自動クライアント再接続認証を変更するには：

1. Citrix Studioを起動します。
2. **自動クライアント再接続認証**ポリシーを開きます。
3. 認証を有効または無効にします。
4. **OK**を選択します。

自動クライアント再接続ログ

この設定は、イベントログへの自動クライアント再接続の記録を有効または無効にします。

ログ記録が有効な場合、サーバーのシステムログは、成功および失敗した自動再接続イベントに関する情報をキャプチャします。サイトは、すべてのサーバーの再接続イベントの結合されたログを提供しません。

デフォルトでは、ログ記録は無効です。

自動クライアント再接続のログ記録を変更するには：

1. Citrix Studioを起動します。
2. 「**自動クライアント再接続ログ**」ポリシーを開きます。
3. ログを有効または無効にします。
4. 「**OK**」を選択します。

自動クライアント再接続のタイムアウト

デフォルトでは、自動クライアント再接続のタイムアウトは120秒に設定されており、自動クライアント再接続のタイムアウトに設定できる最大値は300秒です。

自動クライアント再接続のタイムアウトを変更するには：

1. Citrix Studioを起動します。
2. 「**自動クライアント再接続タイムアウト**」ポリシーを開きます。
3. タイムアウト値を編集します。
4. 「**OK**」を選択します。

再接続UIの透明度レベル

Studioポリシーを使用して、セッションの信頼性再接続時にXenAppまたはXenDesktop®セッションウィンドウに適用される不透明度レベルを構成できます。

デフォルトでは、再接続UIの透明度は80%に設定されています。

再接続ユーザーインターフェイスの不透明度レベルを変更するには：

1. Citrix Studioを起動します。
2. 「**再接続UIの透過レベル**」ポリシーを開きます。
3. 値を編集します。
4. 「**OK**」を選択します。

オーディオポリシー設定

オーディオセクションには、パフォーマンスを低下させることなく、ユーザーデバイスがセッションでオーディオを送受信できるようにするポリシー設定が含まれています。

アダプティブオーディオ

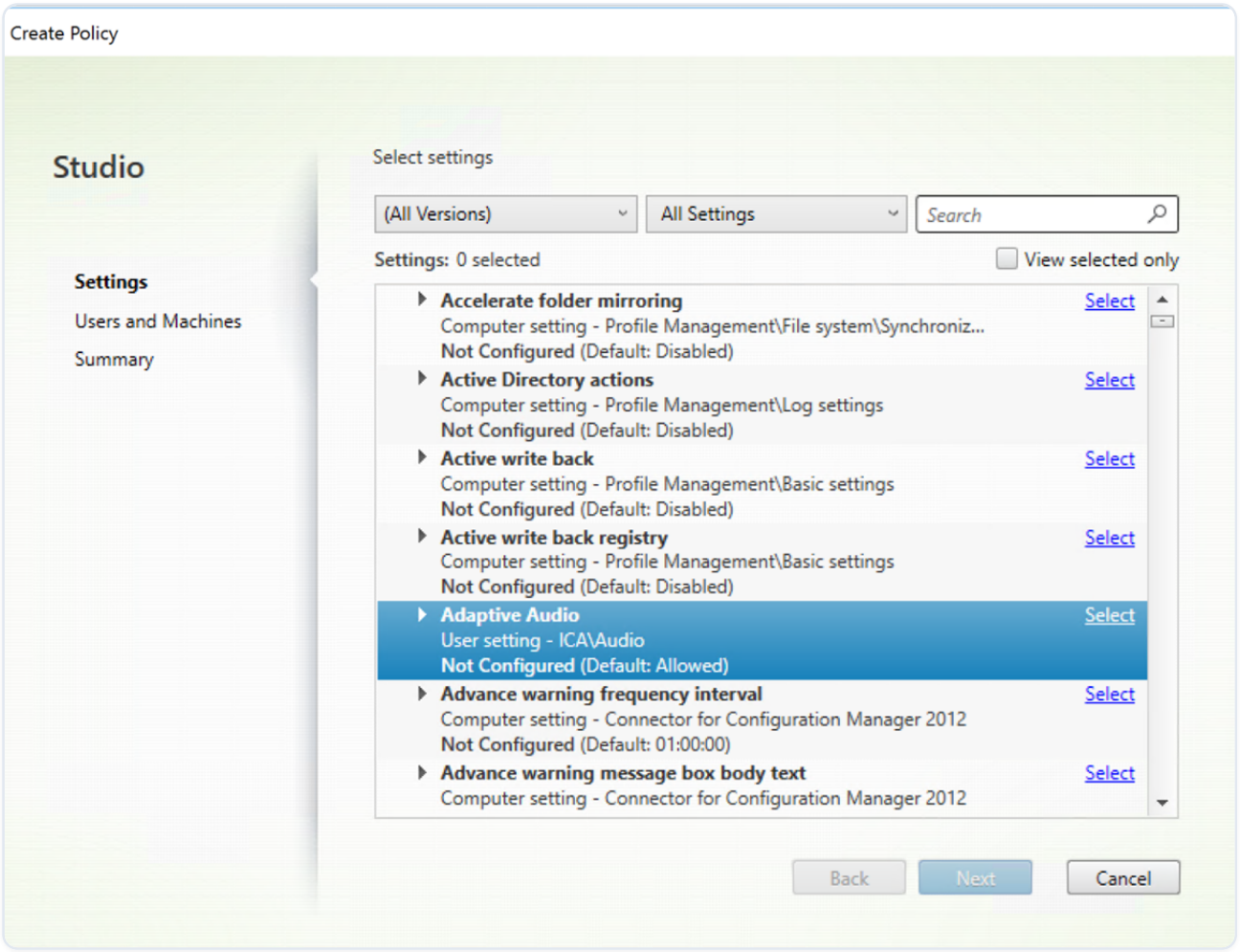
この設定は、アダプティブオーディオを有効または無効にします。このポリシーを有効にすると、最高のユーザーエクスペリエンスを提供するためにオーディオ品質設定が動的に調整されます。この設定は、Citrix Virtual Apps and Desktops™ 2109以降を使用するVDAのシングルセッションOSおよびマルチセッションOSセッションの両方に適用されます。

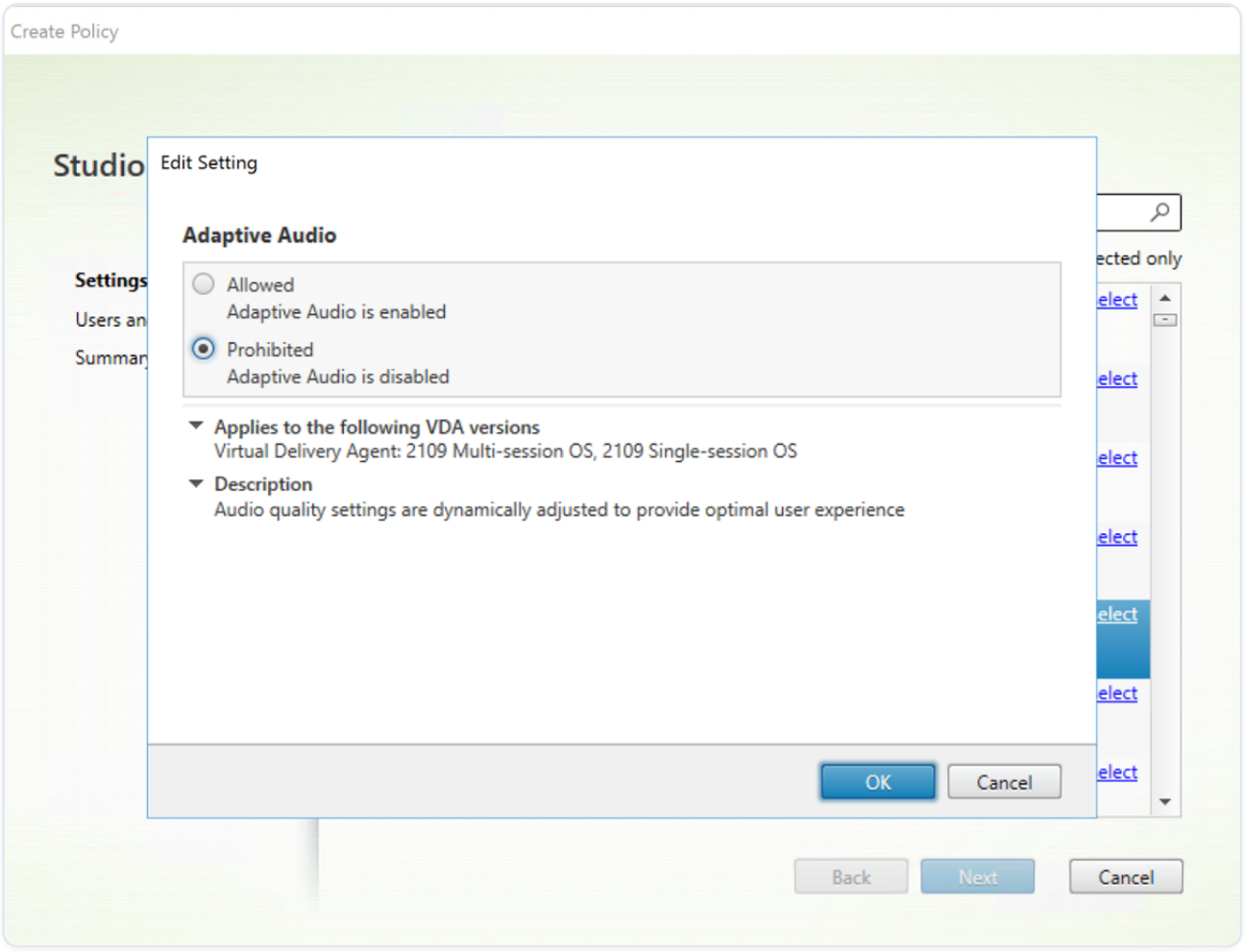
この設定が禁止されている場合、オーディオ品質ポリシーが適用されます。詳細については、「オーディオ品質」を参照してください。

デフォルトでは、アダプティブオーディオポリシーは有効になっています。

アダプティブオーディオを無効にするには：

1. Citrix Studio を起動します。
2. **アダプティブオーディオ**ポリシーを開きます。
3. ポリシーを**禁止**に設定します。





UDPリアルタイムトランスポート経由のオーディオ

この設定は、User Datagram Protocol (UDP) を使用してRTP経由でVDAとユーザーデバイス間でオーディオを送受信することを許可または禁止します。この設定が無効になっている場合、オーディオはTCP経由で送受信されます。

デフォルトでは、UDP経由のオーディオは許可されています。

オーディオプラグアンドプレイ

この設定は、複数のオーディオデバイスを使用してサウンドを録音および再生することを許可または禁止します。

デフォルトでは、複数のオーディオデバイスの使用は許可されています。

この設定は、WindowsマルチセッションOSマシンにのみ適用されます。

オーディオ品質

この設定は、ユーザーセッションで受信されるサウンドの品質レベルを指定します。

デフォルトでは、サウンド品質は「高 - 高精細オーディオ」に設定されています。

サウンド品質を制御するには、次のいずれかのオプションを選択します。

- 低帯域幅接続の場合は、「低 - 低速接続用」を選択します。ユーザーデバイスに送信されるサウンドは最大16 Kbpsに圧縮されます。この圧縮により、サウンドの品質は大幅に低下しますが、低帯域幅接続でも適切なパフォーマンスが得られます。
- 「中」を選択 - 音声に最適化されており、Voice over Internet Protocolアプリケーションを提供します。この設定は、512 Kbps未満の回線、または著しい輻輳やパケット損失があるような、困難なネットワーク接続でメディアアプリケーションを提供します。このコーデックはエンコード時間が速いため、サーバー側のメディア処理が必要な場合に、ソフトフォンやユニファイドコミュニケーションアプリケーションでの使用に最適です。

  ユーザーデバイスに送信されるオーディオは、最大64 Kbpsに圧縮されます。この圧縮により、ユーザーデバイスで再生されるオーディオの品質は中程度に低下しますが、低遅延で低帯域幅の消費を実現します。Voice over Internet Protocolの品質が不十分な場合は、「Audio over UDP Real-time Transport」ポリシー設定が「許可」に設定されていることを確認してください。

  現在、UDP経由のリアルタイムトランスポート（RTP）は、このオーディオ品質が選択されている場合にのみサポートされます。低速（512 Kbps未満）回線のような困難なネットワーク接続でメディアアプリケーションを配信する場合でも、このオーディオ品質を使用してください。また、ネットワークに輻輳やパケット損失がある場合も同様です。
- 「高」を選択 - 帯域幅が豊富で音質が重要な接続には、高精細オーディオを使用します。クライアントはネイティブレートでサウンドを再生できます。サウンドはCD品質まで維持される高音質レベルで圧縮され、最大112 Kbpsの帯域幅を使用します。この量のデータを送信すると、CPU使用率が増加し、ネットワークが輻輳する可能性があります。

帯域幅は、オーディオの録音中または再生中にのみ消費されます。両方が同時に発生する場合、帯域幅の消費量は2倍になります。

最大帯域幅を指定するには、**オーディオリダイレクト帯域幅制限**または**オーディオリダイレクト帯域幅制限率**の設定を構成します。

クライアントオーディオリダイレクト

この設定は、サーバーでホストされているアプリケーションが、ユーザーデバイスにインストールされているサウンドデバイスを介してサウンドを再生できるかどうかを指定します。この設定は、ユーザーがオーディオ入力を録音できるかどうかも指定します。

デフォルトでは、オーディオリダイレクトは許可されています。

この設定を許可した後、オーディオの再生または録音によって消費される帯域幅を制限できます。オーディオによって消費される帯域幅の量を制限すると、アプリケーションのパフォーマンスが向上する可能性がありますが、オーディオ品質が低下する可能性もあります。帯域幅は、オーディオの録音中または再生中にのみ消費されます。両方が同時に発生する場合、帯域幅の消費量は2倍になります。最大帯域幅を指定するには、**オーディオリダイレクト帯域幅制限**または**オーディオリダイレクト帯域幅制限率**の設定を構成します。

WindowsマルチセッションOSマシンでは、複数のオーディオデバイスをサポートするために、**オーディオプラグアンドプレイ**設定が有効になっていることを確認してください。

重要：クライアントオーディオリダイレクトを禁止すると、すべてのHDX™オーディオ機能が無効になります。

クライアントマイクのリダイレクト

この設定は、クライアントマイクのリダイレクトを有効または無効にします。有効にすると、ユーザーはセッションでマイクを使用してオーディオ入力を録音できます。

デフォルトでは、マイクのリダイレクトは許可されています。

セキュリティのため、デバイスによって信頼されていないサーバーがマイクにアクセスしようとすると、ユーザーに警告が表示されます。ユーザーはアクセスを許可するかどうかを選択できます。ユーザーはCitrix Workspace™アプリで警告を無効にできます。

WindowsマルチセッションOSマシンでは、複数のオーディオデバイスをサポートするために、オーディオプラグアンドプレイ設定が有効になっていることを確認してください。

ユーザーデバイスで**クライアントオーディオリダイレクト**設定が無効になっている場合、このルールは無効になります。

帯域幅ポリシー設定

「**帯域幅**」セクションには、クライアントセッションの帯域幅使用に関連するパフォーマンスの問題を回避するためのポリシー設定が含まれています。

重要: これらのポリシー設定を**マルチストリームポリシー**設定と併用すると、予期しない結果が生じる可能性があります。ポリシーでマルチストリーム設定を使用する場合は、これらの帯域幅制限ポリシー設定が含まれていないことを確認してください。

オーディオリダイレクト帯域幅制限

この設定は、ユーザーセッションでオーディオを再生または録音するために許可される最大帯域幅を指定します。許可される最大帯域幅は、1秒あたりのキロビット単位で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**オーディオリダイレクト帯域幅制限の割合**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

オーディオリダイレクトの帯域幅制限（パーセント）

この設定は、オーディオの再生または録音に許可される最大帯域幅制限を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**オーディオリダイレクト帯域幅制限**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

クライアントUSBデバイスリダイレクト帯域幅制限

この設定は、USBデバイスのクライアントとの間のリダイレクトに許可される最大帯域幅を指定します。許可される最大帯域幅は、1秒あたりのキロビット単位で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**クライアントUSBデバイスリダイレクト帯域幅制限の割合**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

クライアントUSBデバイスリダイレクトの帯域幅制限（パーセント）

この設定は、クライアントとの間でUSBデバイスをリダイレクトするために許可される最大帯域幅を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**クライアントUSBデバイスリダイレクト帯域幅制限**設定にも値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

クリップボードリダイレクト帯域幅制限

この設定は、セッションとローカルクリップボード間のデータ転送に許可される最大帯域幅を指定します。許可される最大帯域幅は、キロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**クリップボードリダイレクト帯域幅制限（パーセント）**設定にも値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

クリップボードリダイレクトの帯域幅制限（パーセント）

この設定は、セッションとローカルクリップボード間のデータ転送に許可される最大帯域幅を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**クリップボードリダイレクト帯域幅制限**設定にも値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

COMポートリダイレクトの帯域幅制限

注：Virtual Delivery Agent 7.0から7.8の場合、この設定はレジストリを使用して構成します。詳細については、「レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。

この設定は、クライアント接続でCOMポートにアクセスするために許可される最大帯域幅をキロビット/秒で指定します。この設定に値を入力し、**COMポートリダイレクト帯域幅制限（パーセント）**設定にも値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

COMポートリダイレクトの帯域幅制限（パーセント）

注：Virtual Delivery Agent 7.0から7.8の場合、この設定はレジストリを使用して構成します。詳細については、「レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。

この設定は、クライアント接続でCOMポートにアクセスするために許可される最大帯域幅を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**COMポートリダイレクト帯域幅制限**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な総帯域幅を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

ファイルリダイレクト帯域幅制限

この設定は、ユーザーセッションでクライアントドライブにアクセスするために許可される最大帯域幅を指定します。許可される最大帯域幅は、キロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**ファイルリダイレクト帯域幅制限の割合**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

ファイルリダイレクトの帯域幅制限（パーセント）

この設定は、クライアントドライブにアクセスするために許可される最大帯域幅制限を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**ファイルリダイレクト帯域幅制限**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な総帯域幅を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

HDX™ MediaStream マルチメディアアクセラレーション帯域幅制限

この設定は、HDX MediaStream マルチメディアアクセラレーションを使用してストリーミングオーディオおよびビデオを配信するために許可される最大帯域幅制限を指定します。許可される最大帯域幅は、キロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**HDX MediaStream Multimedia Acceleration帯域幅制限パーセント**設定の両方に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

HDX MediaStream Multimedia Acceleration帯域幅制限パーセント

この設定は、HDX MediaStream Multimedia Accelerationを使用してストリーミングオーディオおよびビデオを配信するために許可される最大帯域幅を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**HDX MediaStream Multimedia Acceleration帯域幅制限**設定の両方に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

LPTポートリダイレクト帯域幅制限

注：Virtual Delivery Agent 7.0から7.8の場合、この設定はレジストリを使用して構成します。詳細については、「レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。

この設定は、単一ユーザーセッションでLPTポートを使用する印刷ジョブに許可される最大帯域幅を指定します。許可される最大帯域幅は、キロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**LPTポートリダイレクト帯域幅制限パーセント**設定の両方に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

LPTポートリダイレクトの帯域幅制限（パーセント）

注：Virtual Delivery Agent 7.0から7.8の場合、この設定はレジストリを使用して構成します。詳細については、「レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。

この設定は、単一クライアントセッションでLPTポートを使用する印刷ジョブの帯域幅制限を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**LPTポートリダイレクト帯域幅制限**設定の両方に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

セッション全体の帯域幅制限

この設定は、ユーザーセッションで利用可能な総帯域幅を、1秒あたりのキロビット単位で指定します。

適用可能な最大帯域幅の上限は20 Mbps (20,000 Kbps)です。デフォルトでは、最大値（ゼロ）は指定されていません。

クライアント接続によって消費される帯域幅の量を制限すると、クライアント接続外の他のアプリケーションが限られた帯域幅を競合している場合に、パフォーマンスが向上する可能性があります。

プリンターリダイレクト帯域幅制限

この設定は、ユーザーセッションでクライアントプリンターにアクセスするために許可される最大帯域幅を指定します。許可される最大帯域幅は、1秒あたりのキロビット単位で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**Printer redirection bandwidth limit percent** 設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

プリンターリダイレクトの帯域幅制限（パーセント）

この設定は、クライアントプリンターにアクセスするために許可される最大帯域幅を、総セッション帯域幅の割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**Printer redirection bandwidth limit** 設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な総帯域幅を指定する**Overall session bandwidth limit** 設定も構成する必要があります。

TWAINデバイスリダイレクト帯域幅制限

この設定は、公開アプリケーションからTWAINイメージングデバイスを制御するために許可される最大帯域幅を指定します。許可される最大帯域幅は、1秒あたりのキロビット単位で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**TWAIN device redirection bandwidth limit percent** 設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

TWAINデバイスリダイレクト帯域幅制限の割合

この設定は、公開アプリケーションからTWAINイメージングデバイスを制御するために許可される最大帯域幅を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**TWAIN device redirection bandwidth limit** 設定にも値を入力した場合、最も制限の厳しい設定（値が小さい方）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**Overall session bandwidth limit** 設定も構成する必要があります。

双方向コンテンツリダイレクトポリシー設定

「**双方向コンテンツリダイレクト**」セクションには、クライアントからホストへ、およびホストからクライアントへのURLリダイレクトを有効または無効にするためのポリシー設定があります。

サーバーポリシーはStudioで設定されます。クライアントポリシーはCitrix Workspace™ appのグループポリシーオブジェクト管理用テンプレートから設定されます。

Citrix®は、ホストからクライアントへのリダイレクトと、クライアントからURLへのリダイレクトのためのLocal App Accessを提供しています。ただし、ドメイン参加済みWindowsクライアントには双方向コンテンツリダイレクトを使用することをお勧めします。

双方向コンテンツリダイレクトを許可

このポリシーを**許可**に設定すると、サーバー (VDA) とクライアント間のリダイレクトが有効になります。既定では**禁止**に設定されています。

「**クライアントにリダイレクトされる許可URL**」ポリシーを使用して、VDAからクライアントへのリダイレクト用のURLリストを構成します。

> **注：**
>
> リダイレクトを許可するには、このポリシーをクライアント上の**双方向コンテンツリダイレクト**ポリシーとともに設定する必要があります。

クライアントにリダイレクトされる許可されたURL

双方向コンテンツリダイレクトが許可されている場合に、クライアントで開くURLのリストを指定します。

セミコロン (;) は区切り文字です。アスタリスク (*) はワイルドカードとして使用できます。例:

```
*.xyz.com;https://www.example.com
```

ブラウザコンテンツリダイレクトポリシー設定

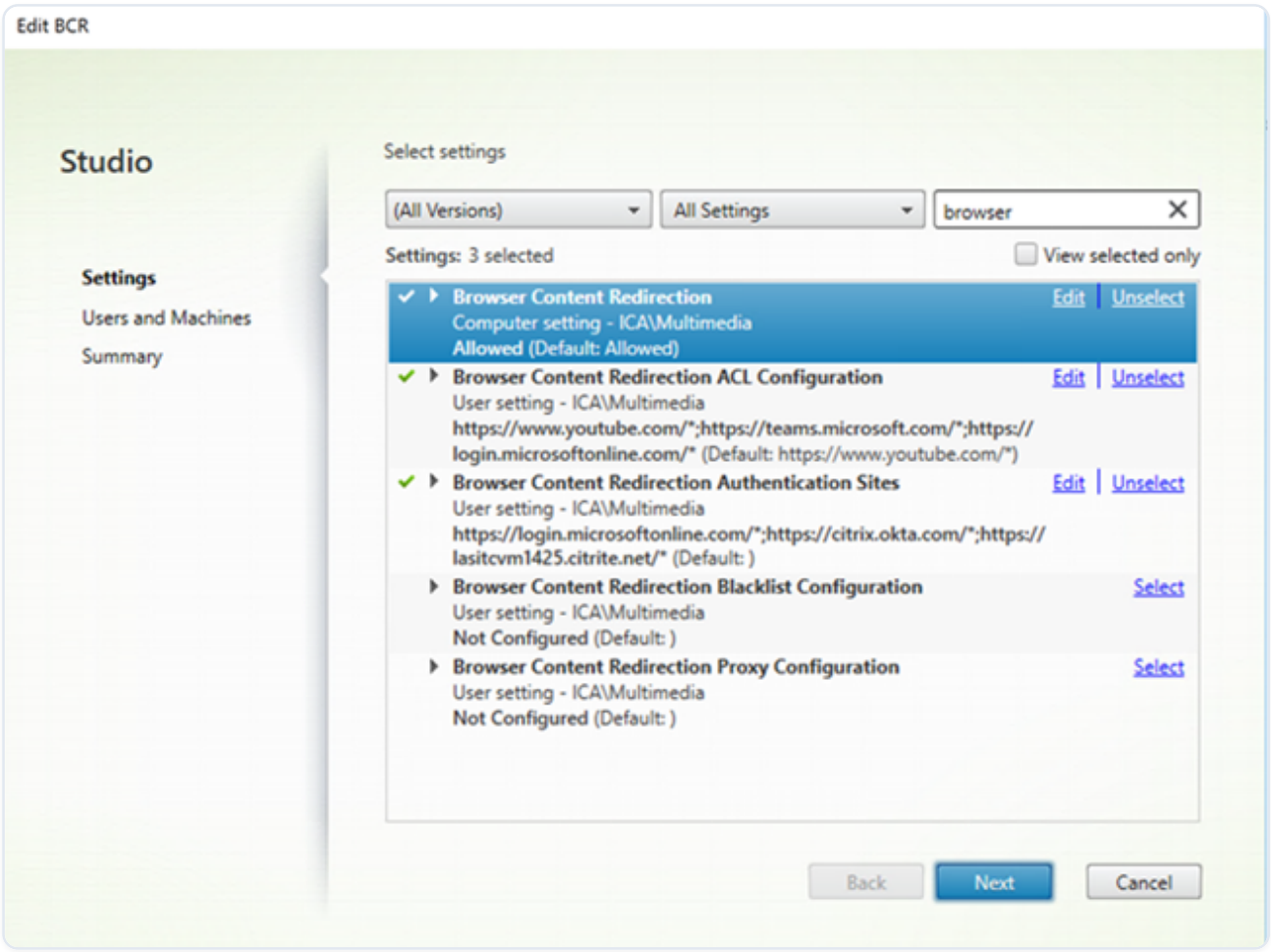
ブラウザコンテンツリダイレクトのセクションには、この機能を構成するためのポリシー設定が含まれています。

ブラウザコンテンツリダイレクトは、Citrix Virtual Apps and Desktops™がWebブラウザコンテンツ（HTML5など）をユーザーに配信する方法を制御し、最適化します。コンテンツが表示されるブラウザの可視領域のみがリダイレクトされます。

HTML5ビデオのリダイレクトとブラウザコンテンツのリダイレクトは、独立した機能です。この機能が動作するためにHTML5ビデオのリダイレクトポリシーは必要ありません。ただし、Citrix HDX HTML5 Video Redirection Serviceはブラウザコンテンツのリダイレクトに使用されます。詳しくは、「ブラウザコンテンツリダイレクト」を参照してください。

ポリシー設定：

Citrix Studioのブラウザコンテンツリダイレクト機能には、以下のポリシー設定が利用可能です。これらのポリシーはVDA上のレジストリキーで上書きできますが、レジストリキーはオプションです。



TLSとブラウザコンテンツリダイレクト

ブラウザコンテンツリダイレクトを使用して、HTTPS Webサイトをリダイレクトできます。これらのWebサイトに挿入されたJavaScriptは、VDAで実行されているCitrix HDX HTML5 Video Redirection Service（WebSocketService.exe）へのTLS接続を確立する必要があります。このリダイレクトを実現し、WebページのTLS整合性を維持するために、Citrix HDX HTML5 Video Redirection ServiceはVDAの証明書ストアに2つのカスタム証明書を生成します。

HdxVideo.jsは、セキュアWebソケットを使用して、VDAで実行されているWebSocketService.exeと通信します。このプロセスはローカルシステムで実行され、SSL終端とユーザーセッションマッピングを実行します。

WebSocketService.exeは、127.0.0.1ポート9001でリッスンしています。

ブラウザコンテンツリダイレクト

デフォルトでは、Citrix Workspace™アプリはクライアントフェッチとクライアントレンダリングを試行します。クライアントフェッチとクライアントレンダリングが失敗した場合、サーバー側レンダリングが試行されます。ブラウザコンテンツリダイレクトプロキシ構成ポリシーも有効にすると、Citrix Workspaceアプリはサーバーフェッチとクライアントレンダリングのみを試行します。

デフォルトでは、この設定は「許可」です。

ブラウザコンテンツリダイレクト統合Windows認証サポート設定

ブラウザコンテンツリダイレクトは、認証にNegotiateスキームを使用するオーバーレイを有効にします。この機能強化により、VDAと同じドメイン内で統合Windows認証（IWA）が構成されたWebサーバーへのシングルサインオンが提供されます。

許可に設定すると、ブラウザコンテンツリダイレクトオーバーレイはユーザーのVDA資格情報を使用してNegotiateチケットを取得します。その後、ユーザーはシングルサインオンでWebサーバーに認証されます。

禁止に設定すると、ブラウザコンテンツリダイレクトオーバーレイはVDAからNegotiateチケットを要求しません。ユーザーは基本認証方法を使用してWebサーバーに認証されます。この認証方法では、ユーザーはWebサーバーにアクセスするたびにVDA資格情報を入力する必要があります。

デフォルトでは、この設定は禁止されています。

ブラウザーコンテンツリダイレクトのサーバーフェッチWebプロキシ認証設定

この設定は、オーバーレイで発生するHTTPトラフィックをダウンストリームWebプロキシ経由でルーティングします。ダウンストリームWebプロキシは、ネゴシエート認証スキームを使用して、VDAユーザーのドメイン資格情報でHTTPトラフィックを承認および認証します。

ブラウザーコンテンツリダイレクトプロキシ構成ポリシーを使用して、PACファイルでサーバーフェッチモードのブラウザーコンテンツリダイレクトを構成する必要があります。PACスクリプトで、オーバーレイトラフィックをダウンストリームWebプロキシ経由でルーティングする手順

を指定します。次に、ネゴシエート認証スキームを使用してVDAユーザーを認証するようにダウンストリームWebプロキシを構成します。

許可に設定すると、Webプロキシは**Proxy-Authenticate: Negotiate**ヘッダーを含む407 Negotiateチャレンジで応答します。ブラウザーコンテンツリダイレクトは、VDAユーザーのドメイン資格情報を使用してKerberosサービスチケットを取得します。また、その後のWebプロキシへの要求にはサービスチケットを含めます。

禁止に設定すると、ブラウザーコンテンツリダイレクトは、オーバーレイとWebプロキシ間のすべてのTCPトラフィックを干渉することなくプロキシします。オーバーレイは、基本認証資格情報またはその他の利用可能な資格情報を使用してWebプロキシに認証します。

デフォルトでは、この設定は禁止されています。

ブラウザーコンテンツリダイレクトアクセス制御リスト（ACL）ポリシー設定

この設定を使用して、ブラウザーコンテンツリダイレクトを使用できる、またはブラウザーコンテンツリダイレクトへのアクセスを拒否されるURLのアクセス制御リスト（ACL）を構成します。

承認されたURLとは、コンテンツがクライアントにリダイレクトされる許可リスト内のURLです。

ワイルドカード * は許可されていますが、プロトコルまたはURLのドメインアドレス部分内では許可されていません。

許可: `http://www.xyz.com/index.html`, `https://www.xyz.com/*`, `http://www.xyz.com/*videos*`

不許可: `http://*.xyz.com/`

URLでパスを指定することで、より詳細な制御が可能です。たとえば、`https://www.xyz.com/sports/index.html`を指定した場合、index.htmlページのみがリダイレクトされます。

デフォルトでは、この設定は`https://www.youtube.com/*`に設定されています。

詳細については、Knowledge Centerの記事CTX238236を参照してください。

ブラウザーコンテンツリダイレクト認証サイト

この設定を使用して、URLのリストを構成します。ブラウザコンテンツリダイレクトを使用してリダイレクトされたサイトは、このリストを使用してユーザーを認証します。この設定は、許可リスト内のURLから移動した場合に、ブラウザコンテンツリダイレクトがアクティブ（リダイレクトされた状態）のままになるURLを指定します。

典型的なシナリオは、認証のためにIDプロバイダー（IdP）に依存するWebサイトです。たとえば、Webサイト `www.xyz.com` はエンドポイントにリダイレクトされる必要がありますが、Okta（ `www.xyz.okta.com`)のようなサードパーティのIdPが認証部分を処理します。管理者は、ブラウザコンテンツリダイレクトACL構成ポリシーを使用して `www.xyz.com` を許可リストに追加します。次に、ブラウザコンテンツリダイレクト認証サイトを使用して `www.xyz.okta.com` を許可リストに追加します。

詳細については、Knowledge Centerの記事CTX238236を参照してください。

ブラウザコンテンツリダイレクトブロックリスト設定

この設定は、ブラウザコンテンツリダイレクトACL構成設定と連携して機能します。ブラウザコンテンツリダイレクトACL構成設定とブロックリスト構成設定の両方にURLが存在する場合を考えます。この場合、ブロックリスト構成が優先され、URLのブラウザコンテンツはリダイレクトされません。

未承認URL: クライアントにリダイレクトされず、サーバーでレンダリングされるブロックリスト内のURLを指定します。

ワイルドカード * は許可されていますが、プロトコルまたはURLのドメインアドレス部分内では許可されていません。

許可されるもの: `http://www.xyz.com/index.html` , `https://www.xyz.com/*` , `http://www.xyz.com/*videos*`

不許可: `http://*.xyz.com/`

URLにパスを指定することで、より詳細な粒度を実現できます。たとえば、 `https://www.xyz.com/sports/index.html` を指定した場合、index.htmlのみがブロックリストに含まれます。

ブラウザコンテンツリダイレクトプロキシ設定

この設定は、ブラウザコンテンツリダイレクト用のVDA上のプロキシ設定の構成オプションを提供します。有効なプロキシアドレスとポート番号、PAC / WPAD URL、または直接/透過設定で有効になっている場合、Citrix Workspaceアプリはサーバーフェッチとクライアントレンダリングのみを試行します。

無効になっているか、構成されておらず、デフォルト値を使用している場合、Citrix Workspaceアプリはクライアントフェッチとクライアントレンダリングを試行します。

デフォルトでは、この設定は禁止されています。

明示的なプロキシの許可パターン:

`http://<hostname/ip address\>:\<port\>`

例:

`http://proxy.example.citrix.com:80` `http://10.10.10.10:8080`

PAC/WPADファイルの許可パターン:

`http://<hostname/ip address>:<port>/<path>/<Proxy.pac>`

例: `http://wpad.myproxy.com:30/configuration/pac/Proxy.pac`

`https://<hostname/ip address>:<port>/<path>/<wpad.dat>`

例: `http://10.10.10.10/configuration/pac/wpad.dat`

直接または透過プロキシに許可されるパターン:

ポリシーのテキストボックスに「**DIRECT**」と入力します。

ブラウザコンテンツリダイレクトのレジストリキーのオーバーライド

> **警告:**

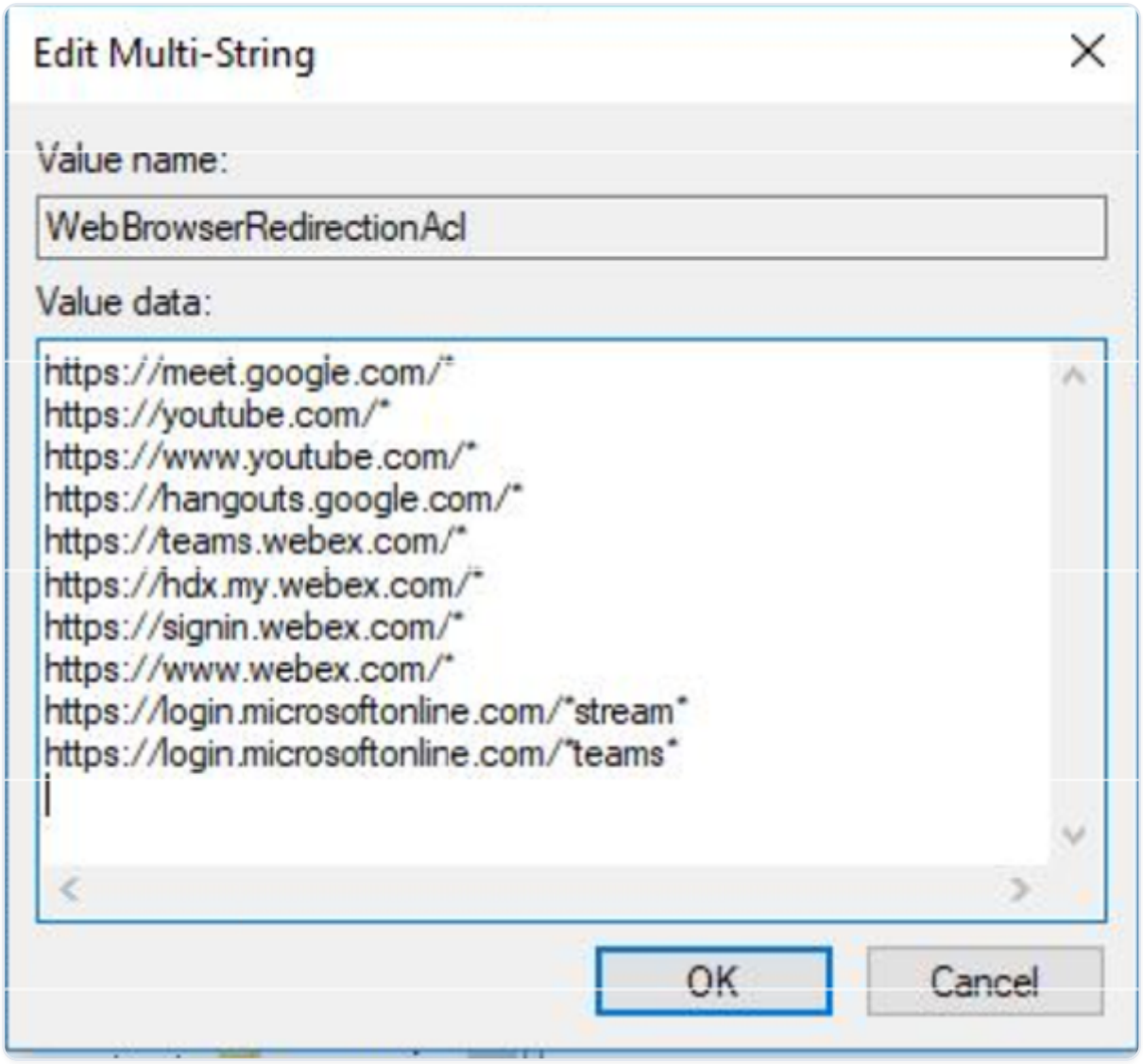
> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrixは、レジストリエディターの誤った使用によって生じる問題が解決されることを保証できません。レジストリエディターの使用は、お客様ご自身の責任において行ってください。編集する前に必ずレジストリをバックアップしてください。

> ポリシー設定のレジストリオーバーライドオプション:

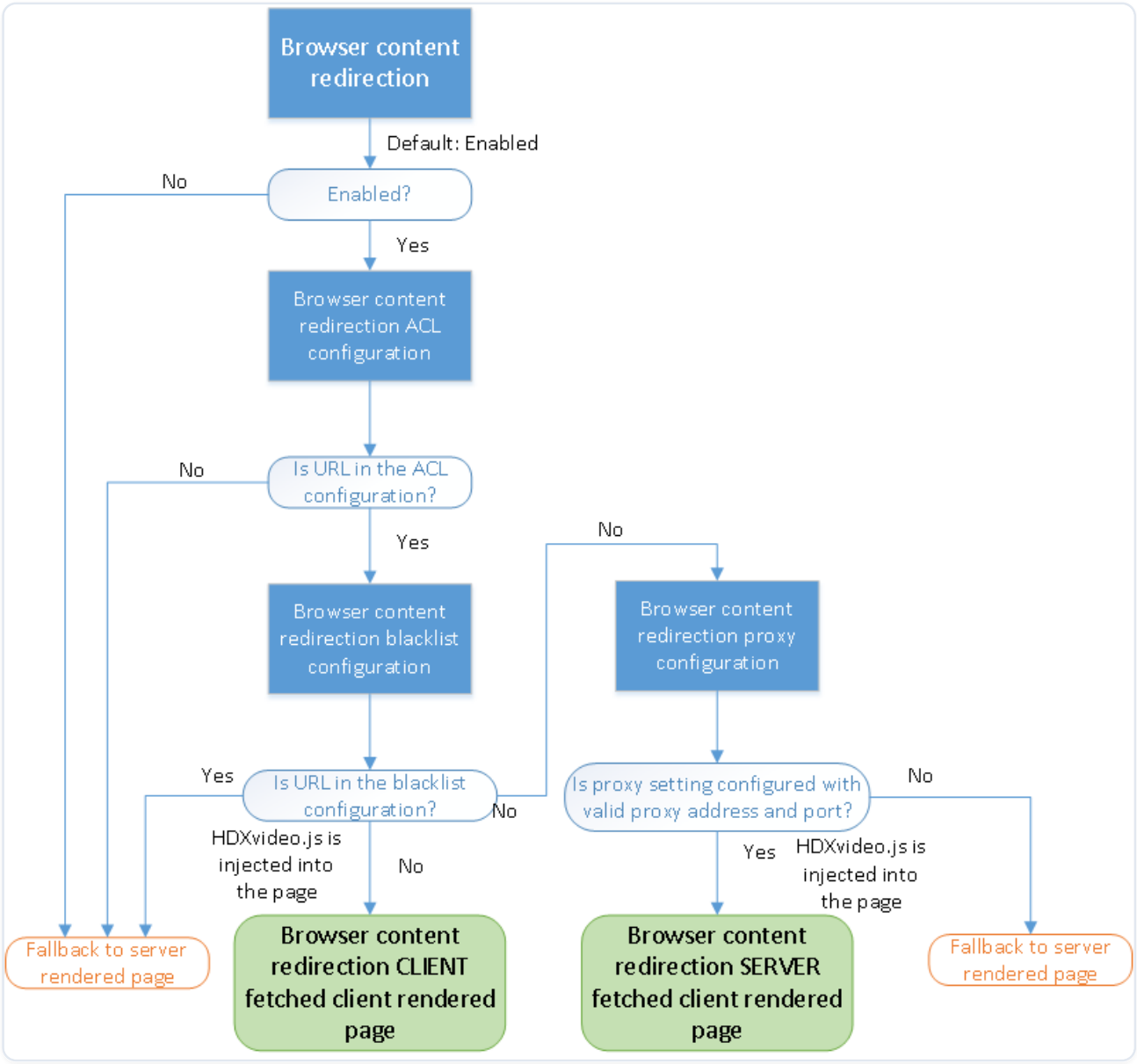
`\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediastream`

名前	タイプ	値
WebBrowserRedirection	DWORD	1=許可、0=禁止
WebBrowserRedirectionAcl	REG_MULTI_SZ	

名前	タイプ	値
WebBrowserRedirectionAuthenticationSites	REG_MULTI_SZ	
WebBrowserRedirectionProxyAddress	REG_SZ	`http://myproxy.citrix.com:8080` または `http://10.10.10.10:8888`
WebBrowserRedirectionBlacklist	REG_MULTI_SZ	



ブラウザコンテンツリダイレクトのためのHDXVideo.jsの挿入



HdxVideo.jsは、ブラウザコンテンツリダイレクトChrome拡張機能またはInternet Explorer Browser Helper Object (BHO) を使用して、ウェブページに挿入されます。BHOはInternet Explorer用のプラグインモデルです。これはブラウザAPIのフックを提供し、プラグインがページのDocument Object Model (DOM) にアクセスしてナビゲーションを制御できるようにします。

BHOは、特定のページにHdxVideo.jsを挿入するかどうかを決定します。この決定は、前のフローチャートに示されている管理ポリシーに基づいています。

JavaScriptを挿入し、ブラウザコンテンツをクライアントにリダイレクトすることを決定した後、VDA上のInternet Explorerブラウザではウェブページが空白になります。**document.body.innerHTML**を空に設定すると、VDA上のウェブページの本文全体が削除されます。ページは、クライアント上のオーバーレイブラウザ (Hdxbrowser.exe) に表示されるように、クライアントに送信される準備ができています。

クライアントセンサーポリシー設定

「**クライアントセンサー**」セクションには、ユーザーセッションでモバイルデバイスのセンサー情報がどのように処理されるかを制御するためのポリシー設定が含まれています。

アプリケーションによるクライアントデバイスの物理的な位置情報の使用を許可する

この設定は、モバイルデバイス上のセッションで実行されているアプリケーションが、ユーザーデバイスの物理的な位置情報を使用できるかどうかを決定します。

デフォルトでは、位置情報の使用は禁止されています。

この設定が禁止されている場合、アプリケーションが位置情報を取得しようとすると、「アクセス拒否」の値が返されます。

この設定が許可されている場合、ユーザーはCitrix Workspace™アプリの位置情報へのアクセス要求を拒否することで、位置情報の使用を禁止できます。AndroidおよびiOSデバイスでは、各セッションで位置情報が最初に要求されたときにプロンプトが表示されます。

「アプリケーションによるクライアントデバイスの物理的な位置情報の使用を許可する」設定を使用するホスト型アプリケーションを開発する際は、以下を考慮してください。

- 位置情報が有効なアプリケーションが位置情報の利用可能性に依存しないようにしてください。その理由は次のとおりです。
    - ユーザーが位置情報へのアクセスを許可しない可能性があります。
    - アプリケーションの実行中に位置情報が利用できない、または変更される可能性があります。
    - ユーザーが位置情報をサポートしていない別のデバイスからアプリケーションセッションに接続する可能性があります。
- 位置情報が有効なアプリケーションは、次の条件を満たす必要があります。
    - 位置情報機能をデフォルトでオフにする。
    - アプリケーションの実行中に、ユーザーがその機能を許可または禁止するオプションを提供する。
    - アプリケーションがキャッシュする位置データをクリアするオプションをユーザーに提供します。(Citrix Workspaceアプリは位置データをキャッシュしません。)
- 位置情報対応アプリケーションは、位置情報の粒度を管理する必要があります。この管理により、取得されたデータがアプリケーションの目的に適切であることが保証されます。また、関連するすべての法域の規制に準拠します。

- 位置情報サービスを使用する場合は、安全な接続 (TLS または VPN の使用など) を強制します。Citrix Workspaceアプリを信頼できるサーバーに接続します。
- 位置情報サービスの使用に関して、法的助言を得ることを検討してください。

デスクトップUIポリシー設定

デスクトップUIセクションには、デスクトップの壁紙、メニューアニメーション、ドラッグイメージなどの視覚効果を制御するポリシー設定が含まれています。これらのポリシー設定は、クライアント接続で使用される帯域幅の管理に役立ちます。帯域幅の使用量を制限することで、WANでのアプリケーションパフォーマンスを向上させることができます。

> **重要:**

> このリリースでは、レガシーグラフィックモードとデスクトップコンポジションリダイレクト（DCR）はサポートされていません。このポリシーは、以下を使用する場合の旧バージョンとの互換性のためだけに含められています。

> - XenApp 7.15 LTSR
> - XenDesktop 7.15 LTSR
> - Windows 7およびWindows 2008 R2を使用している以前のVDAリリース。

デスクトップコンポジションリダイレクト

この設定は、ユーザーによりスムーズなWindowsデスクトップエクスペリエンスを提供するために、ローカルのDirectXグラフィックレンダリングに以下の処理能力を使用するかどうかを指定します。

- ユーザーデバイス上のグラフィック処理ユニット（GPU）
- または、,
- ユーザーデバイス上の統合グラフィックプロセッサ（IGP）

有効にすると、**デスクトップコンポジションリダイレクト**は、サーバーの高いスケーラビリティを維持しながら、応答性の高いWindowsエクスペリエンスを提供します。

デフォルトでは、**デスクトップコンポジションリダイレクト**は無効になっています。

デスクトップコンポジションリダイレクトの選択を解除し、ユーザーセッションで必要な帯域幅を削減するには、この設定をポリシーに追加するときに、**無効**を選択します。

デスクトップコンポジションリダイレクトのグラフィック品質

この設定は、デスクトップコンポジションリダイレクトに使用されるグラフィックの品質を指定します。

デフォルトは「高」です。

「高」、「中」、「低」、または「ロスレス」品質から選択します。

デスクトップの壁紙

この設定は、ユーザーセッションでの壁紙の表示を許可または禁止します。

デフォルトでは、ユーザーセッションで壁紙を表示できます。

デスクトップの壁紙を選択解除し、ユーザーセッションで必要な帯域幅を削減するには、この設定をポリシーに追加する際に「**禁止**」を選択します。

メニューアニメーション

この設定は、ユーザーセッションでのメニューアニメーションを許可または禁止します。

デフォルトでは、メニューアニメーションは許可されています。

メニューアニメーションは、アクセシビリティのためのMicrosoftの個人設定です。有効にすると、短い遅延の後、スクロールまたはフェードインによってメニューが表示されます。メニューの下部には矢印アイコンが表示されます。その矢印をポイントするとメニューが表示されます。

このポリシー設定が「**許可**」に設定されており、メニューアニメーションのMicrosoft個人設定が有効になっている場合、デスクトップでメニューアニメーションが有効になります。

> **注：**
>
> メニューアニメーションのMicrosoft個人設定への変更は、デスクトップに影響を与えます。セッション終了時に変更を破棄するようにデスクトップを設定している場合を考慮してください。この場合、メニューアニメーションを有効にしているユーザーは、その後のセッションでメニューアニメーションを利用できない可能性があります。メニューアニメーションを必要とするユーザーに対しては、デスクトップのメインイメージでMicrosoft設定を有効にするか、デスクトップがユーザーの変更を保持するようにしてください。

ドラッグ中のウィンドウコンテンツの表示

この設定は、画面上でウィンドウをドラッグする際にウィンドウコンテンツの表示を許可または禁止します。

デフォルトでは、ウィンドウコンテンツの表示は許可されています。

「**許可**」に設定すると、ウィンドウをドラッグしたときにウィンドウ全体が移動するように見えます。「**禁止**」に設定すると、ドロップするまでウィンドウのアウトラインのみが移動するように見えます。

エンドユーザー監視ポリシー設定

「**エンドユーザー監視**」セクションには、セッションのトラフィックを測定するためのポリシー設定が含まれています。

ICA®ラウンドトリップ計算

この設定は、アクティブな接続に対してICAラウンドトリップ計算が実行されるかどうかを決定します。

デフォルトでは、アクティブな接続の計算は有効になっています。

デフォルトでは、各ICAラウンドトリップ測定の開始は遅延されます。この遅延は、ユーザーインタラクションを示すトラフィックが発生するまで続きます。この遅延は無期限に続く可能性があり、ICAラウンドトリップ測定がICAトラフィックの唯一の原因となるのを防ぐように設計されています。

ICAラウンドトリップ計算間隔

この設定は、ICAラウンドトリップ計算が実行される頻度を秒単位で指定します。

デフォルトでは、ICAラウンドトリップは15秒ごとに計算されます。

アイドル接続のICAラウンドトリップ計算

この設定は、アイドル接続に対してICAラウンドトリップ計算が実行されるかどうかを決定します。

デフォルトでは、アイドル接続に対して計算は実行されません。

デフォルトでは、各ICAラウンドトリップ測定の開始は遅延されます。この遅延は、ユーザーインタラクションを示すトラフィックが発生するまで続きます。この遅延は無期限に続く可能性があり、ICAラウンドトリップ測定がICAトラフィックの唯一の原因となるのを防ぐように設計されています。

強化されたデスクトップエクスペリエンスポリシー設定

強化されたデスクトップエクスペリエンスポリシー設定は、ローカルのWindows 7デスクトップのように見えるサーバーオペレーティングシステム上でセッションを実行します。

デフォルトでは、この設定は許可されています。

仮想デスクトップ上にWindowsクラシックテーマのユーザープロファイルが存在する場合、このポリシーはそのユーザーに強化されたデスクトップエクスペリエンスを提供しません。Windows 7テーマのユーザープロファイルを持つユーザーが、Windows Server 2012を実行している仮想デスクトップにログオンする場合を考えます。また、このポリシーが構成されていないか、無効になっている場合、そのユーザーはテーマの適用に失敗したことを示すエラーメッセージを目にします。

どちらの場合も、ユーザープロファイルをリセットすることで問題が解決します。

アクティブなユーザーセッションを持つ仮想デスクトップでポリシーを無効にすると、それらのセッションのインターフェイスは、Windows 7およびWindows Classicデスクトップで一貫性がなくなります。この不整合を避けるために、このポリシー設定を変更した後、仮想デスクトップを再起動してください。その後、仮想デスクトップ上のすべてのローミングプロファイルを削除します。Citrix®は、プロファイル間の不整合を避けるために、仮想デスクトップ上の他のユーザープロファイルも削除することを推奨します。

環境でローミングユーザープロファイルを使用しているとします。この場合、プロファイルを共有するすべての仮想デスクトップで、強化されたデスクトップエクスペリエンス機能が有効または無効になっていることを確認してください。

Citrixは、サーバーオペレーティングシステムとクライアントオペレーティングシステムを実行している仮想デスクトップ間でローミングプロファイルを共有することを推奨しません。クライアントおよびサーバーオペレーティングシステムのプロファイルは異なります。両方のタイプ間でローミングプロファイルを共有すると、ユーザーが両者の間を移動する際にプロファイルプロパティに不整合が生じる可能性があります。

ファイルリダイレクトポリシー設定

ファイルリダイレクトセクションには、クライアントドライブマッピングおよびクライアントドライブ最適化に関連するポリシー設定が含まれています。

クライアントドライブの自動接続

この設定は、ユーザーがログオンしたときのクライアントドライブの自動接続を許可または禁止します。

デフォルトでは、自動接続は許可されています。

この設定をポリシーに追加するときは、自動接続するドライブの種類の設定を必ず有効にしてください。たとえば、ユーザーのCD-ROMドライブの自動接続を許可するには、この設定と**クライアント光学ドライブ**設定を構成します。

関連するポリシー設定は次のとおりです。

- **クライアントドライブリダイレクト**
- **クライアントフロッピーディスクドライブ**
- **クライアント光学ドライブ**
- **クライアント固定ドライブ**
- **クライアントネットワークドライブ**
- **クライアントリムーバブルドライブ**

クライアントドライブリダイレクト

この設定は、ユーザーデバイス上のドライブとの間でファイルリダイレクトを有効または無効にします。

デフォルトでは、ファイルリダイレクトは有効になっています。

> **注：**
>
> クライアントドライブリダイレクトポリシー設定は、汎用USBリダイレクトを使用してセッションにマップされたドライブには適用されません。

> 有効にすると、ユーザーはすべてのクライアントドライブにファイルを保存できます。無効にすると、すべてのファイルリダイレクトが防止されます。この構成は、個々のファイルリダイレクト設定の状態に関係なく適用されます。個々のファイルリダイレクト設定には、クライアントフロッピードライブとクライアントネットワークドライブが含まれます。

関連するポリシー設定は次のとおりです。

- **クライアントフロッピードライブ**
- **クライアント光学ドライブ**
- **クライアント固定ドライブ**
- **クライアントネットワークドライブ**
- **クライアントリムーバブルドライブ**

クライアント固定ドライブ

この設定により、ユーザーはユーザーデバイス上の固定ドライブにアクセスしたりファイルを保存したりできるようになります。

デフォルトでは、クライアント固定ドライブへのアクセスは許可されています。

この設定をポリシーに追加する場合は、**クライアントドライブリダイレクト**設定が存在し、許可に設定されていることを確認してください。これらの設定が無効になっている場合、クライアント固定ドライブはマップされず、**クライアント固定ドライブ**設定の状態に関係なく、ユーザーはこれらのドライブに手動でアクセスできません。

ユーザーがログオンしたときに固定ドライブが自動的に接続されるように、**クライアントドライブの自動接続**設定を構成します。

クライアントフロッピードライブ

この設定により、ユーザーはユーザーデバイス上のフロッピードライブにアクセスしたりファイルを保存したりできるようになります。

デフォルトでは、クライアントフロッピードライブへのアクセスは許可されています。

この設定をポリシーに追加する場合、「**クライアントドライブのリダイレクト**」設定が存在し、「許可」に設定されていることを確認してください。これらの設定が無効になっている場合、クライアントフロッピーディスクドライブはマップされず、ユーザーは「**クライアントフロッピーディスクドライブ**」設定の状態にかかわらず、これらのドライブに手動でアクセスできません。

ユーザーがログオンしたときにフロッピーディスクドライブが自動的に接続されるようにするには、「**クライアントドライブの自動接続**」設定を構成します。

クライアントネットワークドライブ

この設定は、ユーザーがユーザーデバイスを介してネットワーク（リモート）ドライブにファイルにアクセスしたり保存したりすることを許可または禁止します。

デフォルトでは、クライアントネットワークドライブへのアクセスは許可されています。

この設定をポリシーに追加する場合、「**クライアントドライブのリダイレクト**」設定が存在し、「許可」に設定されていることを確認してください。これらの設定が無効になっている場合、クライアントネットワークドライブはマップされず、ユーザーはこれらのドライブに手動でアクセスできません。この構成は、「**クライアントネットワークドライブ**」設定の状態にかかわらず適用されます。

ユーザーがログオンしたときにネットワークドライブが自動的に接続されるようにするには、「**クライアントドライブの自動接続**」設定を構成します。

クライアント光学ドライブ

この設定は、ユーザーが以下の場所にファイルにアクセスしたり保存したりすることを許可または禁止します。

- ユーザーデバイス上のCD-ROM
- ユーザーデバイス上のDVD-ROM
- ユーザーデバイス上のBD-ROMドライブ。

デフォルトでは、クライアント光学ドライブへのアクセスは許可されています。

この設定をポリシーに追加する場合、「**クライアントドライブのリダイレクト**」設定が存在し、「**許可**」に設定されていることを確認してください。これらの設定が無効になっている場合、クライアント光学ドライブはマップされず、ユーザーはこれらのドライブに手動でアクセスできません。この構成は、「**クライアント光学ドライブ**」設定の状態にかかわらず適用されます。

ユーザーがログオンしたときに光学ドライブが自動的に接続されるようにするには、「**クライアントドライブの自動接続**」設定を構成します。

クライアントリムーバブルドライブ

この設定により、ユーザーはユーザーデバイス上のUSBドライブへのファイルアクセスまたは保存を許可または禁止されます。

デフォルトでは、クライアントリムーバブルドライブへのアクセスは許可されています。

この設定をポリシーに追加する際は、**クライアントドライブのリダイレクト**設定が存在し、「許可」に設定されていることを確認してください。これらの設定が無効になっている場合、クライアントリムーバブルドライブはマップされず、ユーザーはこれらのドライブに手動でアクセスできません。この構成は、**クライアントリムーバブルドライブ**設定の状態に関係なく適用されます。

ユーザーがログオンしたときにリムーバブルドライブが自動的に接続されるように、**クライアントドライブの自動接続**設定を構成します。

ホストからクライアントへのリダイレクト

この設定により、URLおよび一部のメディアコンテンツのファイルタイプ関連付けを有効または無効にし、ユーザーデバイスで開くことができます。無効にすると、コンテンツはサーバーで開かれます。

デフォルトでは、ファイルタイプ関連付けは無効になっています。

この設定を有効にすると、以下のURLタイプがローカルで開かれます。

- HTTP
- HTTPS
- リアルプレーヤーおよびQuickTime (RTSP)
- リアルプレーヤーおよびQuickTime (RTSPU)
- レガシーReal Player (PNM)
- マイクロソフト メディア サーバー (MMS)

クライアントドライブ文字の保持

この設定により、クライアントドライブをセッション内で同じドライブ文字にマップすることを有効または無効にします。

デフォルトでは、クライアントドライブ文字は保持されません。

この設定をポリシーに追加する場合は、**クライアントドライブのリダイレクト**設定が存在し、許可に設定されていることを確認してください。

読み取り専用クライアントドライブアクセス

この設定は、ユーザーとアプリケーションが以下の操作を行うことを許可または禁止します。

- マップされたクライアントドライブ上にファイルを作成する
- マップされたクライアントドライブ上のファイルを変更する
- マップされたクライアントドライブ上のフォルダーを変更する

デフォルトでは、マップされたクライアントドライブ上のファイルとフォルダーは変更できます。

有効に設定されている場合、ファイルとフォルダーは読み取り専用権限でアクセスできます。

この設定をポリシーに追加する場合は、**クライアントドライブのリダイレクト**設定が存在し、許可に設定されていることを確認してください。

特殊フォルダーのリダイレクト

この設定は、Citrix Workspace™アプリおよびWeb Interfaceのユーザーが、セッションからローカルのドキュメントおよびデスクトップの特殊フォルダーを表示することを許可または禁止します。

デフォルトでは、特殊フォルダーのリダイレクトは許可されています。

この設定は、ポリシーによってフィルター処理されたオブジェクトが特殊フォルダーのリダイレクトを持つことを防ぎます。これは、他の場所に存在する設定に関係なく適用されます。この設定が禁止されている場合、StoreFront™、Web Interface、またはCitrix Workspaceアプリに指定された関連設定はすべて無視されます。

どのユーザーが特殊フォルダーのリダイレクトを使用できるかを定義するには、**許可**を選択し、この機能を適用したいユーザーでフィルター処理されたポリシーにこの設定を含めます。この設定は、他のすべての特殊フォルダーのリダイレクト設定を上書きします。

ユーザーがローカルハードドライブ上のファイルにアクセスしたり保存したりするのを防ぐポリシー設定は、特殊フォルダーリダイレクトの動作も妨げます。この状況は、特殊フォルダーリダイレクトがユーザーデバイスと対話する必要があるために発生します。

この設定をポリシーに追加する際は、**クライアント固定ドライブ**設定が存在し、「許可」に設定されていることを確認してください。

非同期書き込みを使用する

この設定は、非同期ディスク書き込みを有効または無効にします。

デフォルトでは、非同期書き込みは無効になっています。

非同期ディスク書き込みは、比較的高い帯域幅と高い遅延が特徴であるWAN経由でのファイル転送速度とクライアントディスクへの書き込み速度を向上させることができます。ただし、接続またはディスクに障害が発生した場合、書き込み中のクライアントファイルが未定義の状態になる可能性があります。この未定義の状態が発生した場合、ポップアップウィンドウで影響を受けるファイルがユーザーに通知されます。ユーザーは、再接続時またはディスク障害が修正されたときに中断されたファイル転送を再開するなどの是正措置を講じることができます。

Citrix®は、リモート接続が必要で、良好なファイルアクセス速度を持ち、接続またはディスク障害が発生した場合に失われたファイルやデータを容易に回復できるユーザーに対してのみ、非同期ディスク書き込みを有効にすることを推奨します。

この設定をポリシーに追加する際は、**クライアントドライブリダイレクト**設定が存在し、「許可」に設定されていることを確認してください。この設定が無効になっている場合、非同期書き込みは行われません。

グラフィックポリシー設定

グラフィックセクションには、ユーザーセッションで画像がどのように処理されるかを制御するためのポリシー設定が含まれています。

視覚的にロスレスな圧縮を許可する

この設定により、グラフィックに対して、真のロスレス圧縮の代わりに視覚的にロスレスな圧縮を使用できます。視覚的にロスレスな圧縮は、真のロスレス圧縮よりもパフォーマンスが向上しますが、目視では気づかない程度のわずかな損失があります。この設定は、視覚品質設定の値の使用方法を変更します。

デフォルトでは、この設定は無効になっています。

グラフィックステータスインジケーター

この設定は、グラフィックステータスインジケーターをユーザーセッションで実行するように構成します。このツールを使用すると、ユーザーはアクティブなグラフィックモードに関する情報を確認できます。この情報には、ビデオコーデック、ハードウェアエンコード、画質、およびセッションで使用中のモニターに関する詳細が含まれます。グラフィックステータスインジケーターを使用すると、ユーザーはピクセルパーフェクトモードを有効または無効にすることもできます。

Citrix Virtual Apps and Desktops™ 2103以降のリリースには、画質とインタラクティブ性の適切なバランスをユーザーが見つけるのに役立つ画質スライダーが含まれています。

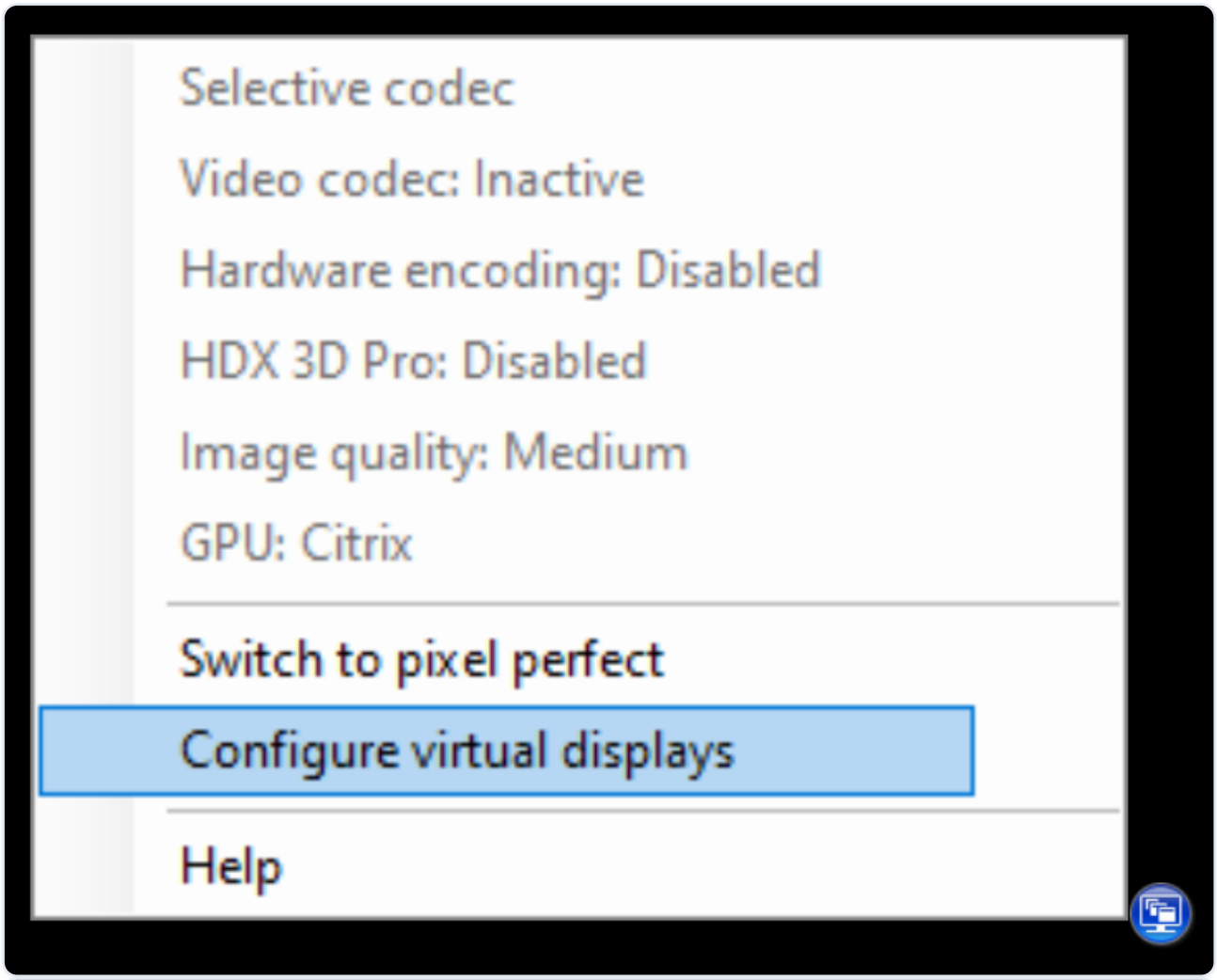
Citrix Virtual Apps and Desktops 2109以降のリリースには、グラフィックステータスインジケーターを使用して起動されるユーザーインターフェイスを介して仮想ディスプレイレイアウトを構成する機能が含まれています。

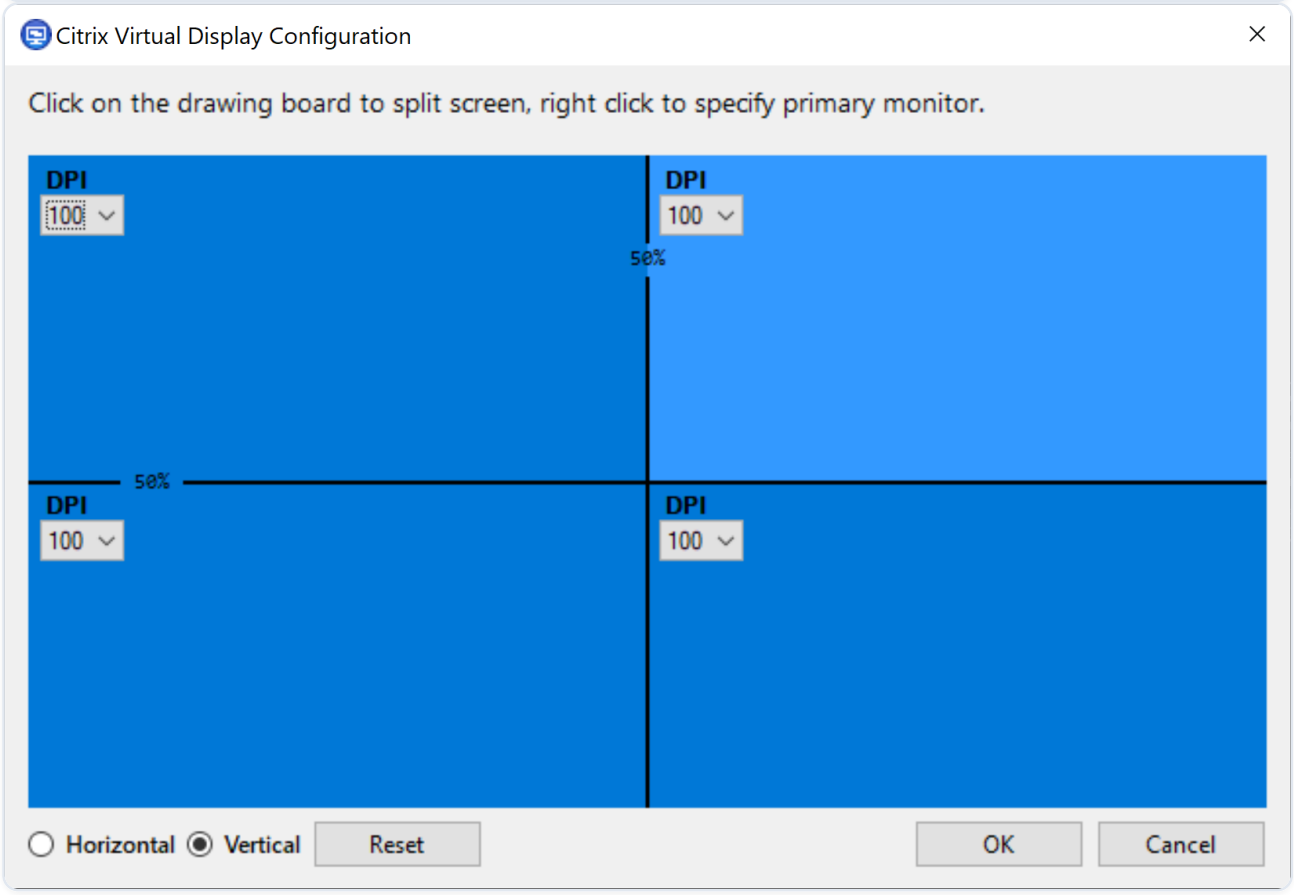
グラフィックステータスインジケーターは、以前のバージョンのロスレスインジケーターツールを置き換えます。このポリシーは、Citrix Virtual Apps and Desktopsバージョン7.16から1809までのでロスレスインジケーターを有効にします。

仮想ディスプレイレイアウト

仮想ディスプレイレイアウト機能は、すでにCitrix Workspace™ app for Windowsの一部ですが、VDAの一部にもなりました。この機能を使用すると、ライブセッション内のVDAで仮想モニターレイアウトを定義し、セッションモニターをリモートデスクトップ上で最大8つの仮想ディスプレイに仮想的に分割できます。グラフィックステータスインジケーターアイコンを右クリックし、仮想ディスプレイ構成UIを起動する**仮想ディスプレイの構成**オプションを選択することで、仮想モニターを構成できます。そこでは、水平線または垂直線を描画して、画面を仮想モニターに分割できます。UI上の仮想モニターを右クリックすると、それがプライマリモニターとしてマークされます。画面は、セッションモニターの解像度の指定された割合に従って分割されます。仮想ディスプレイのDPIを設定することもできます。

仮想モニターレイアウトを定義した後、**OK**をクリックすると、仮想ディスプレイレイアウトがすぐに適用されます。**キャンセル**をクリックすると、UIが閉じられ、すべての変更が破棄されます。


Selective codec
Video codec: Inactive
Hardware encoding: Disabled
HDX 3D Pro: Disabled
Image quality: Medium
GPU: Citrix
Switch to pixel perfect
Configure virtual displays
Help


Citrix Virtual Display Configuration
Click on the drawing board to split screen, right click to specify primary monitor.
DPI
100
DPI
100
50%
50%
DPI
100
DPI
100
Horizontal
Vertical
Reset
OK
Cancel

この構成はデスクトップセッションにのみ適用され、公開アプリケーションには影響しません。マルチモニターのシナリオでは、仮想ディスプレイの総数がサポートされている最大8つの仮想ディスプレイを超えない場合、同じ構成の仮想ディスプレイレイアウトがすべてのセッションモニターに適用されます。この制限を超えた場合、仮想ディスプレイレイアウトは無視され、どのセッションモニターにも適用されません。

定義された仮想ディスプレイ構成は、クライアントデバイスごとにユーザーごとに保存されます。この構成は、特定のユーザーに対する特定のクライアントからの以降のすべての接続に適用されます。セッションのリサイズ、セッションの切断/再接続、セッションのログオフ/ログオン後も保持されます。

この機能をCitrix Workspace Appの既存の仮想ディスプレイ機能と同時に使用しないでください。

画面共有

この設定により、ユーザーは画面コンテンツ、キーボード、マウスを含むセッションを他のユーザーと共有できます。

デフォルトでは、この設定は無効になっています。

VDAは、TCPポート範囲のポートを使用してデータを交換しようとします。これは、最も低いポートから始まり、その後の接続ごとに増分されます。このポートは、インバウンドトラフィックとアウトバウンドトラフィックの両方を処理します。

既定では、TCPポート範囲は52525〜52625に設定されています。

画面共有に使用されるポートは、ファイアウォールの例外リストに追加する必要があります。このオプションは、VDAのインストール時にチェックボックスとして表示されます。既定では、このオプションはチェックされていません。

ディスプレイメモリ制限

この設定は、セッションの最大ビデオバッファサイズをキロバイト単位で指定します。

デフォルトでは、ディスプレイメモリの制限は65,536キロバイトです。

セッションの最大ビデオバッファサイズをキロバイト単位で指定します。128から4,194,303までのキロバイト単位の量を指定します。最大値4,194,303はディスプレイメモリを制限しません。デフォルトでは、ディスプレイメモリは65,536キロバイトです。接続に高い色深度と高解像度を使用すると、より多くのメモリが必要になります。レガシーグラフィックモードでは、メモリ制限に達すると、「ディスプレイモードの劣化設定」に従ってディスプレイが劣化します。

より高い色深度と高解像度を必要とする接続の場合は、制限を増やしてください。次の式を使用して、必要な最大メモリを計算します。

メモリ深度（バイト）=（1ピクセルあたりのビット単位の色深度）/ 8）x（ピクセル単位の垂直解像度）x（ピクセル単位の水平解像度）。

たとえば、色深度が32、垂直解像度が600、水平解像度が800のシナリオを考えてみましょう。この場合、必要な最大メモリは（32 / 8）x（600）x（800）= 1920000バイトであり、ディスプレイメモリの制限は1920 KBになります。

32ビット以外の色深度は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ使用できます。

HDX™ は、各セッションに必要なディスプレイメモリの量のみを割り当てます。したがって、一部のユーザーのみがデフォルトよりも多くを必要とする場合でも、ディスプレイメモリの制限を増やすことによるスケーラビリティへの悪影響はありません。

ディスプレイモードの劣化設定

> **注：**
>
> Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

> セッションの表示メモリ制限に達した場合、この設定は、色深度と解像度のどちらが先に劣化するかを指定します。

デフォルトでは、色深度が先に劣化します。

セッションメモリ制限に達すると、表示される画像の品質を低下させることができます。この品質は、色深度と解像度のどちらを先に劣化させるかを選択することで低下させることができます。色深度が先に劣化する場合、表示される画像はより少ない色を使用します。解像度が先に劣化する場合、表示される画像は1インチあたりのピクセル数が少なくなります。

色深度または解像度が劣化した場合にユーザーに通知するには、「表示モードが劣化した場合にユーザーに通知」設定を構成します。

動的ウィンドウプレビュー

この設定は、シームレスウィンドウの表示を有効または無効にします。

- フリップ-
- フリップ 3D

- タスクバープレビュー
- Windows ピーク

WINDOWS AERO プレビューオプション	説明
タスクバープレビュー	ユーザーがウィンドウのタスクバーアイコンにマウスカーソルを合わせると、そのウィンドウの画像がタスクバーの上に表示されます。
Windows ピーク	ユーザーがタスクバーのプレビュー画像にマウスカーソルを合わせると、ウィンドウのフルサイズの画像が画面に表示されます。
フリップ	ユーザーが ALT+TAB を押すと、開いている各ウィンドウの小さなプレビューアイコンが表示されます。
フリップ 3D	ユーザーが TAB+Windows ロゴキーを押すと、開いているウィンドウの大きな画像が画面にカスケード表示されます。

デフォルトでは、この設定は有効になっています。

イメージキャッシュ

> **注：**
>
> Virtual Delivery Agent 7.x の場合、このポリシー設定は、レガシーグラフィックモードのポリシー設定が有効になっている場合にのみ適用されます。

この設定は、セッション内の画像のセクションのキャッシュと取得を有効または無効にします。画像をセクションにキャッシュし、必要に応じてこれらのセクションを取得すると、次のことが可能になります。

- ユーザーデバイスでのスクロールがよりスムーズになる
- ユーザーデバイスでのネットワーク経由で送信されるデータ量を削減する
- ユーザーデバイスで必要な処理を削減する

デフォルトでは、画像キャッシュ設定は有効になっています。

> **注：**
>
> 画像キャッシュ設定は、画像がどのようにキャッシュされ、取得されるかを制御します。この設定は、画像がキャッシュされるかどうかを制御するものではありません。画像は、レガシーグラフィックモード設定が有効になっている場合にキャッシュされます。

レガシーグラフィックモード - サポートされていません。下位互換性のためのみ

> **重要:**
>
> このリリースでは、レガシーグラフィックモードとデスクトップコンポジションリダイレクト (DCR) はサポートしていません。このポリシーは、XenApp 7.15 LTSR、XenDesktop 7.15 LTSR、およびWindows 7とWindows 2008 R2を使用する以前のVDAリリースとの下位互換性のためのみに含まれています。

> この設定は、リッチグラフィックエクスペリエンスを無効にします。この設定を使用して、レガシーグラフィックエクスペリエンスに戻し、WANまたはモバイル接続での帯域幅消費を削減します。XenAppおよびXenDesktop 7.13で導入された帯域幅削減により、このモードは廃止されました。

デフォルトでは、この設定は無効になっており、ユーザーにはリッチグラフィックエクスペリエンスが提供されます。

レガシーグラフィックモードは以下でサポートされています。

- ウィンドウズ 7
- ウィンドウズ サーバー 2008 R2 VDA。

レガシーグラフィックモードは以下ではサポートされていません。

- Windows 8.xおよび10
- Windows Server 2012、2012 R2、および2016。

XenAppおよびXenDesktop 7.6 FP3以降でのグラフィックモードとポリシーの最適化について詳しくは、CTX202687を参照してください。

最大許容色深度

> **注：**
>
> Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

> この設定は、セッションで許可される最大色深度を指定します。

デフォルトでは、最大許容色深度は32ビット/ピクセルです。

この設定は、Thinwire ドライバーと接続にのみ適用されます。プライマリディスプレイドライバーとしてThinWire以外のドライバーを使用するVDAには適用されません。これらのVDAは、プライマリディスプレイドライバーとしてWindows Display Driver Model (WDDM) ドライバーを使用するVDAです。Windows 8などのWDDMドライバーをプライマリディスプレイドライバーとして使用するシングルセッションOS VDAの場合、この設定は無効です。Windows Server 2012 R2などのWDDMドライバーを使用するWindowsマルチセッションOS VDAの場合、この設定によりユーザーがVDAに接続できなくなる可能性があります。

高い色深度を設定すると、より多くのメモリが必要になります。メモリ制限に達したときに色深度を低下させるには、**表示モードの低下設定**を構成します。色深度が低下すると、表示される画像はより少ない色を使用します。

表示モードが低下したときにユーザーに通知する

> **注：**
>
> Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

> この設定は、色深度または解像度が低下したときに、ユーザーに簡単な説明を表示します。

デフォルトでは、ユーザーへの通知は無効になっています。

3Dグラフィックワークロード向けに最適化

この設定は、グラフィックを多用するワークロードに最適なデフォルト設定を構成します。グラフィックを多用するアプリケーションに重点を置くユーザーに対して、この設定を有効にします。

このポリシーは、セッションでGPUが利用可能な場合にのみ適用してください。このポリシーによって設定されたデフォルト設定を明示的に上書きするその他の設定が優先されます。

デフォルトでは、3Dグラフィックワークロード向けに最適化は無効になっています。

キューイングとトッシング

> **注：**
>
> Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。
>
> この設定は、別の画像に置き換えられたキュー内の画像を破棄します。

デフォルトでは、キューイングとトッシングは有効になっています。

この設定は、グラフィックがユーザーデバイスに送信される際の応答を改善します。この設定を構成すると、フレームがドロップされるため、アニメーションが途切れることがあります。

圧縮にビデオコーデックを使用する

エンドポイントでビデオデコードが利用可能な場合、グラフィックの圧縮にビデオコーデックの使用を許可します。「**画面全体**」が選択されている場合、ビデオコーデックはすべてのデフォルトコーデックとして適用されます。「**アクティブに変化する領域**」が選択されている場合、ビデオコーデックは画面上で常に変化する領域に使用され、その他のデータは静止画圧縮とビットマップキャッシュを使用します。エンドポイントでビデオデコードが利用できない場合、または「**ビデオコーデックを使用しない**」を指定した場合、静止画圧縮とビットマップキャッシュの組み合わせが使用されます。「**推奨時に使用**」が選択されている場合、システムはさまざまな要因に基づいて選択します。選択方法が強化されるにつれて、バージョン間で結果が異なる場合があります。

現在のシナリオに適切な設定をシステムが最善を尽くして選択できるようにするには、「**推奨時に使用**」を選択します。

特にサーバーレンダリングされたビデオや3Dグラフィックを多用する場合に、ユーザーエクスペリエンスと帯域幅の向上を最適化するには、「**画面全体**」を選択します。

特に低帯域幅でビデオパフォーマンスを向上させ、静的およびゆっくりと変化するコンテンツのスケーラビリティを維持するために最適化するには、「**アクティブに変化する領域**」を選択します。この設定はマルチモニター展開でサポートされています。

サーバーのCPU負荷を最適化し、多数のサーバーレンダリングされたビデオやその他のグラフィックを多用するアプリケーションがない場合に最適化するには、「**ビデオコーデックを使用しない**」を選択します。

デフォルトは「**推奨時に使用**」です。

ビデオにハードウェアエンコーディングを使用する

この設定により、利用可能な場合、グラフィックハードウェアを使用してビデオコーデックで画面要素を圧縮できます。そのようなハードウェアが利用できない場合、VDAはソフトウェアビデオコーデックを使用したCPUベースのエンコーディングにフォールバックします。

このポリシー設定のデフォルトオプションは「**有効**」です。

複数のモニターがサポートされています。

ビデオデコードをサポートするCitrix Workspaceアプリはすべて、ハードウェアエンコードで使用できます。

NVIDIA

NVIDIA GRID GPUの場合、ハードウェアエンコードはマルチセッションOSおよびシングルセッションOS用のVDAでサポートされています。

NVIDIA GPUはNVENCハードウェアエンコードをサポートしている必要があります。サポートされているGPUのリストについては、NVIDIA video codec SDKを参照してください。

NVIDIA GRIDにはドライバーバージョン3.1以降が必要です。NVIDIA Quadroにはドライバーバージョン362.56以降が必要です。CitrixはNVIDIA Release R361ブランチのドライバーを推奨しています。

ロスレステキストはNVENCハードウェアエンコードと互換性がありません。ロスレステキストを有効にした場合、ロスレステキストがNVENCハードウェアエンコードよりも優先されます。

アクティブに変化する領域に対するH.264ハードウェアコーデックの選択的な使用がサポートされています。

視覚的にロスレス（YUV 4:4:4）圧縮がサポートされています。視覚的にロスレス（グラフィックポリシー設定、視覚的にロスレス圧縮を許可）には、Citrix Workspaceアプリ1808以降またはCitrix Receiver for Windows 4.5以降が必要です。

インテル

Intel Iris Proグラフィックプロセッサの場合、ハードウェアエンコードはシングルセッションOSおよびマルチセッションOS用のVDAでサポートされています。

Intel Broadwellプロセッサファミリー以降のIntel Iris Proグラフィックプロセッサがサポートされています。Intel Remote Displays SDKバージョン1.0が必要であり、IntelのWebサイトからダウンロードできます: Remote Displays SDK。

ロスレステキストは、ビデオコーデックポリシーが画面全体に設定され、**3Dグラフィックワークロード向けに最適化**ポリシーが無効になっている場合にのみサポートされます。

視覚的にロスレス（YUV 4:4:4）はサポートされていません。

Intelエンコーダーは、最大8つのエンコードセッション（たとえば、1人のユーザーが8台のモニターを使用する場合、または8人のユーザーがそれぞれ1台のモニターを使用する場合）で良好なユーザーエクスペリエンスを提供します。8つ以上のエンコードセッションが必要な場合は、仮想マシンが接続するモニターの数を確認してください。管理者は、良好なユーザーエクスペリエンスを維持するために、このポリシー設定をユーザーごとまたはマシンごとに構成するかどうかを決定します。

AMD

AMDの場合、シングルセッションOS用VDAでハードウェアエンコードがサポートされています。

AMD GPUはRapidFire SDKをサポートする必要があります。例えば、AMD Radeon ProまたはFirePro GPUなどです。

エンコードを機能させるには、最新のAMDドライバーをインストールしてください。これらのドライバーは`<https://www.amd.com/en/support>`からダウンロードできます。

ロスレステキストはAMDハードウェアエンコードと互換性がありません。ロスレステキストを有効にした場合、ロスレステキストがAMDハードウェアエンコードよりも優先されます。

活発に変化する領域向けのH.264ハードウェアコーデックの選択的な使用がサポートされています。

キャッシュポリシー設定

このセクションには、クライアント接続の帯域幅が制限されている場合に、ユーザーデバイスで画像データをキャッシュすることを可能にするポリシー設定が含まれています。

永続キャッシュしきい値

注: Virtual Delivery Agent 7.xの場合、このポリシー設定は、**レガシーグラフィックモード**ポリシー設定が有効になっている場合にのみ適用されます。

この設定は、ユーザーデバイスのハードドライブにビットマップをキャッシュし、それにより、以前のセッションからの大きく頻繁に使用される画像の再利用を可能にします。

デフォルトでは、しきい値は1秒あたり3000000ビットです。

しきい値は、永続キャッシュ機能が有効になる下限を表します。たとえば、デフォルト値を使用すると、帯域幅が3000000 bpsを下回った場合、ビットマップはユーザーデバイスのハードドライブにキャッシュされます。

Framehawkポリシー設定

> **重要:**
>
> Citrix Virtual Apps and Desktops 7 1903以降、Framehawkはサポートされなくなりました。代わりに、Thinwireをアダプティブトランスポートを有効にして使用してください。

> **Framehawk**セクションには、サーバー上のFramehawkディスプレイチャネルを有効にして構成するポリシー設定が含まれています。

FRAMEHAWKディスプレイチャネル

有効にすると、サーバーはユーザーのグラフィックと入力のリモート処理にFramehawkディスプレイチャネルを使用しようとします。このディスプレイチャネルはUDPを使用して、損失と遅延の特性が高いネットワークでより良いユーザーエクスペリエンスを提供します。ただし、他のグラフィックモードよりも多くのサーバーリソースと帯域幅を使用する可能性もあります。

デフォルトでは、Framehawkディスプレイチャネルは無効になっています。

FRAMEHAWKディスプレイチャネルのポート範囲

このポリシー設定は、VDAがユーザーデバイスとFramehawkディスプレイチャネルデータを交換するために使用するUDPポート番号の範囲を指定します。ポート番号は*最小ポート番号*または*最大ポート番号*の形式です。VDAは、最小ポート番号から開始し、その後の試行ごとにインクリメントして、各ポートを使用しようとします。このポートはインバウンドおよびアウトバウンドトラフィックを処理します。

デフォルトでは、ポート範囲は3224,3324です。

キープアライブ ポリシー設定

Keep Alive セクションには、ICA® キープアライブメッセージを管理するためのポリシー設定が含まれています。

ICA キープアライブ タイムアウト

この設定は、連続するICAキープアライブメッセージ間の秒数を指定します。

デフォルトでは、キープアライブメッセージ間の間隔は60秒です。

ICAキープアライブメッセージを送信する1～3600秒の間隔を指定します。ネットワーク監視ソフトウェアが非アクティブな接続を閉じる役割を担っている場合は、この設定を構成しないでください。

ICA キープアライブメッセージ

この設定は、定期的なICAキープアライブメッセージの送信を有効または無効にします。

デフォルトでは、キープアライブメッセージは送信されません。

この設定を有効にすると、切断された接続が切断されるのを防ぎます。サーバーがアクティビティを検出しない場合、この設定により、Remote Desktop Services (RDS) がセッションを切断するのを防ぎます。サーバーは数秒ごとにキープアライブメッセージを送信し、セッションがアクティブであるかどうかを検出します。セッションがアクティブでなくなった場合、サーバーはそのセッションを切断済みとしてマークします。

セッションの信頼性を使用している場合、ICAキープアライブは機能しません。セッションの信頼性を使用していない接続に対してのみ、ICAキープアライブを構成してください。

関連するポリシー設定: セッションの信頼性接続。

ローカルアプリアクセス ポリシー設定

ローカルアプリアクセスセクションには、ユーザーのローカルにインストールされたアプリケーションとホストされたアプリケーションを管理するポリシー設定が含まれています。これらのポリシー設定は、ホストされたデスクトップ環境での統合を管理します。

ローカルアプリアクセスを許可

この設定は、ユーザーのローカルにインストールされたアプリケーションとホストされたアプリケーションの統合を許可または禁止します。これらのポリシー設定は、ホストされたデスクトップ環境での統合を管理します。

ユーザーがローカルにインストールされたアプリケーションを起動すると、そのアプリケーションは実際にはローカルで実行されているにもかかわらず、仮想デスクトップ内で実行されているように見えます。

ローカルアプリアクセスを許可ポリシー設定を**有効**にすると、ブラウザコンテンツリダイレクトはサポートされず、デスクトップセッションにクライアント側の通知領域のバッテリーステータスは表示されません。

デフォルトでは、**ローカルアプリアクセスを許可**は禁止されています。

URLリダイレクトブロックリスト

この設定は、ローカルのWebブラウザにリダイレクトされて起動されるWebサイトを指定します。これらのWebサイトには、次のものが含まれる場合があります。

- msn.comやnewsgoogle.comなど、ロケール情報を必要とするWebサイト
- または
- ユーザーデバイスでより適切にレンダリングされるリッチメディアコンテンツを含むWebサイト。

デフォルトでは、サイトは指定されていません。

URLリダイレクト許可リスト

この設定は、起動された環境でレンダリングされるWebサイトを指定します。

デフォルトでは、サイトは指定されていません。

モバイルエクスペリエンスポリシー設定

「**モバイルエクスペリエンス**」セクションには、Citrix Mobility Packを処理するためのポリシー設定が含まれています。

キーボードの自動表示

この設定は、モバイルデバイスの画面でのキーボードの自動表示を有効または無効にします。

デフォルトでは、キーボードの自動表示は無効になっています。

タッチ最適化デスクトップの起動

この設定は無効になっており、Windows 10またはWindows Server 2016マシンでは使用できません。

この設定は、Citrix Workspace™アプリの全体的なインターフェイス動作を決定します。この設定により、タブレットデバイス向けに最適化されたタッチフレンドリーなインターフェイスを許可または禁止します。

デフォルトでは、タッチフレンドリーなインターフェイスが使用されます。

Windowsインターフェイスのみを使用するには、このポリシー設定を「禁止」に設定します。

コンボボックスのリモート化

この設定は、モバイルデバイスのセッションで表示できるコンボボックスの種類を決定します。このポリシー設定を「許可」に設定すると、デバイスネイティブのコンボボックスコントロールが表

示されます。この設定が許可されている場合、ユーザーはCitrix Workspace app for iOSセッション設定を変更して、Windowsコンボボックスを使用できます。

デフォルトでは、**コンボボックスのリモート化**機能は禁止されています。

マルチメディアポリシー設定

「**マルチメディア**」セクションには、ユーザーセッションにおけるストリーミングHTML5およびWindowsのオーディオとビデオを管理するためのポリシー設定が含まれています。

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

マルチメディアポリシー

デフォルトでは、Delivery Controller™で設定されたすべてのマルチメディアポリシーは、以下のレジストリに保存されます。

マシンポリシー:

HKEY_LOCAL_MACHINE\Software\Policies\Citrix\MultimediaPolicies

ユーザーポリシー:

HKEY_LOCAL_MACHINE\Software\Policies\Citrix{ユーザーセッションID}\User\MultimediaPolicies

現在のユーザーセッションIDを見つけるには、Windowsコマンドラインで**qwinsta**コマンドを発行します。

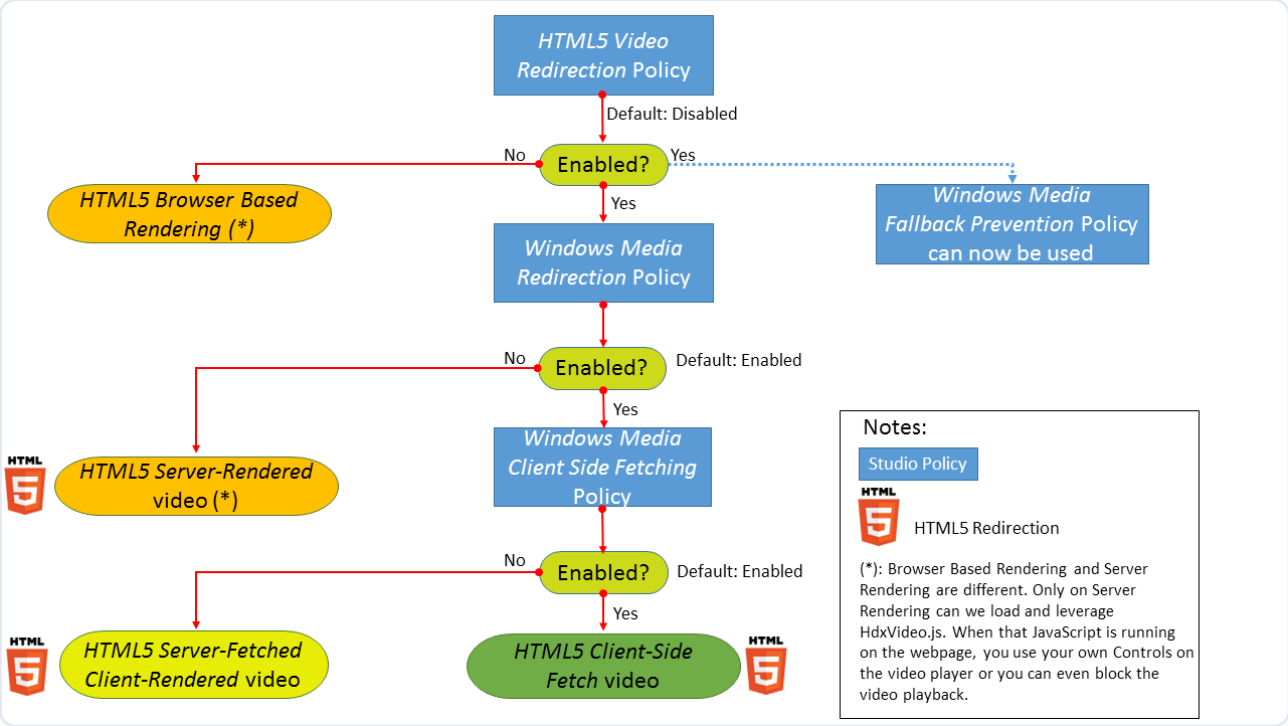
HTML5ビデオリダイレクト

Citrix Virtual Apps and Desktops™サーバーがHTML5マルチメディアWebコンテンツをユーザーに配信する方法を制御し、最適化します。

デフォルトでは、この設定は無効になっています。

HTML5リダイレクト画像(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/redirection2.png)

HTML5リダイレクトのグラフィックイメージ



このリリースでは、この機能は制御されたWebページでのみ利用可能です。HTML5マルチメディアコンテンツが利用可能なWebページ（例: 社内トレーニングサイトのビデオ）にJavaScriptを追加する必要があります。

HTML5ビデオリダイレクトを構成するには:

1. VDAインストール時の%Program Files%/Citrix/ICA Service/HTML5 Video Redirectionから、ファイル**HdxVideo.js**を社内Webページの場所にコピーします。
2. この行をWebページに挿入します（Webページに他のスクリプトがある場合は、それらのスクリプトの前に**HdxVideo.js**を含めます）。 `<script src="HdxVideo.js" type="text/javascript"\></script>`

注: HdxVideo.js がWebページと同じ場所にない場合は、**src** 属性を使用してその完全なパスを指定します。

JavaScriptが管理対象のWebページに追加されておらず、ユーザーがHTML5ビデオを再生する場合を想定します。この場合、Citrix Virtual Apps and Desktopsはデフォルトでサーバー側レンダリングになります。

HTML5ビデオのリダイレクトを機能させるには、***Windows Media Redirection***を許可します。このポリシーは、Server Fetch Client Renderには必須であり、Client Side Fetchingには必要です。Client Side Fetchingは、*Windows Media client-side content fetching*も許可されている必要があります。

Microsoft Edgeはこの機能をサポートしていません。

HdxVideo.jsは、ブラウザのHTML5プレーヤーコントロールを独自のコントロールに置き換えます。特定のWebサイトでHTML5ビデオリダイレクトポリシーが有効になっていることを確認するには、プレーヤーコントロールを、**HTML5ビデオリダイレクト**ポリシーが禁止されているシナリオと比較します。

（ポリシーが許可されている場合のCitrixカスタムコントロール）



（ポリシーが禁止されているか、構成されていない場合のネイティブWebページコントロール）



以下のビデオコントロールがサポートされています。

- 再生
- 一時停止
- シーク
- 繰り返し
- オーディオ
- 全画面表示

HTML5ビデオリダイレクトテストページを表示できます。

TLS、HTML5ビデオリダイレクト、およびブラウザーコンテンツリダイレクト

HTML5ビデオリダイレクトは、次の目的で使用できます。

- HTTPS Webサイトからのビデオのリダイレクト
- または
- Webサイト全体をリダイレクトするためのブラウザーコンテンツリダイレクト

これらのWebサイトに挿入されたJavaScriptは、VDAで実行されているCitrix HDX HTML5 Video Redirection Service (WebSocketService.exe) へのTLS接続を確立する必要があります。VDAの証明書ストアにあるCitrix HDX HTML5 Video Redirection Serviceは、次の目的で2つのカスタム証明書を生成します。

- ビデオのリダイレクトを実現する
- WebページのTLS整合性を維持する

HdxVideo.jsは、Secure WebSocketsを使用して、VDAで実行されているWebSocketService.exeと通信します。このプロセスはローカルシステムアカウントとして実行され、SSL終端とユーザーセッションマッピングを行います。

WebSocketService.exeは、127.0.0.1ポート9001でリッスンしています。

ビデオ品質の制限

この設定は、Windows Mediaにのみ適用され、HTML5には適用されません。**WAN経由のWindows Mediaマルチメディアリダイレクトの最適化**を有効にする必要があります。

この設定は、HDX™接続で許可される最大ビデオ品質レベルを指定します。設定すると、最大ビデオ品質は指定された値に制限され、環境内でマルチメディアのサービス品質 (QoS) が維持されます。

デフォルトでは、この設定は構成されていません。

許可される最大ビデオ品質レベルを制限するには、次のいずれかのオプションを選択します。

- 1080p/8.5Mbps
- 720p/4.0Mbps
- 480p/720Kbps
- 380p/400Kbps
- 240p/200Kbps

同じサーバーで複数のビデオを同時に再生すると、大量のリソースが消費され、サーバーのスケーラビリティに影響を与える可能性があります。

Microsoft Teamsのリダイレクト

この設定は、HDXテクノロジーに基づいてMicrosoft Teamsの最適化を有効にします。

Microsoft Teamsの最適化ポリシー(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/teams-policy.png)

このポリシーが有効で、サポートされているバージョンのCitrix Workspace™アプリを使用している場合、このレジストリキーはVDAで**1**に設定されます。Microsoft Teamsアプリケーションは、VDIモードでロードするためにこのキーを読み取ります。 レジストリキーを手動で設定する必要はありません。

HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream

名前: MSTeamsRedirSupport

値: DWORD (1 - オン, 0 - オフ)

> **注：**
>
> Studioでポリシーが利用できない古いバージョンのControllerで、バージョン1906.2以降のVDAを使用している場合を想定します。Controllerの古いバージョンの例としては、バージョン7.15があります。この場合、HDX最適化はVDAでデフォルトで有効になっています。Workspaceアプリのバージョンが1907以降の場合、Microsoft Teamsは最適化モードで起動します。7.15 LTSR ControllerとCR VDAを混在させる場合の注意点については、Knowledge Centerの記事CTX205549を参照してください。

この場合、特定のユーザーに対して機能を無効にするには、レジストリ設定を上書きできます。ユーザーの組織単位にログオンスクリプトを適用するグループポリシーを使用して、レジストリ設定を上書きします。

デフォルトでは、Microsoft Teamsリダイレクトは有効になっています。

マルチメディア会議

この設定により、ビデオ会議アプリケーションによる最適化されたWebカメラリダイレクトテクノロジーの使用を許可または禁止します。

デフォルトでは、ビデオ会議のサポートは許可されています。

この設定をポリシーに追加する際は、**Windows Mediaリダイレクト**設定が存在し、許可（デフォルト）に設定されていることを確認してください。

マルチメディア会議を使用する場合は、次の条件が満たされていることを確認してください。

- マルチメディア会議に使用するWebカメラのメーカー提供ドライバーがクライアントにインストールされていること。
- ビデオ会議セッションを開始する前に、Webカメラをユーザーデバイスに接続します。サーバーは、一度に1つのインストールされたWebカメラのみを使用します。複数のWebカメラがユーザーデバイスにインストールされている場合、サーバーは各Webカメラを順番に試行します。この試行は、ビデオ会議セッションが正常に作成されるまで続行されます。

汎用USBリダイレクトを使用してWebカメラをリダイレクトする場合、このポリシーは必要ありません。その場合は、WebカメラドライバーをVDAにインストールしてください。

WAN経由のWindows Mediaマルチメディアリダイレクトの最適化

この設定はWindows Mediaにのみ適用され、HTML5には適用されません。この設定により、以下が可能になります。

- リアルタイムマルチメディアトランスコーディング
- 劣化したネットワーク経由でのモバイルデバイスへのオーディオおよびビデオメディアストリーミングを許可
- WAN経由でWindows Mediaコンテンツが配信される方法を改善することで、ユーザーエクスペリエンスを向上させます。

デフォルトでは、WAN経由でのWindows Mediaコンテンツの配信は最適化されています。

この設定をポリシーに追加する際は、**Windows Media Redirection**設定が存在し、**Allowed**に設定されていることを確認してください。

この設定が有効になっている場合、メディアストリーミングを可能にするために、必要に応じてリアルタイムのマルチメディアトランスコーディングが自動的に展開されます。また、極端なネットワーク条件下でもシームレスなユーザーエクスペリエンスを提供します。

WAN経由でのWindows Mediaマルチメディアリダイレクトの最適化にGPUを使用する

この設定はWindows Mediaにのみ適用され、リアルタイムのマルチメディアトランスコーディングをVirtual Delivery Agent (VDA) のグラフィックス処理ユニット (GPU) で実行できるようにします。これにより、サーバーのスケーラビリティが向上します。GPUトランスコーディングは、VDAがハードウェアアクセラレーションをサポートするGPUを搭載している場合にのみ利用可能です。そうでない場合、トランスコーディングはCPUにフォールバックします。

注: GPUトランスコーディングはNVIDIA GPUでのみサポートされています。

デフォルトでは、WAN経由でのWindows Mediaコンテンツの配信を最適化するためにVDA上のGPUを使用することは禁止されています。

この設定をポリシーに追加する際は、以下の設定が存在し、Allowedに設定されていることを確認してください。

- **Windows Mediaリダイレクト**
- **WAN経由でのWindows Mediaマルチメディアリダイレクト設定の最適化**

Windows Mediaフォールバック防止

この設定は、ブラウザコンテンツリダイレクト、HTML5、およびWindows Mediaに適用されます。HTML5をサポートするには、**HTML5 video redirection**ポリシーを**Allowed**に設定します。

管理者は、**Windows Media fallback prevention**ポリシー設定を使用して、ストリーミングコンテンツをユーザーに配信するために試行される方法を指定できます。

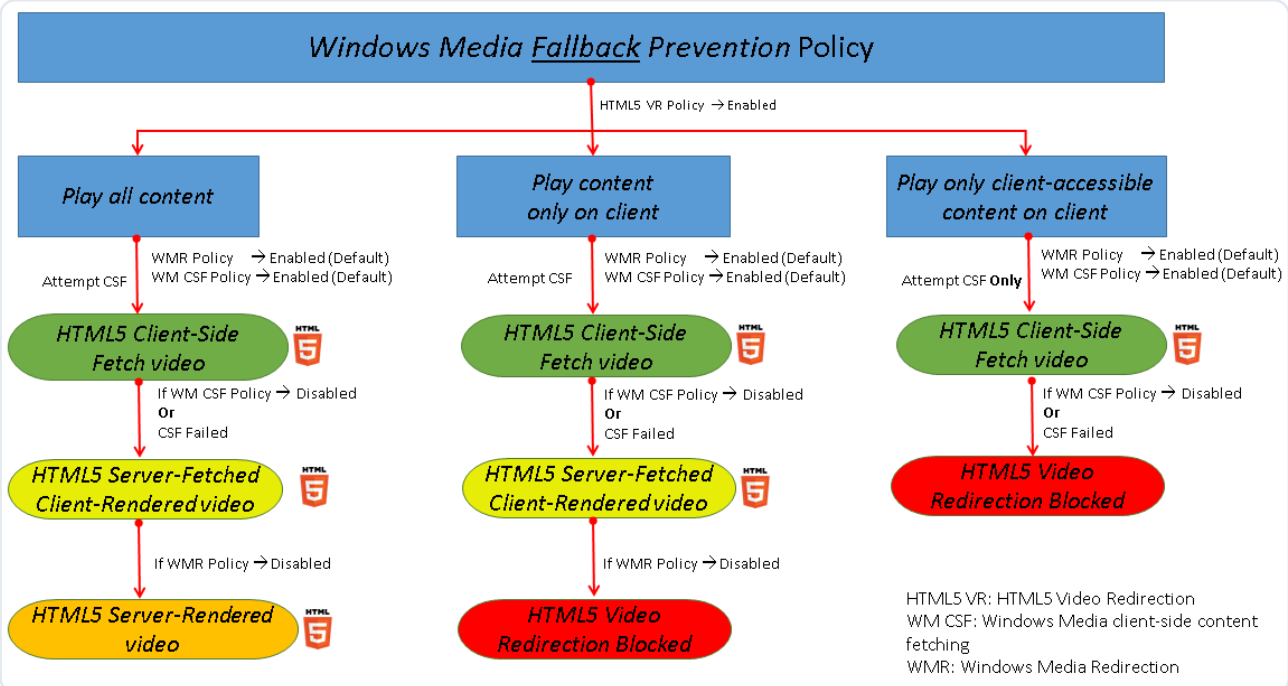
デフォルトでは、この設定は構成されていません。設定が「構成されていません」に設定されている場合、動作は**すべてのコンテンツを再生**と同じになります。

この設定を構成するには、次のいずれかのオプションを選択します。

- **すべてのコンテンツを再生する**。クライアント側でのコンテンツ取得を試行し、次にWindows Mediaリダイレクトを試行します。失敗した場合は、サーバーでコンテンツを再生します。
- **すべてのコンテンツをクライアントでのみ再生する**。クライアント側での取得を試行し、次にWindows Mediaリダイレクトを試行します。失敗した場合、コンテンツは再生されません。
- **クライアントでクライアントがアクセス可能なコンテンツのみを再生する**。クライアント側での取得のみを試行します。失敗した場合、コンテンツは再生されません。

コンテンツが再生されない場合、プレーヤーウィンドウに次のエラーメッセージが表示されます（デフォルトの表示時間は5秒）。

```
"Company has blocked video because of lack of resources"
```



このエラーメッセージの表示時間は、VDA上の次のレジストリキーでカスタマイズできます。レジストリエントリが存在しない場合、表示時間はデフォルトで5秒になります。

レジストリパスは、VDAのアーキテクチャによって異なります。

\HKLM\SOFTWARE\Wow6432Node\Citrix\HdxMediastream

または

\HKLM\SOFTWARE\Citrix\HdxMediastream

レジストリキー：

名前: VideoLoadManagementErrDuration

種類: DWORD

範囲: 1 - DWORD制限まで（デフォルト = 5）

単位: 秒

Windows Mediaクライアント側コンテンツ取得

この設定はHTML5とWindows Mediaの両方に適用されます。この設定により、ユーザーデバイスは、XenAppまたはXenDesktop®ホストサーバーを介さずに、インターネットまたはイントラネット上のソースプロバイダーからマルチメディアファイルを直接ストリーミングできるようになります。

デフォルトでは、この設定は**許可**されています。この設定を許可すると、ネットワーク使用率とサーバーのスケーラビリティが向上します。この改善は、メディアに関するあらゆる処理をホストサーバーからユーザーデバイスに移動することで実現されます。また、Microsoft DirectShowやMedia Foundationなどの高度なマルチメディアフレームワークをユーザーデバイスにインストールする必要がなくなります。ユーザーデバイスには、URLからファイルを再生する機能のみが必要です。

この設定をポリシーに追加するときは、**Windows Mediaリダイレクト**設定が存在し、**許可**に設定されていることを確認してください。**Windows Mediaリダイレクト**が無効になっている場合、ソースプロバイダーからユーザーデバイスへのマルチメディアファイルの直接ストリーミングも無効になります。

Windows Mediaリダイレクト

この設定はHTML5とWindows Mediaの両方に適用され、サーバーがストリーミングオーディオとビデオをユーザーに配信する方法を制御および最適化します。

デフォルトでは、この設定は**許可**されています。HTML5の場合、ポリシー**HTML5ビデオのリダイレクト**が**禁止**されている場合、この設定は有効になりません。

この設定が有効になっている場合、サーバーからレンダリングされるオーディオとビデオの品質は、ユーザーデバイスでローカルに再生されるオーディオとビデオに匹敵するレベルに向上しま

す。サーバーはマルチメディアを元の圧縮形式でクライアントにストリーミングし、ユーザーデバイスがメディアを解凍してレンダリングできるようにします。

Windows Mediaリダイレクトは、Microsoft DirectShow、DirectX Media Objects (DMO)、およびMedia Foundationの標準に準拠するコーデックでエンコードされたマルチメディアファイルを最適化します。特定のマルチメディアファイルを再生するには、そのマルチメディアファイルのエンコード形式と互換性のあるコーデックがユーザーデバイスに存在する必要があります。

デフォルトでは、Citrix Workspaceアプリでオーディオは無効になっています。ユーザーがICA®セッションでマルチメディアアプリケーションを実行できるようにするには、オーディオをオンにするか、Citrix Workspaceアプリインターフェイスでオーディオをオンにする権限をユーザーに付与します。

Windows Mediaリダイレクトを使用してメディアを再生したときの品質が、基本的なICA圧縮と通常のオーディオを使用してレンダリングした場合よりも悪い場合にのみ、**禁止**を選択してください。このような状況はまれですが、たとえばキーフレームの頻度が低いメディアの場合など、低帯域幅の条件下で発生する可能性があります。

Windows Mediaリダイレクトのバッファサイズ

この設定はレガシーであり、HTML5には適用されません。

この設定は、マルチメディアアクセラレーションのバッファサイズを1～10秒で指定します。

デフォルトでは、バッファサイズは5秒です。

Windows Mediaリダイレクトのバッファサイズの使用

この設定はレガシーであり、HTML5には適用されません。

この設定は、**Windows Media Redirection buffer size** 設定で指定されたバッファサイズの使用を有効または無効にします。

デフォルトでは、指定されたバッファサイズは使用されません。

この設定が無効になっている場合、または**Windows Media Redirection buffer size** 設定が構成されていない場合、サーバーはデフォルトのバッファサイズ値（5秒）を使用します。

マルチストリーム接続ポリシー設定

「**マルチストリーム接続**」セクションには、セッション内の複数のICA®接続のサービス品質の優先順位付けを管理するためのポリシー設定が含まれています。

> **注：**

> マルチストリーム接続ポリシーが有効になっている場合、MTU検出はサポートされません。

UDP経由のオーディオ

この設定は、サーバー上でのUDP経由のオーディオを許可または禁止します。

デフォルトでは、サーバー上でのUDP経由のオーディオは許可されています。

有効にすると、この設定はサーバー上でUDPポートを開き、UDP経由のオーディオリアルタイムトランスポートを使用するように構成されたすべての接続をサポートします。

オーディオUDPポート範囲

この設定は、Virtual Delivery Agent (VDA) によって使用されるポート番号の範囲（最小ポート番号、最大ポート番号）を指定します。この指定は、ユーザーデバイスとの間でオーディオパケットデータを交換するのに役立ちます。VDAは、ユーザーデバイスとデータを交換するために各UDPポートペアを使用しようとします。最小値から開始し、その後の試行ごとに2ずつ増やします。各ポートは、インバウンドトラフィックとアウトバウンドトラフィックの両方を処理します。

デフォルトでは、この範囲は16500,16509に設定されています。

マルチポートポリシー

この設定は、ICAトラフィックに使用するTCPポートを指定し、各ポートのネットワーク優先順位を確立します。

デフォルトでは、プライマリポート (2598) は高優先度です。

ポートを構成するとき、次の優先順位を割り当てることができます。

- **非常に高い:** ウェブカメラ会議などのリアルタイムアクティビティ用
- **高:** 画面、キーボード、マウスなどの対話型要素用
- **中:** クライアントドライブマッピングなどのバルク処理用
- **低:** 印刷などのバックグラウンドアクティビティ用

各ポートには一意の優先順位が必要です。たとえば、CGPポート1とCGPポート3の両方に「非常に高」の優先順位を割り当てることはできません。

ポートを優先順位付けから削除するには、ポート番号を0に設定します。プライマリポートを削除したり、その優先順位レベルを変更したりすることはできません。

この設定を構成するときは、サーバーを再起動してください。この設定は、**Multi-Stream computer**設定ポリシー設定が有効になっている場合にのみ有効になります。

マルチストリーム コンピューター設定

この設定は、サーバー上でMulti-Streamを有効または無効にします。

デフォルトでは、Multi-Streamは無効になっています。Citrix SD-WAN™またはサードパーティ製ルーターを使用して目的のQuality of Serviceを実現する場合は、Multi-Stream computerポリシー設定を構成してください。

Multi-Streamが有効になっている場合、Adaptive Transportの機能であるMTU Discoveryはサポートされません。

この設定を構成するときは、変更が有効になるようにサーバーを再起動してください。

> **重要:**
>
> このポリシー設定を、セッション全体の帯域幅制限などの帯域幅制限ポリシー設定と組み合わせて使用すると、予期しない結果が生じる可能性があります。この設定をポリシーに含める場合は、帯域幅制限設定が含まれていないことを確認してください。

マルチストリーム ユーザー設定

この設定は、ユーザーデバイス上でMulti-Streamを有効または無効にします。

デフォルトでは、Multi-Streamはすべてのユーザーに対して無効になっています。Citrix SD-WANまたはサードパーティ製ルーターを使用して目的のQuality of Serviceを実現する場合は、Multi-Stream user設定を構成してください。

この設定は、**マルチストリームコンピューター**設定ポリシー設定が有効になっているホストでのみ有効になります。

> **重要:**
>
> このポリシー設定を、全体的なセッション帯域幅制限などの帯域幅制限ポリシー設定と併用すると、予期しない結果が生じる可能性があります。この設定をポリシーに含める場合は、帯域幅制限設定を含めないようにしてください。

マルチストリーム仮想チャネル割り当て設定

この設定は、マルチストリームが使用されている場合に仮想チャネルが割り当てられるICAストリームを指定します。

これらの設定を構成しない場合、仮想チャネルはデフォルトのストリームに保持されます。仮想チャネルをICAストリームに割り当てるには、仮想チャネル名の横にある**ストリーム番号**リストから目的のストリーム番号（0、1、2、3）を選択します。

環境でカスタム仮想チャネルが使用されている場合は、**追加**をクリックし、**仮想チャネル**の下のテキストボックスに仮想チャネル名を指定し、その横にある**ストリーム番号**リストから目的のストリーム番号を選択します。指定する名前は、フレンドリ名ではなく、実際の仮想チャネル名である必要があります。たとえば、Citrix Browser AccelerationではなくCTXSBRです。

これらの設定は、マルチストリームコンピューター設定を有効にした場合にのみ有効になります。

デフォルトでは、仮想チャネルとそのストリーム割り当ては次のとおりです。

- AppFlow®: 2
- オーディオ: 0
- ブラウザコンテンツリダイレクト: 2
- クライアントCOMポートマッピング: 3
- クライアントドライブマッピング: 2
- クライアントプリンターマッピング: 3
- クリップボード: 2
- CTXDND: 1 (**注:** これは、Citrixセッションとローカルエンドポイント間でファイルをドラッグアンドドロップする機能をサポートします。)
- DVCプラグイン (DVCプラグインのフレンドリ名から自動生成された静的VC名、または管理者によって割り当てられたもの): 2
- エンドユーザーエクスペリエンス監視: 1
- ファイル転送 (HTML5 Receiver): 2
- 汎用データ転送: 2
- ICA制御: 1
- 入力メソッドエディター: 1
- レガシー クライアント プリンター マッピング (COM1): 1, 3

- レガシー クライアント プリンター マッピング (COM2): 2, 3
- レガシー クライアント プリンター マッピング (LPT1): 1, 3
- レガシー クライアント プリンター マッピング (LPT2): 2, 3
- ライセンス管理: 1
- Microsoft Teams/WebRTC リダイレクト: 1
- モバイルレシーバー: 1
- マルチタッチ: 1
- ポートフォワーディング: 2
- リモートオーディオおよびビデオ拡張機能 (RAVE): 2
- シームレス (透過ウィンドウ統合): 1
- センサーと位置情報: 1
- スマートカード: 1
- Thinwire グラフィック: 1
- 透過UI統合/ログオンステータス: 2
- TWAIN リダイレクト: 2
- USB: 2
- ゼロ遅延フォントおよびキーボード: 2
- ゼロ遅延データチャネル: 2

仮想チャネルの割り当てと優先度について詳しくは、Knowledge Center の記事 CTX131001 を参照してください。

ポートリダイレクトポリシー設定

ポートリダイレクトセクションには、クライアントLPTおよびCOMポートマッピングのポリシー設定が含まれています。

Virtual Delivery Agentのバージョンが**7.0より前**の場合、ポートリダイレクトを構成するには以下のポリシー設定を使用します。VDAバージョン**7.0から7.8**の場合、これらの設定はレジストリを使用して構成します。詳細については、「レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。VDAバージョン**7.9**の場合、以下のポリシー設定を使用します。

クライアントCOMポートの自動接続

この設定は、ユーザーがサイトにログオンしたときに、ユーザーデバイス上のCOMポートの自動接続を有効または無効にします。

デフォルトでは、クライアントCOMポートは自動的に接続されません。

クライアントLPTポートの自動接続

この設定は、ユーザーがサイトにログオンしたときに、ユーザーデバイス上のLPTポートの自動接続を有効または無効にします。

デフォルトでは、クライアントLPTポートは自動的に接続されません。

クライアントCOMポートリダイレクト

この設定は、ユーザーデバイス上のCOMポートへのアクセスを許可または禁止します。

デフォルトでは、COMポートリダイレクトは禁止されています。

関連するポリシー設定は次のとおりです。

- COMポートリダイレクトの帯域幅制限
- COMポートリダイレクトの帯域幅制限（パーセント）

クライアントLPTポートリダイレクト

この設定は、ユーザーデバイス上のLPTポートへのアクセスを許可または禁止します。

デフォルトでは、LPTポートリダイレクトは禁止されています。

LPTポートは、LPTポートに印刷ジョブを送信するレガシーアプリケーションでのみ使用されます。これらのポートは、ユーザーデバイス上の印刷オブジェクトに印刷ジョブを送信するレガシーアプリケーションでは使用されません。現在のほとんどのアプリケーションは、印刷ジョブをプリンターオブジェクトに送信できます。このポリシー設定は、LPTポートに印刷するレガシーアプリケーションをホストするサーバーにのみ必要です。

クライアントCOMポートリダイレクトは双方向ですが、LPTポートリダイレクトは出力のみであり、ICAセッション内では`\\client\LPT1`および`\\client\LPT2`に制限されます。

以下のポリシー設定は関連しています。

- LPTポートリダイレクト帯域幅制限
- LPTポートリダイレクトの帯域幅制限（パーセント）

印刷ポリシー設定

印刷セクションには、クライアント印刷を管理するためのポリシー設定が含まれています。

クライアントプリンターリダイレクト

この設定は、ユーザーがセッションにログオンしたときに、クライアントプリンターがサーバーにマップされるかどうかを制御します。

デフォルトでは、クライアントプリンターのマッピングは許可されています。この設定が無効になっている場合、セッション用のPDFプリンターは自動作成されません。

関連するポリシー設定: クライアントプリンターの自動作成

デフォルトプリンター

この設定は、ユーザーデバイス上のデフォルトプリンターがセッションでどのように確立されるかを指定します。

デフォルトでは、ユーザーの現在のプリンターがセッションのデフォルトプリンターとして使用されます。

デフォルトプリンターに現在のRemote Desktop ServicesまたはWindowsユーザープロファイル設定を使用するには、「ユーザーのデフォルトプリンターを調整しない」を選択します。このオプションを選択した場合、デフォルトプリンターはプロファイルに保存されず、他のセッションまたはクライアントプロパティに従って変更されることもありません。セッション内のデフォルトプリンターは、セッションで最初に自動作成されたプリンターであり、次のいずれかです。

- **コントロールパネル > デバイス**と**プリンター**でWindowsサーバーにローカルに追加された最初のプリンター。
- サーバーにローカルに追加されたプリンターがない場合、最初に自動作成されたプリンター。

このオプションを使用すると、プロファイル設定を通じてユーザーに最も近いプリンターを提示できます（近接印刷として知られています）。

プリンターの割り当て

この設定は、デフォルトプリンターとセッションプリンターの設定の代替手段を提供します。個別のデフォルトプリンターとセッションプリンターの設定を使用して、サイト、大規模グループ、または組織単位の動作を構成します。**プリンター割り当て**設定を使用して、多数のプリンターを複数のユーザーに割り当てます。

この設定は、リストされたユーザーデバイス上のデフォルトプリンターがセッションでどのように確立されるかを指定します。

デフォルトでは、ユーザーの現在のプリンターがセッションのデフォルトプリンターとして使用されます。

各ユーザーデバイスのセッションで自動作成されるネットワークプリンターも指定します。デフォルトでは、プリンターは指定されていません。

- デフォルトプリンターの値を設定する場合：

  ユーザーデバイスの現在のデフォルトプリンターを使用するには、「Do not adjust」を選択します。

  デフォルトプリンターに現在のRemote Desktop ServicesまたはWindowsユーザープロファイル設定を使用するには、「Do no adjust」を選択します。このオプションを選択すると、デフォルトプリンターはプロファイルに保存されず、他のセッションまたはクライアントのプロパティに応じて変更されません。セッション内のデフォルトプリンターは、セッションで最初に自動作成されたプリンターであり、次のいずれかです。

  - Windowsサーバーにローカルで追加された最初のプリンター（**コントロールパネル > デバイス**とプリンター）。
  - サーバーにローカルで追加されたプリンターがない場合、最初に自動作成されたプリンター。

- 「セッションプリンター」の値を設定する場合：プリンターを追加するには、自動作成するプリンターのUNCパスを入力します。プリンターを追加した後、ログオンするたびに現在のセッションにカスタマイズされた設定を適用できます。

プリンターの自動作成イベントログ設定

この設定は、プリンターの自動作成プロセス中にログに記録されるイベントを指定します。エラーや警告をログに記録しない、エラーのみをログに記録する、またはエラーと警告をログに記録する、のいずれかを選択できます。

デフォルトでは、エラーと警告がログに記録されます。

警告の例としては、プリンターのネイティブドライバーをインストールできず、代わりにユニバーサルプリントドライバーがインストールされるイベントが挙げられます。このシナリオでユニバーサルプリントドライバーを使用するには、「ユニバーサルプリントドライバーの使用」設定を「ユニバーサル印刷のみを使用」または「要求されたドライバーが利用できない場合にのみユニバーサル印刷を使用」に構成します。

セッションプリンター

この設定は、セッションで自動作成されるネットワークプリンターを指定します。ICA/HDXセッション内では、Citrix Print Managerサービス（CpSvc.exe）が、**セッションプリンター**ポリシー設定で指定された各ネットワークプリンターに対して、セッションログオン中にネットワークプリンター接続を作成します。セッションログオフ中にプリンターを削除します。デフォルトでは、プリンターは指定されていません。

セッションプリンターポリシー設定では、ネットワークプリンターはWindows Print ServerまたはCitrix Universal™ Print Server上に存在できます。

- **Windows Print Server:** 1つ以上のネットワークプリンターを共有します。また、ネットワークプリンターを使用するために必要なネイティブプリンタードライバーも備えています。
- **Universal Print Server:** Citrix Universal Print Serverソフトウェアがインストールされている Windows Print Server。

Windows Print Server を使用する場合、Citrix Print Manager サービスはネイティブプリンタードライバーを使用してネットワークプリンター接続を作成します。Citrix Virtual Apps™ サーバーには、ネイティブプリンタードライバーがインストールされている必要があります。

Citrix Universal Print Server を使用する場合、Citrix Print Manager サービスは、ネイティブプリンタードライバー、Citrix Universal Printer Driver、または Citrix Universal XPS Printer Driver のいずれかを使用してネットワークプリンター接続を作成します。使用するドライバーは、Universal Print Driver の使用ポリシー設定によって制御されます。

すべての Windows プリンタードライバーは現在、v3 または v4 ドライバーバージョンのいずれかに分類されます。詳細については、「Support for the Microsoft V3 and V4 Printer Driver Architectures」を参照してください。

セッションプリンターを追加し、それらがセッションに表示されることを確認するには、次の手順を実行します。

1. Citrix Studioで、**［ポリシー］**タブに移動します。
2. **［ポリシーの編集］**ダイアログボックスで、セッション印刷ポリシーを有効にします。
3. ポリシーで、セッションプリンターを追加します。プリンターを追加するには、自動作成するプリンターのUNCパスを入力します。プリンターを追加した後、ログオンするたびに現在のセッションにカスタマイズされた設定を適用できます。セッションプリンターがリストに表示されている必要があります。

4. ポリシーが設定された後、公開されたアプリケーションにセッションプリンターが表示されない場合があります。この問題は、Citrix Virtual Apps サーバーにプリンタードライバーがないか、ポリシーが作成されたものの有効になっていないために発生する可能性があります。

> **注：**
>
> プリンタードライバーがCitrix Virtual Appsサーバーにインストールされていない場合、管理者がCitrix Virtual Appsサーバーにプリンタードライバーをインストールし忘れるという、セッションプリンターで最もよくある間違いが発生する可能性があります。

5. 公開されたデスクトップを起動し、 **>** でセッションプリンターを手動で追加します。
6. これが失敗した場合は、Citrix Virtual Apps サーバーとプリントサーバー間の通信を調査します。RDP を使用してテストを実行することを検討してください。

プリンターが作成されるのを待つ

この機能は、Citrix Virtual Desktops™用かCitrix Virtual Apps用かによって有効化方法が異なります。Citrix Virtual Desktopsでこの機能を有効にするには、Delivery Controllerのポリシーを使用します。Citrix Virtual Appsでこの機能を有効にするには、Delivery ControllerのPowerShellコマンドレットを使用します。

プリンターの作成を待機する (サーバーデスクトップ):

この設定により、セッションへの接続を遅延させ、クライアントリダイレクトされたプリンターを自動作成できます。

デフォルトでは、接続遅延は発生しません。

プリンターの作成を待機する (Citrix Virtual Apps):

次のPowerShellコマンドレットを設定すると、サーバーデスクトップで作成された仮想アプリへの接続を遅延させ、クライアントリダイレクトされたプリンターを自動作成できるようになります。

```
Set-BrokerApplication -Name <VirualAppName> -WaitForPrinterCreation $true
```

デフォルトでは、接続遅延は発生しません。

クライアントプリンターポリシー設定

クライアントプリンターセクションには、クライアントプリンターのポリシー設定が含まれています。これには、クライアントプリンターの自動作成、プリンタープロパティの保持、プリントサーバーへの接続に関する設定が含まれます。

クライアントプリンターの自動作成

この設定は、自動作成されるクライアントプリンターを指定します。この設定は、デフォルトのクライアントプリンター自動作成設定を上書きします。

デフォルトでは、すべてのクライアントプリンターが自動作成されます。

この設定は、Client printer redirection 設定が存在し、**Allowed** に設定されている場合にのみ有効になります。

この設定をポリシーに追加する際は、オプションを選択してください。

- **すべてのクライアントプリンターを自動作成**すると、ユーザーデバイス上のすべてのプリンターが自動的に作成されます。
- **クライアントのデフォルトプリンターのみを自動作成**すると、ユーザーデバイスでデフォルトプリンターとして選択されているプリンターのみが自動的に作成されます。
- **ローカル（非ネットワーク）クライアントプリンターのみを自動作成**すると、LPT、COM、USB、TCP/IP、またはその他のローカルポートを介してユーザーデバイスに直接接続されているプリンターのみが自動的に作成されます。
- **クライアントプリンターを自動作成しない**を選択すると、ユーザーがログオンしたときにすべてのクライアントプリンターの自動作成が無効になります。このオプションを選択すると、クライアントプリンターの自動作成に関するRemote Desktop Services (RDS) の設定が、優先度の低いポリシーのこの設定を上書きします。

汎用ユニバーサルプリンターの自動作成

この設定は、ユニバーサル印刷と互換性のあるユーザーデバイスが使用されているセッションにおいて、汎用 Citrix Universal™ Printer オブジェクトの自動作成を有効または無効にします。

デフォルトでは、汎用ユニバーサルプリンターオブジェクトは自動作成されません。

関連するポリシー設定は次のとおりです。

- ユニバーサルプリントドライバーの使用状況
- ユニバーサルドライバーの優先順位

PDFユニバーサルプリンターの自動作成

この設定は、Windows 用 Citrix Workspace アプリ (VDA 7.19 以降)、HTML5 用 Citrix Workspace アプリ、または Chrome 用 Citrix Workspace アプリを使用するセッションにおいて、Citrix PDF プリンターの自動作成を有効または無効にします。

デフォルトでは、Citrix PDFプリンターは自動作成されません。

クライアントプリンター名

この設定は、自動作成されたクライアントプリンターの命名規則を選択します。

デフォルトでは、標準のプリンター名が使用されます。

「**標準プリンター名**」を選択すると、「HPLaserJet 4 from client name in session 3」のようなプリンター名が使用されます。

従来のクライアントプリンター名を使用し、製品の XenApp および XenDesktop バージョンに存在するレガシープリンター名との下位互換性を維持するには、**Legacy printer names** を選択します。このオプションは、製品の現在の Citrix Virtual Apps and Desktops バージョンで使用できます。レガシープリンター名の例は、「Client/clientname#/HPLaserJet 4」です。このオプションはセキュリティが低くなります。

Citrix Workspace™ app for HTML5 から起動されたセッションで Citrix PDF プリンターを使用する場合は、**Client printer names** 設定をデフォルトにするか、**Standard printer names** を選択してください。**Legacy printer names** を選択した場合、Citrix Workspace app for HTML5 は Citrix PDF Printer オプションをサポートしません。

印刷サーバーへの直接接続

この設定は、仮想デスクトップまたはアプリケーションをホストするサーバーから、アクセス可能なネットワーク共有でホストされているクライアントプリンターの印刷サーバーへの直接接続を有効または無効にします。

デフォルトでは、直接接続が有効になっています。

ネットワーク印刷サーバーが仮想デスクトップまたはアプリケーションをホストするサーバーからWANを介していない場合は、直接接続を有効にします。ネットワーク印刷サーバーと仮想デスクトップまたはアプリケーションをホストするサーバーが同じLAN上にある場合、直接通信により印刷が高速化されます。

ネットワークがWANを介している場合、または相当な遅延や限られた帯域幅がある場合は、直接接続を無効にします。印刷ジョブはユーザーデバイスを介してルーティングされ、そこでネット

ワーク印刷サーバーにリダイレクトされます。ユーザーデバイスに送信されるデータは圧縮されるため、データがWANを介して転送される際に消費される帯域幅が少なくなります。

2つのネットワークプリンターが同じ名前を持つ場合、ユーザーデバイスと同じネットワーク上のプリンターが使用されます。

プリンタードライバーのマッピングと互換性

この設定は、自動作成されたクライアントプリンターのドライバー置換ルールを指定します。

この設定は、Microsoft OneNoteおよびXPS Document Writerを自動作成されたクライアントプリンターリストから除外するように構成されています。

ドライバー置換ルールを定義すると、指定されたドライバーでプリンターが作成されることを許可または防止できます。また、作成されたプリンターがユニバーサル印刷ドライバーのみを使用することを許可できます。ドライバー置換は、ユーザーデバイスが提供するプリンタードライバー名を上書きまたはマッピングし、サーバー上の同等のドライバーに置き換えます。これにより、サーバーアプリケーションは、サーバーと同じドライバーを持つが、ドライバー名が異なるクライアントプリンターにアクセスできるようになります。

ドライバーマッピングの追加、既存のマッピングの編集、マッピングのカスタム設定の上書き、マッピングの削除、またはリスト内のドライバーエントリの順序変更が可能です。マッピングを追加する際は、クライアントプリンタードライバー名を入力し、置換するサーバードライバーを選択します。

プリンタープロパティの保持

この設定は、プリンターのプロパティを保存するかどうか、およびどこに保存するかを指定します。

デフォルトでは、システムはプリンターのプロパティがユーザーデバイスに保存されるか（利用可能な場合）、またはユーザープロファイルに保存されるかを決定します。

この設定をポリシーに追加するときは、オプションを選択してください。

- クライアントデバイスのみに保存 は、保存されていない必須プロファイルまたは移動プロファイルを持つユーザーデバイス向けです。このオプションは、ファーム内のすべてのサーバーがXenApp 5以降を実行しており、ユーザーがCitrixオンラインプラグインバージョン9〜12.x、またはCitrix Receiver 3.xを使用している場合にのみ選択してください。
- ユーザープロファイルのみに保持 は、帯域幅（このオプションはネットワークトラフィックを削減します）とログオン速度によって制約されるユーザーデバイス、またはレガシープラグインを使用するユーザー向けです。このオプションは、サーバー上のユーザープロファイルにプリンタープロパティを保存し、ユーザーデバイスとのプロパティ交換を防止します。このオプ

ションは、MetaFrame Presentation Server 3.0以前およびMetaFrame Presentation Server Client 8.x以前で使用してください。これは、Remote Desktop Services (RDS) 移動プロファイルが使用されている場合にのみ適用されることに注意してください。

- クライアントに保存されていない場合のみプロファイルに保持 は、システムがプリンタープロパティの保存場所を決定できるようにします。プリンタープロパティは、利用可能な場合はユーザーデバイスに、またはユーザープロファイルに保存されます。このオプションは最も柔軟ですが、ログオン時間を遅くし、システムチェックのために余分な帯域幅を使用する可能性もあります。
- プリンターのプロパティを保持しないは、プリンターのプロパティの保存を防ぎます。

保持および復元されたクライアントプリンター

この設定は、ユーザーデバイス上のプリンターの保持と再作成を有効または無効にします。デフォルトでは、クライアントプリンターは自動的に保持および復元されます。

保持されたプリンターとは、次回のセッション開始時に再度作成される、または記憶されるユーザー作成のプリンターです。Citrix Virtual Apps™ が保持されたプリンターを再作成する場合、**クライアントプリンターの自動作成**設定を除くすべてのポリシー設定が考慮されます。

復元されたプリンターとは、管理者が完全にカスタマイズし、クライアントポートに永続的にアタッチされた保存状態を持つプリンターです。

CITRIX PDFユニバーサルプリンタードライバー

Citrix PDF Universal Printer ドライバーを使用すると、Citrix Virtual Apps and Desktops によって提供されるホスト型アプリケーションまたは仮想デスクトップで実行されているアプリケーションで開かれたドキュメントをユーザーが印刷できます。ユーザーが**Citrix PDF Printer** オプションを選択すると、ドライバーはファイルをPDFに変換し、PDFをローカルデバイスに転送します。その後、PDFはローカルに接続されたプリンターから表示および印刷するために開かれます。PDFは、Citrix Universal Printingでサポートされている形式の1つです（EMFおよびXPSに加えて）。PDFプリンターは、Citrixポリシーを使用して有効化、構成、およびデフォルトとして設定できます。**Citrix PDF Printer** オプションは、Windows、Chrome、およびHTML5用のCitrix Workspaceアプリのユーザーが利用できます。

> **注：**
>
> WindowsエンドポイントにはPDFビューアーが必要です。クライアントには、PDFファイルを開くためにWindowsにファイルタイプ関連付けが登録されているアプリケーションが必要です。

ドライバーポリシー設定

「**ドライバー**」セクションには、プリンタードライバーに関連するポリシー設定が含まれています。

インボックスプリンタードライバーの自動インストール

> **注**
>
> このリリースでは、このポリシーはVDAをサポートしていません。

この設定は、Windowsのインボックスドライバーセット、またはpnputil.exe /aを使用してホストにステージングされたドライバーパッケージからのプリンタードライバーの自動インストールを有効または無効にします。

デフォルトでは、これらのドライバーは必要に応じてインストールされます。

ユニバーサルドライバーの優先順位

この設定は、リストの最初のエントリから始まる、ユニバーサルプリンタードライバーが使用される順序を指定します。

デフォルトでは、優先順位は次のとおりです。

- EMF
- XPS
- PCL5c (ピーシーエルファイブシー)
- PCL4
- PS

ドライバーの追加、編集、削除、およびリスト内のドライバーの順序変更が可能です。

ユニバーサルプリントドライバーの使用

この設定は、ユニバーサル印刷を使用するタイミングを指定します。

既定では、要求されたドライバーが利用できない場合にのみ、ユニバーサル印刷が使用されます。

ユニバーサル印刷では、標準のモデル固有ドライバーの代わりに汎用プリンタードライバーが使用されるため、ホストコンピューターでのドライバー管理の負担が軽減される可能性があります。ユニバーサル印刷ドライバーの可用性は、ユーザーデバイス、ホスト、および印刷サーバーソ

フトウェアの機能によって異なります。特定の構成では、ユニバーサル印刷が利用できない場合があります。

この設定をポリシーに追加する際は、オプションを選択してください。

- プリンターモデル固有のドライバーのみを使用するは、クライアントプリンターがログオン時に自動作成される標準のモデル固有のドライバーのみを使用することを指定します。要求されたドライバーが利用できない場合、クライアントプリンターは自動作成できません。
- ユニバーサル印刷のみを使用するは、標準のモデル固有のドライバーが使用されないことを指定します。プリンターの作成には、ユニバーサル印刷ドライバーのみが使用されます。
- 要求されたドライバーが利用できない場合にのみユニバーサル印刷を使用するは、利用可能な場合はプリンター作成に標準のモデル固有のドライバーを使用します。ドライバーがサーバーで利用できない場合、クライアントプリンターは適切なユニバーサルドライバーで自動的に作成されます。
- ユニバーサル印刷が利用できない場合にのみプリンターモデル固有のドライバーを使用するは、利用可能な場合はユニバーサル印刷ドライバーを使用します。ドライバーがサーバーで利用できない場合、クライアントプリンターは適切なモデル固有のプリンタードライバーで自動的に作成されます。

ユニバーサルプリントサーバーのポリシー設定

「**Universal Print Server**」セクションには、Universal Print Serverを処理するためのポリシー設定が含まれています。

SSL暗号スイート

この設定は、暗号化された印刷データストリーム（CGP）接続のためにUniversal Print Clientが使用するSSL/TLS暗号スイートのセットを指定します。

暗号化された印刷Webサービス (HTTPS/SOAP) 接続のためにUniversal Print Clientで使用される暗号スイートパッケージを制御するには、を参照してください。

デフォルト値: ALL

この設定には次の値があります: ALL、COM、またはGOV。

各値に対応する暗号スイートを以下に示します。

ALL:

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

TLS_ECDHE_RSA_AES128_CBC_SHA

COM:

TLS_ECDHE_RSA_AES128_CBC_SHA

GOV:

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

SSL準拠モード

この設定は、Universal Print Clientが暗号化された印刷データストリーム (CGP) 接続に使用するNIST Special Publication 800-52への準拠レベルを指定します。

デフォルト値: なし。

この設定には次の値があります:

なし。

暗号化された印刷データストリーム (CGP) 接続は、デフォルトの準拠モードを使用します。

SP800-52。

暗号化された印刷データストリーム (CGP) 接続は、NIST Special Publication 800-52準拠モードを使用します。

SSL有効

この設定は、Universal Print Clientが印刷データストリーム（CGP）接続およびWebサービス（HTTP/SOAP）接続にSSL/TLSを使用するかどうかを指定します。

Universal Print Server enable を **Enabled with fallback to Windows' native remote printing** に設定すると、Microsoft Windows Network Print Providerによってフォールバック接続が行われます。この設定は、これらのフォールバック接続には影響しません。

既定値: 無効

この設定は次の値をとります。

有効。

ユニバーサルプリントクライアントは、Universal Print Serverへの接続にSSL/TLSを使用します。

無効。

ユニバーサルプリントクライアントは、Universal Print Serverへの接続にSSL/TLSを使用します。

SSL FIPSモード

この設定は、印刷データストリーム（CGP）接続のためにUniversal Print Clientが使用するSSL/TLS暗号モジュールがFIPSモードで実行されるかどうかを指定します。

既定値: 無効

この設定は次の値をとります。

有効。

FIPSモードがオンになります。

無効。

FIPSモードがオフになります。

SSLプロトコルバージョン

この設定は、Universal Print Client が使用する SSL/TLS プロトコルバージョンを指定します。

デフォルト値: ALL

この設定には次の値があります。

ALL。

TLS バージョン 1.0、1.1、または 1.2 を使用します。

ティーエルエスv1.

