Citrix DaaS

Contents

概要

March 31, 2024

はじめに

Citrix DaaS は、アプリおよびデスクトップの仮想化を提供するサービスであり、IT 担当者は仮想マシン、アプリケーション、セキュリティを完全に制御でき、あらゆるデバイスからのアクセスを提供できます。エンドユーザーは、デバイスで動作するオペレーティングシステムやインターフェイスに依存せずにアプリケーションやデスクトップを使用できます。

Citrix DaaS を使用すると、セキュリティで保護された仮想アプリとデスクトップを任意のデバイスに配信でき、インストール、セットアップ、アップグレードの大半は Citrix が実行します。どのデバイスに対しても最高のユーザーエクスペリエンスを提供しながら、アプリケーション、ポリシー、ユーザーを完全に制御できます。

Citrix DaaS を使用すると、オンプレミスのデータセンターとパブリッククラウドのワークロードをハイブリッド環境で一緒に管理できます。パブリッククラウドの Microsoft Azure、Amazon Web Services（AWS）、Google Cloud に加えて、XenServer、Microsoft Hyper-V、Nutanix AHV、VMware vSphere などのオンプレミスハイパーバイザーに接続できます。ハイブリッドのマルチクラウドアプローチにより、世界中のさまざまなリソースの場所にさまざまなアプリケーションを柔軟に展開することができます。

Citrix DaaS では、アプリとデスクトップを配信するための方法をいくつか提供します。

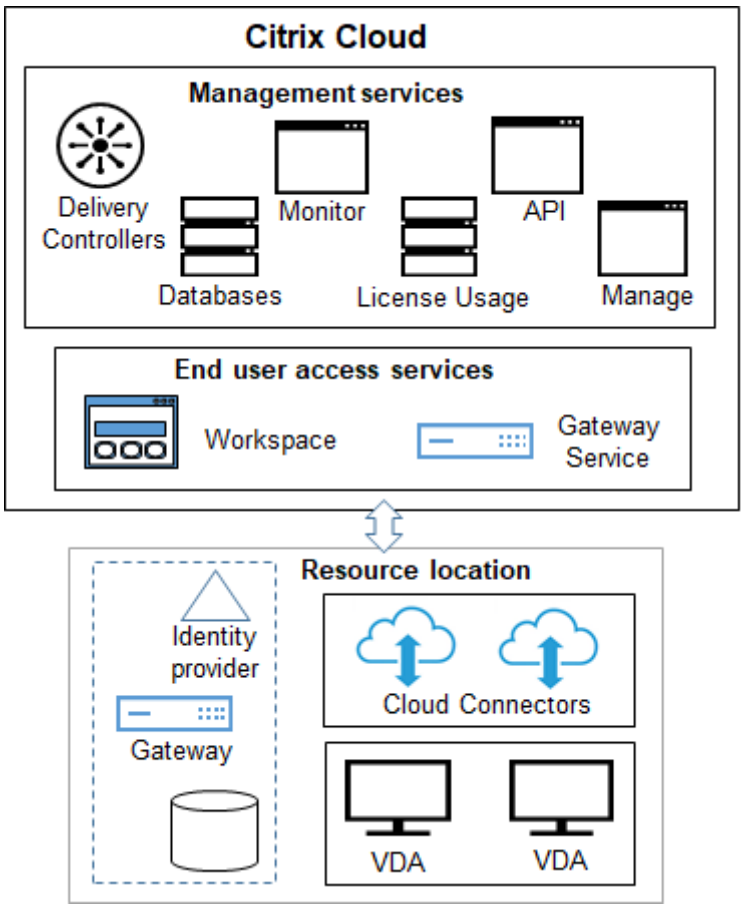
- 主な方法とそのユースケースおよびメリットとデメリットについては、「配信方法」を参照してください。
- その他の選択肢と VDI モデルの比較については、「配信モデル」を参照してください。

Citrix Managed Azureを使用すると、仮想アプリとデスクトップの展開が簡単になります。Citrix Managed Azure では、Citrix は Azure ワークロードのホスティングも管理します。

このサービスを使用するメリットについて詳しくはこちらを参照してください。

サイト概要

次の図は、Citrix 管理者が Citrix DaaS の実稼働環境（サイトとも呼ばれます）で使用するサービスとコンポーネントを示しています。



図に示すように、Ctrix は Citrix Cloud のユーザーアクセスと管理サービスおよびコンポーネントを管理します。ユーザーに配信するアプリケーションとデスクトップは、1 つ以上のリソースの場所にあるマシン上に配置されます。Citrix DaaS の展開では、リソースの場所にはアクセスレイヤーとリソースレイヤーのコンポーネントが含まれます。各リソースの場所は、1 つのゾーンと見なされます。

Citrix Virtual Apps and Desktops から最近移行した場合、Citrix DaaS により、オンプレミス環境に必要なコンポーネントのセットアップ作業のほとんどが不要になることがわかります。

Citrix が管理するコンポーネントとサービス

- **Delivery Controller**： Citrix DaaS は、アプリケーションやデスクトップの負荷分散機能、ユーザーの認証機能、接続をクラウドから直接ブローカーまたは優先順位付けする機能を提供します。Citrix Virtual Apps and Desktops とは異なり、Delivery Controller を管理する必要はありません。
- データベース：サイト構成、監視、および構成ログデータはクラウドサービスによって保存されるため、オンプレミスの Citrix Virtual Apps and Desktops 製品の SQL データベース要件が排除されます。
- ライセンス：ライセンスを管理し、使用状況の情報を提供します。
- 管理インターフェイス：「管理インターフェイス」を参照してください。多くのタスクは、サービス APIでも使用できます。

- 監視インターフェイス：監視インターフェイスを使用することで、IT サポート担当者やヘルプデスクのスタッフは環境の状態を監視し、重大な障害が生じる前にトラブルシューティングを講じたりエンドユーザーをサポートしたりできます。次の情報が表示されます：
  - Controller 上のブローカーサービスからのリアルタイムセッションデータ。これには、Virtual Deliver Agent（VDA）内のブローカーエージェントのデータも含まれます。
  - Controller 上の監視サービスからの履歴データ
  - HDX トラフィック（別名 ICA トラフィック）に関するデータ
- **Cloud Connector**： Cloud Connector は、Citrix Cloud 内のコンポーネントとリソースの場所内のコンポーネント間の通信チャネルです。リソースの場所では、Cloud Connector は Citrix Cloud の Delivery Controller のプロキシとして機能します。

  リソースの場所にはそれぞれ、少なくとも 1 つの Cloud Connector が含まれています。冗長性を確保するためには、2 つ以上の Cloud Connector を推奨します。

  - 完全な構成を使用してマシンをプロビジョニングする場合は、最初に Citrix Cloud コンソールから Cloud Connector をインストールします。詳細については、「Cloud Connector」を参照してください。
  - クイック展開を使用して Azure マシンをプロビジョニングする場合は、カタログを作成するときに Citrix がリソースの場所と Cloud Connector を作成します。

  Cloud Connector のインストール後は、Citrix が Cloud Connector の管理および更新を行います。顧客が処理するタスクは、Cloud Connector への Windows の更新とパッチの適用のみです。

管理インターフェイス

Citrix DaaS の ［管理］タブから、次のインターフェイスを選択できます。

完全な構成

［管理］**>**［完全な構成］インターフェイスから、次のことができます：

- ホームページから Citrix DaaS 展開の概要と最新機能を入手。
- ホストへの接続の作成と管理。
- ユーザーに配信するアプリとデスクトップが含まれるマシンのカタログの作成と管理。
- デリバリーグループ（および必要に応じてアプリケーショングループ）の作成と管理。
- HDX テクノロジと機能の使用と動作、さらにサイトレベルの管理に影響を与えるCitrix ポリシーの作成と管理。これには、セッション、アダプティブトランスポート、デバイス、グラフィックス、マルチメディア、コンテンツのリダイレクト、および VDA のポリシー設定が含まれます。

- 委任管理をカスタマイズして、特定の権限範囲を持つ役割ベースの管理者を作成。
- Autoscale機能を管理して、アプリやデスクトップを配信するマシンをプロアクティブに電源管理。
- マシンの負荷分散
- VDA に対してヘルスチェックを実行し、潜在的な問題を特定して提示された内容を修正。
- 構成ログの内容を表示して、構成の変更やその他の管理アクティビティがいつ発生したか、誰がそれらを開始したかを確認。

クイック展開

［管理］**>**［クイック展開］インターフェイスから、Citrix Managed Azure サブスクリプションまたは独自の Azure サブスクリプションのいずれかを使用する Microsoft Azure ワークロードを簡単に展開および管理できます。詳しくは、「クイック展開」および「Citrix Managed Azure」を参照してください。クイック展開から、次のことができます:

- カタログの作成と管理 。
- Citrix が準備したさまざまなイメージ、または Azure サブスクリプションからインポートしたイメージの、いずれかからのイメージの作成とカスタマイズ。

詳しくは、「クイック展開」を参照してください。

環境の管理

環境の管理インターフェイスから、インテリジェントなリソース管理および Profile Management テクノロジを使用して、最適なパフォーマンス、デスクトップログオン、およびアプリケーションの応答時間を実現できます。詳しくは、「Workspace Environment Management」を参照してください。

顧客が管理するコンポーネントとテクノロジ

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

  Citrix では、Citrix Cloud に Citrix Gateway サービスをインストールして管理します。リソースの場所に Citrix Gateway をインストールすることもできます。

- **Active Directory**: Active Directory は、認証と承認に使用されます。ユーザーを認証し、ユーザーが適切なリソースにアクセスできるようにします。利用者の ID は、利用者が Citrix Cloud でアクセスできるサービスを定義します。この ID は、リソースの場所内のドメインから指定された Active Directory ドメインアカウントによって提供されます。

- **ID** プロバイダー（**IdP**）： IdP は、ユーザーの ID の最終的な機関です。サポートされている IdP には次が含まれます：オンプレミスの Active Directory、Active Directory とトークン、Azure Active Directory、Citrix Gateway、Okta。詳しくは、次のトピックを参照してください：
  - ワークスペース ID
  - ID およびアクセス管理
- **Virtual Delivery Agent**（**VDA**）：リソース（アプリケーションとデスクトップ）を配信する各物理マシンまたは仮想マシンには、Citrix VDA をインストールする必要があります。VDA は、インストールされているマシンとユーザーデバイス間の接続を確立して管理するとともに、構成済みのポリシーをセッションに適用します。

  VDA は、リソースの場所にある Cloud Connector をプロキシとして使用して、Delivery Controller に登録されます。

  次のようないくつかの VDA タイプが利用可能です：
  - Windows マルチセッション OS 対応 VDA では、同時に複数のユーザーがそのマシンに接続できます。この VDA タイプは通常、Windows サーバーにインストールされます。
  - Windows シングルセッション OS 対応 VDA では、一度に 1 人のユーザーがマシンに接続できます。この VDA タイプは通常、VDI に使用されます。

    この VDA タイプのコアバージョンは、リモート PC アクセス機能で使用できます。これには、シングルセッション完全版 VDA の機能のサブセットが含まれています。
  - Linux VDA は、RHEL、CentOS、SUSE または Ubuntu ディストリビューションをベースとした仮想アプリおよびデスクトップをサポートしています。

  このサービスのドキュメントでは、「VDA」という用語は多くの場合、エージェントとそのエージェントがインストールされているマシンを指します。
- ハイパーバイザーとクラウドサービス：ほとんどの実稼働サイトでは、ユーザーが利用できるようにする（公開する）アプリとデスクトップインスタンス（ワークロード）は、サポートされているハイパーバイザーまたはクラウドサービスによって「ホスト」されます。（リモート PC アクセス機能は、通常、物理マシンで使用されます。したがって、マシンのプロビジョニングにハイパーバイザーやクラウドサービスは使用されません。）
  - 完全な構成インターフェイスを使用するときは、サポートされているホストハイパーバイザーまたはクラウドサービスへの接続を作成します。次に、完全な構成インターフェイスから、（そのホストを介して作成された）イメージを使用して、アプリとデスクトップのインスタンスを含むマシンのカタログを作成します。次に、デリバリーグループを作成します。Citrix は、これらのセッションホストの構築および保守方法を簡素化および促進するためのツールを多数提供しています。
  - クイック展開を使用して Azure ワークロードを配信する場合は、カタログを作成するだけで済みます。カタログの作成時に独自の Azure サブスクリプションを使用することもできますが、Citrix Managed Azureサブスクリプションを使用すると、ホストを管理する必要もなくなります。

  公開するアプリとデスクトップインスタンスは、オンプレミス、パブリッククラウドでホスト、または両方が合わさったハイブリッドでホストできます。

- **Citrix StoreFront**: Citrix StoreFrontは、クラウドでホストされる Citrix Workspace の以前の名称です。アプリケーションやデスクトップにアクセスするための Web インターフェイスとして使用されます。

  オプションで、StoreFront サーバーをリソースの場所にインストールできます。ストアをローカルに配置することで、ネットワーク停止中もアプリやデスクトップを提供できます。ローカルホストキャッシュ機能には各リソースの場所に顧客管理の StoreFront が必要です。

  サービス環境で StoreFront を使用する際の考慮事項については、「ユーザーアクセス」を参照してください。

デスクトップとアプリケーションを配信するために構成するオブジェクト

実稼働環境でアプリとデスクトップを配信するには、次の項目を構成します。

- ホスト接続：ホスト接続（前述）は、コントロールプレーン（Citrix Cloud）内のコンポーネントとリソースロケーション内の VDA の間で通信できるようにするのに役立ちます。接続の仕様は次のとおりです：

  - ホストにアクセスするためのアドレスと資格情報
  - 使用する保存方法と、保存用のマシン
  - 仮想マシンが使用できるネットワーク

  注意：クイック展開を使用する場合、接続を作成する必要はありません。また、Citrix Managed Azureを使用すると Citrix がホスティングも管理します。

- カタログ：完全な構成および監視のインターフェイスでは、カタログは「マシンカタログ」と呼ばれます。カタログとは、同じオペレーティングシステムタイプ（Windows マルチセッション、Ubuntu シングルセッションなど）を持つ仮想マシンまたは物理マシンのコレクションです。

  When creating a catalog, you usually use an image, which is also known as a template. (Remote PC Access catalogs usually contain physical machines, so no image is needed.)

  - When using Quick Deploy, Citrix provides several Citrix prepared images you can use to create your own customized images. Or, you can import images from your own Azure subscription.
  - When using Full Configuration to create VMs using a supported host type, the image usually must be created and reside on a host machine. When creating the catalog, you provide the path to that image.

  Regardless of where the image resides, you can install applications on the image, if you want those apps on all machines created from that image (and don’t want to virtualize those apps).

  After the image is ready, you create the catalog.

  - For VMs, MCS creates the machines and the catalog.
  - For Remote PC Access, MCS simply creates the catalog, because the physical machines already exist.

For more information about MCS, see Image management.

- デリバリーグループ：デリバリーグループは以下を指定します：
  - カタログの 1 つ以上のマシン
  - これらのマシンにアクセスできるユーザー。
  - ユーザーが Workspace を介してアクセスできるアプリケーションとデスクトップ。

  クイック展開を使用すると、デリバリーグループが自動的に作成されます。（これは、完全な構成インターフェイスにのみ表示されます。）
- アプリケーショングループ：アプリケーショングループを使用すると、アプリケーションのコレクションを管理できます。異なるデリバリーグループ間で共有されているアプリケーションや、デリバリーグループ内のユーザーのサブセットによって使用されるアプリケーションのアプリケーショングループを作成できます。アプリケーショングループはオプションです。

Citrix Managed Azure

Citrix Managed Azure は、いくつかの Citrix DaaS エディションで利用できるオプションです。Citrix Managed Azure を使用すると、Azure からの仮想アプリとデスクトップの展開が簡単になります。Azure ワークロードをホストするためのインフラストラクチャは Citrix が管理します。

Citrix Managed Azure を使用すると、citrix が管理する専用の Azure サブスクリプションとリソースの場所を取得できます。その Azure サブスクリプションでは、仮想マシンのカタログを作成します。次の操作を実行できます：

- サポートされているさまざまなバージョンからの、シングルセッションおよびマルチセッションの Windows OS マシンまたは Linux OS マシンの展開。
- 選択したリージョンのコンピューティングタイプとストレージオプションの厳選されたリストからの選択。
- それらのマシンでの永続的または非永続的なワークロードをプロビジョニング。
- 最新の VDA がインストールされているいくつかの Citrix 提供イメージからの選択。選択したら、Citrix インターフェイスで、そのテンプレートから独自のイメージを作成し、カスタマイズします。独自の Azure サブスクリプションからイメージをインポートして使用することもできます。

Citrix が Azure の容量を管理している場合でも、独自の Azure サブスクリプションで既存のリソースと通信する場合は、Azure VNET ピアリングを使用してリソースを接続できます。また、Citrix SD-WAN を使用して、オンプレミスリソースに直接接続することもできます。

Citrix Managed Azure を使用する場合のセキュリティと責任範囲については、「Citrix Managed Azure のセキュリティの技術概要」を参照してください。

Citrix Managed Azure の購入

Citrix Managed Azure サブスクリプションを取得するには、サポートされている Citrix のサービスオファリングにサブスクライブしてから、Citrix Managed Azure Consumption Fund を購入する必要があります。Citrix DaaS

と Consumption Fund は、Citrix または Azure Marketplace から注文できます。
Citrix Managed Azure は、次のサービスでサポートされています:

- Citrix Workspace Premium Plus
- Citrix DaaS、Advanced、Advanced Plus、および Premium エディション
- Citrix DaaS Standard for Azure エディション

詳細については、「Citrix DaaS への登録」を参照してください。

Citrix Managed Azure のメリットの概要

Citrix Managed Azure を使用すると、次のような利点があります:

- ハイブリッドクラウドのメリットを受ける最速の方法。
- インフラストラクチャの IT 管理の負荷を軽減。管理やメンテナンスの課題を抱えることなく、IT をコントロールできる管理体験を提供します。
- 作業ソリューションを迅速に拡張可能。
- Citrix が管理および保守する個別の Azure サブスクリプションを提供。これにより、アクティビティが他の Azure サブスクリプションから分離されます。
- 独自の Azure サブスクリプションを使用してワークロードを作成および管理する柔軟性を保持。環境には、Citrix Managed Azure サブスクリプションを使用するワークロードと、独自の（顧客管理の）Azure サブスクリプションを使用するワークロードを含めることができます。
- 真の消費ベースの Infrastructure as a Service（IaaS）モデルを使用。
- 独自のオンプレミスネットワーク（Azure VNET ピアリングや SD-WAN など）への接続を作成するために、いくつかのテクノロジを利用可能。これにより、ユーザーはファイルサーバーなどのネットワークのリソースにアクセスできます。

このサービスから Citrix Managed Azure を展開および管理するには、クイック展開管理インターフェイスを使用します。

詳しくは、Citrix の担当者にお問い合わせください。

アプリケーションとデスクトップをユーザーに配信する

Citrix Workspace

利用者（ユーザー）は、Citrix Workspace を介してデスクトップとアプリにアクセスします。

Citrix DaaS をインストールして構成すると、ワークスペースの URL リンクが表示されます。ワークスペースの URL は、次の 2 か所で確認できます:

- Citrix Cloud コンソールで、左上隅のメニューから ［ワークスペースの構成］を選択します。［アクセス］タブに、ワークスペース URL が表示されます。

- Citrix DaaS の ［ようこそ］ページでは、ページの下部にワークスペース URL が表示されます。

利用者（ユーザー）がアプリとデスクトップにアクセスできるように、ワークスペースの URL リンクをテストしてから利用者と共有します。利用者は、特に構成する必要なくワークスペース URL にアクセスできます。

Citrix Cloud から、ワークスペースを構成します。

- Citrix Workspace と統合されるサービスを指定します。
- 利用者が自分のワークスペースにアクセスするために使用する URL をカスタマイズします。
- ロゴ、色、および環境設定など、利用者のワークスペースの外観をカスタマイズします。
- Active Directory または Azure Active Directory の使用など、利用者がワークスペースに対してどのように認証するかを指定します。
- 利用者が使用するリソースの場所の外部接続を指定します。

詳しくは、「Citrix Workspace」を参照してください。

Citrix Workspace アプリ

Citrix Workspace アプリはユーザー側から、ユーザーデバイスや他のエンドポイント（仮想デスクトップ）にインストールします。Citrix Workspace アプリを使用すると、スマートフォン、タブレット、コンピューターなどのデバイスから、ドキュメント、アプリケーション、デスクトップへの安全にセルフサービス形式でアクセスできます。また、Citrix Workspace アプリにより、Windows、Web、および SaaS（Software as a Service）アプリケーションへのオンデマンドアクセスも可能になります。

Citrix Workspace アプリソフトウェアをインストールできないデバイスでは、HTML5 互換の Web ブラウザーから HTML5 向け Citrix Workspace アプリを使用してアクセスすることもできます。

Citrix Workspace アプリは、さまざまなオペレーティングシステム向けに提供されています。詳しくは、「Citrix Workspace アプリ」を参照してください。

サービスレベルアグリーメント

Citrix DaaS は、業界のベストプラクティスを使用して、クラウドの規模と高度なサービス可用性を実現するように設計されています。

Citrix Cloud サービスの可用性に関する Citrix の目標について詳しくは、「サービスレベルアグリーメント」を参照してください。

この目標に対する実際のパフォーマンスは、https://status.cloud.comでいつでも確認できます。

制限事項

このサービスレベル目標の計算には、以下を原因とする可用性の損失は含まれません。

- 顧客がhttps://docs.citrix.comの製品ドキュメントに記載されている Citrix DaaS の構成要件に従っていない。
- Citrix が管理していないコンポーネント（次を含むがこれに限定されない）が原因である：顧客が管理している物理および仮想マシン、顧客がインストールし保守しているオペレーティングシステム、顧客がインストールし管理しているネットワーク機器またはその他のハードウェア、顧客が定義し管理しているセキュリティ設定、グループポリシーおよびその他の構成ポリシー。パブリッククラウドプロバイダーの障害、インターネットサービスプロバイダーまたは Citrix が管理していない外部組織の障害。
- 自然災害、戦争、テロ行為、政府の方針など、Citrix の制御を超えた理由によるサービスの中断。

追加情報

- Citrix DaaS の図
- Citrix DaaS のリファレンスアーキテクチャと展開方法
- セキュリティの技術概要
- ネットワークポート
- サードパーティ製品についての通知
- システム要件
- 機能
  - ここでは、HDX テクノロジの概要と、デバイス、グラフィック、マルチメディアに関する詳細を紹介します。
  - リモート PC アクセス：ユーザーが社内にある自分の物理的な PC にどこからでもリモートアクセスできるようになります。リモート PC アクセスの構成は、完全な構成またはクイック展開から行えます。
  - コンテンツの公開：リソースへの URL または UNC パスとしてアプリケーションを公開します。
  - サーバー VDI：単一ユーザー用のサーバーオペレーティングシステムからデスクトップを配信します。
- Citrix DaaS Standard for Azure については、この製品ドキュメントを参照してください。
- Citrix DaaS 製品およびエディションで利用可能な機能については、Citrix DaaS の機能マトリックスを参照してください。
- Citrix Cloud Learning シリーズは、Citrix Cloud とそのサービスを導入して実行するための教育コースを提供しています。概要から、計画と構築のサービスまで、すべてのモジュールを順番に確認できます。個々のモジュール、またはモジュール内の特定タスクのセグメントを選択することもできます。Cloud Learning Seriesを参照してください。

開始

展開のセットアップ方法については、まず「展開の計画と構築」を参照してください。この記事には、プロセスの主な手順や、詳細な情報と手順へのリンクがまとめられています。

新機能

June 13, 2024

Citrix は、Citrix DaaS をご使用のお客様に、新機能と製品の更新をいち早くお届けするよう取り組んでいます。新しいリリースでは、より便利な機能をご利用いただけます。今すぐ更新してください。Citrix DaaS のリリースのローリング更新は、約 3 週間間隔で提供されます。

このプロセスは、わかりやすいものになっています。最初の更新は、Citrix 内部サイトのみに適用され、その後徐々に顧客環境に適用されます。段階的に更新することによって、製品の品質を確保しながら、最大限の可用性を実現しています。

クラウドの規模とサービスの可用性に関するサービスレベルアグリーメントについて詳しくは、「サービスレベルアグリーメント」を参照してください。サービスの中断および定期メンテナンスを監視するには、Service Health Dashboardを参照してください。

Virtual Delivery Agent（VDA）

Windows マシン用の VDA は、一般に、Citrix Virtual Apps and Desktops 製品と同時にリリースされます。

- VDA および HDX の新機能については、最新の Citrix Virtual Apps and Desktops リリースの「新機能」および「既知の問題」を参照してください。
- サポートが廃止された VDA プラットフォームおよび機能については、「廃止」を参照してください。この記事では、将来のリリースでサポートが終了する予定のプラットフォームや機能（VDA のインストールをサポートするオペレーティングシステムなど）についても説明しています。

> 重要:
>
> Personal vDisk（PvD）コンポーネントを VDA にインストールしたことがある場合、その VDA をバージョン 1912 LTSR 以降にアップグレードすることはできません。新しい VDA を使用するには、現在の VDA をアンインストールしてから新しくインストールする必要があります（この手順は、Personal vDisk をインストール済みで使用したことがない場合でも適用されます）。詳しくは「VDA に Personal vDisk がインストールされている場合」を参照してください。

2024 年 6 月

新機能と機能強化

Azure カタログ作成中のリソースグループの作成をサポート（**PVS** 用）。以前は、完全な構成を使用して Azure カタログを作成する場合、PowerShell コマンドを使用してリソースグループを作成する必要がありました。この機能を使用することで、Web Studio でのカタログ作成の一環として、リソースグループをシームレスに作成できるように

なりました。この機能強化により、全体的な作成ワークフローがシンプルになります。詳しくは、「完全な構成インターフェイスを使用して Citrix Provisioning マシンカタログを作成する」を参照してください。

2024 年 5 月

新機能と機能強化

Secure HDX（**Technical Preview**）。この機能を使用すると、トラフィックパス内のネットワーク要素が HDX トラフィックを検査できないようにすることができるようになりました。詳しくは、「Secure SDK」を参照してください。

Azure GPU の休止状態のサポート（**Technical Preview**）。GPU を利用可能な Azure マシン SKU の休止状態をサポートするオプションが追加されました。
サポートされる仮想マシンのサイズについて詳しくは、Microsoftのドキュメントを参照してください。

Citrix Provisioning カタログの **Hybrid Azure AD Join** に対するサポートが完全な構成に拡張されました。Citrix Provisioning カタログを作成するとき、［マシンカタログのセットアップ］**>**［マシン **ID**］ページで ID の種類 ［ハイブリッド **Azure Active Directory** 参加］が使用できるようになりました。この新しいオプションを使用すると、Citrix Provisioning を通じて Hybrid Azure AD 参加マシンを作成できます。詳しくは、この Citrix Provisioning の記事を参照してください。

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

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

強化された構成ログ：デリバリーグループのメンバーシップの変更を追跡します。この機能強化により、構成ログはデリバリーグループに追加された、またはデリバリーグループから削除されたユーザー ID とグループ ID をキャプチャして表示するようになりました。構成ログを表示するには、［完全な構成］**>**［ログ］**>**［イベント］に移動します。

検索ノードのタブの順序をカスタマイズします。使用パターンに応じて検索ノードのタブの順序をカスタマイズできるようになり、閲覧エクスペリエンスが向上します。これを行うには、タブの横にある 3 つのドットのアイコンをクリックし、タブを希望の順序にドラッグして、［適用］をクリックします。

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

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

この機能の導入には、次のような利点があります:

- MCS と Citrix Provisioning カタログの両方を管理できる単一の統合 API。
- ID 管理ソリューション、オンデマンドプロビジョニングなどの Citrix Provisioning カタログの新機能を利用可能。

詳しくは、「Citrix Studio での Citrix Provisioning カタログの作成」を参照してください。

VDA アップグレードプロセス中の **VDA** アップグレードサービスにおけるエラーの検出と軽減（**Technical Preview**）。当社のサービスには現在、高度な検出メカニズムが組み込まれています。VDA IPU でエラーが発生し、VDA が使用できなくなる可能性がある問題が検出された場合は、このサービスによってプロアクティブな対策が講じられます。追加のマシンの更新が停止され、現在のワークフローが正常に終了します。このプロアクティブなアプローチは、予期しない問題が発生した場合でも影響を最小限に抑え、スムーズなエクスペリエンスを確保し、発生した問題の潜在的な影響範囲を抑えることを目的としています。詳しくは、「VDA アップグレードプロセス中の VDA アップグレードサービスにおけるエラーの検出と軽減（Technical Preview）」を参照してください

VDA がアクセスできるローカルファイル共有からの **VDA** の更新をサポート（**Technical Preview**）。強化された VDA インストーラーアクセス制御により、Citrix Managed Azure CDN から更新を取得するためのネットワークアクセスを VDA に付与するかどうかを気にすることなく、どの VDA を接続して必要なダウンロード MSI を取得できるかをより柔軟に制御できるようになりました。これにより、より厳格なネットワーク規則を適用しながら、重要な更新へのシームレスなアクセスを確保できます。詳しくは、「VDA がアクセスできるローカルファイル共有からの VDA の更新をサポート」を参照してください

パッケージアプリケーションのシングルセッションの静的デスクトップおよびオフィス **PC** への配信で完全な構成をサポート。この機能強化により、完全な構成を使用して、パッケージアプリケーションをあらゆる種類のデスクトップに配信できるようになりました。パッケージアプリケーションをシングルセッションの静的デスクトップに配信するメリットは次のとおりです:

- アプリケーションはサインイン時に VDA で利用可能ですが、Workspace または StoreFront 経由でオンデマンドでステージングされることはありません。
- パッケージアプリケーションにアクセスするときの起動時間が短縮されました。
- VDA の基本イメージから分離され、パッケージアプリケーションの個別のメンテナンスを容易にします。

パッケージアプリケーションをデスクトップに配信するには、次の方法でそれらのアプリケーションをデリバリーグループに追加します:

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

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

パッケージアプリケーションの **FlexApp** 形式での配信で完全な構成をサポート。［完全な構成］**>**［アプリパッケージ］で、FlexApp アプリを Citrix Cloud にアップロードし、ユーザーに配信できるようになりました。詳しくは、「アプリパッケージ」を参照してください。

OData Pagination。Monitor は OData Pagination の制限を強化します。すべての OData v4 エンドポイントは、応答で 1 ページあたり最大 1000 レコードと次の 1000 レコードへのリンクを返します。すべてのページで大きなデータセットが返されるため、より少ない OData クエリで同じ量の合計データを取得できます。したがって、この機能により、合計データを取得する時間が短縮され、ユーザーエクスペリエンスが向上します。詳しくは、「Accessing Monitor Service data using the OData v4 endpoint in Citrix Cloud」ドキュメントを参照してください。

［完全な構成］を使用した **Azure Confidential VM** の作成と管理をサポート。Azure Confidential VM は、セキュリティニーズを満たすために役立つ、ハードウェアによる強力な境界を提供します。完全な構成ユーザーインターフェイスを使用して、Azure 上で Confidential VM を作成および管理できるようになりました。詳しくは、「Azure Confidential VM（Technical Preview）」を参照してください。

構成ログでクライアント **IP** の表示をサポート。［完全な構成］**>**［ログ］**>**［イベント］では、ログ内の IP アドレスの詳細を表示できるようになり、アクションの発生元の追跡が容易になりました。メインビューに IP アドレス列を表示するには、ログの右上にある 表示する列アイコンをクリックし、クライアント **IP** を選択します。詳しくは、「構成ログの内容の表示」を参照してください。

AWS のマシンプロファイルソースを使用した追加のプロパティのキャプチャをサポート。AWS 環境では、この機能強化により、次の内容を含むマシンプロファイルベースのカタログを作成または更新できるようになりました：

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

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

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

AWS でアクティブなコンピューターアカウントの **ID** 情報を修復。AWS 環境で、ID 関連の問題があるアクティブなコンピューターアカウントの ID 情報をリセットできるようになりました。マシンのパスワードと信頼キーのみをリセットするか、ID ディスクのすべての構成をリセットするかを選択できます。この実装は、永続および非永続の両方の MCS マシンカタログに適用できます。現在、この機能は AWS、Azure、VMware 仮想化環境でのみサポートされています。詳しくは、「アクティブなコンピューターアカウントの ID 情報を修復する」を参照してください。

AWS で **MCS** マシンカタログ **VM** の **ID** ディスクの暗号化をサポート。以前は、AWS 環境では、プロビジョニングされた VM の OS ディスクのみの暗号化が MCS で許可されていました。この機能を使用すると、OS ディスクに加え

て ID ディスクも暗号化できるようになりました。この機能により、AWS KMS キー（顧客管理キーと AWS 管理キー）を使用して、VM に接続されたディスクに対して暗号化操作を実行できるようになります。

OS ディスクと ID ディスクの暗号化では、次のいずれかを構成します：

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

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

AWS でネットワークインターフェイスごとにセキュリティグループを構成。AWS 環境のホスト接続を編集するときに、PowerShell コマンドを使用して、Elastic Network Interface（ENI）ごとに許可されるセキュリティグループの最大数を構成できるようになりました。したがって、ネットワークインターフェイスのクォータあたりのセキュリティグループを増やすと、ホスト接続にも同じ値を構成できます。構成について詳しくは、「ネットワークインターフェイスごとにセキュリティ グループを構成」を参照してください。

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

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

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

［見積もり削減額］は、インフラストラクチャリソースの効率的な利用を評価するのに役立ちます。コスト削減額は、米ドルまたは発生したコストの割合で表示されます。過去 3 か月、6 か月、および 12 か月の結果を表示できます。［見積もり削減額］グラフには次の内容が表示されます：

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

［**Autoscale** 削減額レポート］には、Autoscale が構成され有効になっているデリバリーグループに関する情報が表示されます。このレポートは、電源管理されたマシンにのみ適用されます。詳しくは、「コスト最適化」ページを参照してください。

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

- ユーザーの問題を引き起こす電源オンの失敗

- コストを増加させる電源オフの失敗

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

次の方法を使用して、マシンの電源操作状態を表示できます:

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

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

詳しくは、「最近電源操作を行ったマシンを検査する」を参照してください。

2024 年 4 月

新機能と機能強化

Microsoft Teams の新しいバージョンをサポート。Citrix Monitor は、Microsoft Teams バージョン 2.1 以前をサポートするようになりました。

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

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

詳しくは、「ディスク暗号化を変更する」を参照してください。

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

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

VMware で複数の **NIC** を確認。VMware 環境では、ホスティングユニットとマシンプロファイルテンプレートに複数のネットワークがあり、`New-ProvScheme`および`Set-ProvScheme`コマンドで`-NetworkMapping`パラメーターが使用されている場合の、さまざまな事前チェックが導入されました。複数の NIC の事前チェックリストについて詳しくは、「複数の NIC を確認する」を参照してください。

GCP での **Windows 11 VM** 作成をサポート。GCP で Windows 11 VM を作成できるようになりました。マスターイメージに Windows 11 をインストールする場合は、マスターイメージの作成プロセス中に vTPM を有効にする必要があります。また、マシンプロファイルソース（VM またはインスタンステンプレート）で vTPM を有効にする必要があります。

この機能は以下に適用されます:

- 永続的および非永続的 MCS マシンカタログ。
- 単一テナントノードグループのみ。

単一テナントノードで Windows 11 VM を作成する方法については、「単一テナントノードに Windows 11 VM を作成する」を参照してください。

環境変数に対する仮想チャネル許可リストのサポート。
信頼できるプロセスのパスでシステム環境変数を使用できるようになりました。詳しくは、「システム環境変数の使用」を参照してください。

[完全な構成] で廃止された機能。完全な構成では次の機能と設定が廃止されました:

HDX Plus for Windows 365 クラウド **PC** および **Azure Virtual Desktop** のサポート。Monitor は、HDX Plus for Windows 365クラウド PC および Azure Virtual Desktop（AVD）をサポートするようになりました。詳しくは、「マシンのトラブルシューティング」を参照してください。

Cloud Build サービスアカウントの変更。GCP は、2024 年 4 月 29 日以降に作成された新しいプロジェクトにおいて、Cloud Build サービスのデフォルトの動作とサービスアカウントの使用に関する変更を導入します。詳しくは、「Cloud Build サービスアカウントの変更」を参照してください。ただし、既存の Google プロジェクトと Citrix カタログは、この変更の影響を受けません。詳しくは、次のトピックを参照してください:

- サービスアカウントの構成と更新
- 必要な GCP の権限

HDX Plus for Windows 365 クラウド **PC** および **Azure Virtual Desktop** のサポート。Monitor は、HDX Plus for Windows 365クラウド PC および Azure Virtual Desktop（AVD）をサポートするようになりました。詳しくは、「マシンのトラブルシューティング」を参照してください。

インターネットおよび **URL** フィルタリング用のプロキシを使用した **VDA** 環境（**Technical Preview**）。インターネット接続と Web フィルタリング用のプロキシがある場合、VDA アップグレードサービスを使用して VDA を更新できるようになりました。ポリシーで構成されたプロキシは、レジストリで構成されたプロキシよりも優先されます。

詳しくは、「Install Capture」を参照してください。また、プロキシで許可リストに登録する必要があるURL の一覧も参照してください。

Cloud Build サービスアカウントの変更。GCP は、2024 年 4 月 29 日以降に作成された新しいプロジェクトにおいて、Cloud Build サービスのデフォルトの動作とサービスアカウントの使用に関する変更を導入します。詳しくは、「Cloud Build サービスアカウントの変更」を参照してください。ただし、既存の Google プロジェクトと Citrix カタログは、この変更の影響を受けません。詳しくは、次のトピックを参照してください:

- サービスアカウントの構成と更新
- 必要な GCP の権限

2024 年 3 月

新機能と機能強化

動的なセッション録画。[ユーザーの詳細] 画面から、Session Recording 制御を使って、現在アクティブなセッションを録画することができるようになりました。セッションを再度確立する必要はありません。この機能によって、ユーザーが直面するセッションエクスペリエンス関連の問題のトラブルシューティングをより迅速かつ効果的に行うことができます。これは、再現が難しい問題をデバッグするのに役立ちます。

動的なセッション録画について詳しくは、「Session Recording サービス」の記事を参照してください。

WebSocket を使用して **VDA** をマシンカタログに登録する登録ツール。この登録ツールを使用して、ドメインに参加していない VDA をマシンカタログに安全に登録できるようになりました。この機能により、VDA から Delivery Controller への通信に TLS ポート 443 のみを使用し、ポート 80 のトラフィックを削除するという利点が得られます。詳しくは、「WebSocket VDA 登録ツールを使用してマシンをカタログに登録する」を参照してください。

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

完全な構成：マシンプロファイルを使用して、より多くの **Azure VM** 設定の更新をサポート。完全な構成では、マシンプロファイルを通じて、MCS でプロビジョニングされた Azure のより広範囲の設定を更新できるようになりました。これには以下が含まれます:

- マシンサイズ
- ライセンスの種類
- アベイラビリティゾーン
- 専用ホストグループ ID

マシンプロファイルを更新すると、完全な構成は現在の設定と新しい設定を比較します。差異が存在する場合は、どちらを適用するかを確認するプロンプトが表示されます。この設計により、VM 設定を透過的かつ効率的に更新できます。

完全な構成：**MCS** によってプロビジョニングされた **Azure VM** の、ライトバックキャッシュプロパティの変更をサポート。Machine Creation Services（MCS）を使用してプロビジョニングされた Azure VM の場合、完全な構成を使用してライトバックキャッシュ（WBC）のプロパティ（ディスクキャッシュサイズ、メモリキャッシュサイズ、ストレージコストの削減を有効にする）を変更できるようになりました。さらに、これらの VM の新しいマシンサイズまたはマシンプロファイルを選択すると、完全な構成によって WBC 設定が検証され、新しい選択がメモリ制限を超えているなどの競合を回避できます。競合が発生した場合は、WBC 設定を再構成するように求められます。

2024 年 **2** 月

新機能と機能強化

Workspace のインターフェイスから **VM** を一時停止。Workspace のユーザーインターフェイスから、アクティブなセッションがある永続的な VM を一時停止できるようになりました。この機能強化には、次のメリットがあります：

- 中断したところからシステムを再開できます。
- 停止して割り当てが解除されたマシンと比較して、起動時間が短縮されます。
- コスト効率とエネルギー効率に優れています。
- Autoscale 機能を使用して効率的にリソースを割り当てます。

新しいマシン作成サービス（**MCS**）のストレージ最適化（**MCSIO**）のサポート：MCS プロビジョニング用のイメージを準備するときに、Image Portability Service で MCSIO を追加または削除するオプションが追加されました。詳しくは、「VDA 構成を自動化する」を参照してください。

プローブの概要の強化：プローブメトリックとプローブエラー段階の概要が、［プローブ］>［概要］で利用できるようになりました。プローブメトリックには、スケジュールされた実行、失敗した実行、スキップされた実行、成功した実行の数が表示されます。エラー段階のグラフィック表示は、最も多くのエラーが発生した段階を分析するのに役立ちます。この情報は、プローブ結果のトラブルシューティングを迅速に行うのに役立ちます。詳しくは、「アプリケーションプロービングおよびデスクトッププロービング」の記事を参照してください。

マシンカタログページのイメージ情報。マシンカタログの ［テンプレートのプロパティ］を通じて、次のイメージ情報を表示できるようになりました：

- オペレーティングシステム
- Machine Identity Service
- Machine Creation Services ストレージ
- Azure 展開の`pagefile.sys`のファイルパス

この機能強化により、イメージ情報がより明確になり、管理者はマシンカタログに関するすべての情報を 1 か所で確認できるようになります。

完全な構成による **VDA** 登録トークン管理のサポート。トークンベースの VDA 登録により、Cloud Connector の負荷が軽減され、潜在的な障害ポイントが減少します。これは、Citrix Provisioning 以外のテクノロジを使用してマ

シンを準備するユースケースに最適です。完全な構成を使用すると、Citrix がプロビジョニングしていない VDA の登録トークンを生成および管理できるようになり、登録トークンベースの導入を効率化できます。詳しくは、「登録トークンの生成と管理」を参照してください。

PowerShell のログ。完全な構成では、日常的な UI 操作に対応する PowerShell コマンドを表示できるようになりました。この機能は、基礎となる PowerShell コマンドについて学習するための、詳細な情報を得るのに役立ちます。PowerShell ログを表示するには、[ログ] > [**PowerShell**] に移動してください。詳しくは、「構成ログ」を参照してください。

完全な構成を使用し、プールされたシングルセッション **VDA** に対してローカルホストキャッシュ（**LHC**）を有効にします。デフォルトでは、MCS または Citrix Provisioning を使用してプロビジョニングされた、シングルセッションのプールされた VDA は、LHC モードでは使用できません。完全な構成では、デリバリーグループごとにこのデフォルトの動作を上書きできるようになり、LHC 中の新しい接続でそれらの VDA を利用できるようになります。詳しくは、「デリバリーグループの作成」と「デリバリーグループの管理」を参照してください。

完全な構成で **Citrix Hypervisor** を **XenServer** に名称変更。リブランディング戦略によって、完全な構成内の Citrix Hypervisor のすべてのインスタンスを XenServer に更新しました。

エンドツーエンドのネットワークホップビュー。エンドツーエンドのネットワークホップビューは、Citrix Monitor でトラブルシューティングワークフローを強化するための次のステップです。[ユーザーの詳細] > [セッションパフォーマンス] > [セッションのトポロジ] セクションでは、接続された HDX セッションのエンドツーエンドのネットワークホップビューを視覚的に表現します。セッション内パスは、セッションパスに含まれるコンポーネントとそのメタデータ、コンポーネント間のリンク、および VDA で公開されたアプリケーションを理解するのに役立ちます。セッションのトポロジによって、セッションデータのフローでコンポーネントを理解し、パフォーマンスの問題を引き起こしている可能性のある特定のホップを識別できます。

さらに、接続状態にあるセッションの ICA 遅延および ICA 往復時間測定値が表示されます。詳しくは、「エンドツーエンドのネットワークホップビュー」を参照してください。

マスターイメージのディスク暗号化セット **ID**（**DES ID**）を使用して、カタログ **VM** のすべてのディスクを暗号化する。Azure 環境では以前は、MCS マシンカタログのディスク暗号化セット ID（DES ID）がマシンプロファイルまたはカスタムプロパティから導出されていました。この機能を使用すると、マシンカタログでマスターイメージから DES ID を取得し、カタログ内の VM のすべてのディスクを暗号化することもできます。

移行後に孤立したリソースを検出するために **MCS** タグを更新する。オンプレミス構成からクラウドサイトに移行した後、またはクラウド構成から別のクラウドサイトに移行した後、以前のサイト ID タグを使用していることによって、孤立したリソースが正しく検出されません。この機能を使用すると、孤立したリソースを正しく検出できるように、移行後に PowerShell コマンドを使用して永続カタログの MCS サイト ID タグを更新できます。現在、この機能は Azure に適用されます。詳しくは、「移行後に孤立したリソースを検出するために MCS タグを更新する」を参照してください。

MCS マシンカタログを作成する前に構成を検証する。この機能により、`New-ProvScheme`コマンドのパラメーター`-validate`を使用して、MCS マシンカタログを作成する前に構成設定を検証できるようになりました。パラメーターを指定してこの PowerShell コマンドを実行すると、間違ったパラメーターが使用されている場合、または

パラメーターが別のパラメーターと競合している場合は、適切なエラーメッセージが表示されます。その後、エラーメッセージを使用して問題を解決し、PowerShell を使用して MCS マシンカタログを正常に作成できます。

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

AWS でマシンプロファイルのソースから **VM** へのタグのコピーをサポート。この機能によって、AWS 仮想化環境で、マシンプロファイルで指定されている NIC およびディスク（ID ディスク、ライトバックキャッシュディスク、OS ディスク）上のタグを、MCS マシンカタログ内に新しく作成された VM にコピーできます。これらのタグは、任意のマシンプロファイルソース（AWS EC2 インスタンスまたは AWS 起動テンプレートバージョン）で指定できます。この機能は、永続および非永続のマシンカタログと VM に適用できます。詳しくは、「VM 上のタグをコピーする」を参照してください。

マシンプロファイルの **SCVMM** のサポート。この機能によって、マシンプロファイルを使用して、System Center Virtual Machine Manager（SCVMM）環境で MCS マシンカタログを作成および更新できるようになりました。入れ子構造の仮想化と vTPM を有効にすることもできます。詳しくは、「マシンプロファイルを使用してカタログを作成する」を参照してください。

MCS での **Spot VM** の使用に関する **Azure** のサポート。Azure Spot VM を使用すると、Azure の未使用のコンピューティング容量を活用することで、大幅なコスト削減になります。ただし、削除ポリシーがあるため、Azure Spot VM は、一部の重要ではないアプリケーションやデスクトップに適しています。

この機能を使用すると、マシンプロファイル（VM またはテンプレートスペック）を使用して Azure Spot VM の MCS マシンカタログを作成できます。既存のカタログを更新して、新しく作成された VM として Azure Spot VM を使用することも、標準の Azure VM を使用するように切り替えることもできます。既存の VM を更新して Azure Spot VM にすることもできます。詳しくは、「Azure Spot VM を使用したカタログの作成」を参照してください。

マシンプロファイルからの診断設定のキャプチャをサポート。Azure 環境では、MCS マシンカタログの作成中、または既存の VM の更新中に、マシンプロファイルから VM および NIC の診断設定をキャプチャできるようになりました。したがって、この実装によって、詳細な分析と視覚化のために、診断データを Log Analytics ワークスペースやイベントハブなどの指定された Azure の送信先エンドポイントにシームレスに送信できます。詳しくは、「マシンプロファイルから VM および NIC の診断設定をキャプチャする」を参照してください。

マシンカタログのさまざまなバージョンの管理に関する **MCS** のサポート。この機能によって、PowerShell コマンドを使用してさまざまなバージョンのマシンカタログを管理できます。`Set-ProvScheme`を使用して構成を変更するたびに、新しい構成バージョンが作成されます。次の操作を実行できます:

- バージョンの一覧を表示する。
- 以前のバージョンを使用してマシンカタログを更新する。
- VM で使用されていないバージョンを手動で削除する。
- マシンカタログによって保持されるバージョンの最大数を変更する。

詳しくは、「マシンカタログのバージョンの管理」を参照してください。

App-V、**MSIX**、**MSIX** アプリアタッチのパッケージアプリケーションをシングルセッション **VDA** または共有デスクトップ **VDA** で公開。シングルセッションおよび共有デスクトップ VDA 上の App-V、MSIX、MSIX アプリアタッ

チなどのパッケージアプリケーションにアクセスできるようになりました。この機能強化では、サインイン時にパッケージアプリケーションをすぐに使用できるようになります。この機能により、パッケージアプリケーションの起動が迅速になり、ローカルにインストールされたアプリケーションにアクセスできるようになり、エクスペリエンスが大幅に向上します。詳しくは、「パッケージアプリケーションをシングルセッション VDA または共有デスクトップ VDA で公開」を参照してください。

ライブセッションと録画されたセッションを再生する： Citrix Monitor は、Session Recording サービスを使用して録画されたユーザーセッションとライブのユーザーセッションの再生をサポートするようになりました。再生することで、ユーザーが遭遇したセッション関連の問題を即座に理解できます。この機能を使用すると、監視コンソール内のセッション関連のメトリックとともに録画にすぐにアクセスできるようになります。これは、録画で検出された問題をパフォーマンスメトリックと関連付けるのに役立ちます。複数のセッション録画サーバー間で録画を検索したり、録画を表示するためのサードパーティアプリを探したりする必要がなくなります。

この機能には、VDA および Session Recording サーバーのバージョン 2308 以降が必要です。

Monitor は録画を集中リポジトリに保存し、セッションセレクタモーダルに表示します。［録画のあるセッション］リンクには、過去 24 時間または過去 2 日間にアクティブだったセッションの録画が表示されます。録画は、Citrix Session Recording 再生サーバーを使用して新しいタブで再生されます。

詳しくは、「セッションの録画」を参照してください。

Microsoft Teams の最適化： Monitor には、Microsoft Teams で利用可能な HDX 最適化の状態が表示されます。新しい **Microsoft Teams** の最適化は、［ユーザーの詳細］ページ > ［セッションの詳細］パネルで確認できます。Monitor は、Microsoft Teams が公開アプリとして実行されている場合、または公開デスクトップ内で実行されている場合にのみ、Microsoft Teams の最適化の状態を表示します。この機能強化により、管理者は、ユーザーから報告された Microsoft Teams のセッションパフォーマンスの問題をトラブルシューティングするための情報を表示することができます。詳しくは、「ユーザーの問題のトラブルシューティング」を参照してください。

ユーザーインターフェイスの強化： Citrix Monitor ユーザーインターフェイスが最新の外観へと更新されました。新たに強化されたユーザーインターフェイスにより、ナビゲーションが容易になり、データの表示品質が向上します。エクスペリエンスが改善され、直感的で、Citrix セッションの監視とトラブルシューティングに必要なデータを簡単に把握できるように設計されています。

最適な画面解像度： Citrix Monitor の表示に推奨される最適な画面解像度は 1440 x 1024 に更新されました。

2024 年 **1** 月

新機能と機能強化

コンテンツの双方向リダイレクトの構成の強化 以前は、コンテンツの双方向リダイレクトの構成には、コンテンツの双方向リダイレクトを許可、VDA への URL のリダイレクトの許可、およびクライアントへの URL のリダイレクトの許可という 3 つの異なるポリシーの管理が必要でした。これらのポリシーでは、サーバー側（［**DaaS**］**>** ［完全な構成］で構成）とクライアント側（グループポリシーを通じて構成）の両方で構成が必要です。このリリース以降、3 つのポリシーすべてを 1 つのポリシーに統合しました。これにより、構成プロセスがシンプルになり、強化されるだけ

でなく、クライアント側の構成の要件も削減されます。詳しくは、「コンテンツの双方向リダイレクトの構成」を参照してください。

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

完全な構成から **Global App Configuration Service** へのアクセスをサポート。Global App Configuration Service にリンクするためのアクション項目が完全な構成インターフェイスで提供されています。この統合により、Global App Configuration に簡単にアクセスして、完全な構成でエンドユーザー設定を管理できるようになります。

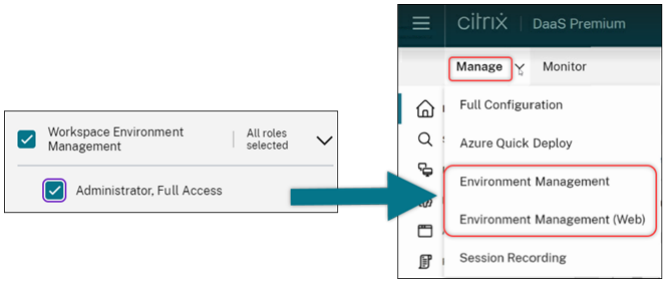
完全な構成からこのサービスにアクセスするには、次の 2 つのオプションがあります：

- **StoreFront** ノードを選択し、サーバーレコードをクリックして、操作バーの ［クライアント設定を構成する］を選択します。
- ポリシーノードを選択し、操作バーの ［クライアント設定を構成する］を選択します。

Citrix Cloud 管理のデリバリーグループで、完全な構成を使用したユーザー割り当て管理をサポート。ユーザー割り当ての管理を Cloud ライブラリから完全な構成に移行する計画の一環として、Citrix Cloud 管理のデリバリーグループのユーザー割り当てを完全な構成を通じて管理できるようになりました。このタスクを実現するには、［完全な構成］**>**［デリバリーグループ］でターゲットのデリバリーグループを編集し、次のメニューのいずれかを使用してデスクトップまたはアプリケーションの使用を許可するユーザーを指定します：デスクトップ（またはデスクトップ割り当て規則）またはアプリケーション割り当て規則。詳しくは、「デリバリーグループの管理」を参照してください。

一方のポータルで行われた更新はもう一方のポータルとシームレスに同期され、両方のポータルで一貫した更新が保証されます。

WEM フルアクセス権管理者の役割への **WEM** コンソールのアクセスを制限します。不正な侵入を防ぐために、Workspace Environment Management（WEM）コンソールのアクセス制御を有効にしました。**Workspace Environment Management** のフルアクセス管理者の役割を持つユーザーのみが、［**DaaS**］**>**［管理］を使用して WEM コンソールにアクセスできるようになりました。



完全な構成：**Azure** カタログは、マスターイメージからの **DES** 設定の継承をサポートします。以前は、完全な構成では、Azure カタログのデフォルトの DES 設定はマシンプロファイルに基づいてのみ設定されていました。この機能は強化されました。この機能強化により、次の場合、［完全な構成］がマスターイメージに基づいて Azure カタログのデフォルトの DES 設定を直接指定します：

- マシンプロファイルが選択されていない場合
- プロファイルでプラットフォーム管理キー（PMK）が指定されている場合

詳しくは、「完全な構成インターフェイスと Azure Resource Manager イメージを使用してマシンカタログを作成する」を参照してください。

強化された検索：フィルターの数が増えて精度が向上しました。検索ノードの検索を強化して、ゾーンとプロビジョニングの種類という 2 つの新しいフィルターを追加することで、精度を高め、使いやすさを向上しました。

完全な構成：**GCP** マシンカタログで **Google Cloud** マシンの種類の選択をサポート。この機能を使用すると、管理者はプロビジョニングされた GCP VM に必要なメモリとプロセッサ構成を柔軟に選択し、特定の運用要件を満たすように調整できます。詳しくは、「完全な構成インターフェイスを使用してマシンカタログを作成する」を参照してください。

GCP VM をプロビジョニングするためのグローバルおよびリージョンの顧客管理暗号キー（**CMEK**）をサポート。任意のプロビジョニングプロジェクトから VM をプロビジョニングするために、グローバルおよびリージョンの CMEK キーを使用できるようになりました。この機能強化により、VM をプロビジョニングし、VM のセキュリティを向上させるためのキー選択の柔軟性が向上します。

2023 年 12 月

新機能と機能強化

メッセージの送信の進行状況。［モニター］>［フィルター］で［メッセージ送信］操作の進行状況を確認できるようになりました。この操作は、サイト上の接続されているすべてのセッションに一括メッセージを送信するのに役立ちます。操作の進行状況がパーセントで表示されます。操作が完了すると、システムは送信されたメッセージの数と失敗したメッセージの数を表示します。メッセージの送信ステータスは、大規模なサイトを管理する場合に役立ちます。これは、メッセージを特定のユーザーに再送信する必要があるかどうかを理解するのに役立ちます。マシンが登録されていない場合、またはセッションに障害がある場合、メッセージの送信は失敗する可能性があります。［メッセージ送信］の詳細については、「ユーザーへのメッセージの送信」を参照してください。

ドメイン資格情報と多要素認証を使用した、**Citrix Gateway** 経由での **Citrix Probe Agent** 認証のサポート。

アプリケーションおよびデスクトッププロービング用の Citrix Probe Agent が、ドメイン資格情報と多要素認証を使用した、Citrix Gateway 経由での認証をサポートするようになりました。この機能は、Citrix Gateway 経由で StoreFront に接続されているマシン上で Probe Agent を実行するのに役立ちます。［モニター］に表示される包括的なプローブ結果は、アプリケーション、ホストマシン、または接続に関連する問題を、ユーザーが経験する前にトラブルシューティングするのに役立ちます。多要素認証と Citrix Gateway のサポートは、は、シングルログインスキーマを使用する LDAP およびネイティブ OTP で構成された Citrix Gateway でのみ使用できます。詳しくは、「アプリケーションプロービングおよびデスクトッププロービング」を参照してください

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

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

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

2023 年 11 月

新機能と機能強化

完全な構成インターフェイスを使用した **Citrix Provisioning** カタログの作成をサポート。Citrix Provisioning カタログを作成するには、Citrix Virtual Apps and Desktops インストールウィザードを使用する必要がありました。この機能により、完全な構成ユーザーインターフェイスと PowerShell を使用して、Citrix Provisioning カタログを作成できるようになりました。

この機能の導入には、次のような利点があります:

- MCS と Citrix Provisioning カタログの両方を管理できる単一の統合コンソール。
- ID 管理ソリューション、オンデマンドプロビジョニングなどの Citrix Provisioning カタログの新機能を利用できる。

現在、この機能は Azure ワークロードでのみ使用できます。詳しくは、「Citrix Studio での Citrix Provisioning カタログの作成」を参照してください。

アプリケーショングループの検索を導入。アプリケーションノードにアプリケーショングループの検索機能を導入しました。この機能強化により、任意のアプリケーションフォルダー内のアプリケーショングループを直接検索できるようになりました。詳しくは、「アプリケーショングループの検索」を参照してください。

構成の制限が変更されました。次の表では、パフォーマンスを向上させ、コスト効率を高めるために DaaS 構成の制限に加えられた変更について説明します。

リソース	古い制限	新しい制限
Active Directory ドメイン	85	100
カタログ	1000	2000

リソース	古い制限	新しい制限
デリバリーグループ	1000	2000
リソースの場所	85	100
リソースの場所 -> 合計セッション数	20,000	25,000

詳しくは、「制限」を参照してください。

電源サイクル中に仮想マシンとシステムディスクを保持する単一のオプション。Azure 上で既存の仮想マシンを起動するほうが、新しい仮想マシンを起動するよりも速くなったため、電源サイクル中に仮想マシンを保持するためのより効率的な選択肢になりました。この変更に対応して、［電源サイクルをまたいで仮想マシンを保持する］オプションと ［電源サイクル中にシステムディスクを保持する］オプションは、1 つのオプション ［電源サイクル中に仮想マシンとシステムディスクを保持する］に統合されました。つまり、このオプションを選択してシステムディスクを保持することで仮想マシンの再起動時間を短縮すると、仮想マシンも同様に保持されます。

［完全な構成］の新機能により、マシンプロファイルの ［ホストでの暗号化］プロパティに基づいてマシンサイズをフィルタリングできます（**Azure** 仮想マシンのみ）。Azure マシンカタログの作成または管理中に ［ホストでの暗号化］が有効になっているマシンプロファイルを選択すると、この機能をサポートするマシンサイズのみが表示されます。

バックアップと復元の操作をすべての管理権限を実行できる管理者の役割に限定します。バックアップおよび復元操作のアクセス制御が強化されました。すべての管理権限を実行できる管理者の役割を持つユーザーのみが ［バックアップと復元］ノードにアクセスして、不正な操作を防止できるようになりました。

検索ノードのデータキャッシュ。Citrix DaaS 検索ノードのデータキャッシュを導入しました。この機能強化により検索のパフォーマンスが向上します。以下は、定期的なタスクを容易にするユースケースです：

- 初めて取得した検索結果をすばやく表示します。
- 検索ノードから移動して戻った後も、結果のページネーションを保持します。

マシンカタログページのイメージ情報。マシンカタログの ［テンプレートのプロパティ］を通じて、次のイメージ情報を表示できるようになりました：

- オペレーティングシステム
- Machine Identity Service
- Machine Creation Services ストレージ
- Azure 展開の`pagefile.sys`のファイルパス。

この機能強化により、イメージ情報がより明確になり、管理者はマシンカタログに関するすべての情報を 1 か所で確認できるようになります。

固定検索フィルターのサポート。すばやい検索エクスペリエンスを提供するために、完全な構成では検索フィルターを固定する機能が有効になります。フィルターピンを使用すると、頻繁に使用する検索フィルターをページ上でアクセス可能にできます。この機能強化は、次のノードの検索パネルで利用できます：

- 検索
- マシンカタログ
- デリバリーグループ
- アプリケーション

詳しくは、「［完全な構成］管理インターフェイスでの［検索］の使用」を参照してください。

メタデータと構成ログの関連付けのサポート。この拡張機能を使用すると、高レベルの操作で`name-value`ペアを関連付けることにより、構成ログにメタデータを添付できるようになりました。詳しくは、「メタデータを構成ログに関連付ける」を参照してください。

特定のタグを持つ孤立したリソースを無視します。Azure 環境では、すべての Citrix タグでタグ付けされた顧客が管理するリソースは、孤立したリソースとして検出されます。この機能では、値が true の別のタグ`CitrixDetectIgnore`をそのリソースに追加すると、孤立したリソースの検出中にリソースは無視されます。

SCCM の **GUID** 重複問題の解決策。MCS を使用して複数の VM を作成した後、GUID が重複しているため、System Center Configuration Manager（SCCM）のコンソールには VM が 1 つしか表示されませんでした。この問題は、イメージの準備に手順を追加することで解決されました。この手順では、マスターイメージ内の既存の証明書と GUID 情報が削除されます。この手順はデフォルトで有効になっています。

アクティブなコンピューターアカウントの **ID** 情報を修復します。この機能では、ID 関連の問題があるアクティブなコンピューターアカウントの ID 情報をリセットできます。マシンのパスワードと信頼キーのみをリセットするか、ID ディスクのすべての構成をリセットするかを選択できます。この実装は、永続および非永続の両方のマシンカタログに適用できます。現在、この機能は Azure、VMware 仮想化環境でのみサポートされています。詳しくは、「アクティブなコンピューターアカウントの ID 情報を修復する」を参照してください。

マシンプロファイルに関連付けられたホスト情報の暗号化を取得する。Azure 環境では、この機能により、PowerShell コマンドを使用してマシンプロファイル入力（VM またはテンプレートスペック）に対してホストでの暗号化が有効になっているかどうかを確認できるようになりました。詳しくは、「マシンプロファイルからホストでの暗号化情報を取得する」を参照してください。

Hybrid Azure AD 参加マシン **ID** のユーザー証明書を修復します。この機能により、Hybrid Azure AD 参加マシン ID のユーザー証明書が破損したり期限切れになった場合に、Powershell コマンドを使用して修復できます。詳しくは、「Hybrid Azure Active Directory 参加済みカタログの作成」を参照してください。

Hybrid Azure AD 参加マシンカタログに対する証明書の有効期限の警告をサポート。完全な構成では、Hybrid Azure AD 参加マシンカタログのユーザー証明書の有効期限が 1 か月前に警告されるようになりました。この機能強化は、証明書の有効期限切れによるサービス中断のリスクを軽減することを目的としています。詳細と推奨されるアクションを表示するには、［マシンカタログ］ノードに移動し、マシンカタログを選択して、［トラブルシューティング］タブをクリックします。

`Get-ProvScheme`コマンドを実行すると、Hybrid Azure AD 参加マシンカタログのユーザー証明書の有効期限に関する情報を取得できます。

Azure Confidential VM のサポート（**Technical Preview**）。Azure Confidential Computing VM によって、

仮想デスクトップは確実にメモリ内で暗号化され、使用中に保護されます。この機能により、MCS を使用して、Azure Confidential VM を含むカタログを作成できるようになりました。このようなカタログを作成するには、マシンプロファイルワークフローを使用する必要があります。VM と ARM テンプレートスペックの両方をマシンプロファイル入力として使用できます。詳しくは、「Azure Confidential VM（Technical Preview）」を参照してください。

AWS 環境で、非マシンプロファイルベースのマシンカタログからマシンプロファイルベースのマシンカタログへの変換をサポート。AWS 環境で、VM または起動テンプレートをマシンプロファイルの入力に使用して、非マシンプロファイルベースのマシンカタログをマシンプロファイルベースのマシンカタログに変換できるようになりました。カタログに追加された新しい VM は、マシンプロファイルからプロパティ値を取得します。詳しくは、「非マシンプロファイルベースのマシンカタログをマシンプロファイルベースのマシンカタログに変換する」を参照してください。

Citrix が管理する **HPE Moonshot** プラグインのサポート（**Technical Preview**）。以前は、HPE Moonshot シャーシで電源管理アクションを実行するために、Hewlett Packard Enterprise（HPE）によって管理される、HPE 管理 Moonshot プラグイン（HPE Moonshot Machine Manager）を使用していました。このプラグインは従来の API に基づいていたため、MCS インフラストラクチャプロジェクトが手間のかかるものになっていました。この機能により、Citrix 管理の HPE Moonshot プラグイン（HPE Moonshot）が導入されます。このプラグインを使用すると、［完全な構成］インターフェイスと PowerShell コマンドを使用して、HPE Moonshot シャーシへの接続の作成、カタログの作成、カタログ内のマシンの電源管理が可能になります。詳しくは、次のトピックを参照してください：

- HPE Moonshot 仮想化環境（Technical Preview）
- HPE Moonshot への接続（Technical Preview）
- HPE Moonshot マシンカタログの作成（Technical Preview）
- HPE Moonshot カタログの管理（Technical Preview）

メモリとディスクキャッシュのサイズを変更する機能。この機能により、新しいマシンカタログを作成せずに、PowerShell コマンドを使用してライトバックキャッシュのメモリおよびディスクキャッシュサイズを変更できるようになりました（MCSIO が有効な場合）。この実装は、ビジネスニーズに適した最適化されたキャッシュ構成を実現するのに役立ちます。この機能は以下に適用されます：

- GCP および Microsoft Azure 環境、および
- MCSIO が有効になっている非永続カタログ

詳しくは、「既存のマシンカタログのキャッシュ構成を変更する」を参照してください。

顧客管理の暗号化キー対応カタログの作成をサポート。Azure 環境では、［完全な構成］インターフェイスと PowerShell コマンドを使用して、顧客管理の暗号化キー（CMEK）が有効になった Citrix Provisioning カタログを作成できるようになりました。詳しくは、「顧客管理の暗号化キー対応カタログを作成する」を参照してください。

Azure 内のすべてのリソースのタグをコピーする機能。この機能により、Azure 環境で、マシンプロファイルで指定されたタグをマシンカタログ内の新しい VM または既存の VM の複数の NIC やディスク（OS ディスク、ID ディスク、ライトバックキャッシュディスク）などのすべてのリソースにコピーできるようになりました。

マシンプロファイルのソースは、VM または ARM テンプレートスペックにすることができます。詳しくは、「すべてのリソースのタグをコピーする」を参照してください。

マシンが一時停止した後、セッション状態が「切断済み」に更新されます。以前は、VM を一時停止した後も、セッションは依然として「アクティブ」として表示されていました。この機能強化により、VM を一時停止した後、関連付けられたセッションの状態が「切断済み」として表示されるようになりました。

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

デリバリーグループレベルでの負荷分散方法の構成のサポート（**Technical Preview**）。この機能を使用すると、デリバリーグループレベルで ［垂直負荷分散］ 方式を選択できます。この機能により、次のマシンの電源がオンになる前に、各マシンが最大負荷インデックスに合わせて調整されます。Autoscale と垂直負荷分散により、次のマシンの電源がオンになるタイミングが決まります。この機能により、各マシンの使用率が最大化され、パブリッククラウドのコスト削減が実現します。この機能により、マシンの負荷分散戦略をより柔軟に管理できます。

サイトレベルの設定から負荷分散方式を継承するか、サイトレベルの負荷分散方式を上書きして代わりに垂直または水平負荷分散方式のいずれかを選択するようにデリバリーグループを構成できます。詳しくは、「手順 2. 負荷分散」を参照してください。

Azure での休止状態対応 **VM** のサポート（**Technical Preview**）。Azure 環境では、休止状態をサポートする MCS マシンカタログを作成できます。この機能を使用すると、VM を一時停止し、ユーザーが再度サインインしたときに VM の以前の状態に再接続できます。詳しくは、「休止状態対応 VM の作成（Technical Preview）」を参照してください。

DaaS 入門ガイド。新しい管理者と経験豊富な管理者の両方を対象に、DaaS の展開と構成を合理化および簡素化するための新しいガイドが導入されました。このガイドには、次のような主なメリットがあります：

- 簡単に利用を開始できる。このガイドは、ステップごとに分けられた質問形式のアプローチを使用して、新しい管理者が展開を迅速にセットアップできるようにします。ガイド全体を通してヘルプ情報が提供されるため、重要な概念や用語の理解を助けます。
- 複雑な構成がシンプルになる。このガイドでは、必要に応じて事前構成された設定が提供され、高度な構成のための［完全な構成］の UI を利用できます。経験豊富な管理者は、より複雑な構成の基盤としてこれを使用できます。

詳しくは、「DaaS 入門ガイドの使用」を参照してください。

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

［完全な構成］を使用したさまざまな **Azure** マシンプロパティの変更をサポートします。Machine Creation Services でプロビジョニングされた Azure マシンの場合、［完全な構成］を使用して次のプロパティ設定を変更でき

るようになりました:

- ストレージの種類
- 専用ホストグループ
- Azure Compute Gallery 設定

これらの設定のいずれかを変更すると、[完全な構成] は関連する設定を自動的に識別し、自動同期を提供したり、関連する設定の再選択を求めるプロンプトメッセージを表示したりします。この機能により、関連する設定全体で一貫した変更が保証され、構成エラーの可能性を防止できます。詳しくは、「カタログの編集」を参照してください。

既存の **ID** プールを使用して、**MCS** でプロビジョニングされたマシンの **ID** を作成します。AD 参加済みのカタログを作成する場合、または [完全な構成] を使用してカタログにマシンを追加する場合、既存の ID プールを使用してマシン ID を割り当てることができるようになりました。この機能を使用すると、複数のカタログにわたって一貫したマシンアカウントの名前付けスキームを適用できます。詳しくは、「マシン ID」を参照してください。

セッションのトポロジ。[セッションのトポロジ] ビューは、[監視] のトラブルシューティングワークフローを強化するための次の段階です。[セッションのトポロジ] パネルは、接続された HDX セッションのセッション内パスを視覚的に表現します。[ユーザーの詳細] **>** [セッションパフォーマンス] でトポロジのビューにアクセスできます。

HDX 接続されたセッションのセッショントポロジには、セッションパスに含まれるコンポーネントとそのメタデータ、コンポーネント間のリンク、および VDA で公開されたアプリケーションが表示されます。さらに、接続状態にあるセッションの ICA 遅延および ICA 往復時間測定値が表示されます。

[セッションのトポロジ] ビューを使用すると、セッションデータのフローでコンポーネントを理解し、パフォーマンスの問題を引き起こしている可能性のある特定のホップを識別できます。詳しくは「セッションのトポロジ」を参照してください。

2023 年 **10** 月

新機能と機能強化

使用履歴を使用して **Autoscale** 設定を調整します。[**Autoscale** の分析情報] という新しい Autoscale 設定のタブには、前週の Autoscale 設定とマシン使用状況データを視覚的に比較する包括的なグラフが表示されます。このグラフによって、Autoscale 設定の有効性関する次のような分析情報を得ることができます:

- 費用対効果が低い。容量の過剰なプロビジョニングにより、財務上の無駄が発生します。
- ユーザーエクスペリエンスの質が低い。容量のプロビジョニング不足によりユーザーエクスペリエンスが悪影響を受けます。
- ユーザーエクスペリエンスとコストのバランスが取れています。プロビジョニングされた容量は、使用履歴に合わせて調整されます。

詳しくは、「Autoscale 設定の有効性の分析」を参照してください。

Azure VM に対する複数の **NIC** のサポート。[完全な構成] では、複数の NIC を構成した Azure 仮想マシンを作成できるようになりました。仮想マシンの最大 NIC 数はマシンサイズ設定によって決まりますが、実際に許可される NIC 数はマシンプロファイル設定によって定義されます。詳しくは、「マシンカタログの作成」を参照してください。

PowerShell コマンドを使用して仮想マシンごとに複数の NIC を構成したカタログを作成または更新する場合は、「VM ごとに複数の NIC を含むカタログを作成または更新する」を参照してください。

セッションパフォーマンスメトリックの傾向。[監視] では新しい [ユーザーの詳細] > [セッションパフォーマンス] タブが導入され、ユーザーセッション内の問題を特定する際にリアルタイムでメトリックを相関させる機能をはじめ、トラブルシューティングのワークフローが強化されています。セッションエクスペリエンスには、ICA RTT、ICA 遅延、フレーム数/秒、利用可能な出力帯域幅、消費された出力帯域幅などのセッションメトリックの傾向が含まれるようになりました。この機能は、単一のビューで複数のパフォーマンスメトリックを関連付けることができるため、解決までの平均時間を短縮するのに役立ちます。詳しくは、「ユーザーの問題」の記事を参照してください。

作成/編集ポリシーの設定ページでの **VDA** バージョンのサポート。ポリシーの作成の一環として、設定の構成時に、システムによって設定の種類を表示するオプションが提供されます。表示できる設定の種類は以下のとおりです:

- すべての設定 - すべての VDA バージョンのすべての設定を表示します
- 現在の設定のみ - 現在の VDA バージョンのみの設定を表示します
- 従来の設定のみ - 廃止された VDA バージョンのみの設定を表示します

詳しくは、「ポリシーの作成」を参照してください

アプリケーションの表示の制限は、**Active Directory** アカウントでのみサポートされます。アプリケーションの表示を制限する機能は、Active Directory ユーザーアカウントでのみ使用でき、Azure Active Directory および Okta アカウントでは使用できません。この機能を支援するために、アプリケーション設定ワークフローの [ユーザーまたはグループの選択] ページで、[**ID** の種類を選択] フィールドの **Azure Active Directory** および **Okta** オプションが無効になっていることに注意してください。

Citrix サイトデータベースから仮想マシンレコードのみを削除する新しい **UI** オプション。ハイパーバイザーへ到達できないためにカタログと仮想マシンの削除が失敗した場合、Citrix サイトデータベースから仮想マシンレコードのみを削除し、ホスト上の仮想マシンをそのまま残すことを選択できるようになりました。詳しくは、 [カタログの削除] を参照してください。

MCS 以外でプロビジョニングされたマシンについて、空のマシンカタログの作成のサポート。空のマシンカタログの作成が、次のような MCS 以外でプロビジョニングされたマシンにも拡張されるようになりました。

- Machine Creation Services 以外のテクノロジーを使用してプロビジョニングされた仮想マシンまたはブレードマシン。
- Citrix DaaS によって電源管理されない物理マシン
- Remote PC アクセスマシン

この機能により、カタログ作成中にマシンを追加しなくても、マシンカタログを作成できるようになりました。

イメージの更新の機能強化。以前はイメージを更新する際に、イメージツリー内の特定のノードが選択されているかどうかに関係なく、ツリー内のすべてのイメージが更新されました。最新の機能強化により、ノードを選択した場合

に、そのノード内のイメージのみが更新されます。このような機能強化を使用することで、よりターゲットを絞った更新プロセスが保証され、イメージの更新速度が大幅に向上します。さらに、CTRL キーを押しながらノードをクリックすることで、イメージツリーで選択したノードをクリアできるようになりました。詳しくは、「マスターイメージ」を参照してください。

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

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

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

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

複数の **Citrix DaaS** インスタンスの監視（**Technical Preview**）。Citrix Monitor を使用して、複数の Citrix DaaS インスタンスにわたる問題を監視およびトラブルシューティングできるようになりました。Citrix DaaS により、顧客はハブアンドスポークモデルを使用して複数のサービスインスタンスを集約できます。この構成により、管理者は、単一の［監視］コンソールから、構成済みのすべての DaaS インスタンスに対してヘルプデスク検索を実行できます。スポークサービスのインスタンスをハブに集約するために必要な構成の詳細については、「複数の Citrix Virtual Apps and Desktops サービスインスタンスの集約」を参照してください。［監視］は、単一のテナント（ハブ）で最大 4 つの DaaS テナント（スポーク）のアグリゲーションをサポートします。
すべての DaaS テナントにわたる統合監視を行うには、ハブアンドスポークインスタンスの双方向列挙を使用します。詳しくは、「複数の DaaS インスタンスにわたる集約検索（Technical Preview）」を参照してください。

vSAN 8.0 のサポート。MCS を使用して、vSAN 8.0 環境で VM をプロビジョニングできるようになりました。

プロビジョニングされた **VM** で **NIC** 設定を保持。以前は、プロビジョニングされた VM 内にマスターイメージの NIC 設定が保持されませんでした。たとえば、マスターイメージで DNS 設定を構成した場合、プロビジョニングされた VM はマスターイメージの構成された DNS 設定を保持しませんでした。この機能により、プロビジョニングされた VM はマスターイメージの NIC 設定を保持できるようになりました。Windows Update 後も設定は保持されます。
フィルタードライバーは、MCS マスターイメージのインストールを通じて Hyper-V が展開されたマシンで VDA バージョン 2308 以降の新規インストールを行う場合に自動的にインストールされます。ただし、現在、古いバージョンの VDA（バージョン 2308 より前のバージョン）からアップグレードし、フィルタードライバーをインストールする場合は、VDA のアップグレード中に ［追加コンポーネント］ページのチェックボックス ［**Citrix HyperV** フィルタードライバー］を選択する必要があります。詳しくは、「追加コンポーネントのインストール」を参照してください。

この機能は以下に適用されます：

- Hyper-V VM（Azure および SCVMM を含む）

- 永続的および非永続的 MCS マシンカタログ
- MCSIO を使用した非永続的 MCS マシンカタログ
- 複数の NIC があるマスターイメージ

孤立した **Azure** リソースを検出する。この機能により、Azure 展開内の孤立したリソースを検出できるようになり、効率的なリソース管理が可能になります。孤立したリソースが特定されたら、生産性の向上とコスト削減を実現するためのさらなるアクションを実行できます。詳しくは、「展開内の孤立した Azure リソースを検出する」を参照してください。

新しいイメージ更新ステータス。[完全な構成] でカタログのイメージ更新ステータスを監視するときに、既存の完全に更新、部分的に更新、および更新が保留中に加えて、新しいステータスであるイメージの準備中を表示できるようになりました。詳しくは、「マスターイメージの変更」を参照してください。

自動タグを作成するための **PowerShell** コマンド（**Technical Preview**）。この機能により、PowerShell コマンドを使用してタグを自動的に作成できるようになりました。詳しくは、「自動タグ」を参照してください。

通知サインがユーザーまたはデリバリーグループに対して表示されます。ポリシーを作成または変更して設定を構成するときに、すべてのデリバリーグループが無効になっている場合、システムは「このフィルター内のどの要素も有効ではありません」のような警告を表示します。少なくとも 1 つのデリバリーグループが有効になっている場合、システムによる警告サインは表示されません。詳しくは、「ポリシー設定」を参照してください。

2023 年 **9** 月

新機能と機能強化

ローカルホストキャッシュ（**LHC**）を管理するための **PowerShell** コマンド。PowerShell コマンドを使用して Citrix Cloud Connector 上で LHC を管理できるようになりました。詳しくは、「Local Host Cache PowerShell commands」を参照してください。

空のマシンカタログの作成のサポート。完全な構成では、仮想マシンをその場で作成せずにマシンカタログを作成できるようになりました。この機能により、バックエンドホストの準備が完了するまで、または仮想マシンのプロビジョニングが完了するまで仮想マシンの作成を延期できるため、より柔軟にカタログ作成を行えるようになります。現在、この機能は Machine Creation Services によってプロビジョニングされたカタログにのみ適用されます。詳しくは、「マシンカタログの作成」を参照してください。

ホームノードのデータキャッシュ。Citrix DaaS **Home** ノードのデータキャッシュを導入しました。この機能強化により、ホームノードに移動するときのページ読み込み時間が短縮され、ユーザーエクスペリエンスが向上します。

アプリケーションの検索機能の強化。検索ノードに導入された新しい設計に合わせて、アプリケーションノードの検索機能を刷新しました。この新機能により、アプリケーションの検索エクスペリエンスが向上し、DaaS 全体で一貫した検索エクスペリエンスが維持されます。フィルター式に含まれるキーワード **Application Name** は、元の意味を保持したまま **Name** に変更されます。詳しくは、「[完全な構成] 管理インターフェイスでの [検索] の使用」を参照してください。

拡張されたスコープ管理：フォルダービューでのオブジェクトの表示。スコープの作成および管理ページでは、マシンカタログ、デリバリーグループ、およびアプリケーショングループが、DaaS での管理に合わせたフォルダー構造で表示されます。このフォルダービューにより、スコープの作成および管理のためにオブジェクトを選択するプロセスが簡素化され、より直観的かつ簡単に選択できるようになります。詳しくは、「スコープの作成と管理」を参照してください。

［ユーザー管理を **Citrix Cloud** に任せる］オプションを削除しました。［管理］>［完全な構成］のでデリバリーグループを作成するときに、［ユーザー］ページでこのオプションがサポートされなくなりました。ユーザー割り当てが Citrix Cloud を通じて処理されたデリバリーグループについては、引き続き Citrix Cloud ライブラリ内でユーザー割り当てを管理します。

Azure Germany オプションを削除しました。2021 年 10 月 29 日の Microsoft Cloud Deutschland の閉鎖に伴い、ホスト接続作成ページから **Azure Germany** オプションを削除しました。

［完全な構成］での予防的なサービスアラート。アラートには 2 つのレベルがあります。ホーム（フラグアイコン）に表示されるサイト全体のアラートと、各ゾーンの［トラブルシューティング］タブに表示されるゾーン関連のアラートです。現在、この機能は、ローカルホストキャッシュとゾーンが正しく構成されていることを確認するための予防的な警告とアラートを提供するため、停止が発生した場合でもローカルホストキャッシュが機能し、ユーザーに影響が及ばなくなります。詳しくは、「サービス正常性アラート」と「ゾーン」を参照してください。

2023 年 **8** 月

新機能と機能強化

完全な構成：マシンプロファイルを使用した **AWS** および **GCP VM** のプロビジョニングのサポート。Machine Creation Services（MCS）を使用して AWS または GCP VM をプロビジョニングするときに、既存の VM をマシンプロファイルとして選択し、カタログ内の VM が選択した VM から設定を継承できるようになりました。

- GCP VM の場合、継承される設定には、ディスク暗号化セット ID、マシンのサイズ、ストレージの種類、ゾーンが含まれます。
- AWS VM の場合、継承される設定はステージに応じて異なります：
  - カタログ作成時：マシンのサイズ、テナントの種類、セキュリティグループ、および NIC の数。
  - カタログ編集中：マシンのサイズとセキュリティグループ。

詳しくは、「マシンカタログの作成」を参照してください。

マシンカタログおよびデリバリーグループノードに検索機能が導入されました。［マシンカタログ］および［デリバリーグループ］ノード内で、直接マシンカタログやデリバリーグループを検索して見つけることができるようになりました。これらのノードの検索機能は、［検索］ノードと同じインターフェイスを提供し、DaaS 全体でシームレスな検索エクスペリエンスを実現します。詳しくは、「［完全な構成］管理インターフェイスでの［検索］の使用」を参照してください。

Device Posture を使用したセッション起動診断でエンドポイントデバイスの状態を表示します。［監視］のセッション起動診断機能は、セッション障害が発生した正確なコンポーネントと段階を絞り込むのに役立ちます。これは、セッションの起動エラーの正確な理由を特定し、推奨される操作を実行するのに役立ちます。

セッション起動シーケンスに関係するすべてのコンポーネントにわたって包括的にこのチェックを行うための次の手順として、エンドポイントデバイスのスキャン結果を表示できるようになりました。コンポーネントの一覧で ［エンドポイントデバイス］をクリックして、Device Posture スキャンの状態を表示します。Device Posture サービスは、管理者が定義したポリシーに基づいて、エンドポイントデバイスのコンプライアンスをスキャンします。

Device Posture の記事で説明されているように、Device Posture サービスが DaaS で構成されていることを確認します。Device Posture によって記録されるエラーについては、「Device Posture のエラーログ」で説明されています。

詳しくは、「セッションの起動エラーを診断する手順」を参照してください。

Citrix Cloud Connector 経由で **API** 要求を **Azure** および **GCP** にルーティングする、完全な構成の新しいオプション。以前は、Azure および GCP への API 要求はパブリックエンドポイント経由でのみルーティングできました。［完全な構成］**>** ［接続およびリソースの追加］の新しいオプションで、Citrix Cloud Connector 経由でルーティングすることで、より安全なアプローチを選択できるようになりました。詳しくは、「完全な構成を使用したサービスプリンシパルと接続の作成」を参照してください。

検索とフィルターの機能が強化されました。検索エクスペリエンスを向上させるために、次の機能強化が行われました：

- 簡易検索：フィルターを使用せずに検索を実行すると、検索の推奨事項が削除され、クリーンで簡単な検索エクスペリエンスが提供されるようになりました。
- **AND/OR** 演算子の更新：「すべて一致（AND 演算子）」および「一部が一致（OR 演算子）」オプションがフィルターパネルで使用できるようになり、フィルターアイコンを 1 回クリックするだけでアクセスできるようになりました。
- 合理化されたフィルター構成：フィルターパネルを使用して、複数のフィルターをシームレスに指定して適用できるようになりました。
- よりクリーンなインターフェイス：「フィルター固定」機能が削除され、UI の混雑が軽減され、検索エクスペリエンスがより直感的になりました。
- クイックフィルターの追加：フィルターを適用した後、プラス記号を使用してフィルター 1 つをさらに追加できるようになりました。
- 保存されたフィルターセットの削除：［フィルターセットの管理］に移動しなくても、検索メニュー内で保存されたフィルターセットを簡単に削除できるようになりました。

詳しくは、「［完全な構成］管理インターフェイスでの［検索］の使用」を参照してください。

Azure クイック展開で作成されたマシンカタログの **VDA** アップグレードをサポート。完全な構成では、Azure クイック展開を通じて作成されたマシンカタログの **VDA** アップグレードを有効にし、それらに対して **VDA** のアップグレードを実行して即時アップグレードまたはスケジュールされたアップグレードを行うことができるようになりました。詳しくは、「完全な構成インターフェイスを使用した VDA のアップグレード」を参照してください。

SCVMM の **MCS** で作成されたマシンカタログ内における永続的な **VM** の **OS** ディスクをリセットする機能。PowerShell コマンド`Reset-ProvVMDisk`を使用して、MCS で作成されたマシンカタログ内の永続的な VM の OS ディスクをリセットできるようになりました。この機能は、OS ディスクをリセットするプロセスを自動化します。たとえば、MCS を使用して作成された永続的な開発デスクトップカタログの初期状態に VM をリセットするのに役立ちます。現在、この機能は Azure、Citrix Hypervisor、SCVMM、VMware 仮想化環境に適用できます。PowerShell コマンドを使用して OS ディスクをリセットする方法について詳しくは、「OS ディスクのリセット」を参照してください。

個別の **VM** のプロパティを更新する。PowerShell コマンドを使用して、永続的な MCS マシンカタログ内の個別の VM のプロパティを更新できるようになりました。この実装により、マシンカタログ全体を更新することなく、個別の VM を効率的に管理できます。現在、この機能は Azure 環境にのみ適用されます。詳しくは、「個別の VM のプロパティを更新する」を参照してください。

管理対象ディスクのアップロードとダウンロードの制限。Azure ポリシーに従って、同じディスクアクセスオブジェクトで同時に 5 つを超えるディスクまたはスナップショットをアップロードまたはダウンロードすることはできません。この機能を使用すると、次の場合、5 つの同時アップロードまたはダウンロードの制限は適用されません:

- `CustomProperties`で`ProxyHypervisorTrafficThroughConnector`を構成している。および
- プライベートエンドポイントを使用する新しいディスクごとにディスクアクセスを自動的に作成するように Azure ポリシーを構成していない。

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

Citrix Hypervisor でのマシンプロファイルをサポート。Citrix Hypervisor で、マシンプロファイルを使用して MCS マシンカタログを作成できるようになりました。マシンプロファイルの入力のソースは VM です。マシンプロファイルは、VM テンプレートからハードウェアプロパティを取得し、カタログ内の新しくプロビジョニングされた VM に適用します。詳しくは、「マシンプロファイルを使用してマシンカタログを作成する」を参照してください。

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

構成セットを管理するための権限。WEM 構成セット管理をより正確に制御できるようにするために、［構成セットの管理］という新しい権限を ［マシンカタログ］権限セットに導入しました。この権限は、構成セットのバインドまた

はバインド解除、カタログの別の構成セットへの切り替えなどのタスクを実行できるユーザーに排他的アクセス権を付与します。詳しくは、「カタログの構成セットの管理」を参照してください。

古い **Azure AD** 参加デバイスのクリーンアップを有効にするオプションが［完全な構成］に新しく追加されました。Citrix DaaS での古い Azure AD 参加デバイスのクリーンアップを簡素化するオプションを［完全な構成］に導入しました。以前は、このタスクを実行するにはカスタム PowerShell スクリプトを実行する必要がありました。このオプションを有効にすると、古い Azure AD 参加デバイスを自動的にクリーンアップするための権限が、ホスト接続に付与されます。詳しくは、「Azure host connections」を参照してください。

［完全な構成］を使用して、カタログのイメージ更新状態を監視できるようになりました。新しい列［イメージを更新］を使用して、非永続マシンカタログのイメージ更新状態を監視できるようになりました。この列は、カタログのイメージが 完全に更新されている（Fully updated）か、部分的に更新されている（Partially updated）か、更新が保留中である（Pending update）かを示します。

［マシンカタログ］テーブルに列を表示するには、次の手順に従います：

1. ［マシンカタログ］ノードで、操作バーの［表示する列］アイコンを選択します。
2. ［マシンカタログ］**>** ［**Image Status**］を選択します。
3. ［**Save**］をクリックします。

［イメージを更新］列を表示すると、コンソールのパフォーマンスが低下する可能性があります。そのため、この列は必要な場合にのみ表示することをお勧めします。

GCP 管理トラフィックのための安全な環境。この機能を使用することで、自身の Google Cloud プロジェクトには、プライベート Google アクセスのみを許可できるようになりました。この実装により、機密データを処理するためのセキュリティが強化されます。これを行うには、Citrix Cloud 環境の場合は`CustomProperties`に`ProxyHypervisorTrafficThroughConnector`を追加します。プライベートワーカープールを使用する場合は、`CustomProperties`に`UsePrivateWorkerPool`を追加します。詳しくは、「GCP 管理トラフィックのための安全な環境の作成」を参照してください。

2023 年 **7** 月

新機能と機能強化

Azure 上の孤立したリソースの一覧を取得できるようになりました。MCS で作成されたのに、MCS で使用されなくなった孤立したリソースの一覧を Azure 環境で取得できるようになりました。この機能は、余分なコストを回避するのに役立ちます。詳しくは、「孤立したリソースの一覧の取得」を参照してください。

完全な構成を使用した永続的なマルチセッションマシンの作成をサポート。マルチセッションマシンのカタログ作成時に、それらを永続化するかどうかを指定できるようになりました。永続的なマルチセッションマシンの場合、ユーザーがデスクトップに加えた変更は保存され、すべての承認されたユーザーがアクセスできることに注意してください。詳しくは、「マシンカタログの作成」を参照してください。

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

- イメージ名
- イメージ ID
- イメージタグ

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

Azure AD デバイスの削除をサポート。この機能を使用すると、Cloud Device Administrator の役割をサービスプリンシパルに割り当て、ホスト接続のカスタムプロパティを変更することで、古い Azure AD デバイスを一貫して削除できます。Azure の古い AD デバイスを削除しない場合、対応する非永続的な仮想マシンは、Azure AD ポータルから手動で削除するまで初期化状態のままになります。詳しくは、「Azure Active Directory 参加済みカタログの作成」を参照してください。

AWS 環境でマシンプロファイルをサポート。Machine Creation Services（MCS）を使用して AWS でマシンをプロビジョニングするためのカタログを作成する場合、マシンプロファイルを使用して、EC2 インスタンス（仮想マシン）からハードウェアプロパティをキャプチャしたり、テンプレートバージョンを起動して、プロビジョニングされたマシンに適用したりできるようになりました。キャプチャされるプロパティには、たとえば、EBS ボリュームプロパティ、インスタンスの種類、EBS の最適化、およびその他のサポートされている AWS 構成が含まれます。カタログを編集する場合、別の仮想マシンまたは起動テンプレートを提供することで、プロビジョニングされたマシンのマシンプロファイルを変更できます。詳しくは、「マシンプロファイルを使用してカタログを作成する」を参照してください。

検索結果のエクスポート制限が **10,000** 件から **30,000** 件に拡張されました。検索結果のエクスポート制限を拡張しました。以前は 10,000 件に制限されていましたが、最大 30,000 件を CSV ファイルにエクスポートできるようになりました。詳しくは、「検索結果を CSV ファイルにエクスポートする」を参照してください。

イメージの更新オプション。マシンカタログのマスターイメージを選択するときに、右上の ［更新］オプションを使用して最新のマスターイメージ一覧をすばやく取得できるようになりました。［更新］オプションは AWS カタログでは使用できないことに注意してください。さらに、Azure カタログのマシンプロファイルとホストグループに対して［更新］オプションを使用できます。

2023 年 6 月

新機能と機能強化

GCP でマシンプロファイル入力からのカスタムプロパティの取得をサポート。以前の GCP 環境では、マシンプロファイル入力を使用して MCS マシンカタログを作成するときに、カスタムプロパティを明示的に指定する必要がありました。このため、追加の作業が必要でした。この機能を使用すると、明示的に定義せずに次のカスタムプロパティを取得できるようになりました:

- ServiceOffering
- CryptoKeyId
- CatalogZones
- Storage

New-ProvSchemeおよびSet-ProvSchemeコマンドを実行し、カスタムプロパティを明示的に指定しない場合、プロパティの値はマシンプロファイル入力から取得されます。

たとえば、New-ProvSchemeコマンドでServiceOfferingを指定しない限り、New-ProvScheme -MachineProfileはマシンプロファイルのマシンの種類をプロビジョニングスキームのServiceOfferingプロパティに書き込みます。Set-ProvVMSchemeを 2 回実行すると、最新のコマンドが有効になります。

AWS 環境のタグを削除。以前は、ForgetVMパラメーターを指定したRemove-ProvVMおよびRemove-ProvScheme PowerShell コマンドは、仮想マシンとマシンカタログを Citrix データベースから削除していました。ただし、このコマンドはタグを削除しませんでした。すべてのリソースで完全に削除されていない仮想マシンとマシンカタログを、個別に管理する必要がありました。この機能では、以下を使用できます:

- Remove-ProvVMをForgetVMパラメーターとともに使用して、マシンカタログの単一の仮想マシンまたは仮想マシンの一覧から仮想マシンとタグを削除します。
- Remove-ProvSchemeをForgetVMパラメーターとともに使用して、Citrix データベースからマシンカタログを削除し、マシンカタログからタグを削除します。

この実装は次の点で役立ちます:

- 漏えいしたリソースを特定する
- 不要なリソースの維持にかかる追加コストを削減する

この機能は、永続的な仮想マシンにのみ適用されます。詳しくは、「タグの削除」を参照してください。

MCS マシンカタログに関連するエラーと警告の履歴を取得する機能。以前は、マシンカタログに関連する最新の警告とエラーのみを取得できました。この機能を使用すると、MCS マシンカタログの警告とエラーの履歴の一覧を取得できるようになります。この一覧は、MCS マシンカタログの問題を把握して修正するために役立ちます。

詳しくは、「カタログに関連した警告とエラーの取得」を参照してください。

Google Cloud における **Citrix** のパフォーマンス向上と容量の拡大。Citrix は、単一の Google Cloud プロジェクトで最大 3,000 の VDA を含むカタログをサポートできるようになりました。この更新により、プロビジョニングと電源管理操作の両方のパフォーマンスが向上しました。

Google Cloud および **AWS** 環境で、**MCS** で作成されたマシンカタログ内の永続的な **VM** の **OS** ディスクをリセットする機能。PowerShell コマンドReset-ProvVMDiskを使用して、MCS で作成されたマシンカタログ内の永続的な VM の OS ディスクをリセットできるようになりました。この機能は、OS ディスクをリセットするプロセスを自動化します。たとえば、MCS を使用して作成された永続的な開発デスクトップカタログの初期状態に VM をリセットするのに役立ちます。現在この機能は、AWS、Azure、Citrix Hypervisor、Google Cloud、VMware 仮想

化環境に適用できます。PowerShell コマンドを使用して OS ディスクをリセットする方法について詳しくは、「OS ディスクのリセット」を参照してください。

GCP の既存のカタログおよび既存の **VM** でディスク関連のカスタムプロパティの変更をサポート。以前は、GCP 環境では、MCS マシンカタログの作成時にのみカスタムプロパティを追加できました。この機能を使用すると、既存のカタログおよびカタログの既存の VM で次のディスク関連のカスタムプロパティを変更できるようになります:

- `PersistOSDisk`
- `PersistWBC`
- `StorageType`
- `IdentityDiskStorageType`
- `WbcDiskStorageType`

この実装により、カタログを作成した後でも、異なるディスクに対して異なるストレージの種類を選択できるため、さまざまなストレージの種類を使用することと価格のバランスを取ることができます。詳しくは、「既存のカタログのディスクに関連したカスタムプロパティを変更する」を参照してください。

動的セッションタイムアウトのサポートが **VDA** バージョン **2203 LTSR CU3** 以降にまで拡張されました。シングルセッション OS デリバリーグループの場合、この機能は VDA のバージョン 2206 CR 以降、または 2203 LTSR CU3 以降に適用されるようになりました。詳しくは、「動的セッションタイムアウト」を参照してください。

[完全な構成] でのホスト接続の作成エクスペリエンスが向上しました。リソースの場所を選択すると、[接続の種類:] ボックスに、Citrix がサポートするすべてのハイパーバイザーとクラウドサービスが表示されます。これらのハイパーバイザーとクラウドサービスの可用性は以下によって異なります:

- アクセス可能な Cloud Connetor がリソースの場所にない場合は、コネクタを使用しない展開をサポートするハイパーバイザーとクラウドサービスだけが利用可能です。
- アクセス可能な Cloud Connetor がリソースの場所にある場合は、それらの Connetor にプラグインが正しくインストールされているハイパーバイザーとクラウドサービスだけが利用可能です。

詳しくは、「接続の作成と管理」を参照してください。

VDA アップグレードにより、追加コンポーネントが選択できるようになりました。VDA のアップグレード中に、アップグレードまたはインストールする追加コンポーネントを選択できるようになりました。詳しくは、「VDA の自動アップグレードの構成」を参照してください。

> 重要:
>
> 追加コンポーネント機能を使用するには、VDA Upgrade Agent がバージョン 7.34 以降であることを確認してください。このバージョンは、VDA インストーラーバージョン 2206 以降に含まれています。

[完全な構成] では、マシンプロファイルに基づいて **Azure** マシンの特定の設定が事前構成されるようになりました。Azure VM をプロビジョニングする場合、[完全な構成] では、選択したマシンプロファイルに基づいて次の設定が事前構成されるようになりました:

- ホストグループ

- ディスク暗号化セット
- アベイラビリティゾーン
- ライセンスの種類

AWS インスタンスの休止がサポートされるようになりました。これで、AWS インスタンスを起動し、希望どおりに設定して、休止することができます。休止プロセスは、インスタンスの状態がプライベート IP アドレスおよび Elastic IP アドレスとともにメモリ内に保存されるので、中断したところから正確に再開できます。休止できる VM の作成について詳しくは、「インスタンスの休止」を参照してください。

AWS の調整の最適化がサポートされるようになりました。AWS を調整する必要もなく、AWS カタログで多数のマシンの電源をオンまたはオフにできるようになりました。調整の問題は、AWS に送信された要求の数が、サーバーが処理できる要求の数を超えると発生します。この機能は、マシンの電源を一括でオンまたはオフにするための AWS 呼び出しの数を減らすことで効率を高めます。また、永続カタログ内のマシンの電源のオン/オフにかかる時間も大幅に短縮されます。

Azure 管理トラフィックのための安全な環境。以前は、パブリックインターネットを利用して、Azure エンドポイントが環境内のリソースとやり取りできるようにしていました。このため、パブリックインターネットにアクセスするので、セキュリティ上の懸念が生じていました。それに対し、この機能を使用すると、MCS により、Citrix Cloud Connector を介してネットワークトラフィックを環境内でルーティングできるようになります。これにより、Azure で管理されるすべてのトラフィックが独自の環境から発生するようになるので、環境が安全になります。これを行うには、`CustomProperties`に`ProxyHypervisorTrafficThroughConnector`を追加します。詳しくは、「Azure 管理トラフィックのための安全な環境の作成」を参照してください。

カスタムプロパティを設定した後、Azure Managed Disks へのプライベートディスクアクセスを許可する Azure ポリシーを構成できます。

Azure Monitor エージェントを使用したカタログ **VM** のプロビジョニングがサポートされるようになりました。Azure Monitor エージェント（AMA）は監視データを収集し、Azure Monitor に配信します。この機能を使用すると、MCS マシンカタログ VM（永続的および非永続的）をプロビジョニングし、AMA を拡張機能としてインストールできます。この実装により、監視データ内の VM を一意に識別することで監視が可能になります。AMA について詳しくは、「Azure Monitor エージェントの概要」を参照してください。

現在、MCS はこの機能でマシンプロファイルワークフローのみをサポートします。AMA を有効にしてマシンカタログ VM をプロビジョニングする方法について詳しくは、「［Azure Monitor エージェントがインストールされたカタログ VM をプロビジョニングする］」を参照してください。

MCS カタログの再起動スケジュールの有効化。以前は、次の再起動を待つか、すべての VM の即時再起動をトリガーすることで、イメージの更新をスケジュール設定していました。今回の機能を使用すると、希望の日時にトリガーされる、カタログの 1 回限りの再起動スケジュールを作成することで、MCS イメージの更新を簡単にすることができます。再起動スケジュールを作成するには、`BrokerCatalogRebootSchedule`コマンドを使用します。詳しくは、「マスターイメージの変更」を参照してください。

期限切れのクライアントシークレットを **Azure** クイック展開で管理できます。Azure クイック展開では、クライアントシークレットの有効期限が切れたことを通知で知ることができるようになったので、シークレット を簡単に更新

して、Azure リソースへの継続的なアクセスを実現できるようになりました。詳しくは、「有効期限が切れたクライアントのシークレットの更新」を参照してください。

2023 年 5 月

新機能と機能強化

検索機能の強化。この機能により、フィルターのビジュアルと操作性が向上し、より優れた検索エクスペリエンスが実現します。詳しくは、「［完全な構成］管理インターフェイスでの［検索］の使用」を参照してください。

ユーザーレイヤーにリダイレクトされないディレクトリパスを定義できる新しいユーザー除外ポリシー。ユーザーの除外はユーザー個人設定レイヤー（UPL）に適用されますが、セッションホストには適用されません。Logoff.txt に、すべてのアクティブなユーザーの除外が含まれるようになりました。詳しくは、「ユーザー個人設定レイヤー」を参照してください。

MCS マシンカタログに追加された新しい **VM** のハードウェアバージョンの更新をサポート。VMware 環境で、マシンプロファイルをソースとして使用して、既存の MCS マシンカタログに新しく追加された VM のハードウェアバージョンを更新できるようになりました。カタログに追加された VM のハードウェアバージョンを更新するために、新しいマシンカタログを作成する必要はありません。この機能を使用するには、マシンプロファイルワークフローを使用する必要があります。

AWS VM インスタンスのフィルタリングのサポート。以前は、AWS VM インスタンスをマシンプロファイルの入力に使用して MCS マシンカタログを作成すると、無効なマシンプロファイルの入力が原因でカタログが正しく作成されなかったり、正しく機能しなかったりすることがありました。この機能を使用することで、有効なマシンプロファイル VM として使用できる AWS VM インスタンスを一覧表示できるようになりました。これを行うには、`Get-HypInventoryItem`コマンドを使用します。詳しくは、「VM インスタンスのフィルタリング」を参照してください。

Azure 環境で、非マシンプロファイルベースのマシンカタログからマシンプロファイルベースのマシンカタログへの変換をサポート。Azure 環境で、VM またはテンプレートスペックをマシンプロファイルの入力に使用して、非マシンプロファイルベースのマシンカタログをマシンプロファイルベースのマシンカタログに変換できるようになりました。既存の VM とカタログに追加された新しい VM は、明示的なカスタムプロパティによって上書きされない限り、マシンプロファイルからプロパティ値を取得します。詳しくは、「非マシンプロファイルベースのマシンカタログをマシンプロファイルベースのマシンカタログに変換する」を参照してください。

Azure 環境で管理対象ディスクの二重暗号化をサポート。Azure 環境で、二重暗号化を使用してマシンカタログを作成できるようになりました。二重暗号化とは、プラットフォーム側の暗号化（デフォルト）と顧客管理の暗号化（CMEK）です。したがって、暗号化アルゴリズム、実装、またはキーの侵害に関するリスクを懸念している、セキュリティに非常に敏感なお客様は、この二重暗号化を選択できます。永続的 OS ディスクとデータディスク、スナップショット、イメージはすべて二重暗号化により保存時に暗号化されます。詳しくは、「管理対象ディスクの二重暗号化」を参照してください。

VMware でマシンプロファイルをサポート。VMware 環境で、マシンプロファイルを使用して MCS マシンカタログを作成できるようになりました。マシンプロファイルの入力のソースは VMware テンプレートです。マシンプロ

ファイルは、VMware テンプレートからハードウェアプロパティを取得し、カタログ内の新しくプロビジョニングされた VM に適用します。詳しくは、「マシンプロファイルを使用してマシンカタログを作成する」を参照してください。

Azure および **Citrix Hypervisor** の **MCS** で作成されたマシンカタログ内で、永続的な **VM** の **OS** ディスクをリセットする機能。PowerShell コマンド`Reset-ProvVMDisk`を使用して、MCS で作成されたマシンカタログ内の永続的な VM の OS ディスクをリセットできるようになりました。この機能は、OS ディスクをリセットするプロセスを自動化します。たとえば、MCS を使用して作成された永続的な開発デスクトップカタログの初期状態に VM をリセットするのに役立ちます。現在、この機能は Azure、Citrix Hypervisor、VMware 仮想化環境に適用できます。PowerShell コマンドを使用して OS ディスクをリセットする方法について詳しくは、「OS ディスクのリセット」を参照してください。

ホスト接続の作成エクスペリエンスが向上。ホスト接続の作成中に次の情報を取得できるようになりました:

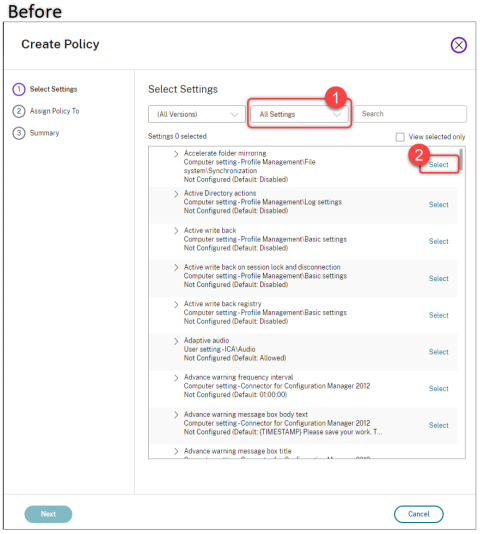
- Citrix がサポートするすべてのハイパーバイザープラグインの一覧（サードパーティのプラグインを含む）
- ハイパーバイザープラグインの可用性。可用性のステータスが false の場合は、Cloud Connector がインストールされていない可能性があります。

この機能は、リソースの場所を正しく設定し、ホスト接続を作成するのに役立ちます。詳しくは、次を参照してください。「手順 1：接続」。

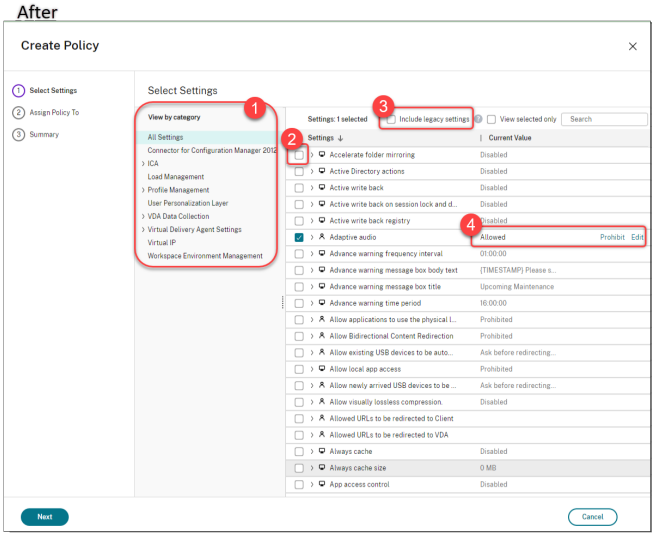
ポリシーノードのユーザーエクスペリエンスが向上。ユーザーエクスペリエンスを向上させ、ポリシー管理をより効率的にするために、［完全な構成］**>**［ポリシー］ノードに対して次のような変更を加えました:

- ［ポリシーの作成］および ［テンプレートの作成］の操作の新しい UI デザイン:
  - ポリシー設定の展開可能なフォルダービュー。［設定項目の選択］ページでは、展開可能なツリービューにすべての設定がカテゴリ別に表示され、設定を見つけやすくなります。
  - 設定を選択するには、［選択］ボタンを使用する代わりに、チェックボックスをクリックするだけです。
  - 従来の設定はデフォルトで非表示になっており、最も関連性の高い設定のみが表示されます。従来の設定が必要な場合は、［従来の設定を含める］を選択します。
  - ブール設定の横にアクションボタンが追加され、設定一覧で値を直接変更できるようになりました。

Before

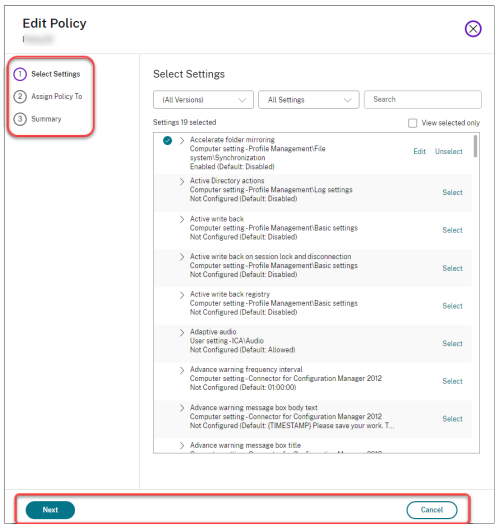


After

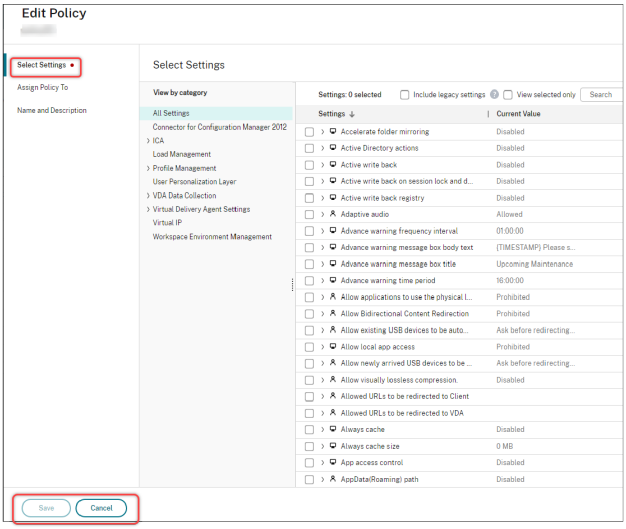


- [ポリシーの編集] 操作の新しい UI デザイン:
  - ナビゲーションメニューが番号なしの一覧に更新されました。一覧内の各項目のページに [保存] ボタンが追加されました。この新しいデザインでは、ナビゲーションメニュー内のすべての項目間を移動しなくても、項目に加えた変更を保存できます。これらの機能向上により、ポリシー管理がより効率的になり、合理化されます。
  - ナビゲーション項目の横に表示された赤い丸は、設定エラーがあることを示します。

Before



After



- ドラッグしてポリシーの優先順位を変更します。優先順位一覧で、ポリシーを目的の位置にドラッグすることで、ポリシーの優先順位を変更できるようになりました。

AutoScale によるユーザーの強制ログオフを無効にするオプションが追加されました。新しいオプション [ユーザーを強制的にログオフしない（通知なし）] が、[**Autoscale** の管理] > [ユーザーログオフ通知] ページで利用できるようになりました。このオプションを選択すると、Autoscale はユーザーにドレイン状態のマシンからのログオフを強制したり、ログオフして別のマシンにログオンするようにユーザーに通知したりしません。詳しくは、「ユーザー

ログオフ通知」を参照してください。

Windows 365 クラウド **PC** を再起動する機能。Citrix DaaS を使用して、Windows 365 クラウド PCを再起動できるようになりました。

セッションの詳細への追加。［完全な構成］**>**［検索］**>**［セッション］でセッションを表示すると、セッションビュー（下ペイン）に表示されるセッションの詳細内容が追加され、クライアントの問題を特定してトラブルシューティングするために役立つようになりました：

- 再接続時間。セッションが切断された後に再接続された時間。
- クライアントプラットフォーム。セッションの起動に使用されるプラットフォーム。
- クライアントバージョン。セッションの起動に使用されるクライアントプラットフォームのバージョン。
- リモートホスト **IP**。Citrix Workspace がホストされているリモートホストの IP アドレス。

VM の **Azure AD** セキュリティグループの名前変更をサポート。Citrix DaaS を通じて Azure AD セキュリティグループに追加された VM の場合、［完全な構成］**>**［マシンカタログの編集］を使用してセキュリティグループの名前を変更できるようになりました。名前の変更は、変更を保存した後に行われます。

マシンアカウントのデフォルトのドメイン選択。カタログを作成すると、リソース（接続）が存在するドメインがデフォルトでマシンアカウントに選択されます。

仮想マシンが参加する **Azure AD** 割り当て済みセキュリティグループを表示する機能。［完全な構成］では、Azure AD 参加済み仮想マシンを作成するときに、［割り当て済みのセキュリティグループをメンバーとして参加させる］オプションが利用可能になりました。これによって、仮想マシンが存在する Azure AD セキュリティグループを割り当て済みセキュリティグループに追加できるようになりました。詳しくは、「Azure Resource Manager イメージを使用してマシンカタログを作成する」を参照してください。

接続用のネットワーク変更のサポート。［完全な構成］で、接続用のネットワークを変更できるようになりました。ネットワークが使用中の場合、接続からネットワークの関連付けを解除することはできません。詳しくは、「ネットワークの編集」を参照してください。

Azure 環境でタグを削除する機能。以前は、`ForgetVM`パラメーターを指定した`Remove-ProvVM`および`Remove-ProvScheme` PowerShell コマンドは、仮想マシンとマシンカタログを Citrix データベースから削除していました。ただし、このコマンドはリソースからタグを削除しませんでした。すべてのリソースで完全に削除されていない仮想マシンとマシンカタログを、個別に管理する必要がありました。この機能では、以下を使用できます：

- `Remove-ProvVM`を`ForgetVM`パラメーターとともに使用して、リソースから作成された仮想マシンとタグをマシンカタログの単一の仮想マシンから、または仮想マシンの一覧から削除します。
- `Remove-ProvScheme`を`ForgetVM`パラメーターとともに使用して、Citrix データベースから単一のマシンカタログを削除し、マシンカタログ全体からリソースで作成されたタグを削除します。

この実装は、MCS によって作成されたものの、MCS で使用されなくなった孤立したリソースを識別するのに役立ちます。

この機能は、永続的な仮想マシンにのみ適用されます。詳しくは、「タグの削除」を参照してください。

障害が発生したマシンアラート。Director のプロアクティブな通知とアラート機能が強化され、デリバリーグループ内の障害が発生したマシンの割合に基づく新しいアラート機能である［障害が発生したマシン（%）］を使用できます。新しいアラート条件を使用すると、アラートのしきい値を、デリバリーグループ内の障害が発生したマシンの割合で構成できます。詳しくは、アラートについての記事の「障害が発生したマシン」セクションを参照してください。

2023 年 4 月

新機能と機能強化

Image Portability Service の **Citrix Provisioning** を使用して、特定のクラウドプラットフォームで公開します。Image Portability Service を使用して AWS、Azure、Google Cloud で公開するための特定のワークフローが利用可能になりました。さらに、Azure とネットワークに必要な権限が更新されました。詳しくは、「ワークロードのパブリッククラウドへの移行」を参照してください。

マシンがメンテナンスモードになっている理由を特定するためのサポート。以前は、PowerShell はマシンがメンテナンスモードになった理由を特定するための唯一の選択肢でした。［完全な構成］でこれを実現できるようになりました：

1. ［検索］ を使用してマシンを検索します。
2. 下部ペインの ［詳細］タブで ［メンテナンスの理由］を確認します。または、［メンテナンスモード］列にカーソルを合わせます。表示される情報には、次のようなものがあります：

- 管理者による：管理者がメンテナンスモードにしました。
- 登録失敗回数の上限：マシンが許可された登録試行回数の最大数を超えたため、メンテナンスモードに移行しました。

また、メンテナンスの理由フィルターが使用できるようになりました。これを使用して、ターゲットマシンを特定できます。

この機能は、メンテナンスモードでのマシンの問題のトラブルシューティングを管理者が行う場合に役立ちます。

変数を使用して、ログオフするまでの残り時間をユーザーに通知します。ユーザーのログオフを強制する場合、%s%または%m%を変数として使用して、通知メッセージで指定された時間を示すことができるようになりました。時間を秒単位で表すには、%s%を使用します。時間を分単位で表すには、%m%を使用します。詳しくは、「ユーザーログオフ通知」を参照してください。

ストレージの種類の変更に失敗したときの電源投入時動作のカスタマイズをサポート。電源をオンにした際に、Azure での障害が原因で、管理対象ディスクのストレージの種類が目的の種類に変更されないことがあります。以前は、このような場合に VM はオフのままになり、エラーメッセージが送信されていました。この機能を使用すると、設定した種類にストレージを復元できない場合でも、VM の電源をオンにするか、VM の電源をオフのままにするかを選択できます。詳しくは、「ストレージの種類の変更に失敗したときの電源投入時の動作をカスタマイズする」を参照してください。

MAK ライセンス認証のサポート。マルチライセンス認証キー（MAK）によってアクティブ化された VM を使用して、永続的および非永続的なマシンカタログをプロビジョニングできるようになりました。この機能により、MCS はプロ

ビジョニングされた VM とも通信できるようになりました。この実装は、アクティベーションカウントを消費せずに Windows システムをアクティブ化するのに役立ちます。詳しくは、「ボリュームライセンス認証」を参照してください。

ホストでの **Azure** ディスク暗号化のサポート。この機能により、ホスト機能での暗号化を使用して、MCS マシンカタログを作成できるようになりました。現在、MCS はこの機能でマシンプロファイルワークフローのみをサポートします。VM またはテンプレートスペックをマシンプロファイルの入力として使用できます。詳しくは、「ホストでの Azure ディスク暗号化」を参照してください。

この種類の暗号化では、VM をホストするサーバーがデータを暗号化し、暗号化されたデータが Azure Storage サーバーを通過します。つまり、この暗号化方法はデータをエンドツーエンドで暗号化します。詳しくは、「ホストでの暗号化 - ご利用の VM データのエンドツーエンド暗号化」を参照してください。

マシンプロファイルの入力用の **GCP** インスタンステンプレートのサポート。この機能により、GCP インスタンステンプレートをマシンプロファイルの入力として選択できるようになりました。インスタンステンプレートは GCP のライトウェイトリソースであるため、費用対効果が非常に高くなります。これを行うには、PowerShell コマンドを使用します。PowerShell コマンドを使用して、GCP インスタンステンプレートでマシンカタログを作成および更新する方法について詳しくは、「インスタンステンプレートとしてマシンプロファイルを使用してマシンカタログを作成する」を参照してください。

Azure AD 動的セキュリティグループ名の変更のサポート。Azure Portal から Azure AD 動的セキュリティグループ名を変更または削除できます。このアクションにより、Azure AD の動的セキュリティグループ名が、マシンカタログに関連付けられている動的セキュリティグループと同期しなくなる可能性があります。この機能では、マシンカタログに関連付けられている Azure AD 動的セキュリティグループ名を変更できるようになりました。

これによって、Azure AD ID プールオブジェクトに格納されている Azure AD 動的セキュリティグループ情報が、Azure Portal に格納されている情報と一致するようになります。詳しくは、「Azure AD 動的セキュリティグループ名の変更」を参照してください。

GCP で必要な権限を追加。以下を実行するために必要な権限が追加されました:

- ホスト接続の作成
- VM の電源管理
- カタログのプロビジョニング

詳しくは、「GCP の権限について」を参照してください。

資格情報の処理。セキュリティ強化のため、デフォルトでは、VDA と同じドメインに属していないユーザーの資格情報はクラウドに転送されません。次の条件がすべて満たされると、ログインの試みは失敗します:

- ユーザーが VDA とは異なるドメインに存在する
- ドメイン間に信頼関係が存在しない
- StoreFront が VDA と同じドメインにインストールされている

以前は、これらの条件下で、ユーザーは StoreFront に認証できませんでした。そのため、Cloud Connector はユーザー資格情報をクラウドに転送して、認証要求をそのユーザーの正しい宛先にルーテ

ィングしました。この動作は、必要に応じて構成できます。詳しくは、DaaS PowerShell SDK のSet-BrokersiteのCredentialForwardingToCloudAllowedパラメーターを参照してください。

2023 年 3 月

新機能と機能強化

管理者の役割とスコープの構成のサポート。Citrix Cloud は、管理者のアクセスを構成する場合に、高度な柔軟性とカスタマイズをサポートするようになりました。以前は、定義済みの役割とスコープのペアしか選択できませんでした。この機能強化により、役割を選択して、選択したスコープと組み合わせることができます。

詳しくは、「管理者のカスタムアクセス権の構成」を参照してください。

既存の割り当て済みセキュリティグループの下に動的セキュリティグループを作成するためのサポート。以前は、マシンカタログの Azure AD 動的セキュリティグループを作成できました。この機能では、既存の Azure AD 割り当て済みセキュリティグループの下に Azure AD 動的セキュリティグループを追加することもできます。以下の操作を実行できます:

- セキュリティグループ情報を取得します。
- オンプレミスの AD サーバーから同期されたすべての既存の Azure AD 割り当て済みセキュリティグループ、または Azure AD の役割を割り当てることができる割り当て済みセキュリティグループを取得します。
- すべての Azure AD 動的セキュリティグループを取得します。
- Azure AD 動的セキュリティグループを Azure AD 割り当て済みグループのメンバーとして追加します。
- Azure AD 動的セキュリティグループがマシンカタログとともに削除されるときに、Azure AD 動的セキュリティグループと Azure AD 割り当て済みセキュリティグループの間のメンバーシップを削除します。

詳しくは、「既存の Azure AD 割り当て済みセキュリティグループの下に Azure AD 動的セキュリティグループを作成する」を参照してください。

Azure AD 参加済み仮想マシンの **Azure AD** 動的セキュリティグループのサポート。Citrix は、MCS マシンカタログの作成中に、カタログの動的セキュリティグループをサポートするようになりました。動的セキュリティグループの規則では、マシンカタログの名前付けスキームに基づいて、カタログ内の仮想マシンを動的セキュリティグループに配置します。これは、Azure Active Directory（Azure AD）によって仮想マシンを管理する場合に役立ちます。これは、条件付きアクセスポリシーを適用したり、Azure AD 動的セキュリティグループで仮想マシンをフィルター処理して Intune からアプリを配布したりする場合にも役立ちます。カタログを削除すると、動的セキュリティグループも削除されます。詳しくは、「Azure Active Directory 動的セキュリティグループ」を参照してください。

動的セキュリティグループを使用するためのライセンス要件について詳しくは、Microsoft ドキュメント「Azure Active Directory で動的グループを作成または更新する」を参照してください。

［完全な構成］による **Azure AD** セキュリティグループへの仮想マシンの追加のサポート。Azure AD 参加済み仮想マシンを作成するときに、オプション ［**Azure AD** セキュリティグループ］を使用できるようになりました。このオプションを使用すると、名前付けスキームに基づいて仮想マシンを Azure AD セキュリティグループに追加できます。詳しくは、「Microsoft Azure カタログの作成」を参照してください。

Azure 環境での仮想マシンのシャットダウン時に、ストレージの種類のダウングレードをサポート。Azure 環境で、VM のシャットダウン時に、既存の VM のストレージの種類を下位レベルに変更することでストレージコストを節約できるようになりました。これを行うには、カスタムプロパティの StorageTypeAtShutdown を使用します。詳しくは、「仮想マシンのシャットダウン時にストレージの種類をダウングレードする」を参照してください。

仮想マシン作成中のセキュリティ識別子追加のサポート。以前は、プロビジョニングスキームで指定した構成で新しい仮想マシンを作成するときに、セキュリティ識別子（ADAccountSid）をNewProvVMコマンドに追加できませんでした。今回の機能により、ADAccountSidパラメーターを追加して、新しい仮想マシンの作成時にマシンを一意に識別できるようになりました。詳しくは、「仮想マシン作成時の SID の追加」を参照してください。

MCS カタログに関連する警告を取得する機能。以前は、マシンカタログに問題があることを示す情報は取得されませんでした。今回の機能により、MCS カタログの問題を把握し、それらの問題を修正するための警告を受け取ることができるようになりました。

警告は、エラーとは異なり、開始されたプロビジョニングタスクが失敗する原因にはなりません。

警告を取得するには、PowerShell コマンドを使用します。詳しくは、「カタログに関連した警告の取得」を参照してください。

接続用の共有テナント。接続のサブスクリプションと Azure Compute Gallery を共有しているテナントとサブスクリプションを追加できるようになりました。その結果、カタログを作成または更新するときに、それらのテナントおよびサブスクリプションから共有イメージを選択できます。詳しくは、「接続の設定の編集」を参照してください。

Azure カタログで **OS** の種類の変更に関するサポートの廃止。カタログイメージを変更すると、使用中のイメージと同じ OS の種類のイメージのみが表示されます。この機能強化により、Citrix DaaS は、Azure カタログの OS の種類に関するカタログ作成後の変更（Windows OS から Linux や、逆方向への変更など）をサポートしなくなりました。

2023 年 2 月

新機能と機能強化

異なる **Azure** テナント間でのイメージ共有のサポート。以前は、Azure 環境で Azure Compute Gallery を使用して、共有サブスクリプションでのみイメージを共有できました。この機能により、別のテナントの別の共有サブスクリプションに属する Azure Compute Gallery のイメージを選択して、MCS カタログを作成および更新できるようになりました。詳細については、「Azure テナント間でのイメージ共有」を参照してください。

ポリシーのモデル作成。ポリシーのモデル作成機能の一般提供が開始されました。計画およびテストのためにポリシーをシミュレーションできます。詳しくは、「ポリシーのモデル作成ウィザードの使用」を参照してください。

プレビュー機能をオンまたはオフにする機能。［完全な構成］>［ホーム］で、フルアクセス権を持つ Citrix Cloud 管理者は、Citrix に連絡することなくプレビュー機能をオンまたはオフにすることができます。詳しくは、「［完全な構成］インターフェイスのホームページ」を参照してください。

セッション診断をユーザー名で検索。この機能により、トランザクション ID がない場合に、ユーザー名から始まるセッション起動診断を使用できるようになります。この機能は、エンドユーザーがトランザクション ID をキャプチャし

ていない場合に、ヘルプデスク管理者が失敗したセッションをトリアージするのに特に役立ちます。
ユーザー名を検索し、ユーザーが過去 48 時間以内に起動を試みて失敗したセッションの一覧からトリアージするセッションを選択できます。セッション起動診断ページに、失敗したセッションの詳細が表示されます。障害が発生した正確なコンポーネントとステージが一覧表示されます。詳しくは、「セッション起動診断」を参照してください。

Secure Private Access を使用したセキュアな **Web/SaaS** アプリの展開。［完全な構成］**>**［アプリケーション］**>**［アプリケーション］タブで、新しいオプションである ［**Web/SaaS** アプリケーションの追加］が操作バーで利用できるようになりました。このオプションによって、Secure Private Access を使用したセキュアな Web/SaaS アプリを展開できます。Citrix Secure Private Access は、リモートユーザーがゼロトラストアプローチを使用して Web、SaaS、およびクライアントサーバーベースのアプリにアクセスするための簡単で柔軟な方法を提供します。これにより、Web および SaaS アプリへのシングルサインオンが可能になり、ウォーターマークやコピー/貼り付けの制御、その他のセキュリティ機能など、詳細にセキュリティを制御できます。Citrix Secure Private Access を使用すると、すべての仮想化アプリと仮想化されていないアプリを 1 か所にまとめて、ユーザーのユーザーエクスペリエンスを向上させることができます。「Citrix Secure Private Access」を参照してください。

特定の期間のログコンテンツのフィルター処理。新しいオプション ［カスタム］が、［完全な構成］**>**［ログ］**>**［イベント］の期間一覧で使用できるようになりました。これを使用して、検索をフィルター処理するイベントの期間を指定します。詳しくは、「構成ログ」を参照してください。

Autoscale の更新。［**Autoscale** がタグ付けされたマシンの電源投入を開始するタイミングを制御する］をわかりやすいように更新しました。このオプションをオンにすると、Autoscale は、タグ付けされていないマシンに残った処理能力のパーセンテージに基づいて、タグ付けされたマシンの電源投入を開始するタイミングを制御できます。パーセンテージがしきい値を下回った場合（デフォルトは 10%）、Autoscale がタグ付けされたマシンの電源投入を開始します。パーセンテージがしきい値を超えると、Autoscale は電源オフモードになります。詳しくは、「タグ付けされたマシンの Autoscale（クラウドバースト）」を参照してください。

App Protection ポリシー。デリバリーグループの作成または編集時にアプリ保護を有効にできるようになりました。この機能は、クライアントセッションのキーロガー対策機能と画面キャプチャ防止機能を提供します。詳しくは、「デリバリーグループの作成」と「デリバリーグループの管理」を参照してください。

AMD GPU で利用可能なリアルタイム **GPU** 使用率。［監視］で AMD Radeon Instinct MI25 GPU および AMD EPYC 7V12（Rome）CPU の GPU 使用率を確認できるようになりました。［監視］はすでに NVIDIA Tesla M60 GPU をサポートしています。［GPU 使用率］では GPU、GPU メモリ、およびエンコーダーとデコーダーの使用率がグラフにパーセント値で表示され、マルチセッションおよびシングルセッション OS の VDA での GPU 関連の問題を解決できます。AMD GPU 使用率グラフは、64 ビット版 Windows および Citrix Virtual Apps and Desktops 7 2212 以降を実行している VDA でのみ使用できます。詳しくは、「GPU 使用率」を参照してください。

Azure での構成の更新のスケジュール設定のサポート。Azure 環境で、PowerShell コマンド`Schedule-ProvVMUpdate`を使用して、既存の MCS プロビジョニング済みマシンの構成の更新について、時間枠をスケジュール設定できるようになりました。スケジュールされた時間枠内で電源をオンまたは再起動すると、スケジュールされたプロビジョニングスキームの更新がマシンに適用されます。`Cancel-ProvVMUpdate`を使用して、スケジュールされた時刻の前に、構成の更新をキャンセルすることもできます。

スケジュール設定およびキャンセルできるのは、以下の構成の更新です：

- 単一または複数の VM
- カタログ全体

詳しくは、「構成の更新のスケジュール設定」を参照してください。

Google Cloud Marketplace から直接 **Citrix Ready** イメージを使用するためのサポート。Google Cloud Marketplace で Citrix 提供イメージを参照して選択することで、MCS カタログを作成できるようになりました。現在、MCS はこの機能でマシンプロファイルワークフローのみをサポートします。詳しくは、「Google Cloud Marketplace」を参照してください。

SCVMM ホスト接続でのホストグループ範囲の制限。以前は、SCVMM にホスト接続するには、管理者が最上位のホストグループを 1 つ構成する必要がありました。これは、管理者が単一の最上位ホストグループにあるすべてのホストグループ、クラスター、またはホストを表示できることを意味します。単一の SCVMM が異なるデータセンターの複数のクラスターを管理する大規模な環境では、この機能を使用して、管理者のホストグループのスコープを制限できるようになりました。これを行うには、Microsoft System Center Virtual Machine Manager（VMM）コンソールで、Delegated Admin の役割を使用して、管理者がアクセスする必要があるホストグループを選択します。詳しくは、「ハイパーバイザーのインストールおよび構成」を参照してください。

Azure でのゾーン冗長ストレージのサポート。以前は、MCS はローカル冗長ストレージのみを提供していました。この機能により、ゾーン冗長ストレージが Azure のオプションになり、使用する冗長の種類に応じてストレージの種類を選択できるようになりました。ゾーン冗長ストレージは複数のアベイラビリティゾーンにわたって Azure Managed Disks を複製するため、別のゾーンの冗長を利用して、ゾーンでの障害から回復できます。詳しくは、「ゾーン冗長ストレージの有効化」を参照してください。

2023 年 1 月

新機能と機能強化

仮想マシンのシャットダウン時にストレージディスクを標準 **HDD** にダウングレードするオプション。Azure カタログを作成または更新するときに、[ストレージコストの削減を有効にする] という新しいオプションを［ディスク設定］ページで使用できるようになりました。このオプションによって、VM のシャットダウン時にストレージディスクとライトバックキャッシュディスクを標準 HDD にダウングレードすることで、ストレージコストを削減できます。VM は、再起動時に元の設定に切り替わります。詳しくは、「Microsoft Azure カタログの作成」を参照してください。

［完全な構成］でのセッションローミングの構成をサポート。以前は、アプリケーションとデスクトップのセッションローミングを構成する場合、PowerShell が唯一の選択肢でした。これを ［完全な構成］で実行できるようになりました。詳しくは、「デリバリーグループの管理」を参照してください。

いくつかのアクションの名前を、実際の機能に合わせてより適切に変更しました。［完全な構成］**>**［マシンカタログ］および ［完全な構成］**>**［デリバリーグループ］で次のアクションの名前を変更しました。これらのアクションを実行するためのワークフローは変更されていません。

- ［マシンの更新］は ［マスターイメージの変更］に名前が変更されました
- ［マシン更新のロールバック］は ［マスターイメージのロールバック］に名前が変更されました

- ［カタログのアップグレード］は ［機能レベルの変更］に名前が変更されました
- ［デリバリーグループのアップグレード］は ［機能レベルの変更］に名前が変更されました
- ［カタログのアップグレードを元に戻す］は ［機能レベルの変更を元に戻す］に名前が変更されました
- ［デリバリーグループのアップグレードを元に戻す］は ［機能レベルの変更を元に戻す］に名前が変更されました

フォルダーを使用したアプリケーショングループの整理をサポート。簡単にアクセスできるように、階層分けされたフォルダーを作成してアプリケーショングループを整理できるようになりました。詳しくは、「フォルダーを使用したアプリケーショングループの整理」を参照してください。

デリバリーグループの制限の強化。以前は、デリバリーグループでアプリまたはデスクトップの使用を制限する場合、デリバリーグループで使用を許可されたユーザーとユーザーグループのみを指定できましたが、ブロックしたいユーザーやユーザーグループを追加することもできるようになりました。この機能強化は、許可リストにユーザーのグループを追加すると同時に、許可リスト内の一部のユーザーをブロックする場合に便利です。詳しくは、「デリバリーグループの作成」を参照してください。

［監視］から **Citrix Analytics for Performance** の［**Session Details**］ページへのアクセス。Citrix Analytics for Performance の［Session Details］ページが［監視］に統合されました。［監視］の［セッション］ページで［セッションタイムラインの表示］をクリックすると、［監視］内で Citrix Analytics for Performance の［Sessions Details］ページが表示されます。これを使用するには、有効な Citrix Analytics for Performance の使用権が必要です。［Sessions Details］は、Citrix Analytics for Performance の［Excellent］、［Fair］、または［Poor］に分類されたセッションで使用できます。

過去 3 日間のセッションのセッションエクスペリエンスの傾向と、エクスペリエンスの要因を確認できます。この情報は、ヘルプデスク管理者がセッションエクスペリエンス関連の問題のトラブルシューティング中に使用するライブデータ（［監視］で利用可能）を補足します。

詳しくは、「サイト分析」の記事を参照してください。

非永続な仮想マシンまたはそれらのマシンカタログを［完全な構成］で削除すると、非永続な仮想マシンはハイパーバイザーまたはクラウドサービスから削除されます。仮想マシンをハイパーバイザーまたはクラウドサービスに保持するオプションは、永続的な VM のみが利用できるようになりました。詳しくは、「マシンカタログの管理」を参照してください。

2022 年 **12** 月

新機能と機能強化

Azure AD 参加済みカタログ、**Hybrid Azure AD** 参加済みカタログ、および **Azure AD** 参加済みマスター **VM** を使用した **Microsoft Intune** 対応カタログの作成のサポート。Azure AD 参加済みカタログ、Hybrid Azure AD 参加済みカタログ、および Azure AD 参加済み、Hybrid Azure AD 参加済み、およびドメイン非参加のマスター VM を使用した Microsoft Intune 対応カタログを作成できるようになりました。Microsoft Intune でマスター VM を

管理する場合は、VDA バージョン 2212 以降を使用し、マシンカタログの作成または更新中にイメージの準備をスキップしないでください。

マシン ID について詳しくは、「Azure Active Directory 参加済み」、「Microsoft Intune」、および「Hybrid Azure Active Directory 参加済み」を参照してください。

ハイパーバイザーにアクセスせずに **VM** オブジェクトを削除する **MCS** のサポート。ハイパーバイザーにアクセスしなくても、MCS で VM オブジェクトを削除できるようになりました。VM またはプロビジョニングスキームを削除する場合、リソースが追跡または識別されないように、MCS はタグを削除する必要があります。以前は、ハイパーバイザーにアクセスできない場合、タグの削除の失敗は無視されていました。この機能により、`Remove-ProvVM`コマンドの使用中にハイパーバイザーにアクセスできない場合、タグの削除は失敗しますが、`PurgeDBOnly`オプションを使用することで、データベースから VM リソースオブジェクトを削除できます。詳しくは、「ハイパーバイザーにアクセスできないマシンの削除」を参照してください。

2022 年 11 月

新機能と機能強化

MSIX および **MSIX** アプリのアタッチアプリ配信のサポート。[完全な構成] > [アプリパッケージ] で、MSIX および MSIX アプリのアタッチパッケージアプリを Citrix Cloud にアップロードし、ユーザーに配信できるようになりました。詳しくは、「アプリパッケージ」を参照してください。

サポートされていない **VDA** バージョンと機能レベルのメッセージ。[完全な構成] インターフェイスで、サポートされていない VDA バージョンと機能レベルについて通知するようになりました。潜在的な問題を回避するには:

- サポートされていないバージョンの VDA を実行しているマシンでは、ユーザーはサポートされているバージョンにアップグレードするよう求められます。
- カタログまたはデリバリーグループの機能レベルがサポートされていない場合は、それをより高いレベルに設定するように求められます。

> ヒント:
>
> VDA は、Citrix Virtual Apps and Desktops の CR（最新リリース）ライフサイクル、および LTSR（長期サービスリリース）ライフサイクル の対象となります。

カタログ作成時にマスターイメージに注釈を付ける機能拡張。[完全な構成] で MCS カタログを作成するとき、マスターイメージに注釈を付けられるようになりました。詳しくは、「マスターイメージ」を参照してください。

[完全な構成] を使用したデスクトップ割り当てデータのエクスポートをサポート。シングルセッション OS デリバリーグループのデスクトップ割り当てを表示する場合、監査のために割り当てデータを CSV ファイルにエクスポートできるようになりました。これを行うには、[完全な構成] > [デリバリーグループ] でシングルセッション OS デリバリーグループを選択し、[デスクトップ] タブに移動して、タブの左上隅にある [エクスポート] をクリックします。

[すべてのアプリケーション] タブと [アプリケーションフォルダー] タブが **1** つに統合。[完全な構成] > [アプリケーション] で、[すべてのアプリケーション] タブと [アプリケーションフォルダー] タブが [アプリケーション] タ

ブに統合されました。この変更により、フォルダービュー管理のユーザーエクスペリエンスが［完全な構成］ノード全体で統一されます。

Azure 環境での仮想マシンのシャットダウン時に、ストレージの種類のダウングレードをサポート。Azure 環境では、仮想マシンのシャットダウン時に管理対象ディスクのストレージの種類をダウングレードすることで、ストレージコストを節約できるようになりました。これを行うには、カスタムプロパティ`StorageTypeAtShutdown`を使用します。仮想マシンをシャットダウンすると、ディスクのストレージの種類が（カスタムプロパティ`StorageTypeAtShutdown`で指定されたものに）ダウングレードされます。仮想マシンの電源をオンにすると、ストレージの種類が（カスタムプロパティ`StorageType`または`WBCDiskStorageType`で指定された）元のストレージの種類に戻ります。詳しくは、「仮想マシンのシャットダウン時にストレージの種類をダウングレードする」を参照してください。

［フィルター］ビューを更新。［監視］の［フィルター］ページが更新され、［保存済み］フィルターと［デフォルト］フィルターの一覧が別々に表示され、フィルターにアクセスしやすくなりました。［マシン］、［セッション］、［接続］、または［アプリケーションインスタンス］からビューを選択できます。その後、［保存済み］フィルターまたは［デフォルト］フィルターの一覧からフィルターを選択すると、フィルタリングされたデータの一覧を表示できます。ドロップダウンリストを使用して、フィルター基準を絞り込むか、既存の条件を編集できます。［保存済み］フィルターの一覧では、フィルターを保存できます。詳しくは、「フィルター」の記事を参照してください。

MCS で作成されたマシンカタログ内の永続的な **VM** の **OS** ディスクをリセットする機能。VMware 仮想環境で、PowerShell コマンド`Reset-ProvVMDisk`を使用して、MCS で作成されたマシンカタログ内の永続的な VM の OS ディスクをリセットできるようになりました。この機能は、OS ディスクをリセットするプロセスを自動化します。たとえば、MCS を使用して作成された永続的な開発デスクトップカタログの初期状態に VM をリセットするのに役立ちます。

PowerShell コマンドを使用して OS ディスクをリセットする方法について詳しくは、「OS ディスクのリセット」を参照してください。

Azure 環境で **MCS** プロビジョニングされたマシンのマシンプロファイルおよび追加のカスタムプロパティの更新をサポート。以前は、Azure 環境では`Request-ProvVMUpdate`を使用して、MCS でプロビジョニングされたマシンのカスタムプロパティ`ServiceOffering`を更新していました。今回、マシンプロファイルと以下のカスタムプロパティを更新できるようになりました：

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`
- `LicenseType`
- `DedicatedHostGroupId`
- `PersistWBC`
- `PersistOsDisk`
- `PersistVm`

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

GCP でのマシンプロファイルをサポート。Google Cloud Platform（GCP）環境で Machine Creation Services（MCS）を使用してマシンをプロビジョニングするためのカタログを作成する場合、マシンプロファイルを使用して、仮想マシンからハードウェアプロパティをキャプチャし、カタログで新しくプロビジョニングされた VM に適用できるようになりました。`MachineProfile`パラメーターが使用されていない場合、ハードウェアプロパティはマスターイメージ VM またはスナップショットからキャプチャされます。

マシンプロファイルは、Linux と Windows の両方のオペレーティングシステムで機能します。

マシンプロファイルを使用してマシンカタログを作成する方法については、「マシンプロファイルを使用してマシンカタログを作成する」を参照してください。

GCP 環境で、**MCS** でプロビジョニングされたマシンの更新をサポート。GCP 環境で、`Set-ProvScheme`はテンプレート（プロビジョニングスキーム）を変更します。既存のマシンには影響しません。PowerShell`Request-ProvVMUpdate`コマンドを使用して、現在のプロビジョニングスキームを既存のマシン、あるいはマシンのセットに適用できるようになりました。現在 GCP では、マシンプロファイルがこの機能でサポートされているプロパティの更新です。詳しくは、「PowerShell を使用してプロビジョニングされたマシンを更新」を参照してください。

2022 年 **10** 月

新機能と機能強化

マシンプロファイルとホストグループの同時使用をサポート。Azure Resource Manager マスターイメージを使用してカタログを作成する際、マシンプロファイルとホストグループを同時に使用できるようになりました。これは、トラステッド起動を使用してセキュリティを向上させ、同時に専用ホスト上でマシンを実行する場合に役立ちます。詳しくは、「Microsoft Azure Resource Manager 仮想化環境」を参照してください。

フォルダーを使用したデリバリーグループの整理をサポート。フォルダーツリーを作成してデリバリーグループを整理し、簡単にアクセスできるようになりました。詳しくは、「フォルダーを使用したデリバリーグループの整理」を参照してください。

［完全な構成］を使用した **1** 回限りのマシン再起動のスケジュール設定をサポート。新しいオプションである ［一度だけ］が、デリバリーグループの再起動スケジュールを作成するときに使用できるようになりました。このオプションを使用すると、指定した日時にデリバリーグループ内のマシンを 1 回再起動するようにスケジュールできます。詳しくは、「再起動スケジュールの作成」を参照してください。

高度なプローブスケジュール設定。［監視］でのアプリケーションプローブとデスクトッププローブのスケジュール設定が改善されました。この機能を使用して、特定の曜日にプローブタスクを実行し、その日の間に指定された間隔で繰り返しプローブタスクを実行するように Citrix Probe Agent を構成できます。これにより、1 つのプローブタスクが特定の曜日の特定の時間に繰り返されるようにスケジュールできます。プローブが適切な時間に定期的に実行されるように設定することで、サイトの正常性を積極的にチェックできるようになりました。この機能により、［監視］でのプローブのセットアップと管理が簡素化されます。詳しくは、「アプリケーションプロービングおよびデスクトッププロービング」を参照してください。

2022 年 9 月

新機能と機能強化

古いバージョンの **Remote PowerShell SDK** は廃止となりました。廃止バージョンを使用している場合、SDK が動作を停止し、現在のバージョンをダウンロードするように求めるエラーメッセージが表示されます。この問題が発生した場合は、Citrix Web サイトから最新の Remote PowerShell SDK をダウンロードします。

Azure でのトラステッド起動を使用したマシンカタログ。Azure 環境では、トラステッド起動が有効になっているマシンカタログを作成し、VM インベントリの`SupportsTrustedLaunch`プロパティを使用して、トラステッド起動をサポートする VM サイズを決定できます。

トラステッド起動は、第 2 世代 VM のセキュリティをシームレスに向上させる方法です。トラステッド起動は、高度かつ永続的な攻撃手法からの保護を提供します。詳しくは、「トラステッド起動を使用したマシンカタログ」を参照してください。

MCS によって作成された **Microsoft System Center Virtual Machine Manager** リソースの識別をサポート。タグを使用して、MCS によって作成された Microsoft System Center Virtual Machine Manager（SCVMM）リソースを識別できるようになりました。MCS がリソースに追加するタグについて詳しくは、「MCS によって作成されたリソースの特定」を参照してください。

MCS によって作成された **VMware** リソースの識別をサポート。タグを使用して、MCS によって作成された VMware リソースを識別できるようになりました。MCS がリソースに追加するタグについて詳しくは、「MCS によって作成されたリソースの特定」を参照してください。

AWS ワークスペースの調整の最適化をサポート。調整の問題なく、AWS ワークスペースで多数のマシンの電源をオンまたはオフにできるようになりました。調整の問題は、AWS ワークスペースに送信された要求の数が、サーバーが処理できる要求の数を超えると発生します。そのため、Citrix は、AWS ワークスペース SDK に送信する前に、複数の要求を 1 つの要求にグループ化するようにしました。

ホームでマシン数を表示する際、マシンの詳細を確認する機能。［ホーム］で可用性の状態別にマシン数を表示する場合、状態をクリックして、その状態のマシンの詳細を表示できるようになりました。詳しくは、「［完全な構成］インターフェイスのホームページ」を参照してください。

同じ **Azure** テナント内の別のサブスクリプションからのイメージを使用したマシンカタログ作成をサポート。以前は、Azure 環境では、サブスクリプション内のイメージを選択してマシンカタログを作成することしかできませんでした。この機能により、別の共有サブスクリプションに属する Azure Compute Gallery（旧称 Shared Imaged Gallery）のイメージを選択し、MCS カタログを作成および更新できるようになりました。

カタログの作成について詳しくは、「Azure Resource Manager イメージを使用してマシンカタログを作成する」を参照してください。

同じテナント内の別のサービスプリンシパルとイメージを共有する方法については、「同じテナント内の別のサービスプリンシパルとのイメージ共有」を参照してください。

別のサブスクリプションからイメージを選択する PowerShell コマンドについて詳しくは、「PowerShell を使用した別のサブスクリプションからのイメージの選択」を参照してください。

Azure Compute Gallery について詳しくは、「Azure Shared Image Gallery」を参照してください。

2022 年 8 月

新機能と機能強化

MCS によって作成された **Citrix Hypervisor** リソースの識別をサポート。タグを使用して、MCS によって作成された Citrix Hypervisor リソースを識別できるようになりました。MCS がリソースに追加するタグについて詳しくは、「MCS によって作成されたリソースの特定」を参照してください。

ホストグループゾーンと **Azure Availability Zones** の同時使用をサポート。Azure 環境では、カスタムプロパティで指定された Azure Availability Zones とホストグループのゾーンに基づいて、マシンカタログの作成が成功するかどうかを事前チェックで評価できるようになりました。アベイラビリティゾーンのカスタムプロパティがホストグループのゾーンと一致しない場合、カタログの作成は失敗します。

ホストグループは、専用ホストのコレクションを表すリソースです。専用ホストは、1 つまたは複数の仮想マシンをホストする物理サーバーを提供するサービスです。
Azure Availability Zones は、各 Azure リージョン内の物理的に離れた場所であり、ローカルの障害に対して耐性があります。

マシンカタログの作成が成功または失敗するアベイラビリティゾーンとホストグループゾーンのさまざまな組み合わせについて詳しくは、「ホストグループゾーンと Azure Availability Zones の同時使用」を参照してください。

VMware でマシンカタログのフォルダー **ID** の更新をサポート。VMware の仮想化環境では、`Set-ProvScheme` のカスタムプロパティ `FolderID` を使用して、MCS マシンカタログのフォルダー ID を更新できるようになりました。フォルダー ID の更新後に作成された仮想マシンは、この新しいフォルダー ID の下に作成されます。このプロパティが `CustomProperties` で指定されていない場合、仮想マシンはマスターイメージが配置されているフォルダーの下に作成されます。フォルダー ID の更新について詳しくは、「マシンカタログのフォルダー ID の更新」を参照してください。

タイムゾーンの設定。[日付と時刻] 設定を使用して、環境設定に合わせてインターフェイスの日時形式を構成できるようになりました。詳しくは、「タイムゾーンの設定」を参照してください。

Image Portability Service（**IPS**）が **Amazon Web Services**（**AWS**）をサポートするようになりました。AWS に必要な権限とコンポーネントを設定することで、AWS アカウントで IPS ワークフローを使用できます。詳しくは、「ワークロードのパブリッククラウドへの移行」を参照してください。

Azure 環境でのイメージ準備中のページファイル設定。Azure 環境で、ページファイルの場所との混同を避けられるようになりました。そのために、イメージの準備中、プロビジョニングスキームを作成する際に、MCS がページファイルの場所を決定するようになりました。この計算は特定の規則に基づいています。エフェメラル OS ディスク（EOS）や MCS I/O などの機能には、それぞれ想定するページファイルの場所があり、相互に排他的です。プロビジョニングスキームの作成からイメージの準備を切り離した場合も、ページファイルの場所は MCS によって正しく決定されます。ページファイルの場所について詳しくは、「ページファイルの場所」を参照してください。

Azure 環境でのページファイル設定の更新をサポート。Azure 環境でカタログを作成するときに、PowerShell コマンドを使用して、場所やサイズなどのページファイル設定を指定できるようになりました。その場合、MCS によって決定されたページファイル設定は上書きされます。これは、`New-ProvScheme`コマンドを実行し、次のカスタムプロパティを使って行うことができます:

- `PageFileDiskDriveLetterOverride`: ページファイルの場所ディスクのドライブ文字
- `InitialPageFileSizeInMB`: 初期ページファイルサイズ（MB）
- `MaxPageFileSizeInMB`: 最大ページファイルサイズ（MB）

ページファイル設定の更新について詳しくは、「ページファイル設定の更新」を参照してください。

ホームページを更新。Get Started（開始）ウィジェットの外観が新しくなりました。ホームページのその他の更新内容は次のとおりです:

- 右上隅に新しく追加された更新アイコンとヘルプアイコン。
- リソースカウントをクリックして、関連するリソースページにすばやくアクセスできるように。
- Dislike（低評価）アイコンの機能強化。推奨事項に対して低評価アイコンを選択した場合、その推奨事項は表示されなくなります。推奨ウィジェットに対して低評価アイコンを選択した場合、そのウィジェットは表示されなくなります。

詳しくは、ホームページを参照してください。

Azure VM 拡張機能の有効化をサポート。ARM テンプレートスペックをマシンプロファイルとして使用してマシンカタログを作成する場合、Azure VM 拡張機能をカタログ内の VM に追加し、サポートされている拡張機能の一覧を表示し、追加した拡張機能を削除できるようになりました。Azure VM 拡張機能は、Azure VM で展開後の構成と自動化タスクを設定できる小さなアプリケーションです。たとえば、VM にソフトウェアのインストール、ウイルス対策保護、または VM 内でスクリプトを実行する機能が必要な場合は、VM 拡張機能を使用できます。Azure VM 拡張機能を有効にする方法について詳しくは、「PowerShell を使用して Azure VM 拡張機能を有効にする」を参照してください。

エフェメラル **OS** ディスクのトラステッド起動をサポート。トラステッド起動で、Windows でエフェメラル OS ディスクを使用して、プロビジョニングスキームを作成できるようになりました。トラステッド起動は、第 2 世代 VM のセキュリティをシームレスに向上させる方法です。セキュアブートやトラステッドプラットフォームモジュール（vTPM）の仮想化バージョンなど、個別に有効にできるテクノロジを組み合わせることで、高度で永続的な攻撃手法から保護します。マシンカタログの作成について詳しくは、「Azure Resource Manager イメージを使用してマシンカタログを作成する」を参照してください。

2022 年 **7** 月

新機能と機能強化

シングルセッション **OS** マシンの動的セッションタイムアウト。動的セッションタイムアウトで、シングルセッション OS マシンがサポートされるようになりました。バージョン 2206 以降の VDA が 1 つ以上あるデリバリーグルー

プが必要です。これらの VDA が Citrix Cloud に最低 1 回は登録されていることを確認してください。詳しくは、「動的セッションタイムアウト」を参照してください。

Autoscale でユーザーを強制的にログオフせずにログオフリマインダーを送信。Autoscale のユーザーログオフ通知（旧称ユーザー強制ログオフ）で新機能を使用できるようになりました。この機能を使用すると、ユーザーにログオフを強制せずに、ログオフリマインダーをユーザーに送信できます。リマインダーにより、ユーザーにセッションからのログオフを強制することで生じるデータ損失の可能性を避けることができます。詳しくは、「ユーザーログオフ通知」を参照してください。

Azure で **Linux** 仮想マシンカタログを作成するときに **Linux OS** のライセンスの種類を設定する機能。［完全な構成］インターフェイスを使用して、Azure で Linux VM カタログを作成するときに Linux OS ライセンスの種類を選択できるようになりました。持ち込みの Linux ライセンスには、Red Hat Enterprise Linux と SUSE Linux Enterprise Server という 2 つの選択肢があります。詳しくは、「Azure Resource Manager イメージを使用してマシンカタログを作成する」を参照してください。

［完全な構成］での検索エクスペリエンスを向上。［検索］ノードでは、次の新機能と拡張機能を提供します：

- 検索結果をエクスポートする機能。検索結果をエクスポートできるようになりました。エクスポートするには、右上隅にあるエクスポートアイコンをクリックします。
- 新しいフィルターを使用できるようになりました。［保留中の電源操作］フィルターを使用できるようになりました。フィルターを使用して検索を絞り込みます。
- 特定のアイテムの「次を含まない」検索のサポート。マシン名やタグなどのアイテムで、「次を含まない」という検索基準がサポートされるようになりました。
- フィルターを追加するときのオブジェクトの検索サポート。以下のオブジェクトにフィルターを追加して検索できるようになりました：接続、マシンカタログ、デリバリーグループ、アプリケーショングループ、タグ。

詳しくは、「［完全な構成］管理インターフェイスでの［検索］の使用」を参照してください。

VMware ストレージプロファイルをサポート。vSAN データストアでマスターイメージを使用してマシンカタログを作成する場合、RAID-1 または RAID-5 情報などのストレージポリシーを、作成されたターゲットデバイスにマスターイメージからコピーできるようになりました。既存のカタログの場合、カタログを更新してもストレージポリシーは変更されません。

RestrictedKrbHost SPN 登録をサポート。Citrix MCS で作成したすべてのコンピューターアカウントがサービスプリンシパル名（SPN）の「`RestrictedKrbHost`」に登録されるようになりました。これにより、MCS がアカウントを作成した後、「`setspn`」コマンドを実行してコンピューターアカウントの SPN を登録する必要がなくなりました。

Microsoft パッケージアプリケーションを配信するための［完全な構成］のアプリパッケージ。［App-V］ノードの名前が［アプリパッケージ］に変更され、より多くの種類の Microsoft パッケージアプリに対応できるように再設計されました。以前は、検出モジュールを使用して、配信用に App-V パッケージアプリを環境に追加する必要がありました。これで、［アプリパッケージ］ノードだけで、アプリを追加および配信できます。詳しくは、「アプリパッケージ」を参照してください。

マシンプロファイルとしての **ARM** テンプレートスペックの使用をサポート。以前は、マシンプロファイルとして使

用できるのは VM だけでした。Azure マシンカタログを作成するときに、マシンプロファイルとして ARM テンプレートスペックも使用できるようになりました。この機能を使用すると、バージョン管理などの Azure ARM テンプレート機能を利用できます。選択したスペックが正しく構成され、必要な構成がなされたことを確認するためには、検証を実行します。検証が失敗した場合、別のマシンプロファイルを選択するように求められます。詳しくは、「Azure Resource Manager イメージを使用してマシンカタログを作成する」を参照してください。

ARM テンプレートスペックの検証サポート。ARM テンプレートスペックを検証して、マシンカタログを作成するためにマシンプロファイルとして使用できることを確認できるようになりました。ARM テンプレートスペックを検証する方法は 2 つあります:

- [完全な構成] 管理インターフェイスを使用する。
- PowerShell コマンドを使用する。

ARM テンプレートスペックの検証について詳しくは、「Azure Resource Manager イメージを使用してマシンカタログを作成する」を参照してください。

2022 年 6 月

新機能と機能強化

シングルセッション **OS** マシンの再起動スケジュールのサポート。以前は、再起動スケジュール機能はマルチセッション OS マシンでのみ使用可能でしたが、シングルセッション OS マシンでも利用できるようになりました。シングルセッション OS マシンを含むデリバリーグループの再起動スケジュールを作成できるようになりました。詳しくは、「デリバリーグループのマシンに対する複数の再起動スケジュールの作成」を参照してください。

ユーザー名の事前チェックを実行するオプション。ドメイン資格情報を入力した場合に、[名前の確認] オプションが使用できるようになりました。このオプションを使用すると、ユーザー名が有効か一意かを確認できます。このオプションは、次のような場合に役立ちます:

- 同じユーザー名が複数のドメインに存在する。目的のユーザーを選択するように求められます。
- ドメイン名を忘れた。ドメイン名を指定せずにユーザー名を入力できます。この確認が完了すると、ドメイン名が自動的に入力されます。

詳しくは、「ドメイン資格情報」を参照してください。

既存のプロビジョニングスキームのネットワーク設定を変更する機能。新しい仮想マシンが新しいサブネットワーク上に作成されるように、既存のプロビジョニングスキームのネットワーク設定を変更できるようになりました。`Set-ProvScheme`コマンドのパラメーター`-NetworkMapping`を使用して、ネットワーク設定を変更します。スキームから新しくプロビジョニングされた仮想マシンにのみ、新しいサブネットワーク設定が指定されます。また、サブネットワークが同じホスティングユニットの下にあることを確認する必要があります。詳しくは、「既存のプロビジョニングスキームのネットワーク設定を変更」を参照してください。

Azure 仮想マシン、管理対象ディスク、スナップショット、**Azure VHD**、および **ARM** テンプレートのリージョン名情報を取得できるようになりました。Azure 仮想マシン、管理対象ディスク、スナップショット、Azure VHD、お

よび ARM テンプレートのリージョン名情報を表示できるようになりました。この情報は、マシンカタログが割り当てられている場合に、マスターイメージ上のリソースに関して表示されます。詳しくは、「Azure 仮想マシン、管理対象ディスク、スナップショット、Azure VHD、および ARM テンプレートのリージョン名情報を取得」を参照してください。

Azure 環境でマシンプロファイルのプロパティ値を使用する機能。マシンプロファイルを使用して Azure カタログを作成すると、カスタムプロパティで値が明示的に定義されていない場合、マシンプロファイルとして使用されている ARM テンプレートスペックまたは仮想マシンのいずれかからプロパティ値が設定されるようになりました。この機能の影響を受けるプロパティは次のとおりです:

- アベイラビリティゾーン
- 専用ホストグループ ID
- ディスク暗号化セット ID
- OS の種類
- ライセンスの種類
- サービスオファリング
- ストレージの種類

一部のプロパティがマシンプロファイルで欠落していて、カスタムプロパティで定義されていないとき、該当する場合はプロパティのデフォルト値が常に適用されます。詳しくは、「マシンプロファイルのプロパティ値を使用する」を参照してください。

VDA のアップグレードの拡張サポート。[完全な構成] インターフェイスを使用して、MCS でプロビジョニングされた永続マシンをアップグレードできるようになりました。カタログごとに、またはマシンごとにアップグレードできます。詳しくは、「完全な構成インターフェイスを使用した VDA のアップグレード」を参照してください。

Citrix Cloud Japan および **Citrix Cloud Government** コントロールプレーンでの **Citrix Probe Agent**。Citrix Probe Agent は、Citrix Cloud Japan および Citrix Cloud Government コントロールプレーンでホストされるサイトをサポートするようになりました。これらのプレーンでプロービングエージェントを使用するには、パスのレジストリ値を「\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region」を、Japan リージョンの場合は 2 に、Government リージョンの場合は 3 に設定します。Citrix Probe Agent では、サイトに公開されている仮想アプリおよび仮想デスクトップの状態チェックプロセスが自動化されます。詳しくは、「アプリケーションプロービングおよびデスクトッププロービング」を参照してください。

VDA と **Cloud Connector** 間の通信に使用するポートをカスタマイズ。特定のセキュリティ要件に基づいて、VDA が Cloud Connector との通信に使用するポートをカスタマイズできるようになりました。この機能は、セキュリティチームがデフォルトポート（ポート 80）を開くことを許可していない場合、またはデフォルトポートが既に使用されている場合に役立ちます。詳しくは、「Cloud Connector と通信するためのポートのカスタマイズ」を参照してください。

フォルダーを使用したマシンカタログの整理に対応。ネストされたフォルダーを作成してマシンカタログを整理し、簡単にアクセスできるようになりました。詳しくは、「フォルダーを使用したカタログの整理」を参照してください。

SCVMM 2022 をサポート。Citrix DaaS は、Microsoft の System Center Virtual Machine Manager（SCVMM）2022 をサポートするようになりました。SCVMM は、仮想マシンの展開に必要なリソースの保守を含むさまざまなサ

ービスを提供します。SCVMM 2022 でサポートされる新機能について詳しくは、System Center Virtual Machine Manager の新機能を参照してください。

AWS での最大同時プロビジョニング操作のパラメーター設定をサポート。Citrix DaaS は、AWS 上の MCS の構成可能なカスタムプロパティとして`MaximumConcurrentProvisioningOperations`をサポートするようになりました。`MaximumConcurrentProvisioningOperations`は、同時に作成または削除できる仮想マシンの数を決定するプロパティです。MCS はデフォルトで最大 100 の同時プロビジョニング操作をサポートしますが、PowerShell コマンドを入力してこの値をカスタマイズできるようになりました。1〜1000 の範囲の値を入力できます。このプロパティを希望の値に設定すると、仮想マシンを作成または削除するときに実行できる並列タスクの数を制御できます。最大同時プロビジョニング操作の構成について詳しくは、「ホスト接続のデフォルト値」を参照してください。

2022 年 5 月

新機能と機能強化

強化されたセッション起動診断。Citrix DaaS では、セッションの詳細な起動エラー診断がサポートされるようになりました。これで、セッションの起動シーケンスに関連するコンポーネントを表示できます。最後に生成されたエラーコードで、失敗したコンポーネントが強調表示されます。これは、セッションの起動エラーの正確な理由を特定し、推奨される操作を実行するのに役立ちます。

[Transaction] ページには、エラーが発生したコンポーネントの一覧が表示される [Transaction Details] パネルが含まれるようになりました。コンポーネント名をクリックすると、コンポーネントの詳細と最後に確認された障害の詳細が表示されます。障害の理由とエラーコードが表示されます。[Learn more] リンクをクリックして、[Error codes] の特定のコードにアクセスし、詳細な説明と推奨される操作を表示します。詳しくは、「セッション診断」を参照してください。

Remote PowerShell SDK での **Set-ProvServiceConfigurationData** の使用のサポート。これで、Remote PowerShell SDK を使用して「`Set-ProvServiceConfigurationData`」を実行し、該当するすべてのパラメーターの設定を行うことができます。このコマンドを使用して、イメージの準備中に DHCP の有効化をスキップすることもできます。以下は、「`Set-ProvServiceConfigurationData`」でサポートされている設定の一覧です:

- イメージ準備タイムアウトの変更: `Set-ProvServiceConfigurationData -Name "ImageManagementPrep_PreparationTimeout"-value 60`
- DHCP 有効化のスキップ:`Set-ProvServiceConfigurationData -Name ImageManagementPrep -Value EnableDHCP`
- Microsoft Windows KMS リセットのスキップ: `Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps -Value OsRearm`
- Microsoft Office KMS リセットのスキップ: `Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps -Value OfficeRearm`

- 準備 VM 自動シャットダウンの無効化:
  ```
  Set-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown
   -Value true
  ```
- ドメインインジェクションの無効化:
  ```
  Set-ProvServiceConfigurationData -Name DisableDomainInjection -
  Value true
  ```

PowerShell コマンドを使用して **Linux** マシンカタログを作成するときに **Linux** ライセンスの種類を設定する機能。PowerShell コマンドを使用して、Linux マシンカタログ作成時に Linux ライセンスの種類を設定できます。Linux ライセンスの持ち込みには、次の 2 つの選択肢があります: RHEL_BYOS および SLES_BYOS。デフォルトの設定は Azure Linux ライセンスです。詳しくは、「Azure Resource Manager イメージを使用してマシンカタログを作成する」を参照してください。

MCS によって作成されたすべての **Azure** リソースを識別するためのサポート。「`provschemeID`」というタグを使用して、ProvScheme に関連付けられているイメージ、ID ディスク、OS ディスク、NIC、VM などの MCS によって作成されたすべての Azure リソースを識別できるようになりました。MCS がリソースに追加するタグについて詳しくは、「MCS によって作成されたリソースの特定」を参照してください。

SCVMM を介した **Azure Stack HCI** プロビジョニングのサポート。MCS は、Microsoft System Center Virtual Machine Manager（SCVMM）を介した Azure Stack HCI プロビジョニングをサポートするようになりました。SCVMM などの既存のツールを使用して、Azure スタック HCI クラスターを管理できます。詳しくは、「Microsoft System Center Virtual Machine Manager 仮想化環境」を参照してください。

Active Directory 以外のユーザーを手動で追加するためのサポート。[完全な構成] 管理インターフェイスを使用して、カタログに Active Directory 以外のユーザーを追加するときに、複数のユーザー名をセミコロン区切りで入力できるようになりました。異なるディレクトリに存在するユーザーを追加するときは、形式を考慮してください。たとえば、これらのユーザーが Active Directory に存在する場合は、名前を直接入力します。そうでない場合は、次の形式で名前を入力します: `<identity provider>:<user name>`。例: `AzureAD:username`。詳しくは、「マシンカタログの作成」を参照してください。

2022 年 4 月

新機能と機能強化

[完全な構成] インターフェイスのホームページ。[完全な構成] にホームページが追加されました。このページで、サブスクリプションを最大限に活用するために役立つ情報と、Citrix DaaS 展開およびワークロードの概要を表示します。このページは次の内容で構成されています:

- サービス概要。Citrix DaaS 展開とワークロードの概要を表示します。
- 推奨事項。サブスクリプションで使用できる機能のお勧めを表示し、フィードバックを収集します。
- 新機能。最新の機能を表示します。
- プレビュー機能。現在プレビュー段階の機能を表示します。

- 開始。初期セットアップの手順を表示します。

詳しくは、ホームページを参照してください。

カタログの作成と更新の進行状況を表示します。［完全な構成］で、カタログの作成と更新に関する最新情報を入手できるようになりました。作成および更新プロセスの概要を取得し、実行した手順の履歴を表示し、現在の手順の進行状況と実行時間を監視できます。詳しくは、「カタログの作成を開始する」を参照してください。

選択したゾーンに基づいて、利用可能なハイパーバイザーとクラウドサービスを表示します。［完全な構成］では、ホスト接続を作成するときに、接続の種類を選択する前にゾーンを選択する必要があります。［接続の種類］ドロップダウンリストには、ゾーンで使用可能なハイパーバイザーとクラウドサービスが表示されます。以前は、必要なハイパーバイザーまたはクラウドサービスを［接続の種類］一覧に表示するには、すべてのゾーンにプラグインをインストールする必要がありました。今回、構成順序が新しくなったことで、必要なゾーンにプラグインをインストールするだけで済むようになりました。

また、PowerShell コマンドを使用して、選択したゾーンで使用できるハイパーバイザープラグインの一覧を取得することもできます。詳しくは、「接続とリソースの作成」を参照してください。

［完全な構成］でのオンプレミスではない **AD** 参加済みユーザーのサポート。［完全な構成］インターフェイスで新しい［**ID** の種類の選択］フィールドを使用できるようになりました。このフィールドで、プロビジョニングされたデスクトップまたはアプリ、デリバリーグループ、あるいはアプリケーショングループに、ユーザーを割り当てます。このフィールドを使用すると、Citrix Cloud が接続されている次の ID プロバイダーのいずれかからユーザーアカウントを選択できるようになります:

- Active Directory
- Azure Active Directory
- Okta

Google Cloud Platform（**GCP**）および **Azure** 環境で、無効なカスタムプロパティを拒否する機能。これにより、`New-ProvScheme`と`Set-ProvScheme`に設定されたカスタムプロパティが有効にならない場合に混乱を避けられるようになりました。存在しないカスタムプロパティを指定した場合、次のエラーメッセージが表示されます。詳しくは、「カスタムプロパティの設定に関する重要な考慮事項」を参照してください。

Azure Active Directory 参加済みマシンの作成のサポート。［完全な構成］でカタログを作成するとき、［マシン **ID**］で［**Azure Active Directory** 参加済み］の ID の種類が使用できるようになりました。MCS でこの種類の ID を使用して、Azure Active Directory 参加済みマシンを作成できます。また、追加オプションの［マシンを **Microsoft Intune** に登録する］により、管理のためにマシンを Microsoft Intune に登録できます。

Azure Active Directory 参加済みカタログの作成については、「マシンカタログの作成」を参照してください。Azure Active Directory 参加関連の要件および考慮事項については、「Azure Active Directory 参加済み」を参照してください。

Hybrid Azure Active Directory 参加済みマシンの作成のサポート。［完全な構成］でカタログを作成するとき、［マシン **ID**］で［**Hybrid Azure Active Directory** 参加済み］の ID の種類が使用できるようになりました。MCS でこの種類の ID を使用して、Hybrid Azure Active Directory 参加済みマシンを作成できます。これらは組

織が所有しているマシンであり、その組織に属した Active Directory Domain Services アカウントでサインインします。

Hybrid Azure Active Directory 参加済みカタログの作成については、「マシンカタログの作成」を参照してください。Hybrid Azure Active Directory 参加関連の要件および考慮事項については、「Hybrid Azure Active Directory 参加済み」を参照してください。

スナップショットのための **Azure** の信頼できる起動のサポート。Azure のトラステッド起動がイメージだけでなくスナップショットでも利用できるようになりました。トラステッド起動が有効になっているスナップショットを選択する場合は、マシンプロファイルを使用する必要があります。また、トラステッド起動が有効になっているマシンプロファイルを選択する必要があります。詳しくは、「Microsoft Azure Resource Manager クラウド環境」を参照してください。

マシンのエクスポート。[マシンカタログのセットアップ] ウィザードの [マシン] ページに表示されるマシンを CSV ファイルにエクスポートして、マシンを一括でカタログに追加するときにテンプレートとして使用できるようになりました。詳しくは、「カタログからのマシンのエクスポート」を参照してください。

Workspace Environment Management Web コンソールにアクセスするためのオプション。[管理] タブのメニューで、[Environment Management（Web）] オプションを使用できるようになりました。このオプションを選択すると、新しい Web ベースの Workspace Environment Management コンソールに移動します。従来のコンソールにアクセスするには、**Environment Management** を使用します。現在、全機能を従来のコンソールから Web コンソールに移行中です。Web コンソールは通常、従来のコンソールよりも速く応答します。詳しくは、「Workspace Environment Management サービス」を参照してください。

ProvScheme パラメーターを管理する機能。MCS でカタログを作成するとき、サポートされていないハイパーバイザーでマシンカタログの作成中に`New-ProvScheme`パラメーターを設定するか、マシンカタログの作成後に`Set-ProvScheme`パラメーターを更新すると、エラーが表示されるようになりました。詳しくは、「マシンカタログの作成」を参照してください。

増加されたリソースの場所の制限。シングルセッション VDA とマルチセッション VDA のリソースの場所の制限が、それぞれ 10000 と 1000 に引き上げられました。詳しくは、「制限」を参照してください。

すべてのセッションをドレインした後に電源管理されていないマシンを再起動するサポート。Citrix DaaS では、すべてのセッションがマシンからドレインされた後、電源管理されていないマシンの再起動スケジュールを作成できるようになりました。[完全な構成] インターフェイスの [再起動の間隔] で [すべてのセッションのドレイン後にすべてのマシンを再起動する] を選択します。詳しくは、「再起動スケジュールの作成」を参照してください。

VDA マシンのアップグレードのサポート（**Technical Preview**）。[完全な構成] インターフェイスを使用して、Citrix DaaS 展開用に VDA マシンをアップグレードできるようになりました。カタログごとに、またはマシンごとにアップグレードできます。この機能は、MCS で作成されていないマシン（物理マシンなど）に適用されます。詳しくは、「完全な構成インターフェイスを使用した VDA のアップグレード」を参照してください。

停止中にマシンがシャットダウンされることはありません。Citrix DaaS では、マシンが存在するゾーンで停止が発生したときに、ブローカーによって仮想マシンがシャットダウンされることがなくなりました。停止が終了すると、マシンは自動的に接続できるようになります。停止後にマシンを使用可能にするために、操作を行う必要はありません。

セッション起動診断。Citrix DaaS では、強化されたセッション起動エラー診断がサポートされるようになりました。Citrix Monitor（つまり、Citrix Director サービス）内から Citrix Workspace アプリで生成された 32 桁 (8-4-4-4-12）のトランザクション ID を使用して、問題が発生した正確なコンポーネントとステージまで絞り込み、問題解決のために推奨される操作を実行します。詳しくは、「セッション起動診断」を参照してください。

Session Recording サービスにアクセスするためのオプション。[管理] タブのメニューで、[Session Recording] オプションを使用できるようになりました。Session Recording サービスの導入により、ポリシー、再生、およびサーバー構成を一元管理できます。組織全体に分散されたオブジェクトを管理および監視するための統合されたエントリポイントを提供することにより、IT 管理者の負担を軽減します。詳しくは、「Session Recording サービス（Technical Preview）」を参照してください。

Citrix Virtual Apps and Desktops サービスの名称を変更。**Citrix Virtual Apps and Desktops** サービスの名称が **Citrix DaaS** に変更されました。名称変更について詳しくは、当社ブログ上のお知らせを参照してください。

Citrix Virtual Apps and Desktops サービスの以下のオファリングの名称が変更されました。

- **Citrix Virtual Apps** サービス **Advanced** の名称が **Citrix DaaS Advanced** に変更されました。
- **Citrix Virtual Apps** サービス **Premium** の名称が **Citrix DaaS Premium** に変更されました。
- **Citrix Virtual Desktops** サービスの名称が **Citrix DaaS Advanced Plus** に変更されました。
- **Citrix Virtual Apps and Desktops** サービス **Advanced** の名称が **Citrix DaaS Advanced Plus** に変更されました。
- **Citrix Virtual Apps and Desktops** サービス **Premium** が **Citrix DaaS Premium** および **Citrix DaaS Premium Plus** として利用できるようになりました。
- **Citrix Virtual Apps and Desktops Standard for Azure** の名称が **Citrix DaaS Standard for Azure** に変更されました。
- **Citrix Virtual Apps and Desktops Standard for Google Cloud** の名称が **Citrix DaaS Standard for Google Cloud** に変更されました。
- **Citrix Virtual Apps and Desktops Premium for Google Cloud** の名称が **Citrix DaaS Premium for Google Cloud** に変更されました。

現在、製品と製品ドキュメントで移行作業が行われています。この移行の間はご迷惑をおかけしますが、何卒ご容赦願います。

- 製品の UI、製品内のコンテンツ、および製品ドキュメント内の画像と手順は、数週間以内に更新されます。
- 既存の顧客のスクリプトの破損を防ぐために、コマンドや MSI などの一部のアイテムでは、以前の名前を引き続き保持できます。
- 関連する製品ドキュメントや、この製品のドキュメントからリンクされているその他のリソース（ビデオやブログの投稿など）には、以前の名前が含まれている場合があります。

> 注:
>
> オンプレミスの **Citrix Virtual Apps and Desktops** の製品名に変更はありません。

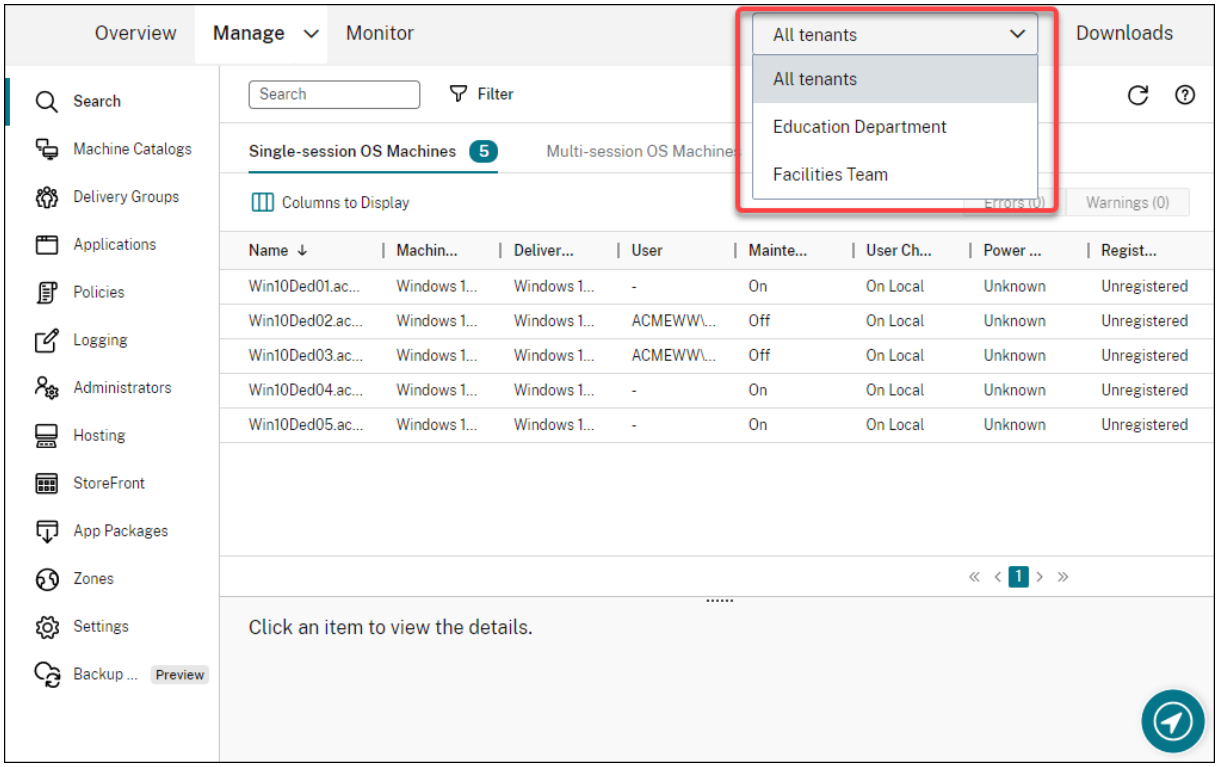
［完全な構成］でのテナントのサポート。単一の Citrix DaaS インスタンス内に構成パーティションを作成できるようになりました。構成パーティションは、［管理者］**>**［スコープ］でテナントスコープを作成し、マシンカタログやデリバリーグループなど、関連する構成オブジェクトをそれらのテナントと関連付けることで作成できます。これにより、テナントへのアクセス権を持つ管理者は、テナントに関連付けられているオブジェクトのみを管理できます。この機能は、たとえば、組織が以下のような場合に役立ちます:

- さまざまなビジネスサイロ（独立した部門または個別の IT 管理チーム）がある、または
- 複数のオンプレミスサイトがあり、単一の Citrix DaaS インスタンスで同じセットアップを維持したいと考えている。

また、［完全な構成］インターフェイスでは、テナント顧客を名前でフィルタリングできます。デフォルトでは、このインターフェイスにはすべてのテナントに関する情報が表示されます。

この機能は、Citrix Service Provider（CSP）と CSP 以外のどちらでも利用できます。CSP 環境のインターフェイスは、テナントの作成に使用されるメソッドを除き、CSP 以外の環境のインターフェイスと基本的に同じです。

- CSP では、テナント顧客を Citrix DaaS にオンボード（登録）し、Citrix DaaS への管理者アクセスを構成します。詳しくは、「Citrix DaaS for Citrix Service Provider」を参照してください。
- CSP 以外では、最初にスコープを作成し、次にそれぞれの管理者のカスタムアクセスを構成することにより、テナント顧客を作成します。詳しくは、「スコープの作成と管理」を参照してください。



Autoscale の更新。Autoscale を更新してブレードスタイルにし、ユーザーエクスペリエンスを向上させました。設定を構成するためのワークフローに変更はありません。Autoscale のその他の更新には次のものがあります:

- 理解しやすいよう、「**Autoscale** の制限」を「タグ付けされたマシンの **Autoscale**」に名称を変更しました。

- 新しく［**Autoscale** がタグ付けされたマシンの電源投入を開始するタイミングを制御する］オプションを追加しました。このオプションをオンにすると、Autoscale は、タグ付けされていないマシンの使用状況に基づいて、タグ付けされたマシンの電源投入を開始するタイミングを制御できます。

タグ付けされたマシンの Autoscale について詳しくは、「タグ付きマシンの Autoscale」を参照してください。

ライセンスの有効性チェック。［完全な構成］インターフェイスでは、ホスト接続で使用されているライセンスの有効性を自動的にチェックするようになりました。ライセンスが無効な場合、ホスト接続はメンテナンスモードになります。その結果、接続の編集やメンテナンスモードのオフなど、特定の操作を実行できなくなります。たとえば、次の場合、ライセンスは無効になります:

- ライセンスの有効期限切れ。この場合、Citrix の営業担当者に連絡して、ライセンスを更新するか、新しいライセンスを購入してください。
- ライセンスがライセンスサーバーから削除された。

マシンカタログおよびポリシーノードにブレードスタイルを適用。［完全な構成］のすべてのノードにブレードスタイルが適用されるようになりました。

Azure 環境で **MCS** プロビジョニングされたマシンを更新するためのサポート。`Set-ProvScheme`はテンプレート（プロビジョニングスキーム）を変更して、既存のマシンには影響しません。Request-ProvVMUpdate コマンドを使用して、現在のプロビジョニングスキームを既存のマシン、あるいはマシンのセットに適用できるようになりました。現在、この機能でサポートされているプロパティ更新は`ServiceOffering`です。詳しくは、「プロビジョニングされたマシンを現在のプロビジョニングスキームの状態に更新する」を参照してください。

2022 年 3 月

新機能と機能強化

Google Cloud Marketplace で入手可能な **Google Cloud** 向け **Citrix Virtual Apps and Desktops**。Google Cloud 向け Citrix Virtual Apps and Desktops が Google Cloud Marketplace で購入可能になりました。Citrix Virtual Apps and Desktops Premium for Google Cloud は、Google Cloud 上で Citrix Virtual Apps and Desktops サービスのコントロールプレーンを実行します。

Azure のトラステッド起動のサポート。［完全な構成］管理インターフェイスで、Azure のトラステッド起動を使用できるようになりました。トラステッド起動が有効になっているイメージを選択する場合は、マシンプロファイルを使用する必要があります。また、トラステッド起動が有効になっているマシンプロファイルを選択する必要があります。詳しくは、「Microsoft Azure Resource Manager クラウド環境」を参照してください。

［完全な構成］の **3** つの追加ノードのウィザードにブレードスタイルを適用。ノードは、［検索］、［デリバリーグループ］、および ［アプリケーション］です。

Image Portability Service（**IPS**）が **GA**（一般公開）リリースされました。IPS は、プラットフォーム間でのイメージの管理をシンプルにします。この機能は、オンプレミスのリソースの場所とパブリッククラウド内のリソースの場所との間でイメージを管理するのに役立ちます。Citrix Virtual Apps and Desktops の REST API を使用して、

Citrix Virtual Apps and Desktops サイト内のリソースの管理を自動化できます。詳しくは、「ワークロードのパブリッククラウドへの移行」を参照してください。

2022 年 2 月

新機能と機能強化

Azure の権限。セキュリティ要件として必須の、リスクを最小限に抑える権限が 2 セットあります。

- 最低限の権限：この権限セットにより、セキュリティ制御が向上します。ただし、最低限の権限であるため、追加の権限を必要とする新機能は失敗します。
- 一般的な権限：この権限セットなら、新しい拡張機能のメリットを得ることができます。

詳しくは、「Azure の権限について」を参照してください。

VM の一時ディスクを使用した、**Azure** 環境でのライトバックキャッシュディスクのホストをサポート。［管理］**>** ［完全な構成］インターフェイスの ［マシンカタログのセットアップ］**>** ［ディスク設定］に、［非永続的なライトバックキャッシュディスクを使用する］オプションを追加しました。プロビジョニングされた VM に対してライトバックキャッシュディスクを保持しない場合は、このオプションを選択します。このオプションをオンにした場合、VM の一時ディスクに十分なスペースがある場合は、その一時ディスクを使用してライトバックキャッシュディスクをホストします。これによりコストを削減できます。詳しくは、「Microsoft Azure Resource Manager クラウド環境」を参照してください。

AWS ホスト接続のデフォルト設定を更新。AWS ホスト接続のデフォルト設定値がより高い値に更新されており、ほとんどの場合、すべての AWS クラウドプラットフォームのセットアップで同じ値になっています。これにより、個々のセットアップでデフォルト設定値を評価および構成することなく、AWS クラウド環境でホスト接続を作成できます。詳しくは、「ホスト接続のデフォルト値」を参照してください。

GCP 環境のさまざまなストレージ階層のサポートを追加。GCP 環境で以下のカスタムプロパティを使用できるようになりました。これにより、新しく作成された VM に接続されているディスクのストレージの種類を設定できます：

- StorageType
- IdentityDiskStorageType
- WBCDiskStorageType

詳しくは、「Citrix Virtual Apps and Desktops サービス SDK」を参照してください。

Azure VM カタログ作成後に特定の **VM** 設定を変更。［完全な構成］管理インターフェイスを使用して、カタログの作成後に以下の設定を変更できるようになりました：

- マシンサイズ
- アベイラビリティゾーン
- マシンプロファイル
- Windows ライセンス

変更するには、［マシンカタログ］ノードでカタログを選択してから、操作バーの ［マシンカタログの編集］を選択します。詳しくは、「カタログの編集」を参照してください。

Azure エフェメラル **OS** ディスクのキャッシュディスクまたは一時ディスクへの保存をサポート。Citrix Virtual Apps and Desktops サービスで、キャッシュディスクまたは Azure 対応仮想マシンの一時ディスクに Azure エフェメラル OS ディスクを保存できるようになりました。この機能は、標準の HDD ディスクよりも高性能の SSD ディスクを必要とする Azure 環境で役立ちます。詳しくは、「Microsoft Azure Resource Manager クラウド環境」を参照してください。

Nutanix Clusters on AWS をサポート。Citrix Virtual Apps and Desktops サービスは、Nutanix Clusters on AWS をサポートします。Nutanix Clusters は、プライベートクラウドまたは複数のパブリッククラウドでのアプリケーションの実行をシンプルにします。詳しくは、「Nutanix clusters on AWS」を参照してください。

VMware Cloud on AWS（**Amazon Web Services**）をサポート。VMware Cloud on AWS（Amazon Web Services）を使用すると、VMware ベースのオンプレミスの Citrix ワークロードを AWS クラウドに移行し、核となる Citrix Virtual Apps and Desktops 環境を Citrix Virtual Apps and Desktops サービスに移行できます。詳しくは、「VMware Cloud on AWS（Amazon Web Services）」を参照してください。

Google Cloud Platform（**GCP**）で実行されているマシンのライトバックキャッシュディスクの構成のサポート。［完全な構成］管理インターフェイスを使用して、GCP にマシンをプロビジョニングする際、次のライトバックキャッシュディスク設定を構成できるようになりました：

- ディスクサイズ
- キャッシュに割り当てられたメモリ
- ディスクストレージの種類
- ディスクの永続性

詳しくは、「Google Cloud Platform 仮想化環境」の「マシンカタログの作成」を参照してください。

2022 年 1 月

新機能と機能強化

Nutanix Clusters on AWS をサポート。Citrix Virtual Apps and Desktops サービスは、Nutanix Clusters on AWS をサポートするようになりました。このサポートは、Nutanix オンプレミスクラスターと同じ機能を提供します。単一のクラスターのみサポートされます（*Prism Element*）。詳しくは、「Nutanix 仮想化環境」を参照してください。

Cloud Health Check で使用可能な新機能。Cloud Health Check は、次のような機能を備えた新しいバージョンに更新されました：

- 自動修正。Cloud Health Check で、実行中のマシンで識別された特定の問題の自動検出と修正がサポートされるようになりました。具体的にどのアクションが実行されたのかを示す結果レポートが生成されるようになります。詳しくは、「自動修正」を参照してください。

- コマンドラインのサポート。Cloud Health Check をコマンドラインから実行できるようになりました。詳しくは、「コマンドラインで Cloud Health Check を実行する」を参照してください。
- **Citrix** ユニバーサルインジェクションドライバーのステータス。Cloud Health Check で、Citrix UVI ドライバーのステータスを表示するとともに、Citrix UVI ドライバーに関連するイベントログチェックを行うようになりました。
- セッションの起動レジストリチェック。Cloud Health Check で、セッションの起動レジストリ設定をチェックするようになりました。
- チェックレポートに対する更新事項。複数のチェックポイントがあるチェック項目の場合、ヘルスチェック中に実行されたアクションを示すために、検証されたすべてのチェックが最終チェックレポートに一覧表示されるようになりました。

詳しくは、「Cloud Health Check」を参照してください。

［完全な構成］を使用した **VDA** 登録とセッション起動の問題のトラブルシューティング。［完全な構成］管理インターフェイスを使用して、VDA の状態を測定するチェックを実行できるようになりました。VDA のヘルスチェックは、一般的な VDA 登録およびセッションの起動の問題を引き起こす原因となるものを見つけ出します。ヘルスチェックは個別と一括で実行できます。詳しくは、「VDA のヘルスチェック」を参照してください。

既存の接続について **Azure** シークレットの有効期限を指定する機能。［完全な構成］管理インターフェイスを使用して、アプリケーションシークレットの有効期限が切れる日付を指定できるようになりました。シークレットの有効期限を表示する方法については、「Microsoft Azure Resource Manager クラウド環境」を参照してください。この機能を使用するときは、次の違いを考慮してください：

- Azure で手動で作成されたサービスプリンシパルの場合、有効期限は ［接続の編集］ **>** ［接続のプロパティ］ページで直接編集できます。
- ユーザーに代わって［完全な構成］を介して作成されたサービスプリンシパルの有効期限を初めて編集する場合は、［接続の編集］ **>** ［設定の編集］ **>** ［既存のものを使用］に移動します。以降の編集は、［接続の編集］ **>** ［接続のプロパティ］ページで行えます。

管理者を追加するためのボタン。［完全な構成］ **>** ［管理者］ **>** ［管理者］タブに、［管理者の追加］のボタンが追加されました。このボタンを使用することで、［**ID** およびアクセス管理］ **>** ［管理者］にすばやく移動でき、そこで管理者を追加（招待）できます。詳しくは、「管理者の追加」を参照してください。

［完全な構成］でのウィザードの外観が変更。ウィザードの次のノードについて、新しいスタイル（色、フォント、その他フォーマットの変更など）で更新し、ユーザーエクスペリエンスを向上させました：管理者、ホスティング、**StoreFront**、アプリパッケージ、ゾーン、設定。新しいウィザードは、より広いビューポートを備えたブレードビューで表示され、より多くのコンテンツを表示できるようになります。設定を構成するためのワークフローに変更はありません。

Google Cloud Platform（**GCP**）で実行されているマシンに対して **MCS I/O** が有効になっている場合にシステムディスクを保持するサポート。［完全な構成］管理インターフェイスにて、GCP でマシンをプロビジョニングするときに、MCS ストレージ最適化（MCS I/O）が有効な場合、電源サイクル中にシステムディスクを保持できるようになりました。詳しくは、「MCS ストレージ最適化の更新を有効にする」を参照してください。

Amazon Web Services（**AWS**）上の **EBS** からの直接アップロードまたはダウンロードのサポート。AWS で、必要なコンテンツとともに EBS ボリュームを直接作成できる API が提供されるようになりました。API を使用して、カタログの作成と VM の追加に必要なボリュームワーカーを排除できるようになりました。この機能に必要な AWS の権限については、「Amazon Web Services クラウド環境」を参照してください。

MCS によって作成された **Amazon Web Services**（**AWS**）リソースを識別する機能。MCS によって作成された AWS リソースを識別するために、`CitrixProvisioningSchemeID`という名前の新しいタグを追加しました。詳しくは、「MCS によって作成されたリソースの特定」を参照してください。

［管理］と［監視］へのアクセス権を構成する機能。［完全な構成］管理インターフェイスに、［管理］と ［監視］へのアクセス権をもつカスタムの役割を付与するかどうかを制御するオプションが追加されました。詳しくは、「役割の作成と管理」を参照してください。

2021 年 **12** 月

新機能と機能強化

Google Cloud VMware Engine のサポート。Google Cloud VMware Engine プラットフォームを使用すると、VMware ベースのオンプレミス Citrix ワークロードを Google Cloud に移行し、核となる Citrix Virtual Apps and Desktops 環境を Citrix Virtual Apps and Desktops サービスに移行できます。詳しくは、「Google Cloud Platform（GCP）VMware Engine のサポート」を参照してください。

名前付けスキームを指定するときに、アカウント名の先頭を指定する機能。このリリースでは、［完全な構成］管理インターフェイスの ［マシンカタログのセットアップ］**>**［マシン **ID**］ページにオプションが追加されました。このオプションを使用すると、アカウント名の先頭にある数字または文字を指定して、カタログ作成時にマシンアカウントに名前付けする方法をより細かく制御できます。詳しくは、「マシン ID」を参照してください。

Nutanix AHV XI および **Nutanix AHV Prism Central**（**PC**）接続の作成のサポート。［完全な構成］管理インターフェイスで、Nutanix AHV XI 接続および Nutanix AHV PC 接続を作成できるようになりました。詳しくは、「Nutanix 仮想化環境」を参照してください。

GCP で **VM** をプロビジョニングするときに、**OS** ディスクのストレージの種類を選択できる機能のサポート。［完全な構成］管理インターフェイスで、GCP の VM をプロビジョニングするとき、OS ディスク用のストレージの種類を選択できるようになりました。［マシンカタログのセットアップ］**>**［ストレージ］ページで使用できるストレージオプションには、［標準永続ディスク］、［バランス永続ディスク］、［**SSD** 永続ディスク］があります。詳しくは、「マシンカタログの作成」を参照してください。

［完全な構成］管理インターフェイスで、**Azure** エフェメラルディスクがサポートされるようになりました。以前は、エフェメラル OS ディスクを使用するマシンを作成できるのは PowerShell だけでした。新しく ［マシンカタログのセットアップ］**>**［ストレージとライセンスの種類］ページに ［**Azure** エフェメラル **OS** ディスク］オプションが追加されました。VM のローカルディスクを使用してオペレーティングシステムディスクをホストする場合は、このオプションを選択します。詳しくは、「Azure Resource Manager イメージを使用してマシンカタログを作成する」を参照してください。

Machine Creation Services（**MCS**）が管理するリソースを誤って削除しないように保護する機能。VM に対して有効になっている GCP の`deletionProtection`フラグを適用することで、Google Cloud Platform（GCP）上の MCS 管理対象リソースを保護できるようになりました。`compute.instances.setDeletionProtection`権限または IAM の Compute Admin の役割を使用して、リソースの削除を許可するフラグをリセットできます。この機能は、永続カタログと非永続カタログの両方に適用できます。詳しくは、「意図しないマシンの削除からの保護」を参照してください。

2021 年 11 月

新機能と機能強化

マシンを更新するときにイメージに注釈を付ける機能。［完全な構成］管理インターフェイスで、MCS で作成したカタログを更新するとき、イメージにメモを追加して注釈を付けることができるようになりました。カタログを更新するたびに、メモを追加するかどうかに関係なく、メモ関連のエントリが作成されます。メモを追加せずにカタログを更新すると、エントリは null（-）として表示されます。イメージのメモ履歴を表示するには、カタログを選択し、下のペインで ［テンプレートのプロパティ］をクリックしてから、［メモの履歴を表示］をクリックします。詳しくは、「カタログの更新」を参照してください。

マルチタイプのライセンスのサポート。［完全な構成］管理インターフェイスでマルチタイプのライセンスがサポートされるようになりました。これにより、サイト（Citrix Virtual Apps and Desktops サービス製品の展開）またはデリバリーグループで使用するライセンス使用権を指定できます。

- サイトレベルでは、ユーザーがデバイスでアプリまたはデスクトップを起動したときに、サイト全体で使用するライセンスを決定します。選択したライセンスは、別のライセンスで構成されているデリバリーグループを除き、すべてのデリバリーグループに適用されます。
- デリバリーグループレベルでは、デリバリーグループに使用するライセンスを自分で決定し、マルチタイプのライセンスの柔軟性と利点を享受できます。

詳しくは、「マルチタイプのライセンス」を参照してください。

Azure Marketplace 購入プラン情報の表示サポート。［完全な構成］管理インターフェイスでマシンカタログを作成する際、Azure Marketplace イメージから作成されたマスターイメージの購入プラン情報を表示できるようになりました。

2021 年 10 月

新機能と機能強化

永続的な **MCS** カタログを更新する機能。［完全な構成］管理インターフェイスの永続的な MCS カタログに ［マシンの更新］オプションが導入されました。このオプションを使用すると、カタログが使用するイメージまたはテンプレートを管理できます。永続カタログを更新するときは、次の点を考慮してください：後でカタログに追加するマシン

のみが新しいイメージまたはテンプレートを使用して作成されます。更新はカタログ内の既存のマシンにロールアウトされません。詳しくは、「カタログの更新」を参照してください。

Azure 専用ホストで **VM** をプロビジョニングするオプション。［完全な構成］管理インターフェイスの ［マシンカタログのセットアップ］**>**［マスターイメージ］ページにオプションとして ［ホストグループを使用する］が追加されました。このオプションを使用すると、Azure 環境で VM をプロビジョニングするときに使用するホストグループを指定できます。詳しくは、「Azure Resource Manager イメージを使用してマシンカタログを作成する」を参照してください。

電源を入れ直したときにプロビジョニングされた **VM** を保持することにより、パフォーマンスを向上。［完全な構成］管理インターフェイスの ［マシンカタログのセットアップ］**>**［ディスク設定］に、［電源サイクルをまたいで仮想マシンを保持する］設定が追加されました。この設定により、Azure 環境で電源を入れ直したときに、プロビジョニングされた VM を保持できます。詳しくは、「MCS ストレージ最適化」を参照してください。または、PowerShell を使用して機能を構成することもできます。詳しくは、「電源を入れ直したときにプロビジョニングされた仮想マシンを保持する」を参照してください。

Workspace Environment Management 構成セットへのマシンカタログのバインド。マシンカタログを作成するときに、それを Workspace Environment Management 構成セットにバインドできるようになりました。そうすることで、Workspace Environment Management をサービスを使用して、可能な限り最良のワークスペース環境をユーザーに提供できます。カタログの作成後にカタログをバインドすることもできます。詳しくは、「マシンカタログの作成」および「マシンカタログの管理」を参照してください。

2021 年 **9** 月

新機能と機能強化

イメージの更新に関する説明の追加。マシンカタログイメージの更新に関連した変更に関する説明を追加できるようになりました。この機能は、カタログで使用されるイメージを更新するときに、管理者が説明ラベル（*Office 365* インストール済みなど）を追加するのに役立ちます。PowerShell コマンドを使用すると、これらのメッセージを作成および表示できます。詳しくは、「イメージへの説明の追加」を参照してください。

Azure VMware Solution（**AVS**）の統合。Citrix Virtual Apps and Desktops サービスでは、AVS（Azure VMware Solution）がサポートされています。AVS では、Azure によって作成された vSphere クラスターを含むクラウドインフラストラクチャが提供されます。オンプレミス環境で vSphere を使用するのと同じ方法で、Citrix Virtual Apps and Desktops サービスで AVS を使用して VDA ワークロードをプロビジョニングします。詳しくは、「Azure VMware Solution の統合」を参照してください。

複数のカタログ用に同じリソースグループ。同じリソースグループを使用して、Citrix Virtual Apps and Desktops サービスで複数のカタログを更新および作成できるようになりました。このプロセスは:

- 1 つまたは複数のマシンカタログを含むどのリソースグループにも適用されます。
- Machine Creation Services によって作成されないリソースグループをサポートしています。
- VM と関連リソースを作成します。

- VM またはカタログが削除されると、リソースグループ内のリソースを削除します。

詳しくは、「Azure リソースグループ」を参照してください。

Azure VM、スナップショット、**OS** ディスク、およびギャラリーイメージ定義の情報の取得。Azure VM、OS ディスク、スナップショット、およびギャラリーイメージ定義について情報を表示できます。この情報は、マシンカタログが割り当てられている場合にマスターイメージ上のリソースに関して表示されます。この機能を使用して、Linux または Windows イメージを表示および選択します。詳しくは、「Azure VM、スナップショット、OS ディスク、およびギャラリーイメージ定義の情報の取得」を参照してください。

自動構成の更新。自動構成は、次のような機能を備えた新しいバージョンに更新されました:

- Machines Creation Services（MCS）のサポート - 自動構成で MCS カタログがサポートされるようになりました。詳しくは、「Machine Creation Services でプロビジョニングされたカタログの移行について」を参照してください。

自動構成のその他の更新には、次のものがあります:

- エクスポート時にオンプレミスのゾーンの名前を、バックアップ時にクラウドのリソースの場所を ZoneMapping.yml ファイルに事前入力することで、ゾーンのサポートを強化しました。
- StoreFront は、トップレベルの管理可能コンポーネントになりました。これ以前は、StoreFront はデリバリーグループの一部として管理されていました。この分離により、サイトのマージがより容易になります。
- 現在のマージオプションと新しいマージオプションのパターンに一致するように`AddMachinesOnly`を`MergeMachines`に変更しました。
- サポートコマンドレットで CustomerInfo.yml を作成および更新する場合に SecurityClient.csv ファイルを使用して ClientId と Secret をインポートする方法を追加しました。
- ユーザーゾーンの優先度の移行を追加しました。
- 日本語のコントロールプレーンのサポートが修正されました。
- その他の修正と改善。

Citrix のダウンロードページで自動構成をダウンロードします。自動構成について詳しくは、「構成の Citrix Cloud への移行」を参照してください。

再起動スケジュールで利用可能なスケジュールオプションを追加。［完全な構成］管理インターフェイスに、再起動の実施がスケジュールされた場合のタイミングを制御するためのオプションが追加されました。毎日の定期的な再起動スケジュールに加えて、毎週および毎月の繰り返しパターンを設定できるようになりました。詳しくは、「再起動スケジュールの作成」を参照してください。

パフォーマンスを低下させるカスタム列を保持。以前は、［完全な構成］管理インターフェイスの検索ノードで、ブラウザーウィンドウを更新するか、コンソールからいったんサインアウトし、再びサインインすると、パフォーマンスを低下させるカスタム列が表示されなくなっていました。現在は、このようなカスタム列を保持するかどうかを制御できるようになっています。詳しくは、「［完全な構成］管理インターフェイスでの［検索］の使用」を参照してください。

自動構成ツールを使用したバックアップおよび復元。［完全な構成］管理インターフェイスにノード ［バックアップと

復元］を追加しました。このノードには、以下に関する情報を含む、自動構成ツールに関連するすべてのリソースが集約されます：

- コマンド 1 つで行われる Citrix Virtual Apps and Desktops 構成の自動バックアップのスケジューリング
- 過去のバックアップからの復元（必要に応じて）
- バックアップと復元のきめ細かな実行
- サポートされているその他のユースケース

詳しくは、自動構成についてのドキュメントを参照してください。

ドメイン非参加カタログのサポート。［完全な構成］管理インターフェイスの ［マシンカタログのセットアップ］> ［マシン **ID**］ページに ID の種類として ［ドメイン非参加］が追加されました。MCS でこの種類の ID を使用して、どのドメインにも参加していないマシンを作成できます。詳しくは、「マシンカタログの作成」を参照してください。

マシンプロファイルの使用のサポート。［完全な構成］管理インターフェイスの ［マシンカタログのセットアップ］> ［マスターイメージ］ページにオプションとして ［マシンプロファイルを使用する］が追加されました。このオプションを使用すると、Azure 環境で VM を作成するときに、VM がどのマシンプロファイルから構成を継承するかを指定できます。その後、カタログ内の VM は、指定したマシンプロファイルから構成を継承できます。構成の例として、次のようなものがあります：

- 高速ネットワーク
- ブート診断
- ホストのディスクキャッシュ（OS および MCSIO ディスク関連）
- マシンサイズ（別途指定されていない場合）
- VM に適用されたタグ

詳しくは、「Azure Resource Manager イメージを使用してマシンカタログを作成する」を参照してください。

Windows Server 2022 のサポート：最小で VDA 2106 が必要です。

2021 年 **8** 月

新機能と機能強化

並べ替え可能なアイテムの数を **500** から **5,000** に拡張します。［完全な構成］管理インターフェイスの ［検索］ノードで、最大 5,000 個のアイテムを任意の列見出しで並べ替えることができるようになりました。アイテム数が 5,000 を超える場合は、フィルターを使用してアイテム数を 5,000 以下に減らし、並べ替えを有効にします。詳しくは、「［完全な構成］管理インターフェイスでの［検索］の使用」を参照してください。

追加の **Azure** ストレージの種類のサポート。MCS を使用する Azure 環境の仮想マシンにさまざまなストレージの種類を選択することができるようになりました。詳しくは、「ストレージの種類」を参照してください。

ライトバックキャッシュディスク用のストレージの種類の選択をサポート。［完全な構成］管理インターフェイスで、MCS カタログを作成するときに、ライトバックキャッシュディスク用のストレージの種類を選択できるようになり

ました。使用可能なストレージの種類には、プレミアム SSD、標準 SSD、および標準 HDD が含まれます。詳しくは、「マシンカタログの作成」を参照してください。

一時停止したマシンのシャットダウン。［管理］**>**［完全な構成］インターフェイスの ［負荷ベースの設定］ページにある、シングルセッション OS デリバリーグループの［Autoscale ユーザーインターフェイスの管理］に、［再接続がない場合（分）］オプションを追加しました。このオプションは、［一時停止］を選択すると使用可能になり、一時停止したマシンをいつシャットダウンするかを指定できます。一時停止したマシンは、切断されたユーザーが再接続すると引き続き使用できますが、新しいユーザーは使用できません。マシンをシャットダウンすると、マシンを再び使用可能にしてすべてのワークロードを処理できます。詳しくは、「Autoscale」を参照してください。

CSV ファイルを使用してマシンをカタログに一括追加する拡張サポート。［管理］**>**［完全な構成］インターフェイスで、CSV ファイルを使用して、データセンターにある既存のマシンをそれらのマシンの電源を管理しているカタログに一括で追加できるようになりました。詳しくは、「マシンカタログの作成」および「マシンカタログの管理」を参照してください。

2021 年 **7** 月

新機能と機能強化

構成ログ。［管理］**>**［完全な構成］の ［ログ］ユーザーインターフェイスが変更されました。このインターフェイスは次の 3 つのタブで構成されています:

- イベント（以前の構成ログ）。このタブでは、構成の変更と管理アクティビティを追跡できます。
- タスク。このタブでは、マシンカタログ操作に関連するタスクを表示できます。
- **API**。このタブでは、特定の期間中に行われた REST API 要求を表示できます。

詳しくは、「構成ログ」を参照してください。

Autoscale で、動的セッションタイムアウトのオプションを使用できるようになりました。ピーク時とオフピーク時に切断されるセッションとアイドル状態になるセッションのタイムアウトを構成して、マシンのドレインを高速化し、コストを削減できます。詳しくは、「動的セッションタイムアウト」を参照してください。

Google Cloud Platform（**GCP**）の顧客管理暗号キー（**CMEK**）のサポート。これにより、MCS カタログで Google の CMEK を使用できます。CMEK により、Google Cloud プロジェクト内のデータの暗号化に使用されるキーをより詳細に制御できます。詳しくは、「顧客管理暗号キー（CMEK）」を参照してください。この機能の構成については、「顧客管理暗号化キー（CMEK）の使用」を参照してください。この機能は、［管理］**>**［完全な構成］の［マシンカタログのセットアップ］**>**［ディスク設定］ページで使用できます。

> 注:
>
> この機能はプレビューとして提供されています。

［管理］タブを更新。［管理］タブのメニューのオプションを更新しました:

- 完全な構成：以前はこのオプションを選択すると従来のコンソールに移動していましたが、現在は、新しい Web ベースのコンソール（Web Studio）に移動します。この Web ベースのコンソールは、従来のコンソールと完全に同等で、いくつかの拡張機能が追加されています。今すぐこの新しいコンソールの使用を開始することをお勧めします。
- 従来の構成：このオプションを選択すると、従来のコンソール（2021 年 9 月に廃止予定）に移動します。2021 年 9 月以降は、［完全な構成］が、すべての構成および管理操作にアクセスできる唯一のインターフェイスになります。

Web Studio で、リモート **PC** アクセスカタログの電源管理接続を選択できるようになりました。以前は、Studio を使用すれば（接続の種類として［リモート **PC Wake on LAN**］を選択することで）リソースの場所への Wake on LAN ホスト接続を作成できましたが、その接続をリモート PC アクセスカタログに関連付けるには、PowerShell を使用する必要がありました。現在は、Studio でこれを実行できるようになりました。詳しくは、「完全な構成インターフェイスを使用して Wake on LAN を構成する」を参照してください。

2021 年 **6** 月

新機能と機能強化

Azure Shared Image Gallery からのイメージへのアクセス。マシンカタログを作成するときに、マスターイメージ画面の Azure Shared Image Gallery からイメージにアクセスできるようになりました。詳しくは、「Azure Shared Image Gallery からイメージにアクセスする」を参照してください。

Google Cloud Platform（**GCP**）でシールドされた仮想マシンをサポート。シールドされた仮想マシンを GCP でプロビジョニングできます。シールドされた仮想マシンは、セキュアブート、仮想トラステッドプラットフォームモジュール、UEFI ファームウェア、整合性監視などの高度なプラットフォームセキュリティ機能を使用して、Compute Engine インスタンスの検証可能な整合性を提供する一連のセキュリティ制御によって強化されます。詳しくは、「シールド VM」を参照してください。

HTTPS または **HTTP** のいずれかを適用。レジストリ設定を使用して、XML サービス経由で HTTPS または HTTP トラフィックを適用します。

Azure 環境でのコストを削減するために、**ID** ディスクには常に標準の **SSD** を使用してください。マシンカタログは、ID ディスクに標準の SSD ストレージの種類を使用します。Azure の標準 SSD は、低 IOPS レベルで安定したパフォーマンスを必要とするワークロードに最適化された、コスト効率の高いストレージオプションです。ストレージの種類について詳しくは、「Azure Resource Manager マスターイメージ」を参照してください。

> 注：
>
> Azure Managed Disks の価格について詳しくは、「Managed Disks の価格」を参照してください。

Web Studio で利用可能な新機能。Web ベースのコンソールで、次の機能が使用できるようになりました：

- **Studio** では、**Azure** に認証してサービスプリンシパルを作成することができるようになりました。Azure に認証してサービスプリンシパルを作成することにより、Azure へのホスト接続を確立できます。このサポート

により、Studio で接続を作成する前に、Azure サブスクリプションでサービスプリンシパルを手動で作成する必要がなくなります。詳しくは、「Microsoft Azure Resource Manager 仮想化環境」を参照してください。

- **Studio** では、既存のマシンカタログを複製できるようになりました。この機能を使用すると、既存のマシンカタログを複製して、新しいマシンカタログのテンプレートとして使用できるため、同様のカタログを最初から作成する必要がなくなります。カタログを複製する場合、オペレーティングシステムとマシンの管理に関連する設定を変更することはできません。複製されたカタログは、元のカタログからこれらの設定を継承します。詳しくは、「カタログの複製」を参照してください。
- [設定] という新しいノードが、**Studio** のナビゲーションペインで使用できるようになりました。[設定] ノードでは、サイト全体（Citrix Virtual Apps and Desktops サービス製品の環境）に適用される設定を構成できます。次の設定を使用できます:
  - マルチセッションカタログの負荷分散。ニーズに合った負荷分散オプションを選択します。この設定は、すべてのカタログに適用されます。以前は、この機能を使用するために、コンソールの右上隅にある歯車アイコンをクリックする必要がありました。詳しくは、「マシンの負荷分散」を参照してください。
- **Studio** の検索エクスペリエンスの向上。このリリースでは、Studio の検索エクスペリエンスが向上しています。フィルターを使用して高度な検索を実行すると、[フィルターの追加] ウィンドウが前面に表示され、後面のビューは変更されません。詳しくは、「［完全な構成］管理インターフェイスでの［検索］の使用」を参照してください。
- **MCS** で **Google Cloud VM** を一時停止および再開する機能。他の VM と同じように、MCS で Google Cloud VM を一時停止および再開できるようになりました。詳しくは、「デリバリーグループの管理」を参照してください。この機能を有効にするには、Google Cloud サービスアカウントで`compute.instances.suspend`と`compute.instances.resume`の権限を設定します。コンピューティング管理者の役割には、これらの権限が付随しています。

  Citrix Virtual Apps and Desktops では、PowerShell コマンドの`New-BrokerHostingPowerAction`を使用して VM を一時停止および再開することもできます。詳しくは、「New-Brokerhostingpoweraction」を参照してください。

  Google Cloud は、一時停止できるインスタンスの種類と構成にいくつかの制限を適用します。詳しくは、Google Cloud サイトの「インスタンスの一時停止と再開」を参照してください。

2021 年 5 月

新機能と機能強化

メンテナンスモードでマシンから切断した後のセッションの再接続。以前は、プールされた（ランダムな）シングルセッションデスクトップ（VDI）ユーザーがメンテナンスモードでマシンから切断された場合、プール内のどのマシンへのセッションの再接続も許可されていませんでした。マルチセッションおよび静的シングルセッションマシンの場合は、その状況で常にセッションの再接続が許可されていました。

現在、PowerShell を使用して、メンテナンスモードのマシンで切断が発生した後にセッションの再接続を許可するかどうかをデリバリーグループレベルで制御できるようになりました。これは、グループ内のすべての VDA（シングルセッションおよびマルチセッション）に適用されます。

詳しくは、「メンテナンスモードでマシンから切断されたときのセッションの再接続の制御」を参照してください。

Citrix Virtual Apps and Desktops サービスの全エディションにおけるアプリケーションプロービングとデスクトッププロービングのサポート。既存の **Premium** Edition のサポートに加えて、アプリケーションプロービングとデスクトッププロービングが **Citrix Virtual Apps Advanced** サービスおよび **Citrix Virtual Apps and Desktops Advanced** サービスで利用できるようになりました。

Web Studio で利用可能な新機能。Web ベースのコンソールで、次の機能が使用できるようになりました:

- **Studio** で、**Azure Availability Zones** の選択がサポートされるようになりました。以前は、Azure 環境の特定のアベイラビリティゾーンにマシンをプロビジョニングするには、PowerShell しか使用できませんでした。Studio を使用してマシンカタログを作成するときに、マシンをプロビジョニングするアベイラビリティゾーンを 1 つ以上選択できるようになりました。ゾーンが指定されていない場合、Machine Creation Services（MCS）により、Azure はマシンをリージョン内に配置します。複数のゾーンが指定されている場合、MCS はマシンをそれらにランダムに分散します。詳しくは、「指定されたアベイラビリティゾーンへのマシンのプロビジョニング」を参照してください。

Azure エフェメラルディスク。Citrix Virtual Apps and Desktops サービスは、Azure エフェメラルディスクをサポートしています。エフェメラルディスクを使用すると、キャッシュディスクを再利用して、Azure 対応の仮想マシンの OS ディスクを保存できます。この機能は、標準の HDD ディスクよりも高性能の SSD ディスクを必要とする Azure 環境で役立ちます。

> 注:
>
> 永続カタログでは、エフェメラル OS ディスクはサポートされていません。また、この機能を使用する場合は、パフォーマンスの高いディスクに追加のコストがかかることを考慮してください。追加の管理対象ディスクにお金を払う代わりに、キャッシュディスクを再利用して OS ディスクを保存すると便利です。

エフェメラル OS ディスクでは、プロビジョニングスキームで管理対象ディスクと Shared Image Gallery を使用する必要があります。詳しくは、「Azure エフェメラルディスク」を参照してください。

Azure 上の **MCS** で管理される **VDA** のパフォーマンスが向上しました。Citrix Virtual Apps and Desktops サービスによって、Azure 上の Machine Creation Services（MCS）で管理される VDA のパフォーマンスが向上します。この機能拡張により、ホスティング接続の絶対同時アクションのデフォルト値が 500 に変更され、ホスティング接続の *1* 分あたりの最大新規アクションが 2,000 に変更されます。この拡張機能を利用するために、手動の構成タスクは必要ありません。詳しくは、「Azure の調整」を参照してください。

Cloud Health Check で使用可能な新機能。Cloud Health Check は、次のような機能を備えた新しいバージョンに更新されました:

- **VDA** マシンの自動検出。Cloud Health Check は、Citrix Virtual Apps and Desktops サービスの環境から VDA を自動的に検出して取得できるようになりました。詳しくは、「VDA マシンの取得」を参照してくださ

い。

- ヘルスチェックのスケジュール設定。Cloud Health Check で、定期的なヘルスチェックを実行するためのスケジュールを設定できるようになりました。詳しくは、「Cloud Health Check スケジューラ」を参照してください。
- **Cloud Health Check** のバージョン情報。使用している Cloud Health Check のバージョンを確認できるようになりました。バージョン情報を表示するには、Cloud Health Check のメインウィンドウの右上隅にある歯車アイコンをクリックします。
- 自動修正。Cloud Health Check で、実行中のマシンで識別された特定の問題の自動検出と修正がサポートされるようになりました。詳しくは、「自動修正」を参照してください。

  > 注:
  >
  > 自動修正はプレビューとして利用できます。

2021 年 4 月

新機能と機能強化

AWS API を使用して動的インスタンスを取得します。Citrix Virtual Apps and Desktops サービスは、インスタンスの種類を動的に取得するよう AWS にクエリを実行するようになりました。この機能により、Citrix Virtual Apps and Desktops サービスで定義されているサイズを超えるマシンサイズを使用するお客様のために、カスタムの`InstanceTypes.xml`ファイルを作成する必要がなくなります。この情報は、以前は`InstanceTypes.xml`ファイルによって提供されていました。利用可能な AWS インスタンスの種類へのこの動的アクセスを容易にするには、ユーザーはサービスプリンシパルの権限を更新して、これに`ec2:DescribeInstanceTypes`権限を含める必要があります。サービスプリンシパルの権限を更新しないことを選択した顧客の下位互換性をサポートするために、`InstanceTypes.xml`にリストされている AWS インスタンスの種類が使用されます。このプロセスにより、MCS CDF ログに警告メッセージが生成されます。

> 注:
>
> Citrix Studio は、CDF ログに含まれる警告メッセージを表示しません。

権限について詳しくは、「IAM 権限の定義」および「AWS 権限について」を参照してください。

Web Studio で利用可能な新機能。Web ベースのコンソールで、次の機能が使用できるようになりました:

- **Studio** でユーザーのタイムゾーンの日付と時刻を表示できるようになりました。以前は、Studio ではシステムのクロックとタイムゾーンに基づく日付と時刻のみが表示されていました。現在は、イベントアイテムの上にマウスポインタを置くと、ローカルのタイムゾーンの日付と時刻を表示できます。時間は UTC で表されます。

一時ストレージのない **Azure VM** で **MCS I/O** を利用できます。MCS I/O が、一時ディスクまたは接続されたストレージがない VM のマシンカタログ作成をサポートするようになりました。このサポートにより:

- スナップショット（管理対象ディスク）が、一時ストレージのないソース VM から取得されます。マシンカタログ内の VM に一時ストレージがありません。
- スナップショット（管理対象ディスク）が、一時ストレージのあるソース VM から取得されます。マシンカタログ内の VM に一時ストレージがあります。

詳しくは、「Machine Creation Services（MCS）ストレージ最適化」を参照してください。

Web Studio で利用可能な新機能。Web ベースのコンソールで、次の機能が使用できるようになりました:

- 強制ログオフ。Autoscale では、設定された猶予期間に達したときに、マシンに存在するセッションを強制的にログオフできるようになり、そのマシンをシャットダウンの対象にします。これにより、Autoscale がマシンの電源をより速くオフにできるため、コストを削減できます。ユーザーをログオフする前に、ユーザーに通知を送信できます。詳しくは、「Autoscale」を参照してください。

自動構成の更新。自動構成は、次のような機能を備えた新しいバージョンに更新されました:

- 複数のサイトのマージ - プレフィックスとサフィックスを使用して名前の衝突を回避しながら、複数のサイトを 1 つのサイトにマージできます。詳しくは、「複数のサイトを 1 つのサイトにマージする」を参照してください。
- サイトのアクティブ化 - オンプレミスまたはクラウドの環境で再起動スケジュールや電源スキームなどのリソースを制御するかどうかを選択できます。詳しくは、「サイトのアクティブ化」を参照してください。

自動構成のその他の更新には、次のものがあります:

- 管理者の役割とスコープを移行する機能。
- コンソールのログ記録を抑制するための選択コマンドレットの`Quiet`パラメーター。
- 認証を必要とする安全なネットワークファイル共有に、CvadAcSecurity.yml ファイルを配置できるようにする`SecurityFileFolder`パラメーター。
- マシンカタログおよびデリバリーグループのマシン名でフィルタリングする機能。
- スイッチパラメーター方式を使用するためのコンポーネント選択パラメーターの改善。コンポーネント名の後に`$true`を追加する必要がなくなりました。
- サポートを受けるために Citrix に送信する、すべてのログファイルを圧縮する新しいコマンドレット（`New-CvadAcZipInfoForSupport`）。

Citrix のダウンロードページで自動構成をダウンロードします。自動構成について詳しくは、「クラウドへの移行」を参照してください。

電源サイクルをまたいで **GCP** インスタンスを保持します。非永続的な Google Cloud Platform（GCP）インスタンスは、電源をオフにしても削除されなくなりました。電源サイクルをまたいでインスタンスは保持されます。非永続インスタンスの電源がオフになると、OS ディスクが接続解除されて削除されます。インスタンスの電源がオンになると、OS ディスクが基本ディスクから再作成され、既存のインスタンスに接続されます。

Azure Gen2 イメージをサポート。Gen2 スナップショットまたは Gen2 管理対象ディスクのいずれかを使用して Gen 2 VM カタログをプロビジョニングし、起動時のパフォーマンスを向上させることができるようになりました。詳しくは、「マシンカタログの作成」を参照してください。次のオペレーティングシステムは、Azure Gen2 イメージでサポートされています:

- Windows Server 2019、2016、2012、および 2012 R2
- Windows 10

> 注:
>
> Gen1 スナップショットまたは管理対象ディスクを使用した Gen2 マシンカタログの作成はサポートされていません。同様に、Gen2 スナップショットまたは管理対象ディスクを使用した Gen1 マシンカタログの作成もサポートされていません。詳しくは、「Azure での第 2 世代仮想マシンのサポート」を参照してください。

テーブルストレージアカウントの無効化。Machine Creation Services（MCS）は、Azure で VDA をプロビジョニングするときに管理対象ディスクを使用するカタログのテーブルストレージアカウントを作成しなくなりました。詳しくは、「Azure テーブルストレージ」を参照してください。

ストレージアカウントのロックを排除。管理対象ディスクを使用して Azure でカタログを作成すると、ストレージアカウントは作成されなくなります。既存のカタログ用に作成されたストレージアカウントは変更されません。この変更は、管理対象ディスクにのみ適用されます。非管理ディスクの場合は、既存の動作に変更はありません。Machine Creation Services（MCS）は、引き続きストレージアカウントとロックを作成します。

Web Studio で利用可能な新機能。Web ベースのコンソールで、次の機能が使用できるようになりました:

- 顧客が管理する暗号化キーを使用して、マシン上のデータを暗号化します。Studio は、顧客が管理する暗号化キーと呼ばれる設定を ［マシンカタログのセットアップ］ **>** ［ディスク設定］ページに追加するようになりました。この設定では、カタログでプロビジョニングされるマシンのデータを暗号化するかどうかを選択できます。詳しくは、「顧客が管理する暗号化キー」を参照してください。
- **Studio** は、**Autoscale** をタグ付きマシンに制限することをサポートするようになりました。以前は、Autoscale をデリバリーグループ内の特定のマシンに制限するために PowerShell を使用する必要がありました。Studio も使用できるようになりました。詳しくは、「デリバリーグループの特定マシンに対する Autoscale の制限」を参照してください。

2021 年 **3** 月

新機能と機能強化

Azure 専用ホスト。Azure 専用ホストを使用すると、一人の顧客専用のハードウェア上に仮想マシンをプロビジョニングできます。専用ホストを使用している間、Azure は、仮想マシンがそのホストで実行されている唯一のマシンであることを保証します。このため、顧客により多くの制御と表示が提供され、規制または内部のセキュリティ要件を確実に満たすことができます。`HostGroupId`パラメーターを使用する場合は、ホスティングユニットの領域に

事前構成された Azure ホストグループが必要です。また、Azure の自動配置が必要です。詳しくは、「Azure 専用ホスト」を参照してください。

> ヒント:
>
> Azure 専用ホストを使用する場合、**Azure Availability Zones** を選択しても効果はありません。仮想マシンは、Azure の自動配置プロセスによって配置されます。

Azure サーバー側の暗号化をサポート。Citrix Virtual Apps and Desktops サービスは、Azure Managed Disks の顧客が管理する暗号化キーをサポートします。このサポートにより、独自の暗号化キーを使用してマシンカタログの管理対象ディスクを暗号化して、組織およびコンプライアンスの要件を管理できます。詳しくは、「Azure サーバー側暗号化」を参照してください。

Azure の指定されたアベイラビリティゾーンにマシンをプロビジョニング。Azure 環境の特定のアベイラビリティゾーンにマシンをプロビジョニングできるようになりました。この機能を使用すると、次のような利点があります:

- Azure で 1 つまたは複数のアベイラビリティゾーンを指定できます。複数のゾーンが提供されている場合、マシンは形式上、提供されているすべてのゾーンに均等に分散されます。
- 仮想マシンと対応するディスクは、指定された 1 つまたは複数のゾーンに配置されます。
- 特定のサービスオファリングまたはリージョンのアベイラビリティゾーンを参照できます。有効なアベイラビリティゾーンは、PowerShell コマンドを使用して表示します。`Get-Item`を使用してサービスオファリングのインベントリアイテムを表示します。

詳しくは、「Azure の指定されたアベイラビリティゾーンにマシンをプロビジョニング」を参照してください。

Web Studio で利用可能な新機能。Web ベースのコンソールで、次の機能が使用できるようになりました:

- **Studio** で、アプリとカスタムアイコンを関連付けることができるようになりました。以前は、PowerShell を使用して、公開アプリケーションで使用するカスタムアイコンを追加する必要がありましたが、これを、Studio を使用して行うことができるようになりました。詳しくは、「アプリケーショングループの管理」を参照してください。
- **Studio** で、マシンカタログにタグを適用できるようになりました。以前は、Studio でカタログに使用するタグを作成または削除できました。ただし、タグをカタログに適用するには、PowerShell を使用する必要がありました。それが、デリバリーグループの場合と同様に、Studio を使用してタグをカタログに適用したりカタログからタグを削除したりできるようになりました。詳しくは、「マシンカタログへのタグの適用」を参照してください。
- **Studio** で、「水平負荷分散」モードと「垂直負荷分散」モードの切り替えができるようになりました。以前は、水平負荷分散モードと垂直負荷分散モードを切り替えるには、PowerShell を使用するしかありませんでした。Studio により、マルチセッション OS マシンの負荷分散方法をより柔軟に制御できるようになりました。詳しくは、「マシンの負荷分散」を参照してください。
- **Studio** で、再起動スケジュールにメンテナンスモードのマシンを含めることができるようになりました。以前は、メンテナンスモードのマシンを再起動するスケジュールは PowerShell でしか構成できませんでした。

Studio を使用して、これらのマシンを再起動スケジュールに含めるかを制御できるようになりました。詳しくは、「再起動スケジュールの作成」を参照してください。

- **Studio** で、リモート **PC** アクセス用の **Wake on LAN** を構成できるようになりました。以前は、PowerShell を使用してリモート PC アクセス用に Wake on LAN を構成する必要がありましたが、Studio を使用して機能を構成することもできるようになりました。詳しくは、「Wake on LAN の構成」を参照してください。
- **Studio** で、**AWS** インスタンスのプロパティの適用と運用リソースのタグ付けができるようになりました。MCS を使用して AWS でマシンをプロビジョニングするカタログを作成する場合、IAM の役割とタグのプロパティをそれらのマシンに適用するかを指定できます。マシンタグを運用リソースに適用するかを指定することもできます。次の 2 つのオプションが使用できます:
  - マシンテンプレートのプロパティを仮想マシンに適用する
  - 運用リソースにマシンタグを適用する

  詳しくは、「AWS インスタンスのプロパティの適用および運用リソースのタグ付け」を参照してください。

Azure Shared Image Gallery。Citrix Virtual Apps and Desktops サービスは、Azure で MCS プロビジョニングされたマシンの公開イメージリポジトリとして Azure Shared Image Gallery をサポートしています。管理者は、イメージをギャラリーに保存して、OS ディスクの作成とハイドレーションを高速化することができます。このプロセスにより、非永続仮想マシンの起動時間とアプリケーションの起動時間が改善されます。この機能について詳しくは、「Azure Shared Image Gallery」を参照してください。

> 注:
>
> Shared Image Gallery の機能は、管理対象ディスクと互換性があります。従来のマシンカタログでは使用できません。

マシンカタログと同じ **Google Cloud Platform** リージョンで作成されたストレージバケット。以前のリリースでは、MCS は、ディスクアップロードプロセスの一部としてプロビジョニング中に一時ストレージバケットを作成していました。これらのバケットは複数のリージョンにまたがっており、Googleはこれらを 2 つ以上の地理的場所を含む大きな地理的領域として定義しています。これらの一時バケットは、カタログがプロビジョニングされた場所に関係なく、米国の地理的な場所に存在していました。現在 MCS は、カタログをプロビジョニングするのと同じリージョンにストレージバケットを作成するようになりました。ストレージバケットは一時的なものではなくなり、プロビジョニングプロセスを完了した後も、Google Cloud Platform プロジェクト内に残ることになります。今後のプロビジョニング操作では、既存のストレージバケットがそのリージョンに存在する場合は、そのストレージバケットを使用します。指定されたリージョンにストレージバケットが存在しない場合は、新しいストレージバケットが作成されます。

2021 年 2 月

新機能と機能強化

Azure Gen2 イメージをサポート。Azure 環境で Gen2 VM を使用して管理対象ディスクをプロビジョニングし、起動時のパフォーマンスを向上させることができるようになりました。次のオペレーティングシステムがサポートされています:

- Windows Server 2019、2016、2012、および 2012 R2
- Windows 10

> 注:
>
> このサポートでは、VM のサブセットのみがサポートされます。たとえば、一部の VM は Gen1 と Gen2 の両方の種類にすることができ、他の VM は Gen1 のみにすることができます。詳しくは、「Azure での第 2 世代仮想マシンのサポート」を参照してください。

マシンの再起動スケジュール。Citrix Studio の ［再起動の間隔］メニューに、［セッションのドレイン後にすべてのマシンを再起動する］というオプションが追加されました。このオプションを使用すると、すべてのセッションをドレインした後にすべてのマシンを再起動するかどうかを選択できます。再起動時間に達し、すべてのセッションがログオフされると、マシンはドレイン状態になり再起動されます。詳しくは、「再起動スケジュールの作成」を参照してください。

Web Studio で利用可能な新機能。Web ベースのコンソールで、次の機能が使用できるようになりました:

- **Studio** で、**CSV** ファイルを使用してマシンをカタログに一括追加できるようになりました。この機能を使用すると、CSV ファイルを使用して次のことを実行できます:
  - マシンが Studio で電源管理されていない場合のマルチセッション OS またはシングルセッション OS カタログにマシンを一括追加する。
  - リモート PC アクセスカタログにマシンを一括追加する。以前は、リモート PC アクセスカタログにマシンを一括追加するためには、OU を選択する必要がありましたが、OU 構造の制限があるシナリオでは、簡単な作業ではありませんでした。この機能により、マシンを一括追加する柔軟性が得られます。（ユーザーの自動割り当てで使用するため）マシンのみを追加することも、ユーザーの割り当てとともにマシンを追加することもできます。

  詳しくは、「マシンカタログの作成」および「マシンカタログの管理」を参照してください。
- **Citrix Managed Azure** の拡張サポート。次の Citrix Virtual Apps and Desktops サービスエディションで、Citrix Managed Azureが利用できるようになりました: Standard for Azure、Advanced、Premium、および Workspace Premium Plus。
- **Azure Shared Image Gallery** へのマスターイメージの配置のサポート。Studio には、マスターイメージを Azure Shared Image Gallery（SIG）に配置するオプションが用意されています。SIG は、画像を管理および共有するためのリポジトリです。これにより、組織全体でイメージを利用できるようになります。大規模

な永続的でないマシンカタログを作成する場合は、よりすばやく VDA OS ディスクをリセットできるため、マスターイメージを SIG に保存することをお勧めします。詳しくは、「Microsoft Azure Resource Manager 仮想化環境」を参照してください。

- **MCS** マシンカタログ用のシステムディスクを **Azure** に保持します。Studio では、電源サイクル中に VDA 用のシステムディスクを保持するかどうかを制御できるようになりました。通常、システムディスクはシャットダウン時に削除され、スタートアップ時に再作成されます。これにより、ディスクは常にクリーンな状態になりますが、VM の再起動時間が長くなります。システムからの書き込みがキャッシュにリダイレクトされ、キャッシュディスクに書き戻される場合、システムディスクは変更されません。不要なディスクが再作成されないようにするには、［マシンカタログのセットアップ］**>**［ディスク設定］ページにある ［電源サイクル中にシステムディスクを保持する］オプションを使用します。このオプションを有効にすると、VM の再起動時間は短縮されますが、ストレージコストは増加します。このオプションは、再起動時間に注意が必要なワークロードが環境に含まれているシナリオで役立ちます。詳しくは、「MCS ストレージ最適化」を参照してください。
- **Studio** で、永続的なライトバックキャッシュディスクの **MCS** マシンカタログの作成がサポートされるようになりました。これまでは、永続的なライトバックキャッシュディスクのカタログを作成するには、PowerShell を使用するしかありませんでした。現在は Studio を使用して、カタログの作成時に Azure でプロビジョニングされた VM に対してライトバックキャッシュディスクを保持するかどうかを制御できるようになっています。無効にすると、ストレージコストを節約するために、各電源サイクル中にライトバックキャッシュディスクが削除され、ディスクにリダイレクトされたデータはすべて失われます。データを保持するには、［マシンカタログのセットアップ］**>**［ディスク設定］ページにある ［永続的なライトバックキャッシュディスクを使用する］オプションを有効にします。詳しくは、「MCS ストレージ最適化」を参照してください。

StoreFront を使用した **Citrix Virtual Apps and Desktops** サービスの **App Protection** のサポート。詳しくは、「App Protection」を参照してください。

2021 年 **1** 月

Web Studio で利用可能な新機能。Web ベースのコンソールで、次の機能が使用できるようになりました:

- **Studio** で、アプリとカスタムアイコンを関連付けることができるようになりました。以前は、PowerShell を使用して、公開アプリケーションで使用するカスタムアイコンを追加する必要がありましたが、これを、Studio を使用して行うことができるようになりました。詳しくは、「アプリケーショングループの管理」を参照してください。
- **Studio** で、マシンカタログにタグを適用できるようになりました。以前は、Studio でカタログに使用するタグを作成または削除できました。ただし、タグをカタログに適用するには、PowerShell を使用する必要がありました。それが、デリバリーグループの場合と同様に、Studio を使用してタグをカタログに適用したりカタログからタグを削除したりできるようになりました。詳しくは、「マシンカタログへのタグの適用」を参照してください。
- **Studio** で、「水平負荷分散」モードと「垂直負荷分散」モードの切り替えができるようになりました。以前は、水平負荷分散モードと垂直負荷分散モードを切り替えるには、PowerShell を使用するしかありませんでし

た。Studio により、マルチセッション OS マシンの負荷分散方法をより柔軟に制御できるようになりました。詳しくは、「マシンの負荷分散」を参照してください。

- **Studio** で、再起動スケジュールにメンテナンスモードのマシンを含めることができるようになりました。以前は、メンテナンスモードのマシンを再起動するスケジュールは PowerShell でしか構成できませんでした。Studio を使用して、これらのマシンを再起動スケジュールに含めるかを制御できるようになりました。詳しくは、「再起動スケジュールの作成」を参照してください。
- **Studio** で、リモート **PC** アクセス用の **Wake on LAN** を構成できるようになりました。以前は、PowerShell を使用してリモート PC アクセス用に Wake on LAN を構成する必要がありましたが、Studio を使用して機能を構成することもできるようになりました。詳しくは、「Wake on LAN の構成」を参照してください。
- **Studio** で、**AWS** インスタンスのプロパティの適用と運用リソースのタグ付けができるようになりました。MCS を使用して AWS でマシンをプロビジョニングするカタログを作成する場合、IAM の役割とタグのプロパティをそれらのマシンに適用するかを指定できます。マシンタグを運用リソースに適用するかを指定することもできます。次の 2 つのオプションが使用できます:

  - マシンテンプレートのプロパティを仮想マシンに適用する
  - 運用リソースにマシンタグを適用する

  詳しくは、「AWS インスタンスのプロパティの適用および運用リソースのタグ付け」を参照してください。
- **AWS** 専用ホスト。Citrix Studio の ［マシンカタログのセットアップ］ **>** ［セキュリティ］ページに、［専用のホストを使用する］というオプションが追加されました。この設定は、ライセンス制限やセキュリティ要件により、専用ホストを使用する必要がある展開に適しています。専用のホストを使用すると、物理ホスト全体を所有することになり、時間単位で課金されます。ホストを所有すると、追加料金なしで、そのホストが許可する数の EC2 インスタンスをスピンアップできます。詳しくは、「AWS テナント」を参照してください。
- **Studio** で、再起動スケジュールをすぐに実行できるようになりました。Studio では、再起動スケジュールをすぐに実行し、そのスケジュールで該当するすべてのマシンを再起動できるようになりました。詳しくは、「再起動スケジュールの即時実行」を参照してください。
- **Autoscale**。Autoscale は、次の新機能と拡張機能を提供します:

  - **Studio** で、ドレイン状態のマシンを表示できるようになりました。以前は、PowerShell でしかドレイン状態のマシンを特定できませんでした。Studio を使用して、ドレイン状態のマシンを特定できるようになりました。詳しくは、「ドレイン状態のマシンの表示」を参照してください。
  - **Studio** で、**VDI** デリバリーグループのピーク時間を **30** 分の細かいレベルで定義できるようになりました。以前は、スケジュールに含まれる日のピーク時間を 30 分の細かいレベルで定義するには、PowerShell コマンドを使用する必要がありました。これを、Studio を使用して行うことができるようになりました。VDI デリバリーグループで実行する最小マシン数を、各日の 30 分ごとに個別に設定できます。

Azure Shared Image Gallery。Citrix Virtual Apps and Desktops サービスは、Azure で MCS プロビジョニングされたマシンの公開イメージリポジトリとして Azure Shared Image Gallery をサポートしています。管理者

は、イメージをギャラリーに保存して、マスターイメージからの OS ディスクの作成とハイドレーションを高速化することができます。このプロセスにより、非永続仮想マシンの起動時間とアプリケーションの起動時間が改善されます。

ギャラリーには、次の 3 つの要素が含まれています:

- ギャラリー。イメージはここに保存されます。MCS は、マシンカタログごとに 1 つのギャラリーを作成します。
- ギャラリーイメージの定義。この定義には、マスターイメージに関する情報（オペレーティングシステムの種類と状態、Azure リージョン）が含まれます。MCS は、カタログ用に作成されたマスターイメージごとに 1 つのイメージ定義を作成します。
- ギャラリーイメージバージョン。Shared Image Gallery の各イメージには複数のバージョンを含めることができ、各バージョンには異なるリージョンに複数のレプリカを含めることができます。各レプリカは、マスターイメージの完全なコピーです。Citrix Virtual Apps and Desktops サービスでは、カタログのリージョンにおいて適切なレプリカ数を持つ各イメージに対して、Standard_LRS イメージバージョン（バージョン 1.0.0）が常に 1 つ作成されます。この構成は、カタログ内のマシンの数、構成されたレプリカの比率、および構成されたレプリカの最大数に基づいています。

> 注:
>
> Shared Image Gallery 機能は、管理対象ディスクでのみ機能します。従来のマシンカタログでは使用できません。

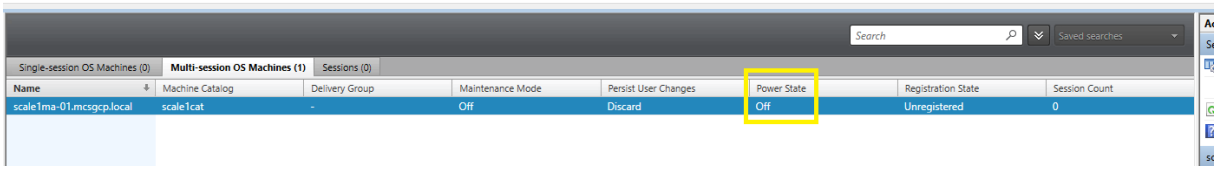
この機能について詳しくは、「Shared Image Gallery を構成する」を参照してください。

マシンカタログと同じ **Google Cloud Platform** リージョンで作成されたストレージバケット。以前のリリースでは、MCS は、ディスクアップロードプロセスの一部としてプロビジョニング中に一時ストレージバケットを作成していました。これらのバケットは複数のリージョンにまたがっており、Googleはこれらを 2 つ以上の地理的場所を含む大きな地理的領域として定義しています。これらの一時バケットは、カタログがプロビジョニングされた場所に関係なく、米国の地理的な場所に存在していました。現在 MCS は、カタログをプロビジョニングするのと同じリージョンにストレージバケットを作成するようになりました。ストレージバケットは一時的なものではなくなり、プロビジョニングプロセスを完了した後も、Google Cloud Platform プロジェクト内に残ることになります。今後のプロビジョニング操作では、既存のストレージバケットを使用します。既存のストレージバケットがそのリージョンに存在する場合はそれが使用され、指定されたリージョンにストレージバケットが存在しない場合は新しいストレージバケットが作成されます。

停止中にプールされた **VDA** を再利用するようにデフォルトを設定する **PowerShell** オプション。新しい PowerShell コマンドオプション（`-DefaultReuseMachinesWithoutShutdownInOutage`）を使用すると、停止中にシャットダウンされなかったプールデスクトップ VDA を再利用するデフォルト設定になります。「アプリケーションとデスクトップのサポート」を参照してください。

Google Cloud Platform のオンデマンドプロビジョニング。Citrix Virtual Apps and Desktops サービスでは、Google Cloud Platform（GCP）がマシンカタログをプロビジョニングする方法が更新されます。マシンカタログを作成する場合、対応するマシンインスタンスは GCP で作成されず、電源状態は **OFF** に設定されます。マシンは、

カタログの作成時にプロビジョニングされるのではなく、マシンの電源が最初にオンになったときにプロビジョニングされます。たとえば、カタログを作成すると、仮想マシンの電源状態が オフに設定されます:

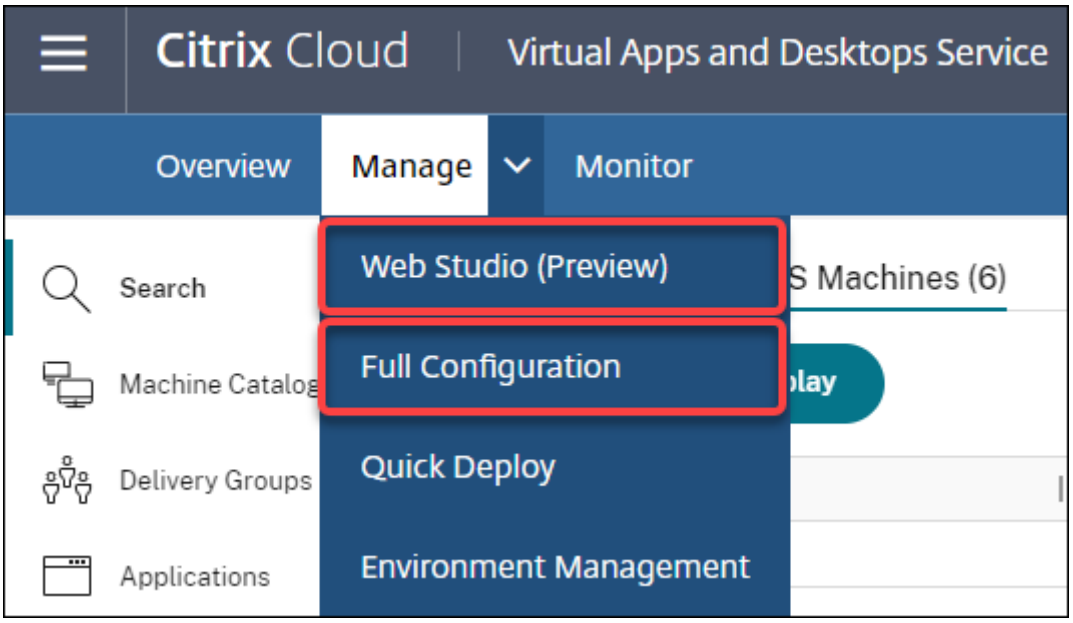


2020 年 12 月

新機能と機能強化

Web Studio はプレビューとして利用できます。新しい Web ベースのコンソールが利用可能になりました。現在、Studio の全機能を従来のコンソールから新しい Web ベースのコンソールに移行中です。Web ベースのコンソールは通常、従来のコンソールよりも速く応答します。デフォルトでは、Web ベースのコンソールに自動的にログオンします。［管理］タブ内から Web ベースのコンソールと従来のコンソールを簡単に切り替えて、構成タスクやサイト管理タスクを実行できます。［管理］の横にある下矢印をクリックして、以下のいずれかのオプションを選択します:

- **Web Studio**（プレビュー）: 新しい Web ベースのコンソールに移動します。
- 完全な構成: 従来のコンソールに移動します。



次の機能は、Web ベースのコンソールでのみ使用できます:

- **Azure** の標準 **SSD** タイプのディスクのサポート。Studio に、標準 SSD タイプのディスクに対するサポートが追加されました。Azure の標準 SSD は、低 IOPS レベルで安定したパフォーマンスを必要とするワークロードに最適化された、コスト効率の高いストレージオプションです。詳しくは、「Azure Resource Manager マスターイメージを使用してマシンカタログを作成する」を参照してください。

- **Studio** では、静的な **VDI** デリバリーグループにおける電源オフの遅延の構成をサポートするようになりました。これまでは、静的な VDI デリバリーグループにおける電源オフの遅延の構成は、PowerShell SDK を介して実行していました。現在 Studio では、静的な VDI デリバリーグループの電源オフの遅延を、Autoscale ユーザーインターフェイスで構成できるようになりました。詳しくは、「Autoscale」を参照してください。

2020 年 10 月

新機能と機能強化

複数のハイパーバイザー通知を破棄します。Citrix Monitor は、2 日以上経過したハイパーバイザー通知の自動破棄をサポートするようになりました。詳しくは、「ハイパーバイザーアラートの監視」を参照してください。

外部 **IP** アドレスを削除します。Google Cloud Platform（GCP）でプロビジョニングされたイメージを準備するためには一時的な VM の外部 IP アドレスが必要であるという要件がなくなりました。この外部 IP アドレスにより、一時的な VM は Google パブリック API にアクセスして、プロビジョニングプロセスを完了することができます。

VM がサブネットから直接 Google パブリック API にアクセスできるようにするには、プライベート Google アクセスを有効にします。詳しくは、「Google プライベートアクセスの有効化」を参照してください。

新しいモデルではマシン **ID** の管理方法を改善しています。マシンカタログで使用されるマシン ID は、Active Directory を使用して管理および保守されてきました。今後、MCS によって作成されたすべてのマシンは Active Directory に参加します。新しい Citrix Virtual Apps and Desktops サービスモデルでは、マシン ID の管理方法を改善しています。このモデルでは、ワークグループまたはドメイン非参加マシンを使用して、マシンカタログを作成できます。

> ヒント：
>
> この機能は、ドメイン非参加マシン用に Citrix Cloud に追加された新しい ID サービスである *FMA* トラストをサポートしています。

MCS は、ID 管理のために新しい FMA トラストサービスと通信します。ID 情報は、Active Directory で使用されるドメインの SID（セキュリティ識別子）とマシンアカウントのパスワードのパラダイムではなく、GUID と秘密キーのペアとして、ID ディスクに保存されます。ドメイン非参加マシンを使用する VDA は、ブローカーの登録にこの GUID と秘密キーの組み合わせを使用します。詳しくは、「ドメイン非参加カタログのサポートの構成」を参照してください。

Azure 管理対象ディスクに直接アップロードを使用します。このリリースでは、Azure 環境で管理対象ディスクを作成するときに直接アップロードを使用できます。この機能により、追加のストレージアカウントに関連するコストが削減されます。管理対象ディスクに変換する前に、VHD をストレージアカウントにステージングする必要がなくなりました。また、直接アップロードにより、空の管理対象ディスクを仮想マシンに接続する必要がなくなります。Azure 管理対象ディスクに直接アップロードすると、オンプレミスの VHD を直接コピーして管理対象ディスクとして使用できるため、ワークフローが簡素化されます。サポートされている管理対象ディスクには、標準 HDD、標準 SSD、およびプレミアム SSD などがあります。

この機能について詳しくは、Microsoft Azure のブログを参照してください。

Azure Managed Disks について詳しくは、このドキュメントページを参照してください。

Azure の単一のリソースグループ。Citrix Virtual Apps and Desktops でカタログを更新および作成するための単一の Azure リソースグループを作成して使用できるようになりました。この拡張機能は、フルスコープと狭いスコープの両方のサービスプリンシパルに適用されます。
以前の、Azure リソースグループごとに仮想マシンは 240、管理対象ディスクは 800 という数の制限はなくなりました。Azure リソースグループごとの VM、管理対象ディスク、スナップショット、およびイメージの数の制限はなくなりました。

詳しくは、「Microsoft Azure Resource Manager 仮想化環境」を参照してください。

2020 年 9 月

新機能と機能強化

クイック展開。新しいクイック展開機能は、以前の Azure クイック展開に置き換わるものです。この新機能は、Microsoft Azure を使用して Citrix Virtual Apps and Desktops サービスを開始するための迅速な方法を提供します。クイック展開を使用して、デスクトップとアプリを配信し、リモート PC アクセスを構成できます。

セッション管理者（組み込みの役割）。Citrix Studio には、新しい組み込みの役割としてセッション管理者が追加されました。この役割により、管理者は ［監視］タブの ［フィルター］ページでデリバリーグループを表示し、関連するセッションとマシンを管理できます。この機能を使用すると、既存の管理者または招待した管理者のアクセス権限を、組織での役割に合わせて構成できます。組み込みの役割について詳しくは、「組み込みの役割とスコープ」を参照してください。組み込みの役割を管理者に割り当てる方法については、「委任管理と監視」を参照してください。

セッションとマシンに関連する ［フィルター］ページへのアクセスをさらに詳細に制御するには、カスタム役割を作成し、Director オブジェクトについて次のいずれかを選択します：［フィルターページの表示 - マシンのみ］、［フィルターページの表示 - セッションのみ］。カスタム役割の作成について詳しくは、「役割の作成と管理」を参照してください。

新しいマシンの種類のサポート。このリリースでは、マシンカタログ用にプレミアムディスクを構成するときに使用できる、AMD マシンの NV v4 および DA v4 シリーズがサポートされるようになりました。詳しくは、「デリバリーグループの作成」を参照してください。

2020 年 8 月

新機能と機能強化

停止状態中に **Remote PowerShell SDK** へのアクセスを制限。以前は、停止状態中に PowerShell コマンドを使用できませんでした。現在、ローカルホストキャッシュにより、停止状態中に Remote PowerShell SDK へのアクセスを制限できます。「停止状態中にできなくなること」を参照してください。

2 つの新しい **Citrix Virtual Apps and Desktops** サービスエディションのサポート。Citrix Monitor は現在、2 つの新しい Citrix Virtual Apps and Desktops サービスエディション、すなわち、**Citrix Virtual Apps Advanced** サービスと **Citrix Virtual Apps and Desktops Advanced** サービスをサポートしています。詳しくは、Citrix Monitor の「機能の互換性マトリックス」を参照してください。

Google Cloud Platform での共有仮想プライベートクラウド（**VPC**）のサポート。Citrix Virtual Apps and Desktops サービスは、Google Cloud Platform 上の共有 VPC をホストリソースとしてサポートするようになりました。マシン作成サービス（MCS）を使用して、共有 VPC 内のマシンをプロビジョニングし、Citrix Studio を使用して管理できます。共有 VPC について詳しくは、「共有仮想プライベートクラウド」を参照してください。

Google Cloud Platform のゾーン選択のサポート。Citrix Virtual Apps and Desktops サービスでは、Google Cloud Platform でのゾーン選択がサポートされています。この機能により、管理者はカタログ作成のために、リージョン内の 1 つまたは複数のゾーンを指定できます。

単一テナントタイプの VM の場合、ゾーン選択により、管理者は選択したゾーン間に単一のテナントノードを配置できます。単一ではないテナントタイプの VM の場合、ゾーンの選択により、選択したゾーン間に VM を確定的に配置できるため、環境を柔軟に設計できます。構成情報については、「ゾーン選択の有効化」を参照してください。

また、次の点についても考慮してください:

- 単一テナントにより、単一テナントノードに排他的にアクセスできます。単一テナントノードは、プロジェクトの VM のみをホストする専用の物理的な Compute Engine サーバーです。これらのノードにより、同じハードウェア上で VM をグループ化したり、他のプロジェクトの VM から分離したりできます。
- 単一テナントノードにより、ライセンス持ち込み（BYOL）シナリオ専用のハードウェア要件を満たすことができます。また、単一テナントノードにより、ネットワークアクセスコントロールポリシー、セキュリティ、および HIPAA などのプライバシー要件に準拠できます。

> 注:
>
> 単一テナントは、Google Cloud で Windows 10 VDI 環境を使用する唯一の方法です。サーバー VDI はこの方法もサポートしています。単一テナントの詳細は、Google ドキュメントサイトで説明しています。

Azure システムディスクの起動パフォーマンスが向上しました。このリリースでは、MCSIO が有効な場合、Azure を使用した Citrix Cloud 実装の起動パフォーマンスが向上しています。このサポートにより、システムディスクを保持できます。これには、次のような利点があります:

- ゴールデンイメージの提供と同様のパフォーマンスで、仮想マシンとアプリケーションを起動できます。
- VM の削除時に発生していた、API クォータ消費、システムディスクの削除と作成、状態遷移の遅延が軽減されます。

たとえば、`New-ProvScheme`コマンドで PowerShell カスタムプロパティ`PersistOSDisk`を使用してこの機能を構成します。

```
1 -CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com
     /2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/
     XMLSchema-instance">
```



```
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
     />
3 <Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="ResourceGroups" Value="
    benvaldev5RG3" />
5 <Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
    />
6 </CustomProperties>'
7 <!--NeedCopy-->
```

構成について詳しくは、「起動パフォーマンスの向上」を参照してください。

2020 年 7 月

新機能と機能強化

［フィルター］ページへの詳細な、役割ベースのアクセスをサポート。Citrix Studio では、カスタム役割を作成する場合の ［モニター］**>** ［フィルター］ページへのアクセスをより詳細に制御できるようになりました。具体的には、任意の組み合わせでマシン、セッション、接続、アプリケーションインスタンスを表示する権限を、カスタム役割に割り当てることができます。［役割の作成］ウィンドウの ［**Director**］オブジェクトには、次の 4 つのオプションが追加されています:

- フィルターページの表示 - アプリケーションインスタンスのみ
- フィルターページの表示 - 接続のみ
- フィルターページの表示 - マシンのみ
- フィルターページの表示 - セッションのみ

役割の作成については、「役割の作成と管理」を参照してください。

割り当てられた **VDI** マシンで電源オフの遅延をサポート（**PowerShell** のみ）。以前のリリースでは、電源オフの遅延は、割り当てられていないマシンにのみ適用されていました。このリリース以降、電源オフの遅延は、マシンが割り当て済みかどうかにかかわらず適用されます。詳しくは、「Autoscale によるマシンの電源管理方法」を参照してください。

Windows クライアントライセンスをサポート。Citrix Virtual Apps and Desktops サービスで、Windows クライアントライセンスを使用して Azure に仮想マシンをプロビジョニングできるようになりました。Windows 10 の VM を Azure で実行するには、マイクロソフトとのボリュームライセンス契約がこの使用に適格であることを確認してください。詳しくは、「Azure Resource Manager マスターイメージを使用してマシンカタログを作成する」を参照してください。