TLS バージョン 1.0 を使用します。

TLSv1.1。

TLS バージョン 1.1 を使用します。

TLSv1.2。

TLS バージョン 1.2 を使用します。

SSL UNIVERSAL PRINT SERVER 暗号化印刷データストリーム (CGP) ポート

この設定は、Universal Print Server 暗号化印刷データストリーム (CGP) ポートの TCP ポート番号を指定します。このポートは、印刷ジョブのデータを受信します。

デフォルト値: 443

SSL UNIVERSAL PRINT SERVER 暗号化 WEB サービス (HTTPS/SOAP) ポート

この設定は、Universal Print Serverの暗号化されたWebサービス（HTTPS/SOAP）ポートのTCPポート番号を指定します。このポートは、印刷コマンドのデータを受信します。

デフォルト値: 8443

UNIVERSAL PRINT SERVERの有効化

この設定は、仮想デスクトップまたはアプリケーションをホストするサーバーでUniversal Print Server機能を有効または無効にします。このポリシー設定は、仮想デスクトップまたはアプリケーションをホストするサーバーを含む組織単位（OU）に適用します。

デフォルトでは、Universal Print Serverは無効になっています。

この設定をポリシーに追加するときは、次のいずれかのオプションを選択します。

- **Windowsネイティブのリモート印刷へのフォールバックを有効にする**。ネットワークプリンター接続は、可能であればUniversal Print Serverによって処理されます。Universal Print Serverが利用できない場合、Windows Print Providerが使用されます。Windows Print Providerは、以前にWindows Print Providerで作成されたすべてのプリンターの処理を継続します。
- **Windowsネイティブのリモート印刷へのフォールバックなしで有効にする**。ネットワークプリンター接続は、Universal Print Serverによってのみ処理されます。Universal Print Serverが利用できない場合、ネットワークプリンター接続は失敗します。この設定は、Windows Print Providerを介したネットワーク印刷を実質的に無効にします。この設定を含むポリシーがアクティブな間は、以前にWindows Print Providerで作成されたプリンターは作成されません。
- **無効**。Universal Print Server機能は無効になります。UNC名を持つネットワークプリンターに接続する際、Universal Print Serverへの接続は試行されません。リモートプリンターへの接続は、引き続きWindowsネイティブのリモート印刷機能を使用します。

UNIVERSAL PRINT SERVER印刷データストリーム (CGP) ポート

この設定は、Universal Print Server印刷データストリームのCommon Gateway Protocol (CGP) リスナーが使用するTCPポート番号を指定します。このポリシー設定は、プリントサーバーを含むOUにのみ適用します。

デフォルトでは、ポート番号は7229に設定されています。

有効なポート番号は1～65535の範囲である必要があります。

UNIVERSAL PRINT SERVERの印刷ストリーム入力帯域幅制限（KBPS）

この設定は、各印刷ジョブからCGPを使用してUniversal Print Serverに配信される印刷データの転送速度の上限（キロビット/秒）を指定します。このポリシー設定は、仮想デスクトップまたはアプリケーションをホストするサーバーを含むOUに適用します。

デフォルトでは、値は0であり、上限がないことを指定します。

ユニバーサルプリントサーバーWEBサービス (HTTP/SOAP) ポート

この設定は、Universal Print ServerのWebサービス（HTTP/SOAP）リスナーが使用するTCPポート番号を指定します。Universal Print Serverは、ネットワーク印刷シナリオでCitrixユニバーサル印刷ドライバーの使用を可能にするオプションコンポーネントです。Universal Print Serverが使用される場合、印刷コマンドはCitrix Virtual Apps and DesktopsホストからHTTP経由のSOAPを介してUniversal Print Serverに送信されます。この設定は、Universal Print Serverが着信HTTP/SOAP要求をリッスンするデフォルトのTCPポートを変更します。

ホストと印刷サーバーのHTTPポートは両方とも同じように構成する必要があります。ポートを同じように構成しない場合、ホストソフトウェアはUniversal Print Serverに接続しません。この設定は、Citrix Virtual Apps and Desktops上のVDAを変更します。さらに、Universal Print Serverのデフォルトポートも変更する必要があります。

デフォルトでは、ポート番号は8080に設定されています。

有効なポート番号は0～65535の範囲である必要があります。

負荷分散用のUNIVERSAL PRINT SERVER

この設定は、他のCitrix®印刷ポリシー設定を評価した後、セッション起動時に確立されたプリンター接続の負荷分散に使用されるUniversal Print Serverを一覧表示します。プリンター作成時間を最適化するために、Citrixはすべての印刷サーバーが同じ共有プリンターのセットを持つことを推奨します。負荷分散のために追加できる印刷サーバーの数に上限はありません。

この設定は、プリントサーバーのフェイルオーバー検出とプリンター接続の回復も実装します。プリントサーバーは定期的に可用性がチェックされます。サーバー障害が検出された場合、そのサーバーは負荷分散スキームから削除され、そのサーバー上のプリンター接続は他の利用可能なプリントサーバーに再分配されます。障害が発生したプリントサーバーが回復すると、負荷分散スキームに戻されます。

Validate Servers をクリックして、各サーバーがプリントサーバーであること、サーバーリストに重複するサーバー名が含まれていないこと、およびすべてのサーバーに同一の共有プリンターセットがインストールされていることを確認します。この操作には時間がかかる場合があります。

UNIVERSAL PRINT SERVERサービス停止しきい値

この設定は、ロードバランサーが利用できないプリントサーバーが回復するのをどのくらいの期間待機するかを指定します。この期間が過ぎると、サーバーは永続的にオフラインであると判断され、その負荷は他の利用可能なプリントサーバーに再分配されます。

デフォルトでは、しきい値は180（秒）に設定されています。

ユニバーサル印刷ポリシー設定

ユニバーサル印刷セクションには、ユニバーサル印刷を管理するためのポリシー設定が含まれています。

ユニバーサル印刷EMF処理モード

この設定は、Windowsユーザーデバイス上のEMFスプールファイルの処理方法を制御します。

デフォルトでは、EMFレコードはプリンターに直接スプールされます。

この設定をポリシーに追加するときは、オプションを選択します。

- プリンター用のEMFを再処理すると、EMFスプールファイルが再処理され、ユーザーデバイス上のGDIサブシステムを介して送信されます。この設定は、EMFの再処理を必要とするが、セッションで自動的に選択されない可能性のあるドライバーに使用できます。
- Citrix Universal™プリンタードライバーで使用する場合、プリンターに直接スプールすると、EMFレコードがスプールされ、処理のためにユーザーデバイスに配信されます。通常、これらのEMFスプールファイルはクライアントのスプールキューに直接挿入されます。EMF形式と互換性のあるプリンターおよびドライバーの場合、これが最速の印刷方法です。

ユニバーサル印刷画像圧縮制限

この設定は、Citrix Universal Print Driverで印刷された画像に利用可能な最大品質と最小圧縮レベルを指定します。

デフォルトでは、画像圧縮制限は「最高品質（ロスレス圧縮）」に設定されています。

「圧縮なし」が選択されている場合、EMF印刷のみ圧縮が無効になります。

この設定をポリシーに追加するときは、オプションを選択します。

- 圧縮なし
- 最高品質 (ロスレス圧縮)
- 高音質
- 標準品質

- 低品質 (最大圧縮)

ユニバーサル印刷最適化のデフォルト設定を含むポリシーにこの設定を追加する場合は、以下の点に注意してください。

- ユニバーサル印刷画像圧縮制限設定の圧縮レベルが、ユニバーサル印刷最適化のデフォルト設定で定義されているレベルよりも低い場合、画像はユニバーサル印刷画像圧縮制限設定で定義されているレベルで圧縮されます。
- 圧縮が無効になっている場合、ユニバーサル印刷最適化のデフォルト設定の「希望する画質」および「ヘビーウェイト圧縮を有効にする」オプションは、ポリシーに影響を与えません。

ユニバーサル印刷最適化のデフォルト

この設定は、セッション用にユニバーサル印刷ドライバーが作成される際の印刷最適化のデフォルト値を指定します。

- 希望する画質は、ユニバーサル印刷に適用されるデフォルトの画像圧縮制限を指定します。デフォルトでは、標準品質が有効になっており、ユーザーは標準または低品質の圧縮を使用してのみ画像を印刷できます。
- ヘビーウェイト圧縮を有効にするは、希望する画質で設定された圧縮レベルを超えて帯域幅を削減するかどうかを有効または無効にします。画質は低下しません。デフォルトでは、ヘビーウェイト圧縮は無効になっています。
- 画像とフォントのキャッシュ設定は、印刷ストリームに複数回出現する画像とフォントをキャッシュするかどうかを指定し、一意の画像またはフォントがプリンターに一度だけ送信されるようにします。デフォルトでは、埋め込み画像とフォントはキャッシュされます。これらの設定は、ユーザーデバイスがこの動作をサポートしている場合にのみ適用されることに注意してください。
- 非管理者によるこれらの設定の変更を許可する設定は、ユーザーがセッション内でデフォルトの印刷最適化設定を変更できるかどうかを指定します。デフォルトでは、ユーザーはデフォルトの印刷最適化設定を変更できません。

注: これらのオプションはすべてEMF印刷でサポートされています。XPS印刷では、「希望する画質」オプションのみがサポートされています。

ユニバーサル印刷画像圧縮制限設定を含むポリシーにこの設定を追加する場合は、以下の点に注意してください。

- ユニバーサル印刷画像圧縮制限設定の圧縮レベルが、ユニバーサル印刷最適化のデフォルト設定で定義されているレベルよりも低い場合、画像はユニバーサル印刷画像圧縮制限設定で定義されているレベルで圧縮されます。

- 圧縮が無効になっている場合、ポリシーでは、ユニバーサル印刷最適化のデフォルト設定の「希望する画質」と「ヘビーウェイト圧縮を有効にする」オプションは無効になります。

ユニバーサル印刷プレビューの優先設定

この設定は、自動作成された、または汎用ユニバーサルプリンターに対して印刷プレビュー機能を使用するかどうかを指定します。

デフォルトでは、自動作成された、または汎用ユニバーサルプリンターに対して印刷プレビューは使用されません。

この設定をポリシーに追加するときは、オプションを選択します。

- 自動作成されたプリンターまたは汎用ユニバーサルプリンターに対して印刷プレビューを使用しない
- 自動作成されたプリンターに対してのみ印刷プレビューを使用する
- 汎用ユニバーサルプリンターに対してのみ印刷プレビューを使用する
- 自動作成されたプリンターと汎用ユニバーサルプリンターの両方に対して印刷プレビューを使用する

ユニバーサル印刷の印刷品質制限

この設定は、セッションで印刷出力を生成するために利用できる最大ドット/インチ (dpi) を指定します。

デフォルトでは、「制限なし」が有効になっており、ユーザーは接続先のプリンターで許可されている最高の印刷品質を選択できます。

この設定が構成されている場合、出力解像度の観点からユーザーが利用できる最大印刷品質が制限されます。印刷品質自体と、ユーザーが接続するプリンターの印刷品質機能の両方が、構成された設定に制限されます。たとえば、中解像度 (600 DPI) に構成されている場合、ユーザーは最大品質600 DPIの出力印刷に制限され、ユニバーサルプリンターダイアログボックスの「詳細設定」タブにある「印刷品質」設定には、中品質 (600 DPI) までの解像度設定のみが表示されます。

この設定をポリシーに追加するときは、オプションを選択します。

- 下書き (150 DPI)
- 低解像度 (300 DPI)
- 中解像度 (600 DPI)
- 高解像度 (1200 DPI)
- 制限なし

セキュリティポリシー設定

「セキュリティ」セクションには、セッション暗号化とログオンデータの暗号化を構成するためのポリシー設定が含まれています。

SecureICAの最小暗号化レベル

この設定は、サーバーとユーザーデバイス間で送信されるセッションデータを暗号化する最小レベルを指定します。

重要: Virtual Delivery Agent 7.xの場合、このポリシー設定は、RC5 128ビット暗号化によるログオンデータの暗号化を有効にするためにのみ使用できます。その他の設定は、Citrix Virtual Apps and Desktopsのレガシーバージョンとの下位互換性のためにのみ提供されています。

VDA 7.xの場合、セッションデータの暗号化はVDAのDelivery Groupの基本設定を使用して行われます。Delivery GroupでEnable Secure ICAが選択されている場合、セッションデータはRC5 (128ビット) 暗号化を使用して暗号化されます。Delivery GroupでEnable Secure ICAが選択されていない場合、セッションデータは基本暗号化で暗号化されます。

この設定をポリシーに追加するときは、オプションを選択してください。

- Basicは、非RC5アルゴリズムを使用してクライアント接続を暗号化します。これにより、データストリームが直接読み取られるのを防ぎますが、復号化は可能です。デフォルトでは、サーバーはクライアント-サーバー間のトラフィックにBasic暗号化を使用します。
- RC5 (128ビット) ログオンは、RC5 128ビット暗号化を使用してログオンデータのみを暗号化し、クライアント接続にはBasic暗号化を使用します。
- RC5 (40ビット) は、RC5 40ビット暗号化を使用してクライアント接続を暗号化します。
- RC5 (56ビット) は、RC5 56ビット暗号化を使用してクライアント接続を暗号化します。
- RC5 (128ビット) は、RC5 128ビット暗号化を使用してクライアント接続を暗号化します。

クライアント/サーバー暗号化に指定する設定は、環境内の他の暗号化設定やWindowsオペレーティングシステムと相互作用する可能性があります。サーバーまたはユーザーデバイスのいずれかでより高い優先度の暗号化レベルが設定されている場合、公開リソースに指定した設定が上書きされることがあります。

特定のユーザーの通信とメッセージの整合性をさらに保護するために、暗号化レベルを上げることができます。ポリシーでより高い暗号化レベルが必要な場合、より低い暗号化レベルを使用しているCitrix Receiversは接続を拒否されます。

SecureICAは認証やデータ整合性のチェックを行いません。サイトにエンドツーエンドの暗号化を提供するには、SecureICAをTLS暗号化と組み合わせて使用してください。

SecureICAはFIPS準拠のアルゴリズムを使用しません。これが問題となる場合は、SecureICAの使用を避けるようにサーバーとCitrix Receiverを構成してください。

SecureICAは、機密保持のためにRFC 2040で説明されているRC5ブロック暗号を使用します。ブロックサイズは64ビット（32ビットワード単位の倍数）です。キー長は128ビットです。ラウンド数は12です。

RC5ブロック暗号のキーは、セッションが作成されるときにネゴシエートされます。ネゴシエーションはDiffie-Hellmanアルゴリズムを使用して実行されます。このネゴシエーションでは、Virtual Delivery Agentがインストールされるときにレジストリに保存されるDiffie-Hellman公開パラメーターを使用します。公開パラメーターは秘密ではありません。Diffie-Hellmanネゴシエーションの結果は秘密鍵であり、そこからRC5ブロック暗号のセッションキーが導出されます。ユーザーログオンとデータ転送には個別のセッションキーが使用され、Virtual Delivery Agentとの間のトラフィックにも個別のセッションキーが使用されます。したがって、各セッションには4つのセッションキーがあります。秘密鍵とセッションキーは保存されません。RC5ブロック暗号の初期化ベクトルも秘密鍵から導出されます。

サーバー制限ポリシー設定

「サーバー制限」セクションには、アイドル接続を制御するためのポリシー設定が含まれています。

サーバーアイドルタイマー間隔

この設定は、ユーザーからの入力がない場合に、中断されないユーザーセッションが維持される期間をミリ秒単位で決定します。

デフォルトでは、アイドル接続は切断されません（サーバーアイドルタイマー間隔 = 0）。Citrix®は、この値を最低60000ミリ秒（60秒）に設定することを推奨します。

ポリシーを表示するには、**複数のバージョン**を選択し、シングルセッションOSのバージョンをクリアしてから、**サーバー制限**を選択します。

> **注**
>
> このポリシー設定が使用されている場合、セッションが指定された時間アイドル状態であったときに、ユーザーに「アイドルタイマーの期限切れ」ダイアログボックスが表示されることがあります。Citrixポリシー設定は、このMicrosoftダイアログボックスメッセージを制御しません。詳細については、`<http://support.citrix.com/article/CTX118618>`を参照してください。

セッション制限ポリシー設定

セッション制限セクションには、セッションが強制的にログオフされるまでに接続を維持する期間を制御するポリシー設定が含まれています。

> **重要:**
>
> - この記事で説明されている設定は、マルチセッションVDAを実行しているマシンには適用されません。マルチセッションVDAを実行しているマシンでのセッション時間制限の構成については、Microsoft KB - セッション時間制限を参照してください。
> - Windows Server 2012以降、Microsoft KB - セッション時間制限で言及されている*ターミナルサービス*という用語は、*リモートデスクトップサービス*を指します。

切断されたセッションタイマー

この設定は、以下を有効または無効にします。

- 切断されロックされたデスクトップが、セッションがログオフされるまでにロックされたままになる時間を指定するタイマー。

このタイマーが有効になっている場合、タイマーの期限が切れると、切断されたセッションはログオフされます。

デフォルトでは、切断されたセッションはログオフされません。

Remote PC Accessの切断されたセッションタイマー

この設定は、タイマーの期限が切れた後に切断されたユーザーセッションをログオフするタイマーを有効または無効にします。この設定を有効にする場合は、**切断されたセッションのタイマー間隔**設定を使用して、ユーザーセッションがログオフされるまでに切断されたデスクトップがロックされたままになる時間を分数で指定します。

デフォルトでは、この設定は無効になっています。

切断されたセッションタイマー間隔

この設定は、切断されロックされたデスクトップが、セッションがログオフされるまでにロックされたままになる時間を分数で指定します。

デフォルトでは、期間は1,440分（24時間）です。

セッション接続タイマー

この設定は、ユーザーデバイスとデスクトップ間の途切れない接続の最大継続時間を指定するタイマーを有効または無効にします。このタイマーが有効になっている場合、タイマーの期限が切れるとセッションは切断されるか、ログオフされます。Microsoft の「**時間制限に達したときにセッションを終了する**」設定が、セッションの次の状態を決定します。

デフォルトでは、このタイマーは無効になっています。

セッション接続タイマー間隔

この設定は、ユーザーデバイスとデスクトップ間の途切れない接続の最大分数（時間）を指定します。

デフォルトでは、最大継続時間は1,440分（24時間）です。

セッションアイドルタイマー

ユーザーが何も入力しない場合、この設定は以下を有効または無効にするために使用されます。

- デスクトップへの途切れないユーザーデバイス接続が維持される期間を指定するタイマー。

このタイマーの期限が切れると、セッションは切断状態になり、「**切断されたセッションタイマー**」が適用されます。「**切断されたセッションタイマー**」が無効になっている場合、セッションはログオフされません。

デフォルトでは、このタイマーは有効になっています。

セッションアイドルタイマー間隔

ユーザーからの入力がない場合、この設定は以下を指定するために使用されます。

- デスクトップへのユーザーデバイスの途切れない接続が維持される分数。

デフォルトでは、アイドル状態の接続は1,440分（24時間）維持されます。

> **注：**

> 2203 LTSR CU2リリース以降、マルチセッションVDAを実行しているマシンに対して、以下のセッション時間制限設定を構成できます。

切断されたセッションタイマー – マルチセッション

この設定は、切断されたRDSセッションがログオフされるまでにどのくらいの期間持続できるかを決定するタイマーを有効または無効にします。デフォルトでは、このタイマーは無効になっており、切断されたセッションはログオフされません。

切断されたセッションタイマー間隔 – マルチセッション

この設定は、切断されたRDSセッションがログオフされるまでにどのくらいの期間（分単位）持続できるかを決定します。デフォルトでは、期間は1440分（24時間）です。

セッション接続タイマー – マルチセッション

この設定は、ユーザーデバイスとターミナルサーバー間の途切れない接続の最大継続時間を指定するタイマーを有効または無効にします。デフォルトでは、このタイマーは無効になっています。

セッション接続タイマー間隔 – マルチセッション

この設定は、ユーザーデバイスとRDSセッション間の途切れない接続の最大分数（時間）を指定します。デフォルトでは、最大継続時間は1440分（24時間）です。

セッションアイドルタイマー – マルチセッション

この設定は、ユーザーデバイスとターミナルサーバー間のアイドル接続の最大期間を決定するタイマーを有効または無効にします。デフォルトでは、このタイマーは無効になっています。

セッションアイドルタイマー間隔 – マルチセッション

この設定は、ユーザーデバイスとRDSセッション間のアイドル接続が何分間維持されるかを指定します。デフォルトでは、最大期間は1440分（24時間）です。

> **注：**
>
> Citrix®ポリシーを使用して構成されたマルチセッションマシンのタイマー設定は、Microsoftグループポリシーを通じて構成されたタイマー設定を上書きすることが想定されています。予期しない動作を避けるため、いずれかの方法を使用してタイマー設定を構成することをお勧めします。

セッションの信頼性ポリシー設定

「セッションの信頼性」セクションには、セッションの信頼性接続を管理するためのポリシー設定が含まれています。

セッションの信頼性接続

この設定により、ネットワーク接続が失われたときにセッションを開いたままにするかどうかが決まります。セッションの信頼性は、自動クライアント再接続と連携して、ネットワーク障害から回復した後にユーザーがCitrix Workspace™アプリセッションに自動的に再接続できるようにします。デフォルトでは、セッションの信頼性は許可されています。

Citrix Studio の設定は、次の目的でクライアントに適用されます。

- Citrix Workspaceアプリ1808以降
- Citrix Receiver for Windows 4.7以降のバージョン。

Citrix Studio ポリシーは、クライアント上の Citrix Receiver™ グループポリシーオブジェクトを上書きします。Studio でこれらのポリシーを更新すると、セッションの信頼性がサーバーからクライアントに同期されます。

> **注：**
>
> - Windows 4.7 以降の Citrix Receiver および Windows 用 Citrix Workspace アプリ - Studio でポリシーを設定します。
> - Windows 4.7 より前の Citrix Receiver - Studio でポリシーを設定します。また、一貫した動作のために、クライアントで Citrix Receiver グループポリシーオブジェクトテンプレートを設定します。

> ネットワーク接続が中断された場合、セッションの信頼性によりセッションがアクティブな状態に保たれ、ユーザーの画面に表示されます。ユーザーは、ネットワーク接続が再開されるまで、使用しているアプリケーションを引き続き見ることができます。

セッションの信頼性を使用して、サーバー上でセッションをアクティブな状態に保ちます。接続が失われたことを示すために、ユーザーのディスプレイは不透明になります。ユーザーは中断中にフリーズしたセッションを見る可能性があります。ネットワーク接続が復元されると、ユーザーはアプリケーションとの対話を再開できます。セッションの信頼性により、再認証のプロンプトなしでユーザーが再接続されます。

セッションの信頼性と自動クライアント再接続の両方を使用する場合、これら2つの機能は順番に動作します。セッションの信頼性は、セッションの信頼性タイムアウト設定で指定された時間の経過後にユーザーセッションを閉じ（または切断し）ます。その後、自動クライアント再接続設定が有効になり、切断されたセッションにユーザーを再接続しようとします。

デフォルトでは、セッションの信頼性は許可されています。

> **注：**
>
> Citrix ADCを使用している場合、ICA接続をプロキシするには、Citrix StoreFront > **Manage Citrix Gateways / Secure Ticket Authority**で**セッションの信頼性を有効にする**を選択する必要があります。

セッションの信頼性を無効にするには：

1. Citrix Studio を起動します。
2. **セッションの信頼性接続**ポリシーを開きます。
3. ポリシーを**禁止**に設定します。



セッションの信頼性ポート番号

この設定は、受信セッションの信頼性接続に使用するTCPポート番号を指定します。

デフォルトでは、ポート番号は2598に設定されています。

セッションの信頼性ポート番号を変更するには：

1. Citrix Studio を起動します。
2. **セッションの信頼性ポート番号**ポリシーを開きます。
3. ポート番号を編集します。
4. **OK**をクリックします。

セッションの信頼性タイムアウト

この設定は、セッションの信頼性プロキシがユーザーの再接続を待機し、セッションが切断されるまでの時間を秒単位で指定します。

セッションが開いている時間を延長することはできますが、この機能は利便性のためであり、ユーザーに再認証を促すものではありません。セッションが開いている時間が長くなるほど、ユーザーがデバイスを放置し、不正なユーザーがアクセスする可能性が高まります。

デフォルトでは、タイムアウトは180秒（3分）に設定されています。

セッションの信頼性タイムアウトを変更するには：

1. Citrix Studio を起動します。
2. **セッションの信頼性タイムアウト**ポリシーを開きます。
3. タイムアウト値を編集します。
4. **OK**をクリックします。

セッションウォーターマークポリシー設定

セッションウォーターマークセクションには、この機能を構成するためのポリシー設定が含まれています。 この機能を有効にすると、VDAマシンのネットワーク帯域幅とCPU使用率が大幅に増加します。利用可能なハードウェアリソースに基づいて、選択したVDAマシンに対してセッションウォーターマークを構成することをお勧めします。

> **重要**
>
> 他のウォーターマークポリシー設定を有効にするには、セッションウォーターマークを有効にします。より良いユーザーエクスペリエンスを実現するために、2つを超えるウォーターマークテキスト項目を有効にしないでください。

セッションウォーターマークを有効にする

この設定を有効にすると、セッションディスプレイには、セッション固有の情報を表示する不透明なテキストウォーターマークが表示されます。他のウォーターマーク設定は、この設定が有効になっているかどうかに依存します。

デフォルトでは、セッションウォーターマークは無効になっています。

クライアントIPアドレスを含める

この設定を有効にすると、セッションは現在のクライアントIPアドレスをウォーターマークとして表示します。

デフォルトでは、クライアントIPアドレスを含めるは無効になっています。

接続時間を含める

この設定を有効にすると、セッションウォーターマークに接続時間が表示されます。形式はyyyy/mm/dd hh:mmです。表示される時刻は、システムクロックとタイムゾーンに基づいています。

デフォルトでは、接続時間を含めるは無効になっています。

ログオンユーザー名を含める

この設定を有効にすると、セッションは現在のログオンユーザー名をウォーターマークとして表示します。表示形式はUSERNAME@DOMAINNAMEです。ユーザー名は最大20文字にすることをお勧めします。ユーザー名が20文字を超えると、文字フォントが過度に小さくなったり、切り捨てられたりして、ウォーターマークの効果が低下する可能性があります。

デフォルトでは、ログオンユーザー名を含めるは有効になっています。

VDAホスト名を含める

この設定を有効にすると、セッションは現在のICA®セッションのVDAホスト名をウォーターマークとして表示します。

デフォルトでは、VDAホスト名を含める設定が有効になっています。

VDA IPアドレスを含める

この設定を有効にすると、セッションは現在のICAセッションのVDA IPアドレスをウォーターマークとして表示します。

デフォルトでは、VDA IPアドレスは無効になっています。

セッションウォーターマークのスタイル

この設定は、単一のウォーターマークテキストラベルを表示するか、複数のラベルを表示するかを制御します。「**値**」ドロップダウンメニューから「**複数**」または「**単一**」を選択します。

「**複数**」は、セッションに5つのウォーターマークラベルを表示します。中央に1つ、四隅に4つです。

「**単一**」は、セッションの中央に単一のウォーターマークラベルを表示します。

デフォルトでは、セッションウォーターマークのスタイルは「複数」です。

ウォーターマークのカスタムテキスト

この設定では、セッションウォーターマークに表示するカスタムテキスト文字列（例：会社名）を指定します。空でない文字列を構成すると、ウォーターマークで有効になっている他の情報に加えて、そのテキストが新しい行に表示されます。 ウォーターマークのカスタムテキストの最大長は25 Unicode文字です。より長い文字列を構成した場合、25文字に切り詰められます。

デフォルトのテキストはありません。

透かしの透明度

ウォーターマークの不透明度を0から100まで指定できます。指定する値が大きいほど、ウォーターマークは不透明になります。

デフォルトでは、値は17です。

タイムゾーン制御ポリシー設定

「タイムゾーン制御」セクションには、セッションでのローカル時間の使用に関連するポリシー設定が含まれています。

レガシークライアントのローカル時間を推定する

この設定は、不正確なタイムゾーン情報をサーバーに送信するユーザーデバイスのローカルタイムゾーンの推定を有効または無効にします。

デフォルトでは、サーバーは必要に応じてローカルタイムゾーンを推定します。

この設定は、詳細なタイムゾーン情報をサーバーに送信しないレガシーなCitrix ReceiverまたはICAクライアントでの使用を目的としています。サポートされているバージョンのCitrix Receiver™ for Windowsなど、詳細なタイムゾーン情報をサーバーに送信するCitrix Receiverと併用した場合、この設定は効果がありません。

セッション切断またはログオフ時にデスクトップOSのタイムゾーンを復元する

この設定は、ユーザーが切断またはログオフしたときに、シングルセッションOS VDAのタイムゾーン設定がマシンの元のタイムゾーンに復元されるかどうかを決定します。この設定を有効にすると、ユーザーが切断またはログオフしたときに、VDAはマシンのタイムゾーンを元の設定に復元します。この設定を有効にするには、**クライアントのローカル時間を使用**を**クライアントのタイムゾーンを使用**に設定します。

デフォルトでは、この設定は有効になっています。

クライアントのローカル時間を使用

この設定は、ユーザーセッションのタイムゾーン設定を決定します。選択肢は、ユーザーセッションのタイムゾーン（サーバータイムゾーン）またはユーザーデバイスのタイムゾーン（クライアントタイムゾーン）です。

デフォルトでは、ユーザーセッションのタイムゾーンが使用されます。

この設定を有効にするには、グループポリシーエディターで**タイムゾーンリダイレクトを許可**設定を有効にします。この設定は、**ローカルコンピューターポリシー** > **コンピューターの構成** > **管理**

用テンプレート > **Windowsコンポーネント** > **リモートデスクトップサービス** > **リモートデスクトップセッションホスト** > **デバイスとリソースのリダイレクト**にあります。

サーバーOSを実行しているマシンでシングルセッションVDA（以前はワークステーションVDAとして知られていました）を使用している場合は、ローカルユーザー権限の**タイムゾーンの変更**を**Everyone**に構成します。このユーザー権限は、**ローカルコンピューターポリシー** > **コンピューターの構成** > **Windowsの設定** > **セキュリティの設定** > **ローカルポリシー** > **ユーザー権利の割り当て**にあります。

> **注：**
>
> シングルセッションOSでは、**ユーザー**はユーザー権利の割り当ての**タイムゾーンの変更**に含まれますが、マルチセッションOSでは含まれません。マルチセッションOSでは、タイムゾーンは次のグループポリシーを使用して同期されます: コンピューターの構成\管理用テンプレート\Windowsコンポーネント\リモートデスクトップサービス\リモートデスクトップセッションホスト\デバイスとリソースのリダイレクト\タイムゾーンリダイレクトを許可。このポリシーは、サーバーがマルチセッションOS VDAのリモートデスクトップセッションホストではない場合（`/ServerVDI`コマンドでインストールされた場合）には適用されません。マルチセッションOSでは、デフォルトで、また設計上、ユーザーはタイムゾーンを変更するローカル権限を持っていません。

TWAINデバイスのポリシー設定

TWAINデバイスセクションには、デジタルカメラやスキャナーなどのクライアントTWAINデバイスのマッピング、およびサーバーからクライアントへの画像転送の最適化に関連するポリシー設定が含まれています。

> **注：**
>
> Citrix Receiver for Windows 4.5では、TWAIN 2.0がサポートされています。

クライアントTWAINデバイスのリダイレクト

TWAINデバイスは、TWAINプロトコルを使用して、サーバーでホストされている画像処理アプリケーションと通信します。

この設定は、ユーザーがユーザーデバイス上のTWAINデバイスにアクセスすることを許可または禁止します。デフォルトでは、TWAINデバイスのリダイレクトは許可されています。

関連するポリシー設定は次のとおりです。

- TWAIN圧縮レベル
- TWAINデバイスのリダイレクト帯域幅制限
- TWAINデバイスリダイレクト帯域幅制限の割合

TWAIN圧縮レベル

この設定は、クライアントからサーバーへの画像転送の圧縮レベルを指定します。最良の画質には「低」、良好な画質には「中」、低い画質には「高」を使用します。デフォルトでは、中程度の圧縮が適用されます。

USBデバイスポリシー設定

USBデバイスセクションには、USBデバイスのファイルリダイレクトを管理するためのポリシー設定が含まれています。

クライアントUSBデバイス最適化ルール

クライアントUSBデバイス最適化ルールは、最適化を無効にするか、最適化モードを変更するためにデバイスに適用できます。

ユーザーがUSB入力デバイスを接続すると、ホストは**USBポリシー**設定がそのデバイスを許可するかどうかを確認します。デバイスが許可されている場合、ホストはデバイスの**クライアントUSBデバイス最適化ルール**を確認します。ルールが指定されていない場合、デバイスは最適化されません。キャプチャモード (04) は、署名デバイスに推奨されるモードです。高遅延によってパフォーマンスが低下する他のデバイスの場合、管理者はインタラクティブモード (02) を有効にできます。この記事の表で利用可能なモードの説明を参照してください。

知っておくとよいこと

- Wacomの署名パッドおよびタブレットを使用する場合は、スクリーンセーバーを無効にすることをお勧めします。スクリーンセーバーを無効にする手順は、このセクションの最後にあります。
- Wacom STU署名パッドおよびタブレットシリーズ製品の最適化のサポートは、Citrix Virtual Apps and Desktops™ポリシーのインストール時に事前設定されています。
- 署名デバイスはCitrix Virtual Apps and Desktops全体で動作し、署名デバイスとして使用するためにドライバーを必要としません。Wacomには、デバイスをさらにカスタマイズするためにインストールできる追加のソフトウェアがあります。`<http://www.wacom.com/>`を参照してください。

- 描画タブレット。特定の描画入力デバイスは、PCI/ACPIバス上でHIDデバイスとして表示される場合があり、サポートされていません。これらのデバイスは、Citrix Virtual Desktopsセッション内でリダイレクトされるように、クライアント上のUSBホストコントローラーに接続してください。

ポリシールールは、空白で区切られたtag=value形式の式を取ります。以下のタグがサポートされています。

タグ名	説明
モード	最適化モードは、class=**03**の入力デバイスでサポートされています。サポートされているモードは次のとおりです。最適化なし - 値**01**。インタラクティブモード - 値**02**。ペンタブレットや3D Proマウスなどのデバイスに推奨されます。キャプチャモード - 値**04**。署名パッドなどのデバイスに推奨されます。
VID	デバイス記述子からのベンダーID。4桁の16進数で指定します。
PID	デバイス記述子からの製品ID。4桁の16進数で指定します。
REV	デバイス記述子からのリビジョンID。4桁の16進数で指定します。
クラス	デバイス記述子またはインターフェース記述子のいずれかからのクラス。
サブクラス	デバイス記述子またはインターフェース記述子のいずれかからのサブクラス。
保護	デバイス記述子またはインターフェース記述子のいずれかからのプロトコル。

例

Mode=00000004 VID=067B PID=1230 class=03 #キャプチャモードで動作する入力デバイス

Mode=00000002 VID=067B PID=1230 class=03 #インタラクティブモードで動作する入力デバイス（デフォルト）

Mode=00000001 VID=067B PID=1230 class=03 #最適化なしで動作する入力デバイス

Mode=00000100 VID=067B PID=1230 #デバイスセットアップの最適化が無効（デフォルト）

Mode=00000200 VID=067B PID=1230 #デバイスセットアップの最適化が有効

Wacom署名パッドデバイスのスクリーンセーバーを無効にする

Wacom署名パッドおよびタブレットを使用するには、Citrix®はスクリーンセーバーを次のように無効にすることをお勧めします。

1. デバイスをリダイレクトした後、**Wacom-STU-Driver**をインストールします。
2. 署名パッドのコントロールパネルにアクセスするには、**Wacom-STU-Display MSI**をインストールします。
3. **コントロールパネル > Wacom STU Display > STU430** または **STU530** に移動し、お使いのモデルのタブを選択します。
4. 「**変更**」を選択し、UACセキュリティウィンドウが表示されたら「**はい**」を選択します。
5. 「**スライドショーを無効にする**」を選択し、「**適用**」を選択します。

1つの署名パッドモデルに対して設定が行われると、その設定はすべてのモデルに適用されます。

クライアントUSBデバイスのリダイレクト

この設定は、USBデバイスのユーザーデバイスとの間のリダイレクトを許可または禁止します。

デフォルトでは、USBデバイスはリダイレクトされません。

クライアントUSBデバイスリダイレクト規則

この設定は、USBデバイスのリダイレクト規則を指定します。

デフォルトでは、ルールは指定されていません。

ユーザーがUSBデバイスを接続すると、ホストデバイスは一致が見つかるまで各ポリシー規則と照合して確認します。いずれかのデバイスに対する最初の一致が最終的なものと見なされます。最初の一致が許可ルールである場合、そのデバイスは仮想デスクトップにリモート接続されます。最初の一致が拒否ルールである場合、そのデバイスはローカルデスクトップでのみ利用可能です。一致が見つからない場合、デフォルトのルールが使用されます。

ポリシー規則は{Allow:`|`Deny:}の形式をとり、その後に空白で区切られたtag=value式のセットが続きます。次のタグがサポートされています。

タグ名	説明
VID	デバイス記述子からのベンダーID

タグ名	説明
PID	デバイス記述子からの製品ID
REL	デバイス記述子からのリリースID
クラス	デバイス記述子またはインターフェイス記述子のいずれかからのクラス
サブクラス	デバイス記述子またはインターフェース記述子のいずれかからのサブクラス
プロトコル	デバイス記述子またはインターフェイス記述子のいずれかからのプロトコル

ポリシー規則を作成する際は、次の点に注意してください。

- 規則では大文字と小文字は区別されません。
- 規則の末尾にはオプションのコメントを付けることができます。コメントは#で始まります。
- 空行と純粋なコメント行は無視されます。
- タグは一致演算子 = を使用する必要があります (例: VID=067B_。
- 各ルールは新しい行で開始するか、セミコロンで区切られたリストの一部である必要があります。
- USB Implementers Forum, Inc. の Web サイトで入手可能な USB クラスコードを参照してください。

管理者定義の USB ポリシールールの例:

- 許可: VID=067B PID=0007 # 別の産業、別のフラッシュドライブ
- 拒否: Class=08 subclass=05 # マスストレージ
- すべての USB デバイスを拒否するルールを作成するには、他のタグなしで「DENY:」を使用します。

クライアント USB プラグアンドプレイデバイスのリダイレクト

この設定により、カメラや販売時点情報管理 (POS) デバイスなどのプラグアンドプレイデバイスをクライアントセッションで使用することを許可または禁止します。

デフォルトでは、プラグアンドプレイデバイスのリダイレクトは許可されています。「許可」に設定すると、特定のユーザーまたはグループのすべてのプラグアンドプレイデバイスがリダイレクトされます。「禁止」に設定すると、デバイスはリダイレクトされません。

USB デバイスの自動リダイレクトを構成する

USBサポートが有効になっており、USBユーザー設定がUSBデバイスを自動的に接続するように設定されている場合、USBデバイスは自動的にリダイレクトされます。

> **注：**

> Receiver for Windows 4.2では、デスクトップアプライアンスモードで動作し、接続バーが表示されていない場合も、USBデバイスは自動的にリダイレクトされます。以前のバージョンのCitrix Receiver for Windowsでは、デスクトップアプライアンスモードまたは仮想マシン（VM）でホストされているアプリケーションで動作している場合も、USBデバイスは自動的にリダイレクトされます。

> すべてのUSBデバイスをリダイレクトすることが常に最適であるとは限りません。ユーザーは、自動的にリダイレクトされないUSBデバイスリストからデバイスを明示的にリダイレクトできます。USBデバイスがリストに表示されたり、リダイレクトされたりするのを防ぐには、クライアントエンドポイントまたはDDCポリシーのいずれかでDeviceRulesを使用します。詳細については、管理者ガイドを参照してください。

> **注意:**

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

USBデバイスの自動リダイレクトに関するユーザー設定

ポリシー:

1. **ローカルグループポリシーエディター**を開き、**管理用テンプレート > Citrixコンポーネント > Citrix Receiver™ > クライアントデバイスのリモート処理 > 汎用USBリモーティング**に移動します。
2. **新しいUSBデバイス**を開き、**有効**を選択し、**OK**をクリックします。
3. **既存のUSBデバイス**を開き、**有効**を選択し、**OK**をクリックします。

シトリックス レシーバー:

1. **Citrix Receiverの環境設定 > 接続**に移動します。
2. 以下に示すオプションが選択されていることを確認します。
   - セッションの開始時に、デバイスを自動的に接続する
   - セッションの実行中に新しいデバイスが接続された場合、デバイスを自動的に接続する。
3. **OK**をクリックします。

すべてのレジストリキーとポリシーの変更は、Windowsクライアントデバイスに適用されます。

通常のUSBプリンターのリダイレクト

通常のUSBプリンターに最適なソリューションは、専用のユニバーサルプリンタードライバーと仮想チャネルを使用して印刷を実行することです。デフォルトでは、通常のUSBプリンターは自動的にリダイレクトされません。

通常のプリンターはヒューリスティックを使用して検出されますが、たとえばスキャン機能を備えた高度なプリンターは、完全に機能させるためにUSBサポートを使用してリダイレクトする必要がある場合があります。

通常のプリンターが自動的にリダイレクトされるかどうかを構成するには、このレジストリを使用します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectPrinters

種類: DWORD

データ: 00000000

デフォルト値は0です（自動的にリダイレクトしません）。値を0より大きい任意の数値に変更すると、通常のUSBプリンターをリダイレクトするためのUSBサポートが有効になります。

Active Directoryポリシーをこのレジストリキーに展開し、両方が存在する場合は非ポリシー値を上書きすることもできます。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectAudio

種類: DWORD

データ: 00000000

通常のオーディオデバイスのリダイレクト

通常のプリンターと同様に、通常のオーディオデバイスからオーディオデータを送信するには、ICA®の専用オーディオ仮想チャネルを使用することで最高のユーザーエクスペリエンスが実現されます。ただし、一部の特殊なデバイスはUSBサポートを使用してリダイレクトする必要がある場合があります。どのデバイスが通常のオーディオデバイスであるかを判断するためにヒューリスティックが使用されます。

通常のオーディオデバイスが自動的にリダイレクトされるかどうかを構成するには、クライアントエンドポイントでこのレジストリを使用します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectAudio

種類: DWORD

データ: 00000000

デフォルトは0に設定されています (自動的にリダイレクトしません)。値を0以外に変更すると、USBサポート付きのプレーンなUSBオーディオデバイスがリダイレクトされます。

Active Directoryポリシーを使用して、この値をレジストリキーに展開し、両方が存在する場合は非ポリシー値を上書きできます。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名前：AutoRedirectVideo

種類: DWORD

データ: 00000000

プレーンなストレージデバイス (マスストレージデバイス) のリダイレクト

プレーンなストレージデバイスの場合、最適化も行うクライアントドライブマッピングなど、専用の仮想チャネルを使用することで、最高のユーザーエクスペリエンスを実現できます。ファイルの単純な読み書きに加えて、CD/DVDの書き込みや暗号化されたファイルシステムデバイスへのアクセスなど、特定の特殊なタスクを実行するには、ジェネリックUSBサポートを使用してデバイスをリダイレクトする必要がある場合があります。

どのデバイスがプレーンなストレージデバイスであるかを判断するために、ヒューリスティックが使用されます。プレーンなストレージデバイスを自動的にリダイレクトするかどうかを設定するには、このレジストリキーを使用します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectStorage

種類: DWORD

データ: 00000000

デフォルトは0に設定されています (自動的にリダイレクトしません)。値を0以外に変更すると、ジェネリックUSBサポートを使用してプレーンなUSBストレージデバイスがリダイレクトされます。

Active Directoryポリシーを使用して、この値を以下のレジストリキーに展開し、両方が存在する場合は非ポリシー値を上書きすることもできます。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectStorage

種類: DWORD

データ: 00000000

> **注：**
>
> 汎用USBサポートを使用している場合、プレーンストレージデバイスへの読み取り専用アクセスは構成できませんが、CDMを使用している場合は構成できます。

ハードウェア暗号化機能付きUSBフラッシュドライブのリダイレクト

ハードウェア暗号化を備えたUSBフラッシュドライブは通常、暗号化されたストレージパーティションと、暗号化されたパーティションのロックを解除するためのユーティリティを含む2番目のユーティリティパーティションで構成されています。USBフラッシュドライブデバイスの場合、最適化も実行する専用のクライアントドライブマッピング/動的サムドライブマッピングHDX仮想チャネルを使用することで、最高のユーザーエクスペリエンスを実現できます。

汎用USBリダイレクトは、Windows以外のクライアント（Linuxクライアントなど）や、顧客がクライアント上のローカル機能へのユーザーアクセスを制限（ロックダウン）しているクライアントに必要です。汎用USBリダイレクトは、ハードウェア暗号化のないあらゆるUSBストレージデバイスを、シングルセッションOSおよびマルチセッションOS VDAセッションの両方にリダイレクトできます。

Citrix Virtual Apps and Desktops 7 1808より前は、ハードウェア暗号化を備えたUSBフラッシュドライブは、シングルセッションOSまたはマルチセッションOS VDAセッションに有用な方法でリダイレクトできませんでした。Citrix Virtual Apps and Desktops 7 1808で導入された新しい機能強化により、ハードウェア暗号化を備えたUSBフラッシュドライブの汎用USBリダイレクトが、シングルセッションOSおよびマルチセッションOS VDAセッションでサポートされるようになりました。 デバイスがリダイレクトされた後、そのドライブはローカルクライアントには表示されません。したがって、ドライブのロック解除が必要な場合は、セッション内で実行してください。この機能には、Windows Update KB4074590が必要です。

プレーン静止画デバイス (スキャナーおよびデジタルカメラ)

通常の静止画デバイスの場合、最適化も実行する専用の仮想チャネル（TWAIN仮想チャネルなど）を使用することで、最高のユーザーエクスペリエンスを実現できます。これらのデバイスは業界標準に準拠している必要があります。デバイスが非準拠であるか、または本来の意図に従って使用されていない場合、汎用USBリダイレクトがデバイスを使用する唯一の方法となる可能性があります。どのデバイスが通常の静止画デバイスであるかを判断するためにヒューリスティックが使用されます。

このレジストリキーを使用して、プレーン静止画デバイスが自動的にリダイレクトされるかどうかを構成します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectImage

種類: DWORD

データ: 00000000

デフォルトは0に設定されています（自動的にリダイレクトされません）。値を0以外に変更すると、汎用USBのプレーンなUSB静止画デバイスがリダイレクトされます。

Active Directoryポリシーを使用して、この値をこのレジストリキーに展開することもでき、両方が存在する場合は非ポリシー値を上書きします。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectImage

種類: DWORD

データ: 00000000

デバイス固有の設定

Citrixが最適化可能なデバイス（プリンター、オーディオ、ビデオ、ストレージ、静止画デバイスなど）を選択するために使用されるヒューリスティックは、必ずしもお客様の希望と一致するとは限りません。上記にリストされていないデバイスの自動リダイレクトを制御したい場合があります。デバイス固有の基準で自動リダイレクトを制御できます。

例として、DemoTech 2,000バーコードリーダーはUSBサポートを使用してリダイレクトする必要はありません。ベンダー識別子は12AB、製品識別子は5678です。これらの16進数はデバイスマネージャーで確認できます。

これが自動的にリダイレクトされるのを防ぐには、このデバイス固有のレジストリキーを作成します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

名前: AutoRedirect

種類: DWORD

データ: 00000000

値が0の場合、デバイスは自動的にリダイレクトされません。0以外の値は、デバイスが自動リダイレクトの対象となることを示します（ユーザー設定による）。ベンダー識別子と製品識別子の間には単一のスペース文字があります。

Active Directoryポリシーを使用して、この値をこのレジストリキーに展開することもできます。両方が存在する場合、非ポリシー値を上書きします。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

名前: AutoRedirect

種類: DWORD

データ: 00000000

デバイス固有のAutoRedirect設定は、上記で説明したより一般的なAutoRedirectXXX値よりも優先されます。Citrix最適化デバイスのデフォルトのヒューリスティックは、デバイスを汎用として誤って解釈する可能性があります。したがって、デバイス固有のAutoRedirect値を1に設定して、自動的にリダイレクトします。

仮想チャネル許可リストポリシー設定

仮想チャネル許可リストポリシー設定は、ICA®セッションで開くことが許可されている仮想チャネルを指定する許可リストの使用を有効にします。

無効にすると、すべての仮想チャネルが許可されます。

有効にすると、Citrix®仮想チャネルのみが許可されます。

カスタムまたはサードパーティの仮想チャネルを使用するには、仮想チャネルをリストに追加します。仮想チャネルをリストに追加するには、仮想チャネル名の後にコンマを入力し、次に仮想チャネルにアクセスするプロセスのパスを入力します。複数の実行可能パスをリストでき、パスはコンマで区切られます。

例:

```
CTXCVC1,C:\VC1\vchost.exe
```

```
CTXCVC2,C:\VC2\vchost.exe,C:\Program Files\Third Party\vcaccess.exe
```

Citrix Virtual Apps and Desktops™ 7 2109以降、仮想チャネル許可リストはデフォルトで有効になっています。

Skype for Business 用の HDX RealTime Optimization Pack を使用している場合は、仮想チャネルを許可リストに追加します。詳細については、「HDX RealTime Optimization Pack のドキュメント」を参照してください。

> **重要:**
>
> 設定を有効にするには、VDAマシンを再起動する必要があります。

> 仮想チャネルの詳細については、「ICA仮想チャネル」を参照してください。

視覚表示ポリシー設定

「ビジュアル表示」セクションには、仮想デスクトップからユーザーデバイスに送信される画像の品質を制御するためのポリシー設定が含まれています。

シンプルなグラフィックの優先色深度

このポリシー設定は、VDAバージョン7.6 FP3以降で利用可能です。8ビットオプションは、VDAバージョン7.12以降で利用可能です。

この設定により、シンプルなグラフィックがネットワーク経由で送信される際の色の深度を下げることができます。ピクセルあたり8ビットまたは16ビットに下げることで、低帯域幅接続での応答性が向上する可能性がありますが、画質はわずかに低下します。「ビデオコーデックを使用して圧縮する」ポリシー設定が「画面全体」に設定されている場合、8ビットの色の深度はサポートされません。

デフォルトの優先色深度はピクセルあたり24ビットです。

8ビット設定がVDAバージョン7.11以前に適用された場合、VDAは24ビット（デフォルト）の色深度にフォールバックします。

ターゲットフレームレート

この設定は、仮想デスクトップからユーザーデバイスに送信される1秒あたりの最大フレーム数を指定します。

デフォルトでは、最大は1秒あたり30フレームです。

1秒あたりのフレーム数を高く設定する（例：30）と、ユーザーエクスペリエンスは向上しますが、より多くの帯域幅が必要になります。1秒あたりのフレーム数を減らす（例：10）と、ユーザーエクスペリエンスを犠牲にしてサーバーのスケーラビリティが最大化されます。CPUが遅いユーザーデバイスの場合、ユーザーエクスペリエンスを向上させるために低い値を指定してください。

1秒あたりの最大サポートフレームレートは60です。

視覚品質

この設定は、ユーザーデバイスに表示される画像の希望する視覚品質を指定します。

デフォルトでは、この設定は「中」です。

画像の品質を指定するには、次のいずれかのオプションを選択します。

- **低** - 帯域幅が制限されたネットワークで、対話性のために視覚的な品質を犠牲にできる場合に推奨されます。
- **中** - ほとんどのユースケースで最高のパフォーマンスと帯域幅効率を提供します。
- **高** - 視覚的にロスレスな画質が必要な場合に推奨されます。
- **ロスレスにビルド** - ネットワークアクティビティが高い期間はロッシー画像をユーザーデバイスに送信し、ネットワークアクティビティが低下した後はロスレス画像を送信します。この設定により、帯域幅が制限されたネットワーク接続でのパフォーマンスが向上します。
- **常にロスレス** - 画像データの保持が不可欠な場合は、「常にロスレス」を選択して、非可逆データがユーザーデバイスに送信されないようにします。たとえば、画質の劣化が許されないX線画像を表示する場合などです。

動きのある画像ポリシー設定

動きのある画像セクションには、動的な画像の圧縮を削除または変更できる設定が含まれています。

最小画像品質

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、アダプティブディスプレイの許容される最小画像品質を指定します。圧縮が少ないほど、表示される画像の品質は高くなります。超高、非常に高、高、標準、低のいずれかの圧縮を選択します。

デフォルトでは、これは標準に設定されています。

動きのある画像の圧縮

この設定は、アダプティブディスプレイが有効になっているかどうかを指定します。アダプティブディスプレイは、利用可能な帯域幅に基づいて、スライドショー内のビデオやトランジションスライドの画像品質を自動的に調整します。アダプティブディスプレイが有効になっている場合、ユーザーは品質の低下なしにスムーズなプレゼンテーションを見ることができます。

デフォルトでは、アダプティブディスプレイは有効になっています。

VDAバージョン7.0から7.6の場合、この設定はレガシーグラフィックモードが有効になっている場合にのみ適用されます。VDAバージョン7.6 FP1以降の場合、この設定はレガシーグラフィックモードが有効になっている場合、またはレガシーグラフィックモードが無効でビデオコーデックがグラフィックの圧縮に使用されていない場合に適用されます。

レガシーグラフィックモードが有効になっている場合、ポリシーの変更を有効にするにはセッションを再起動する必要があります。アダプティブディスプレイはプログレッシブディスプレイと

相互排他的です。アダプティブディスプレイを有効にするとプログレッシブディスプレイが無効になり、その逆も同様です。ただし、プログレッシブディスプレイとアダプティブディスプレイの両方を同時に無効にすることができます。プログレッシブディスプレイはレガシー機能であるため、XenAppまたはXenDesktopでは推奨されません。プログレッシブしきい値レベルを設定すると、アダプティブディスプレイが無効になります。

プログレッシブ圧縮レベル

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、詳細度は低いものの、より高速な画像の初期表示を提供します。

デフォルトでは、プログレッシブ圧縮は適用されません。

通常の非可逆圧縮設定で定義された、より詳細な画像は、利用可能になったときに表示されます。写真などの帯域幅を多く消費するグラフィックの表示を改善するには、非常に高または超高圧縮を使用します。

プログレッシブ圧縮を有効にするには、その圧縮レベルが「ロッシー圧縮レベル」設定よりも高くする必要があります。

注：プログレッシブ圧縮に関連する圧縮レベルの増加は、クライアント接続を介した動的画像の対話性も向上させます。回転する3Dモデルなどの動的画像の品質は、画像が動きを停止するまで一時的に低下し、その時点で通常のロッシー圧縮設定が適用されます。

関連するポリシー設定は次のとおりです。

- プログレッシブ圧縮しきい値
- プログレッシブヘビーウェイト圧縮

プログレッシブ圧縮しきい値

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、プログレッシブ圧縮が適用される接続の最大帯域幅を1秒あたりのキロビットで表します。これは、この帯域幅以下のクライアント接続にのみ適用されます。

デフォルトでは、しきい値は1秒あたり2147483647キロビットです。

関連するポリシー設定は次のとおりです。

- プログレッシブ圧縮しきい値

- プログレッシブヘビーウェイト圧縮

目標最小フレームレート

この設定は、低帯域幅の条件下で、動的画像に対してシステムが維持しようとする1秒あたりの最小フレームレートを指定します。

デフォルトでは、これは10fpsに設定されています。

VDAバージョン7.0から7.6の場合、この設定はレガシーグラフィックモードが有効になっている場合にのみ適用されます。VDAバージョン7.6 FP1以降の場合、この設定はレガシーグラフィックモードが無効または有効になっている場合に適用されます。

静止画像ポリシー設定

静止画像セクションには、静止画像の圧縮を削除または変更できる設定が含まれています。

追加の色圧縮

この設定は、帯域幅が制限されているクライアント接続を介して配信される画像に対する追加の色圧縮の使用を有効または無効にし、表示される画像の品質を低下させることで応答性を向上させます。

デフォルトでは、追加の色圧縮は無効になっています。

有効にすると、追加の色圧縮は、クライアント接続の帯域幅が「追加の色圧縮しきい値」を下回っている場合にのみ適用されます。クライアント接続の帯域幅がしきい値を超えている場合、または「無効」が選択されている場合、追加の色圧縮は適用されません。

追加の色圧縮しきい値

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、追加の色圧縮が適用される接続の最大帯域幅をキロビット/秒で表します。クライアント接続の帯域幅が設定値を下回ると、有効になっている場合、追加の色圧縮が適用されます。

デフォルトでは、しきい値は8192キロビット/秒です。

ヘビーウェイト圧縮

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、より高度でCPU負荷の高いグラフィックアルゴリズムを使用することで、画質を損なうことなくプログレッシブ圧縮を超えて帯域幅を削減することを有効または無効にします。

デフォルトでは、ヘビーウェイト圧縮は無効になっています。

有効にすると、ヘビーウェイト圧縮はすべての非可逆圧縮設定に適用されます。Citrix Workspace™アプリでサポートされていますが、他のプラグインには影響しません。

関連するポリシー設定は次のとおりです。

- プログレッシブ圧縮レベル
- プログレッシブ圧縮しきい値

非可逆圧縮レベル

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、帯域幅が制限されているクライアント接続を介して配信される画像に使用される非可逆圧縮の度合いを制御します。このような場合、圧縮なしで画像を表示すると遅くなることがあります。

デフォルトでは、中程度の圧縮が選択されています。

帯域幅を多く消費する画像の応答性を向上させるには、高圧縮を使用します。画質の劣化が許容されないX線画像を表示する場合など、画像データの保持が不可欠な場合は、非可逆圧縮を使用しない方がよいでしょう。

関連ポリシー設定：非可逆圧縮しきい値

非可逆圧縮しきい値

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、非可逆圧縮が適用される接続の最大帯域幅を1秒あたりのキロビット数で表します。

デフォルトでは、しきい値は1秒あたり2147483647キロビットです。

ポリシーに非可逆圧縮レベル設定を追加し、しきい値を指定しないことで、LAN経由での写真などの高精細ビットマップの表示速度を向上させることができます。

関連ポリシー設定：非可逆圧縮レベル

WebSocketsポリシー設定

「WebSockets」セクションには、HTML5 用 Citrix Workspace™ アプリを使用して仮想デスクトップおよびホスト型アプリケーションにアクセスするためのポリシー設定が含まれています。WebSockets 機能は、ブラウザベースのアプリケーションとサーバー間の双方向通信を行うこと

で、セキュリティを向上させ、オーバーヘッドを削減します。この機能は、複数の HTTP 接続を開くことなくこれを実現します。

WebSockets接続

この設定では、WebSockets接続を許可または禁止します。

デフォルトでは、WebSocket接続は禁止されています。

WebSocketsポート番号

この設定では、受信WebSocket接続のポートを識別します。

デフォルトでは、値は8008です。

WebSockets信頼済みオリジンサーバーリスト

この設定では、通常はWeb向けCitrix Workspaceアプリである、URLとして表現された信頼済みオリジンサーバーのコンマ区切りリストを提供します。サーバーは、これらのアドレスのいずれかから発信されたWebSockets接続のみを受け入れます。

デフォルトでは、ワイルドカード「*」は、すべての Citrix Workspace app for Web URL を信頼するために使用されます。

リストにアドレスを入力する場合は、次の構文を使用します。

\<protocol>://\<ホストの完全修飾ドメイン名>:

プロトコルはHTTPまたはHTTPSである必要があります。ポートが指定されていない場合、HTTPにはポート80が、HTTPSにはポート443が使用されます。

ワイルドカード `*` は、IP アドレス (10.105..) の一部として使用する場合を除き、URL 内で使用できます。

WIA デバイスのポリシー設定

WIAデバイスセクションには、Windows Image Acquisition (WIA) を使用したスキャナーリダイレクトを管理するためのポリシー設定が含まれています。

WIA リダイレクト

デジタルカメラやスキャナーなどの WIA デバイスは、WIA フレームワークを使用して、サーバーでホストされている画像処理アプリケーションと通信します。この設定により、ユーザーがユーザーデバイス上の WIA デバイスにアクセスすることを許可または禁止します。デフォルトでは、WIA リダイレクトは禁止されています。

WIA 準拠デバイスの詳細については、「WIA デバイス」を参照してください。

レジストリで管理されるHDX™機能

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

> レジストリエディターを開くには、サーバーで `regedit.exe` を実行します。次に、設定を追加または編集するレジストリキーに移動します。

デバイス

Bloombergキーボード

Citrix Virtual Apps and Desktops™は、Bloombergモデル4およびモデル3のスターボードキーボードをサポートしています。デフォルトでは、拡張Bloombergキーボードのサポートは無効になっています。

Bloomberg keyboard のサポートを有効にするには、接続を開始する前にクライアントマシンで次のレジストリ値を設定します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICAClient\GenericUSB
- 値の名前: EnableBloombergHID
- 値の型: DWORD
- 値のデータ: 0 = 無効、1 = 有効

詳しくは、「Bloombergキーボード」を参照してください。

マップされたクライアントドライブ

セキュリティ上の予防措置として、ユーザーがCitrix Virtual Apps and Desktopsにログオンすると、デフォルトでは、サーバーはユーザーの実行権限なしでクライアントドライブをマップします。マップされたクライアントドライブにある実行可能ファイルをユーザーが実行できるようにするには、サーバーのレジストリを編集してこのデフォルト設定を上書きします。

アクセスを許可するには、次のレジストリ値を編集します (**CDMSettings**が存在しない場合は作成します)。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\CDMSettings
- 値の名前: ExecuteFromMappedDrive
- 値の型: DWORD
- 値のデータ: 1 = 許可、0 = マップされたドライブでのアクセス拒否

この変更は、レジストリを編集した後に接続されたセッションに適用されます。

詳しくは、マップされたクライアントドライブを参照してください。

マイクロソフト Surface Pro および Surface Book ペン

Citrix Virtual Apps and Desktopsは、Windows Inkベースのアプリケーションで標準のペン機能をサポートしています。デフォルトでは、この機能は有効になっています。

この機能を無効または有効にするには、次のレジストリ値を設定します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Citrix Virtual Desktop Agent\PenApi
- 値の名前: DisablePen
- 値の型: DWORD
- 値のデータ: 1 = 無効、0 = 有効

詳細については、「Microsoft Surface Pro および Surface Book のペン」を参照してください。

Windows Image Acquisitionアプリケーションの許可リスト

この設定により、VDA 上のどのアプリケーションが Windows イメージ取得スキャナーリダイレクトにアクセスできるかを制御できます。

デフォルトでは、どのアプリケーションも Windows イメージ取得にアクセスできません。

VDA 上のアプリケーションに対して Windows イメージ取得を調整するには、次のレジストリ設定を作成します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix
- 値の名前: WIAAllowedProcesses

  WIAAllowedProcesses を選択して右クリックします。「**新規 > 複数行文字列値**」を選択し、新しい値の名前を **AllowProcesses** に変更します。
- 値のデータ: Windows イメージ取得にアクセスできる各アプリケーションの完全なパスとプロセス名を入力します。各アプリケーションは新しい行に入力してください。

この設定への変更は、次回 VDA でセッションを起動したときに有効になります。

全般

VDAへの自動ログオンを構成する

この設定により、Windows 10シングルセッションOSおよびマルチセッションOSのVDAで、Microsoftポリシー設定の**常にパスワードを要求する**を有効または無効にできます。

もし**常にパスワードを要求する**が有効になっている場合、ユーザーはリモートセッションを開始するときにVDAで資格情報を入力する必要があります。この設定が無効になっている場合、ユーザーはVDAで資格情報を提供することなく、自動的にリモートセッションに接続します。

デフォルトでは、Microsoftポリシー設定は無効になっています。**常にパスワードを要求する**設定を有効または無効にするには、VDAで次のレジストリ値を設定します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Portica
- 値の名前: AutoLogon
- 値の型: DWORD
- 値のデータ:
  - 1 - Microsoftポリシー設定を無効にし、ユーザーがリモートセッションに自動的にサインインできるようにします。
  - 0 – Microsoftポリシー設定を有効にし、ユーザーがリモートセッションを起動するときに資格情報の入力を求めます。

タイムアウト警告を無効にする

デフォルトでは、非アクティブまたはアイドル状態のセッションを持つユーザーは、セッションが自動的に切断される2分前に警告メッセージを受け取ります。

この設定は、Windows 2004以降のマルチセッションOSでアイドルセッションのタイムアウト制限に達したユーザーに対する警告メッセージを無効にして削除します。警告を削除するには、VDAで次のレジストリ値を設定します。

- キー: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Winstations\ICA-CGP
- 値の名前: fEnableTimeoutWarning
- 値の型: DWORD
- 値のデータ: 1 = 警告メッセージを無効にする, 0 = 警告メッセージを有効にする

警告メッセージを表示するには、レジストリ値を削除するか、0に設定します。

EDT MTU検出

MTU検出により、EDTはセッション確立時に最大転送単位（MTU）を自動的に決定できます。これにより、パフォーマンスの低下やセッション確立の失敗につながる可能性のあるEDTパケットの断片化を防ぎます。

この設定はデフォルトで有効になっています。EDT MTU検出を無効にするには、以下のレジストリ値を構成し、VDAを再起動します。

- キー: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd
- 値の名前: MtuDiscovery
- 値の型: DWORD
- 値のデータ: 0

この設定はマシン全体に適用され、サポートされているクライアントから接続するすべてのセッションに影響します。

一般的なコンテンツリダイレクト

ホストからクライアントへのリダイレクトにURLタイプを追加する

デフォルトでは、次のURLタイプのリダイレクトをサポートしています: HTTP、HTTPS、RTSP、RTSPU、PNM、およびMMS。Windowsクライアントで次のレジストリキーと値を作成することで、URLタイプをリストに追加できます。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA
- 値の名前: ExtraURLProtocols
- 値の型: REG_SZ
- 値のデータ: 必要なURLタイプをセミコロンで区切って指定します。URLのオーソリティ部分より前のすべてを含めます。例： `ftp://;mailto:;customtype1://;custometype2://`

URLタイプはWindowsクライアントにのみ追加できます。このレジストリ設定がないクライアントは、Citrixセッションへのリダイレクトを拒否します。クライアントには、指定されたURLタイプを処理するようにインストールおよび構成されたアプリケーションが必要です。

詳細については、「ホストからクライアントへのリダイレクト」を参照してください。

クライアントフォルダーリダイレクト

クライアントフォルダーリダイレクトは、クライアント側のファイルがホスト側のセッションでアクセス可能になる方法を変更します。サーバーでクライアントフォルダーリダイレクトを有効にし、ユーザーがユーザーデバイスでそれを構成すると、ユーザーが指定したローカルボリュームの一部がリダイレクトされます。

サーバーでクライアントフォルダーリダイレクトを有効にするには、次のレジストリ値を設定します。

- キー：HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection
- 値の名前: CFROnlyModeAvailable
- 値の型: DWORD
- 値のデータ: 1

詳細については、クライアントフォルダーリダイレクトを参照してください。

特定のWebサイトセットに対するホストからクライアントへのリダイレクト

特定のWebサイトセットに対してホストからクライアントへのリダイレクトを有効にするには、サーバーVDAで次のレジストリ値を設定します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- 値の名前: ValidSites
- 値の型: REG_MULTI_SZ
- 値のデータ: 完全修飾ドメイン名 (FQDN) の任意の組み合わせを指定します。複数のFQDNを別々の行に入力します。プロトコル (`http://` または `https://`) を含めず、FQDNのみを含めます。FQDNには、アスタリスク (`*`) をワイルドカード文字として左端の位置にのみ含めることができます。このワイルドカードは、RFC 6125のルールに準拠した単一レベルのドメインに一致します。例:

`www.example.com`

`*.example.com`

詳細については、ホストからクライアントへのリダイレクトを参照してください。

ログオフ時および切断時のローカルアプリケーションの動作

デフォルトでは、ユーザーが仮想デスクトップからログオフまたは切断しても、ローカルアプリケーションは実行を継続します。再接続後、ローカルアプリケーションが仮想デスクトップで利

用可能な場合、それらは再統合されます。ログオフ時および切断時のローカルアプリケーションの動作を構成するには、ホストされたデスクトップで次のレジストリ値を設定します。

- キー：HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Citrix\Client Hosted Apps\Policies
- 値の名前: Session State
- 値の型: DWORD
- 値のデータ:
  - 1 - ユーザーが仮想デスクトップからログオフまたは切断しても、ローカルアプリケーションは実行を継続します。再接続すると、仮想デスクトップで利用可能な場合、ローカルアプリケーションが再統合されます。
  - 3 - ユーザーが仮想デスクトップからログオフまたは切断すると、ローカルアプリケーションは閉じます。

詳しくは、「Local App Access and URL redirection」を参照してください。

ホストからクライアントへのリダイレクトのデフォルトリストからURLタイプを削除する

デフォルトのリダイレクトリストからURLタイプを削除するには、サーバーVDAで以下のレジストリキーと値を作成します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- 値の名前: DisableServerFTA
- 値の型: DWORD
- 値のデータ: 1
- 値の名前: NoRedirectClasses
- 値の型: REG_MULTI_SZ
- 値のデータ: 次の値の任意の組み合わせを指定します: `http`、`https`、`rtsp`、`rtspu`、`pnm`、または `mms`。複数の値を別々の行に入力します。例:

`http`

`https`

`rtsp`

詳しくは、「Host to client redirection」を参照してください。

サーバーVDAのデフォルトブラウザ構成

ホストからクライアントへのリダイレクトを有効にすると、Server VDA のデフォルトのブラウザ設定を上書きできます。Web URL がリダイレクトされない場合、Citrix ランチャーは `command_backup` レジストリキーで構成されているブラウザに URL を渡します。このキーはデフォルトで Internet Explorer を指していますが、別のブラウザへのパスを含むように変更できます。

- Internet Explorer (デフォルト)
  - キー: HKEY_CLASSES_ROOT\http\shell\open\command_backup
  - 値の名前: Default
  - 値の型: REG_SZ
  - 値のデータ: `"c:\program files\internet explorer\iexplore.exe" %1`
  - キー: HKEY_CLASSES_ROOT\https\shell\open\command_backup`
  - 値の名前: Default
  - 値の型: REG_SZ
  - 値のデータ: `"c:\program files\internet explorer\iexplore.exe" %1`
- グーグル クローム
  - キー: HKEY_CLASSES_ROOT\http\shell\open\command_backup
  - 値の名前: Default
  - 値の型: REG_SZ
  - 値のデータ: `"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" %1`
  - キー: HKEY_CLASSES_ROOT\https\shell\open\command_backup
  - 値の名前: Default
  - 値の型: REG_SZ
  - 値のデータ: `"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" %1`
- マイクロソフト エッジ
  - キー: HKEY_CLASSES_ROOT\http\shell\open\command_backup
  - 値の名前: Default
  - 値の型: REG_SZ

- 値のデータ: `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" %1`
- キー: HKEY_CLASSES_ROOT\https\shell\open\command_backup
- 値の名前: Default
- 値の型: REG_SZ
- 値のデータ: `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" %1`

公開アプリケーションのローカルアプリアクセス

ローカルアプリアクセスは、ローカルにインストールされたWindowsアプリケーションを、デスクトップを切り替えることなくホストされたデスクトップ環境にシームレスに統合します。公開アプリケーションへのアクセスを提供するには、サーバーで次のレジストリ値を設定します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\DesktopStudio
- 値の名前: ClientHostedAppsEnabled
- 値の型: DWORD
- 値のデータ: 1 = 有効、0 = 無効

詳細については、ローカルアプリアクセスとURLリダイレクトを参照してください。

グラフィック

CUDAまたはOpenCLアプリケーションのGPUアクセラレーション

ユーザーセッションで実行されているCUDAおよびOpenCLアプリケーションのGPUアクセラレーションは、デフォルトで無効になっています。

CUDAアクセラレーションのPOC機能を使用するには、次のレジストリ設定を有効にします。

- レジストリキー: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper
- 値の名前: CUDA
- 値の型: DWORD
- 値のデータ: 00000001

OpenCLアクセラレーションのPOC機能を使用するには、次のレジストリ設定を有効にします。

- レジストリキー: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper
- 値の名前: OpenCL
- 値の型: DWORD
- 値のデータ: 00000001

詳細については、WindowsマルチセッションOSのGPUアクセラレーションを参照してください。

プログレッシブモード

プログレッシブモードはデフォルトで無効になっています。以下のレジストリ値でプログレッシブモードの状態を変更できます:

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- 値の型: REG_DWORD
- 値の名前: ProgressiveDisplay
- 値のデータ:
  - 0 = 常にオフ (プログレッシブモードを無効にします。この値がデフォルトです。)
  - 1 = 自動 (ネットワークの状態に基づいて切り替えます。)
  - 2 = 常にオン

詳細については、プログレッシブモードを参照してください。

Windows Presentation Foundation (WPF) レンダリング

HDX 3D Proを使用すると、WindowsマルチセッションOSセッションで実行されているグラフィック負荷の高いアプリケーションを、サーバーのグラフィック処理ユニット (GPU) でレンダリングできます。Windows Presentation Foundation (WPF) のレンダリングをサーバーのGPUに移行することで、グラフィックレンダリングがサーバーのCPUを遅くすることはありません。

サーバーのGPUを使用してWPFアプリケーションのレンダリングを有効にするには、WindowsマルチセッションOSを実行しているサーバーのレジストリに次の設定を作成します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432\Citrix\CtxHook\AppInit_Dlls\Multiple Monitor Hook
- 値の名前: EnableWPFHook
- 値の型: DWORD
- 値のデータ: 00000001

詳細については、WindowsマルチセッションOSのGPUアクセラレーションを参照してください。

マルチメディア

マルチメディア会議中のエコーを回避する

Citrix Virtual Apps and Desktopsは、エコーを最小限に抑えるエコーキャンセルオプションを提供します。この機能はデフォルトで有効になっています。エコーキャンセルを無効にするには、次のいずれかのレジストリ設定を変更できます。

- キー:
  - 32ビット: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio
  - 64ビット: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio
- 値の名前: EchoCancellation
- 値の型: DWORD
- 値のデータ: False

詳細については、オーディオ機能を参照してください。

オーディオの制限

クライアントにオーディオデバイスをインストールし、オーディオリダイレクトを有効にしてRDSセッションを開始した後、オーディオファイルが再生されない場合があります。回避策として、RDSマシンに以下のレジストリキーを追加し、マシンを再起動してください。

- キー: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SCMConfig
- 値の名前: EnableSvchostMitigationPolicy
- 値の型: DWORD
- 値のデータ: 0

詳細については、オーディオ機能を参照してください。

ブラウザコンテンツリダイレクトとDPI

ユーザーのマシンでDPI（スケーリング）が100%を超えて設定されている状態でブラウザコンテンツリダイレクトを使用すると、リダイレクトされたブラウザコンテンツ画面が正しく表示されません。この問題を回避するには、ユーザーのマシンで以下のレジストリ値を作成して、Chromeのブラウザコンテンツリダイレクト GPUアクセラレーションを無効にしてください。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\HdxMediaStream
- 値の名前: GPU
- 値の型: DWORD
- 値のデータ: 0

詳しくは、「ブラウザコンテンツリダイレクトとDPI」を参照してください。

高解像度Webカメラストリーミング

サーバー上のビデオ会議アプリケーションは、サポートされているフォーマットタイプに基づいてWebカメラのフォーマットと解像度を選択します。Citrix Virtual Apps and Desktopsは、最大1920x1080のWebカメラ解像度をサポートしています。高解像度Webカメラストリーミングを無効または有効にするには、以下のレジストリ値を追加します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDXRealTime
- 値の名前: Enable_HighDefWebcam
- 値の型: DWORD
- 値のデータ:
  - 0 = 高解像度Webカメラストリーミングを無効にする
  - 1 = 高解像度Webカメラストリーミングを有効にする

高解像度Webカメラの解像度

メディアタイプのネゴシエーションが失敗した場合、HDXはデフォルトの解像度である352x288 CIFにフォールバックします。クライアントでレジストリキーを使用してデフォルトの解像度を構成できます。以下のレジストリキーを設定する前に、カメラが指定された解像度をサポートしていることを確認してください。

- キー: HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime
- 幅
  - 値の名前: DefaultWidth
  - 値の型: DWORD
  - 値のデータ: 10進数での希望の幅（例: 1280）
- 高さ
  - 値の名前: DefaultHeight
  - 値の型: DWORD

- Value data: 10進数での希望の高さ（例：720）

高解像度Webカメラの帯域幅

HDX Webカメラのビデオ圧縮は、プラグアンドプレイの汎用USBリダイレクトと比較して帯域幅の使用量が少なく、WAN接続でも良好に動作します。帯域幅を調整するには、クライアントで次のレジストリ値を設定します。

- キー: HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime
- 値の名前: TargetBitrate
- 値の型: DWORD
- 値のデータ: 350000

ビット/秒単位で値を入力します。帯域幅を指定しない場合、ビデオ会議アプリケーションはデフォルトで350000 bpsを使用します。

詳細については、HDX webcam video compressionを参照してください。

Microsoft Teamsのフォールバックモード

Microsoft Teamsが最適化されたVDIモードでロードに失敗した場合 (Teams/About/Versionで「Citrix HDX Not Connected」と表示される場合)、VDAはウェブカメラのリダイレクトやクライアントオーディオおよびマイクのリダイレクトなど、従来のHDXテクノロジーにフォールバックします。Microsoft Teamsの最適化をサポートしないWorkspaceアプリのバージョン/プラットフォームOSを使用している場合、フォールバックレジストリキーは適用されません。

フォールバックメカニズムを制御するには、VDA上で以下のいずれかのレジストリ値を設定します。

- キー（いずれか1つのみ必要）:
  - **コンピューター設定:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Teams
  - **ユーザー設定:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Teams
- 値の名前: DisableFallback
- 値の型: DWORD
- 値のデータ: 1 = フォールバックモードを無効にする、2 = オーディオのみを有効にする

値が存在しないか0に設定されている場合、フォールバックモードが有効になります。この機能には、Microsoft Teamsバージョン1.3.0.13565以降が必要です。詳細については、「Microsoft Teamsの最適化」を参照してください。

Citrix App Layering™を使用したMicrosoft Teamsの最適化

Citrix App Layeringを使用してVDAとMicrosoft Teamsのインストールを異なるレイヤーで管理している場合は、**ALLUSER**=1でMicrosoft Teamsをインストールする前に、このレジストリキーをWindowsに展開します。

PortICAという名前の空のレジストリキーを作成し、既定の値の名前、種類、データをそのままにします。

- レジストリエディターの32ビット版のキー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\PortICA
- レジストリエディターの64ビット版のキー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA

詳細については、「Microsoft Teamsの最適化」を参照してください。

ブラウザコンテンツリダイレクトでの統合Windows認証によるシングルサインオン

この設定は、VDAと同じドメイン内で統合Windows認証 (IWA) で構成されたWebサーバーへのシングルサインオンを提供します。シングルサインオンを有効にするには、以下のレジストリ値を1に設定します。

- キー:
  - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediastream

  または
  - HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\HdxMediastream
- 値の名前: WebBrowserRedirectionIwaSupport
- 値の型: DWORD
- 値のデータ: 1

詳細については、「統合 Windows 認証によるシングルサインオン」を参照してください。

ユーザーエージェント要求ヘッダー

ユーザーエージェントヘッダーは、ブラウザコンテンツリダイレクトから送信されるHTTP要求を識別するのに役立ちます。この設定は、プロキシおよびファイアウォールルールを構成する際に役立ちます。たとえば、サーバーがブラウザコンテンツリダイレクトから送信される要求をブロックする場合、ユーザーエージェントヘッダーを含むルールを作成して、特定の要件をバイパスできます。Windowsデバイスのみがユーザーエージェント要求ヘッダーをサポートします。

デフォルトでは、ユーザーエージェント要求ヘッダー文字列は無効になっています。クライアントでレンダリングされるコンテンツのユーザーエージェントヘッダーを有効にするには、レジストリエディターを使用します。

各Citrix Workspace™ app for Windowsクライアントで、以下のいずれかのレジストリ設定を行います。

- キー:
  - 32ビット: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStream
  - 64ビット: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\HdxMediaStream
- 値の名前: EnableCefUserAgentString
- 値の型: DWORD
- 値のデータ: 1

レジストリ値を追加すると、ユーザーエージェントヘッダーにはCitrixBCR/2102.1というテキストが含まれます。ここで2102.1はCitrix Workspace app for Windowsのバージョンです。

Webカメラのソフトウェア圧縮

Webカメラがハードウェアエンコーディングをサポートしている場合、HDXビデオ圧縮はデフォルトでハードウェアエンコーディングを使用します。ハードウェアエンコーディングは、ソフトウェアエンコーディングよりも多くの帯域幅を消費する可能性があります。ソフトウェア圧縮を強制するには、クライアントで以下の値を追加します。

- キー: HKEY_CURRENT_USER\SOFTWARE\Citrix\HdxRealTime
- 値の名前: DeepCompress_ForceSWEncode
- 値の型: DWORD
- 値のデータ: 1

詳細については、HDX webcam video compressionを参照してください。

Webカメラビデオ圧縮

HDX Webカメラビデオ圧縮は、H.264ビデオを仮想セッションで実行されているビデオ会議アプリケーションに直接送信します。VDAリソースを最適化するために、HDX Webカメラ圧縮はWebカメラビデオのエンコード、トランスコード、デコードを行いません。この機能はデフォルトで有効になっています。

サーバーからビデオ会議アプリへの直接ビデオストリーミングを無効にするには、VDAで次のレジストリ値を設定します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxRealTime
- 値の名前: OfferH264ToApp
- 値の型: DWORD
- 値のデータ: 0

詳細については、HDX webcam video compressionを参照してください。

Webカメラビデオ圧縮フレームレート

優先ビデオフレームレートを調整するには、クライアントで次のレジストリ値を編集します。

- キー: HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime
- 値の名前: FramesPerSecond
- 値の型: DWORD
- 値のデータ: 15

ウェブカメラが指定されたフレームレートをサポートしていない場合、アプリケーションはデフォルトで15 FPSを使用します。

詳細については、HDXウェブカメラビデオ圧縮を参照してください。

ロード管理ポリシー設定

ロード管理セクションには、WindowsマルチセッションOSマシンを提供するサーバー間のロード管理を有効にして構成するためのポリシー設定が含まれています。

ロード評価インデックスの計算については、CTX202150を参照してください。

同時ログオン許容数

この設定は、サーバーが受け入れることができる同時ログオンの最大数を指定します。

デフォルトでは、これは2に設定されています。

この設定が有効な場合、負荷分散は、指定された数を超えるログオンが同時にサーバーVDAでアクティブにならないように試みます。ただし、この制限は厳密には適用されません。制限を適用し（指定された数を超える同時ログオンを失敗させる）、次のレジストリキーを作成します。

> HKLM\Software\Citrix\DesktopServer\LogonToleranceIsHardLimit 種類: DWORD 値: 1

CPU使用率

この設定は、サーバーがフルロードを報告するCPU使用率のレベルをパーセンテージで指定します。有効にすると、サーバーがフルロードを報告するデフォルト値は90%です。

デフォルトでは、この設定は無効になっており、CPU使用率は負荷計算から除外されます。

CPU使用率から除外されるプロセスの優先度

> **注：**
>
> マシンがWorkspace Environment Managementによって管理されているシナリオでは、この設定をCPU Priority設定と併用すると、意図しない結果が生じる可能性があります。CPU Priority設定を使用することを選択した場合は、この設定を無効にすることをお勧めします。

> この設定は、プロセスのCPU使用率がCPU使用率負荷インデックスから除外される優先度レベルを指定します。

デフォルトでは、これは**標準以下**または**低**に設定されています。

ディスク使用量

この設定は、サーバーが75%のフルロードを報告するディスクキューの長さを指定します。有効にすると、ディスクキューのデフォルト値は8です。

デフォルトでは、この設定は無効になっており、ディスク使用率は負荷計算から除外されます。

セッションの最大数

この設定は、サーバーがホストできるセッションの最大数を指定します。有効にすると、サーバーがホストできるセッションの最大数のデフォルト設定は250になります。

デフォルトでは、この設定は有効になっています。

メモリ使用量

この設定は、サーバーがフルロードを報告するメモリ使用量のレベルをパーセンテージで指定します。有効にすると、サーバーがフルロードを報告するデフォルト値は90%になります。

デフォルトでは、この設定は無効になっており、メモリ使用量は負荷計算から除外されます。

メモリ使用量のベースロード

この設定は、ベースオペレーティングシステムのメモリ使用量の近似値を指定し、サーバーがゼロロードであると見なされるメモリ使用量をMB単位で定義します。

デフォルトでは、これは768 MBに設定されています。

プロファイル管理ポリシー設定

このセクションには、プロファイル管理を有効にし、プロファイル管理の処理に含めるグループと除外するグループを指定するためのポリシー設定が含まれています。

等価の.iniファイル設定の名前や、ポリシー設定に必要なプロファイル管理のバージョンなどのその他の情報については、「プロファイル管理ポリシー」を参照してください。

高度なポリシー設定

ロックされたファイルへのアクセス時の再試行回数

ロックされたファイルへのアクセス時の再試行回数を設定します。

このポリシーが無効になっている場合、5回の再試行のデフォルト値が使用されます。ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、デフォルト値が使用されます。

ログオフ時にインターネットCookieファイルを処理する

一部の展開では、`Index.dat` が参照しない余分なインターネットCookieが残されます。継続的なブラウジングの後、ファイルシステムに残された余分なCookieは、プロファイルの肥大化につながる可能性があります。このポリシーを使用すると、Profile Managementを有効にしてIndex.datの処理を強制し、余分なCookieを削除できます。このポリシーはログオフ時間を増加させるため、この問題が発生した場合にのみ有効にしてください。

ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、Index.datの処理は行われません。

自動構成を無効にする

Profile Managementは、Citrix Virtual Desktops™環境（パーソナルvDiskの有無など）を検査し、それに応じてグループポリシーを構成します。「未構成」状態のProfile Managementポリシーのみが調整されるため、行ったカスタマイズはすべて保持されます。

このポリシーにより、展開を高速化し、最適化を簡素化できます。このポリシーを構成する必要はありません。ただし、次のいずれかの操作を行う場合は、自動構成を無効にできます。

- 以前のバージョンからの設定を保持するためにアップグレードする
- トラブルシューティング

自動構成は、実行時に環境に応じてデフォルトのポリシー設定を自動的に構成する動的な構成チェッカーと見なすことができます。これにより、設定を手動で構成する必要がなくなります。実行時環境には以下が含まれます。

- ウィンドウズ OS
- Windows OS のバージョン
- シトリックス バーチャル デスクトップの有無
- パーソナル vDisk の有無

環境が変更された場合、自動構成によって以下のポリシーが変更される可能性があります。

- アクティブライトバック
- 常にキャッシュ
- ログオフ時にローカルにキャッシュされたプロファイルを削除
- キャッシュされたプロファイルを削除するまでの遅延
- プロファイルストリーミング

異なる OS でのポリシーのデフォルトの状態については、次の表を参照してください。

	マルチセッションOS	シングルセッションOS
アクティブライトバック	有効	Personal vDiskが使用されている場合は*無効*。それ以外の場合は、有効。
常にキャッシュ	無効	Personal vDiskが使用されている場合は*無効*。それ以外の場合は、有効。
ログオフ時にローカルにキャッシュされたプロファイルを削除	有効	以下のいずれかの状況が発生した場合、*無効*になります: Personal vDiskが使用されている、Citrix Virtual Desktopsが割り当てられている、またはCitrix Virtual Desktopsがインストールされていない。それ以外の場合は有効です。

	マルチセッションOS	シングルセッションOS
キャッシュされたプロファイルを削除するまでの遅延	0秒	ユーザーの変更が永続的でない場合は60秒。それ以外の場合は0秒。
プロファイルストリーミング	有効	Personal vDiskが使用されている場合は*無効*。それ以外の場合は、有効。

ただし、自動構成が無効になっている場合、上記のすべてのポリシーはデフォルトで**無効**になります。

> **重要:**

> Personal vDiskは非推奨です。詳細については、PVD、AppDisk、およびサポートされていないホストの削除を参照してください。

> Profile Management 1909以降、Windows 10 (バージョン1607以降) およびWindows Server 2016以降のスタートメニューで改善されたエクスペリエンスを得ることができます。この改善は、以下のポリシーの自動構成によって実現されます。

- `Appdata\Local\Microsoft\Windows\Caches`と`Appdata\Local\Packages`を**ミラーリングするフォルダー**に追加します。
- `Appdata\Local\Microsoft\Windows\UsrClass.Dat*`を**同期するファイル**に追加します。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

この設定がここで、または.iniファイルで構成されていない場合、自動構成がオンになります。この場合、環境が変更されるとProfile Managementの設定が変更される可能性があります。

問題が発生した場合にユーザーをログオフする

問題が発生した場合に Profile Management がユーザーをログオフさせるかどうかを指定できます。

このポリシーが無効になっているか、構成されていない場合、問題が発生すると Profile Management はユーザーに一時プロファイルを提供します。たとえば、ユーザー ストアが利用できない場合などです。

有効になっている場合、エラーメッセージが表示され、ユーザーはログオフされます。この設定により、問題のトラブルシューティングが簡素化されます。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

この設定がここで、または.iniファイルで構成されていない場合、一時プロファイルが提供されます。

カスタマー エクスペリエンス向上プログラム

デフォルトでは、カスタマー エクスペリエンス向上プログラムが有効になっており、匿名統計と使用状況データを収集することで、Citrix® 製品の品質とパフォーマンスの向上に役立てています。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

Outlook の検索インデックス ローミングを有効にする

ユーザープロファイルとともに Outlook 検索データを自動的にローミングすることで、ユーザーベースの Outlook 検索エクスペリエンスを許可します。この機能には、Outlook の検索インデックスを保存するために、ユーザー ストアに追加のスペースが必要です。

このポリシーを有効にするには、ログオフしてから再度ログオンしてください。

Outlook 検索インデックス データベース – バックアップと復元

Outlook の検索インデックス ローミングを有効にするポリシーが有効になっている場合に、ログオン中に Profile Management が何を行うかを指定できます。

このポリシーが有効になっている場合、Profile Management は、ログオン時に検索インデックス データベースが正常にマウントされるたびに、そのデータベースをバックアップします。Profile Management は、そのバックアップを検索インデックス データベースの良好なコピーとして扱います。データベースの破損により検索インデックス データベースのマウントが失敗した場合、Profile Management は検索インデックス データベースを最後に確認された良好なコピーに戻します。

> 注:
>
> 新しいバックアップが正常に保存されると、Profile Managementは以前に保存されたバックアップを削除します。バックアップは利用可能なVHDXストレージを消費します。

プロファイルコンテナのマルチセッションライトバックを有効にする

マルチセッションシナリオでプロファイルコンテナのライトバックを有効にします。有効にすると、すべてのセッションでの変更がプロファイルコンテナに書き戻されます。そうでない場合、プロファイルコンテナでは最初のセッションのみが読み取り/書き込みモードであるため、最初のセッションでの変更のみが保存されます。Citrix Profile ManagementプロファイルコンテナはCitrix Profile Management 2103以降でサポートされています。FSLogix Profile ContainerはCitrix Profile Management 2003以降でサポートされています。

FSLogix Profile Containerでこのポリシーを使用するには、以下の前提条件が満たされていることを確認してください。

- FSLogix Profile Container機能がインストールされ、有効になっていること。
- FSLogixでプロファイルタイプが **読み取り/書き込みプロファイルを試行し、読み取り専用にフォールバックする** に設定されていること。

ユーザーストアをレプリケートする

ユーザーストアへのパスポリシーで指定されたパスに加えて、ログオンおよびログオフごとにユーザーストアを複数のパスにレプリケートできます。セッション中に変更されたユーザーストアのファイルとフォルダーを同期するには、アクティブライトバックを有効にします。この機能は現在、完全なコンテナソリューションをサポートしていません。このポリシーを有効にすると、システムI/Oが増加し、ログオフが長くなる可能性があります。

ユーザーストアへの資格情報ベースのアクセスを有効にする

デフォルトでは、Citrix Profile Managementは現在のユーザーを偽装してユーザーストアにアクセスします。ユーザーストアへのアクセス時にProfile Managementが現在のユーザーを偽装しないようにする場合は、この機能を有効にしてください。現在のユーザーがアクセス権を持たないストレージリポジトリ（Azure Filesなど）にユーザーストアを配置できます。

Profile Managementがユーザーストアにアクセスできるようにするには、プロファイルストレージサーバーの資格情報をWorkspace Environment Management™ (WEM) またはWindows資格情報マネージャーに保存します。Profile Managementが実行される各マシンで同じ資格情報を構成する必要をなくすために、Workspace Environment Managementを使用することをお勧めします。Windows資格情報マネージャーを使用する場合は、ローカルシステムアカウントを使用して資格情報を安全に保存してください。

> **注：**

> NTFSアクセス許可が保持されるようにするには、プロファイル全体をプロファイルコンテナに配置する必要があります。

> この設定がここで構成されていない場合、.iniファイルの値が使用されます。この設定がここで、または.iniファイルで構成されていない場合、デフォルトで無効になります。

VHDX ファイルのストレージ パスをカスタマイズする

Profile Management は、プロファイル コンテナー、Outlook の検索インデックス ローミング、フォルダー ミラーリングの高速化といった VHDX ベースのポリシーを提供します。デフォルトでは、VHDX ファイルはユーザー ストアに保存されます。このポリシーを使用すると、それらを保存する別のパスを指定できます。

セッションで VHDX ディスクを自動的に再アタッチする

このポリシーを有効にすると、Profile Management は VHDX ベースのポリシーの高い安定性を確保します。デフォルトでは、このポリシーは有効になっています。

このポリシーが有効になっている場合、Profile Management は VHDX ベースのポリシーで使用されている VHDX ディスクを監視します。いずれかのディスクがデタッチされた場合、Profile Management はそのディスクを自動的に再アタッチします。

基本的なポリシー設定

このセクションには、Profile Management の基本的な構成に関連するポリシー設定が含まれています。

Profile Management を有効にする

デフォルトでは、展開を容易にするため、Profile Management はログオンまたはログオフを処理しません。Profile Management は、他のすべてのセットアップタスクを実行し、Citrix® ユーザープロファイルが環境でどのように動作するかをテストした後にのみ有効にしてください。

このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、Profile Management は Windows ユーザープロファイルを一切処理しません。

処理されるグループ

コンピューターローカルグループとドメイングループ（ローカル、グローバル、ユニバーサル）の両方を使用できます。ドメイングループは、DOMAIN NAME\GROUP NAME の形式で指定する必要があります。

このポリシーがここで構成されている場合、Profile Management はこれらのユーザーグループのメンバーのみを処理します。このポリシーが無効になっている場合、Profile Management はすべてのユーザーを処理します。このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、すべてのユーザーグループのメンバーが処理されます。

除外されるグループ

コンピューターローカルグループとドメイングループ（ローカル、グローバル、ユニバーサル）を使用して、特定のユーザープロファイルが処理されないようにすることができます。ドメイングループは、DOMAIN NAME\ GROUP NAME の形式で指定します。

この設定がここで構成されている場合、Profile Management はこれらのユーザーグループのメンバーを除外します。この設定が無効になっている場合、Profile Management はどのユーザーも除外しません。この設定がここで構成されていない場合、.ini ファイルの値が使用されます。この設定がここでも .ini ファイルでも構成されていない場合、どのグループのメンバーも除外されません。

ローカル管理者によるログオンの処理

BUILTIN\Administrators グループのメンバーによるログオンを処理するかどうかを指定します。このポリシーがマルチセッションオペレーティングシステム（Citrix Virtual Apps 環境など）で無効になっているか構成されていない場合、Profile Management は、ドメインユーザーによるログオンは処理する必要があるが、ローカル管理者によるログオンは処理しないと想定します。シングルセッションオペレーティングシステム（Citrix Virtual Desktops 環境など）では、ローカル管理者によるログオンが処理されます。このポリシーにより、ローカル管理者権限を持つドメインユーザー（通常、割り当てられた仮想デスクトップを持つ Citrix Virtual Desktops ユーザー）は、処理をバイパスしてログオンし、Profile Management で問題が発生しているデスクトップのトラブルシューティングを行うことができます。

注：ドメインユーザーのログオンは、通常、製品ライセンスへの準拠を確実にするために、グループメンバーシップによって課される制限の対象となる場合があります。 このポリシーが無効になっている場合、Profile Management はローカル管理者によるログオンを処理しません。このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、管理者は処理されません。

ユーザーストアへのパス

ユーザー設定（レジストリの変更と同期されたファイル）が保存されるディレクトリ（ユーザーストア）へのパスを設定します。

パスは次のいずれかです。

- 相対パス。ホームディレクトリ（通常、Active Directoryのユーザーの#homeDirectory#属性として構成されます）に対する相対パスである必要があります。
- UNCパス。通常、サーバー共有またはDFS名前空間を指定します。
- 無効または未構成。この場合、#homeDirectory#\Windowsの値が想定されます。

このポリシーでは、次の種類の変数を使用できます。

- パーセント記号で囲まれたシステム環境変数（例：%ProfVer%）。システム環境変数は通常、追加のセットアップが必要です。
- ハッシュで囲まれたActive Directoryユーザーオブジェクトの属性（例：#sAMAccountName#）。
- Profile Management変数。詳しくは、Profile Management変数の製品ドキュメントを参照してください。

`%username%`と`%userdomain%`を除き、ユーザー環境変数は使用できません。場所やユーザーなどを完全に定義するために、カスタム属性を作成することもできます。属性では大文字と小文字が区別されます。

例:

- `\\server\share#sAMAccountName#`は、ユーザー設定をUNCパス`\\server\share\JohnSmith`に保存します（現在のユーザーの#sAMAccountName#がJohnSmithに解決される場合）。
- `\\server\profiles$\%USERNAME%.%USERDOMAIN%\!CTX_OSNAME!!CTX_OSBITNESS!`は`\\server\profiles$\JohnSmith.DOMAINCONTROLLER1\Win8x64`に展開される場合があります。

重要：使用する属性または変数に関係なく、このポリシーがNTUSER.DATを含むフォルダーの1つ上のフォルダーに展開されることを確認してください。たとえば、このファイルが`\\server\profiles$\JohnSmith.Finance\Win8x64\UPM_Profile`に含まれる場合、ユーザー ストアへのパスを`\\server\profiles$\JohnSmith.Finance\Win8x64`に設定します（\UPM_Profileサブフォルダーではありません）。

ユーザー ストアへのパスを指定する際に変数を使用する方法について詳しくは、次のトピックを参照してください。

- 複数のファイルサーバーでCitrixユーザープロファイルを共有する
- OU内およびOU間でプロファイルを管理する
- Profile Managementによる高可用性と災害復旧

ユーザーストアへのパスが無効になっている場合、ユーザー設定はホームディレクトリのWindowsサブディレクトリに保存されます。

このポリシーが無効になっている場合、ユーザー設定はホームディレクトリのWindowsサブディレクトリに保存されます。このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここでも.iniファイルでも構成されていない場合、ホームドライブのWindowsディレクトリが使用されます。

ユーザーストアの移行

ユーザー設定（レジストリの変更と同期されたファイル）が以前に保存されていたフォルダーへのパス（以前使用していたユーザーストアパス）を指定します。

この設定が構成されている場合、以前のユーザーストアに保存されているユーザー設定は、「ユーザーストアへのパス」ポリシーで指定された現在のユーザーストアに移行されます。

パスは、絶対UNCパスまたはホームディレクトリに対する相対パスにすることができます。

どちらの場合も、パーセント記号で囲まれたシステム環境変数と、ハッシュ記号で囲まれたActive Directoryユーザーオブジェクトの属性という、次の種類の変数を使用できます。

例:

- フォルダー `Windows\%ProfileVer%` は、ユーザー設定をユーザーストアの `Windows\W2K3` というサブフォルダーに保存します（%ProfileVer% がW2K3に解決されるシステム環境変数である場合）。
- `\\server\share#SAMAccountName#` は、ユーザー設定をUNCパス `\\server\share\<JohnSmith>` に保存します（`#SAMAccountName#` が現在のユーザーに対してJohnSmithに解決される場合）。

パスでは、`%username%` と `%userdomain%` を除くユーザー環境変数を使用できます。

この設定が無効になっている場合、ユーザー設定は現在のユーザーストアに保存されます。

この設定がここで構成されていない場合、.iniファイルの対応する設定が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、ユーザー設定は現在のユーザーストアに保存されます。

アクティブライトバック

変更されたファイルとフォルダー（レジストリエントリを除く）は、ログオフする前にセッション中にユーザーストアに同期できます。

このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここでも.iniファイルでも構成されていない場合、有効になります。

オフラインプロファイルのサポート

このポリシーにより、プロファイルは可能な限り早い機会にユーザーストアと同期できます。これは、ローミングするラップトップまたはモバイルデバイスのユーザーを対象としています。ネットワーク接続が切断されても、再起動または休止状態の後でも、プロファイルはラップトップまたはデバイス上で無傷のままです。モバイルユーザーが作業するにつれて、プロファイルはローカルで更新され、ネットワーク接続が再確立されると最終的にユーザーストアと同期されます。

このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここでも.iniファイルでも構成されていない場合、オフラインプロファイルは無効になります。

アクティブライトバックレジストリ

「アクティブライトバック」と合わせてこのポリシーを使用してください。変更されたレジストリエントリは、セッション中にユーザーストアに同期できます。

ここでこの設定を構成しない場合、.iniファイルの値が使用されます。

ここでも.iniファイルでもこの設定を構成しない場合、アクティブライトバックレジストリは無効になります。

オフラインプロファイルのサポート

オフラインプロファイル機能を有効にします。この機能は、通常、サーバーやデスクトップではなく、ネットワークから頻繁に切断されるコンピューター、特にラップトップやモバイルデバイスを対象としています。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここでも.iniファイルでもこの設定が構成されていない場合、オフラインプロファイルのサポートは無効になります。

クロスプラットフォームポリシー設定

このセクションには、Profile Management のクロスプラットフォーム設定機能を構成するためのポリシー設定が含まれています。

クロスプラットフォーム設定を有効にする

既定では、展開を容易にするため、クロスプラットフォーム設定は無効になっています。この機能を十分に計画しテストした後にのみ、このポリシーを有効にして処理をオンにしてください。

ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、クロスプラットフォーム設定は適用されません。

クロスプラットフォーム設定ユーザーグループ

1つ以上のWindowsユーザーグループを入力します。たとえば、このポリシーを使用して、テストユーザーグループのプロファイルのみを処理できます。このポリシーが構成されている場合、Profile Managementのクロスプラットフォーム設定機能は、これらのユーザーグループのメンバーのみを処理します。このポリシーが無効になっている場合、この機能は、処理済みグループポリシーで指定されたすべてのユーザーを処理します。

ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、すべてのユーザーグループが処理されます。

クロスプラットフォーム定義へのパス

ダウンロードパッケージからコピーした定義ファイルのネットワーク上の場所を識別します。このパスはUNCパスである必要があります。ユーザーはこの場所への読み取りアクセス権を持ち、管理者は書き込みアクセス権を持っている必要があります。この場所は、Server Message Block (SMB) またはCommon Internet File System (CIFS) ファイル共有である必要があります。

ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、クロスプラットフォーム設定は適用されません。

クロスプラットフォーム設定ストアへのパス

ユーザーのクロスプラットフォーム設定が保存されるフォルダーであるクロスプラットフォーム設定ストアへのパスを設定します。ユーザーはこの領域への書き込みアクセス権を持っている必要があります。パスは絶対UNCパスまたはホームディレクトリに対する相対パスにすることができます。

この領域は、複数のプラットフォームで共有されるプロファイルデータが配置されるユーザーストアの共通領域です。ユーザーはこの領域への書き込みアクセス権を持っている必要があります。パスは絶対UNCパスまたはホームディレクトリに対する相対パスにすることができます。**Path to user store** と同じ変数を使用できます。

このポリシーが無効になっている場合、パス Windows\PM_CP が使用されます。ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、既定値が使用されます。

クロスプラットフォーム設定を作成するためのソース

このポリシーがそのプラットフォームのOUで有効になっている場合、プラットフォームをベースプラットフォームとして指定します。このポリシーは、ベースプラットフォームのプロファイルからクロスプラットフォーム設定ストアにデータを移行します。

各プラットフォーム独自のプロファイルセットは、別々のOUに保存されます。クロスプラットフォーム設定ストアのシードに使用するプラットフォームのプロファイルデータを決定する必要があります。これはベースプラットフォームと呼ばれます。クロスプラットフォーム設定ストアにデータのない定義ファイルが含まれている場合、またはシングルプラットフォームプロファイルのキャッシュデータがストア内の定義データよりも新しい場合、このポリシーを無効にしない限り、Profile Management はシングルプラットフォームプロファイルからストアにデータを移行します。

> **重要:**
>
> このポリシーが複数のOU、または複数のユーザーオブジェクトやマシンオブジェクトで有効になっている場合、最初にユーザーがログオンしたプラットフォームがベースプロファイルになります。 デフォルトでは、このポリシーは有効になっています。

ファイルシステム ポリシー設定

このセクションには、ユーザープロファイル内のどのファイルとディレクトリを、プロファイルがインストールされているシステムとユーザー ストアの間で同期するかを設定するポリシーが含まれています。

除外ポリシー設定

このセクションでは、ユーザープロファイル内のどのファイルとディレクトリを同期プロセスから除外するかを設定するためのポリシー設定について説明します。

除外リスト - ファイル

同期中に無視されるファイルのリスト。ファイル名はユーザープロファイル (%USERPROFILE%) に対する相対パスである必要があります。ワイルドカードはファイル名とフォルダー名でサポートされていますが、ファイル名のワイルドカードのみが再帰的に適用されます。

例:

- `Desktop\Desktop.ini` は `Desktop` フォルダー内のファイル `Desktop.ini` を無視します。

- `%USERPROFILE%*.tmp` はプロファイル全体で拡張子 `.tmp` を持つすべてのファイルを無視します。
- `AppData\Roaming\MyApp*.tmp` はプロファイルの一部で拡張子 `.tmp` を持つすべてのファイルを無視します。
- `Downloads*\a.txt` は `Downloads` フォルダーの直下のサブフォルダーにある `a.txt` を無視します。

このポリシーが無効になっている場合、ファイルは除外されません。このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、ファイルは除外されません。

デフォルトの除外リストを有効にする - ディレクトリ

同期中に無視されるディレクトリのデフォルトリスト。このポリシーを使用して、GPO 除外ディレクトリを手動で入力することなく指定できます。

このポリシーを無効にすると、Profile Management はデフォルトでどのディレクトリも除外しません。

このポリシーをここで構成しない場合、Profile Management は .ini ファイルの値を使用します。このポリシーをここでも .ini ファイルでも構成しない場合、Profile Management はデフォルトでどのディレクトリも除外しません。

除外リスト - ディレクトリ

同期中に無視されるフォルダーのリスト。フォルダー名はユーザープロファイル (%USERPROFILE%) に対する相対パスとして指定する必要があります。フォルダー名でのワイルドカードはサポートされていますが、再帰的には適用されません。

例:

- `Desktop` はユーザープロファイル内の `Desktop` フォルダーを無視します

このポリシーが無効になっている場合、フォルダーは除外されません。このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここでも.iniファイルでも構成されていない場合、フォルダーは除外されません。

ログオン除外チェック

この設定は、ユーザー ストア内のプロファイルに除外されたファイルまたはフォルダーが含まれている場合に、Profile Management が何を行うかを構成します。

この設定が無効になっているか、デフォルト値の「ログオン時に除外されたファイルまたはフォルダーを同期する」に設定されている場合、ユーザーがログオンすると、Profile Management はユーザー ストアからローカル プロファイルに除外されたファイルまたはフォルダーを同期します。

この設定が「ログオン時に除外されたファイルまたはフォルダーを無視する」に設定されている場合、ユーザーがログオンすると、Profile Management はユーザー ストア内の除外されたファイルまたはフォルダーを無視します。

この設定が「ログオン時に除外されたファイルまたはフォルダーを削除する」に設定されている場合、ユーザーがログオンすると、Profile Management はユーザー ストア内の除外されたファイルまたはフォルダーを削除します。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

この設定がここまたは .ini ファイルで構成されていない場合、ユーザーがログオンすると、除外されたファイルまたはフォルダーはユーザー ストアからローカル プロファイルに同期されます。

大容量ファイルの処理 - シンボリックリンクとして作成されるファイル

ログオンパフォーマンスを向上させ、サイズの大きいファイルを処理するために、Profile Management はこのリスト内のファイルをコピーする代わりにシンボリックリンクを作成します。

ファイルを参照するポリシーではワイルドカードを使用できます。例: `!ctx_localappdata!\Microsoft\Outlook*.OST`。

Microsoft Outlook のオフラインフォルダーファイル (`*.ost`) を処理するには、**Outlook** フォルダーが Profile Management の対象から除外されていないことを確認してください。

これらのファイルは、複数のセッションで同時にアクセスすることはできません。

同期ポリシー設定

同期セクションでは、ユーザープロファイル内のどのファイルとフォルダーを、プロファイルがインストールされているシステムとユーザー ストアの間で同期するかを指定するためのポリシー設定について説明します。

同期するディレクトリ

デフォルトでは、Profile Management は、ユーザープロファイルがインストールされているシステムとユーザー ストアの間でユーザープロファイルを同期します。同期からフォルダーを除外した場合、このポリシーを使用すると、除外されたフォルダーのサブフォルダーを同期に含めることができます。

このリストのパスは、ユーザープロファイルに対する相対パスである必要があります。フォルダー名でのワイルドカードはサポートされていますが、再帰的には適用されません。

このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、ユーザープロファイル内の除外されていないフォルダーのみが同期されます。

同期するファイル

デフォルトでは、Profile Management は、ユーザープロファイルがインストールされているシステムとユーザー ストアの間でユーザープロファイルを同期します。同期からフォルダーを除外した場合、このポリシーを使用すると、除外されたフォルダー内のファイルを同期に含めることができます。

このリストのパスは、ユーザープロファイルに対する相対パスである必要があります。ファイル名とフォルダー名でワイルドカードがサポートされていますが、ファイル名のワイルドカードのみが再帰的に適用されます。ワイルドカードをネストすることはできません。

例:

- `AppData\Local\Microsoft\Office\Access.qat` は、デフォルト構成で除外されているフォルダーの下にあるファイルを指定します。
- `AppData\Local\MyApp*.cfg` は、プロファイルフォルダー `AppData\Local\MyApp` およびそのサブフォルダー内の拡張子 `.cfg` を持つすべてのファイルを指定します。

このポリシーを無効にすると、有効にして空のリストを構成した場合と同じ効果があります。

このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、ユーザープロファイル内の除外されていないファイルのみが同期されます。

ミラーリングするフォルダー

このポリシーを使用すると、トランザクションフォルダー（参照フォルダーとも呼ばれる）に関連する問題を解決できます。そのフォルダーには、あるファイルが他のファイルを参照する相互依存ファイルが含まれています。

フォルダーのミラーリングにより、プロファイル管理はトランザクションフォルダーとその内容を単一のエンティティとして処理し、プロファイルの肥大化を防ぐことができます。たとえば、**Internet Explorer の Cookie** フォルダーをミラーリングして、Index.dat がインデックス化する Cookie と同期されるようにすることができます。このような状況では、「最後の書き込みが優先

されます」。そのため、複数のセッションで変更されたミラーリングされたフォルダー内のファイルは、最後の更新によって上書きされ、プロファイル変更が失われます。

たとえば、ユーザーがインターネットを閲覧しているときにIndex.datがCookieを参照する方法を考えてみましょう。ユーザーがそれぞれ異なるサーバーで2つのInternet Explorerセッションを持ち、各セッションで異なるサイトにアクセスした場合、各サイトからのCookieは適切なサーバーに追加されます。ユーザーが最初のセッションからログオフするとき（または、アクティブライトバック機能が構成されている場合はセッションの途中で）、2番目のセッションからのCookieが最初のセッションからのCookieを置き換える必要があります。しかし、実際にはそれらはマージされ、Index.dat内のCookieへの参照は古くなります。新しいセッションでのさらなる閲覧は、繰り返しのマージと肥大化したCookieフォルダーにつながります。

Cookieフォルダーをミラーリングすることで、ユーザーがログオフするたびに、Cookieを最後のセッションからのCookieで上書きすることにより、この問題が解決されます。これにより、Index.datは常に最新の状態に保たれます。

ここでこのポリシーが構成されていない場合、.ini ファイルの値が使用されます。ここで、または .ini ファイルでこのポリシーが構成されていない場合、フォルダーはミラーリングされません。

フォルダーのミラーリングを高速化する

このポリシーと**ミラーリングするフォルダー**ポリシーの両方を有効にすると、Profile ManagementはミラーリングされたフォルダーをVHDXベースの仮想ディスクに保存します。ログオン時に仮想ディスクをアタッチし、ログオフ時にデタッチします。このポリシーを有効にすると、ユーザーストアとローカルプロファイルの間でフォルダーをコピーする必要がなくなり、フォルダーのミラーリングが高速化されます。

フォルダーリダイレクトのポリシー設定

このセクションには、プロファイルに一般的に表示されるフォルダーを共有ネットワークの場所にリダイレクトするかどうかを指定するポリシー設定が含まれています。

管理者アクセスの許可

この設定により、管理者はユーザーのリダイレクトされたフォルダーの内容にアクセスできるようになります。

> **注：**
>
> この設定は、ドメインへの完全かつ無制限のアクセス権を持つ管理者に対して権限を付与します。

> デフォルトでは、この設定は無効になっており、ユーザーにはリダイレクトされたフォルダーの内容への排他的なアクセス権が付与されます。

ドメイン名を含める

この設定により、リダイレクトされたフォルダーに指定されたUNCパスの一部として、`%userdomain%` 環境変数を含めることができます。

デフォルトでは、この設定は無効になっており、リダイレクトされたフォルダーに指定されたUNCパスの一部として、`%userdomain%` 環境変数は含まれません。

AppData(Roaming) ポリシー設定

このセクションには、**AppData(Roaming)** フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

APPDATA(ROAMING) パス

この設定は、**AppData(Roaming)** フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

APPDATA(ROAMING) のリダイレクト設定

この設定は、**AppData(Roaming)** フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツはUNCパスにリダイレクトされます。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

連絡先ポリシー設定

このセクションには、**連絡先**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

連絡先パス

この設定は、**連絡先**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

連絡先のリダイレクト設定

この設定は、**連絡先**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツは UNC パスにリダイレクトされます。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

デスクトップポリシー設定

このセクションには、`Desktop` フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

デスクトップパス

この設定は、**デスクトップ**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

デスクトップのリダイレクト設定

この設定は、**デスクトップ**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツは UNC パスにリダイレクトされます。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

ドキュメントポリシー設定

このセクションには、**ドキュメント**フォルダーの内容を共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

ドキュメントパス

この設定は、**ドキュメント**フォルダー内のファイルがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

ドキュメントパス設定は、**ドキュメント**フォルダーへのファイルのリダイレクトだけでなく、**ミュージック**、**ピクチャ**、**ビデオ**フォルダーへのファイルのリダイレクトのためにも有効にする必要があります。

ドキュメントのリダイレクト設定

この設定は、**ドキュメント**フォルダーの内容をリダイレクトする方法を指定します。

デフォルトでは、内容は UNC パスにリダイレクトされます。

ドキュメントフォルダーの内容をリダイレクトする方法を制御するには、次のいずれかのオプションを選択します。

- 次の UNC パスにリダイレクトします。ドキュメントパスポリシー設定で指定された UNC パスにコンテンツをリダイレクトします。
- ユーザーのホームディレクトリにリダイレクトします。コンテンツをユーザーのホームディレクトリにリダイレクトします。これは通常、Active Directoryのユーザーの#homeDirectory#属性として構成されます。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

ダウンロードのポリシー設定

このセクションには、**ダウンロード**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

ダウンロードパス

この設定は、**ダウンロード**フォルダー内のファイルがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

ダウンロードのリダイレクト設定

この設定は、**ダウンロード**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツはUNCパスにリダイレクトされます。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

お気に入りポリシー設定

このセクションには、「**お気に入り**」フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

お気に入りパス

この設定は、「**お気に入り**」フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

この設定がここで構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

お気に入りのリダイレクト設定

この設定は、「**お気に入り**」フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツは UNC パスにリダイレクトされます。

この設定がここで構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

リンクポリシー設定

このセクションには、**リンク**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

リンクのパス

この設定は、**リンク**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

リンクのリダイレクト設定

この設定は、**リンク**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツは UNC パスにリダイレクトされます。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

音楽ポリシー設定

このセクションには、**Music**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

音楽パス

この設定は、**Music**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

音楽のリダイレクト設定

この設定は、**Music**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツはUNCパスにリダイレクトされます。

Musicフォルダーのコンテンツをリダイレクトする方法を制御するには、次のいずれかのオプションを選択します。

- 次のUNCパスにリダイレクトします。Musicパスポリシー設定で指定されたUNCパスにコンテンツをリダイレクトします。
- ドキュメントフォルダーを基準にリダイレクトします。ドキュメントフォルダーを基準としたフォルダーにコンテンツをリダイレクトします。

Documentsフォルダーを基準としたフォルダーにコンテンツをリダイレクトするには、**Documents path**設定を有効にする必要があります。

ここでこの設定が構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

画像ポリシー設定

このセクションには、**画像**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

画像パス

この設定は、**画像**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

画像のリダイレクト設定

この設定は、**画像**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツは UNC パスにリダイレクトされます。

画像フォルダーのコンテンツをリダイレクトする方法を制御するには、次のいずれかのオプションを選択します。

- 次の UNC パスにリダイレクトします。コンテンツを「画像パス」ポリシー設定で指定された UNC パスにリダイレクトします。
- ドキュメントフォルダーを基準にリダイレクトします。コンテンツをドキュメントフォルダーを基準としたフォルダーにリダイレクトします。

コンテンツを**ドキュメント**フォルダーを基準としたフォルダーにリダイレクトするには、**ドキュメントパス**設定を有効にする必要があります。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

Searchesポリシー設定

このセクションには、**Searches**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

SEARCHESのリダイレクト設定

この設定は、**Searches**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツはUNCパスにリダイレクトされます。

ここでこの設定が構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

SEARCHESパス

この設定は、**Searches**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

スタートメニューのポリシー設定

このセクションには、**スタートメニュー**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

スタートメニューのリダイレクト設定

この設定は、**スタートメニュー**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツはUNCパスにリダイレクトされます。

ここでこの設定が構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

スタートメニューのパス

この設定は、**スタートメニュー**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

ログポリシー設定

このセクションには、Profile Management のログ記録を構成するポリシー設定が含まれています。

Active Directory のアクション

この設定は、Active Directory で実行されるアクションの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここまたは.iniファイルで構成されていない場合、エラーと一般情報がログに記録されます。

一般情報

この設定は、一般情報の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここまたは.iniファイルで構成されていない場合、エラーと一般情報がログに記録されます。

一般的な警告

この設定は、一般的な警告の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログの有効化**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、エラーと一般情報がログに記録されます。

ログの有効化

この設定は、デバッグ（詳細ログ）モードでのProfile Managementログを有効または無効にします。デバッグモードでは、"%SystemRoot%\System32\Logfiles\UserProfileManager" にあるログファイルに詳細なステータス情報が記録されます。

デフォルトでは、この設定は無効になっており、エラーのみがログに記録されます。

Citrix®は、Profile Managementのトラブルシューティングを行う場合にのみ、この設定を有効にすることをお勧めします。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、エラーのみがログに記録されます。

ファイルシステムのアクション

この設定は、ファイルシステムで実行されたアクションの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログの有効化**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がここまたは.iniファイルで構成されていない場合、エラーと一般情報がログに記録されます。

ファイルシステム通知

この設定は、ファイルシステム通知の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする際は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がここまたは.iniファイルで構成されていない場合、エラーと一般情報がログに記録されます。

ログオフ

この設定は、ユーザーログオフの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする際は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がここまたは.iniファイルで構成されていない場合、エラーと一般情報がログに記録されます。

ログオン

この設定は、ユーザーログオンの詳細ログ記録を有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここで、または.iniファイルで構成されていない場合、エラーと一般情報がログに記録されます。

ログファイルの最大サイズ

この設定は、Profile Managementログファイルの最大許容サイズをバイト単位で指定します。

デフォルトでは、これは1048576バイト（1 MB）に設定されています。

十分なディスク容量がある場合は、このファイルのサイズを5 MB以上に増やすことをCitrixは推奨します。ログファイルが最大サイズを超えて大きくなった場合、既存のファイルのバックアップ（.bak）は削除され、ログファイルは.bakに名前変更され、新しいログファイルが作成されます。

ログファイルは`%SystemRoot%\System32\Logfiles\UserProfileManager`に作成されます。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここで、または.iniファイルで構成されていない場合、デフォルト値が使用されます。

ログファイルへのパス

この設定は、Profile Managementログファイルを保存するための代替パスを指定します。

デフォルトでは、この設定は無効になっており、ログファイルはデフォルトの場所である%SystemRoot%\System32\Logfiles\UserProfileManagerに保存されます。

パスは、ローカルドライブまたはリモートのネットワークベースドライブ (UNC パス) を指すことができます。リモートパスは大規模な分散環境で役立つ場合がありますが、大量のネットワークトラフィックを生成する可能性があり、ログファイルには不適切である可能性があります。永続的なハードドライブを持つプロビジョニングされた仮想マシンの場合は、そのドライブへのローカルパスを設定します。これにより、マシンが再起動してもログファイルが保持されます。永続的なハードドライブを持たない仮想マシンの場合、UNC パスを設定するとログファイルを保持できますが、マシンのシステムアカウントは UNC 共有への書き込みアクセス権を持っている必要があります。オフラインプロファイル機能によって管理されるラップトップには、ローカルパスを使用します。

ログファイルに UNC パスを使用する場合、Citrix は、承認されたユーザーまたはコンピューターアカウントのみが保存されたファイルにアクセスできるように、ログファイルフォルダーに適切なアクセス制御リストを適用することを推奨します。

ここでこの設定が構成されていない場合、.ini ファイルの値が使用されます。

ここまたは .ini ファイルでこの設定が構成されていない場合、デフォルトの場所 %SystemRoot%\System32\Logfiles\UserProfileManager が使用されます。

パーソナライズされたユーザー情報

この設定は、パーソナライズされたユーザー情報の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合、**ログの有効化**設定も有効になっていることを確認してください。

ここでこの設定が構成されていない場合、.ini ファイルの値が使用されます。

ここまたは .ini ファイルでこの設定が構成されていない場合、エラーと一般情報がログに記録されます。

ログオン時とログオフ時のポリシー値

この設定は、ユーザーがログオンおよびログオフするときのポリシー値の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合、**ログの有効化**設定も有効になっていることを確認してください。

ここでこの設定が構成されていない場合、.ini ファイルの値が使用されます。

この設定がここまたは.iniファイルで構成されていない場合、エラーと一般情報がログに記録されます。

レジストリアクション

この設定は、レジストリで実行されたアクションの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする際は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここまたは.iniファイルで構成されていない場合、エラーと一般情報がログに記録されます。

ログオフ時のレジストリの相違点

この設定は、ユーザーがログオフしたときのレジストリの相違点の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする際は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここまたは.iniファイルで構成されていない場合、エラーと一般情報がログに記録されます。

プロファイル処理ポリシー設定

このセクションには、Profile Management がユーザープロファイルを処理する方法を指定するポリシー設定が含まれています。

キャッシュされたプロファイルを削除するまでの遅延

この設定は、Profile Management がログオフ時にローカルにキャッシュされたプロファイルを削除するまでの遅延を、分単位で任意に延長する時間を指定します。

値が0の場合、ログオフプロセスの終了時にプロファイルがすぐに削除されます。Profile Management は毎分ログオフをチェックするため、値が60の場合、ユーザーがログオフしてから1〜2分後（最後のチェックがいつ行われたかによる）にプロファイルが削除されることが保証されます。ログオフ中にプロセスがファイルまたはユーザーレジストリハイブを開いたままにしていることがわかっている場合、遅延を延長することは有用です。大規模なプロファイルの場合、これによりログオフが高速化されることもあります。

デフォルトでは、これは0に設定されており、Profile Management はローカルにキャッシュされたプロファイルをすぐに削除します。

この設定を有効にする場合は、「ログオフ時にローカルにキャッシュされたプロファイルを削除する」も有効になっていることを確認してください。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここまたは.iniファイルでこの設定が構成されていない場合、プロファイルはすぐに削除されます。

ログオフ時にローカルにキャッシュされたプロファイルを削除する

この設定は、ユーザーがログオフした後にローカルにキャッシュされたプロファイルが削除されるかどうかを指定します。

この設定が有効になっている場合、ユーザーのローカルプロファイルキャッシュはログオフ後に削除されます。Citrix® は、ターミナルサーバーに対してこの設定を有効にすることを推奨しています。

デフォルトでは、この設定は無効になっており、ユーザーのローカルプロファイルキャッシュはログオフ後も保持されます。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここまたは.iniファイルでこの設定が構成されていない場合、キャッシュされたプロファイルは削除されません。

ローカルプロファイルの競合処理

この設定は、ユーザープロファイルがユーザー ストアとローカルの Windows ユーザープロファイル (Citrix ユーザープロファイルではない) の両方に存在する場合の Profile Management の動作を構成します。

デフォルトでは、Profile Management はローカルの Windows プロファイルを使用しますが、それを一切変更しません。

Profile Management の動作を制御するには、次のいずれかのオプションを選択します。

- ローカルプロファイルを使用する。Profile Management はローカルプロファイルを使用しますが、それを一切変更しません。
- ローカルプロファイルを削除する。Profile Management はローカルの Windows ユーザープロファイルを削除し、その後ユーザー ストアから Citrix ユーザープロファイルをインポートします。
- ローカルプロファイルの名前を変更する。Profile Management はローカルの Windows ユーザープロファイルの名前を変更し (バックアップ目的)、その後ユーザー ストアから Citrix ユーザープロファイルをインポートします。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がここで、または .ini ファイルで構成されていない場合、既存のローカルプロファイルが使用されます。

既存プロファイルの移行

この設定は、ユーザーがユーザー ストアに現在のプロファイルを持っていない場合に、ログオン中にユーザー ストアに移行されるプロファイルの種類を指定します。

ユーザーがユーザー ストアにプロファイルを持っていない場合、Profile Management はログオン中に既存のプロファイルを「オンザフライ」で移行できます。その後、ユーザー ストアプロファイルは、現在のセッションと、同じユーザー ストアへのパスで構成された他のすべてのセッションの両方で Profile Management によって使用されます。

デフォルトでは、ローカルプロファイルと移動プロファイルの両方がログオン中にユーザー ストアに移行されます。

ログオン中にユーザー ストアに移行されるプロファイルの種類を指定するには、次のいずれかのオプションを選択します。

- ローカルプロファイルと移動プロファイル
- ローカル
- ローミング
- なし (無効)

なしを選択すると、Profile Managementがインストールされていない環境であるかのように、システムは既存のWindowsメカニズムを使用してプロファイルを作成します。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、既存のローカルプロファイルとローミングプロファイルが移行されます。

既存のアプリケーションプロファイルの自動移行

この設定は、異なるオペレーティングシステム間で既存のアプリケーションプロファイルを自動的に移行するかどうかを有効または無効にします。アプリケーションプロファイルには、`AppData`フォルダー内のアプリケーションデータと、`HKEY_CURRENT_USER\SOFTWARE`の下のレジストリエントリの両方が含まれます。この設定は、異なるオペレーティングシステム間でアプリケーションプロファイルを移行したい場合に役立ちます。

たとえば、オペレーティングシステム（OS）をWindows 10バージョン1803からWindows 10バージョン1809にアップグレードするとします。この設定が有効になっている場合、各ユーザーが最初にログオンするときに、Profile Managementは既存のアプリケーション設定をWindows 10バージョン1809に自動的に移行します。その結果、`AppData`フォルダー内のアプリケーションデータとHKEY_CURRENT_USER\SOFTWAREの下のレジストリエントリが移行されます。

複数の既存のアプリケーションプロファイルがある場合、Profile Managementは次の優先順位で移行を実行します。

1. 同じOSタイプのプロファイル（シングルセッションOSからシングルセッションOS、マルチセッションOSからマルチセッションOS）。
2. 同じWindows OSファミリーのプロファイル（例：Windows 10からWindows 10、またはWindows Server 2016からWindows Server 2016）。

3. 以前のバージョンのOSのプロファイル（例：Windows 7からWindows 10、またはWindows Server 2012からWindows 2016）。
4. 最も近いOSのプロファイル。

注： ユーザーストアパスに変数「!CTX_OSNAME!」を含めることで、OSの短い名前を指定する必要があります。これにより、Profile Managementは既存のアプリケーションプロファイルを特定できます。

ここでこの設定が構成されていない場合、.iniファイルの設定が使用されます。

ここまたは.iniファイルでこの設定が構成されていない場合、デフォルトで無効になります。

テンプレートプロファイルへのパス

この設定は、Profile Managementがユーザープロファイルを作成するためのテンプレートとして使用するプロファイルへのパスを指定します。

指定されたパスは、NTUSER.DATレジストリファイルと、テンプレートプロファイルに必要なその他のフォルダーおよびファイルを含むフォルダーへの完全なパスである必要があります。

注: パスにNTUSER.DATを含めないでください。たとえば、ファイル`\\myservername\myprofiles\template\ntuser.dat`の場合、場所を`\\myservername\myprofiles\template`として設定します。

絶対パスを使用します。これはUNCパスまたはローカルマシン上のパスのいずれかです。後者を使用すると、たとえば、Citrix Provisioning™ Servicesイメージ上にテンプレートプロファイルを永続的に指定できます。相対パスはサポートされていません。

注: この設定は、Active Directory属性、システム環境変数、または`%USERNAME%`および`%USERDOMAIN%`変数の展開をサポートしていません。

デフォルトでは、この設定は無効になっており、新しいユーザープロファイルは、ユーザーが最初にログオンするデバイスのデフォルトユーザープロファイルから作成されます。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここまたは.iniファイルでこの設定が構成されていない場合、テンプレートは使用されません。

テンプレートプロファイルがローカルプロファイルを上書きする

この設定により、ユーザープロファイルの作成時にテンプレートプロファイルがローカルプロファイルを上書きできるようになります。

ユーザーにCitrixユーザープロファイルがないが、ローカルのWindowsユーザープロファイルが存在する場合、デフォルトではローカルプロファイルが使用されます（無効になっていない場合はユーザーストアに移行されます）。このポリシー設定を有効にすると、ユーザープロファイルの作成時に使用されるローカルプロファイルをテンプレートプロファイルが上書きできるようになります。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

この設定がここまたは.iniファイルで構成されていない場合、テンプレートは使用されません。

テンプレートプロファイルが移動プロファイルを上書きする

この設定により、ユーザープロファイルの作成時にテンプレートプロファイルが移動プロファイルを上書きできるようになります。

ユーザーがCitrixユーザープロファイルを持たず、移動Windowsユーザープロファイルが存在する場合、デフォルトでは移動プロファイルが使用されます（無効になっていない場合はユーザーストアに移行されます）。このポリシー設定を有効にすると、ユーザープロファイルの作成時に使用される移動プロファイルをテンプレートプロファイルが上書きできるようになります。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここまたは.iniファイルで構成されていない場合、テンプレートは使用されません。

すべてのログオンでCitrix必須プロファイルとして使用されるテンプレートプロファイル

この設定により、Profile Managementはテンプレートプロファイルをすべてのユーザープロファイルを作成するためのデフォルトプロファイルとして使用できるようになります。

デフォルトでは、この設定は無効になっており、新しいユーザープロファイルは、ユーザーが最初にログオンしたデバイスのデフォルトユーザープロファイルから作成されます。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここまたは.iniファイルで構成されていない場合、テンプレートは使用されません。

プロファイルコンテナのポリシー設定

プロファイルコンテナ

ユーザープロファイルに関連付けられた大きなフォルダーは、ログオンの遅延を引き起こします。Citrix Profile Managementは、プロファイルディスク（VHDXファイル）に含めるフォルダーを指定できるVHDXベースのプロファイルソリューションを提供します。このソリューションは、指定されたフォルダーをネットワークに保存されているプロファイルディスクにマッピングすることで、ログオン時間を短縮します。プロファイルコンテナは、ログオン時にこれらのフォルダーを含

むプロファイルディスクをアタッチするため、フォルダーのコピーをローカルプロファイルに保存する必要がなくなります。これにより、ログオン時間が短縮されます。

プロファイルコンテナのローカルキャッシュを有効にする

このポリシーは、Citrix Profile Managementプロファイルコンテナのローカルキャッシュサポートを有効にします。ポリシーが**有効**に設定されている場合、各ローカルプロファイルは、そのCitrix Profile Managementプロファイルコンテナのローカルキャッシュとして機能します。プロファイルストリーミングが使用されている場合、ローカルにキャッシュされたファイルはオンデマンドで作成されます。それ以外の場合は、ユーザーログオン時に作成されます。ローカルキャッシュ機能を使用するには、ユーザープロファイル全体をCitrix Profile Managementプロファイルコンテナに配置します。

プロファイルコンテナから除外するフォルダー

Citrix Profile Managementプロファイルコンテナから除外するフォルダーのリスト。

プロファイルコンテナに含めるフォルダー

親フォルダーが除外されている場合に、Citrix Profile Managementプロファイルコンテナに保持するフォルダーのリスト。

このリストのフォルダーは、除外されたフォルダーのサブフォルダーである必要があります。そうでない場合、この設定は機能しません。

プロファイルコンテナに含めるファイル

Citrix Profile Managementプロファイルコンテナに含めるファイルのリスト。

このリストのファイルは、除外されたフォルダー内にある必要があります。そうでない場合、この設定は機能しません。

プロファイルコンテナから除外するファイル

Citrix Profile Managementプロファイルコンテナから除外するファイルのリスト。

レジストリポリシー設定

このセクションには、Profile Management の処理から含める、または除外するレジストリキーを指定するポリシー設定が含まれています。

除外リスト

ログオフ時に無視されるHKCUハイブ内のレジストリキーのリスト。

例: Software\Policies

このポリシーが無効になっている場合、レジストリキーは除外されません。ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、レジストリキーは除外されません。

包含リスト

ログオフ時に処理されるHKCUハイブ内のレジストリキーのリスト。

例: Software\Adobe。

このポリシーが有効になっている場合、このリストにあるキーのみが処理されます。このポリシーが無効になっている場合、HKCUハイブ全体が処理されます。ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、HKCUのすべてが処理されます。

デフォルトの除外リストを有効にする - Profile Management 5.5

ユーザープロファイルに同期されないHKCUハイブ内のレジストリキーのデフォルトリスト。このポリシーを使用して、GPO除外ファイルを手動で入力することなく指定できます。

このポリシーを無効にすると、Profile Management はデフォルトでレジストリキーを除外しません。ここでこのポリシーを構成しない場合、Profile Management は .ini ファイルの値を使用します。ここで、または .ini ファイルでこのポリシーを構成しない場合、Profile Management はデフォルトでレジストリキーを除外しません。

NTUSER.DATのバックアップ

NTUSER.DAT の最後に正常に認識されたコピーのバックアップと、破損時のロールバックを有効にします。

ここでこのポリシーを構成しない場合、Profile Management は .ini ファイルの値を使用します。ここで、または .ini ファイルでこのポリシーを構成しない場合、Profile Management は NTUSER.DAT をバックアップしません。

ストリーム配信ユーザープロファイルポリシー設定

このセクションには、Profile Management がストリーム配信ユーザープロファイルを処理する方法を指定するポリシー設定が含まれています。

常にキャッシュ

この設定は、ユーザーがログオンした直後にProfile Managementがストリーミングされたファイルをキャッシュするかどうかを指定します。ユーザーがログオンした後にファイルをキャッシュすると、ネットワーク帯域幅が節約され、ユーザーエクスペリエンスが向上します。

この設定は、**プロファイルストリーミング**設定と組み合わせて使用します。

デフォルトでは、この設定は無効になっており、ユーザーがログオンした直後にストリーミングされたファイルはキャッシュされません。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

この設定がここまたは.iniファイルで構成されていない場合、無効になります。

常にキャッシュするサイズ

この設定は、ストリーム配信されるファイルのサイズの下限を MB 単位で指定します。Profile Management は、このサイズ以上のファイルを、ユーザーのログオン後できるだけ早くキャッシュします。

デフォルトでは、値は 0 (ゼロ) に設定されており、プロファイル全体をキャッシュする機能が使用されます。プロファイル全体をキャッシュする機能が有効になっている場合、Profile Management は、ユーザーのログオン後、ユーザーストア内のすべてのプロファイルコンテンツをバックグラウンドタスクとしてフェッチします。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

この設定がここまたは.iniファイルで構成されていない場合、無効になります。

プロファイルストリーミング

この設定は、Citrix®ストリーミングユーザープロファイル機能を有効または無効にします。有効にすると、プロファイルに含まれるファイルとフォルダーは、ユーザーがログオンした後にアクセスされた場合にのみ、ユーザーストアからローカルコンピューターにフェッチされます。レジストリエントリと保留領域のファイルはすぐにフェッチされます。

デフォルトでは、プロファイルストリーミングは無効になっています。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

この設定がここまたは.iniファイルで構成されていない場合、無効になります。

ストリーム配信ユーザープロファイルグループ

この設定は、Windows ユーザーグループに基づいて、OU 内のどのユーザープロファイルをストリーム配信するかを指定します。

有効にすると、指定されたユーザーグループ内のユーザープロファイルのみがストリーミングされます。その他のすべてのユーザープロファイルは通常どおり処理されます。

デフォルトでは、この設定は無効になっており、OU内のすべてのユーザープロファイルは通常どおり処理されます。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

この設定がここまたは.iniファイルで構成されていない場合、すべてのユーザープロファイルが処理されます。

プロファイルストリーミング除外を有効にするには

プロファイルストリーミング除外が有効になっている場合、Profile Managementは除外リスト内のフォルダーをストリーミングせず、ユーザーがログオンすると、すべてのフォルダーがユーザーストアからローカルコンピューターにすぐにフェッチされます。

詳細については、「ユーザープロファイルのストリーム」を参照してください。

ペンディングエリアロックファイルのタイムアウト

この設定は、サーバーが応答しなくなったときにユーザーストアがロックされたままになる場合に、保留領域からユーザーストアにユーザーのファイルが書き戻されるまでの日数を指定します。これにより、保留領域の肥大化を防ぎ、ユーザーストアに常に最新のファイルが含まれるようにします。

デフォルトでは、1日（1）に設定されています。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

この設定がここで、または.iniファイルで構成されていない場合、デフォルト値が使用されます。

ユーザーパーソナライゼーションレイヤーポリシー設定

Virtual Delivery Agent 内でユーザーレイヤーのマウントを有効にするには、構成パラメーターを使用して以下を指定します。

- ネットワーク上のどこでユーザーレイヤーにアクセスするか。
- 新しいユーザーレイヤーディスクがどのくらい大きくなるか。

そのため、利用可能なポリシーのリストには、次の2つのポリシーが表示されます。

- ユーザーレイヤーリポジトリパス - 「値」フィールドに「\\サーバー名またはアドレス\フォルダー名」の形式でパスを入力します。
- ユーザーレイヤーサイズ (GB) - デフォルトのユーザーレイヤーサイズである10 GBは、推奨される最小値です。ユーザーレイヤーは、使用されるスペースに応じて設定されたサイズまで拡

張するシンプロビジョニングディスクです。ユーザーレイヤーのサイズが小さくなることはありません。

> **注：**
>
> ユーザーレイヤーサイズを増やすと、新しいユーザーレイヤーに影響を与え、既存のユーザーレイヤーを拡張します。レイヤーサイズを減らすと、新しいユーザーレイヤーにのみ影響します。既存のユーザーレイヤーのサイズが小さくなることはありません。

詳細については、「ユーザーパーソナライゼーションレイヤー」を参照してください。

Virtual Delivery Agent ポリシー設定

Virtual Delivery Agent (VDA) セクションには、VDA とサイトのコントローラー間の通信を制御するポリシー設定が含まれています。

重要: 自動更新機能を使用しない場合、VDA は Delivery Controller™ に登録するために、これらの設定によって提供される情報を必要とします。この情報は登録に必要であるため、VDA のインストール中にこの情報を提供しない限り、グループポリシーエディターを使用して以下の設定を構成する必要があります。

- コントローラー登録 IPv6 ネットマスク
- コントローラー登録ポート
- コントローラー SID
- コントローラー
- IPv6 コントローラー登録のみを使用
- サイト GUID

コントローラー登録 IPv6 ネットマスク

このポリシー設定により、管理者はVDAを優先サブネットのみに制限できます（登録されている場合はグローバルIPではなく）。この設定は、VDAが登録するIPv6アドレスとネットワークを指定します。VDAは、指定されたネットマスクに一致する最初のアドレスにのみ登録されます。この設定は、「IPv6コントローラー登録ポリシー設定のみを使用する」が有効な場合にのみ有効です。

デフォルトでは、この設定は空白です。

コントローラー登録ポート

この設定は、「コントローラーの自動更新を有効にする」設定が無効になっている場合にのみ使用してください。

この設定は、レジストリベースの登録を使用する際に、VDAがコントローラーに登録するために使用するTCP/IPポート番号を指定します。

デフォルトでは、ポート番号は80に設定されています。

コントローラーSID

この設定は、「コントローラーの自動更新を有効にする」設定が無効になっている場合にのみ使用してください。

この設定は、レジストリベースの登録を使用する際に、VDAがコントローラーに登録するために使用するコントローラーのセキュリティ識別子（SID）のスペース区切りリストを指定します。これはオプションの設定であり、登録に使用されるコントローラーのリストを制限するために「コントローラー」設定と組み合わせて使用できます。

デフォルトでは、この設定は空白です。

コントローラー

この設定は、「コントローラーの自動更新を有効にする」設定が無効になっている場合にのみ使用してください。

この設定は、レジストリベースの登録を使用する際に、VDAがコントローラーに登録するために使用するコントローラーの完全修飾ドメイン名（FQDN）のスペース区切りリストを指定します。これはオプションの設定であり、「コントローラーSID」設定と組み合わせて使用できます。

デフォルトでは、この設定は空白です。

コントローラーの自動更新を有効にする

この設定により、VDAはインストール後にコントローラーに自動的に登録できるようになります。

VDAが登録されると、登録先のコントローラーは現在のコントローラーFQDNとSIDのリストをVDAに送信します。VDAはこのリストを永続ストレージに書き込みます。各コントローラーは、90分ごとにサイトデータベースでコントローラー情報をチェックします。前回のチェック以降にコントローラーが追加または削除された場合、またはポリシー変更が発生した場合は、コント

ローラーは更新されたリストを登録済みのVDAに送信します。VDAは、受信した最新のリストにあるすべてのコントローラーからの接続を受け入れます。

デフォルトでは、この設定は有効になっています。

IPv6コントローラー登録のみを使用

この設定は、VDAがControllerに登録するために使用するアドレス形式を制御します。

- 有効にすると、VDAはマシンのIPv6アドレスを使用してControllerに登録します。VDAがControllerと通信する場合、次のアドレス順序を使用します: グローバルIPアドレス、ユニークローカルアドレス (ULA)、リンクローカルアドレス (他のIPv6アドレスが利用できない場合)。
- 無効にすると、VDAはマシンのIPv4アドレスを使用してControllerに登録し、通信します。

デフォルトでは、この設定は無効になっています。

サイトGUID

この設定は、「コントローラーの自動更新を有効にする」設定が無効になっている場合にのみ使用してください。

この設定は、Active Directoryベースの登録を使用する際に、VDAがコントローラーに登録するために使用するサイトのグローバル一意識別子（GUID）を指定します。

デフォルトでは、この設定は空白です。

HDX™ 3D Pro ポリシー設定

HDX 3D Proセクションには、ユーザー向けに画質構成ツールを有効化および構成するためのポリシー設定が含まれています。このツールを使用すると、ユーザーは画質と応答性のバランスをリアルタイムで調整することによって、利用可能な帯域幅の使用を最適化できます。

ロスレスを有効にする

この設定は、ユーザーが画質構成ツールを使用してロスレス圧縮を有効または無効にできるかどうかを指定します。デフォルトでは、ユーザーにロスレス圧縮を有効にするオプションは提供されません。

ユーザーがロスレス圧縮を有効にすると、画質はイメージ構成ツールで利用可能な最大値に自動的に設定されます。デフォルトでは、ユーザーデバイスとホストコンピューターの機能に応じて、GPUベースまたはCPUベースの圧縮のいずれかを使用できます。

HDX 3D Pro 品質設定

この設定は、画質構成ツールでユーザーが利用できる画質調整の範囲を定義する最小値と最大値を指定します。

画質の値は0から100（両端を含む）の間で指定します。最大値は最小値以上である必要があります。

監視ポリシー設定

「監視」セクションには、プロセス、リソース監視、およびアプリケーション障害監視のポリシー設定が含まれています。

これらのポリシーのスコープは、サイト、デリバリーグループ、デリバリーグループの種類、組織単位、およびタグに基づいて定義できます。

プロセスおよびリソース監視のポリシー

CPU、メモリ、プロセスの各データポイントはVDAから収集され、監視データベースに保存されます。VDAからデータポイントを送信するとネットワーク帯域幅を消費し、それらを保存すると監視データベースでかなりのスペースを消費します。特定のスコープ（たとえば、特定のデリバリーグループや組織単位）のリソースデータまたはプロセスデータ、あるいはその両方を監視したくない場合は、ポリシーを無効にすることをお勧めします。

プロセス監視を有効にする

この設定を有効にすると、VDAがインストールされているマシンで実行されているプロセスの監視が可能になります。CPUやメモリ使用量などの統計情報は監視サービスに送信されます。これらの統計情報は、Directorでのリアルタイム通知および履歴レポートに使用されます。

この設定のデフォルトは無効です。

リソース監視を有効にする

この設定を有効にすると、VDAがインストールされているマシンで重要なパフォーマンスカウンターの監視が可能になります。統計情報（CPUおよびメモリ使用量、IOPS、ディスク待機時間データなど）は監視サービスに送信されます。これらの統計情報は、Directorでのリアルタイム通知および履歴レポートに使用されます。

この設定のデフォルトは有効です。

スケーラビリティ

CPUおよびメモリデータは、各VDAから5分間隔でデータベースにプッシュされます。プロセスデータ（有効な場合）は10分間隔でデータベースにプッシュされます。IOPSおよびディスク待機時間データは1時間間隔でデータベースにプッシュされます。

CPUとメモリデータ

CPUとメモリデータは、デフォルトで**有効**です。データ保持期間の値は次のとおりです (Platinumライセンス):

データ粒度	日数
5分データ	1日
10分データ	7日
時間データ	30日
日次データ	90日

IOPSとディスク待機時間データ

IOPSとディスク待機時間データは、デフォルトで**有効**です。データ保持期間の値は次のとおりです (Platinumライセンス):

データ粒度	日数
時間データ	3日間
日次データ	90日間

データ保持設定を使用すると、1つのVDAのCPU、メモリ、IOPS、およびディスク待機時間データを1年間保存するために、約276 KBのディスクスペースが必要になります。

マシン数	必要なストレージ容量（概算）
1	276 KB
1K	270 MB
40K	10.6 GB

プロセスデータ

プロセスデータはデフォルトで**無効**です。必要に応じて、一部のマシンでプロセスデータを有効にすることをお勧めします。プロセスデータのデフォルトのデータ保持設定は次のとおりです。

データ粒度	日数
10分データ	1日
1時間データ	7日

プロセスデータがデフォルトの保持設定で有効になっている場合、プロセスデータは1年間でVDAあたり約1.5 MB、ターミナルサービスVDA (TS VDA) あたり3 MBを消費します。

マシン数	必要なストレージの目安 VDA	必要なストレージの目安 TS VDA
1	1.5 MB	3 MB
1K	1.5 GB	3 GB

注：

以前に提示された数値には、インデックス領域は含まれていません。また、すべての計算は概算であり、展開によって異なります。

オプションの構成

デフォルトの保持設定は、必要に応じて変更できます。ただし、これにより追加のストレージが消費されます。以下の設定を有効にすることで、プロセス使用率データの精度を高めることができます。有効にできる構成は次のとおりです。

ENABLEMINUTELEVELGRANULARITYPROCESSUTILIZATION

ENABLEDAYLEVELGRANULARITYPROCESSUTILIZATION

これらの構成は、監視PowerShellコマンドレットから有効にできます: Set-MonitorConfiguration

アプリケーション障害監視のポリシー

デフォルトでは、**アプリケーション障害**タブには、マルチセッションOS VDAからのアプリケーション障害のみが表示されます。アプリケーション障害監視の設定は、以下の監視ポリシーで変更できます。

アプリケーション障害の監視を有効にする

この設定を使用して、アプリケーション障害監視を構成し、アプリケーションエラーまたは障害（クラッシュおよび未処理の例外）、あるいはその両方を監視します。 **値**を**None**に設定すると、

アプリケーション障害監視が無効になります。 この設定のデフォルトは「アプリケーション障害のみ」です。

シングルセッションOS VDAでのアプリケーション障害の監視を有効にする

デフォルトでは、マルチセッションOS VDAでホストされているアプリケーションからの障害のみが監視されます。シングルセッションOS VDAを監視するには、ポリシーを**Allowed**に設定します。 この設定のデフォルトは**Prohibited**です。

障害監視から除外されるアプリケーションのリスト

障害監視の対象としないアプリケーションのリストを指定します。 デフォルトでは、このリストは空です。

Performance Analyticsのデータ収集ポリシー

PERFORMANCE ANALYTICSのVDAデータ収集

このポリシーを使用して、Performance AnalyticsのためにVDAのパフォーマンス関連メトリックを収集するモニターサービスを有効または無効にします。デフォルトでは、ポリシーは**許可**されています。VDAからのデータ収集を停止するには、ポリシーを**禁止**に設定します。

ストレージ計画のヒント

グループポリシー。リソースデータまたはプロセスデータの監視に関心がない場合は、グループポリシーを使用してそのいずれかまたは両方をオフにすることができます。詳細については、「ポリシーの作成」の「グループポリシー」セクションを参照してください。

データグルーミング。デフォルトのデータ保持設定を変更して、データを早期にグルーミングし、ストレージスペースを解放できます。グルーミング設定について詳しくは、「API を使用したデータアクセス」の「データの粒度と保持」を参照してください。

仮想IPポリシー設定

> **重要:**
>
> Windows 10 Enterprise マルチセッションは、リモートデスクトップIP仮想化 (仮想IP) をサポートしていません。また、弊社はWindows 10 Enterprise マルチセッションで仮想IPも仮想ループバックもサポートしていません。

仮想IPセクションには、セッションが独自の仮想ループバックアドレスを持つかどうかを制御するポリシー設定が含まれています。

仮想IPループバックのサポート

この設定が有効な場合、各セッションは独自の仮想ループバックアドレスを持ちます。無効な場合、セッションは個別のループバックアドレスを持ちません。

デフォルトでは、この設定は無効になっています。

仮想IP仮想ループバックプログラムリスト

この設定は、仮想ループバックアドレスを使用できるアプリケーション実行可能ファイルを指定します。プログラムをリストに追加する際は、実行可能ファイル名のみを指定してください。完全なパスを指定する必要はありません。

デフォルトでは、実行可能ファイルは指定されていません。

レジストリを使用してCOMポートおよびLPTポートリダイレクト設定を構成する

VDAバージョン7.0から7.8では、COMポートとLPTポートの設定はレジストリを使用してのみ構成できます。VDAバージョン7.0より前、およびVDAバージョン7.9以降では、これらの設定はStudioで構成できます。詳細については、「ポートリダイレクトポリシー設定」および「帯域幅ポリシー設定」を参照してください。

COMポートおよびLPTポートリダイレクトのポリシー設定は、VDAイメージまたはマシン上のHKLM\Software\Citrix\GroupPolicy\Defaults\Deprecatedにあります。

COMポートおよびLPTポートリダイレクトを有効にするには、次のようにREG_DWORD型の新しいレジストリキーを追加します。

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

レジストリキー	説明	許可される値
AllowComPortRedirection	COMポートリダイレクトを許可または禁止する	1 (許可) または 0 (禁止)
LimitComBw	COMポートリダイレクトチャネルの帯域幅制限	数値

レジストリキー	説明	許可される値
LimitComBWPercent	COMポートリダイレクトチャネルの帯域幅制限（セッションの総帯域幅に対する割合）	0から100までの数値
AutoConnectClientComPorts	ユーザーデバイスからCOMポートを自動的に接続する	1 (許可) または 0 (禁止)
AllowLptPortRedirection	LPTポートリダイレクトを許可または禁止する	1 (許可) または 0 (禁止)
LimitLptBw	LPTポートリダイレクトチャネルの帯域幅制限	数値
LimitLptBwPercent	LPTポートリダイレクトチャネルの帯域幅制限（セッション全体の帯域幅に対する割合）	0から100までの数値
AutoConnectClientLptPorts	ユーザーデバイスからLPTポートを自動的に接続する	1 (許可) または 0 (禁止)

これらの設定を構成した後、マシンカタログを新しいマスターイメージまたは更新された物理マシンを使用するように変更します。ユーザーが次回ログオフしたときに、デスクトップは新しい設定で更新されます。

Configuration Manager 2012向けコネクタのポリシー設定

Configuration Manager 2012向けコネクタのセクションには、Citrix Connector 7.5エージェントを構成するためのポリシー設定が含まれています。

> **重要:**

> 警告、ログオフ、および再起動メッセージポリシーは、手動またはProvisioning Servicesによって管理されるマルチセッションOSマシンカタログへの展開にのみ適用されます。これらのマシンカタログの場合、コネクタサービスは、保留中のアプリケーションのインストールまたはソフトウェアアップデートがある場合にユーザーに警告します。

> MCSによって管理されるカタログの場合、Studioを使用してユーザーに通知します。手動で管理されるシングルセッションOSカタログの場合、Configuration Managerを使用してユーザーに通知します。Provisioning Servicesによって管理されるシングルセッションOSカタログの場合、Provisioning Servicesを使用してユーザーに通知します。

警告頻度間隔

この設定は、ユーザーへの警告メッセージの表示間隔を定義します。

間隔はddd.hh:mm:ssの形式で設定されます。ここで、:

- dddは日数で、オプションのパラメーターであり、0～999の範囲です。
- hhは時間で、0～23の範囲です。
- mmは分で、0～59の範囲です。
- ssは秒で、0～59の範囲です。

デフォルトでは、間隔設定は1時間（01:00:00）です。

警告メッセージボックスの本文

この設定には、今後のソフトウェアアップデートまたはログオフを必要とするメンテナンスについてユーザーに通知するメッセージの編集可能なテキストが含まれています。

デフォルトでは、メッセージは次のとおりです: {TIMESTAMP} 作業を保存してください。サーバーは{TIMELEFT}後にメンテナンスのためオフラインになります。

警告メッセージボックスのタイトル

この設定には、ユーザーへの警告メッセージのタイトルバーの編集可能なテキストが含まれています。

デフォルトでは、タイトルは「Upcoming Maintenance」です。

警告期間

この設定は、メンテナンスのどれくらい前に警告メッセージが最初に表示されるかを定義します。

時刻はddd.hh:mm:ssの形式で設定されます。ここで、:

- dddは日数で、オプションのパラメーターであり、範囲は0～999です。
- hhは時間で、範囲は0～23です。
- mmは分で、範囲は0～59です。

- ssは秒で、範囲は0〜59です。

デフォルトでは、設定は16時間（16:00:00）であり、最初の警告メッセージがメンテナンスの約16時間前に表示されることを示します。

最終強制ログオフメッセージボックスの本文

この設定には、強制ログオフが開始されたことをユーザーに警告するメッセージの編集可能なテキストが含まれています。

デフォルトでは、メッセージは「The server is currently going offline for maintenance」です。

最終強制ログオフメッセージボックスのタイトル

この設定には、最終的な強制ログオフメッセージのタイトルバーの編集可能なテキストが含まれています。

デフォルトでは、タイトルは「ITスタッフからの通知」です。

強制ログオフ猶予期間

この設定は、ユーザーにログオフを通知してから、保留中のメンテナンスを処理するための強制ログオフが実行されるまでの期間を定義します。

時間はddd.hh:mm:ssの形式で設定され、ここで:

- dddは日数で、オプションのパラメーターであり、範囲は0〜999です。
- hhは時間で、範囲は0〜23です。
- mmは分で、範囲は0〜59です。
- ssは秒で、範囲は0〜59です。

デフォルトでは、強制ログオフ猶予期間の設定は5分（00:05:00）です。

強制ログオフメッセージボックスの本文

この設定には、強制ログオフが開始される前に、作業を保存してログオフするようユーザーに伝えるメッセージの編集可能なテキストが含まれています。

デフォルトでは、メッセージには次の内容が含まれています: {TIMESTAMP} 作業を保存してログオフしてください。サーバーは{TIMELEFT}後にメンテナンスのためオフラインになります。

強制ログオフメッセージボックスのタイトル

この設定には、強制ログオフメッセージのタイトルバーの編集可能なテキストが含まれています。

デフォルトでは、タイトルは「ITスタッフからの通知」です。

イメージ管理モード

Connectorエージェントは、Provisioning ServicesまたはMCSによって管理されているマシンのクローン上で実行されているかどうかを自動的に検出します。エージェントは、イメージ管理されたクローンでのConfiguration Managerの更新をブロックし、カタログのマスターイメージに更新を自動的にインストールします。

マスターイメージが更新された後、Studioを使用してMCSカタログクローンの再起動をオーケストレーションします。Connectorエージェントは、Configuration Managerのメンテナンスウィンドウ中にPVSカタログクローンの再起動を自動的にオーケストレーションします。この動作を上書きして、Configuration Managerによってカタログクローンにソフトウェアがインストールされるようにするには、イメージ管理モードを「無効」に変更します。

再起動メッセージボックスの本文

この設定には、サーバーが再起動されるときにユーザーに通知するメッセージの編集可能なテキストが含まれています。

デフォルトでは、メッセージは「サーバーは現在メンテナンスのためオフラインになります。」です。

エージェントタスクを実行する通常の時間間隔

この設定は、Citrix Connector™エージェントタスクが実行される頻度を決定します。

時間はddd.hh:mm:ssの形式で設定されます。ここで、:

- dddは日数で、オプションのパラメーターであり、範囲は0〜999です。
- hhは時間で、範囲は0〜23です。
- mmは分で、範囲は0〜59です。
- ssは秒で、範囲は0〜59です。

デフォルトでは、通常の時間間隔設定は5分（00:05:00）です。

管理

Citrix Virtual Apps and Desktops™ サイトの管理には、さまざまな項目とタスクが含まれます。

ライセンス

サイトを作成するときは、Citrix License Server への有効な接続が必要です。後で、Studio から、ライセンスの追加、ライセンスの種類やモデルの変更、ライセンス管理者の管理など、いくつかのライセンス関連タスクを実行できます。Studio から License Administration Console にアクセスすることもできます。

アプリケーション

デリバリーグループ、およびオプションでアプリケーショングループ内のアプリケーションを管理します。

ゾーン

地理的に分散した展開では、ゾーンを使用してアプリケーションとデスクトップをエンドユーザーの近くに配置し、パフォーマンスを向上させることができます。サイトをインストールして構成すると、すべてのコントローラー、マシンカタログ、およびホスト接続は1つのプライマリゾーンに配置されます。後で、Studio を使用して、これらの項目を含むサテライトゾーンを作成できます。サイトに複数のゾーンがある場合、新しく作成されたマシンカタログ、ホスト接続、または追加されたコントローラーをどのゾーンに配置するかを指定できます。ゾーン間で項目を移動することもできます。

接続とリソース

アプリケーションとデスクトップをユーザーに提供するマシンをホストするためにハイパーバイザーまたはその他のサービスを使用している場合、サイトを作成するときに、そのハイパーバイザーまたはその他のサービスへの最初の接続を作成します。その接続のストレージとネットワークの詳細は、そのリソースを構成します。後で、その接続とそのリソースを変更したり、さらに接続を作成したりできます。構成済みの接続を使用するマシンを管理することもできます。

ローカルホストキャッシュ

ローカルホストキャッシュにより、Delivery Controller™ とサイトデータベース間の接続が失敗した場合でも、サイトでの接続ブローカー操作を続行できます。

仮想IPと仮想ループバック

Microsoft の仮想IPアドレス機能は、公開アプリケーションにセッションごとに一意の動的に割り当てられたIPアドレスを提供します。Citrix の仮想ループバック機能を使用すると、localhost との通信に依存するアプリケーションを、localhost 範囲内の一意の仮想ループバックアドレスを使用するように構成できます。

デリバリーコントローラー

この記事では、サイトへのControllerの追加と削除に関する考慮事項と手順について説明します。また、Controllerを別のゾーンまたはサイトに移動する方法、およびVDAを別のサイトに移動する方法についても説明します。

ControllerへのVDA登録

VDAがアプリケーションとデスクトップの配信を支援するには、Controllerに登録（通信を確立）する必要があります。Controllerのアドレスはいくつかの方法で指定でき、それについてはこの記事で説明します。サイトでControllerが追加、移動、削除される際に、VDAが最新の情報を持っていることが重要です。

セッション

セッションアクティビティを維持することは、最高のユーザーエクスペリエンスを提供するために不可欠です。いくつかの機能により、セッションの信頼性を最適化し、不便さ、ダウンタイム、生産性の損失を軽減できます。

- セッションの信頼性
- クライアントの自動再接続
- ICA®キープアライブ
- ワークスペースコントロール
- セッションローミング

Studioでの検索の使用

Studioでマシン、セッション、マシンカタログ、アプリケーション、またはデリバリーグループに関する情報を表示したい場合は、柔軟な検索機能を使用します。

タグ

タグを使用して、マシン、アプリケーション、グループ、ポリシーなどのアイテムを識別します。その後、特定のタグを持つアイテムに適用されるように特定の操作を調整できます。

IPv4/IPv6

Citrix Virtual Apps and Desktops は、純粋な IPv4、純粋な IPv6、および IPv4 と IPv6 の重複するネットワークを使用するデュアルスタック展開をサポートしています。この記事では、これらの展開について説明し、図解します。また、IPv4 または IPv6 の使用を制御する Citrix ポリシー設定についても説明します。

ユーザープロファイル

デフォルトでは、VDA をインストールすると Citrix Profile Management が自動的にインストールされます。このプロファイルソリューションを使用する場合は、一般的な情報についてこの記事を確認してください。詳細については、Profile Management のドキュメントを参照してください。

Citrix Diagnostic Facility (CDF) トレースの収集

CDFControl ユーティリティは、さまざまな Citrix トレースプロバイダーから表示される Citrix Diagnostic Facility (CDF) トレースメッセージをキャプチャするためのイベントトレースコントローラーまたはコンシューマーです。これは、複雑な Citrix 関連の問題のトラブルシューティング、フィルターサポートの解析、およびパフォーマンスデータの収集のために作成されています。

シトリックス インサイト サービス

Citrix Insight Services (CIS) は、計測、テレメトリ、およびビジネスインサイト生成のための Citrix プラットフォームです。

シトリックス スカウト

Citrix Scout は、診断情報を収集し、ヘルスチェックを実行します。結果は、Citrix Virtual Apps and Desktops 展開におけるプロアクティブなメンテナンスに利用できます。Citrix は、Citrix Insight Services を通じて、診断コレクションの包括的な自動分析を提供します。また、Scout を使用して、単独で、または Citrix サポートのガイダンスを受けて問題をトラブルシューティングすることもできます。

Studio を使用した Citrix Virtual Apps and Desktops™ のライセンス

Studio から、ライセンスサーバーが Studio と同じドメイン内にあるか、信頼されたドメイン内にある場合、ライセンスを管理および追跡できます。ライセンスタスクの詳細については、ライセンスドキュメント および 複数タイプライセンス を参照してください。

License Activation Service (LAS) は、従来の Citrix® レガシーライセンスに代わる新しいクラウドベースのライセンスソリューションです。LAS はアクティベーション用の新しいモジュールを導入し、ライセンス管理へのシームレスで最新のアプローチを保証します。詳細については、License Activation Service を参照してください。

次の表に、サポートされているエディションとライセンスモデルを示します。

製品	エディション	ライセンスモデル
シトリックス バーチャルアプリ™	プレミアム、アドバンスト、スタンダード	同時使用
シトリックス バーチャルデスクトップ	プレミアム、アドバンスト、スタンダード	ユーザー/デバイスおよび同時使用

詳細については、同時使用ライセンス および ユーザー/デバイスライセンス を参照してください。

サポートされているCurrent Release (CR) およびLong Term Service Release (LTSR) のバージョン

サポートされているCurrent Release (CR)、Long Term Service Release (LTSR)、および最小互換LSバージョンについては、Citrix Virtual Apps and Desktops current releaseドキュメントを参照してください。

> **重要:**

> License Server VPXは非推奨となり、今後のメンテナンスやセキュリティ修正は行われません。License Server VPXのバージョン11.16.6以前を使用しているお客様は、できるだけ早く最新バージョンのLicense Server for Windowsに移行することをお勧めします。

> 以下のタスクを完了するには、完全なライセンス管理者である必要があります。Studioでライセンス情報を表示するには、管理者は少なくとも「ライセンスの読み取り」委任管理権限を持っている必要があります。組み込みの「完全管理者」および「読み取り専用管理者」の役割には、その権限があります。

Studioを使用してCitrix®からライセンスをダウンロードしてインストールする

1. Studioナビゲーションペインで、**構成 \> ライセンス**を選択します。
2. アクションペインで、**ライセンスの割り当て**を選択します。
3. ライセンスの購入または更新後にCitrixから電子メールで受け取ったライセンスアクセスコードを入力します。
4. 製品を選択し、**ライセンスの割り当て**を選択します。その製品で利用可能なライセンスが割り当てられ、ダウンロードされます。特定のライセンスアクセスコードのすべてのライセンスを割り当ててダウンロードした後、そのライセンスアクセスコードを再利用することはできません。同じコードで他のトランザクションを行うには、マイアカウントにログオンします。

ローカルコンピューターまたはネットワークに保存されているライセンスを追加する

1. Studioナビゲーションペインで、**構成 > ライセンス**を選択します。
2. アクションペインで、**ライセンスの追加**を選択します。
3. ライセンスファイルを参照し、ライセンスサーバーに追加します。

ライセンスサーバーを変更する

1. Studioナビゲーションペインで、**構成 > ライセンス**を選択します。
2. アクションペインで、**ライセンスサーバーの変更**を選択します。
3. ライセンスサーバーのアドレスを *name:port* の形式で入力します。name は DNS、NetBIOS、または IP アドレスです。ポート番号を指定しない場合、デフォルトのポート (27000) が使用されます。

使用するライセンスの種類を選択します

- サイトを構成するときに、ライセンスサーバーを指定すると、使用するライセンスの種類を選択するよう求められます。サーバーにライセンスがない場合、ライセンスなしで製品を 30 日間試用するオプションが自動的に選択されます。
- サーバーにライセンスがある場合、その詳細が表示され、いずれかを選択できます。または、ライセンスファイルをサーバーに追加してから、そのライセンスを選択することもできます。

製品エディションとライセンスモデルを変更する

1. Studio ナビゲーションペインで、［**構成**］**>**［**ライセンス**］ を選択します。
2. ［操作］ペインで、［**製品エディションの編集**］ を選択します。

3. 適切なオプションを更新します。

ライセンス管理コンソールにアクセスするには、**［操作］** ペインで **［ライセンス管理コンソール］** を選択します。コンソールがすぐに表示されるか、ダッシュボードがパスワード保護されている場合は、ライセンス管理コンソールの資格情報を求められます。コンソールの使用方法の詳細については、ライセンスドキュメントを参照してください。

> **注:**
>
> Citrix Studio でライセンスを切り替えると、その変更が Citrix Director に表示されるまでに最大 5 分かかります。たとえば、Advanced と Premium を切り替える場合などです。

ライセンス管理者を追加する

1. Studio ナビゲーションペインで、**［構成］>［ライセンス］** を選択します。
2. 中央のペインで、［ライセンス管理者］タブを選択します。
3. ［操作］ペインで、**［ライセンス管理者の追加］** を選択します。
4. 管理者として追加するユーザーを参照し、アクセス許可を選択します。

ライセンス管理者の権限を変更するか、ライセンス管理者を削除する

1. Studioナビゲーションペインで、 > を選択します。
2. 中央ペインで タブを選択し、管理者を選択します。
3. ペインで、 または のいずれかを選択します。

ライセンス管理者グループを追加する

1. Studioナビゲーションペインで、 > を選択します。
2. 中央ペインで タブを選択します。
3. ペインで、 を選択します。
4. ライセンス管理者として機能させたいグループを参照し、権限を選択します。Active Directory グループを追加すると、そのグループ内のユーザーにライセンス管理者権限が付与されます。

ライセンス管理者グループの権限を変更するか、ライセンス管理者グループを削除する

1. Studioナビゲーションペインで、 > を選択します。

2. 中央ペインで タブを選択し、管理者グループを選択します。
3. ペインで、 または のいずれかを選択します。

ライセンス情報を表示する

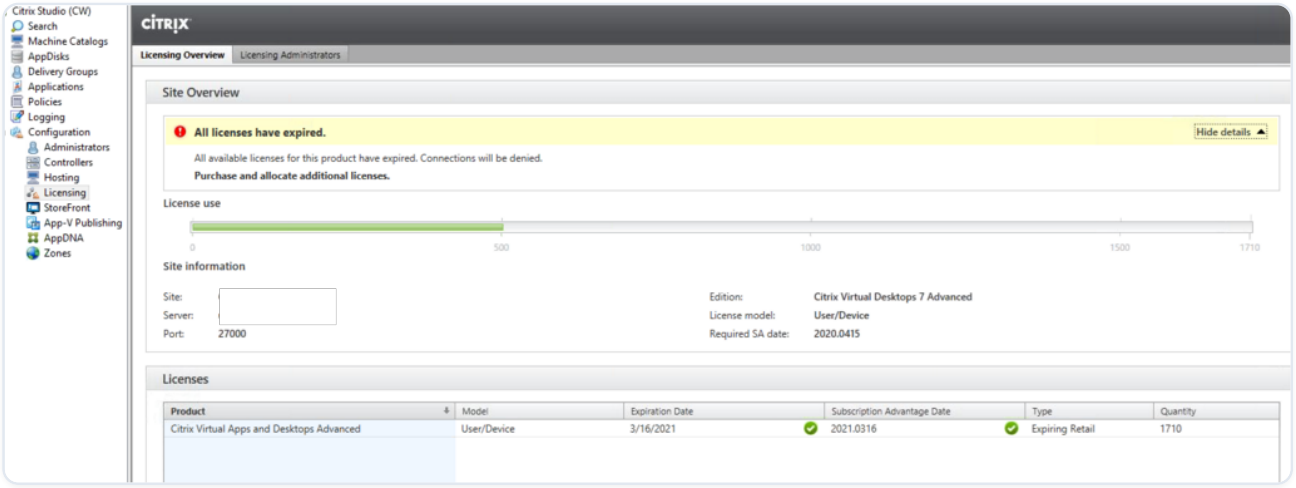
Studioナビゲーションペインで、 > を選択します。サイトのライセンス使用状況と設定の概要が、指定されたライセンスサーバーに現在インストールされているすべてのライセンスのリストとともに表示されます。

サイトのライセンス設定（製品タイプ、ライセンスエディション、ライセンスモデルを含む）が、構成済みのライセンスサーバーが使用するライセンスと一致していることを確認してください。一致しない場合、サイトのライセンス設定に合わせるために、既存のライセンスをダウンロードまたは割り当てる必要がある場合があります。

ライセンスの有効期限アラートを表示する

Citrix Studio は、Citrix License Server からライセンスファイルの有効期限を照会します。ライセンスファイルの有効期限が近づいている場合、またはすでに期限切れになっている場合、管理者にアラートが通知されます。

アラートは Studio ユーザーインターフェイスで確認できます。次の画像は、Citrix Studio UI に表示されるライセンス有効期限アラートを示しています。



関連リンク

- 年間および期間ベースの小売ライセンス向け Citrix オンプレミスサブスクリプションを参照してください。
- ハイブリッド権限による移行とアップグレード (TTU)を参照してください。

ライセンスアクティベーションサービス

ライセンスアクティベーションサービス (LAS) は、従来のCitrix®レガシーライセンスに代わる、新しいクラウドベースのライセンスソリューションです。LASは、アクティベーション用の新しいモジュールを導入し、ライセンス管理へのシームレスで最新のアプローチを保証します。

LASは、Citrixライセンスのエクスペリエンスを簡素化します。ライセンスサーバーで生成、ダウンロード、またはインストールするライセンスアクセスコードやファイルは不要になりました。ライセンスサーバーをアップグレードし、Citrix Cloudに登録するだけで済みます。互換性のある製品がライセンスサーバーを指すように設定されると、自動的にアクティベートされます。

アクティベーション後、ライセンスサーバーはライセンスアクティベーションサービスと定期的に通信し、アクティベーションを最新の状態に保ちます。LASはクラウドテクノロジーで構築されており、パフォーマンスを向上させ、ダウンタイムがないことを保証します。何らかの理由でライセンスサーバーまたはLASに到達できない場合、システムはライセンスキャッシュモードに入ります。これは、システムのライセンスが失われるのを防ぎ、停止を回避するように設計されています。詳細については、「ライセンスキャッシュモード」を参照してください。

LASの詳細については、ライセンスドキュメントの「ライセンスアクティベーションサービス」を参照してください。

前提条件

- ライセンスサーバーをバージョン11.17.2ビルド53100以降にインストールまたは更新します。
- ライセンスサーバー用の信頼性の高い継続的なインターネット接続。
- デスクトップグループレベルのライセンス設定は無効にする必要があります。

> **注:**
>
> DGレベルのライセンスが無効になっていることを確認するには、Get-brokerdesktopgroupを使用し、LicenseModelが「None」であることを確認します。

> **注:**
>
> 2203 LTSR CU7へのアップグレードを開始する前に、Delivery Controllerに.NET Framework 4.8をインストールしてください。これにより、ライセンス互換性チェックツールが適切に実行され、誤ったライセンス警告が防止されます。

考慮事項

- Citrix Studioがアクティベーションを促す前に、すべてのDelivery ControllerがLASと互換性がある必要があります。単一のコントローラーサイトでは、レガシーライセンスまたはLASのいずれかを使用できます。
- 複数のライセンスサーバーを同じCitrix Cloud ID (CCID) またはOrgIDに登録できます。ただし、サイトは1つのライセンスサーバーのみを指すように構成できます。

制限事項

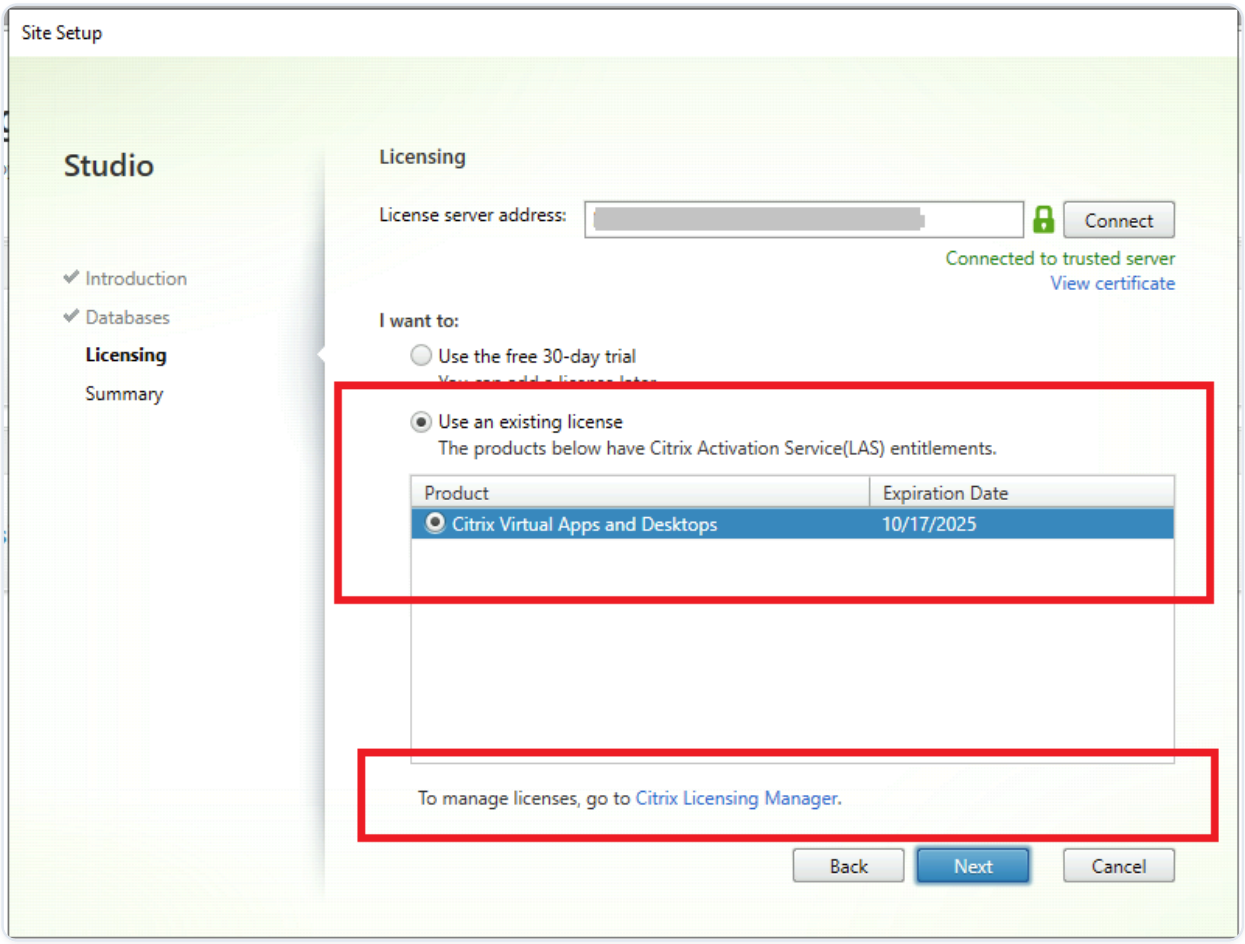
- LASへの移行により、製品エディションは**Premium**に、ライセンスモデルは**Concurrent**に設定されますが、これは将来変更される可能性があります。PowerShellを使用してライセンス構成を変更しないでください。登録やセッション起動に影響を与える可能性があります。
- 既存のレガシーライセンスからLASへのCitrix Virtual Apps and Desktops™サイトの移行は、Citrix Studioのみを使用して実行できます。

主な手順

1. ライセンスサーバーをバージョン11.17.2ビルド53100以降にインストールまたはアップグレードし、「ライセンスアクティベーションサービス用にライセンスサーバーを構成する方法」に記載されている手順に従ってLASを構成します。
2. Citrix Virtual Apps and Desktopsバージョン2203 LTSR CU7以降をインストールします。Citrix Delivery Controller、Citrix Studio、Citrix Directorなどのコアコンポーネントをインストールします。

   > **注:**
   >
   > Citrix Virtual Apps and Desktopsサイト内のすべてのDelivery Controllerは、LASと互換性がある必要があります。

3. 必要なコンポーネントをインストールしたら、Citrix Studioを使用してサイトを作成します。サイトの作成については、「サイトの作成」を参照してください。License ServerがLASを使用するように構成されている場合、Metainstallerはエンタイトルメントを表示します。エンタイトルメントは、対応するライセンス有効期限とともに提供されます。



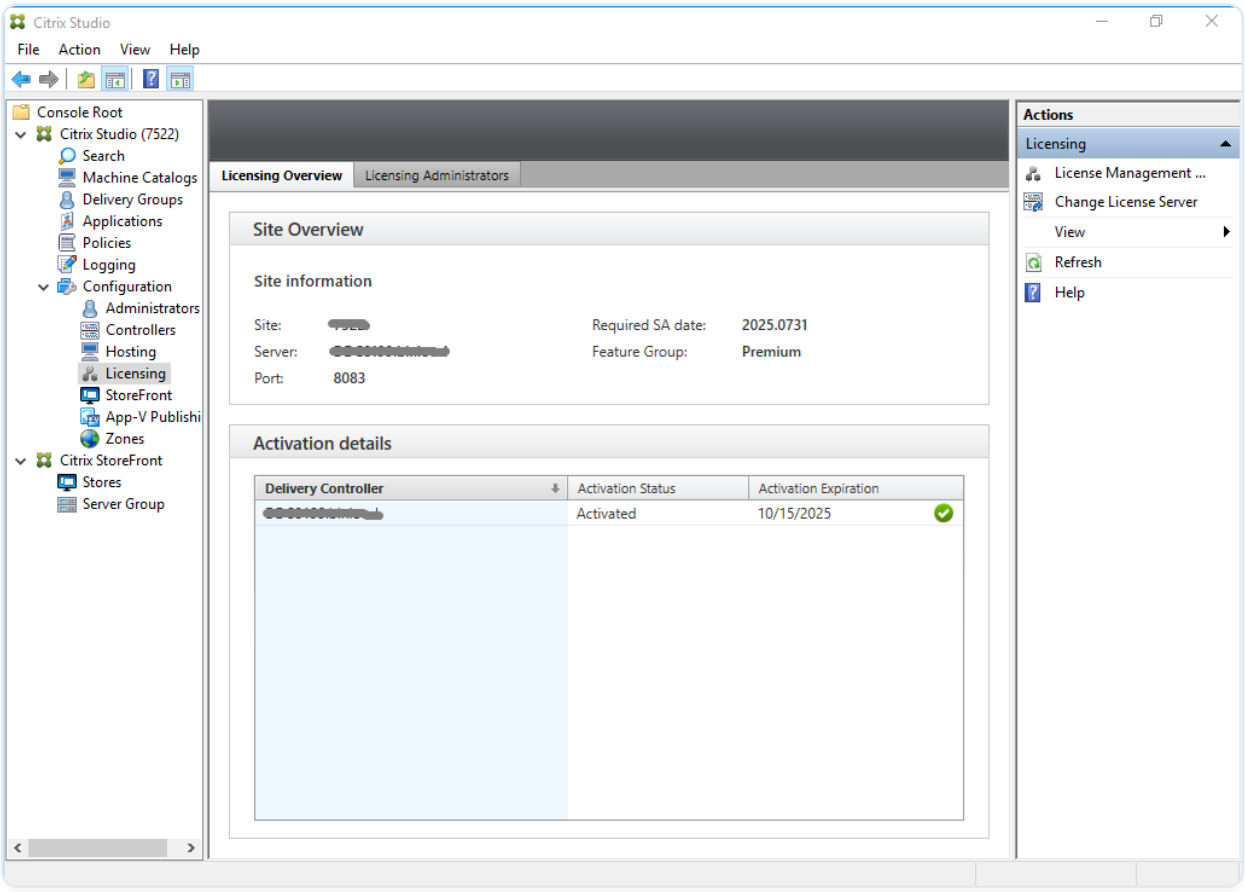
> **注:**
>
> License Serverがバージョン53100以降にアップグレードされていない場合、ライセンスエラーが発生します。これらのエラーを無視してCVADサイトのアップグレードを進めると、サイトが機能しなくなります。

4. ライセンスの詳細を確認する。
5. レガシーライセンスをLASに移行する。

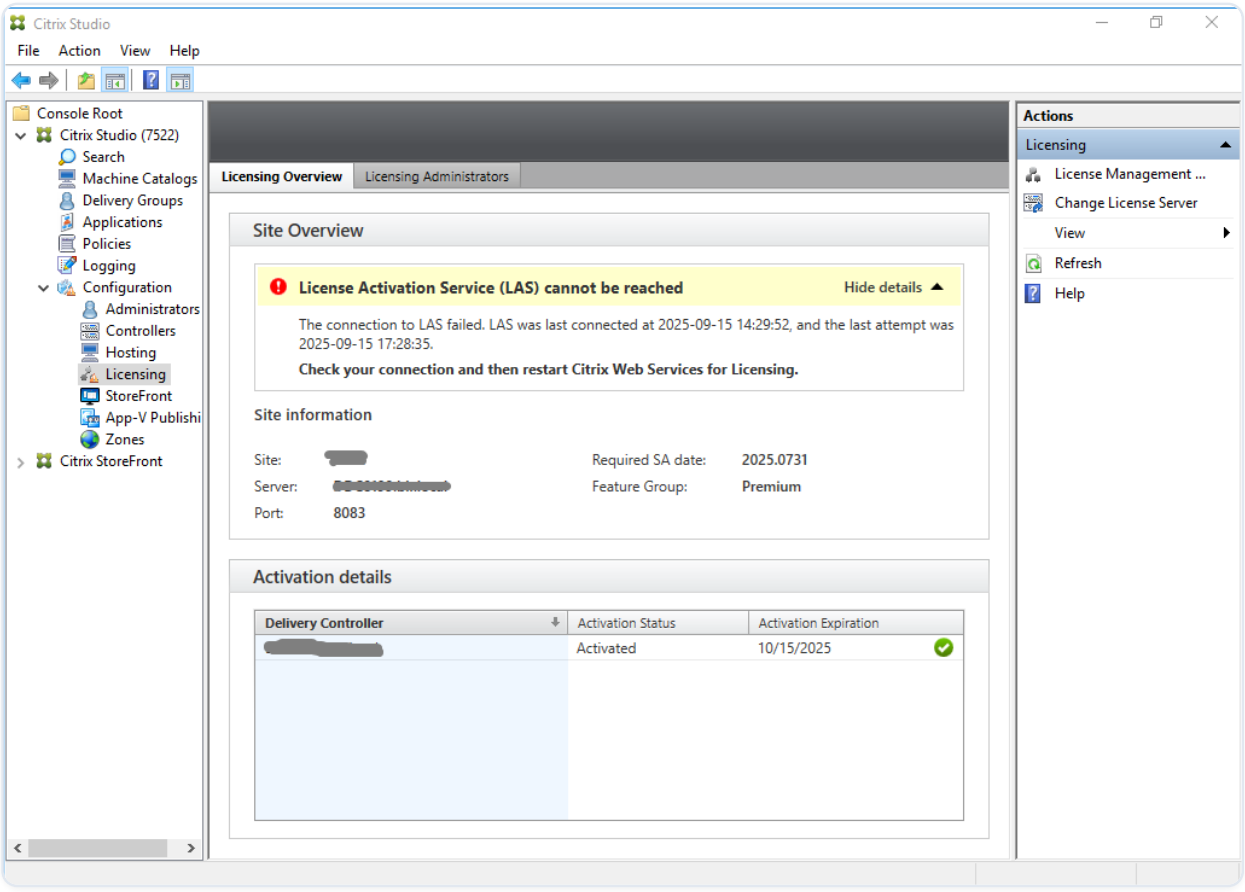
ライセンスの詳細を確認する

サイトを作成したら、Citrix Studioを使用してライセンスの詳細を確認します。

1. Citrix Studioで、**［ライセンス］**ノードを選択します。
2. **［ライセンスの概要］**ページで、Citrix Virtual Apps and Desktopsサイトに適切なライセンスがあるか、またはLAS機能の使用中にライセンスの有効期限が切れていないかを確認します。



LASに到達できない場合、エラーメッセージが表示されることがあります。



License Serverが古いレガシーライセンスをまだ使用しており、Citrix Virtual Apps and DesktopsサイトがLAS対応である場合、Citrix StudioはLicense ServerをCitrix Cloudに登録するよう促します。

LASを使用するためにライセンスサーバーを登録する(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/register-license-server.png)

レガシーライセンスをLASに移行する

Citrix Cloudにライセンスサーバーを登録済みで、必要なエンタイトルメントがある場合は、ユーザーセッションに影響を与えることなく、既存のCitrix Virtual Apps and Desktopsサイトをレガシーライセンスから LASに移行するために、以下の特定の手順に従う必要があります。

1. **ライセンスサーバーのアップグレード:** ライセンスサーバーをサポートされている最小バージョンにアップグレードします。
2. **Delivery Controllerのアップグレード:** サイト内のすべてのDelivery ControllerをLASでサポートされているバージョンにアップグレードします。
3. **デリバリーグループのライセンス割り当てを削除する:**
   - **Migrate to LAS**をクリックする前に、サイトレベルより下に設定されているライセンス割り当てを手動で削除します (つまり、デリバリーグループレベルのライセンス割り当てを削除します)。
4. **割り当ての確認:** LASの割り当てが正確であることを確認します。
5. **Migrate to LASをクリックする:**
   - 前の手順が完了したら、**Migrate to LAS**をクリックします。

     レガシーライセンスからLASに移行する(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/migrate-to-las.png)
   - LASに移行すると、Citrix Virtual Apps and Desktopsサイトの**ライセンスエディション**は**Citrix Virtual Apps and Desktops Premium**に設定され、**ライセンスモデル**は**Concurrent**に構成されます。

LASからレガシーライセンスへのロールバック

LASからレガシーライセンスにロールバックするには、次の手順を実行します。

1. 次のPowerShellコマンドを実行します。

```
Set-ConfigSite -UseLicenseActivationService $false
```

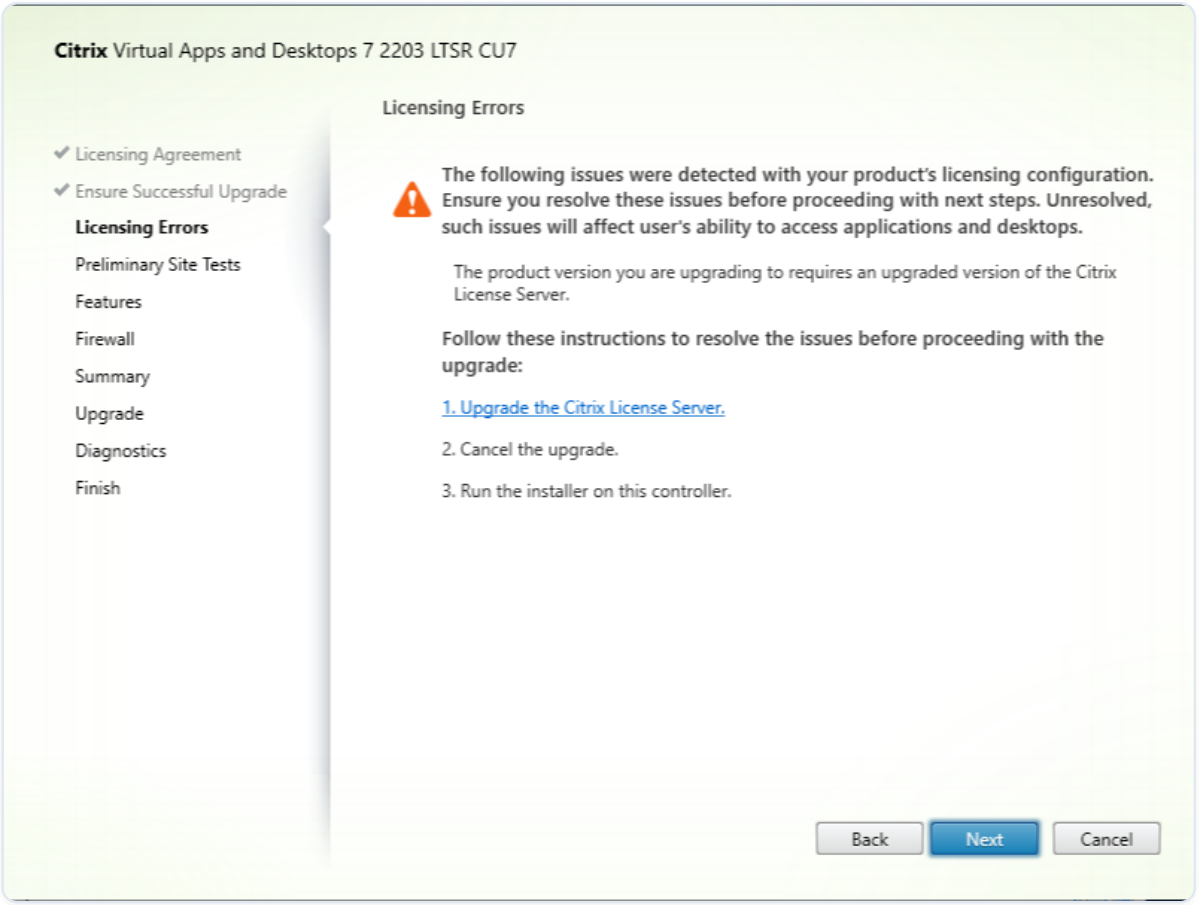
2. Citrix Studioでレガシーライセンスを設定します。

> **注：**
>
> これらの手順は、一時的なトラブルシューティングのみを目的としています。レガシーライセンスファイルは、サポート終了 (EOL) に近づいており、April 15, 2026 以降は機能しません。サービスの中断を避けるため、License Activation Service (LAS) への移行をお勧めします。詳細については、お知らせを参照してください。

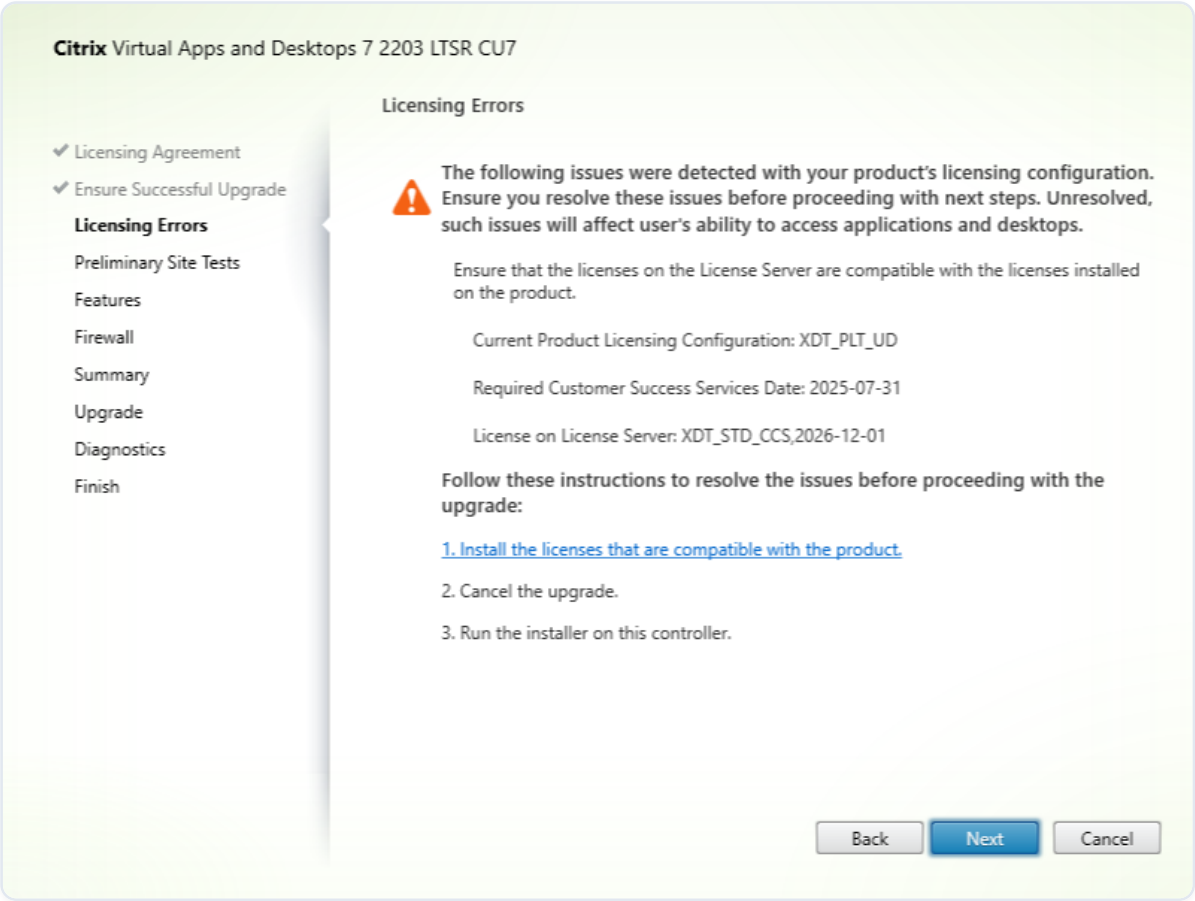
アップグレードに関する重要な考慮事項

以前のCitrix Virtual Apps and Desktopsバージョンから2203 LTSR CU7以降にアップグレードする場合、License Serverを最新バージョン（バージョン11.2.17ビルド53100以降）にアップグレードしてください。

- メタインストーラーUIを使用してアップグレードする際に、ライセンスエラーページで次のエラーが発生します。
  - 最新のLicense Serverバージョンにアップグレードしない場合：



  - 古いLicense Serverやライセンスの利用不可など、互換性の問題がある場合：



- コマンドラインを使用してアップグレードする場合、アップグレードの失敗を避けるために次のコマンドを実行します (マウントされたISOの\x64フォルダー内にいると仮定して)：

1. 次を実行します：

   ```
   \x64\Licensing\CitrixLicensing.exe /quiet
   ```

   ライセンスバイナリをローカルドライブのいずれかにコピーしている場合、次のコマンドを実行します：

   ```
   \x64\Licensing\CitrixLicensing.exe /quiet /l install.log
   ```

2. 次を実行します：

   ```
   \x64\XenDesktop Setup\XenDesktopServerSetup.exe  /components
   "CONTROLLER,DESKTOPSTUDIO,DESKTOPDIRECTOR" /CONFIGURE_FIREWALL
   ```

コアコンポーネントのアンインストール

アップグレード中に、コマンド`\x64\Licensing\CitrixLicensing.exe /quiet`または`\x64\Licensing\CitrixLicensing.exe /quiet /l install.log`を使用してLicense Serverを最初にインストールし、その後コアコンポーネントをインストールした場合、アンインストールも同じ順序で行ってください：

1. コマンドラインを使用してライセンスサーバーをアンインストールします。

   ```
   CitrixLicensing.exe /quiet /uninstall /l uninstall.log
   ```

2. GUIまたはコマンドラインを使用してコンポーネントをアンインストールします。詳細については、「コンポーネントの削除」を参照してください。

コマンドライン`XenDesktopServerSetup.exe`または`removeall`を使用してライセンスサーバーとコンポーネントをアンインストールした場合は、レジストリエントリと残りのファイルをクリーンアップします。

レジストリエントリをクリーンアップするには：

1. レジストリキー`Citrix Licensing`を検索し、そのエントリを削除します。ほとんどの場合、エントリは次の場所にあります。

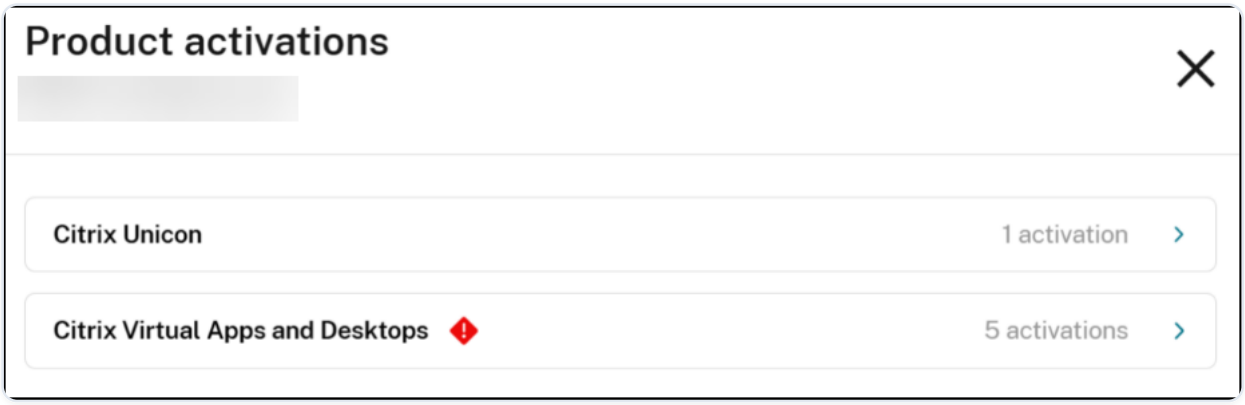
   ```
   "Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Cur
   rentVersion\Uninstall\
   ```

2. レジストリキーの**Uninstall String**が指すフォルダーを削除します。

トラブルシューティング

Citrix Cloudでライセンスサーバーのステータスが緑色以外で表示されている場合は、問題が発生している可能性のあるアクティベーションの詳細を把握するために、次の手順を実行します。

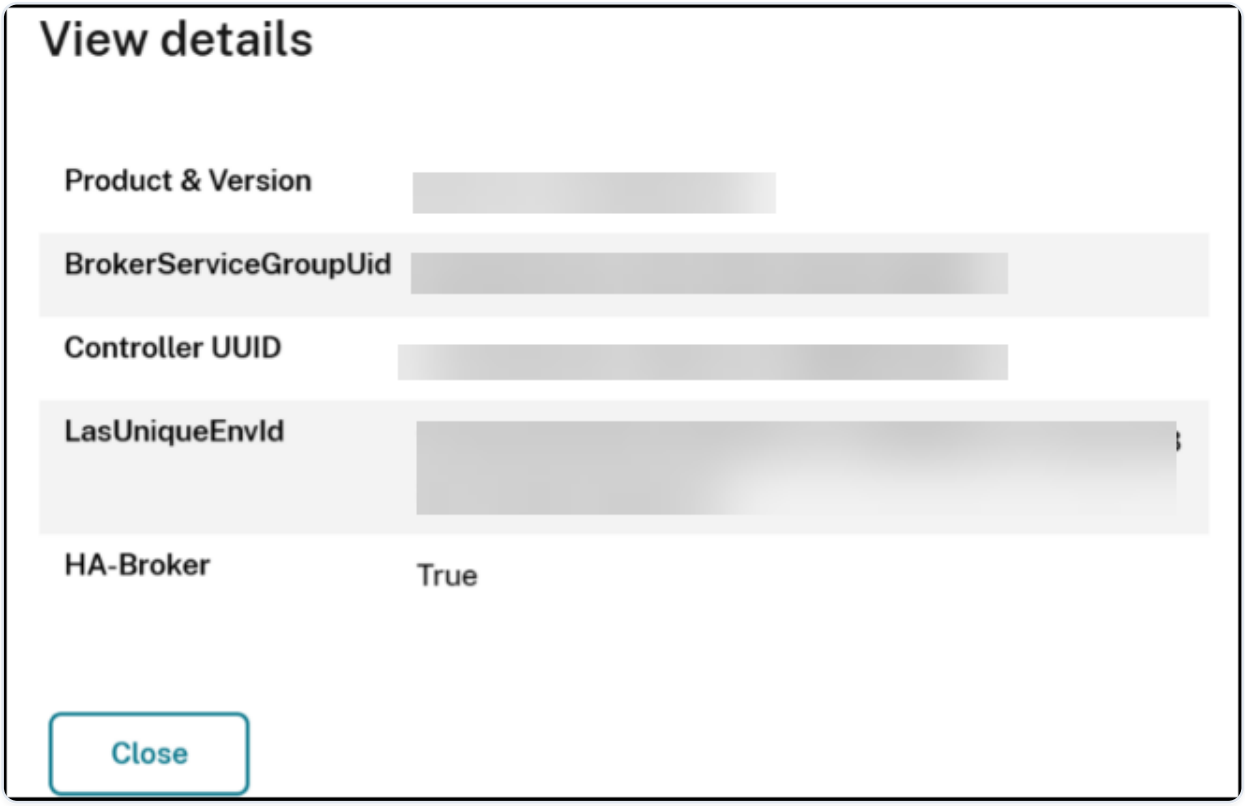
1. Citrix Cloud で、**ライセンス > ライセンス済み展開 > ライセンスサーバー**に移動します。
2. Citrix Virtual Apps and Desktopsの**>**展開ボタンをクリックして、アクティベートされたDelivery Controllerのリストを表示します。



3. アクティベーションの**［View details］**をクリックして、詳細を表示します。

   IDは、アクティベーションを識別するための一意の識別子です。

   次の詳細が提供されます。



- **製品とバージョン**：LASでアクティベートするときに製品が使用するように構成されているProduct_Edition_ModelとBurn In Date。BurnInDateは通常、製品のリリース日です。
- **BrokerServiceGroupUid**: ブローカーサービスグループの UID。
- **コントローラー UUID**: デリバリーコントローラーの UUID。
- **LasUniqueEnvId**: アクティベーションのために LAS によって提供されるインスタンスの一意の ID。
- **HA-Broker**: HA ブローカーかメインブローカーかを示す True または False。

アクティブ化されたホストの詳細を実際のホストにマッピングするには、ホストで次のコマンドを実行します。

- `Get-BrokerSite`: 画面に表示される **BrokerServiceGroupUid** の値を、コマンドの `BrokerServiceGroupId` 出力と比較します。
- `Get-BrokerController`: 画面に表示される **Controller UUID** の値を、コマンドの UUID 出力と比較します。

ライセンスイベントに関連するイベントビューアーログ

イベントID	説明
1112	Citrix Broker Service は、ユーザーからリソースへの接続を仲介できませんでした。サイトの製品およびエディションのライセンス構成では、このタイプのリソースは許可されていません。このサイトに正しいライセンスが選択されていることを確認してください。
1150	Citrix Broker Service はライセンスサーバーへの接続に成功しました。
1151	Citrix Broker Service はライセンスサーバーに接続できません。ライセンスサーバーが正しく機能していること、および XenDesktop 構成でライセンスサーバーを識別する詳細が正しいことを確認してください。
1152	このXenDesktopサイトには、ライセンスサーバーに必要な製品ライセンスがありません。ライセンス管理コンソールを使用して、関連する製品ライセンスをライセンスサーバーに追加してください。
1153	このXenDesktopサイトのライセンスの有効期限が切れました。Citrix Brokerサービスは、ライセンスサーバーから新しいライセンスを要求します。
1154	このコントローラーは、ライセンスサーバーに接続できなかったため、ライセンスキャッシュモードに入りました。このコントローラーがデスクトップおよびアプリケーション

イベントID	説明
	セッションの提供を停止するまで、残り2時間です。
1155	Citrix Brokerサービスは、デスクトップおよびアプリケーションセッションの提供を停止します。このコントローラーは、ライセンスサーバーとの通信が継続的に失敗したため、ライセンスキャッシュモードではなくなりました、またはライセンスキャッシュモードに入ることができませんでした。ライセンスサーバーが機能していることを確認し、必要に応じて、ライセンス管理コンソールを使用して関連するライセンスをライセンスサーバーに追加してください。
1156	Citrix Brokerサービスは、ライセンスサーバーと正常に通信しています。このコントローラーは、ライセンスキャッシュモードではなくなりました。
1157	実行中のライセンスサーバーのバージョンは、Citrix Brokerサービスのバージョンよりも古く、互換性がありません。ライセンスサーバーをアップグレードするか、XenDesktop構成で正しいバージョンのライセンスサーバーの場所を指定してください。
1158	Citrix Brokerサービスは、このエディションのこのサイトでライセンスサーバーが利用可能なライセンス数を超過していることを検出しました。ライセンスサーバーは、オーバードラフトライセンスを付与しました。
1159	Citrix Brokerサービスは、このサイトにインストールされているライセンスの最大数を超過したため、デスクトップ接続を拒否しました。このエディションには3つのライセンスがインストールされていますが、このエディションで許可されているライセンスの最大数は2つです。ライセンス制限に準拠するために、ライ

イベントID	説明
	センスサーバーから関連するライセンスを削除してください。
1160	Citrix Brokerサービスは、ライセンス管理中に内部エラーを検出しました。ライセンスサーバーが正しく機能していること、およびXenDesktop構成でライセンスサーバーを識別する詳細が正しいことを確認してください。Citrix Brokerサービスを再起動すると、問題が解決する場合もあります。この問題が解決しない場合は、Citrix XenDesktop Controllerを再インストールしてください。Citrix Knowledge Baseの記事CTX126990を参照してください。
1161	ライセンスの初期化中にエラーが発生しました。ライセンスサーバーの接続を確認してください。
1162	ライセンスの停止中にエラーが発生しました。ライセンスサーバーの接続を確認してください。
1163	接続ライセンスがありません。解決するには、不要なセッションを閉じてライセンスを解放するか、ライセンスを追加してください。
1164	接続ライセンスのチェックアウト中にエラーが発生しました。ライセンスサーバーの接続を確認してください。
1165	接続ライセンスのチェックイン中にエラーが発生しました。ライセンスサーバーの接続を確認してください。
1166	ライセンスの可用性確認中にエラーが発生しました。ライセンスサーバーの接続を確認してください。
1167	ライセンスの開始に失敗しました。ライセンスサーバーの接続を確認してください。

イベントID	説明
1168	ライセンスユーザー通知設定の読み取り中にエラーが発生しました。ライセンスサーバーの接続を確認してください。
1169	ライセンスサーバーで適切なライセンスが見つからなかったため、このコントローラーは初期設定のライセンスキャッシュモードに入りました。このコントローラーがデスクトップおよびアプリケーションセッションの提供を停止するまで、残り2時間です。
1170	Citrix Broker Serviceは、ライセンスサーバーで適切なライセンスを正常に検出しました。このコントローラーは、初期設定のライセンスキャッシュモードではなくなりました。
1171	ライセンスサーバーが指定されていません。有効なライセンスサーバーが指定されるまで、Citrix Broker Serviceはユーザーにデスクトップとアプリケーションを提供できません。Citrix StudioまたはCitrix PowerShell SDKのSet-ConfigSiteコマンドレットを使用して、ライセンスサーバーを指定できます。
1172	ライセンスサーバーの適合性確認中にエラーが発生しました。Citrix Broker Serviceは、マシンがライセンスサーバーとして使用するのに適しているかを確認する際に、予期しない応答を受け取りました。コントローラーからマシンに接続できること、およびマシンのファイアウォールがコントローラーからの接続を許可していることを確認してください。マシンにライセンスサーバーがインストールされている場合は、それが正しく構成され、動作していることを確認してください。
1173	このXenDesktopサイトには、ライセンスサーバーに必要な起動ライセンスがありません。License Administration Consoleを使用して、関連するライセンスをライセンスサーバーに追加してください。

イベントID	説明
1174	このXenDesktopサイトに構成されている製品エディションはアプリケーションをサポートしていません。アプリケーションリソースは利用できません。
1176	構成された製品エディションはマルチセッションマシンをサポートしていません。登録は拒否されました。
1177	構成された製品エディションはシングルセッションマシンをサポートしていません。登録は拒否されました。
1178	構成された製品エディションはRemotePCをサポートしていません。登録は拒否されました。
1179	構成された製品エディションは、クラウドシステムにプロビジョニングされたマシンをサポートしていません。登録は拒否されました。
1180	このXenDesktopサイト用に構成された製品エディションは、シングルセッション（ワークステーションOS）マシン上のアプリケーションをサポートしていません。アプリケーションリソースの起動は拒否されました。
1181	このXenDesktopサイト用に構成された製品エディションは、マルチセッション（サーバーOS）マシン上のアプリケーションをサポートしていません。アプリケーションリソースの起動は拒否されました。
1182	このXenDesktopサイト用に構成された製品エディションは、シングルセッション（ワークステーションOS）マシン上のデスクトップをサポートしていません。デスクトップリソースの起動は拒否されました。

イベントID	説明
1183	このXenDesktopサイト用に構成された製品エディションは、マルチセッション（サーバーOS）マシン上のデスクトップをサポートしていません。デスクトップリソースの起動が拒否されました。
1196	このコントローラーは、ライセンスサーバー上の使用可能なすべてのライセンスを使い果たしたため、ライセンスバーストモードに入りました。これを解決するには、さらにライセンスを追加してください。このコントローラーがデスクトップおよびアプリケーションセッションの提供を停止するまで、残り2時間です。
1197	Citrix Broker Serviceは、デスクトップおよびアプリケーションセッションの提供を停止します。このコントローラーは、ライセンスサーバー上のライセンス不足のため、ライセンスバーストモードを終了したか、またはライセンスバーストモードに入ることができませんでした。関連するライセンスをライセンスサーバーに追加するには、ライセンス管理コンソールを使用してください。
1198	Citrix Broker Serviceは、ライセンスサーバーからライセンスを正常に消費しています。現在の需要を満たすのに十分なライセンスがサーバー上にあります。このコントローラーは、ライセンス枯渇によって引き起こされたライセンスバーストモードを終了しました。
1199	Citrix Broker Serviceは、デスクトップおよびアプリケーションセッションの提供を停止します。ライセンスサーバーにライセンスがインストールされていないため、このコントローラーはライセンスキャッシュモードを終了したか、またはライセンスキャッシュモードに入ることができませんでした。関連するライセンスをライセンスサーバーに追加するに

イベントID	説明
	は、ライセンス管理コンソールを使用してください。
1205	ソフトウェアメンテナンスの有効期限が切れました。Citrix環境は現在サポートされていません。ライセンスサーバーで期限切れのライセンスを確認し、削除してください。ユーザーが警告メッセージを受け取り始める前に、30日間のライセンスキャッシュモードがあります。
1206	ライセンス証明書のハッシュが無効です。Citrixライセンス証明書のハッシュが無効です。
1300	Citrix Broker Serviceは、デスクトップおよびアプリケーションセッションの提供を停止します。ライセンスサーバーのシステムクロックに問題があります。
1301	ライセンスサーバーのシステムクロックに関する問題が修正されました。Citrix Broker Serviceは正常な動作を再開します。
1302	このコントローラーは、接続ライセンスのチェックインまたはチェックアウトに再度失敗しました。以前に検出された障害はまだ存在します。過剰なイベントログを避けるため、問題が解決されるまで、サービスは関連メッセージ（イベントID 1163、1164、1165）を抑制しています。ライセンスの試行は継続されます。
1303	このコントローラーは、関連メッセージ（イベントID 1163、1164、1165）の抑制を停止しました。
1304	Citrix Broker ServiceはLASに正常に接続しました。

イベントID	説明
1305	Citrix Broker ServiceはLASに接続できません。LASが正しく機能していること、およびLASを識別する詳細がXenDesktop構成で正しいことを確認してください。

詳細情報

サイトのLAS状態の確認、またはサイトがライセンスキャッシュモードであるかどうかの確認については、以下を参照してください。

- サイトのLAS状態を確認するにはどうすればよいですか？
- サイトがライセンスキャッシュモードであるかどうかを確認するにはどうすればよいですか？

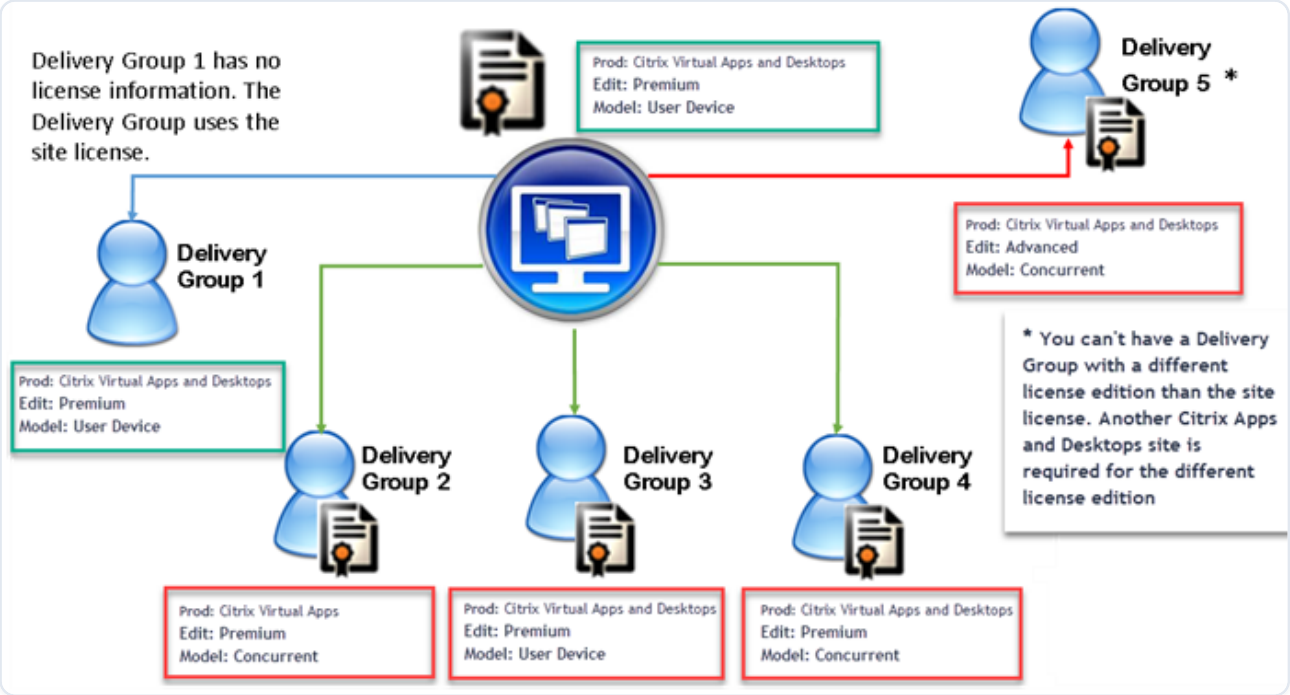
コマンドの詳細については、以下を参照してください。

- Get-BrokerController
- Get-ConfigSite

マルチタイプライセンス

マルチタイプライセンスは、単一の Citrix Virtual Apps and Desktops サイト上のデリバリーグループに対して、異なるライセンスタイプの消費をサポートします。**タイプ**は、製品ID（XDTまたはMPS）とモデル（UserDeviceまたはConcurrent）の単一の組み合わせです。デリバリーグループは、サイトレベルで構成されているものと同じ製品エディション（PLT/PremiumまたはENT/Advanced）を使用する必要があります。Citrix Virtual Apps and Desktops の展開でマルチタイプライセンスを構成する際は、この記事の最後にある特別な考慮事項 に注意してください。

マルチタイプライセンスが構成されていない場合、異なるライセンスタイプは、個別のサイト用に構成されている場合にのみ使用できます。デリバリーグループはサイトライセンスを使用します。マルチタイプライセンスが構成されている場合の重要な通知の制限については、特別な考慮事項 を参照してください。



異なる種類のライセンスを消費するデリバリーグループを特定するには、以下の Broker PowerShell コマンドレットを使用します。

- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup
- Get-BrokerDesktopGroup

ライセンスをインストールするには、以下を使用します。

- シトリックス スタジオ
- シトリックス ライセンシング マネージャー
- citrix.com

Customer Success Services の日付は、各ライセンスファイル、各製品、およびモデルに固有です。異なる設定のデリバリーグループは、互いに異なる Customer Success Services の日付を持つ場合があります。

特別な考慮事項

マルチタイプライセンスは、通常のCitrix Virtual Apps and Desktops™ライセンスとは異なる機能を持ちます。

サイト構成とは異なるタイプを使用するように構成されたデリバリーグループの場合、DirectorまたはStudioからのアラートや通知はありません。

- ライセンス制限に近づいた場合、またはライセンスバーストモードのトリガーや期限切れに関する情報はありません。
- 特定のグループに問題がある場合の通知はありません。

マルチタイプライセンス用に構成されたデリバリーグループは、そのライセンスタイプのみを消費し、完全に消費されてもサイト構成にフォールバックしません。

Citrix Virtual Apps StandardとCitrix Virtual Desktops™ Standardのライセンスエディション名はどちらもStandardであることを示していますが、これらは同じエディションではありません。マルチタイプライセンスは、Citrix Virtual Apps StandardおよびCitrix Virtual Desktop Standardライセンスでは利用できません。

ライセンス互換性マトリックス

この表は、古い製品名、新しい製品名、および関連する機能名を詳述しています。4つの互換性列は、どの製品とライセンスモデルの組み合わせがマルチタイプライセンスと互換性があるかを指定します。CCUとCCSは同時接続ライセンスを表し、UDはユーザー/デバイスライセンスを表します。

Old Name	New Name	Feature	Multi-type licensing compatibility			
			STD	ADV	ENT	PLT
Citrix XenApp Standard	Citrix XenApp Standard	MPS_STD_CCU	X			
Citrix XenApp Advanced	Citrix Virtual Apps Standard	MPS_ADV_CCU		X		
Citrix XenApp Enterprise	Citrix Virtual Apps Advanced	MPS_ENT_CCU			X	
Citrix XenApp Platinum	Citrix Virtual Apps Premium	MPS_PLT_CCU				X
Citrix XenDesktop VDI Edition (XDT-U)	Citrix Virtual Desktops Standard- Per User/Device	XDT_STD_UD	X			
Citrix XenDesktop VDI Edition (XDT-C)	Citrix Virtual Desktops Standard - Concurrent	XDT_STD_CCS	X			
Citrix XenDesktop Enterprise Edition (XDT-C)	Citrix Virtual Apps and Desktops Advanced - Concurrent	XDT_ENT_CCS			X	
Citrix XenDesktop Enterprise Edition (XDT-U)	Citrix Virtual Apps and Desktops Advanced - Per User/Device	XDT_ENT_UD			X	
Citrix XenDesktop Platinum Edition (XDT-C)	Citrix Virtual Apps and Desktops Premium - Concurrent	XDT_PLT_CCS				X
Citrix XenDesktop Platinum Edition (XDT-U)	Citrix Virtual Apps and Desktops Premium - Per User/Device	XDT_PLT_UD				X

ブローカー PowerShell SDK

DesktopGroup オブジェクトには、関連するNew-BrokerDesktopGroupおよびSet-BrokerDesktopGroupコマンドレットを使用して操作できる次の2つのプロパティがあります。

名前	値	制限
LicenseModel	グループのライセンスモデルを指定するパラメーター (Concurrent または UserDevice)。指定されていない場合、サイト全体のライ	機能トグルが無効になっている場合、プロパティを設定しようとすると失敗します。

名前	値	制限
	センスモデルが使用されます。	
ProductCode	XDT (Citrix Virtual Desktops用) またはMPS (Citrix Virtual Apps™用) のテキスト文字列で、グループのライセンス製品IDを指定します。指定されていない場合、サイト全体の製品コードが使用されます。	機能トグルが無効になっている場合、プロパティを設定しようとすると失敗します。

LicenseModelとProductCodeの詳細については、about_Broker_Licensingを参照してください。

New-BrokerDesktopGroup

デスクトップグループのブローカーを管理するためのデスクトップグループを作成します。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerDesktopGroup/>`を参照してください。

Set-BrokerDesktopGroup

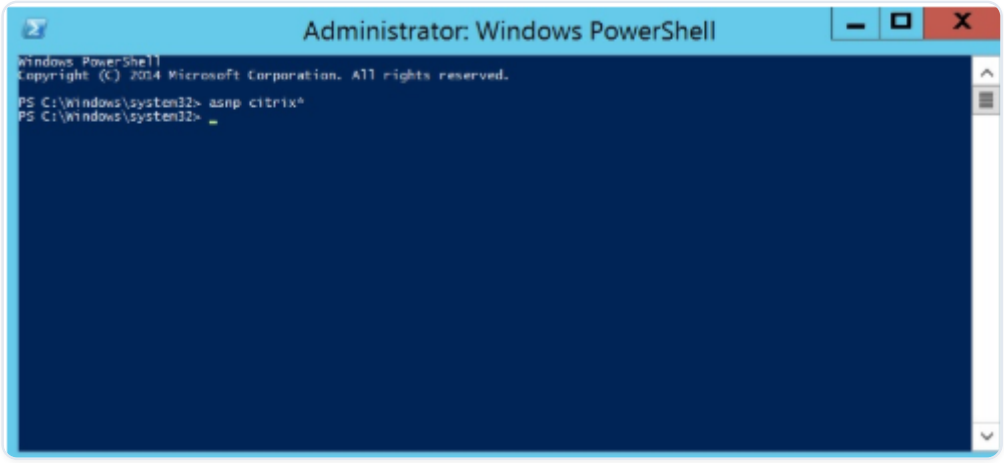
既存のブローカーデスクトップグループを無効または有効にするか、その設定を変更します。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>`を参照してください。

Get-BrokerDesktopGroup

指定された条件に一致するデスクトップグループを取得します。Get-BrokerDesktopGroupコマンドレットの出力には、グループの**ProductCode**および**LicenseModel**プロパティが含まれます。New-BrokerDesktopGroupまたはSet-BrokerDesktopGroupを使用してプロパティが設定されていない場合、null値が返されます。nullの場合、サイト全体のライセンスモデルと製品コードが使用されます。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/Get-BrokerDesktopGroup/>`を参照してください。

デリバリーグループごとに異なるライセンス製品とモデルを構成する

1. 管理者権限でPowerShellを開き、Citrixスナップインを追加します。

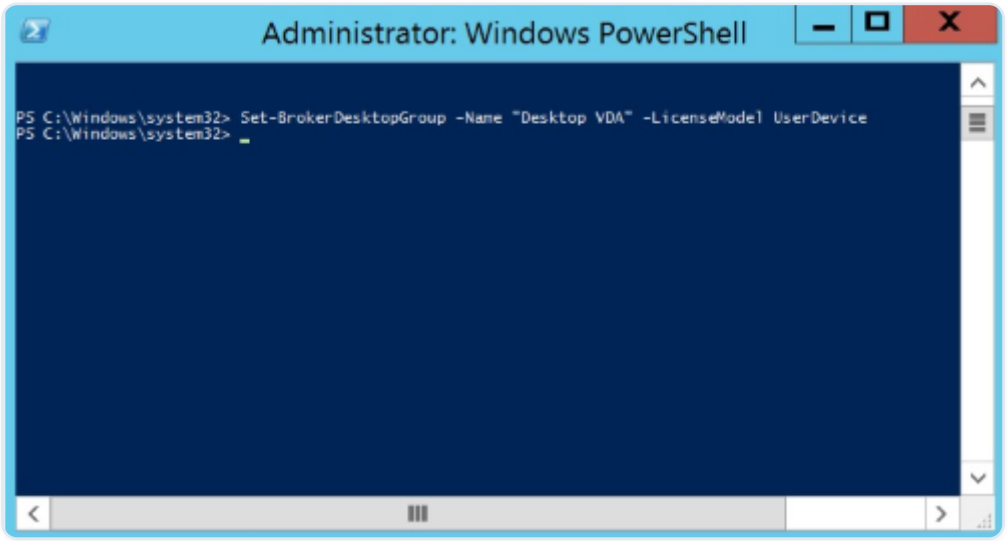


2. コマンド **Get-BrokerDesktopGroup –Name “DeliveryGroupName”** を実行して、現在のライセンス構成を表示します。パラメーター **LicenseModel** と **ProductCode** を見つけます。これらのパラメーターを以前に構成していない場合、空白になっている可能性があります。

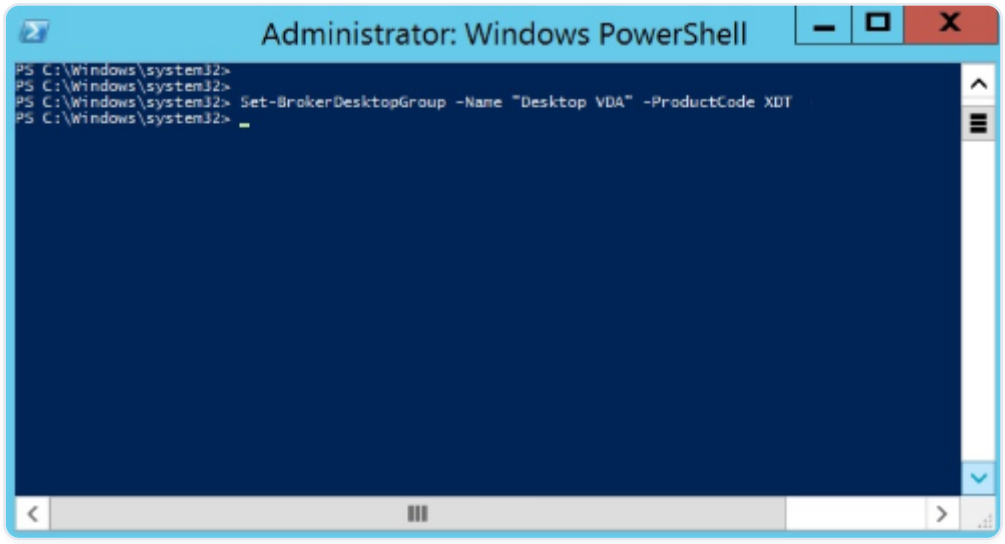
> **注：**
>
> デリバリーグループにライセンス情報が設定されていない場合、デフォルトで**サイトレベルのサイトライセンス**になります。

PowerShellコマンド(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/license-configuration-2.png)

3. コマンド **Set-BrokerDesktopGroup –Name “DeliveryGroupName” –LicenseModel LicenseModel** を実行して、ライセンスモデルを変更します。



4. コマンドを実行してライセンス製品を変更します: **Set-BrokerDesktopGroup –Name “DeliveryGroupName” –ProductCode ProductCode**。



5. 変更を検証するには、コマンド **Get-BrokerDesktopGroup –Name “DeliveryGroupName”** を入力します。

> **注：**
>
> 同じサイト内でエディションを混在させることはできません。たとえば、Premiumライセンスとライセンスなどです。異なるエディションのライセンスがある場合は、複数のサイトが必要です。
>
> PowerShellコマンド(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/license-configuration-5.png)

6. 前の手順で説明したのと同じ **Set-BrokerDesktopGroup** コマンドを実行し、値を **$null** に設定して、ライセンス構成を削除します。

> **注：**
>
> Studioでは、各デリバリーグループのライセンス構成は表示されません。現在の構成を表示するには、PowerShellを使用します。
>
> PowerShellコマンド(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/license-configuration-6.png)

例

このPowerShellコマンドレットの例は、既存の2つのデリバリーグループにマルチタイプライセンスを設定し、3つ目のデリバリーグループを作成して設定する方法を示しています。

デリバリーグループに関連付けられているライセンス製品とライセンスモデルを確認するには、**Get-BrokerDesktopGroup** PowerShellコマンドレットを使用します。

1. 最初のデリバリーグループをXenApp®およびConcurrentに設定しました。

   Set-BrokerDesktopGroup -Name "シトリックス バーチャル アプリケーションズ プレミアム コンカレント 用のデリバリーグループ" -ProductCode MPS -LicenseModel Concurrent

2. 2番目のデリバリーグループをXenDesktop®およびConcurrentに設定しました。

   Set-BrokerDesktopGroup -Name "シトリックス バーチャル デスクトップス プレミアム コンカレント 用のデリバリーグループ" -ProductCode XDT -LicenseModel Concurrent

3. 3番目のデリバリーグループをXenDesktopおよびUserDevice用に作成して設定します。

   New-BrokerDesktopGroup -Name "Citrix Virtual Desktops Premium UserDevice 用のデリバリーグループ" -PublishedName "MyDesktop" -DesktopKind Private -ProductCode XDT -LicenseModel UserDevice

ライセンスに関するFAQ

> **注：**
>
> - COVID-19パンデミックに関連する事業継続リソースについては、CTX27055を参照してください。
> - 事業継続の維持に関する一般情報については、Business continuity — on demandを参照してください。
> - 現在のCitrix License Serverに関する詳細については、Licensingを参照してください。

Citrix®ライセンス

ライセンスファイルはどのように入手できますか?

ライセンスアクセスコードは電子メールで送信されます。ライセンスアクセスコードを使用してライセンスファイルを生成する方法は3つあります。

- `citrix.com`のMyAccountページから**ライセンスの管理**。詳細については、citrix.comでライセンスを管理するを参照してください。
- Citrix Studioで購入を割り当てると、ライセンスファイルはCitrix License Serverに自動的にインストールされます。
- Citrix License Server内のCitrix Licensing Managerで、購入を割り当ててライセンスファイルをインストールします。詳細については、ライセンスのインストールを参照してください。

MyAccountでライセンスを割り当てる方法?

ライセンスの割り当てを参照してください。

割り当てられたライセンスをライセンスサーバーに追加する方法?

ライセンスの変更を参照してください。

CitrixライセンスはどのTCPポートを使用しますか?

- ライセンスサーバーのポート番号は27000です。
- ベンダーデーモンのポート番号は7279です。
- 管理コンソールのWebポートは8082です。
- ライセンス用Webサービスのポートは8083です。

Citrixライセンスサーバーとは何ですか?

Citrixライセンスサーバーは、ネットワーク全体でライセンスを共有できるシステムです。詳しくは、「ライセンス操作の概要」を参照してください。

Citrixライセンスサーバーを仮想化またはクラスター化できますか?

はい。Citrixライセンスサーバーを仮想化またはクラスター化できます。詳しくは、「クラスター化されたライセンスサーバー」を参照してください。

Citrixライセンスサーバーを仮想化すると、どのようなメリットがあります?

Citrixライセンスサーバーを仮想化すると、冗長性のあるソリューションが提供されます。このソリューションにより、ダウンタイムなしで複数の物理サーバー間を移動できます。

Citrixライセンスサーバーを仮想化する場合、考慮すべき制限はありますか?

いいえ。

Citrixライセンスサーバーは、Citrix Virtual Apps and Desktops™展開のすべてのライセンスを管理しますか?

Citrixライセンスサーバーは、Citrix Gatewayで使用されるPremium Editionのライセンスを除く、Citrix Virtual Apps™ and Desktopで受け取るすべてのライセンスを管理します。これらのセキュリティ指向のネットワークデバイスに必要な、ネットワークアプライアンスに組み込まれたライセンスサーバーが、それらのライセンスを管理します。

Citrix Licensing Managerとは何ですか?

Citrix Licensing Managerを使用すると、Citrix Licensing Managerをインストールしたライセンスサーバーからライセンスファイルをダウンロードして割り当てることができます。Citrix Licensing Managerは、推奨されるライセンスサーバー管理方法であり、次の機能を提供します。

- ライセンスサーバーのCitrix Cloud™へのショートコード登録と、登録の簡単な削除。
- ユーザーアカウントとグループアカウントを構成する。
- ダッシュボードを使用して、インストール済み、使用中、期限切れ、利用可能なライセンス、およびCustomer Success Servicesの有効期限を表示する。
- レポート作成に使用するため、ライセンス使用状況データをエクスポートする。
- 履歴使用状況データの保持期間を構成する。デフォルトのデータ保持期間は180日です。
- ライセンスアクセスコードまたはダウンロードしたファイルを使用して、ライセンスサーバーへのライセンスファイルのインストールを簡素化する。
- ライセンスバーストモードを有効化および無効化する。
- Customer Experience Improvement Program (CEIP)およびCall Homeを構成する。
- Customer Success Servicesの更新ライセンスを自動的または手動で確認し、見つかった場合は通知するか、ライセンスをインストールします。
- ライセンスサーバーの状態（起動ライセンスの不足、時間に関する問題、アップローダーの失敗）を通知する。
- 次のポートを変更する：
  - ライセンスサーバー（デフォルト 27000）
  - ベンダーデーモン（デフォルト 7279）
  - ライセンス用Webサービス（デフォルト 8083）

詳細については、「Citrix Licensing Manager」を参照してください。

Citrix License Administration Consoleはどこにありますか?

License Administration Consoleはサポートされなくなり、License Serverバージョン11.16.6から削除されました。Citrix Licensing Managerを使用することをお勧めします。

License ServerがStudioと同じドメイン内、または信頼されたドメイン内にある場合、Studioを使用してライセンスを管理および追跡できます。

詳細については、「Citrix Licensing Manager」を参照してください。

ライセンス割り当て期間とは何ですか?

ライセンス割り当て期間とは、Citrix Virtual Apps and Desktopsライセンスがユーザーまたはデバイスに割り当てられる期間のことです。デフォルトのライセンス割り当て期間は90日です。

組織が購入したライセンスの数を確認するにはどうすればよいですか?

購入したすべてのライセンスは、`<https://www.citrix.com>`の**My Account**ページにある安全な**Manage Licenses**ツールボックスから、いつでも（24時間365日）確認およびアクセスできます。

いつでも使用中のライセンス数を確認するにはどうすればよいですか?

Citrix Licensing ManagerとStudioは、リアルタイムのライセンス使用状況に関する詳細を提供します。

License Serverのディザスターリカバリとメンテナンス

License Serverのディザスターリカバリとメンテナンスについては、Citrix Licensingドキュメントの「ディザスターリカバリとメンテナンス」を参照してください。

Citrix Virtual Apps and Desktopsのライセンス

Citrix Virtual Apps and Desktopsはどのようにライセンスされますか?

Citrix Virtual Apps and Desktopsのライセンスは、ユーザー単位とデバイス単位、および同時使用ライセンスモデルを提供します。

ユーザー/デバイス:

柔軟なユーザー/デバイスモデルは、以下と連携します。

- 全社的なデスクトップ利用。
- 基盤となるMicrosoftデスクトップ仮想化ライセンス。
- 仮想デスクトップとアプリへのアクセスが時々しか必要ないユーザーを持つ顧客向けの同時使用ライセンス。

ユーザー/デバイスライセンスは、ユーザーが任意の数のデバイスから仮想デスクトップとアプリにアクセスできるようにします。デバイスライセンスは、単一のデバイスから任意の数のユーザーが仮想デスクトップとアプリにアクセスできるようにします。このアプローチにより、最大限の柔軟性が提供され、Microsoftデスクトップ仮想化ライセンスとの連携が向上します。

> **重要:**
>
> ライセンスをユーザーまたはデバイスに手動で割り当てることはできません。ライセンスサーバーまたはクラウドサービスがライセンスを割り当てます。ユーザー/デバイスライセンスでは、一度割り当てられたライセンスは、90日間非アクティブになるまで別のユーザーに割り当てることはできません。

> **同時使用:**

同時使用ライセンスは、任意のユーザーおよび任意のデバイスに対して、無制限の数の仮想アプリおよびデスクトップへの1つの接続を許可します。ライセンスはアクティブなセッション中にのみ消費されます。セッションが切断または終了した場合、ライセンスはプールに戻されます。

ユーザー/デバイスライセンスの詳細については、ユーザー/デバイスライセンス を参照してください。同時使用ライセンスについては、同時使用ライセンス を参照してください。

ライセンスを購入する前にCitrix Virtual Apps and Desktopsを試用することはできますか?

はい。Citrix Virtual Apps and Desktopsソフトウェアをダウンロードし、試用モードで実行できます。試用モードでは、ライセンスなしで、オンプレミスでCitrix Virtual Apps and Desktopsを30日間、10接続まで使用できます。詳細については、評価ライセンス を参照してください。

Citrix Cloud向けのCitrix DaaS™ (旧Citrix Virtual Apps and Desktopsサービス) は、承認に基づいて試用サービスとして利用できます。詳細については、Citrix担当者にお問い合わせください。

CitrixはCitrix Virtual Apps and Desktopsの同時使用をどのように定義していますか?

Citrix Virtual Apps and Desktopsの同時接続モデルでは、任意のユーザーと任意のデバイスに対して、無制限の数の仮想アプリとデスクトップへの1つの接続を許可します。ライセンスはアクティブなセッション中にのみ消費されます。セッションが切断または終了した場合、ライセンスは再発行のためにプールに戻されます。詳細については、「同時接続ライセンス」を参照してください。

共通のライセンスサーバーにCitrix Virtual Apps and Desktopsライセンスの複数のエディションを展開できますか?

はい。ライセンスサーバーは、Citrix Virtual AppsとCitrix Virtual Desktopsの両方のライセンスを同時に管理します。最新のライセンスサーバーバージョンをインストールすることをお勧めします。お使いのライセンスサーバーのバージョンが最新であるか不明な場合は、Citrixダウンロードサイトの番号とご自身のバージョンを比較して確認してください。

単一のサイトでCitrix Virtual AppsとCitrix Virtual Apps and Desktopsの両方のライセンスを使用できます?

バージョンによっては、単一のCitrix Virtual AppsまたはCitrix Virtual Apps and Desktopsサイトで、ユーザー/デバイスまたは同時接続の両方のライセンスモデルをサポートできます。単一のCitrix Virtual AppsまたはCitrix Virtual Apps and Desktopsサイトは、1つのエディションのみをサポートできます。詳細については、「マルチタイプライセンス」を参照してください。

マルチタイプライセンスをサポートする最小バージョンは、XenAppおよびXenDesktop 7.15 Long Term Service Release (LTSR) とCitrix Virtual Apps and Desktops 7 1808です。

ライセンスサーバーにCitrix Virtual Apps and Desktopsユーザー/デバイスまたはCitrix Virtual Apps and Desktops同時接続ライセンスがインストールされている場合、製品モデルとしてCitrix Virtual Apps同時接続を選択できます?

Citrix Virtual AppsをCitrix Virtual Apps and Desktops AdvancedまたはPremium Editionの機能として使用する場合、Citrix Virtual Appsのライセンスモデルは、Citrix Virtual Apps and DesktopsのAdvancedまたはPremium Editionと同じになります。Citrix Virtual Apps and Desktopsを購入した場合、Citrix Virtual Appsの機能のみを使用する予定であっても、ライセンスをCitrix Virtual Apps and Desktopsとして構成してください。製品モデルとしてCitrix Virtual Appsを選択するのは、ライセンスサーバーにCitrix Virtual Apps同時接続スタンドアロンライセンスがインストールされている場合のみです。

各Citrix Virtual AppsおよびCitrix Virtual Apps and Desktopsエディションには、どのような製品コンポーネントが含まれていますか?

エディションごとの全機能マトリックスについては、「Citrix Virtual Apps and Desktopsの機能」を参照してください。

Citrix Virtual Apps and Desktops EULAに準拠して、Citrix Virtual Desktops™環境のライセンスを付与するにはどうすればよいですか?

Citrix Virtual Apps and Desktops EULAに準拠して、ユーザー/デバイスまたは同時接続ライセンスモデルでCitrix Virtual Apps and Desktopsを展開するには、ライセンスファイルをライセンスサーバーに適用します。ライセンスサーバーは、ライセンスコンプライアンスを制御および監視します。購入した製品に基づいて製品を構成することをお勧めします。たとえば、Citrix Virtual Apps

and Desktops Premiumを購入したが、Citrix Virtual Apps機能のみを使用したい場合は、コンプライアンスを満たすために製品をCitrix Virtual Apps and Desktopsに構成してください。詳細については、「製品ライセンスコンプライアンスセンター」を参照してください。

Citrix Virtual Apps EULAに準拠して、Citrix Virtual Apps環境のライセンスを付与するにはどうすればよいですか?

Citrix Virtual Apps EULAに準拠して、同時接続ライセンスモデルでCitrix Virtual Appsを展開するには、ライセンスファイルをライセンスサーバーに適用します。ライセンスサーバーは、ライセンスコンプライアンスを制御および監視します。

Citrix Virtual Apps and Desktopsのサービスオプション（Long Term Service Release (LTSR) またはCurrent Release (CR)）にライセンス要件はありますか?

長期サービスリリースなどのCitrix Virtual Apps and Desktops Servicing Optionsは、Customer Success Servicesプログラムの特典です。LTSRの特典を利用するには、アクティブなCustomer Success Servicesが必要です。詳細については、「[Citrix Virtual Apps、Citrix Virtual Apps and Desktops、およびCitrix Hypervisor Servicing Options」を参照してください。

Remote Browser Isolation (RBI) サービスのプールされた時間はどのように機能しますか?

サービスを25ユーザー以上購入すると、すべてのユーザーで共有される5000時間のサービス利用権が付与されます。その後のユーザー権限の購入によって、プールされた時間の権利が増えることはありません。サービス時間の権利を増やすには、アドオンパックを購入してください。

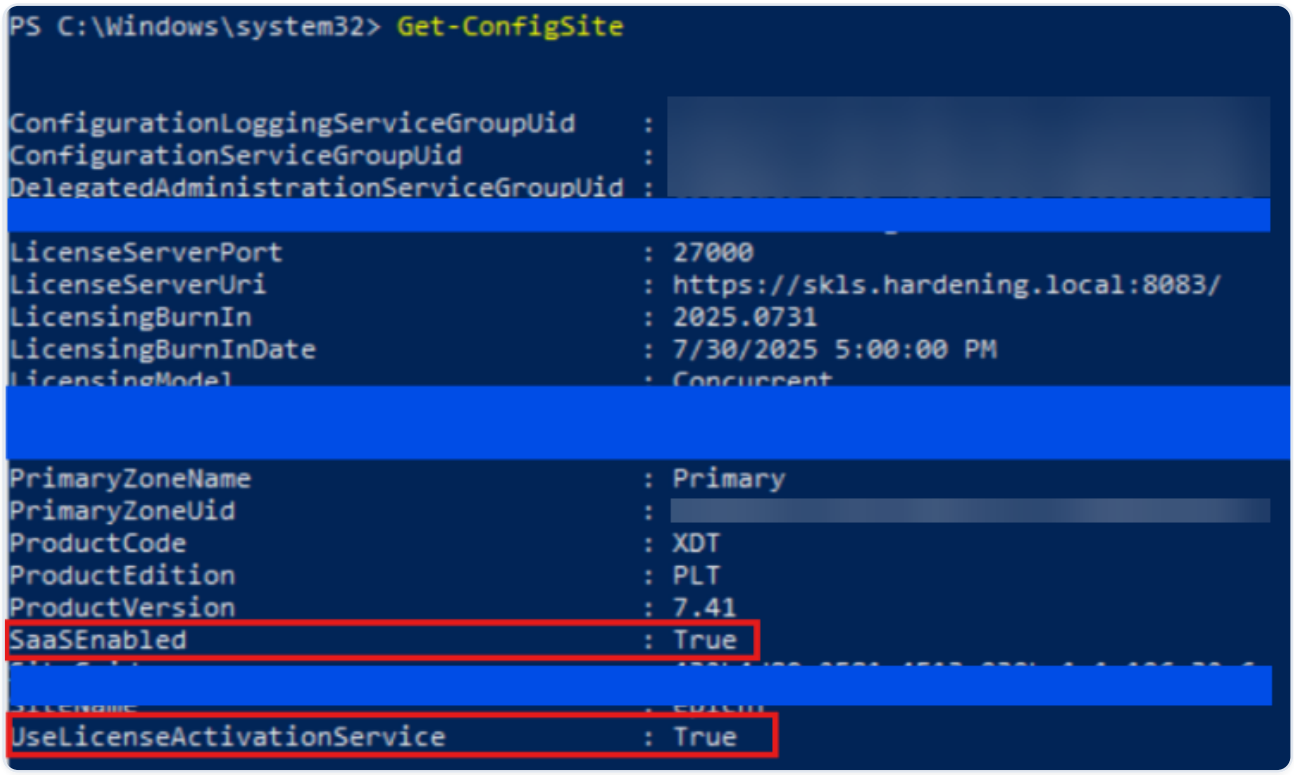
CCUライセンスでRemote PC Accessを使用できますか?

はい。

Remote PC Accessの詳細については、「Remote PC Access」を参照してください。

サイトのLASの状態を確認するにはどうすればよいですか?

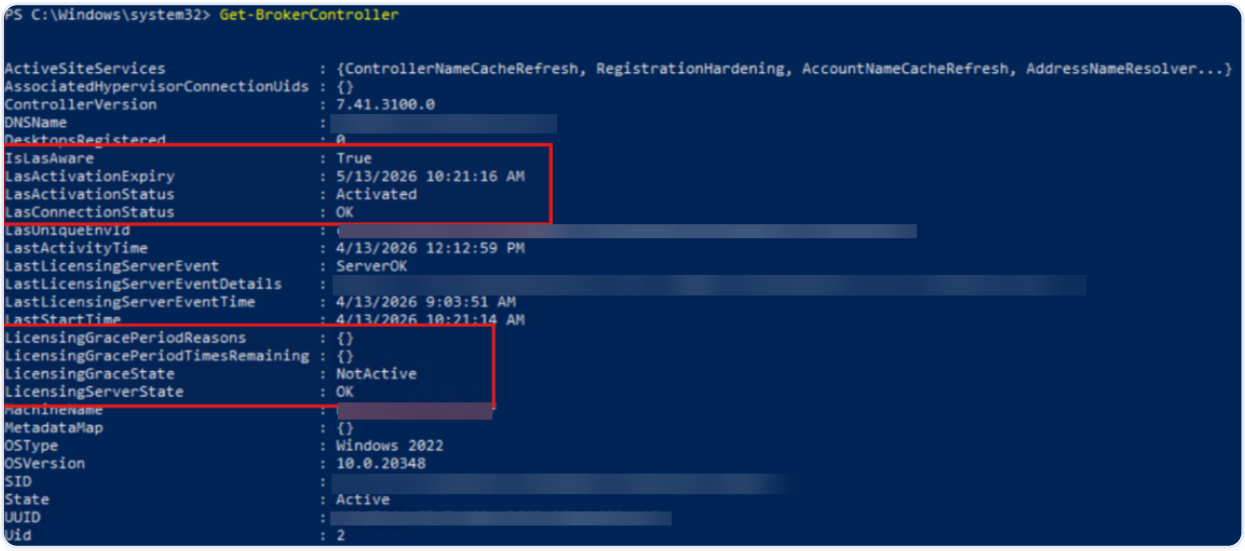
LASアクティベーションの状態とSaaSビットのステータスを確認するには、`Get-configsite`を実行します。



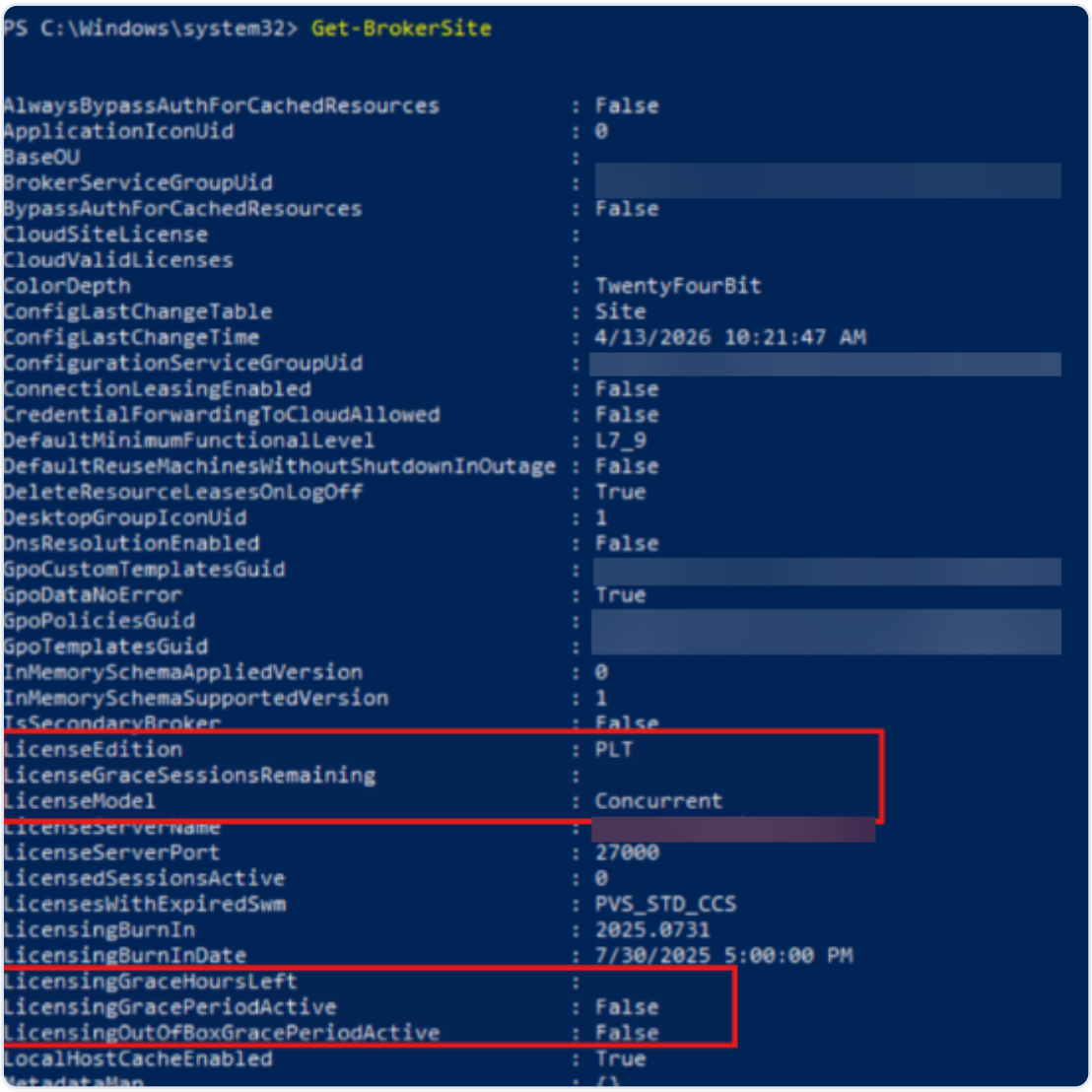
サイトがライセンスキャッシュモードになっているか確認するにはどうすればよいですか?

キャッシュモードと残り時間の詳細を取得するには、`Get-Brokercontroller`と`Get-brokersite`を実行します。

- `Get-Brokercontroller`出力：



- `Get-brokersite`出力：



コマンドの詳細については、以下を参照してください。

- Get-BrokerController
- Get-ConfigSite

ライセンスに関するDelivery Controllerのイベントビューアーログについては、「ライセンスイベントに関連するイベントビューアーログ」を参照してください。

ユーザー/デバイスライセンス

Citrixは、ユーザー/デバイスライセンスモデルでユーザーにライセンスをどのように割り当てますか?

ユーザー/デバイスライセンスモデルでは、ライセンスサーバーはライセンスを一意のユーザーIDに割り当てます。これにより、その単一ユーザーは無制限のデバイスから無制限の接続を行うことができます。ユーザーがデスクトップまたはデバイスに接続する場合、仮想デスクトップまたはアプリケーションにアクセスするには、そのユーザーに割り当てられた1つのライセンスが必要で

す。ライセンスサーバーまたはクラウドサービスがライセンスを割り当てます。これらのライセンスを手動で割り当てることはできません。ライセンスは共有デバイスではなく、ユーザーに割り当てられます。一度ライセンスが割り当てられると、90日間非アクティブになるまで、別のユーザーに割り当てることはできません。詳細については、「ユーザー/デバイスライセンス」を参照してください。

Citrixは、ユーザー/デバイスライセンスモデルでライセンスデバイスをどのように定義しますか?

ライセンスデバイスには、一意のエンドポイントデバイスIDが必要です。ユーザー/デバイスモデルでは、デバイスとは、Citrix Virtual Apps and Desktopsのインスタンスにアクセスするために、個人が使用することを承認したあらゆる機器を指します。共有デバイスの場合、単一のCitrix Virtual Apps and Desktopsユーザー/デバイスライセンスで、デバイスを共有する複数のユーザーをサポートできます。たとえば、共有デバイスは、教室のワークステーションや病院の臨床ワークステーションなどです。

Citrix Virtual Desktops Standard Editionの同時使用ライセンスをユーザー単位とデバイス単位のモデルに変換できますか?

Citrix Virtual Desktops Standard Editionの同時使用ライセンスをCitrix Virtual Desktops Standard Editionのユーザー/デバイスライセンスに変換することはできません。同様に、Citrix Virtual Desktops Standard Editionのユーザー/デバイスライセンスをCitrix Virtual Desktops Standard Editionの同時使用ライセンスに変換することもできません。

Citrix Virtual Desktops Standard Editionの同時使用ライセンスをお持ちで、ユーザー/デバイスライセンスモデルをご希望の場合は、Citrix Virtual Apps and Desktops AdvancedまたはPremium Editionにアップグレードしてください。

元	STANDARD同時使用へ	STANDARDユーザー/デバイスへ	ADVANCEDユーザー/デバイスへ	PREMIUMユーザー/デバイスへ
Citrix Virtual Desktops Standard Editionの同時使用ライセンス	該当なし	同時使用からユーザー/デバイスへの変換は許可されていません	ライセンスモデルを変換することはできませんが、Citrix Virtual Apps and Desktops AdvancedまたはPremium Editionにアップグレードすることはできます。	ライセンスモデルを変換することはできませんが、Citrix Virtual Apps and Desktops AdvancedまたはPremium Editionにアップグレードすることはできます。

元	STANDARD同時使用へ	STANDARDユーザー/デバイスへ	ADVANCEDユーザー/デバイスへ	PREMIUMユーザー/デバイスへ
シトリックス バーチャル デスクトップス スタンダード エディション ユーザー/デバイス ライセンス	ユーザー/デバイスから同時使用への変換は許可されていません	該当なし	該当なし	該当なし

同時使用ライセンスとユーザー/デバイスライセンスの違い?

同時使用ライセンスは、デバイスの同時接続に基づいています。同時使用ライセンスは、デバイスがアクティブな接続を確立している場合にのみ使用されます。接続が終了すると、同時使用ライセンスはすぐに使用可能なライセンスプールに戻されます。このライセンスモデルは、一時的な使用におすすめです。ユーザー/デバイスライセンスは一定期間リースされ、リース期間が終了するまで他のユーザーは利用できません。

ユーザー/デバイスモデルにおける、同じ企業内でのユーザーとデバイスへのライセンス割り当て?

はい。両方のタイプを同じ企業内で使用できます。ライセンスサーバーは、使用状況に基づいてユーザーまたはデバイスにライセンスを最適に割り当てます。これらのライセンスを手動で割り当てることはできません。

ライセンスを付与するユーザーまたはデバイスの数をどのように決定すればよいですか?

適切なライセンス数を決定するために、ユースケースの要件を評価してください。ユーザー/デバイスライセンスは、無制限の数のデバイスから無制限の仮想デスクトップと仮想アプリへの無制限のアクセスを可能にします。同時使用ライセンスは、無制限の数のユーザーが使用できる単一のデバイスから無制限の仮想デスクトップと仮想アプリへの無制限のアクセスを可能にします。次の式を考慮してください。

```
(Number of total users) – (number of users that only access exclusively

 with shared devices) + (number shared devices) = total number

 of licenses to buy.



For example, there are 1000 total users at the hospital. If 700 of them
access only
```

```
Citrix Virtual Desktops from 300 shared devices in the hospital, the
number of

licenses to purchase is 1000 – 700 + 300 = 600 licenses.
```

ユーザー/デバイスモデルでは、ライセンスを持つユーザーが自分の環境に接続するために使用できるデバイスの最大数はいくつですか?

各ライセンスユーザーは、接続されているかオフラインであるかにかかわらず、無制限のデバイスを使用できます。

ユーザー/デバイスモデルでは、ライセンスデバイスにアクセスできるユーザーの最大数?

各ライセンスデバイスは、組織内で無制限のユーザーにサービスを提供できます。

ユーザー/デバイスモデルでは、ライセンスユーザーが一度に利用できる仮想デスクトップまたはRBI Webアプリケーションの最大数?

各ライセンスユーザーは、無制限の仮想デスクトップまたはWebアプリケーションに接続できます。

既存のCitrix Virtual Apps and Desktops環境で、ライセンスユーザー/デバイスの数を増やすためにCitrix Virtual Apps and Desktopsライセンスを購入できますか?

はい。既存のCitrix Virtual Apps and Desktops環境で、ライセンスユーザー/デバイスの数を増やすためにCitrix Virtual Apps and Desktopsライセンスを購入できます。

承認されたユーザー/デバイスライセンスを解放するにはどうすればよいですか?

承認されたユーザー/デバイスの割り当てを解放するには、EULAの条項に従って`udadmin`ユーティリティを使用します。その後、ライセンスサーバーは次の適切なユーザー/デバイスにライセンスを割り当てます。詳細については、「ユーザーまたはデバイスのライセンスの表示または解放」を参照してください。

購入したユーザー/デバイスライセンス数を超過した場合、どうなりますか?

ユーザー/デバイスライセンスには10%の超過分が含まれており、これはライセンスが生成される際に含まれます。この超過分は、インストール済みのライセンス数にも含まれます。使用量の急増が、超過分を含むインストール済みの数を超えた場合、追加ユーザーのアクセスは拒否されます。より多くのユーザーがアクセスできるように、新しいライセンスを購入して展開してください。

ライセンスの超過分を含め、すべてのライセンスが使用されている場合、ライセンスバーストモードにより、製品への無制限の接続が可能になります。ライセンスバーストモードは、最大ライセンス数を超過した理由を特定し、ユーザーを中断することなく追加のライセンスを購入する時間を

与えます。この期間は、15日が経過するか、追加の小売ライセンスをインストールするかのいずれか早い方まで続きます。詳細については、「ライセンスバーストモード」を参照してください。

Directorはライセンスキャッシュモードの状態を表示します。詳細については、「Directorダッシュボードのパネル」を参照してください。

ライセンスユーザーが一度に利用できる仮想アプリケーションの最大数はいくつですか?

各ライセンスユーザーは、無制限の仮想アプリケーションに接続できます。

ライセンスユーザーが組織を離れた場合、どうなりますか?

既存のライセンスユーザーが組織を離れる場合、Citrix に通知することなく、そのユーザーのライセンスを解放できます。ライセンスを解放するには、`udadmin` ユーティリティを使用します。ライセンスを解放しない場合、ライセンスサーバーは 90 日間アクティビティがないと自動的にライセンスを解放します。この情報は、EULA に指定されている条件に従います。

ライセンスユーザーが長期間不在の場合、どうなりますか?

既存のライセンスユーザーが長期間不在の場合、Citrix に通知することなくライセンスを解放し、再割り当てできるようにすることができます。ライセンスを解放するには、`udadmin` ユーティリティを使用します。

組織内のライセンスデバイスを交換した場合、どうなりますか?

既存のライセンスデバイスを交換する場合、Citrix に通知することなくライセンスを解放し、再割り当てできるようにすることができます。ライセンスを解放するには、`udadmin` ユーティリティを使用します。

ライセンスデバイスが長期間サービス停止した場合、どうなりますか?

既存のライセンスデバイスが長期間サービス停止した場合、Citrix に通知することなくライセンスを解放し、再割り当てできるようにすることができます。ライセンスを解放するには、`udadmin` ユーティリティを使用します。ライセンスを解放しない場合、ライセンスサーバーは 90 日間アクティビティがないと自動的にライセンスを解放します。この情報は、EULA に指定されている条件に従います。

ライセンスをデバイスまたはユーザーに割り当てた後で、ユーザーライセンスをデバイスライセンスに、またはその逆に切り替えることはできますか?

はい、可能です。この変更は自動的に行われます。ライセンスサーバーは、使用パターンに基づいてライセンスをユーザーまたはデバイスのいずれかに割り当てます。使用パターンが変更された場合、ライセンスサーバーは新しい使用状況に基づいて割り当てを切り替えることがあります。ライセンスサーバーは常に、お客様にとって最も経済的な方法でライセンスを割り当てます。また、ライセンスサーバーは、90 日間の割り当て期間が経過した後に**未使用**のライセンスを特定するため

にライセンスを監視します。90 日間の割り当て期間後に未使用と識別されたライセンスは、他のユーザーまたはデバイスに再割り当てできます。

同時使用ライセンス

同時使用モデルでは、Citrix Virtual Apps and Desktops のライセンスユーザーが一度に消費できる仮想デスクトップの最大数はいくつですか?

エンドポイントは多数のユーザーにサービスを提供でき、無制限の接続を許可します。

以前のバージョンの Citrix Virtual Apps and Desktops の同時使用ライセンスと、新しいユーザー/デバイスライセンスまたは同時使用ライセンスを、単一のライセンスサーバーに展開できます?

はい。同じライセンスサーバーを使用して、ユーザー/デバイスまたは同時使用ライセンスの展開をサポートし続けることができます。

単一のライセンスサーバーに、同時使用ライセンスとユーザー/デバイスライセンス、または同時使用ライセンスを展開できます?

はい。引き続き同じライセンスサーバーを使用して、同時使用ライセンスとユーザー/デバイスライセンス、または同時使用ライセンスの展開をサポートできます。

Citrix Virtual Apps and Desktops AdvancedおよびPremiumエディションには、Citrix Virtual Appsの同時使用ライセンスが含まれていますか?

Citrix Virtual Apps and Desktops AdvancedおよびPremiumのユーザー/デバイスライセンスには、互換性のためのみにCitrix Virtual Appsの同時使用ライセンスが含まれています。これらの同時使用ライセンスは、ユーザー/デバイスライセンスと互換性のない以前の製品バージョンでのみ使用できます。ユーザー/デバイスライセンスに含まれる同時使用互換ライセンスの使用は、XenApp 6.5より前のバージョンおよびXenDesktop 5.0 Service Pack 1より前のバージョンでのみ許可されます。

購入した同時使用ライセンス数を超過した場合、どうなりますか?

すべてのライセンスが使用中の場合、ライセンスバーストモードにより、製品への無制限の接続が可能になります。ライセンスバーストモードは、最大ライセンス数を超過した理由を特定し、ユーザーを中断することなく追加のライセンスを購入するための時間を提供します。この期間は、15日が経過するか、追加のリテールライセンスをインストールするかのいずれか早い方まで続きます。詳細については、ライセンスバーストモードを参照してください。

Directorはライセンスキャッシュモードの状態を表示します。詳細については、Directorダッシュボードのパネルを参照してください。

超過ライセンス

超過ライセンスはどのように入手できますか?

ユーザー/デバイス、ユーザー、またはデバイスライセンスモデルをサポートする製品（Citrix Cloudを除く）には、アクセス拒否を防ぐために限られた数の追加ライセンスを使用できるライセンス超過機能が含まれています。当社は、超過機能をライセンスエンタイトルメントとしてではなく、便宜のために提供しています。同時使用ライセンスおよびサーバーライセンスには超過機能は含まれていません。使用された超過ライセンスは、初回使用から30日以内に購入する必要がありますが、使用期間は30日に限定されません。Citrixは、新しい製品リリースで超過機能を削除する権利を留保します。詳細については、ライセンス超過を参照してください。

ライセンス超過をどのように識別できますか?

Citrix Licensing Managerで、超過しているライセンス数を含む使用状況情報を表示できます。Studioにも超過使用状況情報が含まれています。

超過ライセンスが消費されるとどうなりますか?

Citrix Virtual Apps and Desktops環境へのアクセスを有効にするために、インストールされているライセンスからライセンスが割り当てられます。この超過ライセンスは、他のライセンスと同等のアクセスと機能を提供します。

超過ライセンスが消費されたときにアラートを受け取ることはできますか?

現在、オーバードラフトライセンスが消費されたときに提供される特定の警告はありません。

オーバードラフトライセンスはどのくらいの期間消費できます?