2020 年 5 月

新機能と機能強化

マシンの再起動スケジュール。再起動スケジュールがメンテナンスモードのマシンに影響するかどうかを指定できるようになりました。この機能は、PowerShell のみで利用可能です。詳しくは、「メンテナンスモードのマシンのスケジュールされた再起動」を参照してください。

リソースの可用性。すべてのゾーン（リソースの場所）でリソースを公開することなく、停止状態中にリソースの可用性を確保できるようになりました。詳しくは、「リソースの可用性」を参照してください。

2020 年 4 月

新機能と機能強化

VDI デリバリーグループのスケジューリング精度が向上しました（**PowerShell** のみ）。Autoscale では、スケジュールに含まれる日のピーク時間を、30 分の細かいレベルで定義できるようになりました。VDI デリバリーグループで実行する最小マシン数を、各日の 30 分ごとに個別に設定できます。また、Autoscale では、VDI デリバリーグループの電源がオンになっているマシンの数を、時間単位ではなく 30 分単位でスケールアップまたはダウンできるようになりました。詳しくは、「Broker PowerShell SDK コマンド」を参照してください。

MTU Discovery。Citrix のプロトコル Enlightened Data Transport（EDT）に、MTU Discovery 機能が導入されました。MTU Discovery を使用すると、EDT でセッションのペイロードサイズを自動的に判断して設定させることができます。この機能により、ICA セッションは、標準以外の最大伝送ユニット（MTU）または最大セグメントサイズ（MSS）要件を持つネットワークに調整できます。この調整機能によって、パフォーマンスの低下や ICA セッションの確立失敗となる可能性のある、パケットのフラグメンテーションが防止されます。この更新には、Windows 向け Citrix Workspace アプリ 1911 以上が必要です。Citrix Gateway を使用している場合、Citrix ADC ファームウェアの最小バージョンは 13.0.52.24 または 12.1.56.22 です。詳しくは、「EDT MTU Discovery」を参照してください。

2020 年 3 月

新機能と機能強化

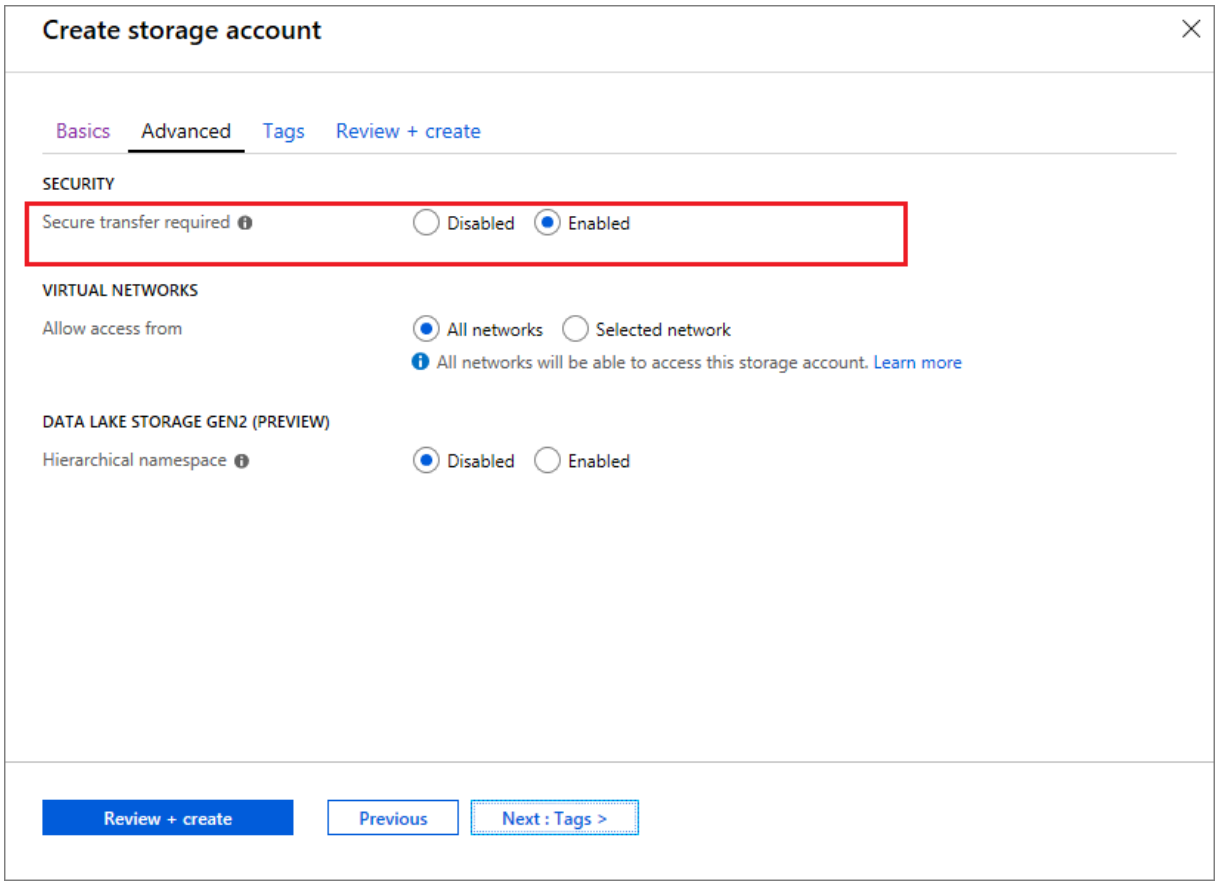
PVS ターゲットデバイスメトリック。Citrix Monitor は、［マシンの詳細］ページに PVS ターゲットデバイスメトリックパネルを配置するようになりました。パネルを使用して、シングルセッション OS およびマルチセッション OS マシンの Provisioning ターゲットデバイスの状態を表示します。このパネルでは［ネットワーク］、［起動］、［キャッシュ］のさまざまなメトリックを表示できます。これらのメトリックは、PVS ターゲットデバイスを監視およびトラブルシューティングして、PVS ターゲットデバイスが稼働していることを確認するのに役立ちます。詳しくは、「PVS ターゲットデバイスメトリック」を参照してください。

AWS インスタンスプロパティのキャプチャ。MCS は AMI が作成されたインスタンスからプロパティを読み取り、マシンの IAM の役割およびタグを目的のカタログにプロビジョニングされたマシンに適用します。このオプション機能を使用する場合、カタログ作成プロセスでは、選択した AMI ソースインスタンスが検索され、限定されたプロパティセットが読み取られます。これらのプロパティは、そのカタログのマシンをプロビジョニングするために使用される AWS 起動テンプレートに保存されます。カタログ内のすべてのマシンがキャプチャされたインスタンスのプロパティを継承します。詳しくは、「AWS インスタンスプロパティのキャプチャ」を参照してください。

AWS 運用リソースのタグ付け。このリリースでは、プロビジョニング中に Citrix コンポーネントで作成されたリソースにタグ付けするオプションを導入します。各タグは、顧客定義のキーおよびオプションの値で構成されたラベルで、より適切にリソースを管理、検索、フィルターするために役立ちます。詳しくは、「AWS 運用リソースのタグ付け」を参照してください。

Azure ストレージでの安全な転送。Machine Creation Services（MCS）では、Azure Resource Manager 環境で MCS プロビジョニングカタログによって作成されたストレージアカウントの機能が拡張されました。この拡張機能は、［安全な転送が必須］プロパティを自動的に有効にします。このオプションは、セキュリティで保護された接続からのアカウントへの要求のみを許可にするため、ストレージアカウントのセキュリティが強化されます。詳しくは、Microsoft 社のサイトで「セキュリティで保護された接続を確保するために安全な転送を要求する」を参照してください。

Azure のストレージアカウントを作成するときに ［安全な転送が必須］プロパティを有効にします:



Azure SSD Managed Disks のサポート。Machine Creation Services（MCS）は、Azure 仮想マシンで Standard

SSD Managed Disks をサポートします。このディスクの種類は安定したパフォーマンスを提供し、HDD ディスクよりも優れた可用性を提供します。詳しくは、「Standard SSD Disks for Azure Virtual machine workloads」を参照してください。

`New-ProvScheme`コマンドまたは`Set-ProvScheme`コマンドで PowerShell `StorageAccountType` カスタムプロパティを使用してこの機能を構成します:

```
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`" Value=`"StandardSSD_LRS`" /><Property xsi:type=`"StringProperty`" Value=`"Windows_Server`" />
<!--NeedCopy-->
```

> 注:
>
> この機能は、カスタムプロパティ`UseManagedDisks`が **true** に設定されているときのみ利用できます。非管理ディスクの場合、標準 HDD やプレミアム SSD のみがサポートされています。

2020 年 1 月

新機能と機能強化

Citrix Studio の言語バー。このリリース以降、Citrix Studio では正しいキーボードマッピングを容易にする言語バーを使用できます。

- Citrix Cloud の言語またはブラウザーの表示言語が英語または日本語に設定されている場合、言語バーが表示されないことがあります。
- Citrix Cloud の言語またはブラウザーの表示言語がドイツ語、スペイン語、またはフランス語に設定されている場合、言語バーは Citrix Studio へのログオン後に表示されます。言語バーの一覧には、2 つの言語オプションがあります。ブラウザーの最上位の言語に一致するオプションを選択します。

  > ヒント:
  >
  > - 言語バーに対して構成した設定が有効にならない場合があります。この場合、いったんログアウトしてから再ログオンします。
  > - 言語バーを使用して、特定の記号や英語以外の文字を入力できない場合があります。この問題を解決するには、Citrix Cloud の言語、Web ブラウザーの表示言語、およびローカルキーボードレイアウトを構成する必要があります。詳しくは、Knowledge Center の記事CTX310743を参照してください。

再起動スケジュールの最大遅延タイマー（**PowerShell** のみ）。サイト構成データベースの停止が原因でデリバリーグループのマシンのスケジュールされた再起動が開始されない場合、スケジュールされた開始時間後の待機時間を指定できます。その時間内にデータベース接続が復元されると、再起動が開始されます。その時間内に接続が復元されない場合、再起動は開始されません。詳しくは、「データベースの停止によるスケジュールされた再起動の遅延」を参照してください。

垂直負荷分散（**PowerShell** のみ）。以前は、サービスではすべての RDS 起動に水平負荷分散が使用されており、受信の負荷を負荷が最小である RDS マシンに割り当てていました。これは引き続きデフォルトの動作です。現在は、PowerShell を使用して、垂直負荷分散をサイト全体の設定として有効化できるようになりました。

垂直負荷分散が有効になっている場合、ブローカーは、負荷が最大であり、まだ最高ウォーターマークに達していないマシンに受信の負荷を割り当てます。これにより、既存のマシンが飽和状態になった後、新しいマシンに移ります。ユーザーが既存のマシンを切断して解放すると、それらのマシンに新しい負荷が割り当てられます。

デフォルトでは、水平負荷分散が有効になっています。垂直負荷分散を表示、有効化、または無効化する場合に、`Get-BrokerSite`および`Set-BrokerSite`コマンドレットが`UseVerticalScalingForRdsLaunches`設定をサポートするようになりました。詳しくは、「デリバリーグループのマシンの負荷管理」を参照してください。

2019 年 12 月

新機能と機能強化

Citrix Service Providers（**CSP**）向けサービス。CSP では、テナント顧客を Virtual Apps and Desktops サービスにオンボードして、サービスへの顧客管理者アクセス権を構成し、フェデレーションドメインを使用して顧客のユーザーに共有または専用のワークスペースを提供できるようになりました。詳しくは、「Citrix Service Provider 用の Citrix Virtual Apps and Desktops サービス」を参照してください。

マシンがメンテナンスモードになっている原因の判別をサポート（**PowerShell** のみ）。PowerShell を使用して、マシンがメンテナンスモードになっている理由を特定できるようになりました。これを行うには、パラメーター`MaintenanceModeReason`を使用します。この機能は、メンテナンスモードでのマシンの問題のトラブルシューティングを管理者が行う場合に役立ちます。詳しくは、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/Broker/Get-BrokerMachine/を参照してください。

Autoscale。Autoscale に、マシンを動的に作成および削除する機能が備わりました。PowerShell スクリプトを使用して、この機能を利用できます。このスクリプトで、現在の負荷条件に基づいて、デリバリーグループ内のマシンの数を動的にスケールアップまたはスケールダウンできます。詳しくは、「Autoscale によるマシンの動的プロビジョニング」を参照してください。

2019 年 11 月

新機能と機能強化

GroomStartHour。［監視］で **GroomStartHour** をサポートするようになりました。管理者がグルーミングの実行を開始する時間を設定できる新しい構成です。詳しくは、Citrix Virtual Apps and Desktops SDKドキュメントを参照してください。

OData Pagination。［監視］で **OData Pagination** をサポートするようになりました。すべての OData v4 エンドポイントは、応答で 1 ページあたり最大 100 レコードと次の 100 レコードへのリンクを返します。詳しくは、「Accessing Monitor Service data using the OData v4 endpoint in Citrix Cloud」を参照してください。

2019 年 10 月

新機能と機能強化

App-V。App-V 機能が Citrix Cloud で利用可能になりました。シングル管理モードまたはデュアル管理モードで、App-V パッケージを Citrix Cloud 構成の Delivery Controller に追加できます。*Virtual Apps and Desktops Service App-V* パッケージ検出モジュールをCitrix のダウンロードページで入手して、App-V パッケージをインポートし、Microsoft App-V サーバーを登録できます。ユーザーはパッケージに含まれるアプリを使用できるようになります。この PowerShell モジュールを使用すると、DNS URL を使用して Microsoft App-V 管理サーバーと公開サーバーを登録できるため、負荷分散メカニズムのサーバーを実際のマシン URL を使用して登録する必要がなくなります。詳しくは、「App-V パッケージおよびサーバー用の Citrix Virtual Apps and Desktops サービス検出モジュール」を参照してください。

Google Cloud Platform。Citrix Virtual Apps and Desktops サービスは、Google Cloud Platform（GCP）でマシンをプロビジョニングするために Machine Creation Services（MCS）を使用するためのサポートを追加しました。詳しくは、「Google Cloud Platform 仮想化環境」を参照してください。

2019 年 9 月

新機能と機能強化

Azure Virtual Desktop の **VDA** サポート。サポートされているオペレーティングシステムと VDA バージョンについては、「Azure Virtual Desktop 環境の VDA」を参照してください。

拡張された電源ポリシー。以前のリリースでは、アクション（切断アクション =「一時停止」または「シャットダウン」）が必要な期間に移行する VDI マシンの電源がオンのままになっていました。このシナリオは、操作（切断アクション =「何もしない」）が不要な期間（ピーク時またはオフピーク時）にマシンが切断された場合に発生しました。

このリリース以降では、指定した切断時間が経過すると、Autoscale はマシンを一時停止または電源をオフにします。これは、その期間に対して構成された切断アクションによって異なります。詳しくは、「セッションが切断された状態で異なる期間に移行する VDI マシンの電源管理」を参照してください。

マシンカタログ：タグ。PowerShell を使用して、マシンカタログにタグを適用できるようになりました。詳しくは、「マシンカタログへのタグの適用」を参照してください。

セッションの開始時間。モニターはセッションの開始時間を Workspace アプリのセッションと VDA のセッションの開始時間に分けて表示するようになりました。このデータはセッションの開始時間が長い場合に問題を把握し、トラブルシューティングを行うのに役立ちます。また、セッションの開始プロセスを構成する各フェーズの実行時間の情報は、それぞれのフェーズに関連する問題のトラブルシューティングに有効です。たとえば、ドライブマッピング

時間が長い場合は、有効なすべてのドライブが GPO やスクリプトで正しくマップされているかどうかを確認できます。この機能は VDA バージョン 1903 以降で使用できます。詳しくは、「セッション開始時の問題の診断」を参照してください。

2019 年 8 月

新機能と機能強化

セッションの自動再接続［傾向］タブの［セッション］ページに、自動再接続数に関する情報が追加されました。自動再接続は、［セッション画面の保持］ポリシーまたは［クライアントの自動再接続］ポリシーが有効な場合に実行されます。自動再接続の情報は中断が発生したネットワーク接続の確認やトラブルシューティングに役立つだけでなく、シームレスなネットワークの分析にも活用できます。

ドリルダウンではセッション画面の保持やクライアントの自動再接続、タイムスタンプ、エンドポイントの IP、Workspace アプリがインストールされているマシンのエンドポイント名などの詳しい情報を確認できます。この機能は、Windows 向け Citrix Workspace アプリ、Mac 向け Citrix Workspace アプリ、Citrix Receiver for Windows、および Citrix Receiver for Mac で使用できます。この機能を使用するには、VDA 1906 以降が必要です。詳しくは、次のトピックを参照してください:

- セッション
- クライアントの自動再接続のポリシー設定
- セッション画面の保持のポリシー設定
- セッションの自動再接続

2019 年 7 月

新機能と機能強化

構成ログ。Remote PowerShell SDK を使用して、構成ログデータベースのコンテンツを定期的に削除できるようになりました。詳しくは、「定期的なデータ削除のスケジュール」を参照してください。

Autoscale。Autoscale には、デリバリーグループ内のマシンのサブセットのみを電源管理できる柔軟性があります。この機能はクラウドの処理が増大した場合に有用であり、クラウドベースのリソースで他の需要（バーストワークロード）が発生する前にオンプレミスのリソースを使用してワークロードを処理できます。詳しくは、「デリバリーグループの特定マシンに対する Autoscale の制限」を参照してください。

ローカルアプリアクセスと **URL** リダイレクト。Citrix Studio では、PowerShell SDK を使用して、サイトの Studio ユーザーインターフェイスに［ローカルアプリアクセスアプリケーションの追加］オプションを追加できるようになりました。詳しくは、「公開アプリケーションへのアクセスのみを提供する」を参照してください。

オペレーティングシステム名の変更。［マシンカタログの作成］**>**［マシンカタログのセットアップ］**>**［オペレーティングシステム］ページおよび ［監視］ページのオペレーティングシステム名が変更されました:

- マルチセッション OS（サーバー OS の新名称）：マルチセッション OS のマシンカタログでは、ユーザーにサーバーの共有デスクトップを提供できます。標準化された Windows マルチセッション OS または Linux OS マシンの大規模展開に適しています。
- シングルセッション OS（デスクトップ OS の新名称）：シングルセッション OS マシンカタログでは、ユーザーの種類に応じて最適な VDI デスクトップを提供できます。

Citrix Profile Management のプロファイルのロード時間。［監視］では、ログオン期間グラフの［プロファイルのロード］バーにプロファイル処理時間が含まれるようになりました。これは、Citrix Profile Management がユーザープロファイルの処理に要する時間です。プロファイルのロードに時間がかかる場合に、管理者が正確にトラブルシューティングのための情報を把握するのに役立ちます。この機能拡張は、VDA 1903 以降で利用できます。詳しくは「プロファイルのロード」を参照してください。

デスクトッププロービング。デスクトッププロービングは、Citrix Virtual Apps and Desktops サービスの機能です。これにより、サイトに公開されている仮想デスクトップのヘルスチェックが自動化されて、ユーザーエクスペリエンスが向上します。デスクトッププロービングを開始するには、Citrix Probe Agent を 1 つまたは複数のエンドポイントにインストールして構成します。デスクトッププロービングは、Premium ライセンスを持つユーザーが使用できます。この機能には、Citrix Probe Agent 1903 以降が必要です。詳しくは、「アプリケーションプロービングおよびデスクトッププロービング」を参照してください。

> 注:
>
> Citrix Probe Agent では、TLS 1.2 がサポートされるようになりました。

2019 年 6 月

新機能と機能強化

タグ制限。タグは、マシン、アプリケーション、デスクトップ、アプリケーショングループ、ポリシーなどのアイテムを識別する文字列です。タグを作成してアイテムに追加すると、以下のように、特定の操作を指定されたタグのあるアイテムのみに適用するように調整できます。詳しくは、「アプリケーショングループ」と「タグ」を参照してください。

メール通知。Citrix Virtual Apps and Desktops サービスは、警告とプローブに関するメール通知を直接送信します。このため、SMTP メールサーバーを構成する必要がありません。［通知設定］ボックスはデフォルトで有効になっており、Citrix Cloud は ［通知設定］セクションに表示されたメールアドレスにアラート通知を送信します。メールアドレス`donotreplynotifications@citrix.com`がメール設定で許可リストに登録されていることを確認してください。

2019 年 5 月

新機能と機能強化

Autoscale。Autoscale は、Citrix Virtual Apps and Desktops サービスの機能であり、プロアクティブにマシンの電源を管理するための、一貫した、高性能なソリューションを提供します。その目的は、コストとユーザーエクスペリエンスのバランスを取ることです。Autoscale により、Smart Scale テクノロジ（廃止）が Studio の電源管理ソリューションに組み込まれます。詳しくは、「Autoscale」を参照してください。［監視］タブの［傾向］ページで Autoscale 管理対象のマシンのメトリックを監視できます。詳しくは、「Autoscale 管理対象マシンの監視」を参照してください。

2019 年 2 月

新機能と機能強化

ハイパーバイザーアラートの監視。Citrix Hypervisor および VMware vSphere からのアラートは ［監視］>［アラート］タブに表示されるようになり、ハイパーバイザーの正常性で以下の状態やパラメーターを監視できます:

- CPU 使用率
- メモリ使用率
- ネットワーク使用状況
- 使用不可のハイパーバイザー接続
- ディスク使用率（vSphere のみ）
- ホスト接続や電源の状態（vSphere のみ）

詳しくは、「アラートおよび通知」の「ハイパーバイザーアラートの監視」セクションを参照してください。

以前のバージョンの **TLS** を使用した通信。サービスのセキュリティを向上させるため、2019 年 3 月 15 日以降、Citrix では Transport Layer Security（TLS）1.0 および 1.1 を介した通信をブロックし、TLS 1.2 による通信のみを許可することになりました。詳しくは、「TLS バージョン」を参照してください。総合的なガイダンスについては、CTX247067を参照してください。

アプリケーショングループ。アプリケーショングループを使用すると、アプリケーションのコレクションを管理できます。異なるデリバリーグループ間で共有されているアプリケーションや、デリバリーグループ内のユーザーのサブセットによって使用されるアプリケーションのアプリケーショングループを作成できます。詳しくは、「アプリケーショングループの作成」を参照してください。

ログオンパフォーマンス - プロファイルドリルダウン。［監視］の ［ユーザーの詳細］ページの ［ログオン期間］パネルに、ログオンプロセスのプロファイルロードフェーズのドリルダウンに関する情報が表示されるようになりました。プロファイルドリルダウンは、現在のセッションのユーザープロファイルに関する有益な情報を提供します。この情報は、管理者がプロファイルのロードに関する重大な問題をトラブルシューティングする際に役立ちます。次のユーザープロファイル情報を含むツールヒントが表示されます:

- ファイルの数
- プロファイルのサイズ
- 大きなファイルの数

詳細なドリルダウンに、個別のフォルダーとそのサイズ、およびファイル数に関する情報が表示されます。この機能は VDA バージョン 1811 以降で使用できます。詳しくは、「ユーザーログオンの問題の診断」を参照してください。

Microsoft RDS ライセンスの正常性。サーバー OS マシンの［マシンの詳細］ページと［ユーザーの詳細］ページの ［マシンの詳細］パネルで、Microsoft RDS（Remote Desktop Services）のライセンスの状態を監視します。ライセンスの状態を示す適切なメッセージが表示されます。詳細アイコン上にマウスポインターを置くと、詳細情報が表示されます。詳しくは、「マシンのトラブルシューティング」の「Microsoft RDS ライセンスの正常性」セクションを参照してください。

アプリケーションプロービング。この機能によって、サイトに公開された Virtual Apps の正常性の評価が自動化されます。

アプリケーションプロービングを開始するには:

- 1 つまたは複数のエンドポイントマシンに、Citrix Application Probe Agent をインストールします。
- Citrix Workspace および Citrix Virtual Apps and Desktops サービスの資格情報で Citrix Application Probe Agent を構成します。
- Citrix Virtual Apps and Desktops サービスの ［監視］>［構成］で、プローブするアプリケーション、プローブを実行するエンドポイントマシン、プローブ時間のスケジュールを構成します。

このエージェントは選択したアプリケーションの起動を Citrix Workspace 経由でテストし、プローブの結果を Citrix Virtual Apps and Desktops サービスの ［監視］タブの以下のページで報告します:

- ［アプリケーションページ］–過去 24 時間のデータおよび ［傾向］ > ［アプリケーションプローブの結果］ページ
- プローブの履歴データとプローブエラーが発生した段階 - Workspace の到達可能性、Workspace の認証、Workspace の列挙、ICA のダウンロード、またはアプリケーションの起動

障害レポートは、設定されているアドレスにメールで送信されます。アプリケーションプローブは、複数の地域にわたってオフピーク時に実行するようにスケジュールできます。このプローブの結果は、アプリケーション、ホストマシン、または接続に関連する問題を、ユーザーが経験する前に予防的にトラブルシューティングするのに役立ちます。詳しくは、「アプリケーションプロービングおよびデスクトッププロービング」を参照してください。

2019 年 1 月

新機能と機能強化

カスタムスコープによる委任管理。監視では、組み込みの委任管理者の役割でカスタムスコープがサポートされるようになりました。監視の組み込みの役割と役割を割り当てる方法について詳しくは、「委任管理者の役割」を参照してください。

2018 年 12 月

新機能と機能強化

Citrix が Transport Layer Security（TLS）1.0 および 1.1 上での通信をブロックする日付が 2018 年 12 月 31 日から 2019 年 1 月 31 日に変更されました。詳しくは、「TLS バージョンの廃止」を参照してください。

2018 年 11 月

新機能と機能強化

OData API を使用したマシン履歴データの取得：マシン分析を含む履歴データを、OData API を介して利用できるようになりました。このデータは 1 時間ごとに収集され、その日にロールアップされます。

- 電源が投入されたマシンの数（電源管理されているマシンの場合）
- 登録されたマシンの数
- メンテナンスモードのマシンの数
- マシンの総数

監視サービスが実行されている期間、データが集約されます。OData API の使用法と例について詳しくは、「Citrix Monitor Service 7 1808」を参照してください。データベーススキーマは、「モニターサービススキーマ」で使用できます。

ログオンパフォーマンス **-** 対話型セッションのドリルダウン：ユーザーやセッションの詳細ビューの ［ログオン期間］パネルに、ログオン処理の対話型セッションのフェーズに関する情報が表示されます。3 つのサブフェーズ（**Pre-userinit**、**Userinit**、および **Shell**）のそれぞれに要した時間は、対話型セッションバーにツールヒントとして表示されます。これにより、ログオンのこのフェーズのより詳細なトラブルシューティングと修復が行われます。サブフェーズとドキュメンテーションへのリンクの間の累積的な時間遅延も提供されます。この機能は、Delivery Controller バージョン 7 1808 以降で使用できます。［対話型セッション］ドリルダウンバーには、現在のセッションの持続時間のみが表示されます。詳しくは、「ユーザーログオンの問題の診断」を参照してください。

ログオンパフォーマンス **- GPO** ドリルダウン：ユーザーおよびセッションの詳細ビューの ［ログオン期間］パネルに、GPO（グループポリシーオブジェクト）の期間が表示されます。これは、ログオンプロセス中に仮想マシンに GPO を適用するのにかかる合計時間です。これで、GPO バーのツールヒントとして CSE（クライアント側拡張機能）ごとに適用された各ポリシーのドリルダウンが表示されます。各ポリシー適用について、ドリルダウンはステータスと経過時間を表示します。この追加情報により、高い GPO 期間に関連する問題のトラブルシューティングと修復が容易になります。ドリルダウンの期間は CSE 処理時間のみを表し、合計 GPO 時間には加算されません。この機能は、Delivery Controller バージョン 7 1808 以降で使用できます。詳しくは、「ユーザーログオンの問題の診断」を参照してください。

解決された問題

監視中に保存したカスタムレポートクエリは、Cloud をアップグレードすると使用できなくなります。[DNA-23420]

2018 年 10 月

新機能と機能強化

アプリケーション：マシンごとの制限。マシンごとにアプリケーションインスタンスの数を制限できるようになりました。この制限は、サイト内のすべてのマシンに適用されます。この制限は、デリバリーグループ内のすべてのユーザーの既存のアプリケーション制限およびユーザーあたりの制限に追加されるものです。この機能は PowerShell を介してのみ使用でき、Studio では使用できません。詳しくは「アプリケーション制限の設定」を参照してください。

Windows Server 2019。「システム要件」に記載されているように、Windows Server 2019 マシンにマルチセッション OS の VDA（以前の VDA for Server OS）をインストールできるようになりました。

2018 年 9 月

新機能と機能強化

委任管理。委任管理により、組織内の役割に応じて管理者に必要となる、すべてのアクセス権限を構成できます。詳しくは、「委任管理」を参照してください。監視は、組み込みの役割の割り当てをサポートします。組み込みの役割は、フルスコープで使用できます。監視の組み込みの役割と役割を割り当てる方法について詳しくは、「委任管理者の役割」を参照してください。

構成ログ。構成ログにより、管理者は構成の変更や管理のアクティビティを追跡できます。詳しくは、「構成ログ」を参照してください。

以前は無効になっていた Remote PowerShell SDK 内の次の PowerShell コマンドレットが有効になり、構成ログとともに使用できるようになりました：

- Log：GetLowLevelOperation
- Log：GetHighLevelOperation
- Log：GetSummary
- Log：GetDataStore
- Log：ExportReport

ローカルホストキャッシュ。ローカルホストキャッシュを十分に利用できるようになりました。ローカルホストキャッシュ機能を使用すると、リソースの場所にある Cloud Connector が Citrix Cloud と通信できなくなった場合でも、接続仲介操作を続行できるようになります。詳しくは、「ローカルホストキャッシュ」を参照してください。

Citrix Provisioning。VDA のプロビジョニングに、Citrix Provisioning または既存の Machine Creation Services を使用できるようになりました。クラウド環境固有の Citrix Provisioning 情報については、「Citrix Cloud で管理される Citrix Provisioning」を参照してください。

解決された問題

以前のバージョンでは、Azure オンデマンドプロビジョニングの使用時は、電源を切るとすべての仮想マシンが削除されました。このバージョンでは、プールされた仮想マシンのみが削除されるようになりました。永続的（専用）の VM は、電源がオフのときに削除されません。

2018 年 8 月

- 新しい製品名

  一定期間 Citrix の顧客かパートナーだった経験がある方は、製品やこの製品ドキュメントに新しい名前が使用されていることにお気付きになるかもしれません。この Citrix 製品を初めてお使いになる場合、製品またはコンポーネントで異なる名前が表示されることがあります。

  新しい製品名とコンポーネント名は、Citrix の製品ラインとクラウド戦略の拡大によるものです。この製品ドキュメントでは、以下の名前を使用します。

  - **Citrix Virtual Apps and Desktops**: Citrix Virtual Apps and Desktops は、クラウドサービスおよびオンプレミス製品として提供される仮想アプリとデスクトップソリューションを提供し、従業員があらゆるデバイス上のどこからでも作業できる自由を確保しつつ IT コストを削減できます。また、Windows、Linux、Web、および SaaS の各アプリケーション、および完全な仮想デスクトップを任意のクラウドから配信できます。クラウドの種類は、パブリック、プライベート、ハイブリッドを問いません。Virtual Apps and Desktops は、以前は XenApp および XenDesktop でした。
  - **Citrix Workspace** アプリ: Citrix Workspace アプリには、既存の Citrix Receiver テクノロジの他に Citrix Workspace クライアントテクノロジが組み込まれています。エンドユーザーに最高の作業を実行するために必要なすべての作業アプリ、ファイル、およびデバイスと対話できる統合されたコンテキスト上のエクスペリエンスをエンドユーザーに提供するための追加機能を提供するように拡張されました。詳しくは、このブログ記事を参照してください。
  - **Citrix SD-WAN**: クラウドテクノロジを使用してブランチネットワークと WAN を変革するお客様やパートナーにとって重要なテクノロジである NetScaler SD-WAN は、Citrix SD-WAN になりました。
  - **Citrix Secure Web Gateway**: Citrix Networking のポートフォリオが拡大してきたため、これまで NetScaler Secure Web Gateway として知られていた堅牢な Citrix Secure Web Gateway サービスを自信をもってご提供します。
  - **Citrix Gateway**: アプリやデータへのセキュアなコンテキストアクセスを可能にする堅牢な NetScaler Unified Gateway が、Citrix Gateway になりました。
  - **Citrix Content Collaboration** および **Citrix Files for Windows**: ShareFile の高度なアクセス、コラボレーション、ワークフロー、権限管理、および統合機能を、セキュアなコンテキスト型統合

Citrix Workspace の Citrix Content Collaboration コンポーネントで利用できるようになりました。Citrix Files for Windows を使用すると、マップされたドライブを介して Content Collaboration ファイルに直接アクセスし、ネイティブの Windows エクスプローラエクスペリエンスを提供できます。

- **Citrix Hypervisor**: XenProject ハイパーバイザーをベースとした仮想化インフラストラクチャ用の XenServer のテクノロジが、Citrix Hypervisor になりました。

ここで簡単に要約します:

新	旧
Citrix Virtual Apps and Desktops	XenApp および XenDesktop
Citrix Workspace アプリ	Citrix Receiver と拡張機能を統合
Citrix SD-WAN	NetScaler SD-WAN
Citrix Secure Web Gateway	NetScaler Secure Web Gateway
Citrix Gateway	NetScaler Unified Gateway
Citrix Content Collaboration	ShareFile
Citrix Files for Windows	ShareFile Desktop App、ShareFile Sync、ShareFile Drive Mapper
Citrix Hypervisor	XenServer
Citrix Provisioning	Citrix Provisioning Services

現在、製品と製品ドキュメントで移行作業が行われています。

- 製品内のコンテンツには、以前の名前が含まれている場合があります。たとえば、コンソールのテキスト、メッセージ、ディレクトリ名またはファイル名に以前の名前が含まれている場合があります。
- 既存の顧客のスクリプトの破損を防ぐために、コマンドや MSI などの一部のアイテムでは、以前の名前を引き続き保持できます。
- 関連する製品ドキュメントや、この製品のドキュメントからリンクされているその他のリソース（ビデオやブログの投稿など）には、以前の名前が含まれている場合があります。
- Citrix Hypervisor の場合: 新しい名前は、2018 年 9 月から Citrix の Web サイトおよび情報提供用の製品資料で使用されています。Citrix Virtual Apps and Desktops など、一部の Citrix 製品の管理者コンソールにも新しい名前が表示されます。XenServer 製品のリリースおよび技術資料では、2019 年の初めまで XenServer 7.x を引き続き使用します。

この移行の間はご迷惑をおかけしますが、何卒ご容赦願います。

新しい名前について詳しくは、https://www.citrix.com/about/citrix-product-guide/を参照してください。

- 製品およびコンポーネントのバージョン番号の変更

Citrix Virtual Apps and Desktops のほとんどのコンポーネントは Citrix がインストールし管理するため、お客様はこれらのバージョン番号を気に掛ける必要はありません。ただし、Cloud Connector をインストールするときや、リソースの場所で VDA をインストールまたはアップグレードするときには、バージョン番号が表示されます。

Citrix Virtual Apps and Desktops 製品およびコンポーネントのバージョン番号は、次の形式で表示されます：**YYMM**。***c.m.b***

- YYMM = 製品またはコンポーネントがリリースされた年と月。たとえば、2018 年 9 月のリリースは 1809 と表示されます。
- c = その月の Citrix Cloud のリリース番号。
- m = 保守バージョン（該当する場合）。
- b = ビルド番号。このフィールドは、コンポーネントの［バージョン情報］ページと、プログラムの削除または変更のための OS 機能にのみ表示されます。

たとえば、**Citrix Virtual Apps and Desktops 1809.1.0** は、そのコンポーネントが 2018 年 9 月にリリースされたことを示します。その月の Citrix Cloud リリース 1 に関連付けられており、メンテナンスバージョンではありません。一部の表記では、バージョンの年と月のみが表示されます：たとえば、**Citrix Virtual Apps and Desktops 1809**。

以前のリリース（7.18 以前）では、バージョン番号は次の形式で表示されました：7.*< バージョン >*。ここで、バージョンはリリースごとに 1 増加します。たとえば、XenApp および XenDesktop 7.17 に続く VDA リリースは 7.18 でした。以前のリリース（7.18 以前）が新しい番号形式を使って更新されることはありません。バージョン >

- **TLS** バージョンの廃止。Citrix Virtual Apps and Desktops サービスのセキュリティを向上させるため、2018 年 12 月 31 日以降、Transport Layer Security（TLS）1.0 および 1.1 を介した通信をブロックすることになりました。詳しくは、「TLS バージョンの廃止」を参照してください。
- **Google Cloud Platform** 仮想化環境。Citrix Virtual Apps and Desktops サービスでは、Google Cloud Platform（GCP）上の Virtual Apps and Desktops 仮想マシンの電源を手動で切断しすぐに投入することができます。詳しくは、「Google Cloud Platform 仮想化環境」を参照してください。

2018 年 7 月

- フィルターデータのエクスポート。［監視］>［フィルター］タブのリアルタイムモニタリングデータを CSV 形式のファイルにエクスポートできるようになりました。エクスポート機能は、マシン、セッション、接続、およびアプリケーションインスタンスのフィルターページで利用できます。定義済みのカスタムフィルターを選択するか、適切なフィルター基準を選択し、テーブルで必要な列を選択して、データをエクスポートすることができます。最大 100,000 レコードのデータをエクスポートできます。エクスポートされた CSV ファイルにより、リアルタイムデータの包括的なビューが提供されるため、大きなデータセットの分析が容易になります。

2018 年 6 月

- **Azure Resource Manager** 接続：Studio の接続作成ウィザードの ［接続］ページで選択できる Azure 環境に、ユーザーの Azure サブスクリプションで有効なすべての Azure クラウドが含まれるようになりました。Azure US Government Cloud および Azure Germany Cloud の一般公開によって、以前のリリースでのこれらの 2 つの環境のプレビューバージョンが置き換えられています。

2018 年 5 月

- **Azure** クイック展開：リソースの場所で Azure Resource Manager マシンを使用してアプリケーションと公開デスクトップを配信する場合、次の展開方法を選択できるようになりました：
  - 完全な構成：これは既存の展開方法であり、Citrix Studio の管理コンソールを使用し、ガイドに従ってマシンカタログとデリバリーグループを順番に作成します。
  - Azure クイック展開：これは新しいオプションであり、簡略化されたインターフェイスによりアプリとデスクトップを短時間で展開できます。
- **Citrix Health Assistant** リンク：監視コンソールの未登録マシンの ［マシンの詳細］ページに、[Health Assistant］ボタンが追加されました。現在、このボタンは、「マシンのトラブルシューティング」および Knowledge Center の記事「Citrix Health Assistant - VDA の登録とセッション起動の問題のトラブルシューティング」にリンクされていて、そこからツールをダウンロードできます。Citrix Health Assistant は、未登録の VDA の構成に関する問題をトラブルシューティングするためのツールです。このツールは、さまざまなヘルスチェックを自動化して、VDA 登録、セッションの起動、タイムゾーンリダイレクトの構成でのよくある問題の根本原因を特定します。
- 対話型セッションのドリルダウン。管理コンソールで、[ユーザー詳細] ビューの ［ログオン期間］パネルに、ログオン処理の対話セッションの段階に関する情報が表示されるようになりました。ログオンのこのフェーズのより詳細なトラブルシューティングと修復を行うために、対話型セッションには、**Pre-userinit**、**Userinit**、**Shell** という 3 つのサブフェーズがあります。このリリースでは、対話型セッション上にマウスカーソルを置くと、サブフェーズと、ドキュメントへのリンクを示すヒントが表示されます。サブフェーズの説明および各フェーズのパフォーマンスを向上させる方法については、「ユーザーログオンの問題の診断」を参照してください。

2018 年 3 月

- アプリケーションインスタンス予測（プレビュー機能）：これは、初めて追加された予測分析に基づく監視機能です。リソースを整理し、リソースごとに必要なライセンスの数を調整するには、リソースの使用パターンの予測が重要になります。アプリケーションインスタンス予測機能では、サイトまたはデリバリーグループごとに、ある期間に起動される可能性のあるホストされているアプリケーションインスタンスの数が示されます。この予測には、既存の履歴データで作成されたデータモデルに基づく機械学習アルゴリズムが使用されます。許容レベルにより、予測の質が示されます。

詳しくは、Director の「アプリケーションインスタンス予測」を参照してください。Citrix Cloud ディスカッションフォーラムで、この機能の有用性やユーザービリティに関するフィードバックをお寄せください。

- **Delivery Groups API -** プレビュー

  Delivery Groups API のプレビューには、デリバリーグループの管理を自動化できる REST API セットが用意されています。使用可能なすべての API は、https://developer.cloud.com/の Citrix Cloud API のドキュメントで確認し、試すことができます。

- **Web Studio** 認証

  Citrix Cloud 上のサービス管理コンソールで、顧客の認証にベアラートークンが使用されるようになりました。このベアラートークンは、Delivery Groups REST API へのアクセスするために必要です。

- **OData** バージョン **4 API** を使用してモニターサービスのデータにアクセスする（プレビュー機能）

  OData V.4 エンドポイントを使用して、モニターサービスのデータに基づいて監視ダッシュボードおよびレポートダッシュボードを作成し、カスタマイズできるようになりました。OData V.4 は、ASP.NET Web API に基づいており、アグリゲーションクエリをサポートしています。V4 エンドポイントでデータにアクセスするには、Citrix Cloud ユーザー名とベアラートークンを使用します。詳細と例については、「Access Monitor Service data using the OData v4 endpoint in Citrix Cloud」を参照してください。

  Citrix Cloud ディスカッションフォーラムで、この機能の実用性に関するフィードバックをお寄せください。

解決された問題

- アプリケーションフォルダーの名前変更、移動、および削除を行えるようになりました。[#STUD-2376]

2018 年 1 月

- **RDS** ライセンスチェック: Windows Server OS マシンを含むマシンカタログの作成に、RDS ライセンスの自動チェックが含まれるようになりました。見つかった RDS ライセンスの問題が表示されるので、サービスのギャップを防ぐために適切な手順を実行できます。詳しくは、「マシンカタログの作成」を参照してください。
- 監視機能からのマシンコンソールへのアクセス: 監視機能の［マシンの詳細］パネルから、XenServer ハイパーバイザーバージョン 7.3 でホストされているマシンのコンソールにアクセスできるようになりました。これにより、監視機能から VDA の問題を直接トラブルシューティングできるようになりました。詳しくは、「マシンのトラブルシューティング」の「マシンコンソールへのアクセス」を参照してください。

2017 年 12 月

新機能と機能強化

- **Citrix Workspace**: XenApp and XenDesktop Service の新規お客様は、Citrix Workspace をご利用いただけるようになりました。詳しくは、「ワークスペース構成」を参照してください。

- アプリケーションの分析。［監視］>［アプリケーション］タブに新しく追加された［アプリケーション分析］ページで、アプリケーションのパフォーマンスを効率的に分析およびモニターできるようになりました。このページには、サイトで公開されているすべてのアプリケーションの正常性と使用状況の統合ビューが表示されます。アプリケーションごとのインスタンス数、公開アプリケーションに関連する障害およびエラーなどのメトリックが表示されます。この機能を使用するには、VDA のバージョン 7.15 以降が必要です。

  詳しくは、「モニター」の「アプリケーションの分析」セクションを参照してください。

2017 年 11 月

新機能と機能強化

- ローカルホストキャッシュ。ローカルホストキャッシュ機能を使用すると、リソースの場所にある Cloud Connector が Citrix Cloud と通信できなくなった場合でも、接続仲介操作を続行できるようになります。詳しくは、「ローカルホストキャッシュ」を参照してください。
- **Azure Managed Disks**：仮想マシンを Azure Resource Manager 環境に MCS でプロビジョニングする場合、デフォルトで Azure Managed Disks が使用されるようになりました。オプションとして、従来のストレージアカウントも使用できます。詳しくは、「Microsoft Azure Resource Manager 仮想化環境」を参照してください。
- ヘルプデスク管理者：Citrix Cloud カスタマーアカウントでサービス管理者を管理する場合に、ヘルプデスク管理者という新しい選択肢が追加されました。ヘルプデスク管理者は、サービスの監視機能にアクセスできます。詳しくは、「管理」を参照してください。

解決された問題

- サービス管理コンソールのウィザードを使用して、リモート PC アクセスマシンカタログを作成できるようになりました。これまでのリリースでは、CTX220737で説明するように、カタログを作成する場合は PowerShell コマンドレットを使用する必要がありました。その後、管理コンソールに戻ってデリバリーグループを作成する必要もありました。この修正により、管理コンソールでカタログとデリバリーグループを順番に作成するようになりました。
- MCS で作成したカタログで、既存の Active Directory マシンアカウントを使用できるようになりました。[#DNA-24566]
- 展開を監視するときに ［傾向］**>**［セッション］のテーブルの結果を並べ替えても、正確に表示されるようになりました。[DNA-51257]

追加情報

- 既知の問題
- サービスに含まれているサードパーティ製ソフトウェアについて詳しくは、「サードパーティ通知」を参照してください。

既知の問題

May 17, 2024

Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）には、次の既知の問題があります：

- AWS でホストされている VMware 環境では、マスターイメージで vTPM が有効になっていると、MCS マシンカタログの作成が失敗します。VMware のサポートについては、「Get Support」を参照してください。[PMCS-37603]
- Pendo の URL（`https://citrix-cloud-content.customer.pendo.io/`）がブロックされていると、モニター画面がロードされない場合があります。
  [DIR-18482]
- Remote PowerShell SDK で`XDHyp:\`を使用してコマンドを実行すると、エラーが発生します。この問題を解決するには、次の手順を実行します：

  1. `Hyp`でコマンドを実行します。たとえば、次のようになります：`Get-HypServiceStatus`
  2. `XDHyp:\`でコマンドを実行します。たとえば、次のようになります：`Get-ChildItem XDHyp:\Connections\`

  [BRK-13723]
- バージョン 2209 で Citrix DaaS アーキテクチャが変更されたため、このリリースより前に展開された Windows デスクトップおよびアプリケーションのデフォルトアイコンは一般的な PC デスクトップアイコンに変更されました。この変更は、デフォルトのアイコンを参照しているデスクトップおよびアプリケーションにのみ適用されます。アイコンを Windows アプリケーションのデフォルトのアイコンに戻す場合は、Remote PowerShell SDK を使用して次のスクリプトを実行します：
  `Get-BrokerApplication -IconUid 1 | Set-BrokerApplication -IconUid 0`。
- ［管理］>［完全な構成］で、Azure カタログの OS の種類を変更しようとすると失敗し、エラーメッセージが表示されます。Azure カタログの OS の種類の変更は、PowerShell を使用している場合でもサポートされなくなりました。[STUD-19819]
- Microsoft Azure 環境で、Azure エフェメラル OS ディスクと MCS I/O を同時に有効にすると、マシンカタログの作成に失敗します。ただし、既存のマシンカタログの場合は、マシンカタログの更新、VM の追加または削除、およびマシンカタログの削除を行うことはできます。[PMCS-21698]
- ［ユーザー詳細］ページと ［マシン詳細］ページで、［平均 IOPS］、［セッション制御］、および［電源制御］ボタンの下向き矢印アイコンが表示されないことがあります。ただし、機能は想定どおりに動作します。メニューのすべてのアイテムを表示するには、ボタンの任意の場所をクリックしてください。[DIR-11875]
- Azure AD Domain Services を使用する場合：ワークスペース（または StoreFront）のログオン UPN（User Principal Name：ユーザープリンシパル名）には、Azure AD Domain Services の有効化時に指定

したドメイン名を含める必要があります。作成したカスタムドメインをプライマリとして指定している場合でも、ログオンにカスタムドメインの UPN を使用することはできません。

- Azure に展開し、ライトバックキャッシュを有効にした MCS カタログバージョン 7.9 以降を作成し、マスターイメージにインストールされている VDA が 1811 以前になると、エラーが発生します。また、Microsoft Azure の Personal vDisk に関連する項目も作成できません。回避策としては、Azure への展開には別のカタログバージョンを選択するか、ライトバックキャッシュを無効にします。カタログの作成時にライトバックキャッシュを無効にするには、［マシン］ページの ［キャッシュに割り当てられたメモリ］チェックボックスと ［ディスクキャッシュサイズ］チェックボックスをオフにします。
- Microsoft Edge 44 および Firefox 68 ESR の Web ブラウザーで ［モニター］**>**［マシン詳細］の ［コンソール］リンクをクリックしても、マシンコンソールが起動しません。[DIR-8160]
- Workspace アプリの Web またはデスクトップで「再起動」オプションを使用しようとすると、「再起動中」のダイアログが開いたままになり終了の報告がありません。ハイパーバイザーはマシンがシャットダウンしたと表示しますが、起動は表示されません。この場合、時間を置くとユーザーが「再起動中」ダイアログを閉じることができ、デスクトップを起動するとデスクトップが起動します。[BRK-5564]

最新の VDA に関連する問題については、「既知の問題」を参照してください。

廃止

March 5, 2024

この記事では、お客様が適宜ビジネス上の決定を下せるように、段階的に廃止される Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）の機能について事前に通知します。Citrix ではお客様の使用状況とフィードバックをチェックして、各機能を撤廃するかどうかを判断しています。お知らせする内容は以降のリリースで変わることがあり、廃止される機能がすべて含まれるわけではありません。製品ライフサイクルサポートについて詳しくは、「製品ライフサイクルサポートポリシー」の記事を参照してください。

> 注:
>
> Citrix Virtual Apps and Desktops の廃止および削除については、独自の「廃止」の記事で説明しています。

廃止と削除

廃止または削除される Citrix DaaS の機能を以下の一覧に示します。

廃止されたアイテムはすぐには削除されません。引き続きサポートされますが、今後のリリースでは削除される予定です。

削除されたアイテムは、Citrix DaaS で削除されたかサポートされなくなりました。太字の日付は最新のアップデートを示しています。

アイテム	廃止が発表されたリリース	削除されたリリース	代替手段
ディスクキャッシュのみを含め、メモリキャッシュを含めないライトバックキャッシュの構成をサポート	2024 年 2 月		メモリキャッシュサイズ構成オプションを使用して、ゼロ以外のサイズを指定します。
オンデマンドプロビジョニング機能（「レガシー」カタログ）が廃止される前に作成された Azure カタログのサポート	2024 年 2 月		Azure レガシーカタログ VM を再作成します。カタログはオンデマンドでプロビジョニングされるため、ストレージコストの節約に役立ちます。
Citrix Connector 3.1 for System Center Configuration Manager のサポート	2023 年 12 月		イメージまたはアプリケーションの手動更新。
カタログが作成されたリージョンとは異なるリージョンでのマスターイメージ使用のサポート	2023 年 12 月		Azure Compute Gallery を使用して、マスターイメージを必要なリージョンに複製します。
AWS ボリュームワーカーのサポート	2023 年 11 月		ディスクの直接アップロードとダウンロードを使用します。「ディスクの直接アップロードとダウンロード」を参照してください。
デリバリーグループの作成に使用される`Leave user management to Citrix Cloud`のサポート	2023 年 9 月	2023 年 9 月	
AWS 環境で使用される`AwsCaptureInstanceProperties`のサポート	2023 年 8 月		マシンプロファイルを使用する「マシンプロファイルを使用してカタログを作成する」を参照してください。
VMware vSphere 6.7 のサポート		2023 年 6 月	VMware vSphere の上位バージョンを使用します。

アイテム	廃止が発表されたリリース	削除されたリリース	代替手段
Schedule-ProvVMUpdate PowerShell コマンド	2023 年 4 月		Set-ProvVMUpdateTimeWindow コマンドを使用します。
Request-ProvVMUpdate PowerShell コマンド	2023 年 4 月		Set-ProvVMUpdateTimeWindow コマンドを-StartsNowおよび-DurationInMinutes -1パラメーターとともに使用します。
Cancel-ProvVMUpdate PowerShell コマンド	2023 年 4 月		Clear-ProvVMUpdateTimeWindow コマンドを使用します。
DedicatedTenancy コマンドで使用するNew-ProvScheme パラメーター	2023 年 3 月		TenancyTypeパラメーターを使用します。
Azure 環境で仮想マシンを作成するための非管理ディスク	2022 年 6 月		
4 つの AWS 固有のコマンドをサポート: Revoke-HypSecurityGroupIngress 、 Revoke-HypSecurityGroupEgress 、 Grant-HypSecuritygroupegress 、およびGrant-HypSecurityGroupIngress	2022 年 5 月		

アイテム	廃止が発表されたリリース	削除されたリリース	代替手段
Azure 環境で使用される`StorageAccountType`パラメーター	2022 年 4 月		`StorageType`を使用します。
従来のコンソール（MMC ベースのコンソール）	2021 年 7 月	2021 年 11 月	［管理］**>**［完全な構成］を使用すると、すべての構成および管理操作にアクセスできます。
Azure クイック展開	2020 年 9 月		［クイック展開］を使用します。
Citrix Provisioning ターゲットデバイスをインポートして、Citrix Studio でカタログを作成する機能。	2020 年 8 月	2021 年 2 月	Citrix Provisioning のデバイスのエクスポートウィザードを使用して、Citrix Provisioning 仮想マシンを Delivery Controller/MCS にプッシュし、カタログを作成します。「デバイスのエクスポートウィザード」を参照してください。

システム要件

June 12, 2024

はじめに

このトピックで説明されていないコンポーネントのシステム要件（Citrix Workspace アプリおよび Citrix Provisioning）については、各コンポーネントのドキュメントを参照してください。

ハードウェアの提供は複雑かつ動的であるため、デスクトップおよびアプリケーションを配信する仮想マシンのサイジングについて、特定の推奨事項を示すことはできません。すべての展開には、固有のニーズがあります。通常、仮想マシンのサイジングはユーザーのワークロードではなくハードウェアに基づきます（RAM 以外。より多く消費するアプリケーションにはより多くの RAM が必要です）。Citrix Tech Zoneには VDA のサイジングに関する最新のガイダンスが含まれています。

> 重要:
>
> この記事で説明されている VDA バージョンは、Citrix 製品ライフサイクルの影響を受けます。詳しくは、Citrix Web サイトの「Product Matrix」を参照してください。
>
> Citrix DaaS での LTSR VDA の使用について詳しくは、CTX205549を参照してください。

注: Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）環境では、コアコンポーネント（Delivery Controller、サイト構成データベース、または管理および監視コンソール）をインストールまたは管理する必要はありません。Virtual Delivery Agent（VDA）のインストールガイダンスについては、以下を参照してください:

- VDA のインストール
- コマンドラインを使用した VDA のインストール

Cloud Connector

詳しくは、「Cloud Connector の技術詳細」を参照してください。

Azure 環境の VDA

以下のオペレーティングシステムがサポートされています:

- Windows 11 マルチセッション
- Windows 11 シングルセッション
- Windows 10 マルチセッション
- Windows 10 シングルセッション
- Windows Server 2022（最低でも VDA 2106 が必要）
- Windows Server 2019
- Windows Server 2016

サポートが終了していないすべての VDA は、Citrix DaaS での使用がサポートされています。LTSR VDA については、最新の累積更新プログラムで使用することをお勧めします。VDA のライフサイクルについて詳しくは、「Citrix 製品マトリクス」を参照してください。

Windows Server 2012 R2 は、VDA 1912（およびそれ以降の CU）でのみサポートされます。

Windows Server には、Microsoft RDS ライセンスが必要です。

Azure Virtual Desktop については、Microsoft 社のドキュメントを参照してください。

シングルセッション OS 対応 VDA

以下の情報は、最新の VDA リリースに適用されます。

以下のオペレーティングシステムがサポートされています:

- Windows 11
- Windows 10
  - エディションのサポートについては、CTX224843を参照してください。この記事には、サポートされている Windows バージョンでの Citrix の既知の問題へのリンクも含まれています。
  - Windows 10 では、デスクトップコンポジションのリダイレクトと従来のグラフィックモードはサポートされません。

要件:

- Microsoft .NET Framework 4.8 以降がインストールされていない場合は、自動的にインストールされます。
- Microsoft Visual C++ 2015～2019 再頒布可能パッケージ
  - マシンに以前のバージョンのランタイム（2015～2017 など）がインストールされている場合、Citrix インストーラーはそれをアップグレードします。
  - マシンに 2015 より前のバージョンが含まれている場合、Citrix は新しいバージョンを並行してインストールします。

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

いくつかのマルチメディアアクセラレーション機能（HDX MediaStream Windows Media リダイレクトなど）では、VDA のインストール先マシンに Microsoft メディアファンデーションをインストールする必要があります。マシンにメディアファンデーションがインストールされていない場合は、マルチメディアアクセラレーション機能がインストールされません。Citrix ソフトウェアのインストール後にマシンからメディアファンデーションを削除しないでください。これを削除すると、ユーザーがマシンにログオンできなくなります。サポートされている Windows デスクトップ OS のほとんどのエディションには、Media Foundation があらかじめインストールされており、削除することはできません。ただし、N エディションには、特定のメディア関連テクノロジは含まれていません。ソフトウェアは、Microsoft またはサードパーティから入手できます。

追加情報:

- Linux VDA については、Linux Virtual Delivery Agentの製品ドキュメントを参照してください。
- サポートされる Windows Server マシンでは、コマンドラインインターフェイスを使用してシングルセッション VDA をインストールし、サーバー VDI 機能を使用できます。詳しくは、「サーバー VDI」を参照してください。
- 古いマシンに VDA をインストールする方法については、「以前のオペレーティングシステム」を参照してください。
- 「Azure Virtual Desktop 環境の VDA」も参照してください。

マルチセッション **OS** 対応 **VDA**

以下の情報は、最新の VDA リリースに適用されます。

以下のオペレーティングシステムがサポートされています:

- Windows Server 2022（最低でも VDA 2106 が必要）
- Windows Server 2019、Standard、および Datacenter エディション。
- Windows Server 2016、Standard、および Datacenter エディション。
- Windows 11
- Windows 10（64 ビット）でサポートされているすべてのバージョン

インストーラーにより、次の必須要素が自動的に展開されます:

- Microsoft .NET Framework 4.8 以降がインストールされていない場合は、自動的にインストールされます。
- Microsoft Visual C++ 2015～2019 再頒布可能パッケージ
  - マシンに以前のバージョンのランタイム（2015～2017 など）がインストールされている場合、Citrix インストーラーはそれをアップグレードします。
  - マシンに 2015 より前のバージョンが含まれている場合、Citrix は新しいバージョンを並行してインストールします。

リモートデスクトップサービスの役割サービスが自動的にインストールされて有効になります。この処理が実行されると、再起動が行われます。

いくつかのマルチメディアアクセラレーション機能（HDX MediaStream Windows Media リダイレクトなど）では、VDA のインストール先マシンに Microsoft メディアファンデーションをインストールする必要があります。マシンにメディアファンデーションがインストールされていない場合は、マルチメディアアクセラレーション機能がインストールされません。Citrix ソフトウェアのインストール後にマシンからメディアファンデーションを削除しないでください。これを削除すると、ユーザーがマシンにログオンできなくなります。ほとんどの Windows Server バージョンでは、メディアファンデーション機能はサーバーマネージャーを介してインストールされます。ただし、N エディションには、特定のメディア関連テクノロジは含まれていません。ソフトウェアは、Microsoft またはサードパーティから入手できます。

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

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

追加情報:

- Linux VDA については、「Linux Virtual Delivery Agent」を参照してください。
- サポートされなくなった Windows オペレーティングシステムに VDA をインストールする方法については、「以前のオペレーティングシステム」を参照してください。
- 「Azure Virtual Desktop 環境の VDA」も参照してください。

ホスト/仮想化リソース

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

- **Amazon Web Services（AWS）**
  - サポートされる Windows サーバー OS で、アプリケーションやデスクトップをプロビジョニングできます。
  - Amazon Relational Database Service（RDS）はサポートされません。

  詳しくは、「AWS クラウド環境」を参照してください。
- **XenServer**（旧称 **Citrix Hypervisor**）

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

  詳しくは、「XenServer 仮想化環境」を参照してください。
- **Google Cloud Platform**

  詳しくは、「Google Cloud 環境」と「Getting Started with Citrix DaaS on Google Cloud」をご覧ください。
- **HPE Moonshot**

  詳しくは、「HPE Moonshot 仮想化環境」を参照してください。
- **Microsoft Azure Resource Manager**

  詳しくは、「Microsoft Azure Resource Manager クラウド環境」を参照してください。
- **Microsoft System Center Virtual Machine Manager**

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

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

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

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

  詳しくは、「Nutanix 仮想化環境」を参照してください。
- **VMware Cloud on AWS**

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

  詳しくは、「VMware Cloud on AWS（Amazon Web Services）」を参照してください。

- **Azure VMware Solution（AVS）**

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

  詳しくは、「Azure VMware Solution（AVS）の統合」を参照してください。

- **Google Cloud VMware Engine**

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

  詳しくは、「Google Cloud VMware Engine」を参照してください。

- **VMware vSphere（vCenter + ESXi）**

  vSphere vCenter のリンクモードはサポートされません。

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

  詳しくは、「VMware 仮想化環境」を参照してください。

> 注:
>
> Citrix DDC または StoreFront サーバーに VDA ソフトウェアをインストールしないでください。VDA はスタンドアロンシステムである必要があります。1 つの仮想マシンに複数のコンポーネントをインストールすることは、概念実証を開発する場合、または Studio 管理コンソールを管理者のみに公開する場合にのみ許可されます。この場合、管理者以外のユーザーが Citrix DDC または StoreFront の仮想マシンにアクセスできないようにする必要があります。

Active Directory の機能レベル

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

- Windows Server 2016
- Windows Server 2012
- Windows Server 2008 R2

Active Directory については詳しくは、「Active Directory 参加済み」を参照してください。

HDX テクノロジ

特定の HDX 機能のサポートおよび要件については、「HDX」を参照してください。

ユニバーサルプリントサーバー

ユニバーサルプリントサーバーは、クライアント側およびサーバー側のコンポーネントで構成されています。UpsClient コンポーネントは、VDA と一緒にインストールされます。UpsServer コンポーネントは、ユーザーセッ

ションで Citrix ユニバーサルプリンタードライバーをプロビジョニングする共有プリンターがある各印刷サーバー上にインストールします。

UpsServer は以下でサポートされています。

- Windows Server 2019
- Windows Server 2016

要件:

- Microsoft .NET Framework 4.8（最小）
- Microsoft Visual C++ 2015～2022 再頒布可能パッケージ
  - マシンに以前のバージョンのランタイム（2015～2017 など）がインストールされている場合、Citrix インストーラーはそれをアップグレードします。
  - マシンに 2015 より前のバージョンが含まれている場合、Citrix は新しいバージョンを並行してインストールします。

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

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

詳しくは、「プリンターのプロビジョニング」を参照してください。

サービス接続

インターネット接続情報 については、「システムおよび接続要件」を参照してください。この情報には、ほとんどの Citrix Cloud サービスに共通の要件に加えて、Citrix DaaS 固有の要件が含まれています。

その他

- Citrix ポリシー情報をサイト構成データベースではなく Active Directory に格納する場合、Microsoft グループポリシー管理コンソール（GPMC）が必要です。`CitrixGroupPolicyManagement_x64.msi`をインストールするマシンには、Visual Studio 2015 ランタイムをインストールしている必要があります。詳しくは、Microsoft のドキュメントを参照してください。
- この製品は、PowerShell のバージョン 3 から 5 までをサポートします。
- Windows サーバーにインストール可能な製品コンポーネントと機能に関しては、Server Core のインストールおよび Nano Server のインストールは、別途記載がない限りサポートされていません。
- 展開のリソース制限について詳しくは、「制限」を参照してください。
- サポートされている StoreFront のバージョンについては、StoreFront のシステム要件を参照してください。

- グローバリゼーションの情報について詳しくは、CTX119253を参照してください。
- Citrix DaaS で使用されるポートについては、「Citrix テクノロジで使用される通信ポート」を参照してください。
- ［クイック展開］管理インターフェイスを使用する場合の要件については、「要件」を参照してください。

制限

June 12, 2024

ここで示された値は、単一の Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）インスタンスの制限に関するものです。これらの制限は、エンドユーザーと管理者に最高のエクスペリエンスを提供できることが Citrix によって何度もテストされているので、推奨できるものです。これらはソフトな制限であり、技術的に強制されるものではありません (ただし、リソースの場所ごとの VDA の総数は除きます)。同時ユーザー数が 125,000 人を超えると、スケールして複数の Citrix DaaS インスタンスを組み合わせることで、あらゆる規模で統合エクスペリエンスを提供できます。

この記事の情報は動的なものです。頻繁に更新を確認してください。今ある要件に対して、公開されている制限が対応していない場合は、Citrix の担当者にお問い合わせください。

構成の制限

ポリシーが制限を超える場合は、Workspace Environment Management サービスまたはActive Directory グループポリシーオブジェクト（GPO） を使用することを Citrix ではお勧めします。

リソース	制限
Active Directory ドメイン	100
アプリケーションフォルダー	1,000
アプリケーショングループ	250
アプリケーション	5,000
カタログ	2,000
デリバリーグループ	2,000
ホスト接続	200
リソースの場所	100
［管理］コンソール（完全な構成）ポリシー	200

リソース	制限
タグ	10,000
VDA	100,000

リソースの場所の制限

次の表は、各リソースの場所の制限です。

要件がこれらの制限を超える場合は、追加のリソースの場所を使用することを Citrix ではお勧めします。

リソース	制限
VDA の合計数 (ハードな制限)	10,000
合計セッション数	25,000
Active Directory ドメイン	1
ホスト接続	40

Citrix Cloud Connector はリソースの場所に割り当てられ、ワークロードを Citrix DaaS にリンクします。Cloud Connector の制限については、「Cloud Connector のサイズおよびスケールの考慮事項」を参照してください。

プロビジョニング制限

以下の表のプロビジョニング制限は、1 つのパブリックプロバイダーサブスクリプションで Citrix が推奨する最大値です。

パブリッククラウドベンダーによっては、さらに少ない値でクォータ制限に達することがあります。このような場合は、ベンダーに連絡してサブスクリプションのクォータを引き上げてください。大規模な展開の場合、Citrix はハブおよびスポークモデルをお勧めします。このモデルでは、VDA が複数のサブスクリプションとホスト接続に分散されます。

詳しくは、次のリファレンスアーキテクチャを参照してください:

- AWS での Citrix DaaS
- Google Cloud での Citrix 仮想化
- Azure での Citrix DaaS

リソース	制限
リージョンごとの Amazon Web Services アカウントあたりの VDA	3,000
Google Cloud Platform プロジェクトごとの VDA	3,000
リージョンごとの Microsoft Azure サブスクリプションごとの VDA	5,000

> 注:
>
> この制限は、Citrix が推奨するものです。

使用制限

管理者の役割とそれぞれの違いについては、以下を参照してください:

- ［管理］（完全な構成）の管理者
- ［監視］（Director）の管理者

リソース	制限
すべての管理権限を実行できる［監視］（Director）の管理者（同時）	40
［監視］（Director）のヘルプデスク管理者（同時）	200
［監視］（Director）のセッション管理者（同時）	50
［管理］（完全な構成）のクラウド管理者（同時）	100
［管理］（完全な構成）のヘルプデスク管理者（同時）	60
エンドユーザー（同時）	125,000
単一のユーザーに公開されたリソース	250
1 分あたりのセッション起動数	3,000

- ［監視］（Director）は、単一のテナント（ハブ）で最大 4 つの Citrix DaaS テナント（スポーク）のアグリゲーションをサポートします。
- ハブインスタンスのヘルプデスク管理者は、特定のインスタンスの委任管理構成に従って、すべてのアグリゲーションインスタンス（ハブおよびスポーク）からのユーザー、マシン、エンドポイント、およびトランザクションを監視およびトラブルシューティングできます。
- Citrix DaaS インスタンスごとの同時接続可能な管理者数は、「使用制限」の表のとおりです。

制限の変更ログ

次の表は、構成制限の変更履歴です：

日付	リソース	説明
22 Nov 2023	Active Directory ドメイン	制限が 85 から 100 に増加しました。
	カタログ	制限が 1000 から 2000 に増加しました。
	デリバリーグループ	制限が 1000 から 2000 に増加しました。
	リソースの場所	制限が 85 から 100 に増加しました。
	リソースの場所 -> 合計セッション数	制限が 20,000 から 25,000 に増加しました。
07 Dec 2023	プロビジョニングの制限 -> リージョンごとの Microsoft Azure サブスクリプションごとの VDA	制限が 2,500 から 5,000 に増加しました。

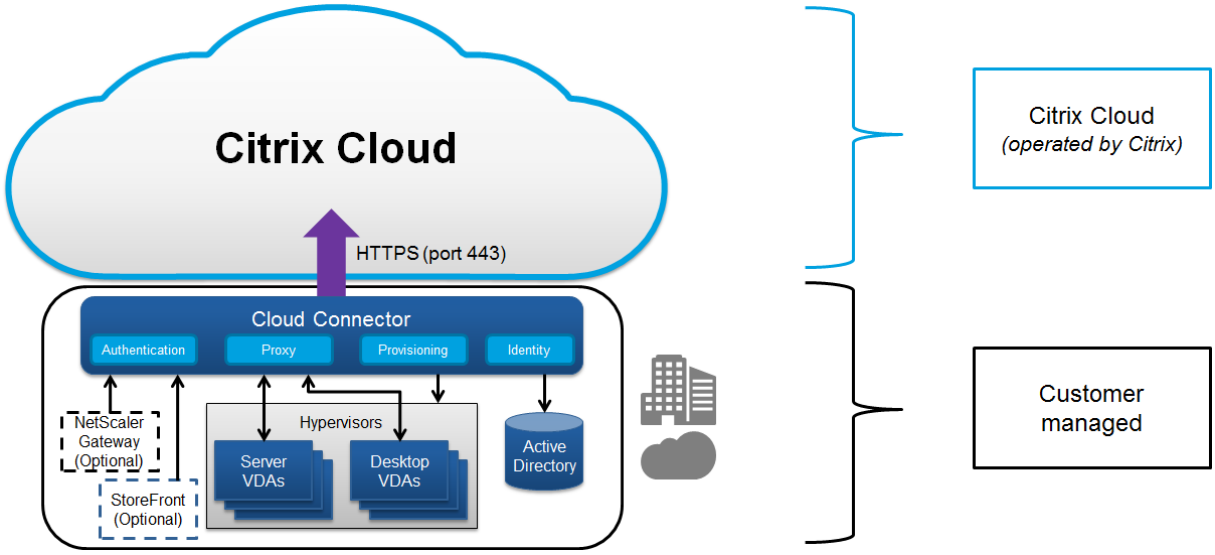
セキュリティの技術概要

May 17, 2024

セキュリティの概要

この記事の対象は、Citrix Cloud でホストされている Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）です。この情報には、Citrix Virtual Apps Essentials と Citrix Virtual Desktops Essentials が含まれます。

Citrix DaaS 環境のコントロールプレーンの操作は、Citrix Cloud により管理されます。コントロールプレーンには、Delivery Controller、管理コンソール、SQL データベース、ライセンスサーバーが含まれ、オプションで StoreFront と Citrix Gateway（旧称 NetScaler Gateway）が含まれます。アプリとデスクトップをホストする Virtual Delivery Agents（VDA）は、クラウドまたはオンプレミスのいずれかのデータセンターでお客様が管理します。これらのコンポーネントは、Citrix Cloud Connector と呼ばれるエージェントを使用してクラウドサービスに接続されます。Citrix Workspace を使用することを選択した場合、お客様はデータセンター内で Citrix Gateway を実行する代わりに、Citrix Gateway サービスを使用することもできます。次の図は、Citrix DaaS とそのセキュリティ境界を示しています。



Citrix クラウドベースのコンプライアンス

2021 年 1 月時点で、さまざまなエディションの Citrix DaaS および Workspace Premium Plus での Citrix Managed Azure Capacity の使用は、Citrix SOC 2（タイプ 1 または 2）、ISO 27001、HIPAA、またはその他のクラウドコンプライアンスの要件に対して評価されていません。Citrix Cloud の認定について詳しくは、「Citrix Trust Center」を参照してください。また、頻繁に更新を確認してください。

データフロー

Citrix DaaS は VDA をホストしないため、プロビジョニングに必要なお客様のアプリケーションデータとイメージは、常にお客様の構成内でホストされます。コントロールプレーンはユーザー名、マシン名、アプリケーションショートカットなどのメタデータにアクセスできますが、お客様の知的財産へのアクセスは制限されています。

クラウドとお客様の施設間でのデータ通信には、ポート 443 を介した安全な TLS 接続が使用されます。

データ分離

Citrix DaaS には、お客様のアプリケーションとデスクトップの仲介および監視に必要なメタデータのみが格納されます。イメージ、ユーザープロファイル、その他のアプリケーションデータなどの機密情報は、お客様の施設内、またはパブリッククラウドベンダーのサブスクリプション内に留まります。

サービスのエディション

Citrix DaaS の機能はエディションによって異なります。たとえば、Citrix Virtual Apps Essentials では、Citrix Gateway サービスと Citrix Workspace のみがサポートされます。サポートされる機能について詳しくは、各製品のマニュアルを参照してください。

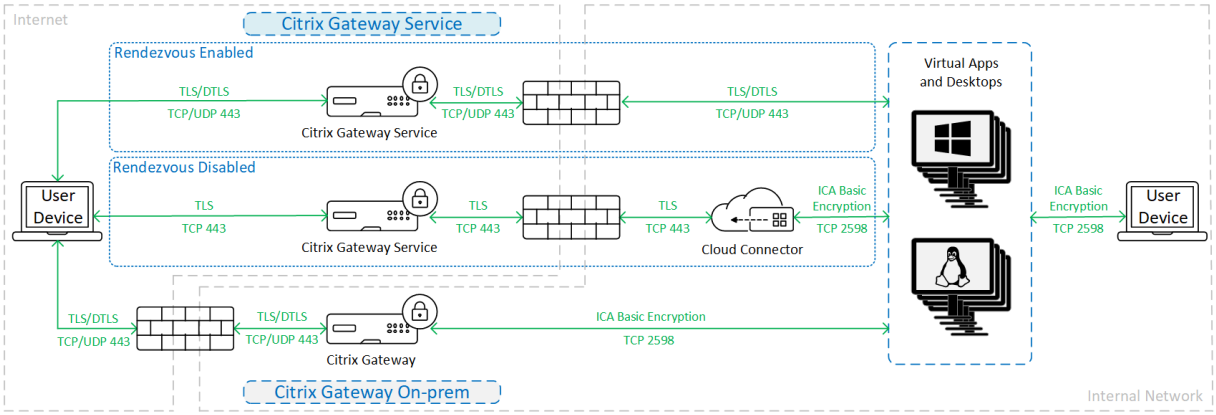
ICA のセキュリティ

Citrix DaaS は、転送中の ICA トラフィックを保護するためのさまざまなオプションを提供します。使用可能なオプションは次のとおりです:

- **Basic encryption**: デフォルト設定。
- **SecureICA**: RC5（128 ビット）暗号化を使用してセッションデータを暗号化できます。
- **VDA TLS/DTLS**: TLS/DTLS を使用してネットワークレベルの暗号化を使用できるようにします。
- **Rendezvous protocol**: Citrix Gateway サービスを使用している場合にのみ使用できます。Rendezvous プロトコルを使用する場合、ICA セッションは TLS/DTLS を使用してエンドツーエンドで暗号化されます。

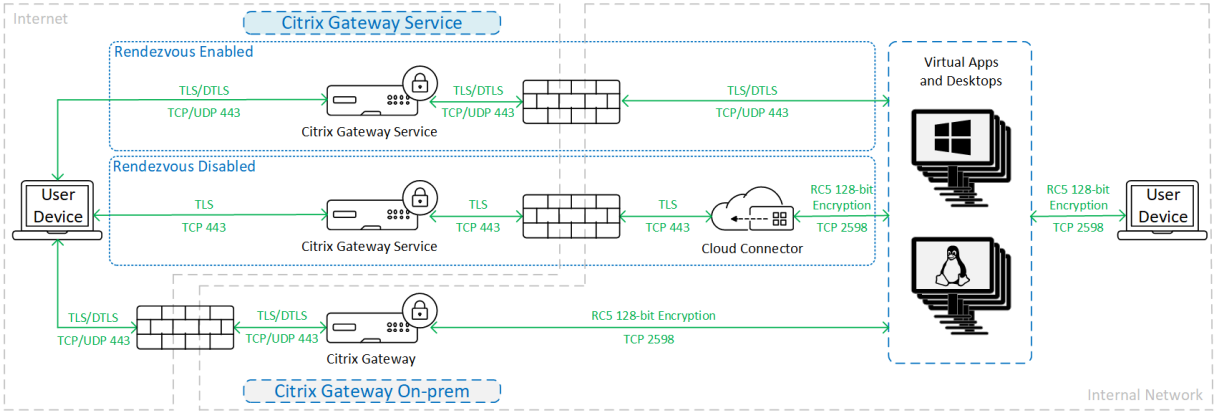
基本の暗号化

基本の暗号化を使用する場合、トラフィックは次の図に示すように暗号化されます。



SecureICA

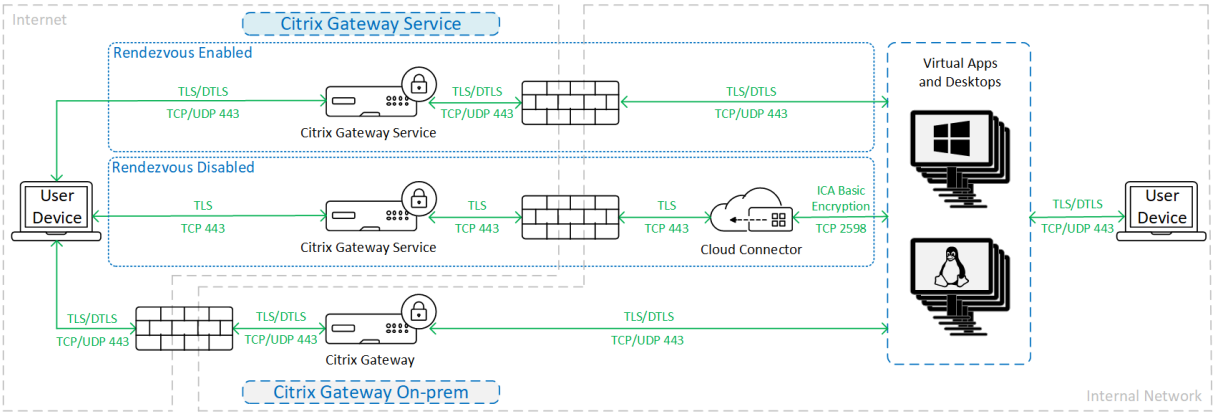
SecureICA を使用する場合、トラフィックは次の図に示すように暗号化されます。



> 注:
>
> HTML5 向け Workspace アプリを使用する場合、SecureICA はサポートされません。

VDA TLS/DTLS

VDA TLS/DTLS 暗号化を使用する場合、トラフィックは次の図に示すように暗号化されます。



> 注:
>
> Rendezvous なしで Gateway サービスを使用する場合、VDA と Cloud Connector 間のトラフィックは TLS 暗号化されません。これは、Cloud Connector はネットワークレベルの暗号化による VDA への接続をサポートしていないためです。

その他のリソース

ICA セキュリティオプションとその設定方法について詳しくは、以下を参照してください。

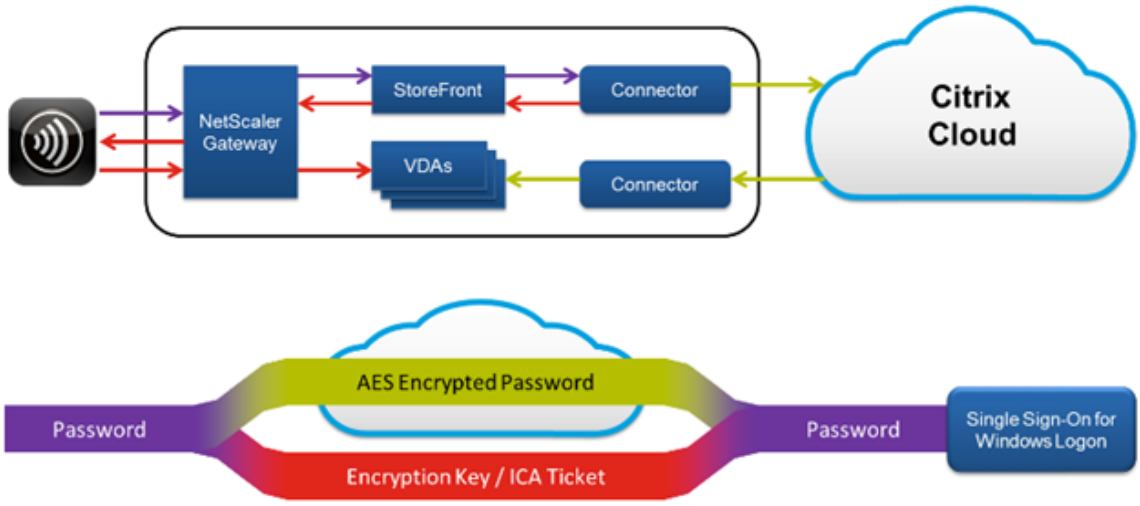
- SecureICA: セキュリティのポリシー設定
- VDA TLS/DTLS: Transport Layer Security
- Rendezvous プロトコル: Rendezvous プロトコル

資格情報の処理

Citrix DaaS は、次の 4 種類の資格情報を処理します:

- ユーザーの資格情報: ユーザー管理 StoreFront を使用する場合、ユーザーの資格情報は、AES-256 暗号化および起動のたびに生成されるランダムなワンタイムキーを使用して Citrix Cloud Connector により暗号化されます。このキーは、クラウドに渡されることはなく、Citrix Workspace アプリにのみ返されます。その後、シングルサインオンを実現するために、Citrix Workspace アプリから VDA に渡され、セッションの開始時にユーザーパスワードの暗号化が解除されます。フローを次の図に示します。

デフォルトでは、ユーザー資格情報は信頼されていないドメイン境界を越えて転送されません。VDA と StoreFront が 1 つのドメインにインストールされていて、別のドメインのユーザーが VDA に接続しようとすると、ドメイン間で信頼が確立されていない限り、ログオンの試みは失敗します。DaaS PowerShell SDK を使用してこの動作を無効にし、信頼されていないドメイン間で資格情報を転送できるようにすることができます。詳しくは、Set-Brokersiteを参照してください。



- 管理者資格情報：管理者は、Citrix Cloud に対して認証を行います。認証により、管理者が Citrix DaaS にアクセスできるようにする 1 回限りの署名付き JSON Web Token（JWT）が生成されます。
- ハイパーバイザーパスワード：認証にパスワードが必要なオンプレミスハイパーバイザーでは、管理者が生成したパスワードがクラウドの SQL データベースに暗号化され保存されています。認証済みのプロセスでのみハイパーバイザーの資格情報が使用されるよう、Citrix がピアキーを管理します。
- Active Directory（AD）資格情報：Machine Creation Services では、お客様の AD でマシンアカウントを作成するために Cloud Connector を使用します。Cloud Connector のマシンアカウントには AD の読み取りアクセス権しかないため、管理者はマシンを作成または削除するたびに資格情報の入力を求められます。これらの資格情報はメモリ内にのみ保管され、単一のプロビジョニングイベントの間だけ保持されます。

展開に関する考慮事項

環境内に Citrix Gateway アプリケーションおよび VDA を導入する場合は、公開されているベストプラクティスのドキュメントを参照することをお勧めします。

Citrix Cloud Connector のネットワークアクセス要件

Citrix Cloud Connector には、インターネットへのポート 443 の送信トラフィックのみが必要であるため、HTTP プロキシの背後でホストできます。

- Citrix Cloud で HTTPS 用に使用される通信は、TLS です。（「TLS バージョンの廃止」を参照してください。）

- 内部ネットワーク内では、Cloud Connector は Citrix DaaS の次のものにアクセスする必要があります:
  - VDA: 送信と受信の両方でポート 80。追加で Citrix Gateway サービスを使用する場合は受信ポート 1494 と 2598
  - StoreFront サーバー: 受信ポート 80。
  - Citrix Gateway（STA として構成されている場合）: 受信ポート 80。
  - Active Directory ドメインコントローラー
  - Hypervisor: 送信のみ。特定のポートについては、「Citrix テクノロジで使用される通信ポート」を参照してください。

VDA と Cloud Connector との間のトラフィックは、Kerberos のメッセージレベルのセキュリティを使用して暗号化されます。

ユーザー管理 **StoreFront**

ユーザー管理 StoreFront は、オンプレミスでのユーザー資格の情報の管理機能など、高度なセキュリティ構成オプションと展開アーキテクチャの柔軟性を備えています。この StoreFront を Citrix Gateway の背後に配置することで、リモートアクセスをセキュリティで保護し、多要素認証を適用できるほか、その他のセキュリティ機能も追加できます。

Citrix Gateway サービス

Citrix Gateway サービスを使用すると、お客様のデータセンター内に Citrix Gateway を導入する必要はなくなります。

詳しくは、「Citrix Gateway サービス」を参照してください。

Cloud Connector と Citrix Cloud 間のすべての TLS 接続は、Cloud Connector から Citrix Cloud に対して開始されます。受信ファイアウォールポートのマッピングは必要ありません。

XML 信頼

この設定は、[完全な構成] > [設定] > [**XML** 信頼を有効にする] で使用でき、デフォルトでは無効になっています。また、Citrix DaaS Remote PowerShell SDK を使用して、XML 信頼を管理できます。

XML 信頼は、以下を使用する展開に適用されます:

- オンプレミス StoreFront。
- パスワードを必要としない利用者（ユーザー）認証テクノロジ。このようなテクノロジの例がドメインパススルー、スマートカード、SAML、Veridium ソリューションです。

XML 信頼を有効にすると、ユーザーはアプリケーションを正常に認証して起動できます。Cloud Connector は、StoreFront から送信された資格情報を信頼します。Citrix Cloud Connector と StoreFront 間の通信を保護して

いる場合にのみ XML 信頼を有効にします（ファイアウォール、IPsec、またはその他のセキュリティ推奨事項を使用）。

このチェックボックスは、デフォルトでオフになっています。

Citrix DaaS Remote PowerShell SDK を使用して、XML 信頼を管理します。

- XML 信頼の現在の値を確認するには、`Get-BrokerSite`を実行して`TrustRequestsSentToTheXMLServic`の値を調べます。
- XML 信頼を有効にするには、`Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true`を実行します。
- XML 信頼を無効にするには、`Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $false`を実行します。

HTTPS または **HTTP** トラフィックの適用

XML Service を使用して HTTPS または HTTP トラフィックを適用するには、各 Cloud Connector で次のレジストリ値セットのいずれかを構成します。

設定を構成したら、各 Cloud Connector で Remote Broker Provider Service を再起動します。

`HKLM\Software\Citrix\DesktopServer\`で:

- HTTPS（HTTP を無視）トラフィックを適用するには: `XmlServicesEnableSsl`を`1`に設定し、`XmlServicesEnableNonSsl`を`0`に設定します。
- HTTP（HTTPS を無視）トラフィックを適用するには: `XmlServicesEnableNonSsl`を`1`に設定し、`XmlServicesEnableSsl`を`0`に設定します。

TLS バージョンの廃止

Citrix DaaS のセキュリティを向上させるため、2019 年 3 月 15 日以降、Transport Layer Security（TLS）1.0 および 1.1 を介した通信をブロックすることになりました。

Citrix Cloud Connector から Citrix Cloud サービスへのすべての接続には、TLS 1.2 が必要です。

ユーザーのデバイスから Citrix Workspace に正常に接続するには、インストールされている Citrix Receiver が以下のバージョン以降であることを確認してください。

Receiver	バージョン
Windows	4.2.1000
Mac	12.0
Linux	13.2

Receiver	バージョン
Android	3.7
iOS	7.0
Chrome/HTML5	最新（ブラウザーでの TLS 1.2 のサポートが必要です）

Citrix Receiver の最新バージョンにアップグレードするには、https://www.citrix.com/products/receiver/にアクセスしてください。

また、TLS 1.2 を使用する新しいCitrix Workspace アプリにアップグレードする方法もあります。Citrix Workspace アプリをダウンロードするには、https://www.citrix.com/downloads/workspace-app/にアクセスしてください。

引き続き TLS 1.0 または 1.1 を使用する必要がある場合（たとえば、以前のバージョンの Receiver for Linux に基づいてシンクライアントを使用している場合）、リソースの場所に StoreFront をインストールします。次に、すべての Citrix Receiver がそれを指すようにします。

追加情報

セキュリティ情報について詳しくは、次のリソースを参照してください：

- Citrix Managed Azure のセキュリティの技術概要。
- Citrix セキュリティサイト。
- セキュリティおよびコンプライアンスの情報：最新のセキュリティ情報などが見つかるセキュリティおよびコンプライアンスセンターです。このセンターには、セキュアで準拠した IT 環境を維持するために重要な標準と認証に関するドキュメントもあります。
- セキュリティで保護された Citrix Cloud プラットフォームの展開ガイド：このガイドには、Citrix Cloud を使用するときのセキュリティのベストプラクティスの概要と、Citrix Cloud が収集し管理する情報が記載されています。このガイドには、Citrix Cloud Connector に関する総合的な情報へのリンクも含まれています。
- システムおよび接続要件。
- セキュリティに関する考慮事項およびベストプラクティス。
- スマートカード。
- Transport Layer Security（TLS）。

> 注：
>
> 本記事は、Citrix Cloud のセキュリティ機能の概要を説明し、Citrix Cloud 環境の保護に関する Citrix とお客様との間の責任分担を定義することを目的としています。Citrix Cloud、またはそのコンポーネントやサー

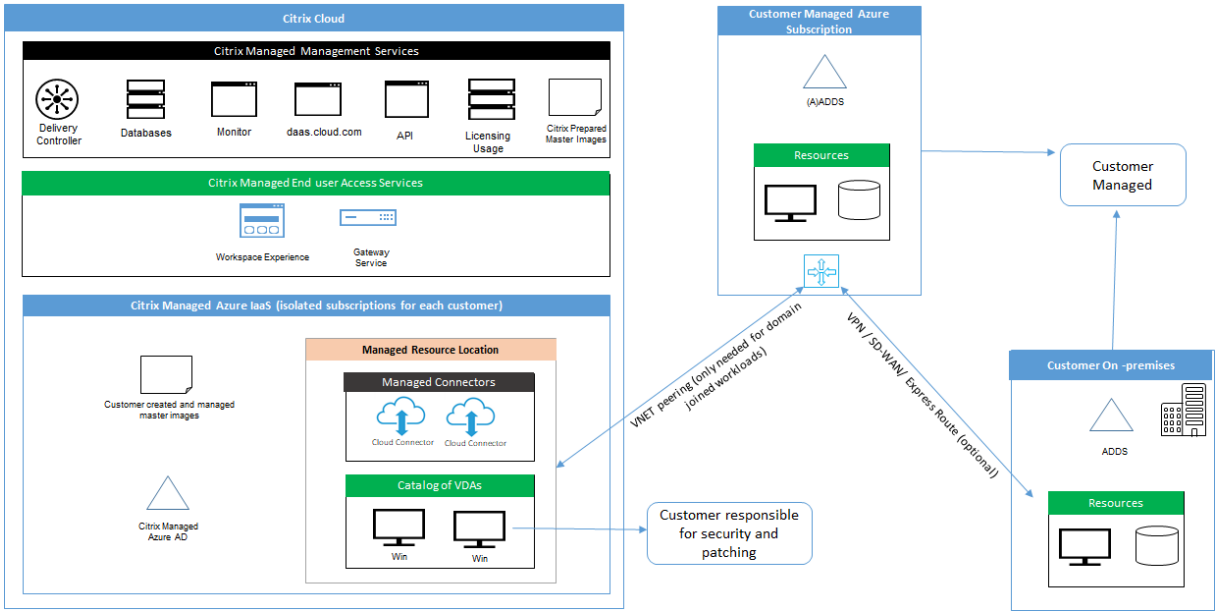
> ビスの構成および管理に関するガイダンスではありません。

Citrix Managed Azure のセキュリティの技術概要

May 17, 2024

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

次の図に、Citrix Managed Azure を使用する Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）展開に含まれるコンポーネントを示します。この例では、VNet ピアリング接続を使用しています。



Citrix Managed Azure を使用すると、デスクトップとアプリを提供する顧客の Virtual Delivery Agent（VDA）と Citrix Cloud Connector が、Citrix 管理の Azure サブスクリプションとテナントに展開されます。

Citrix クラウドベースのコンプライアンス

2021 年 1 月時点で、さまざまなエディションの Citrix DaaS および Workspace Premium Plus での Citrix Managed Azure Capacity の使用は、Citrix SOC 2（タイプ 1 または 2）、ISO 27001、HIPAA、またはその他のクラウドコンプライアンスの要件に対して評価されていません。Citrix Cloud の認定について詳しくは、「Citrix Trust Center」を参照してください。また、頻繁に更新を確認してください。

Citrix の責任

ドメイン非参加カタログ用の **Citrix Cloud Connector**

Citrix Managed Azure サブスクリプションを使用する場合、Citrix DaaS は各リソースの場所に少なくとも 2 つの Cloud Connector を展開します。一部のカタログは、同じ顧客の他のカタログと同じリージョンにある場合、リソースの場所を共有することができます。

Citrix は、ドメイン非参加カタログの Cloud Connector に対する以下のセキュリティ操作に責任があります:

- オペレーティングシステムの更新とセキュリティパッチの適用
- アンチウイルスプログラムのインストールと保守
- Cloud Connector ソフトウェア更新プログラムの適用

顧客には Cloud Connector へのアクセス権限はありません。そのため、Citrix は、ドメイン非参加カタログ Cloud Connector のパフォーマンスに全責任を負います。

Azure サブスクリプションと **Azure Active Directory**

Citrix は、顧客向けに作成された Azure サブスクリプションと Azure Active Directory（AAD）のセキュリティに責任があります。Citrix はテナント分離を保証しているため、各顧客は自身の Azure サブスクリプションと AAD を持ち、異なるテナント間の混線は防止されます。また、Citrix は、AAD へのアクセスを Citrix DaaS と Citrix 運用担当者のみに制限しています。Citrix による各顧客の Azure サブスクリプションへのアクセスは監査されます。

ドメイン非参加カタログを使用している顧客は、Citrix Workspace の認証手段として Citrix 管理の AAD を使用できます。これらの顧客のために、Citrix は Citrix 管理の AAD で制限付き特権のユーザーアカウントを作成します。ただし、顧客のユーザーも管理者も、Citrix 管理の AAD に対して操作を行うことはできません。これらの顧客が代わりに独自の AAD を使用することを選択した場合、そのセキュリティについては顧客が全責任を負います。

仮想ネットワークとインフラストラクチャ

顧客の Citrix Managed Azure サブスクリプション内で、Citrix はリソースの場所を分離するための仮想ネットワークを作成します。Citrix は、これらのネットワーク内で、ストレージアカウント、Key Vault、およびその他の Azure リソースに加え、VDA、Cloud Connector、およびイメージビルダーマシン用の仮想マシンを作成します。Citrix は、Microsoft と提携し、仮想ネットワークファイアウォールを含む仮想ネットワークのセキュリティに対する責任を負います。

Citrix は、デフォルトの Azure ファイアウォールポリシー（ネットワークセキュリティグループ）が、VNet ピアリングおよび SD-WAN 接続のネットワークインターフェイスへのアクセスを制限するように構成されていることを保証します。通常、これは VDA と Cloud Connector への受信トラフィックを制御します。詳しくは、次のページを参照してください:

- Azure VNet ピアリング接続のファイアウォールポリシー

- SD-WAN 接続のファイアウォールポリシー

顧客はこのデフォルトのファイアウォールポリシーを変更することはできませんが、Citrix が作成した VDA マシンに追加のファイアウォール規則を展開することはできます。たとえば、送信トラフィックを部分的に制限できます。Citrix が作成した VDA マシンに、仮想プライベートネットワーククライアント、またはファイアウォール規則をバイパスできるその他のソフトウェアをインストールする顧客は、発生する可能性のあるセキュリティリスクに責任を負います。

Citrix DaaS でイメージビルダーを使用して新しいマシンイメージを作成およびカスタマイズする場合、ポート 3389～3390 が Citrix 管理の VNet で一時的に開かれるため、顧客は新しいマシンイメージを含むマシンに RDP（リモートデスクトッププロトコル）を使用することができ、そのマシンをカスタマイズできます。

Azure VNet ピアリング接続を使用する場合の **Citrix** の責任

Citrix DaaS の VDA がオンプレミスのドメインコントローラー、ファイル共有、またはその他のイントラネットリソースに接続するために、Citrix DaaS は接続オプションとして VNet ピアリングワークフローを提供します。顧客の Citrix 管理の仮想ネットワークは、顧客管理の Azure 仮想ネットワークとピアリングされます。顧客管理の仮想ネットワークでは、Azure ExpressRoute や IPsec トンネルなど、顧客が選択したクラウドからオンプレミスへの接続のソリューションを使用して、顧客のオンプレミスリソースとの接続を有効にすることができます。

VNet ピアリングに対する Citrix の責任は、Citrix と顧客が管理する VNet 間のピアリング関係を確立するためのワークフローと、関連する Azure リソース構成をサポートすることに限定されます。

Azure VNet ピアリング接続のファイアウォールポリシー　Citrix は、VNet ピアリング接続を使用する受信および送信トラフィック用に、以下のポートを開いたり閉じたりします。

ドメイン非参加マシンを使用した **Citrix** 管理の **VNet**

- 受信規則
  - VDA から Cloud Connector へ、および Cloud Connector から VDA への受信には、ポート 80、443、1494、および 2598 を許可します。
  - モニターシャドウイング機能で使用される IP 範囲から VDA への受信には、ポート 49152～65535 を許可します。「Citrix テクノロジで使用される通信ポート」を参照してください。
  - 他のすべての受信を拒否します。これには、VDA から VDA への、および VDA から Cloud Connector への VNet 内トラフィックが含まれます。
- 送信規則
  - すべての送信トラフィックが許可されます。

ドメイン参加済みマシンがある **Citrix** 管理の **VNet**

- 受信規則:
  - VDA から Cloud Connector へ、および Cloud Connector から VDA への受信には、ポート 80、443、1494、および 2598 を許可します。
  - モニターシャドウイング機能で使用される IP 範囲から VDA への受信には、ポート 49152～65535 を許可します。「Citrix テクノロジで使用される通信ポート」を参照してください。
  - 他のすべての受信を拒否します。これには、VDA から VDA への、および VDA から Cloud Connector への VNet 内トラフィックが含まれます。
- 送信規則
  - すべての送信トラフィックが許可されます。

ドメイン参加済みマシンがある顧客管理の **VNet**

- VNet を正しく構成することは顧客の責任です。この責任には、ドメイン参加のために以下のポートを開くことが含まれます。
- 受信規則:
  - 内部起動のために、クライアント IP からの 443、1494、2598 での受信を許可します。
  - Citrix VNet（顧客が指定した IP 範囲）からの 53、88、123、135～139、389、445、636 での受信を許可します。
  - プロキシ構成で開いたポートでの受信を許可します。
  - 顧客が作成したその他の規則。
- 送信規則:
  - 内部起動のために、Citrix VNet（顧客が指定した IP 範囲）への 443、1494、2598 での送信を許可します。
  - 顧客が作成したその他の規則。

SD-WAN 接続を使用する場合の **Citrix** の責任

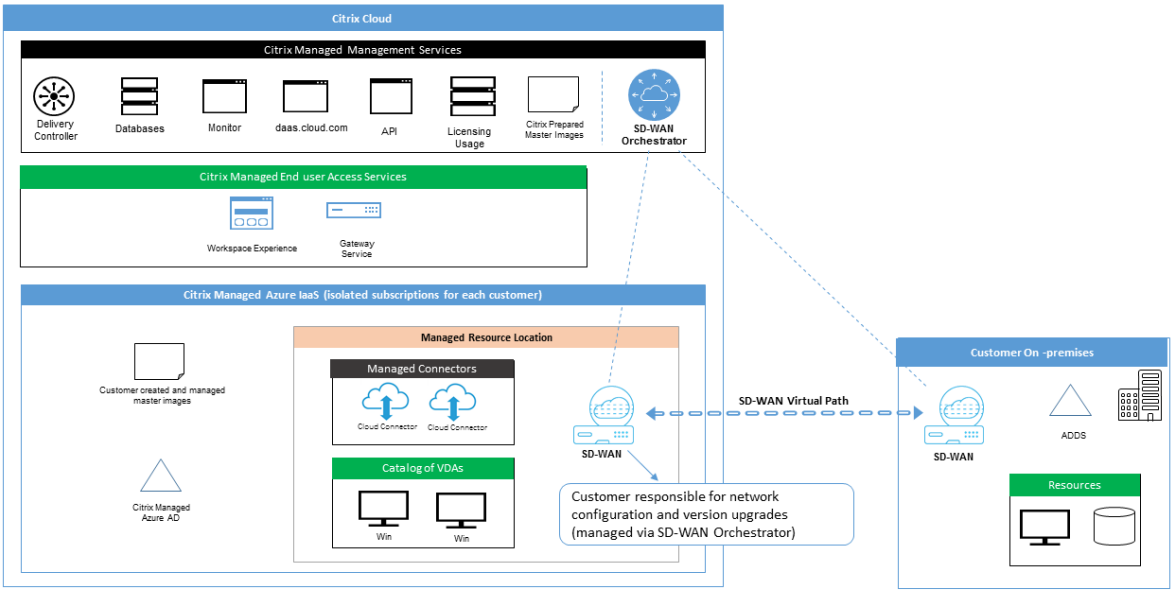
Citrix は、仮想 Citrix SD-WAN インスタンスを完全に自動で展開する方法をサポートしており、これにより Citrix DaaS とオンプレミスリソースとの間の接続が可能です。Citrix SD-WAN 接続には、VNet ピアリングと比較して次のようないくつかのメリットがあります:

VDA からデータセンターへ、および VDA からブランチ（ICA）への接続の高い信頼性とセキュリティ。

- 高度な QoS（サービス品質）機能と VoIP（ボイスオーバー IP）最適化機能を備えた、オフィスワーカーにとって最高のエンドユーザーエクスペリエンス。
- Citrix HDX ネットワークトラフィックとその他のアプリケーションの使用状況を検査、優先順位付け、およびレポートする組み込み機能。

Citrix は、Citrix DaaS で SD-WAN 接続を利用する顧客が、SD-WAN Orchestrator を使用して Citrix SD-WAN ネットワークを管理することを求めます。

次の図は、Citrix Managed Azure サブスクリプションと SD-WAN 接続を使用した Citrix DaaS 展開に追加されたコンポーネントを示しています。



Citrix DaaS の Citrix SD-WAN 展開は、Citrix SD-WAN の標準の Azure 展開構成に似ています。詳しくは、「Citrix SD-WAN Standard Edition インスタンスの Azure への展開」を参照してください。高可用性構成では、Azure Load Balancer を使用した SD-WAN インスタンスのアクティブ/スタンバイペアは、VDA と Cloud Connector を含むサブネットとインターネットの間のゲートウェイとして展開されます。高可用性ではない構成では、単一の SD-WAN インスタンスのみがゲートウェイとして展開されます。仮想 SD-WAN アプライアンスのネットワークインターフェイスには、2 つのサブネットに分割された個別の小さなアドレス範囲からアドレスが割り当てられます。

SD-WAN 接続を構成する場合、Citrix は上記の管理対象デスクトップのネットワーク構成にいくつかの変更を加えます。特に、インターネットの宛先へのトラフィックなど、VNet からの送信トラフィックはすべて、クラウド SD-WAN インスタンスを介してルーティングされます。SD-WAN インスタンスは、Citrix 管理の VNet の DNS サーバーとしても構成されます。

仮想 SD-WAN インスタンスへの管理アクセスには、管理者のログインとパスワードが必要です。SD-WAN の各インスタンスには、SD-WAN 管理者が、SD-WAN Orchestrator UI、仮想アプライアンス管理 UI、および CLI を介してリモートログインしたりトラブルシューティングしたりするための、ランダムで安全な一意のパスワードが割り当てられます。

他のテナント固有のリソースと同様に、特定の顧客の VNet に展開された仮想 SD-WAN インスタンスは、他のすべての VNet から完全に分離されます。

顧客が Citrix SD-WAN 接続を有効にする場合、Citrix は、Citrix DaaS で使用される仮想 SD-WAN インスタンスの

初期展開を自動化し、基盤となる Azure リソース（仮想マシン、ロードバランサーなど）を保守し、仮想 SD-WAN インスタンスの初期構成について安全で効率的な追加設定不要のデフォルト設定を提供し、SD-WAN Orchestrator を使用した継続的な保守とトラブルシューティングを可能にします。また、Citrix は合理的な対策を講じて、SD-WAN ネットワーク構成の自動検証を実行し、既知のセキュリティリスクをチェックし、SD-WAN Orchestrator を使用して対応する通知を表示します。

SD-WAN 接続のファイアウォールポリシー　Citrix は、Azure ファイアウォールポリシー（ネットワークセキュリティグループ）とパブリック IP アドレスの割り当てを使用して、仮想 SD-WAN アプライアンスのネットワークインターフェイスへのアクセスを制限します:

- WAN および管理インターフェイスのみにパブリック IP アドレスが割り当てられ、インターネットへの送信接続を許可します。
- Citrix 管理の VNet のゲートウェイとして機能する LAN インターフェイスは、同じ VNet 上の仮想マシンとのみネットワークトラフィックを交換できます。
- WAN インターフェイスは、（仮想パス接続のために Citrix SD-WAN によって使用される）UDP ポート 4980 への受信トラフィックを制限し、VNet への送信トラフィックを拒否します。
- 管理ポートは、ポート 443（HTTPS）および 22（SSH）への受信トラフィックを許可します。
- HA（高可用性）インターフェイスは、相互に制御トラフィックを交換することのみが許可されます。

インフラストラクチャへのアクセス

Citrix は、顧客の Citrix 管理インフラストラクチャ（Cloud Connector）にアクセスして、顧客に通知せずに、ログの収集（Windows イベントビューアーなど）やサービスの再起動などの特定の管理タスクを実行することがあります。Citrix は、これらのタスクを安全かつ確実に実行し、顧客への影響を最小限に抑える責任があります。また、Citrix は、ログファイルが安全かつ確実に取得、転送、および処理されるようにする責任があります。この方法では、顧客の VDA にアクセスすることはできません。

ドメイン非参加カタログのバックアップ

Citrix は、ドメイン非参加カタログのバックアップを実行する責任を負いません。

マシンイメージのバックアップ

Citrix は、イメージビルダーで作成されたイメージなど、Citrix DaaS にアップロードされたすべてのマシンイメージをバックアップする責任があります。Citrix は、これらのイメージにローカル冗長ストレージを使用します。

ドメイン非参加カタログのバックアップのための踏み台マシン

Citrix の運用担当者は、必要に応じて、顧客の Citrix 管理の Azure サブスクリプションにアクセスして、顧客の問題を診断および修復するための踏み台マシンを作成できます。これは、顧客が問題に気付く前に行われる可能性があります。Citrix は、踏み台マシンを作成するために顧客の同意を必要としません。Citrix が踏み台マシンを作成する場合、Citrix は踏み台マシンに対してランダムに生成される強力なパスワードを作成し、Citrix NAT IP アドレスへの RDP アクセスを制限します。踏み台マシンが不要になると、Citrix 踏み台マシンを処分し、パスワードは無効になります。踏み台マシン（およびそれに付随する RDP アクセス規則）は、操作が完了すると破棄されます。Citrix は、踏み台マシンを使用して、顧客のドメイン非参加の Cloud Connector にのみアクセスできます。Citrix には、ドメイン非参加 VDA またはドメイン参加済み Cloud Connector と VDA にログインするためのパスワードがありません。

トラブルシューティングツールを使用する場合のファイアウォールポリシー

顧客がトラブルシューティングのために踏み台マシンの作成を要求する場合、Citrix 管理の VNet に対して以下のセキュリティグループの変更が行われます：

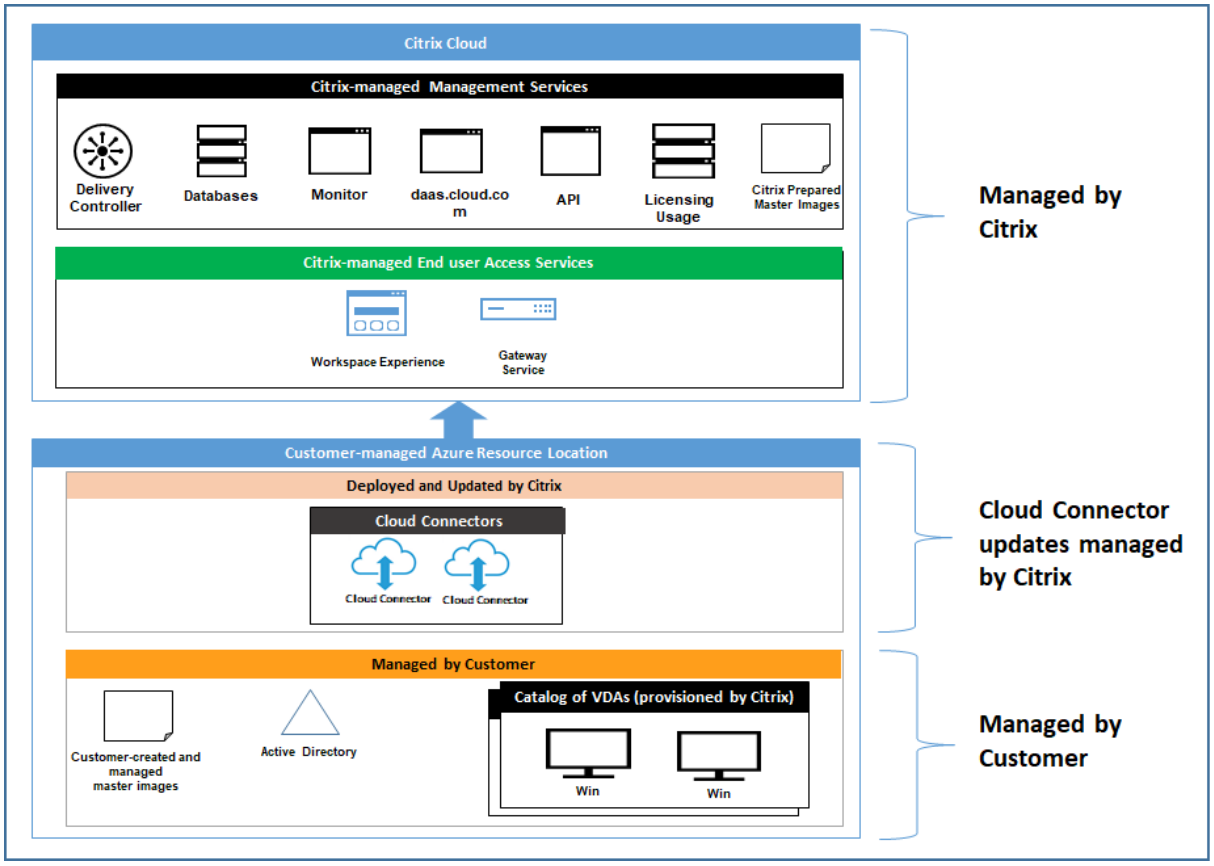
- 顧客指定の IP 範囲から踏み台マシンへの受信に、一時的にポート 3389 を許可します。
- 踏み台マシンの IP アドレスから VNet（VDA および Cloud Connector）内の任意のアドレスへの受信に、一時的にポート 3389 を許可します。
- Cloud Connector、VDA、およびその他の VDA の間の RDP アクセスを引き続き禁止します。

顧客がトラブルシューティングのために RDP アクセスを有効にする場合、Citrix 管理の VNet に対して以下のセキュリティグループの変更が行われます：

- 顧客指定の IP 範囲から VNet（VDA および Cloud Connector）内の任意のアドレスへの受信に、一時的にポート 3389 を許可します。
- Cloud Connector、VDA、およびその他の VDA の間の RDP アクセスを引き続き禁止します。

顧客管理のサブスクリプション

顧客管理のサブスクリプションの場合、Citrix は、Azure リソースの展開時に上記の責任を順守します。展開後、顧客は Azure サブスクリプションの所有者であるため、上記のすべては顧客の責任になります。



顧客の責任

VDA とマシンイメージ

顧客は、以下のような、VDA マシンにインストールされているソフトウェアのすべての側面について責任を負います:

- オペレーティングシステムの更新プログラムとセキュリティパッチ
- ウイルス対策とマルウェア対策
- VDA ソフトウェアの更新プログラムとセキュリティパッチ
- 追加のソフトウェアファイアウォール規則（特に送信トラフィック）
- Citrix の「セキュリティに関する考慮事項およびベストプラクティス」に従ってください。

Citrix は、出発点として意図的に準備されたイメージを提供します。顧客は、このイメージを概念実証やデモンストレーションの目的で、または独自のマシンイメージを構築するためのベースとして、使用できます。Citrix は、この Citrix 提供イメージのセキュリティを保証しません。Citrix は、Citrix 提供イメージ上のオペレーティングシステムと VDA ソフトウェアを最新の状態に保つようにし、これらのイメージ上で Windows Defender を有効にします。

VNet ピアリングを使用する場合の顧客の責任

お客様は、「ドメイン参加済みマシンがある顧客管理の VNet」で指定されているすべてのポートを開く必要があります。

VNet ピアリングが構成されている場合、顧客は、自身の仮想ネットワークとオンプレミスリソースへの接続のセキュリティに責任があります。また、顧客は、Citrix 管理のピア仮想ネットワークからの受信トラフィックのセキュリティに責任があります。Citrix は、Citrix 管理の仮想ネットワークから顧客のオンプレミスリソースへのトラフィックを禁止するための操作を実行しません。

顧客には、受信トラフィックを制限するための以下のオプションがあります:

- Citrix 管理の仮想ネットワークに、顧客のオンプレミスネットワークまたは顧客管理の接続済み仮想ネットワーク内の他の場所で使用されていない IP ブロックを与える。これは VNet ピアリングに必要です。
- 顧客の仮想ネットワークとオンプレミスネットワークに Azure ネットワークセキュリティグループとファイアウォールを追加して、Citrix 管理の IP ブロックからのトラフィックを禁止または制限する。
- Citrix 管理の IP ブロックを対象として、侵入防止システム、ソフトウェアファイアウォール、行動分析エンジンなどの措置を、顧客の仮想ネットワークとオンプレミスネットワークに展開する。

SD-WAN 接続を使用する場合の顧客の責任

SD-WAN 接続が構成されている場合、顧客は、Citrix DaaS で使用される仮想 SD-WAN インスタンスをネットワーク要件に従って極めて柔軟に構成できます。ただし例外として、Citrix 管理の VNet で SD-WAN を確実に正しく動作させるために必要ないくつかの要素があります。顧客の責任には以下のようなものがあります:

- DNS とインターネットトラフィックブレークアウトの規則など、ルーティングとファイアウォールの規則の設計と構成。
- SD-WAN ネットワーク構成の保守。
- ネットワークの運用ステータスの監視。
- Citrix SD-WAN ソフトウェアの更新またはセキュリティの修正のタイムリーな展開。顧客のネットワーク上の Citrix SD-WAN のすべてのインスタンスで、同じバージョンの SD-WAN ソフトウェアを使う必要があるため、更新したバージョンのソフトウェアを Citrix DaaS の SD-WAN インスタンスに展開し、顧客のネットワーク保守スケジュールと制約に従って管理する必要があります。

SD-WAN ルーティングとファイアウォール規則の不適切な構成、または SD-WAN 管理パスワードの誤った管理により、Citrix DaaS の仮想リソースと、Citrix SD-WAN 仮想パスを介して到達可能なオンプレミスリソースの両方に、セキュリティリスクが生じる可能性があります。また、Citrix SD-WAN ソフトウェアを最新の利用可能なパッチリリースに更新しないことにより、セキュリティリスクが生じる可能性もあります。SD-WAN Orchestrator とその他の Citrix Cloud サービスはこうしたリスクに対処するための手段を提供しますが、顧客は仮想 SD-WAN インスタンスが適切に構成されていることを確認する最終的な責任があります。

プロキシ

顧客は、VDA からの送信トラフィックにプロキシを使用するかどうかを選択できます。プロキシを使用する場合、顧客は以下の責任を負います:

- VDA マシンイメージでプロキシ設定を構成してあるか、VDA がドメイン参加済みである場合は、Active Directory グループポリシーを使用します。
- プロキシの保守とセキュリティ。

Citrix Cloud Connector またはその他の Citrix 管理のインフラストラクチャでプロキシを使用することは許可されていません。

カタログの回復性

Citrix は、回復性のレベルが異なる 3 種類のカタログを提供しています:

- 静的: 各ユーザーは、単一の VDA に割り当てられます。このカタログタイプは高可用性を提供しません。ユーザーの VDA がダウンした場合、回復するには新しい VDA に配置される必要があります。Azure は、シングルインスタンス VM に 99.5% の SLA を提供します。顧客は引き続きユーザープロファイルをバックアップできますが、VDA に対して行われたカスタマイズ（プログラムのインストールや Windows の構成など）は失われます。
- ランダム: 各ユーザーは、起動時にサーバー VDA にランダムに割り当てられます。このカタログタイプは、冗長性により高可用性を提供します。VDA がダウンしても、ユーザーのプロファイルが他の場所にあるため、情報が失われることはありません。
- **Windows 10** マルチセッション: このカタログタイプはランダムタイプと同じように動作しますが、サーバー VDA の代わりに Windows10 ワークステーション VDA を使用します。

ドメイン参加済みカタログのバックアップ

顧客が VNet ピアリングでドメイン参加済みカタログを使用している場合、顧客はユーザープロファイルをバックアップする責任があります。オンプレミスのファイル共有を構成し、Active Directory または VDA にポリシーを設定して、これらのファイル共有からユーザープロファイルを取得することをお勧めします。顧客は、これらのファイル共有のバックアップと可用性に責任があります。

障害回復

Azure データが失われた場合、Citrix は Citrix 管理の Azure サブスクリプション内のリソースを可能な限り多く回復します。Citrix は、Cloud Connector と VDA の回復を試みます。Citrix がこれらのアイテムの回復に失敗した場合、顧客には新しいカタログを作成する責任があります。Citrix は、マシンイメージがバックアップされており、顧客がユーザープロファイルをバックアップして、カタログを再構築できることを前提としています。

Azure リージョン全体が失われた場合、顧客は、顧客管理の仮想ネットワークを新しいリージョンで再構築し、Citrix DaaS 内に新しい VNet ピアリングまたは新しい SD-WAN インスタンスを作成する責任があります。

Citrix と顧客が共有する責任

ドメイン参加済みカタログ用の **Citrix Cloud Connector**

Citrix DaaS は各リソースの場所に少なくとも 2 つの Cloud Connector を展開します。一部のカタログは、同じ顧客の他のカタログと同じリージョン、VNet ピアリング、ドメインにある場合、リソースの場所を共有することができます。Citrix は、顧客のドメイン参加済み Cloud Connector を、イメージ上で次のようなセキュリティデフォルト設定に構成します:

- オペレーティングシステムの更新プログラムとセキュリティパッチ
- アンチウイルスプログラム
- Cloud Connector ソフトウェア更新プログラム

顧客には通常、Cloud Connector へのアクセス権限はありません。ただし、カタログのトラブルシューティング手順に従い、ドメインの資格情報を使用してログインすることで、アクセス権限を取得できます。踏み台マシンからログインするときに行った変更については、顧客の責任となります。

顧客は、Active Directory グループポリシーにより、ドメイン参加済み Cloud Connector を制御することもできます。顧客は、Cloud Connector に適用されるグループポリシーが安全で適切であることを確認する責任があります。たとえば、顧客がグループポリシーを使用してオペレーティングシステムの更新を無効にすることを選択した場合、顧客には Cloud Connector でオペレーティングシステムの更新を実行する責任があります。また、顧客は、グループポリシーを使用して、別のアンチウイルスプログラムをインストールするなど、Cloud Connector のデフォルト設定よりも厳格なセキュリティを適用できます。通常、顧客には、ポリシーを使用せず、自身の Active Directory の組織単位に Cloud Connector を配置することをお勧めします。これにより、Citrix が使用するデフォルト設定を問題なく適用できるようになります。

トラブルシューティング

Citrix DaaS のカタログで問題が発生した場合、トラブルシューティングのために次の 2 つのオプションがあります: 踏み台マシンの使用、RDP アクセスの有効化。どちらのオプションも、顧客にセキュリティリスクをもたらします。顧客は、これらのオプションを使用する前に、このリスクを引き受けることを理解し、同意する必要があります。

Citrix は、トラブルシューティング操作を実行するために必要なポートを開閉し、これらの操作中にアクセスできるマシンを制限する責任があります。

踏み台マシンまたは RDP アクセスのいずれかを使用して操作を実行するアクティブユーザーは、アクセスするマシンのセキュリティに責任を負います。顧客が RDP で VDA または Cloud Connector にアクセスし、誤ってウイルスに感染した場合、顧客の責任となります。Citrix のサポート担当者がこれらのマシンにアクセスする場合、安全に操作を実行することはそれらのサポート担当者の責任です。環境内の踏み台マシンや他のマシンにアクセスする人物に

よって生じる脆弱性に対する責任（リストを許可するために IP 範囲を追加する顧客の責任、IP 範囲を正しく実装する Citrix の責任など）については、本ドキュメントの他の場所に説明があります。

どちらのシナリオでも、Citrix はファイアウォールの例外を正しく作成して、RDP トラフィックを許可することに責任があります。Citrix には、顧客が踏み台マシンを処分した後、または Citrix DaaS を介した RDP アクセスを終了した後、これらの例外を取り消す責任もあります。

踏み台マシン　Citrix は、顧客の Citrix 管理サブスクリプション内で顧客の Citrix 管理仮想ネットワークに踏み台マシンを作成し、事前に（顧客への通知なしに）、または顧客が引き起こした問題に対応して、問題を診断および修復することができます。踏み台マシンは、顧客が RDP でアクセスし、RDP で VDA と（ドメイン参加済みカタログの場合は）Cloud Connector にアクセスして、ログの収集、サービスの再起動、またはその他の管理タスクを実行するために使用できるマシンです。デフォルトでは、踏み台マシンを作成すると外部のファイアウォール規則が開き、顧客が指定した範囲の IP アドレスからの踏み台マシンへの RDP トラフィックが許可されます。また、内部のファイアウォール規則が開き、Cloud Connector と VDA への RDP アクセスを許可します。これらの規則が開くと、大きなセキュリティリスクが生じます。

顧客は、ローカルの Windows アカウントで使用するパスワードを強力なものにする責任があります。顧客は、踏み台マシンへの RDP アクセスを可能にする外部 IP アドレス範囲を指定する責任もあります。顧客が IP 範囲を指定しないことを選択した場合（誰でも RDP アクセスできるようにした場合）、悪意のある IP アドレスからのアクセスに対しては顧客が責任を負います。

顧客は、トラブルシューティングが完了した後、踏み台マシンを削除する責任もあります。踏み台マシンホストはさらに攻撃対象領域をさらすため、Citrix は電源を入れてから 8 時間後にマシンを自動的にシャットダウンします。ただし、Citrix が踏み台マシンを自動的に削除することはありません。顧客が期間を延長して踏み台マシンを使用することを選択した場合、顧客にはそれにパッチを適用して更新していく責任があります。踏み台マシンは数日間だけ使用したのち削除することをお勧めします。顧客が最新の踏み台マシンを希望する場合は、現在の踏み台マシンを削除してから新しい踏み台マシンを作成できます。これにより、最新のセキュリティパッチが適用された新しいマシンがプロビジョニングされます。

RDP アクセス　ドメイン参加済みカタログの場合、顧客の VNet ピアリングが機能していれば、顧客はピアリングされた VNet から Citrix 管理の VNet への RDP アクセスを有効にできます。顧客がこのオプションを使用する場合、顧客は VNet ピアリングを介して VDA および Cloud Connector にアクセスする責任があります。送信元 IP アドレスの範囲を指定できるため、顧客の内部ネットワーク内であっても、RDP アクセスをさらに制限できます。顧客は、ドメイン資格情報を使用してこれらのマシンにログインする必要があります。顧客が Citrix のサポート担当者と協力して問題を解決している場合、顧客はこれらの資格情報をサポート担当者と共有する必要がある場合があります。問題が解決した後、顧客は RDP アクセスを無効にする責任があります。顧客のピアネットワークまたはオンプレミスネットワークから RDP アクセスを開いたままにしておくと、セキュリティリスクが発生します。

ドメイン資格情報

顧客がドメイン参加済みカタログを使用することを選択した場合、顧客は、マシンをドメインに参加させるためのアクセス権限があるドメインアカウント（ユーザー名とパスワード）を Citrix DaaS に提供する責任があります。ドメイン資格情報を提供する場合、顧客は次のセキュリティ原則を順守する責任があります：

- 監査可能：アカウントを Citrix DaaS 用として作成し、アカウントの使用目的を容易に監査できるようにする必要があります。
- スコープ：アカウントには、マシンをドメインに参加させるためのアクセス権限のみが必要です。完全なドメイン管理者にするべきではありません。
- 安全：アカウントには強力なパスワードを設定する必要があります。

Citrix には、顧客の Citrix 管理の Azure サブスクリプション内で、Azure Key Vault にこのドメインアカウントを安全に保存する責任があります。このアカウントは、ドメインアカウントのパスワードが操作に必要な場合にのみ取得します。

追加情報

関連情報については、以下を参照してください：

- セキュリティで保護された Citrix Cloud プラットフォームの展開ガイド：Citrix Cloud プラットフォームのセキュリティ情報。
- セキュリティの技術概要：Citrix DaaS のセキュリティ情報
- サードパーティ通知

仮想チャネルの許可リスト

May 17, 2024

仮想チャネル許可リストは、環境内で許可される Citrix 以外の仮想チャネルを制御できる機能です。デフォルトでは、仮想チャネル許可リスト機能が有効になっています。その結果、Citrix 仮想チャネルのみが Citrix Virtual Apps and Desktops セッションで開けるようになっています。自社製、サードパーティ製を問わず、カスタム仮想チャネルを使用する必要がある場合は、これらを許可リストに明示的に追加する必要があります。

構成

仮想チャネル許可リストがデフォルトで有効になっています。この機能は、Citrix ポリシーの次の設定を使用して構成できます：

- 仮想チャネル許可リスト：機能を有効または無効にし、仮想チャネルをリストに追加します。

- 仮想チャネルの許可リストのログ調整：仮想チャネル許可リストのイベント ログの調整期間を設定します。
- 仮想チャネル許可リストのログ：仮想チャネル許可リストのログレベルを設定します。

許可リストへの仮想チャネルの追加

仮想チャネルを許可リストに追加するには、次の情報が必要です：

1. コードで定義されている仮想チャネル名。最大 7 文字の長さにすることができます。例：`CTXCVC1`。
2. VDA マシンで仮想チャネルを開くプロセスのパス。例：`C:\Program Files\Application\run.exe`。

必要な情報を取得したら、仮想チャネルの許可リストポリシー設定を使用して、仮想チャネルを許可リストに追加する必要があります。仮想チャネルをリストに追加するには、仮想チャネル名のあとにコンマを入力してから、その仮想チャネルにアクセスするプロセスへのパスを入力します。プロセスが複数ある場合は、各プロセスをコンマで区切って追加できます。

単一プロセスの場合

前の例を使用して、以下のエントリをリストに追加します：

```
CTXCVC1,C:\Program Files\Application\run.exe
```

複数プロセスの場合

複数のプロセスがある場合は、以下のエントリをリストに追加します：

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application\run2.exe
```

ワイルドカード文字の使用

ワイルドカードの使用（*）がサポートされています。アプリケーションのバージョンに基づいてディレクトリまたは実行可能ファイルの名前が変更された場合、またはサードパーティコンポーネントがユーザーのプロファイルにインストールされている場合は、ワイルドカードを使用できます。

ワイルドカードは次のシナリオで使用できます：

- 完全なディレクトリ名を置き換える場合。
  例：`C:\Program Files\Application\*\run1.exe`
- ディレクトリ名の一部を置き換える場合。
  例：`C:\Program Files\Application\v*\run1.exe`

- 実行可能ファイルの名前を置き換える場合。
  例: C:\Program Files\Application\v1.2*.exe
- 実行可能ファイルの名前の一部を置き換える場合。
  例: C:\Program Files\Application\v1.2\run*.exe

次の制限事項が適用されます:

- ワイルドカードは、単一のディレクトリを置き換えるためにのみ使用できます。たとえば、実行可能ファイルがC:\Program Files\Application\v1.2\run1.exeにある場合、以下のようになります
  - 使用可能: C:\Program Files\Application*\run1.exe
  - 使用不可: C:\Program Files*\run1.exe
- エントリにはファイル拡張子が含まれている必要があります。
  - 使用可能: C:\Program Files\Application\v1.2*.exe
  - 使用不可: C:\Program Files\Application\v1.2*
- すべてのパスはローカルである必要があります。

> 注:
>
> - ネットワークパスの使用は許可されていません。
> - ワイルドカードのサポートは、Citrix Virtual Apps and Desktops 2206 から利用できます。
> - ワイルドカードのサポートは、Citrix Virtual Apps and Desktops 2203 LTSR の CU2 から利用できます。

システム環境変数の使用

システム環境変数を使用すると、許可リスト内の信頼できるプロセスの定義を簡素化できます。%programfiles%、%programfiles(x86)%、%systemdrive%、%systemroot%などの通常の変数を使用できます。

システムレベルで定義されている限り、カスタム環境変数を使用することもできます。

次の例は、通常の環境変数を示しています:

- %programfiles%\Application\v1.2\run.exe
- %programfiles%\Application*\run.exe
- %programfiles(x86)%\Application\v1.*\run.exe

次の例は、カスタムのシステム環境変数を示しています:

- カスタム変数名: app
- カスタム変数値: %programfiles%\Application\
- 許可リストのエントリ: CTXCVC1,%app%\run.exe

> 注:
>
> ユーザー環境変数はサポートされていません。
>
> 環境変数のサポートは、Citrix Virtual Apps and Desktops バージョン 2209 から利用できます。

仮想チャネル名とプロセスの取得

仮想チャネルの名前と VDA マシンで仮想チャネルを開くプロセスを取得する最も簡単な方法は、仮想チャネルを提供した開発者またはサードパーティベンダーから情報を取得することです。

別の方法としては、機能のログを適用し、次の手順に従うことで情報を取得することもできます:

1. カスタム仮想チャネルのクライアントコンポーネントとサーバーコンポーネントを配置したら、仮想アプリケーションまたは仮想デスクトップを起動します。
2. VDA マシンのシステムイベントログにて、開こうとしたカスタム仮想チャネルの名前とプロセスを探します。利用可能なイベントについて詳しくは、「イベントログ」を参照してください。
3. セッションからログアウトします。
4. 仮想チャネル許可リストポリシー設定に、識別された仮想チャネルとプロセスに関するエントリを追加します。
5. マシンを再起動してください。
6. VDA が登録されたら、仮想アプリケーションまたは仮想デスクトップを実行して、カスタム仮想チャネルが正常に開くことを確認します。

Citrix 仮想チャネルに関する考慮事項

組み込みの Citrix 仮想チャネルはすべて信頼されており、追加の構成なしで開くことができます。ただし、次の 2 つの機能は、外部の依存関係のために許可リストに明示的なエントリを必要とします:

- マルチメディアリダイレクト
- HDX RealTime Optimization Pack for Skype for Business

マルチメディアリダイレクト

Windows Media Player 以外のメディアプレーヤーをシステムメディアプレーヤーとして使用する場合は、信頼できるプロセスとして許可リストに追加する必要があります。次の情報は、許可リストのエントリに必要です:

- 仮想チャネル名: `CTXMM`
- プロセス: VDA マシンで使用されているメディアプレーヤーのパス。例: `C:\Program Files (x86)\Windows Media Player\wmplayer.exe`。
- 許可リストのエントリ: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

HDX RealTime Optimization Pack for Skype for Business

次の情報は、許可リストのエントリに必要です:

- 仮想チャネル名: `CTXRMEP`
- プロセス: VDA マシン内の Skype for Business 実行可能ファイルのパス。Skype for Business のバージョンや、カスタムインストールパスの使用の有無によって異なる場合があります。例: `C:\Program Files\Microsoft Office\root\Office16\lync.exe`.
- 許可リストのエントリ: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

配信方法

May 24, 2022

1 つの配信方法で、すべてのニーズを満たせることはまずありません。

アプリケーションの配信方法は複数検討することをお勧めします。適切な配信方法を選べば、スケーラビリティ、管理性、ユーザーエクスペリエンスをより高められます。

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

ます。詳しくは、「ローカルアプリケーションアクセスと URL のリダイレクト」を参照してください。

デスクトップについては、Citrix Virtual Apps 公開デスクトップまたは VDI デスクトップを選択できます。

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

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

ユースケース:

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

特長と注意事項:

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

ユーザーエクスペリエンス:

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

プロセス、ホスト、および配信:

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

セッション管理と割り当て:

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

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

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

VM Hosted Apps

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

ユースケース:

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

特長と注意事項:

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

ユーザーエクスペリエンス：

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

プロセス、ホスト、および配信：

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

セッション管理と割り当て：

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

VDI デスクトップ

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

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

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

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

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

リモート **PC** アクセス

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

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

詳しくは、「リモート PC アクセス」を参照してください。

はじめに：展開の計画と構築

May 17, 2024

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

Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）で使用されるコンポーネント、用語、およびオブジェクトについては、「Citrix DaaS」を参照してください。

カスタマージャーニーの観点については、Citrix Success Centerにアクセスしてください。Success Center では、Citrix をご利用いただくにあたり通過する 5 つの主要な段階（プラン、ビルド、ロールアウト、管理、最適化）に関するガイダンスを提供しています。

- Success Center の情報は、この製品ドキュメントに欠かせない重要なものです。
- Success Center の記事とガイドでは、ソリューションに基づいた幅広い視点を提供しています。また、この製品ドキュメントのサービス固有の詳細へのリンクも含まれています

オンプレミスの Citrix Virtual Apps and Desktops 環境から移行する場合は、「クラウドへの移行」を参照してください。

> 重要:
>
> Citrix Cloud およびサブスクライブしている Citrix サービスに関する重要な情報を確実に取得するには、すべてのメール通知を受信できることを確認してください。
>
> Citrix Cloud コンソールの右上隅で、顧客名と OrgID フィールドの右側にあるメニューを展開します。［アカウント設定］を選択します。［マイプロファイル］タブで、［メール通知］セクションのすべてのエントリを選択します。

この記事の使い方

Citrix DaaS 環境を設定するには、以下に示すタスクを完了します。各タスクの詳細へのリンクがあります。

展開を始める前にプロセスの全体像を確認することで、行う操作を把握できます。また、この記事は、その他の役立つ情報ソースへのリンクも掲載しています。

> 注:
>
> ［クイック展開］インターフェイスを使用して Microsoft Azure マシンをプロビジョニングする場合は、「クイック展開ではじめる」のセットアップガイダンスに従ってください。

計画と準備

Success Center のプランガイダンスでは、目標の設定、ユースケースとビジネス目標の定義、潜在的なリスクの特定、およびプロジェクト計画の作成を支援します。

Citrix Tech Zone のドキュメントで、このサービスの段階的な概念実証ガイドを参照してください。

サインアップ

Citrix アカウントを新規登録して、Citrix DaaS のデモをリクエストします。

リソースの場所を設定する

リソースの場所にはユーザーへのアプリケーションおよびデスクトップの配信に必要なリソースが含まれます。リソースの場所を作成すると、DaaS でそれらのリソースを使用できるようになります。リソースの場所について詳しくは、「Citrix Cloud への接続」を参照してください。

マシンを作成する前に、リソースの場所を DaaS に接続する必要があります。

- ドメイン参加済みマシンでは、Cloud Connector がリソースの場所にインストールされている必要があります。この場合、次のことができます:
  - オンプレミスの Active Directory 参加済みカタログの作成

  - Azure Active Directory 参加済みカタログの作成
  - Hybrid Azure Active Directory 参加済みカタログの作成

  可用性を高めるため、リソースの場所ごとに Cloud Connector を 2 つインストールすることをお勧めします。「Cloud Connector のインストール」を参照してください。

  追加情報:

  - リソースの場所と Cloud Connector とは
  - Cloud Connector のインストールに関するビデオ:

- ドメイン非参加マシンでは Cloud Connector は必要ありませんが、Rendezvous V2 が有効になっている必要があります。Rendezvous プロトコルにより、VDA は Cloud Connector をバイパスして直接かつ安全に DaaS に接続できます。「Rendezvous V2」を参照してください。この場合、次のことができます:

  - ドメイン非参加カタログの作成

クイック展開インターフェイスを使用して Azure 仮想マシンをプロビジョニングしている場合、Citrix ではリソースの場所と Cloud Connector が作成されます。

リソースの場所への接続を作成する

リソースの場所と Cloud Connector を追加したら、Citrix DaaS の［完全な構成］インターフェイスを使用してリソースの場所への接続を作成します。

次のいずれかに当てはまる場合、この手順は必要ありません:

- 単純な概念実証環境を構築している

- クイック展開インターフェイスを使用して Azure 仮想マシンをプロビジョニングしている

追加情報:

- ホストとは
- ホスト接続とは

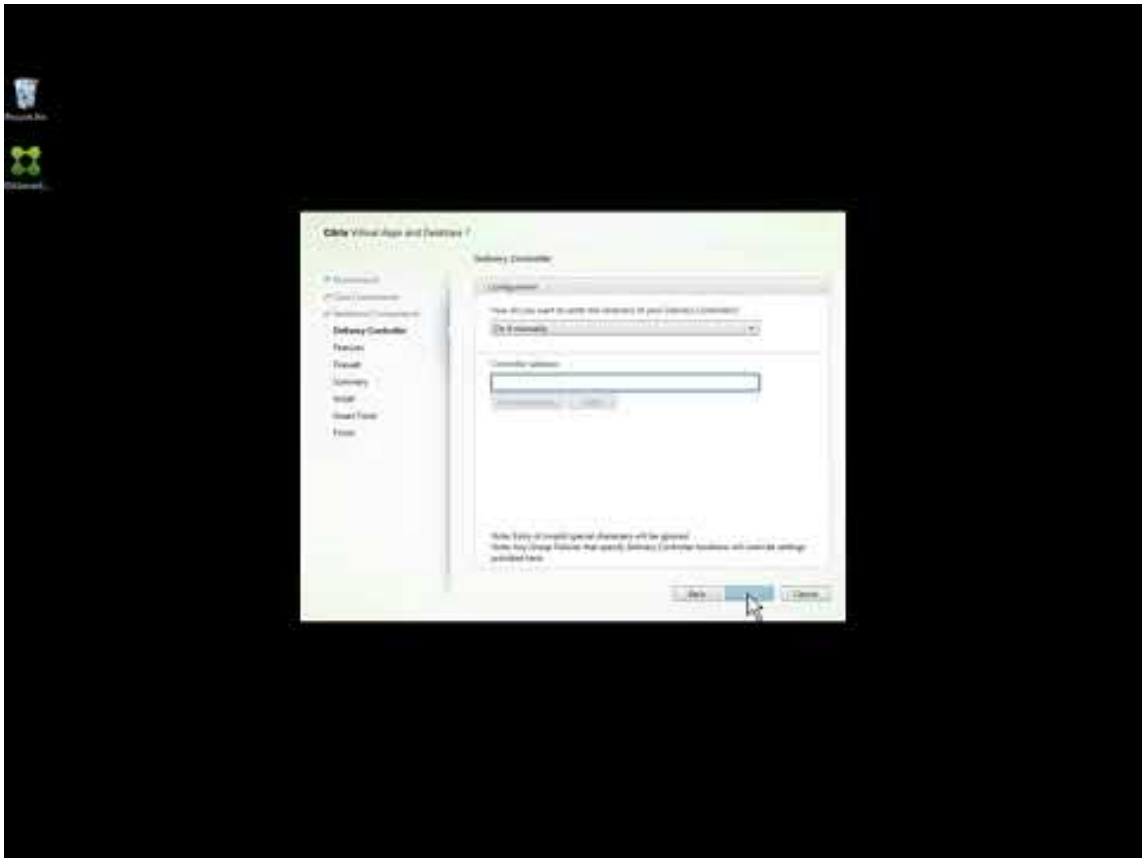
VDA のインストール

アプリケーションとデスクトップをユーザーに配信する各マシンには、Citrix Virtual Delivery Agent（VDA）をインストールする必要があります。

- 単純な概念実証環境を展開する場合は、VDA をダウンロードして 1 台のマシンにインストールします。
- イメージを使用して仮想マシンをプロビジョニングする場合は、イメージに VDA をインストールします。
- リモート PC アクセス機能を使用する場合は、オフィスにある各ユーザーの物理 PC 上にシングルセッション OS 対応 VDA のコアバージョンをインストールします。

ハウツーと詳細情報:

- VDA とは
- インストールの準備と手順
- コマンドラインによる VDA インストール
- VDA のダウンロードとインストールに関するビデオ:

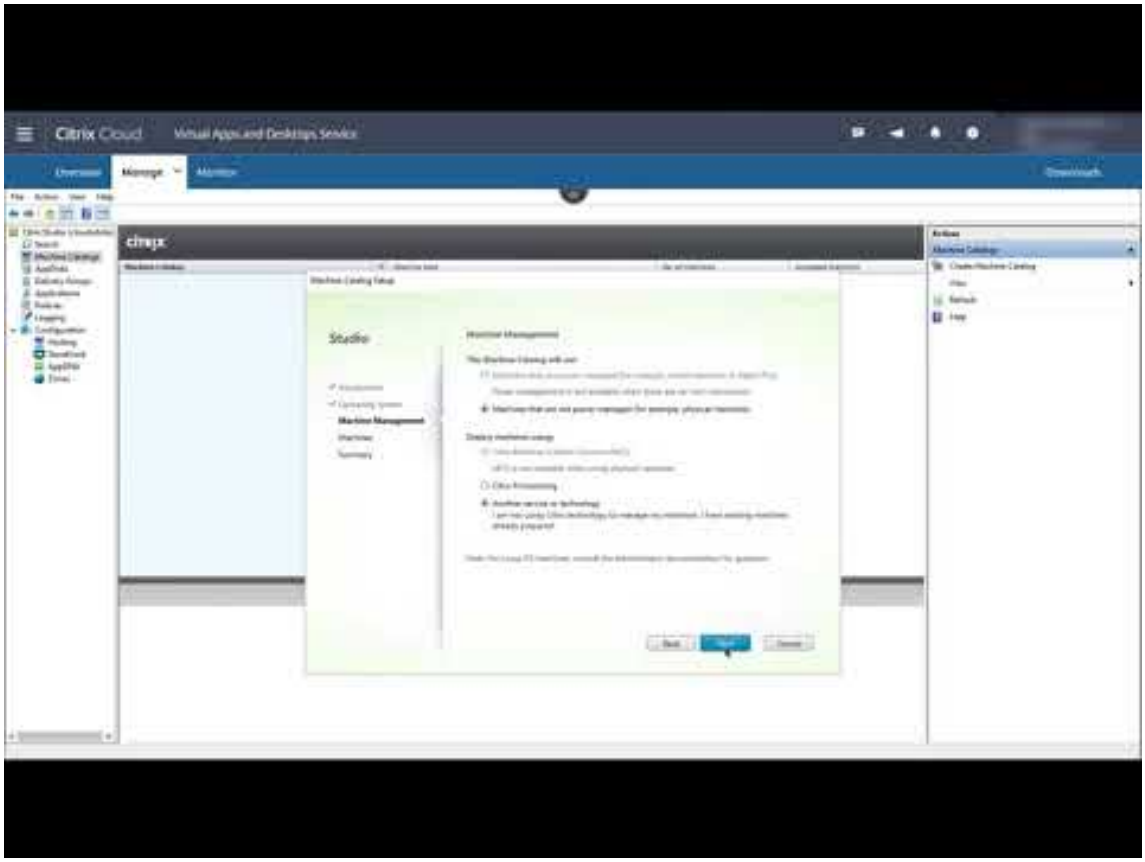


カタログを作成する

リソースの場所への接続を作成すると（必要な場合）、カタログが作成されます。［完全な構成］インターフェイスを使用している場合は、ワークフローによって自動的にこの手順に進みます。

ハウツーと詳細情報：

- カタログとは
- カタログを作成する
- クイック展開インターフェイスを使用して、Azure VM を含むカタログを展開します。
- 完全な構成の管理インターフェイスを使用したカタログの作成に関するビデオ：



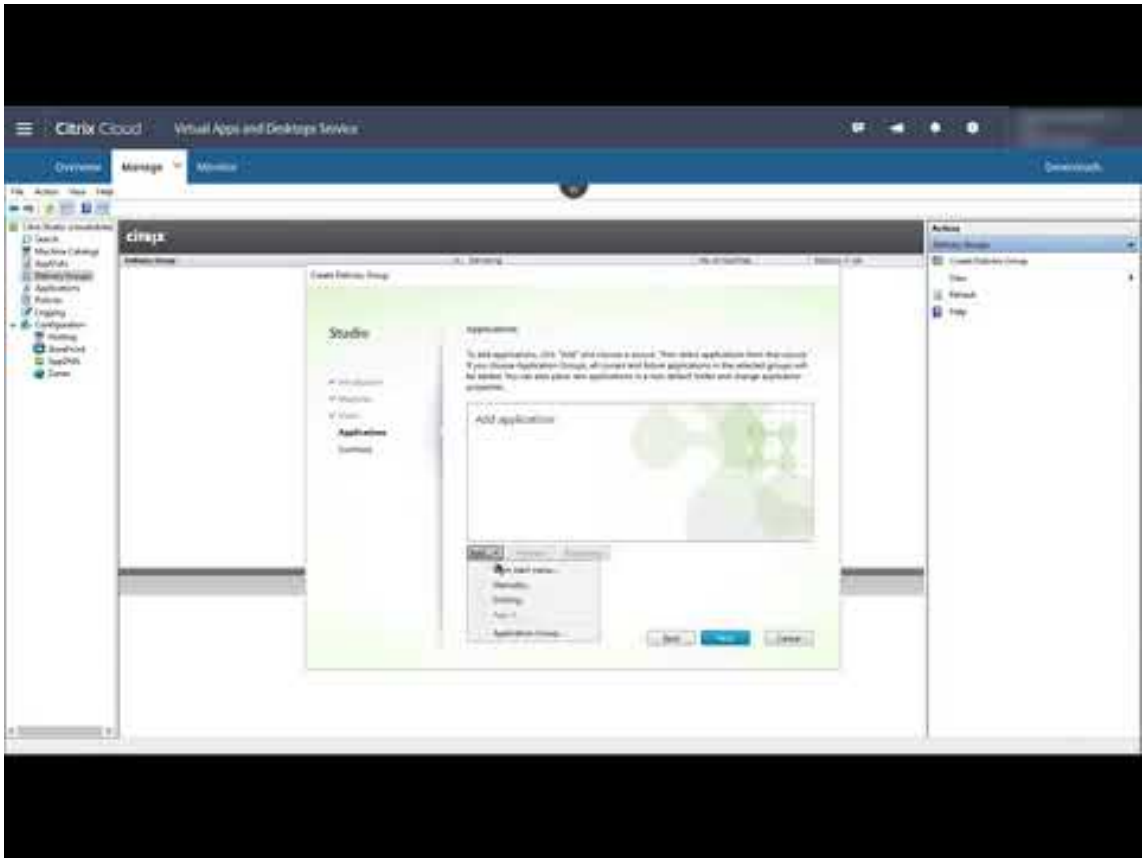
デリバリーグループの作成

最初のカタログを作成すると、サービスの管理ワークフローにデリバリーグループの作成手順が表示されます。

クイック展開インターフェイスを使用して Azure 仮想マシンをプロビジョニングしている場合は、この手順は必要ありません。

ハウツーと詳細情報:

- デリバリーグループとは
- デリバリーグループの作成
- デリバリーグループの作成方法に関するビデオ:



他のコンポーネントとテクノロジの展開

Citrix DaaS 環境をセットアップする上記のタスクを完了したら、Citrix Success Center の「Build」にあるガイダンスに従います。Citrix ソリューションの他のコンポーネントとテクノロジのプロビジョニングと構成に関して確認できる情報は次のとおりです:

- Citrix ポリシー
- StoreFront
- App Layering
- Workspace Environment Management（WEM）サービス
- Citrix Gateway サービス
- ゾーン
- フェデレーション認証サービス（FAS）

構成に適用されるその他のタスクを完了します。たとえば、Windows Server ワークロードの配信を計画している場合は、Microsoft RDS ライセンスサーバーを構成します。

アプリケーションとデスクトップを起動する

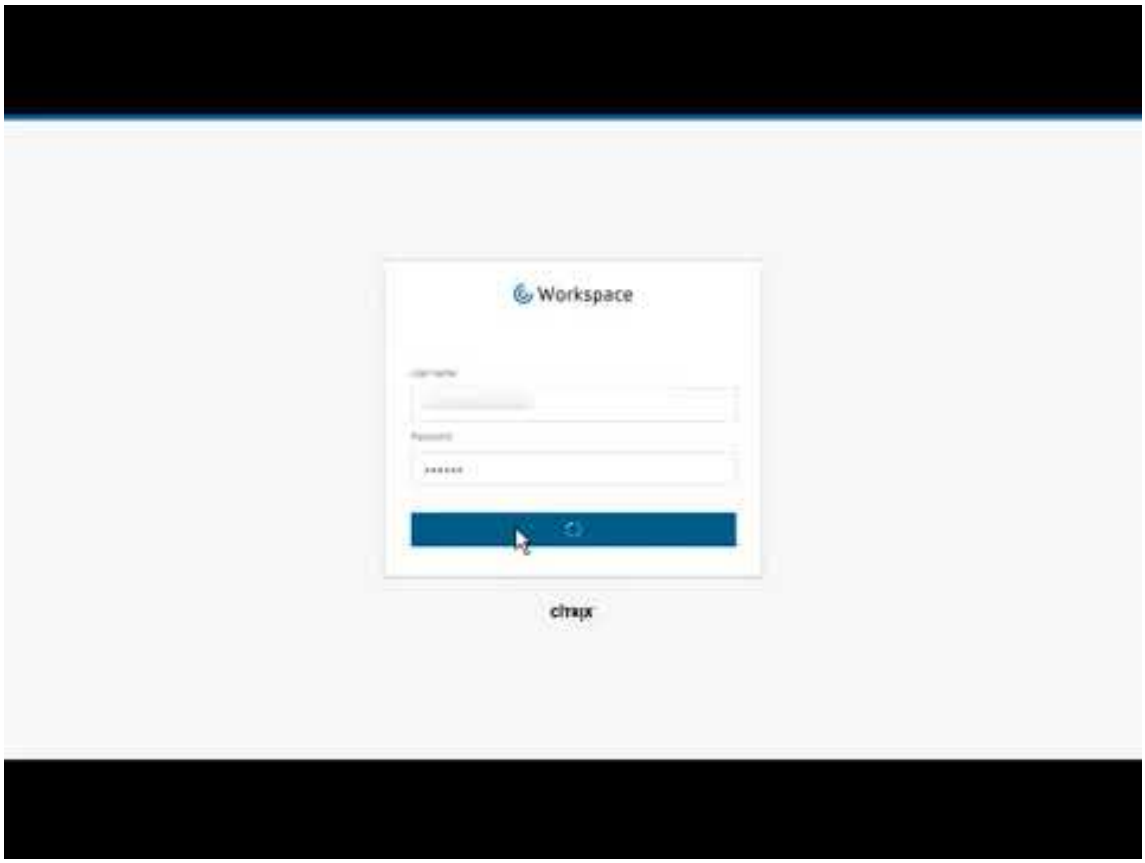
展開を構成すると、公開が自動的に行われます。構成したアプリケーションとデスクトップは、ユーザーが Citrix Workspace 内で利用できます。ユーザーはワークスペース URL にアクセスし、アプリケーションまたはデスクトップを選択するだけで、すぐにそれらを起動できます。

ワークスペース URL をユーザーに送信します。ワークスペース URL は次の 2 つの場所で確認できます:

- Citrix Cloud コンソールで、左上隅のメニューから ［ワークスペースの構成］を選択します。［アクセス］タブに、ワークスペース URL が表示されます。
- Citrix DaaS の ［概要］ページでは、ページの下部にワークスペース URL が表示されます。

追加情報:

- ユーザーが Workspace からアプリケーションやデスクトップを起動する方法に関するビデオ:



追加情報

Citrix Cloud Learning シリーズには、パス別に編成された教育コースが用意されています:

- Citrix DaaS を初めて使用する場合は、Citrix DaaS を初めて使用する場合のラーニングパスを参照してください。

- Citrix Virtual Apps and Desktops 環境から移行する場合は、「Citrix DaaS の Citrix Cloud への移行のラーニングパス」を参照してください。

Citrix DaaS の新規登録

May 24, 2022

はじめに

Citrix または Azure Marketplace から、Citrix DaaS にサブスクライブできます。

Citrix Managed Azureを使用する場合は、シトリックスまたは Azure Marketplace から、Citrix Azure Consumption Fund を購入することもできます。

- シトリックスから購入する場合は、Citrix DaaS と Citrix Azure Consumption Fund を同時に購入できます。
- Azure Marketplace から購入するときは、最初に Citrix DaaS を購入します。次に、Citrix Azure Consumption Fund を別途購入できます。

Citrix DaaS のみを購入する場合は、Azure Marketplace またはシトリックスのアカウント代表者を介して、後から Citrix Azure Consumption Fund を購入できます。

デモとトライアル

シトリックスを経由した要求によって Citrix DaaS を評価できます。トライアルから、有料サービスサブスクリプションに変更できます。

トライアル期間中は、オプションで、カタログ、イメージ、ネットワーク接続に、Citrix Managed Azure サブスクリプションを使用できます。有料サブスクリプションへの変更時に Citrix 管理対象リソースがある場合は、Consumption を購入するか、それらの Citrix 管理対象リソースを削除する必要があります。Consumption を購入しない場合、それらのリソースは自動的に削除され、ユーザーに影響を与えることがあります。

現在 **Citrix DaaS** サービスにサブスクライブしている場合

通常、Citrix Cloud アカウントでは、Citrix OrgID ごとに一度に 1 つの Citrix DaaS のサービス（または、1 つのエディション）にのみサブスクライブできます。たとえば、Citrix DaaS Premium エディションまたは Citrix DaaS for Azure をサブスクライブできますが、両方をサブスクライブすることはできません。

現在 Citrix DaaS にサブスクライブ中で、さらにこのサービスにサブスクライブする場合は、次の 2 つの選択肢があります:

- 別の Citrix Cloud アカウント（OrgID）を使用して、このサービスにサブスクライブする。
- 現在サブスクライブ中の Citrix DaaS を使用停止にしてから、このサービスを購入する。使用停止の指示については、CTX239027を参照してください。

シトリックスから購入する

このサービス（および Citrix Azure Consumption Fund）は、Citrix Cloud またはシトリックスのアカウント代表者を介して購入できます。

Citrix Cloud から：

- 「Citrix Cloud にサインアップする」のガイダンスに従って、Citrix Cloud アカウントと組織 ID を取得します。
- Citrix DaaS のデモを要求できます。Citrix DaaS タイルで、［デモのリクエスト］をクリックします。要求される情報を指定します。

  要件、環境、計画の詳細について、Citrix 担当者が連絡いたします。担当者の評価に応じて、管理者デモまたは概念実証トライアルに参加する権限が付与されます。詳しくは、「Citrix Cloud サービスのトライアル」を参照してください。

トライアルに参加する権限が付与されると、Citrix Cloud コンソールの［Citrix DaaS］タイルのテキストが ［管理］に変わります。

Azure Marketplace から購入する

Azure Marketplace から、次の Citrix 製品を購入できます：

- Citrix DaaS for Azure
- Citrix DaaS Advanced エディション
- Citrix DaaS Premium エディション
- Workspace Premium Plus

Microsoft Azure で Citrix Virtual Apps and Desktops ワークロードをホストする予定で、Citrix Managed Azureサブスクリプションを使用する場合は、Citrix DaaS または Workspace Premium Plus を購入した後に、Citrix Azure Consumption Fund を購入してください。

Citrix Azure Consumption Fund を使用すると、消費した分に対して毎月課金されます。課金額は、選択したホスティングリソースと使用時間によって異なります。Citrix Cloud を介して消費使用量を確認できます。

Azure Marketplace から：

- Citrix DaaS と Consumption Fund を 1 つの注文にまとめることはできません。
- Citrix Azure Consumption Fund の購入プロセスは、基本的に Citrix DaaS の購入と同じですが、事前に Citrix DaaS を購入しておく必要があります。

Azure Marketplace から購入するための要件

- Citrix Cloud アカウントの OrgID。
  - Citrix Cloud アカウントを持っているが、OrgID がわからない場合は、Citrix Cloud コンソールの右上隅を確認してください。または、アカウントの作成時に受け取ったメールをご覧ください。
  - Citrix Cloud アカウントをお持ちでない場合は、「Citrix Cloud にサインアップする」のガイダンスに従ってください。
- Azure アカウントと、そのアカウント内の少なくとも 1 つの Azure サブスクリプション。

Azure Marketplace から購入する手順

この手順に従って、Azure Marketplace から Citrix DaaS または Workspace Premium Plus を購入します（Citrix Managed Azure を使用する場合は、Citrix DaaS を購入した後、Citrix Azure Consumption Fund を別途購入してください）。

1. Azure アカウントの資格情報を使用して、Azure Marketplaceにサインインします。
2. 購入する Citrix 製品を検索して、その製品に移動します。
3. [**Get it now**] を選択します。
4. [**One more thing**] メッセージ上で必要な情報を入力し、同意のチェックボックスをオンにしてから、[**Continue**] を選択します。
5. 製品、プラン、価格、使用状況に関する情報が表示されるタブを確認します。準備ができたら、（複数選択できる場合は）プランを選択し、[**Set up + subscribe**] を選択します。
6. [**Basics**] タブで：
   - **Subscription**：選択したプランが示されます。
   - **Resource group**：リソースグループを選択または作成します。
   - **Name**：後で簡単に識別できるように、購入したサブスクリプションの名前を入力します。
   - [**Plan**] 情報では、選択したプランの課金期間に応じた価格が表示されます。プランの期間を変更するには、[**Change plan**] を選択します。必要な期間を選択し、[**Change plan**] を選択します。
7. [**Review + subscribe**] タブで連絡先情報を確認し、必要に応じて更新します。サブスクリプションの基本情報を確認します。[**Subscribe**] を選択します。
8. [**Subscription in progress**] ページで、[**Configure account now**] を選択します。（ボタンが無効になっている場合は、しばらく待ちます。）Citrix アクティベーションページが表示されます。
9. アクティベーションページで：
   - [**Sign in**] リンクを使用して、Citrix Cloud にサインインします。サインインに成功すると、[**Organization ID**] フィールドに自動的に入力されます。

- **Quantity**: ユーザー数を入力します。(初回購入では 25 以上にする必要があります。) 見積もり価格が表示されます。
- 契約条件に同意してから、[**Activate Order**] を選択します。

Azure Marketplace から購入した後

サービスがプロビジョニングされると、Citrix からメールが届きます。プロビジョニングには時間がかかる場合があります。翌日までにメールが届かない場合は、Citrix サポートまでお問い合わせください。Citrix からメールを受信すると、Citrix DaaS の使用を開始できます。

Citrix Azure Consumption Fund の購入が完了するまで、それほど時間はかかりません。購入したことがシトリックスに通知されると、Citrix DaaS コンソールにバナーが表示され、Citrix Managed Azure サブスクリプションが準備されることが示されます。

Azure の Citrix DaaS リソースを削除しないでください。Azure のサービスリソースを削除すると、サブスクリプションがキャンセルされます。

Google Cloud Marketplace からの購入

Google Cloud Marketplace から、次の Citrix 製品を購入できます:

- Citrix DaaS Standard for Google Cloud
- Citrix DaaS Premium for Google Cloud

Google Cloud Marketplace から購入するには、次のものが必要です:

- Citrix Cloud アカウントの OrgID。
  - Citrix Cloud アカウントを持っているが、OrgID がわからない場合は、Citrix Cloud コンソールの右上隅を確認してください。または、アカウントの作成時に受け取ったメールをご覧ください。
  - Citrix Cloud アカウントをお持ちでない場合は、「Citrix Cloud にサインアップする」のガイダンスに従ってください。
- Google Cloud アカウントとそのアカウントに最低 1 つの Google Cloud サブスクリプション。

購入するには:

1. Google Cloud Marketplaceにサインインします。
2. [Citrix DaaS for Google Cloud] ページの指示に従って購入します。

サービスがプロビジョニングされると、シトリックスからメールが届きます。プロビジョニングには時間がかかる場合があります。翌日までにメールが届かない場合は、Citrix サポートまでお問い合わせください。シトリックスからメールを受信すると、Citrix DaaS の使用を開始できます。

Google Cloud で Citrix DaaS リソースを削除しないでください。Azure のサービスリソースを削除すると、サブスクリプションがキャンセルされます。

次の操作

購入が完了したら、「展開の計画と構築」の次の手順に進みます。

例:

- ハイパーバイザーやクラウドサービス、Active Directory などをまだ設定していない場合は、「リソースの場所を設定する」を参照してください。
- ホスト環境と Active Directory を設定済みの場合は、「接続の作成」を参照してください。

Citrix HDX Plus for Windows 365

April 18, 2024

Citrix HDX Plus for Windows 365 を使用すると、Citrix Cloud を Windows 365 と統合して Citrix HDX テクノロジを使用することができ、管理を容易にする他の Citrix Cloud サービスとともに、強化された、より安全な Windows 365 クラウド PC のエクスペリエンスを実現できます。

詳しくは、「Citrix HDX Plus for Windows 365」を参照してください。

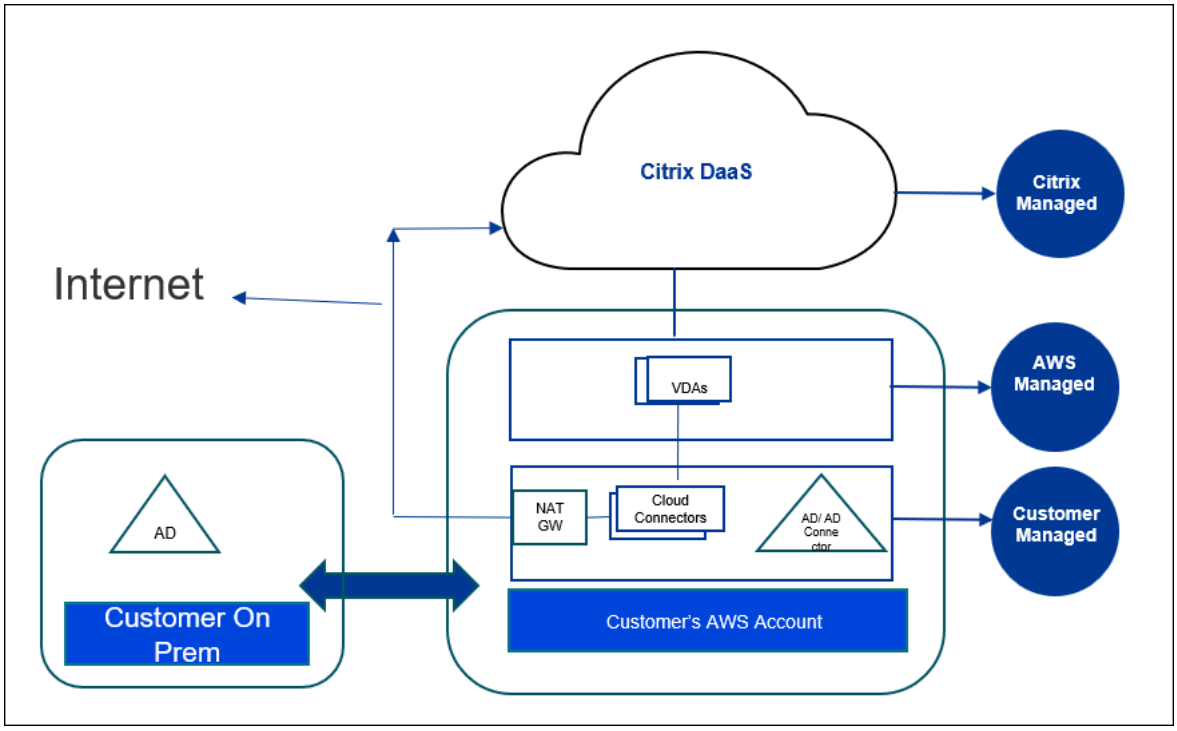
Citrix DaaS for Amazon WorkSpaces Core（Technical Preview）

May 17, 2024

はじめに

この記事では、Citrix for Amazon WorkSpaces Core を使用して展開を準備および作成する方法について説明します。Amazon WorkSpaces Core は Amazon Web Services（AWS）内に存在します。

以下は、Citrix DaaS を使用した AWS の導入とその管理に関する画像です:



この **Preview** について

- この Preview 期間中のサポートについては、AWS サポートまたは Citrix サポートにお問い合わせください。
- この Preview 期間中に Citrix 環境を管理するには、Citrix DaaS の ［管理］コンソールのみを使用してください。この Preview 期間中は、Citrix または AWS API はサポートされません。（Citrix は、将来使用予定の API に関するフィードバックを歓迎いたします。）

展開の準備と作成

クイック展開インターフェイスの展開チェックリストには、手順 1～5 へのリンクが含まれています。

1. はじめに、Citrix Cloud と AWS の前提条件を完了してください。
2. Citrix Cloud にリソースの場所を作成。（この手順も前提条件に含まれています。）
3. AWS アカウントへの接続。この手順により、Citrix DaaS が AWS に接続できるように権限が有効になります。
4. ディレクトリ接続の作成。この手順では、組織の Active Directory へのアクセスを許可する接続を構成します。
5. イメージのインポート。この手順により、ユーザー向けのデスクトップエクスペリエンスを作成できます。
6. 展開の作成。この手順では、展開するマシンと、Citrix Workspace を通じてそれらのマシンにアクセスできるユーザーを指定します。

はじめに

展開の準備と作成を開始する前に、次のタスクを完了していることを確認してください。

1 つ例外があります。Citrix Cloud でのリソースの場所の作成が前提条件として記載されています。これは、展開チェックリストの最初の手順でもあります。したがって、前提条件の一部としてリソースの場所を作成する場合は、チェックリストの実行でその手順をスキップしてください。逆に、まだ実行していない場合は、チェックリストのこの手順を完了するようにしてください。

Citrix Cloud で完了するための前提条件

- Citrix Cloud アカウントを作成し、Citrix DaaS にサブスクライブします。Citrix 担当者がこの作業をお手伝いします。また、担当者は、このプレビュー機能を有効にします。
- Citrix Cloud にリソースの場所を作成。（この手順は、クイック展開インターフェイスにもリンクされています。）

AWS で完了するための前提条件

- AWS ユーザーアカウントを作成します。アカウントには以下が必要です：
  - Citrix API クライアントの役割権限。
  - プログラムによるアクセスの権限。詳しくは、「AWS アカウントのプログラムによるアクセスの権限」を参照してください。
  - workspaces_DefaultRole の役割を作成します。詳しくは、「Create the workspaces_DefaultRole Role」を参照してください。
- Active Directory 内：
  - AD Connector オプションを使用して、情報を保存および管理します。詳しくは、「AD Connector」を参照してください。
  - 仮想マシンが作成される OU を作成します。その OU には、Cloud Connector および Citrix Cloud との通信用の Citrix ポリシーが必要です。詳しくは、リファレンスセクションを参照してください。
  - Citrix Cloud Connector 構成のグループポリシーを設定します：
    1. Citrix ダウンロードサイトから、Citrix が提供する最新のグループポリシー管理コンソールをダウンロードします（CitrixGroupPolicyManagement_64.msi）。
    2. MSI をインストールします（このマシンには、Visual Studio 2015 ランタイムをインストールしている必要があります）。次に、Controller ポリシー設定を含むCitrix ポリシーを作成します。この設定では、Cloud Connector アドレスを指定します。
- NAT ゲートウェイを作成するか、既存の NAT ゲートウェイを使用します。詳しくは、「NAT ゲートウェイ」を参照してください。

- Citrix Cloud Connector が展開された仮想マシンと通信できるようにする 1 つ以上のセキュリティグループを作成するか、既存のセキュリティグループを使用します。詳しくは、「Control traffic to your AWS resources using security groups」を参照してください
- AWS サポートチケットを開いて、アカウントで BYOL を有効にします。開始するには、AWS アカウントマネージャーまたは営業担当者に問い合わせるか、AWS サポートセンターにお問い合わせください。担当者が BYOL を確認して有効にします。詳しくは、「Enable BYOL for your account for BYOL using the Amazon WorkSpaces console」を参照してください。

  > 注:
  >
  > 現在、Windows 10 N および Windows 11 N バージョンは BYOL ではサポートされていません。

  - Citrix DaaS for Amazon WorkSpaces Core 機能を使用すると、AWS WorkSpaces Core の Bring Your Own Protocol（BYOP）機能が自動的に有効になります。
  - 作成するデスクトップの十分な Windows 10 ライセンスが必要です。詳しくは、「Bring Your Own Windows desktop licenses」を参照してください。

一般的な準備

開始する前に、各手順を確認してください。これを実行することにより、プロセスを簡単に完了できます。

リソースの場所の作成

Citrix Cloud にリソースの場所を作成します。

- リソースの場所には、Citrix Cloud と通信する Cloud Connector が 2 つ以上含まれます。Cloud Connector をインストールするサーバーは、EC2 VPC 内に存在し、ドメインに参加しており、インターネットに接続されている必要があります。Cloud Connector は、使用する予定のディレクトリと同じ VPC 内に存在する必要があります。
- Cloud Connector について詳しくは、「Citrix Cloud Connector」とプロビジョニング方法について参照してください。
- リソースの場所には、Active Directory サーバーを含めることもできます。詳しくは、「Active Directory を Citrix Cloud に接続する」を参照してください。

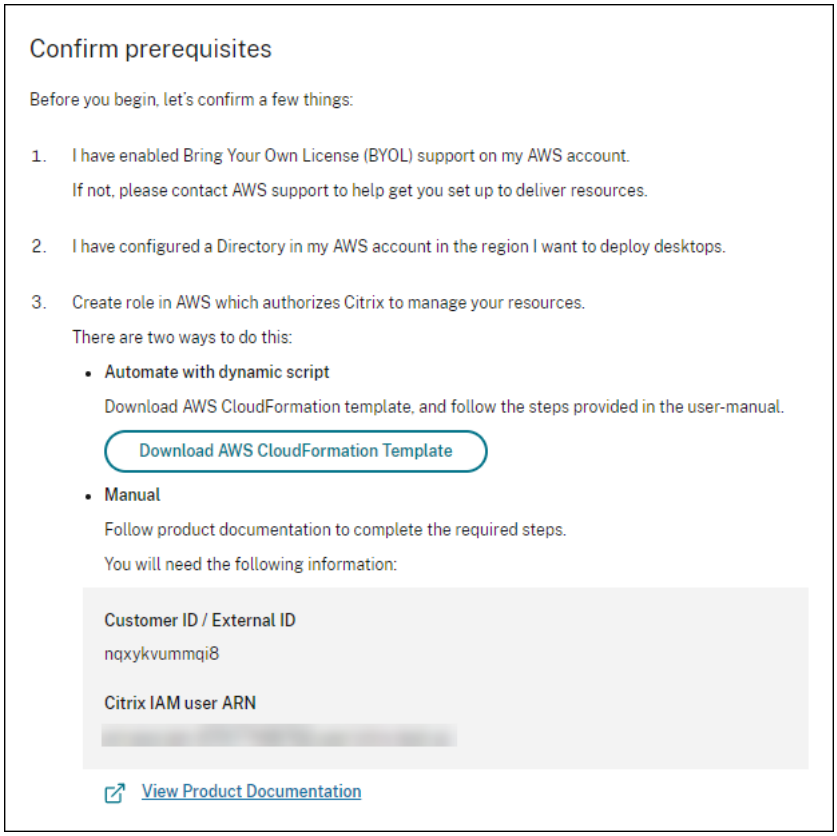
AWS アカウントへの接続

この手順により、Citrix DaaS が AWS に接続できる権限が有効になります。

AWS WorkSpaces Core の AssumeRole を作成するには、次の手順を実行します:

1. Citrix DaaS の ［管理］ **>** ［クイック展開］ **>** ［アカウント］ で ［アカウントの接続］ をクリックします。

2. [**AWS** アカウントの接続] ページの [前提条件の確認] で、[**AWS CloudFormation** テンプレートのダウンロード] をクリックします。テンプレートがダウンロードされたら、[次へ] をクリックします。



1. テンプレートをアップロードするには、「AWS Workspace Core 統合用の AssumeRole を作成する」を参照してください。
2. [アカウントの認証] ページで、[役割 **ID**] フィールドで生成された **Amazon** リソースネーム（ARN）を追加し、[名前] フィールドで [次へ] をクリックします。[リージョンの選択] ページが開きます。

   役割 **ID** は、Citrix にリソースの管理を許可する役割の ARN に対応します。役割 ID は、AWS 管理コンソールで [**IAM**] > [**Roles**] に移動すると確認できます。

   `CloudFormation`スクリプトを使用している場合は、CloudFormation に移動し、役割の作成に使用された対応するスタックをクリックします。[リソース] タブに移動し、LogicalID `CitrixAssumeRole`のリソースをクリックします。

   > 注:
   >
   > 同じ AWS アカウントの同じリージョンにある 2 つのアカウントを接続することはできません。

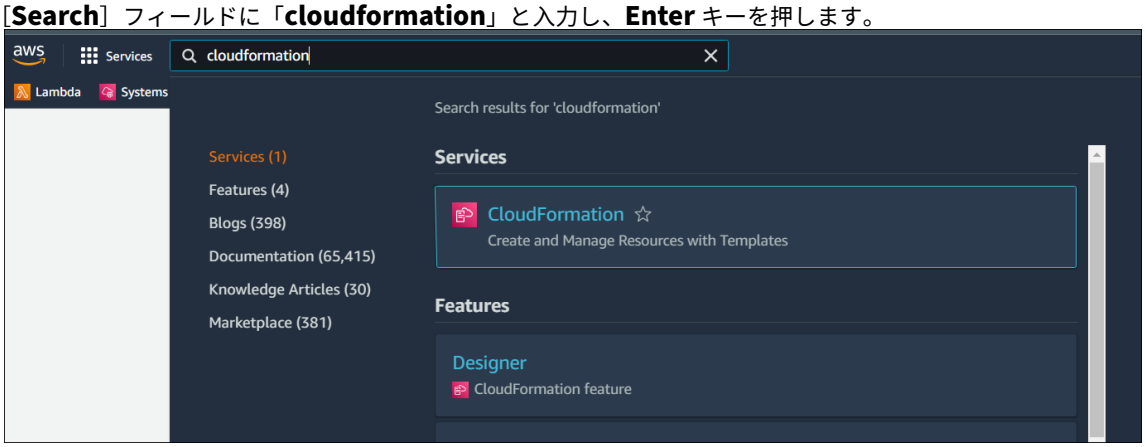
3. [リージョンの選択] ページで、デスクトップを展開するリージョンを選択し、[次へ] をクリックします。
4. [**BYOL** サポートの構成] ページで BYOL サポートを構成するには、安全な Amazon ネットワークに接続されている管理ネットワークインターフェイスが必要です。このインターフェイスとして使用するために検索する IP アドレス範囲を選択します。次に、[使用可能な CIDR ブロックを表示する] を選択します。選択した検索

範囲に使用可能な CIDR ブロックがある場合は、使用可能な CIDR ブロックを選択します。検索のアドレス範囲と使用可能な CIDR ブロックが正常に選択されると、確認のメッセージが表示されます。[次へ] をクリックします。

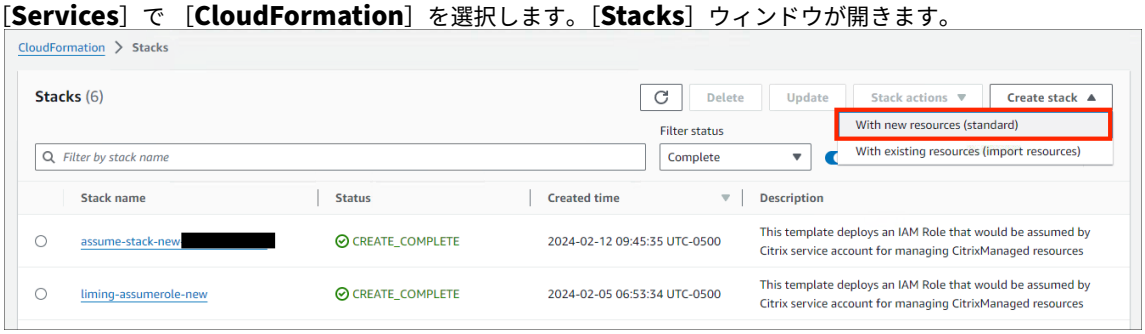
5. [概要] ページで、指定した情報を確認します。前のページに戻ることができます。完了したら、[完了] をクリックします。
   接続プロセスが完了するまでに数時間かかる場合があります。

AWS Workspace Core 統合用の **AssumeRole** を作成する

1. ブラウザーウィンドウで **Amazon Web Services** Web サイトを開いてサインインします。
2. [**Search**] フィールドに「**cloudformation**」と入力し、**Enter** キーを押します。



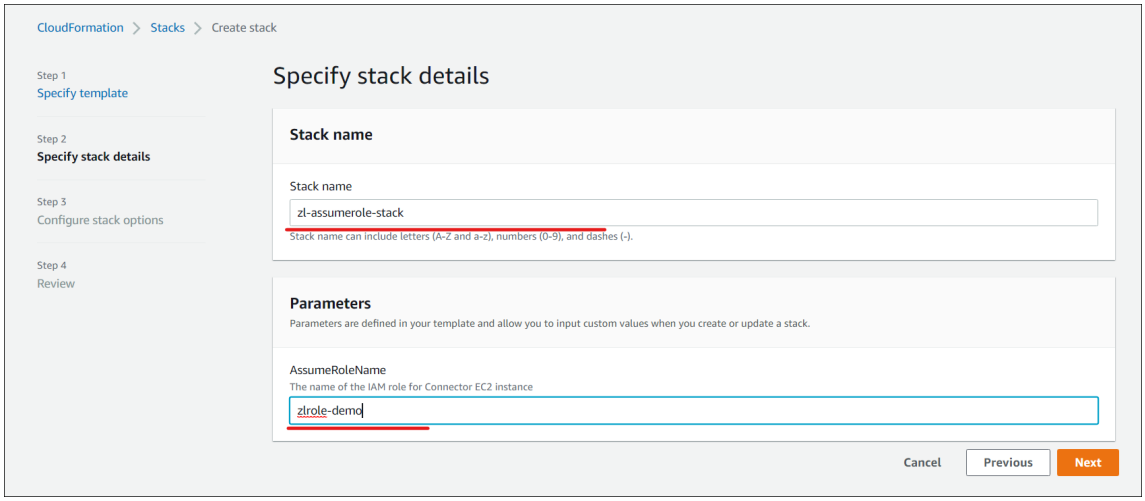
3. [**Services**] で [**CloudFormation**] を選択します。[**Stacks**] ウィンドウが開きます。



4. 右上隅の [**Create stack**] > [**With new resources (standard)**] をクリックします。[**Create stack**] ウィンドウが開きます。

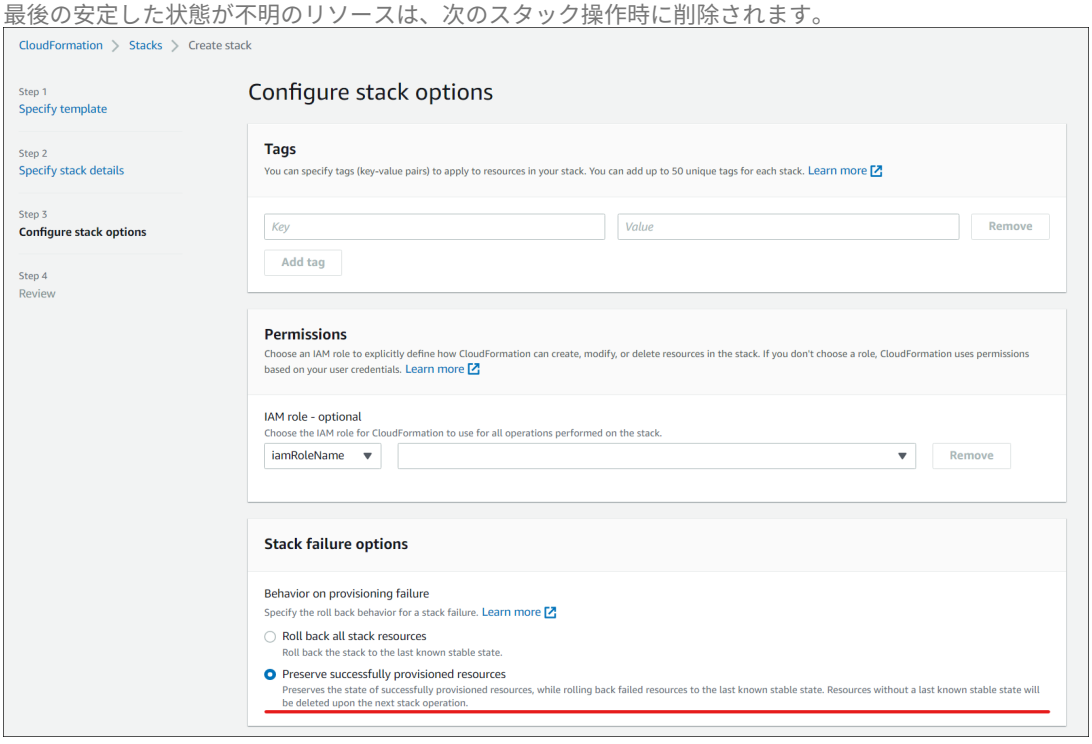
   a) [**Prerequisite –Prepare template**] で [**Template is ready**] を選択します。
   b) [**Specify template**] で [**Upload a template file**] > [**Choose file**] の順にクリックし、[**Next**] をクリックします。[**Specify stack details**] ペインが開きます。

5. [**Specify stack details**] ペインで [**Stack name**] と [**AssumeRoleName**] を指定し、[**Next**] をクリックします。[**Configure stack options**] ペインが開きます。

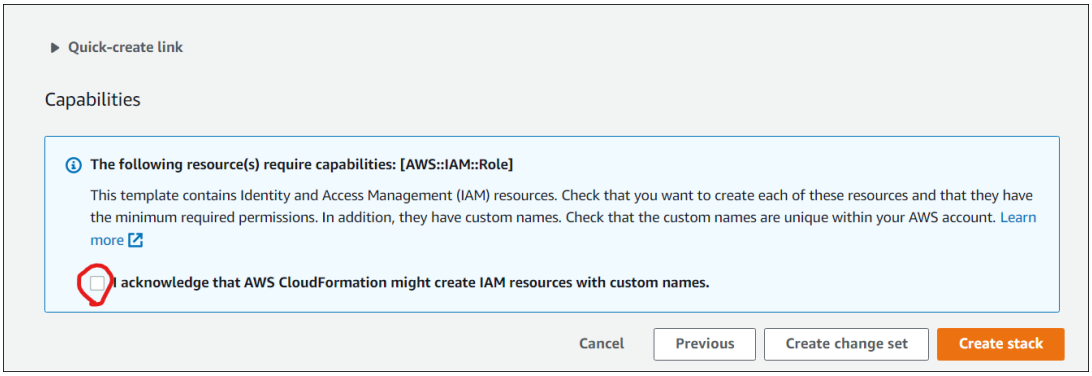


注:

- [**Configure stack options**] ペインで [**Preserve successfully provisioned resources**] オプションを選択します。このオプションは、正常にプロビジョニングされたリソースの状態を保存します。最後の安定した状態が不明のリソースは、次のスタック操作時に削除されます。

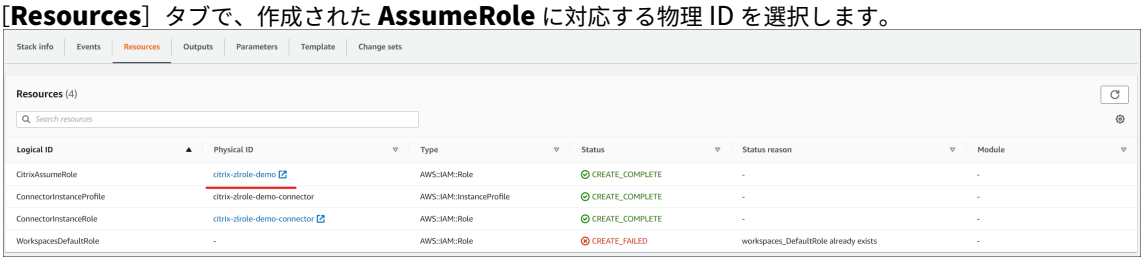


- [**Capabilities**] ポップアップウィンドウで [**I acknowledge that AWS CloudFormation might create IAM resources with custom names**] チェックボックスを選択し、[**Create stack**] を選択します。

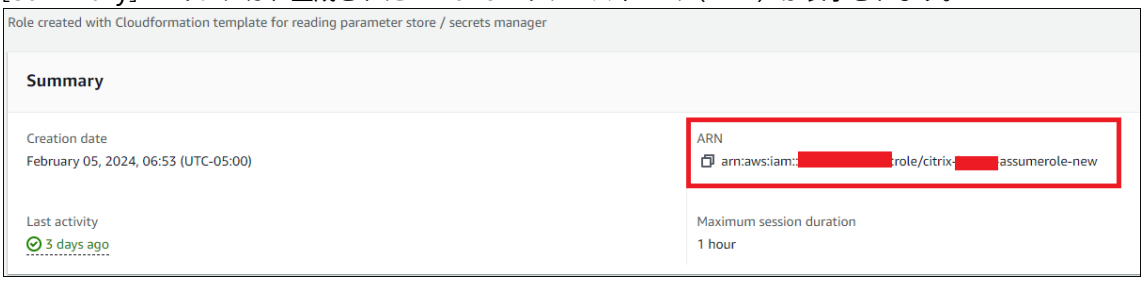


スタックの作成は **workspace_DefaultRole** が既に作成されているため、最終的に失敗する可能性があります。これは **AssumeRole** の作成には影響しません。

1. [**Events**] タブには、作成されたスタックのステータスが表示されます。
2. [**Resources**] タブで、作成された **AssumeRole** に対応する物理 ID を選択します。



3. [Summary] ペインには、生成された **Amazon** リソースネーム（ARN）が表示されます。



4. AWS アカウントの接続の手順 4 から手順を再開します

ディレクトリ接続の作成

> 注:
>
> この手順の始めに、AWS ディレクトリの登録を解除します。Citrix DaaS でディレクトリ接続を作成すると、選択したディレクトリが登録され、Citrix DaaS で Amazon WorkSpaces が作成されます。

この手順では、組織の Active Directory へのアクセスを許可する接続を構成します。

前提条件:

- 2 つの Cloud Connector が含まれるリソースの場所。
- セキュリティグループ。
- Active Directory 内の OU。

前提条件について詳しくは、「はじめに」を参照してください。

この手順は、次の 2 つの場所のいずれかから開始できます:

- 「はじめに」チェックリストのリンク。
- DaaS の ［管理］コンソールから、左側のペインで ［クイック展開］を選択し、［**Amazon WorkSpaces Core**］セクションの ［ディレクトリ接続］を 選択します。次に、「ディレクトリ接続の作成」を選択します。

ディレクトリ接続の作成の手順を実行します:

1. 前提条件の確認: 前提条件を完了している場合は、［次へ］をクリックします。
2. ディレクトリの接続: リソースの場所、アカウント、およびディレクトリを選択します。(選択したアカウントには少なくとも 1 つのディレクトリが必要です。)
    - デスクトップマシンを展開する 2 つのサブネットを選択します。サブネットは、適切なアベイラビリティゾーン内に存在する必要があります。
    - この接続のフレンドリ名を指定します。
    - 完了したら、［次へ］をクリックします。
3. 仮想マシンの設定: 選択した設定は、このディレクトリ接続を使用するすべての仮想マシンに適用されます。
    - 選択した OU は、Citrix グループポリシーの対象となる OU と一致する必要があります。
    - セキュリティグループを選択します。
    - 仮想マシンに割り当てられた各ユーザーに管理者権限を与えるかどうかを指定します。

イメージのインポート

この手順により、ユーザー向けのデスクトップエクスペリエンスを作成できます。

イメージをインポートするための前提条件:

- EC2 イメージである必要があります。
- Citrix Virtual Delivery Agent（VDA）がインストールされている必要があります。
- BYOL の準備が必要です。BYOL スクリプトはBYOLChecker.zipで入手できます。

イメージをインポートするには、次の手順を実行します:

1. 前提条件の確認: 前提条件の手順の後は、［次へ］をクリックします。(BYOL 用のイメージを準備していない場合は、このページからスクリプトをダウンロードできます。) 詳しくは、「要件」を参照してください。
2. イメージの選択後、そのイメージにフレンドリ名を付けます。アカウント、AMI を選択し、説明を追加します。［次へ］をクリックします。［概要］ページが開きます。
3. ［概要］ページで、指定した情報を確認します。確認したら、［イメージのインポート］を選択します。

> 注:
>
> イメージのインポートには数時間かかる場合があります。

イメージをインポートするときに **Microsoft Office 2019** イメージを統合する

イメージをインポートするときに Microsoft Office 2019 イメージを統合するには:

1. [**Web Studio**] **>** [クイック展開] で [イメージ] をクリックします。
2. [マイイメージ] で [イメージのインポート] をクリックします。
3. [イメージのインポート] **>** [前提条件] で [次へ: イメージの選択] をクリックします。
4. [イメージのインポート] **>** [イメージの選択] で:
   - [アカウント] ドロップダウンからアカウントを選択します。
   - [**AMI**] ドロップダウンから AMI を選択します。
   - [名前] フィールドにイメージの名前を入力します。
   - イメージで [イメージに **Microsoft Office 2019 Professional Plus** を含めます] を選択します。
   - [説明] フィールドに説明を入力します。
5. [イメージのインポート] **>** [イメージの選択] で [次へ: 概要] をクリックします。
6. [イメージの選択] **>** [概要] で **Microsoft Office 2019** に [選択済み] が表示されるようにします。
7. [マイイメージ] で [イメージのインポート] をクリックします。
   インポート操作が完了するまで、最近展開されたイメージのステータスにはインポート中と表示されます。
8. [マイイメージ] で、最近展開したイメージを選択し、[詳細の表示] をクリックします。
9. [詳細] パネルの [**Microsoft Office 2019**] フィールドに 含めると表示されます。

> 注:
>
> 次のバージョンの OS のみが互換性があります:
>
> - Windows 10 バージョン 21H2（2021 年 12 月更新）
> - Windows 10 バージョン 22H2（2022 年 11 月更新）
> - Windows 10 Enterprise LTSC 2019（1809）（1809）
> - Windows 10 Enterprise LTSC 2021（21H2）（21H2）
> - Windows 11 バージョン 22H2（2022 年 10 月リリース）

展開の作成

展開とは、ユーザーが Citrix Workspace からアクセスできるデスクトップのグループです。この手順では、デスクトップとして展開する仮想マシンの特性と、どの AD ユーザーがそれらを使用できるかを指定します。

前提条件

「展開の準備と作成」に記載されているすべての手順を完了します。

1. [**Web Studio**] **>** [クイック展開] の [**Amazon Web Services**] で、[展開] をクリックします。[展開の作成] をクリックします。
2. 名前と接続：このマシンのグループのフレンドリ名を入力します。名前は一意である必要があります。ディレクトリ接続を選択し、[次へ：イメージとパフォーマンス] をクリックします。
3. イメージとパフォーマンス：オペレーティングシステムとマシンのパフォーマンスを選択します。ルートボリュームとユーザーボリュームのデフォルトのサイズを指定します。
   このグループでデスクトップを起動した後は、ボリュームのサイズは変更できません。したがって、必要と思われる最大サイズを指定してください。次のページで、ユーザーごとにこれらのサイズを指定することもできます。[次へ：ユーザー] をクリックします。
4. ユーザー：デスクトップへのアクセスを許可するユーザーを検索して選択します。
   ユーザーのボリュームサイズをカスタマイズする場合は、[ユーザーとルートのボリュームサイズを編集する] を選択し、サイズを指定します。[次へ：概要] をクリックします。
5. 概要：提供した情報を確認し、[展開を作成] をクリックします。

Microsoft 365 Windows アプリの統合

Microsoft 365 アプリを統合するには、「Microsoft 365 Apps for enterprise が Amazon WorkSpaces サービスで利用可能に」および「Microsoft 365 Bring Your Own License (BYOL)」を参照してください。

展開内のマシンの管理

「マシンカタログの管理」で説明されているマシン管理機能に加えて、一部のアクションでは、展開から管理するマシンを選択できます。

展開内のマシンを管理するには：

1. [**Web Studio**] **>** [クイック展開] で [展開] を選択します。
2. [展開] ペインで、管理するマシンを含む展開を選択します。
3. [詳細の表示] をクリックします。
4. [展開の詳細] ペインで、管理するマシンを選択します。
5. 表示されたアクションから、マシン上で実行するアクションを選択します：

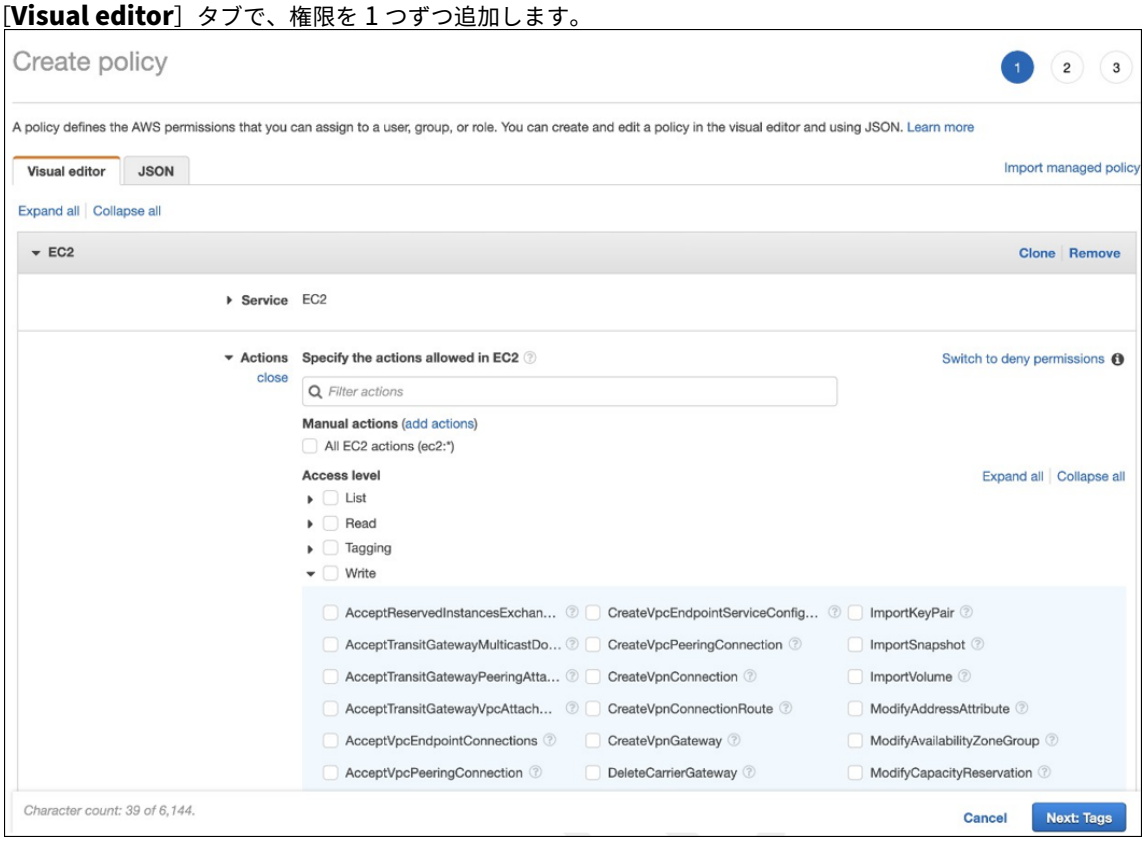
- [ボリュームサイズの編集] をクリックして、マシンのボリュームサイズを変更します。
- [削除] をクリックして、展開および AWS からマシンを削除します。マシンがデリバリーグループに含まれている場合、メンテナンスモードの場合にのみ削除できます。
- [メンテナンスモードをオン/オフにします] をクリックして選択したマシンのメンテナンスモードをオン（オフの場合）またはオフ（オンの場合）にします。

リファレンス

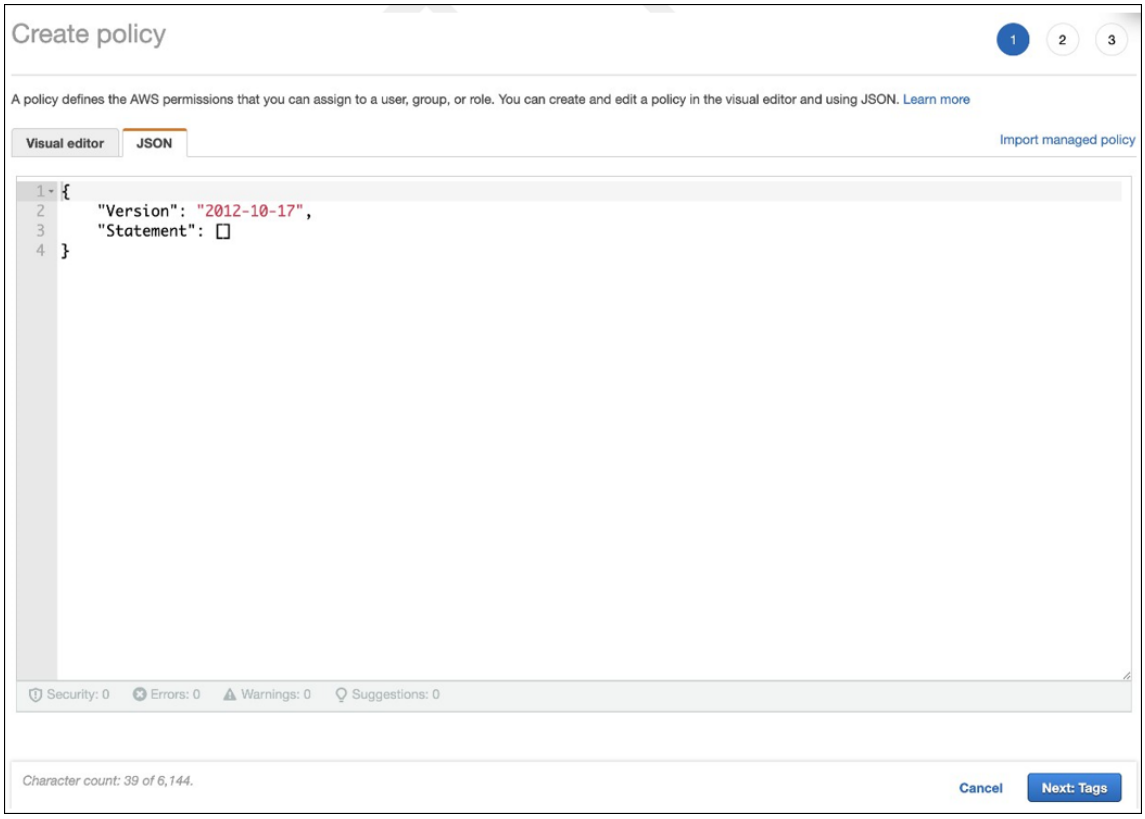
AWS アカウントのプログラムによるアクセスの権限

AWS ユーザーアカウントには、AWS リソースレイヤーへの API 呼び出しを行うために、特定のプログラムによるアクセスの権限が必要です。プログラムによるアクセスでは、アクセスキー ID とシークレットアクセスキーが作成されます。
IAM コンソールでこれらの権限を含むポリシーを作成できます。次の図に示すように、ビジュアルエディター（権限を 1 つずつ追加）または JSON（以下のスニペットを追加）を使用できます。
詳しくは、「Creating an IAM user in your AWS account」を参照してください。

- [**Visual editor**] タブで、権限を 1 つずつ追加します。



- [**JSON**] タブで、次の図の後に記載されているスニペットを追加します。



必要な権限

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                    "workdocs:DeregisterDirectory",
                    "workdocs:RegisterDirectory",
                    "workdocs:AddUserToGroup",
                    "ec2:ImportInstance",
                    "ec2:DescribeImages",
                    "ec2:DescribeImageAttribute"
                    "ec2:CreateKeyPair",
                    "ec2:DescribeKeyPairs",
                    "ec2:ModifyImageAttribute",
                    "ec2:DescribeVpcs",
                    "ec2:DescribeSubnets",
                    "ec2:RunInstances",
                    "ec2:DescribeSecurityGroups",
                    "ec2:CreateTags",
                    "ec2:DescribeRouteTables",
                    "ec2:DescribeInternetGateways",
```



```
                    "ec2:CreateSecurityGroup",
                    "ec2:DescribeInstanceTypes",
                    "servicequotas:ListServices",
                    "servicequotas:GetRequestedServiceQuotaChange",
                    "servicequotas:ListTagsForResource",
                    "servicequotas:GetServiceQuota",
                    "servicequotas:
                       GetAssociationForServiceQuotaTemplate",
                    "servicequotas:ListAWSDefaultServiceQuotas",
                    "servicequotas:ListServiceQuotas",
                    "servicequotas:GetAWSDefaultServiceQuota",
                    "servicequotas:
                       GetServiceQuotaIncreaseRequestFromTemplate",
                    "servicequotas:
                       ListServiceQuotaIncreaseRequestsInTemplate",
                    "servicequotas:
                       ListRequestedServiceQuotaChangeHistory",
                    "servicequotas:
                       ListRequestedServiceQuotaChangeHistoryByQuota",
                    "sts:DecodeAuthorizationMessage",
                    "ds:*",
                    "workspaces:*",
                    "iam:GetRole",
                    "iam:GetContextKeysForPrincipalPolicy",
                    "iam:SimulatePrincipalPolicy"

                ],
                "Resource": "*"
            }

        ]
 }

<!--NeedCopy-->
```

Citrix DaaS for Google Cloud

November 18, 2022

Citrix DaaS for Google Cloud により、Citrix DaaS の［完全な構成］管理インターフェイスを使用して Google Cloud デスクトップおよびアプリを展開できます。Citrix DaaS for Google Cloud には、Standard エディションと Premium エディションが用意されています。

サポートされている機能については、Citrix Virtual Apps and Desktops の機能マトリックスを参照してください。

Citrix DaaS for Google Cloud は、Google Cloud Marketplaceから購入できます。

Citrix DaaS を購入したら、Citrix Cloud にサインインします。左上のメニューで、［マイサービス］**>**［**DaaS**］を選択します。

この製品ドキュメント内の設定手順に従います。［完全な構成］インターフェイスを使用すると、製品の他の種類でそのインターフェイスを使用する場合と同じように、接続、カタログ、およびデリバリーグループを作成できます。（各種とも、現在は［クイック展開］管理インターフェイスがありません。）

［完全な構成］インターフェイスの一部の表示は、このドキュメント内の表示内容と異なる場合があります。たとえば、Google Cloud 向け Citrix Virtual Apps and Desktops で接続を作成する場合、使用可能な接続タイプには、サポートされているハイパーバイザーと Google Cloud が含まれます。他のクラウドサービスは使用できません。

同様に、サポートされているハイパーバイザーと Google Cloud に適用される、製品ドキュメント内の情報を使用してください。

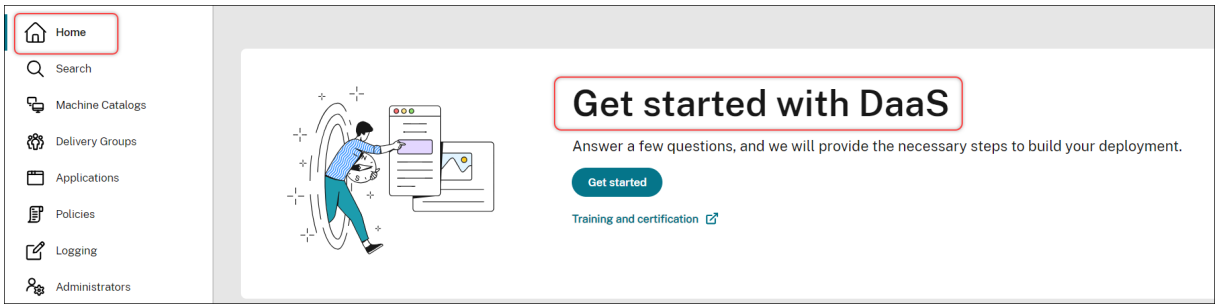
Google Cloud での Citrix DaaS の展開と構成の詳細な手順については、Citrix Tech Zone の記事「Google Cloud での Citrix 仮想化」を参照してください。この記事では、展開アーキテクチャの定義、Google Cloud プロジェクトの準備、ネットワークサービスの設定、Active Directory の展開について説明します。

DaaS 入門ガイド（Technical Preview）の使用

May 17, 2024

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

DaaS 入門ガイドは、新規管理者と経験豊富な管理者の両方を対象として DaaS 展開プロセスを合理化し、容易にするガイドです。このガイドを使用すると、一連の質問に答えることで、DaaS 環境を迅速にセットアップできます。



この記事では、DaaS 展開のセットアッププロセスに関する 5 つの典型的なシナリオについて説明します。

メリット

このガイドを使用すると、次のようなメリットがあります:

- 簡単に利用を開始できる。このガイドでは、質問形式の、ステップごとに分けられたワークフローによって、基本的な展開手順を案内します。新しい管理者の場合は、コンテキストに対応したヘルプを通じて概念や用語を学びながら、環境を迅速にセットアップできます。
- 複雑な構成がシンプルになる。このガイドでは、必要に応じて事前構成された設定が提供され、高度な構成のための［完全な構成］の UI を利用できます。経験豊富な管理者は、このガイドを複雑な構成の開始点として使用できます。

サポートされている展開シナリオ

このガイドでは、次のシナリオに関して迅速に展開する方法を案内します:

何を配信しますか?	マシンは既に存在しますか?	マシンの種類	注釈
Virtual apps and desktops	いいえ	仮想マシン（DaaS によってプロビジョニング）	電源管理されている
Virtual apps and desktops	はい	仮想マシンまたはブレード PC	電源管理されている
Virtual apps and desktops	はい	物理マシンまたは仮想マシン	電源管理されていない
オフィス PC	はい	物理マシン	電源管理されている
オフィス PC	はい	物理マシン	電源管理されていない

詳細な手順については、次のセクションを参照してください:

- アプリとデスクトップを新規に配信する（電源管理されている）
- 既存のマシンを使用してアプリとデスクトップを配信する（電源管理されている）
- 既存のマシンを使用してアプリとデスクトップを配信する（電源管理されていない）
- オフィス PC を配信する（電源管理されている）
- オフィス PC を配信する（電源管理されていない）

用語

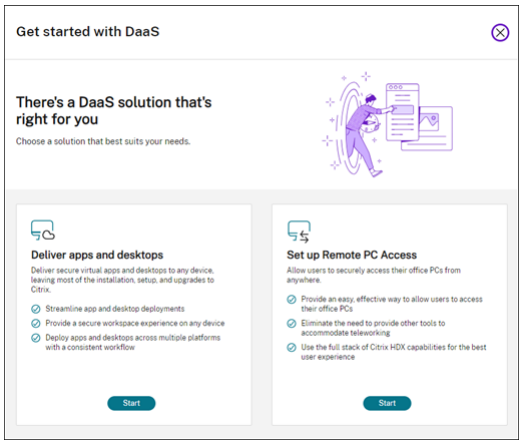
以下は DaaS 固有の用語です:

- リソースの場所。リソースの種類には、ユーザーへのアプリおよびデスクトップの配信に必要なリソースが含まれます。

- ホスト接続。DaaS をリソースの場所にあるホスト（ハイパーバイザーまたはクラウドサービス）に接続します。ホスト上でマシンを作成および管理する場合、または既存のマシンの電源を管理する場合は、ホスト接続の作成が必要です。
- マスターイメージ。ホスト上で仮想マシンを複製するためのテンプレートとして機能します。これには、オペレーティングシステム、アプリケーション、Virtual Delivery Agent（VDA）、およびその他のソフトウェアが含まれます。
- マシンカタログ。同一マシンのコレクション。ニーズに応じて、仮想マシンまたは物理マシンにすることができます。マシンカタログを作成して、ホスト上に同一構成のマシンを作成したり、管理のためにマシンを DaaS にインポートしたりできます。
- デリバリーグループ。マシンカタログのマシンが含まれます。また、それらのマシンを使用できるユーザーと、そのユーザーに提供するアプリケーションおよびデスクトップを指定します。
- マシンプロファイル。仮想マシンのプロパティを指定します。カタログ内の仮想マシンは、マシンプロファイルからプロパティを継承できます。

ガイドへのアクセス

1. ［**DaaS**］**>** ［ホーム］ページに移動します。
2. ［**DaaS** の使用を開始する］を見つけます。
3. ［開始］をクリックして、展開プロセスを開始します。



> 注：
>
> ［閉じる］をクリックすると、いつでもプロセスを終了でき、ガイドが設定を自動的に保存します。構成を続行するには、［続行］をクリックします。新たに始めるには、［やり直す］をクリックします。

アプリとデスクトップを新規に配信する（電源管理されている）

このセクションでは、仮想マシンを作成し、それを使用してアプリとデスクトップを配信する展開プロセスについて説明します。

前提条件

開始するには、以下が必要です：

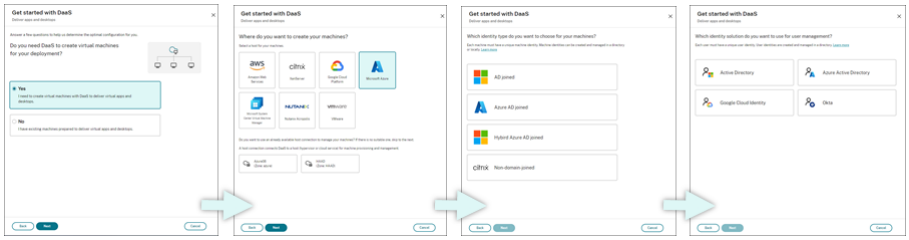
- Citrix Cloud からターゲット ID プロバイダーへの接続

  詳しくは、「ID プロバイダー」の対応するセクションを参照してください。
- 役割：すべての管理権限を実行できる管理者、または Cloud 管理者
- ターゲットのハイパーバイザーまたはクラウドサービスで必要な権限。

  詳しくは、「接続の作成と管理」を参照してください。
- 仮想マシンアカウントを作成するための管理者の資格情報

準備

画面上の質問に答えて、次のインフラストラクチャレベルの設定を完了します。詳しくは、次の表を参照してください。

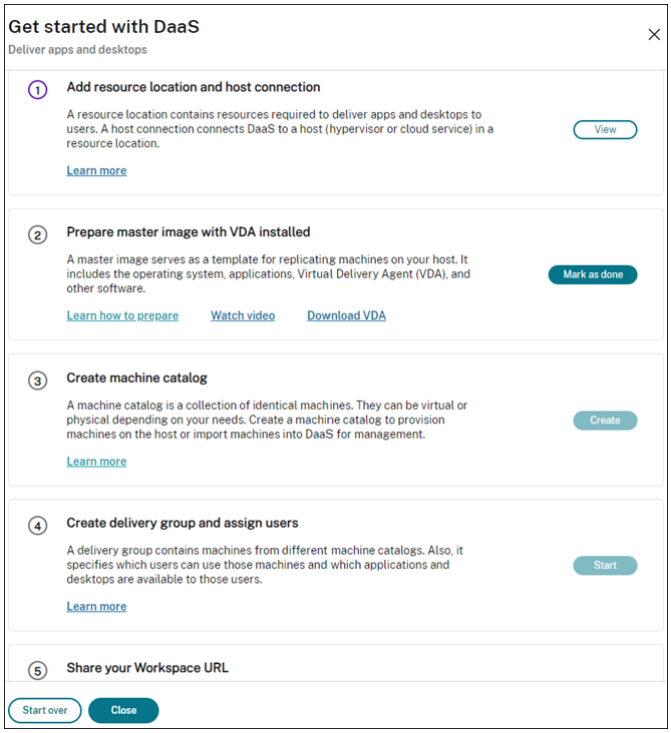


#	設定	説明
1	仮想マシンの作成が必要かどうかを指定する	［はい］を選択します。
2	ホストの種類を選択する	展開のホストの種類を選択します。

#	設定	説明
		オプション：AWS、XenServer（旧称 Citrix Hypervisor）、Google Cloud Platform、Microsoft Azure、Microsoft System Center Virtual Machine Manager、Nutanix Acropolis、および VMware
3	マシン ID の種類を選択する	マシン管理の ID の種類を選択します。 オプション：AD 参加、Azure AD 参加、Hybrid Azure AD 参加、およびドメイン非参加
4	ユーザー ID の種類を選択する	ユーザー管理の ID の種類を選択します。 オプション：Active Directory、Azure Active Directory、Google Cloud Identity、および Okta

展開手順

インフラストラクチャ レベルの設定を完了すると、この展開シナリオに固有の手順が次のように表示されます。



画面の指示に従って設定を完了してください。

手順 **1**：リソースの場所とホスト接続の追加　Cloud Connector をインストールしてリソースの場所を設定し、その場所でハイパーバイザーまたはクラウド サービスへの接続を構成します。

1. リソースの場所の名前を入力します。
2. Cloud Connector をダウンロードして、少なくとも 2 台の Windows Server マシンにインストールします。
3. インストールされている Cloud Connector を検出します。
4. リソースの場所のホスト接続を追加して構成します。接続の詳細設定には以下が含まれます：
    - 接続アドレス、ユーザー名、パスワードなどの接続の詳細。
    - ストレージリソース
    - ネットワークリソース。

    > 注：
    >
    > DaaS は、これらの接続を通じてホスト上で仮想マシンを作成および管理します。マシンカタログを作成するときに接続を指定する必要があります。

手順 **2**：マシンのマスターイメージの準備　リソースの場所にある仮想マシン上でマスターイメージを準備します。詳しくは、「ハイパーバイザーまたはクラウドサービスでのマスターイメージの準備」を参照してください。

手順 **3**：マシンカタログの作成　マシンカタログを作成して、ホスト上に同一構成のマシンのグループを作成します。詳細な手順は次のとおりです：

1. カタログに名前を付けます。
2. マシンの種類を選択します。

   オプション：マルチセッション、シングルセッションの静的（個人用デスクトップ）、およびシングルセッションのランダム（プールデスクトップ）。
3. ホスト接続を選択します。

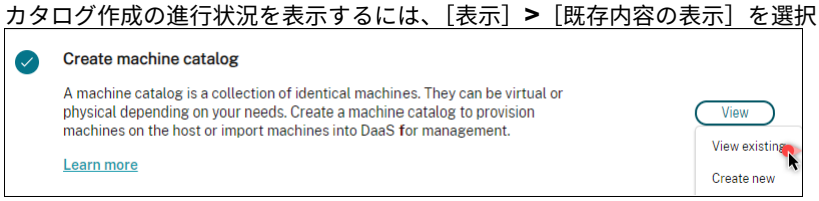
   オプションは、手順 1 でリソースの場所に対して構成したすべてのホスト接続が含まれます。
4. マスターイメージを選択します。
5. マシンプロファイルを選択します。

   > 注：
   >
   > マシンプロファイルのサポートは現在、Azure、GCP、AWS クラウドサービスで利用できます。GCP ではマシンプロファイルの使用はオプションです。
6. 作成するマシンの数を設定します。
7. マシン ID を設定します。

   デフォルトでは、準備段階で選択したマシン ID の種類が表示されます。ドメイン、OU、名前付けスキームなど、仮想マシンに必要な ID 設定を指定します。
8. マシンの作成に必要な管理者の資格情報を入力します。
9. ［**Create**］をクリックします。

   > ヒント：
   >
   > ［作成］ボタンは、必要な設定をすべて指定した後にのみ使用できます。

   カタログ作成の進行状況を表示するには、［表示］**>**［既存内容の表示］を選択します。



手順 **4**：デリバリーグループの作成とユーザーの割り当て

> ヒント：
>
> デリバリーグループを作成する前に、既存のカタログを表示して、少なくとも 1 つのカタログが正常に作成されていることを確認してください。そうしないと、デリバリーグループを作成できなくなります。

デリバリーグループの作成には、次のサブタスクが含まれます：

- 仮想マシンをグループに追加する
- ユーザーをグループに割り当てる
- 割り当てられたユーザーが使用できるアプリとデスクトップを指定する

1. グループに名前を付けます。
2. マシンカタログを選択し、グループで使用できる仮想マシンの数を指定することにより、グループにマシンを追加します。
3. このグループで使用可能なアプリケーションとデスクトップを指定します:
    - 選択したカタログ内の実行中のマシンからアプリケーションを追加するには、［新規追加］**>**［スタートメニューから］をクリックします。
    - ネットワーク共有で展開されたアプリケーションを追加するには、［新規追加］**>**［手動］をクリックし、パス、作業ディレクトリなどの必要な設定を指定します。
    - （マルチセッション OS マシンでのみ表示されます）デスクトップ配信の場合は、［デスクトップの配信を有効にする］を選択したままにします。
4. このグループのアプリとデスクトップにアクセスできるユーザーを追加します。

手順 **5**：**Workspace URL** をユーザーと共有　ワークスペースの ［構成］**>**［アクセス］から Workspace URL をユーザーと共有します。

既存のマシンを使用してアプリとデスクトップを配信する（電源管理されている）

このセクションでは、既存のマシンを使用してアプリとデスクトップを配信する（電源管理されている）展開のプロセスについて説明します。

前提条件

開始するには、以下が必要です:

- Citrix Cloud からターゲット ID プロバイダーへの接続

  詳しくは、「ID プロバイダー」の対応するセクションを参照してください。

- 役割：すべての管理権限を実行できる管理者、または Cloud 管理者

準備

画面上の質問に答えて、次のインフラストラクチャレベルの設定を完了します。

#	設定	説明
1	仮想マシンの作成が必要かどうかを指定する	［いいえ］を選択します。
2	電源管理が必要かどうかを選択する	電源管理されているマシン（仮想マシン、ブレード **PC** など）を選択します。
3	ホストプラットフォームを選択する	既存のマシンが存在するホストプラットフォームを選択します。 オプション：AWS、Citrix、Google Cloud Platform、Microsoft Azure、Microsoft System Center Virtual Machine Manager、Nutanix Acropolis、および VMware
4	ユーザー ID の種類を選択する	ユーザー管理の ID の種類を選択します。 オプション：Active Directory、Azure Active Directory、Google Cloud Identity、および Okta

展開手順

インフラストラクチャレベルの設定を完了すると、この展開シナリオに固有の手順が表示されます。画面の指示に従って設定を完了してください。

手順 **1**：リソースの場所とホスト接続の追加　Cloud Connector をインストールしてリソースの場所を設定し、その場所でハイパーバイザーまたはクラウドサービスへの接続を構成します。

1. リソースの場所の名前を入力します。
2. Cloud Connector をダウンロードして、少なくとも 2 台の Windows Server マシンにインストールします。
3. インストールされている Cloud Connector を検出します。
4. リソースの場所のホスト接続を追加して構成します。接続設定の例には、接続アドレス、ユーザー名、パスワードが含まれます。

> 注:
>
> DaaS は、接続を通じてリソースの場所にあるマシンの電源を管理します。マシンをカタログにインポートするときに接続を指定する必要があります。

手順 **2**：マシンカタログの作成　マシンカタログを作成し、そこにマシンをインポートします。

1. カタログに名前を付けます
2. マシンの種類を選択します。

   オプション：マルチセッション、シングルセッションの静的（個人用デスクトップ）、およびシングルセッションのランダム（プールデスクトップ）。
3. リソースの場所を選択します。
4. マシンをカタログにインポートします。
   マシンはホスト接続ごとに編成されます。関連するマシンをインポートするためのホスト接続を選択します。
5. ［**Create**］をクリックします。

手順 **3**：デリバリーグループの作成とユーザーの割り当て　デリバリーグループを作成するには、以下が必要です：

- 仮想マシンをグループに追加する
- ユーザーをグループに割り当てる
- 割り当てられたユーザーが使用できるアプリとデスクトップを指定する

1. グループに名前を付けます。
2. 必要に応じてマシンカタログを選択し、デリバリーグループで使用できるマシンの数を指定します。
3. このグループで使用可能なアプリケーションとデスクトップを指定します：
   - 選択したカタログ内の実行中のマシンからアプリケーションを追加するには、［新規追加］**>**［スタートメニューから］をクリックします。
   - ネットワーク共有で展開されたアプリケーションを追加するには、［新規追加］**>**［手動］をクリックし、パス、作業ディレクトリなどの必要な設定を指定します。
   -（マルチセッション OS マシンでのみ表示されます）デスクトップ配信の場合は、［デスクトップの配信を有効にする］を選択したままにします。
4. ユーザーをグループに追加します。

手順 **4**：**Workspace URL** をユーザーと共有　ワークスペースの ［構成］**>**［アクセス］から Workspace URL をユーザーと共有します。

既存のマシンを使用してアプリとデスクトップを配信する（電源管理されていない）

このセクションでは、既存のマシンを使用してアプリとデスクトップを配信する（電源管理されていない）展開のプロセスについて説明します。

前提条件

開始するには、以下が必要です:

- Citrix Cloud からターゲット ID プロバイダーへの接続

  詳しくは、「ID プロバイダー」の対応するセクションを参照してください

- 役割: すべての管理権限を実行できる管理者、または Cloud 管理者

準備

画面上の質問に答えて、次のインフラストラクチャレベルの設定を完了します。

#	設定	説明
1	仮想マシンの作成が必要かどうかを指定する	［いいえ］を選択します。
2	電源管理が必要かどうかを選択する	電源管理されていないマシン（物理マシンなど）を選択します。
3	ユーザー ID の種類を選択する	ユーザー管理の ID の種類を選択します。 オプション: Active Directory、Azure Active Directory、Google Cloud Identity、および Okta

展開手順

インフラストラクチャレベルの設定を完了すると、この展開シナリオに固有の手順が表示されます。画面の指示に従って設定を完了してください。

手順 **1**: リソースの場所の追加　Cloud Connector をインストールしてリソースの場所をセットアップします。

1. リソースの場所の名前を入力します。
2. Cloud Connector をダウンロードして、少なくとも 2 台の Windows Server マシンにインストールします。
3. インストールされている Cloud Connector を検出します。

> 注:
>
> ホスト接続の作成は、マシンの電源を管理する場合にのみ必要です。

手順 **2**：マシンカタログの作成　マシンカタログを作成し、そこにマシンをインポートします。

1. カタログに名前を付けます
2. マシンの種類を選択します。

   オプション：マルチセッション、シングルセッションの静的（個人用デスクトップ）、およびシングルセッションのランダム（プールデスクトップ）。
3. リソースの場所を選択します。
4. マシンをカタログにインポートします。

   マシン検索を容易にするには、部分的なコンピューター名とディレクトリ選択を使用します。
5. ［**Create**］をクリックします。

手順 **3**：デリバリーグループの作成とユーザーの割り当て　デリバリーグループを作成するには、以下が必要です：

- 仮想マシンをグループに追加する
- ユーザーをグループに割り当てる
- 割り当てられたユーザーが使用できるアプリとデスクトップを指定する

1. グループに名前を付けます。
2. 必要に応じてマシンカタログを選択し、デリバリーグループで使用できるマシンの数を指定します。
3. このグループで使用可能なアプリケーションとデスクトップを指定します：
   - 選択したカタログ内の実行中のマシンからアプリケーションを追加するには、［新規追加］**>**［スタートメニューから］をクリックします。
   - ネットワーク共有で展開されたアプリケーションを追加するには、［新規追加］**>**［手動］をクリックし、パス、作業ディレクトリなどの必要な設定を指定します。
   - （マルチセッション OS マシンでのみ表示されます）デスクトップ配信の場合は、［デスクトップの配信を有効にする］を選択したままにします。
4. ユーザーをグループに追加します。

手順 **4**：**Workspace URL** をユーザーと共有　ワークスペースの ［構成］**>**［アクセス］から Workspace URL をユーザーと共有します。

オフィス **PC** を配信する（電源管理されている）

このセクションでは、オフィス PC を配信する（電源管理されている）展開のプロセスについて説明します。

前提条件

開始する前に、以下が必要です:

- PC のマシン名。
- Citrix Virtual Delivery Agent（VDA）を各 PC にインストールする。（この手順はカタログの作成後に実行できます。）

  詳しくは、「VDA のダウンロード」を参照してください。

準備

画面上の質問に答えて、次のインフラストラクチャレベルの設定を完了します。

#	手順	説明
1	マシンの割り当ての種類を選択する。	マシンの割り当て方法を選択します。 オプション：静的自動割り当て、静的事前割り当て、ランダムプール未割り当て
2	ユーザーによるマシンの電源投入を許可するかを決定する	［リモートユーザーがマシンの電源を自分でオンにする］を選択します。
3	ユーザー ID の種類を選択する	ユーザー管理の ID の種類を選択します。 オプション：Active Directory、Azure Active Directory、Google Cloud Identity、および Okta

展開手順

インフラストラクチャレベルの設定を完了すると、この展開シナリオに固有の手順が表示されます。画面の指示に従って設定を完了してください。

手順 **1**：リソースの場所とホスト接続の追加　Cloud Connector をインストールしてリソースの場所を設定し、種類が ［リモート **PC Wake on LAN**］の接続を追加します。

1. リソースの場所の名前を入力します。
2. Cloud Connector をダウンロードして、少なくとも 2 台の Windows Server マシンにインストールします。
3. インストールされている Cloud Connector を検出します。
4. ［新規追加］をクリックして接続を追加します:

a) リソースの場所（ゾーン）を選択します。
b)［接続の種類］で ［リモート **PC Wake on LAN**］を選択します。
c) 接続の名前を入力します。

> 注:
>
> DaaS は、構成された接続を通じてマシンの電源を管理します。電源管理されたマシンのリモート PC アクセスカタログを作成する場合は、接続の種類 ［リモート **PC Wake on LAN**］を構成する必要があります。

手順 **2**: リモート **PC** アクセスカタログの作成　マシンカタログを作成し、そこにオフィス PC をインポートします。

1. カタログに名前を付けます
2. リソースの場所を選択します。
3. マシンの割り当ての種類を選択します。デフォルトでは、準備段階で選択した種類が表示されます。
4. [**Wake on LAN** 接続］を選択します。オプションは、選択した場所に対して構成した種類 ［リモート **PC Wake on LAN**］の接続です。
5. マシンをインポートします。
6. [**Create**］をクリックします。

手順 **3**: デリバリーグループの作成とユーザーの割り当て　デリバリーグループを作成して、配信するマシンをグループ化し、それらのマシンにアクセスできるユーザーを指定します。

1. グループに名前を付けます。
2. 必要に応じてマシンカタログを選択します。[リモート **PC** アクセス］カタログのみが表示されます。
3. ユーザーをグループに割り当てます。

手順 **4**: **Workspace URL** をユーザーと共有　ワークスペースの ［構成］**>**［アクセス］から Workspace URL をユーザーと共有します。

オフィス **PC** を配信する（電源管理されていない）

このセクションでは、オフィス PC を配信する（電源管理されていない）展開のプロセスについて説明します。

前提条件

開始する前に、以下が必要です:

- PC のマシン名。

- Citrix Virtual Delivery Agent（VDA）を各 PC にインストールする。（この手順はカタログの作成後に実行できます。）

  詳しくは、「VDA のダウンロード」を参照してください。

準備

画面上の質問に答えて、次のインフラストラクチャレベルの設定を完了します。

#	設定	説明
1	マシンの割り当ての種類を選択する。	マシンの割り当て方法を選択します。 オプション：静的自動割り当て、静的事前割り当て、ランダムプール未割り当て
2	ユーザーによるマシンの電源投入を許可するかを決定する	［リモートユーザーがマシンの電源を自分でオンにする］をオフのままにします。
3	ユーザー ID の種類を選択する	ユーザー管理の ID の種類を選択します。 オプション：Active Directory、Azure Active Directory、Google Cloud Identity、および Okta

展開手順

インフラストラクチャレベルの設定を完了すると、この展開シナリオに固有の手順が表示されます。画面の指示に従って設定を完了してください。

手順 **1**：リソースの場所の追加　Cloud Connector をインストールしてリソースの場所をセットアップします。

1. リソースの場所の名前を入力します。
2. Cloud Connector をダウンロードして、少なくとも 2 台の Windows Server マシンにインストールします。
3. インストールされている Cloud Connector を検出します。

> 注：
>
> ホスト接続の作成は、マシンの電源を管理する場合にのみ必要です。

手順 **2**：リモート **PC** アクセスカタログの作成　カタログを作成し、そこにオフィス PC をインポートします。

1. カタログに名前を付けます
2. リソースの場所を選択します。
3. 割り当ての種類を選択します。デフォルトでは、準備段階で選択した種類が表示されます。
4. マシンをインポートします。
5. [**Create**] をクリックします。

手順 **3**：デリバリーグループの作成とユーザーの割り当て　配信するマシンのデリバリーグループを作成して、それらのマシンにアクセスできるユーザーを指定します。

1. グループに名前を付けます。
2. 必要に応じてマシンカタログを選択します。[リモート **PC** アクセス] カタログのみが表示されます。
3. ユーザーをグループに割り当てます。

手順 **4**：**Workspace URL** をユーザーと共有　ワークスペースの [構成] **>** [アクセス] から Workspace URL をユーザーと共有します。

マシン **ID**

October 30, 2023

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

マシン **ID** の種類

次のマシン ID の種類がサポートされています。

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

マシン **ID** の種類	説明
Azure AD に参加済み	ID が Azure AD で作成および管理されます。プロビジョニングされたマシンは、割り当てられたマシン ID を使用して Azure AD に参加します。Citrix DaaS への仮想マシンのインポートはサポートされていません。
Hybrid Azure AD 参加済み	ID がオンプレミスの Active Directory で作成され、Azure AD Connect で Azure AD と同期されます。プロビジョニングされたマシンは、オンプレミスの Active Directory および Azure AD に参加します。その後、マシンは Hybrid Azure AD 参加済みになります。ハイブリッド Azure AD 参加済み仮想マシンをインポートする場合、その仮想マシンは Citrix DaaS によって Active Directory 参加済み仮想マシンとして扱われます。
ドメイン非参加	ID がローカルのマシンで作成および管理されます。Citrix DaaS への仮想マシンのインポートはサポートされていません。

サポートされる構成

以下は、各シナリオでサポートされている構成の詳細です。

サポートされるインフラストラクチャ

マシン **ID**	**Citrix DaaS**	**Citrix Workspace**	**Citrix StoreFront**	**Citrix Gateway** サービス	**Citrix Gateway**
AD に参加済み	はい	はい	はい	はい	はい
Azure AD に参加済み	はい	はい	いいえ	はい	いいえ
Hybrid Azure AD 参加済み	はい	はい	はい	はい	はい
ドメイン非参加	はい	はい	はい	はい	はい

> 注

> Storefront を使用する場合、ローカルホストキャッシュもサービス継続性も、ドメイン非参加セッションホストでは使用できません。

サポートされるワークスペース認証 **ID** プロバイダー

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

Active Directory 参加済み

July 3, 2023

ID がオンプレミスの Active Directory で作成および管理されます。プロビジョニングされたマシンは、割り当てられたマシン ID を使用してオンプレミスの Active Directory に参加します。フォレストとドメインのサポート対象の機能レベルについて詳しくは、「Active Directory の機能レベル」を参照してください。

Citrix DaaS を使用して Active Directory（AD）参加済みカタログを作成する方法については、「マシンカタログの作成」を参照してください。

Azure Active Directory 参加済み

May 17, 2024

> 注:
>
> 2023 年 7 月より、Microsoft は Azure Active Directory（Azure AD）の名前を Microsoft Entra ID に変

> 更しました。このドキュメントでは、Azure Active Directory、Azure AD、または AAD への言及はすべて、Microsoft Entra ID を意味することになります。

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

要件

- コントロールプレーン：「サポートされる構成」を参照してください。
- VDA の種類：シングルセッション（デスクトップのみ）、またはマルチセッション（アプリとデスクトップ）
- VDA バージョン：2203 以降
- プロビジョニングの種類：Machine Creation Services（MCS）、マシンプロファイルワークフローを使用した永続および非永続
- 割り当ての種類：専用およびプール
- ホストプラットフォーム：Azure のみ
- Rendezvous V2 を有効にする必要があります

制限事項

- サービスの継続性はサポートされていません。
- 仮想デスクトップへのシングルサインオンはサポートされていません。ユーザーは、デスクトップに資格情報を手動で入力する必要があります。
- 仮想デスクトップでの Windows Hello によるログインはサポートされていません。現時点では、ユーザー名とパスワードのみがサポートされています。ユーザーが Windows Hello メソッドを使用してログインしようとすると、ブローカーユーザーではないことを示すエラーが表示され、セッションが切断されます。関連するメソッドには、PIN、FIDO2 キー、MFA などがあります。
- Microsoft Azure Resource Manager クラウド環境のみがサポートされています。
- 仮想デスクトップセッションの初回起動時、Windows サインイン画面に、最後にログオンしたユーザーのログオンプロンプトが表示され、別のユーザーに切り替えるオプションがない場合があります。ユーザーは、ログオンがタイムアウトしてデスクトップのロック画面が表示されるまで待ってから、ロック画面をクリックしてログオン画面をもう一度表示する必要があります。この時点で、ユーザーは ［他のユーザー］を選択して資格情報を入力できます。この動作は、マシンが非永続的であるすべての新しいセッションで見られます。

注意事項

イメージの構成

- Citrix Optimizerツールを使用して Windows イメージを最適化することを検討してください。

Azure AD に参加済み

- ユーザーが仮想デスクトップにログインしたときにセットアップのメッセージが表示されないように、Windows Hello を無効にすることを検討してください。VDA 2209 以降を使用している場合、自動で無効になります。以前のバージョンでは、次の 2 つの方法のいずれかでこれを実行できます:
  - グループポリシーまたはローカルポリシー
    - ［コンピューターの構成］**>** ［管理用テンプレート］**>** ［**Windows** コンポーネント］**>** ［**Windows Hello for Business**］に移動します。
    - ［**Windows Hello for Business** を使用する］を次のように設定します:
      - ［無効］、または
      - ［有効］にして、［**Do not start Windows Hello provisioning after sign-in**］を選択します。
  - Microsoft Intune
    - Windows Hello for Business を無効にするデバイスプロファイルを作成します。詳しくは、Microsoft のドキュメントを参照してください。
    - 現在、Microsoft は永続マシンの Intune 登録のみをサポートしています。つまり、非永続マシンを Intune で管理することはできません。
- ユーザーは、AAD 資格情報を使用してマシンにログインするために、Azure での明示的なアクセスが許可されている必要があります。これは、リソースグループレベルで役割の割り当てを追加することで容易になります。
  1. Azure ポータルにサインインします。
  2. ［**Resource Groups**］を選択します。
  3. 仮想デスクトップワークロードが存在するリソースグループをクリックします。
  4. ［**Access control (IAM)**］を選択します。
  5. ［**Add role assignment**］をクリックします。
  6. **Virtual Machine User Login** を検索して一覧から選択し、［次へ］をクリックします。
  7. ［**User, group, or service principal**］を選択します。
  8. ［メンバーの選択］をクリックして、仮想デスクトップへのアクセスを提供するユーザーとグループを選択します。
  9. ［**Select**］をクリックします。
  10. ［**Review + assign**］をクリックします。
  11. ［**Review + assign**］を再度クリックします。

> 注:
>
> MCS に仮想デスクトップのリソースグループを作成させることを選択した場合は、マシンカタログの作成後にこの役割の割り当てを追加します。

- マスター VM は、Azure AD 参加済み、またはドメイン非参加にすることができますが、この機能には、VDA バージョン 2212 以降が必要です。

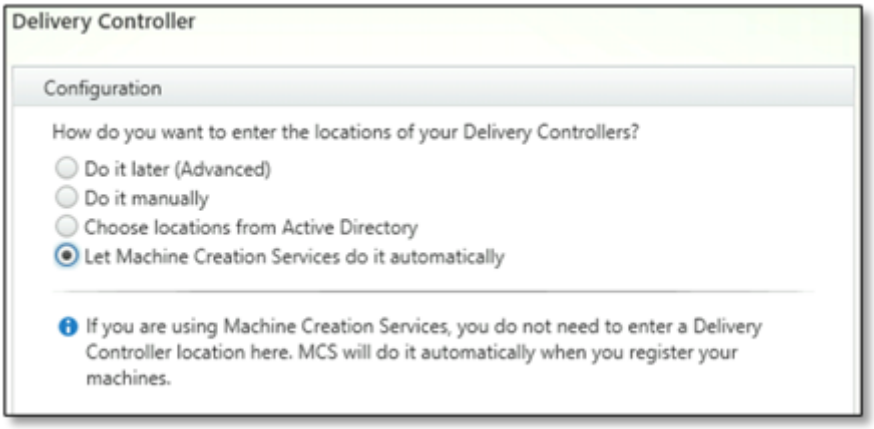
VDA のインストールと構成

VDA をインストールするための手順に従います:

1. インストールウィザードで次のオプションを選択してください:

   - ［環境］ページで、［マスター **MCS** イメージを作成する］を選択します。

   - ［Delivery Controller］ページで、［**Machine Creation Services** で自動的に指定する］を選択します。



2. VDA をインストールした後、次のレジストリ値を追加します:

   - キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent
   - 値の種類: DWORD
   - 値の名前: GctRegistration
   - 値のデータ: 1

3. Windows 11 22H2 ベースのマスター VM の場合、SYSTEM アカウントを使ったシステム起動時に、次のコマンドを実行するスケジュールされたタスクをマスター VM に作成します。マスター VM でタスクをスケジュールするこのタスクは、VDA バージョン 2212 以前でのみ必要です。


```
reg ADD HKLM\Software\AzureAD\VirtualDesktop /v Provider /t REG_SZ
    /d Citrix /f
<!--NeedCopy-->
```

4. マスター VM を Azure AD に参加させた後、dsregcmdユーティリティで参加を手動で解除する場合は、HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Azure\CurrentVersion\AADLoginForWindowsExtensio のAADLoginForWindowsExtensionJoinedの値が 0（ゼロ）あることを確認してください。

次の手順

リソースの場所とホスト接続が使用可能になったら、マシンカタログの作成に進みます。Azure Active Directory 参加済みマシンカタログの作成について詳しくは、「Azure Active Directory 参加済みカタログの作成」を参照してください。

Microsoft Intune

June 12, 2024

この記事では、「Citrix DaaS のシステム要件」セクションで概説されている要件に加えて、Citrix DaaS を使用して Microsoft Intune 対応カタログを作成するための要件について説明します。

Microsoft Intune は、モバイルデバイス管理（MDM）とモバイルアプリケーション管理（MAM）に重点を置いたクラウドベースのサービスです。携帯電話、タブレット、ラップトップなど、組織のデバイスの使用方法を制御します。詳しくは、「Microsoft Intune」を参照してください。デバイスは、最小システム要件を満たしている必要があります。詳しくは、Microsoft 社のドキュメント「Intune でサポートされるオペレーティングシステムとブラウザー」を参照してください。

Microsoft Intune は、Azure AD の機能を使用して動作します。

> 重要:
>
> この機能を有効にする前に、Azure 環境で、Microsoft Intune を使用するためのライセンス要件を満たしていることを確認してください。詳しくは、Microsoft 社のドキュメントを参照してください: https://docs.microsoft.com/en-us/mem/intune/fundamentals/licenses。適切な Intune ライセンスがない場合は、この機能を有効にしないでください。

要件

- コントロールプレーン: Citrix DaaS
- VDA の種類: シングルセッション OS VDA
- VDA バージョン: 2203 以降

- プロビジョニングの種類：マシンプロファイルワークフローのみを使用した Machine Creation Services（MCS）による永続
- 割り当ての種類：専用

制限事項

- シングルセッションの Azure AD 参加済みの永続的な VM のみをサポートします。
- 共同管理機能でユーザー資格情報またはデバイス資格情報を使用して、シングルセッションのハイブリッド Azure AD 参加済み永続 VM のみをサポートします。詳しくは、「グループポリシーを使用して Windows デバイスを自動的に登録する」を参照してください。
- マシンカタログの作成中または更新中にイメージの準備をスキップしないでください。

注意事項

- Windows Hello for Business を無効にするデバイスプロファイルを作成します。
- マスター VM を Microsoft Intune で管理する必要がある場合は、VDA バージョン 2212 以降を使用してください。

次の手順

Microsoft Intune 対応カタログの作成について詳しくは、「Microsoft Intune 対応カタログの作成」を参照してください。

Hybrid Azure Active Directory 参加済み

May 17, 2024

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

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

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

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

要件

- コントロールプレーン:「サポートされる構成」を参照してください。
- VDA の種類:シングルセッション(デスクトップのみ)、またはマルチセッション(アプリとデスクトップ)
- VDA バージョン:2212 以降
- プロビジョニングの種類:Machine Creation Services(MCS)、永続および非永続
- 割り当ての種類:専用およびプール
- ホストプラットフォーム:ハイパーバイザーまたはクラウドサービス

制限事項

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

注意事項

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

  1. `gpedit.msc`を実行します。
  2. [コンピューターの構成] > [管理用テンプレート] > [**Windows** コンポーネント] > [デバイスの登録] に移動します。