最初に使用してから30日以内に使用されたオーバードラフトライセンスを購入してください。

その他の製品固有のライセンス情報

- シトリックス ADC
- シトリックス クラウド
- シトリックス エンドポイント マネジメント
- シトリックス ゲートウェイ
- シトリックス ハイパーバイザー
- シトリックス ライセンシング

アプリケーション

はじめに

展開でデリバリーグループのみを使用している場合（アプリケーショングループは使用しない場合）、アプリケーションはデリバリーグループに追加します。アプリケーショングループも使用している場合は、通常、代わりにアプリケーショングループにアプリケーションを追加します。このガイダンスにより、管理が容易になります。アプリケーションは常に少なくとも1つのデリバリーグループまたはアプリケーショングループに属している必要があります。

アプリケーションの追加ウィザードでは、1つ以上のデリバリーグループ、または1つ以上のアプリケーショングループを選択できますが、両方は選択できません。後でアプリケーションのグループ関連付けを変更することはできますが（たとえば、アプリケーショングループからデリバリーグループにアプリケーションを移動するなど）、ベストプラクティスでは、そのような複雑さを追加することは推奨されません。アプリケーションは1種類のグループに保持してください。

アプリケーションを複数のグループに関連付ける場合、それらのすべてのグループでアプリケーションを表示するのに十分な権限がないと、可視性の問題が発生する可能性があります。そのような場合は、より高い権限を持つ管理者に相談するか、アプリケーションが関連付けられているすべてのグループを含むようにスコープを拡張してください。

同じ名前のアプリケーションを2つ（異なるグループからである可能性もあります）同じユーザーに公開する場合、Studioで`Application name (for user)`プロパティを変更してください。そうしないと、ユーザーはCitrix Workspace™アプリで重複した名前を目にすることになります。

アプリケーションのプロパティ（設定）は、追加時または後で変更できます。アプリケーションが配置されているアプリケーションフォルダーも、アプリケーションの追加時または後で変更できます。

詳細については、以下を参照してください。

- デリバリーグループの作成
- アプリケーショングループの作成
- タグ

アプリケーションの追加

デリバリーグループまたはアプリケーショングループを作成するときにアプリケーションを追加できます。これらの手順については、デリバリーグループの作成およびアプリケーショングループ

の作成で詳しく説明されています。次の手順では、グループ作成後にアプリケーションを追加する方法について説明します。

知っておくと良いこと:

- Remote PC Accessデリバリーグループにアプリケーションを追加することはできません。
- アプリケーションの追加ウィザードを使用して、デリバリーグループまたはアプリケーショングループからアプリケーションを削除することはできません。これは別の操作です。

1つ以上のアプリケーションを追加するには：

1. Studioのナビゲーションペインで**アプリケーション**を選択し、アクションペインで**アプリケーションの追加**を選択します。
2. アプリケーションの追加ウィザードが**はじめに**ページとともに起動します。このページは、今後のウィザードの起動時に表示しないように設定できます。
3. ウィザードは、**グループ**、**アプリケーション**、**概要**の各ページを案内します。各ページの作業が完了したら、**概要**ページに到達するまで**次へ**をクリックします。

単一のデリバリーグループまたはアプリケーショングループにアプリケーションを追加する場合の、手順1の代替方法：

- **アプリケーションを1つのデリバリーグループのみに追加するには：** 手順1で、Studioのナビゲーションペインで**デリバリーグループ**を選択し、中央のペインでデリバリーグループを選択してから、アクションペインで**アプリケーションの追加**を選択します。ウィザードには**グループ**ページが表示されません。
- **アプリケーションを1つのアプリケーショングループのみに追加するには：** 手順1で、Studioのナビゲーションペインで**アプリケーション**を選択し、中央のペインでアプリケーショングループを選択してから、アクションペインでアプリケーショングループ名の下にある**アプリケーションの追加**エントリを選択します。ウィザードには**グループ**ページが表示されません。

グループページ

このページには、サイト内のすべてのデリバリーグループが一覧表示されます。アプリケーショングループも作成している場合は、アプリケーショングループとデリバリーグループが一覧表示されます。どちらかのグループを選択できますが、両方のグループを選択することはできません。つまり、アプリケーショングループとデリバリーグループに同時にアプリケーションを追加することはできません。通常、アプリケーショングループを使用している場合は、デリバリーグループではなくアプリケーショングループにアプリケーションを追加します。

アプリケーションを追加するときは、少なくとも1つのデリバリーグループ（または、利用可能な場合はアプリケーショングループ）の横にあるチェックボックスをオンにします。すべてのアプリケーションは、常に少なくとも1つのグループに関連付けられている必要があります。

アプリケーションページ

追加をクリックして、アプリケーションソースを表示します。

- **スタートメニューから：** 選択したデリバリーグループ内のマシンで検出されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストを含む新しいページが起動します。追加するアプリケーションのチェックボックスをオンにして、**OK**をクリックします。

  このソースは、(1)関連付けられたデリバリーグループがないアプリケーショングループを選択した場合、(2)関連付けられたデリバリーグループにマシンが含まれていないアプリケーショングループを選択した場合、または(3)マシンが含まれていないデリバリーグループを選択した場合は、選択できません。
- **手動で定義：** サイト内またはネットワーク内の他の場所にあるアプリケーション。このソースを選択すると、新しいページが起動します。実行可能ファイルへのパス、作業ディレクトリ、オプションのコマンドライン引数、管理者およびユーザーの表示名を入力します。この情報を入力したら、**OK**をクリックします。
- **既存:** 以前サイトに追加されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストを含む新しいページが起動します。追加するアプリケーションのチェックボックスを選択し、**OK**をクリックします。

  サイトにアプリケーションがない場合、このソースは選択できません。
- **App-V：** App-Vパッケージ内のアプリケーション。このソースを選択すると、App-Vサーバーまたはアプリケーションライブラリを選択する新しいページが起動します。表示された画面から、追加するアプリケーションのチェックボックスを選択し、**OK**をクリックします。詳しくは、「App-V」を参照してください。

  App-Vがサイト用に構成されていない場合、このソースは選択できません。
- **アプリケーショングループ**: アプリケーショングループ。このソースを選択すると、アプリケーショングループのリストを含む新しいページが起動します。（表示には各グループ内のアプリケーションもリストされますが、個々のアプリケーションではなくグループのみを選択できます。）選択したグループ内の現在および将来のすべてのアプリケーションが追加されます。追加するアプリケーショングループのチェックボックスを選択し、**OK**をクリックします。

このソースは、(1) アプリケーショングループがない場合、または (2) 選択したデリバリーグループがアプリケーショングループをサポートしていない場合（たとえば、静的に割り当てられたマシンを持つデリバリーグループ）には選択できません。

表に示されているように、**追加**リストの一部のソースは、そのタイプの有効なソースがない場合、選択できません。互換性のないソース（たとえば、アプリケーショングループにアプリケーショングループを追加できないなど）はリストに含まれません。選択したグループに既に追加されているアプリケーションは選択できません。

このページまたは後で、アプリケーションのプロパティ（設定）を変更できます。

デフォルトでは、追加されたアプリケーションは`Applications`という名前のアプリケーションフォルダーに配置されます。アプリケーションはこのページから、または後で変更できます。同じ名前のアプリケーションが同じフォルダーに存在する場合にアプリケーションを追加しようとすると、追加しようとしているアプリケーションの名前を変更するよう求められます。提示された新しい名前を受け入れるか、拒否してアプリケーションの名前を変更するか、別のフォルダーを選択できます。たとえば、**アプリケーション**フォルダーに`app`が既に存在し、そのフォルダーに`app`という名前の別のアプリケーションを追加しようとすると、新しい名前`app_1`が提示されます。

概要ページ

10個以下のアプリケーションを追加する場合、その名前は**追加するアプリケーション**にリストされます。10個を超えるアプリケーションを追加する場合、合計数が指定されます。

概要情報を確認し、**「完了」**をクリックします。

アプリケーションのグループ関連付けを変更する

アプリケーションを追加した後、そのアプリケーションが関連付けられているデリバリーグループとアプリケーショングループを変更できます。

アプリケーションを別のグループにドラッグできます。これは、アクションペインのコマンドを使用する代わりの方法です。

アプリケーションが複数のデリバリーグループまたはアプリケーショングループに関連付けられている場合、グループの優先順位を使用して、複数のグループがアプリケーションを検索するためにチェックされる順序を指定できます。デフォルトでは、すべてのグループの優先順位は0（最高）です。同じ優先順位のグループは負荷分散されます。

アプリケーションは、アプリケーションを配信できる共有（プライベートではない）マシンを含むデリバリーグループに関連付けることができます。また、共有マシンを含むデリバリーグループがデスクトップのみを配信する場合でも、(1) デリバリーグループに共有マシンが含まれており、XenDesktop 7.xバージョン7.9より前に作成された場合、および (2) `Edit delivery group` 権限がある場合は、そのデリバリーグループを選択できます。プロパティダイアログがコミットされると、デリバリーグループの種類は自動的に `desktops and applications` に変換されます。

1. Studioのナビゲーションペインで**アプリケーション**を選択し、中央のペインでアプリケーションを選択します。
2. アクションペインで**プロパティ**を選択します。
3. **「グループ」**ページを選択します。
    - グループを追加するには、**「追加」をクリックし、「アプリケーショングループ」または「デリバリーグループ」を選択します。（アプリケーショングループを作成していない場合、唯一の項目は**「デリバリーグループ」**です。）次に、1つ以上の利用可能なグループを選択します。アプリケーションと互換性のないグループ、またはすでにアプリケーションに関連付けられているグループは選択できません。
    - グループを削除するには、1つ以上のグループを選択し、**「削除」**をクリックします。グループの関連付けを削除した結果、アプリケーションがどのグループとも関連付けられなくなる場合、アプリケーションが削除されることを警告されます。
    - グループの優先度を変更するには、グループを選択し、**「優先度の編集」をクリックします。優先度値を選択し、**「OK」**をクリックします。
4. 完了したら、**「適用」をクリックして変更を適用し、ウィンドウを開いたままにするか、**「OK」**をクリックして変更を適用し、ウィンドウを閉じます。

アプリケーションの複製、有効化または無効化、名前の変更、または削除

次のアクションが利用可能です。

- **複製：** 異なるパラメーターまたはプロパティを持つ別のバージョンを作成するために、アプリケーションを複製したい場合があります。アプリケーションを複製すると、一意のサフィックスで自動的に名前が変更され、元のアプリケーションの隣に配置されます。また、アプリケーションを複製してから、別のグループに追加したい場合もあります。（複製後、アプリケーションを移動する最も簡単な方法はドラッグすることです。）
- **有効化または無効化：** アプリケーションの有効化と無効化は、デリバリーグループまたはアプリケーショングループの有効化と無効化とは異なるアクションです。

- **名前の変更：** 一度に1つのアプリケーションのみ名前を変更できます。アプリケーションの名前を変更しようとして、同じ名前のアプリケーションが同じフォルダーまたはグループに存在する場合、別の名前を指定するように求められます。
- **削除：** アプリケーションを削除すると、関連付けられていたデリバリーグループおよびアプリケーショングループから削除されますが、元々アプリケーションを追加するために使用されたソースからは削除されません。アプリケーションの削除は、デリバリーグループまたはアプリケーショングループから削除するのとは異なるアクションです。

アプリケーションを複製、有効化、無効化、名前変更、または削除するには：

1. Studioのナビゲーションペインで**アプリケーション**を選択します。
2. 中央のペインで1つ以上のアプリケーションを選択し、アクションペインで適切なタスクを選択します。
3. プロンプトが表示されたら、アクションを確認します。

デリバリーグループからアプリケーションを削除する

アプリケーションは、少なくとも1つのデリバリーグループまたはアプリケーショングループに関連付けられている（属している）必要があります。アプリケーションをデリバリーグループから削除しようとして、そのアプリケーションがどのデリバリーグループまたはアプリケーショングループとの関連付けも失われる場合、続行するとアプリケーションが削除されることが通知されます。その場合、そのアプリケーションを配信したい場合は、有効なソースから再度追加する必要があります。

1. Studioのナビゲーションペインで**［デリバリーグループ］**を選択します。
2. デリバリーグループを選択します。中央下のペインの タブで、削除するアプリケーションを選択します。
3. アクションペインから**アプリケーションの削除**を選択します。
4. 削除を確認します。

アプリケーショングループからアプリケーションを削除する

アプリケーションは、少なくとも1つのデリバリーグループまたはアプリケーショングループに属している必要があります。アプリケーションをアプリケーショングループから削除しようとしたときに、そのアプリケーションがどのグループにも属さなくなる場合、続行するとアプリケーションが削除されるという通知が表示されます。その場合、そのアプリケーションを配信したい場合は、有効なソースから再度追加する必要があります。

1. Studioナビゲーションペインで**アプリケーション**を選択します。

2. 中央のペインでアプリケーショングループを選択し、1つまたは複数のアプリケーションを選択します。
3. アクションペインで**アプリケーショングループから削除**を選択します。
4. 削除を確認します。

アプリケーションのプロパティを変更する

アプリケーションのプロパティは、一度に1つしか変更できません。

アプリケーションのプロパティを変更するには：

1. Studioナビゲーションペインで**アプリケーション**を選択します。
2. アプリケーションを選択し、アクションペインで**アプリケーションプロパティの編集**を選択します。
3. 変更するプロパティが含まれるページを選択します。
4. 完了したら、 をクリックして変更を適用し、ウィンドウを開いたままにするか、 をクリックして変更を適用してウィンドウを閉じます。

次のリストでは、ページが括弧内に表示されます。

プロパティ	ページ
Citrix Workspaceアプリにアプリケーションが表示されるカテゴリまたはフォルダー	配信
コマンドライン引数。「公開アプリケーションへのパラメーターの受け渡し」を参照してください。	場所
アプリケーションが利用可能なデリバリーグループとアプリケーショングループ	グループ
説明	識別
ファイル名拡張子とファイルの種類関連付け：アプリケーションが自動的に開く拡張子	ファイルの種類関連付け
アイコン	配信
StoreFront™のキーワード	識別

プロパティ	ページ
制限; アプリケーション制限の構成を参照	配信
名前: ユーザーおよび管理者に表示される名前	識別
実行可能ファイルへのパス; 公開アプリケーションへのパラメーターの受け渡しを参照	場所
ユーザーのデスクトップ上のショートカット: 有効または無効	配信
可視性: Citrix Workspaceアプリでアプリケーションを表示できるユーザーを制限します。非表示のアプリケーションでも起動できます。利用不可かつ非表示にするには、別のグループに追加します。	可視性の制限
作業ディレクトリ	場所

アプリケーションの変更は、現在のアプリケーションユーザーがセッションからログオフするまで有効にならない場合があります。

アプリケーション制限を構成する

アプリケーションの使用状況を管理するために、アプリケーション制限を構成します。たとえば、アプリケーション制限を使用して、アプリケーションに同時にアクセスするユーザーの数を管理できます。同様に、アプリケーション制限は、リソースを大量に消費するアプリケーションの同時インスタンス数を管理するためにも使用できます。この制限は、サーバーのパフォーマンスを維持し、サービスの劣化を防ぐのに役立ちます。

この機能は、Controller によって仲介されるアプリケーションの起動数（Citrix Workspace アプリや StoreFront からの起動など）を制限するものであり、他の方法で起動できる実行中のアプリケーションの数を制限するものではありません。これは、アプリケーション制限が同時使用を管理する際に管理者を支援するものの、すべてのシナリオで強制力を持つわけではないことを意味します。たとえば、Controller が停止モードの場合、アプリケーション制限は適用できません。

デフォルトでは、同時に実行できるアプリケーションインスタンスの数に制限はありません。アプリケーション制限の設定はいくつかあります。それらのいずれか、またはすべてを構成できます。

- デリバリーグループ内のすべてのユーザーによるアプリケーションの同時インスタンスの最大数。
- デリバリーグループ内のユーザーごとのアプリケーションのインスタンス数（1つ）。
- マシンごとのアプリケーションの同時インスタンスの最大数（PowerShell のみ）。

制限が構成されている場合、ユーザーが構成された制限を超えるアプリケーションインスタンスを起動しようとすると、エラーメッセージが生成されます。複数の制限が構成されている場合、最初に到達した制限でエラーが報告されます。

アプリケーション制限の使用例：

- **同時インスタンス数の最大制限:** デリバリーグループで、アプリケーション `Alpha` の同時インスタンスの最大数を 15 に構成します。その後、そのデリバリーグループのユーザーは、そのアプリケーションのインスタンスを 15 個同時に実行しています。そのデリバリーグループのいずれかのユーザーが `Alpha` を起動しようとすると、エラーメッセージが生成されます。`Alpha` は、構成された同時アプリケーションインスタンス制限（15）を超えるため、起動されません。
- **ユーザーごとのアプリケーションインスタンス数制限:** 別のデリバリーグループで、アプリケーション `Beta` に対してユーザーごとのインスタンス数オプションを有効にします。ユーザーのTonyはアプリケーション `Beta` を正常に起動します。その日の後半、Tonyのセッションでそのアプリケーションがまだ実行されている間に、彼は `Beta` の別のインスタンスを起動しようとします。エラーメッセージが生成され、ユーザーごとのインスタンス数制限を超えるため、 `Beta` は起動されません。
- **同時インスタンス数の最大制限とユーザーごとのインスタンス数制限:** 別のデリバリーグループで、同時インスタンスの最大数を 10 に構成し、アプリケーション `Delta` のユーザーごとのインスタンス数オプションを有効にします。その後、そのデリバリーグループの 10 人のユーザーがそれぞれ `Delta` のインスタンスを実行している場合、そのデリバリーグループの他のユーザーが `Delta` を起動しようとすると、エラーメッセージが表示されます。`Delta` は起動されません。現在の 10 人の `Delta` ユーザーのいずれかがそのアプリケーションの 2 番目のインスタンスを起動しようとすると、エラーメッセージが表示され、2 番目のインスタンスは起動されません。
- **マシンごとの同時インスタンス数の最大制限とタグ制限の使用:** アプリケーション `Charlie` には、特定のサーバーで同時に実行できるインスタンスの数を規定するライセンスおよびパフォーマンス要件があります。これらの要件は、サイト内のすべてのサーバーで同時に実行できるインスタンスの数も規定します。

アプリケーションのインスタンス数/マシン制限は、サイト内のすべてのサーバーに影響します（特定のデリバリーグループ内のマシンだけでなく）。サイトに 3 台のサーバーがあるとします。アプリケーション `Charlie` の場合、マシンあたりのアプリインスタンス制限を 2 に構成します。したがって、サイト全体でアプリケーション `Charlie` のインスタンスは 6 つまでしか起動できません。（これは、3 台のサーバーそれぞれで Charlie のインスタンスが 2 つという制限です。）

アプリケーションの使用をデリバリーグループ内の特定のコンピューターのみに制限するには（サイト全体のすべてのコンピューターでのインスタンス制限に加えて）：

- それらのマシンにタグ付け機能を使用します。
- そのアプリケーションのマシンごとの最大インスタンス数を構成します。

アプリケーションがControllerの仲介以外の方法（たとえば、Controllerが停止モードの場合など）で起動され、構成された制限を超過した場合、ユーザーは制限を超過しないように十分な数のインスタンスを閉じるまで、それ以上のインスタンスを起動できません。制限を超過したインスタンスは強制的にシャットダウンされません。ユーザーが閉じるまで継続して実行が許可されます。

セッションローミングを無効にする場合は、ユーザーごとのアプリケーションインスタンス数制限を無効にします。ユーザーごとのアプリケーションインスタンス数制限を有効にする場合は、新しいデバイスでの新しいセッションを許可する2つの値のいずれも構成しないでください。ローミングについて詳しくは、「セッション」を参照してください。

デリバリーグループごとの最大インスタンス数制限と、ユーザーごとのインスタンス数制限を構成するには：

1. Studioナビゲーションペインで**アプリケーション**を選択し、アプリケーションを選択します。
2. アクションペインで**アプリケーションプロパティの編集**を選択します。
3. **［配信］** ページで、次のいずれかのオプションを選択します。
   - **アプリケーションの無制限の使用を許可する**。同時に実行されるインスタンスの数に制限はありません。これがデフォルトです。
   - **アプリケーションの制限を設定する**。制限の種類は2つあります。いずれかまたは両方を指定します。
     - 同時に実行できるインスタンスの最大数を指定します
     - ユーザーごとにアプリケーションのインスタンスを1つに制限する
4. **［OK］** をクリックして変更を適用し、ダイアログボックスを閉じます。または、 **［適用］** をクリックして変更を適用し、ダイアログボックスを開いたままにします。

マシンごとの最大インスタンス数制限を構成するには（PowerShellのみ）：

- PowerShellで（Citrix Cloud™展開の場合はRemote PowerShell SDKを、オンプレミス展開の場合はPowerShell SDKを使用して）、適切な `BrokerApplication` コマンドレットを `MaxPerMachineInstances` パラメーターとともに指定します。
- ガイダンスについては、`Get-Help` コマンドレットを使用してください。例:

  ```
  Get-Help Set-BrokerApplication –Parameter MaxPerMachineInstances
  ```

公開アプリケーションにパラメーターを渡す

アプリケーションのプロパティの**場所**ページを使用して、コマンドラインを入力し、公開アプリケーションにパラメーターを渡します。

公開アプリケーションをファイルの種類に関連付けると、`“%*”` (二重引用符で囲まれたパーセント記号とアスタリスク記号) がアプリケーションのコマンドラインの末尾に追加されます。これらの記号は、ユーザーデバイスに渡されるパラメーターのプレースホルダーとして機能します。

公開アプリケーションが期待どおりに起動しない場合は、そのコマンドラインに正しい記号が含まれていることを確認してください。デフォルトでは、`“%*”` 記号が追加されると、ユーザーデバイスから提供されるパラメーターが検証されます。ユーザーデバイスから提供されるカスタマイズされたパラメーターを使用する公開アプリケーションの場合、コマンドライン検証をバイパスするために、`“%**”` 記号がコマンドラインに追加されます。アプリケーションのコマンドラインにこれらの記号が表示されない場合は、手動で追加してください。

実行可能ファイルへのパスにスペースを含むディレクトリ名が含まれている場合 (例: `“C:\Program Files”`)、スペースがコマンドラインの一部であることを示すために、アプリケーションのコマンドラインを二重引用符で囲みます。これを行うには、パスを二重引用符で囲み、`%*` 記号を別の二重引用符で囲みます。パスの閉じ引用符と `%*` 記号の開始引用符の間にスペースを含めるようにしてください。

たとえば、公開アプリケーションであるWindows Media Playerのコマンドラインは次のとおりです。

```
“C:\Program Files\Windows Media Player\mplayer1.exe” “%*”
```

> **注：**
>
> 公開アプリケーションを起動するためのコマンドラインの最大文字数 (引数を含む) は203文字です。

アプリケーションフォルダーの管理

デフォルトでは、デリバリーグループに追加する新しいアプリケーションは、**Applications**という名前のフォルダーに配置されます。デリバリーグループの作成時、アプリケーションの追加時、または後で別のフォルダーを指定できます。

知っておくと良いこと:

- Applicationsフォルダーの名前を変更したり削除したりすることはできませんが、その中に含まれるすべてのアプリケーションを、作成した他のフォルダーに移動することはできます。
- フォルダー名には1～64文字を含めることができます。スペースも使用できます。
- フォルダーは最大5レベルまでネストできます。
- フォルダーにアプリケーションを含める必要はありません。空のフォルダーも許可されます。
- フォルダーは、移動するか、作成時に別の場所を指定しない限り、Studioでアルファベット順に表示されます。
- 同じ名前のフォルダーを複数持つことができますが、それぞれ異なる親フォルダーを持つ必要があります。同様に、同じ名前のアプリケーションを複数持つことができますが、それぞれ異なるフォルダーに存在する必要があります。
- フォルダー内のアプリケーションを表示するには`View Applications`権限が必要です。また、アプリケーションを含むフォルダーを削除、名前変更、または削除するには、そのフォルダー内のすべてのアプリケーションに対して`Edit Application Properties`権限が必要です。
- 以下のほとんどの手順では、Studioのアクションペインを使用してアクションを要求します。または、右クリックメニューを使用するか、項目をドラッグすることもできます。たとえば、意図しない場所にフォルダーを作成または移動した場合、ドラッグアンドドロップで正しい場所に移動できます。

アプリケーションフォルダーを管理するには、Studioナビゲーションペインで**アプリケーション**を選択します。以下のリストを参考にしてください。

- **すべてのフォルダー（ネストされたフォルダーを除く）を表示するには：** フォルダーリストの上にある**すべて表示**をクリックします。
- **最上位レベル（ネストされていない）にフォルダーを作成するには: アプリケーション**フォルダーを選択します。新しいフォルダーを**アプリケーション**以外の既存のフォルダーの下に配置するには、そのフォルダーを選択します。次に、アクションペインで**フォルダーの作成**を選択します。名前を入力します。

- **フォルダーを移動するには:** フォルダーを選択し、アクションペインで**フォルダーの移動**を選択します。ネストされたフォルダーが含まれている場合を除き、一度に1つのフォルダーしか移動できません。（フォルダーを移動する最も簡単な方法は、ドラッグすることです。）」
- **フォルダーの名前を変更するには:** フォルダーを選択し、ペインで**フォルダー名の変更**を選択します。名前を入力します。
- **フォルダーを削除するには:** フォルダーを選択し、ペインで**フォルダーの削除**を選択します。アプリケーションや他のフォルダーを含むフォルダーを削除すると、それらのオブジェクトも削除されます。アプリケーションを削除すると、デリバリーグループからのアプリケーション割り当てが削除されます。ただし、マシンからは削除されません。
- **アプリケーションをフォルダーに移動するには:** 1つまたは複数のアプリケーションを選択します。次に、ペインで**アプリケーションの移動**を選択します。フォルダーを選択します。

デリバリーグループまたはアプリケーショングループを作成する際に、**アプリケーション**ページで追加するアプリケーションをフォルダーに配置することもできます。デフォルトでは、追加されたアプリケーションは**アプリケーション**フォルダーに入ります。**変更**をクリックしてフォルダーを選択または作成します。

公開デスクトップでのアプリケーションのローカル起動を制御する

ユーザーが公開デスクトップ内から公開アプリケーションを起動する際、そのデスクトップセッションでアプリケーションを起動するか、公開アプリケーションとして起動するかを制御できます。Citrix Workspaceアプリは、VDA上のWindowsレジストリでアプリケーションのインストールパスを検索し、存在する場合はアプリケーションのローカルインスタンスを起動します。それ以外の場合は、ホストされたアプリケーションのインスタンスが起動されます。VDAにインストールされていないアプリケーションを起動すると、ホストされたアプリケーションが起動されます。詳細については、「vPrefer起動」を参照してください。

PowerShell（Citrix Cloud展開環境ではRemote PowerShell SDK、オンプレミス展開環境ではPowerShell SDKを使用）で、このアクションを変更できます。

`New-Broker` Applicationまたは`Set-BrokerApplication` コマンドレットで、`LocalLaunchDisabled` オプションを使用します。例：

```
Set-BrokerApplication -LocalLaunchDisabled <Boolean>
```

デフォルトでは、このオプションの値はfalse（`-LocalLaunchDisabled $false`）です。公開デスクトップ内から公開アプリケーションを起動すると、そのデスクトップセッション内でアプリケーションが起動されます。

オプションの値をtrue（`-LocalLaunchDisabled $true`）に設定すると、公開アプリケーションが起動されます。これにより、公開デスクトップから公開アプリケーションへの個別の追加セッションが（Citrix Workspaceアプリ for Windowsを使用して）作成されます。

要件と制限：

- アプリケーションの`ApplicationType`の値は`HostedOnDesktop`である必要があります。
- このオプションは、適切なPowerShell SDKを介してのみ利用できます。現在、Studioのグラフィカルインターフェイスでは利用できません。
- このオプションには、StoreFront 3.14、Citrix Receiver for Windows 4.11、およびDelivery Controller 7.17が最低限必要です。

ユニバーサル Windows プラットフォームアプリ

ユニバーサル Windows プラットフォーム (UWP) アプリについては、以下の Microsoft ドキュメントを参照してください。

- ユニバーサル Windows プラットフォーム (UWP) アプリとは
- Windows パッケージマネージャー

要件と制限

Citrix Virtual Apps and Desktops™ は、以下の Windows マシン上の VDA で UWP アプリを使用することをサポートしています。

- Windows 10 以降のバージョン
- Windows Server 2016 以降のバージョン

VDA はバージョン 7.11 以降である必要があります。

UWP アプリを使用する場合、以下の Citrix Virtual Apps and Desktops の機能はサポートされていないか、制限されています。

- ファイルタイプの関連付けはサポートされていません。
- ローカルアプリアクセスはサポートされていません。
- 動的プレビュー：セッションで実行中のアプリが重なっている場合、プレビューにはデフォルトのアイコンが表示されます。動的プレビューに使用される Win32 API は、UWP アプリではサポートされていません。

- アクションセンターのリモート処理：UWP アプリは、セッション内のメッセージを表示するためにアクションセンターを使用できます。これらのメッセージは現在、ユーザーに表示するためにエンドポイントにリダイレクトされません。

同じサーバーから UWP アプリと非 UWP アプリを起動することはサポートされていません。代わりに、UWP アプリと非 UWP アプリを別々のデリバリーグループまたはアプリケーショングループに配置してください。

マシンにインストールされているすべてのUWPアプリが列挙されるため、Citrix®はWindowsストアへのユーザーアクセスを無効にすることを推奨します。これにより、あるユーザーがインストールしたUWPアプリが別のユーザーによってアクセスされるのを防ぎます。

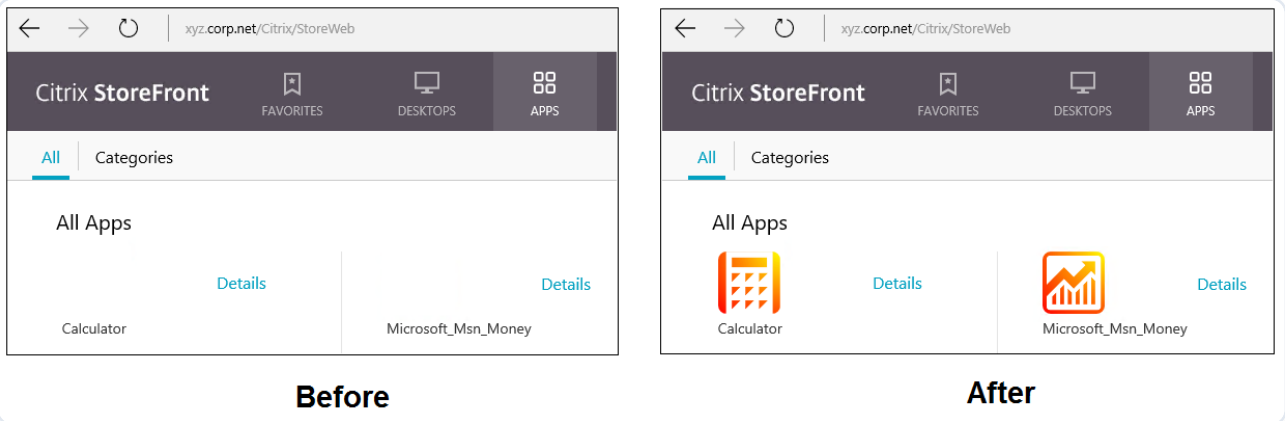
サイドローディング中、UWPアプリはマシンにインストールされ、他のユーザーが使用できるようになります。別のユーザーがアプリを起動すると、アプリがインストールされ、OSはそのAppXデータベースを更新して、そのユーザーによって「インストール済み」であることを示します。

固定またはシームレスウィンドウで起動された公開UWPアプリから開始されたグレースフルログオフは、VDAセッションの終了を妨げ、ユーザーを強制的にログオフさせる可能性があります。このような場合、VDAセッションに残っているいくつかのプロセスが、セッションが適切に終了するのを妨げます。これを解決するには、VDAセッションの終了を妨げているプロセスを特定し、CTX891671のガイダンスに従って、「LogoffCheckSysModules」レジストリキー値に追加します。

UWPアプリのアプリケーション表示名と説明が正しくない場合があります。アプリケーションをデリバリーグループに追加する際に、これらのプロパティを編集して修正してください。

その他の問題については、既知の問題を確認してください。

現在、いくつかのUWPアプリは透明度が有効な白いアイコンを使用しており、StoreFront表示の白い背景に対してアイコンが見えなくなることがあります。この問題を回避するには、背景を変更できます。たとえば、StoreFrontマシンでファイル`C:\inetpub\wwwroot\Citrix\StoreWeb\custom\style.css`を編集します。ファイルの最後に`.storeapp-icon {background-image: radial-gradient( circle at top right, yellow, red ); }`を追加します。次の図は、この例の変更前と変更後を示しています。



Windows Server 2016以降のバージョンでは、UWPアプリの起動時にサーバーマネージャーも起動する場合があります。これを防ぐには、`HKLM\Software\Microsoft\ServerManager\DoNotOpenServerManagerAtLogon`レジストリキーを使用して、ログオン時のサーバーマネージャーの自動起動を無効にします。詳細については、`<https://blogs.technet.microsoft.com/rmilne/2014/05/30/how-to-hide-server-manager-at-logon/>`を参照してください。

UWPアプリのインストールと公開

UWPアプリのサポートはデフォルトで有効になっています。

VDA（またはマスターイメージ）に1つ以上のUWPアプリをインストールするには、次のいずれかの方法を使用します。

- Windows Store for Businessからオフラインインストールを完了し、Deployment Image Servicing and Management (DISM) などのツールを使用してアプリをデスクトップイメージに展開します。詳細については、Windows Package Managerを参照してください。
- アプリをサイドロードします。詳細については、Windows クライアントデバイスで基幹業務 (LOB) アプリをサイドロードするを参照してください。
- 各対象ユーザー向けに、Windows Store for Businessから直接UWPアプリをインストールします。

Citrix Virtual AppsまたはCitrix Virtual Desktops™で1つ以上のUWPアプリを追加（公開）するには：

1. マシンにUWPアプリがインストールされたら、UWPアプリをデリバリーグループまたはアプリケーショングループに追加します。これは、グループの作成時または後で行うことができます。**アプリケーション**ページで、**追加**メニューから**スタートメニューから**を選択します。
2. アプリケーションリストが表示されたら、公開するUWPアプリを選択します。
3. ウィザードを続行するか、編集ダイアログを閉じます。

User Profile Manager (UPM) を使用する際の追加の構成要件については、 Windows Apps - Microsoft Storeを参照してください。

VDAでUWPアプリの使用を無効にするには、`HKLM\Software\Citrix\VirtualDesktopAgent\FeatureToggle`にレジストリ設定 **EnableUWASeamlessSupport** を追加し、**0** に設定します。

UWPアプリのアンインストール

`Remove-AppXPackage`のようなコマンドでUWPアプリをアンインストールすると、その項目は管理者に対してのみアンインストールされます。アプリを起動して使用した可能性のあるユーザーのマシンからアプリを削除するには、各マシンで削除コマンドを実行します。1つのコマンドですべてのユーザーのマシンからAppXパッケージをアンインストールすることはできません。

ゾーン

WANで接続された広範囲に分散した場所にまたがる展開では、ネットワークの遅延と信頼性により課題が生じる可能性があります。これらの課題を軽減する2つのオプションがあります。

- 複数のサイトを展開し、それぞれに独自のSQL Serverサイトデータベースを持たせる。

  このオプションは、大規模なエンタープライズ展開に推奨されます。複数のサイトは個別に管理され、それぞれに独自のSQL Serverサイトデータベースが必要です。各サイトは独立したCitrix Virtual Apps™展開です。

- 単一サイト内に複数のゾーンを構成する。

  ゾーンを構成することで、リモート地域のユーザーがWANの大部分を通過することなくリソースに接続できるようになります。ゾーンを使用すると、単一のCitrix Studioコンソール、Citrix Director、およびサイトデータベースから効果的なサイト管理が可能になります。これにより、リモートロケーションに個別のデータベースを含むより多くのサイトを展開、人員配置、ライセンス供与、および運用するコストを節約できます。

  ゾーンは、あらゆる規模の展開で役立ちます。ゾーンを使用して、アプリケーションとデスクトップをエンドユーザーの近くに配置することで、パフォーマンスを向上させることができます。ゾーンには、冗長性と回復性のために1つ以上のControllerをローカルにインストールできますが、必須ではありません。

  サイトに構成されているControllerの数は、サイト自体に新しいControllerを追加するなどの一部の操作のパフォーマンスに影響を与える可能性があります。これを避けるため、Citrix

Virtual AppsまたはCitrix Virtual Desktops™サイトのゾーン数を50以下に制限することをお勧めします。

ゾーンのネットワーク遅延が250ミリ秒RTTを超える場合は、ゾーンではなく複数のサイトを展開することをお勧めします。

この記事全体を通して、「ローカル」という用語は、議論されているゾーンを指します。たとえば、「VDAがローカルControllerに登録する」とは、VDAがVDAが配置されているゾーン内のControllerに登録することを意味します。

このリリースでのゾーンは、XenAppバージョン6.5以前のゾーンと似ていますが、同一ではありません。たとえば、このゾーンの実装では、データコレクターはありません。サイト内のすべてのControllerは、プライマリゾーンの1つのサイトデータベースと通信します。また、このリリースではフェールオーバーゾーンと優先ゾーンの動作が異なります。

ゾーンの種類

サイトには常に1つのプライマリゾーンがあります。オプションで1つ以上のサテライトゾーンを持つこともできます。サテライトゾーンは、災害復旧、地理的に離れたデータセンター、支店、クラウド、またはクラウド内のアベイラビリティゾーンに使用できます。

プライマリゾーン:

プライマリゾーンのデフォルト名は「Primary」です。このゾーンには、SQL Serverサイトデータベース（および使用されている場合は高可用性SQLサーバー）、Studio、Director、Citrix StoreFront™、Citrix License Server、およびCitrix Gatewayが含まれます。サイトデータベースは常にプライマリゾーンに保持してください。

プライマリゾーンには、冗長性のために少なくとも2つのControllerが必要です。プライマリゾーンには、データベースおよびインフラストラクチャと密接に連携するアプリケーションを持つVDAを配置できます。

サテライトゾーン:

サテライトゾーンには、1つ以上のVDA、Controller、StoreFrontサーバー、およびCitrix Gatewayサーバーが含まれます。通常の運用では、サテライトゾーンのControllerはプライマリゾーンのデータベースと直接通信します。

サテライトゾーン、特に大規模なゾーンには、そのゾーンのマシンをプロビジョニングおよび保存するために使用されるハイパーバイザーが含まれる場合もあります。サテライトゾーンを構成する

際、ハイパーバイザーまたはその他のサービス接続を関連付けることができます。（その接続を使用するカタログがすべて同じゾーンにあることを確認してください。）

サイトには、独自のニーズと環境に基づいて、さまざまな構成のサテライトゾーンを含めることができます。次の図は、プライマリゾーンとサテライトゾーンの例を示しています。

プライマリゾーンとサテライトゾーンの図(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/zones1.png)

図では、次のようになります。

- **プライマリゾーン：** 2つのController、Studio、Director、StoreFront、License Server、およびサイトデータベース（高可用性SQL Server展開を含む）が含まれます。プライマリゾーンには、複数のVDAとCitrix Gatewayも含まれます。
- **サテライトゾーン1: Controllerを持つVDA:** サテライトゾーン1には、Controller、VDA、およびStoreFrontサーバーが含まれます。このサテライトゾーンのVDAは、ローカルのControllerに登録されます。ローカルのControllerは、プライマリゾーンのサイトデータベースおよびライセンスサーバーと通信します。

  WANが失敗した場合、ローカルホストキャッシュ機能により、サテライトゾーンのControllerは、そのゾーンのVDAへの接続の仲介を続行できます。このような展開は、従業員がローカルのStoreFrontサイトとローカルのControllerを使用してローカルリソースにアクセスするオフィスで効果的です。
- **サテライトゾーン2: 冗長Controllerを持つVDA:** サテライトゾーン2には、2つのController、VDA、およびStoreFrontサーバーが含まれます。これは最も回復力のあるゾーンタイプであり、WANとローカルControllerの1つが同時に障害を起こした場合でも保護を提供します。

VDAの登録先とControllerのフェールオーバー先

プライマリゾーンとサテライトゾーンを含むサイトで、VDAの最小バージョンが7.7の場合:

- プライマリゾーンのVDAは、プライマリゾーンのControllerに登録されます。プライマリゾーンのVDAは、サテライトゾーンのControllerに登録しようとすることはありません。
- サテライトゾーンのVDAは、可能であればローカルのControllerに登録されます。（これは優先Controllerと見なされます。）ローカルのControllerが利用できない場合（たとえば、VDAの登録をこれ以上受け入れられない、または障害が発生した場合など）、VDAはプライマリゾーンのControllerに登録しようとします。この場合、サテライトゾーンのControllerが再び利用可能になったとしても、VDAはプライマリゾーンに登録されたままになります。サテライトゾーンのVDAは、別のサテライトゾーンのControllerに登録しようとすることはありません。

- VDAのController検出で自動更新が有効になっており、VDAのインストール中にControllerアドレスのリストを指定した場合、初期登録のためにそのリストからControllerがランダムに選択されます（Controllerがどのゾーンにあるかに関わらず）。そのVDAを持つマシンが再起動されると、VDAはローカルゾーンのControllerへの登録を優先し始めます。
- サテライトゾーンのControllerが故障した場合、可能であれば別のローカルControllerにフェールオーバーします。ローカルControllerが利用できない場合は、プライマリゾーンのControllerにフェールオーバーします。
- Controllerをゾーンの内外に移動し、自動更新が有効になっている場合、両方のゾーンのVDAは、どのControllerがローカルで、どのControllerがプライマリゾーンにあるかを示す更新されたリストを受け取り、どのControllerに登録し、どのControllerから接続を受け入れることができるかを知ることができます。
- カタログを別のゾーンに移動すると、そのカタログ内のVDAは、カタログを移動したゾーンのControllerに再登録します。（カタログを別のゾーンに移動する際は、このゾーンと関連するホスト接続があるゾーンが適切に接続されていることを確認してください。帯域幅が制限されているか、待ち時間が長い場合は、ホスト接続を関連するマシンカタログを含む同じゾーンに移動してください。）

プライマリゾーンのすべてのControllerが故障した場合：

- Studioはサイトに接続できません。
- プライマリゾーンのVDAへの接続はできません。
- プライマリゾーンのControllerが利用可能になるまで、サイトのパフォーマンスが低下します。

VDAバージョン7.7より前のバージョンを含むサイトの場合：

- サテライトゾーンのVDAは、ローカルゾーンおよびプライマリゾーンのControllerからの要求を受け入れます。（最小バージョン7.7のVDAは、他のサテライトゾーンのController要求を受け入れることができます。）
- サテライトゾーンのVDAは、プライマリゾーンまたはローカルゾーンのControllerにランダムに登録します。（最小バージョン7.7のVDAはローカルゾーンを優先します。）

ゾーンの優先順位

ゾーン優先機能を使用するには、最小限StoreFront 3.7およびCitrix Gateway 11.0-65.xを使用している必要があります。

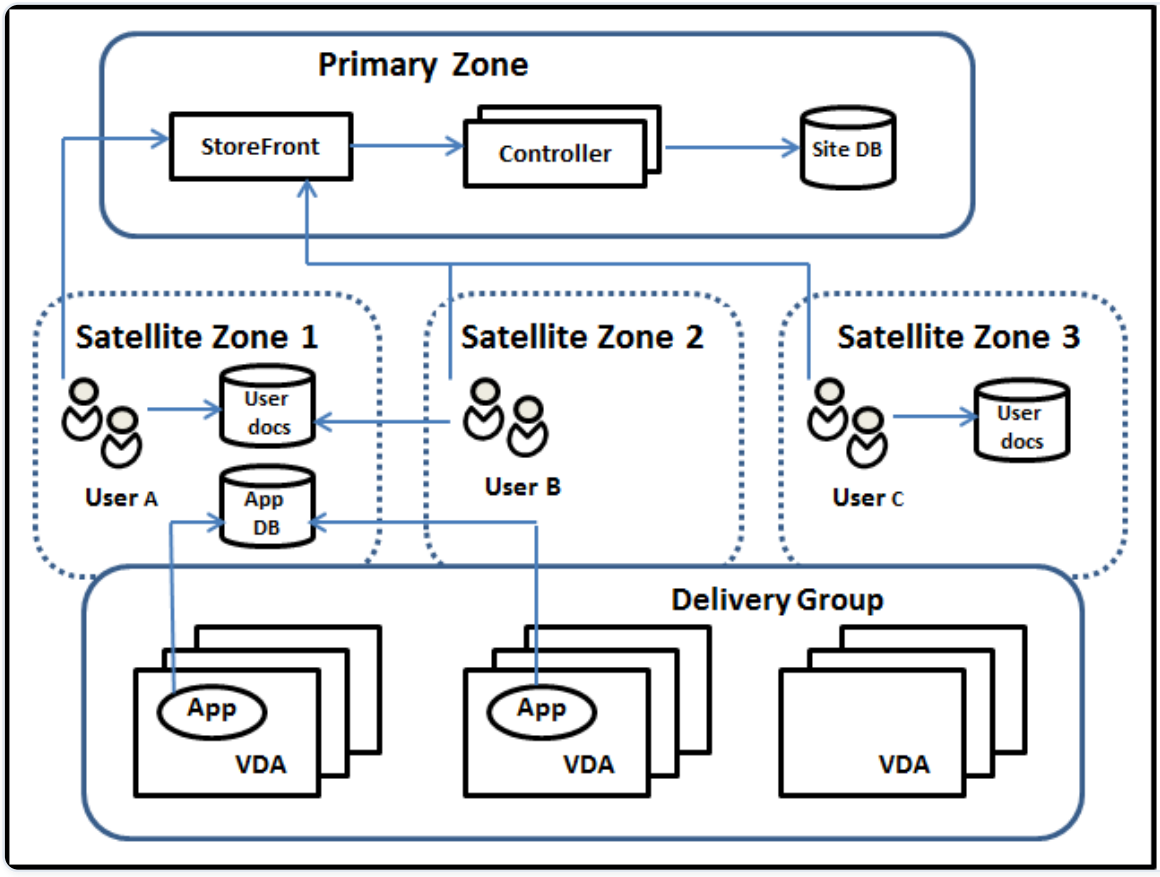
マルチゾーンサイトでは、ゾーン優先機能により、管理者はアプリケーションまたはデスクトップの起動に使用されるVDAをより柔軟に制御できます。

ゾーンの優先順位の仕組み

ゾーンの優先順位には3つの形式があります。特定のゾーンのVDAを使用することを優先する場合があります。その理由は次のとおりです。

- アプリケーションのデータが保存されている場所。これはアプリケーションホームと呼ばれます。
- ユーザーのホームデータ（プロファイルやホーム共有など）の場所。これはユーザーホームと呼ばれます。
- ユーザーの現在の場所（Citrix Workspace™アプリが実行されている場所）。これはユーザーの場所と呼ばれます。

次の図は、マルチゾーン構成の例を示しています。



この例では、VDAは3つのサテライトゾーンに分散していますが、すべて同じデリバリーグループに属しています。そのため、ブローカーはユーザーの起動リクエストに対してどのVDAを使用するかを選択する可能性があります。この例は、ユーザーがCitrix Workspaceアプリのエンドポイントを実行できる場所がいくつかあることを示しています。

- ユーザーAは、サテライトゾーン1でCitrix Workspaceアプリがインストールされたデバイスを使用しています。
- ユーザーBは、サテライトゾーン2でデバイスを使用しています。

- ユーザーのドキュメントはさまざまな場所に保存できます。
  - ユーザーAとBは、サテライトゾーン1にある共有を使用します。
  - ユーザーCは、サテライトゾーンCの共有を使用します。
  - 公開されているアプリケーションの1つは、サテライトゾーン1にあるデータベースを使用します。

ユーザーまたはアプリケーションのホームゾーンを構成することで、ユーザーまたはアプリケーションをゾーンに関連付けます。Delivery Controller™のブローカーは、リソースが利用可能な場合、これらの関連付けを使用してセッションが起動されるゾーンの選択を支援します。次のことができます。

- ユーザーをゾーンに追加して、ユーザーのホームゾーンを構成します。
- アプリケーションのプロパティを編集して、アプリケーションのホームゾーンを構成します。

ユーザーまたはアプリケーションは、一度に1つのホームゾーンしか持つことができません。（ユーザーグループのメンバーシップにより複数のゾーンメンバーシップが発生する場合、ユーザーには例外が発生する可能性があります。「その他の考慮事項」セクションを参照してください。ただし、この場合でも、ブローカーは1つのホームゾーンのみを使用します。）

ユーザーとアプリケーションのゾーン設定を構成できますが、ブローカーは起動に対して1つの優先ゾーンのみを選択します。優先ゾーンを選択するためのデフォルトの優先順位は、アプリケーションホーム \> ユーザーホーム \> ユーザーロケーションです。この順序を制限できます。詳細については、ゾーン設定の調整を参照してください。ユーザーがアプリケーションを起動すると：

- そのアプリケーションにゾーン関連付け（アプリケーションホーム）が構成されている場合、優先ゾーンはそのアプリケーションのホームゾーンになります。
- アプリケーションにゾーン関連付けが構成されていないが、ユーザーにゾーン関連付け（ユーザーホーム）が構成されている場合、優先ゾーンはそのユーザーのホームゾーンになります。
- アプリケーションにもユーザーにもゾーン関連付けが構成されていない場合、優先ゾーンはユーザーがCitrix Workspaceアプリインスタンスを実行しているゾーン（ユーザーロケーション）になります。そのゾーンが定義されていない場合、ランダムなVDAとゾーンの選択が使用されます。優先ゾーン内のすべてのVDAに負荷分散が適用されます。優先ゾーンがない場合、デリバリーグループ内のすべてのVDAに負荷分散が適用されます。

ゾーンの優先順位の調整

ユーザーまたはアプリケーションのホームゾーンを構成（または削除）する際、ゾーン設定の使用方法をさらに制限することもできます。

- **必須のユーザーホームゾーンの使用：** デリバリーグループでは、セッションがユーザーのホームゾーン（構成されている場合）で起動し、ホームゾーンに利用可能なリソースがない場合に他のゾーンへのフェイルオーバーを行わないように指定できます。この制限は、ゾーン間で大きなプロファイルやデータファイルをコピーするリスクを回避する必要がある場合に役立ちます。言い換えれば、別のゾーンでセッションを起動するよりも、セッションの起動を拒否する方が望ましいということです。
- **アプリケーションのホームゾーンの強制使用:** 同様に、アプリケーションのホームゾーンを構成する場合、そのアプリケーションは、アプリケーションのホームゾーンでリソースが利用できない場合に別のゾーンにフェールオーバーすることなく、そのゾーンでのみ起動されるように指定できます。
- **アプリケーションのホームゾーンなし、および構成されたユーザーホームゾーンを無視:** アプリケーションのホームゾーンを指定しない場合、そのアプリケーションを起動するときに、構成されたユーザーゾーンを考慮しないように指定することもできます。たとえば、一部のユーザーが異なるホームゾーンを持っている場合でも、ユーザーロケーションゾーンの優先設定を使用して、ユーザーがデバイスの近くのVDAでアプリケーションを実行することを好む場合があります。

優先ゾーンがセッションの使用に与える影響

ユーザーがアプリケーションまたはデスクトップを起動すると、ブローカーは既存のセッションを使用するよりも優先ゾーンを使用することを優先します。

アプリケーションまたはデスクトップを起動するユーザーが、起動されるリソースに適したセッション（たとえば、アプリケーションのセッション共有を使用できるセッション、または起動されるリソースがすでに実行されているセッション）をすでに持っているが、そのセッションがユーザー/アプリケーションの優先ゾーン以外のゾーンのVDAで実行されている場合、システムは新しいセッションを作成する可能性があります。これにより、そのユーザーのセッション要件にとって優先度の低いゾーンのセッションに再接続するよりも前に、正しいゾーンでの起動（利用可能な容量がある場合）が満たされます。

到達不能になる可能性のある孤立したセッションを防ぐため、既存の切断されたセッションへの再接続は、それらが非優先ゾーンにある場合でも許可されます。

起動を満たすためのセッションの望ましさの順序は次のとおりです。

1. 優先ゾーン内の既存のセッションに再接続する。
2. 優先ゾーン以外のゾーンで、既存の切断されたセッションに再接続する。
3. 優先ゾーンで新しいセッションを開始します。
4. 優先ゾーン以外のゾーンで、接続されている既存のセッションに再接続する。

5. 優先ゾーン以外のゾーンで、新しいセッションを開始する。

その他のゾーン優先度に関する考慮事項

- ユーザーグループ（セキュリティグループなど）にホームゾーンを構成すると、そのグループのユーザー（直接的または間接的なメンバーシップを通じて）は指定されたゾーンに関連付けられます。ただし、ユーザーは複数のセキュリティグループのメンバーになることができ、そのため、他のグループメンバーシップを通じて異なるホームゾーンが構成されている場合があります。このような場合、そのユーザーのホームゾーンの決定は曖昧になる可能性があります。

ユーザーがグループメンバーシップを通じて取得したものではない構成済みのホームゾーンを持っている場合、そのゾーンがゾーン優先度に使用されます。グループメンバーシップを通じて取得されたゾーン関連付けはすべて無視されます。

ユーザーがグループメンバーシップのみを通じて取得した複数の異なるゾーン関連付けを持っている場合、ブローカーはゾーンの中からランダムに選択します。ブローカーがこの選択を行うと、そのゾーンは、ユーザーのグループメンバーシップが変更されるまで、その後のセッション起動に使用されます。

- ユーザーロケーションゾーンの優先設定では、デバイスが接続するCitrix Gatewayによって、エンドポイントデバイス上のCitrix Workspaceアプリが検出される必要があります。Citrix Gatewayは、IPアドレスの範囲を特定のゾーンに関連付けるように構成する必要があり、検出されたゾーンIDはStoreFrontを介してControllerに渡される必要があります。

ゾーンの優先設定の詳細については、「ゾーンの優先設定の内部」を参照してください。

考慮事項、要件、およびベストプラクティス

- ゾーンには、Controller、マシンカタログ、ホスト接続、ユーザー、およびアプリケーションを配置できます。カタログがホスト接続を使用する場合、カタログと接続が同じゾーンにあることを確認してください。（ただし、低遅延で高帯域幅の接続が利用可能な場合は、異なるゾーンに配置することもできます。）」
- サテライトゾーンにアイテムを配置すると、サイトがそれらやそれらに関連する他のオブジェクトとどのようにやり取りするかに影響します。
    - Controllerがサテライトゾーンに配置されると、それらのマシンは同じゾーン内のハイパーバイザーおよびVDAに対して良好な（ローカル）接続性を持っていると見なされます。そのサテライトゾーンのControllerは、それらのハイパーバイザーおよびVDAマシンを処理するために、プライマリゾーンのControllerよりも優先して使用されます。

  - ハイパーバイザー接続がサテライトゾーンに配置されると、そのハイパーバイザー接続を介して管理されるすべてのハイパーバイザーもそのサテライトゾーンに存在すると見なされます。そのサテライトゾーンのControllerは、そのハイパーバイザー接続と通信する際に、プライマリゾーンのControllerよりも優先して使用されます。
  - マシンカタログがサテライトゾーンに配置されると、そのカタログ内のすべてのVDAマシンがサテライトゾーンにあると見なされます。各VDAの最初の登録後にControllerリストの自動更新メカニズムがアクティブになった後、サイトへの登録を試みる際には、プライマリゾーンのControllerよりもローカルのControllerが優先して使用されます。
  - Citrix Gatewayインスタンスもゾーンに関連付けることができます。これは、ここで説明されている他の要素の場合のようにサイト構成の一部としてではなく、StoreFront Optimal HDX™ルーティング構成の一部として行われます。Citrix Gatewayがゾーンに関連付けられている場合、そのゾーン内のVDAマシンへのHDX接続が使用されるときに、そのCitrix Gatewayが優先的に使用されます。

- 実稼働サイトを作成し、最初のカタログとデリバリーグループを作成すると、すべての項目はプライマリゾーンに配置されます。この初期設定が完了するまで、サテライトゾーンを作成することはできません。（空のサイトを作成した場合、プライマリゾーンには最初はコントローラーのみが含まれます。カタログとデリバリーグループを作成する前または後にサテライトゾーンを作成できます。）
- 1つ以上の項目を含む最初のサテライトゾーンを作成すると、サイト内の他のすべての項目はプライマリゾーンに残ります。
- プライマリゾーンのデフォルト名は「Primary」ですが、この名前は変更できます。Studioの表示ではどのゾーンがプライマリゾーンであるかが示されますが、プライマリゾーンには識別しやすい名前を使用するのがベストプラクティスです。プライマリゾーンを再割り当て（つまり、別のゾーンをプライマリゾーンにする）することはできますが、常にサイトデータベースとすべての高可用性サーバーが含まれている必要があります。
- サイトデータベースは常にプライマリゾーンに保持してください。
- ゾーンを作成した後、後で項目をあるゾーンから別のゾーンに移動できます。この柔軟性により、近接して最適に機能する項目を分離できる可能性があります。たとえば、カタログ内のマシンを作成する接続（ホスト）とは異なるゾーンにカタログを移動すると、パフォーマンスに影響を与える可能性があります。項目をゾーン間で移動する前に、潜在的な意図しない影響を考慮してください。カタログとそれが使用するホスト接続は同じゾーンに、または適切に接続されたゾーン（たとえば、低遅延で高帯域幅のネットワーク経由）に保持してください。
- 最適なパフォーマンスを得るには、StudioとDirectorはプライマリゾーンにのみインストールしてください。サテライトゾーンに別のStudioインスタンスが必要な場合（たとえば、プライマリゾーンにアクセスできなくなった場合のフェイルオーバーとしてControllerを含むサテライ

トゾーン）、Studioをローカルで公開されたアプリケーションとして実行します。DirectorはWebアプリケーションであるため、サテライトゾーンからアクセスすることもできます。

- 理想的には、サテライトゾーンのCitrix Gatewayは、他のゾーンまたは外部の場所からそのゾーンに入ってくるユーザー接続に使用されますが、ゾーン内の接続にも使用できます。
- 注意: ゾーン優先機能を使用するには、StoreFront 3.7およびCitrix Gateway 11.0-65.x以降を使用している必要があります。

接続品質の制限

サテライトゾーンのコントローラーは、サイトデータベースと直接SQL対話を行います。これにより、サテライトゾーンとサイトデータベースを含むプライマリゾーン間のリンクの品質にいくつかの制限が課せられます。具体的な制限は、サテライトゾーンに展開されているVDAの数と、それらのVDA上のユーザーセッションの数に比例します。したがって、VDAとセッションが少ないサテライトゾーンは、VDAとセッションが多いサテライトゾーンよりも、データベースへの接続品質が低い場合でも機能できます。

詳細については、「Latency and SQL Blocking Query Improvements」を参照してください。

遅延がブローカリングパフォーマンスに与える影響

ゾーンによってユーザーは高遅延リンク上にいることができますが、ローカルブローカーが存在する場合でも、追加の遅延は必然的にエンドユーザーエクスペリエンスに影響を与えます。ユーザーが行うほとんどの作業において、サテライトゾーンのコントローラーとサイトデータベース間のラウンドトリップによって引き起こされる遅延を経験します。

アプリケーションを起動する場合、セッションブローカリングプロセスがセッション起動要求を送信するのに適したVDAを特定する際に、追加の遅延が発生します。

ゾーンの作成と管理

フル管理者であれば、すべてのゾーン作成および管理タスクを実行できます。ただし、ゾーンの作成、編集、削除を許可するカスタムロールを作成することもできます。ゾーン間でアイテムを移動する場合、ゾーン関連の権限（ゾーン読み取り権限を除く）は必要ありませんが、移動するアイテムに対する編集権限が必要です。たとえば、カタログをあるゾーンから別のゾーンに移動するには、そのカタログに対する編集権限が必要です。詳しくは、「委任管理」を参照してください。

Citrix Provisioning™を使用する場合： Citrix Provisioningコンソールはゾーンを認識しないため、CitrixではStudioを使用してサテライトゾーンのカタログを作成することを推奨しています。Studioでカタログを作成し、正しいサテライトゾーンを指定します。その後、Citrix Provisioningコンソールを使用して、そのカタログ内のマシンをプロビジョニングします。（Citrix Provisioning

ウィザードを使用してカタログを作成した場合、カタログはプライマリゾーンに配置されます。後でStudioを使用してサテライトゾーンに移動する必要があります。）

ゾーンの作成

1. Studioナビゲーションペインで、**Configuration \> Zones** を選択します。
2. ［操作］ペインで、**［ゾーンの作成］** を選択します。
3. ゾーンの名前と説明（オプション）を入力します。名前はサイト内で一意である必要があります。
4. 新しいゾーンに配置するアイテムを選択します。選択可能なアイテムのリストをフィルター処理したり、検索したりできます。空のゾーンを作成することもできます。その場合は、どのアイテムも選択しないでください。
5. 「**保存**」をクリックします。

この方法の代替として、Studioで1つ以上の項目を選択し、［操作］ペインで**［ゾーンの作成］** を選択することもできます。

ゾーン名または説明の変更

1. Studioナビゲーションペインで、**Configuration \> Zones** を選択します。
2. 中央ペインでゾーンを選択し、［操作］ペインで**［ゾーンの編集］** を選択します。
3. ゾーン名、説明、またはその両方を変更します。プライマリゾーンの名前を変更する場合は、そのゾーンがプライマリゾーンとして容易に識別できることを確認してください。
4. **［OK］** または **［適用］** をクリックします。

ゾーン間でアイテムを移動する

1. Studioナビゲーションペインで、**Configuration \> Zones** を選択します。
2. 中央ペインでゾーンを選択し、1つ以上の項目を選択します。
3. 項目を移動先のゾーンにドラッグするか、［操作］ペインで**［項目の移動］** を選択し、移動先のゾーンを指定します。

確認メッセージには、選択したアイテムが一覧表示され、それらすべてを移動してもよろしいかどうかが尋ねられます。

注意: カタログがハイパーバイザーまたはその他のサービスへのホスト接続を使用する場合、カタログと接続の両方を同じゾーンに配置してください。そうしないと、パフォーマンスに影響が出る可能性があります。一方を移動する場合は、もう一方も移動してください。

ゾーンを削除する

ゾーンは、削除する前に空である必要があります。プライマリゾーンは削除できません。

1. Studioナビゲーションペインで、**構成 \> ゾーン**を選択します。
2. 中央のペインでゾーンを選択します。
3. アクションペインで**ゾーンの削除**を選択します。ゾーンが空でない場合（項目が含まれている場合）、それらの項目を移動するゾーンを選択するよう求められます。
4. 削除を確認します。

ユーザーのホームゾーンを追加する

ユーザーのホームゾーンを構成することは、*ユーザーをゾーンに追加する*とも呼ばれます。

1. Studioナビゲーションペインで**構成 \> ゾーン**を選択し、次に中央ペインでゾーンを選択します。
2. アクションペインで**ゾーンへのユーザーの追加**を選択します。
3. **Add Users to Zone**ダイアログボックスで、**Add**をクリックし、ゾーンに追加するユーザーとユーザーグループを選択します。すでにホームゾーンを持つユーザーを指定した場合、メッセージに2つの選択肢が表示されます。**Yes** = ホームゾーンを持たない指定したユーザーのみを追加します。**No** = ユーザー選択ダイアログに戻ります。
4. **OK**をクリックします。

ホームゾーンが構成されているユーザーの場合、セッションをそのホームゾーンからのみ起動するように要求できます。

1. デリバリーグループを作成または編集します。
2. **ユーザー**ページで、**セッションは、構成されている場合、ユーザーのホームゾーンで起動する必要があります**チェックボックスをオンにします。

そのデリバリーグループのユーザーによって起動されたすべてのセッションは、そのユーザーのホームゾーン内のマシンから起動する必要があります。デリバリーグループ内のユーザーに構成されたホームゾーンがない場合、この設定は無効です。

ユーザーのホームゾーンを削除する

この手順は、ゾーンからユーザーを削除することとも呼ばれます。

1. Studioナビゲーションペインで**構成 \> ゾーン**を選択し、次に中央ペインでゾーンを選択します。
2. アクションペインで**ゾーンからのユーザーの削除**を選択します。

3. **ゾーンへのユーザーの追加**ダイアログボックスで、**削除**をクリックし、ゾーンから削除するユーザーとグループを選択します。この操作では、ゾーンからのみユーザーが削除されます。これらのユーザーは、所属するデリバリーグループおよびアプリケーショングループに残ります。
4. プロンプトが表示されたら削除を確定します。

アプリケーションのホームゾーンを管理する

アプリケーションのホームゾーンを構成することは、アプリケーションをゾーンに追加することとも呼ばれます。デフォルトでは、マルチゾーン環境では、アプリケーションにホームゾーンはありません。

アプリケーションのホームゾーンは、アプリケーションのプロパティで指定されます。アプリケーションをグループに追加するとき、または後でアプリケーションのプロパティを構成できます。

- デリバリーグループを作成するとき、アプリケーショングループを作成するとき、または既存のグループにアプリケーションを追加するときに、ウィザードの**Applications**ページで**Properties**を選択します。
- アプリケーションの追加後にそのプロパティを変更するには、Studioナビゲーションペインで**アプリケーション**を選択します。アプリケーションを選択し、次にアクションペインで**アプリケーションプロパティの編集**を選択します。

アプリケーションのプロパティ/設定の ページで、次の操作を行います。

- アプリケーションにホームゾーンを設定する場合：
  - **Use the selected zone to decide**ラジオボタンを選択し、ゾーンを選択します。
  - アプリケーションを、選択したゾーンからのみ（他のゾーンからは起動しないように）起動する場合は、ゾーン選択の下にあるチェックボックスをオンにします。
- アプリケーションにホームゾーンを設定しない場合：
  - ラジオボタンを選択します。
  - このアプリケーションを起動する際に、ブローカーが構成済みのユーザーゾーンを考慮しないようにする場合は、ラジオボタンの下にあるチェックボックスを選択します。この場合、アプリケーションまたはユーザーのホームゾーンのいずれも、このアプリケーションを起動する場所を決定するために使用されません。

ゾーンの指定を含むその他のアクション

少なくとも1つのサテライトゾーンを作成した後、ホスト接続を追加するか、カタログを作成する際にゾーンを指定できます。

通常、プライマリゾーンがデフォルトです。Machine Creation Services™を使用してカタログを作成する場合、ホスト接続用に構成されたゾーンが自動的に選択されます。

サイトにサテライトゾーンが含まれていない場合、プライマリゾーンが想定され、ゾーン選択ボックスは表示されません。

接続とリソース

重要:

Citrix Virtual Apps and Desktops™ 7 2006以降、現在の展開で以下のいずれかのテクノロジーを使用している場合、それらのテクノロジーを使用するサポート終了（EOL）アイテムを削除した後にのみ、現在のリリースに展開をアップグレードできます。

- パーソナルvDisk (PvDs)
- AppDisks™
- パブリッククラウドホストの種類：Citrix CloudPlatform、Microsoft Azure Classic

詳細については、「PvD、AppDisks、およびサポートされていないホストの削除」を参照してください。

展開にパブリッククラウドホスト接続を使用する場合は、新規インストールまたは現在のリリースへのアップグレードを完了するためにHybrid Rights Licenseが必要です。

インストーラーがサポートされていないテクノロジーの1つ以上、またはHybrid Rights Licenseなしのホスト接続を検出すると、アップグレードが一時停止または停止し、説明メッセージが表示されます。インストーラーのログに詳細が含まれています。詳しくは、「展開のアップグレード」を参照してください。

Hybrid Rights Licenseがホスト接続に与える影響

Hybrid Rights Licenseの資格に基づいて、パブリッククラウドホストへのホスト接続が影響を受ける3つのシナリオがあります。

- パブリッククラウドホストへの新しいホスト接続を作成するには、Hybrid Rights Licenseが必要です。
- Hybrid Rights Licenseを所有しているがライセンスの有効期限が切れている場合、パブリッククラウドホストへの既存の接続は資格なしとマークされ、メンテナンスモードに入ります。既存のホスト接続がメンテナンスモードの場合、次の操作はできません。
  - ホスト接続の追加または変更
  - カタログの作成とイメージの更新
  - 電源操作の実行
- 資格なしのホスト接続が資格ありに変更されると、既存のホスティング接続が再度有効になります。

はじめに

サイトを作成するときに、ホスティングリソースへの最初の接続をオプションで作成できます。後で、その接続を変更したり、他の接続を作成したりできます。接続の構成には、サポートされているハイパーバイザーの中から接続タイプを選択すること、およびその接続のリソースから選択するストレージとネットワークが含まれます。

読み取り専用管理者は、接続とリソースの詳細を表示できます。接続とリソースの管理タスクを実行するには、完全な管理者である必要があります。詳細については、「委任管理」を参照してください。

接続タイプに関する情報の場所

サポートされている仮想化プラットフォームを使用して、Citrix Virtual AppsまたはCitrix Virtual Desktops環境でマシンをホストおよび管理できます。「システム要件」の記事に、サポートされている種類が記載されています。

詳細については、以下の情報源を参照してください。

- **シトリックス ハイパーバイザー™ (旧称 XenServer):**
  - Citrix Hypervisor仮想化環境。
  - Citrix Hypervisorのドキュメント。

- **ニュータニックス アクロポリス:**
  - Nutanix仮想化環境。
  - Nutanixドキュメント。
- **ヴイエムウェア:**
  - VMware仮想化環境。
  - VMware製品ドキュメント。
- **Microsoft ハイパーV:**
  - Microsoft System Center Virtual Machine Manager 仮想化環境の記事。
  - Microsoft ドキュメント。
- **パブリッククラウドホスト接続 (AWS、Microsoft Azure、Google Cloud):** パブリッククラウドホストに関する情報については、「リソースの種類を設定する」を参照してください。

> **注：**
>
> 情報ソースは、Citrix DaaS™のドキュメントを参照するよう指示しています。Citrix DaaS製品のパブリッククラウドホストに慣れている場合でも、オンプレミスバージョンにはいくつかの違いがあります。Citrix DaaSでは、管理インターフェイスは「Full Configuration」として知られています。オンプレミスのVirtual Apps and Desktopsでは、管理インターフェイスは「Citrix Studio」として知られています。更新はサービスに約4週間ごとに展開されます。そのため、サービスで利用できる特定の機能がオンプレミスバージョンでは利用できない場合があります。

ホストストレージ

サポートされているハイパーバイザーによって管理されている場合、ストレージ製品はサポートされます。Citrix Supportは、これらのストレージ製品ベンダーが問題のトラブルシューティングと解決を支援し、必要に応じてナレッジセンターにそれらの問題を文書化します。

マシンをプロビジョニングする際、データはタイプ別に分類されます。

- マスターイメージを含むオペレーティングシステム（OS）データ。

- 一時データ。このデータには、MCSプロビジョニングマシンに書き込まれるすべての非永続データ、Windowsページファイル、ユーザープロファイルデータ、およびShareFileと同期されるすべてのデータが含まれます。このデータは、マシンが再起動するたびに破棄されます。

データタイプごとに個別のストレージを提供することで、各ストレージデバイスの負荷を軽減し、パフォーマンスを向上させ、ホストの利用可能なリソースを最大限に活用できます。また、異なるデータタイプに適したストレージを使用できるようになります。一部のデータでは、永続性と回復性が他のデータよりも重要になります。

ストレージは共有（中央に配置され、どのホストからも独立しており、すべてのホストで使用される）することも、ハイパーバイザーにローカルに配置することもできます。たとえば、中央共有ストレージは、1つ以上のWindows Server 2012クラスター化ストレージボリューム（接続ストレージの有無にかかわらず）、またはストレージベンダーのアプライアンスである場合があります。中央ストレージは、ハイパーバイザーストレージ制御パスやパートナープラグインを介した直接アクセスなど、独自の最適化を提供する可能性もあります。

一時データをローカルに保存することで、共有ストレージにアクセスするためにネットワークを介する必要がなくなります。また、共有ストレージデバイスの負荷も軽減されます。共有ストレージはより高価になる可能性があるため、データをローカルに保存することで費用を削減できます。これらの利点は、ハイパーバイザーサーバー上の十分なストレージの可用性と比較検討する必要があります。

接続を作成する際、ハイパーバイザー間で共有されるストレージ、またはハイパーバイザーにローカルなストレージの2つのストレージ管理方法のいずれかを選択します。

一時データストレージとして1つ以上のCitrix Hypervisorホストでローカルストレージを使用する場合、プール内の各ストレージの場所に一意の名前があることを確認してください。（XenCenter®で名前を変更するには、ストレージを右クリックして名前プロパティを編集します。）

ハイパーバイザーで共有されるストレージ

ハイパーバイザー間で共有されるストレージ方式は、長期的な永続性が必要なデータを中央に保存し、一元的なバックアップと管理を提供します。このストレージにはOSディスクが格納されます。

この方法を選択すると、一時的なマシンデータにローカルストレージ（同じハイパーバイザープール内のサーバー上）を使用するかどうかを選択できます。この方法は、共有ストレージ内のデータほど永続性や回復性を必要としません。これは*一時データキャッシュ*と呼ばれます。ローカルディスクは、メインOSストレージへのトラフィックを削減するのに役立ちます。このディスクは、マシンが再起動するたびにクリアされます。ディスクはライトスルーメモリキャッシュを介してアクセスされます。一時データにローカルストレージを使用する場合、プロビジョニングされた

VDAは特定のハイパーバイザーホストに紐付けられます。そのホストが故障すると、VMは起動できません。

例外: Microsoft System Center Virtual Machine Managerは、クラスター共有ボリューム（CSV）を使用する場合、ローカルストレージ上の一時データキャッシュディスクを許可しません。

一時データをローカルに保存するための接続を作成し、各VMのキャッシュディスクサイズとメモリサイズの非デフォルト値を有効にして構成します。デフォルト値は接続タイプに合わせて調整されており、ほとんどのケースで十分です。詳細については、「マシンカタログの作成」を参照してください。

ハイパーバイザーは、ディスクイメージをローカルで読み取りキャッシュすることにより、最適化テクノロジーも提供できます。たとえば、Citrix HypervisorはIntelliCache™を提供し、中央ストレージへのネットワークトラフィックを削減します。

ハイパーバイザーのローカルストレージ

ハイパーバイザーにローカルなストレージ方式では、データをハイパーバイザーにローカルに保存します。この方式では、マスターイメージやその他のOSデータがサイト内のハイパーバイザーに転送されます。このプロセスは、最初のマシン作成時と将来のイメージ更新時に発生します。このプロセスにより、管理ネットワークでかなりのトラフィックが発生します。イメージ転送には時間がかかり、イメージは各ホストで異なるタイミングで利用可能になります。

接続とリソースを作成する

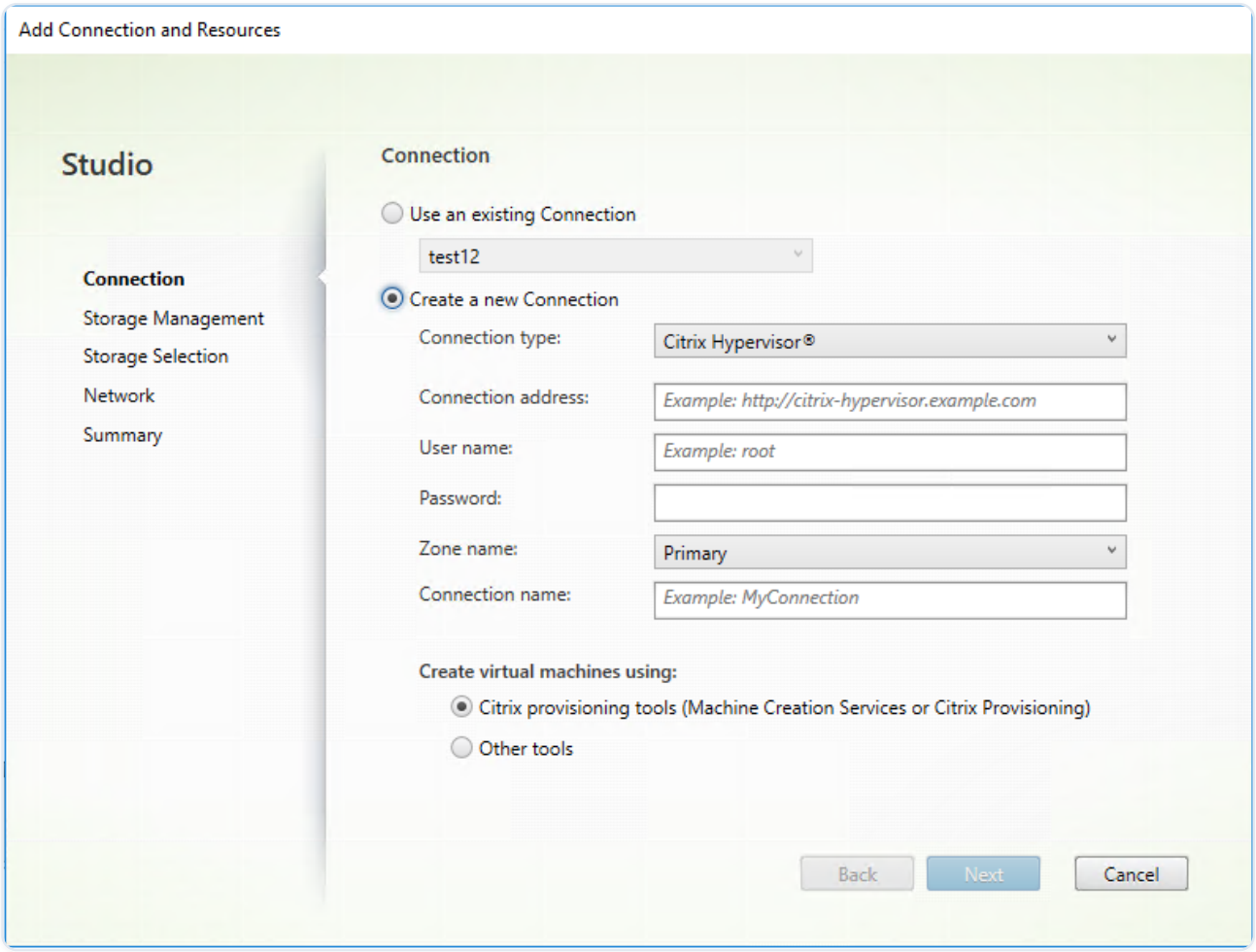
サイトの作成時に、最初の接続をオプションで作成できます。サイト作成ウィザードには、以下のセクションで説明する接続関連のページが含まれています。

サイトの作成後に接続を作成する場合は、手順1から開始します。

> **重要:**
>
> 接続を作成する前に、ホストリソース（ストレージとネットワーク）が利用可能である必要があります。

1. **Studio**ナビゲーションペインで、 **>** を選択します。
2. ペインで、 を選択します。
3. ウィザードは、以下のページ（特定のページの内容は選択した接続タイプによって異なります）を案内します。各ページを完了したら、 をクリックして ページに進みます。

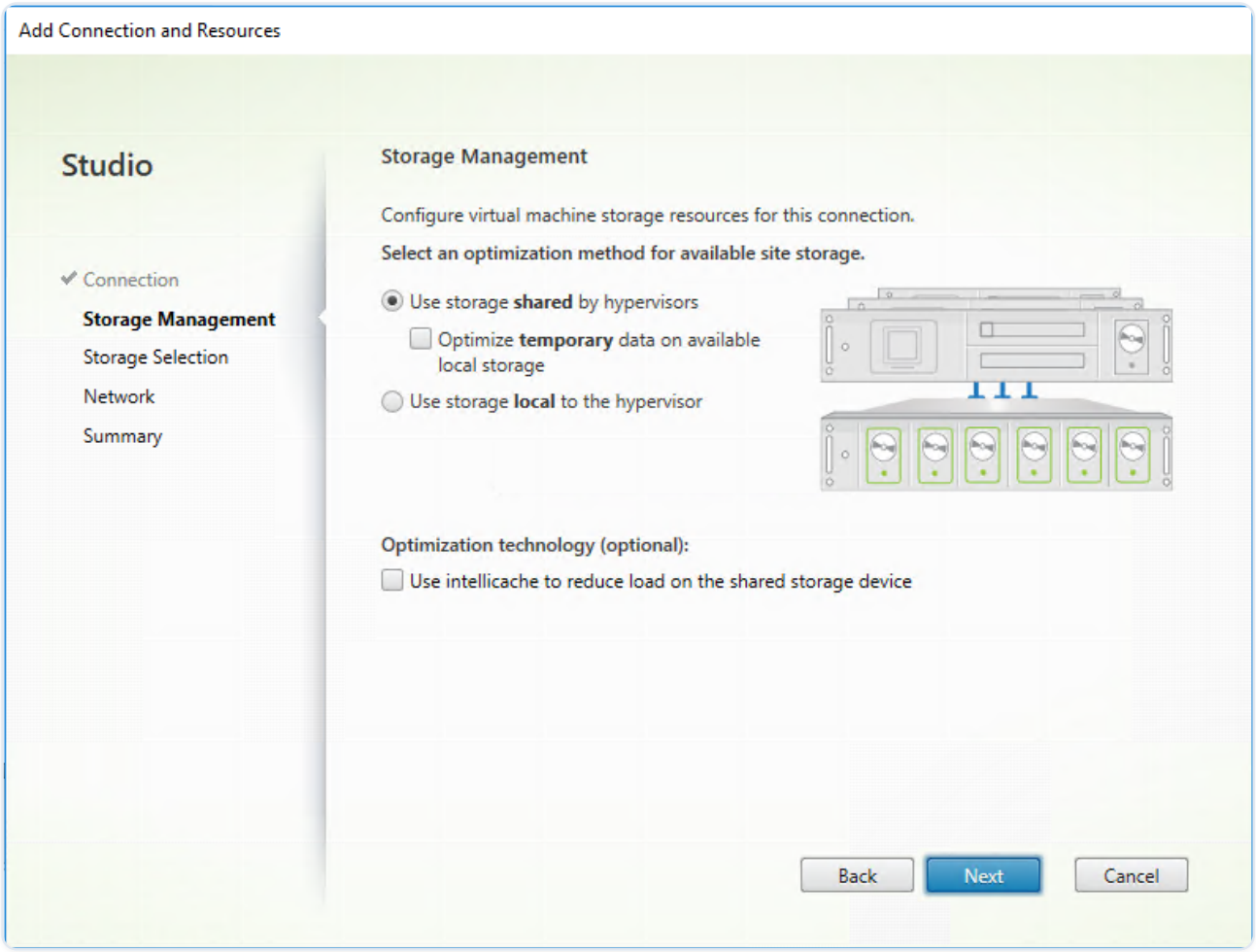
接続



「**接続**」ページで：

- 接続を作成するには、 を選択します。既存の接続と同じホスト構成に基づいて接続を作成するには、 を選択し、関連する接続を選択します。
- フィールドで、使用しているハイパーバイザーを選択します。パブリッククラウドホスト接続は、Hybrid Rights Licenseを使用している場合にのみドロップダウンリストに表示されます。
- 接続アドレスと資格情報フィールドは、選択した接続タイプによって異なります。要求された情報を入力します。
- 接続名を入力します。この名前はStudioに表示されます。
- 仮想マシンの作成に使用するツールを選択します。Studioツール（Machine Creation Services™やCitrix Provisioningなど）またはその他のツールです。

ストレージ管理



ストレージ管理の種類と方法については、「ホストストレージ」を参照してください。

Hyper-V または VMware ホストへの接続を構成している場合は、クラスター名を参照して選択します。その他の接続タイプでは、クラスター名は要求されません。

ストレージ管理方法を選択します。ハイパーバイザーによって共有されるストレージ、またはハイパーバイザーにローカルなストレージ。

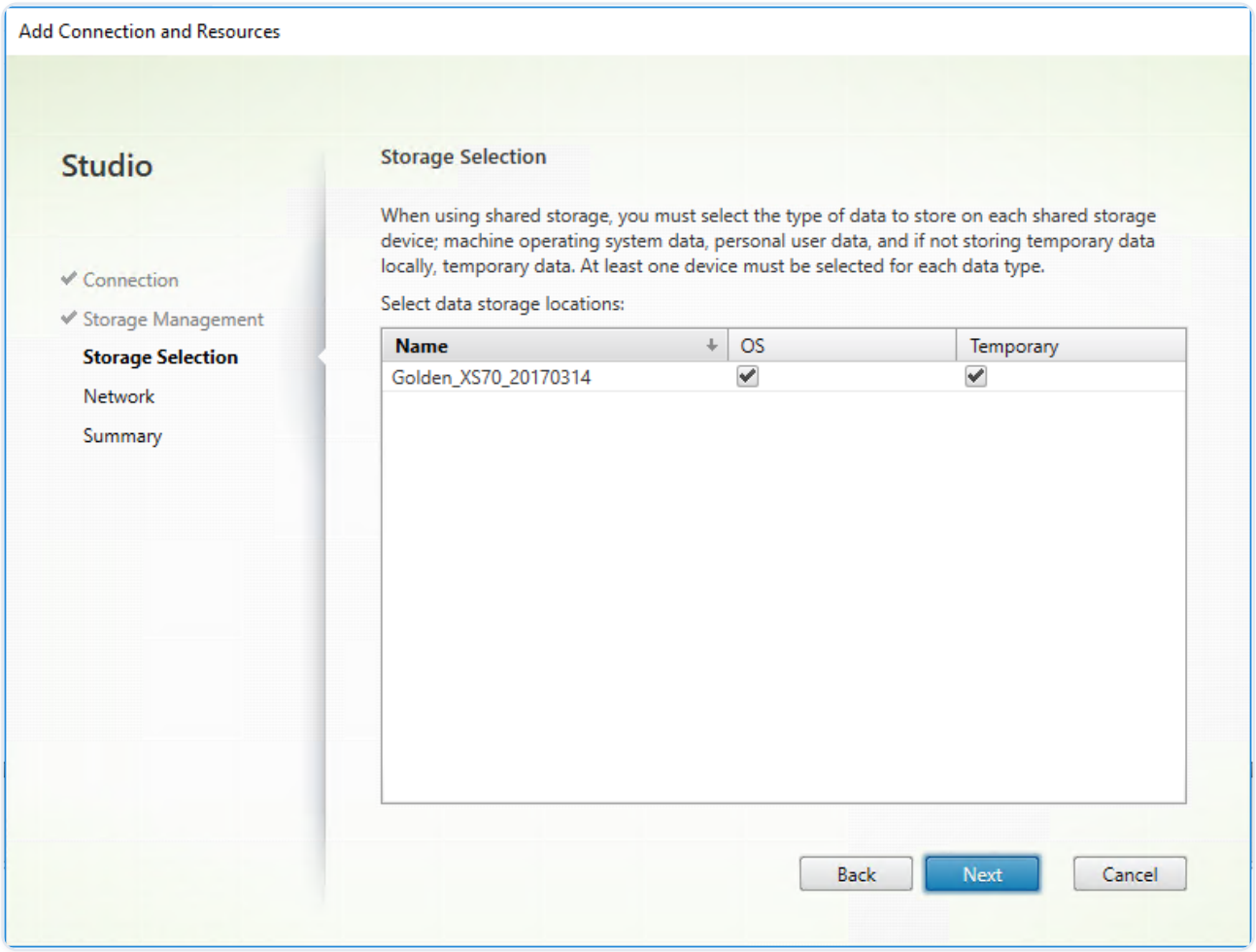
- ハイパーバイザー間で共有されるストレージを選択した場合、利用可能なローカルストレージに一時データを保持するかどうかを指定します。（この接続を使用するマシンカタログで、デフォルト以外のサイズの一時ストレージを指定できます。）**例外:** クラスター共有ボリューム（CSV）を使用する場合、Microsoft System Center Virtual Machine Managerはローカルストレージに一時データキャッシュディスクを許可しません。Studioでそのストレージ管理設定を構成すると失敗します。

Citrix Hypervisorプールで共有ストレージを使用している場合は、共有ストレージデバイスの負荷を軽減するためにIntelliCacheを使用するかどうかを指定します。詳細については、Citrix Hypervisor接続でのIntelliCacheの使用を参照してください。

注：

XenServer®、VMware、および SCVMM 仮想化環境では、OS ディスクと同じストレージ場所にライトバックキャッシュ (WBC) ディスクを配置できます。このためには、「**利用可能なローカルストレージで一時データを最適化する**」を選択しないでください。

ストレージの選択



ストレージの選択の詳細については、「ホストストレージ」を参照してください。

利用可能なデータタイプごとに、少なくとも1つのホストストレージデバイスを選択します。前のページで選択したストレージ管理方法によって、このページで選択できるデータタイプが決まります。ウィザードの次のページに進む前に、サポートされているデータタイプごとに少なくとも1つのストレージデバイスを選択してください。

注：

> XenServer、VMware、SCVMMの仮想化環境では、利用可能なOSストレージリストと利用可能な一時ストレージリストを同じに構成した場合、MCSはライトバックキャッシュ（WBC）ディスクをOSディスクと同じストレージ場所に配置します。

> 「**ストレージの選択**」ページの下部には、ハイパーバイザーで共有されるストレージを選択し、前のページで「**利用可能なローカルストレージ上の一時データを最適化**」を有効にした場合に、さらに多くの構成オプションが含まれています。一時データに使用するローカルストレージデバイスを選択できます。

現在選択されているストレージデバイスの数が表示されます (上記のグラフィックでは「1 storage device selected」)。そのエントリにカーソルを合わせると、選択されているデバイス名が表示されます。

1. 使用するストレージデバイスを変更するには、**選択**をクリックします。
2. **ストレージの選択**ダイアログボックスで、ストレージデバイスのチェックボックスをオンまたはオフにして、**OK**をクリックします。

ネットワーク

Networkページで、リソースの名前を入力します。この名前は、接続に関連付けられているストレージとネットワークの組み合わせを識別するためにStudioに表示されます。

VMが使用するネットワークを1つ以上選択します。

概要

概要ページで、選択内容を確認します。完了したら、**完了**をクリックします。

注意: 一時データをローカルに保存すると、この接続を使用するマシンを含むマシンカタログを作成する際に、一時データストレージの非デフォルト値を構成できます。「マシンカタログの作成」を参照してください。

接続設定の編集

この手順を使用して接続の名前を変更したり、接続を作成したりしないでください。それらの接続は異なる操作です。現在ホストしているマシンに新しいアドレスがある場合にのみ、アドレスを変更してください。別のアドレスを別のマシンに入力すると、接続のマシンカタログが破損します。

このリソースにアクセスするマシンカタログは、適切なGPU固有のマスターイメージを使用する必要があるため、接続の**GPU**設定を変更することはできません。接続を作成してください。

1. **Studio**ナビゲーションペインで、**Configuration \> Hosting**を選択します。
2. 接続を選択し、**Actions**ペインで**Edit Connection**を選択します。
3. 接続を編集する際に利用できる設定のガイダンスに従ってください。
4. 完了したら、 をクリックして変更を適用し、ウィンドウを開いたままにするか、 をクリックして変更を適用してウィンドウを閉じます。

接続プロパティページ:

- 接続アドレスと資格情報を変更するには、**Edit settings**を選択し、新しい情報を入力します。
- Citrix Hypervisor接続の高可用性サーバーを指定するには、**Edit HA servers**を選択します。Citrixでは、プールマスターが失敗した場合にCitrix Hypervisorとの通信を可能にするため、プール内のすべてのサーバーを選択することをお勧めします。

詳細設定ページ:

- Remote PC Accessで使用されるMicrosoft System Center Configuration Manager (ConfMgr) Wake on LAN接続タイプの場合、**ConfMgr Wake Proxy**、マジックパケット、およびパケット送信情報を入力します。
- スロットリングしきい値設定を使用すると、接続で許可される電源操作の最大数を指定できます。これらの設定は、電源管理設定によって同時に起動できるマシンの数が多すぎたり少なすぎたりする場合に役立ちます。各接続タイプには、ほとんどの場合に適しており、変更すべきではない特定のデフォルト値があります。
- **同時アクション (すべてのタイプ)** 設定では、この接続で同時に発生できる最大絶対数と、この接続を使用するすべてのマシンの最大割合という2つの値を指定します。絶対値とパーセンテージ値の両方を指定する必要があります。実際に適用される制限は、これらの値のうち小さい方です。

  たとえば、34台のマシンがある展開で、**Simultaneous actions (all types)**が絶対値10、パーセンテージ値10に設定されている場合、適用される実際の制限は3です（つまり、34の10パーセントを最も近い整数に丸めたもので、絶対値10台のマシンよりも小さい）。
- **Maximum new actions per minute**は絶対数です。パーセンテージ値はありません。
- 「**接続オプション**」フィールドには、Citrixサポート担当者の指示または明示的なドキュメントの指示がある場合にのみ情報を入力してください。

接続のメンテナンスモードをオンまたはオフにする

接続のメンテナンスモードをオンにすると、新しい電源操作が接続に保存されているマシンに影響を与えるのを防ぎます。ユーザーは、マシンがメンテナンスモードの場合、マシンに接続できま

せん。ユーザーがすでに接続している場合、メンテナンスモードはログオフ時に有効になります。

1. **Studio**ナビゲーションペインで、**Configuration > Hosting**を選択します。
2. 接続を選択します。メンテナンスモードをオンにするには、**Actions**ペインで**Turn On Maintenance Mode**を選択します。メンテナンスモードをオフにするには、**Turn Off Maintenance Mode**を選択します。

個々のマシンに対してメンテナンスモードをオンまたはオフにすることもできます。また、マシンカタログまたはデリバリーグループ内のマシンに対してメンテナンスモードをオンまたはオフにすることもできます。

接続を削除する

接続を削除すると、多数のマシンが削除され、データが失われる可能性があります。影響を受けるマシン上のユーザーデータがバックアップされているか、不要であることを確認してください。

接続を削除する前に、以下を確認してください。

- すべてのユーザーが接続に保存されているマシンからログオフしていること。
- 切断されたユーザーセッションが実行されていないこと。
- プールされたマシンと専用マシンのメンテナンスモードがオンになっていること。
- 接続で使用されているマシンカタログ内のすべてのマシンは電源がオフになります。

カタログによって参照されている接続を削除すると、マシンカタログは使用できなくなります。この接続がカタログによって参照されている場合、カタログを削除するオプションがあります。カタログを削除する前に、他の接続で使用されていないことを確認してください。

1. **Studio**ナビゲーションペインで、**Configuration > Hosting**を選択します。
2. 接続を選択し、**Actions**ペインで**Delete Connection**を選択します。
3. この接続にマシンが保存されている場合、マシンを削除するかどうかを尋ねられます。削除する場合は、関連するActive Directoryコンピューターアカウントをどうするかを指定します。

接続の名前を変更またはテストする

1. **Studio**ナビゲーションペインで、**Configuration > Hosting**を選択します。
2. 接続を選択し、**Actions**ペインで**Rename Connection**または**Test Connection**を選択します。

接続上のマシンの詳細を表示する

1. **Studio**ナビゲーションペインで、**Configuration > Hosting**を選択します。
2. 接続を選択し、**Actions**ペインで**View Machines**を選択します。

上部のペインには、接続を介してアクセスされるマシンが一覧表示されます。マシンを選択すると、下部のペインにその詳細が表示されます。開いているセッションのセッション詳細も提供されます。

検索機能を使用して、マシンをすばやく見つけます。ウィンドウ上部のリストから保存された検索を選択するか、新しい検索を作成します。マシン名の全部または一部を入力して検索するか、高度な検索に使用する式を作成できます。式を作成するには、 をクリックし、プロパティと演算子のリストから選択します。

接続上のマシンを管理する

1. 「**Studio**」ナビゲーションペインで、「**構成 > ホスティング**」を選択します。
2. 接続を選択し、 ペインで を選択します。
3. **操作**ペインで、次のいずれかを選択します。一部の操作は、マシンの状態と接続ホストの種類によっては使用できません。

アクション	説明
起動	マシンが電源オフまたは一時停止状態の場合に起動します。
一時停止	マシンをシャットダウンせずに一時停止し、マシンリストを更新します。
シャットダウン	オペレーティングシステムにシャットダウンを要求します。
強制シャットダウン	マシンを強制的に電源オフにし、マシンリストを更新します。
再起動	オペレーティングシステムにシャットダウンを要求し、その後マシンを再起動します。オペレーティングシステムがこれに応じられない場合、デスクトップは現在の状態のままになります。

アクション	説明
メンテナンスモードを有効にする	マシンへの接続を一時的に停止します。この状態のマシンにはユーザーは接続できません。ユーザーが接続している場合、メンテナンスモードはログオフ時に有効になります。（上記のように、接続を介してアクセスされるすべてのマシンに対してメンテナンスモードをオンまたはオフにすることもできます。）
デリバリーグループから削除	Delivery Groupからマシンを削除しても、そのDelivery Groupが使用するMachine Catalogからは削除されません。マシンは、ユーザーが接続していない場合にのみ削除できます。マシンを削除している間、ユーザーが一時的に接続できないようにするには、メンテナンスモードをオンにします。
削除	マシンを削除すると、ユーザーはそのマシンにアクセスできなくなり、マシンはMachine Catalogから削除されます。マシンを削除する前に、すべてのユーザーデータがバックアップされているか、不要になっていることを確認してください。マシンは、ユーザーが接続していない場合にのみ削除できます。マシンを削除している間、ユーザーが一時的に接続できないようにするには、メンテナンスモードをオンにします。

マシンのシャットダウンを伴う操作の場合、マシンが10分以内にシャットダウンしないと、電源がオフになります。シャットダウン中にWindowsが更新プログラムのインストールを試みると、更新が完了する前にマシンの電源がオフになるリスクがあります。

ストレージの編集

接続を使用するVMのオペレーティングシステムデータと一時データを保存するために使用されるサーバーのステータスを表示できます。また、各データタイプのストレージにどのサーバーを使用するかを指定することもできます。

1. 「**Studio**」ナビゲーションペインで、「**構成 > ホスティング**」を選択します。
2. 接続を選択し、**操作**ペインで**ストレージの編集**を選択します。

3. 左側のペインで、データタイプ（オペレーティングシステムまたは一時）を選択します。
4. 選択したデータタイプについて、1つ以上のストレージデバイスのチェックボックスをオンまたはオフにします。
5. **OK**をクリックします。

リスト内の各ストレージデバイスには、その名前とストレージステータスが含まれています。有効なストレージステータスの値は次のとおりです。

- **使用中:** ストレージはマシンの作成に使用されています。
- **廃止済み:** ストレージは既存のマシンにのみ使用されています。このストレージには新しいマシンは追加されません。
- **未使用:** ストレージはマシンの作成に使用されていません。

現在**使用中**のデバイスのチェックボックスをオフにすると、そのステータスは**廃止済み**に変わります。既存のマシンはそのストレージデバイスを引き続き使用し（データを書き込むこともできます）、そのため、マシンの作成に使用されなくなった後でも、その場所がいっぱいになる可能性があります。

リソースの削除、名前の変更、またはテスト

1. 「**Studio**」ナビゲーションペインで、「**構成 > ホスティング**」を選択します。
2. リソースを選択し、**操作**ペインで適切なエントリ（**リソースの削除**、**リソース名の変更**、または**リソースのテスト**）を選択します。

接続タイマー

ポリシー設定を使用して、3つの接続タイマーを構成できます。

- 「**最大接続タイマー**」：ユーザーデバイスと仮想デスクトップ間の途切れない接続の最大期間を決定します。「**セッション接続タイマー**」および「**セッション接続タイマー間隔**」ポリシー設定を使用します。
- 「**接続アイドルタイマー**」：ユーザーからの入力がない場合に、仮想デスクトップへの途切れないユーザーデバイス接続が維持される期間を決定します。「**セッションアイドルタイマー**」および「**セッションアイドルタイマー間隔**」ポリシー設定を使用します。
- **接続解除タイマー:** 接続が解除され、ロックされた仮想デスクトップが、セッションがログオフされるまでロックされたままになる時間を決定します。「**接続解除セッションタイマー**」および「**接続解除セッションタイマー間隔**」ポリシー設定を使用します。

これらの設定のいずれかを更新する場合は、展開全体で一貫性があることを確認してください。

詳細については、ポリシー設定のドキュメントを参照してください。

ローカルホストキャッシュ

Citrix Virtual Apps and Desktopsサイトデータベースが常に利用可能であることを保証するため、CitrixはMicrosoftの高可用性ベストプラクティスに従って、フォールトトレラントなSQL Server展開から始めることを推奨します。(サポートされているSQL Serverの高可用性機能については、データベースを参照してください。)しかし、ネットワークの問題や中断により、ユーザーがアプリケーションやデスクトップに接続できなくなる可能性があります。

ローカルホストキャッシュ機能により、障害発生時にサイトでの接続仲介操作を継続できます。障害は、オンプレミスのCitrix®環境でDelivery Controller™とサイトデータベース間の接続が失敗したときに発生します。サイトデータベースに90秒間アクセスできない場合、ローカルホストキャッシュが作動します。

XenAppおよびXenDesktop 7.16以降、接続リース機能（以前のリリースにおける先行の高可用性機能）は製品から削除され、利用できなくなりました。

データコンテンツ

ローカルホストキャッシュには、メインデータベースの情報の一部である以下の情報が含まれます。

- サイトから公開されたリソースへの権限が割り当てられているユーザーおよびグループの ID。
- 現在使用している、または最近使用した、サイトから公開されたリソースのユーザーの ID。
- サイトで構成されている VDA マシン（リモート PC アクセス マシンを含む）の ID。
- 公開されたリソースへの接続に積極的に使用されているクライアントCitrix Receiver™マシンのID（名前とIPアドレス）。

また、メインデータベースが利用できなかった間に確立された、現在アクティブな接続に関する情報も含まれます。

- Citrix Receiverによって実行されたクライアントマシンのエンドポイント分析の結果。
- サイトに関与するインフラストラクチャマシン（NetScaler GatewayやStoreFront™サーバーなど）のID。
- ユーザーによる最近のアクティビティの日時と種類。

動作の仕組み

次の図は、通常の操作中のローカルホストキャッシュのコンポーネントと通信パスを示しています。

ローカルホストキャッシュの通常の操作中の通信パスの図(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/lhc-normal1.png)

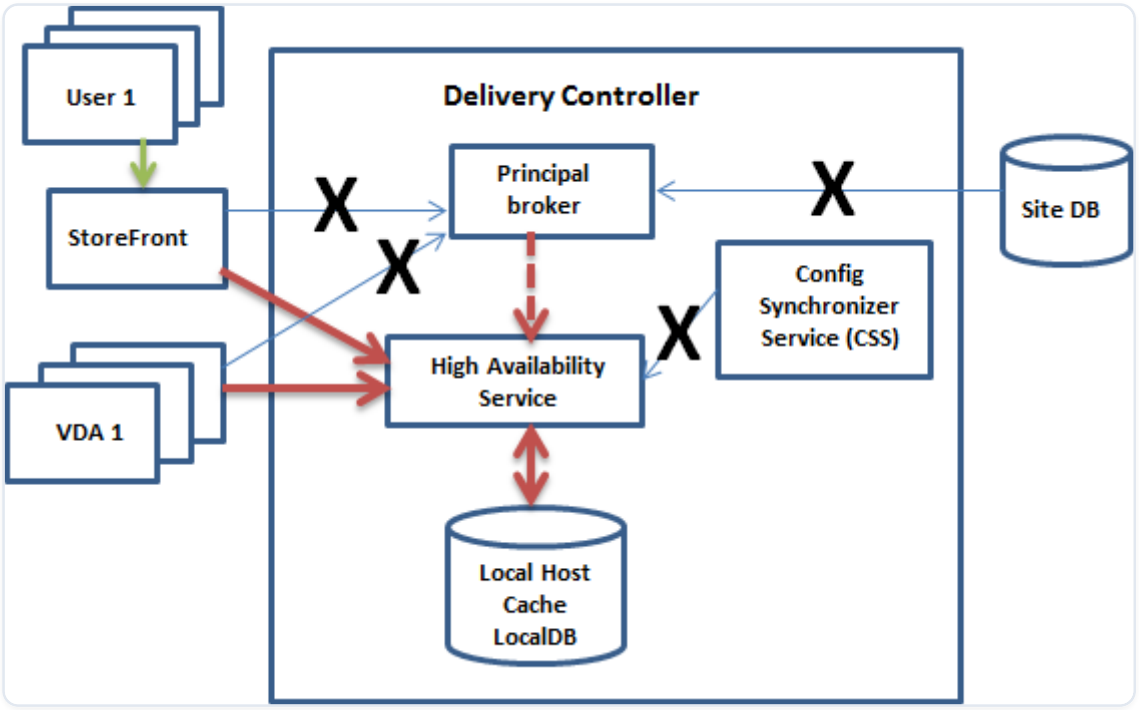
通常の操作中

- Controller上の *プリンシパルブローカー* (Citrix Broker Service) は、StoreFrontからの接続要求を受け入れます。ブローカーはサイトデータベースと通信し、ユーザーをControllerに登録されているVDAに接続します。
- Citrix Config Synchronizer Service (CSS) は、約5分ごとにブローカーに問い合わせて、変更があったかどうかを確認します。これらの変更は、管理者によって開始されたもの（デリバリーグループのプロパティの変更など）またはシステムアクション（マシンの割り当てなど）である可能性があります。
- 前回のチェック以降に構成変更があった場合、CSS は情報を Controller 上のセカンダリブローカーに同期 (コピー) します。(セカンダリブローカーは高可用性サービスとも呼ばれます。)

  前回のチェック以降に変更された項目だけでなく、すべての構成データがコピーされます。CSS は構成データを Controller 上の Microsoft SQL Server Express LocalDB データベースにインポートします。このデータベースはローカルホストキャッシュデータベースと呼ばれます。CSS は、ローカルホストキャッシュデータベースの情報がサイトデータベースの情報と一致することを確認します。ローカルホストキャッシュデータベースは、同期が行われるたびに再作成されます。

  Microsoft SQL Server Express LocalDB (ローカルホストキャッシュデータベースで使用) は、Controller をインストールするときに自動的にインストールされます。(コマンドラインから Controller をインストールする際に、このインストールを禁止できます。) ローカルホストキャッシュデータベースは、複数の Controller 間で共有できません。ローカルホストキャッシュデータベースをバックアップする必要はありません。構成変更が検出されるたびに再作成されます。
- 前回のチェック以降に変更がない場合、データはコピーされません。

次の図は、プリンシパルブローカーがサイトデータベースとの接続を失った場合 (停止が開始された場合) の通信パスの変化を示しています。



停止中

停止が開始されると:

- セカンダリブローカーは接続要求のリッスンと処理を開始します。
- 停止が開始されると、セカンダリブローカーは最新の VDA 登録データを持っていませんが、VDA がセカンダリブローカーと通信すると、登録プロセスがトリガーされます。そのプロセス中に、セカンダリブローカーはその VDA に関する現在のセッション情報も取得します。
- セカンダリブローカーが接続を処理している間、ブローカリングプリンシパルは接続を監視し続けます。接続が復元されると、ブローカリングプリンシパルはセカンダリブローカーに接続情報のリッスンを停止するよう指示し、ブローカリングプリンシパルはブローカリング操作を再開します。次に VDA がブローカリングプリンシパルと通信するときに、登録プロセスがトリガーされます。セカンダリブローカーは、以前の停止からの残りの VDA 登録をすべて削除します。CSS は、展開で構成変更が発生したことを認識すると、情報の同期を再開します。

同期中に停止が開始されるという万が一の事態が発生した場合、現在のインポートは破棄され、最後に認識された構成が使用されます。

イベントログ には、同期と停止に関する情報が提供されます。

停止モードでの運用に時間制限はありません。

通常モードと停止モード間の移行は、既存のセッションには影響しません。新しいセッションの起動のみに影響します。

意図的に停止をトリガーすることもできます。その理由と方法の詳細については、Force an outageを参照してください。

複数のControllerがあるサイト

CSSは、他のタスクの中でも、ゾーン内のすべてのControllerに関する情報をセカンダリブローカーに定期的に提供します。(展開に複数のゾーンが含まれていない場合、このアクションはサイト内のすべてのControllerに影響します。)その情報を持つことで、各セカンダリブローカーは、ゾーン内の他のControllerで実行されているすべてのピアセカンダリブローカーについて認識します。

セカンダリブローカーは、別のチャネルで相互に通信します。これらのブローカーは、停止が発生した場合にゾーン内でブローカー操作を行うセカンダリブローカーを決定（選出）するために、実行されているマシンのFQDN名のアルファベット順リストを使用します。停止中、すべてのVDAは選出されたセカンダリブローカーに登録します。ゾーン内の選出されていないセカンダリブローカーは、受信接続およびVDA登録要求を積極的に拒否します。

停止中に選出されたセカンダリブローカーが失敗した場合、別のセカンダリブローカーが引き継ぐために選出され、VDAは新しく選出されたセカンダリブローカーに登録します。

停止中にControllerが再起動された場合：

- そのControllerが選出されたブローカーでない場合、再起動による影響はありません。
- そのControllerが選出されたブローカーである場合、別のControllerが選出され、VDAが登録されます。再起動されたControllerが起動すると、自動的にブローカー処理を引き継ぎ、VDAが再度登録されます。このシナリオでは、登録中にパフォーマンスが影響を受ける可能性があります。

通常の操作中にControllerの電源をオフにし、停止中に電源をオンにした場合、そのControllerがブローカーとして選出されても、そのControllerではローカルホストキャッシュを使用できません。

イベントログは、選出に関する情報を提供します。

停止中に利用できないもの、およびその他の違い

停止モードでの運用に時間制限はありません。ただし、Citrixは可能な限り迅速に接続を復元することを推奨しています。

停止中：

- Studioを使用できません。
- PowerShell SDKへのアクセスは制限されます。

    - まず、次の操作を行う必要があります。
        - 値が1のレジストリキー `EnableCssTestMode` を追加します: `New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTestMode -PropertyType DWORD -Value 1`
        - ポート89を使用します: `Get-BrokerMachine -AdminAddress localhost:89 | Select MachineName, ContollerDNSName, DesktopGroupName, RegistrationState`
    - これらのコマンドを実行すると、以下にアクセスできます。
        - すべての `Get-Broker*` コマンドレット。

- ハイパーバイザーの資格情報はホストサービスから取得できません。すべてのマシンは不明な電源状態になり、電源操作は発行できません。ただし、電源がオンになっているホスト上のVMは、接続要求に使用できます。
- 割り当てられたマシンは、通常の操作中に割り当てが行われた場合にのみ使用できます。停止中は新しい割り当てを行うことはできません。
- リモートPCアクセス マシンの自動登録と構成はできません。ただし、通常の操作中に登録および構成されたマシンは使用できます。
- サーバーでホストされているアプリケーションおよびデスクトップのユーザーは、リソースが異なるゾーンにある場合、構成されているセッション制限よりも多くのセッションを使用する可能性があります。
- ユーザーは、現在アクティブ/選出されているセカンダリブローカーを含むゾーン内の登録済みVDAからのみアプリケーションとデスクトップを起動できます。停止中は、ゾーンをまたいだ起動（あるゾーンのセカンダリブローカーから別のゾーンのVDAへの起動）はサポートされません。
- デリバリーグループ内のVDAのスケジュールされた再起動が開始される前にサイトデータベースの停止が発生した場合、再起動は停止が終了したときに開始されます。これにより、予期しない結果が生じる可能性があります。詳しくは、「データベースの停止によりスケジュールされた再起動が遅延する」を参照してください。
- ゾーン優先度 は構成できません。構成されている場合でも、セッション起動時には優先度は考慮されません。
- タグがゾーンの指定に使用されるタグ制限 は、セッション起動ではサポートされません。このようなタグ制限が構成され、StoreFrontストアの高度なヘルスチェック オプションが有効になっている場合、セッションの起動が断続的に失敗する可能性があります。

アプリケーションとデスクトップのサポート

ローカルホストキャッシュは、サーバーでホストされるアプリケーションとデスクトップ、および静的（割り当て済み）デスクトップをサポートします。

ローカルホストキャッシュは、プールされたデリバリーグループ内のデスクトップVDAを次のようにサポートします。

- デフォルトでは、`ShutdownDesktopsAfterUse`プロパティが有効になっているプールされたデリバリーグループ（MCSまたはCitrix Provisioning™によって作成されたもの）内の電源管理されたデスクトップVDAは、ローカルホストキャッシュイベント中に新しい接続に利用できません。このデフォルトを変更して、ローカルホストキャッシュ中にこれらのデスクトップを使用できるようにすることができます。

  ただし、停止中の電源管理に頼ることはできません。（通常の操作が再開された後、電源管理が再開されます。）また、これらのデスクトップは再起動されていないため、以前のユーザーのデータが含まれている可能性があります。
- デフォルトの動作を上書きするには、サイト全体で、および影響を受ける各デリバリーグループで有効にする必要があります。次のPowerShellコマンドレットを実行します。

  サイト全体：

  ```
  Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
  ```

  影響を受ける各デリバリーグループに対して、次のPowerShellコマンドを実行します。

  ```
  Set-BrokerDesktopGroup -Name "name" -ReuseMachinesWithoutShutdownInOutage $true
  ```

  サイトおよびデリバリーグループでこの機能を有効にしても、構成された`ShutdownDesktopsAfterUse`プロパティが通常の操作中にどのように機能するかには影響しません。この機能が有効になっている場合、LHCイベントが完了してもVDAは自動的に再起動しません。プールされたデリバリーグループ内の電源管理されたデスクトップVDAは、VDAが再起動されるまで以前のセッションのデータを保持できます。これは、ユーザーが非LHC操作中にVDAからログオフした場合、または再起動が手動でトリガーされた場合に発生する可能性があります。

> **重要:**

> サイトレベルでReuseMachinesWithoutShutdownInOutageAllowedを有効にし、デリバリーグループレベルでReuseMachinesWithoutShutdownInOutageを有効にしないと、ローカルホストキャッシュイベント中にプールされたデリバリーグループ内の電源管理されたデスクトップVDAへのすべてのセッション起動試行が失敗します。

RAM サイズに関する考慮事項

LocalDBサービスは、約1.2 GBのRAM（データベースキャッシュに最大1 GB、SQL Server Express LocalDBの実行に200 MB）を使用できます。障害が長期間続き、多くのログオンが発生する場合（たとえば、10,000ユーザーで12時間）、セカンダリブローカーは最大1 GBのRAMを使用できます。これらのメモリ要件は、コントローラーの通常のRAM要件に追加されるため、合計RAM容量を増やす必要がある場合があります。

サイトデータベースにSQL Server Expressインストールを使用している場合、サーバーには2つのsqlserver.exeプロセスがあります。

CPU コアとソケット構成に関する考慮事項

コントローラーのCPU構成、特にSQL Server Express LocalDBで利用可能なコア数は、メモリ割り当てよりもさらに、ローカルホストキャッシュのパフォーマンスに直接影響します。このCPUオーバーヘッドは、データベースに到達できず、セカンダリブローカーがアクティブな障害期間中にのみ観測されます。

LocalDBは複数のコア（最大4つ）を使用できますが、単一のソケットに制限されています。ソケットを追加してもパフォーマンスは向上しません（たとえば、1コアずつ4つのソケットがある場合）。代わりに、Citrixは複数のコアを持つ複数のソケットを使用することを推奨しています。Citrixのテストでは、2x3（2ソケット、3コア）構成は4x1および6x1構成よりも優れたパフォーマンスを提供しました。

ストレージに関する考慮事項

障害中にユーザーがリソースにアクセスすると、LocalDBは増大します。たとえば、1秒あたり10ログオンで実行されるログオン/ログオフテスト中に、データベースは2〜3分ごとに1 MB増加しました。通常の操作が再開されると、ローカルデータベースが再作成され、スペースが返されます。ただし、障害中のデータベースの増大を許容するために、LocalDBがインストールされているドライブに十分なスペースが利用可能である必要があります。ローカルホストキャッシュは、障害中により多くのI/Oも発生させます。約3 MB/秒の書き込みと、数十万回の読み取りです。

パフォーマンスに関する考慮事項

障害発生時には、1つのセカンダリブローカーがすべての接続を処理するため、通常の操作中に複数のコントローラー間で負荷分散を行うサイト（またはゾーン）では、選出されたセカンダリブローカーが障害発生時に通常よりもはるかに多くの要求を処理する必要がある場合があります。したがって、CPUの要求は高くなります。サイト（ゾーン）内のすべてのセカンダリブローカーは、ローカルホストキャッシュデータベースと影響を受けるすべてのVDAによって課される追加の負荷を処理できる必要があります。これは、障害発生時に選出されるセカンダリブローカーが変更される可能性があるためです。

VDIの制限:

- シングルゾーンVDI展開では、障害発生時に最大10,000台のVDAを効果的に処理できます。
- マルチゾーンVDI展開では、停止中に各ゾーンで最大10,000のVDA、サイト全体で最大40,000のVDAを効果的に処理できます。例えば、以下の各サイトは停止中に効果的に処理できます。
  - 4つのゾーンを持ち、各ゾーンに10,000のVDAを含むサイト。
  - 7つのゾーンを持ち、1つは10,000のVDAを含み、残りの6つはそれぞれ5,000のVDAを含むサイト。

停止中、サイト内の負荷管理が影響を受ける可能性があります。負荷評価器（特にセッション数ルール）が超過する可能性があります。

すべてのVDAがセカンダリブローカーに登録するのにかかる間、そのサービスは現在のセッションに関する完全な情報を持っていない可能性があります。そのため、その期間中のユーザー接続要求は、既存のセッションへの再接続が可能であったとしても、新しいセッションが起動される結果となる可能性があります。この期間（「新しい」セカンダリブローカーが再登録中にすべてのVDAからセッション情報を取得する間）は避けられません。停止が開始されたときに接続されているセッションは移行期間中に影響を受けませんが、新しいセッションやセッションの再接続は影響を受ける可能性があります。

この期間は、VDAが登録する必要がある場合に発生します。

- 停止が開始されたとき: プリンシパルブローカーからセカンダリブローカーに移行するとき。
- 停止中のセカンダリブローカーの障害: 障害が発生したセカンダリブローカーから新しく選出されたセカンダリブローカーに移行するとき。
- 停止からの復旧: 通常の操作が再開され、プリンシパルブローカーが制御を再開するとき。

Citrix Broker Protocolの`HeartbeatPeriodMs`レジストリ値（デフォルト = 600000 ms、つまり10分）を下げることで、間隔を短縮できます。このハートビート値は、VDAがpingに使用する間隔の2倍であるため、デフォルト値では5分ごとにpingが実行されます。

例えば、次のコマンドはハートビートを5分（300000ミリ秒）に変更し、2.5分ごとにpingが実行されるようにします。

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer -Name HeartbeatPeriodMs -PropertyType DWORD –Value 300000
```

ハートビート値を変更する際は注意してください。頻度を上げると、通常モードと停止モードの両方でControllerへの負荷が増大します。

VDAがどれだけ迅速に登録されても、この間隔を完全に排除することはできません。

セカンダリブローカー間の同期にかかる時間は、オブジェクト（VDA、アプリケーション、グループなど）の数が増えるにつれて長くなります。例えば、5000のVDAを同期するには10分以上かかる場合があります。

XenApp 6.xリリースとの違い

このローカルホストキャッシュの実装は、XenApp 6.xおよびそれ以前のXenAppリリースにおけるローカルホストキャッシュ機能と同じ名前を共有していますが、大幅な改善が施されています。この実装は、より堅牢で破損の影響を受けません。定期的な`dsmaint`コマンドの必要性を排除するなど、メンテナンス要件が最小限に抑えられています。このローカルホストキャッシュは、技術的には全く異なる実装です。

ローカルホストキャッシュの管理

ローカルホストキャッシュが正しく機能するには、各ControllerのPowerShell実行ポリシーをRemoteSigned、Unrestricted、またはBypassに設定する必要があります。

SQL Server エクスプレス ローカルDB

ローカルホストキャッシュが使用するMicrosoft SQL Server Express LocalDBソフトウェアは、Controllerをインストールするか、バージョン7.9より前のControllerをアップグレードする際に自動的にインストールされます。このデータベースと通信するのはセカンダリブローカーのみです。PowerShellコマンドレットを使用して、このデータベースに関する何かを変更することはできません。LocalDBは複数のController間で共有できません。

SQL Server Express LocalDBデータベースソフトウェアは、ローカルホストキャッシュが有効になっているかどうかにかかわらずインストールされます。

そのインストールを防ぐには、`XenDesktopServerSetup.exe`コマンドを使用してControllerをインストールまたはアップグレードし、`/exclude "Local Host Cache Storage (LocalDB)"`オ

プションを含めます。ただし、ローカルホストキャッシュ機能はデータベースなしでは機能せず、セカンダリブローカーで別のデータベースを使用することはできないことに注意してください。

このLocalDBデータベースのインストールは、サイトデータベースとして使用するためにSQL Server Expressをインストールするかどうかには影響しません。

以前のSQL Server Express LocalDBバージョンを新しいバージョンに置き換える方法については、「Replace SQL Server Express LocalDB」を参照してください。

製品のインストールとアップグレード後のデフォルト設定

Citrix Virtual Apps and Desktopsの新規インストール時（最小バージョン7.16）には、ローカルホストキャッシュが有効になります。

アップグレード後（バージョン7.16以降）は、展開全体で10,000未満のVDAがある場合、ローカルホストキャッシュが有効になります。

ローカルホストキャッシュの有効化と無効化

- ローカルホストキャッシュを有効にするには、次のように入力します。

  ```
  Set-BrokerSite -LocalHostCacheEnabled $true
  ```

  ローカルホストキャッシュが有効になっているかどうかを確認するには、`Get-BrokerSite`と入力します。`LocalHostCacheEnabled`プロパティが`True`であることを確認します。
- ローカルホストキャッシュを無効にするには、次のように入力します。

  ```
  Set-BrokerSite -LocalHostCacheEnabled $false
  ```

注意: XenAppおよびXenDesktop 7.16以降、接続リース（バージョン7.6からローカルホストキャッシュに先行していた機能）は製品から削除され、利用できなくなりました。

ローカルホストキャッシュが機能していることを確認する

ローカルホストキャッシュが正しく設定され、機能していることを確認するには：

- 同期インポートが正常に完了していることを確認します。イベントログを確認してください。
- 各Delivery ControllerにSQL Server Express LocalDBデータベースが作成されていることを確認します。これにより、必要に応じてセカンダリブローカーが引き継ぐことができることが確認されます。
  - Delivery Controllerサーバーで、`C:\Windows\ServiceProfiles\NetworkService`を参照します。

    - `HaDatabaseName.mdf`と`HaDatabaseName_log.ldf`が作成されていることを確認します。

- Delivery Controllerで障害を強制的に発生させます。ローカルホストキャッシュが機能することを確認したら、すべてのControllerを通常モードに戻すことを忘れないでください。これには約15分かかる場合があります。

イベントログ

イベントログは、同期と障害が発生した時期を示します。イベントビューアログでは、障害モードは*HAモード*と呼ばれます*。

構成同期サービス:

通常の操作中、CSSがローカルホストキャッシュブローカーを使用して構成データをローカルホストキャッシュデータベースにインポートする際に、次のイベントが発生する可能性があります。

- 503: Citrix Config Sync Serviceが更新された構成を受信しました。このイベントは、同期プロセスの開始を示します。
- 504: Citrix Config Sync Serviceが更新された構成をインポートしました。構成のインポートが正常に完了しました。
- 505: Citrix Config Sync Serviceがインポートに失敗しました。構成のインポートは正常に完了しませんでした。以前に正常な構成が利用可能な場合、障害発生時にそれが使用されます。ただし、それは現在の構成から古くなっています。以前の構成が利用できない場合、サービスは障害発生時にセッションブローカーに参加できません。この場合、トラブルシューティングセクションを参照し、Citrixサポートに連絡してください。
- 507: システムが障害モードであり、ローカルホストキャッシュブローカーがブローカー処理に使用されているため、Citrix Config Sync Serviceがインポートを中止しました。サービスは新しい構成を受信しましたが、障害が発生したためインポートは中止されました。これは予期される動作です。
- 510: プライマリ構成サービスから構成サービス構成データが受信されませんでした。
- 517: プライマリブローカーとの通信中に問題が発生しました。
- 518: セカンダリブローカー（高可用性サービス）が実行されていないため、構成同期スクリプトが中止されました。

高可用性サービス:

このサービスは、ローカルホストキャッシュブローカーとも呼ばれます。

- 3502: 停止が発生し、ローカルホストキャッシュブローカーがブローカー操作を実行しています。
- 3503: 停止が解決され、通常の操作が再開されました。
- 3504: どのローカルホストキャッシュブローカーが選出されたか、および選出に関与した他のローカルホストキャッシュブローカーを示します。

停止を強制する

意図的に停止を強制したい場合があります。

- ネットワークが繰り返しダウンする場合。ネットワークの問題が解決されるまで停止を強制すると、通常モードと停止モード間の継続的な移行（およびその結果として頻繁に発生するVDA登録ストーム）を防ぐことができます。
- ディザスタリカバリ計画をテストするため。
- ローカルホストキャッシュが正しく機能していることを確認するため。
- サイトデータベースサーバーの交換または保守中。

停止を強制するには、Delivery Controller を含む各サーバーのレジストリを編集します。`HKLM\Software\Citrix\DesktopServer\LHC`で、`OutageModeForced`を`REG_DWORD`として`1`に作成して設定します。この設定により、データベースの状態に関係なく、ローカルホストキャッシュブローカーは停止モードに入ります。値を`0`に設定すると、ローカルホストキャッシュブローカーは停止モードを終了します。

イベントを確認するには、`C:\ProgramData\Citrix\WorkspaceCloud\Logs\Plugins\HighAvailabilityService`にある`Current_HighAvailabilityService`ログファイルを監視します。

トラブルシューティング

ローカルホストキャッシュデータベースへの同期インポートが失敗し、505イベントが投稿された場合、いくつかのトラブルシューティングツールが利用可能です。

CDFトレース: `ConfigSyncServer`および`BrokerLHC`モジュールのオプションが含まれています。これらのオプションは、他のブローカーモジュールとともに、問題を特定するのに役立つでしょう。

レポート: 同期インポートが失敗した場合、レポートを生成できます。このレポートは、エラーの原因となっているオブジェクトで停止します。このレポート機能は同期速度に影響するため、Citrixは使用しないときは無効にすることを推奨します。

CSSトレースレポートを有効にして生成するには、次のコマンドを入力します。

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -PropertyType DWORD -Value 1
```

HTMLレポートは`C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\CitrixBrokerConfigSyncReport.htm`に投稿されます。

レポートが生成されたら、レポート機能を無効にするには次のコマンドを入力します。

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -Value 0
```

ブローカー構成のエクスポート: デバッグ目的で正確な構成を提供します。

```
Export-BrokerConfiguration | Out-File <file-pathname>
```

例: `Export-BrokerConfiguration | Out-File C:\\BrokerConfig.xml`。

仮想IPおよび仮想ループバック

> **重要:**

> Windows 10 Enterprise マルチセッションは、リモートデスクトップIP仮想化 (仮想IP) をサポートしていません。また、弊社はWindows 10 Enterprise マルチセッションで仮想IPも仮想ループバックもサポートしていません。

> 仮想IPおよび仮想ループバック機能は、Windows Server 2016マシンでサポートされています。これらの機能は、WindowsデスクトップOSマシンには適用されません。

Microsoftの仮想IPアドレス機能は、公開アプリケーションにセッションごとに一意の動的に割り当てられたIPアドレスを提供します。Citrixの仮想ループバック機能を使用すると、localhost (デフォルトでは127.0.0.1) との通信に依存するアプリケーションを、localhost範囲 (127.*) 内の一意の仮想ループバックアドレスを使用するように構成できます。

CRMやCTI（Computer Telephony Integration）などの特定のアプリケーションは、アドレス指定、ライセンス、識別、または一意のIPアドレスやループバックアドレスを必要とするその他の目的でIPアドレスを使用します。他のアプリケーションは静的ポートにバインドする可能性があるため、マルチユーザー環境でアプリケーションの追加インスタンスを起動しようとすると、ポート

が使用中であるために失敗します。このようなアプリケーションがCitrix Virtual Apps™環境で正しく機能するには、デバイスごとに一意のIPアドレスが必要です。

仮想IPと仮想ループバックは独立した機能です。どちらか一方、または両方を使用できます。

管理者アクションの概要:

- Microsoft仮想IPを使用するには、Windowsサーバーで有効にして構成します。(Citrix®ポリシー設定は不要です。)
- Citrix仮想ループバックを使用するには、Citrixポリシーで2つの設定を構成します。

仮想IP

仮想IPがWindowsサーバーで有効になり構成されると、セッションで実行されている構成済みの各アプリケーションは、一意のアドレスを持っているように見えます。ユーザーは、他の公開アプリケーションにアクセスするのと同じ方法で、Citrix Virtual Appsサーバー上のこれらのアプリケーションにアクセスします。プロセスが仮想IPを必要とするのは、次のいずれかのケースです。

- プロセスがハードコードされたTCPポート番号を使用している
- プロセスがWindowsソケットを使用しており、一意のIPアドレスまたは指定されたTCPポート番号を必要としている

アプリケーションが仮想IPアドレスを使用する必要があるかどうかを判断するには:

1. MicrosoftからTCPViewツールを入手します。このツールは、特定のIPアドレスとポートをバインドするすべてのアプリケーションを一覧表示します。
2. ホスト名ではなくアドレスが表示されるように、機能を無効にします。
3. アプリケーションを起動し、TCPViewを使用して、アプリケーションが開いているIPアドレスとポート、およびこれらのポートを開いているプロセス名を確認します。
4. サーバーのIPアドレス、0.0.0.0、または127.0.0.1を開くプロセスを構成します。
5. アプリケーションが異なるポートで同じIPアドレスを開かないようにするには、アプリケーションの別のインスタンスを起動します。

Microsoft Remote Desktop (RD) IP仮想化の仕組み

- Microsoftサーバーで仮想IPアドレス指定を有効にする必要があります。

  たとえば、Windows Server 2016環境では、サーバーマネージャーから **>** を展開して、RD IP仮想化機能を有効にし、セッションごとまたはプログラムごとに動的ホスト構成プロトコル

（DHCP）サーバーを使用してIPアドレスを動的に割り当てる設定を構成します。手順については、Microsoftのドキュメントを参照してください。

- この機能が有効になると、セッションの起動時に、サーバーはDHCPサーバーから動的に割り当てられたIPアドレスを要求します。
- RD IP仮想化機能は、リモートデスクトップ接続にセッションごとまたはプログラムごとにIPアドレスを割り当てます。複数のプログラムにIPアドレスを割り当てる場合、それらはセッションごとのIPアドレスを共有します。
- セッションにアドレスが割り当てられると、以下の呼び出しが行われるたびに、システムプライマリIPアドレスではなく仮想アドレスがセッションで使用されます:
  `bind`, `closesocket`, `connect`, `WSAConnect`, `WSAAccept`, `getpeername`, `getsockname`, `sendto`, `WSASendTo`, `WSASocketW`, `gethostbyaddr`, `getnameinfo`, `getaddrinfo`。

リモートデスクトップセッションホスティング構成内でMicrosoft IP仮想化機能を使用する場合、アプリケーションとWinsock関数呼び出しの間に「フィルター」コンポーネントを挿入することで、アプリケーションは特定のIPアドレスにバインドされます。これにより、アプリケーションは使用すべき正しいIPアドレスのみを認識します。アプリケーションがTCPまたはUDP通信をリッスンしようとすると、自動的に割り当てられた仮想IPアドレス（またはループバックアドレス）にバインドされます。アプリケーションによって開かれた発信接続はすべて、アプリケーションにバインドされたIPアドレスから発信されます。

アドレスを返す関数（Windowsポリシーによって制御される `GetAddrInfo()` など）でローカルホストのIPアドレスが要求された場合、仮想IPは返されたIPアドレスを確認し、それをセッションの仮想IPアドレスに変更します。このような名前関数を介してローカルサーバーのIPアドレスを取得しようとするアプリケーションは、そのセッションに割り当てられた一意の仮想IPアドレスのみを認識します。このIPアドレスは、bindやconnectなどの後続のソケット呼び出しでよく使用されます。Windowsポリシーの詳細については、「RDS IP Virtualization in Windows Server」を参照してください。

多くの場合、アプリケーションはアドレス0.0.0.0でリッスンするためにポートへのバインドを要求します。アプリケーションがこれを行い、静的ポートを使用する場合、アプリケーションの複数のインスタンスを起動することはできません。仮想IPアドレス機能は、これらの呼び出しタイプで0.0.0.0も検索し、特定の仮想IPアドレスでリッスンするように呼び出しを変更します。これにより、複数のアプリケーションが同じコンピューター上の同じポートでリッスンできるようになります。これは、すべて異なるアドレスでリッスンしているためです。呼び出しは、ICAセッション内であり、仮想IPアドレス機能が有効になっている場合にのみ変更されます。たとえば、異なるセッションで実行されているアプリケーションの2つのインスタンスが、両方ともすべてのインターフェイス（0.0.0.0）と特定のポート（9000など）にバインドしようとすると、それらはVIPAddress1:9000とVIPAddress2:9000にバインドされ、競合は発生しません。

仮想ループバック

Citrix仮想IPループバックポリシー設定を有効にすると、各セッションが通信用に独自のループバックアドレスを持つことができます。アプリケーションがWinsock呼び出しでlocalhostアドレス（デフォルト = 127.0.0.1）を使用する場合、仮想ループバック機能は127.0.0.1を127.X.X.Xに置き換えます。ここで、X.X.Xはセッション ID + 1を表します。たとえば、セッションIDが7の場合、アドレスは127.0.0.8になります。セッションIDが4番目のオクテット（255より大きい）を超えるという万が一の事態が発生した場合、アドレスは次のオクテット（127.0.1.0）に繰り上がり、最大127.255.255.255までとなります。

プロセスが仮想ループバックを必要とするのは、次のいずれかのケースです。

- プロセスがWindowsソケットループバック（localhost）アドレス（127.0.0.1）を使用している場合
- プロセスがハードコードされたTCPポート番号を使用している場合

プロセス間通信にループバックアドレスを使用するアプリケーションには、仮想ループバックポリシー設定を使用します。追加の構成は不要です。仮想ループバックは仮想IPに依存しないため、Microsoftサーバーを構成する必要はありません。

- 仮想IPループバックサポート。有効にすると、このポリシー設定により、各セッションが独自の仮想ループバックアドレスを持つことができます。この設定はデフォルトで無効になっています。この機能は、仮想IP仮想ループバックプログラムリストポリシー設定で指定されたアプリケーションにのみ適用されます。
- 仮想IP仮想ループバックプログラムリスト。このポリシー設定は、仮想IPループバック機能を使用するアプリケーションを指定します。この設定は、仮想IPループバックサポートポリシー設定が有効になっている場合にのみ適用されます。

関連機能

仮想IPよりも仮想ループバックが優先されるように、以下のレジストリ設定を使用できます。この機能は「優先ループバック」と呼ばれます。ただし、注意して進めてください。

- 優先ループバックは、仮想IPと仮想ループバックの両方が有効になっている場合にのみ使用してください。そうしないと、予期しない結果が生じる可能性があります。
- レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrixは、レジストリエディターの誤った使用によって生じる問題が解決できることを保証できません。レジストリエディターは自己責任で使用してください。編集する前に必ずレジストリをバックアップしてください。

アプリケーションが常駐するサーバーでregeditを実行します。

- `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP`
- 名前: PreferLoopback, 種類: REG_DWORD, データ: 1
- 名前: PreferLoopbackProcesses, 種類: REG_MULTI_SZ, データ: \<プロセスのリスト\>

デリバリーコントローラー

Delivery Controllerは、ユーザーアクセスの管理、接続の仲介と最適化を担当するサーバー側コンポーネントです。コントローラーは、デスクトップおよびサーバーイメージを作成するMachine Creation Services™も提供します。

サイトには少なくとも1つのコントローラーが必要です。最初のコントローラーをインストールした後、サイトの作成時または後でコントローラーを追加できます。サイトに複数のコントローラーを配置することには、主に2つの利点があります。

- **冗長性:** ベストプラクティスとして、本番サイトでは、常に異なる物理サーバー上に少なくとも2つのコントローラーを配置してください。1つのコントローラーが故障した場合でも、他のコントローラーが接続を管理し、サイトを管理できます。
- **スケーラビリティ:** サイトのアクティビティが増加すると、コントローラーのCPU使用率とデータベースのアクティビティも増加します。追加のコントローラーにより、より多くのユーザー、アプリケーション、およびデスクトップ要求を処理できるようになり、全体的な応答性を向上させることができます。

各コントローラーはサイトデータベースと直接通信します。複数のゾーンがあるサイトでは、各ゾーンのコントローラーは、プライマリゾーンのサイトデータベースと通信します。

> **重要:**
>
> サイトの構成後、コントローラーのコンピューター名またはドメインメンバーシップを変更しないでください。

VDAがコントローラーに登録する方法

VDAを使用する前に、サイト内のDelivery Controllerに登録（通信を確立）する必要があります。VDA登録の詳細については、「VDA registration with Controllers」を参照してください。

コントローラーの追加、削除、または移動

コントローラーを追加、削除、または移動するには、「Databases」の記事に記載されているサーバーロールとデータベースロールの権限が必要です。

SQLクラスタリングまたはSQLミラーリングインストール内のノードにコントローラーをインストールすることはサポートされていません。

サイトにDelivery Controller™を追加するときは、高可用性のために使用するすべてのレプリカSQL Serverに、そのマシンのログオン資格情報を追加してください。

展開でデータベースミラーリングを使用している場合:

- コントローラーを追加、削除、または移動する前に、プリンシパルデータベースとミラーデータベースの両方が実行されていることを確認してください。さらに、SQL Server Management Studioでスクリプトを使用している場合は、スクリプトを実行する前にSQLCMDモードを有効にしてください。
- コントローラーを追加、削除、または移動した後にミラーリングを確認するには、PowerShell `Get-configdbconnection` コマンドレットを実行します。このコマンドレットは、ミラーへの接続文字列にフェールオーバーパートナーが設定されていることを確認します。

Controller を追加、削除、または移動した後:

- 自動更新が有効になっている場合、VDA は 90 分以内に更新された Controller のリストを受け取ります。
- 自動更新が有効になっていない場合は、すべての VDA で Controller ポリシー設定または ListOfDDCs レジストリキーが更新されていることを確認してください。Controller を別のサイトに移動した後、両方のサイトでポリシー設定またはレジストリキーを更新してください。

Controller を追加する

サイトの作成時および後から Controller を追加できます。このソフトウェアの以前のバージョンでインストールされた Controller を、このバージョンで作成されたサイトに追加することはできません。

1. サポートされているオペレーティングシステムを含むサーバーでインストーラーを実行します。Delivery Controller コンポーネントと、必要なその他のコアコンポーネントをインストールします。インストールウィザードを完了します。
2. サイトをまだ作成していない場合は、Studio を起動します。サイトの作成を促されます。サイト作成ウィザードの ページで、 ボタンをクリックし、追加の Controller をインストールしたサーバーのアドレスを追加します。

データベースを初期化するスクリプトを生成する予定がある場合は、スクリプトを生成する前に Controller を追加してください。

3. サイトをすでに作成している場合は、追加の Controller をインストールしたサーバーに Studio を向けます。 をクリックし、サイトアドレスを入力します。

Controller を削除する

サイトから Controller を削除しても、Citrix® ソフトウェアやその他のコンポーネントがアンインストールされるわけではありません。この操作により、Controller はデータベースから削除され、接続の仲介やその他のタスクの実行に使用できなくなります。Controller を削除しても、後で同じサイトまたは別のサイトに再度追加できます。サイトには少なくとも1つの Controller が必要であるため、Studio にリストされている最後の Controller を削除することはできません。

サイトから Controller を削除しても、データベースサーバーへの Controller のログオンは削除されません。これにより、同じマシン上の他の製品のサービスで使用されているログオンが誤って削除されるのを防ぎます。ログオンが不要になった場合は、手動で削除する必要があります。ログオンを削除するには、`securityadmin` サーバーロールの権限が必要です。

Controller を削除した後:

- 自動更新を使用しているVDAは、他の利用可能なコントローラーに再登録します。この再登録は、自動更新メカニズムが有効になっており、VDAが他のコントローラー（削除されたコントローラーと同じセカンダリゾーン内、またはオンプレミス展開のプライマリゾーン内）に到達できる場合にのみ発生します。
- Citrix StoreFrontでコントローラー情報を更新します。詳細については、「コントローラーの管理」を参照してください。
- Citrix StoreFrontで、Citrix Gatewayを介したリモートアクセス用のSecure Ticket Authority (STA) URLを更新します。詳細については、「Secure Ticket Authority の管理」を参照してください。
- Citrix Gatewayで、仮想サーバーのSTA URLを更新します。詳細については、「Citrix Gateway」を参照してください。

> **重要:**
>
> サイトからコントローラーを削除するまでは、Active Directoryからコントローラーを削除しないでください。

1. Studio が1時間以内にロードされるように、Controller の電源がオンになっていることを確認してください。Studio が削除する Controller をロードしたら、プロンプトが表示されたら Controller の電源をオフにします。
2. Studio ナビゲーションペインで を選択し、削除する Controller を選択します。
3. ペインで を選択します。適切なデータベースロールと権限がない場合は、データベース管理者が Controller を削除できるようにするスクリプトを生成するオプションが提示されます。
4. データベースサーバーから Controller のマシンアカウントを削除する必要があります。削除する前に、別サービスがそのアカウントを使用していないことを確認してください。

Studio を使用して Controller を削除した後、現在のタスクが適切に完了するように、その Controller へのトラフィックが短時間残る場合があります。短時間で Controller の削除を強制したい場合は、Citrix は、Controller がインストールされていたサーバーをシャットダウンするか、そのサーバーを Active Directory から削除することを推奨します。その後、サイト上の他の Controller を再起動して、削除された Controller とのそれ以上の通信がないことを確認します。

Controller を別のゾーンに移動する

サイトに複数のゾーンが含まれている場合、Controller を別のゾーンに移動できます。この移動が VDA 登録やその他の操作にどのように影響するかについては、「ゾーン」の記事を参照してください。

1. Studio ナビゲーションペインで を選択し、移動する Controller を選択します。
2. ペインで を選択します。
3. Controller を移動するゾーンを指定します。

Controller を別のサイトに移動する

このソフトウェアの以前のバージョンで作成されたサイトに Controller を移動することはできません。

1. Controller が配置されているサイト (古いサイト) で、Studio ナビゲーションペインで を選択します。次に、移動する Controller を選択します。
2. ペインで を選択します。適切なデータベース権限がない場合は、それらの権限を持つユーザー (データベース管理者など) が Controller を削除できるようにするスクリプトを生成できます。サイトには少なくとも1つの Controller が必要であるため、Studio にリストされている最後の Controller を削除することはできません。
3. 移動するControllerでStudioを開き、プロンプトが表示されたらサービスをリセットし、「**既存のサイトに参加**」を選択して、新しいサイトのアドレスを入力します。

VDA を別のサイトに移動する

Citrix Provisioning™ を使用してプロビジョニングされた VDA、または既存のイメージである VDA は、アップグレード時や、テストサイトで作成された VDA イメージを本番サイトに移動する際に、別のサイト（サイト 1 からサイト 2 へ）に移動できます。Machine Creation Services (MCS) を使用してプロビジョニングされた VDA は、あるサイトから別のサイトに移動できません。MCS は、VDA が Controller に登録するためにチェックする ListOfDDCs の変更をサポートしていません。MCS を使用してプロビジョニングされた VDA は、常に作成されたサイトに関連付けられた ListOfDDCs をチェックします。

VDA を別のサイトに移動する方法は、インストーラーを使用する方法と Citrix ポリシーを使用する方法の 2 つがあります。

インストーラー

インストーラーを実行し、サイト2のControllerのFQDN（DNSエントリ）を指定してControllerを追加します。

インストーラーでControllerを指定するのは、Controllerポリシー設定が使用されていない場合のみです。

グループポリシーエディター

次の例では、複数のVDAをサイト間で移動します。

1. サイト1で以下の設定を含むポリシーを作成し、そのポリシーをデリバリーグループレベルにフィルターして、サイト間の段階的なVDA移行を開始します。
    - Controller: サイト2の1つ以上のControllerのFQDN（DNSエントリ）を含みます。
    - Controllerの自動更新を有効にする: 無効に設定します。
2. デリバリーグループ内の各VDAは、新しいポリシーが適用されてから90分以内に通知を受け取ります。VDAは受信したControllerのリストを無視し（自動更新が無効になっているため）、ポリシーで指定されたControllerの1つを選択します。このポリシーにはサイト2のControllerがリストされています。
3. VDAがサイト2のControllerに正常に登録されると、サイト2のListOfDDCsとポリシー情報を受け取ります。これらはデフォルトで自動更新が有効になっています。VDAがサイト1で登録されていたControllerは、サイト2のControllerから送信されたリストには含まれていません。そのため、VDAはサイト2のリストにあるControllerの中から選択して再登録します。それ以降、VDAはサイト2からの情報で自動的に更新されます。

VDA登録

はじめに

> **注：**
>
> オンプレミス環境では、VDAはDelivery Controllerに登録します。Citrix Cloudサービス環境では、VDAはCloud Connectorに登録します。ハイブリッド環境では、一部のVDAはDelivery Controllerに登録し、他のVDAはCloud Connectorに登録します。

> VDAを使用する前に、サイト上の1つ以上のControllerまたはCloud Connectorに登録（通信を確立）する必要があります。VDAは、`ListofDDCs`と呼ばれるリストを確認して、ControllerまたはConnectorを見つけます。VDA上の`ListOfDDCs`には、そのVDAをサイト上のControllerまたはCloud Connectorにポイントするエントリが含まれています。負荷分散のために、VDAはリスト内のすべてのControllerまたはCloud Connectorに接続を自動的に分散します。

VDA登録がそれほど重要であるのはなぜですか？

- セキュリティの観点から見ると、登録は機密性の高い操作です。ControllerまたはCloud ConnectorとVDA間の接続を確立しています。このような機密性の高い操作では、すべてが完璧な状態でない場合、接続を拒否するのが期待される動作です。実質的に、VDAからControllerまたはCloud Connectorへ、およびControllerまたはCloud ConnectorからVDAへの2つの別々の通信チャネルを確立しています。接続にはKerberosが使用されるため、時刻同期やドメインメンバーシップの問題は許容されません。Kerberosはサービスプリンシパル名 (SPN) を使用するため、ロードバランスされたIP\ホスト名は使用できません。
- Controller（またはCloud Connector）を追加および削除する際に、VDAが正確で最新のControllerまたはCloud Connector情報を持っていない場合、VDAは、リストにないControllerまたはCloud Connectorによって仲介されるセッション起動を拒否する可能性があります。無効なエントリは、仮想デスクトップシステムソフトウェアの起動を遅らせる可能性があります。VDAは、不明で信頼できないControllerまたはCloud Connectorからの接続を受け入れません。

`ListofDDCs`に加えて、`ListOfSIDs`（セキュリティID）は、`ListofDDCs`内のどのマシンが信頼されているかを示します。`ListofSIDs`は、Active Directoryの負荷を軽減したり、侵害されたDNSサーバーからの潜在的なセキュリティ脅威を回避したりするために使用できます。詳細については、ListOfSIDsを参照してください。

`ListofDDCs`が複数のControllerまたはCloud Connectorを指定している場合、VDAはランダムな順序でそれらに接続しようとします。オンプレミス展開では、`ListofDDCs`にはControllerグループも含まれる場合があります。VDAは、`ListofDDCs`内の他のエントリに移動する前に、グループ内の各Controllerに接続しようとします。

Citrix Virtual Apps and Desktops™は、VDAのインストール中に構成されたControllerまたはCloud Connectorへの接続を自動的にテストします。ControllerまたはCloud Connectorに到達できない場合、エラーが表示されます。ControllerまたはCloud Connectorに接続できないという警告を無視した場合（またはVDAのインストール中にControllerまたはCloud Connectorのアドレスを指定しなかった場合）、メッセージが表示されて通知されます。

ControllerまたはCloud Connectorアドレスを構成する方法

管理者は、VDAが初めて登録するとき（初回登録）に使用する構成方法を選択します。初回登録中に、VDA上に永続的なキャッシュが作成されます。その後の登録では、構成の変更が検出されない限り、VDAはこのローカルキャッシュからControllerまたはCloud Connectorのリストを取得します。

その後の登録でそのリストを取得する最も簡単な方法は、自動更新機能を使用することです。自動更新はデフォルトで有効になっています。詳細については、「自動更新」を参照してください。

VDA上でControllerまたはCloud Connectorアドレスを構成する方法はいくつかあります。

- ポリシーベース（LGPOまたはGPO）
- レジストリベース（手動、グループポリシー設定（GPP）、VDAインストール時に指定）
- Active Directory OUベース（レガシーOU検出）
- MCSベース (personality.ini)

VDAをインストールする際に、初期登録方法を指定します。(自動更新を無効にした場合、VDAインストール時に選択した方法がその後の登録に使用されます。)

次の図は、VDAインストールウィザードの**Delivery Controller**ページを示しています。

VDAインストールウィザードのDelivery Controllerページ(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/vda-install-controllers-all.png)

ポリシーベース (LGPO\\GPO)

Citrix®は、初期VDA登録にGPOを使用することを推奨します。これは最も高い優先順位を持ちます。(自動更新が最も高い優先順位としてリストされていますが、自動更新は初期登録後にのみ使

用されます。) ポリシーベースの登録は、構成にグループポリシーを使用することによる一元化の利点を提供します。

この方法を指定するには、以下の両方の手順を完了します。

- VDAインストールウィザードの**Delivery Controller**ページで、**後で実行 (詳細設定)** を選択します。VDAインストール中にControllerアドレスを指定しない場合でも、ウィザードはControllerアドレスを指定するよう何度か通知します。(VDA登録はそれほど重要です。)
- `Virtual Delivery Agent Settings > Controllers`設定を使用して、Citrixポリシーを介してポリシーベースのVDA登録を有効または無効にします。(セキュリティが最優先事項である場合は、`Virtual Delivery Agent Settings > Controller SIDs`設定を使用します。)

この設定は`HKLM\Software\Policies\Citrix\VirtualDesktopAgent (ListOfDDCs)`に保存されます。

レジストリベース

この方法を指定するには、以下のいずれかの手順を完了します。

- VDAインストールウィザードの**Delivery Controller**ページで、**手動で実行** を選択します。次に、インストールされているControllerのFQDNを入力し、**追加** をクリックします。複数のControllerをインストールしている場合は、それらのアドレスを追加します。
- コマンドラインVDAインストールの場合、/controllersオプションを使用し、インストールされているControllerまたはCloud ConnectorのFQDNを指定します。

この情報は、レジストリキー`HKLM\Software\Citrix\VirtualDesktopAgent`または`HKLM\Software\Wow6432Node\Citrix\VirtualDesktopAgent`の下のレジストリ値`ListOfDDCs`に保存されます。

このレジストリキーを手動で構成することも、グループポリシー設定 (GPP) を使用することもできます。この方法は、ポリシーベースの方法よりも好ましい場合があります (たとえば、異なるControllerまたはCloud Connectorの条件付き処理が必要な場合。例: XDW-001-で始まるコンピューター名にはXDC-001を使用する)。

`ListOfDDCs` レジストリキーを更新します。このキーには、サイト内のすべてのControllerまたはCloud ConnectorのFQDNが一覧表示されます。(このキーはActive DirectoryサイトOUに相当します。)

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfDDCs (REG_SZ)`

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent`レジストリの場所に`ListOfDDCs`と`FarmGUID`の両方のキーが含まれている場合、`ListOfDDCs`がControllerまたはCloud Connectorの検出に使用されます。`FarmGUID`は、VDAのインストール中にサイトOUが指定された場合に存在します。(これはレガシー展開で使用される可能性があります。)

オプションで、`ListOfSIDs` レジストリキーを更新します (詳細については、「ListOfSIDs」を参照してください)。

```
HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs (REG_SZ)
```

注意：Citrixポリシーを介してポリシーベースのVDA登録も有効にすると、VDAインストール中に指定した設定が上書きされます。これは、ポリシーベースの登録の方が優先度の高い方法であるためです。

Active Directory OUベース (レガシー)

この方法は主に下位互換性のためにサポートされており、推奨されません。まだこの方法を使用している場合は、Citrixは別の方法に変更することを推奨します。

この方法を指定するには、以下の両方の手順を完了します。

- VDAインストールウィザードの **Delivery Controller** ページで、**Active Directoryから場所を選択** を選択します。
- `Set-ADControllerDiscovery.ps1` スクリプト (すべてのControllerで利用可能) を使用します。また、各VDAで `FarmGuid` レジストリエントリを構成して、適切なOUを指すようにします。この設定はグループポリシーを使用して構成できます。

詳細については、「Active Directory OUベースの検出」を参照してください。

MCSベース

MCSを使用してVMをプロビジョニングする場合、MCSはControllerまたはCloud Connectorのリストを設定します。この機能は自動更新と連携します。カタログの作成時、MCSは初期プロビジョニング中にControllerまたはCloud Connectorのリストを `Personality.ini` ファイルに挿入します。自動更新により、リストは最新の状態に保たれます。

この方法を指定するには、VDAインストールウィザードの **Delivery Controller** ページで、**Machine Creation Services™に任せる** を選択します。

レビューと推奨事項

ベストプラクティスとして:

- 初期登録にはグループポリシー登録方法を使用します。
- 自動更新（デフォルトで有効）を使用して、Controller のリストを最新の状態に保ちます。
- マルチゾーン展開では、初期構成にはグループポリシーを使用します（Controller または Cloud Connector が少なくとも2つある場合）。VDA を、そのゾーン内のローカルな Controller または Cloud Connector に向けます。自動更新を使用して、それらを最新の状態に保ちます。自動更新は、サテライトゾーンの VDA の `ListofDDCs` を自動的に最適化します。
- Controllerが利用できない場合の登録の問題を防ぐため、`ListOfDDCs`レジストリキーに複数のControllerをスペースまたはコンマで区切ってリストします。例：

```
DDC7x.xd.local DDC7xHA.xd.local



32-bit: HKEY_LOCAL_MACHINE
\Software\Citrix\VirtualDesktopAgent\ListOfDDCs



HKEY_LOCAL_MACHINE \Software\Citrix\VirtualDesktopAgent\ListOfDDCs
(REG_SZ)
```

- `ListofDDCs` の下にリストされているすべての値が有効な完全修飾ドメイン名にマッピングされていることを確認し、起動時の登録遅延を防ぎます。

自動更新

自動更新（XenApp および XenDesktop 7.6 で導入）は、デフォルトで有効になっています。これは、VDA 登録を最新の状態に保つための最も効率的な方法です。初期登録には使用されませんが、初期登録時に自動更新ソフトウェアが `ListofDDCs` をダウンロードし、VDA 上の永続キャッシュに保存します。このプロセスは、各 VDA に対して実行されます。キャッシュにはマシンポリシー情報も保持され、ポリシー設定が再起動後も維持されるようにします。

自動更新は、MCS または Citrix Provisioning™ を使用してマシンをプロビジョニングする場合にサポートされます。ただし、Citrix Provisioning のサーバー側キャッシュは除きます。サーバー側キャッシュは、自動更新キャッシュ用の永続ストレージがないため、一般的なシナリオではありません。

この方法を指定するには:

- 設定 `Virtual Delivery Agent Settings > Enable auto update of Controllers` を含む Citrix ポリシーを通じて、自動更新を有効または無効にします。この設定はデフォルトで有効になっています。

仕組み:

- VDA が再登録されるたびに（たとえば、マシンの再起動後）、キャッシュが更新されます。各 Controller または Cloud Connector も、90分ごとにサイトデータベースをチェックします。前回のチェック以降に Controller または Cloud Connector が追加または削除された場合、あるいは VDA 登録に影響するポリシー変更が発生した場合、Controller または Cloud Connector は登録済みの VDA に更新されたリストを送信し、キャッシュが更新されます。VDA は、最新のキャッシュされたリストにあるすべての Controller または Cloud Connector からの接続を受け入れます。
- VDA が、登録されている Controller または Cloud Connector を含まないリストを受け取った場合（つまり、その Controller または Cloud Connector がサイトから削除された場合）、VDA は、`ListofDDCs` 内の Controller または Cloud Connector の中から選択して再登録します。

例:

- 展開には、A、B、C の3つの Controller があります。VDA は Controller B に登録されます（これは VDA のインストール中に指定されました）。
- その後、2つの Controller（D と E）がサイトに追加されます。90分以内に、VDA は更新されたリストを受け取り、Controller A、B、C、D、E からの接続を受け入れます。（VDA が再起動されるまで、負荷はすべての Controller に均等に分散されません。）
- さらにその後、Controller B が別のサイトに移動されます。90分以内に、元のサイトの VDA は、前回のチェック以降に Controller の変更があったため、更新されたリストを受け取ります。元々 Controller B に登録されていた VDA（リストにはもうありません）は、現在のリスト（A、C、D、E）にある Controller の中から選択して再登録します。

マルチゾーン展開では、サテライトゾーンの自動更新は、まずすべてのローカル Controller を自動的にキャッシュします。プライマリゾーンのすべての Controller は、バックアップグループにキャッシュされます。サテライトゾーンにローカル Controller が利用できない場合、プライマリゾーンの Controller で登録が試行されます。

次の例に示すように、キャッシュファイルにはホスト名とセキュリティID (`ListofSIDs`) のリストが含まれています。VDAはSIDを照会しないため、Active Directoryの負荷が軽減されます。

VDAの登録キャッシュファイルの例(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/vda-registration-cache-file.png)

キャッシュファイルはWMI呼び出しで取得できます。ただし、SYSTEMアカウントのみが読み取り可能な場所に保存されています。

> **重要:**
>
> この情報は情報提供のみを目的としています。このファイルを変更しないでください。このファイルまたはフォルダーへの変更は、サポートされていない構成になります。

```
Get-WmiObject -Namespace “Root\Citrix\DesktopInformation” -Class “Citrix_VirtualDesktopInfo” -Property “PersistentDataLocation”
```

セキュリティ上の理由から (Active Directoryの負荷軽減とは別に) `ListofSIDs` を手動で構成する必要がある場合、自動更新機能は使用できません。詳細については、ListOfSIDs を参照してください。

自動更新の優先順位の例外

自動更新は通常、すべてのVDA登録方法の中で最も高い優先順位を持ち、他の方法の設定を上書きしますが、例外があります。キャッシュ内の `NonAutoListOfDDCs` 要素は、初期VDA構成方法を指定します。自動更新はこの情報を監視します。初期登録方法が変更された場合、登録プロセスは自動更新をスキップし、次に高い優先順位で構成された方法を使用します。このプロセスは、VDAを別のサイトに移動する場合 (たとえば、ディザスターリカバリー中) に役立ちます。

構成に関する考慮事項

一般的なVDA登録構成を表示します。

<iframe src="https://www.youtube.com/embed/vrngwl2rc3" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
VDA登録手順を表示します。

<iframe src="https://www.youtube.com/embed/9qpt0p609f" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
VDA登録に影響を与える可能性のある項目を構成する際は、次の点を考慮してください。

ControllerまたはCloud Connectorのアドレス

ControllerまたはCloud Connectorを指定するためにどの方法を使用するかにかかわらず、CitrixはFQDNアドレスを使用することを推奨します。IPアドレスは信頼できる構成とは見なされません。

DNSレコードよりもIPを侵害する方が簡単だからです。`ListofSIDs`を手動で入力する場合、`ListofDDCs`でIPを使用できます。ただし、FQDNが引き続き推奨されます。

負荷分散

前述のとおり、VDAは `ListofDDCs` 内のすべてのControllerまたはCloud Connectorに接続を自動的に分散します。フェールオーバーと負荷分散機能は、Citrix Brokering Protocol (CBP) に組み込まれています。構成で複数のControllerまたはCloud Connectorを指定した場合、必要に応じて登録はそれらの間で自動的にフェールオーバーします。自動更新により、すべてのVDAで自動フェールオーバーが自動的に発生します。

セキュリティ上の理由から、Citrix ADCなどのネットワークロードバランサーを使用することはできません。VDA登録はKerberos相互認証を使用します。この認証では、クライアント (VDA) がサービス (Controller) に対して自身のIDを証明する必要があります。ただし、ControllerまたはCloud ConnectorもVDAに対して自身のIDを証明する必要があります。これは、VDAとControllerまたはCloud Connectorが同時にサーバーとクライアントとして機能することを意味します。この記事の冒頭で述べたように、VDAからController/Cloud Connectorへ、およびController/Cloud ConnectorからVDAへの2つの通信チャネルがあります。

このプロセスにおけるコンポーネントは、サービスプリンシパル名 (SPN) と呼ばれ、Active Directoryコンピューターオブジェクトのプロパティとして保存されます。VDAがControllerまたはCloud Connectorに接続するときは、通信相手を指定する必要があります。このアドレスがSPNです。負荷分散されたIPを使用する場合、相互Kerberos認証は、そのIPが予期されたControllerまたはCloud Connectorに属していないことを正しく認識します。

詳細については、以下を参照してください。

- Kerberosの概要
- Kerberosを使用した相互認証

自動更新によるCNAMEの置き換え

自動更新機能は、XenAppおよびXenDesktop 7.xより前のバージョンにおけるCNAME (DNSエイリアス) 機能を置き換えます。CNAME機能は、XenAppおよびXenDesktop 7以降では無効になっています。CNAMEの代わりに自動更新を使用してください。(CNAMEを使用する必要がある場合は、CTX137960を参照してください。DNSエイリアスを常に機能させるには、自動更新とCNAMEを同時に使用しないでください。)

Controller/Cloud Connectorグループ

特定のシナリオでは、ControllerまたはCloud Connectorをグループで処理し、一方のグループを優先し、すべてのController/Cloud Connectorが失敗した場合に他方のグループをフェールオーバーに使用したい場合があります。ControllerまたはCloud Connectorはリストからランダムに選択されるため、グループ化することで優先的な使用を強制するのに役立ちます。

これらのグループは、単一のサイト内での使用を目的としています（複数のサイトではありません）。

Controller/Cloud Connectorのグループを指定するには、かっこを使用します。たとえば、4つのController（プライマリ2つとバックアップ2つ）がある場合、グループ化は次のようになります。

```
(XDC-001.cdz.lan XDC-002.cdz.lan) (XDC-003.cdz.lan XDC-004.cdz.lan)
```

この例では、最初のグループのController（001と002）が最初に処理されます。両方が失敗した場合、2番目のグループのController（003と004）が処理されます。

XenDesktop 7.0以降の場合、**登録グループ**機能を使用するには追加の手順が必要です。Citrix Studioから**Controllerの自動更新を有効にする**ポリシーを**禁止**する必要があります。

ListOfSIDs

VDAが登録のために連絡できるControllerのリストは`ListofDDCs`です。VDAはどのControllerを信頼すべきかも知っている必要があります。VDAは`ListofDDCs`内のControllerを自動的に信頼しません。`ListofSIDs` (セキュリティID) は信頼されたControllerを識別します。VDAは信頼されたControllerにのみ登録を試みます。

ほとんどの環境では、`ListofSIDs`は`ListofDDCs`から自動的に生成されます。CDFトレースを使用して`ListofSIDs`を読み取ることができます。

一般的に、`ListofSIDs`を手動で変更する必要はありません。いくつかの例外があります。最初の2つの例外は、新しいテクノロジーが利用可能になったため、もはや有効ではありません。

- **Controller の役割の分離:** XenApp および XenDesktop 7.7 でゾーンが導入される前は、Controller の一部のみが登録に使用される場合、`ListofSIDs` は手動で構成されていました。たとえば、XDC-001 と XDC-002 を XML ブローカーとして使用し、XDC-003 と XDC-004 を VDA 登録に使用する場合、すべての Controller を `ListofSIDs` に、XDC-003 と XDC-004 を `ListofDDCs` に指定していました。これは一般的または推奨される構成ではありません。新しい環境では使用しないでください。代わりにゾーンを使用してください。
- **Active Directory の負荷軽減:** XenApp および XenDesktop 7.6 で自動更新機能が導入される前は、ドメインコントローラーの負荷を軽減するために `ListofSIDs` が使用されていました。

`ListofSIDs` を事前に入力することで、DNS 名から SID への解決をスキップできます。ただし、この永続キャッシュには SID が含まれているため、自動更新機能によりこの作業は不要になります。Citrix は自動更新機能を有効にしておくことを推奨します。

- **セキュリティ:** 一部の高度に保護された環境では、侵害されたDNSサーバーからの潜在的なセキュリティ脅威を回避するために、信頼されたControllerのSIDが手動で構成されていました。ただし、これを行う場合は、自動更新機能も無効にする必要があります。そうしないと、永続キャッシュからの構成が使用されます。

したがって、特別な理由がない限り、`ListofSIDs` を変更しないでください。

`ListofSIDs` を変更する必要がある場合は、`HKLM\Software\Citrix\VirtualDesktopAgent` の下に `ListOfSIDs (REG_SZ)` という名前のレジストリキーを作成します。値は信頼された SID のリストで、複数ある場合はスペースで区切ります。

次の例では、1 つの Controller が VDA 登録 (`ListofDDCs`) に使用されていますが、2 つの Controller がブローカー処理 (List OfSIDs) に使用されています。

登録とブローカー処理に使用される異なる Controller の例(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/vda-registration-listofsids.png)

VDA 登録中の Controller 検索

VDA が登録を試行すると、Broker Agent はまずローカルドメインで DNS ルックアップを実行し、指定された Controller に到達できることを確認します。

最初のルックアップで Controller が見つからない場合、Broker Agent は AD でフォールバックのトップダウンクエリを開始できます。このクエリはすべてのドメインを検索し、頻繁に繰り返されます。Controller アドレスが無効な場合 (たとえば、管理者が VDA のインストール時に誤った FQDN を入力した場合)、そのクエリのアクティビティがドメインコントローラーで分散型サービス拒否 (DDoS) 状態を引き起こす可能性があります。

次のレジストリキーは、Broker Agent が最初の検索中に Controller を見つけられない場合に、フォールバックのトップダウンクエリを使用するかどうかを制御します。

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent`

- 名前: `DisableDdcWildcardNameLookup`
- 種類: `DWORD`
- 値: `0` (デフォルト) または任意のゼロ以外の値

`0` に設定すると、フォールバック検索が有効になります。Controller の最初の検索が失敗した場合、フォールバックのトップダウン検索が開始されます。これはデフォルトの動作です。ただし、ゼロ以外の値に設定すると、フォールバック検索は無効になります。Controller の最初の検索が失敗した場合、Broker Agent は検索を停止します。

VDA登録の問題のトラブルシューティング

前述のとおり、仲介されたセッションを起動する際に考慮されるには、VDAがDelivery ControllerまたはCloud Connectorに登録されている必要があります。未登録のVDAは、利用可能なリソースの利用率低下につながる可能性があります。VDAが登録されない理由はさまざまあり、その多くは管理者がトラブルシューティングできます。Studioは、カタログ作成ウィザードと、デリバリーグループ作成後にトラブルシューティング情報を提供します。

- **マシンカタログ作成中の問題の特定:** カタログ作成ウィザードで、既存のマシンを追加した後、コンピューターアカウント名のリストは、各マシンがカタログに追加するのに適しているかどうかを示します。各マシンの横にあるアイコンにカーソルを合わせると、そのマシンに関する情報メッセージが表示されます。

  メッセージで問題のあるマシンが特定された場合、そのマシンを削除する（**削除**ボタンを使用）か、マシンを追加することができます。たとえば、マシンに関する情報が取得されなかった（おそらく一度も登録されなかったため）ことを示すメッセージが表示された場合でも、そのマシンを追加することを選択できます。

  カタログの機能レベルは、カタログ内のマシンで利用できる製品機能を制御します。新しい製品バージョンで導入された機能を使用するには、新しいVDAが必要になる場合があります。機能レベルを設定すると、そのバージョンで導入されたすべての機能（および機能レベルが変更されない場合はそれ以降のバージョン）がカタログ内のマシンで利用可能になります。ただし、以前のVDAバージョンを持つカタログ内のマシンは登録できません。
- **デリバリーグループ作成後の問題の特定:** デリバリーグループを作成すると、Studioはそのグループに関連付けられているマシンに関する詳細を表示します。

  デリバリーグループの詳細ペインには、登録されるべきだが登録されていないマシンの数が表示されます。つまり、電源が入っていてメンテナンスモードではないが、現在Controllerに登録されていないマシンが1台以上存在する可能性があります。「登録されていないが、登録されるべき」マシンを表示する際は、詳細ペインの**トラブルシューティング**タブで考えられる原因と推奨される是正措置を確認してください。

VDA登録のトラブルシューティングに関する詳細情報

- 機能レベルの詳細については、「VDAのバージョンと機能レベル」を参照してください。

- VDA登録のトラブルシューティングについて詳しくは、「CTX136668」を参照してください。
- VDA登録とセッション起動のトラブルシューティングには、Citrix Scoutのヘルスチェックも使用できます。詳細については、「ヘルスチェックについて」を参照してください。

セキュリティキーの管理

> **注:**
>
> この機能は、StoreFront™ 1912 LTSR CU2以降と組み合わせて使用する必要があります。

> この機能を使用すると、承認されたStoreFrontおよびCitrix Gatewayマシンのみがcitrix Delivery Controllerと通信できるようになります。この機能を有効にすると、キーを含まないすべての要求はブロックされます。この機能を使用して、内部ネットワークから発生する攻撃から保護するための追加のセキュリティ層を追加します。

この機能を使用するための一般的なワークフローは次のとおりです。

1. Studioで機能設定を表示できるようにします。
2. サイトの設定を構成します (Studioコンソールまたは PowerShellを使用)。
3. StoreFrontで設定を構成します (PowerShellを使用)。
4. Citrix ADCで設定を構成します (PowerShellを使用)。

Studioで機能設定を表示できるようにする

デフォルトでは、セキュリティキーの設定はStudioに表示されません。Studioでこれらを表示できるようにするには、次のようにPowerShell SDKを使用します。

この機能を有効にするには、次の手順を実行します。

1. Citrix Virtual Apps and Desktops™ リモート パワーシェル SDK を実行します。
2. コマンドウィンドウで、次のコマンドを実行します。
   - `Add-PSSnapIn Citrix*`。このコマンドはCitrixスナップインを追加します。
   - `Set-ConfigSiteMetadata -Name "Citrix_DesktopStudio_SecurityKeyManagementEnabled" -Value "True"`

Remote PowerShell SDKの詳細については、「SDKとAPI」を参照してください。

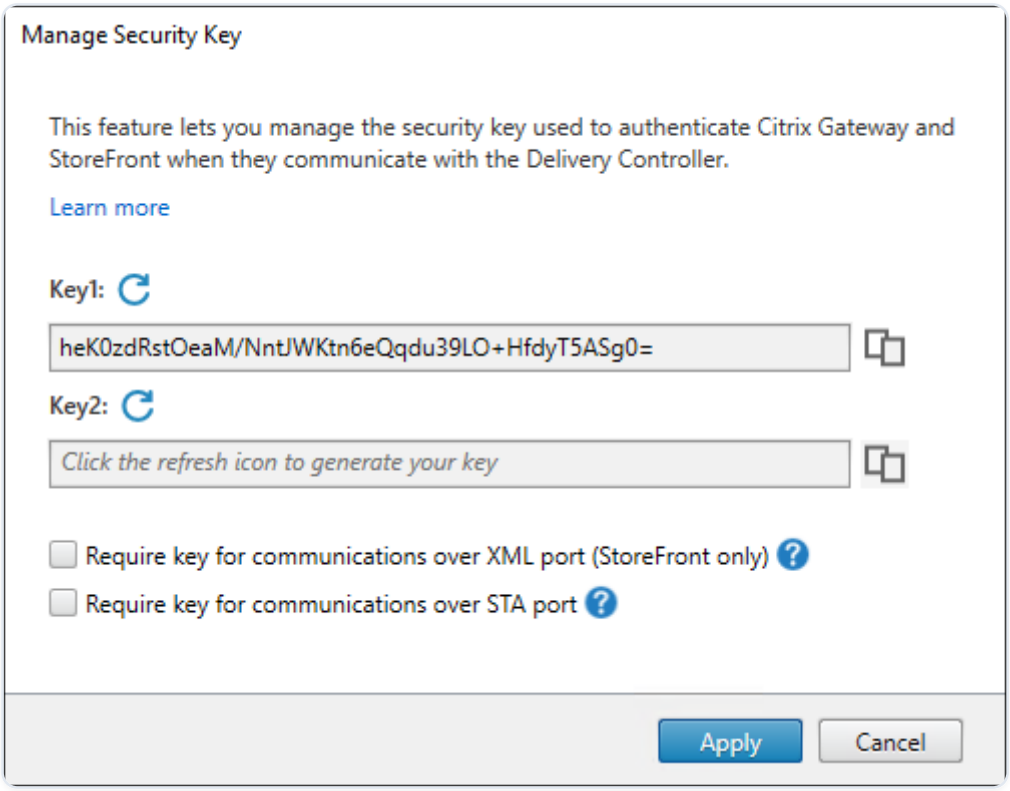
サイトの設定を構成する

StudioコンソールまたはPowerShellを使用して、Studioで設定を構成できます。

Studioコンソールを使用する

「Studioで機能設定を表示できるようにした後、**Studio > 構成 > セキュリティキーの管理** に移動します。**セキュリティキーの管理** オプションが表示されない場合は、**更新** をクリックする必要がある場合があります。

セキュリティキーの管理 をクリックすると、**セキュリティキーの管理** ウィンドウが表示されます。



重要:

- 使用できるキーは2つあります。XMLポートおよびSTAポートを介した通信には、同じキーまたは異なるキーを使用できます。一度に1つのキーのみを使用することをお勧めします。未使用のキーは、キーローテーションにのみ使用されます。
- 使用中のキーを更新するために更新アイコンをクリックしないでください。クリックすると、サービスが中断されます。

更新アイコンをクリックして、新しいキーを生成します。

XMLポートを介した通信にキーを要求する（StoreFrontのみ）。選択した場合、XMLポートを介した通信を認証するためにキーが必要になります。StoreFrontはこのポートを介してCitrix Cloudと通信します。XMLポートの変更については、Knowledge Centerの記事CTX127945を参照してください。

STAポートを介した通信にキーを要求する。選択した場合、STAポートを介した通信を認証するためにキーが必要になります。Citrix GatewayとStoreFrontはこのポートを介してCitrix Cloudと通信します。STAポートの変更については、Knowledge Centerの記事CTX101988を参照してください。

変更を適用した後、**閉じる** をクリックして **セキュリティキーの管理** ウィンドウを終了します。

PowerShell を使用する

以下は、Studio操作に相当するPowerShellの手順です。

1. Citrix Virtual Apps and Desktops Remote PowerShell SDK を実行します。
2. コマンドウィンドウで、次のコマンドを実行します。
   - `Add-PSSnapIn Citrix*`
3. キーを生成し、Key1を設定するには、次のコマンドを実行します。
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey1 <the key you generated>`
4. 以下のコマンドを実行してキーを生成し、Key2 をセットアップします。
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey2 <the key you generated>`
5. 通信の認証でキーの使用を有効にするには、以下のコマンドのいずれか、または両方を実行します。
   - XMLポート経由の通信を認証するには:
     - `Set-BrokerSite -RequireXmlServiceKeyForNFuse $true`
   - STAポート経由の通信を認証するには:
     - `Set-BrokerSite -RequireXmlServiceKeyForSta $true`

ガイダンスと構文については、PowerShellコマンドのヘルプを参照してください。

StoreFront で設定を構成する

Studioでの構成が完了したら、PowerShellを使用してStoreFrontで関連設定を構成する必要があります。

StoreFront サーバーで、以下の PowerShell コマンドを実行します。

XMLポートを介した通信のキーを構成するには、コマンド を使用します。例:

```
$store = Get-STFStoreService -VirtualPath [Path to store]

$farm = Get-STFStoreFarm -StoreService $store -FarmName [Resource feed
name]

Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true
-XMLValidationSecret [secret]
```

次のパラメータに適切な値を入力します。

- `Path to store`
- `Resource feed name`
- `secret`

STAポート経由の通信用にキーを構成するには、`New-STFSecureTicketAuthority`および`Set-STFRoamingGateway`コマンドを使用します。例:

```
$gateway = Get-STFRoamingGateway -Name [Gateway name]

$sta1 = New-STFSecureTicketAuthority -StaUrl [STA1 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

$sta2 = New-STFSecureTicketAuthority -StaUrl [STA2 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

Set-STFRoamingGateway -Gateway $gateway -SecureTicketAuthorityObjs
$sta1,$sta2
```

次のパラメータに適切な値を入力します。

- `Gateway name`
- `STA URL`

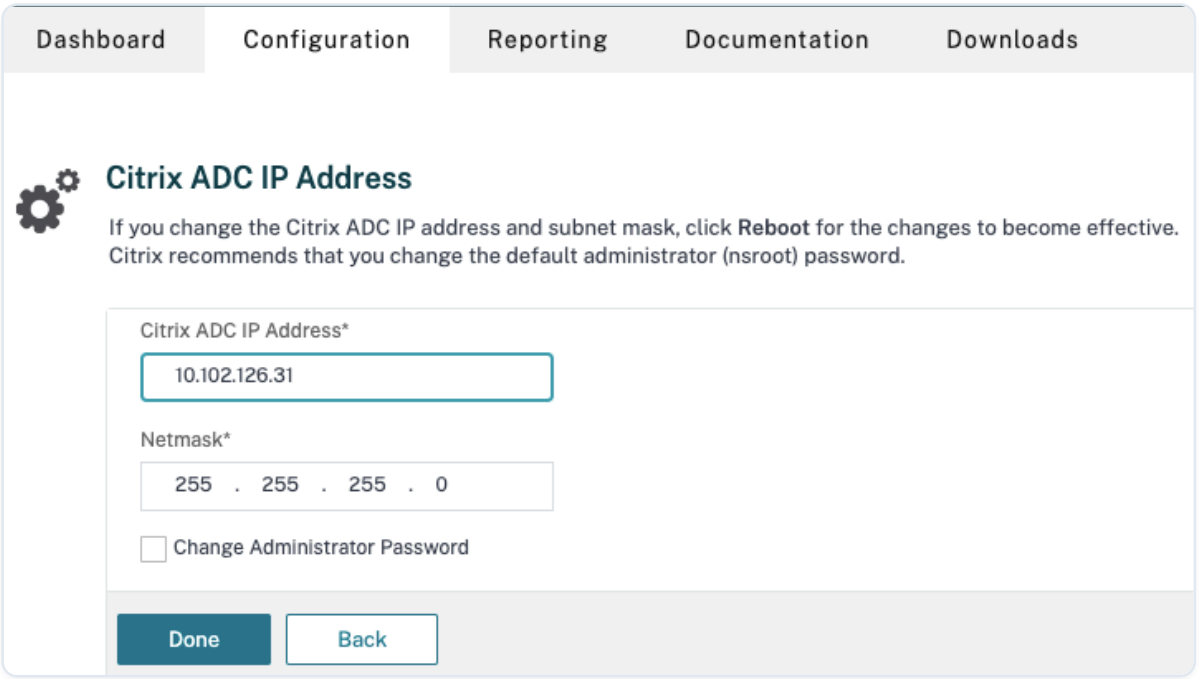
- `Secret`

ガイダンスと構文については、PowerShellコマンドのヘルプを参照してください。

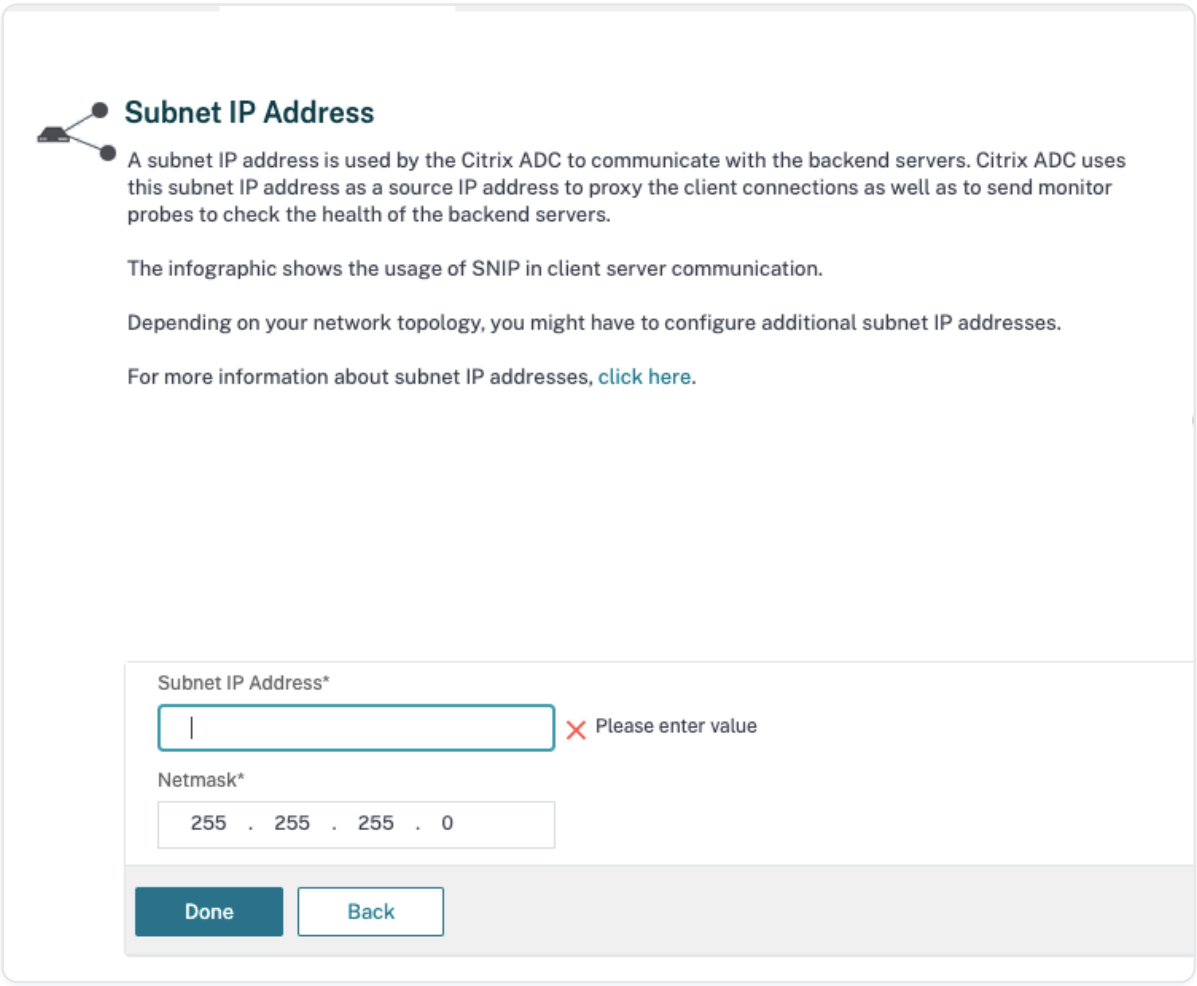
Citrix ADCでの設定

> **注:**
>
> Citrix ADCをゲートウェイとして使用しない限り、Citrix ADCでこの機能を構成する必要はありません。Citrix ADCを使用する場合は、以下の手順に従ってください。

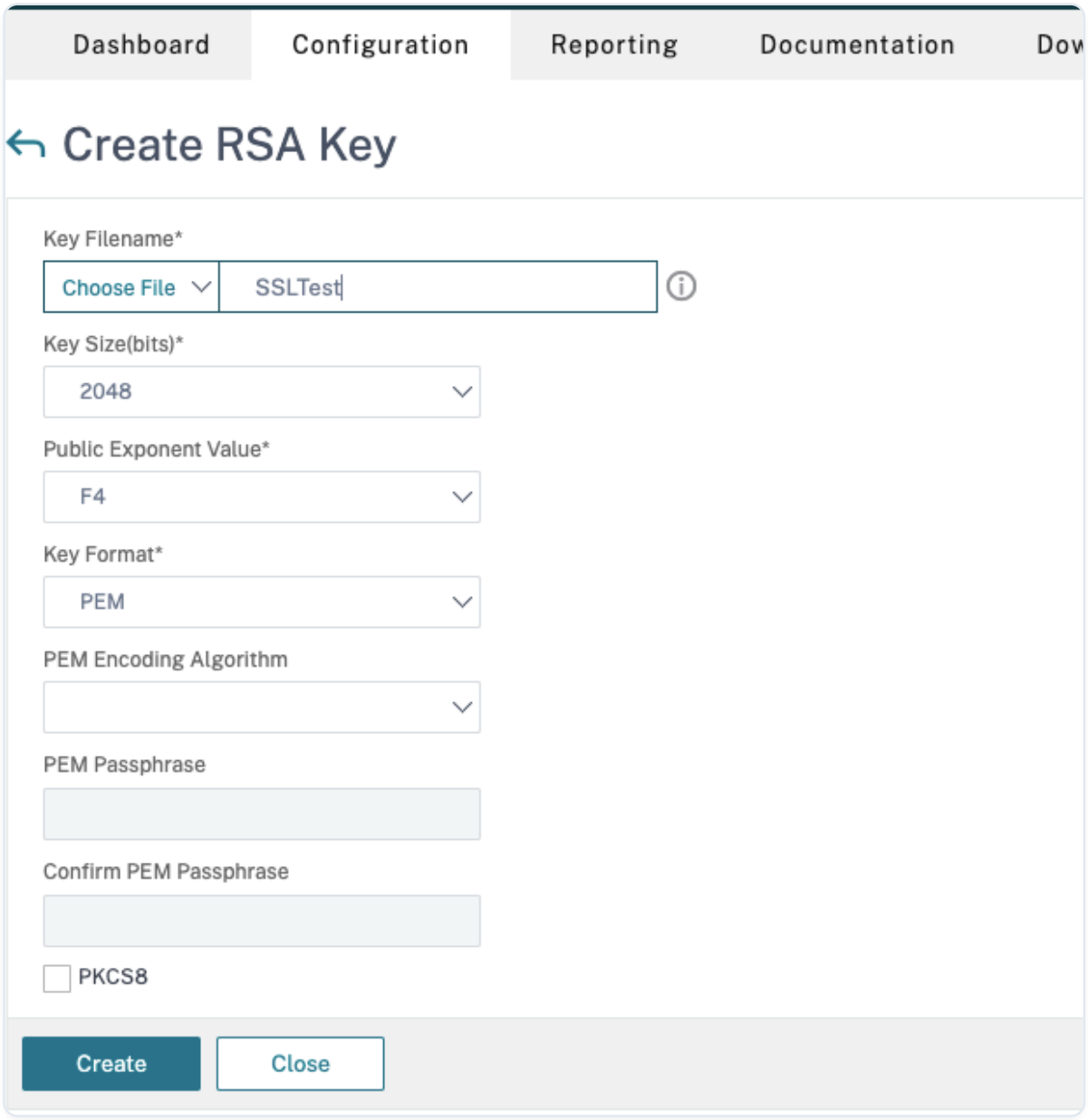
1. 次の前提条件となる構成がすでに設定されていることを確認してください。
   - 次のCitrix ADC関連のIPアドレスが構成されています。
     - Citrix ADCコンソールにアクセスするための Citrix ADC管理IP (NSIP) アドレス。詳細については、「NSIPアドレスの構成」を参照してください。



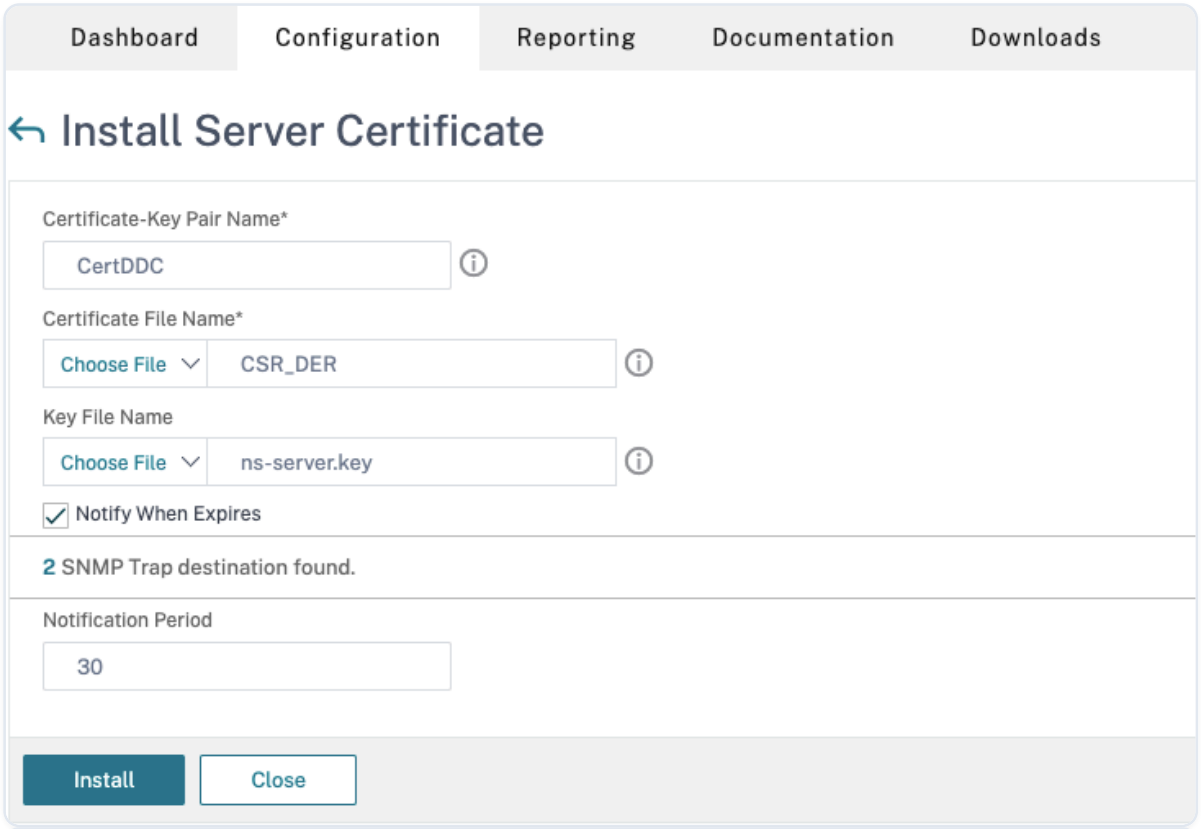
     - Citrix ADCアプライアンスとバックエンドサーバー間の通信を有効にするためのサブネットIP（SNIP）アドレス。詳細については、「サブネットIPアドレスの構成」を参照してください。
     - セッション起動のためにADCアプライアンスにログインするためのCitrix Gateway仮想IPアドレスとロードバランサー仮想IPアドレス。詳細については、「仮想サーバーの作成」を参照してください。

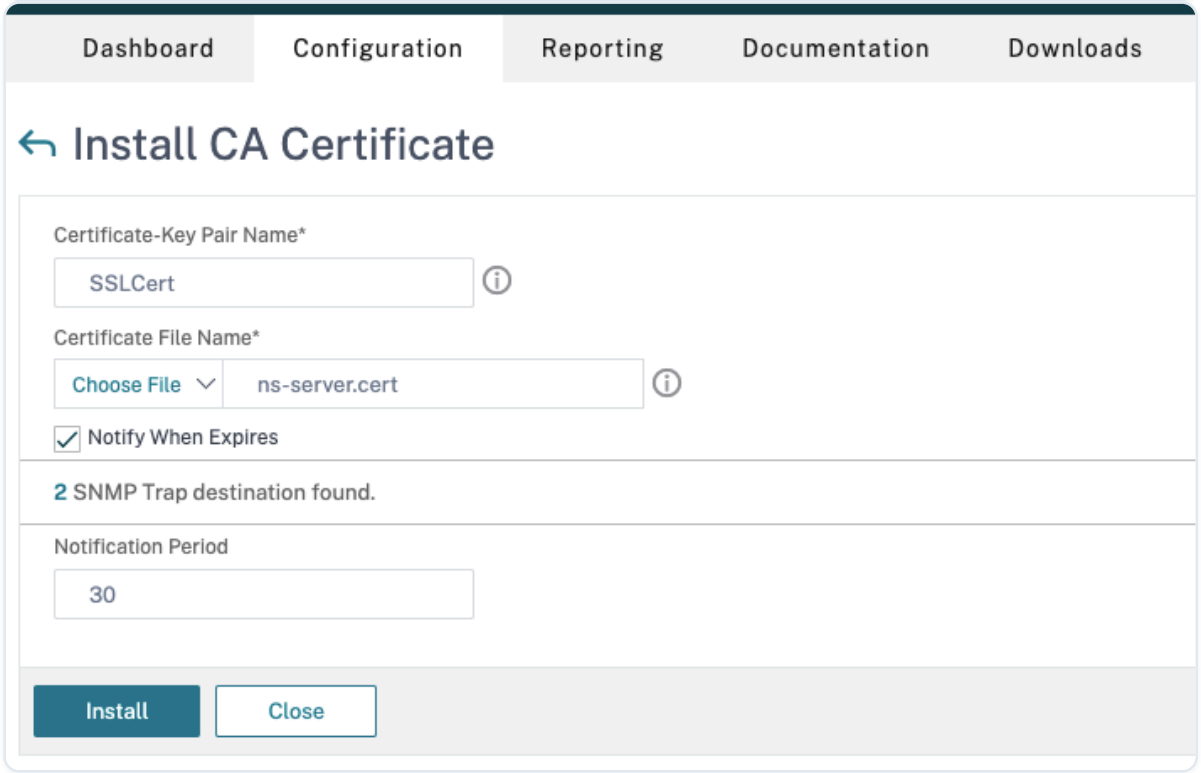


- Citrix ADCアプライアンスで必要なモードと機能が有効になっています。
  - モードを有効にするには、Citrix ADC GUIで **System > Settings > Configure Mode** に移動します。
  - 機能を有効にするには、Citrix ADC GUIで **System > Settings > Configure Basic Features** に移動します。
- 証明書関連の構成が完了しています。
  - 証明書署名要求（CSR）が作成されます。詳細については、「証明書の作成」を参照してください。

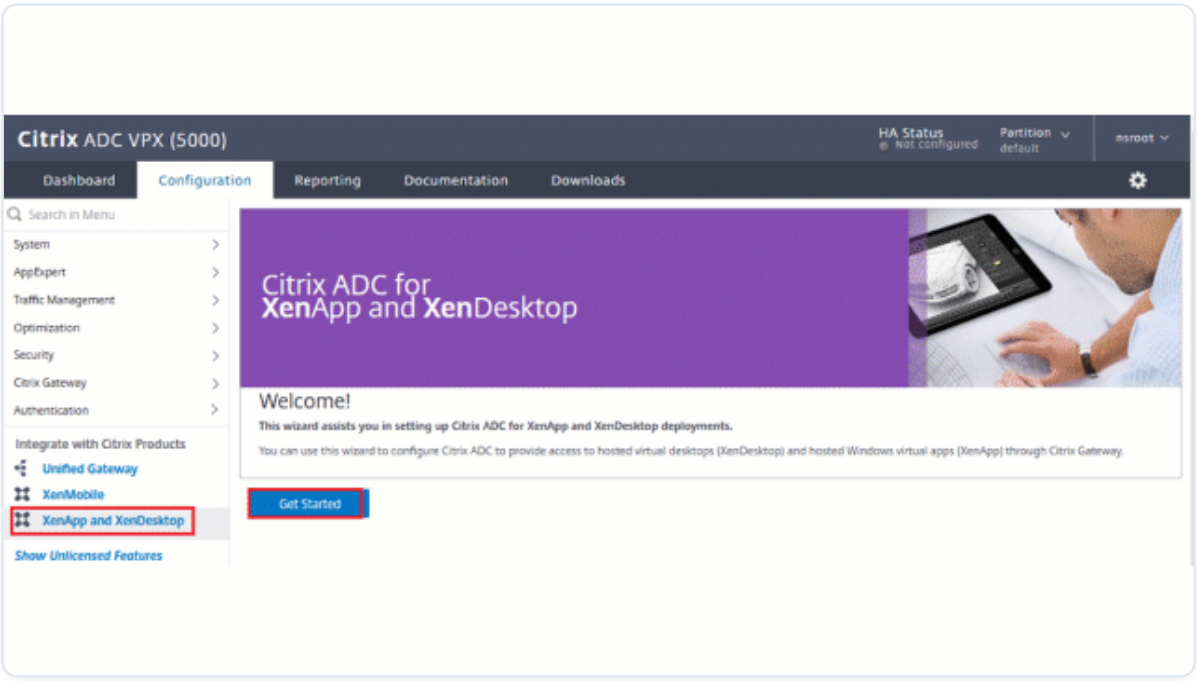


- サーバー証明書、CA証明書、およびルート証明書がインストールされます。詳細については、「インストール、リンク、および更新」を参照してください。





- Citrix Virtual Desktops用にCitrix Gatewayが作成されています。**STA接続のテスト** ボタンをクリックして接続をテストし、仮想サーバーがオンラインであることを確認します。詳細については、「Citrix Virtual Apps and Desktops向けCitrix ADCのセットアップ」を参照してください。



2. リライトアクションを追加します。詳細については、「リライトアクションの構成」を参照してください。

   a. 「**AppExpert > Rewrite > Actions**」に移動します。

   b. **追加** をクリックして、書き換えアクションを追加します。アクションの名前を「set Type to INSERT_HTTP_HEADER」にすることができます。

   書き換えアクションの追加(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/adc-appexpert-rewrite-action.png)

   a. **タイプ**で、**INSERT_HTTP_HEADER**を選択します。

   b. **ヘッダー名**に「X-Citrix-XmlServiceKey」と入力します。

   c. **式**に、引用符付きで`<XmlServiceKey1 value>`を追加します。XmlServiceKey1 の値は、Desktop Delivery Controller™ の構成からコピーできます。

   XMLサービスキーの値(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/xml-service-key-values.png)

3. 書き換えポリシーを追加します。詳細については、「書き換えポリシーの構成」を参照してください。

   a. 「**AppExpert > Rewrite > Policies**」に移動します。

   b. **追加** をクリックして、ポリシーを追加します。

   書き換えポリシーの追加(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/adc-appexpert-rewrite-policy.png)

a. **アクション**で、前の手順で作成したアクションを選択します。

b. **式**に「HTTP.REQ.IS_VALID」を追加します。

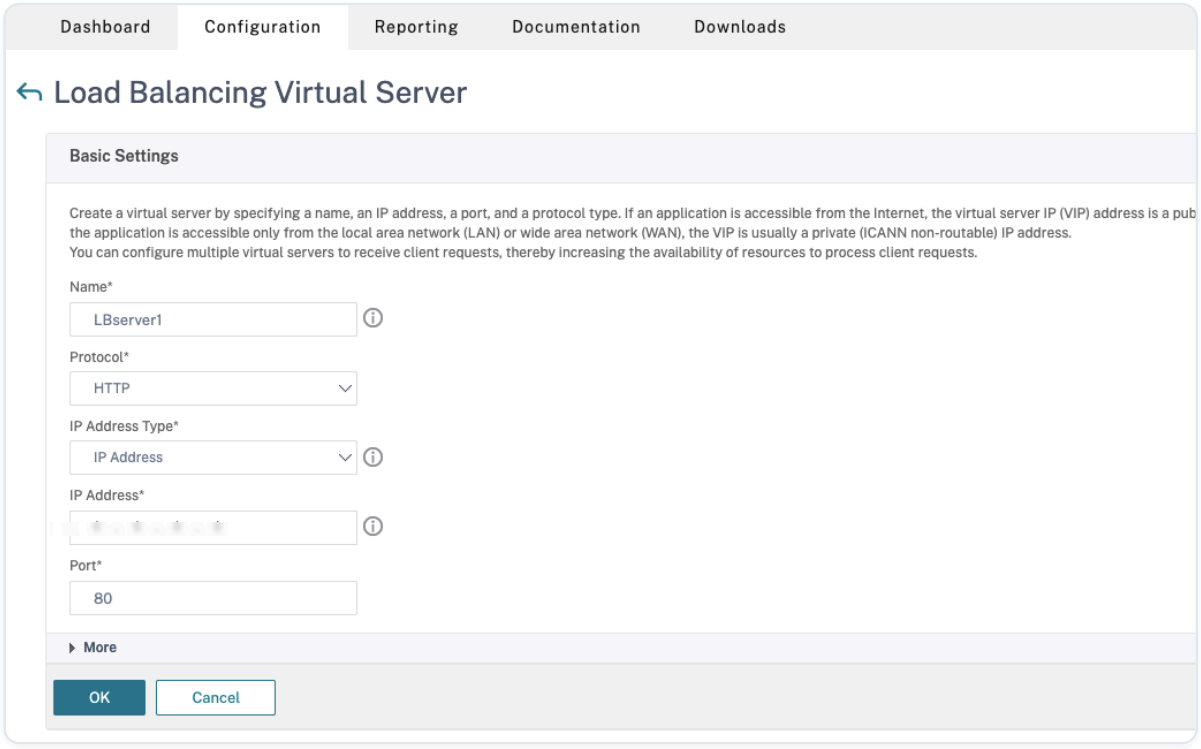
c. **OK**をクリックします。

4. 負荷分散を設定します。STAサーバーごとに1つの負荷分散仮想サーバーを構成する必要があります。構成しない場合、セッションの起動に失敗します。

   詳細については、基本的な負荷分散のセットアップを参照してください。

   a. 負荷分散仮想サーバーを作成します。

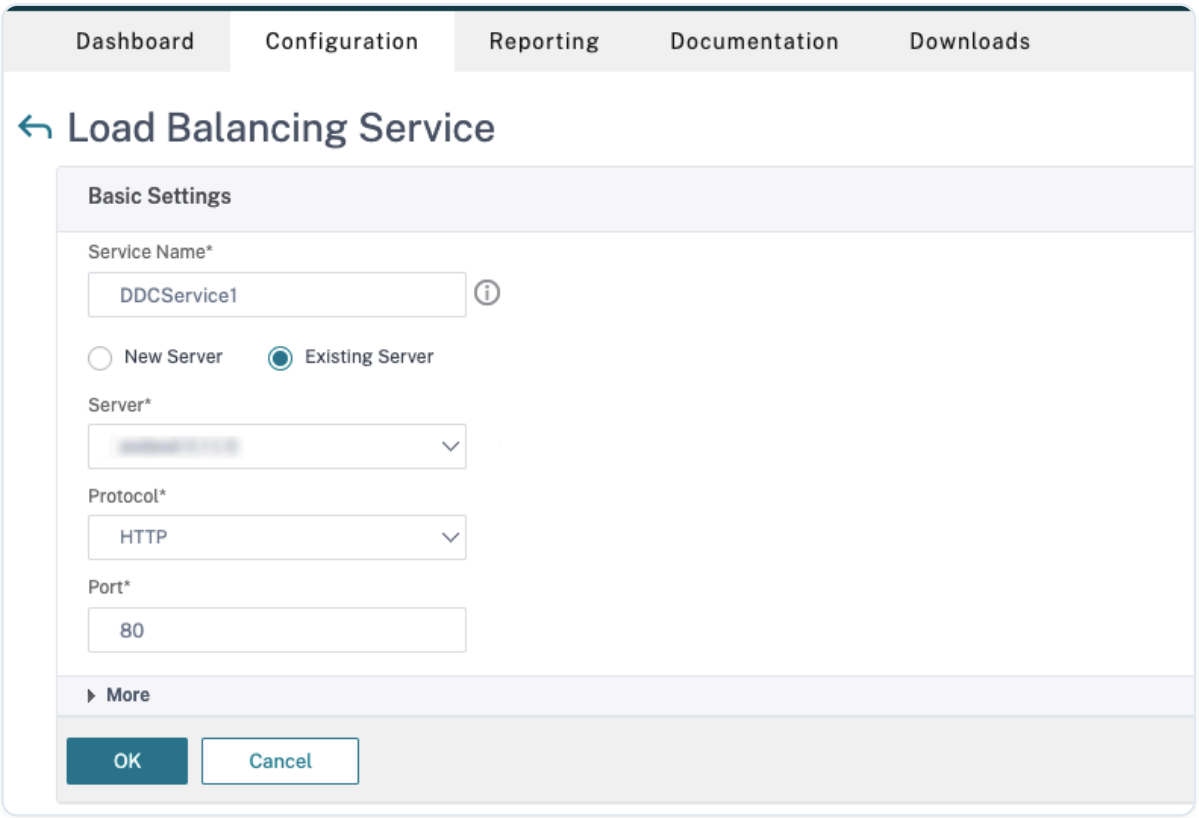
      - **トラフィック管理 > ロードバランシング > サーバー**に移動します。
      - **仮想サーバー** ページで、**追加** をクリックします。



      - **Protocol**で、**HTTP**を選択します。
      - 負荷分散仮想IPアドレスを追加し、**Port**で**80**を選択します。
      - **OK**をクリックします。

   b. 負荷分散サービスを作成します。

      - **トラフィック管理 > ロードバランシング > サービス**に移動します。



- **Existing Server**で、前のステップで作成した仮想サーバーを選択します。
- **Protocol**で**HTTP**を選択し、**Port**で**80**を選択します。
- **OK**をクリックし、その後**Done**をクリックします。

c. サービスを仮想サーバーにバインドします。

- 以前に作成した仮想サーバーを選択し、**編集**をクリックします。
- **サービスとサービスグループ**で、**ロードバランシング仮想サーバーサービスバインディングなし**をクリックします。

仮想サーバーにサービスをバインド(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/adc-bind-service-to-lbvserver.png)

- **サービスバインディング** で、以前に作成したサービスを選択します。
- **バインド**をクリックします。

d. 以前に作成した書き換えポリシーを仮想サーバーにバインドします。

- 以前に作成した仮想サーバーを選択し、**編集**をクリックします。
- **詳細設定**で、**ポリシー**をクリックし、次に**ポリシー**セクションで**+**をクリックします。

書き換えポリシーをバインド(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/adc-bind-rewrite-policy.png)

- **ポリシーの選択**で**書き換え**を選択し、**タイプの選択**で**要求**を選択します。
- **続行**をクリックします。
- **ポリシーの選択**で、以前に作成した書き換えポリシーを選択します。
- **バインド**をクリックします。
- **完了**をクリックします。

e. 必要に応じて、仮想サーバーの永続性を設定します。

- 以前に作成した仮想サーバーを選択し、**編集**をクリックします。
- **詳細設定**で、**永続性**をクリックします。

永続性の設定(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/adc-lb-vserver-persistence.png)

- 永続性の種類として**その他**を選択します。
- 仮想サーバーによって選択されたサービスのIPアドレス（宛先IPアドレス）に基づいて永続性セッションを作成するには、**DESTIP**を選択します。
- **IPv4ネットマスク**で、DDCと同じネットワークマスクを追加します。
- **OK**をクリックします。

f. 他の仮想サーバーについても、これらの手順を繰り返します。

Citrix ADCアプライアンスがCitrix Virtual Desktops™で既に構成されている場合の構成変更

Citrix ADCアプライアンスをCitrix Virtual Desktopsで既に構成している場合、Secure XML機能を使用するには、以下の構成変更を行う必要があります。

- セッション起動前に、ゲートウェイの**セキュリティチケット機関URL**を、負荷分散仮想サーバーのFQDNを使用するように変更します。
- `TrustRequestsSentToTheXmlServicePort` パラメーターがFalseに設定されていることを確認してください。デフォルトでは、`TrustRequestsSentToTheXmlServicePort` パラメーターはFalseに設定されています。ただし、顧客がCitrix Virtual Desktops用にCitrix ADCを既に構成している場合、`TrustRequestsSentToTheXmlServicePort` はTrueに設定されます。

1. Citrix ADC GUIで、**構成 > Citrix製品との統合**に移動し、**XenApp and XenDesktop®**をクリックします。
2. ゲートウェイインスタンスを選択し、編集アイコンをクリックします。

   既存のゲートウェイ構成を編集(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/edit-gateway-instance.png)
3. StoreFrontペインで、編集アイコンをクリックします。

   StoreFrontの詳細を編集(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/edit-storefront-details.png)
4. **Secure Ticket Authority URL**を追加します。

   - Secure XML機能が有効になっている場合、STA URLはロードバランシングサービスのURLである必要があります。
   - Secure XML機能が無効になっている場合、STA URLはSTAのURL（DDCのアドレス）である必要があり、DDC上のTrustRequestsSentToTheXmlServicePortパラメーターはTrueに設定する必要があります。

   STA URLを追加(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/add-sta-urls.png)

セッション

セッションアクティビティを維持することは、最高のユーザーエクスペリエンスを提供するために不可欠です。信頼性の低いネットワーク、変動の大きいネットワーク遅延、ワイヤレスデバイスの範囲制限による接続の喪失は、ユーザーの不満につながる可能性があります。デバイス間を素早く移動し、ログオンするたびに同じアプリケーションにアクセスすることは、医療従事者などの多くのモバイルワーカーにとって優先事項です。

この記事で説明する機能は、セッションの信頼性を最適化し、不便さ、ダウンタイム、生産性の損失を軽減します。これらの機能を使用することで、モバイルユーザーはデバイス間を迅速かつ簡単にローミングできます。

ユーザーをセッションからログオフさせたり、セッションを切断したり、セッションの事前起動と維持を設定したりすることもできます。「デリバリーグループの管理」を参照してください。

セッションの信頼性

ネットワーク接続が中断された場合でも、セッションの信頼性により、セッションはアクティブな状態を保ち、ユーザーの画面に表示され続けます。ユーザーは、ネットワーク接続が再開されるまで、使用しているアプリケーションを引き続き見ることができます。

この機能は、ワイヤレス接続を使用するモバイルユーザーにとって特に便利です。たとえば、ワイヤレス接続を使用しているユーザーが鉄道トンネルに入り、一時的に接続が失われたとします。通常、セッションは切断され、ユーザーの画面から消え、ユーザーは切断されたセッションに再接続する必要があります。セッションの信頼性を使用すると、セッションはマシン上でアクティブなままになります。接続が失われたことを示すために、ユーザーのディスプレイはフリーズし、カーソルはトンネルの反対側で接続が再開されるまで回転する砂時計に変わります。ユーザーは中断中もディスプレイにアクセスし続け、ネットワーク接続が復元されたときにアプリケーションとの対話を再開できます。セッションの信頼性により、ユーザーは再認証のプロンプトなしで再接続されます。

Citrix Workspace™アプリのユーザーは、Controllerの設定を上書きできません。

セッションの信頼性は、トランスポート層セキュリティ (TLS) とともに使用できます。TLSは、ユーザーデバイスとCitrix Gatewayの間で送信されるデータのみを暗号化します。

次のポリシー設定でセッションの信頼性を有効にして構成します。

- セッションの信頼性接続ポリシー設定は、セッションの信頼性を許可または禁止します。
- セッションの信頼性タイムアウトポリシー設定のデフォルトは180秒、つまり3分です。セッションの信頼性がセッションを開いたままにする時間を延長することはできますが、この機能はユーザーの利便性のために設計されています。そのため、ユーザーに再認証を促すことはありません。セッションを開いたままにする時間を延長すると、ユーザーが注意散漫になり、ユーザーデバイスから離れてしまう可能性が高まります。これらの行動は、セッションを不正なユーザーがアクセスできる状態にする可能性があります。
- 受信セッションの信頼性接続は、セッションの信頼性ポート番号ポリシー設定でポート番号を変更しない限り、ポート2598を使用します。
- ユーザーが再認証なしで中断されたセッションに再接続するのを防ぐには、自動クライアント再接続機能を使用します。自動クライアント再接続認証ポリシー設定を構成して、中断されたセッションに再接続する際にユーザーに再認証を促すことができます。

セッションの信頼性と自動クライアント再接続の両方を使用する場合、これら2つの機能は順次動作します。セッションの信頼性は、セッションの信頼性タイムアウトポリシー設定で指定した時間の経過後、ユーザーセッションを閉じるか、切断します。その後、自動クライアント再接続ポリシー設定が有効になり、切断されたセッションにユーザーを再接続しようとします。

クライアントの自動再接続

自動クライアント再接続機能を使用すると、Citrix WorkspaceアプリはICA®セッションの意図しない切断を検出し、影響を受けるセッションにユーザーを自動的に再接続できます。この機能が

サーバーで有効になっている場合、ユーザーは作業を続行するために手動で再接続する必要はありません。

アプリケーションセッションの場合、Citrix Workspaceアプリは、再接続が成功するか、ユーザーが再接続の試行をキャンセルするまで、セッションへの再接続を試みます。

デスクトップセッションの場合、Citrix Workspaceアプリは、再接続が成功するか、ユーザーが再接続の試行をキャンセルしない限り、指定された期間、セッションへの再接続を試行します。デフォルトでは、この期間は5分です。この期間を変更するには、ユーザーデバイスで以下のレジストリ設定を編集します（`seconds` は、セッションの再接続がそれ以上試行されなくなるまでの秒数です）。

`HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds; DWORD;<seconds>`

以下のポリシー設定でAuto Client Reconnectを有効にして構成します。

- **Auto Client Reconnect:** 接続が中断された後にCitrix Workspaceアプリによる自動再接続を有効または無効にします。
- **Auto Client Reconnect authentication:** 自動再接続後のユーザー認証の要件を有効または無効にします。
- **Auto Client Reconnect logging:** イベントログへの再接続イベントのログ記録を有効または無効にします。ログ記録はデフォルトで無効になっています。有効にすると、サーバーのシステムログに、成功および失敗した自動再接続イベントに関する情報が記録されます。各サーバーは、再接続イベントに関する情報を独自のシステムログに保存します。サイトは、すべてのサーバーの再接続イベントの統合ログを提供しません。

Auto Client Reconnectは、暗号化されたユーザー資格情報に基づく認証メカニズムを組み込んでいます。ユーザーが最初にログオンすると、サーバーはユーザー資格情報を暗号化してメモリに保存します。サーバーはまた、暗号化キーを含むCookieを作成し、Citrix Workspaceアプリに送信します。Citrix Workspaceアプリは、再接続のためにキーをサーバーに送信します。サーバーは資格情報を復号化し、認証のためにWindowsログオンに送信します。Cookieの有効期限が切れると、ユーザーはセッションに再接続するために再認証する必要があります。

Auto Client Reconnect認証設定を有効にすると、Cookieは使用されません。代わりに、Citrix Workspaceアプリが自動的に再接続を試みるときに、資格情報を要求するダイアログボックスがユーザーに表示されます。

ユーザー資格情報とセッションを最大限に保護するために、クライアントとサイト間のすべての通信に暗号化を使用してください。

icaclient.admファイルを使用して、Windows版Citrix WorkspaceアプリでAuto Client Reconnectを無効にします。詳細については、お使いのWindows版Citrix Workspaceアプリのバージョンのドキュメントを参照してください。

接続の設定もAuto Client Reconnectに影響します。

- デフォルトでは、前述のとおり、Auto Client Reconnectはサイトレベルのポリシー設定によって有効になっています。ユーザーの再認証は不要です。ただし、サーバーのICA TCP接続が、通信リンクが切断されたセッションをリセットするように構成されている場合、自動再接続は行われません。Auto Client Reconnectは、接続が切断されたかタイムアウトした場合にサーバーがセッションを切断する場合にのみ機能します。このコンテキストでは、ICA TCP接続とは、TCP/IPネットワーク上のセッションに使用されるサーバーの仮想ポート（実際のネットワーク接続ではなく）を指します。
- デフォルトでは、サーバー上のICA TCP接続は、切断された接続またはタイムアウトした接続を持つセッションを切断するように設定されています。切断されたセッションはシステムメモリにそのまま残り、Citrix Workspaceアプリによる再接続が可能です。
- 接続は、切断された接続またはタイムアウトした接続を持つセッションをリセットまたはログオフするように構成できます。セッションがリセットされると、再接続を試みると新しいセッションが開始されます。使用中のアプリケーションでユーザーを同じ場所に戻すのではなく、アプリケーションが再起動されます。
- サーバーがセッションをリセットするように構成されている場合、Auto Client Reconnectは新しいセッションを作成します。このプロセスでは、ユーザーがサーバーにログオンするために資格情報を入力する必要があります。
- Citrix Workspaceアプリまたはプラグインが誤った認証情報を送信した場合、自動再接続が失敗することがあります。これは、攻撃中に発生したり、サーバーが切断された接続を検出してから時間が経ちすぎたと判断した場合に起こりえます。

ICA キープアライブ

ICA Keep-Alive機能を有効にすると、途切れた接続が切断されるのを防ぎます。有効にすると、サーバーがアクティビティを検出しない場合、この機能によりリモートデスクトップサービスがそのセッションを切断するのを防ぎます。アクティビティがない例としては、クロックの変更、マウスの移動、画面の更新がないことなどが挙げられます。サーバーは数秒ごとにキープアライブパケットを送信して、セッションがアクティブであるかどうかを検出します。セッションがアクティブでなくなった場合、サーバーはそのセッションを切断済みとしてマークします。

> **重要:**

> ICA Keep-Aliveは、セッションの信頼性を使用していない場合にのみ機能します。セッションの信頼性には、途切れた接続が切断されるのを防ぐ独自のメカニズムがあります。ICA Keep-Aliveは、セッションの信頼性を使用しない接続に対してのみ構成してください。

> ICA Keep-Alive設定は、Windowsグループポリシーで構成されているキープアライブ設定を上書きします。

次のポリシー設定を使用して、ICA Keep-Aliveを有効にして構成します。

- **ICAキープアライブタイムアウト:** ICAキープアライブメッセージの送信に使用される間隔（1～3600秒）を指定します。途切れた接続が非常にまれで、ユーザーがセッションに再接続できることが問題にならない環境で、ネットワーク監視ソフトウェアに非アクティブな接続を閉じさせたい場合は、このオプションを構成しないでください。

  デフォルトの間隔は60秒です。ICA Keep-Aliveパケットは60秒ごとにユーザーデバイスに送信されます。ユーザーデバイスが60秒以内に応答しない場合、ICAセッションのステータスは切断済みに変わります。
- **ICAキープアライブ:** ICAキープアライブメッセージの送信を許可または禁止します。

ワークスペースコントロール

ワークスペースコントロールにより、デスクトップとアプリケーションはユーザーに追従し、デバイス間を移動できます。このローミング機能により、ユーザーはログオンするだけで、各デバイスでデスクトップやアプリケーションを再起動することなく、どこからでもすべてのデスクトップや開いているアプリケーションにアクセスできます。たとえば、ワークスペースコントロールは、病院で異なるワークステーション間を素早く移動し、ログオンするたびに同じアプリケーションセットにアクセスする必要がある医療従事者を支援できます。ワークスペースコントロールオプションを許可するように構成すると、これらの医療従事者は1つのクライアントデバイスで複数のアプリケーションから切断し、別のクライアントデバイスで同じアプリケーションを開くために再接続できます。

ワークスペースコントロールは、次のアクティビティに影響します。

- **ログオン:** デフォルトでは、ワークスペースコントロールにより、ユーザーはログオン時に実行中のすべてのデスクトップとアプリケーションに自動的に再接続でき、手動で再開する必要がなくなります。ワークスペースコントロールを通じて、ユーザーは切断されたデスクトップまたはアプリケーション、および別のクライアントデバイスでアクティブなものを開くことができます。デスクトップまたはアプリケーションから切断しても、それはサーバー上で実行されたままになります。一部のデスクトップまたはアプリケーションを1つのクライアントデバ

イスで実行したままにし、別のクライアントデバイスでデスクトップまたはアプリケーションのサブセットに再接続する必要があるローミングユーザーがいる場合、ユーザーが以前に切断したデスクトップまたはアプリケーションのみを開くようにログオン再接続動作を構成できます。

- **再接続:** サーバーにログオンした後、ユーザーは「再接続」をクリックすることで、いつでもすべてのデスクトップまたはアプリケーションに再接続できます。デフォルトでは、「再接続」は切断されたデスクトップまたはアプリケーション、および現在別のクライアントデバイスで実行中のものを開きます。ユーザーが以前に切断したデスクトップまたはアプリケーションのみを開くように「再接続」を構成できます。
- **ログオフ:** StoreFront™を介してデスクトップまたはアプリケーションを開くユーザーの場合、**ログオフ**コマンドを構成して、ユーザーをStoreFrontとすべてのアクティブなセッションからログオフさせるか、StoreFrontからのみログオフさせることができます。
- **切断:** ユーザーは、個別に切断する必要なく、実行中のすべてのデスクトップとアプリケーションから一度に切断できます。

ワークスペースコントロールは、Citrix StoreFront接続を介してデスクトップおよびアプリケーションにアクセスするCitrix Workspaceアプリユーザーのみが利用できます。デフォルトでは、ワークスペースコントロールは仮想デスクトップセッションでは無効になっていますが、ホスト型アプリケーションでは有効になっています。公開されたデスクトップと、それらのデスクトップ内で実行されている公開されたアプリケーションとの間で、セッション共有はデフォルトでは行われません。

ユーザーが新しいクライアントデバイスに移動すると、ユーザーポリシー、クライアントドライブマッピング、およびプリンター構成が適切に変更されます。ポリシーとマッピングは、ユーザーがセッションにログオンしているクライアントデバイスに応じて適用されます。たとえば、医療従事者が救急治療室のデバイスからログオフし、X線検査室のワークステーションにログオンする場合、X線検査室でのセッションに適したポリシー、プリンターマッピング、およびクライアントドライブマッピングがセッション開始時に有効になります。

ユーザーが場所を変更したときに表示されるプリンターをカスタマイズできます。また、ユーザーがローカルプリンターに印刷できるかどうか、ユーザーがリモートで接続したときに消費される帯域幅の量、およびその他の印刷エクスペリエンスの側面を制御することもできます。

ユーザー向けにワークスペースコントロールを有効化および構成する方法については、StoreFrontのドキュメントを参照してください。

セッションローミング

デフォルトでは、セッションはユーザーとともにクライアントデバイス間をローミングします。ユーザーがセッションを起動し、別のデバイスに移動すると、同じセッションが使用され、両方のデバイスでアプリケーションが利用可能になります。アプリケーションは、デバイスや現在のセッションの有無にかかわらず追従します。多くの場合、アプリケーションに割り当てられたプリンターやその他のリソースも追従します。

このデフォルトの動作には多くの利点がありますが、すべての場合に理想的とは限りません。PowerShell SDKを使用してセッションローミングを防止できます。

例1：医療従事者が2つのデバイスを使用しており、デスクトップPCで保険フォームを完成させ、タブレットで患者情報を閲覧しています。

- セッションローミングが有効になっている場合、両方のアプリケーションが両方のデバイスに表示されます（1つのデバイスで起動されたアプリケーションは、使用中のすべてのデバイスで表示されます）。これはセキュリティ要件を満たさない可能性があります。
- セッションローミングが無効になっている場合、患者記録はデスクトップPCに表示されず、保険フォームはタブレットに表示されません。

例2：生産管理者が自分のオフィスにあるPCでアプリケーションを起動します。デバイス名と場所によって、そのセッションで利用可能なプリンターやその他のリソースが決まります。その日の後半、彼は会議のために隣の建物のオフィスに行き、プリンターを使用する必要があります。

- セッションローミングが有効になっている場合、生産管理者は会議室近くのプリンターにアクセスできない可能性があります。なぜなら、彼がオフィスで以前に起動したアプリケーションによって、その場所近くのプリンターやその他のリソースが割り当てられたためです。
- セッションローミングが無効になっている場合、彼が別のマシンに（同じ資格情報を使用して）ログオンすると、新しいセッションが開始され、近くのプリンターやリソースが利用可能になります。

セッションローミングの構成

セッションローミングを構成するには、「SessionReconnection」プロパティを持つ以下のエンタイトルメントポリシー規則コマンドレットを使用します。オプションで、「LeasingBehavior」プロパティも指定できます。

デスクトップセッションの場合：

```
Set-BrokerEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection <value> -LeasingBehavior Allowed|Disallowed
```

アプリケーションセッションの場合：

```
Set-BrokerAppEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection <value> -LeasingBehavior Allowed|Disallowed
```

`value` には、次のいずれかを指定できます。

- **Always:** セッションは、クライアントデバイスやセッションが接続されているか切断されているかに関係なく、常にローミングします。これがデフォルト値です。
- **DisconnectedOnly:** 既に切断されているセッションにのみ再接続します。それ以外の場合は、新しいセッションを起動します。（セッションは、最初に切断するか、Workspace Control を使用して明示的にローミングすることで、クライアントデバイス間をローミングできます。）別のクライアントデバイスからのアクティブな接続済みセッションは使用されません。代わりに、新しいセッションが起動されます。
- **SameEndpointOnly:** ユーザーは、使用するクライアントデバイスごとに一意のセッションを取得します。これにより、ローミングが完全に無効になります。ユーザーは、以前セッションで使用したのと同じデバイスにのみ再接続できます。

「LeasingBehavior」プロパティについては、以下で説明します。

その他の設定による影響：

セッションローミングを無効にすると、デリバリーグループのアプリケーションのプロパティにあるアプリケーション制限 **ユーザーごとにアプリケーションのインスタンスを1つのみ許可する** の影響を受けます。

- セッションローミングを無効にする場合は、「アプリケーションのインスタンスを1つのみ許可する...」アプリケーション制限も無効にします。
- 「アプリケーションのインスタンスを1つのみ許可する...」アプリケーション制限を有効にする場合は、新しいデバイスで新しいセッションを許可する2つの値のいずれも構成しないでください。

ログオン間隔

デスクトップVDAを含む仮想マシンがログオンプロセス完了前に閉じられた場合、そのプロセスにより多くの時間を割り当てることができます。バージョン7.6以降のデフォルトは180秒です（バージョン7.0〜7.5のデフォルトは90秒です）。

マシン（またはマシンカタログで使用されるマスターイメージ）で、次のレジストリキーを設定します。

キー: `HKLM\SOFTWARE\Citrix\PortICA`

- 値: `AutoLogonTimeout`
- 種類: `DWORD`
- 0〜3600の範囲で、10進数の時間を秒単位で指定します。

マスターイメージを変更した場合は、カタログを更新します。

この設定は、デスクトップVDAを持つVMにのみ適用されます。Microsoftは、サーバーVDAを持つマシンでのログオンタイムアウトを制御します。

Studioでの検索の使用

検索機能を使用して、特定の仮想マシン、セッション、マシンカタログ、アプリケーション、またはデリバリーグループに関する情報を表示します。

1. Studioのナビゲーションペインで**検索**を選択します。

   検索ボックスを使用して、マシンカタログまたはデリバリーグループのタブ内を検索することはできません。ナビゲーションペインの検索ノードを使用してください。

   表示に追加の検索条件を表示するには、検索ドロップダウンフィールドの横にあるプラス記号をクリックします。マイナスボタンをクリックして検索条件を削除します。
2. 名前を入力するか、ドロップダウンリストを使用して、検索したい項目の別の検索オプションを選択します。
3. 必要に応じて、**名前を付けて保存**を選択して検索を保存します。検索は**保存された検索**リストに表示されます。

または、**検索の展開**アイコン（二重下向き山括弧）をクリックして、検索プロパティのメニューを表示します。メニューのプロパティから式を構築することで、高度な検索を実行できます。

検索を強化するためのヒント：

- 検索および並べ替えが可能な表示に追加の特性を表示するには、任意の列を右クリックして**列の選択**を選択します。
- マシンに接続されているユーザーデバイスを見つけるには、**クライアント (IP)** と **Is** を使用し、デバイスのIPアドレスを入力します。
- アクティブなセッションを見つけるには、**セッション状態**、**Is**、および **接続済み** を使用します。

- デリバリーグループ内のすべての仮想マシンを一覧表示するには、ナビゲーションペインで**デリバリーグループ**を選択し、グループを選択してから、アクションペインで**仮想マシンの表示**を選択します。

タグ

はじめに

タグは、マシン、アプリケーション、デスクトップ、デリバリーグループ、アプリケーショングループ、ポリシーなどの項目を識別する文字列です。タグを作成して項目に追加すると、特定のタグを持つ項目にのみ適用されるように特定の操作を調整できます。

- Studioでの検索表示を調整します。

  例えば、テスター向けに最適化されたアプリケーションのみを表示するには、「test」という名前のタグを作成し、それらのアプリケーションに追加（適用）します。これで、「test」タグを使用してStudioの検索をフィルタリングできます。
- アプリケーショングループからアプリケーションを公開したり、デリバリーグループから特定のデスクトップを公開したりする際に、選択したデリバリーグループ内のマシンの一部のみを考慮します。これは*タグ制限*と呼ばれます。

  タグ制限を使用すると、既存のマシンを複数の公開タスクに使用できるため、より多くのマシンを展開および管理するコストを節約できます。タグ制限は、デリバリーグループ内のマシンを細分化（またはパーティション分割）するものと考えることができます。その機能は、XenApp 7.xより前のリリースにおけるワーカーグループと似ていますが、同一ではありません。

  タグ制限付きのアプリケーショングループまたはデスクトップを使用すると、デリバリーグループ内のマシンの一部を分離してトラブルシューティングする際に役立ちます。
- デリバリーグループ内のマシンの一部に対して定期的な再起動をスケジュールします。

  マシンにタグ制限を使用すると、新しいPowerShellコマンドレットを使用して、デリバリーグループ内のマシンの一部に対して複数の再起動スケジュールを構成できます。例と詳細については、「デリバリーグループの管理」を参照してください。
- 指定されたタグを持つ（または持たない）デリバリーグループ、デリバリーグループの種類、またはOU内のマシンのサブセットに対して、Citrix®ポリシーの適用（割り当て）を調整します。

  例えば、より高性能なワークステーションにのみCitrixポリシーを適用したい場合は、それらのマシンに「high power」という名前のタグを追加します。その後、ポリシー作成ウィザード

のポリシーの割り当てページで、そのタグと有効にするチェックボックスを選択します。デリバリーグループにタグを追加し、そのグループにCitrixポリシーを適用することもできます。詳細については、「ポリシーの作成」を参照してください。

タグは以下に適用できます。

- マシン
- アプリケーション
- マシンカタログ（PowerShellのみ。詳細については、「マシンカタログのタグ」を参照してください）
- デリバリーグループ
- アプリケーショングループ

タグ制限は、Studioで以下を作成または編集する際に構成できます。

- 共有デリバリーグループ内のデスクトップ
- アプリケーショングループ

> **重要:**
>
> タグは、明示的にマシンに適用することも、マシンカタログまたはデリバリーグループレベルで明示的に適用することもできます。タグがマシンカタログまたはデリバリーグループレベルで適用されると、そのカタログまたはデリバリーグループ内のすべてのマシンが暗黙的にそのタグを継承します。これらの継承されたタグは、マシンレベルで削除することはできません。タグの効果を削除するには、マシンカタログまたはデリバリーグループレベルからタグを削除する必要があります。

デスクトップまたはアプリケーショングループのタグ制限

タグ制限にはいくつかの手順があります。

- タグを作成し、マシンに追加（適用）します。
- タグ制限付きのグループを作成または編集します（つまり、「タグxを持つマシンへの起動を制限する」）。

タグ制限は、ブローカーのマシン選択プロセスを拡張します。ブローカーは、アクセスポリシー、構成されたユーザーリスト、ゾーン設定、起動準備、およびタグ制限（存在する場合）に従って、関連付けられたデリバリーグループからマシンを選択します。アプリケーションの場合、

ブローカーは優先順位に従って他のデリバリーグループにフォールバックし、検討対象の各デリバリーグループに同じマシン選択ルールを適用します。

例1：シンプルなレイアウト

この例では、タグ制限を使用して、特定のデスクトップおよびアプリケーションの起動に考慮されるマシンを制限するシンプルなレイアウトを紹介します。このサイトには、1つの共有デリバリーグループ、1つの公開デスクトップ、および2つのアプリケーションで構成された1つのアプリケーショングループがあります。

シンプルなレイアウトでタグ制限を使用する例。(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/tags-example.png)

- 3台のマシン（VDA 101-103）のそれぞれにタグが追加されています。
- 共有デリバリーグループ内のデスクトップは、「Red」という名前のタグ制限付きで作成されました。デスクトップは、そのデリバリーグループ内で「Red」タグを持つマシン（VDA 101および102）でのみ起動できます。
- アプリケーショングループは「Orange」タグ制限付きで作成されたため、そのアプリケーション（CalculatorとNotepad）はそれぞれ、「Orange」タグを持つデリバリーグループ内のマシン（VDA 102および103）でのみ起動できます。

マシンVDA 102は両方のタグ（RedとOrange）を持っているため、アプリケーションとデスクトップの起動に考慮されます。

例2：より複雑なレイアウト

この例には、タグ制限付きで作成された複数のアプリケーショングループが含まれています。これにより、デリバリーグループのみを使用した場合に必要となるよりも少ないマシンで、より多くのアプリケーションを配信できるようになります。

例2の構成方法は、この例でタグを作成および適用し、タグ制限を構成するために使用される手順を示しています。

複雑なレイアウトでタグ制限を使用する例。(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/tags-example2.png)

この例では、10台のマシン（VDA 101-110）、1つのデリバリーグループ（D01）、および3つのアプリケーショングループ（A100、A200、A300）を使用します。各マシンにタグを適用し、各アプリケーショングループを作成する際にタグ制限を指定することで、次のようになります。

- グループ内の経理ユーザーは、5台のマシン（VDA 101～105）で必要なアプリにアクセスできます

- グループ内のCAD設計者は、5台のマシン（VDA 106-110）で必要なアプリにアクセスできます
- Officeアプリケーションを必要とするグループのユーザーは、10台のマシン（VDA 101-110）でOfficeアプリにアクセスできます

使用されるマシンは10台のみで、デリバリーグループは1つだけです。デリバリーグループのみを使用する場合（アプリケーショングループなし）は、マシンが1つのデリバリーグループにしか属せないため、2倍の数のマシンが必要になります。

タグとタグ制限の管理

タグは、Studioの**タグの管理**アクションを通じて、選択したアイテムから作成、追加（適用）、編集、削除されます。

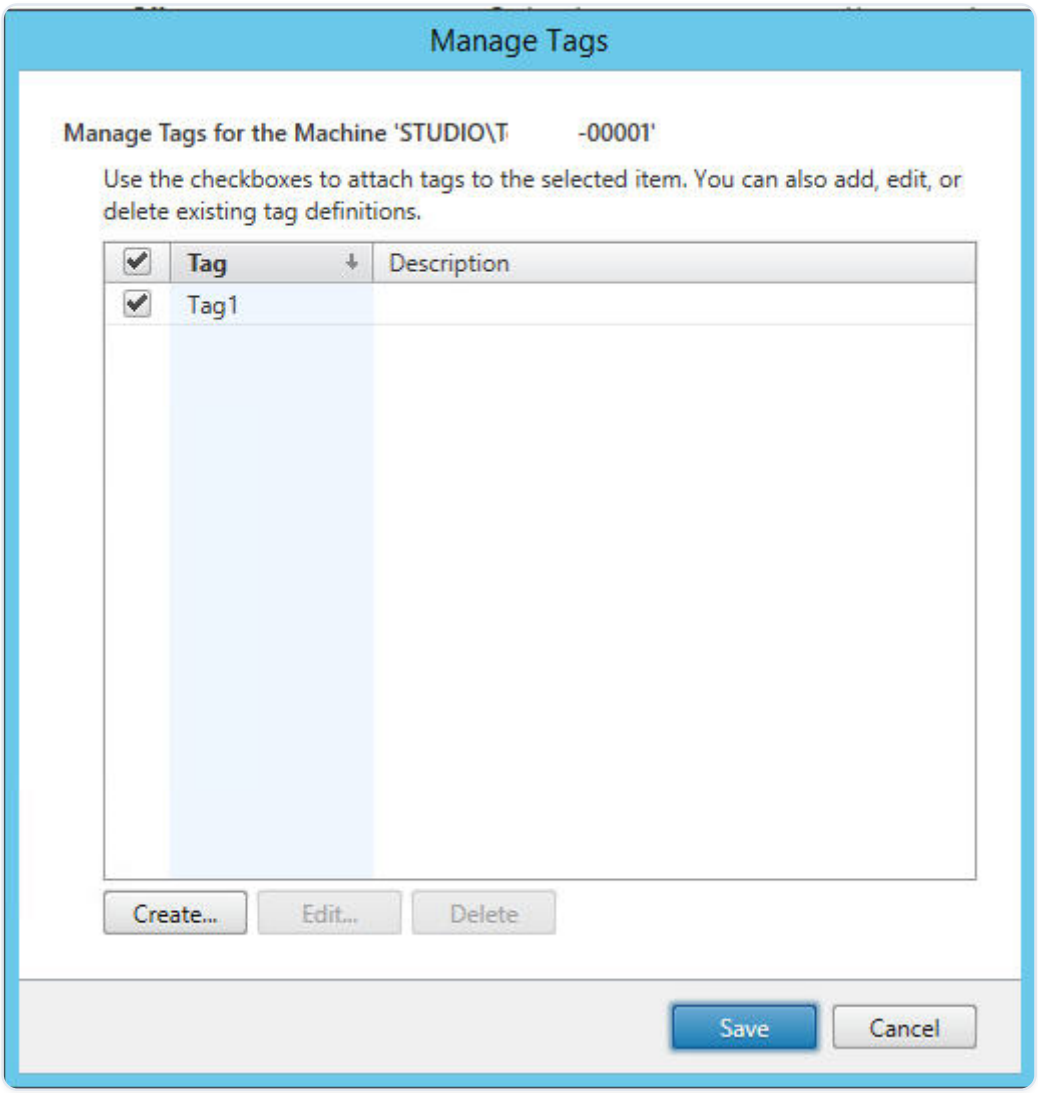
（例外：ポリシー割り当てに使用されるタグは、Studioの**タグの管理**アクションを通じて作成、編集、削除されます。ただし、タグはポリシーを作成する際に適用（割り当て）されます。詳細については、「ポリシーの作成」を参照してください。）

タグ制限は、デリバリーグループでデスクトップを作成または編集するとき、およびアプリケーショングループを作成および編集するときに構成されます。

Studioでタグの管理ダイアログを使用する

Studioで、タグを適用したいアイテム（1つ以上のマシン、アプリケーション、デスクトップ、デリバリーグループ、またはアプリケーショングループ）を選択し、その後、アクションペインで**タグの管理**を選択します。ダイアログボックスには、選択したアイテムだけでなく、サイトで作成されたすべてのタグが表示されます。

- チェックマークが付いたチェックボックスは、そのタグが選択したアイテムに既に追加されていることを示します。（以下のスクリーンショットでは、選択したマシンに「Tag1」という名前のタグが適用されています。）
- 複数のアイテムを選択した場合、ハイフンが付いたチェックボックスは、選択したアイテムの一部にのみそのタグが追加されていることを示します。



次のアクションは、**［タグの管理］**ダイアログボックスから利用できます。タグの操作に関する注意点を必ず確認してください。

- **タグを作成するには:**

  作成をクリックします。名前と説明を入力します。タグ名は一意である必要があり、大文字と小文字は区別されません。次に、**OK**をクリックします。（タグを作成しても、選択した項目に自動的に適用されるわけではありません。チェックボックスを使用してタグを適用します。）

- **1つ以上のタグを追加（適用）するには:**

  タグ名の横にあるチェックボックスをオンにします。複数の項目を選択していて、タグの横にあるチェックボックスにハイフンが含まれている場合（選択した項目の一部にのみタグが適用されていることを示す）、それをチェックマークに変更すると、選択したすべてのマシンに影響します。

1つ以上のマシンにタグを追加しようとして、そのタグがアプリケーショングループで制限として使用されている場合、その操作によってそれらのマシンが起動可能になる可能性があるという警告が表示されます。それが意図したとおりであれば、続行してください。

- **1つ以上のタグを削除するには:**

  タグ名の横にあるチェックボックスをオフにします。複数の項目を選択していて、タグの横にあるチェックボックスにハイフンが含まれている場合（選択した項目の一部にのみタグが適用されていることを示す）、チェックボックスをオフにすると、選択したすべてのマシンからタグが削除されます。

  タグを制限として使用しているマシンからタグを削除しようとすると、その操作が起動対象となるマシンに影響を与える可能性があるという警告が表示されます。それが意図したとおりであれば、続行してください。

- **タグを編集するには:**

  タグを選択し、**編集**をクリックします。新しい名前、説明、またはその両方を入力します。一度に編集できるタグは1つだけです。

- **1つ以上のタグを削除するには:**

  タグを選択し、**削除**をクリックします。「タグの削除」ダイアログボックスには、現在選択されているタグを使用している項目の数が表示されます（例：「2台のマシン」）。項目をクリックすると、詳細情報が表示されます。たとえば、「2台のマシン」項目をクリックすると、そのタグが適用されている2台のマシンの名前が表示されます。タグを削除するかどうかを確認します。

  制限として使用されているタグをStudioで削除することはできません。まず、アプリケーショングループを編集し、タグ制限を削除するか、別のタグを選択してください。

タグの管理ダイアログボックスでの作業が完了したら、**保存**をクリックします。

マシンにタグが適用されているかを確認するには：ナビゲーションペインで**デリバリーグループ**を選択します。中央ペインでデリバリーグループを選択し、その後、アクションペインで**マシンの表示**を選択します。中央ペインでマシンを選択し、その後、**詳細**ペインで**タグ**タブを選択します。

タグ制限を管理する

タグ制限の構成は複数の手順からなるプロセスです。まずタグを作成し、それをマシンに追加/適用します。次に、アプリケーショングループまたはデスクトップに制限を追加します。

- **タグを作成して適用する：**

タグを作成し、前述の**タグの管理**アクションを使用して、タグ制限の影響を受けるマシンにそのタグを追加（適用）します。

- **アプリケーショングループにタグ制限を追加するには：**

  アプリケーショングループを作成または編集します。**デリバリーグループ**ページで、**タグを持つマシンへの起動を制限する**を選択し、リストからタグを選択します。

- **アプリケーショングループのタグ制限を変更または削除するには：**

  グループを編集します。**デリバリーグループ**ページで、リストから別のタグを選択するか、**タグを持つマシンへの起動を制限する**のチェックを外してタグ制限を完全に削除します。

- **デスクトップにタグ制限を追加するには：**

  デリバリーグループを作成または編集します。**デスクトップ**ページで、**追加**または**編集**をクリックします。「デスクトップの追加」ダイアログボックスで、**タグを持つマシンへの起動を制限する**を選択し、メニューからタグを選択します。

- **デリバリーグループのタグ制限を変更または削除するには：**

  グループを編集します。デスクトップページで、**編集**をクリックします。ダイアログボックスで、リストから別のタグを選択するか、**タグを持つマシンへの起動を制限する**のチェックを外してタグ制限を完全に削除します。

タグを使用する際の注意点

アイテムに適用されたタグは、さまざまな目的に使用できます。そのため、タグの追加、削除、および削除が意図しない影響を与える可能性があることに留意してください。タグを使用して、Studioの検索フィールドでマシンの表示を並べ替えることができます。アプリケーショングループまたはデスクトップを構成する際に、同じタグを制限として使用できます。そのタグは、起動の考慮事項を、そのタグを持つ指定されたデリバリーグループ内のマシンのみに制限します。

デスクトップまたはアプリケーショングループのタグ制限として構成されたタグをマシンに追加しようとすると、警告が表示されます。そのタグを追加すると、マシンが追加のアプリケーションまたはデスクトップの起動に利用可能になる可能性があります。それが意図したものであれば、続行してください。そうでない場合は、操作をキャンセルできます。

たとえば、「Red」というタグ制限を持つアプリケーショングループを作成したとします。その後、そのアプリケーショングループで使用されている同じデリバリーグループに、他の複数のマシンを追加します。そのマシンに「Red」タグを追加しようとすると、Studioに次のようなメッセージが表示されます。「タグ「Red」は、以下のアプリケーショングループで制限として使用されています。このタグを追加すると、選択したマシンがこのアプリケーショングループでアプリケー

ションを起動できるようになる可能性があります。」その後、それらの追加マシンへのタグの追加を確定またはキャンセルできます。

同様に、アプリケーショングループが起動を制限するためにタグを使用している場合、Studioは、制限として削除するためにグループを編集するまでタグを削除できないことを警告します。（アプリケーショングループで制限として使用されているタグを削除できた場合、そのアプリケーショングループに関連付けられているデリバリーグループ内のすべてのマシンでアプリケーションの起動が許可される可能性があります。）タグがデスクトップ起動の制限として使用されている場合も、タグの削除に対する同じ禁止事項が適用されます。そのタグ制限を削除するために、デリバリーグループ内のアプリケーショングループまたはデスクトクトップを編集した後、タグを削除できます。

すべてのマシンが同じアプリケーションセットを持っているとは限りません。ユーザーは複数のアプリケーショングループに属することができ、それぞれ異なるタグ制限と、デリバリーグループからの異なるまたは重複するマシンセットを持っています。以下の表は、マシンの考慮事項がどのように決定されるかを示しています。

アプリケーションが追加された場合	選択されたデリバリーグループ内のこれらのマシンが起動対象と見なされます
タグ制限のない1つのアプリケーショングループ	任意のマシン。
タグ制限Aのある1つのアプリケーショングループ	タグAが適用されているマシン。
2つのアプリケーショングループ（1つはタグ制限A、もう1つはタグ制限B）	タグAとタグBを持つマシン。利用可能なマシンがない場合は、タグAまたはタグBを持つマシン。
2つのアプリケーショングループ（1つはタグ制限A、もう1つはタグ制限なし）	タグAを持つマシン。利用可能なマシンがない場合は、任意のマシン。

マシンの再起動スケジュールでタグ制限を使用した場合、タグの適用または制限に影響する変更は、次回のマシンの再起動サイクルに影響します。変更が行われている間に進行中の再起動サイクルには影響しません。

例2の構成方法

以下の手順では、タグを作成して適用し、2番目の例で示されているアプリケーショングループのタグ制限を構成する手順を示します。

VDAとアプリケーションはすでにマシンにインストールされており、デリバリーグループも作成されています。

マシンにタグを作成して適用します。

1. Studioで、デリバリーグループD01を選択し、アクションペインで を選択します。
2. マシンVDA 101-105を選択し、アクションペインで を選択します。
3. タグの管理ダイアログボックスで、**作成**をクリックし、`CADApps`という名前のタグを作成します。**OK**をクリックします。
4. もう一度**作成**をクリックし、OfficeAppsという名前のタグを作成します。**OK**をクリックします。
5. **タグの管理**ダイアログボックスにいる間に、新しく作成したタグを、各タグの名前（`CADApps`と`OfficeApps`）の横にあるチェックボックスを有効にすることで、選択したマシンに追加（適用）します。完了したら、ダイアログボックスを閉じます。
6. デリバリーグループD01を選択し、アクションペインで を選択します。
7. マシンVDA 106-110を選択し、アクションペインで を選択します。
8. **タグの管理**ダイアログボックスで、**作成**をクリックします。`AcctgApps`という名前のタグを作成します。**OK**をクリックします。
9. 新しく作成した`AcctgApps`タグと`OfficeApps`タグを、各タグ名の横にあるチェックボックスをクリックして、選択したマシンに適用し、ダイアログボックスを閉じます。

タグ制限付きのアプリケーショングループを作成します。

1. Studioで、ナビゲーションペインの を選択し、アクションペインの を選択します。アプリケーショングループ作成ウィザードが起動します。
2. ウィザードの**デリバリーグループ**ページで、デリバリーグループD01を選択します。**タグを持つマシンへの起動を制限する**を選択し、リストから`AcctgApps`タグを選択します。
3. ウィザードを完了し、会計ユーザーと会計アプリケーションを指定します。(アプリケーションを追加する際は、`AcctgApps`タグを持つマシン上のアプリケーションを検索する****ソースを選択します。) ****ページで、グループに`A100`という名前を付けます。
4. 前述の手順を繰り返して、`CADApps`タグを持つマシンと、適切なユーザーおよびアプリケーションを指定し、アプリケーショングループ`A200`を作成します。
5. 手順を繰り返して、`OfficeApps`タグを持つマシンと、適切なユーザーおよびアプリケーションを指定し、アプリケーショングループ`A300`を作成します。

マシンカタログのタグ

マシンカタログでタグを使用できます。タグを作成してカタログに適用する全体的な手順は、前述のとおりです。ただし、カタログへのタグの適用はPowerShellインターフェイスを介してのみサポートされています。Studioを使用してカタログにタグを適用したり、カタログからタグを削除したりすることはできません。Studioのカタログ表示では、タグが適用されているかどうかは示されません。

概要：StudioまたはPowerShellを使用して、カタログで使用するタグを作成または削除できます。PowerShellを使用してタグをカタログに適用します。

カタログでタグを使用する例をいくつか示します。

- デリバリーグループには複数のカタログのマシンが含まれていますが、特定のカタログ内のマシンのみに操作（再起動スケジュールなど）を適用したい場合があります。そのカタログにタグを適用することで、これが実現します。
- アプリケーショングループでは、アプリケーションセッションを特定のカタログ内のマシンに制限したい場合があります。そのカタログにタグを適用することで、これが実現します。

影響を受けるPowerShellコマンドレット:

- `Add-BrokerTag`や`Remove-BrokerTag`などのコマンドレットにカタログオブジェクトを渡すことができます。
- `Get-BrokerTagUsage`は、タグを含むカタログの数を示します。
- `Get-BrokerCatalog`には、`Tags`という名前のプロパティがあります。

たとえば、次のcmdletは、`acctg`という名前のカタログに`fy2018`という名前のタグを追加します。`Get-BrokerCatalog -Name acctg | Add-BrokerTag fy2018`。（このタグは、以前にStudioまたはPowerShellのいずれかを使用して作成されました。）

詳細なガイダンスと構文については、PowerShellコマンドレットのヘルプを参照してください。

詳細情報

ブログ投稿: 特定のサーバーにデスクトップを割り当てる方法。

IPv4/IPv6 のサポート

このリリースでは、純粋な IPv4、純粋な IPv6、および重複する IPv4 と IPv6 ネットワークを使用するデュアルスタック展開をサポートしています。

次のコンポーネントは IPv4 のみをサポートします。その他すべてのコンポーネントは IPv4 と IPv6 をサポートします。

- シトリックス プロビジョニング™
- シトリックス ハイパーバイザー™
- **IPv6 Controller 登録のみを使用**ポリシー設定によって制御されていないVirtual Delivery Agent (VDA)

IPv6 通信は、VDA 接続に関連する2つの Citrix® ポリシー設定によって制御されます。

- **IPv6 の使用を強制する主要な設定:** IPv6 Controller 登録のみを使用。

  このポリシー設定は、VDA が Delivery Controller に登録するために使用するアドレス形式を制御します。

  有効にすると、VDA は次の優先順位で選択された単一の IPv6 アドレスを使用して Controller と登録および通信します: グローバル IP アドレス、ユニークローカルアドレス (ULA)、リンクローカルアドレス (他の IPv6 アドレスが利用できない場合のみ)。

  無効にすると、VDA はマシンの IPv4 アドレスを使用して Controller と登録および通信します。これがデフォルト値です。

  チームが頻繁に IPv6 ネットワークを使用する場合は、**IPv6 Controller 登録のみを使用**ポリシー設定が有効になっているイメージまたは組織単位 (OU) に基づいて、それらのユーザー向けにデスクトップとアプリケーションを公開します。

  チームが頻繁に IPv4 ネットワークを使用する場合は、**IPv6 Controller 登録のみを使用**ポリシー設定が無効になっているイメージまたは OU に基づいて、それらのユーザー向けにデスクトップとアプリケーションを公開します。
- **IPv6 ネットマスクを定義する依存設定:** Controller 登録 IPv6 ネットマスク。

  マシンは複数の IPv6 アドレスを持つことができます。このポリシー設定により、管理者は、登録されている場合に、VDA をグローバル IP ではなく、優先サブネットのみに制限できます。この設定は、VDA が登録するネットワークを指定します。VDA は、指定されたネットマスクに一致する最初のアドレスにのみ登録します。

  この設定は、**IPv6 Controller 登録のみを使用**ポリシー設定が有効になっている場合にのみ有効です。デフォルト = 空の文字列

展開に関する考慮事項

環境にIPv4とIPv6の両方のネットワークが含まれている場合は、IPv4のみのクライアントと、IPv6ネットワークにアクセスできるクライアント向けに、個別のデリバリーグループ構成を作成します。ユーザーを区別するために、命名規則、手動のActive Directoryグループ割り当て、またはSmartAccessフィルターの使用を検討してください。

接続がIPv6ネットワークで開始され、その後、IPv4アクセスのみを持つクライアントから再接続しようとすると、セッションの再接続が失敗する可能性があります。

ユーザープロファイル

デフォルトでは、Virtual Delivery Agentをインストールすると、Citrix Profile Managementはマスターイメージにサイレントインストールされますが、プロファイルソリューションとしてProfile Managementを使用する必要はありません。

ユーザーのさまざまなニーズに合わせて、Citrix Virtual Apps and Desktops™ポリシーを使用して、各デリバリーグループのマシンに異なるプロファイル動作を適用できます。たとえば、あるデリバリーグループでは、テンプレートが1つのネットワークロケーションに保存されているCitrix強制プロファイルが必要な場合があります。一方、別のデリバリーグループでは、複数のリダイレクトされたフォルダーを持つ別のロケーションに保存されているCitrixローミングプロファイルが必要な場合があります。

- 組織内の他の管理者がCitrix Virtual Apps and Desktopsポリシーを担当している場合は、それらの管理者と協力して、Delivery Group全体でプロファイル関連のポリシーが設定されていることを確認してください。
- Profile Managementポリシーは、グループポリシー、Profile Management .iniファイル、および個々の仮想マシン上でローカルに設定することもできます。プロファイル動作を定義するこれらの複数の方法は、次の順序で読み取られます。

  a. グループポリシー（.admまたは.admxファイル）

  b. ポリシーノード内のCitrix Virtual Apps and Desktopsポリシー

  c. ユーザーが接続する仮想マシン上のローカルポリシー

  d. Profile Management .iniファイル

  たとえば、グループポリシーとポリシーノードの両方で同じポリシーを構成した場合、システムはグループポリシーのポリシー設定を読み取り、Citrix Virtual Apps and Desktopsポリシー設定を無視します。

どのプロファイルソリューションを選択しても、Director管理者は診断情報にアクセスし、ユーザープロファイルのトラブルシューティングを行うことができます。詳細については、Directorのドキュメントを参照してください。

自動構成

デスクトップの種類は、Virtual Delivery Agentのインストールに基づいて自動的に検出され、Studioで行う構成の選択に加えて、それに応じてProfile Managementのデフォルトを設定します。

Profile Managementが調整するポリシーを次の表に示します。デフォルト以外のポリシー設定はすべて保持され、この機能によって上書きされることはありません。各ポリシーの詳細については、Profile Managementのドキュメントを参照してください。プロファイルを作成するマシンの種類は、調整されるポリシーに影響します。主な要因は、マシンが永続的かプロビジョニング済みか、および複数のユーザーで共有されるか、1人のユーザー専用であるかです。

永続システムには何らかのローカルストレージがあり、その内容はシステムがオフになっても永続することが期待されます。永続システムは、SANなどのストレージテクノロジーを使用して、ローカルディスクのエミュレーションを提供する場合があります。対照的に、プロビジョニングシステムは、ベースディスクと何らかのIDディスクから「オンザフライ」で作成されます。ローカルストレージは通常、RAMディスクまたはネットワークディスクによってエミュレートされ、後者は高速リンクを備えたSANによって提供されることがよくあります。プロビジョニングテクノロジーは通常、Citrix ProvisioningまたはMachine Creation Services™（あるいはサードパーティの同等品）です。プロビジョニングシステムが永続的なローカルストレージを持つこともあります。これらは永続的として分類されます。

これら2つの要素を合わせると、以下のマシンタイプが定義されます。

- **永続的と専用の両方** -- 例としては、Machine Creation Servicesで作成された静的割り当てと永続的なローカルストレージを持つシングルセッションOSマシン、VDI-in-a-Boxで作成された永続ストレージを持つデスクトップ、物理ワークステーション、ラップトップなどがあります。
- **永続的と共有の両方** -- 例としては、Machine Creation Servicesで作成されたマルチセッションOSマシンなどがあります。
- **プロビジョニング済みと専用の両方** -- 例としては、Citrix Provisioning™で作成された、静的割り当てを持つが永続ストレージを持たないシングルセッションOSマシンなどがあります。
- **プロビジョニング済みと共有の両方** -- 例としては、Citrix Provisioningで作成されたランダム割り当てを持つシングルセッションOSマシン、およびVDI-in-a-Boxで作成された永続ストレージを持たないデスクトップなどがあります。

以下のProfile Managementポリシー設定は、異なるマシンタイプに対する推奨ガイドラインです。ほとんどの場合にうまく機能しますが、展開の要件に応じてこれらから逸脱することもできます。

> **重要:**
>
> **ログオフ時にローカルにキャッシュされたプロファイルを削除**、**プロファイルストリーミング**、および**常にキャッシュ**は、自動構成機能によって適用されます。その他のポリシーは手動で調整してください。

永続マシン

ポリシー	永続的かつ専用	永続的かつ共有
ログオフ時にローカルにキャッシュされたプロファイルを削除する	無効	有効
プロファイルストリーミング	無効	有効
常にキャッシュ	有効 (注1)	無効 (注2)
アクティブライトバック	無効	無効 (注3)
ローカル管理者によるログオンの処理	有効	無効 (注4)

プロビジョニング済みマシン

ポリシー	プロビジョニング済みと専用の両方	プロビジョニング済みと共有の両方
ログオフ時にローカルにキャッシュされたプロファイルを削除する	無効 (注5)	有効
プロファイルストリーミング	有効	有効
常にキャッシュ	無効 (注6)	無効
アクティブライトバック	有効	有効

ポリシー	プロビジョニング済みと専用の両方	プロビジョニング済みと共有の両方
ローカル管理者によるログオンの処理	有効	有効 (注7)

1. このマシンタイプでは**Profile streaming**が無効になっているため、**Always cache**設定は常に無視されます。
2. **Always cache**を無効にします。ただし、このポリシーを有効にし、ファイルサイズ制限 (MB単位) を定義することで、ログオン後できるだけ早く大きなファイルがプロファイルにロードされるようにすることができます。このサイズ以上のファイルは、できるだけ早くローカルにキャッシュされます。
3. Citrix Virtual Appsサーバー間をローミングするユーザーのプロファイルに変更を保存する場合を除き、**Active write back**を無効にします。この場合は、このポリシーを有効にします。
4. ホスト型共有デスクトップの場合を除き、**Process logons of local administrators**を無効にします。この場合は、このポリシーを有効にします。
5. **Delete locally cached profiles on logoff**を無効にします。この設定は、ローカルにキャッシュされたプロファイルを保持します。マシンはログオフ時にリセットされますが、個々のユーザーに割り当てられているため、プロファイルがキャッシュされているとログオンが高速になります。
6. **Always cache**を無効にします。ただし、このポリシーを有効にし、ファイルサイズ制限 (MB単位) を定義することで、ログオン後できるだけ早く大きなファイルがプロファイルにロードされるようにすることができます。このサイズ以上のファイルは、できるだけ早くローカルにキャッシュされます。
7. Citrix Virtual Apps and Desktopsサーバー間をローミングするユーザーのプロファイルの場合を除き、**Process logons of local administrators**を有効にします。この場合は、このポリシーを無効にします。

フォルダーリダイレクト

フォルダーリダイレクトを使用すると、プロファイルが保存されている場所とは異なるネットワーク共有にユーザーデータを保存できます。フォルダーリダイレクトはプロファイルのサイズとロード時間を削減しますが、ネットワーク帯域幅に影響を与える可能性があります。フォルダーリダイレクトは、Citrixユーザープロファイルが使用されていることを必要としません。独自のユーザープロファイルを管理し、フォルダーをリダイレクトすることもできます。

StudioのCitrixポリシーを使用してフォルダーリダイレクトを構成します。

- リダイレクトされたフォルダーのコンテンツを保存するために使用されるネットワークの場所が利用可能であり、適切な権限を持っていることを確認してください。場所のプロパティは検証されます。
- リダイレクトされたフォルダーはネットワーク上に設定され、その内容はログオン時にユーザーの仮想デスクトップから取り込まれます。

フォルダーリダイレクトは、CitrixポリシーまたはActive Directoryグループポリシーオブジェクトのいずれか一方のみを使用して構成し、両方は使用しないでください。両方のポリシーエンジンを使用してフォルダーリダイレクトを構成すると、予期しない動作が発生する可能性があります。

高度なフォルダーリダイレクト

複数のオペレーティングシステム（OS）を使用する展開では、ユーザープロファイルの一部を各OSで共有したい場合があります。プロファイルの残りの部分は共有されず、1つのOSでのみ使用されます。OS間で一貫したユーザーエクスペリエンスを確保するには、各OSで異なる構成、つまり高度なフォルダーリダイレクトが必要です。たとえば、2つのOSで実行されているアプリケーションの異なるバージョンが共有ファイルを読み取ったり編集したりする必要がある場合、両方のバージョンがアクセスできる単一のネットワーク場所にリダイレクトすることを選択できます。あるいは、**スタートメニュー**フォルダーの内容が2つのOSで異なる構造になっているため、両方ではなく1つのフォルダーのみをリダイレクトすることを選択できます。このアプローチにより、各OSで**スタートメニュー**フォルダーとその内容が分離され、ユーザーに一貫したエクスペリエンスが保証されます。

展開で高度なフォルダーリダイレクトが必要な場合は、ユーザーのプロファイルデータの構造を理解し、そのどの部分をOS間で共有できるかを判断する必要があります。フォルダーリダイレクトが正しく使用されないと、予期しない動作が発生する可能性があります。

高度な展開でフォルダーをリダイレクトするには：

- 各OSに個別のデリバリーグループを使用します。
- 仮想デスクトップ上の仮想アプリケーションを含む、仮想アプリケーションがユーザーデータと設定をどこに保存するか、およびデータがどのように構造化されているかを理解します。
- 安全にローミングできる共有プロファイルデータ（各OSで同じ構造であるため）については、各デリバリーグループ内のコンテナフォルダーをリダイレクトします。
- ローミングできない非共有プロファイルデータについては、デスクトップグループのいずれか1つ（通常は最も使用されているOSまたはデータが最も関連性の高いOS）のコンテナフォルダーをリダイレクトします。あるいは、OS間でローミングできない非共有データについては、両方のシステムのコンテナフォルダーを別々のネットワーク場所にリダイレクトします。

高度な展開の例

この展開には、Windows 10デスクトップで実行されるMicrosoft OutlookおよびInternet Explorerのバージョンを含むアプリケーションと、Windows Server 2019によって配信されるOutlookおよびInternet Explorerの他のバージョンを含むアプリケーションがあります。2つのOS用に2つのデリバリーグループを既に設定しています。ユーザーは、両方のアプリケーションのバージョンで同じ**連絡先**と**お気に入り**のセットにアクセスしたいと考えています。

重要： 以下の決定とアドバイスは、説明されているOSと展開に有効です。組織では、リダイレクトするフォルダーとそれらを共有するかどうかの決定は、特定の展開に固有のさまざまな要因によって異なります。

- デリバリーグループに適用されるポリシーを使用して、次のフォルダーをリダイレクトするように選択します。

フォルダ	WINDOWS 10でリダイレクトされますか？	WINDOWS SERVER 2019でリダイレクトされますか？
マイドキュメント	はい	はい
アプリケーションデータ	いいえ	いいえ
連絡先	はい	はい
デスクトップ	はい	いいえ
ダウンロード	いいえ	いいえ
お気に入り	はい	はい
リンク	はい	いいえ
マイミュージック	はい	はい
マイピクチャ	はい	はい
マイビデオ	はい	はい
検索	はい	いいえ
保存されたゲーム	いいえ	いいえ
スタートメニュー	はい	いいえ

- 共有され、リダイレクトされるフォルダーの場合：
  - OutlookとInternet Explorerの異なるバージョンによって保存されたデータの構造を分析した結果、**連絡先**フォルダーと**お気に入り**フォルダーを共有しても安全であると判断しました。
  - **マイドキュメント**、**マイミュージック**、**マイピクチャ**、**マイビデオ**フォルダーの構造はOS間で標準的であることがわかっています。そのため、これらのフォルダーを各デリバリーグループで同じネットワークロケーションに保存しても安全です。
- 共有されない、リダイレクトされるフォルダーの場合：
  - Windows Serverデリバリーグループでは、デスクトップ、リンク、検索、または**スタートメニュー**フォルダーをリダイレクトしません。これらのフォルダー内のデータは2つのOSで異なる方法で整理されているためです。したがって、共有することはできません。
  - この共有されないデータの予測可能な動作を保証するために、Windows 10デリバリーグループでのみリダイレクトします。Windows 10は、ユーザーが日常業務でより頻繁に使用します。ユーザーはWindows Serverによって提供されるアプリケーションにたまにしかアクセスしません。また、この場合、共有されないデータはアプリケーション環境よりもデスクトップ環境により関連性が高くなります。たとえば、デスクトップショートカットは**デスクトップ**フォルダーに保存され、Windows 10マシンから作成されたものであれば役立つ可能性がありますが、Windows Serverマシンから作成されたものではありません。
- リダイレクトされないフォルダーの場合:
  - ユーザーがダウンロードしたファイルでサーバーを煩雑にしたくないため、ダウンロードフォルダーをリダイレクトしないことを選択します
  - 個々のアプリケーションからのデータは互換性やパフォーマンスの問題を引き起こす可能性があるため、アプリケーションデータフォルダーをリダイレクトしないことを決定します

フォルダーリダイレクトの詳細については、「フォルダーリダイレクト、オフラインファイル、および移動ユーザープロファイルの概要」を参照してください。

フォルダーリダイレクトと除外

Citrix Profile Management（Studioではない）では、パフォーマンス強化により、除外を使用してフォルダーが処理されないようにすることができます。この機能を使用する場合、リダイレクトされたフォルダーを除外しないでください。フォルダーリダイレクト機能と除外機能は連携して動作します。リダイレクトされたフォルダーが除外されないようにすることで、後でリダイレクトしないと決定した場合でも、Profile Managementはそれらをプロファイルフォルダー構造に戻

し、データの整合性を維持できます。除外の詳細については、「項目の含める/除外」を参照してください。

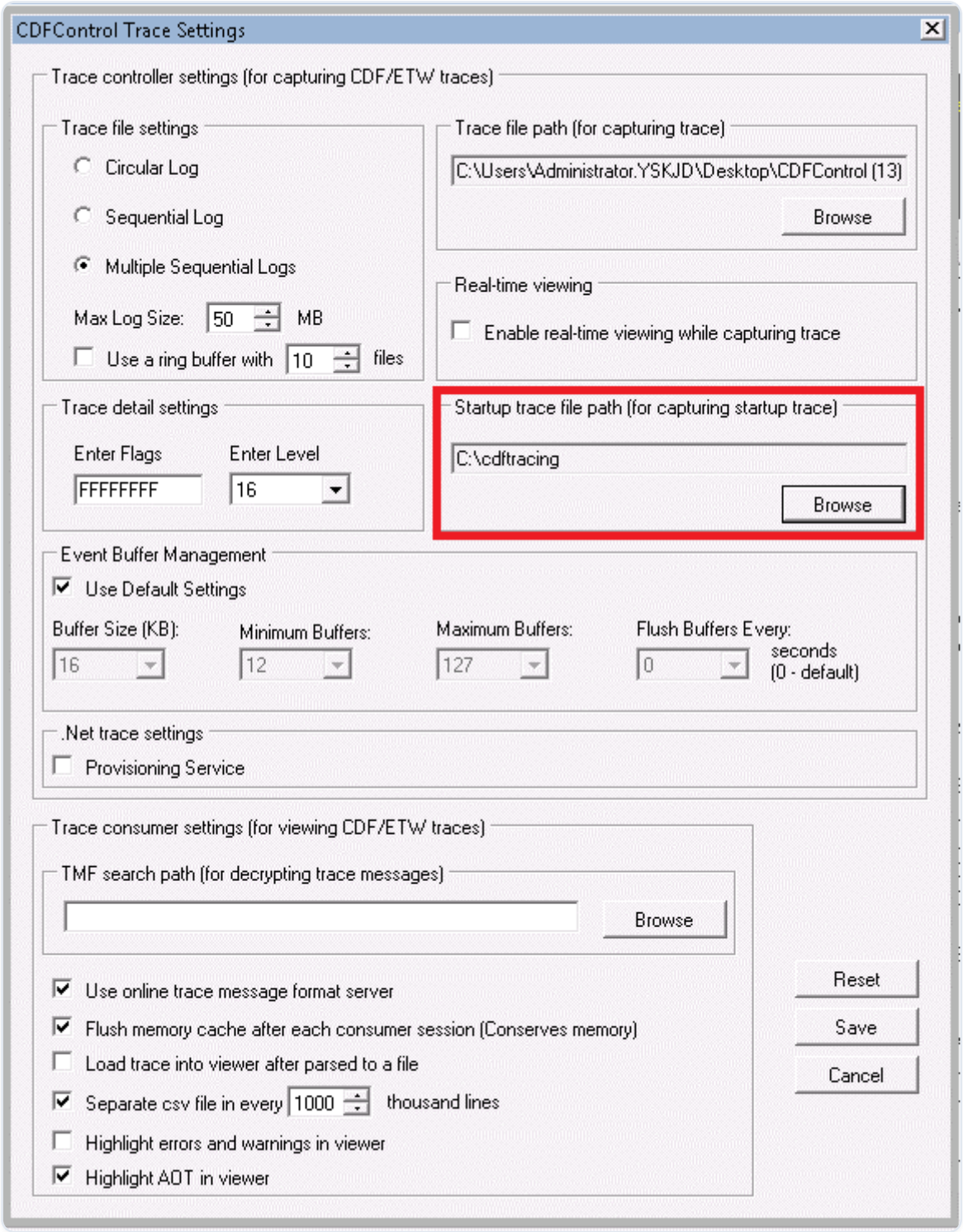
システム起動時にCitrix Diagnostic Facility (CDF) トレースを収集する

CDFControlユーティリティは、さまざまなCitrixトレースプロバイダーから表示されるCitrix Diagnostic Facility (CDF) トレースメッセージをキャプチャするためのイベントトレースコントローラーまたはコンシューマーです。これは、複雑なCitrix関連の問題のトラブルシューティング、フィルターサポートの解析、およびパフォーマンスデータの収集を目的としています。CDFControlユーティリティをダウンロードするには、CTX111961を参照してください。

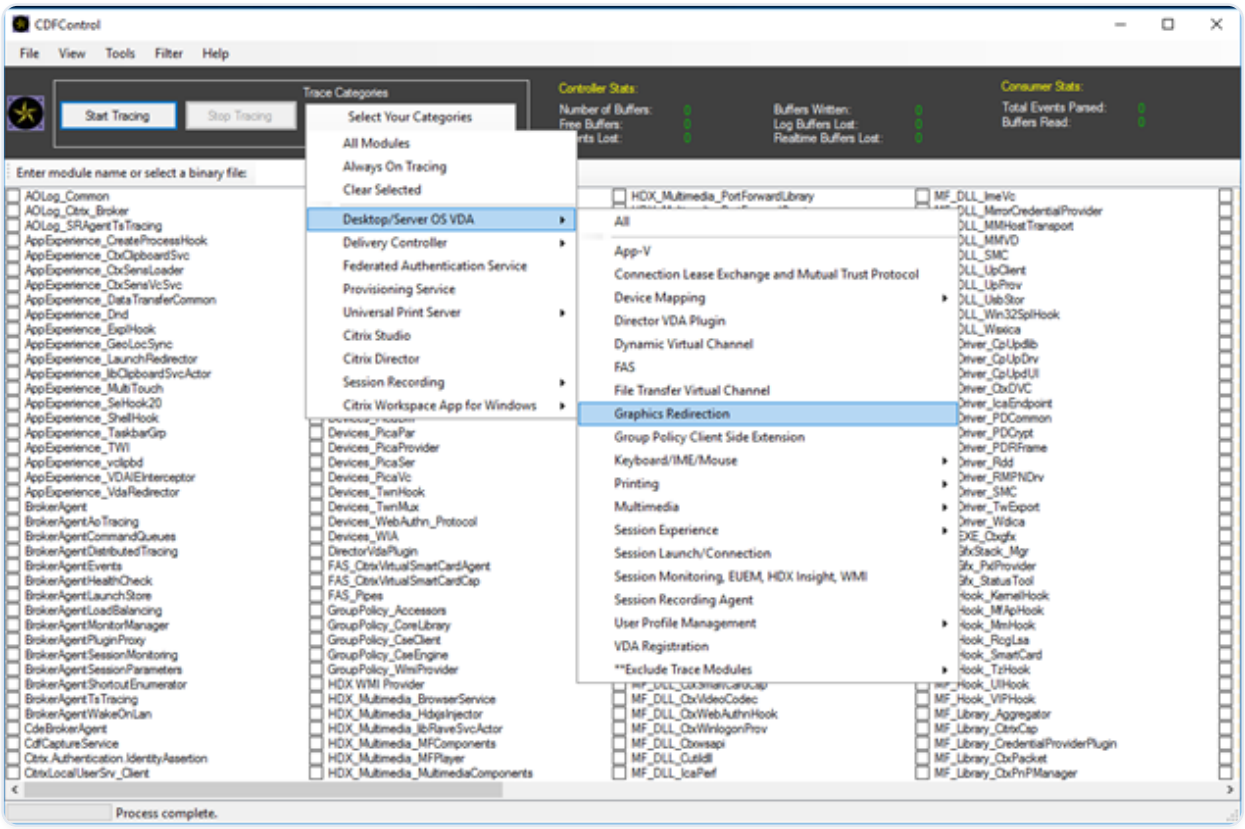
システム起動時にトレースを収集する

システム起動時にCDFトレースを収集するには、次の手順を使用します。管理者権限が必要です。

1. **CDFControl**を起動し、**ツール**メニューから**オプション**を選択します。
2. **起動トレースをキャプチャするための起動トレースファイルパス**セクションでトレースファイルパスを指定します。次に、**保存**をクリックします。



3. Citrixサポートが推奨する**トレースカテゴリ**を選択します。（以下の例では、**グラフィックリダイレクト**が選択されています。この選択は単なる例です。トラブルシューティングしている特定の問題に対してプロバイダーを有効にすることをお勧めします。）



4. **起動トレース**を選択し、**ツール**メニューから**有効にする**を選択します。

   有効にするを選択すると、アニメーションバーがスクロールを開始します。このアクティビティは手順に影響しません。次のステップに進みます。

5. **起動トレース**が有効になったら、**CDFControlユーティリティ**を閉じ、システムを再起動します。

6. **CDFControl**ユーティリティを起動します。システムが再起動し、エラーが表示されたら、**ツール**メニューから**起動トレース**を選択し、**無効にする**をクリックして起動トレースを無効にします。

7. 手順2で指定したトレースファイルパスに移動し、分析のためにトレースログファイル（.etl）を収集します。

シトリックス インサイト サービス

Citrix Insight Services (CIS)は、計測、テレメトリ、ビジネスインサイト生成のためのCitrixプラットフォームです。その計測およびテレメトリ機能により、技術ユーザー（顧客、パートナー、エンジニア）は問題を自己診断して修正し、環境を最適化できます。CISとその仕組みに関する詳細および最新情報については、`<https://cis.citrix.com>`を参照してください（Citrixアカウントの資格情報が必要です）。

Citrixにアップロードされるすべての情報は、トラブルシューティングと診断の目的、および製品の品質、信頼性、パフォーマンスの向上のために使用されます。ただし、以下に従います。

- シトリックス インサイト サービス ポリシー (https://cis.citrix.com/legal)
- Citrixプライバシーポリシー（`<https://www.cloud.com/privacy-policy>`）

このCitrix Virtual Apps and Desktops™リリースは、以下のテクノロジーをサポートしています。

- Citrix Virtual Apps and Desktopsのインストールおよびアップグレード分析
- Citrixカスタマーエクスペリエンス向上プログラム（CEIP）
- シトリックス コール ホーム
- シトリックス スカウト

CISおよびCitrix Analyticsとは別に（加えて）、Studioをインストール（またはアップグレード）すると、Google Analyticsが自動的に収集され（その後アップロードされ）ます。Studioのインストール後、レジストリキー`HKLM\Software\Citrix\DesktopStudio\GAEnabled`を使用してこの設定を変更できます。値が1の場合は収集とアップロードが有効になり、0の場合は収集とアップロードが無効になります。

インストールおよびアップグレード分析

フルプロダクトインストーラーを使用してCitrix Virtual Apps and Desktopsコンポーネントを展開またはアップグレードすると、インストールプロセスに関する匿名情報が収集され、コンポーネントをインストール/アップグレードしているマシンに保存されます。このデータは、Citrixが顧客のインストールエクスペリエンスを向上させるのに役立てられます。

この情報は、`%ProgramData%\Citrix\CTQs`にローカルに保存されます。

このデータの自動アップロードは、フルプロダクトインストーラーのグラフィカルインターフェイスとコマンドラインインターフェイスの両方で、デフォルトで有効になっています。

- レジストリ設定のデフォルト値を変更できます。インストール/アップグレード前にレジストリ設定を変更した場合、フルプロダクトインストーラーを使用する際にその値が使用されます。
- コマンドでオプションを指定することにより、コマンドラインインターフェイスでインストール/アップグレードする際にデフォルト設定を上書きできます。

自動アップロードの制御:

- インストール/アップグレード分析の自動アップロードを制御するレジストリ設定 (デフォルト = 1):

  - 場所: `HKLM:\Software\Citrix\MetaInstall`
  - 名前: SendExperienceMetrics
  - 値: 0 = 無効、1 = 有効

- PowerShell を使用すると、次のコマンドレットでインストール/アップグレード分析の自動アップロードが無効になります:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\MetaInstall -Name
SendExperienceMetrics -PropertyType DWORD -Value 0
```

- XenDesktopServerSetup.exe または XenDesktopVDASetup.exe コマンドで自動アップロードを無効にするには、`/disableexperiencemetrics` オプションを含めます。

  XenDesktopServerSetup.exe または XenDesktopVDASetup.exe コマンドで自動アップロードを有効にするには、`/sendexperiencemetrics` オプションを含めます。

Citrix カスタマーエクスペリエンス向上プログラム

Citrix カスタマーエクスペリエンス向上プログラム (CEIP) に参加すると、匿名の統計情報と使用状況情報が Citrix に送信され、Citrix 製品の品質とパフォーマンスの向上に役立てられます。詳細については、https://more.citrix.com/XD-CEIP を参照してください。

サイト作成時またはアップグレード時の登録

サイトを作成すると (最初の Delivery Controller™ をインストールした後)、CEIP に自動的に登録されます。データの最初のアップロードは、サイト作成後約7日後に行われます。サイト作成後はいつでも参加を停止できます。Studio ナビゲーションペインの **構成** ノード (**製品サポート** タブ) を選択し、ガイダンスに従ってください。

Citrix Virtual Apps and Desktops 展開をアップグレードする場合:

- CEIP をサポートしていないバージョンからアップグレードする場合、参加するかどうかを尋ねられます。
- CEIPをサポートしていたバージョンからアップグレードし、参加が有効になっていた場合、アップグレードされたサイトでCEIPが有効になります。
- CEIPをサポートしていたバージョンからアップグレードし、参加が無効になっていた場合、アップグレードされたサイトでCEIPが無効になります。
- CEIPをサポートしていたバージョンからアップグレードし、参加状況が不明な場合、参加を希望するかどうか尋ねられます。

収集された情報は匿名であるため、Citrix Insight Servicesにアップロードされた後は閲覧できません。

VDAインストール時の登録

デフォルトでは、Windows VDAをインストールすると、CEIPに自動的に登録されます。このデフォルト設定はレジストリ設定で変更できます。VDAをインストールする前にレジストリ設定を変更した場合、その値が使用されます。

CEIPへの自動登録を制御するレジストリ設定（デフォルト = 1）：

場所: `HKLM:\Software\Citrix\Telemetry\CEIP` 名前: Enabled 値: 0 = 無効, 1 = 有効

デフォルトでは、`Enabled` プロパティはレジストリに隠されています。指定されていない場合、自動アップロード機能は有効になります。

PowerShellを使用すると、次のコマンドレットでCEIPへの登録を無効にできます。

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name Enabled
-PropertyType DWORD -Value 0
```

収集されたランタイムデータポイントは、定期的にファイルとして出力フォルダー（デフォルト %programdata%/Citrix/VdaCeip）に書き込まれます。

データの初回アップロードは、VDAのインストール後約7日で行われます。

その他の製品およびコンポーネントのインストール時の登録

関連するCitrix製品、コンポーネント、テクノロジー（Citrix Provisioning™、AppDNA、Citrix License Server、Windows向けCitrix Workspace™アプリ、Universal Print Server、Session Recordingなど）をインストールする際にも、CEIPに参加できます。インストールと参加のデフォルト値の詳細については、それぞれのドキュメントを参照してください。

Citrix コールホーム

Citrix Virtual Apps and Desktops に特定のコンポーネントと機能をインストールすると、Citrix Call Home に参加する機会が提供されます。Call Home は診断データを収集し、そのデータを含むテレメトリパッケージを分析とトラブルシューティングのために Citrix Insight Services に直接（デフォルトポート 443 の HTTPS 経由で）定期的にアップロードします。

Citrix Virtual Apps and Desktops では、Call Home は Citrix Telemetry Service という名前のバックグラウンドサービスとして実行されます。詳しくは、https://more.citrix.com/XD-CALLHOME を参照してください。

Call Home のスケジュール機能は Citrix Scout でも利用できます。詳しくは、Citrix Scout を参照してください。

収集される情報

Citrix Diagnostic Facility (CDF) トレースは、トラブルシューティングに役立つ情報をログに記録します。Call Home は、一般的な障害（VDA 登録やアプリケーション/デスクトップの起動など）のトラブルシューティングに役立つ CDF トレースのサブセットを収集します。このテクノロジーは、常時オンのトレース (AOT) として知られています。AOT ログは、C:\Users\CitrixTelemetryService\Appdata\Local\CitrixAOT にディスクに保存されます。

Call Home は、その他の Event Tracing for Windows (ETW) 情報を収集せず、またそのように構成することもできません。

Call Home は、次のようなその他の情報も収集します。

- `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix` の下に Citrix Virtual Apps and Desktops によって作成されたレジストリ。
- Citrix 名前空間下の Windows Management Instrumentation (WMI) 情報。
- 実行中のプロセスの一覧。
- `%PROGRAMDATA%\Citrix\CDF` に保存されている Citrix プロセスのクラッシュダンプ。
- インストールおよびアップグレード情報。これには、製品の完全なメタインストーラーログ、失敗した MSI ログ、MSI ログアナライザーからの出力、StoreFront™ ログ、ライセンス互換性チェックログ、および予備的なサイトアップグレードテストの結果が含まれる場合があります。

トレース情報は、収集時に圧縮されます。Citrix Telemetry Service は、最大 10 MB の圧縮された最新のトレース情報を、最大 8 日間保持します。

- データを圧縮することで、Call Home は VDA 上で小さなフットプリントを維持できます。
- プロビジョニングされたマシンでの IOPs を回避するために、トレースはメモリに保持されます。
- トレースバッファは、トレースをメモリに保持するために循環メカニズムを使用します。

Call Home は、Call Home の主要データポイント に記載されている主要なデータポイントを収集します。

構成と管理の概要

Call Home には、製品版インストールウィザードを使用するか、後で PowerShell コマンドレットを使用して登録できます。登録すると、デフォルトで診断情報が収集され、毎週日曜日の現地時間午前 3 時頃に Citrix にアップロードされます。アップロードは、指定された時刻から 2 時間の間隔でランダム化されます。これは、デフォルトのスケジュールを使用するアップロードが午前 3 時から午前 5 時の間に行われることを意味します。

診断情報を定期的にアップロードしたくない場合（またはスケジュールを変更したい場合）は、PowerShell コマンドレットを使用して診断情報を手動で収集してアップロードするか、ローカルに保存することができます。

スケジュールされた Call Home アップロードに登録する場合、および診断情報を手動で Citrix にアップロードする場合、Citrix アカウントまたは Citrix Cloud™ の資格情報を提供します。Citrix は、資格情報をアップロードトークンと交換します。このトークンは、顧客を識別し、データをアップロードするために使用されます。資格情報は保存されません。

アップロードが行われると、Citrix アカウントに関連付けられているアドレスに通知メールが送信されます。

コンポーネントのインストール時に Call Home を有効にした場合、後で無効にできます。

前提条件

- マシンは PowerShell 3.0 以降を実行している必要があります。
- Citrix Telemetry Service がマシン上で実行されている必要があります。
- システム変数 `PSModulePath` は、Telemetry のインストールパス（例: `C:\Program Files\Citrix\Telemetry Service\`）に設定されている必要があります。

コンポーネントのインストール中に Call Home を有効にする

VDA のインストールまたはアップグレード中: 製品版インストーラーのグラフィカルインターフェイスを使用して Virtual Delivery Agent をインストールまたはアップグレードする際に、Call Home に参加するかどうかを尋ねられます。次の 2 つのオプションがあります。

- Call Home に参加する。
- Call Home に参加しない。

VDAをアップグレードしていて、以前にCall Homeに登録していた場合、そのウィザードページは表示されません。

Controllerのインストールまたはアップグレード中: グラフィカルインターフェイスを使用してDelivery Controllerをインストールまたはアップグレードすると、Call Homeに参加するかどうかを尋ねられます。3つのオプションがあります。

Controllerをインストールする際、そのサーバーに「サービスとしてログオン」ポリシー設定が適用されたActive Directory GPOがある場合、インストールウィザードのCall Homeページで情報を構成することはできません。詳細については、CTX218094を参照してください。

Controllerをアップグレードしていて、以前にCall Homeに登録していた場合、参加について尋ねられることはありません。

PowerShellコマンドレット

PowerShellヘルプには、これらの一般的なユースケースでは使用されないコマンドレットとパラメーターの説明を含む、包括的な構文が記載されています。

アップロードにプロキシサーバーを使用するには、「プロキシサーバーの構成」を参照してください。

- **スケジュールされたアップロードを有効にする:** 診断コレクションはCitrixに自動的にアップロードされます。カスタムスケジュール用の追加のコマンドレットを入力しない場合、デフォルトのスケジュールが使用されます。