3. ［ドメインに参加しているコンピューターをデバイスとして登録する］を ［無効］に設定します。

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

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

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

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

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

        break;
     }


    if ($provider -eq 1)
    {

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

   }


  Start-Sleep 1
 }

<!--NeedCopy-->
```


次の手順

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

ドメイン非参加

November 22, 2023

この記事では、「Citrix DaaS のシステム要件」セクションで概説されている要件に加えて、Citrix DaaS を使用してドメイン非参加カタログを作成するための要件について説明します。

要件

- コントロールプレーン:「サポートされる構成」を参照してください。
- VDA の種類: シングルセッション（デスクトップのみ）、またはマルチセッション（アプリとデスクトップ）
- VDA バージョン: 2203 以降
- プロビジョニングの種類: Machine Creation Services（MCS）、永続および非永続
- 割り当ての種類: 専用およびプール
- ホストプラットフォーム: MCS でサポートされているすべてのプラットフォーム
- Rendezvous V2 を有効にする必要があります
- Cloud Connector: オンプレミスハイパーバイザーでマシンをプロビジョニングする予定の場合、または Workspace で Active Directory を ID プロバイダーとして使用する場合にのみ必要です。

制限事項

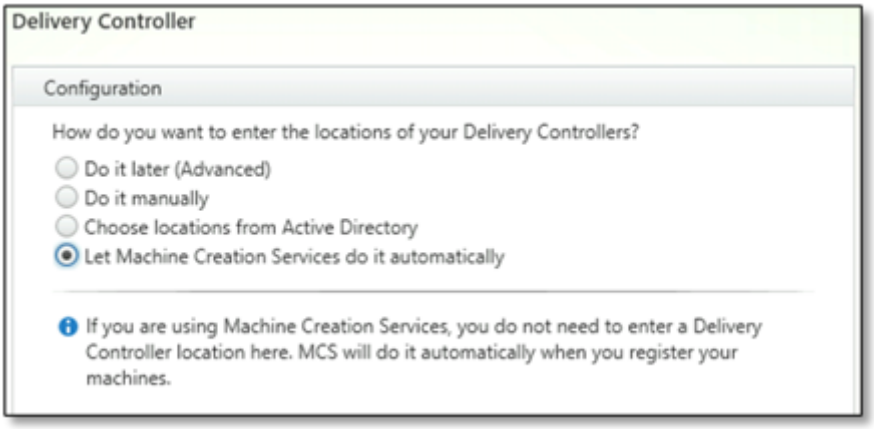
- サービスの継続性はサポートされていません。
- ドメイン非参加マルチセッション VDA を使用する場合、ローカルユーザーのプロファイルデータは保持されず、ログオフ時に削除されます。

VDA のインストールと構成

VDA をインストールするための手順に従います:

1. インストールウィザードで次のオプションを選択してください:
    - [環境] ページで、[マスター **MCS** イメージを作成する] を選択します。

- ［Delivery Controller］ページで、［**Machine Creation Services** で自動的に指定する］を選択します。



2. VDA をインストールした後、次のレジストリ値を追加します:

   - キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent
   - 値の種類: DWORD
   - 値の名前: GctRegistration
   - 値のデータ: 1

次の手順

リソースの場所とホスト接続が使用可能になったら、マシンカタログの作成に進みます。ドメイン非参加マシンカタログの作成について詳しくは、「ドメイン非参加カタログの作成」を参照してください。

リソースの場所の設定

June 12, 2024

リソースの場所にはユーザーへのアプリケーションおよびデスクトップの配信に必要なリソースが含まれます。リソースは、Citrix Cloud で管理します。一般的なリソースには以下のものがあります:

- ホストとして知られているハイパーバイザーまたはクラウドサービスには、次のものが含まれます:
  - Active Directory ドメインコントローラー。
  - Virtual Delivery Agent（VDA）: VDA は、アプリケーションとデスクトップをユーザーに配信するマシンにインストールされます。
  - Citrix Gateway（オプション）: ユーザーに提供するアプリケーションやデスクトップに外部から安全にアクセスできるようにするには、Citrix Gateway VPX アプライアンスをリソースの場所に追加します。次に、Citrix Gateway を設定します。
  - Citrix StoreFront サーバー。
  - Citrix Cloud と通信するには、すべてのリソースの場所に Citrix Cloud Connector を配置する必要があります。リソースの場所ごとに Cloud Connector を 2 つ以上配置することをお勧めします。

ゾーンは、リソースの場所に相当します。リソースの場所を作成して Cloud Connector をインストールすると、ゾーンが自動的に作成されます。詳しくは、「ゾーン」を参照してください。

リソースの種類について詳しくは、「Citrix Cloud への接続」を参照してください。

ホストの要件

VM をプロビジョニングするハイパーバイザーまたはクラウドサービスには、固有の権限または設定が必要です。

- ハイパーバイザーまたはクラウドサービスを使用するのに仮想ネットワークが必要な場合は、そのマニュアルのガイダンスに従ってください。
- リソースの場所に追加するマシン用に適切な仮想プライベートクラウド（VPC）（AWS または GCP の場合）または仮想ネットワーク（VNET）（Azure の場合）を作成します。
- 仮想ネットワーク内のマシン間の送信および受信トラフィックを保護する適切なルールを作成します。たとえば、AWS を使用する場合は、VPC のセキュリティグループに適切なルールを構成して、指定した IP アドレスのみに VPC 内のマシンがアクセスできるようにします。

次のホストタイプがサポートされています:

- Amazon Web Services（AWS）仮想化環境
- XenServer 仮想化環境
- Google Cloud Platform 仮想化環境
- HPE Moonshot 仮想化環境

- Microsoft Azure Resource Manager 仮想化環境
- Microsoft System Center Virtual Machine Manager 仮想化環境
- Nutanix 仮想化環境
- Nutanix クラウドおよびパートナーソリューション
- VMware 仮想化環境
- VMware クラウドおよびパートナーソリューション

Active Directory

Windows サーバーをプロビジョニングし、Active Directory ドメインサービス（AD DS）をインストールしてドメインコントローラーに昇格します。ガイダンスについては、Microsoft のドキュメント「Active Directory ドメインサービスの概要」を参照してください。

重要な考慮事項は次のとおりです：

- Active Directory ドメインサービスを実行するドメインコントローラーが少なくとも 1 つ必要です。
- ドメインコントローラーには Citrix コンポーネントをインストールしないでください。

詳しくは、次のトピックを参照してください：

- Active Directory の機能レベル
- Citrix Cloud の ［ID およびアクセス管理］ 。
- Active Directory を Citrix Cloud に接続する
- Active Directory で Connector Appliance を使用した展開シナリオ

Cloud Connector

Cloud Connector は、VDA、StoreFront、クラウドベースの Delivery Controller 間の通信を可能にする、Citrix Cloud のサービス集合体です。Cloud Connector は、対話形式またはコマンドラインでインストールできます。

Cloud Connector について詳しくは、以下を参照してください：

- Citrix Cloud Connector
- Citrix Cloud Connector の技術詳細
- プロキシとファイアウォールの構成
- インストール
- コネクタの更新

サイズおよびスケールの考慮事項

- Citrix DaaS のサイジングとスケーラビリティを評価する場合、すべてのコンポーネントを考慮する必要があります。

- 特定の要件に応じて、Cloud Connector と StoreFront の構成を調査し、テストします。
- マシンのサイズを縮小すると、システムのパフォーマンスに悪影響を与える可能性があります。

記事「Cloud Connector のサイズおよびスケールの考慮事項」の内容は次のとおりです:

- サイズとスケールのテストに関する情報
- テスト済みの最大容量
- Cloud Connector マシン構成の推奨ベストプラクティス

リソースの種類の追加

1. Citrix Cloudにサインインします。
2. 左上隅のメニューで、［リソースの場所］を選択します。
3. ［**+** リソースの場所］を選択してリソースの場所を追加します。
4. リソースの場所の名前を入力し、［保存］をクリックします。命名に関する考慮事項については、「命名制限」を参照してください。
5. 新しいリソースの場所から、［**+ Cloud Connectors**］を選択します。
6. Cloud Connector ソフトウェアをダウンロードして、Citrix DaaS リソースがあるドメイン内の少なくとも 2 台のサーバーにインストールします。
   - インストール中に、これまでの手順で作成したリソースの場所を選択します。
   - インストール後、Citrix Cloud はサーバーをリソースの場所に追加し、Cloud Connector をインストールしたドメインを登録します。
7. 登録されたドメインがアクティブであることを確認します:
   - Citrix Cloud メニューで、**Identity Access Management** を選択します。
   - ドメインを選択します。Cloud Connector が展開されているドメインの一覧が表示されます。
   - Citrix DaaS で使用しているドメインを見つけます。アクティブなドメインは、ドメインエントリの左側に緑色のバーが表示されます。

   視覚的なインジケーターがないドメインは ［未使用］状態です。マシンカタログのセットアップ中に未使用のドメインを指定すると、カタログの作成に失敗します。マシンカタログのセットアップがエラーなしで行われるようにするには、「未使用のドメインをアクティブ化する」手順に従います。

   詳しくは、CTX473009：DaaS カタログ作成ウィザード：新しいマシンアカウントの作成時の「内部サーバーエラー」を参照してください。

未使用ドメインのアクティブ化

1. ［ドメイン］タブの ［**ID** およびアクセス管理］で、［未使用のドメインを表示］を選択します。このオプションを選択すると、ラベルが ［未使用のドメインを非表示］に変わります。

2. 一覧で未使用のドメインを見つけます。未使用のドメインには、ドメインエントリの左側に灰色のバーが表示され、右側にオプション 1 つの省略記号メニューが表示されます。
3. 省略記号メニューを選択し、［ドメインを使用する］を選択します。灰色のバーが緑色になり、省略記号メニューが ［無効］に変わります。

次の手順

- 単純な概念実証環境を展開する場合、ユーザーにアプリまたはデスクトップを配信するように指定されたマシンへの ［VDA のインストール］ を実行します。
- 特定のホストタイプのリソースの場所を設定する場合:
  - AWS 仮想化環境
  - Google Cloud 仮想化環境
  - HPE Moonshot 仮想化環境
  - Microsoft Azure Resource Manager 仮想化環境
  - Microsoft System Center Virtual Machine Manager 仮想化環境
  - Nutanix 仮想化環境
  - Nutanix クラウドおよびパートナーソリューション
  - VMware 仮想化環境
  - VMware クラウドおよびパートナーソリューション
  - XenServer 仮想化環境
- 完全展開の場合は、リソースの場所に接続とリソースを作成して管理します。
- インストールおよび構成プロセスのすべての手順を確認します

AWS 仮想化環境

March 31, 2024

この記事では、Citrix DaaS で使用できるリソースの場所として AWS アカウントを設定する方法について説明します。

このリソースの場所には基本的なコンポーネントセットのみが含まれており、概念実証など、リソースを複数のアベイラビリティゾーンに展開する必要のない展開に最適です。

この記事のタスクを完了すると、リソースの場所に次のコンポーネントが追加されます:

- 単一アベイラビリティゾーン内にパブリックサブネットとプライベートサブネットを持つ仮想プライベートクラウド（VPC）。

- VPC のプライベートサブネットに配置され、Active Directory ドメインコントローラーと DNS サーバーの両方として実行されるインスタンス。
- VPC のプライベートサブネットに配置され、Citrix Cloud Connector がインストールされた 2 つのドメイン参加済みインスタンス。
- VPC のパブリックサブネットに配置され、要塞ホストとして機能するインスタンス。このインスタンスは、管理目的でプライベートサブネット内のインスタンスへの RDP 接続を開始するために使用されます。リソースの場所の設定が完了したら、このインスタンスをシャットダウンし、アクセスできないようにしてもかまいません。プライベートサブネット内の他のインスタンス（VDA インスタンスなど）を管理する必要性が生じた場合に、このインスタンスを再起動できます。

本記事のタスクの完了後、VDA のインストール、マシンのプロビジョニング、マシンカタログの作成、デリバリーグループの作成を行えます。

タスクの概要

パブリックサブネットとプライベートサブネットを持つ仮想プライベートクラウド（**VPC**）の設定。このタスクを完了すると、パブリックサブネット内のエラスティック IP アドレスを持つ NAT ゲートウェイが AWS によって展開されます。これにより、プライベートサブネット内のインスタンスからインターネットにアクセスできるようになります。パブリックサブネット内のインスタンスが受信パブリックトラフィックにアクセスできるようになりますが、プライベートサブネット内のインスタンスはアクセスできません。

セキュリティグループの構成。セキュリティグループは、VPC 内のインスタンスのトラフィックを制御する仮想ファイアウォールとして機能します。セキュリティグループにルールを追加することで、パブリックサブネット内のインスタンスがプライベートサブネット内のインスタンスと通信できるようになります。また、これらのセキュリティグループを仮想プライベートクラウド内の各インスタンスに関連付けることもできます。

DHCP オプションセットの作成。Amazon VPC ではデフォルトで DHCP サービスと DHCP サービスが提供されるため、Active Directory ドメインコントローラーの DNS の構成方法が変わります。Amazon の DHCP を無効にすることはできません。また Amazon の DNS は、Active Directory の名前解決には使用できず、パブリック DNS 解決にのみ使用できます。DHCP 経由でインスタンスに渡すドメインサーバーとネームサーバーを指定するため、DHCP オプションセットを作成します。このセットにより Active Directory ドメインサフィックスを割り当てて、VPC 内のすべてのインスタンスに DNS サーバーを指定します。ドメインへのインスタンスの参加時にホスト（A）レコードと逆引き参照（PTR）レコードが自動的に登録されるようにするため、プライベートサブネットに追加するインスタンスごとに、ネットワークアダプタープロパティを構成します。

VPC への要塞ホスト、ドメインコントローラー、**Citrix Cloud Connector** の追加。要塞ホストにより、プライベートサブネット内のインスタンスにログオンし、ドメインの設定、ドメインへのインスタンスの追加、Cloud Connector のインストールを行うことができます。

タスク **1**：**VPC** を設定する

1. AWS マネジメントコンソールで ［**VPC**］を選択します。

2. VPC ダッシュボードで、[**Create VPC**] を選択します。
3. [**VPC and more**] を選択します。
4. [NAT gateways ($)] で [**In 1 AZ**] または [**1 per AZ**] を選択します。
5. [DNS] オプションで [**Enable DNS hostnames**] が選択されたままにします。
6. [**Create VPC**] を選択します。AWS により、パブリックサブネット、プライベートサブネット、インターネットゲートウェイ、ルートテーブル、デフォルトのセキュリティグループが作成されます。

> 注:
>
> AWS コンソールで AWS 仮想プライベートクラウド（VPC）の名前を変更すると、Citrix Cloud の既存のホスティングユニットが破損します。ホスティングユニットが破損している場合、カタログを作成したり、既存のカタログにマシンを追加したりすることはできません。既知の問題から：PMCS-7701

タスク **2**：セキュリティグループを構成する

このタスクでは、VPC 用に次のセキュリティグループを作成して構成します:

- パブリックサブネット内のインスタンスを関連付けるパブリックセキュリティグループ。
- プライベートサブネット内のインスタンスを関連付けるプライベートセキュリティグループ。

セキュリティグループを作成するには:

1. VPC ダッシュボードで、[**Security Groups**] を選択します。
2. パブリックセキュリティグループのセキュリティグループを作成します。[**Create Security Group**] を選択し、グループの名前タグと説明を入力します。[VPC] では、先ほど作成した VPC を選択します。[**Yes, Create**] を選択します。

パブリックセキュリティグループを構成する

1. セキュリティグループの一覧で、先ほど作成したパブリックセキュリティグループを選択します。
2. [**Inbound Rules**] タブを選択し、[Edit] を選択して次の規則を作成します:

種類	接続元
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	パブリックセキュリティグループを選択します。
ICMP	0.0.0.0/0
22（SSH）	0.0.0.0/0
80（HTTP）	0.0.0.0/0
443（HTTPS）	0.0.0.0/0

種類	接続元
1494（ICA/HDX）	0.0.0.0/0
2598（セッション画面の保持）	0.0.0.0/0
3389（RDP）	0.0.0.0/0

3. 最後に ［**Save**］を選択します。
4. ［**Outbound Rules**］タブを選択し、［**Edit**］を選択して次の規則を作成します。

種類	接続先
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	0.0.0.0/0
ICMP	0.0.0.0/0

5. 最後に ［**Save**］を選択します。

プライベートセキュリティグループを構成する

1. セキュリティグループの一覧で、先ほど作成したプライベートセキュリティグループを選択します。
2. パブリックセキュリティグループからのトラフィックに対する設定をまだ行っていない場合は、TCP ポートを設定する必要があります。［**Inbound Rules**］タブを選択し、［**Edit**］を選択して次の規則を作成します:

種類	接続元
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	パブリックセキュリティグループを選択します。
ICMP	パブリックセキュリティグループを選択します。
TCP 53（DNS）	パブリックセキュリティグループを選択します。
UDP 53（DNS）	パブリックセキュリティグループを選択します。
80（HTTP）	パブリックセキュリティグループを選択します。
TCP 135	パブリックセキュリティグループを選択します。
TCP 389	パブリックセキュリティグループを選択します。
UDP 389	パブリックセキュリティグループを選択します。

種類	接続元
443（HTTPS）	パブリックセキュリティグループを選択します。
TCP 1494（ICA/HDX）	パブリックセキュリティグループを選択します。
TCP 2598（セッション画面の保持）	パブリックセキュリティグループを選択します。
3389（RDP）	パブリックセキュリティグループを選択します。
TCP 49152～65535	パブリックセキュリティグループを選択します。

3. 最後に ［**Save**］を選択します。
4. ［**Outbound Rules**］タブを選択し、［**Edit**］を選択して次の規則を作成します。

種類	接続先
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	0.0.0.0/0
ICMP	0.0.0.0/0
UDP 53（DNS）	0.0.0.0/0

5. 最後に ［**Save**］を選択します。

タスク **3**：インスタンスを起動する

次の手順に従い、EC2 インスタンスを 4 つ作成し、Amazon で生成されたデフォルトの管理者パスワードの暗号化を解除します：

1. AWS マネジメントコンソールで ［**EC2**］を選択します。
2. EC2 ダッシュボードで ［**Launch Instance**］を選択します。
3. Windows Server マシンのイメージとインスタンスの種類を選択します。
4. ［**Configure Instance Details**］ページで、インスタンスの名前を入力し、先ほど設定した VPC を選択します。
5. ［**Subnet**］で、各インスタンスに対して次の選択を行います：
   - Bastion host：パブリックサブネットを選択します
   - Domain controller and Connectors：プライベートサブネットを選択します
6. ［**Auto-assign Public IP address**］で、各インスタンスに対して次の選択を行います：

- Bastion host：[**Enable**] を選択します
- Domain controller and Connectors：[**Use default setting**] または [**Disable**] を選択します

7. [**Network Interfaces**] で、ドメインコントローラーインスタンスと Cloud Connector インスタンスに、プライベートサブネットの IP 範囲に含まれるプライマリ IP アドレスを入力します。
8. 必要に応じて、[**Add Storage**] ページでディスクサイズを変更します。
9. [**Tag Instance**] ページで、各インスタンスにわかりやすい名前を付けます。
10. [**Configure Security Groups**] ページで、[**Select an existing security group**] を選択し、インスタンスごとに次の選択を行います：

    - Bastion host：パブリックセキュリティグループを選択します。
    - Domain controller and Cloud Connectors：プライベートセキュリティグループを選択します。

11. 選択した内容を確認し、[**Launch**] を選択します。
12. 新しいキーペアを作成するか、既存のキーペアを選択します。新しいキーペアを作成する場合は、秘密キー（`.pem`）ファイルをダウンロードして安全な場所に保管します。インスタンスのデフォルトの管理者パスワードを取得するときに、この秘密キーを提供する必要があります。
13. [**Launch Instances**] を選択します。[**View Instances**] をクリックしてインスタンスの一覧を表示します。新しく起動したインスタンスがすべての状態チェックに合格するまで待ってから、インスタンスにアクセスします。
14. 各インスタンスのデフォルトの管理者パスワードを取得します。

    a) インスタンスの一覧で目的のインスタンスを選択し、[**Connect**] を選択します。
    b) [**RDP client**] タブに移動し、[**Get Password**] を選択し、プロンプトが表示されたら秘密キー（`.pem`）ファイルをアップロードします。
    c) 人間が判読できるパスワードを取得するには、[**Decrypt Password**] を選択します。AWS にデフォルトのパスワードが表示されます。

15. 4 つのインスタンスを作成し終わるまで、手順 2 以降のすべてのステップを繰り返します：

    - パブリックサブネットに含まれる 1 つの踏み台ホストインスタンス
    - プライベートサブネットに含まれる 3 つのインスタンスは次のように使用されます：
      - 1 つをドメインコントローラーとして使用
      - 2 つを Cloud Connector として使用

タスク **4**：**DHCP** オプションセットを作成する

1. VPC ダッシュボードで [**DHCP Options Sets**] を選択します。
2. 次の情報を入力します：

- Name tag：オプションセットのフレンドリ名を入力します。
- Domain name：ドメインコントローラーインスタンスの構成に使用する完全修飾ドメイン名を入力します。
- Domain name servers：ドメインコントローラーインスタンスに割り当てたプライベート IP アドレスと、「**AmazonProvidedDNS**」という文字列をカンマで区切って入力します。
- NTP servers：このフィールドは空白のままにします。
- NetBIOS name servers：ドメインコントローラーインスタンスのプライベート IP アドレスを入力します。
- NetBIOS node type：「**2**」と入力します。

3. ［**Yes, Create**］を選択します。
4. 新しく作成したセットを VPC に関連付けます：

   a) VPC ダッシュボードで ［**Your VPCs**］を選択し、先ほど設定した VPC を選択します。
   b) ［**Actions**］**>** ［**Edit DHCP Options Set**］の順に選択します。
   c) プロンプトが表示されたら、新しく作成したセットを選択して ［**Save**］を選択します。

タスク **5**：インスタンスを構成する

1. RDP クライアントを使用して、要塞ホストインスタンスのパブリック IP アドレスに接続します。プロンプトが表示されたら、管理者アカウントの資格情報を入力します。
2. 踏み台ホストインスタンスでリモートデスクトップ接続を起動し、構成するインスタンスのプライベート IP アドレスに接続します。プロンプトが表示されたら、インスタンスの管理者アカウントの資格情報を入力します。
3. プライベートサブネット内のすべてのインスタンスに対して、DNS 設定を構成します：

   a) ［スタート］**>** ［コントロールパネル］**>** ［ネットワークとインターネット］**>** ［ネットワークと共有センター］**>** ［アダプターの設定の変更］の順に選択します。表示されたネットワーク接続をダブルクリックします。
   b) ［プロパティ］**>** ［インターネットプロトコルバージョン **4**（**TCP/IPv4**）］**>** ［プロパティ］を選択します。
   c) ［詳細設定］**>** ［**DNS**］を選択します。次の設定を有効にして ［**OK**］を選択します：

      - この接続のアドレスを **DNS** に登録する
      - この接続の **DNS** サフィックスを **DNS** 登録に使う

4. ドメインコントローラーを構成する：

   a) サーバーマネージャーを使用して、すべてのデフォルト機能を持つ Active Directory ドメインサービスの役割を追加します。

b) インスタンスをドメインコントローラーに昇格させます。昇格時には、DNS を有効にして、DHCP オプションセットの作成時に指定したドメイン名を使用します。メッセージに従ってインスタンスを再起動します。

5. 最初の Cloud Connector を構成する:

a) インスタンスをドメインに参加させ、プロンプトが表示されたら再起動します。踏み台ホストインスタンスから、RDP を使用してインスタンスに再び接続します。
b) Citrix Cloud にサインインします。左上のメニューで、［リソースの場所］を選択します。
c) Cloud Connector をダウンロードします。
d) プロンプトが表示されたら、`cwcconnector.exe`ファイルを実行して Citrix Cloud の資格情報を入力します。ウィザードの指示に従って操作します。
e) ウィザードが完了したら、[更新] を選択して［リソースの場所］ページを表示します。Cloud Connector が登録されると、インスタンスがページに表示されます。

6. 2 番目の Cloud Connector を構成するため、Cloud Connector を構成する手順を繰り返します。
7. IAM ポリシーを Cloud Connector にアタッチして、役割ベースの承認により AWS ホスト接続をサポートします。リソースの場所にあるすべての Cloud Connector に同じ IAM ポリシーをアタッチする必要があります。AWS 権限については、「Required AWS permissions」を参照してください。

次の手順

- 単純な概念実証環境を展開する場合、ユーザーにアプリまたはデスクトップを配信するように指定されたマシンへの ［VDA のインストール］ を実行します。
- 接続の作成と管理については、「AWS への接続」を参照してください。
- インストールおよび構成プロセスのすべての手順を確認します

追加情報

- 接続とリソースの作成と管理
- マシンカタログの作成

Google Cloud 仮想化環境

May 17, 2024

Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）を使用すると、Google Cloud でマシンをプロビジョニングおよび管理できます。

前提条件

Google Cloud Platform（GCP）への VM のプロビジョニングを開始する前に、次の前提条件が満たされていることを確認する必要があります。

1. Citrix サブスクリプションには、ハイブリッドマルチクラウドワークロードのサポートが含まれている必要があります。詳しくは、「Compare Citrix subscription features」を参照してください。
2. 管理者アカウントには、ホスト接続、マシンカタログ、およびデリバリーグループを作成するための十分な権限が必要です。詳しくは、「管理者権限の委任の構成」を参照してください。
3. マシンカタログに関連付けられたすべてのコンピューティングリソースが保存される、Google Cloud プロジェクトを特定します。既存のプロジェクトでも新しいプロジェクトでもかまいません。詳しくは、「Google Cloud プロジェクト」をご覧ください。
4. Citrix DaaS との統合に必要な Google Cloud API を有効にします。詳しくは、「Google Cloud API の有効化」をご覧ください。
5. Google Cloud でサービスアカウントを作成し、適切な権限を付与します。詳しくは、「サービスアカウントの構成と更新」を参照してください。
6. Citrix Cloud サービスアカウントのキーファイルをダウンロードします。詳しくは、「Citrix Cloud サービスアカウントキー」を参照してください。
7. 仮想マシンは、パブリック IP アドレスなしで Google API にアクセスできる必要があります。詳しくは、「プライベート Google アクセスの有効化」を参照してください。

Google Cloud プロジェクト

基本的に、Google Cloud プロジェクトには次の 2 種類があります:

- プロビジョニングプロジェクト: この場合、現在の管理者アカウントは、プロジェクトでプロビジョニングされたマシンを所有しています。このプロジェクトは、ローカルプロジェクトとも呼ばれます。
- 共有 VPC プロジェクト: プロビジョニングプロジェクトで作成されたマシンが、共有 VPC プロジェクトの VPC を使用するプロジェクト。プロジェクトのプロビジョニングに使用される管理者アカウントには、このプロジェクトでの権限が制限されています。具体的には、VPC を使用する権限のみです。

サービスエンドポイント URL

次の URL にアクセスできる必要があります:

- https://oauth2.googleapis.com
- https://cloudresourcemanager.googleapis.com
- https://compute.googleapis.com
- https://storage.googleapis.com
- https://cloudbuild.googleapis.com

Google Cloud API の有効化

Citrix DaaS の完全な構成インターフェイスで Google Cloud 機能を使用するには、Google Cloud プロジェクトで次の API を有効にします:

- Compute Engine API
- Cloud Resource Manager API
- Identity and Access Management（IAM）API
- Cloud Build API

Google Cloud コンソールから、次の手順を実行します:

1. 左上隅のメニューで ［**API** とサービス］**>**［**Enabled APIs & services**］を選択します。
2. ［**Enabled APIs & services**］画面で、［Compute Engine API］が有効になっていることを確認します。有効になっていない場合、次の手順を実行します:

   a) ［**API** とサービス］**>**［ライブラリ］の順に選択します。
   b) 検索ボックスに 「*Compute Engine*」と入力します。
   c) 検索結果から、［**Compute Engine API**］を選択します。
   d) ［**Compute Engine API**］ページで、［**Enable**］を選択します。

3. Cloud Resource Manager API を有効にします。

   a) ［**API** とサービス］**>**［ライブラリ］の順に選択します。
   b) 検索ボックスに 「*Cloud Resource Manager*」と入力します。
   c) 検索結果から、［**Cloud Resource Manager API**］を選択します。
   d) ［**Cloud Resource Manager API**］ページで、［**Enable**］を選択します。API のステータスが表示されます。

4. 同様に、［**Identity and Access Management (IAM) API**］、［**Cloud Build API**］、および ［**Cloud Key Management Service (KMS) API**］を有効にします。

Google Cloud Shell を使用して API を有効にすることもできます。これを行うには、以下の手順に従います:

1. Google コンソールを開き、Cloud Shell を読み込みます。
2. Cloud Shell で次の 4 つのコマンドを実行します:

   - gcloud services enable compute.googleapis.com
   - gcloud services enable cloudresourcemanager.googleapis.com
   - gcloud services enable iam.googleapis.com
   - gcloud services enable cloudbuild.googleapis.com
   - gcloud services enable cloudbuild.googleapis.com

3. Cloud Shell でプロンプトが表示されたら、［**Authorize**］をクリックします。

サービスアカウントの構成と更新

> 注:
>
> 2024 年 4 月 29 日、GCP は Cloud Build サービスのデフォルトの動作とサービスアカウントの使用に関する変更を導入します。詳しくは、「Cloud Build サービスアカウントの変更」を参照してください。2024 年 4 月 29 日より前に Cloud Build API が有効になっていた既存の Google プロジェクトは、この変更の影響を受けません。ただし、4 月 29 日以降も既存の Cloud Build サービスの動作を継続する場合は、Cloud Build API を有効にする前に、制約の適用を無効にする組織ポリシーを作成または適用できます。これにより、以下のコンテンツは「2024 年 4 月 29 日より前」と「2024 年 4 月 29 日以降」の 2 つに分割されます。新しい組織ポリシーを設定する場合は、「2024 年 4 月 29 日より前」のセクションに従ってください。

2024 年 **4** 月 **29** 日より前

Citrix Cloud は、Google Cloud プロジェクト内で次の 3 つの個別のサービスアカウントを使用します:

- *Citrix Cloud* サービスアカウント: このサービスアカウントにより、Citrix Cloud は Google プロジェクトにアクセスし、マシンをプロビジョニングおよび管理できます。このサービス アカウントは、Google Cloud によって生成された キー を使用して Google Cloud に対して認証されます。

  ここで説明するように、このサービスアカウントを手動で作成する必要があります。詳しくは、「Citrix Cloud サービスアカウントの作成」を参照してください。

  このサービスアカウントは、メールアドレスで識別できます。例: `<my-service-account>@<project-id>.iam.gserviceaccount.com`。

- *Cloud Build* サービスアカウント: このサービスアカウントは、「Google Cloud API の有効化」に記載されているすべての API を有効にすると自動的にプロビジョニングされます。自動的に作成されたサービスアカウントをすべて表示するには、**Google Cloud** コンソールで ［**IAM & admin**］**>** ［**IAM**］の順に移動し、［**Google** 提供のロール付与を含める］チェックボックスをオンにします。

  このサービスアカウントは、**Project ID** と、**cloudbuild** で始まるメールアドレスで識別できます。例: `<project-id>@cloudbuild.gserviceaccount.com`

  サービスアカウントに次の役割が付与されているかどうかを確認します。役割を追加する必要がある場合は、「Cloud Build サービスアカウントへの役割の追加」で説明されている手順に従います。

  - Cloud Build サービスアカウント
  - コンピューティングインスタンス管理者
  - サービスアカウントユーザー

- *Cloud Compute* サービスアカウント: このサービスアカウントは、Compute API がアクティブ化されると、Google Cloud で作成されたインスタンスに Google Cloud によって追加されます。このアカウントには、操作を行うための IAM の基本編集者の役割があります。ただし、より詳細な制御を行うためにデフォルトのアクセス権限を削除する場合は、次のアクセス権限を必要とする ストレージ管理者の役割を追加する必要があります:

- resourcemanager.projects.get
- storage.objects.create
- storage.objects.get
- storage.objects.list

このサービスアカウントは、**Project ID** と、**compute** で始まるメールアドレスで識別できます。例：<project-id>-compute@developer.gserviceaccount.com。

Citrix Cloud サービスアカウントの作成　Citrix Cloud サービスアカウントを作成するには、次の手順に従います：

1. Google Cloud コンソールで、［**IAM** と管理］**>**［サービスアカウント］の順に選択します。
2. ［**Service accounts**］ページで、［**CREATE SERVICE ACCOUNT**］を選択します。
3. ［**Create service account**］ページで必要な情報を入力してから、［**CREATE AND CONTINUE**］を選択します。
4. ［**Grant this service account access to project**］ページで、［**Select a role**］ドロップダウンメニューをクリックし、必要な役割を選択します。役割を追加する場合は、［**+ADD ANOTHER ROLE**］をクリックします。

   各アカウント（個人またはサービス）には、プロジェクトの管理を定義するさまざまな役割があります。このサービスアカウントに次の役割を付与します：

   - コンピューティング管理者
   - ストレージ管理者
   - Cloud Build エディター
   - サービスアカウントユーザー
   - クラウドデータストアユーザー
   - Cloud KMS Crypto Operator

   Cloud KMS Crypto Operator には次の権限が必要です：

   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.get
   - cloudkms.keyRings.list

   > 注：
   >
   > すべての API を有効にして、新しいサービスアカウントの作成中に、使用できる役割の完全な一覧を取得してください。

5. ［**CONTINUE**］をクリックします

6. [**Grant users access to this service account**] ページでユーザーまたはグループを追加し、このサービスアカウントで操作を実行できるアクセス権をユーザーに付与します。
7. [**DONE**] をクリックします。
8. IAM メインコンソールに移動します。
9. 作成されたサービスアカウントを識別します。
10. 役割が正常に割り当てられていることを確認します。

注意事項:

サービスアカウントを作成するときは、次の点を考慮してください:

- [**Grant this service account access to project**] と **Grant users access to this service account**] の手順は任意です。これらのオプションの構成手順をスキップする場合、新しく作成されたサービスアカウントは [**IAM** と管理] **>** [**IAM**] ページには表示されません。
- サービスアカウントに関連付けられている役割を表示するには、オプションの手順をスキップせずに役割を追加します。このプロセスにより、構成されたサービスアカウントの役割が確実に表示されます。

Citrix Cloud サービスアカウントキー　Citrix DaaS で接続を作成するには、Citrix Cloud サービスアカウントキーが必要です。キーは資格情報ファイル（.json）に含まれています。キーを作成すると、ファイルが自動的にダウンロードされ、「**Downloads**」フォルダーに保存されます。キーを作成するときは、必ずキータイプを JSON に設定してください。それ以外の場合、Citrix の完全な構成インターフェイスでは解析できません。

サービスアカウントキーを作成するには、[**IAM & Admin**] **>** [**Service accounts**] に移動して Citrix Cloud サービスアカウントのメールアドレスをクリックします。[**Keys**] タブを選択してから、[**Add Key**] **>** [**Create new key**] を選択します。キーの種類として必ず **JSON** を選択してください。

> ヒント:
>
> Google Cloud コンソールの [**Service accounts**] ページを使用してキーを作成します。セキュリティのために、キーを定期的に変更することをお勧めします。既存の Google Cloud 接続を編集することで、Citrix Virtual Apps and Desktops アプリケーションに新しいキーを提供できます。

Citrix Cloud サービスアカウントへの役割の追加　Citrix Cloud サービスアカウントに役割を追加するには:

1. Google Cloud コンソールで、[**IAM** と管理] **>** [**IAM**] の順に選択します。
2. [**IAM**] **>** [**PERMISSIONS**] ページで、作成したサービスアカウントを見つけ、メールアドレスで識別します。

   例: `<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. 鉛筆アイコンを選択して、サービスアカウントのプリンシパルへのアクセス権を編集します。
4. 選択したプリンシパルオプションの [**Edit access to** “**project-id**”] ページで、[**ADD ANOTHER ROLE**] を選択してサービスアカウントに必要な役割を 1 つずつ追加し、[**SAVE**] を選択します。

Cloud Build サービスアカウントへの役割の追加　Cloud Build サービスアカウントに役割を追加するには:

1. Google Cloud コンソールで、[**IAM** と管理] **>** [**IAM**] の順に選択します。
2. [**IAM**] ページで、**Project ID** と、**cloudbuild** で始まるメールアドレスで識別できる Cloud Build サービスアカウントを見つけます。

   例: <project-id>@cloudbuild.gserviceaccount.com
3. 鉛筆アイコンを選択して、Cloud Build アカウントの役割を編集します。
4. 選択したプリンシパルオプションの [**Edit access to "project-id"**] ページで、[**ADD ANOTHER ROLE**] を選択して Cloud Build サービスアカウントに必要な役割を 1 つずつ追加し、[**SAVE**] を選択します。

   > 注:
   >
   > すべての API を有効にして、役割の完全な一覧を取得します。

2024 年 **4** 月 **29** 日以降

Citrix Cloud は、Google Cloud プロジェクト内で次の 2 つの個別のサービスアカウントを使用します:

- *Citrix Cloud* サービスアカウント: このサービスアカウントにより、Citrix Cloud は Google プロジェクトにアクセスし、マシンをプロビジョニングおよび管理できます。このサービス アカウントは、Google Cloud によって生成された キー を使用して Google Cloud に対して認証されます。

  このサービスアカウントは手動で作成する必要があります。

  このサービスアカウントは、メールアドレスで識別できます。例: <my-service-account>@<project-id>.iam.gserviceaccount.com。
- *Cloud Compute* サービスアカウント: このサービスアカウントは、「Google Cloud API の有効化」に記載されているすべての API を有効にすると自動的にプロビジョニングされます。自動的に作成されたサービスアカウントをすべて表示するには、**Google Cloud** コンソールで [**IAM & admin**] **>** [**IAM**] の順に移動し、[**Google** 提供のロール付与を含める] チェックボックスをオンにします。このアカウントには、操作を行うための IAM の基本編集者の役割があります。ただし、より詳細な制御を行うためにデフォルトのアクセス権限を削除する場合は、次のアクセス権限を必要とする ストレージ管理者の役割を追加する必要があります:

  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

  このサービスアカウントは、**Project ID** と、**compute** で始まるメールアドレスで識別できます。例: <project-id>-compute@developer.gserviceaccount.com.

  サービスアカウントに次の役割が付与されているかどうかを確認します。

- Cloud Build サービスアカウント
- コンピューティングインスタンス管理者
- サービスアカウントユーザー

Citrix Cloud サービスアカウントの作成　Citrix Cloud サービスアカウントを作成するには、次の手順に従います:

1. Google Cloud コンソールで、[**IAM** と管理] **>** [サービスアカウント] の順に選択します。
2. [**Service accounts**] ページで、[**CREATE SERVICE ACCOUNT**] を選択します。
3. [**Create service account**] ページで必要な情報を入力してから、[**CREATE AND CONTINUE**] を選択します。
4. [**Grant this service account access to project**] ページで、[**Select a role**] ドロップダウンメニューをクリックし、必要な役割を選択します。役割を追加する場合は、[**+ADD ANOTHER ROLE**] をクリックします。

   各アカウント（個人またはサービス）には、プロジェクトの管理を定義するさまざまな役割があります。このサービスアカウントに次の役割を付与します:

   - コンピューティング管理者
   - ストレージ管理者
   - Cloud Build エディター
   - サービスアカウントユーザー
   - クラウドデータストアユーザー
   - Cloud KMS Crypto Operator

   Cloud KMS Crypto Operator には次の権限が必要です:

   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.get
   - cloudkms.keyRings.list

   > 注:
   >
   > すべての API を有効にして、新しいサービスアカウントの作成中に、使用できる役割の完全な一覧を取得してください。

5. [**CONTINUE**] をクリックします
6. [**Grant users access to this service account**] ページでユーザーまたはグループを追加し、このサービスアカウントで操作を実行できるアクセス権をユーザーに付与します。
7. [**DONE**] をクリックします。

8. IAM メインコンソールに移動します。
9. 作成されたサービスアカウントを識別します。
10. 役割が正常に割り当てられていることを確認します。

注意事項:

サービスアカウントを作成するときは、次の点を考慮してください:

- [**Grant this service account access to project**] と **Grant users access to this service account**] の手順は任意です。これらのオプションの構成手順をスキップする場合、新しく作成されたサービスアカウントは [**IAM** と管理] **>** [**IAM**] ページには表示されません。
- サービスアカウントに関連付けられている役割を表示するには、オプションの手順をスキップせずに役割を追加します。このプロセスにより、構成されたサービスアカウントの役割が確実に表示されます。

Citrix Cloud サービスアカウントキー　Citrix DaaS で接続を作成するには、Citrix Cloud サービスアカウントキーが必要です。キーは資格情報ファイル（.json）に含まれています。キーを作成すると、ファイルが自動的にダウンロードされ、「**Downloads**」フォルダーに保存されます。キーを作成するときは、必ずキータイプを JSON に設定してください。それ以外の場合、Citrix の完全な構成インターフェイスでは解析できません。

サービスアカウントキーを作成するには、[**IAM & Admin**] **>** [**Service accounts**] に移動して Citrix Cloud サービスアカウントのメールアドレスをクリックします。[**Keys**] タブを選択してから、[**Add Key**] **>** [**Create new key**] を選択します。キーの種類として必ず **JSON** を選択してください。

> ヒント:
>
> Google Cloud コンソールの [**Service accounts**] ページを使用してキーを作成します。セキュリティのために、キーを定期的に変更することをお勧めします。既存の Google Cloud 接続を編集することで、Citrix Virtual Apps and Desktops アプリケーションに新しいキーを提供できます。

Citrix Cloud サービスアカウントへの役割の追加　Citrix Cloud サービスアカウントに役割を追加するには:

1. Google Cloud コンソールで、[**IAM** と管理] **>** [**IAM**] の順に選択します。
2. [**IAM**] **>** [**PERMISSIONS**] ページで、作成したサービスアカウントを見つけ、メールアドレスで識別します。

   例: `<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. 鉛筆アイコンを選択して、サービスアカウントのプリンシパルへのアクセス権を編集します。
4. 選択したプリンシパルオプションの [**Edit access to** “**project-id**”] ページで、[**ADD ANOTHER ROLE**] を選択してサービスアカウントに必要な役割を 1 つずつ追加し、[**SAVE**] を選択します。

Cloud Compute サービスアカウントに役割を追加する　Cloud Compute サービスアカウントに役割を追加するには:

1. Google Cloud コンソールで、[**IAM** と管理] **>** [**IAM**] の順に選択します。
2. [**IAM**] ページで、**Project ID** と、**compute** で始まるメールアドレスで識別できる Cloud Build サービスアカウントを見つけます。

   例: `<project-id>-compute@developer.gserviceaccount.com`
3. 鉛筆アイコンを選択して、Cloud Build アカウントの役割を編集します。
4. 選択したプリンシパルオプションの [**Edit access to "project-id"**] ページで、[**ADD ANOTHER ROLE**] を選択して Cloud Build サービスアカウントに必要な役割を 1 つずつ追加し、[**SAVE**] を選択します。

   > 注:
   >
   > すべての API を有効にして、役割の完全な一覧を取得します。

ストレージ権限とバケットの管理

Citrix DaaS は、Google Cloud サービスのクラウドビルドエラーのレポートプロセスを改善します。このサービスは、Google Cloud でビルドを実行します。Citrix DaaS は、Google Cloud サービスがビルドログ情報をキャプチャする`citrix-mcs-cloud-build-logs-{ region } -{ 5 random characters }`という名前のストレージバケットを作成します。このバケットには、30 日後にコンテンツを削除するオプションが設定されています。このプロセスでは、接続に使用するサービスアカウントで、Google Cloud の権限が`storage.buckets.update`に設定されている必要があります。サービスアカウントにこの権限が設定されていない場合、Citrix DaaS はエラーを無視し、カタログの作成プロセスを続行します。この権限がないと、ビルドログのサイズが大きくなり、手動によるクリーンアップが必要になります。

プライベート **Google** アクセスの有効化

ネットワークインターフェイスに割り当てられた外部 IP アドレスが VM にない場合、パケットは他の内部 IP アドレスの宛先にのみ送信されます。プライベートアクセスを有効にすると、VM は Google API および関連サービスで使用される外部 IP アドレスのセットに接続します。

> 注:
>
> プライベート Google アクセスが有効になっているかどうかに関係なく、パブリック IP アドレスを持つ VM もパブリック IP アドレスを持たない VM もすべて、特にサードパーティのネットワークアプライアンスが環境にインストールされている場合、Google パブリック API にアクセスできる必要があります。

サブネット内の VM が、MCS プロビジョニング用のパブリック IP アドレスなしで Google API にアクセスできるようにするには:

1. Google Cloud で、[**VPC network configuration**] にアクセスします。
2. [**Subnets in current project**] タブで、Citrix 環境に利用されているサブネットを特定します。
3. サブネットの名前をクリックし、**Private Google Access** を有効にします。

詳しくは、「プライベート Google アクセスの構成」を参照してください。

> 重要:
>
> インターネットへの VM アクセスを防止するようにネットワークが構成されている場合は、VM が接続されているサブネットに対してプライベート Google アクセスを有効にすることに関連するリスクを、組織が想定していることを確認してください。

次の手順

- 単純な概念実証環境を展開する場合、ユーザーにアプリまたはデスクトップを配信するように指定されたマシンへの ［VDA のインストール］ を実行します。
- 接続の作成と管理については、「Google クラウド環境への接続」を参照してください。
- インストールと構成プロセスの手順をすべて確認します。

追加情報

- 接続とリソースの作成と管理
- マシンカタログの作成

HPE Moonshot 仮想化環境

June 12, 2024

Citrix DaaS は、DaaS コントロールプレーンに存在する Citrix が管理する HPE Moonshot プラグインを通じて HPE Moonshot ワークロードを管理します。このプラグインを使用すると、HPE Moonshot シャーシへの接続の作成、カタログの作成、カタログ内のマシンの電源管理が可能になります。

主な手順

1. HPE 環境をセットアップします。
2. HPE Moonshot シャーシへの接続を作成します。

   > 注:
   >
   > フィーチャートグルを有効にすると、Citrix が管理する HPE Moonshot プラグインが自動的にインストールされます。したがって、HPE 管理の HPE Moonshot プラグインの代わりに Citrix 管理の Moonshot プラグインを使用して、既存のマシンカタログを引き続き使用できます。

3. マシンカタログを作成します。

> 注:
>
> カタログを作成する前に、1 つ以上の HPE Moonshot カートリッジノードが存在し、それらのノードに VDA がインストールされていることを確認してください。HPE Moonshot シャーシをハイパーバイザーとして、カートリッジノードを VM として考えることができます。

4. デリバリーグループを作成します。
5. 残りの非管理対象 HPE Moonshot ノードを管理対象カタログまたはデリバリーグループに移行します。

次の手順

- 単純な概念実証環境を展開する場合、ユーザーにアプリまたはデスクトップを配信するマシン上で ［VDA のインストール］ を実行します。
- 接続の作成と管理については、「HPE Moonshot への接続」を参照してください。
- インストールと構成プロセスの手順をすべて確認します。

追加情報

- 接続とリソースの作成と管理
- マシンカタログの作成

Microsoft Azure Resource Manager 仮想化環境

May 17, 2024

Microsoft Azure Resource Manager を使用して、Citrix DaaS 環境で仮想マシンをプロビジョニングする場合は、以下をよく理解しておいてください:

- Microsoft Entra ID とは
- Integrating Microsoft Entra ID with applications getting started guide
- Microsoft Entra ID のアプリケーションおよびサービスプリンシパルオブジェクト

Microsoft Azure Resource Manager を設定するには、「リソースの場所のセットアップ」を参照してください。

次の手順

- 単純な概念実証環境を展開する場合、ユーザーにアプリまたはデスクトップを配信するように指定されたマシンへの ［VDA のインストール］ を実行します。
- 接続の作成と管理については、「Microsoft Azure への接続」を参照してください。
- インストールと構成プロセスの手順をすべて確認します。

追加情報

- 接続とリソースの作成と管理
- マシンカタログの作成
- CTX219211：Microsoft Entra ID アカウントの設定
- CTX219243：Azure サブスクリプションへの XenApp および XenDesktop アクセス権の付与
- CTX219271：サイト間 VPN を使用したハイブリッドクラウドの展開

Microsoft System Center Virtual Machine Manager 仮想化環境

January 25, 2024

Hyper-V と Microsoft System Center Virtual Machine Manager（VMM）を使用して仮想マシンを提供する場合は、このトピックのガイダンスに従ってください。

サポートされる VMM のバージョン一覧については、「システム要件」を参照してください。

Machine Creation Services または Citrix Provisioning（旧称 Provisioning Services）を使用して、次のものをプロビジョニングできます：

- 第 1 世代デスクトップまたはサーバー OS の VM
- 第 2 世代 Windows Server 2016、Windows Server 2019、Windows Server 2022、Windows 10、Windows 11 VM（Secure Boot あり、またはなし）

ハイパーバイザーのインストールおよび構成

サーバー上に Microsoft Hyper-V の役割および VMM をインストールします。

次のアカウント情報を確認します：

［管理］**>**［完全な構成］で、接続の作成時に指定するアカウントは、VMM 管理者またはその Hyper-V マシンの VMM 委任管理者である必要があります。指定したアカウントに設定されている役割が VMM の委任管理者のみの場合、接続の作成時にストレージデータが ［完全な構成］インターフェイスの一覧に表示されません。

使用するユーザーアカウントは、仮想マシンのライフサイクル管理（仮想マシンの作成、更新、削除など）を実行できるように、各 Hyper-V サーバー上の Administrators ローカルセキュリティグループのメンバーでもある必要があります。

単一の SCVMM が異なるデータセンターの複数のクラスターを管理する大規模な環境では、管理者のホストグループのスコープを制限できます。

ホストグループのスコープを制限するには、Microsoft System Center Virtual Machine Manager（VMM）コンソールで委任された管理者の役割を使用します。

1. [**Create User Roles Wizard**] で、ユーザー役割として **Fabric Administrator**（委任された管理者）を選択します。
2. [**Members**] で、委任された管理者として使用するユーザーアカウントを Active Directory に追加します。
3. [**Scope**] で、委任された管理者にアクセス権を与えるホストグループを選択します。
4. 委任された管理者のユーザー資格情報で、新しい実行アカウントを作成します。これらの資格情報を使用して、後でハイパーバイザー接続を作成します。メインの管理者の役割アカウントは使用しないでください。

VMM コンソールのインストール

Citrix Cloud Connector を搭載した各サーバーに、System Center Virtual Machine Manager コンソールをインストールします。

コンソールのバージョンは管理サーバーと同じバージョンにする必要があります。古いコンソールを管理サーバーに接続することはできますが、バージョンが異なる場合、VDA のプロビジョニングは失敗します。

SCVMM を介した **Azure Stack HCI** プロビジョニング

Azure Stack HCI は、ハイパーコンバージドインフラストラクチャ（HCI）クラスターソリューションであり、ハイブリッドのオンプレミス環境で、仮想化された Windows および Linux ワークロードとそれらのストレージをホストします。

Azure ハイブリッドサービスは、クラウドベースの監視、サイト回復、VM バックアップなどの機能でクラスターを強化します。Azure Portal ですべての Azure Stack HCI 展開を表示することもできます。

Azure Stack HCI の **SCVMM** との統合

Azure Stack HCI を SCVMM と統合するには、最初に Azure Stack HCI クラスターを作成してから、そのクラスターを SCVMM と統合する必要があります。

1. Azure Stack HCI クラスターを作成して Azure に登録する方法については、Microsoft のドキュメント「Azure Stack HCI を Azure に接続する」を参照してください。
2. Azure Stack HCI クラスターを SCVMM と統合するには、次の手順を実行します：

   a) SCVMM サーバーをホストする準備ができているマシンにログインし、SCVMM 2019 UR3 以降をインストールします。

   > 注：
   >
   > SCVMM 2019 UR3 以降の管理者コンソールを Cloud Connector VM にインストールします。

   b) VMM コンソールの ［設定］ページで、実行アカウントを作成します。

c) SCVMM サーバーで管理者権限を使用して次の PowerShell コマンドを実行し、ホストとして Azure Stack HCI クラスターを追加します:

```
$runAsAccountName = 'Admin'
$runAsAccount = Get-SCRunAsAccount -Name $runAsAccountName
$hostGroupName = 'All Hosts'
$hostGroup = Get-SCVMHostGroup -Name $hostGroupName
$hostCluster = 'FQDN of Azure Stack HCI cluster'
Add-SCVMHostCluster -Name $hostCluster -RunAsynchronously -
    VMHostGroup
$hostGroup -Credential $runAsAccount -RemoteConnectEnabled
    $true
<!--NeedCopy-->
```

d) これで、VMM コンソールのノードと合わせて Azure Stack HCI クラスターを確認できるようになりました。

e)［完全な構成］インターフェイスで、SCVMM ホスト接続を作成します。

次の手順

- 単純な概念実証環境を展開する場合、ユーザーにアプリまたはデスクトップを配信するように指定されたマシンへの ［VDA のインストール］ を実行します。
- 接続の作成と管理については、「Microsoft System Center Virtual Machine Manager への接続」を参照してください。
- インストールと構成プロセスの手順をすべて確認します。

追加情報

- 接続とリソースの作成と管理
- マシンカタログの作成

Nutanix 仮想化環境

February 9, 2024

Citrix DaaS 環境で Nutanix Acropolis を使用して仮想マシンを提供する場合は、以下のガイダンスに従ってください。セットアッププロセスには、Nutanix プラグインを Citrix DaaS 環境にインストールして登録するというタスクが含まれます。

『Nutanix Acropolis MCS Plugin Installation Guide』について詳しくは、Nutanix サポートポータルを参照してください。

> 重要:
>
> Nutanix プラグインのインストールを、Citrix DaaS によって Nutanix ハイパーバイザーを持つリソースの場所へのホスト接続を作成する必要があるすべての Cloud Connector に対して行う必要があります。

Nutanix プラグインのインストールと登録

すべての Cloud Connector に Nutanix プラグインをインストールして登録する手順を実行します。Citrix Cloud の ［管理］ > ［完全な構成］ 機能を使用して、Nutanix への接続を作成します。

Nutanix プラグインのインストールについて詳しくは、Nutanix のドキュメントサイトを参照してください。

Nutanix 仮想化環境のセットアップ方法について詳しくは、「リソースの種類を追加するか、Citrix Cloud で未使用のドメインをアクティブ化する」を参照してください。

次の手順

- 単純な概念実証環境を展開する場合、ユーザーにアプリまたはデスクトップを配信するように指定されたマシンへの ［VDA のインストール］ を実行します。
- 接続の作成と管理については、「Nutanix への接続」を参照してください。
- インストールと構成プロセスの手順をすべて確認します。

追加情報

- 接続とリソースの作成と管理
- マシンカタログの作成

Nutanix クラウドおよびパートナーソリューション

January 25, 2024

Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）は、次の Nutanix クラウドおよびパートナーソリューションをサポートしています:

- Nutanix Cloud Clusters on AWS

Nutanix Cloud Clusters on AWS

Citrix DaaS は、Nutanix Cloud Clusters on AWS をサポートします。Nutanix Clusters は、プライベートクラウドまたは複数のパブリッククラウドでのアプリケーションの実行をシンプルにします。Nutanix Cloud Clusters on AWS について詳しくは、「Nutanix Cloud Clusters on AWS Deployment and User Guide」を参照してください。

> ヒント：
>
> このサポートは、Nutanix オンプレミスクラスターと同じ機能を提供します。単一のクラスターのみサポートされます（*Prism Element*）。詳しくは、こちらを参照してください。

要件

Nutanix Clusters on AWS を使用するには、以下のアカウントが必要です：

- Nutanix アカウント
- 次の権限を持つ AWS アカウント：
  - IAMFullAccess
  - AWSConfigRole
  - AWSCloudFormationFullAccess

Nutanix Cluster の作成

Nutanix Cluster を作成するには：

1. Nutanix アカウントにログインします。
2. [**Nutanix cluster**] オプションを見つけ、[**Launch**] をクリックします。[**Nutanix Console**] が開きます。詳しくは、「Get Started with Nutanix Cluster on AWS」を参照してください。
3. [**new VPC**] の作成を選択します。

クラスター作成プロセスは、次のエラーで失敗することがあります：

- Cluster failed to create within a given time. Deleting cluster.（指定された時間内にクラスターを作成できませんでした。クラスターを削除しています）
- Host Nutanix Cluster - Node `XXXXXXXXXXX: Instance i-xxxxxxxxxxxxx: disable network interface source/dest check error.`
- Host Nutanix Cluster - Node `XXXXXXXXXXX: Unable to obtain instance i-xxxxxxxxxxxxxx network interface info.`

クラスターの作成に失敗した場合は、以下を行ってください：

- もう一度、別のリージョンで 1 つ作成してみてください。

- もう一度試す前に、必ず Nutanix CloudFormation スタック（CFS）を削除してください。

他のリソースに加えて、Nutanix CFS は以下を作成します：

- 「*Nutanix Cluster xxxxxxxxxxxx* 10.0.0.0/16」という名前の 1 つの VPC
- 「10.0.128.0/24」と「10.0.129.0/24」という 2 つのサブネット
- 1 つのインターネットゲートウェイ
- 1 つの NAT ゲートウェイ

クラスターが作成されたら、**Nutanix Prism** のアドレスを取得します：

1. ［**Nutanix Console**］に移動します。
2. コンソールの右上にある ［**Launch Prism Element**］リンクにホバーして、URL をコピーします。

次の手順

- 単純な概念実証環境を展開する場合、ユーザーにアプリまたはデスクトップを配信するように指定されたマシンへの ［VDA のインストール］ を実行します。
- 接続の作成と管理については、「Nutanix クラウドおよびパートナーソリューションへの接続」を参照してください。
- インストールと構成プロセスの手順をすべて確認します。

追加情報

- 接続とリソースの作成と管理
- マシンカタログの作成

VMware 仮想化環境

January 25, 2024

VMware を使用して仮想マシンを提供する場合は、このトピックのガイダンスに従ってください。

vCenter Server および必要な管理ツールをインストールします（vSphere vCenter のリンクモードはサポートされません。）

> 注：
>
> vSphere vCenter のリンクモードはサポートされません。

Machine Creation Services（MCS）を使用する場合は、「Disabling the vCenter Server Datastore Browser」の説明に従って vCenter Server のデータストアブラウザー機能を無効にすることは避けてください。この機能を無効にすると、MCS が正しく動作しなくなります。

VMware 仮想化環境をセットアップするには、「リソースの種類を追加するか、Citrix Cloud で未使用のドメインをアクティブ化する」を参照してください。

次の手順

- 単純な概念実証環境を展開する場合、ユーザーにアプリまたはデスクトップを配信するように指定されたマシンへの ［VDA のインストール］ を実行します。
- 接続の作成と管理については、「VMware への接続」を参照してください。
- インストールと構成プロセスの手順をすべて確認します。

追加情報

- 接続とリソースの作成と管理
- マシンカタログの作成

VMware クラウドおよびパートナーソリューション

January 25, 2024

Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）は、次の VMware Cloud およびパートナーソリューションをサポートしています:

- Azure VMware Solution（AVS）
- Google Cloud VMware Engine
- VMware Cloud on AWS（Amazon Web Services）

Citrix DaaS を使用して、VMware ベースのオンプレミスの Citrix ワークロードをそれぞれの VMware パートナーソリューションに移行します。

Azure VMware Solution（AVS）の統合

Citrix DaaS は AVSをサポートしています。AVS では、Azure インフラストラクチャによって作成された vSphere クラスターを含むクラウドインフラストラクチャが提供されます。オンプレミス環境で vSphere を使用するのと同じ方法で、DaaS を活用して VDA ワークロードのプロビジョニングに AVS を使用できます。

AVS クラスターのセットアップ

Citrix DaaS で AVS を使用できるようにするには、Azure で次の手順を実行します:

- ホストクォータの要求
- `Microsoft.AVS`リソースプロバイダーの登録
- ネットワーク計画のチェックリストの確認
- ネットワークチェックリスト
- AVS プライベートクラウドの作成
- AVS プライベートクラウドへのアクセス
- Azure での VMware プライベートクラウドのネットワークの構成
- DHCP の AVS 向け構成
- AVS でのネットワークセグメントの追加
- AVS 環境の確認

Azure Enterprise Agreement の顧客のホストクォータの要求　Azure Portal の［**Help + Support**］ページで［**New support request**］を選択し、次の情報を含めます:

- Issue type:［Technical］
- Subscription:サブスクリプションを選択します
- Service:［**All services**］**>**［**Azure VMware Solution**］
- Resource:［General question］
- Summary:［Need capacity］
- Problem type:［Capacity Management Issues］
- Problem subtype:［Customer Request for Additional Host Quota/Capacity］

サポートチケットの［**Description**］で［**Details**］タブに次の情報を含めます:

- 概念実証または実稼働
- リージョン名
- ホストの数
- その他の詳細

> 注:
>
> AVS には少なくとも 3 つのホストが必要です。冗長性のため 1 つ多くホストを使用することをお勧めします。

サポートチケットの詳細を指定した後、［**Review + Create**］を選択して Azure に要求を送信します。

Microsoft.AVS リソースプロバイダーの登録　ホストクォータを要求した後、リソースプロバイダーを登録します:

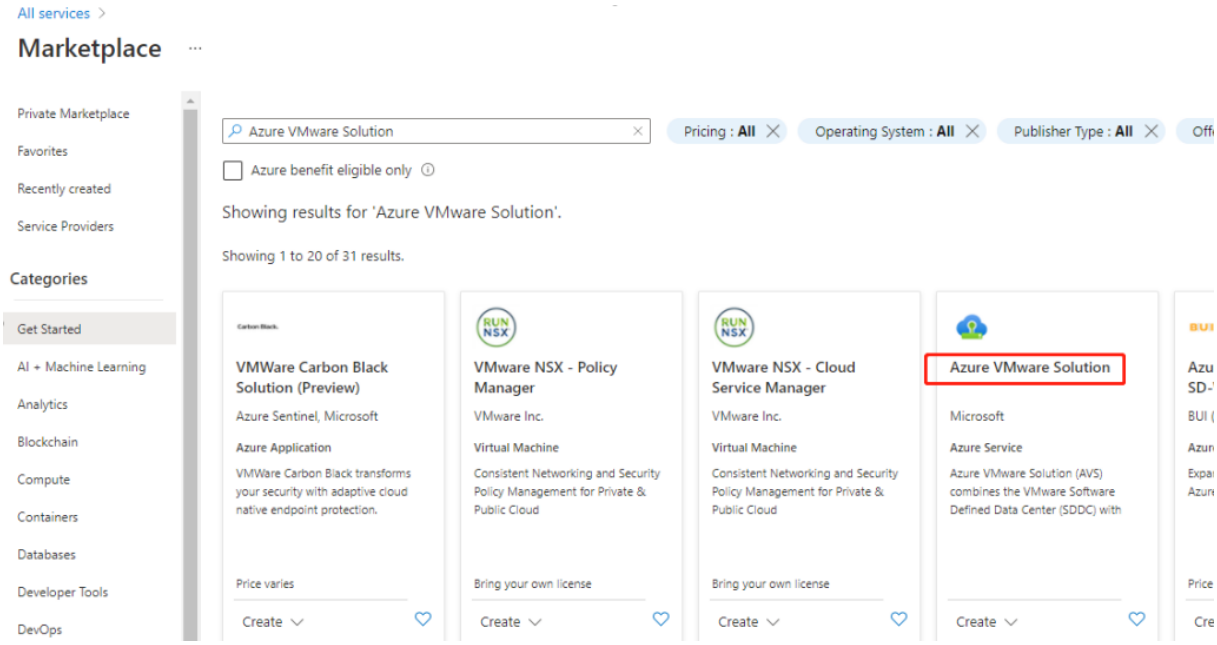
1. Azure Portal にサインインします。

2. Azure Portal のメニューで、[**All services**] を選択します。
3. [**All services**] メニューで、サブスクリプションを入力し、[**Subscriptions**] を選択します。
4. サブスクリプション一覧からサブスクリプションを選択します。
5. [**Resource providers**] を選択し、検索バーに 「**Microsoft.AVS**」と入力します。
6. リソースプロバイダーが登録されていない場合は、[**Register**] を選択します。

ネットワークに関する考慮事項　AVS では、特定のネットワークアドレス範囲とファイアウォールポートを必要とするネットワークサービスが提供されます。詳しくは、「Azure VMware Solution のネットワーク計画のチェックリスト」を参照してください。

AVS プライベートクラウドの作成　ご使用の環境のネットワーク要件を検討した後、ASV プライベートクラウドを作成します:

1. Azure Portal にサインインします。
2. [**Create a new resource**] を選択します。
3. [**Search the Marketplace**] ボックスで、「*Azure VMware Solution*」と入力し、一覧から [**Azure VMware Solution**] を選択します。



[**Azure VMware Solution**] ウィンドウで、次のことを行います:

1. [作成] を選択します。
2. [**Basics**] タブに移動します。
3. 以下の表内の情報を使用してフィールドの値を入力します:

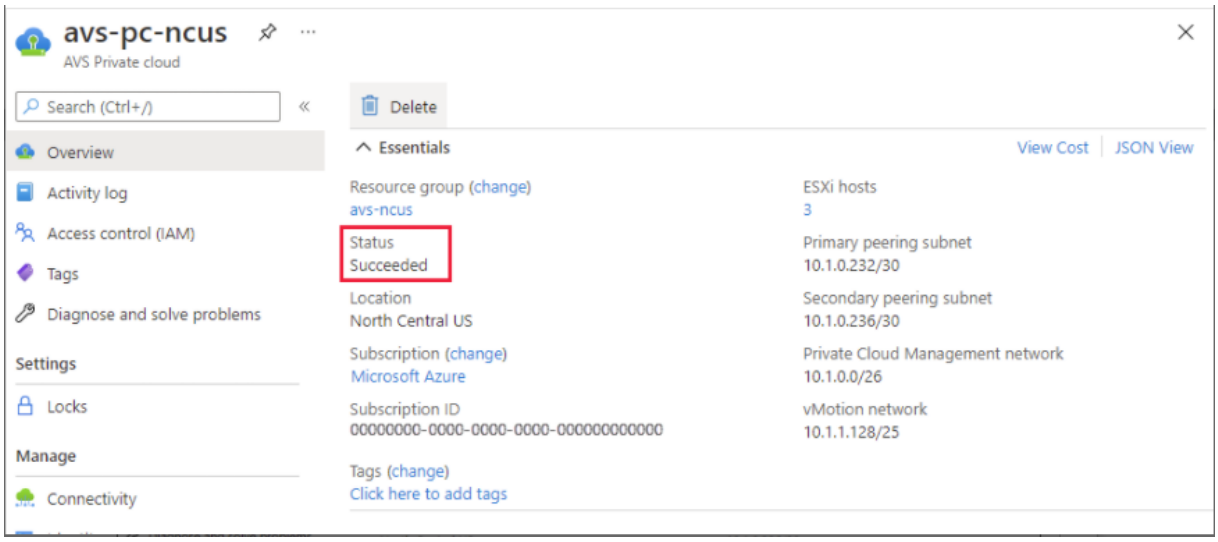
フィールド	値
Subscription	環境で使用する予定のサブスクリプションを選択します。Azure サブスクリプション内のすべてのリソースが一緒に請求されます。
リソースグループ	プライベートクラウドのリソースグループを選択します。Azure リソースグループは、Azure リソースが展開され管理される論理コンテナです。または、自分のプライベートクラウド用の新しいリソースグループを作成することもできます。
場所	米国東部など、場所を選択します。これは、計画フェーズで定義したリージョンです。
リソース名	Azure VMware Solution プライベートクラウドの名前を入力します。
Size of host	必要なサイズを選択します。
ホストの数	プライベートクラウドのクラスターに割り当てられているホストの数を示します。デフォルト値は 3 であり、展開後に増減できます。
Address block for private cloud	プライベートクラウド用に IP アドレスブロックを提供します。CIDR（クラスレスドメイン間ルーティング）は、プライベートクラウド管理ネットワークを表し、vCenter Server や NSX-T Manager などのクラスター管理サービスに使用されます。/22 アドレススペースを使用します。たとえば、10.175.0.0/22 です。アドレスは一意である必要があり、他の Azure 仮想ネットワークやオンプレミスネットワークと重複しないようにする必要があります。

［**Create a private cloud**］画面で、次のことを行います：

1. ［場所］フィールドで、AVS があるリージョンを選択します。リソースグループのリージョンは、この AVS のリージョンと同じになります。
2. ［**Size of host**］フィールドで、必要なサイズを選択します。
3. ［**Address Block for private cloud**］フィールドで IP アドレスを指定します。たとえば、10.15.0.0/22 です。
4. ［**Review + Create**］を選択します。
5. 情報を確認したら、［**Create**］をクリックします。

> ヒント：
>
> プライベートクラウドの作成には 3～4 時間かかる場合があります。単一のホストをクラスターに追加するには、30～45 分かかる場合があります。

展開が成功したことを確認します。作成したリソースグループに移動し、プライベートクラウドを選択します。［**Status**］が ［**Succeeded**］になると、展開は完了です。



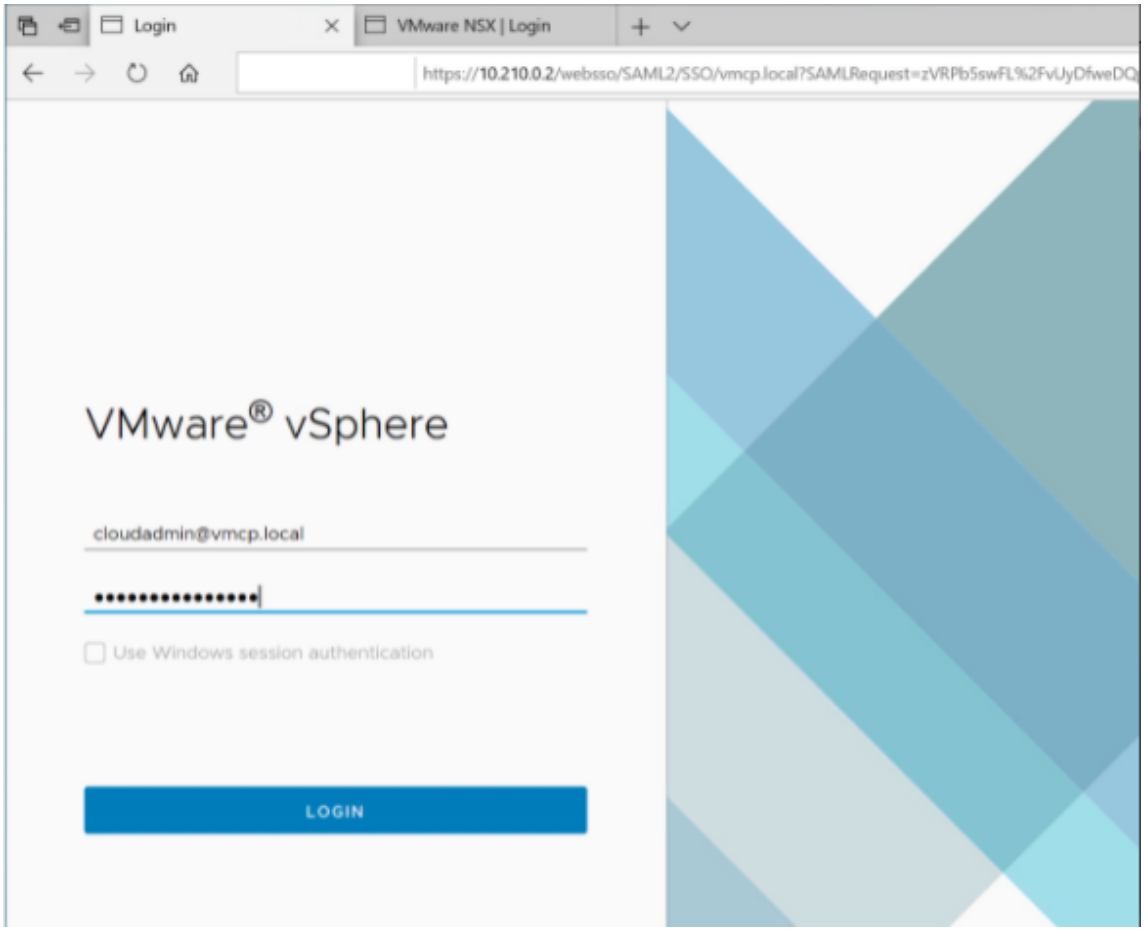
AVS プライベートクラウドへのアクセス　プライベートクラウドを作成したら、Windows VM を作成し、プライベートクラウドのローカル vCenter に接続します。

新しい **Windows** 仮想マシンの作成

1. ［リソースグループ］で、［**+ Add**］を選択してから、「**Microsoft Windows 10/11**」または「**Windows Server 2016/2019**」を検索して選択します。
2. 必要な情報を入力してから、［**Review + Create**］を選択します。
3. 検証に合格したら、［**Create**］を選択して仮想マシン作成プロセスを開始します。

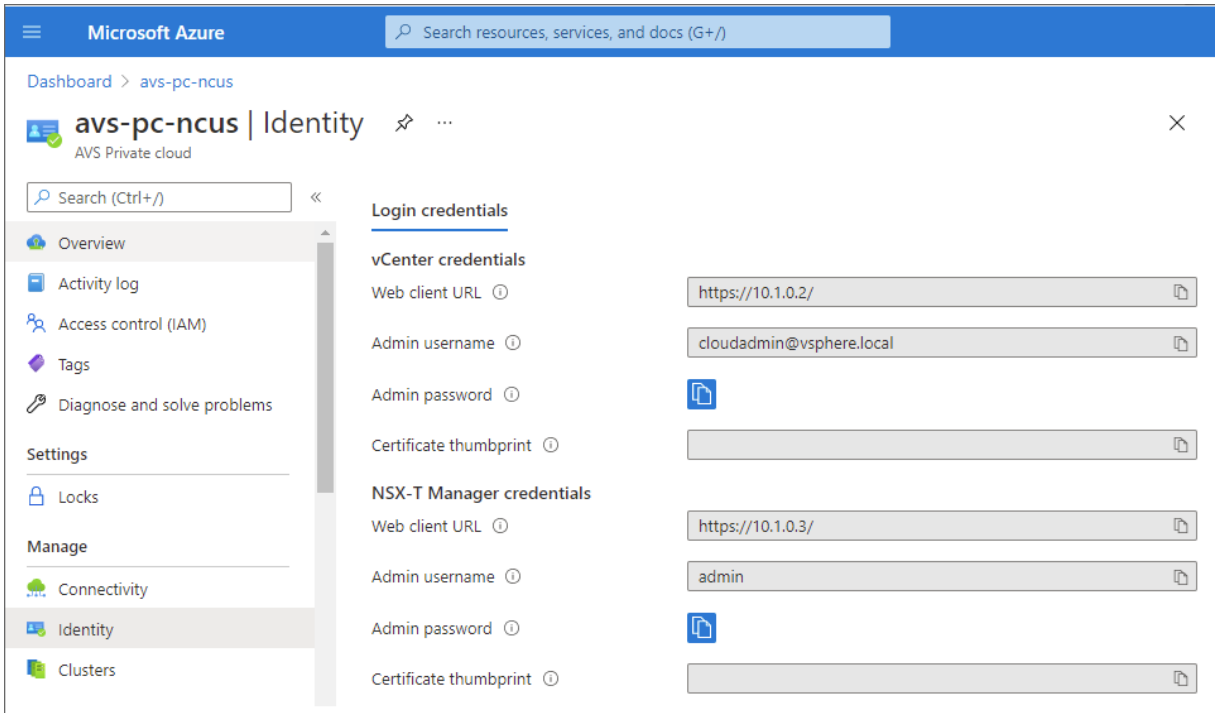
プライベートクラウドのローカル **vCenter** への接続

1. クラウド管理者として **vSphere Client with VMware vCenter SSO** にサインインします。



2. Azure Portal で、プライベートクラウドを選択してから、［**Manage**］**>**［**Identity**］を選択します。

プライベートクラウドの vCenter と NSX-T Manager について、URL、およびユーザーの資格情報が表示されます:



Display private cloud vCenter and NSX Manager URLs and credentials.

URL およびユーザーの資格情報を確認した後、次のことを行います:

1. 前の手順で作成した VM に移動し、その仮想マシンに接続します。
2. Windows VM で、ブラウザーを開き、2 つのブラウザータブで vCenter および NSX-T Manager の URL に移動します。[vCenter] タブで、前の手順のユーザー資格情報「*cloudadmin@vmcp.local*」を入力します。

Azure での **VMware** プライベートクラウドのネットワークの構成　ASV プライベートクラウドにアクセスした後、仮想ネットワークとゲートウェイを作成することでネットワークを構成します。

仮想ネットワークの作成

1. Azure Portal にサインインします。
2. 以前に作成したリソースグループに移動します。
3. [**+ Add**] を選択して新しいリソースを定義します。
4. [**Search the Marketplace**] ボックスに「*virtual network*」と入力します。仮想ネットワークリソースを見つけて選択します。
5. [**Virtual Network**] ページで、[**Create**] を選択してプライベートクラウドの仮想ネットワークをセットアップします。
6. [**Create Virtual Network**] ページで、仮想ネットワークの詳細を入力します。
7. [**Basics**] タブで、仮想ネットワークの名前を入力し、適切なリージョンを選択して、[**Next : IP Addresses**] をクリックします。
8. [**IP Addresses**] タブで、IPv4 アドレススペースの下に、以前に作成したアドレスを入力します。

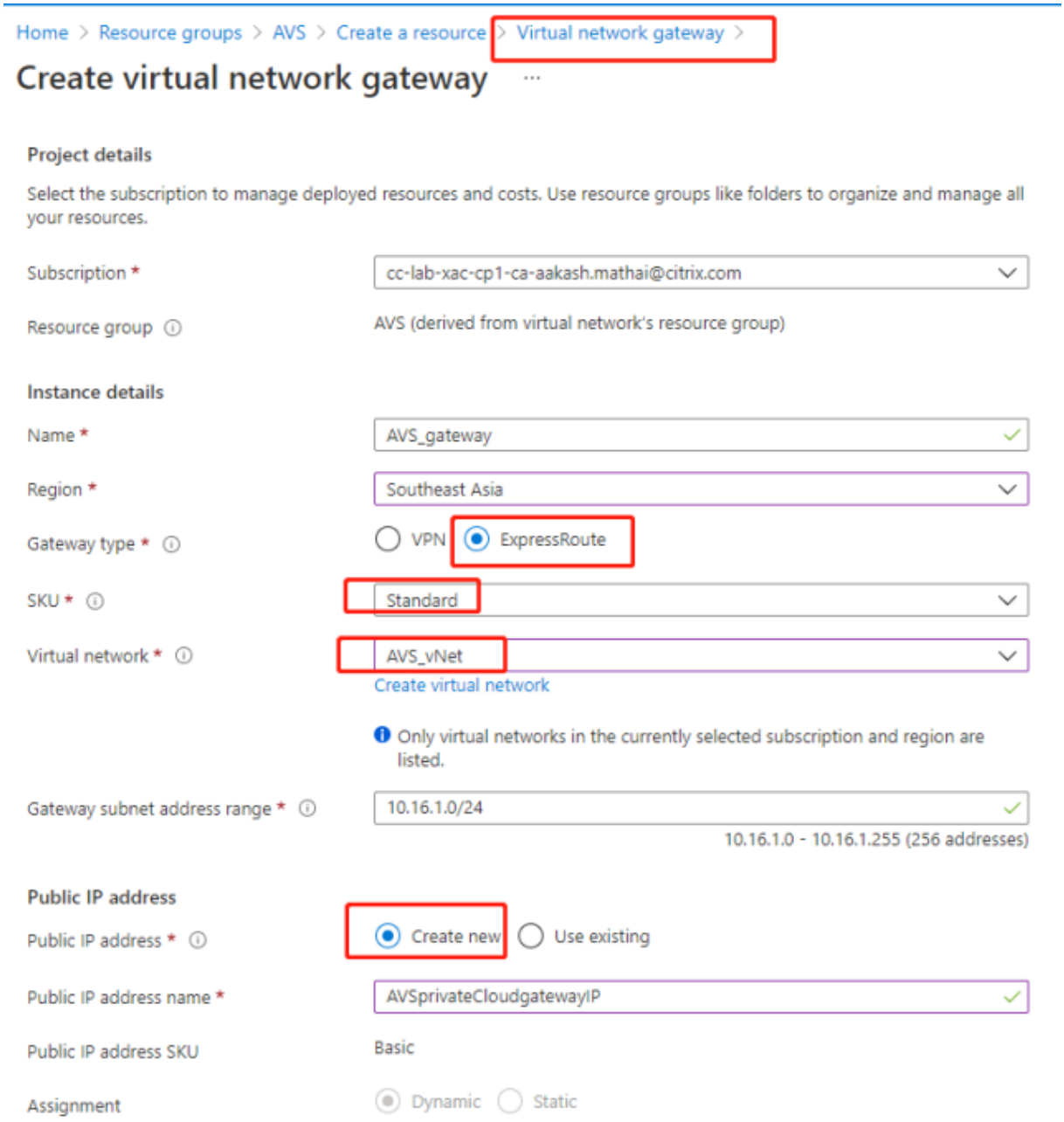
> 重要:
>
> プライベートクラウドの作成時に使用したアドレススペースと重複しないアドレスを使用してください。

アドレススペースに入った後、次のことを行います:

1. [**+ Add subnet**] を選択します。
2. [**Add subnet**] ページで、サブネットに名前と適切なアドレス範囲を指定します。
3. [**Add**] をクリックします。
4. [**Review + create**] を選択します。
5. 情報を確認し、[**Create**] をクリックします。展開が完了すると、仮想ネットワークがリソースグループに表示されます。

仮想ネットワークゲートウェイの作成　仮想ネットワークを作成したら、仮想ネットワークゲートウェイを作成します。

1. リソースグループで、[**+ Add**] を選択して新しいリソースを追加します。
2. [**Search the Marketplace**] ボックスに 「*virtual network gateway*」と入力します。仮想ネットワークリソースを見つけて選択します。
3. [**Virtual Network gateway**] ページで、[**Create**] をクリックします。
4. [**Create virtual network gateway**] ページの [**Basics**] タブで、フィールドに値を入力します。
5. [**Review + create**] をクリックします。

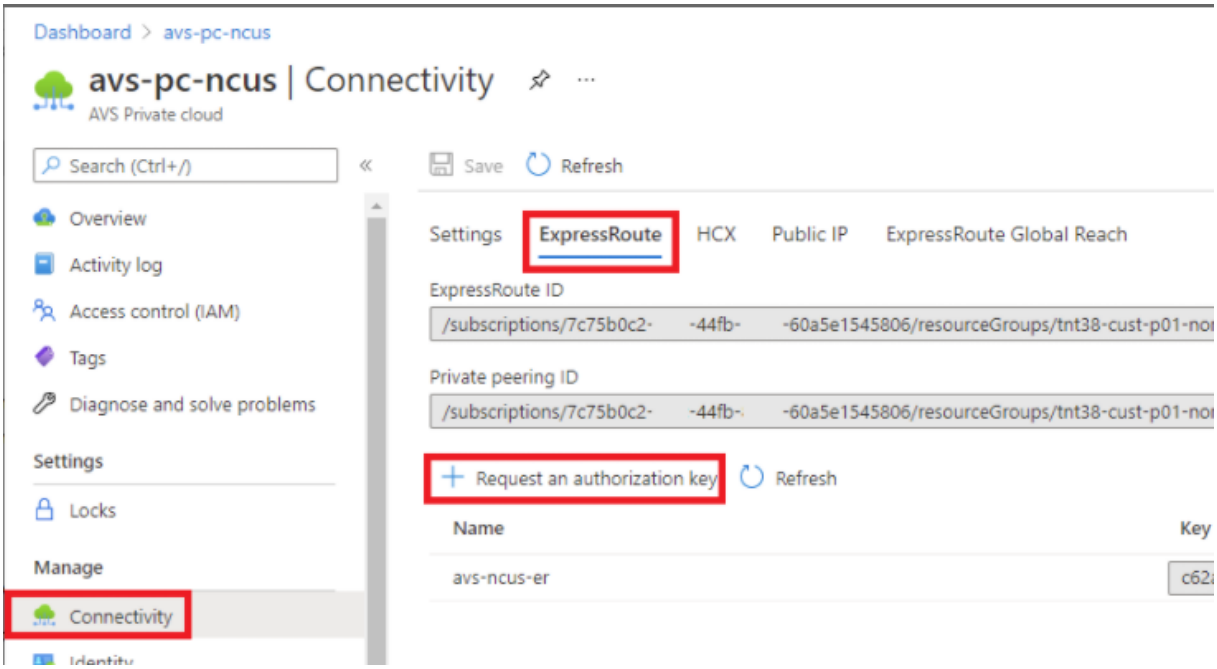


仮想ネットワークゲートウェイの構成を確認したら、[**Create**]をクリックして仮想ネットワークゲートウェイを展開します。
展開が完了したら、**ExpressRoute** を、Azure AVS プライベートクラウドを含む仮想ネットワークゲートウェイに接続します。

仮想ネットワークゲートウェイへの **ExpressRoute** の接続　仮想ネットワークゲートウェイを展開した後、仮想ネットワークゲートウェイと Azure AVS プライベートクラウドの間の接続を追加します:

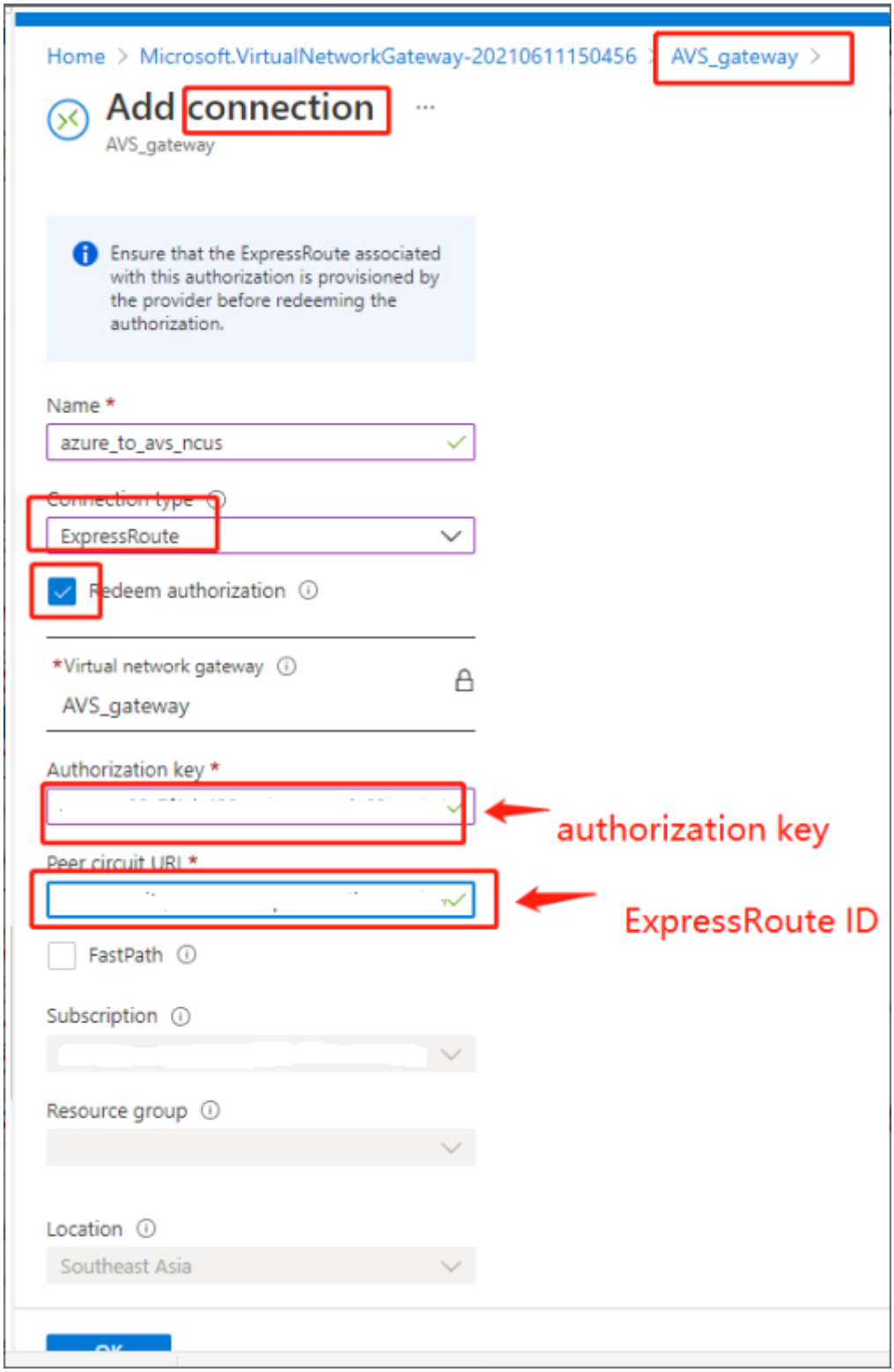
1. ExpressRoute 承認キーを要求します。

2. Azure Portal で、**Azure VMware Solution** プライベートクラウドに移動します。[**Manage**] > [**Connectivity**] > [**ExpressRoute**] を選択してから、[**+ Request an authorization key**] を選択します。

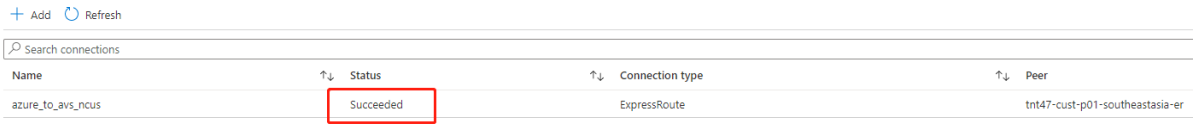


承認キーを要求した後、次のことを行います:

1. キーの名前を入力し、[**Create**] をクリックします。キーの作成には約 30 秒かかる場合があります。作成されると、新しいキーがプライベートクラウドの承認キーの一覧に表示されます。
2. その承認キーと **ExpressRoute ID** をコピーします。ピアリングプロセスを完了するためにそれらが必要になります。表示された承認キーはしばらくすると消えるので、表示されたらコピーします。
3. 使用する予定の仮想ネットワークゲートウェイに移動し、[**Connections> + Add**] を選択します。
4. [**Add connection**] ページで、フィールドに値を入力し、[**OK**] を選択します。



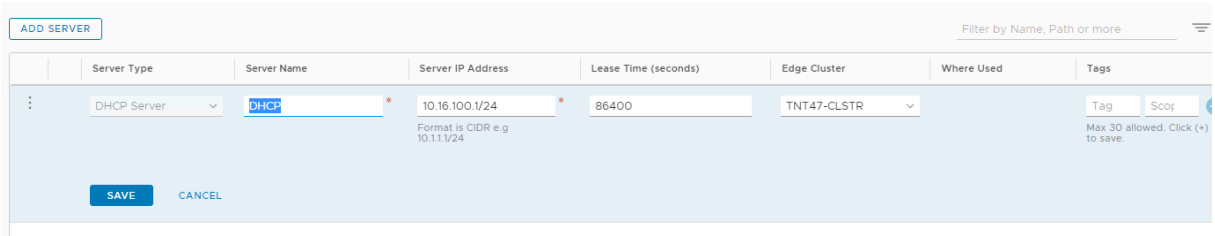
ExpressRoute 回線と仮想ネットワークの間に接続が確立されます:



Azure VMware Solution の **DHCP** の構成　ExpressRoute を仮想ゲートウェイに接続した後、DHCP を構成します。

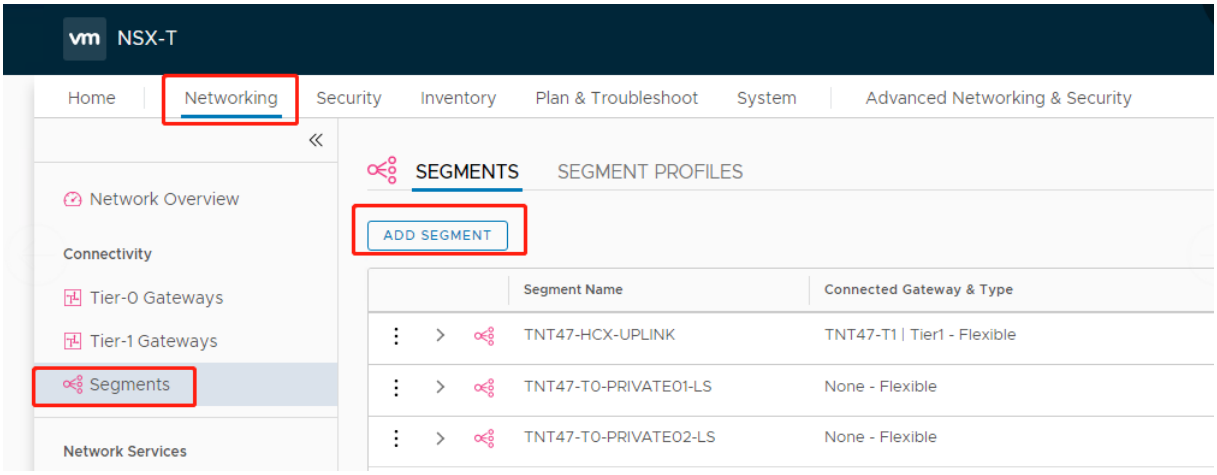
NSX-T の使用による **DHCP** サーバーのホスト　NSX-T Manager で、次のことを行います:

1. [**Networking**] > [**DHCP**] を選択してから、[**Add Server**] を選択します。
2. [**Server Type**] として [**DHCP**] を選択し、サーバー名と IP アドレスを入力します。
3. [保存] をクリックします。
4. [**Tier 1 Gateways**] を選択し、Tier-1 ゲートウェイの縦の省略記号を選択してから、[**Edit**] を選択します。
5. [**No IP Allocation Set**] を選択してサブネットを追加します。
6. [**Type**] として [**DHCP Local Server**] を選択します。
7. [**DHCP Server**] で、[**Default DHCP**] を選択してから、[**Save**] をクリックします。
8. もう一度 [**Save**] をクリックしてから、[**Close Editing**] を選択します。



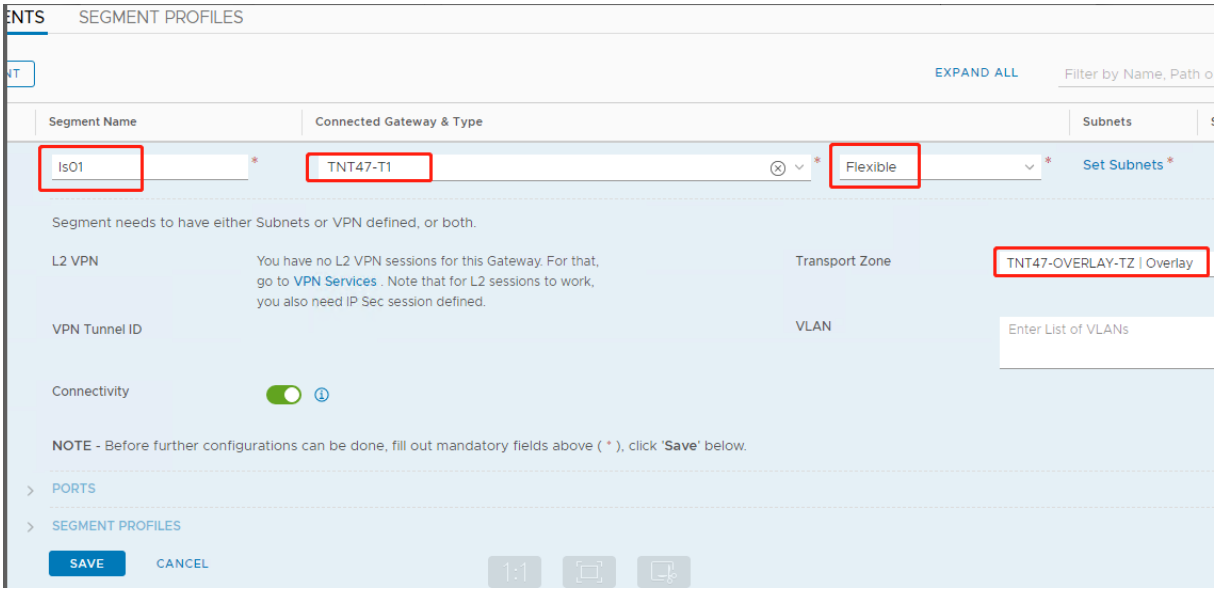
Azure VMware Solution でのネットワークセグメントの追加　DHCP をセットアップした後、ネットワークセグメントを追加します。

ネットワークセグメントを追加するには、NSX-T Manager で、[**Networking**] > [**Segments**] を選択してから [**Add Segment**] をクリックします。



[**Segments profile**] 画面で、次のことを行います:

1. [セグメント名] にセグメント名を入力します。
2. [**Connected Gateway**] として [**Tier-1 Gateway (TNTxx-T1)**] を選択し、[**Type**] を [**Flexible**] のままにします。
3. 事前設定されたオーバーレイ [**Transport Zone(TNTxx-OVERLAY-TZ)**] を選択します。
4. [**Set Subnets**] をクリックします。



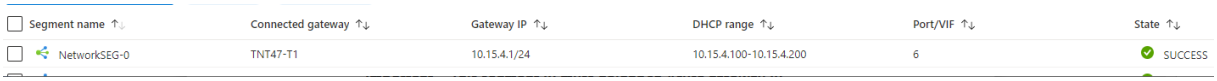
[**Azure ASV**] セクションで、次のことを行います:

1. ゲートウェイの IP アドレスを入力します。
2. [**Add**] を選択します。

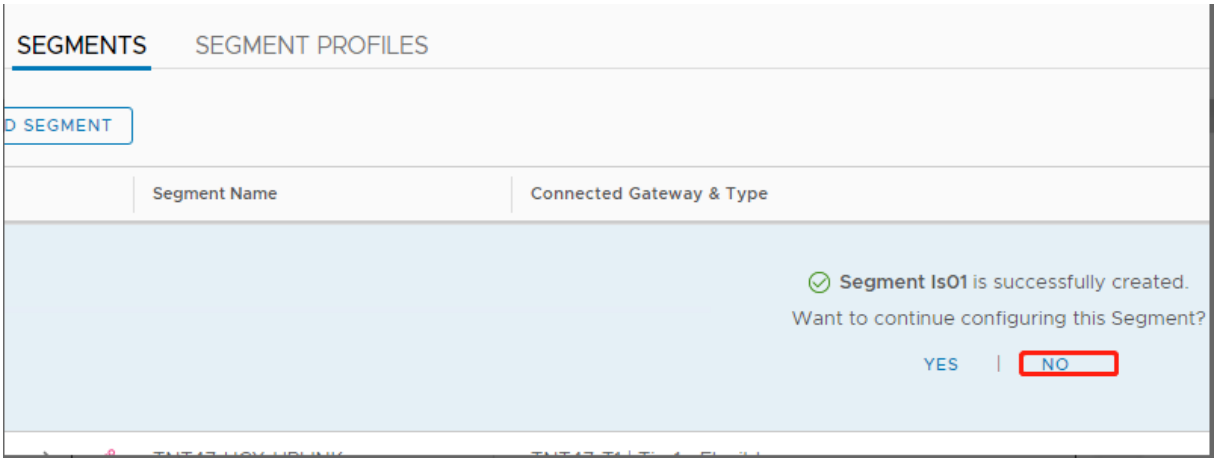
> 重要:
>
> このセグメント IP アドレスは、Azure ゲートウェイの IP アドレス（10.15.0.0/22）に属している必要があり

> ます。

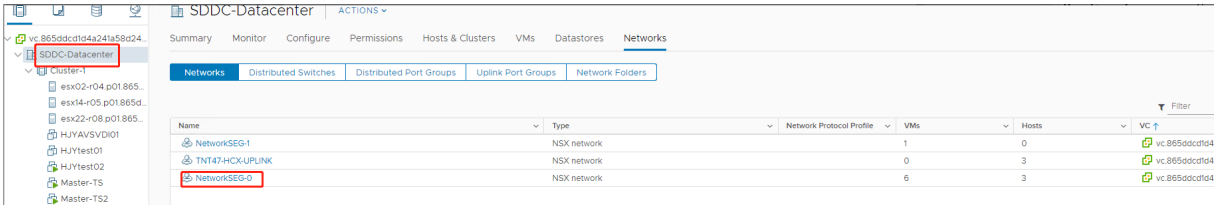
DHCP 範囲はセグメント IP アドレスに属している必要があります:



[**No**] を選択して、セグメントの構成を続行するオプションを拒否します:



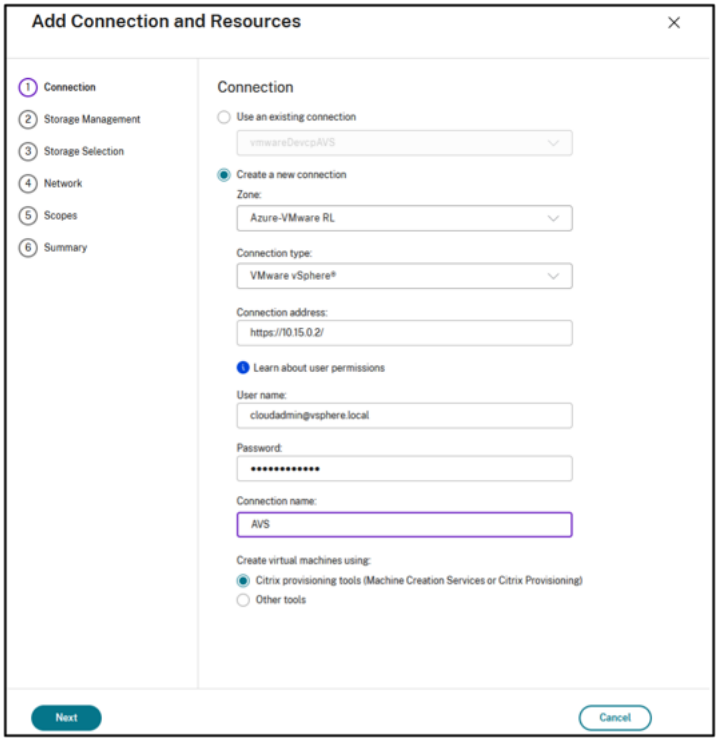
vCenter で、[**Networking**] > [**SDDC-Datacenter**] を選択します:



AVS 環境の確認　AVS プライベートクラウドのリソースの場所を設定し、クラウドコネクタのペアをインストールします。

Citrix Studio での **AVS** 接続の作成

1. vCenter でマシンを作成し、そのマシンに Cloud Connector のペアをインストールします。「インスタンスを構成する」を参照してください。
2. [管理] > [完全な構成] の左側ペインで [ホスト] を選択します。
3. ホスティングノードを選択し、[接続およびリソースの追加] をクリックします。
4. [接続] 画面で [新しい接続を作成する] を選択し、次のことを行います:



a) ［接続の種類］で ［**VMware vSphere**］を選択します。
b) ［接続アドレス］に、vCenter プライベート IP アドレスを入力します。
c) vCenter の資格情報を入力します。
d) 接続名を入力します。
e) 仮想マシンを作成するツールを選択します。

5. ［ネットワーク］画面で、NSX-T サーバーで作成したサブネットを選択します。
6. ウィザードを完了します。

Google Cloud VMware Engine

Citrix DaaS を使用して、VMware ベースのオンプレミスの Citrix ワークロードを Google Cloud VMware Engine に移行できます。

Google Cloud VMware Engine の構成

次の手順では、Google Cloud VMware Engine でクラスターを取得して設定する方法について説明します。

VMware Engine ポータルへのアクセス

1. **Google Cloud** コンソールで、ナビゲーションメニューをクリックします。

2. [**Compute**] セクションで、[**VMware Engine**] をクリックして、新しいブラウザータブで VMware Engine を開きます。

最初のプライベートクラウドを作成するための要件　Google Cloud VMware Engine、使用可能な VMware Engine ノードクォータ、および適切な IAM 役割にアクセスできる必要があります。プライベートクラウドの作成を続行する前に、次の要件を満たすようにセットアップを行ってください:

1. API アクセス権とノードクォータを要求します。詳しくは、「API のアクセス権と割り当てのリクエスト」を参照してください。
2. VMware 管理アプライアンスと HCX 展開ネットワークに使用するアドレス範囲に注意してください。詳しくは、「ネットワーキングの要件」を参照してください。

   > 注:
   >
   > HCX の展開は、IP Plan バージョン 1.0 にのみ適用できます。

3. VMware Engine Service Admin IAM 役割を取得します。

最初のプライベートクラウドの作成

1. VMware Engine ポータルにアクセスします。
2. VMware Engine のホームページで、[**Create a private cloud**] をクリックします。ホスティングの場所とハードウェアノードの種類が一覧表示されます。
3. プライベートクラウドのノード数を選択します。少なくとも 3 つのノードが必要です。
4. VMware 管理ネットワークのクラスレスドメイン間ルーティング（CIDR）範囲を入力します。
5. HCX 展開ネットワークの CIDR 範囲を入力します。

   > 重要:
   >
   > - CIDR 範囲は、オンプレミスのサブネットまたはクラウドのサブネットと重複してはいけません。CIDR 範囲は、「/27」以上である必要があります。
   > - HCX の展開は、IP Plan バージョン 1.0 にのみ適用できます。

6. [**Review and create**] を選択します。
7. 設定を確認します。設定を変更するには、[**Back**] をクリックします。
8. [**Create**] をクリックして、プライベートクラウドの作成を開始します。

VMware Engine は、新しいプライベートクラウドを作成するときに、いくつかの VMware コンポーネントを展開し、プライベートクラウド内のクラスターの初期の Autoscale ポリシーを設定します。プライベートクラウドの作成には、30 分～2 時間かかることがあります。プロビジョニングが完了すると、メールが届きます。

Google Cloud VMware Engine VPN Gateway のセットアップ　Google Cloud VMware Engine への初期接続を確立するために、VPN ゲートウェイを使用できます。これは OpenVPN ベースのクライアント VPN であり、これを使用して VMware Software Defined Data Center（SDDC）vCenter に接続し、必要な初期の構成を行うことができます。

VPN ゲートウェイを展開する前に、SDDC が展開されているリージョンの［**Edge Services**］範囲を構成します。これを行うには、以下の手順に従います：

1. **Google Cloud VMware Engine** ポータルにログオンし、［**Network**］**>**［**Regional Settings**］に移動します。［**Add Region**］をクリックします。
2. SDDC が展開されているリージョンを選択し、［**Internet Access**］と［**Public IP Service**］を有効にします。
3. 計画時にメモした［Edge Services］範囲を指定し、［**Submit**］をクリックします。これらのサービスを有効にするには、10〜15 分かかります。

   完了すると、［Regional Settings］ページの［Edge Services］が［**Enabled**］として表示されます。これらの設定を有効にすると、パブリック IP アドレスを SDDC に割り当てることができます。これは、VPN ゲートウェイを展開するための要件です。

VPN ゲートウェイの展開

1. **Google Cloud VMware Engine** ポータルで、［**Network**］**>**［**VPN Gateways**］に移動します。［**Create New VPN Gateway**］をクリックします。
2. 計画時に用意した VPN ゲートウェイとクライアントサブネットの名前を指定します。VPN の場所はプライベートクラウドのリージョンと同じである必要があります。［次へ］をクリックします。
3. VPN アクセスを許可するユーザーを選択します。［次へ］をクリックします。
4. VPN 経由でアクセスが必要なネットワークを指定します。［次へ］をクリックします。
5. 概要画面が表示されます。選択内容を確認し、［**Submit**］をクリックして VPN ゲートウェイを作成します。［VPN Gateways］ページが表示され、新しい VPN ゲートウェイのステータスが［**Creating**］として表示されます。
6. ステータスが［**Operational**］に変わったら、その新しい VPN ゲートウェイをクリックします。
7. ［**Download my VPN configuration**］をクリックして、VPN ゲートウェイ用に事前構成した OpenVPN プロファイルを含む ZIP ファイルをダウンロードします。UDP/1194 と TCP/443 を使用した接続のプロファイルを使用できます。基本設定を選択して、その設定を Open VPN にインポートし、接続します。
8. ［**Resources**］に移動し、SDDC を選択します。

VPN の接続

1. VPN ゲートウェイのセットアップを通じて、オンプレミスネットワークとプライベートクラウドの間にポイント対サイト接続を確立します。詳しくは、Google Cloud VMware Engine VPN Gateway のセットアップを参照してください。

2. 「Google Cloud VMware Engine VPN Gateway のセットアップ」でダウンロードした VPN 構成をアップロードします。
3. その VPN 構成を OpenVPN Connect などの VPN クライアントにインポートします。

詳しくは、VPN を使用した接続を参照してください。

最初のサブネットの作成

VMware Engine ポータルからの **NSX-T Manager** へのアクセス　サブネットを作成するプロセスは、VMware Engine を介してアクセスする NSX-T で行います。NSX-T Manager にアクセスするには、次の手順を実行します。

1. [**Google Cloud VMware Engine**] ポータルにログオンします。
2. メインナビゲーションから、[**Resources**] に移動します。
3. サブネットを作成するプライベートクラウドに対応するプライベートクラウド名をクリックします。
4. プライベートクラウドの詳細ページで、[**vSphere Management Network**] タブをクリックします。
5. NSX-T Manager に対応する **FQDN** をクリックします。
6. プロンプトが表示されたら、サインイン資格情報を入力します。vIDM を設定し、それを Active Directory などの ID ソースに接続している場合は、代わりに ID ソースの資格情報を使用してください。

> 注意：
>
> 生成された資格情報は、プライベートクラウドの詳細ページから取得できます。

サブネットの **DHCP** サービスのセットアップ　サブネットを作成する前に、DHCP サービスをセットアップします：

NSX-T Manager で、次のことを行います：

1. [**Networking**] **>** [**DHCP**] に移動します。ネットワークダッシュボードでは、1 つの Tier-0 ゲートウェイと、1 つの Tier-1 ゲートウェイが DHCP サービスによって作成されることが示されます。
2. DHCP サーバーのプロビジョニングを開始するには、[**Add Server**] をクリックします。
3. [**Server Type**] として [**DHCP**] を選択し、サーバー名と IP アドレスを入力します。
4. [**Save**] をクリックして、DHCP サービスを作成します。

この DHCP サービスを、関連する Tier-1 ゲートウェイに接続するには、次のことを行います：デフォルトの Tier-1 ゲートウェイは、DHCP サービスによって既にプロビジョニングされています：

1. [**Tier 1 Gateways**] を選択し、Tier-1 ゲートウェイの縦の省略記号を選択してから、[**Edit**] を選択します。
2. [**IP Address Management**] フィールドで、[**No IP Allocation Set**] を選択します。
3. [**Type**] として [**DHCP Local Server**] を選択します。

4. ［**DHCP Server**］用に作成した DHCP サーバーを選択します。
5. ［保存］をクリックします。
6. ［**Close Editing**］をクリックします。

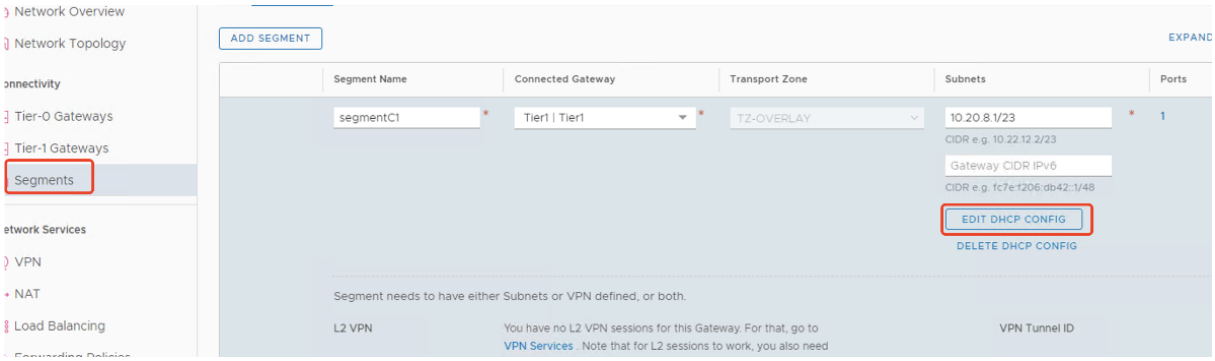
これで、NSX-T でネットワークセグメントを作成できます。NSX-T の DHCP について詳しくは、DHCP に関する VMware のドキュメントを参照してください。

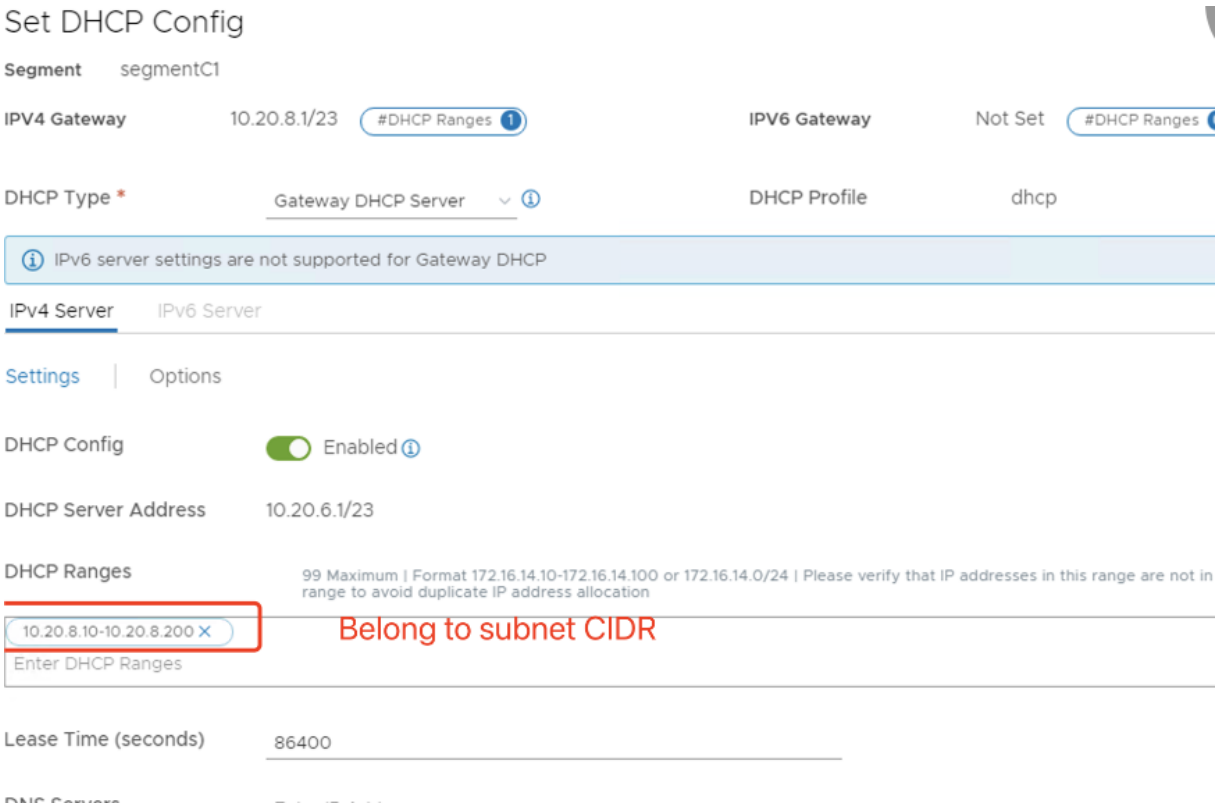
NSX-T でのネットワークセグメントの作成　ワークロード VM の場合、プライベートクラウドの NSX-T ネットワークセグメントとしてサブネットを作成します：

1. NSX-T Manager で、［**Networking**］**>**［**Segments**］に移動します。
2. ［**Add Segment**］をクリックします。
3. ［セグメント名］にセグメント名を入力します。
4. ［**Connected Gateway**］として ［**Tier-1**］を選択し、［Type］を ［**Flexible**］のままにします。
5. ［**Set Subnets**］をクリックします。
6. ［**Add Subnets**］をクリックします。
7. ［**Gateway IP/Prefix Length**］にサブネット範囲を入力します。最後のオクテットとして「**.1**」を付けて、サブネット範囲を指定します。例：**10.12.2.1/24**。
8. DHCP 範囲を指定し、［**ADD**］をクリックします。
9. ［**Transport Zone**］のドロップダウンリストで ［**TZ-OVERLAY**］を選択します。
10. ［保存］をクリックします。VM を作成する際、vCenter でこのネットワークセグメントを選択できるようになりました。

特定のリージョンでは、プライベートサービスアクセス権を使用して、VMware Engine から VPC ネットワークに一意のルートを最大 100 個設定できます。これには、たとえば、プライベートクラウド管理の IP アドレス範囲、NSX-T ワークロードネットワークセグメント、および HCX ネットワーク IP アドレス範囲が含まれます。この制限には、リージョン内のすべてのプライベートクラウドが含まれます。

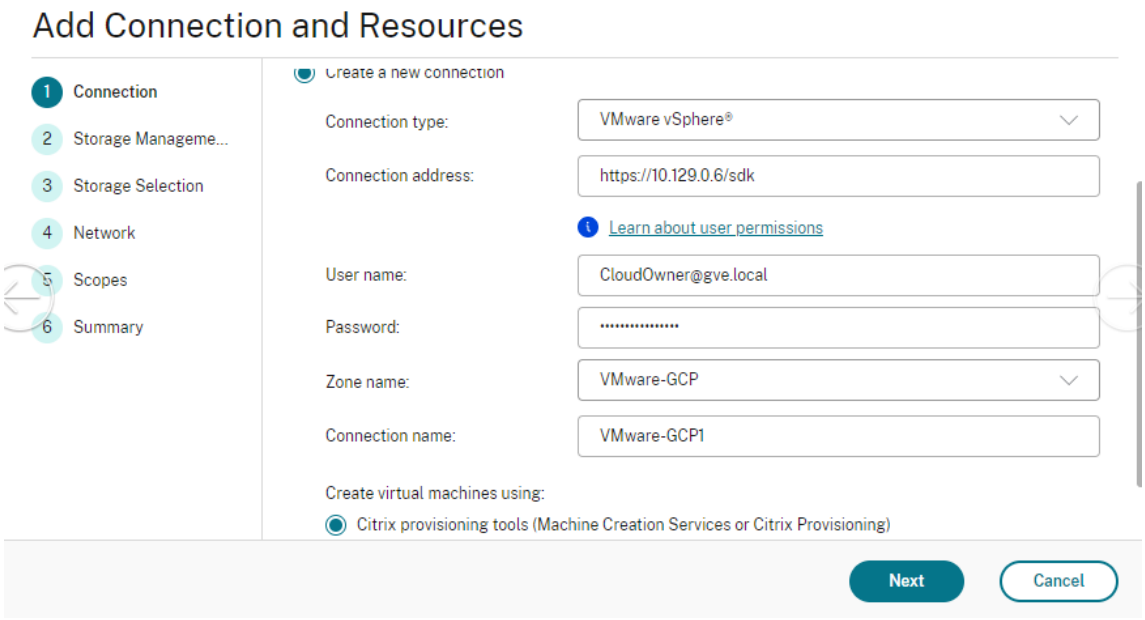
> 注：
>
> DHCP 範囲設定を数回構成する必要があることによる、Google Cloud の構成の問題があります。そのため、必ず Google Cloud を構成した後に DHCP 範囲を構成してください。［**EDIT DHCP CONFIG**］をクリックして、DHCP 範囲を構成します。





Citrix Studio での **Google Cloud VMware** 接続の作成

1. vCenter でマシンを作成し、そのマシンに Cloud Connector のペアをインストールします。「インスタンスを構成する」を参照してください。
2. Citrix Studio を起動します。
3. ホスティングノードを選択し、［接続およびリソースの追加］をクリックします。
4. ［接続］画面で ［新しい接続を作成する］を選択し、次のことを行います:



a) ［接続の種類］で ［**VMware vSphere**］を選択します。
b) ［接続アドレス］に、vCenter プライベート IP アドレスを入力します。
c) vCenter の資格情報を入力します。
d) 接続名を入力します。
e) 仮想マシンを作成するツールを選択します。

5. ［ネットワーク］画面で、NSX-T サーバーで作成したサブネットを選択します。
6. ウィザードを完了します。

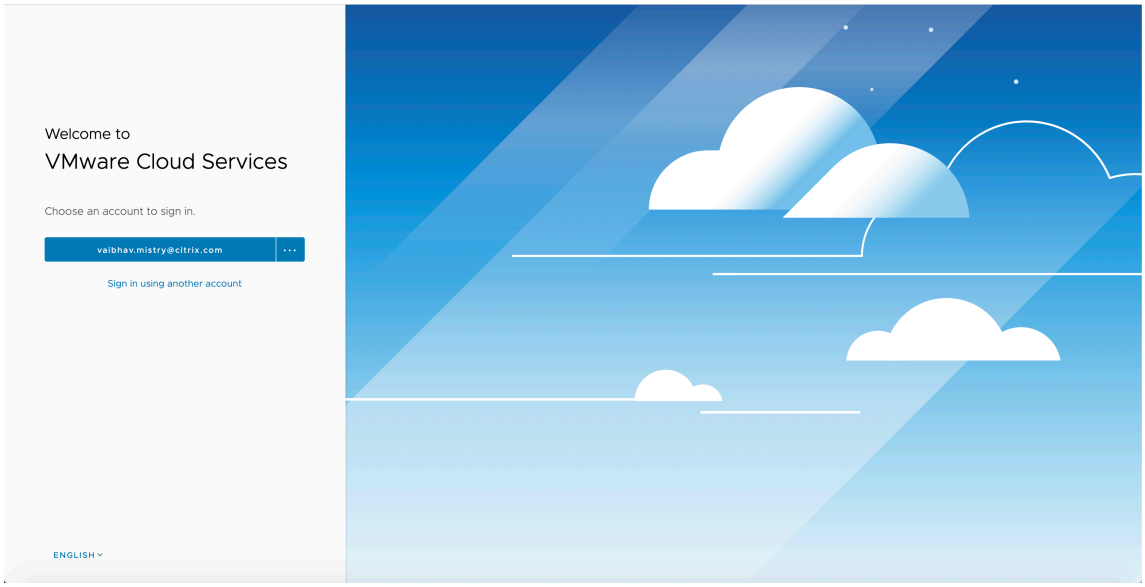
VMware Cloud on AWS（Amazon Web Services）

VMware Cloud on AWS（Amazon Web Services）を使用すると、VMware ベースのオンプレミスの Citrix ワークロードを AWS Cloud に移行し、核となる Citrix Virtual Apps and Desktops 環境を Citrix DaaS に移行できます。

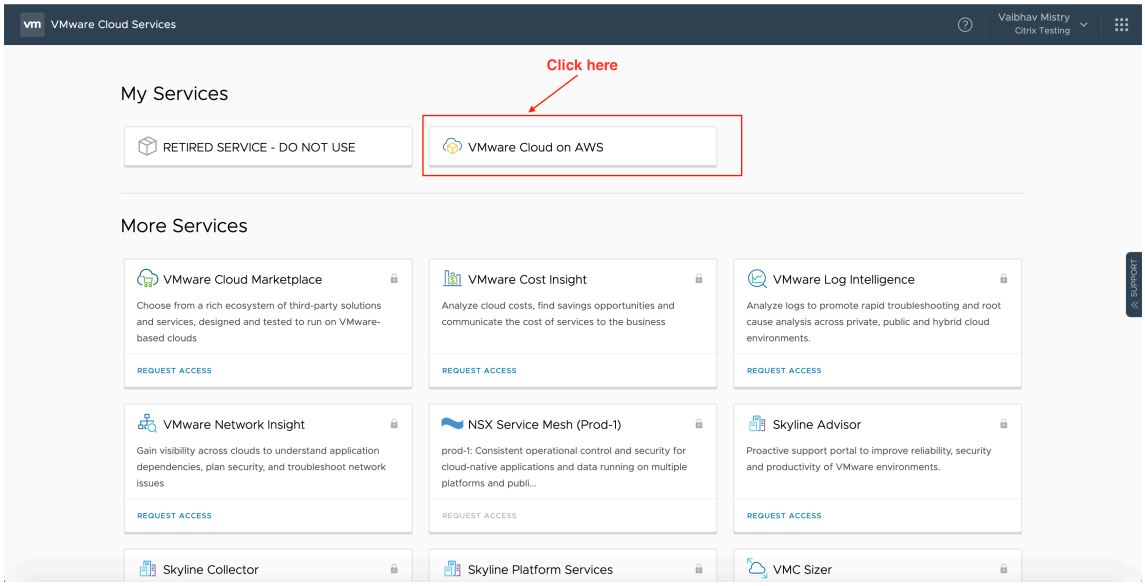
この記事では、VMware Cloud on AWS をセットアップする手順について説明します。

VMware クラウド環境へのアクセス

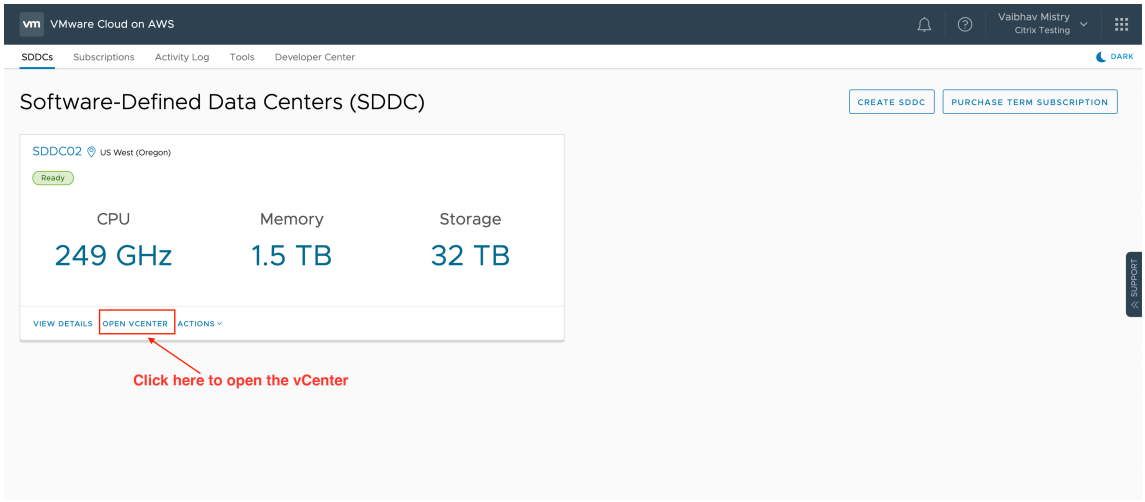
1. URL「https://console.cloud.vmware.com/」を使用して、VMware Cloud サービスにログインします。

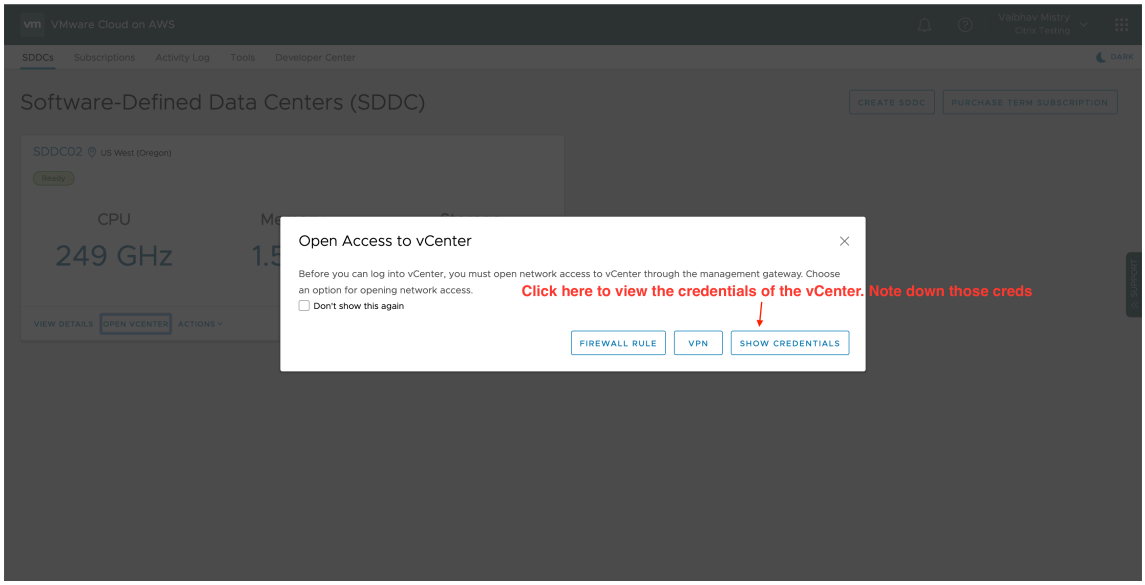


2. [**VMware Cloud on AWS**] をクリックします。ソフトウェア定義データセンター（SDDC：Software-Defined Data Centers）ページが表示されます。

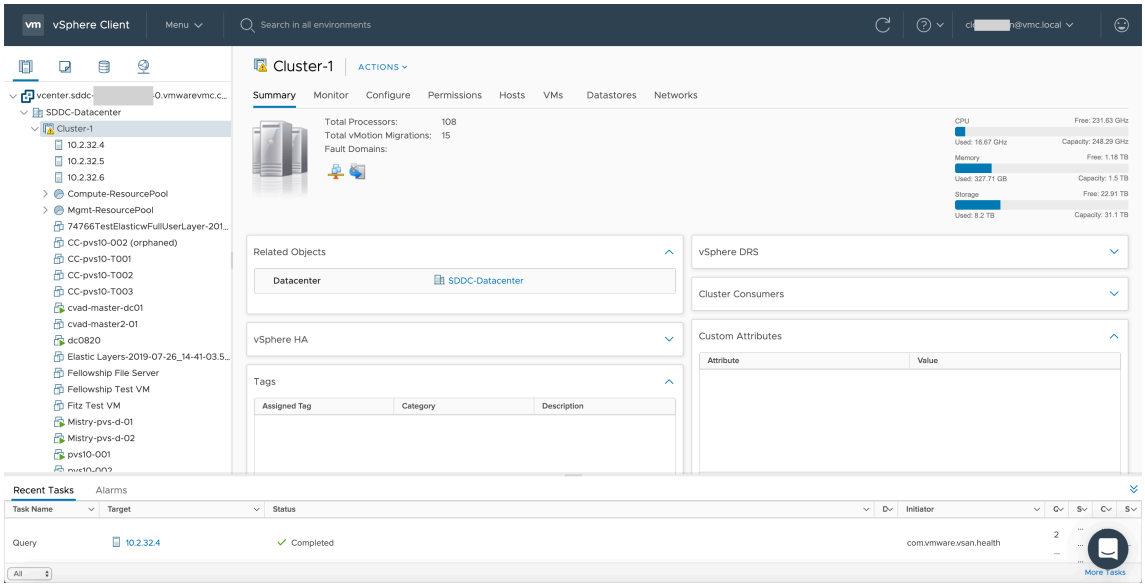


3. [**OPEN VCENTER**] をクリックしてから、[**SHOW CREDENTIALS**] をクリックします。後で使用するために資格情報をメモしておきます。





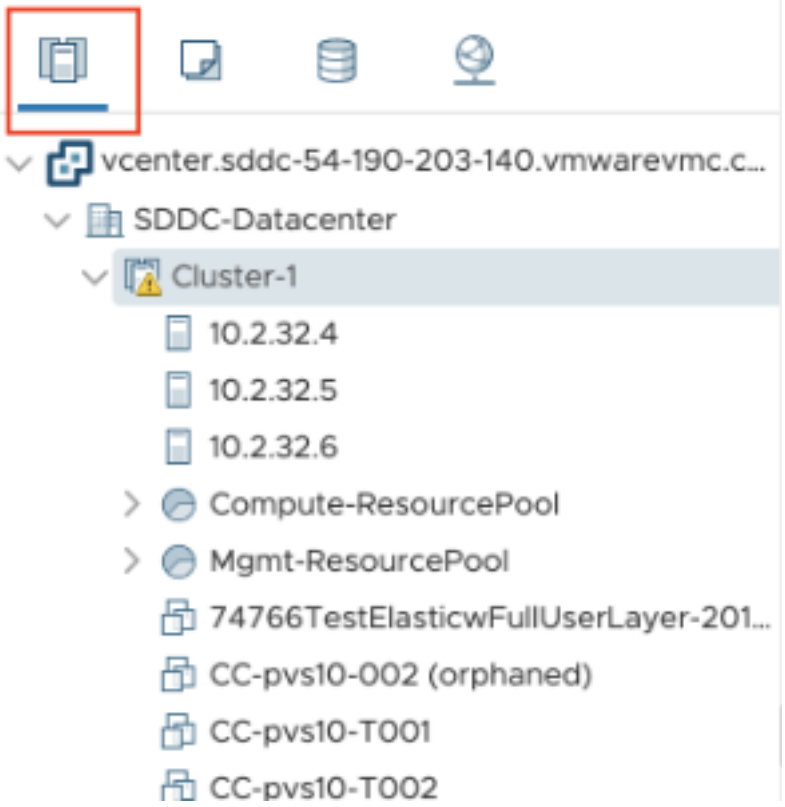
4. Web ブラウザーを開き、vSphere Web Client の URL を入力します。
5. メモした資格情報を入力し、［**Login**］をクリックします。vSphere クライアントの Web ページは、オンプレミス環境に似ています。



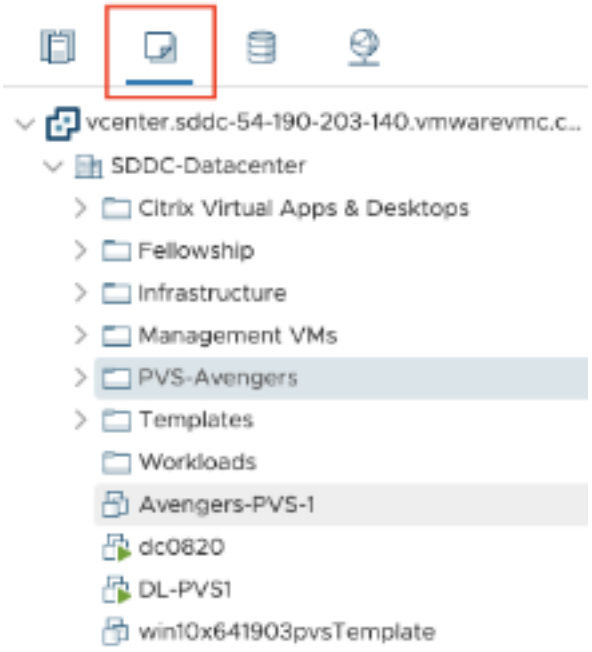
VMware クラウド環境について

vSphere クライアントの Web ページには 4 つのビューがあります。

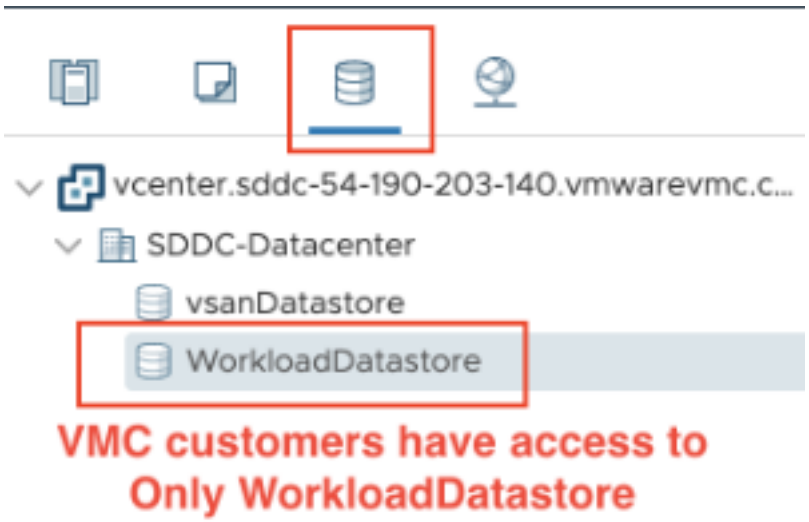
- Host and Cluster ビュー：新しい Cluster を作成することはできませんが、クラウド管理者は複数のリソースプールを作成できます。



- VM and Template ビュー：クラウド管理者は多くのフォルダーを作成できます。



- Storage ビュー：Citrix Studio にホスティングユニットを追加する場合は、Workload Datastore にしかアクセスできないため、**WorkloadDatastore** ストレージを選択します。



- Network ビュー：VMware Cloud ネットワークと不透明ネットワークでアイコンが異なります。

クラスターをセットアップした後、接続とリソースの追加については、「VMware 仮想化環境」を参照してください。

次の手順

- 単純な概念実証環境を展開する場合、ユーザーにアプリまたはデスクトップを配信するように指定されたマシンへの［VDA のインストール］を実行します。

- 接続の作成と管理については、「VMware クラウドおよびパートナーソリューションへの接続」を参照してください。
- インストールと構成プロセスの手順をすべて確認します。

追加情報

- 接続とリソースの作成と管理
- マシンカタログの作成

XenServer 仮想化環境

January 25, 2024

XenServer は運用管理を簡素化し、集中的なワークロードに対して高品位なユーザーエクスペリエンスを保証します。

XenServer の設定方法については、「リソースの種類を追加するか、Citrix Cloud で未使用のドメインをアクティブ化する」を参照してください。

次の手順

- 単純な概念実証環境を展開する場合、ユーザーにアプリまたはデスクトップを配信するように指定されたマシンへの ［VDA のインストール］ を実行します。
- 接続の作成と管理については、「XenServer への接続」を参照してください。
- インストールと構成プロセスの手順をすべて確認します。

追加情報

- 接続とリソースの作成と管理
- マシンカタログの作成

Cloud Connector のサイズおよびスケールの考慮事項

January 25, 2024

Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）のサイジングとスケーラビリティを評価する場合、すべてのコンポーネントを考慮する必要があります。特定の要件に応じて、Citrix Cloud Connector と

StoreFront の構成を調査し、テストします。サイジングとスケーラビリティのためのリソースが不十分だと、お使いの環境のパフォーマンスに悪影響を及ぼします。

> 注:
>
> - これらの推奨事項は、Citrix DaaS およびCitrix DaaS Standard for Azureに適用されます。
> - この記事に記載されているテストと推奨事項は、テストを実行するためのガイドラインです。正しいコネクタのサイズを確認するため、ご使用の環境でテストを実行することをお勧めします。

この記事では、テスト済みの最大容量の詳細と、Cloud Connector のマシン構成に関するベストプラクティスの推奨事項について説明します。テストは、StoreFront およびローカルホストキャッシュ（LHC）が構成された環境で実施されました。

説明内容は、各リソースの場所に VDI ワークロードまたは RDS ワークロードのいずれかが含まれる環境に適用されます。VDI ワークロードと RDS ワークロードが一緒に含まれるリソースの場所については、Citrix コンサルティングサービスにお問い合わせください。

Cloud Connector は、次の方法でワークロードを Citrix DaaS にリンクします:

- VDA と Citrix DaaS 間の通信用プロキシの提供
- Citrix DaaS とお使いの Active Directory（AD）およびハイパーバイザー間の通信用プロキシの提供
- StoreFront サーバーを含む環境では、Cloud Connector は、クラウドの停止時に一時的なセッションブローカーとして機能し、ユーザーにリソースへの継続的なアクセスを提供

特定のニーズを満たすために、Cloud Connector を適切なサイズと構成にすることが重要です。

Cloud Connector の各セットは、リソースの場所（ゾーンとも呼ばれます）に割り当てられます。リソースの場所は、どのリソースがその Cloud Connector のセットと通信するかを指定する論理的な分離です。Active Directory（AD）と通信するには、ドメインごとに少なくとも 1 つのリソースの場所が必要です。

各マシンカタログとホスティング接続は、リソースの場所に割り当てられます。

複数のリソースの場所を使用する環境では、マシンカタログと VDA をリソースの場所に割り当て、停止中に接続を仲介する LHC の機能を最適化します。リソースの場所の作成と管理について詳しくは、「Citrix Cloud への接続」を参照してください。最適なパフォーマンスを得るには、VDA、Active Directory サーバー、およびハイパーバイザーへの低遅延接続で Cloud Connector を構成します。

推奨されるプロセッサとストレージ

今回のテストと同様のパフォーマンスを得るには、SHA 拡張機能に対応している最新のプロセッサを使用してください。SHA 拡張機能により、CPU の暗号化負荷が軽減されます。推奨されるプロセッサは次のとおりです:

- Advanced Micro Devices（AMD）Zen 以降のプロセッサ
- Intel Ice Lake 以降のプロセッサ

推奨されているプロセッサは効率的に実行されます。古いプロセッサを使用することもできますが、CPU 負荷が高くなる可能性があります。そのような動作に対応するため、仮想 CPU の数を増やすことをお勧めします。

この記事で説明されているテストは、AMD EPYC プロセッサおよび Intel Cascade Lake プロセッサを使用して行われました。

Cloud Connector では、クラウドとの通信中に暗号化の負荷が高くなります。SHA 拡張機能対応のプロセッサを使用する Cloud Connector では、CPU の負荷が低くなります。これは、Windows Local Security Authority Subsystem Service（LSASS）による CPU 使用率の低下によって示されています。

特に、LHC を使用する環境では、1 秒あたりの I/O 操作数（IOPS）が十分な最新のストレージを使用することを Citrix ではお勧めします。ソリッドステートドライブ（SSD）が推奨されますが、プレミアムクラウドストレージ階層は必要ありません。Cloud Connector がデータベースの小さなコピーを実行することを想定している LHC の場合は、より高い IOPS が必要です。このデータベースは、サイト構成の変更にともなって定期的に更新され、Citrix Cloud の停止時にリソースの場所に仲介機能を提供します。

推奨されるローカルホストキャッシュのコンピューティング構成

ローカルホストキャッシュ（LCH）は、Cloud Connector が Citrix Cloud と通信できなくなった場合でも、環境での接続仲介操作を続行できることによって、高可用性を提供します。

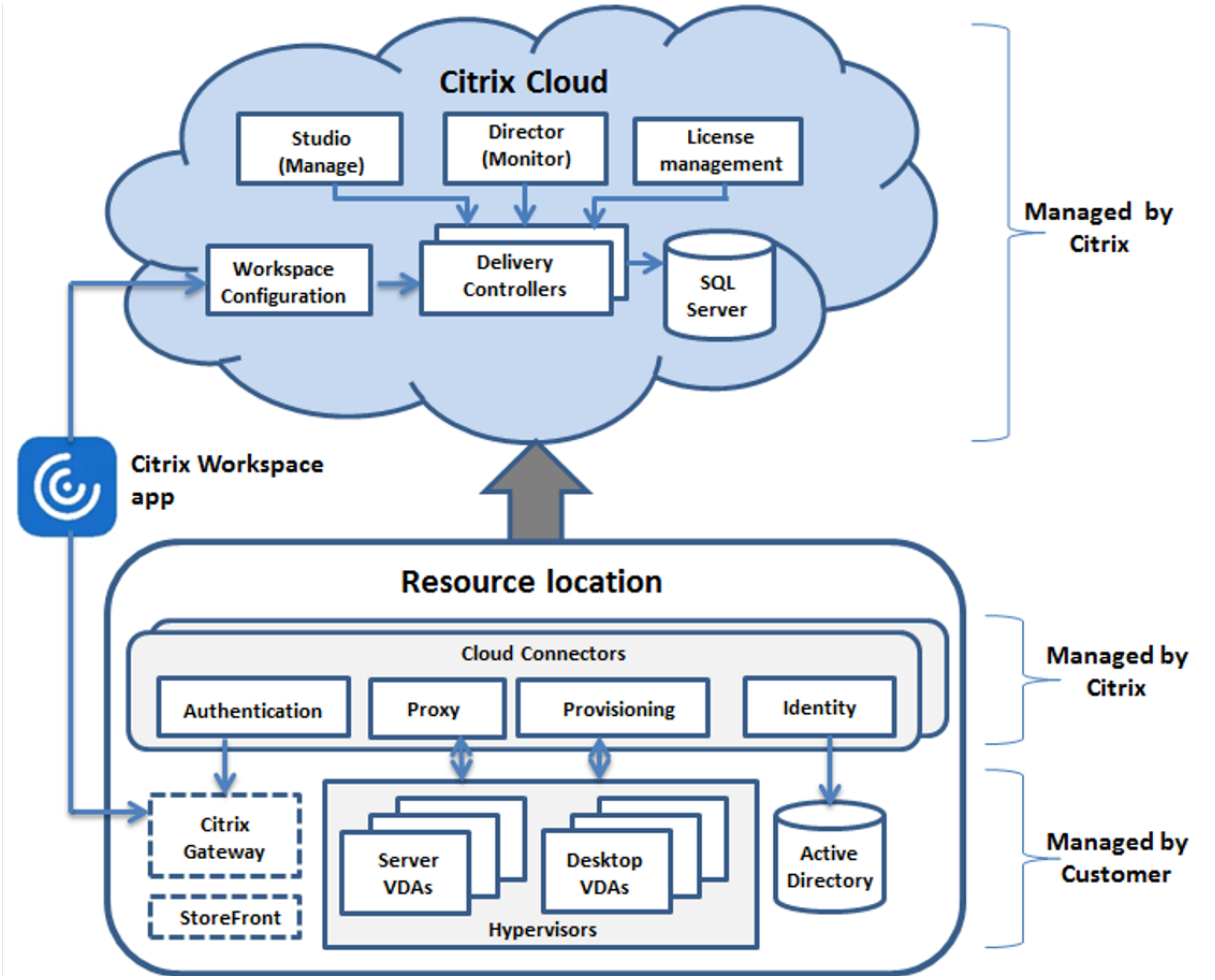
Cloud Connector は、インストール時に自動的にインストールされる Microsoft SQL Express Server LocalDB を実行します。Cloud Connector の CPU 構成、特に SQL Express Server LocalDB で使用可能なコアの数が、LHC のパフォーマンスに直接影響します。SQL Server Express Server LocalDB で使用可能な CPU コアの数は、メモリ割り当てよりも大きな影響を LHC のパフォーマンスに与えます。この CPU オーバーヘッドは、Citrix DaaS との通信ができず、LHC ブローカーがアクティブな LHC モードの場合にのみ確認されます。LHC を使用するすべての環境では、ソケットごとに 4 つのコアと、Citrix では Cloud Connector ごとに最低 4 つの CPU コアを使用することをお勧めします。SQL Express Server LocalDB のコンピューティングリソースの構成については、「SQL Server のエディションごとの処理能力の上限」を参照してください。

SQL Express Server LocalDB で使用可能なコンピューティングリソースが正しく構成されていない場合、構成の同期時間が長くなり、停止中のパフォーマンスが低下する可能性があります。一部の仮想化環境では、処理能力は CPU コアの数ではなく、論理プロセッサの数に依存します。

テスト結果の要約

この概要のすべての結果は、詳細セクションに記載されたとおりに構成されたテスト環境での結果に基づきます。ここに表示されている結果は、単一のリソースの場所に関するものです。異なるシステム構成では、異なる結果になる可能性があります。

この図は、テストされた構成の概要をグラフィカルに示しています。



この表は、リソースの場所のサイズを決定するためのクイックガイドを提供します。1 つのリソースの場所における最大値は 10,000 です。リソースの場所の制限については、「制限」を参照してください。

> 注:
>
> 制限を超えると、停止中に接続やパフォーマンスの問題が発生する可能性があります。したがって、未登録の VDA が発生する可能性があるため、推奨される制限を超えないようにする必要があります。

結果は Citrix の内部テストに基づいています。記載されている構成は、高レートセッション起動テストや登録ストームなど、さまざまなワークロードでテストされました。

	中	大	最大
VDA	1000 VDI または 250 RDS	5,000 VDI または 500 RDS	10,000 VDI または 1000 RDS
ホスト接続	20	40	40
コネクタ用 **CPU**	仮想 CPU×4	仮想 CPU×4	仮想 CPU×8

	中	大	最大
コネクタ用メモリ	6GB	8GB	10GB

テスト方法

負荷を追加し、環境コンポーネントのパフォーマンスを測定するためのテストが実施されました。コンポーネントの監視では、パフォーマンスデータと手順のタイミング（ログオン時間、登録時間など）のデータを収集しました。VDA とセッションをシミュレートすることが必要だったときに、独自の Citrix シミュレーションツールが使用されました。これらのツールは、実際のセッションや VDA をホストするために必要なリソースがなくても、従来の VDA やセッションと同様に Citrix コンポーネントを使用できるように設計されています。Citrix StoreFront を使用するテストは、クラウドブローカリングモードと LHC モードの両方で実施されました。

この記事の Cloud Connector のサイジングの推奨事項は、これらのテストから収集されたデータに基づいています。

実施されたテストは次のとおりです:

- セッションログオン/起動ストーム：ログオンが集中する期間をシミュレートするテスト。
- **VDA** 登録ストーム： VDA の登録が集中する期間をシミュレートするテスト。たとえば、アップグレードサイクルの後、またはクラウドブローカリングモードとローカルホストキャッシュモード間の移行。
- **VDA** 電源操作ストーム：大量の VDA 電源操作をシミュレートするテスト。

テストシナリオと条件

これらのテストは、LHC が構成された環境で実施されました。LHC の使用について詳しくは、「ローカルホストキャッシュ」を参照してください。LHC には、オンプレミスの StoreFront サーバーが必要です。StoreFront について詳しくは、StoreFront 製品のドキュメントを参照してください。

StoreFront 構成の推奨事項:

- 1 つの StoreFront サーバーまたはサーバーグループで複数のリソースの場所がある場合は、StoreFront ストアの高度なヘルスチェックオプションを有効にします。「ローカルホストキャッシュ」の、「StoreFront の要件」を参照してください。
- セッション起動レートを高くするには、StoreFront サーバーグループを使用します。StoreFront 製品ドキュメントの、「サーバーグループの構成」を参照してください。

テスト条件:

- CPU とメモリの要件は、ベース OS と Citrix サービスのみです。サードパーティのアプリやサービスには、追加のリソースが必要になる場合があります。
- VDA は、Citrix Virtual Delivery Agent を実行している仮想マシンまたは物理マシンです。

- テストは Windows VDA のみを使用して実行されます。
- テストされたすべての VDA は、Citrix DaaS を使用して電力管理されました。
- 1000～10,000 の VDI サーバーと 250～1000 の RDS サーバーのワークロードと、1000～20,000 のセッションがテストされました。
- リソースの場所ごとに、最大 20,000 RDS セッションまでテストを実施しました。
- テストは、通常の運用中と停止中の両方で、1 つの Cloud Connector を使用して実行されました。可用性を高めるため、Cloud Connector を 2 つ以上使用することをお勧めします。停止モードの場合、VDA の登録とブローカーには 1 つのコネクタのみが使用されます。
- Intel Cascade Lake プロセッサで構成された Cloud Connector でテストを実施しました。
- セッションは、単一の Citrix StoreFront サーバーを介して開始されました。
- LHC 停止セッションは、マシンが再登録された後に実行されるテストを開始します。

RDS セッション数は推奨値であり、上限ではありません。ご使用の環境下での RDS セッション上限をテストしてください。

> 注:
>
> セッション数と起動レートは、RDS にとって VDA の数よりも重要です。

中規模のワークロード

これらのワークロードに対して、4 つの vCPU と 6 GB のメモリでテストを実施しました。

テストのワークロード	サイトの状態	VDA 登録時間	登録 CPU とメモリ使用状況	起動テストの長さ	セッション起動 CPU とメモリ使用状況	起動レート
1,000 VDI	オンライン	5 分	CPU 最大 = 36%、CPU 平均 = 33%、メモリ最大 = 5.3 GB	2 分	CPU 最大 = 29%、CPU 平均 = 27%、メモリ最大 = 3.7 GB	毎分 500
1,000 VDI	停止	4 分	CPU 最大 = 11%、CPU 平均 = 10%、メモリ最大 = 4.5 GB	2 分	CPU 最大 = 42%、CPU 平均 = 28%、メモリ最大 = 4.0 GB	毎分 500
250 RDS、5000 セッション	オンライン	3 分	CPU 最大 = 14%、CPU 平均 = 4%、メモリ最大 = 3.5 GB	9 分	CPU 最大 = 46%、CPU 平均 = 21%、メモリ最大 = 3.7 GB	毎分 555

テストのワークロード	サイトの状態	VDA 登録時間	登録 CPU とメモリ使用状況	起動テストの長さ	セッション起動 CPU とメモリ使用状況	起動レート
250 RDS、5000 セッション	停止	3 分	CPU 最大 = 15%、CPU 平均 = 5%、メモリ最大 = 3.7	9 分	CPU 最大 = 51%、CPU 平均 = 32%、メモリ最大 = 4.2 GB	毎分 555

大規模なワークロード

これらのワークロードに対して、4 つの vCPU と 8 GB のメモリでテストを実施しました。

テストのワークロード	サイトの状態	VDA 登録時間	登録 CPU とメモリ使用状況	起動テストの長さ	セッション起動 CPU とメモリ使用状況	起動レート
5,000 VDI	オンライン	3～4 分	CPU 最大 = 45%、CPU 平均 = 25%、メモリ最大 = 7.0 GB	5 分	CPU 最大 = 75%、CPU 平均 = 55%、メモリ最大 = 7.0 GB	毎分 1,000
5,000 VDI	停止	4～6 分	CPU 最大 = 15%、CPU 平均 = 5%、メモリ最大 = 7.5 GB	5 分	CPU 最大 = 45%、CPU 平均 = 40%、メモリ最大 = 7.5 GB	毎分 1,000
500 RDS、10,000 セッション	オンライン	3 分	CPU 最大 = 45%、CPU 平均 = 25%、メモリ最大 = 7.0 GB	10 分	CPU 最大 = 75%、CPU 平均 = 55%、メモリ最大 = 7.0 GB	毎分 1,000
500 RDS、10,000 セッション	停止	3 分	CPU 最大 = 15%、CPU 平均 = 5%、メモリ最大 = 7.5	10 分	CPU 最大 = 45%、CPU 平均 = 40%、メモリ最大 = 7.5 GB	毎分 1,000

最大ワークロード

これらのワークロードに対して、8 つの vCPU と 10 GB のメモリでテストを実施しました。

テストのワークロード	サイトの状態	VDA 登録時間	登録 CPU とメモリ使用状況	起動テストの長さ	セッション起動 CPU とメモリ使用状況	起動レート
10,000 VDI	オンライン	3〜4 分	CPU 最大 = 85%、CPU 平均 = 10%、メモリ最大 = 8.5 GB	7 分	CPU 最大 = 66%、CPU 平均 = 28%、メモリ最大 = 7.0 GB	毎分 1,400
10,000 VDI	停止	4〜5 minutes	CPU 最大 = 90%、CPU 平均 = 17%、メモリ最大 = 8.2 GB	5 分	CPU 最大 = 90%、CPU 平均 = 45%、メモリ最大 = 8.5 GB	毎分 2,000
1,000 RDS、20,000 セッション	オンライン	1〜2 分	CPU 最大 = 60%、CPU 平均 = 20%、メモリ最大 = 8.6 GB	17 分	CPU 最大 = 66%、CPU 平均 = 25%、メモリ最大 = 6.8 GB	毎分 1,200
1,000 RDS、20,000 セッション	停止	3〜4 分	CPU 最大 = 22%、CPU 平均 = 10%、メモリ最大 = 8.5	21 分	CPU 最大 = 90%、CPU 平均 = 50%、メモリ最大 = 7.5 GB	毎分 1,000

> 注:
>
> ここに示すワークロードは、1 つのリソースの場所で推奨される最大値です。これ以上のサイズのワークロードをサポートするには、リソースの場所を追加します。

構成同期リソース使用量

構成の同期プロセスにより、Cloud Connector が Citrix DaaS で最新の状態に保たれます。更新プログラムは自動的に Cloud Connector に送信され、停止が発生した際には Cloud Connector がいつでもブローカリングを引き継げる状態になっています。構成の同期により、LHC データベースである SQL Express Server LocalDB が更新されます。プロセスはデータを一時データベースにインポートし、インポートされるとそのデータベースに切り替えます。これにより、引き継ぎ可能な LHC データベースが常に存在することが保証されます。

データが一時データベースにインポートされている間、CPU、メモリ、およびディスクの使用率が一時的に増加します。

テスト結果:

- データのインポート時間: 7〜10 分
- **CPU** 使用率:
  - 最大 = 25%
  - 平均 = 15%
- メモリ使用率:
  - 最大 = 9GB
  - 約 2 GB から 3 GB の増加
- ディスク使用率:
  - 4 MB/s のディスク読み取りスパイク
  - 18 MB/s のディスク書き込みスパイク
  - 構成ファイルのダウンロードおよび書き込み中に、70 MB/s の xml ディスク書き込みスパイク
  - インポート完了時に、4 MB/s のディスク読み取りスパイク
- **LHC** データベースのサイズ:
  - 400〜500 MB のデータベースファイル
  - 200〜300 MB のログデータベース

テスト条件:

- 8 つの仮想 CPU AMD EPYC でテストを実施
- インポートされたサイト構成データベースは、サイト全体で合計 80,000 VDA および 300,000 ユーザー（100,000 ユーザーの 3 シフト）の環境用
- データのインポート時間は、10,000 VDI のリソースの場所でテスト

リソース使用に関する補足的な注意事項:

- インポート中に、完全なサイト構成データがダウンロードされます。このダウンロードは、サイトのサイズによってはメモリスパイクを引き起こす可能性があります。
- テストされたサイトでは、データベースとデータベースログファイルの合計で約 800 MB を使用しました。構成の同期中に、これらのファイルは、最大合計サイズ約 1,600 MB で複製されます。Cloud Connector に複製ファイル用の十分なディスクスペースがあることを確認してください。ディスクがいっぱいになると、構成の同期プロセスは失敗します。

VDA のインストール

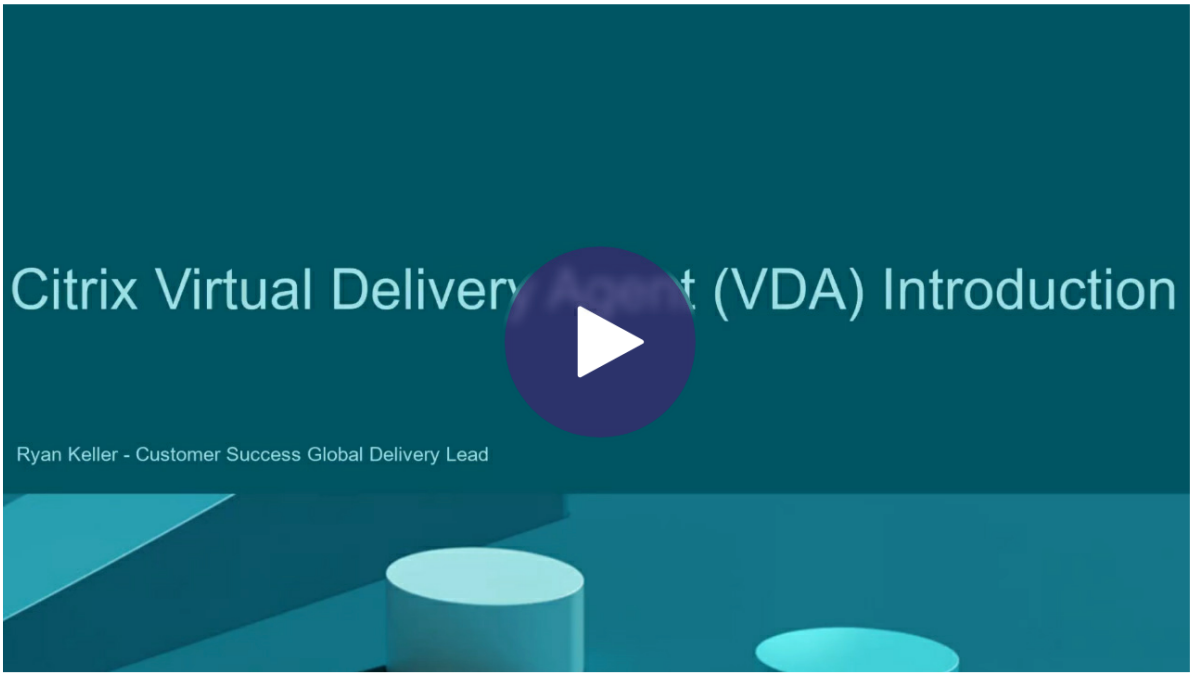
May 17, 2024

はじめに

この記事では、まず Windows VDA と使用可能な VDA インストーラーについて説明します。その後、VDA インストールウィザードの手順について説明します。同等の機能を持つコマンドラインが用意されています。詳しくは、「コマンドラインを使用した VDA のインストール」を参照してください。

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

VDA の概要を表示します。



インストールの考慮事項

VDA の概要と役割については、「Citrix DaaS」で説明しています。以下は詳細です。

- 分析情報の収集：コンポーネントのインストールまたはアップグレード時に、分析情報が自動で収集されます。デフォルトでは、インストールの完了時に、そのデータが Citrix へ自動的にアップロードされます。また、コンポーネントをインストールすると、自動的にCitrix カスタマーエクスペリエンス向上プログラム（CEIP）に登録され、匿名データがアップロードされます。また、インストールまたはアップグレード中に、Call Home に登録するかどうかを選択できます。

VDA のインストールが失敗すると、MSI アナライザーはエラーのある MSI ログを解析し、正確なエラーコードを表示します。このアナライザーは、既知の問題であった場合は、CTX 記事を示します。アナライザーはまた、故障エラーコードに関する匿名化データも収集します。このデータは、CEIP によって収集された他のデータに含まれます。CEIP への登録を終了すると、収集された MSI アナライザーのデータは Citrix に送信されなくなります。

これらのプログラムについて詳しくは、「Citrix Insight Services」を参照してください。

- **Citrix Workspace** アプリ： VDA をインストールした場合、デフォルトでは Windows 向け Citrix Workspace アプリはインストールされません。Windows 向け Citrix Workspace アプリおよび他の Citrix Workspace アプリは、Citrix Web サイトからダウロードして、インストールまたはアップグレードできます。また、Workspace または StoreFront サーバーでこれらの Citrix Workspace アプリを公開することもできます。
- 印刷スプーラーサービス： Microsoft の印刷スプーラーサービスを有効にする必要があります。そのサービスが無効になっている場合、VDA を正常にインストールすることはできません。
- **Microsoft** メディアファンデーション：サポート対象のほとんどの Windows のエディションには、Microsoft メディアファンデーションが既にインストールされています。VDA のインストール先のマシンに Microsoft メディアファンデーションがインストールされていない場合（N エディション等）は、マルチメディア機能の一部はインストールされず、動作しません。

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

  その制限を認識するか、VDA のインストールを中止して、Media Foundation をインストールした後に再開してください。グラフィカルユーザーインターフェイス上に、この選択がメッセージとして表示されます。制限を認識するには、コマンドラインで/`no_mediafoundation_ack`オプションを使用してください。
- ローカルユーザーグループ： VDA をインストールすると、Direct Access Users と言う名前の新しいローカルユーザーグループが自動的に作成されます。シングルセッション OS VDA では、このグループは RDP 接続のみに適用されます。マルチセッション OS VDA では、このグループは ICA 接続と RDP 接続に適用されます。
- **Cloud Connector** のアドレス要件： VDA には、通信に使用する有効な Cloud Connector アドレス（同じリソースロケーション内）が少なくとも 1 つ必要です。保持されていない場合は、セッションを確立することができません。Cloud Connector のアドレスは、VDA のインストール時に指定します VDA を登録可能な Cloud Connector アドレスを指定する他の方法については、「VDA 登録」を参照してください。
- オペレーティングシステムの考慮事項：

  - サポートされるプラットフォーム、オペレーティングシステム、バージョンについては、「システム要件」を参照してください。
  - 各オペレーティングシステムは最新の状態に維持してください。

  - VDA のシステムクロックを同期しておく必要があります。この同期は、Kerberos でマシン間の通信を保護するために必要です。
  - Windows 10 マシンでの最適化ガイダンスは、CTX216252にあります。
  - 対象の Windows VDA バージョンでサポートされていない OS にその VDA をインストール（またはアップグレード）しようとすると、選択肢を示すメッセージが表示されます。たとえば、古い Windows マシンに最新の VDA をインストールしようとすると、CTX139030へのリンクを示すメッセージが表示されます。詳しくは、「以前のオペレーティングシステム」を参照してください。

- インストールされた **MSI**： VDA をインストールすると、いくつかの MSI が自動的にインストールされます。グラフィカルインターフェイスの ［追加コンポーネント］ページまたは CLI で/excludeオプションを使用して、MSI の一部がインストールされないようにすることができます。それほか、それらがインストールされないようにする唯一の方法は、CLI の/excludeオプションを使用することです。
- ドメイン参加済み： VDA ソフトウェアをインストールする前に、マシンがドメイン参加済みであることを確認してください。

VDA サポートツール

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

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

サポート MSI 内の現在のツール：

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

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

VDA インストール時の再起動

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

VDA インストール中のほかの再起動の回数を最小限に抑えるには：

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

VDA インストール前にこれらの前提条件をインストールしない場合:

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

再起動するたびに、VDA のインストールが続行されますコマンドラインからインストールしている場合は、/noresumeオプションで自動の再起動を防ぐことができます。

VDA をバージョン 7.17 またはそれ以降のサポート対象バージョンにアップグレードするときは、アップグレード中に再起動が行われます。この再起動を避けることはできません。

インストールまたはアップグレードの失敗時の復元

> 注:
>
> この機能は、シングルセッション VDA でのみ使用できます。

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

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

デフォルトでは、この機能は無効になっています。

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

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

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

  インストールまたはアップグレードが正常に完了すると、復元ポイントは使用されませんが、保持されます。

- /enablerestoreまたは/enablerestorecleanupオプションを指定して、VDA インストーラーを実行します。
  - /enablerestorecleanupオプションを指定した場合、インストールまたはアップグレードが正常に完了すると、復元ポイントは自動的に削除されます。
  - /enablerestoreオプションを指定した場合、インストールまたはアップグレードが正常に完了すると、復元ポイントは使用されませんが、保持されます。

VDA インストーラー

VDA インストーラーは、Citrix Cloud コンソールから直接ダウンロードできます。

デフォルトでは、自己抽出型のインストーラーのファイルはTempフォルダーに抽出されます。Tempフォルダーに抽出されたファイルは、インストールの完了後に自動で削除されます。または、絶対パスとともに/extractコマンドを使用できます。

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

VDAServerSetup.exe マルチセッション OS VDA をインストールします。

VDAWorkstationSetup.exe シングルセッション OS VDA をインストールします。

VDAWorkstationCoreSetup.exe リモート PC アクセス展開またはコア VDI インストールに最適化されたシングルセッション OS VDA をインストールします。リモート PC アクセスマシンでは物理マシンを使用します。コア VDI インストールとは、イメージとして使用されない仮想マシンのことを指します。このインストーラーでは、VDA 接続に必要なコアサービスのみが展開されます。このため、サポートされるオプションは、VDAWorkstationSetup インストーラーで有効なオプションのうちの一部に限られます。

この最新リリース用インストーラーは、以下で使用されるコンポーネントをインストールせず、また含んでもいません:

- App-V。
- Profile Management。インストールから Citrix Profile Management を除外すると、［監視］タブの表示に影響が生じます。
- Machine Identity Service。
- Windows 向け Citrix Workspace アプリ。
- Citrix Supportability Tools
- Citrix Files for Windows
- Citrix Files for Outlook
- ストレージ最適化用 MCSIO 書き込みキャッシュ

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

このインストーラーは自動的に Web ブラウザーコンテンツリダイレクト MSI をインストールします。自動インストールは、VDA リリース 2003 以降でサポートされているリリースで使用できます。

VDAWorkstationCoreSetup.exeを使用することは、全製品またはVDAWorkstationSetup.exeインストーラーを使用してシングルセッション OS VDA をインストールすることと同等であり、次のどちらかでインストールします:

- グラフィカルインターフェイス:［環境］ページで ［リモート **PC** アクセス］オプションを選択します。
- コマンドラインインターフェイス: /remotepcオプションを指定します。
- コマンドラインインターフェイス: /components vdaおよび/exclude "Citrix Personalization for App-V - VDA""Personal vDisk""Machine Identity Service""Citrix Profile Management""Citrix Profile Management WMI Plugin""Citrix Supportability Tools""Citrix Files for Windows""Citrix Files for Outlook""Citrix MCS IODriver"を指定します。

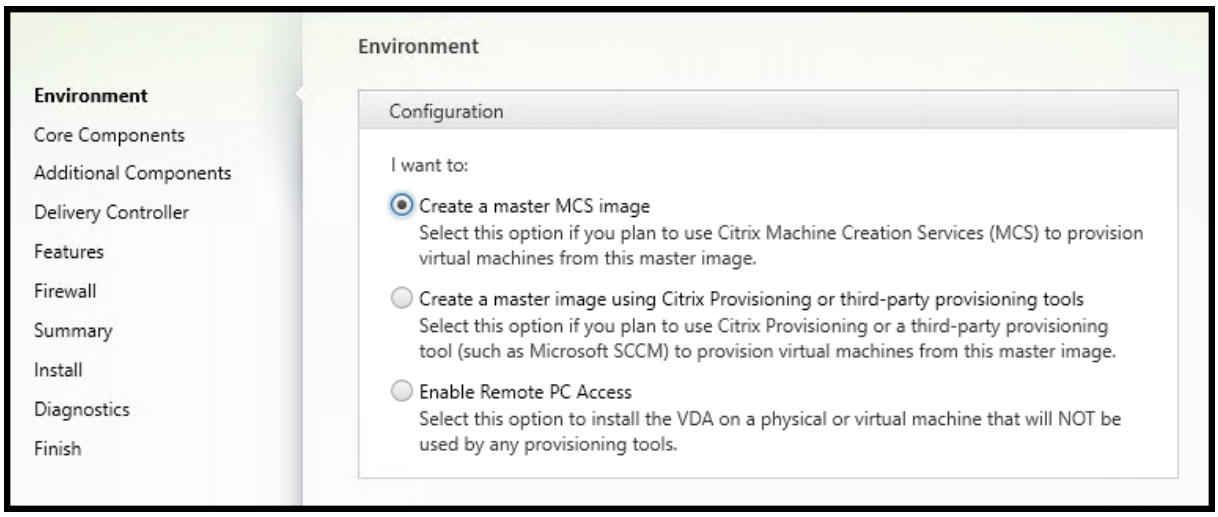
VDAWorkstationCoreSetup.exeインストーラーを使用して VDA をインストールし、後でVDAWorkstationSetup.exeインストーラーを使用してその VDA をアップグレードする場合には、必要に応じて省略したコンポーネントや機能をインストールできます。

手順 **1**: 製品ソフトウェアをダウンロードしてウィザードを起動する

1. VDA をインストールするマシンで、Citrix Cloudにサインインします。
2. 左上のメニューで、［マイサービス］リストにある Citrix DaaS を選択します。
3. 右側にある ［ダウンロード］をクリックし、［**VDA** のダウンロード］を選択します。VDA ダウンロードページにリダイレクトされます。目的の VDA インストーラーを見つけて、［ファイルのダウンロード］を選択します。
4. ダウンロードが完了したら、ダウンロードしたファイルを右クリックし、［管理者として実行］を選択します。インストールウィザードが起動します。

手順 1～3 の代わりに、VDA をCitrix のダウンロードページから直接ダウンロードすることもできます。

手順 **2**: **VDA** の使用方法を指定する



［環境］ページで、マシンをプロビジョニングするためにこのマシンをイメージとして使用するかどうかなど、VDA の使用方法を選択します。選択したオプションにより、どの Citrix Provisioning ツール（存在する場合）が自動でインストールされるか、および VDA インストーラーの ［追加コンポーネント］ページのデフォルト値が決定されます。

次のいずれかのオプションを選択します：

- マスター **MCS** イメージを作成する：仮想マシンのプロビジョニングに Machine Creation Services を使用する場合は、このオプションを選択して仮想マシンイメージに VDA をインストールします。このオプションは、Machine Identity Service をインストールします。これはデフォルトのオプションです。

  コマンドラインオプション：/mastermcsimageまたは/masterimage

- **Citrix Provisioning** またはサードパーティのプロビジョニングツールを使用してマスターイメージを作成する： Citrix Provisioning またはサードパーティのプロビジョニングツール（Microsoft System Center Configuration Manager など）を使用する場合は、このオプションを選択して仮想マシンイメージに VDA をインストールします。このオプションは、Citrix Provisioning の読み取り/書き込みディスクから起動された、以前プロビジョニングされた VM に使用します。

  コマンドラインオプション：/masterpvsimage

- （マルチセッション OS マシンでのみ表示）サーバーへの仲介接続を有効にする：イメージとして使用しない物理マシンまたは仮想マシンに VDA をインストールするには、このオプションを選択します。

  コマンドラインオプション：/remotepc

- （マルチセッション OS マシンでのみ表示）リモート **PC** アクセスを有効にする：リモート PC アクセスで使用する物理マシンに VDA をインストールするには、このオプションを選択します。

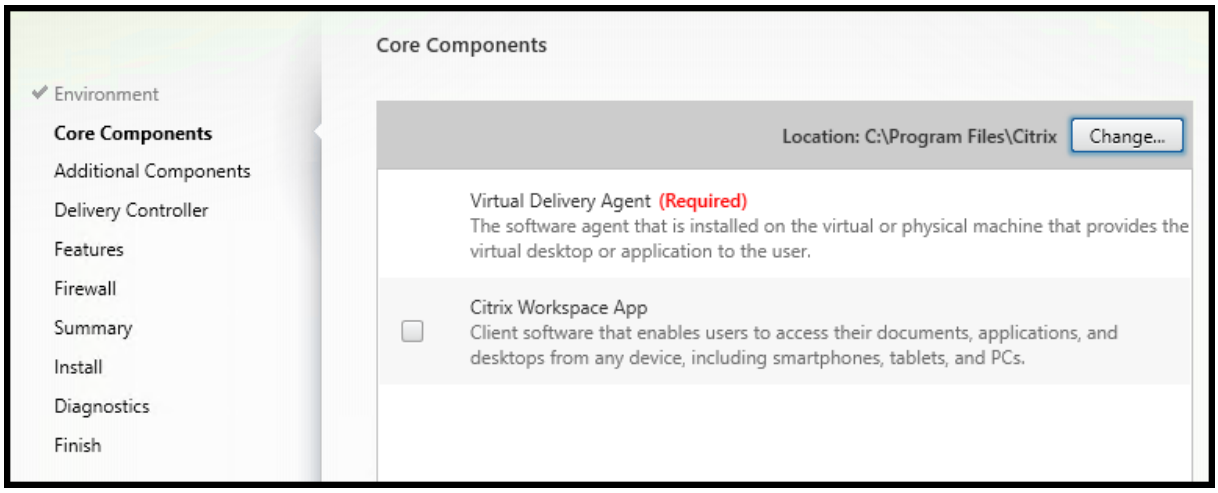
  コマンドラインオプション：/remotepc

［次へ］を選択します。

次の場合、このページは表示されません：

- VDA をアップグレードする場合。
- VDAWorkstationCoreSetup.exeインストーラーを使用する場合。

手順 **3**：インストールするコンポーネントおよびインストール場所を選択する



［コアコンポーネント］ページで次の作業を行います：

- 場所：デフォルトでは、`C:\Program Files\Citrix`に各コンポーネントがインストールされます。ほとんどの展開ではデフォルトで十分です。別の場所を指定する場合、指定した場所にはネットワークサービスの実行権限が必要です。

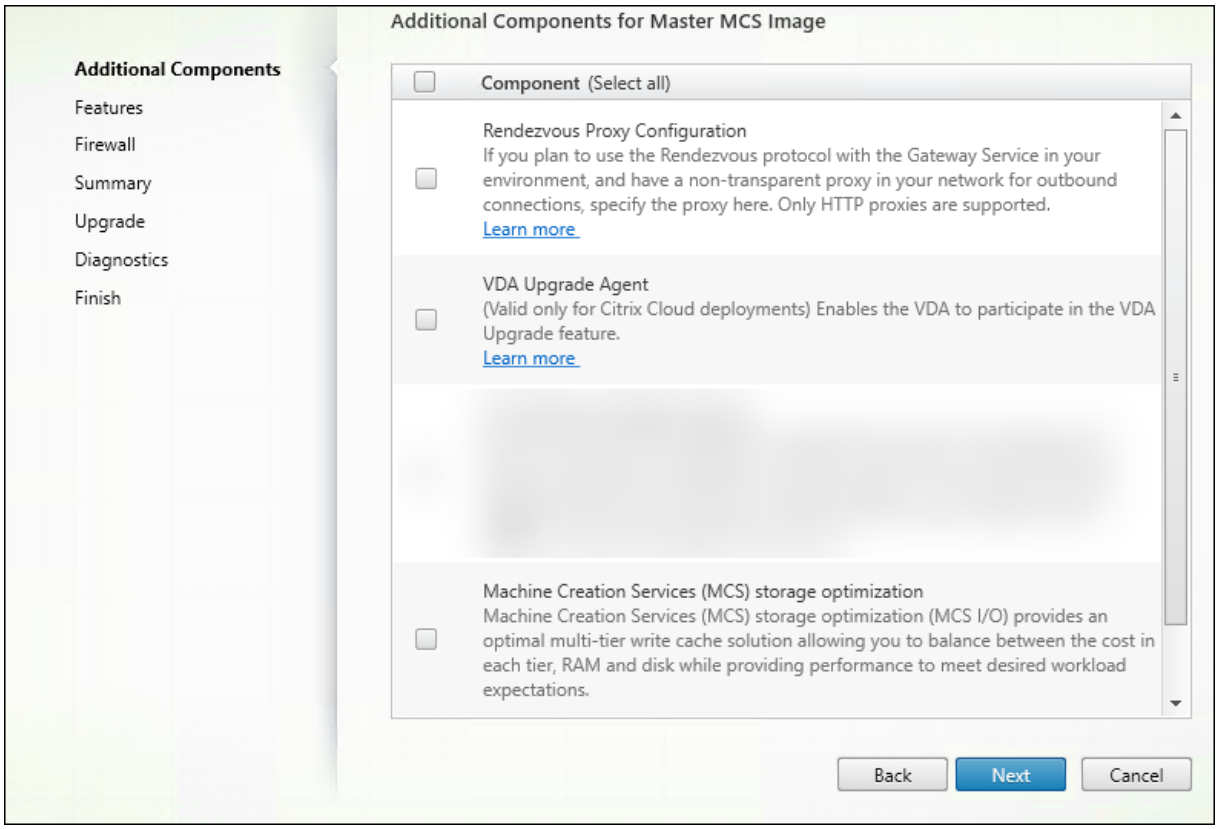
  コマンドラインオプション：`/installdir`

- コンポーネント：デフォルトでは、Windows 向け Citrix Workspace アプリは VDA とともにインストールされません。`VDAWorkstationCoreSetup.exe`インストーラーを使用する場合、Windows 向け Citrix Workspace アプリはインストールされないため、このチェックボックスは表示されません。

  コマンドラインオプション：VDA および Windows 向け Citrix Workspace アプリをインストールする場合は「`/components vda,plugin`」。

［次へ］を選択します。

手順 **4**：追加コンポーネントのインストール



［追加コンポーネント］ページには、VDA とともにほかの機能やテクノロジをインストールするかどうかを指定するチェックボックスがあります。コマンドラインインストールでは、`/exclude`オプションまたは`/includeadditional`オプションを指定して、使用可能な 1 つまたは複数のコンポーネントを除外またはインストールすることができます。

次の表に、このページの項目のデフォルト設定を示します。デフォルトの設定は、［環境］ページで選択したオプションによって異なります。

［追加コンポーネント］ページ	［環境］ページ：［マスター MCS イメージを作成する］または［Citrix Provisioning またはサードパーティの…］を選択	［環境］ページ：［サーバーへの仲介接続を有効にする］（マルチセッション OS 対応）または［リモート PC アクセスを有効にする］（シングルセッション OS 対応）を選択
Citrix Personalization for App-V	未選択	未選択
ユーザー個人設定レイヤー	未選択	このユースケースでは無効なため表示されません。
Citrix Supportability Tools	選択済み	未選択
Citrix Profile Management	選択済み	未選択

[追加コンポーネント] ページ	[環境] ページ：[マスター MCS イメージを作成する] または [Citrix Provisioning またはサードパーティの…] を選択	[環境] ページ：[サーバーへの仲介接続を有効にする]（マルチセッション OS 対応）または [リモート PC アクセスを有効にする]（シングルセッション OS 対応）を選択
Citrix Profile Management WMI プラグイン	選択済み	未選択
Citrix VDA Upgrade Agent	未選択	未選択
Citrix Backup and Restore	未選択	未選択
Citrix Files for Windows	未選択	未選択
Citrix Files for Outlook	未選択	未選択
Machine Creation Services（MCS）ストレージ最適化	未選択	未選択
Rendezvous プロトコルの構成	未選択	未選択

次の場合、このページは表示されません：

- `VDAWorkstationCoreSetup.exe`インストーラーを使用している。また、追加コンポーネント用のコマンドラインオプションはこのインストーラーでは無効です。
- VDA をアップグレードしており、追加コンポーネントが既にすべてインストールされている。追加コンポーネントのいくつかが既にインストールされている場合、このページにはインストールされていないものだけが表示されます。

一覧には、次のコンポーネントが表示されます：

- **Citrix Personalization for App-V**： Microsoft App-V パッケージのアプリケーションを使用する場合、このコンポーネントをインストールします。詳しくは、「App-V」を参照してください。

  コマンドラインオプション：インストールする場合は`/includeadditional "Citrix Personalization for App-V - VDA"`、インストールしない場合は`/exclude "Citrix Personalization for App-V - VDA"`

- **Citrix** ユーザー個人設定レイヤー：ユーザー個人設定レイヤーの MSI をインストールします。詳しくは、「ユーザー個人設定レイヤー」を参照してください。

  このコンポーネントは、シングルセッション Windows 10 マシンに VDA をインストールするときにのみ表示されます。

  コマンドラインオプション：インストールする場合は`/includeadditional "User Personalization Layer"`、インストールしない場合は`/exclude "User Personalization Layer"`

- **Citrix Supportability Tools**: Citrix のサポートツールを含む MSI をインストールします。

  コマンドラインオプション: インストールする場合は `/includeadditional "Citrix Supportability Tools"`、インストールしない場合は`/exclude "Citrix Supportability Tools"`

- **Citrix Profile Management**: このコンポーネントは、ユーザープロファイル内のユーザーの個人設定を管理します。詳しくは、「Profile Management」を参照してください。

  インストール対象から Citrix Profile Management を除外すると、Citrix Cloud での VDA の監視やトラブルシューティングに影響が生じます。

  - ［ユーザーの詳細］ページおよび［監視］タブの［**EndPoint**］ページで、［個人設定］パネルおよび［ログオン処理時間］パネルに不具合が発生します。
  - ［ダッシュボード］ページと ［傾向］ページでは、Profile Management がインストールされているマシンについてのデータしか ［平均ログオン処理時間］パネルに表示されません。

  サードパーティのユーザープロファイル管理ソリューションを使用している場合でも、Citrix Profile Management Service をインストールして実行することを Citrix ではお勧めします。Citrix Profile Management Service の有効化は、必須ではありません。

  コマンドラインオプション: インストールする場合は `/includeadditional "Citrix Profile Management"`、インストールしない場合は`/exclude "Citrix Profile Management"`

- **Citrix Profile Management WMI** プラグイン: このプラグインは、プロファイルプロバイダー、プロファイルの種類、サイズ、ディスク使用率などの Profile Management ランタイム情報を、WMI（Windows Management Instrumentation）オブジェクトに格納して提供します。WMI オブジェクトは、Director にセッション情報を提供します。

  コマンドラインオプション: インストールする場合は `/includeadditional "Citrix Profile Management WMI Plugin"`、インストールしない場合は`/exclude "Citrix Profile Management WMI Plugin"`

- **VDA Upgrade Agent**:（Citrix DaaS 展開にのみ適用可能。）VDA がVDA アップグレード機能に参加できるようになります。この機能を使用すると、管理コンソールから、直ちに、またはスケジュールされた時間に、カタログの VDA をアップグレードできます。このエージェントがインストールされていない場合は、マシン上で VDA インストーラーを実行することで VDA をアップグレードできます。

  コマンドラインオプション: インストールする場合は`/includeadditional "Citrix VDA Upgrade Agent"`、インストールしない場合は`/exclude "Citrix VDA Upgrade Agent"`

- **Citrix Files for Windows**: このコンポーネントを使用すると、ユーザーは自分の Citrix Files アカウントに接続できるようになります。これにより、コンテンツの完全同期を行わなくても、Windows ファイルシステムのマッピング済みドライブから Citrix Files にアクセスできるようになります。

コマンドラインオプション：インストールする場合は/includeadditional "Citrix Files for Windows"、インストールしない場合は/exclude "Citrix Files for Windows"

- **Citrix Files for Outlook**：このコンポーネントによって、添付ファイルやメールを Citrix Files 経由で、ファイルサイズの制限を回避しながらセキュリティを強化して送信できます。ファイルアップロード要求を安全に、メールで直接送信できます。詳しくは、「[Citrix Files for Outlook]」(/en-us/citrix-content-collaboration/citrix-files-app/citrix-files-outlook.html) を参照してください。

  コマンドラインオプション：インストールする場合は/includeadditional "Citrix Files for Outlook"、インストールしない場合は/exclude "Citrix Files for Outlook"

- **Machine Creation Services**（**MCS**）ストレージ最適化： Citrix MCS IO ドライバーをインストールします。詳しくは、「ハイパーバイザー間で共有されるストレージ」および「一時データ用キャッシュの構成」を参照してください。

  コマンドラインオプション：インストールする場合は/includeadditional "Citrix MCS IODriver"、インストールしない場合は/exclude "Citrix MCS IODriver"

- プロキシの構成：ご使用の環境において Citrix Gateway サービスで Rendezvous プロトコルを使用する予定であり、ネットワークに発信接続用の非透過プロキシがある場合は、このコンポーネントをインストールします。HTTP プロキシのみがサポートされています。

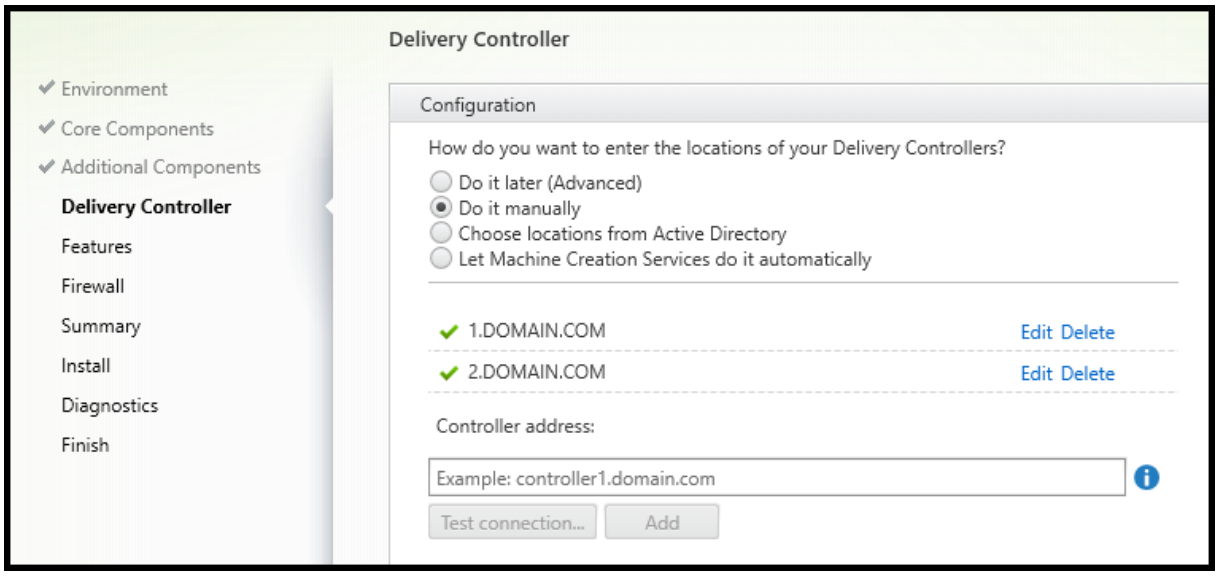
  このコンポーネントをインストールする場合は、[**Rendezvous** プロキシの構成] ページでプロキシのアドレス、または PAC ファイルパスを指定します。機能について詳しくは、「Rendezvous プロトコル」を参照してください。

  コマンドラインオプション：インストールする場合は/includeadditional "Citrix Rendezvous V2"、インストールしない場合は/exclude "Citrix Rendezvous V2"

- **Citrix Backup and Restore**： VDA のインストールまたはアップグレードが失敗した場合、このコンポーネントはマシンをインストールまたはアップグレードする前に実行されたバックアップに戻すことができます。

  コマンドラインオプション:インストールする場合は/includeadditional "Citrix Backup and Restore"、インストールしない場合は/exclude "Citrix Backup and Restore"。

手順 **5**：**Cloud Connector** のアドレス



[**Delivery Controller**] ページで、[手動で指定する] を選択します。インストール済みの Cloud Connector の DNS 名を入力して、[追加] を選択します。リソースの場所に追加の Cloud Connector をインストールしている場合は、それらの DNS 名も追加します。

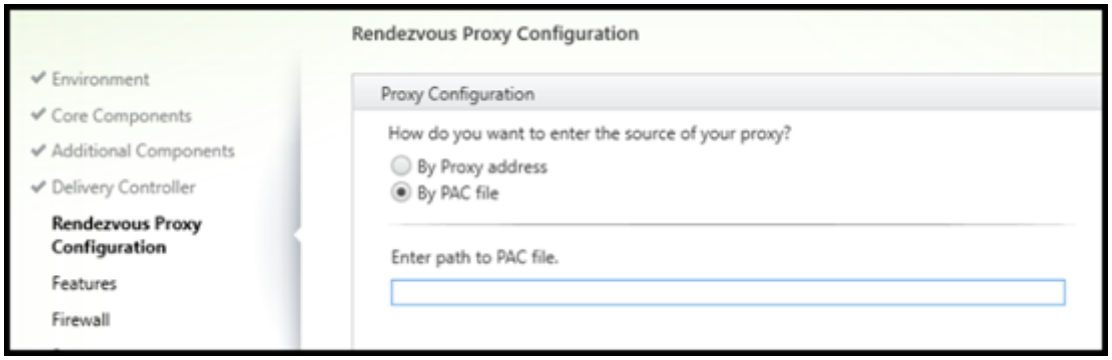
[次へ] を選択します。

注意事項:

- アドレスに使用できるのは、英数字のみです。
- VDA 登録を行うには、Cloud Connector との通信に使用するファイアウォールポートが開放されている必要があります。デフォルトでは、ウィザードの [ファイアウォール] ページでこのポートの開放が有効化されています。

コマンドラインオプション：`/controllers`

手順 **6**：プロキシ構成



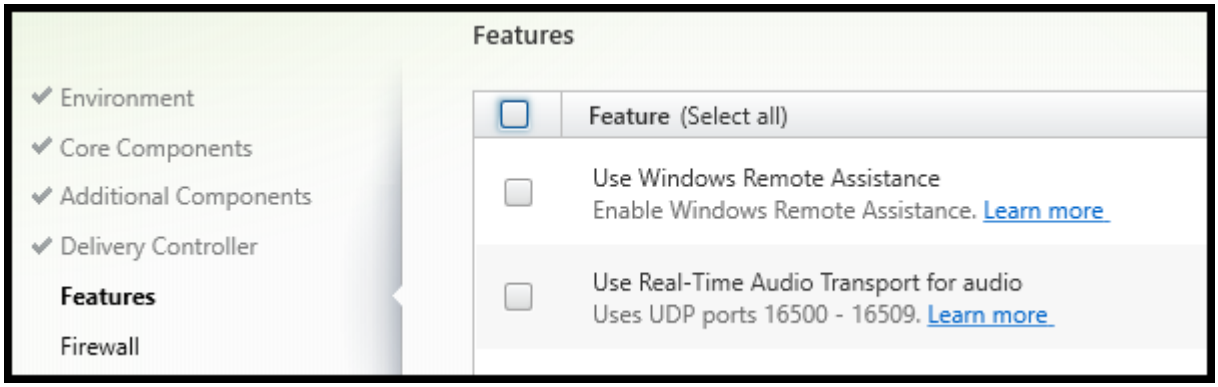
［**Rendezvous** プロキシの構成］ページは、［追加コンポーネント］ページの ［**Rendezvous** プロキシの構成］チェックボックスをオンにした場合にのみ表示されます。

1. プロキシアドレスまたは PAC ファイルパスのどちらでプロキシソースを指定するかを選択します。
2. プロキシアドレスまたは PAC ファイルパスを指定します。
   - プロキシアドレスの形式：`http://<url-or-ip>:<port>`
   - PAC ファイルの形式：`http://<url-or-ip>:<port>/<path>/<filename>.pac`

接続テストを成功させるには、プロキシポートのファイアウォールが開いている必要があります。プロキシに接続できない場合は、VDA のインストールを続行するかどうかを選択できます。

コマンドラインオプション：`/proxyconfig`

手順 **7**：機能を有効または無効にする



［機能］ページで、チェックボックスを使用して、使用する機能を有効または無効にします。

- **Windows** リモートアシスタンスの使用：この機能を有効にすると、Citrix Cloud の Director コンポーネントのユーザーシャドウ機能で、Windows リモートアシスタンスが使用されます。Windows リモートアシスタンスによってファイアウォールで動的ポートが解放されます。（デフォルト = 無効）

  コマンドラインオプション：`/enable_remote_assistance`

- オーディオにリアルタイムオーディオ転送を使用：ネットワークで Voice over IP が広く使われている場合、この機能を有効化します。この機能を使用すると、遅延が短縮され、損失の多いネットワーク経由の音声復元性が改善されます。オーディオデータを UDP トランスポート経由の RTP を使用して伝送することが可能になります。（デフォルト = 無効）

  コマンドラインオプション：`/enable_real_time_transport`

- 画面共有の使用：有効にすると、画面共有で使用されるポートが Windows ファイアウォールで開きます。（デフォルト = 無効）

  コマンドラインオプション：`/enable_ss_ports`

- この **VDA** はクラウドの仮想マシンにインストールされていますか：この設定は、Citrix が、オンプレミスおよびサービス（Citrix Cloud）の VDA 展開でテレメトリのために適切なリソースの場所を特定するのに役立ちます。この機能が、お客様のサービスのご利用に影響を与えることはありません。ご自身の環境で Citrix DaaS を使用する場合に、この設定を有効にします。（デフォルト = 無効）

  コマンドラインオプション：`/xendesktopcloud`

［次へ］を選択します。

このページに **MCS I/O** という名前の機能が含まれている場合、その機能は使用しないでください。MCS IO 機能は、［追加コンポーネント］ページで構成されます。

手順 **8**：ファイアウォールポート

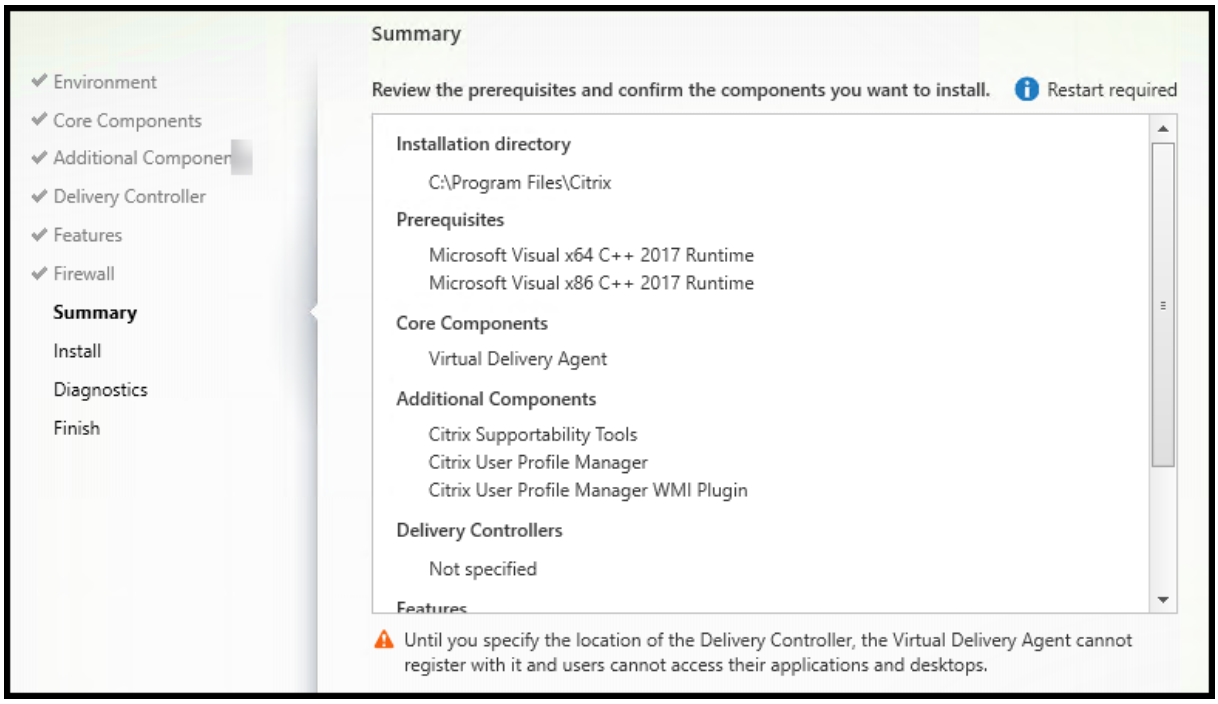
［ファイアウォール］ページには、VDA と Cloud Connector 間の通信に使用するポートが表示されます。Windows ファイアウォールサービスが実行されている場合、ファイアウォールが無効になっていてもこれらのポートはデフォルトで開放されます。ほとんどの展開ではデフォルト設定で十分です。

ポートについて詳しくは、「ネットワークポート」を参照してください。

［次へ］を選択します。

コマンドラインオプション：`/enable_hdx_ports`

手順 **9**：インストール前に前提条件を確認する

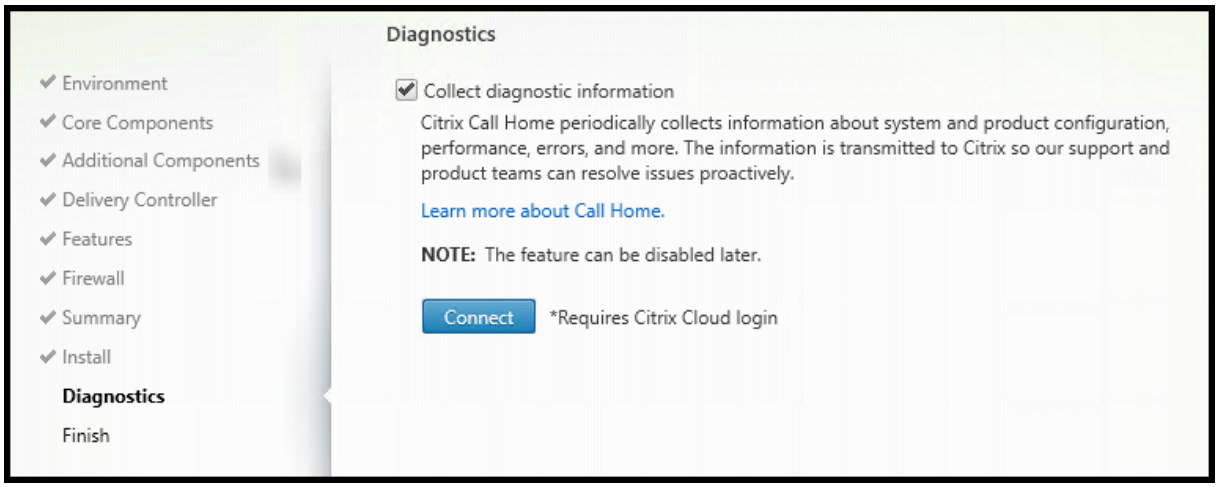


［概要］ページに、インストールされるものが表示されます。必要に応じて、前のウィザードページに戻り、選択を変更できます。

（シングルセッション VDA のみ）失敗時の復元機能を有効にするには、［更新に失敗した場合に自動復元を有効にする］チェックボックスをオンにします。詳しくは、「インストールまたはアップグレードの失敗時の復元」を参照してください。

準備ができたら、［インストール］を選択します。

手順 **10**：診断する

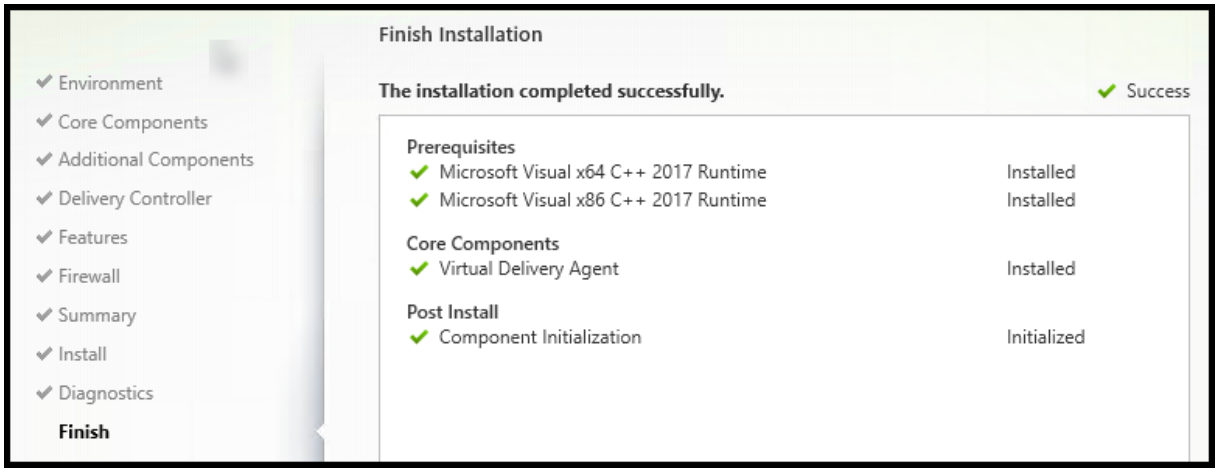


［診断］ページで、Citrix Call Home に参加するかどうかを選択します。参加することを選択する場合（デフォルト）、［接続］を選択します。求められたら、Citrix アカウント資格情報を入力します。

資格情報が確認されたら（あるいは参加しないことを選択した場合）、［次へ］を選択します。

詳しくは、「Call Home」を参照してください。

手順 **11**：このインストールを完了する



［完了］ページに、すべての前提条件と正常にインストールおよび初期化されたコンポーネントが緑色のチェックマークで示されます。

［完了］を選択します。デフォルトでは、マシンは自動的に再起動します自動再起動を無効にすることもできますが、マシンを再起動するまで VDA は使用できません。

（イメージではなく）個々のマシンに VDA をインストールする場合は、必要に応じて上記の手順を繰り返し、残りのマシンに VDA をインストールします。

トラブルシューティング

デリバリーグループの ［管理］**>**［完全な構成］画面では、詳細ペインの ［インストール済み **VDA** のバージョン］エントリがマシンにインストールされているバージョンではないことがあります。マシンの Windows の［プログラムと機能］には、VDA の実際のバージョンが表示されます。

Citrix Optimizer

Citrix Optimizer は、さまざまなコンポーネントを削除して最適化することで、Citrix の管理者が VDA を最適化できるよう支援する Windows OS 用のツールです。

VDA をインストールして最後の再起動を完了したら、Citrix Optimizer をダウンロードしてインストールします。CTX224676を参照してください。CTX の記事には、ダウンロードパッケージに加えて、Citrix Optimizer のインストールと使用に関する手順が含まれています。

VDA のカスタマイズ

インストールした VDA を後でカスタマイズする（情報を変更する）には:

1. プログラムの削除と変更を行う Windows のコントロールパネルで、[**Citrix Virtual Delivery Agent**] または [**Citrix Remote PC Access/VDI Core Services VDA**] を選択します。次に右クリックして [変更] を選択します。
2. [**Virtual Delivery Agent** 設定のカスタマイズ] を選択します。

インストーラーが起動したら、使用可能な設定を変更します。

Cloud Connector と通信するためのポートのカスタマイズ

特定のセキュリティ要件に基づいて、VDA が Cloud Connector との通信に使用するポートをカスタマイズできます。この機能は、セキュリティチームがデフォルトポート（ポート 80）を開くことを許可していない場合、またはデフォルトポートが既に使用されている場合に役立ちます。

ポートをカスタマイズするには、次の手順を実行します:

1. Citrix Cloud Connector に Controller ポート番号を追加します。
2. VDA に VDA ポート番号を追加します。

Citrix Cloud Connector に Controller ポート番号を追加

Citrix Cloud Connector に移動し、次の 2 つの PowerShell コマンドを実行します:

- `PS C:\> & 'C:\Program Files\Citrix\XaXdCloudProxy\XaXdCloudProxy.exe'-VdaPort <port number>`
- `PS C:\> & 'C:\Program Files\Citrix\Broker\Service\HighAvailabilityService.exe'-VdaPort <port number> -ConfigureFirewall`

例:

- `PS C:\> & 'C:\Program Files\Citrix\XaXdCloudProxy\XaXdCloudProxy.exe'-VdaPort 18000`
- `PS C:\> & 'C:\Program Files\Citrix\Broker\Service\HighAvailabilityService.exe'-VdaPort 18000 -ConfigureFirewall`

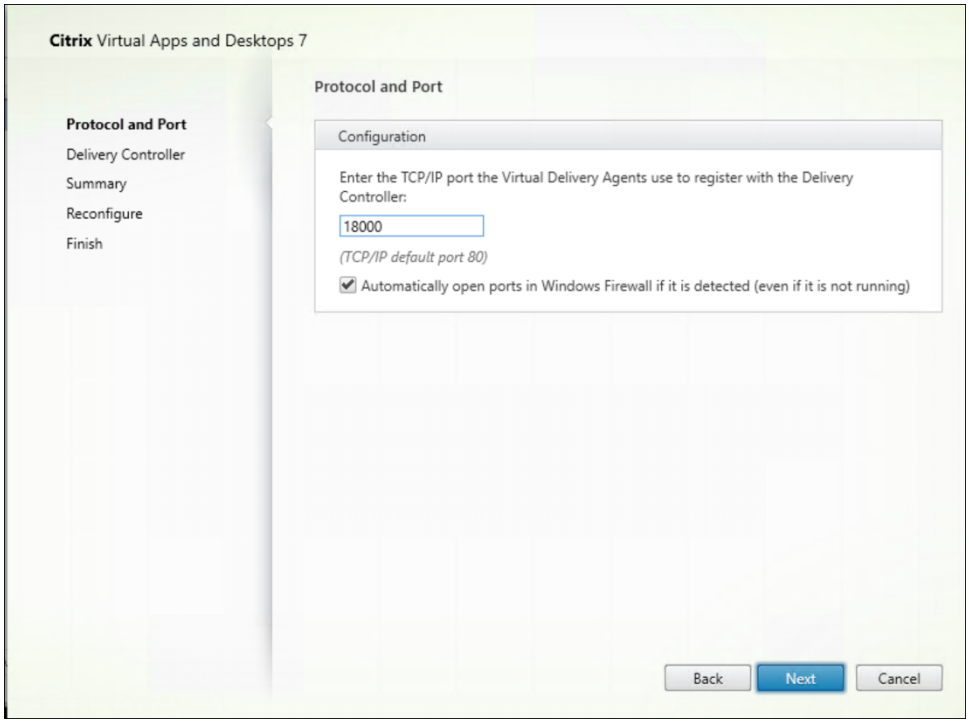
ポートをカスタマイズするときは、次の点を考慮してください:

- 両方のコマンドで同じポート番号を使用する必要があります。
- すべての *Cloud Connector* で両方のコマンドを実行する必要があります。
- Cloud Connector と正常に通信するには、すべての VDA が同じポート番号を使用していることを確認してください。
- 構成したポートは、コネクタの更新後も保持されます。

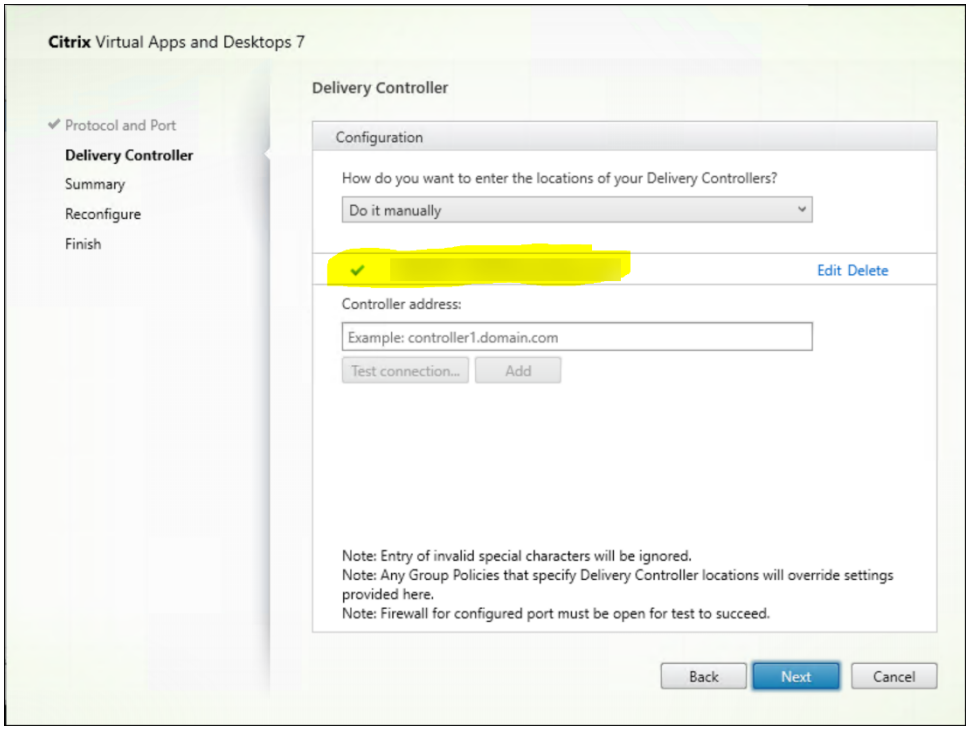
VDA に **VDA** ポート番号を追加

デフォルト設定で VDA をインストールし、次のように構成します。VDA が既にインストールされている場合は、以下の手順に進みます。

1. VDA で、`C:\Program Files\Citrix\XenDesktopVdaSetup\XenDesktopVdaSetup.exe` にある **XenDesktopVdaSetup.exe** を開きます。
2. [プロトコルとポート] ページで、カスタムポート番号を追加します。



3. [**Delivery Controller**] ページで、Controller の FQDN を入力します。



4. ［次へ］をクリックしてウィザードを続行し、構成を完了します。

その後、ポート番号は正常に再構成されます。

> 注:
>
> Controller 接続をテストすると、次のエラーメッセージが表示される場合があります: < 入力した Controller アドレス > に実行中の Controller インスタンスがありません。アドレスが正しい場合は、メッセージを閉じることができます。入力した Controller アドレス >

トラブルシューティング

カスタムポートが正しく構成されているかどうかを確認するには、Cloud Connector に移動して、次のトラブルシューティング手順を実行します:

1. 次の 2 つのレジストリキーが存在することを確認します。

   HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XaXdCloudProxyPersist
   名前: CustomVDAPortNumber
   タイプ: REG_DWORD
   データ: 18000

   HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XaXdCloudProxyPersist
   名前: CustomVDAPortNumberHA
   タイプ: REG_DWORD
   データ: 18000

2. 次のコマンドを実行して、.txt ファイルを作成します。

   - `netsh http show urlacl > <filepath>.txt`

   例:

   - `netsh http show urlacl > c:\reservations.txt`

3. .txt ファイルを開き、次の 4 つの URL をチェックして、正しいポートが使用されていることを確認します。

   - `http://+:18000/Citrix/CdsController/IRegistrar/`
   - `http://+:18000/Citrix/CdsController/ITicketing/`
   - `http://+:18000/Citrix/CdsController/IDynamicDataSink/`
   - `http://+:18000/Citrix/CdsController/INotifyBroker/`

4. 次の 2 つのファイアウォールの規則が作成され、必要なポートが開いていることを確認します。

   - Citrix XaXdProxy
   - Citrix Broker Service（TCP-In）

その他の情報

- VDA をインストールした後、Cloud Health Checkを使用してサイトとそのコンポーネントの正常性と可用性を確認できます。

次の手順

マシンカタログを作成します。

構成プロセスの全体像については、「展開の計画と構築」を参照してください。

コマンドラインを使用した **VDA** のインストール

June 9, 2023

はじめに

この記事の対象は、Windows オペレーティングシステムがインストールされたマシンでの Virtual Delivery Agent（VDA）のインストール、アップグレード、カスタマイズです。

この記事では、VDA のインストールコマンドの実行方法について説明します。インストールを始める前に、「VDA のインストール」を参照して、インストールに関する考慮事項、インストーラー、インストール中に指定する内容について確認してください。

コマンドラインによる **VDA** のインストール

VDA のインストールおよびコマンド実行の進行状況と戻り値の確認を行うには、管理権限を持っているか、［管理者として実行］を使用する必要があります。

1. VDA をインストールするマシンで、Citrix Cloudにサインインします。
2. 左上のメニューで、［マイサービス］**>** ［**DaaS**］を選択します。
3. 右上の ［ダウンロード］をクリックし、［**VDA** のダウンロード］を選択します。VDA ダウンロードページにリダイレクトされます。目的の VDA インストーラーを見つけて、［ファイルのダウンロード］をクリックします。
4. ダウンロードが完了したら、ダウンロードしたファイル名を指定して実行します。この記事で説明するオプションを使用してください。
   - マルチセッション OS Virtual Delivery Agent の場合は、`VDAServerSetup.exe`を実行します。
   - シングルセッション OS Virtual Delivery Agent の場合は、`VDAWorkstationSetup.exe`を実行します。
   - シングルセッション OS Core Services Virtual Delivery Agent の場合は、`VDAWorkstationCoreSetup.exe`を実行します。

インストール前にファイルを展開するには、絶対パスを指定して`/extract`を実行します（例：`.\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia`）。（ディレクトリはあらかじめ存在する必要があります。それ以外の場合、抽出は失敗します。）次に、別のコマンドで、この記事に記載されている有効なオプションを使用して、適切なコマンドを実行します。

- `VDAServerSetup_XXXX.exe`については、`<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`を実行します。
- `VDAWorkstationCoreSetup_XXXX.exe`については、`<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopRemotePCSetup.exe`を実行します。
- `VDAWorkstationSetup_XXXX.exe`については、`<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`を実行します。

VDA のインストールで使用するコマンドラインオプション

次のオプションは、`VDAServerSetup.exe`、`VDAWorkstationSetup.exe`、`VDAWorkstationCoreSetup.exe`の各コマンドの 1 つ以上で使用できます。

- **/components** *component*[,*component*]

  インストールまたは削除するコンポーネントをコンマ区切りのリストで指定します。以下の値を指定します：

  - **VDA**: Virtual Delivery Agent
  - **PLUGINS**: Windows 向け Citrix Workspace アプリ

  VDA および Citrix Workspace アプリをインストールするには、「/components vda,plugins」と指定します。

  pluginsオプションを指定しない場合、VDA のみがインストールされます（Citrix Workspace アプリはインストールされません）。

  このオプションは、VDAWorkstationCoreSetup.exeインストーラーを使用している場合無効です。このインストーラーでは、Citrix Workspace アプリはインストールできません。

- **/controllers** *"controller* [*controller*]…"

  VDA が通信可能な Citrix Cloud Controller の FQDN を、直線の二重引用符で囲んだスペース区切りのリストで指定します。/site_guidと/controllersの両方を指定しないでください。

- **/disableexperiencemetrics**

  インストール、アップグレード、または削除中に収集される分析の Citrix への自動アップロードが阻止されます。

- **/enable_hdx_ports**

  Windows ファイアウォールサービスが実行されている場合に（ファイアウォールが無効になっていても）、VDA および有効な機能 (Windows リモートアシスタンスは除く) で必要なポートが開放されます。Windows 以外のファイアウォールを使用している場合は、手作業でファイアウォールを構成する必要があります。ポートについて詳しくは、「ネットワークポート」を参照してください。

  HDX アダプティブトランスポートが使用する UDP ポートを解放するには、/enable_hdx_portsに加えて、/enable_hdx_udp_portsを指定します。

- **/enable_hdx_udp_ports**

  Windows ファイアウォールサービスが検出された場合に（ファイアウォールが無効になっていても）、HDX アダプティブトランスポートが必要とする UDP ポートが Windows ファイアウォールで開放されます。Windows 以外のファイアウォールを使用している場合は、手作業でファイアウォールを構成する必要があります。ポートについて詳しくは、「ネットワークポート」を参照してください。

  VDA が使用するポートを解放するには、/enable_hdx_udp_portsに加えて、/enable_hdx_portsを指定します。

- **/enable_real_time_transport**

  オーディオパケットで UDP を使用してパフォーマンスを向上させる機能（RealTime Audio Transport）を有効または無効にします。この機能を有効にすると、オーディオパフォーマンスを向上させることができます。Windows ファイアウォールサービスが検出されたときに UDP ポートが開放されるようにするには、/enable_hdx_portsを指定してください。

- **/enable_remote_assistance**

  監視機能で使用する Windows リモートアシスタンスのシャドウ機能を有効にします。このオプションを指定すると、Windows リモートアシスタンスによってファイアウォールで動的ポートが解放されます。

- **/enablerestore** または**/enablerestorecleanup**

  （シングルセッション VDA にのみ有効）これにより、VDA のインストールまたはアップグレードが失敗した場合に、復元ポイントへの自動復帰が有効になります。

  インストールまたはアップグレードが正常に完了した場合：

  - /enablerestorecleanupは、復元ポイントを削除するようインストーラーに指示します。
  - /enablerestoreは、復元ポイントが使用されなかった場合でも、その復元ポイントを維持するようインストーラーに指示します。

  詳しくは、「インストールまたはアップグレードの失敗時の復元」を参照してください。

- **/enable_ss_ports**

  Windows ファイアウォールサービスが検出された場合に（ファイアウォールが無効になっていても）、画面共有に必要なポートが Windows ウォールで開放されます。Windows 以外のファイアウォールを使用している場合は、手作業でファイアウォールを構成する必要があります。

- **/exclude** “*component*”[,”*component*”]

  二重引用符で囲まれた、オプションコンポーネントをインストールしません。複数のコンポーネントを指定する場合は、カンマで区切って、それぞれ直線の二重引用符で囲みます。たとえば、MCS 管理のイメージ上で VDA をインストールまたはアップグレードするには、Machine Identity Service コンポーネントが必要です。以下の値を指定します：

  - Machine Identity Service
  - Citrix Profile Management
  - Citrix Profile Management WMI プラグイン
  - Citrix Personalization for App-V - VDA
  - Citrix Supportability Tools
  - Citrix MCS IODriver
  - Citrix VDA Upgrade Agent
  - Citrix Rendezvous V2

  インストール対象（/exclude "Citrix Profile Management"）から Citrix Profile Management を除外すると、［監視］タブでの VDA の監視やトラブルシューティングに影響が生じます。［ユーザーの詳細］ページの［個人設定］パネル、および ［エンドポイント］ページの［ログオン処理時間］パネルに不具合が発生します。［ダッシュボード］ページと ［傾向］ページでは、Profile Management がインストールされているマシンについてのデータしか［平均ログオン処理時間］パネルに表示されません。

サードパーティのユーザープロファイル管理ソリューションを使用している場合でも、Citrix では、Citrix Profile Management サービスをインストールして実行することをお勧めします。Citrix Profile Management Service の有効化は、必須ではありません。

MCS を使用して VM をプロビジョニングする場合は、Machine Identity Service を除外しないでください。

/excludeおよび/includeadditionalの両方に同じコンポーネント名を指定した場合、そのコンポーネントはインストールされません。

このオプションは、VDAWorkstationCoreSetup.exeインストーラーを使用している場合無効です。そのインストーラーは、これらの項目の多くを自動的に除外します。

- **/h** または **/help**

  コマンドのヘルプを表示します。

- **/includeadditional** “*component*” [,” *component*”] …

  インストールするオプションコンポーネントを 1 つ以上、それぞれ直線の二重引用符で囲みコンマ区切りで指定します。コンポーネント名の大文字と小文字は区別されます。

  このオプションを使用すると、リモート PC アクセス展開を作成する場合に、デフォルトでは含まれないコンポーネントをインストールできます。以下の値を指定します:

  - Citrix Profile Management
  - Citrix Profile Management WMI プラグイン
  - Citrix Personalization for App-V - VDA
  - Citrix Supportability Tools
  - Citrix MCS IODriver
  - Citrix VDA Upgrade Agent
  - Citrix Rendezvous V2
  - ユーザー個人設定レイヤー
  - Citrix WebSocket VDA 登録ツール

  /excludeおよび/includeadditionalの両方に同じコンポーネント名を指定した場合、そのコンポーネントはインストールされません。

- **/installdir** *directory*

  コンポーネントのインストール先として既存の空ディレクトリを指定します。デフォルト値: c:\Program Files\Citrix

- **/install_mcsio_driver**

  使用しないでください。代わりに、/includeadditional "Citrix MCS IODriver"または/exclude "Citrix MCS IODriver"を使用してください。

- **/logpath** *path*

ログファイルのパスを指定します。既存のフォルダーを指定する必要があります。インストーラーによって作成されません。Default = 「%TEMP%\Citrix\XenDesktop Installer」

このオプションはグラフィカルインターフェイスでは使用できません。

- **/masterimage**

  仮想マシン上に VDA をインストールする場合にのみ有効です。VDA をイメージとしてセットアップします。このオプションは/mastermcsimageと同等です。

  このオプションは、VDAWorkstationCoreSetup.exeインストーラーを使用している場合無効です。

- **/mastermcsimage**

  インストールするマシンを、Machine Creation Services で使用するイメージに指定します。このオプションは/masterimageと同等です。

- **/masterpvsimage**

  インストールするマシンを、Citrix Provisioning またはサードパーティのプロビジョニングツール（Microsoft System Center Configuration Manager など）で使用するイメージに指定します。

- **/no_mediafoundation_ack**

  Microsoft の Media Foundation がインストールされていなければ、複数の HDX マルチメディア機能はインストールされず、動作しないものがあることを認識します。このオプションが省略されていて、Media Foundation がインストールされていない場合、VDA インストールは失敗します。サポートされているほとんどの Windows のエディションには、N エディションの例外を除けば、Media Foundation が既にインストールされています。

- **/nodesktopexperience**

  マルチセッション OS VDA をインストールする場合にのみ有効です。デスクトップエクスペリエンス拡張機能を無効にします。この機能の有効/無効は、Citrix ポリシー設定の［拡張デスクトップエクスペリエンス］でも制御できます。

- **/noreboot**

  インストール後の再起動を無効にします。VDA は、再起動後にのみ使用できます。

- **/noresume**

  デフォルトでは、インストール中にマシンの再起動が必要になった場合、再起動が完了すると自動的にインストーラーが再開します。デフォルトを上書きするには、/noresumeを指定します。これは、メディアを再マウントする必要がある場合、または自動インストール中に情報をキャプチャする必要がある場合に役立ちます。

- **/portnumber** *port*

  /reconfigオプションを指定する場合にのみ有効です。Virtual Delivery Agent と Controller 間の通信で使用されるポート番号を変更します。変更前のポートは無効になります（ポート 80 を除く）。

- **/proxyconfig** “アドレスまたは *PAC* ファイルパス”

  コマンドに/includeadditional "Citrix Rendezvous V2"が含まれている場合にのみ有効です。Rendezvous プロトコルで使用するためのプロキシのアドレス、または PAC ファイルパス。機能について詳しくは、「Rendezvous プロトコル」を参照してください。

  - プロキシアドレスの形式：http://<url-or-ip>:<port>
  - PAC ファイルの形式：http://<url-or-ip>:<port>/<path>/<filename>.pac

- **/quiet** または **/passive**

  ユーザーインターフェイスを表示せずにインストールを実行します。インストールおよび構成プロセスは、Windows タスクマネージャーにのみ表示されます。このオプションを指定しない場合、インストールウィザードが表示されます。

- **/reconfigure**

  インストール済みの Virtual Delivery Agent 設定をカスタマイズします。/portnumber、/controllers、または/enable_hdx_portsオプションと一緒に使用します。/quietオプションを指定しない場合は、VDA をカスタマイズするためのグラフィカルインターフェイスが開きます。

- **/remotepc**

  リモート PC アクセス展開（シングルセッション OS）または仲介接続（マルチセッション OS）でのみ有効です。

  このオプションは、VDAWorkstationCoreSetup.exeインストーラーを使用している場合無効です。このインストーラーは、上記のコンポーネントのインストールを自動的に除外します。

- **/remove_appdisk_ack**

  AppDisks VDA プラグインがインストールされている場合、それをアンインストールする権限を VDA インストーラーに与えます。

- **/remove_pvd_ack**

  Personal vDisk がインストールされている場合、それをアンインストールする権限を VDA インストーラーに与えます。

- **/remove**

  /componentsオプションで指定したコンポーネントを削除します。

- **/removeall**

  VDA を削除します。Citrix Workspace アプリは削除されません（インストールされている場合）。

- **/sendexperiencemetrics**

  Citrix Insight Services へのインストール、アップグレード、または削除中に収集される分析が自動的に送信されます。これが省略される場合（または/disableexperiencemetricsが指定される場合）、分析はローカルで収集されますが、自動的には送信されません。

- **/servervdi**

  サポートされる Windows サーバーにシングルセッション OS VDA をインストールします。Windows サーバー上にマルチセッション VDA をインストールする場合は、このオプションを指定しないでください。このオプションを使用する前に、「サーバー VDI」を参照してください。

- **/site_guid** *guid*

  サイトの Active Directory 組織単位（OU）のグローバル一意識別子（GUID）を指定します。Active Directory OU ベースの Controller 検出を使用する場合、GUID により仮想デスクトップとサイトが関連付けられます（デフォルトの検出方法である自動更新を使用することをお勧めします）。サイト GUID は、［管理］**>**［完全な構成］に表示されるサイトプロパティです。/site_guidと/controllersの両方を指定しないでください。

- **/tempdir** *directory*

  インストール時に一時ファイルを作成するディレクトリを指定しますデフォルト値：c:\Windows\Temp

  このオプションはグラフィカルインターフェイスでは使用できません。

- **/virtualmachine**

  仮想マシン上に VDA をインストールする場合にのみ有効です。インストーラーによる物理マシンの検出を上書きして、BIOS 情報を仮想マシンに渡して物理マシンとして振る舞うようにします。

  このオプションはグラフィカルインターフェイスでは使用できません。

- **/xendesktopcloud**

  VDA が Citrix DaaS（Citrix Cloud）展開にインストールされていることを示します。

例：**VDA** のインストール

- マルチセッション **OS** に **VDA** をインストールします。次のコマンドでは、マルチセッション OS に VDA をインストールします。

  ```
  VDAServerSetup.exe /quiet /controllers "Contr-East.domain.com"/
  enable_hdx_ports /masterimage
  ```

  VDA はイメージとして使用されます。

- マルチセッション **OS VDA** またはシングルセッション **OS VDA** をインストールします。次のコマンドは、マルチセッション OS VDA またはシングルセッション OS VDA をインストールします。

  ```
  VDAServerSetup_XXXX.exe /quiet /controllers "ddc1.abc.com",
  "ddc2.abc.com"/enable_hdx_ports /enable_Remote_Assistance /
  enable_real_time_transport /enable_ss_ports /noreboot
  ```

  各 Delivery Controller FQDN はコンマで区切ります。XXXXは VDA のバージョンを表しています。

- **Core Services VDA** をシングルセッション **OS** にインストールします。次のコマンドは、リモート PC アクセスまたは VDI 展開で使用するためにシングルセッション OS に Core Services VDA をインストールします。

  ```
  VDAWorkstationCoreSetup.exe /quiet /controllers "Contr-East.
  domain.com"/enable_hdx_ports /noreboot
  ```

  Citrix Workspace アプリとその他の非コアサービスはインストールされません。Cloud Connector のアドレスが指定され、Windows ファイアウォールサービスのポートが自動的に開放されます。管理者が再起動を処理します。

コマンドラインを使った **VDA** のカスタマイズ

VDA をインストールした後で、いくつかの設定をカスタマイズできます。次のオプションの 1 つまたは複数を使用して、`XenDesktopVDASetup.exe`を実行します。

- `/reconfigure`（VDA をカスタマイズする場合は必須のオプションです）
- `/h` または `/help`
- `/quiet`
- `/noreboot`
- `/controllers`
- `/portnumber port`
- `/enable_hdx_ports`

次の手順

- マシンカタログの作成
- 構成プロセスの全体像については、「展開の計画と構築」を参照してください。

接続とリソースの作成と管理

February 19, 2024

はじめに

接続の構成作業としては、サポートされているハイパーバイザーとクラウドサービスのリストから接続タイプを選択する作業、およびその接続について、適切なストレージとネットワークリソースを選択する作業が含まれます。

> 注:
>
> 接続とリソースの管理に関連するタスクを実行するには、すべての管理権限が必要です。

接続の種類に関する情報の参照先

「システム要件」には、サポートされているハイパーバイザーとクラウドサービスのバージョンのリストと、ホスト固有の情報へのリンクが記載されています。

ホストストレージ

ストレージ製品は、サポートされているハイパーバイザーで管理される場合にサポートされます。Citrix サポートでは、問題のトラブルシューティングや解決を行い、必要に応じてそれらの問題と解決策を Knowledge Center に文書化する場合にのみストレージ製品ベンダーにサポートを提供します。

マシンのプロビジョニング時、データは種類別に分類されます:

- オペレーティングシステム（OS）: イメージを含む
- 以下を含む一時データ: MCS でプロビジョニングされたマシンに書き込まれるすべての非永続データ、Windows ページファイル、および ShareFile と同期されるすべてのデータ。このデータは、マシンの再起動のたびに破棄されます。基本イメージにユーザープロファイルデータが含まれている場合、そのデータは永続するものとなります。一元管理型ユーザープロファイルソリューションを使用している場合、ユーザープロファイルデータは外部プロファイルストアと同期されます。ローカルにキャッシュされているユーザープロファイルデータは、マシンが再起動されるたびに破棄されます。

データの種類ごとに個別のストレージリソースを割り当てることで、システム負荷を最小限に抑え、IOPS（1 秒あたりの入出力演算回数）のパフォーマンスを向上させることができます。この戦略的な割り当てにより、ホストの利用可能なリソースが最適に利用されます。また、データの種類ごとの固有ニーズ（例: 永続性や回復性の向上）に基づいて最適なストレージメディアを選択することもできます。

- 共有およびローカルストレージオプション: ストレージ リソースは、集中管理する、つまり特定のホストに限定せずにすべてのホストで使用することも、特定のハイパーバイザーに限定することもできます。一元管理型のオプションの中には、Windows クラスター共有ボリュームが含まれています。さらに、Windows クラスター共有ボリュームには、ストレージベンダーの追加のアプライアンスや接続ストレージがある場合とない場合があります。一元管理型のストレージソリューションは、ハイパーバイザー固有のストレージ制御パスやプラグインへの直接アクセスなど、先進的な最適化機能を提供することができます。
- ローカルストレージの利点とトレードオフ: 一時データをローカルに保存することにより、共有ストレージにアクセスするためにネットワークにアクセスする必要がなくなるので、共有リソースの IOPS 負荷が軽減されます。一元管理型のストレージが高コストになる可能性があるのに対し、ローカルストレージの使用はコスト効率の高い代替オプションとなります。こうした利点は、ハイパーバイザーサーバー上で十分なストレージを使用できることよりも重要になるでしょう。

ハイパーバイザー間で共有されるストレージ

ハイパーバイザー間でストレージを共有する方法では、長期間保持する必要のあるデータが保存され、バックアップおよび管理を一元的に行うことができます。このストレージは OS ディスクを保持します。

この方法を選択する場合、一時マシンデータに（同じハイパーバイザープール内のサーバー上の）ローカルストレージを使用するかどうかを選択できます。このデータは、共有ストレージ内のデータほど永続性や復元性を必要としません。これは一時データキャッシュと呼ばれます。ローカルディスクを使用することにより、メイン OS ストレージへのトラフィックが軽減されます。このディスクは、マシンの再起動のたびにクリアされます。ディスクは、ライトスルーメモリキャッシュを介してアクセスされます。一時データにローカルストレージを使用すると、プロビジョニングされた VDA は特定のハイパーバイザーホストに関連付けられることに注意してください。このホストで障害が生じると、VM を起動できなくなります。

例外：クラスターストレージボリューム（CSV）を使用する場合、Microsoft System Center Virtual Machine Manager で、ローカルストレージに一時データキャッシュディスクを作成することはできません。

一時データをローカルに保存する場合、この接続を使用するマシンカタログを作成する際に、各仮想マシンのキャッシュディスクとメモリのサイズにデフォルト以外の値を有効にして構成することができます。ただし、デフォルト値は接続の種類に適切な値に設定されており、ほとんどの場合はデフォルト値で十分です。

また、ハイパーバイザーはディスクイメージのローカルなインメモリ読み取りキャッシュによる最適化テクノロジを提供します。（例：XenServer の IntelliCache）。これも、中央ストレージへのネットワークトラフィックを軽減します。

ハイパーバイザーのローカルに配置するストレージ

ストレージをハイパーバイザーのローカルに配置する方法では、データはハイパーバイザー上にローカルで保存されます。この方法を使用する場合、最初のマシン作成時およびその後のイメージ更新時に、イメージおよびほかの OS データはサイトで使用されるすべてのハイパーバイザーに転送されます。これにより、管理ネットワークでかなりのトラフィックが生じます。イメージ転送も時間がかかる処理であり、各ホストでイメージを利用できるようになるタイミングも異なります。

接続とリソースの作成

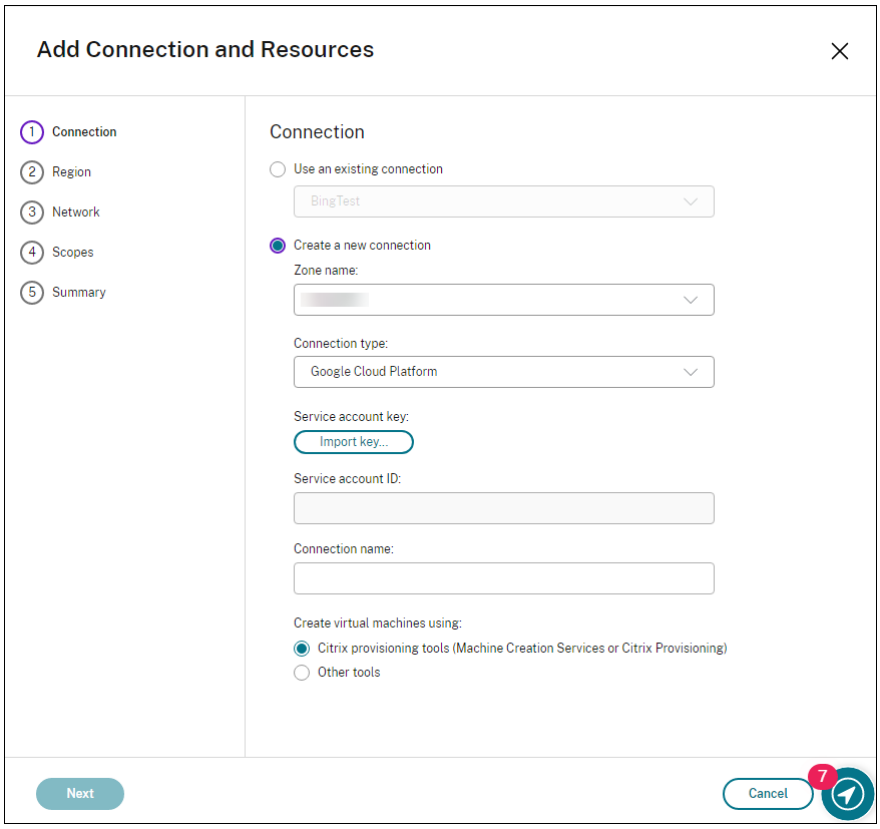
> 重要：
>
> 接続を作成する前に、リソースの場所にホストリソース（ストレージとネットワーク）を用意する必要があります。

1. Citrix Cloud にサインインします。
2. 左上のメニューに移動し、［マイサービス］**>**［**DaaS**］を選択します。
3. ［管理］**>**［完全な構成］の左側ペインで ［ホスト］を選択します。
4. 操作バーの ［接続およびリソースの追加］をクリックします。

5. 表示されるウィザードは、次の手順に示す構成プロセスをガイドします。特定のページの内容は、選択した接続の種類によって異なります。各ページでは、手順を終えたら、［概要］ページに到達するまで ［次へ］を選択します。

> 注:
>
> ウィザード内の各ページの内容は、選択した接続の種類に応じて異なってきます。

手順 **1**: 接続



［接続］ページで以下を実行します:

- 新しい接続を作成するには、［新しい接続を作成する］をクリックします。既存の接続と同じホスト構成に基づいて接続を作成する場合は、［既存の接続を使用する］を選択してから該当の接続を選択します。
- ［ゾーン名］フィールドでゾーンを選択します。選択できるオプションは、構成したすべてのリソースの場所です。
- ［接続の種類］フィールドで、ハイパーバイザーまたはクラウドサービスを選択します。このフィールドの設定値としては、Citrix がサポートするすべてのハイパーバイザーとクラウドサービスがあります:
  - アクセス可能な Cloud Connetor がリソースの場所にない場合は、コネクタを使用しない展開をサポートするハイパーバイザーとクラウドサービスだけが利用可能です。

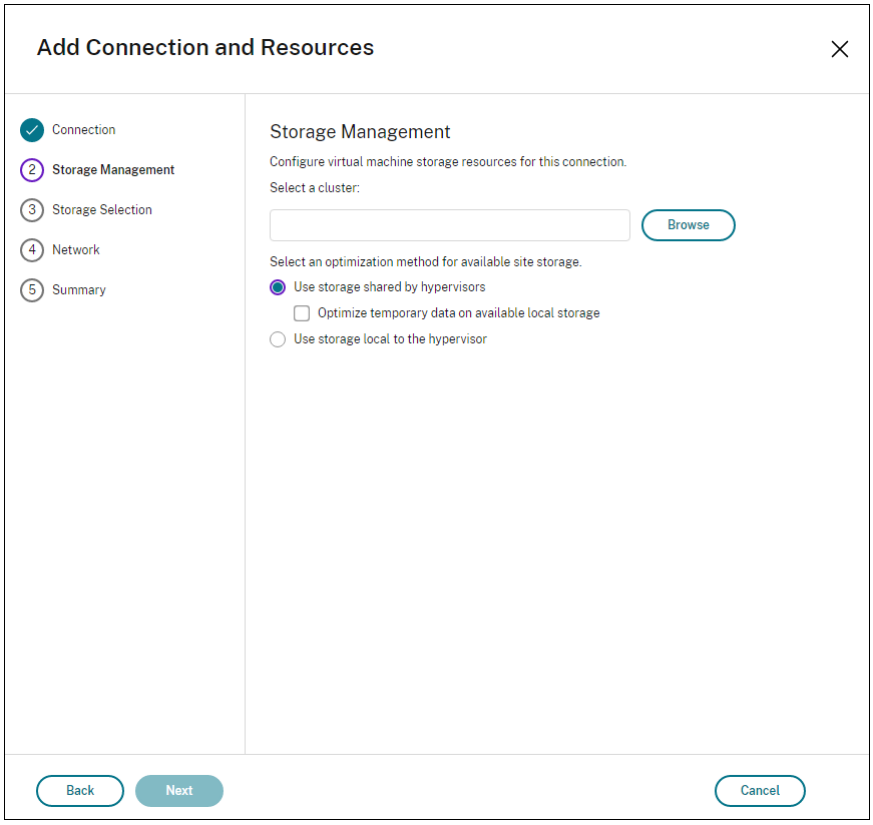
- アクセス可能な Cloud Connetor がリソースの場所にある場合は、それらの Connetor にプラグインが正しくインストールされているハイパーバイザーとクラウドサービスだけが利用可能です。

または、PowerShell コマンド「`Get-HypHypervisorPlugin [-ZoneUid] $rluid [-IncludeUnavailable]` false または true」を使用して、利用可能なハイパーバイザーとクラウドサービスの一覧を出力することもできます。

- 接続名を入力します。入力した名前はホスト画面に表示されます。
- 仮想マシンを作成するツールを選択します。

> 注:
>
> [接続] ページの情報は、使用する接続の種類またはホストによって異なります。たとえば、Azure Resource Manager を使用する場合、既存のサービスプリンシパルを使用するか、新しいサービスプリンシパルを作成できます。詳しくは、「Microsoft Azure への接続」を参照してください。

手順 **2**: ストレージの管理



ストレージ管理の種類と方法について詳しくは、「ホストストレージ」を参照してください。

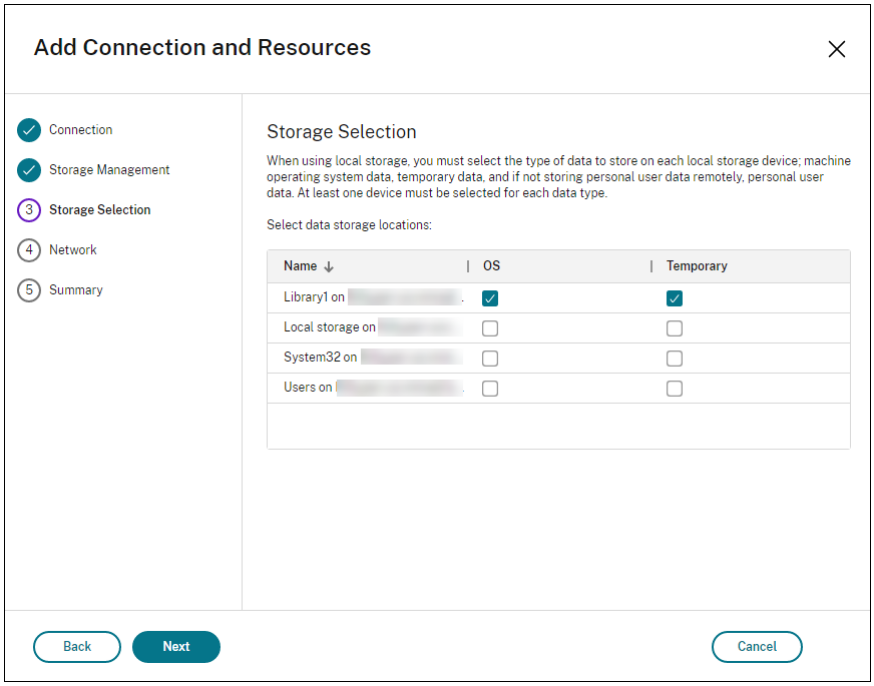
Hyper-V または VMware ホストに対する接続を構成している場合は、クラスター名を参照してから選択します。他の接続の種類では、クラスター名は要求されません。

ストレージ管理方法（ハイパーバイザー間で共有されるストレージまたはハイパーバイザーのローカルに配置するストレージ）を選択します。

詳しくは、「ハイパーバイザー間で共有されるストレージ」および「ハイパーバイザーのローカルに配置するストレージ」を参照してください。

XenServer プール上で共有ストレージを使用する場合は、IntelliCache を使用して共有ストレージデバイスにかかる負荷を減らすかどうかを指定します。「XenServer 接続での IntelliCache の使用」を参照してください。

手順 **3**：ストレージの選択



ストレージの選択について詳しくは、「ホストストレージ」を参照してください。

使用可能なデータの種類ごとに 1 つ以上のストレージデバイスを選択します。前のページで選択したストレージ管理方法によって、このページで選択できるデータの種類が変化します。ウィザードの次のページに進むには、サポートされる各データの種類に対して 1 つ以上のストレージデバイスを選択する必要があります。

[**Storage Management**] ページで ［利用可能なローカルストレージ上で一時データを最適化します］と ［ハイパーバイザーによって共有されるストレージ］をオンにした場合、［ストレージの選択］ページの下部に表示される構成オプションが増えます。たとえば、一時データに使用する（同じハイパーバイザープールにある）ローカルストレージデバイスを選択できます。

現在選択中のストレージデバイスの数が表示されます（上図では「1 個のストレージデバイスが選択されました」）。このエントリの上にマウスを合わせると、選択したデバイスの名前が表示されます（構成されたデバイスがある場合のみ）。

1. 使用するストレージデバイスを変更するには ［選択］を選択します。

2. ［ストレージの選択］ダイアログボックスで、ストレージデバイスのチェックボックスをオンまたはオフにして［**OK**］を選択します。

手順 **4**：リージョン

> 注：
>
> ［リージョン］ページは、一部のホストタイプに対してのみ表示されます。

リージョンの選択内容によって、VM の展開先が決まります。可能であれば、アプリケーションにアクセスするユーザーの場所に近いリージョンを選択してください。

手順 **5**：ネットワーク

リソースの名前を入力します。この名前は［管理］コンソールに表示され、これにより接続に関連付けられたストレージとネットワークの組み合わせを識別できます。

仮想マシンで使用するネットワークを 1 つまたは複数選択します。

一部の接続の種類（Azure Resource Manager など）では、VM が使用するサブネットも表示されます。サブネットを 1 つまたは複数選択します。

手順 **6**：まとめ

選択内容を確認します。変更を行う場合は、前のウィザードページに戻ります。確認が完了したら、［完了］を選択します。

> 注：
>
> - 一時データをローカルに保存する場合、この接続を使用するマシンを含むカタログを作成するときに、一時データストレージにデフォルト以外の値を設定できます。
> - フルアクセス権管理者については、スコープは表示されません。詳しくは、「管理者、役割、およびスコープ」を参照してください。

接続の設定の編集

この手順は、次のことには使用できません：

- 接続の名前を変更するか、新しい接続を作成すること。
- 接続の GPU 設定を変更すること。このリソースにアクセスするカタログでは、適切な GPU 固有のイメージを使用する必要があります。したがって、GCP 設定を変更する場合は、既存の接続を編集するのではなく、新規の接続を作成します。

接続の編集

1. ［管理］**>**［完全な構成］の左側ペインで ［ホスト］を選択します。
2. 接続を選択し、操作バーの ［接続の編集］を選択します。
3. ［接続のプロパティ］ページで、接続アドレスと資格情報を変更します。現在のホストマシンに新しいアドレスがある場合にのみ、アドレスを変更します。別のマシンへのアドレスを入力すると、接続のマシンカタログが壊れます。

    - ［設定の編集…］を選択し、新しい情報を入力します。
    - XenServer 接続に対して高可用性サーバーを指定する場合は、［設定の編集…］でサーバーを選択します。プールマスターに障害が生じても XenServer との通信が中断されないように、プール内のすべてのサーバーを選択することをお勧めします。

        > 注:
        >
        > HTTPS を使用していて、高可用性サーバーを構成する場合は、ワイルドカード証明書をプール内のすべてのサーバーにインストールしないようにしてください。サーバーごとに個別の証明書が必要です。詳しくは、「XenServer への接続を作成する」を参照してください。

4. ［詳細設定］ページを使用して設定を編集し、ホスト接続ごとの同時アクション（または同時実行マシン）の最大数を指定します。電源管理設定で同時に起動するマシンの数が多すぎたり少なすぎたりする場合に、この設定を行います。接続の種類のそれぞれには固有のデフォルト値が設定されています。これらの値は、ほとんどのケースで適切であり、通常は変更する必要はありません。

    - ［同時操作（すべての種類）］と ［**Personal vDisk** ストレージインベントリの同時更新］設定について、この接続で同時に実行できる操作の最大数を絶対値で、すべてのマシンのうちこの接続を使用できる最大マシン数をパーセンテージで指定します。絶対値とパーセンテージ値の両方が必要です。実際に適用される制限は、いずれか値の小さい方になります。

        たとえば、［同時操作（すべての種類）］の絶対値が 10、パーセンテージ値が 10、この接続の総仮想マシン数が 34 の場合、実際に適用される上限値は、絶対値の 10 よりも小さい、34 の 10% を四捨五入した 3 になります。

    - ［**1** 分あたりの最大新規操作］は、絶対値です。パーセンテージ値はありません。
    - ［接続オプション］への情報の入力は、Citrix サポート担当者からの指示があった場合だけ行ってください。

5. ［スコープ］ページを使用して、このホストに対して 1 つ以上のスコープを選択します。

    > 注:
    >
    > フルアクセス権管理者については、スコープは表示されません。定義上は、これらの管理者は、顧客が管

> 理する Citrix Cloud、およびサブスクライブしているサービスのオブジェクトすべてにアクセスできます。

詳しくは、「管理者、役割、およびスコープ」を参照してください。

6. ［共有テナント］ページを使用して、この接続のサブスクリプションと Azure Compute Gallery を共有しているテナントとサブスクリプションを追加します。

   a) この接続に関連付けられているアプリケーションのアプリケーションシークレットを入力します。この情報を使用して、Azure に認証できます。セキュリティを確保にするために、キーを定期的に変更することをお勧めします。
   b) 共有テナントとサブスクリプションを追加します。最大 8 つの共有テナントを追加できます。テナントごとに最大 8 つのサブスクリプションを追加できます。

7. ［保存］と［適用］をクリックすると、行った変更が適用されて、ウィンドウは開いたままになります。［**OK**］をクリックした場合は、変更が適用されてウィンドウが閉じます。

接続のメンテナンスモードのオン/オフの切り替え

接続のメンテナンスモードをオンにすると、その接続（ホスト）上に格納されているマシンに新規の電源操作が適用されるのを防ぐことができます。ユーザーは、メンテナンスモードになっているマシンには接続できません。ユーザーが既に接続している場合は、そのユーザーがログオフした時点でメンテナンスモードが有効になります。

1. ［管理］**>**［完全な構成］の左側ペインで ［ホスト］を選択します。
2. 接続を選択します。メンテナンスモードをオンにする場合は、操作バーの ［メンテナンスモードをオンにする］を選択します。メンテナンスモードをオフにするには、［メンテナンスモードをオフにする］を選択します。

また、個々のマシンのメンテナンスモードをオンまたはオフにすることもできます。マシンカタログ内またはデリバリーグループ内のマシンに対し、メンテナンスモードをオンまたはオフにすることもできます。

接続の削除

> 注意：
>
> 接続の削除は、多くのマシンおよびそのデータの損失が発生する可能性のある操作です。削除されるマシン上に重要なユーザーデータがないかどうかを確認し、重要なデータがある場合はバックアップを作成しておいてください。

接続を削除する前に、以下の点について確認してください：

- 接続上に格納されているマシンからすべてのユーザーがログオフしていること。
- 実行したまま切断されたユーザーセッションがないこと。
- プールおよび専用のマシンの場合は、メンテナンスモードになっていること。
- 接続で使用するマシンカタログ内のすべてのマシンの電源がオフになっていること。

マシンカタログが参照している接続を削除すると、そのカタログを使用できなくなります。削除する接続がマシンカタログにより参照されている場合は、同時にそのカタログを削除することもできます。ただし、そのマシンカタログがほかの接続で使用されていないことを確認してから削除してください。

1. ［管理］**>**［完全な構成］の左側ペインで ［ホスト］を選択します。
2. 接続を選択し、操作バーの ［接続の削除］を選択します。
3. この接続上にマシンが格納されている場合、マシンを削除するかどうかを確認するメッセージが表示されます。削除する場合は、それらのマシンの Active Directory コンピューターアカウントに対する操作を指定します。

接続名の変更

1. ［管理］**>**［完全な構成］の左側ペインで ［ホスト］を選択します。
2. 接続を選択し、［接続名の変更］を選択します。

接続のテスト

1. ［管理］**>**［完全な構成］の左側ペインで ［ホスト］を選択します。
2. 接続を選択し、［接続のテスト］を選択します。

接続上のマシンの詳細の表示

1. ［管理］**>**［完全な構成］の左側ペインで ［ホスト］を選択します。
2. 接続を選択し、操作バーで ［マシンの表示］を選択します。

上ペインにその接続でアクセスするマシンの一覧が表示されます。マシンを選択すると、その詳細が下ペインに表示されます。実行中のセッションがある場合は、そのセッションの詳細も表示されます。

検索機能を使うと、マシンをすばやく見つけることができます。ウィンドウ上部の一覧から保存済みの検索を選択するか、または新しい検索を作成します。マシン名の一部または全体を入力して検索したり、詳細な検索式を作成したりできます。検索式を作成するには、［展開］を選択して、ドロップダウンの一覧からプロパティや演算子を選択します。

接続上のマシンの管理

1. ［管理］**>**［完全な構成］の左側ペインで ［ホスト］を選択します。
2. 接続を選択し、操作バーの ［マシンの表示］を選択します。
3. 操作バーで次のいずれかを選択します。マシンの状態や接続ホストの種類によっては、一部の操作を選択できない場合があります。

    - 起動：電源がオフまたは一時停止状態のマシンを起動します。

- 一時停止：マシンをシャットダウンすることなく一時的に停止して、マシン一覧を更新します。
- シャットダウン：オペレーティングシステムにシャットダウンを要求します。
- 強制シャットダウン：マシンの電源を強制的に切って、マシン一覧を更新します。
- 再起動：オペレーティングシステムに再起動を要求します。オペレーティングシステムで再起動を実行できない場合、デスクトップの状態は変更されません。
- メンテナンスモードの有効化：マシンへの接続を一時的に停止します。この状態のマシンにユーザーが接続することはできません。ユーザーが既に接続している場合は、そのユーザーがログオフした時点でメンテナンスモードが有効になります（前述のとおり、接続上のすべてのマシンのメンテナンスモードをオンまたはオフにすることもできます）。
- デリバリーグループから削除：デリバリーグループからマシンを削除しても、そのデリバリーグループで使用されているマシンカタログからは削除されません。ユーザーが接続しているマシンは削除できません。削除するマシンにユーザーが接続しないようにするには、メンテナンスモードを一時的にオンにしてください。
- 削除：マシンを削除すると、ユーザーはそのマシンにアクセスできなくなります。また、そのマシンはマシンカタログから削除されます。マシンを削除する前に、必要なユーザーデータをすべてバックアップしておいてください。ユーザーが接続しているマシンは削除できません。削除するマシンにユーザーが接続しないようにするには、メンテナンスモードを一時的にオンにしてください。

マシンのシャットダウンを伴う操作でマシンが 10 分以内にシャットダウンしない場合、電源が切れ、強制的にシャットダウンされます。シャットダウン中に Windows が更新のインストールを開始すると、更新が完了する前にマシンの電源が切れる危険性があります。

ストレージの編集

接続を使用する仮想マシンのオペレーティングシステムデータ、一時データ、および個人（PvD）データの保存に使用されているサーバーの状態を表示できます。データの種類それぞれの保存に使用するサーバーを指定することもできます。

1. ［管理］**>**［完全な構成］の左側ペインで ［ホスト］を選択します。
2. 接続を選択し、操作バーの ［ストレージの編集］を選択します。
3. 左ペインでデータの種類：オペレーティングシステムデータ、または一時データを選択します。
4. 選択したデータの種類に対し、1 つ以上のストレージデバイスのチェックボックスをオンまたはオフにします。
5. ［**OK**］を選択します。

一覧の各ストレージデバイスには、デバイス名とストレージの状態が表示されます。有効なストレージの状態の値は次のとおりです：

- 使用中：ストレージはマシンの作成に使用されています。
- 一時停止：ストレージは既存のマシン用にだけ使用されています。このストレージに新しいマシンは追加されません。
- 使用中でない：ストレージはマシンの作成に使用されていません。

現在使用中のデバイスのチェックボックスをオフにすると、ステータスが一時停止に変更されます。既存のマシンは引き続きそのストレージデバイスを使用します（また、データを書き込むことができます）。そのため、その場所は、マシンの作成に使用されなくなった後でも容量がいっぱいになる可能性があります。

孤立した **Azure** リソースを検出する

孤立したリソースはシステム内に存在する未使用のリソースであり、不要な出費につながる可能性があります。

この機能を使用すると、クラウドサイト上のホスト内で孤立した Azure リソースを検出できます。

Citrix DaaS で以下の手順を実行します：

1. ［管理］**>**［完全な構成］の左側ペインで ［ホスト］を選択します。
2. 接続を選択し、アクションバーで ［孤立したリソースを検出する］を選択します。［孤立したリソースを検出する］ダイアログボックスに孤立したリソースのレポートが表示されます。
3. 孤立したリソースのレポートを表示するには、［レポートの表示］を選択します。

または、PowerShell を使用して孤立した Azure リソースを検出することもできます。詳しくは、「孤立したリソースの一覧の取得」を参照してください。

孤立したリソースの背後にある理由を理解し、それらへの対処をさらに進める方法について詳しくは、「Citrix を使用して孤立した Azure リソースを効率的に管理する」を参照してください。

接続タイマー

Citrix ポリシー設定を使用して、以下の 3 つの接続タイマーを構成できます：

- 最長接続タイマー：ユーザーデバイスと仮想デスクトップ間の連続セッションを自動的にログオフするまでの時間を制御します。これを構成するには、ポリシーの［セッション接続タイマー］設定および［セッション接続タイマー間隔］設定を使用します。
- 接続アイドルタイマー：ユーザーからの入力がないユーザーデバイスとデスクトップ間の連続セッションを自動的にログオフするまでの時間を制御します。これを構成するには、ポリシーの ［セッションアイドルタイマー］設定および ［セッションアイドルタイマーの間隔］設定を使用します。
- 切断タイマー：切断状態でロックされた仮想デスクトップセッションを自動的にログオフするまでの時間を制御します。これを構成するには、ポリシーの ［切断セッションタイマー］設定および ［切断セッションタイマーの間隔］設定を使用します。

これらの設定項目を変更する場合は、環境全体で設定が一貫していることを確認してください。

詳しくは、ポリシー設定のドキュメントを参照してください。

リソースのネットワークの編集

接続するネットワークを変更できます。以下を実行します：

1. ［管理］**>**［完全な構成］**>**［ホスト］に移動します。
2. 接続のターゲットリソースを選択し、操作バーの ［**Edit Network**］を選択します。
3. 仮想マシンで使用するネットワークを選択してください。
4. ［保存］をクリックすることで、変更を保存して終了します。

リソースの削除、名前変更、またはテスト

1. ［管理］**>**［完全な構成］の左側ペインで ［ホスト］を選択します。
2. 接続のターゲットリソースを選択し、操作バー内の必要なエントリを選択します:
   - リソースの削除
   - リソース名の変更
   - リソースのテスト

孤立したリソースの一覧の取得

MCS で作成されたのに、MCS で追跡されなくなった孤立したリソースの一覧を取得できます。これは現時点では Azure 環境で適用可能です。リストを取得するには、PowerShell コマンドを使用できます。接続を使用してフィルタリングできます。

> 注:
>
> プロビジョニングまたはイメージの更新が処理中の場合、PowerShell コマンドは拒否されます。

制限事項

- 組み込みのすべての管理権限を実行できる管理者、または Cloud Admin の役割を持つ管理ユーザーのみが PowerShell コマンドを実行して、孤立したリソースの一覧を取得できます。
- 孤立したリソースをフィルタリングしている間は VM の電源を入れないでください。孤立したリソースが誤って認識されるのを避けるためです。
- ワークロードが高くなる可能性がある場合、孤立したリソースとしては約 2,000 レコードのみが表示されます。

孤立したリソースの一覧の表示

孤立したリソースの一覧を表示するには、以下を実行します

1. **PowerShell** ウィンドウを開きます。
2. `asnp citrix*`を実行します。
3. 次のコマンドを実行します:

a) 接続 UID を取得します。接続 UID は、HypervisorConnectionUid 属性の値です。

```
Get-ChildItem xdhyp:\connections | where {
  $_.PluginId -like 'Azure*'  }
 "
<!--NeedCopy-->
```

b) 孤立したリソースの一覧を取得します。

```
get-provorphanedresource
-HypervisorConnectionUid <connection uid>
<!--NeedCopy-->
```

サブスクリプション **ID** から孤立したリソースの一覧を表示

サブスクリプション ID から、孤立したリソースの一覧を表示するには:

1. **PowerShell** ウィンドウを開きます。
2. `asnp citrix*`を実行します。
3. 次のコマンドを実行します:

a) サブスクリプション ID を使用して接続 UID を見つけます。接続 UID は、HypervisorConnectionUid 属性の値です。

```
Get-ChildItem xdhyp:\connections | where {
  $_.CustomProperties -match '<subscriptionId>'  }

<!--NeedCopy-->
```

b) 孤立したリソースの一覧を取得します。

```
get-provorphanedresource -HypervisorConnectionUid <connection
    uid>
<!--NeedCopy-->
```

> 注:
>
> 削除する前にリソースを慎重に確認してください。

次の手順

- 特定のホストの種類への接続については、次を参照してください:
  - AWS への接続
  - Google クラウド環境への接続
  - Microsoft Azure への接続

- Microsoft System Center Virtual Machine Manager への接続
- Nutanix への接続
- Nutanix クラウドおよびパートナーソリューションへの接続
- VMware への接続
- VMware クラウドおよびパートナーソリューションへの接続
- XenServer への接続

初期展開プロセスを行っている場合は、マシンカタログを作成します。

AWS への接続

May 17, 2024

「接続とリソースの作成と管理」では接続を作成するためのウィザードについて説明しています。以下の情報は、AWS クラウド環境に固有の詳細について説明しています。

> 注:
>
> AWS への接続を作成する前に、まず AWS をリソースの場所として設定する必要があります。「AWS 仮想化環境」を参照してください。

接続の作成

完全な構成インターフェイスから接続を作成する場合:

- API キーと秘密キーの値を指定する必要があります。AWS でこれらの値を含んでいるキーファイルをエクスポートしてから、値をインポートすることができます。また、リージョン、アベイラビリティゾーン、仮想プライベートクラウド名、サブネットアドレス、ドメイン名、セキュリティグループ名、および資格情報も必要になります。
- AWS コンソールから取得するルート AWS アカウント用の資格情報ファイルでは、標準的な AWS ユーザーのものとは異なる形式が使用されています。このため、このファイルを Citrix DaaS で使用して API キーと秘密キーの情報を入力することはできません。AWS Identity Access Management（IAM）形式の資格情報ファイルを使用してください。

> 注:
>
> 接続を作成した後、API キーと秘密キーを更新しようとすると失敗することがあります。この問題を解決するには、プロキシサーバーまたはファイアウォールの制限を確認し、次のアドレスに接続できることを確認してください: `https://*.amazonaws.com`。

制限事項

AWS コンソールで AWS 仮想プライベートクラウド（VPC）の名前を変更すると、Citrix Cloud の既存のホスティングユニットが破損します。ホスティングユニットが破損している場合、カタログを作成したり、既存のカタログにマシンを追加したりすることはできません。この問題を解決するには、AWS VPC の名前を元の名前に戻します。

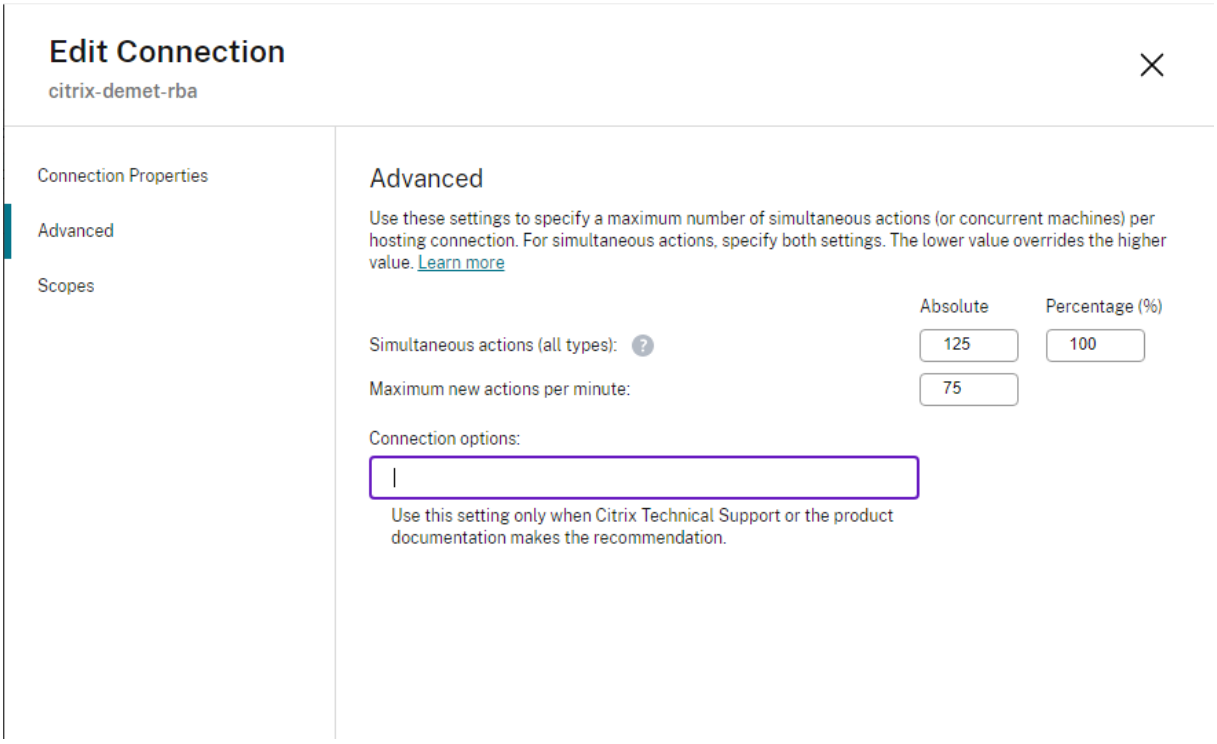
ホスト接続のデフォルト値

AWS クラウド環境の完全な構成インターフェイスでホスト接続を作成すると、次のデフォルト値が表示されます:

オプション	絶対	パーセンテージ
同時操作（すべての種類）	125	100
1 分あたりの最大新規操作	150	-
最大同時プロビジョニング操作	100	-

MCS は、デフォルトで最大 100 の同時プロビジョニング操作をサポートします。

これらの値は、Citrix Studio の ［接続の編集］画面の ［詳細設定］セクションで構成できます:



または、Remote PowerShell SDK を使用して、環境ごとに最適な同時操作の最大数を設定することもできます。

PowerShell カスタムプロパティ`MaximumConcurrentProvisioningOperations`を使用して、同時 AWS プロビジョニング操作の最大数を指定します。

構成前:

- PowerShell SDK for Cloud がインストールされていることを確認してください。
- MaximumConcurrentProvisioningOperationsのデフォルト値は 100 であることに留意してください。

MaximumConcurrentProvisioningOperations値をカスタマイズするには、次の手順を実行します:

1. **PowerShell** ウィンドウを開きます。
2. asnp citrix*を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. 「cd xdhyp:\Connections\」を入力します。
4. dirを入力して、接続を一覧表示します。
5. カスタムプロパティ文字列を変更または初期化します:
   - カスタムプロパティ文字列に値がある場合は、カスタムプロパティをメモ帳にコピーします。次に、MaximumConcurrentProvisioningOperationsプロパティを希望の値に変更します。1〜1000 の範囲の値を入力できます。
     例:<Property xsi:type="IntProperty"Name="MaximumConcurrentProvisioningO
     "Value="xyz"/>。
   - カスタムプロパティ文字列が空または null の場合、スキーマとMaximumConcurrentProvisioningOpera
     プロパティの両方に適切な構文を入力して、文字列を初期化する必要があります。
6. **PowerShell** ウィンドウで、変更したカスタムプロパティをメモ帳から貼り付け、変更したカスタムプロパティに変数を割り当てます。カスタムプロパティを初期化した場合は、構文の後に次の行を追加します:

   ```
   $customProperties = '<CustomProperties xmlns="http://schemas.
   citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
   org/2001/XMLSchema-instance"><Property xsi:type="IntProperty"
   Name="MaximumConcurrentProvisioningOperations" Value="100"/></
   CustomProperties>'。
   ```

   この文字列は、MaximumConcurrentProvisioningOperationsプロパティを 100 に設定します。カスタムプロパティ文字列で、MaximumConcurrentProvisioningOperationsプロパティをニーズに合った値に設定する必要があります。
7. Get-XDAuthenticationと入力すると、資格情報の入力を求められます。
8. $cred = Get-Credentialを実行すると、パスワードのみ（または名前とパスワード）の入力を求められる場合があります。また、アプリケーション ID と関連するシークレットの入力を求められる場合があります。役割ベースの認証を使用する接続の場合、**role_based_auth** は名前とパスワードの両方です。それ以外の場合は、AWS API ID とシークレットを入力します。

9. `set-item -PSPath 'XDHyp:\Connections<connection-name>'-CustomProperties $customProperties -username $cred.username -Securepassword $cred.password`を実行します。*<connection-name>* に接続名を設定する必要があります。
10. `dir`を入力して、更新された CustomProperties 文字列を確認します。

ネットワークインターフェイスごとにセキュリティグループを構成

ホスト接続を編集するときに、PowerShell コマンドを使用して、Elastic Network Interface（ENI）ごとに許可されるセキュリティグループの最大数を構成できるようになりました。AWS セキュリティグループのクォータ値について詳しくは、「セキュリティグループ」を参照してください。

ネットワークインターフェイスごとにセキュリティグループを構成するには、以下の手順を実行します:

1. PowerShell ウィンドウを開きます。
2. `asnp citrix*`を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. `cd xdhyp:\Connections\`を実行します。
4. `dir`を実行して接続を一覧表示します。
5. 次の PowerShell コマンドを実行して、ネットワークインターフェイスごとにセキュリティグループを構成します:

```
Set-HypHypervisorConnectionMetadata -HypervisorConnectionName aws
    -Name "Citrix_MachineManagement_Options" -Value "
    AwsMaxENISecurityGroupLimit=<number>"
<!--NeedCopy-->
```

> 注:
>
> `AwsMaxENISecurityGroupLimit`に値を設定しない場合は、デフォルト値の 5 が使用されます。

サービスエンドポイント **URL**

標準ゾーンのサービスエンドポイント **URL**

MCS を使用すると、API キーと API シークレットで新しい AWS 接続が追加されます。この情報と認証済みアカウントで、MCS は AWS DescribeRegions EC2 API 呼び出しを使用して、サポートされているゾーンのクエリを AWS に対して実行します。このクエリは、一般的な EC2 サービスエンドポイント URL の`https://ec2.amazonaws.com/`を使用して行われます。MCS を使用して、サポートされているゾーンの一覧から、接続するゾーンを選択します。そのゾーンで優先される AWS サービスエンドポイント URL が自動的に選択されます。ただし、サービスエンドポイント URL を作成した後は、URL を設定または変更することはできなくなります。

非標準のサービスエンドポイント **URL**

接続で自動的に選択された AWS サービスエンドポイント URL が必要ない場合があります。必要ない場合、Citrix Cloud SDK と PowerShell を使用して、非標準のサービスエンドポイント URL で接続を作成できます。たとえば、サービスエンドポイント URL のhttps://ec2.cn-north-1.amazonaws.com.cnを使用して接続を作成するには:

1. AWS がホストする Cloud Connector をセットアップし、接続できることを確認します。
2. 以下の PowerShell コマンドを実行して、Cloud Connector の一覧を表示します。

```
1  PS C:> asnp citrix.*
2  PS C:> Get-XDAuthentication
3  PS C:> Get-ConfigEdgeServer
4 <!--NeedCopy-->
```

3. 新しく作成された Cloud Connector から ZoneUid を見つけて、以下の PowerShell コマンドに入力します。イタリック体の項目をそれぞれの値に置き換えます。

```
PS C:\> $hyp= New-Item -Path xdhyp:\Connections -ZoneUidZoneUid-
Name “My New Connection” -ConnectionType "AWS"-HypervisorAddress @("
https://ec2.cn-north-1.amazonaws.com.cn")-UserName“APIkey” -Password
“APISecret” -Persist
PS C:\> New-BrokerHypervisorConnection -HypHypervisorConnectionUid
 $hyp. HypervisorConnectionUid
```

4. [完全な構成] > [ホスト] タブを更新して、EC2 接続が作成されたことを確認します。
5. 新しい接続を使用して、リソースの場所を追加します。

IAM 権限の定義

このセクションの情報を使用して、AWS 上の Citrix DaaS の IAM アクセス権限を定義します。Amazon の IAM サービスでは、複数のユーザーを持つアカウントが許可されており、さらにグループに編成することができます。これらのユーザーは、アカウントに関連付けられた操作の実行を制御できるさまざまな権限を持つことができます。IAM アクセス権限について詳しくは、「IAM JSON ポリシーのリファレンス」を参照してください。

IAM アクセス権限ポリシーを新しいユーザーグループに適用するには、次を実行します:

1. AWS 管理コンソールにログインし、ドロップダウンリストから [**IAM service**] を選択します。
2. [**Create a New Group of Users**] を選択します。
3. 新しいユーザーグループの名前を入力し、[**Continue**] を選択します。
4. [**Permissions**] ページで [**Custom Policy**]、[**Select**] を選択します。
5. [**Permissions policy**] の名前を入力します。
6. [**Policy Document**] セクションで、関連する権限の情報を入力します。

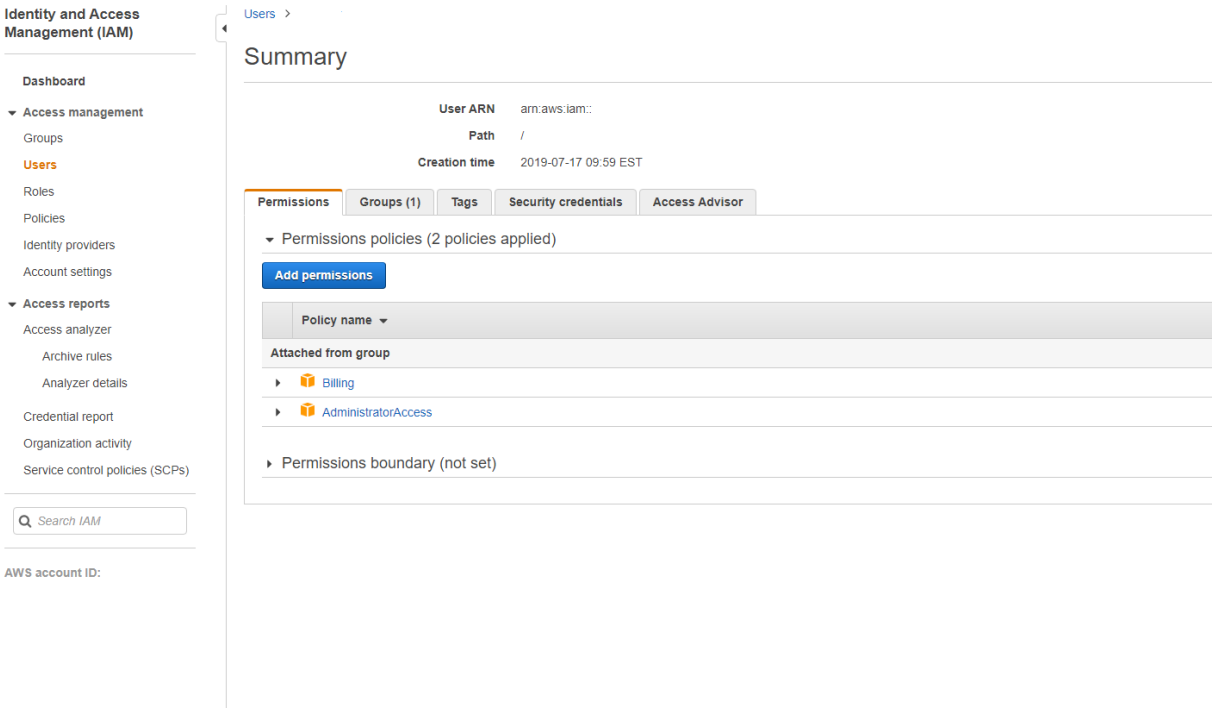
ポリシー情報の入力後、［**Continue**］を選択してユーザーのグループに対して IAM 権限ポリシーのアプリケーションを完了します。グループ内のユーザーには、Citrix DaaS に必要なアクションのみを実行するためのアクセス権限が付与されます。

> 重要：
>
> 上記の例で提供されているポリシーテキストを使用して、Citrix DaaS が特定のリソースに限定せずに AWS アカウント内でアクションを実行するために使用するアクションを一覧表示します。Citrix では、この例はテスト目的で使用することをお勧めします。実稼働環境では、リソースにさらに制限を加えることを選択できます。

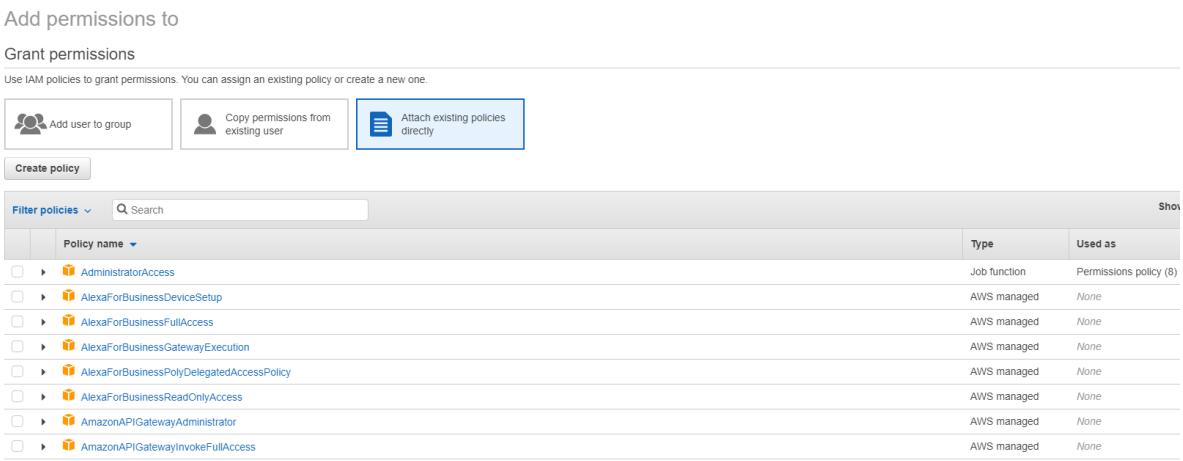
IAM アクセス権限の追加

AWS マネジメントコンソールの ［**IAM**］セクションで、権限を追加します：

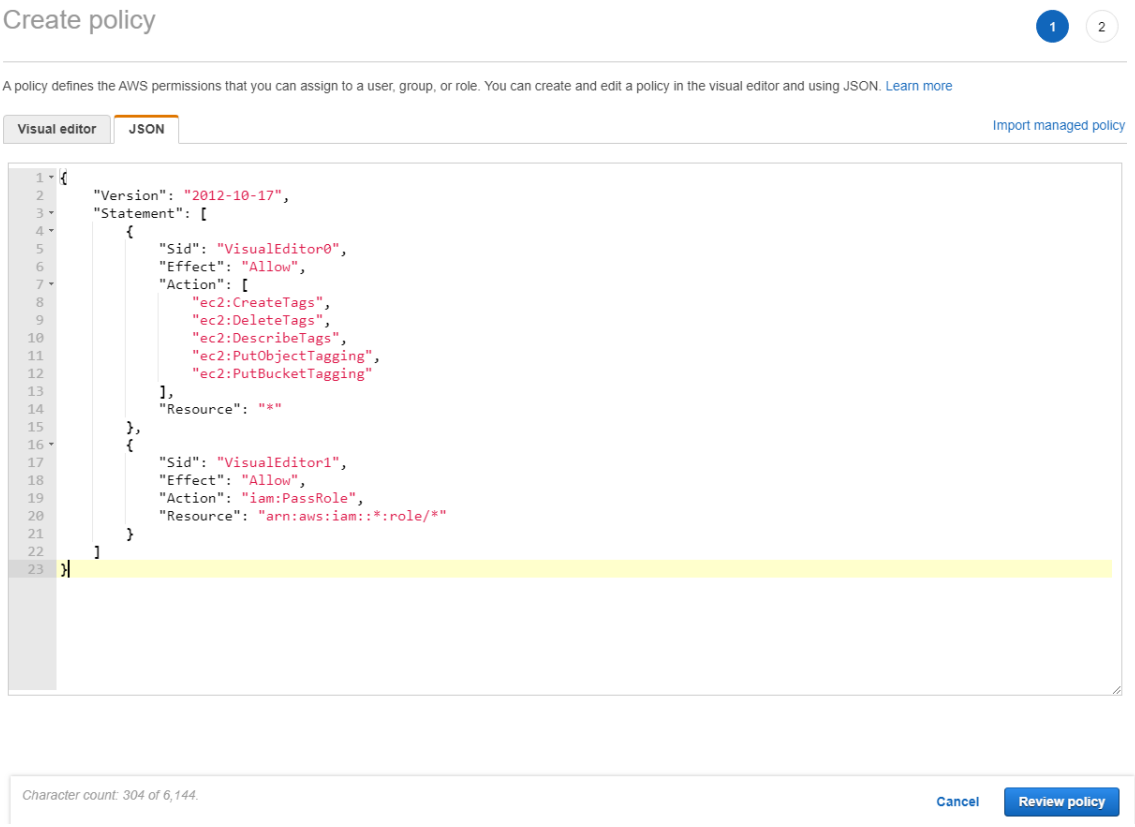
1. ［**Summary**］パネルで ［**Permissions**］タブを選択します。
2. ［**Add permissions**］を選択します。



［**Add Permissions to**］画面でアクセス許可を付与します：



以下は［**JSON**］タブの例です：



> ヒント：
>
> JSON の例には、環境に対するすべての権限が含まれているとは限らないことに注意してください。詳しくは、「AWS 権限について」を参照してください。

必要な **AWS** 権限

このセクションでは、AWS 権限の完全なリストが示されています。機能を正しく動作させるには、このセクションで示した権限の完全なセットを使用します。

> 注:
>
> *iam:PassRole* 権限は、**role_based_auth** でのみ必要です。

ホスト接続の作成

AWS から取得した情報を使用して、新しいホスト接続が追加されます。

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs"
            ],
            "Effect": "Allow",
            "Resource": "*"
         }

    ]
 }

<!--NeedCopy-->
```

VM の電源管理

マシンインスタンスの電源がオンまたはオフです。

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:AttachVolume",
```



```
                    "ec2:CreateVolume",
                    "ec2:DeleteVolume",
                    "ec2:DescribeInstances",
                    "ec2:DescribeVolumes",
                    "ec2:DetachVolume",
                    "ec2:StartInstances",
                    "ec2:StopInstances"
                ],
                "Effect": "Allow",
                "Resource": "*"
            }

        ]
    }

<!--NeedCopy-->
```

VM の作成、更新、または削除

マシンカタログは、AWS インスタンスとしてプロビジョニングされた VM で、作成、更新、または削除されます。

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteVolume",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeLaunchTemplates",
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
```



```
                "ec2:DescribeSpotInstanceRequests",
                "ec2:DescribeInstanceCreditSpecifications",
                "ec2:DescribeInstanceAttribute",

                "ec2:GetLaunchTemplateData",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
,
        {

            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
,
        {

            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:PutBucketAcl",
                "s3:PutBucketTagging",
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:PutObjectTagging"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::citrix*"
        }
,
        {

            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
```



```
                    "ebs:PutSnapshotBlock",
                    "ebs:CompleteSnapshot",
                    "ebs:ListSnapshotBlocks",
                    "ebs:ListChangedBlocks",
                    "ec2:CreateSnapshot"
                ],
                "Effect": "Allow",
                "Resource": "*"
            }

        ]
    }

<!--NeedCopy-->
```

> 注:
>
> - SecurityGroups に関連する EC2 セクションは、カタログの作成中に準備 VM 用に分離セキュリティグループを作成する必要がある場合にのみ必要です。これが行われると、これらの権限は必要ありません。

ディスクの直接アップロードとダウンロード　ディスクの直接アップロードは、マシンカタログプロビジョニングのボリュームワーカー要件をなくし、代わりに AWS が提供するパブリック API を使用します。この機能により、追加のストレージアカウントに関連するコストと、ボリュームワーカーの操作を維持する複雑さが軽減されます。

> 注:
>
> ボリュームワーカーのサポートは廃止されました。

次の権限をポリシーに追加する必要があります:

- ebs:StartSnapshot
- ebs:GetSnapshotBlock
- ebs:PutSnapshotBlock
- ebs:CompleteSnapshot
- ebs:ListSnapshotBlocks
- ebs:ListChangedBlocks
- ec2:CreateSnapshot
- ec2:DeleteSnapshot
- ec2:DescribeLaunchTemplates

> 重要:
>
> - ボリュームワーカー AMI やボリュームワーカー VM などのボリュームワーカーリソースがなくても、既存のマシンカタログに新しい VM を追加できます。
> - 以前にボリュームワーカーを使用していた既存のカタログを削除すると、ボリュームワーカーに関連するすべてのアーティファクトが削除されます。

作成されたボリュームの **EBS** 暗号化

AMI が暗号化されている場合、または EBS がすべての新しいボリュームを暗号化するように構成されている場合、EBS は新しく作成されたボリュームを自動で暗号化できます。ただし、この機能を実装するには、次の権限が IAM ポリシーに含まれている必要があります。

```
{

     "Version": "2012-10-17",
     "Statement": [
        {

            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:GenerateDataKey",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": "*"
         }

    ]
 }

<!--NeedCopy-->
```

> 注:
>
> Resource と Condition のブロックを含めることにより、ユーザーの裁量で権限を特定のキーに制限できます。たとえば、**Condition** を使用した **KMS** 権限:

```
{

     "Version": "2012-10-17",
     "Statement": [
        {

            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:GenerateDataKey",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": [
```



```
                "arn:aws:kms:us-east-2:123456789012:key/abcd1234-a123
                   -456d-a12b-a123b4cd56ef"
            ],
            "Condition": {

                "Bool": {

                    "kms:GrantIsForAWSResource": true
                 }

             }

          }

    ]
 }

<!--NeedCopy-->
```

以下のキーポリシーステートメントは、アカウントが IAM ポリシーを使用して KMS キーの全操作（kms:*）の権限を委任できるようにするために必要な KMS キーのデフォルトのキーポリシー全体です。

```
{

"Sid": "Enable IAM policies",
"Effect": "Allow",
"Principal": {

"AWS": "arn:aws:iam::111122223333:root"
 }
 ,
"Action": "kms:",
"Resource": ""
 }

<!--NeedCopy-->
```

詳しくは、AWS Key Management Service 公式ドキュメントを参照してください。

IAM 役割ベースの認証

以下の権限が、役割ベースの認証をサポートするために追加されています。

```
{

      "Version": "2012-10-17",
      "Statement": [
         {

             "Effect": "Allow",
             "Action": "iam:PassRole",
```



```
            "Resource": "arn:aws:iam::*:role/*"
        }

    ]
 }

<!--NeedCopy-->
```

最低限の **IAM** 権限ポリシー

以下の JSON は、現在サポートされているすべての機能に使用できます。このポリシーを使用して、ホスト接続の作成、VM の作成、更新、削除、および電源管理を行うことができます。
「IAM 権限の定義」セクションで説明されているように、ポリシーをユーザーに適用できます。または、**role_based_auth** セキュリティキーと秘密キーを使用して、役割ベースの認証を使用することもできます。

> 重要:
>
> **role_based_auth** を使用するには、クラウドコネクタを設定するときに、まずクラウドコネクタ EC2 インスタンスで目的の IAM 役割を設定します。Citrix Studio を使用して、ホスティング接続を追加し、認証キーとシークレットの role_based_auth を指定します。これらの設定のホスティング接続は、役割ベースの認証を使用します。

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateNetworkInterface",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteLaunchTemplate",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DeregisterImage",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeIamInstanceProfileAssociations",
```



```
                    "ec2:DescribeImages",
                    "ec2:DescribeInstances",
                    "ec2:DescribeInstanceTypes",
                    "ec2:DescribeLaunchTemplates",
                    "ec2:DescribeLaunchTemplateVersions",
                    "ec2:DescribeNetworkInterfaces",
                    "ec2:DescribeRegions",
                    "ec2:DescribeSecurityGroups",
                    "ec2:DescribeSnapshots",
                    "ec2:DescribeSubnets",
                    "ec2:DescribeTags",
                    "ec2:DescribeSpotInstanceRequests",
                    "ec2:DescribeInstanceCreditSpecifications",
                    "ec2:DescribeInstanceAttribute",
                    "ec2:GetLaunchTemplateData",
                    "ec2:DescribeVolumes",
                    "ec2:DescribeVpcs",
                    "ec2:DetachVolume",
                    "ec2:DisassociateIamInstanceProfile",
                    "ec2:RebootInstances",
                    "ec2:RunInstances",
                    "ec2:StartInstances",
                    "ec2:StopInstances",
                    "ec2:TerminateInstances"
                ],
                "Effect": "Allow",
                "Resource": "*"
            }
    ,
            {

                "Action": [
                    "ec2:AuthorizeSecurityGroupEgress",
                    "ec2:AuthorizeSecurityGroupIngress",
                    "ec2:CreateSecurityGroup",
                    "ec2:DeleteSecurityGroup",
                    "ec2:RevokeSecurityGroupEgress",
                    "ec2:RevokeSecurityGroupIngress"
                ],
                "Effect": "Allow",
                "Resource": "*"
            }
    ,
            {

                "Action": [
                    "s3:CreateBucket",
                    "s3:DeleteBucket",
                    "s3:DeleteObject",
                    "s3:GetObject",
                    "s3:PutBucketAcl",
                    "s3:PutObject",
                    "s3:PutBucketTagging",
```



```
                "s3:PutObjectTagging"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::citrix*"
         }
,
        {

            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
         }
,
        {

            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:GenerateDataKey",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": "*"
         }
,
        {

            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/*"
         }

    ]
}

<!--NeedCopy-->
```

注:

- SecurityGroups に関連する EC2 セクションは、カタログの作成中に準備 VM 用に分離セキュリティグループを作成する必要がある場合にのみ必要です。これが行われると、これらの権限は必要ありません。

> - EBS ボリューム暗号化を使用している場合は、KMS セクションのみが必要です。
> - `iam:PassRole`権限セクションは、**role_based_auth** でのみ必要です。
> - 要件と環境に基づいて、フルアクセス権限の代わりに、特定のリソースレベルのアクセス権限を追加できます。詳しくは、AWS ドキュメントの「Demystifying EC2 Resource-Level Permissions」と「AWS リソースのアクセス管理」を参照してください。
> - `ec2:CreateNetworkInterface`および`ec2:DeleteNetworkInterface`権限は、ボリュームワーカー方式を使用している場合にのみ使用してください。

次の手順

- 初期展開プロセスを行っている場合は、「マシンカタログの作成」を参照してください。
- AWS 固有の情報については、「AWS カタログの作成」を参照してください。

追加情報

- 接続とリソースの作成と管理
- AWS 仮想化環境

Google クラウド環境への接続

April 18, 2024

「接続とリソースの作成と管理」では接続を作成するためのウィザードについて説明しています。以下の情報は、Google クラウド環境に固有の詳細について説明しています。

> 注:
>
> Google クラウド環境への接続を作成する前に、まず Google クラウドアカウントをリソースの場所として設定する必要があります。「Google Cloud 仮想化環境」を参照してください。

接続の追加

［完全な構成］インターフェイスで、「Create and manage connections and resources」のガイダンスに従います。次の説明は、ホスト接続を設定する手順を示しています:

1. ［管理］**>**［完全な構成］の左側ペインで ［ホスト］を選択します。
2. 操作バーの ［接続およびリソースの追加］を選択します。
3. ［接続］ページで、［新しい接続を作成する］と ［**Citrix** プロビジョニングツール］を選択してから ［次へ］を選択します。

- ゾーン名。ホストリソースを配置するゾーン（リソースの場所に相当）を選択します。ゾーンは、リソースの場所を作成して Cloud Connector を追加すると自動的に作成されます。詳しくは、「ゾーン」を参照してください。
- 接続の種類。メニューから［**Google Cloud Platform**］を選択します。
- サービスアカウントキー。Google 資格情報ファイル（.json）に含まれるキーをインポートします。インポートを行うには、資格情報ファイルからキーを貼り付ける方法と、資格情報ファイルを参照する方法があります。キーを貼り付けるには：

  a) 資格情報ファイルを見つけます
  b) メモ帳（または任意のテキストエディター）でファイルを開きます
  c) キーの値をコピーします。
  d) ［接続］ページに戻り、［キーの追加］を選択し、キーの値を貼り付けてから［**Done**］を選択します。

- サービスアカウント **ID**。このフィールドには、サービスアカウントキーの情報が自動的に入力されます。
- 接続名。接続名を入力します。
- **Citrix Cloud Connector** を介してトラフィックをルーティングします。このチェックボックスをオンにすると、利用可能な Citrix Cloud Connector 経由で API 要求をルーティングできます。セキュリティを強化するには、［**Google Cloud Build** を有効にしてプライベートプールを使用する］チェックボックスをオンにします。

  また、PowerShell を使用してこの機能を有効にすることもできます。詳しくは、「GCP 管理トラフィックのための安全な環境の作成」を参照してください。

> 注：
>
> このオプションは、展開内にアクティブな Citrix Cloud Connector がある場合にのみ使用できます。この機能は現時点では Connector Appliance でサポートされていません。

- 仮想マシンの作成ツール。仮想マシンの作成ツールを選択できます。

4. ［リージョン］ページで、メニューからプロジェクト名を選択し、使用するリソースを含むリージョンを選択して、［次へ］を選択します。
5. ［ネットワーク］ページで、リソースの名前を入力し、メニューから仮想ネットワークを選択し、サブセットを選択してから ［次へ］を選択します。このリージョンとネットワークの組み合わせを識別するためのわかりやすいリソース名を指定してください。名前に *(Shared)* サフィックスが付加された仮想ネットワークは、共有 VPC を表しています。共有 VPC にサブネットレベルの IAM 役割を設定する場合、共有 VPC の特定のサブネットのみがサブネットリストに表示されます。

> 注：
>
> - リソース名は 1～64 文字にし、空白スペースのみにしたり記号（\ / ; : # . * ? = < > | [ ] { } "' ( )')）を含めたりすることはできません。

6. ［概要］ページで情報を確認してから、［完了］を選択し、［接続およびリソースの追加］ウィンドウを終了します。

接続とリソースを作成すると、作成した接続とリソースが一覧表示されます。接続を構成するには、接続を選択してから、操作バーで該当するオプションを選択します。

同様に、接続の下で作成されたリソースを削除、名前変更、またはテストすることができます。これを行うには、接続の下のリソースを選択してから、操作バーで該当するオプションを選択します。

GCP 管理トラフィックのための安全な環境の作成

自身の Google Cloud プロジェクトには、プライベート Google アクセスのみを許可できます。この実装により、機密データを処理するためのセキュリティが強化されます。このためには、以下の手順を実行します:

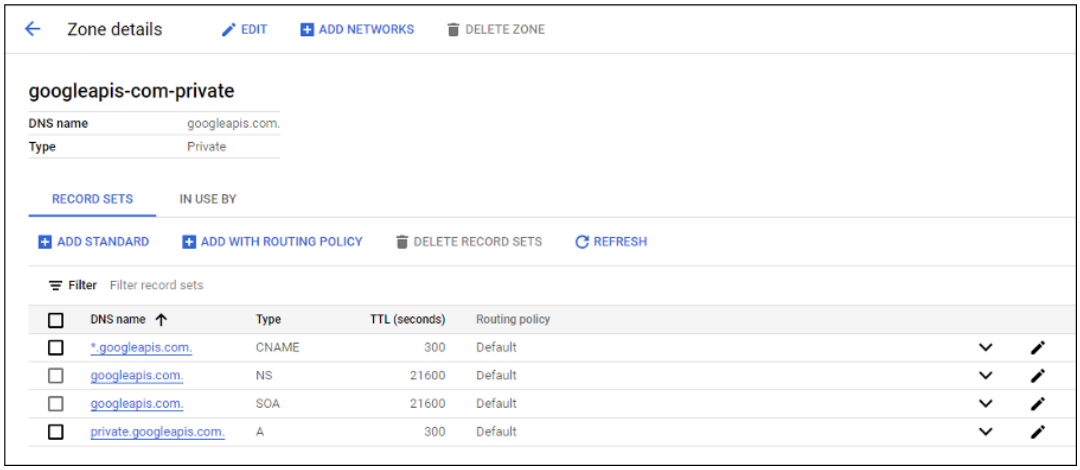
1. VPC サービスの制御を適用する VPC に Cloud Connector をインストールします。詳しくは、「VPC サービスの制御」を参照してください。
2. Citrix Cloud 環境の場合は、`CustomProperties`に`ProxyHypervisorTrafficThroughConnector`を追加します。プライベートワーカープールを使用する場合は、`CustomProperties`に`UsePrivateWorkerPool`を追加します。プライベートワーカープールについて詳しくは、「プライベートプールの概要」を参照してください。

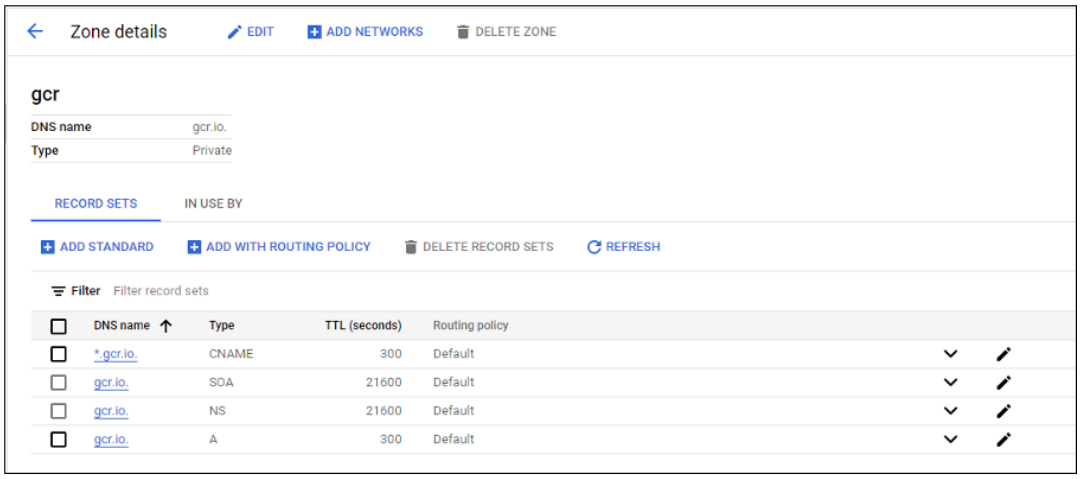
> 注:
>
> この機能は現時点では Connector Appliance でサポートされていません。

GCP 管理トラフィックのための安全な環境の作成要件

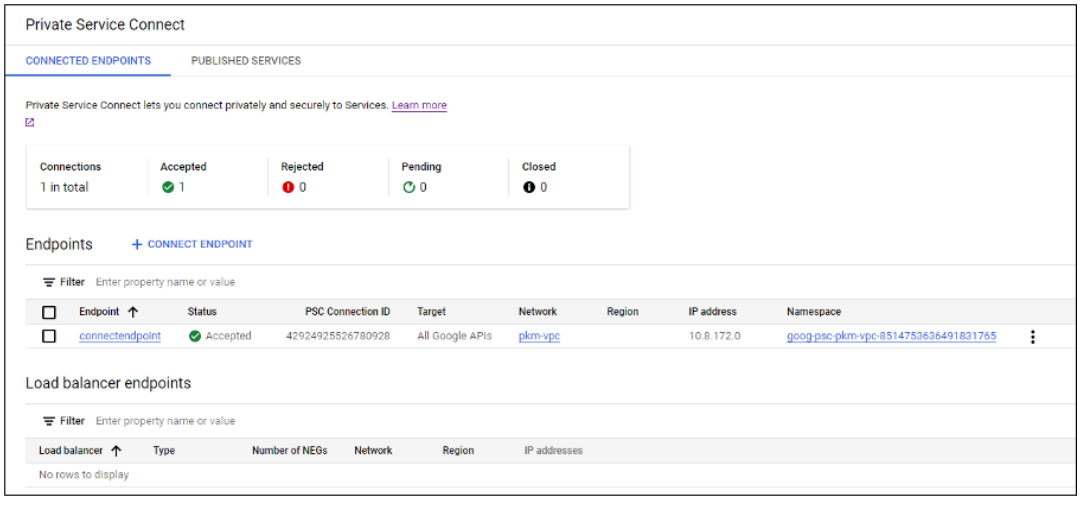
GCP 管理トラフィックのための安全な環境の作成要件は以下のとおりです。

- カスタムプロパティを更新するときは、ホスト接続がメンテナンスモードであることを確認する。
- プライベートワーカープールを使用するには、以下の変更が必要です。
  - Citrix Cloud Services アカウントの場合、以下の IAM ロールを追加します。
    - Cloud Build サービスアカウント
    - コンピューティングインスタンス管理者
    - サービスアカウントユーザー
    - サービスアカウントトークン作成者
    - Cloud Build ワーカープールの所有者
  - ホスト接続の作成に使用するのと同じプロジェクトに、Citrix Cloud Services のアカウントを作成します。
  - 「DNS 構成」の説明に従って、**`private`**`.googleapis.com`および`gcr.io`用の DNS ゾーンを設定します。

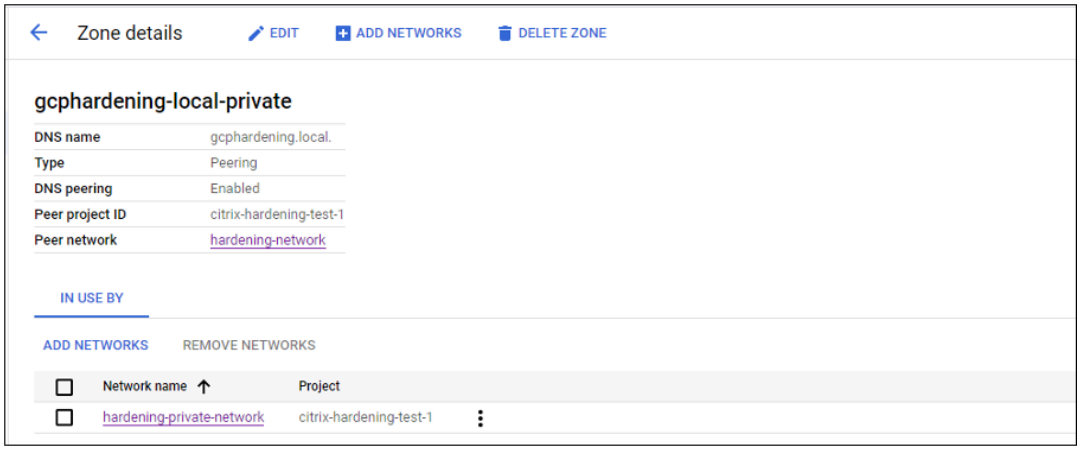




- プライベートネットワークアドレス変換 (NAT) を設定するか、プライベートサービス接続を使用します。詳しくは、「エンドポイントから Google API にアクセスする」を参照してください。



- ピアリングされた VPC を使用する場合は、ピアリングされた VPC にピアリングする Cloud DNS ゾーンを作成します。詳しくては、「ピアリングゾーンを作成する」を参照してください。



- VPC サービスの制御で、API と VM がインターネットと通信できるように送信用の規則を設定します。送信用の規則はオプションです。例:

```
Egress Rule 1
From:
Identities:ANY_IDENTITY
To:
Projects =
All projects
Service =
Service name: All services
<!--NeedCopy-->
```

プロキシを有効にする

このプロキシを有効にするには、ホスト接続でカスタムプロパティを次のように設定します。

1. Delivery Controller ホストから PowerShell ウィンドウを開くか、Remote PowerShell SDK を使用します。Remote PowerShell SDK について詳しくは、「SDK および API」を参照してください。
2. 次のコマンドを実行します:

   a) `Add-PSSnapin citrix*`
   b) `cd XDHyp:\Connections\`
   c) `dir`

3. 接続の`CustomProperties`をメモ帳にコピーします。
4. 以下のプロパティ設定を追加します。

   - クラウド環境の場合 (パブリックプールを使用): プロキシを有効にするには、プロパティ設定<`Property xsi:type="StringProperty"Name="ProxyHypervisorTrafficThroughC` `"Value="True"/>`を`CustomProperties`に追加します。例:


```
<CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema
    -instance" xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation">
<Property xsi:type="StringProperty" Name="
    ProxyHypervisorTrafficThroughConnector" Value="True"/>
</CustomProperties>
<!--NeedCopy-->
```

VPC サービス境界で Cloud Build サービスアカウントの送信用規則を許可します。例:

```
Ingress Rule 1
From:
Identities:
<ProjectID>@cloudbuild.gserviceaccount.com
Source > All sources allowed
To:
Projects =
All projects
Services =
Service name: All services
<!--NeedCopy-->
```

VPC サービス境界について詳しくは、「サービス境界の詳細と構成」を参照してください。

- クラウド環境のプライベートワーカープールの場合は、プロパティ設定<Property xsi:type="StringProperty"Name="ProxyHypervisorTrafficThroughConnector"Value="True"/>と<Property xsi:type="StringProperty"Name="UsePrivateWorkerPool"Value="True"/>をCustomPropertiesに追加してプロキシを有効にします。例:

```
<CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema
    -instance" xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation">
<Property xsi:type="StringProperty" Name="
    ProxyHypervisorTrafficThroughConnector" Value="True"/>
<Property xsi:type="StringProperty" Name="
    UsePrivateWorkerPool" Value="True"/>
</CustomProperties>
<!--NeedCopy-->
```

5. PowerShell ウィンドウで、変更したカスタムプロパティに変数を割り当てます。例: `$customProperty = '<CustomProperties…</CustomProperties>'`。
6. `$gcpServiceAccount = "<ENTER YOUR SERVICE ACCOUNT EMAIL HERE>"`を実行します。
7. `$gcpPrivateKey = "<ENTER YOUR SERVICE ACCOUNT PRIVATE KEY HERE AFTER REMOVING ALL INSTANCES OF \n >"`を実行します。
8. `$securePassword = ConvertTo-SecureString $gcpPrivateKey -AsPlainText`

-Forceを実行します。

9. 以下を実行して、既存のホスト接続を更新します。

```
Set-Item -PassThru -Path @('XDHyp:\Connections\<ENTER YOUR
    CONNECTION NAME HERE>') -SecurePassword $securePassword -
    UserName $gcpServiceAccount -CustomProperties $customProperty
<!--NeedCopy-->
```

必要な **GCP** 権限

このセクションでは、GCP の権限の完全な一覧が示されています。機能を正しく動作させるには、このセクションで示した権限の完全なセットを使用します。

> 注:
>
> GCP は、2024 年 4 月 29 日以降、Cloud Build サービスのデフォルトの動作とサービスアカウントの使用に関する変更を導入します。詳しくは、「Cloud Build サービスアカウントの変更」を参照してください。2024 年 4 月 29 日より前に Cloud Build API を有効にしていた既存の Google プロジェクトは、この変更の影響を受けません。ただし、4 月 29 日以降も既存の Cloud Build サービスの動作を維持する場合は、API を有効にする前に、制約の適用を無効にする組織ポリシーを作成または適用できます。新しい組織ポリシーを設定する場合でも、このセクションの既存の権限と、「**Cloud Build** サービスアカウントの変更前」と表示されている項目に従うことができます。そうでない場合は、「**Cloud Build** サービスアカウントの変更後」と表示されている既存の権限と項目に従います。

ホスト接続の作成

- プロビジョニングプロジェクトにおいて Citrix Cloud サービスアカウントに必要な最低限の権限:

```
compute.instanceTemplates.list
compute.instances.list
compute.networks.list
compute.projects.get
compute.regions.list
compute.subnetworks.list
compute.zones.list
resourcemanager.projects.get
<!--NeedCopy-->
```

  次の Google 定義の役割には、上に一覧表示された権限があります:

  - コンピューティング管理者
  - クラウドデータストアユーザー

- 共有 VPC プロジェクトにおいて Citrix Cloud サービスアカウントの共有 VPC に必要な追加の権限:


```
compute.networks.list
compute.subnetworks.list
resourcemanager.projects.get
<!--NeedCopy-->
```

次の Google 定義の役割には、上に一覧表示された権限があります:

- コンピューティングネットワークユーザー

VM の電源管理

プロビジョニングプロジェクトにおいて Citrix Cloud サービスアカウントに必要な最低限の権限（電源管理のみのカタログの場合）:

```
compute.instanceTemplates.list
compute.instances.list
compute.instances.get
compute.instances.reset
compute.instances.resume
compute.instances.start
compute.instances.stop
compute.instances.suspend
compute.networks.list
compute.projects.get
compute.regions.list
compute.subnetworks.list
compute.zones.list
resourcemanager.projects.get
compute.zoneOperations.get
<!--NeedCopy-->
```

次の Google 定義の役割には、上に一覧表示された権限があります:

- コンピューティング管理者
- クラウドデータストアユーザー

VM の作成、更新、または削除

- プロビジョニングプロジェクトにおいて Citrix Cloud サービスアカウントに必要な最低限の権限:

```
cloudbuild.builds.create
cloudbuild.builds.get
cloudbuild.builds.list
compute.acceleratorTypes.list
compute.diskTypes.get
compute.diskTypes.list
compute.disks.create
compute.disks.createSnapshot
```



```
compute.disks.delete
compute.disks.get
compute.disks.list
compute.disks.setLabels
compute.disks.use
compute.disks.useReadOnly
compute.firewalls.create
compute.firewalls.delete
compute.firewalls.list
compute.globalOperations.get
compute.images.create
compute.images.delete
compute.images.get
compute.images.list
compute.images.setLabels
compute.images.useReadOnly
compute.instanceTemplates.create
compute.instanceTemplates.delete
compute.instanceTemplates.get
compute.instanceTemplates.list
compute.instanceTemplates.useReadOnly
compute.instances.attachDisk
compute.instances.create
compute.instances.delete
compute.instances.detachDisk
compute.instances.get
compute.instances.list
compute.instances.reset
compute.instances.resume
compute.instances.setDeletionProtection
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setServiceAccount
compute.instances.setTags
compute.instances.start
compute.instances.stop
compute.instances.suspend
compute.machineTypes.get
compute.machineTypes.list
compute.networks.list
compute.networks.updatePolicy
compute.nodeGroups.list
compute.nodeTemplates.get
compute.projects.get
compute.regions.list
compute.snapshots.create
compute.snapshots.delete
compute.snapshots.list
compute.snapshots.get
compute.snapshots.setLabels
compute.snapshots.useReadOnly
compute.subnetworks.get
compute.subnetworks.list
```



```
compute.subnetworks.use
compute.zoneOperations.get
compute.zoneOperations.list
compute.zones.get
compute.zones.list
iam.serviceAccounts.actAs
resourcemanager.projects.get
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
compute.networks.get
compute.resourcePolicies.use

<!--NeedCopy-->
```

次の Google 定義の役割には、上に一覧表示された権限があります：

- コンピューティング管理者
- ストレージ管理者
- Cloud Build エディター
- サービスアカウントユーザー
- クラウドデータストアユーザー

- 共有 VPC プロジェクトから VPC およびサブネットワークを使用してホスティングユニットを作成するために、共有 VPC プロジェクトにおいて Citrix Cloud サービスアカウントの共有 VPC で必要な追加の権限：

```
compute.firewalls.list
compute.networks.list
compute.projects.get
compute.regions.list
compute.subnetworks.get
compute.subnetworks.list
compute.subnetworks.use
compute.zones.list
resourcemanager.projects.get
<!--NeedCopy-->
```

次の Google 定義の役割には、上に一覧表示された権限があります：

- コンピューティングネットワークユーザー
- クラウドデータストアユーザー

- （Cloud Build サービスアカウントの変更前）準備の指示ディスクを MCS にダウンロードするときに、プロビジョニングプロジェクトにおいて Cloud Build サービスアカウントで Google Cloud Build サービスが必要とする最低限の権限：

- （Cloud Build サービスアカウントの変更後）準備の指示ディスクを MCS にダウンロードするときに、プロビジョニングプロジェクトにおいて Cloud Compute サービスアカウントで Google Cloud Compute サービスが必要とする最低限の権限：

```
compute.disks.create
compute.disks.delete
compute.disks.get
compute.disks.list
compute.disks.setLabels
compute.disks.use
compute.disks.useReadOnly
compute.images.get
compute.images.list
compute.images.useReadOnly
compute.instances.create
compute.instances.delete
compute.instances.get
compute.instances.getSerialPortOutput
compute.instances.list
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setServiceAccount
compute.machineTypes.list
compute.networks.get
compute.networks.list
compute.projects.get
compute.subnetworks.list
compute.subnetworks.use
compute.subnetworks.useExternalIp
compute.zoneOperations.get
compute.zones.list
iam.serviceAccounts.actAs
logging.logEntries.create
pubsub.topics.publish
resourcemanager.projects.get
source.repos.get
source.repos.list
storage.buckets.create
storage.buckets.get
storage.buckets.list
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
<!--NeedCopy-->
```

次の Google 定義の役割には、上に一覧表示された権限があります：

  - Cloud Build サービスアカウント（Cloud Build サービスアカウントの変更後は、Cloud Compute サービスアカウントになります）
  - コンピューティングインスタンス管理者
  - サービスアカウントユーザー

- 準備の指示ディスクを MCS にダウンロードするときに、プロビジョニングプロジェクトにおいて Cloud Compute サービスアカウントで Google Cloud Build サービスが必要とする最低限の権限:

```
resourcemanager.projects.get
storage.objects.create
storage.objects.get
storage.objects.list
<!--NeedCopy-->
```

  次の Google 定義の役割には、上に一覧表示された権限があります:

  - コンピューティングネットワークユーザー
  - ストレージアカウントユーザー
  - クラウドデータストアユーザー

- (Cloud Build サービスアカウントの変更前) 準備の指示ディスクを MCS にダウンロードするときに、プロビジョニングプロジェクトにおいて Cloud Build サービスアカウントの共有 VPC で Google Cloud Build サービスが必要とする追加の権限:

- (Cloud Build サービスアカウントの変更後) 準備の指示ディスクを MCS にダウンロードするときに、プロビジョニングプロジェクトにおいて Cloud Compute サービスアカウントの共有 VPC で Google Cloud Compute サービスが必要とする追加の権限:

```
compute.firewalls.list
compute.networks.list
compute.subnetworks.list
compute.subnetworks.use
resourcemanager.projects.get
<!--NeedCopy-->
```

  次の Google 定義の役割には、上に一覧表示された権限があります:

  - コンピューティングネットワークユーザー
  - ストレージアカウントユーザー
  - クラウドデータストアユーザー

- プロビジョニングプロジェクトにおいて Citrix Cloud サービスアカウントのクラウドキー管理サービス (KMS) に必要な追加の権限:

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.list
cloudkms.keyRings.get
cloudkms.keyRings.list
<!--NeedCopy-->
```

  次の Google 定義の役割には、上に一覧表示された権限があります:

  - コンピューティング KMS 閲覧者

一般的な権限

以下はプロビジョニングプロジェクトで MCS がサポートするすべての機能に対する Citrix Cloud サービスアカウントの権限です。これらの権限では、今後も必要な互換性を提供する予定です。

```
resourcemanager.projects.get
cloudbuild.builds.create
cloudbuild.builds.get
cloudbuild.builds.list
compute.acceleratorTypes.list
compute.diskTypes.get
compute.diskTypes.list
compute.disks.create
compute.disks.createSnapshot
compute.disks.delete
compute.disks.get
compute.disks.setLabels
compute.disks.use
compute.disks.useReadOnly
compute.firewalls.create
compute.firewalls.delete
compute.firewalls.list
compute.globalOperations.get
compute.images.create
compute.images.delete
compute.images.get
compute.images.list
compute.images.setLabels
compute.images.useReadOnly
compute.instanceTemplates.create
compute.instanceTemplates.delete
compute.instanceTemplates.get
compute.instanceTemplates.list
compute.instanceTemplates.useReadOnly
compute.instances.attachDisk
compute.instances.create
compute.instances.delete
compute.instances.detachDisk
compute.instances.get
compute.instances.list
compute.instances.reset
compute.instances.resume
compute.instances.setDeletionProtection
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setTags
compute.instances.start
compute.instances.stop
compute.instances.suspend
compute.instances.update
compute.instances.updateAccessConfig
compute.instances.updateDisplayDevice
compute.instances.updateSecurity
```



```
compute.instances.updateShieldedInstanceConfig
compute.instances.updateShieldedVmConfig
compute.machineTypes.get
compute.machineTypes.list
compute.networks.list
compute.networks.updatePolicy
compute.nodeGroups.list
compute.nodeTemplates.get
compute.projects.get
compute.regions.list
compute.snapshots.create
compute.snapshots.delete
compute.snapshots.list
compute.snapshots.get
compute.snapshots.setLabels
compute.snapshots.useReadOnly
compute.subnetworks.get
compute.subnetworks.list
compute.subnetworks.use
compute.subnetworks.useExternalIp
compute.zoneOperations.get
compute.zoneOperations.list
compute.zones.get
compute.zones.list
resourcemanager.projects.get
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.list
cloudkms.keyRings.get
cloudkms.keyRings.list
compute.disks.list
compute.instances.setServiceAccount
compute.networks.get
compute.networks.use
compute.networks.useExternalIp
iam.serviceAccounts.actAs
compute.resourcePolicies.use
<!--NeedCopy-->
```

次の手順

- 初期展開プロセスを行っている場合は、「マシンカタログの作成」を参照してください。
- Google Cloud Platform（GCP）固有の情報については、「Google Cloud Platform カタログの作成」を

参照してください。

追加情報

- 接続とリソースの作成と管理
- Google Cloud 仮想化環境。

HPE Moonshot への接続

May 17, 2024

「接続とリソースの作成と管理」では接続を作成するためのウィザードについて説明しています。以下の情報は、HPE Moonshot に固有の詳細について説明しています。

> 注:
>
> HPE Moonshot への接続を作成する前に、まず HPE アカウントの設定を完了する必要があります。「HPE Moonshot 仮想化環境」を参照してください。

接続の作成

以下を使用して、HPE Moonshot への接続を作成できます:

- 完全な構成インターフェイス
- PowerShell コマンド

完全な構成インターフェイスを使用して接続を作成する

1. [接続およびリソースの追加] ページで、接続の種類として [**HPE Moonshot**] を選択します。
2. Moonshot iLO Chassis Manager の接続アドレスを入力します。アドレスには、IP アドレス、ホスト名、または FQDN を使用できます。
3. シャーシの管理資格情報とわかりやすい接続名を入力します。

次のいずれかの状況が発生すると、接続のセットアップは停止します:

- DaaS がエラーのあるパブリック CA 署名証明書を受信した場合: エラーメッセージが表示されます。画面上の指示に従って問題を解決してください。解決しない限り、接続の作成を続行できません。
- DaaS はプライベート CA 署名証明書を受信します。警告ページが表示されます。受信した拇印をサーバーの拇印と比較して、証明書の有効性を確認します。有効な場合は、[証明書を信頼する] を選択し、[**OK**] をクリックして接続の作成を続行します。その後、DaaS は証明書を信頼し、今後の検証のために拇印を保存します。

PowerShell コマンドを使用して接続を作成する

PowerShell コマンドを使用して接続を作成する場合は、次の情報を指定します:

- IP: HPE サーバーの IP アドレス
- ユーザー名: HPE ユーザー名
- パスワード: HPE パスワード

例:

```
New-Item -ConnectionType "Custom" -HypervisorAddress $IP -Metadata @{
 "Citrix_Orchestration_Hypervisor_Secret_Allow_Edit"="false" }
  -Path @("XDHyp:\Connections$connectionName") -Persist -PluginId "
     HPMoonshotFactory" -Scope @() -SecurePassword $Password -UserName
     $UserName -sslthumbprint $SslThumbprint New-
     BrokerHypervisorConnection -HypHypervisorConnectionUid
     $HypervisorConnectionID
<!--NeedCopy-->
```

> 注:
>
> `sslthumbprint`パラメーターは、プライベート CA 署名証明書の場合にのみ必須です。

証明書と拇印の検証

HPE Moonshot への接続を正常に作成するには、証明書にエラーがなく、拇印に正しい値が含まれている必要があります。証明書と拇印の検証に関連するユースケースは次のとおりです:

- パブリック CA 署名証明書にエラーがあります。接続が正常に作成されません。エラーの詳細を確認して問題を解決してください。
- パブリック CA 署名証明書にエラーがありません。接続は正常に作成され、`SslThumbprints`の値は **Null** です。
- プライベート CA 署名証明書にエラーがなく、`sslthumbprint`の値がありません。接続は正しい`SslThumbprints`の値で正常に作成されます。
- プライベート CA 署名証明書の拇印の値が正しくありません。接続が正常に作成されません。
- プライベート CA 署名証明書にエラーがありません。接続は正常に作成されます。接続を作成するとき、`SSlThumbprints`は **Null** です。`SSlThumbprints`の値は、サイトサービスによる値に更新されます。

接続の管理

このセクションでは、接続を管理する方法について詳しく説明します:

- 完全な構成インターフェイスを使用して証明書の問題を修正する
- PowerShell コマンドを使用して拇印の値を更新する

証明書の問題を修正する

DaaS は、証明書の問題が発生すると HPE Moonshot 接続をブロックし、ユーザーは関連する HPE Moonshot ノードでワークロードを配信および管理できなくなります。［ホスト接続］リストの接続の横にエラーアイコンが表示されます。特定の問題と解決策については、次の表を参照してください。

問題	解決策
パブリック CA 署名証明書で証明書エラーが発生する 受信した証明書はプライベート CA 署名証明書であるものの、有効期限が切れている。	接続をクリックし、［トラブルシューティング］タブを選択します。エラーの詳細を表示し、問題を解決します。ホスト接続を編集して証明書の拇印を更新します。詳細な手順: 1. 接続を選択し、［接続の編集］をクリックします。 1.［接続のプロパティ］ページで、［設定の編集］をクリックします。 1. HPE Moonshot シャーシに接続するためのパスワードを入力し、［保存］をクリックします。 1. 表示される ［警告］ページで、受信した拇印とサーバーの拇印を比較して証明書の有効性を確認します。 1. それらが同じ場合は、［証明書を信頼する］を選択し、［**OK**］をクリックします。

拇印の値を更新する

接続を作成した後、`Set-Item` PowerShell コマンドを使用して接続の拇印の値を更新できます。たとえば、次のコマンドを実行します:

1. 接続の詳細を取得します。例:

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
<!--NeedCopy-->
```

2. 拇印の値を更新します。例:

```
Set-Item -LiteralPath xdhyp:\connections\SinMoonshot-101 -Username
    Administrator -SslThumbprint
   xxxxxxxxxxx12AD048480631BB7AB10D69xxxxx
<!--NeedCopy-->
```

3. 更新された拇印の値を確認します。例:


```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
<!--NeedCopy-->
```

> 注:
>
> 正しくない拇印の値を`Set-Item`コマンドで指定すると、更新は失敗します。

次の手順

- 初期展開プロセスを行っている場合は、「マシンカタログの作成」を参照してください。
- HPE Moonshot 固有の情報については、「HPE Moonshot マシンカタログの作成」を参照してください。

追加情報

- 接続とリソースの作成と管理
- HPE Moonshot 仮想化環境

Microsoft Azure への接続

May 17, 2024

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

「接続とリソースの作成と管理」では接続を作成するためのウィザードについて説明しています。以下の情報は、Azure Resource Manager クラウド環境に固有の詳細について説明しています。

> 注:
>
> Microsoft Azure への接続を作成する前に、Azure アカウントをリソースの場所として設定する必要があります。「Microsoft Azure Resource Manager 仮想化環境」を参照してください。

サービスプリンシパルと接続の作成

接続を作成する前に、接続で Azure リソースへのアクセスに使用されるサービスプリンシパルを設定する必要があります。接続は次の 2 つの方法で作成できます。

- 完全な構成を使用したサービスプリンシパルと接続の作成
- 以前に作成したサービスプリンシパルを使用した接続の作成

このセクションでは、次のタスクを完了する方法を説明します。

- 完全な構成を使用したサービスプリンシパルと接続の作成
- PowerShell を使用したサービスプリンシパルの作成
- Azure でのアプリケーションシークレットの取得
- 既存のサービスプリンシパルを使用した接続の作成

注意事項

始める前に、次の考慮事項に注意してください:

- *Contributor*（投稿者）の役割でサービスプリンシパルを使用することを Citrix ではお勧めします。ただし、最低限の権限の一覧を取得する方法については、「最低限の権限」セクションを参照してください。
- 最初の接続を作成するときに、必要な権限付与を求めるプロンプトが Azure で表示されます。その後の接続でも認証は必要ですが、Azure では以前の同意が記憶され、このプロンプトは再表示されません。
- Azure で初めて認証すると、認証されたアカウントの代わりに、Citrix 所有のマルチテナントアプリケーション（ID: 08b70dc3-76c5-4611-ba7d-3312ba36cb2b）が Azure Active Directory に招待されます。［接続の詳細］ページで ［**Azure AD** 参加済みデバイスの管理を有効にする］を選択した場合は、Citrix はこのアプリケーションを使用して新しいサービスプリンシパルを作成し、ワークロードのプロビジョニングと Azure AD デバイス管理に適した権限を付与します。
- 認証に使用されるアカウントは、サブスクリプションの共同管理者である必要があります。
- 認証に使用されるアカウントは、サブスクリプションのディレクトリのメンバーである必要があります。注意すべき 2 つのタイプのアカウントがあります。「職場または学校」と「個人用 Microsoft アカウント」です。詳しくは、CTX219211を参照してください。
- 既存の Microsoft アカウントは、サブスクリプションのディレクトリのメンバーとして追加することで使用できますが、ユーザーが以前にそのディレクトリのリソースのいずれかへのゲストアクセスを許可されていた場合は、複雑になる可能性があります。この場合、必要な権限を与えないディレクトリにプレースホルダーエントリが存在し、エラーが返されることがあります。

  このエラーを修正するには、ディレクトリからリソースを削除し、明示的に追加し直します。ただし、そのアカウントがアクセスできる他のリソースに対して、予期しない影響を与えるので、このオプションは注意深く実行してください。
- 特定のアカウントが実際にメンバーであるときにディレクトリゲストとして検出されるという既知の問題があります。このような構成は、通常、以前に設定されたディレクトリアカウントで発生します。回避策: アカウントをディレクトリに追加します。これにより適切なメンバーシップ値が取得されます。

- リソースグループはリソースのコンテナにすぎず、そのリージョン以外のリージョンのリソースを含む場合があります。これが原因で、リソースグループのリージョンに表示されているリソースを利用できると期待した場合に、混乱を招く可能性があります。
- ネットワークとサブネットが、必要な数のマシンをホストするのに十分な大きさであることを確認してください。これには多少先見の明が必要ですが、Microsoft が、アドレススペースの容量に関するガイダンスを示して、適切な値を指定できるようサポートします。

完全な構成を使用したサービスプリンシパルと接続の作成

> 重要:
>
> この機能は、Azure China のサブスクリプションではまだ利用できません。

完全な構成では、サービスプリンシパルと接続の両方を 1 つのワークフローで作成できます。サービスプリンシパルにより、接続で Azure リソースにアクセスできるようになります。Azure に認証してサービスプリンシパルを作成すると、Azure にアプリケーションが登録されます。登録されたアプリケーションの秘密キー（クライアントシークレットまたはアプリケーションシークレットと呼ばれる）が作成されます。登録されたアプリケーション（この場合は接続）は、クライアントシークレットを使用して Azure AD に認証します。

手順を開始する前に、次の前提条件を満たしていることを確認してください。

- サブスクリプションの Azure Active Directory テナントにユーザーアカウントがあること。
- Azure AD のユーザーアカウントが、リソースのプロビジョニングに使用する Azure サブスクリプションの共同管理者でもあること。
- 認証のグローバル管理者、アプリケーション管理者、またはアプリケーション開発者の権限があること。この権限は、ホスト接続の作成後に失効する可能性があります。役割について詳しくは、「Azure AD の組み込みロール」を参照してください。

接続およびリソースの追加ウィザードを使用して、サービスプリンシパルと接続を同時に作成します。

1. ［接続］ページで ［新しい接続を作成する］を選択します。次に、接続の種類として ［**Microsoft Azure**］を選択し、Azure 環境を選択します。
2. 仮想マシンの作成にどのツールを使用するかを選択し、［次へ］を選択します。
3. ［接続の詳細］ページで、サービスプリンシパルを作成し、接続名を次のように設定します。

    a) 古い Azure AD 参加デバイスを自動的にクリーンアップするための接続権限を付与するには、［**Enable Azure AD joined device management**］を選択します。このオプションを選択することを推奨するケースは、そのような接続を使用して Azure AD 参加マシンを作成したい場合です。詳しくは、「Azure AD 参加デバイス管理を有効にする」を参照してください。

    b) Azure サブスクリプション ID と接続の名前を入力しますサブスクリプション ID を入力すると、［新規作成］ボタンが有効になります。

> 注:
>
> 接続名は 1～64 文字にし、空白スペースのみにしたり記号（\/;:#.*?=<>|[]{ } "'()'）を含めたりすることはできません。

a) ［新規作成］を選択してから、Azure Active Directory アカウントのユーザー名とパスワードを入力します。

b) ［サインイン］を選択します。

c) ［承認］を選択して、表示された権限を Citrix DaaS に付与します。Azure によって、指定されたユーザーの代わりに Citrix DaaS が Azure リソースを管理できるようにするサービスプリンシパルが作成されます。

d) ［承認］を選択すると、［接続の詳細］ページに戻ります。

> 注:
>
> Azure への認証に成功すると、［新規作成］ボタンと ［既存を使用］ボタンが表示されなくなります。緑色のチェックマークが付いた「接続に成功しました」というテキストが表示され、これは Azure サブスクリプションへの接続に成功したことを示します。

e) API 要求を Citrix Cloud Connector 経由で Azure にルーティングするには、［**Citrix Cloud Connector** 経由のトラフィックをルーティングする］チェックボックスをオンにします。

また、PowerShell を使用してこの機能を有効にすることもできます。詳しくは、「Azure 管理トラフィックのための安全な環境の作成」を参照してください。

> 注:
>
> このオプションは、展開内にアクティブな Citrix Cloud Connector がある場合にのみ使用できます。この機能は現時点では Connector Appliance でサポートされていません。

f) ［次へ］を選択します。

> 注:
>
> Azure への認証が完了し、必要な権限の付与に同意しない限り、次のページに進むことはできません。

4. 接続用のリソースを次の手順で構成します:

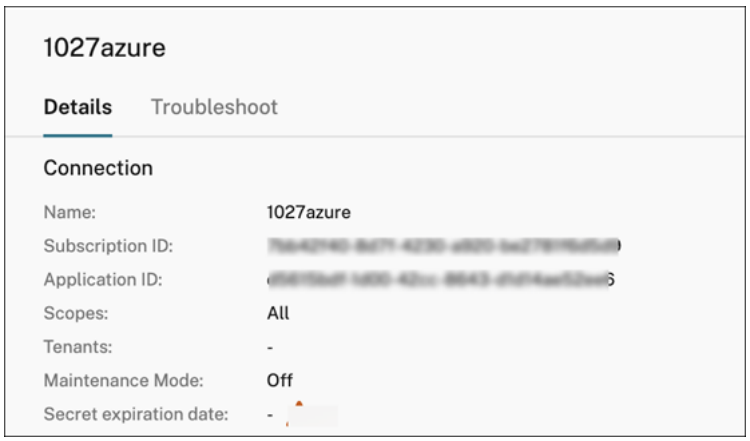
- ［リージョン］ページで領域を選択します。
- ［ネットワーク］ページで、次の手順を実行します:
  - 1～64 文字のリソース名を入力して、リージョンとネットワークの組み合わせを特定できるようにします。リソース名は、空白のみにしたり記号（\/;:#.*?=<>|[]{ } "'()'）を含めたりすることはできません。

- 仮想ネットワークとリソースグループのペアを選択します。（複数の仮想ネットワークを同じ名前にする場合、ネットワーク名とリソースグループをペアリングすると一意の組み合わせになります。）前のページで選択したリージョンに仮想ネットワークがない場合は、前のページに戻って仮想ネットワークのあるリージョンを選択します。

5. ［概要］ページで、設定の概要を表示し、［完了］を選択してセットアップを完了します。

アプリケーション **ID** の表示　接続を作成した後、その接続で Azure リソースへのアクセスに使用されるアプリケーション ID を表示できます。

［接続およびリソースの追加］一覧で、接続を選択して詳細を表示します。［詳細］タブで、アプリケーション ID が表示されます。



PowerShell を使用したサービスプリンシパルの作成

PowerShell を使用してサービスプリンシパルを作成するには、Azure Resource Manager サブスクリプションに接続して、後述の PowerShell コマンドレットを使用します。

以下のアイテムを必ず準備してください。

- **SubscriptionId**: VDA をプロビジョニングするサブスクリプションの Azure Resource Manager `SubscriptionID`。
- **ActiveDirectoryID**: Azure AD に登録したアプリケーションのテナント ID。
- **ApplicationName**: Azure AD 内で作成されるアプリケーションの名前。

詳細な手順は次のとおりです:

1. Azure Resource Manager サブスクリプションに接続します。

   ```
   Connect-AzAccount
   ```

2. サービスプリンシパルを作成する Azure Resource Manager サブスクリプションを選択します。


```
Get-AzSubscription -SubscriptionId $subscriptionId | Select-
AzSubscription
```

3. AD テナントでアプリケーションを作成します。

```
$AzureADApplication = New-AzADApplication -DisplayName $ApplicationName
```

4. サービスプリンシパルを作成します。

```
New-AzADServicePrincipal -ApplicationId $AzureADApplication.AppId
```

5. サービスプリンシパルに役割を割り当てます。

```
New-AzRoleAssignment -RoleDefinitionName Contributor -ServicePrincipalName
 $AzureADApplication.AppId -scope /subscriptions/$SubscriptionId
```

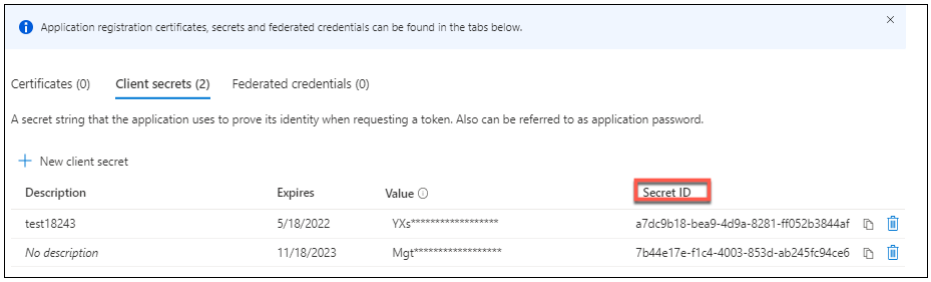
6. PowerShell コンソールの出力ウィンドウから、ApplicationId をメモします。この ID は、ホスト接続を作成するときに使用します。

Azure でのアプリケーションシークレットの取得

既存のサービスプリンシパルを使用して接続を作成するには、まず Azure Portal でサービスプリンシパルのアプリケーション ID とシークレットを取得する必要があります。

詳細な手順は次のとおりです:

1. アプリケーション **ID** は、[完全な構成] インターフェイスから、または PowerShell を使用して取得します。
2. Azure Portal にサインインします。
3. Azure で [**Azure Active Directory**] を選択します。
4. Azure AD の [**App registrations**] でアプリケーションを選択します。
5. [**Certificates & secrets**] に移動します。
6. [**Client secrets**] をクリックします。



既存のサービスプリンシパルを使用した接続の作成

サービスプリンシパルが既にある場合は、そのサービスプリンシパルと完全な構成を使用して接続を作成できます。

以下のアイテムを必ず準備してください。

- サブスクリプション ID
- Active Directory ID（テナント ID）
- アプリケーション ID
- アプリケーションシークレット

  詳しくは、「アプリケーションシークレットの取得」を参照してください。
- シークレットの有効期限

詳細な手順は次のとおりです：

接続およびリソースの追加ウィザードで以下を行います：

1. ［接続］ページで ［新しい接続を作成する］を選択します。次に、接続の種類として ［**Microsoft Azure**］を選択し、Azure 環境を選択します。
2. 仮想マシンの作成にどのツールを使用するかを選択し、［次へ］を選択します。
3. ［接続の詳細］ページで、Azure サブスクリプション ID と接続の名前を入力します。

   > 注：
   >
   > 接続名は 1～64 文字にし、空白スペースのみにしたり記号（`\/;:#.*?=<>|[]{ } "'()'`）を含めたりすることはできません。

4. ［既存を使用］を選択します。［既存のサービスプリンシパルの詳細］ウィンドウで、既存のサービスプリンシパルに次の設定を入力します。詳細を入力すると、［保存］ボタンが有効になります。［**Save**］を選択します。有効な詳細を入力しない限り、このページの先には進めません。

   - サブスクリプション **ID**。Azure サブスクリプション ID を入力します。サブスクリプション ID を取得するには、Azure Portal にサインインし、［**Subscriptions**］**>** ［**Overview**］に移動します。
   - **Active Directory ID**（テナント ID）。Azure AD に登録したアプリケーションのディレクトリ（テナント）ID を入力します。
   - アプリケーション **ID**。Azure AD に登録したアプリケーションのアプリケーション（クライアント）ID を入力します。
   - アプリケーションシークレット。秘密キー（クライアントシークレット）。登録されたアプリケーションは、キーを使用して Azure AD への認証を行います。セキュリティのために、キーを定期的に変更することをお勧めします。後でキーを取得することはできないため、必ずキーを保存してください。
   - シークレットの有効期限。アプリケーションシークレットの有効期限が切れる日付を入力します。シークレットキーの有効期限が切れる前に、コンソールに通知が表示されます。ただし、秘密キーの有効期限が切れると、エラーが発生します。

> 注:
>
> セキュリティ上の理由から、有効期限は現在から 2 年を超えることはできません。

- 認証 **URL**。このフィールドは自動的に入力され、編集できません。
- 管理 **URL**。このフィールドは自動的に入力され、編集できません。
- ストレージのサフィックス。このフィールドは自動的に入力され、編集できません。

  Azure で MCS カタログを作成するには、次のエンドポイントへのアクセスが必要です。これらのエンドポイントにアクセスすると、ネットワークと Azure Portal およびそのサービスとの間の接続が最適化されます。

  - 認証 URL: https://login.microsoftonline.com/
  - 管理 URL: https://management.azure.com/。これは、Azure Resource Manager プロバイダー API の要求 URL です。管理用のエンドポイントは環境によって異なります。たとえば、Azure Global の場合はhttps://management.azure.com/、Azure US Government の場合はhttps://management.usgovcloudapi.net/です。
  - ストレージのサフィックス: https://*.core.windows.net./。ここで「*」は、ストレージ サフィックスのワイルドカード文字です。例: https://demo.table.core.windows.net/。

5. [保存] を選択すると、[接続の詳細] ページに戻ります。[次へ] を選択して、次のページに進みます。
6. 接続用のリソースを次の手順で構成します:

   - [リージョン] ページで領域を選択します。
   - [ネットワーク] ページで、次の手順を実行します:
     - 1〜64 文字のリソース名を入力して、リージョンとネットワークの組み合わせを特定できるようにします。リソース名は、空白のみにしたり記号（`\/;:#.*?=<>|[]{ } "'()'`）を含めたりすることはできません。
     - 仮想ネットワークとリソースグループのペアを選択します。（複数の仮想ネットワークを同じ名前にする場合、ネットワーク名とリソースグループをペアリングすると一意の組み合わせになります。）前のページで選択したリージョンに仮想ネットワークがない場合は、前のページに戻って仮想ネットワークのあるリージョンを選択します。
7. [概要] ページで、設定の概要を表示し、[完了] を選択してセットアップを完了します。

サービスプリンシパルと接続の管理

このセクションでは、サービスプリンシパルと接続を管理する方法について説明します。

- Azure の調整設定の構成
- Azure AD 参加デバイスの管理を有効にする
- 既存のホスト接続のサービスプリンシパルを管理する

- Azure でイメージの共有を有効にする
- ［完全な構成］を使用して共有テナントを接続に追加する
- PowerShell を使用した画像共有の実装
- Azure 管理トラフィックのための安全な環境の作成
- アプリケーションシークレットとその有効期限の管理

Azure の調整設定の構成

Azure Resource Manager はサブスクリプションおよびテナントの要求を調整し、プロバイダーの特定のニーズに対応して定義された制限を基にルーティングします。詳しくは、Microsoft 社のサイトの「Resource Manager の要求のスロットル」を参照してください。制限は、サブスクリプションやテナントで多数のマシンの管理が問題となりうる場合に存在します。たとえば、多数のマシンを含むサブスクリプションは、電源操作に関連してパフォーマンスの問題が発生することがあります。

> ヒント：
>
> 詳しくは「Machine Creation Services による Azure のパフォーマンスの向上」を参照してください。

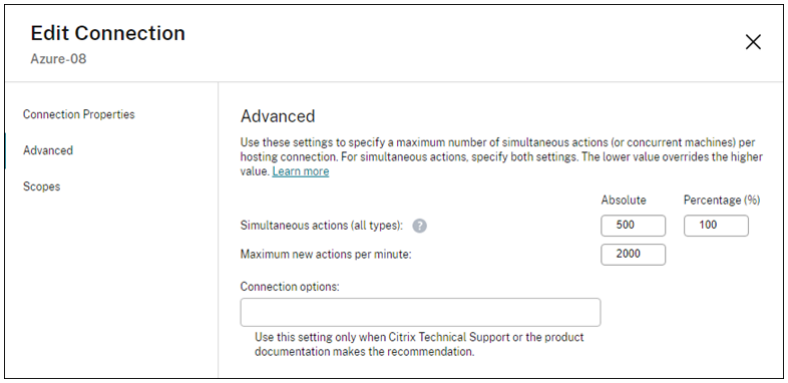
Citrix DaaS では、これらの問題の影響を軽減するために MCS 内部の調整を削除して、より高い値の Azure の要求クォータを利用することができます。

大量のサブスクリプション（1,000 台の仮想マシンを含む場合など）で仮想マシンをオンまたはオフにする場合、次の最適設定をお勧めします：

- 絶対同時操作：500
- 1 分あたりの最大新規操作：2000
- 最大同時操作：500

［完全な構成］インターフェイスを使用して、指定のホスト接続で Azure 操作を構成します：

1. ［管理］**>**［完全な構成］の左側ペインで ［ホスト］を選択します。
2. Azure 関連の接続を選択して編集します。
3. 接続の編集ウィザードで ［詳細設定］を選択します。
4. ［詳細設定］画面で構成オプションを使用し、同時操作の数、1 分あたりの最大新規操作、その他追加の接続オプションを指定します。



MCS は、デフォルトで最大 500 の同時操作をサポートします。または、Remote PowerShell SDK を使用して、同時操作の最大数を設定することもできます。

PowerShell プロパティ`MaximumConcurrentProvisioningOperations`を使用して、同時 Azure プロビジョニング操作の最大数を指定します。このプロパティを使用するときは、次のことを考慮してください:

- `MaximumConcurrentProvisioningOperations`のデフォルト値は 500 です。
- PowerShell コマンド`Set-item`を使用して`MaximumConcurrentProvisioningOperations`パラメーターを構成します。

Azure AD 参加デバイスの管理を有効にする

Azure 内で古い Azure AD 参加デバイスがあると、新しいマシンが Azure AD に参加できなくなるので、正常に動作できなくなる可能性があります。問題発生の可能性をなくすために、Azure AD 参加デバイスを管理する権限を接続に付与できます。接続は、この権限を使用することで、古くなった Azure AD 参加デバイスを自動的にクリーンアップできます。

> 注:
>
> マシンまたはマシンカタログを削除するときに、Azure AD 参加デバイスを Azure AD から削除することはできません。

1. ［管理］**>**［完全な構成］の左側ペインで［ホスト］を選択します。
2. 接続を選択し、操作バーの ［接続の編集］を選択します。
3. 左側ペインから ［接続のプロパティ］を選択します。
4. 表示される 「接続のプロパティ」ページで、次の手順を実行します。
    a) ［**Enable Azure AD joined device management**］を選択します。
    b) ［**Save**］をクリックします。
    c) 表示される Azure のサインインウィンドウで、サブスクリプションのパスワードを入力し、［サインイン］を選択します。

サインインが完了すると、ホスト接続とリソースのリストに戻ります。リスト内の接続をクリックし、下部ペインの「詳細」タブをクリックします。[**Azure AD joined device management**]フィールドに“有効”と表示されますので、確認してください。

完全な構成で Azure AD 参加デバイスの管理を有効にする場合は、選択したホスト接続の作成方法（新規作成または既存の使用）に関わらず、Azure AD で認証する必要があります。Azure AD の組み込みのクラウドデバイス管理者役割は、サービスプリンシパルに割り当てられます。Azure AD 参加デバイスの管理に対する最小限の権限を採用するには、サービスプリンシパルからクラウドデバイス管理者役割の割り当てを手動で削除し、最小限の権限のみを含んでいる Azure AD カスタム役割を作成して、それをサービスプリンシパルに割り当てることができます。

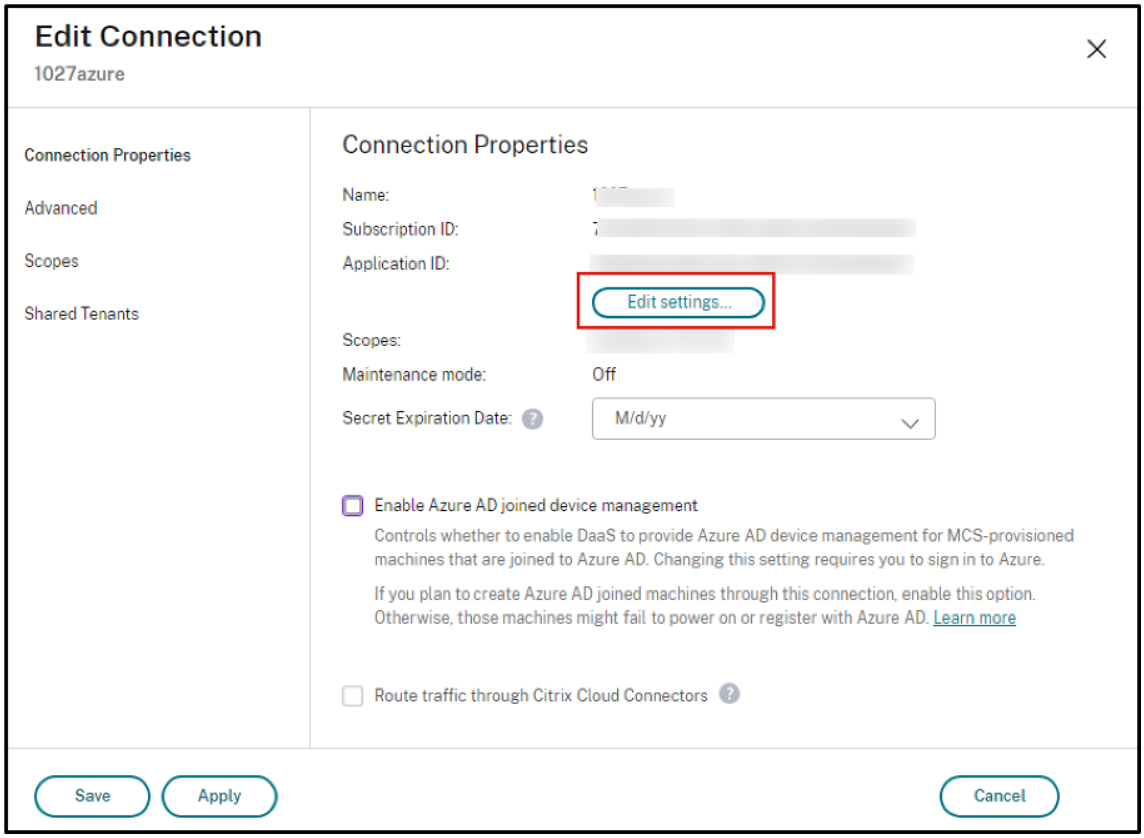
> 注:
>
> - Azure AD 参加デバイス管理の最小限の権限は、Azure Resource Manager の権限ではなく、Azure AD の権限です。これらをサービスプリンシパルに明示的に割り当てることはできません。これらの権限を含んでいるカスタム役割を Azure AD に作成し、サービスプリンシパルに割り当てる必要があります。詳しくは、「Azure Active Directory でのカスタム役割の作成と割り当て」を参照してください。
> - Azure AD でカスタム役割を作成するには、Azure AD Premium P1 または P2 ライセンスが必要です。

既存のホスト接続のサービスプリンシパルを管理する

サービスプリンシパルを使用してホスト接続を作成した後、次のホスト接続を編集することを選択できます:

- 新しいサービスプリンシパル
- 別の既存のサービスプリンシパルを使用する

1. ［管理］**>**［完全な構成］の左側ペインで ［ホスト］を選択します。
2. 接続を選択し、操作バーの ［接続の編集］を選択します。
3. 左側ペインから ［接続のプロパティ］を選択します。
4. 開いた ［接続のプロパティ］ページで、［設定の編集］をクリックします。新しいサービスプリンシパルを作成するか、別の既存のサービスプリンシパルを使用するかを選択できます。



- 新しいサービスプリンシパルを作成するには、［サービスプリンシパルを作成する］をクリックします。プロンプトに従って、Azure AD ユーザーアカウントにログインします。Citrix は、マルチテナントアプリケーション ID 08b70dc3-76c5-4611-ba7d-3312ba36cb2bを使用して、既存のホスト接続用の新しいサービスプリンシパルを作成し、適切な権限を付与します。

  ［接続プロパティ］ページで ［**Azure AD** 参加済みデバイスの管理を有効にする］を選択すると、新しく作成されたサービスプリンシパルに Azure AD 組み込みのクラウドデバイス管理者の役割が割り当てられます。

- ホスト接続に別の既存のサービスプリンシパルを使用するには、［既存を使用する］をクリックします。ただし、次の 2 つの場合が考えられます：

  – ［**Azure AD** 参加デバイスの管理を有効にする］を選択する場合は、Azure AD ユーザーアカウントにログインするように求められます。Citrix は、マルチテナントアプリケーション ID 08b70dc3-76c5-4611-ba7d-3312ba36cb2bを使用して、Azure AD 組み込みのクラウドデバイス管理者の役割を既存のサービスプリンシパルに割り当てます。
  – ［**Azure AD** 参加デバイスの管理を有効にする］を選択しない場合は、Azure AD ユーザーアカウントにログインするように求められません。既存のサービスプリンシパルのアプリケーション ID とシークレットを入力します。

Azure AD 参加済みデバイスの管理を有効にする方法については、「Azure AD 参加済みデバイスの管理を有効にする」を参照してください。

Azure でイメージの共有を有効にする

マシンカタログを作成または更新するときに、(Azure Compute Gallery を介して共有する) さまざまな Azure テナントおよびサブスクリプションからイメージを選択できます。テナント内またはテナント間での画像の共有を有効にするには、Azure で必要な設定を行う必要があります。

- 単一のテナント内（サブスクリプション間）でのイメージの共有
- テナント間でのイメージの共有

単一のテナント内（サブスクリプション間）でのイメージの共有　別のサブスクリプションに属する Azure Compute Gallery のイメージを選択するには、そのイメージをそのサブスクリプションのサービスプリンシパル（SPN）と共有する必要があります。

たとえば、Studio で次のように構成されているサービスプリンシパル（SPN 1）があるとします:

サービスプリンシパル: SPN 1

サブスクリプション: サブスクリプション 1

テナント: テナント 1

画像が別のサブスクリプションにあり、Studio で次のように構成されているとします:

サブスクリプション: サブスクリプション 2

テナント: テナント 1

サブスクリプション 2 のイメージをサブスクリプション 1（SPN 1）と共有する場合は、サブスクリプション 2 に移動し、リソースグループを SPN 1 と共有します。

イメージは、Azure の役割ベースのアクセス制御（RBAC）を使用して別の SPN と共有する必要があります。Azure RBAC は、Azure リソースへのアクセスを管理するために使用される承認システムです。Azure RBAC について詳しくは、Microsoft 社のドキュメント「Azure ロールベースのアクセス制御（Azure RBAC）とは」を参照してください。アクセス権を付与するには、Contributor の役割を使用して、リソースグループのスコープでサービスプリンシパルに役割を割り当てます。Azure の役割を割り当てるには、ユーザーアクセス管理者や所有者などの`Microsoft.Authorization/roleAssignments/write`権限が必要です。別の SPN と画像を共有する方法について詳しくは、Microsoft 社のドキュメント「Azure portal を使用して Azure ロールを割り当てる」を参照してください。

テナント間でのイメージの共有　Azure Compute Gallery を使用してテナント間でイメージを共有するには、アプリケーション登録を作成します。

たとえば、2 つのテナント（テナント 1 とテナント 2）があり、イメージギャラリーをテナント 1 と共有する場合は、次のようにします:

1. テナント 1 のアプリケーション登録を作成します。詳しくは、「アプリの登録を作成する」を参照してください。

2. ブラウザーでサインインを要求し、テナント 2 にアプリケーションへのアクセスを許可します。Tenant2 IDをテナント 1 のテナント ID に置き換えます。Application (client)ID を、作成したアプリケーション登録のアプリケーション ID に置き換えます。置換が完了したら、この URL をブラウザーに貼り付け、サインインプロンプトに従ってテナント 2 にサインインします。例:

```
https://login.microsoftonline.com/<Tenant 2 ID>/oauth2/authorize?
    client_id=<Application (client) ID>&response_type=code&
    redirect_uri=https%3A%2F%2Fwww.microsoft.com%2F
<!--NeedCopy-->
```

詳しくは、「テナント 2 にアクセス権を付与する」を参照してください。

3. テナント 2 リソースグループへのアプリケーションアクセスを許可します。テナント 2 としてサインインし、アプリケーション登録に、ギャラリーイメージを含むリソースグループへのアクセスを許可します。詳しくは、「テナントをまたいだ認証要求」を参照してください。

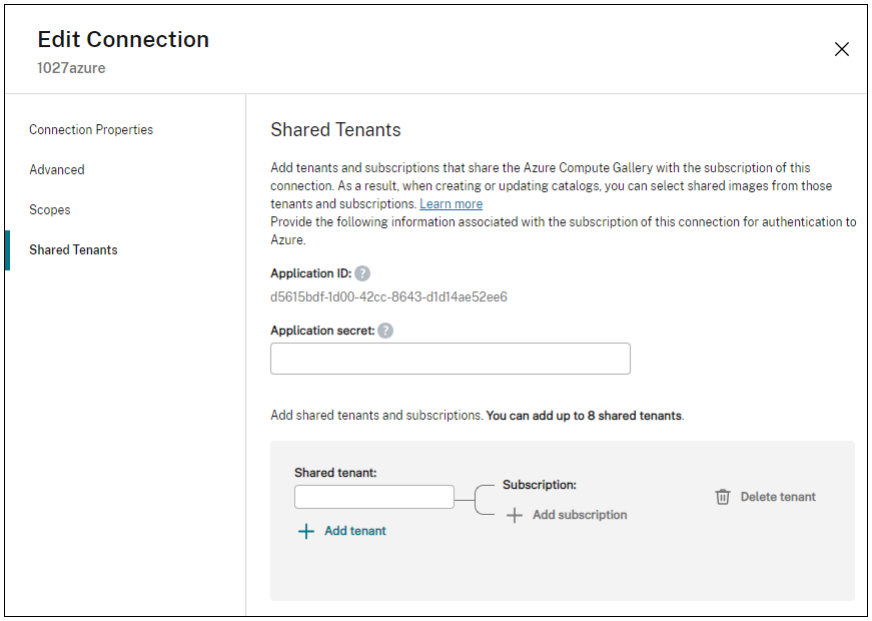
[完全な構成] を使用して共有テナントを接続に追加する

[完全な構成] インターフェイスでマシンカタログを作成または更新するときに、(Azure Compute Gallery を介して共有する) さまざまな Azure テナントおよびサブスクリプションから共有イメージを選択できます。この機能では、関連付けられたホスト接続の共有テナントおよびサブスクリプション情報を提供する必要があります。

> 注:
>
> テナント間での画像の共有を有効にするための必要な設定を Azure で構成したことを確認してください。詳しくは、「テナント間でのイメージの共有」を参照してください。

接続ごとに次の手順を実行します:

1. [管理] > [完全な構成] の左側ペインで [ホスト] を選択します。
2. 接続を選択し、操作バーの [接続の編集] を選択します。



3. ［共有テナント］で、次の操作を行います：

   a) 接続のサブスクリプションに関連付けられているアプリケーション ID とアプリケーションシークレットを提供します。DaaS は、この情報を使用して Azure AD に認証します。
   b) 接続のサブスクリプションと Azure Compute Gallery を共有しているテナントとサブスクリプションを追加します。テナントごとに最大 8 つの共有テナントと 8 つのサブスクリプションを追加できます。

4. 完了したら、［適用］を選択して行った変更を適用しウィンドウを開いたままにするか、［**OK**］を選択して変更を適用しウィンドウを閉じます。

PowerShell を使用した画像共有の実装

このセクションでは、PowerShell を使用して画像を共有するプロセスについて説明します。

- 別のサブスクリプションでの画像の選択
- ホスト接続のカスタムプロパティの共有テナント ID の更新
- 別のテナントでの画像の選択

別のサブスクリプションでの画像の選択　同じ Azure テナント内の別の共有サブスクリプションに属する Azure Compute Gallery のイメージを選択し、PowerShell コマンドを使用して MCS カタログを作成および更新できます。

1. ホスティングユニットのルートフォルダーに、`sharedsubscription`という名前の新しい共有サブスクリプションフォルダーが作成されます。
2. テナント内のすべての共有サブスクリプションを表示します。


```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\sharedsubscription.folder"
<!--NeedCopy-->
```

3. 1 つの共有サブスクリプションを選択し、その共有サブスクリプションのすべての共有リソースグループを表示します。

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123.sharedsubscription"
<!--NeedCopy-->
```

4. リソースグループを選択し、そのリソースグループのすべてのギャラリーを表示します。

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123.sharedsubscription\ xyz.resourcegroup"
<!--NeedCopy-->
```

5. ギャラリーを選択し、そのギャラリーのすべてのイメージ定義を表示します。

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resourcegroup\testgallery.gallery"
<!--NeedCopy-->
```

6. 1 つのイメージ定義を選択し、そのイメージ定義のすべてのイメージバージョンを表示します。

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resourcegroup\sigtestdef.imagedefinition"
<!--NeedCopy-->
```

7. 次の要素を使用して、MCS カタログを作成および更新します:

   - リソースグループ
   - ギャラリー
   - ギャラリーイメージの定義
   - ギャラリーイメージのバージョン

   Remote PowerShell SDK を使用してカタログを作成する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/を参照してください。

ホスト接続のカスタムプロパティの共有テナント **ID** の更新　`Set-Item`を使用して、ホスト接続のカスタムプロパティを共有テナント ID とサブスクリプション ID で更新します。`CustomProperties`にプロパティ`SharedTenants`を追加します。`Shared Tenants`の形式は次のとおりです:

```
[{
 "Tenant":"94367291-119e-457c-bc10-25337231f7bd","Subscriptions":["7bb42f40-8d7f-4230-a920-be2781f6d5d9"] }
```



```
 ,{
 "Tenant":"50e83564-c4e5-4209-b43d-815c45659564","Subscriptions":["06
    ab8944-6a88-47ee-a975-43dd491a37d0"] }
 ]
<!--NeedCopy-->
```

例:

```
Set-Item -CustomProperties "<CustomProperties xmlns=`"http://schemas.
   citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org
   /2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`" Value=`"
   123`" />
<Property xsi:type=`"StringProperty`" Name=`"ManagementEndpoint`" Value
   =`"https://management.azure.com/`" />
<Property xsi:type=`"StringProperty`" Name=`"AuthenticationAuthority`"
   Value=`"https://login.microsoftonline.com/`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageSuffix`" Value=`"
   core.windows.net`" />
<Property xsi:type=`"StringProperty`" Name=`"TenantId`" Value=`"123abc`
   " />
<Property xsi:type=`"StringProperty`" Name=`"SharedTenants`" Value=`"`[
    {
  'Tenant':'123abc', 'Subscriptions':['345', '567']  }
  ]`"` />
</CustomProperties>"
-LiteralPath @("XDHyp:\Connections\aazure") -PassThru -UserName "
   advc345" -SecurePassword
$psd
<!--NeedCopy-->
```

> 注:
>
> 複数のテナントを追加できます。各テナントは複数のサブスクリプションを持つことができます。

別のテナントでの画像の選択　別の Azure テナントに属する Azure Compute Gallery のイメージを選択し、PowerShell コマンドを使用して MCS カタログを作成および更新できます。

1. ホスティングユニットのルートフォルダーに、sharedsubscriptionという名前の新しい共有サブスクリプションフォルダーが作成されます。
2. すべての共有サブスクリプションを表示します。

   ```
   Get-ChildItem XDHyp:\HostingUnits\azres\sharedsubscription.folder
   <!--NeedCopy-->
   ```

3. 1 つの共有サブスクリプションを選択し、その共有サブスクリプションのすべての共有リソースグループを表示します。

   ```
   Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
      sharedsubscription
   ```



```
<!--NeedCopy-->
```

4. リソースグループを選択し、そのリソースグループのすべてのギャラリーを表示します。

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription\ xyz.resourcegroup
<!--NeedCopy-->
```

5. ギャラリーを選択し、そのギャラリーのすべてのイメージ定義を表示します。

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription\xyz.resourcegroup\efg.gallery
<!--NeedCopy-->
```

6. 1 つのイメージ定義を選択し、そのイメージ定義のすべてのイメージバージョンを表示します。

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription\xyz.resourcegroup\efg.gallery\hij.
    imagedefinition
<!--NeedCopy-->
```

7. 次の要素を使用して、MCS カタログを作成および更新します:

   - リソースグループ
   - ギャラリー
   - ギャラリーイメージの定義
   - ギャラリーイメージのバージョン

   Remote PowerShell SDK を使用してカタログを作成する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/を参照してください。

Azure 管理トラフィックのための安全な環境の作成

MCS により、Cloud Connector を介してネットワークトラフィック（Citrix Cloud から Azure Hypervisor への API 呼び出し）を環境内でルーティングできるようになります。この実装により、Azure サブスクリプションを認証して、特定の IP アドレスからのネットワークトラフィックを許可することができます。これを行うには、`CustomProperties`に`ProxyHypervisorTrafficThroughConnector`を追加します。カスタムプロパティを設定した後、Azure Managed Disks へのプライベートディスクアクセスを許可する Azure ポリシーを構成できます。

プライベートエンドポイントを使用するために、新しいディスクごとにディスクアクセスを自動的に作成するように Azure ポリシーを構成した場合、Azure によって適用される同じディスクアクセスオブジェクトで、同時に 5 つを超えるディスクまたはスナップショットをアップロードまたはダウンロードすることはできません。この制限は、Azure ポリシーをリソースグループレベルで構成する場合はマシンカタログごとに適用され、Azure ポリシーをサブスクリプションレベルで構成する場合はすべてのマシンカタログに適用されます。

プライベートエンドポイントを使用する新しいディスクごとにディスクアクセスを自動的に作成するように Azure ポリシーを構成していない場合、同時操作に関する 5 つの制限は適用されません。

> 注:
>
> この機能は現時点では Connector Appliance でサポートされていません。この機能に関連した Azure の制限については、「Azure Private Link を使用してマネージドディスクに対するインポートおよびエクスポートのアクセスを制限する」を参照してください。

プロキシを有効にする　このプロキシを有効にするには、ホスト接続でカスタムプロパティを次のように設定します。

1. Remote PowerShell SDK を使用して PowerShell ウィンドウを開きます。詳しくは、https://docs.citrix.com/en-us/citrix-daas/sdk-api.html#citrix-virtual-apps-and-desktops-remote-powershell-sdk/を参照してください。
2. 次のコマンドを実行します:

```
Add-PSSnapin citrix*.
cd XDHyp:\Connections\
dir
<!--NeedCopy-->
```

3. 接続からCustomPropertiesをメモ帳にコピーし、プロパティ設定<Property xsi:type="StringProperty"Name="ProxyHypervisorTrafficThroughConnector"Value="True"/>をCustomPropertiesに追加してプロキシを有効にします。例:

```
<CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance" xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation">
<Property xsi:type="StringProperty" Name="SubscriptionId" Value="
    4991xxxx-2xxx-4xxx-8xxx-ff59a830xxxx" />
<Property xsi:type="StringProperty" Name="ManagementEndpoint"
    Value="https://management.azure.com/" />
<Property xsi:type="StringProperty" Name="AuthenticationAuthority"
     Value="https://login.microsoftonline.com/" />
<Property xsi:type="StringProperty" Name="StorageSuffix" Value="
    core.windows.net" />
<Property xsi:type="StringProperty" Name="TenantId" Value="5cxxxxx
    -9xxx-4xxx-8xxx-dffe3efdxxxx" />
<Property xsi:type="StringProperty" Name="
    ProxyHypervisorTrafficThroughConnector" Value="True" />
</CustomProperties>
<!--NeedCopy-->
```

4. PowerShell ウィンドウで、変更したカスタムプロパティに変数を割り当てます。例:

```
$customProperty = '<CustomProperties xmlns:xsi="http://www.w3.org
    /2001/XMLSchema-instance" xmlns="http://schemas.citrix.com
    /2014/xd/machinecreation">
```



```
<Property xsi:type="StringProperty" Name="SubscriptionId" Value
    ="4991xxxx-2xxx-4xxx-8xxx-ff59a830xxxx" />
<Property xsi:type="StringProperty" Name="ManagementEndpoint"
    Value="https://management.azure.com/" />
<Property xsi:type="StringProperty" Name="AuthenticationAuthority"
     Value="https://login.microsoftonline.com/" />
<Property xsi:type="StringProperty" Name="StorageSuffix" Value="
    core.windows.net" />
<Property xsi:type="StringProperty" Name="TenantId" Value="5cxxxxx
    -9xxx-4xxx-8xxx-dffe3efdxxxx" />
<Property xsi:type="StringProperty" Name="
    ProxyHypervisorTrafficThroughConnector" Value="True" />
</CustomProperties>'
<!--NeedCopy-->
```

5. `$cred = Get-Credential`を実行します。プロンプトが表示されたら、接続の資格情報を入力します。資格情報は Azure アプリケーション ID とシークレットです。
6. `Set-Item -PSPath XDHyp:\Connections\<Connection_Name> -CustomProperties $customProperty -username $cred.username -Securepassword $cred.password`を実行します。

> 重要:
>
> 「`SubscriptionId`が欠落しています」というメッセージが表示された場合は、当該のカスタムプロパティ内で、すべての二重引用符（”）をバッククォート文字とそれに続く二重引用符（‘”）に置き換えます。例:

```
<CustomProperties xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
    instance`" xmlns=`"http://schemas.citrix.com/2014/xd/
    machinecreation`">
<Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`"
    Value=`"4991xxxx-2xxx-4xxx-8xxx-ff59a830xxxx`" />
<Property xsi:type=`"StringProperty`" Name=`"ManagementEndpoint`"
    Value=`"https://management.azure.com/`" />
<Property xsi:type=`"StringProperty`" Name=`"
    AuthenticationAuthority`" Value=`"https://login.microsoftonline
    .com/`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageSuffix`" Value
    =`"core.windows.net`" />
<Property xsi:type=`"StringProperty`" Name=`"TenantId`" Value=`"5
    cxxxxx-9xxx-4xxx-8xxx-dffe3efdxxxx`" />
<Property xsi:type=`"StringProperty`" Name=`"
    ProxyHypervisorTrafficThroughConnector`" Value=`"True`" />
</CustomProperties>
<!--NeedCopy-->
```

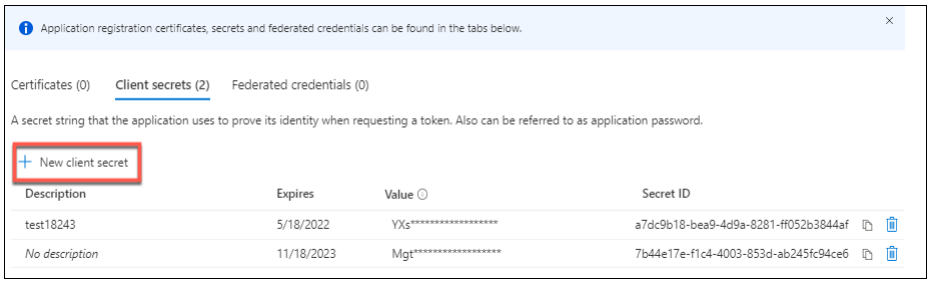
7. `dir`を実行して、更新された`CustomProperties`設定を確認します。

アプリケーションシークレットとその有効期限の管理

接続のアプリケーションシークレットは、その有効期限が切れる前に必ず変更してください。秘密キーの有効期限が切れる前に、［完全な構成］インターフェイスにアラートが表示されます。

Azure でのアプリケーションシークレットの作成　Azure Portal で、接続のアプリケーションシークレットを作成できます。

1. ［**Azure Active Directory**］を選択します。
2. Azure AD の ［**App registrations**］でアプリケーションを選択します。
3. ［**Certificates & secrets**］に移動します。
4. ［**Client secrets**］**>** ［**New client secret**］をクリックします。



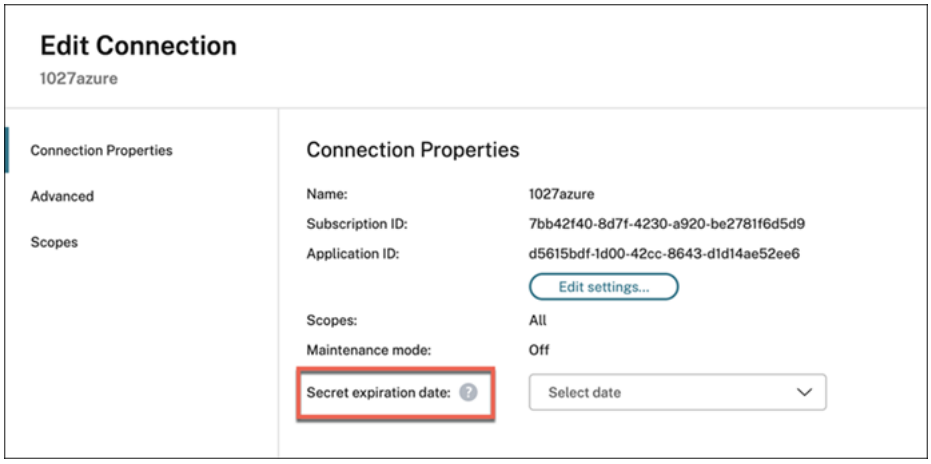
5. シークレットの説明を入力し、期間を指定します。完了したら、［追加］を選択します。

   > 注:
   >
   > クライアントシークレットは後で取得できないため、必ず保存してください。

6. クライアントシークレット値と有効期限をコピーします。
7. ［完全な構成］インターフェイスで、対応する接続を編集し、［アプリケーションシークレット］および ［シークレットの有効期限］フィールドの値を、コピーした値に置き換えます。

シークレットの有効期限の変更　［完全な構成］インターフェイスで、使用中のアプリケーションシークレットの有効期限を追加または変更できます。

1. ［接続とリソースの追加］ウィザードで接続を右クリックし、［接続の編集］をクリックします。
2. ［接続のプロパティ］ページで ［シークレットの有効期限］をクリックして、使用中のアプリケーションシークレットの有効期限を追加または変更します。



必要な **Azure** 権限

このセクションでは、Azure に必要な 最低限の権限と一般的な権限について説明します。

最低限の権限

最低限の権限により、セキュリティ制御が向上します。ただし、最低限の権限だけが付与されている場合は、追加の権限が必要な新機能が失敗します。このセクションでは、アクションごとに最低限の権限の一覧を表示します。

ホスト接続の作成　Azure から取得した情報を使用して、ホスト接続を追加します。

```
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/disks/read",
"Microsoft.Resources/providers/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Resources/tenants/read"
<!--NeedCopy-->
```

VM の電源管理　マシンインスタンスの電源をオンまたはオフにします。

```
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/start/action",
"Microsoft.Compute/virtualMachines/restart/action",
"Microsoft.Insights/diagnosticsettings/delete",
"Microsoft.Insights/diagnosticsettings/read",
"Microsoft.Insights/diagnosticsettings/write",
<!--NeedCopy-->
```


VM の作成、更新、または削除　マシンカタログを作成してから、マシンを追加、削除、更新し、マシンカタログを削除します。

以下は、マスターイメージが管理対象ディスクである場合、またはスナップショットがホスティング接続と同じリージョンにある場合に必要となる最低限の権限の一覧です。

```
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Resources/tags/read",
"Microsoft.Resources/tags/write",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/snapshots/read",
"Microsoft.Compute/snapshots/write",
"Microsoft.Compute/snapshots/delete",
"Microsoft.Compute/snapshots/beginGetAccess/action",
"Microsoft.Compute/snapshots/endGetAccess/action",
"Microsoft.Compute/disks/read",
"Microsoft.Compute/disks/write",
"Microsoft.Compute/disks/delete",
"Microsoft.Compute/disks/beginGetAccess/action",
"Microsoft.Compute/disks/endGetAccess/action",
"Microsoft.Compute/locations/publishers/artifacttypes/types/versions/
   read",
"Microsoft.Compute/skus/read",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Features/providers/features/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/locations/usages/read",
<!--NeedCopy-->
```

以下の機能の最低限の権限に基づき、以下の追加の権限が必要です:

- マスターイメージが、ホスト接続と同じリージョンにあるストレージアカウント内の VHD である場合:

  ```
  "Microsoft.Storage/storageAccounts/read",
  "Microsoft.Storage/storageAccounts/listKeys/action",
  <!--NeedCopy-->
  ```

- マスターイメージが、Azure Compute Gallery（旧称：Shared Image Gallery）の ImageVersion であ

る場合：

```
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/read",
<!--NeedCopy-->
```

- マスターイメージが管理対象ディスクかスナップショットである場合、または VHD がホスティング接続のリージョンとは異なるリージョンにある場合：

```
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/checknameavailability/read",
"Microsoft.Storage/locations/usages/read",
"Microsoft.Storage/skus/read",
<!--NeedCopy-->
```

- Citrix 管理対象リソースグループを使用する場合：

```
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
<!--NeedCopy-->
```

- 共有テナントまたはサブスクリプションでマスターイメージを、Azure Compute Gallery（旧称：Shared Image Gallery）に配置した場合：

```
"Microsoft.Compute/galleries/write",
"Microsoft.Compute/galleries/images/write",
"Microsoft.Compute/galleries/images/versions/write",
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/read",
"Microsoft.Compute/galleries/delete",
"Microsoft.Compute/galleries/images/delete",
"Microsoft.Compute/galleries/images/versions/delete",
"Microsoft.Resources/subscriptions/read",
<!--NeedCopy-->
```

- Azure 専用ホストサポートを使用する場合：

```
"Microsoft.Compute/hostGroups/read",
"Microsoft.Compute/hostGroups/write",
"Microsoft.Compute/hostGroups/hosts/read",
<!--NeedCopy-->
```

- 顧客管理キー（CMK）でサーバー側暗号化（SSE）を使用する場合：

```
"Microsoft.Compute/diskEncryptionSets/read",
<!--NeedCopy-->
```


- ARM テンプレート（マシンプロファイル）を使用して VM を展開する場合:

```
"Microsoft.Resources/deployments/write",
"Microsoft.Resources/deployments/operationstatuses/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/delete",
"Microsoft.Insights/DataCollectionRuleAssociations/Read",
"Microsoft.Insights/dataCollectionRules/read",
<!--NeedCopy-->
```

- Azure テンプレートスペックをマシンプロファイルとして使用する場合:

```
"Microsoft.Resources/templateSpecs/read",
"Microsoft.Resources/templateSpecs/versions/read",
<!--NeedCopy-->
```

非管理対象ディスクを使用するマシンの作成、更新、および削除　以下は、マスターイメージが VHD であり、管理者から提供されたリソースグループを使用する場合に必要となる最低限の権限の一覧です:

```
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/tags/read",
"Microsoft.Resources/tags/write",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/checknameavailability/read",
"Microsoft.Storage/locations/usages/read",
"Microsoft.Storage/skus/read",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/locations/usages/read",
<!--NeedCopy-->
```

Azure AD 参加デバイスの管理　Azure AD 参加デバイスの管理に必要な最小限の権限のリストは次のとおりです。


```
microsoft.directory/devices/standard/read
microsoft.directory/devices/delete
<!--NeedCopy-->
```

一般的な権限

Contributor（投稿者）の役割には、すべてのリソースを管理するための完全なアクセス権があります。この一連の権限は、新しい機能の取得を妨げるものではありません。

以下の一連の権限は、現在の機能セットで必要とされるよりも多くの権限が含まれていますが、今後の互換性の面でベストなものを提供します：

```
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/disks/beginGetAccess/action",
"Microsoft.Compute/disks/delete",
"Microsoft.Compute/disks/endGetAccess/action",
"Microsoft.Compute/disks/read",
"Microsoft.Compute/disks/write",
"Microsoft.Compute/galleries/delete",
"Microsoft.Compute/galleries/images/delete",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/delete",
"Microsoft.Compute/galleries/images/versions/read",
"Microsoft.Compute/galleries/images/versions/write",
"Microsoft.Compute/galleries/images/write",
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/write",
"Microsoft.Compute/hostGroups/hosts/read",
"Microsoft.Compute/hostGroups/read",
"Microsoft.Compute/hostGroups/write",
"Microsoft.Compute/snapshots/beginGetAccess/action",
"Microsoft.Compute/snapshots/delete",
"Microsoft.Compute/snapshots/endGetAccess/action",
"Microsoft.Compute/snapshots/read",
"Microsoft.Compute/snapshots/write",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/restart/action",
"Microsoft.Compute/virtualMachines/start/action",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/locations/publishers/artifacttypes/types/versions/
   read",
"Microsoft.Compute/skus/read",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
```



```
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/locations/usages/read",
"Microsoft.Resources/deployments/operationstatuses/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Resources/deployments/write",
"Microsoft.Resources/deployments/delete",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
"Microsoft.Resources/providers/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Resources/subscriptions/read",
"Microsoft.Resources/tags/read",
"Microsoft.Resources/tags/write",
"Microsoft.Resources/tenants/read",
"Microsoft.Resources/templateSpecs/read",
"Microsoft.Resources/templateSpecs/versions/read",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/checknameavailability/read",
"Microsoft.Storage/locations/usages/read",
"Microsoft.Storage/skus/read",
"Microsoft.Features/providers/features/read",
"Microsoft.Insights/DataCollectionRuleAssociations/Read",
"Microsoft.Insights/dataCollectionRules/read",
"Microsoft.Insights/diagnosticsettings/delete",
"Microsoft.Insights/diagnosticsettings/read",
"Microsoft.Insights/diagnosticsettings/write",
<!--NeedCopy-->
```

Azure AD の権限　Azure AD 参加マシンのカタログを作成する場合に、Azure AD 参加デバイス管理を有効にすると、MCS が Azure AD デバイスを管理します。Azure AD の組み込みのクラウド デバイス管理者役割には、現在の機能セットで必要となる以上の権限が含まれていますが、今後も最高の互換性があります。

次の手順

- 初期展開プロセスを行っている場合は、「マシンカタログの作成」を参照してください。
- Azure 固有の情報については、「Microsoft Azure カタログの作成」を参照してください。

追加情報

- 接続とリソースの作成と管理
- Microsoft Azure Resource Manager 仮想化環境

Microsoft System Center Virtual Machine Manager への接続

January 25, 2024

「接続とリソースの作成と管理」では接続を作成するためのウィザードについて説明しています。次の情報は、Microsoft System Center Virtual Machine Manager（VMM）に固有の詳細について説明しています。

> 注:
>
> VMM への接続を作成する前に、まず VMM アカウントをリソースの場所として設定する必要があります。「Microsoft System Center Virtual Machine Manager 仮想化環境」を参照してください。

接続の作成

MCS を使用して仮想マシンをプロビジョニングした場合は、接続作成ウィザードで次の操作を行います:

- アドレスにホストサーバーの完全修飾ドメイン名を入力します。
- 先ほど設定した管理者アカウントの資格情報を入力します。このアカウントには、仮想マシンを新規作成できる権限が必要です。
- [ホスト詳細] ダイアログボックスで、仮想マシンの作成時に使用するクラスターまたはスタンドアロンホストを選択します。

  > 重要
  >
  > 単一 Hyper-V ホストによる展開でも、クラスターまたはスタンドアロンホストを参照します。

次の手順

- 初期展開プロセスを行っている場合は、「マシンカタログの作成」を参照してください。
- SMB 3 ファイル共有で MCS を使用してマシンカタログを作成する方法については、「Microsoft System Center Virtual Machine Manager カタログの作成」を参照してください。

追加情報

- 接続とリソースの作成と管理
- Microsoft System Center Virtual Machine Manager 仮想化環境。

Nutanix への接続

January 25, 2024

「接続とリソースの作成と管理」では接続を作成するためのウィザードについて説明しています。以下の情報は、Nutanix に固有の詳細について説明しています。

> 注:
>
> Nutanix への接続を作成する前に、まず Nutanix アカウントをリソースの場所として設定する必要があります。「Nutanix 仮想化環境」を参照してください。

Nutanix との接続の作成

以下の情報は、「接続の作成と管理」のガイダンスを補足するものです。Nutanix 接続を作成するときは、Nutanix に固有の詳細に注意しながら、その記事の一般的なガイダンスに従ってください。

接続とリソースの追加 ウィザードの ［接続］ページで、接続の種類として ［**Nutanix**］を選択し、アドレスと資格情報、接続の名前を指定します。［ネットワーク］ページで、ホスティングユニットのネットワークを選択します。

選択できる接続の種類は次のとおりです：**Nutanix AHV**、**Nutanix AHV DRaaS**、**Nutanix AHV PC**。

- **Nutanix AHV** の場合は、Prism Element（PE）クラスターのアドレスと資格情報を指定します。
- ［**Nutanix AHV PC**］の場合は、ハイパーバイザーのアドレスと資格情報を指定します。

  > 注:
  >
  > 現在、接続の種類として **Nutanix AHV PC** を使用するのは、Nutanix Cloud Cluster（NC2）on Azure への接続を作成する場合に限られます。また、マシンカタログは、NC2 on Azure 接続内の単一のクラスターでのみホストできます。

- **Nutanix AHV DRaaS** の場合は、アドレスとユーザー名を指定してから、Nutanix DRaaS 資格情報ファイル（`.pem`）に含まれる公開キーおよび秘密キーをインポートします。（公開キーと秘密キーは、Nutanix DRaaS 管理者によって Nutanix DRaaS クラウドで生成されます。）
  - キーをインポートするには、資格情報ファイルを検索し、メモ帳（または任意のテキストエディター）でそのファイルを開き、コンテンツをコピーします。その後、［接続］ページに戻り、［キーのインポート］を選択し、コンテンツを貼り付けてから ［保存］を選択します。

注意：資格情報の内容またはその形式を変更しないでください。

> ヒント：
>
> Nutanix AHV（Prism Element）をリソースとして使用してマシンを展開する場合は、VM のディスクが存在するコンテナを選択します。

次の手順

- 初期展開プロセスを行っている場合は、「マシンカタログの作成」を参照してください。
- Nutanix 固有の情報については、「Nutanix カタログの作成」を参照してください。

追加情報

- 接続とリソースの作成と管理
- Nutanix 仮想化環境
- Nutanix クラウドおよびパートナーソリューション

Nutanix クラウドおよびパートナーソリューションへの接続

January 25, 2024

「接続とリソースの作成と管理」では接続を作成するためのウィザードについて説明しています。以下の情報は、Nutanix クラウドおよびパートナーソリューションに固有の詳細について説明しています。

Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）は、次の Nutanix クラウドおよびパートナーソリューションをサポートしています：

- Nutanix Cloud Clusters on AWS

> 注：
>
> - Nutanix クラウドおよびパートナーソリューションへの接続を作成する前に、まずそれぞれのアカウントをリソースの場所として設定する必要があります。「Nutanix クラウドおよびパートナーソリューション」を参照してください。
> - Nutanix クラウドの設定に関する最新情報については、「Nutanix Cloud Clusters on AWS Deployment and User Guide」に従ってください。

Nutanix Prism への接続

Nutanix クラスターを作成したら、Nutanix Prism に接続します。
Nutanix Prism に接続するには、次の手順を実行します：

1. 「10.0.129.0/24」サブネットに踏み台 VM を作成します。
2. 踏み台 VM に RDP（リモートデスクトッププロトコル）で接続し、前のセクションでコピーした **Prism Element** の URL に移動します。
3. デフォルトの資格情報を使用してログインします：`admin`:`nutanix`/4u。忘れずにパスワードを変更してください。

Nutanix Cluster での **VM** の作成

Nutanix Prism に接続した後、Nutanix クラスター上に VMを作成します。

VM がインターネットアクセスを必要とする場合

1. AWS コンソールに移動します。
2. Nutanix CFS によって作成されたものと同じ VPC で、新しく「10.0.130.0/24」サブネットを作成します。
3. このサブネットのルートテーブルにルートを追加して、すべての非ローカルトラフィックを上記の NAT ゲートウェイに転送します。
4. 踏み台 VM に RDP（リモートデスクトッププロトコル）で接続し、前のセクションでコピーした **Prism Element** の URL に移動して、ログインします。
5. 新しいネットワークの追加［**Settings**］**>**［**Network Configuration**］**>**［**Create Subnet**］に移動します。AWS で使用しているものと同じ「10.0.130.0/24」サブネットを使用します。
6. その新しいサブネットにすべての VM（AD、CC、VDA など）を作成します。

VM がインターネットアクセスを必要としない場合

1. 踏み台 VM に RDP（リモートデスクトッププロトコル）で接続し、前のセクションでコピーした **Prism Element** の URL に移動して、ログインします。
2. 新しいネットワークの追加［**Settings**］**>**［**Network Configuration**］**>**［**Create Subnet**］に移動します。「10.0.129.0/24」サブネットを使用します。
3. そのサブネットにすべての VM（AD、CC、VDA など）を作成します。

> ヒント：
>
> VM の時間とタイムゾーン情報が正しく設定されていることを確認してください。これは特に AD（Active Directory）に当てはまります。

ホスト接続の作成

1. ［管理］**>**［完全な構成］の左側ペインで ［ホスト］を選択します。
2. ［接続およびリソースを追加］をクリックします。
3. ［接続］画面で、［新しい接続を作成する］を選択し、［接続アドレス］に「`https://xxx.xxx.xxx.xxx:9440`」を入力します。
4. UI に従ってウィザードを完了します。

> 注:
>
> Citrix Studio で Nutanix のオプションを使用できるようにするには、Nutanix プラグインが（Nutanix ゾーンで使用されていなくても）すべてのコネクタ VM にインストールされている必要があります。

次の手順

- 初期展開プロセスを行っている場合は、「マシンカタログの作成」を参照してください。
- Nutanix 固有の情報については、「Nutanix カタログの作成」を参照してください。

追加情報

- 接続とリソースの作成と管理
- Nutanix 仮想化環境
- Nutanix クラウドおよびパートナーソリューション

VMware への接続

May 17, 2024

「接続とリソースの作成と管理」では接続を作成するためのウィザードについて説明しています。以下の情報は、VMware 仮想化環境に固有の詳細について説明しています。

> 注:
>
> VMware への接続を作成する前に、まず VMware アカウントをリソースの場所として設定する必要があります。「VMware 仮想化環境」を参照してください。

必要な権限

この記事にリストされている権限の組み合わせまたはそのすべてを使用して、VMware ユーザーアカウントおよび 1 つまたは複数の VMware の役割を作成します。役割の作成は、さまざまな Citrix DaaS 処理をいつでも要求可能に

する上で、ユーザーの権限に必要となるレベルまで細分化して行ってください。いつでもユーザー固有の権限を付与できるようにするために、データセンター以上のレベルで［**Propagate to children**］オプションを選択して、ユーザーを各役割に関連付けます。

以下の表に、Citrix DaaS の処理と最低限必要な VMware 権限の間の対応関係を示します。

接続およびリソースの追加

SDK	ユーザーインターフェイス
System.Anonymous、System.Read、および System.View	自動的に追加されます。組み込みの読み取り専用の役割を使用できます。

電源管理

SDK	ユーザーインターフェイス
VirtualMachine.Interact.PowerOff	[Virtual machine] > [Interaction] > [Power Off]
VirtualMachine.Interact.PowerOn	[Virtual machine] > [Interaction] > [Power On]
VirtualMachine.Interact.Reset	[Virtual machine] > [Interaction] > [Reset]
VirtualMachine.Interact.Suspend	[Virtual machine] > [Interaction] > [Suspend]
Datastore.Browse	[Datastore] > [Browse datastore]

マシンのプロビジョニング（**Machine Creation Services**）

MCS を使用してマシンをプロビジョニングするには、次の権限が必須です：

SDK	ユーザーインターフェイス
Datastore.AllocateSpace	[Datastore] > [Allocate space]
Datastore.Browse	[Datastore] > [Browse datastore]
Datastore.FileManagement	[Datastore] > [Low level file operations]
Network.Assign	[Network] > [Assign network]
Resource.AssignVMToPool	[Resource] > [Assign virtual machine to resource pool]

SDK	ユーザーインターフェイス
VirtualMachine.Config.AddExistingDisk	[Virtual machine] > [Configuration] > [Add existing disk]
VirtualMachine.Config.AddNewDisk	[Virtual machine] > [Configuration] > [Add new disk]
Virtual machine.Config.Add or remove device	[Virtual machine] > [Configuration] > [Add or remove device]
VirtualMachine.Config.AdvancedConfig	[Virtual machine] > [Configuration] > [Advanced]
VirtualMachine.Config.RemoveDisk	[Virtual machine] > [Configuration] > [Remove disk]
VirtualMachine.Config.CPUCount	[Virtual machine] > [Configuration] > [Change CPU count]
VirtualMachine.Config.Memory	[Virtual machine] > [Configuration] > [Change memory]
VirtualMachine.Config.Settings	[Virtual machine] > [Configuration] > [Change settings]
VirtualMachine.Interact.PowerOff	[Virtual machine] > [Interaction] > [Power Off]
VirtualMachine.Interact.PowerOn	[Virtual machine] > [Interaction] > [Power On]
VirtualMachine.Interact.Reset	[Virtual machine] > [Interaction] > [Reset]
VirtualMachine.Interact.Suspend	[Virtual machine] > [Interaction] > [Suspend]
VirtualMachine.Inventory.CreateFromExisting	[Virtual machine] > [Inventory] > [Create from existing]
VirtualMachine.Inventory.Create	[Virtual machine] > [Inventory] > [Create new]
VirtualMachine.Inventory.Delete	[Virtual machine] > [Inventory] > [Remove]
VirtualMachine.Provisioning.Clone	[Virtual machine] > [Provisioning] > [Clone virtual machine]
VirtualMachine.State.CreateSnapshot	vSphere 5.0、Update 2、vSphere 5.1、Update 1、および vSphere 6.x。Update 1：［仮想マシン］> ［状態］> ［スナップショットの作成］。vSphere 5.5：［仮想マシン］> ［スナップショット管理］> ［スナップショットの作成］。vSphere 8.0：［仮想マシン］> ［スナップショット管理］> ［スナップショットの作成］

イメージの更新とロールバック

SDK	ユーザーインターフェイス
Datastore.AllocateSpace	[Datastore] > [Allocate space]
Datastore.Browse	[Datastore] > [Browse datastore]
Datastore.FileManagement	[Datastore] > [Low level file operations]
Network.Assign	[Network] > [Assign network]
Resource.AssignVMToPool	[Resource] > [Assign virtual machine to resource pool]
VirtualMachine.Config.AddExistingDisk	[Virtual machine] > [Configuration] > [Add existing disk]
VirtualMachine.Config.AddNewDisk	[Virtual machine] > [Configuration] > [Add new disk]
VirtualMachine.Config.AdvancedConfig	[Virtual machine] > [Configuration] > [Advanced]
VirtualMachine.Config.RemoveDisk	[Virtual machine] > [Configuration] > [Remove disk]
VirtualMachine.Interact.PowerOff	[Virtual machine] > [Interaction] > [Power Off]
VirtualMachine.Interact.PowerOn	[Virtual machine] > [Interaction] > [Power On]
VirtualMachine.Interact.Reset	[Virtual machine] > [Interaction] > [Reset]
VirtualMachine.Inventory.CreateFromExisting	[Virtual machine] > [Inventory] > [Create from existing]
VirtualMachine.Inventory.Create	[Virtual machine] > [Inventory] > [Create new]
VirtualMachine.Inventory.Delete	[Virtual machine] > [Inventory] > [Remove]
VirtualMachine.Provisioning.Clone	[Virtual machine] > [Provisioning] > [Clone virtual machine]

プロビジョニングされたマシンの削除

SDK	ユーザーインターフェイス
Datastore.Browse	[Datastore] > [Browse datastore]
Datastore.FileManagement	[Datastore] > [Low level file operations]
VirtualMachine.Config.RemoveDisk	[Virtual machine] > [Configuration] > [Remove disk]
VirtualMachine.Interact.PowerOff	[Virtual machine] > [Interaction] > [Power Off]

SDK	ユーザーインターフェイス
VirtualMachine.Inventory.Delete	[Virtual machine] > [Inventory] > [Remove]

ストレージプロファイル（**vSAN**）

vSAN データストアでのカタログ作成中にストレージポリシーを表示、作成、または削除するには、次の権限が必須です：

SDK	ユーザーインターフェイス
StorageProfile.Update	PROFILE 駆動のストレージ > Profile 駆動のストレージ更新。vSphere 8 の場合：VM ストレージポリシー > Update VM storage policies
StorageProfile.View	PROFILE 駆動のストレージ > Profile 駆動のストレージ表示。vSphere 8 の場合：VM ストレージポリシー > View VM storage policies

タグとカスタム属性

タグとカスタム属性を使用すると、vSphere インベントリで作成された VM にメタデータをつなげて、これらのオブジェクトを検索およびフィルタリングしやすくすることができます。タグまたはカテゴリを作成、編集、割り当て、および削除するには、次の権限が必須です：

SDK	ユーザーインターフェイス
InventoryService.Tagging.CreateTag	vSphere のタグ付け > vSphere タグの作成
InventoryService.Tagging.CreateCategory	vSphere のタグ付け > vSphere タグカテゴリの作成
InventoryService.Tagging.EditTag	vSphere のタグ付け > vSphere タグの編集
InventoryService.Tagging.EditCategory	vSphere のタグ付け > vSphere タグカテゴリの編集
InventoryService.Tagging.DeleteTag	vSphere のタグ付け > vSphere タグの削除
InventoryService.Tagging.DeleteCategory	vSphere のタグ付け > vSphere タグカテゴリの削除
InventoryService.Tagging.AttachTag	vSphere のタグ付け > vSphere タグの割り当てまたは割り当て解除
InventoryService.Tagging.ObjectAttachable	vSphere のタグ付け > オブジェクトへの vSphere タグの割り当てまたは割り当て解除
Global.ManageCustomFields	[Global] > [Manage custom attributes]

SDK	ユーザーインターフェイス
Global.SetCustomField	[Global] > [Set custom attribute]

> 注:
>
> MCS は、マシンカタログを作成するときに、ターゲット VM に特別な名前タグを付けます。これらのタグは、マスターイメージを MCS 作成 VM と区別し、イメージの準備に MCS 作成 VM を使用できないようにします。vCenter の`XdProvisioned`属性の値で違いを識別できます。MCS で VM を作成する場合、この属性は **True** に設定されます。

暗号化操作

暗号化操作権限は、誰がどのタイプのオブジェクトに対してどの種類の暗号化操作を実行できるかを制御します。vSphere Native Key Provider は`Cryptographer.*`権限を使用します。暗号化操作には、次の最低限の権限が必要です:

> 注:
>
> これらの権限は、vTPM が組み込まれた VM で MCS マシンカタログを作成するために必要です。

SDK	ユーザーインターフェイス
Cryptographic operations.Direct Access	[Privileges] > [All Privileges] > [Cryptographic operations] > [Direct Access]
Cryptographic operations.Add disk	[Privileges] > [All Privileges] > [Cryptographic operations] > [Add disk]
Cryptographic operations.Clone	[Privileges] > [All Privileges] > [Cryptographic operations] > [Clone]
Cryptographic operations.Encrypt	[Privileges] > [All Privileges] > [Cryptographic operations] > [Encrypt]
Cryptographic operations.Encrypt new	[Privileges] > [All Privileges] > [Cryptographic operations] > [Encrypt new]
Cryptographic operations.Decrypt	[Privileges] > [All Privileges] > [Cryptographic operations] > [Decrypt]
Cryptographic operations.Migrate	[Privileges] > [All Privileges] > [Cryptographic operations] > [Clone]
Cryptographic operations.Read KMS information	[Privileges] > [All Privileges] > [Cryptographic operations] > [Read KMS information]

マシンのプロビジョニング（**Citrix Provisioning**）

Citrix Provisioning コンソールで、Citrix Virtual Apps and Desktops インストールウィザード、およびデバイスのエクスポートウィザードを使用して仮想マシンをプロビジョニングするには、テンプレートを複製および展開する権限が必要です。ホスト接続を作成するときに権限を設定します。
マシンのプロビジョニング（Machine Creation Services）のすべての権限と、以下が必要です。

SDK	ユーザーインターフェイス
VirtualMachine.Config.AddRemoveDevice	[Virtual machine] > [Configuration] > [Add or remove device]
VirtualMachine.Config.CPUCount	[Virtual machine] > [Configuration] > [Change CPU Count]
VirtualMachine.Config.Memory	[Virtual machine] > [Configuration] > [Memory]
VirtualMachine.Config.Settings	[Virtual machine] > [Configuration] > [Settings]
VirtualMachine.Provisioning.CloneTemplate	[Virtual machine] > [Provisioning] > [Clone template]
VirtualMachine.Provisioning.DeployTemplate	[Virtual machine] > [Provisioning] > [Deploy template]
vApp.Export	[vApp] > [Export]

> 注:
>
> `vApp.Export`は、マシンプロファイルを使用して MCS マシンカタログを作成するために必要です。

VMware 環境への接続の保護

vCenter への`HTTPS`/`SSL`接続を使用するには、その接続が Citrix DaaS によって信頼される必要があります。

2 つのオプションがあります:

- （推奨）Citrix DaaS データベースには SSL の拇印機能がインストールされています。SSL の拇印は、Citrix DaaS が vCenter への接続を信頼するために、各 Cloud Connector で使用されます。
- （別のオプション）各 Cloud Connector は vCenter 証明書を信頼し、Cloud Connector 上のサービスはこの信頼を再利用します。この信頼は、以下のものによって得られます:
  - 認証機関によって発行され、Windows によって信頼されている、vCenter 証明書。これにより、Windows と vCenter との間で信頼が確立されます。
  - Windows にインストールされた vCenter 証明書。これにより、Windows と vCenter.OT との間で信頼が確立されます

> 注:
>
> VMware Cloud とそのパートナーソリューションには、vCenter 証明書と VMware SSL 拇印は必要ありません。

VMware SSL の拇印機能

VMware SSL の拇印機能は、VMware vSphere ハイパーバイザーへのホスト接続を確立するときに頻繁に報告されるエラーに対処するためのものです。これまでは、接続を確立する前に、サイト内の Citrix が管理する Delivery Controller と、ハイパーバイザーの証明書間の信頼関係を管理者が手動で作成する必要がありました。VMware SSL の拇印機能により、この手作業が不要になりました。信頼性されていない証明書の拇印はサイトのデータベースに保管されるようになったため、ハイパーバイザーは、Controller から信頼されているとみなされない場合も、Citrix DaaS からは常に信頼できるとみなされます。

vSphere のホスト接続を確立する場合、接続しようとしているマシンの証明書をダイアログボックスで見ることができます。その証明書を見て、信頼するかどうかを選択できます。

VMware SSL 拇印は、PowerShell SDK「`Set-Item -LiteralPath "<FullPath_to_connection>"-username $cred.username -Securepassword $cred.password -SslThumbprint "<New ThumbPrint>"-hypervisorAddress <vcenter URL>`」を使用して後で更新できます。

> ヒント:
>
> 証明書の拇印は大文字で書く必要があります。

証明書の取得とインポート

vSphere 通信を保護するため、Citrix では HTTP ではなく HTTPS を使用することをお勧めします。HTTPS を使用するにはデジタル証明書が必要です。組織のセキュリティポリシーに従って、証明書機関により発行されるデジタル証明書を使用することを Citrix ではお勧めします。

証明機関のデジタル証明書を使用できない場合は、VMware によりインストールされる自己署名証明書を使用することもできます（組織のセキュリティポリシーで許可される場合）。VMware vCenter の証明書を各 Cloud Connector に追加します。

1. vCenter Server を実行しているコンピューターの完全修飾ドメイン名（FQDN）を、そのサーバーのホストファイル（%SystemRoot%/WINDOWS/system32/Drivers/etc/）に追加します。この手順は、vCenter Server を実行しているコンピューターの FQDN がドメイン名システムに登録されていない場合にのみ必要です。
2. 以下の 3 つの内いずれかの方法で、vCenter の証明書を入手します:

   vCenter サーバーからコピーする:

a) vCenter サーバー上の rui.crt ファイルを、Cloud Connector からアクセス可能な場所にコピーします。
b) Cloud Connector で、エクスポートした証明書の保存先に移動し、rui.crt ファイルを開きます。

Web ブラウザーで証明書をダウンロードする： Internet Explorer で証明書をダウンロードまたはインストールするには、Internet Explorer を右クリックして ［管理者として実行］を選択する必要があります。

a) Web ブラウザーを開き、vCenter サーバー（https://server1.domain1.comなど）への保護された接続を確立します。
b) セキュリティに関する警告を受け入れます。
c) 証明書のエラーが表示されるアドレスバーをクリックします。
d) ［**Certificate is not valid**］をクリックし、［詳細］タブをクリックします。
e) ［エクスポート…］をクリックします
f) エクスポートした証明書を保存します。
g) エクスポートした証明書の CER ファイルを開きます。

管理者として実行する **Internet Explorer** で直接インポートする：

a) Web ブラウザーを開き、vCenter サーバー（https://server1.domain1.comなど）への保護された接続を確立します。
b) セキュリティに関する警告を受け入れます。
c) 証明書のエラーが表示されるアドレスバーをクリックします。
d) 証明書を表示します。

3. 各 Cloud Connector 上の証明書ストアに証明書をインポートします。

a) ［証明書のインストール］をクリックして ［ローカルマシン］を選択し、［次へ］をクリックします。
b) ［証明書をすべて次のストアに配置する］を選択して、［参照］をクリックします。以降のサポート対象バージョン：［信頼されたユーザー］を選択して ［**OK**］をクリックします。［次へ］、［完了］の順にクリックします。

> 重要：
>
> インストール後に vSphere サーバーの名前を変更する場合は、サーバー上で新しい自己署名証明書を作成してから、新しい証明書をインポートする必要があります。

次の手順

- 初期展開プロセスを行っている場合は、「マシンカタログの作成」を参照してください。
- VMware 固有の情報については、「VMware カタログの作成」を参照してください。

追加情報

- 接続とリソースの作成と管理

- VMware 仮想化環境
- VMware クラウドおよびパートナーソリューション

VMware クラウドおよびパートナーソリューションへの接続

January 25, 2024

Azure VMware Solution（AVS）クラスター、Google Cloud VMware Engine、VMware cloud on AWSをセットアップしたら、接続を作成します。接続の作成については、「VMware 仮想化環境への接続」を参照してください。

次の手順

- 初期展開プロセスを行っている場合は、「マシンカタログの作成」を参照してください。
- VMware 固有の情報については、「VMware カタログの作成」を参照してください。

追加情報

- 接続とリソースの作成と管理
- VMware 仮想化環境。
- VMware クラウドおよびパートナーソリューション

XenServer への接続

April 18, 2024

ウィザードを使用して接続を作成する手順について詳しくは、「Create and manage connections and resources」を参照してください。XenServer（旧称 Citrix Hypervisor）への接続を確立する前に、まず XenServer をホストとして設定する必要があります。「リソースの種類を追加するか、Citrix Cloud で未使用のドメインをアクティブ化する」を参照してください。

XenServer への接続を作成する

XenServer への接続の作成時には、仮想マシンパワー管理者（VM パワー管理者）以上の権限を持つアカウントの資格情報を指定する必要があります。

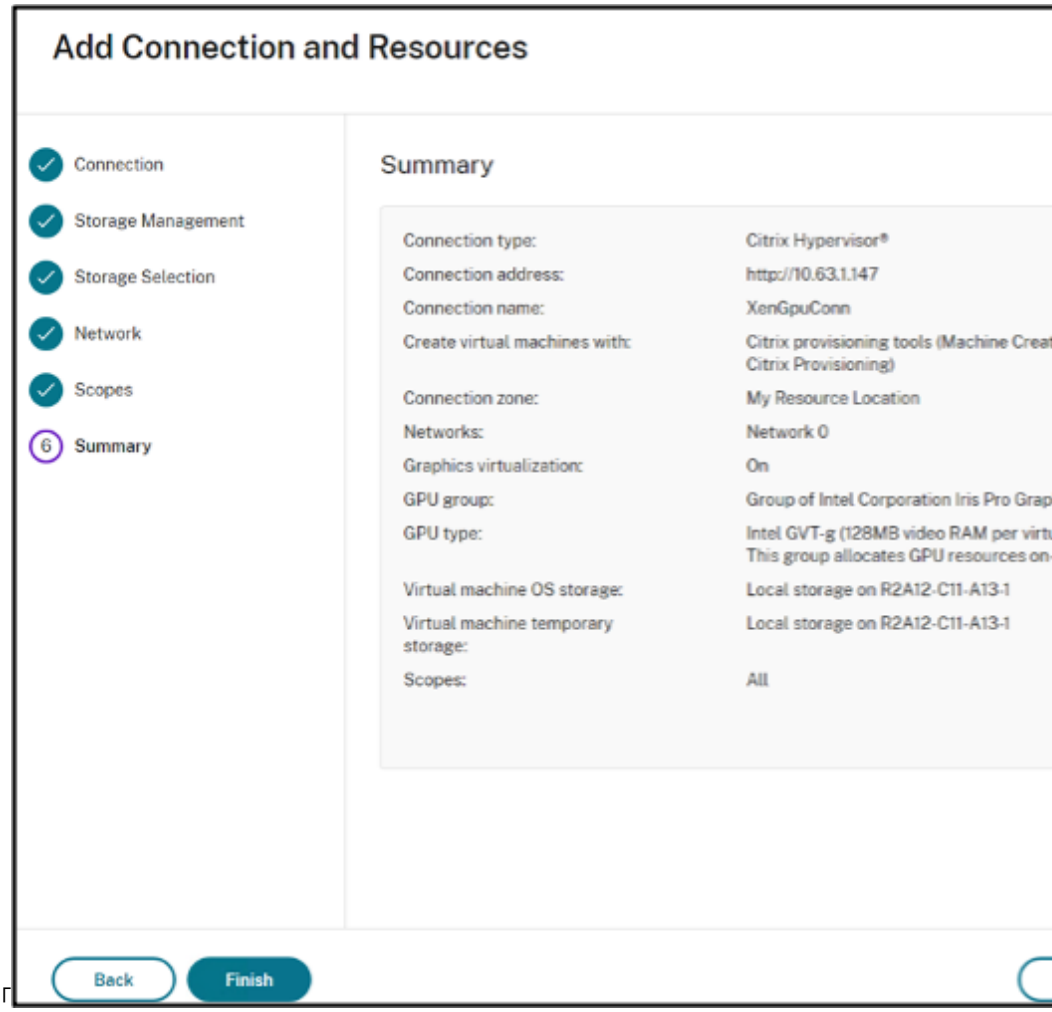
XenServer との通信を HTTPS で保護することをお勧めします。HTTPS を使用するには、XenServer にインストールされているデフォルトの TLS 証明書を置き換える必要があります。詳しくは、「TLS 証明書のサーバーへのインストール」を参照してください。

高可用性機能で使用されるハイパーバイザーを選択することもできます（XenServer サーバーの高可用性が有効な場合）。プールマスターに障害が生じても XenServer サーバーとの通信が中断されないように、（[**Edit High Availability**] から）プール内のすべてのサーバーを選択することをお勧めします。

> 注:
>
> HTTPS を使用していて、高可用性サーバーを構成する場合は、ワイルドカード証明書をプール内のすべてのサーバーにインストールしないようにしてください。サーバーごとに個別の証明書が必要です。

1 つまたは複数の XenServer ホスト上のローカルストレージを一時データストレージとして使用する場合は、プール内の各ストレージの場所に一意の名前が付いていることを確認してください。（XenCenter で名前を変更するには、ストレージを右クリックして名前のプロパティを編集します。）

vGPU をサポートする XenServer に接続する場合は、接続を作成するウィザードの [概要] ページで GPU グループと GPU タイプを確認します。



XenServer 接続作成に関する「

ページ

XenServer 接続での IntelliCache の使用

IntelliCache を使用すると、共有ストレージとローカルストレージを組み合わせて使用できるようになり、VDI 展開のコスト効率が向上します。これによってパフォーマンスが向上し、ネットワークトラフィックが減少します。この機能では、共有ストレージ上のマスターイメージがローカルストレージにキャッシュされ、共有ストレージでのデータ読み取りが減少します。共有デスクトップの場合、差分ディスクへの書き込みはホスト上のローカルストレージに書き込まれ、共有ストレージには書き込まれません。

重要な考慮事項は次のとおりです:

- IntelliCache を使用する場合、共有ストレージは NFS である必要があります。
- パフォーマンスを向上させるため、高パフォーマンスのローカルストレージデバイスを使用することをお勧めします。

IntelliCache を使用するには、以下の手順で IntelliCache を有効にします:

- XenServer をインストールするときに、［シンプロビジョニングの有効化］を選択します。ローカルメディアから XenServer ホストをインストールする方法については、「XenServer ホストのインストール」を参照してください。IntelliCache が有効なサーバーと無効なサーバーを同一プールで混在させることはサポートされません。
- Citrix DaaS では、IntelliCache はデフォルトで無効になっています。この機能は XenServer 接続の作成時にのみ有効にできます。IntelliCache を後で無効にすることはできません。XenServer 接続を作成するには:
  - ストレージの種類として、［共有］を選択します。
  - ［**IntelliCache** を使用して共有ストレージデバイス上の負荷を軽減させる］チェックボックスをオンにします。

詳しくは、「IntelliCache」を参照してください。

必要な XenServer の権限

XenServer の権限は役割ベース（RBAC）です。XenServer の役割ベースのアクセス制御（RBAC：Role Based Access Control）機能では、特定のユーザー（つまり XenServer 管理者）に役割を割り当てて、XenServer へのアクセスや実行可能な管理タスクを制御できます。この機能では、ユーザー（またはグループ）が XenServer の管理タスクの定義済みセットである「役割」にマップされ、この役割に基づいて、特定の管理タスクを実行するために必要な XenServer ホストへのアクセス許可が決定されます。

詳しくは、「役割ベースのアクセス制御」を参照してください。

役割の階層は、権限が増加していく順に、読み取り専用 → VM オペレーター → VM 管理者 → VM パワー管理者 → プールオペレーター → プール管理者です。

次のセクションでは、各プロビジョニングタスクに必要な最小限の役割についてまとめます。

ホスト接続の作成

タスク	最低限必要な役割
XenServer から取得した情報を使用して、ホスト接続を追加する	読み取り専用
ユーザーと割り当てられた役割を表示する	読み取り専用

VM の電源管理

タスク	最低限必要な役割
VM の電源オン/オフ	VM オペレーター

VM の作成、更新、または削除

タスク	最低限必要な役割
既存のスナップショットスケジュールに対して VM を追加または削除する	VM パワー管理者
スナップショットスケジュールを追加、変更、削除する	プールオペレーター
マスターイメージを公開する	プールオペレーター（スイッチポートのロックが必要）
マシンカタログの作成	プールオペレーター：スイッチポートのロックが必要
VM を追加または削除する（GPU を有効にした VM は除く）	VM 管理者
VM を追加または削除する（GPU を有効にした VM）	プールオペレーター
仮想ディスクまたは CD デバイスを追加、削除、または構成する	VM 管理者
タグの管理	VM オペレーター

RBAC の役割について詳しくは、「RBAC の役割とアクセス権」を参照してください。

スイッチ ポートロックについて詳しくは、「スイッチポートロックの使用」を参照してください。

次の手順

- 初期展開プロセスを行っている場合は、「マシンカタログの作成」を参照してください。

- XenServer 固有の情報については、「XenServer カタログの作成」を参照してください。

追加情報

- 接続とリソースの作成と管理
- XenServer 仮想化環境

マシンカタログの作成

June 13, 2024

> 注:
>
> この記事では、完全な構成インターフェイスを使用してカタログを作成する方法について説明します。クイック展開を使用して Azure リソースを作成している場合は、「［クイック展開］を使用したカタログの作成」のガイダンスに従ってください。

物理マシンまたは仮想マシンのグループは、「マシンカタログ」と呼ばれる単一のエンティティとして管理されます。1 つのマシンカタログ内では、すべてのマシンが同じオペレーティングシステムの種類を共用します。種類としては、Windows または Linux ベースのシステムなど、マルチセッション OS またはシングルセッション OS のいずれかになります。

［管理］**>**［完全な構成］インターフェイスは、最初のマシンカタログを作成するためのガイドです。最初のカタログを作成した後、最初のデリバリーグループを作成します。作成したカタログを後で変更したり、追加のカタログを作成したりすることができます。

概要

仮想マシンのカタログの作成時には、それらの仮想マシンのプロビジョニング方法を指定します。Machine Creation Services（MCS）を使用できます。または、独自のツールを使用してマシンをプロビジョニングすることもできます。

- MCS を使用して仮想マシンをプロビジョニングする場合、カタログ内に同じ仮想マシンを作成するためのイメージ（またはスナップショット）を提供します。カタログを作成する前にまず、選択したハイパーバイザーまたはクラウドサービスへのホスト接続を設定し、マシンにマスターイメージを作成して構成する必要があります。マスターイメージを構成するために、場合によって必要となるタスクとしては、ドメインへの参加、必要なドライバーや公開するアプリケーションのインストール、イメージへの Virtual Delivery Agent（VDA）の展開などがあります。

- マスターイメージを作成した後、［管理］**>**［完全な構成］インターフェイスでマシンカタログを作成します。そのイメージ（またはイメージのスナップショット）を選択し、カタログで作成する仮想マシンの数を指定して、追加情報を構成します。
- マシンが既に提供されている場合でも、VM をカタログにインポートするには、マシンカタログを 1 つ以上作成する必要があります。

MCS を使用して最初のカタログを作成する場合は、以前に作成したホスティングユニットを指定します。ホスティングユニットは、仮想マシンを作成するためのリソース構成を提供します。後で（最初のマシンカタログおよびデリバリーグループを作成した後に）、そのホスティングユニットやその親ホスト接続に関する情報を変更したり、接続やホスティングユニットを追加で作成したりすることができます。

Cloud Connector が正常に動作していない場合、MCS プロビジョニング操作（カタログ更新など）は通常よりも時間がかかり、管理インターフェイスのパフォーマンスが大幅に低下します。

RDS ライセンスチェック

Windows マルチセッション OS マシンを含むマシンカタログの作成には、有効な Microsoft RDS ライセンスの自動チェックが含まれます。電源が投入され登録されたマシンのカタログが検出され、このチェックが実行されます。

- 電源が投入され登録されたマシンが見つからない場合は、RDS ライセンスチェックが実行できないことを示す警告が表示されます。
- マシンは見つかったがエラーが検出された場合は、検出された問題を含むカタログの警告メッセージが ［管理］**>**［完全な構成］画面に表示されます。カタログから RDS ライセンス警告を削除する（画面に表示されないようにする）には、カタログを選択して、［**RDS** ライセンスの警告を削除］を選択します。確認のメッセージが表示されたら、操作を確定します。

VDA 登録

仲介セッションを起動する場合、検討対象の Cloud Connector に VDA が登録されている必要があります。VDA が登録されていないと、登録されていれば使用されるはずの資源が使用されない場合があります。VDA が登録されない理由はさまざまですが、その多くはトラブルシューティングできるものです。カタログ作成ウィザードでは、カタログをデリバリーグループに登録した後に、トラブルシューティング情報が表示されます。

カタログ作成ウィザードで、既存のマシンを追加すると、コンピューターアカウント名の一覧に、各マシンがカタログに追加するのに適しているかどうかが示されます。各マシンの横にあるアイコンにマウスを合わせると、そのマシンに関する情報メッセージが表示されます。

メッセージで問題のあるマシンが示された場合は、該当のマシンを（［削除］ボタンを使って）削除することも、そのマシンを追加することもできます。たとえば、（登録されたことがないなどの理由により）マシンに関する情報を取得できないことを示すメッセージが表示された場合は、そのマシンを追加する可能性があります。

VDA 登録のトラブルシューティングについて詳しくは、CTX136668を参照してください。

MCS カタログ作成の概要

以下は、カタログの作成ウィザードに情報を入力した後のデフォルトの MCS 操作の簡単な概要です。

- （スナップショットではなく）イメージを選択した場合、MCS によりスナップショットが作成されます。
- MCS でスナップショットの完全コピーが作成され、ホスト接続で定義されたストレージの各場所に格納されます。
- MCS によってマシンが Active Directory に追加され、そこで一意の識別子が作成されます。
- ウィザードで指定した数の仮想マシンが MCS によって作成され、各仮想マシンに対して 2 つのディスクが定義されます。1 つの VM につき、2 つのディスクに加えて、スナップショットまたはマスターイメージの完全なコピーも、ディスクと同じストレージの場所に保存されます。ストレージの場所が複数定義されている場合、それぞれの場所に以下の種類のディスクが割り当てられます。
  - スナップショットの完全コピー（前述の説明を参照）。読み取り専用であり、作成した仮想マシン間で共有されます。
  - 各仮想マシンに一意の識別子を与える、一意の ID ディスク（16MB）。各仮想マシンに対し、1 つの ID ディスクが割り当てられます。
  - 仮想マシンへの書き込みを保存する、一意の差分ディスク。このディスクは（ホストストレージでサポートされている場合）シンプロビジョニングされ、必要に応じてマスターイメージの最大サイズまで拡大します。各 VM は差分ディスクを取得します。差分ディスクには、セッション中に加えられた変更が保存されます。専用デスクトップの場合、この変更は無期限に保存されます。プールされたデスクトップの場合、再起動のたびにこの変更は削除され、新しい変更が作成されます。

または、仮想マシンを作成して静的デスクトップを配信する場合、（カタログの作成ウィザードの ［マシン］ページで）シックな（完全なコピーの）仮想マシンのクローンを指定できます。完全なクローンでは、すべてのデータストアにマスターイメージを保持する必要はありません。各仮想マシンに独自のファイルが存在します。

Machine Creation Services のストレージの考慮事項

Machine Creation Services（MCS）のストレージソリューション、構成、容量を決定する際には、多くの要因があります。以下に、適切なストレージ容量を決定するための考慮事項を示します:

容量に関する考慮事項:

- ディスク

  ほとんどの MCS 環境において、デルタ（差分）ディスクが各 VM の容量を一番多く占めます。MCS により作成される仮想マシンには、作成時にディスクが 2 つ以上割り当てられます。

  - ディスク 0（= 差分ディスク）: OS がマスターイメージ基本ディスクからコピーされて、格納されます。
  - ディスク 1 = ID ディスク: 16MB - 各仮想マシンの Active Directory データが含まれます。

  製品の進化にともない、特定のユースケースや機能の消費容量に合わせたディスクの追加が必要になることがあります。例:

  - MCS ストレージ最適化では、仮想マシンごとに書き込みキャッシュ形式のディスクが作成されます。
  - 前述のデルタディスクの使用例とは対照的に、MCS には、完全なクローンを使用する機能が追加されています。

  Hypervisor の機能も、こうした要因になることがあります。例:

  - XenServer IntelliCacheは、各 XenServer のローカルストレージ上に読み取りディスクを作成します。このオプションはイメージに対する IOPS を保存します。このイメージは、共有ストレージの場所に保存することもできます。

- ハイパーバイザーのオーバーヘッド

  ハイパーバイザーごとに固有のファイルを使用するため、このファイルが仮想マシンのオーバーヘッドとなります。ハイパーバイザーは、管理操作および一般的なログ記録でストレージを使用します。容量は、以下のオーバーヘッドを考慮して計算してください:

  - ログファイル
  - ハイパーバイザー固有のファイル。例:
    * VMware により、**VM storage** フォルダーにファイルが追加されます。VMware のベストプラクティスを参照してください。
    * 仮想マシン全体で必要なサイズを計算してください。たとえば、仮想ディスクに 20GB、スワップファイルに 16GB、ログファイルに 100MB を使用している仮想マシンでは、合計で 36.1GB を消費することを考慮に入れます。
  - XenServer のスナップショットおよびVMware のスナップショット。

- プロセスのオーバーヘッド

  カタログの作成と更新、およびマシンの追加を行なうと、それぞれ以下のようにストレージに影響が及びます。例:

  - カタログを初めて作成する場合、各ストレージの場所に基本ディスクをコピーする必要があります。
    * また、一時的に準備用の仮想マシンを作成する必要もあります。
  - カタログにマシンを追加する場合は、各ストレージの場所に基本ディスクをコピーする必要はありません。ただし、カタログの作成方法は、選択した機能によって異なります。
  - カタログを更新して、ストレージの場所ごとに基本ディスクを追加で作成します。また、カタログに含まれる仮想マシンに一定期間にわたって 2 つの差分ディスクが割り当てられるため、一時的にストレージ占有量が急増することになります。

そのほかの考慮事項:

- **RAM** のサイズ設定: I/O 最適化ディスク、書き込みキャッシュ、スナップショットファイルなど、特定のハイパーバイザーファイルとディスクのサイズに影響します。
- シン/シックプロビジョニング: シンプロビジョニング機能を備えているため、NFS ストレージが推奨されます。

Machine Creation Services（**MCS**）ストレージ最適化

Machine Creation Services（MCS）ストレージ最適化機能は、MCS I/O とも呼ばれます。この機能は、Azure、GCP、XenServer、VMware、SCVMM でのみ使用できます。

- 書き込みキャッシュコンテナは、Citrix Provisioning と同様にファイルベースです。たとえば、Citrix Provisioning の書き込みキャッシュのファイル名は「`D:\vdiskdif.vhdx`」、MCS I/O 書き込みキャッシュのファイル名は「`D:\mcsdif.vhdx`」です。
- 書き込みキャッシュディスクへの Windows クラッシュダンプファイルの書き込みをサポートするなどの方法によって、診断機能が向上します。
- MCS I/O は、引き続きハードディスクへのオーバーフローありで *RAM* にキャッシュするテクノロジを利用して、複数層の書き込みキャッシュに関して最適なソリューションを提供します。この機能により、管理者は各層のコスト、RAM とディスク、パフォーマンスのバランスを取りながら、必要なワークロードに対応できます。

書き込みキャッシュの方法をディスクベースからファイルベースに更新するには、以下の変更が必要です：

1. MCS I/O では、RAM のみのキャッシュはサポートされなくなります。マシンカタログの作成中にディスクサイズを指定します。
2. 仮想マシンの初回起動時に、書き込みキャッシュディスクが自動的に作成およびフォーマットされます。仮想マシンが起動すると、書き込みキャッシュファイル`mcsdif.vhdx`はフォーマット済みボリューム`MCSWCDisk`に書き込まれます。
3. ページファイルは、このフォーマットされたボリュームの`MCSWCDisk`にリダイレクトされます。その結果、このディスクサイズはディスクスペースの合計を考慮します。これには、ディスクサイズと生成されたワークロードの差分、およびページファイルサイズが含まれます。これは通常、VM RAM サイズに関連しています。

MCS ストレージ最適化の更新を有効にする　MCS I/O ストレージ最適化機能を有効にするには、Delivery Controller と VDA を最新バージョンの Citrix DaaS にアップグレードします。

> 注：
>
> MCS I/O が有効化された既存の環境をアップグレードする場合、追加の構成は必要ありません。VDA および Delivery Controller アップグレードにより、MCS I/O アップグレードが処理されます。

ライトバックキャッシュディスクへの特定のドライブ文字の割り当てについては、「MCS I/O ライトバックキャッシュディスクへの特定のドライブ文字の割り当て」を参照してください。

ハイパーバイザーまたはクラウドサービスでのマスターイメージの準備

マスターイメージには、オペレーティングシステム、仮想化しないアプリケーション、VDA、およびそのほかのソフトウェアをインストールしておきます。

ヒント：

- マスターイメージは、「クローンイメージ」、「ゴールデンイメージ」、「ベース仮想マシン」、または「基本イメージ」と呼ばれることがあります。ホストベンダーとクラウドサービスプロバイダーで、異なる用語を使用する場合もあります。
- ハイパーバイザーまたはクラウドサービスに、作成されたマシン数に対応する十分なプロセッサ、メモリ、ストレージがあることを確認してください。
- デスクトップとアプリケーションで必要な適切な量のハードディスク領域を構成します。この値は、後で、またはマシンカタログ内で変更することはできません。
- リモート PC アクセスのマシンカタログでは、マスターイメージを使用しません。
- MCS 使用時の Microsoft KMS ライセンス認証に関する注意事項：VDA 7.x を XenServer 6.1、XenServer 6.2、vSphere、または Microsoft System Center Virtual Machine Manager ホストで使用している場合、Microsoft Windows や Microsoft Office のライセンスを手動でリセットする必要はありません。

マスターイメージに以下のソフトウェアをインストールして構成します：

- ハイパーバイザー用の統合ツール（Citrix VM Tools、Hyper-V 統合サービス、VMware Tools など）。この手順を省略すると、アプリケーションやデスクトップが正しく動作しなくなる場合があります。
- VDA。最新の機能を利用できるように、VDA の最新バージョンをインストールすることをお勧めします。マスターイメージに VDA をインストールできないと、カタログ作成が失敗します。
- アンチウイルスプログラムや電子ソフトウェア配信エージェントなどのサードパーティツール（必要に応じて）。ユーザーやマシンの種類に適した設定で、サービス（更新機能など）を構成します。
- 仮想化せずにユーザーに提供するサードパーティのアプリケーション。ただし、可能な場合はアプリケーションを仮想化することを Citrix ではお勧めします。仮想化することで、アプリケーションを追加したり再構成したりするたびにマスターイメージを更新する必要がなくなり、コストが削減されます。また、各デスクトップにインストールするアプリケーションが少なくなるため、マスターイメージのハードディスクのサイズを減らしてストレージコストを節約できます。
- App-V アプリケーションを公開する場合は、推奨設定の App-V クライアント。App-V Client は、Microsoft 社から提供されます。
- MCS で作成したマシンカタログで、ローカライズされた Microsoft Windows を配信する場合は、マスターイメージに言語パックをインストールして言語オプション（システムロケールや表示言語など）を設定しておく必要があります。これにより、プロビジョニング時にスナップショットが作成されると、その言語パックおよび言語オプションが仮想マシンで使用されます。

> 重要：
>
> MCS を使用する場合は、マスターイメージ上で Microsoft System Preparation Utility（Sysprep）を実行しないでください。

マスターイメージを準備するには

1. ハイパーバイザーの管理ツールを使用して、マスターイメージを作成してから、オペレーティングシステムと、すべてのサービスパックおよび更新プログラムをインストールします。仮想 CPU の数を指定します。また、PowerShell を使用してマシンカタログを作成する場合、仮想 CPU の値を指定することもできます。[管理]

> ［完全な構成］でカタログを作成する場合には、仮想 CPU の数は指定できません。デスクトップとアプリケーションで必要な量のハードディスク領域を構成します。この値は、後で、またはカタログ内で変更することはできません。

2. ハードディスクはデバイスの場所「0」で接続されている必要があります。多くの標準マスターイメージテンプレートでは、デフォルトでこの場所にハードディスクが構成されますが、カスタムテンプレートを使用する場合は注意してください。
3. マスターイメージに前述のソフトウェアをインストールして構成します。
4. MCS を使用していない場合、マスターイメージはアプリケーションとデスクトップがメンバーとなっているドメインに統合します。マスターイメージが、仮想マシンを作成するホスト上で使用できることを確認してください。MCS を使用している場合、ドメインへのマスターイメージの統合は必要ありません。プロビジョニングされたマシンは、カタログの作成ウィザードで指定されたドメインに統合されます。
5. マスターイメージのスナップショットを作成して、わかりやすい名前を付けておくことを Citrix ではお勧めします。カタログの作成時にスナップショットの代わりにマスターイメージを指定すると、管理インターフェイスでスナップショットが作成されますが、そのスナップショットにわかりやすい名前を付けることはできません。

ボリュームライセンス認証

MCS は、Windows オペレーティングシステムと Microsoft Office のライセンス認証を自動化および管理するためのボリュームライセンス認証をサポートしています。MCS でサポートされるボリュームライセンス認証モデルは、次の 3 種類です:

- キー管理サービス（KMS）
- Active Directory によるライセンス認証（ADBA）
- マルチライセンス認証キー（MAK）

マシンカタログを作成した後にライセンス認証の設定を変更できます。

キー管理サービス（**KMS**）

KMS は、専用システムを必要としない軽量のサービスであり、他のサービスを提供するシステムで簡単に共同ホストできます。この機能は、Citrix がサポートするすべての Windows バージョンでサポートされています。イメージの準備中に、MCS は Microsoft Windows と Microsoft Office の KMS リセットを行います。コマンド`Set-Provserviceconfigurationdata`を実行すると、リセットをスキップできます。イメージ準備中の Microsoft Windows KMS リセットおよび Microsoft Office KMS リセットについて詳しくは、「Machine Creation Services: Image Preparation Overview and Fault-Finding」を参照してください。KMS のアクティブ化について詳しくは、「Activate using Key Management Service」を参照してください。

> 注:
>
> コマンド`Set-Provserviceconfigurationdata`の実行後に作成されたすべてのマシンカタログ

> は、コマンドで指定されたものと同じ設定になります。

Active Directory によるライセンス認証（**ADBA**）

ADBA を使用すると、ドメイン接続を介してマシンをアクティブ化できます。マシンは、ドメインに参加するとすぐにアクティブになります。これらのマシンは、ドメインに参加し、ドメインに接続している限り、アクティブのままです。この機能は、Citrix がサポートするすべての Windows バージョンでサポートされています（Windows Server 2022 を除く）。Active Directory によるライセンス認証について詳しくは、「Active Directory によるライセンス認証」を参照してください。

マルチライセンス認証キー（**MAK**）

MAK はボリュームをアクティブ化する方法の 1 つで、Microsoft サーバーの助けを借りて Windows システムを認証します。一定数のアクティベーションカウントが割り当てられている MAK キーを Microsoft から購入する必要があります。Windows システムがアクティブ化されるたびに、アクティベーションカウントが減少します。システムをアクティブ化するには、次の 2 つの方法があります：

- オンラインアクティベーション：アクティブ化する Windows システムがインターネットにアクセスできる場合、システムはプロダクトキーのインストール時に Windows を自動的にアクティブ化します。このプロセスにより、対応する MAK のアクティベーションカウントが 1 減ります。
- オフラインアクティベーション：Windows システムがインターネットに接続してオンラインアクティベーションを実行できない場合、MCS は Microsoft サーバーから確認 ID とインストール ID を取得して、Windows システムをアクティブ化します。このアクティベーション方法は、非永続的なマシンカタログに役立ちます。

> 注：
>
> - MCS は MAK を使用した Microsoft Office のアクティベーションをサポートしていません。
> - 必要な VDA の最小バージョンは 2303 です。

主な要件

- Delivery Controller にはインターネットアクセスが必要です。
- 更新される新しいイメージの MAK キーが元のイメージと異なる場合は、新しいカタログを作成します。
- マスターイメージ上に MAK キーをインストールします。Windows システムに MAK キーをインストールする手順については、「Deploy MAK Activation」を参照してください。
- イメージの準備を使用しない場合：
  1. `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation`の下に DWORD レジストリ値`Manual`を追加します。
  2. 値を`1`に設定します。

ライセンス認証数　MAK キーの残りのライセンス認証の数を表示したり、VM が 2 つ以上のライセンス認証を使用しているかどうかを確認するには、Volume Activation Management Tool（VAMT）を使用します。「VAMT のインストール」を参照してください。

MAK を使用して **Windows** システムをアクティブ化する　MAK を使用して Windows システムをアクティブ化するには:

1. マスターイメージにプロダクトキーをインストールします。この手順では、1 つのアクティベーションカウントが消費されます。
2. MCS マシンカタログを作成します。
3. イメージの準備を使用していない場合:

   a) `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation`の下に DWORD レジストリ値`Manual`を追加します。
   b) 値を`1`に設定します。

   この方法では、オンラインアクティベーションのオプションが無効になります。
4. VM をマシンカタログに追加します。
5. VM の電源をオンにします。
6. オンラインアクティベーションかオフラインアクティベーションかに応じて、Windows システムがアクティブ化されます。

   - アクティベーションがオンラインの場合、プロダクトキーのインストール後に Windows システムがアクティブ化されます。
   - アクティベーションがオフラインの場合、MCS はプロビジョニングされた VM と通信して、Windows システムのアクティベーションステータスを取得します。次に、MCS は確認 ID とインストール ID を Microsoft サーバーから取得します。これらの ID は、Windows システムをアクティブ化するために使用されます。

トラブルシューティング　プロビジョニングした VM がインストールした MAK キーでライセンス認証されない場合は、PowerShell ウィンドウで`Get-ProvVM`または`Get-ProvScheme`コマンドを実行します。

- コマンド`Get-ProvScheme`: 最新のマスターイメージから MCS マシンカタログに関連付けられたパラメータ`WindowsActivationType`を参照します。
- コマンド`Get-ProvVM`:パラメータ`WindowsActivationType`、`WindowsActivationStatus`、`WindowsActivationStatusErrorCode`、および`WindowsActivationStatusError`を参照してください。

エラーを確認し、問題解決の手順を確認できます。

完全な構成インターフェイスを使用してマシンカタログを作成する

カタログを作成する前に:

- マシンをホストするハイパーバイザーやクラウドサービスなどのリソースに対して、接続を作成していることを確認してください。
- マシンをプロビジョニングするためのマスターイメージを作成している場合。そのマスターイメージに VDA がインストールされていることを確認してください。

> 注:
>
> 仮想マシンをホストするのにクラウドサービスやハイパーバイザーを使用している場合、カタログ作成ウィザードでホスト固有の追加ページが表示されることがあります。たとえば、Azure Resource Manager マスターイメージを使用する場合、カタログ作成ウィザードには ［ストレージとライセンスの種類］ページが含まれます。ホスト固有の情報については、「次のステップ」のリンク先に説明されている各記事を参照してください。

カタログ作成ウィザードの起動

1. Citrix Cloudにサインインします。左上のメニューで、［マイサービス］**>** ［**DaaS**］を選択します。
2. ［管理］を選択します。
3. 初めてカタログを作成する場合には、適切な選択を行うためのガイドが表示されます（「マシンをセットアップし、マシンカタログを作成して、アプリとデスクトップを実行します」など）。カタログ作成ウィザードが開きます。
4. すでにカタログを作成済みで、別のカタログを作成したい場合は、次の手順に従います:
   a) ［管理］**>** ［完全な構成］の左側ペインで ［マシンカタログ］を選択します。
   b) フォルダーを使用してカタログを整理するには、デフォルトのマシンカタログフォルダーの下にフォルダーを作成します。詳しくは、「カタログフォルダーの作成」を参照してください。
   c) カタログを作成するフォルダーを選択し、［マシンカタログの作成］をクリックします。カタログ作成ウィザードが開きます。

ウィザードの指示に従って、以下のセクションで説明されているページの操作を行います。表示されるページは、選択内容と使用する（ホストへの）接続によって異なります。［ホスト/仮想化リソース］ には、サポートされているホストタイプの情報ソースが一覧表示されます。

マシンの種類の選択

カタログごとに含めることができるマシンは、同じ（種類の）OS を使用しているマシンに限ります。［マシンの種類］ページで次のいずれかを選択します:

- マルチセッション **OS**：マルチセッション OS カタログは、ホストされた共有デスクトップを提供します。マシンではサポートされているバージョンの Windows または Linux オペレーティングシステムを実行できますが、カタログに Windows と Linux オペレーティングシステムの両方を含めることはできません。
- シングルセッション **OS**：シングルセッション OS カタログでは、さまざまなユーザーに割り当てることができる VDI デスクトップが提供されます。
- リモート **PC** アクセス：リモート PC アクセスのカタログでは、オフィスにあるユーザーの物理デスクトップマシンへのリモートアクセスが提供されます。リモート PC アクセスでは、セキュリティを保護するための VPN が不要です。

マシン管理オプションの選択

> 注：
>
> ［マシンの種類］ページで ［リモート **PC** アクセス］を選択した場合、［マシン管理］ページは表示されません。

［マシン管理］ページには、マシンの管理方法と、マシンの展開に使用できるツールが表示されます。

完全な構成インターフェイスでマシンの電源を管理できる方法を指定するために、以下のオプションのいずれかを選択します。

- 電源管理されているマシン（仮想マシン、ブレード **PC** など）：このオプションは、ハイパーバイザーやクラウドサービスへの接続が構成済みの場合にのみ使用可能です。
- 電源管理されていないマシン（物理マシンなど）

［電源管理されているマシン（仮想マシン、ブレード **PC** など）］オプションを選択した場合は、VM を作成できる以下のツールを選択します：

- **Citrix MCS**（**Machine Creation Services**）：マスターイメージを使用して仮想マシンを作成および管理します。クラウド環境内のマシンカタログでは MCS が使用されます。MCS は物理マシンでは使用できません。
- ほかのサービスまたはテクノロジ：データセンター内の既存のマシンを管理するための、上記以外のツール。この場合、Microsoft System Center Configuration Manager またはほかのサードパーティアプリケーションを使用してカタログ内のマシン構成の一貫性を保つことを Citrix ではお勧めします。

> 注：
>
> Linux OS マシンについては、「Machine Creation Services（MCS）を使用した Linux VDA の作成」を参照してください。

デスクトップエクスペリエンスの選択

> 注：
>
> ［デスクトップエクスペリエンス］ページに表示されるオプションは、［マシンの種類］ページで選択したマシンの種類に応じて異なります。

- マルチセッション **OS** マシンの場合、ユーザーには、ログインするたびにランダム（な）デスクトップが割り当てられます。［デスクトップエクスペリエンス］ページには次のオプションがあります：
  - ［Persistent］：仮想デスクトップをホストしているマシンのローカルディスクに変更を保存します
  - ［Non-persistent］：ユーザーがログオフすると、すべての変更を破棄し、仮想デスクトップをクリアします

  > 注：
  >
  > 永続的なマルチセッションマシンの場合、ユーザーがデスクトップに加えた変更は保存され、すべての承認されたユーザーがアクセスできます。

- シングルセッション OS マシンの場合、［デスクトップエクスペリエンス］ページには次のオプションが表示されます：
  - ［ユーザーがログインするたびに新しい（ランダムな）デスクトップに接続します］。
  - ［ユーザーがログインするたびに同じ（静的な）デスクトップに接続します］。

  さらに、ユーザーが行った変更をログオフ後に保存するか破棄するかを決定できます。

イメージの選択

> 注：
>
> - このページが表示されるのは、［マシン管理］ページで［**Citrix Machine Creation Services (MCS)**］を選択した場合に限ります。
> - このページで選択可能なオプションは、ハイパーバイザーまたはクラウドサービスによって異なります。

このページの設定を完了するには、次の手順に従います：

1. マシンカタログのイメージの種類を選択し、イメージを選択します。次の 2 種類のイメージを使用できます：
   - マスターイメージ：マスターイメージとして作成されたスナップショットまたは VM。カタログ作成の開始時に自動的にイメージが準備されます。必要に応じて、選択したイメージにメモを追加できます。

     > 注：
     >
     > - MCS を使用する場合は、マスターイメージ上で Microsoft System Preparation Utility（Sysprep）を実行しないでください。
     > - スナップショットの代わりにマスターイメージを指定すると、管理インターフェイスでスナップショットが作成されますが、そのスナップショットにわかりやすい名前を付けることはできません。
     > - ウィザードで過去に選択したマシン管理テクノロジとの互換性がないスナップショットまたは仮想マシンを選択すると、エラーメッセージが表示されます。
     > - 画像ノード内の画像を更新するには、ツリー内で画像を選択し、右上隅にある ［更新］オプションをクリックします。画像ノードを選択せずに ［更新］をクリックすると、ツリー内の

> すべての画像が更新されます。ツリー内で選択したノードをクリアするには、**Ctrl** キーを押しながらノードをクリックします。

- 準備されたイメージ：イメージの準備が完了し、VM の作成に直接使用できるようになったイメージ。カタログ作成にマスターイメージではなく準備されたイメージを選択すると、イメージのライフサイクル管理が合理化されるとともに、マシンカタログの作成がより迅速になり、信頼性が高くなります。

イメージの準備について詳しくは、「Machine Creation Service: Image Preparation Summary and Fault-Finding」を参照してください。

2. マシンプロファイルから VM 設定を継承するには、［マシンプロファイルを使用する］を選択し、マシンプロファイルとして使用する VM または ARM テンプレートスペック（Azure に固有）を選択します。

   > 注：
   >
   > 現在、マシンプロファイルの使用は、Azure、AWS、および GCP VM に制限されています。

3. カタログの最小機能レベルを選択します。最新の製品機能を使用できるようにするため、マスターイメージに最新の VDA バージョンがインストールされていることを確認してください。

マシンの構成

> 注：
>
> - このページのタイトルは、［マシン管理］ページで選択した項目：［マシン］、［仮想マシン］、［マシンとユーザー］によって変わります。
> - ［マシンの種類］ページで［リモート **PC** アクセス］を選択した場合、このページは表示されません。
> - 空のカタログを作成できます。これは、そのカタログにはマシンが含まれていないことを意味します。

- **MCS** を使ってマシンを作成する場合：
  - 作成する仮想マシンの数を指定します。何も作成しない場合は、**0**（ゼロ）を入力します。後で空のカタログに対して仮想マシンを作成する場合は、［マシンの追加］を実行します。
  - 各仮想マシンのメモリ量（MB 単位）を選択します。

    > 重要：
    >
    > 作成された各仮想マシンにハードディスクがあります。そのサイズはマスターイメージで設定されます。カタログでハードディスクのサイズを変更することはできません。

  - ［デスクトップエクスペリエンス］ページでユーザーによる静的デスクトップへの変更を専用の Personal vDisk に保存することを指定した場合は、仮想ディスクサイズ（GB 単位）とドライブ文字を指定します。
  - 展開に複数のゾーン（リソースの場所）が含まれている場合、カタログのゾーンを選択できます。

  - 静的なデスクトップ仮想マシンを作成する場合は、仮想マシンコピーモードを選択します。「仮想マシンコピーモード」を参照してください。
  - ランダムな非永続デスクトップ仮想マシンを作成している場合は、マシン上の一時データのライトバックキャッシュを有効にして構成すると、I/O パフォーマンスが向上します。詳しくは、「一時データ用キャッシュの構成」を参照してください。

- 他のツールを使ってマシンを配信する場合:

  マシンアカウント名を追加（またはアカウント名一覧をインポート）します。仮想マシンのアカウント名は、追加またはインポートした後に変更できます。［デスクトップエクスペリエンス］ページで静的なマシンを指定すると、追加する各仮想マシンで使用するユーザー名をオプションで指定できます。

  > ヒント:
  >
  > ユーザーを追加するには、ユーザーを参照するか、ユーザー名をセミコロンで区切って手動入力します。ユーザーが Active Directory にいる場合は、名前を直接入力します。そうでない場合は、次の形式で名前を入力します: `<identity provider>:<user name>`。例: `AzureAD:username`。

  名前を追加またはインポートした後で、［削除］ボタンを使用して、ユーザーはウィザードページで一覧から名前を削除できます。

- 他のツール（**MCS** 以外）を使う場合:

  追加（またはインポート）する各マシンのアイコンとヒントにより、カタログに追加できない可能性のあるマシン、または Cloud Connector に登録できない可能性のあるマシンを特定できます。

仮想マシンコピーモード　［マシン］ページで指定するコピーモードによって、MCS がマスターイメージからシン（簡易コピー）クローンまたはシック（完全なコピー）クローンのどちらを作成するかが決まります。（デフォルトはシンクローン）

- 簡易コピークローンは、効率的にストレージを使用し、すばやくマシンを作成したい場合に使います。
- 完全コピークローンは、マシン作成後に IOPS が潜在的に低下した場合に、質の高いデータの復元と移行サポートが必要な場合に使います。

一時データ用キャッシュの構成　MCS を使用してカタログ内のランダムな非永続マシンを管理する場合、マシンのライトバックキャッシュを有効にして、I/O パフォーマンスを向上させることができます。

ライトバックキャッシュは MCSIO と呼ばれます。詳しくは、このブログ記事を参照してください。

前提条件　ライトバックキャッシュを有効にするには、カタログが次の要件を満たしている必要があります:

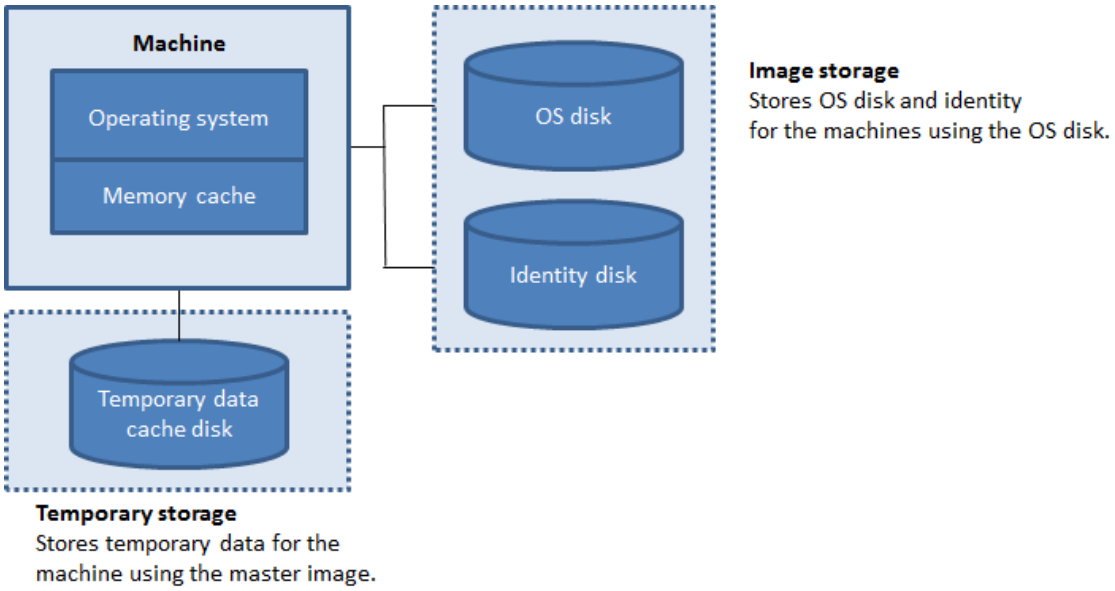
- 一時データのストレージを指定する接続を使用します。詳しくは、「接続およびリソース」を参照してください。
- VDA はバージョン 7.9 以降であり、最新の MCSIO ドライバーがインストールされている必要があります。

> 注:
>
> このドライバーは、VDA のインストール時またはアップグレード時にオプションとしてインストールできます。デフォルトでは、このドライバーはインストールされません。

- ディスクキャッシュのドライブ文字の割り当てを有効にするには、仮想マシンが次の追加の要件を満たしている必要があります:
  - オペレーティングシステム: Windows
  - VDA バージョン: 2305 以降

注意事項

- ライトバックキャッシュには、メモリキャッシュとディスクキャッシュがあります。デフォルトでは、接続の種類によってデフォルト値が異なります。通常は、デフォルト値で十分なことが多いですが、次のデータに必要な容量を検討してください:
  - Windows ページファイルなどの、Windows 自体が作成する一時データファイル
  - ユーザープロファイルデータ
  - ユーザーのセッションに同期される ShareFile データ。
  - セッションユーザーによって作成またはコピーされるデータや、ユーザーがセッション内にインストールするアプリケーション。



- ディスクキャッシュのみを使用し、メモリキャッシュを使用しないライトバックキャッシュの構成は廃止されました。一時データのキャッシュを有効にするには、[ディスクキャッシュサイズ (**GB**)] と [キャッシュに割り当てられたメモリ (**MB**)] の両方を選択し、メモリキャッシュに 0 より大きいサイズを指定することをお勧めします。一時データは最初にメモリキャッシュに書き込まれます。メモリキャッシュが、構成された制限に達すると、古いデータから先に一時データキャッシュディスクに移動されます。

- メモリキャッシュは、各マシンの合計メモリ容量の一部です。そのため、［メモリキャッシュサイズ（**MB**）（推奨）］チェックボックスをオンにする場合は、各マシンの合計メモリ容量を増やすことを検討してください。
- ［ディスクキャッシュサイズ（**GB**）］をデフォルト値から変更すると、パフォーマンスに影響することがあります。サイズはユーザー要件とマシンの負荷に合わせる必要があります。

  > 重要：
  >
  > ディスクキャッシュの容量が不足すると、ユーザーセッションは利用できなくなります。

- ［ディスクキャッシュサイズ］チェックボックスをオフにすると、キャッシュディスクは作成されません。この場合、［キャッシュに割り当てられたメモリ］にすべての一時的なデータを保持するのに十分な値を指定します。これは、各仮想マシンへの割り当てに大量の RAM が使用できる場合にのみ可能です。
- 両方のチェックボックスをオフにすると、一時データはキャッシュされず、各仮想マシンの差分ディスク（OS ストレージにあります）に書き込まれます。（これは、7.9 より前のリリースでは、プロビジョニングアクションです。）
- このカタログを使用して AppDisk を作成しようとしている場合は、キャッシュを有効にしないでください。
- マシンカタログの作成後は、キャッシュ値を変更できません。

CSV ファイルを使用したマシンの一括追加　［完全な構成］管理インターフェイスを使用する場合は、CSV ファイルを使用してマシンを一括で追加できます。この機能は、MCS（Machine Creation Services）を介して作成されたカタログを除いて、すべてのカタログで使用できます。

CSV ファイルを使用してマシンを一括追加する一般的なワークフローは次のとおりです：

1. ［マシン］ページで、［**CSV** ファイルの追加］を選択します。［マシンを一括で追加］ウィンドウが開きます。
2. ［**CSV** テンプレートのダウンロード］を選択します。
3. テンプレートファイルに入力します。
4. ファイルをドラッグまたは参照してアップロードします。
5. ［検証］を選択して、インポートの検証チェックを実行します。
6. ［インポート］を選択して完了します。

CSV ファイルの注意事項については、「CSV ファイルを使用してマシンを追加する場合の考慮事項」を参照してください。

同じ［マシン］ページのカタログからマシンをエクスポートすることもできます。エクスポートされたマシンの CSV は、マシンを一括で追加するときにテンプレートとして使用できます。マシンをエクスポートするには：

1. ［マシン］ページで、［**CSV** ファイルのエクスポート］を選択します。マシン一覧を含む CSV ファイルがダウンロードされます。
2. CSV ファイルを開き、必要に応じてマシンを追加または編集します。保存した CSV ファイルを使用してマシンを一括で追加するには、前のセクション「CSV ファイルを使用したマシンの一括追加」を参照してください。

> 注:
>
> - この機能は、リモート PC アクセスカタログでは使用できません。
> - CSV ファイルでのマシンのエクスポートとインポートは、同じ種類のカタログ間でのみサポートされます。

マシンの **NIC** の構成

［マシンの種類］ページで［リモート **PC** アクセス］を選択した場合、［**NIC**］ページは表示されません。

複数の NIC を使用する場合は、各 NIC に仮想ネットワークを関連付けます。たとえば、特定のセキュアネットワークへのアクセスに 1 つの NIC を割り当てて、より一般的なネットワークへのアクセスに別の NIC を割り当てることができます。また、このページで NIC を追加または削除することもできます。

マシンアカウントの追加

> 注:
>
> ［マシンアカウント］ページが表示されるのは、［マシンの種類］ページで ［リモート **PC** アクセス］を選択した場合に限ります。

Active Directory マシンアカウントまたは組織単位（OU）を追加します。組織単位名にはスラッシュ（/）を使用しないでください。

構成済みの電源管理接続を選択するか、電源管理を使用しないことを選択します。電源管理に必要な接続が構成済みでない場合は、マシンカタログの作成後に新しい接続を作成してから、そのマシンカタログを編集して電源管理設定を更新できます。

また、CSV ファイルを使用してマシンを一括で追加できます。これを行うための一般的なワークフローは次のとおりです:

1. ［マシンアカウント］ページで、［**CSV** ファイルの追加］を選択します。［マシンを一括で追加］ウィンドウが開きます。
2. ［**CSV** テンプレートのダウンロード］を選択します。
3. テンプレートファイルに入力します。
4. ファイルをドラッグまたは参照してアップロードします。
5. ［検証］を選択して、インポートの検証チェックを実行します。
6. ［インポート］を選択して完了します。

CSV ファイルの注意事項については、「CSV ファイルを使用してマシンを追加する場合の考慮事項」を参照してください。

カタログでマシンの **ID** を構成する

> 注:
>
> - ［マシン **ID**］ページが表示されるのは、［マシンの種類］ページで ［リモート **PC** アクセス］を選択せず、かつ ［マシン管理］ページで ［**Citrix Machine Creation Services (MCS)**］を選択する場合に限ります。

カタログ内の各マシンは、一意の ID を持っている必要があります。このページでは、カタログ内のマシンの ID を構成できます。マシンは、プロビジョニングされた後、ID に結合されます。カタログの作成後に ID の種類を変更することはできません。

このページで設定を構成するための一般的なワークフローは次のとおりです:

1. 一覧から ID を選択します。
2. アカウントを作成するか既存のアカウントを選択して、アカウントの場所（ドメイン）を指定します。

次のいずれかのオプションを選択できます:

- オンプレミス **Active Directory**: 組織が所有しているマシンで、その組織に属した Active Directory アカウントでサインインしたマシン。これらのマシンはオンプレミスに存在します。

  > 注:
  >
  > デフォルトでは、リソース（接続）が存在するドメインが選択されます。

- **Azure AD** 参加: 組織が所有しているマシンであり、その組織に属した Azure Active Directory アカウントでサインインしたマシン。作成済みのマシンはクラウドにのみ存在します。要件、制限、および考慮事項については、「Azure Active Directory 参加済み」を参照してください。

  > 注:
  >
  > このオプションを使用するには、マスターイメージがオペレーティングシステムの前提条件を満たしている必要があります。詳しくは、Microsoft のドキュメント「Microsoft Entra joined devices」を参照してください。

- **Hybrid Azure Active Directory** 参加済み。組織が所有しているマシンであり、その組織に属した Active Directory Domain Services アカウントでサインインしたマシン。これらのマシンはクラウドとオンプレミスに存在します。要件、制限、および考慮事項については、「Hybrid Azure Active Directory 参加済み」を参照してください。

  > 注:
  >
  > - Hybrid Azure Active Directory 参加を使用する前に、Azure 環境が前提条件を満たしていることを確認してください。「Microsoft Entra ハイブリッド参加を構成する」を参照してください。
  > - このオプションを使用するには、マスターイメージがオペレーティングシステムの前提条件を満た

> している必要があります。詳しくは、「Microsoft Entra hybrid joined devices」を参照してください。

- ドメイン非参加。どのドメインにも参加していないマシン。要件と制限については、「ドメイン非参加」を参照してください。

> 重要:
>
> - ID の種類に［オンプレミス **Active Directory**］または［**Hybrid Azure Active Directory joined**］を選択した場合、カタログ内の各マシンには、対応する Active Directory コンピューターアカウントが必要です。
> - ID の種類が ［ドメイン非参加］である場合には、カタログの最小機能レベルとしてバージョン 1811 以降の VDA が必要です。この VDA は最小機能レベルを更新すると使用可能になります。
> - ［**Azure Active Directory** 参加済み］および［ハイブリッド **Azure Active Directory** 参加］の ID タイプを使用するには、カタログの最小機能レベルとして、バージョン 2203 以降の VDA が必要です。これらの VDA は最小機能レベルを更新すると使用可能になります。

アカウントを作成する場合は、マシンが存在する OU にコンピューターアカウントを作成する権限が必要です。カタログ内の各マシンは、一意の名前である必要があります。作成するマシンのアカウント名前付けスキームを指定します。詳しくは、「マシンのアカウント名前付けスキーム」を参照してください。

> 注:
>
> OU 名にスラッシュ（/）が使用されていないことを確認してください。

既存のアカウントを使用する場合、アカウントを参照するか、［インポート］をクリックしてアカウント名が含まれる`.csv`ファイルを指定します。インポートするファイルでは、次の形式を使用する必要があります:
`[ADComputerAccount] ADcomputeraccountname.domain`

追加するすべてのマシンに十分な数のアカウントをインポートする必要があります。完全な構成インターフェイスで、これらのアカウントを管理します。そのため、すべてのアカウントのパスワードのリセットを［完全な構成］インターフェイスに許可するか、アカウントのパスワードを指定します（すべてのアカウントで同じパスワードを使用する必要があります）。

物理マシンまたは既存のマシン用のカタログでは、既存のアカウントを選択またはインポートして、各マシンを Active Directory コンピューターアカウントおよびユーザーアカウントに割り当てます。

マシンのアカウント名前付けスキーム　カタログ内の各マシンは、一意の名前である必要があります。カタログを作成するときに、マシンのアカウント名前付けスキームを指定する必要があります。名前で、連続した数字または文字を表示するには、プレースホルダーとしてワイルドカード（ハッシュ記号）を使用します。

名前付けスキームを指定するときは、次の点を考慮してください:

- 許可される最大文字数は 15 文字です。

- 名前付けスキームには、少なくとも 1 個のワイルドカード文字を含める必要があります。すべてのワイルドカードは同時に指定する必要があります。
- 名前全体には、ワイルドカードを含め、2 文字以上 15 文字以下が含まれている必要があります。少なくとも 1 つの数字ではない値と、1 つの #（ワイルドカード）文字を含める必要があります。
- 名前にスペースや次の文字を含めることはできません：`,~!@'$%^&.()} { \/*?"<>|=+[];:_".`。
- 名前をハイフン「-」で終了することはできません。
- 文字数は、マシンアカウント数の増加に応じて増加します。たとえば、「veryverylong#」というスキームで 1,000 個のマシンアカウントを作成するとします。最後に作成されるアカウント名（veryverylong1000）には、許可される最大文字数を超える 16 文字が含まれることになります。

連続する値を数字（0～9）にするか、文字（A～Z）にするかを指定できます：

- **0～9**。選択した場合、指定したワイルドカードは連番になります。

  > 注：
  >
  > ワイルドカードが 1 つ（#）しかない場合、アカウント名は 1 で始まります。2 つある場合、アカウント名は 01 で始まります。3 つある場合、アカウント名は 001 で始まります。

- **A-Z**。選択した場合、指定したワイルドカードは連続した文字になります。

たとえば、名前付けスキームとして「PC-Sales-##」を指定して［**0-9**］を選択すると、PC-Sales-01、PC-Sales-02、PC-Sales-03 などのアカウント名が作成されます。

オプションで、アカウント名の先頭を指定できます。

- ［**0-9**］を選択すると、アカウントには指定した数字から順番に名前が付けられます。前のフィールドで使用するワイルドカードの数に応じて、1 つまたは複数の数字を入力します。たとえば、2 つのワイルドカードを使用する場合は、2 桁以上を入力します。
- ［**A-Z**］を選択すると、アカウントには指定した文字から順番に名前が付けられます。前のフィールドで使用するワイルドカードの数に応じて、1 つまたは複数の文字を入力します。たとえば、2 つのワイルドカードを使用する場合は、2 文字以上を入力します。

ドメイン資格情報の追加

［資格情報の入力］を選択して、ターゲットの Active Directory ドメインでアカウント操作を実行する権限を持つ管理者の資格情報を入力します。

［名前の確認］オプションを使用して、ユーザー名が有効か一意かを確認します。このオプションは、次のような場合に役立ちます：

- 同じユーザー名が複数のドメインに存在する。目的のユーザーを選択するように求められます。
- ドメイン名を忘れた。ドメイン名を指定せずにユーザー名を入力できます。この確認が完了すると、ドメイン名が自動的に入力されます。

> 注:
>
> ［マシン **ID**］で選択した ID の種類が ［**Hybrid Azure Active Directory joined**］である場合、入力する資格情報に`Write userCertificate`権限が付与されている必要があります。

Workspace Environment Management 構成セットの選択（オプション）

［**WEM**］ページは、Citrix DaaS の Advanced または Premium を使用している場合にのみ表示されます。

カタログをバインドする Workspace Environment Management（WEM）構成セットを選択します。構成セットは、WEM 構成のセットを編成するために使用される論理コンテナです。カタログを構成セットにバインドすると、WEM を使用して、可能な限り優れたワークスペース環境をユーザーに提供できます。

> 重要:
>
> - カタログを構成セットにバインドする前に、WEM サービス環境をセットアップする必要があります。Citrix Cloud にサインインしてから、WEM サービスを起動します。詳しくは、「Workspace Environment Management サービスの開始」を参照してください。
> - 既に WEM を使用している場合は、プロビジョニングしようとしているカタログ内のマシンが構成セットに既に存在している可能性があります。たとえば、Active Directory を介して存在しているケースなどです。その場合は、Active Directory を一貫して使用して構成を実行し、この構成をスキップすることをお勧めします。

選択した構成セットに WEM の基本構成に関連する設定が含まれていない場合は、次のオプションが表示されます:

- [基本設定を構成セットに適用します]。このオプションを使用すると、構成セットに基本設定を適用することで、WEM をすばやく開始できます。基本設定には、CPU スパイク保護、CPU スパイクの自動防止、およびインテリジェントな CPU 最適化が含まれています。基本設定を表示するには、こちらのリンクをクリックしてください。変更するには、WEM コンソールを使用します。

VDA のアップグレード（オプション）

> 重要:
>
> - スムーズにアップグレードするには、VDA を CR または LTSR CU バージョンにアップグレードする前に、前提条件を満たしていることを確認し、既知の問題を確認してください。「完全な構成インターフェイスを使用した VDA のアップグレード」を参照してください。
> - LTSR VDA を LTSR 累積更新プログラム（CU）バージョンにアップグレードする場合は、VDA 上で実行されている Citrix VDA Upgrade Agent のバージョンが 7.36.0.7 以降であることを確認してください。詳しくは、「完全な構成インターフェイスを使用した VDA のアップグレード」を参照してください。

この機能は、次のマシンの種類に適用されます:

- MCS でプロビジョニングされた永続マシン。カタログの作成中に、[マシン管理] ページの [**Citrix Machine Creation Services**] を使用してそれらを展開します。
- MCS で作成されていないマシン（物理マシンなど）。カタログの作成中に、[マシン管理] ページの [ほかのサービスまたはテクノロジ] を使用してそれらを展開します。

2 つのオプションについて詳しくは、「マシン管理」を参照してください。

[**VDA** のアップグレード] ページで、アップグレード先の VDA バージョンを選択します。指定した場合、VDA Upgrade Agent がインストールされているカタログ内の VDA は、選択したバージョンにすぐに、またはスケジュールした時間に、アップグレードできます。

> 注:
>
> - この機能は、最新の VDA へのアップグレードのみをサポートします。VDA アップグレードスケジュールを作成する、または VDA をアップグレードするタイミングによって、VDA の最新バージョンが決まります。
> - VDA アップグレード設定を構成した後、[**VDA** アップグレード] フィールドに最新のステータスが反映されるまでに最大 15 分かかる場合があります。[**VDA** のアップグレード] 列を表示するには、[列] をクリックして右上隅にアイコンを表示し、[マシンカタログ] **>** [**VDA** のアップグレード] を選択して、[保存] をクリックします。

展開に適した VDA トラックを選択します:

> 重要:
>
> 以前のバージョンから新しいバージョンに切り替えれば、CR VDA と LTSR VDA を切り替えることができます。ダウングレードと見なされるため、新しいバージョンから以前のバージョンに切り替えることはできません。たとえば、2212 CR から 2203 LTSR（任意の CU）にダウングレードすることはできませんが、2112 CR から 2203 LTSR（任意の CU）にアップグレードすることはできます。

- 最新の **CR VDA**。最新リリース（CR）は、最新の画期的なアプリ、デスクトップ、サーバー仮想化機能を提供します。
- 最新の **LTSR VDA**。長期サービスリリース（LTSR）は、長期間にわたって同じ基本バージョンを維持する必要がある大企業の実稼働環境に適しています。

カタログの作成後、必要に応じて VDA をアップグレードできます。詳しくは、「VDA のアップグレード」を参照してください。

後で VDA のアップグレードを有効にする場合は、カタログ作成後にカタログを編集することで、このページに戻ることができます。詳しくは、「カタログを編集して VDA アップグレード設定を構成する」を参照してください。

設定の確認

[概要] ページで、指定した設定を確認します。カタログの名前と説明を入力します。この情報は、[完全な構成] 管理インターフェイスに表示されます。

完了したら、［完了］をクリックしてカタログの作成を開始します。

［マシンカタログ］では、新しいカタログがインラインプログレスバーとともに表示されます。

作成の進行状況の詳細を表示するには：

1. マシンカタログの上にマウスポインターを置きます。
2. 表示されるツールチップで、［詳細の表示］をクリックします。

   手順ごとの進行状況グラフが表示され、次のことがわかります：

   - 手順の履歴
   - 現在の手順の進行状況と実行時間
   - 残りの手順

PowerShell コマンドを使用して **MCS** マシンカタログを作成する

MCS マシンカタログを作成する別の方法として、PowerShell コマンドを使用する方法もあります。詳しくは、次のトピックを参照してください：

- SDK および API
- Manage Citrix DaaS using Remote PowerShell SDKs
- New-ProvScheme

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

MCS I/O ライトバックキャッシュディスクに特定のドライブ文字を割り当てることができます。この機能の導入は、使用するアプリケーションのドライブ文字と MCS I/O ライトバックキャッシュディスクのドライブ文字の間の競合を回避するのに役立ちます。これを行うには、PowerShell コマンドを使用できます。サポートされているハイパーバイザーは、Azure、GCP、VMware、SCVMM、および XenServer です。

> 注：
>
> この機能では、VDA バージョン 2305 以降が必要です。

制限事項

- Windows オペレーティングシステムのみに適用されます
- ライトバックキャッシュディスクに適用できるドライブ文字：E～Z
- Azure 一時ディスクがライトバックキャッシュディスクとして使用されている場合は適用されません
- 新しいマシンカタログを作成する場合にのみ適用されます

ライトバックキャッシュディスクにドライブ文字を割り当てる　ライトバックキャッシュディスクにドライブ文字を割り当てるには、次の手順を実行します:

1. **PowerShell** ウィンドウを開きます。
2. `asnp citrix*`を実行します。
3. ID プールをまだ作成していない場合は作成します。詳しくは、「Creating a Catalog」を参照してください。
4. `New-ProvScheme`コマンドをプロパティ`WriteBackCacheDriveLetter`で使用してプロビジョニングスキームを作成します。例:

```
New-ProvScheme -CleanOnBoot `
-HostingUnitName "<name>" `
-IdentityPoolName $schemeName `
-ProvisioningSchemeName $schemeName `
-InitialBatchSizeHint 1 `
-UseWriteBackCache -WriteBackCacheDiskSize 127 -
   WriteBackCacheMemorySize 256 -WriteBackCacheDriveLetter E `
-MasterImageVM "XDHyp:\HostingUnits<name>\image.folder\abcd-
   resources.resourcegroup\
   MCSIOMasterVm_OsDisk_1_d3e2d6352xxxxxxxx2130aa145ec77.
   manageddisk" `
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\name\virtualprivatecloud.folder\East US.
    region\virtualprivatecloud.folder\abcd-resources.resourcegroup
    \abcd-resources-vnet.virtualprivatecloud\default.network" }
  `
-ServiceOffering "XDHyp:\HostingUnits\<name>\serviceoffering.
   folder\Standard_D2s_v5.serviceoffering" `
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.
   com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="
   true" />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows"
   />
<Property xsi:type="StringProperty" Name="StorageType" Value="
   Premium_LRS"/>
<Property xsi:type="StringProperty" Name="PersistWBC" Value="false
   " />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="
   false" />
<Property xsi:type="StringProperty" Name="PersistVm" Value="false"
    />
<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
   Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value
   ="false" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
   abcd-group1" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
   Windows_Client" />
```



```
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2"
    />
</CustomProperties>'
<!--NeedCopy-->
```

5. カタログの作成を完了します。

カスタムプロパティの設定に関する重要な考慮事項

カスタムプロパティは、GCP および Azure 環境の`New-ProvScheme`と`Set-ProvScheme`で正しく設定する必要があります。存在しないカスタムプロパティを指定すると、次のエラーメッセージが表示され、コマンドの実行に失敗します。

```
Invalid property found: <invalid property>. Ensure that the CustomProperties
 parameter supports the property.
```

ProvScheme パラメーターの設定に関する重要な考慮事項

MCS を使用してカタログを作成するとき、以下を実行した場合にエラーが発生します:

- マシンカタログを作成するときに、サポートされていないハイパーバイザーに次の`New-ProvScheme`パラメーターを設定した:

パラメーター	サポートされるハイパーバイザー
`UseWriteBackCache`	VMware Hyper-V XenServer Azure GCP
`DedicatedTenancy`	Azure GCP AWS
`TenancyType`	Azure GCP AWS
`UseFullDiskCloneProvisioning`	VMware Hyper-V

パラメーター	サポートされるハイパーバイザー
	XenServer

- マシンカタログを作成した後、次のSet-ProvSchemeパラメーターを更新した:
  - CleanOnBoot
  - UseWriteBackCache
  - DedicatedTenancy
  - TenancyType
  - UseFullDiskCloneProvisioning

仮想マシン作成時の **SID** の追加

ADAccountSidパラメーターを追加することで、新しい仮想マシンの作成時にマシンを一意に識別できます。

これを行うには、以下の手順に従います:

1. サポートされている ID タイプでカタログを作成します。
2. NewProvVMを使用してマシンをカタログに追加します。例:

```
New-ProvVM  -ProvisioningSchemeName "name"  -ADAccountSid @("SID "
    )  -RunAsynchronously
<!--NeedCopy-->
```

ただし、次のものを使用してマシンをプロビジョニングすることはできません:

- カタログ ID プールにない AD アカウント
- 使用可能な状態にない AD アカウント

MCS マシンカタログを作成する前に構成を検証

New-ProvSchemeコマンドで-validateパラメーターを使用して、MCS マシンカタログを作成する前に構成設定を検証できます。パラメーターを指定してこの PowerShell コマンドを実行すると、間違ったパラメーターが使用されている場合、またはパラメーターが別のパラメーターと競合している場合は、適切なエラーメッセージが表示されます。その後、エラーメッセージを使用して問題を解決し、PowerShell を使用して MCS マシンカタログを正常に作成できます。現在、この機能は Azure、GCP、および VMware 仮想化環境に適用できます。

> 注:
>
> 検証中は、実際の MCS マシンカタログを作成しないでください。コマンドの結果を使用してエラーを修正し、

> 正常なカタログを作成する必要があります。したがって、New-ProvSchemeコマンドの実行中は、偽の ID プール名を使用します。

構成を検証するには、次の手順を実行します:

1. Delivery Controller ホストから PowerShell ウィンドウを開きます。
2. asnp citrix*を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. New-ProvSchemeコマンドを実行し、パラメーター-validateを使用します。コマンドが機能するように偽の ID プール名を指定します。例:

```
$result =New-ProvScheme  -CleanOnBoot -HostingUnitName "vSanRg" -
    IdentityPoolName "mptmpcatalogdemo" -InitialBatchSizeHint 1  -
    MasterImageVM "XDHyp:\HostingUnits\vSanRg\Windows19MasterImage.
    vm\Citrix_XD_NonMachineProfileWin19Machines.snapshot" -
    NetworkMapping @{
 "0"="XDHyp:\HostingUnits\vSanRg\VM Network.network" }
  -ProvisioningSchemeName "MachineProfileW10Machines"  -Scope @()
-VMCpuCount 2  -VM
MemoryMB 6143 -MachineProfile "XDHyp:\HostingUnits\vSanRg\TRW-
    Win11-tpm-BL-TEMPLATE.template" -TenancyType Shared  -
    FunctionalLevel "L7_20" -Validate
$result.TerminatingError | Format-List -Property *
<!--NeedCopy-->
```

エラーメッセージ:

```
ErrorData     : {
 [[ValidationFailureCount, xxx], [InvalidMemoryValue, The memory
    size provided 6143 must be a multiple of 4 MB and must be
    greater than or equal to 4 MB.], [InconsistentGuestOsSetting,
    The GuestOs setting - windows9_64Guest of the selected machine
     profile does not match with the setting -
    windows2019srv_64Guest of master image. Please select a
    machine profile that matches the GuestOs setting of the master
     image.], [InconsistentVtpmSetting, The vTPM setting of the
    selected machine profile does not match with the selected
    master image. Please select a machine profile that matches the
     vTPM setting of the master image.], [
    InconsistentFirmwareSetting, The firmware setting - efi of the
     selected machine profile does not match with the setting -
    bios of master image. Please select a machine profile that
    matches the firmware setting of the master image ErrorId
    : ValidationFailure
ErrorMessage : ValidationFailure
Operation    : ValidatingInputs
<!--NeedCopy-->
```

4. 構成設定を検証した後、実際の ID プール名と正しいパラメーターを使用して MCS マシンカタログを作成できます。

次の手順

特定のハイパーバイザーカタログの作成については、次を参照してください:

- AWS カタログの作成
- Google Cloud Platform カタログの作成
- Microsoft Azure カタログの作成
- Microsoft System Center Virtual Machine Manager カタログの作成
- Nutanix カタログの作成
- VMware カタログの作成
- XenServer カタログの作成

最初のカタログを作成すると、デリバリーグループを作成する手順が表示されます。

構成プロセスの全体像については、「展開の計画と構築」を参照してください。

完全な構成ユーザーインターフェイスと PowerShell を使用して、Citrix Provisioning カタログを作成できるようになりました。
この機能の導入には、次のような利点があります:

- MCS と Citrix Provisioning カタログの両方を管理できる単一の統合コンソール。
- ID 管理ソリューション、オンデマンドプロビジョニングなどの Citrix Provisioning カタログの新機能を利用できる。

現在、この機能は Azure および VMware のワークロードでのみ使用できます。ただし、VMware 環境では、現在 PowerShell コマンドのみを使用してカタログを作成できます。詳しくは、「Citrix Studio での Citrix Provisioning カタログの作成」を参照してください。

追加情報

- Citrix Virtual Apps and Desktops のイメージ管理
- 接続とリソースの作成と管理
- マシン ID 参加済みカタログの作成
- マシンカタログの管理

AWS カタログの作成

May 17, 2024

「マシンカタログの作成」では、マシンカタログを作成するウィザードについて説明します。以下の情報は、AWS 仮想化環境に固有の詳細について説明しています。

> 注:
>
> AWS カタログを作成する前に、AWS への接続の作成を完了する必要があります。「AWS への接続」を参照してください。

イメージの準備中のネットワーク設定

イメージの準備中に、元の仮想マシンに基づいて準備用の仮想マシン（VM）が作成されます。この準備 VM はネットワークから切断されています。ネットワークを準備 VM から切断するために、すべての受信および送信トラフィックを拒否するネットワークセキュリティグループが作成されます。このネットワークセキュリティグループは保持され、再利用されます。ネットワークセキュリティグループの名前は`Citrix.XenDesktop.IsolationGroup-GUID`で、GUID がランダムに生成されます。

AWS テナント

AWS には、共有テナント（デフォルトの種類）と専用テナントのテナントオプションが用意されています。共有テナントの場合、さまざまな顧客の複数の Amazon EC2 インスタンスが同じ物理ハードウェア上に存在する可能性があります。専用テナントの場合、EC2 インスタンスは、ユーザーが展開したほかのインスタンスを含むハードウェア上のみで実行されます。ほかの顧客は同じハードウェアを使用しません。

[完全な構成] インターフェイスまたは PowerShell を使用することで、MCS を使用して AWS 専用ホストをプロビジョニングできます。

AWS ホストへのプロビジョニングの要件

- インポートされた BYOL（ライセンス持ち込み）のイメージ（AMI）。専用ホストでは、既存のライセンスを使用および管理します。
- プロビジョニング要求を満たすのに十分な使用率を持つ専用ホストの割り当て。
- 自動配置の有効化。

完全な構成インターフェイスを使用した **AWS** 専用ホストテナントの構成

MCS を使用してカタログを作成し、AWS でマシンをプロビジョニングすると、[マシンカタログのセットアップ] > [セキュリティ] ページには以下のオプションが表示されます:

- 共有されているハードウェアを使用する。この設定は、一般的な環境に適しています。複数の顧客が相互に通信していなくても、ハードウェアを共有します。共有ハードウェアの使用は、Amazon EC2 インスタンスを実行するための最も安価なオプションです。

- 専用のホストを使用する。Amazon EC2 専用ホストは、完全に専用の EC2 インスタンス容量を搭載した物理サーバーです。既存のソケット単位または VM 単位のソフトウェアライセンスを使用することができます。専用ホストには、インスタンスの種類に基づいて使用率が事前に設定されています。たとえば、C4 ラージインスタンスの種類の 1 つの割り当てられた専用ホストは、16 個のインスタンスの実行に限定されます。詳しくは、AWS のサイトを参照してください。
- 専用のインスタンスを使用する。この設定は、セキュリティまたはコンプライアンス上の要件を満たす必要がある環境に適しています。専用のインスタンスを使用すると、ホストをほかの AWS の顧客と分離することによる利点を活用しながら、ホスト全体に対する支払いが不要になります。ホストの容量を心配する必要はありませんが、使用するインスタンスに対してより高い料金が請求されます。

  この設定は、ライセンス制限やセキュリティ要件により、専用ホストを使用する必要がある展開に適しています。専用のホストを使用すると、物理ホスト全体を所有することになり、時間単位で課金されます。ホストを所有すると、追加料金なしで、そのホストが許可する数の EC2 インスタンスをスピンアップできます。

> 注:
>
> 進行中のカタログ作成タスクまたはイメージ更新タスクがない場合は、使用可能な準備 ID ディスクを削除できます。

PowerShell を使用した **AWS** 専用ホストテナントの構成

または、PowerShell を使用して AWS 専用のホストをプロビジョニングすることもできます。`Host`に設定した`TenancyType`パラメーターを付けた`New-ProvScheme`コマンドレットを使用します。

AWS インスタンスプロパティのキャプチャ

AWS で Machine Creation Services（MCS）を使用してマシンをプロビジョニングするカタログを作成する場合、このカタログのマスターイメージに相当する AMI を選択します。MCS は、この AMI からディスクのスナップショットを使用します。

> ヒント:
>
> AWS インスタンスプロパティキャプチャを使用するには、AMI に関連付けられた VM が必要です。

MCS は AMI が作成されたインスタンスからプロパティを読み取り、マシンの ID アクセス管理（IAM）の役割およびタグを提供されたカタログにプロビジョニングされたマシンに適用します。このオプション機能を使用する場合、カタログ作成プロセスでは、選択した AMI ソースインスタンスが検索され、限定されたプロパティセットが読み取られます。これらのプロパティは、そのカタログのマシンをプロビジョニングするために使用される AWS 起動テンプレートに保存されます。カタログ内のすべてのマシンがキャプチャされたインスタンスのプロパティを継承します。

キャプチャされたプロパティには、以下が含まれます:

- IAM 役割: プロビジョニングされたインスタンスに適用されます。

- タグ：プロビジョニングされたインスタンスやそのディスク、NIC に適用されます。これらのタグは次のような一時的な Citrix リソースに適用されます：S3 バケットおよびオブジェクト、AMI、スナップショット、起動テンプレート。

> ヒント：
>
> 一時的な Citrix リソースのタグ付けはオプションで、カスタムプロパティ `AwsOperationalResourcesTagging` を使用して構成できます。タグを正常に適用し、運用リソースのタグ付けを使用して AWS カタログを作成するには、AMI の作成に使用された EC2 インスタンスを削除しないでください。

AWS インスタンスプロパティのキャプチャ

この機能は、AWS ホスト接続でプロビジョニングスキーム作成時にカスタムプロパティ `AwsCaptureInstancePropertie` を指定することで使用できます：

```
New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true"
…<standard provscheme parameters
```

詳しくは、「New-ProvScheme」を参照してください。

> 注：
>
> `AwsCaptureInstanceProperties` は廃止済みです。代わりに、マシンプロファイルを使用して VM のマシンプロパティを指定することをお勧めします。

AWS 運用リソースのタグ付け

Amazon Machine Image（AMI）は、Amazon クラウド環境内で仮想マシンを作成するために使用される、一般に EC2 と呼ばれる仮想アプライアンスの種類を表します。AMI を使用して、EC2 環境を使用するサービスを展開します。AWS で MCS を使用してマシンをプロビジョニングするカタログを作成する場合、このカタログのゴールデンイメージとして機能する **AMI** を選択します。

> 重要：
>
> インスタンスプロパティと起動テンプレートをキャプチャしてカタログを作成することは、運用リソースのタグ付けに必要です。

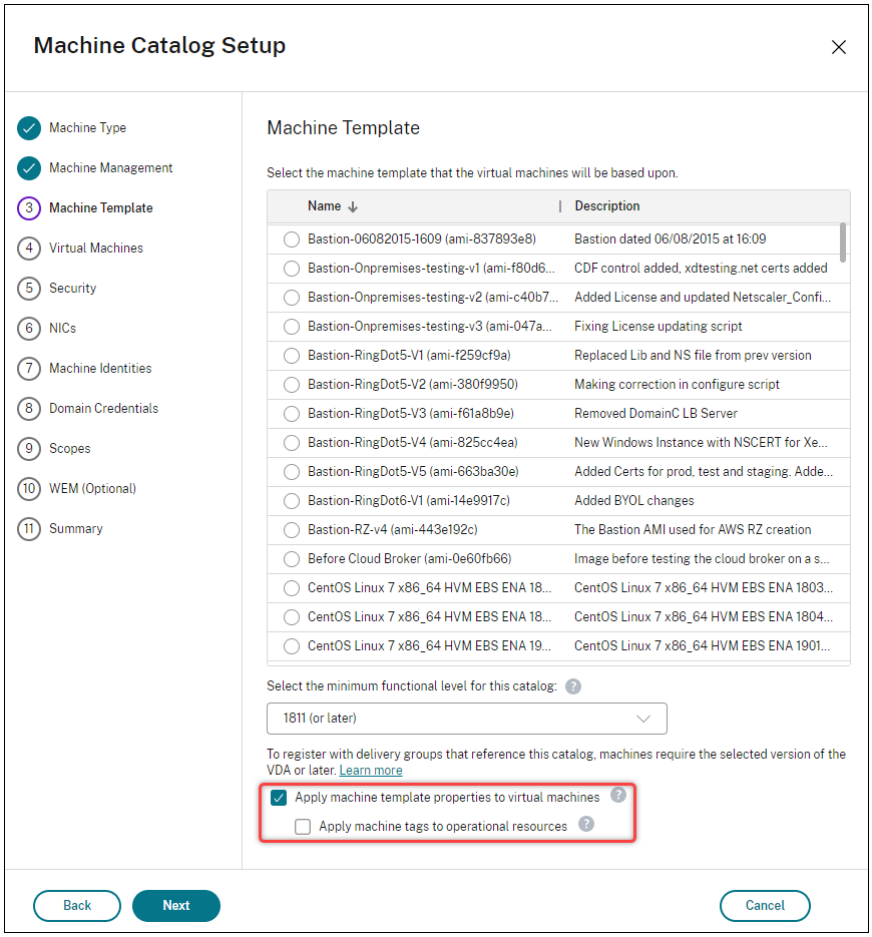
AWS カタログを作成するには、最初にゴールデンイメージとして使用するインスタンスの AMI を作成する必要があります。MCS は、そのインスタンスからタグを読み取り、起動テンプレートに組み込みます。起動テンプレートタグは、AWS 環境で作成されたすべての Citrix リソースに適用されます。これには以下が含まれます：

- 仮想マシン
- VM ディスク
- VM ネットワークインターフェイス
- S3 バケット

- S3 オブジェクト
- 起動テンプレート
- AMI

完全な構成インターフェイスでの **AWS** インスタンスのプロパティの適用および運用リソースのタグ付け

MCS を使用して AWS でマシンをプロビジョニングするカタログを作成する場合、IAM の役割とタグのプロパティをそれらのマシンに適用するかを制御できます。マシンタグを運用リソースに適用するかを制御することもできます。次の 2 つのオプションが使用できます:



- マシンテンプレートのプロパティを仮想マシンに適用する
  - 選択したマシンテンプレートに関連付けられた IAM の役割とタグのプロパティを、このカタログ内の仮想マシンに適用するかを制御します。
- 運用リソースにマシンタグを適用する
  - マシンのプロビジョニングを容易にするマシンタグを AWS 環境で作成された項目に適用するかを制御します。カタログ作成の副産物として運用リソースが作成されます。運用リソースには、準備 VM インスタンスや AMI などの一時的なリソースと永続的なリソースの両方が含まれます。

PowerShell を使用した運用リソースへのタグ付け

PowerShell を使用してリソースにタグを付けるには、次の手順を実行します:

1. DDC ホストから PowerShell ウィンドウを開きます。
2. コマンド`asnp citrix`を実行し、Citrix 固有の PowerShell モジュールをロードします。

プロビジョニングされた仮想マシンのリソースにタグを付けるには、カスタムプロパティ`AwsOperationalResourcesTag`を使用します。以下はこのプロパティの構文です:

```
New-ProvScheme -CustomProperties “AwsCaptureInstanceProperties, true; AwsOperationalResourcesTagging,true” …<standard provscheme parameters>
```

PowerShell を使用してマシンプロファイルベースのマシンカタログを作成する

マシンプロファイルを使用して、EC2 インスタンス（VM）からハードウェアプロパティをキャプチャしたり、テンプレートバージョンを起動してプロビジョニングされたマシンに適用したりできます。キャプチャされるプロパティには、たとえば、EBS ボリュームプロパティ、インスタンスの種類、EBS の最適化、CPU オプション、テナントの種類、休止状態機能、およびその他のサポートされている AWS 構成が含まれます。

AWS EC2 インスタンス（VM）または AWS 起動テンプレートのバージョンをマシンプロファイルの入力として使用できます。

> 注:
>
> EBS ボリュームのプロパティは、マシンプロファイルからの値のみを使用します。

重要な注意事項

MCS マシンカタログを作成する際の重要注意事項は以下のとおりです:

- `New-ProvScheme`および`Set-ProvScheme`コマンドにマシンのハードウェアプロパティのパラメーターを追加すると、パラメーターで指定された値がマシンプロファイルの値を上書きします。
- `AwsCaptureInstanceProperties`を**`true`**として設定し、`MachineProfile`プロパティを設定しない場合は、IAM の役割とタグのみがキャプチャされます。
- `AwsCaptureInstanceProperties`と`MachineProfile`を同時に設定することはできません。

  > ** 注:
  >
  > `AwsCaptureInstanceProperties`は廃止済みです。

- マシンプロファイルが指定されていない場合は、以下のプロパティの値を明示的に指定する必要があります:

  - セキュリティグループ
  - ENI または仮想ネットワーク

- AwsCaptureInstancePropertiesを有効にするか、マシンプロファイルを指定する場合にのみ、AwsOperationalResourcesTaggingを有効にすることができます。

MCS マシンカタログを作成した後の重要な注意事項は以下のとおりです:

- マシンプロファイルベースのカタログのカタログを非マシンプロファイルベースのカタログに変更することはできません。

マシンプロファイルを使用してマシンカタログを作成する

マシンプロファイルを使用してマシンカタログを作成するには、以下の手順を実行します:

1. **PowerShell** ウィンドウを開きます。
2. asnp citrix*を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. ID プールをまだ作成していない場合は作成します。例:

```
1 New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms## -
     Domain abcdf -NamingSchemeType Numeric
2 <!--NeedCopy-->
```

4. New-ProvScheme コマンドを実行します。例:

```
1 New-ProvScheme -ProvisioningSchemeName demet-test-1
2 -HostingUnitUid aa633238-9xxd-4cf6-80e8-232a758a1xx1
3 -IdentityPoolUid 34d5b088-e312-416f-907d-16573xxxxxc4
4 -CleanOnBoot
5 -MasterImageVM 'XDHyp:\HostingUnits\cvad-test-scalestress\citrix-
     demet-ami.0 (ami-0ca813xxxxxx061ef).template'
6 -MachineProfile 'XdHyp:\HostingUnits\cvad-test-scalestress\us-east
     -1a.availabilityzone\machine-profile-instance i (i-0xxxxxxxx).
     vm'
7 <!--NeedCopy-->
```

5. カタログの作成を完了します。

マシンプロファイルの更新

マシンプロファイルを使用して最初にプロビジョニングされたカタログのマシンプロファイルを更新するには、次の手順を実行します。MCS マシンカタログを編集するときに、マシンプロファイルソースのテナントの種類と休止状態機能を変更することもできます。

1. Set-ProvSchemeコマンドを実行します。例:


```
Set-ProvScheme `
-ProvisioningSchemeUid "<ID" `
-MachineProfile "XDHyp:\HostingUnits\abc\us-east-1a.
    availabilityzone\citrix-cvad-machineprofile-instance (i-0
    xxxxxxxx).vm"
<!--NeedCopy-->
```

PowerShell と起動テンプレートのバージョンを使用してカタログを作成する

起動テンプレートのバージョンをマシンプロファイルの入力に使用して、MCS マシンカタログを作成できます。マシンプロファイルカタログの入力に関しては、仮想マシンから起動テンプレートのバージョンに更新したり、起動テンプレートのバージョンから仮想マシンに更新したりすることもできます。

AWS EC2 コンソールでは、起動テンプレートのインスタンス構成情報をバージョン番号とともに指定できます。マシンカタログの作成または更新時に起動テンプレートのバージョンをマシンプロファイルの入力に指定すると、そのバージョンの起動テンプレートのプロパティが、プロビジョニングされた VDA VM にコピーされます。

次のプロパティは、マシンプロファイル入力を使用するか、`New-ProvScheme`または`Set-ProvScheme`コマンドのパラメーターとして明示的に指定して提供できます。これらが`New-ProvScheme`または`Set-ProvScheme`コマンドで指定された場合、これらのプロパティのマシンプロファイル値よりも優先されます。

- サービスオファリング
- ネットワーク
- セキュリティグループ
- テナントの種類

> 注:
>
> サービスオファリングがマシンプロファイル起動テンプレートで、または`New-ProvScheme`コマンドのパラメーターとして提供されていない場合は、関連のエラーが発生します。

起動テンプレートのバージョンをマシンプロファイルの入力として使用してカタログを作成するには、次の手順を実行します:

1. **PowerShell** ウィンドウを開きます。
2. `asnp citrix*`を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. 起動テンプレートに関して、起動テンプレートのバージョン一覧を取得します。例:

```
XDHyp:\HostingUnits\test\test-mp-sard (lt-01xxxxx).launchtemplate>
    ls | Select FullPath
<!--NeedCopy-->
```

4. ID プールを作成していない場合は作成します。例:


```
New-AcctIdentityPool `
-IdentityPoolName "abc11" `
-NamingScheme "abc1-##" `
-NamingSchemeType Numeric `
-Domain "citrix-xxxxxx.local" `
-ZoneUid "xxxxxxxx" `
<!--NeedCopy-->
```

5. マシンプロファイルの入力として起動テンプレートのバージョンを使用してプロビジョニングスキームを作成します。例:

```
New-ProvScheme `
-ProvisioningSchemeName "MPLT1" `
-HostingUnitUid "c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `
-IdentityPoolUid "bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxx" `
-MasterImageVM "XDHyp:\HostingUnits\xxxd-ue1a\apollo-non-
   persistent-vda-win2022 (ami-0axxxxxxxxxx).template" `
-CleanOnBoot `
-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
   (lt-01xxxxx).launchtemplate\lt-01xxxxx (1).
   launchtemplateversion"
<!--NeedCopy-->
```

6. プロビジョニングスキームをブローカーカタログとして登録します。例:

```
New-BrokerCatalog -Name "MPLT1" `
-AllocationType Random `
-Description "Machine profile catalog" `
-ProvisioningSchemeId fe7df345-244e-4xxxx-xxxxxxxxx `
-ProvisioningType Mcs `
-SessionSupport MultiSession `
-PersistUserChanges Discard
<!--NeedCopy-->
```

7. カタログの作成を完了します。

マシンプロファイルのソースを更新する

マシンプロファイルカタログの入力に関しては、仮想マシンから起動テンプレートのバージョンに更新したり、起動テンプレートのバージョンから仮想マシンに更新したりすることもできます。例:

- マシンプロファイルカタログの入力を仮想マシンから起動テンプレートのバージョンに更新するには、以下を実行します:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest"
    `
-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
    (lt-0bxxxxxxxxxxxx).launchtemplate\lt-0bxxxxxxxxxxx (1).
   launchtemplateversion"
<!--NeedCopy-->
```


- マシンプロファイルカタログの入力を起動テンプレートのバージョンから仮想マシンに更新するには、以下を実行します:

```
1 Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest"
    `
2 -MachineProfile "XDHyp:\HostingUnits\sard-ue1a\us-east-1a.
    availabilityzone\apollo-non-persistent-vda-win2022-2 (i-08
    xxxxxxxxx).vm"
3 <!--NeedCopy-->
```

OS ディスクと ID ディスクを暗号化する

OS ディスクと ID ディスク（ID）の暗号化に使用できる AWS KMS キー（顧客管理キーと AWS 管理キー）を使用して、VM の永続カタログおよび非永続カタログを作成できます。

- AWS 管理キーは毎年自動的にローテーションされます。
- 顧客管理キーは自動ローテーションのオプションであり、手動で管理できます。

KMS キーの詳細については、次の AWS ドキュメントを参照してください:

- AWS KMS について
- 自動キーローテーションの仕組み

OS ディスクと ID ディスクの暗号化では、次のいずれかを構成します:

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

制限事項

次の制限事項に注意してください:

- MCS は現在、マスターイメージ AMI 上で 1 つのディスクのみをサポートしています。
- 既存の暗号化されていない EBS ボリュームまたはスナップショットを直接暗号化したり、既存の暗号化されたボリュームの KMS キーを変更したりすることはできません。このためには、以下を実行する必要があります:

  1. そのボリュームの新しいスナップショットを作成します。
  2. そのスナップショットから新しいボリュームを作成します
  3. この新しいボリュームを暗号化します。

次の AWS ドキュメントを参照してください:

- 暗号化されていないリソースの暗号化
- EBS ボリュームの自動暗号化またはデフォルトの暗号化の制限：既存および新しい Amazon EBS ボリュームを自動的に暗号化します。

ディスク暗号化でカタログを作成する

ディスク暗号化で MCS マシンカタログを作成するには、以下を使用します：

- マスターイメージ
- マシンプロファイル

マシンプロファイルの入力を使用する場合の考慮事項は次のとおりです：

- マシンプロファイルの入力の KMS キーは、マスターイメージの KMS キーよりも優先されます。
- マシンプロファイルの入力が指定されていない場合は、マスターイメージ AMI の KMS キーを使用してカタログ VM のディスクが暗号化されます。
- マシンプロファイルにブロックデバイスマッピングが存在する場合、マスターイメージテンプレート（AMI）とマシンプロファイルに存在するブロックデバイスが一致する必要があります。たとえば、AMI に`/dev/sda1`定義されたデバイスがある場合、マシンプロファイルにも`/dev/sda1`で定義されたデバイスが必要です。
- マシンプロファイルのソースにキーがなく、マスターイメージが暗号化されていない場合、カタログ VM のディスクは暗号化されません。
- マスターイメージが暗号化されている場合、有効な入力と見なされるためには、マシンプロファイルのソース VM または起動テンプレートに暗号化されたルートボリュームが必要です。

既存のカタログを変更する

既存のカタログを、次が含まれるように、`Set-ProvScheme` PowerShell コマンドを使用して変更できます：

- 新しい KMS キーを含むボリュームがあるマシンプロファイルの入力。
- 新しい KMS キーで暗号化されたマスターイメージテンプレート AMI。

重要な注意事項：

- カタログに追加された新しい VM のボリュームは、新しい KMS キーで暗号化されます。
- 既存のマシンプロファイルがある場合に暗号化設定を更新するには、新しいマシンプロファイルで`Set-ProvScheme`を実行します。
- 既存のカタログを、暗号化されたボリュームから暗号化されていないボリュームに変更することはできません。暗号化されたマスター AMI から暗号化されていないマスター AMI へのイメージ更新を実行することはできません。

VM 上のタグをコピーする

マシンプロファイルで指定されている NIC およびディスク（ID ディスク、ライトバックキャッシュディスク、OS ディスク）上のタグを、MCS マシンカタログ内に新しく作成された VM にコピーできます。これらのタグは、任意のマシンプロファイルソース（AWS VM インスタンスまたは AWS 起動テンプレートバージョン）で指定できます。この機能は、永続および非永続のマシンカタログと VM に適用できます。

> 注:
>
> - AWS EC2 コンソールでは、**Launch Template Version Resource Tags** の下に **Tag Network Interfaces** の値が表示されません。ただし、PowerShell コマンド`aws ec2 describe-launch-template-versions --launch-template-id lt-0bb652503d45dcbcd --versions 12`を実行してタグの仕様を確認することができます。
> - マシンプロファイルソース（仮想マシンまたは起動テンプレートバージョン）に 2 つのネットワークインターフェイス（eni-1 と eni-2）があり、eni-1 にタグ t1 があり、eni-2 にタグ t2 がある場合、仮想マシンは 2 つのネットワークインターフェイスのタグ両方を取得します。

PowerShell を使用して VM インスタンスをフィルタリングする

マシンプロファイル VM として使用する AWS VM インスタンスは、マシンカタログを作成して正しく機能させるために互換性が必要です。マシンプロファイルの入力 VM として使用できる AWS VM インスタンスを一覧表示するには、`Get-HypInventoryItem`コマンドを使用できます。このコマンドは、ホスティングユニットで使用可能な VM のインベントリに対して、ページネーションとフィルタリングを実行できます。

ページネーション:

Get-HypInventoryItem は、次の 2 つのページネーションモードをサポートしています:

- ページングモードでは、`-MaxRecords`および`-Skip`パラメーターを使用して項目のセットを返します:
  - `-MaxRecords`: デフォルトは **1** です。これにより、返される項目の数が制御されます。
  - `-Skip`: デフォルトは **0** です。これは、ハイパーバイザー内の一覧の絶対的な先頭（または絶対的な末尾）からスキップする項目の数を制御します。
- スクロールモードでは、`-MaxRecords`、`-ForwardDirection`、および`-ContinuationToken`パラメーターを使用してレコードをスクロールできます:
  - `-ForwardDirection`: デフォルトは **True** です。これは`-MaxRecords`とともに使用され、次の一致するレコードのセットまたは前の一致するレコードのセットを返します。
  - `-ContinuationToken`: 直後（または`ForwardDirection`が **false** の場合は直前）の項目を返しますが、`ContinuationToken`で指定された項目は含まれません。

ページネーションの例:

- 一番下にある名前を持つマシンテンプレートの単一レコードを返します。`AdditionalData`フィールドには、`TotalItemsCount`と`TotalFilteredItemsCount`が含まれます:


```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template
<!--NeedCopy-->
```

- 一番下にある名前のマシンテンプレート 10 個のレコードを返すには、以下を実行します:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -MaxRecords 10 | select Name
<!--NeedCopy-->
```

- 一番上にある名前で終わるレコードの配列を返すには、以下を実行します:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -ForwardDirection $False -MaxRecords 10
     | select Name
<!--NeedCopy-->
```

- 指定された`ContinuationToken`に関連付けられたマシンテンプレートで始まるレコードの配列を返すには、以下を実行します:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -ContinuationToken "ami-07xxxxxxxxx" -
    MaxRecords 10
<!--NeedCopy-->
```

フィルタリング:

フィルタリングでは、次の追加のオプションパラメーターがサポートされています。これらのパラメーターをページネーションオプションと組み合わせることができます。

- `-ContainsName "my_name"`:指定された文字列が AMI 名の一部と一致する場合、その AMI は`Get`結果に含まれます。例:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -MaxRecords 100 -ContainName  'apollo'
     | select Name
<!--NeedCopy-->
```

- `-Tags '{ "Key0": "Value0", "Key1": "Value1", "Key2": "Value2" } '`: AMI にこれらのタグの少なくとも 1 つがある場合、その AMI は`Get`結果に含まれます。例:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -MaxRecords 100 -Tags '{
"opex owner": "Not tagged" }
' | select Name
<!--NeedCopy-->
```


> 注:
>
> 2 つのタグ値がサポートされています。**Not Tagged** タグ値は、タグの一覧に指定されたタグが含まれていない項目と一致します。**All values** タグ値は、タグの値に関係なくタグを持つ項目と一致します。それ以外の場合、項目にタグがあり、その値がフィルターで指定されたものと等しい場合にのみ一致が発生します。

- `-Id "ami-0a2d913927e0352f3"`: AMI が指定された ID と一致する場合、その AMI は`Get`結果に含まれます。例:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -Id ami-xxxxxxxxxxxxx
<!--NeedCopy-->
```

AdditionalData パラメーターのフィルタリング:

`AdditionalData`フィルターパラメーターは、機能、サービスオファリング、または AdditionalData 内のプロパティに基づいてテンプレートまたは VM を一覧表示します。例:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -
    LiteralPath "XDHyp:\HostingUnits\aws" -MaxRecords 200).
    AdditionalData
<!--NeedCopy-->
```

`-Warn`パラメーターを追加して、互換性のない VM を示すこともできます。この VM は、**Warning** という名前の`AdditionalData`フィールドに含まれます。例:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -
    LiteralPath "XDHyp:\HostingUnits\aws" -MaxRecords 200 -Template "ami
    -015xxxxxxxxx" -Warn $true).AdditionalData
<!--NeedCopy-->
```

次の手順

- 最初のカタログを作成すると、デリバリーグループを作成する手順が表示されます。
- 構成プロセスの全体像については、「展開の計画と構築」を参照してください。
- カタログを管理するには、「マシンカタログの管理」と「AWS カタログの管理」を参照してください。

追加情報

- 接続とリソースの作成と管理
- AWS への接続
- マシンカタログの作成

Google Cloud Platform カタログの作成

May 22, 2024

「マシンカタログの作成」では、マシンカタログを作成するウィザードについて説明します。以下の情報は、Google クラウド環境に固有の詳細について説明しています。

> 注:
>
> Google Cloud Platform（GCP）カタログを作成する前に、GCP への接続の作成を完了する必要があります。「Google クラウド環境への接続」を参照してください。

マスター仮想マシンインスタンスと永続ディスクを準備する

> ヒント:
>
> 永続ディスクは、仮想ディスクを表す Google Cloud の用語です。

マスター仮想マシンインスタンスを準備するには、計画されたマシンカタログの複製された VDA インスタンスに必要な構成と一致するプロパティで仮想マシンインスタンスを作成して構成します。構成は、インスタンスのサイズとタイプのみに適用されるわけではありません。また、メタデータ、タグ、GPU 割り当て、ネットワークタグ、サービスアカウントプロパティなどのインスタンス属性も含まれます。

マスタリングプロセスの一部として、MCS はマスター VM インスタンスを使用して Google Cloud インスタンステンプレートを作成します。次に、インスタンステンプレートを使用して、マシンカタログを構成する複製された VDA インスタンスを作成します。複製されたインスタンスは、インスタンステンプレートが作成されたマスター仮想マシンインスタンスのプロパティ（VPC、サブネット、および永続ディスクのプロパティを除く）を継承します。

マスター仮想マシンインスタンスのプロパティを仕様に合わせて構成した後、インスタンスを起動し、インスタンスの永続ディスクを準備します。

ディスクのスナップショットを手動で作成することをお勧めします。これにより、意味のある命名規則を使用してバージョンを追跡でき、マスターイメージの以前のバージョンを管理するためのオプションが増え、マシンカタログの作成時間を節約できます。独自のスナップショットを作成しない場合、MCS が一時的なスナップショットを作成します（これはプロビジョニングプロセスの最後に削除されます）。

ゾーン選択の有効化

Citrix DaaS はゾーン選択をサポートしています。ゾーン選択では、VM を作成するゾーンを指定します。ゾーン選択により、管理者は選択したゾーン間に単一のテナントノードを配置できます。単一テナントを構成するには、Google Cloud で次の手順を実行する必要があります:

- Google Cloud の単一テナントノードを予約する
- VDA マスターイメージを作成する

Google Cloud の単一テナントノードを予約する

単一テナントノードを予約するには、Google Cloud のドキュメントを参照してください。

> 重要:
>
> ノードテンプレートは、ノードグループで予約されているシステムのパフォーマンス特性を示すために使用されます。これらの特性には、vGPU の数、ノードに割り当てられたメモリの量、ノード上に作成されたマシンに使用されるマシンの種類が含まれます。詳しくは、Google Cloud のドキュメントを参照してください。

VDA マスターイメージを作成する

単一テナントノードにマシンを正常に展開するには、マスター VM イメージの作成時に追加の手順を実行する必要があります。Google Cloud 上のマシンインスタンスには、ノードアフィニティラベルと呼ばれるプロパティがあります。単一テナントノードに展開されたカタログのマスターイメージとして使用されるインスタンスには、ターゲットノードグループの名前と一致するノードアフィニティラベルが必要です。これを実現するには、次の点に注意してください:

- 新しいインスタンスの場合は、インスタンスの作成時に Google Cloud コンソールでラベルを設定します。詳しくは、「インスタンスの作成時にノードアフィニティラベルを設定する」を参照してください。
- 既存のインスタンスの場合は、**gcloud** コマンドラインを使用してラベルを設定します。詳しくは、「既存のインスタンスのノードアフィニティラベルを設定する」を参照してください。

> 注:
>
> 共有 VPC で単一テナントを使用する場合は、「共有仮想プライベートクラウド」を参照してください。

インスタンスの作成時にノードアフィニティラベルを設定する　ノードアフィニティラベルを設定するには、次の手順に従います:

1. Google Cloud コンソールで、[**Compute Engine**] > [**VM instances**] に移動します。
2. [**VM instances**] ページで、[**Create instance**] を選択します。
3. [**Instance creation**] ページで、必要な情報を入力または設定し、[**management**]、[**security**]、[**disks**]、[**networking**]、[**sole tenancy**] の順に選択して設定パネルを開きます。
4. [**Sole tenancy**] タブで、[**Browse**] を選択して、現在のプロジェクトで使用可能なノードグループを表示します。[**Sole-tenant node**] ページが開き、使用可能なノードグループのリストが表示されます。
5. [**Sole-tenant node**] ページで、リストから該当するノードグループを選択し、[**Select**] を選択して [**Sole tenancy**] タブに戻ります。[node affinity labels] フィールドに、選択した情報が入力されます。この設定により、インスタンスから作成されたマシンカタログが、選択したノードグループに展開されます。
6. [**Create**] を選択してインスタンスを作成します。

既存のインスタンスのノードアフィニティラベルを設定する　ノードアフィニティラベルを設定するには、次の手順に従います:

1. Google Cloud Shell 端末ウィンドウで、*gcloud compute instances* コマンドを使用してノードアフィニティラベルを設定します。**gcloud** コマンドに次の情報を含めます:

   - 仮想マシンの名前。たとえば、「s*2019-vda-base」という名前の既存の VM を使用します。*
   - ノードグループの名前。以前に作成したノードグループ名を使用します。例: mh-sole-tenant-node-group-1。
   - インスタンスが存在するゾーン。たとえば、仮想マシンは*us-east-1b* zoneにあります。

   たとえば、端末ウィンドウで次のコマンドを入力します:

   - `gcloud compute instances set-scheduling "s2019-vda-base"--node-group="mh-sole-tenant-node-group-1"--zone="us-east1-b"`

   gcloud compute instances コマンドについて詳しくは、Google デベロッパーツールのドキュメント（https://cloud.google.com/sdk/gcloud/reference/beta/compute/instances/set-scheduling）を参照してください。

2. インスタンスの［**VM instance details**］ページに移動し、［**Node Affinities**］フィールドにラベルが入力されていることを確認します。

マシンカタログの作成

> 注:
>
> マシンカタログを作成する前にリソースを作成してください。マシンカタログを構成するときは、Google Cloud で定められた命名規則を使用します。詳しくは、「バケットとオブジェクトの命名ガイドライン」を参照してください。

マシンカタログは次の 2 つの方法で作成できます。

- 完全な構成インターフェイス
- PowerShell。「Manage Citrix DaaS using Remote PowerShell SDKs」を参照してください。PowerShell を使用して特定の機能を実装する方法については、「PowerShell の使用」を参照してください

完全な構成インターフェイスを使用してマシンカタログを作成する

「マシンカタログの作成」のガイダンスに従ってください。次の説明は、Google Cloud のカタログに固有の説明です。

1. ［管理］**>**［完全な構成］の左側ペインで ［マシンカタログ］を選択します。
2. 操作バーで ［マシンカタログの作成］を選択します。

3. ［マシンの種類］ページで、［マルチセッション **OS**］を選択し、［次へ］を選択します。Citrix DaaS は、シングルセッション OS もサポートしています。
4. ［マシン管理］ページで、［電源管理されているマシン］および ［**Citrix Machine Creation Services**］オプションを選択してから ［次へ］を選択します。複数のリソースがある場合は、メニューから 1 つ選択してください。
5. ［イメージ］ページで、必要に応じて次の手順を実行し、［次へ］をクリックします。

   a) スナップショットまたは VM をマスターイメージとして選択します。単一テナント機能を使用する場合は、必ずノードグループプロパティが正しく構成されているイメージを選択してください。「ゾーン選択の有効化」を参照してください。

   b) 既存の VM をマシンプロファイルとして使用するには、［マシンプロファイルを使用する］を選択し、VM を選択します。

   > 注:
   >
   > 現在、このカタログ内の VM は、ディスク暗号化セット ID、マシンサイズ、ストレージの種類、およびゾーン設定をマシンプロファイルから継承します。

   c) カタログの最小機能レベルを選択します。
6. ［ストレージ］ページで、このマシンカタログのオペレーティングシステムを格納するために使用するストレージの種類を選択します。次のストレージオプションにはそれぞれ、固有の価格とパフォーマンスの特性があります ID ディスクは、常にゾーン標準永続ディスクを使用して作成されます。

   - 標準永続ディスク
   - バランス永続ディスク
   - SSD 永続ディスク

   Google Cloud ストレージオプションについて詳しくは、「ストレージオプション」を参照してください。
7. ［仮想マシン］ページで、作成する VM の数を指定し、VM の詳細な仕様を表示してから、マシンの種類で Google Cloud を選択し、［次へ］を選択します。マシンカタログに単一テナントノードグループを使用する場合は、予約済み単一テナントノードが使用可能なゾーンのみを選択するようにしてください。「ゾーン選択の有効化」を参照してください。
8. ［ディスク設定］ページで、次の設定を構成できます:

   - ライトバックキャッシュを有効にするかどうかを選択します。ライトバックキャッシュを有効にした後、次の操作を実行できます:
     - 一時データのキャッシュに使用するディスクと RAM のサイズを構成する。詳しくは、「一時データ用キャッシュの構成」を参照してください。
     - ライトバックキャッシュディスク用のストレージの種類を選択します。ライトバックキャッシュディスクには、次のストレージのオプションを使用できます:

    * 標準永続ディスク
    * バランス永続ディスク
    * SSD 永続ディスク

    Google Cloud ストレージオプションについて詳しくは、「ストレージオプション」を参照してください。

  - ライトバックキャッシュディスクの種類を選択します。

    * 非永続的なライトバックキャッシュディスクを使用する。選択した場合、ライトバックキャッシュディスクは、プロビジョニングされた VM で保持されません。電源を入れ直すとディスクが削除され、ディスクにリダイレクトされたデータはすべて失われます。
    * 永続的なライトバックキャッシュディスクを使用する。選択した場合、ライトバックキャッシュディスクは、プロビジョニングされた VM で保持されます。このオプションを有効にすると、ストレージコストが増加します。

- MCS ストレージ最適化（MCS I/O）が有効になっている場合、電源サイクル中に VDA 用のシステムディスクを保持するかどうかを選択できます。詳しくは、「MCS ストレージ最適化の更新を有効にする」を参照してください。
- ディスクの内容を保護するために独自のキーを使用するかどうかを選択します。この機能を使用するには、最初に独自の顧客管理暗号キー（CMEK：Customer Managed Encryption Keys）を作成する必要があります。詳しくは、「顧客管理暗号キー（CMEK）の使用」を参照してください。

  > 注：
  >
  > これは ［管理］ > ［完全な構成］ インターフェイスでのみ使用できます。

  キーを作成したら、一覧からこれらのキーの 1 つを選択できます。カタログの作成後にキーを変更することはできません。Google Cloud では、既存の永続ディスクまたはイメージでのキーの交換をサポートしていません。そのため、カタログをプロビジョニングした後、カタログは特定のバージョンのキーに関連付けられます。そのキーが無効化または破棄された場合、そのキーで暗号化されたインスタンスとディスクは、そのキーが再度有効化または復元されるまで使用できなくなります。

9. ［マシン **ID**］ページで、Active Directory アカウントを選択してから ［次へ］ を選択します。

   - ［新しい **Active Directory** アカウントを作成する］ を選択する場合、ドメインを選択してから Active Directory で作成されたプロビジョニング済みの VM コンピューターアカウントで名前付けスキームに対応した文字列を入力します。アカウント名前付けスキームに指定できる文字数は 1～64 文字であり、空白スペース、非 ASCII 文字、および特殊文字を含めることはできません。
   - ［既存の **Active Directory** アカウントを使用する］ を選択した場合、［参照］ を選択し、選択したマシンの既存の Active Directory コンピューターアカウントに移動します。

10. ［ドメイン資格情報］ ページで、［資格情報の入力］ を選択し、ユーザー名とパスワードを入力し、［保存］ を選択してから ［次へ］ を選択します。

- 入力する資格情報には、Active Directory アカウント操作を実行する権限が必要です。

11. ［スコープ］ページで、マシンカタログのスコープを選択してから、［次へ］を選択します。

    - オプションのスコープを選択するか、必要に応じてスコープをカスタマイズするためのカスタムスコープを選択できます。

12. ［概要］ページで、情報を確認し、カタログの名前を指定してから、［完了］を選択します。

    > 注:
    >
    > カタログ名は 1～39 文字にし、空白スペースのみにしたり記号（`\ / ; : # . * ? = < > | [ ] { } "' ( )' )`）を含めたりすることはできません。

マシンカタログの作成が完了するまでに時間がかかる場合があります。完了すると、カタログが一覧表示されます。Google Cloud コンソールで、ターゲットノードグループにマシンが作成されていることを確認できます。

手動で作成した **Google Cloud** マシンのインポート

この機能を使用することで、以下のことを実行できます:

- 手動で作成した Google Cloud マルチセッション OS マシンを Citrix DaaS カタログにインポートする。
- 手動で作成した Google Cloud マルチセッション OS マシンを Citrix DaaS カタログから削除する。
- 既存の Citrix DaaS の電源管理機能を使用して、Google Cloud Windows マルチセッション OS マシンの電源管理を行います。たとえば、これらのマシンの再起動スケジュールを設定します。

この機能を使用するのに、Citrix DaaS の既存のプロビジョニングワークフローの変更や、既存機能の削除を行う必要はありません。

手動で作成された Google Cloud マシンをインポートする代わりに、MCS を使用して Citrix DaaS の完全な構成インターフェイスでマシンをプロビジョニングすることをお勧めします。

共有仮想プライベートクラウド

共有仮想プライベートクラウド（VPC）は、共有サブネットが使用可能なホストプロジェクトと、リソースを使用する 1 つ以上のサービスプロジェクトで構成されます。共有 VPC は、企業の共有 Google Cloud リソースの制御、使用、管理を一元的に行うため、大規模なインストールでは望ましいオプションです。詳しくは、Google のドキュメントのサイトを参照してください。

この機能により、Machine Creation Services（MCS）は、共有 VPC に展開されたマシンカタログのプロビジョニングと管理をサポートします。このサポートは、現在ローカル VPC で提供されているサポートと同等の機能ですが、次の 2 つの点が異なります:

- ホスト接続の作成に使用するサービスアカウントに追加の権限を付与する必要があります。このプロセスにより、MCS は共有 VPC リソースにアクセスして使用できるようになります。「新しい権限が必要」を参照してください。
- 受信用と送信用の 2 つのファイアウォール規則を作成する必要があります。これらのファイアウォール規則は、イメージのマスタリングプロセスで使用されます。「ファイアウォール規則」を参照してください。

共有 VPC の構成については、「共有 VPC の構成」を参照してください。

新しい権限が必要

ホスト接続を作成するときは、特定の権限を持つ Google Cloud サービスアカウントが必要です。これらの追加の権限は、VPC ベースのホスト接続を作成するために使用されるすべてのサービスアカウントに付与する必要があります。

> ヒント:
>
> これらの追加のアクセス権限は、Citrix DaaS にとって新しいものではありません。これらは、ローカル VPC の実装を容易にするために使用されます。共有 VPC の場合、これらの追加権限により、共有 VPC リソースへのアクセスが許可されます。

共有 VPC をサポートするには、ホスト接続に関連付けられたサービスアカウントに追加の権限を最大 4 つ付与する必要があります:

- **compute.firewalls.list** - この権限は必須です。これにより、MCS は共有 VPC に存在するファイアウォール規則のリストを取得できます。
- **compute.networks.list** - この権限は必須です。これにより、MCS がサービスアカウントで使用可能な共有 VPC ネットワークを識別できます。
- **compute.subnetworks.list** –この権限は、VPC の使用方法に応じてオプションとなります。これにより、MCS は可視の共有 VPC 内のサブネットを識別できます。この権限は、ローカル VPC を使用する場合は既に必須ですが、共有 VPC ホストプロジェクトでも割り当てる必要があります。
- **compute.subnetworks.use** - この権限は、VPC の使用方法に応じてオプションとなります。プロビジョニングされたマシンカタログでは、サブネットリソースを使用する必要があります。この権限は、ローカル VPC を使用する場合は既に必須ですが、共有 VPC ホストプロジェクトでも割り当てる必要があります。

これらの権限を使用する場合は、マシンカタログの作成に使用する権限の種類によって方法が異なることを考慮してください:

- プロジェクトレベルの権限:
  - ホストプロジェクト内のすべての共有 VPC へのアクセスを許可します。
  - 権限`compute.subnetworks.list`と`compute.subnetworks.use`をサービスアカウントに割り当てる必要があります。
- サブネットレベルの権限:

- 共有 VPC 内の特定のサブネットへのアクセスを許可します。
- 権限`compute.subnetworks.list`と`compute.subnetworks.use`は、サブネットレベルの割り当てに組み込まれているため、サービスアカウントに直接割り当てる必要はありません。

組織のニーズとセキュリティ基準に合ったアプローチを選択します。

> ヒント:
>
> プロジェクトレベルとサブネットレベルの権限の違いについて詳しくは、「サービスプロジェクト管理者」を参照してください。

ファイアウォール規則

マシンカタログの準備中に、カタログのマスターイメージシステムディスクとして機能するマシンイメージが準備されます。このプロセスが発生すると、ディスクは一時的に仮想マシンに接続されます。この VM は、すべての受信および送信ネットワークトラフィックが禁止された、分離された環境で実行する必要があります。これは、2 つの deny-all ファイアウォール規則によって実現されます: 1 つは受信トラフィック用で、もう 1 つは送信トラフィック用です。Google Cloud ローカル VCP を使用する場合、MCS はこのファイアウォールをローカルネットワーク上に作成し、マスタリングのためにマシンに適用します。マスタリングが完了すると、ファイアウォール規則がイメージから削除されます。

Shared VPC を使用するために必要な新しい権限の数は最小限に抑えることを推奨します。共有 VPC は、より高レベルの企業リソースであり、通常はより厳格なセキュリティプロトコルを採用しています。このため、共有 VPC リソース上のホストプロジェクトに 2 つのファイアウォール規則を作成します。1 つは受信用、もう 1 つは送信用です。それらに最も高い優先度を割り当てます。次の値を使用して、これらの各規則に新しいターゲットタグを適用します:

```
citrix-provisioning-quarantine-firewall
```

MCS は、マシンカタログを作成または更新するときに、このターゲットタグを含むファイアウォール規則を検索します。次に、規則が正しいかを調べ、カタログのマスターイメージの準備で使用されたマシンにそれを適用します。ファイアウォール規則が見つからない場合、または規則は見つかったが規則やその優先度が正しくない場合には、次のようなメッセージが表示されます:

```
"Unable to find valid INGRESS and EGRESS quarantine firewall rules
for VPC <name> in project <project>. "Please ensure you have created
 'deny all'firewall rules with the network tag  ‘citrix-provisioning-
quarantine-firewall'and proper priority." "Refer to Citrix Documentation
 for details."
```

共有 **VPC** の構成

Citrix DaaS の完全な構成インターフェイスで共有 VPC をホスト接続として追加する前に、次の手順を実行して、プロビジョニングするプロジェクトのサービスアカウントを追加します:

1. IAM 役割を作成します。
2. ホストプロジェクトの IAM 役割にサービスアカウントを追加する。
3. Cloud Build サービスアカウントを共有 VPC に追加する。
4. ファイアウォール規則を作成します。

IAM 役割を作成する　役割のアクセスレベルを決定します:

- プロジェクトレベルのアクセス、または
- サブネットレベルのアクセスを使用する、より制限されたモデル。

IAM 役割のプロジェクトレベルのアクセス。プロジェクトレベルの IAM 役割には、次の権限を含めます:

- compute.firewalls.list
- compute.networks.list
- compute.subnetworks.list
- compute.subnetworks.use

プロジェクトレベルの IAM 役割を作成するには、次の手順を実行します:

1. Google Cloud コンソールで、[**IAM & admin**] **>** [**Roles**] の順に選択します。
2. [**Roles**] ページで、[**CREATE ROLE**] を選択します。
3. [**Create Role**] ページで、役割名を指定します。[**ADD PERMISSIONS**] を選択します。

    a) [**Add permissions**] ページで、役割に権限を個別に追加します。権限を追加するには、[**Filter table**] フィールドで権限の名前を入力します。権限を選択し、[**ADD**] を選択します。
    b) [**CREATE**] を選択します。

サブネットレベルの **IAM** 役割。この役割では、[**CREATE ROLE**] を選択した後、権限`compute.subnetworks.list`と`compute.subnetworks.use`の追加が省略されます。この IAM アクセスレベルでは、新しい役割に権限`compute.firewalls.list`と`compute.networks.list`を適用する必要があります。

サブネットレベルの IAM 役割を作成するには、次の手順を実行します:

1. Google Cloud コンソールで、[**VPC network**] > [**Shared VPC**] に移動します。[**Shared VPC**] ページが開き、ホストプロジェクトに含まれる共有 VPC ネットワークのサブネットが表示されます。
2. [**Shared VPC**] ページで、アクセスするサブネットを選択します。
3. 右上隅にある [**ADD MEMBER**] を選択して、サービスアカウントを追加します。
4. [**Add members**] ページで、次の手順を実行します:

    a) [**New members**] フィールドにサービスアカウントの名前を入力し、メニューでサービスアカウントを選択します。
    b) [**Select a role**] フィールドを選択し、[**Compute Network User**] を選択します。
    c) [**SAVE**] を選択します。

5. Google Cloud コンソールで、[**IAM & admin**] > [**Roles**] の順に選択します。

6. [**Roles**] ページで、[**CREATE ROLE**] を選択します。
7. [**Create Role**] ページで、役割名を指定します。[**ADD PERMISSIONS**] を選択します。

    a) [**Add permissions**] ページで、役割に権限を個別に追加します。権限を追加するには、[**Filter table**] フィールドで権限の名前を入力します。権限を選択し、[**ADD**] を選択します。
    b) [**CREATE**] を選択します。

ホストプロジェクトの **IAM** 役割にサービスアカウントを追加する　IAM 役割を作成した後、次の手順を実行して、ホストプロジェクトのサービスアカウントを追加します:

1. Google Cloud コンソールでホストプロジェクトに移動し、[**IAM & admin**] **>** [**IAM**] の順に選択します。
2. [**IAM**] ページで、[**ADD**] を選択してサービスアカウントを追加します。
3. [**Add members**] ページで、次の操作を行います:

    a) [**New members**] フィールドにサービスアカウントの名前を入力し、メニューでサービスアカウントを選択します。
    b) 役割のフィールドを選択し、作成した IAM 役割を入力して、メニューでその役割を選択します。
    c) [**SAVE**] を選択します。

これで、ホストプロジェクト用のサービスアカウントが構成されました。

Cloud Build サービスアカウントを共有 **VPC** に追加する　すべての Google Cloud サブスクリプションは、プロジェクト ID 番号の後にサービスアカウントが指定され、その後に`cloudbuild.gserviceaccount`が続きます。例: `705794712345@cloudbuild.gserviceaccount`。

プロジェクトのプロジェクト ID 番号を確認するには、Google Cloud コンソールで [クラウドの概要] **>** [ダッシュボード] を選択します。プロジェクト ID とプロジェクト番号が、プロジェクトのダッシュボードの [Project Info] カードに表示されます:

Cloud Build サービスアカウントを共有 VPC に追加するには、次の手順を実行します:

1. Google Cloud コンソールでホストプロジェクトに移動し、[**IAM & admin**] > [**IAM**] の順に選択します。
2. [**Permissions**] ページで、[**ADD**] を選択してアカウントを追加します。
3. [**Add members**] ページで、次の手順を実行します:

    a) [**New members**] フィールドに Cloud Build サービスアカウントの名前を入力し、メニューでサービスアカウントを選択します。
    b) [**Select a role**] フィールドを選択し、`Computer Network User`を入力して、メニューで役割を選択します。
    c) [**SAVE**] を選択します。

ファイアウォール規則の作成　マスタリングプロセスの一部として、MCS は選択されたマシンイメージをコピーし、それを使用してカタログ用のマスターイメージシステムディスクを準備します。マスタリングでは、MCS がディスク

を一次仮想マシンに接続し、そこで準備スクリプトが実行されます。この VM は、すべての受信および送信ネットワークトラフィックが禁止された、分離された環境で実行する必要があります。

分離された環境を作成するには、MCS に 2 つの *deny all* ファイアウォール規則（受信規則と送信規則）が必要です。したがって、ホストプロジェクトに次のように 2 つのファイアウォール規則（受信規則と送信規則）を作成します：

1. Google Cloud コンソールでホストプロジェクトに移動し、［**VPC network**］**>**［**Firewall**］の順に選択します。
2. ［**Firewall**］ページで、［**CREATE FIREWALL RULE**］を選択します。
3. ［**Create a firewall rule**］ページで、次の操作を行います：
    - 名前。規則名を入力します。
    - **Network**：受信ファイアウォール規則を適用する共有 VPC ネットワークを選択します。
    - **Priority**：値が小さいほど、規則の優先度は高くなります。小さい値（10 など）を指定することをお勧めします。
    - **Direction of traffic**：［**Ingress**］を選択します。
    - **Action on match**：［**Deny**］を選択します。
    - **Targets**：デフォルトの ［**Specified target tags**］を使用します。
    - **Target tags**：「`citrix-provisioning-quarantine-firewall`」と入力します。
    - **Source filter**：デフォルトの ［**IP ranges**］を使用します。
    - **Source IP ranges**：すべてのトラフィックに一致する範囲を入力します。「`0.0.0.0/0`」と入力します。
    - **Protocols and ports**：［**Deny all**］を選択します。
4. ［**CREATE**］を選択して規則を作成します。
5. さらに規則を作成するには、上記の手順を繰り返します。［**Direction of traffic**］で、［**Egress**］を選択します。

顧客管理暗号キー（**CMEK**）の使用

MCS カタログでは、顧客管理暗号キー（CMEK：Customer Managed Encryption Keys）を使用できます。この機能を使用する場合は、Google Cloud キー管理サービスの`CryptoKey Encrypter/Decrypter`役割を Compute Engine サービスエージェントに割り当てます。Citrix DaaS アカウントには、キーが保存されているプロジェクトで正しい権限が必要です。「Citrix DaaS アカウントへのアクセス権限の割り当て」を参照してください。詳しくは、「Cloud KMS 鍵を使用してリソースを保護する」を参照してください。

Compute Engine サービスエージェントの形式は次のとおりです：`service-<Project _Number>@compute-system.iam.gserviceaccount.com`。この形式は、デフォルトの Compute Engine サービスアカウントとは異なります。

> 注：
>
> この Compute Engine サービスアカウントは、Google コンソールの ［**IAM Permissions**］画面に表示さ

> れないことがあります。このような場合は、「Cloud KMS 鍵を使用してリソースを保護する」で説明されているgcloudコマンドを使用します。

Citrix DaaS アカウントへのアクセス権限の割り当て

Google Cloud KMS の権限はさまざまな方法で設定できます。プロジェクトレベルの KMS 権限、またはリソースレベルの KMS 権限のいずれかを指定できます。詳しくは、「権限と役割」を参照してください。

プロジェクトレベルの **KMS** 権限　1 つのオプションは、Citrix DaaS アカウントに Cloud KMS リソースを参照するためのプロジェクトレベルの権限を提供することです。これを行うには、カスタム役割を作成し、次の権限を追加します:

- `cloudkms.keyRings.list`
- `cloudkms.keyRings.get`
- `cloudkms.cryptokeys.list`
- `cloudkms.cryptokeys.get`

Citrix DaaS アカウントにこのカスタム役割を割り当てます。これにより、インベントリ内の関連プロジェクトの地域キーを参照できます。

リソースレベルの **KMS** 権限　もう 1 つのオプションであるリソースレベルの権限の場合、Google Cloud コンソールで、MCS プロビジョニングに使用する`cryptoKey`を参照します。Citrix DaaS アカウントを、カタログプロビジョニングに使用するキーリングまたはキーに追加します。

> ヒント:
>
> このオプションを使用すると、Citrix DaaS アカウントに Cloud KMS リソースに対するプロジェクトレベルのリスト権限がないため、インベントリ内のプロジェクトの地域キーを参照できません。ただし、`ProvScheme`カスタムプロパティで正しい`cryptoKeyId`を指定することにより、CMEK を使用してカタログをプロビジョニングできます。「カスタムプロパティと CMEK を使用してカタログを作成する」を参照してください。

顧客管理キーの交換

Google Cloud では、既存の永続ディスクまたはイメージでのキーの交換をサポートしていません。マシンがプロビジョニングされると、作成時に使用されていたバージョンのキーに関連付けられます。ただし、新しいバージョンのキーを作成することはでき、その新しいキーは、カタログが新しいマスターイメージで更新されたときに作成される、新しくプロビジョニングされたマシンまたはリソースに使用されます。

キーリングに関する重要な注意事項　キーリングの名前を変更したり、削除したりすることはできません。また、構成時に予期しない料金が発生する場合があります。キーリングを削除すると、Google Cloud は次のエラーメッセージを表示します:

```
Sorry, you can't delete or rename keys or key rings. We were concerned about the security implications of allowing multiple keys or key versions over time to have the same resource name, so we decided to make names immutable. (And you can't delete them, because we wouldn't be able to do a true deletion--there would still have to be a tombstone tracking that this name had been used and couldn't be reused).
We're aware that this can make things untidy, but we have no immediate plans to change this.
If you want to avoid getting billed for a key or otherwise make it unavailable, you can do so by deleting all the key versions; neither keys nor key rings are billed for, just the active key versions within the keys.
<!--NeedCopy-->
```

> ヒント:
>
> 詳しくは、「Editing or deleting a key ring from the console」を参照してください。

均一なバケットレベルのアクセスの互換性

Citrix DaaS は、Google Cloud の均一なバケットレベルのアクセス制御ポリシーと互換性があります。この機能は、サービスアカウントにアクセス許可を付与して、ストレージバケットなどのリソースの操作を許可する IAM ポリシーの使用を強化します。均一なバケットレベルのアクセス制御により、Citrix DaaS では、アクセス制御リスト（ACL）を使用して、ストレージバケットまたはそれらに格納されているオブジェクトへのアクセスを制御できます。Google Cloud の均一なバケットレベルのアクセスに関する概要情報については、「均一なバケットレベルのアクセス」を参照してください。構成情報については、「均一なバケットレベルのアクセス」を参照してください。

PowerShell の使用

このセクションでは、PowerShell を使用して次のタスクを実行する方法について説明します:

- 永続的なライトバックキャッシュディスクのカタログを作成する
- MCSIO による起動パフォーマンスの向上
- カスタムプロパティと CMEK を使用してカタログを作成する
- マシンプロファイルを使用してマシンカタログを作成する
- インスタンステンプレートとしてマシンプロファイルを使用してマシンカタログを作成する
- シールドされた VM でカタログを作成する
- 単一テナントノードに Windows 11 VM を作成する

永続的なライトバックキャッシュディスクのカタログを作成する

永続的なライトバックキャッシュディスクのカタログを構成するには、PowerShell コマンド`New-ProvScheme CustomProperties`を使用します。

> ヒント:
>
> PowerShell パラメーター`New-ProvScheme CustomProperties`は、クラウドベースのホスティング接続にのみ使用してください。オンプレミスソリューション（XenServer など）で永続的なライトバックキャッシュディスクを使用してマシンをプロビジョニングする場合、ディスクは自動的に永続化されるため、PowerShell は必要ありません。

このコマンドでは追加プロパティ`PersistWBC`をサポートしており、これを使用することで、MCS でプロビジョニングされたマシンのライトバックキャッシュディスクを永続化させる方法を指定できます。`PersistWBC`プロパティは、`UseWriteBackCache`パラメーターが指定され、`WriteBackCacheDiskSize`パラメーターがディスクが作成されたことを示すよう設定された場合のみ使用されます。

> 注:
>
> この動作は、電源を入れ直したときにデフォルトの MCSIO ライトバックキャッシュディスクが削除されて再作成される Azure および GCP の両方に適用されます。ディスクを永続化すると、MCSIO ライトバックキャッシュディスクの削除と再作成を回避できます。

以下は、`PersistWBC`をサポートする前に`CustomProperties`パラメーターで使用されるプロパティの例です:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
   benvaldev5RG3" />
</CustomProperties>
<!--NeedCopy-->
```

> 注:
>
> この例は Azure にのみ適用されます。このプロパティは GCP 環境では異なります。

これらのプロパティを使用するときは、プロパティが`CustomProperties`パラメーターから省略されている場合にデフォルトの値が含まれるようにしてください。`PersistWBC`プロパティには、次の 2 つの値が設定可能です：**true** または **false**。

`PersistWBC`プロパティを **true** に設定すると、Citrix DaaS 管理者が管理インターフェイスでマシンをシャットダウンしたときに、ライトバックキャッシュディスクが消去されなくなります。

PersistWBCプロパティを **false** に設定すると、Citrix DaaS 管理者が管理インターフェイスでマシンをシャットダウンしたときに、ライトバックキャッシュディスクが消去されます。

> 注:
>
> PersistWBCプロパティを省略する場合、デフォルトは **false** になり、管理インターフェイスでマシンをシャットダウンするとライトバックキャッシュは消去されます。

例: CustomPropertiesパラメーターを使用してPersistWBCを true に設定した場合:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
   benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />
</CustomProperties>
<!--NeedCopy-->
```

> 重要:
>
> PersistWBCプロパティは、New-ProvScheme PowerShell コマンドレットを使用してのみ設定できます。作成後にプロビジョニングスキームのCustomPropertiesを変更しようとしても、マシンがシャットダウンしたときにマシンカタログやライトバックキャッシュディスクの永続性は影響を受けません。

例: PersistWBCプロパティを true に設定するときにNew-ProvSchemeを設定してライトバックキャッシュを使用した場合:

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
   /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
   XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
   UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
   StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
   /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
   Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
   =`"PersistWBC`" Value=`"true`" /></CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
   GoldImages.resourcegroup\W10MCSIO-01
   _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
    CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
    adSubnetScale1.network" }
```



```
9
10 -ProvisioningSchemeName "BV-WBC1-CAT1"
11 -ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
      folder\Standard_D2s_v3.serviceoffering"
12 -UseWriteBackCache
13 -WriteBackCacheDiskSize 127
14 -WriteBackCacheMemorySize 256
15 <!--NeedCopy-->
```

MCSIO による起動パフォーマンスの向上

MCSIO が有効な場合、Azure や GCP の管理対象ディスクの起動パフォーマンスを向上させることができます。New-ProvSchemeコマンドで PowerShell カスタムプロパティPersistOSDiskを使用してこの機能を構成します。New-ProvSchemeに関連するオプションは次のとおりです:

```
1 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
      />
3 <Property xsi:type="StringProperty" Name="StorageAccountType" Value="
     Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="Resource<!--NeedCopy-->
5 ``````<!--NeedCopy-->
6 ````````Groups" Value="benvaldev5RG3" />
7 <Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
     />
8 </CustomProperties>
9 <!--NeedCopy-->
```

この機能を有効にするには、カスタムプロパティPersistOSDiskを **true** に設定します。例:

```
1 New-ProvScheme
2 -CleanOnBoot
3 -CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
     /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
     XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
     UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
     StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
     /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
     Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
     =`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"
4 -HostingUnitName "adSubnetScale1"
5 -IdentityPoolName "BV-WBC1-CAT1"
6 -MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
     GoldImages.resourcegroup\W10MCSIO-01
     _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
7 -NetworkMapping @{
8  "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
      CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
      adSubnetScale1.network" }
```



```
9
10 -ProvisioningSchemeName "BV-WBC1-CAT1"
11 -ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
      folder\Standard_D2s_v3.serviceoffering"
12 -UseWriteBackCache
13 -WriteBackCacheDiskSize 127
14 -WriteBackCacheMemorySize 256
15 <!--NeedCopy-->
```

カスタムプロパティと **CMEK** を使用してカタログを作成する

PowerShell でプロビジョニングスキームを作成するときは、ProvScheme CustomPropertiesでCryptoKeyIdプロパティを指定します。例:

```
1 '<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance">
2     <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="<
        yourCryptoKeyId>" />
3 </CustomProperties>'
4 <!--NeedCopy-->
```

cryptoKeyIdは次の形式で指定する必要があります:

projectId:location:keyRingName:cryptoKeyName

たとえば、リージョンus-east1にあるキーリングmy-example-key-ringのキーmy-example-keyと、ID がmy-example-project-1のプロジェクトを使用する場合、ProvSchemeカスタム設定は次のようになります:

```
1 '<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance">
2     <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-
        example-project-1:us-east1:my-example-key-ring:my-example-key"
        />
3 </CustomProperties>'
4 <!--NeedCopy-->
```

このプロビジョニングスキームに関連するすべての MCS プロビジョニングされたディスクとイメージは、このCMEK（顧客管理暗号キー）を使用します。

> ヒント:
>
> グローバルキーを使用する場合、顧客プロパティの場所はリージョン名ではなくglobalである必要があります。上記の例では、**us-east1** です。例: <Property xsi:type="StringProperty"Name="CryptoKeyId"Value="my-example-project-1:global:my-example-key-ring:my-example-key"/>。