  ```
  $cred = Get-Credential

  Enable-CitrixCallHome -Credential $cred
  ```

  スケジュールされたアップロードが有効になっていることを確認するには、`Get-CitrixCallHome`と入力します。有効になっている場合、戻り値は`IsEnabled=True`と`IsMasterImage=False`です。

- **マスターイメージから作成されたマシンに対するスケジュールされたアップロードを有効にする:** マスターイメージでスケジュールされたアップロードを有効にすると、マシンカタログで作成される各マシンを構成する必要がなくなります。

  `Enable-CitrixCallHome -Credential $cred -MasterImage`

  スケジュールされたアップロードが有効になっていることを確認するには、**Get-CitrixCallHome**と入力します。有効になっている場合、戻り値は`IsEnabled=True`と`IsMasterImage=True`です。

- **カスタムスケジュールを作成する:** 診断コレクションとアップロードの毎日または毎週のスケジュールを作成します。

```
$timespan = New-TimeSpan –Hours hours -Minutes minutes

Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek day
-UploadFrequency {Daily|Weekly}
```

例:

次のコマンドレットは、毎晩22:20にデータをバンドルしてアップロードするスケジュールを作成します。Hoursパラメーターは24時間形式を使用します。`UploadFrequency`パラメーターの値がDailyの場合、`DayOfWeek`パラメーターは指定されていても無視されます。

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20

Set-CitrixCallHomeSchedule –TimeOfDay $timespan -UploadFrequency Daily
```

スケジュールを確認するには、`Get-CitrixCallHomeSchedule`と入力します。上記の例では、`StartTime=22:20:00, DayOfWeek=Sunday (ignored), Upload Frequency=Daily`が返されます。

次のコマンドレットは、毎週水曜日の夜10時20分にデータをバンドルしてアップロードするスケジュールを作成します。

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20

Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek Wed
-UploadFrequency Weekly
```

スケジュールを確認するには、`Get-CitrixCallHomeSchedule`と入力します。上記の例では、`StartTime=22:20:00, DayOfWeek=Wednesday, Upload Frequency=Weekly`が返されます。

Call Homeを無効にする

PowerShellコマンドレットを使用するか、Citrix Scoutを介してCall Homeを無効にできます。

Call Homeのスケジュールされたアップロードが無効になっている場合でも、AOTログは収集され、ディスクに保存されます。(スケジュールされたアップロードが無効になっている場合、AOT

ログはCitrixに自動的にアップロードされません。) AOTログの収集とローカルストレージを無効にすることができます。

PowerShellでCall Homeを無効にする

次のコマンドレットを実行すると、診断データはCitrixに自動的にアップロードされなくなります。(Citrix ScoutまたはテレメトリPowerShellコマンドレットを使用して、診断データをアップロードすることは引き続き可能です。)

```
Disable-CitrixCallHome
```

Call Homeが無効になっていることを確認するには、`Get-CitrixCallHome`と入力します。無効になっている場合、戻り値は`IsEnabled=False`と`IsMasterImage=False`です。

Citrix Scoutを使用して収集スケジュールを無効にする

Citrix Scoutを使用して診断収集スケジュールを無効にするには、コレクションのスケジュールのガイダンスに従ってください。ステップ3で、**オフ**をクリックして、選択したマシンのスケジュールをキャンセルします。

AOTログの収集を無効にする

次のコマンドレットを実行すると(`Enabled`フィールドを`false`に設定すると)、AOTログは収集されなくなります。

```
Enable-CitrixTrace -Listen'{"trace":{"enabled":false,"persistDirectory":"C:\Users\Public","maxSizeBytes":1000000, "sliceDurationSeconds":300}}'
```

`Listen`パラメーターには、JSON形式の引数が含まれています。

Call Homeアップロード用のプロキシサーバーを構成する

Call Homeが有効になっているマシンで、次のタスクを完了します。以下の手順の例の図には、サーバーアドレスとポート10.158.139.37:3128が含まれています。お客様の情報は異なります。

1. ブラウザーにプロキシサーバー情報を追加します。Internet Explorer で、 **\> \>** を選択します。「**LAN にプロキシ サーバーを使用する**」を選択し、プロキシサーバーのアドレスとポート番号を入力します。
2. PowerShell で `netsh winhttp import proxy source=ie` を実行します。

   プロキシサーバーを構成する際の netsh コマンド実行例(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/call-home-proxy-ie.png)
3. テキストエディターを使用して、`C:\Program Files\Citrix\Telemetry Service` にある TelemetryService.exe 構成ファイルを編集します。赤枠で示されている情報を追加します。

TelemetryService.exe ファイルにプロキシ情報を追加(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/call-home-proxy-config.png)

4. テレメトリサービスを再起動します。

PowerShell で Call Home コマンドレットを実行します。

診断情報を手動で収集してアップロードする

CIS Webサイトを使用して、診断情報バンドルをCISにアップロードできます。PowerShell コマンドレットを使用して、診断情報を収集し、CISにアップロードすることもできます。

CIS Webサイトを使用してバンドルをアップロードするには：

1. Citrixアカウントの資格情報を使用して、Citrix Insight Servicesにログオンします。
2. を選択します。
3. を選択し、データの場所に移動します。

CISは、データアップロードを管理するいくつかのPowerShellコマンドレットをサポートしています。このドキュメントでは、2つの一般的なケースのコマンドレットについて説明します。

- `Start-CitrixCallHomeUpload` コマンドレットを使用して、診断情報バンドルを手動で収集し、CISにアップロードします。（バンドルはローカルに保存されません。）
- `Start-CitrixCallHomeUpload` コマンドレットを使用して、データを手動で収集し、診断情報バンドルをローカルに保存します。これにより、データをプレビューできます。その後、`Send-CitrixCallHomeBundle` コマンドレットを使用して、そのバンドルのコピーをCISに手動でアップロードします。(最初に保存したデータはローカルに残ります。)

PowerShellヘルプには、これらの一般的なユースケースでは使用されないコマンドレットとパラメーターの説明を含む、包括的な構文が記載されています。

CISにデータをアップロードするコマンドレットを入力すると、アップロードの確認を求められます。アップロードが完了する前にコマンドレットがタイムアウトした場合は、システムイベントログでアップロードのステータスを確認してください。サービスがすでにアップロードを実行している場合、アップロード要求は拒否される可能性があります。

データの収集とバンドルのCISへのアップロード:

```
Start-CitrixCallHomeUpload [-Credential] PSCredential [-InputPath string]
[-Description string] [-IncidentTime string] [-SRNumber string] [-Name
```

```
string] [-UploadHeader string] [-AppendHeaders string] [-Collect string]
[<CommonParameters>]
```

データの収集とローカルへの保存:

```
Start-CitrixCallHomeUpload -OutputPath <String> [-InputPath string] [-
Description string] [-IncidentTime string] [-SRNumber string] [-Name
string] [-UploaderHeader string] [-AppendHeaders string] [-Collect
strings] [<CommonParameters>]
```

次のパラメーターが有効です。

- **Credential:** CISへのアップロードを指示します。
- **InputPath:** バンドルに含めるzipファイルの場所。これは、Citrixサポートが要求する追加ファイルである可能性があります。.zip拡張子を含めるようにしてください。
- **OutputPath:** 診断情報が保存される場所。このパラメーターは、Call Homeデータをローカルに保存する場合に必須です。
- **Description and Incident Time:** アップロードに関する自由形式の情報。
- **SRNumber:** Citrixテクニカルサポートのインシデント番号。
- **Name:** バンドルを識別する名前。
- **UploadHeader:** CISにアップロードされるアップロードヘッダーを指定するJSON形式の文字列。
- **AppendHeaders:** CISにアップロードされる追加ヘッダーを指定するJSON形式の文字列。
- **Collect:** 収集または省略するデータを指定するJSON形式の文字列で、{'collector': {'enabled':Boolean}} の形式で、Booleanはtrueまたはfalseです。 有効なコレクター値は次のとおりです。
  - 'WMI'
  - 'プロセス'
  - 'レジストリ
  - 'クラッシュレポート'
  - 'トレース'
  - 'ファイル'
  - 'MSI'
  - 'ローカルデータ'

- 'サイトデータ'
- 'SFB'

デフォルトでは、「sfb」を除くすべてのコレクターが有効になっています。

「sfb」コレクターは、Skype for Businessの問題を診断するためにオンデマンドで使用するように設計されています。「enabled」パラメーターに加えて、「sfb」コレクターは、ターゲットユーザーを指定するための「account」および「accounts」パラメーターをサポートしています。次のいずれかの形式を使用します。

- "-収集 "`{'sfb':{'account':'domain\user1'}}`"
- "-収集 "`{'sfb':{'accounts':['domain\user1', 'domain\user2']}}`"

- **共通パラメーター:** PowerShellのヘルプを参照してください。

以前にローカルに保存されたデータをアップロードする:

`Send-CitrixCallHomeBundle -Credential <PSCredentia\> -Path string [<CommonParameters>]`

`Path` パラメーターは、以前に保存されたバンドルの場所を指定します。

例:

以下のコマンドレットは、Call Home データ（WMI コレクターからのデータを除く）を CIS にアップロードするよう要求します。このデータは、Citrix Support ケース 123456 について午後 2 時 30 分に記録された Citrix Provisioning VDA の登録失敗に関連しています。Call Home データに加えて、ファイル「`c:\Diagnostics\ExtraData.zip`」がアップロードされたバンドルに組み込まれます。

```
C:\PS\>Start-CitrixCallHomeUpload -InputPath "c:
\Diagnostics\ExtraData.zip" -Description "Registration failures with
Citrix Provisioning VDAs" -IncidentTime "14:30" -SRNumber 123456 -Name
"RegistrationFailure-021812016" -Collect "{'wmi':{'enabled':false}}"
-UploadHeader "{'key1':'value1'}" -AppendHeaders "{'key2':'value2'}"
```

以下のコマンドレットは、午前 8 時 15 分に記録された Citrix Support ケース 223344 に関連する Call Home データを保存します。データはネットワーク共有上のファイル mydata.zip に保存されます。Call Home データに加えて、ファイル「`c:\Diagnostics\ExtraData.zip`」が保存されたバンドルに組み込まれます。

```
C:\PS\>Start-CitrixCallHomeUpload -OutputPath \
\mynetwork\myshare\mydata.zip -InputPath "c:\Diagnostics\ExtraData.zip"
-Description "Diagnostics for incident number 223344" -IncidentTime "8:15"
-SRNumber 223344
```

以下のコマンドレットは、以前に保存したデータバンドルをアップロードします。

```
$cred=Get-Credential

C:\PS>Send-CitrixCallHomeBundle –Credential $cred -Path \
\mynetwork\myshare\mydata.zip
```

シトリックス スカウト

はじめに

Citrix Scout は診断情報を収集し、ヘルスチェックを実行します。その結果を使用して、Citrix Virtual Apps and Desktops™ の展開を維持できます。Citrix は、Citrix Insight Services を通じて、診断情報収集の包括的な自動分析を提供します。また、Scout を使用して、単独で、または Citrix サポートのガイダンスを受けて、問題をトラブルシューティングすることもできます。

収集ファイルを Citrix にアップロードして、Citrix サポートからの分析とガイダンスを受けることができます。または、収集をローカルに保存して自分で確認し、後で収集ファイルを Citrix にアップロードして分析することもできます。

Scout は次の手順を提供します。

- **収集:** サイトで選択したマシンに対して、1 回限りの診断情報収集を実行します。その後、ファイルを Citrix にアップロードするか、ローカルに保存できます。
- **トレースと再現:** 選択したマシンで手動トレースを開始します。次に、それらのマシンで問題を再現します。問題を再現した後、トレースは停止されます。その後、Scout は他の診断情報を収集し、ファイルを Citrix にアップロードするか、ローカルに保存します。
- **スケジュール:** 選択したマシンで、指定した時間に毎日または毎週診断情報収集が実行されるようにスケジュールします。ファイルは自動的に Citrix にアップロードされます。
- **ヘルスチェック:** サイトとそのコンポーネントの健全性と可用性を測定するチェックを実行します。Delivery Controller、Virtual Delivery Agent (VDA)、StoreFront™ サーバー、および Citrix License Server のヘルスチェックを実行できます。チェック中に問題が発見された場合、Scout は詳細なレポートを提供します。Scout が起動するたびに、更新されたヘルス

チェックスクリプトがチェックされます。新しいバージョンが利用可能な場合、Scout はそれらを自動的にダウンロードし、次回のヘルスチェック実行時に使用します。

> **注：**
>
> **トレースと再現、スケジュール、ヘルスチェック**の手順は、現在 Linux VDA では利用できません。

> この記事で説明されているグラフィカルインターフェイスは、Scout を使用する主要な方法です。または、PowerShell を使用して、1 回限りまたはスケジュールされた診断情報収集とアップロードを構成することもできます。(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/manage-deployment/cis.html#citrix-call-home)を参照してください。

Scout の実行場所:

- オンプレミス展開では、Delivery Controller™ から Scout を実行して、1 つ以上の Virtual Delivery Agent (VDA)、Delivery Controller、StoreFront サーバー、および License Server で診断情報を取得したり、チェックを実行したりできます。VDA から Scout を実行して、ローカル診断情報を収集することもできます。
- Citrix DaaS (旧 Citrix Virtual Apps and Desktops サービス) を使用する Citrix Cloud 環境では、VDA から Scout を実行してローカル診断情報を収集します。

Scout アプリケーションのログは `C:\ProgramData\Citrix\TelemetryService\ScoutUI.log` に保存されます。このファイルはトラブルシューティングに使用できます。

Citrix Scout のデモンストレーションを見る。

<iframe src="https://www.youtube.com/embed/2y9k07r8i0" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>

収集される情報

Scoutによって収集される診断情報には、Citrix Diagnostic Facility（CDF）トレースログファイルが含まれます。Always-on Tracing（AOT）と呼ばれるCDFトレースのサブセットも含まれます。AOT情報は、VDA登録やアプリケーション/デスクトップの起動などの一般的な問題のトラブルシューティングに役立ちます。その他のEvent Tracing for Windows（ETW）情報は収集されません。

収集される情報には以下が含まれます。

- Citrix Virtual Apps and Desktopsによって`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`の下に作成されたレジストリエントリ。
- **Citrix名前空間**の下のWindows Management Instrumentation（WMI）情報。
- 実行中のプロセス。
- `%PROGRAMDATA%\Citrix\CDF`に保存されているCitrixプロセスのクラッシュダンプ。
- Citrixポリシー情報（CSV形式）。
- インストールおよびアップグレード情報。収集される情報には、製品の完全なメタインストーラーログ、失敗したMSIログ、MSIログアナライザーからの出力、StoreFrontログ、ライセンス互換性チェックログ、および予備的なサイトアップグレードテストの結果が含まれる場合があります。

トレース情報について：

- トレース情報は収集時に圧縮され、マシン上のフットプリントを小さく保ちます。
- 各マシンで、Citrix Telemetry Serviceは圧縮された最新のトレース情報を最大8日間保持します。
- Citrix Virtual Apps and Desktops 7 1808以降、AOTトレースはデフォルトでローカルディスクに保存されます。（以前のバージョンでは、トレースはメモリに保持されていました。）デフォルトパス = `C:\Users\CitrixTelemetryService\AppData\Local\CitrixAOT`。
- Citrix Virtual Apps and Desktops 7 1811以降、ネットワーク共有に保存されたAOTトレースは、他の診断情報とともに収集されます。
- `Enable-CitrixTrace` cmdletまたは`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Telemetry DefaultListen`レジストリ文字列を使用して、最大サイズ（デフォルト = 10 MB）とスライス期間を変更できます。
- トレースは、ファイルが`MaxSize`の10%に達するまでファイルに追加されます。

Scoutが収集するデータポイントのリストについては、「Call Home key datapoints」を参照してください。

Scoutの構成

ScoutはLinux VDAで動作するように構成できます。Linux VDAとテレメトリの詳細については、「Citrix Telemetry Serviceとの統合」を参照してください。

Linux VDAは、`ctxtelemetry`ソケットポートまたはテレメトリサービス用のポートを自動的に変更する場合があります。その場合は、ポートを手動で構成する必要があります。

1. C:\Program Files\Citrix\Telemetry Serviceに移動します。

2. ScoutUI.exe.configファイルを開きます。
3. LinuxVDATelemetryServicePortまたはLinuxVDATelemetryWakeupPortの値を、Linux VDAで構成された値に変更します。

- `<add key="LinuxVDATelemetryServicePort" value="7502"/>`
- `<add key="LinuxVDATelemetryWakeupPort" value="7503"/>`

1. 変更を保存してファイルを閉じます。
2. 最新の構成が読み込まれていることを確認するために、Scoutを再度開きます。

ヘルスチェックについて

ヘルスチェックデータは、`C:\ProgramData\Citrix\TelemetryService\`の下のフォルダーに保存されます。

サイトのヘルスチェック

サイトのヘルスチェックは、FlexCast Management Architecture (FMA) サービスを包括的に評価する環境テストサービスに含まれています。これらのチェックでは、サービスの可用性を確認するだけでなく、データベース接続などの他のヘルスインジケーターも確認します。

サイトのヘルスチェックはDelivery Controllerで実行されます。サイトの規模によっては、これらのチェックの完了に最大1時間かかる場合があります。

DELIVERY CONTROLLER の構成チェック

サイトの健全性チェックの一環として、Delivery Controller の構成チェックでは、Virtual Apps and Desktops サイトに関する Citrix の推奨事項に基づいて、以下の問題が存在するかどうかを確認します。

- 1 つ以上の Delivery Controller が失敗状態にある。
- サイトに Delivery Controller が 1 つしかない。
- Delivery Controller のバージョンが異なる。

健全性チェックの 権限と要件 を満たすことに加えて、Delivery Controller の構成チェックには以下が必要です。

- 少なくとも 1 つの Controller の電源がオンになっていること。
- Controller 上で Broker Service が実行されていること。
- Controller からサイトデータベースへの接続が機能していること。

VDA の健全性チェック

VDA の健全性チェックは、一般的な VDA 登録、セッション起動、およびタイムゾーンリダイレクトの問題の考えられる原因を特定します。

VDA での登録について、Scout は以下をチェックします。

- VDA ソフトウェアのインストール
- VDA マシンのドメインメンバーシップ
- VDA 通信ポートの可用性
- VDA サービスステータス
- Windows ファイアウォール構成
- Controller との通信
- Controller との時刻同期
- VDA 登録ステータス

VDA でのセッション起動について、Scout は以下をチェックします。

- セッション起動通信ポートの可用性
- セッション起動サービスのステータス
- セッション起動 Windows ファイアウォール構成
- VDA リモートデスクトップサービス クライアントアクセスライセンス
- VDA アプリケーション起動パス
- セッション起動レジストリ設定

VDA でのタイムゾーンリダイレクトについて、Scout は以下をチェックします。

- Windows ホットフィックスのインストール
- Citrix ホットフィックスのインストール
- Microsoft グループポリシー設定
- Citrix グループポリシー設定

VDA 上の Profile Management について、Scout は以下をチェックします。

- ハイパーバイザーの検出
- プロビジョニングの検出
- シトリックス バーチャル アプリ アンド デスクトップ

- Personal vDisk の構成
- ユーザー ストア
- Profile Management Service の状態検出
- Winlogon.exe フックテスト

Profile Management のチェックを実行するには、VDA に Profile Management をインストールして有効にする必要があります。Profile Management の構成チェックの詳細については、Knowledge Center の記事 CTX132805 を参照してください。

StoreFront のヘルスチェック

StoreFront のチェックでは、以下を確認します。

- Citrix Default Domain サービスが実行中であること
- Citrix Credential Wallet サービスが実行中であること
- StoreFront サーバーから Active Directory ポート 88 への接続
- StoreFrontサーバーからActive Directoryポート389への接続
- ベースURLが有効なFQDNであること
- ベースURLから正しいIPアドレスを取得できること
- IISアプリケーションプールが.NET 4.0を使用していること
- 証明書がホストURLのSSLポートにバインドされているかどうか
- 証明書チェーンが完全であるかどうか
- 証明書の有効期限が切れているかどうか
- 証明書がまもなく（30日以内に）期限切れになるかどうか

ライセンスサーバーのチェック

ライセンスサーバーのチェックでは、以下を確認します。

- Delivery Controllerからのライセンスサーバー接続
- ライセンスサーバーのファイアウォールリモートアクセスステータス
- Citrix Licensingサービスのステータス
- ライセンスサーバーの猶予期間の状態
- ライセンスサーバーポートの接続
- Citrix ベンダーデーモン (CITRIX) が実行されているかどうか
- システムクロックが同期されているかどうか

- Citrix Licensing サービスがローカルサービスアカウントで実行されているかどうか
- `CITRIX.opt` ファイルの存在
- カスタマーサクセスサービス資格日
- Citrix ライセンスサーバーの更新
- ライセンスサーバー証明書がDelivery Controllerの信頼されたルートストアにあるかどうか

ヘルスチェックの権限と要件を満たすことに加えて、ライセンスサーバーはドメインに参加している必要があります。そうでない場合、ライセンスサーバーは検出されません。

ヘルスチェックの実行

ヘルスチェック手順は、マシンの選択、チェックの開始、および結果レポートの確認で構成されます。

1. Scout を起動します。マシンの メニューから、 > を選択します。開始ページで、 をクリックします。
2. マシンを選択します。 をクリックしてマシンを検出します。 ページには、サイトで検出されたすべての VDA、Delivery Controller、およびライセンスサーバーが一覧表示されます。表示はマシン名でフィルタリングできます。診断を収集する各マシンの横にあるチェックボックスをオンにして、 をクリックします。

   その他のコンポーネントタイプ（StoreFront サーバーや VDA マシンなど）を追加するには、「Add machines manually」および「Import VDA machines」を参照してください。Citrix Provisioning™ サーバーまたはライセンスサーバーを手動で追加することはできません。

   Scout は、選択された各マシンで検証テストを自動的に起動し、Verification tests に記載されている基準を満たしていることを確認します。検証に失敗した場合、 列にメッセージが表示され、そのマシンのチェックボックスがオフになります。次のいずれかを実行できます。

   - 問題を解決してから、マシンのチェックボックスを再度オンにします。これにより、検証テストが再試行されます。
   - そのマシンをスキップします（チェックボックスは選択解除のままにします）。そのマシンではヘルスチェックは実行されません。

   検証テストが完了したら、**続行**をクリックします。
3. 選択したマシンでヘルスチェックを実行します。概要には、テストが実行されたマシン（検証テストに合格した選択済みのマシン）が一覧表示されます。**チェック開始**をクリックします。

   チェック中およびチェック後：

- **ステータス**列は、マシンの現在のチェック状態を示します。
- 進行中のすべてのチェックを停止するには、ページ右下隅にある**チェック停止**をクリックします。（単一のマシンのヘルスチェックをキャンセルすることはできず、選択したすべてのマシンのみをキャンセルできます。チェックが完了したマシンからの情報は保持されます。）.
- 選択したすべてのマシンのチェックが完了すると、右下隅の**チェック停止**ボタンが**完了**に変わります。
- チェックが失敗した場合は、**アクション**列の**再試行**をクリックできます。
- チェックが問題なく完了した場合、**アクション**列は空になります。
- チェックで問題が見つかった場合は、**詳細表示**をクリックして結果を表示します。
- 選択したすべてのマシンのチェックが完了した後、**戻る**をクリックしないでください。（クリックすると、チェック結果が失われます。）

4. チェックが完了したら、**完了**をクリックしてScoutの開始ページに戻ります。

ヘルスチェックの結果

レポートを生成するCitrixチェックの場合、レポートには以下が含まれます。

- 結果レポートが生成された日時
- チェックされたマシン
- ターゲットマシンでチェックが探した条件

権限と要件

権限:

- 診断情報を収集するには:
  - 診断情報を収集する各マシンで、ローカル管理者およびドメインユーザーである必要があります。
  - 各マシンで LocalAppData ディレクトリへの書き込み権限が必要です。
- ヘルスチェックを実行するには:
  - ドメインユーザーグループのメンバーである必要があります。
  - フル管理者であるか、サイトに対する読み取り専用および **Run Environment Tests** 権限を持つカスタムロールを持っている必要があります。

    - スクリプトの実行を許可するには、スクリプト実行ポリシーを少なくとも `RemoteSigned` に設定します。例: `Set-ExecutionPolicy RemoteSigned`。**注:** 他のスクリプト実行権限でも機能する場合があります。

- Scout の起動時には、**管理者として実行**を使用します。

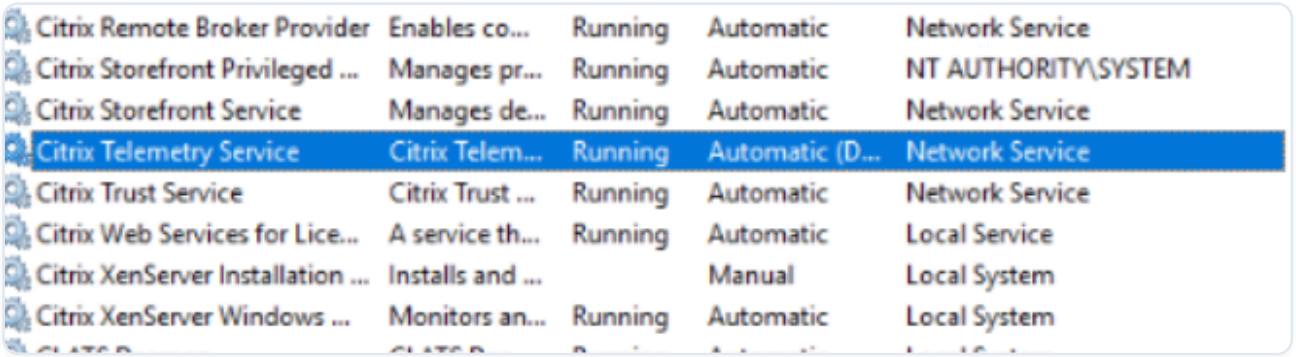
診断情報を収集したり、ヘルスチェックを実行したりする各マシンについて:

- Scout がマシンと通信できる必要があります。
- ファイルとプリンターの共有がオンになっている必要があります。
- PSRemotingとWinRMを有効にする必要があります。マシンではPowerShell 3.0以降も実行されている必要があります。
- マシンでCitrix Telemetry Serviceが実行されている必要があります。
- マシンでWindows Management Infrastructure (WMI) アクセスが有効になっている必要があります。
- 診断コレクションのスケジュールを設定するには、マシンで互換性のあるScoutバージョンが実行されている必要があります。

パス名で指定するユーザー名にドル記号 ($) を使用しないでください。診断情報の収集が妨げられます。

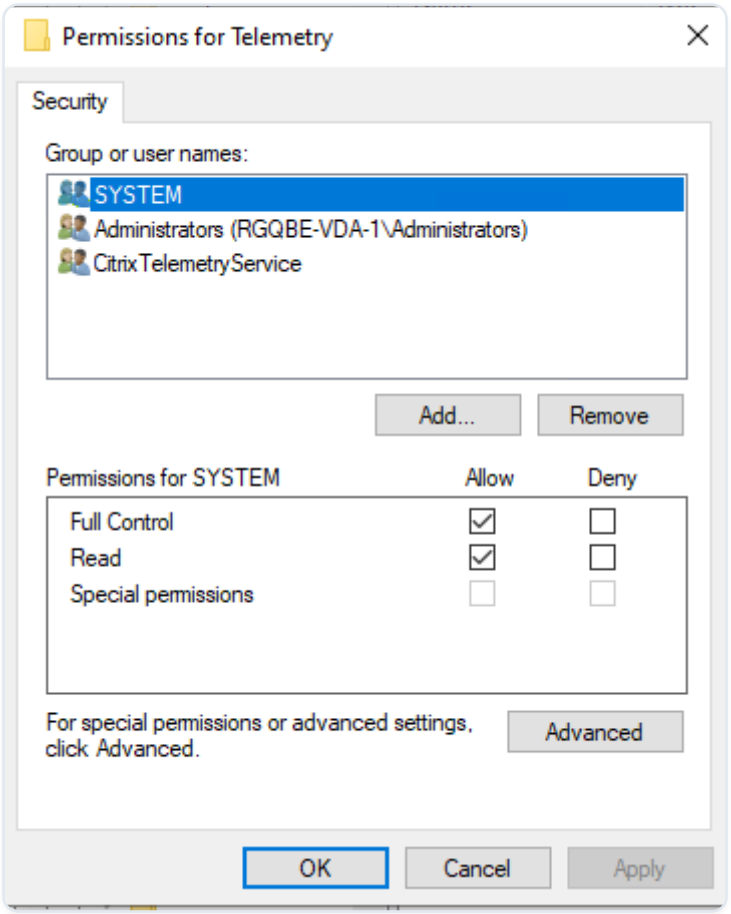
Scoutは、選択したマシンで検証テストを実行し、これらの要件が満たされていることを確認します。

Windows用Telemetry Serviceは、ネットワークサービスで実行されます。

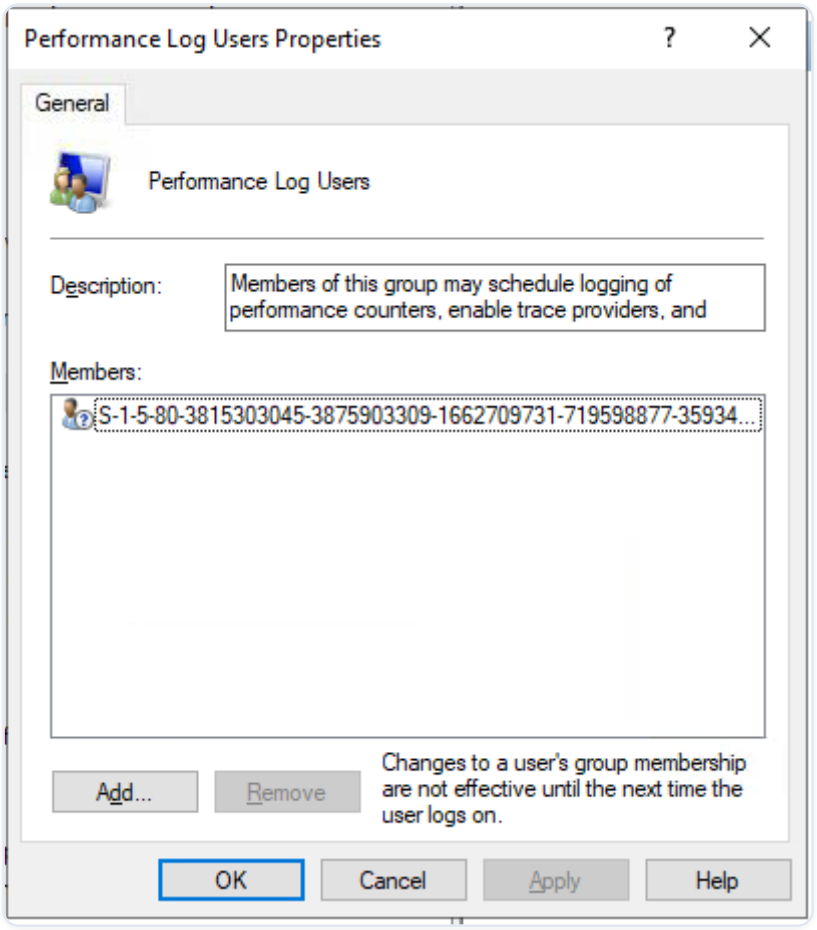


AOTトレースフォルダーは `C:\ProgramData\Citrix\TelemetryService\CitrixAOT` に保存されます。

Administratorグループ、System、およびTelemetry Service SIDのユーザーのみが、`HKEYLOCALMACHINE:SOFTWARE\Citrix\Telemetry` レジストリにアクセスする権限を持っています。



Telemetry Serviceをアンインストールした後も、Telemetry Service SIDはPerformance Log Usersグループに残りますが、手動で削除できます。



検証テスト

診断コレクションまたはヘルスチェックが開始される前に、選択された各マシンに対して検証テストが自動的に実行されます。これらのテストは、要件が満たされていることを確認します。マシンのテストが失敗した場合、Scoutは推奨される修正措置とともにメッセージを表示します。

- **Scoutがこのマシンに到達できません** - 以下を確認してください。
  - マシンが電源オンになっていること。
  - ネットワーク接続が正常に機能していること。(これには、ファイアウォールが適切に構成されていることの確認が含まれる場合があります。)
  - ファイルとプリンターの共有がオンになっていること。手順については、Microsoftのドキュメントを参照してください。
- **PSRemotingとWinRMを有効にする** - PowerShellリモート処理とWinRMを同時に有効にできます。**管理者として実行**を使用して、`Enable-PSRemoting`コマンドレットを実行します。詳細については、コマンドレットに関するMicrosoftのヘルプを参照してください。
- **ScoutにはPowerShell 3.0 (最小) が必要です** - マシンにPowerShell 3.0 (またはそれ以降) をインストールし、PowerShellリモート処理を有効にしてください。

- **このマシン上のLocalAppDataディレクトリにアクセスできません** - アカウントに、マシン上のLocalAppDataディレクトリへの書き込み権限があることを確認してください。
- **Citrix Telemetry Serviceが見つかりません** - Citrix Telemetry Serviceがマシンにインストールされ、開始されていることを確認してください。
- **スケジュールを取得できません** - マシンを(最小) XenApp and XenDesktop 7.14にアップグレードしてください。
- **WMIがマシンで実行されていません** - Windows Management Instrumentation (WMI) アクセスが有効になっていることを確認してください。
- **WMI接続がブロックされています** - WindowsファイアウォールサービスでWMIを有効にしてください。
- **より新しいバージョンのCitrix Telemetry Serviceが必要です** - (バージョンはCollectおよびTrace & Reproduceでのみチェックされます。) マシン上のTelemetry Serviceのバージョンをアップグレードしてください (インストールとアップグレードを参照)。サービスをアップグレードしない場合、そのマシンは**Collect**または**Trace & Reproduce**アクションに含まれません。
- **Scoutがこのマシン上のsystemdソケットに接続できません** - 以下を確認してください。
  - ポート7503が開いていること。systemd ctxtelemetry.socketがマシン上のポート7503でリッスンしていることを確認してください。ctxtelemetry.socketポートが変更されている場合、ポートが異なる可能性があります。ポートを調整するには、Scoutの構成を参照してください。
  - ネットワーク接続が正しく機能していることを確認します。（これには、ファイアウォールが適切に構成されていることの確認が含まれる場合があります。）
- **このマシンでLinux VDAテレメトリーサービスが開始されていません** - 以下を確認してください。
  - ポート7502が開いていることを確認します。Linux VDAテレメトリーサービスがマシンにインストールされ、開始されていることを確認します。テレメトリーサービスポートが変更されている場合、ポートが異なる可能性があります。ポートを調整するには、Scoutの構成を参照してください。
  - ネットワーク接続が正しく機能していることを確認します。（これには、ファイアウォールが適切に構成されていることの確認が含まれる場合があります。）

バージョン互換性

このバージョンのScout (3.x) は、Citrix Virtual Apps and Desktops (または最低でもXenApp and XenDesktop 7.14) のコントローラーおよびVDAで実行することを目的としています。

機能	スカウト 2.23	スカウト 3.0
Citrix Virtual Apps and Desktops (およびXenApp and XenDesktop 7.14〜7.18) をサポート	はい	はい
XenDesktop 5.x、7.1〜7.13 をサポート	はい	いいえ
XenApp 6.x、7.5〜7.13をサポート	はい	いいえ
製品に同梱	7.1〜7.13	7.14以降
CTX記事からダウンロード可能	はい	いいえ
CDFトレースをキャプチャ	はい	はい
Always-on-Traces (AOT) をキャプチャ	いいえ	はい
診断データの収集を許可	一度に最大10台のマシン（デフォルト）	無制限（リソースの可用性による）
診断データをCitrixに送信することを許可	はい	はい
診断データをローカルに保存することを許可	はい	はい
Citrix Cloud™資格情報をサポート	いいえ	はい
Citrix資格情報をサポート	はい	はい
アップロード用のプロキシサーバーをサポート	はい	はい
スケジュールを調整	該当なし	はい
スクリプトのサポート	コマンドライン（ローカルControllerのみ）	Call Homeコマンドレットを使用したPowerShell

機能	スカウト 2.23	スカウト 3.0
		（Telemetry Serviceがインストールされているすべてのマシン）
ヘルスチェック	いいえ	はい
データマスキング	いいえ	3.17以降

インストールとアップグレード

デフォルトでは、VDAまたはControllerをインストールまたはアップグレードすると、Citrix Telemetry Serviceの一部としてScoutが自動的にインストールまたはアップグレードされます。

VDAのインストール時にCitrix Telemetry Serviceを省略した場合、または後でサービスを削除した場合は、Citrix Virtual Apps and Desktopsインストールメディアの`x64\Virtual Desktop Components`または`x86\Virtual Desktop Components`フォルダーから`TelemetryServiceInstaller_xx.msi`を実行します。

Collectまたは**Trace & Reproduce**アクションを選択すると、マシンで古いバージョンのCitrix Telemetry Serviceが実行されている場合に通知されます。Citrixでは、サポートされている最新バージョンを使用することをお勧めします。そのマシンでTelemetry Serviceをアップグレードしない場合、そのマシンは**Collect**または**Trace & Reproduce**アクションに含まれません。Telemetry Serviceをアップグレードするには、インストールと同じ手順を使用します。

アップロードの承認

診断コレクションをCitrixにアップロードする予定がある場合は、CitrixアカウントまたはCitrix Cloudアカウントが必要です。（これらは、Citrixダウンロードにアクセスしたり、Citrix Cloud Control Centerにアクセスしたりするために使用する資格情報です。）アカウントの資格情報が検証されると、トークンが発行されます。

- Citrixアカウントで認証する場合、トークン発行プロセスは表示されません。アカウントの資格情報を入力するだけです。Citrixが資格情報を検証すると、Scoutウィザードを続行できます。
- Citrix Cloudアカウントで認証する場合、リンクをクリックして、デフォルトのブラウザーでHTTPSを使用してCitrix Cloudにアクセスします。Citrix Cloudの資格情報を入力すると、トークンが表示されます。トークンをコピーしてScoutに貼り付けます。その後、Scoutウィザードを続行できます。

トークンは、Scoutを実行しているマシンにローカルに保存されます。次回**Collect**または**Trace & Reproduce**を実行するときにそのトークンを使用できるようにするには、**Store token and skip this step in the future**チェックボックスをオンにします。

Scoutの開始ページで**Schedule**を選択するたびに、再承認する必要があります。スケジュールを作成または変更するときに、保存されたトークンを使用することはできません。

アップロードにプロキシを使用する

プロキシサーバーを使用してコレクションをCitrixにアップロードする場合は、ブラウザーのインターネットプロパティ用に構成されたプロキシ設定を使用するようにScoutに指示できます。または、プロキシサーバーのIPアドレスとポート番号を指定することもできます。

マシンの検索

Collect、**Trace & Reproduce**、および**Schedule**の手順では、Scoutは自動的に検出したControllerとVDAを一覧表示します。

Delivery Controller から Scout Health Check を実行するときは、**Find machine** をクリックして、デリバリーコントローラー、VDA、ライセンスサーバー、StoreFront サーバーなどのマシンを検出します。

Delivery Controller ではないドメイン参加済みマシンから Scout Health Check を実行すると、Scout はマシンを自動的に検出できません。マシンを手動で追加する か、VDA マシンをインポートする 必要があります。

マシンを手動で追加する

Scout が検出したコントローラーと VDA を一覧表示した後、StoreFront サーバー、ライセンスサーバー、Citrix Provisioning サーバーなど、展開内の他のマシンを手動で追加できます。

ヘルスチェック の実行時：

- ドメイン内の Citrix ライセンスサーバーは自動的に検出されます。ライセンスサーバーを手動で追加することはできません。
- ヘルスチェックは現在、Citrix Provisioning サーバーをサポートしていません。

検出されたマシンを一覧表示する Scout ページで、**+ Add machine** をクリックします。追加するマシンの FQDN を入力し、**Continue** をクリックします。必要に応じて、他のマシンを追加するために繰り返します。（FQDN の代わりに DNS エイリアスを入力しても有効に見える場合がありますが、ヘルスチェックが失敗する可能性があります。）

手動で追加されたマシンは、常に検出されたマシンよりも上の、マシンリストの先頭に表示されます。

手動で追加されたマシンを識別する簡単な方法は、行の右端にある赤い削除ボタンです。そのボタンがあるのは手動で追加されたマシンのみです。検出されたマシンにはありません。

手動で追加されたマシンを削除するには、行の右端にある赤いボタンをクリックします。削除を確認します。他の手動で追加されたマシンを削除するために繰り返します。

Scout は、手動で追加されたマシンを削除するまで記憶しています。Scout を閉じてから再度開くと、手動で追加されたマシンは引き続きリストの先頭に表示されます。

StoreFront サーバーで **Trace & Reproduce** を使用する場合、CDF トレースは収集されません。ただし、その他のすべてのトレース情報は収集されます。

VDA マシンをインポートする

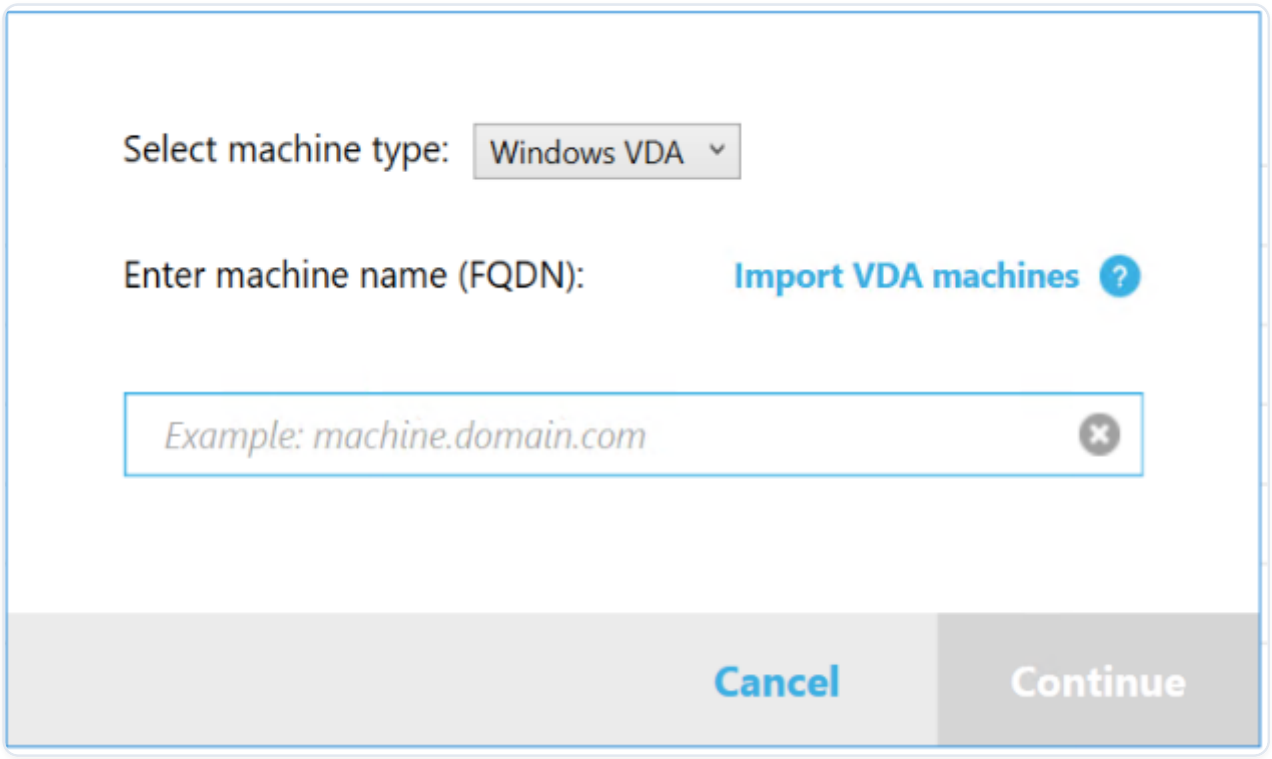
ヘルスチェック の実行時に、展開内の VDA マシンをインポートできます。

1. Delivery Controller または Connector で、PowerShell コマンドを使用してマシンリストファイルを生成します。Connector では、Citrix 資格情報を入力し、ポップアップダイアログで顧客を選択する必要があります。

   ```
   Get-BrokerMachine| foreach { $_.DnsName } | out-file C:\machineList.txt
   ```

2. machineList.txt ファイルを、Scout Health Check を起動するドメイン参加済みマシンにコピーします。
3. Scout Health Check ページで、 をクリックします。
4. マシンタイプを選択します。
5. をクリックします。
6. machineList.txt ファイルを選択します。
7. をクリックします。

インポートされた VDA マシンが Scout Health Check ページに一覧表示されます。



診断情報の収集

手順には、マシンの選択、診断情報収集の開始、および収集を含むファイルを Citrix にアップロードするかローカルに保存する作業が含まれます。

1. Scout を起動します。マシンの メニューから、 > を選択します。開いたページで、 をクリックします。
2. マシンを選択します。

   - Controller では、 ページにサイト内のすべての VDA と Controller が一覧表示されます。マシン名で表示をフィルターできます。他のマシン（StoreFront や Citrix Provisioning サーバーなど）を手動で追加するには、「マシンを手動で追加する」を参照してください。
   - その他のコンポーネント（VDA サーバーなど）では、 ページにはローカルマシンのみが表示されます。マシンの手動追加はサポートされていません。

   診断情報を収集する各マシンの横にあるチェックボックスをオンにして、**続行**をクリックします。

   Scoutは、選択した各マシンで検証テストを自動的に起動し、検証テストに記載されている基準を満たしていることを確認します。検証に失敗すると、**ステータス**列にメッセージが表示され、そのマシンのチェックボックスがオフになります。次のいずれかを実行できます。

   - 問題を解決してから、そのマシンのチェックボックスを再度オンにします。これにより、検証テストが再試行されます。

- そのマシンをスキップします（チェックボックスをオフのままにします）。そのマシンからは診断情報は収集されません。

検証テストが完了したら、**続行**をクリックします。

3. 診断情報を収集します。概要には、診断情報が収集されるすべてのマシン（検証テストに合格した選択済みのマシン）が一覧表示されます。**収集開始**をクリックします。

   収集中:

   - **ステータス**列には、マシンの現在の収集状態が表示されます。
   - 単一マシンでの進行中の収集を停止するには、そのマシンの**アクション**列にある**キャンセル**をクリックします。
   - 進行中のすべての収集を停止するには、ページの右下隅にある**収集を停止**をクリックします。収集が完了したマシンからの診断情報は保持されます。収集を再開するには、各マシンの**アクション**列にある**再試行**をクリックします。
   - 選択したすべてのマシンで収集が完了すると、右下隅にある**収集を停止**ボタンが**続行**に変わります。
   - 診断情報を再度収集するには、そのマシンの**アクション**列にある**再度収集**をクリックします。新しい収集は以前の収集を上書きします。
   - 収集に失敗した場合は、**アクション**列にある**再試行**をクリックできます。正常に収集されたもののみがアップロードまたは保存されます。
   - 選択したすべてのマシンで収集が完了した後、**戻る**をクリックしないでください。（クリックすると、収集は失われます。）

   収集が完了したら、**続行**をクリックします。

4. コレクションを保存またはアップロードします。ファイルをCitrixにアップロードするか、ローカルマシンに保存するかを選択します。

   今すぐファイルをアップロードする場合は、手順5に進みます。

   ファイルをローカルに保存することを選択した場合:

   - Windowsの**保存**ダイアログボックスが表示されます。目的の場所に移動します。
   - ローカル保存が完了すると、ファイルのパス名が表示され、リンクされます。ファイルを表示できます。後でファイルをCitrixにアップロードできます。CTX136396を参照してください。

   完了をクリックしてScoutの開始ページに戻ります。この手順でこれ以上ステップを完了する必要はありません。

5. アップロードの認証を行い、必要に応じてプロキシを指定します。詳細については、(#upload-authorization)を参照してください。

   - Scoutを通じて認証していない場合は、この手順に進みます。
   - Scoutを通じて認証済みの場合、保存されている認証トークンがデフォルトで使用されます。これを行う場合は、このオプションを選択して**続行**をクリックします。このコレクションの資格情報は要求されません。手順6に進みます。
   - 以前に認証済みだが、再認証して新しいトークンを取得したい場合は、**変更/再認証**をクリックしてこの手順に進みます。

   アップロードを認証するためにCitrix資格情報を使用するか、Citrix Cloud資格情報を使用するかを選択します。**続行**をクリックします。資格情報ページは、保存されたトークンを使用していない場合にのみ表示されます。

   資格情報ページで:

   - ファイルアップロードにプロキシサーバーを使用したい場合は、**プロキシの構成**をクリックします。Scoutにブラウザのインターネットプロパティに設定されているプロキシ設定を使用するように指示できます。または、プロキシサーバーのIPアドレスとポート番号を入力することもできます。プロキシダイアログボックスを閉じます。
   - Citrix Cloudアカウントの場合、**トークンの生成**をクリックします。デフォルトのブラウザがCitrix Cloudページに起動し、トークンが表示されます。トークンをコピーし、Scoutページに貼り付けます。
   - Citrixアカウントの場合、資格情報を入力します。

   完了したら、「**続行**」をクリックします。
6. アップロードに関する情報を入力します。

   - 名前フィールドには、収集された診断ファイルのデフォルト名が含まれています。ほとんどのコレクションではこれで十分ですが、名前を変更することもできます。(デフォルト名を削除して名前フィールドを空のままにすると、デフォルト名が使用されます。)
   - 必要に応じて、8桁のCitrixサポートケース番号を指定します。
   - オプションの「**説明**」フィールドに、問題について説明し、該当する場合は問題が発生した時期を示します。

   完了したら、「**アップロードの開始**」をクリックします。

   アップロード中、ページの左下部分にアップロードの完了率が概算で表示されます。進行中のアップロードをキャンセルするには、「**アップロードの停止**」をクリックします。

アップロードが完了すると、その場所のURLが表示され、リンクされます。リンクをたどってCitrixの場所にアクセスし、アップロードの分析を表示したり、リンクをコピーしたりできます。

「**完了**」をクリックして、Scoutの開始ページに戻ります。

トレースと再現

「**トレースと再現**」手順は、マシンの選択、トレースの開始、問題の再現、診断コレクションの完了、そしてファイルをCitrixにアップロードするかローカルに保存することから構成されます。

この手順は標準の「**収集**」手順に似ています。ただし、マシンでトレースを開始し、それらのマシンで問題を再作成することができます。すべての診断コレクションにはAOTトレース情報が含まれています。この手順では、トラブルシューティングに役立つCDFトレースが追加されます。

1. Scoutを起動します。マシンの「**スタート**」メニューから「**Citrix > Citrix Scout**」を選択します。開始ページで、「**トレースと再現**」をクリックします。
2. マシンを選択します。「**マシンの選択**」ページには、サイト内のすべてのVDAとControllerが一覧表示されます。マシン名で表示をフィルタリングできます。トレースと診断を収集する各マシンの横にあるチェックボックスをオンにします。次に、「**続行**」をクリックします。

   その他のマシンを手動で追加するには (StoreFrontまたはCitrix Provisioningサーバーなど)、マシンを手動で追加するを参照してください。

   Scout は、選択された各マシンで検証テストを自動的に起動し、検証テスト に記載されている基準を満たしていることを確認します。マシンの検証が失敗した場合、**Status** 列にメッセージが投稿され、そのマシンのチェックボックスは選択解除されます。次のいずれかを実行できます。

   - 問題を解決してから、そのマシンのチェックボックスを再度選択します。これにより、検証テストが再試行されます。
   - そのマシンをスキップします（チェックボックスは選択解除のままにします）。そのマシンからは診断情報とトレースは収集されません。

   検証テストが完了したら、**Continue** をクリックします。
3. トレースを開始します。概要には、トレースが収集されるすべてのマシンが一覧表示されます。**Start Tracing** をクリックします。

   選択したマシンのいずれかまたは複数で、発生した問題を再現します。その間、トレースの収集は続行されます。問題の再現が完了したら、Scout で **Continue** をクリックします。これによりトレースが停止します。

トレースを停止した後、トレース中に問題を再現したかどうかを示します。

4. マシンから診断情報を収集します。**Start Collecting** をクリックします。収集中に：

   - **Status** 列には、マシンの現在の収集状態が表示されます。
   - 単一マシンで進行中の収集を停止するには、そのマシンの **Action** 列にある **Cancel** をクリックします。
   - 進行中のすべての収集を停止するには、ページの右下隅にある **Stop Collection** をクリックします。収集が完了したマシンからの診断情報は保持されます。収集を再開するには、各マシンの **Action** 列にある **Retry** をクリックします。
   - 選択したすべてのマシンで収集が完了すると、右下隅の **Stop Collection** ボタンが **Continue** に変わります。
   - マシンから診断情報を再度収集するには、そのマシンの **Action** 列にある **Collect Again** をクリックします。新しい収集は以前のものを上書きします。
   - 収集が失敗した場合、**Action** 列にある **Retry** をクリックできます。正常に収集されたもののみがアップロードまたは保存されます。
   - 選択したすべてのマシンで収集が完了したら、**Back** をクリックしないでください。（クリックすると、収集は失われます。）

   収集が完了したら、**続行**をクリックします。

5. コレクションを保存またはアップロードします。ファイルをCitrixにアップロードするか、ローカルに保存するかを選択します。

   今すぐファイルをアップロードする場合は、手順6に進みます。

   ファイルをローカルに保存する場合:

   - Windowsの保存ダイアログボックスが表示されます。目的の場所を選択します。
   - ローカル保存が完了すると、ファイルのパス名が表示され、リンクされます。ファイルを表示できます。注意: ファイルは後でCitrixからアップロードできます。Citrix Insight Servicesについては、CTX136396を参照してください。

   完了をクリックしてScoutの開始ページに戻ります。この手順でこれ以上完了する必要のある手順はありません。

6. アップロードの認証を行い、必要に応じてプロキシを指定します。このプロセスの詳細については、アップロードの承認を参照してください。

   - Scoutを介して認証していない場合は、この手順に進みます。

- Scoutを介して認証した場合、保存されている認証トークンがデフォルトで使用されます。この操作を行う場合は、このオプションを選択して**続行**をクリックします。このコレクションの資格情報は要求されません。手順7に進みます。
- 以前に認証済みで、再認証して新しいトークンを取得したい場合は、**変更/再認証**をクリックしてこの手順に進みます。

アップロードを認証するために、Citrix資格情報を使用するか、Citrix Cloud資格情報を使用するかを選択します。**続行**をクリックします。資格情報ページは、保存されたトークンを使用していない場合にのみ表示されます。

資格情報ページで:

- ファイルアップロードにプロキシサーバーを使用する場合は、**プロキシの構成**をクリックします。Scoutに、ブラウザーのインターネットプロパティで構成されているプロキシ設定を使用するように指示できます。または、プロキシサーバーのIPアドレスとポート番号を入力することもできます。プロキシダイアログボックスを閉じます。
- Citrix Cloudアカウントの場合、**トークンの生成**をクリックします。デフォルトのブラウザーがCitrix Cloudページを起動し、トークンが表示されます。トークンをコピーし、Scoutページに貼り付けます。
- Citrixアカウントの場合は、資格情報を入力します。

完了したら、**続行**をクリックします。

7. アップロードに関する情報を提供します。

アップロードの詳細を入力します。

- 名前フィールドには、収集された診断ファイルのデフォルト名が含まれています。ほとんどの収集ではこれで十分ですが、名前を変更することもできます。(デフォルト名を削除して名前フィールドを空のままにした場合、デフォルト名が使用されます。)
- オプションで、8桁のCitrixサポートケース番号を指定します。
- オプションの「説明」フィールドに、問題について説明し、該当する場合は問題が発生した時期を示します。

完了したら、**アップロードの開始**をクリックします。

アップロード中、ページの左下部分にアップロードの完了率が概算で表示されます。進行中のアップロードをキャンセルするには、**アップロードの停止**をクリックします。

アップロードが完了すると、その場所のURLが表示され、リンクされます。リンクをたどってCitrixの場所に移動し、アップロードの分析を表示したり、リンクをコピーしたりできます。

完了をクリックして、Scoutの開始ページに戻ります。

追加のログ収集を有効にする

追加のログ収集を有効にする機能を使用すると、perfmon、Netsh、DebugView、Wiresharkなどのツールでトレースおよび再現機能を使用できます。

> **注：**
>
> これはローカルマシンにのみ適用されます。

> 追加のログ収集を設定するには：

1. Citrix Scout を起動します。
2. **設定**ギアをクリックします。
3. **追加ツールによるログ収集を有効にする**をクリックします。
4. 「**保存**」をクリックします。

追加のログを収集するには：

1. Scout のホームページで、**トレースと再現**をクリックします。
2. **マシンの選択**ページで、ローカルマシンの右側にあるギアをクリックします。
3. **ログ記録に必要なツールの選択**ページで、**ツールのダウンロード**をクリックします。
4. **ツールのダウンロード**ページで、使用したいツールを選択し、**ダウンロード**をクリックします。Wireshark を除くツールがダウンロードされます。Wireshark は手動でのみダウンロードおよびインストールできます。 注：他のツールを手動でダウンロードすることを選択した場合、ダウンロードした .zip ファイルの内容を `C:\ProgramData\Citrix\TelemetryService\CDC\Lib\Resources\Tools\<toolname>` に抽出する必要があります。たとえば、DebugView.zip ファイルをダウンロードした場合、そのファイルの内容を `C:\ProgramData\Citrix\TelemetryService\CDC\Lib\Resources\Tools\DebugView\` に解凍します。
5. **ログ記録に必要なツールの選択**ページで、**ステータスの更新**をクリックします。選択したすべてのツールが、ステータス列の下に**存在**として表示されます。
6. ログ記録用のツールを選択し、**次へ**をクリックします。
7. トレースと再現 の手順に従います。

8. 完了後、zip ファイル内のログを確認します。ログは *CDCLogs* フォルダーに圧縮されています。

> **注：**
>
> トレースに Procmon ツールが選択されている場合、Process Monitor のログはすぐに大きくなる可能性があります。必要なツールのみを選択するようにしてください。ログのサイズは *%temp%\Scout-CDC-Log* で監視することもできます。

コレクションのスケジュール設定

> **注：**
>
> 現在、コレクションはスケジュールできますが、ヘルスチェックはできません。

スケジュール手順は、マシンを選択し、スケジュールを設定またはキャンセルすることで構成されます。スケジュールされたコレクションは、Citrixに自動的にアップロードされます。(PowerShellインターフェイスを使用して、スケジュールされたコレクションをローカルに保存できます。(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/manage-deployment/cis.html#citrix-call-home)を参照してください。)

1. Scoutを起動します。マシンのスタートメニューから、**Citrix > Citrix Scout**を選択します。開いたページで、**Schedule**をクリックします。
2. マシンを選択します。サイト内のすべてのVDAとコントローラーが一覧表示されます。マシン名で表示をフィルターできます。

   グラフィカルインターフェイスを使用してVDAとコントローラーをインストールしたときに、Call Homeスケジュールを設定した場合 ((/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/manage-deployment/cis.html#citrix-call-home)を参照)、Scoutはデフォルトでそれらの設定を表示します。このバージョンのScoutを使用して、スケジュールされたコレクションを初めて開始したり、以前に構成したスケジュールを変更したりできます。

   コンポーネントのインストール中にマシンごとにCall Homeを有効/無効にした場合でも、Scoutで構成されたスケジュールは、選択したすべてのマシンに影響します。

   診断情報を収集する各マシンの横にあるチェックボックスをオンにして、**Continue**をクリックします。

その他のマシン (StoreFrontサーバーやCitrix Provisioningサーバーなど) を手動で追加するには、(#add-machines-manually)を参照してください。

Scoutは、選択した各マシンで検証テストを自動的に起動し、(#verification-tests)の基準を満たしていることを確認します。マシンの検証が失敗した場合、**Status**列にメッセージが表示され、そのマシンのチェックボックスはオフになります。次のいずれかを実行できます。

- 問題を解決してから、そのマシンのチェックボックスを再度オンにします。これにより、検証テストが再試行されます。
- そのマシンをスキップします (チェックボックスをオフのままにします)。そのマシンからは診断情報 (またはトレース) は収集されません。

検証テストが完了したら、**Continue**をクリックします。

概要ページには、スケジュールが適用されるマシンが一覧表示されます。**Continue**をクリックします。

3. スケジュールを設定します。診断情報を収集するタイミングを指定します。注意：スケジュールは、選択したすべてのマシンに影響します。

   - 選択したマシンに週次スケジュールを構成するには、**Weekly**をクリックします。曜日を選択します。コレクションを開始する時刻 (24時間形式) を入力します。
   - 選択したマシンに日次スケジュールを構成するには、**Daily**をクリックします。コレクションを開始する時刻 (24時間形式) を入力します。
   - 選択したマシンに対する既存のスケジュールをキャンセルし（別のスケジュールに置き換えない）、 をクリックします。これにより、それらのマシンに対して以前に構成されていたスケジュールがすべてキャンセルされます。

   続行をクリックします。

4. アップロードの認証を行い、必要に応じてプロキシを指定します。このプロセスの詳細については、アップロード認証 を参照してください。注意：Scout スケジュールを使用している場合、保存されたトークンを使用して認証することはできません。

   アップロードの認証に Citrix 資格情報を使用するか、Citrix Cloud 資格情報を使用するかを選択します。 をクリックします。

   資格情報ページで：

   - ファイルのアップロードにプロキシサーバーを使用する場合は、 をクリックします。Scout に、ブラウザーのインターネットプロパティで構成されているプロキシ設定を使用

するように指示できます。または、プロキシサーバーの IP アドレスとポート番号を入力することもできます。プロキシダイアログボックスを閉じます。

- Citrix Cloud アカウントの場合は、 をクリックします。デフォルトのブラウザーが Citrix Cloud ページに起動し、トークンが表示されます。トークンをコピーし、Scout ページに貼り付けます。
- Citrix アカウントの場合は、資格情報を入力します。

完了したら、 をクリックします。

構成されたスケジュールを確認します。 をクリックして Scout の開始ページに戻ります。

コレクション中、選択された各マシンの Windows アプリケーションログには、コレクションとアップロードに関するエントリが含まれます。

データマスキング

Citrix Scout を使用して収集された診断情報には、セキュリティ上機密性の高い情報が含まれる場合があります。Citrix Scout のデータマスキング機能を使用すると、診断ファイルを Citrix にアップロードする前に、機密データをマスクできます。

Scout のデータマスキングは、IP アドレス、マシン名、ドメイン名、ユーザー名、ハイパーバイザー名、デリバリーグループ名、カタログ名、アプリケーション名、および SID をマスクするように構成されています。

> **注：**

> CDF トレースは暗号化されており、マスクできません。

> Linux VDA ログは `.tar.gz2` 形式に圧縮されており、マスクできません。

新しい診断情報を収集し、データマスキングを実行する

Citrix Scoutのデータマスキング機能を使用するには、コマンドラインからScoutを起動します。

1. Windowsで、コマンドプロンプトを管理者として開きます。
2. Scoutがインストールされているディレクトリに移動します: `cd C:\Program Files\Citrix\Telemetry Service`。
3. Scoutを起動します: `ScoutUI.exe datamasking`。
4. 診断情報を収集するには、**Collect** または **Trace & Reproduce** をクリックします。

5. 収集が完了したら、**Enable data masking** を選択します。このオプションはデフォルトで有効になっています。
6. データマスクを構成します。デフォルトのルールを使用することも、ルールをカスタマイズすることもできます。
7. 診断情報コレクションをアップロードするか保存するかを選択します。

    - **Upload the diagnostics collection to Citrix** を選択すると、マスクされた診断ファイルがCitrixにアップロードされます。
    - **Save the diagnostics collection on your local machine** を選択すると、元の診断情報とマスクされた診断情報の両方が指定された場所に保存されます。

既存の診断情報に対してデータマスキングを実行する

1. Windowsで、コマンドプロンプトを管理者として開きます。
2. Scoutがインストールされているディレクトリに移動します: `cd C:\Program Files\Citrix\Telemetry Service`。
3. データマスキングモードでScoutを直接起動します: `ScoutUI.exe datamasking filePath`。
4. 「データマスキングを有効にする」を選択して続行します。このオプションはデフォルトで有効になっています。
5. データマスクを構成します。デフォルトのルールでデータマスキングを実行することも、ルールをカスタマイズすることもできます。
6. 診断コレクションをアップロードするか保存するかを選択します。

    - **診断コレクションをCitrixにアップロード**を選択した場合、マスクされた診断ファイルがCitrixにアップロードされます。
    - **診断コレクションをローカルマシンに保存**を選択した場合、元の診断とマスクされた診断の両方が指定された場所に保存されます。

マスクされたデータファイルとマッピングファイルの場所

診断コレクションをアップロードまたは保存した後、リンクをクリックして元の診断とマスクされた診断を開き、マッピング情報ファイルを開きます。

使用状況データ収集

Scoutを使用すると、CitrixはGoogle Analyticsを使用して匿名の使用状況データを収集し、将来の製品機能と改善に役立てます。データ収集はデフォルトで有効になっています。

使用状況データの収集とアップロードを変更するには、Scout UIの**設定**アイコンをクリックします。その後、**はい**または**いいえ**を選択し、**保存**をクリックして情報を送信するかどうかを選択できます。

Scoutの使用状況データ収集(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/scout-usage.png)

Call Home の主要データポイント

Call Home は、以下の主要データポイントを収集します。

(M) = 手動収集時のみ取得 (PowerShell コマンドレット `Start-CitrixCallHomeUpload`)

ファイル名	カテゴリ	データグループ
		マシン
		エックスディーサイト
		サイト情報
		ブローカーDB情報 (M)
		インストールされているDBバージョン (M)
		ブローカーサービスステータス (M)
		登録済みサービスインスタンス (M)
		ブローカーライセンステスト (M)
		アクティブなHDX™セッション (M)
		ブローカー管理者
		ブローカー管理者権限

		RDS構成 (LicensingSettings、SessionSettings、SpecifiedLicenseServers、および RegisteredLicenseServersを含む)
		監視サービス (M) (MonitorConfiguration、MonitorDataStore、MonitorDBConnection、MonitorDBSchemaVersion、MonitorService、MonitorServiceAddedCapability、MonitorServiceInstance、MonitorServiceStatus、およびMonitorInstalledDBVersionを含む)
		構成ログ
		接続ログ
		ハイパーバイザー接続 (M)
		ブローカーハイパーバイザー接続
		ハイパーバイザーアラート
		カタログ
		マルチセッションOSエージェント (M)
		シングルセッションOSエージェント (M)
		公開アプリケーション
		デリバリー グループ

		構成済みデリバリーエージェント

		Citrixインストール済みコンポーネント
		Citrix Brokerサービス情報
		ブローカーサービス構成ファイル
		Machine Creation Services™ 構成ファイル
		ホストサービス構成ファイル
		AD IDサービス構成ファイル
		構成サービス構成ファイル
		構成ログサービス構成ファイル
		委任管理サービス構成ファイル
		環境テストサービス構成ファイル
		監視サービス構成ファイル
		Storefront™ サービス構成ファイル
		ワークステーションエージェント構成ファイル
		Citrix VDA情報
		Citrix XD ホットフィックス
		Citrix_VirtualChannel_Graphics_Enum

		Citrix_VirtualChannel_Flash_Enum
		Citrix_VirtualChannel_Printer_Enum

		コンピューター
		BIOS
		メモリ情報
		プロセッサ
		PNP デバイス
		デバイス
		ディスクドライブ
		論理ドライブ
		ページファイル使用状況
		ネットワークアダプター
		ネットワークアダプター構成
		ipConfig
		ビデオコントローラー
		IDE コントローラー
		SCSI コントローラー

		HKLM:\Software\Wow6432Node\Citrix

		HKLM: \System\CurrentControlSet\Control\Citrix
		HKLM: \SOFTWARE\Policies\Citrix
		HKLM: \Software\Microsoft\Cryptography
		HKLM: \Software\Wow6432Node\Microsoft\Cryptography
		HKLM: \Software\Microsoft\Windows NT\CurrentVersion\Windows
		HKLM: \Software\Microsoft\Windows NT\CurrentVersion\Winlogon
		HKLM: \Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
		HKLM: \Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer
		HKLM: \SYSTEM\CurrentControlSet\Control\Print\Environments
		HKLM: \System\CurrentControlSet\Control\Session Manager

		HKLM:\System\CurrentControlSet\Control\Terminal Server
		HKCU:\Control Panel\Desktop
		HKLM:\SOFTWARE\Classes\ShockwaveFlash.ShockwaveFlash\CurVer
		HKLM:\SYSTEM\CurrentControlSet\Control\SystemInformation
		HKLM:\SYSTEM\CurrentControlSet\Control\FileSystem
		HKLM:\SYSTEM\CurrentControlSet\Control\Windows
		HKLM:\SYSTEM\CurrentControlSet\Control\TimeZoneInformation

		ドライバー
		EnvVariables
		OS
		プロセス
		サービス
		サービスパック
		ジーピーリザルト
		Microsoft ホットフィックス

		ネットスタット
		PNP ドライバー

		システムイベントログ
		AOT (常時オンのトレース)
		クラッシュダンプ

		アップタイム
		メモリ
		コンピューターシステム
		プロセッサ
		ビデオコントローラー
		ディスクドライブ
		ブラウザ情報
		再起動回数
		メモリ使用量
		ディスク使用量
		ICAセッション解像度
		ICAカラー深度
		メタインストーラーCEIPマシンID

		ストア数
		サーバーグループ内のサーバー数

		ストアあたりのDelivery Controller™数
		HTTPS有効
		Citrix Receiver™のクラシックエクスペリエンスが有効
		Citrix レシーバー 用の HTML5 レシーバー設定
		Citrix Receiver向けワークスペースコントロールの有効化
		ストア向けリモートアクセスの有効化
		ゲートウェイ数
		統合されたNetScaler®認証用の明示的なJSONサービス

モニター

管理者とヘルプデスク担当者は、さまざまな機能とツールを使用してCitrix Virtual Apps and Desktops™サイトを監視できます。これらのツールを使用すると、以下を監視できます。

- ユーザーセッションとセッションの使用状況
- ログオンパフォーマンス
- 接続とマシン（障害を含む）
- 負荷評価
- 履歴トレンド
- インフラストラクチャ

Citrix Director (シトリックス ディレクター)

Directorは、監視とトラブルシューティング、およびエンドユーザーのサポートタスクの実行に使用できるリアルタイムのWebツールです。

詳細については、Director の記事を参照してください。

構成ログ

構成ログを使用すると、管理者はサイトへの管理変更を追跡できます。構成ログは、構成変更が行われた後の問題の診断とトラブルシューティング、変更管理と構成の追跡を支援し、管理アクティビティを報告するのに役立ちます。

Studioからログに記録された情報を表示し、レポートを生成できます。また、Directorでトレンドビューを使用して、構成変更の通知を提供するためにログに記録された項目を表示することもできます。この機能は、Studioにアクセスできない管理者にとって役立ちます。

トレンドビューは、一定期間にわたる構成変更の履歴データを提供するため、管理者は、サイトに対してどのような変更がいつ誰によって行われたかを評価し、問題の原因を特定できます。このビューは、構成情報を次の3つのカテゴリに分類します。

- 接続障害
- 失敗したシングルセッションマシン

- 失敗したマルチセッションマシン

構成ログを有効にして構成する方法の詳細については、構成ログを参照してください。Directorの記事では、そのツールからログに記録された情報を表示する方法について説明しています。

イベントログ

Services within Citrix Virtual Apps and Desktops log events that occur. Event logs are used to monitor and troubleshoot operations.

詳細については、イベントログを参照してください。個々の機能の記事にもイベント情報が含まれている場合があります。

構成ログ

構成ログは、サイト構成の変更と管理アクティビティをデータベースにキャプチャする機能です。この機能はデフォルトで有効になっています。ログに記録されたコンテンツは、次の目的で使用できます。

- 構成変更後、問題の診断とトラブルシューティングを行います。ログは追跡記録を提供します。
- 変更管理の支援と構成の追跡。
- 管理アクティビティを報告します。

Citrix Studioから、構成ログ設定の指定、構成ログの表示、HTMLおよびCSVレポートの生成を行うことができます。構成ログの表示は、日付範囲や全文検索結果でフィルタリングできます。強制ログが有効になっている場合、ログに記録できない構成変更は行えません。適切な権限があれば、構成ログからエントリを削除できます。構成ログ機能を使用してログコンテンツを編集することはできません。

構成ログは、PowerShell SDKと構成ログサービスを使用します。構成ログサービスは、サイト内のすべてのControllerで実行されます。いずれかのControllerが失敗した場合、別のControllerのサービスが自動的にログ要求を処理します。

デフォルトでは、構成ログ機能は有効になっており、サイト作成時に作成されるデータベース（サイト構成データベース）を使用します。データベースの別の場所を指定できます。構成ログデータベースは、サイト構成データベースと同じ高可用性機能をサポートしています。

構成ログへのアクセスは、委任管理を通じて、「ログ設定の編集」および「構成ログの表示」の権限で制御されます。

構成ログは作成時にローカライズされます。たとえば、英語で作成されたログは、リーダーのロケールに関係なく、英語で読み取られます。

ログに記録される内容

Studio、Director、およびPowerShellスクリプトから開始された構成変更と管理アクティビティがログに記録されます。ログに記録される構成変更の例には、以下に関する作業（作成、編集、削除、割り当て）が含まれます。

- マシンカタログ
- デリバリーグループ（電源管理設定の変更を含む）
- 管理者ロールとスコープ
- ホストリソースと接続
- Studioを介したCitrixポリシー

ログに記録される管理変更の例には、以下が含まれます。

- 仮想マシンまたはユーザーデスクトップの電源管理
- StudioまたはDirectorがユーザーにメッセージを送信する

次の操作はログに記録されません。

- プール管理による仮想マシンの電源投入などの自律的な操作。
- グループポリシー管理コンソール (GPMC) を介して実装されたポリシーアクション。これらのアクションのログを表示するには、Microsoftツールを使用してください。
- レジストリ、データベースへの直接アクセス、またはStudio、Director、PowerShell以外のソースを通じて行われた変更。
- 展開が初期化されると、最初の構成ログサービスインスタンスが構成サービスに登録されたときに、構成ログが利用可能になります。したがって、構成の初期段階（たとえば、データベーススキーマが取得および適用されるとき、ハイパーバイザーが初期化されるとき）はログに記録されません。

構成ログの管理

デフォルトでは、構成ログはサイトの作成時に作成されるデータベース（サイト構成データベースとも呼ばれます）を使用します。Citrixは、次の理由により、構成ログデータベース（および監視データベース）に別の場所を使用することを推奨します。

- 構成ログデータベースのバックアップ戦略は、サイト構成データベースのバックアップ戦略とは異なる可能性があります。
- 構成ログ（および監視サービス）のために収集されるデータ量によって、サイト構成データベースで利用可能な領域に悪影響が及ぶ可能性があります。
- これにより、3つのデータベースの単一障害点が分割されます。

構成ログをサポートしない製品エディションには、Studioにログノードがありません。

構成ログと強制ログの有効化と無効化

デフォルトでは、構成ログは有効になっており、強制ログは無効になっています。

1. Studioナビゲーションペインで**Logging**を選択します。
2. Actionsペインで**Preferences**を選択します。構成ログダイアログボックスには、データベース情報が含まれており、構成ログと必須ログが有効か無効かを示します。
3. 希望するアクションを選択します。

   構成ログを有効にするには、**Enable** を選択します。これはデフォルト設定です。データベースに書き込みができない場合、ログ情報は破棄されますが、操作は続行されます。

   構成ログを無効にするには、**Disable** を選択します。以前にログが有効になっていた場合、既存のログはPowerShell SDKで読み取り可能です。

   強制ログを有効にするには、**Prevent changes to the site configuration when the database is not available** を選択します。通常ログに記録される構成変更や管理アクティビティは、構成ログデータベースに書き込みが可能な場合にのみ許可されます。強制ログは、構成ログが有効になっている場合（**Enable** が選択されている場合）にのみ有効にできます。構成ログサービスが失敗し、高可用性が使用されていない場合、強制ログが有効であると見なされます。そのような場合、通常ログに記録される操作は実行されません。

   強制ログを無効にするには、**Allow changes when to the site configuration when the database is not available** を選択します。構成ログデータベースにアクセスできない場合でも、構成変更と管理アクティビティが許可されます。これはデフォルト設定です。

構成ログデータベースの場所を変更する

強制ログが有効になっている場合、データベースの場所を変更することはできません。場所の変更には、ログに記録できない短い切断期間が含まれるためです。

1. サポートされているSQL Serverバージョンを使用して、データベースサーバーを作成します。
2. Studioナビゲーションペインで**Logging**を選択します。

3. ActionsペインでPreferencesを選択します。
4. ログ設定ダイアログボックスで、**Change logging database** を選択します。
5. ログデータベースの変更ダイアログボックスで、新しいデータベースサーバーを含むサーバーの場所を指定します。有効な形式については、データベースアドレス形式を参照してください。
6. Studio がデータベースを作成できるようにするには、**OK** をクリックします。プロンプトが表示されたら **OK** をクリックすると、データベースが自動的に作成されます。Studio は、現在のStudioユーザーの資格情報を使用してデータベースにアクセスしようとします。それが失敗した場合、データベースユーザーの資格情報の入力を求められます。その後、Studio はデータベーススキーマをデータベースにアップロードします。（資格情報はデータベース作成中のみ保持されます。）
7. データベースを手動で作成するには、**データベーススクリプトの生成**をクリックします。生成されたスクリプトには、データベースを手動で作成するための手順が含まれています。スキーマをアップロードする前に、データベースが空であり、少なくとも1人のユーザーがデータベースにアクセスして変更する権限を持っていることを確認してください。

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

構成ログコンテンツの表示

構成の変更や管理アクティビティを開始すると、StudioとDirectorによって作成された上位レベルの操作が、Studioの上部中央ペインに一覧表示されます。上位レベルの操作は、1つ以上のサービスおよびSDK呼び出し（下位レベルの操作）をもたらします。上部ペインで上位レベルの操作を選択すると、下部ペインに下位レベルの操作が表示されます。

操作が完了する前に失敗した場合、ログ操作がデータベースで完了しないことがあります。たとえば、開始レコードに対応する停止レコードがない場合があります。このような場合、ログには情報が不足していることが示されます。時間範囲に基づいてログを表示すると、ログ内のデータが条件と一致する場合、不完全なログが表示されます。たとえば、過去5日間のすべてのログが要求され、過去5日間に開始時刻があるが終了時刻がないログが存在する場合、それは含まれます。

PowerShellコマンドレットを呼び出すスクリプトを使用する場合、親の上位レベルの操作を指定せずに下位レベルの操作を作成すると、構成ログは代替の上位レベルの操作を作成します。

構成ログコンテンツを表示するには、Studioナビゲーションペインで**Logging**を選択します。デフォルトでは、中央ペインにログコンテンツが日付ごとに区切られ、時系列順（最新のエントリが最初）に一覧表示されます。次のことができます。

- 列見出しで表示を並べ替えます。
- 日付間隔を指定するか、**Search**ボックスにテキストを入力して表示をフィルターします。検索を使用した後に標準表示に戻るには、**Search**ボックスのテキストをクリアします。

レポートを生成する

構成ログデータを含むCSVおよびHTMLレポートを生成できます。

- CSVレポートには、指定された時間間隔のすべてのログデータが含まれます。データベース内の階層データは、単一のCSVテーブルにフラット化されます。データのどの側面もファイル内で優先されません。書式設定は使用されず、人間が読み取れることは想定されていません。ファイル（MyReportという名前）には、普遍的に利用可能な形式でデータが含まれています。CSVファイルは、データのアーカイブや、Microsoft Excelなどのレポート作成ツールまたはデータ操作ツールのデータソースとしてよく使用されます。
- HTMLレポートは、指定された時間間隔のログデータを人間が読み取れる形式で提供します。変更を確認するための構造化されたナビゲート可能なビューを提供します。HTMLレポートは、SummaryとDetailsという名前の2つのファイルで構成されます。Summaryには、各操作がいつ、誰によって、どのような結果になったかなど、高レベルの操作が一覧表示されます。各操作の横にある**Details**リンクをクリックすると、Detailsファイル内の低レベルの操作に移動し、追加情報が表示されます。

構成ログレポートを生成するには、Studioナビゲーションペインで**Logging**を選択し、Actionsペインで**Create custom report**を選択します。

- レポートの日付範囲を選択します。
- レポート形式（CSV、HTML、またはその両方）を選択します。
- レポートを保存する場所を参照します。

構成ログコンテンツを削除する

構成ログを削除するには、特定の委任管理権限とSQL Serverデータベース権限が必要です。

- **委任管理:** 展開構成の読み取りを許可する委任管理ロールが必要です。完全管理者ロールにはこの権限があります。カスタムロールには、カテゴリでまたはが選択されている必要があります。

構成ログデータを削除する前にバックアップを作成するには、カスタムロールのカテゴリでまたはが選択されている必要もあります。

- **SQL Serverデータベース:** データベースからレコードを削除する権限を持つSQL Serverログインが必要です。これには2つの方法があります。
  - データベースサーバー上のあらゆるアクティビティを実行できるsysadminサーバーロールを持つSQL Serverデータベースログインを使用します。または、`serveradmin`または`setupadmin`サーバーロールを使用すると、削除操作を実行できます。
  - 展開でより高いセキュリティが必要な場合は、データベースからレコードを削除する権限を持つデータベースユーザーにマッピングされた非sysadminデータベースログインを使用します。
    a. SQL Server Management Studioで、「sysadmin」以外のサーバーロールを持つSQL Serverログインを作成します。
    b. ログインをデータベース内のユーザーにマッピングします。SQL Serverは、ログインと同じ名前のユーザーをデータベース内に自動的に作成します。
    c. データベースロールメンバーシップで、データベースユーザーのロールメンバーのうち少なくとも1つを指定します: `ConfigurationLoggingSchema_ROLE` または`dbowner`。

    詳細については、SQL Server Management Studioのドキュメントを参照してください。

構成ログを削除するには:

1. Studioナビゲーションペインで**Logging**を選択します。
2. Actionsペインで**Delete logs**を選択します。
3. ログを削除する前にバックアップを作成するかどうかを尋ねられます。バックアップを作成することを選択した場合、バックアップアーカイブが保存される場所を参照します。バックアップはCSVファイルとして作成されます。

構成ログがクリアされた後、ログの削除は空のログに投稿される最初のアクティビティです。そのエントリには、誰がいつログを削除したかに関する詳細が記載されています。

イベントログ

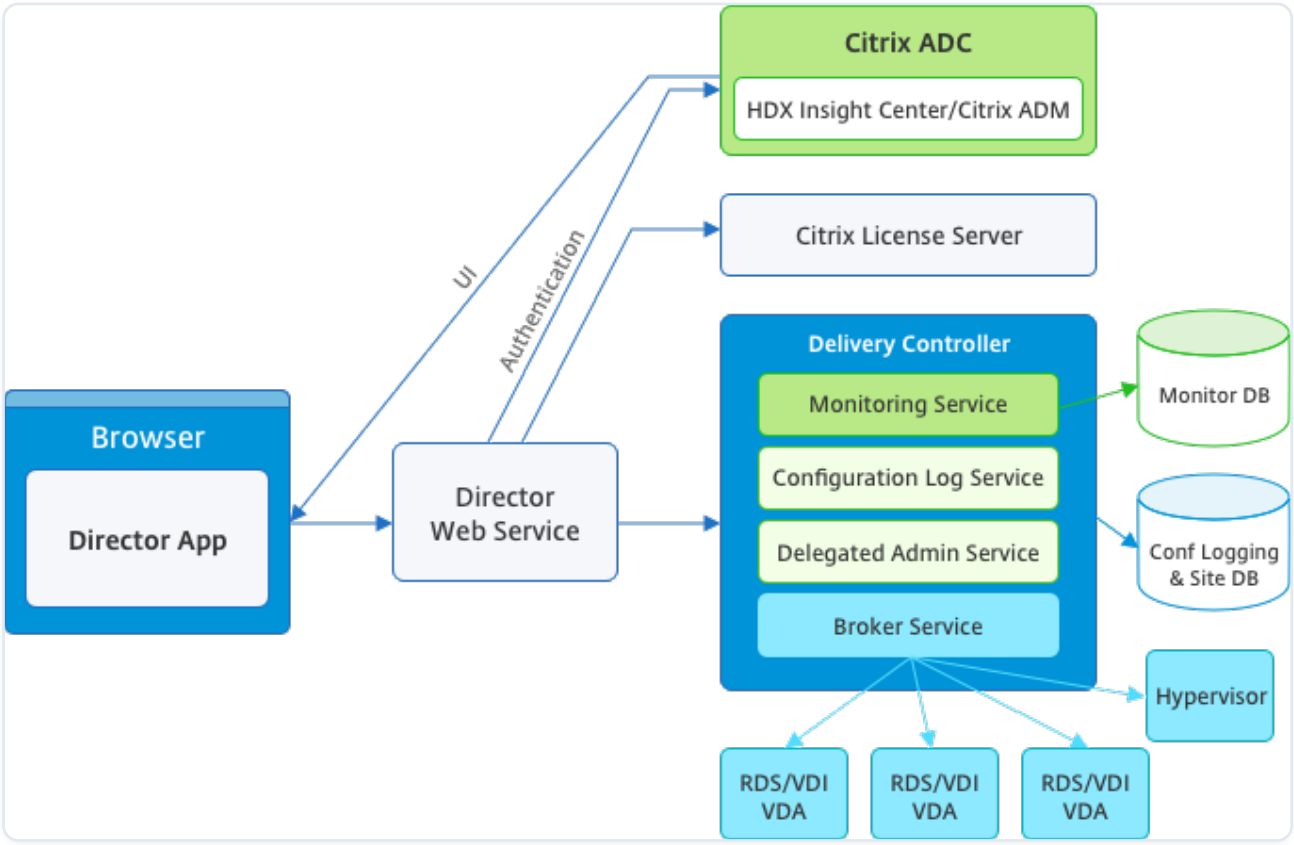
以下の記事では、Citrix Virtual Apps and Desktops 内のサービスによってログに記録される可能性のあるイベントを一覧表示し、説明します。

この情報は網羅的ではありません。読者は、追加のイベント情報について、個々の機能記事を確認してください。

- Citrix Broker Service イベント
- Citrix FMA Service SDK イベント
- シトリックス コンフィギュレーションサービス イベント
- シトリックス デリゲート管理サービス イベント

ディレクター

ディレクターは、Citrix Virtual Apps and Desktops 用の監視およびトラブルシューティングコンソールです。



ディレクターは以下にアクセスできます:

- Analytics、Performance Manager、および Network Inspector と統合された統合コンソールを使用して、Broker Agent からリアルタイムデータにアクセスします。以下の分析はCitrix ADMによって提供され、Citrix Virtual Apps™ または Desktops 環境におけるネットワークに起因するボトルネックを特定します:
  - 健全性と容量の保証のためのパフォーマンス管理
  - 履歴トレンドとネットワーク分析
- Configuration Loggingデータベースにアクセスするために Monitorデータベースに保存されている履歴データ。
- Citrix ADM を使用してCitrix Gateway からのICA®データ。

- Citrix Virtual Apps または Desktops の仮想アプリケーション、デスクトップ、およびユーザーのエンドユーザーエクスペリエンスの可視性を得る。
- 効果的なトラブルシューティングのために、ネットワークデータをアプリケーションデータおよびリアルタイムメトリックと関連付ける。
- Citrix Virtual Desktop 7 Director監視ツールと統合する。

ディレクターは、Citrix Virtual Apps または Desktops Site のリアルタイムおよび履歴の健全性監視を提供するトラブルシューティングダッシュボードを使用します。この機能により、リアルタイムで障害を確認でき、エンドユーザーが何を経験しているかをよりよく把握できます。

Director機能とDelivery Controller (DC)、VDA、およびその他の依存コンポーネントとの互換性に関する詳細については、「機能互換性マトリックス」を参照してください。

> **注：**
>
> MeltdownおよびSpectreの投機的実行サイドチャネル脆弱性の開示に伴い、Citrixは、関連する緩和パッチをインストールすることを推奨します。これらのパッチはSQL Serverのパフォーマンスに影響を与える可能性があります。詳細については、Microsoftサポート記事「SpectreおよびMeltdownサイドチャネル脆弱性からのSQL Serverの保護」を参照してください。Citrixは、本番環境にパッチを展開する前に、規模をテストし、ワークロードを計画することを推奨します。

> Director は、デフォルトで Delivery Controller 上の Web サイトとしてインストールされます。前提条件およびその他の詳細については、このリリースの システム要件 ドキュメントを参照してください。Director のインストールと構成に関する具体的な情報については、Director のインストールと構成 を参照してください。

Director へのログオン

Director の Web サイトは、https または `http://<Server FQDN>/Director` にあります。

マルチサイト展開でいずれかのサイトがダウンしている場合、ダウンしているサイトへの接続を試行するため、ログオンに少し時間がかかります。

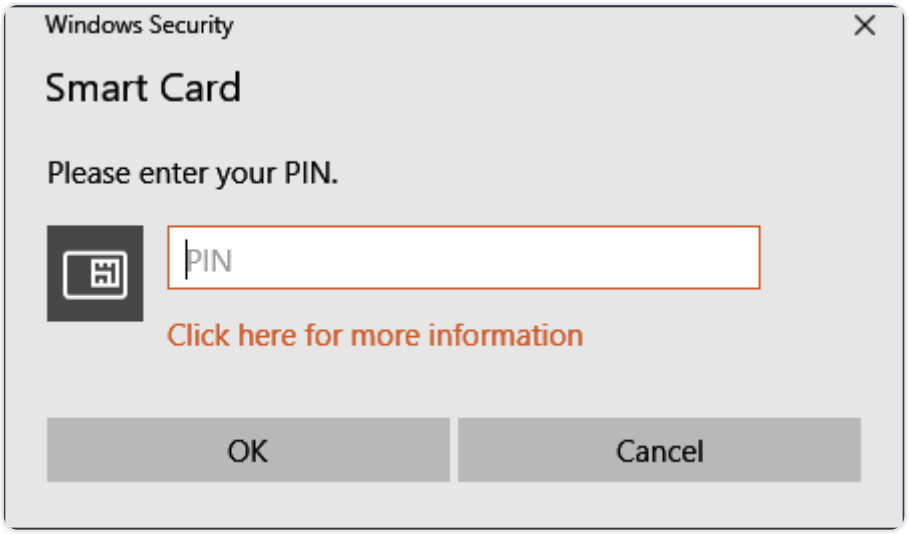
PIV スマートカード認証での Director の使用

Director は、Personal Identity Verification (PIV) ベースのスマートカード認証によるログオンをサポートするようになりました。この機能は、アクセス制御にスマートカードベースの認証を使用する組織や政府機関にとって有用です。 スマートカード認証には、Director サーバーおよび Active Directory での特定の構成が必要です。構成手順については、PIV スマートカード認証の構成 で詳しく説明されています。

> **注：**
>
> スマートカード認証は、同じ Active Directory ドメインのユーザーのみがサポートされます。

必要な構成を実行した後、スマートカードを使用して Director にログオンできます。

1. スマートカードをスマートカードリーダーに挿入します。
2. ブラウザーを開き、Director の URL `https://<directorfqdn>/Director` にアクセスします。
3. 表示されたリストから有効なユーザー証明書を選択します。
4. スマートカードトークンを入力します。



5. 認証されると、Director ログオンページで追加の資格情報を入力することなく Director にアクセスできます。

統合 Windows 認証での Director の使用

統合Windows認証（IWA）を使用すると、ドメイン参加ユーザーはDirectorログオンページで資格情報を再入力することなく、Directorに直接アクセスできます。統合Windows認証とDirectorを使用するための前提条件は次のとおりです。

- DirectorをホストするIIS Webサイトで統合Windows認証を有効にします。Directorをインストールすると、匿名認証とフォーム認証が有効になります。統合Windows認証とDirectorをサポートするには、匿名認証を無効にし、Windows認証を有効にします。ドメイン外のユーザーの認証のために、フォーム認証は有効のままにしておく必要があります。

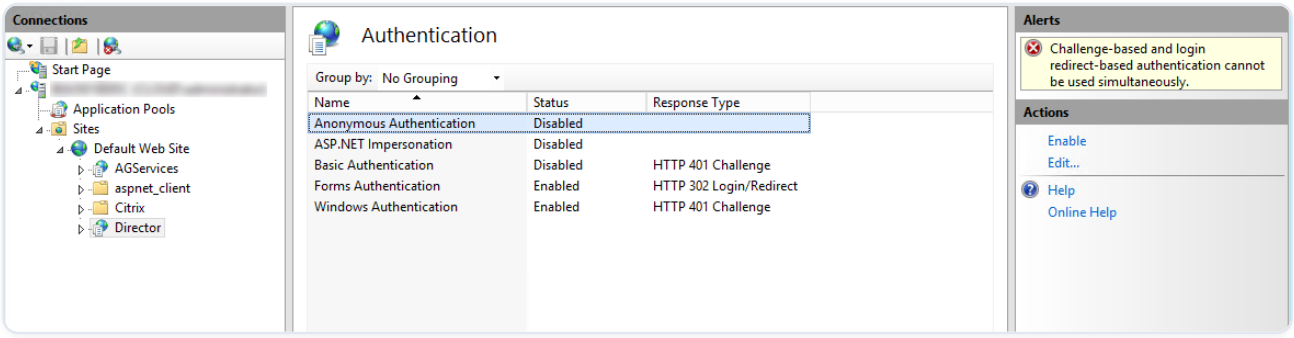
  a. IISマネージャーを起動します。

  b. **サイト** \> **既定のWebサイト** \> **Director**に移動します。

  c. **認証**を選択します。

  d. **匿名認証**を右クリックし、**無効**を選択します。

  e. **Windows認証**を右クリックし、**有効**を選択します。



- Directorマシンに対してActive Directoryの委任権限を構成します。構成が必要となるのは、DirectorとDelivery Controller™が別々のマシンにインストールされている場合のみです。

  a. Active Directoryマシンで、Active Directory管理コンソールを開きます。

  b. Active Directory管理コンソールで、**ドメイン名** \> **コンピューター**に移動します。Directorマシンを選択します。

  c. 右クリックして**プロパティ**を選択します。

  d. プロパティで、**委任**タブを選択します。

  e. **このコンピューターを、任意のサービスへの委任のために信頼する（Kerberosのみ）**オプションを選択します。

- Directorへのアクセスに使用するブラウザーは、統合Windows認証をサポートしている必要があります。FirefoxおよびChromeでは、追加の構成手順が必要になる場合があります。詳細については、ブラウザーのドキュメントを参照してください。

- 監視サービスは、Microsoft .NET Framework 4.5.1 以降の、Director のシステム要件に記載されているサポート対象バージョンを実行している必要があります。詳しくは、「」(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/system-requirements.html#citrix-director)を参照してください。

ユーザーがDirectorからログオフするか、セッションがタイムアウトすると、ログオンページが表示されます。ログオンページから、ユーザーは認証の種類を**自動ログオン**または**ユーザー資格情報**に設定できます。

インターフェイスビュー

Directorは、特定の管理者向けに調整されたさまざまなインターフェイスビューを提供します。製品の権限によって、表示される内容と利用可能なコマンドが決まります。

たとえば、ヘルプデスク管理者は、ヘルプデスクタスクに合わせて調整されたインターフェイスを表示します。Directorを使用すると、ヘルプデスク管理者は問題を報告しているユーザーを検索し、そのユーザーに関連付けられたアクティビティを表示できます。たとえば、ユーザーのアプリケーションとプロセスのステータスなどです。応答しないアプリケーションやプロセスを終了する、ユーザーのマシンでシャドウ操作を実行する、マシンを再起動する、ユーザープロファイルをリセットするなどのアクションを実行することで、問題を迅速に解決できます。

対照的に、完全な管理者はサイト全体を表示および管理し、複数のユーザーおよびマシンに対してコマンドを実行できます。ダッシュボードは、セッションのステータス、ユーザーログオン、サイトインフラストラクチャなど、展開の主要な側面を概観できます。情報は毎分更新されます。問題が発生した場合、発生した障害の数と種類に関する詳細が自動的に表示されます。

Directorにおけるさまざまな役割とその権限について詳しくは、「」(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/director/install-and-configure/permissions.html)を参照してください。

Google Analyticsによる使用状況データの収集

Director Serviceは、DirectorのインストールGoogle Analyticsを使用して使用状況データの収集を開始します。トレンドページの利用状況に関する統計情報と、OData API呼び出しの分析情報が収集されます。分析情報の収集は、Citrixプライバシーポリシーに準拠しています。Directorをインストールすると、データ収集はデフォルトで有効になります。

Google Analyticsのデータ収集をオプトアウトするには、Directorがインストールされているマシンでレジストリキーを編集します。レジストリキーが存在しない場合は、作成して目的の値に設定します。レジストリキーの値を変更した後、Directorインスタンスを更新してください。

注意：レジストリエディターを誤って使用すると、オペレーティングシステムの再インストールが必要になる深刻な問題が発生する可能性があります。Citrixは、レジストリエディターの誤用によって発生した問題が解決されることを保証できません。レジストリエディターは、ご自身の責任において使用してください。Citrixは、Windowsレジストリを変更する前にバックアップすることをお勧めします。

場所：HKEY_LOCAL_MACHINE\Software\Citrix\Director

名前：DisableGoogleAnalytics

値：0 = 有効（デフォルト）、1 = 無効

Google Analyticsによるデータ収集を無効にするには、次のPowerShellコマンドレットを使用できます。

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director



New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name
DisableGoogleAnalytics -PropertyType DWORD -Value 1
```

新機能ガイド

Directorには、Pendoを使用して、現在のバージョンのDirectorでリリースされた新機能に関する洞察を提供する製品内ガイドがあります。適切な製品内メッセージと組み合わせた簡単な概要は、製品の新機能を理解するのに役立ちます。

この機能をオプトアウトするには、Directorがインストールされているマシンで、以下に説明するようにレジストリキーを編集します。レジストリキーが存在しない場合は、作成して目的の値に設定します。レジストリキーの値を変更した後、Directorインスタンスを更新してください。

注意:

レジストリエディターを誤って使用すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrixは、レジストリエディターの誤った使用に起因する問題が解決できることを保証できません。レジストリエディターは自己責任で使用してください。Citrixは、変更を加える前にWindowsレジストリをバックアップすることをお勧めします。

> 場所: HKEY_LOCAL_MACHINE\Software\Citrix\Director

名前: DisableGuidedHelp

値: 0 = 有効（デフォルト）、1 = 無効

製品内ガイドを無効にするには、次のPowerShellコマンドレットを使用できます。

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director



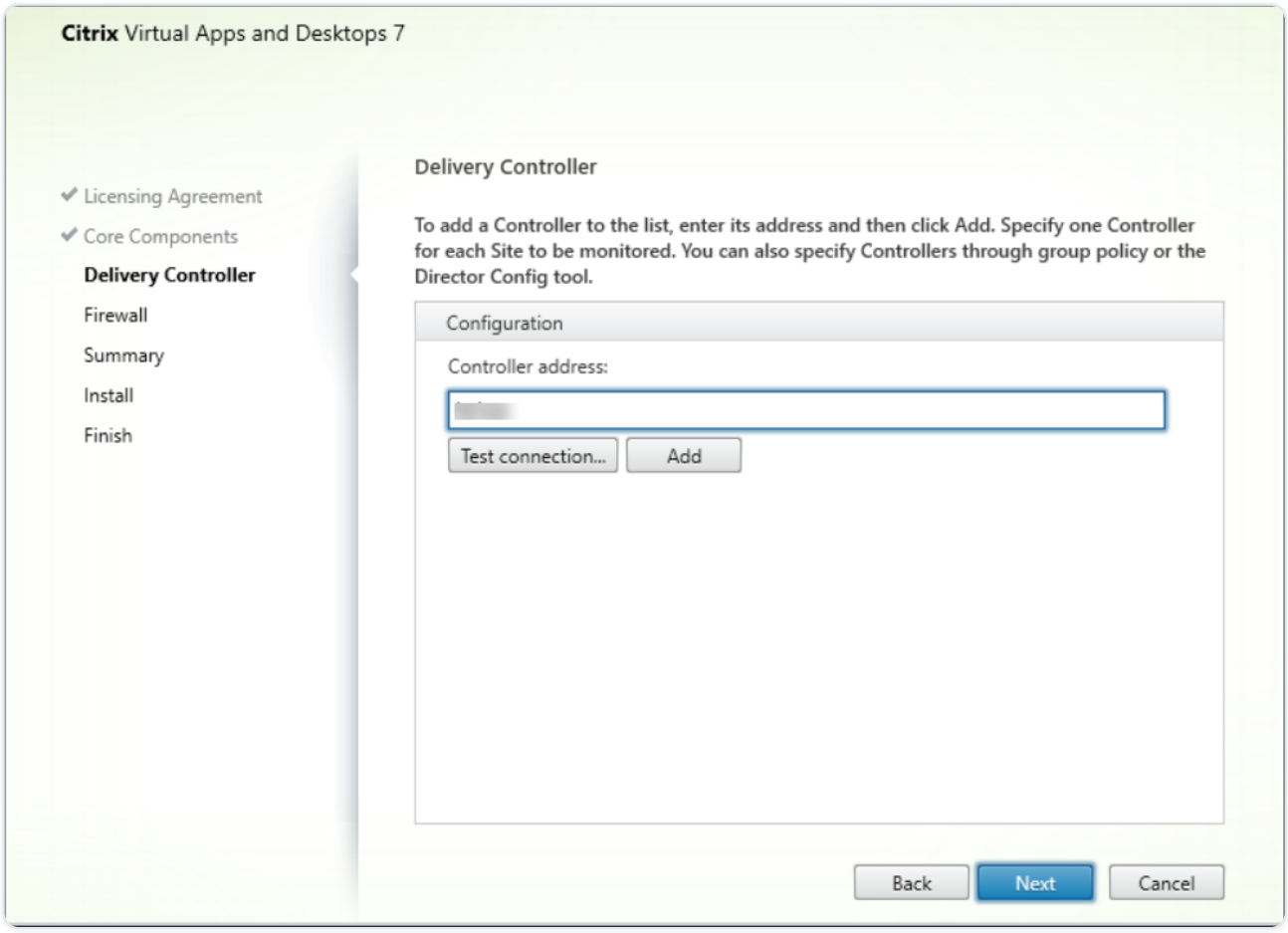
New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name DisableGuidedHelp
-PropertyType DWORD -Value 1
```

インストールと構成

Directorのインストール

Citrix Virtual Apps and Desktopsのフル製品ISOインストーラーを使用してDirectorをインストールします。これにより、前提条件の確認、不足しているコンポーネントのインストール、Director Webサイトのセットアップ、および基本的な構成が実行されます。前提条件およびその他の詳細については、このリリースのシステム要件ドキュメントを参照してください。このリリースのDirectorは、Virtual Apps 6.5より前の展開、またはVirtual Desktops 7より前の展開とは互換性がありません。 ISOインストーラーによって提供されるデフォルト構成は、一般的な展開に対応します。インストール時にDirectorが含まれていなかった場合は、ISOインストーラーを使用してDirectorを追加します。追加のコンポーネントを追加するには、ISOインストーラーを再実行し、インストールするコンポーネントを選択します。ISOインストーラーの使用方法については、インストールドキュメントのコアコンポーネントのインストールを参照してください。Citrixでは、.MSIファイルではなく、フル製品ISOインストーラーのみを使用してインストールすることをお勧めします。

DirectorがControllerにインストールされている場合、サーバーアドレスとしてlocalhostが自動的に構成され、Directorはデフォルトでローカルの Controllerと通信します。Controllerから離れた専用サーバーにDirectorをインストールする場合は、ControllerのFQDNまたはIPアドレスを入力するよう求められます。



注：

追加をクリックして、監視するControllerを追加します。

Directorはデフォルトで、指定されたControllerと通信します。監視するサイトごとにControllerアドレスを1つだけ指定してください。Directorは、同じサイト内の他のすべてのControllerを自動的に検出し、指定したControllerが失敗した場合は、それらの他のControllerにフォールバックします。

注：

DirectorはController間で負荷分散を行いません。

ブラウザーとWebサーバー間の通信を保護するために、Citrix®は、DirectorをホストするIIS WebサイトでTLSを実装することをお勧めします。手順については、Microsoft IISのドキュメントを参照してください。TLSを有効にするためにDirectorの構成は必要ありません。

Directorの展開と構成

Directorが複数のサイトを含む環境で使用される場合、Controller、Director、およびその他のコアコンポーネントがインストールされているすべてのサーバーでシステムクロックを同期してください。そうしないと、Directorでサイトが正しく表示されない可能性があります。

> **重要:**
>
> ネットワーク経由でプレーンテキストで送信されるユーザー名とパスワードのセキュリティを保護するため、Director接続にはHTTPではなくHTTPSのみを使用してください。特定のツールは、HTTP（暗号化されていない）ネットワークパケット内のプレーンテキストのユーザー名とパスワードを読み取ることができ、ユーザーにとって潜在的なセキュリティリスクを生み出す可能性があります。

権限の構成

Directorにログオンするには、Directorの権限を持つ管理者はActive Directoryドメインユーザーであり、以下の権限を持っている必要があります。

- 検索対象となるすべてのActive Directoryフォレストにおける読み取り権限（高度な構成を参照）。
- 構成された委任管理者ロール ((/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/director/install-and-configure/permissions.html)の「委任管理とDirector」を参照)。
- ユーザーをシャドウするには、管理者はWindowsリモートアシスタンス用のMicrosoftグループポリシーを使用して構成する必要があります。さらに：
  - VDAをインストールする際、すべてのユーザーデバイスでWindowsリモートアシスタンス機能が有効になっていることを確認してください（デフォルトで選択されています）。
  - Directorをサーバーにインストールする場合、Windowsリモートアシスタンスがインストールされていることを確認してください（デフォルトで選択されています）。ただし、サーバーではデフォルトで無効になっています。Directorがエンドユーザーにアシスタンスを提供するために、この機能を有効にする必要はありません。Citrixは、サーバーのセキュリティを向上させるために、この機能を無効のままにしておくことを推奨します。
  - 管理者がWindowsリモートアシスタンスを開始できるようにするには、リモートアシスタンス用の適切なMicrosoftグループポリシー設定を使用して、必要な権限を付与します。詳しくは、CTX127388: How to Enable Remote Assistance for Desktop Directorを参照してください。

高度な構成

Director は、ユーザー、Delivery Controller (DC)、VDA、および Director が異なるフォレストに配置されているフォレスト構成にまたがるマルチフォレスト環境をサポートできます。これには、フォレスト間の信頼関係と構成設定の適切なセットアップが必要です。

マルチフォレスト環境での推奨構成

推奨される構成では、ドメイン全体の認証を使用して、フォレスト間で送信および受信フォレスト信頼関係を作成する必要があります。

マルチフォレストサイト構成(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/multiforest-config.png)

Director からの信頼関係により、異なるフォレストにあるユーザーセッション、VDA、および Delivery Controller の問題をトラブルシューティングできます。

Director が複数のフォレストをサポートするために必要な高度な構成は、インターネットインフォメーションサービス (IIS) マネージャーで定義された設定によって制御されます。

> **重要:**

> IIS で設定を変更すると、Director サービスは自動的に再起動し、ユーザーをログオフします。

> IIS を使用して高度な設定を構成するには:

1. インターネットインフォメーションサービス (IIS) マネージャーコンソールを開きます。
2. デフォルトの Web サイトの下にある Director Web サイトに移動します。
3. をダブルクリックします。
4. 設定をダブルクリックして編集します。
5. をクリックして新しい設定を追加します。

Director は Active Directory を使用してユーザーを検索し、より多くのユーザーおよびマシン情報を参照します。デフォルトでは、Director は次のドメインまたはフォレストを検索します。

- 管理者アカウントがメンバーです。
- Director Webサーバーがメンバーです（異なる場合）。

Directorは、Active Directoryグローバルカタログを使用してフォレストレベルで検索を実行しようとします。フォレストレベルで検索する権限がない場合、ドメインのみが検索されます。

別のActive Directoryドメインまたはフォレストからデータを検索または参照するには、検索するドメインまたはフォレストを明示的に設定する必要があります。IISマネージャーで、Director Webサイトに次のアプリケーション設定を構成します。

```
Connector.ActiveDirectory.Domains = (user),(server)
```

値属性のuserとserverは、それぞれDirectorユーザー（管理者）とDirectorサーバーのドメインを表します。

追加のドメインまたはフォレストからの検索を有効にするには、この例に示すように、ドメイン名をリストに追加します。

```
Connector.ActiveDirectory.Domains = (user),(server),\&lt;domain1\>,
\&lt;domain2\>
```

リスト内の各ドメインについて、Directorはフォレストレベルで検索を実行しようとします。フォレストレベルで検索する権限がない場合、ドメインのみが検索されます。

ドメインローカルグループの構成

ほとんどのCitrix Service Provider（CSP）は、インフラストラクチャフォレストにVDA、DC、およびDirectorで構成される同様の環境設定を持っています。ユーザーまたはユーザーグループのレコードはカスタマーフォレストに属します。インフラストラクチャフォレストからカスタマーフォレストへの一方向の送信信頼が存在します。

CSP管理者は通常、インフラストラクチャフォレストにドメインローカルグループを作成し、カスタマーフォレストのユーザーまたはユーザーグループをこのドメインローカルグループに追加します。

推奨されるマルチフォレストサイト構成(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/domainlocalgroup-config.png)

Directorはこのようなマルチフォレスト設定をサポートし、ドメインローカルグループを使用して構成されたユーザーのセッションを監視できます。

1. IISマネージャーで、Director Webサイトに次のアプリケーション設定を追加します。

```
Connector.ActiveDirectory.DomainLocalGroupSearch= true



DomainLocalGroupSearchDomains= \&lt;domain1\>,\&lt;domain2\>
```

\<domain1\>\<domain2\> は、ドメインローカルグループが存在するフォレストの名前です。

2. ドメインローカルグループをCitrix Studioのデリバリーグループに割り当てます。
3. IISを再起動し、変更を有効にするためにDirectorに再度ログオンします。これで、Directorはこれらのユーザーのセッションを監視し、表示できるようになります。

Directorにサイトを追加する

Directorがすでにインストールされている場合は、複数のサイトで動作するように構成します。構成するには、各DirectorサーバーでIISマネージャーコンソールを使用して、アプリケーション設定のサーバーアドレスリストを更新します。

各サイトのControllerのアドレスを次の設定に追加します。

```
Service.AutoDiscoveryAddresses = SiteAController,SiteBController
```

SiteAControllerとSiteBControllerは、2つの異なるサイトのDelivery Controllerのアドレスです。

アクティビティマネージャーで実行中のアプリケーションの可視性を無効にする

デフォルトでは、DirectorのActivity Managerは、ユーザーセッションで実行されているすべてのアプリケーションのリストを表示します。この情報は、DirectorのActivity Manager機能にアクセスできるすべての管理者によって表示されます。委任された管理者ロールの場合、これにはフル管理者、デリバリーグループ管理者、およびヘルプデスク管理者が含まれます。

ユーザーのプライバシーと実行中のアプリケーションを保護するために、実行中のアプリケーションを一覧表示する**アプリケーション**タブを無効にすることができます。

警告:

レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrixは、レジストリエディターの誤った使

> 用によって生じる問題が解決されることを保証しません。レジストリエディターは自己責任で使用してください。編集する前に必ずレジストリをバックアップしてください。

1. VDAで、`HKEY_LOCAL_MACHINE\Software\Citrix\Director\TaskManagerDataDisplayed`にあるレジストリキーを変更します。デフォルトでは、キーは1に設定されています。値を0に変更すると、VDAから情報が収集されず、Activity Managerに表示されなくなります。
2. Directorがインストールされているサーバーで、実行中のアプリケーションの可視性を制御する設定を変更します。デフォルトでは、値は「true」であり、アプリケーションタブで実行中のアプリケーションの可視性を許可します。値を「false」に変更すると、可視性が無効になります。このオプションは、DirectorのActivity Managerのみに影響し、VDAには影響しません。次の設定の値を変更します。 UI.TaskManager.EnableApplications = false

> **重要:**
>
> 実行中のアプリケーションの表示を無効にするには、Activity Managerにデータが表示されないように両方の変更を行います。

PIVスマートカード認証を構成する

この記事では、スマートカード認証機能を有効にするためにDirectorサーバーおよびActive Directoryで必要な構成について説明します。

> **注：**
>
> スマートカード認証は、同じActive Directoryドメインのユーザーのみがサポートされます。

Directorサーバーの構成

Directorサーバーで以下の構成手順を実行します。

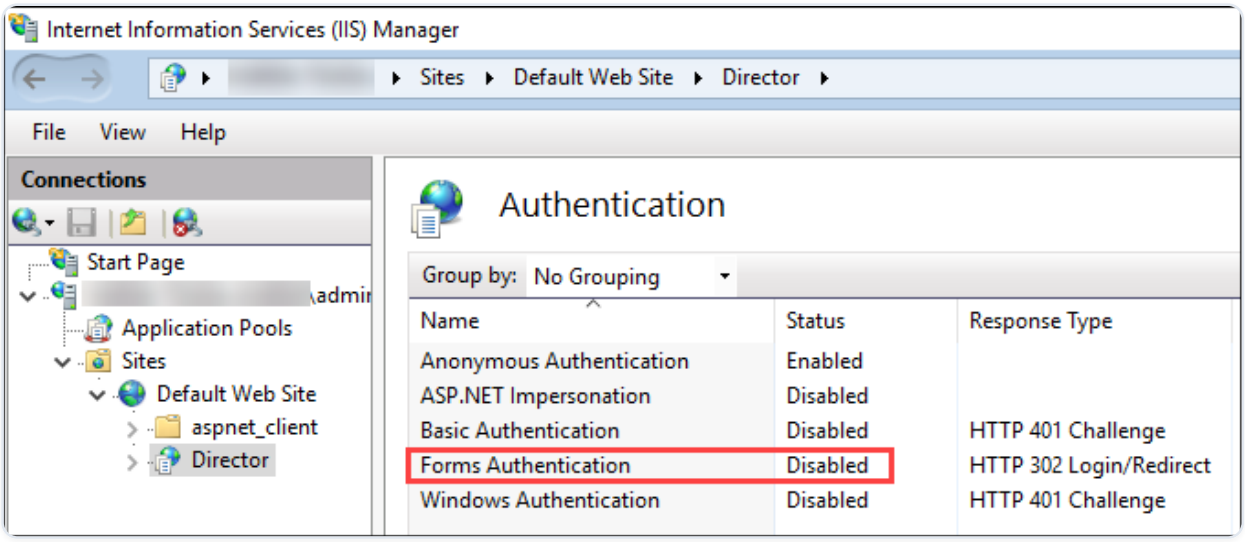
1. クライアント証明書マッピング認証をインストールして有効にします。Microsoftドキュメントのクライアント証明書マッピング認証にある**Active Directoryを使用したクライアント証明書マッピング認証**の手順に従います。
2. Directorサイトでフォーム認証を無効にします。

   IISマネージャーを起動します。

サイト \> **既定のWebサイト** \> **Director** に移動します。

認証 を選択します。

フォーム認証 を右クリックして、**無効** を選択します。



3. クライアント証明書認証のために、DirectorのURLをより安全なhttpsプロトコル (HTTPではなく) に構成します。

   a. IISマネージャーを起動します。

   b. **サイト** \> **既定のWebサイト** \> **Director** に移動します。

   c. 「**SSL Settings**」を選択します。

   d. 「**SSLを必須にする**」と「**クライアント証明書**」\>「**必須**」を選択します。

   SSL設定(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/dir-smartcard-config2.png)

4. web.config を更新します。テキストエディターを使用して、web.config ファイル（`c:\inetpub\wwwroot\Director` にあります）を開きます。

`<system.webServer>` 親要素の下に、次のスニペットを最初の子要素として追加します。

```
&lt;defaultDocument>

   &lt;files>

       &lt;add value="LogOn.aspx"/>

   &lt;/files>
```

```
&lt;/defaultDocument>
```

Active Directory の構成

デフォルトでは、Director アプリケーションは、**アプリケーションプール**の ID プロパティで実行されます。スマートカード認証には委任が必要であり、そのためには Director アプリケーションの ID がサービスホスト上で Trusted Computing Base (TCB) 権限を持っている必要があります。

Citrix では、アプリケーションプールの ID 用に個別のサービスアカウントを作成することをお勧めします。MSDN Microsoft の記事「Protocol Transition with Constrained Delegation Technical Supplement」の手順に従って、サービスアカウントを作成し、TCB 権限を割り当てます。

新しく作成したサービスアカウントを Director アプリケーションプールに割り当てます。次の図は、サンプルサービスアカウント「Domain Pool」のプロパティダイアログを示しています。

サンプルサービスアカウント(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/dir-smartcard-config3.png)

このアカウントに対して、次のサービスを構成します:

- デリバリーコントローラー™: ホスト、HTTP
- Director: ホスト、HTTP
- Active Directory のプロトコル: GC、LDAP

構成するには、,

1. 「ユーザーアカウントのプロパティ」ダイアログで、「**追加**」をクリックします。
2. 「**サービスの追加**」ダイアログで、「ユーザー」または「コンピューター」をクリックします。
3. Delivery Controllerのホスト名を選択します。
4. 「**利用可能なサービス**」リストから、HOSTとHTTPの「**サービスの種類**」を選択します。

サービスを構成する(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/dir-smartcard-config4.png)

同様に、**Director**および**Active Directory**ホストのサービスの種類を追加します。

Firefoxブラウザーの構成

Firefoxブラウザーを使用するには、OpenSC 0.17.0で入手可能なPIVドライバーをインストールします。インストールと構成の手順については、Installing OpenSC PKCS#11 Module in Firefox, Step by Stepを参照してください。 Directorでのスマートカード認証機能の使用方法については、

Directorの記事のUse Director with PIV based smart card authenticationセクションを参照してください。

ネットワーク分析の構成

> **注：** この機能の利用可否は、組織のライセンスと管理者権限によって異なります。

> DirectorはCitrix ADMと統合され、ネットワーク分析とパフォーマンス管理を提供します。

- ネットワーク分析は、Citrix ADMのHDX™ Insightレポートを使用して、ネットワークのアプリケーションおよびデスクトップのコンテキストビューを提供します。この機能により、Directorは展開環境におけるICAトラフィックの詳細な分析を提供します。
- パフォーマンス管理は、履歴保持と傾向レポートを提供します。リアルタイム評価ではなくデータの履歴保持により、キャパシティと健全性の傾向を含む傾向レポートを作成できます。

Directorでこの機能を有効にすると、HDX InsightレポートはDirectorに追加情報を提供します。

- ［傾向］ページの［ネットワーク］タブには、展開環境全体におけるアプリケーション、デスクトップ、およびユーザーの遅延と帯域幅の影響が表示されます。
- ［ユーザー詳細］ページには、特定のユーザーセッションに固有の遅延と帯域幅の情報が表示されます。

制限事項:

- ［傾向］ビューでは、7より前のVDAのHDX接続ログオンデータは収集されません。それより前のVDAの場合、グラフデータは0と表示されます。

ネットワーク分析を有効にするには、DirectorにCitrix ADMをインストールして構成する必要があります。Directorには、Citrix ADMバージョン11.1ビルド49.16以降が必要です。MASはCitrix XenServerで実行される仮想アプライアンスです。ネットワーク分析を使用すると、Directorは展開環境に関連する情報を通信および収集します。

詳しくは、Citrix ADMドキュメントを参照してください。

> **注：** Citrix NetScaler Insight Centerは、15 May 2018をもってメンテナンス終了日を迎えました。Citrix Product Matrixを参照してください。ネットワーク分析のためにDirectorをCitrix ADMと統合してください。NetScaler Insight CenterからCitrix ADMへの移行については、NetScaler Insight CenterからCitrix ADMへの移行を参照してください。

1. Directorがインストールされているサーバーで、`C:\inetpub\wwwroot\Director\tools`にあるDirectorConfigコマンドラインツールを見つけ、コマンドプロンプトからパラメーター/confignetscalerを指定して実行します。
2. プロンプトが表示されたら、Citrix ADMマシン名（FQDNまたはIPアドレス）、ユーザー名、パスワード、HTTPS接続タイプ（HTTPよりも推奨）、およびCitrix ADM統合を選択します。
3. 変更を確認するには、ログオフして再度ログオンします。

> **注:**

> セキュリティ上の理由から、HDX Insightのみにアクセスするのに十分な権限を持つ、DirectorとのADM統合のためのカスタムロールを作成することをお勧めします。

> ADM Director統合のユーザーロール(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/dir-adm-user-role.png)

> 詳細については、アクセスポリシーの構成を参照してください。

委任管理とDirector

委任管理では、管理者、役割、スコープという3つの概念を使用します。権限は、管理者の役割と、その役割のスコープに基づいています。たとえば、管理者は、スコープが1つのサイトのエンドユーザーに対する責任を含むヘルプデスク管理者ロールを割り当てられる場合があります。

委任管理者の作成については、メインの委任管理の記事を参照してください。

管理権限によって、管理者に表示されるDirectorインターフェイスと、実行できるタスクが決まります。権限によって以下が決定されます。

- 管理者がアクセスできるビュー（総称してビューと呼ばれます）。
- 管理者が表示および操作できるデスクトップ、マシン、セッション。
- 管理者が実行できるコマンド（ユーザーセッションのシャドウイングやメンテナンスモードの有効化など）。

組み込みの役割と権限は、管理者がDirectorをどのように使用するかを決定します。

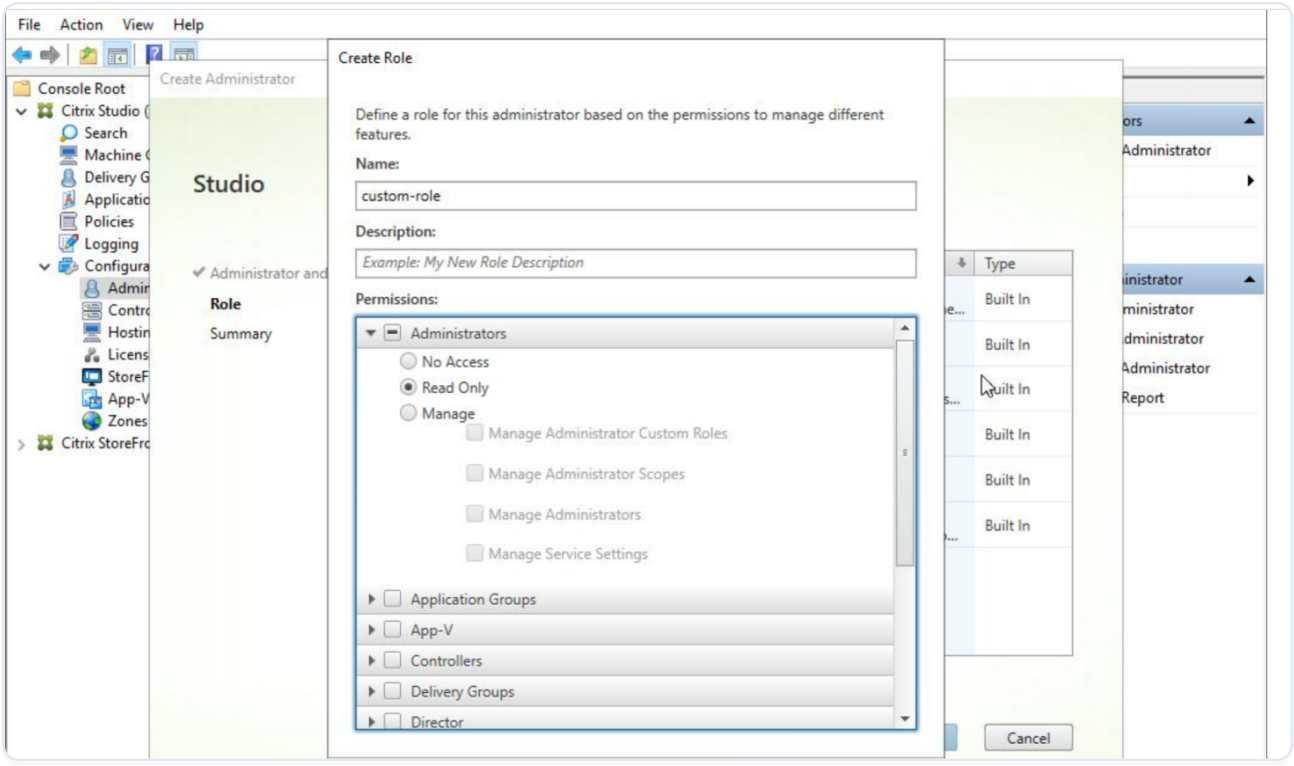
管理者ロール	DIRECTORでの権限
フル管理者	すべてのビューへのフルアクセス、およびすべてのコマンド（ユーザーセッションのシャドウイング、メンテナンスモードの有効化、トレンドデータのエクスポートなど）を実行できます。
デリバリーグループ管理者	すべてのビューへのフルアクセス、およびすべてのコマンド（ユーザーセッションのシャドウイング、メンテナンスモードの有効化、トレンドデータのエクスポートなど）を実行できます。
読み取り専用管理者	指定されたスコープ内のすべてのビューにアクセスし、すべてのオブジェクトとグローバル情報を表示できます。HDX™チャネルからレポートをダウンロードでき、トレンドビューの「エクスポート」オプションを使用してトレンドデータをエクスポートできます。その他のコマンドを実行したり、ビュー内の何かを変更したりすることはできません。
ヘルプデスク管理者	ヘルプデスクビューとユーザー詳細ビューのみにアクセスでき、管理者が管理を委任されているオブジェクトのみを表示できます。ユーザーセッションのシャドウイングを行い、そのユーザーのコマンドを実行できます。メンテナンスモード操作を実行できます。シングルセッションOSマシンに対して電源制御オプションを使用できます。ダッシュボード、トレンド、アラート、またはフィルタービューにはアクセスできません。マルチセッションOSマシンに対して電源制御オプションを使用することはできません。
マシンカタログ管理者	マシン詳細ページ（マシンベース検索）のみにアクセスできます。
ホスト管理者	アクセスなし。この管理者はDirectorではサポートされておらず、データを表示できません。

Director管理者用のカスタム役割を構成する

Studioでは、組織の要件により厳密に一致させ、権限をより柔軟に委任するために、Director固有のカスタム役割を構成することもできます。たとえば、組み込みのヘルプデスク管理者役割を制限して、この管理者がセッションをログオフできないようにすることができます。

Director権限を持つカスタム役割を作成する場合、その役割に他の一般的な権限も付与する必要があります。

- Delivery Controller™ にログオンするための権限 - 管理者ノードで少なくとも読み取り専用アクセス
- Directorでそれらのデリバリーグループに関連するデータを表示するためのデリバリーグループへの権限 - 少なくとも読み取り専用アクセス



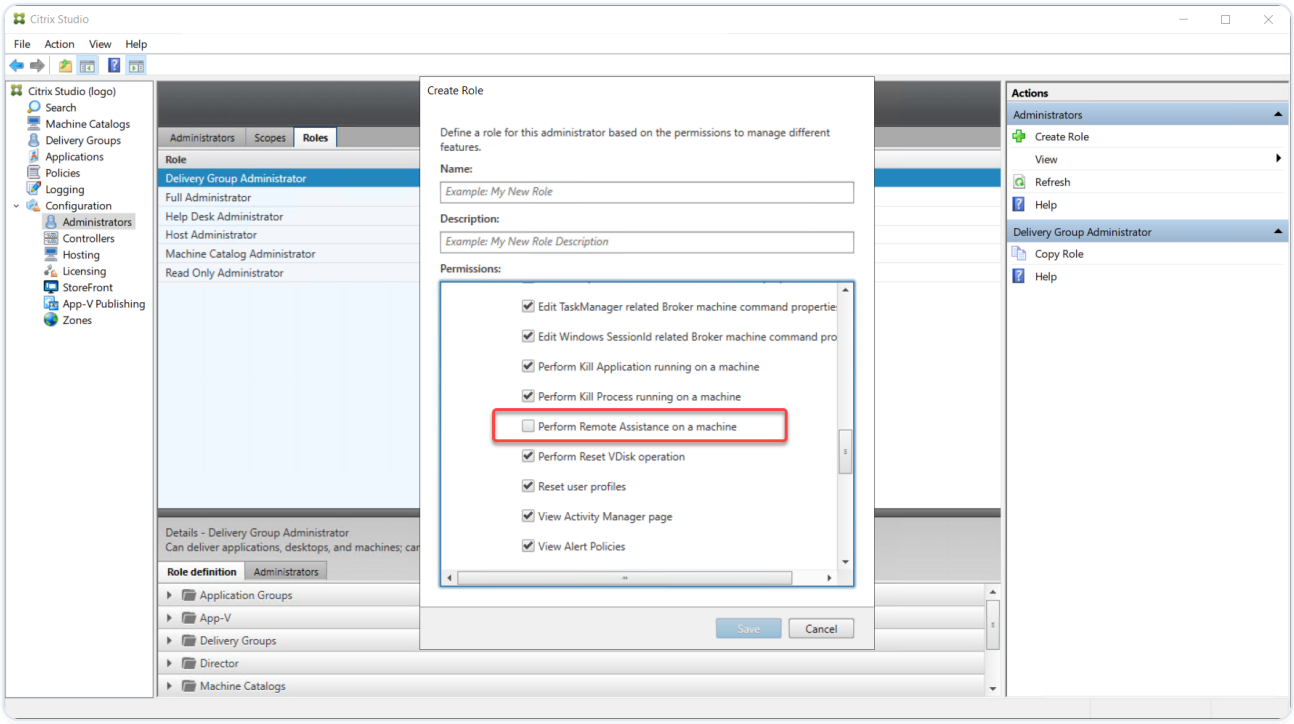
または、既存のロールをコピーして、さまざまなビューの追加の権限を含めることで、カスタムロールを作成できます。たとえば、ヘルプデスクロールをコピーして、ダッシュボードまたはフィルターページを表示する権限を含めることができます。

カスタムロールのDirector権限を選択します。これには以下が含まれます。

- マシン上で実行中のアプリケーションの強制終了を実行する
- マシン上で実行中のプロセスの強制終了を実行する
- マシン上でリモートアシスタンスを実行する
- ユーザープロファイルをリセットする

- クライアント詳細ページを表示
- ダッシュボードページの表示
- フィルターページを表示する
- マシン詳細ページを表示
- トレンドページの表示
- ユーザー詳細ページを表示

この例では、シャドウイング（マシン上でリモートアシスタンスを実行する）が無効になっています。



権限は、UIで適用可能になるために他の権限に依存する場合があります。たとえば、**マシン上で実行中のアプリケーションの強制終了を実行する**権限を選択すると、ロールに権限があるパネルでのみ**アプリケーションの終了**機能が有効になります。次のパネル権限を選択できます。

- フィルターページを表示する
- ユーザー詳細ページを表示
- マシン詳細ページを表示
- クライアント詳細ページを表示

さらに、他のコンポーネントの権限リストから、デリバリーグループの以下の権限を検討してください。

- デリバリーグループのメンバーシップを使用して、マシンのメンテナンスモードを有効/無効にする。

- デリバリーグループのメンバーシップを使用して、Windowsデスクトップマシンで電源操作を実行する。
- デリバリーグループのメンバーシップを使用して、マシンでセッション管理を実行する。

Directorの展開を保護する

この記事では、Directorの展開および構成時にシステムセキュリティに影響を与える可能性のある領域について説明します。

Microsoft インターネット インフォメーション サービス (IIS) の構成

制限されたIIS構成でDirectorを構成できます。

アプリケーションプールのリサイクル制限

次のアプリケーションプールリサイクル制限を設定できます。

- 仮想メモリ制限: 4,294,967,295
- プライベートメモリ制限: StoreFront™サーバーの物理メモリのサイズ
- 要求制限: 4,000,000,000

ファイル名拡張子

リストにないファイル名拡張子を許可しないように設定できます。

Directorは、要求フィルタリングで次のファイル名拡張子を必要とします。

- .aspx ファイル
- ．css
- .html ファイル
- .js
- ．png
- ．svc
- ．gif
- ドットジェイソン
- ドットウォフ
- ドットウォフ2
- ドットティーティーエフ

Directorは、要求フィルタリングで次のHTTP動詞を必要とします。リストにない動詞を許可しないように設定できます。

- GET
- POST
- HEAD

Directorは以下を必要としません。

- ISAPIフィルター
- ISAPI拡張機能
- CGIプログラム
- FastCGIプログラム

> **重要:**
>
> - Directorは完全信頼を必要とします。グローバルな.NET信頼レベルをHigh以下に設定しないでください。
> - Directorは個別のアプリケーションプールを維持します。Directorの設定を変更するには、Directorサイトを選択して変更します。

ユーザー権限の構成

Directorがインストールされると、そのアプリケーションプールには次のものが付与されます。

- **サービスとしてログオン**のログオン権限
- **プロセスに対するメモリクォータの調整**、**セキュリティ監査の生成**、および**プロセスレベルトークンの置き換え**の特権

言及されている権限と特権は、アプリケーションプールが作成される際の通常のインストール動作です。

これらのユーザー権限を変更する必要はありません。これらの特権は Director では使用されず、自動的に無効になります。

Directorの通信

実稼働環境では、Directorとサーバー間でやり取りされるデータを保護するために、インターネットプロトコルセキュリティ (IPsec) またはHTTPSプロトコルを使用します。

IPsecは、データ整合性とリプレイ保護を備えた認証済み暗号化通信を提供する、インターネットプロトコルの標準拡張機能のセットです。IPsecはネットワーク層プロトコルセットであるため、上位レベルのプロトコルは変更なしで使用できます。HTTPSは、トランスポート層セキュリティ (TLS) プロトコルを使用して強力なデータ暗号化を提供します。

注：

- Citrix®は、イントラネットネットワーク内でのDirectorコンソールへのアクセスを制限することを強くお勧めします。
- Citrixは、実稼働環境でDirectorへの保護されていない接続を有効にしないことを強くお勧めします。
- Directorからの安全な通信には、接続ごとに個別の構成が必要です。
- SSLプロトコルは推奨されません。代わりに、より安全なTLSプロトコルを使用してください。
- Citrix ADCとの通信は、IPsecではなくTLSを使用して保護してください。

DirectorとCitrix Virtual Apps and Desktopsサーバー間の通信 (監視およびレポート用) を保護するには、データアクセスセキュリティを参照してください。

DirectorとCitrix ADC間の通信 (Citrix Insight用) を保護するには、ネットワーク分析の構成を参照してください。

Directorとライセンスサーバー間の通信を保護するには、ライセンス管理コンソールを保護するを参照してください。

Director のセキュリティ分離

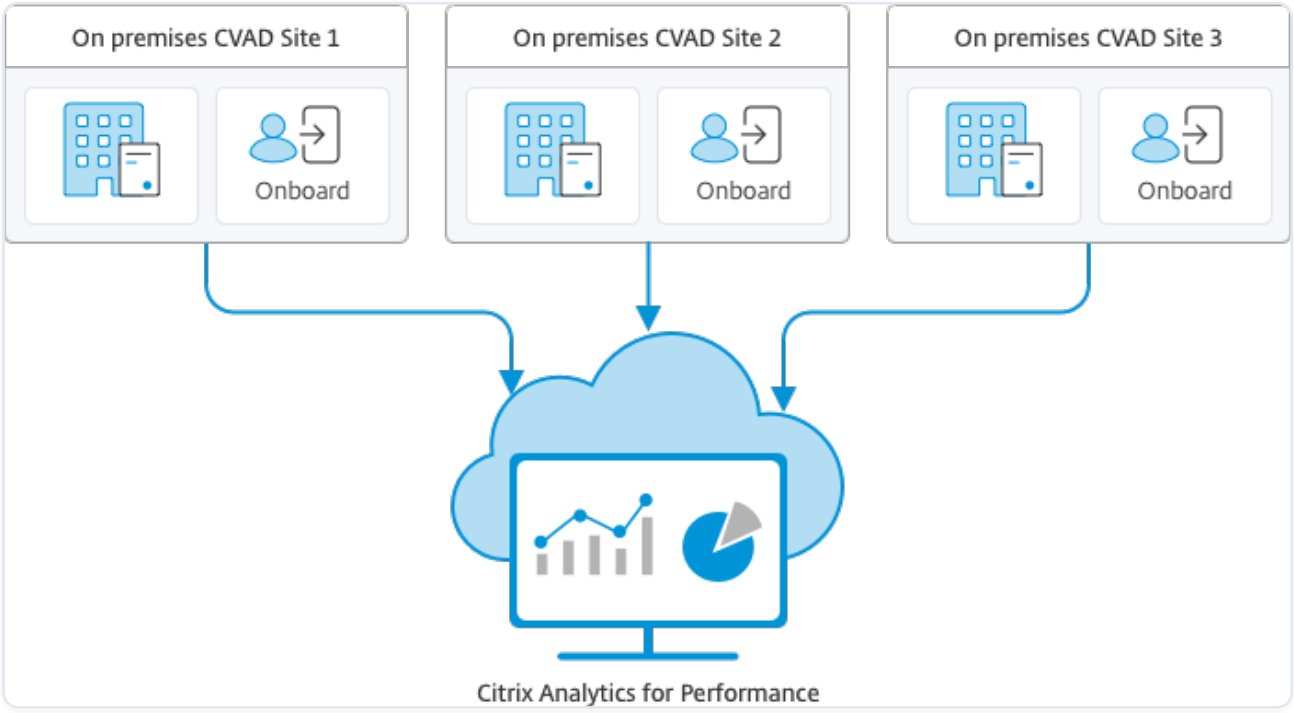
Director と同じ Web ドメイン（ドメイン名とポート）に任意の Web アプリケーションを展開できます。ただし、それらの Web アプリケーションのセキュリティリスクは、Director 展開のセキュリティを低下させる可能性があります。より高度なセキュリティ分離が必要な場合は、Citrix では Director を別の Web ドメインに展開することをお勧めします。

Citrix Analytics for Performance™ を使用したオンプレミスサイトの構成

Citrix Analytics for Performance (Performance Analytics) は、Citrix Analytics Cloud Serviceが提供する包括的なパフォーマンス監視ソリューションです。Performance Analyticsは、パフォーマンスメトリックに基づいて構築された高度なインサイトと分析を提供します。Performance Analyticsは、組織内の1つ以上のCitrix Virtual Apps and Desktops™サイトの使用状況とパフォーマンスメトリックを監視および表示するのに役立ちます。

Performance Analyticsの詳細については、Performance Analyticsの記事を参照してください。

サイトからCitrix Cloud™上のCitrix Analytics for Performanceにパフォーマンスデータを送信して、その高度なパフォーマンス分析機能を活用できます。Performance Analyticsを表示および使用するには、まず**Director**の**Analytics**タブからCitrix Analytics for Performanceを使用してオンプレミスサイトを構成する必要があります。



Performance Analyticsは安全な方法でデータにアクセスし、Citrix Cloudからオンプレミス環境にデータが転送されることはありません。

前提条件

DirectorからCitrix Analytics for Performanceを構成するために、新しいコンポーネントをインストールする必要はありません。次の要件が満たされていることを確認してください。

- Delivery ControllerとDirectorがバージョン1912 CU2以降であること。詳細については、機能互換性マトリックスを参照してください。

> **注：**

- Delivery ControllerがMicrosoft .NET Frameworkバージョン4.8より前のバージョンを実行している場合、DirectorからCitrix Analytics for Performanceを使用してオンプレミスサイトを構成すると、失敗する可能性があります。回避策として、Delivery Controllerの.NET Frameworkをバージョン4.8にアップグレードしてください。LCM-9255。
- DirectorからCitrix Analytics for Performanceを使用してCitrix Virtual Apps and Desktopsバージョン2012を実行しているオンプレミスサイトを構成すると、構成が数時間後、またはDelivery ControllerでCitrix Monitor Serviceを再起動した後に失敗する可能性があります。この場合、Analyticsタブには「未接続」ステータスが表示されます。回避策として、Delivery Controllerのレジストリにencryptionフォルダーを作成します。場所: HKEY_LOCAL_MACHINE\Software\Citrix\XDservices\Monitor、フォルダー名: Encryption。CitrixMonitorアカウントがEncryptionフォルダーに対してフルコントロールアクセス権を持っていることを確認してください。Citrix Monitor Serviceを再起動します。DIR-14324。

- この構成を実行するための**Analytics**タブへのアクセスは、フル管理者のみが利用できます。
- Performance Analyticsがパフォーマンスメトリックにアクセスできるようにするには、すべてのDelivery ControllerとDirectorがインストールされているマシンで、アウトバウンドインターネットアクセスが利用可能である必要があります。具体的には、次のURLへのアクセス可能性を確認してください。
  - Citrixキー登録: `https://*.citrixnetworkapi.net/`
  - シトリックス クラウド: `https://*.citrixworkspacesapi.net/`
  - シトリックス アナリティクス: `https://*.cloud.com/`
  - Microsoft Azure: `https://*.windows.net/` Delivery ControllerとDirectorマシンがイントラネット内にあり、アウトバウンドインターネットアクセスがプロキシサーバー経由である場合、以下を確認してください。
- プロキシサーバーは、上記のURLリストを許可する必要があります。
- Director web.config および citrix.monitor.exe.config ファイルに次の構成を追加します。この構成は **configuration** タグ内に追加してください。