マシンプロファイルを使用してマシンカタログを作成する

Machine Creation Services（MCS）を使用してマシンをプロビジョニングするためのカタログを作成する場合、マシンプロファイルを使用して、仮想マシンからハードウェアプロパティをキャプチャし、カタログで新しくプロビジョニングされた VM に適用できます。`MachineProfile`パラメーターが使用されていない場合、ハードウェアプロパティはマスターイメージ VM またはスナップショットからキャプチャされます。
明示的に定義する一部のプロパティ（`StorageType`、`CatalogZones`、`CryptoKeyId`など）は、マシンプロファイルから無視されます。

- マシンプロファイルを含むカタログを作成するには、`New-ProvScheme`コマンドを使用します。例: `New-ProvScheme -MachineProfile "path to VM"`。`MachineProfile`パラメーターを指定しない場合、ハードウェアプロパティはマスターイメージ VM からキャプチャされます。
- 新しいマシンプロファイルでカタログを更新するには、`Set-ProvScheme`コマンドを使用します。例: `Set-ProvScheme -MachineProfile "path to new VM"`。このコマンドは、カタログ内の既存 VM のマシンプロファイルを変更しません。新しいマシンプロファイルは、カタログに追加された新しく作成された VM のみにあります。
- マスターイメージを更新することもできますが、マスターイメージを更新しても、ハードウェアプロパティは更新されません。ハードウェアプロパティを更新する場合は、`Set-ProvScheme`コマンドを使用してマシンプロファイルを更新する必要があります。これらの変更は、カタログ内の新しいマシンにのみ適用されます。既存マシンのハードウェアプロパティを更新する場合、`-StartsNow`および`-DurationInMinutes -1`パラメーターを指定した`Set-ProvVMUpdateTimeWindow`コマンドを使用できます。

  > 注:
  >
  > - `StartsNow`は、スケジュールの開始時刻が現在時刻であることを指定します。
  > - 負の数（-1 など）の`DurationInMinutes`は、スケジュールの期間に上限がないことを示します。

インスタンステンプレートとしてマシンプロファイルを使用してマシンカタログを作成する

マシンプロファイルの入力として GCP インスタンステンプレートを選択できます。インスタンステンプレートは GCP のライトウェイトリソースであるため、費用対効果が非常に高くなります。

インスタンステンプレートとしてマシンプロファイルを使用して新しいマシンカタログを作成する

1. PowerShell ウィンドウを開きます。
2. `asnp citrix*`を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. 次のコマンドを使用して、GCP プロジェクトでインスタンステンプレートを見つけます:


```
cd XDHyp:\HostingUnits<HostingUnitName>\instanceTemplates.folder
<!--NeedCopy-->
```

4. NewProvScheme コマンドを使用して、インスタンステンプレートとしてマシンプロファイルを使用して新しいマシンカタログを作成します:

```
New-ProvScheme -ProvisioningSchemeName <CatalogName>  -
    HostingUnitName <HostingUnitName> -IdentityPoolName <identity
    pool name> -MasterImageVM
XDHyp:\HostingUnits<HostingUnitName>\Base.vm\Base.snapshot -
    MachineProfile XDHyp:\HostingUnits<HostingUnitName>\
    instanceTemplates.folder\mytemplate.template
<!--NeedCopy-->
```

New-ProvScheme コマンドについて詳しくは、「https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/New-ProvScheme/」を参照してください。

5. PowerShell コマンドを使用して、マシンカタログの作成を完了します。

マシンプロファイルとしてインスタンステンプレートを含むようにマシンカタログを更新する

1. PowerShell ウィンドウを開きます。
2. `asnp citrix*`を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. 次のコマンドを実行します:

```
Set-ProvScheme -ProvisioningSchemeName  <CatalogName> -
    MachineProfile XDHyp:\HostingUnits<HostingUnitName>\
    instanceTemplates.folder<TemplateName>.template
<!--NeedCopy-->
```

Set-ProvScheme コマンドについて詳しくは、「https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/Set-ProvScheme/」を参照してください。

シールドされた **VM** でカタログを作成する

シールドされた仮想マシンプロパティを使用して MCS マシンカタログを作成できます。シールドされた仮想マシンは、セキュアブート、仮想トラステッドプラットフォームモジュール、UEFI ファームウェア、整合性監視などの高度なプラットフォームセキュリティ機能を使用して、Compute Engine インスタンスの検証可能な整合性を提供する一連のセキュリティ制御によって強化されます。

MCS は、マシンプロファイルワークフローを使用したカタログの作成をサポートしています。マシンプロファイルワークフローを使用する場合は、仮想マシンインスタンスのシールドされた仮想マシンプロパティを有効にする必要があります。その後、この仮想マシンインスタンスをマシンプロファイルの入力で使用できます。

シールドされた **VM** で **MCS** マシンカタログを作成する

1. Google Cloud コンソールで仮想マシンインスタンスのシールドされた仮想マシンオプションを有効にします。「クイックスタート: Shielded VM オプションを有効にする」を参照してください。
2. 仮想マシンインスタンスを使用して、マシンプロファイルワークフローで MCS マシンカタログを作成します。
   a) PowerShell ウィンドウを開きます。
   b) `asnp citrix*`を実行し、Citrix 固有の PowerShell モジュールをロードします。
   c) ID プールをまだ作成していない場合は作成します。
   d) `New-ProvScheme`コマンドを実行します。例:

```
New-ProvScheme -ProvisioningSchemeName <catalog-name>
-HostingUnitName gcp-hostint-unit
-MasterImageVM XDHyp:\HostingUnits\gcp-hostint-unit\catalog-
    vda.vm
-MachineProfile XDHyp:\HostingUnits\gcp-hostint-unit\catalog-
    machine.vm
<!--NeedCopy-->
```

3. マシンカタログの作成を完了します。

新しいマシンプロファイルでマシンカタログを更新する

1. `Set-ProvScheme`コマンドを実行します。例:

```
Set-ProvScheme -ProvisioningSchemeName <catalog-name>
-MasterImageVM XDHyp:\HostingUnits<hostin-unit>\catalog-vda.vm
-MachineProfile "DHyp:\HostingUnits<hostin-unit>\catalog-machine.
    vm
<!--NeedCopy-->
```

`Set-ProvScheme`で行った変更を既存の仮想マシンに適用するには、`Set-ProvVMUpdateTimeWindow`コマンドを実行します。

1. `Set-ProvVMUpdateTimeWindow`コマンドを実行します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
    VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

2. VM を再起動します。

単一テナントノードに **Windows 11 VM** を作成する

GCP で Windows 11 VM を作成できます。ただし、マスターイメージに Windows 11 をインストールする場合は、マスターイメージの作成プロセス中に vTPM を有効にする必要があります。また、マシンプロファイルソース（VM

またはインスタンステンプレート）で vTPM を有効にする必要があります。

単一テナントノードに Windows 11 VM を作成するための主な手順は次のとおりです：

1. Google Cloud 仮想化環境をセットアップします。詳しくは、「Google Cloud 環境」を参照してください。
2. VDA のインストール。「VDA のインストール」を参照してください。
3. Google クラウド環境への接続を作成します。詳しくは、「Google クラウド環境への接続」を参照してください。
4. Windows 11 のライセンス持ち込み（BYOL）マスターイメージを作成し、そのイメージを Google Cloud にインポートします。「Windows 11 BYOL マスターイメージを作成する」を参照してください。
5. マシンプロファイルソースを作成します。単一テナントノードで VM をプロビジョニングし、ソースマシンプロファイルの vTPM を有効にします。「単一テナントノードに VM をプロビジョニングする」を参照してください。
6. vTPM が有効になっている Windows 11 マシンプロファイルソースを使用して、MCS マシンカタログを作成します。マシンプロファイルソースは、単一テナントノードで説明されているものと同じインスタンスの種類である必要があります。「Windows 11 マシンプロファイルソースを使用して MCS マシンカタログを作成する」を参照してください。

Windows 11 BYOL マスターイメージを作成する

Windows 11 BYOL マスターイメージを作成し、そのマスターイメージを Google Cloud にインポートするには、次の 2 つのオプションがあります：

- Google Cloud Cloud Build ツールを使用する
- 他のハイパーバイザー上にマスターイメージを作成する

Google Cloud Cloud Build ツールを使用する

1. Windows 11 ISO、GCP SDK、.NET フレームワーク、PowerShell インストーラーファイルを GCP ストレージバケットにアップロードします。
2. Cloud Build `.yaml`ファイル内のファイルの場所をパラメーターとして指定します。
3. 最終的な Windows 11 イメージを構築するには、コマンドラインから次の Cloud Build を実行します。GCP は、GCP の Daisy ワークフローを使用して、選択したプロジェクトでマスターイメージをブートストラップして作成し、マスターイメージを GCP にインポートします。

```
1 gcloud compute instances import INSTANCE-NAME--source-uri=gs://
    BUCKET/IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE
    --byol --machine-type=MACHINE-TYPE --zone=ZONE
2 <!--NeedCopy-->
```


> 注:
>
> すべての大文字のテキストを実際のリソースの詳細に置き換えます。

詳しくは、「カスタム Windows BYOL イメージを作成する」を参照してください。

他のハイパーバイザー上にマスターイメージを作成する

1. 他のハイパーバイザーを使用して Windows 11 マスターイメージを作成します。
2. マスターイメージを OVF 形式でローカルマシンにエクスポートします。
3. ローカル gcloud CLI を使用して、OVF ファイルを GCP ストレージバケットにアップロードします。

```
gsutil cp LOCAL_IMAGE_PATH_OVF_FILES gs://BUCKET_NAME/
<!--NeedCopy-->
```

4. 最終的な Windows 11 イメージを構築するには、コマンドラインから次の Cloud Build を実行します。GCP は、GCP の Daisy ワークフローを使用して、選択したプロジェクトでマスターイメージをブートストラップして作成し、マスターイメージを GCP にインポートします。

```
gcloud compute instances import INSTANCE-NAME --source-uri=gs://
    BUCKET/IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE
    --byol --machine-type=MACHINE-TYPE --zone=ZONE
<!--NeedCopy-->
```

> 注:
>
> すべての大文字のテキストを実際のリソースの詳細に置き換えます。

単一テナントノードに **VM** をプロビジョニングする

単一テナントノードを使用すると、VM を他のプロジェクトの VM から物理的に分離したり、同じホストハードウェア上で VM をグループ化したりできます。単一テナントノードについて詳しくは、GCP ドキュメントの「単一手ナンシーの概要」を参照してください。

単一テナントノードで VM（マシンプロファイルソース）をプロビジョニングする方法については、GCP ドキュメントの「単一テナントノードに VM をプロビジョニングする」を参照してください。

> 注:
>
> - ノードグループと同じインスタンスの種類とリージョンを選択します。
> - Shielded VM セクションで vTPM を有効にします。詳しくは、「クイックスタート: Shielded VM オプションを有効にする」を参照してください。
> - ソース VM 上の Bitlocker を無効にします。

Windows 11 マシンプロファイルソースを使用して **MCS** マシンカタログを作成する

完全な構成インターフェイスまたは PowerShell コマンドを使用して、MCS マシンカタログを作成し、Windows 11 VM を作成できます。

> 注:
>
> - マスターイメージには、Windows 11 スナップショットまたは VM を選択します。
> - マシンプロファイルソースには、マシンプロファイルとして Windows 11 VM を選択します。マシンプロファイルソースは、単一テナントノードで説明されているものと同じインスタンスの種類である必要があります。

完全な構成インターフェイスについて詳しくは、「完全な構成インターフェイスを使用してマシンカタログを作成する」を参照してください。

PowerShell コマンドについて詳しくは、「マシンプロファイルを使用してマシンカタログを作成する」を参照してください。

カタログを作成して VM の電源をオンにすると、Google Cloud コンソールの単一テナントノードで実行されている Windows 11 VM を確認できます。

Google Cloud Marketplace

Google Cloud Marketplace で Citrix 提供イメージを参照して選択することで、マシンカタログを作成できます。現在、MCS はこの機能でマシンプロファイルワークフローのみをサポートします。

Google Cloud Marketplace で Citrix VDA VM 製品を検索するには、https://console.cloud.google.com/marketplace/にアクセスしてください。

カスタムイメージ、または Google Cloud Marketplace の Citrix Ready イメージを使用して、マシンカタログのイメージを更新できます。

> 注:
>
> マシンプロファイルにストレージの種類の情報が含まれていない場合、値はカスタムプロパティから取得されます。

サポートされている Google Cloud Marketplace イメージは次のとおりです:

- Windows 2019 シングルセッション
- Windows 2019 マルチセッション
- Ubuntu

マシンカタログを作成するためのソースとして Citrix Ready イメージを使用する例:


```
New-ProvScheme -ProvisioningSchemeName GCPCatalog \
-HostingUnitName GcpHu -IdentityPoolName gcpPool -CleanOnBoot \
-MasterImageVM XDHyp:\HostingUnits\GcpHu\images.folder\citrix-daas-
   win2019-single-vda-v20220819.publicimage \
-MachineProfile XDHyp:\HostingUnits\GcpHu\Base.vm
<!--NeedCopy-->
```

次の手順

- 最初のカタログを作成すると、デリバリーグループを作成する手順が表示されます。
- 構成プロセスの全体像については、「展開の計画と構築」を参照してください。
- カタログを管理するには、「マシンカタログの管理」と「Google Cloud Platform カタログの管理」を参照してください。

追加情報

- 接続とリソースの作成と管理
- Google クラウド環境への接続
- マシンカタログの作成

HPE Moonshot マシンカタログの作成

May 17, 2024

「マシンカタログの作成」では、マシンカタログを作成するウィザードについて説明します。以下の情報は、HPE Moonshot 環境に固有の詳細について説明しています。

> 注:
>
> - HPE Moonshot への接続を作成する
> - 必ず 1 つ以上の HPE Moonshot ノードを利用可能にして、それらのノードに VDA をインストールしてください。
> - 初期の HPE Moonshot カートリッジイメージの作成については、Moonshot での OS 展開ユーザーガイドを参照してください。

以下を使用して、HPE Moonshot マシンカタログを作成できます:

- 完全な構成インターフェイス
- PowerShell コマンド

完全な構成インターフェイスを使用してマシンカタログを作成する

マシンカタログセットアップウィザードで、以下を実行します:

1. ［オペレーティングシステム］ページで、［マルチセッション **OS**］または ［シングルセッション **OS**］を選択します。
2. ［マシン管理］ページで、［電源管理されているマシン］と ［ほかのサービスまたはテクノロジ］を選択します。
3. ［仮想マシン］ページで、マシンとその Active Directory マシンアカウントを追加します。次のいずれかを実行できます:
   - ［マシンの追加］をクリックしてマシンを手動で追加します。［**VM** の選択］ウィンドウが表示されます。既に作成した HPE Moonshot シャーシ接続を展開し、追加するノード（VM）を選択します。次に、関連するマシンアカウント名を追加します。
   - ［**CSV** ファイルの追加］をクリックしてマシンを一括追加します。CSV ファイルを使用してマシンを追加する方法については、「CSV ファイルを使用してマシンをカタログに一括追加する」を参照してください。

［スコープ］ページおよび ［概要］ページには、HPE Moonshot 固有の情報は表示されません。

PowerShell コマンドを使用してマシンカタログを作成する

New-BrokerCatalogおよびNew-BrokerMachine PowerShell コマンドを実行してブローカーカタログを作成し、マシンをブローカーカタログにインポートします。

例:

```
1 New-BrokerCatalog -AllocationType "Random" -IsRemotePC $False -
    MachinesArePhysical $False -MinimumFunctionalLevel "L7_20" -Name "
    BurMC" -PersistUserChanges "OnLocal" -ProvisioningType "Manual" -
    Scope @() -SessionSupport "MultiSession" -ZoneUid "e166e2cb-25dc
    -4578-bc07-bcf2a82d1463"
2 New-BrokerMachine -CatalogUid 3 -HostedMachineId "c10n1" -
    HypervisorConnectionUid 4 -IsReserved $False -MachineName "S
    -1-5-21-2589939477-3963209805-1860259709-1121"
3 <!--NeedCopy-->
```

次の手順

- 最初のカタログを作成すると、デリバリーグループを作成する手順が表示されます。
- 構成プロセスの全体像については、「展開の計画と構築」を参照してください。
- カタログを管理するには、「マシンカタログの管理」と「HPE Moonshot カタログの管理」を参照してください。

追加情報

- 接続とリソースの作成と管理
- HPE Moonshot への接続
- マシンカタログの作成

Microsoft Azure カタログの作成

June 13, 2024

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

「マシンカタログの作成」では、マシンカタログを作成するウィザードについて説明します。以下の情報は、Microsoft Azure Resource Manager クラウド環境に固有の詳細について説明しています。

> 注:
>
> Microsoft Azure カタログを作成する前に、Microsoft Azure への接続の作成を完了する必要があります。「Microsoft Azure への接続」を参照してください。

マシンカタログの作成

マシンカタログは次の 2 つの方法で作成できます。

- ［完全な構成］インターフェイス。
- PowerShell。「Manage Citrix DaaS using Remote PowerShell SDKs」を参照してください。PowerShell を使用して特定の機能を実装する方法については、「PowerShell の使用」を参照してください。

完全な構成インターフェイスと Azure Resource Manager イメージを使用してマシンカタログを作成する

これは、「マシンカタログの作成」のガイダンスを補完する情報です。

イメージは、マシンカタログ内に VM を作成するために使用される Azure Compute Gallery 内のイメージ定義のイメージバージョンの場合もあれば、ディスクまたはスナップショットの場合もあります。

マシンカタログを作成する前に、Azure Resource Manager でイメージを作成します。

> 注:
>
> - 非管理ディスクを使用して仮想マシンをプロビジョニングすることは推奨されません。
> - ホスト接続で構成されたリージョンとは異なるリージョンからマスターイメージを使用することに対するサポートは、廃止されました。Azure Compute Gallery を使用して、マスターイメージを目的のリージョンに複製します。

イメージの準備中に、元の仮想マシンに基づいて準備用の仮想マシン(VM)が作成されます。この準備 VM はネットワークから切断されています。ネットワークを準備 VM から切断するために、すべての受信および送信トラフィックを拒否するネットワークセキュリティグループが作成されます。ネットワークセキュリティグループは、自動的にカタログごとに 1 回作成されます。ネットワークセキュリティグループの名前は`Citrix-Deny-All-a3pgu-GUID`で、GUID がランダムに生成されます。例: `Citrix-Deny-All-a3pgu-3f161981-28e2-4223-b797-88b04d336dd1`。

マシンカタログ作成ウィザードで次の操作を行います:

1. [マシンの種類] ページと [マシン管理] ページには、Azure 固有の情報は含まれていません。「マシンカタログの作成」のガイダンスに従ってください。
2. [イメージ] ページで、カタログ内のすべてのマシンのマスターイメージとして使用するイメージを選択します。[イメージの選択] ウィザードが表示されます。イメージを選択するには、次の手順に従います:

   a) (テナント内またはテナント間で共有イメージを使用して構成された接続にのみ適用可能) イメージが存在するサブスクリプションを選択します。
   b) リソースグループの選択
   c) Azure 管理対象ディスク、Azure Compute Gallery、または Azure イメージバージョンに移動します。

   イメージを選択するときは、次の点を考慮してください:

   - Citrix VDA がイメージにインストールされていることを確認します。
   - VM に接続されているディスクを選択した場合は、次の手順に進む前に VM をシャットダウンする必要があります。

   > 注:
   >
   > - カタログにマシンを作成した接続(ホスト)のサブスクリプションは、緑色の点で示されます。他のサブスクリプションは、Azure Compute Gallery をそのサブスクリプションと共有します。これらのサブスクリプションでは、共有ギャラリーのみが表示されます。共有サブスクリプションの構成方法については、「単一のテナント内(サブスクリプション間)での画像の共有」および「テナント間での画像の共有」を参照してください。
   > - トラステッド起動で、Windows でエフェメラル OS ディスクを使用して、プロビジョニングスキームを作成できます。トラステッド起動でイメージを選択する場合は、vTPM が有効になっているトラステッド起動でマシンプロファイルを選択する必要があります。エフェメラル OS ディスクを使用してマシンカタログを作成する方法については、「エフェメラル OS ディスクを使用してマシ

> ンを作成する方法」を参照してください。
> - イメージのレプリケーション中に、先に進んでそのイメージをマスターイメージとして選択し、セットアップを完了することができます。ただし、イメージのレプリケーション中は、カタログ作成完了までの時間が長くなることがあります。MCS では、カタログの作成開始から 1 時間以内にレプリケーションを完了する必要があります。レプリケーションがタイムアウトすると、カタログの作成は失敗します。レプリケーションステータスは Azure で確認できます。レプリケーションがまだ保留中の場合、またはレプリケーションが完了した後で再試行してください。
> - Gen2 イメージを使用して Gen 2 VM カタログをプロビジョニングし、起動時のパフォーマンスを向上させることができます。ただし、Gen1 イメージを使用した Gen2 マシンカタログの作成はサポートされていません。同様に、Gen2 イメージを使用した Gen1 マシンカタログの作成もサポートされていません。また、世代情報を持たない古いイメージはすべて Gen1 イメージです。

カタログ内の VM がマシンプロファイルから構成を継承するかどうかを選択します。デフォルトでは、［マシンプロファイルを使用する（**Azure Active Directory** では必須）］チェックボックスがオンになっています。［マシンプロファイルを選択］を クリックして、リソースグループの一覧から VM または ARM テンプレートスペックを参照します。

VM がマシンプロファイルから継承できる構成の例として、次のようなものがあります:

- 高速ネットワーク
- ブート診断
- ホストのディスクキャッシュ（OS および MCSIO ディスク関連）
- マシンサイズ（別途指定されていない場合）
- VM に適用されたタグ

> 注:
>
> - Azure でマシンカタログのマスターイメージを選択すると、選択されたマスターイメージに基づいてマシンプロファイルがフィルタリングされます。たとえば、マシンプロファイルは、Windows OS、セキュリティの種類、休止のサポート、およびマスターイメージのディスク暗号化セット ID に基づいてフィルタリングされます。
> - トラステッド起動が有効になっているイメージまたはスナップショットを選択する場合は、［セキュリティの種類］としてトラステッド起動が選択されているマシンプロファイルを使用する必要があります。次に、［マシンプロファイル］の値を指定することにより、SecureBoot と vTPM を有効または無効にできます。Azure のトラステッド起動については、「https://docs.microsoft.com/en-us/azure/virtual-machines/trusted-launch」を参照してください。

ARM テンプレートスペックを検証して、マシンカタログを作成するためにマシンプロファイルとして使用できるかどうかを確認します。Azure テンプレートスペックの作成について詳しくは、「Azure テンプレートスペックの作成」を参照してください。

ARM テンプレートスペックを検証する方法は 2 つあります:

- リソースグループの一覧から ARM テンプレートスペックを選択したら、［次へ］をクリックします。ARM テンプレートスペックにエラーがある場合、エラーメッセージが表示されます。
- 次の PowerShell コマンドのいずれかを実行します：
  - `Test-ProvInventoryItem -HostingUnitName <string> -InventoryPath <string>`
  - `Test-ProvInventoryItem -HostingUnitUid <Guid> -InventoryPath <string>`

  例：

```
Test-ProvInventoryItem -HostingUnitName "we-vdi0101-d-vnet" -
    InventoryPath machineprofile.folder/vdi01-d-rg.
    resourcegroup/VDD-templ-spec.templatespec/1.5.
    templatespecversion
<!--NeedCopy-->
```

カタログを作成した後、イメージがマシンプロファイルから継承している構成を表示できます。［マシンカタログ］ノードで、カタログを選択して下部ペインに詳細を表示します。次に、［テンプレートのプロパティ］タブをクリックしてマシンプロファイルのプロパティを表示します。［タグ］セクションには、最大 3 つのタグが表示されます。その VM に配置されているすべてのタグを表示するには、［すべて表示］をクリックします。

MCS で Azure 専用ホストに VM をプロビジョニングする場合は、［ホストグループを使用する］チェックボックスをオンにし、リストからホストグループを選択します。ホストグループは、専用ホストのコレクションを表すリソースです。専用ホストは、1 つまたは複数の仮想マシンをホストする物理サーバーを提供するサービスです。サーバーは Azure サブスクリプション専用であり、他のサブスクライバーとは共有されません。専用ホストを使用する場合、Azure は、VM がそのホストで実行されている唯一のマシンであることを保証します。この機能は、規制または内部のセキュリティ要件を満たす必要があるシナリオに適しています。ホストグループとそれらを使用する際の考慮事項について詳しくは、「Azure 専用ホストでの VM のプロビジョニング」を参照してください。

> 重要：
>
> - Azure の自動配置が有効になっているホストグループのみが表示されます。
> - ホストグループを使用すると、ウィザードの後半で表示される［**Virtual Machines**］ページが変更されます。選択したホストグループに含まれるマシンサイズのみが、このページに表示されます。また、アベイラビリティゾーンは自動的に選択され、選択できません。

3. ［ストレージとライセンスの種類］ページは、Azure Resource Manager イメージを使用するときのみ表示されます。

   マシンカタログに使用するストレージの種類は次のとおりです：

   - プレミアム **SSD**：I/O を多用するワークロードを持つ VM に適した、高性能かつ低遅延のディスクストレージオプションを提供します。

- 標準 **SSD**：低 IOPS レベルで安定したパフォーマンスを必要とするワークロードに適した、コスト効率の高いストレージオプションを提供します。
- 標準 **HDD**：遅延の影響を受けないワークロードを実行している VM に対して、信頼性の高い低コストのディスクストレージオプションを提供します。
- **Azure** エフェメラル **OS** ディスク VM のローカルディスクを再利用してオペレーティングシステムディスクをホストする、コスト効率の高いストレージオプションを提供します。または、PowerShell を使用して、エフェメラル OS ディスクを使用するマシンを作成することもできます。詳しくは、「Azure エフェメラルディスク」を参照してください。エフェメラル OS ディスクを使用する場合は、次の点を考慮してください：
  - Azure エフェメラル OS ディスクと MCS I/O を同時に有効にすることはできません。
  - エフェメラル OS ディスクを使用するマシンを更新するには、サイズが仮想マシンのキャッシュディスクまたは一時的ディスクのサイズを超えないイメージを選択する必要があります。
  - ウィザードの後半で表示される［電源サイクル中に仮想マシンとシステムディスクを保持する］オプションを使用することはできません。

> 注：
>
> ID ディスクは、選択したストレージの種類に関係なく、常に標準 SSD を使用して作成されます。

ストレージの種類によって、ウィザードの［仮想マシン］ページに表示されるマシンのサイズが変わります。MCS は、ローカル冗長ストレージ（LRS）を使用するようにプレミアムディスクと標準ディスクを構成します。LRS は、単一のデータ センター内でデータの複数の同期コピーを作成します。Azure エフェメラル OS ディスクは、VM のローカルディスクを使用してオペレーティングシステムを格納します。Azure のストレージの種類およびストレージの複製について詳しくは、以下のドキュメントを参照してください：

- Azure Storage の概要
- Azure Premium Storage：高パフォーマンス向け設計
- Azure Storage の冗長性

既存の Windows ライセンスを使用するか Linux ライセンスを使用するかを選択します：

- Windows ライセンス：Windows ライセンスと Windows イメージ（Azure プラットフォームのサポートイメージまたはカスタムイメージ）を使用すると、Azure で Windows VM を低コストで実行できます。ライセンスには次の 2 種類があります：
  - **Windows Server** ライセンス。Windows Server ライセンスまたは Azure Windows Server ライセンスを使用できます。これにより、Azure Hybrid 特典を使用できます。詳しくは、https://azure.microsoft.com/en-us/pricing/hybrid-benefit/を参照してください。Azure Hybrid 特典を使用すると、Azure ギャラリーからの Windows Server 追加ライセンス料金が不要になるため、Azure での仮想マシン実行コストを基本計算料金のみに抑えられます。
  - **Windows** クライアントライセンス。Windows 10 ライセンスおよび Windows 11 ライセンスを Azure に移行できるため、追加のライセンスなしで Windows 10 VM および Windows 11 VM

を Azure で実行できます。詳しくは、「クライアントアクセスライセンスと管理ライセンス」を参照してください。

- Linux ライセンス：bring-your-own-subscription（BYOS）Linux ライセンスを使用すると、ソフトウェアの料金を支払う必要がありません。BYOS の料金には、コンピューティングハードウェアの料金のみが含まれます。ライセンスには次の 2 種類があります：
  - **RHEL_BYOS**：RHEL_BYOS の種類を正しく使用するには、Azure サブスクリプションで Red Hat Cloud Access を有効にします。
  - **SLES_BYOS**：SLES の BYOS バージョンには、SUSE からのサポートが含まれています。

以下を参照してください：

- Windows ライセンスの確認
- Linux ライセンスの構成

ライセンスの種類と利点を理解するには、次のドキュメントを参照してください：

- https://docs.microsoft.com/en-us/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet
- https://docs.microsoft.com/en-us/azure/virtual-machines/linux/azure-hybrid-benefit-linux

Azure Compute Gallery は、イメージを管理および共有するためのリポジトリです。これにより、組織全体でイメージを利用できるようになります。大規模な永続的でないマシンカタログを作成する場合は、よりすばやく VDA OS ディスクをリセットできるため、イメージを Azure Compute Gallery に保存することをお勧めします。［準備されたイメージを **Azure Compute Gallery** に配置します］を選択すると、［**Azure Computer Gallary** の設定］セクションが表示され、追加の Azure Computer Gallary 設定を指定できます：

- イメージレプリカに対する仮想マシンの比率。Azure で保持するイメージレプリカに対する仮想マシンの比率を指定できます。デフォルトでは、Azure は 40 台の非永続的なマシンごとに 1 つのイメージレプリカを保持します。永続マシンの場合、その数はデフォルトで 1,000 になります。
- 最大レプリカ数。Azure で保持するイメージレプリカの最大数を指定できます。デフォルトは 10 です。

Azure Compute Gallery について詳しくは、「Azure Compute Gallery」を参照してください。

4. ［仮想マシン］ページで、作成する VM の数とマシンサイズを指定します。カタログ作成後、カタログを編集してマシンサイズを変更できます。
5. ［**NIC**］ページには、Azure 固有の情報は表示されません。「マシンカタログの作成」のガイダンスに従ってください。
6. ［ディスク設定］ページで、ライトバックキャッシュを有効にするかどうかを選択します。MCS ストレージ最適化機能を有効にすると、カタログを作成するときに以下の設定を構成できます。これらの設定は、Azure 環境と GCP 環境の両方に適用されます。

ライトバックキャッシュを有効にした後、次の操作を実行できます:

- 一時データのキャッシュに使用するディスクと RAM のサイズを構成する。詳しくは、「一時データ用キャッシュの構成」を参照してください。
- ライトバックキャッシュディスク用のストレージの種類を選択します。ライトバックキャッシュディスクには、次のストレージのオプションを使用できます:
  - プレミアム SSD
  - 標準 SSD
  - 標準 HDD
- プロビジョニングされた VM に対してライトバックキャッシュディスクを保持するかどうかを選択します。このオプションを使用可能にするには、[ライトバックキャッシュを有効にする] を選択します。デフォルトでは、[非永続的なライトバックキャッシュディスクを使用する] が選択されています。
- ライトバックキャッシュディスクの種類を選択します。
  - 非永続的なライトバックキャッシュディスクを使用する。選択した場合、ライトバックキャッシュディスクは電源サイクル中に削除されます。リダイレクトされたデータはすべて失われます。VM の一時ディスクに十分なスペースがある場合、それはライトバックキャッシュディスクのホストに使用され、コストを削減します。カタログの作成後、プロビジョニングされたマシンが一時ディスクを使用しているかどうかを確認できます。これを行うには、カタログをクリックして、[テンプレートのプロパティ] タブの情報を確認します。一時ディスクが使用されている場合は、[非永続的なライトバックキャッシュディスク] が表示され、その値は [はい（**VM** の一時ディスクを使用)] になっていますそうでない場合は、[非永続的なライトバックキャッシュディスク] が表示され、その値は [いいえ]（**VM** の一時ディスクを使用しない）になっています。
  - 永続的なライトバックキャッシュディスクを使用する。選択した場合、ライトバックキャッシュディスクは、プロビジョニングされた VM で保持されます。このオプションを有効にすると、ストレージコストが増加します。
- 電源サイクル中に VDA 用の仮想マシンとシステムディスクを保持するかどうかを選択します。

  電源サイクル中に仮想マシンおよびシステムディスクを保持します。[ライトバックキャッシュを有効にする] を選択した場合に使用できます。デフォルトでは、仮想マシンとシステムディスクはシャットダウン時に削除され、スタートアップ時に再作成されます。仮想マシンの再起動時間を短縮したい場合は、このオプションを選択します。このオプションを有効にすると、ストレージコストも増加することに注意してください。
- ストレージコストの削減を有効にする かどうかを選択します。有効にすると、VM のシャットダウン時にストレージディスクを標準 HDD にダウングレードすることで、ストレージコストを削減できます。VM は、再起動時に元の設定に切り替わります。このオプションは、ストレージディスクとライトバックキャッシュディスクの両方に適用されます。または、PowerShell を使用することもできます。「仮想マシンのシャットダウン時にストレージの種類をダウングレードする」を参照してください。

> 注:
>
> Microsoft は、VM のシャットダウン中のストレージの種類の変更に制限を課しています。Microsoft が将来的にストレージの種類の変更を禁止する可能性もあります。詳しくは、Microsoft 社の記事を参照してください。

- このカタログ内のマシン上のデータを暗号化するかどうかを選択し、使用する暗号キーを選択します。顧客管理キー（CMK）を使用したサーバー側暗号化により、管理対象ディスクレベルで暗号化を管理し、カタログ内のマシン上のデータを保護できます。デフォルト設定はマシンプロファイルまたはマスターイメージから継承され、プロファイルが優先されます:
  - *CMK* を含むマシンプロファイルを使用している場合、[次のキーを使用して各マシンのデータを暗号化] オプションが自動的に選択され、デフォルトでマシンプロファイルのキーが使用されます。
  - プラットフォーム管理キー（PMK）を含むマシンプロファイルを使用し、マスターイメージが *CMK* で暗号化されている場合、[次のキーを使用して各マシンのデータを暗号化] オプションが自動的に選択され、デフォルトでマスターイメージのキーが使用されます。
  - マシンプロファイルを使用せず、マスターイメージが *CMK* で暗号化されている場合、[次のキーを使用して各マシンのデータを暗号化] オプションが自動的に選択され、デフォルトでマスターイメージのキーが使用されます。

詳しくは、「Azure サーバー側暗号化」を参照してください。

7. [リソースグループ] ページで、リソースグループを作成するか、既存のグループを使用するかを選択します。
   - リソースグループを作成する場合は、[次へ] を選択します。
   - 既存のリソースグループを使用する場合は、[使用可能なプロビジョニングリソースグループ] ボックスの一覧からグループを選択します。

   > 注:
   >
   > カタログで作成しているマシンを収容するのに十分なグループを選択してください。選択が少なすぎると、メッセージが表示されます。後でカタログにさらに VM を追加する予定がある場合は、必要最小限よりも多く選択しておくことをお勧めします。カタログが作成された後、カタログにリソースグループをさらに追加することはできません。

   詳しくは、「Azure リソースグループ」を参照してください。

8. [マシン **ID**] ページで ID の種類を選択し、このカタログ内のマシンの ID を設定します。[**Azure Active Directory** 参加] として仮想マシンを選択すると、それらを Azure AD セキュリティグループに追加できます。詳細な手順は次のとおりです:

   a) [**ID** の種類] フィールドから、[**Azure Active Directory** 参加] を選択します。[**Azure AD** セキュリティグループ（オプション）] オプションが表示されます。
   b) [**Azure AD** セキュリティグループ: 新規作成] をクリックします。
   c) グループ名を入力して、[作成] をクリックします。

d) 画面の指示に従って、Azure にサインインします。
グループ名が Azure に存在しない場合は、緑色のアイコンが表示されます。それ以外の場合は、新しい名前の入力を求めるエラーメッセージが表示されます。

e) 割り当て済みセキュリティ グループにこのセキュリティグループを追加するには、［割り当て済みのセキュリティグループをメンバーとして参加させる］を選択し、［グループの選択］をクリックしてから、参加させる割り当て済みグループを選択します。

f) 仮想マシンのマシンアカウント名前付けスキームを入力します。

カタログの作成後、Citrix DaaS はユーザーに代わって Azure にアクセスし、セキュリティグループとグループの動的メンバーシップ規則を作成します。この規則に基づいて、このカタログで指定された名前付けスキームの仮想マシンがセキュリティグループに自動的に追加されます。

このカタログに別の名前付けスキームの仮想マシンを追加するには、Azure にサインインする必要があります。その後、Citrix DaaS は Azure にアクセスし、新しい名前付けスキームに基づいて動的メンバーシップ規則を作成できます。

このカタログを削除する場合、Azure からセキュリティグループを削除するには、Azure へのサインインも必要です。

> 注:
>
> カタログの作成後に Azure AD セキュリティグループの名前を変更するには、カタログを編集し、左側のナビゲーションから ［**Azure AD** セキュリティグループ］に移動します。Azure AD セキュリティグループの名前には、次の文字を含めることはできません: `@ "\ / ; : # . * ? = < > | [ ] ( )'`。

- ［ドメイン資格情報］ページおよび ［概要］ページには、Azure 固有の情報は表示されません。「マシンカタログの作成」のガイダンスに従ってください。

ウィザードを完了します。

Azure テンプレートスペックを作成する

Azure Portal で Azure テンプレートスペックを作成し、それを［完全な構成］インターフェイスと PowerShell コマンドで使用して、MCS マシンカタログを作成または更新できます。

既存の仮想マシンの Azure テンプレートスペックを作成するには、以下の手順に従います:

1. Azure Portal に移動します。リソースグループを選択してから、仮想マシンとネットワークインターフェイスを選択します。上の［…］メニューで、［**Export template**］をクリックします。
2. カタログプロビジョニング用のテンプレートスペックを作成する場合は、［**Include parameters**］チェックボックスをオフにします。
3. テンプレートスペックを後で変更するには、［**Add to library**］をクリックします。

4. [**Importing template**] ページで、**Name**、**Subscription**、**Resource Group**、**Location**、**Version** などの必要な情報を入力します。[**Next: Edit Template**] をクリックします。
5. カタログをプロビジョニングする場合は、独立したリソースとしてネットワークインターフェイスも必要です。したがって、テンプレートスペックで指定されている dependsOn を削除する必要があります。例:

```
"dependsOn": [
"[resourceId('Microsoft.Network/networkInterfaces', 'tnic937')]"
],
<!--NeedCopy-->
```

6. [**Review+Create**] を作成してテンプレートスペックを作成します。
7. [**Template Specs**] ページで、作成したテンプレートスペックを確認します。テンプレートスペックをクリックします。左側のパネルで、[**Versions**] をクリックします。
8. [**Create new version**] をクリックして、新しいバージョンを作成できます。新しいバージョン番号を指定し、現在のテンプレートスペックを変更して、[**Review + Create**] をクリックし、新しいバージョンのテンプレートスペックを作成します。

次の PowerShell コマンドを使用して、テンプレートスペックとテンプレートのバージョンに関する情報を取得できます:

- テンプレートスペックに関する情報を取得するには、次を実行します:

```
get-item XDHyp:\HostingUnits\East\machineprofile.folder\abc.
   resourcegroup\bggTemplateSpec.templatespec
<!--NeedCopy-->
```

- テンプレートスペックのバージョンに関する情報を取得するには、次を実行します:

```
get-item XDHyp:\HostingUnits\East\machineprofile.folder\abc.
   resourcegroup\bggTemplateSpec.templatespec\bgg1.0.
   templatespecversion
<!--NeedCopy-->
```

カタログの作成または更新でテンプレートスペックを使用する

テンプレートスペックをマシンプロファイルの入力に使用して、MCS マシンカタログを作成または更新できます。これを行う場合、完全な構成 インターフェイスまたは PowerShell コマンドを使用できます。

- [完全な構成] インターフェイスを使用する:「[完全な構成] インターフェイスで Azure Resource Manager イメージを使用してマシンカタログを作成する」を参照してください。
- PowerShell については、「PowerShell を使用したカタログの作成または更新でテンプレートスペックを使用する」を参照してください

指定されたアベイラビリティゾーンへのマシンのプロビジョニング

Azure 環境の特定のアベイラビリティゾーンにマシンをプロビジョニングできます。これは、完全な構成インターフェイスまたは PowerShell を使用して実行できます

> 注:
>
> ゾーンが指定されていない場合、MCS は Azure にマシンをリージョン内に配置させます。複数のゾーンが指定されている場合、MCS はマシンをそれらにランダムに分散します。

完全な構成インターフェイスを使用したアベイラビリティゾーンの構成

マシンカタログを作成するときに、マシンをプロビジョニングするアベイラビリティゾーンを指定できます。[仮想マシン] ページで、マシンを作成するアベイラビリティゾーンを 1 つ以上選択します。

アベイラビリティゾーンが使用できない理由は 2 つあります: リージョンにアベイラビリティゾーンがないか、選択したマシンサイズが使用できないことです。

PowerShell コマンドを使用した構成について詳しくは、「PowerShell を使用したアベイラビリティゾーンの構成」を参照してください。

Azure エフェメラルディスク

Azure エフェメラルディスクを使用すると、キャッシュディスクまたは一時ディスクを再利用して、Azure 対応の仮想マシンの OS ディスクを保存できます。この機能は、標準の HDD ディスクよりも高性能の SSD ディスクを必要とする Azure 環境で役立ちます。Azure エフェメラルディスクを使用したカタログの作成については、「Azure エフェメラルディスクを使用したカタログの作成」を参照してください。

> 注:
>
> 永続カタログでは、エフェメラル OS ディスクはサポートされていません。

エフェメラル OS ディスクでは、プロビジョニングスキームで管理対象ディスクと Azure Compute Gallery を使用する必要があります。詳しくは、「Azure Shared Image Gallery」を参照してください。

エフェメラル **OS** 一時ディスクの保存

エフェメラル OS ディスクを VM 一時ディスクまたはリソースディスクに保存するオプションがあります。この機能により、キャッシュがないか、キャッシュが不十分な VM で、エフェメラル OS ディスクを使用できます。このような VM には、Ddv4などのエフェメラル OS ディスクを保存するための一時ディスクまたはリソースディスクがあります。

以下に注意してください:

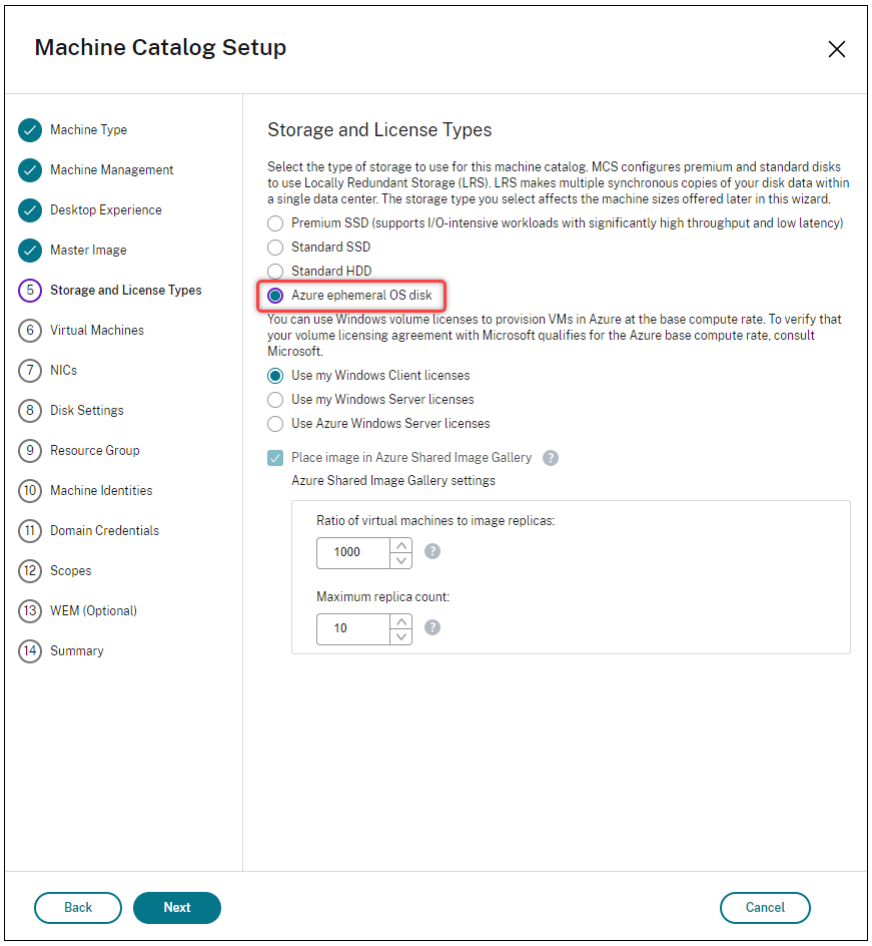
- エフェメラルディスクは、VM キャッシュディスクまたは VM の一時（リソース）ディスクのいずれかに保存されます。キャッシュディスクが OS ディスクの内容を保持するのに十分な大きさでない場合を除き、キャッシュディスクは一時ディスクよりも優先されます。
- 更新の際は、キャッシュディスクよりも大きいが一時ディスクよりも小さい新しいイメージにより、エフェメラル OS ディスクが VM の一時ディスクに置き換えられます。

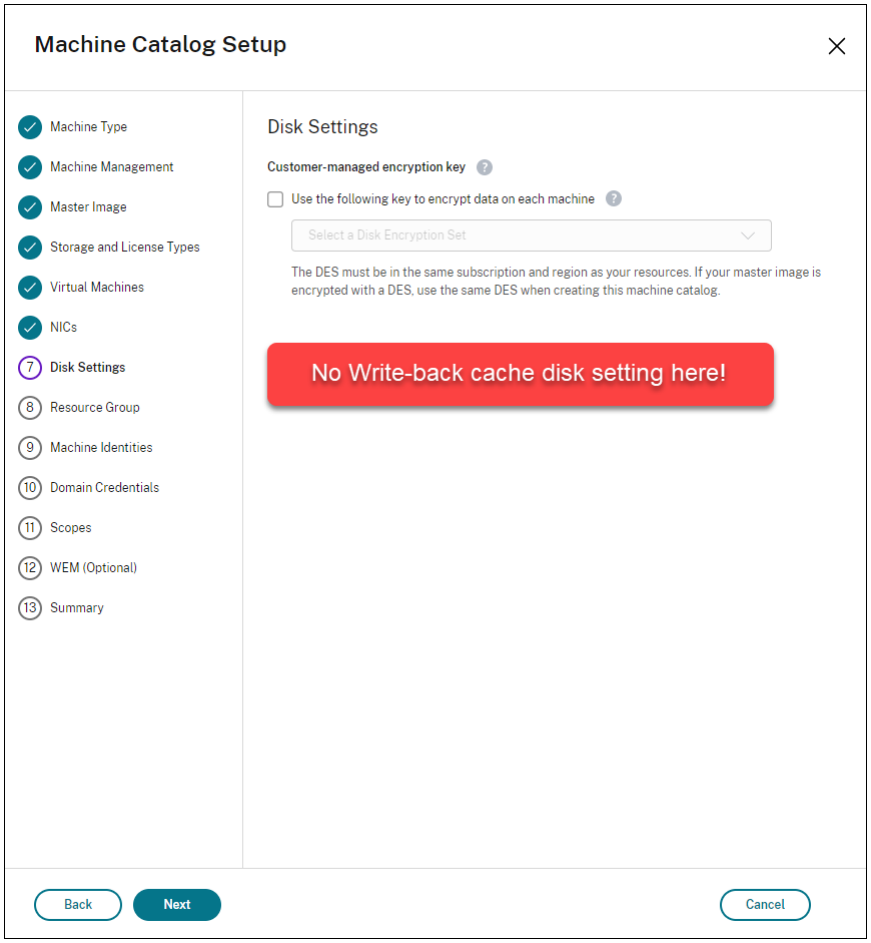
Azure エフェメラルディスクと **Machine Creation Services**（**MCS**）ストレージ最適化（**MCS I/O**）

Azure エフェメラル OS ディスクと MCS I/O を同時に有効にすることはできません。

重要な考慮事項は次のとおりです：

- エフェメラル OS ディスクと MCS I/O の両方を同時に有効にしてマシンカタログを作成することはできません。
- マシンカタログのセットアップウィザードで、［ストレージとライセンスの種類］ページの ［**Azure** エフェメラル **OS** ディスク］を選択した場合、［ディスク設定］ページでライトバックキャッシュディスク のオプションは使用できません。





- New-ProvSchemeまたはSet-ProvSchemeが「**true**」に設定された PowerShell パラメーター（UseWriteBackCacheおよびUseEphemeralOsDisk）を使用すると、適切なエラーメッセージが表示されて失敗します。
- 両方の機能を有効にして作成した既存のマシンカタログについては、次のことができます：
  - マシンカタログの更新。
  - VM の追加または削除。
  - マシンカタログの削除。

Azure Compute Gallery

Azure において、MCS でプロビジョニングされたマシンの公開イメージリポジトリとして Azure Shared Image Gallery（旧称：Shared Image Gallery）を使用します。公開イメージをギャラリーに保存して、OS ディスクの作成とハイドレーションを高速化し、非永続仮想マシンの起動時間とアプリケーションの起動時間を改善できます。Azure Compute Gallery には、次の 3 つの要素が含まれています：

- ギャラリー：イメージはここに保存されます。MCS は、マシンカタログごとに 1 つのギャラリーを作成します。

- ギャラリーイメージの定義：この定義には、公開イメージに関する情報（オペレーティングシステムの種類と状態、Azure リージョン）が含まれます。MCS は、カタログ用に作成されたイメージごとに 1 つのイメージ定義を作成します。
- ギャラリーイメージバージョン：Azure Compute Gallery の各イメージには複数のバージョンを含めることができ、各バージョンには異なるリージョンに複数のレプリカを含めることができます。各レプリカは、公開イメージの完全なコピーです。Citrix DaaS では、カタログ内のマシン数、構成されたレプリカの比率、および構成されたレプリカの最大数に基づき、カタログのリージョンにおいて適切なレプリカ数を持つ各イメージに対して、Standard_LRS イメージバージョン（バージョン 1.0.0）が 1 つ作成されます。

> 注：
>
> Azure Compute Gallery の機能は、管理対象ディスクとのみ互換性があります。従来のマシンカタログでは使用できません。

詳しくは、「Azure Shared Image Gallery の概要」を参照してください。

Azure Compute Galleryy からイメージにアクセスする

マシンカタログの作成に使用するイメージを選択するときに、Azure Compute Gallery で作成したイメージを選択できます。これらのイメージは、マシンカタログインストールウィザードの ［イメージ］ページのイメージ一覧に表示されます。

これらのイメージを表示するには、次のことを行う必要があります：

1. Citrix DaaS をセットアップします。
2. Azure Resource Managerに接続します。
3. Azure ポータルで、リソースグループを作成します。詳しくは、「ポータルを使用して Azure Shared Image Gallery を作成する」を参照してください。
4. リソースグループで、Azure Compute Gallery を作成します。
5. Azure Compute Gallery で、イメージ定義を作成します。
6. イメージ定義で、イメージバージョンを作成します。

Azure Compute Gallery について詳しくは、「Configure Azure Compute Gallery」を参照してください。

Azure 一時ディスクをライトバックキャッシュディスクとして使用するための条件

次のすべての条件が満たされている場合にのみ、Azure 一時ディスクをライトバックキャッシュディスクとして使用できます：

- Azure 一時ディスクは永続データには適していないため、ライトバックキャッシュディスクは非永続である必要があります。
- 選択した Azure VM のサイズには、一時ディスクが含まれている必要があります。

- エフェメラル OS ディスクを有効にする必要はありません。
- ライトバックキャッシュファイルを Azure 一時ディスクに保存することを受け入れます。
- Azure 一時ディスクのサイズは、「ライトバックキャッシュディスクサイズ + ページングファイル用に予約されたスペース + 1GB のバッファスペース」の合計サイズよりも大きい必要があります。

非永続的なライトバックキャッシュディスクのシナリオ

次の表は、マシンカタログの作成中に一時ディスクがライトバックキャッシュに使用される場合の 3 つの異なるシナリオを示しています。

シナリオ	結果
ライトバックキャッシュに一時ディスクを使用するためのすべての条件が満たされている。	WBC ファイル`mcsdif.vhdx`は一時ディスクに保存されます。
一時ディスクに、ライトバックキャッシュを使用するための十分なスペースがない。	VHD ディスク「MCSWCDisk」が作成され、WBC ファイル`mcsdif.vhdx`がこのディスクに保存されます。
一時ディスクに、ライトバックキャッシュを使用するための十分なスペースがあるが、`UseTempDiskForWBC`は false に設定されている。	VHD ディスク「MCSWCDisk」が作成され、WBC ファイル`mcsdif.vhdx`がこのディスクに保存されます。

次の PowerShell トピックを参照してください:

- 非永続的なライトバックキャッシュディスクのマシンカタログを作成する
- 永続的なライトバックキャッシュディスクのマシンカタログを作成する

Azure サーバー側暗号化

Citrix DaaS は、Azure Key Vault を使用して Azure Managed Disks の顧客が管理する暗号化キーをサポートします。このサポートにより、独自の暗号化キーを使用してマシンカタログの管理対象ディスクを暗号化して、組織およびコンプライアンスの要件を管理できます。詳しくは、「Azure Disk Storage のサーバー側暗号化」を参照してください。

管理対象ディスクにこの機能を使用する場合:

- ディスクが暗号化されているキーを変更するには、`DiskEncryptionSet`の現在のキーを変更します。`DiskEncryptionSet`に関連付けられているすべてのリソースは、新しいキーで暗号化されるように変更されます。
- キーを無効にするか削除すると、そのキーを使用するディスクのある VM はすべて自動的にシャットダウンします。シャットダウン後、キーを再度有効にするか、新しいキーを割り当てない限り、VM は使用できません。このキーを使用するカタログの電源をオンにすることはできません。また、VM をカタログに追加することもできません。

顧客が管理する暗号化キーを使用する場合の重要な考慮事項

この機能を使用するときは、次のことに注意してください:

- 顧客が管理するキーに関連するすべてのリソース（Azure Key Vault、ディスク暗号化セット、VM、ディスク、スナップショット）は、同じサブスクリプションとリージョンに配置される必要があります。
- 顧客が管理するキーで暗号化されたディスク、スナップショット、イメージは、別のリソースグループおよびサブスクリプションに移動できません。
- リージョンごとのディスク暗号化セットの制限については、Microsoft 社のサイトを参照してください。

> 注:
>
> Azure サーバー側暗号化の構成については、「クイックスタート: Azure Portal を使用してキーコンテナを作成する」を参照してください。

Azure の顧客が管理する暗号キー

マシンカタログを作成するときに、カタログでプロビジョニングされるマシンのデータを暗号化するかどうかを選択できます。顧客が管理する暗号化キーを使用したサーバー側暗号化により、管理対象ディスクレベルで暗号化を管理し、カタログ内のマシン上のデータを保護できます。ディスク暗号化セット（DES）は、顧客が管理するキーを表します。この機能を使用するには、最初に Azure で DES を作成する必要があります。DES の形式は次のとおりです:

- `/subscriptions/12345678-1234-1234-1234-123456789012/resourceGroups/Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/SampleEncryption`

一覧から DES を選択します。選択した DES は、リソースと同じサブスクリプションおよびリージョンに存在する必要があります。

暗号化キーを使用してカタログを作成し、後で Azure で対応する DES を無効にすると、カタログ内のマシンの電源をオンにしたり、カタログにマシンを追加したりできなくなります。

「顧客管理暗号キーを使用したマシンカタログの作成」を参照してください。

ホストでの **Azure** ディスク暗号化

ホスト機能での暗号化を使用して、MCS マシンカタログを作成できます。現在、MCS はこの機能でマシンプロファイルワークフローのみをサポートします。VM またはテンプレートスペックをマシンプロファイルの入力として使用できます。

この暗号化方法は、Azure Storage でデータを暗号化しません。VM をホストするサーバーがデータを暗号化し、暗号化されたデータが Azure Storage サーバーを通過します。つまり、この暗号化方法はデータをエンドツーエンドで暗号化します。

制限:

ホストでの Azure ディスク暗号化は:

- すべての Azure マシンサイズでサポートされているわけではありません
- Azure Disk Encryption と互換性がありません

詳しくは、次のトピックを参照してください:

- ホストでの暗号化機能を使用してマシンカタログを作成する。
- マシンプロファイルからホストでの暗号化情報を取得する

管理対象ディスクの二重暗号化

二重暗号化を使用してマシンカタログを作成できます。この機能を使用して作成されたカタログでは、すべてのディスクがプラットフォームキーと顧客管理キーの両方によってサーバー側で暗号化されています。Azure Key Vault、暗号キー、およびディスク暗号化セット（DES）は、顧客が所有し、維持します。

二重暗号化とは、プラットフォーム側の暗号化（デフォルト）と顧客管理の暗号化（CMEK）です。したがって、暗号化アルゴリズム、実装、またはキーの侵害に関するリスクを懸念している、セキュリティに非常に敏感なお客様は、この二重暗号化を選択できます。永続的 OS ディスクとデータディスク、スナップショット、イメージはすべて二重暗号化により保存時に暗号化されます。

> 注:
>
> - 完全な構成インターフェイスを使用するか、PowerShell コマンドを実行することで、二重暗号化を使用してマシンカタログを作成し、更新できます。
> - 二重暗号化を使用してマシンカタログを作成または更新するには、非マシンプロファイルベースのワークフローまたはマシンプロファイルベースのワークフローを使用できます。
> - 非マシンプロファイルベースのワークフローを使用してマシンカタログを作成する場合は、保存されている`DiskEncryptionSetId`を再利用できます。
> - マシンプロファイルを使用する場合は、VM またはテンプレートスペックをマシンプロファイルの入力に使用できます。

制限事項

- 二重暗号化は、Ultra Disk または Premium SSD v2 ディスクではサポートされていません。
- 二重暗号化は、非管理ディスクではサポートされません。
- カタログに関連付けられているディスク暗号化セットキーを無効にすると、カタログの VM が無効になります。
- 顧客が管理するキーに関連するすべてのリソース（Azure Key Vault、ディスク暗号化セット、VM、ディスク、スナップショット）は、同じサブスクリプションとリージョンに存在する必要があります。
- サブスクリプションごとに、リージョンあたり最大 50 のディスク暗号化セットのみを作成できます。

次の PowerShell トピックを参照してください:

- 二重暗号化を使用したマシンカタログの作成
- 暗号化されていないカタログを二重暗号化を使用するように変換
- カタログが二重暗号化されていることの確認

Azure リソースグループ

Azure プロビジョニングのリソースグループは、アプリケーションとデスクトップをユーザーに提供する VM をプロビジョニングする方法を提供します。MCS マシンカタログを作成するときに既存の空の Azure リソースグループを追加するか、新しいリソースグループを作成することができます。Azure リソースグループについて詳しくは、Microsoft 社のドキュメントを参照してください。

Azure リソースグループの使用

Azure リソースグループごとの仮想マシン、管理対象ディスク、スナップショット、およびイメージの数に制限はありません（Azure リソースグループごとに仮想マシンは 240、管理対象ディスクは 800 という数の制限はなくなりました）。

- フルスコープのサービスプリンシパルを使用してマシンカタログを作成する場合、MCS は 1 つの Azure リソースグループのみを作成し、カタログのこのグループを使用します。
- スコープの狭いサービスプリンシパルを使用してマシンカタログを作成する場合、事前に作成された空の Azure リソースグループを指定する必要があります。

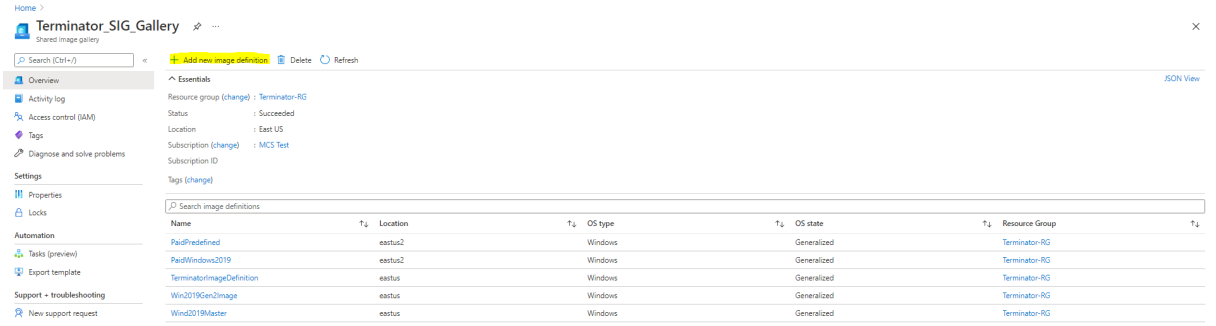
Azure Marketplace

Citrix DaaS は、マシンカタログを作成するためのプラン情報を含む Azure 上のマスターイメージの使用をサポートしています。詳しくは、Microsoft Azure Marketplaceを参照してください。

> ヒント：
>
> 標準の Windows Server イメージなど、Azure Marketplace にある一部のイメージには、プラン情報が追加されていません。Citrix DaaS 機能は有料イメージ用です。

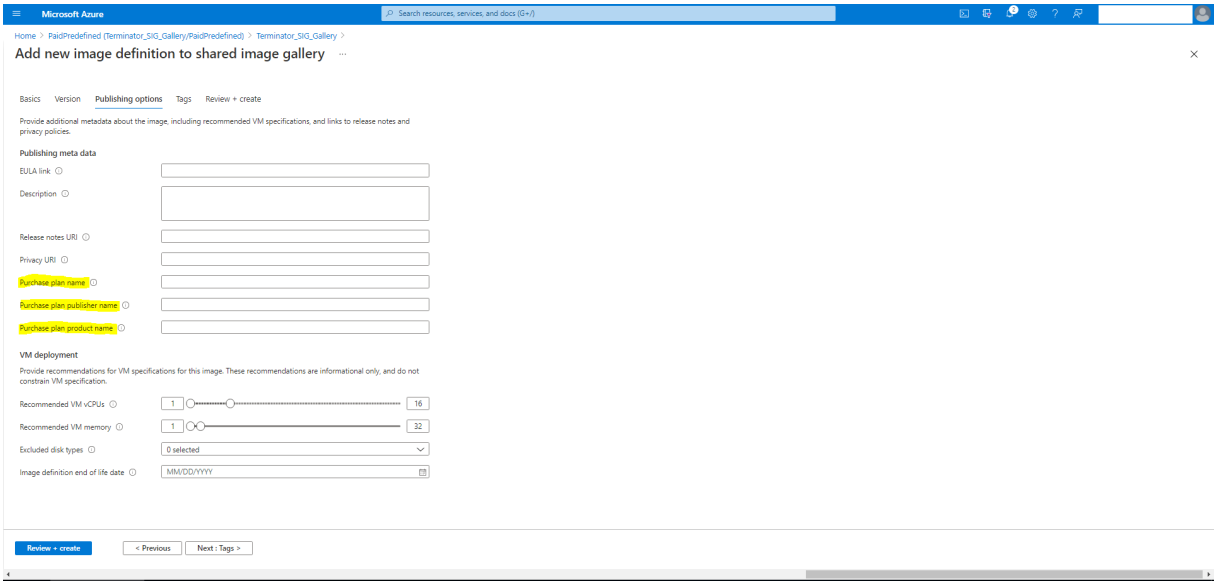
Azure Compute Gallery で作成されたイメージに Azure プラン情報が含まれていることを確認する

このセクションの手順を使用して、完全な構成インターフェイスで Azure Compute Gallery のイメージを表示します。これらのイメージは、マスターイメージに使用することもできます。イメージを Azure Compute Gallery に追加するには、ギャラリーでイメージ定義を作成します。

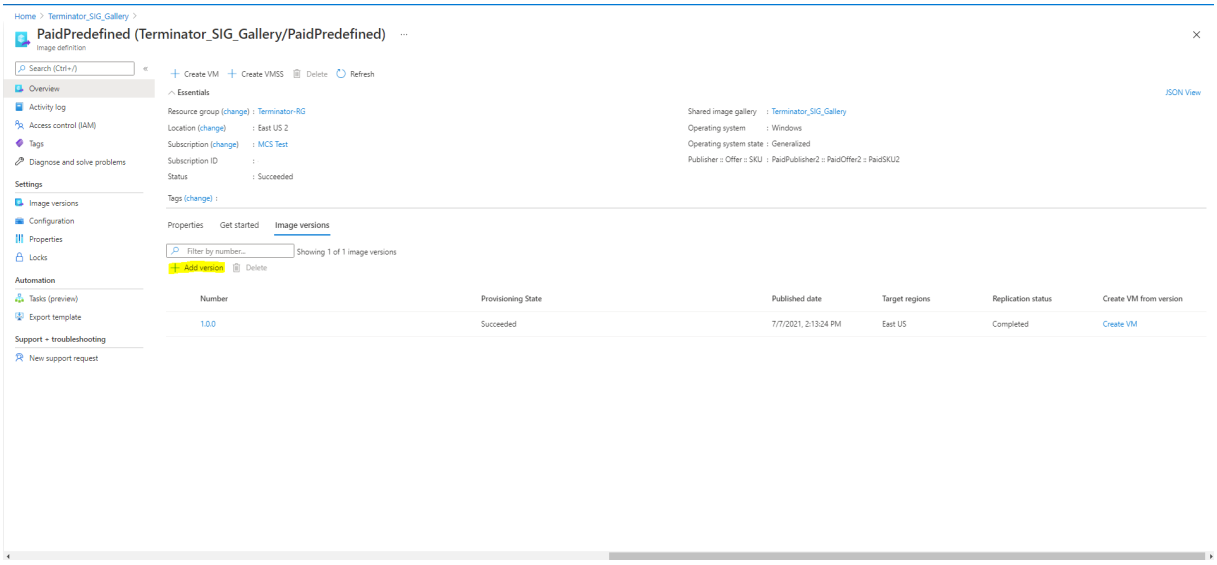


［公開オプション］ページで、購入プラン情報を確認します。

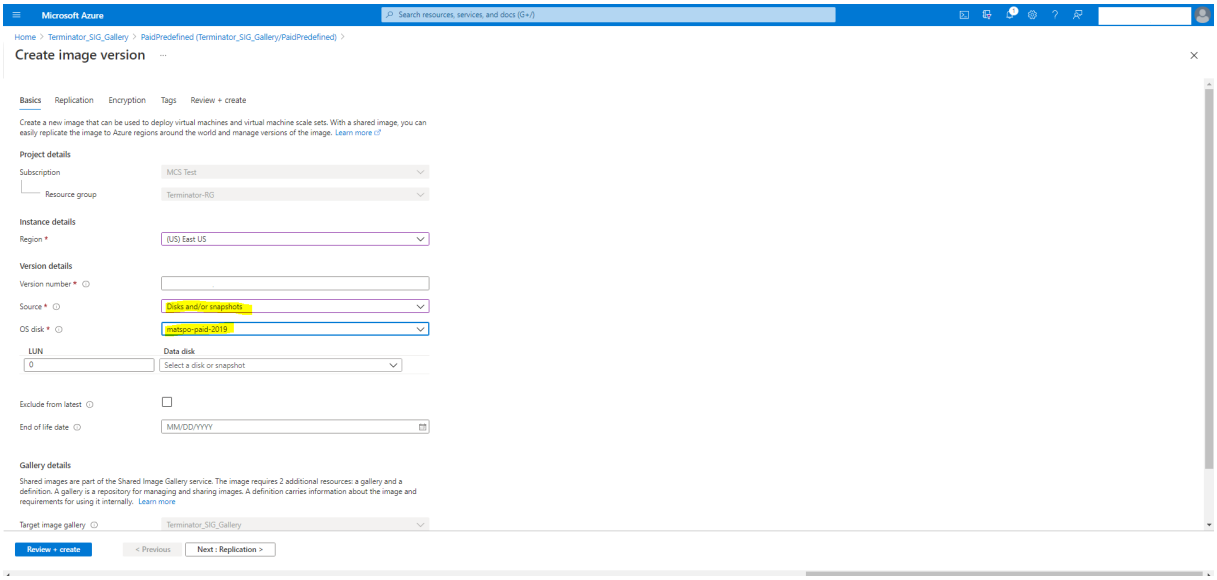
購入プラン情報フィールドは最初は空欄です。これらのフィールドに、イメージに使用されている購入プラン情報を入力します。購入プラン情報を入力しないと、マシンカタログプロセスが失敗する可能性があります。



購入プラン情報を確認した後、定義内にイメージバージョンを作成します。これはマスターイメージとして使用されます。［バージョンの追加］をクリックします:



[バージョンの詳細] セクションで、ソースとしてイメージスナップショットか管理対象ディスクを選択します:



[**Azure Monitor** エージェントがインストールされたカタログ **VM** をプロビジョニングする]

Azure の監視は、Azure 環境および社内のオンプレミス環境からテレメトリデータを収集、分析し、それに基づいて操作するために使用できるサービスです。

Azure Monitor エージェント（AMA）は、仮想マシンなどのコンピューティングリソースから監視データを収集し、そのデータを Azure Monitor に配信します。現在、イベントログ、Syslog、パフォーマンスメトリックの収集がサポートされており、収集した結果を Azure Monitor メトリックと Azure Monitor Log のデータソースとして送信します。

監視データ内の VM を一意に識別して監視を有効にするには、AMA を拡張機能としてインストールして MCS マシンカタログの VM をプロビジョニングします。

要件

- 権限:「Azure の権限について」で規定されている最小限の Azure の権限と、Azure Monitor を使用するための次の権限を持っていることを確認します:
  - `Microsoft.Compute/virtualMachines/extensions/read`
  - `Microsoft.Compute/virtualMachines/extensions/write`
  - `Microsoft.Insights/DataCollectionRuleAssociations/Read`
  - `Microsoft.Insights/dataCollectionRuleAssociations/write`
  - `Microsoft.Insights/DataCollectionRules/Read`
- データ収集規則（DCR）: Azure Portal でデータ収集規則を設定します。DCR の設定について詳しくは、「データ収集規則の作成」を参照してください。DCR はプラットフォーム（Windows または Linux）に固有です。必要なプラットフォームに応じた DCR を必ず作成してください。
  AMA はデータ収集規則（DCR）を使用して、VM などのリソースと、Azure Monitor メトリックや Azure Monitor の Log Analytics エージェントなどのデータ ソースとのマッピングを管理します。
- デフォルトのワークスペース: Azure Portal でワークスペースを作成します。ワークスペースの作成については、「Log Analytics ワークスペースの作成」を参照してください。収集したログとデータの情報は、ワークスペースに保存されます。ワークスペースは、一意のワークスペース ID とリソース ID を持っています。ワークスペース名は、特定のリソースグループに対して固有のものにする必要があります。ワークスペースを作成した後、データがワークスペースに保存されるようにデータソースとソリューションを構成します。
- モニター拡張機能を許可リストに登録しました: 拡張機能`AzureMonitorWindowsAgent`および`AzureMonitorLinuxAgent`が、Citrix が定義している許可リストに登録されました。許可リストに登録されている拡張機能の一覧を表示するには、PowerShell コマンド`Get-ProvMetadataConfiguration`を使用します。
- マスターイメージ: Microsoft では、既存のマシンから新しいマシンを作成する前に、既存のマシンから拡張機能を削除することを推奨しています。拡張子を削除しないと、ファイルが残ったり、予期しない動作が行われたりする可能性があるからです。詳しくは、「既存の VM を再作成する場合」を参照してください。

PowerShell を使用して AMA を有効にしたカタログを作成する方法については、「AMA を有効にしたカタログ VM のプロビジョニング」を参照してください。

Azure Confidential VM

Azure Confidential Computing VM によって、仮想デスクトップは確実にメモリ内で暗号化され、使用中に保護されます。

MCS を使用して、Azure Confidential VM を含むカタログを作成できます。このようなカタログを作成するには、マシンプロファイルワークフローを使用する必要があります。VM と ARM テンプレートスペックの両方をマシンプロファイル入力として使用できます。

Confidential VM に関する重要な考慮事項

サポートされる VM サイズと、Confidential VM を含むマシンカタログの作成に関する重要な考慮事項は次のとおりです:

- サポートされる VM サイズ: Confidential VM は次の VM サイズをサポートします:
  - DCasv5 シリーズ
  - DCadsv5 シリーズ
  - ECasv5 シリーズ
  - ECadsv5 シリーズ
- Confidential VM を含むマシンカタログを作成します。
  - 完全な構成インターフェイスと PowerShell コマンドを使用することで、Azure Confidential VM を使用してマシンカタログを作成できます。
  - Azure Confidential VM でマシンカタログを作成するには、マシンプロファイルベースのワークフローを使用する必要があります。VM またはテンプレートスペックをマシンプロファイルの入力として使用できます。
  - マスターイメージとマシンプロファイル入力は両方とも同じ機密のセキュリティの種類で有効にする必要があります。セキュリティの種類は次のとおりです:
    - VMGuestStateOnly: VM ゲスト状態のみが暗号化された Confidential VM
    - DiskWithVMGuestState: OS ディスクと VM ゲスト状態の両方がプラットフォーム管理キーまたは顧客管理キーで暗号化された Confidential VM。通常の OS ディスクとエフェメラル OS ディスクの両方を暗号化できます。
  - AdditionalData パラメーターを使用すると、管理対象ディスク、スナップショット、Azure Compute Gallery イメージ、VM、ARM テンプレートスペックなど、さまざまなリソースの種類の Confidential VM 情報を取得できます。例:

    ```
    PS C:\Users\username> (get-item XDHyp:\HostingUnits\mynetwork
       \image.folder\username-dev-testing-rg.resourcegroup\
       username-dev-tsvda.vm).AdditionalData
    <!--NeedCopy-->
    ```

    追加のデータフィールドは次のとおりです:
    - DiskSecurityType
    - ConfidentialVMDiskEncryptionSetId
    - DiskSecurityProfiles

    マシンサイズの Confidential Computing プロパティを取得するには、次のコマンドを実行します: `(Get-Item -path "XDHyp:\Connections\my-connection-name\East US.region\serviceoffering.folder\abc.serviceoffering").AdditionalData`

追加のデータフィールドは`ConfidentialComputingType`です。

- マスターイメージまたはマシンプロファイルを機密のセキュリティの種類から機密以外のセキュリティ種類に、または機密以外のセキュリティに酒類から機密のセキュリティの種類に変更することはできません。
- 構成が正しくない場合は、適切なエラーメッセージが表示されます。

マスターイメージとマシンプロファイルを準備する

Confidential VM のセットを作成する前に、次の手順に従ってそれらのマスターイメージとマシンプロファイルを準備します:

1. Azure ポータルで、次のような特定の設定で Confidential VM を作成します:
   - セキュリティの種類: Confidential VM
   - **OS** ディスクの機密暗号化: 有効になっています。
   - キー管理: プラットフォーム管理キーを使用した機密ディスクの暗号化
     Confidential VM の作成について詳しくは、こちらの Microsoft の記事を参照してください。
2. 作成した VM 上でマスターイメージを準備します。作成した VM 上で必要なアプリケーションと VDA をインストールします。

   > 注:
   >
   > VHD を使用した Confidential VM の作成はサポートされていません。代わりに、Azure Compute Gallery、Managed Disks、またはスナップショットを使用します。

3. 次のいずれかの方法でマシンプロファイルを作成します:
   - 手順 1 で作成した既存の VM に必要なマシンプロパティがある場合は、それを使用します。
   - マシンプロファイルとして ARM テンプレートスペックを選択する場合は、必要に応じてテンプレートスペックを作成します。具体的には、*SecurityEncryptionType* や *diskEncryptionSet*（顧客管理キーの場合）など、Confidential VM の要件を満たすパラメーターを構成します。詳しくは、「Azure テンプレートスペックの作成」を参照してください。

     > 注:
     >
     > - マスターイメージとマシンプロファイルのセキュリティキーの種類が同じであることを確認します。
     > - 顧客管理キーを使用して OS ディスクの機密暗号化を必要とする Confidential VM を作成するには、マスターイメージとマシンプロファイルの両方のディスク暗号化セット ID が同一であることを確認します。

完全な構成または **PowerShell** コマンドを使用して **Confidential VM** を作成する

Confidential VM のセットを作成するには、マスターイメージと、目的の Confidential VM に基づくマシンプロファイルを使用してマシンカタログを作成します。

完全な構成を使用してカタログを作成するには、「マシンカタログの作成」で説明されている手順に従います。次の考慮事項に留意してください:

- [イメージ] ページで、Confidential VM の作成用に準備したマスターイメージとマシンプロファイルを選択します。マシンプロファイルの選択は必須であり、選択したマスターイメージと同じセキュリティ暗号化の種類に一致するプロファイルのみが選択可能です。
- [仮想マシン] ページでは、Confidential VM をサポートするマシンサイズのみが選択肢に表示されます。
- [ディスク設定] ページでは、選択したマシンプロファイルから継承されるため、ディスク暗号化セットを指定することはできません。

PowerShell の使用

このセクションでは、PowerShell を使用して次のタスクを実行する方法について説明します:

- PowerShell を使用したカタログの作成または更新でテンプレートスペックを使用する
- Azure VM の拡張機能の有効化
- トラステッド起動を使用したマシンカタログ
- マシンプロファイルのプロパティ値を使用する
- PowerShell を使用したアベイラビリティゾーンの構成
- Azure 専用ホストへの VM のプロビジョニング
- ストレージの種類の構成
- ゾーン冗長ストレージの有効化
- マシンプロファイルから VM および NIC の診断設定をキャプチャする
- Windows ライセンスの確認
- Linux ライセンスの構成
- Azure エフェメラルディスクを使用したマシンカタログの作成
- Azure Compute Gallery を構成する
- VM ごとに複数の NIC を含むカタログを作成または更新する
- 非永続的なライトバックキャッシュディスクのマシンカタログを作成する
- 永続的なライトバックキャッシュディスクのマシンカタログを作成する
- MCSIO による起動パフォーマンスの向上
- 顧客管理暗号キーを使用したマシンカタログの作成
- ホスト機能での暗号化を使用してマシンカタログを作成する
- 二重暗号化を使用したマシンカタログの作成
- ページファイルの場所の決定
- ページファイル設定シナリオ

- ページファイル設定を指定する
- ページファイル設定を変更する
- AMA を有効にしたカタログ VM をプロビジョニングする
- Azure Spot VM を使用したカタログの作成
- すべてのリソースのタグをコピーする

PowerShell を使用したカタログの作成または更新でテンプレートスペックを使用する

テンプレートスペックをマシンプロファイルの入力に使用して、MCS マシンカタログを作成または更新できます。これを行う場合、完全な構成 インターフェイスまたは PowerShell コマンドを使用できます。

完全な構成インターフェイスについては、「完全な構成インターフェイスで Azure Resource Manager イメージを使用してマシンカタログを作成する」を参照してください。

PowerShell コマンドを使用する:

1. **PowerShell** ウィンドウを開きます。
2. `asnp citrix*`を実行します。
3. カタログを作成または更新します。

    - カタログを作成するには:

        a) マシンプロファイルの入力で、テンプレートスペックを`New-ProvScheme`コマンドとともに使用します。例:

        ```
        New-ProvScheme -MasterImageVM "XDHyp:/HostingUnits/azure/
            image.folder/fgthj.resourcegroup/nab-ws-
            vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
        MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.
            folder/fgthj.resourcegroup/test.templatespec/V1.
            templatespecversion"
        -ProvisioningSchemeName <String>
        -HostingUnitName <String>
        -IdentityPoolName <String>
        [-ServiceOffering <String>][-CustomProperties <String>]
        [<CommonParameters>]
        <!--NeedCopy-->
        ```

        b) カタログの作成を完了します。

    - カタログを更新するには、マシンプロファイルの入力で、テンプレートスペックを`Set-ProvScheme`コマンドとともに使用します。例:

        ```
        Set-ProvScheme -MasterImageVm 'XDHyp://Connections/Azure/East
            Us.region/vm.folder/MasterDisk.vm'
        MachineProfile 'XDHyp:/HostingUnits/azure/machineprofile.
            folder/fgthj.resourcegroup/testing.templatespec/V1.
            templatespecversion'
        [-ProvisioningSchemeName] <String>
        ```



```
    [-CustomProperties <String>][-ServiceOffering <String>] [-
        PassThru]
    [<CommonParameters>]
    <!--NeedCopy-->
```

Azure VM の拡張機能の有効化

ARM（Azure Resource Manager）テンプレートスペックを選択したら、次の PowerShell コマンドを実行して、Azure VM（仮想マシン）拡張機能を操作します：

- サポートされている Azure VM 拡張機能の一覧を表示するには：`Get-ProvMetadataConfiguration`
- さらに VM 拡張機能を追加するには：`Add-ProvMetadataConfiguration`。例：`Add-ProvMetadataConfiguration -PluginType "AzureRM"-ConfigurationName "Extension"-ConfigurationValue "CustomScriptExtension"`

  次のいずれかを追加しようとするとコマンドが失敗し、エラーメッセージが表示されます：

  - Citrix 定義の拡張機能。
  - 既存のユーザー定義の拡張機能。
  - サポートされていない構成キー。現在、サポートされている構成キーは`Extension`です。
- 一覧から拡張機能を削除するには：`Remove-ProvMetadataConfiguration`。追加した拡張機能は削除できます。

トラステッド起動を使用したマシンカタログ

トラステッド起動でマシンカタログを正常に作成するには、次を使用します：

- トラステッド起動を使用したマシンプロファイル
- トラステッド起動をサポートする VM サイズ
- トラステッド起動をサポートする Windows VM バージョン。現在、Windows 10、Windows 11、Windows Server 2016、2019、および 2022 はトラステッド起動をサポートしています。

> 重要：
>
> MCS は、トラステッド起動が有効な VM を使用した新しいカタログの作成をサポートしています。ただし、既存の永続カタログと既存の VM を更新するには、Azure Portal を使用する必要があります。非永続カタログのトラステッド起動を更新することはできません。詳しくは、Microsoft ドキュメント「既存の Azure VM でトラステッド起動を有効にする」を参照してください。

Citrix DaaS オファリングのインベントリアイテムを表示し、VM サイズがトラステッド起動をサポートしているかどうかを判断するには、次のコマンドを実行します：

1. PowerShell ウィンドウを開きます。
2. **asnp citrix*** を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. 次のコマンドを実行します:

```
$s = (ls XDHyp:\HostingUnits<name of hosting unit>\serviceoffering
    .folder"<VM size>".serviceoffering)
<!--NeedCopy-->
```

4. `$s | select -ExpandProperty Additionaldata`を実行します
5. `SupportsTrustedLaunch`属性の値を確認してください。
   - `SupportsTrustedLaunch`が **True** の場合、VM サイズはトラステッド起動をサポートします。
   - `SupportsTrustedLaunch`が **False** の場合、VM サイズはトラステッド起動をサポートしません。

Azure の PowerShell に従って、次のコマンドを使用してトラステッド起動をサポートする VM サイズを決定できます:

```
(Get-AzComputeResourceSku | where {
 $_.Locations.Contains($region) -and ($_.Name -eq "<VM size>")  }
 )[0].Capabilities
<!--NeedCopy-->
```

以下は、「Azure PowerShell コマンドを実行した後、VM サイズがトラステッド起動をサポートするかどうか」について示した例です。

- 例 *1*: Azure VM が第 1 世代のみをサポートしている場合、その VM はトラステッド起動をサポートしていません。したがって、Azure PowerShell コマンドを実行した後、`TrustedLaunchDisabled`機能は表示されません。
- 例 *2*: Azure VM が第 2 世代のみをサポートし、`TrustedLaunchDisabled`機能が **True** の場合、第 2 世代の VM サイズはトラステッド起動ではサポートされません。
- 例 *3*:Azure VM が第 2 世代のみをサポートし、PowerShell コマンドの実行後に`TrustedLaunchDisabled`機能が表示されない場合、第 2 世代の VM サイズはトラステッド起動でサポートされます。

Azure 仮想マシンのトラステッド起動ついて詳しくは、Microsoft のドキュメント「Azure Virtual Machines のトラステッド起動」を参照してください。

トラステッド起動を使用したマシンカタログの作成

1. トラステッド起動が有効になっているマスターイメージを作成します。Microsoft のドキュメント「トラステッド起動 VM イメージ」を参照してください。
2. セキュリティの種類をトラステッド起動 **VM** として VM またはテンプレートスペックを作成します。VM またはテンプレートスペックの作成について詳しくは、Microsoft ドキュメント「トラステッド起動の VM をデプロイする」を参照してください。

3. 完全な構成インターフェイスまたは PowerShell コマンドを使用して、マシンカタログを作成します。

   - 完全な構成インターフェイスを使用する場合、「完全な構成インターフェイスで Azure Resource Manager イメージを使用してマシンカタログを作成する」を参照してください。
   - PowerShell コマンドを使用する場合は、New-ProvSchemeコマンドを使用し、マシンプロファイルの入力に VM またはテンプレートスペックを指定します。カタログ作成コマンドの完全な一覧については、「Creating a catalog」を参照してください。

     マシンプロファイルの入力に VM を使用したNew-ProvSchemeの例:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name" -
    IdentityPoolName "name" -InitialBatchSizeHint 1
-MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/fgthj.
    resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
-MachineProfile "XDHyp:\HostingUnits<adnet>\machineprofile.
    folder<def.resourcegroup><machine profile vm.vm>"
-ProvisioningSchemeName <String>
-HostingUnitName <String>
-IdentityPoolName <String>
[-ServiceOffering <String>][-CustomProperties <String>]
[<CommonParameters>]
<!--NeedCopy-->
```

     マシンプロファイルの入力にテンプレートスペックを使用したNew-ProvSchemeの場合:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name" -
    IdentityPoolName "name" -InitialBatchSizeHint 1
-MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/fgthj.
    resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.
    folder/fgthj.resourcegroup/test.templatespec/V1.
    templatespecversion"
-ProvisioningSchemeName <String>
-HostingUnitName <String>
-IdentityPoolName <String>
[-ServiceOffering <String>][-CustomProperties <String>]
[<CommonParameters>]
<!--NeedCopy-->
```

トラステッド起動でマシンカタログを作成する際のエラー

トラステッド起動を使用してマシンカタログを作成しているときに、次のシナリオに応じたエラーが発生します:

シナリオ	エラー
非管理対象カタログの作成中にマシンプロファイルを選択した場合	MachineProfileNotSupportedForUnmanagedCata

シナリオ	エラー
非管理対象ディスクをマスターイメージとしてカタログを作成するときに、トラステッド起動をサポートするマシンプロファイルを選択した場合	SecurityTypeNotSupportedForUnmanagedDisk
セキュリティの種類でトラステッド起動を使用し、マスターイメージソースを使用して管理カタログを作成するときに、マシンプロファイルを選択しない場合	MachineProfileNotFoundForTrustedLaunchMaste
マスターイメージとは異なるセキュリティの種類のマシンプロファイルを選択した場合	SecurityTypeConflictBetweenMasterImageAndMa
トラステッド起動をサポートしない VM サイズを選択しながら、カタログの作成時にトラステッド起動をサポートするマスターイメージを使用する場合	MachineSizeNotSupportTrustedLaunch

マシンプロファイルのプロパティ値を使用する

マシンカタログは、カスタムプロパティで定義されている次のプロパティを使用します:

- アベイラビリティゾーン
- 専用ホストグループ ID
- ディスク暗号化セット ID
- OS の種類
- ライセンスの種類
- ストレージの種類

これらのカスタムプロパティが明示的に定義されていない場合、プロパティ値はマシンプロファイルとして使用されている ARM テンプレートスペックの指定または仮想マシンのいずれかから設定されます。また、ServiceOfferingが指定されていない場合は、マシンプロファイルから設定されます。

> 注:
>
> 一部のプロパティがマシンプロファイルで指定されておらず、カスタムプロパティで定義されていないとき、プロパティのデフォルト値が常に適用されます（該当する場合）。

次のセクションでは、CustomPropertiesですべてのプロパティが定義されている場合、または値が MachineProfile から由来している場合、New-ProvSchemeおよびSet-ProvSchemeでのシナリオについて説明します。

- New-ProvScheme シナリオ
  - MachineProfile ですべてのプロパティが定義され、CustomProperties は定義されていません。例:


```
New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpA.vm"
```

カタログのカスタムプロパティとして、次の値が設定されています:

```
1  Get-ProvScheme | select CustomProperties
2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
      machinecreation" xmlns:xsi="http://www.w3.org/2001/
      XMLSchema-instance">
3  <Property xsi:type="StringProperty" Name="StorageAccountType"
       Value="<mpA-value>"/>
4  <Property xsi:type="StringProperty" Name="OSType" Value="<mpA
      -value>"/>
5  <Property xsi:type="StringProperty" Name="LicenseType" Value=
      "<mpA-value>"/>
6  <Property xsi:type="StringProperty" Name="DiskEncryptionSetId
      " Value="<mpA-value>"/>
7  <Property xsi:type="StringProperty" Name="
      DedicatedHostGroupId" Value="<mpA-value>"/>
8  <Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
      value>"/>
9  </CustomProperties>
10 <!--NeedCopy-->
```

- MachineProfile で一部のプロパティが定義され、CustomProperties は定義されていません。例: MachineProfile には LicenseType と OsType のみが含まれます。

  ```
  New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
  \machineprofile.folder\azure.resourcegroup\mpA.vm"
  ```

  カタログのカスタムプロパティとして、次の値が設定されています:

  ```
  1  Get-ProvScheme | select CustomProperties
  2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
        machinecreation" xmlns:xsi="http://www.w3.org/2001/
        XMLSchema-instance">
  3  <Property xsi:type="StringProperty" Name="OSType" Value="<mpA
        -value>"/>
  4  <Property xsi:type="StringProperty" Name="LicenseType" Value=
        "<mpA-value>"/>
  5  </CustomProperties>
  6  <!--NeedCopy-->
  ```

- MachineProfile と CustomProperties の両方がすべてのプロパティを定義します。例:

  ```
  New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
  \machineprofile.folder\azure.resourcegroup\mpA.vm"-CustomProperties
   $CustomPropertiesA
  ```

  カスタムプロパティが優先されます。カタログのカスタムプロパティとして、次の値が設定されています:


```
Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/
    XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageAccountType"
     Value="<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="OSType" Value="<
    CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
    "<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId
    " Value="<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="
    DedicatedHostGroupId" Value="<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="Zones" Value="<
    CustomPropertiesA-value>"/>
</CustomProperties>
<!--NeedCopy-->
```

- 一部のプロパティは MachineProfile で定義され、一部のプロパティは CustomProperties で定義されます。例:

  * CustomProperties は、LicenseType と StorageAccountType を定義します
  * MachineProfile は、LicenseType、OsType、Zones を定義します

  ```
  New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
  \machineprofile.folder\azure.resourcegroup\mpA.vm"-CustomProperties
   $CustomPropertiesA
  ```

  カタログのカスタムプロパティとして、次の値が設定されています:

  ```
  Get-ProvScheme | select CustomProperties
  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
      machinecreation" xmlns:xsi="http://www.w3.org/2001/
      XMLSchema-instance">
  <Property xsi:type="StringProperty" Name="StorageAccountType"
       Value="<CustomPropertiesA-value>"/>
  <Property xsi:type="StringProperty" Name="OSType" Value="<mpA
      -value>"/>
  <Property xsi:type="StringProperty" Name="LicenseType" Value=
      "<CustomPropertiesA-value>"/>
  <Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
      value>"/>
  </CustomProperties>
  <!--NeedCopy-->
  ```

- 一部のプロパティは MachineProfile で定義され、一部のプロパティは CustomProperties で定義されます。また、ServiceOffering は定義されていません。例:

  * CustomProperties は StorageType を定義します
  * MachineProfile は LicenseType を定義します


```
New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
    \machineprofile.folder\azure.resourcegroup\mp.vm"
-ServiceOffering "XDHyp:\HostingUnits\azureunit\
    serviceoffering.folder<explicit-machine-size>.
    serviceoffering"
<!--NeedCopy-->
```

カタログのカスタムプロパティとして、次の値が設定されています:

```
Get-ProvScheme | select ServiceOffering
serviceoffering.folder<explicit-machine-size>.serviceoffering

Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/
    XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageAccountType"
     Value="explicit-storage-type"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
    "value-from-machineprofile"/>
</CustomProperties>
<!--NeedCopy-->
```

- OsType が CustomProperties にも MachineProfile にもない場合、次のようになります:
  - 値はマスターイメージから読み取られます。
  - マスターイメージが非管理対象ディスクの場合、OsType は Windows に設定されます。例:

```
New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpA.vm"-MasterImageVM
 "XDHyp:\HostingUnits\azureunit\image.folder\linux-master-
image.manageddisk"
```

マスターイメージの値は、カスタムプロパティに書き込まれます（この場合は Linux)。

```
Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/
    XMLSchema-instance">
<Property xsi:type="StringProperty" Name="OSType" Value="
    Linux"/>
</CustomProperties>
<!--NeedCopy-->
```

- Set-ProvScheme シナリオ
  - 既存のカタログ:
    - `StorageAccountType`および OsType の CustomProperties
    - Zones を定義する MachineProfile `mpA.vm`

- 更新:
  - StorageAccountType を定義する MachineProfile mpB.vm
  - LicenseType と OsType を定義するカスタムプロパティの新しいセット $CustomPropertiesB

```
Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpB.vm"-CustomProperties
 $CustomPropertiesB
```

カタログのカスタムプロパティとして、次の値が設定されています:

```
1  Get-ProvScheme | select CustomProperties
2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
      machinecreation" xmlns:xsi="http://www.w3.org/2001/
      XMLSchema-instance">
3  <Property xsi:type="StringProperty" Name="StorageAccountType"
       Value="<mpB-value>"/>
4  <Property xsi:type="StringProperty" Name="OSType" Value="<
      CustomPropertiesB-value>"/>
5  <Property xsi:type="StringProperty" Name="LicenseType" Value=
      "<CustomPropertiesB-value>"/>
6       </CustomProperties>
7  <!--NeedCopy-->
```

- 既存のカタログ:
  - StorageAccountTypeおよび OsType の CustomProperties
  - StorageAccountType と LicenseType を定義する MachineProfile mpA.vm

- 更新:
  - StorageAccountType と OsType を定義するカスタムプロパティの新しいセット $Custom-PropertiesB

```
Set-ProvScheme -CustomProperties $CustomPropertiesB
```

カタログのカスタムプロパティとして、次の値が設定されています:

```
1  Get-ProvScheme | select CustomProperties
2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
      machinecreation" xmlns:xsi="http://www.w3.org/2001/
      XMLSchema-instance">
3  <Property xsi:type="StringProperty" Name="StorageAccountType"
       Value="<CustomPropertiesB-value>"/>
4  <Property xsi:type="StringProperty" Name="OSType" Value="<
      CustomPropertiesB-value>"/>
5  <Property xsi:type="StringProperty" Name="LicenseType" Value=
      "<mp-A-value>"/>
6  </CustomProperties>
7  <!--NeedCopy-->
```

- 既存のカタログ:

    * StorageAccountTypeおよび OsType の CustomProperties
    * Zones を定義する MachineProfile mpA.vm

  - 更新:

    * StorageAccountType と LicenseType を定義する MachineProfile mpB.vm
    * ServiceOfferingは指定されていません

    ```
    Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
    \machineprofile.folder\azure.resourcegroup\mpB.vm"
    ```

    カタログのカスタムプロパティとして、次の値が設定されています:

    ```
    1  Get-ProvScheme | select ServiceOffering
    2  serviceoffering.folder<value-from-machineprofile>.
           serviceoffering
    3
    4  Get-ProvScheme | select CustomProperties
    5  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
           machinecreation" xmlns:xsi="http://www.w3.org/2001/
           XMLSchema-instance">
    6  <Property xsi:type="StringProperty" Name="StorageAccountType"
            Value="<mpB-value>"/>
    7  <Property xsi:type="StringProperty" Name="OSType" Value="<
           prior-CustomProperties-value>"/>
    8  <Property xsi:type="StringProperty" Name="LicenseType" Value=
           "<mpB-value>"/>
    9  </CustomProperties>
    10 <!--NeedCopy-->
    ```

PowerShell を使用したアベイラビリティゾーンの構成

PowerShell を使用する場合、Get-Itemで Citrix DaaS オファリングのインベントリアイテムを表示できます。たとえば、米国東部リージョン Standard_B1lsのサービスオファリングを表示するには、以下を実行します:

```
1  $serviceOffering = Get-Item -path "XDHyp:\Connections\my-connection-
       name\East US.region\serviceoffering.folder\Standard_B1ls.
       serviceoffering"
2  <!--NeedCopy-->
```

ゾーンを表示するには、アイテムのAdditionalDataパラメーターを使用します:

```
$serviceOffering.AdditionalData
```

アベイラビリティゾーンが指定されていない場合、マシンのプロビジョニング方法に変更はありません。

PowerShell を使用してアベイラビリティゾーンを構成するには、New-ProvScheme操作で、使用可能な **Zones** カスタムプロパティを使用します。**Zones** プロパティは、マシンをプロビジョニングするアベイラビリティゾーンの一覧を定義します。これらのゾーンには、1 つまたは複数のアベイラビリティゾーンを含めることが

できます。たとえば、Zones 1 と 3 の場合は、<Property xsi:type="StringProperty"Name="Zones"Value="1, 3"/> のようになります。

Set-ProvSchemeコマンドを使用して、プロビジョニングスキームのゾーンを更新します。

無効なゾーンが指定された場合、プロビジョニングスキームは更新されず、無効なコマンドを修正する方法を示すエラーメッセージが表示されます。

> ヒント:
>
> 無効なカスタムプロパティを指定すると、プロビジョニングスキームは更新されず、関連するエラーメッセージが表示されます。

ホストグループゾーンと **Azure Availability Zones** の同時使用の結果

カスタムプロパティで指定されたアベイラビリティゾーンとホストグループのゾーンに基づいて、マシンカタログの作成が成功するかどうかを評価する事前チェックがあります。アベイラビリティゾーンのカスタムプロパティがホストグループのゾーンと一致しない場合、カタログの作成は失敗します。

PowerShell を使用してアベイラビリティゾーンを構成する方法については、「PowerShell を使用したアベイラビリティゾーンの構成」を参照してください。

Azure 専用ホストについて詳しくは、「Azure 専用ホスト」を参照してください。

次の表は、アベイラビリティゾーンとホストグループゾーンのさまざまな組み合わせと、マシンカタログの作成が成功または失敗する結果を示しています。

ホストグループゾーン	カスタムプロパティの **Azure** アベイラビリティゾーン	マシンカタログの作成結果
指定。たとえば、ホストグループはゾーン 1 にあります	指定なし	成功。マシンはホストグループのゾーンに作成されます
指定。たとえば、ホストグループはゾーン 1 にあります	ホストグループゾーンと同じゾーン。たとえば、カスタムプロパティのゾーンは 1 に設定されます	成功。マシンはゾーン 1 に作成されます
指定。たとえば、ホストグループはゾーン 1 にあります	ホストグループゾーンとは異なります。たとえば、カスタムプロパティのゾーンは 2 に設定されます	指定されたアベイラビリティゾーンとホストグループのゾーンが一致しないため、事前チェック中に関連するエラーが発生してカタログの作成が失敗します
指定。たとえば、ホストグループはゾーン 1 にあります	複数のゾーンが指定されました。たとえば、カスタムプロパティのゾーンは 1、2 または 2、3 に設定されます	指定されたアベイラビリティゾーンとホストグループのゾーンが一致しないため、事前チェック中に関連するエラーが発生してカタログの作成が失敗します

ホストグループゾーン	カスタムプロパティの **Azure** アベイラビリティゾーン	マシンカタログの作成結果
指定なし。たとえば、ホスト グループのゾーンはNoneです	指定なし	指定したアベイラビリティゾーンとホストグループのゾーンが一致する（つまり、ゾーンがない）ため、カタログの作成は成功します。マシンはどのゾーンにも作成されません
指定なし。たとえば、ホスト グループのゾーンはNoneです	指定。たとえば、カスタムプロパティのゾーンは 1 つまたは複数のゾーンに設定されます	指定されたアベイラビリティゾーンとホストグループのゾーンが一致しないため、事前チェック中に関連するエラーが発生してカタログの作成が失敗します

Azure 専用ホストへの **VM** のプロビジョニング

MCS を使用して、Azure 専用ホストで VM をプロビジョニングできます。Azure 専用ホストで VM をプロビジョニングする前に、以下を実行します:

- ホストグループを作成します。
- そのホストグループにホストを作成します。
- カタログと仮想マシンを作成するために十分なホスト容量が確保されていることを確認してください。

管理者は、次の PowerShell スクリプトで定義されたホストテナントを持つマシンのカタログを作成できます:

```
1 New-ProvScheme <otherParameters> -CustomProperties '<CustomProperties
     xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi
     ="http://www.w3.org/2001/XMLSchema-instance">
2  <Property xsi:type="StringProperty" Name="HostGroupId" Value="
      myResourceGroup/myHostGroup" />
3  ...other Custom Properties...
4  </CustomProperties>
5 <!--NeedCopy-->
```

MCS を使用して、Azure 専用ホストで仮想マシンをプロビジョニングする場合、次の点を考慮してください:

- 専用ホストはカタログプロパティであり、カタログの作成後に変更することはできません。専用テナントは現在、Azure ではサポートされていません。
- HostGroupIdパラメーターを使用する場合は、ホスティングユニットの領域に事前構成された Azure ホストグループが必要です。
- Azure の自動配置が必要です。この機能は、ホストグループに関連付けられたサブスクリプションをオンボードするように要求します。詳しくは、「Azure 専用ホストの VM スケールセット - パブリックプレビュー」を参照してください。自動配置が有効になっていない場合、MCS はカタログの作成中にエラーをスローします。

ストレージの種類の構成

MCS を使用する Azure 環境の仮想マシン用に異なるストレージの種類を選択します。ターゲット VM の場合、MCS は以下をサポートします:

- OS ディスク: プレミアム SSD、SSD または HDD
- ライトバックキャッシュディスク: プレミアム SSD、SSD、または HDD

これらのストレージの種類を使用するときは、次の点を考慮してください:

- VM が選択したストレージの種類をサポートしていることを確認してください。
- 構成で Azure エフェメラルディスクを使用している場合、ライトバックキャッシュディスク設定のオプションは使用できません。

> ヒント:
>
> StorageTypeは、OS タイプとストレージアカウント用に構成されています。WBCDiskStorageTypeは、ライトバックキャッシュのストレージの種類用に構成されています。通常のカタログの場合、StorageTypeが必要です。WBCDiskStorageTypeが構成されていない場合は、WBCDiskStorageTypeのデフォルトとしてStorageTypeが使用されます。

WBCDiskStorageType が構成されていない場合、WBCDiskStorageType のデフォルトとして StorageType が使用されます

VM のストレージの種類の構成

VM 用のストレージの種類を構成するには、New-ProvSchemeのStorageTypeパラメーターを使用します。既存カタログのStorageTypeパラメーター値を、サポートされているストレージ種類の 1 つに更新するには、Set-ProvSchemeコマンドを使用します。

以下は、プロビジョニングスキームで使用するCustomPropertiesパラメーターのセットの例です:

```
1 Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
     <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
      />
3 <Property xsi:type="StringProperty" Name="StorageType" Value="
     Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="LicenseType" Value="
     Windows_Client" />
5 </CustomProperties>'
6 <!--NeedCopy-->
```


ゾーン冗長ストレージの有効化

カタログの作成中にゾーン冗長ストレージを選択できます。ゾーン冗長ストレージは複数のアベイラビリティゾーンにわたって Azure Managed Disks を同期的に複製するため、別のゾーンの冗長を利用して、ゾーンでの障害から回復できます。

ストレージの種類のカスタムプロパティで **Premium_ZRS** および **StandardSSD_ZRS** を指定できます。ZRS ストレージは、既存のカスタムプロパティを使用するか、**MachineProfile** テンプレートを使用して設定できます。ZRS ストレージは、`-StartsNow`および`-DurationInMinutes -1`パラメーターを指定した`Set-ProvVMUpdateTimeWindow`コマンドでもサポートされます。既存の VM を LRS ストレージから ZRS ストレージに変更できるのです。

> 注:
>
> - `StartsNow`は、スケジュールの開始時刻が現在時刻であることを指定します。
> - 負の数（-1 など）の`DurationInMinutes`は、スケジュールの期間に上限がないことを示します。

制限事項:

- 管理対象ディスクでのみサポートされます
- プレミアムおよびスタンダードのソリッドステートドライブ（SSD）でのみサポートされます
- `StorageTypeAtShutdown`ではサポートされません
- 特定のリージョンでのみ利用できます。
- ZRS ディスクを大量に作成すると、Azure のパフォーマンスが低下します。したがって、最初の電源投入時には、小規模なバッチ（一度に 300 台未満のマシン）ごとにマシンの電源をオンにします。

ゾーン冗長ストレージをディスクストレージの種類として設定する

最初のカタログ作成時にゾーン冗長ストレージを選択するか、既存のカタログでストレージの種類を更新できます。

PowerShell コマンドを使用してゾーン冗長ストレージを選択する

`New-ProvScheme` Powershell コマンドを使用して Azure で新しいカタログを作成するときは、`StorageAccountType`の値として`Standard_ZRS`を使用します。
例:

```
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    StandardSSD_ZRS" />
<!--NeedCopy-->
```

この値を設定すると、適切に使用できるかどうかを判断する動的 API によって検証されます。ZRS の使用がカタログで有効でない場合、次の例外が発生する可能性があります:

- **StorageTypeAtShutdownNotSupportedForZrsDisks**：StorageTypeAtShutdown カスタムプロパティは、ZRS ストレージでは使用できません。
- **StorageAccountTypeNotSupportedInRegion**：この例外は、ZRS をサポートしていない Azure リージョンで ZRS ストレージを使用しようとすると発生します。
- **ZrsRequiresManagedDisks**：ゾーン冗長ストレージは、管理対象ディスクでのみ使用できます。

次のカスタムプロパティを使用して、ディスクストレージの種類を設定できます：

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`

> 注：
>
> カスタムプロパティが設定されていない場合、カタログの作成中にマシンプロファイルの OS ディスク（`StorageType`）が使用されます。

マシンプロファイルから **VM** および **NIC** の診断設定をキャプチャする

マシンカタログの作成中、既存のマシンカタログの更新中、および既存の VM の更新中に、マシンプロファイルから VM および NIC の診断設定をキャプチャできます。

VM またはテンプレートスペックをマシンプロファイルのソースとして使用できます。

主な手順

1. Azure で必要な ID を設定します。これらの ID をテンプレートスペックで指定する必要があります。
    - ストレージアカウント
    - Log Analytics ワークスペース
    - 標準レベルの料金設定のイベントハブ名前空間
2. マシンプロファイルのソースを作成します。
3. 新しいマシンカタログを作成するか、既存のカタログを更新するか、既存の VM を更新します。

Azure で必要な **ID** を設定する

Azure で次のいずれかを設定します：

- ストレージアカウント
- Log Analytics ワークスペース
- 標準レベルの料金設定のイベントハブ名前空間

ストレージアカウントをセットアップする　Azure で標準ストレージアカウントを作成します。テンプレートスペックでは、ストレージアカウントの完全な resourceId を`storageAccountId`として指定します。

データをストレージアカウントに記録するように VM を設定すると、データは`insights-metrics-pt1m`コンテナの下に表示されます。

Log Analytics ワークスペースをセットアップする　Log Analytics ワークスペースを作成します。テンプレートスペックでは、Log Analytics ワークスペースの完全な resourceId を workspaceId として指定します。

ワークスペースにデータを記録するように VM を設定すると、Azure のログでデータを照会できるようになります。ログで Azure の次のコマンドを実行すると、リソースによって記録されたすべてのメトリックの数を表示できます:

‘AzureMetrics
| summarize Count=count() by ResourceId# Microsoft Azure カタログの作成

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

「マシンカタログの作成」では、マシンカタログを作成するウィザードについて説明します。以下の情報は、Microsoft Azure Resource Manager クラウド環境に固有の詳細について説明しています。

> 注:
>
> Microsoft Azure カタログを作成する前に、Microsoft Azure への接続の作成を完了する必要があります。「Microsoft Azure への接続」を参照してください。

マシンカタログの作成

マシンカタログは次の 2 つの方法で作成できます。

- ［完全な構成］インターフェイス。
- PowerShell。「Manage Citrix DaaS using Remote PowerShell SDKs」を参照してください。PowerShell を使用して特定の機能を実装する方法については、「PowerShell の使用」を参照してください。

完全な構成インターフェイスと **Azure Resource Manager** イメージを使用してマシンカタログを作成する

これは、「マシンカタログの作成」のガイダンスを補完する情報です。

イメージは、マシンカタログ内に VM を作成するために使用される Azure Compute Gallery 内のイメージ定義のイメージバージョンの場合もあれば、ディスクまたはスナップショットの場合もあります。

マシンカタログを作成する前に、Azure Resource Manager でイメージを作成します。

> 注:
>
> - 非管理ディスクを使用して仮想マシンをプロビジョニングすることは推奨されません。
> - ホスト接続で構成されたリージョンとは異なるリージョンからマスターイメージを使用することに対するサポートは、廃止されました。Azure Compute Gallery を使用して、マスターイメージを目的のリージョンに複製します。

イメージの準備中に、元の仮想マシンに基づいて準備用の仮想マシン（VM）が作成されます。この準備 VM はネットワークから切断されています。ネットワークを準備 VM から切断するために、すべての受信および送信トラフィックを拒否するネットワークセキュリティグループが作成されます。ネットワークセキュリティグループは、自動的にカタログごとに 1 回作成されます。ネットワークセキュリティグループの名前は <!JEKYLL@5180@0> で、GUID がランダムに生成されます。例：<!JEKYLL@5180@1>。

マシンカタログ作成ウィザードで次の操作を行います：

1. ［マシンの種類］ページと ［マシン管理］ページには、Azure 固有の情報は含まれていません。「マシンカタログの作成」のガイダンスに従ってください。
2. ［イメージ］ページで、カタログ内のすべてのマシンのマスターイメージとして使用するイメージを選択します。［イメージの選択］ウィザードが表示されます。イメージを選択するには、次の手順に従います：

   a) (テナント内またはテナント間で共有イメージを使用して構成された接続にのみ適用可能) イメージが存在するサブスクリプションを選択します。
   b) リソースグループの選択
   c) Azure 管理対象ディスク、Azure Compute Gallery、または Azure イメージバージョンに移動します。

   イメージを選択するときは、次の点を考慮してください：

   - Citrix VDA がイメージにインストールされていることを確認します。
   - VM に接続されているディスクを選択した場合は、次の手順に進む前に VM をシャットダウンする必要があります。

   > 注:
   >
   > - カタログにマシンを作成した接続（ホスト）のサブスクリプションは、緑色の点で示されます。他のサブスクリプションは、Azure Compute Gallery をそのサブスクリプションと共有します。これらのサブスクリプションでは、共有ギャラリーのみが表示されます。共有サブスクリプションの構成方法については、「単一のテナント内（サブスクリプション間）での画像の共有」および「テナント間での画像の共有」を参照してください。
   > - トラステッド起動で、Windows でエフェメラル OS ディスクを使用して、プロビジョニングスキームを作成できます。トラステッド起動でイメージを選択する場合は、vTPM が有効になっているトラステッド起動でマシンプロファイルを選択する必要があります。エフェメラル OS ディスクを使用してマシンカタログを作成する方法については、「エフェメラル OS ディスクを使用してマシ

> ンを作成する方法」を参照してください。
> - イメージのレプリケーション中に、先に進んでそのイメージをマスターイメージとして選択し、セットアップを完了することができます。ただし、イメージのレプリケーション中は、カタログ作成完了までの時間が長くなることがあります。MCS では、カタログの作成開始から 1 時間以内にレプリケーションを完了する必要があります。レプリケーションがタイムアウトすると、カタログの作成は失敗します。レプリケーションステータスは Azure で確認できます。レプリケーションがまだ保留中の場合、またはレプリケーションが完了した後で再試行してください。
> - Gen2 イメージを使用して Gen 2 VM カタログをプロビジョニングし、起動時のパフォーマンスを向上させることができます。ただし、Gen1 イメージを使用した Gen2 マシンカタログの作成はサポートされていません。同様に、Gen2 イメージを使用した Gen1 マシンカタログの作成もサポートされていません。また、世代情報を持たない古いイメージはすべて Gen1 イメージです。

カタログ内の VM がマシンプロファイルから構成を継承するかどうかを選択します。デフォルトでは、［マシンプロファイルを使用する（**Azure Active Directory** では必須）］チェックボックスがオンになっています。［マシンプロファイルを選択］を クリックして、リソースグループの一覧から VM または ARM テンプレートスペックを参照します。

VM がマシンプロファイルから継承できる構成の例として、次のようなものがあります:

- 高速ネットワーク
- ブート診断
- ホストのディスクキャッシュ（OS および MCSIO ディスク関連）
- マシンサイズ（別途指定されていない場合）
- VM に適用されたタグ

> 注:
>
> - Azure でマシンカタログのマスターイメージを選択すると、選択されたマスターイメージに基づいてマシンプロファイルがフィルタリングされます。たとえば、マシンプロファイルは、Windows OS、セキュリティの種類、休止のサポート、およびマスターイメージのディスク暗号化セット ID に基づいてフィルタリングされます。
> - トラステッド起動が有効になっているイメージまたはスナップショットを選択する場合は、［セキュリティの種類］としてトラステッド起動が選択されているマシンプロファイルを使用する必要があります。次に、［マシンプロファイル］の値を指定することにより、SecureBoot と vTPM を有効または無効にできます。Azure のトラステッド起動については、「https://docs.microsoft.com/en-us/azure/virtual-machines/trusted-launch」を参照してください。

ARM テンプレートスペックを検証して、マシンカタログを作成するためにマシンプロファイルとして使用できるかどうかを確認します。Azure テンプレートスペックの作成について詳しくは、「Azure テンプレートスペックの作成」を参照してください。

ARM テンプレートスペックを検証する方法は 2 つあります:

- リソースグループの一覧から ARM テンプレートスペックを選択したら、［次へ］をクリックします。ARM テンプレートスペックにエラーがある場合、エラーメッセージが表示されます。
- 次の PowerShell コマンドのいずれかを実行します：
  - <!JEKYLL@5180@2>
  - <!JEKYLL@5180@3>

  例：

  <!JEKYLL@5180@4>

カタログを作成した後、イメージがマシンプロファイルから継承している構成を表示できます。［マシンカタログ］ノードで、カタログを選択して下部ペインに詳細を表示します。次に、［テンプレートのプロパティ］タブをクリックしてマシンプロファイルのプロパティを表示します。［タグ］セクションには、最大 3 つのタグが表示されます。その VM に配置されているすべてのタグを表示するには、［すべて表示］をクリックします。

MCS で Azure 専用ホストに VM をプロビジョニングする場合は、［ホストグループを使用する］チェックボックスをオンにし、リストからホストグループを選択します。ホストグループは、専用ホストのコレクションを表すリソースです。専用ホストは、1 つまたは複数の仮想マシンをホストする物理サーバーを提供するサービスです。サーバーは Azure サブスクリプション専用であり、他のサブスクライバーとは共有されません。専用ホストを使用する場合、Azure は、VM がそのホストで実行されている唯一のマシンであることを保証します。この機能は、規制または内部のセキュリティ要件を満たす必要があるシナリオに適しています。ホストグループとそれらを使用する際の考慮事項について詳しくは、「Azure 専用ホストでの VM のプロビジョニング」を参照してください。

> 重要：
>
> - Azure の自動配置が有効になっているホストグループのみが表示されます。
> - ホストグループを使用すると、ウィザードの後半で表示される［**Virtual Machines**］ページが変更されます。選択したホストグループに含まれるマシンサイズのみが、このページに表示されます。また、アベイラビリティゾーンは自動的に選択され、選択できません。

3. ［ストレージとライセンスの種類］ページは、Azure Resource Manager イメージを使用するときのみ表示されます。

   マシンカタログに使用するストレージの種類は次のとおりです：

   - プレミアム **SSD**：I/O を多用するワークロードを持つ VM に適した、高性能かつ低遅延のディスクストレージオプションを提供します。
   - 標準 **SSD**：低 IOPS レベルで安定したパフォーマンスを必要とするワークロードに適した、コスト効率の高いストレージオプションを提供します。
   - 標準 **HDD**：遅延の影響を受けないワークロードを実行している VM に対して、信頼性の高い低コストのディスクストレージオプションを提供します。
   - **Azure** エフェメラル **OS** ディスク VM のローカルディスクを再利用してオペレーティングシステムディスクをホストする、コスト効率の高いストレージオプションを提供します。または、PowerShell を

使用して、エフェメラル OS ディスクを使用するマシンを作成することもできます。詳しくは、「Azure エフェメラルディスク」を参照してください。エフェメラル OS ディスクを使用する場合は、次の点を考慮してください:

- Azure エフェメラル OS ディスクと MCS I/O を同時に有効にすることはできません。
- エフェメラル OS ディスクを使用するマシンを更新するには、サイズが仮想マシンのキャッシュディスクまたは一時的ディスクのサイズを超えないイメージを選択する必要があります。
- ウィザードの後半で表示される［電源サイクル中に仮想マシンとシステムディスクを保持する］オプションを使用することはできません。

> 注:
>
> ID ディスクは、選択したストレージの種類に関係なく、常に標準 SSD を使用して作成されます。

ストレージの種類によって、ウィザードの［仮想マシン］ページに表示されるマシンのサイズが変わります。MCS は、ローカル冗長ストレージ（LRS）を使用するようにプレミアムディスクと標準ディスクを構成します。LRS は、単一のデータ センター内でデータの複数の同期コピーを作成します。Azure エフェメラル OS ディスクは、VM のローカルディスクを使用してオペレーティングシステムを格納します。Azure のストレージの種類およびストレージの複製について詳しくは、以下のドキュメントを参照してください:

- Azure Storage の概要
- Azure Premium Storage: 高パフォーマンス向け設計
- Azure Storage の冗長性

既存の Windows ライセンスを使用するか Linux ライセンスを使用するかを選択します:

- Windows ライセンス: Windows ライセンスと Windows イメージ（Azure プラットフォームのサポートイメージまたはカスタムイメージ）を使用すると、Azure で Windows VM を低コストで実行できます。ライセンスには次の 2 種類があります:
  - **Windows Server** ライセンス。Windows Server ライセンスまたは Azure Windows Server ライセンスを使用できます。これにより、Azure Hybrid 特典を使用できます。詳しくは、https://azure.microsoft.com/en-us/pricing/hybrid-benefit/を参照してください。Azure Hybrid 特典を使用すると、Azure ギャラリーからの Windows Server 追加ライセンス料金が不要になるため、Azure での仮想マシン実行コストを基本計算料金のみに抑えられます。
  - **Windows** クライアントライセンス。Windows 10 ライセンスおよび Windows 11 ライセンスを Azure に移行できるため、追加のライセンスなしで Windows 10 VM および Windows 11 VM を Azure で実行できます。詳しくは、「クライアントアクセスライセンスと管理ライセンス」を参照してください。
- Linux ライセンス: bring-your-own-subscription（BYOS）Linux ライセンスを使用すると、ソフトウェアの料金を支払う必要がありません。BYOS の料金には、コンピューティングハードウェアの料金のみが含まれます。ライセンスには次の 2 種類があります:

  - **RHEL_BYOS**：RHEL_BYOS の種類を正しく使用するには、Azure サブスクリプションで Red Hat Cloud Access を有効にします。
  - **SLES_BYOS**：SLES の BYOS バージョンには、SUSE からのサポートが含まれています。

以下を参照してください：

- Windows ライセンスの確認
- Linux ライセンスの構成

ライセンスの種類と利点を理解するには、次のドキュメントを参照してください：

- https://docs.microsoft.com/en-us/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet
- https://docs.microsoft.com/en-us/azure/virtual-machines/linux/azure-hybrid-benefit-linux

Azure Compute Gallery は、イメージを管理および共有するためのリポジトリです。これにより、組織全体でイメージを利用できるようになります。大規模な永続的でないマシンカタログを作成する場合は、よりすばやく VDA OS ディスクをリセットできるため、イメージを Azure Compute Gallery に保存することをお勧めします。［準備されたイメージを **Azure Compute Gallery** に配置します］を選択すると、［**Azure Computer Gallary** の設定］セクションが表示され、追加の Azure Computer Gallary 設定を指定できます：

- イメージレプリカに対する仮想マシンの比率。Azure で保持するイメージレプリカに対する仮想マシンの比率を指定できます。デフォルトでは、Azure は 40 台の非永続的なマシンごとに 1 つのイメージレプリカを保持します。永続マシンの場合、その数はデフォルトで 1,000 になります。
- 最大レプリカ数。Azure で保持するイメージレプリカの最大数を指定できます。デフォルトは 10 です。

Azure Compute Gallery について詳しくは、「Azure Compute Gallery」を参照してください。

4. ［仮想マシン］ページで、作成する VM の数とマシンサイズを指定します。カタログ作成後、カタログを編集してマシンサイズを変更できます。
5. ［**NIC**］ページには、Azure 固有の情報は表示されません。「マシンカタログの作成」のガイダンスに従ってください。
6. ［ディスク設定］ページで、ライトバックキャッシュを有効にするかどうかを選択します。MCS ストレージ最適化機能を有効にすると、カタログを作成するときに以下の設定を構成できます。これらの設定は、Azure 環境と GCP 環境の両方に適用されます。

   ライトバックキャッシュを有効にした後、次の操作を実行できます：

   - 一時データのキャッシュに使用するディスクと RAM のサイズを構成する。詳しくは、「一時データ用キャッシュの構成」を参照してください。

- ライトバックキャッシュディスク用のストレージの種類を選択します。ライトバックキャッシュディスクには、次のストレージのオプションを使用できます:
  - プレミアム SSD
  - 標準 SSD
  - 標準 HDD
- プロビジョニングされた VM に対してライトバックキャッシュディスクを保持するかどうかを選択します。このオプションを使用可能にするには、［ライトバックキャッシュを有効にする］を選択します。デフォルトでは、［非永続的なライトバックキャッシュディスクを使用する］が選択されています。
- ライトバックキャッシュディスクの種類を選択します。
  - 非永続的なライトバックキャッシュディスクを使用する。選択した場合、ライトバックキャッシュディスクは電源サイクル中に削除されます。リダイレクトされたデータはすべて失われます。VM の一時ディスクに十分なスペースがある場合、それはライトバックキャッシュディスクのホストに使用され、コストを削減します。カタログの作成後、プロビジョニングされたマシンが一時ディスクを使用しているかどうかを確認できます。これを行うには、カタログをクリックして、［テンプレートのプロパティ］タブの情報を確認します。一時ディスクが使用されている場合は、［非永続的なライトバックキャッシュディスク］が表示され、その値は ［はい（**VM** の一時ディスクを使用)］になっていますそうでない場合は、［非永続的なライトバックキャッシュディスク］が表示され、その値は ［いいえ］（**VM** の一時ディスクを使用しない）になっています。
  - 永続的なライトバックキャッシュディスクを使用する。選択した場合、ライトバックキャッシュディスクは、プロビジョニングされた VM で保持されます。このオプションを有効にすると、ストレージコストが増加します。
- 電源サイクル中に VDA 用の仮想マシンとシステムディスクを保持するかどうかを選択します。

  電源サイクル中に仮想マシンおよびシステムディスクを保持します。［ライトバックキャッシュを有効にする］を選択した場合に使用できます。デフォルトでは、仮想マシンとシステムディスクはシャットダウン時に削除され、スタートアップ時に再作成されます。仮想マシンの再起動時間を短縮したい場合は、このオプションを選択します。このオプションを有効にすると、ストレージコストも増加することに注意してください。
- ストレージコストの削減を有効にする かどうかを選択します。有効にすると、VM のシャットダウン時にストレージディスクを標準 HDD にダウングレードすることで、ストレージコストを削減できます。VM は、再起動時に元の設定に切り替わります。このオプションは、ストレージディスクとライトバックキャッシュディスクの両方に適用されます。または、PowerShell を使用することもできます。「仮想マシンのシャットダウン時にストレージの種類をダウングレードする」を参照してください。

  > 注:
  >
  > Microsoft は、VM のシャットダウン中のストレージの種類の変更に制限を課しています。Microsoft が将来的にストレージの種類の変更を禁止する可能性もあります。詳しくは、Microsoft 社の記事を参照してください。

- このカタログ内のマシン上のデータを暗号化するかどうかを選択し、使用する暗号キーを選択します。顧客管理キー（CMK）を使用したサーバー側暗号化により、管理対象ディスクレベルで暗号化を管理し、カタログ内のマシン上のデータを保護できます。デフォルト設定はマシンプロファイルまたはマスターイメージから継承され、プロファイルが優先されます：
  - *CMK* を含むマシンプロファイルを使用している場合、［次のキーを使用して各マシンのデータを暗号化］オプションが自動的に選択され、デフォルトでマシンプロファイルのキーが使用されます。
  - プラットフォーム管理キー（PMK）を含むマシンプロファイルを使用し、マスターイメージが *CMK* で暗号化されている場合、［次のキーを使用して各マシンのデータを暗号化］オプションが自動的に選択され、デフォルトでマスターイメージのキーが使用されます。
  - マシンプロファイルを使用せず、マスターイメージが *CMK* で暗号化されている場合、［次のキーを使用して各マシンのデータを暗号化］オプションが自動的に選択され、デフォルトでマスターイメージのキーが使用されます。

詳しくは、「Azure サーバー側暗号化」を参照してください。

7. ［リソースグループ］ページで、リソースグループを作成するか、既存のグループを使用するかを選択します。
   - リソースグループを作成する場合は、［次へ］を選択します。
   - 既存のリソースグループを使用する場合は、［使用可能なプロビジョニングリソースグループ］ボックスの一覧からグループを選択します。

   > 注：
   >
   > カタログで作成しているマシンを収容するのに十分なグループを選択してください。選択が少なすぎると、メッセージが表示されます。後でカタログにさらに VM を追加する予定がある場合は、必要最小限よりも多く選択しておくことをお勧めします。カタログが作成された後、カタログにリソースグループをさらに追加することはできません。

   詳しくは、「Azure リソースグループ」を参照してください。

8. ［マシン **ID**］ページで ID の種類を選択し、このカタログ内のマシンの ID を設定します。［**Azure Active Directory** 参加］として仮想マシンを選択すると、それらを Azure AD セキュリティグループに追加できます。詳細な手順は次のとおりです：
   a) ［**ID** の種類］フィールドから、［**Azure Active Directory** 参加］を選択します。［**Azure AD** セキュリティグループ（オプション）］オプションが表示されます。
   b) ［**Azure AD** セキュリティグループ：新規作成］をクリックします。
   c) グループ名を入力して、［作成］をクリックします。
   d) 画面の指示に従って、Azure にサインインします。
   グループ名が Azure に存在しない場合は、緑色のアイコンが表示されます。それ以外の場合は、新しい名前の入力を求めるエラーメッセージが表示されます。
   e) 割り当て済みセキュリティ グループにこのセキュリティグループを追加するには、［割り当て済みのセキュリティグループをメンバーとして参加させる］を選択し、［グループの選択］をクリックしてから、参加させる割り当て済みグループを選択します。

f) 仮想マシンのマシンアカウント名前付けスキームを入力します。

カタログの作成後、Citrix DaaS はユーザーに代わって Azure にアクセスし、セキュリティグループとグループの動的メンバーシップ規則を作成します。この規則に基づいて、このカタログで指定された名前付けスキームの仮想マシンがセキュリティグループに自動的に追加されます。

このカタログに別の名前付けスキームの仮想マシンを追加するには、Azure にサインインする必要があります。その後、Citrix DaaS は Azure にアクセスし、新しい名前付けスキームに基づいて動的メンバーシップ規則を作成できます。

このカタログを削除する場合、Azure からセキュリティグループを削除するには、Azure へのサインインも必要です。

> 注:
>
> カタログの作成後に Azure AD セキュリティグループの名前を変更するには、カタログを編集し、左側のナビゲーションから［**Azure AD** セキュリティグループ］に移動します。Azure AD セキュリティグループの名前には、次の文字を含めることはできません：<!JEKYLL@5180@5>。

- ［ドメイン資格情報］ページおよび ［概要］ページには、Azure 固有の情報は表示されません。「マシンカタログの作成」のガイダンスに従ってください。

ウィザードを完了します。

Azure テンプレートスペックを作成する

Azure Portal で Azure テンプレートスペックを作成し、それを［完全な構成］インターフェイスと PowerShell コマンドで使用して、MCS マシンカタログを作成または更新できます。

既存の仮想マシンの Azure テンプレートスペックを作成するには、以下の手順に従います：

1. Azure Portal に移動します。リソースグループを選択してから、仮想マシンとネットワークインターフェイスを選択します。上の［…］メニューで、［**Export template**］をクリックします。
2. カタログプロビジョニング用のテンプレートスペックを作成する場合は、［**Include parameters**］チェックボックスをオフにします。
3. テンプレートスペックを後で変更するには、［**Add to library**］をクリックします。
4. ［**Importing template**］ページで、**Name**、**Subscription**、**Resource Group**、**Location**、**Version** などの必要な情報を入力します。［**Next: Edit Template**］をクリックします。
5. カタログをプロビジョニングする場合は、独立したリソースとしてネットワークインターフェイスも必要です。したがって、テンプレートスペックで指定されている <!JEKYLL@5180@6> を削除する必要があります。例：

   <!JEKYLL@5180@7>
6. ［**Review+Create**］を作成してテンプレートスペックを作成します。

7. [**Template Specs**] ページで、作成したテンプレートスペックを確認します。テンプレートスペックをクリックします。左側のパネルで、[**Versions**] をクリックします。
8. [**Create new version**] をクリックして、新しいバージョンを作成できます。新しいバージョン番号を指定し、現在のテンプレートスペックを変更して、[**Review + Create**] をクリックし、新しいバージョンのテンプレートスペックを作成します。

次の PowerShell コマンドを使用して、テンプレートスペックとテンプレートのバージョンに関する情報を取得できます:

- テンプレートスペックに関する情報を取得するには、次を実行します:

  <!JEKYLL@5180@8>

- テンプレートスペックのバージョンに関する情報を取得するには、次を実行します:

  <!JEKYLL@5180@9>

カタログの作成または更新でテンプレートスペックを使用する

テンプレートスペックをマシンプロファイルの入力に使用して、MCS マシンカタログを作成または更新できます。これを行う場合、完全な構成 インターフェイスまたは PowerShell コマンドを使用できます。

- [完全な構成] インターフェイスを使用する:「[完全な構成] インターフェイスで Azure Resource Manager イメージを使用してマシンカタログを作成する」を参照してください。
- PowerShell については、「PowerShell を使用したカタログの作成または更新でテンプレートスペックを使用する」を参照してください

指定されたアベイラビリティゾーンへのマシンのプロビジョニング

Azure 環境の特定のアベイラビリティゾーンにマシンをプロビジョニングできます。これは、完全な構成インターフェイスまたは PowerShell を使用して実行できます

> 注:
>
> ゾーンが指定されていない場合、MCS は Azure にマシンをリージョン内に配置させます。複数のゾーンが指定されている場合、MCS はマシンをそれらにランダムに分散します。

完全な構成インターフェイスを使用したアベイラビリティゾーンの構成

マシンカタログを作成するときに、マシンをプロビジョニングするアベイラビリティゾーンを指定できます。[仮想マシン] ページで、マシンを作成するアベイラビリティゾーンを 1 つ以上選択します。

アベイラビリティゾーンが使用できない理由は 2 つあります: リージョンにアベイラビリティゾーンがないか、選択したマシンサイズが使用できないことです。

PowerShell コマンドを使用した構成について詳しくは、「PowerShell を使用したアベイラビリティゾーンの構成」を参照してください。

Azure エフェメラルディスク

Azure エフェメラルディスクを使用すると、キャッシュディスクまたは一時ディスクを再利用して、Azure 対応の仮想マシンの OS ディスクを保存できます。この機能は、標準の HDD ディスクよりも高性能の SSD ディスクを必要とする Azure 環境で役立ちます。Azure エフェメラルディスクを使用したカタログの作成については、「Azure エフェメラルディスクを使用したカタログの作成」を参照してください。

> 注:
>
> 永続カタログでは、エフェメラル OS ディスクはサポートされていません。

エフェメラル OS ディスクでは、プロビジョニングスキームで管理対象ディスクと Azure Compute Gallery を使用する必要があります。詳しくは、「Azure Shared Image Gallery」を参照してください。

エフェメラル OS 一時ディスクの保存

エフェメラル OS ディスクを VM 一時ディスクまたはリソースディスクに保存するオプションがあります。この機能により、キャッシュがないか、キャッシュが不十分な VM で、エフェメラル OS ディスクを使用できます。このような VM には、<!JEKYLL@5180@10> などのエフェメラル OS ディスクを保存するための一時ディスクまたはリソースディスクがあります。

以下に注意してください:

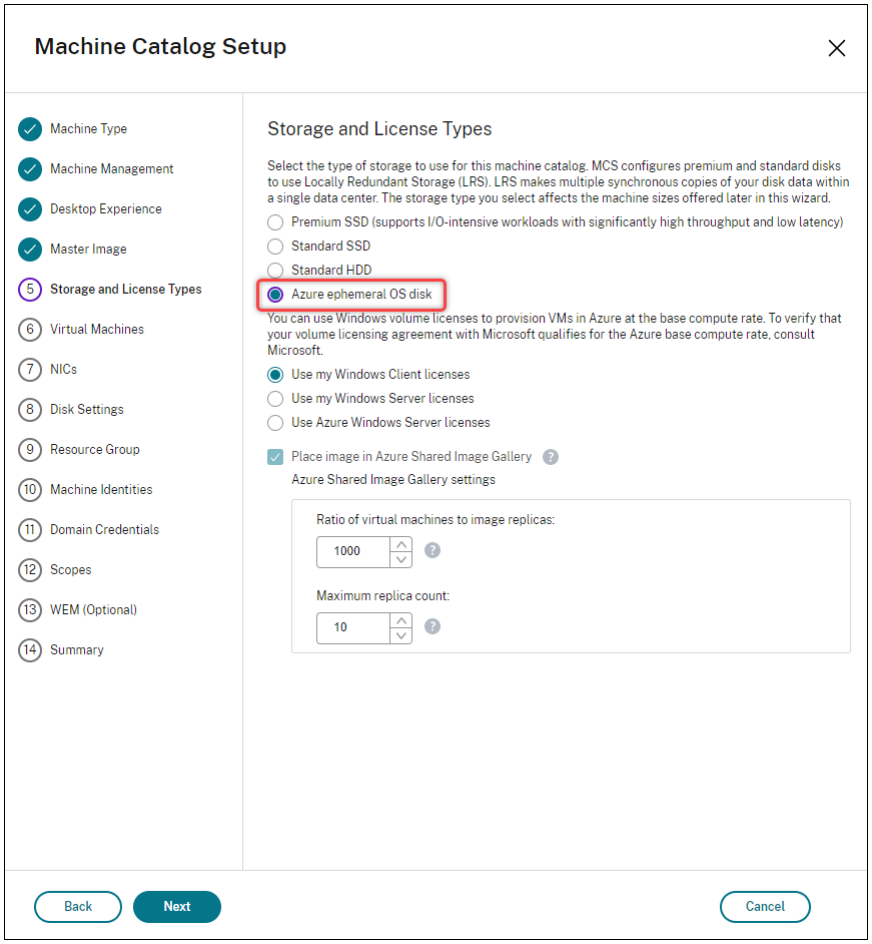
- エフェメラルディスクは、VM キャッシュディスクまたは VM の一時（リソース）ディスクのいずれかに保存されます。キャッシュディスクが OS ディスクの内容を保持するのに十分な大きさでない場合を除き、キャッシュディスクは一時ディスクよりも優先されます。
- 更新の際は、キャッシュディスクよりも大きいが一時ディスクよりも小さい新しいイメージにより、エフェメラル OS ディスクが VM の一時ディスクに置き換えられます。

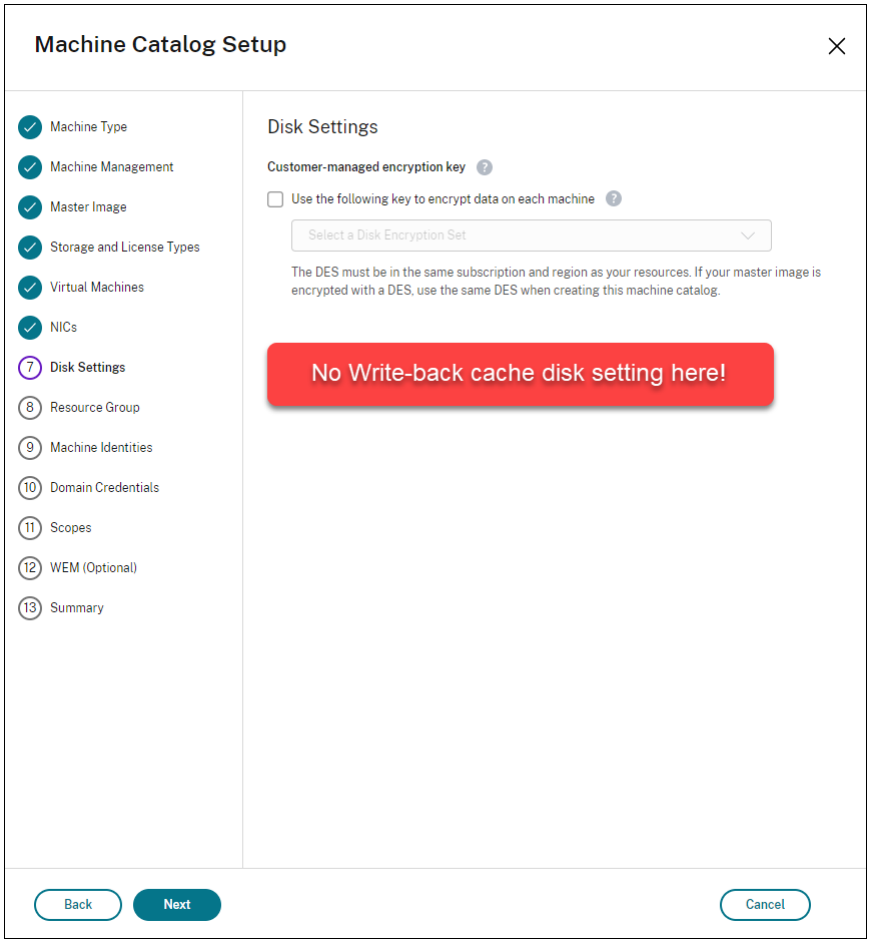
Azure エフェメラルディスクと Machine Creation Services（MCS）ストレージ最適化（MCS I/O）

Azure エフェメラル OS ディスクと MCS I/O を同時に有効にすることはできません。

重要な考慮事項は次のとおりです:

- エフェメラル OS ディスクと MCS I/O の両方を同時に有効にしてマシンカタログを作成することはできません。
- マシンカタログのセットアップウィザードで、［ストレージとライセンスの種類］ページの ［**Azure** エフェメラル **OS** ディスク］を選択した場合、［ディスク設定］ページでライトバックキャッシュディスク のオプションは使用できません。





- <!JEKYLL@5180@11> または <!JEKYLL@5180@12> が「**true**」に設定された PowerShell パラメーター（<!JEKYLL@5180@13> および <!JEKYLL@5180@14>）を使用すると、適切なエラーメッセージが表示されて失敗します。
- 両方の機能を有効にして作成した既存のマシンカタログについては、次のことができます：
  - マシンカタログの更新。
  - VM の追加または削除。
  - マシンカタログの削除。

Azure Compute Gallery

Azure において、MCS でプロビジョニングされたマシンの公開イメージリポジトリとして Azure Shared Image Gallery（旧称：Shared Image Gallery）を使用します。公開イメージをギャラリーに保存して、OS ディスクの作成とハイドレーションを高速化し、非永続仮想マシンの起動時間とアプリケーションの起動時間を改善できます。Azure Compute Gallery には、次の 3 つの要素が含まれています：

- ギャラリー：イメージはここに保存されます。MCS は、マシンカタログごとに 1 つのギャラリーを作成します。

- ギャラリーイメージの定義：この定義には、公開イメージに関する情報（オペレーティングシステムの種類と状態、Azure リージョン）が含まれます。MCS は、カタログ用に作成されたイメージごとに 1 つのイメージ定義を作成します。
- ギャラリーイメージバージョン：Azure Compute Gallery の各イメージには複数のバージョンを含めることができ、各バージョンには異なるリージョンに複数のレプリカを含めることができます。各レプリカは、公開イメージの完全なコピーです。Citrix DaaS では、カタログ内のマシン数、構成されたレプリカの比率、および構成されたレプリカの最大数に基づき、カタログのリージョンにおいて適切なレプリカ数を持つ各イメージに対して、Standard_LRS イメージバージョン（バージョン 1.0.0）が 1 つ作成されます。

> 注：
>
> Azure Compute Gallery の機能は、管理対象ディスクとのみ互換性があります。従来のマシンカタログでは使用できません。

詳しくは、「Azure Shared Image Gallery の概要」を参照してください。

Azure Compute Galleryy からイメージにアクセスする

マシンカタログの作成に使用するイメージを選択するときに、Azure Compute Gallery で作成したイメージを選択できます。これらのイメージは、マシンカタログインストールウィザードの ［イメージ］ページのイメージ一覧に表示されます。

これらのイメージを表示するには、次のことを行う必要があります：

1. Citrix DaaS をセットアップします。
2. Azure Resource Managerに接続します。
3. Azure ポータルで、リソースグループを作成します。詳しくは、「ポータルを使用して Azure Shared Image Gallery を作成する」を参照してください。
4. リソースグループで、Azure Compute Gallery を作成します。
5. Azure Compute Gallery で、イメージ定義を作成します。
6. イメージ定義で、イメージバージョンを作成します。

Azure Compute Gallery について詳しくは、「Configure Azure Compute Gallery」を参照してください。

Azure 一時ディスクをライトバックキャッシュディスクとして使用するための条件

次のすべての条件が満たされている場合にのみ、Azure 一時ディスクをライトバックキャッシュディスクとして使用できます：

- Azure 一時ディスクは永続データには適していないため、ライトバックキャッシュディスクは非永続である必要があります。
- 選択した Azure VM のサイズには、一時ディスクが含まれている必要があります。

- エフェメラル OS ディスクを有効にする必要はありません。
- ライトバックキャッシュファイルを Azure 一時ディスクに保存することを受け入れます。
- Azure 一時ディスクのサイズは、「ライトバックキャッシュディスクサイズ + ページングファイル用に予約されたスペース + 1GB のバッファスペース」の合計サイズよりも大きい必要があります。

非永続的なライトバックキャッシュディスクのシナリオ

次の表は、マシンカタログの作成中に一時ディスクがライトバックキャッシュに使用される場合の 3 つの異なるシナリオを示しています。

シナリオ	結果
ライトバックキャッシュに一時ディスクを使用するためのすべての条件が満たされている。	WBC ファイル <!JEKYLL@5180@15> は一時ディスクに保存されます。
一時ディスクに、ライトバックキャッシュを使用するための十分なスペースがない。	VHD ディスク「MCSWCDisk」が作成され、WBC ファイル <!JEKYLL@5180@16> がこのディスクに保存されます。
一時ディスクに、ライトバックキャッシュを使用するための十分なスペースがあるが、<!JEKYLL@5180@17> は false に設定されている。	VHD ディスク「MCSWCDisk」が作成され、WBC ファイル <!JEKYLL@5180@18> がこのディスクに保存されます。

次の PowerShell トピックを参照してください:

- 非永続的なライトバックキャッシュディスクのマシンカタログを作成する
- 永続的なライトバックキャッシュディスクのマシンカタログを作成する

Azure サーバー側暗号化

Citrix DaaS は、Azure Key Vault を使用して Azure Managed Disks の顧客が管理する暗号化キーをサポートします。このサポートにより、独自の暗号化キーを使用してマシンカタログの管理対象ディスクを暗号化して、組織およびコンプライアンスの要件を管理できます。詳しくは、「Azure Disk Storage のサーバー側暗号化」を参照してください。

管理対象ディスクにこの機能を使用する場合:

- ディスクが暗号化されているキーを変更するには、<!JEKYLL@5180@19> の現在のキーを変更します。<!JEKYLL@5180@20> に関連付けられているすべてのリソースは、新しいキーで暗号化されるように変更されます。
- キーを無効にするか削除すると、そのキーを使用するディスクのある VM はすべて自動的にシャットダウンします。シャットダウン後、キーを再度有効にするか、新しいキーを割り当てない限り、VM は使用できません。

このキーを使用するカタログの電源をオンにすることはできません。また、VM をカタログに追加することもできません。

顧客が管理する暗号化キーを使用する場合の重要な考慮事項

この機能を使用するときは、次のことに注意してください:

- 顧客が管理するキーに関連するすべてのリソース（Azure Key Vault、ディスク暗号化セット、VM、ディスク、スナップショット）は、同じサブスクリプションとリージョンに配置される必要があります。
- 顧客が管理するキーで暗号化されたディスク、スナップショット、イメージは、別のリソースグループおよびサブスクリプションに移動できません。
- リージョンごとのディスク暗号化セットの制限については、Microsoft 社のサイトを参照してください。

> 注:
>
> Azure サーバー側暗号化の構成については、「クイックスタート: Azure Portal を使用してキーコンテナを作成する」を参照してください。

Azure の顧客が管理する暗号キー

マシンカタログを作成するときに、カタログでプロビジョニングされるマシンのデータを暗号化するかどうかを選択できます。顧客が管理する暗号化キーを使用したサーバー側暗号化により、管理対象ディスクレベルで暗号化を管理し、カタログ内のマシン上のデータを保護できます。ディスク暗号化セット（DES）は、顧客が管理するキーを表します。この機能を使用するには、最初に Azure で DES を作成する必要があります。DES の形式は次のとおりです:

- <!JEKYLL@5180@21>

一覧から DES を選択します。選択した DES は、リソースと同じサブスクリプションおよびリージョンに存在する必要があります。

暗号化キーを使用してカタログを作成し、後で Azure で対応する DES を無効にすると、カタログ内のマシンの電源をオンにしたり、カタログにマシンを追加したりできなくなります。

「顧客管理暗号キーを使用したマシンカタログの作成」を参照してください。

ホストでの **Azure** ディスク暗号化

ホスト機能での暗号化を使用して、MCS マシンカタログを作成できます。現在、MCS はこの機能でマシンプロファイルワークフローのみをサポートします。VM またはテンプレートスペックをマシンプロファイルの入力として使用できます。

この暗号化方法は、Azure Storage でデータを暗号化しません。VM をホストするサーバーがデータを暗号化し、暗号化されたデータが Azure Storage サーバーを通過します。つまり、この暗号化方法はデータをエンドツーエンドで暗号化します。

制限:

ホストでの Azure ディスク暗号化は:

- すべての Azure マシンサイズでサポートされているわけではありません
- Azure Disk Encryption と互換性がありません

詳しくは、次のトピックを参照してください:

- ホストでの暗号化機能を使用してマシンカタログを作成する。
- マシンプロファイルからホストでの暗号化情報を取得する

管理対象ディスクの二重暗号化

二重暗号化を使用してマシンカタログを作成できます。この機能を使用して作成されたカタログでは、すべてのディスクがプラットフォームキーと顧客管理キーの両方によってサーバー側で暗号化されています。Azure Key Vault、暗号キー、およびディスク暗号化セット（DES）は、顧客が所有し、維持します。

二重暗号化とは、プラットフォーム側の暗号化（デフォルト）と顧客管理の暗号化（CMEK）です。したがって、暗号化アルゴリズム、実装、またはキーの侵害に関するリスクを懸念している、セキュリティに非常に敏感なお客様は、この二重暗号化を選択できます。永続的 OS ディスクとデータディスク、スナップショット、イメージはすべて二重暗号化により保存時に暗号化されます。

> 注:
>
> - 完全な構成インターフェイスを使用するか、PowerShell コマンドを実行することで、二重暗号化を使用してマシンカタログを作成し、更新できます。
> - 二重暗号化を使用してマシンカタログを作成または更新するには、非マシンプロファイルベースのワークフローまたはマシンプロファイルベースのワークフローを使用できます。
> - 非マシンプロファイルベースのワークフローを使用してマシンカタログを作成する場合は、保存されている <!JEKYLL@5180@22> を再利用できます。
> - マシンプロファイルを使用する場合は、VM またはテンプレートスペックをマシンプロファイルの入力に使用できます。

制限事項

- 二重暗号化は、Ultra Disk または Premium SSD v2 ディスクではサポートされていません。
- 二重暗号化は、非管理ディスクではサポートされません。
- カタログに関連付けられているディスク暗号化セットキーを無効にすると、カタログの VM が無効になります。
- 顧客が管理するキーに関連するすべてのリソース（Azure Key Vault、ディスク暗号化セット、VM、ディスク、スナップショット）は、同じサブスクリプションとリージョンに存在する必要があります。
- サブスクリプションごとに、リージョンあたり最大 50 のディスク暗号化セットのみを作成できます。

次の PowerShell トピックを参照してください:

- 二重暗号化を使用したマシンカタログの作成
- 暗号化されていないカタログを二重暗号化を使用するように変換
- カタログが二重暗号化されていることの確認

Azure リソースグループ

Azure プロビジョニングのリソースグループは、アプリケーションとデスクトップをユーザーに提供する VM をプロビジョニングする方法を提供します。MCS マシンカタログを作成するときに既存の空の Azure リソースグループを追加するか、新しいリソースグループを作成することができます。Azure リソースグループについて詳しくは、Microsoft 社のドキュメントを参照してください。

Azure リソースグループの使用

Azure リソースグループごとの仮想マシン、管理対象ディスク、スナップショット、およびイメージの数に制限はありません（Azure リソースグループごとに仮想マシンは 240、管理対象ディスクは 800 という数の制限はなくなりました）。

- フルスコープのサービスプリンシパルを使用してマシンカタログを作成する場合、MCS は 1 つの Azure リソースグループのみを作成し、カタログのこのグループを使用します。
- スコープの狭いサービスプリンシパルを使用してマシンカタログを作成する場合、事前に作成された空の Azure リソースグループを指定する必要があります。

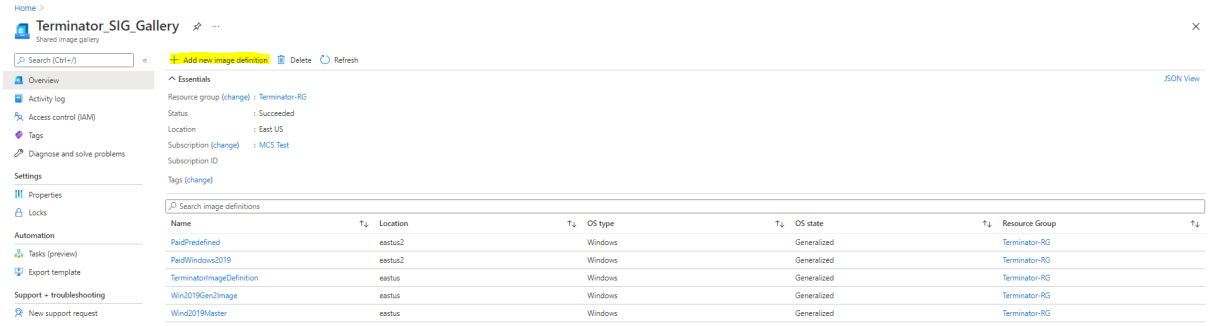
Azure Marketplace

Citrix DaaS は、マシンカタログを作成するためのプラン情報を含む Azure 上のマスターイメージの使用をサポートしています。詳しくは、Microsoft Azure Marketplaceを参照してください。

> ヒント：
>
> 標準の Windows Server イメージなど、Azure Marketplace にある一部のイメージには、プラン情報が追加されていません。Citrix DaaS 機能は有料イメージ用です。

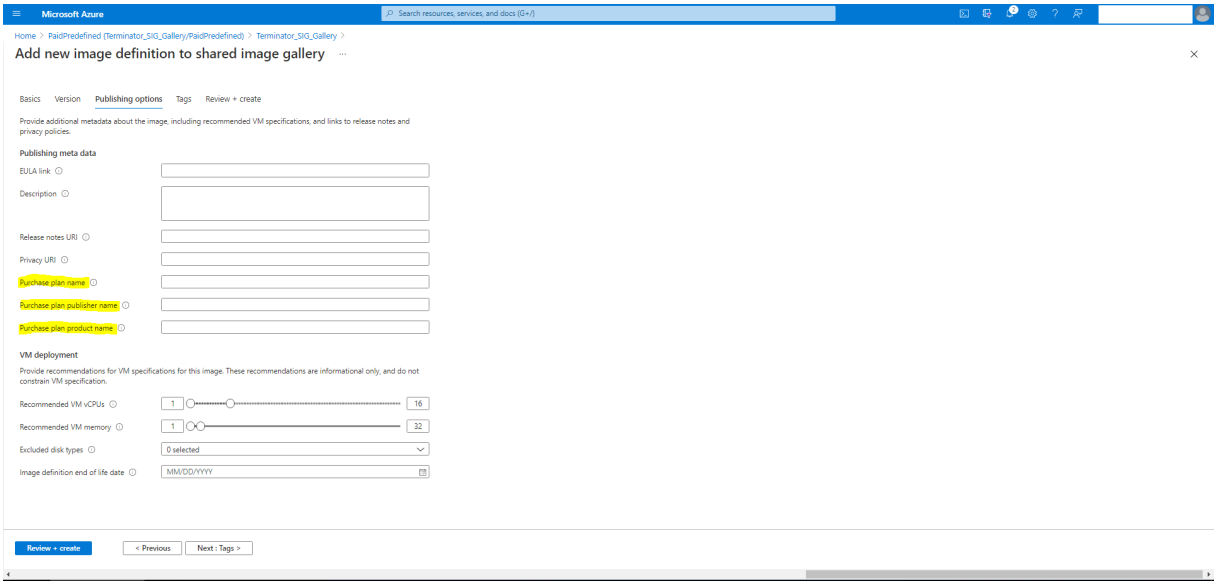
Azure Compute Gallery で作成されたイメージに Azure プラン情報が含まれていることを確認する

このセクションの手順を使用して、完全な構成インターフェイスで Azure Compute Gallery のイメージを表示します。これらのイメージは、マスターイメージに使用することもできます。イメージを Azure Compute Gallery に追加するには、ギャラリーでイメージ定義を作成します。

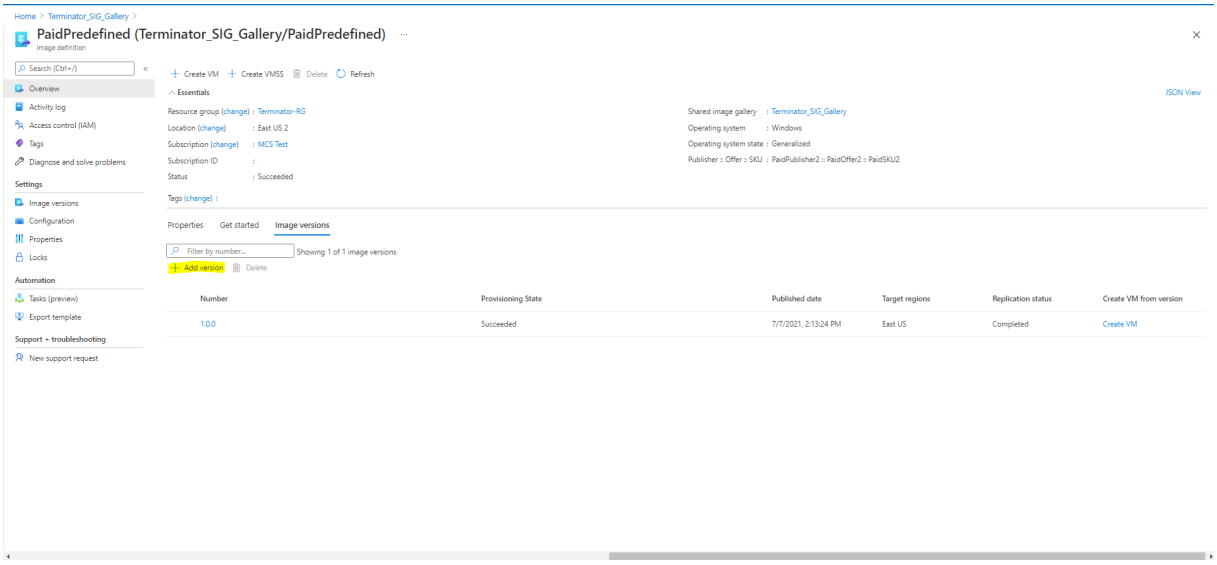


［公開オプション］ページで、購入プラン情報を確認します。

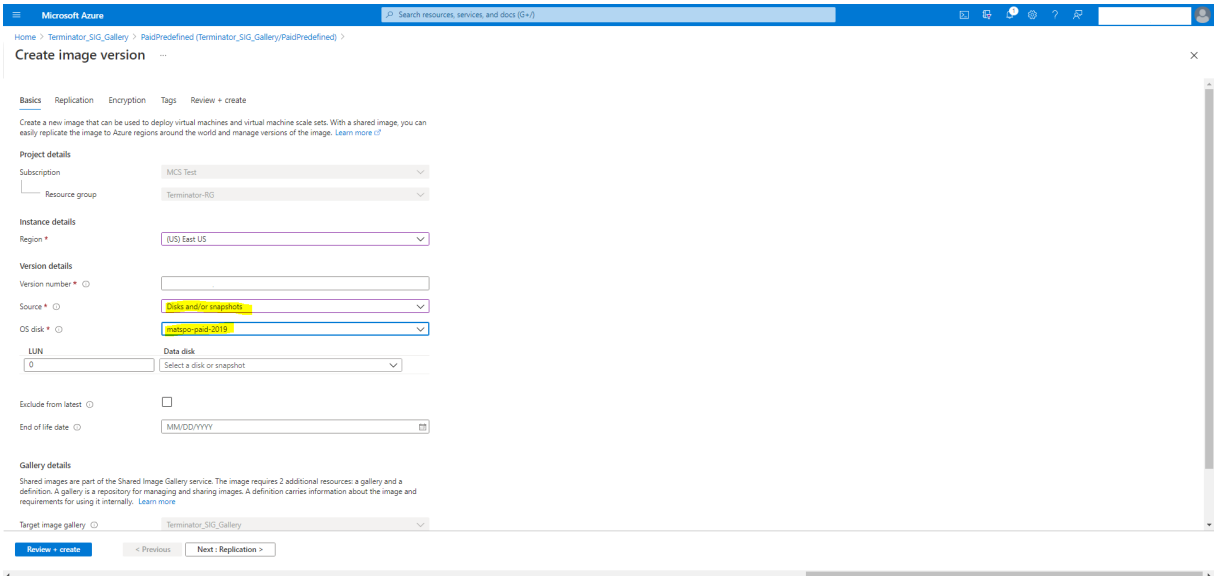
購入プラン情報フィールドは最初は空欄です。これらのフィールドに、イメージに使用されている購入プラン情報を入力します。購入プラン情報を入力しないと、マシンカタログプロセスが失敗する可能性があります。



購入プラン情報を確認した後、定義内にイメージバージョンを作成します。これはマスターイメージとして使用されます。［バージョンの追加］をクリックします:



[バージョンの詳細] セクションで、ソースとしてイメージスナップショットか管理対象ディスクを選択します:



[**Azure Monitor** エージェントがインストールされたカタログ **VM** をプロビジョニングする]

Azure の監視は、Azure 環境および社内のオンプレミス環境からテレメトリデータを収集、分析し、それに基づいて操作するために使用できるサービスです。

Azure Monitor エージェント（AMA）は、仮想マシンなどのコンピューティングリソースから監視データを収集し、そのデータを Azure Monitor に配信します。現在、イベントログ、Syslog、パフォーマンスメトリックの収集がサポートされており、収集した結果を Azure Monitor メトリックと Azure Monitor Log のデータソースとして送信します。

監視データ内の VM を一意に識別して監視を有効にするには、AMA を拡張機能としてインストールして MCS マシンカタログの VM をプロビジョニングします。

要件

- 権限:「Azure の権限について」で規定されている最小限の Azure の権限と、Azure Monitor を使用するための次の権限を持っていることを確認します:
  - <!JEKYLL@5180@23>
  - <!JEKYLL@5180@24>
  - <!JEKYLL@5180@25>
  - <!JEKYLL@5180@26>
  - <!JEKYLL@5180@27>
- データ収集規則（DCR）: Azure Portal でデータ収集規則を設定します。DCR の設定について詳しくは、「データ収集規則の作成」を参照してください。DCR はプラットフォーム（Windows または Linux）に固有です。必要なプラットフォームに応じた DCR を必ず作成してください。
  AMA はデータ収集規則（DCR）を使用して、VM などのリソースと、Azure Monitor メトリックや Azure Monitor の Log Analytics エージェントなどのデータ ソースとのマッピングを管理します。
- デフォルトのワークスペース: Azure Portal でワークスペースを作成します。ワークスペースの作成については、「Log Analytics ワークスペースの作成」を参照してください。収集したログとデータの情報は、ワークスペースに保存されます。ワークスペースは、一意のワークスペース ID とリソース ID を持っています。ワークスペース名は、特定のリソースグループに対して固有のものにする必要があります。ワークスペースを作成した後、データがワークスペースに保存されるようにデータソースとソリューションを構成します。
- モニター拡張機能を許可リストに登録しました: 拡張機能 <!JEKYLL@5180@28> および <!JEKYLL@5180@29> が、Citrix が定義している許可リストに登録されました。許可リストに登録されている拡張機能の一覧を表示するには、PowerShell コマンド <!JEKYLL@5180@30> を使用します。
- マスターイメージ: Microsoft では、既存のマシンから新しいマシンを作成する前に、既存のマシンから拡張機能を削除することを推奨しています。拡張子を削除しないと、ファイルが残ったり、予期しない動作が行われたりする可能性があるからです。詳しくは、「既存の VM を再作成する場合」を参照してください。

PowerShell を使用して AMA を有効にしたカタログを作成する方法については、「AMA を有効にしたカタログ VM のプロビジョニング」を参照してください。

Azure Confidential VM

Azure Confidential Computing VM によって、仮想デスクトップは確実にメモリ内で暗号化され、使用中に保護されます。

MCS を使用して、Azure Confidential VM を含むカタログを作成できます。このようなカタログを作成するには、マシンプロファイルワークフローを使用する必要があります。VM と ARM テンプレートスペックの両方をマシンプロファイル入力として使用できます。

Confidential VM に関する重要な考慮事項

サポートされる VM サイズと、Confidential VM を含むマシンカタログの作成に関する重要な考慮事項は次のとおりです:

- サポートされる VM サイズ: Confidential VM は次の VM サイズをサポートします:
  - DCasv5 シリーズ
  - DCadsv5 シリーズ
  - ECasv5 シリーズ
  - ECadsv5 シリーズ
- Confidential VM を含むマシンカタログを作成します。
  - 完全な構成インターフェイスと PowerShell コマンドを使用することで、Azure Confidential VM を使用してマシンカタログを作成できます。
  - Azure Confidential VM でマシンカタログを作成するには、マシンプロファイルベースのワークフローを使用する必要があります。VM またはテンプレートスペックをマシンプロファイルの入力として使用できます。
  - マスターイメージとマシンプロファイル入力は両方とも同じ機密のセキュリティの種類で有効にする必要があります。セキュリティの種類は次のとおりです:
    * VMGuestStateOnly: VM ゲスト状態のみが暗号化された Confidential VM
    * DiskWithVMGuestState: OS ディスクと VM ゲスト状態の両方がプラットフォーム管理キーまたは顧客管理キーで暗号化された Confidential VM。通常の OS ディスクとエフェメラル OS ディスクの両方を暗号化できます。
  - AdditionalData パラメーターを使用すると、管理対象ディスク、スナップショット、Azure Compute Gallery イメージ、VM、ARM テンプレートスペックなど、さまざまなリソースの種類の Confidential VM 情報を取得できます。例:

    <!JEKYLL@5180@31>

    追加のデータフィールドは次のとおりです:

    * DiskSecurityType
    * ConfidentialVMDiskEncryptionSetId
    * DiskSecurityProfiles

    マシンサイズの Confidential Computing プロパティを取得するには、次のコマンドを実行します: <!JEKYLL@5180@32>

    追加のデータフィールドは <!JEKYLL@5180@33> です。
  - マスターイメージまたはマシンプロファイルを機密のセキュリティの種類から機密以外のセキュリティ種類に、または機密以外のセキュリティに酒類から機密のセキュリティの種類に変更することはできません。

- 構成が正しくない場合は、適切なエラーメッセージが表示されます。

マスターイメージとマシンプロファイルを準備する

Confidential VM のセットを作成する前に、次の手順に従ってそれらのマスターイメージとマシンプロファイルを準備します:

1. Azure ポータルで、次のような特定の設定で Confidential VM を作成します:
   - セキュリティの種類: Confidential VM
   - **OS** ディスクの機密暗号化: 有効になっています。
   - キー管理: プラットフォーム管理キーを使用した機密ディスクの暗号化
     Confidential VM の作成について詳しくは、こちらの Microsoft の記事を参照してください。
2. 作成した VM 上でマスターイメージを準備します。作成した VM 上で必要なアプリケーションと VDA をインストールします。

   > 注:
   >
   > VHD を使用した Confidential VM の作成はサポートされていません。代わりに、Azure Compute Gallery、Managed Disks、またはスナップショットを使用します。

3. 次のいずれかの方法でマシンプロファイルを作成します:
   - 手順 1 で作成した既存の VM に必要なマシンプロパティがある場合は、それを使用します。
   - マシンプロファイルとして ARM テンプレートスペックを選択する場合は、必要に応じてテンプレートスペックを作成します。具体的には、*SecurityEncryptionType* や *diskEncryptionSet*（顧客管理キーの場合）など、Confidential VM の要件を満たすパラメーターを構成します。詳しくは、「Azure テンプレートスペックの作成」を参照してください。

     > 注:
     >
     > - マスターイメージとマシンプロファイルのセキュリティキーの種類が同じであることを確認します。
     > - 顧客管理キーを使用して OS ディスクの機密暗号化を必要とする Confidential VM を作成するには、マスターイメージとマシンプロファイルの両方のディスク暗号化セット ID が同一であることを確認します。

完全な構成または **PowerShell** コマンドを使用して **Confidential VM** を作成する

Confidential VM のセットを作成するには、マスターイメージと、目的の Confidential VM に基づくマシンプロファイルを使用してマシンカタログを作成します。

完全な構成を使用してカタログを作成するには、「マシンカタログの作成」で説明されている手順に従います。次の考慮事項に留意してください:

- ［イメージ］ページで、Confidential VM の作成用に準備したマスターイメージとマシンプロファイルを選択します。マシンプロファイルの選択は必須であり、選択したマスターイメージと同じセキュリティ暗号化の種類に一致するプロファイルのみが選択可能です。
- ［仮想マシン］ページでは、Confidential VM をサポートするマシンサイズのみが選択肢に表示されます。
- ［ディスク設定］ページでは、選択したマシンプロファイルから継承されるため、ディスク暗号化セットを指定することはできません。

PowerShell の使用

このセクションでは、PowerShell を使用して次のタスクを実行する方法について説明します：

- PowerShell を使用したカタログの作成または更新でテンプレートスペックを使用する
- Azure VM の拡張機能の有効化
- トラステッド起動を使用したマシンカタログ
- マシンプロファイルのプロパティ値を使用する
- PowerShell を使用したアベイラビリティゾーンの構成
- Azure 専用ホストへの VM のプロビジョニング
- ストレージの種類の構成
- ゾーン冗長ストレージの有効化
- マシンプロファイルから VM および NIC の診断設定をキャプチャする
- Windows ライセンスの確認
- Linux ライセンスの構成
- Azure エフェメラルディスクを使用したマシンカタログの作成
- Azure Compute Gallery を構成する
- VM ごとに複数の NIC を含むカタログを作成または更新する
- 非永続的なライトバックキャッシュディスクのマシンカタログを作成する
- 永続的なライトバックキャッシュディスクのマシンカタログを作成する
- MCSIO による起動パフォーマンスの向上
- 顧客管理暗号キーを使用したマシンカタログの作成
- ホスト機能での暗号化を使用してマシンカタログを作成する
- 二重暗号化を使用したマシンカタログの作成
- ページファイルの場所の決定
- ページファイル設定シナリオ
- ページファイル設定を指定する
- ページファイル設定を変更する
- AMA を有効にしたカタログ VM をプロビジョニングする
- Azure Spot VM を使用したカタログの作成
- すべてのリソースのタグをコピーする

PowerShell を使用したカタログの作成または更新でテンプレートスペックを使用する

テンプレートスペックをマシンプロファイルの入力に使用して、MCS マシンカタログを作成または更新できます。これを行う場合、完全な構成 インターフェイスまたは PowerShell コマンドを使用できます。

完全な構成インターフェイスについては、「完全な構成インターフェイスで Azure Resource Manager イメージを使用してマシンカタログを作成する」を参照してください。

PowerShell コマンドを使用する：

1. **PowerShell** ウィンドウを開きます。
2. <!JEKYLL@5180@34> を実行します。
3. カタログを作成または更新します。
    - カタログを作成するには：
        a) マシンプロファイルの入力で、テンプレートスペックを <!JEKYLL@5180@35> コマンドとともに使用します。例：

        <!JEKYLL@5180@36>

        b) カタログの作成を完了します。
    - カタログを更新するには、マシンプロファイルの入力で、テンプレートスペックを <!JEKYLL@5180@37> コマンドとともに使用します。例：

        <!JEKYLL@5180@38>

Azure VM の拡張機能の有効化

ARM（Azure Resource Manager）テンプレートスペックを選択したら、次の PowerShell コマンドを実行して、Azure VM（仮想マシン）拡張機能を操作します：

- サポートされている Azure VM 拡張機能の一覧を表示するには：<!JEKYLL@5180@39>
- さらに VM 拡張機能を追加するには：<!JEKYLL@5180@40>。例：<!JEKYLL@5180@41>

  次のいずれかを追加しようとするとコマンドが失敗し、エラーメッセージが表示されます：

  - Citrix 定義の拡張機能。
  - 既存のユーザー定義の拡張機能。
  - サポートされていない構成キー。現在、サポートされている構成キーは <!JEKYLL@5180@42> です。
- 一覧から拡張機能を削除するには：<!JEKYLL@5180@43>。追加した拡張機能は削除できます。

トラステッド起動を使用したマシンカタログ

トラステッド起動でマシンカタログを正常に作成するには、次を使用します：

- トラステッド起動を使用したマシンプロファイル
- トラステッド起動をサポートする VM サイズ
- トラステッド起動をサポートする Windows VM バージョン。現在、Windows 10、Windows 11、Windows Server 2016、2019、および 2022 はトラステッド起動をサポートしています。

> 重要:
>
> MCS は、トラステッド起動が有効な VM を使用した新しいカタログの作成をサポートしています。ただし、既存の永続カタログと既存の VM を更新するには、Azure Portal を使用する必要があります。非永続カタログのトラステッド起動を更新することはできません。詳しくは、Microsoft ドキュメント「既存の Azure VM でトラステッド起動を有効にする」を参照してください。

Citrix DaaS オファリングのインベントリアイテムを表示し、VM サイズがトラステッド起動をサポートしているかどうかを判断するには、次のコマンドを実行します:

1. PowerShell ウィンドウを開きます。
2. **asnp citrix*** を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. 次のコマンドを実行します:

   <!JEKYLL@5180@44>
4. <!JEKYLL@5180@45> を実行します
5. <!JEKYLL@5180@46> 属性の値を確認してください。

   - <!JEKYLL@5180@47> が **True** の場合、VM サイズはトラステッド起動をサポートします。
   - <!JEKYLL@5180@48> が **False** の場合、VM サイズはトラステッド起動をサポートしません。

Azure の PowerShell に従って、次のコマンドを使用してトラステッド起動をサポートする VM サイズを決定できます:

<!JEKYLL@5180@49>

以下は、「Azure PowerShell コマンドを実行した後、VM サイズがトラステッド起動をサポートするかどうか」について示した例です。

- 例 *1*: Azure VM が第 1 世代のみをサポートしている場合、その VM はトラステッド起動をサポートしていません。したがって、Azure PowerShell コマンドを実行した後、<!JEKYLL@5180@50> 機能は表示されません。
- 例 *2*: Azure VM が第 2 世代のみをサポートし、<!JEKYLL@5180@51> 機能が **True** の場合、第 2 世代の VM サイズはトラステッド起動ではサポートされません。
- 例 *3*: Azure VM が第 2 世代のみをサポートし、PowerShell コマンドの実行後に <!JEKYLL@5180@52> 機能が表示されない場合、第 2 世代の VM サイズはトラステッド起動でサポートされます。

Azure 仮想マシンのトラステッド起動ついて詳しくは、Microsoft のドキュメント「Azure Virtual Machines のトラステッド起動」を参照してください。

トラステッド起動を使用したマシンカタログの作成

1. トラステッド起動が有効になっているマスターイメージを作成します。Microsoft のドキュメント「トラステッド起動 VM イメージ」を参照してください。
2. セキュリティの種類をトラステッド起動 **VM** として VM またはテンプレートスペックを作成します。VM またはテンプレートスペックの作成について詳しくは、Microsoft ドキュメント「トラステッド起動の VM をデプロイする」を参照してください。
3. 完全な構成インターフェイスまたは PowerShell コマンドを使用して、マシンカタログを作成します。
   - 完全な構成インターフェイスを使用する場合、「完全な構成インターフェイスで Azure Resource Manager イメージを使用してマシンカタログを作成する」を参照してください。
   - PowerShell コマンドを使用する場合は、<!JEKYLL@5180@53> コマンドを使用し、マシンプロファイルの入力に VM またはテンプレートスペックを指定します。カタログ作成コマンドの完全な一覧については、「Creating a catalog」を参照してください。

     マシンプロファイルの入力に VM を使用した <!JEKYLL@5180@54> の例:

     <!JEKYLL@5180@55>

     マシンプロファイルの入力にテンプレートスペックを使用した <!JEKYLL@5180@56> の場合:

     <!JEKYLL@5180@57>

トラステッド起動でマシンカタログを作成する際のエラー

トラステッド起動を使用してマシンカタログを作成しているときに、次のシナリオに応じたエラーが発生します:

シナリオ	エラー
非管理対象カタログの作成中にマシンプロファイルを選択した場合	<!JEKYLL@5180@58>
非管理対象ディスクをマスターイメージとしてカタログを作成するときに、トラステッド起動をサポートするマシンプロファイルを選択した場合	<!JEKYLL@5180@59>
セキュリティの種類でトラステッド起動を使用し、マスターイメージソースを使用して管理カタログを作成するときに、マシンプロファイルを選択しない場合	<!JEKYLL@5180@60>
マスターイメージとは異なるセキュリティの種類のマシンプロファイルを選択した場合	<!JEKYLL@5180@61>
トラステッド起動をサポートしない VM サイズを選択しながら、カタログの作成時にトラステッド起動をサポートするマスターイメージを使用する場合	<!JEKYLL@5180@62>

マシンプロファイルのプロパティ値を使用する

マシンカタログは、カスタムプロパティで定義されている次のプロパティを使用します:

- アベイラビリティゾーン
- 専用ホストグループ ID
- ディスク暗号化セット ID
- OS の種類
- ライセンスの種類
- ストレージの種類

これらのカスタムプロパティが明示的に定義されていない場合、プロパティ値はマシンプロファイルとして使用されている ARM テンプレートスペックの指定または仮想マシンのいずれかから設定されます。また、<!JEKYLL@5180@63> が指定されていない場合は、マシンプロファイルから設定されます。

> 注:
>
> 一部のプロパティがマシンプロファイルで指定されておらず、カスタムプロパティで定義されていないとき、プロパティのデフォルト値が常に適用されます（該当する場合）。

次のセクションでは、<!JEKYLL@5180@64> ですべてのプロパティが定義されている場合、または値が MachineProfile から由来している場合、<!JEKYLL@5180@65> および <!JEKYLL@5180@66> でのシナリオについて説明します。

- New-ProvScheme シナリオ
  - MachineProfile ですべてのプロパティが定義され、CustomProperties は定義されていません。例:

    <!JEKYLL@5180@67>

    カタログのカスタムプロパティとして、次の値が設定されています:

    <!JEKYLL@5180@68>
  - MachineProfile で一部のプロパティが定義され、CustomProperties は定義されていません。例: MachineProfile には LicenseType と OsType のみが含まれます。

    <!JEKYLL@5180@69>

    カタログのカスタムプロパティとして、次の値が設定されています:

    <!JEKYLL@5180@70>
  - MachineProfile と CustomProperties の両方がすべてのプロパティを定義します。例:

    <!JEKYLL@5180@71>

    カスタムプロパティが優先されます。カタログのカスタムプロパティとして、次の値が設定されています:

    <!JEKYLL@5180@72>

  - 一部のプロパティは MachineProfile で定義され、一部のプロパティは CustomProperties で定義されます。例:

    * CustomProperties は、LicenseType と StorageAccountType を定義します
    * MachineProfile は、LicenseType、OsType、Zones を定義します

    <!JEKYLL@5180@73>

    カタログのカスタムプロパティとして、次の値が設定されています:

    <!JEKYLL@5180@74>

  - 一部のプロパティは MachineProfile で定義され、一部のプロパティは CustomProperties で定義されます。また、ServiceOffering は定義されていません。例:

    * CustomProperties は StorageType を定義します
    * MachineProfile は LicenseType を定義します

    <!JEKYLL@5180@75>

    カタログのカスタムプロパティとして、次の値が設定されています:

    <!JEKYLL@5180@76>

  - OsType が CustomProperties にも MachineProfile にもない場合、次のようになります:

    * 値はマスターイメージから読み取られます。
    * マスターイメージが非管理対象ディスクの場合、OsType は Windows に設定されます。例:

    <!JEKYLL@5180@77>

    マスターイメージの値は、カスタムプロパティに書き込まれます（この場合は Linux）。

    <!JEKYLL@5180@78>

- Set-ProvScheme シナリオ

  - 既存のカタログ:

    * <!JEKYLL@5180@79> および OsType の CustomProperties
    * Zones を定義する MachineProfile <!JEKYLL@5180@80>

  - 更新:

    * StorageAccountType を定義する MachineProfile mpB.vm
    * LicenseType と OsType を定義するカスタムプロパティの新しいセット $CustomPropertiesB

    <!JEKYLL@5180@81>

    カタログのカスタムプロパティとして、次の値が設定されています:

    <!JEKYLL@5180@82>

  - 既存のカタログ:

    * <!JEKYLL@5180@83> および OsType の CustomProperties
    * StorageAccountType と LicenseType を定義する MachineProfile <!JEKYLL@5180@84>

  – 更新:

    * StorageAccountType と OsType を定義するカスタムプロパティの新しいセット $Custom-PropertiesB

  <!JEKYLL@5180@85>

  カタログのカスタムプロパティとして、次の値が設定されています:

  <!JEKYLL@5180@86>

  – 既存のカタログ:

    * <!JEKYLL@5180@87> および OsType の CustomProperties
    * Zones を定義する MachineProfile <!JEKYLL@5180@88>

  – 更新:

    * StorageAccountType と LicenseType を定義する MachineProfile mpB.vm
    * <!JEKYLL@5180@89> は指定されていません

  <!JEKYLL@5180@90>

  カタログのカスタムプロパティとして、次の値が設定されています:

  <!JEKYLL@5180@91>

PowerShell を使用したアベイラビリティゾーンの構成

PowerShell を使用する場合、<!JEKYLL@5180@92> で Citrix DaaS オファリングのインベントリアイテムを表示できます。たとえば、米国東部リージョン <!JEKYLL@5180@93> のサービスオファリングを表示するには、以下を実行します:

<!JEKYLL@5180@94>

ゾーンを表示するには、アイテムの <!JEKYLL@5180@95> パラメーターを使用します:

<!JEKYLL@5180@96>

アベイラビリティゾーンが指定されていない場合、マシンのプロビジョニング方法に変更はありません。

PowerShell を使用してアベイラビリティゾーンを構成するには、<!JEKYLL@5180@97> 操作で、使用可能な **Zones** カスタムプロパティを使用します。**Zones** プロパティは、マシンをプロビジョニングするアベイラビリティゾーンの一覧を定義します。これらのゾーンには、1 つまたは複数のアベイラビリティゾーンを含めることができます。たとえば、Zones 1 と 3 の場合は、<!JEKYLL@5180@98> のようになります。

<!JEKYLL@5180@99> コマンドを使用して、プロビジョニングスキームのゾーンを更新します。

無効なゾーンが指定された場合、プロビジョニングスキームは更新されず、無効なコマンドを修正する方法を示すエラーメッセージが表示されます。

> ヒント：
>
> 無効なカスタムプロパティを指定すると、プロビジョニングスキームは更新されず、関連するエラーメッセージが表示されます。

ホストグループゾーンと **Azure Availability Zones** の同時使用の結果

カスタムプロパティで指定されたアベイラビリティゾーンとホストグループのゾーンに基づいて、マシンカタログの作成が成功するかどうかを評価する事前チェックがあります。アベイラビリティゾーンのカスタムプロパティがホストグループのゾーンと一致しない場合、カタログの作成は失敗します。

PowerShell を使用してアベイラビリティゾーンを構成する方法については、「PowerShell を使用したアベイラビリティゾーンの構成」を参照してください。

Azure 専用ホストについて詳しくは、「Azure 専用ホスト」を参照してください。

次の表は、アベイラビリティゾーンとホストグループゾーンのさまざまな組み合わせと、マシンカタログの作成が成功または失敗する結果を示しています。

ホストグループゾーン	カスタムプロパティの **Azure** アベイラビリティゾーン	マシンカタログの作成結果
指定。たとえば、ホストグループはゾーン 1 にあります	指定なし	成功。マシンはホストグループのゾーンに作成されます
指定。たとえば、ホストグループはゾーン 1 にあります	ホストグループゾーンと同じゾーン。たとえば、カスタムプロパティのゾーンは 1 に設定されます	成功。マシンはゾーン 1 に作成されます
指定。たとえば、ホストグループはゾーン 1 にあります	ホストグループゾーンとは異なります。たとえば、カスタムプロパティのゾーンは 2 に設定されます	指定されたアベイラビリティゾーンとホストグループのゾーンが一致しないため、事前チェック中に関連するエラーが発生してカタログの作成が失敗します
指定。たとえば、ホストグループはゾーン 1 にあります	複数のゾーンが指定されました。たとえば、カスタムプロパティのゾーンは 1、2 または 2、3 に設定されます	指定されたアベイラビリティゾーンとホストグループのゾーンが一致しないため、事前チェック中に関連するエラーが発生してカタログの作成が失敗します

ホストグループゾーン	カスタムプロパティの **Azure** アベイラビリティゾーン	マシンカタログの作成結果
指定なし。たとえば、ホスト グループのゾーンは <!JEKYLL@5180@100> です	指定なし	指定したアベイラビリティゾーンとホストグループのゾーンが一致する（つまり、ゾーンがない）ため、カタログの作成は成功します。マシンはどのゾーンにも作成されません
指定なし。たとえば、ホスト グループのゾーンは <!JEKYLL@5180@101> です	指定。たとえば、カスタムプロパティのゾーンは 1 つまたは複数のゾーンに設定されます	指定されたアベイラビリティゾーンとホストグループのゾーンが一致しないため、事前チェック中に関連するエラーが発生してカタログの作成が失敗します

Azure 専用ホストへの **VM** のプロビジョニング

MCS を使用して、Azure 専用ホストで VM をプロビジョニングできます。Azure 専用ホストで VM をプロビジョニングする前に、以下を実行します:

- ホストグループを作成します。
- そのホストグループにホストを作成します。
- カタログと仮想マシンを作成するために十分なホスト容量が確保されていることを確認してください。

管理者は、次の PowerShell スクリプトで定義されたホストテナントを持つマシンのカタログを作成できます:

<!JEKYLL@5180@102>

MCS を使用して、Azure 専用ホストで仮想マシンをプロビジョニングする場合、次の点を考慮してください:

- 専用ホストはカタログプロパティであり、カタログの作成後に変更することはできません。専用テナントは現在、Azure ではサポートされていません。
- <!JEKYLL@5180@103> パラメーターを使用する場合は、ホスティングユニットの領域に事前構成された Azure ホストグループが必要です。
- Azure の自動配置が必要です。この機能は、ホストグループに関連付けられたサブスクリプションをオンボードするように要求します。詳しくは、「Azure 専用ホストの VM スケールセット - パブリックプレビュー」を参照してください。自動配置が有効になっていない場合、MCS はカタログの作成中にエラーをスローします。

ストレージの種類の構成

MCS を使用する Azure 環境の仮想マシン用に異なるストレージの種類を選択します。ターゲット VM の場合、MCS は以下をサポートします:

- OS ディスク：プレミアム SSD、SSD または HDD
- ライトバックキャッシュディスク：プレミアム SSD、SSD、または HDD

これらのストレージの種類を使用するときは、次の点を考慮してください：

- VM が選択したストレージの種類をサポートしていることを確認してください。
- 構成で Azure エフェメラルディスクを使用している場合、ライトバックキャッシュディスク設定のオプションは使用できません。

> ヒント：
>
> <!JEKYLL@5180@104> は、OS タイプとストレージアカウント用に構成されています。<!JEKYLL@5180@105> は、ライトバックキャッシュのストレージの種類用に構成されています。通常のカタログの場合、<!JEKYLL@5180@106> が必要です。<!JEKYLL@5180@107> が構成されていない場合は、<!JEKYLL@5180@108> のデフォルトとして <!JEKYLL@5180@109> が使用されます。

WBCDiskStorageType が構成されていない場合、WBCDiskStorageType のデフォルトとして StorageType が使用されます

VM のストレージの種類の構成

VM 用のストレージの種類を構成するには、<!JEKYLL@5180@110> の <!JEKYLL@5180@111> パラメーターを使用します。既存カタログの <!JEKYLL@5180@112> パラメーター値を、サポートされているストレージ種類の 1 つに更新するには、<!JEKYLL@5180@113> コマンドを使用します。

以下は、プロビジョニングスキームで使用する <!JEKYLL@5180@114> パラメーターのセットの例です：

<!JEKYLL@5180@115>

ゾーン冗長ストレージの有効化

カタログの作成中にゾーン冗長ストレージを選択できます。ゾーン冗長ストレージは複数のアベイラビリティゾーンにわたって Azure Managed Disks を同期的に複製するため、別のゾーンの冗長を利用して、ゾーンでの障害から回復できます。

ストレージの種類のカスタムプロパティで **Premium_ZRS** および **StandardSSD_ZRS** を指定できます。ZRS ストレージは、既存のカスタムプロパティを使用するか、**MachineProfile** テンプレートを使用して設定できます。ZRS ストレージは、<!JEKYLL@5180@116> および <!JEKYLL@5180@117> パラメーターを指定した <!JEKYLL@5180@118> コマンドでもサポートされます。既存の VM を LRS ストレージから ZRS ストレージに変更できるのです。

> 注：
>
> - <!JEKYLL@5180@119> は、スケジュールの開始時刻が現在時刻であることを指定します。

> • 負の数（-1 など）の <!JEKYLL@5180@120> は、スケジュールの期間に上限がないことを示します。

制限事項:

- 管理対象ディスクでのみサポートされます
- プレミアムおよびスタンダードのソリッドステートドライブ（SSD）でのみサポートされます
- <!JEKYLL@5180@121> ではサポートされません
- 特定のリージョンでのみ利用できます。
- ZRS ディスクを大量に作成すると、Azure のパフォーマンスが低下します。したがって、最初の電源投入時には、小規模なバッチ（一度に 300 台未満のマシン）ごとにマシンの電源をオンにします。

ゾーン冗長ストレージをディスクストレージの種類として設定する

最初のカタログ作成時にゾーン冗長ストレージを選択するか、既存のカタログでストレージの種類を更新できます。

PowerShell コマンドを使用してゾーン冗長ストレージを選択する

<!JEKYLL@5180@122> Powershell コマンドを使用して Azure で新しいカタログを作成するときは、<!JEKYLL@5180@123> の値として <!JEKYLL@5180@124> を使用します。
例:

<!JEKYLL@5180@125>

この値を設定すると、適切に使用できるかどうかを判断する動的 API によって検証されます。ZRS の使用がカタログで有効でない場合、次の例外が発生する可能性があります:

- **StorageTypeAtShutdownNotSupportedForZrsDisks**: StorageTypeAtShutdown カスタムプロパティは、ZRS ストレージでは使用できません。
- **StorageAccountTypeNotSupportedInRegion**: この例外は、ZRS をサポートしていない Azure リージョンで ZRS ストレージを使用しようとすると発生します。
- **ZrsRequiresManagedDisks**: ゾーン冗長ストレージは、管理対象ディスクでのみ使用できます。

次のカスタムプロパティを使用して、ディスクストレージの種類を設定できます:

- <!JEKYLL@5180@126>
- <!JEKYLL@5180@127>
- <!JEKYLL@5180@128>

> 注:
>
> カスタムプロパティが設定されていない場合、カタログの作成中にマシンプロファイルの OS ディスク（<!JEKYLL@5180@129>）が使用されます。

マシンプロファイルから **VM** および **NIC** の診断設定をキャプチャする

マシンカタログの作成中、既存のマシンカタログの更新中、および既存の VM の更新中に、マシンプロファイルから VM および NIC の診断設定をキャプチャできます。

VM またはテンプレートスペックをマシンプロファイルのソースとして使用できます。

主な手順

1. Azure で必要な ID を設定します。これらの ID をテンプレートスペックで指定する必要があります。
    - ストレージアカウント
    - Log Analytics ワークスペース
    - 標準レベルの料金設定のイベントハブ名前空間
2. マシンプロファイルのソースを作成します。
3. 新しいマシンカタログを作成するか、既存のカタログを更新するか、既存の VM を更新します。

Azure で必要な **ID** を設定する

Azure で次のいずれかを設定します:

- ストレージアカウント
- Log Analytics ワークスペース
- 標準レベルの料金設定のイベントハブ名前空間

ストレージアカウントをセットアップする　Azure で標準ストレージアカウントを作成します。テンプレートスペックでは、ストレージアカウントの完全な resourceId を <!JEKYLL@5180@130> として指定します。

データをストレージアカウントに記録するように VM を設定すると、データは <!JEKYLL@5180@131> コンテナの下に表示されます。

Log Analytics ワークスペースをセットアップする　Log Analytics ワークスペースを作成します。テンプレートスペックでは、Log Analytics ワークスペースの完全な resourceId を workspaceId として指定します。

ワークスペースにデータを記録するように VM を設定すると、Azure のログでデータを照会できるようになります。ログで Azure の次のコマンドを実行すると、リソースによって記録されたすべてのメトリックの数を表示できます:

‘AzureMetrics

イベントハブをセットアップする　Azure Portal でイベントハブをセットアップするには、次の手順を実行します:

1. 標準レベルの料金設定でイベントハブ名前空間を作成します。
2. 名前空間の下にイベントハブを作成します。
3. イベントハブの下の **Capture** に移動します。Avro 出力タイプでキャプチャするにはトグルをオンにします。
4. 既存のストレージアカウントに新しいコンテナを作成して、ログをキャプチャします。
5. テンプレートスペックでは、`eventHubAuthorizationRuleId`を次の形式で指定します: `/subscriptions/093f4c12-704b-4b1d-8339-f339e7557f60/resourcegroups/matspo/providers/Microsoft.EventHub/namespaces/matspoeventhub/authorizationrules/RootManageSharedAccessKey`
6. イベントハブの名前を指定します。

イベントハブにデータを記録するように VM が設定されると、データは構成されたストレージコンテナにキャプチャされます。

マシンプロファイルのソースを作成する

VM またはテンプレートスペックをマシンプロファイルのソースとして使用できます。

診断設定を使用した **VM** ベースのマシンプロファイルの作成　VM をマシンプロファイルとして作成する場合は、まずテンプレート VM 自体で診断設定をセットアップします。Microsoft ドキュメント「Azure Monitor の診断設定」に記載されている詳細な手順を参照してください。

次のコマンドを実行して、VM または NIC に関連付けられた診断設定があることを確認できます:

```
az monitor diagnostic-settings list --resource-group matspo --resource
    matspo-tog-cc2659 --resource-type microsoft.network/
    networkInterfaces
<!--NeedCopy-->
```

```
az monitor diagnostic-settings list --resource-group matspo --resource
    matspo-tog-cc2 --resource-type microsoft.compute/virtualMachines
<!--NeedCopy-->
```

診断設定を使用したテンプレートスペックベースのマシンプロファイルの作成　既に診断設定が有効になっている VM を使用し、それを ARM テンプレートスペックにエクスポートする場合、これらの設定はテンプレート内に自動的に含まれません。ARM テンプレート内の診断設定を手動で追加または変更する必要があります。

ただし、マシンプロファイルとして VM が必要な場合、MCS は重要な診断設定が正確にキャプチャされ、MCS カタログ内のリソースに適用されることを保証します。

1. VM と NIC を定義する標準テンプレートスペックを作成します。

2. スペックに従って診断設定を展開するためのリソースを追加します：Microsoft.Insights diagnosticSettings。スコープについては、テンプレート内の VM または NIC を、部分的な ID を含めた名前で参照します。たとえば、テンプレートスペックで「test-VM」という名前の VM にアタッチされた診断設定を作成するには、スコープを次のように指定します：

```
"scope": "microsoft.compute/virtualMachines/test-VM",
<!--NeedCopy-->
```

3. テンプレートスペックをマシンプロファイルのソースとして使用します。

診断設定を使用したカタログの作成または更新

マシンプロファイルのソースを作成した後、`New-ProvScheme`コマンドを使用してマシンカタログを作成し、`Set-ProvScheme`コマンドを使用して既存のマシンカタログを更新し、`Request-ProvVMUpdate`コマンドを使用して既存の VM を更新できるようになりました。

Windows ライセンスの確認

プロビジョニングされた仮想マシンがライセンス特典を使用していることを確認するには、次の PowerShell コマンドを実行します：`Get-AzVM -ResourceGroup MyResourceGroup -Name MyVM`。

- [Windows Server のライセンスの種類] で、ライセンスの種類が [**Windows_Server**] であることを確認します。詳しくは、https://docs.microsoft.com/en-us/azure/virtual-machines/windows/hybrid-use-benefit-licensing/を参照してください。
- [Windows クライアントのライセンスの種類]で、ライセンスの種類が [**Windows_Client**]であることを確認します。詳しくは、https://docs.microsoft.com/en-us/azure/virtual-machines/windows/windows-desktop-multitenant-hosting-deployment/を参照してください。

または、`Get-Provscheme` PowerShell SDK を使用して確認することもできます。例: `Get-Provscheme -ProvisioningSchemeName "My Azure Catalog"`。このコマンドレットについて詳しくは、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Get-ProvScheme/を参照してください。

Linux ライセンスの構成

bring-your-own-subscription（BYOS）Linux ライセンスを使用すると、ソフトウェアの料金を支払う必要がなくなります。BYOS の料金には、コンピューティングハードウェアの料金のみが含まれます。ライセンスには次の 2 種類があります：

- **RHEL_BYOS**：RHEL_BYOS の種類を正しく使用するには、Azure サブスクリプションで Red Hat Cloud Access を有効にします。

- **SLES_BYOS**: SLES の BYOS バージョンには、SUSE からのサポートが含まれています。

LicenseType 値を`New-ProvScheme`および`Set-ProvScheme`で Linux オプションに設定できます。

LicenseType を`New-ProvScheme`で RHEL_BYOS に設定した例:

```
New-ProvScheme -CleanOnBoot -ProvisioningSchemeName "azureCatalog" -
    RunAsynchronously -Scope @() -SecurityGroup @() -CustomProperties '<
    CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"><Property xsi:type="StringProperty" Name="UseManagedDisks"
     Value="true" /><Property xsi:type="StringProperty" Name="
    StorageAccountType" Value="StandardSSD_LRS" /><Property xsi:type="
    StringProperty" Name="ResourceGroups" Value="hu-dev-mcs" /><Property
     xsi:type="StringProperty" Name="OsType" Value="Linux" /><Property
    xsi:type="StringProperty" Name="LicenseType" Value="RHEL_BYOS" /></
    CustomProperties>'
<!--NeedCopy-->
```

LicenseType を`Set-ProvScheme`で SLES_BYOS に設定した例:

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog" -CustomProperties
     '<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"><Property xsi:type="StringProperty" Name="UseManagedDisks"
     Value="true" /><Property xsi:type="StringProperty" Name="
    StorageAccountType" Value="StandardSSD_LRS" /><Property xsi:type="
    StringProperty" Name="ResourceGroups" Value="hu-dev-mcs" /><Property
     xsi:type="StringProperty" Name="OsType" Value="Linux" /><Property
    xsi:type="StringProperty" Name="LicenseType" Value="SLES_BYOS" /></
    CustomProperties>'
<!--NeedCopy-->
```

> 注:
>
> `LicenseType`値が空の場合、デフォルト値は、OsType 値に応じて、Azure Windows Server ライセンスまたは Azure Linux ライセンスになります。

LicenseType を空にした例:

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog" -CustomProperties
     '<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"><Property xsi:type="StringProperty" Name="UseManagedDisks"
     Value="true" /><Property xsi:type="StringProperty" Name="
    StorageAccountType" Value="StandardSSD_LRS" /><Property xsi:type="
    StringProperty" Name="ResourceGroups" Value="hu-dev-mcs" /><Property
     xsi:type="StringProperty" Name="OsType" Value="Linux" /></
    CustomProperties>'
<!--NeedCopy-->
```


Azure エフェメラルディスクを使用したマシンカタログの作成

New-ProvSchemeを使用してエフェメラル OS ディスクのプロビジョニングをするには、次の制約を考慮してください:

- カタログに使用される VM サイズは、エフェメラル OS ディスクをサポートする必要があります。
- VM サイズに関連付けられているキャッシュまたは一時ディスクのサイズは、OS ディスクのサイズ以上である必要があります。
- 一時ディスクのサイズは、キャッシュディスクのサイズよりも大きい必要があります。

これらの制約を考慮する必要があるのは、以下の場合です:

- プロビジョニングスキームを作成する場合
- プロビジョニングスキームを変更する場合
- イメージを更新する場合

エフェメラルディスクを使用するには、New-ProvSchemeを実行するとき、カスタムプロパティUseEphemeralOsDiskを **true** に設定する必要があります。

> 注:
>
> カスタムプロパティUseEphemeralOsDiskが **false** に設定されているか、値が指定されていない場合、プロビジョニングされたすべての VDA は引き続きプロビジョニングされた OS ディスクを使用します。

以下は、プロビジョニングスキームで使用するカスタムプロパティのセットの例です:

```
"CustomProperties": [
            {

                "Name": "UseManagedDisks",
                "Value": "true"
             }
 ,
            {

                "Name": "StorageType",
                "Value": "Standard_LRS"
             }
 ,
            {

                "Name": "UseSharedImageGallery",
                "Value": "true"
             }
 ,
            {

                "Name": "SharedImageGalleryReplicaRatio",
                "Value": "40"
             }
```



```
25  ,
26              {
27
28                  "Name": "SharedImageGalleryReplicaMaximum",
29                  "Value": "10"
30               }
31  ,
32              {
33
34                  "Name": "LicenseType",
35                  "Value": "Windows_Server"
36               }
37  ,
38              {
39
40                  "Name": "UseEphemeralOsDisk",
41                  "Value": "true"
42               }
43
44          ],
45  <!--NeedCopy-->
```

既存のカタログのエフェメラルディスクを構成する

既存のカタログの Azure エフェメラル OS ディスクを構成するには、Set-ProvSchemeのUseEphemeralOsDiskパラメーターを使用します。UseEphemeralOsDiskパラメーターの値を「**true**」に設定します。

> 注:
>
> この機能を使用するには、パラメーターのUseManagedDisksとUseSharedImageGalleryも有効にする必要があります。

例:

```
1  Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties <
       CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
       machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
       instance">
2  <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
        />
3  <Property xsi:type="StringProperty" Name="UseSharedImageGallery" Value=
       "true" />
4  <Property xsi:type="StringProperty" Name="UseEphemeralOsDisk" Value="
       true" />
5  </CustomProperties>'
6  <!--NeedCopy-->
```


Azure Compute Gallery を構成する

`New-ProvScheme`コマンドを使用することで、Azure Compute Gallery をサポートするプロビジョニングスキームを作成します。`Set-ProvScheme`コマンドでは、プロビジョニングスキームでのこの機能の有効化または無効化と、レプリカの比率およびレプリカの最大値の変更が可能です。

Azure Compute Gallery 機能をサポートするために、プロビジョニングスキームに 3 つのカスタムプロパティが追加されました:

`UseSharedImageGallery`

- Azure Compute Gallery を使用して公開イメージを保存するかどうかを定義します。**True** に設定すると、イメージは Azure Compute Gallery イメージとして保存されます。True に設定しない場合、イメージはスナップショットとして保存されます。
- 有効な値は、**True** および **False** です。
- プロパティが定義されていない場合、デフォルト値は **False** です。

`SharedImageGalleryReplicaRatio`

- ギャラリーイメージバージョンのレプリカに対するマシンの比率を定義します。
- 有効な値は、0 より大きい整数です。
- プロパティが定義されていない場合は、デフォルト値が使用されます。永続 OS ディスクのデフォルト値は 1000 であり、非永続 OS ディスクのデフォルト値は 40 です。

`SharedImageGalleryReplicaMaximum`

- 各ギャラリーイメージバージョンのレプリカの最大数を定義します。
- 有効な値は、0 より大きい整数です。
- プロパティが定義されていない場合、デフォルト値は 10 です。
- Azure は現在、ギャラリーイメージの単一バージョンに対して最大 10 個のレプリカをサポートしています。プロパティが Azure でサポートされている値よりも大きい値に設定されている場合、MCS は指定された値を使用しようとします。Azure はエラーを生成し、MCS ログでは現在のレプリカ数が変更されずに残ります。

> ヒント:
>
> Azure Compute Gallery を使用して MCS プロビジョニングされたカタログの公開イメージを保存する場合、MCS は、カタログ内のマシンの数、レプリカの比率、およびレプリカの最大数に基づいて、ギャラリーイメージバージョンのレプリカ数を設定します。レプリカ数は、カタログ内のマシンの数をレプリカ比率（最も近い整数値に切り上げ）で除算し、最大レプリカ数で値を制限することによって計算されます。たとえば、レプリカの比率が 20 で最大 5 の場合、0～20 台のマシンで 1 つのレプリカが作成され、21～40 台で 2 つ、41～60 台で 3 つ、61～80 台で 4 つ、81 台以上で 5 つのレプリカが作成されます。

ユースケース：**Azure Compute Gallery** のレプリカ比率とレプリカの最大値を更新する

既存のマシンカタログは Azure Compute Gallery を使用します。Set-ProvSchemeコマンドを使用して、カタログ内の既存のすべてのマシンおよび将来のマシンのカスタムプロパティを更新します：

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"> <Property xsi:type="StringProperty" Name="StorageType"
    Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="
    UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
    Name="UseSharedImageGallery" Value="True"/> <Property xsi:type="
    IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/> <
    Property xsi:type="IntProperty" Name="
    SharedImageGalleryReplicaMaximum" Value="20"/></CustomProperties>'
<!--NeedCopy-->
```

ユースケース：**Azure Compute Gallery** カタログをスナップショットカタログに変換する

このユースケースの場合：

1. UseSharedImageGalleryフラグを **True** に設定してSet-ProvSchemeを実行します。オプションで、SharedImageGalleryReplicaRatioおよびSharedImageGalleryReplicaMaximumプロパティを含めます。
2. カタログを更新します。
3. マシンの電源を入れ直して、強制的に更新します。

例：

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"> <Property xsi:type="StringProperty" Name="StorageType"
    Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="
    UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
    Name="UseSharedImageGallery" Value="True"/> <Property xsi:type="
    IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/> <
    Property xsi:type="IntProperty" Name="
    SharedImageGalleryReplicaMaximum" Value="20"/></CustomProperties>'
<!--NeedCopy-->
```

> ヒント：
>
> パラメーターSharedImageGalleryReplicaRatioおよびSharedImageGalleryReplicaMaximumは必須ではありません。Set-ProvSchemeコマンドが完了した後、Azure Compute Gallery イメージはまだ作成されていません。ギャラリーを使用するようにカタログを構成すると、次回のカタログ更新操作で公開イメージがギャラリーに保存されます。カタログ更新コマンドは、ギャラリー、ギャラリーイメージ、および

> イメージバージョンを作成します。マシンの電源を入れ直すとマシンが更新されます。そのとき、必要に応じてレプリカ数が更新されます。それ以降、既存のすべての非永続マシンは Azure Compute Gallery イメージを使用してリセットされ、新しくプロビジョニングされたすべてのマシンはイメージを使用して作成されます。古いスナップショットは、数時間以内に自動的にクリーンアップされます。

ユースケース：**Azure Compute Gallery** カタログをスナップショットカタログに変換する

このユースケースの場合：

1. `UseSharedImageGallery`フラグを **False** に設定するか、定義せずに`Set-ProvScheme`を実行します。
2. カタログを更新します。
3. マシンの電源を入れ直して、強制的に更新します。

例：

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"> <Property xsi:type="StringProperty" Name="StorageType"
    Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="
    UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
    Name="UseSharedImageGallery" Value="False"/></CustomProperties>'
<!--NeedCopy-->
```

> ヒント：
>
> スナップショットから Azure Compute Gallery カタログへの更新とは異なり、各マシンのカスタムデータの更新では、また、新しいカスタムプロパティが反映されていません。次のコマンドを実行して、元の Azure Compute Gallery のカスタムプロパティを表示します：`Get-ProvVm -ProvisioningSchemeName catalog-name`。`Set-ProvScheme`コマンドが完了した後、イメージスナップショットはまだ作成されていません。ギャラリーを使用しないようにカタログを構成すると、次回のカタログ更新操作で公開イメージがスナップショットとして保存されます。その時点から、既存のすべての非永続マシンはスナップショットを使用してリセットされ、新しくプロビジョニングされたすべてのマシンはスナップショットから作成されます。マシンの電源を入れ直すと更新され、そのときカスタムマシンデータが更新されて、`UseSharedImageGallery`が **False** に設定されていることが反映されます。古い Azure Compute Gallery アセット（ギャラリー、画像、バージョン）は、数時間以内に自動的にクリーンアップされます。

VM ごとに複数の **NIC** を含むカタログを作成または更新する

MCS は、仮想マシンごとに複数の NIC をサポートします。仮想マシン上の複数の NIC を複数のサブネットに関連付けることができますが、それらのサブネットは同じ仮想ネットワーク（vNet）内に存在する必要があります。PowerShell コマンドを使用して、次のことができます：

- 仮想マシン上に複数の NIC を含むカタログを作成する
- 既存のカタログ構成を更新して仮想マシン上に複数の NIC を設定し、新しく作成された仮想マシンに複数の NIC が割り当てられるようにする
- 複数の NIC が割り当てられるように既存の仮想マシンを更新する

非マシンプロファイルベースのマシンカタログまたはマシンプロファイルベースのマシンカタログを作成または更新して、仮想マシン上で複数の NIC を割り当てることができます。現在、マシンプロファイルベースのマシンカタログの場合、ソースであるマシンプロファイルで指定されているのと同じ数の NIC のみを持つことができます。

高速ネットワークやネットワークセキュリティグループなどのプロパティは、マシンプロファイルをソースとして設定されます。

> 注:
>
> 仮想マシンのサイズは、同じ数の NIC と対応する高速ネットワークをサポートしている必要があります。サポートしていない場合は、エラーが発生します。

選択した仮想マシンサイズに割り当てられた NIC の最大数を取得できます。`MaxNetworkInterfaces`という PowerShell プロパティは、`get-item` PowerShell コマンドに`AdditionalData`パラメーターを指定して実行すると、NIC の最大数を表示します。

最大 **NIC** 数を取得する

最大 NIC 数を取得するには、以下の手順を実行します:

1. Delivery Controller ホストから **PowerShell** ウィンドウを開きます。
2. `asnp citrix*`を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. `Get-ChildItem -Path "XDHyp:\Connections\abc-connection\East US.region\serviceoffering.folder"`を実行して、利用可能なすべての仮想マシンサイズを一覧表示します。
4. `get-item -Path "XDHyp:\Connections\abc-connection\East US.region\serviceoffering.folder\Standard_M416ms_v2.serviceoffering").AdditionalData`を実行します
5. NIC の最大数を取得するには、`MaxNetworkInterfaces`を確認します。

仮想マシン上に複数の **NIC** を含むカタログを作成する

仮想マシン上に複数の NIC を含むカタログを作成するには、次の手順を実行します:

1. Delivery Controller ホストから PowerShell ウィンドウを開きます。
2. `asnp citrix*`を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. ID プールをまだ作成していない場合は作成します。
4. プロビジョニングスキームを作成します:

- 非マシンプロファイルベースのマシンカタログを作成する場合は、New-ProvSchemeコマンドにNetworkMappingsパラメーターを指定して実行します。パラメーターNetworkMappingsには複数のサブネットを追加できます。例:

```
New-Provscheme -NetworkMappings @{
"0"="subnetpath1";"1"="subnetpath1" }

<!--NeedCopy-->
```

- マシンプロファイルベースのマシンカタログを作成する場合は、以下を実行します:

  a) Azure に仮想マシンを作成して複数の NIC を設定します。詳しくは、「複数の NIC を持つ Windows 仮想マシンの作成と管理」を参照してください。新しい仮想マシンを作成し、Azure Portal の［Networking］ページでネットワーク インターフェイスをアタッチすることもできます。

  b) New-ProvSchemeコマンドを実行して、仮想マシンをマシンプロファイルの入力に使用します。

> 注:
>
> マシンプロファイルベースのマシンカタログを作成する場合、NetworkMappingsの数はマシンプロファイルのNetworkInterfaceCountと同じである必要があります。NetworkInterfaceCountはGet-item -Path "machine profile path"の AdditionalDataから取得できます。

5. カタログの作成を完了します。

VM 上で複数の **NIC** を含むカタログを更新する

仮想マシン上で複数の NIC を含むカタログを更新するには、次の手順を実行します:

1. Delivery Controller ホストから **PowerShell** ウィンドウを開きます。
2. asnp citrix*を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. プロビジョニングスキームを更新します:

- 非マシンプロファイルベースのマシンカタログを作成する場合は、Set-ProvSchemeコマンドにNetworkMappingsパラメーターを指定して実行します。パラメーターNetworkMappingsに複数のサブネットを追加できます。例:

```
Set-Provscheme -NetworkMappings @{
"0"="subnetpath1";"1"="subnetpath1" }

<!--NeedCopy-->
```

- マシンプロファイルに基づいてマシンカタログを作成するには、以下の手順を実行します:

  a) Azure に仮想マシンを作成して複数の NIC を設定します。詳しくは、「複数の NIC を持つ Windows 仮想マシンの作成と管理」を参照してください。

b) Set-ProvSchemeコマンドを実行して、仮想マシンをマシンプロファイルの入力に使用します。

VM 上で複数の **NIC** が割り当てられるように既存の仮想マシンを更新する

Set-ProvVMUpdateTimeWindowを使用して既存の仮想マシンを更新したり、更新作業時間中に既存の仮想マシンの電源を入れ直したりすることもできます。既存の仮想マシンの更新について詳しくは、「プロビジョニングされたマシンを現在のプロビジョニングスキームの状態に更新する」を参照してください。

非永続的なライトバックキャッシュディスクのマシンカタログを作成する

非永続的なライトバックキャッシュディスクのカタログを構成するには、PowerShell パラメーターNew-ProvScheme CustomPropertiesを使用します。カスタムプロパティは次のとおりです:

- UseTempDiskForWBC。このプロパティは、ライトバックキャッシュファイルを保存するのに、Azure一時ストレージの使用を受け入れるかどうかを示します。一時ディスクをライトバックキャッシュディスクとして使用する場合は、New-ProvSchemeを実行時に「true」に設定する必要があります。このパラメーターが指定されていない場合、デフォルトは False に設定されます。

例: CustomPropertiesパラメーターを使用してUseTempDiskForWBCを true に設定した場合:

```
    -CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/XMLSchema-instance"> `
    <Property xsi:type="StringProperty" Name="PersistWBC" Value="false"/> `
    <Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false"/> `
    <Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `
    <Property xsi:type="StringProperty" Name="StorageAccountType" Value="Premium_LRS"/> `
    <Property xsi:type="StringProperty" Name="WBCDiskStorageType" Value="Premium_LRS"/> `
    <Property xsi:type="StringProperty" Name="LicenseType" Value="Windows_Client"/> `
    <Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value="true"/> `
    </CustomProperties>'
<!--NeedCopy-->
```

> 注:
>
> マシンカタログをコミットして、ライトバックキャッシュファイル用として Azure ローカル一時ストレージを使用すると、後から VHD を使用するように変更することはできません。

永続的なライトバックキャッシュディスクのマシンカタログを作成する

永続的なライトバックキャッシュディスクのカタログを構成するには、PowerShell パラメーターNew-ProvScheme CustomPropertiesを使用します。

> ヒント:
>
> PowerShell パラメーターNew-ProvScheme CustomPropertiesは、クラウドベースのホスティング接続にのみ使用してください。オンプレミスソリューション（XenServer など）で永続的なライトバックキャッシュディスクを使用してマシンをプロビジョニングする場合、ディスクは自動的に永続化されるため、PowerShell は必要ありません。

このパラメーターでは追加プロパティPersistWBCをサポートしており、これを使用することで、MCS でプロビジョニングされたマシンのライトバックキャッシュディスクを永続化させる方法を指定できます。PersistWBCプロパティは、UseWriteBackCacheパラメーターが指定され、WriteBackCacheDiskSizeパラメーターがディスクが作成されたことを示すよう設定された場合のみ使用されます。

> 注:
>
> この動作は、電源を入れ直したときにデフォルトの MCSIO ライトバックキャッシュディスクが削除されて再作成される Azure および GCP の両方に適用されます。ディスクを永続化すると、MCSIO ライトバックキャッシュディスクの削除と再作成を回避できます。

以下は、PersistWBCをサポートする前にCustomPropertiesパラメーターで使用されるプロパティの例です:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
   benvaldev5RG3" />
</CustomProperties>
<!--NeedCopy-->
```

> 注:
>
> この例は Azure にのみ適用されます。このプロパティは GCP 環境では異なります。

これらのプロパティを使用するときは、プロパティがCustomPropertiesパラメーターから省略されている場合にデフォルトの値が含まれるようにしてください。PersistWBCプロパティには、次の 2 つの値が設定可能です：**true** または **false**。

PersistWBCプロパティを **true** に設定すると、Citrix DaaS 管理者が管理インターフェイスでマシンをシャットダウンしたときに、ライトバックキャッシュディスクが消去されなくなります。

PersistWBCプロパティを **false** に設定すると、Citrix DaaS 管理者が管理インターフェイスでマシンをシャットダウンしたときに、ライトバックキャッシュディスクが消去されます。

> 注:
>
> PersistWBCプロパティを省略する場合、デフォルトは **false** になり、管理インターフェイスでマシンをシャットダウンするとライトバックキャッシュは消去されます。

例: CustomPropertiesパラメーターを使用してPersistWBCを true に設定した場合:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
   benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />
</CustomProperties>
<!--NeedCopy-->
```

> 重要:
>
> PersistWBCプロパティは、New-ProvScheme PowerShell コマンドレットを使用してのみ設定できます。作成後にプロビジョニングスキームのCustomPropertiesを変更しようとしても、マシンがシャットダウンしたときにマシンカタログやライトバックキャッシュディスクの永続性は影響を受けません。

例: PersistWBCプロパティを true に設定するときにNew-ProvSchemeを設定してライトバックキャッシュを使用した場合:

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
   /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
   XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"
   true`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`" Value
   =`"Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`" Value=`"
   benvaldev5RG3`" />
<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"true`
   " />
</CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
   GoldImages.resourcegroup\W10MCSIO-01
   _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
```



```
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
    CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
    adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
   folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
<!--NeedCopy-->
```

MCSIO による起動パフォーマンスの向上

MCSIO が有効な場合、Azure や GCP の管理対象ディスクの起動パフォーマンスを向上させることができます。New-ProvSchemeコマンドで PowerShell カスタムプロパティPersistOSDiskを使用してこの機能を構成します。New-ProvSchemeに関連するオプションは次のとおりです:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
   benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
   />
</CustomProperties>
<!--NeedCopy-->
```

この機能を有効にするには、カスタムプロパティPersistOSDiskを **true** に設定します。例:

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
   /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
   XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
   UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
   StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
   /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
   Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
   =`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
   GoldImages.resourcegroup\W10MCSIO-01
   _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
```



```
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
    CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
    adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
   folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
<!--NeedCopy-->
```

顧客管理暗号キーを使用したマシンカタログの作成

PowerShell コマンドを使用して、暗号化キーが顧客管理キーであるマシンカタログを作成する場合は、次の手順を実行します:

1. PowerShell ウィンドウを開きます。
2. `asnp citrix*`を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. 「`cd xdhyp:/`」を入力します。
4. 「`cd .\HostingUnits\(your hosting unit)`」を入力します。
5. 「cd diskencryptionset.folder」と入力します。
6. 「dir」と入力して、ディスク暗号化セットのリストを取得します。
7. ディスク暗号化セットの ID をコピーします。
8. ディスク暗号化セットの ID を含むカスタムプロパティ文字列を作成します。例:

```
$customProperties = "<CustomProperties xmlns=`"http://schemas.
   citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.
   org/2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"persistWBC`" Value=`"
   False`" />
<Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`" Value
   =`"false`" />
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
   Value=`"true`" />
<Property xsi:type=`"StringProperty`" Name=`"DiskEncryptionSetId`"
    Value=`"/subscriptions/0xxx4xxx-xxb-4bxx-xxxx-xxxxxxxx/
   resourceGroups/abc/providers/Microsoft.Compute/
   diskEncryptionSets/abc-des`"/>
</CustomProperties>
<!--NeedCopy-->
```

9. ID プールをまだ作成していない場合は作成します。例:


```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms## -
    Domain def.local -NamingSchemeType Numeric
<!--NeedCopy-->
```

10. New-ProvScheme コマンドを実行します。例:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name" -
    IdentityPoolName "name" -InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits\azure-res2\image.folder\def.
    resourcegroup\def.snapshot"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\azure-res2\virtualprivatecloud.folder\
     def.resourcegroup\def-vnet.virtualprivatecloud\subnet1.network
     " }

-ProvisioningSchemeName "name"
-ServiceOffering "XDHyp:\HostingUnits\azure-res2\serviceoffering.
    folder\Standard_DS2_v2.serviceoffering"
-MachineProfile "XDHyp:\HostingUnits<adnet>\machineprofile.folder<
    def.resourcegroup><machine profile vm.vm>"
-CustomProperties $customProperties
<!--NeedCopy-->
```

11. マシンカタログの作成を完了します。

ホスト機能での暗号化を使用してマシンカタログを作成する

ホスト機能での暗号化を使用してマシンカタログを作成するには

1. ホスト機能での暗号化がサブスクリプションで有効になっているかどうかを確認します。確認する方法については、「https://learn.microsoft.com/en-us/rest/api/resources/features/get?tabs=HTTP/」を参照してください。有効になっていない場合は、サブスクリプションの機能を有効にする必要があります。サブスクリプションでこの機能を有効にする方法については、「https://learn.microsoft.com/en-us/azure/virtual-machines/disks-enable-host-based-encryption-portal?tabs=azure-powershell#prerequisites/」を参照してください。
2. 使用する Azure VM のサイズがホストでの暗号化をサポートしているかどうかを確認します。確認するには、PowerShell ウィンドウで次のいずれかを実行します:

```
PS XDHyp:\Connections<your connection>\east us.region\
    serviceoffering.folder>
<!--NeedCopy-->
```

```
PS XDHyp:\HostingUnits<your hosting unit>\serviceoffering.folder>
<!--NeedCopy-->
```

3. Azure Portal でホストでの暗号化を有効にして、マシンプロファイルの入力として、VM またはテンプレートスペックを作成します。

- VM を作成する場合は、ホストでの暗号化をサポートしている VM サイズを選択します。VM を作成すると、VM プロパティの［**Encryption at host**］が有効になります。
- テンプレートスペックを使用する場合は、`Encryption at Host`パラメーターを`securityProfile`内で **true** にします。

4. VM またはテンプレートスペックを選択して、マシンプロファイルワークフローで MCS マシンカタログを作成します。

   - OS ディスクまたはデータディスク：顧客管理キーとプラットフォーム管理キーによって暗号化されます
   - エフェメラル OS ディスク：プラットフォーム管理キーだけで暗号化されます
   - キャッシュディスク：顧客管理キーとプラットフォーム管理キーによって暗号化されます

   完全な構成インターフェイスを使用するか、PowerShell コマンドを実行して、マシンカタログを作成できます。

マシンプロファイルからホストでの暗号化情報を取得する

`AdditionalData`パラメーターを指定して PowerShell コマンドを実行すると、マシンプロファイルからホストでの暗号化情報を取得できます。`EncryptionAtHost`パラメーターが **True** の場合、ホストでの暗号化がマシンプロファイルに対して有効であることを示します。

例：マシンプロファイル入力が VM の場合、次のコマンドを実行します：

```
(get-item XDHyp:\HostingUnits\myAzureNetwork\machineprofile.folder\abc.
    resourcegroup\def.vm).AdditionalData
<!--NeedCopy-->
```

例：マシンプロファイル入力がテンプレートスペックの場合、次のコマンドを実行します：

```
(get-item XDHyp:\HostingUnits\myAzureNetwork\machineprofile.folder\abc.
    resourcegroup\def_templatespec.templatespec\EncryptionAtHost.
    templatespecversion).AdditionalData
<!--NeedCopy-->
```

二重暗号化を使用したマシンカタログの作成

完全な構成インターフェイスを使用するか、PowerShell コマンドを実行することで、二重暗号化を使用してマシンカタログを作成し、更新できます。

二重暗号化を使用してマシンカタログを作成する方法の詳細な手順は次のとおりです。

1. プラットフォーム管理キーと顧客が管理するキーを使用して Azure Key Vault と DES を作成します。Azure Key Vault と DES を作成する方法については、「Azure portal を使用して、マネージドディスクの保存時の二重暗号化を有効にします」を参照してください。

2. ホスト接続で利用可能なディスク暗号化セットを参照するには、次の手順を実行します:

   a) **PowerShell** ウィンドウを開きます。
   b) 次の PowerShell コマンドを実行します:

      i. `asnp citrix*`
      ii. `cd xdhyp:`
      iii. `cd HostingUnits`
      iv. `cd YourHostingUnitName (ex. azure-east)`
      v. `cd diskencryptionset.folder`
      vi. `dir`

   `DiskEncryptionSet`の ID を使用したカスタムプロパティで、カタログを作成または更新できます。

3. マシンプロファイルワークフローを使用する場合は、マシンプロファイルの入力用に VM またはテンプレートスペックを作成します。

   - VM をマシンプロファイルの入力に使用する場合は、次の手順を実行します:

     a) Azure Portal で VM を作成します。
     b) **Disks > Key management** に移動して、VM を`DiskEncryptionSetID`で直接暗号化します。

   - テンプレートスペックをマシンプロファイルの入力に使用する場合は、次の手順を実行します:

     a) テンプレートの`properties>storageProfile>osDisk>managedDisk`の下に`diskEncryptionSet`パラメーターを追加し、二重暗号化の DES の ID を追加します。

4. マシンカタログを作成します。

   - 完全な構成インターフェイスを使用している場合は、「マシンカタログの作成」の手順に加えて、次のいずれかを実行します。

     - マシンプロファイルベースのワークフローを使用しない場合は、[ディスク設定] ページで、[次のキーを使用して各マシンのデータを暗号化] を選択します。次に、ドロップダウンリストから二重暗号化の DES を選択します。カタログの作成を続けます。
     - マシンプロファイルワークフローを使用している場合は、[イメージ] ページでマスターイメージ（または準備されたイメージ）とマシンプロファイルを選択します。マシンプロファイルのプロパティにディスク暗号化セット ID があることを確認してください。

     カタログ内に作成されたすべてのマシンは、選択した DES に関連付けられたキーによって二重暗号化されます。

   - PowerShell コマンドを使用する場合は、次のいずれかを実行します:

     - マシンプロファイルベースのワークフローを使用しない場合は、`New-ProvScheme`コマンドにカスタムプロパティ`DiskEncryptionSetId`を追加します。例:


```
New-ProvScheme -CleanOnBoot -CustomProperties '<
    CustomProperties xmlns="http://schemas.citrix.com/2014/
    xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/
    XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks"
     Value="true" />
<Property xsi:type="StringProperty" Name="
    StorageAccountType" Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="
    DiskEncryptionSetId" Value="/subscriptions/12345678-
    xxxx-1234-1234-123456789012/resourceGroups/Sample-RG/
    providers/Microsoft.Compute/diskEncryptionSets/
    SampleEncryptionSet" />
</CustomProperties>'
-HostingUnitName "Redacted"
-IdentityPoolName "Redacted"
-InitialBatchSizeHint 1
-MasterImageVM "Redacted"
-NetworkMapping @{
"0"="Redacted" }

-ProvisioningSchemeName "Redacted"
-ServiceOffering "Redacted"
<!--NeedCopy-->
```

- マシンプロファイルベースのワークフローを使用する場合は、New-ProvSchemeコマンドで入力したマシンプロファイルを使用します。例:

```
New-ProvScheme -CleanOnBoot
-HostingUnitName azure-east
-IdentityPoolName aio-ip
-InitialBatchSizeHint 1
-MasterImageVM XDHyp:\HostingUnits\azure-east\image.folder
    \abc.resourcegroup\fgb-vda-snapshot.snapshot
-NetworkMapping @{
"0"="XDHyp:\HostingUnits\azure-east\virtualprivatecloud.
    folder\apa-resourceGroup.resourcegroup\apa-
    resourceGroup-vnet.virtualprivatecloud\default.network"
     }

-ProvisioningSchemeName aio-test
-MachineProfile XDHyp:\HostingUnits\azure-east\
    machineprofile.folder\abc.resourcegroup\abx-mp.
    templatespec\1.0.0.templatespecversion
<!--NeedCopy-->
```

Remote PowerShell SDK を使用してカタログの作成を完了します。Remote PowerShell SDK を使用してカタログを作成する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/を参照してください。カタログ内に作成されたすべてのマシンは、選択した DES に関連付けられたキーによって二重暗号化されます。

暗号化されていないカタログを二重暗号化を使用するように変換

マシンカタログの暗号化の種類を（カスタムプロパティまたはマシンプロファイルを使用して）更新できます。

- マシンプロファイルベースのワークフローを使用しない場合は、Set-ProvSchemeコマンドにカスタムプロパティ DiskEncryptionSetId を追加します。例:

```
1  Set-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
2  -CustomProperties '<CustomProperties xmlns="http://schemas.citrix
       .com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org
       /2001/XMLSchema-instance">
3  <Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
       Value="/subscriptions/12345678-xxxx-1234-1234-123456789012/
       resourceGroups/Sample-RG/providers/Microsoft.Compute/
       diskEncryptionSets/SampleEncryptionSet" />
4  </CustomProperties>'
5  <!--NeedCopy-->
```

- マシンプロファイルベースのワークフローを使用する場合は、Set-ProvSchemeコマンドで入力したマシンプロファイルを使用します。例:

```
1  Set-ProvScheme -ProvisioningSchemeName mxiao-test -MachineProfile
        XDHyp:\HostingUnits\azure-east\machineprofile.folder\aelx.
       resourcegroup\elx-mp.templatespec\1.0.0.templatespecversion
2  <!--NeedCopy-->
```

成功すると、カタログ内に追加されたすべてのマシンは、選択した DES に関連付けられたキーによって二重暗号化されます。

カタログが二重暗号化されていることの確認

- 完全な構成インターフェイスで以下の手順を実行します:
  1. ［マシンカタログ］に移動します。
  2. 確認するカタログを選択します。画面の下部近くにある ［テンプレートのプロパティ］タブをクリックします。
  3. ［**Azure** の詳細］の ［ディスク暗号化セット］でディスク暗号化セット ID を確認します。カタログの DES ID が空白の場合、カタログは暗号化されていません。
  4. Azure Portal で、DES ID に関連付けられた DES の暗号化の種類が、プラットフォーム管理キーと顧客が管理するキーであることを確認します。
- PowerShell コマンドを使用して以下の手順を実行します:
  1. **PowerShell** ウィンドウを開きます。
  2. asnp citrix*を実行し、Citrix 固有の PowerShell モジュールをロードします。
  3. Get-ProvSchemeを使用して、マシンカタログの情報を取得します。例:


```
Get-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
<!--NeedCopy-->
```

4. マシンカタログの DES ID カスタムプロパティを取得します。例:

```
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
     Value="/subscriptions
    /12345678-1234-1234-1234-123456789012/resourceGroups/Sample
    -RG/providers/Microsoft.Compute/diskEncryptionSets/
    SampleEncryptionSet" />
<!--NeedCopy-->
```

5. Azure Portal で、DES ID に関連付けられた DES の暗号化の種類が、プラットフォーム管理キーと顧客が管理するキーであることを確認します。

ページファイルの場所の決定

ページファイルの場所は、次のシナリオに従って決定されます:

> 注:
>
> デフォルトのページファイルの場所は OS ディスク上です。

シナリオ	場所
ページファイル設定はカスタムプロパティで指定される	カスタムプロパティで指定された場所
エフェメラル OS ディスクまたは休止状態が有効になっている	OS ディスク
VM に一時ディスクがある	一時ディスク
MCS IO が有効になっている	WBC ディスク

ページファイル設定シナリオ

次の表は、イメージの準備およびプロビジョニングスキーム更新中のページファイル設定について、いくつかの可能なシナリオを示しています:

タイミング	シナリオ	結果
イメージの準備時	ソースイメージページファイルを一時ディスクに設定しており、プロビジョニングスキームで指定した VM サイズに一時ディスクがない	ページファイルは OS に保存されます
イメージの準備時	ソースイメージページファイルを OS ディスクに設定しており、プロビジョニングスキームで指定した VM サイズに一時ディスクがない	ページファイルは一時ディスクに保存されます
イメージの準備時	ソースイメージページファイルを一時ディスクに設定しており、エフェメラル OS ディスクがプロビジョニングスキームで有効になっている	ページファイルは OS ディスクに保存されます
プロビジョニングスキームの更新時	VDA バージョンが 2311 より前の場合にプロビジョニングスキームを更新しようとした	警告でページファイル設定を変更します
プロビジョニングスキームの更新時	VDA バージョンが 2311 以降の場合にプロビジョニングスキームを更新しようとした	ページファイルの場所の決定に従ってページファイルの場所を決定します

ページファイル設定を指定する

PowerShell コマンドを使用して、場所やサイズなどのページファイル設定を指定できます。その場合、ページファイルの場所の決定に従って、MCS によって決定されたページファイル設定は上書きされます。これを行うには、マシンカタログの作成中に次の`New-ProvScheme`コマンドを実行します。

重要な注意事項

カタログの作成を進める前に、以下の点を考慮してください:

- `New-ProvScheme`コマンドですべてのカスタムプロパティ(「PageFileDiskDriveLetterOverride」、「InitialPageFileSizeInMB」、および「MaxPageFileSizeInMB」)を指定するか、いずれも指定しないでください。
- この機能は Citrix Studio ではサポートされていません。
- 初期ページファイルサイズは、16MB～16,777,216MB である必要があります。
- 最大ページファイルサイズは、初期ページファイルサイズ以上で、16,777,216MB 未満である必要があります。
- 初期ページファイルサイズと最大ページファイルサイズの両方を同時に 0 に設定できます。

> 注:
>
> マスターイメージを更新せずに、既存のカタログに新しく追加された VM のページファイル設定を変更できます。ページファイル設定を変更するには、VDA バージョン 2311 以降が必要です。PowerShell コマンドを使用してページファイルの設定を変更できます。詳しくは、「ページファイル設定を変更する」を参照してください。

```
New-ProvScheme -CleanOnBoot `
-HostingUnitName "zijinnet" `
-IdentityPoolName "PageFileSettingExample" `
-ProvisioningSchemeName "PageFileSettingExample" `
-InitialBatchSizeHint 1 `
-MasterImageVM "XDHyp:\HostingUnits\zijinnet\image.folder\neal-zijincloud-resources.resourcegroup\CustomWin10VDA_OsDisk_1_9473d7c8a6174b2c8284c7d3efeea88f.manageddisk" `
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\zijinnet\virtualprivatecloud.folder\East US. region\virtualprivatecloud.folder\neal-zijincloud-resources. resourcegroup\neal-zijincloud-resources-vnet.virtualprivatecloud\default.network" }
  `
-ServiceOffering "XDHyp:\HostingUnits\zijinnet\serviceoffering.folder\Standard_B2ms.serviceoffering" `
-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/XMLSchema-instance"> `
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false"/> `
<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `
<Property xsi:type="StringProperty" Name="PageFileDiskDriveLetterOverride" Value="d"/> `
<Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB" Value="2048"/> `
<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB" Value="8196"/> `
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="Premium_LRS"/> `
<Property xsi:type="StringProperty" Name="LicenseType" Value="Windows_Client"/> `
</CustomProperties>'
<!--NeedCopy-->
```

ページファイル設定を変更する

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

ページファイル設定を変更するには、VDA バージョン 2311 以降が必要です。PowerShell コマンドを使用してページファイルの設定を変更できます。

Azure 環境で変更できるさまざまなページファイル設定を次に示します:

- PageFileDiskDriveLetterOverride
- InitialPageFileSizeInMB
- MaxPageFileSizeInMB

既存のカタログのページファイル設定を変更する

既存のマシンカタログのページファイル設定を変更するには、Set-ProvSchemeコマンドを実行します。この場合、更新はカタログに追加された新しい VM にのみ適用されます。例:

```
Set-ProvScheme -ProvisioningSchemeName $schemeName -CustomProperties '<
    CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
     />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />
<Property xsi:type="StringProperty" Name="StorageType" Value="
    StandardSSD_LRS" />
<Property xsi:type="StringProperty" Name="
    PageFileDiskDriveLetterOverride" Value="D" />
<Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
    Value="2048" />
<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB" Value
    ="8196" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client" />
<Property  xsi:type="StringProperty" Name="Zones" Value="1" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="neal-
    test-group1" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
</CustomProperties>'
<!--NeedCopy-->
```

> 注:
>
> ライトバックキャッシュを有効にし、PowerShell コマンドを使用してPageFileDiskDriveLetterOverrideをC:に設定しようとすると、MCS IO ドライバーはページファイルをC:ではなく正しいディスクドライブに自動的にリダイレクトします。

AMA を有効にしたカタログ **VM** をプロビジョニングする

1. マシンプロファイルテンプレートを設定します。
    - VM をマシンプロファイルテンプレートとして使用する場合は、次の手順を実行します:
        a) Azure Portal で VM を作成します。

b) VM の電源を入れます。

c) ［リソース］で、VM をデータ収集規則に追加します。これにより、テンプレート VM へのエージェントのインストールが起動されます。

> 注:
>
> Linux カタログを作成する場合は、Linux マシンをセットアップします。

- テンプレートスペックをマシンプロファイルテンプレートとして使用する場合は、次の手順を実行します:

  a) テンプレートスペックを設定します。

  b) 生成されたテンプレートスペックに次の拡張機能とデータ収集規則の関連付けを追加します:

```
{

"type": "Microsoft.Compute/virtualMachines/extensions",
"apiVersion": "2022-03-01",
"name": "<vm-name>/AzureMonitorWindowsAgent",
"dependsOn": [
    "Microsoft.Compute/virtualMachines/<vm-name>"
],
"location": "<azure-region>",
"properties": {

    "publisher": "Microsoft.Azure.Monitor",
    "type": "AzureMonitorWindowsAgent",
    "typeHandlerVersion": "1.0",
    "autoUpgradeMinorVersion": true,
    "enableAutomaticUpgrade": true
 }

 }
 ,
 {

    "type": "Microsoft.Insights/
       dataCollectionRuleAssociations",
    "apiVersion": "2021-11-01",
    "name": "<associatio-name>",
    "scope": "Microsoft.Compute/virtualMachines/<vm-name>",
    "dependsOn": [
     "Microsoft.Compute/virtualMachines/<vm-name>",
    "Microsoft.Compute/virtualMachines/<vm-name>/extensions
       /AzureMonitorWindowsAgent"
    ],
    "properties": {

       "description": "Association of data collection rule.
           Deleting this association will break the data
          collection for this Arc server.",
     "dataCollectionRuleId": "/subscriptions/<azure-
        subscription>/resourcegroups/<azure-resource-group
```



```
            >/providers/microsoft.insights/datacollectionrules
            /<azure-data-collection-rule>"
35        }
36
37      }
38
39  <!--NeedCopy-->
```

> 注:
>
> Microsoft Sentinel データコネクタを使用してデータ収集規則を設定している場合は、通常の DCR の関連付けと同じ方法で、テンプレートスペックに`dataCollectionRuleAssociation`を追加するだけです。その後、カタログ VM が Sentinel DCR に表示され、AMA がそれらの VM にインストールされます。データ収集規則作成のベストプラクティスについては、「Azure Monitor でのデータ収集ルールの作成と管理のベストプラクティス」を参照してください。

2. MCS マシンカタログを作成または更新します。

   - 新しい MCS カタログを作成するには:

     a) 完全な構成インターフェイスで、前述の VM またはテンプレートスペックをマシンプロファイルとして選択します。
     b) 次の手順に進んでカタログを作成します。

   - 既存の MCS カタログを更新する場合は、次の PowerShell コマンドを使用します。この場合、新しい VM のみが更新されたマシンプロファイルテンプレートを取得します。

     ```
     1  Set-ProvScheme -ProvisioningSchemeName "name"
     2  -MachineProfile "XDHyp:\HostingUnits\Unit1\machineprofile.
           folder\abc.resourcegroup\ab-machine-profile.vm"
     3  <!--NeedCopy-->
     ```

   - 更新されたマシンプロファイルテンプレートを使用して既存の VM を更新するには、`Set-ProvScheme`を実行してから`Set-ProvVMUpdateTimeWindow`を実行します:

     ```
     1  Set-ProvScheme -ProvisioningSchemeName "name" -MachineProfile
           "XDHyp:\HostingUnits\Unit1\machineprofile.folder\abc.
          resourcegroup\ab-machine-profile.vm"
     2  Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
           -StartsNow -DurationInMinutes -1
     3  <!--NeedCopy-->
     ```

3. カタログ VM の電源を入れます。

4. Azure Portal に移動し、モニター拡張機能が VM にインストールされているかどうか、および VM が DCR の［リソース］の下に表示されているかどうかを確認します。数分後、監視データが Azure Monitor に表示されます。

トラブルシューティング

Azure Monitor エージェントのトラブルシューティングガイダンスについて詳しくは、以下を参照してください:

- https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-troubleshoot-windows-vm/
- https://learn.microsoft.com/en-us/azure/azure-resource-manager/troubleshooting/create-troubleshooting-template/

Azure Spot VM を使用したカタログの作成

Azure Spot VM を使用すると、Azure の未使用のコンピューティング容量を活用することで、大幅なコスト削減になります。ただし、Azure Spot VM を割り当てることができるかどうかは、現在の容量と料金によって異なります。したがって、Azure は削除ポリシーに従って、実行中の VM を削除したり、VM の作成に失敗したり、VM の電源投入に失敗したりする可能性があります。そのため、Azure Spot VM は、一部の重要ではないアプリケーションやデスクトップに適しています。詳しくは、「Azure Spot Virtual Machines を使用する」を参照してください。

制限事項

- Azure Spot VM では、すべての VM サイズがサポートされているわけではありません。詳しくは、「制限」を参照してください。

  次の PowerShell コマンドを実行して、VM サイズが Spot VM をサポートしているかどうかを確認できます。VM サイズが Spot VM をサポートしている場合、`SupportsSpotVM`は **True** です。

  ```
  (Get-Item "XDHyp:\HostingUnits\azure-res-conn2\serviceoffering.
     folder\Standard_D2ds_v4.serviceoffering"). AdditionalData
  <!--NeedCopy-->
  ```

- 現在、Azure Spot VM は休止状態をサポートしていません。

条件

Azure Spot VM カタログのマシンプロファイルのソース（VM またはテンプレートスペック）を作成するときに、Azure Spot インスタンスを選択するか（VM を使用する場合）、`priority`を`Spot`に設定するか（テンプレートスペックを使用する場合）を選択する必要があります。

Azure Spot VM を使用してカタログを作成する手順

1. マシンプロファイルのソース（VM または起動テンプレート）を作成します。

- Azure Portal を使用して VM を作成する場合は、「Azure portal を使用して Azure Spot Virtual Machines をデプロイする」を参照してください。
- テンプレートスペックを作成する場合は、テンプレートスペックの **resources > type: Microsoft.Compute/virtualMachines > properties** の下に次のプロパティを追加します。例:

```
"priority": "Spot",
"evictionPolicy": "Deallocate",
"billingProfile": {

"maxPrice": 0.01
 }

<!--NeedCopy-->
```

> 注:
>
> - 削除ポリシーは、**Deallocate** または **Delete** にできます。
>   - 非永続的な VM の場合、MCS は常に削除ポリシーを **Delete** として設定します。VM が削除されると、非永続ディスク (OS ディスクなど) とともに削除されます。永続ディスク (ID ディスクなど) は削除されません。ただし、カタログの種類が永続的であるか、`PersistOsDisk`カスタムプロパティが True に設定されている場合、OS ディスクは永続的です。同様に、`PersistWbc`カスタムプロパティが **True** に設定されている場合、WBC ディスクは永続的です。
>   - 永続的な VM の場合、MCS は常に削除ポリシーを Deallocate として設定します。VM が削除されると、割り当てが解除されます。ディスクには変更は加えられません。
> - 最大価格は、1 時間あたり支払い可能な金額です。**Capacity Only** を使用している場合、これは **-1** です。最大価格は、null、-1、または 0 より大きい小数値のみにすることができます。詳しくは、「価格」を参照してください。

2. 次の PowerShell コマンドを実行すると、マシンプロファイルで Azure Spot VM が有効になっているかどうかを確認できます。`SpotEnabled`パラメーターが **True** で、`SpotEvictionPolicy`が **Deallocate** または **Delete** に設定されている場合、マシンプロファイルは Azure Spot VM が有効になっています。例:

   - マシンプロファイルのソースが VM の場合、次のコマンドを実行します:

```
(Get-Item "XDHyp:\HostingUnits\azure-res-conn2\machineprofile
    .folder\fifthcolumn.resourcegroup\kb-spot-delete.vm").
    AdditionalData
<!--NeedCopy-->
```

   - マシンプロファイルのソースがテンプレートスペックの場合、次のコマンドを実行します:

```
(Get-Item "XDHyp:\HostingUnits\azure-res-conn2\machineprofile
    .folder\fifthcolumn.resourcegroup\fc-aeh-templatespec.
    templatespec\14.0.0-spot-delete.templatespecversion").
    AdditionalData
```



```
<!--NeedCopy-->
```

3. New-ProvScheme PowerShell コマンドを使用し、マシンプロファイルを使用してマシンカタログを作成します。

Set-ProvSchemeコマンドを使用してカタログを更新できます。PowerShell コマンドSet-ProvVmUpdateTimeWindowを使用して既存の VM を更新することもできます。マシンプロファイルは、次回の電源投入時に更新されます。

実行中の **Azure Spot VM** での削除

コンピューティング容量が利用できない場合、または 1 時間あたりの料金が構成された最大価格より高い場合、Azure は実行中の Spot VM を削除します。デフォルトでは、削除は通知されません。VM は単にフリーズしてから削除されます。Microsoft は、スケジュールされたイベントを使用して削除を監視することを推奨しています。「削除の発生を継続的に監視する」を参照してください。VM 内からスクリプトを実行して、削除前に通知を受け取ることもできます。たとえば、Microsoft には Python ScheduledEvents.csのポーリング スクリプトがあります。

トラブルシューティング

- Get-ProvVMコマンドを使用すると、プロビジョニングされた VM の customMachineData 内の Spot VM プロパティを確認できます。priority フィールドが **Spot** に設定されている場合、Spot は使用中です。
- VM が Azure Portal で Spot を使用しているかどうかを確認できます:

  1. Azure Portal で VM を見つけます。
  2. **Overview** ページに移動します。
  3. 一番下までスクロールして、**Azure Spot** セクションを見つけます。
     - Spot が使用中ではない場合、このフィールドは空です。
     - Spot が使用中の場合、**Azure Spot** と **Azure Spot eviction policy** フィールドが設定されます。

1. [Configuration] ページで、VM の請求プロファイルまたは時間あたりの最大価格を確認できます。

すべてのリソースのタグをコピーする

マシンプロファイルで指定されたタグを、マシンカタログ内の新しい VM または既存の VM の複数の NIC やディスク（OS ディスク、ID ディスク、ライトバックキャッシュディスク）などのすべてのリソースにコピーできます。マシンプロファイルのソースは、VM または ARM テンプレートスペックにすることができます。

> 注:
>
> タグにポリシーを追加するか（「タグの準拠のためのポリシー定義を割り当てる」を参照）、マシンプロファイルのソースにタグを追加してリソース上のタグを保持する必要があります。

前提条件

マシンプロファイルのソース（VM または ARM テンプレートスペック）を作成して、VM、ディスク、およびその VM の NIC にタグを付けます。

- VM をマシンプロファイルの入力で使用する場合は、Azure Portal 内の VM とすべてのリソースにタグを適用します。「Azure Portal を使用してタグを適用する」を参照してください。
- ARM テンプレートスペックをマシンプロファイルの入力として使用する場合は、各リソースの下に次のタグブロックを追加します。

```
1   "tags": {
2
3  "TagC": "Value3"
4   }
5  ,
6  <!--NeedCopy-->
```

> 注:
>
> テンプレートスペックには、最大 1 つのディスクと少なくとも 1 つの NIC を含めることができます。

新しいマシンカタログ内の **VM** のリソースにタグをコピーする

1. VM または ARM テンプレートスペックをマシンプロファイル入力として使用して、非永続カタログまたは永続カタログを作成します。
2. VM をカタログに追加し、電源をオンにします。マシンプロファイルで指定されたタグがその VM の対応するリソースにコピーされている必要があります。

   > 注:
   >
   > マシンプロファイルで指定された NIC の数と VM で使用する NIC の数が一致しない場合、エラーが発生します。

既存の **VM** のリソースのタグを変更する

1. すべてのリソースのタグを使用してマシンプロファイルを作成します。
2. 更新されたマシンプロファイルで既存のマシンカタログを更新します。例:


```
Set-ProvScheme -ProvisioningSchemeName <YourCatalogName> -
    MachineProfile <PathToYourMachineProfile>
<!--NeedCopy-->
```

3. 更新を適用する VM をオフにします。
4. VM のスケジュールされた更新を要求します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName <
    YourCatalogName>  -VMName machine1 -StartsNow -
    DurationInMinutes -1
<!--NeedCopy-->
```

5. 仮想マシンの電源を入れます。
6. マシンプロファイルで指定されたタグが対応するリソースにコピーされている必要があります。

> 注:
>
> マシンプロファイルで指定された NIC の数と`Set-ProvScheme`で指定された NIC の数が一致しない場合、エラーが発生します。

次の手順

- 最初のカタログを作成すると、デリバリーグループを作成する手順が表示されます。
- 構成プロセスの全体像については、「展開の計画と構築」を参照してください。
- カタログを管理するには、「マシンカタログの管理」と「Microsoft Azure カタログの管理」を参照してください。

追加情報

- 接続とリソースの作成と管理
- Microsoft Azure Resource Manager への接続
- マシンカタログの作成

Microsoft System Center Virtual Machine Manager カタログの作成

February 19, 2024

「マシンカタログの作成」では、マシンカタログを作成するウィザードについて説明します。次の情報は、Microsoft System Center Virtual Machine Manager（VMM）仮想化環境に固有の詳細について説明しています。

> 注:
>
> VMM カタログを作成する前に、VMM への接続の作成を完了する必要があります。「Microsoft System Center Virtual Machine Manager への接続」を参照してください。

マスター仮想マシンの作成

- マスター仮想マシンに VDA をインストールします。このとき、デスクトップを最適化するオプションを選択してください。これにより、パフォーマンスが向上します。
- バックアップのため、マスター仮想マシンのスナップショットを作成します。
- 仮想デスクトップを作成します。

SMB 3 ファイル共有の MCS

SMB 3 ファイル共有の仮想マシンストレージ上で MCS を使用して作成されたマシンカタログの場合、XenServer HCL（ハイパーバイザー通信ライブラリ）からの呼び出しを SMB ストレージに適切に接続できるよう、資格情報は以下の要件を満たしている必要があります。

- VMM のユーザー資格情報には、SMB ストレージに対する完全な読み取りおよび書き込みアクセス権限が必要です。
- 仮想マシンのライフサイクルイベント中のストレージ仮想ディスク操作では、Hyper-V サーバーを介して VMM のユーザー資格情報が使用されます。

SMB 3 について詳しくは、「Overview of file sharing using the SMB 3 protocol in Windows Server」を参照してください。

Windows Server 2012 の Hyper-V で VMM 2012 SP1 を使用する場合：SMB をストレージとして使用する際には、Cloud Connector から各 Hyper-V マシンへの認証用 CredSSP（Credential Security Support Provider）を有効にしてください。詳しくは、CTX137465を参照してください。

標準の PowerShell V3 リモートセッションを使用する場合、Cloud Connector の HCL は CredSSP を使って Hyper-V マシンへの接続を開きます。この機能では、Kerberos で暗号化されたユーザーの資格情報が Hyper-V マシンに渡され、この資格情報（この場合は VMM ユーザーの資格情報）を使用してリモートの Hyper-V マシン上のセッション内で PowerShell コマンドが実行されます。これにより、ストレージに対する通信コマンドが正しく動作します。

以下のタスクでは、HCL で作成される PowerShell スクリプトを使用します。その後スクリプトは、SMB 3.0 ストレージ上で動作する Hyper-V マシンに送信されます。

マスターイメージの統合：イメージにより、新しい MCS プロビジョニングスキーム（マシンカタログ）が作成されます。作成された新しいディスクから新しい仮想マシンを作成できるようにマスター仮想マシンを複製およびフラット化（および元のマスター仮想マシンの依存関係を削除）します。

root\virtualization\v2 名前空間で ConvertVirtualHardDisk を実行します。

例:

```
$ims = Get-WmiObject -class $class -namespace "root\virtualization\v2";
$result = $ims.ConvertVirtualHardDisk($diskName, $vhdastext)
$result
<!--NeedCopy-->
```

差分ディスクの作成：イメージを統合して作成されたイメージから、差分ディスクを作成します。この差分ディスクは、新しい仮想マシンに接続されます。

root\virtualization\v2 名前空間で CreateVirtualHardDisk を実行します。

例:

```
$ims = Get-WmiObject -class $class -namespace "root\virtualization\v2";
$result = $ims.CreateVirtualHardDisk($vhdastext);
$result
<!--NeedCopy-->
```

ID ディスクのアップロード：HCL では、ID ディスクを SMB ストレージに直接アップロードすることはできません。そのため、Hyper-V マシンが ID ディスクをストレージにアップロードしてコピーする必要があります。Hyper-V マシンは Cloud Connector のディスクを読み取れないため、HCL で Hyper-V マシンを介して ID ディスクをコピーしておく必要があります。

1. HCL は管理者共有を介して ID ディスクを Hyper-V マシンにアップロードします。
2. PowerShell リモートセッションで実行される PowerShell スクリプトにより、Hyper-V マシンが ID ディスクを SMB ストレージにコピーします。

   Hyper-V マシン上にフォルダーが作成され、（リモート PowerShell 接続を介して）そのフォルダーに対する権限が VMM ユーザーのみにロックされます。
3. HCL が管理者共有からファイルを削除します。
4. HCL が Hyper-V マシンへの ID ディスクのアップロードを完了すると、リモート PowerShell セッションによって ID ディスクは SMB ストレージにコピーされ、Hyper-V マシンから削除されます。

ID ディスクフォルダーが削除された場合は再作成され、再使用できるようになります。

ID ディスクのダウンロード：アップロードの場合と同様に、ID ディスクが Hyper-V マシンから HCL に渡されます。次の処理により、Hyper-V サーバー上に VMM ユーザー権限のみを持つフォルダーが作成されます（存在しない場合）。

1. PowerShell V3 リモートセッションで実行される PowerShell スクリプトにより、Hyper-V マシンが SMB ストレージからローカルの Hyper-V ストレージに ID ディスクをコピーします。
2. HCL が Hyper-V マシンの管理者共有から ID ディスクをメモリ内に読み取ります。
3. HCL が管理者共有からファイルを削除します。

マシンプロファイルを使用してカタログを作成する

マシンプロファイルを使用して、System Center Virtual Machine Manager（SCVMM）環境で MCS マシンカタログを作成および更新できます。入れ子構造の仮想化と vTPM を有効にすることもできます。

重要な注意事項

- マスターイメージはスナップショットのみにすることができます。VM にすることはできません。
- VM はマシンプロファイルのソースとしてのみ使用できます。
- VTPM は、SCVMM コンソールからではなく、Hyper-V コンソールから構成できます。
- マスターイメージで vTPM が有効になっている場合は、マシンプロファイルのソースで vTPM を有効にする必要があります。
- vTPM は、第 2 世代マシンでのみサポートされます。
- 次のパラメーターは、個別に指定されている場合、マシンプロファイルでキャプチャされた値を上書きします:
  - VMCpuCount
  - VMMemoryMB
  - Disk storage
- `Set-ProvScheme`コマンドを使用して既存のカタログを更新できます。

マシンプロファイルを使用してカタログを作成する手順

1. マシンプロファイルのソースになる VM を作成します。詳しくは、「VMM ファブリックで仮想マシンをプロビジョニングする」を参照してください。一度選択した世代は変更できません。
   - 入れ子構造の仮想化を有効にする場合は、［**Select Source**］ページで ［**Enable Nested Virtualization**］チェックボックスを選択します。
   - vTPM を有効にする場合は、VM を作成した後 Hyper-V ホストにログインし、**Hyper-V** マネージャーで VM を見つけます。VM を右クリックし、［**Settings**］に移動します。［**Security**］で ［**Enable Trusted Platform Module**］チェックボックスをオンにします。
2. **PowerShell** ウィンドウを開きます。
3. `asnp citrix*`を実行し、Citrix 固有の PowerShell モジュールをロードします。
4. ブローカーカタログを作成します。このカタログには、これから作成されるマシンが含まれています。
5. ID プールを作成します。これは、作成予定のマシン用に作成される AD アカウントのコンテナになります。
6. マシンプロファイルを使用してプロビジョニングスキームを作成します。例:


```
New-ProvScheme -HostingUnitName "<hostingunit name>"
-IdentityPoolName "ID1" -MasterImageVM "XDHyp:\HostingUnits\HU1<
    path to the checkpoint/snapshot>"
-ProvisioningSchemeName "<catalogname>"  -MachineProfile "XDHyp:<
    path to the machine profile VM>"
<!--NeedCopy-->
```

7. プロビジョニングスキームの一意の ID でブローカーカタログを更新します。
8. VM を作成してカタログに追加します。

Set-ProvScheme コマンドを使用して、既存のカタログを更新できます。例:

```
Set-ProvScheme -ProvisioningSchemeName "<catalogname>" -MachineProfile
    "XDHyp:<path to the machine profile VM>"
<!--NeedCopy-->
```

次の手順

- 最初のカタログを作成すると、デリバリーグループを作成する手順が表示されます。
- 構成プロセスの全体像については、「展開の計画と構築」を参照してください。
- カタログを管理するには、「マシンカタログの管理」と「Microsoft System Center Virtual Machine Manager カタログの管理」を参照してください。

追加情報

- 接続とリソースの作成と管理
- Microsoft System Center Virtual Machine Manager への接続
- マシンカタログの作成

Nutanix カタログの作成

February 9, 2024

「マシンカタログの作成」では、マシンカタログを作成するウィザードについて説明します。以下の情報は、Nutanix 仮想化環境に固有の詳細について説明しています。

> 注:
>
> Nutanix カタログを作成する前に、Nutanix への接続の作成を完了する必要があります。「Nutanix への接続」を参照してください。

Nutanix スナップショットを使用するマシンカタログの作成

選択したスナップショットは、カタログの仮想マシンの作成に使用されるテンプレートです。カタログを作成する前に、Nutanix でイメージとスナップショットを作成してください。詳しくは、Nutanix ドキュメントを参照してください。

カタログ作成ウィザードで次の操作を行います:

- ［オペレーティングシステム］ページと ［マシン管理］ページには、Nutanix 固有の情報は含まれていません。
- ［コンテナ］または ［クラスターとコンテナ］ページは、Nutanix に固有のものです。
  - Nutanix AHV XI をリソースとして使用してマシンを展開する場合は、［コンテナ］ページで、VM の ID ディスクを配置するコンテナを選択します。
  - Nutanix AHV Prism Central（PC）をリソースとして使用してマシンを展開すると、［クラスターとコンテナ］ページが表示されます。VM の展開に使用するクラスターを選択してから、コンテナを選択します。
- ［イメージ］ページで、イメージのスナップショットを選択します。必要に応じて、Acropolis コンソールを使用してスナップショットの名前を変更します。スナップショットの名前を変更した場合は、カタログ作成ウィザードを再起動して、最新の一覧を表示します。
- ［仮想マシン］ページで、仮想 CPU の数と仮想 CPU あたりのコア数を指定します。
- ［**NIC**］ページで、NIC（ネットワークインターフェイスカード）の種類を選択して、関連するネットワークをフィルタリングします。このオプションは、Nutanix AHV PC 接続でのみ使用できます。NIC には、［**VLAN**］と ［**OVERLAY**］の 2 種類があります。マスターイメージに含まれる 1 つまたは複数の NIC を選択してから、NIC ごとに関連付けられた仮想ネットワークを選択します。
- ［マシン **ID**］ページ、［ドメイン資格情報］ページ、［スコープ］ページ、および ［概要］ページには、Nutanix に固有の情報は含まれていません。

制限事項

Nutanix ホスト接続（具体的には、Nutanix AHV プラグイン 2.7.1 および Nutanix AHV プラグイン 2.5.1）を使用して MCS カタログを作成すると、プロビジョニングされた VM のハードディスクサイズが 完全な構成インターフェイスに誤って表示されます。

- Nutanix AHV プラグイン 2.7.1：表示されるサイズは、実際のストレージサイズよりもはるかに小さい（1GB）。
- Nutanix AHV プラグイン 2.5.1：表示されるサイズは、実際のストレージサイズよりもはるかに小さい（32GB）。

ただし、それはそれとして、マスターイメージ VM が VM 内のスナップショットの場合は、プロビジョニングされた VM は設計どおりに機能します。

次の手順

- 最初のカタログを作成すると、デリバリーグループを作成する手順が表示されます。
- 構成プロセスの全体像については、「展開の計画と構築」を参照してください。
- カタログを管理するには、「マシンカタログの管理」を参照してください。

追加情報

- 接続とリソースの作成と管理
- Nutanix への接続
- Nutanix クラウドおよびパートナーソリューションへの接続
- マシンカタログの作成

VMware カタログの作成

May 17, 2024

「マシンカタログの作成」では、マシンカタログを作成するウィザードについて説明します。

> 注:
>
> VMware カタログを作成する前に、VMware への接続の作成を完了する必要があります。「VMware への接続」を参照してください。

マシンプロファイルを使用してマシンカタログを作成する

マシンプロファイルを使用して MCS マシンカタログを作成できます。マシンプロファイルの入力のソースは VMware テンプレートです。マシンプロファイルは、VMware テンプレートからハードウェアプロパティを取得し、カタログ内の新しくプロビジョニングされた VM に適用します。

> 注:
>
> - マスターイメージの入力（スナップショット）とマシンプロファイルの入力（VMware テンプレート）は、vTPM が両方とも有効になっているか無効になっている必要があります。この規則は`New-ProvScheme`と`Set-ProvScheme`の両方に適用されます。
> - マスターイメージで vTPM が有効になっている場合、VMware テンプレートはマスターイメージと同じ VM ソースからのみ取得できます。
> - 暗号化ストレージポリシーは完全クローンのみをサポートします。

カタログへの VM のプロビジョニングを可能にするには、マシンプロファイル内の VMware テンプレートがカタログのライフサイクル中に存在する必要があります。VMware テンプレートがないと、新しい VM をプロビジョニング

できません。VMware テンプレートが削除された場合は、`Set-ProvScheme`コマンドを使用して新しいテンプレートを提供する必要があります。

- MCS は、VMware テンプレートのプロパティをキャプチャします。`Get-Provscheme`コマンドを使用して、VMware テンプレートの保存されたプロパティを参照することで、新しい VMware テンプレートを作成できます。
- また、マシンカタログとプロビジョニングされた VM が存在する場合は、MCS でプロビジョニングされたマシンを使用して新しい VMware テンプレートを作成することもできます。

さまざまな OS に基づいて、さまざまな構成のマシンカタログを作成できます:

- Windows 11 がマスターイメージにインストールされている場合は、マスターイメージで vTPM を有効にする必要があります。したがって、マシンプロファイルのソースである VMware テンプレートには、vTPM が組み込まれている必要があります。
- Windows 10 が、vTPM が組み込まれていないマスターイメージにインストールされている場合は、マシンプロファイルのソースとして vTPM が含まれない VMware テンプレートを使用してマシンカタログを作成できます。

暗号化されたストレージポリシーが適用されたマシンプロファイルテンプレートを使用して、完全なコピーディスクモードでマシンカタログを作成できる別の構成もあります。

PowerShell コマンドを使用し、マシンプロファイルを入力に使用して新しいマシンカタログを作成するには、次の手順を実行します:

1. **PowerShell** ウィンドウを開きます。
2. `asnp citrix*`を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. 次のコマンドを実行します:

    - vTPM が組み込まれた VMware テンプレートをマシンプロファイルの入力のソースとして使用し、Windows 11 がインストールされたマスターイメージを使用してマシンカタログを作成するには、以下を実行します:

```
$identityPool = New-AcctIdentityPool
-IdentityPoolName "<string>"
-NamingScheme "<string>-###"
-NamingSchemeType Numeric
-Domain "<domain name"
-ZoneUid "<Uid>"  -Scope @()
<!--NeedCopy-->
```

```
$provScheme =New-ProvScheme  -CleanOnBoot
-HostingUnitName "vSanRg"
-IdentityPoolName "<string>"
-InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits<hosting unit name><
   snapshot name>.snapshot"
```



```
-NetworkMapping @{
"0"="XDHyp:\HostingUnits<hosting unit name>\<network name>.
   network" }

-ProvisioningSchemeName "<string>"
-Scope @() -VMCpuCount 4  -VMMemoryMB 6144
-MachineProfile "XDHyp:\HostingUnits<hosting unit name><
   template name>.template"
-TenancyType Shared
-FunctionalLevel "L7_20"
<!--NeedCopy-->
```

```
$catalog = New-BrokerCatalog
-AllocationType "Static"
-PersistUserChanges  "OnLocal"
-Description "<string>"  -IsRemotePC $False
-MinimumFunctionalLevel 'L7_9' -Name "<catalog name>" -
   ProvisioningType 'MCS'
-Scope @()  -SessionSupport "SingleSession"
-ZoneUid "<Uid>"
<!--NeedCopy-->
```

```
Set-BrokerCatalog -Name "<string>"
-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
<!--NeedCopy-->
```

- vTPM が組み込まれていない VMware テンプレートをマシンプロファイル入力のソースとして使用し、Windows 10 がインストールされたマスターイメージを使用してマシンカタログを作成するには、以下を実行します:

```
$identityPool = New-AcctIdentityPool
-IdentityPoolName "<string>"
-NamingScheme "<string>-###"
-NamingSchemeType Numeric
-Domain "<domain name>"
-ZoneUid "<Uid>"  -Scope @()
<!--NeedCopy-->
```

```
$provScheme =New-ProvScheme  -CleanOnBoot
-HostingUnitName "<string>"
-IdentityPoolName "<string>"
-InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits<hosting unit name><
   snapshot name>.snapshot"
-NetworkMapping @{
"0"="XDHyp:\HostingUnits<hosting unit name>\<string>.network"
    }

-ProvisioningSchemeName "<string>"  -Scope @() -VMCpuCount 4
    -VMMemoryMB 8192
-MachineProfile "XDHyp:\HostingUnits<hosting unit name><
   template name>.template"
```



```
-TenancyType Shared  -FunctionalLevel "L7_20"
<!--NeedCopy-->
```

```
$catalog = New-BrokerCatalog
-AllocationType "Static"
-PersistUserChanges  "OnLocal"  -Description "<string>"  -
   IsRemotePC $False
-MinimumFunctionalLevel 'L7_9' -Name "<string>" -
   ProvisioningType 'MCS' -Scope @()  -SessionSupport "
   SingleSession" -ZoneUid "<Uid"
<!--NeedCopy-->
```

```
Set-BrokerCatalog -Name "<string>"
-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
<!--NeedCopy-->
```

- 暗号化されたストレージポリシーが適用されたマシンプロファイルテンプレートを使用して、完全なコピーディスクモードでマシンカタログを作成するには、以下を実行します:

```
$identityPool = New-AcctIdentityPool
-IdentityPoolName "<string>"
-NamingScheme "<string>-###"
-NamingSchemeType Numeric
-Domain "<domain name>"
-ZoneUid "<Uid>"  -Scope @()
<!--NeedCopy-->
```

```
$provScheme =New-ProvScheme
-HostingUnitName "<string>"
-IdentityPoolName "<string>" -InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits<hosting unit name><
   snapshot name>.snapshot"
-NetworkMapping @{
"0"="XDHyp:\HostingUnits<hosting unit name>\<string>.network"
    }

-ProvisioningSchemeName "<string>"  -Scope @() -VMCpuCount 4
    -VMMemoryMB 8192
-MachineProfile "XDHyp:\HostingUnits<hosting unit name><
   template name>.template"
-TenancyType Shared  -FunctionalLevel "L7_20"
-UseFullDiskCloneProvisioning
<!--NeedCopy-->
```

```
$catalog = New-BrokerCatalog
-AllocationType "Static"
-PersistUserChanges  "OnLocal"
-Description "<string>"
-IsRemotePC $False
-MinimumFunctionalLevel 'L7_9' -Name "<string>" -
   ProvisioningType 'MCS' -Scope @()
-SessionSupport "SingleSession" -ZoneUid "<Uid>"
```



```
<!--NeedCopy-->
```

```
Set-BrokerCatalog -Name "<string>"
-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
<!--NeedCopy-->
```

- マシンプロファイルを更新するには、Set-ProvSchemeコマンドを使用します。例:

```
Set-ProvScheme -ProvisioningSchemeName 'name' -
    IdentityPoolName 'name' -MachineProfile 'XDHyp:\
    HostingUnits<hosting unit name><template name>.template
<!--NeedCopy-->
```

複数の **NIC** を確認する

マシンプロファイルとNew-ProvSchemeおよびSet-ProvSchemeコマンドのNetworkMappingパラメーターを使用すると、複数の NIC の事前チェック中にさまざまなエラーメッセージが表示されます。

複数の NIC の事前チェックリストは次のとおりです:

- マシンプロファイルテンプレートからの NIC 数のみが使用され、検証されます。これらの NIC が参照するネットワークは、ホスティングユニットのネットワークに対して使用または検証されません。
- マシンプロファイルテンプレートの NIC 数がホスティングユニット内のネットワーク数より大きい場合は、エラーメッセージが表示されます。
- マシンプロファイルテンプレートの NIC 数がゼロの場合、エラーメッセージが表示されます。
  マシンプロファイルテンプレートの NIC 数が 1 の場合:
  - If no network mapping is specified in the New-ProvScheme or Set-ProvScheme command, and the hosting unit network is one, then the hosting unit network is used.
  - If network mapping is specified, then the specified network mapping is used if it is valid.
- マシンプロファイルテンプレートの NIC 数が 1 より大きい場合、またはホスティングユニットのネットワーク数が 1 より大きい場合:
  - コマンドには有効なネットワークマッピングが必要であり、各 NIC のマッピングを提供する必要があります（つまり、NetworkMapping の数はマシンプロファイルの NIC の数と同じである必要があります)。
  - ホスティングユニット内の同じネットワークに複数の NIC をマッピングすることはできません。
  - NetworkMapping数とマシンプロファイルの NIC 数は、ホスティングユニットのネットワーク数以下である必要があります。
  - NetworkMappingは、各 ID に対して 0 から n-1 までで指定される必要があります。ここで、n はマシンプロファイルテンプレート内のネットワークアダプターの数です。

トラブルシューティング

カタログの作成に失敗した場合は、CTX294978を参照してください。

次の手順

- 最初のカタログを作成すると、デリバリーグループを作成する手順が表示されます。
- 構成プロセスの全体像については、「展開の計画と構築」を参照してください。
- カタログを管理するには、「マシンカタログの管理」と「VMware カタログの管理」を参照してください。

追加情報

- 接続とリソースの作成と管理
- VMware への接続
- VMware クラウドおよびパートナーソリューションへの接続
- マシンカタログの作成

XenServer カタログの作成

March 5, 2024

「マシンカタログの作成」では、マシンカタログを作成するウィザードについて説明します。以下の情報は、XenServer（旧称 Citrix Hypervisor）仮想化環境に固有の詳細について説明しています。

> 注:
>
> XenServer カタログを作成する前に、XenServer への接続の作成を完了する必要があります。「XenServer への接続」を参照してください。

GPU 対応 XenServer を使用してマシンカタログを作成する

GPU 対応のマシンでは、専用のマスターイメージが必要です。これらの仮想マシンには、GPU をサポートするビデオカードドライバーが必要です。仮想マシンが GPU を使用して稼働するソフトウェアによって動作できるように、GPU 対応のマシンを構成します。

1. XenCenter を使用して、標準的な VGA、ネットワーク、および vCPU を指定して仮想マシンを作成します。
2. 作成した仮想マシンの構成を変更して、GPU 機能（パススルーまたは仮想 GPU）を有効にします。
3. 仮想マシンに適切なオペレーティングシステムをインストールして、RDP を有効にします。
4. Citrix VM Tools と NVIDIA ドライバーをインストールします。

5. パフォーマンスを最適化するため、Virtual Network Computing（VNC）Admin Console をオフにして、仮想マシンを再起動します。
6. RDP の使用を確認するメッセージが表示されます。RDP を使用して VDA をインストールし、仮想マシンを再起動します。
7. 必要に応じて、仮想マシンのスナップショットを作成します。このスナップショットは、ほかの GPU マスターイメージのテンプレートとして使用できます。
8. RDP を使用して、XenCenter で構成され、GPU を使用する顧客固有のアプリケーションをインストールします。

PowerShell を使用してマシンプロファイルベースのマシンカタログを作成する

MCS を使用してマシンをプロビジョニングするためのカタログを作成する場合、マシンプロファイルを使用して、仮想マシンからハードウェアプロパティをキャプチャし、カタログで新しくプロビジョニングされた VM に適用できます。`MachineProfile`パラメーターが使用されていない場合、ハードウェアプロパティはマスターイメージ VM またはスナップショットからキャプチャされます。

> 注:
>
> 現在、マシンプロファイル入力として使用できるのはスナップショットのみです。

次のパラメーターを明示的に構成して、マシンプロファイル入力のパラメーターの値を上書きできます。

- `VMCpuCount`
- `VMMemory`
- `NetworkMapping`

マシンプロファイルを使用してカタログを作成する

1. PowerShell ウィンドウを開きます。
2. `asnp citrix*`を実行します。
3. ID プールを作成します。ID プールは、作成される VM の Active Directory（AD）アカウントのコンテナです。例:

```
New-AcctIdentityPool -Domain "citrix-xxxxxx.local" -
    IdentityPoolName "ExampleIdentityPool" -NamingScheme "abc1-##"
    -NamingSchemeType "Numeric" -Scope @() -ZoneUid "xxxxxxxx"
<!--NeedCopy-->
```

4. Active Directory に必要な AD コンピューターアカウントを作成します。

```
$password = "password123" | ConvertTo-SecureString -AsPlainText -
    Force
New-AcctADAccount -IdentityPoolName "ExampleIdentityPool" -Count
    10 -ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
```



```
Set-AcctAdAccountUserCert -IdentityPoolName "ExampleIdentityPool"
    -ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
<!--NeedCopy-->
```

5. New-ProvSchemeコマンドを実行してカタログを作成します。例:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "ExampleHostingUnit"
    -IdentityPoolName "ExampleIdentityPool" -InitialBatchSizeHint 2
     -CustomProperties '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="
    true" />
</CustomProperties>'
-MasterImageVM "XDHyp:\HostingUnits\ExampleHostingUnit\ExampleVDA.
    vm\ExampleVDA.snapshot" -ProvisioningSchemeName "ExampleCatalog
    " -Scope @() -SecurityGroup @()
-MachineProfile "XDHyp:\HostingUnits\ExampleHostingUnit\
    ExampleMachineProfile.vm\ExampleSnapshot.snapshot"
<!--NeedCopy-->
```

6. プロビジョニングスキームをブローカーカタログとして登録します。例:

```
$ConfigZone = Get-ConfigZone | Where-Object {
  $_.Name -eq "xxxxxx"  }

New-BrokerCatalog -Name "MPLT1" -AllocationType Random -
    Description "Machine profile catalog" -ProvisioningSchemeId
    fe7df345-244e-4xxxx-xxxxxxxxx -ProvisioningType Mcs -
    SessionSupport MultiSession -PersistUserChanges Discard -
    ZoneUid ($ConfigZone.Uid)
<!--NeedCopy-->
```

7. VM をマシンカタログに追加します。

新しいマシンプロファイルでマシンカタログを更新する

> 注:
>
> - この場合、Set-ProvSchemeコマンドは、カタログ内の既存 VM のマシンプロファイルを変更しません。新しいマシンプロファイルは、カタログに追加された新しく作成された VM のみにあります。
> - マシンプロファイルベースのマシンカタログを非マシンプロファイルベースのマシンカタログに変換することはできません。

新しいマシンプロファイルでマシンカタログを更新するには、次の手順を実行します:

1. Set-ProvSchemeコマンドを実行します。例:

```
Set-ProvScheme -ProvisioningSchemeName "ExampleCatalog" -
    MachineProfile "XDHyp:\HostingUnits\ExampleHostingUnit\
```



```
        ExampleMachineProfileVm.vm\ExampleMachineProfileSnapshot.
        snapshot"
2   <!--NeedCopy-->
```

Set-ProvScheme コマンドについて詳しくは、「Set-ProvScheme」を参照してください。

次の手順

- 最初のカタログを作成すると、デリバリーグループを作成する手順が表示されます。
- 構成プロセスの全体像については、「展開の計画と構築」を参照してください。
- カタログを管理するには、「マシンカタログの管理」と「Manage a XenServer catalog」を参照してください。

追加情報

- 接続とリソースの作成と管理
- XenServer への接続
- マシンカタログの作成

参加の種類が異なるカタログの作成

July 3, 2023

MCS を使用すると、ドメイン非参加、オンプレミス AD 参加済み、Azure AD 参加済み、またはハイブリッド Azure AD 参加済みのマシンをプロビジョニングできます。

[完全な構成] インターフェイスでマシン ID を構成する方法については、「マシンカタログの作成」を参照してください。

マシン ID 参加済みカタログの作成方法については、以下を参照してください:

- Azure Active Directory 参加済みカタログの作成
- Microsoft Intune 対応カタログの作成
- Hybrid Azure Active Directory 参加済みカタログの作成
- ドメイン非参加カタログの作成

Azure Active Directory 参加済みカタログの作成

February 9, 2024

この記事では、Citrix DaaS を使用して Azure Active Directory（AD）参加済みカタログを作成する方法について説明します。

要件、制限、および考慮事項については、「Azure Active Directory 参加済み」を参照してください。

マシンカタログを作成する前に、次のものが必要です:

1. 新しいリソースの場所
    - Citrix Cloud の管理 UI で左上のハンバーガーメニューから ［リソースの場所］ を選択します。
    - ［**+** リソースの場所］ をクリックします。
    - リソースの場所の新しい名前を入力し、［保存］ をクリックします。
2. ホスト接続を作成します。詳しくは、「接続の作成と管理」セクションを参照してください。Azure にマシンを展開する場合は、「Azure Resource Manager への接続」を参照してください。
3. 古い Azure AD デバイスを一貫して削除し、新しいデバイスが Azure AD に参加できるようにするために、Cloud Device Administrator の役割をプロビジョニングのサービスプリンシパルに割り当てることができます。Azure の古い AD デバイスを削除しない場合、対応する非永続的な仮想マシンは、Azure AD ポータルから手動で削除するまで初期化状態のままになります。これを行うには、完全な構成インターフェイスを使用してホスト接続の Azure AD 参加済みデバイスの管理を有効にするか、次の手順を実行します:
    a) Azure Portal にサインインし、［**Azure Active Directory**］ **>** ［**Roles and administrators**］ に移動します。
    b) 組み込みの **Cloud Device Administrator** の役割を検索し、［**Add assignments**］ をクリックして、ホスト接続で使用されるアプリケーションのサービスプリンシパルにこの役割を割り当てます。
    c) Citrix Remote PowerShell SDK を使用して次のコマンドを実行し、ホスト接続の既存の`CustomProperties`を取得します。`${ HostingConnectionName }`はホスト接続の名前です。
        i. **PowerShell** ウィンドウを開きます。
        ii. `asnp citrix*`を実行し、Citrix 固有の **PowerShell** モジュールをロードします。
        iii. 次のコマンドを実行して、ホスト接続の既存のカスタムプロパティを取得します。

```
(Get-Item -LiteralPath XDHyp:\Connections${
 HostingConnectionName }
 ).CustomProperties
<!--NeedCopy-->
```

        iv. CustomProperties を接続からメモ帳にコピーし、プロパティ設定`<Property xsi:type="StringProperty"Name="AzureAdDeviceManagement"Value="true"/>`を追加します。
        v. **PowerShell** ウィンドウで、変更したカスタムプロパティに変数を割り当てます。 例: `$UpdatedCustomProperties='<CustomProperties …</CustomProperties>'`。

vi. カスタムプロパティをホスト接続に設定し直します:

```
Set-Item -LiteralPath XDHyp:\Connections${
 HostingConnectionName }
  -CustomProperties ${
 UpdatedCustomProperties }
  -ZoneUid ${
 ZoneUid }

<!--NeedCopy-->
```

vii. コマンド(`Get-Item -LiteralPath XDHyp:\Connections\${ HostingConnection } ).CustomProperties`を実行して、更新されたカスタムプロパティ設定を確認します。

完全な構成インターフェイスまたは **PowerShell** を使用して、Azure AD 参加済みカタログを作成できます。

完全な構成インターフェイスの使用

以下の情報は、「マシンカタログの作成」のガイダンスを補完する情報です。Azure AD 参加済みカタログを作成するには、Azure AD 参加済みカタログに固有の詳細に注意しながら、その記事の一般的なガイダンスに従ってください。

カタログ作成ウィザードで次の操作を行います:

1. イメージ ページ:
   - 機能レベルとして 2106 以降を選択します。
   - [マシンプロファイルを使用する] を選択し、一覧から適切なマシンを選択します。
2. [マシン **ID**] ページで、[**Azure Active Directory** 参加済み] を選択します。作成済みのマシンは、組織によって所有され、その組織に属する Azure AD アカウントでサインインします。作成済みのマシンはクラウドにのみ存在します。

   > 注:
   >
   > - [**Azure Active Directory** 参加済み] の ID の種類を使用するには、カタログの最小機能レベルとして、バージョン 2106 以降が必要です。
   > - マシンは、ホスト接続がバインドされているテナントに関連付けられた Azure AD ドメインに参加済みです。

3. ユーザーは、AAD 資格情報を使用してマシンにログインするために、Azure での明示的なアクセスが許可されている必要があります。詳しくは、「Azure Active Directory 参加済み」セクションを参照してください。

PowerShell の使用

以下は、［完全な構成］インターフェイスでの操作と同じ **PowerShell** での手順です。Remote PowerShell SDK を使用してカタログを作成する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/を参照してください。

オンプレミス AD 参加済みカタログと Azure AD 参加済みカタログの違いは、ID プールとプロビジョニングスキームの作成にあります。

Azure AD 参加済みカタログの ID プールを作成するには、以下の手順に従います:

```
1 New-AcctIdentityPool -AllowUnicode -IdentityType="AzureAD" -
     WorkgroupMachine -IdentityPoolName "AzureADJoinedCatalog" -
     NamingScheme "AzureAD-VM-##" -NamingSchemeType "Numeric" -Scope @()
     -ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
2 <!--NeedCopy-->
```

Azure AD 参加済みカタログのプロビジョニングスキームを作成するには、New-ProvScheme に **MachineProfile** パラメーターが必要です:

```
1 New-ProvScheme -CustomProperties "<CustomProperties xmlns=`"http://
     schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.
     w3.org/2001/XMLSchema-instance`"><Property xsi:type=`"StringProperty
     `" Name=`"UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
     StringProperty`" Name=`"StorageType`" Value=`"StandardSSD_LRS`" /><
     Property xsi:type=`"StringProperty`" Name=`"LicenseType`" Value=`"
     Windows_Server`" /></CustomProperties>" -HostingUnitName "
     AzureResource" -IdentityPoolName "AzureADJoinedCatalog" -
     InitialBatchSizeHint 1 -MachineProfile "XDHyp:\HostingUnits\
     AzureResource\image.folder\azuread-rg.resourcegroup\MasterVDA.vm" -
     MasterImageVM "XDHyp:\HostingUnits\AzureResource\image.folder\
     azuread-rg.resourcegroup\azuread-
     small_OsDisk_1_5fb42fadf7ff460bb301ee0d56ea30da.manageddisk" -
     NetworkMapping @{
2  "0"="XDHyp:\HostingUnits\AzureResource\virtualprivatecloud.folder\East
       US.region\virtualprivatecloud.folder\azuread-rg.resourcegroup\
      azuread-vnet.virtualprivatecloud\Test_VNET.network" }
3   -ProvisioningSchemeName "AzureADJoinedCatalog" -RunAsynchronously -
       Scope @() -SecurityGroup @() -ServiceOffering "XDHyp:\HostingUnits
       \AzureResource\serviceoffering.folder\Standard_DS1_v2.
       serviceoffering"
4 <!--NeedCopy-->
```

Azure AD 参加済みカタログを作成するために使用される他のすべてのコマンドは、従来のオンプレミス AD 参加済みカタログの場合と同じです。

Azure AD 参加プロセスのステータスの表示

完全な構成インターフェイスでは、デリバリーグループ内の Azure AD 参加済みマシンが電源オンの状態にあるときに、Azure AD 参加プロセスのステータスが表示されます。ステータスを表示するには、［検索］を使用してそれら

のマシンを識別し、下ペインの ［詳細］タブで ［マシン **ID**］を 1 つずつチェックします。次の情報が ［マシン **ID**］に表示されることがあります:

- Azure AD に参加済み
- Azure AD 未参加

> 注:
>
> マシンが Azure AD 参加済み状態にならない場合、それらのマシンは Delivery Controller に登録されません。このような登録ステータスは ［初期化］状態として表示されます

また、完全な構成インターフェイスで、マシンが使用できない理由を知ることができます。これを行うには、［検索］ノードでマシンをクリックし、下ペインの ［詳細］タブで ［登録］をオンにしてから、ツールチップを読んで追加情報を確認します。

デリバリーグループ

詳しくは、「デリバリーグループの作成」セクションを参照してください。

Rendezvous を有効にする

デリバリーグループの作成後、Rendezvous を有効化できます。詳しくは、「Rendezvous V2」を参照してください。

トラブルシューティング

マシンが Azure AD 参加済みにならない場合は、次の手順を実行します:

- システムに割り当てられた管理対象 ID がマシンに対して有効になっているかどうかを確認します。MCS でプロビジョニングされたマシンでは、自動的にこれが有効になります（有効にする必要があります）。システムに割り当てられた管理対象 ID がないと、Azure AD への参加プロセスで失敗します。MCS でプロビジョニングされたマシンでシステムに割り当てられた管理対象 ID が有効になっていない場合、考えられる原因は次のとおりです:
  - プロビジョニングスキームに関連付けられている ID プールの`IdentityType`が、`AzureAD`に設定されていない。これを確認するには、`Get-AcctIdentityPool`を実行します。
- VDA バージョン 2206 以前のマスターイメージを使用するカタログの場合は、マシンの **AADLoginForWindows** 拡張機能のプロビジョニングステータスを確認してください。**AADLoginForWindows** 拡張機能が存在しない場合、考えられる原因は次のとおりです:
  - プロビジョニングスキームに関連付けられている ID プールの`IdentityType`が、`AzureAD`に設定されていない。これを確認するには、`Get-AcctIdentityPool`を実行します。

  - **AADLoginForWindows** 拡張機能のインストールは、Azure ポリシーによってブロックされます。

- **AADLoginForWindows** 拡張機能のプロビジョニングの失敗についてトラブルシューティングするには、MCS でプロビジョニングされたマシンの`C:\WindowsAzure\Logs\Plugins\Microsoft.Azure.ActiveDirectory.AADLoginForWindows`にあるログを確認します。

  > 注:
  >
  > VDA バージョン 2209 以降のマスターイメージを使用する場合、MCS は`AADLoginForWindows`拡張機能に依存せずに VM を Azure AD に参加させます。この場合、`AADLoginForWindows`拡張機能は、MCS でプロビジョニングされたマシンにインストールされません。したがって、`AADLoginForWindows`拡張機能プロビジョニングログを収集できません。

- MCS でプロビジョニングされたマシンで`dsregcmd /status`コマンドを実行して、Azure AD の参加ステータスを確認し、ログをデバッグします。
- [アプリケーションとサービスログ] > [**Microsoft**] > [**Windows**] > [ユーザーデバイス登録] にある Windows イベントログを確認します。
- `Get-Item -LiteralPath XDHyp:\Connections\${ HostingConnectionName }`を実行して、Azure AD デバイス管理が正しく構成されているかどうかを確認します。

  次の値を確認してください:

  - `CustomProperties`内の`AzureAdDeviceManagement`プロパティが **true**
  - メタデータの`Citrix_MCS_AzureAdDeviceManagement_PermissionGranted`プロパティが **true**

  `Citrix_MCS_AzureAdDeviceManagement_PermissionGranted`が **false** の場合、ホスト接続で使用されるアプリケーションの`ServicePrincipal`に、Azure AD デバイス管理を実行するための十分な権限が付与されていないことを示します。これを解決するには、`ServicePrincipal`に **Cloud Device Administrator** の役割を割り当てます。

Azure Active Directory 動的セキュリティグループ

動的グループの規則では、マシンカタログの名前付けスキームに基づいて、カタログ内の仮想マシンを動的セキュリティグループに配置します。

マシンカタログの名前付けスキームが Test###（# は番号を意味します）の場合、Citrix が動的セキュリティグループに動的メンバーシップの規則「^*Test[0-9]{3}$*」を作成します。これで、Citrix によって作成された仮想マシンの名前が Test001 から Test999 までのいずれかである場合、その仮想マシンは動的セキュリティグループに含まれます。

> 注:
>
> 手動で作成した仮想マシンの名前が Test001 から Test999 のいずれかである場合、その仮想マシンも動的セキュリティグループに含まれます。これは、動的セキュリティグループの制限の 1 つです。

動的セキュリティグループ機能は、Azure Active Directory（Azure AD）によって仮想マシンを管理する場合に役立ちます。これは、条件付きアクセスポリシーを適用したり、Azure AD 動的セキュリティグループで仮想マシンをフィルター処理して Intune からアプリを配布したりする場合にも役立ちます。

PowerShell コマンドを使用して、次のことができます:

- Azure AD 動的セキュリティグループを使用してマシンカタログを作成する
- Azure AD カタログのセキュリティグループ機能を有効にする
- Azure AD 参加済みデバイスのセキュリティグループを使用してマシンカタログを削除する

> 重要:
>
> - Azure AD 動的セキュリティグループを使用してマシンカタログを作成し、マシンをカタログに追加し、マシンカタログを削除するには、Azure AD アクセストークンが必要です。Azure AD アクセストークンの取得については、https://docs.microsoft.com/en-us/graph/graph-explorer/graph-explorer-features#consent-to-permissions/を参照してください。
> - Azure AD でアクセストークンを要求するために、Citrix は Microsoft Graph API の **Group.ReadWrite.All** 権限を要求します。テナント全体の管理者の同意権限を持つ Azure AD ユーザーは、Microsoft Graph API の **Group.ReadWrite.All** 権限を付与できます。Azure Active Directory（Azure AD）内のアプリケーションにテナント全体の管理者の同意を付与する方法については、Microsoft のドキュメント（https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent/）を参照してください。

Azure AD 動的セキュリティグループを使用してマシンカタログを作成する

1. Web ベースのコンソールの、マシンカタログのセットアップ用ユーザーインターフェイスで、［マシン **ID**］ページの ［**Azure Active Directory** 参加］を選択します。
2. Azure AD にログインします。
3. MS Graph API へのアクセストークンを取得します。**PowerShell** コマンドを実行するときに、このアクセストークンを$AzureADAccessTokenパラメーターの値として使用します。
4. 次のコマンドを実行して、動的セキュリティグループ名がテナントに存在するかどうかを確認します。

```
Get-AcctAzureADSecurityGroup
 -AccessToken  $AzureADAccessToken
 -Name "SecurityGroupName"
<!--NeedCopy-->
```


5. テナント ID、アクセストークン、および動的セキュリティグループを使用してマシンカタログを作成します。次のコマンドを実行し、IdentityType=AzureADを使用して IdentityPool を作成し、Azure に動的セキュリティグループを作成します。

```
New-AcctIdentityPool
-AllowUnicode
-IdentityPoolName "SecurityGroupCatalog"
-NamingScheme "SG-VM-###"
-NamingSchemeType "Numeric" -Scope @()
-ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
-WorkgroupMachine
-IdentityType "AzureAD"
-DeviceManagementType "None"
-AzureADTenantId  620387bb-9167-4bdd-8435-e3dccc58369e
-AzureADSecurityGroupName "SecurityGroupName"
-AzureADAccessToken $AzureADAccessToken
<!--NeedCopy-->
```

Azure AD カタログのセキュリティグループ機能を有効にする

動的セキュリティグループ機能を有効にせずに作成された Azure AD カタログの動的セキュリティ機能を有効にすることができます。これを行うには、以下の手順に従います:

1. 新しい動的セキュリティグループを手動で作成します。既存の動的セキュリティグループを再利用することもできます。
2. Azure AD にログインし、MS Graph API へのアクセストークンを取得します。**PowerShell** コマンドを実行するときに、このアクセストークンを$AzureADAccessTokenパラメーターの値として使用します。

   > 注:
   >
   > Azure AD ユーザーに必要な権限については、https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent#prerequisites/を参照してください。

3. 次のコマンドを実行し、IdentityPool を作成済みの Azure AD 動的セキュリティグループに接続します。

```
Set-AcctIdentityPool
-IdentityPoolName "SecurityGroupCatalog"
-AzureADTenantId 620387bb-9167-4bdd-8435-e3dccc58369e
-AzureADSecurityGroupNam "ExistingSecurityGroupName"
-AzureADAccessToken $AzureADAccessToken
<!--NeedCopy-->
```

名前付けスキームを更新すると、Citrix はその名前付けスキームで新しいメンバーシップ規則を更新します。カタログを削除すると、セキュリティグループではなく、メンバーシップ規則が削除されます。

Azure AD 参加済みデバイスのセキュリティグループを使用してマシンカタログを削除する

マシンカタログを削除すると、Azure AD 参加済みデバイスのセキュリティグループも削除されます。

Azure AD 動的セキュリティグループを削除するには、次の手順を実行します:

1. Azure AD にログインします。
2. MS Graph API へのアクセストークンを取得します。**PowerShell** コマンドを実行するときに、このアクセストークンを`$AzureADAccessToken`パラメーターの値として使用します。
3. 次のコマンドを実行します:

```
Remove-AcctIdentityPool
-IdentityPoolName "SecurityGroupCatalog"
-AzureADAccessToken $AzureADAccessToken
<!--NeedCopy-->
```

既存の **Azure AD** 割り当て済みセキュリティグループの下に **Azure AD** 動的セキュリティグループを作成する

既存の Azure AD 割り当て済みセキュリティグループの下に Azure AD 動的セキュリティグループを作成できます。以下の操作を実行できます:

- セキュリティグループ情報を取得します。
- オンプレミスの AD サーバーから同期されたすべての既存の Azure AD 割り当て済みセキュリティグループ、または Azure AD の役割を割り当てることができる割り当て済みセキュリティグループを取得します。
- すべての Azure AD 動的セキュリティグループを取得します。
- Azure AD 動的セキュリティグループを Azure AD 割り当て済みグループのメンバーとして追加します。
- Azure AD 動的セキュリティグループがマシンカタログとともに削除されるときに、Azure AD 動的セキュリティグループと Azure AD 割り当て済みセキュリティグループの間のメンバーシップを削除します。

操作のいずれかが失敗した場合にも、明示的なエラーメッセージが表示される可能性があります。

要件:

PowerShell コマンドを実行するときは、MS Graph API へのアクセストークンが必要です。

アクセストークンを取得するには、以下の手順に従います:

1. Microsoft Graph エクスプローラーを開き、Azure AD にログインします。
2. **Group.ReadWrite.All** および **GroupMember.ReadWrite.All** 権限に対する同意があることを確認してください。
3. Microsoft Graph エクスプローラーからアクセストークンを取得します。**PowerShell** コマンドを実行するときに、このアクセストークンを使用します。

グループ ID でセキュリティグループ情報を取得するには、以下の手順に従います:

1. アクセストークンを取得します。
2. Azure Portal からグループオブジェクト ID を検索します。
3. **PowerShell** コンソールで次の **PowerShell** コマンドを実行します:

```
Get-AcctAzureADSecurityGroup
-AccessToken <token> -GroupId <GroupUid>
<!--NeedCopy-->
```

グループの表示名でセキュリティグループを取得するには、以下の手順に従います:

1. アクセストークンを取得します。
2. **PowerShell** コンソールで次の **PowerShell** コマンドを実行します:

```
Get-AcctAzureADSecurityGroup
-AccessToken <token>
-Name <TargetGroupDisplayName>
<!--NeedCopy-->
```

表示名に部分文字列が含まれるセキュリティグループを取得するには、以下の手順に従います:

1. アクセストークンを取得します。
2. **PowerShell** コンソールで次の **PowerShell** コマンドを実行します:

```
Get-AcctAzureADSecurityGroup
-AccessToken <token>
-SearchString <displayNameSubString>
<!--NeedCopy-->
```

オンプレミスの AD サーバーから同期されたすべての既存の Azure AD 割り当て済みセキュリティグループ、または Azure AD の役割を割り当てることができる割り当て済みセキュリティグループを取得するには、以下の手順に従います:

1. アクセストークンを取得します。
2. **PowerShell** コンソールで次の **PowerShell** コマンドを実行します:

```
Get-AcctAzureADSecurityGroup
-AccessToken <token>
-Assigned true
<!--NeedCopy-->
```

すべての Azure AD 動的セキュリティグループを取得するには、以下の手順に従います:

1. アクセストークンを取得します。
2. **PowerShell** コンソールで次の **PowerShell** コマンドを実行します:


```
Get-AcctAzureADSecurityGroup
-AccessToken <token>
-Dynamic true
<!--NeedCopy-->
```

Azure AD 割り当て済みセキュリティグループを最大レコード数とともに取得するには、以下の手順に従います:

1. アクセストークンを取得します。
2. **PowerShell** コンソールで次の **PowerShell** コマンドを実行します:

```
Get-AcctAzureADSecurityGroup
-AccessToken <token>
-Assigned true
-MaxRecordCount 10
<!--NeedCopy-->
```

Azure AD 動的セキュリティグループを Azure AD 割り当て済みグループのメンバーとして追加するには、以下の手順に従います:

1. アクセストークンを取得します。
2. **PowerShell** コンソールで次の **PowerShell** コマンドを実行します:

```
Add-AcctAzureADSecurityGroupMember
-AccessToken <token>
-GroupId <ASG-Id>
-RefGroupId <DSG-Id>
<!--NeedCopy-->
```

Azure AD 割り当て済みセキュリティグループメンバーを取得するには、以下の手順に従います:

1. アクセストークンを取得します。
2. **PowerShell** コンソールで次の **PowerShell** コマンドを実行します:

```
Get-AcctAzureADSecurityGroupMember
-AccessToken <token>
-GroupId <ASG-Id>
<!--NeedCopy-->
```

> 注:
>
> `Get-AcctAzureADSecurityGroupMember`は、Azure AD 割り当て済みセキュリティグループの下の、種類がセキュリティグループの直接のメンバーのみを指定します。

Azure AD 動的セキュリティグループがマシンカタログとともに削除されるときに、Azure AD 動的セキュリティグループと Azure AD 割り当て済みセキュリティグループの間のメンバーシップを削除するには、以下の手順に従います:

1. アクセストークンを取得します。
2. **PowerShell** コンソールで次の **PowerShell** コマンドを実行します:

```
Remove-AcctIdentityPool
-IdentityPoolName "SecurityGroupCatalog"
-AzureADAccessToken $AzureADAccessToken
<!--NeedCopy-->
```

Azure AD 動的セキュリティグループ名の変更

マシンカタログに関連付けられている Azure AD 動的セキュリティグループ名を変更できます。この変更により、Azure AD ID プールオブジェクトに格納されているセキュリティグループ情報が、Azure ポータルに格納されている情報と一致するようになります。

> 注:
>
> Azure AD 動的セキュリティグループには、オンプレミス AD から同期されたセキュリティグループや、Office 365 グループなどの他のグループの種類は含まれません。

完全構成インターフェイスと **PowerShell** コマンドを使用して、Azure AD 動的セキュリティグループ名を変更できます。

PowerShell を使用して Azure AD 動的セキュリティグループ名を変更するには、以下の手順に従います:

1. **PowerShell** ウィンドウを開きます。
2. `asnp citrix*`を実行し、Citrix 固有の **PowerShell** モジュールをロードします。
3. コマンド`Set-AcctIdentityPool -AzureAdSeurityGroupName [DSG-Name]`を実行します。

Azure AD 動的セキュリティグループ名を変更できない場合は、適切なエラーメッセージが表示されます。

Microsoft Intune 対応カタログの作成

May 17, 2024

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

この記事では、Citrix DaaS を使用して Microsoft Intune 対応カタログを作成する方法について説明します。[完全な構成] インターフェイスまたは PowerShell を使用して、Microsoft Intune を有効にすることができます。

要件、制限事項、および考慮事項については、「Microsoft Intune」を参照してください。

完全な構成インターフェイスの使用

以下の情報は、「マシンカタログの作成」のガイダンスを補完する情報です。この機能を使用するには、カタログの作成時に［マシン **ID**］で［**Azure Active Directory** 参加済み］を選択する必要があります。この機能に固有の詳細に注意しながら、その記事の一般的なガイダンスに従ってください。

カタログ作成ウィザードで次の操作を行います:

- ［マシン **ID**］ページで、［**Azure Active Directory** 参加済み］を選択してから［マシンを **Microsoft Intune** に登録する］を選択します。有効になっている場合は、管理のためにマシンを Microsoft Intune に登録します。

PowerShell の使用

以下は、［完全な構成］インターフェイスでの操作と同じ PowerShell での手順です。

リモート PowerShell SDK を使用して Microsoft Intune にマシンを登録するには、`New-AcctIdentityPool` の `DeviceManagementType` パラメーターを使用します。この機能を使用するには、カタログが Azure AD 参加済みであること、および Azure AD に正しい Microsoft Intune ライセンスがあることが必要です。例:

```
1 New-AcctIdentityPool -AllowUnicode -DeviceManagementType "Intune"
     IdentityType="AzureAD" -WorkgroupMachine -IdentityPoolName "
     AzureADJoinedCatalog" -NamingScheme "AzureAD-VM-##" -
     NamingSchemeType "Numeric" -Scope @() -ZoneUid "81291221-d2f2-49d2-
     ab12-bae5bbd0df05"
2 <!--NeedCopy-->
```

トラブルシューティング

マシンを Microsoft Intune に登録できない場合は、次の手順を実行します:

- MCS でプロビジョニングされたマシンが Azure AD 参加済みかどうかを確認します。Azure AD 参加済みでないマシンは Microsoft Intune に登録できません。Azure AD 参加の問題のトラブルシューティングについては、https://docs.citrix.com/en-us/citrix-daas/install-configure/create-machine-identities-joined-catalogs/create-azure-ad-joined-catalogs.htmlを参照してください。
- Azure AD テナントに適切な Intune ライセンスが割り当てられているかどうかを確認します。Microsoft Intune のライセンス要件については、https://learn.microsoft.com/en-us/mem/intune/fundamentals/licensesにアクセスしてください。
- VDA バージョン 2206 以前のマスターイメージを使用するカタログの場合は、マシンの **AADLoginForWindows** 拡張機能のプロビジョニングステータスを確認してください。**AADLoginForWindows** 拡張機能が存在しない場合、考えられる原因は次のとおりです:

  - プロビジョニングスキームに関連付けられている ID プールの`IdentityType`が`AzureAD`に設定されていない、または`DeviceManagementType`が`Intune`に設定されていない。これを確認するには、`Get-AcctIdentityPool`を実行します。
  - **AADLoginForWindows** 拡張機能のインストールは、Azure ポリシーによってブロックされます。

- **AADLoginForWindows** 拡張機能のプロビジョニングの失敗についてトラブルシューティングするには、MCS でプロビジョニングされたマシンの`C:\WindowsAzure\Logs\Plugins\Microsoft.Azure.ActiveDirectory.AADLoginForWindows`にあるログを確認します。

  > 注:
  >
  > MCS は、VDA バージョン 2209 以降のマスターイメージを使用する場合、`AADLoginForWindows`拡張機能を使用しなくても、VM を Azure AD に参加させ、Microsoft Intune に登録することができます。この場合、`AADLoginForWindows`拡張機能は、MCS でプロビジョニングされたマシンにインストールされません。したがって、`AADLoginForWindows`拡張機能プロビジョニングログを収集できません。

- [アプリケーションとサービスログ] > [**Microsoft**] > [**Windows**] > [ユーザーデバイス登録] > [**DeviceManagement-Enterprise-Diagnostics-Provider**] にある Windows イベントログを確認します。

Hybrid Azure Active Directory 参加済みカタログの作成

May 17, 2024

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

この記事では、Citrix DaaS を使用して Hybrid Azure Active Directory（AD）参加済みカタログを作成する方法について説明します。

完全な構成インターフェイスまたは PowerShell を使用して、Azure AD 参加済みカタログを作成できます。

要件、制限、および考慮事項については、「Hybrid Azure Active Directory 参加済み」を参照してください。

完全な構成インターフェイスの使用

以下の情報は、「マシンカタログの作成」のガイダンスを補完する情報です。Hybrid Azure AD 参加済みカタログを作成するには、Hybrid Azure AD 参加済みカタログに固有の詳細に注意しながら、その記事の一般的なガイダンス

に従ってください。

カタログ作成ウィザードで次の操作を行います:

- ［マシン **ID**］ページで、［**Hybrid Azure Active Directory joined**］を選択します。作成済みマシンは組織によって所有され、その組織に属した Active Directory Domain Services アカウントでサインインします。これらのマシンはクラウドとオンプレミスに存在します。

> 注:
>
> ID の種類に ［**Hybrid Azure Active Directory joined**］を選択した場合、カタログ内の各マシンには、対応する AD コンピューターアカウントが必要です。

PowerShell の使用

以下は、［完全な構成］インターフェイスでの操作と同じ PowerShell での手順です。Remote PowerShell SDK を使用してカタログを作成する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/を参照してください。

オンプレミス AD 参加済みカタログと Hybrid Azure AD 参加済みカタログの違いは、ID プールとマシンアカウントの作成にあります。

Hybrid Azure AD 参加済みカタログのアカウントとともに ID プールを作成するには、次のようにします:

```
1 New-AcctIdentityPool -AllowUnicode -IdentityType "HybridAzureAD" -
    Domain "corp.local" -IdentityPoolName "HybridAADJoinedCatalog" -
    NamingScheme "HybridAAD-VM-##" -NamingSchemeType "Numeric" -OU "CN=
    AADComputers,DC=corp,DC=local" -Scope @() -ZoneUid "81291221-d2f2-49
    d2-ab12-bae5bbd0df05"
2 New-AcctADAccount -IdentityPoolName "HybridAADJoinedCatalog" -Count 10
    -ADUserName "corp\admin1" -ADPassword $password
3 Set-AcctAdAccountUserCert -IdentityPoolName "HybridAADJoinedCatalog" -
    All -ADUserName "corp\admin1" -ADPassword $password
4 <!--NeedCopy-->
```

> 注:
>
> `$password`は、書き込み権限を持つ AD ユーザーアカウントに一致するパスワードです。

Hybrid Azure AD 参加済みカタログを作成するために使用される他のすべてのコマンドは、従来のオンプレミス AD 参加済みカタログの場合と同じです。

Hybrid Azure AD 参加プロセスのステータスの表示

［完全な構成］インターフェイスでは、デリバリーグループ内の Hybrid Azure AD 参加済みマシンが電源オンの状態にあるときに、ハイブリッド Azure AD 参加プロセスのステータスが表示されます。ステータスを表示するには、

［検索］ を使用してそれらのマシンを識別し、下ペインの ［詳細］タブで ［マシン **ID**］を 1 つずつチェックします。次の情報が ［マシン **ID**］に表示されることがあります:

- Hybrid Azure AD 参加済み
- Azure AD 未参加

> 注:
>
> - マシンの電源を最初にオンにしたとき、Hybrid Azure AD の参加が遅れることがあります。これは、デフォルトのマシン ID 同期間隔（Azure AD Connect の 30 分）が原因です。マシンは、マシン ID が Azure AD Connect を介して Azure AD に同期された後でのみ、Hybrid Azure AD 参加済み状態になります。
> - マシンが Hybrid Azure AD 参加済み状態にならない場合、それらのマシンは Delivery Controller に登録されません。このような登録ステータスは ［初期化］状態として表示されます。

また、完全な構成インターフェイスで、マシンが使用できない理由を知ることができます。これを行うには、［検索］ノードでマシンをクリックし、下ペインの ［詳細］タブで ［登録］をオンにしてから、ツールチップを読んで追加情報を確認します。

トラブルシューティング

マシンが Hybrid Azure AD 参加済みにならない場合は、次の手順を実行します:

- Microsoft Azure AD ポータルでそのマシンアカウントが Azure AD に同期されているかどうかを確認します。同期されている場合、［**Azure AD** 未参加］と表示され、登録ステータスが保留中であることを示します。

  マシンアカウントを Azure AD に同期するには、次のことを確認してください:

  - そのマシンアカウントが、Azure AD と同期するように構成されている OU（組織単位）内にあること。**userCertificate** 属性のないマシンアカウントは、同期するように構成された OU 内にあっても、Azure AD に同期されません。
  - **userCertificate** 属性が、そのマシンアカウントに事前設定されていること。属性は Active Directory Explorer を使用して表示できます。
  - Azure AD Connect が、マシンアカウントの作成後に少なくとも 1 回同期されていること。一度も同期されていない場合は、Azure AD Connect マシンの PowerShell コンソールで、手動で`Start-ADSyncSyncCycle -PolicyType Delta`コマンドを実行し、即時の同期をトリガーします。

- **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix** の **DeviceKeyPair-Restored** の値をクエリすることにより、Hybrid Azure AD 参加用の Citrix 管理対象デバイスのキーペアが正しくマシンにプッシュされているかどうかを確認します。

  値が「1」であることを確認します。1 でない場合、考えられる理由は次のとおりです:

  - プロビジョニングスキームに関連付けられている ID プールのIdentityTypeが、HybridAzureADに設定されていない。これを確認するには、Get-AcctIdentityPoolを実行します。
  - マシンが、マシンカタログと同じプロビジョニングスキームを使用してプロビジョニングされていない。
  - マシンが、ローカルドメインに参加していない。ローカルドメイン参加済みであることは、Hybrid Azure AD 参加の前提条件です。

- MCS プロビジョニングマシンでdsregcmd /status /debugコマンドを実行して診断メッセージを確認します。

  - Hybrid Azure AD 参加に成功した場合、コマンドラインの出力で「**AzureAdJoined**」と「**DomainJoined**」が「**YES**」と表示されます。
  - YES と表示されない場合は、Microsoft 社のドキュメントを参照し、問題のトラブルシューティングを行ってください：https://docs.microsoft.com/en-us/azure/active-directory/devices/troubleshoot-hybrid-join-windows-current
  - 「サーバーメッセージ：**ID** が **xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx** のデバイスにユーザー証明書が見つかりません」というエラーメッセージが表示された場合は、次の PowerShell コマンドを実行してユーザー証明書を修復します：

    ```
    1  Repair-AcctIdentity -IdentityAccountName TEST\VM1 -Target
          UserCertificate
    2  <!--NeedCopy-->
    ```

ユーザー証明書の問題について詳しくは、CTX566696を参照してください。

ドメイン非参加カタログの作成

November 14, 2022

この記事では、Citrix DaaS を使用してドメイン非参加カタログを作成する方法について説明します。

要件、制限事項、および考慮事項について詳しくは、「ドメイン非参加」を参照してください。

マシンカタログを作成する前に、次のものが必要です：

1. 新しいリソースの場所
   - Citrix Cloud の管理 UI で左上のハンバーガーメニューから ［リソースの場所］ を選択します。
   - [**+** リソースの場所］ をクリックします。
   - リソースの場所の新しい名前を入力し、［保存］ をクリックします。
2. ホスト接続を作成します。詳しくは、「接続の作成と管理」セクションを参照してください。

Citrix DaaS を使用して、ワークグループまたはドメイン非参加マシンに基づいてカタログを作成できます。ドメイン非参加マシンの作成方法は、アカウント ID プールの作成方法によって異なります。アカウント ID プールは、カタログのプロビジョニング中にマシン名を作成および追跡するために MCS が使用するメカニズムです。

［完全な構成］インターフェイスまたは PowerShell を使用して、ドメイン非参加カタログを作成できます。

完全な構成インターフェイスの使用

以下の情報は、「マシンカタログの作成」のガイダンスを補完する情報です。ドメイン非参加カタログを作成するには、ドメイン非参加カタログに固有の詳細に注意しながら、その記事の一般的なガイダンスに従ってください。

カタログ作成ウィザードで次の操作を行います：

- ［マシン **ID**］ページで、［ドメイン非参加］を選択します。作成されたマシンはどのドメインにも参加していません。

> 注：
>
> ID の種類が ［ドメイン非参加］である場合には、カタログの最小機能レベルとしてバージョン 1811 以降の VDA が必要です。使用できるようにするために、必要であれば最小機能レベルを更新します。

PowerShell の使用

以下は、［完全な構成］インターフェイスでの操作と同じ PowerShell での手順です。

リモート PowerShell SDK を使用して、ドメイン非参加カタログの ID プールを作成できます。

たとえば、過去のリリースでは、すべての Active Directory フィールドが単一のインスタンスで提供されていました：

```
1 New-AcctIdentityPool -AllowUnicode -Domain "corp.local" -
    IdentityPoolName "NonDomainJoinedCatalog" -NamingScheme "NDJ-VM-##"
    -NamingSchemeType "Numeric" -OU "CN=Computers,DC=corp,DC=local"* -
    Scope @() -ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
2 <!--NeedCopy-->
```

現在、MCS では、新しい PowerShell パラメーターの **WorkgroupMachine** と **IdentityType** を使用して、ドメイン非参加カタログの ID プールを作成するようになりました。上記の同じ例を使用すると、これらのパラメーターにより、ドメイン管理者の資格情報を含むすべての AD（Active Directory）固有のパラメーターを指定する必要があるという要件がなくなります：

```
1 New-AcctIdentityPool -AllowUnicode -IdentityType "Workgroup" -
    WorkgroupMachine -IdentityPoolName "NonDomainJoinedCatalog" -
    NamingScheme "NDJ-VM-##" -NamingSchemeType "Numeric" -Scope @() -
    ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
2 <!--NeedCopy-->
```


ドメイン非参加カタログを作成するために使用される他のすべてのコマンドは、従来のオンプレミス Active Directory 参加済みカタログの場合と同じです。

マシンカタログの管理

June 13, 2024

> 注:
>
> この記事では、完全な構成インターフェイスと PowerShell コマンドを使用してカタログを管理する方法について説明します。［クイック展開］インターフェイスを使用してカタログを作成し、このインターフェイスを引き続き使用してカタログを管理する場合は、「クイック展開でのカタログ管理」の手順に従ってください。

はじめに

マシンカタログにマシンを追加したり、カタログからマシンを削除したり、マシンカタログの名前や説明を変更したりすることができます。また、カタログの Active Directory コンピューターアカウントを管理できます。

カタログの管理には、最新の OS アップデート、アンチウイルスプログラムのアップデート、オペレーティングシステムのアップグレード、または構成の変更が、各マシンに適用されていることの確認作業も含めることができます。

- Machine Creation Services（MCS）を使用して作成されたプール（ランダム）マシンが含まれるカタログは、カタログで使用されるイメージを更新してからマシンを更新することにより、マシンを管理できます。この方法により、多数のユーザーマシンを効率的に更新することができます。
- 静的で永続的に割り当てられたマシンが含まれるカタログの場合、それらのカタログが現在使用しているイメージまたはテンプレートを管理できますが、後でカタログに追加するマシンのみが新しいイメージまたはテンプレートを使用して作成されます。
- リモート PC アクセスカタログの場合は、ユーザーのマシンに対する更新を［完全な構成］管理インターフェイス外で管理します。サードパーティ製のソフトウェア配信ツールを使用して、個々のデスクトップまたはデスクトップのグループを管理します。

ホストハイパーバイザーおよびクラウドサービスへの接続の作成と管理については、「接続の作成と管理」を参照してください。

> 注:
>
> MCS では、Windows 10 IoT Core および Windows 10 IoT Enterprise はサポートされていません。詳しくは、Microsoft 社のサイトを参照してください。

永続インスタンスについて

永続マシンを含む MCS カタログのマスターイメージを更新すると、カタログに追加された新しいマシンは更新されたイメージを使用します。既存のマシンは引き続き元のマスターイメージを使用します。他の種類のカタログでも、イメージの更新プロセスは同様です。以下に注意してください:

- 永続ディスクカタログでは、既存のマシンは新しいイメージに更新されませんが、追加されたマシンは新しいイメージを使用します。
- 永続ディスクカタログではない場合、次回、Studio または PowerShell 内でマシンが再起動された場合にのみ、マシンイメージが更新されます。Studio の外部のハイパーバイザーからマシンを再起動した場合、ディスクはリセットされません。
- 永続的ではないカタログの場合、マシンごとに異なるイメージを使用するには、個別のカタログ内にイメージが存在する必要があります。

マシンカタログの管理

マシンカタログは次の 2 つの方法で管理できます。

- 完全な構成インターフェイスの使用
- PowerShell の使用

完全な構成インターフェイスの使用

このセクションでは、完全な構成インターフェイスを使用してカタログを管理する方法について説明します:

- カタログの詳細の表示
- カタログへのマシンの追加
- カタログからのマシンの削除
- カタログの編集
- カタログ名の変更
- カタログの削除
- カタログにおける Active Directory コンピューターアカウントの管理
- カタログのマスターイメージの変更
- 機能レベルを変更するか変更を元に戻す
- カタログの複製
- フォルダーを使用したカタログの整理
- VDA の自動アップグレードの構成
- カタログの構成セットの管理
- カタログの作成の再試行
- (Citrix 以外でプロビジョニングされた VDA のみ) 登録トークンの生成と管理

カタログの詳細の表示

1. 検索機能を使用して、特定のマシンカタログを見つけます。手順については、「インスタンスの検索」を参照してください。
2. 検索結果から必要に応じてカタログを選択します。
3. カタログ列の説明については、次の表を参照してください。
4. このカタログの詳細については、下部の詳細ペインのタブをクリックしてください。

列	説明
マシンカタログ	カタログ名と割り当ての種類。以下は割り当ての種類です: ランダム：カタログ内のマシンはユーザーにランダムに割り当てられます。 静的：カタログ内のマシンは、ユーザーに無期限で割り当てられます。
マシンの種類	設定可能な値は次のとおりです: OS の種類：マルチセッション OS（仮想）。ユーザーデータ：破棄。 OS の種類：マルチセッション OS（仮想）。ユーザーデータ：ローカルディスク上 OS の種類：シングルセッション OS（リモート PC アクセス） OS の種類：シングルセッション OS（仮想）。使用可能なプロビジョニング方法には、Machine Creation Services（MCS）、手動、および Citrix Provisioning Services が含まれます。
マシンの数	このカタログのマシン数。
割り当て済み（個）	デリバリーグループに割り当てられたカタログ内のマシンの数。
フォルダー	マシンカタログツリー内のカタログの場所。カタログが含まれているフォルダーの名前（末尾のバックスラッシュを含む）、またはカタログがルートレベルにある場合は–が表示されます。
VDA のアップグレード	VDA のアップグレードの状態。設定可能な値には、未構成、スケジュール設定済み、使用可能、および、最新です、が含まれます。
イメージの状態	カタログのイメージの更新状態。非永続マシンカタログにのみ適用されます。設定可能な値は次のとおりです: 完全に更新されました、一部更新されました、更新保留中、準備中

カタログへのマシンの追加

以下の点に注意してください:

- 追加するマシンの数に応じて十分なプロセッサ、メモリ、ストレージが仮想化ホスト（ハイパーバイザーまたはクラウドサービスプロバイダー）上にあることを確認してください。
- 十分な数の Active Directory コンピューターアカウントが使用可能であることを確認してください。既存のアカウントを使用している場合、使用可能なアカウントの数により、追加できるマシンの数が制限されることに注意してください。
- ［完全な構成］管理インターフェイスで、追加するマシン用に Active Directory コンピューターアカウントを作成する場合は、適切なドメイン管理者権限も必要です。

> ヒント:
>
> マシンカタログへのマシンの追加に使用される Citrix DaaS アカウントで AD 権限が制限されている場合は、［.. にログイン］画面で使用する予定のすべての Cloud Connector を追加します。

マシンカタログにマシンを追加するには、以下の手順に従います:

1. ［管理］**>**［完全な構成］の左側ペインで ［マシンカタログ］を選択します。
2. マシンカタログを選択し、操作バーの ［マシンの追加］を選択します。
3. ［仮想マシン］ページで、追加する仮想マシンの数を選択します。
4. ［マシン **ID**］ページで、次のように設定を構成します:

    - 一覧から ID を選択します。
    - 該当する場合は、アカウントを作成するか既存のアカウントを選択して、アカウントの場所（ドメイン）を指定します。

      追加する仮想マシンの数に対し、既存の Active Directory アカウントの数が不足している場合は、作成するアカウントのドメインと場所を選択します。

      既存の Active Directory アカウントを使用する場合、アカウントを参照するか、［インポート］を選択してアカウント名の一覧の `.csv` ファイルを指定します。追加するマシンに十分な数のアカウントをインポートする必要があります。完全な構成インターフェイスは、これらのアカウントを管理します。すべてのアカウントのパスワードのリセットを［完全な構成］インターフェイスに許可するか、アカウントのパスワードを指定します（すべてのアカウントで同じパスワードを使用する必要があります）。
    - この ID プールが他のカタログで使用されている場合、［完全な構成］を使用して別のプールに変更することはできません。代わりに、**Set-ProvScheme** PowerShell コマンドレットを使用してください。詳しくは、Citrix Virtual Apps and Desktops SDKドキュメントを参照してください。
    - アカウント名前付けスキームを指定します。番号記号（#）により、名前に追加される連番または文字とその位置が定義されます。たとえば、名前付けスキームとして「PC-Sales-##」を指定して［0〜9］を

選択すると、PC-Sales-01、PC-Sales-02、PC-Sales-03 などのコンピューターアカウント名が作成されます。

- オプションで、アカウント名の先頭を指定できます。

  アカウント名の先頭を指定するときは、次のシナリオに注意してください：開始の数字または文字が既に使用されている場合、最初に作成されるアカウントは、その後の最も近い未使用の数字または文字で名前付けされます。

  MCS を使用して展開されるマシンのシーケンス番号を PowerShell コマンドでカスタマイズするには、「マシン名のシーケンス番号の管理」を参照してください。

5. ［ドメイン資格情報］ページで ［資格情報の入力］を選択し、マシンアカウントを作成するために十分な権限を持つユーザー資格情報を入力します。

マシンの作成はバックグラウンドプロセスとして実行され、多くのマシンを追加する場合には時間がかかることがあります。［完全な構成］管理インターフェイスを閉じても、マシンの作成は続行されます。

CSV ファイルを使用してマシンをカタログに一括追加する

CSV ファイルを使用してマシンを一括で追加できます。この機能は、MCS（Machine Creation Services）でプロビジョニングされるカタログを除いて、すべてのカタログで使用できます。

マシンをカタログに一括追加するには、次の手順を実行します：

1. ［管理］**>**［完全な構成］の左側ペインで ［マシンカタログ］を選択します。
2. マシンカタログを選択し、操作バーの ［マシンの追加］を選択します。［マシンの追加］ウィンドウが開きます。
3. ［**CSV** ファイルの追加］を選択します。［マシンを一括で追加］ウィンドウが開きます。
4. ［**CSV** テンプレートのダウンロード］を選択します。
5. テンプレートファイルに入力します。
6. ファイルをドラッグまたは参照してアップロードします。
7. ［検証］を選択して、インポートの検証チェックを実行します。
8. ［インポート］を選択して処理を完了します。

CSV ファイルを使用してマシンを追加する場合の考慮事項

> 注：
>
> - Active Directory 以外のユーザーの場合は、次の形式で名前を入力する必要があります：`<identity provider>:<user name>`。例：`AzureAD:username`。
> - 仮想マシン名では大文字と小文字が区別されます。仮想マシンパスを入力するときは、仮想マシン名を正しく入力してください。

CSV テンプレートファイルを編集するときは、次の点に注意してください：

- この機能により、CSV ファイルを使用してマシンを一括追加する柔軟性が得られます。このファイルでは、（ユーザーの自動割り当てで使用するために）マシンのみを追加するか、ユーザーの割り当てとともにマシンを追加することができます。次の形式でデータを入力します：
  - マシンアカウントとユーザー名（samName）のペアの場合：
    - Domain\ComputerName1, Domain\Username1
    - Domain\ComputerName2, Domain\Username1;Domain\Username2
    - Domain\ComputerName3, AzureAD:username
  - マシンアカウントのみの場合：
    - Domain\ComputerName1
    - Domain\ComputerName2
  - VM とユーザー名のペアの場合：
    - XDHyp:\Connections\ConnectionName\RegionName\vm.folder\VMName1.vm,Domain\Compute
    - XDHyp:\Connections\ConnectionName\RegionName\vm.folder\VMName2.vm,Domain\Compute
  - VM のみの場合：
    - XDHyp:\Connections\ConnectionName\RegionName\vm.folder\VMName1.vm,Domain\Compute
    - XDHyp:\Connections\ConnectionName\RegionName\vm.folder\VMName2.vm,Domain\Compute

    例：
    `XDHyp:\Connections\xpace-scale\East US.region\vm.folder\wsvdaV3-2.vm`

    各項目の意味は次のとおりです。
    - `xpace-scale`は接続名です（[完全な構成] > [ホスト] > [接続およびリソースの追加] に入力した接続名）。詳しくは、「接続とリソースの作成」を参照してください。
    - `East US.region`はリージョン名です（拡張子として`.region`を含むリージョンの名前）。
    - `wsvdaV3-2.vm`は VM 名です（拡張子が`.vm`の仮想マシンの名前）。
- ファイルに含めることができるマシンの最大数は、1,000 です。1,000 台を超えるマシンをインポートするには、複数のファイルに分割してから、ファイルを 1 つずつインポートします。インポートするマシンは 1,000 台を超えないようにすることをお勧めします。そうしないと、マシンカタログの作成が完了するまでに時間がかかる場合があります。

同じ [マシンの追加] ページのカタログからマシンをエクスポートすることもできます。エクスポートされたマシンの CSV は、マシンを一括で追加するときにテンプレートとして使用できます。マシンをエクスポートするには：

1. [管理] > [完全な構成] の左側ペインで [マシンカタログ] を選択します。
2. マシンカタログを選択し、操作バーの [マシンの追加] を選択します。[マシンの追加] ウィンドウが開きます。
3. [**CSV** にエクスポート] を選択します。マシン一覧を含む CSV ファイルがダウンロードされます。

4. CSV ファイルを開き、必要に応じてマシンを追加または編集します。保存した CSV ファイルを使用してマシンを一括で追加するには、前のセクション「CSV ファイルを使用してマシンをカタログに一括追加する」を参照してください。

> 注:
>
> - この機能は、リモート PC アクセスカタログおよび MCS プロビジョニングカタログでは使用できません。
> - CSV ファイルでのマシンのエクスポートとインポートは、同じ種類のカタログ間でのみサポートされます。

WebSocket VDA 登録ツールを使用してマシンをカタログに登録する

WebSocket VDA 登録ツールによって、VDA マシンのトークンベースの登録が容易になります。このツールは、登録トークンを使用して VDA をマシンカタログに追加することで、接続を WebSocket 接続に変換することができます。

> 注:
>
> このツールは、どのマシンカタログにも登録されていない VDA マシンを登録するために設計されています。

登録ツールを実行するには、次の手順に従います:

1. VDA にログインします。
2. `C:\Program Files\Citrix\Virtual Desktop Agent\Web Socket Vda Enrollment Tool`内でツール（`EnrollMachine.exe`）を見つけます。
3. 適切な入力パラメーターを使用してツールを実行します。例:
   `EnrollMachine.exe -websocket_token_string:xxxxxxxxx`

次の表は、登録ツールの入力パラメーターについて説明しています:

パラメーター名	必須	説明	例
`-websocket_token_stdin`	はい	登録トークンを読み取ります。	`.\EnrollMachine.exe -websocket_token_stdin`
`-websocket_token_string`		コマンドラインパラメーターから直接登録トークンを読み取ります。	`.\EnrollMachine.exe -websocket_token_string:<token>`

パラメーター名	必須	説明	例
-websocket_token_file:[token-file-path]		指定されたパスから登録トークンを読み取ります。	.\EnrollMachine.exe -websocket_token_file:C:\token\test2.txt
log:[log-file-path]	いいえ	登録ツールのログを表示します。	.\EnrollMachine.exe log:[C:\ProgramData\Citrix\EnrollMachine\EnrollMachine.txt]
-help	いいえ	簡単なヘルプテキストを表示します。	.\EnrollMachine.exe -help

登録が成功すると、ツールとログに成功メッセージが表示されます。必ず［完全な構成］にサインインして、VDA マシンがカタログに追加され、マシンのステータスが登録されていることを確認してください。

トラブルシューティング　デフォルトでは、登録ツールのログは次の場所にあります：

C:\ProgramData\Citrix\EnrollMachine\EnrollMachine.txt

ログに別のパスを指定した場合は、log:[log-file-path]を使用してログを取得できます。

次の表は、登録ツールによって返されるコードの一覧です：

コード	文字列	説明
0	成功	VDA がマシンカタログに正常に追加されました。
-1	InvalidArgument	登録トークンの入力パラメーターが無効です。
-2	BrokerAgentNotFound	ブローカーエージェントサービスが見つかりません。
-3	TokenInvalid	入力されたトークンは無効です。
-4	TokenMissingRequiredClaims	トークンに必要なクレーム（CustomerId や Enrollment URI など）がありません。

コード	文字列	説明
-5	InternalError	一般的なエラーが発生しました。
-6	TimedOut	タスクがタイムアウトになりました。
-7	FailedToDetermineMachineADJoinStatus	マシンの AD 参加状態を返すサービスが失敗しました。
-8	ADMachineFailedToFindSid	AD マシンの SID を返すサービスが失敗しました。
-9	EnrollRequestFailed	HTTP エラーのため要求は失敗しました。
-10	EnrollResponseMissingRequiredFields	登録ツールの応答にパラメーター`VirtualSiteId`がありません。
-11	InsufficientPermission	タスクを実行するために必要な権限がありません。
-12	FailedToDetermineMachineAadJoinStatus	マシンの AD 参加状態をチェックするサービスがエラーをスローします。
-13	AadMachineFailedToFindDeviceId	システムによって追加された追加パラメーター`AAD device id`が空です。
-14	AadDeviceIdNotValid	システムによって追加された追加パラメーター`AAD device id`は有効な GUID ではありません。
-15	NoValidMacAddress	無効な MAC アドレスです。
-16	FailedToGetComputerHostNameForVdaInstanceName	追加パラメーター`VdaInstanceName`を設定するためのコンピューターのホスト名を取得できませんでした。
-17	VirtualDesktopAgentRegistryKeyFailedToOpen	Delivery Controller の一覧を書き込むために VDA レジストリキーを開くことができませんでした。
-18	Failed Token reached the max count	失敗したトークンが最大数に達しました。

カタログからのマシンの削除

マシンをマシンカタログから削除すると、ユーザーはそのマシンにアクセスできなくなります。そのため、マシンを削除する前に以下の点について確認してください:

- マシン上に重要なユーザーデータがなく、データがある場合はバックアップ済みであること。
- すべてのユーザーがログオフしていること。メンテナンスモードをオンにすると、マシンに新たに接続できなくなります。
- マシンの電源がオフになっていること。

カタログからマシンを削除するには、以下の手順に従います:

1. ［管理］**>**［完全な構成］の左側ペインで ［マシンカタログ］を選択します。
2. マシンカタログを選択し、操作バーの ［マシンの表示］を選択します。
3. 1 台または複数のマシンを選択し、操作バーの ［削除］を選択します。
4. 永続マシンをカタログから削除する場合は、ハイパーバイザーまたはクラウドサービスのどちらからも削除するかを選択します。両方を削除する場合は、それらの Active Directory アカウントを保持するか、無効にするか、削除するかを指定します。

Azure Resource Manager カタログから永続マシンを削除すると、マシンと関連するリソースグループを保持するように指定しても、Azure から削除されます。

非永続マシンをカタログから削除すると、ハイパーバイザーまたはクラウドサービスから自動的に削除されます。

カタログの編集

1. ［管理］**>**［完全な構成］の左側ペインで ［マシンカタログ］を選択します。
2. マシンカタログを選択し、操作バーの ［マシンカタログの編集］を選択します。
3. ［スコープ］ページで、スコープを変更します。
4. ［**NIC**］ページで、次の操作を実行します:

    - NIC のサブネットマッピングを変更するには、［割り当て済みネットワーク］フィールドからネットワークを選択します。
    - サブネットマッピングを追加するには、［**NIC** を追加］を選択し、［割り当て済みネットワーク］フィールドからネットワークを選択し、［保存］を選択します。

    カタログに関連付けられたホストに存在するサブネットのみが、［割り当て済みネットワーク］フィールドに表示されます。

    マシンプロファイルがない場合のみ、Azure マシンカタログに NIC を追加できます。

    > 注:
    >
    > - AWS マシンカタログの場合、同じサブネットを複数の NIC にマッピングすることはできません。
    > - マシンプロファイルを含むマシンカタログの場合、カタログ上の NIC の数は、マシンプロファイル上の NIC の数と同じである必要があります。
    > - この機能は、IBM Cloud ハイパーバイザーではサポートされていません。
    > - この機能は、Nutanix ハイパーバイザーの場合、Nutanix Prism Element でのみサポートされ

> ます。

5. [**VDA** のアップグレード] ページで、アップグレード先の VDA バージョンを変更または選択します。詳しくは、「VDA のアップグレード」を参照してください。
6. カタログの種類によっては、別のページが表示されることがあります。

   Azure Resource Manager イメージを使用して作成されたカタログの場合、以下のページが表示されます。変更は、後でカタログに追加したマシンにのみ適用されることに注意してください。既存のマシンは変更されません。

   - [仮想マシン] ページで、マシンサイズと、マシンを作成するアベイラビリティゾーンを変更します。

     > 注:
     >
     > - カタログがサポートするマシンサイズのみが表示されます。
     > - 必要に応じて、[ほかのマシンカタログで使用されるマシンサイズのみを表示する] を選択して、マシンサイズ一覧をフィルタリングします。

   - [マシンプロファイル] ページで、マシンプロファイルを使用するか変更するかを選択します。
   - (カタログが専用グループホストで構成されている場合のみ) [専用ホストグループ] ページで、ホストグループを変更するかどうかを選択します。
   - [ストレージとライセンスの種類] ページで、ストレージの種類、ライセンスの種類、および Azure Compute Gallery 設定 ([準備されたイメージを **Azure Compute Gallery** に配置します] が使用中の場合のみ利用可能) を変更するかどうかを選択します。

     > 注:
     >
     > 新しく選択した設定が現在のマシンサイズをサポートしていない場合、設定を変更するとマシンサイズ設定がリセットされることを通知する警告ダイアログボックスが表示されます。続行を選択すると、仮想マシンメニューの横に赤い点が表示され、新しいマシンサイズを選択するよう求められます。

   これらのページで使用可能な設定について詳しくは、「Azure Resource Manager イメージを使用してマシンカタログを作成する」を参照してください。

   リモート PC アクセスカタログの場合、次のページが表示されます:

   - [電源管理] ページでは、電源管理設定の変更、および電源管理接続の選択を行います。
   - [組織単位] ページでは、Active Directory 組織単位を追加または削除します。

7. [説明] ページでは、カタログの説明を変更します。
8. [適用] をクリックして変更を適用し、[保存] をクリックして終了します。

カタログ名の変更

1. ［管理］**>**［完全な構成］の左側ペインで ［マシンカタログ］を選択します。
2. マシンカタログを選択し、操作バーの ［マシンカタログの名前を変更］を選択します。
3. 新しい名前を入力します。

カタログの削除

カタログを削除する前に、以下の点について確認してください:

- すべてのユーザーがログオフしており、実行中の切断セッションがないこと。
- カタログ内のすべてのマシンのメンテナンスモードがオンで、新たに接続できないこと。
- カタログ内のすべてのマシンの電源がオフになっていること。
- そのカタログがデリバリーグループに関連付けられていないこと。すなわち、そのカタログのマシンがデリバリーグループに含まれていないこと。

カタログを削除するには、以下の手順に従います:

1. ［管理］**>**［完全な構成］の左側ペインで ［マシンカタログ］を選択します。
2. マシンカタログを選択し、操作バーの ［マシンカタログの削除］を選択します。
3. カタログに永続マシンが含まれている場合は、ハイパーバイザーまたはクラウドサービスのどちらからも削除するかを指定します。削除する場合は、それらの Active Directory アカウントを保持するか、無効にするか、削除するかを指定します。
4. 必要に応じて ［進行状況を隠す］を選択して、バックグラウンドで削除を実行します。

> 注:
>
> - Azure Resource Manager カタログを削除すると、関連するマシンとリソースグループを保持するように指定しても、Azure から削除されます。
> - 非永続マシンを含むカタログを削除すると、それらのマシンはハイパーバイザーまたはクラウドサービスから削除されます。
> - カタログの削除中にハイパーバイザーまたはクラウド サービスに到達できない場合、カタログと仮想マシンは両方とも削除に失敗します。必要に応じて、Citrix サイトデータベースから仮想マシンレコードのみを削除することができます。これを行うには、［マシンカタログ］ノードでマシンカタログを選択し、［トラブルシューティング］タブに示されている削除を実行します。この操作により、仮想マシンはホスト上にそのまま残ることに注意してください。

カタログにおける **Active Directory** コンピューターアカウントの管理

マシンカタログの Active Directory アカウントについて、次の操作を行えます:

- シングルセッションカタログおよびマルチセッションカタログから Active Directory コンピューターアカウントを削除して未使用のマシンアカウントを解放する。解放したアカウントは、ほかのマシンで使用可能になります。
- カタログに追加するマシン用のコンピューターアカウントを追加しておく。組織単位名にはスラッシュ（/）を使用しないでください。

Active Directory アカウントを管理するには、以下の手順に従います:

1. ［管理］**>**［完全な構成］の左側ペインで ［マシンカタログ］を選択します。
2. カタログを選択し、操作バーの ［**Active Directory** アカウント管理］を選択します。
3. 必要に応じてコンピューターアカウントを追加または削除します。アカウントを追加する場合は、すべてのアカウントのパスワードをリセットするか、すべてのアカウントに適用されるパスワードを入力するかを選択します。

   アカウントの現在のパスワードがわからない場合は、すべてのアカウントのパスワードをリセットするオプションを選択します。パスワードをリセットするための権限が必要です。パスワードを指定する場合は、アカウントのインポート時にパスワードが変更されます。アカウントを削除する場合は、そのアカウントを Active Directory 内で保持するか、無効にするか、削除するかを選択します。

カタログからマシンを削除するか、カタログを削除する場合にも、Active Directory アカウントを保持するか、無効にするか、削除するかを指定することができます。

カタログのマスターイメージの変更

カタログのマスターイメージを変更する前に、イメージのコピーまたはスナップショットを保存しておくことをお勧めします。データベースには、各マシンカタログで使用されたイメージの履歴記録が保持されます。デスクトップに展開した新しいイメージによりユーザーの操作に問題が発生した場合は、カタログ内のマシンをロールバックして以前のバージョンのマスターイメージに戻し、ユーザーのダウンタイムを最小限に抑えることができます。イメージの削除、移動、または名前変更を行わないでください。そうしないと、マスターイメージをロールバックできません。

> 重要:
>
> 永続カタログのマスターイメージを変更するときは、次の点を考慮してください: 後でカタログに追加するマシンのみが新しいイメージを使用して作成されます。新しいイメージはカタログ内の既存のマシンにロールアウトされません。

マシンは、更新後に自動的に再起動されます。

イメージの更新または作成

既存のイメージを更新するか新しく作成することで、ホストハイパーバイザー上に新しいイメージを準備してから、カタログのマスターイメージを変更します。

1. ハイパーバイザー上またはクラウドサービスプロバイダー上で、現在の仮想マシンのスナップショットを作成してわかりやすい名前を付けます。このスナップショットを使用して、マスターイメージをロールバックできます。
2. 必要に応じて、イメージをオンにしてログオンします。
3. 更新をインストールするか、イメージに対して必要な変更を加えます。
4. イメージで Personal vDisk が使用される場合は、インベントリを更新します。
5. 仮想マシンの電源を切ります。
6. 仮想マシンのスナップショットを作成してわかりやすい名前を付けます。この名前はマスターイメージの変更時に使用されます。

> 注:
>
> スナップショットは管理インターフェイスを使用して作成することもできますが、ハイパーバイザー側の管理コンソールでスナップショットを作成し、そのスナップショットを［完全な構成］管理インターフェイスで選択することをお勧めします。これにより、スナップショットに自動生成される名前を付けるのではなく、わかりやすい名前と説明を指定できます。GPU の仮想化機能を使用したイメージを更新する場合は、XenServer の XenCenter コンソールを使用する必要があります。

マスターイメージの変更

新しいマスターイメージをカタログ内のすべてのマシンにロールアウトするには:

1. ［管理］**>**［完全な構成］の左側ペインで ［マシンカタログ］を選択します。
2. カタログを選択し、操作バーの ［マスターイメージの変更］を選択します。
3. ［イメージ］ページで、ホストおよびロールアウトするイメージを選択します。

   > ヒント:
   >
   > MCS で作成したカタログの場合、イメージにメモを追加することで、そのイメージに注釈を付けることができます。メモには最大 500 文字を含めることができます。マスターイメージを変更するたびに、メモを追加するかどうかに関係なく、メモ関連のエントリが作成されます。メモを追加せずにカタログを更新すると、エントリは null（-）として表示されます。イメージのメモ履歴を表示するには、カタログを選択し、下のペインで ［テンプレートのプロパティ］をクリックしてから、［メモ履歴の表示］をクリックします。

4. ［ロールアウト方法］ページで、マシンカタログ内のマシンを新しいイメージによって変更するタイミング：次回シャットダウン時または即時を選択します。

   > 注:
   >
   > ロールアウトは非永続的な VM にのみ適用されるため、永続的な VM では ［ロールアウト戦略］ページを使用できません。

5. ［概要］ページの情報を確認し、［完了］を選択します。各マシンは、更新後に自動的に再起動されます。

   更新の進行状況を追跡するには、［マシンカタログ］でカタログを見つけて、インラインの進行状況バーと手順ごとの進行状況グラフを表示します。非永続カタログの場合は、［イメージを更新］列を通じて、完全に更新されている、部分的に更新されている、更新が保留中であるなどのイメージ更新状態を追跡できます。

   > ヒント：
   >
   > ［イメージを更新］列を表示するには、操作バーの［表示する列］を選択し、［マシンカタログ］**>** ［**Image Status**］を選択し、［保存］をクリックします。

PowerShell SDK を使用してカタログを更新する場合、イメージまたはそのスナップショットの代わりに、ハイパーバイザーテンプレート（`VMTemplates`）を指定できます。

ロールアウト方法

次回のシャットダウン時にイメージを変更すると、現在使用されていないマシン、つまりアクティブなユーザーセッションのないマシンにも即座に反映されます。現在アクティブなセッションが終了すると、使用中のシステムも更新を受け取ります。

> 注：
>
> ロールアウト戦略は、非永続的な VM にのみ適用されます。

以下に注意してください：

- 新しいセッションは、該当するマシンで更新が完了するまで起動できません。
- シングルセッションマシンでは、マシンが使用されていないとき、またはユーザーがログインしていないときに、即座にマシンが更新されます。
- 子マシンがあるマルチセッション OS の場合、再起動は自動的に行われません。手動でシャットダウンし、再起動する必要があります。

> ヒント：
>
> ホスト接続の詳細設定を使用して、再起動するマシンの数を制限します。これらの設定を使用して、特定のカタログに対して実行されるアクションを変更します。詳細設定は Hypervisor によって異なります。

マスターイメージのロールバック

更新後または新規のイメージは、ロールアウトした後にロールバックすることができます。ロールバックは、新たに更新されたマシンで問題が発生した場合に必要になることがあります。ロールバックした場合、カタログ内のマシンは前回の動作イメージまでロールバックされます。より新しいイメージを必要とする新機能は、利用できなくなりました。ロールアウトと同様に、ロールバックでもマシンは再起動されます。

1. ［管理］**>** ［完全な構成］の左側ペインで ［マシンカタログ］を選択します。

2. カタログを選択し、操作バーの ［マスターイメージのロールバック］を選択します。
3. ロールアウト処理について前述したとおり、古いイメージをマシンに適用するタイミングを指定します。

ロールバックは、復元が必要なマシンにのみ適用されます。たとえば、イメージの変更時にログアウトしなかったユーザーなど、新しいまたは更新したイメージに変更されていないマシンのユーザーは、通知メッセージを受信したり強制的にログオフされたりすることはありません。

ロールバックの進行状況を追跡するには、［マシンカタログ］でカタログを見つけて、インラインの進行状況バーと手順ごとの進行状況グラフを表示します。

次のような場合、ロールバックできません（［マスターイメージのロール バック］オプションは表示されません）。

- ロールバックする権限がない。
- カタログが MCS を使用して作成されていない。
- カタログが、OS ディスクのイメージを使用して作成されている。
- カタログの作成に使用されたスナップショットが破損した。
- カタログ内のマシンに対してユーザーが行った変更が保持されない。
- カタログ内のマシンが実行中である。

機能レベルを変更するか変更を元に戻す

マシン上の VDA を新しいバージョンにアップグレードした場合は、マシンカタログの機能レベルを変更する必要があります。すべての VDA を最新バージョンにアップグレードして、最新の機能をすべて使用できるようにすることをお勧めします。

マシンカタログの機能レベルを変更する前に：

- アップグレードしたマシンを起動して、Citrix DaaS が登録できるようにします。このときに、そのマシンカタログ内のマシンについてアップグレードが必要かどうかが管理インターフェイスによりチェックされます。

カタログの機能レベルを変更するには：

1. ［管理］**>**［完全な構成］の左側ペインで ［マシンカタログ］を選択します。
2. カタログを選択します。下ペインの ［詳細］タブにバージョン情報が表示されます。
3. ［機能レベルの変更］を選択します。管理インターフェイスにより機能レベルの変更が必要なことが検出されると、メッセージが表示されます。画面の指示に従って操作します。変更できないマシンがある場合は、その理由を説明する以下のようなメッセージが表示されます。すべてのマシンが適切に機能することを確認するため。これらの問題を解決した上で ［変更］をクリックすることをお勧めします。

カタログをアップグレードした後でマシンを以前の VDA バージョンに戻すには、カタログを選択し、操作バーで ［機能レベルの変更を元に戻す］を選択します。

カタログの複製

カタログを複製する前に、次の考慮事項に注意してください：

- オペレーティングシステムとマシンの管理に関連する設定は変更できません。複製されたカタログは、元のカタログからこれらの設定を継承します。
- カタログの複製は、完了するまでに時間がかかることがあります。必要に応じて ［進行状況を隠す］を選択して、バックグラウンドで複製を実行します。
- 複製されたカタログは元のカタログの名前を継承し、サフィックスとして「Copy」が付きます。この名前は変更できます。「カタログ名の変更」を参照してください。
- 複製が完了したら、複製したカタログを必ずデリバリーグループに割り当ててください。
- 複製することによって空のカタログを作成できます。カタログの複製中に、MCS でプロビジョニングされたカタログのマシン数をゼロに設定し、MCS 以外でプロビジョニングされたカタログのマシンを追加しないようにすることができます。

1. ［管理］**>**［完全な構成］の左側ペインで ［マシンカタログ］を選択します。
2. カタログを選択し、操作バーの ［複製］を選択します。
3. ［選択したマシンカタログの複製］ウィンドウで、複製されたカタログの設定を表示し、必要に応じて設定を構成します。［次へ］を選択して、次のページに進みます。
4. ［概要］ページで、設定の概要を表示し、［完了］を選択して複製を開始します。
5. 必要に応じて ［進行状況を隠す］を選択して、バックグラウンドで複製を実行します。

フォルダーを使用したカタログの整理

カタログを整理するためのフォルダーを作成して、アクセスを簡単にすることができます。たとえば、イメージの種類や組織構造ごとにカタログを整理できます。

必須の役割

デフォルトでは、カタログフォルダーを作成および管理するために、クラウド管理者、すべての管理権限を実行できる管理者、またはマシンカタログ管理者という組み込みの役割が必要です。必要に応じて、カタログフォルダーを作成および管理するための役割をカスタマイズできます。詳しくは、「必要な権限」を参照してください。

カタログフォルダーの作成

始める前に、まずカタログを整理する方法を計画します。以下に注意してください:

- 最大で 5 レベルまでの階層構造でフォルダーをネストできます（デフォルトのルートフォルダーを除く）。
- カタログフォルダーには、カタログとサブフォルダーを含めることができます。
- バックエンドのフォルダーツリーは、［完全な構成］のすべてのノード（［マシンカタログ］や ［アプリケーション］ノードなど）で共有されます。フォルダーの名前変更や移動時に他のノードと名前が競合しないように、異なるノードの第 1 レベルのフォルダーには異なる名前を付けることをお勧めします。

カタログフォルダーを作成するには、次の手順に従います:

1. ［管理］**>**［完全な構成］の左側ペインで ［マシンカタログ］を選択します。
2. フォルダー階層でフォルダーを選択し、［アクション］バーで ［フォルダーの作成］を選択します。
3. 新しいフォルダーの名前を入力し、［完了］をクリックします。

> ヒント：
>
> 意図しない場所にフォルダーを作成した場合は、それを正しい場所にドラッグできます。

カタログの移動

フォルダー間でカタログを移動できます。詳細な手順は次のとおりです：

1. ［管理］**>**［完全な構成］の左側ペインで ［マシンカタログ］を選択します。
2. フォルダーごとにカタログを表示します。フォルダー階層の上にある ［すべて表示］をオンにして、一度にすべてのカタログを表示することもできます。
3. カタログを右クリックし、［マシンカタログの移動］を選択します。
4. カタログの移動先のフォルダーを選択し、［完了］をクリックします。

> ヒント：
>
> カタログをフォルダーにドラッグできます。

カタログフォルダーの管理

カタログフォルダーの削除、名前変更、および移動を行うことができます。

フォルダーの削除は、フォルダーとそのサブフォルダーにカタログが含まれていない場合にのみ可能となります。

フォルダーを管理するには、次の手順に従います：

1. ［管理］**>**［完全な構成］の左側ペインで ［マシンカタログ］を選択します。
2. フォルダー階層でフォルダーを選択し、必要に応じて ［アクション］バーでアクションを選択します：
   - フォルダーの名前を変更するには、［フォルダーの名前変更］を選択します。
   - フォルダーを削除するには、［フォルダーの削除］を選択します。
   - フォルダーを移動するには、［フォルダーの移動］を選択します。
3. 画面の指示に従って、残りの手順を完了します。

必要な権限

次の表に、カタログフォルダーでアクションを実行するために必要な権限を示します。

アクション	必要な権限
カタログフォルダーの作成	マシンカタログフォルダーの作成
カタログフォルダーの削除	マシンカタログフォルダーの削除
カタログフォルダーの移動	マシンカタログフォルダーの移動
カタログフォルダーの名前変更	マシンカタログフォルダーの編集
カタログをフォルダーに移動	マシンカタログフォルダーの編集とマシンカタログプロパティの編集

VDA の自動アップグレードの構成

> 重要:
>
> - スムーズにアップグレードするには、VDA を CR または LTSR CU バージョンにアップグレードする前に、前提条件を満たしていることを確認し、既知の問題を確認してください。「完全な構成インターフェイスを使用した VDA のアップグレード」を参照してください。
> - LTSR VDA を LTSR 累積更新プログラム（CU）バージョンにアップグレードする場合は、VDA 上で実行されている Citrix VDA Upgrade Agent のバージョンが 7.36.0.7 以降であることを確認してください。詳しくは、「完全な構成インターフェイスを使用した VDA のアップグレード」を参照してください。
> - 以前のバージョンから新しいバージョンに切り替えれば、CR VDA と LTSR VDA を切り替えることができます。ダウングレードと見なされるため、新しいバージョンから以前のバージョンに切り替えることはできません。たとえば、2212 CR から 2203 LTSR（任意の CU）にダウングレードすることはできませんが、2112 CR から 2203 LTSR（任意の CU）にアップグレードすることはできます。
> - PowerShell を使用して VDA をアップグレードすることもできます。「PowerShell を使用した VDA のアップグレード」を参照してください。

この機能では、以下を実行できます:

- カタログごとに VDA をアップグレードする
- スケジュールされた VDA アップグレードを編集またはキャンセルする
- カタログ作成後に VDA アップグレード設定を構成する
- マシンごとに VDA をアップグレードする

> 注:
>
> - カタログの VDA アップグレードをスケジュールする場合、アップグレードできるのは、VDA Upgrade Agent がインストールされているカタログ内の VDA のみです。
> - マシンがメンテナンスモードの場合、またはマシンでセッションが実行されている場合、VDA のアップグレードは失敗します。

サポートされているマシンの種類

この機能は、次のマシンの種類に適用されます:

- MCS でプロビジョニングされた永続的なマシン（AD 参加、Azure AD 参加、およびドメイン非参加）。カタログの作成中に、［マシン管理］ページの ［**Citrix Machine Creation Services**］を使用してそれらを展開します。
- Remote PC アクセスマシン
- Citrix HDX Plus for Windows 365 マシン
- Citrix Provisioning Service 以外または関連テクノロジ以外を使用してプロビジョニングされたその他の永続的なマシン。カタログの作成中に、［マシン管理］ページの ［ほかのサービスまたはテクノロジ］を使用して、管理のために DaaS にこれらのマシンを追加します。

Citrix Machine Creation Services およびその他のサービスまたはテクノロジのオプションについて詳しくは、「マシン管理」を参照してください。

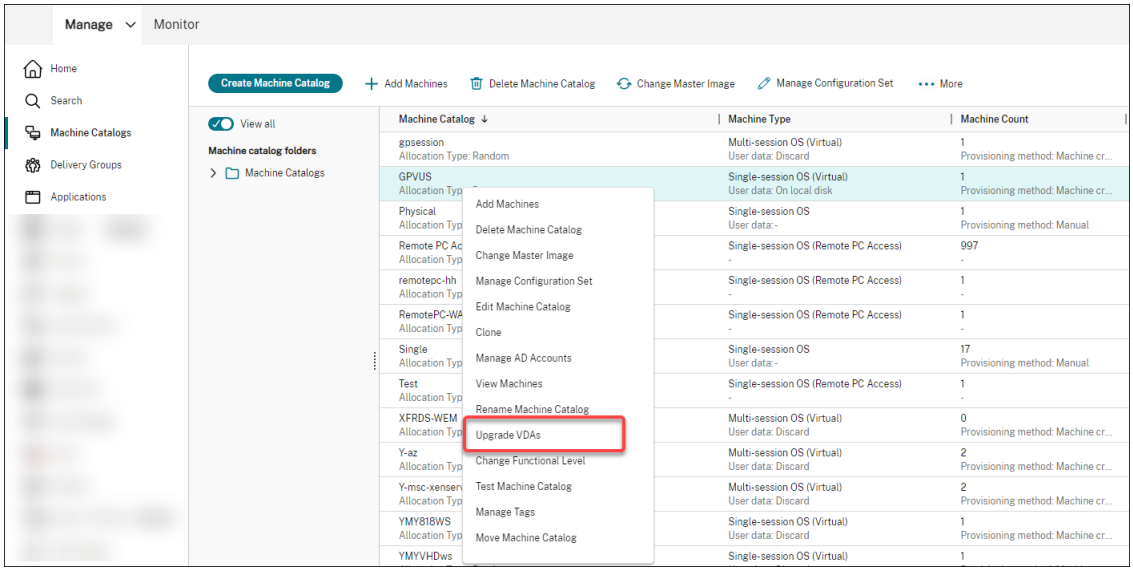
> 注:
>
> MCS でプロビジョニングされたマシンの場合、静的な永続マシンのみがサポートされます。ランダムマシンは永続的であってもサポートされません。

カタログごとに **VDA** をアップグレードする

> 注:
>
> カタログの VDA アップグレードをスケジュールするときは、カタログ内のすべてのマシンがアップグレード対象に含まれることに注意してください。したがって、アップグレードを開始する前に、これらのマシンのバックアップを作成することをお勧めします。

カタログの VDA アップグレードを有効にした後、カタログ内の VDA をすぐにアップグレードする、またはカタログのアップグレードをスケジュールすることができます。そのためには、次の手順を実行します:

1. ［管理］**>** ［完全な構成］から、［マシンカタログ］を選択します。
2. カタログを選択してから、コンテキストメニューまたは操作バーで ［**VDA** のアップグレード］を選択します。（右クリックしてコンテキストメニューを表示します。）［VDA のアップグレード］ウィンドウが表示されます。



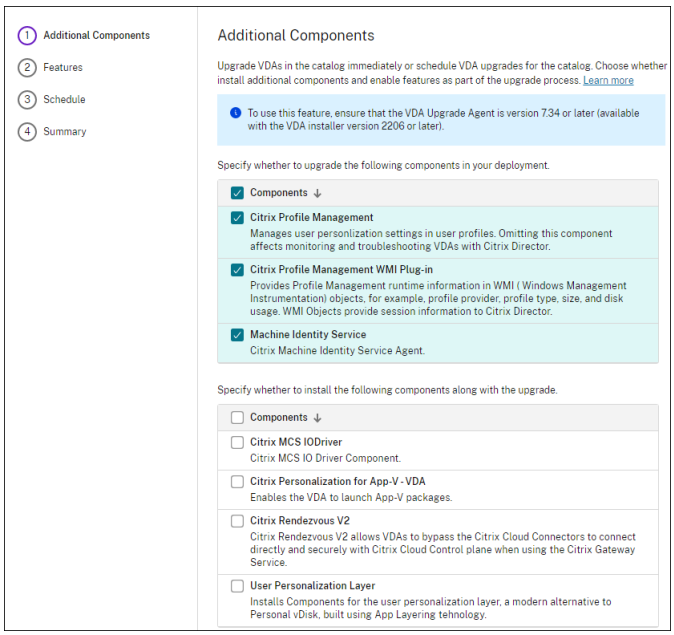
3. 環境内の追加コンポーネントをアップグレードするかどうかを選択します。また、アップグレードだけでなく、特定のコンポーネントをインストールすることもできます。コンポーネントを構成する必要がある場合は、［構成］をクリックして行います。構成後に構成を変更するには、［編集］をクリックします。

   重要:

   - 追加コンポーネント機能を使用するには、VDA Upgrade Agent がバージョン 7.34 以降であることを確認してください。このバージョンは、VDA インストーラーバージョン 2206 以降に含まれています。

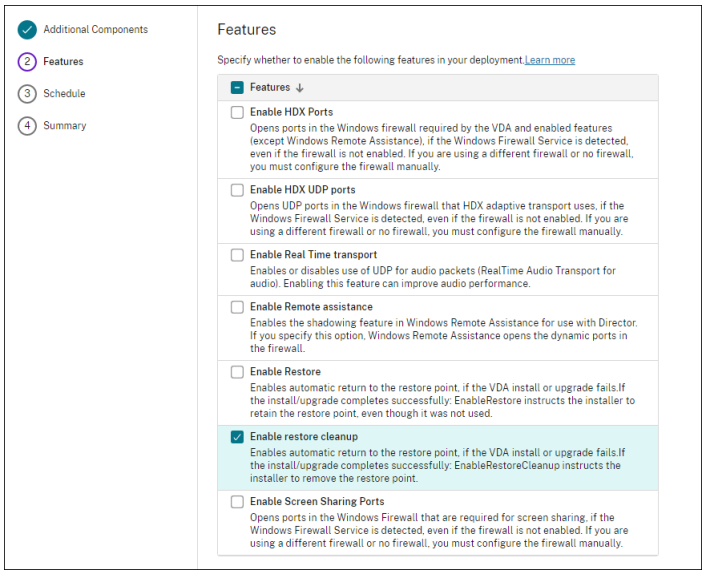
   注:

   - コンポーネントをアップグレードしない場合は、環境内でコンポーネントが現行バージョンのままになります。
   - 追加コンポーネントを網羅した一覧については、「VDA のインストール」を参照してください。



4. ［次へ］をクリックします。
5. 一覧に表示された機能のいずれを有効にするかを選択します。［次へ］をクリックします。

> 注:
>
> デフォルトでは、［クリーンアップの復元を有効にする］チェックボックスがオンにされています。この復元機能を有効にすることをお勧めします。この機能を有効にすると、アップグレードの開始前にシステムの復元ポイントが作成されます。VDA のインストールが正常に完了すると、復元ポイントは削除されます。詳しくは、［「インストールまたはアップグレードの失敗時の復元」を参照してください。



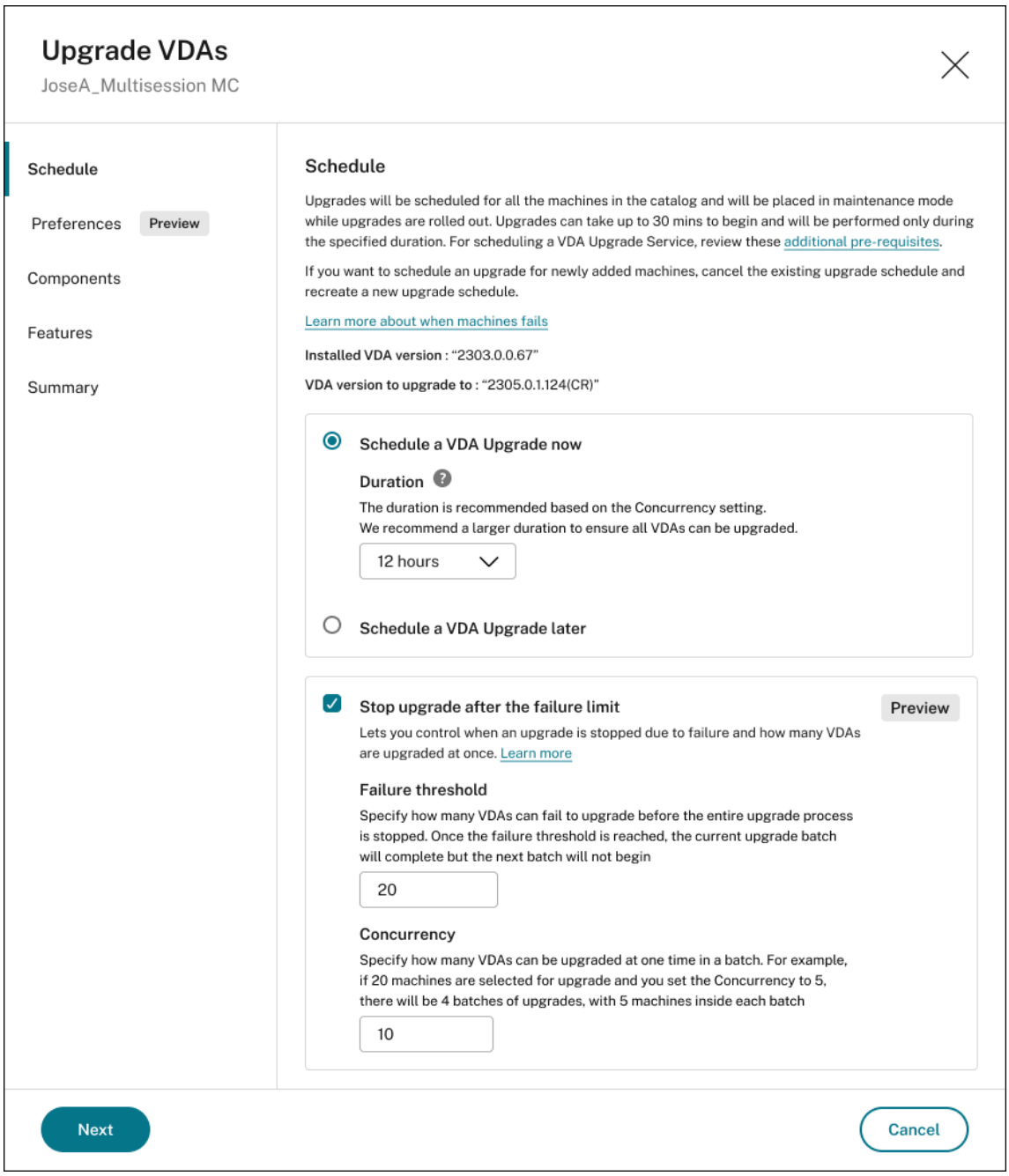
6. VDA をすぐにアップグレードするか、スケジュールされた時間にアップグレードするかを選択します。
   - VDA をすぐにアップグレードするには、［今すぐアップグレード］を選択して、期間を指定します。

期間とは、VDA Upgrade Service が追加のアップグレードを開始しなくなるまでの時間（時間単位）です。進行中のアップグレードは完了するまで実行されます。その期間、DaaS は（アクティブなセッションがなくなった場合など）VDA が適格になると、VDA のアップグレードを開始します。

アップグレードが必要な VDA が多いほど、この期間は長くなります。大きな値（たとえば、12 時間）を選択することをお勧めします。そうしないと、VDA の数によっては、一部の VDA がこの期間内に DaaS でアップグレードできないままの可能性があります。

- アップグレードをスケジュールするには、［後でアップグレード］を選択し、アップグレードをいつ実行するかを指定します。

  アップグレードは、今後 7 日間のみスケジュールできます。スケジュールしたアップグレードは、現在カタログにあるマシンにのみ適用されます。後でカタログにマシンを追加し、それらもアップグレードしたいという場合は、スケジュールされたアップグレードをキャンセルしてから、スケジュールを再作成します。



7. [**Stop upgrade after the failure limit**] オプションを選択します。

> 注:
>
> デフォルトでは、この機能は無効になっていますが、管理者は利用できます。

動作の詳細

- 失敗のしきい値と同時実行レベルはゼロより大きい値である必要があります。
- 失敗のしきい値と同時実行レベルは、アップグレードがスケジュールされているマシンの合計数以下で

ある必要があります

失敗のしきい値 (FailureThreshold)	同時実行レベル (ConcurrencyLevel)	動作
指定されている	指定されていない、または 0	FailureThreshold が適用され、ConcucrrencyLevel は以前と同様にロードバランサーによって決定されます。
指定されていない、または 0	指定されている	FailureThreshold のデフォルトは 10000（カタログあたりの最大マシン数）で、ConcucrrencyLevel はバッチ処理に使用されます。
指定されていない、または 0	指定されていない、または 0	デフォルトの動作は、ロードバランサーによって更新された同時実行レベルに適用されます。

8. **FailureThreshold** を入力します。

   > 注:
   >
   > 失敗のしきい値は、アップグレードエージェントによって取得されない後続のバッチの保留中のアップグレードインストールを、VUS が停止するまで失敗できる回数です。

9. **Concurrency** を入力します。

   > 注:
   >
   > 同時アップグレードとは、アップグレード期間中の任意の時点で同時にアップグレードできる仮想マシンの数です。

10. ［次へ］をクリックします。
11. ［概要］ページで選択内容を確認し、［完了］をクリックして設定を適用し、ウィンドウを終了します。

> 注:
>
> - ［**VDA** のアップグレード］オプションは、カタログの VDA アップグレードを有効にした後でのみ使用できます。VDA アップグレードを有効にするには、カタログを編集します。
> - アップグレードが展開されている間、カタログ内のすべてのマシンはメンテナンスモードになります。アップグレードは、開始まで最大 30 分かかる場合があり、指定した期間中にのみ実行されます。

［マシンカタログ］ノードの ［**VDA** アップグレード］列には、カタログの VDA アップグレード情報が表示されます。表示される情報には、次のようなものがあります:

> ヒント：
>
> ［**VDA** のアップグレード］列を表示するには、操作バーの ［表示する列］を選択し、［マシンカタログ］**>** ［**VDA** のアップグレード］を選択して、［保存］をクリックします。

- 利用可能：新しい VDA バージョンが利用可能です。
- スケジュール設定済み：VDA のアップグレードはスケジュール設定済みです。
- 未構成：カタログの VDA アップグレードを有効にしていない場合に表示されます。
- 最新：カタログの VDA は最新です。
- 不明：VDA のアップグレードに必要な情報を取得できません。考えられる理由は次のとおりです：
  - VDA がアップグレード期間中に使用されていた。
  - 進行中のアップグレード数が上限の 500 に達した。
  - アップグレード期間中、VDA Upgrade Agentが応答しなかった。エージェントが VDA で実行中で、Citrix DaaS と通信できることを確認してください。
  - アップグレードの検証チェックを実行できない。「VDA のアップグレード要件」を参照してください。

カタログの VDA アップグレードのステータスを表示することもできます。これを行うには、カタログをクリックしてから、［詳細］タブの ［**VDA** アップグレード状態］の情報を確認します。表示される情報には、次のようなものがあります：

- スケジュール未設定：カタログの VDA アップグレードを有効にしましたが、アップグレードスケジュールが設定されていません。
- スケジュール設定済み：カタログのアップグレードスケジュールを作成済みです。たとえば、スケジュールを`09:00 PM, December 14, 2030`開始に設定すると、情報は次のように表示されます：「`December 14, 2030 09:00 PM UTC`でスケジュール設定済み」。
- 進行中：VDA アップグレードが開始しています。
- キャンセル済み：スケジュールされたアップグレードをキャンセルしました。
- 失敗：カタログには、VDA が正常にアップグレードされなかったマシンが 1 つまたは複数含まれています。
- 成功：カタログ内のすべての VDA が正常にアップグレードされました。

カタログの推奨操作を実行して、VDA アップグレードの問題をトラブルシューティングすることもできます。これを行うには、カタログをクリックしてから ［トラブルシューティング］タブに移動します。

特定の VDA アップグレード状態のカタログにすばやくドリルダウンするために、フィルターを使用できます。詳しくは、「［完全な構成］管理インターフェイスでの［検索］の使用」を参照してください。

次の考慮事項に注意してください：

- ［**VDA** アップグレード］または ［**VDA** アップグレード状態］フィルターは、次のフィルターでのみ使用できます：［名前］および ［マシンカタログ］。
- ［**VDA** アップグレード］または ［**VDA** アップグレード状態］フィルターを使用すると、右上隅の ［エラー］と［警告］が使用できなくなります。

スケジュールされた **VDA** アップグレードを編集またはキャンセルする

カタログのアップグレードをスケジュールした後、スケジュールされたアップグレードを編集またはキャンセルする必要が生じることがあります。そのためには、次の手順を実行します:

1. ［管理］**>** ［完全な構成］から、［マシンカタログ］を選択します。
2. カタログを選択してから、操作バーで［スケジュールされた **VDA** アップグレードの編集］を選択します。[VDA アップグレードの編集］ウィンドウで、インストールされている VDA バージョンとアップグレードする VDA バージョンに関する情報が表示されます。
3. スケジュールされたアップグレードを編集するかキャンセルするかを選択します。
    - アップグレードをキャンセルするには、［スケジュールされたアップグレードのキャンセル］をクリックします。注意事項：スケジュールされたアップグレードをキャンセルしても、進行中のアップグレードは強制的に停止されません。
4. ［完了］をクリックしてウィンドウを終了します。

カタログを編集して **VDA** アップグレード設定を構成する

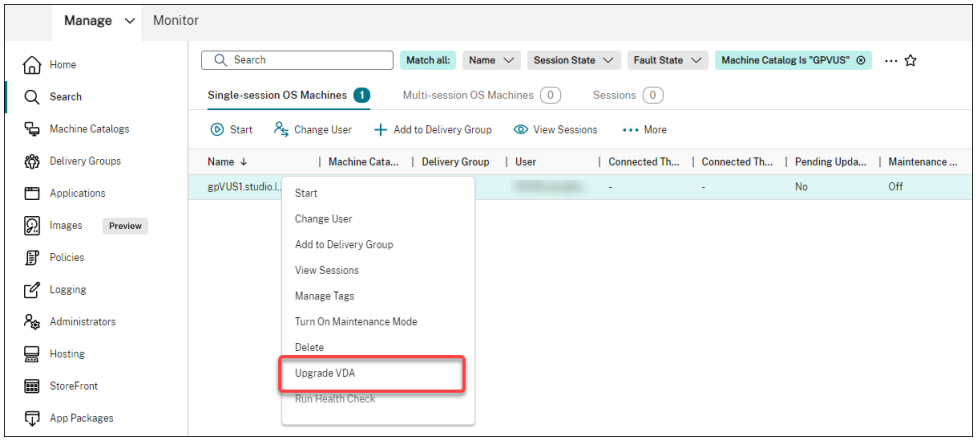
カタログの作成後、カタログを編集して VDA アップグレード設定を構成できます。編集を開始する前に、次のことを考慮してください:

- カタログ内のすべてのマシンが同じ VDA（CR または LTSR）トラック上にあることを確認してください。そうしないと、特定の VDA アップグレードが失敗します。たとえば、［最新の **LTSR VDA**］を選択した場合、CR VDA のアップグレードが失敗します。
- カタログ内の一部のマシンのアップグレードが既に開始されている場合があります。既に進行中のアップグレードは変更できません。進行中のアップグレードは続行されます。まだ開始していないアップグレードは、指定のバージョンにアップグレードされます。

マシンごとに **VDA** をアップグレードする

カタログの VDA アップグレードを有効にした後、カタログの VDA を 1 つずつ、またはバッチで、アップグレードできます。そのためには、次の手順を実行します:

1. ［管理］**>** ［完全な構成］から、［検索］を選択します。
2. 1 つまたは複数のマシンを選択し、コンテキストメニューまたは操作バーの ［**VDA** のアップグレード］を選択します。（右クリックするとコンテキストメニューが表示されます。）



> 注:
>
> - [**VDA** のアップグレード] オプションを使用できるようにするには、選択したマシンが存在するカタログに対して VDA アップグレードを有効にし、それらのマシンに VDA Upgrade Agent がインストールされていることを確認してください。VDA アップグレードを有効にするには、カタログを編集します。
> - アップグレードが展開されている間、マシンはメンテナンスモードになります。アップグレードは、開始まで最大 30 分かかる場合があります。
> - 使用できる VDA アップグレードがない、またはアップグレードが保留中（スケジュール設定済み、進行中、またはアップグレード待機中）のマシンが選択に含まれている場合、それらのマシンのアップグレードはスキップされます。

[検索] ノードで、[**VDA** アップグレード] 列を追加できます。カスタム列を追加する方法については、「表示する列のカスタマイズ」を参照してください。カスタム列は便利です。マシンの VDA アップグレード情報を確認できます。表示される情報には、次のようなものがあります:

- 利用可能: 新しい VDA バージョンが利用可能です。
- スケジュール設定済み: VDA のアップグレードはスケジュール設定済みです。
- 未構成: マシンの VDA アップグレードを有効にしていない場合に表示されます。
- 最新: VDA は最新です。
- 不明: VDA のアップグレードに関する情報はまだ利用できません。

マシンの VDA アップグレードのステータスを表示することもできます。これを行うには、マシンをクリックしてから、[詳細] タブの [**VDA** アップグレード状態] の情報を確認します。表示される情報には、次のようなものがあります:

- 不明: VDA のアップグレードに必要な情報を取得できません。考えられる理由は次のとおりです:
  - VDA がアップグレード期間中に使用されていた。
  - 進行中のアップグレード数が上限の 500 に達した。
  - アップグレード期間中、VDA Upgrade Agentが応答しなかった。エージェントが VDA で実行中で、Citrix DaaS と通信できることを確認してください。

  - アップグレードの検証チェックを実行できない。「VDA のアップグレード要件」を参照してください。

- スケジュール済み：アップグレードスケジュールを設定しました。たとえば、スケジュールを09:00 PM , December 14, 2030開始に設定すると、情報は次のように表示されます：「December 14, 2030 09:00 PM UTCでスケジュール設定済み」。
- アップグレード待機中：アップグレードの待機中、マシンはメンテナンスモードになります（アップグレードを続行できるように、ユーザーがセッションからログアウトしていることを確認してください）。
- 進行中：VDA アップグレードが開始しています。
- アップグレード失敗：VDA をアップグレードしようとして失敗しました。
- 検証失敗：VDA アップグレード設定を検証しようとして失敗しました。
- キャンセル済み：マシンのアップグレードはキャンセルされました。
- 成功：VDA が正常にアップグレードされました。

マシンの推奨操作を実行して、VDA アップグレードの問題をトラブルシューティングすることもできます。これを行うには、マシンをクリックしてから ［トラブルシューティング］ タブに移動します。

特定の VDA アップグレード状態のマシンにすばやくドリルダウンするために、フィルターを使用できます。詳しくは、「［完全な構成］管理インターフェイスでの［検索］の使用」を参照してください。次の考慮事項に注意してください：

- ［**VDA** アップグレード］または ［**VDA** アップグレード状態］フィルターは、次のフィルターでのみ使用できます：［名前］および ［マシンカタログ］。
- ［**VDA** アップグレード］または ［**VDA** アップグレード状態］フィルターを使用すると、右上隅の ［エラー］と［警告］が使用できなくなります。

カタログの構成セットの管理

開始する前に、WEM サービス環境がセットアップされていることを確認します。詳しくは、「Workspace Environment Management サービスの開始」を参照してください。

> 注：
>
> デフォルトで、クラウド管理者、フルアクセス権管理者、またはマシンカタログ管理者の役割がある場合は、カタログの構成セットを管理できます。必要に応じて、役割に構成セットの管理権限を付与することで、構成セットの管理を許可できます。

構成セットへのカタログのバインド

> 重要：
>
> Citrix DaaS と WEM サービスのインスタンスが同じリージョンに存在しない場合、カタログを構成セットにバインドすることはできません。その場合は、WEM サービスを Citrix DaaS と同じリージョンに移行してください。

カタログを構成セットにバインドするには、次の手順を実行します:

1. ［管理］**>** ［完全な構成］から、［マシンカタログ］を選択します。
2. マシンカタログを選択してから、アクションバーで ［構成セットの管理］を選択します。［構成セットの管理］ウィンドウが開きます。
3. カタログをバインドする WEM 構成セットを選択します。

   > 注:
   >
   > 選択した構成セットに WEM の基本構成に関連する設定が含まれていない場合は、［基本設定を構成セットに適用します］が表示されます。基本設定を構成セットに適用するオプションを選択することをお勧めします。

4. ［保存］をクリックして変更を保存します。

別の構成セットへの切り替え

カタログの別の構成セットに切り替えるには、次の手順を実行します:

1. ［管理］**>** ［完全な構成］から、［マシンカタログ］を選択します。
2. マシンカタログを選択してから、アクションバーで ［構成セットの管理］を選択します。［構成セットの管理］ウィンドウが開きます。
3. カタログをバインドする別の WEM 構成セットを選択します。
4. ［保存］をクリックして変更を保存します。

構成セットからのカタログのバインドの解除

構成セットからカタログのバインドを解除するには、次の手順を実行します:

1. ［管理］**>** ［完全な構成］から、［マシンカタログ］を選択します。
2. マシンカタログを選択してから、アクションバーで ［構成セットの管理］を選択します。［構成セットの管理］ウィンドウが開きます。
3. 選択した構成セットの右側にある X アイコンをクリックします。
4. ［保存］をクリックして変更を保存します。

カタログの作成の再試行

> 注:
>
> この機能は MCS カタログにのみ適用されます。

失敗したカタログにはエラーアイコンが表示されます。詳細を確認するには、各カタログの ［トラブルシューティング］タブに移動します。カタログの作成を再試行する前に、次の考慮事項を確認してください:

- まずトラブルシューティング情報を確認してから、問題を解決します。この情報は、見つかった問題について説明し、それらを解決するための推奨事項を提供します。
- オペレーティングシステムとマシンの管理に関連する設定は変更できません。カタログは、元のカタログからこれらの設定を継承します。
- 作成が完了するまでに時間がかかる場合があります。必要に応じて ［進行状況を隠す］を選択して、バックグラウンドで作成を実行します。

カタログの作成を再試行するには、次の手順を実行します：

1. ［管理］**>**［完全な構成］の左側ペインで ［マシンカタログ］を選択します。
2. カタログを選択し、［トラブルシューティング］タブに移動します。
3. 再試行のハイパーリンクをクリックして、カタログの作成を再試行します。
4. 表示されるウィザードで、必要に応じて設定を変更します。変更を加える必要がない場合は、［概要］ページに直接移動できます。
5. 完了したら、［完了］を選択して作成を開始します。

（**Citrix** 以外でプロビジョニングされた **VDA** のみ）登録トークンの生成と管理

Citrix でプロビジョニングされていないマシンに対してトークンベースの登録を選択した場合、マシンカタログごとにトークンを生成し、それを VDA インストール管理者と共有する必要があります。

登録トークンの特徴は次のとおりです：

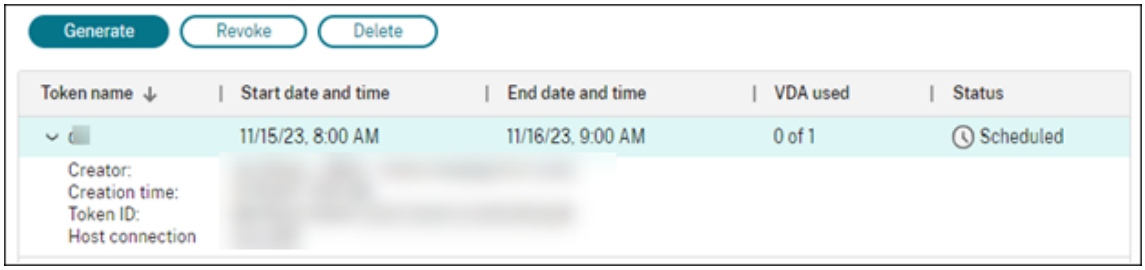
- 登録範囲：1～100 台の VDA マシン
- 有効期間：1 時間～14 日間

完全な構成を使用してカタログのトークンを生成するには、次の手順を実行します：

1. ［完全な構成］**>**［マシンカタログ］で MCS 以外でプロビジョニングされたカタログを見つけます。［マシンの数］列に ［プロビジョニング方法：手動］が表示されています。
2. カタログを右クリックし、［登録トークンを管理する］を選択します。
3. 表示された ［登録トークンを生成する］ページで、次のトークン情報を指定します：
   - トークンの名前を入力します。
   - 有効期間を入力します。期間は 1 時間から 14 日間にする必要があります。トークンは指定された期間のみ有効です。
   - （オプション）トークンに登録された VDA の電源管理のホスト接続を選択します。オプションには、このカタログのゾーンにあるすべてのホスト接続が含まれます。
   - トークンの使用制限を入力します（1～100）。
4. ［生成］をクリックします。

5. 表示された ［トークンが生成されました］ウィンドウでトークンをコピーして安全な場所に保存するか、［ダウンロード］をクリックしてダウンロードフォルダーにダウンロードします。

   トークンのレコードがトークン一覧に表示されます。



6. トークンを VDA インストール管理者と共有します。

   マシンへの VDA およびトークンのインストール方法について詳しくは、「VDA のインストール」を参照してください。

トークンを管理する

トークンを取り消して、VDA 登録に利用できないようにするには、2 つのオプションがあります:

- 取り消し: トークンを取り消しますが、ログ記録のために一覧に保持します。
- 削除: トークンを取り消し、一覧から削除します。

> 注:
>
> 期限切れのトークンは 14 日後に自動的に削除されます。

PowerShell の使用

このセクションでは、PowerShell を使用してカタログを管理する方法について説明します。

- PowerShell を使用して VDA のアップグレードステータスと VDA バージョンを確認する
- マシン名のシーケンス番号の管理
- 1 回限りの再起動スケジュールを有効にする
- イメージへの説明の追加
- OS ディスクのリセット
- アクティブなコンピューターアカウントの ID 情報を修復する
- 既存のマシンカタログのネットワーク設定を変更する
- マシンカタログのバージョンの管理
- 既存のマシンカタログのキャッシュ構成を変更する
- 非マシンプロファイルベースのマシンカタログをマシンプロファイルベースのマシンカタログに変換する
- カタログに関連した警告とエラーの取得
- ハイパーバイザーにアクセスできないマシンの削除

- ローカルファイル共有アクセスによる VDA の更新をサポート

PowerShell を使用して **VDA** のアップグレードステータスと **VDA** バージョンを確認する

`Get-VusCatalog` PowerShell コマンドを使用して、VDA のアップグレードステータスを確認します。カタログ名を`wuhanTestMC1`とした場合、コマンドプロンプトで次のように入力できます:

- `PS C:\> Get-VusCatalog -Name wuhanTestMC1`

```
PS C:\Users\hanw> Get-VusCatalog -Name  wuhanTestMC1


CancelledUpgrades            : 0
DurationInHours              : 8
FailedUpgrades               : 0
InProgressUpgrades           : 0
LastStateChangeInUtc         : 4/22/2022 7:52:51 AM
MaxConcurrentUpgrades        : 100
Name                         : wuhanTestMC1
ProvisioningType             : MCS
ScheduledTimeInUtc           : 4/22/2022 7:20:56 AM
SecurityCheckFailedUpgrades  : 0
SessionSupport               : SingleSession
StateId                      : UpgradeSuccessful
SuccessfulUpgrades           : 1
TotalMachines                : 1
Uid                          : 12
UpgradeState                 : UpgradeAvailable
UpgradeType                  : CR
UpgradeVersion               : 2112.0.0.32068
Uuid                         : 339e7bce-271b-4c37-9a1c-bce287008b65
```

この例では、`UpgradeState`が`UpgradeAvailable`であるため、カタログに対して VDA のアップグレードが有効になっていることを意味します。`StateId`は`UpgradeSuccessful`であるため、カタログが 2112.0.0.32068（`UpgradeVersion`）に正常にアップグレードされたことを意味します。

`Get-BrokerMachine` PowerShell コマンドを使用して、現在の VDA のバージョンを取得します。


```
SessionProtocol              :
SessionSecureIcaActive       :
SessionSmartAccessTags       :
SessionStartTime             :
SessionState                 :
SessionStateChangeTime       :
SessionSupport               : MultiSession
SessionType                  :
SessionUid                   :
SessionUserName              :
SessionUserSID               :
SessionsEstablished          : 0
SessionsPending              : 0
SummaryState                 : Unregistered
SupportedPowerActions        : {}
Tags                         : {}
UUID                         : 9c0c4623-a4dc-44f9-ae4b-54c86cc76a7f
Uid                          : 4
VMToolsState                 : NotPresent
WillShutdownAfterUse         : False
WillShutdownAfterUseReason   : None
WindowsConnectionSetting     : LogonEnabled
ZoneHealthy                  : False
ZoneName                     : My Resource Location
ZoneUid                      : ae0366c2-3001-459d-89ff-0b159c9d436d

AgentVersion                 : 2112.0.0.32068
AllocationType               : Static
ApplicationsInUse            : {}
AssignedClientName           :
AssignedIPAddress            :
AssignedUserSIDs             : {}
AssociatedTenantId           :
AssociatedUserFullNames      : {}
AssociatedUserNames          : {}
AssociatedUserSIDs           : {}
AssociatedUserUPNs           : {}
AzureADJoinedMode            : NotAadJoined
BrowserName                  :
Capabilities                 : {}
CatalogName                  : wuhanTestMC1
CatalogUUID                  : 339e7bce-271b-4c37-9a1c-bce287008b65
CatalogUid                   : 12
CbpVersion                   :
ColorDepth                   :
ControllerDNSName            :
DNSName                      : wuhanVUSTest02.WHCloud.Internal
DeliveryType                 :
Description                  :
DesktopConditions            : {}
```

`Get-VusAvailableVdaVersion` PowerShell コマンドを使用して、最新の VDA のバージョンを取得します。

```
PS C:\Users\hanw> Get-VusAvailableVdaVersion

UpgradeType Version
----------- -------
         CR 2203.0.0.33220
       LTSR 2203.0.0.33220
```


マシン名のシーケンス番号の管理

MCS を使用して展開されるマシンのシーケンス番号を PowerShell コマンドでカスタマイズするには、次の手順を実行します:

1. Delivery Controller で管理者として Powershell を開きます。
2. コマンド`asnp citrix*`を実行して Citrix の PowerShell モジュールをロードします。
3. 次のコマンドを実行して、カタログの ID プールに当初含まれるマシンの数（StartCount）を確認します:

```
Get-AcctIdentityPool -IdentityPoolName xxx
<!--NeedCopy-->
```

   `IdentityPoolName`はカタログ名です。

4. StartCount を別の値（X）に設定するには、StartCount に X を指定し、次のコマンドを実行します:

```
Set-AcctIdentityPool -IdentityPoolName xxx -StartCount X
<!--NeedCopy-->
```

5. 必要な数のマシンが作成されるように、それらのマシンをカタログに追加します。
6. マシンを作成したら、次のコマンドを実行して StartCount を元の値 Y に戻します:

```
Set-AcctIdentityPool -IdentityPoolName xxx -StartCount Y
<!--NeedCopy-->
```

1 回限りの再起動スケジュールを有効にする

PowerShell を使用して 1 回限りの再起動スケジュールを有効にする場合は、以下の`BrokerCatalogRebootSchedule`の PowerShell コマンドを使用して、再起動スケジュールを作成、変更、および削除します:

- `Get-BrokerCatalogRebootSchedule`
- `New-BrokerCatalogRebootSchedule`
- `Set-BrokerCatalogRebootSchedule`
- `Remove-BrokerCatalogRebootSchedule`
- `Rename-BrokerCatalogRebootSchedule`

例:

- **BankTellers** という名前のカタログ内の VM の再起動スケジュールを作成して、2022 年 2 月 3 日の午前 2 時から午前 4 時の間に開始します。

```
 New-BrokerCatalogRebootSchedule -Name BankTellers
 -CatalogName BankTellers
 -StartDate "2022-02-03"
 -StartTime "02:00"
 -Enabled $true
```



```
-RebootDuration 120
<!--NeedCopy-->
```

- UID 17 を持つカタログ内の VM の再起動スケジュールを作成して、2022 年 2 月 3 日の午前 1 時から午前 5 時の間に開始します。再起動の 10 分前に、各 VM は、すべてのユーザーセッションで「**WARNING: Reboot pending**（警告：再起動保留中）」というタイトルのメッセージボックスと、「**Save your work**（作業を保存してください）」というメッセージを表示するように設定されています。

```
New-BrokerCatalogRebootSchedule
-Name 'Update reboot'
-CatalogUid 17
-StartDate "2022-02-03"
-StartTime "01:00" -Enabled $true -RebootDuration 240
-WarningTitle "WARNING: Reboot pending"
-WarningMessage "Save your work" -WarningDuration 10
<!--NeedCopy-->
```

- **Old Name** という名前のカタログ再起動スケジュールを **New Name** という名前に変更します。

```
Rename-BrokerCatalogRebootSchedule -Name "Old Name" -NewName "New
    Name"
<!--NeedCopy-->
```

- UID 1 のすべてのカタログ再起動スケジュールを表示し、UID 1 のカタログ再起動スケジュールの名前を **New Name** に変更します。

```
Get-BrokerCatalogRebootSchedule -Uid 1 | Rename-
   BrokerCatalogRebootSchedule -NewName "New Name" -PassThru
<!--NeedCopy-->
```

- **Accounting** という名前のカタログ再起動スケジュールを設定して、各仮想マシンの再起動の 10 分前に「**WARNING: Reboot pending**（警告：再起動保留中）」というタイトルのメッセージと、「**Save your work**（作業を保存してください）」というメッセージを表示します。このメッセージは、その VM のすべてのユーザーセッションに表示されます。

```
Set-BrokerCatalogRebootSchedule -Name Accounting
-WarningMessage "Save your work"
-WarningDuration 10 -WarningTitle "WARNING: Reboot pending"
<!--NeedCopy-->
```

- 無効になっているすべての再起動スケジュールを表示し、有効にします。

```
Get-BrokerCatalogRebootSchedule -Enabled $false | Set-
   BrokerCatalogRebootSchedule -Enabled $true
<!--NeedCopy-->
```

- UID 17 でカタログ再起動スケジュールを設定して、「**Rebooting in %m% minutes**（あと%m% 分で再起動）」というメッセージを表示します（各 VM の再起動の 15 分、10 分、5 分前）。


```
Set-BrokerCatalogRebootSchedule 17 -WarningMessage "Rebooting in
    %m% minutes." -WarningDuration 15 -WarningRepeatInterval 5
<!--NeedCopy-->
```

- **MyCatalog** という名前のカタログのタイムゾーンを構成します。

```
Set-BrokerCatalog -Name "MyCatalog" -TimeZone <TimeZone>
<!--NeedCopy-->
```

イメージへの説明の追加

マシンカタログイメージの更新に関連した変更に関する説明を追加できます。カタログを作成するとき、またはカタログの既存のマスターイメージを更新するときに、この機能を使用して説明を追加します。カタログ内の各マスターイメージの情報を表示することもできます。この機能は、カタログで使用されるマスターイメージを更新するときに、管理者が説明ラベル（*Office 365* インストール済みなど）を追加するのに役立ちます。次のコマンドを使用して、イメージの説明を追加または表示します:

- `NewProvScheme`。新しいパラメーター`masterImageNote`を使用すると、イメージにメモを追加できます。例:

```
C:\PS>New-ProvScheme -ProvisioningSchemeName XenPS -HostingUnitName
    XenHu -IdentityPoolName idPool1 -MasterImageVM XDHyp:\HostingUnits\
    XenHU\Base.vm\Base.snapshot -MasterImageNote "Office365 installed"
<!--NeedCopy-->
```

- `Publish-ProvMasterVMImage`。このパラメーターを使用して、メモを公開します。例:

```
C:\PS>Publish-ProvMasterVMImage -ProvisioningSchemeName MyScheme -
    MasterImageVM XDHyp:\HostingUnits\HostUnit1\RhoneCC_baseXP.vm\base.
    snapshot -MasterImageNote "Visual Studio 2019 installed"
<!--NeedCopy-->
```

- `Get-ProvSchemeMasterVMImageHistory`。各イメージの情報を表示します。例:

```
C:\PS>Get-ProvSchemeMasterVMImageHistory -ProvisioningSchemeName
    MyScheme -Showall

VMImageHistoryUid : 3cba3a75-89cd-4868-989b-27feb378fec5

ProvisioningSchemeUid : 7585f0de-192e-4847-a6d8-22713c3a2f42

ProvisioningSchemeName : MyScheme

MasterImageVM : /Base.vm/base.snapshot

Date : 17/05/2021 09:27:50

MasterImageNote : Office365 installed
```



```
<!--NeedCopy-->
```

OS ディスクのリセット

PowerShell コマンドReset-ProvVMDiskを使用して、MCS で作成されたマシンカタログ内の永続的な VM の OS ディスクをリセットします。この機能は現時点では Azure、Google Cloud、SCVMM、VMware、および XenServer の仮想化環境に適用できます。

PowerShell コマンドを正常に実行するには、次のことを確認してください:

- ターゲット VM が永続的な MCS カタログにある。
- MCS マシンカタログが正常に機能している。これは、プロビジョニングスキームとホストが存在し、プロビジョニングスキームに正しいエントリがあることを意味します。
- ハイパーバイザーはメンテナンスモードではない。
- ターゲット VM の電源がオフで、メンテナンスモードになっている。

OS ディスクをリセットするには、以下の手順を実行します:

1. **PowerShell** ウィンドウを開きます。
2. asnp citrix* を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. 次のいずれかの方法で、PowerShell コマンドReset-ProvVMDiskを実行します:
   - VM の一覧をコンマ区切りの一覧として指定し、各 VM でリセットを実行します:

     ```
     Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName ("abc"
         ,"def") -OS
     <!--NeedCopy-->
     ```

   - Get-ProvVMコマンドからの出力として VM の一覧を指定し、各 VM でリセットを実行します:

     ```
     (Get-ProvVM -ProvisioningSchemeName "xxx") | Reset-ProvVMDisk
         "abc" -OS
     <!--NeedCopy-->
     ```

   - 単一の VM を名前で指定します:

     ```
     Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
         -OS
     <!--NeedCopy-->
     ```

   - Get-ProvVMコマンドによって返される VM ごとに個別のリセットタスクを作成します。これは、VM ごとのハイパーバイザー機能チェック、接続チェックなど、各タスクが同じ冗長チェックを実行するため、効率が低下します。

     ```
     Get-ProvVM -ProvisioningSchemeName "xxx" | Reset-ProvVMDisk -
         ProvisioningSchemeName "xxx" -OS
     <!--NeedCopy-->
     ```


4. リセットする VM を一覧表示する確認プロンプトと、回復不能な操作であるという警告メッセージが表示されます。回答を入力せずに **Enter** キーを押すと、それ以上のアクションは実行されません。

   PowerShell コマンド`-WhatIf`を実行して、実行するアクションを出力し、アクションを実行せずに終了できます。

   次のいずれかの方法を使用して、確認プロンプトを回避することもできます:

   - `-Force`パラメーターを指定します:

     ```
     Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
         -OS -Force
     <!--NeedCopy-->
     ```

   - `-Confirm:$false`パラメーターを指定します:

     ```
     Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
         -OS -Confirm:$false
     <!--NeedCopy-->
     ```

   - `Reset-ProvVMDisk`を実行する前に、`$ConfirmPreference`を None に変更します:

     ```
     PS C:\Windows\system32> $ConfirmPreference='None'
     PS C:\Windows\system32> $ConfirmPreference
     None
     PS C:\Windows\system32> Reset-ProvVMDisk -
         ProvisioningSchemeName "xxx" -VMName "abc" -OS
     <!--NeedCopy-->
     ```

   > 注:
   >
   > リセットプロセスが完了するまで、VM のメンテナンスモードを解除したり、電源を入れたりしないでください。

5. `Reset-ProvVMDisk`コマンドで返されたタスクのステータスを取得するには、`Get-ProvTask`を実行します。

アクティブなコンピューターアカウントの **ID** 情報を修復する

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

> 注:
>
> 現在、この機能は Azure、VMware 仮想化環境でのみサポートされています。

条件

ID ディスクを正常にリセットするには、次のことを確認してください:

- VM をオフにしてメンテナンスモードに設定する
- PowerShell コマンドにパラメーター「-OS」を含めない

ID 情報をリセットする

ID 情報をリセットするには:

1. **PowerShell** ウィンドウを開きます。
2. `asnp citrix*`を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. ID 情報をリセットします。

   - マシンのパスワードと信頼キーのみをリセットするには、次のコマンドを次の順序で実行します:

     ```
     1  Repair-AcctIdentity -IdentityAccountName TEST\VM1 -
            PrivilegedUserName TEST\admin1 -PrivilegedUserPassword
            $password -Target IdentityInfo
     2  <!--NeedCopy-->
     ```

     コマンドで使用されるパラメーターの説明は次のとおりです:

     - `IdentityAccountName`: 修復が必要な ID アカウントの名前。
     - `PrivilegedUserName`: ID プロバイダー（AD または Azure AD）に対する書き込み権限を持つユーザーアカウント。
     - `PrivilegedUserPassword`: PrivilegedUserName のパスワード。
     - `Target`: 修復作業のターゲット。これには、アカウントのパスワード/信頼キーを修復するための IdentityInfo、および Hybrid Azure AD に参加しているマシンの ID のユーザー証明書属性を修復するための UserCertificate があります。

     ```
     1  Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMname <name
            > -Identity -ResetIdentityInfo
     2  <!--NeedCopy-->
     ```

     `ResetIdentityInfo`パラメーターは以下をリセットします:

     - パスワードと信頼キー: VM が AD ドメインに参加している場合（Citrix DaaS のみ）
     - 信頼キーのみ: VM が AD ドメインに参加していない場合（Citrix DaaS のみ）
     - パスワードのみ: VM が AD ドメインに参加している場合（Citrix Virtual Apps and Desktops のみ）

   - ID ディスクのすべての構成をリセットするには、次のコマンドを次の順序で実行します:


```
Repair-AcctIdentity -IdentityAccountName TEST\VM1 -
    PrivilegedUserName TEST\admin1 -PrivilegedUserPassword
    $password -Target IdentityInfo
<!--NeedCopy-->
```

```
Reset-ProvVMDisk ProvisioningSchemeName <name> -VMName <name>
     -Identity
<!--NeedCopy-->
```

4. 「**y**」と入力してアクションを確認します。-Forceパラメーターを使用して確認プロンプトをスキップすることもできます。例:

```
Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMName <name> -
    Identity -Force
<!--NeedCopy-->
```

5. Get-ProvVM -ProvisioningSchemeName <name -VMName <name>を実行して、更新された ID ディスク設定を確認します。ID ディスクの属性（IdentityDiskIdなど）を更新する必要があります。StorageIdとIdentityDiskIndexは変更しないでください。

既存のマシンカタログのネットワーク設定を変更する

新しい仮想マシンが新しいサブネットワーク上に作成されるように、既存のマシンカタログのネットワーク設定を変更できます。Set-ProvSchemeコマンドのパラメーター-NetworkMappingを使用して、ネットワーク設定を変更します。

既存のプロビジョニングスキームのネットワーク設定を変更するには、以下を実行します:

1. PowerShell ウィンドウで、コマンドasnp citrix*を実行して PowerShell モジュールをロードします。
2. (Get-Provscheme -ProvisioningSchemeName "name").NetworkMapsを実行して、変更するネットワークパスにアクセスします。
3. 新しいネットワーク設定に変数を割り当てます。例:

```
$NewNetworkMap = @{
 "0"= "XDHYP:\HostingUnits\MyNetworks\Network 0.network" }

<!--NeedCopy-->
```

4. Set-ProvScheme -ProvisioningSchemeName "name"-NetworkMapping $NewNetworkMapを実行します。
5. (Get-Provscheme -ProvisioningSchemeName "name").NetworkMapsを実行して、既存のプロビジョニングスキームの新しいネットワーク設定を確認します。

マシンカタログのバージョンの管理

MCS マシンカタログが`Set-ProvScheme`コマンドで更新されると、現在の設定がバージョンとして保存されます。その後、PowerShell コマンドを使用してさまざまなバージョンのマシンカタログを管理できます。次の操作を実行できます:

- マシンカタログのバージョンの一覧を表示する
- 以前のバージョンを使用してマシンカタログを更新する
- そのマシンカタログの VM で使用されていないバージョンを手動で削除する
- マシンカタログによって保持されるバージョンの最大数を変更する（デフォルトは 99）

バージョンには、マシンカタログの次の情報が含まれます:

- VMCpuCount
- VMMemoryMB
- CustomProperties
- ServiceOffering
- MachineProfile
- NetworkMapping
- SecurityGroup

（例として提供された）次のコマンドを実行して、マシンカタログのさまざまなバージョンを管理します。

- マシンカタログのさまざまなバージョンの構成の詳細を表示する場合:

```
1 Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog
2 <!--NeedCopy-->
```

- マシンカタログの特定のバージョンの構成の詳細を表示する場合:

```
1 Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -
     Version 2
2 <!--NeedCopy-->
```

- マシンカタログに関連付けられているバージョンの合計数を確認する場合:

  ‘‘‘

  (Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog).Count

- 以前のバージョンを使用してマシンカタログを更新する場合:

```
1 Set-ProvScheme -ProvisioningSchemeName AzureCatalog -Version 2
2 <!--NeedCopy-->
```

- そのマシンカタログの VM で使用されていないバージョンを手動で削除する場合:

```
1 Remove-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -
     Version 3
2 <!--NeedCopy-->
```


- マシンカタログで保持されるバージョンの最大数を設定する場合（デフォルトは 99）。この設定はすべてのカタログに適用されます。たとえば、この場合、MCS でプロビジョニングされたすべてのカタログに対して最大 15 のバージョンが保持されます。

```
Set-ProvServiceConfigurationData -Name "MaxProvSchemeVersions" -
    Value 15
<!--NeedCopy-->
```

バージョン数が最大バージョン数に達した場合、マシンカタログ内のいずれかの VM で古いバージョンが使用されていると、新しいバージョンを作成できなくなります。その場合は、次のいずれかを実行します：

- マシンカタログで保持されるバージョンの最大数の上限を増やします。
- 古いバージョンの一部の VM を更新して、それらの古いバージョンがどの VM からも参照されなくなり、削除できるようにします。

既存のマシンカタログのキャッシュ構成を変更する

MCSIO を有効にして非永続カタログを作成した後、`Set-ProvScheme`コマンドを使用して次のパラメーターを変更できます：

- WriteBackCacheMemorySize
- WriteBackCacheDiskSize

この機能は現在、以下に適用されます：

- GCP および Microsoft Azure 環境、および
- MCSIO が有効になっている非永続カタログ

要件

キャッシュ構成を変更するための要件は次のとおりです：

- VDA の最新バージョン（2308 以降）に更新します。
- 既存のマシンカタログのパラメーター`UseWriteBackCache`を有効にします。`UseWriteBackCache`を有効にしてマシンカタログを作成するには、`New-ProvScheme`を使用します。例：

```
New-ProvScheme -ProvisioningSchemeName $CatalogName -
    HostingUnitUid $HostingUnitUid `
-IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `
-MasterImageVM $MasterImage `
-ServiceOffering $ServiceOffering `
-NetworkMap $NetworkMap `
-SecurityGroup $SecurityGroup `
-UseWriteBackCache -WriteBackCacheDiskSize 8
<!--NeedCopy-->
```


キャッシュ構成を変更する

Set-ProvSchemeコマンドを実行します。例:

```
Set-ProvScheme -ProvisioningSchemeName $provScheme.
    ProvisioningSchemeName -WriteBackCacheDisk32 -
    WriteBackCacheMemorySize 128
<!--NeedCopy-->
```

> 注:
>
> - 少なくとも 1GB のキャッシュディスクストレージが必要であるため、WriteBackCacheDiskSizeの値は 0 より大きい必要があります。
> - WriteBackCacheMemorySizeの値は、マシンカタログのメモリサイズより小さくなければなりません。
> - これらの変更は、変更後にカタログに追加された新しい VM にのみ影響します。既存の VM はこれらの変更の影響を受けません。

非マシンプロファイルベースのマシンカタログをマシンプロファイルベースのマシンカタログに変換する

VM、テンプレートスペック（Azure の場合）、または起動テンプレート（AWS の場合）をマシンプロファイルの入力に使用して、非マシンプロファイルベースのマシンカタログをマシンプロファイルベースのマシンカタログに変換できます。カタログに追加された新しい VM は、マシンプロファイルからプロパティ値を取得します。

> 注:
>
> 既存のマシンプロファイルベースのマシンカタログを、非マシンプロファイルベースのマシンカタログに変更することはできません。

これを行うには、以下の手順に従います:

1. VM を使用し、マシンプロファイルを使用せずに、永続的または非永続的なマシンカタログを作成します。
2. **PowerShell** ウィンドウを開きます。
3. Set-ProvSchemeコマンドを実行して、マシンプロファイルのプロパティ値をマシンカタログに追加された新しい VM に適用します。例:

   - Azure の場合:

     ```
     Set-ProvScheme = Set-ProvScheme -ProvisioningSchemeName xxxx
         -MachineProfile XDHyp:\HostingUnits<HostingUnitName>\
         machineprofile.folder<ResourceGroupName><TemplateSpecName
         ><VersionName>
     <!--NeedCopy-->
     ```

   - AWS の場合:


```
Set-ProvScheme = Set-ProvScheme -ProvisioningSchemeName xxxx
    -MachineProfile "XDHyp:\HostingUnits<hosting-unit><launch-
    template>.launchtemplate<launch-template-version>.
    launchtemplateversion"
<!--NeedCopy-->
```

カタログに関連した警告とエラーの取得

MCS カタログの問題を把握して修正するために、エラーと警告の履歴を取得することができます。

PowerShell コマンドを使用すると、次のことができます:

- エラーまたは警告の一覧を取得する
- 警告ステータスを **New**（新規）から **Acknowledged**（確認済み）に変更する
- エラーまたは警告を削除する

PowerShell コマンドを実行するには:

1. PowerShell ウィンドウを開きます。
2. `asnp citrix*`を実行し、Citrix 固有の PowerShell モジュールをロードします。

エラーと警告の一覧を取得するには:

`Get-ProvOperationEvent`コマンドを実行します。

- パラメーターなし: すべてのエラーと警告を取得します
- `LinkedObjectType`および`LinkedObjectUid`パラメーターあり: 特定のプロビジョニングスキームに関連付けられたすべてのエラーと警告を取得します
- `EventId`パラメーターあり: このイベント ID に一致する特定のエラーまたは警告を取得します
- `Filter`パラメーターあり: カスタマイズされたフィルターによってエラーまたは警告を取得します

エラーまたは警告の状態を **New**（新規）から **Acknowledged**（確認済み）に変更するには:

`Confirm-ProvOperationEvent`コマンドを実行します。

- `EventId`パラメーターあり: このイベント ID に一致する特定のエラーまたは警告の状態を設定します。`Get-ProvOperationEvent`コマンドからの出力として特定のエラーまたは警告の`EventId`を取得できます
- `LinkedObjectType`および`LinkedObjectUid`パラメーターあり: 特定のプロビジョニングスキームに関連付けられたすべてのエラーと警告の状態を設定します
- `All`パラメーターあり: すべてのエラーと警告の状態を **Acknowledged**（確認済み）に設定します

エラーまたは警告を削除するには:

`Remove-ProvOperationEvent`コマンドを実行します。

- `EventId`パラメーターあり：このイベント ID に一致する特定のエラーまたは警告を削除します。`Get-ProvOperationEvent`コマンドからの出力として特定のエラーまたは警告の`EventId`を取得できます
- `LinkedObjectType`および`LinkedObjectUid`パラメーターあり：特定のプロビジョニングスキームに関連付けられたすべてのエラーと警告を削除します
- `All`パラメーターあり：すべてのエラーと警告を削除します

詳しくは、「Citrix PowerShell SDK」を参照してください。

ハイパーバイザーにアクセスできないマシンの削除

VM またはプロビジョニングスキームを削除する場合、MCS は、削除オプションに含まれるリソースが MCS によって追跡または識別されなくなるように、VM から（場合によってはベース ディスクからも）タグを削除する必要があります。ただし、これらのリソースの一部は、ハイパーバイザーを介してのみアクセスできます。ハイパーバイザーにアクセスできない場合は、`Remove-ProvVM`PowerShell の`PurgeDBOnly`オプションを使用して、VM、基本ディスク、ACG 内のイメージなどの VM リソースオブジェクトをデータベースから削除します。

このオプションは以下で有効になります：

- サポートされるすべてのハイパーバイザー
- 永続的および非永続的な VM

制限事項

コマンド-PurgeDBOnly と-ForgetVM を同時に使用することはできません。

PurgeDBOnly コマンドを使用する

PowerShell コマンド`Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -ForgetVM`を実行すると、次のシナリオで削除操作が失敗することがあります：

- ホスト接続がメンテナンス モードである
- 無効な資格情報
- 認証エラー
- 不正な操作
- ハイパーバイザーに到達できない

> 注：
>
> Remove-provVM -ForgetVM は、永続的な VM のみを対象としています。一覧にあるいずれかの VM が非永続的である場合、操作は失敗します。

ハイパーバイザーに到達できないために操作が失敗すると、次のプロンプトが表示されます:

```
Try to use -PurgeDBOnly option to clean DDC database.
```

`Remove-ProvVM`PowerShell コマンドで`-PurgeDBOnly`オプションを使用して、VM のリファレンスを MCS データベースから削除します。例:

```
Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -
PurgeDBOnly
```

ローカルファイル共有アクセスによる **VDA** の更新をサポート

PowerShell コマンドレットを使用して VDA インストーラーの場所を指定すると、各 VDA が Citrix Managed Azure CDN から新しい VDA インストーラーを取得できるようにするためのネットワーク規則を提供する手間が軽減されます。

PowerShell コマンドレット

New-VusCatalogSchedule および **New-VusMachineUpgrade** コマンドレットに 2 つの新しいオプションのパラメーターが追加され、ローカルファイル共有からインストーラーを使用できるようになりました

- **VdaWorkstationPackageUri** - ワークステーション OS VDA インストーラーへの UNC パスを指定します
- **VdaServerPackageUri** - サーバー OS VDA インストーラーへの UNC パスを指定します

前提条件

- VDA Upgrade Agent をバージョン 7.40.0.35 以降にアップグレードします（VDA インストーラーバージョン 2311 以降を使用）
- Virtual Apps and Desktops Remote PowerShell SDK バージョン 7.40 以降（2024 年 1 月 10 日以降にリリース）
- リモート PowerShell SDK バージョン 7.42 以降（2024 年 2 月 16 日以降にリリース）

ファイル共有権限を設定する方法

VDA インストーラーパッケージを含むネットワーク共有には、ローカルシステム（NT AUTHORITY\SYSTEM プリンシパル）として実行される VDA Upgrade Agent サービスの読み取りアクセス権が必要です。

- ドメイン参加ファイルの共有権限

  VDA マシンがドメイン参加の場合、ローカル システムアカウント（VUA はローカルシステムとして実行されます）は、ネットワーク共有にアクセスするときにコンピューターの資格情報を使用します。

  ドメインコンピューターに読み取りアクセスを許可することで、最小限の権限を設定できます。

1. ネットワーク上でファイルを共有するユーザーを選択します。
2. ［共有の詳細設定］をクリックして、［ファイルとプリンターの共有］をオンにします。

- ドメイン非参加ファイルの共有権限

  VDA マシンがドメイン非参加の場合、ローカルシステムアカウント（VUA はローカルシステムとして実行されます）は、ネットワーク共有にアクセスするときに **ANONYMOUS LOGON** を使用します。

  1. 共有フォルダーを選択します。
  2. パスワード保護を無効にします。
     a) フォルダーの ［プロパティ］に移動します。
     b) ［ネットワークと共有センター］を選択します。
     c) ［パスワード保護共有］をオフにします。
  3. 共有権限を付与するには、［詳細な共有］をクリックします。
     a) ［アクセス許可］を選択します。
     b) **ANONYMOUS LOGON** に読み取り共有権限を付与します。
  4. フォルダーの権限を付与するには ［セキュリティ］タブを選択します
     a) 共有フォルダーに権限を追加するには ［編集］をクリックします
     b) **ANONYMOUS LOGON** にフォルダー権限を付与する共有フォルダーを選択します。
  5. ［詳細設定］をクリックして、［ファイルとプリンターの共有］をオンにします。
  6. 共有フォルダー名をネットワークアクセスセキュリティポリシーに追加します。

  > 注:
  >
  > 変更をすぐに有効にするには、マシンを再起動してください。

ローカルファイル共有から **VDA** を更新する

1. VDA インストーラーをダウンロードし、共有ファイルに格納します。

   > 注:
   >
   > 仮想アップグレードサービスでは、現在のリリーストラックまたは LTSR トラックのいずれかを選択できます。
   >
   > 例：マシンカタログが現在のリリース（2311）に設定されており、VDA バージョンが 2305 の場合、VDA をバージョン 2311 にアップグレードする必要があります。

   a) 当社 Web サイトのダウンロードページに移動します。
   b) 製品で **Citrix Virtual Apps and Desktops** を選択します。
   c) **Citrix Virtual Apps and Desktops 7 2311, All Editions** を選択します。
   d) 製品 **ISO** に含まれており、個別に展開可能なパッケージも用意されているコンポーネントから VDA インストーラーを選択します。

2. カタログの種類に基づいて、関連する VDA インストーラーを選択します。

   - カタログの種類がマルチセッションの場合は、マルチセッション **OS VDA** インストーラーをダウンロードします
   - カタログの種類がシングルセッションの場合は、シングルセッション **OS VDA** インストーラーをダウンロードします
   - カタログの種類がリモート **PC** アクセスの場合は、シングルセッション **OS** コアサービス **VDA** インストーラーをダウンロードします

> 注:
>
> ファイル共有インストーラーのバージョンは、VUS によってクラウドに公開された最新のインストーラーバージョンと完全に一致する必要があります。

トラブルシューティング

- マシンの状態が「`Power State Unknown`」の場合は、CTX131267を参照してください。
- 継続的に不明な電源状態を示す仮想マシンを修正するには、How to fix VMs that continuously show an unknown power stateを参照してください。
- Cloud Connector が正常に動作していない場合、MCS プロビジョニング操作（カタログの更新など）は通常よりも時間がかかり、管理コンソールのパフォーマンスが大幅に低下します。

次の手順

特定のハイパーバイザーカタログの管理については、次を参照してください:

- AWS カタログの管理
- Google Cloud Platform カタログの管理
- Microsoft Azure カタログの管理
- Microsoft System Center Virtual Machine Manager カタログの管理
- VMware カタログの管理
- XenServer カタログの管理

AWS カタログの管理

January 25, 2024

「マシンカタログの管理」では、マシンカタログを管理するウィザードについて説明します。以下の情報は、AWS クラウド環境に固有の詳細について説明しています。

> 注:
>
> AWS カタログを管理する前に、AWS カタログの作成を完了する必要があります。「AWS カタログの作成」を参照してください。

タグの削除

カタログまたは 仮想マシンを作成すると、次のリソースにタグが作成されます:

- 仮想マシン
- ルートディスクボリューム
- ID ディスクボリューム
- Elastic Network Interface（ENI）
- ルートディスクイメージ（AMI）
- 起動テンプレート
- AMI またはルートディスクのスナップショット

仮想マシンとマシンカタログを Citrix データベースから削除し、Citrix 作成タグを削除できます。以下を使用できます:

- `Remove-ProvVM`を`ForgetVM`パラメーターとともに使用して、マシンカタログの単一の仮想マシンまたは仮想マシンの一覧から仮想マシンと Citrix 作成タグを削除します。

  > 注:
  >
  > `ForgetVM`パラメーターを使用すると、VM は Citrix のプロビジョニングスキームデータベースからは削除されますが、ハイパーバイザー内には残り続けます。

- `Remove-ProvScheme`を`ForgetVM`パラメーターとともに使用して、Citrix データベースからマシンカタログを削除し、マシンカタログからタグを削除します。

これを行うには、以下の手順に従います:

1. **PowerShell** ウィンドウを開きます。
2. `asnp citrix*`を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. 仮想マシンを削除する前に、仮想マシンのロックを解除します。例:

   ```
   1 Unlock-ProvVM -ProvisioningSchemeName "<name>" -VMID "<id"
   2 <!--NeedCopy-->
   ```

4. 次のコマンドのいずれかを実行して、リソースから仮想マシン、マシンカタログ、および Citrix 作成タグを削除します。

   - `Remove-ProvVM`を`ForgetVM`とともに実行して、Citrix データベースから仮想マシンを削除し、仮想マシンから Citrix 作成タグを削除します。例:


```
Remove-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name
    >" -ForgetVM
<!--NeedCopy-->
```

- Remove-ProvSchemeを実行して、Citrix データベースからマシンカタログを削除し、マシンカタログからリソースを削除します。例:

```
Run Remove-ProvScheme -ProvisioningSchemeName "<name>" -
    ForgetVM
<!--NeedCopy-->
```

5. 仮想マシンが Delivery Controller からは削除されているが、ハイパーバイザーからは削除されていないことを確認します。

   a) Get-ProvVM -ProvisioningSchemeName "<name>"-VMName "<name>"を実行します。これによって何も返されないことが必要です。

   b) AWS EC2 コンソールに移動します。仮想マシンが表示されるが、Citrix 作成タグは削除されている必要があります。次のリソースの Citrix 作成タグが削除されます:

      - 仮想マシン
      - ルートディスクボリューム
      - ID ディスクボリューム
      - ENI

6. マシンカタログを削除する場合は、カタログが Delivery Controller から削除されていることを確認してください。

   a) Get-ProvScheme -ProvisioningSchemeName "forgetvmdemo"を実行します。これによって、エラーが返される必要があります。

   b) AWS EC2 コンソールで、次のリソースが削除されていることを確認します。

      - ルートディスクイメージ（AMI）
      - 起動テンプレート
      - AMI またはルートディスクのスナップショット

MCS によって作成されたリソースの特定

以下は、MCS が AWS プラットフォームのリソースに追加するタグです。表のタグは、「” キー” :” 値”」として表示されます。

リソース名	タグ
ID ディスク	“Name” : “VMName_IdentityDisk”

リソース名	タグ
	“XdConfig”： “XdProvisioned=true” “CitrixProvisioningSchemeId”： “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
イメージ	“XdConfig”： “XdProvisioned=true” “CitrixProvisioningSchemeId”： “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
ENI	“Description”： “XD Nic” “XdConfig”： “XdProvisioned=true” “CitrixProvisioningSchemeId”： “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
OS ディスク	“Name”： “VMName_rootDisk” “XdConfig”： “XdProvisioned=True” “CitrixProvisioningSchemeId”： “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
PrepVM	[when AwsCaptureInstanceProperties = true] “Citrix Resource”： “” [when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] “CitrixOperationalResource”： “” “Name”： “Preparation - CatalogName - xxxxxxxxxx” “XdConfig”： “XdProvisioned=true” “CitrixProvisioningSchemeId”： “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
公開されたスナップショット	[when AwsCaptureInstanceProperties = true] “Citrix Resource”： “” [when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] “CitrixOperationalResource”： “” “XdConfig”： “XdProvisioned=true”
テンプレート	ボリュームワーカー AMI のスナップショットでない場合は、”CitrixProvisioningSchemeId”： “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [when AwsCaptureInstanceProperties = true] “XdConfig”： “XdProvisioned=true”

リソース名	タグ
カタログ内の VM	[when AwsCaptureInstanceProperties = true] “CitrixProvisioningSchemeId” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [when AwsCaptureInstanceProperties = true] “CitrixResource” : “” [when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] “CitrixOperationalResource” : “” “XdConfig” : “XdProvisioned=true”
ボリュームワーカー AMI	“CitrixProvisioningSchemeId” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [when AwsCaptureInstanceProperties = true] “CitrixResource” : “” [when AwsCaptureInstanceProperties = true] “aws:ec2launchtemplate:id” :” lt-xxxx” [when AwsCaptureInstanceProperties = true] “aws:ec2launchtemplate:version” : “n” [when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] “CitrixOperationalResource” : “” “XdConfig” : “XdProvisioned=true”
ボリュームワーカーのブートストラッパー	“Name” : “XenDesktop Temp” “XdConfig” : “XdProvisioned=true” “CitrixProvisioningSchemeId” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] “CitrixVolumeWorkerBootstrapper” : “”
ボリュームワーカーのインスタンス	“Name” : “Citrix.XD.Volumeworker-xxxx-xx-xx-xx-xxxx” “XdConfig” : “XdProvisioned=true”

追加情報

- 接続とリソースの作成と管理
- AWS への接続

- マシンカタログの作成
- AWS カタログの作成
- マシンカタログの管理

Google Cloud Platform カタログの管理

February 9, 2024

「マシンカタログの管理」では、マシンカタログを管理するウィザードについて説明します。以下の情報は、Google クラウド環境に固有の詳細について説明しています。

> 注:
>
> Google Cloud Platform カタログを管理する前に、Google Cloud Platform カタログの作成を完了する必要があります。「Google Cloud Platform カタログの作成」を参照してください。

カタログへのマシンの追加

マシンをカタログに追加するには、次の手順を実行します:

1. ［管理］**>**［完全な構成］の左側ペインで ［マシンカタログ］を選択します。
2. マシンを追加するマシンカタログを選択します。
3. 操作バーの ［マシンの追加］を選択します。
4. ［仮想マシン］ページで、追加するマシンの数を指定し、［次へ］を選択します。
5. ［マシン **ID**］ページで、Active Directory アカウントを選択してから ［次へ］を選択します。
6. ［ドメイン資格情報］ページで、［資格情報の入力］を選択し、ユーザー名とパスワードを入力し、［保存］を選択してから ［次へ］を選択します。
7. ［概要］ページで情報を確認してから、［完了］を選択します。

マシンの更新

この機能は、マスターイメージまたは最小機能レベルを更新する場合に役立ちます。

マシンを更新するには、次の手順を実行します:

1. ［管理］**>**［完全な構成］の左側ペインで ［マシンカタログ］を選択します。
2. 更新するマシンを含むマシンカタログを選択します。
3. 操作バーで ［マスターイメージの変更］を選択します。
4. ［イメージ］ページで、VM とカタログの最小機能レベルを選択してから ［次へ］を選択します。
5. ［ロールアウト方法］ページで、マシンを更新するタイミングを指定し、［次へ］を選択します。
6. ［概要］ページで情報を確認してから、［完了］を選択します。

マシン更新のロールバック

マシンの更新をロールバックするには、次の手順を実行します:

> 重要:
>
> マスターイメージの名前変更、削除、または移動は行わないでください。さもないと、更新をロールバックできません。

1. ［管理］**>**［完全な構成］の左側ペインで ［マシンカタログ］を選択します。
2. マシンの更新をロールバックするマシンカタログを選択します。
3. 操作バーで ［マスターイメージのロールバック］を選択します。
4. ［概要］ページで情報を確認してから ［次へ］を選択します。
5. ［ロールアウト方法］ページで、ロールアウト方法を構成し、［次へ］を選択します。
6. ［概要］ページで情報を確認してから、［完了］を選択します。

電源管理

Citrix DaaS を使用すると、Google Cloud マシンの電源管理が可能になります。ナビゲーションペインの ［検索］ノードを使用して、電源管理するマシンを検索します。次の電源操作が使用可能です:

- 削除
- 起動
- 再起動
- 強制再起動
- シャットダウン
- 強制シャットダウン
- デリバリーグループに追加
- タグの管理
- メンテナンスモードをオンにする

Autoscale を使用して Google Cloud マシンの電源を管理することもできます。これを行うには、Google Cloud マシンをデリバリーグループに追加し、そのデリバリーグループの Autoscale を有効にします。Autoscale について詳しくは、「Autoscale」を参照してください。

PowerShell を使用してプロビジョニングされたマシンを更新

`Set-ProvScheme`コマンドは、プロビジョニングスキームを変更します。ただし、既存のマシンには影響しません。PowerShell コマンドの`Set-ProvVMUpdateTimeWindow`を使用して、現在のプロビジョニングスキームを既存の永続的マシンや非永続的マシン、またはマシンのセットに適用できるようになりました。現在、GCP に

おいてこの機能でサポートされているのは、マシンプロファイル、サービスオファリング、カスタムカタログ設定などのプロパティ更新です。

以下を更新できます:

- 単一の VM
- プロビジョニングスキーム ID に関連付けられている特定の VM またはすべての既存の VM のリスト
- プロビジョニングスキーム名に関連付けられている特定の VM またはすべての既存の VM のリスト

既存の VM を更新するには:

1. 既存のマシンの構成を確認します。例:

```
Get-ProvScheme | select ProvisioningSchemeName,
   ProvisioningSchemeVersion
<!--NeedCopy-->
```

2. プロビジョニングスキームを更新します。例:

   - マシンプロファイルの更新

```
`Set-ProvScheme  - ProvisioningSchemeName "my-catalog"  -
   MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
   machineprofileinstance.vm"
<!--NeedCopy-->
```

   - サービスオファリングの更新

```
 Set-ProvScheme -ProvisioningSchemeName "my-catalog" -
    ServiceOffering  “XDHyp:\HostingUnits<hosting-unit>\
    serviceoffering.folder<service-offering>.serviceoffering"
 <!--NeedCopy-->
```

3. VM の現在のプロパティが現在のプロビジョニングスキームと一致するかどうか、および VM に保留中の更新アクションがあるかどうかを確認します。例:

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
   ProvisioningSchemeVersion
<!--NeedCopy-->
```

   特定のバージョンのマシンを見つけることもできます。例:

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select
   VMName, ProvisioningSchemeVersion
<!--NeedCopy-->
```

4. 既存のマシンを更新します。

   - すべての既存のマシンを更新するには:


```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

- 特定のマシンのリストを更新するには:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes
    -1
<!--NeedCopy-->
```

- Get-ProvVMの出力に基づいてマシンを更新するには:

```
Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
    ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

> 注:
>
> - StartsNowは、スケジュールの開始時刻が現在時刻であることを指定します。
> - 負の数（-1 など）のDurationInMinutesは、スケジュールの期間に上限がないことを示します。

5. スケジュール済みの更新があるマシンを見つけます。例:

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName
    , ProvisioningSchemeUpdateAfter
<!--NeedCopy-->
```

6. マシンを再起動します。次回の電源投入時に、プロパティの変更が既存のマシンに適用されます。次のコマンドを使用して、更新されたステータスを確認できます:

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

既存のカタログのディスクに関連したカスタムプロパティを変更する

既存のカタログおよびカタログの既存の VM で次のディスク関連のカスタムプロパティを変更できます:

- PersistOSDisk
- PersistWBC
- StorageType
- IdentityDiskStorageType
- WbcDiskStorageType

> 注:
>
> - StorageTypeプロパティは OS ディスク用です
> - PersistOsDiskプロパティは、ライトバックキャッシュを有効にした非永続カタログに対してのみ設定できます

この実装により、カタログを作成した後でも、異なるディスクに対して異なるストレージの種類を選択できるため、さまざまなストレージの種類を使用することと価格のバランスを取ることができます。

これを行うには、PowerShell コマンドSet-ProvSchemeおよびSet-ProvVMUpdateTimeWindowを使用します:

1. **PowerShell** ウィンドウを開きます。
2. asnp citrix*を実行します。
3. Get-ProvVM -VMName <VM name>を実行してカスタムプロパティを取得します。
4. カスタムプロパティ文字列を変更します:
   a) カスタムプロパティをメモ帳にコピーし、カスタムプロパティを変更します。
   b) **PowerShell** ウィンドウで、変更したカスタムプロパティをメモ帳から貼り付け、変更したカスタムプロパティに変数を割り当てます。例:

```
$cp =  '<CustomProperties xmlns=http://schemas.citrix.com
    /2014/xd/machinecreation xmlns:xsi="http://www.w3.org/2001/
    XMLSchema-instance">
<Property xsi:type="StringProperty" Name="CatalogZones" Value
    ="" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="
    true" />
<Property xsi:type="StringProperty" Name="PersistOSDisk" Value
    ="true" />
<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
    Value="pd-standard" />
<Property xsi:type="StringProperty" Name="StorageType" Value="
    pd-standard" />
</CustomProperties>'
<!--NeedCopy-->
```

5. 既存のカタログを更新します。例:

```
Set-ProvScheme -ProvisioningSchemeName <yourCatalogName> -
    CustomProperties $cp
<!--NeedCopy-->
```

6. 既存の VM を更新します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
    VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```


7. VM を再起動します。次回の電源投入時に、カスタムプロパティの変更が既存の VM に適用されます。

意図しないマシンの削除からの保護

Citrix DaaS を使用すると、Google Cloud 上の MCS リソースを保護し、誤って削除されないようにすることができます。`deletionProtection`フラグを TRUE に設定して、プロビジョニングされた VM を構成します。

デフォルトでは、MCS または Google Cloud プラグインを介してプロビジョニングされた VM は、InstanceProtection が有効な状態で作成されます。この実装は、永続カタログと非永続カタログの両方に適用できます。非永続カタログは、インスタンスがテンプレートから再作成されるときに更新されます。既存の永続マシンの場合、Google Cloud コンソールでフラグを設定できます。フラグの設定について詳しくは、Google のドキュメントのサイトを参照してください。永続カタログに追加された新しいマシンは、`deletionProtection`が有効な状態で作成されます。

`deletionProtection`フラグを設定した VM インスタンスを削除しようとすると、その要求は失敗します。ただし、権限の`compute.instances.setDeletionProtection`が付与されているか、IAM の **Compute Admin** の役割が割り当てられている場合は、リソースの削除を許可するフラグをリセットできます。

MCS によって作成されたリソースの特定

以下は、MCS が GCP プラットフォームのリソースに追加するタグです。表のタグは、「”キー”:”値”」として表示されます。

リソース名	タグ
ID ディスク	“CitrixResource”： “internal” “CitrixProvisioningSchemeId”： “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
イメージ	“CitrixResource”： “internal” “CitrixProvisioningSchemeId”： “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
OS ディスク	“CitrixResource”： “internal” “CitrixProvisioningSchemeId”： “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
準備用の仮想マシン	“CitrixResource”： “internal” “CitrixProvisioningSchemeId”： “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
公開されたスナップショット	“CitrixResource”： “internal”
ストレージバケット	“CitrixResource”： “internal”

リソース名	タグ
テンプレート	“CitrixResource”： “internal” “CitrixProvisioningSchemeId”： “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
カタログ内の VM	“CitrixResource”： “internal” “CitrixProvisioningSchemeId”： “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”．プラグインは、MCS でプロビジョニングされた VM に次のラベルも追加します:”citrix-provisioning-scheme-id”： “provSchemeId”。このラベルは、GCP コンソールでカタログによるフィルタリングに使用できます。
WBC ディスク	“CitrixResource”： “internal” CitrixProvisioningSchemeId”： “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”

> 注:
>
> MCS によって作成されたリソースとして識別するために **CitrixResource** タグが追加されている場合、VM は Citrix インベントリに表示されません。タグを削除するか名前を変更すると、表示できるようになります。

追加情報

- 接続とリソースの作成と管理
- Google クラウド環境への接続
- マシンカタログの作成
- Google Cloud Platform カタログの作成
- マシンカタログの管理

HPE Moonshot カタログを管理する

May 17, 2024

「マシンカタログの管理」では、マシンカタログを管理するウィザードについて説明します。以下の情報は、HPE Moonshot カタログに固有の詳細について説明しています。

> 注:
>
> HPE Moonshot カタログを管理する前に、HPE Moonshot カタログの作成を完了する必要があります。「HPE Moonshot マシンカタログの作成」を参照してください。

電源管理

Citrix DaaS を使用すると、HPE Moonshot マシンの電源管理を行うことができます。ナビゲーションペインの［検索］ノードを使用して、電源管理するマシンを検索します。次の電源操作が使用可能です:

- 開始
- シャットダウン
- 強制シャットダウン
- 再起動
- リセット

> 注:
>
> 電源操作の ［一時停止］および ［再開］はサポートされていません。

追加情報

- 接続とリソースの作成と管理
- HPE Moonshot への接続
- マシンカタログの作成
- HPE Moonshot マシンカタログの作成
- マシンカタログの管理

Microsoft Azure カタログの管理

May 17, 2024

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

「マシンカタログの管理」では、マシンカタログを管理するウィザードについて説明します。以下の情報は、Microsoft Azure Resource Manager クラウド環境に固有の詳細について説明しています。

> 注:
>
> Microsoft Azure カタログを管理する前に、Microsoft Azure カタログの作成を完了する必要があります。「Microsoft Azure カタログの作成」を参照してください。

仮想マシンのシャットダウン時にストレージの種類をダウングレードする

仮想マシンのシャットダウン時に管理対象ディスクのストレージの種類をダウングレードすると、ストレージコストを節約できます。これを行うには、カスタムプロパティ`StorageTypeAtShutdown`を使用します。

仮想マシンをシャットダウンすると、ディスクのストレージの種類が(カスタムプロパティ`StorageTypeAtShutdown`で指定されたものに) ダウングレードされます。仮想マシンの電源をオンにすると、ストレージの種類が (カスタムプロパティ`StorageType`またはカスタムプロパティ`WBCDiskStorageType`で指定された) 元に戻ります。

> 重要:
>
> - ディスクは、仮想マシンの電源を少なくとも 1 回オンにするまで存在しません。このため、仮想マシンの初回電源投入時にストレージの種類を変更することはできません。
> - ストレージの種類をダウングレードすると、VM の起動にかかる時間が少し長くなる場合があります。

要件

- 管理対象ディスクに適用できます。これは、カスタムプロパティ`UseManagedDisks`を true に設定することを意味します。
- 永続 OS ディスクがある永続カタログおよび非永続カタログに適用できます。これは、カスタムプロパティ`persistOsDisk`を true に設定することを意味します。
- 永続 WBC ディスクがある非永続カタログに適用できます。これは、カスタムプロパティ`persistWBC`を true に設定することを意味します。

制限事項

- Microsoft によると、ディスクの種類を変更できるのは 1 日に 2 回のみです。Microsoft ドキュメントを参照してください。Citrix に関しては、`StorageType`の更新は VM の開始または割り当て解除操作があるたびに行われます。したがって、VM ごとの電源操作の数を 1 日あたり 2 回に制限します。たとえば、朝に 1 回の電源操作で VM を起動し、夕方にもう 1 回の電源操作で VM の割り当てを解除します。

ストレージの種類をダウングレードするには

手順に進む前に、「要件」と「制限事項」を参照してください。

1. カスタムプロパティStorageTypeAtShutdownを追加し、値を Standard_LRS（HDD）に設定し、New-ProvSchemeを使用してカタログを作成します。PowerShell を使用してカタログを作成する方法については、「https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/」を参照してください。

   > 注:
   >
   > StorageTypeAtShutdownの値が空または Standard_LRS（HDD）以外の場合、操作は失敗します。

   永続カタログの作成中にカスタムプロパティを設定する例:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />
<Property xsi:type="StringProperty" Name="StorageType" Value="Premium_LRS “ />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown" Value="Standard_LRS" />
</CustomProperties>’
<!--NeedCopy-->
```

   非永続カタログの作成中にカスタムプロパティを設定する例:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />
<Property xsi:type="StringProperty" Name="StorageType" Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="WbcDiskStorageType" Value="Standard_SSD_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />
```



```
<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true
    />
<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=
    true />
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
    Value="Standard_LRS" />
</CustomProperties>'
<!--NeedCopy-->
```

> 注:
>
> マシンプロファイルを使用する場合、カスタムプロパティは`MachineProfile`で定義されたプロパティよりも優先されます。

2. 仮想マシンをシャットダウンし、Azure Portal で仮想マシンのストレージの種類を確認します。ディスクのストレージの種類がカスタムプロパティ`StorageTypeAtShutdown`で指定されたものにダウングレードされます。
3. 仮想マシンの電源を入れます。ディスクのストレージの種類は、以下に記載されているストレージの種類に切り替わります:
   - OS ディスクのカスタムプロパティ`StorageType`
   - `CustomProperties`で指定した場合のみ WBC ディスクのカスタムプロパティ`WBCDiskStorageType`。それ以外の場合は、`StorageType`に記載されているストレージの種類に切り替わります。

StorageTypeAtShutdown を既存のカタログに適用する

手順に進む前に、「要件」と「制限事項」を参照してください。

`Set-ProvScheme`を使用して、既存のカタログに追加された新しい VM に`StorageTypeAtShutdown`を適用します。

仮想マシンを既存のカタログに追加するときにカスタムプロパティを設定する例:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com
    /2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageType" Value="
    Premium_LRS" />
<Property xsi:type="StringProperty" Name="WbcDiskStorageType" Value="
    Standard_SSD_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />
<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />
```



```
<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown" Value
    ="Standard_LRS" />
</CustomProperties>'

$ProvScheme = Get-Provscheme -ProvisioningSchemeName $CatalogName

Set-ProvScheme -ProvisioningSchemeName $ProvScheme.
    ProvisioningSchemeName -CustomProperties $customProperties
<!--NeedCopy-->
```

シャットダウン時に既存の **VM** のストレージの種類を下位レベルに変更する

手順に進む前に、「要件」と「制限事項」を参照してください。

VM のシャットダウン時に、既存の VM のストレージの種類を下位レベルに変更することで、ストレージコストを節約できます。

VM のシャットダウン時に、カタログ内の既存のマシンのストレージの種類を下位レベルに変更するには、次の手順を実行します:

1. PowerShell ウィンドウを開きます。
2. `asnp citrix*`を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. `Get-Provscheme -ProvisioningSchemeName $CatalogName`を実行します。
4. カスタムプロパティ文字列を変更します。

   ```
   $customProperties = '<CustomProperties xmlns="http://schemas.
       citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
       org/2001/XMLSchema-instance">
   <Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
       Value="Standard_LRS" />
   </CustomProperties>'
   <!--NeedCopy-->
   ```

5. 既存のカタログのプロビジョニングスキームを更新します。この更新は、`Set-ProvScheme`の実行後に追加された新しい仮想マシンに適用されます。

   ```
   Set-ProvScheme -ProvisioningSchemeName $CatalogName -
       CustomProperties $customProperties
   <!--NeedCopy-->
   ```

6. 既存の VM を更新して`StorageTypeAtShutdown`を有効にします。

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
       StartsNow -DurationInMinutes -1
   <!--NeedCopy-->
   ```


7. 次にマシンの電源を入れると、マシンのStorageTypeAtShutdownプロパティが更新されます。ストレージの種類は、次回のシャットダウン時に変更されます。
8. 次のコマンドを実行して、カタログ内の各 VM のStorageTypeAtShutdown値を表示します。

```
Get-ProvVM -ProvisioningSchemeName <catalog-name> | foreach {
  $vmName = $_.VMName; $storageTypeAtShutdown = ($_.CustomVmData |
       ConvertFrom-Json).StorageTypeAtShutdown.
      DiskStorageAccountType; return New-Object psobject -Property
      @{
  "VMName" = $vmName; "StorageTypeAtShutdown" =
      $storageTypeAtShutdown  }
   }

<!--NeedCopy-->
```

プロビジョニングされたマシンを現在のプロビジョニングスキームの状態に更新する

Set-ProvSchemeコマンドは、プロビジョニングスキームを変更します。ただし、既存のマシンには影響しません。PowerShell コマンドのSet-ProvVMUpdateTimeWindowを使用して、現在のプロビジョニングスキームを既存の永続的マシンや非永続的マシン、またはマシンのセットに適用できます。既存の MCS プロビジョニング済みマシンの構成の更新について、時間枠をスケジュール設定できます。スケジュールされた時間枠内で電源をオンまたは再起動すると、スケジュールされたプロビジョニングスキームの更新がマシンに適用されます。現在、Azure では、ServiceOffering、MachineProfileおよび次のカスタムプロパティを更新できます:

- StorageType
- WBCDiskStorageType
- IdentityDiskStorageType
- LicenseType
- DedicatedHostGroupId
- PersistWBC
- PersistOsDisk
- PersistVm

> 注:
>
> - Azure環境では、管理対象ディスクを使用してカタログのStorageType、WBCDiskStorageType、およびIdentityDiskStorageTypeのカスタムプロパティのみを更新できます。
> - Set-ProvVMUpdateTimeWindowを 2 回実行すると、最新のコマンドが有効になります。

以下を更新できます:

- 単一の VM
- プロビジョニングスキーム ID に関連付けられている特定の VM またはすべての既存の VM のリスト

- プロビジョニングスキーム名（マシンカタログ名）に関連付けられている特定の VM またはすべての既存の VM のリスト

プロビジョニングスキームに次の変更を加えた後、Azure の永続カタログの VM インスタンスが再作成されます：

- `MachineProfile`を変更
- `LicenseType`を削除
- `DedicatedHostGroupId`を削除

> 注：
>
> 既存マシンの OS ディスクとそのすべてのデータはそのまま残り、新しい仮想マシンはディスクに接続されます。

既存の VM を更新する前に、以下を実行します：

1. 既存のマシンの構成を確認します。例：

```
Get-ProvScheme | select ProvisioningSchemeName,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

2. プロビジョニングスキームを更新します。例：

   - VM をマシンプロファイルの入力に使用する場合：

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog" -
    MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
    machineprofile.folder<resource-group>.resourcegroup<
    virtual-machine>.vm"
<!--NeedCopy-->
```

   - テンプレートスペックをマシンプロファイルの入力に使用する場合：

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog"
-MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
    machineprofile.folder<resource-group>.resourcegroup<
    template-spec>.templatespec<template-spec-version>.
    templatespecversion"
-ServiceOffering "XDHyp:\HostingUnits<hosting-unit>\
    serviceoffering.folder<service-offering>.serviceoffering"
<!--NeedCopy-->
```

   - サービスオファリングだけを使用する場合：

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog" -
    ServiceOffering "XDHyp:\HostingUnits<hosting-unit>\
    serviceoffering.folder<service-offering>.serviceoffering"
<!--NeedCopy-->
```


3. VM の現在のプロパティが現在のプロビジョニングスキームと一致するかどうか、および VM に保留中の更新アクションがあるかどうかを確認します。例:

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

特定のバージョンのマシンを見つけることもできます。例:

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select
    VMName, ProvisioningSchemeVersion
<!--NeedCopy-->
```

既存のマシンの更新を次回の再起動時に適用するように要求するには、次の手順を実行します:

1. 次のコマンドを実行して既存のマシンを更新し、次回の再起動時に更新を適用します。

   - すべての既存のマシンを更新するには、例:

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
       -StartsNow -DurationInMinutes -1
   <!--NeedCopy-->
   ```

   - 特定のマシンのリストを更新するには:例:

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
       -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes
      -1
   <!--NeedCopy-->
   ```

   - Get-ProvVM の出力に基づいてマシンを更新するには、例:

   ```
   Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
      ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
      -StartsNow -DurationInMinutes -1
   <!--NeedCopy-->
   ```

   > 注:
   >
   > - StartsNowは、スケジュールの開始時刻が現在時刻であることを指定します。
   > - 負の数(-1 など)のDurationInMinutesは、スケジュールの期間に上限がないことを示します。

2. スケジュール済みの更新があるマシンを見つけます。例:

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName
    , ProvisioningSchemeUpdateAfter
<!--NeedCopy-->
```

3. マシンを再起動します。次回の電源投入時に、プロパティの変更が既存のマシンに適用されます。次のコマンドを使用して、更新されたステータスを確認できます。例:


```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

次回、スケジュールされた時間帯に VM が起動したとき、最新のプロビジョニング設定に更新するようにスケジュールします:

1. 次のコマンドを実行します:

   - 開始時刻を現在時刻として更新をスケジュールするには:

     ```
     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
         -VMName vm1 -StartsNow -DurationInMinutes 120
     <!--NeedCopy-->
     ```

   - 週末に更新をスケジュールするには:

     ```
     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName “my-
         catalog” -VMName “vm1” -StartTimeInUTC “10/15/2022
         9:00am” -DurationInMinutes (New-TimeSpan -Days 2).
         TotalMinutes
     <!--NeedCopy-->
     ```

   > 注:
   >
   > - VMNameはオプションです。指定しない場合、更新はカタログ全体に対してスケジュールされます。
   > - StartTimeInUTCの代わりにStartsNowを使用して、スケジュールの開始時刻が現在時刻であることを指定します。
   > - DurationInMinutesはオプションです。デフォルトは 120 分です。負の数（-1 など）は、スケジュールの時間枠に上限がないことを示します。

2. 更新状況を確認します。

   ```
   Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
       ProvisioningSchemeUpdateUntil, ProvisioningSchemeVersion
   <!--NeedCopy-->
   ```

3. VM の電源を入れます。スケジュールされた時間枠の後にマシンの電源をオンにした場合、構成の更新は適用されません。スケジュールされた時間枠内にマシンの電源を入れた場合、

   - マシンの電源がオフになっていて、
     - マシンの電源をオンにしない場合、構成の更新は適用されません
     - マシンの電源をオンにする場合、構成の更新は適用されます
   - マシンの電源がオンになっていて、
     - マシンを再起動しない場合、構成の更新は適用されません

- マシンを再起動する場合、構成の更新は適用されます

構成の更新をキャンセルするには、以下の手順を実行します:

単一の VM、複数の VM、またはカタログ全体の構成の更新をキャンセルすることもできます。構成の更新をキャンセルするには:

1. `Clear-ProvVMUpdateTimeWindow`を実行します。例:

   - 単一の VM に対してスケジュールされた構成の更新をキャンセルするには:

   ```
   Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName “ my-catalog “ -VMName “vm1”
   <!--NeedCopy-->
   ```

   - 複数の VM に対してスケジュールされた構成の更新をキャンセルするには:

   ```
   Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-catalog" -VMName "vm1","vm2"
   <!--NeedCopy-->
   ```

> 注:
>
> VM は同じカタログにある必要があります。

個別の **VM** のプロパティを更新する

PowerShell コマンド`Set-ProvVM`を使用して、永続的な MCS マシンカタログ内の個別の VM のプロパティを更新できるようになりました。ただし、更新はすぐには適用されません。更新を適用するには、PowerShell コマンド`Set-ProvVMUpdateTimeWindow`を使用して時間枠を設定する必要があります。

この実装により、マシンカタログ全体を更新することなく、個別の VM を効率的に管理できます。現在、この機能は Azure 環境にのみ適用されます。

以下は、現在更新できるプロパティです:

- `CustomProperties`
- `ServiceOffering`
- `MachineProfile`

この機能を使用することで、以下のことを実行できます:

- VM のプロパティを更新する
- マシンカタログが更新された後も、VM 上で更新されたプロパティを保持する
- VM に適用された構成の更新を元に戻す

VM のプロパティを更新する前に、以下を実行します:

1. **PowerShell** ウィンドウを開きます。

2. asnp citrix*を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. 既存のマシンカタログの構成を確認します。例:

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
<!--NeedCopy-->
```

4. 更新を適用する VM の構成を確認します。例:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

VM のプロパティを更新する

VM 上のプロパティを更新するには、次の手順を実行します:

1. 更新を適用する VM をオフにします。
2. VM のプロパティを更新します。たとえば、カスタムプロパティの VM のストレージの種類（StorageType）を更新する場合は、次のコマンドを実行します:

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1 -
    CustomProperties "...<Property Name='StorageType' Value='
    Premium_LRS' />..."
<!--NeedCopy-->
```

マシンカタログ内の 2 台の VM のプロパティを同時に更新できます。例:

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1 -
    CustomProperties "...<Property Name='StorageType' Value='
    Premium_LRS' />..."
<!--NeedCopy-->
```

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine2 -
    CustomProperties "...<Property Name='StorageType' Value='
    StandardSSD_LRS' />..."
<!--NeedCopy-->
```

> 注:
>
> 更新はすぐには適用されません。

3. 更新するように指定されたプロパティの一覧と構成バージョンを取得します。例:

```
Get-ProvVMConfiguration -ProvisioningSchemeName AzureCatalog -
    VMName machine1
<!--NeedCopy-->
```

Versionのプロパティ値と更新するプロパティ（この場合はStorageType）を確認します。

4. 構成バージョンを確認します。例:


```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

`ProvVMConfigurationVersion`のプロパティ値を確認します。更新はまだ適用されていません。VM はまだ古い構成のままです。

5. スケジュールされた更新を要求します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
    StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

スケジュールされた更新について詳しくは、「プロビジョニングされたマシンを現在のプロビジョニングスキームの状態に更新する」を参照してください。

> 注:
>
> 保留中のプロビジョニングスキームの更新も適用されます。

6. 仮想マシンを再起動します。例:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
<!--NeedCopy-->
```

7. 構成バージョンを確認します。例:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

`ProvVMConfigurationVersion`のプロパティ値を確認します。更新が適用されました。VM には新しい構成が適用されました。

8. VM にさらに構成の更新を適用するには、VM をオフにして、手順を繰り返します。

マシンカタログが更新された後も、**VM** 上で更新されたプロパティを保持する

VM 上の更新されたプロパティを保持するには、次の手順を実行します:

1. 更新を適用する VM をオフにします。
2. マシンカタログを更新します。たとえば、VM のサイズ（`ServiceOffering`）とストレージの種類（`StorageType`）を更新する場合は、次のコマンドを実行します:

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -
    ServiceOffering Standard_E4_v3 -CustomProperties "...<Property
    Name='StorageType' Value='StandardSSD_LRS' />..."
<!--NeedCopy-->
```

3. マシンカタログの構成の詳細を取得します。例:


```
1 Get-ProvScheme -ProvisioningSchemeName AzureCatalog
2 <!--NeedCopy-->
```

ProvisioningSchemeVersionが 1 つ増えます。VM のサイズとストレージの種類も更新されます。

4. VM のプロパティを更新します。たとえば、マシンプロファイルを VM に提供します。

```
1 Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1 -
      MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
      machineprofile.folder<resource-group>.resourcegroup<template-
      spec>.templatespec<template-spec-version>.templatespecversion"
2 <!--NeedCopy-->
```

> 注:
>
> マシンプロファイル入力にはタグがあり、別の VM サイズ（ServiceOffering）が指定されています。

5. VM 上の構成の更新をマシンカタログの更新とマージした後に VM のプロパティの一覧を取得します。例:

```
1 Get-ProvVMConfigurationResultantSet -ProvisioningSchemeName
      AzureCatalog -VMName machine1
2 <!--NeedCopy-->
```

> 注:
>
> VM 上の更新はすべて、マシンカタログ上で行われた更新を上書きします。

6. VM のスケジュールされた更新を要求します。例:

```
1 Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
      VMName machine1 -StartsNow -DurationInMinutes -1
2 <!--NeedCopy-->
```

7. 仮想マシンを再起動します。例:

```
1 New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
2 <!--NeedCopy-->
```

VM は、マシンプロファイルに基づいて更新された VM サイズを維持します。マシンプロファイルで指定されたタグ値も VM に適用されます。ただし、ストレージの種類は最新のプロビジョニングスキームに基づきます。

8. VM の構成バージョンを取得します。例:

```
1 Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
2 <!--NeedCopy-->
```

ProvisioningSchemeVersionとProvVMConfigurationVersionには最新バージョンが表示されるようになりました。

VM に適用された構成の更新を元に戻す

1. VM に更新を適用した後、VM をオフにします。
2. 次のコマンドを実行して、VM に適用されている更新を削除します。例:

```
Set-ProvVM -RevertToProvSchemeConfiguration -
    ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

3. VM のスケジュールされた更新を要求します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
    VMName machine1 -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

4. 仮想マシンを再起動します。例:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
<!--NeedCopy-->
```

5. VM の構成バージョンを確認します。例:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

`ProvVMConfigurationVersion`の値は、マシンカタログの構成バージョンを表示するようになりました。

ディスク暗号化を変更する

Azure 仮想化環境でディスク暗号化を変更し、次の操作を実行できます:

- `New-ProvScheme`コマンドを使用して、マスターイメージのディスク暗号化セット（DES）とは異なる DES の MCS マシンカタログを作成します。例:

```
$customProperties = @"
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
<Property xsi:type="DiskEncryptionSetId" Name="Zones" Value="/
    subscriptions/XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX/resourceGroups/
    testrsg/providers/Microsoft.Compute/diskEncryptionSets/test-
    diskEncryptionSet"/>
</CustomProperties>
"@
New-ProvScheme -CleanOnBoot `
-ProvisioningSchemeName $provisioningSchemeName `
-HostingUnitName $hostingUnitName `
-IdentityPoolName $identityPoolName `
```



```
-InitialBatchSizeHint $numberOfVms `
-masterImagePath $masterImagePath `
-NetworkMapping $networkMapping `
-CustomProperties $customProperties
<!--NeedCopy-->
```

- Set-ProvScheme およびSet-ProvVMUpdateTimeWindowコマンドを使用して、既存の MCS マシンカタログおよび既存の VM のディスク暗号化の種類を 1 つの DES キーから別の DES キーに変更します。VM を再起動すると、更新された DES キーが表示されます。例:

```
$customProperties = '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
    Value="/subscriptions/456c683e2ed7/resourceGroups/testrg/
    providers/Microsoft.Compute/diskEncryptionSets/
    diskEncryptionSet1" />
</CustomProperties>'
Set-ProvScheme -ProvisioningSchemeName azure-catalog -
    CustomProperties $customProperties
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
    -VMName azu01, azu02 -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

- Set-ProvSchemeおよびSet-ProvVMUpdateTimeWindowコマンドを使用して、以前に CMEK が有効になっていなかった MCS マシンカタログと VM を更新し、顧客管理の暗号化キー（CMEK）の暗号化（DES）、ホストでのディスク暗号化、または二重暗号化を有効にします。さまざまな暗号化の種類について詳しくは、「Azure サーバー側暗号化」、「ホストでの Azure ディスク暗号化」、および「管理対象ディスクの二重暗号化」を参照してください。

- Set-ProvSchemeおよびSet-ProvVMUpdateTimeWindowコマンドを使用して、以前に暗号化されていた既存の MCS マシンカタログと VM を暗号化されていない状態に更新します。例:

```
$customProperties = '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
    Value="" />
</CustomProperties>'
Set-ProvScheme -ProvisioningSchemeName azure-catalog -
    CustomProperties $customProperties
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
    -VMName azu01, azu02 -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

- プライベートエンドポイント（ProxyHypervisorTrafficThroughConnectorが有効になっているホスト接続を使用した MCS マシンカタログ）でディスク暗号化を有効にします。ProxyHypervisorTrafficThroughConnectorについて詳しくは、「Azure 管理トラフィックのための安全な環境の作成」を参照してください。プライベートエンドポイントでディスク暗号化を有効に

する方法について詳しくは、「プライベートエンドポイントでディスク暗号化を有効にする」を参照してください。

プライベートエンドポイントでディスク暗号化を有効にする

Azure の制限により、現在、プライベートエンドポイントに対して顧客管理キーを使用したサーバー側暗号化を行うことはできません。ただし、既存の MCS マシンカタログと VM をプライベートエンドポイントで更新して、DES キーで暗号化することができます。

プライベートエンドポイントを使用して既存のマシンカタログを更新する　既存のマシンカタログをプライベートエンドポイントで更新する詳細な手順は次のとおりです:

1. ProxyHypervisorTrafficThroughConnectorでディスク暗号化を使用せずにカタログを作成します。ProxyHypervisorTrafficThroughConnectorについて詳しくは、「Azure 管理トラフィックのための安全な環境の作成」を参照してください。
2. Set-ProvSchemeを実行してDiskEncryptionSetIdでカタログを更新します。

   > 注:
   >
   > DiskEcryptionSetIdはCustomPropertiesまたはMachineProfileで構成できます。CustomPropertiesとMachineProfileの両方で定義されている場合は、CustomPropertiesで定義されたプロパティが適用されます。

   CustomPropertiesを使用する場合の例:

   ```
   $customProperties = '<CustomProperties xmlns="http://schemas.
       citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
       org/2001/XMLSchema-instance">
   <Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
       Value="/subscriptions/456c683e2ed7/resourceGroups/testrg/
       providers/Microsoft.Compute/diskEncryptionSets/
       diskEncryptionSet1"/>
   </CustomProperties>'
   Set-ProvScheme -ProvisioningSchemeName azure-catalog -
       CustomProperties $customProperties
   <!--NeedCopy-->
   ```

   MachineProfile を使用する場合の例：ディスク暗号化が有効になっている VM か、ディスク暗号化設定を含むテンプレートスペックを使用します:

   ```
   Set-ProvScheme -ProvisioningSchemeName azure-catalog -
       MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.
       folder\testrg.resourcegroup\new-template.vm"
   <!--NeedCopy-->
   ```

   または、完全な構成インターフェイスを使用してマシンプロファイルを更新することもできます。

3. 既存のカタログ VM を更新するには、Set-ProvVMUpdateTimeWindowを実行します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -
    VMName azu01, azu02 -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

4. VM を再起動すると、Azure Portal で VM のディスク上の更新されたディスク暗号化を確認できます。

5. 新しいカタログ VM を追加する前に、Set-ProvSchemeを実行してディスク暗号化を解除します。

   > 注:
   >
   > プライベートエンドポイントカタログを更新するため、この手順は必須です。この手順を実行しないと、カタログに新しい VM を追加しようとしたときにエラーが発生します。

   例:

```
$customProperties = '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
    Value="" />
</CustomProperties>'
Set-ProvScheme -ProvisioningSchemeName azure-catalog -
    CustomProperties $customProperties
<!--NeedCopy-->
```

6. 新しい VM をカタログに追加します。

個々のカタログ **VM** を更新する　個々のカタログ VM を更新するための詳細な手順は次のとおりです:

1. ProxyHypervisorTrafficThroughConnectorでディスク暗号化を使用せずにカタログを作成します。ProxyHypervisorTrafficThroughConnectorについて詳しくは、「Azure 管理トラフィックのための安全な環境の作成」を参照してください。

2. Set-ProvVMを実行してDiskEncryptionSetIdでカタログ VM を更新します。

   > 注:
   >
   > DiskEcryptionSetIdはCustomPropertiesまたはMachineProfileのいずれかで設定できます。

   CustomPropertiesを使用する場合の例:

```
$customProperties = '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
    Value="/subscriptions/456c683e2ed7/resourceGroups/testrg/
    providers/Microsoft.Compute/diskEncryptionSets/
    diskEncryptionSet1" />
```



```
</CustomProperties>'
Set-ProvVM -ProvisioningSchemeName azure-catalog  -VMName azu01 -
    CustomProperties $customProperties
<!--NeedCopy-->
```

MachineProfile を使用する場合の例:

```
Set-ProvVM -ProvisioningSchemeName azure-catalog  -VMName azu01 -
    MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.
    folder\testrg.resourcegroup\new-template.vm"
<!--NeedCopy-->
```

3. 既存のカタログ VM を更新するには、`Set-ProvVMUpdateTimeWindow`を実行します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -
    VMName azu01 -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

4. VM を再起動すると、Azure Portal で VM のディスク上の更新されたディスク暗号化を確認できます。
5. 新しい VM をカタログに追加します。

Azure VM、スナップショット、**OS** ディスク、およびギャラリーイメージ定義の情報の取得

OS ディスクと種類、スナップショット、ギャラリーイメージ定義など、Azure VM の情報を表示できます。この情報は、マシンカタログが割り当てられている場合にマスターイメージ上のリソースに関して表示されます。この機能を使用して、Linux または Windows イメージを表示および選択します。PowerShell プロパティ`TemplateIsWindowsTemplate`が`AdditionDatafield`パラメーターに追加されました。このフィールドには、Azure 固有の情報（VM タイプ、OS ディスク、ギャラリーイメージ情報、OS の種類情報）が含まれます。`TemplateIsWindowsTemplate`を **True** に設定することで、OS の種類が Windows であることを示します。`TemplateIsWindowsTemplate`を **False** に設定することで、OS の種類が Linux であることを示します。

> ヒント:
>
> PowerShell プロパティ`TemplateIsWindowsTemplate`によって表示される情報は、Azure API から取得されます。このフィールドが空の場合があります。たとえば、OS の種類をスナップショットから取得できないため、データディスクからのスナップショットには`TemplateIsWindowsTemplate`フィールドが含まれません。

たとえば、PowerShell を使用して Windows OS の種類の Azure VM パラメーター`AdditionData`を **True** に設定します:

```
PS C:\Users\username> (get-item XDHyp:\HostingUnits\mynetwork\image.
    folder\username-dev-testing-rg.resourcegroup\username-dev-tsvda.vm).
    AdditionalData
Key Value
ServiceOfferingDescription Standard_B2ms
```



```
HardDiskSizeGB 127
ResourceGroupName FENGHUAJ-DEV-TESTING-RG
ServiceOfferingMemory 8192
ServiceOfferingCores 2
TemplateIsWindowsTemplate True
ServiceOfferingWithTemporaryDiskSizeInMb 16384
SupportedMachineGenerations Gen1,Gen2
<!--NeedCopy-->
```

Azure 仮想マシン、管理対象ディスク、スナップショット、**Azure VHD**、および **ARM** テンプレートのリージョン名情報を取得

Azure 仮想マシン、管理対象ディスク、スナップショット、Azure VHD、および ARM テンプレートのリージョン名情報を表示できます。この情報は、マシンカタログが割り当てられている場合に、マスターイメージ上のリソースに関して表示されます。`RegionName`という PowerShell プロパティは、`AdditionalData`パラメーターを指定して PowerShell コマンドを実行すると、リージョン名情報を表示します。

たとえば、次の PowerShell コマンドを使用して、Azure の仮想マシン情報を取得します。

```
PS C:\Windows\system32> (get-item XDHyp:\HostingUnits\myAzureNetwork\
    image.folder\hu-dev-testing-rg.resourcegroup\hu-dev-tsvda.vm).
    AdditionalData
Key Value
HardDiskSizeGB 127
ResourceGroupName HU-DEV-TESTING-RG
RegionName East US
TemplateIsWindowsTemplate True
LicenseType
ServiceOfferingDescription Standard_B2ms
ServiceOfferingMemory 8192
ServiceOfferingCores 2
SupportedMachineGenerations Gen1,Gen2
ServiceOfferingWithTemporaryDiskSizeInMb 16384
SecurityType
SecureBootEnabled
VTpmEnabled
<!--NeedCopy-->
```

MCS によって作成されたリソースの特定

以下は、MCS が Azure プラットフォームのリソースに追加するタグです。表のタグは、「” キー”:” 値”」として表示されます。

リソース名	タグ
ID ディスク	“CitrixProvisioningSchemeId” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource” : “Internal”
イメージ	“CitrixProvisioningSchemeId” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource” : “Internal”
NIC	“CitrixProvisioningSchemeId” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource” : “Internal”
OS ディスク	“CitrixProvisioningSchemeId” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource” : “Internal”
準備 VM	“CitrixProvisioningSchemeId” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource” : “Internal”
公開されたスナップショット	“CitrixProvisioningSchemeId” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource” : “Internal”
リソースグループ	“CitrixResource” : “Internal” CitrixSchemaVersion: 2.0
ストレージアカウント	“CitrixProvisioningSchemeId” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixProvisioningSchemeId” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource” : “Internal”
カタログ内の VM	“CitrixProvisioningSchemeId” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource” : “Internal”
WBC ディスク	“CitrixProvisioningSchemeId” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource” : “Internal”

> 注:
>
> MCS によって作成されたリソースとして識別するために **CitrixResource** タグが追加されている場合、VM

> は Citrix インベントリに表示されません。タグを削除するか名前を変更すると、表示できるようになります。

タグの削除

カタログまたは 仮想マシンを作成すると、次のリソースにタグが作成されます:

- リソースグループ
- 仮想マシン
- OS ディスク
- ID ディスク
- ネットワークインターフェイス
- ストレージアカウント

仮想マシンとマシンカタログを Citrix データベースから削除し、タグを削除できます。以下を使用できます:

- `Remove-ProvVM`を`ForgetVM`パラメーターとともに使用して、マシンカタログの単一の仮想マシンまたは仮想マシンの一覧から仮想マシンとタグを削除します。
- `Remove-ProvScheme`を`ForgetVM`パラメーターとともに使用して、Citrix データベースから単一のマシンカタログを削除し、マシンカタログ全体からタグを削除します。

この機能は、永続的な仮想マシンにのみ適用されます。

これを行うには、以下の手順に従います:

1. **PowerShell** ウィンドウを開きます。
2. **asnp citrix*** を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. `Remove-ProvVM`を実行して、Citrix データベースから仮想マシンを削除し、仮想マシンからタグを削除します。
   例:

```
1 Remove-ProvVM -ProvisioningSchemeName “ProvisioningSchemeName” -
    VMName “vmname” -ForgetVM
2 <!--NeedCopy-->
```

4. `Remove-ProvScheme`を実行して、Citrix データベースからマシンカタログを削除し、マシンカタログからタグを削除します。例:

```
1 Remove-ProvScheme -ProvisioningSchemeName “ProvisioningSchemeName
    ” -ForgetVM
2 <!--NeedCopy-->
```

> 注:
>
> `Remove-ProvScheme`で`ForgetVM`パラメーターを使用した後、プロビジョニングスキームが独自のリソースグループ（BYORG）または Citrix 管理のリソースグループのいずれかに存在する場合、

> MCS は基本ディスクのスナップショットを含むすべてのスナップショットを削除します。

追加情報

- 接続とリソースの作成と管理
- Microsoft Azure への接続
- マシンカタログの作成
- Microsoft Azure カタログの作成
- マシンカタログの管理

Microsoft System Center Virtual Machine Manager カタログの管理

January 25, 2024

「マシンカタログの管理」では、マシンカタログを管理するウィザードについて説明します。次の情報は、Microsoft System Center Virtual Machine Manager（VMM）仮想化環境に固有の詳細について説明しています。

> 注:
>
> VMM カタログを管理する前に、VMM カタログの作成を完了する必要があります。「Microsoft System Center Virtual Machine Manager カタログの作成」を参照してください。

MCS によって作成されたリソースの特定

以下は、MCS が SCVMM プラットフォームのリソースに追加するタグです。表のタグは、「” キー” :” 値”」として表示されます。

リソース名	タグ
準備用の仮想マシン	Tag string: “CitrixProvisioningSchemeId” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” Custom property entry: “XdConfig:” XdProvisioned=True”
カタログ内の VM	Tag string: “CitrixProvisioningSchemeId” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” Custom property entry: “XdConfig:” XdProvisioned=True”

追加情報

- 接続とリソースの作成と管理
- Microsoft System Center Virtual Machine Manager への接続
- マシンカタログの作成
- Microsoft System Center Virtual Machine Manager カタログの作成
- マシンカタログの管理

VMware カタログの管理

June 12, 2024

「マシンカタログの管理」では、マシンカタログを管理するウィザードについて説明します。以下の情報は、VMware 仮想化環境に固有の詳細について説明しています。

> 注:
>
> VMware カタログを管理する前に、VMware カタログの作成を完了する必要があります。「VMware カタログの作成」を参照してください。

マシンカタログのフォルダー ID の更新

`Set-ProvScheme`コマンドのカスタムプロパティで`FolderId`を指定することにより、MCS マシンカタログのフォルダー ID を更新できます。フォルダー ID の更新後に作成された仮想マシンは、この新しいフォルダー ID の下に作成されます。このプロパティが`CustomProperties`で指定されていない場合、仮想マシンはマスターイメージが配置されているフォルダーの下に作成されます。

マシンカタログのフォルダー ID を更新するには、次の手順を実行します。

1. Web ブラウザーを開き、**vSphere Web Client** の URL を入力します。
2. 資格情報を入力し、[**Login**] をクリックします。
3. **vSphere Web Client** で仮想マシンを配置するフォルダーを作成します。
4. PowerShell ウィンドウを開きます。
5. **asnp citrix*** を実行し、Citrix 固有の PowerShell モジュールをロードします。
6. `Set-ProvScheme`の`CustomProperties`に`FolderID`を指定します。この例では、フォルダー ID の値は`group-v2406`です。


```
Set-ProvScheme -ProvisioningSchemeUid "50bb319c-2e83-4a37-9ea1-94
    f630687372" -CustomProperties "<CustomProperties xmlns=""http
    ://schemas.citrix.com/2014/xd/machinecreation"" xmlns:xsi=""
    http://www.w3.org/2001/XMLSchema-instance""><Property xsi:type=
    ""StringProperty"" Name=""FolderId"" Value=""group-v2406"" /></
    CustomProperties>"
<!--NeedCopy-->
```

7. Studio を使用して仮想マシンをマシンカタログに追加します。
8. vSphere Web Client で新しい仮想マシンを確認します。新しい仮想マシンは、新しいフォルダーの下に作成されます。

PowerShell コマンドを使用してフォルダー **ID** を検索する

Powershell コマンド`Get-HypConfigurationDataForItem`を使用して、VMware ハイパーバイザー内の既存フォルダーのフォルダー ID を検索できます。

VMware Hypervisor に対し、ホスト接続およびリソースのグループを 1 つ作成します。次に、以下の手順を実行して、そのハイパーバイザー内のフォルダーのフォルダー ID を検索します。

1. vm フォルダーツリーのルートへの`XDHyp`のパスを決定します。例:

```
XDHyp:\Connections\VMwareConn\Datacenter.datacenter
<!--NeedCopy-->
```

2. `Get-HypConfigurationDataForItem`を使用してツリー構造を取得します。例:

```
Get-HypConfigurationDataForItem -LiteralPath XDHyp:\Connections\
    VMwareConn\Datacenter.datacenter
<!--NeedCopy-->
```

3. 次のコマンドを実行して、出力 XML からフォルダー ID を検索します。この例では、XML 出力から`ExampleFolder`のフォルダー ID を検索しています。

```
$result = Get-HypConfigurationDataForItem -LiteralPath XDHyp:\
    Connections\VMwareConn\Datacenter.datacenter
$result.VmPlacementFolder
<!--NeedCopy-->
```

XML 出力:

```
<?xml version="1.0" encoding="utf-16"?>
<CtxVmPlacementFolder xmlns:xsd="http://www.w3.org/2001/XMLSchema"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Name>vm</Name>
<Id>group-v4</Id>
<SubFolder>
<CtxVmPlacementFolder>
  <Name>vCLS</Name>
```



```
    <Id>group-v75</Id>
    <SubFolder />
  </CtxVmPlacementFolder>
  <CtxVmPlacementFolder>
    <Name>MyOtherFolder</Name>
    <Id>group-v1110</Id>
    <SubFolder />
  </CtxVmPlacementFolder>
  <CtxVmPlacementFolder>
    <Name>ExampleFolder</Name>
    <Id>group-v4658</Id>
    <SubFolder />
  </CtxVmPlacementFolder>
  </SubFolder>
  </CtxVmPlacementFolder>
  <!--NeedCopy-->
```

vSphere でフォルダー **ID** を確認

任意の ESXi または vCenter サーバーシステムで MOB にアクセスして、VM のフォルダー ID を見つけます。

管理対象オブジェクトブラウザ（MOB）は、すべての ESX/ESXi および vCenter サーバーシステムに組み込まれている、Web ベースのサーバーアプリケーションです。この vSphere ユーティリティを使用すると、VM、データストア、リソースプールなどのオブジェクトに関する詳細情報を表示できます。

1. Web ブラウザーを開き、`http://x.x.x.x/mob`と入力します。ここで x.x.x.x は、vCenter Server の、または ESX/ESXi ホストの IP アドレスです。例：https://10.60.4.70/mob。
2. MOB のホームページで、プロパティ **content** の値をクリックします。
3. **rootFolder** の値をクリックします。
4. **childEntity** の値をクリックします。
5. **vmFolder** の値をクリックします。
6. フォルダー ID は、**childEntity** の値で確認できます。

VM のストレージ移行

既存の VM のディスクストレージを古いストレージから新しいストレージに移動できます。移行中、MCS は電源管理、OS ディスクのリセットなどの VM 機能を保持します。新しいディスクストレージを使用して、新しい VM をマシンカタログに追加することもできます。これを行うには、PowerShell コマンド`Move-ProvVMDisk`を使用します。

現在、移行できるのは完全なクローンの永続的な VM のみです。

新しいストレージは次の条件を満たしている必要があります：

- 古いストレージの同じクラスター内にある必要があります。

- VM が実行されているホストは、古いデータストアと新しいデータストアの両方にアクセスできる必要があります。

次のタスクを実行できます:

- ディスクストレージの移行
- 古いストレージの廃止

ディスクストレージの移行

ディスクストレージを移行するには、以下の手順を実行します:

1. 新しいストレージを既存のホスティングユニットに追加します。古いストレージを **Superseded** に変更します。これを行う場合、[完全な構成] インターフェイスまたは PowerShell コマンドを使用できます。
   - [完全な構成] インターフェイスを使用する場合は、「ストレージの編集」を参照してください。
   - PowerShell コマンドを使用する場合:
     - `Add-Hyphostingunitstorage`を実行して、新しいストレージを既存のホスティングユニットに追加します。
     - `Set-Hyphostingunitstorage`で **Superseded** を「true」に設定して、古いストレージでの新しい VM の作成を無効にします。
2. VM をオフにして、メンテナンスモードをオンにします。
3. VM のディスクストレージを新しいストレージに移動し、ストレージ情報を更新します。例:

```
Move-ProvVMDisk -ProvisioningSchemeName "myFullCloneProvScheme" -
    VMName ("VMware-TestVM01", "VMware-TestVM02") -DiskType OS,
    Identity -DestinationStorageId datastore1,datastore1
<!--NeedCopy-->
```

4. 移行のタスク ID を取得します。例:

```
,(Get-ProvVM -ProvisioningSchemeName xxxxx) | Move-ProvVMDisk -
    ProvisioningSchemeName xxxxx -DiskType OS,Identity -
    DestinationStorageId datastore1,datastore1
<!--NeedCopy-->
```

5. 移行の状態を確認します。
   - `(Get-ProvTask -TaskID xxxxxxxxx).DiskMovedVirtualMachines`: 既に新しいストレージに移行されている VM を含む、ディスク移行が成功した VM の一覧を提供します。
   - `(Get-ProvTask -TaskID xxxxxxxxx).DiskMoveFailedVirtualMachines`: 移行に失敗した VM の一覧を提供します。
   - `(Get-ProvTask -TaskID xxxxxxxxx).NotStartedVirtualMachines`:移行がまだ開始されていない VM の一覧を提供します。

- `Get-ProvVM -ProvisioningSchemeName xxxxx -VMName "VMware -TestVM01`：移行後に更新された VM プロパティを提供します。`StorageId`、`AssignedImage`、`BootedImage`、`IdentityDiskId`、`IdentityDiskStorage`、および`LastBootTime`などのプロパティを確認します。

スナップショットを使用して MCS 作成の VM のディスクを移行した後、**VSphere Client** に統合が必要ですという警告が表示される場合があります。統合してデータの損失を回避するには、以下の手順を実行します：

1. VMware VM のバックアップを作成します。たとえば、すべての VM ファイルをデータストア上の別のフォルダーに転送します。
2. 警告が表示されたら、[**Consolidate**] をクリックし、[**OK**] をクリックして統合を確認します。

古いストレージの廃止

VM のディスク移行後に古いストレージを廃止するには、以下の手順を実行します：

1. ホスティングユニットの各ディスクストレージ内の基本ディスクとマシン数に関する情報を取得します。例：

```
$result=Get-ProvSchemeResourceInStorage -ProvisioningSchemeName
    xxxxx
$result
$result.ProvResourceInStorage | Format-List -Property *
<!--NeedCopy-->
```

   移行が成功すると、MCS は古い基本ディスクを自動的に削除するため、古いストレージにはマシンがなくなります。したがって、コマンドの実行後、古いストレージにマシンと基本ディスクが存在しないことを確認してください。

2. `Remove-Hyphostingunitstorage`を実行して、ホスティングユニットから古いストレージを完全に削除します。[完全な構成] インターフェイスを使用して古いストレージを削除することもできます。

MCS によって作成されたリソースの特定

以下は、MCS が VMware プラットフォームのリソースに追加するタグです。表のタグは、「” キー” :” 値”」として表示されます。

リソース名	タグ
準備用の仮想マシン	“CitrixProvisioningSchemeId” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “XdConfig:” XdProvisioned=True”
カタログ内の VM	“CitrixProvisioningSchemeId” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”

リソース名	タグ
	“XdConfig:” XdProvisioned=True”

追加情報

- 接続とリソースの作成と管理
- VMware への接続
- マシンカタログの作成
- VMware カタログの作成
- マシンカタログの管理

XenServer カタログの管理

January 25, 2024

「マシンカタログの管理」では、マシンカタログを管理するウィザードについて説明します。以下の情報は、XenServer 仮想化環境に固有の詳細について説明しています。

> 注:
>
> XenServer カタログを管理するには、その前に XenServer カタログの作成を完了しておく必要があります。「XenServer カタログの作成」を参照してください。

MCS によって作成されたリソースの特定

Machine Creation Services（MCS）は、ディスクなどのリソースを生成するときに、それらのリソースをより有効に活用するための ProvisioningScheme ID タグを割り当てます。

タグは、管理者がリソースをより適切に管理および整理できるようにするので、管理者にとって便利です。たとえば、未使用のディスクなどのリソースがタグ付けされていれば、管理者はリソースが作成された場所を簡単に特定できるため、クリーンアッププロセスを効率的に行うことができます。

以下は、MCS が XenServer プラットフォームのリソースに追加するタグです。表のタグは、「” キー” :” 値”」として表示されます。

リソース名	タグ
各ネットワークまたはローカルストレージ上のディスクのコピー（オンプレミスのみ）	“CitrixProvisioningSchemeId”：“xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
ID ディスク	“CitrixProvisioningSchemeId”：“xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
OS ディスク	“CitrixProvisioningSchemeId”：“xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
準備用の仮想マシン	“CitrixProvisioningSchemeId”：“xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
カタログ内の VM	“CitrixProvisioningSchemeId”：“xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
WBC ディスク	“CitrixProvisioningSchemeId”：“xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”

プロビジョニングスキームに関する情報の取得

プロビジョニングスキームに関する詳細情報を取得するには、次の PowerShell コマンドを実行します。以下のxxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxは、実際のプロビジョニングスキーム ID に置き換えてください：

1. プレースホルダー ID を実際のプロビジョニングスキーム ID に置き換える

```
$provisioningSchemeId = "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
<!--NeedCopy-->
```

2. プロビジョニングスキームに関する詳細情報を取得します：

```
Get-ProvisioningScheme -Id $provisioningSchemeId
<!--NeedCopy-->
```

MCS によって作成されたリソースのリストを取得する

次のコマンドを実行して、MCS によって作成されたリソースを網羅したリストを取得します。

1. プレースホルダー ID を実際のプロビジョニングスキーム ID に置き換えます。

```
$provisioningSchemeId = "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
<!--NeedCopy-->
```

2. MCS によって作成されたすべてのリソースのリストを取得します。

```
Get-ProvResource -ProvisioningSchemeUid $provisioningSchemeId |
    ConvertTo-JSON -Depth 6
```



```
<!--NeedCopy-->
```

実行後、次の出力が得られます:

- プロビジョニングスキームの名前と ID。
- プロビジョニングスキームに含まれているプロビジョニングイメージのバージョンのリスト。各エントリには次の内容が含まれます:
  - イメージ名とイメージ ID。
  - ディスクのディスク ID とストレージ ID。
- プロビジョニング VM のリスト。各エントリには次の内容が含まれます:
  - OS ディスクの OS ディスク ID と親ディスク ID。
  - OS ディスクのストレージ ID。
  - ID ディスクとそのストレージ ID。

追加情報

- 接続とリソースの作成と管理
- XenServer への接続
- マシンカタログの作成
- XenServer カタログの作成
- マシンカタログの管理

電源管理

December 5, 2023

Citrix DaaS を使用すると、サポートされているさまざまなハイパーバイザーやクラウドサービスにわたって、MCS でプロビジョニングされた VM の電源管理を行うことができます。電源管理操作により、次のことが可能になります:

- 最適なユーザーエクスペリエンス
- コスト管理と省電力

利用可能な電源操作は次のとおりです:

- 起動
- シャットダウン
- 再起動
- 一時停止
- 再開

- 強制再起動
- 強制シャットダウン

> 注:
>
> - 非永続的な VM の場合は、電源サイクル（シャットダウン/起動および再起動）により、OS ディスクがリセットされます。
> - 電源操作の機能と動作は、ハイパーバイザーまたはクラウドサービスによって異なります。

この記事では、サポートされている特定のハイパーバイザーに関連する主要な電源管理機能について説明します。

- AWS VM の電源管理
- Azure VM の電源管理

AWS VM の電源管理

May 17, 2024

必要な権限については、「AWS 権限について」を参照してください。

インスタンスの休止

休止プロセスでは、インスタンスの状態がプライベート IP アドレスおよび Elastic IP アドレスとともにメモリ内に保存されるので、中断したところから正確に再開できます。

休止するように指示したインスタンスは、ルート EBS ボリューム内のファイルにメモリ内の状態を書き込み、その後、自身をシャットダウンします。Amazon EBS ボリュームは、インスタンスに接続できる、耐久性のあるブロックレベルのストレージデバイスです。インスタンスに接続した後のボリュームは、物理ハードドライブを使用するのと同じように使用できます。インスタンスのルート EBS ボリュームを暗号化します。暗号化により、メモリから EBS ボリュームにコピーされた機密データが適切に保護されるようになります。EBS 暗号化について詳しくは、「Amazon EBS 暗号化」を参照してください。

サポートされているインスタンスの休止に関する制限は、次のとおりです:

- 最大 150GB までのインスタンスメモリ（RAM）だけがサポートされます。
- UEFI ブートモードはサポートされていません。
- 汎用 SSD とプロビジョンド IOPS SSD は、EBS ボリュームタイプとしてのみサポートされます。

休止をサポートする **VM** の作成

休止をサポートする VM を作成するには:

1. ホスト接続を作成します。「AWS への接続」を参照してください。
2. EBS ルートを暗号化して **Stop-Hibernate** プロパティを有効にしたインスタンスを起動します。詳しくは、次のトピックを参照してください:
   - Instance lifecycle
   - Amazon EBS encryption
   - 休止状態の前提条件
   - インスタンスの休止の有効化
   - オンデマンドインスタンスまたはスポットインスタンスを休止状態にする
3. このインスタンスをマスターイメージとして使用して、AMI を作成します。
4. マスターイメージを準備します:
   a) マスターイメージに VDA をインストールします。最新の機能を利用できるように、最新バージョンをインストールすることを Citrix ではお勧めします。マスターイメージに VDA をインストールできないと、カタログ作成が失敗します。VDA のインストール方法について詳しくは、「VDA のインストール」を参照してください。
   b) アプリケーションとデスクトップがメンバーとなっているドメインにマスターイメージを統合します。マスターイメージが、仮想マシンを作成するホスト上で使用できることを確認してください。
5. そのインスタンスから AMI を作成します。インスタンスから AMI を作成する方法については、「Amazon EC2 インスタンスからの AMI の作成」を参照してください。
6. New-ProvScheme コマンドを使用してマシンカタログを作成します。カスタムプロパティ AwsCaptureInstanceProperties を **True** に設定します。[完全な構成] インターフェイスで AWS インスタンスのプロパティを有効にする方法については、「完全な構成インターフェイスでの AWS インスタンスのプロパティの適用および運用リソースのタグ付け」を参照してください。

```
New-ProvScheme  -AdminAddress "xxx" -CleanOnBoot
-CustomProperties "AwsCaptureInstanceProperties,true;"
-HostingUnitName "xxx" -IdentityPoolName $catalog_name -
   InitialBatchSizeHint 1
-MasterImageVM "xyz.template" -NetworkMapping @{
 "0"="XDHyp:\HostingUnits\MyConn\us-east-2a.availabilityzone
    \10.0.0.0``/24 (vpc-0f1771e45671aedcd).network" }

-ProvisioningSchemeName $catalog_name
-RunAsynchronously -Scope @() -SecurityGroup @("xxx") -
   ServiceOffering "xxx"
<!--NeedCopy-->
```

   PowerShell コマンドを使用してマシンカタログを作成する方法については、「https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/」を参照してください。

休止できる VM は、次の場合に作成されます:

- マスターイメージから作成された AMI のうち、**Stop-Hibernate** プロパティが有効になっている AMI を選択した場合
- マスター VM がドメインに参加しており、VDA がインストールされている場合
- 休止を処理できる正しい VM サイズ（サービスオファリング）を選択した場合

次の場合、**New-ProvScheme** コマンドは失敗し、該当するエラーメッセージが表示されます:

- マスター VM は休止が有効になっているが、サービスオファリングが休止を処理できない場合
- マスター VM がドメインに参加しておらず、VDA がインストールされていない場合

サービスオファリングと **AMI** の休止状態

サービスオファリングと AMI（テンプレート）の休止状態を表示するには、次のコマンドを実行します:

- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\WIN2016-ADDC-2021.09.10.145334-a1968709-10c4-47d5-9642-21e743159a7b(ami-0e6c5b33a52d2a6b6).template'`
- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\R6i Sixteen Extra Large Instance.serviceoffering'`

既存の休止でサポートされるプロビジョニングスキームに関するサービスオファリングの更新

1. `Set-ProvScheme`コマンドを実行します。例:

```
Set-ProvScheme -ProvisioningSchemeName <String> -ServiceOffering <String>
<!--NeedCopy-->
```

サービス提供に互換性がない場合、システムは例外メッセージを表示します。

休止状態をサポートするマシンカタログを作成する

マシンカタログを作成する場合、休止状態をサポートするマシンプロファイルを使用できます。

1. カタログ作成ウィザードでは、マシンプロファイルの選択まで指示に従います。
2. [マシンテンプレート] ページで、[マシンプロファイルを選択] をクリックしてマシンプロファイルを選択します。
3. [仮想マシン] ページで、編集アイコンをクリックして VM を選択します。

> 注:

> マシンプロファイルで休止状態が有効になっている場合、システムは休止状態にできる VM のみを表示します。

4. 画面の指示に従ってすべての設定を完了してください。［概要］ページには、カタログの休止状態が表示されます。

> 注:
>
> ［マシンカタログの編集］で、マシンプロファイルを休止状態が有効なプロファイルに変更すると、それに応じて VM を再構成するように求められます。

休止をサポートするマシンカタログの更新

休止をサポートしていないマシンカタログを使用して既存のマシンカタログを更新しようとすると、更新が失敗し、該当するエラーメッセージが表示されます。

休止状態の **VM** の電源管理

休止状態の VM に対して実行できる電源管理操作は、次のとおりです:

1. VM を実行状態から一時停止する。
2. VM を一時停止状態から再開する。
3. VM を一時停止状態から再起動する。

電源管理オプションを確認するには、［管理］**>**［完全な構成］インターフェイスで、休止状態の VM を右クリックします。

また、各 VM に対して実行する電源操作に応じて、VM の電源状態が一時停止中または一時停止として表示されます。

Azure VM の電源管理

June 12, 2024

必要な権限については、「必要な Azure 権限」を参照してください。

Azure のオンデマンドプロビジョニング

Azure のオンデマンドプロビジョニングでは、VM は、プロビジョニング完了後、Citrix DaaS で電源投入操作が開始されたときにのみ作成されます。

MCS を使用して Azure Resource Manager でマシンカタログを作成する場合、Azure のオンデマンドプロビジョニング機能は次のことを実現します:

- ストレージコストを削減する。
- カタログ作成を高速化する

MCS カタログを作成すると、Azure Portal にリソースグループ内のネットワークセキュリティグループ、ネットワークインターフェイス、基本イメージ、ID ディスクが表示されます。

Azure Portal では、Citrix DaaS が VM の電源投入操作を開始するまで、その VM は表示されません。次に、［完全な構成］インターフェイスの VM のステータスがオンに変わります。次のような違いがある 2 種類のマシンがあります:

- プールされたマシンの場合、オペレーティングシステムのディスクとライトバックキャッシュは、VM が存在する場合にのみ存在します。プールされたマシンをコンソールでシャットダウンすると、VM は Azure Portal に表示されません。マシンを定期的に（たとえば、勤務時間外に）シャットダウンすると、ストレージコストを大幅に節約できます。
- 専用マシンでは、VM の初回電源投入時にオペレーティングシステムのディスクが作成されます。Azure Portal の VM は、マシン ID が削除されるまでストレージに残ります。専用マシンをコンソールでシャットダウンすると、VM は引き続き Azure Portal に表示されます。

> 注:
>
> オンデマンドプロビジョニング機能（「レガシー」カタログ）が廃止される前に作成された Azure カタログのサポートは廃止されます。したがって、Azure レガシーカタログ VM を再作成してください。カタログはオンデマンドとしてプロビジョニングされるため、ストレージコストが節約されます。

電源を入れ直したときにプロビジョニングされた仮想マシンを保持する

電源を入れ直したときに、プロビジョニングされた仮想マシンを保持するかどうかを選択します。PowerShell パラメーター`New-ProvScheme CustomProperties`を使用します。このパラメーターではプロパティ`PersistVm`を追加することができ、これを使用して、電源を入れ直したときにプロビジョニングされた仮想マシンが保持されるかどうかを指定できます。`PersistVm`プロパティを **true** に設定して、電源がオフのときに仮想マシンが保持されるように設定するか、プロパティを **false** に設定して、電源がオフのときに仮想マシンが保持されないように設定します。

> 注:
>
> `PersistVm`プロパティは、`CleanOnBoot`および`UseWriteBackCache`のプロパティが有効なプロビジョニングスキームにのみ適用されます。非永続仮想マシンに`PersistVm`プロパティが指定されていない場合、非永続仮想マシンは電源がオフのときに Azure 環境から削除されます。

次の例では、`New-ProvScheme CustomProperties`パラメーターで`PersistVm`プロパティが **true** に設定されています:


```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageType" Value="
   Standard_LRS" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
   />
<Property xsi:type="StringProperty" Name="PersistVm" Value="true" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="demo-
   resourcegroup" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
   Windows_Client" />
</CustomProperties>
<!--NeedCopy-->
```

次の例では、New-ProvScheme CustomPropertiesパラメーターでPersistVMを **true** に設定することで、ライトバックキャッシュが維持されます:

```
 New-ProvScheme
 -AzureAdJoinType "None"
 -CleanOnBoot
 -CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
    /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
    XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
    UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
    StringProperty`" Name=`"StorageType`" Value=`"Standard_LRS`" /><
    Property xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"
    false`" /><Property xsi:type=`"StringProperty`" Name=`"
    PersistOsDisk`" Value=`"true`" /><Property xsi:type=`"
    StringProperty`" Name=`"PersistVm`" Value=`"true`" /><Property xsi:
    type=`"StringProperty`" Name=`"ResourceGroups`" Value=`"demo-
    resourcegroup`" /><Property xsi:type=`"StringProperty`" Name=`"
    LicenseType`" Value=`"Windows_Client`" /></CustomProperties>"
 -HostingUnitName "demo"
 -IdentityPoolName "NonPersistent-MCSIO-PersistVM"
 -MasterImageVM "XDHyp:\HostingUnits\demo\image.folder\scale-test.
    resourcegroup\demo-snapshot.snapshot"
 -NetworkMapping @ {
 "0"="XDHyp:\HostingUnits\demo\virtualprivatecloud.folder\East US.
    region\virtualprivatecloud.folder\ji-test.resourcegroup\jitest-vnet
    .virtualprivatecloud\default.network" }

-ProvisioningSchemeName "NonPersistent-MCSIO-PersistVM"
 -ServiceOffering "XDHyp:\HostingUnits\demo\serviceoffering.folder\
    Standard_B2ms.serviceoffering" -UseWriteBackCache
 -WriteBackCacheDiskSize 127
 -WriteBackCacheMemorySize 256
 <!--NeedCopy-->
```


> ヒント:
>
> PersistVmプロパティは、プロビジョニングされた仮想マシンを保持するかどうかを決定します。PersistOsdiskプロパティは、OS ディスクを永続化するかどうかを決定します。プロビジョニングされた仮想マシンを保持するには、最初に OS ディスクを保持します。仮想マシンを削除してからでないと、OS ディスクを削除することはできません。PersistVmパラメーターを指定せずにPersistOsdiskプロパティを使用することができます。

ストレージの種類の変更に失敗したときの電源投入時の動作をカスタマイズする

電源をオンにした際に、Azure での障害が原因で、管理対象ディスクのストレージの種類が目的の種類に変更されないことがあります。この場合、VM はオフのままになり、エラーメッセージが送信されます。ただし、設定した種類にストレージを復元できない場合でも、VM の電源をオンにするか、VM の電源をオフのままにするかを選択できます。

- カスタムプロパティのFailSafeStorageTypeを **true**（デフォルト設定）にするか、New-ProvSchemeまたはSet-ProvSchemeコマンドで値を指定しない場合:
  - 電源投入時、VM が正しくないストレージの種類でオンになります。
  - シャットダウン時、VM が正しくないストレージの種類でオフのままになります。
- New-ProvSchemeまたはSet-ProvSchemeコマンドでカスタムプロパティのFailSafeStorageTypeを **false** にした場合:
  - 電源投入時、VM が正しくないストレージの種類でオフのままになります。
  - シャットダウン時、VM が正しくないストレージの種類でオフのままになります。

カスタムプロパティのFailSafeStorageTypeを含むマシンカタログを作成します:

1. PowerShell ウィンドウを開きます。
2. asnp citrix*を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. ID プールをまだ作成していない場合は作成します。
4. New-ProvSchemeにカスタムプロパティを追加します。例:

```
1 New-ProvScheme -HostingUnitName "Azure-Resources-1" -
     IdentityPoolName "name" -InitialBatchSizeHint 1
2 -MasterImageVM "XDHyp:\HostingUnits\Azure-Resources-1\image.folder
     \abc.resourcegroup\def.snapshot"
3 -NetworkMapping @{
4  "0"="XDHyp:\HostingUnits\Azure-Resources-1\ght.folder\abc.
      resourcegroup\abc-vnet.virtualprivatecloud\default.network" }
5
6 -ProvisioningSchemeName "name"
7 -ServiceOffering "XDHyp:\HostingUnits\Azure-Resources-1\
     serviceoffering.folder\Standard_DS2_v2.serviceoffering"
```



```
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"StorageType`" Value=`"Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageTypeAtShutdown`" Value=`"Standard_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`" Value=`"true`" />
</CustomProperties>"
<!--NeedCopy-->
```

5. マシンカタログを作成します。Remote PowerShell SDK を使用してカタログを作成する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/を参照してください。

既存のマシンカタログを更新してカスタムプロパティのFailSafeStorageTypeを含めるようにします。この更新は、既存の VM には影響しません。

1. Set-ProvSchemeコマンドでカスタムプロパティを更新します。例:

```
Set-ProvScheme -ProvisioningSchemeName <String> -CustomProperties "
<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"StorageType`" Value=`"Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"IdentityDiskStorageType`" Value=`"Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`" Value=`"false`" />
</CustomProperties>"
<!--NeedCopy-->
```

Set-ProvScheme で行った変更を既存の VM に適用するには、Request-ProvVMUpdateコマンドを実行します。

1. Request-ProvVMUpdate コマンドを実行します。例:

```
Request-ProvVMUpdate -ProvisioningSchemeName <String> -VMName <List-Of-Vm-Names>
<!--NeedCopy-->
```

2. VM を再起動します。

休止状態対応 **VM** の作成

Azure 環境では、休止状態をサポートする MCS マシンカタログを作成できます。この機能を使用すると、VM を一時停止し、ユーザーが再度サインインしたときに VM の以前の状態に再接続できます。

休止状態機能は以下に適用されます:

- シングルセッション OS
- 永続的および非永続的な VM
- 静的およびランダム（プール）VDI デスクトップ

VDI デスクトップが静的かランダムかに関係なく、VM を休止状態にした後に同じセッションを再開できます。

このセクションでは、以下を参照してください:

- 前提条件
- 制限事項
- 休止状態対応マシンカタログを作成および管理する
- 既存の休止状態対応 VM のマシンカタログを作成する
- MCS でプロビジョニングされた既存の VM で休止状態を有効にする
- 休止状態のプロパティを確認する
- VM の電源管理（手動および自動）

休止状態を使用するための前提条件

休止状態を使用するには、次のタスクを必ず完了してください:

- Windows と Linux の両方のマスターイメージに Azure VM エージェントをインストールします。Windows イメージのページファイルは一時ディスク上に置くことができます。マシンカタログで休止状態が有効になっている場合、MCS はページファイルの場所を基本ディスクの「C:」ドライブに設定します。
- MCS は、生成されたリソースの休止状態プロパティを自動的に設定します。休止状態をサポートするためにマスターリソースのプロパティを構成する必要はありません。
- 休止状態をサポートする VM サイズをサブスクリプションで使用します。
- VM が休止機能を継承できるように、休止状態対応マシンプロファイル（VM またはテンプレートスペック）を作成します。VM を作成するには、「休止機能の使用を開始する」を参照してください。

  > 注:
  >
  > Microsoft については、休止状態が有効な VM を OS ディスクから展開できます。この機能は現在、特定のリージョンでサポートされており、間もなくすべてのリージョンで利用できるようになる予定です。詳しくは、「休止機能が有効な VM を OS ディスクからデプロイする」を参照してください。

  テンプレートスペックを作成するには、次の手順を実行します:

  1. Azure Portal を開きます。テンプレートで使用する構成の VM を選択します。左側のペインで ［テンプレートのエクスポート］を選択します。
  2. ［パラメーターを含める］チェックボックスをオフにします。コンテキストをコピーし、JSON ファイルとして保存します（例: `VMExportTemplate.json`）。

3. テンプレートのパラメーター`hibernationEnabled`が**`true`**であることを確認してください。パラメーターが**`true`**ではない場合は、使用した VM 構成を確認してください。サポートされる VM サイズをテンプレートファイルで指定できます。ただし、カタログの作成時にマシンのサイズを指定することもできます。
4. ネットワークインターフェイスリソースのテンプレートを JSON ファイル`VMExportTemplate.json`に追加します。その結果、2 つのリソースを持つ ARM テンプレートファイルが作成されます。
5. [**Azure Portal**] **>** [テンプレートスペック] **>** [テンプレートのインポート] **>** [ローカルテンプレートファイルを選択] を選択して、このテンプレートファイルを ARM テンプレートスペックとしてインポートします。
6. ARM テンプレートスペックを作成したら、マシンプロファイルとして使用できます。

> 注:
>
> Citrix Studio と同期するまでに数分かかる場合があります。

詳しくは、Microsoft のドキュメント「休止状態を使用するための前提条件」を参照してください。

制限事項

- シングルセッション OS マシンカタログ（永続的および非永続的）のみがサポートされます。
- エフェメラル OS ディスクと MCS I/O 機能は Azure の休止状態をサポートしていません。
- Windows の自動更新中に休止機能が失敗する場合があります。

詳しくは、Microsoft のドキュメントを参照してください。

休止状態対応マシンカタログを作成および管理する

休止状態対応 VM を作成するために、以下を使用して休止状態対応マシンカタログを作成および管理できます:

- 完全な構成インターフェイス、または
- PowerShell コマンド

完全な構成インターフェイスを使用してカタログを作成する

1. Citrix Cloud にサインインします。左上のメニューで、[マイサービス] **>** [**DaaS**] を選択します。
2. [管理] **>** [完全な構成] の左側ペインで [マシンカタログ] を選択します。
3. [マシンカタログの作成] を選択します。カタログ作成ウィザードが開きます。
4. [マシンの種類] ページで、このカタログのマシンの種類 [シングルセッション **OS**] を選択します。
5. [マシン管理] ページで、次のように設定を選択します:

a) 電源管理されているマシン（仮想マシン、ブレード **PC** など）を選択します。
b) ［**Citrix Machine Creation Services**（**MCS**）］を選択します。

6. ［デスクトップエクスペリエンス］ページで、必要に応じてランダムまたは静的なデスクトップエクスペリエンスを選択します。
7. ［イメージ］ページで、マスターイメージを選択します。［マシンプロファイルを使用する］チェックボックスを選択し、休止状態をサポートするマシンプロファイルを選択します。ヒントをクリックすると、マシンプロファイルが休止状態をサポートしているかどうかがわかります。
8. ［ストレージとライセンスの種類］ページで、このカタログに使用するストレージとライセンスを選択します。
9. ［仮想マシン］ページで、仮想マシンの数、仮想マシンのサイズ、およびアベイラビリティ ゾーンを選択します。

> 注:
>
> 休止状態をサポートするマシンサイズは、選択のためにのみ表示されます。GPU VM シリーズは Technical Preview 段階です。

10. ［**NIC**］ページで、仮想マシンで使用する NIC を追加します。
11. ［ディスク設定］ページで、ライトバックキャッシュディスクのストレージの種類とサイズを選択します。
12. ［リソースグループ］ページで、仮想マシンをプロビジョニングするリソースグループを選択します。
13. ［マシン **ID**］ページで、［新しい **Active Directory** アカウントを作成する］を選択します。次に、アカウントの名前付けスキームを指定します。
14. ［ドメイン資格情報］ページで、［資格情報の入力］をクリックします。ドメイン資格情報を入力して、ターゲットの Active Directory ドメインでアカウント作成を実行します。
15. ［概要］ページで、マシンカタログの名前を入力し、［完了］をクリックします。

MCS マシンカタログの作成が完了したら、カタログ一覧でカタログを見つけて、［テンプレートのプロパティ］タブをクリックします。パラメーター **Hibernation** の値は **Supported** である必要があります。

マシンカタログを編集する場合は、次の制限を考慮してください:

- 現在のマシンカタログが休止状態をサポートしている場合、次のことはできません:
  - VM サイズを休止状態に対応しないサイズに変更する。
  - マシンプロファイルを休止状態に対応しないプロファイルに変更する。
- 現在のマシンカタログが休止状態をサポートしていない場合、次のことはできません:
  - ［完全な構成］インターフェイスを使用してマシンプロファイルを休止状態対応プロファイルに変更すること。ただし、これは PowerShell コマンドを使用して行うことができます。「MCS でプロビジョニングされた既存の VM で休止状態を有効にする」を参照してください。

既存の休止状態対応の **VM** を管理するためのマシンカタログを作成する　既に休止状態対応の VM があり、それらを一時停止して再開したい場合は、マシンカタログを作成して、電源管理のためにそれらの VM をインポートします。

> 注:
>
> 休止状態対応の VM と休止状態に対応できない VM の両方を含むマシンカタログを作成できます。ただし、休止状態関連の機能が必要な場合は、休止状態対応の VM のみを含むマシンカタログを作成する必要があります。

[完全な構成] インターフェイスを使用して既存の休止状態対応の VM のカタログを作成するには、画面上の指示に従って手順を完了し、次の主要な設定に注意してください:

1. [マシン管理] ページで、[電源管理されているマシン] を選択し、マシンを展開する方法として [ほかのサービスまたはテクノロジ] を選択します。
2. [仮想マシン] ページで、休止状態対応の VM のみを追加またはインポートします。

PowerShell コマンドを使用してマシンカタログを作成する　休止状態を使用するための要件をすべて満たしたら、`New-ProvScheme`コマンドを使用して休止状態対応のマシンカタログを作成できます。Remote PowerShell SDK を使用してカタログを作成する方法については、「Manage Citrix DaaS using Remote PowerShell SDKs」を参照してください。

カタログの作成中に、次の PowerShell コマンドを使用して、VM サイズとマシンプロファイルが休止状態をサポートしているかどうかを確認できます:

- VM サイズについては、次のコマンドを実行し、プロパティ`supportsHibernation`が **True** であるかどうかを確認します。例:

```
Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\ <
    VirtualNetwork> \serviceoffering.folder") | select Name,
    AdditionalData | ConvertTo-Json
<!--NeedCopy-->
```

- マシンプロファイルについては、次のコマンドを実行し、プロパティ`supportsHibernation`が **True** であるかどうかを確認します。例:

```
Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\ <
    VirtualNetwork> \machineprofile.folder\abc.resourcegroup")|
    select Name, AdditionalData|ConvertTo-Json
<!--NeedCopy-->
```

マシンカタログを編集する場合は、次の制限を考慮してください:

- 現在のマシンカタログが休止状態をサポートしている場合、次のことはできません:
  - VM サイズを休止状態に対応しないサイズに変更する
  - マシンプロファイルを休止状態に対応しないプロファイルに変更する
- 現在のマシンカタログが休止状態をサポートしていない場合、次のことはできません:

- ［完全な構成］インターフェイスを使用してマシンプロファイルを休止状態対応プロファイルに変更すること。ただし、これは PowerShell コマンドを使用して行うことができます。「MCS でプロビジョニングされた既存の VM で休止状態を有効にする」を参照してください。

Remote PowerShell SDK を使用してカタログの VM サイズとマシンプロファイルを変更する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Set-ProvScheme/を参照してください。

MCS でプロビジョニングされた既存の VM で休止状態を有効にする

以下の既存のもので Azure 休止状態を有効にできます:

- 一時ディスクを使用せずに作成された、Windows MCS によってプロビジョニングされたマシンカタログの VM。
- 一時ディスクを使用して、または使用せずに作成された、Linux MCS によってプロビジョニングされたマシンカタログの VM。

> 注:
>
> - MCS によってプロビジョニングされた既存の VM には、Azure VM エージェントがインストールされている必要があります。
> - 現在、この機能を有効にするには PowerShell コマンドのみを使用できます。

これを行うには、以下の手順に従います:

1. **PowerShell** ウィンドウを開きます。
2. `asnp citrix*`を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. 既存のマシンの構成を確認します。例:

```
Get-ProvScheme | select ProvisioningSchemeName,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

4. `Set-ProvScheme`コマンドを使用して、このマシンカタログで休止状態を有効にします。例:

```
Set-ProvScheme -provisioningSchemeName xxxx
-machineprofile <path-to-machineprofile-with-hibernation-enabled>
-serviceoffering "XDHyp:\HostingUnits\msc-dev\serviceoffering.
    folder\Standard_D4as_v5.serviceoffering"
<!--NeedCopy-->
```

5. マシンカタログ内の既存の VM で更新を要求します。

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeUid xxxx -VMName <
    String[]
<!--NeedCopy-->
```


6. VM を再起動して、既存の VM での更新をトリガーします。例:

```
New-BrokerHostingPowerAction -machinename "<name>" -Action Restart
<!--NeedCopy-->
```

休止状態のプロパティを確認する

PowerShell コマンドを使用して、マシンカタログ、VM、およびブローカーマシンの休止状態プロパティを確認できます:

- プロビジョニングスキームの休止状態プロパティを確認するには、次の PowerShell コマンドを実行します。`HibernationEnabled` パラメーターは`True`である必要があります。

```
(Get-ProvScheme -provisioningSchemeName <YourSchemeName>).
   VMMetadata -join "" |  ConvertFrom-Json | Select
   HibernationEnabled
<!--NeedCopy-->
```

- プロビジョニング VM の休止状態プロパティを確認するには、次の PowerShell コマンドを実行します。`SupportsHibernation` パラメーターは`True`である必要があります。

```
(Get-ProvVM -VMName <YourVMName>).CustomVmData | ConvertFrom-Json
    | Select SupportsHibernation
<!--NeedCopy-->
```

- ブローカーマシンの休止状態を確認するには、次の PowerShell コマンドを実行します。電源操作の ［一時停止］および ［再開］は休止機能を示します。