```
&lt;system.net>

    &lt;defaultProxy>
```

```
        &lt;proxy  usesystemdefault = "false"  proxyaddress = "http://
&lt;your_proxyserver_address>:80" bypassonlocal = "true"  />

    &lt;/defaultProxy>

&lt;/system.net>
```

- Director web.config は、Director がインストールされているマシンの `C:\inetpub\wwwroot\Director\web.config` にあります。
- citrix.monitor.exe.config は、Delivery Controller がインストールされているマシンの `C:\Program Files\Citrix\Monitor\Service\Citrix.Monitor.exe.Config` にあります。

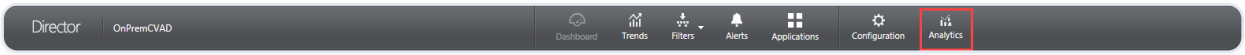
この設定は、IIS 上で Microsoft によって提供されます。詳細については、`https://docs.microsoft.com/ja-jp/dotnet/framework/network-programming/proxy-configuration` を参照してください。 構成ファイルの **defaultproxy** フィールドは、Director および Monitor Service のアウトバウンドアクセスを制御します。Performance Analytics との構成および通信には、**defaultproxy** フィールドを **true** に設定する必要があります。有効なポリシーによってこのフィールドが false に設定されている可能性があります。この場合、フィールドを手動で true に設定する必要があります。変更を行う前に構成ファイルのバックアップを取ってください。変更を有効にするには、Delivery Controller™ 上の監視サービスを再起動してください。

- Citrix Analytics for Performance の有効な Citrix Cloud エンタイトルメントをお持ちであること。
- Citrix Cloudアカウントは、製品登録エクスペリエンスに対する権限を持つ管理者アカウントである必要があります。管理者権限の詳細については、「管理者権限の変更」を参照してください。

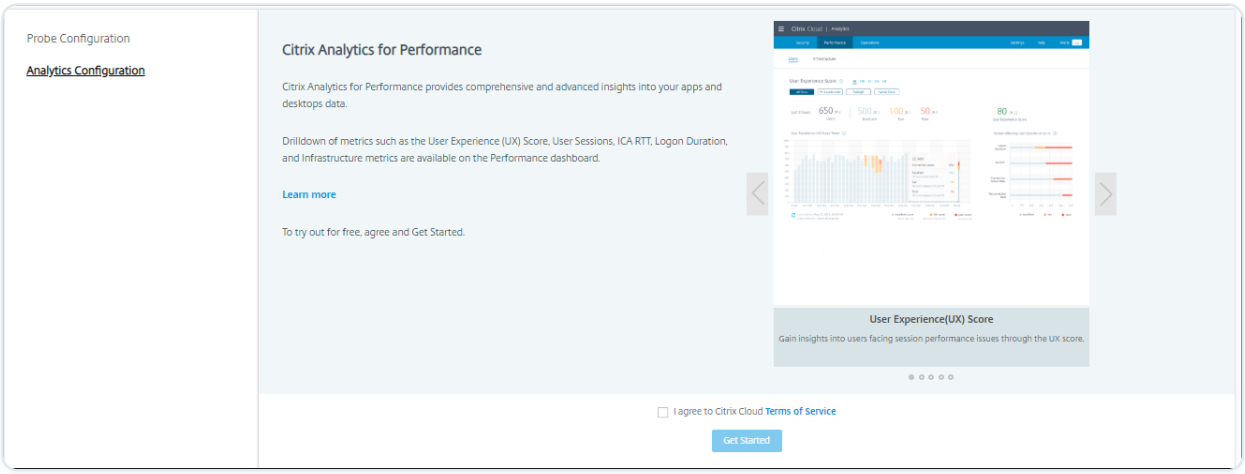
構成手順

前提条件を確認したら、次の手順を実行します。

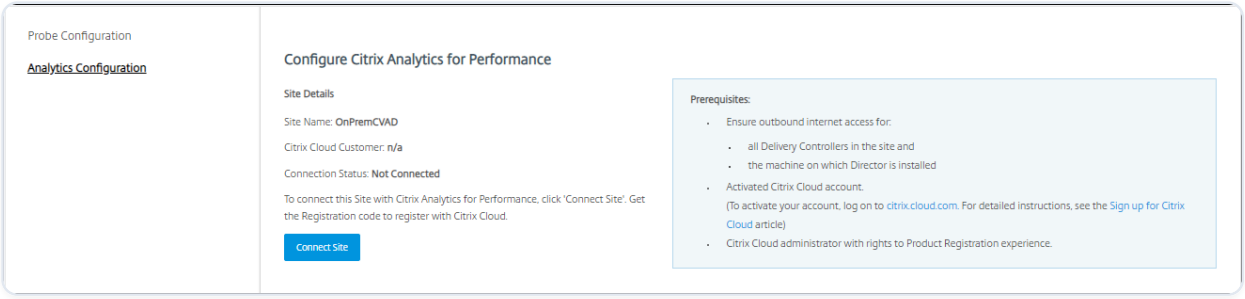
1. Directorにフル管理者としてログオンし、Performance Analyticsで構成するサイトを選択します。
2. **Analytics**タブをクリックします。**Configuration**ページが表示されます。



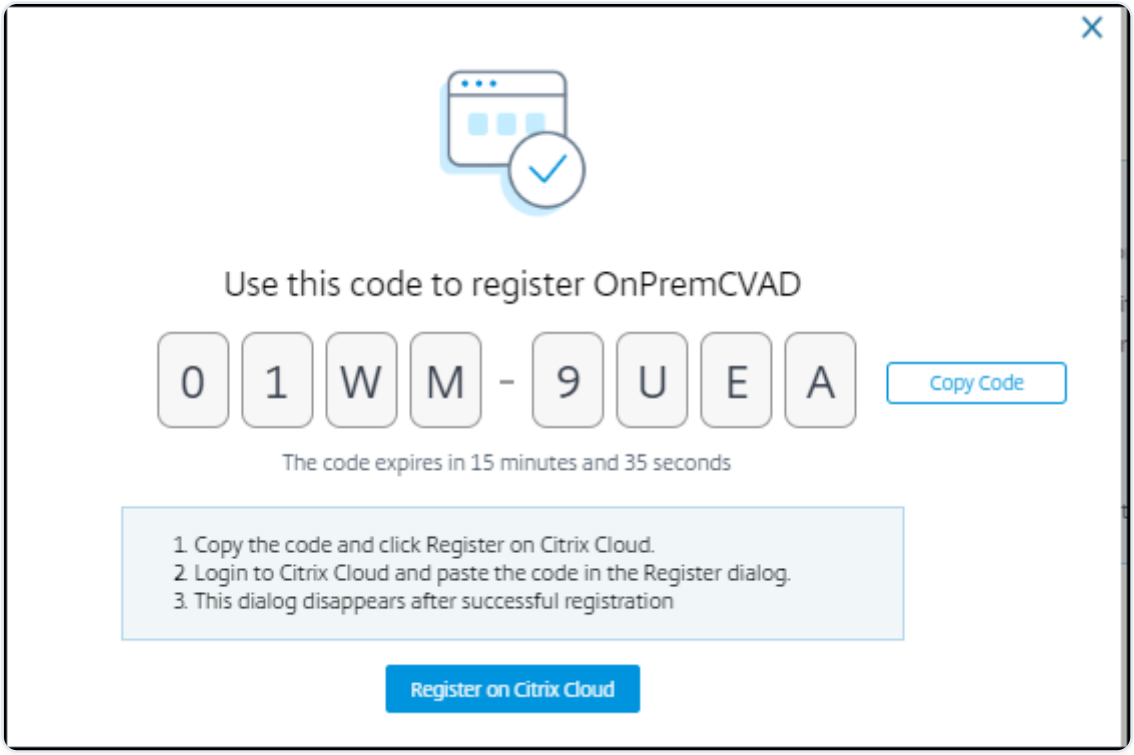
3. 手順を確認し、サービス規約を選択してから、**Get Started**をクリックします。



4. 前提条件を確認し、それらが満たされていることを確認します。サイトの詳細を確認します。
5. 構成プロセスを開始するには、**サイトの接続**をクリックします。



6. このサイトを Citrix Cloud に登録するために使用する、一意の8桁の登録コードが生成されます。

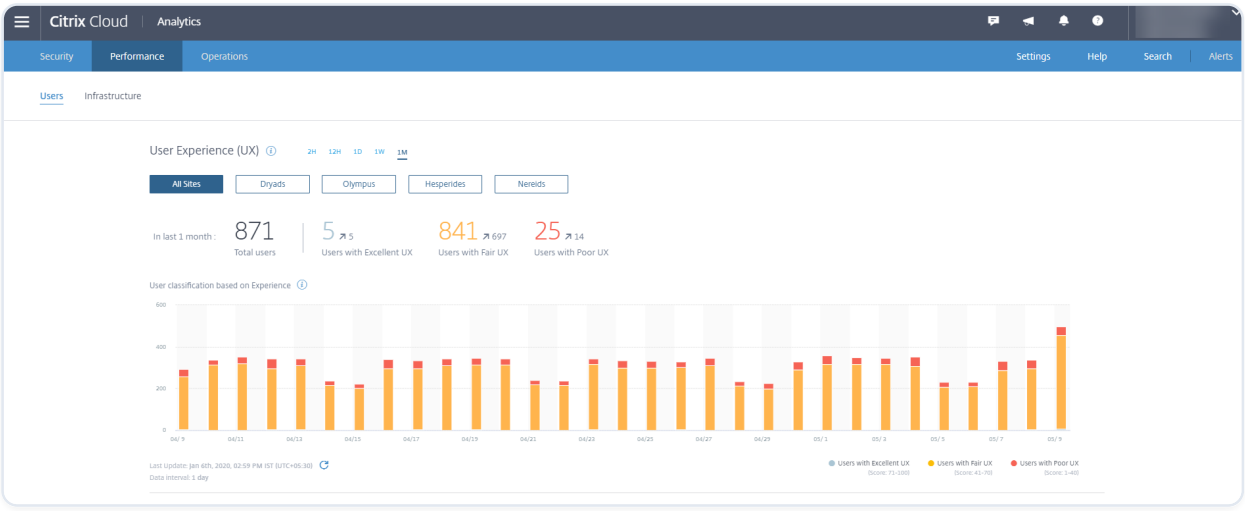


7. コードをコピーするには**Copy Code**をクリックし、次に**Register on Citrix Cloud**をクリックします。

8. Citrix Cloudの登録URLにリダイレクトされます。Citrix Cloudの資格情報でログインし、顧客を選択します。
9. Citrix Cloudの「製品登録」ページに、コピーした登録コードを貼り付けます。登録するには、**［続行］**をクリックします。登録の詳細を確認し、**［登録］**をクリックします。

   Citrix Cloudでの登録(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/dir-onboarding6.png)
10. オンプレミスサイトがCitrix Cloudに登録されます。次に、**Director**から、**Analytics**タブの**Go to Analytics**をクリックします。

    Analyticsに移動(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/dir-onboarding7.png)
11. Performance Analyticsがブラウザの新しいタブで開きます。



   Citrix Cloudセッションの有効期限が切れている場合、Citrix.comまたはMy Citrixアカウントのログオンページにリダイレクトされることがあります。
12. 複数のサイトをPerformance Analyticsに登録するには、Directorから各サイトについて前述の構成手順を繰り返します。構成されているすべてのサイトのメトリックがPerformance Analyticsダッシュボードに表示されます。

    サイトごとに複数のDirectorインスタンスが実行されている場合は、いずれか1つのDirectorインスタンスから構成します。サイトに接続されている他のすべてのDirectorインスタンスは、構成プロセス後の次回の更新時に更新されます。
13. サイトをCitrix Cloudから切断するには、**［サイトの切断］**をクリックします。このオプションは、既存の構成を削除します。

> **注:**

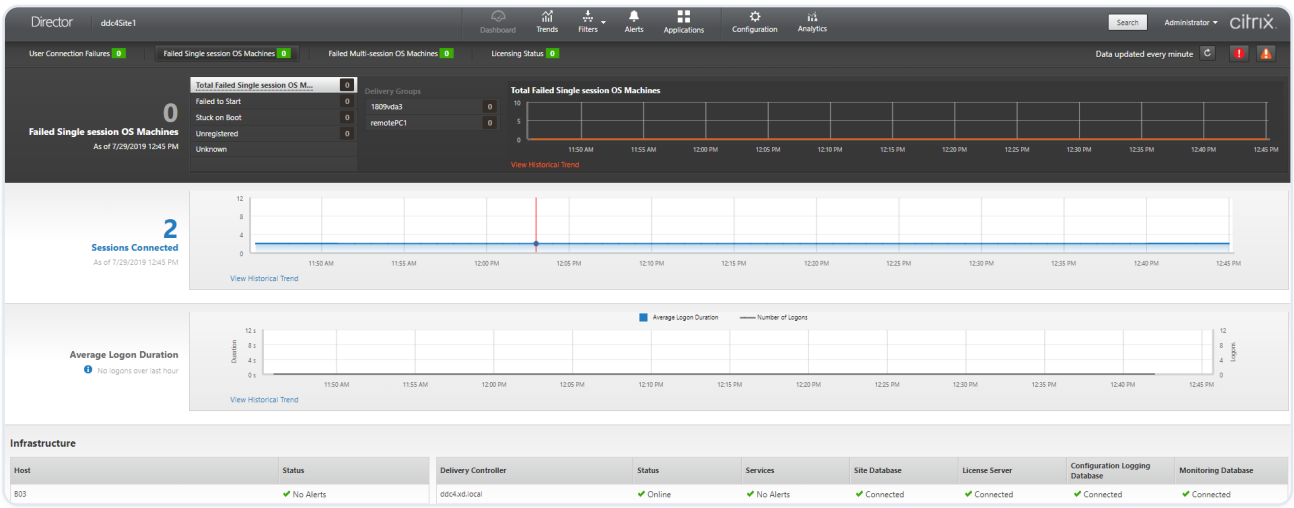
> サイトを初めて構成するとき、サイトからのイベントの処理には時間がかかる場合があり（約1時間）、Performance Analyticsダッシュボードにメトリックが表示されるまでに遅延が生じます。その後、イベントは定期的に更新されます。

> 切断後、新しいアカウントからのイベントが送信されるまで、古いアカウントからのデータ送信はしばらく継続されます。データ送信が停止してから約1時間、古いアカウントに関連する分析はPerformance Analyticsダッシュボードに表示されたままになります。

> Citrix Analyticsサービスへのエンタイトルメントの有効期限が切れると、サイトメトリックがPerformance Analyticsに送信されなくなるまでに最大1日かかります。

サイト分析

完全な管理者権限があれば、Directorを開くと、ダッシュボードは、サイトの健全性と使用状況を監視するための一元的な場所を提供します。



現在障害がなく、過去60分間に障害が発生していない場合、パネルは折りたたまれたままになります。障害が発生すると、特定の障害パネルが自動的に表示されます。

> **注：**
>
> 組織のライセンスと管理者権限によっては、一部のオプションまたは機能が利用できない場合があります。

Director ダッシュボードのパネル

ユーザー接続障害

過去60分間の接続障害。合計数の横にあるカテゴリをクリックすると、その種類の障害のメトリックが表示されます。隣接するテーブルでは、その数がデリバリーグループ別に分類されています。接続障害には、アプリケーション制限に達したことによる障害が含まれます。アプリケーション制限の詳細については、「アプリケーション」を参照してください。

失敗したシングルセッションOSマシンまたは失敗したマルチセッションOSマシン

過去60分間の合計障害数（デリバリーグループ別）。障害は、起動失敗、起動中に停止、未登録などの種類別に分類されます。マルチセッションOSマシンでは、障害には最大負荷に達したマシンも含まれます。

ライセンスステータス

ライセンスサーバーアラートには、ライセンスサーバーから送信されたアラートと、アラートを解決するために必要なアクションが表示されます。ライセンスサーバーバージョン11.12.1以降が必要です。デリバリーコントローラーアラートには、コントローラーから見たライセンス状態の詳細が表示され、コントローラーによって送信されます。XenApp 7.6またはXenDesktop 7.6以降のコントローラーが必要です。Studioでアラートのしきい値を設定できます。**Delivery Controllers** > **Details** > **Product Editions** > **PLT** に表示されるライセンスステータスは、**Premium** を示し、**Platinum** ではありません。

猶予状態

Directorには、次のいずれかの猶予状態が表示されます。この情報はデリバリーコントローラーから取得されます。

1. **非アクティブ:** いかなる種類のライセンスキャッシュモードでもありません。通常のライセンス制限が適用されます。
2. **緊急猶予:** ライセンスサーバーに到達できない場合、または接続を仲介している間にライセンス情報を取得できない場合に有効になります。ユーザーには影響ありません。Directorに表示されるエラーは、ライセンスサーバーに到達可能になるまで閉じることができません。
3. **猶予期間の期限切れ:** 緊急ライセンスキャッシュモードの有効期限が切れました。

詳細については、ライセンスの超過 および ライセンスバーストモード を参照してください。

接続されたセッション

過去60分間のすべてのデリバリーグループにわたる接続セッション。

平均ログオン時間

過去60分間のログオンデータ。左側の大きな数字は、1時間あたりの平均ログオン時間です。XenDesktop 7.0より前のVDAのログオンデータは、この平均には含まれません。詳細については、ユーザーログオンの問題の診断 を参照してください。

インフラストラクチャ

サイトのインフラストラクチャ（ホストとコントローラー）を一覧表示します。Citrix HypervisorまたはVMwareのインフラストラクチャの場合、パフォーマンスアラートを表示できます。たとえば、管理対象サーバーまたは仮想マシンでCPU、ネットワークI/O、またはディスクI/Oの使用率が指定されたしきい値を超えたときに、XenCenterがパフォーマンスアラートを生成するように構成できます。デフォルトでは、アラートの繰り返し間隔は60分ですが、これも構成できます。詳細については、Citrix Hypervisor製品ドキュメントの「XenCenterパフォーマンスアラート」セクションを参照してください。

> **注：**
>
> 特定のメトリックにアイコンが表示されない場合、そのメトリックは使用しているホストの種類でサポートされていないことを示します。たとえば、System Center Virtual Machine Manager（SCVMM）ホスト、AWS、CloudStackでは、正常性情報は利用できません。

以下のオプションを使用して問題のトラブルシューティングを続行します（以下のセクションで説明されています）。

- ユーザーマシンの電源を制御する
- マシンへの接続を防止する

セッションの監視

セッションが切断されても、セッションはアクティブなままでアプリケーションは実行され続けますが、ユーザーデバイスはサーバーと通信しなくなります。

アクション	説明
ユーザーの現在接続されているマシンまたはセッションを表示する	アクティビティマネージャーとユーザー詳細ビューから、ユーザーが現在接続しているマシンまたはセッション、およびこのユーザーがアクセスできるすべてのマシンとセッションのリストを表示します。このリストにアクセス

アクション	説明
	するには、ユーザータイトルバーのセッションスイッチャーアイコンをクリックします。詳細については、セッションの復元 を参照してください。
すべてのデリバリーグループにおける接続済みセッションの総数を表示する	ダッシュボードの**接続済みセッション**ペインで、過去60分間のすべてのデリバリーグループにおける接続済みセッションの合計数を表示します。次に、大きな合計数をクリックすると、フィルタービューが開き、選択したデリバリーグループと範囲、およびデリバリーグループ全体の使用状況に基づいてグラフィカルなセッションデータを表示できます。
アイドルセッションを終了する	セッションフィルタービューには、すべてのアクティブなセッションに関連するデータが表示されます。関連ユーザー、デリバリーグループ、セッション状態、およびしきい値期間を超えるアイドル時間に基づいてセッションをフィルター処理します。フィルター処理されたリストから、ログオフまたは切断するセッションを選択します。詳細については、アプリケーションのトラブルシューティング を参照してください。
より長い期間のデータを表示する	トレンドビューで、**セッション**タブを選択すると、より長い期間（つまり、過去60分より前のセッション合計）の接続済みセッションと切断済みセッションに関するより具体的な使用状況データをドリルダウンして表示できます。この情報を表示するには、**履歴トレンドの表示**をクリックします。

注：

ユーザーデバイスがレガシーVirtual Delivery Agent（VDA）（バージョン7より前のVDAやLinux VDAなど）を実行している場合、Directorはセッションに関する完全な情報を表示できません。代わりに、情報が利用できないことを示すメッセージが表示されます。

デスクトップ割り当てルールの制限事項: Citrix Studioでは、異なるユーザーまたはユーザーグループに対して複数のデスクトップ割り当てルール（DAR）をデリバリーグループ内の単一のVDAに割り当てることができます。StoreFront™は、ログインしているユーザーのDARに従って、対応する**表示名**とともに割り当てられたデスクトップを表示します。ただし、DirectorはDARをサポートしておらず、ログインしているユーザーに関係なく、デリバリーグループ名を使用して割り当てられたデスクトップを表示します。その結果、Directorで特定のデスクトップをマシンにマッピングすることはできません。 StoreFrontに表示される割り当てられたデスクトップを、Directorに表示されるデリバリーグループ名にマッピングするには、次のPowerShellコマンドを使用します。

```
Get-BrokerDesktopGroup | Where-Object { $\_.Uid -eq (Get-
BrokerAssignmentPolicyRule | Where-Object { $\_.PublishedName -eq
"\&lt;Name on StoreFront\>" }).DesktopGroupUid } | Select-Object -Property
Name, Uid
```

セッション転送プロトコル

セッションの詳細パネルで、現在のセッションのHDX接続タイプで使用されている転送プロトコルを表示します。この情報は、VDAバージョン7.13以降で起動されたセッションで利用できます。

転送プロトコル (/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/sessions-transport-protocol.png)

- **HDX™** 接続タイプの場合、,
  - HDX接続にEDTが使用されている場合、プロトコルは **UDP** と表示されます。
  - HDX接続にTCPが使用されている場合、プロトコルは **TCP** と表示されます。
- **RDP**接続タイプの場合、プロトコルは**n/a**と表示されます。

アダプティブトランスポートが構成されている場合、セッション転送プロトコルは、ネットワークの状態に基づいてEDT（UDP経由）とTCPの間で動的に切り替わります。EDTを使用してHDXセッションを確立できない場合、TCPプロトコルにフォールバックします。

アダプティブトランスポートの構成の詳細については、「アダプティブトランスポート」を参照してください。

レポートのエクスポート

定期的な使用状況および容量管理レポートを生成するために、トレンドデータをエクスポートできます。エクスポートは、PDF、Excel、CSVのレポート形式をサポートしています。PDFおよび

Excel形式のレポートには、グラフと表で表されたトレンドが含まれます。CSV形式のレポートには、ビューを生成するために処理できる、またはアーカイブできる表形式のデータが含まれます。

レポートをエクスポートするには：

1. **トレンド**タブに移動します。
2. フィルター条件と期間を設定し、**適用**をクリックします。傾向グラフと表にデータが入力されます。
3. **エクスポート**をクリックし、レポートの名前と形式を入力します。

Directorは、選択したフィルター条件に基づいてレポートを生成します。フィルター条件を変更した場合は、**エクスポート**をクリックする前に**適用**をクリックしてください。

> **注：**
>
> 大量のデータをエクスポートすると、Directorサーバー、Delivery Controller、およびSQLサーバーのメモリとCPUの使用量が大幅に増加します。最適なエクスポートパフォーマンスを実現するために、サポートされる同時エクスポート操作の数とエクスポートできるデータ量は、デフォルトの制限に設定されています。

サポートされるエクスポート制限

エクスポートされたPDFおよびExcelレポートには、選択されたフィルター条件に対する完全なグラフが含まれます。ただし、すべてのレポート形式の表形式データは、テーブル内の行数またはレコード数のデフォルト制限を超えると切り捨てられます。サポートされるデフォルトのレコード数は、レポート形式に基づいて定義されます。

Internet Information Services (IIS) のDirectorアプリケーション設定を構成することで、デフォルトの制限を変更できます。

レポート形式	サポートされるレコードのデフォルト数	DIRECTORアプリケーション設定のフィールド	サポートされるレコードの最大数
PDF	500	UI.ExportPdfDrilldownLimit	5000
エクセル	100,000	UI.ExportExcelDrilldownLimit	100,000

レポート形式	サポートされるレコードのデフォルト数	DIRECTORアプリケーション設定のフィールド	サポートされるレコードの最大数
CSV	100,000 (「**セッション**」タブでは10,000,000)	UI.ExportCsvDrilldownLimit	100,000

エクスポートできるレコード数の制限を変更するには：

1. IISマネージャーコンソールを開きます。
2. デフォルトのWebサイトの下にあるDirector Webサイトに移動します。
3. 「**アプリケーション設定**」をダブルクリックします。
4. 必要に応じて、UI.ExportPdfDrilldownLimit、UI.ExportExcelDrilldownLimit、またはUI.ExportCsvDrilldownLimitフィールドの設定を編集または追加します。

アプリケーション設定でこれらのフィールド値を追加すると、デフォルト値が上書きされます。

> **警告:**
>
> サポートされている最大レコード数を超えるフィールド値を設定すると、エクスポートのパフォーマンスに影響を与える可能性があり、サポートされていません。

エラー処理

このセクションでは、エクスポート操作中に発生する可能性のあるエラーの対処方法について説明します。

- **Directorがタイムアウトしました**

このエラーは、ネットワークの問題、DirectorサーバーまたはMonitor Serviceでの高いリソース使用率が原因で発生する可能性があります。

デフォルトのタイムアウト期間は100秒です。Director Serviceのタイムアウト期間を長くするには、Internet Information Services (IIS) のDirectorアプリケーション設定で、**Connector.DataServiceContext.Timeoutフィールド**の値を設定します。

1. IISマネージャーコンソールを開きます。
2. デフォルトのWebサイトの下にあるDirector Webサイトに移動します。

3. **アプリケーション設定**をダブルクリックします。
4. **Connector.DataServiceContext.Timeout**の値を編集します。

- **Monitorがタイムアウトしました**

このエラーは、ネットワークの問題、Monitor ServiceまたはSQLサーバーでの高いリソース使用率が原因で発生する可能性があります。

Monitor Serviceのタイムアウト期間を長くするには、Delivery Controllerで次のPowerShellコマンドを実行します。

```
asnp Citrix.*

Get-MonitorConfiguration

Set-MonitorConfiguration -MonitorQueryTimeoutSeconds &lt;timeout value>
```

- **同時実行中のエクスポートまたはプレビュー操作の最大数**

Directorは、エクスポートまたはプレビューのインスタンスを1つサポートしています。「**同時実行中のエクスポートまたはプレビュー操作の最大数**」エラーが発生した場合は、次のエクスポート操作を後でもう一度試してください。

同時実行できるエクスポートまたはプレビュー操作の数を増やすことは可能ですが、Directorのパフォーマンスに影響を与える可能性があり、サポートされていません。

1. IISマネージャーコンソールを開きます。
2. デフォルトのWebサイトの下にあるDirector Webサイトに移動します。
3. **アプリケーション設定**をダブルクリックします。
4. 値**UI.ConcurrentExportLimit**を編集します。

- **Directorのディスク容量不足**

各エクスポート操作には、Windows Tempフォルダーに最大2 GBのハードディスク容量が必要です。空き容量を確保するか、Directorサーバーにハードディスク容量を追加してから、エクスポートを再試行してください。

Monitorのホットフィックス

特定のVDAマシン（物理またはVM）にインストールされているホットフィックスを表示するには、「**マシンの詳細**」ビューを選択します。

ユーザーマシンの電源状態を制御する

Directorで選択したマシンの状態を制御するには、電源制御オプションを使用します。これらのオプションは、シングルセッションOSマシンで利用できますが、マルチセッションOSマシンでは利用できない場合があります。

注：

この機能は、物理マシンまたはリモートPCアクセスを使用するマシンでは利用できません。

コマンド	機能
再起動	VMの順序だった（ソフト）シャットダウンを実行し、VMを再起動する前に実行中のすべてのプロセスを個別に停止します。たとえば、Directorで「起動に失敗しました」と表示されるマシンを選択し、このコマンドを使用して再起動します。
強制再起動	シャットダウン手順を最初に実行せずにVMを再起動します。このコマンドは、物理サーバーのプラグを抜き、再度差し込んで電源を入れ直すのと同じように機能します。
シャットダウン	VMの正常な（ソフト）シャットダウンを実行します。すべての実行中のプロセスは個別に停止されます。
強制シャットダウン	シャットダウン手順を最初に実行せずにVMをシャットダウンします。このコマンドは、物理サーバーのプラグを抜くのと同じように機能します。常にすべての実行中のプロセスをシャットダウンするとは限らず、この方法でVMをシャットダウンするとデータが失われるリスクがあります。
一時停止	実行中のVMを現在の状態で一時停止し、その状態をデフォルトのストレージリポジト

コマンド	機能
	リ上のファイルに保存します。このオプションを使用すると、VMのホストサーバーをシャットダウンし、後で再起動した後、VMを再開して元の実行状態に戻すことができます。
再開	一時停止されたVMを再開し、元の実行状態に戻します。
開始	VMがオフのときに起動します（コールドスタートとも呼ばれます）。

電源制御アクションが失敗した場合、アラートにマウスを重ねると、失敗の詳細を示すポップアップメッセージが表示されます。

マシンへの接続を防止する

適切な管理者がイメージのメンテナンス作業を実行している間、メンテナンスモードを使用して新しい接続を一時的に防止します。

マシンでメンテナンスモードを有効にすると、無効にするまで新しい接続は許可されません。ユーザーが現在ログオンしている場合、すべてのユーザーがログオフするとすぐにメンテナンスモードが有効になります。ログオフしないユーザーには、マシンが特定の時間にシャットダウンされることを通知するメッセージを送信し、電源制御を使用してマシンを強制的にシャットダウンします。

1. ユーザー詳細ビューから、またはフィルタービューでマシンのグループから、マシンを選択します。
2. **メンテナンスモード**を選択し、オプションをオンにします。

ユーザーが割り当てられたデスクトップにメンテナンスモード中に接続しようとすると、デスクトップが利用できないことを示すメッセージが表示されます。メンテナンスモードを無効にするまで、新しい接続はできません。

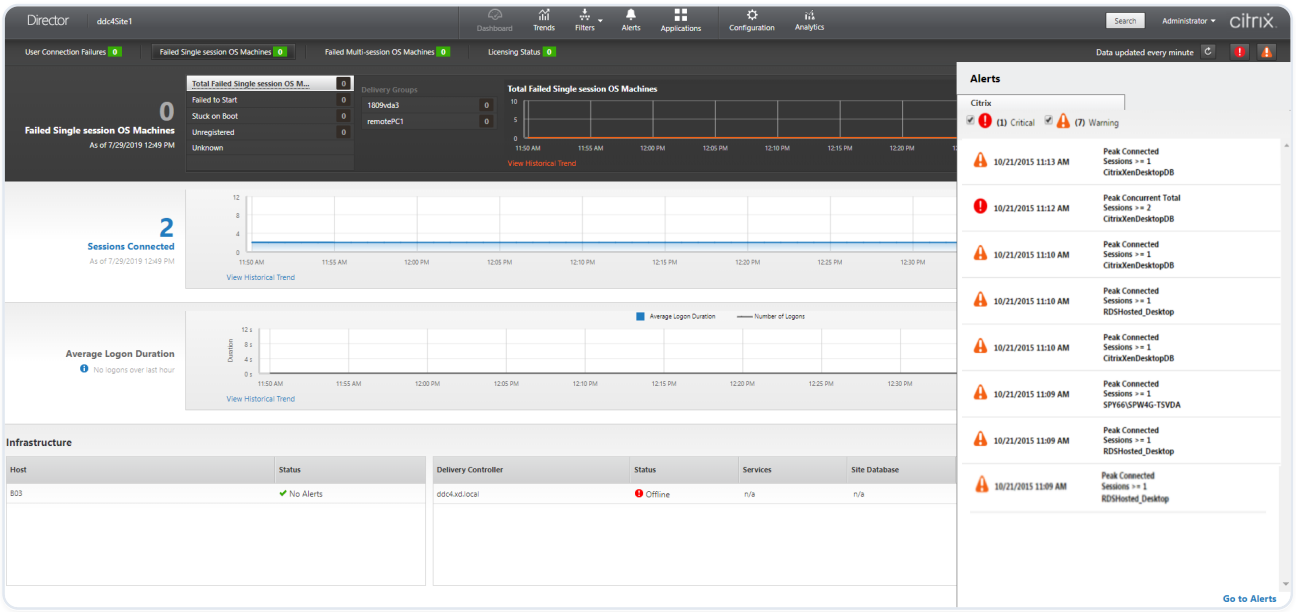
アプリケーション分析

アプリケーションタブには、アプリケーションベースの分析が単一の統合ビューで表示され、アプリケーションのパフォーマンスを効率的に分析および管理するのに役立ちます。サイトで公開されているすべてのアプリケーションの健全性と使用状況に関する貴重な洞察を得ることができます。プローブ結果、アプリケーションごとのインスタンス数、公開されているアプリケーション

に関連する障害やエラーなどのメトリックが表示されます。詳細については、**アプリケーションのトラブルシューティング**のアプリケーション分析セクションを参照してください。

アラートと通知

アラートは、Directorのダッシュボードやその他の上位レベルのビューに、警告および重大なアラートシンボルとともに表示されます。アラートは**Premium**ライセンスサイトで利用できます。アラートは1分ごとに自動的に更新されます。オンデマンドでアラートを更新することもできます。

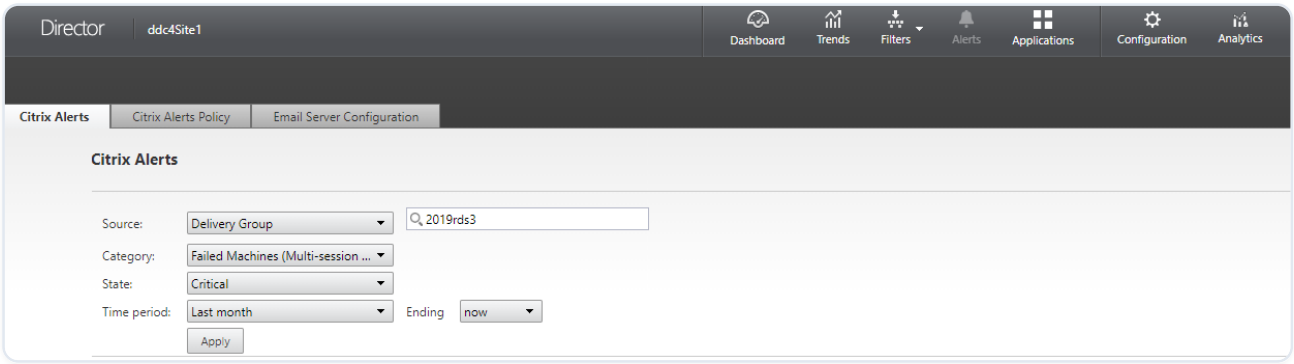


警告アラート（琥珀色の三角形）は、条件の警告しきい値に達したか、それを超えたことを示します。

重大なアラート（赤い円）は、条件の重大なしきい値に達したか、それを超えたことを示します。

アラートの詳細情報を表示するには、サイドバーからアラートを選択するか、サイドバーの下部にある**Go to Alerts**リンクをクリックするか、Directorページの上部から**Alerts**を選択します。

アラートビューでは、アラートをフィルター処理してエクスポートできます。たとえば、特定のデリバリーグループの過去1か月間の失敗したマルチセッションOSマシン、または特定のユーザーのすべてのアラートなどです。詳細については、「レポートのエクスポート」を参照してください。



Citrix®アラート

Citrixアラートは、Citrixコンポーネントから発生し、Directorで監視されるアラートです。Citrixアラートは、Directorの**Alerts** \> **Citrix Alerts Policy**で構成できます。構成の一部として、アラートが設定したしきい値を超えたときに、個人やグループにメールで通知を送信するように設定できます。Citrixアラートの設定の詳細については、「アラートポリシーの作成」を参照してください。

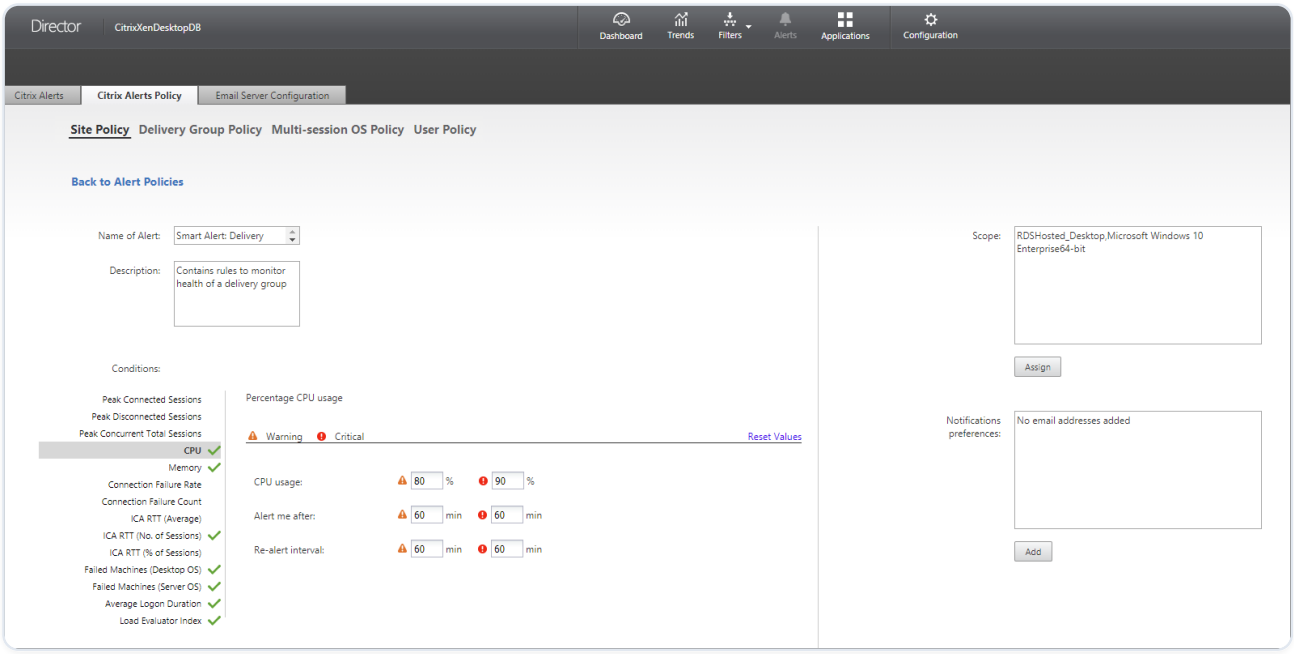
> **注：**
>
> ファイアウォール、プロキシ、またはMicrosoft Exchange Serverがメールアラートをブロックしないようにしてください。

スマートアラートポリシー

事前定義されたしきい値を持つ一連の組み込みアラートポリシーは、デリバリーグループおよびマルチセッションOS VDAスコープで利用できます。この機能には、Delivery Controllerバージョン7.18以降が必要です。組み込みアラートポリシーのしきい値パラメーターは、**Alerts** \> **Citrix Alerts Policy**で変更できます。 これらのポリシーは、サイトに少なくとも1つのアラートターゲット（デリバリーグループまたはマルチセッションOS VDA）が定義されている場合に作成されます。さらに、これらの組み込みアラートは、新しいデリバリーグループまたはマルチセッションOS VDAに自動的に追加されます。

Directorとサイトをアップグレードする場合、以前のDirectorインスタンスのアラートポリシーが引き継がれます。組み込みアラートポリシーは、Monitorデータベースに対応するアラートルールが存在しない場合にのみ作成されます。

組み込みアラートポリシーのしきい値については、「アラートポリシーの条件」セクションを参照してください。

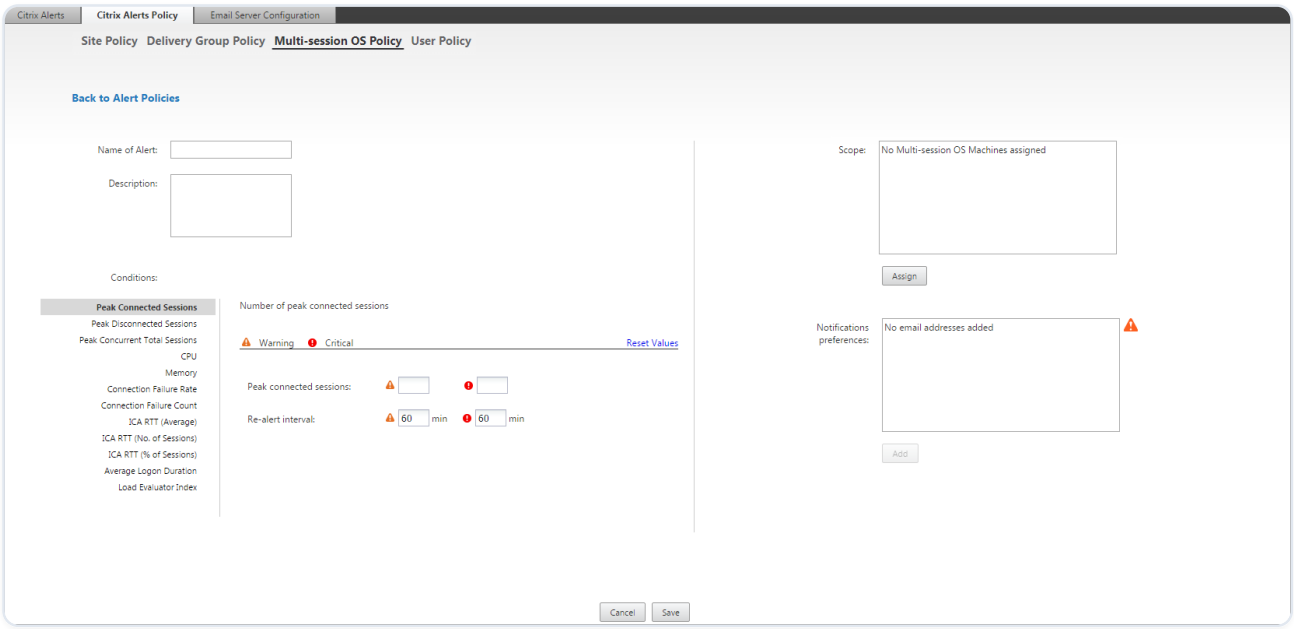


SCOMアラート

SCOMアラートは、Microsoft System Center 2012 Operations Manager (SCOM) からのアラート情報を表示し、Director内でデータセンターの健全性とパフォーマンスをより包括的に示します。詳細については、「SCOMアラート統合の構成」セクションを参照してください。

サイドバーを展開する前にアラートアイコンの横に表示されるアラートの数は、CitrixアラートとSCOMアラートの合計です。

アラートポリシーを作成する



新しいアラートポリシーを作成するには、たとえば、特定のセッション数条件が満たされたときにアラートを生成するには、次の手順を実行します。

1. **アラート** \> **Citrixアラートポリシー** に移動し、たとえば、マルチセッションOSポリシーを選択します。
2. **Create** をクリックします。
3. ポリシーに名前を付けて説明し、アラートがトリガーされるために満たす必要がある条件を設定します。たとえば、ピーク接続セッション、ピーク切断セッション、およびピーク同時合計セッションの警告値と危険値を指定します。警告値は危険値より大きくしてはいけません。詳細については、アラートポリシーの条件を参照してください。
4. 再アラート間隔を設定します。アラートの条件が引き続き満たされている場合、この時間間隔でアラートが再度トリガーされ、アラートポリシーで設定されている場合は、メール通知が生成されます。却下されたアラートは、再アラート間隔でメール通知を生成しません。
5. スコープを設定します。たとえば、特定のデリバリーグループに設定します。
6. 通知設定で、アラートがトリガーされたときにメールで通知されるべきユーザーを指定します。アラートポリシーでメール通知設定を行うには、**Email Server Configuration**タブでメールサーバーを指定する必要があります。
7. 「**保存**」をクリックします。

スコープで20以上のデリバリーグループが定義されたポリシーを作成すると、構成の完了に約30秒かかる場合があります。この間、スピナーが表示されます。

最大20のユニークなデリバリーグループ（合計1000のデリバリーグループターゲット）に対して50を超えるポリシーを作成すると、応答時間が増加する（5秒を超える）可能性があります。

アクティブなセッションを含むマシンをあるデリバリーグループから別のデリバリーグループに移動すると、マシンパラメーターを使用して定義された誤ったデリバリーグループアラートがトリガーされる可能性があります。

アラートポリシーの条件

以下に、アラートカテゴリ、アラートを軽減するための推奨アクション、および定義されている場合は組み込みポリシー条件を示します。組み込みのアラートポリシーは、アラートおよび再アラートの間隔が60分に設定されています。

ピーク接続セッション

- Directorのセッショントレンドビューで、接続済みセッションのピークを確認します。
- セッション負荷に対応する十分な容量があることを確認してください。
- 必要に応じて新しいマシンを追加する

ピーク切断セッション

- Directorのセッショントレンドビューで、切断済みセッションのピークを確認します。
- セッション負荷に対応できる十分な容量があることを確認します。
- 必要に応じて、新しいマシンを追加します。
- 必要に応じて、切断されたセッションをログオフします。

ピーク時の同時合計セッション数

- Directorのセッショントレンドビューで、同時セッションのピークを確認します。
- セッション負荷に対応できる十分な容量があることを確認します。
- 必要に応じて、新しいマシンを追加します。
- 必要に応じて、切断されたセッションをログオフします。

CPU

CPU 使用率の割合は、プロセスを含む VDA 上の全体的な CPU 消費量を示します。個々のプロセスによる CPU 使用率の詳細については、対応する VDA の ページで確認できます。

- **［マシン詳細］>［履歴使用率の表示］>［上位10プロセス］** に移動し、CPUを消費しているプロセスを特定します。プロセスレベルのリソース使用状況統計の収集を開始するには、プロセス監視ポリシーが有効になっていることを確認してください。
- 必要に応じてプロセスを終了します。
- プロセスを終了すると、保存されていないデータが失われます。
- すべてが期待どおりに機能している場合は、将来的に追加のCPUリソースを追加します。

> **注：**
>
> ポリシー設定 **［リソース監視を有効にする］** は、VDAがインストールされたマシンでのCPUおよびメモリのパフォーマンスカウンターの監視に対して、デフォルトで許可されています。このポリシー設定が無効になっている場合、CPUおよびメモリの状態に関するアラートはトリガーされません。詳しくは、「監視ポリシー設定」を参照してください。

> **スマートポリシー条件:**

- **スコープ：** デリバリーグループ、マルチセッションOSスコープ
- **しきい値:** 警告 - 80%、危険 - 90%

メモリ

メモリ使用率は、VDA上の全体的なメモリ消費量（プロセスによるものを含む）を示します。
個々のプロセスによるメモリ使用量に関する詳細な情報は、対応するVDAの**マシン詳細**ページから取得できます。

- **［マシン詳細］>［履歴使用率の表示］>［上位10プロセス］** に移動し、メモリを消費しているプロセスを特定します。プロセスレベルのリソース使用状況統計の収集を開始するには、プロセス監視ポリシーが有効になっていることを確認してください。
- 必要に応じてプロセスを終了します。
- プロセスを終了すると、保存されていないデータが失われます。
- すべてが期待どおりに機能している場合は、将来的に追加のメモリを追加します。

> **注：**
>
> ポリシー設定 **［リソース監視を有効にする］** は、VDAがインストールされたマシンでのCPUおよびメモリのパフォーマンスカウンターの監視に対して、デフォルトで許可されています。このポリシー設定が無効になっている場合、CPUおよびメモリの状態に関するアラートはトリガーされません。詳しくは、「監視ポリシー設定」を参照してください。
>
> **スマートポリシー条件:**
>
> - **スコープ：** デリバリーグループ、マルチセッションOSスコープ
> - **閾値:** 警告 - 80%、危機的 - 90%

接続失敗率

過去1時間の接続失敗の割合。

- 試行された総接続数に対する総失敗数に基づいて計算されます。
- Directorの接続失敗トレンドビューで、構成ログから記録されたイベントを確認します。
- アプリケーションまたはデスクトップが到達可能であるかどうかを判断します。

接続失敗数

過去1時間の接続失敗数。

- Director Connection Failures Trendsビューで、構成ログから記録されたイベントを確認します。

- アプリケーションまたはデスクトップが到達可能であるかどうかを判断します。

ICA® RTT (平均)

平均ICAラウンドトリップ時間。

- ICA RTTの内訳についてCitrix ADMを確認し、根本原因を特定します。詳細については、Citrix ADMドキュメントを参照してください。
- Citrix ADMが利用できない場合は、DirectorのユーザーDetailビューでICA RTTと遅延を確認し、ネットワークの問題か、アプリケーションまたはデスクトップの問題かを判断します。

ICA RTT (セッション数)

閾値のICAラウンドトリップ時間を超えるセッションの数。

- ICA RTTが高いセッション数についてCitrix ADMを確認します。詳細については、Citrix ADMドキュメントを参照してください。
- Citrix ADMが利用できない場合は、ネットワークチームと協力して根本原因を特定します。

  スマートポリシーの条件:

  - **スコープ:** デリバリーグループ、マルチセッションOSスコープ
  - **しきい値:** 警告 - 5セッション以上で300ミリ秒、重大 - 10セッション以上で400ミリ秒

ICA RTT (セッションの割合)

平均ICAラウンドトリップ時間を超えるセッションの割合。

- ICA RTTが高いセッション数についてCitrix ADMを確認します。詳細については、Citrix ADMドキュメントを参照してください。
- Citrix ADMが利用できない場合は、ネットワークチームと協力して根本原因を特定します。

ICA RTT (ユーザー)

指定されたユーザーによって起動されたセッションに適用されるICAラウンドトリップ時間。ICA RTTが少なくとも1つのセッションでしきい値を超えた場合、アラートがトリガーされます。

失敗したマシン（シングルセッションOS）

失敗したシングルセッションOSマシンの数。失敗は、Directorのダッシュボードおよびフィルタービューに示されているように、さまざまな理由で発生する可能性があります。

- Citrix Scout診断を実行して根本原因を特定します。詳細については、ユーザーの問題のトラブルシューティングを参照してください。

スマートポリシー条件:

- **スコープ:** デリバリーグループスコープ
- **しきい値:** 警告 - 1、重大 - 2

失敗したマシン (マルチセッションOS)

失敗したマルチセッションOSマシンの数。失敗は、Directorのダッシュボードおよびフィルタービューに示されているように、さまざまな理由で発生する可能性があります。

- Citrix Scout診断を実行して、根本原因を特定します。

スマートポリシー条件:

- **スコープ:** デリバリーグループ、マルチセッションOSスコープ
- **しきい値:** 警告 - 1、重大 - 2

平均ログオン時間

過去1時間に発生したログオンの平均ログオン時間。

- Directorダッシュボードでログオン期間に関する最新のメトリックを確認します。短期間に多数のユーザーがログオンすると、ログオン期間が増加する可能性があります。
- ログオンのベースラインと内訳を確認して、原因を絞り込みます。詳細については、「ユーザーログオンの問題の診断」を参照してください。

スマートポリシー条件:

- **スコープ:** デリバリーグループ、マルチセッションOSスコープ
- **しきい値:** 警告 - 45秒、重大 - 60秒

ログオン時間（ユーザー）

過去1時間に発生した、指定されたユーザーのログオンのログオン時間。

負荷評価インデックス

過去5分間の負荷評価インデックスの値。

- ピーク負荷（最大負荷）が発生している可能性のあるマルチセッションOSマシンについて、Directorで確認します。ダッシュボード（障害）とトレンドの負荷評価インデックスレポートの両方を確認します。

スマートポリシーの条件:

- **スコープ:** デリバリーグループ、マルチセッションOSスコープ
- **しきい値:** 警告 - 80%、重大 - 90%

ハイパーバイザーアラートの監視

Directorは、ハイパーバイザーの健全性を監視するためのアラートを表示します。Citrix Hypervisor™およびVMware vSphereからのアラートは、ハイパーバイザーのパラメーターと状態の監視に役立ちます。ハイパーバイザーへの接続ステータスも監視され、ホストのクラスターまたはプールが再起動されたり、利用できなくなったりした場合にアラートが提供されます。

ハイパーバイザーアラートを受信するには、Citrix Studioでホスティング接続が作成されていることを確認してください。詳細については、「接続とリソース」を参照してください。これらの接続のみがハイパーバイザーアラートの監視対象となります。次の表に、ハイパーバイザーアラートのさまざまなパラメーターと状態を示します。

アラート	サポートされているハイパーバイザー	トリガー元	条件	構成
CPU使用率	Citrix ハイパーバイザー、VMware vSphere	ハイパーバイザー	CPU使用率アラートのしきい値に達したか、超えた場合	アラートのしきい値はハイパーバイザーで構成する必要があります。
メモリ使用量	Citrix ハイパーバイザー、VMware vSphere	ハイパーバイザー	メモリ使用量アラートしきい値に達したか、超過しました	アラートのしきい値はハイパーバイザーで構成する必要があります。
ネットワーク使用量	Citrix ハイパーバイザー、VMware vSphere	ハイパーバイザー	ネットワーク使用量アラートしきい値に達したか、超過しました	アラートのしきい値はハイパーバイザーで構成する必要があります。
ディスク使用量	ヴイエムウェアブイスフィア	ハイパーバイザー	ディスク使用量アラートしきい値に達したか、超過しました	アラートのしきい値はハイパーバイザーで構成する必要があります。

アラート	サポートされているハイパーバイザー	トリガー元	条件	構成
ホスト接続または電源状態	ヴイエムウェア ブイスフィア	ハイパーバイザー	ハイパーバイザーホストが再起動されたか、利用できません	アラートはVMware vSphereにプリビルドされています。追加の構成は不要です。
ハイパーバイザー接続が利用できません	Citrix ハイパーバイザー、VMware vSphere	デリバリーコントローラー™	ハイパーバイザー（プールまたはクラスター）への接続が失われたか、電源がオフになったか、再起動されました。このアラートは、接続が利用できない間、1時間ごとに生成されます。	アラートはDelivery Controllerにプリビルドされています。追加の構成は不要です。

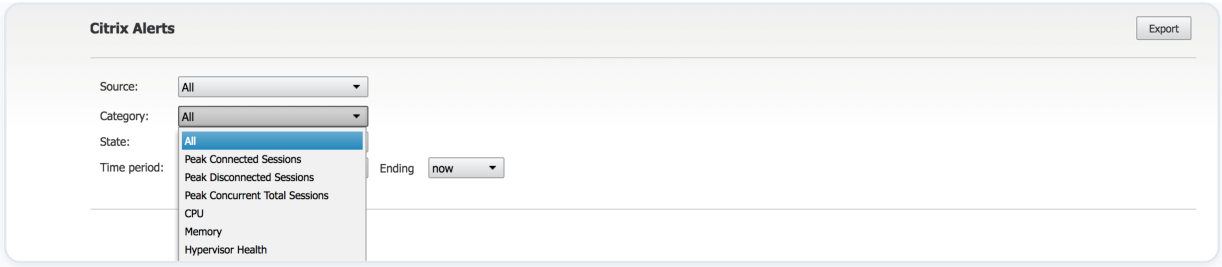
注：

アラートの構成の詳細については、Citrix XenCenter Alerts を参照するか、VMware vCenter Alertsのドキュメントを確認してください。

メール通知設定は、**Citrix Alerts Policy > サイトポリシー > ハイパーバイザーの健全性**で構成できます。ハイパーバイザーアラートポリシーのしきい値条件は、Directorからではなく、ハイパーバイザーからのみ構成、編集、無効化、または削除できます。ただし、メール設定の変更やアラートの解除はDirectorで行うことができます。

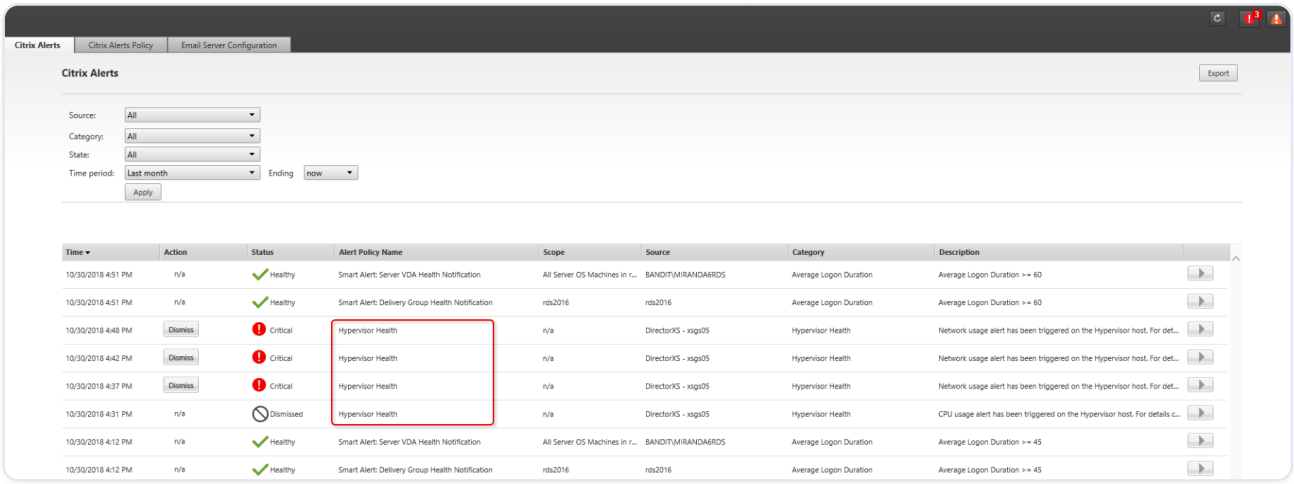
重要:

- ハイパーバイザーによってトリガーされたアラートは、Directorで取得および表示されます。ただし、ハイパーバイザーアラートのライフサイクル/状態の変更はDirectorには反映されません。
- ハイパーバイザーコンソールで正常、解除済み、または無効になっているアラートは、Directorに表示され続け、明示的に解除する必要があります。
- Directorで解除されたアラートは、ハイパーバイザーコンソールでは自動的に解除されません。



ハイパーバイザーの健全性という新しいアラートカテゴリが追加され、ハイパーバイザーアラートのみをフィルターできるようになりました。これらのアラートは、しきい値に達するか超えると表示されます。ハイパーバイザーアラートは次のいずれかです。

- 重大 — ハイパーバイザーアラームポリシーの重大なしきい値に達したか、超えた場合
- 警告 — ハイパーバイザーアラームポリシーの警告しきい値に達したか、超えた場合
- 却下済み — アクティブなアラートとして表示されなくなったアラート



この機能には、Delivery Controllerバージョン7 1811以降が必要です。サイト7 1811以降で古いバージョンのDirectorを使用している場合、ハイパーバイザーアラートの数のみが表示されます。アラートを表示するには、Directorをアップグレードする必要があります。

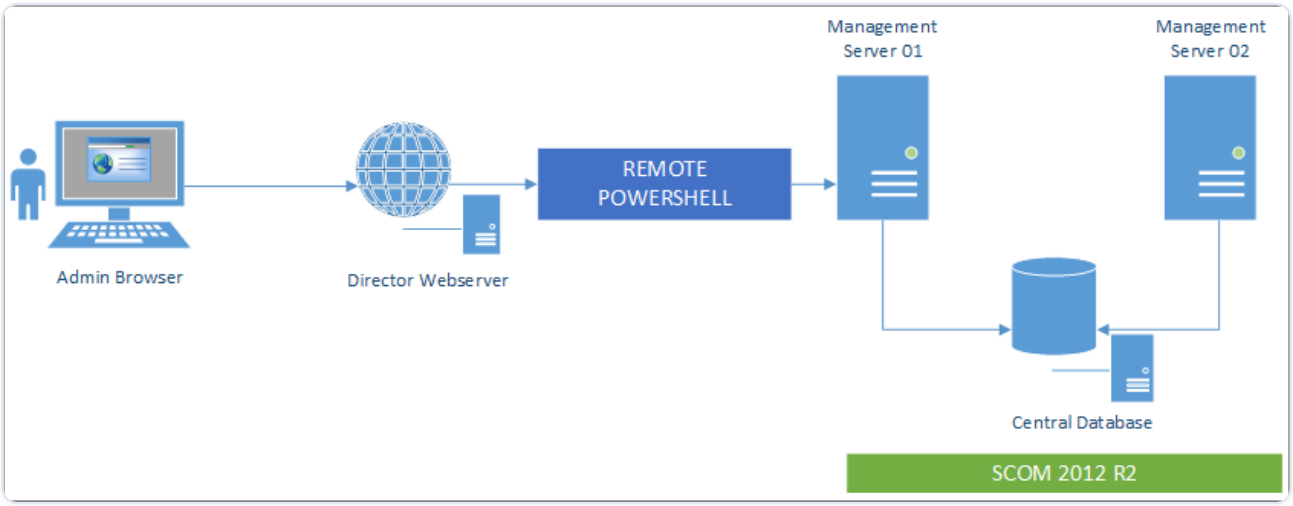
SCOMアラート統合の構成

DirectorとSCOMを統合すると、SCOMからのアラート情報をダッシュボードやDirectorの他の上位レベルのビューで表示できます。

SCOMアラートは、Citrixアラートとともに画面に表示されます。サイドバーのSCOMタブからSCOMアラートにアクセスしてドリルダウンできます。

1か月前までの履歴アラートを表示し、並べ替え、フィルター処理を行い、フィルター処理された情報をCSV、Excel、PDFレポート形式でエクスポートできます。詳細については、「レポートのエクスポート」を参照してください。

SCOM統合は、リモートPowerShell 3.0以降を使用してSCOM管理サーバーからデータをクエリし、ユーザーのDirectorセッションで永続的な実行空間接続を維持します。DirectorとSCOMサーバーは同じPowerShellバージョンである必要があります。



SCOM統合の要件は次のとおりです。

- ウィンドウズ サーバー 2012 R2
- システム センター 2012 R2 オペレーションズ マネージャー
- PowerShell 3.0以降（DirectorとSCOMサーバーのPowerShellバージョンは一致している必要があります）
- クアッドコアCPU、16 GB RAM（推奨）
- SCOMのプライマリ管理サーバーは、Directorのweb.configファイルで構成する必要があります。これはDirectorConfigツールを使用して実行できます。

Citrixでは、Directorで完全なアラート情報を取得できるように、Director管理者アカウントをSCOMオペレーターロールとして構成することをお勧めします。これが不可能な場合は、

DirectorConfigツールを使用して、SCOM管理者アカウントをweb.configファイルで構成できます。

Citrixでは、最適なパフォーマンスを確保するために、SCOM管理サーバーあたり10を超えるDirector管理者を構成しないことをさらに推奨します。

Directorサーバーで：

1. PowerShell リモート処理を有効にするには、**Enable-PSRemoting** と入力します。
2. SCOM管理サーバーをTrustedHostsリストに追加します。PowerShellプロンプトを開き、次のコマンドを実行します。
   - TrustedHostsの現在のリストを取得します

     Get-Item WSMAN:\localhost\Client\TrustedHosts
   - SCOM Management Server の FQDN を TrustedHosts のリストに追加します。\<Old Values\> は、Get-Item コマンドレットから返される既存のエントリのセットを表します。

     Set-Item WSMAN:\localhost\Client\TrustedHosts -Value "\<FQDN SCOM Management Server\>,\<Old Values\>"
3. DirectorConfig ツールを使用して SCOM を構成します。

   C:\inetpub\wwwroot\Director\ツール\DirectorConfig.exe /コンフィグSCOM

SCOM 管理サーバーで:

1. Director 管理者を SCOM 管理者ロールに割り当てます。
   a. SCOM 管理コンソールを開き、**管理** \> **セキュリティ** \> **ユーザーロール** に移動します。
   b. ユーザーロールでは、新しいユーザーロールを作成したり、既存のユーザーロールを変更したりできます。SCOM データへのアクセスの性質を定義する SCOM オペレーターロールには、4つのカテゴリがあります。たとえば、読み取り専用ロールでは、管理ペインが表示されず、ルール、マシン、アカウントを検出または管理できません。オペレーターロールは、完全な管理者ロールです。

      > **注：**
      >
      > Director 管理者が非オペレーターロールに割り当てられている場合、次の操作は利用できません。

> - 複数の管理サーバーが構成されており、プライマリ管理サーバーが利用できない場合、Director 管理者はセカンダリ管理サーバーに接続できません。プライマリ管理サーバーは、Director の web.config ファイルで構成されているサーバーであり、上記のステップ3で DirectorConfig ツールで指定されたサーバーと同じです。セカンダリ管理サーバーは、プライマリサーバーのピア管理サーバーです。
> - アラートをフィルタリングしている間、Director 管理者はアラートソースを検索できません。これにはオペレーターレベルの権限が必要です。

c. ユーザーロールを変更するには、ロールを右クリックし、**プロパティ** をクリックします。

d. ユーザーロールのプロパティダイアログで、指定されたユーザーロールから Director 管理者を追加または削除できます。

2. SCOM Management Server の Remote Management Users グループに Director 管理者を追加します。これにより、Director 管理者はリモート PowerShell 接続を確立できます。
3. PowerShell リモート処理を有効にするには、**Enable-PSRemoting** と入力します。
4. WS-Managementプロパティの制限を設定します。

a. MaxConcurrentUsersを変更します。

CLIの場合:

```
winrm set winrm/config/winrs @{MaxConcurrentUsers = "20"}
```

PSの場合:

```
Set-Item WSMan:\localhost\Shell\MaxConcurrentUsers 20
```

b. MaxShellsPerUserを変更します。

CLIの場合:

```
winrm set winrm/config/winrs @{MaxShellsPerUser="20"}
```

PSの場合:

```
Set-Item WSMan:\localhost\Shell\MaxShellsPerUser 20
```

a. MaxMemoryPerShellMBを変更します。

CLIの場合:

```
winrm set winrm/config/winrs @{MaxMemoryPerShellMB="1024"}
```

PSの場合:

```
Set-Item WSMan:\localhost\Shell\MaxMemoryPerShellMB 1024
```

5. SCOM統合が混在ドメイン環境で機能するように、次のレジストリエントリを設定します。

パス:
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`

キー: LocalAccountTokenFilterPolicy

種類: DWord

値: 1

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

SCOM統合が設定されると、「最新のSCOMアラートを取得できません。詳細については、Directorサーバーのイベントログを参照してください」というメッセージが表示されることがあります。サーバーのイベントログは、問題の特定と修正に役立ちます。原因としては、次のようなものが考えられます。

- DirectorまたはSCOMマシンでのネットワーク接続の喪失。
- SCOMサービスが利用できないか、応答できないほどビジーである。
- 構成されたユーザーの権限変更による認証の失敗。
- SCOMデータの処理中にDirectorでエラーが発生した。
- DirectorとSCOMサーバー間のPowerShellバージョンの不一致。

障害のトラブルシューティングのためにデータをフィルタリングする

ダッシュボードの数値をクリックするか、フィルターメニューから事前定義されたフィルターを選択すると、選択したマシンまたは障害タイプに基づいてデータを表示するフィルタービューが開きます。

事前定義されたフィルターは編集できませんが、事前定義されたフィルターをカスタムフィルターとして保存し、後で変更できます。また、すべてのデリバリーグループにわたるマシン、接続、セッション、およびアプリケーションインスタンスのカスタムフィルタービューを作成できます。

1. ビューを選択します。

- **マシン**。シングルセッションOSマシンまたはマルチセッションOSマシンを選択します。これらのビューには、構成されたマシンの数が表示されます。マルチセッションOSマシンのタブには、ロード評価インデックスも含まれており、これはパフォーマンスカウンターの分布と、リンクにカーソルを合わせると表示されるセッション数のツールヒントを示します。
- **セッション**。セッションビューからセッション数を確認することもできます。アイドル時間測定を使用して、しきい値期間を超えてアイドル状態のセッションを特定します。
- **接続**。過去60分、過去24時間、過去7日間など、異なる期間で接続をフィルターします。
- **アプリケーションインスタンス**。このビューには、サーバーおよびシングルセッションOSのVDA上のすべてのアプリケーションインスタンスのプロパティが表示されます。マルチセッションOSのVDA上のアプリケーションインスタンスでは、セッションアイドル時間測定が利用可能です。

> **注：**
>
> Windows 10 1809コンピューターにインストールされたVDAでデスクトップセッションを起動した場合、Directorのアクティビティマネージャーでは、Microsoft EdgeとOfficeがアクティブに実行されているアプリケーションとして表示されることがありますが、実際にはバックグラウンドでのみ実行されています。

2. **フィルター条件**で、基準を選択します。
3. 必要に応じて、各ビューの追加タブを使用してフィルターを完了します。
4. 必要に応じて、追加の列を選択してさらにトラブルシューティングを行います。
5. フィルターを保存して名前を付けます。
6. 複数のDirectorサーバーからフィルターにアクセスするには、それらのサーバーからアクセス可能な共有フォルダーにフィルターを保存します。
   - 共有フォルダーには、Directorサーバー上のアカウントに対する変更権限が必要です。
   - Directorサーバーは、共有フォルダーにアクセスするように構成する必要があります。構成するには、**IIS マネージャー**を実行します。**サイト \> 既定の Web サイト \> Director\ > アプリケーション設定**で、**Service.UserSettingsPath**設定を共有フォルダーのUNCパスを反映するように変更します。

7. 後でフィルターを開くには、**フィルター**メニューからフィルタータイプ（マシン、セッション、接続、またはアプリケーションインスタンス）を選択し、保存されたフィルターを選択します。
8. **エクスポート**をクリックして、データをCSV形式ファイルにエクスポートします。最大100,000レコードのデータをエクスポートできます。この機能は、Delivery Controller™バージョン1808以降で利用可能です。
9. 必要に応じて、**マシン**または**接続**ビューでは、フィルターされたリストで選択したすべてのマシンに対して電源コントロールを使用します。セッションビューでは、セッションコントロールまたはメッセージ送信オプションを使用します。
10. **マシン**ビューと**接続**ビューで、失敗したマシンまたは接続の**失敗理由**をクリックすると、失敗の詳細な説明と、失敗のトラブルシューティングに推奨されるアクションが表示されます。マシンおよび接続の失敗理由と推奨されるアクションについては、Citrix Director 7.12 Failure Reasons Troubleshooting Guideを参照してください。
11. **マシン**ビューで、マシン名リンクをクリックすると、対応する**マシン詳細**ページに移動します。このページには、マシンの詳細が表示され、電源コントロールが提供され、CPU、メモリ、ディスク監視、および GPU 監視グラフが表示されます。また、**履歴使用率の表示**をクリックすると、マシンのリソース使用率の傾向を確認できます。詳細については、マシンのトラブルシューティングを参照してください。
12. **アプリケーションインスタンス**ビューで、しきい値期間より長い**アイドル時間**に基づいて並べ替えまたはフィルターします。終了するアイドル状態のアプリケーションインスタンスを選択します。アプリケーションインスタンスのログオフまたは切断は、同じセッション内のすべてのアクティブなアプリケーションインスタンスを終了します。詳細については、アプリケーションのトラブルシューティングを参照してください。Director、Delivery Controller、およびVDAがバージョン7.13以降の場合、アプリケーションインスタンスフィルターページとセッションフィルターページのアイドル時間測定が利用可能です。

注: Citrix Studioでは、配信グループ内の単一のVDAに、異なるユーザーまたはユーザーグループに対して複数のデスクトップ割り当てルール（DAR）を割り当てることができます。StoreFront™は、ログインユーザーのDARに従って、対応する表示名で割り当てられたデスクトップを表示します。ただし、DirectorはDARをサポートしておらず、ログインユーザーに関係なく、配信グループ名を使用して割り当てられたデスクトップを表示します。その結果、Directorで特定のデスクトップをマシンにマッピングすることはできません。StoreFrontに表示される割り当てられたデスクトップをDirectorに表示される配信グループ名にマッピングするには、次のPowerShellコマンドを使用します。

```
Get-BrokerDesktopGroup | Where-Object { $\_.Uid -eq (Get-
BrokerAssignmentPolicyRule | Where-Object { $\_.PublishedName -eq "\<Name
on StoreFront\>" }).DesktopGroupUid } | Select-Object -Property Name, Uid
```

サイト全体の履歴トレンドを監視する

トレンドビューは、以下のパラメータについて、各サイトの履歴トレンド情報にアクセスします。

- セッション
- 接続障害
- マシン障害
- ログオンパフォーマンス
- 負荷評価
- キャパシティ管理
- マシン使用状況
- リソース使用率
- 各サイトのネットワーク分析。

この情報を見つけるには、**トレンド**メニューをクリックします。

ズームイン ドリルダウン機能を使用すると、期間をズームイン（グラフのデータポイントをクリック）し、トレンドに関連する詳細を表示するためにドリルダウンすることで、トレンドグラフをナビゲートできます。この機能により、誰が、または何が影響を受けているかの詳細をよりよく理解できます。

各グラフのデフォルトのスコープを変更するには、データに別のフィルターを適用します。

履歴トレンド情報が必要な期間を選択してください。期間の利用可能性は、Directorの展開によって次のように異なります。

- Premiumライセンスサイトでは、最大1年間 (365日) のトレンドレポートを利用できます。
- Advancedライセンスサイトでは、最大1か月間 (31日) のトレンドレポートを利用できます。
- PremiumおよびAdvanced以外のライセンスサイトでは、最大7日間のトレンドレポートを利用できます。

注：

- すべてのDirector展開において、期間が「先月」（**現在まで**）以下に設定されている場合、セッション、障害、ログオンパフォーマンスのトレンド情報はグラフとテーブルとして利用できます。期間がカスタム終了日を指定した「先月」または「昨年」として選択されている場合、トレンド情報はグラフとして利用でき、テーブルとしては利用できません。
- Monitor Serviceのグルーミング保持値によって、トレンドデータの可用性が制御されます。デフォルト値は、データ粒度と保持で確認できます。Premiumライセンスサイトのお客様は、グルーミング保持を希望する保持日数に変更できます。
- IIS Managerの以下のパラメータは、選択可能なカスタム終了日の範囲を制御します。ただし、選択された日付のデータ可用性は、測定される特定のメトリックのグルーミング保持設定によって異なります。

パラメーター	デフォルト値
UI.TrendsLast2HoursRange	3
UI.TrendsLast24HoursRange	32
UI.TrendsLast7DaysRange	32
UI.TrendsLastMonthRange	365

利用可能なトレンド

セッションの傾向を表示: 「**セッション**」タブから、デリバリーグループと期間を選択して、同時セッション数に関する詳細情報を表示します。

「**セッションの自動再接続**」列には、セッション内の自動再接続の数が表示されます。自動再接続は、セッションの信頼性ポリシーまたはクライアント自動再接続ポリシーが有効な場合に有効になります。エンドポイントでネットワークの中断が発生した場合、次のポリシーが有効になります。

- セッションの信頼性が有効になり（デフォルトで3分間）、Citrix Receiver™またはCitrix Workspace™アプリがVDAへの接続を試行します。
- クライアント自動再接続が3分から5分の間に有効になり、クライアントがVDAへの接続を試行します。

両方の再接続がキャプチャされ、ユーザーに表示されます。この情報は、再接続が発生してからDirector UIに表示されるまでに最大5分かかる場合があります。

自動再接続情報は、中断のあるネットワーク接続の表示とトラブルシューティングに役立ちます。また、シームレスなエクスペリエンスを持つネットワークも分析します。フィルターで選択した特定のデリバリーグループまたは期間の再接続数を表示できます。ドリルダウンでは、セッションの信頼性やクライアント自動再接続、タイムスタンプ、エンドポイントIP、Workspaceアプリがインストールされているマシンのエンドポイント名などの追加情報が提供されます。

デフォルトでは、ログはイベントのタイムスタンプの降順でソートされます。この機能は、Windows用Citrix Workspaceアプリ、Mac用Citrix Workspaceアプリ、Windows用Citrix Receiver、およびMac用Citrix Receiverで利用できます。この機能には、Delivery Controller™バージョン7 1906以降、およびVDA 1906以降が必要です。

セッションの再接続の詳細については、「セッション」を参照してください。

ポリシーの詳細については、「クライアント自動再接続ポリシー設定」および「セッションの信頼性ポリシー設定」を参照してください。

自動再接続データがDirectorに表示されない場合があります。その理由は次のとおりです。

- WorkspaceアプリがVDAに自動再接続データを送信していません。
- VDAがモニターサービスにデータを送信していません。
- Delivery Controllerは、対応するセッションがない可能性があるため、VDAペイロードを破棄します。

> **注：**
>
> 特定のCitrix Gatewayポリシーが設定されている場合、クライアントIPアドレスが正しく取得されないことがあります。

> **接続障害の傾向を表示:** 「障害」タブから、接続、マシンタイプ、障害タイプ、デリバリーグループ、および期間を選択して、サイト全体のユーザー接続障害に関する詳細情報を含むグラフを表示します。

マシン障害の傾向を表示: Single-session OS Machine FailuresタブまたはMulti-session OS Machinesタブから、障害タイプ、デリバリーグループ、および期間を選択すると、サイト全体のマシン障害に関する詳細情報を含むグラフが表示されます。

ログオンパフォーマンスの傾向を表示: ログオンパフォーマンスタブから、デリバリーグループと期間を選択して、サイト全体のユーザーログオン時間の詳細情報と、ログオン数がパフォーマンスに影響するかどうかを示すグラフを表示します。このビューには、ブローカー処理時間やVM起動時間など、ログオンフェーズの平均時間も表示されます。 このデータはユーザーログオン専用であり、切断されたセッションから再接続しようとするユーザーは含まれません。 グラフの下の表には、ユーザーセッションごとのログオン時間が表示されます。表示する列を選択し、任意の列でレポートを並べ替えることができます。 詳しくは、「ユーザーログオンの問題の診断」を参照してください。

負荷評価の傾向を表示: Load Evaluator Indexタブから、Multi-session OSマシン間で分散される負荷に関する詳細情報を含むグラフを表示します。このグラフのフィルターオプションには、デリバリーグループまたはデリバリーグループ内のMulti-session OSマシン、Multi-session OSマシン（デリバリーグループ内のMulti-session OSマシンが選択されている場合にのみ利用可能）、および範囲が含まれます。

ホストされたアプリケーションの使用状況を表示: この機能の利用可能性は、組織のライセンスによって異なります。 **Capacity Management**タブから、**Hosted Applications Usage**タブを選択します。デリバリーグループと期間を選択すると、ピーク時の同時使用状況を示すグラフと、アプリケーションベースの使用状況を示す表が表示されます。Application Based Usage表から、特定のアプリケーションを選択して詳細と、そのアプリケーションを使用している、または使用したユーザーのリストを確認できます。

Single-sessionおよびMulti-session OSの使用状況を表示: トレンドビューには、サイト別およびデリバリーグループ別のSingle-session OSの使用状況が表示されます。**サイト**を選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、ユーザーごとの使用状況が表示されます。 トレンドビューには、サイト別、デリバリーグループ別、およびマシン別のMulti-session OSの使用状況も表示されます。**サイト**を選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、マシンごとおよびユーザーごとの使用状況が表示されます。マシンが選択されている場合は、ユーザーごとの使用状況が表示されます。

仮想マシンの使用状況を表示: マシン使用状況タブから、**シングルセッションOSマシンまたはマルチセッションOSマシン**を選択すると、VMの使用状況をリアルタイムで確認でき、サイトのキャパシティニーズを迅速に評価できます。 シングルセッションOSの可用性 - サイト全体または特定のデリバリーグループにおけるシングルセッションOSマシン（VDI）の可用性による現在の状態を表示します。 マルチセッションOSの可用性 - サイト全体または特定のデリバリーグループにおけるマルチセッションOSマシンの可用性による現在の状態を表示します。

注： 利用可能なカウンターに表示されるマシンの数には、メンテナンスモードのマシンが含まれます。

リソース使用率の表示: リソース使用率タブから、**シングルセッションOSマシンまたはマルチセッションOSマシン**を選択すると、CPUおよびメモリ使用量、IOPS、各VDIマシンのディスク待機時間に関する履歴トレンドデータを確認でき、より適切なキャパシティプランニングに役立ちます。 この機能には、Delivery ControllerおよびVDAの**バージョン7.11**以降が必要です。 グラフには、平均CPU、平均メモリ、平均IOPS、ディスク待機時間、ピーク時の同時セッションのデータが表示されます。マシンにドリルダウンして、CPUを消費している上位10個のプロセスのデータとグラフを表示できます。

注：

この表に表示されるプロセスが多すぎると、大量のデータが消費され、パフォーマンスに影響する可能性があります。これを避けるため、平均CPUまたは平均メモリが1%を超えるプロセスのみが表示されます。そのため、表には10未満のプロセスしか表示されない場合があります。

デリバリーグループと期間でフィルターします。CPU、メモリ使用量、およびピーク時の同時セッションのグラフは、過去2時間、24時間、7日間、月、年で利用できます。平均IOPSおよびディスク待機時間のグラフは、過去24時間、月、年で利用できます。

注：

- 履歴マシン使用率ページの「上位10プロセス」テーブルでデータを収集して表示するには、監視ポリシー設定の**プロセス監視を有効にする**を**許可**に設定する必要があります。このポリシーは、デフォルトで**禁止**に設定されています。すべてのリソース使用率データはデフォルトで収集されます。これは、**リソース監視を有効にする**ポリシー設定を使用して無効にできます。グラフの下のテーブルには、マシンごとのリソース使用率データが表示されます。詳細については、「監視ポリシー設定」を参照してください。
- 平均IOPSは日次平均を示します。ピークIOPSは、選択した期間のIOPS平均の最高値として計算されます。（IOPS平均とは、VDAで1時間中に収集されたIOPSの時間平均です）。

> **ネットワーク分析データの表示:** この機能の可用性は、組織のライセンスと管理者権限によって異なります。この機能には、Delivery Controllerの**バージョン7.11**以降が必要です。

ネットワークタブから、ネットワーク分析を監視します。これにより、ネットワークのユーザー、アプリケーション、デスクトップのコンテキストビューが提供されます。この機能により、DirectorはCitrix ADMからのHDX Insightレポートを通じて、展開におけるICAトラフィックの高度な分析を提供します。詳細については、「ネットワーク分析の構成」を参照してください。

アプリケーション障害の表示: アプリケーション障害タブには、VDA上の公開アプリケーションに関連する障害が表示されます。

この機能には、Delivery ControllerおよびVDAの**バージョン7.15**以降が必要です。Windows Vista以降を実行するシングルセッションOS VDA、およびWindows Server 2008以降を実行するマルチセッションOS VDAがサポートされています。 詳細については、「履歴アプリケーション障害監視」を参照してください。

デフォルトでは、マルチセッションOS VDAからのアプリケーション障害のみが表示されます。監視ポリシーを使用して、アプリケーション障害の監視を設定できます。詳細については、「監視ポリシー設定」を参照してください。

アプリケーションプローブの結果を表示: アプリケーションプローブの結果タブには、構成ページでプローブ用に構成されたアプリケーションのプローブ結果が表示されます。ここでは、アプリケーション起動の失敗が発生した起動段階が記録されます。

この機能には、Delivery ControllerおよびVDAの**バージョン7.18**以降が必要です。詳しくは、「アプリケーションプローブ」を参照してください。

カスタマイズされたレポートの作成: カスタムレポートタブは、監視データベースからリアルタイムおよび履歴データを表形式で含むカスタムレポートを生成するためのユーザーインターフェイスを提供します。

この機能には、Delivery Controllers **バージョン7.12**以降が必要です。

以前に保存したカスタムレポートクエリのリストから、**実行してダウンロード**をクリックしてレポートをCSV形式でエクスポートしたり、**ODataをコピー**をクリックして対応するODataクエリをコピーして共有したり、**編集**をクリックしてクエリを編集したりできます。 マシン、接続、セッション、またはアプリケーションインスタンスに基づいてカスタムレポートクエリを作成できます。マシン、デリバリーグループ、期間などのフィールドに基づいてフィルター条件を指定します。カスタムレポートに必要な追加の列を指定します。プレビューには、レポートデータのサンプ

ルが表示されます。カスタムレポートクエリを保存すると、保存されたクエリのリストに追加されます。

コピーしたODataクエリに基づいてカスタムレポートクエリを作成できます。これを行うには、ODataクエリオプションを選択し、コピーしたODataクエリを貼り付けます。結果のクエリは後で実行するために保存できます。

> **注：** ODataクエリを使用して生成されたプレビューおよびエクスポートレポートの列名はローカライズされておらず、英語で表示されます。

> グラフ上のフラグアイコンは、特定の期間における重要なイベントまたはアクションを示します。フラグにマウスを合わせ、クリックしてイベントまたはアクションを一覧表示します。

> **注：**
>
> - HDX™接続ログオンデータは、7より前のVDAでは収集されません。それより前のVDAの場合、グラフデータは0と表示されます。
> - Citrix Studioで削除されたデリバリーグループは、関連データが整理されるまで、Director Trendsフィルターで選択可能です。削除されたデリバリーグループを選択すると、保持期間までの利用可能なデータのグラフが表示されます。ただし、テーブルにはデータは表示されません。
> - アクティブなセッションを含むマシンをあるデリバリーグループから別のデリバリーグループに移動すると、新しいデリバリーグループの**リソース使用率と負荷評価インデックス**テーブルに、古いデリバリーグループと新しいデリバリーグループから統合されたメトリックが表示されます。

展開のトラブルシューティング

ヘルプデスク管理者として、問題を報告しているユーザーを検索し、そのユーザーに関連付けられているセッションまたはアプリケーションの詳細を表示できます。同様に、問題が報告されているマシンまたはエンドポイントを検索します。関連するメトリックを監視し、適切なアクションを実行することで、問題を迅速に解決します。

利用可能なアクションは次のとおりです。

- 応答しないアプリケーションまたはプロセスを終了する
- ユーザーのマシンでの操作をシャドウする
- 応答しないセッションからログオフする
- マシンを再起動する
- マシンをメンテナンスモードにする
- ユーザープロファイルをリセットする

アプリケーションのトラブルシューティング

アプリケーション分析

「**アプリケーション**」ビューには、アプリケーションベースの分析が単一の統合ビューで表示され、アプリケーションのパフォーマンスを効率的に分析および管理するのに役立ちます。サイトに公開されているすべてのアプリケーションの正常性と使用状況に関する貴重な情報を得ることができます。デフォルトビューは、上位の実行中アプリケーションを特定するのに役立ちます。この機能には、Delivery Controllersバージョン7.16以降およびVDAsバージョン7.15以降が必要です。

「アプリケーション」ページ(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/dir-app-analytics.png)

「**プローブ結果**」列には、過去24時間で実行されたアプリケーションプローブの結果が表示されます。プローブ結果リンクをクリックすると、「**傾向**」\>「**アプリケーションプローブ結果**」ページで詳細を確認できます。アプリケーションプローブの構成方法の詳細については、「アプリケーションプローブ」を参照してください。

「**インスタンス**」列には、アプリケーションの使用状況が表示されます。これは、現在実行中のアプリケーションインスタンスの数（接続済みおよび切断済みの両方のインスタンス）を示します。さらにトラブルシューティングを行うには、「**インスタンス**」フィールドをクリックして、対応する「**アプリケーションインスタンス**」フィルターページを表示します。ここで、ログオフまたは切断するアプリケーションインスタンスを選択できます。

> **注：**
>
> カスタムスコープ管理者向けには、Directorはアプリケーショングループの下に作成されたアプリケーションインスタンスを表示しません。すべてのアプリケーションインスタンスを表示するには、完全な管理者である必要があります。詳細については、Knowledge Centerの記事「CTX256001」を参照してください。

> 「**アプリケーション障害**」および「**アプリケーションエラー**」列を使用して、サイトに公開されているアプリケーションの正常性を監視します。これらの列には、過去1時間に該当するアプリケーションの起動中に発生した障害とエラーの集計数が表示されます。「**アプリケーション障害**」または「**アプリケーションエラー**」フィールドをクリックすると、選択したアプリケーションに対応する「**傾向**」\>「**アプリケーション障害**」ページで障害の詳細を確認できます。

アプリケーション障害ポリシー設定は、障害とエラーの可用性と表示を管理します。ポリシーとその変更方法の詳細については、「**監視ポリシー**」設定の「アプリケーション障害監視のポリシー」を参照してください。

リアルタイムアプリケーション監視

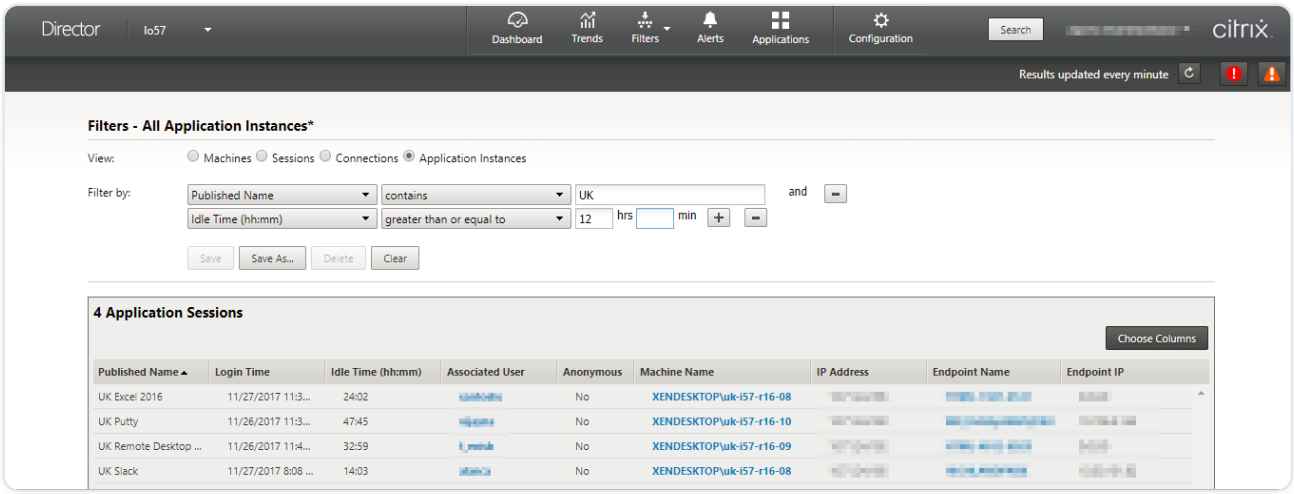
アイドル時間メトリックを使用して、特定の時間制限を超えてアイドル状態になっているインスタンスを特定することで、アプリケーションとセッションのトラブルシューティングを行うことができます。

アプリケーションベースのトラブルシューティングの典型的なユースケースは、従業員がアプリケーションライセンスを共有する医療分野にあります。そこでは、Citrix Virtual Apps and Desktops™環境をパージしたり、パフォーマンスの低いサーバーを再構成したり、アプリケーションを保守およびアップグレードしたりするために、アイドル状態のセッションとアプリケーションインスタンスを終了する必要があります。

アプリケーションインスタンスフィルターページには、サーバーおよびシングルセッションOSのVDA上のすべてのアプリケーションインスタンスが一覧表示されます。関連するアイドル時間測定値は、少なくとも10分間アイドル状態であったマルチセッションOSのVDA上のアプリケーションインスタンスに対して表示されます。

> **注:** アプリケーションインスタンスのメトリックは、すべてのライセンスエディションのサイトで利用できます。

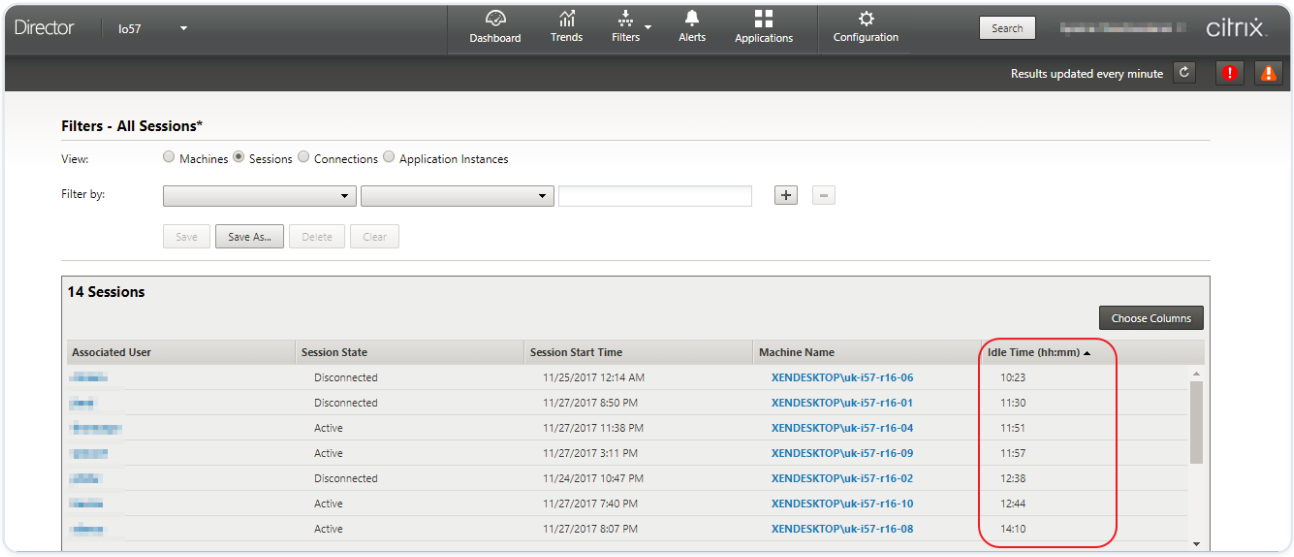
> この情報を使用して、特定の期間を超えてアイドル状態になっているアプリケーションインスタンスを特定し、必要に応じてログオフまたは切断します。これを行うには、**フィルター \> アプリケーションインスタンス**を選択し、事前に保存されたフィルターを選択するか、**すべてのアプリケーションインスタンス**を選択して独自のフィルターを作成します。



フィルターの例は次のとおりです。**フィルター条件**として、**公開名**（アプリケーションの）と**アイドル時間**を選択します。次に、**アイドル時間**を特定の時間制限**以上**に設定し、再利用のためにフィルターを保存します。フィルターされたリストから、アプリケーションインスタンスを選択します。メッセージを送信するオプションを選択するか、**セッション制御**ドロップダウンから**ログオフ**または**切断**を選択してインスタンスを終了します。

> **注:** アプリケーションインスタンスをログオフまたは切断すると、現在のセッションがログオフまたは切断され、同じセッションに属するすべてのアプリケーションインスタンスが終了します。

セッションフィルターページから、セッションの状態とセッションアイドル時間メトリックを使用して、アイドル状態のセッションを特定できます。**アイドル時間**列で並べ替えるか、特定の時間制限を超えてアイドル状態になっているセッションを特定するためのフィルターを定義します。アイドル時間は、少なくとも10分間アイドル状態であったマルチセッションOSのVDA上のセッションに対して表示されます。



セッションまたはアプリケーションインスタンスが次の条件の場合、**アイドル時間**は**N/A**と表示されます。

- 10分以上アイドル状態になっていない場合、,
- シングルセッションOSのVDAで起動されている場合、または
- Version 7.12以前のVDAで起動されます。

アプリケーション障害の履歴監視

トレンド -\> **アプリケーション障害**タブには、VDA上の公開アプリケーションに関連する障害が表示されます。

アプリケーション障害の傾向は、PremiumおよびAdvancedライセンスサイトでは過去2時間、24時間、7日間、および1か月間利用できます。その他のライセンスタイプでは、過去2時間、24時間、および7日間利用できます。「Application Errors」をソースとしてイベントビューアにログ記録されたアプリケーション障害が監視されます。**エクスポート**をクリックすると、CSV、Excel、またはPDF形式でレポートを生成できます。

アプリケーション障害監視のグルーミング保持設定であるGroomApplicationErrorsRetentionDaysとGroomApplicationFaultsRetentionDaysは、Premiumおよび非Premiumライセンスサイトの両方で、デフォルトで1日に設定されています。この設定は、PowerShellコマンドを使用して変更できます。