```
(Get-BrokerMachine -MachineName <YourMachineName>).
   SupportedPowerActions
<!--NeedCopy-->
```

休止状態対応の **VM** の電源管理

休止状態対応の VM に対して実行できる電源管理操作は、次のとおりです:

- VM を実行状態から一時停止にする
- VM を一時停止状態から再開する
- VM を一時停止状態から強制的にシャットダウンする
- VM を一時停止状態から強制的に再起動する

詳しくは、以下を参照してください:

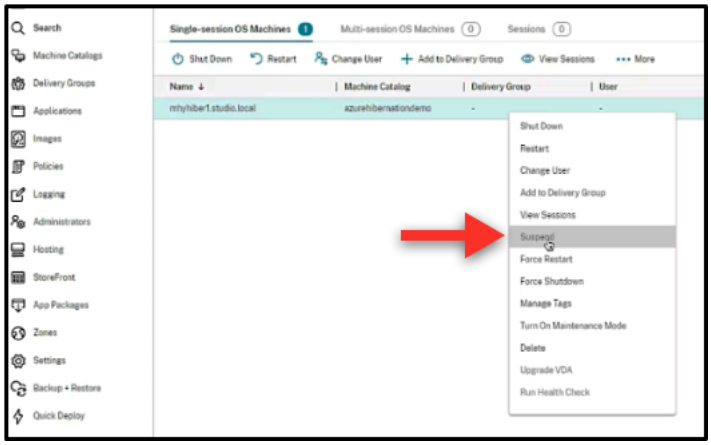
- 一時停止
- 再開

一時停止　次のいずれかの方法を使用して VM を一時停止できます：

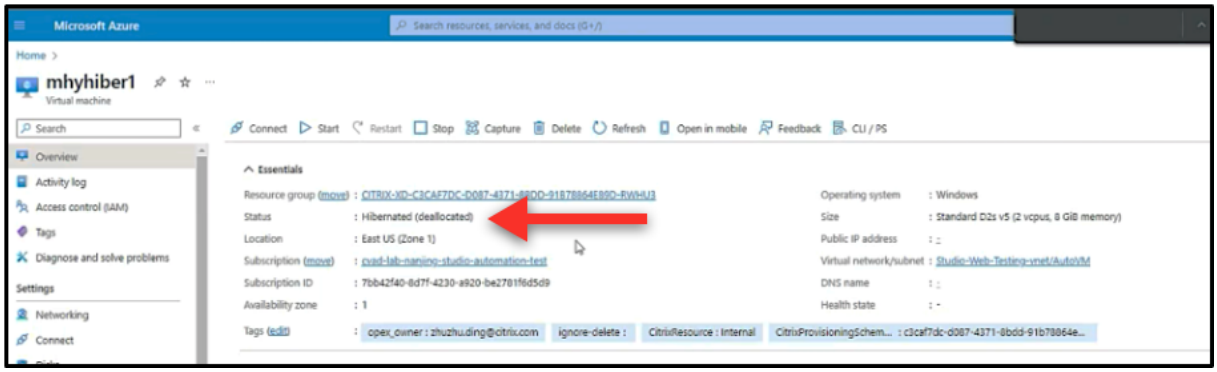
- ［完全な構成］インターフェイスを使用して手動で行う
- タイムアウトポリシーを使用して自動的に行う：詳しくは、「その他の設定」を参照してください。

VM を手動で一時停止するには：

1. VM を右クリックし、［一時停止］を選択します。［はい］をクリックしてアクションを確認します。［電源の状態］が ［一時停止中］から ［一時停止］に変わります。

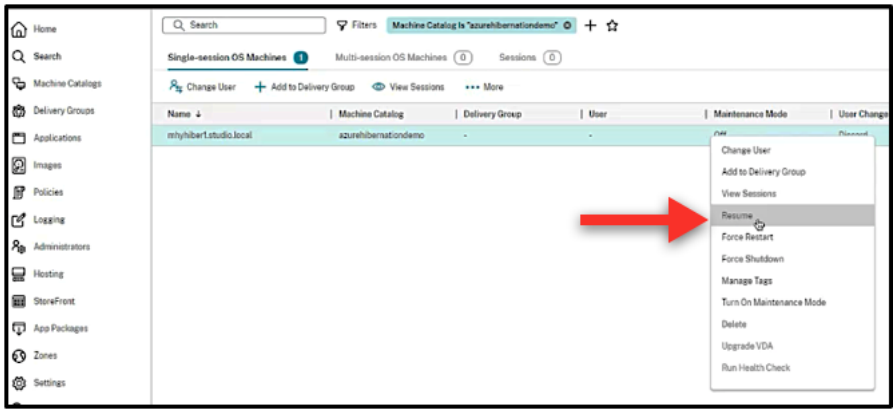


Azure Portal で VM のステータスを確認できます。

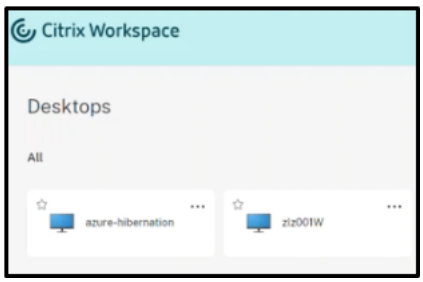


再開　休止状態の VM を再開するには、次のいずれかの方法を使用します：

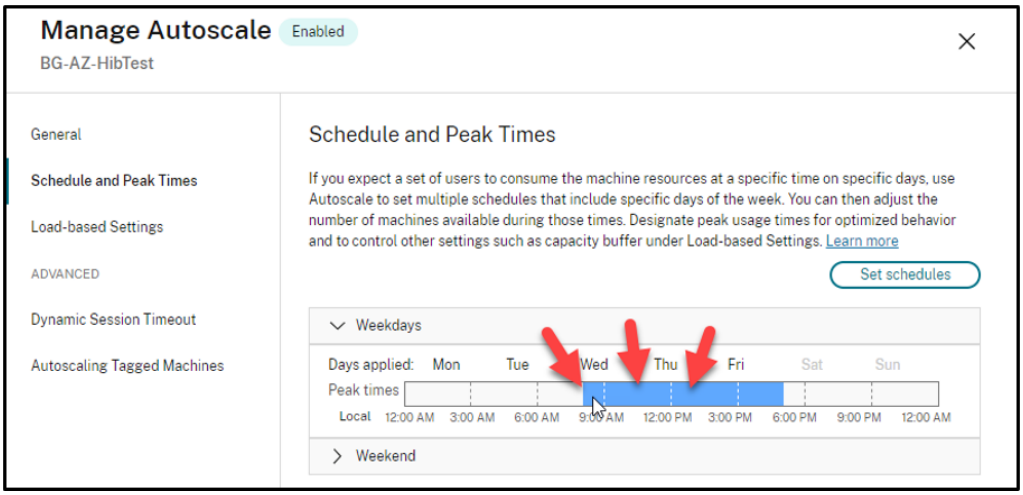
- 手動：
  - 管理者は、［完全な構成］インターフェイスを使用して VM を再開できます。



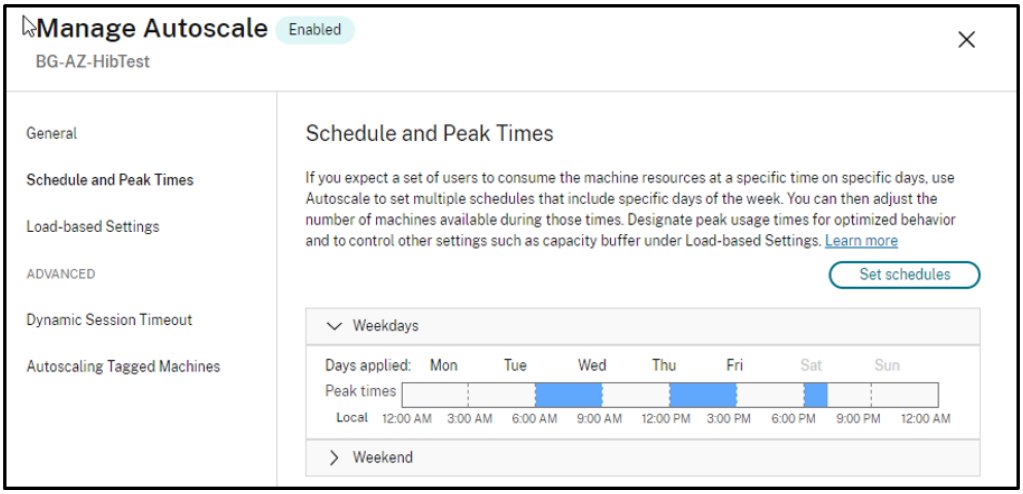
- エンドユーザーは、デスクトップアイコンをクリックすると、Citrix Workspace メニューを使用して VM を起動できます。



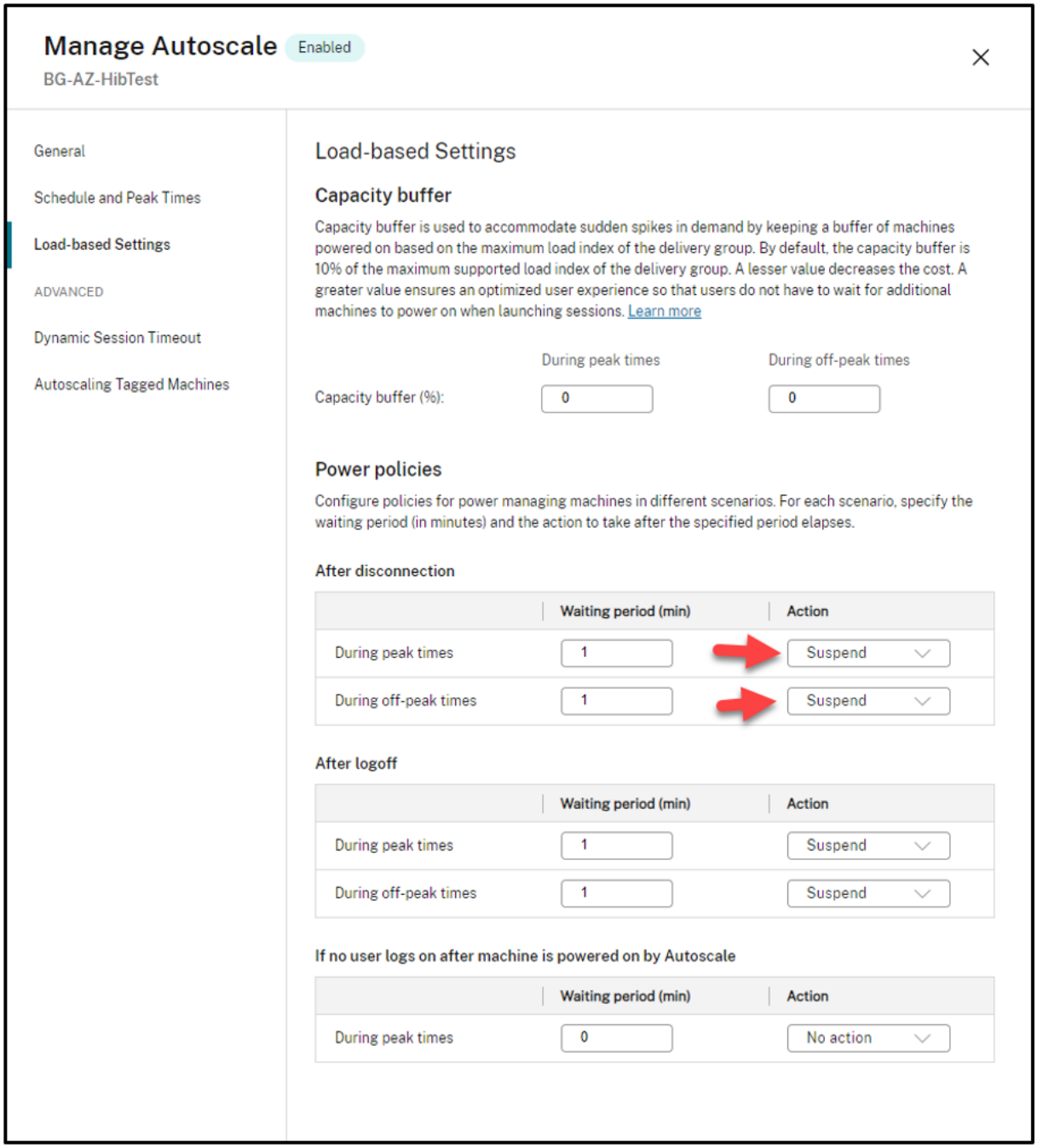
- 自動:
  - ピーク時間を正しく構成すると、Autoscale は休止状態のマシンの電源を自動的にオンにします。タイムスケジュールをクリックすると、ピーク時間を 30 分間隔で設定できます。青いフレームは、それぞれピーク時間としてマークされた時間枠を表します。ピーク時間には、連続した時間枠と連続しない時間枠があります。
    - 連続した時間枠



    - 連続しない時間枠



> 注:
>
> [**Autoscale** の管理] > [負荷ベースの設定] で、[アクション] が [一時停止] として構成されている場合は、そのデリバリーグループ内のすべての VM に休止機能があることを確認してください。休止機能がないと、休止状態にできない VM は引き続き実行されます。



追加情報

Citrix Azure の休止状態について詳しくは、Citrix Tech Zone の記事を参照してください。

セキュリティポリシー

April 10, 2023

この記事では、サポートされているさまざまなハイパーバイザーのセキュリティ機能について説明します。セキュリティ機能には以下が含まれます:

- セキュリティグループ
- セキュアブート
- 暗号化機能

セキュリティグループ

April 17, 2023

セキュリティグループは、仮想ネットワーク内のリソース間のネットワークトラフィックをフィルター処理するためのセキュリティ規則のグループです。セキュリティ規則は、さまざまなリソースの種類に対する受信ネットワークトラフィック、または送信ネットワークトラフィックを許可または拒否します。各規則は、次のプロパティを指定します:

- Name: ネットワークセキュリティグループ内の一意の名前
- Priority: 規則は優先度順に処理されます。数値が小さいほど優先度が高いため、数値が小さいほど大きい数値より先に処理されます
- Source または Destination: 任意の、または個別の IP アドレス、クラスレスドメイン間ルーティング (CIDR) ブロック (たとえば、10.0.0.0/24)、サービスタグ、またはアプリケーションセキュリティグループ
- Protocol: 各セキュリティグループの規則を追加する際の基準となるプロトコル
- Direction: 規則が受信または送信トラフィックに適用されるかどうか
- Port range: 個別のポートまたはポートの範囲を指定できます
- Action: 許可または拒否

サポートされているハイパーバイザーについて詳しくは、次を参照してください:

- AWS のセキュリティグループ
- Microsoft Azure のセキュリティグループ
- Google Cloud Platform のセキュリティグループ

AWS のセキュリティグループ

セキュリティグループは、VPC 内のインスタンスのトラフィックを制御する仮想ファイアウォールとして機能します。セキュリティグループにルールを追加することで、パブリックサブネット内のインスタンスがプライベートサブ

ネット内のインスタンスと通信できるようになります。また、これらのセキュリティグループを仮想プライベートクラウド内の各インスタンスに関連付けることもできます。受信規則はインスタンスへの受信トラフィックを制御し、送信規則はインスタンスからの送信トラフィックを制御します。

イメージの準備中のネットワーク設定について詳しくは、「イメージの準備中のネットワーク設定」を参照してください。

インスタンスを起動するときに、1 つまたは複数のセキュリティグループを指定できます。セキュリティグループを構成するには、「セキュリティグループの構成」を参照してください。

Microsoft Azure のセキュリティグループ

Citrix DaaS は、Azure のネットワークセキュリティグループをサポートしています。ネットワークセキュリティグループは、サブネットに関連付けられることが想定されています。詳しくは、「ネットワークセキュリティグループ」を参照してください。

ネットワークセキュリティグループについて詳しくは、「Azure Resource Manager イメージを使用してマシンカタログを作成する」を参照してください。

Google Cloud Platform のセキュリティグループ

マシンカタログの準備中に、カタログのマスターイメージシステムディスクとして機能するマシンイメージが準備されます。このプロセスが発生すると、ディスクは一時的に仮想マシンに接続されます。この VM は、すべての受信および送信ネットワークトラフィックが禁止された、分離された環境で実行する必要があります。これは、2 つの deny-all ファイアウォール規則によって実現されます。詳しくは、「ファイアウォール規則」を参照してください。

セキュアブート

May 17, 2024

セキュアブートは、信頼できるソフトウェアのみがシステムの起動に使用されるように設計されています。ファームウェアには、信頼できる証明書のデータベースがあり、ロードするイメージがいずれかの信頼できる証明書によって署名されていることを確認します。そのイメージがさらにイメージをロードする場合、そのイメージも同じ方法で検証する必要があります。
vTPM は、従来の物理 TPM モジュールの仮想化されたソフトウェアインスタンスです。vTPM は、仮想マシンのブートチェーン全体（UEFI、OS、システム、およびドライバー）を測定することにより、構成証明を有効にします。

サポートされているハイパーバイザーについて詳しくは、次を参照してください:

- Google Cloud Platform でのセキュアブート
- Microsoft Azure でのセキュアブート

- VMware でのセキュアブート

Google Cloud Platform でのセキュアブート

シールドされた仮想マシンを GCP でプロビジョニングできます。シールドされた仮想マシンは、セキュアブート、仮想トラステッドプラットフォームモジュール、UEFI ファームウェア、整合性監視などの高度なプラットフォームセキュリティ機能を使用して、Compute Engine インスタンスの検証可能な整合性を提供する一連のセキュリティ制御によって強化されます。

PowerShell を使用してシールドされた VM でカタログを作成する方法について詳しくは、「PowerShell を使用してシールドされた VM でカタログを作成する」を参照してください。

> 注:
>
> マスターイメージに Windows 11 をインストールする場合は、マスターイメージの作成プロセス中に vTPM を有効にする必要があります。また、マシンプロファイルソース（VM またはインスタンステンプレート）で vTPM を有効にする必要があります。単一テナントノードで Windows 11 VM を作成する方法については、「単一テナントノードに Windows 11 VM を作成する」を参照してください。

Microsoft Azure でのセキュアブート

Azure 環境で、トラステッド起動を有効にしたマシンカタログを作成できます。Azure では、第 2 世代 VM のセキュリティをシームレスに向上させる方法として、トラステッド起動が提供されています。トラステッド起動は、高度かつ永続的な攻撃手法からの保護を提供します。トラステッド起動の根底にあるのは、VM のセキュアブートです。トラステッド起動は、vTPM を使用してクラウドによるリモート構成証明も実行します。これは、プラットフォームのヘルスチェックと、信頼ベースの決定を行うために使用されます。セキュアブートと vTPM を個別に有効にすることができます。
トラステッド起動によるマシンカタログの作成について詳しくは、「トラステッド起動を使用したマシンカタログ」を参照してください。

VMware でのセキュアブート

MCS は、vTPM が組み込まれた VMware テンプレートをマシンプロファイルの入力のソースとして使用した、マシンカタログの作成をサポートします。Windows 11 がマスターイメージにインストールされている場合は、マスターイメージで vTPM を有効にすることが要件です。したがって、マシンプロファイルのソースである VMware テンプレートには、vTPM が組み込まれている必要があります。詳しくは、「マシンプロファイルを使用してマシンカタログを作成する」を参照してください。

暗号化機能

June 12, 2024

暗号化機能は、共有仮想マシンホスト上の悪意のあるゲストによる攻撃や、ホスト上のすべての仮想マシンを管理するハイパーバイザー制御ソフトウェアによって開始される攻撃から、仮想マシンのコンテンツを保護します。

サポートされているハイパーバイザーについて詳しくは、次を参照してください:

- AWS の暗号化機能
- Google Cloud Platform の暗号化機能
- Microsoft Azure の暗号化機能)

AWS の暗号化機能

このセクションでは、AWS 仮想化環境の暗号化機能について説明します。

自動暗号化

新しい Amazon EBS Volume と、アカウントで作成されたコピーのスナップショットの自動暗号化をオンにすることができます。詳しくは、「自動暗号化」を参照してください。

Google Cloud Platform の暗号化機能

このセクションでは、Google Cloud Platform（GCP）仮想化環境の暗号化機能について説明します。

Google が管理する暗号キーよりもキーの操作を細かく制御する必要がある場合は、顧客管理暗号キーを使用できます。顧客管理暗号キーを使用する場合、オブジェクトはバケットに保存されるときに Cloud Storage によってキーで暗号化され、オブジェクトがリクエスタに提供されるときに Cloud Storage によって自動的に暗号化が解除されます。詳しくは、「顧客管理の暗号鍵」を参照してください。

MCS カタログでは、顧客管理暗号キー（CMEK：Customer Managed Encryption Keys）を使用できます。詳しくは、「顧客管理暗号キー（CMEK）の使用」を参照してください。

Microsoft Azure の暗号化機能

このセクションでは、Azure 仮想化環境の暗号化機能について説明します。

Azure サーバー側暗号化

ほとんどの Azure Managed Disks は、サーバー側暗号化（SSE）を使用してデータを保護し、セキュリティとコンプライアンスの必要性を満たすのに役立つ Azure Storage 暗号化で暗号化されています。Citrix DaaS は、Azure Key Vault を使用して Azure Managed Disks の顧客が管理する暗号化キーをサポートします。詳しくは、「Azure サーバー側暗号化」を参照してください。

ホストでの **Azure** ディスク暗号化

ホスト機能での暗号化を使用して、MCS マシンカタログを作成できます。

この暗号化方法は、Azure Storage でデータを暗号化しません。VM をホストするサーバーがデータを暗号化し、暗号化されたデータが Azure Storage サーバーを通過します。つまり、この暗号化方法はデータをエンドツーエンドで暗号化します。

ホストでの暗号化機能を使用した MCS マシンカタログの作成について詳しくは、「ホストでの Azure ディスク暗号化」を参照してください。

Azure の二重暗号化

二重暗号化とは、プラットフォーム側の暗号化（デフォルト）と顧客管理の暗号化（CMEK）です。したがって、暗号化アルゴリズム、実装、またはキーの侵害に関するリスクを懸念している、セキュリティに非常に敏感なお客様は、この二重暗号化を選択できます。永続的 OS ディスクとデータディスク、スナップショット、イメージはすべて二重暗号化により保存時に暗号化されます。詳しくは、「管理対象ディスクの二重暗号化」を参照してください。

Azure Confidential VM

Azure Confidential Computing VM によって、仮想デスクトップは確実にメモリ内で暗号化され、使用中に保護されます。

MCS を使用して、Azure Confidential VM を含むカタログを作成できます。このようなカタログを作成するには、マシンプロファイルワークフローを使用する必要があります。VM と ARM テンプレートスペックの両方をマシンプロファイル入力として使用できます。

詳しくは、「Azure Confidential VM」を参照してください。

クイック展開

November 22, 2023

はじめに

Citrix DaaS で、［管理］**>**［クイック展開］インターフェイスを使用すると、Microsoft Azure でデスクトップとアプリをホストしている場合に、アプリとデスクトップを短時間で展開できます。このインターフェイスでは基本的な構成のみが可能であり、詳細な構成は行えません。

［クイック展開］を使用して、次のことを実行できます:

- Microsoft Azure でホストされているデスクトップとアプリを提供する仮想マシンとカタログのプロビジョニング。
- 既存のマシンのリモート PC アクセスカタログの作成。

［クイック展開］では、Citrix Managed Azureサブスクリプションまたは自身の Azure サブスクリプションを使用できます。

（名前は似ていますが、クイック展開は、［クイック展開］インターフェイスでカタログを作成する簡易作成（クイック作成）という方法と同じではありません。）

［クイック展開］の代わりに ［完全な構成］インターフェイスを使用すれば詳細な構成が可能です。［管理］タブのオプションについては、「管理インターフェイス」を参照してください。

管理インターフェイスの違い

次の表では、［完全な構成］インターフェイスと［クイック展開］インターフェイスを比較しています。

機能	クイック展開	完全な構成
Azure を使用して展開する	はい	はい *
他のクラウドサービスを使用して展開する	いいえ	はい
オンプレミスのハイパーバイザーを使用して展開する	いいえ	はい
Citrix 提供イメージを使用できる	はい	いいえ
簡素化されたユーザーエクスペリエンス	はい	いいえ

* Citrix Managed Azure サブスクリプションを使用する場合、イメージまたはカタログを作成するときに［クイック展開］を使用する必要があります。

完全な構成を使用してカタログを作成および管理することに慣れている方の場合、クイック展開には次の違いがあります。

- 異なる用語。

  - クイック展開では、カタログを作成します。
  - 完全な構成では、マシンカタログを作成します。実際には、単にカタログと書かれていることがよくあります。

- リソースの場所と Cloud Connector

  - クイック展開は、最初のカタログを作成するとき、2 つの Cloud Connector を含むリソースの場所を自動的に作成します。
  - ［完全な構成］では、リソースの場所の作成と Cloud Connector の追加を、カタログの作成前に Citrix Cloud で別の手順として行う必要があります。

- カタログの作成に使用されるイメージ。

  - ［クイック展開］では、複数の Windows マシンおよび Linux マシンの Citrix 提供イメージを提供します。これらのイメージを使用してカタログを作成できます。

    これらのイメージを使用してイメージを作成し、独自の展開ニーズに合わせてその新しいイメージをカスタマイズすることもできます。この機能は、イメージビルダーとして知られています。自身の Azure サブスクリプションから画像をインポートすることもできます。

  - 完全な構成では、使用しているサポート対象のホストのイメージをカスタマイズします。Citrix 提供イメージは使用できません。

- カタログ表示:

  - ［クイック展開］で作成されたカタログは、［クイック展開］画面と［完全な構成］画面に表示されます。
  - ［完全な構成］で作成されたカタログは、［クイック展開］画面に表示されません。

- デリバリーグループ:

  - クイック展開ではデリバリーグループを作成しません。［クイック展開］では、カタログでマシン、アプリケーション、デスクトップ、およびユーザー（サブスクライバー）を指定します。

    デリバリーグループは、クイック展開カタログごとに、カタログと同じ名前を使用して Citrix で自動で作成されます。この操作はバックグラウンドで行われます。管理者は、デリバリーグループを作成するために何かする必要はありません。デリバリーグループは、［クイック展開］ではなく［完全な構成］インターフェイスにのみ表示されます。

  - 完全な構成では、デリバリーグループを作成し、それに含まれるマシンを指定します。オプションで、アプリケーション、デスクトップ、およびユーザーも指定します。アプリケーショングループを作成することもできます。

- レイアウトとユーザーインターフェイス。

  - クイック展開インターフェイスは、完全な構成とはレイアウトとスタイルが異なります。［クイック展開］には、より多くの画面上のガイダンスが表示されます。

クイック展開インターフェイスと完全な構成インターフェイスは相互に排他的ではありません。クイック展開を使用していくつかのカタログを作成してから、完全な構成を使用して他のカタログを作成できます。

クイック展開インターフェイスで作成されたカタログの管理

［クイック展開］インターフェイスでカタログを作成した後は、引き続きそのインターフェイスでそのカタログを管理できます。詳しくは、「クイック展開でのカタログ管理」を参照してください。［完全な構成］インターフェイスを使用することもできます。

［クイック展開］でカタログを作成すると、そのカタログ（およびバックグラウンドで自動的に作成されるデリバリーグループとホスト接続）に`Citrix managed object`のスコープが割り当てられます。スコープは、オブジェクトをグループ化するために、委任管理で使用されます。

`Citrix managed object`スコープを使用するカタログ、デリバリーグループ、接続は、［完全な構成］インターフェイスでの特定の操作では禁止されています。（［完全な構成］でこれらの操作を許可すると、［クイック展開］と［完全な構成］の両方をサポートするシステムの機能に悪影響を与えることがあるため、これらの操作は無効です。）［完全な構成］インターフェイスでは：

- カタログ：ほとんどのカタログ管理操作は使用できません。カタログは削除できません。
- デリバリーグループ：ほとんどのデリバリーグループ管理操作を使用できます。デリバリーグループは削除できません。
- 接続：ほとんどの接続管理操作は使用できません。接続は削除できません。`Citrix managed object`スコープの接続に基づく接続を作成することはできません。

独自の Azure サブスクリプション（［クイック展開］に追加したもの）を使用して［クイック展開］でカタログを作成し、カタログ（とそのデリバリーグループおよび接続）をすべて［完全な構成］で管理する場合は、カタログを変換できます。

- カタログを変換すると、その管理は［完全な構成］インターフェイスのみに制限されます。カタログが変換されると、［クイック展開］インターフェイスを使用してそのカタログを管理することはできなくなります。
- カタログが変換された後、以前は［完全な構成］で使用できなかった操作を選択できるようになります。（`Citrix managed object`スコープは、変換されたカタログ、デリバリーグループ、ホスト接続から削除されます。）
- カタログを変換するには：

  ［管理］**>**［クイック展開］ダッシュボードで、カタログのエントリの任意の場所をクリックします。［詳細］タブの［詳細設定］で、［カタログを変換］を選択します。確認のメッセージが表示されたら、変換を確定します。
- Citrix Managed Azure サブスクリプションを使用して、［クイック展開］で作成されたカタログを変換することはできません。

以前の **Azure** クイック展開インターフェイスの置き換え

クイック展開は、Azure クイック展開という名前の以前のインターフェイスに置き換わります。クイック展開画面には、Azure クイック展開を使用して作成したすべてのカタログが表示されます。

Azure クイック展開でカタログの作成を開始したが完了しなかったという場合、そのカタログはクイック展開カタログリストに表示されます。ただし、クイック展開でできる操作は、それを削除することだけです。

要件

- クイック展開は、Azure のワークロードのみをサポートします。他のクラウドホストタイプ、サービス、またはハイパーバイザーでは使用できません。
- ［クイック展開］は、Citrix DaaS for Azure、Premium、Advanced、および Workspace Premium Plus でのみ使用できます。
- Citrix Cloud アカウントを取得し、Citrix DaaS にサブスクライブする必要があります。
- Citrix Managed Azure Consumption Fund を注文した場合は、カタログとイメージを作成するときに Citrix Managed Azure サブスクリプションを使用できます。

  Consumption Fund を注文しなかった場合（または自身の Azure サブスクリプションの使用を希望する場合）は、Azure サブスクリプションが必要です。
- ［管理］タブを表示するには、Citrix DaaS の適切な権限が必要です。詳しくは、「委任管理」を参照してください。

> 重要:
>
> Citrix Cloud およびサブスクライブしている Citrix サービスに関する重要な情報を確実に取得するには、すべてのメール通知を受信できることを確認してください。たとえば、Citrix は、Azure の消費量（使用量）の詳細を記載した情報通知メールを毎月送信します。
>
> Citrix Cloud コンソールの右上隅で、顧客名と OrgID フィールドの右側にあるメニューを展開します。［アカウント設定］を選択します。［マイプロファイル］タブで、［メール通知］セクションのすべてのエントリを選択します。

Citrix Gateway に関する考慮事項

独自の Citrix Gateway を使用する場合、カタログ作成ウィザードで指定した VNet に Citrix Gateway からアクセスできる必要があります。このアクセスは、VPN を使用することで可能になります。

Citrix Gateway サービスを使用すれば、クイック展開カタログに自動でアクセスできます。

次の操作

「クイック展開ではじめる」の［クイック展開］セットアップガイダンスに従ってください。

［クイック展開］を使用して環境をセットアップすると、引き続き以下の管理タスクにこのインターフェイスを使用できます。

- カタログの管理。カタログ管理にはマシンの追加または削除、アプリの管理、電源管理スケジュールの管理などが含まれます。
- イメージの管理。イメージ管理には、イメージの準備またはインポート、新しいイメージを使用したカタログの更新、イメージの名前の変更またはイメージの削除、イメージ上の VDA のインストールまたはアップグレードなどが含まれます。
- カタログでユーザーを追加または削除する。
- リソースの場所の管理。

クイック展開 - はじめに

May 25, 2023

この記事では、Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）の［クイック展開］インターフェイスを使用してデスクトップとアプリを配信するセットアップタスクについて説明します。実際に実行する前に各手順を確認し、何をするのかを把握しておくことをお勧めします。

［クイック展開］を使用して、リモート PC アクセス展開をセットアップする方法については、「リモート PC アクセス」を参照してください。

セットアップタスクの概要

この記事の以下のセクションで、セットアップタスクについて説明します：

1. 「システムの要件と準備」で必要なタスクを確認して完了します。
2. 概念実証のクイック展開または 実稼働環境を設定します。
3. ワークスペース URL をユーザーに提供します

システムの要件と準備

- Citrix Cloud および Citrix DaaS の新規登録。

  また、Citrix Managed Azureを使用する場合は、Citrix または Azure Marketplace から、（Citrix DaaS に加えて）Citrix Azure Consumption Fund を購入してください。

- **Windows** ライセンス： Windows Server ワークロードまたは Windows 10 の Azure Virtual Desktop ライセンスのいずれかをリモートデスクトップサービスが実行するための適切なライセンスがあることを確認します。詳しくは、「Microsoft RDS ライセンスサーバーの構成」を参照してください。
- Citrix Managed Azure サブスクリプションを使用する予定で、Active Directory グループポリシーを使用して VDA をドメインに参加させるには、Active Directory でその操作を実行する権限を持つ管理者である必要があります。詳しくは、「顧客の責任」を参照してください。

- 企業のオンプレミスネットワークへの接続を構成するには、追加の要件があります。
  - 任意の接続（Azure VNet ピアリングまたは SD-WAN）：すべての接続の要件。
  - Azure VNet ピアリング接続：VNet ピアリングの要件と準備。
  - SD-WAN 接続：SD-WAN 接続の要件と準備。
- カタログを作成するときに自身の Azure イメージを使用する場合は、これらのイメージが特定の要件を満たしている必要があります。
- インターネット接続要件：システムおよび接続要件。
- Citrix DaaS 展開におけるリソース制限：制限。

サポートされるオペレーティングシステム

Citrix Managed Azure サブスクリプションでクイック展開を使用する場合：

- Windows 10 シングルセッション
- Windows 10 マルチセッション
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Red Hat Enterprise Linux および Ubuntu

顧客が管理する Azure サブスクリプションでクイック展開を使用する場合：

- Windows 10 Enterprise シングルセッション
- Windows 10 Enterprise Virtual Desktop マルチセッション
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Red Hat Enterprise Linux および Ubuntu

概念実証のクイック展開のセットアップ

この手順には、Citrix Managed Azure サブスクリプションが必要です。

1. 簡易作成を使用してカタログを作成します。
2. 管理対象 Azure AD にユーザーを追加します。
3. カタログにユーザーを追加します。
4. ワークスペース URL をユーザーに通知します。

実稼働環境のセットアップ

1. ユーザーの認証に自身の Active Directory または Azure Active Directory を使用する場合は、接続して Citrix Cloud でその方法を設定します。
2. ドメイン参加済みのマシンを使用している場合は、有効な DNS サーバーエントリがあることを確認してください。
3. （Citrix Managed Azure サブスクリプションの代わりに）自身の Azure サブスクリプションを使用する場合は、Azure サブスクリプションを追加します。
4. イメージを作成またはインポートします。Citrix 提供イメージの 1 つをカタログでそのまま使用できますが、これらは主に概念実証の展開を目的としています。
5. Citrix Managed Azure サブスクリプションを使用していて、ユーザーがネットワーク内のアイテム（ファイルサーバーなど）にアクセスできるようにする場合は、Azure VNet ピアリングまたはCitrix SD-WAN接続を設定します。
6. カスタム作成を使用してカタログを作成します。
7. マルチセッションマシンのカタログを作成する場合は、必要に応じてカタログにアプリを追加します。
8. Citrix Managed Azure AD を使用してユーザーを認証している場合は、ディレクトリにユーザーを追加します。
9. カタログにユーザーを追加します。
10. ワークスペース URL をユーザーに通知します。

展開をセットアップした後、［クイック展開］**>**［監視］ダッシュボードを使用して、デスクトップ使用量、セッション、およびマシンを確認します。

ワークスペース **URL**

カタログを作成してユーザーを割り当てたら、デスクトップとアプリがある場所のワークスペース URL をユーザーに通知します。ワークスペース URL は、すべてのカタログとユーザーで同じです。

ワークスペース URL は、次の 2 つの場所で使用できます：

- Citrix DaaS の ［管理］**>**［クイック展開］で、右側の ［ユーザーアクセスと認証］を開いて URL を表示します。
- Citrix Cloud コンソールの左上隅のメニューで ［ワークスペースの構成］を選択します。［アクセス］タブに、ワークスペース URL が表示されます。

ワークスペース URL のカスタマイズについては、「ワークスペース URL をカスタマイズする」を参照してください。

ユーザーはワークスペース URL に移動して認証した後、デスクトップとアプリを起動できます。

サポートが必要な場合

- 「トラブルシューティング」の記事を確認してください。
- Citrix DaaS で引き続き問題が発生する場合は、「ヘルプとサポートの利用」の手順に従ってチケットを作成してください。

クイック展開を使用したカタログの作成

May 17, 2024

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

この記事の手順に従い、［クイック展開］管理インターフェイスを使用して Microsoft Azure マシンのカタログを作成します。

カタログを作成する前に手順全体を確認しておくことで、何をするのかを把握できます。

［完全な構成］インターフェイスを使用してカタログを作成する方法については、「マシンカタログの作成」を参照してください。

マシンの種類

［クイック展開］カタログには、次の種類のマシンのいずれかを含めることができます:

- 静的：このカタログには、シングルセッションの静的マシン（パーソナルデスクトップ、専用デスクトップ、または永続デスクトップとも呼ばれます）が含まれます。静的とは、ユーザーがデスクトップを起動すると、そのデスクトップがそのユーザーに「属する」ことを意味します。そのユーザーがデスクトップに加えた変更は、ログオフ時に保持されます。後で、そのユーザーが Citrix Workspace に戻ってデスクトップを起動すると、同じデスクトップになります。
- ランダム：このカタログには、シングルセッションのランダムマシン（非永続デスクトップとも呼ばれます）が含まれます。ランダムとは、ユーザーがデスクトップを起動したときに、そのユーザーがデスクトップに加えた変更がログオフ後に破棄されることを意味します。後で、そのユーザーが Citrix Workspace に戻ってデスクトップを起動すると、同じデスクトップである場合とそうでない場合があります。
- マルチセッション：このカタログには、アプリとデスクトップを備えたマシンが含まれます。複数のユーザーがこれらの各マシンに同時にアクセスできます。ユーザーは、ワークスペースからデスクトップまたはアプリ

を起動できます。アプリセッションは共有できます。アプリとデスクトップ間でのセッション共有は許可されていません。

- マルチセッションカタログを作成するときに、作業負荷を選択します：低（データエントリなど）、中（オフィスアプリなど）、高（エンジニアリングなど）、またはカスタム。各オプションは、特定のマシン数とマシンあたりのセッション数を表します。それにより、カタログがサポートするセッションの総数が得られます。
- カスタムの作業負荷を選択する場合は、CPU、RAM、およびストレージの使用可能な組み合わせから選択します。マシン数およびマシンあたりのセッション数を入力します。それにより、カタログがサポートするセッションの総数が得られます。

デスクトップを展開する場合、静的およびランダムなマシンの種類は「デスクトップタイプ」と呼ばれることがあります。

［クイック展開］を使用してカタログを作成する方法

カタログを作成して構成する方法はいくつかあります：

- 簡易作成は、最速で開始できる方法です。提供する情報は最小限で済み、残りは Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）が処理します。簡易作成カタログは、テスト環境や概念実証に最適です。
- カスタム作成は、簡易作成より多くの構成項目を選択できます。簡易作成カタログよりも実稼働環境に適しています。
- リモート **PC** アクセスカタログには、ユーザーがリモートでアクセスする既存のマシン（通常は物理）が含まれます。これらのカタログの詳細と手順については、「リモート PC アクセス」を参照してください。

簡易作成とカスタム作成の比較を次に示します：

簡易作成	カスタム作成
指定する情報が少ない。	指定する情報が多い。
一部の機能の選択肢が少ない。	一部の機能の選択肢が多い。
Citrix 管理の Azure Active Directory ユーザー認証。	選択肢：Citrix 管理の Azure Active Directory、または Active Directory か Azure Active Directory。
オンプレミスネットワークに接続しない	選択肢：オンプレミスネットワークに接続しない、Azure VNet ピアリングに接続しない、および SD-WAN に接続しない。
Citrix 提供の Windows 10 イメージを使用する。このイメージには、現在のデスクトップ VDA が含まれる。	選択肢：Citrix 提供イメージ、Azure からインポートしたイメージ、または Citrix 提供イメージかインポートしたイメージから Citrix DaaS に組み込んだイメージ。

簡易作成	カスタム作成
各デスクトップには、Azure 標準ディスク（HDD）ストレージがある。	複数のストレージオプションを利用できる。
静的デスクトップのみ。	静的、ランダム、またはマルチセッションのデスクトップ。
作成中に電源管理スケジュールを構成できない。セッションが終了すると、デスクトップをホストしているマシンの電源がオフになる。（この設定は後で変更できます。）	作成中に電源管理スケジュールを構成できる。（[クイック展開］の電源管理スケジュールは、［完全な構成］管理インターフェイスを使用して作成できる電源管理スケジュールとは異なります。）
Citrix Managed Azureサブスクリプションを使用する必要があります。	Citrix Managed Azure サブスクリプション、または自身の Azure サブスクリプションを使用できる。

手順について詳しくは、以下を参照してください：

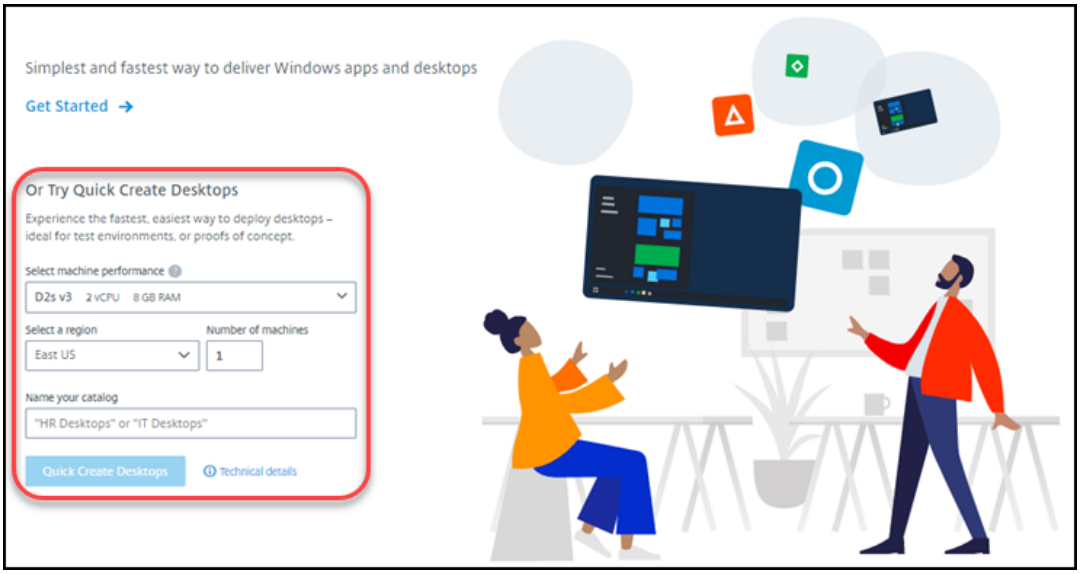
- 簡易作成を使用した［クイック展開］カタログの作成
- カスタム作成を使用した［クイック展開］カタログの作成

> 重要：
>
> Citrix Managed Azure サブスクリプションを使用してカタログ（またはイメージ）を初めて作成するときに、発生した料金に対する責任を承認し、同意するよう求められます。Citrix Managed Azure サブスクリプションを使用してカタログまたはイメージをさらに作成する場合にも、この同意のリマインダーが表示されることがあります。

簡易作成を使用した［クイック展開］カタログの作成

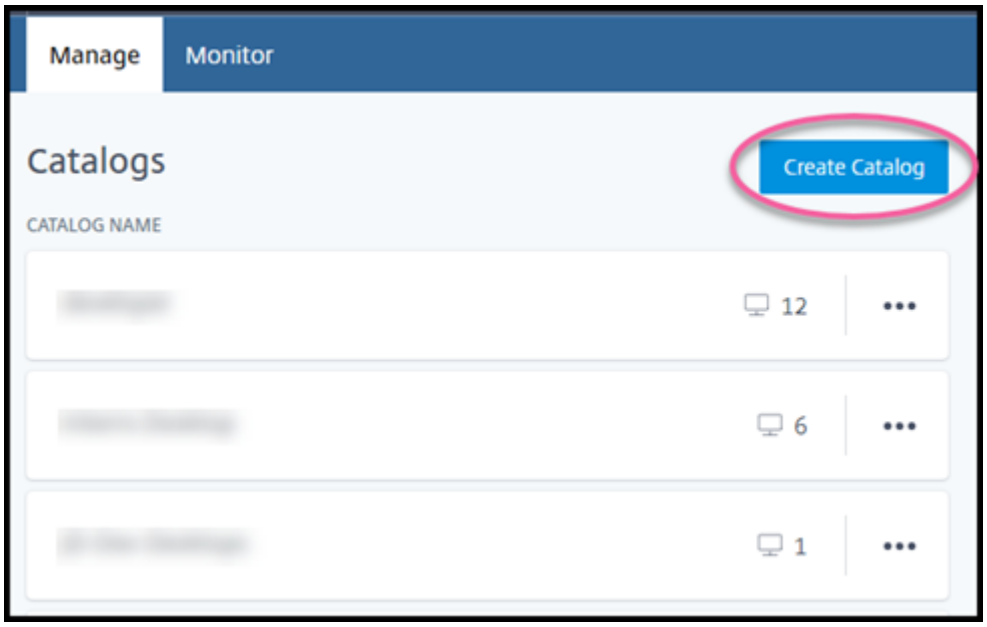
簡易作成では、Citrix Managed Azure サブスクリプションと Citrix 提供の Windows 10 イメージを使用して、静的マシンを含むカタログを作成します。電源管理設定は、低コストプリセット値を使用します。企業ネットワークへの接続はありません。ユーザーは、Citrix Managed Azure AD を使用して追加する必要があります。

1. Citrix Cloudにサインインします。
2. 左上のメニューで、［マイサービス］**>**［**DaaS**］を選択します。
3. ［管理］**>**［クイック展開］を選択します。
4. カタログがまだ作成されていない場合は、［ようこそ］ページに移動します。次のいずれかを選択します：
   - このページでカタログを構成します。引き続き、手順 6～10 を実行します。

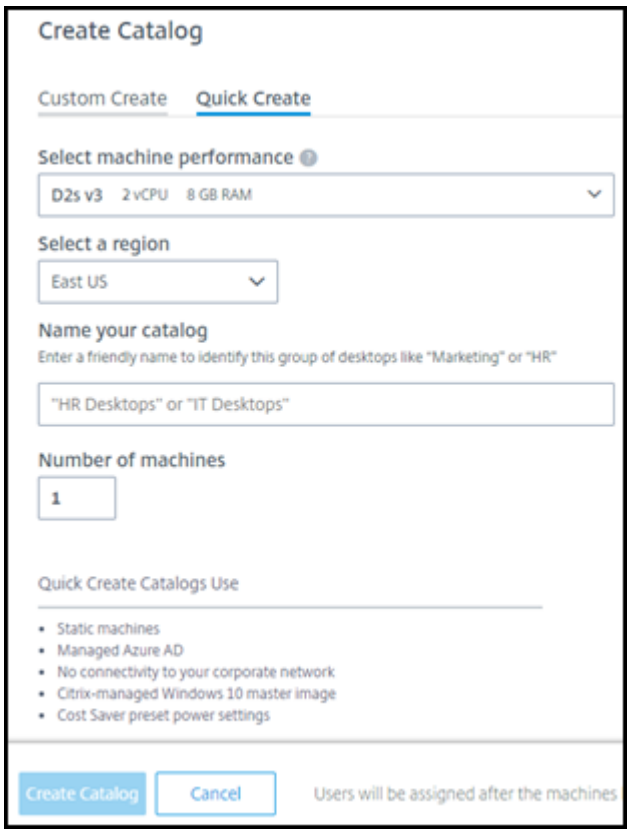


- ［はじめに］を選択します。［管理］**>**［クイック展開］ダッシュボードに移動します。［カタログの作成］を選択します。

5. カタログが既に作成されている場合（そして別のカタログを作成する場合）、［管理］**>**［クイック展開］ダッシュボードに移動します。［カタログの作成］を選択します。



6. まだ選択していない場合は、ページ上部にある ［簡易作成］を選択します。



- マシンパフォーマンス：マシンの種類を選択します。それぞれの選択肢には、CPU、RAM、およびストレージの独自の組み合わせがあります。高性能のマシンは月額費用が高くなります。
- リージョン：マシンを作成するリージョンを選択します。ユーザーに近いリージョンを選択できます。
- 名前：カタログの名前を入力します。このフィールドは必須であり、デフォルト値はありません。
- マシン数：必要なマシンの数を入力します。

7. 完了したら、[カタログの作成] を選択します。([ようこそ] ページから最初のカタログを作成する場合は、[デスクトップの簡易作成] を選択します。)
8. これが Citrix Managed Azure サブスクリプションを使用して作成する最初のカタログである場合は、プロンプトが表示されたら、関連する料金に対する責任を承認します。

カタログの作成中に、カタログの名前がカタログ一覧に追加され、作成の進行状況が表示されます。

また、Citrix DaaS は、リソースの場所を自動的に作成し、2 つの Citrix Cloud Connector を追加します。

次にやること：

- カタログの作成中に、管理対象 Azure AD ディレクトリにユーザーを追加できます。
- カタログが作成されたら、カタログにユーザーを追加します。

カスタム作成を使用した［クイック展開］カタログの作成

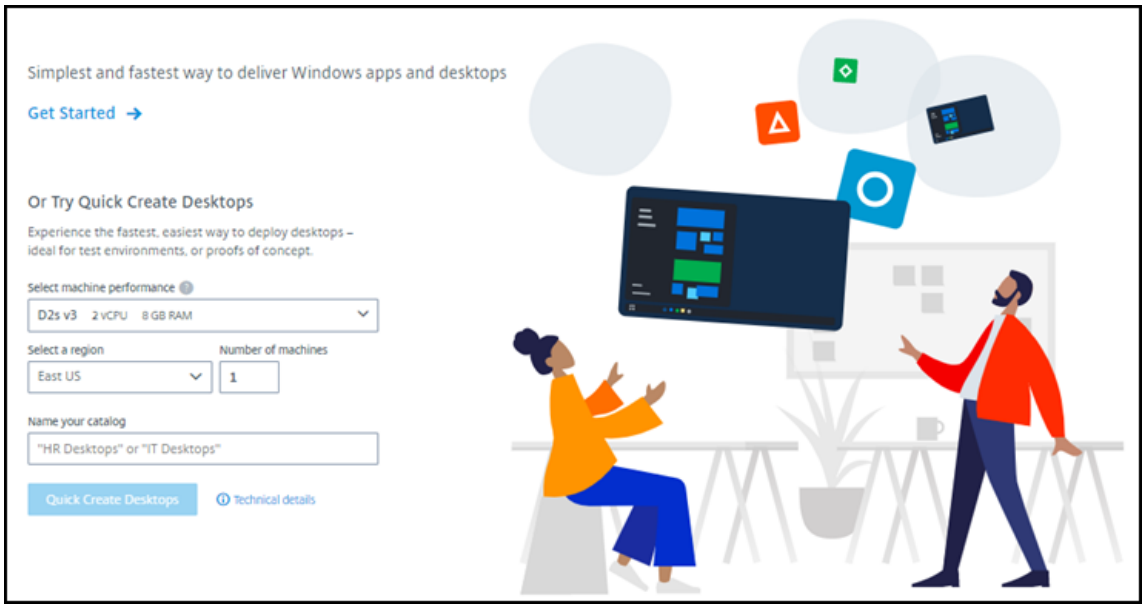
Citrix Managed Azure サブスクリプションを使用していて、オンプレミスネットワークのリソースへの接続を使用する予定の場合は、カタログを作成する前にネットワーク接続を作成します。ユーザーがオンプレミスまたはその他のネットワークのリソースにアクセスできるようにするには、その場所の Active Directory 情報も必要です。

Citrix Managed Azure サブスクリプションがない場合は、次の選択肢があります:

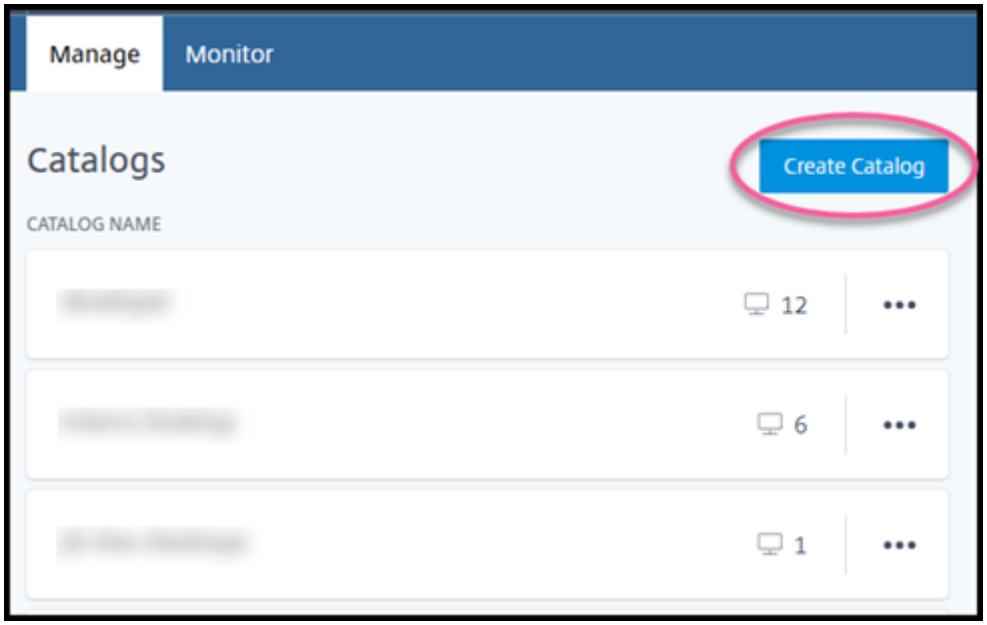
- Citrix Managed Azure サブスクリプションを提供する Azure Marketplace からAzure Consumption Fund を注文します。
- カタログを作成する前に、1 つまたは複数の独自の Azure サブスクリプションを Citrix DaaS にインポート（追加）します。

カタログを作成するには:

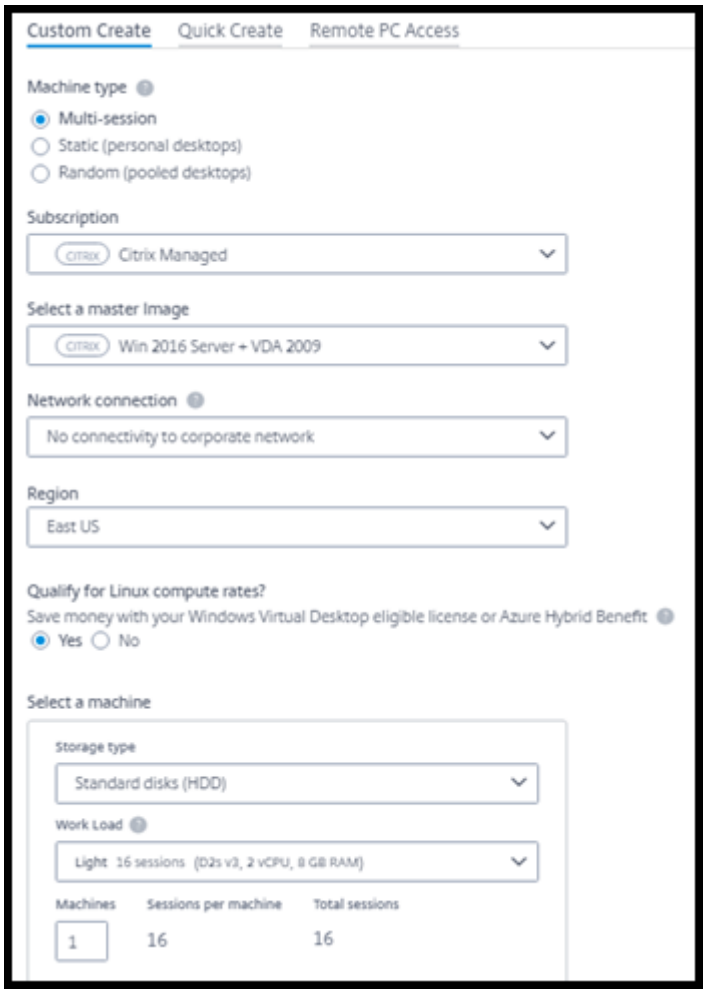
1. Citrix Cloudにサインインします。
2. 左上のメニューで、［マイサービス］**>**［**DaaS**］を選択します。
3. ［管理］**>**［クイック展開］を選択します。
4. カタログがまだ作成されていない場合は、［ようこそ］ページに移動します。［はじめに］を選択します。［はじめに］ページの最後で、［管理］**>**［クイック展開］ダッシュボードに移動します。［カタログの作成］を選択します。



カタログが既に作成されている場合は、［管理］**>**［クイック展開］ダッシュボードに移動します。［カタログの作成］を選択します。



5. まだ選択されていない場合は、ページ上部の ［カスタム作成］を選択します。



6. 次のフィールドに入力します。(一部のフィールドは、特定のマシンの種類に対してのみ有効です。フィールドの順序は異なる場合があります。)

   - マシンの種類。マシンの種類を選択します。詳しくは、「マシンの種類」を参照してください。
   - サブスクリプション。［Azure サブスクリプション］ を選択します。
   - マスターイメージ：カタログのマシンに使用するオペレーティングシステムのイメージを選択します。
   - ネットワーク接続：ネットワーク内のリソースへのアクセスに使用するネットワーク接続を選択します。

     Citrix Managed Azure サブスクリプションを選択した場合、選択肢は次のとおりです：

     - 接続なし：ユーザーは、オンプレミスの企業ネットワーク上の場所やリソースにアクセスできません。
     - 接続： VNet ピアリングや SD-WAN 接続など、以前に作成した接続を選択します。

     顧客が管理する Azure サブスクリプションを選択した場合は、適切なリソースグループ、仮想ネットワーク、およびサブネットを選択します。

   - リージョン：(［ネットワーク接続］で ［接続なし］を選択した場合のみ使用できます。) デスクトップを作成するリージョンを選択します。ユーザーに近いリージョンを選択できます。

     ［ネットワーク接続］で接続を選択した場合、カタログはそのネットワークのリージョンを使用します。

   - **Linux** コンピューティングレートの対象**?** (Windows イメージを選択した場合のみ使用できます。) 適格なライセンスまたは Azure Hybrid Benefit を使用するとコストを節約できます。

     Windows Virtual Desktop 特典：以下のものに対するユーザーごとの Windows 10 または Windows 7 の適格なライセンス：

     - Microsoft 365 E3/ES
     - Microsoft 365 A3/AS/Student Use Benefits
     - Microsoft 365 F3
     - Microsoft 365 Business Premium
     - Windows 10 Enterprise E3/E5
     - Windows 10 Education A3/A5
     - ユーザーごとに Windows 10 VDA

     Windows Server ワークロード用の Software Assurance が付いた RDS CAL のユーザーごとまたはデバイスごとのライセンス。

     Azure Hybrid 特典：アクティブな Software Assurance が付いた Windows Server ライセンス、またはそれと同等の適格なサブスクリプションライセンス。https://azure.microsoft.com/en-us/pricing/hybrid-benefit/を参照してください。

   - マシン

     - ストレージの種類。HDD または SSD。

- マシンパフォーマンス（マシンの種類が ［静的］または ［ランダム］の場合）、または ［ワークロード］（マシンの種類がマルチセッションの場合）。選択肢には、選択したイメージの世代の種類（gen1 または gen2）に一致するオプションのみが含まれます。

  カスタムの作業負荷を選択する場合は、［マシンパフォーマンス］フィールドにマシン数とマシンあたりのセッション数を入力します。

- マシン。このカタログに必要なマシンの数。

- マシンの名前付けスキーム：「マシンの名前付けスキーム」を参照してください。
- 名前：カタログの名前を入力します。この名前は、［管理］ダッシュボードに表示されます。
- 電源スケジュール：デフォルトでは、［後で構成します］チェックボックスがオンになっています。詳しくは、「電力管理スケジュール」を参照してください。（この電源管理スケジュールは、Citrix DaaS の［完全な構成］管理インターフェイスで使用可能な電源管理機能とは異なります。）
- ローカルの **Active Directory** ドメインに参加：（［ネットワーク接続］で Azure VNet ピアリング接続を選択した場合のみ使用できます。）［はい］または ［いいえ］を選択します。［はい］を選択した場合は、以下を入力します：
  - ドメインの FQDN（たとえば、Contoso.com）。
  - 組織単位（OU）：デフォルトの OU（コンピューター）を使用するには、このフィールドを空のままにします。
  - Citrix DaaS アカウント名：name@domain または domain\name という形式のドメインまたはエンタープライズ管理者である必要があります。
  - Citrix DaaS アカウント名のパスワード。
- 詳細設定：「カタログ作成時のリソースの場所の設定」を参照してください。

7. 完了したら、［カタログの作成］を選択します。
8. これが Citrix Managed Azure サブスクリプションを使用して作成する最初のカタログである場合は、プロンプトが表示されたら、関連する料金に対する責任を承認します。

［管理］**>**［クイック展開］ダッシュボードには、カタログ作成日時が表示されます。また、Citrix DaaS は、リソースの場所を自動的に作成し、2 つの Citrix Cloud Connector を追加します。

次にやること：

- ユーザーが Citrix Workspace に認証するための認証方法の構成をまだ行っていない場合は、構成します。
- カタログが作成されたら、カタログにユーザーを追加します。
- マルチセッションカタログを作成した場合は、（ユーザーを追加する前または後に）アプリケーションを追加します。

カタログ作成時のリソースの場所の設定

カタログを作成するときに、オプションでいくつかのリソースの場所の設定を構成できます。

カタログ作成ダイアログボックスで ［詳細設定］ を選択すると、Citrix DaaS はリソースの場所の情報を取得します。

- カタログ用に選択したドメインとネットワーク接続のリソースの場所が既にある場合は、作成するカタログで使用するためにそのリソースの場所を保存できます。

  そのリソースの場所に Cloud Connector が 1 つしかない場合は、別の Cloud Connector が自動的にインストールされます。オプションで、追加する Cloud Connector の詳細設定を指定できます。

- カタログ用に選択したドメインとネットワーク接続にリソースの場所を設定していない場合は、リソースの場所を構成するように求められます。

詳細設定の構成:

- （リソースの場所が既に設定されている場合にのみ必要です。）リソースの場所の名前。
- 外部接続の種類: Citrix Gateway サービスを使用、または企業ネットワーク内から。
- Cloud Connector 設定:
  - （顧客が管理する Azure サブスクリプションを使用する場合にのみ使用できます）マシンパフォーマンス。この選択肢は、リソースの場所にある Cloud Connector に使用されます。
  - （顧客が管理する Azure サブスクリプションを使用する場合にのみ使用できます）Azure リソースグループ。この選択肢は、リソースの場所にある Cloud Connector に使用されます。デフォルトは、そのリソースの場所で最後に使用されたリソースグループです（該当する場合）。
  - 組織単位（OU）。デフォルトは、そのリソースの場所で最後に使用された OU です（該当する場合）。

詳細設定が完了したら、［保存］ を選択してカタログ作成ダイアログボックスに戻ります。

カタログを作成した後、リソースの場所のいくつかの操作を使用できます。詳しくは、「リソースの場所の操作」を参照してください。

マシンの名前付けスキーム

カタログの作成時にマシンの名前付けスキームを指定するには、［マシンの名前付けスキームを指定する］ を選択します。1〜4 個のワイルドカード（ハッシュ記号）を使用して、名前の連続した数字または文字が表示される場所を示します。規則

- 名前付けスキームには、少なくとも 1 個のワイルドカードを含める必要がありますが、4 個を超えてはいけません。すべてのワイルドカードは一緒に使用する必要があります。
- ワイルドカードを含む名前全体は、2〜15 文字である必要があります。
- 名前には、空白（スペース）、スラッシュ、バックスラッシュ、コロン、アスタリスク、山かっこ、パイプ、コンマ、チルダ、感嘆符、記号、ドル記号、パーセント記号、キャレット、丸括弧、中括弧、または下線を含めることはできません。
- 名前をピリオドで始めることはできません。

- 名前を数字だけにすることはできません。
- 名前の末尾に次の文字を使用しないでください：-GATEWAY、-GW、および-TAC。

連続する値を数字（0～9）にするか、文字（A～Z）にするかを指定します。

たとえば、名前付けスキームとして「PC-Sales-##」を指定して「**0**～**9**」を指定すると、コンピューターアカウントの名前がPC-Sales-01、PC-Sales-02、PC-Sales-03などになります。

増加の余地を十分に持たせてください。

- たとえば、2 つのワイルドカードとその他 13 文字（たとえば、MachineSales-##）を使用する名前付けスキームでは、最大文字数（15 文字）を使用します。
- そのため、カタログに 99 台のマシンが含まれていると、その次のマシン作成は失敗します。Citrix DaaS は、3 桁（100）を使ってマシンを作成しようとしますが、それは 16 文字の名前を作成することになるからです。最大文字数は 15 文字です。
- そのため、この例では、もっと短い名前（たとえば、PC-Sales-##）を使用することで、99 台を超えるマシンをスケーリングできるようになります。

マシンの名前付けスキームを指定していない場合、Citrix DaaS はデフォルトの名前付けスキームDAS %%%%%-**-###を使用します。

- %%%%% = リソースの場所のプレフィックスに一致する 5 文字のランダムな英数字
- ** = カタログ用の 2 文字のランダムな英数字
- ### = 3 桁。

関連情報

- リモート PC アクセスカタログ
- プロキシサーバーを使用するネットワークでのカタログ作成
- カタログ情報の表示
- クイック展開でのカタログ管理

クイック展開でのカタログ管理

April 22, 2022

この記事では、［クイック展開］で作成されたカタログの管理に使用できるカタログ管理タスクについて説明します。

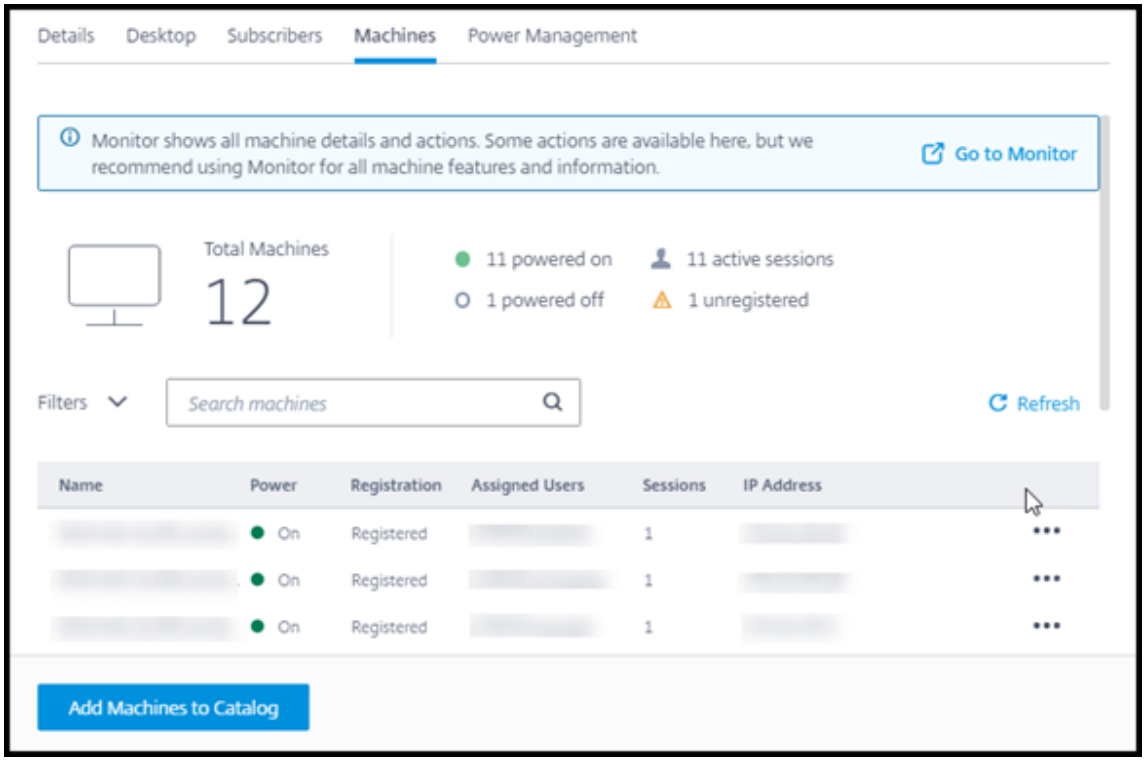
注意事項：［クイック展開］を使用してカタログを作成し、次に［完全な構成］インターフェイスを使用してそのカタログの管理タスクを実行した場合、そのカタログについては［クイック展開］インターフェイスを使用できなくなります。

（［完全な構成］管理インターフェイスでのカタログの管理については、「マシンカタログの管理」を参照してください。）

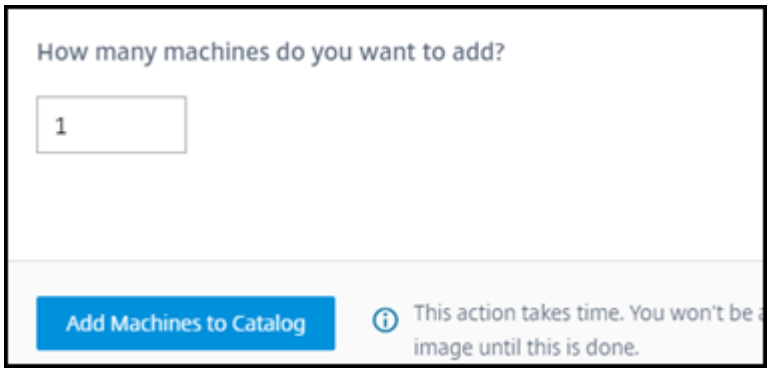
カタログへのマシンの追加

マシンが［クイック展開］カタログに追加されている間は、そのカタログに他の変更を加えることはできません。

1. ［管理］**>**［クイック展開］で、カタログのエントリの任意の場所をクリックします。
2. ［マシン］タブで、［カタログへのマシンの追加］を選択します。



3. カタログに追加するマシンの数を入力します。



4. （カタログがドメイン参加済みである場合にのみ有効です。）Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）アカウントのユーザー名とパスワードを入力します。

5. ［カタログへのマシンの追加］を選択します。

カタログのマシン数を減らすことはできません。ただし、電源管理スケジュール設定を使用して、電源がオンになっているマシンの数を制御したり ［マシン］タブから個別のマシンを削除したりできます。［マシン］タブからマシンを削除する方法については、「カタログ内のマシンの管理」を参照してください。

マシンあたりのセッション数の変更

マルチセッションマシンあたりのセッション数を変更すると、ユーザーエクスペリエンスに影響を与えることがあります。この値を増やすと、同時セッションに割り当てられるコンピューティングリソースが減少します。

推奨事項：利用状況データを観察して、ユーザーエクスペリエンスとコストの適切なバランスを判断します。

1. ［管理］**>**［クイック展開］で、マルチセッションマシンを含むカタログを選択します。
2. ［詳細］タブで、［マシンあたりのセッション数］の横にある ［編集］を選択します。
3. マシンあたりのセッション数の新しい値を入力します。
4. ［セッション数の更新］を選択します。
5. 要求を確認します。

この変更は、現在のセッションには影響しません。最大セッション数をマシンの現在アクティブなセッションの数よりも低い値に変更すると、新しい値はアクティブなセッションの通常減少により実装されます。

更新プロセスが開始する前に障害が発生した場合、カタログの ［詳細］画面には正しいセッション数が表示されます。更新プロセス中に障害が発生した場合、画面には求めたセッション数が示されます。

カタログ内のマシンの管理

> 注：
>
> ［管理］**>**［クイック展開］で使用できる操作の多くは、［クイック展開］の ［監視］タブでも使用できます。

［管理］**>**［クイック展開］で操作を選択するには：

1. ［管理］**>**［クイック展開］で、カタログのエントリの任意の場所をクリックします。
2. ［マシン］タブで、管理するマシンを見つけます。そのマシンの省略記号（…）メニューで、目的の操作を選択します：
   - 再起動：選択したマシンを再起動します。
   - 起動：選択したマシンを起動します。この操作は、マシンの電源がオフになっている場合にのみ使用できます。
   - シャットダウン：選択したマシンをシャットダウンします。この操作は、マシンの電源がオンになっている場合にのみ使用できます。

- メンテナンスモードをオン/オフにする：選択したマシンのメンテナンスモードをオン（オフの場合）またはオフ（オンの場合）にします。デフォルトでは、マシンのメンテナンスモードはオフになっています。

  メンテナンスモードをオンにしている間は、そのマシンに新たに接続できなくなります。ユーザーはそのマシンの既存のセッションに接続できますが、そのマシンの新しいセッションを開始することはできなくなります。

  パッチを適用する前、またはトラブルシューティングの際には、マシンをメンテナンスモードにすることをお勧めします。

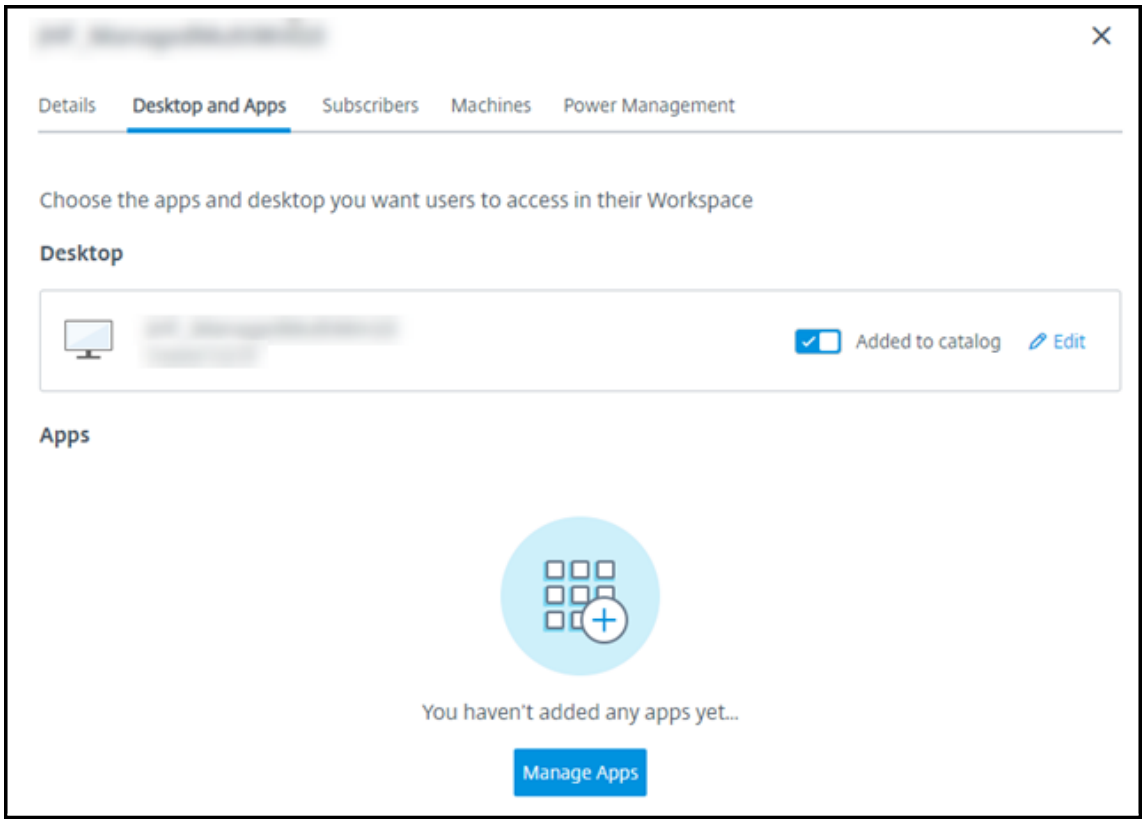
- 削除：選択したマシンを削除します。この操作は、マシンのセッション数が 0 の場合にのみ使用できます。削除を確認します。

  マシンが削除されると、マシン上のすべてのデータが削除されます。

- 強制再起動：選択したマシンを強制的に再起動します。マシンの ［再起動］操作が失敗した場合のみ、この操作を選択してください。

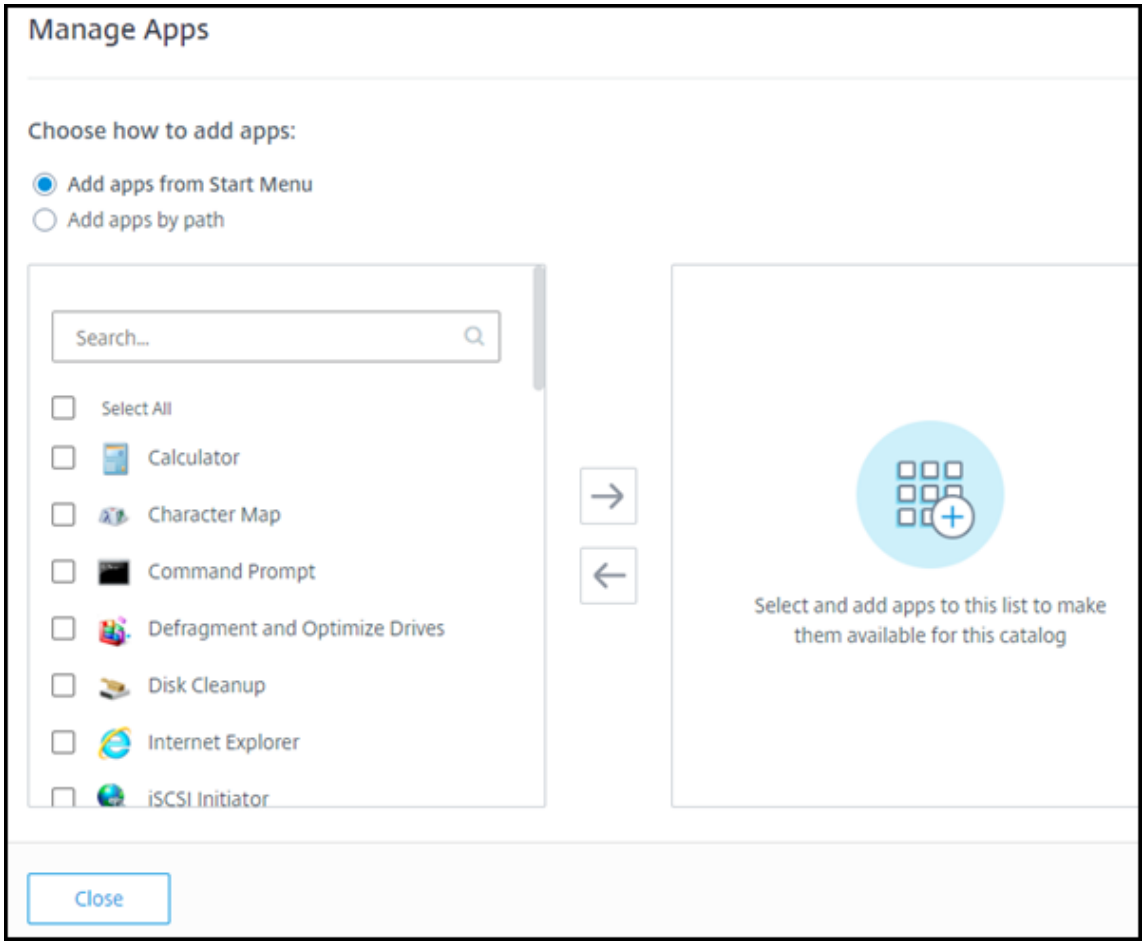
カタログへのアプリの追加

1. ［管理］**>**［クイック展開］で、カタログのエントリの任意の場所をクリックします。
2. ［デスクトップとアプリ］タブで、［アプリの管理］を選択します。



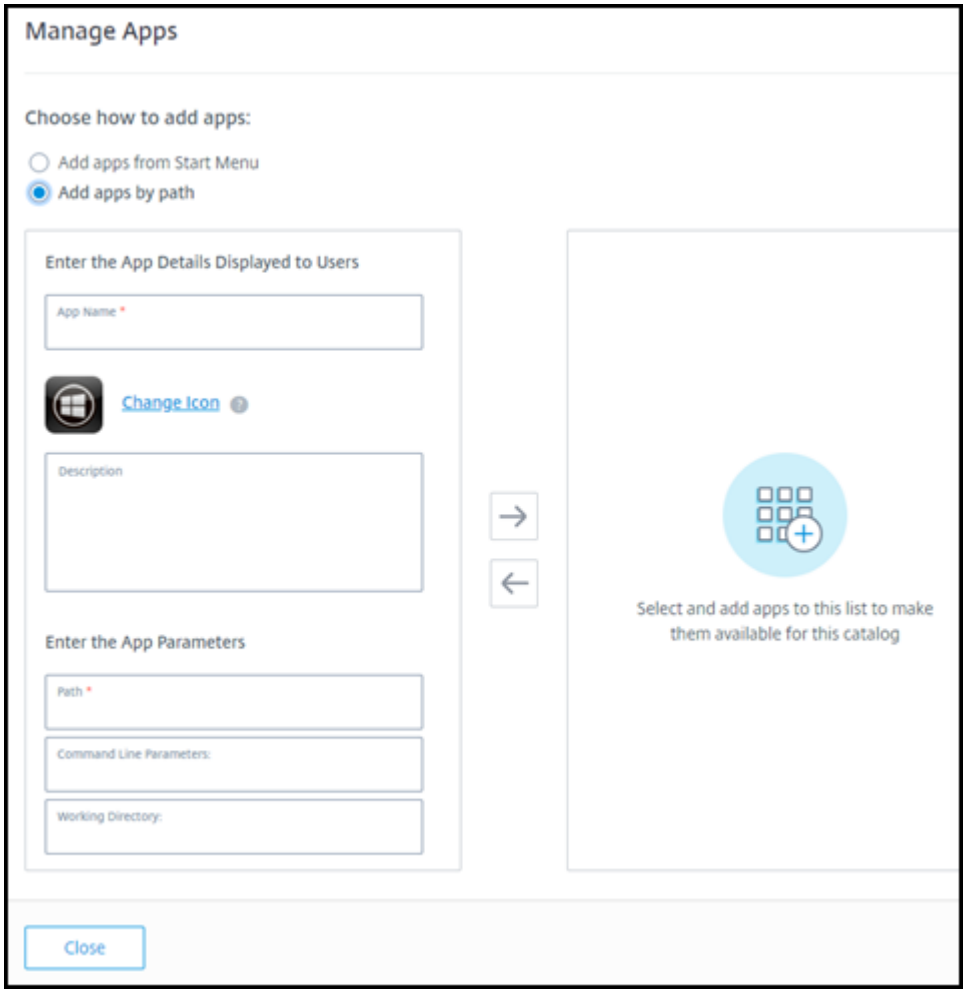
3. アプリを追加する方法を選択します：カタログ内のマシンの ［スタート］メニューから、またはマシン上の別のパスから。

4. ［スタート］メニューからアプリを追加するには：



   - 左側の列で使用可能なアプリを選択します（［検索］を使用してアプリ一覧を調整します）。列の間の右矢印を選択します。選択したアプリが右側の列に移動します。
   - 同様に、アプリを削除するには、右側の列で対象のアプリを選択し、列と列の間の左矢印を選択します。
   - ［スタート］メニューに、同名でバージョンが複数あるアプリがある場合、追加できるのは 1 つだけです。そのアプリの別のバージョンを追加するには、そのバージョンを編集して名前を変更します。そのあと、そのバージョンのアプリを追加できます。

5. パスによりアプリを追加するには：



- アプリの名前を入力します。これは、ユーザーが Citrix Workspace で表示する名前です。
- 表示アイコンは、Citrix Workspace でユーザーに表示されるアイコンです。別のアイコンを選択するには、［アイコンの変更］を選択し、表示したいアイコンに移動します。
- （オプション）アプリケーションの説明を入力します。
- アプリへのパスを入力します。このフィールドは必須です。必要に応じて、コマンドラインパラメーターと作業ディレクトリを追加します。コマンドラインパラメーターについて詳しくは、「公開アプリケーションにパラメーターを渡す」を参照してください。

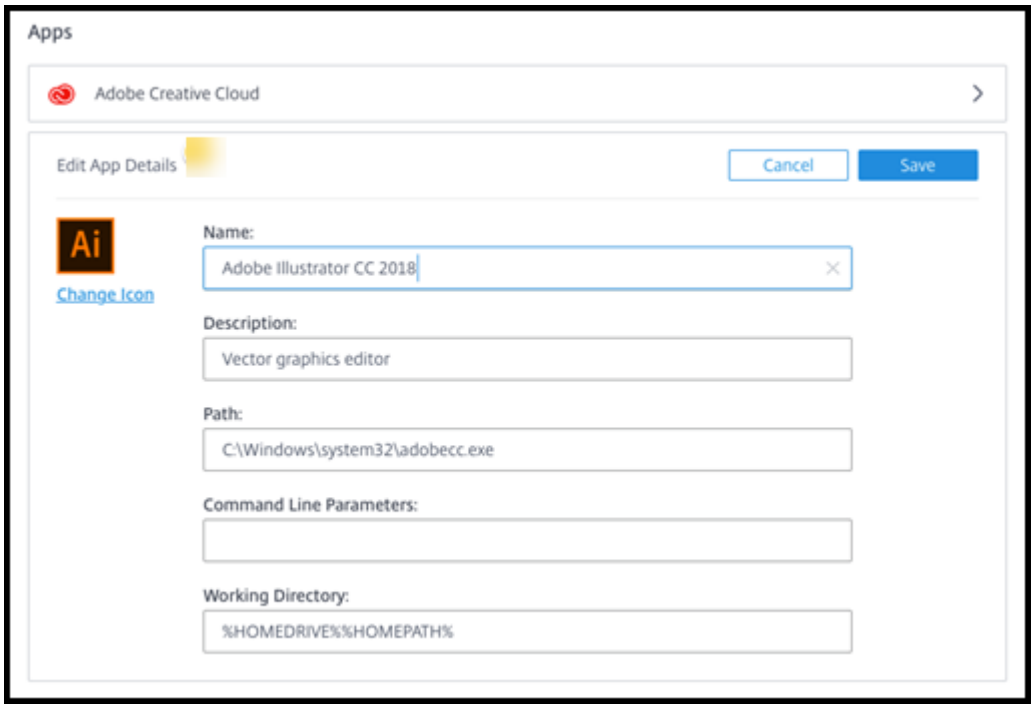
6. 完了したら、［閉じる］を選択します。

Windows Server 2019 VDA では、構成中およびユーザーのワークスペースに、一部のアプリケーションアイコンが正しく表示されない場合があります。回避策として、アプリケーションの公開後に、アプリを編集して、正しく表示される別のアイコンを割り当てる ［アイコンの変更］機能を使用します。

カタログ内のアプリの編集

1. ［管理］**>**［クイック展開］で、カタログのエントリの任意の場所をクリックします。

2. ［デスクトップとアプリ］タブで、編集するアプリが含まれている行の任意の場所をクリックします。
3. 鉛筆アイコンを選択します。



4. 次のいずれかのフィールドに変更内容を入力します:
   - 名前：ユーザーが Citrix Workspace で表示する名前。
   - 説明
   - パス：実行可能ファイルへのパス。
   - コマンドラインパラメーター：詳しくは、「公開アプリケーションにパラメーターを渡す」を参照してください。
   - 作業ディレクトリ
5. Citrix Workspace でユーザーに表示されるアイコンを変更するには、［アイコンの変更］を選択し、表示したいアイコンに移動します。
6. 完了したら、［保存］を選択します。

公開アプリケーションにパラメーターを渡す

公開アプリケーションをファイルタイプに関連付けると、コマンドライン（実行可能ファイルのパス）の末尾に（二重引用符で囲んだ）パーセント記号とアスタリスク記号が追加されます。これらの記号は、ユーザーデバイス側に渡されるパラメーターのプレースホルダーとして機能します。

- ファイルタイプに関連付けられている公開アプリケーションが起動しない場合は、記号が正しくコマンドラインに含まれていることを確認してください。記号が追加されている場合、デフォルトでは、ユーザーデバイスから渡されるパラメーターが検証されます。

特殊なパラメーターを必要とする公開アプリケーションでは、コマンドラインに”%”（二重引用符で囲んだパーセント記号と 2 個のアスタリスク記号）が追加されています。これによりコマンドライン検証が無効になります。コマンドラインにこれらの記号が含まれていない場合は、手作業で追加できます。

- 実行可能ファイルのパスに、「“C:\Program Files”」のようなスペースを使ったフォルダー名が含まれている場合は、アプリケーションのコマンドラインを二重引用符で囲み、このスペースがコマンドラインに属していることを示します。パスの前後に二重引用符を追加し、パーセント記号とアスタリスク記号の前後にもう 1 組の二重引用符を追加します。このとき、パスの末尾の二重引用符と、パーセント記号およびアスタリスク記号の前の二重引用符の間に、必ずスペースを 1 つ追加してください。

  たとえば、公開アプリケーション Windows Media Player のコマンドラインは次のようになります: “C:\Program Files\Windows Media Player\mplayer1.exe” “%*”

カタログからのアプリの削除

カタログからアプリを削除しても、マシンからは削除されません。Citrix Workspace で表示されなくなるだけです。

1. ［管理］**>**［クイック展開］で、カタログのエントリの任意の場所をクリックします。
2. ［デスクトップとアプリ］タブで、削除するアプリの横にあるゴミ箱アイコンを選択します。

カタログの削除

カタログを削除すると、カタログ内のすべてのマシンが完全に破棄されます。カタログの削除は元に戻すことができません。

1. ［管理］**>**［クイック展開］で、カタログのエントリの任意の場所をクリックします。
2. ［詳細］タブで、［カタログの削除］を選択します。
3. 削除を確認します。

削除する必要がある残りの Active Directory マシンアカウントを特定するのに役立つよう、マシン名と Cloud Connector 名の一覧をダウンロードできます。

電源管理スケジュールの管理

電源管理スケジュールは、カタログ内のすべてのマシンに影響します。スケジュールは以下を提供します:

- 最適なユーザーエクスペリエンス: ユーザーは必要なときにマシンを使用できます。
- セキュリティ: 指定した期間アイドル状態のままであるデスクトップセッションは切断され、ユーザーはワークスペースで新しいセッションを起動する必要があります。
- コスト管理と省電力: デスクトップがアイドル状態のままであるマシンの電源はオフになります。マシンは、スケジュールされた実際の需要を満たすために電源がオンになります。

カスタムカタログを作成するとき、または後で作成するときに、電源スケジュールを構成できます。スケジュールが選択または構成されていない場合、セッションが終了するとマシンの電源がオフになります。

簡易作成でカタログを作成する場合、電源スケジュールを選択または構成することはできません。デフォルトでは、簡易作成カタログは、コスト削減用プリセットスケジュールを使用します。後でそのカタログに対して別のスケジュールを選択または構成できます。

スケジュール管理には次のことが含まれています:

- スケジュールに含まれる情報を知ること
- スケジュールを作成すること

スケジュール内の情報

次の図は、マルチセッションマシンを含むカタログのスケジュール設定を示しています。シングルセッション（ランダムまたは静的）マシンを含むカタログの設定は、少し異なります。

電源管理スケジュールには、次の情報が含まれています。

プリセットスケジュール　Citrix DaaS は、いくつかのプリセットスケジュールを提供します。カスタムスケジュールを構成して保存することもできます。カスタムプリセットを削除することはできますが、シトリックス提供のプリセットを削除することはできません。

タイムゾーン　電源がオンのマシンの設定とともにこれを使用することで、選択したタイムゾーンに基づいて営業時間と営業時間外を設定できます。

この設定は、すべてのマシンタイプで有効です。

電源オンのマシン：営業時間と営業時間外　営業時間を形成する曜日とその曜日の開始-終了時間。これは通常、マシンの電源をオンにする間隔を示します。これらの間隔外の時間は、営業時間外と見なされます。いくつかのスケジュール設定では、営業時間と営業時間外に別々の値を入力できます。他の設定は常に適用されます。

この設定は、すべてのマシンタイプで有効です。

アイドル時のデスクトップセッションの切断　セッションが切断されるまで、デスクトップがアイドル状態（未使用）のままでいられる時間。セッションが切断された後、ユーザーは Workspace に移動してデスクトップを起動し直す必要があります。これはセキュリティ設定です。

この設定は、すべてのマシンタイプで有効です。1 つの設定が常に適用されます。

アイドル状態のデスクトップの電源オフ　マシンの電源がオフになるまで、マシンが切断状態のままでいられる時間。マシンが電源オフになった後、ユーザーは Workspace に移動してデスクトップを起動し直す必要があります。これは省電力設定です。

たとえば、デスクトップが 10 分間アイドル状態になった後、デスクトップを切断するとします。次に、マシンがさらに 15 分間切断されたままだった場合は、マシンの電源をオフにします。

Tom さんがデスクトップを使用することをやめ、1 時間の会議に参加するため席を離れた場合、デスクトップは 10 分後に切断されます。さらに 15 分後、マシンの電源がオフになります（合計 25 分）。

ユーザーの立場から見ると、2 つのアイドル状態の設定（切断と電源オフ）は同じ効果があります。Tom さんがデスクトップから 12 分離れようと 1 時間離れようと、Workspace からデスクトップを起動し直す必要があります。この 2 つのタイマーの違いは、デスクトップを提供する仮想マシンの状態に影響を与えます。

この設定は、シングルセッション（静的またはランダム）マシンに有効です。営業時間と営業時間外の値を入力できます。

切断されたセッションのログオフ　セッションが閉じるまで、マシンが切断状態のままでいられる時間。

この設定は、マルチセッションマシンで有効です。1 つの設定が常に適用されます。

電源オフの遅延　マシンの電源がオフになる（および他の基準）まで、マシンの電源をオンにしておく必要がある最小時間。この設定により、セッション需要が不安定な期間にマシンが電源オンとオフを繰り返さないようにします。

この設定は、マルチセッションマシンで有効であり、常に適用されます。

実行中の最小マシン数　アイドル状態または切断状態の時間に関係なく、電源をオンのままにしておく必要があるマシンの数。

この設定は、ランダムおよびマルチセッションマシンで有効です。営業時間と営業時間外の値を入力できます。

処理能力バッファ　処理能力バッファは、バッファのマシンの電源をオンにしておくことで、需要の突然の急増に対応するのに役立ちます。このバッファは、現在のセッション需要のパーセンテージとして指定します。たとえば、アクティブなセッションが 100 個あり、処理能力バッファが 10% の場合、Citrix DaaS はセッション 110 個分の処理能力を提供します。需要の急増は、営業時間中、またはカタログへの新しいマシンの追加中に発生する可能性があります。

値が低いほど、コストが低くなります。値が高いほど、ユーザーエクスペリエンスの最適化に役立ちます。セッションを開始するとき、ユーザーは追加のマシンの電源がオンになるのを待つ必要はありません。

(処理能力バッファを含め）カタログに必要な電源オンのマシンの数をサポートするのに十分な数のマシンがある場合、追加のマシンの電源をオフにします。オフピーク時間だった、セッションがログオフした、またはカタログ内のマシンの数が少なかったことが原因で、電源オフが発生することがあります。マシンの電源をオフにする判断が下されるには、次の基準を満たす必要があります:

- マシンの電源がオンになっており、メンテナンスモードではない。
- マシンが使用可能なものとして登録されている、または電源をオンにした後で登録を待機している。
- マシンにアクティブなセッションがない。残りのセッションがすべて終了している（マシンがアイドルタイムアウト期間中アイドル状態だった)。
- 少なくとも「X」分間、マシンの電源がオンになっている（「X」はカタログで指定する電源オフの遅延時間)。

  静的カタログ内のすべてのマシンが割り当てられた後は、処理能力バッファがマシンの電源のオン/オフに関与することはなくなります。

この設定は、すべてのマシンタイプで有効です。営業時間と営業時間外の値を入力できます。

電源管理スケジュールの作成

1. ［管理］**>**［クイック展開］で、カタログのエントリの任意の場所をクリックします。
2. ［電源管理］タブで、（上部のメニューにある）プリセットスケジュールのいずれかがニーズを満たしているかどうかを確認します。プリセットを選択して、使用する値を確認します。プリセットを使用する場合は、選択したままにします。
3. いずれかのフィールド（日、時間、間隔など）の値を変更すると、プリセットの選択が自動的に ［カスタム］に変更されます。アスタリスク記号は、カスタム設定が保存されていないことを示します。
4. カスタムのスケジュールに必要な値を設定します。
5. 上部にある ［カスタム］を選択し、現在の設定を新しいプリセットとして保存します。新しいプリセットの名前を入力し、チェックマークをオンにします。

6. 完了したら、［変更の保存］を選択します。

後で、［プリセット］メニューの鉛筆アイコンまたはゴミ箱アイコンを使用することで、カスタムプリセットを編集または削除できます。共通プリセットを編集または削除することはできません。

関連情報

- 新しいイメージでカタログを更新
- カタログでユーザーを追加または削除する

クイック展開での **Azure** サブスクリプション

May 17, 2024

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

はじめに

［クイック展開］でカタログを作成するかイメージを作成するときは、使用可能な Azure サブスクリプションの中から選択します。［クイック展開］では、Citrix Managed Azure サブスクリプションと顧客自身の顧客管理の Azure サブスクリプションをサポートしています。

- 自身の Azure サブスクリプションを使用するには、最初に Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）のサブスクリプションの 1 つまたは複数をサービスにインポート（追加）します。この操作により、Citrix DaaS が Azure サブスクリプションにアクセスできるようになります。
- Citrix Managed Azure サブスクリプションを使用するために、サブスクリプションの構成は必要ありません。ただし、Citrix Managed Azure サブスクリプションは、Citrix DaaS のほか、Citrix Azure Consumption Fund を購入している場合にのみ使用できます。

一部の Citrix DaaS の機能は、カタログが Citrix Managed Azure サブスクリプションを使用するか、自身の Azure サブスクリプションを使用するかによって異なります。

Citrix Managed Azure サブスクリプション	顧客自身の Azure サブスクリプション
ドメイン参加済みマシンまたはドメイン非参加マシンをサポート。	ドメイン参加済みマシンのみをサポート。

Citrix Managed Azure サブスクリプション	顧客自身の Azure サブスクリプション
カタログの簡易作成およびカスタム作成をサポート。	カタログのカスタム作成のみをサポート。
カタログやイメージを作成するときにいつでも使用可能。	カタログを作成する前に、Citrix DaaS に Azure サブスクリプションを追加する必要がある。
ユーザー認証の場合、Citrix Managed Azure Active Directory または自身の Active Directory をサポート。	自身の Active Directory と Azure Active Directory を接続可能。
ネットワーク接続オプションに、［接続なし］などがある。	ネットワーク接続オプションに、自身の仮想ネットワークのみがある。
Azure VNet ピアリングを使用してリソースに接続する場合は、Citrix DaaS で VNet ピア接続を作成する必要がある。	既存の仮想ネットワークを選択する。
Azure からイメージをインポートするときは、イメージの URI を指定する。	イメージをインポートするとき、Azure サブスクリプションで VHD を選択するか、ストレージを参照することができる。
顧客の Azure サブスクリプションに踏み台マシンを作成して、マシンのトラブルシューティングを行うことができる。	サブスクリプション内のマシンに既にアクセスできるため、踏み台マシンを作成する必要がない。

Azure サブスクリプションの表示

Azure サブスクリプションの詳細を表示するには、［管理］**>**［クイック展開］の右側にある ［**Cloud** サブスクリプション］を開きます。次に、サブスクリプションエントリを選択します。

- ［詳細］ページには、マシン数のほか、サブスクリプションを使用するカタログとイメージの数と名前が表示されます。
- ［リソースの場所］ページには、サブスクリプションが使用されているリソースの場所が一覧表示されます。

顧客管理の **Azure** サブスクリプションを追加する

顧客管理の Azure サブスクリプションを使用するには、カタログを作成する前、またはそのサブスクリプションを使用するイメージを作成する前に、そのサブスクリプションを Citrix DaaS に追加する必要があります。Azure サブスクリプションを追加する場合は、次の 2 つのオプションがあります:

- ディレクトリのグローバル管理者であり、サブスクリプションの所有者権限がある場合： Azure アカウントに認証するだけで済みます。
- グローバル管理者ではなく、サブスクリプションの所有者権限を持っている場合：サブスクリプションを Citrix DaaS に追加する前に、Azure AD で Azure アプリを作成し、サブスクリプションの共同作成者としてそのアプリを追加します。そのサブスクリプションを Citrix DaaS に追加すると、関連するアプリ情報が提供されます。

グローバル管理者である場合に、顧客管理の **Azure** サブスクリプションを追加する

このタスクには、ディレクトリのグローバル管理者権限とサブスクリプションの所有者権限が必要です。

1. ［管理］**>**［クイック展開］を選択してから、右側にある ［**Cloud** サブスクリプション］を開きます。
2. ［**Azure** サブスクリプションを追加する］を選択します。
3. ［サブスクリプションの追加］ページで、［**Azure** サブスクリプションの追加］を選択します。
4. ユーザーに代わって Citrix DaaS が Azure サブスクリプションにアクセスできるようにするボタンを選択します。
5. ［**Azure** アカウントを認証する］を選択します。Azure のサインインページが表示されます。
6. Azure の資格情報を入力します。
7. 自動的に Citrix DaaS に戻ります。［サブスクリプションの追加］ページには、検出された Azure サブスクリプションが一覧表示されます。必要に応じて、検索ボックスを使用して一覧をフィルタリングします。1 つまたは複数のサブスクリプションを選択します。完了したら、［サブスクリプションの追加］を選択します。
8. 選択したサブスクリプションを追加することを確認します。

［サブスクリプション］を開くと、選択した Azure サブスクリプションが一覧表示されます。追加されたサブスクリプションは、カタログまたはイメージを作成するときに選択できます。

グローバル管理者でない場合に、顧客管理の **Azure** サブスクリプションを追加する

グローバル管理者でない場合に Azure サブスクリプションを追加するプロセスは、次の 2 つ部分で構成されます：

- Citrix DaaS にサブスクリプションを追加する前に、Azure AD でアプリを作成し、そのアプリをサブスクリプションの Contributor（共同作成者）として追加します。
- Azure で作成したアプリに関する情報を使用して、Citrix DaaS にサブスクリプションを追加します。

Azure AD でアプリを作成し、共同作成者として追加する

1. Azure AD に新しいアプリケーションを登録します：
   a) Web ブラウザーからhttps://portal.azure.comに移動します。
   b) 左上のメニューで、［**Azure Active Directory**］を選択します。
   c) ［**Manage**］一覧で、［**App registrations**］を選択します。
   d) ［**+ New registration**］を選択します。
   e) ［**Register an application**］ページで、次の情報を入力します：
      - **Name**：接続名を入力します
      - **Application type**：［**Web app / API**］を選択します
      - **Redirect URI**：空白のままにします

f) ［作成］を選択します。

2. アプリケーションのシークレットアクセスキーを作成し、役割の割り当てを追加します：

a) 前述の手順で、［**App Registration**］を選択して詳細を表示します。

b) ［**Application ID**］と ［**Directory ID**］をメモします。これは、後でサブスクリプションを Citrix DaaS に追加するときに使用します。

c) ［**Manage**］にある ［**Certificates & secrets**］を選択します。

d) ［**Client secrets**］ページで、［**+ New client secret**］を選択します。

e) ［**Add a client secret**］ページで説明を入力し、有効期限を選択します。次に、［**Add**］を選択します。

f) クライアントシークレットの値をメモします。これは、後でサブスクリプションを Citrix DaaS に追加するときに使用します。

g) Citrix DaaS にリンク（追加）する Azure サブスクリプションを選択し、［**Access control (IAM)**］を選択します。

h) ［**Add a role assignment**］ボックスで、［**Add**］を選択します。

i) ［**Add role assignment**］タブで、以下を選択します：

- **Role**： Contributor（共同作成者）
- **Assign access to**： Azure AD ユーザー、グループ、またはサービスプリンシパル
- **Select**：以前に作成した Azure アプリの名前。

j) ［**Save**］を選択します。

Citrix DaaS にサブスクリプションを追加する　Azure AD で作成したアプリのアプリケーション ID、ディレクトリ ID、クライアントシークレットの値が必要です。

1. ［管理］**>**［クイック展開］を選択してから、右側にある ［**Cloud** サブスクリプション］を開きます。
2. ［**Azure** サブスクリプションを追加する］を選択します。
3. ［サブスクリプションの追加］ページで、［**Azure** サブスクリプションの追加］を選択します。
4. ［サブスクリプションの共同作成者の役割を持つ **Azure** アプリがある］を選択します。
5. Azure で作成したアプリのテナント ID（ディレクトリ ID）、クライアント ID（アプリケーション ID）、およびクライアントシークレットを入力します。
6. ［サブスクリプションの選択］を選択してから、必要なサブスクリプションを選択します。

後から、Citrix DaaS ダッシュボードのサブスクリプションの ［詳細］ページで、クライアントシークレットを更新するか、省略記号（…）メニューから Azure アプリを置き換えることができます。

追加後に Citrix DaaS が Azure サブスクリプションにアクセスできない場合、いくつかのカタログ電源管理と個々のマシン操作が許可されません。メッセージには、サブスクリプションを再度追加するオプションが表示されます。サブスクリプションが元々 Azure アプリを使用して追加されたものである場合は、Azure アプリを置き換えることができます。

Citrix Managed Azure サブスクリプションの追加

Citrix Managed Azure サブスクリプションは、特定の数のマシンをサポートします（ここでは、マシンとは Citrix VDA がインストールされている VM を指します。これらのマシンは、アプリとデスクトップをユーザーに配信します。Cloud Connector など、リソースの場所にある他のマシンは含まれません）。

Citrix Managed Azure サブスクリプションがまもなく制限に達する可能性があり、十分な Citrix ライセンスがある場合は、別の Citrix Managed Azure サブスクリプションを要求できます。ダッシュボードには、制限に近づいたときに通知が表示されます。

その Citrix Managed Azure サブスクリプションを使用するすべてのカタログのマシンの総数が制限を超える場合、カタログを作成（またはカタログにマシンを追加）することはできません。

たとえば、Citrix Managed Azure サブスクリプションごとに 1,000 台のマシンという架空の制限があるとします。

- 同じ Citrix Managed Azure サブスクリプションを使用する 2 つのカタログ（`Cat1`と`Cat2`）があるとします。`Cat1`には現在 500 台のマシンがあり、`Cat2`には 250 台のマシンがあります。
- 将来の容量のニーズを考慮して、`Cat2`に 200 台のマシンを追加します。Citrix Managed Azure サブスクリプションは、現在、950 台のマシンをサポートしています（`Cat 1`で 500 台、`Cat 2`で 450 台）。ダッシュボードには、サブスクリプションが制限に近づいているという通知が表示されます。
- さらに 75 台のマシンが必要な場合、そのサブスクリプションを使用して、75 台のマシンでカタログを作成する（または既存のカタログに 75 台のマシンを追加する）ことはできません。サブスクリプションの制限を超えてしまうためです。代わりに、別の Citrix Managed Azure サブスクリプションを要求します。次に、そのサブスクリプションを使用してカタログを作成できます。

複数の Citrix Managed Azure サブスクリプションがある場合：

- これらのサブスクリプション間で共有されるものはありません。
- 各サブスクリプションには一意の名前があります。
- 以下を実行する場合に、Citrix Managed Azure サブスクリプション（および追加した顧客管理の Azure サブスクリプション）の中から選択できます：
  - カタログの作成。
  - イメージの作成またはインポート。
  - VNet ピアリングまたは SD-WAN 接続の作成。

要件：

- 別の Citrix Managed Azure サブスクリプションを確実に追加できるようにするには、十分な Citrix ライセンスが必要です。前述の架空の例では、Citrix Managed Azure サブスクリプションを使用して少なくとも 1,500 台のマシンを展開することを見越し、2,000 個の Citrix ライセンスがある場合、別の Citrix Managed Azure サブスクリプションを追加できます。

Citrix Managed Azure サブスクリプションを追加するには:

1. Citrix の担当者に連絡して、別の Citrix Managed Azure サブスクリプションを要求してください。続行できるようになれば、担当者がお知らせします。
2. ［管理］**>**［クイック展開］を選択してから、右側にある ［**Cloud** サブスクリプション］を開きます。
3. ［**Azure** サブスクリプションを追加する］を選択します。
4. ［サブスクリプションの追加］ページで、［**Citrix Managed Azure** サブスクリプションの追加］を選択します。
5. ［**Citrix Managed** サブスクリプションの追加］ページ下部で、［サブスクリプションの追加］を選択します。

Citrix Managed Azure サブスクリプションの作成中にエラーが発生したという通知があった場合は、Citrix サポートにお問い合わせください。

Azure サブスクリプションの削除

Azure サブスクリプションを削除する前に、それを使用するすべてのカタログとイメージを削除する必要があります。

1 つまたは複数の Citrix Managed Azure サブスクリプションがある場合、それらすべてを削除することはできません。少なくとも 1 つは残っている必要があります。

1. ［管理］**>**［クイック展開］を選択してから、右側にある ［**Cloud** サブスクリプション］を開きます。
2. サブスクリプションエントリを選択します。
3. ［詳細］タブで、［サブスクリプションの削除］を選択します。
4. ［**Azure** アカウントを認証する］を選択します。Azure のサインインページが表示されます。
5. Azure の資格情報を入力します。
6. 自動的に Citrix DaaS に戻ります。削除対象を確認してから、［はい、サブスクリプションを削除します］を選択します。

有効期限が切れたクライアントシークレットの更新

サブスクリプションのクライアントシークレットの有効期限が切れると、そのサブスクリプションのマシンカタログを作成できなくなり、サブスクリプションのエントリに通知が表示されます。この問題の解決方法としては、以下の 2 つの選択肢があります。

- 使用中の Azure アプリのクライアントシークレットを更新する
- 有効期限が切れていない Azure アプリに切り替える

使用中の **Azure** アプリのクライアントシークレットを更新する

既存の Azure アプリを引き続き使用して Azure リソースにアクセスするには、次の手順に従います。

1. Azure で、使用中の Azure アプリ向けにクライアントシークレットを作成します。新規作成したシークレットとその有効期限を今後使用できるように書き留めておきます。詳しくは、「Azure でのアプリケーションシークレットの作成」を参照してください。
2. DaaS で、新規作成したシークレット情報をサブスクリプションに提供します。詳細な手順は次のとおりです:

    a) Citrix DaaS for Azure で［管理者］から［**Azure Quick Deploy**］を選択して表示されるダッシュボードで、右側の［**Cloud** サブスクリプション］を展開します。
    b) シークレットの更新が必要なサブスクリプションをクリックします。
    c) 表示されるサブスクリプションページで、**Azure** アプリの詳細ペインの省略記号メニューをクリックし、［クライアントシークレットの更新］を選択します。
    d)［クライアントシークレットの更新］ページで、新しい クライアントシークレットとシークレットの有効期限を入力します。
    e)［シークレットの更新］をクリックします。

有効期限が切れていない **Azure** アプリに切り替える

有効な Azure アプリに切り替えて Azure リソースにアクセスするには、次の手順を使用して必要なアプリ情報を取得し、サブスクリプションに提供します。

1. Azure で、有効な Azure アプリを取得し、その詳細を書き留めます。新しい Azure アプリに共同作成者の役割が割り当てられていることを確認してます。詳しくは、「Azure AD でアプリを作成し、共同作成者として追加する」を参照してください。
2. DaaS で、Azure アプリの詳細をサブスクリプションに提供します。詳細な手順は次のとおりです:

    a) Citrix DaaS for Azure で［管理者］から［**Azure Quick Deploy**］を選択して表示されるダッシュボードで、右側の［**Cloud** サブスクリプション］を展開します。
    b) シークレットの更新が必要なサブスクリプションをクリックします。
    c) 表示されるサブスクリプションページで、［**Azure** アプリの詳細］ペインの省略記号メニューをクリックし、［**Azure** アプリの置き換え］を選択します。
    d)［**Azure** アプリの置き換え］ページで、［ディレクトリ **(**テナント**) ID**］、［アプリケーション **(**クライアント**) ID**］、［クライアントシークレット］、および［**Secret Expiration Date for the service principal**］の各フィールドに対応する同名のフィールドに、新しい Azure アプリの詳細を入力します。
    e)［アプリの置き換え］をクリックします。

クイック展開でのイメージ

May 17, 2024

デスクトップまたはアプリを配信するためにカタログを作成すると、マシンを作成するためのテンプレートとしてイメージが（他の設定とともに）使用されます。

［クイック展開］では、事前提供されているイメージのセットを使用でき、その中から選択して［クイック展開］内でイメージを作成およびカスタマイズできます。顧客自身の Azure サブスクリプションからイメージをインポート（追加）することもできます。

Citrix 提供イメージ

［クイック展開］では、Citrix 提供イメージを使用できます:

- Windows 11 Pro （シングルセッション）
- Windows 11 Enterprise Virtual Desktop（マルチセッション）
- Office 365 ProPlus を使用する Windows 11 Enterprise Virtual Desktop（マルチセッション）
- Windows 10（シングルセッション）
- Windows 10 Enterprise Virtual Desktop（マルチセッション）
- Office 365 ProPlus を使用する Windows 10 Enterprise Virtual Desktop（マルチセッション）
- Windows Server 2022（マルチセッション）
- Windows Server 2019（マルチセッション）
- Windows Server 2016（マルチセッション）
- Linux Ubuntu 22.04 LTS（シングルセッション）
- Linux Ubuntu 22.04 LTS（マルチセッション）

Citrix 提供イメージには、現在の Citrix Virtual Delivery Agent（VDA）とトラブルシューティングツールがインストールされています。VDA は、ユーザーのマシンと、Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）を管理する Citrix Cloud インフラストラクチャとの間の通信メカニズムです。Citrix 提供イメージには **CITRIX** 表記があります。

Citrix 提供イメージは、Citrix DaaS の［完全な構成］インターフェイスでは使用できません。

Azure から顧客自身のイメージをインポートして使用することもできます。

クイック展開でイメージを使用する方法

次の操作を実行できます:

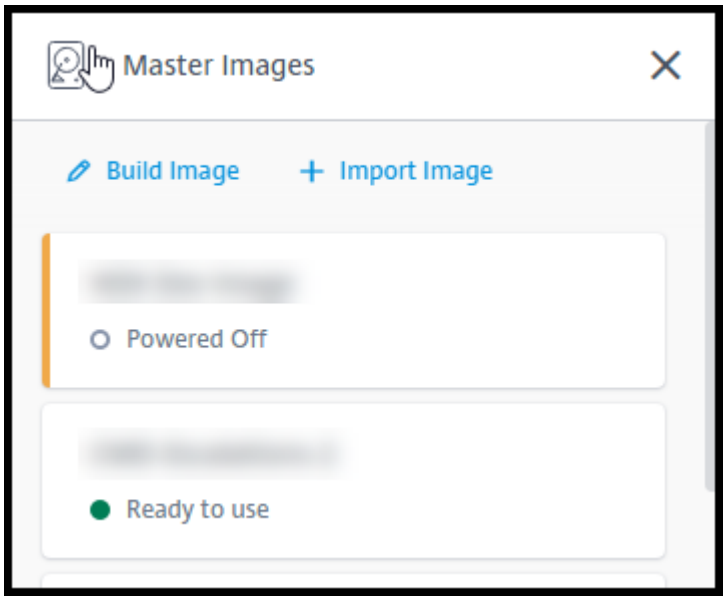
- カタログ作成時に、**Citrix** 提供イメージを使用する。この選択肢は、概念実証の展開を行う場合にのみ推奨されます。
- **Citrix** 提供イメージを使用して、別のイメージを作成する。新しいイメージの作成後、ユーザーが必要とするアプリケーションやその他のソフトウェアを追加して、イメージをカスタマイズします。その後、カタログを作成するときに、そのカスタマイズされたイメージを使用できます。
- **Azure** からイメージをインポートする。Azure からイメージをインポートした後、カタログを作成するときに、そのイメージを使用できます。

または、そのイメージを使用して新しいイメージを作成し、アプリを追加してカスタマイズすることもできます。その後、カタログを作成するときに、そのカスタマイズされたイメージを使用できます。

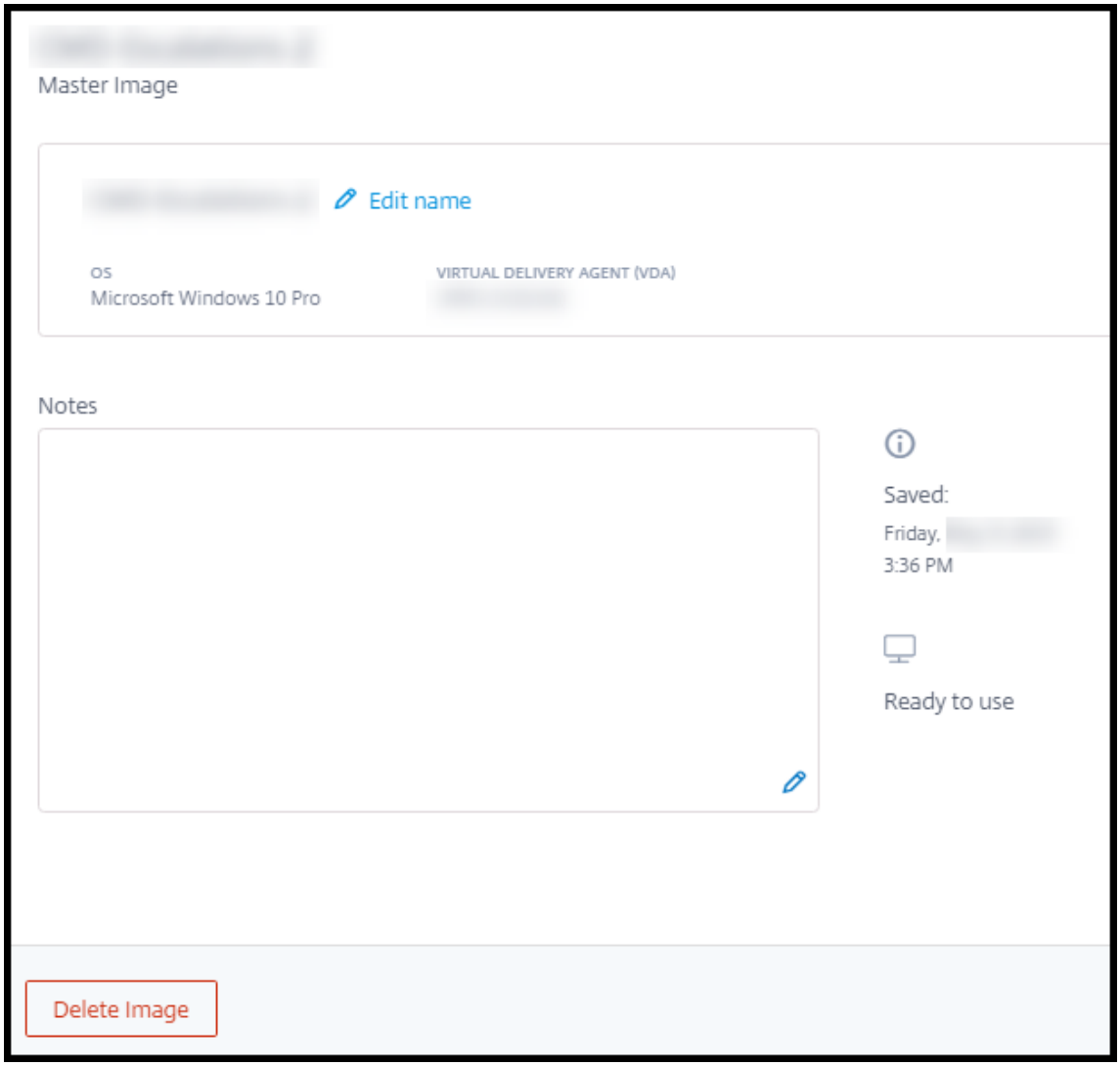
カタログを作成すると、Citrix DaaS は、イメージで有効なオペレーティングシステムが使用されていること、および Citrix VDA とトラブルシューティングツールがインストールされていることを（他のチェックとともに）確認します。

イメージ情報の表示

1. ［管理］**>**［クイック展開］の右側にある ［マスターイメージ］を開きます。画面には、Citrix 提供イメージとインポートしたイメージが一覧表示されます。



2. イメージを選択して詳細を表示します。



この詳細カードで、次のことができます:

- イメージ名の変更（編集）。
- メモを追加および編集（これは、Citrix 提供イメージではなく、事前提供のイメージまたはインポートしたイメージでのみ使用できます）。
- イメージの削除。

新しいイメージの準備

新しいイメージの準備には、イメージを作成してからそれをカスタマイズする作業が含まれます。イメージを作成すると、新しい VM が作成され、新しいイメージを読み込みます。

要件:

- マシンに必要なパフォーマンス特性を把握すること。たとえば、CAD アプリを実行するには、他の Office アプリとは異なる CPU、RAM、およびストレージが必要になる場合があります。

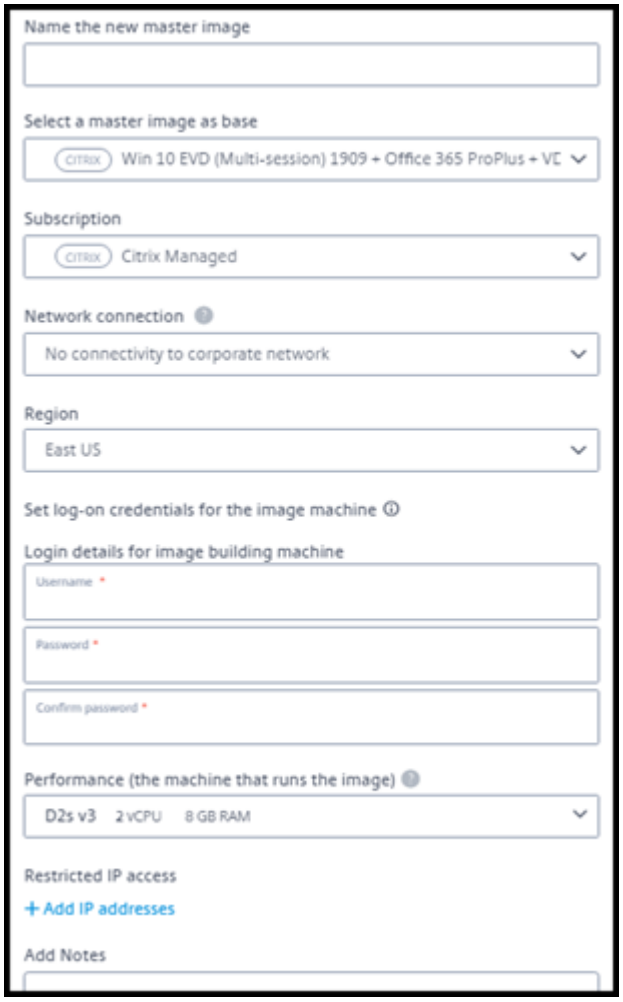
- オンプレミスリソースへの接続を行う予定の場合は、イメージとカタログを作成する前にその接続を設定すること。詳しくは、「ネットワーク接続」を参照してください。

Citrixs 提供の Ubuntu イメージを使用して新しいイメージを作成すると、新しいイメージのルートパスワードが作成されます。このルートパスワードは変更できますが、変更できるのはイメージの作成およびカスタマイズを行うときのみです（イメージがカタログで使用された後に、ルートパスワードを変更することはできません）。

- イメージが作成されると、指定した管理者アカウント（イメージ作成マシンのログインの詳細）が`sudoers`グループに追加されます。
- 新しいイメージを含むマシンに RDP 接続した後、端末アプリケーションを起動し、「`sudo passwd root`」と入力します。プロンプトが表示されたら、イメージの作成時に指定したパスワードを入力します。確認後、ルートユーザーの新しいパスワードを入力するように求められます。

イメージを作成するには：

1. ［管理］**>**［クイック展開］の右側にある ［マスターイメージ］を開きます。
2. ［イメージの作成］を選択します。



3. 次のフィールドに値を入力します：

- 名前：新しいイメージの名前を入力します。
- マスターイメージ：既存のイメージを選択します。これは、新しいイメージを作成するために使用されるベースイメージです。
- サブスクリプション： Azure サブスクリプションを選択します。
- ネットワーク接続：
  - Citrix Managed Azure サブスクリプションを使用している場合は、［接続なし］または以前に作成した接続を選択します。
  - 独自の顧客管理の Azure サブスクリプションを使用している場合は、リソースグループ、仮想ネットワーク、およびサブネットを選択します。次に、ドメインの詳細：FQDN、OU、Citrix DaaS アカウント名、および資格情報を追加します。
- リージョン：（［接続なし］の場合にのみ使用可能。）イメージを含むマシンを作成するリージョンを選択します。
- イメージマシンのログオン資格情報：後で、新しいイメージを含むマシンに接続（RDP）するときに、これらの資格情報を使用して、アプリやその他のソフトウェアをインストールできるようにします。
- マシンパフォーマンス：これは、イメージを実行するマシンの CPU、RAM、およびストレージの情報です。アプリの要件を満たすマシンパフォーマンスを選択します。
- 制限付き **IP** アクセス：特定のアドレスへのアクセスを制限する場合は、［**IP** アドレスの追加］を選択してから、1 つまたは複数のアドレスを入力します。アドレスを追加したら、［完了］を選択して ［イメージの作成］カードに戻ります。
- 注：オプションで、最大 1,024 文字のメモを追加できます。イメージが作成されたら、イメージの詳細画面でメモを更新できます。
- ローカルドメインへの参加：ローカルの Active Directory ドメインに参加するかどうかを指定します。
  - ［はい］を選択した場合は、FQDN、OU、Citrix DaaS アカウント名、および資格情報を入力します。
  - ［いいえ］を選択した場合は、ホストマシンの資格情報を入力します。

4. 完了したら、［イメージの作成］を選択します。

イメージの作成には最大 30 分かかることがあります。［管理］**>**［クイック展開］の右側にある ［マスターイメージ］を開き、現在の状態（[Building image]や [Ready to customize]など）を確認します。

次にやること：新しいイメージに接続してカスタマイズします。

新しいイメージへの接続とカスタマイズ

新しいイメージが作成されると、その名前がイメージ一覧に追加され、状態は [Ready to customize]（または類似の表現）になります。そのイメージをカスタマイズするには、最初に RDP ファイルをダウンロードします。

そのファイルを使用してイメージに接続すると、アプリケーションやその他のソフトウェアをイメージに追加できます。

1. ［管理］**>**［クイック展開］の右側にある ［マスターイメージ］を開きます。接続するイメージを選択します。
2. ［**RDP** ファイルのダウンロード］を選択します。RDP クライアントがダウンロードされます。

   イメージマシンを作成した直後に RDP を実行しないと、イメージマシンの電源がオフになる場合があります。これはコスト節約のためです。その場合は、［電源オン］を選択してください。
3. ダウンロードした RDP クライアントを起動します。自動的に、新しいイメージを含むマシンのアドレスに接続しようとします。プロンプトが表示されたら、イメージの作成時に指定した資格情報を入力します。
4. マシンに接続したら、アプリを追加または削除し、更新プログラムをインストールして、その他のカスタマイズ作業を完了します。

   イメージに Sysprep を使用しないでください。
5. 新しいイメージのカスタマイズが完了したら、［マスターイメージ］ボックスに戻り、［作成の完了］を選択します。新しいイメージは自動的に検証テストを受けます。

後でカタログを作成すると、選択可能なイメージの一覧にこの新しいイメージが表示されます。

［管理］**>**［クイック展開］の右側のイメージ画面には、各イメージを使用するカタログとマシンの数が表示されます。

> 注:
>
> イメージをファイナライズした後は、イメージを編集できなくなります。新しいイメージを作成（オプションで以前のイメージを開始点として使用）し、新しいイメージを更新する必要があります。

Azure からのイメージのインポート

Citrix VDA とユーザーが必要とするアプリケーションを備えたイメージを Azure からインポートすると、そのイメージを使用してカタログを作成したり、既存のカタログのイメージを置き換えたりすることができます。

インポートされたイメージの要件

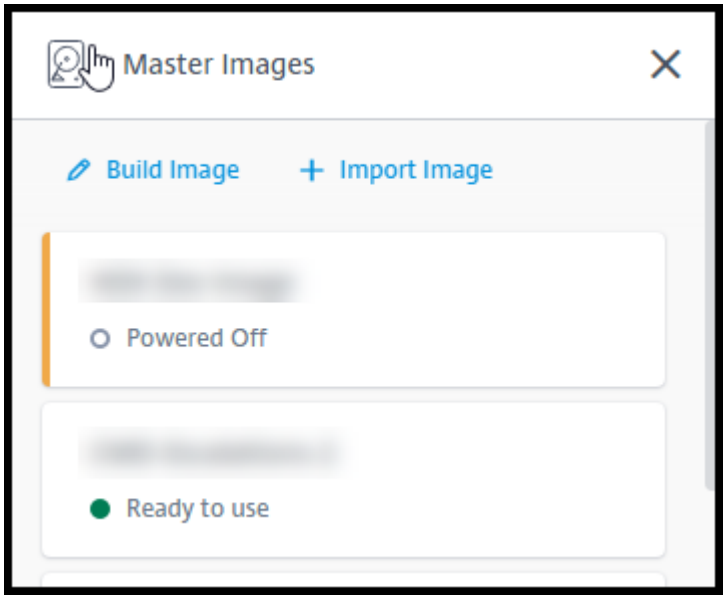
Citrix は、インポートされたイメージに対して検証テストを実行します。Citrix DaaS にインポートするイメージを準備するときは、次の要件が満たされていることを確認してください。

- サポートされるオペレーティングシステム：イメージはサポートされている OSである必要があります。Windows OS のバージョンを確認するには、「`Get-WmiObject Win32_OperatingSystem`」を実行します。
- サポートされている世代：第 1 世代の仮想マシンは、ほとんどのゲストオペレーティングシステムをサポートします。第 2 世代の仮想マシンは、Windows のほとんどの 64 ビットバージョンと、Linux オペレーティングシステムの最新バージョンをサポートします。

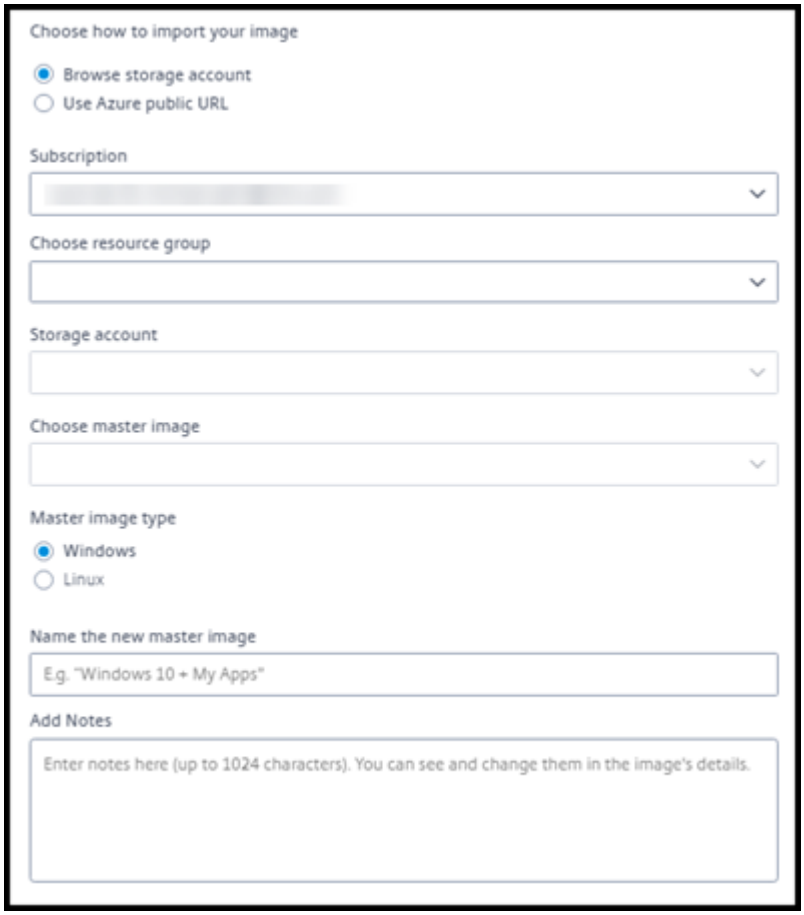
- 一般化しない イメージは一般化されてはいけません。
- 構成された **Delivery Controller** がない：イメージで Citrix Delivery Controller が構成されていないことを確認します。次のレジストリキーがないことを確認してください。
  - `HKLM:\SOFTWARE\Citrix\VirtualDesktopAgent\ListOfDDCs`
  - `HKLM:\SOFTWARE\Policies\Citrix\VirtualDesktopAgent\ListOfDDCs`
  - `HKLM:\SOFTWARE\Citrix\VirtualDesktopAgent\FarmGUID`
  - `HKLM:\SOFTWARE\Policies\Citrix\VirtualDesktopAgent\FarmGUID`
- **Personality.ini** ファイル： `personality.ini`ファイルはシステムドライブに存在する必要があります。
- 有効な **VDA**：イメージには 7.11 より新しい Citrix VDA がインストールされている必要があります。
  - Windows：確認するには、`Get HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Citrix Virtual Desktop Agent`を使用します。インストール手順については、「イメージへの Windows VDA のインストール」を参照してください。
  - Red Hat Enterprise Linux および Ubuntu：インストール手順については、製品ドキュメントを参照してください。
- **Azure** 仮想マシンエージェント：イメージをインポートする前に、Azure 仮想マシンエージェントがイメージにインストールされていることを確認してください。詳しくは、Microsoft 社の記事「Azure 仮想マシンエージェントの概要」を参照してください。

クイック展開を使用したイメージのインポート

1. ［管理］**>**［クイック展開］の右側にある ［マスターイメージ］を開きます。



2. ［イメージのインポート］を選択します。



3. イメージのインポート方法を選択します。

   - 管理対象ディスクの場合は、エクスポート機能を使用して SAS URL を生成します。有効期限を 7,200 秒以上に設定してください。
   - ストレージアカウントの VHD の場合は、次のいずれかを選択します:
     - VHD ファイルの SAS URL を生成する。
     - ブロックストレージコンテナのアクセスレベルを BLOB またはコンテナに更新する。その後、ファイルの URL を取得する。

4. ［ストレージアカウントの参照］を選択した場合:

   a) ［サブスクリプション］>［リソースグループ］>［ストレージアカウント］>［イメージ］の順に選択します。
   b) イメージに名前を付けます。

5. ［**Azure** パブリック **URL**］を選択した場合:

   a) VHD の Azure 生成 URL を入力します。ガイダンスについては、Microsoft 社のドキュメント「Azure から Windows VHD をダウンロードする」へのリンクを選択してください。

b) サブスクリプションを選択します（Linux イメージは、顧客管理のサブスクリプションを選択した場合にのみインポートできます）。
c) イメージに名前を付けます。

6. 完了したら、［イメージのインポート］を選択します。

新しいイメージでのクイック展開カタログの更新

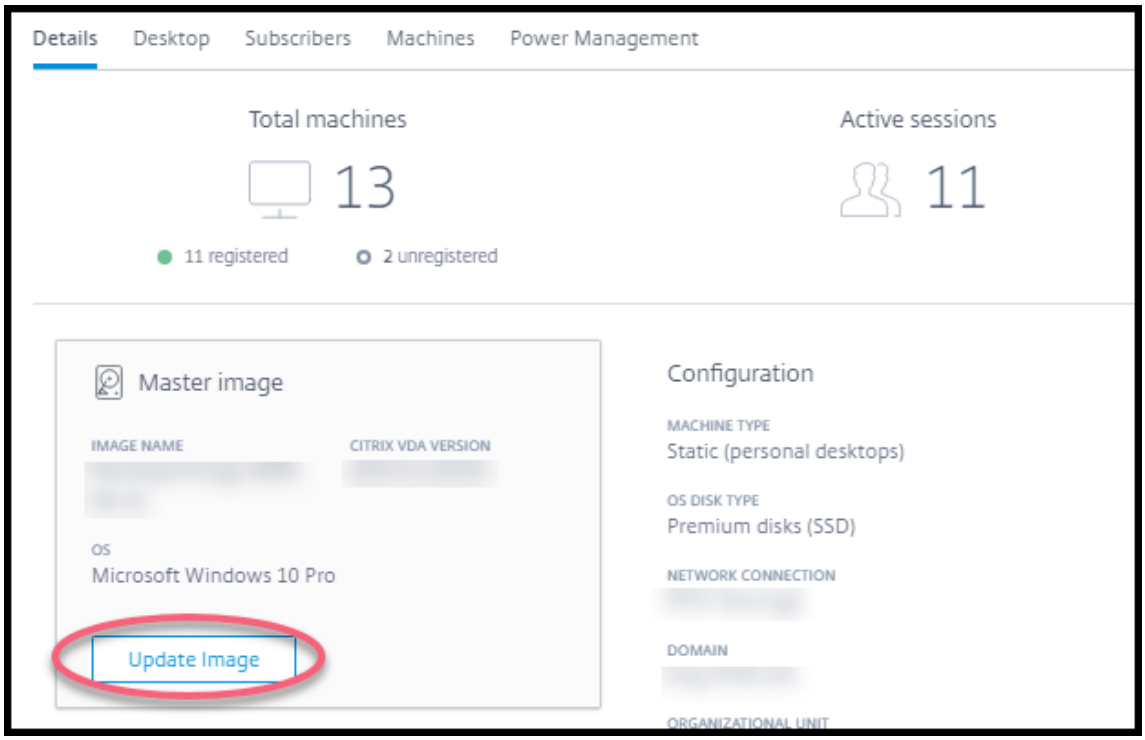
カタログの種類によって、カタログを更新するときに更新されるマシンが決まります。

- ランダムカタログの場合、現在カタログにあるすべてのマシンが最新のイメージで更新されます。そのカタログにさらにデスクトップを追加すると、それらのデスクトップは最新のイメージに基づきます。
- 静的カタログの場合、現在カタログにあるマシンは最新のイメージで更新されません。現在カタログにあるマシンは、作成元のイメージを引き続き使用します。ただし、そのカタログにさらにマシンを追加すると、それらのマシンは最新のイメージに基づきます。

カタログのマシンが第 2 世代をサポートしている場合は、第 1 世代イメージのマシンを含むカタログを第 2 世代イメージで更新できます。同様に、カタログのマシンが第 1 世代をサポートしている場合は、第 2 世代マシンを含むカタログを第 1 世代イメージで更新できます。

新しいイメージでカタログを更新するには:

1. ［管理］**>**［クイック展開］で、カタログのエントリの任意の場所をクリックします。
2. ［詳細］タブで、［イメージの更新］を選択します。



3. イメージを選択します。
4. ランダムカタログまたはマルチセッションカタログの場合：ログオフ間隔を選択します。Citrix DaaS が最初のイメージ処理を完了すると、利用者は、作業を保存してデスクトップからログオフするよう警告を受け取ります。ログオフ間隔は、利用者がメッセージを受け取ってからセッションが自動的に終了するまでの時間を示します。
5. ［イメージの更新］を選択します。

クイック展開からのイメージの削除

1. ［管理］**>**［クイック展開］の右側にある ［マスターイメージ］を開きます。
2. 削除するイメージを選択します。
3. カードの下部にある ［イメージの削除］を選択します。削除を確認します。

イメージへの **Windows VDA** のインストール

Citrix DaaS にインポートする予定の Windows イメージを準備するときは、次の手順に従います。

Linux VDA インストールの手順については、Linux VDA の製品ドキュメントを参照してください。

1. Azure 環境で、イメージ VM に接続します（まだ接続していない場合）。
2. Citrix Cloud のナビゲーションバーの ［ダウンロード］リンクから、VDA をダウンロードできます。または、ブラウザーで Citrix DaaSダウンロードページに移動します。

   VDA を VM にダウンロードします。デスクトップ（シングルセッション）OS 用と、サーバー（マルチセッション）OS 用に、別々の VDA ダウンロードパッケージがあります。
3. ダウンロードしたファイルをダブルクリックして、VDA インストーラーを起動します。インストールウィザードが起動します。
4. ［環境］ページで、MCS を使用してイメージを作成するオプションを選択してから ［次へ］を選択します。
5. ［コアコンポーネント］ページで ［次へ］を選択します。
6. ［**Delivery Controller**］ページで、［**Machine Creation Services** で自動的に指定する］を選択して ［次へ］を選択します。プロンプトが表示されたら、選択内容を確認します。
7. ［追加コンポーネント］、［機能］、［ファイアウォール］の各ページの設定については、Citrix から別途指示がない限りデフォルトのままにします。各ページで ［次へ］を選択します。
8. ［概要］ページで ［インストール］を選択します。前提条件のインストールが始まります。再起動を求められたら、同意します。
9. VDA のインストールは自動的に再開されます。前提条件のインストールが完了すると、コンポーネントと機能がインストールされます。［**Call Home**］ページの設定は、Citrix から別途指示がない限りデフォルトのままにします。接続したら、［次へ］を選択します。

10. ［完了］を選択します。マシンが自動的に再起動します。
11. 正常に構成されたことを確認するため、VM にインストールしたアプリケーションを 1 つまたは複数起動します。
12. 仮想マシンをシャットダウンします。Sysprep は使用しないでください。

VDA のインストールについて詳しくは、「VDA のインストール」を参照してください。

クイック展開でのネットワーク接続

May 17, 2024

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

はじめに

この記事では、Citrix Managed Azure サブスクリプションを使用する場合に、企業リソースへのネットワーク接続を作成する方法について詳しく説明します。

独自の顧客管理の Azure サブスクリプションを使用する場合、ネットワーク接続を作成する必要はありません。

クイック展開カタログを作成するとき、ユーザーが Citrix のデスクトップとアプリから企業のオンプレミスネットワーク上の場所とリソースにアクセスするかどうか、およびアクセス方法を指定します。接続を使用する場合は、カタログを作成する前に接続を作成する必要があります。

Citrix Managed Azure サブスクリプションを使用する場合、選択肢は次のとおりです:

- 接続なし
- Azure VNet ピアリング
- SD-WAN

カタログの作成後にカタログの接続の種類を変更することはできません。

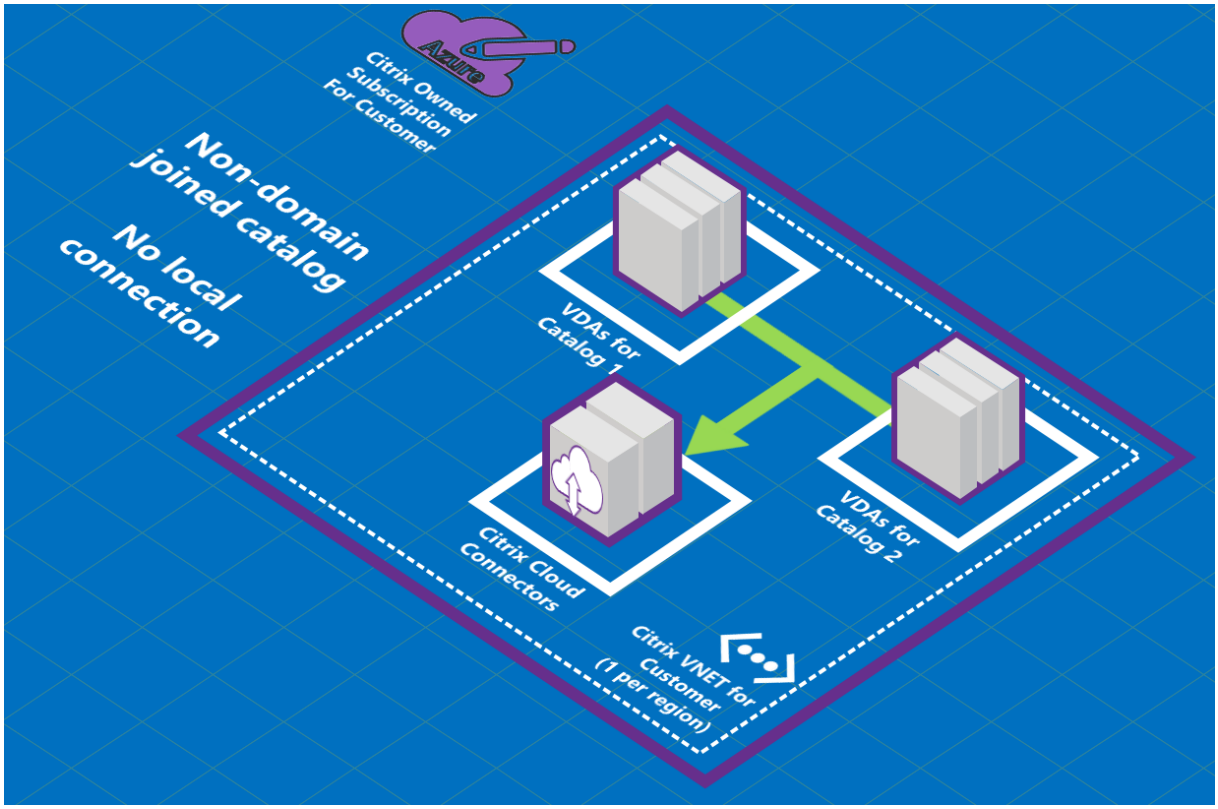
すべてのネットワーク接続の要件

- 接続を作成するときは、有効なDNS サーバーエントリが必要です。

- Secure DNS またはサードパーティの DNS プロバイダーを使用する場合は、Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）で使用するために割り当てられたアドレス範囲を、許可リストにある DNS プロバイダーの IP アドレスに追加する必要があります。このアドレス範囲は、接続を作成するときに指定します。
- 接続を使用するすべてのサービスリソース（ドメイン参加済みマシン）は、確実に時間同期できるよう、ネットワークタイムプロトコル（NTP）サーバーに到達できる必要があります。

接続なし

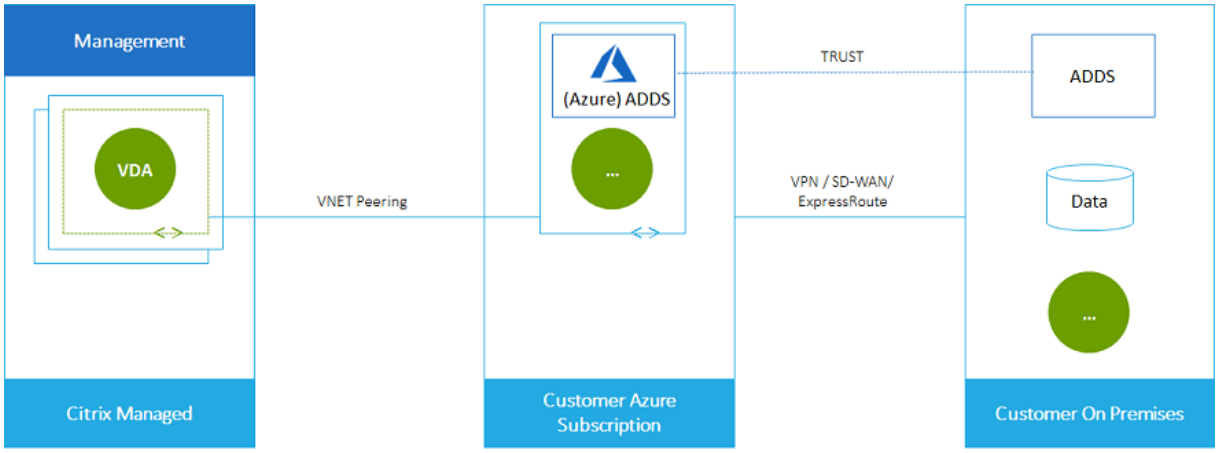
カタログが ［接続なし］で構成されている場合、ユーザーはオンプレミスまたは他のネットワーク上のリソースにアクセスできません。簡易作成を使用してカタログを作成する場合、これが唯一の選択肢です。



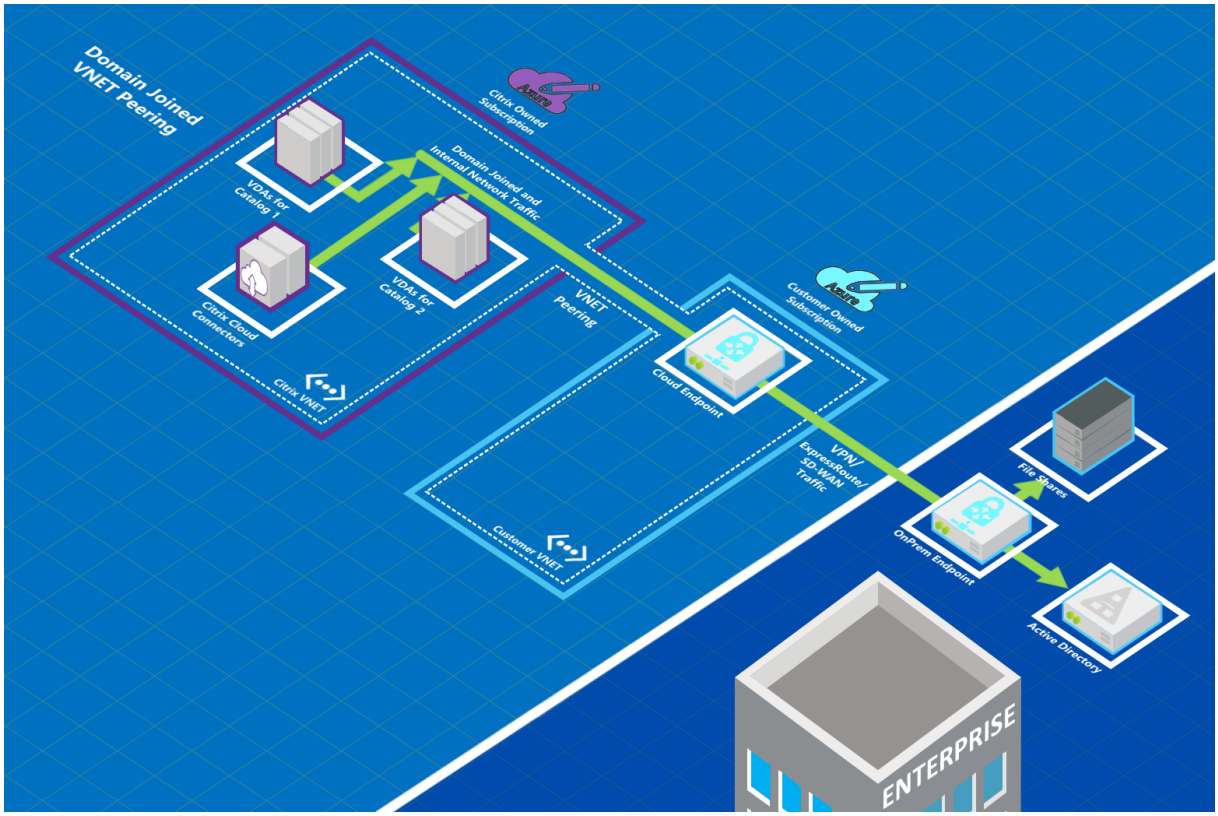
Azure VNet ピアリング接続について

仮想ネットワークピアリングは、2 つの Azure 仮想ネットワーク（VNet）：つまりユーザーのネットワークと Citrix DaaS VNet を、シームレスに接続します。ピアリングは、ユーザーがオンプレミスネットワークからファイルやその他のアイテムにアクセスできるようにするのにも役立ちます。

次の図に示すように、Azure VNet ピアリングを使用して、Citrix Managed Azure サブスクリプションから会社の Azure サブスクリプションの VNet への接続を作成します。



これは、VNet ピアリングの別の図です。



ユーザーは、カタログの作成時にローカルドメインに参加することで、ネットワークリソース（ファイルサーバーなど）にアクセスできます（つまり、ファイル共有やその他の必要なリソースが存在する AD ドメインに参加します）。Azure サブスクリプションは、これらのリソースに接続します（図では、VPN または Azure ExpressRoute を使用しています）。カタログを作成するときに、ドメイン、OU、およびアカウントの資格情報を指定します。

> 重要：
>
> - このサービスで使用する前に、Azure VNet ピアリングについて詳細を把握しておいてください。
> - VNet ピアリング接続を使用するカタログを作成する前に、VNet ピアリング接続を作成します。

Azure VNet ピアリングカスタムルート

カスタムまたはユーザー定義のルートは、VNet ピアリング、オンプレミスネットワーク、およびインターネットの仮想マシン間でトラフィックを転送するため、Azure のデフォルトのシステムルートよりも優先されます。Citrix DaaS のリソースがアクセスする予定だが VNet ピアリングで直接接続されていないというネットワークがある場合は、カスタムルートを使用できます。たとえば、強制的にトラフィックをネットワークアプライアンス経由でインターネットまたはオンプレミスネットワークサブネットに転送するカスタムルートを作成できます。

カスタムルートを使用するには:

- Citrix DaaS 環境には、既存の Azure 仮想ネットワークゲートウェイ、または Citrix SD-WAN などのネットワークアプライアンスが必要です。
- カスタムルートを追加するときは、エンドツーエンドの接続を確保するために、Citrix DaaS の接続先 VNet 情報を使用して会社のルートテーブルを更新する必要があります。
- カスタムルートは、入力した順序で Citrix DaaS に表示されます。この表示順序は、Azure がルートを選択する順序には影響しません。

カスタムルートを使用する前に、Microsoft 社の記事「仮想ネットワークトラフィックのルーティング」を確認して、カスタムルートの使用方法、次ホップの種類、および Azure が送信トラフィックのルートを選択する方法について把握しておいてください。

Azure VNet ピアリング接続を作成するとき、または Citrix DaaS 環境内の既存の接続に、カスタムルートを追加できます。VNet ピアリングでカスタムルートを使用する準備ができたら、この記事の次のセクションを参照してください:

- 新しい Azure VNet ピアリングを使用するカスタムルートの場合：Azure VNet ピアリング接続の作成
- 既存の Azure VNet ピアリングを使用するカスタムルートの場合：既存の Azure VNet ピア接続のカスタムルートの管理

AzureVNet ピアリングの要件と準備

- Azure サブスクリプション所有者の資格情報。これは Azure Active Directory アカウントである必要があります。このサービスは、live.com や外部の Azure AD アカウント（別のテナント内）など、他のアカウントの種類をサポートしていません。
- Azure サブスクリプション、リソースグループ、および仮想ネットワーク（VNet）。
- Citrix Managed Azure サブスクリプションの VDA がネットワークの場所と通信できるように、Azure ネットワークルートを設定します。
- VNet から指定 IP 範囲までの Azure ネットワークセキュリティグループを開きます。
- **Active Directory**：ドメイン参加済みのシナリオでは、ピアリングされた VNet でなんらかの形式の Active Directory サービスを実行していることをお勧めします。これは、Azure VNet ピアリングテクノロジの低遅延特性を利用します。

たとえば、構成には、Azure Active Directory Domain Services（AADDS）、VNet のドメインコントローラー VM、またはオンプレミス Active Directory への Azure AD Connect が含まれる場合があります。

AADDS を有効にした後、管理対象ドメインを削除せずにその管理対象ドメインを別の VNet に移動することはできません。そのため、管理対象ドメインを有効にするには、正しい VNet を選択することが重要です。先に進む前に、Microsoft 社の記事「Azure Active Directory Domain Services の仮想ネットワーク設計の考慮事項と構成オプション」を確認してください。

- **VNet IP** 範囲：接続を作成するとき、ネットワークリソースと接続中 Azure VNet との間で一意の使用可能な CIDR アドレス空間（IP アドレスとネットワークプレフィックス）を入力する必要があります。これは、Citrix DaaS のピアリングされた VNet 内の VM に割り当てられた IP 範囲です。

  Azure およびオンプレミスネットワークで使用するアドレスと重複しない IP 範囲を指定していることを確認してください。

  - たとえば、Azure VNet のアドレス空間が 10.0.0.0 /16 の場合、Citrix DaaS で 192.168.0.0 /24 などの VNet ピアリング接続を作成します。
  - この例では、10.0.0.0 /24 の IP 範囲でピアリング接続を作成すると、アドレス範囲に重複すると見なされます。

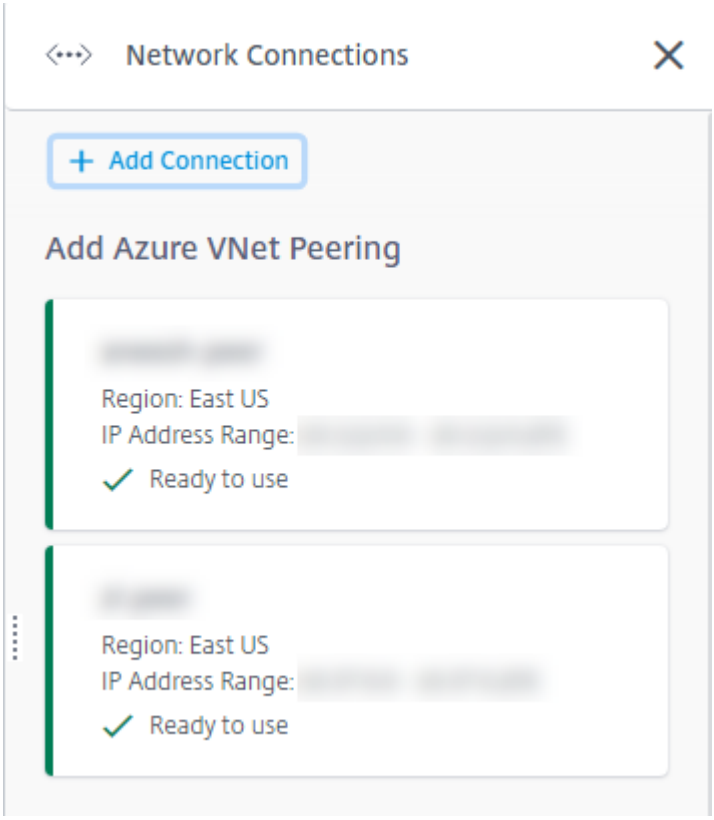
  アドレスが重複している場合、VNet ピアリング接続が正常に作成されない可能性があります。また、サイト管理タスクで接続が正しく機能しません。

VNet ピアリングについては、次の Microsoft 社の記事を参照してください。

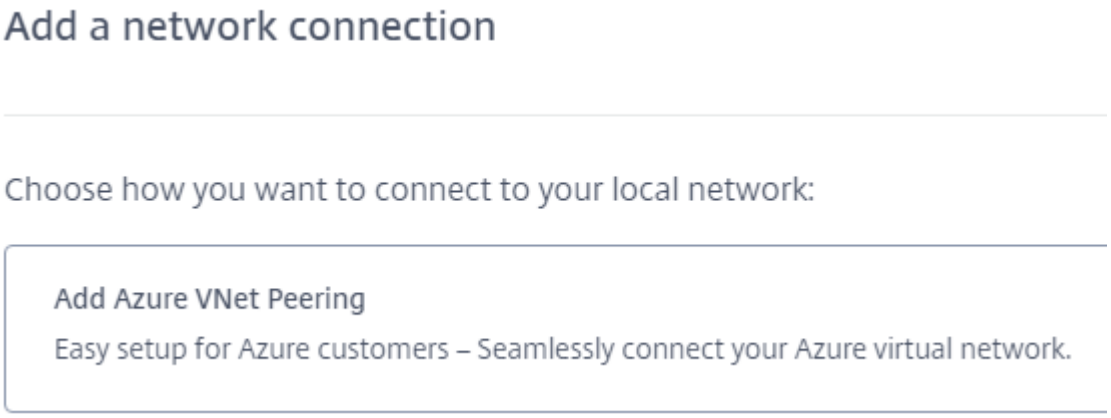
- 仮想ネットワークピアリング
- Azure VPN ゲートウェイ
- Azure ポータルでのサイト間接続の作成
- VPN ゲートウェイに関するよくある質問（「重複」（overlap）を検索）

Azure VNet ピアリング接続の作成

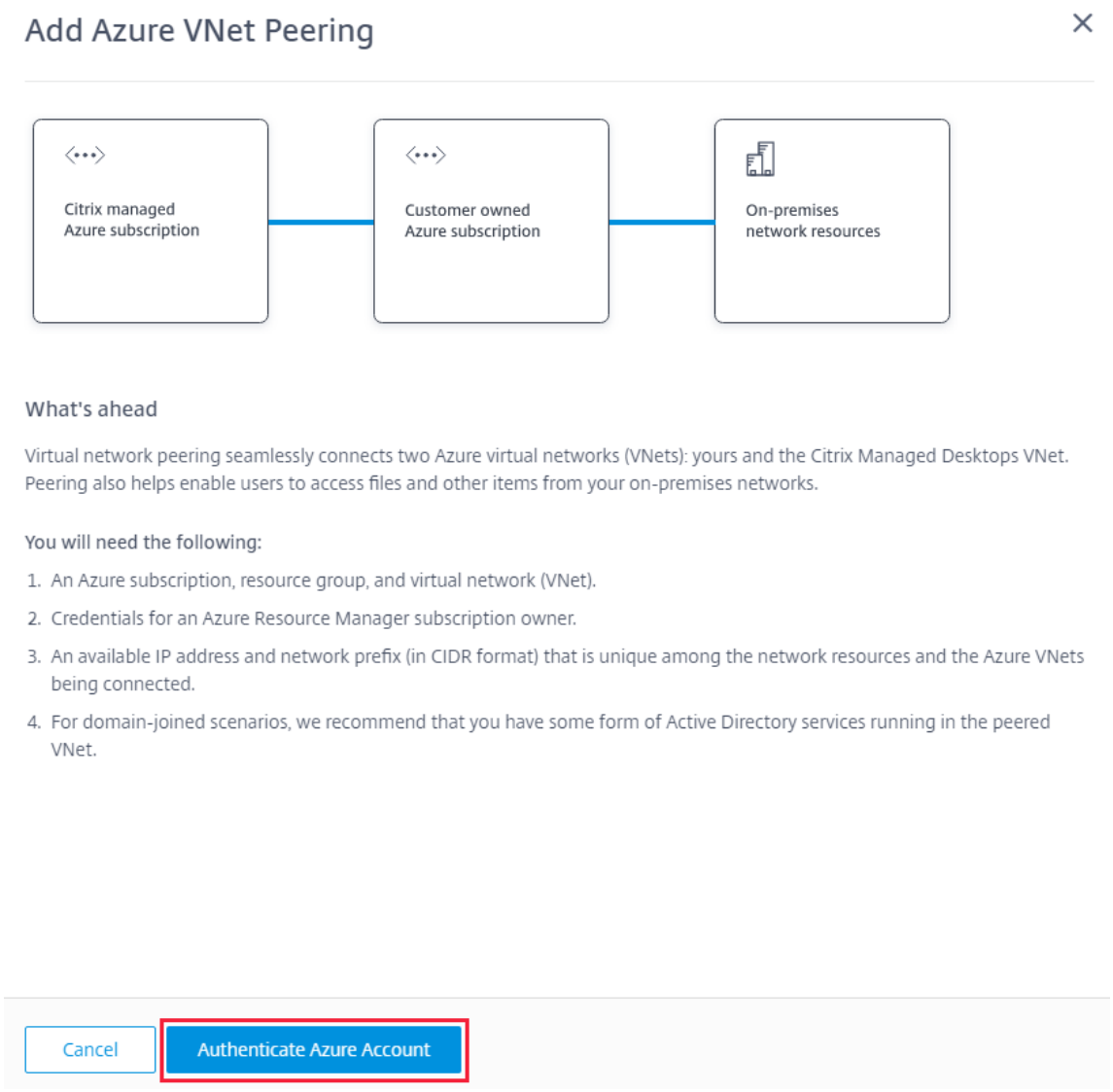
1. ［管理］**>**［クイック展開］を選択し、右側にある ［ネットワーク接続］を展開します。既に接続を設定している場合は、それらの接続が一覧表示されます。



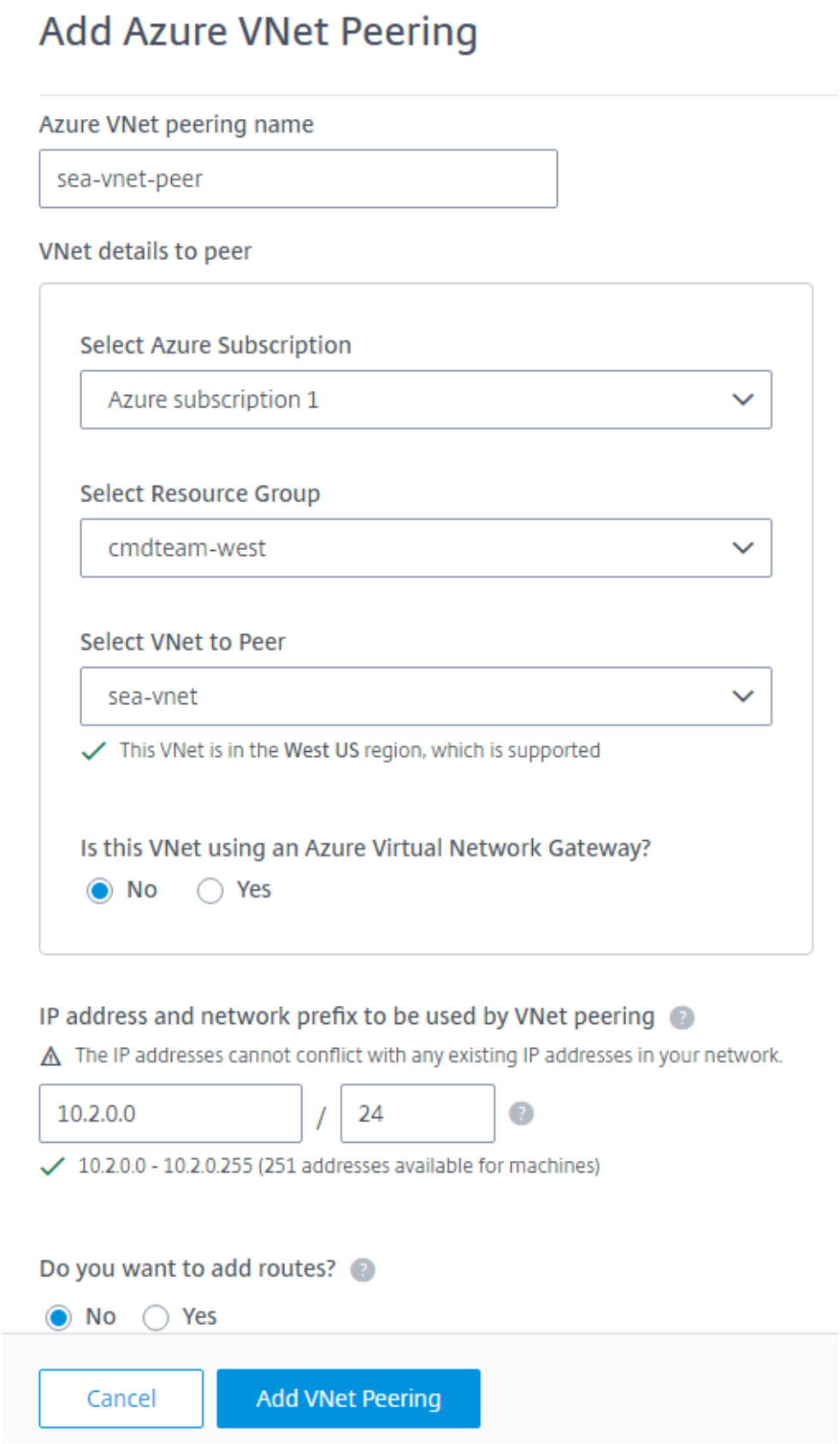
2. ［接続の追加］を選択します。
3. ［**Azure VNet** ピアリングの追加］ボックスの任意の場所をクリックします。



4. ［**Azure** アカウントを認証する］を選択します。



5. Citrix DaaS では、Azure サブスクリプションを認証するために Azure サインインページに自動的に移動します。グローバル管理者アカウントの資格情報を使用して Azure にサインインし、条件に同意すると、接続作成の詳細ダイアログボックスに戻ります。



6. Azure VNet ピアの名前を入力します。
7. ピアリングする Azure サブスクリプション、リソースグループ、および VNet を選択します。
8. 選択した VNet が Azure 仮想ネットワークゲートウェイを使用するかどうかを指定します。詳しくは、Microsoft 社の記事「Azure VPN ゲートウェイ」を参照してください。
9. 前の手順で ［はい］と答えた場合（VNet が Azure 仮想ネットワークゲートウェイを使用する場合）は、仮想ネットワークゲートウェイのルート伝達を有効にするかどうかを指定します。有効にすると、Azure はゲートウェイを通過するすべてのルートを自動的に学習（追加）します。

   この設定は、後で接続の ［詳細］ページで変更できます。ただし、これを変更すると、ルートパターンが変更され、VDA トラフィックが中断されることがあります。また、後で無効にする場合は、VDA が使用するネットワークに手動でルートを追加する必要があります。
10. IP アドレスを入力し、ネットマスクを選択します。使用するアドレス範囲と、その範囲がサポートするアドレスの数が表示されます。IP 範囲が Azure およびオンプレミスネットワークで使用するアドレスと重複していないことを確認します。

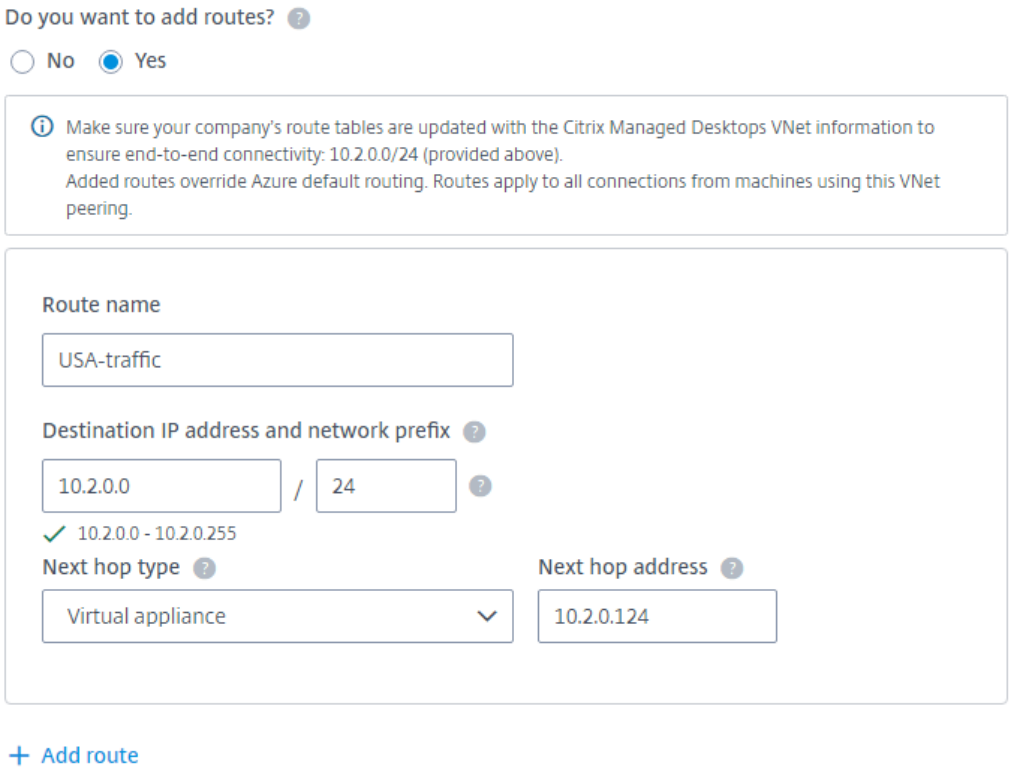
    - たとえば、Azure VNet のアドレス空間が 10.0.0.0 /16 の場合、Citrix DaaS で 192.168.0.0 /24 などの VNet ピアリング接続を作成します。
    - この例では、10.0.0.0 /24 の IP 範囲で VNet ピアリング接続を作成すると、アドレス範囲に重複すると見なされます。

    アドレスが重複している場合、VNet ピアリング接続が正常に作成されない可能性があります。また、サイト管理タスクで接続が正しく機能しません。
11. VNet ピアリング接続にカスタムルートを追加するかどうかを指定します。［はい］を選択した場合は、次の情報を入力します：

    a) カスタムルートのフレンドリ名を入力します。

    b) ターゲット IP アドレスとネットワークプレフィックスを入力します。ネットワークプレフィックスは 16～24 である必要があります。

    c) トラフィックをルーティングする場所の次ホップの種類を選択します。［仮想アプライアンス］を選択した場合は、アプライアンスの内部 IP アドレスを入力します。



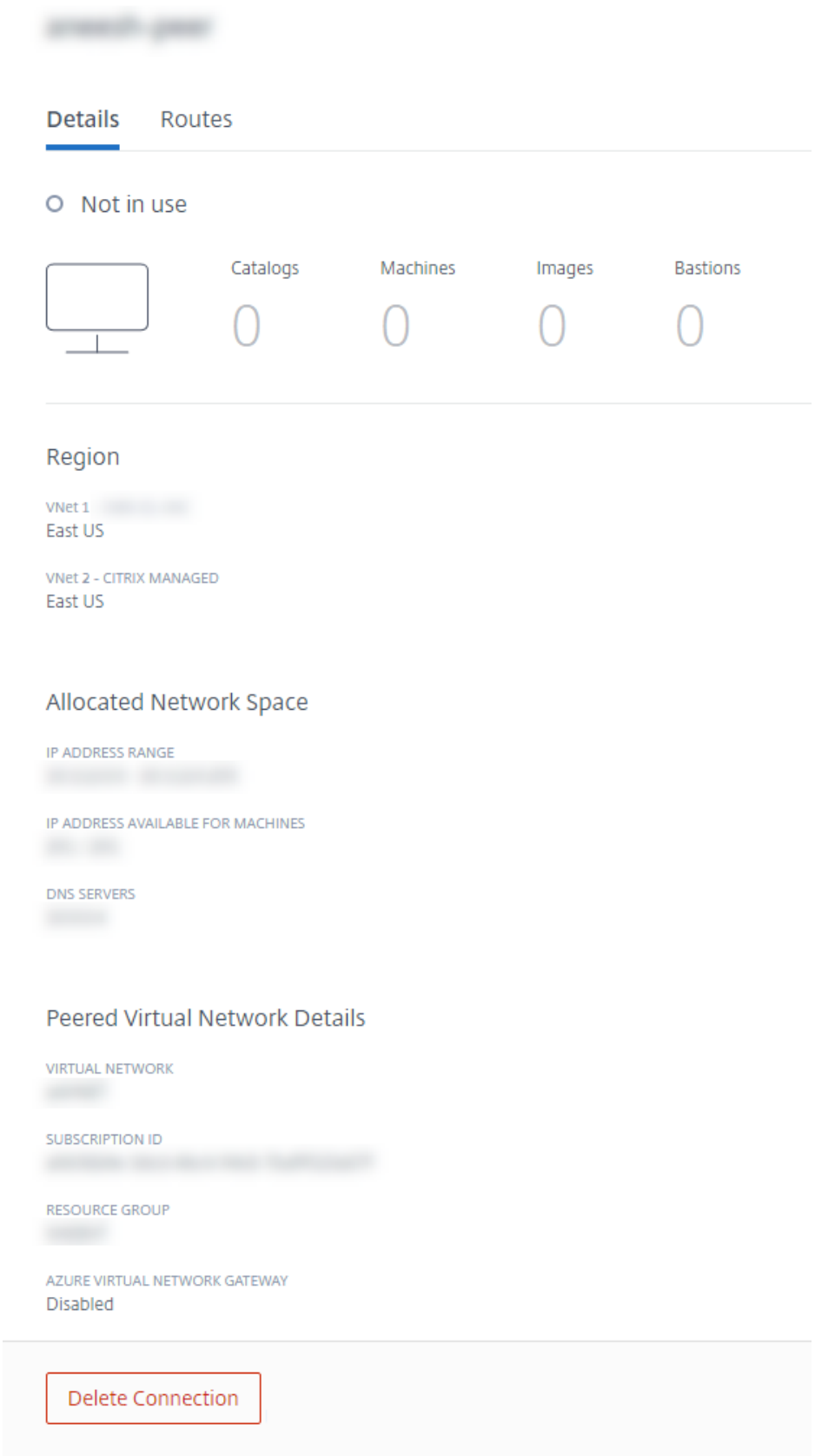
次ホップの種類について詳しくは、Microsoft 社の記事「仮想ネットワークトラフィックのルーティング」の「カスタムルート」セクションを参照してください。

d) 接続用に別のカスタムルートを作成するには、［ルートの追加］を選択します。

12. ［**VNet** ピアリングの追加］を選択します。

接続が作成されると、［管理］**>**［クイック展開］ダッシュボードの右側にある ［ネットワーク接続］**>**［**Azure VNet** ピア］に表示されます。カタログを作成すると、この接続は使用可能なネットワーク接続の一覧に表示されます。

Azure VNet ピアリング接続の詳細の表示



1. ［管理］**>**［クイック展開］を選択し、右側にある ［ネットワーク接続］を展開します。
2. 表示する Azure VNet ピアリング接続を選択します。

詳細には以下が表示されます：

- この接続を使用するカタログ、マシン、イメージ、および踏み台マシンの数。
- リージョン、割り当てネットワーク領域、およびピアリングされた VNet。
- VNet ピアリング接続用に現在構成されているルート。

既存の **Azure VNet** ピア接続のカスタムルートの管理

新しいカスタムルートを既存の接続に追加したり、カスタムルートの無効化や削除など、既存のカスタムルートを変更したりできます。

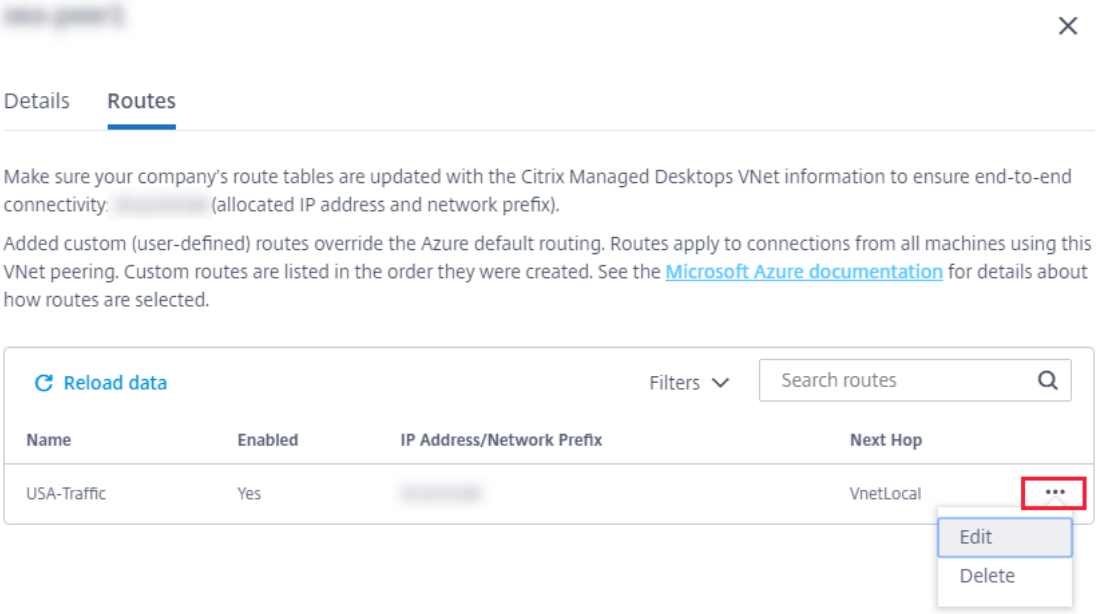
> 重要：
>
> カスタムルートを変更、無効化、または削除すると、接続のトラフィックフローが変更され、アクティブである可能性があるユーザーセッションが中断されることがあります。

カスタムルートを追加するには：

1. ［管理］**>**［クイック展開］を選択し、右側にある ［ネットワーク接続］を展開します。
2. 削除する接続を選択します。
3. 接続の詳細で、［ルート］を選択してから ［ルートの追加］を選択します。
4. フレンドリ名、ターゲット IP アドレスとプレフィックス、および使用する次ホップの種類を入力します。次ホップの種類として ［仮想アプライアンス］を選択した場合は、アプライアンスの内部 IP アドレスを入力します。
5. カスタムルートを有効にするかどうかを指定します。デフォルトでは、カスタムルートは有効になっています。
6. ［ルートの追加］を選択します。

カスタムルートを変更または無効にするには：

1. ［管理］**>**［クイック展開］を選択し、右側にある ［ネットワーク接続］を展開します。
2. 削除する接続を選択します。
3. 接続の詳細で ［ルート］を選択し、管理するカスタムルートを見つけます。
4. 省略記号（…）メニューの ［編集］を選択します。



5. 必要に応じて、ターゲット IP アドレスとプレフィックス、または次ホップの種類に必要な変更を加えます。
6. カスタムルートを有効または無効にするには、［このルートを有効にしますか?］で ［はい］または ［いいえ］を選択します。
7. ［**Save**］を選択します。

カスタムルートを削除するには:

1. ［管理］**>**［クイック展開］を選択し、右側にある ［ネットワーク接続］を展開します。
2. 削除する接続を選択します。
3. 接続の詳細で ［ルート］を選択し、管理するカスタムルートを見つけます。
4. 省略記号（…）メニューの ［削除］を選択します。
5. ［ルートを削除すると、アクティブなセッションが中断される可能性があります］を選択すると、カスタムルートを削除したときの影響を確認できます。
6. ［ルートの削除］を選択します。

Azure VNet ピアリング接続の削除

Azure VNet ピアリング接続を削除する前に、それに関連付けられているカタログをすべて削除します。「カタログの削除」を参照してください。

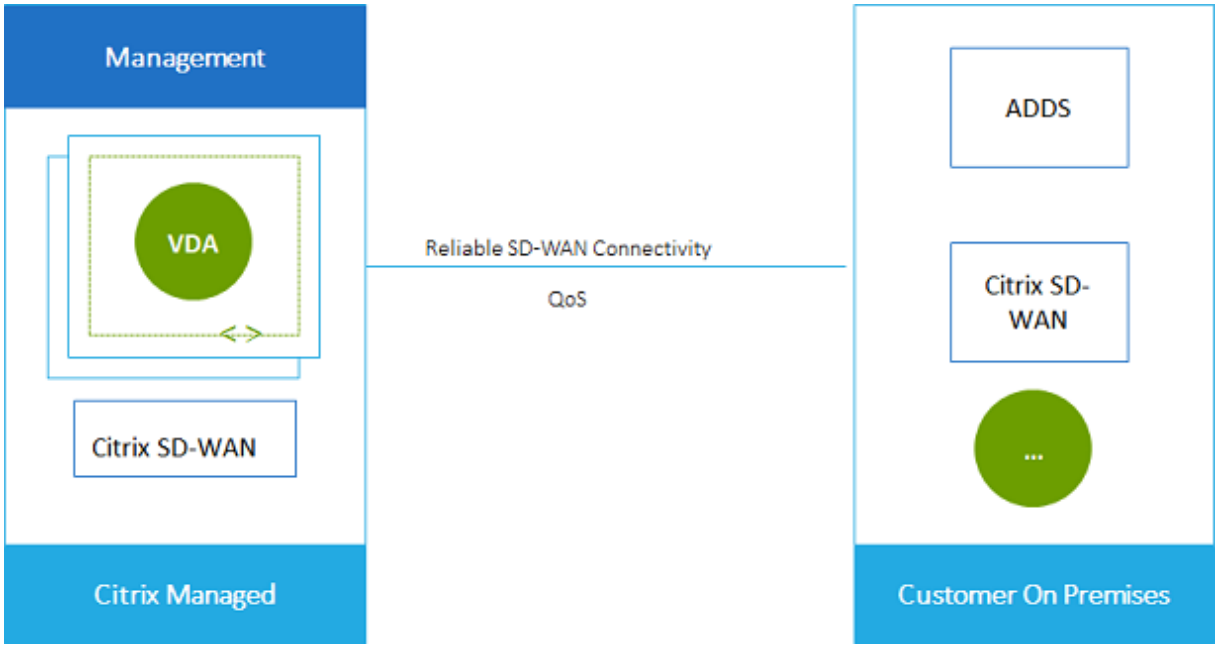
1. ［管理］**>**［クイック展開］を選択し、右側にある ［ネットワーク接続］を展開します。
2. 削除する接続を選択します。
3. 接続の詳細から、［接続の削除］を選択します。

SD-WAN 接続について

Citrix SD-WAN は、Citrix DaaS に必要なすべてのネットワーク接続を最適化します。Citrix SD-WAN は、HDX テクノロジと連携して、ICA と、アウトオブバンドの Citrix DaaS トラフィックに、QoS（サービス品質）と接続の信頼性を提供します。Citrix SD-WAN は、次のネットワーク接続をサポートしています：

- ユーザーとその仮想デスクトップ間のマルチストリーム ICA 接続
- 仮想デスクトップから、Web サイト、SaaS アプリ、およびその他のクラウドプロパティへのインターネットアクセス
- 仮想デスクトップから、Active Directory、ファイルサーバー、およびデータベースサーバーなどのオンプレミスリソースに戻るアクセス
- Workspace アプリのメディアエンジンから、Microsoft Teams などのクラウドでホストされている総合コミュニケーションサービスへの、RTP で伝送されるリアルタイム/インタラクティブトラフィック
- YouTube や Vimeo などのサイトからのクライアント側の動画取得

次の図に示すように、Citrix Managed Azure サブスクリプションからサイトへの SD-WAN 接続を作成します。接続の作成中に、SD-WAN VPX アプライアンスが Citrix Managed Azure サブスクリプションに作成されます。SD-WAN の観点からは、この場所はブランチとして扱われます。



SD-WAN 接続の要件と準備

- 以下の要件が満たされていない場合、SD-WAN ネットワーク接続オプションは使用できません。
  - Citrix Cloud サービスの使用権：Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）と SD-WAN Orchestrator。

  - インストールおよび構成された SD-WAN 展開。展開には、クラウド内かオンプレミスかに関係なく、マスターコントロールノード（MCN）が含まれ、SD-WAN Orchestrator で管理される必要があります。

- VNet IP 範囲：接続中のネットワークリソースの間で一意の使用可能な CIDR アドレス空間（IP アドレスとネットワークプレフィックス）を入力します。これは、Citrix DaaS の VNet 内の VM に割り当てられた IP 範囲です。

  クラウドおよびオンプレミスネットワークで使用するアドレスと重複しない IP 範囲を指定していることを確認してください。

  - たとえば、ネットワークのアドレス空間が 10.0.0.0 /16 の場合、Citrix DaaS で 192.168.0.0 /24 などの接続を作成します。
  - この例では、10.0.0.0 /24 の IP 範囲で接続を作成すると、アドレス範囲に重複すると見なされます。

  アドレスが重複している場合、接続が正常に作成されない可能性があります。また、サイト管理タスクで接続が正しく機能しません。

- 接続構成プロセスには、ユーザー（Citrix DaaS 管理者）と SD-WAN Orchestrator 管理者が完了する必要のあるタスクが含まれています。また、タスクを完了するには、SD-WAN Orchestrator 管理者から提供される情報が必要です。

  実際に接続を作成する前に、このドキュメントのガイダンスと SD-WAN ドキュメントの両方を確認することをお勧めします。

SD-WAN 接続の作成

> 重要：
>
> SD-WAN 構成について詳しくは、「Citrix DaaS 統合の SD-WAN 構成」を参照してください。

1. ［管理］**>**［クイック展開］を選択し、右側にある ［ネットワーク接続］を展開します。
2. ［接続の追加］を選択します。
3. ［ネットワーク接続の追加］ページで、［SD-WAN］ボックスの任意の場所をクリックします。
4. 次のページには、この後にやることがまとめられています。読み終えたら、［**SD-WAN** の構成を開始する］を選択します。
5. ［**SD-WAN** の構成］ページで、SD-WAN Orchestrator 管理者から提供された情報を入力します。

   - 展開モード：［高可用性］を選択すると、2 つの VPX アプライアンスが作成されます（実稼働環境用に推奨）。［スタンドアロン］を選択すると、1 つのアプライアンスが作成されます。この設定を後で変更することはできません。展開モードに変更するには、ブランチおよび関連するすべてのカタログを削除して再作成する必要があります。
   - 名前： SD-WAN サイトの名前を入力します。
   - スループットとオフィス数：この情報は、SD-WAN Orchestrator 管理者から提供されます。

- リージョン： VPX アプライアンスが作成されるリージョン。
- **VDA** サブネットと **SD-WAN** サブネット：この情報は、SD-WAN Orchestrator 管理者から提供されます。競合の回避については、「SD-WAN 接続の要件と準備」を参照してください。

6. 完了したら、［ブランチの作成］を選択します。
7. 次のページには、［管理］**>**［クイック展開］ダッシュボードで何を探すかがまとめられています。読み終えたら、［了解］を選択します。
8. ［管理］**>**［クイック展開］の ［ネットワーク接続］にある新しい SD-WAN エントリは、構成プロセスの進行状況を示します。「`Awaiting activation by SD-WAN administrator`」というメッセージが表示されてエントリがオレンジ色に変わったら、SD-WAN Orchestrator 管理者に知らせてください。
9. SD-WAN Orchestrator 管理者のタスクについては、SD-WAN Orchestrator の製品ドキュメントを参照してください。
10. SD-WAN Orchestrator 管理者が作業を完了すると、［ネットワーク接続］にある SD-WAN エントリが緑色に変わり、「`You can create catalogs using this connection`」というメッセージが表示されます。

SD-WAN 接続の詳細の表示

1. ［管理］**>**［クイック展開］を選択し、右側にある ［ネットワーク接続］を展開します。
2. SD-WAN が唯一の選択肢ではない場合は、［**SD-WAN**］を選択します。
3. 表示する接続を選択します。

画面には次のものが表示されます：

- ［詳細］タブ：接続の構成時に指定した情報。
- ［ブランチ接続］タブ：各ブランチと MCN の名前、クラウド接続、可用性、帯域幅階層、役割、および場所。

SD-WAN 接続の削除

SD-WAN 接続を削除する前に、それに関連付けられているカタログをすべて削除します。「カタログの削除」を参照してください。

1. ［管理］**>**［クイック展開］を選択し、右側にある ［ネットワーク接続］を展開します。
2. SD-WAN が唯一の選択肢ではない場合は、［SD-WAN］を選択します。
3. 削除する接続を選択し、詳細を表示します。
4. ［詳細］タブで、［接続の削除］を選択します。
5. 削除を確認します。

クイック展開でのユーザーと認証

May 17, 2024

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

ユーザー認証方法

ユーザーは、デスクトップまたはアプリを起動するために Citrix Workspace にログインするとき、認証する必要があります。

［クイック展開］は、次のユーザー認証方法をサポートしています:

- 管理対象 **Azure AD**: 管理対象 Azure AD は、Citrix が提供および管理する Azure Active Directory（AAD）です。お客様自身の Active Directory 構造を提供する必要はありません。ユーザーをディレクトリに追加するだけです。
- **ID** プロバイダー: Citrix Cloud で使用可能な任意の認証方法を使用できます。

> 注:
>
> - リモート PC アクセスの展開では、Active Directory のみを使用します。詳しくは、「リモート PC アクセス」を参照してください。
> - Azure AD Domain Services を使用する場合: ワークスペースのログオン UPN（User Principal Name: ユーザープリンシパル名）には、Azure AD Domain Services の有効化時に指定したドメイン名を含める必要があります。作成したカスタムドメインをプライマリとして指定している場合でも、ログオンにカスタムドメインの UPN を使用することはできません。

ユーザー認証の設定には、次の手順があります:

1. Citrix Cloud および Workspace の構成で、ユーザー認証方法を構成します。
2. ユーザー認証に管理対象 Azure AD を使用している場合は、ディレクトリにユーザーを追加します。
3. カタログにユーザーを追加します。

Citrix Cloud でのユーザー認証の構成

Citrix Cloud でユーザー認証を構成するには:

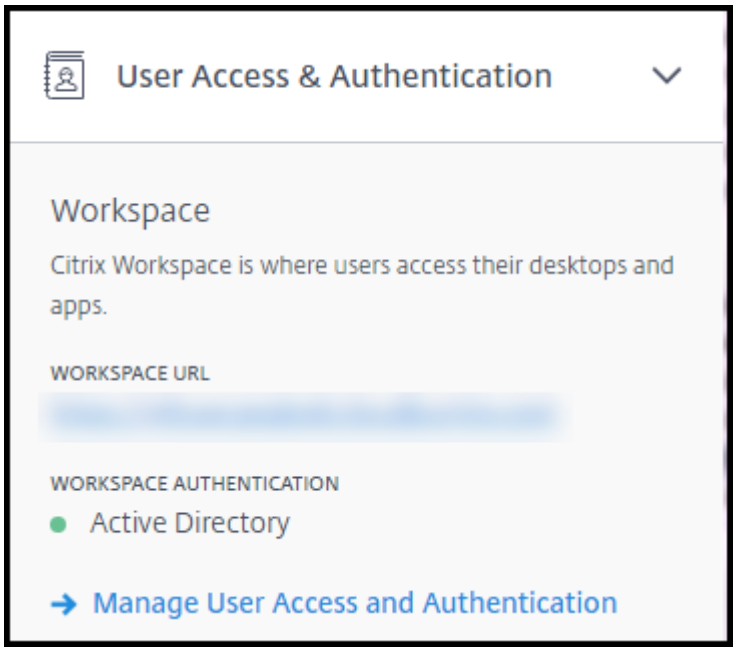
- 使用するユーザー認証方法に接続します（Citrix Cloud では、認証方法から「接続」または「切断」します）。

- Citrix Cloud で、この接続方法を使用するように Workspace 認証を設定します。

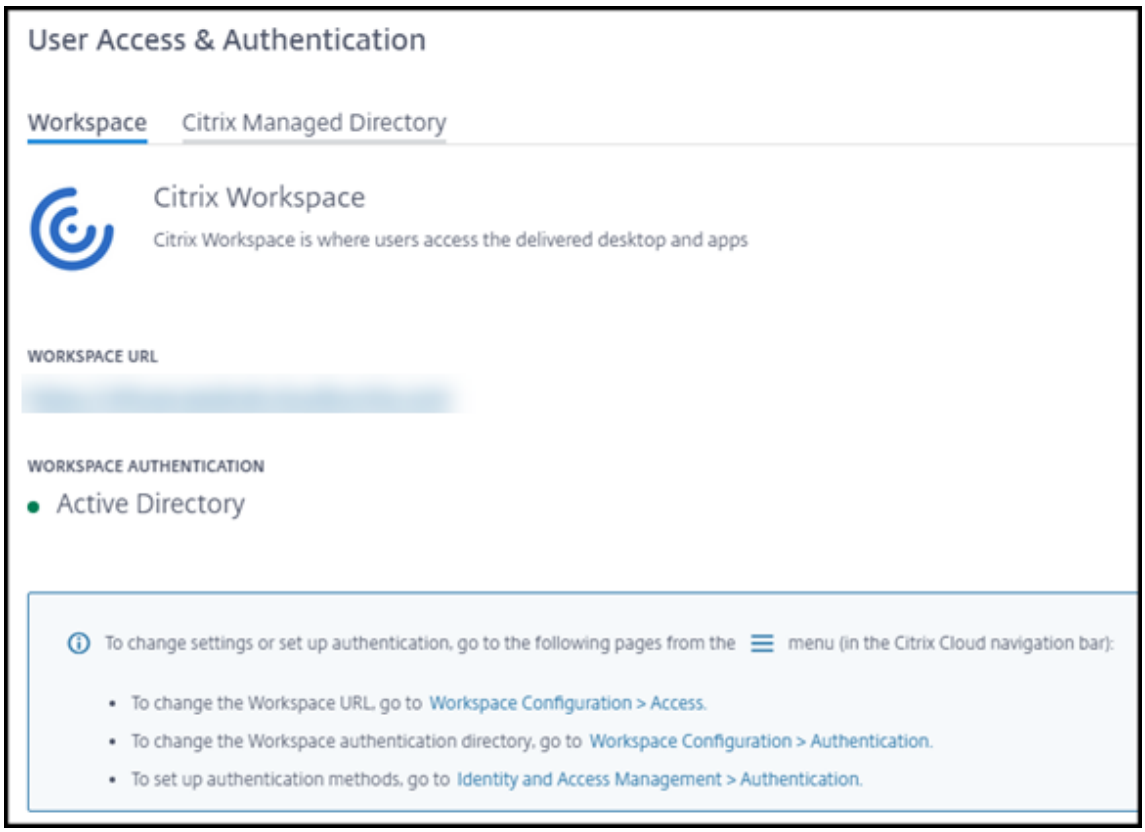
> 注:
>
> デフォルトでは、管理対象 Azure AD 認証方法が構成されています。つまり、Citrix Cloud に自動的に接続され、Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）に管理対象 Azure AD を使用するように Workspace 認証が自動的に設定されます。この方法を使用する場合（および以前に別の方法を構成したことがない場合）は、「管理対象 Azure AD でのユーザーの追加と削除」に進みます。
> 管理対象 Azure AD が切断されると、Workspace の認証は Active Directory に切り替わります。別の認証方法を使用する場合は、以下の手順に従ってください。

認証方法を変更するには:

1. ［管理］**>**［クイック展開］を選択してから、右側にある ［ユーザーアクセスおよび認証］を選択します。



2. ［ユーザーアクセスおよび認証の管理］を選択します。まだ選択されていない場合は、［**Workspace**］タブを選択します（もう 1 つのタブは、現在構成されているユーザー認証方法を示します）。



3. ［認証方法を設定するには］リンクをクリックすると、Citrix Cloud に移動します。選択する方法の省略記号メニューで ［接続］を選択します。
4. 引き続き Citrix Cloud で、左上隅のメニューの ［ワークスペースの構成］を選択します。［認証］タブで、必要な方法を選択します。

次にやること:

- 管理対象 Azure AD を使用している場合は、ディレクトリにユーザーを追加します。
- すべての認証方法で、カタログにユーザーを追加します。

管理対象 **Azure AD** でのユーザーの追加と削除

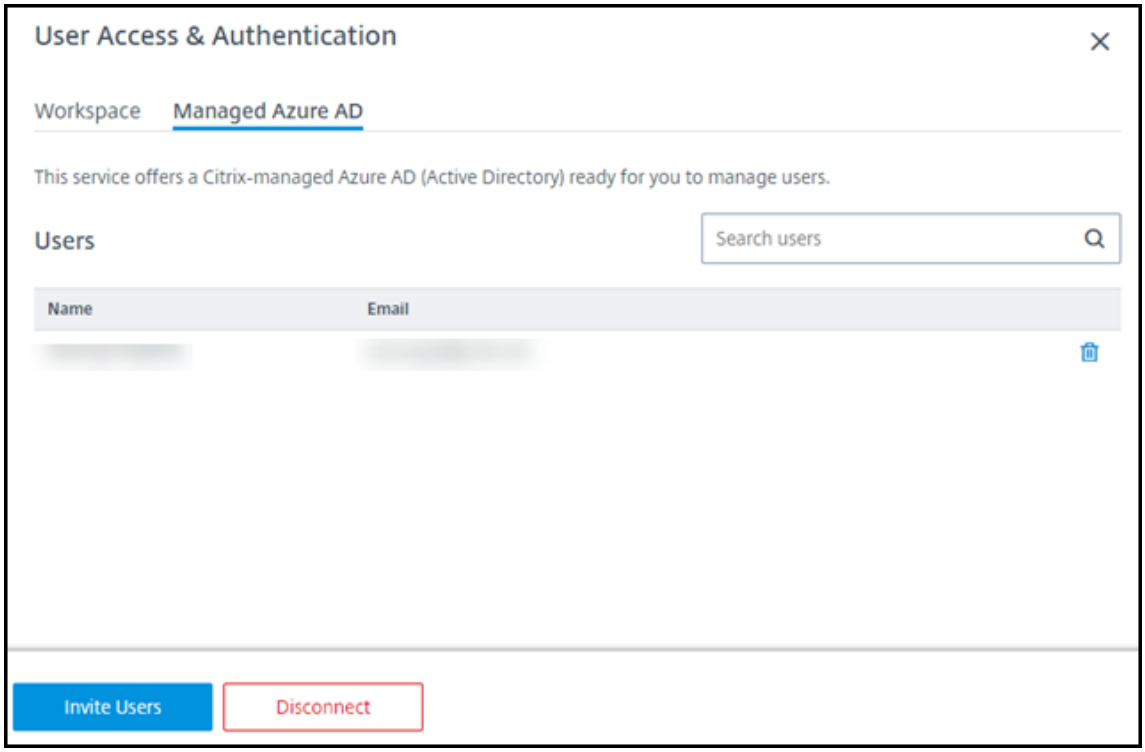
Citrix Workspace へのユーザー認証に管理対象 Azure AD を使用している場合にのみ、以下の手順に従ってください。

ユーザーの名前とメールアドレスを入力します。次に、Citrix が各ユーザーに招待状をメール送信します。メールでは、ユーザーに Citrix 管理対象 Azure AD に参加するリンクを選択するように指示があります。

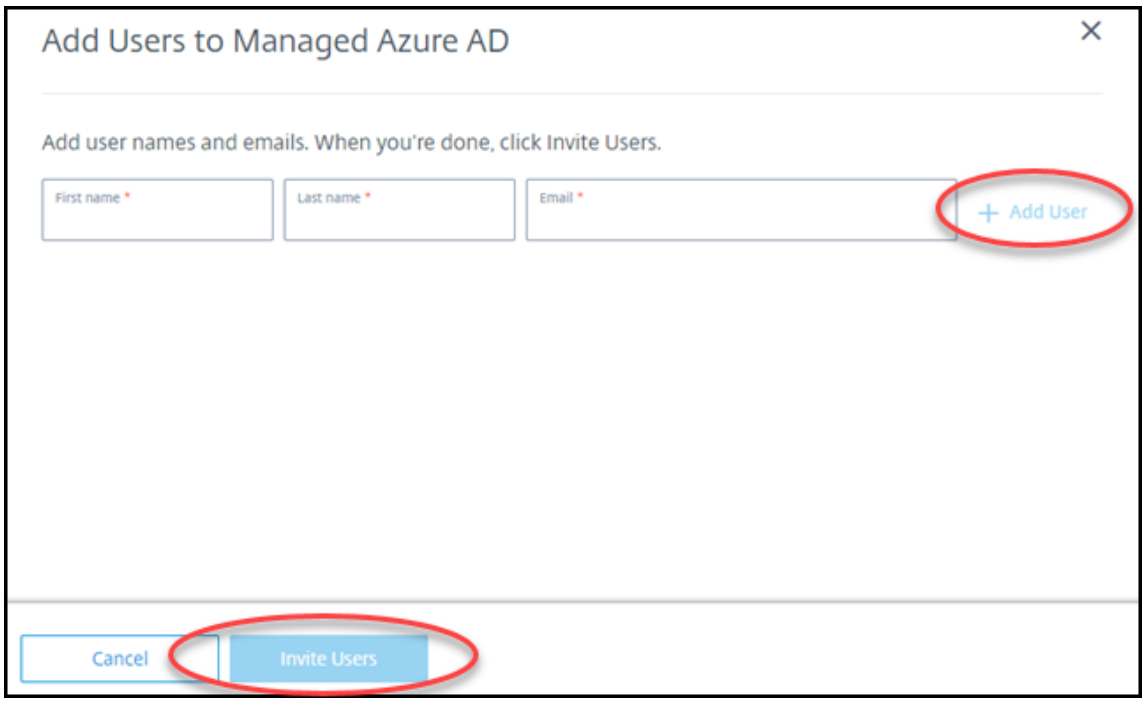
- ユーザー指定のメールアドレスを使用した Microsoft アカウントを既に持っている場合は、そのアカウントが使用されます。
- ユーザーがメールアドレスを使用した Microsoft アカウントを持っていない場合、Microsoft 社がアカウントを作成します。

ユーザーを管理対象 Azure AD に追加して招待するには:

1. ［管理］**>**［クイック展開］を選択してから、右側にある ［ユーザーアクセスおよび認証］を開きます。［ユーザーアクセスおよび認証の管理］を選択します。
2. ［管理対象 **Azure AD**］タブを選択します。
3. ［ユーザーの招待］を選択します。



4. ユーザーの名前とメールアドレスを入力し、［ユーザーの追加］を選択します。



5. 前の手順を繰り返して、他のユーザーを追加します。
6. ユーザー情報の追加が完了したら、カードの下部にある ［ユーザーの招待］を選択します。

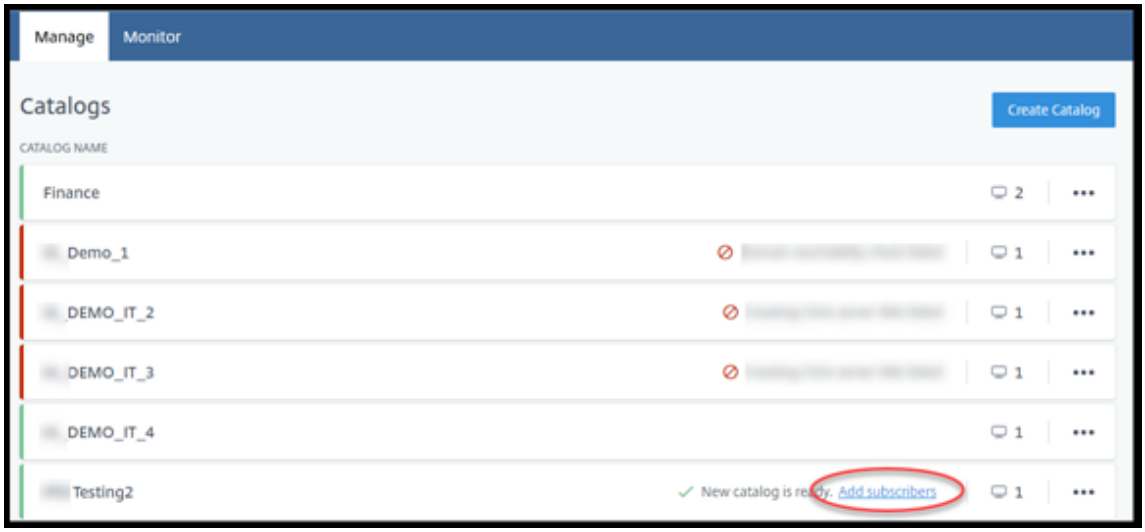
管理対象 Azure AD からユーザーを削除するには、ディレクトリから削除するユーザーの名前の横にあるゴミ箱アイコンを選択します。削除を確認します。

次にやること：カタログにユーザーを追加する

カタログでユーザーを追加または削除する

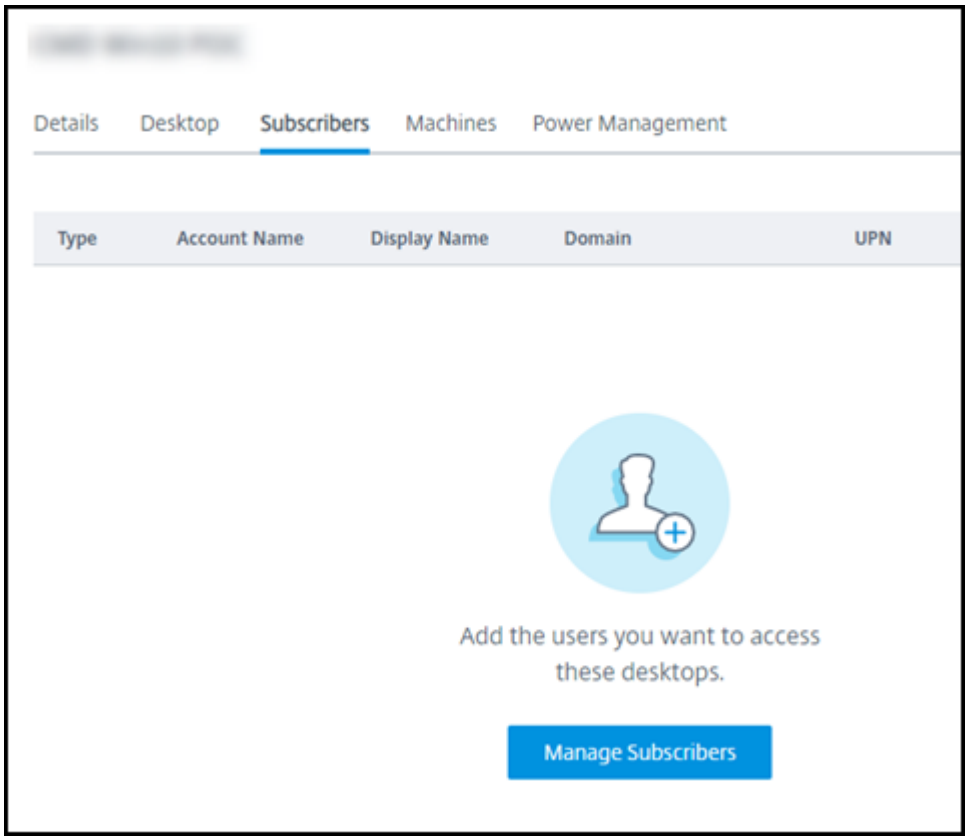
使用する認証方法に関係なく、以下の手順に従ってください。

1. ［管理］**>**［クイック展開］で、カタログにユーザーを追加していない場合は、［利用者の追加］を選択します。

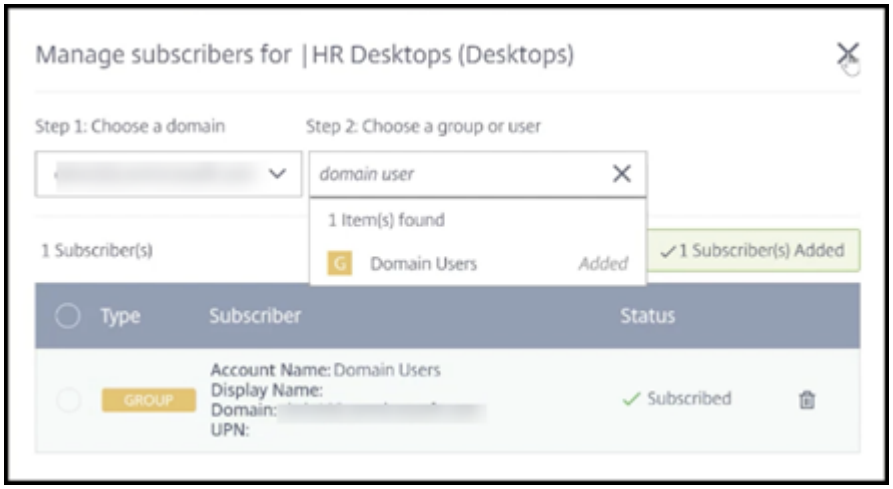


既にユーザーがいるカタログにユーザーを追加するには、カタログのエントリの任意の場所をクリックします。

2. ［利用者］タブで、［利用者の管理］を選択します。



3. ドメインを選択します（ユーザー認証に管理対象 Azure AD を使用している場合、ドメインフィールドにはエントリが 1 つだけあります）。次に、ユーザーを選択します。



4. 必要に応じて、他のユーザーを選択します。完了したら、右上隅の［**X**］を選択します。

カタログからユーザーを削除するには、手順 1 と 2 に従います。手順 3 で、（ドメインとグループ/ユーザーを選択する代わりに）削除するユーザーの名前の横にあるゴミ箱アイコンを選択します。この操作により、ユーザーはソース（管理対象 Azure AD やお客様自身の AD または AAD など）からではなく、カタログから削除されます。

次にやること：

- マルチセッションマシンを含むカタログの場合、まだ追加していない場合はアプリケーションを追加します。
- すべてのカタログで、Citrix Workspace URL をユーザーに送信します。

追加情報

Citrix Cloud での認証について詳しくは、「ID およびアクセス管理」を参照してください。

クイック展開でのリモート **PC** アクセス

February 24, 2023

はじめに

Citrix リモート PC アクセスにより、ユーザーはオフィスにある物理的な Windows または Linux マシンをリモートで使用できます。ユーザーは、Citrix HDX を使用して社内 PC セッションを提供することで、最高のユーザーエクスペリエンスを実現できます。

リモート PC アクセスは、ドメイン参加済みマシンをサポートします。

この記事では、［クイック展開］インターフェイスを使用して、リモート PC アクセス展開を作成する方法について説明します。［完全な構成］インターフェイスを使用してリモート PC アクセス展開を作成する方法については、「リモート PC アクセス」を参照してください。

仮想デスクトップおよびアプリの提供との違い

仮想デスクトップおよびアプリの提供に慣れている方は、リモート PC アクセス機能には以下のような違いがあります:

- リモート PC アクセスカタログには通常、既存の物理マシンが含まれています。そのため、リモート PC アクセスを使用するために、イメージを準備したり、マシンをプロビジョニングしたりする必要はありません。デスクトップおよびアプリの提供では通常、仮想マシン（VM）が使用され、VM をプロビジョニングするためのテンプレートとしてイメージが使用されます。
- リモート PC アクセスで、ランダムにプールされたカタログ内のマシンが電源オフになっても、イメージの元の状態にリセットされることはありません。
- リモート PC アクセスの静的ユーザー割り当てカタログの場合、割り当ては、ユーザーが（マシンまたは RDP で）ログインした後に行われます。デスクトップとアプリを提供するときにマシンが使用可能であれば、ユーザーが割り当てられます。

インストールと構成の概要

タスクを開始する前に、このセクションを確認してください。

1. 以下の点に注意してください:
   a) 要件と考慮事項を確認してください。
   b) 準備作業を完了してください。
2. Citrix Cloud で:
   a) Citrix Cloud アカウントを設定し、Citrix DaaS にサブスクライブします。
   b) Active Directory リソースにアクセスできるリソースの場所を設定します。リソースの場所に少なくとも 2 つの Cloud Connector をインストールします。Cloud Connector は Citrix Cloud と通信します。

      「リソースの場所の作成とその場所への Cloud Connector のインストール」のガイダンスに従います。このガイダンスには、システム要件、準備、および手順が記載されています。
   c) Active Directory を Citrix Cloud に接続します。
3. ユーザーがリモートでアクセスする各マシンに、Citrix Virtual Delivery Agent（VDA）をインストールします。VDA は、リソースの場所にある Cloud Connector を介して Citrix Cloud と通信します。
4. ［管理］**>**［クイック展開］で:

a) リモート PC アクセスカタログを作成します。この手順では、リソースの場所の場所を指定し、ユーザーの割り当て方法を選択します。
b) 必要があれば、利用者（ユーザー）をカタログに追加します。ユーザー割り当て方法のうち、静的自動割り当てまたはランダムプールのいずれかの方法をカタログで使用している場合は、カタログにユーザーを追加します。静的事前割り当てのカタログにユーザーを追加する必要はありません。

5. ワークスペース URL をユーザーに送信します。ユーザーは自分のワークスペースから、オフィスの自分のマシンにログオンできます。

要件および考慮事項

このセクションで言及しているマシンとは、ユーザーがリモートでアクセスするマシンのことです。

一般

- マシンは、シングルセッションの Windows 10 または Linux（Red Hat Enterprise Linux および Ubuntu）オペレーティングシステムを実行している必要があります。
- マシンは Active Directory Domain Services ドメインに参加している必要があります。
- Citrix Virtual Apps and Desktops でリモート PC アクセスを使用することに慣れている方は、Citrix DaaS では Wake-on-LAN 機能が使用できないことに注意してください。

ネットワーク

- マシンにはアクティブなネットワーク接続が必要です。信頼性と帯域幅を高めるには、有線接続をお勧めします。
- Wi-Fi を使用している場合：
  - 電源設定でワイヤレスアダプターの電源を入れたままにするようにします。
  - ユーザーがサインインする前にワイヤレスネットワークに自動的に接続できるように、ワイヤレスアダプターとネットワークプロファイルを構成します。そうしないと、ユーザーがログオンするまで VDA は登録されません。ユーザーがログオンするまでは、マシンをリモートアクセスに使用できません。
  - Wi-Fi ネットワークから Cloud Connector にアクセスできることを確認してください。

デバイスと周辺機器

- 以下のデバイスはサポートされていません：
  - KVM スイッチ、またはセッションを切断する可能性のあるそのほかのコンポーネント。
  - ハイブリッド PC（オールインワンおよび NVIDIA Optimus ノートブックおよび PC を含む）。

- キーボードとマウスをマシンに直接接続します。電源を切ったり接続を切断したりできるモニターなどのコンポーネントに接続すると、これらの周辺機器が使用できなくなることがあります。キーボードやマウスをモニターなどのデバイス経由で接続する必要がある場合は、それらのコンポーネントの電源をオフにしないでください。
- ノートブックと Surface Pro デバイスの場合：ノートブックがバッテリーで動作しているのではなく、電源に接続されていることを確認します。デスクトップマシンのオプションに合わせて、ノートブックの電源オプションを構成します。例：

  - 休止機能を無効にする。
  - スリープ機能を無効にする。
  - カバーを閉じた場合の動作を ［何もしない］ に設定する。
  - 電源ボタンを押したときの操作を ［シャットダウン］ に設定する。
  - ビデオカードおよび NIC の省電力設定を無効にする。

  ドッキングステーションを使用している場合、ノートブックをドッキング解除して再接続できます。ドッキング解除すると、VDA は Wi-Fi で Cloud Connector に再登録されます。ただし、ノートブックを再接続した場合、ワイヤレスアダプターを外さない限り、VDA は有線接続を使用するように切り替わりません。有線接続が確立されると、組み込まれた機能がワイヤレスアダプターを切断するデバイスもあります。それ以外のデバイスでは、ワイヤレスアダプターを切断するためのカスタムソリューションかサードパーティ製のユーティリティが必要です。前述の Wi-Fi に関する考慮事項を確認してください。

  デバイスのリモート PC アクセスでドッキングとドッキング解除を有効にするには：

  - ［スタート］ **>** ［設定］ **>** ［システム］ **>** ［電源とスリープ］ で、［スリープ］ を ［なし］ に設定します。
  - ［デバイスマネージャー］ **>** ［ネットワークアダプター］ **>** ［イーサネットアダプター］ で ［電源管理］ に移動し、［電力の節約のために、コンピューターでこのデバイスの電源をオフにできるようにする］ をオフにします。［このデバイスで、コンピューターのスタンバイ状態を解除できるようにする］ チェックボックスがオンになっていることを確認します。

Linux VDA

- Linux VDA は、非 3D モードの物理マシンでのみ使用します。NVIDIA のドライバーの制限により、HDX 3D モードが有効になっている場合、PC のローカル画面はブラックアウトせず、画面にはセッションのアクティビティが表示されます。この画面の表示は、セキュリティ上のリスクです。
- Linux マシンのカタログは、静的に事前に割り当てられたユーザー割り当て方法を使用する必要があります。Linux マシンを含むカタログでは、静的自動割り当てまたはランダムプールの割り当て方法を使用できません。

Workspace に関する考慮事項

- 同じ社内 PC にアクセスする複数のユーザーには、Citrix Workspace で同じアイコンが表示されます。ユーザーが Citrix Workspace にサインインすると、そのマシンは他のユーザーによって既に使用されている場合

は使用不可と表示されます。

準備

- マシンに VDA をインストールする方法を決定します。いくつかの方法が使用可能です:
  - 各マシンに VDA を手動でインストールします。
  - スクリプトを使用し、グループポリシーを使用して VDA のインストールをプッシュします。
  - Microsoft System Center Configuration Manager（SCCM）などの電子ソフトウェア配信（ESD: Electronic Software Distribution）ツールを使用して、VDA のインストールをプッシュします。詳しくは、「SCCM を使用した VDA のインストール」を参照してください。
- ユーザー割り当て方法について学習し、使用する方法を決定します。リモート PC アクセスカタログを作成するときに方法を指定します。
- マシン（実際にはマシンにインストールする VDA）を Citrix Cloud に登録する方法を決定します。VDA は、Citrix Cloud のセッションブローカーとの通信を確立するために登録する必要があります。

  VDA は、リソースの場所にある Cloud Connector を介して登録します。VDA をインストールするとき、または後で、Cloud Connector アドレスを指定できます。

  VDA の最初の（初期）登録には、ポリシーベースの GPO（グループポリシーオブジェクト）または LGPO を使用することをお勧めします。初期登録後は、デフォルトで有効になっている自動更新を使用することをお勧めします。VDA 登録についてはさらに詳しい説明があります。

VDA のインストール

ユーザーがリモートでアクセスする各物理マシンに、VDA をダウンロードしてインストールします。

VDA のダウンロード

- Windows VDA をダウンロードするには:
  1. Citrix Cloud アカウントの資格情報を使用して、Citrix DaaS ダウンロードページにアクセスします。
  2. 最新の VDA をダウンロードします。2 種類のインストールパッケージを使用できます。VDA タイトルの年と月の値は、場合によって異なります。
- リモート PC アクセス用の Linux VDA をダウンロードするには、Linux VDA ドキュメントのガイダンスに従ってください。

Windows VDA インストールパッケージの種類　Citrix ダウンロードサイトでは、リモート PC アクセスマシンに使用できる 2 種類の Windows VDA インストールパッケージを提供しています:

- シングルセッションコア VDA インストーラー(*release* は *yymm* です):`VDAWorkstationCoreSetup_release.exe`

  シングルセッションコア VDA インストーラーは、リモート PC アクセス用に特別に調整されています。ネットワークを介してすべてのマシンに（他の VDA インストーラーよりも）軽量で簡単に展開できます。Citrix Profile Management、Machine Identity Service、ユーザー個人設定レイヤーなど、こうした展開では通常必要とされないコンポーネントは含まれていません。

  ただし、Citrix Profile Management がインストールされていない場合、Citrix Analytics for Performance 画面と一部のモニターの詳細は使用できません。これらの制限について詳しくは、ブログ投稿記事の「Monitor and troubleshoot Remote PC Access machines」を参照してください。

  完全な分析と監視を表示する必要がある場合は、シングルセッションの完全版 VDA インストーラーを使用してください。

- シングルセッション完全版 VDA インストーラー(*release* は *yymm* です):`VDAWorkstationSetup_release.exe`

  シングルセッション完全版 VDA インストーラーは、シングルセッションコア VDA インストーラーよりも大きなパッケージですが、必要なコンポーネントのみをインストールするように調整できます。たとえば、Profile Management をサポートするコンポーネントをインストールできます。

リモート **PC** アクセス用 **Windows VDA** の対話式インストール

1. ダウンロードした VDA インストールファイルをダブルクリックします。
2. ［環境］ページで ［リモート **PC** アクセスを有効にする］を選択し、［次へ］をクリックします。
3. ［**Delivery Controller**］ページで、次のいずれかを選択します:

   - Cloud Connector のアドレスがわかっている場合は、［手動で指定する］を選択します。Cloud Connector の FQDN（完全修飾ドメイン名）を入力し、［追加］をクリックします。リソースの場所にある他の Cloud Connector についても、同じ作業を繰り返します。
   - Active Directory（AD）構造のどこに Cloud Connector をインストールしたかがわかっている場合は、［**Active Directory** から場所を選択する］を選択して、その場所に移動します。他の Cloud Connector についても、同じ作業を繰り返します。
   - Citrix グループポリシーで Cloud Connector アドレスを指定する場合は、［後で実行（上級）］を選択し、プロンプトが表示されたらその選択を確認します。

   完了したら、［次へ］をクリックします。

4. シングルセッション完全版 VDA インストーラーを使用している場合は、［追加コンポーネント］ページで、Profile Management など、インストールするコンポーネントを選択します（シングルセッションコア VDA インストーラーを使用している場合、このページは表示されません）。

5. ［機能］ページで、［次へ］をクリックします。
6. ［ファイアウォール］ページで、［自動］を選択します（まだ選択されていない場合）。［次へ］をクリックします。
7. ［概要］ページで ［インストール］をクリックします。
8. ［診断］ページで、［接続］をクリックします。チェックボックスがオンになっていることを確認します。求められたら、Citrix アカウント資格情報を入力します。資格情報が確認されたら、［次へ］をクリックします。
9. ［完了］ページで、［完了］をクリックします。

フルインストールについて詳しくは、「VDA のインストール」を参照してください。

コマンドラインを使用したリモート **PC** アクセス用 **Windows VDA** のインストール

- シングルセッションコア VDA インストーラーを使用している場合：VDAWorkstationCoreSetup.exeを実行し、/quiet、/enable_hdx_ports、および/enable_hdx_udp_portsオプションを含めます。Cloud Connector アドレスを指定するには、/controllersオプションを使用します。

  たとえば、次のコマンドはシングルセッションコア VDA をインストールします。Citrix Workspace アプリとその他の非コアサービスはインストールされません。2 つの Cloud Connector の FQDN が指定され、Windows ファイアウォールサービスのポートが自動的に開放されます。管理者が再起動を処理します。

  ```
  VDAWorkstationCoreSetup .exe /quiet /controllers "Connector-East
  .domain.com" “Connector-East2.domain.com” /enable_hdx_ports /
  noreboot
  ```

- シングルセッション完全版 VDA インストーラーを使用していて、Profile Management（またはその他のオプションのコンポーネント）を含める場合：VDAWorkstationSetup.exeを実行し、/remotepcおよび/includeadditionalオプションを含めます。/remotepcオプションを使用すると、ほとんどの追加コンポーネントがインストールされなくなります。/includeadditionalオプションは、インストールする追加コンポーネントを正確に指定します。

  たとえば、次のコマンドにより、Profile Management を除くすべてのオプションの追加コンポーネントがインストールされなくなります。