```
Set-MonitorConfiguration -\<setting name\> \<value\>
```

アプリケーション障害の傾向(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/dir_application_faults.png)

障害は、その重大度に基づいて**アプリケーションフォールト**または**アプリケーションエラー**として表示されます。アプリケーションフォールトタブには、機能またはデータの損失に関連する障害が表示されます。アプリケーションエラーは、すぐには関連しない問題を示し、将来問題を引き起こす可能性のある状態を示します。

公開アプリケーション名、**プロセス名**、**デリバリーグループ**、および**期間**に基づいて障害をフィルタリングできます。テーブルには、フォールトまたはエラーコードと障害の簡単な説明が表示されます。詳細な障害の説明はツールチップとして表示されます。

> **注:** 対応するアプリケーション名を導出できない場合、公開されたアプリケーション名は「不明」と表示されます。これは通常、起動されたアプリケーションがデスクトップセッ

ションで失敗した場合、または依存する実行可能ファイルによって引き起こされた未処理の例外が原因で失敗した場合に発生します。

デフォルトでは、マルチセッションOS VDAでホストされているアプリケーションの障害のみが監視されます。監視グループポリシー（アプリケーション障害の監視を有効にする、シングルセッションOS VDAでのアプリケーション障害の監視を有効にする、障害監視から除外されるアプリケーションのリスト）を通じて監視設定を変更できます。詳細については、監視ポリシー設定のアプリケーション障害監視のポリシーを参照してください。

トレンド \> アプリケーションプローブ結果ページには、過去24時間および7日間にサイトで実行されたアプリケーションプローブの結果が表示されます。アプリケーションプローブの構成方法の詳細については、アプリケーションプローブを参照してください。

アプリケーションプロービング

アプリケーションプロービングは、サイトで公開されているCitrix Virtual Apps™の健全性チェックプロセスを自動化します。アプリケーションプロービングの結果はDirectorで利用できます。

要件:

- Delivery Controllerはバージョン7.18以降を実行していること。
- プローブエージェントを実行するエンドポイントマシンは、Citrix Receiver for Windowsバージョン4.8以降、またはCitrix Workspaceアプリ for Windows（旧Citrix Receiver for Windows）バージョン1808以降を搭載したWindowsマシンです。Unified Windows Platform（UWP）用Workspaceアプリはサポートされていません。
- DirectorとStoreFront™は、デフォルトのフォームベース認証をサポートしています。

アプリケーションプロービングの実行に必要なユーザーアカウント/権限:

- 各エンドポイントマシンでプローブを実行するための固有のStoreFrontユーザー。StoreFrontユーザーは管理者である必要はありません。プローブは非管理者コンテキストで実行できます。
- エンドポイントマシンにCitrix Probe Agentをインストールおよび構成するためのWindows管理者権限を持つユーザーアカウント
- フル管理者ユーザーアカウント、または以下の権限を持つカスタムロール。アプリケーションプロービングに既存のユーザーアカウントを再利用すると、ユーザーのアクティブセッションからログオフされる可能性があります。
    - デリバリーグループの権限:

    - 読み取り専用
  - Directorの権限:
    - アラートメールサーバー構成の作成\\編集\\削除 - (メールサーバーがまだ構成されていない場合)
    - プローブ構成の作成\\編集\\削除
    - 構成ページの表示
    - トレンドページの表示

アプリケーションプロービングの構成

アプリケーションプローブは、複数の地域でオフピーク時に実行するようにスケジュールできます。包括的なプローブ結果は、ユーザーが問題に遭遇する前に、アプリケーション、ホストマシン、または接続に関連する問題をトラブルシューティングするのに役立ちます。

Citrix Probe Agentバージョン2103は、サイト集約をサポートしています。アプリケーションとデスクトップは、集約されたサイトから列挙および起動できます。プローブエージェントを構成する際に、集約されたサイトからのアプリケーションとデスクトップの列挙を有効にするには、**Workspace (StoreFront) Site Aggregation Enabled**オプションを選択します。以下のサイトの組み合わせがサポートされています。

- 1つの StoreFront URL を持つ複数のオンプレミスサイト。
- StoreFront または Workspace URL のいずれかを持つオンプレミスサイトとクラウドサイト。
- 1つの Workspace URL を持つ複数のクラウドサイト。

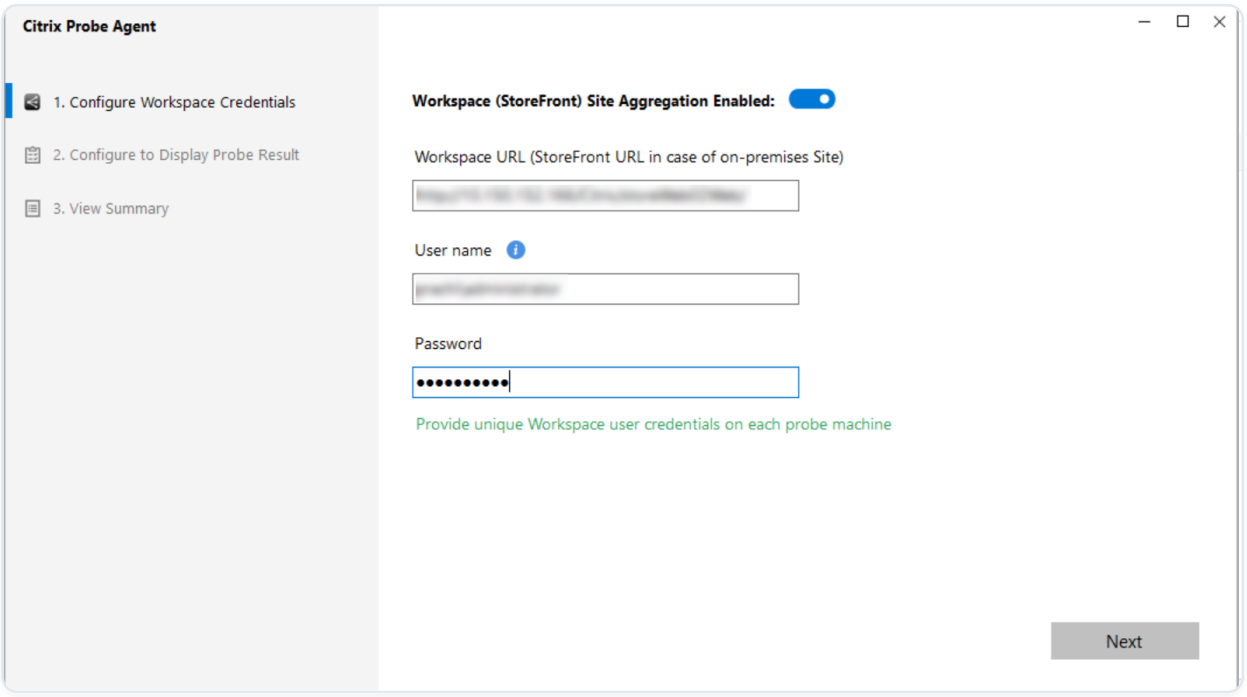
> **注：**
>
> 1つのサイトにのみアクセスできるプローブを構成するには、個別の管理者またはユーザーを作成する必要があります。

ステップ1：CITRIX PROBE AGENTをインストールして構成する

Citrix Probe Agentは、StoreFrontを介したユーザーによる実際のアプリケーション起動をシミュレートするWindows実行可能ファイルです。Directorで構成されたアプリケーション起動をテストし、その結果をDirectorに報告します。

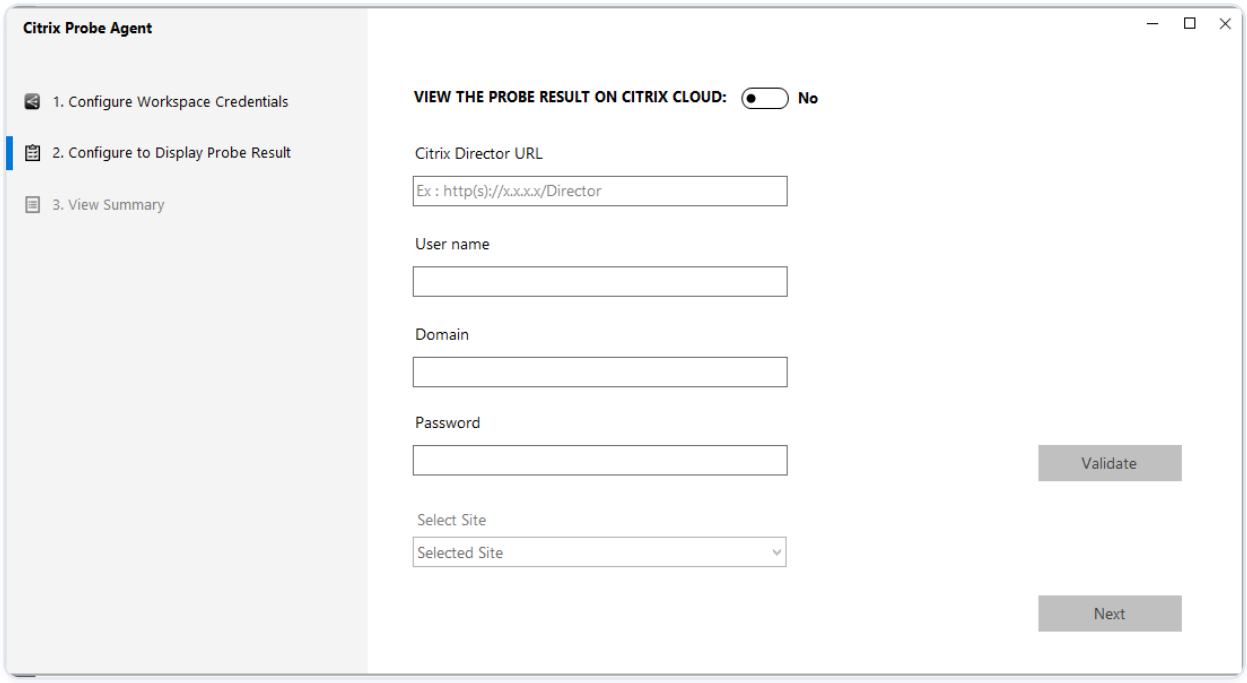
1. アプリケーションプロービングを実行するエンドポイントマシンを特定します。

2. 管理者権限を持つユーザーは、エンドポイントマシンにCitrix Probe Agentをインストールおよび構成できます。`<https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html>`で入手可能なCitrix Probe Agent実行可能ファイルをダウンロードします。
3. エージェントを起動し、StoreFront Receiver for Webの資格情報を構成します。各エンドポイントマシンで固有のStoreFrontユーザーを構成します。資格情報は暗号化され、安全に保存されます。



> **注：**
>
> ネットワーク外部から調査対象サイトにアクセスするには、StoreFront URLフィールドにCitrix GatewayのログインURLを入力します。Citrix Gatewayは、要求を対応するサイトのStoreFront URLに自動的にルーティングします。この機能は、Citrix Gatewayバージョン12.1以降（RfWebUIテーマ）およびDelivery Controllers 1811以降で利用できます。

4. タブで、Director の資格情報を入力し、 をクリックします。



5. サイトを選択し、**次へ**をクリックします。

ステップ2：DIRECTORでアプリケーションプロービングを構成する

制限事項:

対話型ログオンメッセージバナーが有効になっているWindows VDAからアプリケーションがテスト起動されると、プロービングは失敗します。これは、対話型ログオンメッセージの承認を待機している間にタイムアウトが発生するためです。 サーバーVDAでログオンメッセージを無効にするには。コンピューターの構成 > Windowsの設定 > セキュリティの設定 > ローカルポリシー > セキュリティオプションに移動します。

以下のフィールドのテキストを削除し、Microsoftポリシーを更新します。

- 対話型ログオン: ログオンしようとしているユーザーへのメッセージテキスト
- 対話型ログオン: ログオンしようとしているユーザーへのメッセージタイトル

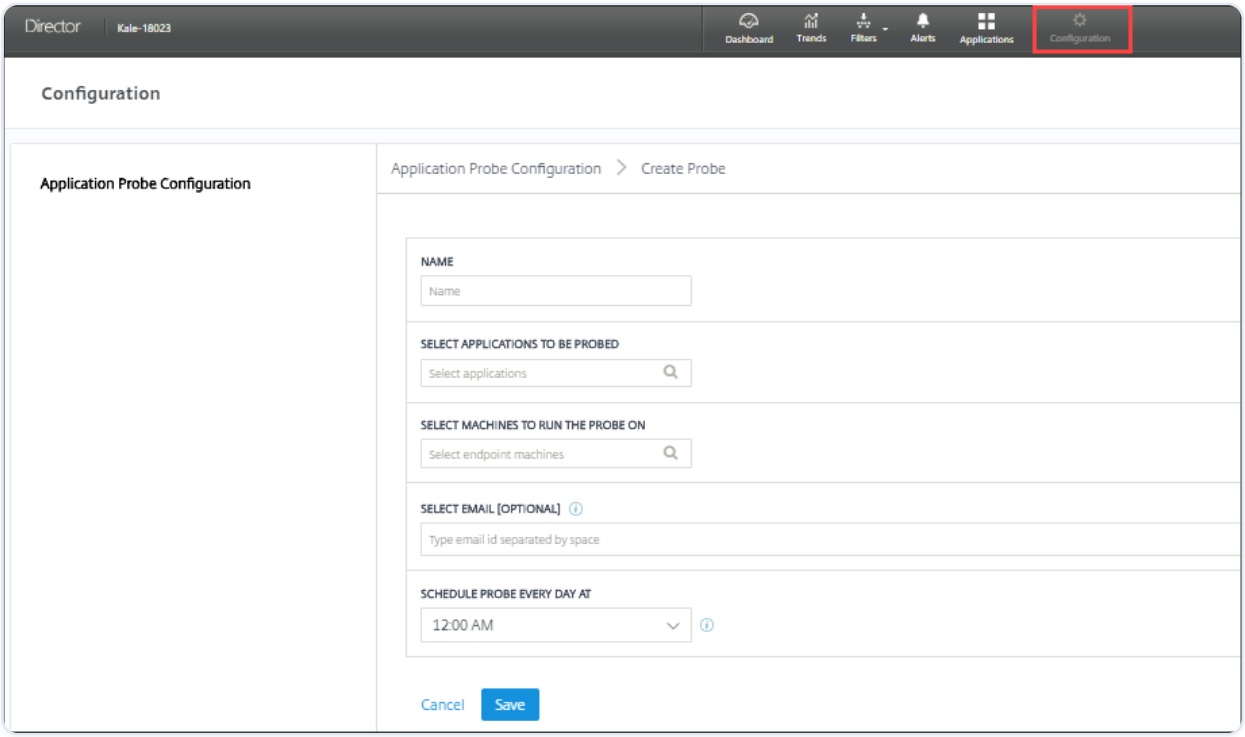
プローブがアプリケーション起動状態を通過できるように、対話型ログオンメッセージバナーを無効にしたこの特定のサーバーVDAにプローブユーザーを割り当てます。

> 詳細については、`<https://learn.microsoft.com/ja-jp/windows/security/threat-protection/security-policy-settings/interactive-logon-message-text-for-users-attempting-to-log-on>`を参照してください。

1. **構成** \> **アプリケーションプローブの構成**に移動します。
2. プローブを作成し、次を選択します。

   - プローブするアプリケーション、,
   - プローブを実行する必要があるエンドポイントマシン、,
   - 失敗したプローブ結果が送信されるメールアドレス（**アラート** -\> **メールサーバーの構成**でメールサーバーを構成します）、および
   - プローブを実行する必要がある時刻（エンドポイントマシンのローカルタイムゾーンに従って）。

   Directorでの構成後、エージェントはプロービングを開始する準備が整うまでに10分かかります。その後、次の時間から構成されたプローブを実行します。



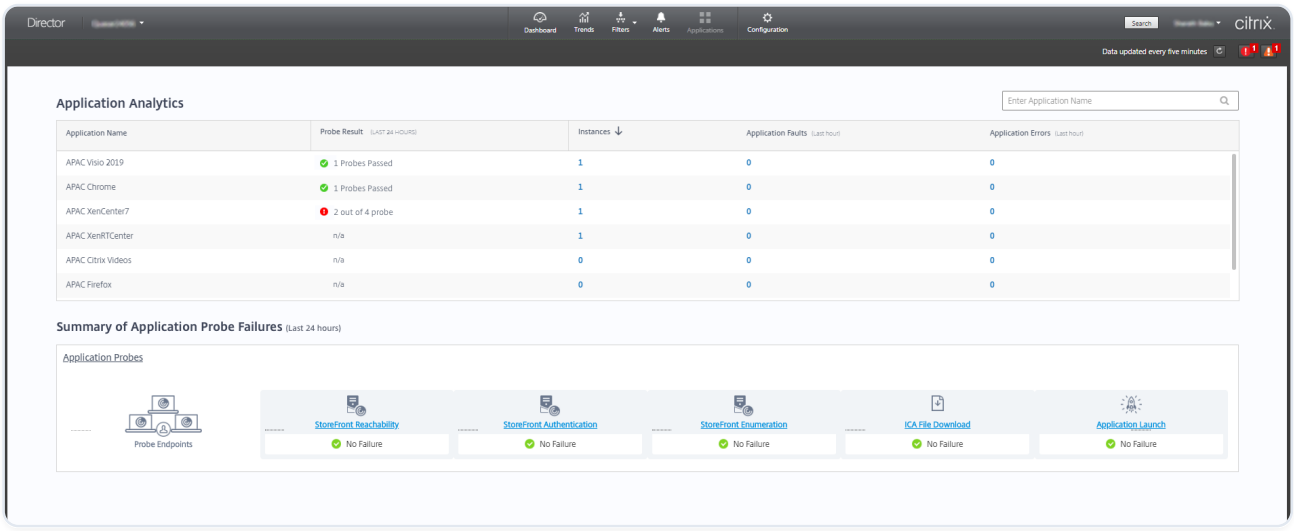
ステップ3：プローブの実行

エージェントは、Directorから定期的に取得するプローブ構成に従ってアプリケーションプロービングを実行します。StoreFrontを使用して、選択したアプリケーションを順次起動します。エージェントは、Monitorデータベースを介して結果をDirectorに報告します。失敗は、次の5つの特定の段階で報告されます。

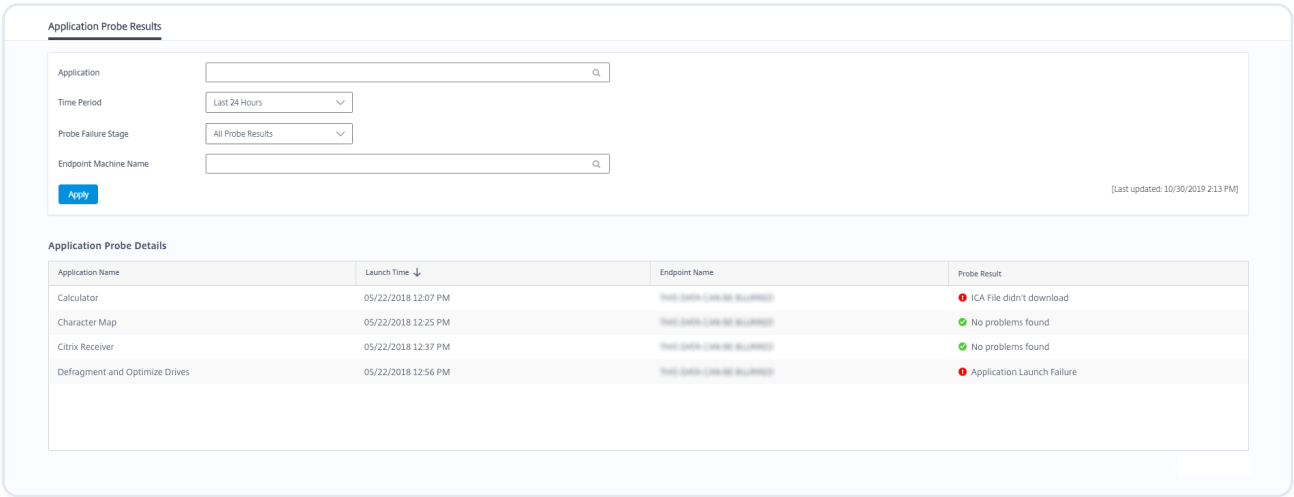
- **StoreFront到達可能性** - 構成されたStoreFront URLに到達できません。
- **StoreFront認証** - 構成されたStoreFront資格情報が無効です。
- **StoreFrontの列挙** - StoreFrontの列挙アプリケーションリストに、プローブ対象のアプリケーションが含まれていません。
- **ICA®ダウンロード** - ICAファイルが利用できません。
- **アプリケーションの起動** – アプリケーションを起動できません。

ステップ4：プローブ結果の表示

アプリケーションページで最新のプローブ結果を表示できます。



さらにトラブルシューティングを行うには、プローブ結果リンクをクリックして、**トレンド** \> **アプリケーションプローブ結果**ページで詳細を表示します。



このページでは、過去24時間または過去7日間の統合されたプローブ結果データを利用できます。プローブが失敗したステージを確認できます。特定のアプリケーション、プローブ失敗ステージ、またはエンドポイントマシンでテーブルをフィルタリングできます。

デスクトッププロービング

デスクトッププロービングは、サイトで公開されているCitrix Virtual Desktops™の正常性をチェックするプロセスを自動化します。デスクトッププロービングの結果はDirectorで確認できます。

Directorの［構成］ページで、プローブするデスクトップ、プローブを実行するエンドポイントマシン、およびプローブ時間を構成します。エージェントは、StoreFront™を使用して選択したデスクトップの起動をテストし、結果をDirectorに報告します。プローブ結果はDirector UIに表示されます。過去24時間のデータは［アプリケーション］ページに、過去のプローブデータは**［傾向］>［プローブ結果］>［デスクトッププローブ結果］**ページに表示されます。ここでは、プローブの失敗が発生した段階（StoreFront Reachability、StoreFront Authentication、StoreFront Enumeration、ICA download、またはDesktop launch）を確認できます。失敗レポートは、構成されたメールアドレスに送信されます。デスクトッププローブは、複数の地域でオフピーク時に実行するようにスケジュールできます。包括的な結果は、ユーザーが問題を経験する前に、プロビジョニングされたデスクトップ、ホストマシン、または接続に関連する問題をプロアクティブにトラブルシューティングするのに役立ちます。デスクトッププロービングは、Premiumライセンスサイトで利用できます。この機能には、Delivery Controllersバージョン7 1906以降、およびProbe Agent 1903以降が必要です。

要件:

- Delivery Controller™がバージョン1906以降を実行している。
- プローブエージェントを実行するエンドポイントマシンは、Citrix Receiver for Windowsバージョン4.8以降、またはCitrix Workspace app for Windows（旧Citrix Receiver for Windows）バージョン1906以降が動作するWindowsマシンです。Workspace app for Unified Windows Platform（UWP）はサポートされていません。
- DirectorとStoreFrontは、デフォルトのフォームベース認証をサポートしています。

デスクトッププロービングの実行に必要なユーザーアカウントまたは権限：

- 各エンドポイントマシンでプローブする一意のStoreFrontユーザー。StoreFrontユーザーは管理者である必要はありません。プローブは非管理者コンテキストで実行できます。
- エンドポイントマシンにCitrix Probe Agentをインストールおよび構成するためのWindows管理者権限を持つユーザーアカウント
- フル管理者ユーザーアカウント、または次の権限を持つカスタムロール。デスクトッププロービングに通常のユーザーアカウントを再利用すると、ユーザーのアクティブなセッションからログオフする可能性があります。
    - デリバリーグループの権限:

    - 読み取り専用
  - Directorの権限:
    - アラートメールサーバー構成の作成、編集、削除 - メールサーバーがまだ構成されていない場合
    - プローブ構成の作成、編集、削除
    - 構成ページの表示
    - トレンドページの表示

デスクトッププロービングの構成

デスクトッププローブは、複数の地域でオフピーク時に実行するようにスケジュールできます。包括的なプローブ結果は、ユーザーが問題を経験する前に、デスクトップ、ホストマシン、または接続に関連する問題をトラブルシューティングするのに役立ちます。

Citrix Probe Agentバージョン2103は、サイト集約をサポートしています。アプリケーションとデスクトップは、集約されたサイトから列挙および起動できます。プローブエージェントを構成する際に、集約されたサイトからのアプリケーションとデスクトップの列挙を有効にするには、**Workspace (StoreFront) Site Aggregation Enabled**オプションを選択します。以下のサイトの組み合わせがサポートされています。

- 1つの StoreFront URL を持つ複数のオンプレミスサイト。
- StoreFront または Workspace URL のいずれかを持つオンプレミスサイトとクラウドサイト。
- 1つの Workspace URL を持つ複数のクラウドサイト。

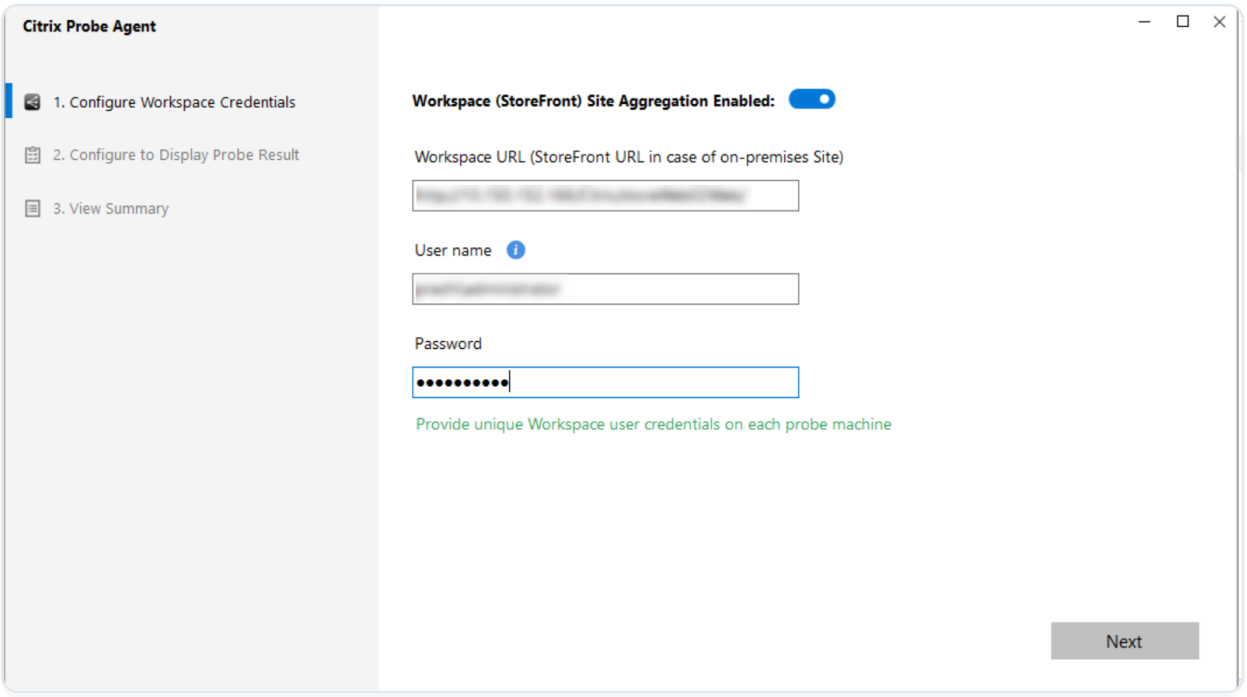
> **注：**
>
> 1つのサイトにのみアクセスできるプローブを構成するには、個別の管理者またはユーザーを作成する必要があります。

ステップ1：CITRIX PROBE AGENTをインストールして構成する

Citrix Probe Agentは、ユーザーがStoreFrontを介して実際のデスクトップ起動をシミュレートするWindows実行可能ファイルです。Directorで構成されたデスクトップ起動をテストし、結果をDirectorに報告します。

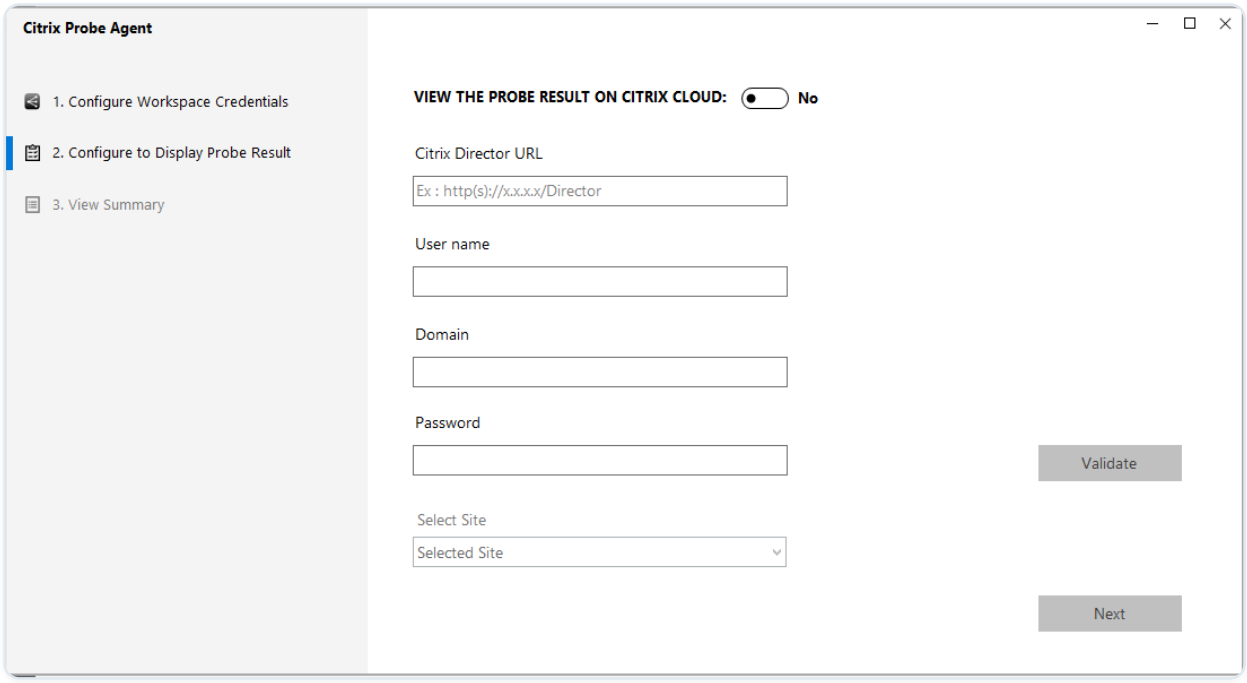
1. デスクトッププロービングを実行するエンドポイントマシンを特定します。

2. 管理者権限を持つユーザーは、エンドポイントマシンにCitrix Probe Agentをインストールして構成できます。Citrix Probe Agentの実行可能ファイルは`<https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html>`からダウンロードできます。
3. エージェントを起動し、StoreFront Receiver for Webの資格情報を構成します。各エンドポイントマシンで一意のStoreFrontユーザーを構成します。資格情報は暗号化され、安全に保存されます。



> **注：**
>
> - ネットワーク外部からプローブ対象サイトにアクセスするには、StoreFront URLフィールドにCitrix Gatewayのログインページ URLを入力します。Citrix Gatewayは、要求を対応するサイトのStoreFront URLに自動的にルーティングします。この機能は、Citrix Gatewayバージョン12.1以降、およびDelivery Controllers 1811以降で利用できます。
> - 構成された一意のStoreFrontユーザーに対して、対話型ログオンを有効にする必要があります。

4. タブで、Director の資格情報を入力し、 をクリックします。



5. サイトを選択し、**次へ**をクリックします。

ステップ2：DIRECTORでデスクトッププロービングを構成する

> **制限事項:**

> 対話型ログオンメッセージバナーが有効になっているWindows VDAからデスクトップがテスト起動されると、プロービングは失敗します。これは、対話型ログオンメッセージの承認を待機している間にタイムアウトが発生するためです。 サーバーVDAでログオンメッセージを無効にするには、 > > > > に移動します。

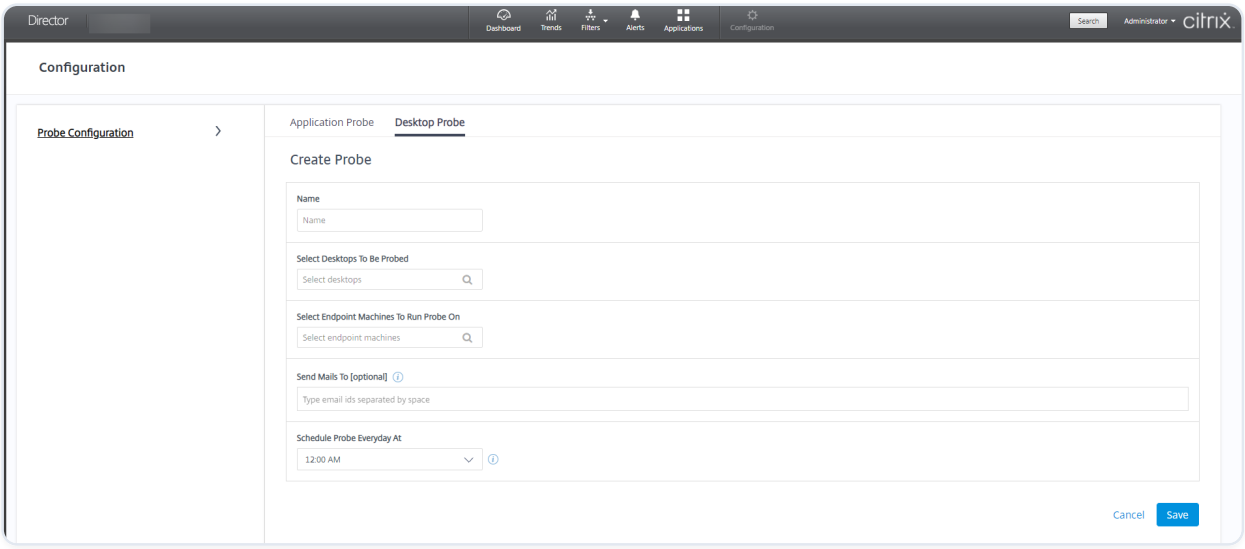
> 以下のフィールドのテキストを削除し、Microsoftポリシーを更新します。

> - 対話型ログオン: ログオンしようとしているユーザーへのメッセージテキスト
> - 対話型ログオン: ログオンしようとしているユーザーへのメッセージタイトル

> プローブがデスクトップ起動状態を通過できるように、対話型ログオンメッセージバナーが無効になっているこの特定のサーバーVDAにプローブユーザーを割り当てます。

> 詳細については、`<https://learn.microsoft.com/ja-jp/windows/security/threat-protection/security-policy-settings/interactive-logon-message-text-for-users-attempting-to-log-on>`を参照してください。

1. **構成** > **デスクトッププローブ構成** に移動します。
2. プローブを作成するには、詳細を入力して**保存**をクリックします。



注：

アラート > **メールサーバー構成** でメールサーバーを構成します。

デスクトッププロービングの構成が完了すると、エージェントはプロービングを開始する準備が整うまでに10分かかります。その後、次の時間から構成されたプローブを実行します。

ステップ3：プローブの実行

エージェントは、Directorから定期的に取得するプローブ構成に従ってデスクトッププロービングを実行します。StoreFrontを使用して、選択されたデスクトップを順次起動します。エージェントは、Monitorデータベースを介して結果をDirectorに報告します。障害は5つの特定の段階で報告されます。

- **StoreFront到達可能性** - 構成されたStoreFront URLに到達できません。
- **StoreFront認証** - 構成されたStoreFront資格情報が無効です。
- **StoreFront列挙** - StoreFrontのデスクトップ列挙リストに、プローブ対象のデスクトップが含まれていません。
- **ICA®ダウンロード** - ICAファイルが利用できません。
- **デスクトップ起動** – デスクトップを起動できません。

ステップ4：プローブ結果の表示

最新のプローブ結果は、**デスクトップ**ページで確認できます。

Directorデスクトップ分析ページ(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/dir-desktop-probe-results.png)

さらにトラブルシューティングを行うには、プローブ結果リンクをクリックして、**トレンド** > **プローブ結果** > **デスクトッププローブ結果**ページで詳細を確認します。

Directorデスクトッププローブ結果(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/dir-desktop-probing-trends.png)

このページでは、過去24時間または過去7日間の統合されたプローブ結果データを利用できます。プローブが失敗した段階を確認できます。特定のデスクトップ、プローブ失敗段階、またはエンドポイントマシンでテーブルをフィルタリングできます。

マシンのトラブルシューティング

> **注：**
>
> **Citrix Health Assistant** は、未登録のVDAにおける構成の問題をトラブルシューティングするためのツールです。このツールは、VDA登録の失敗、セッション起動の問題、タイムゾーンリダイレクト構成の問題の根本原因を特定するために、いくつかのヘルスチェックを自動化します。Knowledge Centerの記事「Citrix Health Assistant - Troubleshoot VDA Registration and Session Launch」には、**Citrix Health Assistant** ツールのダウンロードと使用方法が記載されています。

> Directorコンソールの **フィルター > マシン** ビューには、サイトで構成されているマシンが表示されます。「マルチセッションOSマシン」タブには、パフォーマンスカウンターの分布を示すロード評価インデックスと、リンクにカーソルを合わせるとセッション数のツールヒントが表示されます。

失敗したマシンの**失敗理由**列をクリックすると、失敗の詳細な説明と、その失敗のトラブルシューティングに推奨されるアクションが表示されます。マシンおよび接続の失敗に関する失敗理由と推奨されるアクションは、Citrix Director 7.12 Failure Reasons Troubleshooting Guideで確認できます。

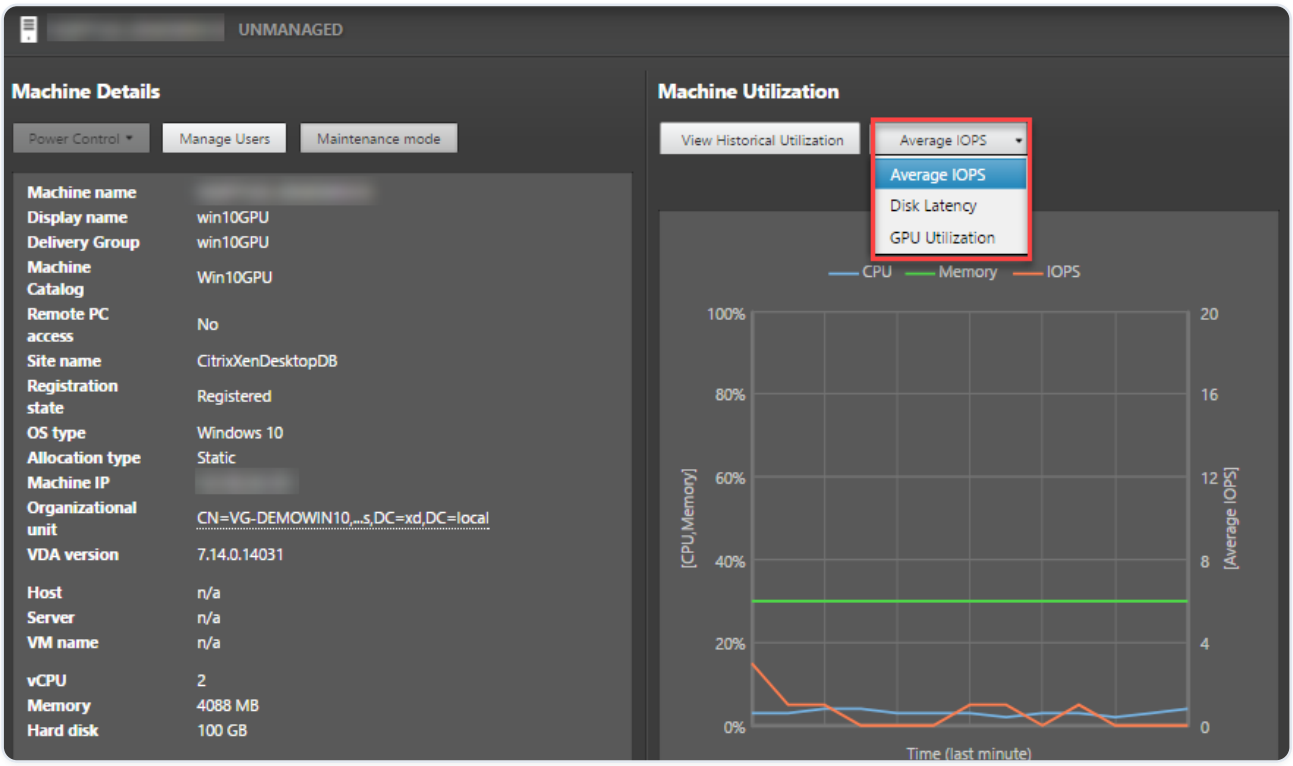
マシン名のリンクをクリックすると、**マシン詳細** ページに移動します。

マシン詳細ページには、マシンの詳細、インフラストラクチャの詳細、およびマシンに適用されたホットフィックスの詳細が一覧表示されます。

マシンベースのリアルタイムリソース使用率

マシン使用率パネルには、CPUとメモリのリアルタイム使用率を示すグラフが表示されます。さらに、Delivery ControllerとVDAのバージョンが**7.14**以降のサイトでは、ディスクおよびGPU監視グラフも利用できます。

ディスク監視グラフ、平均IOPS、およびディスク遅延は、VDAディスクに関連する問題を監視およびトラブルシューティングするのに役立つ重要なパフォーマンス測定値です。平均IOPSグラフは、ディスクへの読み取りおよび書き込みの平均数を表示します。**ディスク遅延**を選択すると、データ要求からディスクからの応答までの遅延（ミリ秒単位で測定）を示すグラフが表示されます。



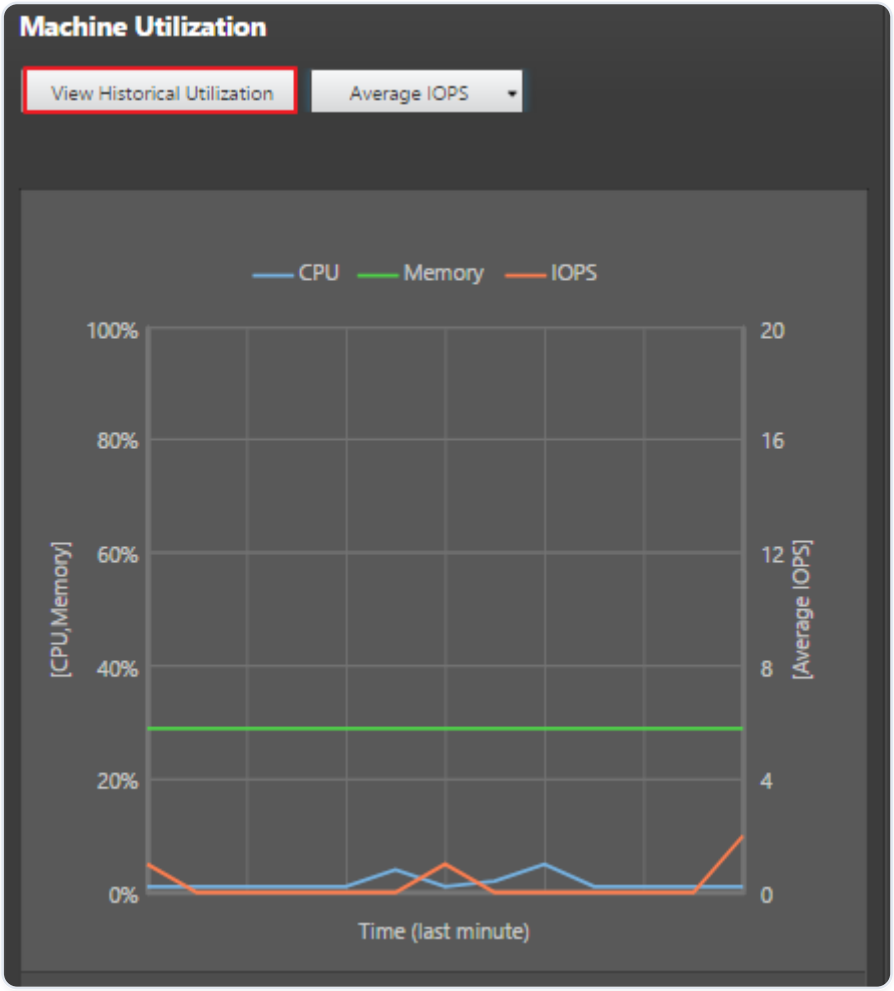
ServerまたはSingle-session OS VDAでGPU関連の問題をトラブルシューティングするには、**GPU使用率**を選択して、GPU、GPUメモリ、およびエンコーダーとデコーダーの使用率をパーセンテージで確認します。GPU使用率グラフは、NVIDIA Tesla M60 GPUを搭載し、ディスプレイドライバーバージョン369.17以降を実行している64ビットWindowsを実行しているVDAでのみ利用可能です。 VDAは、GPUアクセラレーションを提供するためにHDX™ 3D Proが有効になっている必要があります。詳しくは、「Windows Single-session OSのGPUアクセラレーション」および「Windows Multi-session OSのGPUアクセラレーション」を参照してください。 VDAが複数のGPUにアクセスする場合、使用率グラフには個々のGPUから収集されたGPUメトリックの平均が表示されます。GPUメトリックは、個々のプロセスではなく、VDA全体に対して収集されます。

マシンベースの履歴リソース使用率

マシン使用率パネルで、**履歴使用率の表示**をクリックして、選択したマシンのリソースの履歴使用率を表示します。 使用率グラフには、CPU、メモリ、ピーク時の同時セッション、平均IOPS、ディスク遅延の重要なパフォーマンスカウンターが含まれます。

> **注：**
>
> 監視ポリシー設定の**プロセス監視を有効にする**は、履歴マシン使用率ページの「上位10プロセス」テーブルでデータを収集および表示するために、「許可」に設定する必要があります。収集はデフォルトで禁止されています。

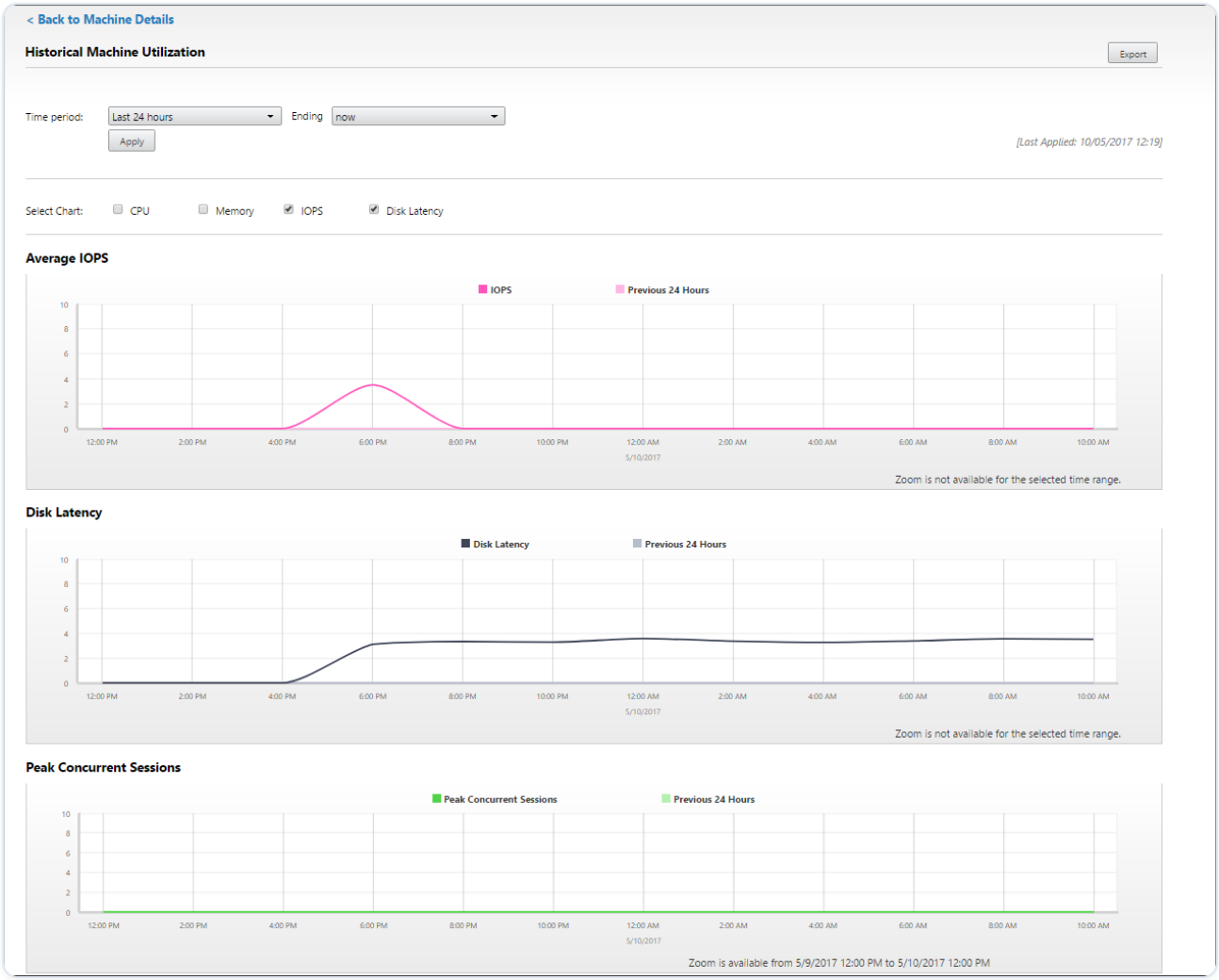
> CPUとメモリの使用率、平均IOPS、ディスク待機時間のデータはデフォルトで収集されます。**リソース監視を有効にする**ポリシー設定を使用して、この収集を無効にできます。



1. **マシン詳細**ビューの**マシン使用率**パネルから、**履歴使用率の表示**を選択します。
2. **履歴マシン使用率**ページで、**期間**を「過去2時間」、「過去24時間」、「過去7日間」、「月」、「年」に設定して使用状況を表示します。

> **注：**
>
> 平均IOPSとディスク遅延の使用状況データは、現在までの過去24時間、月、年についてのみ利用可能です。カスタム終了時刻はサポートされていません。

3. **適用**をクリックし、必要なグラフを選択します。
4. グラフの異なるセクションにカーソルを合わせると、選択した期間の詳細情報が表示されます。



たとえば、**過去2時間**を選択した場合、ベースライン期間は選択した時間範囲の前の2時間です。過去2時間とベースライン時間のCPU、メモリ、セッションの傾向を表示します。**過去1か月**を選択した場合、ベースライン期間は前月です。過去1か月とベースライン時間の平均IOPSとディスク待機時間を表示するように選択します。

1. 選択した期間のリソース使用率データをエクスポートするには、**エクスポート**をクリックします。詳しくは、「展開の監視」の「レポートのエクスポート」セクションを参照してください。

2. グラフの下の表には、CPUまたはメモリ使用率に基づいて上位10個のプロセスが一覧表示されます。選択した時間範囲におけるアプリケーション名、ユーザー名、セッションID、平均CPU、ピークCPU、平均メモリ、ピークメモリを表示する任意の列で並べ替えることができます。IOPSとディスク遅延の列は並べ替えることができません。

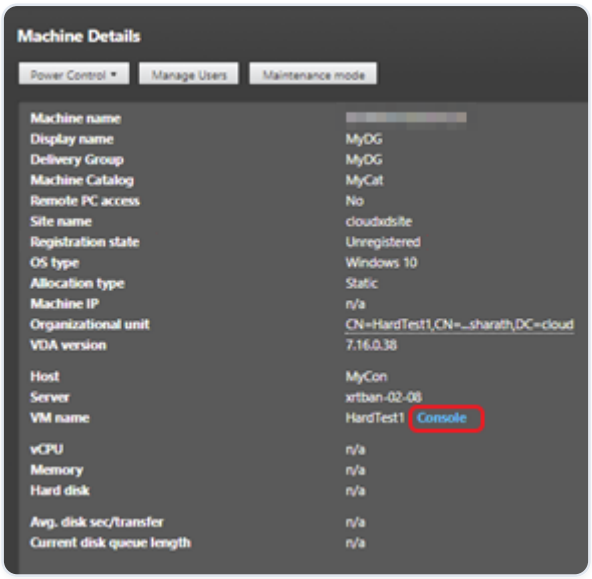
   > **注：**
   >
   > システムプロセスのセッションIDは「0000」と表示されます。

3. 特定のプロセスのリソース消費の履歴傾向を表示するには、上位10個のプロセスのいずれかをドリルダウンします。

マシンコンソールへのアクセス

XenServerバージョン7.3以降でホストされているシングルセッションおよびマルチセッションOSマシンのコンソールには、Directorから直接アクセスできます。これにより、XenServerでホストされているVDAの問題をトラブルシューティングするためにXenCenterは必要ありません。この機能を利用するには：

- バージョン7.16以降のDelivery Controllerが必要です。
- マシンをホストしているXenServerはバージョン7.3以降である必要があり、Director UIからアクセスできる必要があります。



マシンのトラブルシューティングを行うには、対応するマシン詳細パネルの**コンソール**リンクをクリックします。提供されたホスト資格情報が認証されると、WebベースのVNCクライアントで

あるnoVNCを使用して、マシンコンソールが別のタブで開きます。これで、コンソールにキーボードとマウスでアクセスできるようになります。

注：

- この機能はInternet Explorer 11ではサポートされていません。
- マシンコンソールのマウスカーソルがずれている場合は、問題を解決する手順についてCTX230727を参照してください。
- Directorは新しいタブでコンソールアクセスを起動します。ブラウザの設定でポップアップが許可されていることを確認してください。
- セキュリティ上の理由から、Citrix®はブラウザにSSL証明書をインストールすることを推奨しています。

Microsoft RDSライセンスの健全性

Multi-session OSマシンについては、**マシンの詳細**ページと**ユーザーの詳細**ページのマシン詳細パネルでMicrosoft RDSライセンスのステータスを表示できます。



次のいずれかのメッセージが表示されます。

- ライセンス利用可能
- 適切に構成されていません（警告）
- ライセンスエラー（エラー）
- 互換性のないVDAバージョン（エラー）

注：

有効なライセンスを持つ猶予期間中のマシンのMicrosoft RDSライセンスの正常性ステータスは、緑色で**ライセンス利用可能**というメッセージを表示します。ライセンスの有効期限が切れる前に更新してください。

警告メッセージとエラーメッセージについては、情報アイコンにカーソルを合わせると、次の表に示す追加情報が表示されます。

メッセージの種類	DIRECTOR内のメッセージ
エラー	VDAバージョン7.16以降で利用可能です。
エラー	新しいRDS接続は許可されません。
エラー	Microsoft RDSライセンスの猶予期間が過ぎました。
エラー	必要なOSレベルに対して、デバイスごとのクライアントアクセスライセンスの種類でライセンスサーバーが構成されていません。
エラー	構成されているライセンスサーバーは、デバイスごとのクライアントアクセスライセンスの種類でRDSホストOSレベルと互換性がありません。
警告	Personal Terminal Serverは、Citrix Virtual Apps and Desktops™展開において有効なRDSライセンスの種類ではありません。

メッセージの種類	DIRECTOR内のメッセージ
警告	管理用リモートデスクトップは、Citrix Virtual Apps and Desktops展開において有効なライセンスの種類ではありません。
警告	RDSライセンスの種類が構成されていません。
警告	ユーザーごとのクライアントアクセスRDSライセンスの種類では、ドメインコントローラーまたはライセンスサーバーに到達できません。
警告	デバイスごとのクライアントアクセスライセンスの種類では、必要なOSレベルのライセンスサーバーに到達できないため、クライアントデバイスライセンスを判別できません。

注：

この機能は、Microsoft RDS CAL (クライアントアクセスライセンス) にのみ適用されます。

ユーザーの問題のトラブルシューティング

Directorの**ヘルプデスク**ビュー（**アクティビティマネージャー**ページ）を使用して、ユーザーに関する情報を表示します。

- ユーザーのログオン、接続、およびアプリケーションに関する詳細を確認します。
- ユーザーのマシンをシャドウします。
- ICA®セッションを記録します。
- 以下の表に記載されている推奨されるアクションで問題をトラブルシューティングし、必要に応じて適切な管理者に問題をエスカレートしてください。

トラブルシューティングのヒント

ユーザーの問題	提案
ログオンに時間がかかる、または断続的または繰り返し失敗する	ユーザーログオンの問題を診断する
セッションの起動に時間がかかる、または断続的または繰り返し失敗する	セッション起動の問題を診断する
アプリケーションが遅い、または応答しない	アプリケーション障害の解決
接続に失敗しました	デスクトップ接続の復元
セッションが遅い、または応答しない	セッションの復元
セッションを記録する	セッションの記録
ビデオが遅い、または品質が悪い	HDXチャネルシステムレポートの実行

> **注：** マシンがメンテナンスモードでないことを確認するには、ユーザー詳細ビューからマシン詳細パネルを確認します。

検索のヒント

検索フィールドにユーザー名を入力すると、Directorは、Directorをサポートするように構成されているすべてのサイトのActive Directoryでユーザーを検索します。

検索フィールドにマルチユーザーマシンの名前を入力すると、Director は指定されたマシンのマシン詳細を表示します。

検索フィールドにエンドポイント名を入力すると、Directorは、特定のEndpointに接続されている認証されていない（匿名）セッションと認証済みセッションを使用します。これにより、認証されていないセッションのトラブルシューティングが可能になります。認証されていないセッションのトラブルシューティングを可能にするには、エンドポイント名が一意であることを確認してください。

検索結果には、現在マシンを使用していない、またはマシンに割り当てられていないユーザーも含まれます。

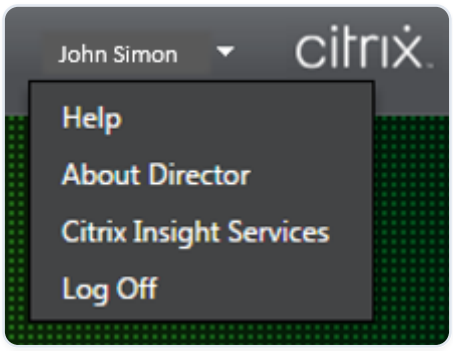
- 検索では大文字と小文字は区別されません。
- 部分的な入力では、一致する可能性のあるリストが生成されます。

- スペースで区切られた2つの部分からなる名前（ユーザー名、姓と名、または表示名）の数文字を入力すると、両方の文字列に一致する結果が表示されます。たとえば、「jo rob」と入力すると、「John Robertson」や「Robert, Jones」などの文字列が結果に含まれる場合があります。

ランディングページに戻るには、**Director ロゴ**をクリックします。

Citrix Insight Servicesへのアクセス

Directorの**ユーザー**ドロップダウンリストからCitrix Insight Services（CIS）にアクセスして、追加の診断情報を取得できます。CISで利用できるデータは、Call HomeやCitrix Scoutなどのソースから取得されます。



トラブルシューティング情報をCitrixテクニカルサポートにアップロードする

単一のDelivery Controller™またはVDAからCitrix Scoutを実行して、主要なデータポイントとCitrix Diagnostics Facility (CDF) トレースをキャプチャし、選択したコンピューターのトラブルシューティングを行います。Scoutは、データをCISプラットフォームに安全にアップロードして、Citrixテクニカルサポートのトラブルシューティングを支援する機能を提供します。Citrixテクニカルサポートは CISプラットフォームを使用して、顧客から報告された問題の解決時間を短縮します。

Scoutは、Citrix Virtual Apps and Desktops™コンポーネントとともにインストールされます。Windowsのバージョンによっては、Citrix Virtual Apps and Desktopsをインストールまたはアップグレードすると、ScoutがWindowsのスタートメニューまたはスタート画面に表示されます。

Scoutを起動するには、スタートメニューまたはスタート画面からCitrix \> Citrix Scoutを選択します。

Scoutの使用方法と構成、およびFAQについては、CTX130147を参照してください。

セッション起動の問題を診断する

ユーザーログオンの問題の診断セクションで述べられているログオンプロセスフェーズに加えて、Directorはセッション起動時間を表示します。これは、**ユーザーの詳細**ページと**マシンの詳細**ページで、Workspace Appセッション起動時間とVDAセッション起動時間に分けられます。これらの2

つの期間は、さらに個々のフェーズを含み、その起動時間も表示されます。このデータは、セッション起動時間の長さの原因を理解し、トラブルシューティングするのに役立ちます。さらに、セッション起動に関わる各フェーズの期間は、個々のフェーズに関連する問題のトラブルシューティングに役立ちます。たとえば、ドライブマッピングの時間が長い場合、GPOまたはスクリプトですべての有効なドライブが正しくマッピングされているか確認できます。この機能は、Delivery Controllerバージョン7 1906以降およびVDA 1903以降で利用可能です。

前提条件

セッション起動時間のデータが表示されるには、以下の前提条件が満たされていることを確認してください。

- デリバリーコントローラー™ 7 1906 以降。
- VDA 1903以降。
- Citrix End User Experience Monitoring (EUEM)サービスがVDAで実行されている必要があります。

制限事項

Directorがセッション起動時間のデータを表示する際には、以下の制限が適用されます。

- セッション起動時間は、HDX™セッションでのみ利用可能です。
- iOSおよびAndroid OSからのセッション起動の場合、VDA起動時間のみが利用可能です。
- ICA®ファイルダウンロード時間 (IFDCD) は、ブラウザから起動する際にWorkspace Appが検出された場合にのみ利用可能です。
- macOSからのセッション起動の場合、IFDCDはWorkspaceアプリ1902以降でのみ利用可能です。
- Windows OSからのセッション起動の場合、IFDCDはWorkspaceアプリ1902以降で利用可能です。それ以前のバージョンでは、Workspaceアプリが検出されたブラウザからのアプリ起動の場合にのみIFDCDが表示されます。

注:

- 前提条件が満たされた後もセッション起動時間の表示に問題がある場合は、CTX130320に記載されているDirectorサーバーおよびVDAログを確認してください。 共有セッション（同じセッションで複数のアプリケーションが起動された場合）の場合、Workspace Appの起動メトリックは、最新の接続または最新のアプリケーション起動に対して表示されます。

- VDAセッション起動の一部のメトリックは、再接続時には適用されません。そのような場合、メッセージが表示されます。

セッション起動(/en-us/citrix-virtual-apps-desktops/2203-ltsr/media/session_startup.png)

Workspace App セッション起動フェーズ

セッション起動クライアント期間 (SSCD)

このメトリックが高い場合、起動時間が長くなるクライアント側の問題を示しています。問題の根本原因を特定するために、後続のメトリックを確認してください。SSCD は、要求 (マウスクリック) の時刻にできるだけ近い時点から開始されます。クライアントデバイスと VDA 間の ICA 接続が確立されたときに終了します。共有セッションの場合、サーバーへの新しい接続の作成に関連するセットアップコストの多くが発生しないため、この期間ははるかに短くなります。次のレベルでは、いくつかの詳細なメトリックが利用可能です。

ICAファイルダウンロード期間 (IFDCD)

これは、クライアントがサーバーから ICA ファイルをダウンロードするのにかかる時間です。全体的なプロセスは次のとおりです。

1. ユーザーは Workspace Application でリソース (アプリケーションまたはデスクトップ) をクリックします。
2. ユーザーからの要求は、Citrix Gateway (構成されている場合) を介して StoreFront™ に送信され、StoreFront™ はその要求を Delivery Controller に送信します。
3. Delivery Controller は要求に利用可能なマシンを見つけ、マシン情報とその他の詳細を StoreFront に送信します。また、StoreFront は Secure Ticket Authority からワンタイムチケットを要求し、受け取ります。
4. StoreFront は ICA ファイルを生成し、Citrix Gateway (構成されている場合) を介してユーザーに送信します。

IFDCD は、完全なプロセス (ステップ 1〜4) にかかる時間を表します。IFDCD 期間は、クライアントが ICA ファイルを受信したときにカウントを停止します。

LPWD は、プロセスの StoreFront コンポーネントです。

IFDCD が高い (ただし LPWD が正常である) 場合、起動のサーバー側処理は成功しましたが、クライアントデバイスと StoreFront の間に通信の問題がありました。これは、2つのマシン間のネットワークの問題に起因します。したがって、まず潜在的なネットワークの問題をトラブルシューティングできます。

起動ページ WEB サーバー期間 (LPWD)

これは、StoreFront で起動ページ (launch.aspx) を処理するのにかかる時間です。LPWD が高い場合、StoreFront にボトルネックがある可能性があります。

考えられる原因は次のとおりです。

- StoreFrontの負荷が高い。Internet Information Services (IIS) のログや監視ツール、タスクマネージャー、パフォーマンスモニターなどを確認して、遅延の原因を特定してください。
- StoreFrontがDelivery Controllerなどの他のコンポーネントとの通信に問題がある。StoreFrontとDelivery Controller間のネットワーク接続が遅いか、一部のDelivery Controllerがダウンしているか、過負荷になっていないかを確認してください。

名前解決WEBサーバー期間 (NRWD)

これは、Delivery Controllerが公開アプリケーション/デスクトップの名前をVDAマシンのIPアドレスに解決するのにかかる時間です。

このメトリックが高い場合、Delivery Controllerが公開アプリケーションの名前をIPアドレスに解決するのに時間がかかっていることを示します。

可能性のある原因としては、クライアント側の問題、Delivery Controllerの過負荷などのDelivery Controllerの問題、またはそれらの間のネットワークリンクの問題が挙げられます。

チケット応答WEBサーバー期間 (TRWD)

この期間は、Secure Ticket Authority (STA) サーバーまたはDelivery Controllerからチケットを取得するのにかかる時間を示します（必要な場合）。この期間が長い場合、STAサーバーまたはDelivery Controllerが過負荷になっていることを示します。

セッション検索クライアント期間 (SLCD)

この期間は、要求された公開アプリケーションをホストするためにすべてのセッションを照会するのにかかる時間を表します。既存のセッションがアプリケーション起動要求を処理できるかどうかを判断するために、クライアントでチェックが実行されます。使用される方法は、セッションが新規か共有かによって異なります。

セッション作成クライアント期間 (SCCD)

この期間は、wfica32.exe（または同様の同等ファイル）が起動されてから接続が確立されるまでの、セッション作成にかかる時間を表します。

VDAセッション起動フェーズ

セッション起動VDA期間 (SSVD)

この期間は、VDAが起動操作全体を実行するのにかかる時間を含む、高レベルのサーバー側接続起動メトリックです。このメトリックが高い場合、セッション起動時間を増加させるVDAの問題があることを示します。これには、VDAで起動操作全体を実行するのに費やされた時間が含まれます。

資格情報取得VDA期間 (COVD)

VDAがユーザー資格情報を取得するのにかかる時間。

ユーザーが時間内に資格情報を提供できない場合、この期間は人為的に増加する可能性があります。そのため、VDA起動期間には含まれません。この時間は、手動ログインが使用され、サーバー側の資格情報ダイアログが表示される場合（またはログイン開始前に法的通知が表示される場合）にのみ重要となる可能性があります。

資格情報認証VDA期間 (CAVD)

これは、VDAが認証プロバイダーに対してユーザーの資格情報を認証するのにかかる時間です。認証プロバイダーは、Kerberos、Active Directory、またはセキュリティサポートプロバイダーインターフェイス (SSPI) のいずれかです。

グループポリシーVDA期間 (GPVD)

この期間は、ログオン中にグループポリシーオブジェクトを適用するのにかかる時間です。

ログオンスクリプト実行VDA期間 (LSVD)

これは、VDAがユーザーのログオンスクリプトを実行するのにかかる時間です。

ユーザーまたはグループのログオンスクリプトを非同期にすることを検討してください。アプリケーション互換性スクリプトを最適化するか、代わりに環境変数を使用することを検討してください。

プロファイルロードVDA期間 (PLVD)

これは、VDAがユーザープロファイルをロードするのにかかる時間です。

この期間が長い場合は、ユーザープロファイル構成を検討してください。ローミングプロファイルのサイズと場所は、セッションの起動が遅くなる原因となります。ユーザーがターミナルサービスローミングプロファイルとホームフォルダーが有効になっているセッションにログオンすると、ローミングプロファイルの内容と当該フォルダーへのアクセスがログオン中にマッピングされます。これには追加のリソースが必要です。場合によっては、CPU使用率を大幅に消費することがあります。この問題を軽減するために、リダイレクトされた個人フォルダーとともに**ターミナルサービスホーム**フォルダーを使用することを検討してください。一般に、Citrix環境でユーザープ

ロファイルを管理するには、Citrix Profile Managementの使用を検討してください。Citrix Profile Managementを使用しており、ログオン時間が遅い場合は、アンチウイルスソフトウェアがCitrix Profile Managementツールをブロックしていないか確認してください。

プリンター作成VDA期間 (PCVD)

これは、VDAがユーザーのクライアントプリンターを同期的にマッピングするのにかかる時間です。プリンター作成が非同期で実行されるように構成されている場合、セッション起動の完了に影響しないため、PCVDの値は記録されません。

プリンターのマッピングに過剰な時間が費やされるのは、多くの場合、プリンターの自動作成ポリシー設定が原因です。ユーザーのクライアントデバイスにローカルで追加されたプリンターの数と、印刷構成がセッションの開始時間に直接影響を与える可能性があります。セッションが開始されると、Citrix Virtual Apps and Desktops™ は、クライアントデバイス上のローカルにマップされたすべてのプリンターを作成する必要があります。特にユーザーが多数のローカルプリンターを持っている場合は、作成されるプリンターの数を減らすために、印刷ポリシーを再構成することを検討してください。これを行うには、Delivery Controller および Citrix Virtual Apps and Desktops でプリンターの自動作成ポリシーを編集します。

ドライブマッピングVDA期間 (DMVD)

これは、VDAがユーザーのクライアントドライブ、デバイス、ポートをマッピングするのにかかる時間です。

ICAプロトコルを最適化し、セッション全体のパフォーマンスを向上させるために、ベースポリシーに未使用の仮想チャネル（オーディオやCOMポートのマッピングなど）を無効にする設定が含まれていることを確認してください。

アプリケーション/デスクトップ起動VDA期間 (ALVD/DLVD)

このフェーズは、UserinitとShellの期間の組み合わせです。ユーザーがWindowsマシンにログオンすると、winlogonがuserinit.exeを実行します。Userinit.exeはログオンスクリプトを実行し、ネットワーク接続を再確立してからExplorer.exeを開始します。Userinitは、userinit.exeの開始から仮想デスクトップまたはアプリケーションのユーザーインターフェイスの開始までの期間を表します。Shell期間は、ユーザーインターフェイスの初期化からユーザーがキーボードとマウスの制御を受け取るまでの時間です。

セッション作成VDA期間 (SCVD)

この時間には、VDAでのセッション作成時間におけるその他の遅延が含まれます。

ユーザーログオンの問題を診断する

ユーザーログオンの問題をトラブルシューティングするには、ログオン期間データを使用します。

ログオン期間は、HDX を使用したデスクトップまたはアプリへの初回接続の場合にのみ測定されます。このデータには、リモートデスクトッププロトコルで接続しようとしているユーザーや、切断されたセッションから再接続しているユーザーは含まれません。具体的には、ユーザーが最初に非 HDX プロトコルを使用して接続し、HDX を使用して再接続する場合、ログオン期間は測定されません。

ユーザー詳細ビューでは、期間が数値として表示されます。この数値の下には、ログオンが発生した時刻と、ログオンプロセスのフェーズを示すグラフが表示されます。

ユーザーがCitrix Virtual Apps and Desktops™にログオンすると、Monitor Serviceはログオンプロセスのフェーズを追跡します。フェーズは、ユーザーがCitrix Workspace™アプリから接続した時点から、デスクトップが使用可能になるまでの時間で始まります。

左側の大きな数字は合計ログオン時間です。これは、接続を確立し、Delivery Controller™ からデスクトップを取得するのに費やされた時間と、仮想デスクトップに認証してログオンするのに費やされた時間を組み合わせて計算されます。期間情報は秒（または秒の端数）で表示されます。

前提条件

ログオン期間データとドリルダウンが表示されるように、次の前提条件が満たされていることを確認してください。

1. VDA に **Citrix User Profile Manager** と **Citrix User Profile Manager WMI Plugin** をインストールします。
2. Citrix Profile Management Service が実行されていることを確認します。
3. XenApp および XenDesktop サイト 7.15 以前の場合、GPO 設定 **レガシー実行リストを処理しない** を無効にします。
4. 対話型セッションのドリルダウンには、監査プロセス追跡を有効にする必要があります。
5. GPO ドリルダウンの場合、グループポリシーの運用ログのサイズを増やします。

> **注:**
>
> - ログオン時間は、デフォルトのWindowsシェル (explorer.exe) でのみサポートされ、カスタムシェルではサポートされません。
> - Remote PC Accessのログオン時間は、Remote PC Accessのインストール中に**Citrix User Profile Manager**と**Citrix User Profile Manager WMI Plugin**が追加コンポーネントとしてインストールされている場合にのみ利用可能です。詳細については、「Remote PC Accessの構成とシーケンスに関する考慮事項」のステップ4を参照してください。

ユーザーログオンの問題をトラブルシューティングする手順

1. **ユーザー詳細**ビューから、ログオン時間パネルを使用してログオン状態をトラブルシューティングします。
   - ユーザーがログオン中の場合、ビューにはログオンのプロセスが反映されます。
   - ユーザーがログオンしている場合、ログオン時間パネルには、ユーザーが現在のセッションにログオンするまでにかかった時間が表示されます。
2. ログオンプロセスのフェーズを検査します。

ログオンプロセスのフェーズ

ブローカリング

ユーザーに割り当てるデスクトップを決定するまでにかかった時間。

VM起動

セッションでマシンの起動が必要な場合、VM起動は仮想マシンを起動するのにかかった時間です。

HDX接続

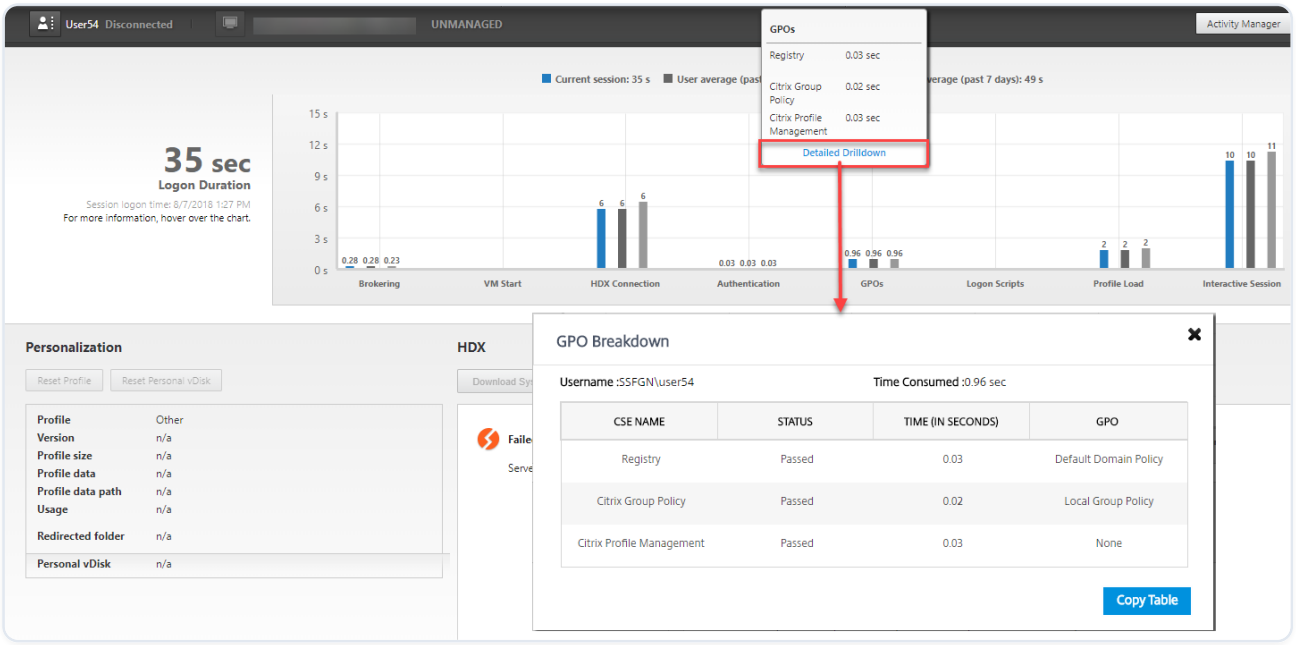
クライアントから仮想マシンへのHDX接続の設定に必要な手順を完了するのにかかった時間。

認証

リモートセッションへの認証を完了するのにかかった時間。

GPO

仮想マシンでグループポリシー設定が有効になっている場合、これはログオン中にグループポリシーオブジェクトを適用するのにかかった時間です。GPOバーにカーソルを合わせると、CSE（クライアント側拡張）に従って各ポリシーを適用するのにかかった時間のドリルダウンがツールチップとして表示されます。



詳細ドリルダウンをクリックすると、ポリシーの状態と対応するGPO名を含むテーブルが表示されます。ドリルダウンの期間はCSE処理時間のみを表し、合計GPO時間には加算されません。トラブルシューティングやレポートでの使用のために、ドリルダウンテーブルをコピーできます。ポリシーのGPO時間はイベントビューアログから取得されます。ログは、運用ログに割り当てられたメモリ（デフォルトサイズは4 MB）に応じて上書きされる可能性があります。運用ログのログサイズを増やす方法の詳細については、Microsoft TechNetの記事イベントログの構成を参照してください。

ログオンスクリプト

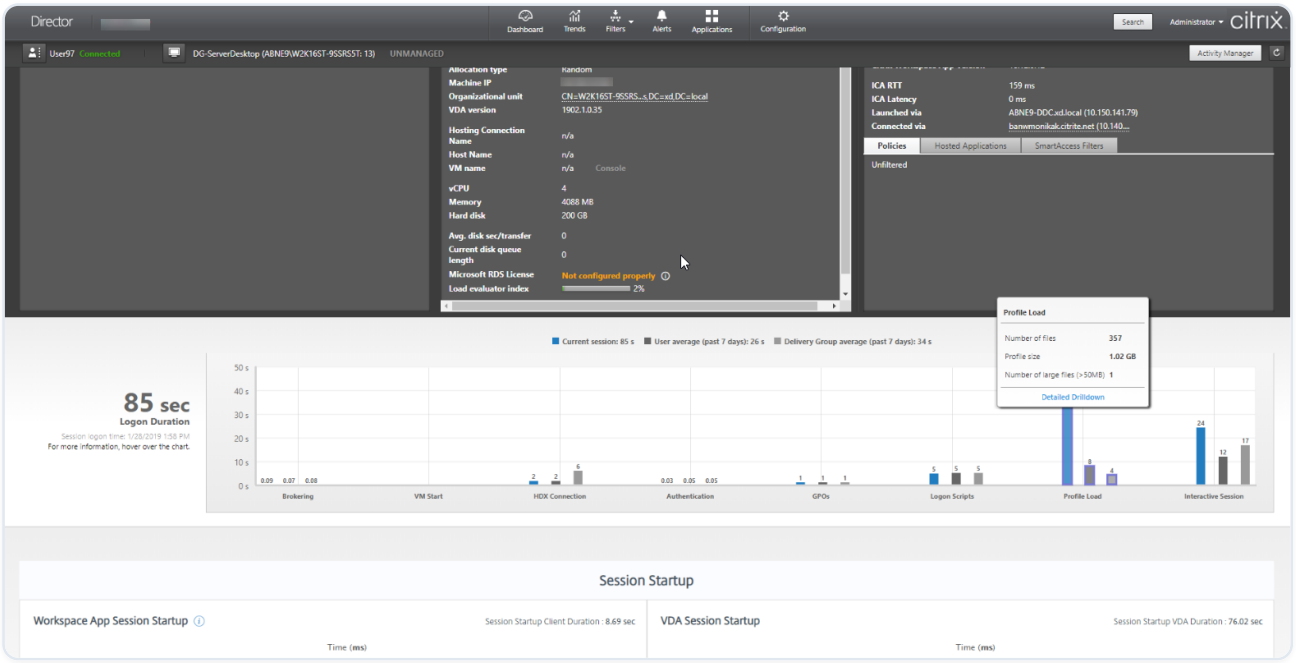
セッションにログオンスクリプトが構成されている場合、これはログオンスクリプトの実行にかかる時間です。

プロファイル読み込み

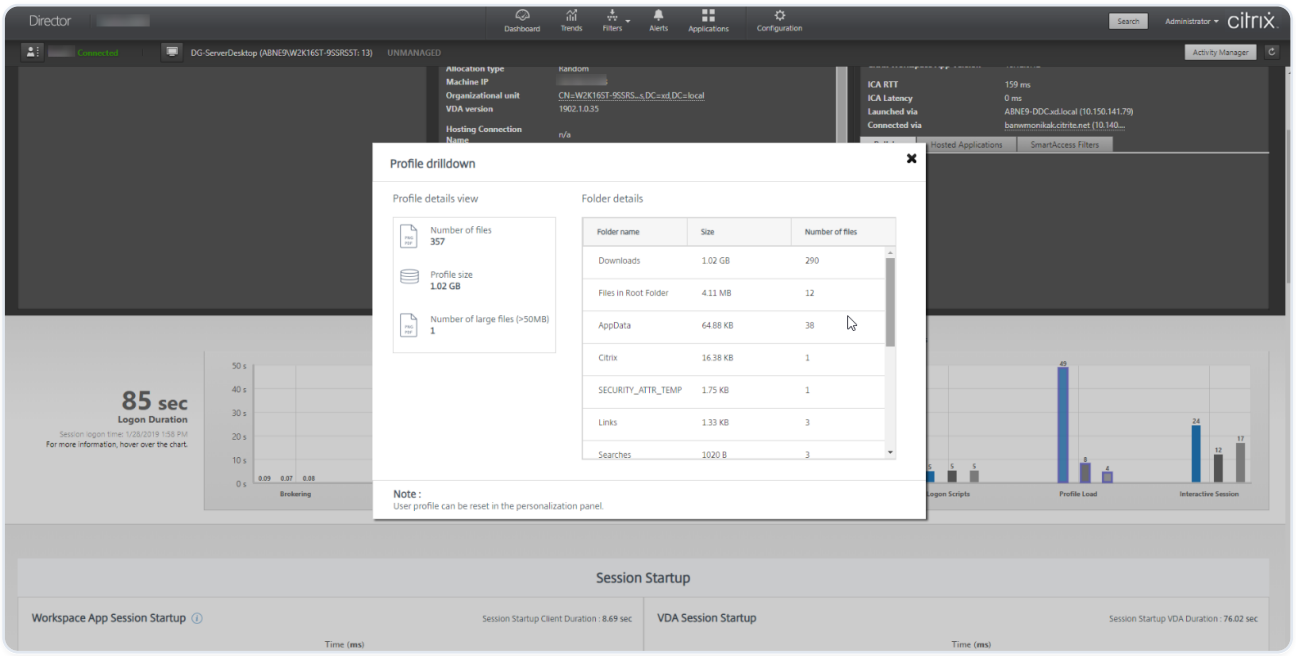
ユーザーまたは仮想マシンにプロファイル設定が構成されている場合、これはプロファイルの読み込みにかかる時間です。

Citrix Profile Managementが構成されている場合、プロファイルロードバーには、Citrix Profile Managementがユーザープロファイルを処理するのにかかった時間が含まれます。この情報は、管理者がプロファイル処理時間の長い問題をトラブルシューティングするのに役立ちます。Profile Managementが構成されている場合、プロファイルロードバーは増加した期間を表示します。この増加はこの機能強化によって引き起こされるものであり、パフォーマンスの低下を反映するものではありません。この機能強化はVDA 1903以降で利用可能です。

プロファイルロードバーにカーソルを合わせると、現在のセッションのユーザープロファイルの詳細を示すツールチップが表示されます。



詳細ドリルダウンをクリックすると、プロファイルルートフォルダー（例: C:/Users/username）内の個々のフォルダー、そのサイズ、およびファイル数（ネストされたフォルダー内のファイルを含む）をさらにドリルダウンできます。



プロファイルのドリルダウンは、Delivery Controllerバージョン7 1811以降およびVDA 1811以降で利用できます。プロファイルのドリルダウン情報を使用して、高いプロファイルロード時間に関連する問題を解決できます。次のことができます。

- ユーザープロファイルをリセットする
- 不要な大きなファイルを削除してプロファイルを最適化する
- ネットワーク負荷を軽減するためにファイル数を減らす
- プロファイルストリーミングを使用する

デフォルトでは、プロファイルルート内のすべてのフォルダーがドリルダウンに表示されます。フォルダーの表示を非表示にするには、VDAマシンで次のレジストリ値を編集します。

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

1. VDAで、HKEY_LOCAL_MACHINE\Software\Citrix\Director\ に新しいレジストリ値 **ProfileFoldersNameHidden** を追加します。
2. 値を1に設定します。この値はDWORD（32ビット）値である必要があります。これでフォルダー名の表示が無効になります。
3. フォルダー名を再度表示するには、値を0に設定します。

> **注:** 複数のマシンにレジストリ値の変更を適用するには、GPOまたはPowerShellコマンドを使用できます。GPOを使用してレジストリ変更を展開する方法の詳細については、ブログを参照してください。

追加情報

- プロファイルのドリルダウンでは、リダイレクトされたフォルダーは考慮されません。
- ルートフォルダー内のNTUser.datファイルは、エンドユーザーには表示されない場合があります。ただし、これらはプロファイルのドリルダウンに含まれ、**ルートフォルダー**のファイルリストに表示されます。
- AppDataフォルダー内の一部の隠しファイルは、プロファイルのドリルダウンには含まれません。
- ファイル数とプロファイルサイズデータは、特定のWindowsの制限により、パーソナライゼーションパネルのデータと一致しない場合があります。

対話型セッション

これは、ユーザープロファイルがロードされた後、キーボードとマウスの制御をユーザーに「引き渡す」のにかかった時間です。通常、ログオンプロセスのすべてのフェーズの中で最も長い期間であり、**対話型セッション期間 = デスクトップ準備完了イベントタイムスタンプ (VDA上の**

EventId 1000) - ユーザープロファイルロード済みイベントタイムスタンプ (VDA上のEventId 2) として計算されます。対話型セッションには、Pre-userinit、Userinit、Shellの3つのサブフェーズがあります。対話型セッションにカーソルを合わせると、次の情報を示すツールチップが表示されます。

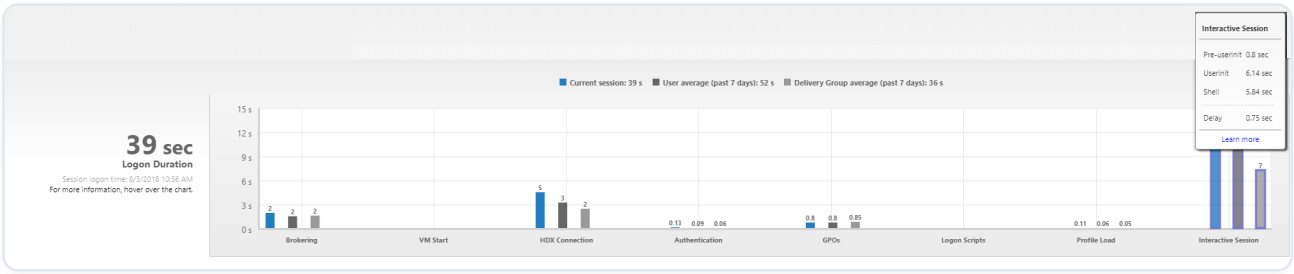
- サブフェーズ
- 各サブフェーズにかかる時間
- これらのサブフェーズ間の累積合計時間遅延
- ドキュメントへのリンク。

> **注：**
>
> この機能はVDA 1811以降で利用できます。7.18より前のサイトでセッションを起動し、その後7.18以降にアップグレードした場合、「サーバーエラーのためドリルダウンが利用できません」というメッセージが表示されます。ただし、アップグレード後にセッションを起動した場合は、エラーメッセージは表示されません。

> 各サブフェーズの期間を表示するには、VM (VDA) で監査プロセス追跡を有効にします。監査プロセス追跡が無効になっている場合 (デフォルト)、Pre-userinitの期間と、UserinitおよびShellの合計期間が表示されます。グループポリシーオブジェクト (GPO) を使用して監査プロセス追跡を有効にするには、次の手順を実行します。

1. GPOを作成し、GPOエディターを使用して編集します。
2. **コンピューターの構成 > Windows の設定 > セキュリティの設定 > ローカル ポリシー > 監査ポリシー**に移動します。
3. 右側のペインで、**監査プロセス追跡**をダブルクリックします。
4. **成功**を選択し、OKをクリックします。
5. このGPOを必要なVDAまたはグループに適用します。

監査プロセス追跡とその有効化または無効化の詳細については、Microsoftドキュメントの監査プロセス追跡を参照してください。



ユーザー詳細ビューのログオン期間パネル。

- **インタラクティブセッション – Pre-userinit:** グループポリシーオブジェクトとスクリプトと重複するインタラクティブセッションのセグメント。このサブフェーズは、GPOとスクリプトを最適化することで短縮できます。
- **インタラクティブセッション – Userinit:** ユーザーがWindowsマシンにログオンすると、Winlogonはuserinit.exeを実行します。Userinit.exeはログオンスクリプトを実行し、ネットワーク接続を再確立してから、Windowsユーザーインターフェイスであるexplorer.exeを起動します。インタラクティブセッションのこのサブフェーズは、Userinit.exeの開始から仮想デスクトップまたはアプリケーションのユーザーインターフェイスの開始までの期間を表します。
- **インタラクティブセッション – シェル:** 前のフェーズで、UserinitはWindowsユーザーインターフェイスの初期化を開始します。シェルサブフェーズは、ユーザーインターフェイスの初期化から、ユーザーがキーボードとマウスの制御を受け取るまでの期間を捕捉します。
- **遅延:** これは、**Pre-userinitとUserinit**サブフェーズ間、および**Userinitとシェル**サブフェーズ間の累積時間遅延です。

合計ログオン時間は、これらのフェーズの正確な合計ではありません。たとえば、一部のフェーズは並行して発生し、一部のフェーズでは、合計よりも長いログオン期間につながる可能性のあるより多くの処理が発生します。 合計ログオン時間には、ICAファイルのダウンロードとアプリケーションのICAファイル起動の間の時間であるICA®アイドル時間は含まれません。 アプリケーション起動時にICAファイルを自動的に開くには、ICAファイルのダウンロード時にICAファイルを自動的に起動するようにブラウザを設定します。詳細については、CTX804493を参照してください。

> **注:** ログオン期間グラフは、ログオンフェーズを秒単位で表示します。1秒未満の期間値はサブ秒値として表示されます。1秒を超える値は、最も近い0.5秒に丸められます。グラフは、Y軸の最大値が200秒になるように設計されています。200秒を超える値は、バーの上に実際の値が表示されます。

トラブルシューティングのヒント

グラフ内の異常な値や予期しない値を特定するには、現在のセッションの各フェーズにかかった時間と、このユーザーの過去7日間の平均所要時間、およびこのデリバリーグループ内のすべてのユーザーの過去7日間の平均所要時間を比較します。

必要に応じてエスカレートします。例えば、VMの起動が遅い場合、問題はハイパーバイザーにある可能性があるため、ハイパーバイザー管理者にエスカレートできます。あるいは、ブローカリング時間が遅い場合は、サイト管理者に問題をエスカレートして、Delivery Controllerの負荷分散を確認してもらうことができます。

以下を含む異常な相違点を調べます。

- 欠落している（現在の）ログオンバー
- 現在の所要時間とこのユーザーの平均所要時間の間の大きな不一致。原因は次のとおりです。
    - 新しいアプリケーションがインストールされた。
    - オペレーティングシステムのアップデートが行われた。
    - 構成変更が行われた。
    - ユーザーのプロファイルサイズが大きい。この場合、プロファイルロードが高い。
- ユーザーのログオン数（現在の所要時間と平均所要時間）とデリバリーグループの平均所要時間の間の大きな不一致。

必要に応じて、**再起動**をクリックしてユーザーのログオンプロセスを監視し、VMの起動やブローカリングなどの問題をトラブルシューティングします。

シャドウユーザー

Directorから、シャドウユーザー機能を使用して、ユーザーの仮想マシンまたはセッションを直接表示したり操作したりできます。Windows VDAとLinux VDAの両方をシャドウできます。シャドウするマシンにユーザーが接続している必要があります。これは、ユーザーのタイトルバーに表示されているマシン名を確認することで検証できます。

Directorは新しいタブでシャドウを開始します。DirectorのURLからのポップアップを許可するようにブラウザ設定を更新してください。

シャドウ機能は、**ユーザーの詳細**ビューからアクセスします。ユーザーセッションを選択し、アクティビティマネージャービューまたはセッション詳細パネルで**シャドウ**をクリックします。

Linux VDAのシャドウ

シャドウは、RHEL7.3またはUbuntuバージョン16.04のLinuxディストリビューションを実行している、バージョン7.16以降のLinux VDAで利用できます。

注：

- シャドウが機能するには、VDAがDirector UIからアクセス可能である必要があります。したがって、シャドウはDirectorクライアントと同じイントラネット内のLinux VDAでのみ可能です。
- DirectorはFQDNを使用してターゲットLinux VDAに接続します。Directorクライアントが Linux VDAのFQDNを解決できることを確認してください。
- VDAには、python websockifyおよびx11vncパッケージがインストールされている必要があります。
- VDAへのnoVNC接続はWebSocketプロトコルを使用します。デフォルトでは、**ws://** WebSocketプロトコルが使用されます。セキュリティ上の理由から、Citrixは安全な **wss://** プロトコルを使用することを推奨します。各DirectorクライアントとLinux VDAにSSL証明書をインストールしてください。

セッションシャドウ の手順に従って、シャドウ用にVDAを構成してください。

1. **シャドウ**をクリックすると、シャドウ接続が初期化され、ユーザーデバイスに確認プロンプトが表示されます。
2. ユーザーに**はい**をクリックするよう指示して、マシンまたはセッションの共有を開始します。
3. 管理者はシャドウされたセッションを表示することのみ可能です。

Windows VDA のシャドウイング

Windows VDA セッションは、Windows リモートアシスタンスを使用してシャドウイングされます。VDA のインストール中に、**ユーザー Windows リモートアシスタンス**機能を有効にします。詳細については、「機能の有効化または無効化」を参照してください。

1. **シャドウ**をクリックすると、シャドウイング接続が初期化され、.msrc インシデントファイルを開くか保存するかを求めるダイアログボックスが表示されます。
2. デフォルトで選択されていない場合は、リモートアシスタンスビューアーでインシデントファイルを開きます。ユーザーデバイスに確認プロンプトが表示されます。
3. ユーザーに**はい**をクリックするよう指示して、マシンまたはセッションの共有を開始します。

4. より詳細な制御を行うには、ユーザーにキーボードとマウスの制御を共有するよう依頼します。

シャドウイング用に MICROSOFT INTERNET EXPLORER ブラウザーを合理化する

ダウンロードした Microsoft Remote Assistance (.msra) ファイルをリモートアシスタンスクライアントで自動的に開くように、Microsoft Internet Explorer ブラウザーを構成します。

これを行うには、グループポリシーエディターで 設定を有効にする必要があります。

コンピューターの構成 \> 管理用テンプレート \> Windows コンポーネント \> Internet Explorer \> インターネットコントロールパネル \> セキュリティページ \> インターネットゾーン \> ファイルのダウンロード時に自動的に確認する。

デフォルトでは、このオプションはローカルイントラネットゾーンのサイトで有効になっています。Director サイトがローカルイントラネットゾーンにない場合は、このゾーンにサイトを手動で追加することを検討してください。

ユーザーにメッセージを送信する

Directorから、1台以上のマシンに接続しているユーザーにメッセージを送信します。この機能を使用して、デスクトップのメンテナンス、マシンのログオフと再起動、プロファイルのリセットなど、差し迫った管理操作に関する即時通知を送信します。

1. アクティビティマネージャービューで、ユーザーを選択し、 をクリックします。
2. ユーザー詳細ビューで、セッション詳細パネルを見つけ、 をクリックします。
3. および フィールドにメッセージ情報を入力し、 をクリックします。

メッセージが正常に送信されると、Directorに確認メッセージが表示されます。メッセージはユーザーのマシンに表示されます。

メッセージが正常に送信されなかった場合、Directorにエラーメッセージが表示されます。エラーメッセージに従って問題をトラブルシューティングします。完了したら、件名とメッセージテキストを再度入力し、もう一度 をクリックします。

アプリケーションの障害を解決する

「**アクティビティマネージャー**」ビューで、タブをクリックします。このユーザーがアクセスできるすべてのマシン上のすべてのアプリケーション（現在接続されているマシンのローカルアプリケーションとホスト型アプリケーションを含む）と、それぞれのステータスを表示できます。

> **注：**

> タブがグレー表示されている場合は、タブを有効にする権限を持つ管理者に連絡してください。

> このリストには、セッション内で起動されたアプリケーションのみが含まれます。

マルチセッションOSマシンおよびシングルセッションOSマシンでは、切断されたセッションごとにアプリケーションが一覧表示されます。ユーザーが接続されていない場合、アプリケーションは表示されません。

アクション	説明
応答しないアプリケーションを終了する	応答しないアプリケーションを選択し、[アプリケーションの終了]をクリックします。アプリケーションが終了したら、ユーザーに再度起動するよう依頼します。
応答しないプロセスを終了する	必要な権限がある場合は、[プロセス]タブをクリックします。アプリケーションに関連する、または大量のCPUリソースやメモリを使用しているプロセスを選択し、[プロセスの終了]をクリックします。ただし、プロセスを終了するのに必要な権限がない場合、プロセスを終了しようとしても失敗します。
ユーザーのマシンを再起動する	シングルセッションOSマシンのみの場合、選択したセッションで[再起動]をクリックします。または、[マシン詳細]ビューから、電源コントロールを使用してマシンを再起動またはシャットダウンします。アプリケーションを再確認できるように、ユーザーに再度ログオンするよう指示します。マルチセッションOSマシンでは、再起動オプションは利用できません。代わりに、ユーザーからログオフし、ユーザーに再度ログオンさせます。
マシンをメンテナンスモードにする	マシンのイメージにパッチやその他の更新などのメンテナンスが必要な場合は、マシンをメンテナンスモードにします。[マシン詳細]ビューから[詳細]をクリックし、メンテナンスモードオプションをオンにします。適切な管理者にエスカレートしてください。

デスクトップ接続を復元する

Directorから、ユーザーのタイトルバーで現在のマシンに対するユーザーの接続ステータスを確認します。

デスクトップ接続が失敗した場合、失敗の原因となったエラーが表示され、トラブルシューティングの方法を決定するのに役立ちます。

アクション	説明
マシンがメンテナンスモードではないことを確認します	ユーザー詳細ページで、メンテナンスモードがオフになっていることを確認します。
ユーザーのマシンを再起動する	マシンを選択し、**再起動**をクリックします。ユーザーのマシンが応答しない、または接続できない場合にこのオプションを使用します。たとえば、マシンが異常に高いCPUリソースを使用しており、CPUが使用不能になっている場合などです。

セッションを復元する

セッションが切断されても、セッションはアクティブなままでアプリケーションは実行され続けますが、ユーザーデバイスはサーバーと通信しなくなります。

ユーザー詳細ビューで、**セッションの詳細**パネルのセッション障害をトラブルシューティングします。セッションIDで示される現在のセッションの詳細を表示できます。

アクション	説明
応答しないアプリケーションまたはプロセスを終了する	**アプリケーション**タブをクリックします。応答しないアプリケーションを選択し、**アプリケーションの終了**をクリックします。同様に、応答しない対応するプロセスを選択し、**プロセスの終了**をクリックします。また、異常に大量のメモリまたはCPUリソースを消費しているプロセスを終了します。これにより、CPUが使用不能になる可能性があります。
Windowsセッションを切断する	**セッション制御**をクリックし、**切断**を選択します。このオプションは、ブローカーされたマルチセッションOSマシンでのみ利用可能で

アクション	説明
	す。ブローカーされていないセッションの場合、このオプションは無効になります。
ユーザーのセッションからログオフする	**セッション制御**をクリックし、**ログオフ**を選択します。

セッションをテストするには、ユーザーはセッションに再度ログオンを試みることができます。また、ユーザーをシャドウして、このセッションをより詳細に監視することもできます。

HDX™ チャネルシステムレポートを実行する

ユーザーの詳細ビューで、**HDX**パネルにあるユーザーのマシン上のHDXチャネルのステータスを確認します。このパネルは、ユーザーのマシンがHDXを使用して接続されている場合にのみ利用可能です。

情報が現在利用できないことを示すメッセージが表示された場合は、ページが更新されるまで1分間待つか、**更新**ボタンを選択します。HDXデータの更新には、他のデータよりも少し時間がかかります。

詳細については、エラーまたは警告アイコンをクリックしてください。

> ヒント:

> タイトルバーの左隅にある左右の矢印をクリックすると、同じダイアログボックスで他のチャネルに関する情報を表示できます。

> HDXチャネルシステムレポートは、主にCitrixサポートがさらなるトラブルシューティングのために使用します。

1. HDXパネルで、をクリックします。
2. .xmlレポートファイルを表示または保存できます。
    - .xmlファイルを表示するには、をクリックします。.xmlファイルは、Directorアプリケーションと同じウィンドウに表示されます。
    - .xmlファイルを保存するには、をクリックします。ウィンドウが表示され、Directorマシン上のファイルのダウンロード先を尋ねられます。

ユーザープロファイルをリセットする

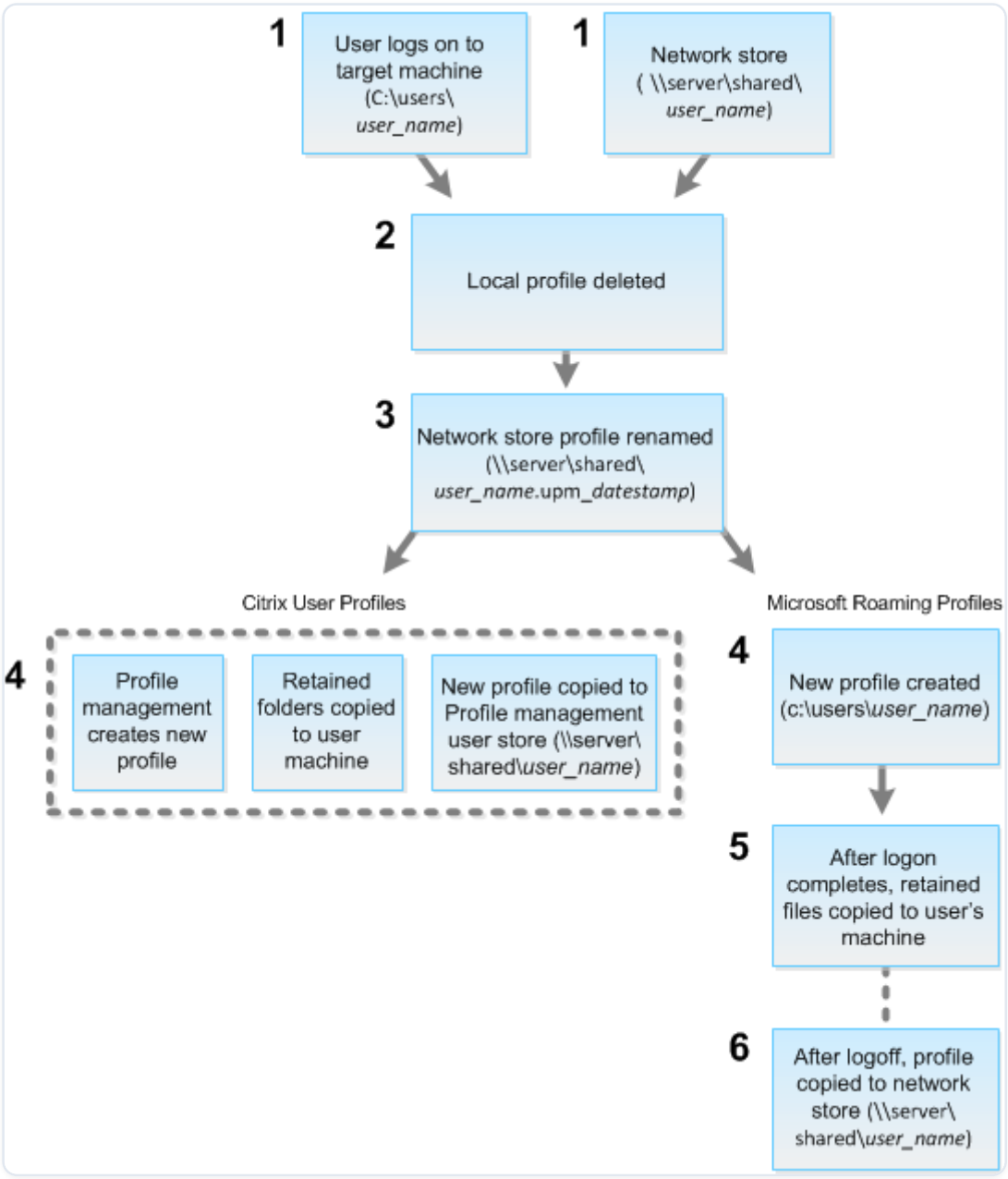
> **注意:**
>
> プロファイルがリセットされると、ユーザーのフォルダーとファイルは保存され、新しいプロファイルにコピーされます。ただし、ほとんどのユーザープロファイルデータは失われます（たとえば、レジストリがリセットされ、アプリケーション設定が削除される可能性があります）。

> Profile Management 2106以降、リセット機能はCitrix Managementプロファイルコンテナベースのユーザープロファイルソリューションで利用できます。

リセットされたプロファイルの処理方法

任意のCitrixユーザープロファイルまたはMicrosoftローミングプロファイルをリセットできます。ユーザーがログオフし、リセットコマンド（DirectorまたはPowerShell SDKを使用して）を選択すると、Directorはまず使用中のユーザープロファイルを識別し、適切なリセットコマンドを発行します。Directorは、プロファイルのサイズ、種類、ログオン時間に関する情報を含め、Profile Managementを介して情報を受け取ります。

この図は、ユーザープロファイルがリセットされた場合の、ユーザーログオン後のプロセスを示しています。



Directorによって発行されるリセットコマンドは、プロファイルの種類を指定します。その後、Profile Managementサービスはその種類のプロファイルをリセットしようとし、適切なネットワーク共有（ユーザーストア）を探します。ユーザーがProfile Managementによって処理されているにもかかわらず、ローミングプロファイルコマンドを受け取った場合、それは拒否されます（またはその逆も同様です）。

1. ローカルプロファイルが存在する場合、それは削除されます。
2. ネットワークプロファイルの名前が変更されます。
3. 次のアクションは、リセットされるプロファイルがCitrixユーザープロファイルかMicrosoftローミングプロファイルかによって異なります。

Citrixユーザープロファイルの場合、新しいプロファイルはProfile Managementのインポートルールを使用して作成されます。フォルダーはネットワークプロファイルにコピーされ、ユーザーは通常どおりログオンできます。リセットにローミングプロファイルが使用される場合、ローミングプロファイル内のレジストリ設定はリセットされたプロファイルに保持されます。必要に応じて、テンプレートプロファイルがローミングプロファイルを上書きするようにProfile Managementを構成できます。

Microsoftローミングプロファイルの場合、Windowsはプロファイルを作成し、ユーザーがログオンすると、フォルダーはユーザーデバイスにコピーされます。ユーザーが再度ログオフすると、新しいプロファイルはネットワークストアにコピーされます。

Directorでユーザープロファイルをリセットするには

Citrix Virtual Desktops™ (Desktop VDA) を使用している場合は、次の操作を行います。

1. **Director** で、プロファイルをリセットするユーザーを検索し、そのユーザーのセッションを選択します。
2. をクリックします。
3. ユーザーにすべてのセッションからログオフするよう指示します。
4. ユーザーに再度ログオンするよう指示します。 ユーザーのプロファイルから保存されたフォルダーとファイルは、新しいプロファイルにコピーされます。

Citrix Virtual Desktops (Server VDA) を使用している場合、プロファイルのリセットを実行するにはログオンしている必要があります。その後、ユーザーはログオフし、再度ログオンしてプロファイルのリセットを完了する必要があります。

> **重要:**

> ユーザーが複数のプラットフォーム (Windows 8 や Windows 7 など) でプロファイルを持っている場合、ユーザーが問題として報告したのと同じデスクトップまたはアプリに最初に再度ログオンするよう指示します。このログオン操作により、正しいプロファイルがリセットされます。プロファイルがCitrixユーザープロファイルの場合、ユーザーのデスクトップが表示されるまでにプロファイルはすでにリセットされています。プロファイルがMicrosoftローミングプロファイルの場合、フォルダーの復元が短時間進行中の可能性があります。ユーザーは復元が完了するまでログオンしたままにする必要があります。

> プロファイルが正常にリセットされない場合 (たとえば、ユーザーがマシンに正常にログオンできない、または一部のファイルが欠落している場合) は、元のプロファイルを手動で復元する必要があります。

次の点に注意してください。

- ユーザープロファイルソリューションとしてユーザーストアが有効になっている場合、新しいプロファイルには元のユーザープロファイルから次の個人用フォルダーが含まれます。
  - デスクトップ
  - クッキー
  - お気に入り
  - ドキュメント
  - ピクチャ
  - ミュージック
  - ビデオ
- Citrix Managementプロファイルコンテナがユーザープロファイルソリューション全体として有効になっている場合、新しいプロファイルには以前の個人用フォルダーは含まれません。
- Windows 8以降では、プロファイルがリセットされると、Cookieは新しいプロファイルにコピーされません。

リセットに失敗したプロファイルを手動で復元するには

1. ユーザーにすべてのセッションからログオフするよう指示します。
2. ローカルプロファイルが存在する場合は削除します。
3. ネットワーク共有上で、フォルダー名に日付と時刻が付加されたアーカイブフォルダー（.upm_datestamp拡張子を持つフォルダー）を見つけます。
4. 現在のプロファイル名、つまりupm_datestamp拡張子がない方を削除します。
5. アーカイブされたフォルダーを元のプロファイル名にリネームします。つまり、日付と時刻の拡張子を削除します。これにより、プロファイルはリセット前の元の状態に戻ります。

PowerShell SDKを使用してプロファイルをリセットするには

Broker PowerShell SDKを使用してプロファイルをリセットできます。

NEW-BROKERMACHINECOMMAND

特定のユーザー、セッション、またはマシンへの配信のためにキューに入れられたコマンドを作成します。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerMachineCommand/>`を参照してください。

例

プロファイルをリセットするためのPowerShellコマンドレットの使用方法の詳細については、以下の例を参照してください。

Profile Managementプロファイルをリセットする

- user1のプロファイルをリセットしたいとします。New-BrokerMachineCommand PowerShellコマンドを使用します。例：
  - `New-BrokerMachineCommand -Category UserProfileManager -CommandName "ResetUpmProfile" -DesktopGroups 1 -CommandData $byteArray -SendTrigger logon -user domain1\user1`

> **重要:**
>
> `CommandData $byteArray`は次の形式である必要があります: `<SID>[,<backup path>]`。バックアップパスを指定しない場合、Profile Managementは現在の日時で名前が付けられたバックアップフォルダーを生成します。

Windowsローミングプロファイルをリセットする

- user1 のローミングプロファイルをリセットしたいとします。New-BrokerMachineCommand PowerShell コマンドを使用します。例:
  - `New-BrokerMachineCommand -Category UserProfileManager -CommandName "ResetRoamingProfile" -DesktopGroups 1 -CommandData $byteArray -SendTrigger logon -user domain1\user1`

セッションを記録する

Directorの**ユーザー詳細**画面と**マシン詳細**画面にあるセッション記録コントロールを使用して、ICA®セッションを記録できます。この機能は、**Premium**サイトのお客様にご利用いただけます。

DirectorConfig ツールを使用して Director でセッション録画を構成するには、録画ポリシーの作成と有効化 の「**Director でセッション録画サーバーを使用するように構成する**」セクションを参照してください。 セッション録画コントロールは、ログインしているユーザーがセッション録画ポリシーを変更する権限を持っている場合にのみ Director で利用できます。この権限は、録画ポリシーの作成と有効化 で説明されているように、セッション録画承認コンソールで設定できます。

> **注：** Director またはセッション録画ポリシーコンソールを通じてセッション録画設定に加えられた変更は、その後の ICA セッションから有効になります。

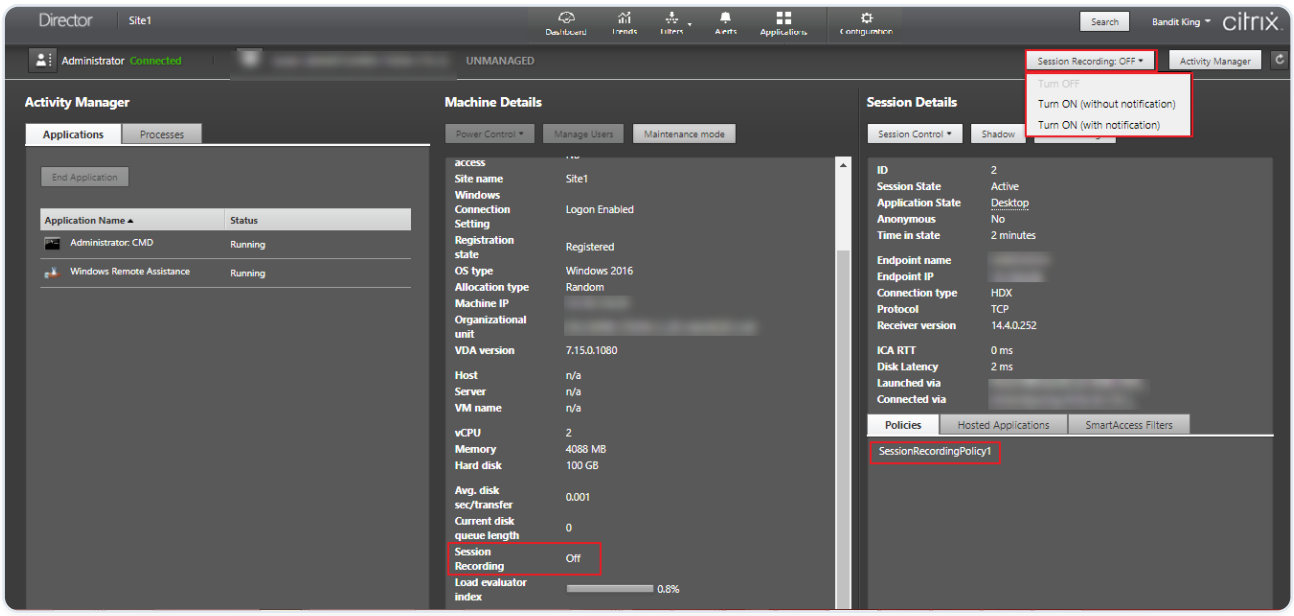
Directorのセッション記録コントロール

アクティビティマネージャーまたは**ユーザー詳細**画面で、特定のユーザーに対してセッション録画を有効にできます。その後のセッションは、サポートされているすべてのサーバーで特定のユーザーに対して録画されます。

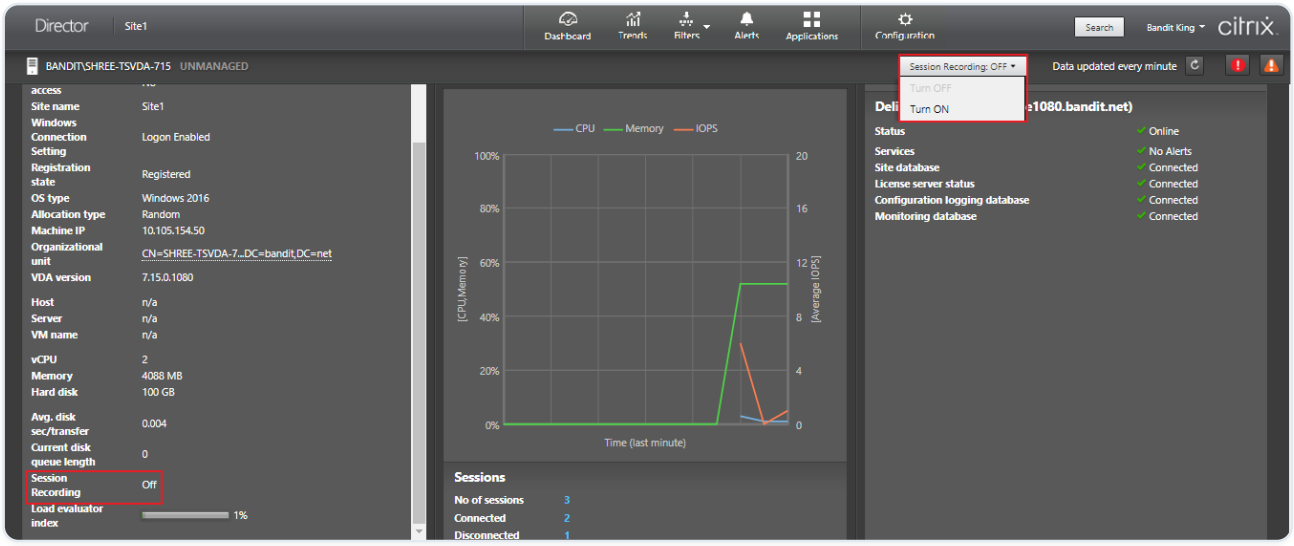
次のことができます。

- オンにする（通知あり） - ICA セッションにログオンすると、ユーザーにセッションが録画されていることが通知されます。
- オンにする（通知なし） - ユーザーに通知することなく、セッションはサイレントに録画されます。
- オフにする - ユーザーのセッション記録を無効にする。

ポリシーパネルには、アクティブなセッション記録ポリシーの名前が表示されます。



マシン詳細ページから、特定のコンピューターに対してセッション録画を有効にできます。その後のコンピューター上のセッションは録画されます。**マシン詳細**パネルには、そのコンピューターのセッション録画ポリシーのステータスが表示されます。



機能互換性マトリックス

Citrix Director 7 2203 は以下と互換性があります:

- Citrix Virtual AppsおよびDesktops™ 7 2112 以降
- Citrix Virtual AppsおよびDesktops 7 1912 長期サービスリリース

各サイト内で、Director を以前のバージョンの Delivery Controller™ とともに使用することはできますが、Director の最新バージョンのすべての機能が利用できるとは限りません。Citrix は、Director、Delivery Controller、および VDA を同じバージョンにすることを推奨しています。

> **注：**
>
> Delivery Controller をアップグレードした後、Studio を開くとサイトのアップグレードを促されます。詳細については、展開のアップグレード の「**アップグレードシーケンス**」セクションを参照してください。

> Director のアップグレード後に初めてログインすると、構成済みのサイトでバージョンチェックが実行されます。いずれかのサイトが Director より古いバージョンの Controller を実行している場合、Director コンソールにサイトのアップグレードを推奨するメッセージが表示されます。さらに、サイトのバージョンが Director より古い間は、この不一致を示すメモが Director ダッシュボードに表示され続けます。

注：

以前のバージョンの Citrix Director では、最近の VDA バージョンで実行されているユーザーセッションに適用されたポリシーは表示されません。Citrix Director 1912 およびそれ以前のバージョンでは、VDA バージョン 2003 以降で実行されているユーザーセッションに適用されたポリシーは表示されません。これらのポリシーを表示するには、Citrix Director バージョン 2003 以降を使用してください。

Director の特定の機能と、必要な Delivery Controller (DC)、VDA、その他の依存コンポーネントの最小バージョン、およびライセンスエディションを以下に示します。

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
1909	Citrix Analytics for Performance を使用してオンプレミスサイトを構成する(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/director/install-and-configure/onboarding.html)	DC 7 1906および VDA 1906	すべて
1906	セッションの自動再接続	DC 7 1906および VDA 1906	すべて
1906	セッション起動時間	DC 7 1906および VDA 1903	すべて
1906	デスクトッププロービング	DC 7 1906 と シトリックス プローブ エージェント 1903	プレミアム
7.9以降	プロファイルロードにおけるCitrix Profile Managementの期間	VDA 1903	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
1811	プロファイルドリルダウン	DC 7 1811およびVDA 1811	すべて
1811	ハイパーバイザーアラート監視	DC 7 1811	プレミアム
1811	アプリケーションプロービング	DC 7 1811 および Citrix アプリケーション プローブ エージェント 1811	プレミアム
1811	Microsoft RDS ライセンスの健全性	DC 7 1811 および VDA 7.16	すべて
1808	フィルターデータの書き出し	DC 7 1808	すべて
1808	インタラクティブセッションのドリルダウン	DC 7 1808およびVDA 1808	すべて
1808	GPOのドリルダウン	DC 7 1808およびVDA 1808	すべて
1808	OData APIを使用したマシンの履歴データ利用可能	DC 7 1808	すべて
7.18	アプリケーションプロービング	DC 7.18	プレミアム (旧 Platinum)
7.18	スマートアラートポリシー	DC 7.18	プレミアム (旧 Platinum)
7.18	Health Assistant リンク	なし	すべて
7.18	インタラクティブセッションのドリルダウン	なし	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
7.17	PIV スマートカード認証	なし	すべて
7.16	アプリケーション分析	DC 7.16およびVDA 7.15	すべて
7.16	OData API バージョン4	DC 7.16	すべて
7.16	Shadow Linux VDA ユーザー	VDA 7.16	すべて
7.16	ドメインローカルグループのサポート	なし	すべて
7.16	マシンコンソールアクセス	DC 7.16	すべて
7.15	アプリケーション障害監視	DC 7.15およびVDA 7.15	すべて
7.14	アプリケーション中心のトラブルシューティング	DC 7.13およびVDA 7.13	すべて
7.14	ディスク監視	DC 7.14およびVDA 7.14	すべて
7.14	GPU監視	DC 7.14およびVDA 7.14	すべて
7.13	セッション詳細パネルのトランスポートプロトコル	DC 7.x および VDA 7.13	すべて
7.12	ユーザーフレンドリーな接続およびマシン障害の説明	DC 7.12 および VDA 7.x	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
7.12	Enterpriseエディションでの履歴データ可用性の向上	DC 7.12 および VDA 7.x	エンタープライズ
7.12	カスタムレポート	DC 7.12 および VDA 7.x	プレミアム (旧 Platinum)
7.11	リソース使用率レポート	DC 7.11およびVDA 7.11	すべて
7.11	CPU、メモリ、ICA RTT条件に対するアラート機能の拡張	DC 7.11およびVDA 7.11	プレミアム (旧 Platinum)
7.11	レポートのエクスポート機能の改善	DC 7.11およびVDA 7.x	すべて
7.11	Citrix ADMとの統合	DC 7.11、VDA 7.x、およびMASバージョン11.1ビルド49.16	プレミアム (旧 Platinum)
7.9	ログオン期間の内訳	DC 7.9 および VDA 7.x	すべて
7.7	プロアクティブな監視とアラート	DC 7.7 および VDA 7.x	プレミアム (旧 Platinum)
7.7	SCOM連携(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/director/site-analytics/alerts-notifications.html#configure-scom-alerts-integration)	DC 7.7、VDA 7.x、SCOM 2012 R2、および PowerShell 3.0	プレミアム (旧 Platinum)
7.7	Windows認証統合	DC 7.x および VDA 7.x	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
7.7	シングルセッションおよびマルチセッションOSの使用状況	DC 7.7 および VDA 7.x	プレミアム (旧 Platinum)
7.6.300	Framehawk仮想チャネルのサポート(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/director/troubleshoot-deployments/user-issues/hdx-channel-reports.html)	DC 7.6 および VDA 7.6	すべて
7.6.200	セッション記録の統合(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/director/troubleshoot-deployments/user-issues/record-sessions.html)	DC 7.6 および VDA 7.x	プレミアム (旧 Platinum)
7	HDX Insightの統合(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/director/install-and-configure/hdx-insight.html)	DC 7.6、VDA 7.x、およびCitrix ADM	プレミアム (旧 Platinum)

データ粒度と保持

データ値の集計

Monitor Serviceは、ユーザーセッションの使用状況、ユーザーログオンパフォーマンスの詳細、セッション負荷分散の詳細、接続およびマシン障害情報など、さまざまなデータを収集します。データはカテゴリに応じて異なる方法で集計されます。OData Method APIを使用して提示されるデータ値の集計を理解することは、データを解釈するために不可欠です。例:

- 接続されたセッションとマシン障害は一定期間に発生します。したがって、それらは期間中の最大値として公開されます。
- ログオン期間は時間の長さを測定するものであるため、期間中の平均値として公開されます。
- ログオン数と接続障害は一定期間に発生した回数であるため、期間中の合計値として公開されます。

同時データ評価

セッションは、同時と見なされるためには重複している必要があります。ただし、時間間隔が1分の場合、その1分間のすべてのセッション（重複しているかどうかにかかわらず）は同時と見なされます。間隔のサイズが非常に小さいため、精度を計算するのに伴うパフォーマンスオーバーヘッドは、追加される価値に見合いません。セッションが同じ時間内に発生しても、同じ分内に発生しない場合、それらは重複しているとは見なされません。

サマリーテーブルと生データの相関

データモデルは、メトリックを2つの異なる方法で表します。

- サマリーテーブルは、分、時間、日ごとの時間粒度でメトリックの集計ビューを表します。
- 生データは、セッション、接続、アプリケーション、およびその他のオブジェクトで追跡される個々のイベントまたは現在の状態を表します。

API呼び出し間またはデータモデル自体内でデータを相関させようとするときは、以下の概念と制限を理解することが重要です。

- **部分的な間隔のサマリーデータはありません。** メトリックのサマリーは、長期間にわたる履歴トレンドのニーズを満たすように設計されています。これらのメトリックは、完全な間隔でサマリーテーブルに集計されます。データ収集の開始時（利用可能な最も古いデータ）または終了時の部分的な間隔には、サマリーデータはありません。1日の集計（Interval=1440）を表示する場合、これは最初と最新の不完全な日にはデータがないことを意味します。これらの部分的な間隔には生データが存在する可能性がありますが、それは決して要約されません。特定のデータ粒度について、特定のサマリーテーブルから最小および最大のSummaryDateを抽出することで、最も早い集計間隔と最も遅い集計間隔を決定できます。SummaryDate列は間隔の開始を表します。Granularity列は、集計データの期間の長さを表します。
- **時間による相関。** メトリックは、前述のセクションで説明されているように、完全な間隔でサマリーテーブルに集計されます。これらは履歴トレンドに使用できますが、生イベントはトレンド分析のために要約されたものよりも現在の状態をより正確に反映している可能性があります。サマリーと生データの時間ベースの比較では、発生する可能性のある部分的な間隔、または期間の開始と終了にはサマリーデータがないことを考慮する必要があります。

- **見逃されたイベントと潜在的なイベント。** 集計テーブルに集計されるメトリックは、イベントが見逃されたり、集計期間に対して潜在的であったりする場合、わずかに不正確になる可能性があります。モニターサービスは正確な現在の状態を維持しようとしますが、見逃されたイベントや潜在的なイベントのために、集計テーブルの集計を再計算するために過去に遡ることはありません。
- **接続の高可用性。** 接続の高可用性中、現在の接続のサマリーデータカウントにギャップが生じますが、セッションインスタンスは引き続き生データで実行されます。
- **データ保持期間。** サマリーテーブルのデータは、生イベントデータのスケジュールとは異なるグルーミングスケジュールで保持されます。サマリーテーブルまたは生テーブルからグルーミングによってデータが削除されたため、データが欠落している可能性があります。保持期間は、サマリーデータの異なる粒度によっても異なる場合があります。粒度の低いデータ（分単位）は、粒度の高いデータ（日単位）よりも早くグルーミングされます。グルーミングによってある粒度からデータが欠落している場合でも、より高い粒度で見つかる可能性があります。API呼び出しは要求された特定の粒度のみを返すため、ある粒度でデータが受信されないからといって、同じ期間のより高い粒度でデータが存在しないという意味ではありません。
- **タイムゾーン。** メトリックはUTCタイムスタンプで保存されます。サマリーテーブルは、時間単位のタイムゾーン境界で集計されます。時間単位の境界に該当しないタイムゾーンの場合、データが集計される場所に関して多少の不一致が生じる可能性があります。

粒度と保持

Directorによって取得される集計データの粒度は、要求された時間 (T) スパンの関数です。ルールは次のとおりです。

- 0 \< T \<= 1時間 - 分単位の粒度を使用
- 0 \< T \<= 30日 - 時間単位の粒度を使用
- T \> 31日 - 日単位の粒度を使用

集約データから取得されない要求データは、生のセッションおよび接続情報から取得されます。このデータは急速に増加する傾向があるため、独自のグルーミング設定があります。グルーミングにより、関連データのみが長期的に保持されます。グルーミングは、レポート作成に必要な粒度を維持しながら、パフォーマンスを向上させます。Premiumライセンスサイトのお客様は、グルーミング保持期間を希望する保持日数に変更できます。変更しない場合は、デフォルトが使用されます。サイトデータベースとの接続が失われた場合、Monitor Serviceは、以下の表に指定されているPremiumエンタイトルメントのデフォルトの保持日数を使用します。

設定にアクセスするには、Delivery Controller™ で次のPowerShellコマンドを実行します。

```
asnp Citrix.*

 Get-MonitorConfiguration

 Set-MonitorConfiguration -<setting name> <value>
```

#	設定名	影響を受けるスキーマテーブル	モニターページで影響を受けるテーブルとグラフ	PREMIUMの保持日数	ADVANCEDの保持日数
1	GroomSessionsRetentionDays	MonitorData.Session および Monitordata.Connection テーブル	この設定は、トレンドページのセッションの詳細、ユーザーセッションごとのログオン期間、アプリケーションベースの使用状況テーブルに影響します。	90	31
2	GroomFailuresRetentionDays	MonitorData.MachineFailureLog および MonitorData.ConnectionFailureLog	トレンドページ：この設定は、障害タブのグラフとテーブルに影響します。	90	31
3	GroomLoadIndexesRetentionDays	MonitorData.LoadIndex	この設定は、トレンドページの「ロードエバリュエーターイン	3	3

#	設定名	影響を受けるスキーマテーブル	モニターページで影響を受けるテーブルとグラフ	PREMIUMの保持日数	ADVANCEDの保持日数
			デックス」タブに表示されるデータに影響します。		
4	GroomDeletedRetentionDays	LifecycleStateが「Deleted」であるMonitorData.Machine、MonitorData.Catalog、MonitorData.DesktopGroup、およびMonitorData.Hypervisorエンティティ。この設定は、関連するSession、SessionDetail、Summary、Failure、またはLoadIndexレコードも削除します。	LifecycleStateが「Deleted」であるMachine、Catalog、DesktopGroup、およびHypervisorエンティティ。この設定は、関連するSession、SessionDetail、Summary、Failure、またはLoadIndexレコードも削除します。	90	31
5	GroomSummariesRetentionDays	MonitorData.DesktopGroupSummary、MonitorData	この設定は、トレンドページ上のすべてのグラフデー	365	31

#	設定名	影響を受けるスキーマテーブル	モニターページで影響を受けるテーブルとグラフ	PREMIUMの保持日数	ADVANCEDの保持日数
		.FailureLogSummary、およびMonitorData.LoadIndexSummary	タに影響します。		
6	GroomMachineHotfixLogRetentionDays	MonitorData.Hotfix	この設定は、マシン詳細ページに表示されるVDAホットフィックスデータに影響します。	90	31
7	GroomMinuteRetentionDays	すべてのサマリーテーブル	この設定は、トレンドページに表示される「過去2時間」の時間期間のグラフに影響します。	3	3
8	GroomHourlyRetentionDays	すべてのサマリーテーブル	これは、トレンドページに表示される週次グラフに影響します。	32	31
9	GroomApplicationInstanceRetentionDays	MonitorData.ApplicationInstance	この設定は、キャパシティ管理タブのグラフとテーブ	90	該当なし

#	設定名	影響を受けるスキーマテーブル	モニターページで影響を受けるテーブルとグラフ	PREMIUMの保持日数	ADVANCEDの保持日数
			ル、およびトレンドページのアプリケーション使用状況テーブルに影響します。		
10	GroomNotificationLogRetentionDays	MonitorData.NotificationLog	この設定は、Monitorに表示されるアラートに影響します。	90	該当なし
11	GroomResourceUsageRawDataRetentionDays	MonitorData.Resourceutilization	この設定は、「Historical Machine Utilization」の「Machine Details」ページに表示されるCPUおよびメモリのグラフに影響します。	3	3
12	GroomResourceUsageMinuteDataRetentionDays	MonitorData.ResourceUtilizationSummary	この設定は、「Historical Machine Utilization」の「Machine Details」	7	7

#	設定名	影響を受けるスキーマテーブル	モニターページで影響を受けるテーブルとグラフ	PREMIUMの保持日数	ADVANCEDの保持日数
			ページに表示される「Last 2 Hours」の時間期間のCPUおよびメモリのグラフに影響します。		
13	GroomResourceUsageHourDataRetentionDays	MonitorData.Resourceutilizationsummary	この設定は、「Historical Machine Utilization」の「Machine Details」ページに表示されるCPUおよびメモリのグラフに影響します。	30	30
14	GroomResourceUsageDayDataRetentionDays	MonitorData.Resourceutilizationsummary	この設定は、トレンドページの「リソース使用率」のマシンに表示されるCPUとメモリのグラフ、および特定の「マシン使用率」ページ	365	31

#	設定名	影響を受けるスキーマテーブル	モニターページで影響を受けるテーブルとグラフ	PREMIUMの保持日数	ADVANCEDの保持日数
			に影響します。		
15	GroomProcessUsageRawDataRetentionDays	MonitorData.ProcessUtilization	この設定は、マシンの履歴使用状況ページに表示されるプロセスごとのリソース傾向情報に影響します。	1	1
16	GroomProcessUsageMinuteDataRetentionDays	MonitorData.ProcessUtilizationMinuteSummary	この設定は、履歴マシン使用率ページに表示される「過去2時間」のプロセスごとのCPUとメモリ使用量グラフに影響します。	3	3
17	GroomProcessUsageHourDataRetentionDays	MonitorData.ProcessUtilizationHourSummary	この設定は、マシンの履歴使用状況ページに表示されるプロセスごとのCPUおよびメモリ使用量の傾向に影響します。	7	7

#	設定名	影響を受けるスキーマテーブル	モニターページで影響を受けるテーブルとグラフ	PREMIUMの保持日数	ADVANCEDの保持日数
18	GroomProcessUsageDayDataRetentionDays	MonitorData.ProcessUtilizationDaySummary	この設定は、マシンの履歴使用状況ページに表示されるプロセスごとのCPUおよびメモリ使用量の傾向に影響します。	30	30
19	GroomSessionMetricsDataRetentionDays	MonitorData.Sessionmetrics	この設定は、ユーザー詳細ページの「セッションパフォーマンス」タブに表示されるすべてのグラフに影響します。	1	1
20	GroomMachineMetricDataRetentionDays	MonitorData.Machinemetrics	この設定は、トレンドページの「リソース使用率」タブにあるグラフと表に影響します。	3	3
21	GroomMachineMetricDaySummaryD	MonitorData.MachineMe	この設定は、トレンドページの	365	31

#	設定名	影響を受けるスキーマテーブル	モニターページで影響を受けるテーブルとグラフ	PREMIUMの保持日数	ADVANCEDの保持日数
	ataRetentionDays	tricDaySummary	「リソース使用率」タブにあるグラフと表に影響します。		
22	GroomApplicationErrorsRetentionDays	MonitorData.ApplicationError	この設定は、アプリケーションページの「アプリケーションエラー」列に表示されるエラー詳細に影響します。	1	1
23	GroomApplicationFaultsRetentionDays	MonitorData.Applicationfailure	この設定は、アプリケーションページの「アプリケーション障害」列に影響します。	1	1

注意:

Monitor Serviceデータベースの値を変更した場合、新しい値を有効にするにはサービスを再起動する必要があります。Monitor Serviceデータベースへの変更は、Citrixサポートの指示の下でのみ行うことをお勧めします。

> 設定GroomProcessUsageRawDataRetentionDays、GroomResourceUsageRawDataRetentionDays、およびGroomSessionMetricsDataRetentionDaysはデフォルト値の1に制限されており、GroomProcessUsageMinuteDataRetentionDaysはデフォルト値の3に制限されています。プロセス使用状況データは急速に増加する傾向があるため、これらの値を設定するPowerShellコマンドは無効になっています。 また、ライセンスベースの保持設定は次のとおりです。

- **Premiumライセンスサイト -** すべての設定のグルーミング保持期間は1000日（Citrixは365日を推奨）に制限されています。
- **Advancedライセンスサイト -** すべての設定のグルーミング保持期間は31日に制限されています。
- **その他のすべてのサイト -** すべての設定のグルーミング保持期間は7日に制限されています。

例外:

- GroomApplicationInstanceRetentionDays は、Premiumライセンスサイトでのみ設定できます。
- GroomApplicationErrorsRetentionDays および GroomApplicationFaultsRetentionDays は、Premiumライセンスサイトでは31日間に制限されます。

長期間データを保持すると、テーブルサイズに以下の影響があります:

- **時間単位のデータ。** 時間単位のデータが最大2年間データベースに残ることを許可すると、1000のデリバリーグループを持つサイトでは、データベースが次のように増加する可能性があります:

  1000のデリバリーグループ x 24時間/日 x 365日/年 x 2年 = 17,520,000行のデータ。集計テーブル内のこれほど大量のデータがパフォーマンスに与える影響は甚大です。ダッシュボードデータはこのテーブルから取得されるため、データベースサーバーへの要件は大きくなる可能性があります。過度に大量のデータは、パフォーマンスに劇的な影響を与える可能性があります。

- **セッションおよびイベントデータ。** セッションが開始され、接続/再接続が行われるたびに収集されるデータです。大規模なサイト（10万ユーザー）の場合、このデータは急速に増加します。たとえば、これらのテーブルの2年分のデータは1TBを超えるデータとなり、ハイエンドのエンタープライズレベルのデータベースが必要になります。

Citrix Director の障害理由とトラブルシューティング

以下の表は、さまざまな障害カテゴリ、その理由、および問題を解決するために必要なアクションについて説明しています。詳細については、「列挙型、エラーコード、および説明」を参照してください。

接続障害エラー

カテゴリ	理由	問題	アクション
該当なし	[0] 不明。このエラーコードはマッピングされていません。	監視サービスは、ブローカリングサービスから共有された情報から、報告された起動または接続障害の理由を判断できません。	コントローラーでCDFログを収集し、Citrixサポートに連絡してください。
[0] なし	[1] なし	なし	該当なし
[2] MachineFailure	[2] SessionPreparation	デリバリーコントローラーからVDAへのセッション準備要求が失敗しました。考えられる原因：コントローラーとVDA間の通信の問題、Broker Serviceが準備要求を作成する際に発生した問題、またはVDAが要求を受け入れない原因となるネットワークの問題。	コントローラーとVDA間の通信問題を引き起こす一般的な問題については、ナレッジセンターの記事「Citrix Virtual Apps and Desktopsにおけるデリバリーコントローラーへの Virtual Delivery Agent登録のトラブルシューティング」に記載されているトラブルシューティング手順を参照してください。
[2] MachineFailure	[3] RegistrationTimeout	VDAは電源がオンになっていましたが、デリバリーコントローラーへの登録中にタイムアウトが発生しました。	Citrix Broker Serviceがデリバリーコントローラーで実行されていること、およびDesktopサービスがVDAで実行されてい

カテゴリ	理由	問題	アクション
			ることを確認します。停止している場合は、それぞれを開始します。
[1] クライアント接続の失敗	[4] ConnectionTimeout	セッション起動のためにVDAが準備された後、クライアントがVDAに接続しませんでした。セッションは正常に仲介されましたが、クライアントがVDAに接続するのを待っている間にタイムアウトが発生しました。考えられる原因：ファイアウォール設定、ネットワーク中断、またはリモート接続を妨げる設定。	Directorコンソールで、クライアントが現在アクティブな接続を持っているかどうかを確認します。アクティブな接続がある場合、ユーザーは影響を受けていません。セッションが存在しない場合は、クライアントとVDAのイベントログでエラーを確認します。クライアントとVDA間のネットワーク接続に関する問題を解決します。
[4] 利用可能なライセンスなし	[5] ライセンス	ライセンス要求が失敗しました。考えられる原因：ライセンス数が不足しているか、ライセンスサーバーが30日以上ダウンしている。	ライセンスサーバーがオンラインで到達可能であることを確認します。ライセンスサーバーへのネットワーク接続の問題を解決するか、ライセンスサーバーが誤動作しているように見える場合は再起動します。環境内に十分なライセンスがあることを確認し、必要に応じて追加で割り当てます。
[1] クライアント接続の失敗	[6] チケット	チケット発行中に障害が発生しました。	デリバリーグループで定義されたユー

カテゴリ	理由	問題	アクション
		これは、VDAへのクライアント接続が仲介された要求と一致しないことを示しています。起動要求チケットはBrokerによって準備され、ICA®ファイルで配信されます。ユーザーがセッションを起動しようとすると、VDAはICAファイル内の起動チケットをBrokerで検証します。考えられる原因：ICAファイルが破損しているか、ユーザーが不正な接続を試みている。	ザーグループに基づいて、ユーザーがアプリケーションまたはデスクトップにアクセスできることを確認します。ユーザーにアプリケーションまたはデスクトップを再起動するよう指示し、これが一時的な問題であるかどうかを判断します。問題が再度発生する場合は、クライアントデバイスのイベントログでエラーを確認します。ユーザーが接続しようとしているVDAが登録されていることを確認します。登録されていない場合は、VDAのイベントログを確認し、登録に関する問題を解決します。
[1] クライアント接続の失敗	[7] その他	クライアントがVDAに最初に接続した後、接続シーケンスを完了する前に、セッションがVDAから終了したと報告されました。	起動前にユーザーによってセッションが終了されなかったことを確認します。セッションを再起動してみてください。問題が解決しない場合は、CDFログを収集してCitrixサポートに連絡してください。
[1] クライアント接続の失敗	[8] 一般的な失敗	セッションの起動に失敗しました。考え	Citrix Broker Serviceが実行されているこ

カテゴリ	理由	問題	アクション
		られる原因：ブローカーが起動中または初期化中にブローカーによる起動が要求されたか、起動のブローカー処理フェーズ中に内部エラーが発生しました。	とを確認し、セッションの起動を再試行してください。
[5] 構成	[9] メンテナンスモード	VDA、またはVDAが属するデリバリーグループがメンテナンスモードに設定されています。	メンテナンスモードが必要かどうかを判断します。不要な場合は、該当するデリバリーグループまたはマシンでメンテナンスモードを無効にし、ユーザーに再接続を試みるよう指示してください。
[5] 構成	[10] アプリケーション無効	アプリケーションは管理者によって無効にされているため、エンドユーザーはアクセスできません。	アプリケーションが本番環境で使用されることを意図している場合は、アプリケーションを有効にし、ユーザーに再接続するよう指示してください。
[4] 利用可能なライセンスなし	[11] ライセンス機能が拒否されました	使用されている機能は、既存のライセンスではカバーされていません。	既存のCitrix Virtual Apps and Desktops™ライセンスのエディションとタイプでカバーされている機能を確認するには、Citrixの営業担当者にお問い合わせください。

カテゴリ	理由	問題	アクション
[3] NoCapacityAvailable	[13] セッション制限に達しました	すべてのVDAが使用中で、これ以上セッションをホストする容量がありません。考えられる原因: すべてのVDAが使用中である（シングルセッションOS VDAの場合）、またはすべてのVDAが構成された最大同時セッション数に達している（マルチセッションOS VDAの場合）。	メンテナンスモードのVDAがないか確認してください。より多くの容量を解放するために不要な場合は、メンテナンスモードを無効にしてください。サーバーVDAあたりのセッション数を増やすには、Citrixポリシー設定の**最大セッション数**の値を増やすことを検討してください。マルチセッションOS VDAを追加することを検討してください。シングルセッションOS VDAを追加することを検討してください。
[5] 構成	[14] 許可されていないプロトコル	ICAおよびRDPプロトコルは許可されていません。	デリバリーコントローラーで**Get-BrokerAccessPolicyRule** PowerShellコマンドを実行し、**AllowedProtocols**の値に目的のプロトコルがすべてリストされていることを確認してください。この問題は、構成ミスがある場合にのみ発生します。
[5] 構成	[15] リソースが利用できません	ユーザーが接続しようとしているアプリケーションまたはデスクトップが利用できません。このアプ	アプリケーションまたはデスクトップがまだ公開されており、VDAがメンテナンスモードではない

カテゴリ	理由	問題	アクション
		リケーションまたはデスクトップが存在しないか、実行できるVDAがありません。考えられる原因: アプリケーションまたはデスクトップが非公開になっている、アプリケーションまたはデスクトップをホストしているVDAが最大負荷に達している、またはアプリケーションまたはデスクトップがメンテナンスモードに設定されている。	ことを確認してください。マルチセッションOS VDAがフルロード状態であるかどうかを判断してください。もしそうであれば、より多くのマルチセッションOS VDAをプロビジョニングしてください。接続に利用可能なシングルセッションOS VDAがあることを確認してください。必要に応じて、より多くのシングルセッションOS VDAをプロビジョニングしてください。
[5] 構成	[16] ActiveSessionReconnectDisabled	ICAセッションはアクティブで、別のエンドポイントに接続されています。ただし、**アクティブセッションの再接続**が無効になっているため、クライアントはアクティブなセッションに接続できません。	デリバリーコントローラーで、**アクティブセッションの再接続**が有効になっていることを確認します。レジストリの **HKEY_LOCAL_MACHINE\Software\Citrix\Desktop\Server** にある **DisableActiveSessionReconnect**の値が0に設定されていることを確認します。
[2] MachineFailure	[17] NoSessionToReconnect	クライアントは特定のセッションへの再接続を試みましたが、セッションは終了しました。	ワークスペースコントロールの再接続を再試行してください。

カテゴリ	理由	問題	アクション
[2] MachineFailure	[18] SpinUpFailed	セッション起動のためにVDAの電源をオンにできません。これはハイパーバイザーによって報告された問題です。	マシンがまだ電源オフの状態である場合は、Citrix Studioからマシンの起動を試行します。これが失敗する場合は、ハイパーバイザーの接続と権限を確認します。VDAがPVSプロビジョニングされたマシンの場合は、PVSコンソールでマシンが実行されていることを確認します。実行されていない場合は、マシンにパーソナルvDiskが割り当てられていることを確認し、ハイパーバイザーにログインしてVMをリセットします。
[2] MachineFailure	[19] 拒否	デリバリーコントローラーは、エンドユーザーからの接続に備えるようVDAに要求を送信しますが、VDAはこの要求を積極的に拒否します。	pingで、デリバリーコントローラーとVDAが正常に通信できることを確認します。できない場合は、ファイアウォールまたはネットワークルーティングの問題を解決してください。
[2] MachineFailure	[20] 構成セットの失敗	セッション起動中に、デリバリーコントローラーがポリシー設定やセッション情報などの必要な構成データをVDAに送信しませんでし	-

カテゴリ	理由	問題	アクション
		た。考えられる原因としては、コントローラーとVDA間の通信の問題、構成セット要求の作成中にBroker Serviceで発生した問題、またはVDAが要求を受け入れない原因となるネットワークの問題が挙げられます。	
[3] NoCapacityAvailable	[21] 最大インスタンス数を超過	アプリケーションの最大インスタンス数に達しました。VDA上でアプリケーションの追加インスタンスを開くことはできません。この問題は、アプリケーション制限機能に関連しています。	ライセンスが許す場合、アプリケーション設定の「**同時に実行するインスタンス数を制限する**」をより高い値に増やすことを検討してください。
[3] NoCapacityAvailable	[22] ユーザーごとの最大インスタンス数を超過	ユーザーがアプリケーションの複数のインスタンスを開こうとしていますが、アプリケーションはユーザーごとに1つのインスタンスのみを許可するように構成されています。この問題は、アプリケーション制限機能に関連しています。	デフォルトでは、ユーザーごとにアプリケーションのインスタンスは1つのみ許可されています。ユーザーごとに複数のインスタンスが必要な場合は、アプリケーション設定で「**ユーザーごとに1つのインスタンスに制限する**」設定をクリアすることを検討してください。
[1] クライアント接続の失敗	[23] 通信エラー	デリバリーコントローラーは、接続の準備を要求するなど	すでに開始されている場合は、VDA上のデスクトップサービ

カテゴリ	理由	問題	アクション
		の情報をVDAに送信しようとしましたが、通信中にエラーが発生しました。これはネットワークの中断が原因である可能性があります。	スを再起動して登録プロセスを再開し、VDAが正常に登録されていることを確認します。アプリケーションイベントログの詳細を通じて、VDA用に構成されているデリバリーコントローラーが正確であることを確認します。
[3] NoCapacityAvailable	[100] NoMachineAvailable監視サービスは、[12] NoDesktopAvailableをこのエラーコードに変換します。	セッションを起動するために割り当てられたVDAが無効な状態であるか、利用できません。考えられる原因：VDAの電源状態が不明または利用できない、前回のユーザーセッション以降VDAが再起動されていない、現在のセッションでセッション共有が必要なのに無効になっている、またはVDAがデリバリーグループまたはサイトから削除された。	VDAがデリバリーグループ内にあることを確認します。ない場合は、適切なデリバリーグループに追加します。公開された共有デスクトップまたはユーザーが要求したアプリケーションを起動できるように、十分なVDAが登録され、準備状態にあることを確認します。VDAをホストしているハイパーバイザーがメンテナンスモードではないことを確認します。
[2] MachineFailure	[101] MachineNotFunctional。監視サービスは、[12] NoDesktopAvailableをこのエラーコードに変換します。	VDAが動作していません。考えられる原因：VDAがデリバリーグループから削除された、VDAが未登録である、VDAの電源状態が利用できない、またはVDAが	VDAがデリバリーグループ内にあることを確認します。ない場合は、適切なデリバリーグループに追加します。VDAがCitrix Studioで電源オンとして表示されていることを確認しま

カテゴリ	理由	問題	アクション
		内部的な問題を抱えている。	す。複数のマシンの電源状態が不明な場合は、ハイパーバイザーへの接続に関する問題またはホストの障害を解決します。VDAをホストしているハイパーバイザーがメンテナンスモードではないことを確認します。これらの問題が解決されたら、VDAを再起動します。

マシン障害の種類

エラーコード	エラーコードID	問題	アクション
不明	-	-	-
未登録	3	-	-
MaxCapacity (Director コンソールでは最大負荷として表示)	4	マシンが最大容量、つまり最大負荷インデックスを報告しています	すべてのハイパーバイザーの電源がオンになっていることを確認します。ハイパーバイザーの容量を増やすか、ハイパーバイザーを追加することによって、影響を受けるデリバリーグループにマシンを追加します。
StuckOnBoot	2	VMが起動シーケンスを完了せず、ハイパーバイザーと通信していません。	VMがハイパーバイザー上で正常に起動したことを確認します。OSの問題など、VM上の他のメッセージを確認しま

エラーコード	エラーコードID	問題	アクション
			す。ハイパーバイザーツールがVMにインストールされていることを確認します。VDAがVMにインストールされていることを確認します。
FailedToStart	1	VMがハイパーバイザー上で起動しようとしたときに問題が発生しました。	ハイパーバイザーのログを確認します。
なし	0	-	-

マシンの登録解除理由 (障害の種類が「未登録」または「不明」の場合に適用)

エラーコード	エラーコードID	問題	アクション
AgentShutdown	0	VDAは正常にシャットダウンされました。	既存の電源管理ポリシーに基づいてVDAがオフになっていると想定されない場合は、VDAの電源をオンにします。イベントログのエラーを確認します。
AgentSuspended	1	VDAは休止状態またはスリープモードです。	VDA を休止状態から復帰させます。電源設定を介して、Citrix Virtual Apps and Desktops VDA の休止状態を無効にすることを検討してください。

エラーコード	エラーコードID	問題	アクション
IncompatibleVersion	100	Citrixプロトコルバージョンの不一致により、VDAはデリバリーコントローラーと通信できません。	VDAとデリバリーコントローラーのバージョンを合わせてください。
AgentAddressResolutionFailed	101	デリバリーコントローラーはVDAのIPアドレスを解決できませんでした。	VDAマシンアカウントがADに存在することを確認します。存在しない場合は、作成します。DNS内のVDAの名前とIPアドレスが正確であることを確認します。正確でない場合は、修正します。広範囲にわたる場合は、デリバリーコントローラーのDNS設定を検証します。コントローラーから `nslookup` コマンドを実行してDNS解決を確認します。
[Cloud]:AgentAddressResolutionFailed	101	デリバリーコントローラーはVDAのIPアドレスを解決できませんでした。	VDAマシンアカウントがADに存在することを確認します。存在しない場合は、作成します。DNS内のVDAの名前とIPアドレスが正確であることを確認します。正確でない場合は、修正します。
AgentNotContactable	102	デリバリーコントローラーとVDA間で通信の問題が発生しました。	pingを使用して、デリバリーコントローラーとVDAが正常に通信できることを確認します。通信でき

エラーコード	エラーコードID	問題	アクション
			ない場合は、ファイアウォールまたはネットワークの問題を解決してください。コントローラーとVDA間の通信問題を引き起こす一般的な問題については、Knowledge Centerの記事「Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668)」に記載されているトラブルシューティング手順を参照してください。
[Cloud]: AgentNotContactable	102	デリバリーコントローラーとVDA間で通信の問題が発生しました。	コントローラーとVDA間の通信問題を引き起こす一般的な問題については、Knowledge Centerの記事「Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668)」に記載されているトラブルシューティング手順を参照してくださ

エラーコード	エラーコードID	問題	アクション
			い。Citrixサポートに連絡してください。
AgentWrongActiveDirectoryOU	103	Active Directoryの検出設定が誤っています。VDAレジストリで構成されているサイト固有のOU（サイトコントローラー情報がADに保存されている場所）が、別のサイト用です。	Active Directoryの設定が正しいことを確認するか、レジストリ設定を確認してください。
EmptyRegistrationRequest	104	VDAからデリバリーコントローラーに送信された登録要求が空でした。これは、VDAソフトウェアのインストールが破損していることが原因である可能性があります。	VDA上のDesktopサービスを再起動して、登録プロセスを再開し、アプリケーションイベントログを介してVDAが正しく登録されていることを確認してください。
MissingRegistrationCapabilities	105	VDAのバージョンがデリバリーコントローラーと互換性がありません。	VDAをアップグレードするか、VDAを削除してから再インストールしてください。
MissingAgentVersion	106	VDAのバージョンがデリバリーコントローラーと互換性がありません。	問題がすべてのマシンに影響している場合は、VDAソフトウェアを再インストールしてください。
InconsistentRegistrationCapabilities	107	VDAはBrokerにその機能を通知できません。これは、VDAとデリバリーコントローラーのバージョン間の非互換性が原	VDAとデリバリーコントローラーのバージョンを合わせてください。

エラーコード	エラーコードID	問題	アクション
		因である可能性があります。バージョンごとに変更される登録機能は、登録要求と一致しない形式で表現されています。	
NotLicensedForFeature	108	使用しようとしている機能はライセンスされていません。	Citrixライセンスエディションを確認するか、VDAを削除してから再インストールしてください。
[Cloud]: NotLicensedForFeature	108	使用しようとしている機能はライセンスされていません。	Citrixサポートにお問い合わせください。
サポートされていないCredentialSecurityバージョン	109	VDAとデリバリーコントローラーが同じ暗号化メカニズムを使用していません。	VDAとデリバリーコントローラーのバージョンを合わせてください。
無効な登録リクエスト	110	VDAがブローカーに登録リクエストを行いましたが、リクエストの内容が破損しているか無効です。	コントローラーとVDA間の通信問題を引き起こす一般的な問題については、Knowledge Centerの記事「Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668)」に記載されているトラブルシューティング手順を参照してください。

エラーコード	エラーコードID	問題	アクション
シングル/マルチセッションの不一致	111	VDAのオペレーティングシステムタイプは、マシンカタログまたはデリバリーグループと互換性がありません。	VDAを、適切なマシンカタログタイプまたは同じオペレーティングシステムを持つマシンを含むデリバリーグループに追加してください。
FunctionalLevelTooLowForCatalog	112	マシンカタログは、インストールされているVDAバージョンよりも高いVDA機能レベルに設定されています。	VDAのマシンカタログ機能レベルがVDAの機能レベルと一致していることを確認してください。マシンカタログをVDAの機能レベルに合わせてアップグレードまたはダウングレードしてください。
FunctionalLevelTooLowForDesktopGroup	113	デリバリーグループは、インストールされているVDAバージョンよりも高いVDA機能レベルに設定されています。	VDAのデリバリーグループ機能レベルがVDAの機能レベルと一致していることを確認してください。マシンカタログをVDAの機能レベルに合わせてアップグレードまたはダウングレードしてください。
PowerOff	200	VDAが正常にシャットダウンされませんでした。	VDAが電源オン状態であるべき場合は、Citrix StudioからVDAの起動を試み、VDAが正常に起動して登録されることを確認してください。起動または登録に関する問題があればトラブルシューティングを

エラーコード	エラーコードID	問題	アクション
			行ってください。VDAが再び稼働したら、イベントログを確認してシャットダウンの根本原因を特定するのに役立ててください。
AgentRejectedSettingsUpdate	203	Citrixポリシーなどの設定が変更または更新されましたが、VDAへの更新の送信中にエラーが発生しました。これは、更新がインストールされているVDAバージョンと互換性がない場合に発生する可能性があります。	必要に応じてVDAをアップグレードしてください。適用された更新がVDAバージョンでサポートされているかどうかを確認してください。
SessionPrepareFailure	206	ブローカーは、VDAで実行されているセッションの監査を完了しませんでした。	広範囲にわたる場合は、デリバリーコントローラーでCitrix Broker Serviceを再起動してください。
[Cloud]: SessionPrepareFailure	206	ブローカーは、VDAで実行されているセッションの監査を完了しませんでした。	Citrixサポートにお問い合わせください。
ContactLost	207	デリバリーコントローラーがVDAとの接続を失いました。これはネットワーク障害が原因である可能性があります。	デリバリーコントローラーでCitrix Broker Serviceが実行されており、VDAでDesktop Serviceが実行されていることを確認します。停止している場合は、それぞれを開始しま

エラーコード	エラーコードID	問題	アクション
			す。すでに開始されている場合は、VDAでDesktop Serviceを再起動して登録プロセスを再開し、VDAが正常に登録されることを確認します。アプリケーションイベントログの詳細を通じて、VDA用に構成されているデリバリーコントローラーが正確であることを確認します。pingを使用して、デリバリーコントローラーとVDAが正常に通信できることを確認します。通信できない場合は、ファイアウォールまたはネットワークの問題を解決します。
[Cloud]: ContactLost	207	デリバリーコントローラーがVDAとの接続を失いました。これはネットワーク障害が原因である可能性があります。	VDAでDesktop Serviceが実行されていることを確認します。停止している場合は開始します。
BrokerRegistrationLimitReached	301	デリバリーコントローラーが、同時に登録できるVDAの構成済み最大数に達しました。デフォルトでは、デリバリーコントローラーは10,000の同時VDA登録を許可します。	サイトにデリバリーコントローラーを追加するか、サイトを作成することを検討してください。また、**HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer\MaxWorkers** レジス

エラーコード	エラーコードID	問題	アクション
			トリキーを使用して、デリバリーコントローラーに同時に登録できるVDAの数を増やすこともできます。詳細については、Knowledge Centerの記事「Citrix Virtual Apps and Desktops で使用されるレジストリキーエントリ (CTX117446)」を参照してください。この数を増やすと、コントローラーにより多くのCPUおよびメモリリソースが必要になる場合があります。
SettingsCreationFailure	208	ブローカーがVDAに送信する設定と構成のセットを構築しませんでした。ブローカーがデータを収集できない場合、登録は失敗し、VDAは登録解除されます。	デリバリーコントローラーのイベントログでエラーを確認してください。ログに特定の問題が明らかでない場合は、ブローカーサービスを再起動してください。ブローカーサービスが再起動されたら、影響を受けるVDAでデスクトップサービスを再起動し、それらが正常に登録されることを確認してください。
[Cloud]: SettingsCreationFailure	208	ブローカーがVDAに送信する設定と構成のセットを構築しませんでした。ブロー	影響を受けるVDAでデスクトップサービスを再起動し、それらが正常に登録され

エラーコード	エラーコードID	問題	アクション
		カーがデータを収集できない場合、登録は失敗し、VDAは登録解除されます。	ることを確認してください。Citrixサポートに連絡してください。
SendSettingsFailure	204	ブローカーが設定および構成データをVDAに送信しませんでした。ブローカーがデータを収集できるが送信できない場合、登録は失敗します。	単一のVDAに限定される場合は、VDA上のデスクトップサービスを再起動して再登録を強制し、アプリケーションイベントログを介してVDAが正常に登録されることを検証してください。発生したエラーをトラブルシューティングしてください。コントローラーとVDA間の通信問題を引き起こす一般的な問題については、Knowledge Centerの記事「Citrix Virtual Apps and Desktops でのデリバリーコントローラーとのVirtual Delivery Agent登録のトラブルシューティング (CTX136668)」に記載されているトラブルシューティング手順を参照してください。
エージェント要求	2	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
デスクトップの再起動	201	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。

エラーコード	エラーコードID	問題	アクション
デスクトップが削除されました	202	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
セッション監査の失敗	205	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
UnknownError	300	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
RegistrationStateMismatch	302	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
不明	-	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。

サードパーティ通知

Citrix Virtual Apps and Desktops™ のこのリリースには、以下のドキュメントに定義されている条件に基づいてライセンス供与されたサードパーティ製ソフトウェアが含まれている場合があります。

- Citrix Virtual Apps and Desktops サードパーティ通知(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/downloads/third-party-notices-apps-and-desktops.pdf) (PDFダウンロード)
- FlexNet Publisher 2017 (11.15.0.0) の非商用ソフトウェア開示(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/downloads/fnp-licensing-11-15-0-ncsd-summary.pdf) (PDFダウンロード)
- FlexNet Publisher 11.15.0 で使用されている FlexNet Publisher ドキュメント補足 サードパーティおよびオープンソースソフトウェア(/ja-jp/citrix-virtual-apps-desktops/2203-ltsr/downloads/fnp-licensing-11-15-0-opensource.pdf) (PDFダウンロード)

SDKおよびAPI

このリリースでは、いくつかのSDKとAPIが利用可能です。SDKとAPIにアクセスするには、Build anything with Citrixにアクセスしてください。そこから、**Citrix Workspace**を選択して、Citrix Virtual Apps and Desktopsおよび関連コンポーネントのプログラミング情報にアクセスします。

> **注：**

> Citrix Virtual Apps and Desktops™ SDKとCitrix Group Policy SDKは、モジュールまたはスナップインとしてインストールできます。いくつかのコンポーネントSDK（Citrix Licensing、Citrix Provisioning、StoreFrontなど）は、スナップインのみを使用してインストールされます。

> この製品はPowerShellバージョン3から5をサポートしています。

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

このSDKは、Delivery Controller™またはStudioをインストールすると、PowerShellモジュールとして自動的にインストールされます。これにより、スナップインを追加することなく、このSDKのコマンドレットを使用できます。（このSDKをスナップインとしてインストールすることを選択した場合の指示は以下に記載されています。）

権限

Citrix管理権限を持つIDを使用してシェルまたはスクリプトを実行する必要があります。Controller上のローカル管理者グループのメンバーは、Citrix Virtual AppsまたはCitrix Virtual Desktops™をインストールするための完全な管理権限を自動的に持っていますが、Citrixは、通常の操作では、ローカル管理者アカウントを使用するのではなく、適切な権限を持つCitrix管理者を作成することを推奨します。

コマンドレットにアクセスして実行する

1. PowerShellでシェルを起動します。Studioを開き、**PowerShell**タブを選択し、**Launch PowerShell**をクリックします。
2. スクリプト内でSDKコマンドレットを使用するには、PowerShellで実行ポリシーを設定します。PowerShellの実行ポリシーについては、Microsoftのドキュメントを参照してください。
3. (モジュールではなく) スナップインを使用する場合は、`Add-PSSnapin` (または`asnp`) コマンドレットを使用してスナップインを追加します。

   V1とV2はスナップインのバージョンを示します。XenDesktop 5のスナップインはバージョン1です。Citrix Virtual Apps and Desktops、およびそれ以前のXenDesktop 7バージョンのスナップインはバージョン2です。例えば、Citrix Virtual Apps and Desktopsスナップインをインストールするには、`Add-PSSnapin Citrix.ADIdentity.Admin.V2`と入力します。すべてのコマンドレットをインポートするには、次のように入力します: `Add-PSSnapin Citrix.*.Admin.V*`

これで、コマンドレットとヘルプファイルを使用できます。

- このSDKのヘルプファイルにアクセスするには、Categoriesリストで製品またはコンポーネントを選択し、次に**Citrix Virtual Apps and Desktops SDK**を選択します。
- PowerShellのガイダンスについては、Windows PowerShell Integrated Scripting Environment (ISE)を参照してください。

グループポリシーSDK

Citrix Group Policy SDKを使用すると、グループポリシーの設定とフィルターを表示および構成できます。このSDKは、PowerShellプロバイダーを使用して、マシンおよびユーザーの設定とフィルターに対応する仮想ドライブを作成します。このプロバイダーは、`New-PSDrive`の拡張機能として表示されます。

Group Policy SDKを使用するには、StudioまたはCitrix Virtual Apps and Desktops SDKのいずれかがインストールされている必要があります。

Citrix Group Policy PowerShell プロバイダーは、モジュールまたはスナップインとして利用できます。

- モジュールを使用する場合、追加の作業は不要です。
- スナップインを追加するには、`Add-PSSnapin citrix.common.grouppolicy` と入力します。

ヘルプにアクセスするには、`help New-PSDrive -path localgpo:/` と入力します。

仮想ドライブを作成し、設定をロードするには、`New-PSDrive <Standard Parameters> [-PSProvider] CitrixGroupPolicy -Controller <string>` と入力します。ここで、Controller 文字列は、接続して設定をロードしたいサイト内の Controller の完全修飾ドメイン名です。

モニターサービス OData

Monitor API を使用すると、OData API のバージョン 3 または 4 を使用して Monitor Service データにアクセスできます。Monitor Service データからクエリされたデータに基づいて、カスタマイズされた監視およびレポートダッシュボードを作成できます。OData V.4 は ASP.NET Web API に基づいており、集計クエリをサポートしています。

詳細については、Monitor Service OData API を参照してください。

__index__

サイト全体の履歴トレンドを監視する

トレンドビューは、以下のパラメータについて、各サイトの履歴トレンド情報にアクセスします。

- セッション
- 接続障害
- マシン障害
- ログオンパフォーマンス
- 負荷評価
- キャパシティ管理
- マシン使用状況
- リソース使用率
- 各サイトのネットワーク分析。

この情報を見つけるには、**トレンド**メニューをクリックします。

ズームイン ドリルダウン機能を使用すると、期間をズームイン（グラフのデータポイントをクリック）し、トレンドに関連する詳細を表示するためにドリルダウンすることで、トレンドグラフをナビゲートできます。この機能により、誰が、または何が影響を受けているかの詳細をよりよく理解できます。

各グラフのデフォルトのスコープを変更するには、データに別のフィルターを適用します。

履歴トレンド情報が必要な期間を選択してください。期間の利用可能性は、Directorの展開によって次のように異なります。

- Premiumライセンスサイトでは、最大1年間 (365日) のトレンドレポートを利用できます。
- Advancedライセンスサイトでは、最大1か月間 (31日) のトレンドレポートを利用できます。
- PremiumおよびAdvanced以外のライセンスサイトでは、最大7日間のトレンドレポートを利用できます。

> **注：**

- すべてのDirector展開において、期間が「先月」（**現在まで**）以下に設定されている場合、セッション、障害、ログオンパフォーマンスのトレンド情報はグラフとテーブルとして利用できます。期間がカスタム終了日を指定した「先月」または「昨年」として選択されている場合、トレンド情報はグラフとして利用でき、テーブルとしては利用できません。
- Monitor Serviceのグルーミング保持値によって、トレンドデータの可用性が制御されます。デフォルト値は、データ粒度と保持で確認できます。Premiumライセンスサイトのお客様は、グルーミング保持を希望する保持日数に変更できます。
- IIS Managerの以下のパラメータは、選択可能なカスタム終了日の範囲を制御します。ただし、選択された日付のデータ可用性は、測定される特定のメトリックのグルーミング保持設定によって異なります。

パラメーター	デフォルト値
UI.TrendsLast2HoursRange	3
UI.TrendsLast24HoursRange	32
UI.TrendsLast7DaysRange	32
UI.TrendsLastMonthRange	365

利用可能なトレンド

セッションの傾向を表示: 「**セッション**」タブから、デリバリーグループと期間を選択して、同時セッション数に関する詳細情報を表示します。

「**セッションの自動再接続**」列には、セッション内の自動再接続の数が表示されます。自動再接続は、セッションの信頼性ポリシーまたはクライアント自動再接続ポリシーが有効な場合に有効になります。エンドポイントでネットワークの中断が発生した場合、次のポリシーが有効になります。

- セッションの信頼性が有効になり（デフォルトで3分間）、Citrix Receiver™またはCitrix Workspace™アプリがVDAへの接続を試行します。
- クライアント自動再接続が3分から5分の間に有効になり、クライアントがVDAへの接続を試行します。

両方の再接続がキャプチャされ、ユーザーに表示されます。この情報は、再接続が発生してからDirector UIに表示されるまでに最大5分かかる場合があります。

自動再接続情報は、中断のあるネットワーク接続の表示とトラブルシューティングに役立ちます。また、シームレスなエクスペリエンスを持つネットワークも分析します。フィルターで選択した特定のデリバリーグループまたは期間の再接続数を表示できます。ドリルダウンでは、セッションの信頼性やクライアント自動再接続、タイムスタンプ、エンドポイントIP、Workspaceアプリがインストールされているマシンのエンドポイント名などの追加情報が提供されます。

デフォルトでは、ログはイベントのタイムスタンプの降順でソートされます。この機能は、Windows用Citrix Workspaceアプリ、Mac用Citrix Workspaceアプリ、Windows用Citrix Receiver、およびMac用Citrix Receiverで利用できます。この機能には、Delivery Controller™バージョン7 1906以降、およびVDA 1906以降が必要です。

セッションの再接続の詳細については、「セッション」を参照してください。

ポリシーの詳細については、「クライアント自動再接続ポリシー設定」および「セッションの信頼性ポリシー設定」を参照してください。

自動再接続データがDirectorに表示されない場合があります。その理由は次のとおりです。

- WorkspaceアプリがVDAに自動再接続データを送信していません。
- VDAがモニターサービスにデータを送信していません。
- Delivery Controllerは、対応するセッションがない可能性があるため、VDAペイロードを破棄します。

> **注：**
>
> 特定のCitrix Gatewayポリシーが設定されている場合、クライアントIPアドレスが正しく取得されないことがあります。

> **接続障害の傾向を表示:** 「障害」タブから、接続、マシンタイプ、障害タイプ、デリバリーグループ、および期間を選択して、サイト全体のユーザー接続障害に関する詳細情報を含むグラフを表示します。

マシン障害の傾向を表示: Single-session OS Machine FailuresタブまたはMulti-session OS Machinesタブから、障害タイプ、デリバリーグループ、および期間を選択すると、サイト全体のマシン障害に関する詳細情報を含むグラフが表示されます。

ログオンパフォーマンスの傾向を表示: ログオンパフォーマンスタブから、デリバリーグループと期間を選択して、サイト全体のユーザーログオン時間の詳細情報と、ログオン数がパフォーマンスに影響するかどうかを示すグラフを表示します。このビューには、ブローカー処理時間やVM起動時間など、ログオンフェーズの平均時間も表示されます。 このデータはユーザーログオン専用であり、切断されたセッションから再接続しようとするユーザーは含まれません。 グラフの下の表には、ユーザーセッションごとのログオン時間が表示されます。表示する列を選択し、任意の列でレポートを並べ替えることができます。 詳しくは、「ユーザーログオンの問題の診断」を参照してください。

負荷評価の傾向を表示: Load Evaluator Indexタブから、Multi-session OSマシン間で分散される負荷に関する詳細情報を含むグラフを表示します。このグラフのフィルターオプションには、デリバリーグループまたはデリバリーグループ内のMulti-session OSマシン、Multi-session OSマシン（デリバリーグループ内のMulti-session OSマシンが選択されている場合にのみ利用可能）、および範囲が含まれます。

ホストされたアプリケーションの使用状況を表示: この機能の利用可能性は、組織のライセンスによって異なります。 **Capacity Management**タブから、**Hosted Applications Usage**タブを選択します。デリバリーグループと期間を選択すると、ピーク時の同時使用状況を示すグラフと、アプリケーションベースの使用状況を示す表が表示されます。Application Based Usage表から、特定のアプリケーションを選択して詳細と、そのアプリケーションを使用している、または使用したユーザーのリストを確認できます。

Single-sessionおよびMulti-session OSの使用状況を表示: トレンドビューには、サイト別およびデリバリーグループ別のSingle-session OSの使用状況が表示されます。**サイト**を選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、ユーザーごとの使用状況が表示されます。 トレンドビューには、サイト別、デリバリーグループ別、およびマシン別のMulti-session OSの使用状況も表示されます。**サイト**を選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、マシンごとおよびユーザーごとの使用状況が表示されます。マシンが選択されている場合は、ユーザーごとの使用状況が表示されます。

仮想マシンの使用状況を表示: マシン使用状況タブから、**シングルセッションOSマシンまたはマルチセッションOSマシン**を選択すると、VMの使用状況をリアルタイムで確認でき、サイトのキャパシティニーズを迅速に評価できます。 シングルセッションOSの可用性 - サイト全体または特定のデリバリーグループにおけるシングルセッションOSマシン（VDI）の可用性による現在の状態を表示します。 マルチセッションOSの可用性 - サイト全体または特定のデリバリーグループにおけるマルチセッションOSマシンの可用性による現在の状態を表示します。

注： 利用可能なカウンターに表示されるマシンの数には、メンテナンスモードのマシンが含まれます。

リソース使用率の表示: リソース使用率タブから、**シングルセッションOSマシンまたはマルチセッションOSマシン**を選択すると、CPUおよびメモリ使用量、IOPS、各VDIマシンのディスク待機時間に関する履歴トレンドデータを確認でき、より適切なキャパシティプランニングに役立ちます。 この機能には、Delivery ControllerおよびVDAの**バージョン7.11**以降が必要です。 グラフには、平均CPU、平均メモリ、平均IOPS、ディスク待機時間、ピーク時の同時セッションのデータが表示されます。マシンにドリルダウンして、CPUを消費している上位10個のプロセスのデータとグラフを表示できます。

注：

この表に表示されるプロセスが多すぎると、大量のデータが消費され、パフォーマンスに影響する可能性があります。これを避けるため、平均CPUまたは平均メモリが1%を超えるプロセスのみが表示されます。そのため、表には10未満のプロセスしか表示されない場合があります。

デリバリーグループと期間でフィルターします。CPU、メモリ使用量、およびピーク時の同時セッションのグラフは、過去2時間、24時間、7日間、月、年で利用できます。平均IOPSおよびディスク待機時間のグラフは、過去24時間、月、年で利用できます。

注：

- 履歴マシン使用率ページの「上位10プロセス」テーブルでデータを収集して表示するには、監視ポリシー設定の**プロセス監視を有効にする**を**許可**に設定する必要があります。このポリシーは、デフォルトで**禁止**に設定されています。すべてのリソース使用率データはデフォルトで収集されます。これは、**リソース監視を有効にする**ポリシー設定を使用して無効にできます。グラフの下のテーブルには、マシンごとのリソース使用率データが表示されます。詳細については、「監視ポリシー設定」を参照してください。
- 平均IOPSは日次平均を示します。ピークIOPSは、選択した期間のIOPS平均の最高値として計算されます。（IOPS平均とは、VDAで1時間中に収集されたIOPSの時間平均です）。

> **ネットワーク分析データの表示:** この機能の可用性は、組織のライセンスと管理者権限によって異なります。この機能には、Delivery Controllerの**バージョン7.11**以降が必要です。

ネットワークタブから、ネットワーク分析を監視します。これにより、ネットワークのユーザー、アプリケーション、デスクトップのコンテキストビューが提供されます。この機能により、DirectorはCitrix ADMからのHDX Insightレポートを通じて、展開におけるICAトラフィックの高度な分析を提供します。詳細については、「ネットワーク分析の構成」を参照してください。

アプリケーション障害の表示: アプリケーション障害タブには、VDA上の公開アプリケーションに関連する障害が表示されます。

この機能には、Delivery ControllerおよびVDAの**バージョン7.15**以降が必要です。Windows Vista以降を実行するシングルセッションOS VDA、およびWindows Server 2008以降を実行するマルチセッションOS VDAがサポートされています。 詳細については、「履歴アプリケーション障害監視」を参照してください。

デフォルトでは、マルチセッションOS VDAからのアプリケーション障害のみが表示されます。監視ポリシーを使用して、アプリケーション障害の監視を設定できます。詳細については、「監視ポリシー設定」を参照してください。

アプリケーションプローブの結果を表示: アプリケーションプローブの結果タブには、構成ページでプローブ用に構成されたアプリケーションのプローブ結果が表示されます。ここでは、アプリケーション起動の失敗が発生した起動段階が記録されます。

この機能には、Delivery ControllerおよびVDAの**バージョン7.18**以降が必要です。詳しくは、「アプリケーションプローブ」を参照してください。

カスタマイズされたレポートの作成: カスタムレポートタブは、監視データベースからリアルタイムおよび履歴データを表形式で含むカスタムレポートを生成するためのユーザーインターフェイスを提供します。

この機能には、Delivery Controllers **バージョン7.12**以降が必要です。

以前に保存したカスタムレポートクエリのリストから、**実行してダウンロード**をクリックしてレポートをCSV形式でエクスポートしたり、**ODataをコピー**をクリックして対応するODataクエリをコピーして共有したり、**編集**をクリックしてクエリを編集したりできます。 マシン、接続、セッション、またはアプリケーションインスタンスに基づいてカスタムレポートクエリを作成できます。マシン、デリバリーグループ、期間などのフィールドに基づいてフィルター条件を指定します。カスタムレポートに必要な追加の列を指定します。プレビューには、レポートデータのサンプ

ルが表示されます。カスタムレポートクエリを保存すると、保存されたクエリのリストに追加されます。

コピーしたODataクエリに基づいてカスタムレポートクエリを作成できます。これを行うには、ODataクエリオプションを選択し、コピーしたODataクエリを貼り付けます。結果のクエリは後で実行するために保存できます。

注： ODataクエリを使用して生成されたプレビューおよびエクスポートレポートの列名はローカライズされておらず、英語で表示されます。

グラフ上のフラグアイコンは、特定の期間における重要なイベントまたはアクションを示します。フラグにマウスを合わせ、クリックしてイベントまたはアクションを一覧表示します。

注：

- HDX™接続ログオンデータは、7より前のVDAでは収集されません。それより前のVDAの場合、グラフデータは0と表示されます。
- Citrix Studioで削除されたデリバリーグループは、関連データが整理されるまで、Director Trendsフィルターで選択可能です。削除されたデリバリーグループを選択すると、保持期間までの利用可能なデータのグラフが表示されます。ただし、テーブルにはデータは表示されません。
- アクティブなセッションを含むマシンをあるデリバリーグループから別のデリバリーグループに移動すると、新しいデリバリーグループの**リソース使用率と負荷評価インデックス**テーブルに、古いデリバリーグループと新しいデリバリーグループから統合されたメトリックが表示されます。