  ```
  VDAWorkstationSetup.exe /quiet /remotepc /includeadditional “
  Citrix User Profile Manager”,“Citrix User Profile Manager WMI
  Plugin” /controllers “connector.domain.com” “connector2.domain.
  com” /enable_hdx_ports /noresume /noreboot
  ```

詳しくは、「VDA のインストールで使用するコマンドラインオプション」を参照してください。

Linux VDA のインストール

Linux VDA を対話式でインストールする、またはコマンドラインを使用する方法については、Linux ドキュメントのガイダンスに従ってください。

リモート **PC** アクセスカタログの作成

カタログを正常に作成するには、少なくとも 2 つの Cloud Connector を含むリソースの場所が存在している必要があります。

> 重要:
>
> マシンは同時に 1 つのカタログにしか属することはできません。カタログに追加するマシンを指定するときには、この制限は適用されません。しかし、制限を無視すると、後で問題が発生する可能性があります。

1. Citrix Cloudにサインインします。
2. 左上のメニューで、［マイサービス］**>**［**DaaS**］を選択します。
3. カタログをまだ作成していない場合は、［ようこそ］ページで ［開始］をクリックします。
4. ［管理］**>**［クイック展開］を選択します。
5. ［カタログの作成］を選択します。
6. ［リモート **PC** アクセス］タブで、ユーザーをマシンに割り当てる方法を選択します。
7. カタログの名前を入力し、作成したリソースの場所を選択します。
8. マシンを追加します。
9. ［カタログの作成］をクリックします。
10. ［リモート **PC** アクセスカタログを作成中です］ページで、［完了］をクリックします。
11. 新しいカタログのエントリが ［管理］**>**［クイック展開］ダッシュボードに表示されます。

    カタログが正常に作成されたら、リンクの 1 つをクリックして、利用者（ユーザー）をカタログに追加 します。ユーザー割り当て方法のうち、静的自動割り当てまたはランダムプール未割り当てのいずれかの方法をカタログで使用している場合は、この手順を適用します。

カタログを作成して（必要があれば）ユーザーを追加してから、ユーザーにワークスペース URL を送信します。

ユーザー割り当て方法

カタログの作成時に選択するユーザー割り当て方法は、マシンへのユーザーの割り当て方法を指定します。

- 静的自動割り当て：ユーザー割り当ては、VDA がマシンにインストールされた後、ユーザーがマシンにログオンしたときに発生します（Citrix を使用しない場合、たとえば対面や RDP）。後で、他のユーザーが（Citrix を使用せずに）そのマシンにログオンすると、それらのユーザーも割り当てられます。同時に 1 人のユーザーのみがそのマシンを使用できます。これは、コンピューターを共有するオフィスワーカーまたはシフトワーカーの一般的な設定です。

  この方法は、Windows マシンでサポートされています。Linux マシンでは使用できません。

- 静的事前割り当て：ユーザーはマシンに事前割り当てされています（これは通常、マシンとユーザーのマッピング情報を含む CSV ファイルをアップロードすることによって構成されます）。VDA のインストール後、ユーザーがログオンして割り当てる必要はありません。また、カタログの作成後にユーザーをカタログに割り当てる必要もありません。これはオフィスワーカーに最適です。

  この方法は、Windows と Linux のマシンでサポートされています。

- ランダムプール未割り当て：ユーザーは使用可能なマシンにランダムに割り当てられます。同時に 1 人のユーザーのみがそのマシンを使用できます。これは学校のコンピューターラボに最適です。

  この方法は、Windows マシンでサポートされています。Linux マシンでは使用できません。

カタログにマシンを追加する方法

注意事項：各マシンには VDA がインストールされている必要があります。

カタログを作成または編集する場合、マシンをカタログに追加する方法は 3 つあります：

- マシンアカウントを 1 つずつ選択する。
- OU（組織単位）を選択する。
- CSV ファイルを使用して一括で追加する。この CSV ファイル用のテンプレートを使用できます。

マシン名の追加

この方法は、マシンアカウントを 1 つずつ追加します。

1. ドメインを選択します。
2. マシンアカウントを検索します。
3. ［追加］をクリックします。
4. マシンの追加を繰り返します。
5. マシンの追加が終了したら、［完了］をクリックします。

OU の追加

この方法は、マシンアカウントが存在する組織単位（OU）に従って、マシンアカウントを追加します。
OU を選択するときは、より細分化するために下位レベルの OU を選択します。そうした細分性が必要ない場合は、上位レベルの OU を選択できます。

たとえば、`Bank`/`Officers`/`Tellers`の場合、より細分性を高めるために［`Tellers`］を選択します。それ以外の場合は、要件に基づいて［`Officers`］または［`Bank`］を選択できます。

OU がリモート PC アクセスカタログに割り当てられた後に OU を移動または削除すると、VDA の関連付けに影響し、今後の割り当てで問題が発生します。AD（Active Directory）の変更を計画するときは、カタログに対する OU の割り当てを更新することも考慮に入れてください。

OU を追加するには:

1. ドメインを選択します。
2. 追加するマシンアカウントを含む OU を選択します。
3. 選択に含まれるサブフォルダーを含めるかどうかをチェックボックスで指定します。
4. OU の選択が終了したら、［完了］をクリックします。

一括で追加

1. ［**CSV** テンプレートのダウンロード］をクリックします。
2. テンプレートに、マシンアカウント情報（最大 100 エントリ）を追加します。CSV ファイルには、各マシンに割り当てられているユーザーの名前を含めることもできます。
3. ファイルを保存します。
4. ［マシンを一括で追加］ページにファイルをドラッグするか、ファイルを参照します。
5. ファイル内容のプレビューが表示されます。それが目的のファイルでない場合は、別のファイルを作成してから、そのファイルをドラッグまたは参照できます。
6. 完了したら、［完了］をクリックします。

リモート **PC** アクセスカタログの管理

リモート PC アクセスカタログの構成情報を表示または変更するには、［管理］**>**［クイック展開］ダッシュボードで（カタログのエントリの任意の場所をクリックして）カタログを選択します。

- ［詳細］タブで、マシンを追加または削除できます。
- ［利用者］タブで、ユーザーを追加または削除できます。
- ［マシン］タブで、次のことができます:
  - マシンの追加または削除:［マシンの追加または削除］ボタン。
  - ユーザー割り当ての変更:［割り当ての削除］ゴミ箱アイコン、省略記号メニューの ［マシン割り当てを編集］。
  - 登録されているマシンを確認し、マシンを保守モードにするか、保守モードを解除します。

クイック展開での監視

May 18, 2022

［監視］ダッシュボードでは、Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）展開のデスクトップの使用状況、セッション、およびマシンを表示できます。また、セッションの制御、マシンの電源管理、アプリケーション実行の終了、およびプロセス実行の終了も可能です。

［監視］ダッシュボードにアクセスするには：

1. まだCitrix Cloudにサインインしていない場合は、サインインします。左上のメニューで、［マイサービス］**>** ［**DaaS**］を選択します。
2. ［管理］**>** ［クイック展開］ダッシュボードで、［監視］タブを選択します。

デスクトップ使用状況の監視

このページの表示は 5 分ごとに更新されます。

- マシンとセッションの概要：すべてのカタログ（デフォルト）または選択したカタログに関する情報を表示するように表示を調整できます。期間を調整することもできます：最後の日、週、月、または 3 か月。

  画面上部のカウントは、マシンの総数に加えて、電源がオンまたはオフになっているマシンの数を示します。値にカーソルを合わせると、シングルセッションとマルチセッションの数が表示されます。

  カウントの下のグラフは、選択した期間中の定期ポイントでの、電源がオンになっていたマシンとピーク同時セッションの数を示しています。グラフのポイントにカーソルを合わせると、そのポイントでのカウントが表示されます。

- トップ **10**：トップ 10 の表示を調整するには、期間を選択します：過去の 1 週間（デフォルト）、1 か月、または 3 か月。シングルセッションマシン、マルチセッションマシン、またはアプリケーションに関連するアクティビティについての情報のみを表示するように表示を調整することもできます。
  - トップ **10** アクティブユーザー：期間中に最も頻繁にデスクトップを開始したユーザーを一覧表示します。行にカーソルを合わせると、起動の総数が表示されます。
  - トップ **10** アクティブカタログ：選択した期間中に最も長い時間アクティブだったカタログを一覧表示します。この時間は、そのカタログのすべてのユーザーセッションを合計したものです。

デスクトップ使用状況レポート

先月のマシン起動についての情報を含むレポートをダウンロードするには、［起動アクティビティ］を選択します。要求が処理中であることを示すメッセージが表示されます。レポートは、ローカルマシンのデフォルトのダウンロード場所に自動的にダウンロードされます。

マシンとセッションを監視するためのフィルタリングと検索

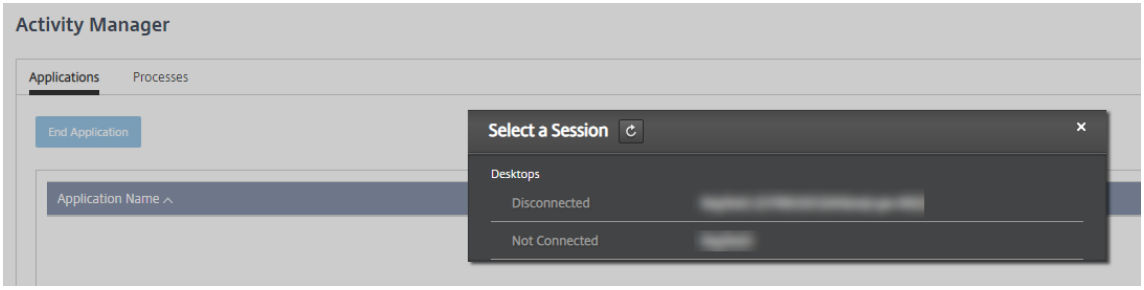
セッションとマシンの情報を監視している場合、デフォルトですべてのマシンまたはセッションが表示されます。次の操作を実行できます：

- マシン、セッション、接続、またはアプリケーションで表示をフィルタリングします。
- 必要な条件を選択し、式を使用してフィルターを作成することにより、セッションまたはマシンの表示を調整します。
- 作成したフィルターを再利用できるように保存します。

ユーザーのアプリケーションの制御

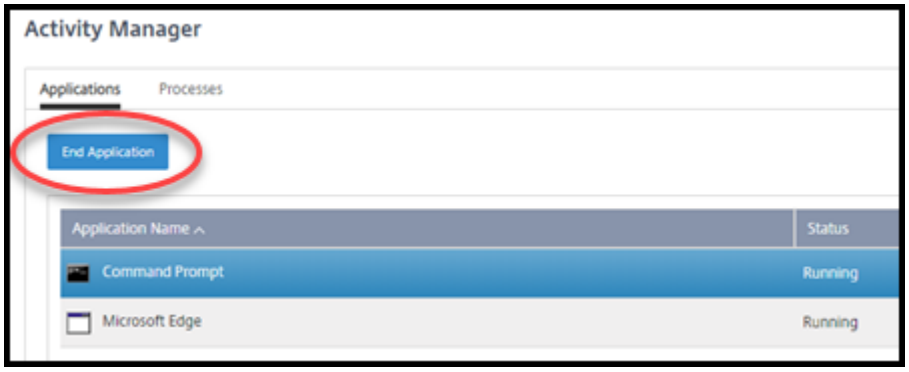
セッションを実行しているユーザーまたはデスクトップが割り当てられているユーザーのアプリケーションとプロセスを表示および管理できます。

1. Citrix DaaS の ［監視］ダッシュボードで ［検索］を選択し、ユーザー名（またはユーザー名の開始文字）、マシン、またはエンドポイントを入力します。検索結果の中から、探しているアイテムを選択します。（検索せずに検索ボックスを折りたたむには、もう一度 ［検索］を選択します。）
2. セッションを選択します。



アクティビティマネージャーは、ユーザーのセッションのアプリケーションとプロセスを一覧表示します。

3. アプリケーションを終了するには、アクティビティマネージャーの ［アプリケーション］タブのアプリケーション行で、そのアプリケーションを選択してから ［アプリケーションの終了］を選択します。



4. プロセスを終了するには、アクティビティマネージャーの ［プロセス］タブのプロセス行で、そのプロセスを選択してから ［プロセスの終了］を選択します。
5. セッションの詳細を表示するには、右上の ［詳細］を選択します。アプリケーションとプロセスの表示に戻るには、右上の［アクティビティマネージャー］を選択します。
6. セッションを制御するには、[セッション制御] > [ログオフ] または ［セッション制御］> ［切断］を選択します。

ユーザーのシャドウ

シャドウ機能を使用すると、ユーザーの仮想マシンまたはセッションを直接表示したり操作したりできます。Windows と Linux VDA をシャドウできます。この機能を使用するには、そのマシンにユーザーが接続している必要があります。その接続を確認するには、`User`タイトルバーに表示されるマシン名を確認します。

シャドウは新しい Web ブラウザータブで起動します。Web ブラウザーで Citrix Cloud URL からのポップアップが許可されていることを確認してください。

シャドウ機能は、ドメイン参加済みマシンのユーザーに対してのみサポートされます。ドメイン非参加マシンをシャドウするには、踏み台マシンをセットアップする必要があります。詳しくは、「踏み台マシンアクセス」を参照してください。

シャドウは、ドメイン参加済みマシンと同じ仮想ネットワークにあるマシンから開始する必要があり、ポートの要件も満たしている必要があります。

シャドウの有効化

1. [管理] > [クイック展開] > [監視] で、[ユーザーの詳細] ビューに移動します。
2. ユーザーセッションを選択し、[アクティビティマネージャー] ビューまたは ［セッション詳細］パネルで、[シャドウ] を選択します。

Linux VDA のシャドウ

シャドウは、RHEL7.3 または Ubuntu バージョン 16.04 Linux ディストリビューションを実行する Linux VDA バージョン 7.16 以降で使用できます。

［監視］は完全修飾ドメイン名（Fully Qualified Domain Name：FQDN）を使用してターゲットの Linux VDA に接続します。［監視］クライアントが Linux VDA の完全修飾ドメイン名を解決できるようにしてください。

- VDA には、`python-websockify`パッケージと`x11vnc` パッケージがインストールされている必要があります。
- VDA への`noVNC`接続は、WebSocket プロトコルを使用します。デフォルトでは、`ws://` WebSocket プロトコルが使用されます。セキュリティ上の理由から、セキュリティ保護された `wss://` プロトコルを使用することをお勧めします。各監視クライアントおよび Linux VDA に SSL 証明書をインストールします。

Linux VDA をシャドウ用に設定するには、「セッションのシャドウ」の手順に従います。

1. シャドウを有効にすると、シャドウ接続が初期化され、確認プロンプトがユーザーデバイスに表示されます。
2. ユーザーが ［はい］を選択すると、マシンまたはセッション共有が開始されます。
3. 管理者は、シャドウセッションのみを表示できます。

Windows VDA のシャドウ

Windows VDA セッションは、Windows リモートアシスタンスを使用してシャドウされます。VDA をインストールするときに`Use Windows Remote Assistance`機能を有効にします。

1. シャドウを有効にするとシャドウ接続が初期化されます。これにより、`.msrc incident`ファイルを開くか保存するかを確認するダイアログボックスが開きます。
2. デフォルトで選択されていない場合は、Remote Assistance Viewer でそのインシデントファイルを開きます。ユーザーデバイス側には、確認のメッセージが表示されます。
3. ユーザーが ［はい］を選択すると、マシンまたはセッション共有が開始されます。
4. ユーザーがマウスやキーボードの制御を許可すると、管理者がシャドウセッションを制御できるようになります。

セッションの監視と制御

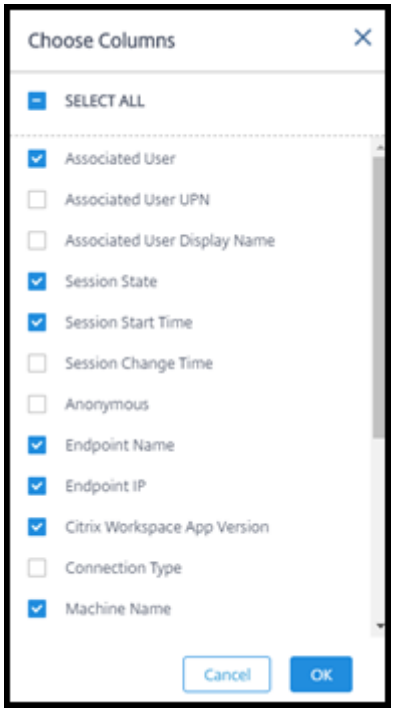
セッションの表示は毎分更新されます。

セッションの表示のほか、1 つまたは複数のセッションを切断したり、ユーザーをセッションからログオフしたりできます。

1. ［管理］**>**［クイック展開］**>**［監視］で、［フィルター］を選択します。

2. [セッション] ビューを選択します。

3. 表示を調整するには、[列の選択] を選択し、表示するアイテムのチェックボックスをオンにします。完了したら、[**OK**] を選択します。セッション表示は自動的に更新されます。



4. 制御する各セッションの左側にあるチェックボックスをオンにします。
5. セッションをログオフまたは切断するには、[セッション制御] **>** [ログオフ] または [セッション制御] **>** [切断] を選択します。

カタログの電源管理スケジュールでは、セッションの切断と、切断されたセッションからのユーザーのログオフも制御できることを覚えておいてください。

上記の手順の代わりとして、ユーザーを ［検索］し、制御するセッションを選択してから、セッションの詳細を表示することもできます。ログオフと切断のオプションもここで使用できます。

セッション情報レポート

セッション情報をダウンロードするには、セッション画面で ［エクスポート］を選択します。要求が処理中であることを示すメッセージが表示されます。レポートは、ローカルマシンのデフォルトのダウンロード場所に自動的にダウンロードされます。

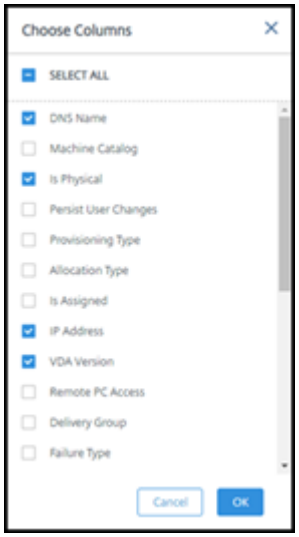
監視および電源制御マシン

マシンの表示は毎分更新されます。

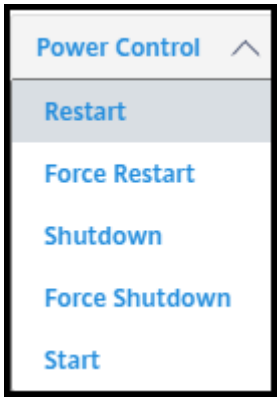
1. ［管理］**>**［クイック展開］**>**［監視］で、［フィルター］を選択します。
2. ［マシン］ビューを選択します。

デフォルトでは、画面にシングルセッション OS マシンが一覧表示されます。または、マルチセッションマシンを表示することもできます。

3. 表示を調整するには、［列の選択］を選択し、表示するアイテムのチェックボックスをオンにします。完了したら、［**OK**］を選択します。マシン表示は自動的に更新されます。



4. マシンの電源を制御したり、保守モードのオン/オフを切り替えたりするには、制御する各マシンの左側にあるチェックボックスをオンにします。
5. 選択したマシンの電源を制御するには、［電源制御］を選択して操作を選択します。



6. 選択したマシンについて保守モードのオン/オフを切り替えるには、［保守モード］**>**［オン］または ［保守モード］**>**［オフ］を選択します。

検索機能を使用してマシンを検索して選択すると、マシンの詳細、使用率、履歴使用率（過去 7 日間）、および平均 IOPS が表示されます。

マシン情報レポート

セッション情報をダウンロードするには、マシン画面で ［エクスポート］を選択します。要求が処理中であることを示すメッセージが表示されます。レポートは、ローカルマシンのデフォルトのダウンロード場所に自動的にダウンロードされます。

アプリとデスクトップの状態のチェック

プロービングは、公開されたアプリとデスクトップの状態をチェックするプロセスを自動化します。ヘルスチェックの結果は、［監視］ダッシュボードから入手できます。詳しくは、次のページを参照してください：

- アプリケーションプロービング
- デスクトッププロービング

クイック展開でのトラブルシューティング

April 22, 2022

はじめに

リソースの場所には、デスクトップとアプリを提供するマシンが含まれています。これらのマシンはカタログで作成されるため、カタログはリソースの場所の一部と見なされます。各リソースの場所には、Cloud Connector も含まれています。Cloud Connector により、Citrix Cloud はリソースの場所と通信できるようになります。通常、シトリックスが Cloud Connector のインストールおよび更新を行います。

オプションで、複数の Cloud Connector およびリソースの場所の操作を開始できます。参照:

- リソースの場所の操作
- カタログ作成時のリソースの場所の設定

Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）には、デスクトップとアプリ（VDA）を提供するマシンとの構成および通信の問題を解決するのに役立つトラブルシューティングツールとサポートツールがあります。たとえば、カタログの作成に失敗したり、ユーザーがデスクトップやアプリを起動できなかったりすることがあります。

このトラブルシューティングには、踏み台マシンまたは直接 RDP で Citrix Managed Azure サブスクリプションにアクセスすることが含まれます。サブスクリプションにアクセスした後、Citrix サポートツールを使用して問題を特定して解決できます。詳しくは、次のページを参照してください:

- 踏み台マシンまたは直接 RDP を使用した VDA のトラブルシューティング
- 踏み台マシンアクセス
- 直接 RDP アクセス

踏み台マシンまたは直接 **RDP** を使用した **VDA** のトラブルシューティング

サポート機能は、Citrix サービスの問題のトラブルシューティングをした経験がある人を対象としています。以下が対象となります:

- Citrix DaaS 製品の技術的知識とトラブルシューティングの経験を持つ、Citrix Service Provider（CSP）など。
- Citrix サポート担当者。

Citrix コンポーネントのトラブルシューティングに慣れていない、または自信がない場合は、Citrix サポートにサポートを依頼できます。Citrix サポート担当者から、このセクションで説明されているアクセス方法の 1 つを設定するように求められる場合があります。ただし、Citrix のツールと技術を使用した実際のトラブルシューティングは Citrix の担当者が行います。

> 重要:
>
> これらのサポート機能は、ドメイン参加済みマシンにのみ有効です。カタログ内のマシンがドメイン未参加の場合、Citrix サポートはトラブルシューティングのヘルプを要求するよう案内します。

アクセス方法

以下のアクセス方法は、Citrix Managed Azure サブスクリプションでのみ有効です。詳しくは、「Azure サブスクリプション」を参照してください。

2 つのサポートアクセス方法が提供されています。

- 顧客専用の Citrix Managed Azure サブスクリプション内の踏み台マシンを使用して、リソースにアクセスします。踏み台マシンは、サブスクリプション内のマシンへのアクセスを許可する単一のエントリポイントです。指定された範囲の IP アドレスからのリモートトラフィックを許可することにより、これらのリソースへの安全な接続を提供します。

  この方法の手順は次のとおりです:

  - 踏み台マシンを作成する
  - RDP エージェントをダウンロードする
  - 踏み台マシンに RDP アクセスする
  - サブスクリプション内の踏み台マシンから他の Citrix マシンに接続する

  踏み台マシンは短期間の使用を目的としています。この方法は、カタログまたはイメージマシンの作成に関連する問題を対象としています。

- 顧客専用の Citrix Managed Azure サブスクリプション内のマシンに直接 RDP アクセスします。RDP トラフィックを許可するには、ネットワークセキュリティグループでポート 3389 を定義する必要があります。

  この方法は、ユーザーがデスクトップを起動できないなど、作成以外のカタログの問題を対象としています。

注意事項：これら 2 つのアクセス方法以外の方法については、Citrix サポートにお問い合わせください。

踏み台マシンアクセス

1. ［管理］**>**［クイック展開］を選択してから、右側にある ［トラブルシューティングとサポート］を開きます。
2. ［トラブルシューティングオプションの表示］をクリックします。
3. ［トラブルシューティング］ページで、最初の 2 種類の問題のいずれかを選択し、［トラブルシューティングマシンを使用する］をクリックします。
4. ［踏み台マシンを使ってトラブルシューティングを行う］ページで、カタログを選択します。

   - 選択したカタログのマシンがドメイン未参加の場合は、Citrix サポートに連絡するように指示されます。
   - 選択したカタログのネットワーク接続への RDP アクセスで踏み台マシンが既に作成されている場合は、手順 8 にスキップします。

5. RDP アクセス範囲が表示されます。ネットワーク接続で許可されている範囲よりも狭い範囲に RDP アクセスを制限する場合は、［**IP** アドレス範囲内のコンピューターのみに **RDP** アクセスを制限する］チェックボックスをオンにして、目的の範囲を入力します。

6. 踏み台マシンに RDP アクセスするとき、ログインに使用するユーザー名とパスワードを入力します。パスワードの要件。

   ユーザー名に Unicode 文字を使用しないでください。

7. ［踏み台マシンを作成］をクリックします。

   踏み台マシンが正常に作成されると、ページタイトルが踏み台 **-** 接続に変わります。

   踏み台マシンの作成が失敗した場合（または操作中に失敗した場合）、失敗通知ページの下部にある ［削除］をクリックします。もう一度、踏み台マシンの作成を試行してください。

   踏み台マシンの作成後に、RDP 範囲の制限を変更できます。［編集］をクリックします。新しい値を入力し、チェックマークをクリックして変更を保存します（変更をキャンセルするには、［**X**］をクリックします）。

8. ［**RDP** ファイルのダウンロード］をクリックします。
9. 踏み台マシンの作成時に指定した資格情報を使用して、踏み台マシンに RDP アクセスします（踏み台マシンのアドレスは、ダウンロードした RDP ファイルに埋め込まれています）。
10. サブスクリプション内の踏み台マシンから他の Citrix マシンに接続します。その後、ログを収集して診断を実行できます。

踏み台マシンは、作成時に電源がオンになります。コストを節約するため、マシンが起動後にアイドル状態のままである場合、マシンの電源は自動的にオフになります。マシンは数時間後に自動的に削除されます。

ページの下部にあるボタンを使用して、踏み台マシンを電源管理または削除できます。踏み台マシンの削除を選択した場合は、マシン上のアクティブなセッションが自動的に終了になることを確認する必要があります。また、マシンに保存されていたデータやファイルはすべて削除されます。

直接 **RDP** アクセス

1. ［管理］**>**［クイック展開］を選択してから、右側にある ［トラブルシューティングとサポート］を開きます。
2. ［トラブルシューティングオプションの表示］をクリックします。
3. ［トラブルシューティング］ページで、［その他のカタログの問題］を選択します。
4. ［**RDP** アクセスを使ってトラブルシューティングを行う］ページで、カタログを選択します。

   選択したカタログのネットワーク接続への RDP アクセスが既に有効になっている場合は、手順 7 にスキップします。

5. RDP アクセス範囲が表示されます。ネットワーク接続で許可されている範囲よりも狭い範囲に RDP アクセスを制限する場合は、［**IP** アドレス範囲内のコンピューターのみに **RDP** アクセスを制限する］チェックボックスをオンにして、目的の範囲を入力します。
6. ［**RDP** アクセスを有効にする］をクリックします。

   RDP アクセスが正常に有効になると、ページタイトルが **RDP** アクセス **-** 接続に変わります。

RDP アクセスが正常に有効になっていない場合は、失敗通知ページの下部にある ［**RDP** の有効化を再試行］をクリックします。

7. Active Directory 管理者の資格情報を使用してマシンに接続します。その後、ログを収集して診断を実行できます。

支援が必要な場合

引き続き問題が発生する場合は、「ヘルプとサポートの利用」の手順に従ってチケットを作成してください。

クイック展開リファレンス

August 8, 2022

［クイック展開］ダッシュボードの［カタログ］タブ

Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）の ［管理］**>**［クイック展開］ダッシュボードで、カタログのエントリの任意の場所をクリックします。次のタブには、カタログに関する情報が表示されます:

- 詳細: カタログの作成時（または最新の編集時）に指定した情報を一覧表示します。また、カタログの作成に使用されたイメージに関する情報も含まれます。

  このタブで、次のことができます:

  - カタログで使用されているイメージの変更。
  - カタログの削除。
  - カタログで使用されているリソースの場所の詳細が含まれるページにアクセスします。

- デスクトップ: シングルセッション（静的またはランダム）マシンを含むカタログでのみ使用できます。このタブで、カタログの名前と説明を変更できます。

- デスクトップとアプリ:［デスクトップとアプリ］タブは、マルチセッションマシンを含むカタログでのみ使用できます。このタブで、次のことができます:

  - カタログのユーザーが Citrix Workspace でアクセスできるアプリケーションの追加、編集、または削除。
  - カタログの名前と説明の変更。

- 利用者: 種類（ユーザーまたはグループ）、アカウント名、表示名、および Active Directory ドメインとユーザープリンシパル名を含むすべてのユーザーを一覧表示します。

  このタブで、カタログのユーザーを追加または削除できます。

- マシン：カタログ内のマシンの総数のほか、登録済みのマシン、未登録のマシン、および保守モードがオンのマシンの数を表示します。

  カタログ内の各マシンについて、画面には各マシンの名前、電源状態（オン/オフ）、登録の状態（登録済み/未登録）、割り当て済みユーザー、セッション数（0/1）、および保守モードの状態（オンまたはオフを示すアイコン）などが表示されます。

  このタブで、次のことができます：

  - マシンの追加または削除
  - マシンの起動、再起動、強制再起動、またはシャットダウン
  - マシンの保守モードのオン/オフの切り替え

  詳しくは、「カタログの管理」を参照してください。マシン操作の多くは、［クイック展開］ダッシュボードの［監視］タブでも使用できます。「監視および電源制御マシン」を参照してください。

- 電源管理：カタログ内のマシンの電源がオン/オフになるタイミングを管理できます。スケジュールは、アイドル状態のマシンがいつ切断されるかも示します。

  カスタムのカタログを作成するとき、または後で、電源スケジュールを構成できます。スケジュールが明示的に設定されていない場合、セッションが終了するとマシンの電源がオフになります。

  簡易作成を使用してカタログを作成する場合、電源スケジュールを選択または構成することはできません。デフォルトでは、簡易作成カタログは、コスト削減用プリセットスケジュールを使用します。ただし、後でそのカタログを編集したりスケジュールを変更したりできます。

  詳しくは、「電源管理スケジュールの管理」を参照してください。

DNS サーバー

このセクションの内容は、ドメイン参加済みマシンを含むすべての展開に適用されます。ドメイン非参加マシンのみを使用する場合は、このセクションを無視してかまいません。

1. ドメイン参加済みカタログ（または、Citrix Managed Azure サブスクリプションを使用している場合は、接続）を作成する前に、パブリックドメイン名とプライベートドメイン名を解決できる DNS サーバーエントリがあるかどうかを確認してください。

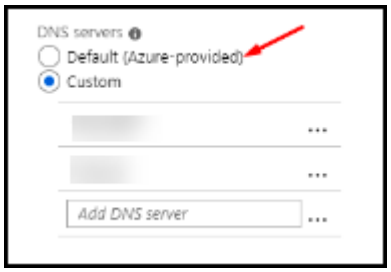
   Citrix DaaS は、カタログまたは接続を作成するとき、少なくとも 1 つの有効な DNS サーバーエントリを探します。有効なエントリが見つからない場合、作成操作は失敗します。

   確認する場所：

   - 自身の Azure サブスクリプションを使用している場合は、Azure の ［**DNS** サーバー］エントリを確認します。
   - Citrix Managed Azure サブスクリプションを使用していて、Azure VNet ピアリング接続を作成している場合は、ピアリングしている Azure VNet の ［**DNS** サーバー］エントリを確認します。

- Citrix Managed Azure サブスクリプションを使用していて、SD-WAN 接続を作成している場合は、SD-WAN Orchestratorの DNS エントリを確認します。

2. Azure では、［カスタム］設定に少なくとも 1 つの有効なエントリが必要です。このサービスは、Azure 提供の ［規定］設定では使用できません。



- Azure 提供の ［規定］が有効になっている場合は、設定を ［カスタム］に変更し、少なくとも 1 つの DNS サーバーエントリを追加します。
- ［カスタム］の下に DNS サーバーのエントリが既にある場合は、このサービスで使用するエントリがパブリックドメインとプライベートドメインの IP 名を解決できることを確認してください。
- ドメイン名を解決できる DNS サーバーがない場合は、それらの機能を備えた Azure 提供の DNS サーバーを追加することを Citrix ではお勧めします。

3. DNS サーバーのエントリを変更した場合は、仮想ネットワークに接続されているすべてのマシンを再起動します。再起動すると、新しい DNS サーバー設定が割り当てられます（VM は、再起動するまで現在の DNS 設定を使用し続けます）。

接続の作成後、後で DNS アドレスを変更する場合：

- 自身の Azure サブスクリプションを使用する場合は、（前の手順で説明したように）Azure で変更できます。または、このサービス内で変更できます。
- Citrix Managed Azure サブスクリプションを使用する場合、このサービスは、Azure で行った DNS アドレスの変更を同期しません。ただし、このサービスでは接続の DNS 設定を変更できます。

DNS サーバーアドレスを変更すると、その接続を使用するカタログ内のマシンの接続に問題が生じる可能性があることに注意してください。

このサービスを使用した **DNS** サーバーの追加

DNS サーバーアドレスを接続に追加する前に、その DNS サーバーがパブリックドメイン名と内部ドメイン名を解決できることを確認してください。DNS サーバーを追加する前に、Citrix では、DNS サーバーへの接続をテストすることをお勧めします。

1. 接続の作成時に DNS サーバーアドレスを追加、変更、または削除するには、接続の種類の ［追加］ページで［**DNS** サーバーの編集］を選択します。または、DNS サーバーアドレスが見つからなかったことを示すメッセージが表示された場合は、［**DNS** サーバーの追加］を選択します。手順 3 に進みます。

2. 既存の接続の DNS サーバーアドレスを追加、変更、または削除するには:

   a) ［管理］**>** ［クイック展開］を選択し、右側にある ［ネットワーク接続］を展開します。
   b) 編集する接続を選択します。
   c) ［**DNS** サーバーの編集］を選択します。

3. アドレスを追加、変更、または削除します。

   a) アドレスを追加するには、［**DNS** サーバーの追加］を選択してから、IP アドレスを入力します。
   b) アドレスを変更するには、アドレスフィールド内をクリックして数値を変更します。
   c) アドレスを削除するには、アドレスエントリの横にあるゴミ箱アイコンを選択します。すべての DNS サーバーアドレスを削除することはできません。接続には、少なくとも 1 つのアドレスが必要です。

4. 完了したら、ページの下部にある ［変更の確認］を選択します。
5. その接続を使用するすべてのマシンを再起動します。再起動すると、新しい DNS サーバー設定が割り当てられます（VM は、再起動するまで現在の DNS 設定を使用し続けます）。

ポリシー

ドメイン未参加マシンのグループポリシーの設定

1. イメージに使用されているマシンに RDP で接続します。
2. Citrix グループポリシー管理をインストールします:

   a) CTX220345を参照します。添付ファイルをダウンロードしてください。
   b) ダウンロードしたファイルをダブルクリックします。`Group Policy Templates 1912 > Group Policy Management`フォルダーにある`CitrixGroupPolicyManagement_x64.msi`をダブルクリックしてください。

3. 「**Run**」コマンドを実行して、`gpedit.msc`を起動し、グループポリシーエディターを開きます。
4. `User Configuration Citrix Policies > Unfiltered`で ［ポリシーの編集］を選択します。

   グループポリシー管理コンソールで障害が発生した場合は（CTX225742を参照）、Microsoft Visual C++ 2015 のランタイム（またはそのランタイムの以降のバージョン）をインストールします。

5. 必要に応じて、ポリシー設定を有効にします。例:

   - ［設定］タブの ［コンピューターの構成］または ［ユーザーの構成］で作業をする場合（構成するものに応じて選択）、`Category > ICA / Printing`で ［**PDF** ユニバーサルプリンターを自動作成する］を選択して［Enabled］に設定します。
   - ログインしたユーザーをデスクトップの管理者にする場合は、［対話型ユーザー］グループを組み込みの管理者グループに追加します。

6. 完了したら、イメージを保存します。
7. 新しいイメージを使用して、既存のカタログの更新または新しいカタログの作成を行います。

ドメイン参加済みマシンのグループポリシーの設定

1. グループポリシー管理機能がインストールされていることを確認します。
   - Windows マルチセッションマシンには、役割と機能を追加するための Windows ツール（[役割と機能の追加］など）を使用して、グループポリシー管理機能を追加します。
   - Windows シングルセッションマシンには、適切なオペレーティングシステムのリモートサーバー管理ツールをインストールします（このインストールにはドメイン管理者アカウントが必要です）。インストール後、［スタート］メニューでグループポリシー管理コンソールを使用できます。
2. Citrix のダウンロードページから Citrix グループポリシー管理パッケージをダウンロードしてインストールし、必要に応じてポリシー設定を構成します。「ドメイン未参加マシンのグループポリシーの設定」の手順 2 から最後までの手順に従います。

使用可能なものについては、「ポリシー設定リファレンス」の記事を参照してください。すべてのポリシー機能は、Citrix DaaS の［完全な構成］インターフェイスで使用できます。

リソースの場所の操作

デスクトップとアプリを公開するための最初のカタログを作成すると、Citrix によりリソースの場所と 2 つの Cloud Connector が自動的に作成されます。カタログを作成するときに、そのリソースの場所に関連するいくつかの情報を指定できます。カタログ作成時のリソースの場所の設定を参照してください。

リモート PC アクセスの場合、リソースの場所と Cloud Connector を作成します。

このセクションでは、リソースの場所が作成された後に使用可能な操作について説明します。

1. ［管理］**>**［クイック展開］を選択してから、右側にある ［**Cloud** サブスクリプション］を開きます。
2. サブスクリプションを選択します。
   - ［詳細］タブには、サブスクリプション内のカタログとイメージの数と名前が表示されます。デスクトップまたはアプリを提供できるマシンの数も表示されます。この数には、イメージ、Cloud Connector、RDS ライセンスサーバーなど、他の目的で使用されるマシンは含まれません。
   - ［リソースの場所］タブには、各リソースの場所が一覧表示されます。各リソースの場所のエントリには、そのリソースの場所内の各 Cloud Connector の状態とアドレスが含まれます。

リソースの場所のエントリにある省略記号メニューには、次の操作が含まれます。

ヘルスチェックの実行

［ヘルスチェックの実行］を選択すると、接続チェックがすぐに開始されます。チェックに失敗した場合、その Cloud Connector は Citrix Cloud と通信していないため、状態は不明です。Cloud Connector を再起動することをお勧めします。

Connector の再起動

Citrix では、一度に 1 つの Cloud Connector のみを再起動することをお勧めします。再起動すると Cloud Connector がオフラインになり、ユーザーアクセスとマシン接続が中断されます。

再起動する Cloud Connector のチェックボックスをオンにします。［再起動］を選択します。

Connector の追加

Cloud Connector の追加は、通常、完了するまでに 20 分かかります。

以下の情報を入力します:

- 追加する Cloud Connector の数。
- Cloud Connector マシンをドメインに参加させるために使用されるドメインサービスアカウントの資格情報。
- マシンパフォーマンス。
- Azure リソースグループ。デフォルトは、リソースの場所によって最後に使用されたリソースグループです。
- 組織単位（OU）。デフォルトは、リソースの場所で最後に使用された OU です。
- ネットワークにインターネット接続用のプロキシサーバーが必要かどうか。［はい］を指定した場合は、プロキシサーバーの FQDN または IP アドレス、およびポート番号を入力します。

完了したら、［**Connector** の追加］を選択します。

Connector の削除

Cloud Connector が Citrix Cloud と通信できず、再起動しても問題が解決しない場合、Citrix サポートはその Cloud Connector を削除することを推奨する場合があります。

削除する Cloud Connector のチェックボックスをオンにします。次に、［削除］を選択します。確認のメッセージが表示されたら、［削除］をクリックします。

使用可能な Cloud Connector を削除することもできます。ただし、その Cloud Connector を削除することでリソースの場所で使用可能な Cloud Connector が 2 つ未満になる場合は、選択した Cloud Connector を削除することはできません。

更新時間の選択

Citrix は、Cloud Connector のソフトウェア更新プログラムを自動的に提供します。更新中、1 つの Cloud Connector がオフラインになって更新されますが、他の Cloud Connector はサービスを継続します。最初の更新が完了すると、別の Cloud Connector がオフラインになって更新されます。このプロセスは、リソースの場所にあるすべての Cloud Connector が更新されるまで続きます。多くの場合、更新を開始するのに最適な時間は、通常の営業時間外です。

更新を開始する時間を選択するか、更新プログラムが利用可能になったときに更新を開始すると指定します。完了したら、［保存］を選択します。

名前の変更

リソースの場所の新しい名前を入力します。［保存］を選択します。

接続の構成

ユーザーが、Citrix Gateway サービスを介してデスクトップとアプリにアクセスできるのか、それとも企業ネットワーク内からのみアクセスできるのかを指定します。

Profile Management

Profile Managementを使用すると、ユーザーデバイスの場所に関係なく、ユーザーの仮想アプリケーションに個人設定が適用されるようになります。

Profile Management の構成は任意です。

Profile Management は、プロファイル最適化サービスで有効にできます。このサービスを利用することで、Windows でプロファイル設定を確実に管理できます。プロファイルを管理するとユーザーに単一のプロファイルのみが適用されるようになるため、一貫したユーザーエクスペリエンスを確保できます。ユーザープロファイルが自動的に集約および最適化されるため、管理と保存の手間が最小化されます。プロファイル最適化サービスにより、必要な管理、サポート、インフラストラクチャを最低限に抑えられます。また、ログオンおよびログオフ時のユーザーエクスペリエンスも向上します。

プロファイル最適化サービスを使用するには、すべての個人設定を保存するファイル共有が必要になります。そのファイルサーバーを管理します。これらのファイルサーバーへのアクセスを許可するようにネットワーク接続を設定することをお勧めします。ファイル共有は UNC パスとして指定する必要があります。このパスには、システム環境変数、Active Directory のユーザー属性、Profile Management の変数を含めることができます。UNC テキスト文字列の書式について詳しくは、「ユーザーストアへのパスの指定」を参照してください。

Profile Management を有効にする場合は、ユーザーのプロファイルをさらに最適化するため、フォルダーリダイレクトを構成してユーザープロファイルのサイズの影響を最小限に抑えることも検討してください。フォルダーリダ

イレクトを適用することで、Profile Management ソリューションを強化できます。詳しくは、「Microsoft フォルダーリダイレクト」を参照してください。

Windows Server ワークロード用の Microsoft RDS ライセンスサーバーの構成

このサービスは、Windows 2016 などの Windows Server ワークロードを配信するとき、Windows Server リモートセッション機能にアクセスします。これには通常、リモートデスクトップサービスクライアントアクセスライセンス（RDS CAL）が必要です。Citrix VDA がインストールされている Windows マシンは、RDS CAL の要求のために RDS ライセンスサーバーに接続できる必要があります。

ライセンスサーバーをインストールしてアクティブ化してください。詳しくは、Microsoft 社のドキュメント「リモートデスクトップサービスライセンスサーバーをアクティブ化する」を参照してください。概念実証環境では、Microsoft から提供される猶予期間を利用できます。

この方法により、Citrix DaaS でライセンスサーバーの設定を適用できます。イメージの RDS コンソールでは、ライセンスサーバーおよび接続ユーザー数モードを構成できます。また、Microsoft のグループポリシー設定を使用して、ライセンスサーバーを構成することもできます。詳しくは、Microsoft 社のドキュメント「クライアントアクセスライセンス（CAL）を使用して RDS 展開をライセンスする」を参照してください。

グループポリシー設定を使用して RDS ライセンスサーバーを構成するには

1. 使用可能な VM のいずれかに、リモートデスクトップサービスのライセンスサーバーをインストールします。この VM は常に使用可能なものである必要があります。また、Citrix DaaS のワークロードが常にこのライセンスサーバーに接続できる必要があります。
2. Microsoft のグループポリシーを使用して、ライセンスサーバーアドレスと単一ユーザーライセンスモードを指定します。　詳しくは、Microsoft 社のドキュメント「Specify the Remote Desktop Licensing Mode for an RD Session Host Server」を参照してください。

Windows 10 ワークロードには、適切な Windows 10 ライセンスのアクティブ化が必要です。Microsoft のドキュメントに従って、Windows 10 ワークロードをアクティブ化することをお勧めします。

消費コミットメントの使用状況

> 注:
>
> この機能はプレビュー段階です。

［管理］**>**［クイック展開］で、［全般］カードを選択します。［消費］の値は、現在のカレンダー月に使用された消費量を示します。この値には、月単位および期間のコミットメントが含まれます。

［全般］を選択すると、［通知］タブには次のものが表示されます:

- その月に使用された総消費量（月単位および期間）。
- 月単位の消費コミットメントのユニット数。

- 期間の消費コミットメントのパーセンテージ。

値と進行状況バーにより、潜在的または実際の使用量の超過が通知されることがあります。

実際のデータが表示されるまでに 24 時間かかることがあります。使用状況と課金データは、カレンダー月の終わりから 72 時間後が最終と見なされます。

使用状況について詳しくは、「ライセンスおよびアクティブな使用状況の監視」を参照してください。

オプションで、消費使用状況（月単位、期間、またはその両方のコミットメント）が指定のレベルに達したときに、[管理] > [クイック展開] ダッシュボードに通知を表示するよう要求できます。デフォルトでは、通知は無効になっています。

1. [通知] タブで、[通知設定の編集] を選択します。
2. 通知を有効にするには、スライダーをクリックしてチェックマークを表示します。
3. 値を入力します。必要に応じて、他の消費タイプについても同じ作業を繰り返します。
4. [保存] を選択します。

通知を無効にするには、スライダーをクリックしてチェックマークを非表示にしてから [保存] を選択します。

Citrix ライセンスの使用状況の監視

Citrix ライセンスの使用状況情報を表示するには、「ライセンスおよびアクティブな使用状況の監視」のガイダンスに従ってください。以下を表示できます:

- ライセンスの概要
- 使用状況レポート
- 使用状況の傾向とライセンスアクティビティ
- ライセンス使用ユーザー

ライセンスを解放することもできます。

負荷分散

負荷分散は、シングルセッションマシンではなく、マルチセッションマシンに適用されます。

> 重要:
>
> 負荷分散方法を変更すると、展開内のすべてのカタログに影響します。これには、サポートされているホストの種類（クラウドベースおよびオンプレミス）を使用して作成したすべてのカタログが含まれます。カタログの作成に使用したインターフェイス（[完全な構成] や [クイック展開] など）は関係ありません。
>
> 続行する前に、すべてのカタログにセッションの上限が設定されていることを確認してください。

> • ［クイック展開］では、この設定は各カタログの ［詳細］タブにあります。
> • ［完全構成］では、「マシンの負荷分散」を参照してください。

負荷分散により、マシンの負荷が測定され、現在の条件下で受信ユーザーセッション用として選択されるマルチセッションマシンが決定されます。この選択は、構成済みの負荷分散方法に基づきます。

水平または垂直の 2 つの負荷分散方法のいずれかを構成できます。この方法は、Citrix DaaS 展開内のすべてのマルチセッションカタログ（つまり、すべてのマルチセッションマシン）に適用されます。

- 水平負荷分散：受信ユーザーセッションを、最も負荷が少なく電源がオンになっている使用可能なマシンに割り当てます。

  簡単な例：それぞれ 10 セッション用に構成された 2 つのマシンがあるとします。最初のマシンは 5 つの同時セッションを処理します。2 つ目のマシンは他の 5 つのセッションを処理します。

  水平負荷分散によって高いユーザーパフォーマンスを実現できますが、より多くのマシンの電源をオンにして使用し続けるので、コストが増加する可能性があります。

  デフォルトでは、この方法が有効になっています。

- 垂直負荷分散：受信ユーザーセッションを、読み込みインデックスが最も高く電源がオンになっているマシンに割り当てます Citrix DaaS は、すべてのマルチセッションマシンの読み込みインデックスを計算してから割り当てます。この計算では、CPU、メモリ、同時実行性などの要素が考慮されます。

  この方法により、既存のマシンが飽和状態になった後、新しいマシンに移ります。ユーザーが既存のマシンを切断して容量を解放すると、それらのマシンに新しく負荷が割り当てられます。

  簡単な例：それぞれ 10 セッション用に構成された 2 つのマシンがあるとします。最初のマシンは、最初の 10 個の同時セッションを処理します。2 つ目のマシンは、11 番目のセッションを処理します。

  垂直負荷分散により、セッションは電源オンのマシンの容量を最大化し、マシンコストを節約できます。

負荷分散方法を構成するには：

1. ［管理］**>**［クイック展開］を選択してから、右側にある ［全般］を開きます。
2. ［グローバル設定］で ［すべて表示］を選択します。
3. ［グローバル設定］ページの ［マルチセッションカタログの負荷分散］で、負荷分散方法を選択します。
4. ［確認］を選択します。

プロキシサーバーを使用するネットワークでのカタログ作成

ネットワークにインターネット接続用のプロキシサーバーが必要であり、自身の Azure サブスクリプションを使用している場合は、以下の手順に従ってください（プロキシサーバーを必要とするネットワークでの Citrix Managed Azure サブスクリプションの使用はサポートされていません）。

1. ［管理］**>**［クイック展開］で、必要な情報を入力してカタログ作成プロセスを開始し、ページの下部にある ［カタログの作成］を選択します。

2. プロキシ要件が原因で、カタログの作成は失敗します。ただし、リソースの場所は作成されます。カタログの作成時にリソースの場所の名前を指定した場合を除き、そのリソースの場所の名前は「DAS」で始まる名前になります。［管理］**>**［クイック展開］ダッシュボードで、右側にある［**Cloud** サブスクリプション］を開きます。［リソースの場所］タブで、新しく作成されたリソースの場所に Cloud Connector があるかどうかを確認します。ある場合は、それらを削除します。
3. Azure で、2 つの VM を作成します（「Cloud Connector のシステム要件」を参照）。それらのマシンをドメインに参加させます。
4. Citrix Cloud コンソールで、各 VM にCloud Connector をインストールします。以前に作成されたのと同じリソースの場所に Cloud Connector があることを確認してください。以下のガイダンスに従います：
   - Cloud Connector のプロキシとファイアウォールの構成
   - システムおよび接続要件
5. ［管理］**>**［クイック展開］で、カタログ作成プロセスを繰り返します。カタログが作成されると、前の手順で作成したリソースの場所と Cloud Connector が使用されます。

支援が必要な場合

- 「トラブルシューティング」を確認してください。
- Citrix DaaS についてさらにサポートが必要な場合は、「ヘルプとサポートの利用」のガイダンスに従ってチケットを開いてください。

デリバリーグループの作成

June 12, 2024

はじめに

デリバリーグループは、いくつかのマシンカタログから選択したマシンをグループ化したものです。また、デリバリーグループでは、それらのマシンを使用できるユーザーと、これらのユーザーに提供するアプリケーションとデスクトップも指定できます。

デリバリーグループの作成は、展開の構成でマシンカタログを作成した後に行います。その後、最初のデリバリーグループの初期設定を変更し、別のデリバリーグループを作成することができます。また、デリバリーグループの作成時ではなく、その編集時にのみ構成できる機能と設定もあります。

デリバリーグループを作成する前に：

- 以下のセクションを確認して、選択する項目および指定する情報について理解しておいてください。

- マシンをホストするハイパーバイザーやクラウドサービスなどのリソースに対して、接続を作成していることを確認してください。
- 仮想マシンまたは物理マシンが含まれるマシンカタログを作成していることを確認してください。

デリバリーグループ作成ウィザードを起動するには:

1. Citrix Cloudにサインインします。左上のメニューで、［マイサービス］**>**［**DaaS**］を選択します。
2. ［管理］を選択します。
3. 初めてデリバリーグループを作成する場合、コンソールでは適切な選択を行うためのガイドが表示されます（［サービスとして表示させるデリバリーグループをセットアップします］など）。デリバリーグループ作成ウィザードが開き、手順が示されます。
4. 既にデリバリーグループを作成済みで、別のデリバリーグループを作成する場合は、次の手順に従います:
   a) ［管理］**>**［完全な構成］の左側ペインで ［デリバリーグループ］を選択します。
   b) フォルダーを使用してデリバリーグループを整理するには、デフォルトの ［**Delivery Groups**］フォルダーの下にフォルダーを作成します。詳しくは、「グループフォルダーの作成」を参照してください。
   c) グループを作成するフォルダーを選択し、［デリバリーグループの作成］をクリックします。グループ作成ウィザードが開きます。

ウィザードの指示に従って、以下のセクションで説明されているページの操作を行います。選択内容によっては、異なるウィザードページが表示されることがあります。

手順 **1**: マシン

マシンカタログを選択して、そのマシンカタログから使用するマシンの数を選択します。

ヒント:

- マシンカタログに未使用のマシンが残っていない場合、そのカタログを選択することはできません。
- カタログは、複数のデリバリーグループで指定できます。マシンは 1 つのデリバリーグループでのみ使用できます。
- デリバリーグループでは、複数のカタログのマシンを使用できます。ただし、これらのマシンカタログに同じ種類のマシン（マルチセッション OS、シングルセッション OS、リモート PC アクセス）が含まれている必要があります。つまり、異なる種類のマシンをデリバリーグループに混在させることはできません。同様に、展開に Windows マシンのカタログと Linux マシンのカタログが含まれている場合、デリバリーグループには、両方ではなくいずれかの種類のオペレーティングシステムのマシンのみを含めることができます。
- MCS デリバリーグループには、MCS タイプのカタログのみを追加できます。
- 最新の VDA バージョンをインストールするか VDA を最新バージョンにアップグレードしてから、必要に応じてマシンカタログおよびデリバリーグループに対して機能レベルの変更を実行することを Citrix ではお勧めします。デリバリーグループの作成時に、異なる VDA バージョンがインストールされたマシンを選択した場

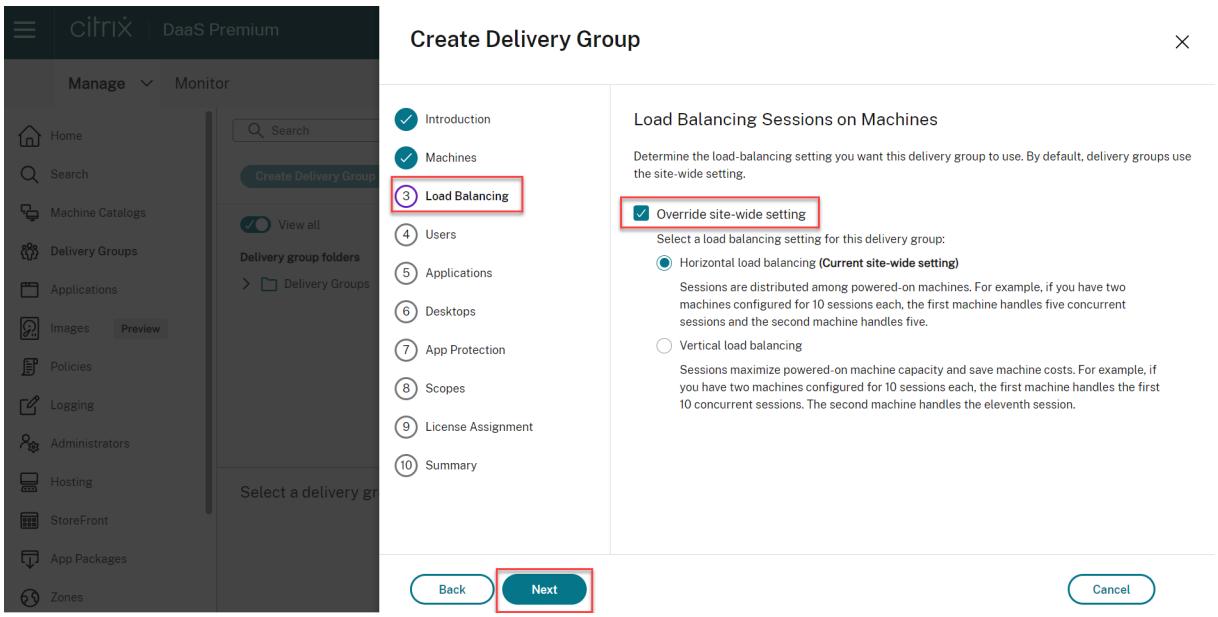
合、デリバリーグループは最も古いバージョンと互換性を持ちますたとえば、選択したマシンの 1 つに VDA Version 7.1 がインストールされており、ほかのマシンにはそれ以降のバージョンがインストールされている場合、グループ内のすべてのマシンで使用できるのは、VDA 7.1 でサポートされている機能のみです。すなわち、7.1 より後のバージョンの VDA が必要な機能は、このデリバリーグループでは利用できない可能性があります。

- 次の互換性チェックが実行されます:
  - MinimumFunctionalLevel に互換性があること
  - SessionSupport に互換性があること
  - AllocationType は SingleSession に対する互換性があること
  - ProvisioningType に互換性があること
  - PersistChanges は MCS および Citrix Provisioning に対する互換性があること
  - RemotePC カタログは RemotePC カタログとのみ互換性があること
  - AppDisk 関連のチェック

手順 **2**：負荷分散（**Technical Preview**）

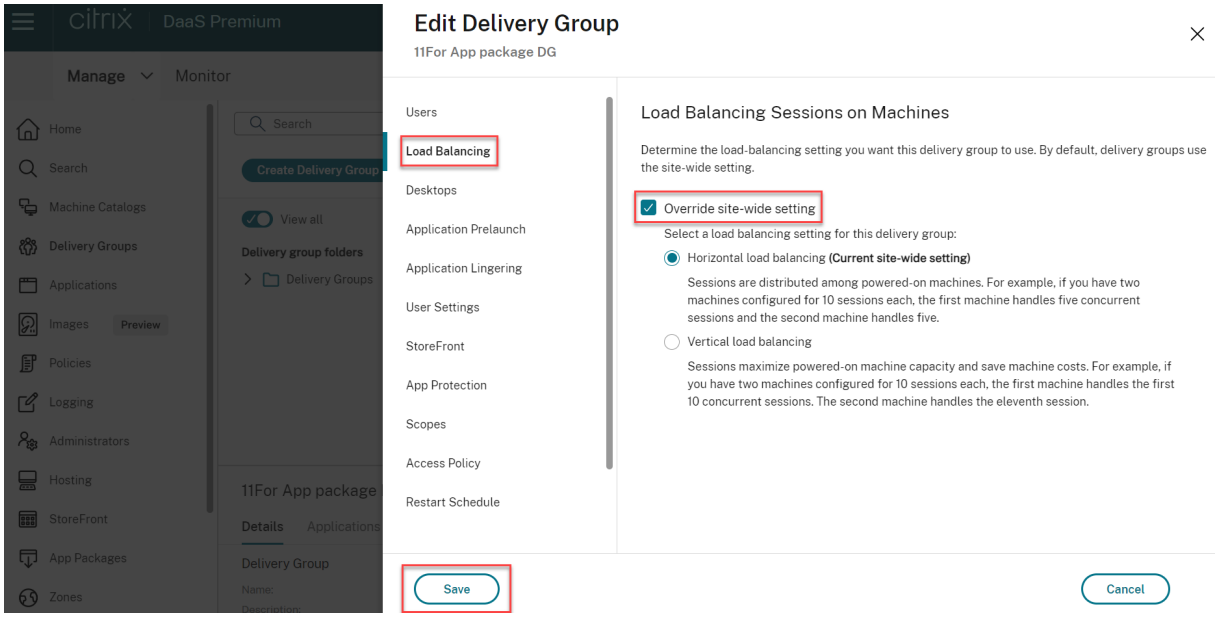
デリバリーグループの作成時に負荷分散設定を構成するには、次の手順を実行します:

1. DaaS Premium にログインします。
2. 左側のナビゲーションで、［デリバリーグループ］をクリックします。
3. ［デリバリーグループ］ページで、［デリバリーグループの作成］をクリックします。
4. デリバリーグループの作成ウィザードで、［次へ］をクリックします。［マシン］ウィザードが開きます。
5. ［マシン］ウィザードで、必要なマシンカタログを選択し、［次へ］をクリックします。負荷分散ウィザードが開きます。
6. 負荷分散 ウィザードで、［サイト全体の設定を上書きする］チェックボックスを選択します。
7. 必要に応じて［水平負荷分散］または ［垂直負荷分散］オプションを選択し、［次へ］をクリックします。

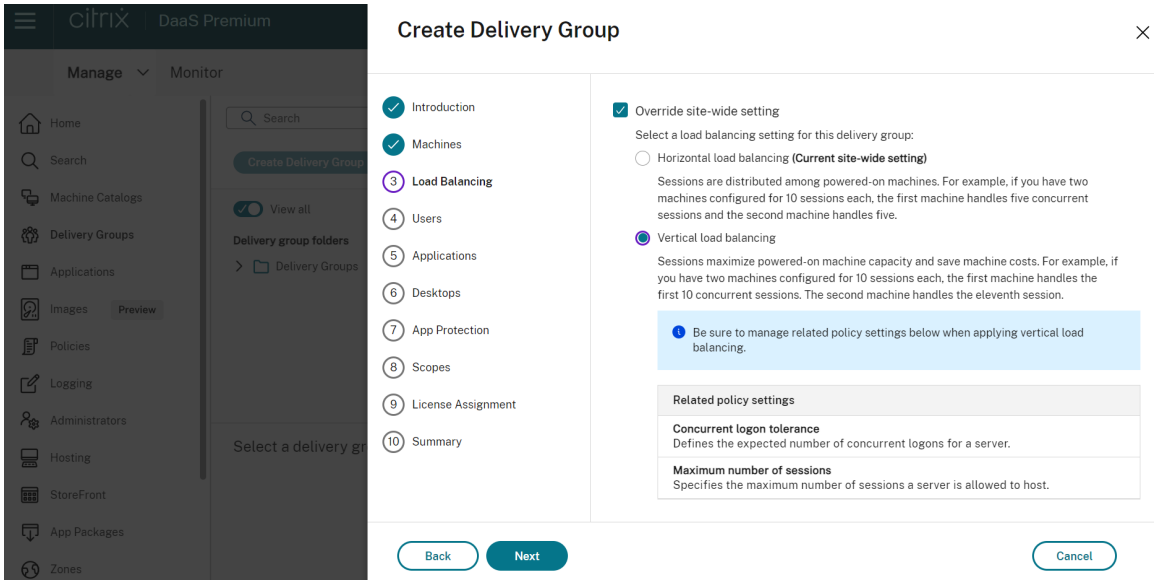


既存のデリバリーグループの編集中に負荷分散設定を構成するには、次の手順を実行します:

1. DaaS Premium にログインします。
2. 左側のナビゲーションで、[デリバリーグループ] をクリックします。
3. 一覧から [デリバリーグループ] を選択し、[編集] をクリックします。デリバリーグループの編集ウィザードが開きます。
4. [デリバリーグループの編集] ページで、[負荷分散] をクリックします。
5. [サイト全体の設定を上書きする] チェックボックスを選択します。
6. 必要に応じて [水平負荷分散] または [垂直負荷分散] オプションを選択し、[保存] をクリックします。



> 注:
>
> 垂直負荷分散設定が適用されている場合は、［同時ログオントレランス］と ［最大セッション数］ポリシーが適切に構成されていることを確認してください。



サイトレベルおよびデリバリーグループレベルでの負荷分散について詳しくは、「マシンの負荷分散」を参照してください。

手順 **3**: 配信の種類

このページは、静的な（割り当て済み）シングルセッションOS マシンを含むマシンカタログを選択した場合にのみ開きます。［アプリケーション］または ［デスクトップ］を選択します。両方を有効にすることはできません。

マルチセッション OS またはシングルセッション OS のランダム（プール）カタログのマシンを選択した場合、配信の種類はアプリケーションとデスクトップと見なされます。この場合は、アプリケーションかデスクトップ、またはその両方を配信できます。

手順 **4**: **AppDisk**

このページは無視してください。［次へ］を選択します。

手順 **5**: ユーザー

このデリバリーグループで配信されるアプリケーションやデスクトップを使用できるユーザーおよびユーザーグループを指定します。

ユーザー一覧の指定場所

以下の作成時または編集時に、ユーザー一覧を指定します:

- 展開のユーザーアクセス一覧（このコンソールでは構成しません）。アプリケーション資格ポリシー規則には、デフォルトではすべてのユーザーが含まれます。詳しくは、PowerShell SDKの`BrokerAppEntitlementPolicyRule`コマンドレットを参照してください。
- デリバリーグループ。
- アプリケーション。

> 注:
>
> ユーザー一覧を指定する場合、Citrix Cloud アカウントが接続されている次の ID プロバイダーのいずれかからユーザーアカウントを選択できます: Active Directory、Azure Active Directory（Microsoft Entra ID）、または Okta。

アプリケーションにアクセスできるユーザーの一覧は、上記の各ユーザー一覧の共通部分になります。

認証が必要なユーザーおよび認証が不要なユーザー

ユーザーには、認証が必要なユーザーと認証が不要なユーザーの 2 種類があります（認証が不要なユーザーは「匿名ユーザー」とも呼ばれます）。いずれか一方または両方の種類のユーザーをデリバリーグループ内に構成できます。

- 認証が必要なユーザー: 特定のアカウント名で指定したユーザーおよびグループメンバーは、アプリケーションとデスクトップにアクセスするときに、StoreFront または Citrix Workspace アプリで資格情報（スマートカード、またはユーザー名とパスワードなど）による認証を求められます。デリバリーグループにシングルセッションOS マシンが含まれる場合、後にそのデリバリーグループを編集することでユーザーデータ（ユーザーの一覧）をインポートできます。
- 認証が不要なユーザー（匿名ユーザー）: マルチセッション OS マシンを含むデリバリーグループでは、StoreFront または Citrix Workspace アプリでの認証が不要な匿名アクセスを許可できます。たとえば、キオスクのアプリケーションでは資格情報を必須にして、Citrix アクセスポータルやツールでは不要にできます。最初の Delivery Controller をインストールすると、匿名のユーザーグループが作成されます。

  認証が不要なユーザーのアクセスを許可するには、デリバリーグループの各マシンにマルチセッション OS VDA がインストールされている必要があります。認証が不要なユーザーのアクセスを有効にする場合は、認証が不要な StoreFront ストアを作成しておく必要があります。

  認証が不要なユーザーアカウントはセッション開始時にオンデマンドで作成され、AnonXYZ（XYZ は一意の 3 桁の値）という名前が付けられます。

  認証が不要なユーザーセッションにはデフォルトで 10 分のアイドルタイムアウトが設定され、セッションを切断すると自動的にログオフされます。切断セッションへの再接続、デバイス間のローミング、およびワークスペースコントロールはサポートされません。

次の表に、［ユーザー］ページでの選択肢を示します：

アクセスを許可するユーザー	ユーザーおよびユーザーグループを追加/割り当てるかどうか	［認証が不要な（匿名）ユーザーのアクセスを許可する］チェックボックスをオンにするかどうか
認証が必要なユーザーのみ	はい	いいえ
認証が不要なユーザーのみ	いいえ	はい
認証が必要なユーザーおよび認証が不要なユーザー	はい	はい

ユーザーまたはグループのアクセス制限

また、ユーザーまたはユーザーグループを許可リストに追加して、デリバリーグループの使用を制限することもできます。許可リストに登録されたユーザーのみがデリバリーグループのアプリとデスクトップにアクセスできます。また、［禁止リストを追加］をクリックしてユーザーやユーザーグループを禁止リストに追加することもできます。これにより、ユーザーは選択したデリバリーグループのアプリやデスクトップを使用できなくなります。禁止リストは、許可リスト内のユーザーをブロックするために使用された場合にのみ意味があります。

手順 **6**：アプリケーション

ヒント：

- パッケージアプリケーションを、シングルセッションの静的デリバリーグループおよびリモート *PC* アクセスのデリバリーグループに追加できます。これらのアプリケーションを含むパッケージは、ユーザーがデスクトップまたはリモート PC にサインインするたびに自動的にマウントされます。
- アプリケーションをデリバリーグループに追加すると、デフォルトで「アプリケーション」という名前のフォルダー内に表示されます。別のフォルダーを指定することもできます。詳しくは、「アプリケーション」を参照してください。
- アプリケーションのプロパティは、デリバリーグループへの追加時、または後で変更できます。詳しくは、「アプリケーション」を参照してください。
- アプリケーションの追加時に、そのフォルダー内に同じ名前のアプリケーションが既に存在する場合、追加するアプリケーションの名前を変更するよう指示するメッセージが表示されます。名前の変更を拒否すると、アプリケーションはサフィックス付きで追加され、そのアプリケーションフォルダー内で名前が一意になります。
- アプリケーションを複数のデリバリーグループに追加する場合、そのすべてのデリバリーグループのアプリケーションを見る権限を有していなければ、表示上の問題が発生する可能性があります。そのような問題が発生した場合は、より上位の権限を持つ管理者に相談するか、または自身の権限を拡張して、アプリケーションを追加したデリバリーグループをすべて含めるようにします。

- 同じ名前の 2 つのアプリケーションを同じユーザーに公開する場合は、［アプリケーション名（ユーザー用）］ボックスに別の名前を入力します。これを行わないと、Citrix Workspace アプリで同じ名前が 2 つ表示されます。

［追加］メニューを選択して、アプリケーションのソースを表示します。

- ［スタート］メニューから：選択したカタログのイメージから作成されたマシンで検出されたアプリケーション。このソースを選択すると、新たなページが開き、検出されたアプリケーションが一覧表示されるので、追加するアプリケーションを選択して ［**OK**］を選択します。
- 手動：展開またはネットワーク内の別の場所にあるアプリケーション。このソースを選択すると、新たなページが開くので、そのページで実行可能ファイルのパス、作業ディレクトリ、オプションのコマンドライン引数、管理者およびユーザー用の表示名を入力します。この情報を入力したら、［**OK**］を選択します。
- 既存：過去に展開に追加された、おそらく別のデリバリーグループのアプリケーション。このソースを選択すると、新たなページが開き、検出されたアプリケーションが一覧表示されるので、追加するアプリケーションを選択して ［**OK**］を選択します。
- アプリケーションパッケージ： App-V、MSIX、MSIX アプリのアタッチ、または FlexApp アプリケーションパッケージ内のアプリケーション。このソースを選択すると、［パッケージからアプリケーションの追加］ページが開きます。アプリケーションパッケージのソースを選択して、表示結果からグループに追加するアプリケーション、［**OK**］の順に選択します

  > 注:
  >
  > MSIX または MSIX アプリのアタッチアプリを公開するには、デリバリーグループの機能レベルが 2106 以降である必要があります。FlexApp アプリの場合、機能レベルは 2206 以降である必要があります。機能レベルの要件が満たされていない場合、［アプリケーションパッケージのソース］ドロップダウンリスト内の対応するオプションは選択不可になります。

- アプリケーショングループ：展開内に存在するアプリケーショングループ。

あるアプリケーションのソースまたはアプリケーションが選択できない、または無効な場合、そのアプリケーションは見ることができないか、選択できないかのどちらかです。たとえば、展開に追加されたアプリケーションがない場合、［既存］のソースを選択することはできません。アプリケーションが、選択したマシンカタログのマシン上でサポートされるセッションの種類との互換性を備えていない場合も同様です。

手順 **7**：**App Protection**

次の情報は、Citrix Virtual Apps and Desktops ドキュメントの「App Protection」の記事を補足するものです。Citrix DaaS 環境で App Protection を使用するには、次の詳細に注意して、記事内の一般的なガイダンスに従ってください。

- 有効な Citrix Cloud サブスクリプションと有効な App Protection の使用権が必要です。App Protection 機能を購入するには、Citrix の営業担当者にお問い合わせください。

- App Protection には XML 信頼が必要です。XML 信頼を有効にするには、［設定］**>**［**XML** 信頼を有効にする］に移動します。
- 画面キャプチャ防止機能について：
  - Windows と macOS では、保護されたコンテンツのウィンドウのみが空白になります。保護されたウィンドウが最小化されていない場合に、App Protection がアクティブになります。
  - Linux では、キャプチャ全体が空白になります。App Protection は、保護されたウィンドウが最小化されているかどうかに関係なくアクティブです。

手順 **8**：デスクトップ（またはデスクトップ割り当て規則）

このページのタイトルは、ウィザードの前半で選択したマシンカタログによって異なります：

- プールされたマシンを含むマシンカタログを選択した場合、このページのタイトルは ［デスクトップ］になります。
- 割り当て済みのマシンを含むマシンカタログを選択し、［配信の種類］ページで［デスクトップ］を指定した場合、このページのタイトルは「デスクトップ割り当て規則」になります。
- 割り当て済みのマシンを含むマシンカタログを選択し、［配信の種類］ページで［アプリケーション］を指定した場合、このページのタイトルは「アプリケーション」になります。

［**Add**］を選択します。ダイアログボックスで次の操作を実行します：

- ［表示名］フィールドと ［説明］フィールドに、Citrix Workspace アプリで表示する情報を入力します。
- デスクトップにタグ制約を追加するには、［このタグでマシンの起動を制限します:］を選択し、メニューからタグを選択します。
- ラジオボタンを使用すると、次のいずれかを行うことができます：
  - このデリバリーグループにアクセスするすべての人にデスクトップの使用を許可する。デリバリーグループのすべてのユーザーは、デスクトップを起動することができる（プールされたマシンがあるグループの場合）か、デスクトップを起動したときにマシンを割り当てられることができます（マシンが割り当てられているグループの場合）。
  - 許可リストにユーザーとユーザーグループを追加して、デスクトップの使用を制限します。許可リストに登録されているユーザーのみがデスクトップにアクセスできます。また、［禁止リストを追加］をクリックしてユーザーとユーザーグループを禁止リストに追加することもできます。これにより、ユーザーは選択したデリバリーグループのデスクトップを使用できなくなります。禁止リストは、許可リスト内のユーザーをブロックするために使用された場合にのみ意味があります。
- 割り当て済みのマシンがグループに含まれる場合、ユーザーあたりの最大デスクトップ数を指定します。1 以上の値を入力する必要があります。
- （プールされたマシンの）デスクトップ、または（割り当て済みのマシンに対する）デスクトップ割り当て規則を有効または無効にします。デスクトップを無効にすると、デスクトップ配信が停止します。デスクトップ割り当て規則を無効にすると、ユーザーへのデスクトップの自動割り当てが停止されます。
- ダイアログボックスの操作を終了したら、［**OK**］を選択します。

手順 **9**：ライセンス割り当て

デリバリーグループに使用させるライセンスを決定します。デフォルトでは、デリバリーグループでサイトのライセンスが使用されます。詳しくは、「マルチタイプのライセンス」を参照してください。

手順 **10**：ローカルホストキャッシュ設定

この設定は、電源管理されたシングルセッションのプールされたマシンを含むデリバリーグループにのみ表示されます。

デフォルトでは、ローカルホストキャッシュ（LHC）モードの場合、漏えいの危険があるため、これらのマシンは使用できません。デフォルトの動作を変更して、LHC モードのときに新しいユーザー接続で使用できるようにするには、［リソースを使用可能な状態に維持する］を選択します。

または、PowerShell コマンドを使用してデフォルトの動作を変更することもできます。詳しくは、「アプリケーションおよびデスクトップのサポート」を参照してください。

> 重要：
>
> 電源管理された、シングルセッションのプールされたマシンへのアクセスを有効にすると、以前のユーザーセッションからのデータと変更が後続のセッションに残る可能性があります。

手順 **11**：まとめ

デリバリーグループの名前を入力します。オプションで、Workspace アプリと［完全な構成］管理インターフェイスに表示される説明を入力することもできます。

概要の情報を確認し、［完了］を選択します。アプリケーションを 1 つも選択しなかった場合、または配信するデスクトップを 1 つも指定しなかった場合、続行するかどうかを確認するメッセージが表示されます。

追加情報

- デリバリーグループの管理
- アプリケーション

デリバリーグループの管理

June 12, 2024

はじめに

この記事では、管理コンソールでデリバリーグループを管理する手順について説明します。グループ作成時に指定した設定を変更できるほかに、デリバリーグループ作成時には使用できなかった設定を構成することも可能です。

手順は全般的な設定、ユーザー設定、マシン設定、セッション設定のカテゴリ別にまとめられています。タスクによっては複数のカテゴリに関係します。たとえば、「マシンへのユーザーの接続を禁止する」のタスクはマシン設定のカテゴリで説明されていますが、ユーザー設定のカテゴリにもかかわります。そのため、あるカテゴリで見つからないタスクがある場合は、関連するカテゴリを確認してください。

この他の記事にも関連情報が記載されています:

- 「アプリケーション」には、デリバリーグループでのアプリケーションの管理に関する情報が記載されています。
- デリバリーグループを管理するには、デリバリーグループ管理者の組み込みの役割権限が必要です。詳しくは、「委任管理」を参照してください。

一般

- グループの詳細の表示
- 配信方法の変更
- StoreFront アドレスの変更
- 機能レベルの変更
- リモート PC アクセスのデリバリーグループの管理
- デリバリーグループのライセンスの変更
- フォルダーを使用したデリバリーグループの整理
- App Protection の管理

グループの詳細の表示

1. 検索機能を使用して、特定のデリバリーグループを見つけます。手順については、「インスタンスの検索」を参照してください。
2. 検索結果から必要に応じてグループを選択します。
3. グループ列の説明については、次の表を参照してください。
4. このグループの詳細については、下部の詳細ペインのタブをクリックしてください。

列	説明
デリバリーグループ	グループ名とセッションの種類。セッションの種類には、シングルセッション OS とマルチセッション OS があります。

列	説明
配信	このグループから配信されるリソースの種類。設定可能な値には、アプリケーション、デスクトップ、およびアプリケーションとデスクトップが含まれます。デリバリーグループが専用マシンで構成されている場合、「静的マシン割り当て」が表示されます。
使用中のセッション	セットアップされているマシンの数と、切断状態にあるマシンの数。
割り当て済み（個）	デリバリーグループに割り当てられたカタログ内のマシンの数。
フォルダー	デリバリーグループツリー内のグループの場所。グループが含まれているフォルダーの名前（末尾のバックスラッシュを含む）、またはグループがルートレベルにある場合は–が表示されます。

デリバリーグループの配信の種類の変更

配信の種類は、アプリケーション、デスクトップ、またはその両方のうち、そのグループが配信できるものを示します。

この種類を ［アプリケーション］から ［デスクトップ］に変更する前に、グループからすべてのアプリケーションを削除します。

1. ［管理］**>**［完全な構成］の左側ペインで ［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［編集］を選択します。
3. ［配信の種類］ページで、配信の種類を選択します。
4. ［適用］を選択して、ウィンドウを閉じずに行った変更を適用します。または、［**OK**］を選択し、変更を適用してウィンドウを閉じます。

StoreFront アドレスの変更

1. ［管理］**>**［完全な構成］の左側ペインで ［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［編集］を選択します。
3. ［**StoreFront**］ページで、後で StoreFront サーバーアドレスを指定するか（［手動］）、［新規追加］を選択して使用予定の StoreFront サーバーを指定するか（［自動］）を指定します。
4. ［適用］を選択して、ウィンドウを閉じずに行った変更を適用します。または、［**OK**］を選択し、変更を適用してウィンドウを閉じます。

StoreFront サーバーのアドレスは、後で指定することもできます。これを行うには、コンソールの左側ペインで［**StoreFront**］を選択します。

機能レベルの変更

デリバリーグループの機能レベルの変更は、マシン上の VDA、およびデリバリーグループで使用されているマシンを含むマシンカタログをアップグレードしてから行ってください。

以下の点に注意してください：

- Citrix Provisioning（旧称 Provisioning Services）を使用している場合は、Citrix Provisioning コンソールで VDA をアップグレードします。
- アップグレードした VDA がインストールされているマシンを起動して、Citrix DaaS に登録できるようにします。これによって、デリバリーグループで変更が必要なものがコンソールで特定されます。
- VDA をアップグレードせずに使用を継続すると、新しい製品機能を使用できなくなる場合があります。詳しくは、アップグレードのドキュメントを参照してください。

デリバリーグループの機能レベルを変更するには：

1. ［管理］**>**［完全な構成］の左側ペインで ［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［機能レベルの変更］を選択します。［機能レベルの変更］アクションは、アップグレードされた VDA が検出された場合にのみ表示されます。

ディスプレイには、機能レベルに変更できないマシンがある場合、そのマシンとその理由が表示されます。その後、変更アクションをキャンセルし、マシンの問題を解決してから変更アクションを再度実行できます。

変更が完了したら、マシンを以前の状態に戻すことができます。デリバリーグループを選択して、操作バーの ［機能レベルの変更を元に戻す］を選択します。

リモート **PC** アクセスのデリバリーグループの管理

リモート PC アクセス用のマシンカタログでユーザーに割り当てられていないマシンは、そのカタログに関連付けられたデリバリーグループに一時的に割り当てられます。この一時的な割り当てにより、そのマシンを後でユーザーに割り当てられるようになります。

デリバリーグループとマシンカタログとの関連付けには優先度値があります。この優先度により、マシンをシステムに登録したりユーザーにマシンを割り当てたりするときのデリバリーグループが決定されます：値が小さければ小さいほど、優先度は高くなります。リモート PC アクセスマシンカタログに複数のデリバリーグループ割り当てがある場合、優先度が最も高い割り当てが選択されます。この優先度値は設定するには PowerShell SDK を使用します。

リモート PC アクセス用のマシンカタログの初回作成時に、デリバリーグループが関連付けられます。この関連付けは、カタログに後から追加したマシンアカウントまたは組織単位を、このデリバリーグループに追加できるということを意味します。この関連付けは、必要に応じて有効にしたり無効にしたりできます。

リモート PC アクセスマシンカタログとデリバリーグループとの関連付けを追加または削除するには：

1. ［管理］**>**［完全な構成］の左側ペインで ［デリバリーグループ］を選択します。
2. リモート PC アクセスのグループを選択します。
3. ［詳細］セクションで ［マシンカタログ］タブを選択し、リモート PC アクセス用のカタログを選択します。
4. 関連付けを追加または復元するには、［デスクトップの追加］を選択します。関連付けを削除するには、［関連付けの削除］を選択します。

デリバリーグループのライセンスの変更

デリバリーグループのライセンス使用権を変更するには、次の手順に従います:

1. ナビゲーションペインで ［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［編集］をクリックします。
3. ［ライセンス割り当て］ページで、グループで使用するライセンスを選択します。
4. ［適用］をクリックして、ウィンドウを閉じずに行った変更を適用します。または、［保存］をクリックして、変更を適用してウィンドウを閉じます。

デリバリーグループレベルの使用権について詳しくは、「マルチタイプのライセンス」を参照してください。

フォルダーを使用したデリバリーグループの整理

簡単にアクセスできるように、フォルダーを作成してデリバリーグループを整理できます。

必須の役割　デフォルトでは、デリバリーグループフォルダーを作成および管理するには、次の組み込みの役割が必要です: クラウド管理者、完全な管理者、またはデリバリーグループ管理者。必要に応じて、デリバリーグループフォルダーを作成および管理するための役割をカスタマイズできます。詳しくは、「必要な権限」を参照してください。

デリバリーグループフォルダーの作成　開始する前に、デリバリーグループを整理する方法を計画します。以下に注意してください:

- 最大で 5 レベルまでの階層構造でフォルダーをネストできます（デフォルトのルートフォルダーを除く）。
- フォルダーには、デリバリーグループとサブフォルダーを含めることができます。
- バックエンドのフォルダーツリーは、［完全な構成］のすべてのノード（［マシンカタログ］や ［アプリケーション］、および ［デリバリーグループ］ノードなど）で共有されます。フォルダーの名前変更や移動時に他のノードと名前が競合しないように、異なるノードの第 1 レベルのフォルダーには異なる名前を付けることをお勧めします。

デリバリーグループフォルダーを作成するには、次の手順に従います:

1. ［管理］**>**［完全な構成］の左側ペインで ［デリバリーグループ］を選択します。

2. フォルダー階層でフォルダーを選択し、［アクション］バーで ［フォルダーの作成］を選択します。
3. 新しいフォルダーの名前を入力し、［完了］をクリックします。

> ヒント：
>
> 意図しない場所にフォルダーを作成した場合は、それを正しい場所にドラッグできます。

デリバリーグループの移動

デリバリーグループはフォルダー間で移動できます。詳細な手順は次のとおりです：

1. ［管理］**>**［完全な構成］の左側ペインで ［デリバリーグループ］を選択します。
2. フォルダー別にグループを表示します。フォルダー階層の上にある ［すべて表示］をオンにして、一度にすべてのグループを表示することもできます。
3. グループを右クリックしてから、［デリバリーグループの移動］を選択します。
4. グループの移動先のフォルダーを選択し、［完了］をクリックします。

> ヒント：
>
> グループはフォルダーにドラッグできます。

デリバリーグループフォルダーの管理

デリバリーグループフォルダーの削除、名前変更、および移動を行うことができます。

フォルダーの削除は、フォルダーとそのサブフォルダーにデリバリーグループが含まれていない場合にだけ可能となりますのでご注意ください。

フォルダーを管理するには、次の手順に従います：

1. ［管理］**>**［完全な構成］の左側ペインで ［デリバリーグループ］を選択します。
2. フォルダー階層でフォルダーを選択し、必要に応じて ［アクション］バーでアクションを選択します：
   - フォルダーの名前を変更するには、［フォルダーの名前変更］を選択します。
   - フォルダーを削除するには、［フォルダーの削除］を選択します。
   - フォルダーを移動するには、［フォルダーの移動］を選択します。
3. 画面の指示に従って、残りの手順を完了します。

必要な権限　次の表に、デリバリーグループフォルダーでアクションを実行するために必要な権限を示します。

アクション	必要な権限
デリバリーグループフォルダーの作成	デリバリーグループフォルダーの作成
デリバリーグループフォルダーの削除	デリバリーグループフォルダーの削除
デリバリーグループフォルダーの移動	デリバリーグループフォルダーの移動
デリバリーグループフォルダー名の変更	デリバリーグループフォルダーの編集
デリバリーグループのフォルダーへの移動	デリバリーグループフォルダーの編集およびデリバリーグループプロパティの編集

App Protection の管理

次の情報は、Citrix Virtual Apps and Desktops ドキュメントの「App Protection」の記事を補足するものです。Citrix DaaS 環境で App Protection を使用するには、次の詳細に注意して、記事内の一般的なガイダンスに従ってください。

1. ［管理］**>**［完全な構成］の左側ペインで ［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［編集］を選択します。
3. ［**App Protection**］ページで、［キーロガー対策］と ［画面キャプチャ防止］を有効にできます。

- 有効な Citrix Cloud サブスクリプションと有効な App Protection の使用権が必要です。App Protection 機能を購入するには、Citrix の営業担当者にお問い合わせください。
- App Protection には XML 信頼が必要です。XML 信頼を有効にするには、［設定］**>**［**XML** 信頼を有効にする］に移動します。
- 画面キャプチャ防止機能について：
  - Windows と macOS では、保護されたコンテンツのウィンドウのみが空白になります。保護されたウィンドウが最小化されていない場合に、App Protection がアクティブになります。
  - Linux では、キャプチャ全体が空白になります。App Protection は、保護されたウィンドウが最小化されているかどうかに関係なくアクティブです。

ユーザー

> 注：
>
> ［ユーザー管理を **Citrix Cloud** に任せる］オプションは削除されました。ユーザー管理を **Citrix Cloud** に任せるに設定されている既存のデリバリーグループのユーザー割り当てを管理するには、Citrix Cloud ライブラリまたは完全な構成の 2 つのオプションがあります。完全な構成アプローチについて詳しくは、「Citrix Cloud ライブラリ管理のデリバリーグループのユーザー割り当てを管理」を参照してください。

このトピックでは以下のセクションについて説明します。

- ユーザー設定の変更
- ユーザーの追加と削除
- Citrix Cloud ライブラリ管理のデリバリーグループのユーザー割り当てを管理

デリバリーグループのユーザー設定を変更する

このページの名前には、［ユーザー設定］または ［基本設定］のどちらかが表示されます。

1. ［管理］**>**［完全な構成］の左側ペインで ［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［編集］を選択します。
3. ［ユーザー設定］ページで、次の表のいずれかの設定を変更します。
4. ［適用］を選択して、ウィンドウを閉じずに行った変更を適用します。または、［**OK**］を選択し、変更を適用してウィンドウを閉じます。

設定	説明
説明	Citrix Workspace（または StoreFront）でユーザーに表示される説明です。
デリバリーグループの有効化	このデリバリーグループを有効にするかどうかを設定します。
タイムゾーン	このデリバリーグループのマシンが存在する必要があるタイムゾーン。このオプションにより、サイトでサポートされているタイムゾーンが一覧表示されます。注：デリバリーグループのタイムゾーンを変更すると、そのデリバリーグループ内のマシンが再起動される場合があります。これを回避するには、必ず運用時間外にタイムゾーン設定を変更してください。
SecureICA の有効化	デリバリーグループのマシンとの通信を、ICA プロトコルを暗号化する SecureICA を使用してセキュリティで保護します。デフォルトレベルは 128 ビットです。レベルは SDK を使用して変更できます。パブリックネットワークが使用される環境では、TLS などの暗号化方法を追加することを Citrix ではお勧めします。また、SecureICA では、メッセージの整合性チェックが行われません。
ユーザーごとの最大デスクトップ数	ユーザーが持てるデスクトップの数。

デリバリーグループのユーザーを追加または削除する

ユーザーについて詳しくは、「ユーザー」を参照してください。

1. ［管理］**>**［完全な構成］の左側ペインで ［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［デリバリーグループの編集］を選択します。
3. ユーザーページで以下の手順を実行します：
   - ユーザーを追加するには、［追加］を選択し、追加するユーザーを指定します。
   - ユーザーを削除する場合は、1 人または複数のユーザーを選択し、［削除］を選択します。
   - 認証されていないユーザーによるアクセスを許可するかどうかを設定するチェックボックスを、オンまたはオフにします。
4. ［適用］を選択して、ウィンドウを閉じずに行った変更を適用します。または、［**OK**］を選択し、変更を適用してウィンドウを閉じます。

ユーザー割り当ての管理　ユーザー割り当てを管理するには：

1. ［管理］**>**［完全な構成］で、［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［編集］を選択します。
3. ［マシンの割り当て］ページで、ユーザーを追加または削除します。ユーザーを追加するには、ユーザーを参照するか、ユーザー名をセミコロンで区切って入力します。

ユーザー名を入力するときは、次の点を考慮してください：

- ユーザーが Active Directory にいる場合は、名前を直接入力します。そうでない場合は、次の形式で名前を入力します：`<identity provider>:<user name>`。例：`AzureAD:username`。

Citrix Cloud ライブラリ管理のデリバリーグループのユーザー割り当てを管理

Citrix Cloud ライブラリ管理のデリバリーグループのユーザー割り当てを管理するには、Citrix Cloud ライブラリまたは完全な構成を使用します。

完全な構成を使用してこのタスクを実行するには、次の手順に従います：

1. ［管理］**>**［完全な構成］の左側ペインで ［デリバリーグループ］を選択します。
2. Citrix Cloud 管理のデリバリーグループを選択して、操作バーで ［編集］を選択します。
3. デスクトップの使用を特定のユーザーに制限するには、次の手順に従います：
   a) ［デスクトップ］または ［デスクトップ割り当て規則］ページでデスクトップを選択し、［編集］をクリックします。［デスクトップの使用を制限する］オプションが選択された状態で ［デスクトップの編集］ページが表示されます。
   b) ［追加］をクリックし、必要に応じて 1 人以上のユーザーを選択してから ［完了］をクリックします。

c) ［**OK**］をクリックします。

4. このグループ内のアプリケーションの使用を特定のユーザーに制限するには、左側のペインで ［アプリケーション割り当て規則］をクリックし、手順 3 の説明と同様の手順に従ってユーザーを追加します。

マシン

- ユーザーへのマシン割り当ての変更
- プールされたシングルセッション VDA に対してローカルホストキャッシュ（LHC）を有効にする
- マシンの更新
- デスクトップのタグ制約の追加、変更、または削除
- マシンの削除
- リソースへのアクセスを制限
- マシンへのユーザーの接続を禁止する（メンテナンスモード）
- マシンのシャットダウンと再起動
- マシンに対する再起動スケジュールの作成と管理
- マシンの負荷管理
- Autoscale の管理

この記事で説明されている機能の他に、マシンのプロアクティブな電源管理については、「Autoscale」を参照してください。

デリバリーグループのユーザーへのマシン割り当ての変更

MCS でプロビジョニングされたシングルセッションOS マシンの割り当てを変更することができます。マルチセッション OS マシンや、Citrix Provisioning でプロビジョニングされたマシンの割り当てを変更することはできません。

1. ［管理］**>** ［完全な構成］の左側ペインで ［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［編集］を選択します。
3. ［マシン割り当て］ページで、新しいユーザーを指定します。
4. ［適用］を選択して、ウィンドウを閉じずに行った変更を適用します。または、［**OK**］を選択し、変更を適用してウィンドウを閉じます。

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

デフォルトでは、電源管理されたシングルセッションのプールされたマシンは、ローカルホストキャッシュモードでは使用できません。デフォルトの動作は、デリバリーグループごとに上書きできます。詳細な手順は次のとおりです:

1. ［管理］**>**［完全な構成］の左側ペインで ［デリバリーグループ］を選択します。

   グループ一覧では、MCS または Citrix Provisioning によってプロビジョニングされた、シングルセッションのプールされたマシンを含むグループには警告アイコンが表示されます。

2. 必要に応じてグループを選択して、操作バーの ［編集］を選択します。
3. ［ローカルホストキャッシュ］ページで、［リソースを使用可能な状態に維持する］を選択します。
4. ［適用］を選択して、ウィンドウを閉じずに行った変更を適用します。または、［**OK**］を選択し、変更を適用してウィンドウを閉じます。

または、PowerShell コマンドを使用してデフォルトの動作を上書きすることもできます。詳しくは、「アプリケーションおよびデスクトップのサポート」を参照してください。

> 重要：
>
> 電源管理された、シングルセッションのプールされたマシンへのアクセスを有効にすると、以前のユーザーセッションからのデータと変更が後続のセッションに残る可能性があります。

デリバリーグループのマシンの更新

1. ［管理］**>**［完全な構成］の左側ペインで ［デリバリーグループ］を選択します。
2. グループを選択し、操作バーの ［マシンの表示］を選択します。
3. マシンを選択して、操作バーの ［マシンの更新］を選択します。

別のイメージを選択するには、［イメージ］を選択し、スナップショットを選択します。

変更内容を適用し、マシンのユーザーに通知するには、［エンドユーザーへのロールアウト通知］を選択します。次に、以下を指定します：

- イメージを更新するタイミング：今すぐ、または次の起動時
- 再起動分散時間（グループ内のすべてのマシンの更新を開始する合計時間）
- ユーザーに再起動を通知するかどうか
- ユーザーが受け取るメッセージ

デスクトップのタグ制約の追加、変更、または削除

タグによる制限を追加、変更、および削除すると、どのデスクトップが起動の対象となるかについて、予期しない結果を招くことがあります。「タグ」に記載されている考慮事項と注意を確認してください。

1. ［管理］**>**［完全な構成］の左側ペインで ［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［編集］を選択します。
3. ［デスクトップ］ページでデスクトップを選択し、［編集］を選択します。
4. タグによる制限を追加するには、［タグでマシンの起動を制限します］をオンにし、タグを選択します。

5. タグ制限を変更または削除するには、次のいずれかを行います：

    - 別のタグを選択する。
    - ［タグでマシンの起動を制限します］をオフにしてタグによる制限を削除する。

6. ［適用］を選択して、ウィンドウを閉じずに行った変更を適用します。または、［**OK**］を選択し、変更を適用してウィンドウを閉じます。

デリバリーグループからのマシンの削除

マシンを削除すると、そのマシンはデリバリーグループから削除されます。この場合でも、マシンはそのデリバリーグループで使用するマシンカタログからは削除されません。このため、そのマシンをほかのデリバリーグループに割り当てることができます。

マシンを削除する前に、マシンをシャットダウンする必要があります。デリバリーグループから削除せずにマシンを一時的に使用できなくする場合は、そのマシンをメンテナンスモードにしてからシャットダウンしてください。

マシンには個人データが保存されている可能性があるため、そのマシンを別のユーザーに割り当てる場合は注意が必要です。マシンをイメージから再作成することを検討してください。

1. ［管理］**>**［完全な構成］の左側ペインで ［デリバリーグループ］を選択します。
2. グループを選択し、操作バーの ［マシンの表示］を選択します。
3. マシンがシャットダウン状態であることを確認します。
4. マシンを選択し、操作バーの ［デリバリーグループから削除］を選択します。

マシンが使用する接続からも、デリバリーグループからマシンを削除できます。

デリバリーグループ内のリソースへのアクセスを制限

デリバリーグループでリソースへのアクセス制限を変更した場合、使用する方法にかかわらず既存の設定より優先されます。次の操作を実行できます：

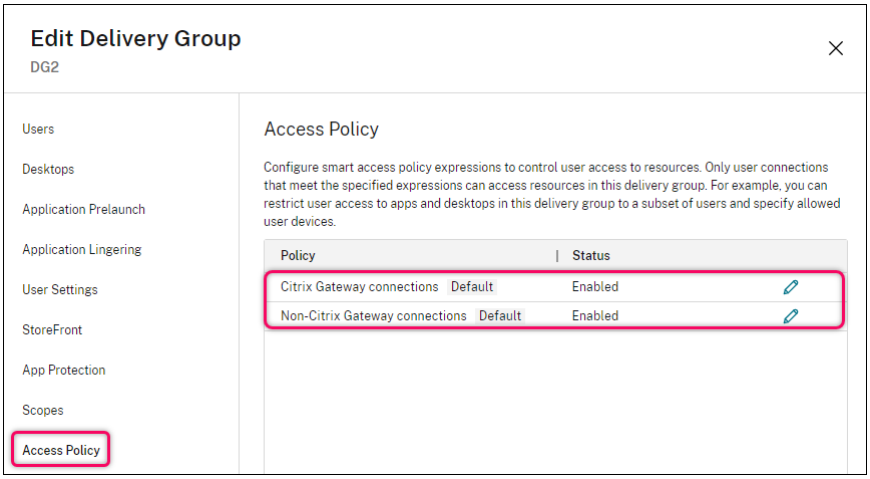
- 管理者のアクセスを制限する場合は、委任管理スコープを使用します：すべてのアプリケーションへのアクセスを許可するスコープや、特定のアプリケーションへのアクセスのみを許可するスコープを作成して管理者に割り当てることができます。詳しくは、「委任管理」を参照してください。
- スマートアクセスポリシー式を使用してユーザーのアクセスを制限します：アクセスポリシー規則を構成して、特定のデリバリーグループへのユーザーアクセスを制御できます。以下に例を示します：
    - ユーザーのサブセットのアクセスを制限し、許可されたユーザーデバイスを指定できます。
    - （StoreFront ではなく）Workspace 経由で接続しているユーザーへのアクセスを制限します。
    - 特定の Workspace URL 経由で接続しているユーザーへのアクセスを制限します。

このセクションでは、アクセスポリシー規則を使用してデリバリーグループへのユーザーアクセスを制限する方法について説明します：

- アクセスポリシー規則について
- アクセスポリシー規則の追加
- 完全な構成を使用したアクセスポリシー規則の管理
- PowerShell を使用したポリシー規則の追加および調整

アクセスポリシー規則について　デリバリーグループに対して複数のアクセスポリシー規則を設定できます。デリバリーグループ内のアプリとデスクトップは、ユーザーの接続がデリバリーグループに対して定義したアクセスポリシー規則と一致すると、順不同でユーザーの StoreFront または Workspace に表示されます。

各規則は個別に有効または無効にすることができます。無効な規則は、アクセスポリシーの評価時に無視されます。



完全な構成では、アクセスポリシー一覧に次のデフォルトの SmartAccess ポリシー規則が含まれます。必要に応じてさらに追加できます。

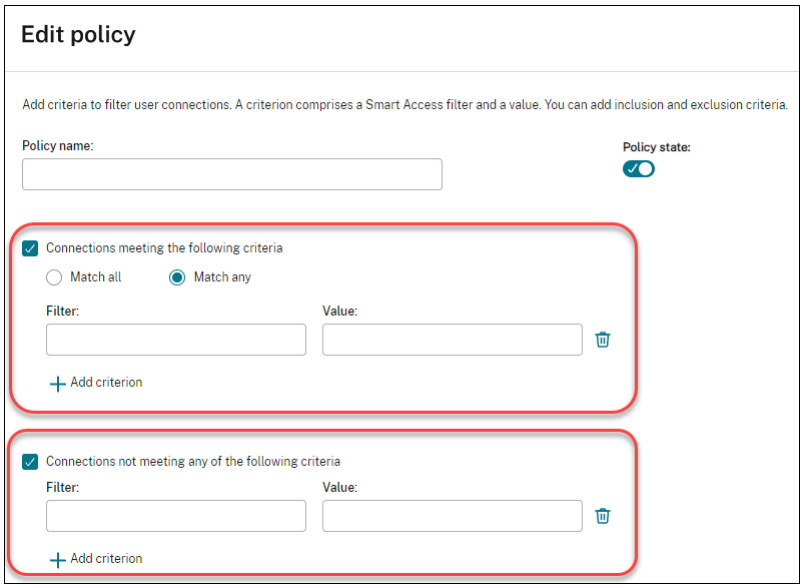
- **Citrix Gateway** 接続。このポリシーでは、Citrix Gateway 経由で行われたユーザー接続のみがデリバリーグループ内のリソースにアクセスできるようにします。デバイスポスチャ機能またはネットワークの場所機能が有効になっている場合に Workspace を介して行われたユーザー接続も、Citrix Gateway 経由の接続とみなされます。
- **Citrix Gateway** 以外の接続。このポリシーでは、Citrix Gateway を経由しないユーザー接続のみがデリバリーグループ内のリソースにアクセスできるようにします。

> 注:
>
> - デフォルトの規則が新しく構成された規則を上書きしないようにするには、デフォルトの規則を無効にするか、デフォルトの規則を調整して、新しいポリシーで使用されるフィルターを除外する必要があります。
> - デフォルトのポリシーは削除できませんが、無効にすることはできます。ポリシーを無効にするには、編集アイコンをクリックし、［ポリシーの状態］を ［無効］に変更します。
> - ポリシー一覧には、PowerShell コマンドを使用して追加された規則も表示されます。これらのポリシーは削除できますが、［完全な構成］では編集できません。

完全な構成を使用したアクセスポリシー規則の追加　アクセスポリシー規則は一連のフィルターで構成されています。フィルターについて詳しくは、こちらの記事を参照してください。アクセスポリシー規則を追加するときに、必要に応じて複数の条件フィルターを規則に追加します。

完全な構成を使用してデリバリーグループのポリシーを追加するには、次の手順を実行します:

1. ［管理］**>**［完全な構成］の左側ペインで ［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［編集］をクリックします。
3. ［アクセスポリシー］ページで、［追加］をクリックします。［ポリシーの追加］ページが開きます。



4. ［ポリシー名］フィールドに、ポリシーのわかりやすい名前を入力します。名前は展開内で一意である必要があります。
5. 許可されるユーザー接続の基準を定義するには、次の手順を実行します:

   a) ［次の条件に一致する接続］を選択します。

   b) ［条件の追加］をクリックします。

   c) ［フィルター］フィールドに、使用するフィルターの名前を入力します。［値］フィールドで、フィルターに必要な値を入力します。たとえば、（StoreFront ではなく）Workspace 経由で接続したユーザーのみがこのデリバリーグループ内のリソースにアクセスできるようにするには、［フィルター］に`Citrix-Via-Workspace`、［値］に`True`を入力します。

   d) さらに条件を追加するには、手順 b から c を繰り返します。

   e) 条件間の関係を選択します:

      - 一部が一致。受信ユーザー接続が構成されたフィルター基準のいずれかを満たしている場合にのみ、アクセスを許可します。
      - すべて一致。受信ユーザー接続が構成されたフィルター基準をすべて満たす場合にのみ、アクセスを許可します。

6. 禁止されるユーザー接続の条件を定義するには、次の手順を実行します:

   a) ［次の条件のいずれにも一致しない接続］を選択します。

   b) ［条件の追加］をクリックします。

   c) ［フィルター］フィールドに、使用するフィルターの名前を入力します。［値］フィールドで、フィルターに必要な値を入力します。たとえば、`example.cloud.com`Workspace URL 経由で接続しているユーザーがこのデリバリーグループ内のリソースにアクセスすることを禁止します。［フィルター］に`Citrix.Workspace.UsingDomain`を入力し、［値］に`example.cloud.com`を入力します。

   d) さらに条件を追加するには、手順 b から c を繰り返します。

   > 注:
   >
   > 構成された条件のいずれかを満たすユーザー接続は、このデリバリーグループ内のリソースへのアクセスが禁止されます。

7. ［完了］をクリックします。

   新しいポリシーがポリシー一覧に表示されます。

8. この新しいポリシーの対象となる接続との意図しない重複を避けるため、デフォルトのポリシー 規則を確認して調整します。既存のポリシーを調整するには、次の方法を使用します:

   - デフォルトのポリシー規則を無効にします。
   - 新しいポリシーの包含基準に追加した SmartAccess フィルターを除外するように、デフォルトのポリシー規則を構成します。詳しくは、「完全な構成を使用したポリシー規則の管理」および「PowerShell を使用したアクセスポリシー規則の追加および管理」を参照してください。

   > 重要:
   >
   > 「アクセスポリシー規則について」で説明されているように、ユーザーの接続がデリバリーグループ内の 1 つ以上のポリシー規則に一致すると、ユーザーはそのリソースにアクセスできます。したがって、規則を作成した後、既存の規則を慎重に確認して調整し、新しい規則の対象となる接続との意図しない重複を避ける必要があります。

完全な構成を使用したアクセスポリシー規則の管理　包含基準と除外基準を使用して、デフォルトのポリシーを調整できます。たとえば、これらの接続のサブセットのアクセスを制限するには、次の手順を実行します:

1. デフォルトのポリシーを編集します。
2. ［次の条件のいずれかに一致する接続］を選択します。
3. 接続を許可するユーザーを特定する SmartAccess ポリシー式を追加、編集、または削除します。

詳しくは、Citrix Gateway のドキュメントを参照してください。

PowerShell を使用したアクセスポリシー規則の追加および管理　次の PowerShell コマンドレットを使用して、デリバリー グループのアクセスポリシー規則を追加および管理できます:

- New-BrokerAccessPolicyRule
- Get-BrokerAccessPolicyRule
- Set-BrokerAccessPolicyRule
- Rename-BrokerAccessPolicyRule
- Remove-BrokerAccessPolicyRule

詳しくは、Citrix 開発者向けドキュメントの関連する記事を参照してください。

デリバリーグループのマシンへのユーザーの接続を禁止する（メンテナンスモード）

一時的に新しい接続を停止する必要がある場合は、デリバリーグループの 1 台またはすべてのマシンに対してメンテナンスモードを有効にすることができます。パッチを適用したりメンテナンスツールを使用したりする場合は、メンテナンスモードを有効にしてから実行することをお勧めします。

- メンテナンスモードのマルチセッション OS マシンでは、既存のセッションに接続することはできますが、新しいセッションを開始することはできません。
- メンテナンスモードのシングルセッションOS マシン（またはリモート PC アクセスを使用している PC）では、新しいセッションを開始することも既存のセッションに再接続することもできません。実行中の接続は、ユーザーが切断またはログオフするまでは保持されます。

メンテナンスモードをオンまたはオフにするには、次の手順に従います。

1. ［管理］**>**［完全な構成］の左側ペインで ［デリバリーグループ］を選択します。
2. グループを選択します。
3. デリバリーグループのすべてのマシンをメンテナンスモードにするには、操作バーの ［メンテナンスモードをオンにする］を選択します。

   1 つのマシンをメンテナンスモードにするには、操作バーの ［マシンの表示］を選択します。マシンを選択し、操作バーの ［メンテナンスモードをオンにする］を選択します。
4. 特定のマシンまたはデリバリーグループのすべてのマシンのメンテナンスモードを解除するには、上記の手順に従って、操作バーで ［メンテナンスモードをオフにする］を選択します。

Windows リモートデスクトップ接続（RDC）の設定も、マルチセッション OS マシンをメンテナンスモードにするかどうかに影響します。次の状態のいずれかが発生すると、サーバーがメンテナンスモードになります:

- 上記の手順で［メンテナンスモードをオンにする］が選択された。
- RDC が ［このコンピューターへの接続を許可しない］に設定された。
- RDC が ［このコンピューターへの接続を許可しない］に設定されておらず、リモートホスト構成のユーザーログオンモード設定が ［再接続を許可するが、新しいログオンを許可しない］または ［再接続を許可するが、サーバーが再起動するまで新しいログオンを許可しない］に設定されている。

次のものについて、メンテナンスモードのオン/オフを切り替えることもできます:

- 接続。この接続を使用するマシンに影響が及びます。
- マシンカタログ。このカタログ内のマシンに影響が及びます。

デリバリーグループのマシンのシャットダウンと再起動

ここで説明する内容は、リモート PC アクセスマシンではサポートされません。

1. ［管理］**>**［完全な構成］の左側ペインで ［デリバリーグループ］を選択します。
2. グループを選択し、操作バーの ［マシンの表示］を選択します。
3. マシンを選択してから、アクションバーで次のアクションのいずれかを選択します:

   > 注:
   >
   > - 次のアクションは、電源管理されているマシンにのみ適用されます。
   > - マシンの状態によっては、一部のオプションを使用できない場合があります。

   - 強制シャットダウン：マシンの電源を強制的に切って、マシン一覧を更新します。
   - 再起動：オペレーティングシステムに再起動を要求します。オペレーティングシステムで再起動を実行できない場合、マシンの状態は変更されません。
   - 強制再起動：オペレーティングシステムを強制的にシャットダウンしてから、マシンを再起動します。
   - 一時停止：マシンをシャットダウンすることなく一時的に停止して、マシン一覧を更新します。
   - シャットダウン：オペレーティングシステムにシャットダウンを要求します。

非強制操作の場合、マシンが 10 分以内にシャットダウンしないと、電源が切れ、強制的にシャットダウンされます。シャットダウン中に Windows が更新のインストールを開始すると、更新が完了する前にマシンの電源が切れる危険性があります。

デリバリーグループのマシンに対する再起動スケジュールの作成と管理

> 注:
>
> - Autoscale が有効になっているデリバリーグループに再起動スケジュールが適用されると、そのマシンの電源がオフになり、Autoscale が電源をオンにするまでそのままです。
> - 再起動スケジュールがランダムにシングルセッションマシンに適用される場合、コストを節約する場合に、それらのマシンは再起動されるのではなく電源がオフになります。Autoscale を使用してマシンの電源をオンにすることをお勧めします。
> - デリバリーグループのタイムゾーンを変更すると、そのデリバリーグループ内のマシンが再起動される場合があります。これを回避するには、必ず運用時間外にタイムゾーン設定を変更してください。

再起動のスケジュールにより、デリバリーグループ内のマシンを定期的に再起動するタイミングが指定されます。1 つのデリバリーグループに対して、1 つ以上のスケジュールを作成できます。スケジュールは次のいずれかに影響します:

- グループ内のすべてのマシン。
- グループ内の 1 つ以上のマシン（すべてではない）。マシンは、マシンに適用するタグで識別されます。これは、タグによって、タグがあるアイテム（この場合はマシン）のみにアクションが制限されるため、「タグ制限」と呼ばれます。

たとえば、すべてのマシンが 1 つのデリバリーグループに属しているとします。すべてのマシンを毎週 1 回再起動し、経理チームが使用するマシンを毎日再起動するとします。これを実現するには、すべてのマシンに対して 1 つのスケジュールを設定し、経理チームのマシンのみ別途スケジュールを設定します。

スケジュールには、再起動が開始される日時と期間が含まれます。期間は、「影響を受けるすべてのマシンを同時に起動する」か、影響を受けるすべてのマシンを再起動するのに必要な間隔のいずれかです。

スケジュールは有効または無効にできます。テストのときや、特別な間隔のとき、必要になる前にスケジュールを準備するときは、スケジュールを無効にすると役立ちます。

スケジュールは、管理コンソールからの自動パワーオンまたはシャットダウンには使用できません。再起動の場合にのみ使用できます。

スケジュールの重複　複数のスケジュールを重複させることができます。上記の例では、両方のスケジュールが経理チームのマシンに影響します。これらのマシンは、日曜日に 2 回再起動される可能性があります。スケジュールコードは、同じマシンを意図した回数より多く再起動しないよう設計されていますが、保証はされません。

- スケジュールで開始時刻と処理時間が正確に一致する場合、マシンが一度のみ再起動される可能性は高くなります。
- スケジュールの開始時間と期間が異なるほど、再起動が複数回発生する可能性が高くなります。
- スケジュールの影響を受けるマシンの数は、重複の可能性にも影響します。例では、すべてのマシンに影響がある週次スケジュールは、経理チームのマシンの日次スケジュールより速く再起動を開始する可能性があります（それぞれに指定された期間により異なる）。

再起動スケジュールについて詳しくは、「Reboot schedule internals」を参照してください。

再起動スケジュールの表示

1. ［管理］**>**［完全な構成］の左側ペインで ［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［編集］を選択します。
3. ［再起動スケジュール］ページを選択します。

［再起動スケジュール］ページには、構成された各スケジュールに関する次の情報が表示されます：

- スケジュール名。
- 使用されるタグ制限（ある場合）。
- マシンの再起動が発生する頻度。
- マシンのユーザーが通知を受信するかどうか。
- スケジュールが有効かどうか。テストのときや、特別な間隔のとき、必要になる前にスケジュールを準備するときは、スケジュールを無効にすると役立ちます。

タグの追加（適用）　タグ制限を使用する再起動スケジュールを構成する場合、そのスケジュールの影響を受けるマシンにタグが追加（適用）されていることを確認してください。上記の例では、経理チームによって使用されるそれぞれのマシンにタグが適用されます。詳しくは、「タグ」を参照してください。

1 つのマシンに複数のタグを適用することもできますが、再起動スケジュールでは 1 つのタグしか指定できません。

1. ［管理］**>**［完全な構成］の左側ペインで ［デリバリーグループ］を選択します。
2. スケジュールによって制御されるマシンを含むグループを選択します。
3. ［マシンの表示］を選択し、タグを追加するマシンを選択します。
4. 操作バーの ［タグの管理］を選択します。
5. タグが存在する場合は、タグ名の隣にあるチェックボックスをオンにします。タグが存在しない場合は、［作成］を選択し、タグの名前を指定します。タグが作成されたら、新しく作成したタグ名の隣にあるチェックボックスをオンにします。
6. ［タグの管理］ダイアログボックスの ［保存］を選択します。

再起動スケジュールの作成

1. ［管理］**>**［完全な構成］の左側ペインで ［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［編集］を選択します。
3. ［再起動スケジュール］ページで、［追加］を選択します。
4. ［再起動スケジュールの追加］ページで次の操作を行います：

    - スケジュールを有効にするには、［はい］を選択します。スケジュールを無効にするには、［いいえ］を選択します。
    - スケジュールの名前と説明を入力します。
    - ［タグに制限］では、タグの制限を適用します。
    - ［メンテナンスモードのマシンを含める］で、メンテナンスモードのマシンをこのスケジュールに含めるかどうかを選択します。代わりに PowerShell を使用する場合については、「メンテナンスモードのマシンのスケジュールされた再起動」を参照してください。
    - ［再起動の頻度］では、再起動の頻度を次の中から選択します：毎日、毎週、毎月、または一度だけ。［毎週］または ［毎月］を選択した場合は、1 つ以上の特定の曜日または日付を指定できます。
    - ［繰り返し間隔］には、スケジュールを実行する頻度を指定します。
    - ［開始日］には、スケジュールを設定する期間の最初の日を指定します。
    - ［再起動の開始］では、再起動の開始時刻を 24 時間形式で指定します。
    - ［再起動の間隔］の場合：
        - 自然な再起動を使用しない場合は、［すべてのマシンを同時に再起動する］または ［すべてのマシンを（一定期間内に）再起動する］を選択します。

- 自然な再起動を使用する場合は、［セッションのドレイン後にすべてのマシンを再起動する］を選択します。

  自然再起動を使用するように構成された再起動スケジュールを開始すると、次のようになります:

  * デリバリーグループに属するすべてのアイドル状態のマシンがすぐに再起動されます
  * 1 つまたは複数のアクティブなセッションがあるデリバリーに属する各マシンは、すべてのセッションがログオフされると再起動されます。

  > 注:
  >
  > このオプションは、電源管理されているマシンと、電源管理されていないマシンに使用できます。

- ［ユーザーへ通知を送信］で、再起動を開始する前に、該当するマシンに通知メッセージを表示するかどうかを選択します。デフォルトでは、メッセージは表示されません。
- 再起動開始の 15 分前にメッセージが表示されるように選択した場合、最初のメッセージの後、5 分ごとにメッセージが繰り返し送信されるように ［通知の頻度］で選択できます。デフォルトでは、メッセージは繰り返して送信はされません。
- 通知のタイトルと本文を入力します。デフォルトのテキストはありません。

  メッセージに再起動までのカウントダウンを含める場合は、変数 **%m%** を入れます。すべてのマシンを同時に再起動することを選択した場合を除き、メッセージは、再起動前の適切なタイミングで各マシンに表示されます。

5. ［完了］をクリックして変更を適用し、［再起動スケジュールの追加］ウィンドウを閉じます。
6. ［適用］をクリックすると、［デリバリー グループの編集］ウィンドウを開いたまま、変更が適用されます。または、［保存］をクリックして、変更を適用してウィンドウを閉じます。

再起動スケジュールの即時実行　再起動のスケジュールにより、デリバリーグループ内のマシンを定期的に再起動するタイミングが指定されます。再起動スケジュールをすぐに実行して、そのスケジュールでマシンを再起動することもできます。

再起動スケジュールをすぐに実行するには、次の手順を実行します:

1. ［管理］**>**［完全な構成］の左側ペインで ［デリバリーグループ］を選択します。
2. 該当するデリバリーグループを選択し、操作バーの ［編集］を選択します。
3. ［再起動スケジュール］ページで、実行するスケジュールを選択し、［今すぐスケジュールを実行］を選択します。

> 注:
>
> - ［セッションのドレイン後にすべてのマシンを再起動する］設定でスケジュールが構成されている場合、スケジュールをすぐに実行することはできません。
> - ［今すぐスケジュールを実行］のみ、一度に 1 つのスケジュールに適用できます。

> - スケジュールを編集すると、［今すぐスケジュールを実行］が使用できなくなります。［適用］を選択して、使用できるようにします。

再起動スケジュールの編集、削除、有効化、無効化

1. ［管理］**>**［完全な構成］の左側ペインで ［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［編集］を選択します。
3. ［再起動スケジュール］ページで、スケジュールのチェックボックスをオンにします。

    - スケジュールを編集するには、［編集］を選択します。スケジュール設定を更新します。更新の方法については、「再起動スケジュールの作成」を参照してください。
    - スケジュールを有効または無効にするには、［編集］を選択します。［再起動スケジュールを有効にする］チェックボックスを、オンまたはオフにします。
    - スケジュールを削除するには、［削除］を選択します。削除を確認します。スケジュールを削除しても、影響を受けるマシンに適用済みのタグには影響しません。

データベースの停止によるスケジュールされた再起動の遅延

> 注:
>
> この機能は、PowerShell のみで利用可能です。

デリバリーグループ内のマシン（VDA）に対してスケジュールされた再起動が開始される前にサイトデータベースの停止が発生した場合、停止が終了すると再起動が開始されます。この操作により、意図しない結果につながる可能性があります。

たとえば、デリバリーグループの再起動が実稼働時間外に（3:00 から）行われるようにスケジュールしたとします。サイト構成データベースの停止が、スケジュールされた再起動が始まる 1 時間前（午前 2 時）に発生します。停止は 6 時間続きます（午前 8 時まで）。Delivery Controller とサイトデータベース間の接続が復元されると、再起動スケジュールが開始されます。VDA の再起動は、元のスケジュールの 5 時間後に開始されます。この操作により、生産時間中に VDA が再起動する可能性があります。

この状況を回避するには、`New-BrokerRebootScheduleV2`および`Set-BrokerRebootScheduleV2`コマンドレットの`MaxOvertimeStartMins`パラメーターを使用できます。この値により、スケジュールされた開始時間の最大何分後に再起動スケジュールを開始できるかを指定します。

- その時間（スケジュールされた時間 + `MaxOvertimeStartMins`）内にデータベース接続が復元された場合、VDA の再起動が開始されます。
- その時間内にデータベース接続が復元されない場合には、VDA の再起動は開始されません。
- このパラメーターを省略するか値に 0 を設定すると、停止時間に関係なく、スケジュールされた再起動はデータベースへの接続の復元時に開始されます。

詳しくは、コマンドレットのヘルプを参照してください。この機能は、PowerShell のみで利用可能です。

メンテナンスモードのマシンのスケジュールされた再起動　再起動スケジュールがメンテナンスモードのマシンに影響を与えるかを指定するには、BrokerRebootScheduleV2コマンドレットでIgnoreMaintenanceModeオプションを使用します。

たとえば、次のコマンドレットは、メンテナンスモードのマシンおよびメンテナンスモードではないマシンの両方を再起動するスケジュールを作成します。

```
New-BrokerRebootSchedulev2 rebootSchedule1 -DesktopGroupName <myDesktopGroup> -IgnoreMaintenanceMode $true
```

次のコマンドレットは、既存の再起動スケジュールを変更します。

```
Set-BrokerRebootSchedulev2 rebootSchedule1 -IgnoreMaintenanceMode $true
```

詳しくは、コマンドレットのヘルプを参照してください。

デリバリーグループのマシンの負荷管理

負荷管理できるのはマルチセッション OS マシンのみです。

負荷管理機能では、測定されたサーバー負荷に基づいて最適なサーバーが選択されます。この選択は、以下の基準により行われます。

- サーバーのメンテナンスモードの状態：メンテナンスモードがオフのマルチセッション OS マシンだけが負荷分散の対象として選択されます。
- サーバー負荷指数：マルチセッション OS マシンの配信サーバーの負荷に基づいて、そのサーバーがどれだけの接続を受け入れられるかが決定されます。サーバー負荷指数は、セッション数とパフォーマンス測定値（CPU、ディスク、メモリ使用量など）で計算される負荷評価基準の組み合わせを指します。負荷評価基準は、ポリシーの負荷管理に関する設定項目で指定します。

  [負荷指数] 列に値 10000 が表示される場合、そのサーバーが負荷限界状態であることを示しています。ほかに使用可能なサーバーがない場合は、ユーザーがセッションを起動したときに、デスクトップまたはアプリケーションを使用できないという内容のメッセージが表示されます。

  Director（監視）、[完全な構成] 管 f 理インターフェイスの [検索] ノード、および SDK を使用して、負荷指数を監視できます。

  コンソールで [サーバー負荷インデックス] 列（デフォルトでは非表示）を表示するには、マシンを選択し、列見出しを右クリックして [列の選択] を選択します。[マシン] カテゴリ の [負荷指数] を選択します。

  SDK では、Get-BrokerMachineコマンドレットを使用します。詳しくは、CTX202150を参照してください。
- 同時ログオントレランスのポリシー設定：サーバーが同時に処理できるログオン要求の最大数です。この設定項目は、XenApp バージョン 6.x の「負荷調整」に相当します。

すべてのサーバーが同時ログオントレランスの設定値に達した場合、それ以降のログオン要求は保留中のログオン数が最も少ないサーバーに割り当てられます。同時ログオントレランスの設定値に達しないサーバーがいくつか存在する場合は、負荷指数が最小のサーバーにログオン要求が割り当てられます。

Autoscale の管理

デフォルトでは、デリバリーグループの Autoscale は無効になっています。デリバリーグループの Autoscale を管理するには（該当する場合）、次の手順を実行します：

1. ［管理］**>**［完全な構成］の左側ペインで ［デリバリーグループ］を選択します。
2. グループを選択し、操作バーの ［**Autoscale** の管理］を選択します。［**Autoscale** の管理］ウィンドウが開きます。
3. 必要に応じて設定を行います。Autoscale の設定について詳しくは、「AutoScale」を参照してください。
4. ［適用］を選択して、ウィンドウを閉じずに行った変更を適用します。または、［保存］を選択し、変更を適用してウィンドウを閉じます。

セッション

- セッションのログオフ/切断、またはユーザーへのメッセージ送信
- セッションの事前起動およびセッション残留の構成
- セッションローミングを構成する
- メンテナンスモードでマシンから切断されたときのセッションの再接続の制御

セッションのログオフ/切断、またはデリバリーグループユーザーへのメッセージ送信

1. ［管理］**>**［完全な構成］の左側ペインで ［デリバリーグループ］を選択します。
2. グループを選択し、操作バーの ［マシンの表示］を選択します。
3. ユーザーをセッションからログオフするには、セッションまたはデスクトップを選択し、操作バーの ［ログオフ］を選択します。セッションが閉じて、ほかのユーザーがそのマシンを使用できるようになります（そのマシンが特定のユーザーに割り当てられてない場合）。
4. セッションを切断するには、セッションまたはデスクトップを選択し、操作バーの ［切断］を選択します。ユーザーのアプリケーションはそのまま実行され、マシンはそのユーザーに割り当てられたままになります。ユーザーは同じマシンに再接続できます。
5. ユーザーにメッセージを送信するには、セッション、マシン、またはユーザーを選択し、操作バーの ［メッセージの送信］を選択します。メッセージを入力します。

デリバリーグループのセッションの事前起動および残留セッションの構成

これらの機能は、マルチセッション OS マシンでのみサポートされます。

セッションの事前起動機能と残留セッション機能では、指定されたユーザーがアプリケーションにすばやくアクセスできるように、以下を実行します:

- 要求される前にセッションを開始する（セッションの事前起動）
- ユーザーがすべてのアプリケーションを閉じた後もアプリケーションセッションをアクティブな状態で保持する（セッション残留）

デフォルトでは、セッションの事前起動とセッション残留は無効になっています。セッションはユーザーがアプリケーションを開始すると開始（起動）され、セッションで開いていた最後のアプリケーションを閉じるまでアクティブな状態で保持されます。

注意事項:

- これらの機能を使用するには、デリバリーグループでアプリケーションが配信されている必要があります。また、マシンでマルチセッション OS 対応 VDA バージョン 7.6 以降が動作している必要があります。
- これらの機能は Windows 向け Citrix Workspace アプリを使用している場合にのみサポートされ、Citrix Workspace アプリ側での構成も必要になります。詳しくは、使用中のバージョンの Windows 向け Citrix Workspace アプリに関する製品ドキュメントで、「セッションの事前起動」を検索してください。
- HTML5 向け Citrix Workspace アプリはサポートされません。
- セッションの事前起動を使用するときに、ユーザーのマシンが一時停止状態または休止状態の場合は、（セッションの事前起動設定にかかわらず）事前起動は機能しません。ユーザーはマシン/セッションをロックできます。ただし、ユーザーが Citrix Workspace アプリからログオフすると、セッションが終了し、事前起動は適用されなくなります。
- セッションの事前起動を使用するときは、物理クライアントマシンでは一時停止または休止状態の電源管理機能を使用できません。クライアントマシンのユーザーはセッションをロックすることはできますが、ログオフすることはできません。
- 事前起動セッションと残留セッションは、接続されている間のみ同時使用ライセンスを消費します。ユーザーライセンスまたはデバイスライセンスを使用する場合、ライセンスは 90 日間有効です。使用されない事前起動セッションと残留セッションは、デフォルトで 15 分後に切断されます。この値は PowerShell（`New`/`Set-BrokerSessionPreLaunch`コマンドレット）で構成できます。
- これらの機能が相互に補完し合うよう調整するには、ユーザーの使用状況を監視して慎重に計画することが重要です。最適に構成することで、ライセンス消費やリソース割り当ての効率化とユーザーの利便性を両立させることができます。
- Citrix Workspace アプリ側で、セッションの事前起動を有効にする時間帯を構成できます。

使用されない事前起動セッションや残留セッションがアクティブのまま保持される時間　ユーザーがアプリケーションを起動しない場合に、使用されないセッションをどのくらい保持するかを指定するには、タイムアウトおよびサーバー負荷のしきい値を構成します。これらのすべてを設定することができます。最初に発生したイベントによって未使用のセッションが終了します。

- タイムアウト：使用されない事前起動セッションや残留セッションを保持する日数、時間数、または分数を指定できます。この値が短すぎると事前起動セッションがすぐに終了してしまい、ユーザーがアプリケーション

にすばやくアクセスできるというメリットが活かされません。また、タイムアウト値が長すぎると、サーバーのリソースが足りなくなり、ユーザーの接続要求が拒否される場合があります。

このタイムアウトの設定は、管理コンソールではなく SDK からのみ(`New-BrokerSessionPreLaunch` / `Set-BrokerSessionPreLaunch` コマンドレット）有効にできます。タイムアウトを無効にすると、コンソールや ［デリバリーグループの編集］ページにそのデリバリーグループのタイムアウトが表示されなくなります。

- しきい値：サーバーの負荷が高くなったときに事前起動セッションや残留セッションを自動的に終了することができます。これにより、サーバーの負荷が低い間は可能な限りセッションが保持されます。新しいユーザーセッション用のリソースが必要になったときに事前起動セッションや残留セッションが自動的に終了するため、これらのセッションが原因で接続が拒否されることはありません。

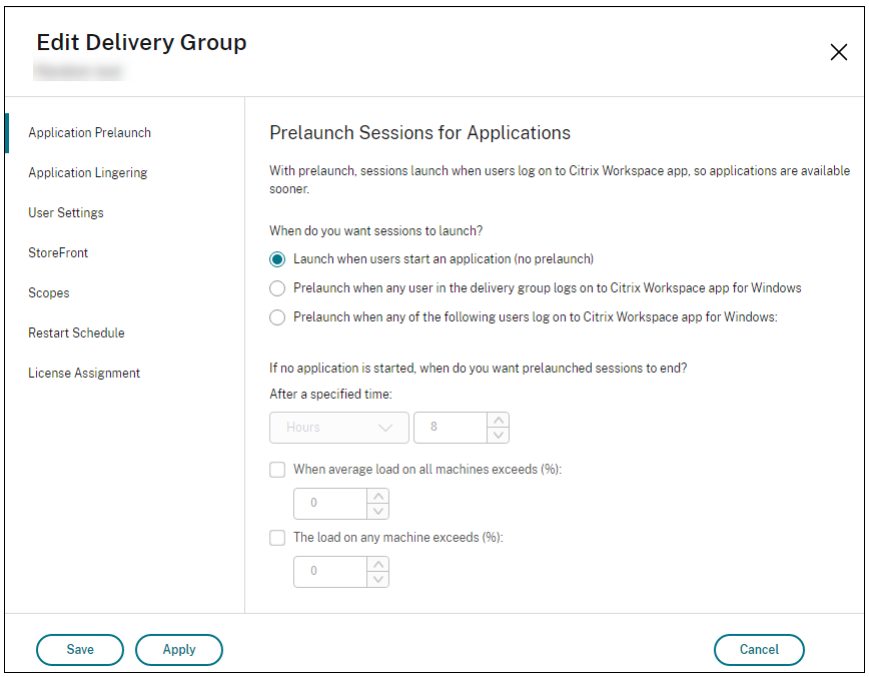
  次の 2 つのしきい値を構成できます：デリバリーグループ内の全サーバーの平均負荷パーセンテージと、グループ内のいずれかのサーバーの最大負荷パーセンテージ。サーバーの負荷がいずれかのしきい値を超えると、最も長い時間保持された事前起動セッションまたは残留セッションが終了します。その後、負荷がしきい値を下回るまで、分間隔で 1 つずつセッションが終了します。しきい値を超えている間は、新たな事前起動セッションは開始されません。

Controller に登録されていない VDA が動作するサーバーやメンテナンスモードのサーバーは、負荷限界状態として認識されます。サーバーで計画外の停止状態が発生した場合、事前起動セッションや残留セッションは自動的に終了してリソースが解放されます。

セッションの事前起動を有効にするには、次の手順に従います

1. ［管理］**>**［完全な構成］の左側ペインで ［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［編集］を選択します。
3. ［アプリケーションの事前起動］ページで、セッションを起動するタイミングを選択します：

   - アプリケーションの起動時にセッションを起動する。これがデフォルトの設定です。セッションの事前起動機能は無効になっています。
   - デリバリーグループ内のすべてのユーザーで、Windows 向け Citrix Workspace アプリへのログオン時に事前起動する。
   - 一覧に含まれるユーザーおよびユーザーグループでのみ、Windows 向け Citrix Workspace アプリへのログオン時に事前起動する。このオプションを選択する場合は、ユーザーまたはユーザーグループを一覧に追加してください。



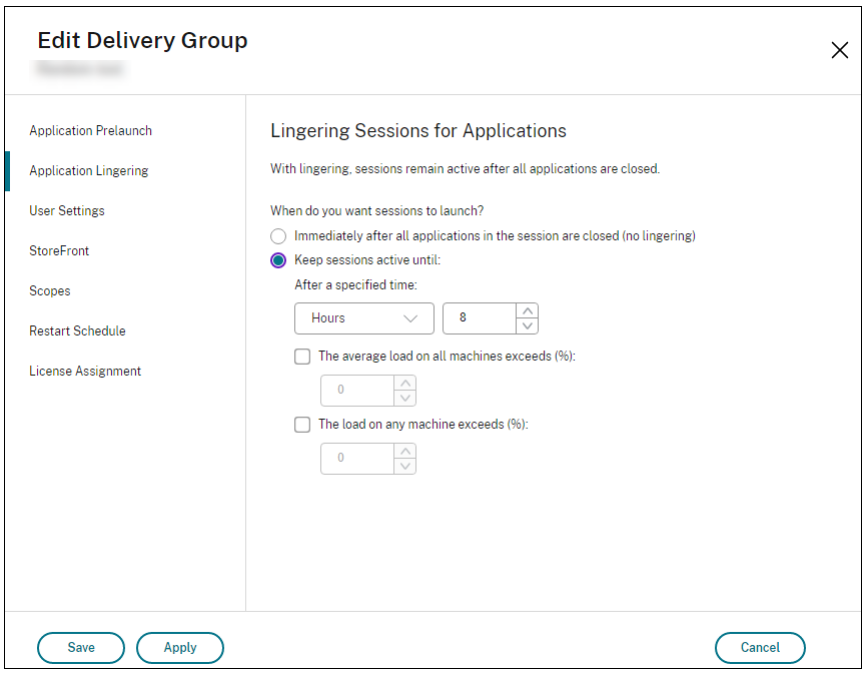
4. 事前起動セッションは、ユーザーがアプリケーションを起動すると通常のセッションに置き換わります。ユーザーがアプリケーションを起動しない場合（事前起動セッションが使用されない場合）、以下の設定に従って事前起動セッションが終了します。

   - この時間が経過したときにセッションを終了する。セッションを自動的に終了するまでの時間を指定します（1～99 日間、1～2,376 時間、または 1～142,560 分）。
   - デリバリーグループ内のすべてのマシンの平均負荷が指定上限値 1%～99% を超えたときに終了する。
   - デリバリーグループ内のいずれかのマシンの負荷が指定上限値 1%～99% を超えたときに終了する。

   事前起動セッションは、ユーザーがいずれかのアプリケーションを起動したとき、指定した時間が経過したとき、または指定した負荷のしきい値を超えたときのいずれかの状態が発生するまで保持されます。

セッション残留を有効にするには、次の手順に従います

1. ［管理］**>**［完全な構成］の左側ペインで ［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［編集］を選択します。
3. ［アプリケーションの残留］ページで、［セッションをアクティブのまま保持する期間を指定する］をクリックします。



4. ユーザーが別のアプリケーションを起動しない場合、残留セッションを保持する時間は複数の設定によって決定されます。

   - この時間が経過したときにセッションを終了する。セッションを自動的に終了するまでの時間を指定します（1～99 日間、1～2,376 時間、または 1～142,560 分）。
   - デリバリーグループ内のすべてのマシンの平均負荷が指定上限値 1%～99% を超えたときに終了する。
   - デリバリーグループ内のいずれかのマシンの負荷が指定上限値 1%～99% を超えたときに終了する。

   要約：残留セッションは、次のいずれかの状態が発生するまで保持されます：ユーザーがいずれかのアプリケーションを起動したとき、指定した時間が経過したとき、または指定した負荷のしきい値を超えたとき。

セッションローミングを構成する

デフォルトでは、デリバリーグループでセッションローミングが有効になっています。ユーザーのクライアントデバイス間でセッションローミングが行われます。ユーザーがセッションを開始した後に別のデバイスに移動した場合、同じセッションが使用され、両方のデバイスで同時にアプリケーションを使用することができます。複数のデバイスでアプリケーションを表示できます。デバイスや、現在のセッションが存在するかどうかに関係なく、アプリケーションが引き継がれます。たいていの場合、アプリケーションに割り当てられたプリンターやそのほかのリソースも引き継がれます。または、PowerShell を使用することもできます。詳しくは、「セッションローミング」を参照してください。

アプリケーションのセッションローミングを構成する　アプリケーションのセッションローミングを構成するには、次の手順に従います：

1. ［管理］**>**［完全な構成］の左側ペインで ［デリバリーグループ］を選択します。

2. グループを選択して、操作バーの ［デリバリーグループの編集］を選択します。
3. ［ユーザー］ページで、［ユーザーがデバイス間を移動するときにセッションローミングを行う］チェックボックスをオンにして、セッションローミングを有効にします。
    - 有効にすると、ユーザーがアプリケーションセッションを開始した後に別のデバイスに移動した場合、同じセッションが使用され、両方のデバイスでアプリケーションを使用することができます。無効にすると、セッションはデバイス間でローミングしなくなります。
4. ［**OK**］を選択して、変更を適用してウィンドウを閉じます。

デスクトップのセッションローミングを構成する　デスクトップのセッションローミングを構成するには、次の手順に従います:

1. ［管理］**>**［完全な構成］の左側ペインで ［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［デリバリーグループの編集］を選択します。
3. ［デスクトップ］ページでデスクトップを選択し、［編集］を選択します。
4. ［セッションローミング］チェックボックスをオンにして、セッションローミングを有効にします。
    - 有効にすると、ユーザーがデスクトップを開始した後に別のデバイスに移動した場合、同じセッションが使用され、両方のデバイスでアプリケーションを使用することができます。無効にすると、セッションはデバイス間でローミングしなくなります。
5. ［**OK**］を選択して、変更を適用してウィンドウを閉じます。

メンテナンスモードでマシンから切断されたときのセッションの再接続の制御

> 注:
>
> この機能は、PowerShell のみで利用可能です。

メンテナンスモードのマシンで切断されたセッションが、デリバリーグループ内のマシンに再接続できるかどうかを制御できます。

2021 年 5 月下旬以前は、メンテナンスモードでマシンから切断されたシングルセッションのプールされたデスクトップセッションについて、再接続は許可されていませんでした。現在は、メンテナンスモードでマシンから切断された後、（セッションタイプに関係なく）再接続を許可または禁止するようにデリバリーグループを構成できるようになりました。

デリバリーグループを作成または編集する場合(`New-BrokerDesktopGroup`、`Set-BrokerDesktopGroup`）は、`-AllowReconnectInMaintenanceMode <boolean>`パラメーターを使用して、メンテナンスモードでマシンから切断されたマシンの再接続を許可または禁止します。

- true に設定すると、セッションはグループ内のマシンに再接続できます。

- false に設定すると、セッションはグループ内のマシンに再接続できません。

デフォルト値:

- シングルセッション: 無効
- マルチセッション: 有効

アプリケーション

デリバリーグループ内のアプリケーションを表示し、必要に応じてさらに追加します。

1. ［管理］**>**［完全な構成］の左側ペインで ［デリバリーグループ］を選択します。
2. グループを選択します。このグループにアプリケーションが含まれている場合は、操作バーに ［アプリケーションの表示］が表示されます。
3. ［アプリケーションの表示］を選択します。このグループで利用可能なすべてのアプリケーションが表示される［アプリケーション］ノードに移動します。
4. このグループにさらにアプリケーションを追加するには、［デリバリーグループ］ノードに移動し、グループを選択して、操作バーで ［アプリケーションの追加］を選択します。

トラブルシューティング

- 仲介セッションを起動する場合、Delivery Controller に登録されていない VDA は考慮されません。これにより、登録されていれば使用されるはずのリソースが使用されない場合があります。VDA が登録されない理由はさまざまですが、その多くは管理者がトラブルシューティングできます。詳細画面ではカタログ作成ウィザードで、またはカタログをデリバリーグループに登録した後に、トラブルシューティング情報を提供します。

  デリバリーグループを作成すると、デリバリーグループの［詳細］ペインに、登録される予定でまだ登録されていないマシンの数が表示されます。たとえば、1 台または複数台のマシンの電源が入っておりメンテナンスモードではないのに、Controller に現在登録されていない場合があります。「未登録だが登録する必要がある」のマシンが表示された場合は、［詳細］ペインの ［トラブルシューティング］タブで、考えられる原因と推奨される修正アクションを確認します。

  機能レベルに関するメッセージについては、「VDA バージョンと機能レベル」を参照してください。

  VDA 登録のトラブルシューティングについて詳しくは、CTX136668を参照してください。

- デリバリーグループの表示では、［詳細］ペインの ［インストール済み **VDA** のバージョン］が、マシンにインストールされている実際のバージョンと異なる可能性があります。マシンの Windows の［プログラムと機能］には、VDA の実際のバージョンが表示されます。
- マシンの状態が「**Power State Unknown**」の場合、CTX131267を参照してください。

アプリケーショングループの作成

June 12, 2024

はじめに

アプリケーショングループを使用すると、アプリケーションのコレクションを管理できます。異なるデリバリーグループ間で共有されているアプリケーションや、デリバリーグループ内のユーザーのサブセットによって使用されるアプリケーションのアプリケーショングループを作成できます。アプリケーショングループはオプションです。複数のデリバリーグループに同じアプリケーションを追加する代わりの手段となります。デリバリーグループは複数のアプリケーショングループに関連付けることができ、アプリケーショングループは複数のデリバリーグループに関連付けることができます。

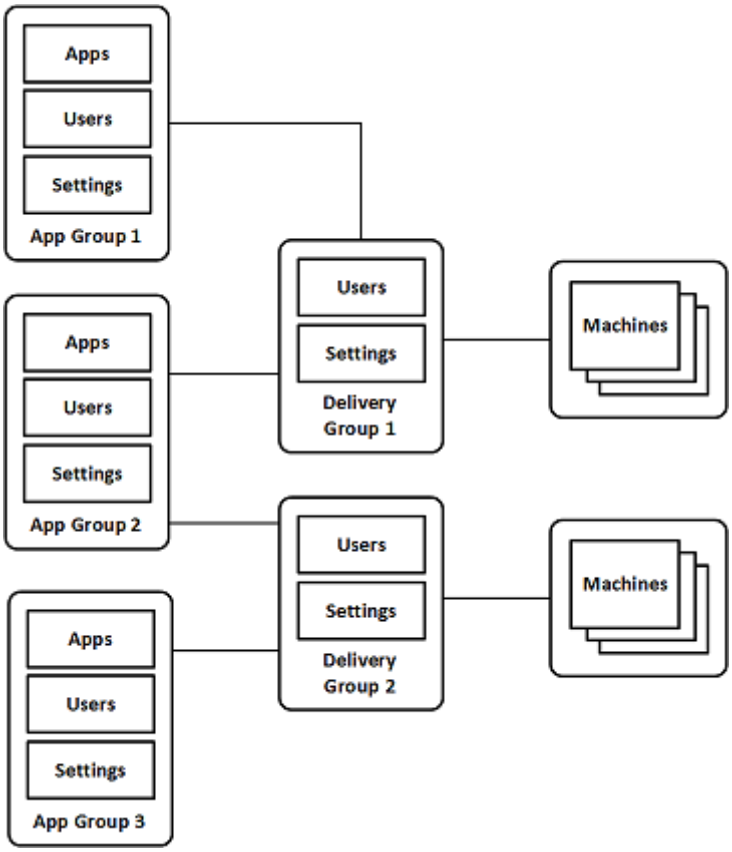
アプリケーショングループの使用は、さらに多くのデリバリーグループを使用するのに比べて、アプリケーション管理とリソース制御に利点をもたらします:

- アプリケーションおよびその設定を論理的にグループ化することで、アプリケーションを 1 つの単位として管理することができます。たとえば、同じアプリケーションをそれぞれのデリバリーグループに 1 つずつ追加（公開）する必要はありません。
- アプリケーショングループ間でのセッション共有により、リソースの消費を削減できます。また、アプリケーショングループ間のセッション共有を無効にすることが有益な場合もあります。
- タグ制限機能を使用すると、選択したデリバリーグループ内のマシンのサブセットだけを対象にして、アプリケーショングループからアプリケーションを公開できます。タグ制約で、複数の公開タスクに既存のマシンを使用できるので、追加のマシンを展開、管理するコストを節約できます。タグ制限は、デリバリーグループのマシンをさらに分割（またはパーティション化）するものと考えることができます。タグ制限のあるアプリケーショングループやデスクトップを使用すると、デリバリーグループ内のマシンのサブセットを分離してトラブルシューティングするときに便利です。

構成例

例 **1**

次の図は、アプリケーショングループを含む環境を示しています:



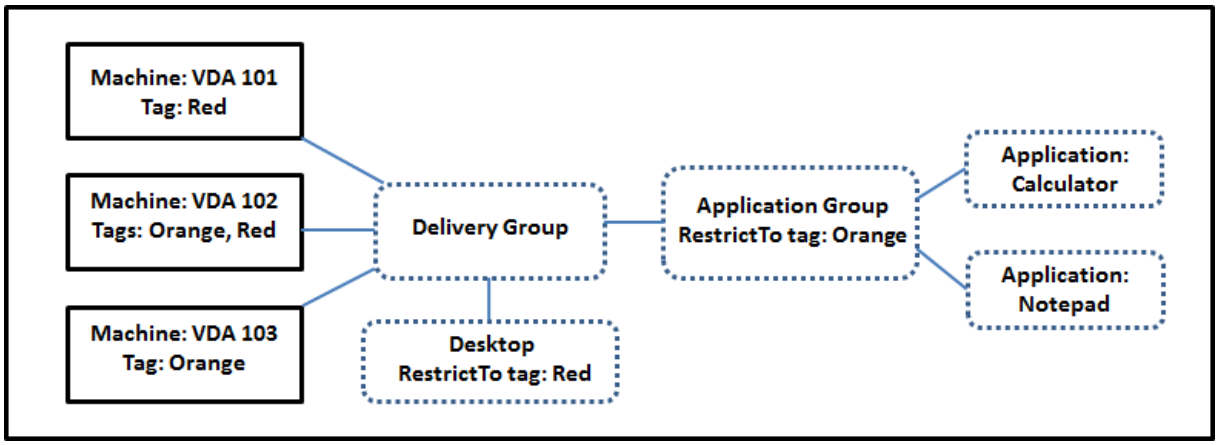
この構成では、アプリケーションはデリバリーグループではなくアプリケーショングループに追加されます。デリバリーグループでは、使用するマシンを指定します。（表示されていませんが、マシンはマシンカタログに含まれています。）

アプリケーショングループ 1 はデリバリーグループ 1 に関連付けられています。アプリケーショングループ 1 のアプリケーションには、アプリケーショングループ 1 で指定されているユーザーが、デリバリーグループ 1 のユーザー一覧にも含まれている限り、アクセスできます。これは、アプリケーショングループのユーザー一覧は関連付けられているデリバリーグループのユーザー一覧のサブセット（制限）でなければならないというガイダンスに従っています。アプリケーショングループ 1 の設定（アプリケーショングループ間で共有されるアプリケーションセッション、関連付けられているデリバリーグループなど）は、このグループのアプリケーションとユーザーに適用されます。デリバリーグループ 1 の設定（匿名ユーザーサポートなど）は、アプリケーショングループ 1 および 2 のユーザーに適用されます。この 2 つのアプリケーショングループがこのデリバリーグループに関連付けられているためです。

アプリケーショングループ 2 は、デリバリーグループ 1 と 2 に関連付けられています。この 2 つのデリバリーグループそれぞれにアプリケーショングループ 2 の優先度を割り当てることで、アプリケーション起動時にデリバリーグループをチェックする順序を指定できます。同等の優先度が割り当てられたデリバリーグループ間では、負荷が分散されます。アプリケーショングループ 2 のアプリケーションには、アプリケーショングループ 2 で指定されているユーザーが、デリバリーグループ 1 とデリバリーグループ 2 のユーザー一覧にも含まれている限り、アクセスできます。

例 **2**

この単純なレイアウトでは、あるデスクトップおよびアプリケーションの起動に関係するマシンを、タグ制約を使用して制限します。サイトには、1 つの共有デリバリーグループ、1 つの公開デスクトップ、および 2 つのアプリケーションで構成された 1 つのアプリケーショングループがあります。



3 台のマシン（VDA 101～103）それぞれにタグが追加されています。

アプリケーショングループは「Orange」のタグ制限で作成されているので、各アプリケーション（電卓とメモ帳）は、デリバリーグループの、タグが「Orange」のマシン VDA 102 および 103 上でのみ起動できます。

アプリケーショングループ（およびデスクトップ）でのタグ制限の使用に関する包括的な例やガイダンスは、「タグ」を参照してください。

ガイダンスおよび考慮事項

Citrix では、アプリケーショングループとデリバリーグループの両方ではなく、どちらか一方にアプリケーションを追加することをお勧めします。両方に追加すると、アプリケーションを 2 種類のグループに追加することにより複雑度が増加し、管理が困難になる可能性があります。

デフォルトでは、アプリケーショングループが有効になっています。アプリケーショングループ作成後、グループを編集してこの設定を変更できます。「アプリケーショングループの管理」を参照してください。

デフォルトでは、アプリケーショングループ間でのアプリケーションセッションの共有が有効になっています。「アプリケーショングループ間のセッション共有」を参照してください。

Citrix では、デリバリーグループを最新のバージョンにアップグレードすることをお勧めします。これには、次のことが必要です：

1. デリバリーグループで使用されているマシン上の VDA のアップグレード
2. それらのマシンを含むマシンカタログをより高い機能レベルに変更
3. デリバリーグループをより高い機能レベルに変更

詳しくは、「デリバリーグループの管理」を参照してください。

アプリケーショングループを使用するには、コアコンポーネントがバージョン 7.9 以上である必要があります。

アプリケーショングループを作成するには、デリバリーグループ管理者組み込みの役割の配信管理者権限が必要です。詳しくは、「委任管理」を参照してください。

この記事では、アプリケーションを複数のアプリケーショングループに「関連付ける」と表現することで、このアクションと、利用可能なソースからアプリケーションの新しいインスタンスを追加することを区別しています。同様に、デリバリーグループはアプリケーショングループに関連付けられ、アプリケーショングループはデリバリーグループに関連付けられます。追加されるのでも、お互いのコンポーネントになるのでもありません。

アプリケーショングループを使用したセッション共有

アプリケーションセッション共有を有効にすると、すべてのアプリケーションが同一のアプリケーションセッションで起動されるようになります。これにより、追加のアプリケーションセッションの起動にかかるコストが抑えられるとともに、クリップボードを使用するアプリケーション機能（コピーアンドペーストなど）を使用できます。ただし、セッション共有の無効化が必要になる場合もあります。

アプリケーショングループを使用する場合、以下の 3 通りの方法でアプリケーションセッション共有を構成して、デリバリーグループのみを使用ときに利用できる標準的なセッション共有の動作を拡張できます：

- アプリケーショングループ間でセッション共有を有効にする。
- 同一のアプリケーショングループに含まれるアプリケーション間でのみセッション共有を有効にする。
- セッション共有を無効にする。

アプリケーショングループ間のセッション共有

アプリケーショングループ間のアプリケーションセッション共有を有効にすることも、この共有を無効化して、アプリケーションセッション共有を同一のアプリケーショングループに含まれるアプリケーションのみに限定することもできます。

- アプリケーショングループ間のセッション共有を有効にすることが役立つ例：

  アプリケーショングループ 1 には、Word や Excel などの Microsoft Office アプリケーションが含まれています。アプリケーショングループ 2 にはメモ帳や電卓などその他のアプリケーションが含まれており、両方のアプリケーショングループは同じデリバリーグループに接続されています。両方のアプリケーショングループへのアクセス権を持つユーザーが、Word を起動してアプリケーションセッションを開始してから、メモ帳を起動するとします。このユーザーの Word が実行されている既存のセッションがメモ帳の実行にも適していると判断されると、メモ帳は既存のセッション内で起動されます。メモ帳を既存のセッションで実行できない場合（タグによる制限でセッションの実行元のマシンが除外されている場合など）、セッション共有を使用せず適切なマシン上に新しいセッションが作成されます。

- アプリケーショングループ間のセッション共有を無効にすることが役立つ例：

同じソフトウェアスイートの 2 つの異なるバージョンや、同じ Web ブラウザーの 2 つの異なるバージョンなど、同時に使用することがあまりない一連のアプリケーションが同じマシンにインストールされています。管理者は、同じセッションで両方のバージョンを起動することをユーザーに許可しないほうがいいと考えました。

ソフトウェアスイートの各バージョン用にアプリケーショングループを 1 つ作成し、ソフトウェアスイートの各バージョンのアプリケーションを対応するアプリケーショングループに追加します。これらの各アプリケーショングループでグループ間のセッション共有を無効にすると、各グループで指定されたユーザーは同じセッションで同じバージョンのアプリケーションを実行でき、同時に他のアプリケーションを別のセッションで実行できます。ユーザーが異なるバージョンのアプリケーション（異なるアプリケーショングループに含まれるアプリケーション）を起動するか、アプリケーショングループには含まれていないアプリケーションを起動すると、そのアプリケーションは新しいセッションで起動されます。

このアプリケーショングループ間のセッション共有機能は、セキュリティサンドボックス機能ではありません。完全に信頼することはできず、ユーザーが別の手段（Windows エクスプローラーなど）を使用してセッションにアプリケーションを起動することは防げません。

マシンがフル稼働の場合、そのマシンで新しいセッションは開始されません。新しいアプリケーションは、必要に応じてセッション共有を使用し、既存のセッション内で起動されます（この動作が、ここで説明するセッション共有の制限に従っている場合）。

事前起動セッションは、アプリケーションセッション共有が許可されているアプリケーショングループでのみ利用できます（残留セッション機能を使用するセッションは、すべてのアプリケーショングループで利用できます）。これらの機能は、アプリケーショングループに関連付けるデリバリーグループごとに有効にして構成する必要があります。アプリケーショングループでは設定できません。

デフォルトでは、アプリケーショングループの作成時、アプリケーショングループ間のアプリケーションセッション共有は有効になっています。グループを作成するときにこれを変更することはできません。アプリケーショングループ作成後、グループを編集してこの設定を変更できます。「アプリケーショングループの管理」を参照してください。

アプリケーショングループ内でのセッション共有の無効化

同一のアプリケーショングループに含まれるアプリケーション間で、アプリケーションセッション共有を無効にすることができます。

- アプリケーショングループ内のセッション共有を無効にすることが役立つ例：

  ユーザーが別々のモニターで、アプリケーションの複数の全画面セッションへ同時にアクセスできるようにする場合。

  アプリケーショングループを作成して、そのグループにアプリケーションを追加する場合。アプリケーショングループ内のアプリケーション間でのセッション共有が禁止されている場合、グループ内で指定されたユーザーは別々のセッションでアプリケーションを 1 つずつ起動することになり、各アプリケーションを個別のモニターに移動することができます。

デフォルトでは、アプリケーショングループ作成時にはアプリケーションセッションの共有が有効になっています。グループを作成するときにこれを変更することはできません。アプリケーショングループ作成後、グループを編集してこの設定を変更できます。「アプリケーショングループの管理」を参照してください。

アプリケーショングループの作成

アプリケーショングループを作成するプロセスで、Citrix Workspace アプリにアプリケーションカテゴリを作成します。アプリケーションカテゴリを使用して、Citrix Workspace 内のアプリケーションのコレクションを管理できます。

アプリケーショングループを作成するには:

1. ［管理］**>**［完全な構成］の左側ペインで ［アプリケーション］を選択してから、［アプリケーショングループ］タブを選択します。
2. フォルダーを使用してアプリケーショングループを整理するには、**Application Groups** ルートフォルダーの下にフォルダーを作成します。
3. グループを作成するフォルダーを選択し、［アプリケーショングループの作成］をクリックします。グループ作成ウィザードが起動し、［はじめに］ページが表示されます。このウィザードで、今後このページが表示されないようにできます。
4. ウィザードに従って、以下に説明するページで設定を構成します。各ページの操作を終えたら、［概要］ページに到達するまで ［次へ］を選択します。

手順 **1**: デリバリーグループ

［デリバリーグループ］ページには、すべてのデリバリーグループが、各グループに含まれるマシンの数とともに表示されます。

- ［互換性のあるデリバリーグループ］リストには、選択可能なデリバリーグループが含まれています。互換性のあるデリバリーグループには、ランダムな（永続的ではない、つまり静的に割り当てられていない）サーバーやデスクトップ OS マシンが含まれます。
- ［互換性のないデリバリーグループ］リストには、選択できないデリバリーグループが含まれています。各エントリで、静的に割り当てられたマシンを含む、などの互換性がない理由が説明されます。

アプリケーショングループは、アプリケーションを配信可能な共有（プライベートではない）マシンが含まれるデリバリーグループに関連付けることができます。

次の両方の条件が満たされている場合は、デスクトップのみを配信する共有マシンが含まれるデリバリーグループを選択することもできます:

- デリバリーグループは、共有マシンが含まれ、7.9 より前のバージョンの XenDesktop で作成されたものです。
- デリバリーグループの編集権限があります。

グループ作成ウィザードをコミットすると、デリバリーグループの種類が自動的に「デスクトップおよびアプリケーション」に変換されます。

おそらくはアプリケーションを整理したり現在は使用されていないアプリケーションのストレージとして使用したりするために、デリバリーグループに関連付けないアプリケーショングループを作成することができますが、アプリケーショングループで少なくとも 1 つのデリバリーグループを指定するまでは、そのアプリケーショングループを使用してアプリケーションを配信することはできませんまた、デリバリーグループが指定されていない場合は、［スタート］メニューから のソースからアプリケーショングループにアプリケーションを追加することもできません。

選択するデリバリーグループで、アプリケーションの配信に使用するマシンを指定します。アプリケーショングループに関連付けるデリバリーグループの横にあるチェックボックスをオンにします。

タグ制約を追加するには、［タグでマシンの起動を制限します:］を選択し、ドロップダウンからタグを選択します。

手順 **2**：ユーザー

アプリケーショングループのアプリケーションを使用できるユーザーを指定します。1 つ前のページで選択したデリバリーグループのすべてのユーザーとユーザーグループに許可するか、このデリバリーグループの特定のユーザーとユーザーグループを選択することができます。指定したユーザーの使用を制限した場合は、デリバリーグループとアプリケーショングループで指定したユーザーだけが、このアプリケーショングループのアプリケーションにアクセスできます。基本的に、アプリケーショングループのユーザー一覧は、デリバリーグループのユーザー一覧のフィルターとして機能します。

認証されていないユーザーによるアプリケーション使用の有効化または無効化は、デリバリーグループでのみ行えます。アプリケーショングループではできません。

展開内のユーザー一覧が指定されている場所については、「ユーザー一覧の指定場所」を参照してください。

手順 **3**：アプリケーション

ヒント:

- アプリケーションをデリバリーグループに追加すると、デフォルトで「アプリケーション」という名前のフォルダー内に表示されます。別のフォルダーを指定することもできます。アプリケーションの追加時に、そのフォルダー内に同じ名前のアプリケーションが既に存在する場合、追加するアプリケーションの名前を変更するよう指示するメッセージが表示されます。提案された一意の名前を受け入れると、アプリケーションにその新しい名前が追加されます。それ以外の場合は、追加する前に名前を変更する必要があります。詳しくは、「アプリケーションフォルダーの管理」を参照してください。
- アプリケーションのプロパティ（設定）は、追加時、または後で変更できます。「アプリケーションプロパティの変更」を参照してください。同じ名前の 2 つのアプリケーションを同じユーザーに公開する場合は、［完全な構成］管理インターフェイスの ［アプリケーション名（ユーザー用）］プロパティに別の名前を入力します。これを行わないと、Citrix Workspace アプリには同じ名前が 2 つ表示されます。

- アプリケーションを複数のアプリケーショングループに追加する場合、そのすべてのアプリケーショングループのアプリケーションを見ることができる十分な権限を有していなければ、表示上の問題が発生する可能性があります。そのような問題が発生した場合は、より上位の権限を持つ管理者に相談するか、または自身の権限を拡張して、アプリケーションを追加したグループをすべて含めるようにします。

［追加］ボックスを選択して、アプリケーションのソースを表示します。

- ［スタート］メニューから：選択したデリバリーグループのマシンで検出されたアプリケーション。このソースを選択すると、新たなページが開き、検出されたアプリケーションが一覧表示されます。追加するアプリケーションのチェックボックスをオンにし、［**OK**］を選択します。

  このソースは、次のいずれかを選択した場合は選択できません：

  - 関連するデリバリーグループのないアプリケーショングループ。
  - マシンを含まないデリバリーグループが関連付けられたアプリケーショングループ。
  - マシンを含まないデリバリーグループ。

- 手動：サイトまたはネットワーク内の別の場所にあるアプリケーション。このソースを選択すると、新たなページが開くので、そのページで実行可能ファイルのパス、作業ディレクトリ、オプションのコマンドライン引数、管理者およびユーザー用の表示名を入力します。この情報を入力したら、［**OK**］を選択します。
- 既存：以前サイトに追加したアプリケーション。このソースを選択すると、新たなページが開き、検出されたアプリケーションが一覧表示されます。追加するアプリケーションのチェックボックスをオンにし、［**OK**］を選択します。このソースは、サイトにアプリケーションが含まれていない場合は選択できません。
- アプリケーションパッケージ：App-V、MSIX、MSIX アプリのアタッチ、または FlexApp アプリケーションパッケージ内のアプリケーション。このソースを選択すると、［パッケージからアプリケーションの追加］ページが開きます。アプリケーションパッケージのソースを選択して、表示結果からグループに追加するアプリケーション、［**OK**］の順に選択します

  > 注：
  >
  > MSIX または MSIX アプリのアタッチアプリを公開するには、デリバリーグループの機能レベルが 2106 以降である必要があります。FlexApp アプリの場合、機能レベルは 2206 以降である必要があります。機能レベルの要件が満たされていない場合、［アプリケーションパッケージのソース］ドロップダウンリスト内の対応するオプションは選択不可になります。
  > 注：
  >
  > VDA バージョン 2003 以降では、HTTP URL からの App-V パッケージの公開はサポートされていません。これらのアプリケーションをリストから選択することはできません。

上述のとおり、［追加］ボックスの特定のエントリは、そのタイプの有効なソースがない場合は選択できません。互換性のないソースは、一切表示されません。たとえば、アプリケーショングループにアプリケーショングループは追加できないため、このソースはアプリケーショングループ作成時には表示されません。

手順 **4**：スコープ

このページは、カスタムスコープを作成済みの場合にのみ表示されます。デフォルトでは、すべてのスコープが選択されています。詳しくは、「管理者権限の委任」を参照してください。

手順 **5**：まとめ

アプリケーショングループの名前を入力します。必要に応じて説明も入力できます。

概要の情報を確認し、［完了］を選択します。

アプリケーショングループの管理

January 26, 2023

はじめに

この記事では、作成済みのアプリケーショングループの管理方法について説明します。

以下の操作方法を含む、アプリケーショングループまたはデリバリーグループでのアプリケーションの管理について詳しくは、「アプリケーション」を参照してください：

- アプリケーショングループのアプリケーションの追加または削除
- アプリケーショングループの関連付けの変更

アプリケーショングループの管理には、組み込みの役割であるデリバリーグループ管理者の委任管理権限が必要です。詳しくは、「委任管理」を参照してください。

アプリケーショングループの有効化または無効化

アプリケーショングループを有効にすると、このグループに追加されたアプリケーションを配信できます。アプリケーショングループを無効にすると、グループ内のアプリケーションもすべて無効になります。ただし、これらのアプリケーションが他の有効なアプリケーショングループにも関連付けられている場合は、これらの他のアプリケーショングループから配信できます。同様に、アプリケーションが（アプリケーショングループへの追加に加えて）アプリケーショングループに関連付けられているデリバリーグループに明示的に追加されている場合は、アプリケーショングループを無効にしても、これらのデリバリーグループに追加されたアプリケーションには影響しません。

アプリケーショングループは、作成すると有効になります。グループを作成するときにこれを変更することはできません。

1. ［管理］**>**［完全な構成］の左側ペインで ［アプリケーション］を選択してから、［アプリケーショングループ］タブを選択します。
2. アプリケーショングループを選択し、操作バーで ［アプリケーショングループを編集します］を選択します。
3. ［設定］ページで、［アプリケーショングループを有効にする］チェックボックスをオンまたはオフにします。
4. ［適用］を選択して行った変更を適用しウィンドウを開いたままにするか、［**OK**］を選択して変更を適用しウィンドウを閉じます。

アプリケーショングループ間でのアプリケーションセッション共有の有効化または無効化

アプリケーショングループの作成時、アプリケーショングループ間でのセッション共有は有効になっています。グループを作成するときにこれを変更することはできません。詳しくは、「アプリケーショングループを使用したセッション共有」を参照してください。

1. ［管理］**>**［完全な構成］の左側ペインで ［アプリケーション］を選択してから、［アプリケーショングループ］タブを選択します。
2. アプリケーショングループを選択し、操作バーで ［アプリケーショングループを編集します］を選択します。
3. ［設定］ページで、［アプリケーショングループ間のアプリケーションのセッション共有を有効にします］チェックボックスをオンまたはオフにします。
4. ［適用］を選択して行った変更を適用しウィンドウを開いたままにするか、［**OK**］を選択して変更を適用しウィンドウを閉じます。

アプリケーショングループ内でのアプリケーションセッション共有の無効化

アプリケーショングループを作成すると、同じアプリケーショングループのアプリケーション間のセッション共有がデフォルトで有効になります。アプリケーショングループ間でのアプリケーションセッション共有を無効化しても、同じアプリケーショングループのアプリケーション間のセッション共有は引き続き有効です。

PowerShell SDK を使用して、所属するアプリケーション間のセッション共有を無効化したアプリケーショングループを構成できます。状況によっては、この機能が望ましい場合もあります。たとえば、ユーザーが複数の非シームレスアプリケーションを個別のモニターのフルサイズのアプリケーションウィンドウで起動できるようにする場合などです。

アプリケーショングループ内でのアプリケーションセッション共有を無効にした場合、そのグループ内の各アプリケーションは新しいアプリケーションセッションで起動します。適切な切断されたセッションで同じアプリケーションが動作中の利用可能なセッションがあれば、そのセッションが再接続されます。たとえば、Notepad を起動する場合、Notepad が動作中の切断されたセッションがあれば、新しいセッションを作成しないでそのセッションが再接続されます。複数の適切な切断セッションが利用可能な場合、そのうちの 1 つのセッションが再接続先として、ランダムだが決定的な方法で選択されます。同じ状況で同じ状態が再現した場合は、同じセッションが選択されます。しかし、そうでない場合は再接続されるセッションは、予測できるとは限りません。

PowerShell SDK を使用して、既存のアプリケーショングループのすべてのアプリケーションでアプリケーション

セッション共有を無効化するか、アプリケーションセッション共有を無効化したアプリケーショングループを作成できます。

PowerShell コマンドレット例

セッション共有を無効化するには、Broker PowerShell コマンドレットの New-BrokerApplicationGroup、または Set-BrokerApplicationGroup を -SessionSharingEnabled パラメーターを False に、-SingleAppPerSession パラメーターを True に設定して実行します。

- たとえば、グループ内のすべてのアプリケーションでアプリケーションセッション共有が無効のアプリケーショングループを作成するには、以下を実行します:

  ```
  New-BrokerApplicationGroup AppGr1 -SessionSharingEnabled $False -SingleAppPerSession $True
  ```

- たとえば、既存のアプリケーショングループ内のすべてのアプリケーション間でアプリケーションセッション共有を無効化するには、以下を実行します:

  ```
  Set-BrokerApplicationGroup AppGR1 -SessionSharingEnabled $False -SingleAppPerSession $True
  ```

注意事項

- SingleAppPerSessionプロパティを有効にするには、SessionSharingEnabledプロパティを False に設定する必要があります。この 2 つのプロパティは、同時に有効化してはなりません。SessionSharingEnabledパラメーターは、アプリケーショングループ間のセッション共有に関するものです。
- アプリケーションセッション共有は、アプリケーショングループに関連付けられているが、デリバリーグループには関連付けられていないアプリケーションに対してのみ有効です。デリバリーグループに直接関連付けられているアプリケーションはすべてデフォルトでセッションを共有します。
- 1 つのアプリケーションが複数のアプリケーショングループに割り当てられている場合、グループどうしで設定が矛盾しないようにしてください。たとえば、同じオプションを一方のグループでは True に、他方のグループでは False に設定していると、予想のつかない動作を引き起こします。

アプリケーショングループ名の変更

1. ［管理］**>**［完全な構成］の左側ペインで ［アプリケーション］を選択してから、［アプリケーショングループ］タブを選択します。
2. アプリケーショングループを選択し、操作バーで ［アプリケーショングループ名を変更します］を選択します。
3. 新しい一意の名前を指定して、［**OK**］を選択します。

アプリケーショングループとデリバリーグループの関連付けの追加、削除、または優先度変更

アプリケーショングループは、アプリケーションを配信可能な共有（プライベートではない）マシンが含まれるデリバリーグループに関連付けることができます。

次の両方の条件が満たされている場合は、デスクトップのみを配信する共有マシンが含まれるデリバリーグループを選択することもできます：

- デリバリーグループは、共有マシンが含まれ、7.9 より前のバージョンで作成されたものです。
- デリバリーグループの編集権限があります。

デリバリーグループの種類は、［アプリケーショングループを編集します］ダイアログボックスが表示されると、自動的に「デスクトップとアプリケーション」に変換されます。

1. ［管理］**>**［完全な構成］の左側ペインで ［アプリケーション］を選択してから、［アプリケーショングループ］タブを選択します。
2. アプリケーショングループを選択し、操作バーで ［アプリケーショングループを編集します］を選択します。
3. ［デリバリーグループ］ページを選択します。
4. デリバリーグループを追加するには、［追加］を選択します。使用可能なデリバリーグループのチェックボックスをオンにします（互換性のないデリバリーグループは選択できません）。選択が完了したら、［**OK**］を選択します。
5. デリバリーグループを削除するには、削除するグループのチェックボックスをオンにして、［削除］を選択します。確認のメッセージが表示されたら、削除を確定します。
6. デリバリーグループの優先度を変更するには、デリバリーグループのチェックボックスをオンにして、［優先度の編集］を選択します。優先順位（0 が最高）を入力し、［**OK**］を選択します。
7. ［適用］を選択して行った変更を適用しウィンドウを開いたままにするか、［**OK**］を選択して変更を適用しウィンドウを閉じます。

アプリケーショングループのタグ制限の追加、変更、または削除

タグによる制限を追加、変更、および削除すると、どのマシンがアプリケーション起動の対象となるかについて、予期しない結果を招くことがあります。「タグ」に記載されている考慮事項と注意を確認してください。

1. ［管理］**>**［完全な構成］の左側ペインで ［アプリケーション］を選択してから、［アプリケーショングループ］タブを選択します。
2. アプリケーショングループを選択し、操作バーで ［アプリケーショングループを編集します］を選択します。
3. ［デリバリーグループ］ページを選択します。
4. タグ制約を追加するには、［タグでマシンの起動を制限します：］を選択し、メニューからタグを選択します。
5. タグ制約を変更または削除するには、異なるタグをメニューから選択するか、［次のタグを持つマシンに起動を制約する：］をオフにして、タグ制約を削除します。
6. ［適用］を選択して行った変更を適用しウィンドウを開いたままにするか、［**OK**］を選択して変更を適用しウィンドウを閉じます。

アプリケーショングループのユーザーの追加または削除

ユーザーについて詳しくは、「アプリケーショングループの作成」を参照してください。

1. ［管理］**>**［完全な構成］の左側ペインで ［アプリケーション］を選択してから、［アプリケーショングループ］タブを選択します。
2. アプリケーショングループを選択し、操作バーで ［アプリケーショングループを編集します］を選択します。
3. ［ユーザー］ページを選択します。アプリケーショングループ内のアプリケーションの使用を、関連付けられたデリバリーグループ内のすべてのユーザーに許可するか、特定のユーザーおよびグループにのみ許可するかを指定します。ユーザーを追加するには、［追加］を選択し、追加するユーザーを指定します。ユーザーを削除する場合は、1 人または複数のユーザーを選択し、［削除］を選択します。
4. ［適用］を選択して行った変更を適用しウィンドウを開いたままにするか、［**OK**］を選択して変更を適用しウィンドウを閉じます。

アプリケーショングループのアプリケーションアイコンの追加、変更、または削除

アプリケーションアイコンを追加、変更、または削除するには、次の手順を実行します。

1. ナビゲーションペインで ［アプリケーション］を選択します。
2. ［すべてのアプリケーション］タブで ［プロパティ］を選択します。

   アプリケーショングループレベルで変更を加えるには、［アプリケーショングループ］タブに移動し、グループ内のアプリケーションを選択して、［プロパティ］を選択します。
3. ［デリバリー］ページを選択してから、［変更］を選択します。［アイコンの選択］ウィンドウが開きます。
4. ［アイコンの選択］ウィンドウで、次のいずれかを実行します:

   - アイコンを追加するには、［追加］を選択して、対象のアイコンを参照します。
   - アイコンを削除するには、対象のアイコンを選択して、［削除］を選択します。
   - アイコンを変更するには、対象アプリケーション用のアイコンを選択します。

   > 重要:
   >
   > - サイズが 200KB を超えるアイコンを追加することはできません。
   > - 追加できるのは.icon ファイルのみです。
   > - 組み込みのアイコンは削除できません。
   > - 使用中のアプリケーションのアイコンを削除することはできません。
5. ［**OK**］を選択して、変更を適用してウィンドウを閉じます。

アプリケーショングループのスコープの変更

スコープの変更は、スコープを作成済みの場合のみ行うことができます（［すべて］のスコープを編集することはできません）。詳しくは、「管理者権限の委任」を参照してください。

1. ［管理］**>**［完全な構成］の左側ペインで ［アプリケーション］を選択してから、［アプリケーショングループ］タブを選択します。
2. 中央ペインでアプリケーショングループを選択し、操作バーで ［アプリケーショングループを編集します］を選択します。
3. ［スコープ］ページを選択します。変更するスコープの横にあるチェックボックスをオンまたはオフにします。
4. ［適用］を選択して行った変更を適用しウィンドウを開いたままにするか、［**OK**］を選択して変更を適用しウィンドウを閉じます。

アプリケーショングループの削除

アプリケーションは、デリバリーグループかアプリケーショングループの少なくとも 1 つに割り当てる必要があります。アプリケーショングループの削除により 1 つまたは複数のアプリケーションがグループに属していない状態になる場合は、グループを削除するとこれらのアプリケーションも削除されることを通知する警告メッセージが表示されます。削除を確定またはキャンセルすることができます。

アプリケーションを削除しても、元のソースからは削除されません。ただし、再度使用可能にする場合は、再度追加する必要があります。

1. ［管理］**>**［完全な構成］の左側ペインで ［アプリケーション］を選択してから、［アプリケーショングループ］タブを選択します。
2. アプリケーショングループを選択し、操作バーで ［グループの削除］を選択します。
3. 確認のメッセージが表示されたら、削除を確定します。

フォルダーを使用したアプリケーショングループの整理

簡単にアクセスできるように、フォルダーを作成してアプリケーショングループを整理できます。

必須の役割

デフォルトでは、アプリケーショングループのフォルダーを作成および管理するには、次の組み込みの役割のいずれかが必要です:

- クラウド管理者
- すべての管理権限を実行できる管理者
- アプリケーショングループ管理者

カスタム役割を作成することで、管理アクションを他のユーザーに委任できます。次の表に、各アクションに必要な権限を示します。

操作	必要な権限
アプリケーショングループフォルダーを作成する	アプリケーショングループフォルダーの作成
アプリケーショングループフォルダーを削除する	アプリケーショングループフォルダーの削除
アプリケーショングループフォルダーを移動する	アプリケーショングループフォルダーの移動
アプリケーショングループフォルダーの名前を変更する	アプリケーショングループフォルダーの編集
アプリケーショングループをフォルダーに移動する	アプリケーショングループフォルダーの編集、アプリケーショングループのプロパティの編集

詳しくは、「役割の作成と管理」を参照してください。

フォルダーの作成と管理

操作バーまたは右クリックメニューを使用して、アプリケーショングループフォルダーを作成および管理できます。さらに、アプリケーショングループまたはフォルダーをフォルダーツリー内の目的の場所にドラッグできます。

ヒント:

- 最大で 5 レベルまでの階層構造でフォルダーをネストできます（デフォルトのルートフォルダーを除く）。
- フォルダーには、アプリケーショングループとサブフォルダーを含めることができます。フォルダーの削除は、フォルダーとそのサブフォルダーにアプリケーショングループが含まれていない場合にのみ可能となります。
- バックエンドのフォルダーツリーは、[完全な構成] のすべてのリソース（マシンカタログ、デリバリーグループ、アプリケーション、およびアプリケーショングループなど）で共有されます。フォルダーの名前変更や移動時に他のリソースフォルダーと名前が競合しないように、異なるフォルダーツリーの第 1 レベルのフォルダーには異なる名前を付けることをお勧めします。

リモート PC アクセス

July 25, 2023

> 注:
>
> この記事では、[完全な構成] インターフェイスを使用してリモート PC アクセスを構成する方法について説明します。[クイック展開] インターフェイスを使用する場合は、「クイック展開でのリモート PC アクセス」のガイダンスに従ってください。

リモート PC アクセスは Citrix Virtual Apps and Desktops の機能であり、組織で従業員が安全な方法でリモートから企業リソースに簡単にアクセスできるようにします。Citrix プラットフォームでは、ユーザーが社内の物理的な

PC にアクセスできるようにすることで、この安全なアクセスを可能にします。ユーザーが社内 PC にアクセスできる場合、作業に必要なすべてのアプリケーション、データ、リソースにアクセスできます。リモート PC アクセスにより、テレワークに対応するために他のツールを導入したり提供したりする必要がなくなります。たとえば、仮想デスクトップまたはアプリケーション、および関連するインフラストラクチャなどです。

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

この機能は、種類がリモート **PC** アクセスのマシンカタログで構成され、次の機能が提供されます:

- OU を指定してマシンを追加する機能。この機能によって PC の一括追加を円滑に実行できます。
- CSV ファイルを使用してマシンを追加する機能。この機能により、OU 構造が制限されているシナリオで PC を一括で追加できます。
- 社内の Windows PC にログインするユーザーに基づいた自動ユーザー割り当て。単一ユーザーおよび複数ユーザーの割り当てをサポートしています。デフォルトでは、複数のユーザーが次の未割り当てのマシン: に自動的に割り当てられます。自動割り当てを 1 人のユーザーに制限するには、［完全な構成］**>**［設定］に移動して、［リモート **PC** アクセスの複数ユーザー自動割り当てを有効にする］設定をオフにします。

Citrix Virtual Apps and Desktops では、他の種類のマシンカタログを使用することで、物理 PC のユースケースが増えます。これらのユースケースには次のようなものがあります:

- 物理 Linux PC
- プールされた物理 PC（ランダムに割り当てられ、専用ではありません）

> 注:
>
> サポートされている OS バージョンについて詳しくは、VDA のシステム要件（「シングルセッション OS」と「Linux VDA」）を参照してください。
>
> オンプレミス展開の場合、リモート PC アクセスは、Citrix DaaS の Advanced または Premium ライセンスでのみ有効です。セッションでは、他の Citrix Virtual Desktops セッションと同様にライセンスが消費されます。Citrix Cloud の場合、リモート PC アクセスは、Citrix DaaS および Workspace Premium Plus で有効です。

注意事項

Citrix Virtual Apps and Desktops および Citrix DaaS 全般に適用される技術的要件および考慮事項はすべて、リモート PC アクセスにも適用されますが、一部は物理 PC のユースケースに対してより関連性があるか、または排他的な場合もあります。

> 重要:
>
> Windows 11（と一部の Windows 10 を実行している）物理システムには仮想化ベースのセキュリティ機能が含まれているため、VDA ソフトウェアがそれらを仮想マシンとして誤って検出します。この問題を緩和するには、次のオプションがあります。
>
> - VDA コマンドラインを使用したインストールで、「/physicalmachine」オプションを「/remotepc」オプションとともに使用します。
> - 前述のオプションを使用しなかった場合は、VDA のインストール後に次のレジストリ値を追加します `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`
>
> - 名前：ForceEnableRemotePC
> - 種類：DWORD
> - データ：1

展開に関する考慮事項

リモート PC アクセスの導入を計画する際は、以下の全般的な項目について判断してください。

- 既存の Citrix Virtual Apps and Desktops および Citrix DaaS 展開にリモート PC アクセスを追加できます。このオプションを選択する前に、以下の点を考慮してください:
  - リモート PC アクセスの VDA に関連する追加の負荷をサポートするために、現在の Delivery Controller または Cloud Connector のサイズは適切か?
  - オンプレミスのサイトデータベースとデータベースサーバーは、リモート PC アクセスの VDA に関連する追加の負荷をサポートするために適切なサイズか?
  - 既存の VDA と新しいリモート PC アクセスの VDA は、サイトあたりサポートされる VDA の最大数を超えているか?
- VDA は、自動プロセスによって社内 PC に展開する必要があります。使用可能な 2 つのオプションは次のとおりです:
  - SCCM などの電子ソフトウェア配信（ESD）ツール：SCCM を使用した VDA のインストール。
  - 展開スクリプト：スクリプトを使用した VDA のインストール。
- 「リモート PC アクセスのセキュリティに関する考慮事項」を確認してください。

マシンカタログに関する考慮事項

必要なマシンカタログの種類は、ユースケースによって異なります:

- リモート PC アクセスのマシンカタログ
  - Windows/Linux 専用 PC

  - Windows/Linux 専用マルチユーザー PC。このユースケースは、複数のユーザーが異なるシフトでリモートアクセスできる物理的なオフィス PC に当てはまります。
  - プールされた Windows/Linux PC。このユースケースは、コンピューターラボなど、複数のランダムユーザーがアクセスできる物理 PC に適用されます。

マシンカタログの種類を特定したら、次の点を考慮してください:

- リモート PC アクセスでは、1 つのマシンを複数のマシンカタログに同時に関連付けることはできません。
- 委任管理を円滑に進めるために、各カタログの管理を適切な管理者に容易に委任できる地理的な場所、部署、またはその他のグループに基づいて、マシンカタログを作成することを検討してください。
- マシンアカウントが存在する OU を選択する場合は、より細分化するために下位レベルの OU を選択します。このような細分性が必要ない場合は、上位レベルの OU を選択できます。たとえば、Bank/Officers/Tellers の場合、より細分性を高めるために **Tellers** を選択します。それ以外の場合は、要件に基づいて ［役員］または ［銀行］を選択できます。
- リモート PC アクセスマシンカタログに割り当てた後に OU を移動または削除すると、VDA の関連付けに影響し、今後の割り当てで問題が発生します。したがって、マシンカタログの OU 割り当ての更新が Active Directory 変更計画で考慮されるように、適切な計画を立ててください。
- OU を選択して、マシンをマシンカタログに一括で追加できます。一部のシナリオでは、OU 構造の制限のため、これを行うのは簡単ではありません。代わりに、CSV ファイルを使用してマシンを一括で追加できます。この機能により、マシンを一括追加する柔軟性が得られます。（ユーザーの自動割り当てで使用するため）マシンのみを追加することも、ユーザーの割り当てとともにマシンを追加することもできます。
- 統合された Wake on LAN は、リモート **PC** アクセスタイプのマシンカタログでのみ使用できます。

Linux VDA に関する考慮事項

次の考慮事項は、Linux VDA に固有のものです:

- リモート PC アクセス VDA の物理モニターのブランキングは使用できますが、すべての Linux ディストリビューションで使用できるわけではありません。サポートされていない Linux ディストリビューションの場合、非 3D モードの物理マシンでのみ Linux VDA を使用してください。または、NVIDIA のドライバーの制限により、HDX 3D モードが有効になっている場合、PC のローカル画面は黒い表示にならず、画面にはセッションのアクティビティが表示されます。この画面の表示は、セキュリティ上のリスクです。
- 物理 Linux マシンには、シングルセッション OS タイプのマシンカタログを使用することをお勧めします。

技術的な要件および考慮事項

このセクションでは、物理 PC の技術要件と考慮事項について説明します。

- 以下はサポートされていません:
  - KVM スイッチ、またはセッションを切断する可能性のあるそのほかのコンポーネント。

  - ハイブリッド PC（オールインワンおよび NVIDIA Optimus ノートブックおよび PC を含む）。
  - デュアルブートマシン。

- キーボードとマウスを PC に直接接続します。電源を切ったり接続を切断したりできるモニターなどのコンポーネントに接続すると、これらの周辺機器が使用できなくなることがあります。キーボードやマウスをモニターなどのデバイス経由で接続する必要がある場合は、それらのコンポーネントの電源をオフにしないでください。
- PC は Active Directory ドメインサービスドメインに参加している必要があります。
- セキュアブートは Windows 10 でのみサポートされています。
- PC にはアクティブなネットワーク接続が必要です。信頼性と帯域幅を高めるには、有線接続をお勧めします。
- Wi-Fi を使用する場合、以下の点を確認します：

  1. 電源設定でワイヤレスアダプターの電源を入れたままにするようにします。
  2. ユーザーがサインインする前にワイヤレスネットワークに自動的に接続できるように、ワイヤレスアダプターとネットワークプロファイルを構成します。そうしないと、ユーザーがログオンするまで VDA は登録されません。ユーザーがログオンするまで、PC ではリモートアクセスを使用できません。
  3. Wi-Fi ネットワークから Delivery Controller または Cloud Connector にアクセスできることを確認してください。

- リモート PC アクセスはノートブックコンピューターで使用できます。ノートブックがバッテリーで動作しているのではなく、電源に接続されていることを確認します。デスクトップ PC のオプションに合わせて、ノートブックの電源オプションを構成します。例：

  1. 休止機能を無効にする。
  2. スリープ機能を無効にする。
  3. カバーを閉じた場合の動作を ［何もしない］ に設定する。
  4. 電源ボタンを押したときの操作を ［シャットダウン］ に設定する。
  5. ビデオカードおよび NIC の省電力設定を無効にする。

- リモート PC アクセスは、Surface Pro デバイス上の Windows 10 でサポートされます。前述のノートブックと同じガイドラインに従います。
- ドッキングステーションを使用している場合、ノートブックをドッキング解除して再接続できます。ドッキング解除すると、VDA は Wi-Fi で Delivery Controller または Cloud Connector に再登録されます。ただし、ノートブックを再接続した場合、ワイヤレスアダプターを外さない限り、VDA は有線接続を使用するように切り替わりません。有線接続が確立されると、組み込まれた機能がワイヤレスアダプターを切断するデバイスもあります。それ以外のデバイスでは、ワイヤレスアダプターを切断するためのカスタムソリューションかサードパーティ製のユーティリティが必要です。前述の Wi-Fi に関する考慮事項を確認してください。

  デバイスのリモート PC アクセスでドッキングとドッキング解除を有効にするには、以下の操作を実行します：

  1. ［スタート］ メニューの ［設定］ **>** ［システム］ **>** ［電源とスリープ］ で ［スリープ］ を ［なし］ に設定します。

2. ［デバイスマネージャー］**>**［ネットワーク アダプター］**>**［イーサネットアダプター］の［電源管理］で［電力の節約のために、コンピューターでこのデバイスの電源をオフにできるようにする］に移動します。［このデバイスで、コンピューターのスタンバイ状態を解除できるようにする］チェックボックスがオンになっていることを確認します。

- 同じ社内 PC にアクセスする複数のユーザーには、Citrix Workspace で同じアイコンが表示されます。ユーザーが Citrix Workspace にログオンすると、そのリソースが他のユーザーによって既に使用されている場合は使用不可と表示されます。
- 社内 PC へアクセスする各クライアントデバイス（自宅の PC など）に、Citrix Workspace アプリをインストールします。

構成の順序

このセクションでは、リモート **PC** アクセスタイプのマシンカタログを使用する場合にリモート PC アクセスを構成する方法の概要について説明します。他のタイプのマシンカタログを作成する方法については、「マシンカタログの作成」を参照してください。

1. オンプレミスサイトのみ - 統合された Wake on LAN 機能を使用するには、「Wake on LAN」で説明されている前提条件を構成します。
2. リモート PC アクセス用に新しい Citrix Virtual Apps and Desktops サイトが作成された場合：

   a) リモート **PC** アクセスサイトの種類を選択します。
   b) 管理者は、［電源管理］ページで、デフォルトのリモート PC アクセスマシンカタログのマシンの電源管理機能を有効または無効にできます。この設定は、後でマシンカタログのプロパティを編集して変更できます。Wake on LAN の構成について詳しくは、「Wake on LAN」を参照してください。
   c)「ユーザー」ページと「マシンアカウント」ページの情報を入力します。

   これらの手順を完了すると、「リモート **PC** アクセスマシン」という名前のマシンカタログと、「リモート **PC** アクセスデスクトップ」という名前のデリバリーグループが作成されます。

3. 既存の Citrix Virtual Apps and Desktops サイトに追加する場合：

   a) リモート **PC** アクセスタイプのマシンカタログを作成します（ウィザードの［オペレーティングシステム］ページ）。マシンカタログの作成方法について詳しくは、「マシンカタログの作成」を参照してください。ターゲットの PC をリモート PC アクセスで使用できるように、正しい組織単位が割り当てられていることを確認します。
   b) デリバリーグループを作成して、ユーザーがマシンカタログの PC にアクセスできるようにします。デリバリーグループの作成方法について詳しくは、「デリバリーグループの作成」を参照してください。PC へのアクセスが必要なユーザーが含まれる Active Directory グループにこのデリバリーグループを割り当てます。

4. VDA を社内 PC に展開します。

- シングルセッション OS コア VDA インストーラー（`VDAWorkstationCoreSetup.exe`）を使用することをお勧めします。
- シングルセッション OS フル VDA インストーラー（`VDAWorkstationSetup.exe`）を`/remotepc /physicalmachine`オプションで使用することもできます。これにより、コア VDA インストーラーを使用する場合と同じ結果が得られます。
- ヘルプデスクチームが Citrix Director を通じてリモートサポートを提供できるように、Windows リモートアシスタンスを有効にすることを検討してください。そのために、`/enable_remote_assistance`オプションを使用します。詳しくは、「コマンドラインを使ったインストール」を参照してください。
- Director でログオン時間情報を表示するには、シングルセッション完全版 VDA インストーラーを使用して **Citrix User Profile Management WMI Plugin** コンポーネントを含める必要があります。`/includeadditional`オプションを使用してこのコンポーネントを含めます。詳しくは、「コマンドラインを使ったインストール」を参照してください。
- SCCM を使用した VDA の展開については、「SCCM を使用した VDA のインストール」を参照してください。
- 展開スクリプトを使用した VDA の展開については、「スクリプトを使用した VDA のインストール」を参照してください。

手順 2〜4 を正常に完了すると、ユーザーが PC にローカルでログインしたときに、自動的にマシンが割り当てられます。

5. 社内 PC へのリモート接続で使用する各クライアントデバイスに、Citrix Workspace アプリをダウンロードしインストールするようユーザーに指示します。Citrix Workspace アプリは Citrix のダウンロードサイトから、またはサポートされるモバイルデバイス向けのアプリストアから入手できます。

レジストリで管理される機能

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

スリープモード（バージョン **7.16** 以降）

リモート PC アクセスマシンがスリープ状態に入ることを許可するには、このレジストリ設定を VDA に追加してからマシンを再起動します。再起動後は、オペレーティングシステムの省電力設定が優先されます。設定済みのアイドルタイマー間隔が経過すると、マシンはスリープモードに入ります。マシンがスリープモードから復帰すると、Delivery Controller に再登録されます。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 値の名前：DisableRemotePCSleepPreventer
- 種類：DWORD
- データ：1

セッション管理

デフォルトでは、ローカルユーザーがそのマシンで Ctrl+Alt+Del キーを押してセッションを開始すると、リモートユーザーのセッションは自動的に切断されます。自動的に切断されないようにするには、社内 PC に次のレジストリエントリを追加してから、マシンを再起動します。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- 値の名前：SasNotification
- 種類：DWORD
- データ：1

デフォルトでは、接続メッセージがタイムアウト期間内に承認されなかった場合にリモートユーザーがローカルユーザーより優先されます。この動作を構成するには、次の設定を使用します：

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- 値の名前：RpcaMode
- 種類：DWORD
- データ：
  - 1 - 指定のタイムアウト期間に Messaging UI へ応答しない場合、リモートユーザーが常に優先されます。この設定が構成されていない場合、この動作がデフォルトです。
  - 2 - ローカルユーザーが優先されます。

リモート PC アクセスモードを強制するまでのタイムアウト期間はデフォルトでは 30 秒です。このタイムアウト期間は変更できますが、30 秒より短く設定しないでください。タイムアウトを構成するには、次のレジストリ設定を使用します：

`HKLM\SOFTWARE\Citrix\PortICA\RemotePC`

- 値の名前：RpcaTimeout
- 種類：DWORD
- データ：10 進数のタイムアウト値（秒単位）

ユーザーがコンソールに強制的にアクセスできるようにするには：ローカルユーザーが Ctrl+Alt+Del キーを 10 秒以内に 2 回押すことによって、リモートセッションのローカル制御を取得して切断イベントを強制的に発生します。

レジストリを変更してマシンを再起動した後に、リモートユーザーが使用中の PC にローカルユーザーが Ctrl+Alt+Del キーを押してログオンすると、プロンプトがリモートユーザーに表示されます。このプロンプトは、ローカルユーザーの接続を許可するか拒否するかを尋ねます。接続を許可すると、リモートユーザーのセッションは切断されます。

Wake-on-LAN

リモート PC アクセスでは Wake on LAN がサポートされ、物理 PC をリモートから起動できます。この機能により、ユーザーが退社時に PC の電源をオフにできるようになるため、消費電力を節約できます。また、電源が突然オフになった PC にもリモートアクセスできるようになります。

Wake on LAN 機能を使用すると、Delivery Controller の指示に従って、PC 上で実行中の VDA から PC が存在するサブネットにマジックパケットが直接送信されます。これにより、マジックパケットを配信するための追加のインフラストラクチャコンポーネントまたはサードパーティ製ソリューションに依存することなく、Wake on LAN 機能を実行できます。

Wake on LAN 機能は、従来の SCCM ベースの Wake on LAN 機能とは異なります。SCCM 統合 Wake on LAN は、リモート PC アクセスの代替 Wake on LAN オプションであり、オンプレミスの Citrix Virtual Apps and Desktops でのみ使用できます。SCCM ベースの Wake on LAN については、「Wake on LAN –SCCM 統合」を参照してください。

システム要件

以下は、Wake on LAN 機能を使用するためのシステム要件です:

- コントロールプレーン:
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2009 以降
- 物理 PC:
  - VDA バージョン 2009 以降
  - Windows10 または Windows11。サポートの詳細については、「VDA のシステム要件」を参照してください。
  - BIOS/UEFI で Wake on LAN が有効になっている
  - Windows 構成内のネットワークアダプターのプロパティで Wake on LAN が有効になっている

Wake on LAN の構成

Wake on LAN を構成するために、［完全な構成］管理インターフェイスまたは PowerShell を使用できます。

完全な構成インターフェイスを使用して **Wake on LAN** を構成する　Wake on LAN 接続を作成するには:

1. 左側の ［ホスト］ノードに移動します。
2. ［接続およびリソースの追加］を選択します。
3. ウィザードの ［接続］ページで、次の情報を入力します:

a) 接続の種類：リモート PC Wake on LAN
b) ゾーン名：リモート PC アクセスカタログが存在するゾーンを選択します
c) 接続名：Wake on LAN 接続名を入力します

4. 接続およびリソースの追加ウィザードで、残りの手順を完了します。

Wake on LAN 接続をリモート PC アクセスのマシンカタログに追加するには：

1. 新しいリモート PC アクセスのマシンカタログを作成する場合は、ドロップダウンリストを使用して、マシンカタログインストールウィザードの ［マシンの種類］ページで、接続を追加できます。
2. Wake on LAN 接続を既存のマシンカタログに追加する場合：

a) 左側の ［マシンカタログ］ノードに移動します。
b) 適切なリモート PC アクセスのマシンカタログを選択します。
c) マシンカタログを右クリックするか、上の ［その他］メニューを選択します。
d)［マシンカタログの編集］を選択します。
e)［電源管理］ページで ［はい］を選択します。
f) ドロップダウンリストから適切な接続を選択します。
g)［**Save**］を選択します。

> 注：
>
> ［完全な構成］インターフェイスを使用した Wake on LAN の構成は、現時点では Citrix DaaS でのみ使用できます。

PowerShell を使用して **Wake on LAN** を構成する　PowerShell を使用して Wake on LAN を構成するには：

1. リモート PC アクセスマシンカタログをまだ作成していない場合は作成します。
2. Wake on LAN ホスト接続をまだ作成していない場合は作成します。
3. Wake on LAN ホスト接続の一意の識別子を取得します。
4. Wake onLAN ホスト接続をマシンカタログに関連付けます。

Wake on LAN ホスト接続を作成するには：

```
# Load Citrix SnapIns
Add-PSSnapIn -Name "\*citrix\*"

# Provide the name of the Wake on LAN host connection
[string]$connectionName = "Remote PC Access Wake on LAN"

# Create the hypervisor connection
$hypHc = New-Item -Path xdhyp:\Connections `
                -Name $connectionName `
                -HypervisorAddress "N/A" `
                -UserName "woluser" `
                -Password "wolpwd" `
                -ConnectionType Custom `
```



```
                -PluginId VdaWOLMachineManagerFactory `
                -CustomProperties "<CustomProperties></CustomProperties
                    >" `
                -Persist

$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
    $hypHc.HypervisorConnectionUid

# Wait for the connection to be ready before trying to use it
while (-not $bhc.IsReady)
{

    Start-Sleep -s 5
    $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
        $hypHc.HypervisorConnectionUid
 }

<!--NeedCopy-->
```

ホスト接続の準備ができたら、次のコマンドを実行して、ホスト接続の一意の識別子を取得します:

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"
$hypUid = $bhc.Uid
<!--NeedCopy-->
```

接続の一意の識別子を取得したら、次のコマンドを実行して、その接続をリモート PC アクセスマシンカタログに関連付けます:

```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog -
    RemotePCHypervisorConnectionUid $hypUid
<!--NeedCopy-->
```

設計上の考慮事項

リモート PC アクセスで Wakeon LAN を使用する場合は、次の点を考慮してください:

- 複数のマシンカタログでは同じ Wake on LAN ホスト接続を使用できます。
- PC が別の PC をウェイクアップするには、両方の PC が同じサブネット内にあり、同じ Wake on LAN ホスト接続を使用する必要があります。PC が同じマシンカタログにあるか、別のマシンカタログにあるかは関係ありません。
- ホスト接続は特定のゾーンに割り当てられます。環境に複数のゾーンがある場合は、各ゾーンに Wake on LAN ホスト接続が必要です。同じことがマシンカタログにも当てはまります。
- マジックパケットは、グローバルブロードキャストアドレス 255.255.255.255 を使用してブロードキャスト配信されます。このアドレスがブロックされていないことを確認してください。
- そのサブネット内のマシンをウェイクアップできるようにするには、サブネット内で（Wake on LAN 接続ごとに）少なくとも 1 台の PC がオンになっている必要があります。

運用上の考慮事項

以下は、Wake on LAN 機能を使用する場合の考慮事項です:

- 統合された Wake on LAN 機能を使用して PC をウェイクアップするには、VDA を少なくとも 1 回登録する必要があります。
- Wake on LAN は、PC のウェイクアップにのみ使用できます。再起動やシャットダウンなど、他の電源操作はサポートしていません。
- マジックパケットは、次の 2 つの方法のいずれかで送信されます:

  1. ユーザーが PC へのセッションを開始しようとしたときに、VDA が登録解除されている場合
  2. 管理者が［完全な構成］インターフェイスまたは PowerShell から電源オンのコマンドを手動で送信する場合

- Delivery Controller は PC の電源の状態を認識しないため、［完全な構成］インターフェイスでは電源の状態のところに ［サポートされていません］と表示されます。Delivery Controller は、VDA 登録状態を使用して PC がオンかオフかを判断します。

トラブルシューティング

モニターのブランキングが機能しない

アクティブな HDX セッションがあるときに Windows PC のローカルモニターが空白になっていない場合（ローカルモニターはセッションで発生していることを表示します）、GPU ベンダーのドライバーに問題があることが原因である可能性があります。この問題を解決するには、次のレジストリ値を設定して、Citrix Indirect Display ドライバー（IDD）にグラフィックカードのベンダードライバーよりも高い優先度を与えます:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits`

- 名前: CitrixIDD
- 種類: DWORD
- データ: 3

ディスプレイアダプターの優先度とモニターの作成について詳しくは、Knowledge Center のCTX237608を参照してください。

セッション管理通知が有効になっているマシンで **Ctrl+Alt+Del** を選択すると、セッションが切断される

レジストリ値 **SasNotification** によって制御されるセッション管理通知は、VDA でリモート PC アクセスモードが有効になっている場合にのみ機能します。物理 PC で Hyper-V の役割または仮想化ベースのセキュリティ機能が有効になっている場合、PC は仮想マシンとして報告します。VDA が仮想マシン上で実行されていることを検出すると、リモート PC アクセスモードが自動的に無効になります。リモート PC アクセスモードを有効にするには、次のレジストリ値を追加します:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA

- 名前：ForceEnableRemotePC
- 種類：DWORD
- データ：1

設定を有効にするには、PC を再起動します。

診断情報

リモート PC アクセスの診断情報は、Windows のアプリケーションイベントログに書き込まれます。情報メッセージは調整されません。エラーメッセージは重複メッセージの破棄により調整されます。

- 3300（情報）：マシンカタログへのマシンの追加
- 3301（情報）：デリバリーグループへのマシンの追加
- 3302（情報）：ユーザーへのマシンの割り当て
- 3303（エラー）：例外の発生

電源の管理

リモート PC アクセス用の電源管理を有効にすると、サブネット向けのブロードキャストでのマシンの起動に失敗することがあります。この問題は、Controller とマシンが異なるサブネット上に存在する場合に発生します。AMT がサポートされない場合に異なるサブネット間でサブネット向けのブロードキャストを使用するには、ウェイクアッププロキシまたはユニキャストを使用してください。これらの詳細設定は、電源管理接続のプロパティで有効にできます。

アクティブなリモートセッションは、ローカルのタッチスクリーン入力を記録します

VDA でリモート PC アクセスモードを有効にすると、アクティブなセッション中にローカルタッチスクリーン入力が無視されます。物理 PC で Hyper-V の役割または仮想化ベースのセキュリティ機能が有効になっている場合、PC は仮想マシンとして報告します。VDA が仮想マシン上で実行されていることを検出すると、リモート PC アクセスモードが自動的に無効になります。リモート PC アクセスモードを有効にするには、次のレジストリ設定を追加します：

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA

- 名前：ForceEnableRemotePC
- 種類：DWORD
- データ：1

設定を有効にするには、PC を再起動します。

その他のリソース

リモート PC アクセスのその他のリソースは次のとおりです:

- ソリューション設計ガイダンス:「リモート PC アクセス設計の決定」。
- リモート PC アクセスアーキテクチャの例:「Citrix のリモート PC アクセスソリューションのリファレンスアーキテクチャ」。

コンポーネントの削除

February 24, 2023

インストール済みのコンポーネント（VDA など）を削除するには、プログラムの削除（アンインストール）や変更を行う Windows の機能を使用することをお勧めします。または、コマンドラインかスクリプトを使用してコンポーネントを削除することもできます。

コンポーネントをアンインストールしても、そのコンポーネントと一緒にインストールされたサードパーティ製ソフトウェアはアンインストールされず、ファイアウォール設定も変更されません。

VDA を削除すると、削除後にデフォルトでマシンが自動的に再起動します。

プログラムの削除や変更を行う **Windows** の機能を使用してコンポーネントをアンインストールする

プログラムの削除や変更を行うための Windows 機能（コントロールパネルの［プログラムと機能］など）を開き、以下の操作を行います:

- VDA を削除するには、［**Citrix Virtual Delivery Agent** <*version*>］を選択し、右クリックしてから ［アンインストール］を選択します。インストーラーが起動したら、アンインストールするコンポーネントを選択します。
- ユニバーサルプリントサーバーをアンインストールするには、［**Citrix** ユニバーサルプリントサーバー］を選択してから右クリックし、［アンインストール］を選択します。

コマンドラインを使って **VDA** をアンインストールする

VDA のインストールに使用したコマンド（`VDAServerSetup.exe`、`VDAWorkstationSetup.exe`、または`VDAWorkstationCoreSetup.exe`）を実行します。構文の説明については、「コマンドラインを使用したインストール」を参照してください。

- VDA と Citrix Workspace アプリのどちらかのみをアンインストールするには、`/remove`および`/components`オプションを使用します。

- VDA と Citrix Workspace アプリの両方をアンインストールするには、/`removeall`オプションを使用します。

たとえば、マルチセッション OS マシンから VDA と Citrix Workspace アプリをアンインストールするには、次のコマンドを実行します。

```
VDAServerSetup.exe /removeall
```

また、シングルセッションOS マシンで Windows 向け Citrix Workspace アプリ（インストールされている場合）を残して VDA のみをアンインストールするには、次のコマンドを実行します。

```
VDAWorkstationSetup.exe /remove /components vda
```

また、シトリックスが用意したスクリプトを使用して VDA を削除することもできます。「スクリプトを使って VDA を削除する」を参照してください。

ユーザー個人設定レイヤー

February 9, 2024

Citrix Virtual Apps and Desktops のユーザー個人設定レイヤー機能は、非永続マシンカタログの機能を拡張し、セッション間でユーザーのデータとローカルにインストールされたアプリケーションを保持します。基盤となる Citrix App Layering テクノロジを活用して、ユーザー個人設定レイヤー機能は、永続的ではないマシンカタログの Citrix Provisioning と Machine Creation Services（MCS）をサポートします。

このユーザー個人設定レイヤーコンポーネントを、マスターイメージ内の Virtual Delivery Agent と一緒にインストールします。VHD ファイルには、ユーザーがインストールしたアプリケーションがローカルに格納されます。イメージにマウントされている VHD は、ユーザー独自の仮想ハードドライブとして機能します。

> 重要:
>
> Citrix Virtual Apps and Desktops にユーザー個人設定レイヤーを展開するか、イメージテンプレートで有効な App Layering ユーザーレイヤーを展開することができます。両方ではありません。App Layering 内のレイヤーにユーザー個人設定レイヤー機能をインストールしないでください。

これは、Personal vDisk（PvD）に代わる機能で、プールされた非永続的なデスクトップ環境のユーザーに、永続的なワークスペース環境を提供します。

ユーザー個人設定レイヤー機能を展開するには、この記事で説明されている手順を使用してユーザー個人設定レイヤー機能をインストールして構成します。それまでは、この機能は利用できません。

アプリケーションサポート

次の例外を除き、ユーザーがローカルでデスクトップにインストールするすべてのアプリケーションは、ユーザー個人設定レイヤーでサポートされます。

例外

次のアプリケーションは例外であり、ユーザー個人設定レイヤーでサポートされません：

- MS Office や Visual Studio などのエンタープライズアプリケーション。
- ネットワークスタックまたはハードウェアを変更するアプリケーション。例：VPN クライアント。
- ブートレベルのドライバーを備えたアプリケーション。例：ウイルススキャナー。
- ドライバーストアを使用するドライバーを備えたアプリケーション。例：プリンタードライバー。

  > 注：
  >
  > Windows グループポリシーオブジェクト（GPO）を使用して、プリンターを使用可能にすることができます。

ユーザーがサポートされていないアプリケーションをローカルでインストールできないようにしてください。このようなアプリケーションは、マスターイメージに直接インストールします。

ローカルユーザーまたは管理者アカウントを必要とするアプリケーション

ユーザーがアプリケーションをローカルにインストールすると、そのアプリケーションはユーザーレイヤーに入ります。その後、ユーザーがローカルユーザーやローカルグループを追加または編集した場合、その変更はセッションを超えて保持されません。

> 重要：
>
> 必要なローカルユーザーまたはグループをマスターイメージに追加します。

要件

ユーザー個人設定レイヤー機能には、次のコンポーネントが必要です：

- Citrix Virtual Apps and Desktops 7 1909 以降
- Virtual Delivery Agent（VDA）、バージョン 1912 以降
- Citrix Provisioning バージョン 1909 以降
- Windows ファイル共有（SMB）、またはオンプレミス AD 認証が有効な Azure ファイル

OS がシングルセッションとして展開されている場合、次の Windows バージョンにユーザー個人設定レイヤー機能を展開できます。サポートは、1 セッションの 1 ユーザーに制限されています。

- Windows 11 Enterprise x64
- Windows 10 Enterprise x64 バージョン 1607 以降
- Windows 10 マルチセッション（Azure ファイルをサポート）
- Windows Server 2016（Azure ファイルをサポート）

- Windows Server 2019（Azure ファイルをサポート）

Citrix Virtual Apps and Desktops 7 では、ユーザー個人設定レイヤーを持つ Azure ファイルの使用が、Windows Server 2019、Windows Server 2016v、および Windows 10 クライアントでサポートされています。

> 注:
>
> サーバー OS を使用している場合は、サーバー VDI のみがサポートされます。展開について詳しくは、「サーバー VDI」の記事を参照してください。
>
> ユーザー個人設定レイヤーは、マシンごとに一度に 1 人のユーザーのみをサポートします。その後、マシンを再起動してディスクをリセットする必要があります。マルチセッションサーバー OS ではユーザー個人設定レイヤーを使用することはできません。シングルセッションサーバーシステムでのみ使用できます。ユーザー個人設定レイヤーは、非永続デスクトップでのみ機能します。

ユーザー個人設定レイヤー機能がインストールされている場合は、アンインストールします。最新リリースをインストールする前に、マスターイメージを再起動してください。

ファイル共有の設定

ユーザー個人設定レイヤー機能には、Windows サーバーメッセージブロック（SMB）ストレージが必要です。Windows ファイル共有を作成するには、使用している Windows オペレーティングシステムの通常の手順に従います。

Azure ベースのカタログで Azure ファイルを使用する方法について詳しくは、「ユーザー個人設定レイヤー用の Azure Files ストレージの設定」を参照してください。

推奨事項

ユーザー個人設定レイヤーを展開するには、このセクションの推奨事項に従ってください。

Microsoft System Center Configuration Manager（SCCM）

ユーザー個人設定レイヤー機能を SCCM とともに使用している場合は、VDI 環境でイメージを準備するための Microsoft ガイドラインに従ってください。詳しくは、このMicrosoft TechNet の記事を参照してください。

ユーザーレイヤーサイズ

ユーザーレイヤーは、ディスク上の領域が使用されると拡張するシンプロビジョニングされたディスクです。ユーザーレイヤーのデフォルトのサイズは 10GB で、Citrix で推奨される最小サイズです。

> 注:
>
> インストール時にこの値がゼロ（0）に設定されている場合、デフォルトのユーザーレイヤーサイズは 10GB に設定されます。

ユーザーレイヤーサイズを変更する場合は、Studio の ［ユーザーレイヤーサイズ］ポリシーに別の値を入力してください。「オプション: ユーザーレイヤーサイズ（**GB**）の横の［選択］をクリックします」の「手順 **5**: デリバリーグループのカスタムポリシーの作成」を参照してください。

ユーザーレイヤーサイズを上書きするためのツール（オプション）

Windows のツールを使用して、ユーザーレイヤーファイル共有のクォータを定義することにより、ユーザーレイヤーサイズを上書きできます。

次の Microsoft クォータツールのいずれかを使用して、**Users** という名前のユーザーレイヤーディレクトリにハードクォータを設定します:

- ファイルサーバーリソースマネージャー（FSRM）
- クォータマネージャー

> 注:
>
> クォータを増やすと、新しいユーザーレイヤーに影響し、既存のユーザーレイヤーが拡張されます。クォータを減らすと、新しいユーザーレイヤーにのみ影響します。既存のユーザーレイヤーのサイズが小さくなることはありません。

ユーザー個人設定レイヤーの展開

ユーザー個人設定機能を展開する場合は、Studio 内でポリシーを定義します。次に、この機能が展開されているマシンカタログにバインドされているデリバリーグループにポリシーを割り当てます。

マスターイメージにユーザー個人設定レイヤーを構成しない場合、サービスはアイドル状態のままになり、オーサリングアクティビティに干渉しません。

マスターイメージでポリシーを設定すると、サービスが実行されてユーザーレイヤーをマスターイメージ内にマウントしようとします。この場合、マスターイメージは予期しない動作と不安定性を示します。

ユーザー個人設定レイヤー機能を展開するには、次の手順をこの順序で実行します:

- 手順 1: Citrix Virtual Apps and Desktops 環境の可用性を検証します。
- 手順 2: マスターイメージを準備します。
- 手順 3: マシンカタログを作成します。
- 手順 4: デリバリーグループを作成します。
- 手順 5: デリバリーグループのカスタムポリシーを作成します。

> 注:
>
> イメージで Windows 10 をアップグレードした後に初めてログオンすると、通常よりも時間がかかります。ユーザーのレイヤーを新しいバージョンの Windows 10 に合わせて更新する必要があるため、ログオン時間が長くなります。

手順 **1**: **Citrix Virtual Apps and Desktops** 環境の可用性を検証

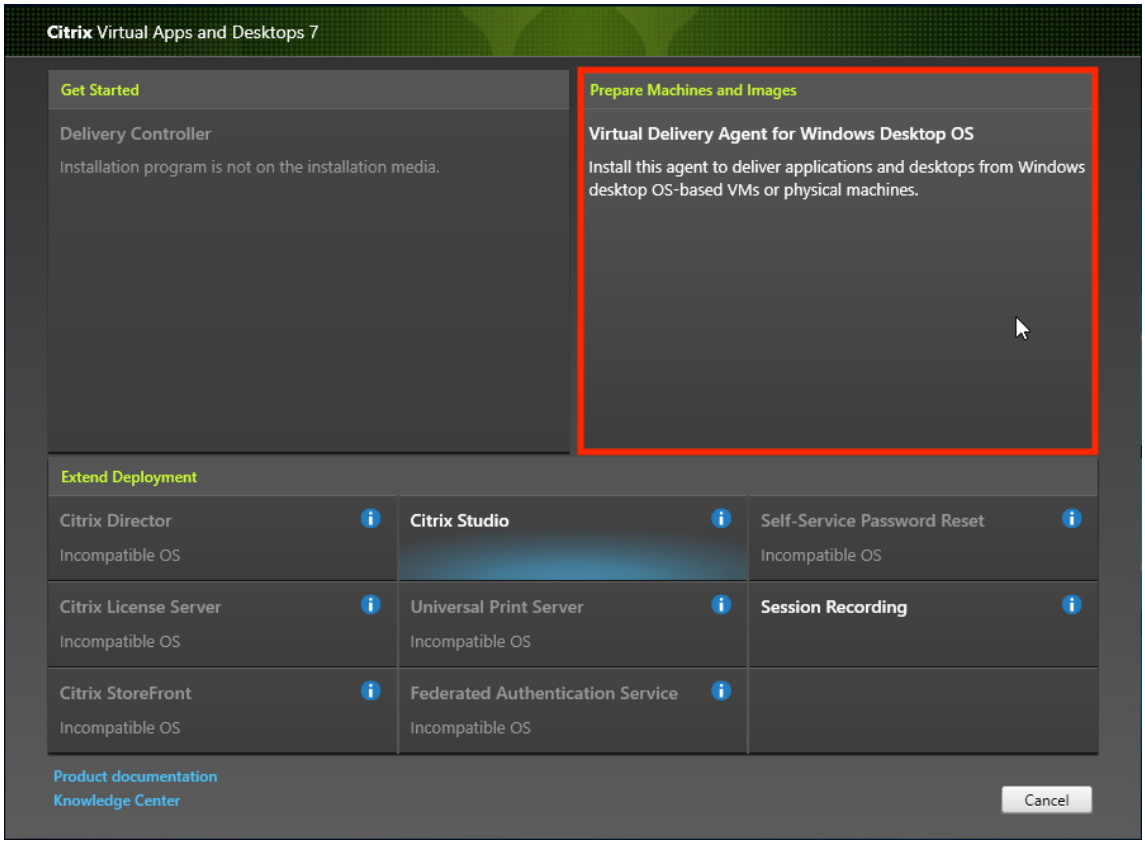
Citrix Virtual Apps and Desktops 環境でこの新機能を使用できることを確認してください。セットアップについて詳しくは、「Citrix Virtual Apps and Desktops のインストールと構成」を参照してください。

手順 **2**: マスターイメージの準備

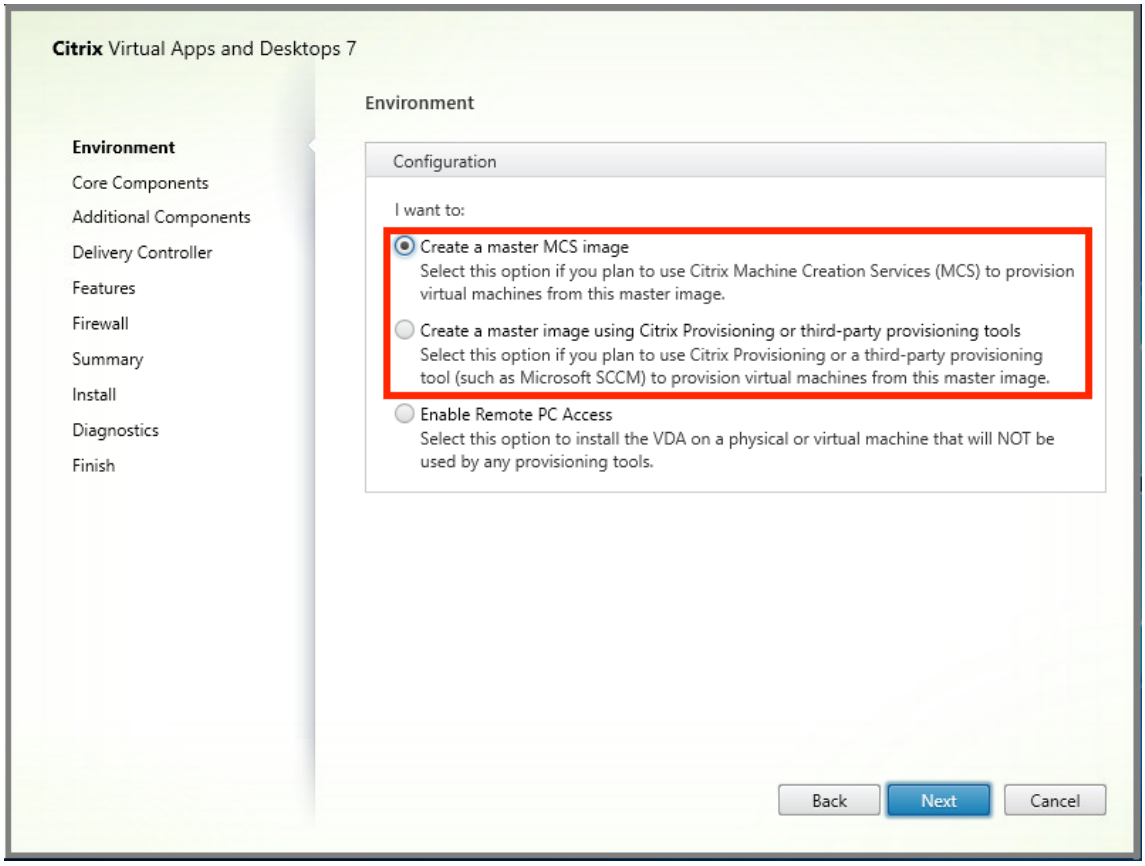
マスターイメージを準備するには:

1. マスターイメージを見つけます。組織のエンタープライズアプリケーションと、一般的にユーザーが有用だと見なすその他のアプリをインストールします。
2. サーバー VDI を展開する場合は、「サーバー VDI」に記載の手順に従ってください。オプションのコンポーネントであるユーザー個人設定レイヤーが含まれていることを確認します。詳しくは、「VDA のインストールで使用するコマンドラインオプション」を参照してください。
3. Windows 10 を使用している場合は、Virtual Delivery Agent（VDA）1912 以降をインストールします。古いバージョンの VDA が既にインストールされている場合は、最初に古いバージョンをアンインストールします。新しいバージョンをインストールするときは、次のようにオプションのコンポーネントである **Citrix** ユーザー個人設定レイヤーを選択してインストールしてください:

    a) [**Virtual Delivery Agent for Windows Desktop OS**] のタイルをクリックします:

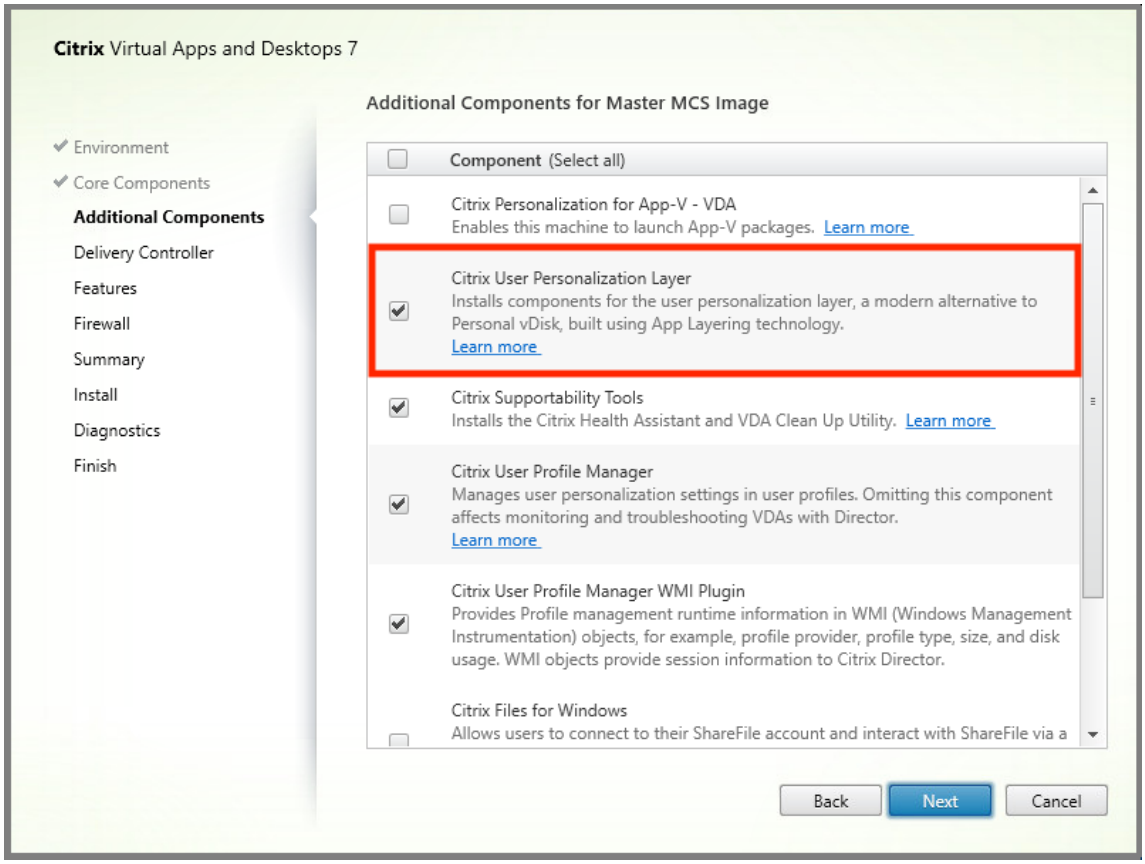


a) 環境：［マスター **MCS** イメージを作成する］か、［**Citrix Provisioning** またはサードパーティのプロビジョニングツールを使用してマスターイメージを作成する］を選択します。



a) コアコンポーネント：［次へ］をクリックします。

b) 追加のコンポーネント：［**Citrix User Personalization Layer**］をオンにします。



a) 残りのインストール画面をクリックして進みながら、必要に応じて VDA を構成し、［インストール］をクリックします。イメージはインストール中に 1 回または複数回再起動します。

4. **Windows** の更新プログラムは無効のままにします。ユーザー個人設定レイヤーインストーラーは、イメージの Windows の更新プログラムを無効にします。更新プログラムを無効のままにします。

イメージを Studio にアップロードする準備ができました。

> 注:
>
> ユーザーパーソナライズレイヤー（UPL）をアップグレードしたいだけの場合は、新しいバージョンの UPL とスタンドアロンパッケージを使用してアップグレードできます。VDA をアップグレードする必要はありません。

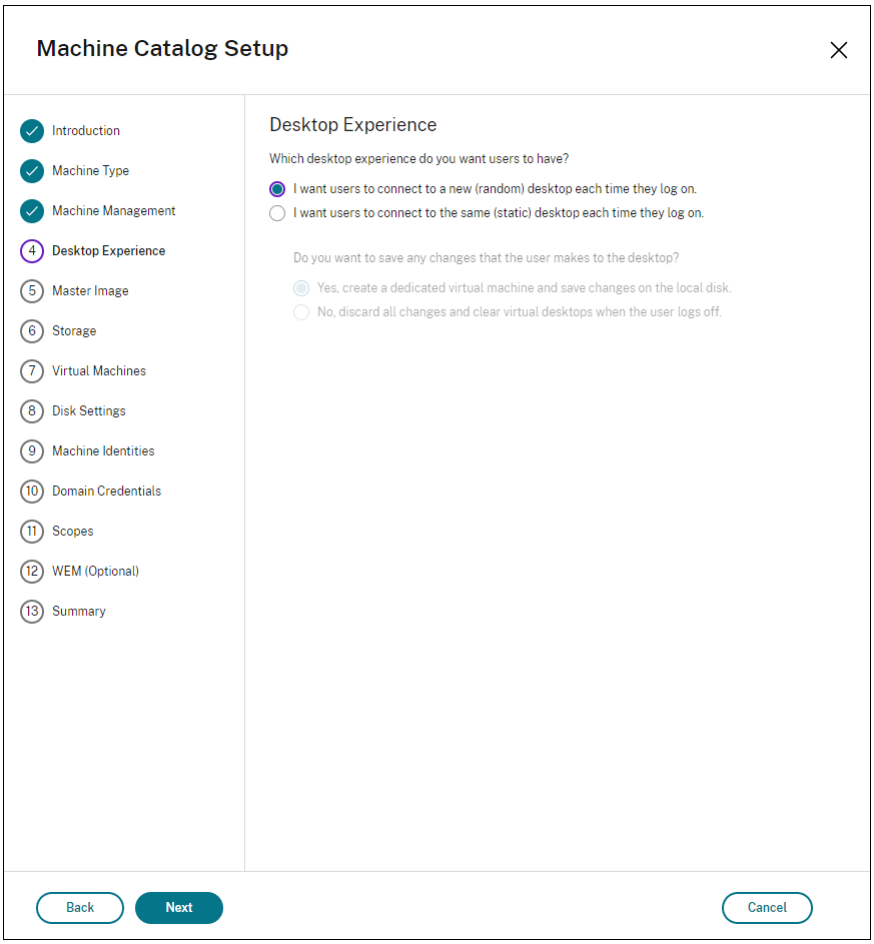
手順 **3**: マシンカタログの作成

Studio で、手順に従ってマシンカタログを作成します。カタログの作成時に次のオプションを使用します:

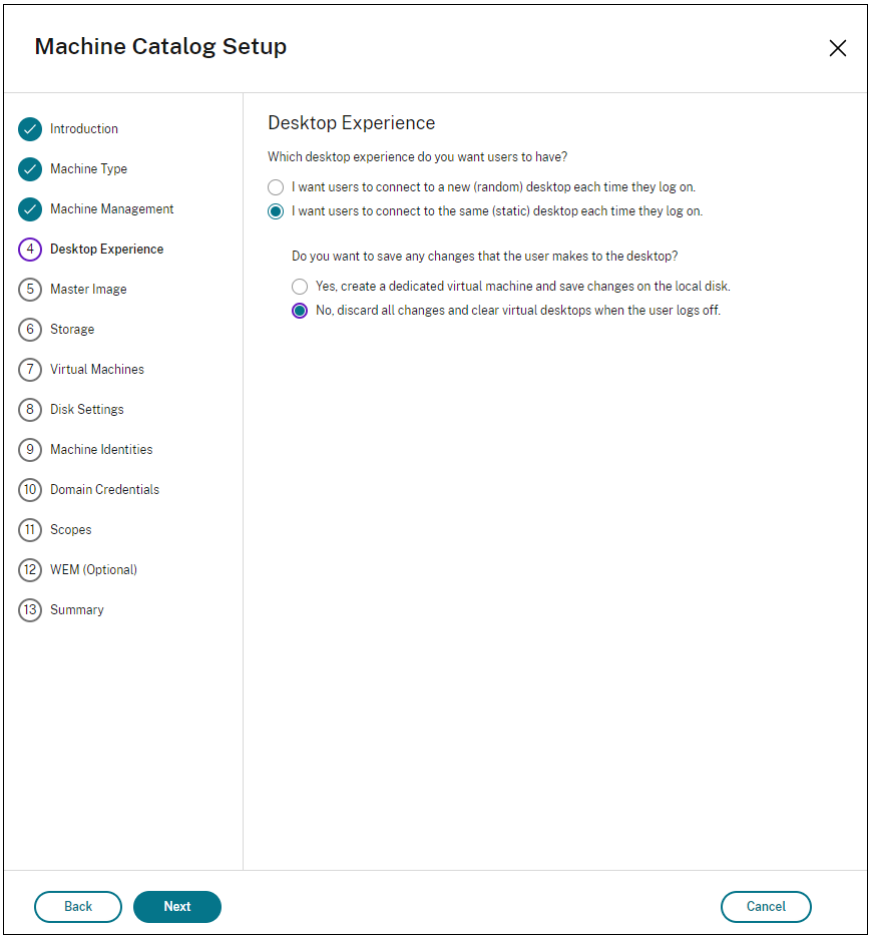
1. ［オペレーティングシステム］を選択して ［シングルセッション **OS**］に設定します。
2. ［マシン管理］を選択して ［電源管理されているマシン］に設定します。たとえば、仮想マシンまたはブレード PC などです。

3. ［デスクトップエクスペリエンス］を選択して、次の例のようにカタログの種類 **Pooled-random** または **Pooled-static** を選択します：

   - **Pooled-random**：



   - **Pooled-static**：Pooled-static を選択する場合、デスクトップを構成して、以下のスクリーンショットのようにユーザーのログオフ時にすべての変更を破棄して仮想デスクトップを消去するようにします：



> 注:
>
> ユーザー個人設定レイヤーは、Citrix Personal vDisk を使用するように構成された、または専用仮想マシンとして割り当てられた Pooled-static カタログをサポートしていません。

4. MCS を使用している場合、イメージと前述のセクションで作成されたイメージのスナップショットを選択します。
5. 環境で必要な場合、残りのカタログプロパティを構成します。

手順 **4**: デリバリーグループの作成

作成したマシンカタログのマシンも含めて、デリバリーグループを作成して構成します。詳しくは、「デリバリーグループの管理」を参照してください。

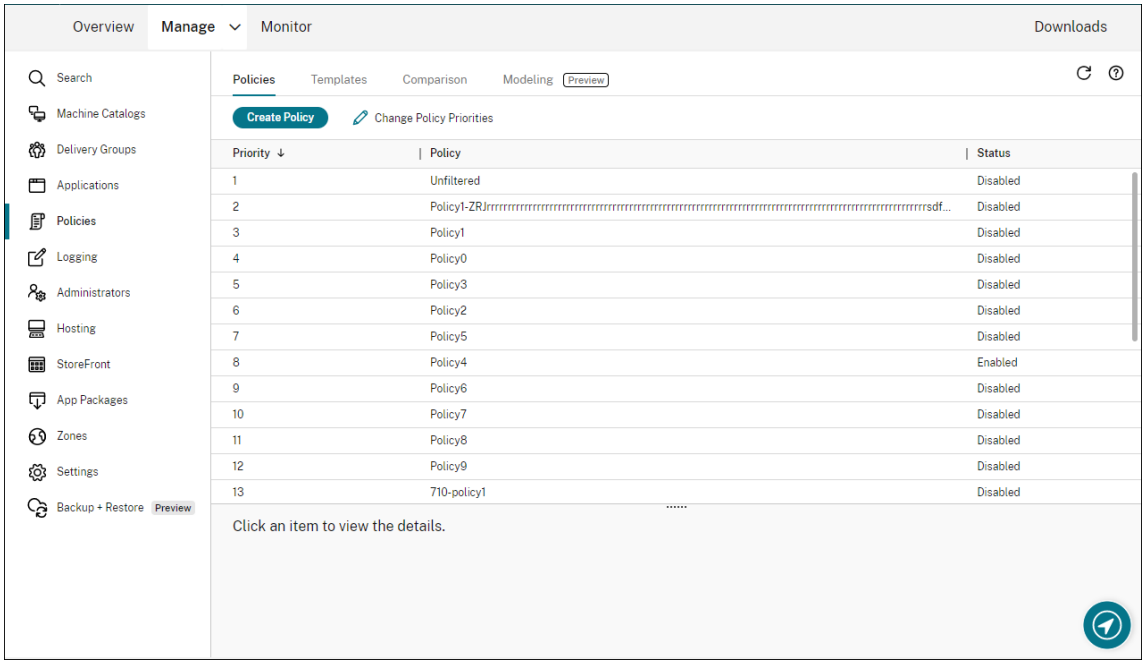
手順 **5:** デリバリーグループのカスタムポリシーの作成

Virtual Delivery Agent 内のユーザーレイヤーのマウントを有効にするには、構成パラメーターを使用して以下を指定します:

- ユーザーレイヤーにアクセスするネットワーク上の場所。
- ユーザーレイヤーディスクの拡大上限。

Web Studio でパラメーターをカスタム Citrix ポリシーとして定義し、デリバリーグループに割り当てる方法を説明します。

1. Web Studio にサインインし、左側のペインで ［ポリシー］をクリックします:



2. 操作バーの ［ポリシーの作成］を選択します。［ポリシーの作成］ウィンドウが開きます。
3. 検索フィールドに「ユーザーレイヤー」と入力します。次の 3 つのポリシーが利用可能なポリシーの一覧に表示されます:

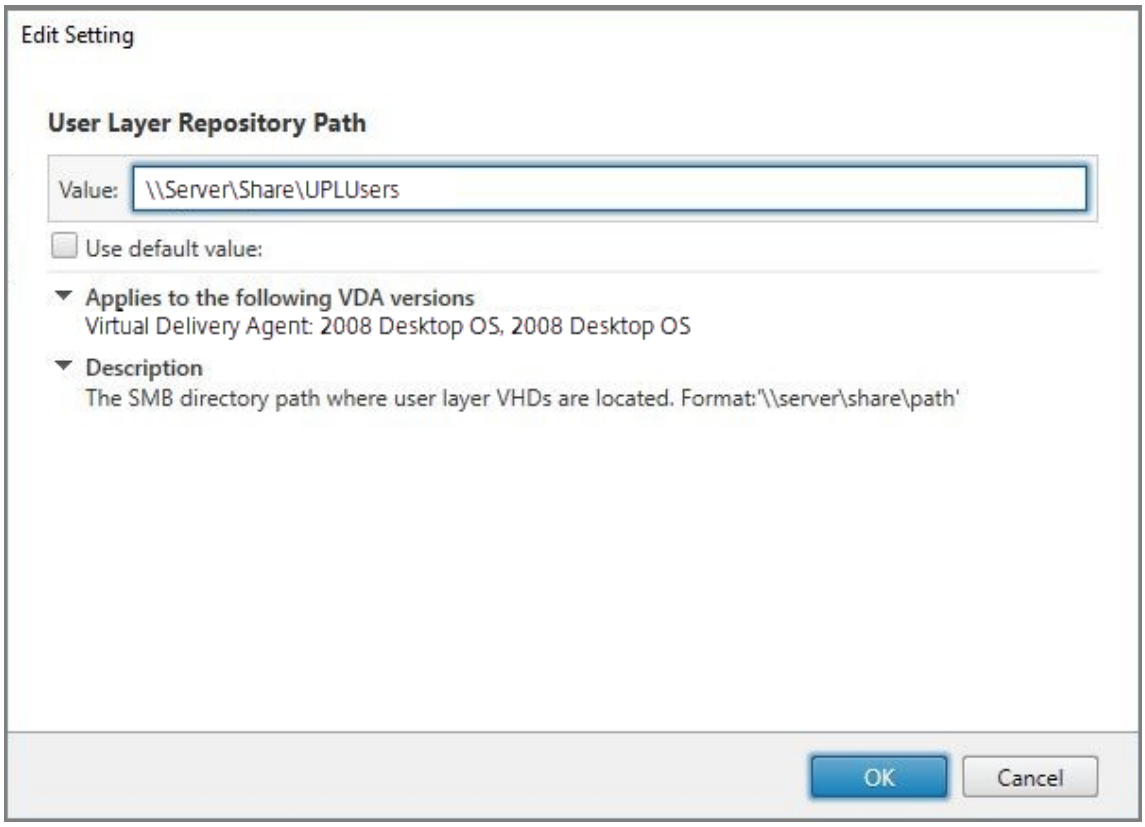
   - ユーザー レイヤーからの除外
   - ユーザーレイヤーリポジトリパス
   - ユーザーレイヤーサイズ（GB）

   > 注:
   >
   > サイズを大きくすると、新しいユーザーレイヤーに影響し、既存のユーザーレイヤーが拡張されます。サイズを小さくすると、新しいユーザーレイヤーにのみ影響します。既存のユーザーレイヤーのサイズが小さくなることはありません。

4. ［ユーザーレイヤーリポジトリパス］の横にあるチェックボックスをオンにして、［編集］をクリックします。［設定の変更］ウィンドウが開きます。
5. ［値］フィールドに次の形式でパスを入力し、［保存］をクリックします:

   - パスの形式: `\\server-name-or-address\share-name\folder`

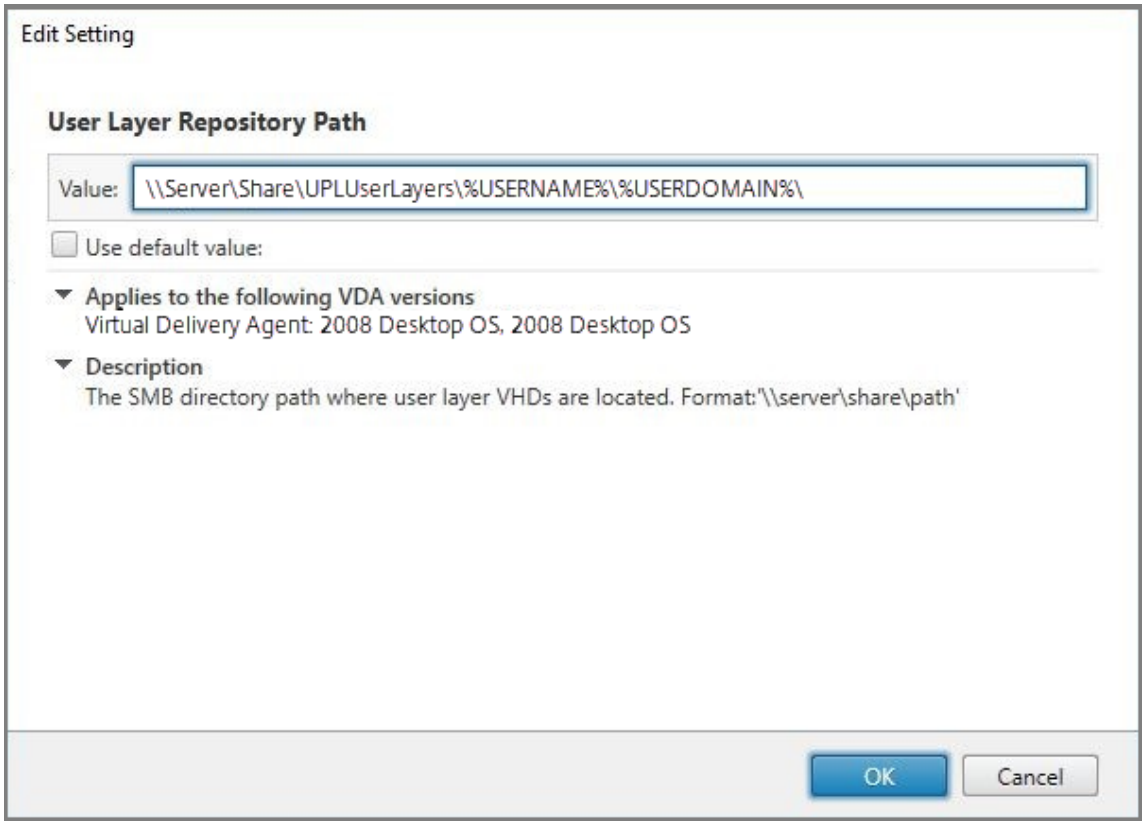
- パスの例： \\Server\Share\UPLUsers
- 結果のパスの例： **CoolCompanyDomain** の **Alex** という名前のユーザーの場合、パスは次のようになります：\\Server\Share\UPLUsers\Users\CoolCompanyDomain_Alex\A_OK



%USERNAME%および%USERDOMAIN%変数、マシン環境変数、Active Directory（AD）属性を使用してパスをカスタマイズできます。これらの変数を展開すると、明示的なパスになります。

環境変数の例：

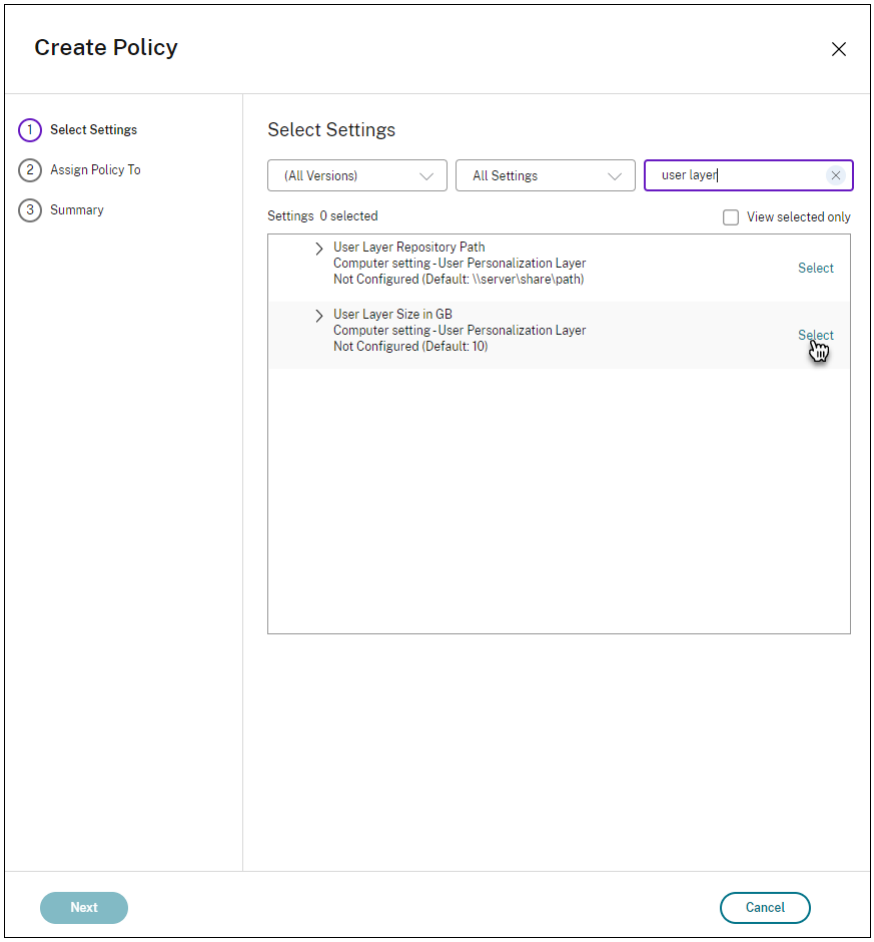
- パスの形式： \\Server-name-or-address\share-name\folder-with-environment-variables
- パスの例： \\Server\Share\UPLUserLayers\\%USERNAME%\\%USERDOMAIN%
- 結果のパスの例：**CoolCompanyDomain** の **Alex** という名前のユーザーの場合、パスは次のようになります：\\Server\Share\UPLUserLayers\Alex\CoolCompanyDomain\A_OK



カスタム AD 属性の例:

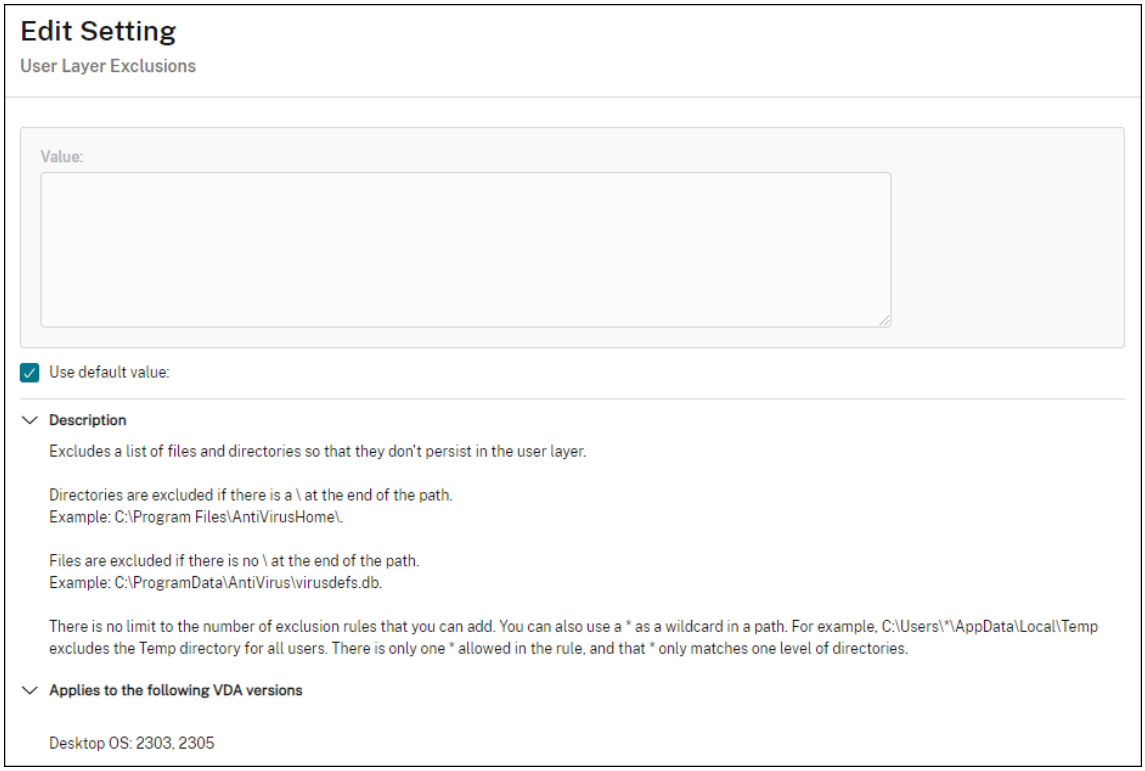
- パスの形式: `\\Server-name-or-address\share-name\AD-attribute`
- パスの例: `\\Server\share\\#sAMAccountName#`
- 結果のパスの例: `\\Server\share\JohnSmith`（#sAMAccountName# が現在のユーザーの JohnSmith に解決される場合）

6. オプション:［ユーザーレイヤーサイズ（**GB**）］の横にあるチェックボックスをオンにして、［編集］をクリックします:

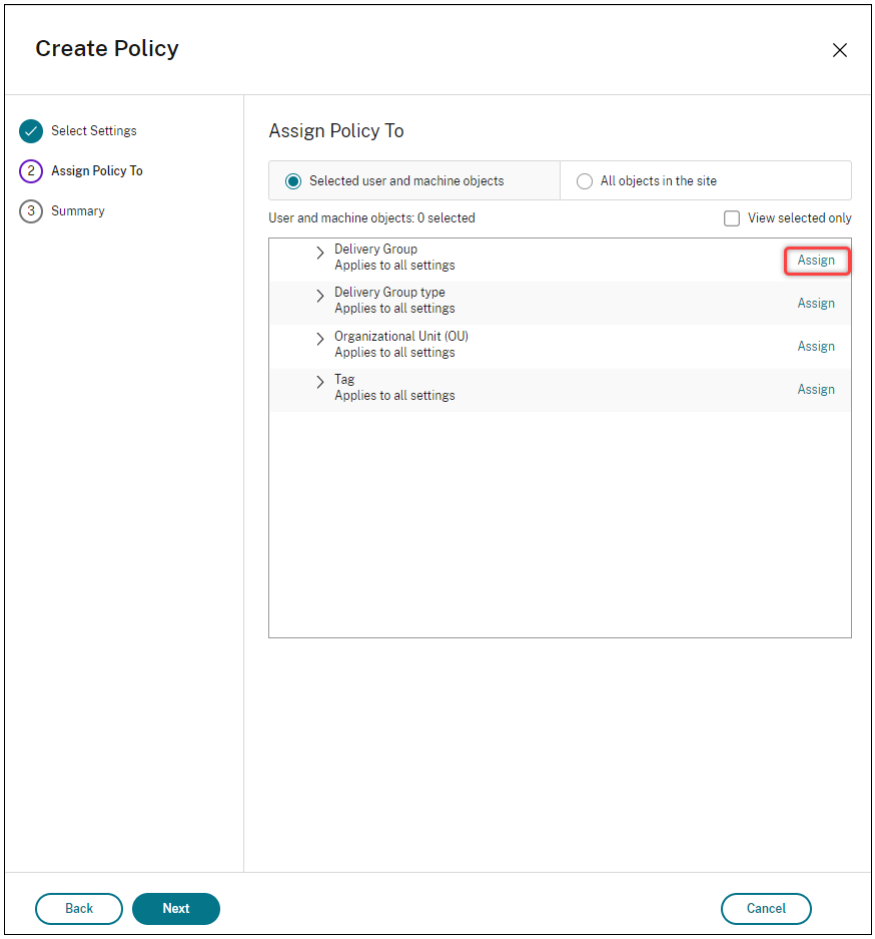


［設定の編集］ウィンドウが開きます。

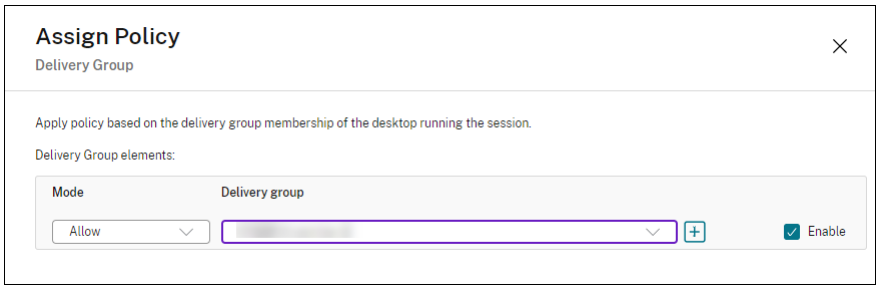
7. オプション：デフォルト値の **10GB** からユーザーレイヤーが拡大できる最大サイズに変更します。［保存］をクリックします。
8. オプション：［ユーザーレイヤーからの除外］の横にあるチェックボックスをオンにして、［編集］をクリックします。



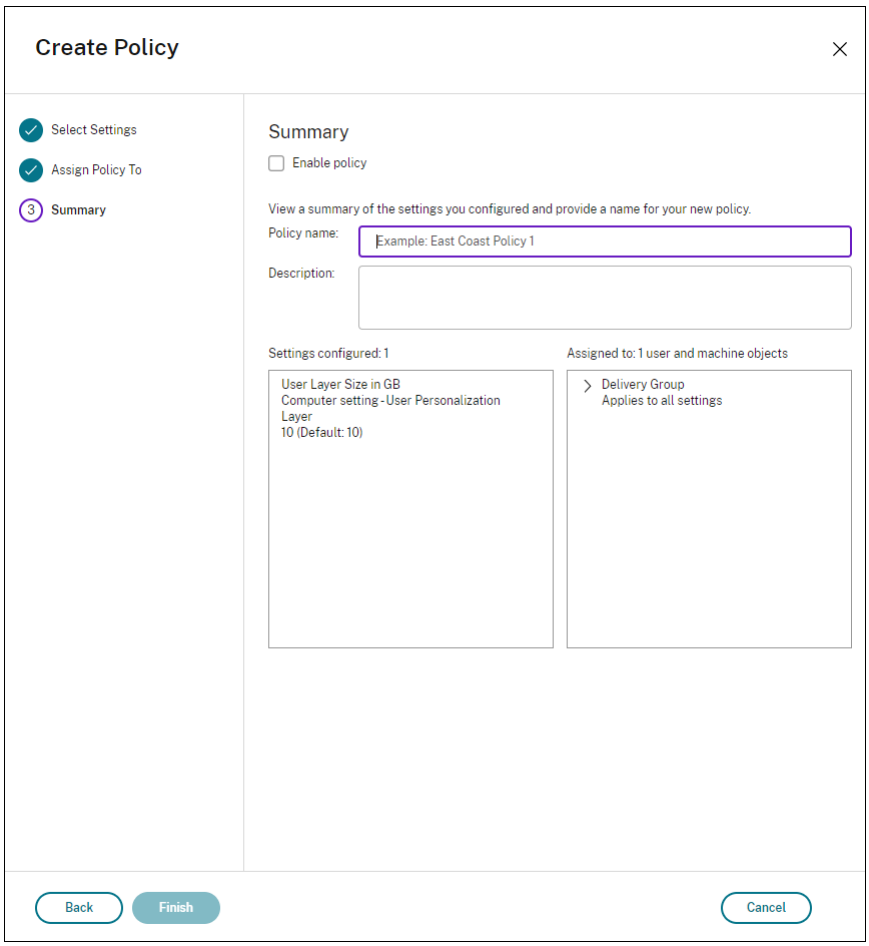
9. オプション：除外するファイルとフォルダーを指定し、［保存］をクリックします。詳しくは、Citrix App Layering のドキュメントを参照してください。
10. ［次へ］をクリックして、割り当てるユーザーとマシンを構成します。この画像で強調表示されている ［デリバリーグループ割り当て］リンクをクリックします：



11. ［デリバリーグループ］メニューで、前のセクションで作成したデリバリーグループを選択します。［**OK**］をクリックします。



12. ポリシーの名前を入力します。チェックボックスをクリックしてポリシーを有効にし、［完了］をクリックします。



ユーザーレイヤーフォルダーのセキュリティ設定の構成

ドメイン管理者は、ユーザーレイヤーに複数のストレージの場所を指定できます。各ストレージの場所（デフォルトの場所を含む）に対して、「\Users」サブフォルダーを作成します。次の設定を使用して各場所を保護します。

設定名	Value	適用先
作成所有者	変更	サブフォルダーおよびファイルのみ
所有者の権利	変更	サブフォルダーおよびファイルのみ
ユーザーまたはグループ:	フォルダーの作成/データの追加; フォルダーのスキャン/ファイルの実行; フォルダーの一覧化/データの読み取り; 属性の読み取り	選択したフォルダーのみ
システム	フルコントロール	選択したフォルダー、サブフォルダーおよびファイル

設定名	Value	適用先
ドメイン管理者、および選択した管理者グループ	フルコントロール	選択したフォルダー、サブフォルダーおよびファイル

ユーザーレイヤーメッセージ

ユーザーがユーザーレイヤーにアクセスできない場合、これらの通知メッセージのいずれかを受信します。

- 使用中のユーザーレイヤー

  ```
  We were unable to attach your user layer because it is in use.
  Any changes you make to application settings or data will not be
  saved. Be sure to save any work to a shared network location.<!--
  NeedCopy-->
  ```

- 利用できないユーザーレイヤー

  ```
  We were unable to attach your user layer. Any changes you make to
   application settings or data will not be saved. Be sure to save
  any work to a shared network location.<!--NeedCopy-->
  ```

- ユーザーのサインアウト後にリセットされないシステム

  ```
  This system was not shut down properly. Please log off immediately
   and contact your system administrator.<!--NeedCopy-->
  ```

トラブルシューティング時に使用するログファイル

ログファイル ulayersvc.log には、変更が記録されたユーザー個人設定レイヤーソフトウェアの出力が含まれています。

```
1 C:\ProgramData\Unidesk\Logs\ulayersvc.log
2 <!--NeedCopy-->
```

制限事項

ユーザー個人設定レイヤー機能をインストールして使用する場合、次の制限に留意してください。

- App Layering 内のレイヤーにユーザー個人設定レイヤーソフトウェアを展開しようとしないでください。Citrix Virtual Apps and Desktops にユーザー個人設定レイヤーを展開するか、App Layering イメージテンプレートでユーザーレイヤーを有効にします。両方ではありません。どちらのプロセスでも、必要なユーザーレイヤーが生成されます。

- 永続マシンカタログを使用してユーザー個人設定レイヤー機能を構成しないでください。
- セッションホストは使用しないでください。
- (Windows 10 のバージョンが同じ場合であっても）新しい OS インストールを実行しているイメージのマシンカタログを更新しないでください。ベストプラクティスは、マシンカタログの作成時に使用したものと同じマスターイメージ内の OS に更新を適用することです。
- 起動時ドライバー、または以前の起動用個人設定を使用しないでください。
- Personal vDisk データをユーザー個人設定レイヤー機能に移行しないでください。
- App Layering 完全製品から既存のユーザーレイヤーをユーザー個人設定レイヤー機能に移行しないでください。
- 別のマスター OS イメージを使用して作成されたユーザーレイヤーにアクセスするためにユーザーレイヤーの SMB パスを変更しないでください。
- ユーザーがセッションからログアウトしてから再度ログインすると、新しいセッションはプール内の別のマシンで実行されます。VDI 環境において、Microsoft Software Center は最初のマシンではアプリケーションをインストール済みと表示しますが、2 番目のマシンでは使用不可と表示します。

  アプリケーションの実際のステータスを確認するには、ソフトウェアセンターでアプリケーションを選択して［インストール］をクリックするよう、ユーザーに指示します。次に、SCCM はステータスを true の値に更新します。
- ソフトウェアセンターは、ユーザー個人設定レイヤー機能が有効になっている VDA 内で起動した直後に停止することがあります。この問題を回避するには、XenDesktop VDI 環境での SCCM の実装についての Microsoft の推奨事項に従ってください。また、ソフトウェアセンターを開始する前に、`ccmexec`サービスが実行されていることを確認してください。
- グループポリシー（コンピューター設定）では、ユーザーレイヤー設定はマスターイメージに適用された設定を上書きします。そのため、GPO を使用して［コンピューターの設定］で行った変更が、次のセッションログインまで保持されるとは限りません。

  この問題を回避するには、コマンドを発行するユーザーログオンスクリプトを作成します:

  ```
  gpupdate /force
  ```

  たとえば、ある顧客は各ユーザーログインで実行するように次のコマンドを設定します:

  ```
  gpudate /Target:Computer /force
  ```

  最適な結果を得るには、ユーザーのログイン後、ユーザーレイヤーで［コンピューターの設定］に直接変更を適用します。
- ドメインユーザーアカウントが、マスターイメージにログインした最後のユーザーにならないようにします。これを怠ると、そのイメージからプロビジョニングされたマシンに問題が発生します。

- 純粋な Azure AD 環境で UPL が有効になっている場合、Azure 上で実行されている Windows が原因の問題によって、カスタム証明書が保持されません。Microsoft による将来の機能強化でこの問題が修正された場合、この記事を更新します。

VDA のアップグレード

May 17, 2024

はじめに

お客様の環境に含まれる Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）コンポーネントは、VDA を除きすべて Citrix が管理します。

VDA のアップグレードを始める前に：

- 成り行きを予想できるように、この記事全体を確認してください。
- Citrix DaaS のライフサイクルポリシーを確認してください。

VDA をアップグレードするには、VDA インストーラーをダウンロードして、マシンまたはイメージ上で実行します。インストーラーのグラフィックインターフェイスとコマンドラインインターフェイスのどちらを使用しても構いません。ガイダンスについては、以下を参照してください：

- VDA インストーラー
- グラフィックインターフェイスを使用した VDA のインストール
- コマンドラインを使用した VDA のインストール

最初に`VDAWorkstationCoreSetup.exe`を使用して VDA をインストールした場合：

- 同じインストーラーの最新バージョンでアップグレードを行うと、その構成が保持されます。
- このマシンで`VDAWorkstationSetup.exe`を実行すると、`VDAWorkstationCoreSetup.exe`でサポートされていない機能を有効にできます。こうした機能の一部は、`VDAWorkstationSetup.exe`インストーラーでデフォルトで有効にされていることに注意してください。また、Citrix Workspace アプリをインストールすることもできます。

> 注：
>
> VDA をバージョン 7.17 以降のサポート対象バージョンにアップグレードするときは、アップグレードプロセス中にマシンの再起動が行われます。この再起動を避けることはできません。再起動後に、アップグレードが再開されます（コマンドラインで`/noresume`を指定していない場合）。

VDA をアップグレードしたら、その VDA を使用するイメージとカタログを更新します。

[完全な構成] インターフェイスを使用した **VDA** のアップグレード

> 重要:
>
> - ベストプラクティスとして、実稼働環境に移行する前に VDA のアップグレードを徹底的にテストすることをお勧めします。
> - 以前のバージョンから新しいバージョンに切り替えれば、CR VDA と LTSR VDA を切り替えることができます。ダウングレードと見なされるため、新しいバージョンから以前のバージョンに切り替えることはできません。たとえば、2212 CR から 2203 LTSR（任意の CU）にダウングレードすることはできませんが、2112 CR から 2203 LTSR（任意の CU）にアップグレードすることはできます。
> - オンデマンドの更新（メジャーリリース間の Hotfix やパッチなど）はサポートされていません。
> - CVAD 2402 VDA は、VDA アップグレードサービスで入手できます。

[完全な構成] インターフェイスを使用すると、カタログごとまたはマシンごとに VDA をアップグレードできます。すぐに、またはスケジュールした時間に、アップグレードできます。

VDA アップグレードサービスの詳細については、「技術概要: Citrix VDA アップグレードサービス」を参照してください。サービスの概要、詳細情報、その他役立つリソースが掲載されています。

前提条件

- コントロールプレーン：Citrix DaaS
- VDA の種類：シングルセッションまたはマルチセッションの OS VDA。現在サポートされているのは Windows VDA のみです。
- VDA バージョン 2109 以降、または 2203 LTSR 以降

  > 注:
  >
  > 最新の CR VDA または最新の LTSR CU VDA を使用することをお勧めします。

- プロビジョニングの種類：永続的なマシン（MCS でプロビジョニングされたマシン、リモート PC アクセスマシン、Citrix HDX Plus for Windows 365など）。「サポートされているマシンの種類」を参照してください。
- VDA には、VDA Upgrade Agentがインストールされ、サービスが実行されている必要があります。
- VDA をアップグレードする権限があります。
- VDA のアップグレードは、適切な CR または LTSR トラックを使用して［完全な構成］で設定されます。
- VDA は使用中ではありません（ユーザーは VDA からサインオフしている必要があります）。

  > 注:
  >
  > 使用中または切断状態の VDA のアップグレードはスキップされます。アップグレード期間をスケジュールし、VDA からログオフするようユーザーに求めることをお勧めします。

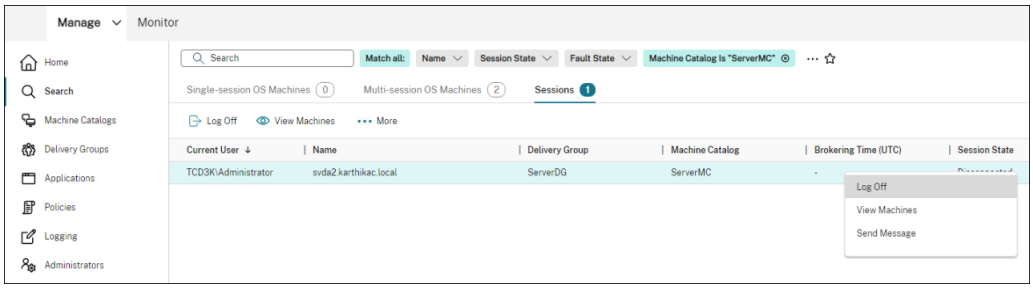
- VDA はメンテナンスモードではありません（VDA は管理者がメンテナンスモードにすることができます。登録試行回数の上限を超えた場合、VDA を自動的にメンテナンスモードにすることもできます）。
- URL フィルタリングが設定されている場合、関連する URL が許可リストに追加されています。「VDA のアップグレード要件」を参照してください。
- VDA はデリバリーグループに属し、DaaS に登録されている必要があります。
- 機能レベルが適切に設定されていると、VDA アップグレード機能を使用できます。「VDA バージョンと機能レベル」を参照してください。
- アップグレード先の VDA は、現在の VDA のオペレーティングシステムをサポートします。

既知の問題

問題 **1**：**LTSR VDA** を **LTSR** 累積更新プログラム（**CU**）バージョンにアップグレードしようとすると失敗する
LTSR VDA を LTSR 累積更新プログラム（CU）バージョンにアップグレードしようとすると失敗する場合があります。［完全な構成］ではアップグレードプロセスが正常に完了したように見えますが、インストールされている VDA のバージョンは変更されず、1～2 分後にステータスが ［アップグレード可能］に戻ります。この問題は、VDA Upgrade Agent バージョン 7.35.0.7 以前がインストールされている VDA で発生します。

この問題を回避するには、VDA にログオンし、VDA Upgrade Agent をバージョン 7.37.0.7 以降にアップグレードします（VDA インストーラーバージョン 2303 以降を使用）。バージョン 7.37.0.7 以降、VDA Upgrade Agent は自動アップグレードをサポートするため、VDA 上で実行されている以前のバージョンのエージェントを自動的に最新バージョンにアップグレードできます。この自動アップグレード機能を使用すると、VDA アップグレードサービスはエージェントによって報告された VDA バージョンをチェックし、1 時間以内にアップグレードをスケジュールして、エージェントを最新バージョンに自動的にアップグレードします。この自動アップグレード機能により、メンテナンスの労力が軽減されます。

VDA 上のエージェントを自動的にアップグレードするには、VDA アップグレードサービスが自動アップグレードを開始できるように、必ずセッションをログオフしてください。［完全な構成］でセッションをログオフできます。



エージェントが自動的にアップグレードできない場合は、VDA にログオンし、次のようにエージェントを手動でアップグレードします：

1. 次のコマンドレットを実行して、［コントロールパネル］>［プログラムのアンインストールと変更］で VDA Upgrade Agent を表示します


```
(Get-ChildItem  -Path 'HKLM:\SOFTWARE\Microsoft\Windows\
   CurrentVersion\Uninstall' | ? {
  $_.GetValue('DisplayName') -eq 'Citrix VDA Upgrade Agent Service
      - x64'  }
 ).GetValue('SystemComponent')
(Get-ChildItem  -Path 'HKLM:\SOFTWARE\Microsoft\Windows\
   CurrentVersion\Uninstall' | ? {
  $_.GetValue('DisplayName') -eq 'Citrix VDA Upgrade Agent Service
      - x64'  }
 ) | Set-ItemProperty -Name SystemComponent -Value 0
<!--NeedCopy-->
```

2. 最新の VDA Upgrade Agent をインストールします。サイレントインストールを実行するには、次のコマンドレットを使用します:

   - `msiexec /i CitrixUpgradeAgent_x64.msi /q`

コマンドレットまたはスクリプトを使用して、VDA Upgrade Agent のバージョンを識別できます。「トラブルシューティング」を参照してください。

問題 **2**: プロキシがサポートされていない　現在、VDA Upgrade Agent はプロキシ構成をサポートしていません。この制限により、エージェントがプロキシサーバー経由で接続を確立しようとすると、接続の問題が発生する可能性があります。

回避策を適用して問題に対処できます。次の手順を実行します:

1. VDA Upgrade Agent 構成ファイルを`C:\Program Files\Citrix\CitrixUpgradeAgent\Citrix.UpdateServices.UpdateAgent.exe.config`で見つけます。
2. テキストエディターを使用して構成ファイルを開きます。
3. ファイルの最後に次の行を追加し、`ProxyServerName`を実際のプロキシサーバー名に置き換えます:

```
<system.net>
  <defaultProxy enabled="true" useDefaultCredentials="true">
    <proxy proxyaddress="http://PROXYSERVER:PORT" usesystemdefault
       ="false" />
  </defaultProxy>
</system.net>
</configuration>
<!--NeedCopy-->
```

4. Citrix VDA Upgrade Agent サービスを再起動して、更新された構成を適用します。

一般的なワークフロー

[完全な構成] インターフェイスを使用して VDA をアップグレードするための一般的なワークフローは次のとおりです:

1. カタログの VDA アップグレードを有効にします。

   - カタログの作成時に VDA アップグレードを有効にできます。
   - カタログの編集時に VDA アップグレードを有効にできます。

2. カタログごとに、またはマシンごとに、VDA をアップグレードします。詳しくは、「VDA の自動アップグレードの構成」を参照してください。

   > 注:
   >
   > カタログの VDA アップグレードをスケジュールするときは、カタログ内のすべてのマシンがアップグレード対象に含まれることに注意してください。したがって、アップグレードを開始する前に、これらのマシンのバックアップを作成することをお勧めします。

トラブルシューティング

アップグレードに失敗した場合は、次のログを使用して問題を自分でトラブルシューティングできます。または、Citrix テクニカルサポートに連絡してサポートを受けるときにこのログを提供できます。

- %temp%/Citrix/XenDesktop Installerにある VDA の初回インストールにおけるインストール ログ
- C:\Windows\Temp\Citrix\XenDesktop Installerにあるアップグレードログ

VDA Upgrade Agent のバージョンを確認するには、次のコマンドレットを使用します: Get-VusComponentVersion -ComponentType VUS。すべての VDA とその VDA Upgrade Agent のバージョンが一覧表示されます。

VDA 名を取得するには、次のコマンドレットを使用します: Get-BrokerMachine -UUID "<version number>"。<version number>は、Get-VusComponentVersionコマンドレットから取得した VDA Upgrade Agent のバージョンです。

VDA Upgrade Agent のバージョンをカタログレベルで確認するには、次のスクリプトを使用できます:

> 注:
>
> このスクリプトは例として提供されており、特定の環境に合わせた調整が必要な場合があります。実稼働環境で使用する前に、スクリプトを徹底的にテストすることをお勧めします。

```
Param(
    [Parameter (Mandatory=$true)]
    [string] $CatalogName
)

try
{

```



```
    $Uuids = Get-BrokerMachine -CatalogName $CatalogName | Select-
        Object -Property UUID

    if($Uuids -eq $null)
    {

        throw "Cannot find CatalogName "+$CatalogName
     }

    Write-Output("Catalog Name passed is "+$CatalogName)

   foreach($Uuid in $Uuids)
    {

        $compVersion = Get-VusComponentVersion -MachineId $machine.UUID
            -ComponentType VUS
        $Machine = Get-BrokerMachine -UUID $compVersion.MachineId
        Write-Output("MachineName: "+$Machine.MachineName+", Machine
            UUID:"+$machine.MachineId+", VUA Version:"+$compVersion.
            Version)
     }

 }

catch
{

    Write-Output("Exception Occured")
    Write-Host $_
 }

<!--NeedCopy-->
```

VDA Upgrade Agent に関連するログ　VDA Upgrade Agent に関連するログを収集することもできます。収集できるログには、以下が含まれます:

- **Citrix Diagnostic Facility**（**CDF**）トレース。
- **Windows** イベントログ。Windows イベントログに書き込まれる情報。[イベントビューア] **>** [アプリケーションとサービスログ] **>** [**Citrix VDA Upgrade Agent** サービス] でログを表示します。

必要に応じて、ログが継続的にファイルに書き込まれるように VDA Upgrade Agent 構成ファイルを変更できます。ファイルへのログ記録を有効にするには、次の手順を実行します:

1. フォルダー`C:\Program Files\Citrix\CitrixUpgradeAgent`に移動します。
2. ファイル`Citrix.UpdateServices.UpdateAgent.exe.config`を開きます。
3. `LogToFile`の値を`1`に変更します。
4. Citrix VDA Upgrade Agent サービスを再起動します。これにより、`C:\ProgramData\Citrix\Update Services\Logs`にログ ファイルが作成されます。

> 注:
>
> - ファイルへのログ記録を有効にすると、ログが継続的に書き込まれ、ストレージ領域が消費される可能性があります。問題が解決したら、忘れずにログ記録を無効にしてください。ログを無効にするには、まずLogToFileを0に設定してから、Citrix VDA Upgrade Agent サービスを再起動します。
> - LogToFile=1を設定すると、ログはファイルにのみ書き込まれます。これらは CDF トレースには表示されません。

VDA アップグレードのダウンロードエラーに関するトラブルシューティング　VDA アップグレード機能に関連するダウンロードエラーのトラブルシューティングと解決を行うには、次の手順を実行します:

1. URL フィルタリングが設定されている場合、関連する URL が許可リストに追加されていることを確認してください。「VDA のアップグレード要件」を参照してください。
2. 必要な URL を許可リストに追加した後、VDA アップグレードのスケジュールを変更してみてください。

CDF トレースを有効にするか、LogToFileを1に設定して、分析用の詳細なログをキャプチャできます。ダウンロードエラーの問題が解決しない場合は、エラー内容を確認してください。「ダウンロードに失敗しました: このアクセス制御リストは正規形式ではないため、変更できません（Download Failed: This access control list is not in canonical form and therefore cannot be modified）」というエラーメッセージが表示された場合は、フォルダーC:/ProgramData/Citrix/UpgradeServices/Downloads/VDAの権限が正しくないことを示しています。この問題に対処するには、次のいずれかを実行します:

- オプション **1**: 次のコマンドを使用して、フォルダーのアクセス制御リスト（ACL）をリセットします。（このコマンドは、一致するすべてのファイルのデフォルトで継承された ACL を使用して ACL をリセットします。）

  ```
  - icacls.exe "C:\ProgramData\Citrix\UpgradeServices\Downloads\
    VDA"/reset /T /C /L /Q
  ```

- オプション **2**: ダウンロードの下の VDA フォルダーを削除し、VDA アップグレードをスケジュールします。

VDA アップグレードの検証エラーに関するトラブルシューティング　VDA アップグレード機能に関連するダウンロードエラーのトラブルシューティングと解決を行うには、次の手順を実行します:

1. URL フィルタリングが設定されている場合は、関連する URL、特に失効チェックに必要な証明書失効一覧（CRL）または Online Certificate Status Protocol（OCSP）の URL が許可リストに追加されていることを確認してください。「VDA のアップグレード要件」を参照してください。
2. 必要な URL を許可リストに追加した後、VDA アップグレードのスケジュールを変更してみてください。

CDF トレースを有効にするか、LogToFileを1に設定して、分析用の詳細なログをキャプチャできます。ログには次のエラーが含まれる場合があります:

- RevocationStatusUnknown

- The revocation function was unable to check the revocation status for the certificate.（失効機能は証明書の失効ステータスを確認できませんでした。）
- The revocation function was unable to check revocation because the revocation server was offline.（失効サーバーがオフラインのため、失効機能が失効を確認できませんでした。）

VDA Upgrade Agent は、証明書の検証と失効チェックの実行を Windows のシステムコールに依存しています。上記のエラーは、エージェントが CRL または OCSP の URL への接続を確立できないことを示しています。

現在、VDA Upgrade Agent はプロキシ設定をサポートしていないことに注意してください。CryptoAPI による CRL および OCSP の発信呼び出しはプロキシ構成を認識しないため、失敗する可能性があります。

環境にプロキシが設定されている場合は、VDA 上でシステムプロキシを構成して、CRL の発信呼び出しを有効にすることができます。システムプロキシを構成するには、次の手順を実行します:

```
netsh winhttp import proxy source=ie

Or

netsh winhttp set proxy proxy-server=http://Proxy_Server:Port
<!--NeedCopy-->
```

PowerShell を使用した VDA のアップグレード

Remote PowerShell SDK を使用して VDA のアップグレードを構成できます。Remote PowerShell SDK について詳しくは、「Citrix DaaS Remote PowerShell SDK」を参照してください。

以下は PowerShell コマンドレットです:

- **Get-VusCatalog**

  このコマンドレットを使用して、`Name`、`Uid`、`Uuid`、`UpgradeState`（`Available`、`UpToDate`、`Scheduled`、`Unknown`）、`UpgradeType`（CR/LTSR）、`Upgrade scheduled`、および`StateId`（`Upgrade scheduled`のステータス）などのカタログの詳細を取得します。

- **Get-VusMachine**

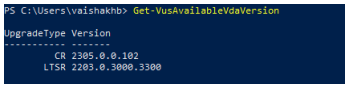
  このコマンドレットを使用して、`MachineName`、`Uid`、`Uuid`、`UpgradeState`（`Available`、`UpToDate`、`Scheduled`、`Unknown`）、`UpgradeType`（CR/LTSR）、`StateId`（`Upgrade scheduled`のステータス）などのマシンの詳細を取得します。

- **Get-VusComponentVersion**

  このコマンドレットを使用して、VDA がコンポーネントのバージョンを報告したかどうかを確認します。`MachineId`を使用して VDA をフィルタリングします。`MachineId`は`Get-BrokerMachine`の UUID です。

- **Get-VusAvailableVdaVersion**

このコマンドレットを使用して、VDA Update Service 経由でリリースされた最新の CR/LTSR バージョンを確認します。



- **Set-VusCatalogUpgradeType**

  このコマンドレットを使用して、カタログのアップグレードの種類を CR または LTSR に設定します。アップグレードの種類は、マシンカタログレベルでのみ設定できます。

- **New-VusMachineUpgrade**

  このコマンドレットを使用して、マシンレベルで VDA のアップグレードを構成します。

- **New-VusCatalogSchedule**

  このコマンドレットを使用して、マシンカタログレベルで VDA のアップグレードをスケジュールします。

マシンレベルのコマンドレットの例

- アップグレードの種類を設定します。

  例:

  ```
  - Set-VusCatalogUpgradeType -CatalogName test-catalog -UpgradeType
    LTSR
  ```

- カタログ内のマシンの`UpgradeState`を確認するには、`Get-VusMachine`を使用します。

  例:

  ```
  -Get-VusMachine -CatalogName test-catalog
  ```



```
PS C:\Users> Get-VusMachine -CatalogName test-catalog


CatalogName       : test-catalog
DNSName           : test-machine-1
DurationInHours   :
LastStateChange   :
MachineName       : test-machine-1
MachineUid        : 35
MachineUuid       : d664614a-cd37-44d6-b1f0-6f6b70f8299c
ProvisioningType  : MCS
ScheduledTime     :
SessionSupport    : SingleSession
StateId           :
StatusMessage     :
UpgradeState      : UpgradeAvailable
UpgradeType       : LTSR
UpgradeVersion    :

CatalogName       : test-catalog
DNSName           : test-machine-2
DurationInHours   :
LastStateChange   :
MachineName       : test-machine-2
MachineUid        : 36
MachineUuid       : cfa55303-6000-4973-bee8-e38c9916719e
ProvisioningType  : MCS
ScheduledTime     :
SessionSupport    : SingleSession
StateId           :
StatusMessage     :
UpgradeState      : UpgradeAvailable
UpgradeType       : LTSR
UpgradeVersion    :
```

`UpgradeState`が`Unknown`である場合、考えられる理由の 1 つは、VDA にインストールされている Citrix VDA Upgrade Agent が VDA Update Service にバージョンを報告していないことです。`Get-VusComponentVersion`コマンドレットを使用して、VDA がコンポーネントのバージョンを報告したかどうかを確認できます。

- `Get-VusComponentVersion -MachineId ""`

```
PS C:\Users> Get-VusComponentVersion -MachineId  d664614a-cd37-44d6-b1f0-6f6b70f8299c

      ComponentType MachineId                            Uid                                  Version
      ------------- ---------                            ---                                  -------
                VDA d664614a-cd37-44d6-b1f0-6f6b70f8299c 7505fa4c-1811-ee11-907e-0022484becbd 2203.0.0.33220
                VUS d664614a-cd37-44d6-b1f0-6f6b70f8299c 7705fa4c-1811-ee11-907e-0022484becbd 7.37.0.7
                Mps d664614a-cd37-44d6-b1f0-6f6b70f8299c 7805fa4c-1811-ee11-907e-0022484becbd 7.33.0.26
SupportabilityTools d664614a-cd37-44d6-b1f0-6f6b70f8299c 7a05fa4c-1811-ee11-907e-0022484becbd 1.5.0.17
                Upm d664614a-cd37-44d6-b1f0-6f6b70f8299c 7c05fa4c-1811-ee11-907e-0022484becbd 22.3.0.7
       UpmVdaPlugin d664614a-cd37-44d6-b1f0-6f6b70f8299c 7d05fa4c-1811-ee11-907e-0022484becbd 22.3.0.7
```

結果が表示されない場合は、次のことを確認してください:

- VDA がカタログおよびデリバリーグループの一部である。
- VDA Upgrade Agent が VDA にインストールされ、実行されている。必要に応じて、エージェントを再起動してみてください。

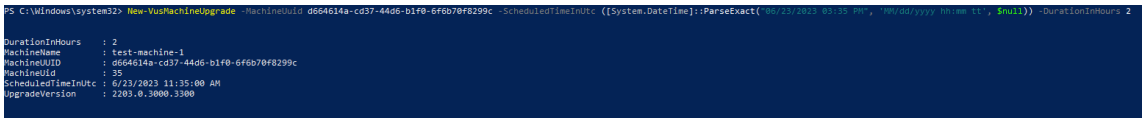
注：結果が残っていない場合は、VDA Upgrade Agent の再起動中に Citrix Diagnostic Facility トレースを収集し、問題のトラブルシューティングを行います。

- VDA のアップグレードをスケジュールします。始める前に、以下の点に留意してください：
  - DurationInHours：アップグレードプロセスの期間を時間単位で指定できます。VDA はメンテナンスモードになります。VDA インストーラーがダウンロードされ、アップグレードが実行されます。アップグレードする VDA が多数ある場合は、より長い期間を指定します。
  - UpgradeNow：このスイッチを使用してアップグレードをすぐにスケジュールするか、ScheduledTimeInUtcを設定します。
  - ScheduledTimeInUtc：特定の日時にアップグレードをスケジュールできます。

  例：

  - `New-VusMachineUpgrade -MachineUuid d664614a-cd37-44d6-b1f0-6f6b70f8299c -ScheduledTimeInUtc ([System.DateTime]::ParseExact("06/23/2023 03:35 PM", 'MM/dd/yyyy hh:mm tt', $null))-DurationInHours 2`

  MachineUuid、MachineUid、およびMachineNameを使用して、VDA のアップグレードをスケジュールできます。



- アップグレードのステータスを確認します。

  例：

  `-Get-VusMachine -MachineName test-machine-1`

```
PS C:\Windows\system32> Get-VusMachine -MachineName test-machine-1


CatalogName       : test-catalog
DNSName           : test-machine-1
DurationInHours   : 2
LastStateChange   : 6/23/2023 11:47:35 AM
MachineName       : test-machine-1
MachineUid        : 35
MachineUuid       : d664614a-cd37-44d6-b1f0-6f6b70f8299c
ProvisioningType  : MCS
ScheduledTime     : 6/23/2023 11:35:00 AM
SessionSupport    : SingleSession
StateId           : UpgradeInProgress
StatusMessage     :
UpgradeState      : UpgradeScheduled
UpgradeType       : LTSR
UpgradeVersion    : 2203.0.3000.3300
```



```
PS C:\Users\vaishakhb> Get-VusMachine -MachineName test-machine-1


CatalogName      : test-catalog
DNSName          : test-machine-1
DurationInHours  : 4
LastStateChange  : 6/23/2023 12:18:21 PM
MachineName      : test-machine-1
MachineUid       : 35
MachineUuid      : d664614a-cd37-44d6-b1f0-6f6b70f8299c
ProvisioningType : MCS
ScheduledTime    : 6/23/2023 12:00:00 PM
SessionSupport   : SingleSession
StateId          : UpgradeSuccess
StatusMessage    : Upgrade completed successfully or is already up to date
UpgradeState     : UpToDate
UpgradeType      : LTSR
UpgradeVersion   : 2203.0.3000.3300
```

カタログレベルのコマンドレットの例

- マシンカタログレベルでアップグレードの種類を設定します。

  例:

  - `Set-VusCatalogUpgradeType -CatalogName test-catalog -UpgradeType LTSR`

- カタログ内のマシンの`UpgradeState`を確認するには、`Get-VusCatalog`を使用します。

  例:

  - `Get-VusCatalog -Name test-catalog`

```
PS C:\Windows\system32> Get-VusCatalog -Name test-catalog


CancelledUpgrades           :
DurationInHours             :
FailedUpgrades              :
InProgressUpgrades          :
LastStateChangeInUtc        :
MaxConcurrentUpgrades       :
Name                        : test-catalog
ProvisioningType            : MCS
ScheduledTimeInUtc          :
SecurityCheckFailedUpgrades :
SessionSupport              : SingleSession
StateId                     :
SuccessfulUpgrades          :
TotalMachines               :
Uid                         : 30
UpgradeState                : UpgradeAvailable
UpgradeType                 : LTSR
UpgradeVersion              :
Uuid                        : 3ad4253c-3dfa-4982-8e6e-7686bf904da1
```


UpgradeStateがUnknownである場合、考えられる理由の 1 つは、VDA にインストールされている Citrix VDA Upgrade Agent が VDA Update Service にバージョンを報告していないことです。Get-VusComponentVersionコマンドレットを使用して、VDA がコンポーネントのバージョンを報告したかどうかを確認できます。

- `Get-VusComponentVersion -MachineId ""`

```
PS C:\Users> Get-VusComponentVersion -MachineId  d664614a-cd37-44d6-b1f0-6f6b70f8299c

      ComponentType MachineId                            Uid                                  Version
      ------------- ---------                            ---                                  -------
                VDA d664614a-cd37-44d6-b1f0-6f6b70f8299c 7505fa4c-1811-ee11-907e-0022484becbd 2203.0.0.33220
                VUS d664614a-cd37-44d6-b1f0-6f6b70f8299c 7705fa4c-1811-ee11-907e-0022484becbd 7.37.0.7
                Mps d664614a-cd37-44d6-b1f0-6f6b70f8299c 7805fa4c-1811-ee11-907e-0022484becbd 7.33.0.26
SupportabilityTools d664614a-cd37-44d6-b1f0-6f6b70f8299c 7a05fa4c-1811-ee11-907e-0022484becbd 1.5.0.17
                Upm d664614a-cd37-44d6-b1f0-6f6b70f8299c 7c05fa4c-1811-ee11-907e-0022484becbd 22.3.0.7
       UpmVdaPlugin d664614a-cd37-44d6-b1f0-6f6b70f8299c 7d05fa4c-1811-ee11-907e-0022484becbd 22.3.0.7
```

結果が表示されない場合は、次のことを確認してください:

  - VDA がカタログおよびデリバリーグループの一部である。
  - VDA Upgrade Agent が VDA にインストールされ、実行されている。必要に応じて、エージェントを再起動してみてください。

注: 結果が残っていない場合は、VDA Upgrade Agent の再起動中に Citrix Diagnostic Facility トレースを収集し、問題のトラブルシューティングを行います。

- VDA のアップグレードをスケジュールします。始める前に、以下の点に留意してください:
  - DurationInHours: アップグレードプロセスの期間を時間単位で指定できます。VDA はメンテナンスモードになります。VDA インストーラーがダウンロードされ、各 VDA でアップグレードが実行されます。カタログに多数の VDA が含まれている場合は、より長い期間を指定します。
  - UpgradeNow: このスイッチを使用してアップグレードをすぐにスケジュールするか、ScheduledTimeInUtcを設定します。
  - ScheduledTimeInUtc: 特定の日時にアップグレードをスケジュールできます。

  例:

  - `New-VusCatalogSchedule -CatalogName test-catalog -ScheduledTimeInUtc ([System.DateTime]::ParseExact("06/23/2023 04:00 PM", 'MM/dd/yyyy hh:mm tt', $null))-DurationInHours 4`

  CatalogName、Uid、およびUuidを使用して、アップグレードをスケジュールできます。

```
PS C:\Windows\system32> New-VusCatalogSchedule -CatalogName test-catalog -ScheduledTimeInUtc ([System.DateTime]::ParseExact("06/23/2023 04:00 PM", 'MM/dd/yyyy hh:mm tt', $null)) -DurationInHours 4

CatalogName          : test-catalog
CatalogUUID          : 3ad4253c-3dfa-4982-8e6e-7686bf904da1
CatalogUid           : 30
DurationInHours      : 4
LastStateChangeInUtc : 6/23/2023 12:08:14 PM
ScheduledTimeInUtc   : 6/23/2023 12:00:00 PM
State                : UpgradeScheduled
UpgradeVersion       : 2203.0.3000.3300
```

- アップグレードのステータスを確認します。Get-VusCatalogまたはGet-VusMachineコマンドレットを使用して、VDA のアップグレードステータスを定期的に確認します。MachineUuid、MachineUid、およびMachineNameを使用して VDA をフィルタリングします。

例：

```
-Get-VusCatalog -Name test-catalog
```

```
PS C:\Windows\system32> Get-VusCatalog -Name test-catalog


CancelledUpgrades            : 0
DurationInHours              : 4
FailedUpgrades               : 0
InProgressUpgrades           : 0
LastStateChangeInUtc         : 6/23/2023 12:08:43 PM
MaxConcurrentUpgrades        : 100
Name                         : test-catalog
ProvisioningType             : MCS
ScheduledTimeInUtc           : 6/23/2023 12:00:00 PM
SecurityCheckFailedUpgrades  : 0
SessionSupport               : SingleSession
StateId                      : UpgradeInProgress
SuccessfulUpgrades           : 0
TotalMachines                : 2
Uid                          : 30
UpgradeState                 : UpgradeScheduled
UpgradeType                  : LTSR
UpgradeVersion               : 2203.0.3000.3300
Uuid                         : 3ad4253c-3dfa-4982-8e6e-7686bf904da1
```

カタログ内の各マシンの VDA アップグレードステータスを表示するには、`Get-VusMachine`を使用します。

```
PS C:\Users\vaishakhb> Get-VusMachine -CatalogName test-catalog


CatalogName      : test-catalog
DNSName          : test-machine-1
DurationInHours  : 4
LastStateChange  : 6/23/2023 12:18:21 PM
MachineName      : test-machine-1
MachineUid       : 35
MachineUuid      : d664614a-cd37-44d6-b1f0-6f6b70f8299c
ProvisioningType : MCS
ScheduledTime    : 6/23/2023 12:00:00 PM
SessionSupport   : SingleSession
StateId          : UpgradeSuccess
StatusMessage    : Upgrade completed successfully or is already up to date
UpgradeState     : UpToDate
UpgradeType      : LTSR
UpgradeVersion   : 2203.0.3000.3300

CatalogName      : test-catalog
DNSName          : test-machine-2
DurationInHours  : 4
LastStateChange  : 6/23/2023 12:17:33 PM
MachineName      : test-machine-2
MachineUid       : 36
MachineUuid      : cfa55303-6000-4973-bee8-e38c9916719e
ProvisioningType : MCS
ScheduledTime    : 6/23/2023 12:00:00 PM
SessionSupport   : SingleSession
StateId          : UpgradeInProgress
StatusMessage    :
UpgradeState     : UpgradeScheduled
UpgradeType      : LTSR
UpgradeVersion   : 2203.0.3000.3300
```


VDA に **Personal vDisk** がインストールされている場合

Personal vDisk（PvD）コンポーネントを VDA にインストールしたことがある場合、コンポーネントを削除するまで、VDA をバージョン 1912 LTSR 以降にアップグレードすることはできません。

この手順は、PvD を使用したことがない場合でも適用されます。PvD コンポーネントが以前のバージョンでどのようにインストールされていたかは次のとおりです：

- VDA インストーラーのグラフィカルインターフェイスでは、PvD は ［追加コンポーネント］ページのオプションです。7.15 LTSR およびそれ以前の 7.x リリースでは、デフォルトでこのオプションが有効になっています。そのため、デフォルトを変更しない場合（または任意のリリースでこのオプションを有効にすることを選択した場合）、PvD がインストールされました。
- コマンドラインでは、`/baseimage`オプションによって PvD がインストールされます。このオプションを指定した場合、またはこのオプションを含むスクリプトを使用した場合、PvD がインストールされました。

必要なアクション

VDA インストーラーが現在インストールされている VDA 内の PvD コンポーネントを検出しない場合、アップグレードは通常どおり続行されます。

インストーラーが現在インストールされている VDA で PvD コンポーネントを検出した場合：

- グラフィカルインターフェイス：アップグレードが一時停止します。サポートされていないコンポーネントを自動的に削除するかどうかを尋ねるメッセージが表示されます。［**OK**］をクリックすると、コンポーネントが自動的に削除され、アップグレードが続行されます。
- **CLI**：インストーラーが PvD コンポーネントを検出すると、このコマンドは失敗します。コマンドの失敗を回避するには、このコマンドに次のオプションを含めます：`/remove_pvd_ack`。

Windows 10（1607 以前、更新なし）マシンで PvD を引き続き使用する場合、使用できる最新バージョンは VDA 7.15 LTSR です。XenApp および XenDesktop 7.15 LTSR の拡張サポートプログラムは、Citrix DaaS で使用される VDA には適用されないことに注意してください。詳しくは、Citrix Support Knowledge Center の「Extended Support Customer Guide」を参照してください。

以前のオペレーティングシステム

「システム要件」の記事には、現在のリリースの VDA でサポートされている Windows オペレーティングシステムが掲載されています。

- LTSR VDA については、ご利用の LTSR バージョンのシステム要件の記事を参照してください。
- Linux VDA については、Linux Virtual Delivery Agentのドキュメントを参照してください。

最新の VDA をインストールできない OS を搭載した Windows マシンには、以下のいくつかのオプションがあります。

WVD 以外の環境の場合:

- サポートされている Windows バージョンにマシンを再イメージ化してから、新しい VDA をインストールします。
- マシンの再イメージ化はしないが、OS をアップグレードする場合は、OS をアップグレードする前に VDA をアンインストールします。そうしないと、VDA はサポートされていない状態になります。OS をアップグレードした後、新しい VDA をインストールします。
- マシンにバージョン 7.15 LTSR がインストールされており、これより新しい VDA をインストールしようとした場合、最新のサポートされているバージョンを使用していることを示すメッセージが表示されます。
- マシンに 7.15 LTSR より前の VDA がインストールされている場合は、CTX139030 へのリンクを示すメッセージが表示されます。7.15 LTSR VDA は、Citrix の Web サイトからダウンロードできます。

構成の **Citrix Cloud** への移行

March 31, 2024

自動構成を使用する理由

大規模または複雑な環境を担当する IT 管理者は、多くの場合、移行が面倒なプロセスであることに気付きます。このタスクはユースケース特有である傾向があるため、多くは、正常に実行するために独自のツールを作成することになります。

自動構成ツールを使用して移行プロセスを自動化することにより、Citrix ではこのプロセスの簡易化に役立ちたいと考えています。管理者は、Citrix Cloud で現在の構成を簡単にテストし、現在の環境を損なわずに、Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）が提供する利点を活用することができます。自動構成はバックグラウンドでシームレスに動作するため、エンドユーザーへの影響もありません。このような利点には、バックエンドおよびコントロールプレーンの一部を Citrix が管理する場合に管理上の過負荷が軽減されることや、Citrix Cloud コンポーネントの更新がカスタマイズ可能で自動化されていることなどが含まれます。

Citrix では業界標準のコードでの構成を使用して、移行プロセスの自動化を支援するメカニズムを提供します。自動構成では、オンプレミスサイトが構成ファイルのコレクションとして検出されエクスポートされます。これらのファイルの構成は、その後、Citrix DaaS にインポートできます。

自動構成により、管理者は、名前の競合を防ぎながら複数のオンプレミスサイトを単一のサイトにマージすることもできます。管理者は、オンプレミス構成とクラウド構成のどちらがリソースを制御するかを管理できます。

自動構成では、1 回限りの移行だけでなく、Citrix Cloud での日常的な構成の自動化もできます。Citrix DaaS の構成を移行すると、次のような多くの理由でメリットがあります:

- テストまたはステージから実稼働環境へのサイトの同期
- 構成のバックアップと復元

- リソース制限に達する
- あるリージョンから別のリージョンへの移行

次の 2 分間のビデオでは、自動構成を簡単に紹介するクイックツアーを提供しています。

これは埋め込みビデオです。リンクをクリックしてビデオを見る

自動構成について詳しくは、Tech Zone の「概念実証：自動構成ツール」を参照してください。

環境の移動、および移行のためのオンプレミス構成の準備について詳しくは、Tech Zone の「展開ガイド：Citrix Virtual Apps and Desktops のオンプレミスから Citrix Cloud への移行」を参照してください。

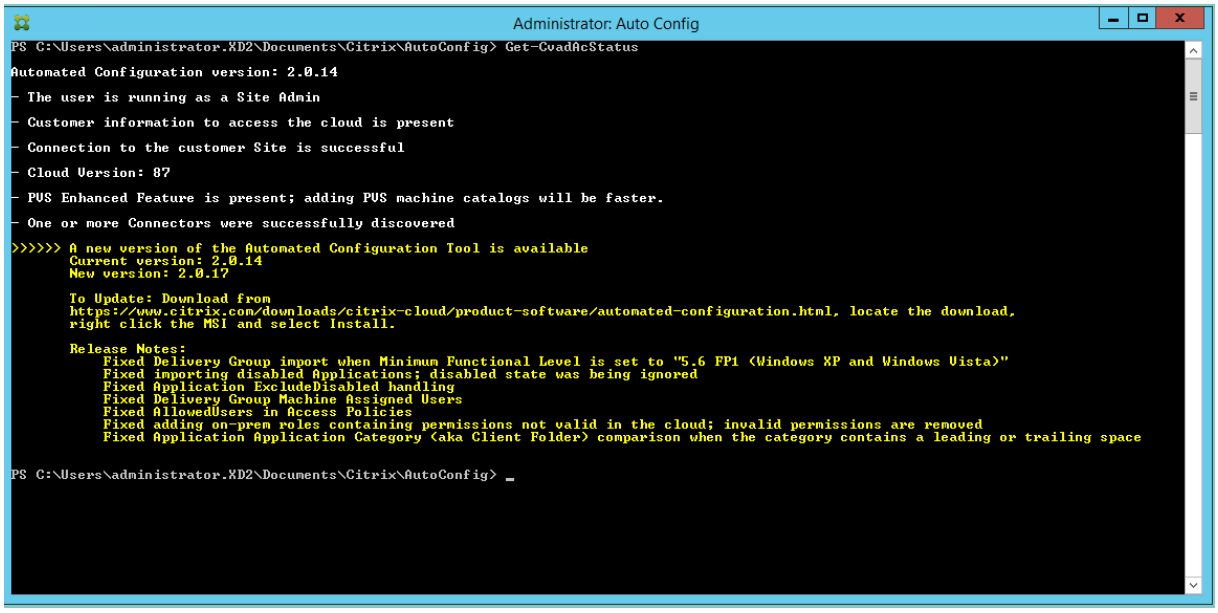
自動構成のダウンロード

Citrix のダウンロードから自動構成ツールをダウンロードしてインストールします。

> 重要：
>
> 機能エラーを防止するために、常に最新バージョンの自動構成を使用してください。

自動構成のアップグレード

自動構成でクラウドにアクセスするコマンドレットを実行するときに、ダウンロード可能な新しいバージョンがある場合、ツールから通知が行われます。



以下の手順に従って、最新バージョンであることを確認できます：

1. 自動構成アイコンをダブルクリックします。PowerShell ウィンドウが表示されます。

2. 次のコマンドを実行して、バージョン番号を確認します。

   ```
   Get-CvadAcStatus
   ```

3. 通知またはCitrix のダウンロードに表示されているバージョンと、使用しているツールのバージョンを確認します。ツールの最新バージョンはそこにあります。
4. ツールの最新バージョンをダウンロードしてインストールします。自動構成をアップグレードするために古いバージョンをアンインストールする必要はありません。

> 注:
>
> 通知は、クラウドにアクセスするコマンドレットを実行するたびに表示されます。コマンドレットについて詳しくは、「自動構成ツールコマンドレット」を参照してください。

既知の制限事項

- Machine Creation Services を通じてプロビジョニングされたマシンカタログには、特別な考慮事項があります。Machine Creation Services について詳しくは、「Machine Creation Services でプロビジョニングされたカタログの移行について」を参照してください。

サポートされている移行オブジェクト

自動構成では、次のコンポーネントの構成の移動がサポートされています:

- タグ
- 代理管理者
  - スコープ
  - 役割
- ホスト接続
  - 単一リソースプール
  - 管理者スコープ
- マシンカタログ
  - 管理者スコープ
  - マシン
  - リモート PC アクセス、物理、プール、プロビジョニング済み、MCS、割り当て済み
- StoreFront
- デリバリーグループ
  - アクセスポリシー

  - 管理者スコープの関連付け
  - アプリケーションアクセスポリシー
  - 割り当てポリシー
  - 使用権/デスクトップポリシー
  - 電源スケジュール
  - 残留セッション
  - セッションの事前起動
  - 再起動スケジュール
  - タグ

- アプリケーショングループ

  - 管理者スコープの関連付け
  - デリバリーグループ
  - ユーザーおよびグループ

- アプリケーション

  - アプリケーションフォルダー
  - アイコン
  - アプリケーション
  - ブローカー構成済み FTA
  - タグ

- グループポリシー
- ユーザーゾーンの優先度

コンポーネントの移行順序

コンポーネントとその依存関係はこちらに一覧表示されています。コンポーネントをインポートまたはマージする前に、コンポーネントの依存関係が適切に設定されている必要があります。依存関係が欠落していると、インポートまたはマージコマンドが失敗する可能性があります。インポートまたはマージが失敗した場合、欠落している依存関係がログファイルの **Fixups** セクションに表示されます。

1. タグ

   - 事前依存関係なし

2. 代理管理者

   - 事前依存関係なし

3. ホスト接続

   - CvadAcSecurity.yml のセキュリティ情報

4. マシンカタログ
    - Active Directory に存在するマシン
    - ホスト接続
    - タグ
5. StoreFront
6. デリバリーグループ
    - Active Directory に存在するマシン
    - Active Directory に存在するユーザー
    - マシンカタログ
    - タグ
7. アプリケーショングループ
    - デリバリーグループ
    - タグ
8. アプリケーション
    - デリバリーグループ
    - アプリケーショングループ
    - タグ
9. グループポリシー
    - デリバリーグループ
    - タグ
10. ユーザーゾーンの優先度

一般的な前提条件

以下は、自動構成が正しく機能するために必要な一般的な前提条件です。これらの前提条件は、オンプレミスからクラウドへの移行とクラウドからクラウドへの移行の両方で使用されます。

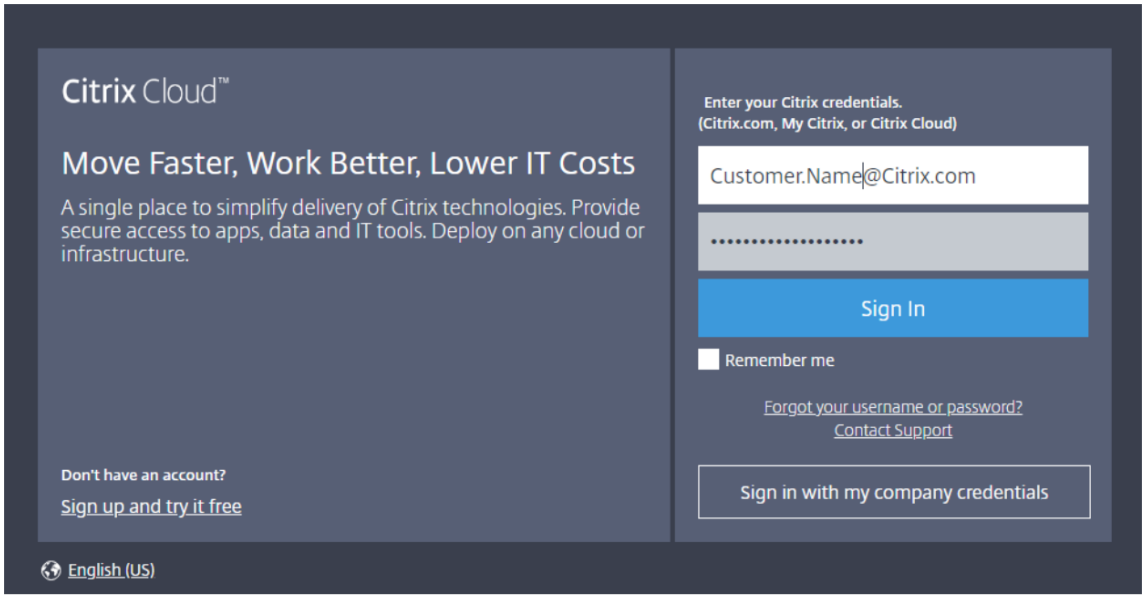
顧客 **ID**、クライアント **ID**、および秘密キーの生成

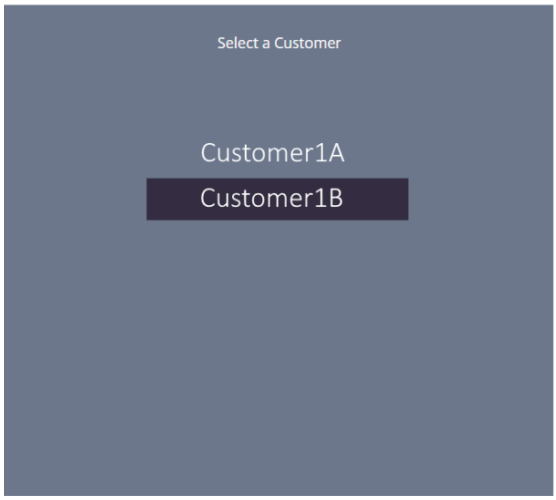
自動構成を使用して移行を開始する前に、Citrix Cloud 顧客 ID が必要であり、構成を Citrix Cloud にインポートするためのクライアント ID と秘密キーを作成する必要があります。クラウドにアクセスするすべてのコマンドレットには、これらの値が必要です。

次の手順で、顧客 ID を取得し、クライアント ID と秘密キーを作成できます。

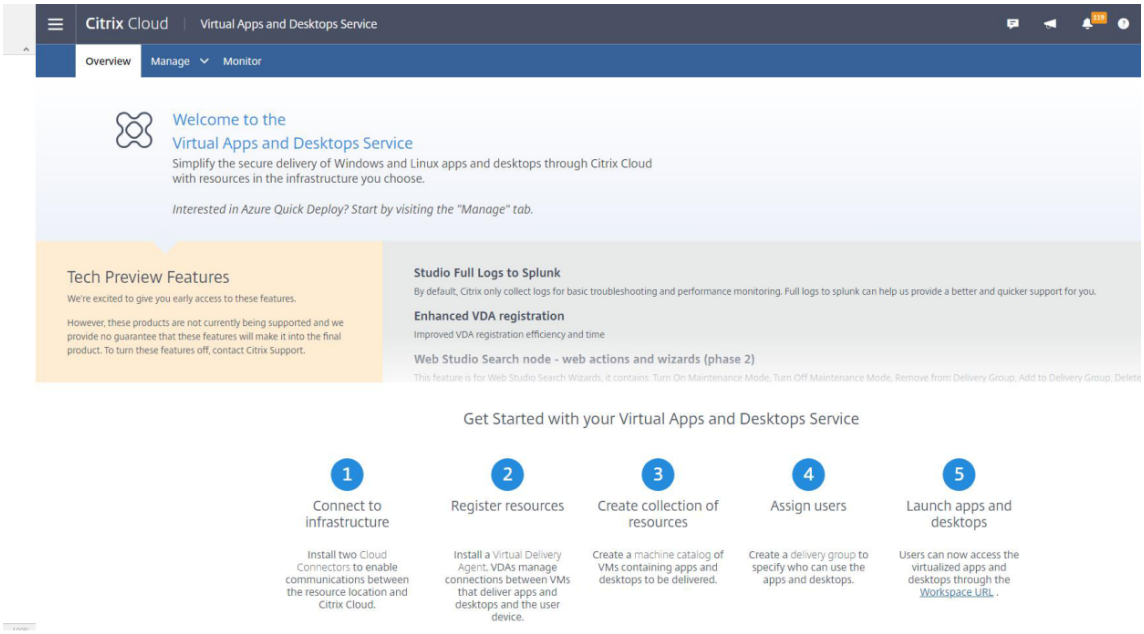
顧客 **ID** を取得するには:

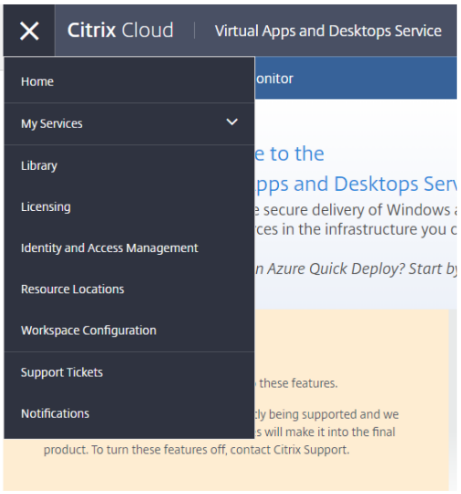
1. Citrix Cloud アカウントにサインインして、顧客を選択します。



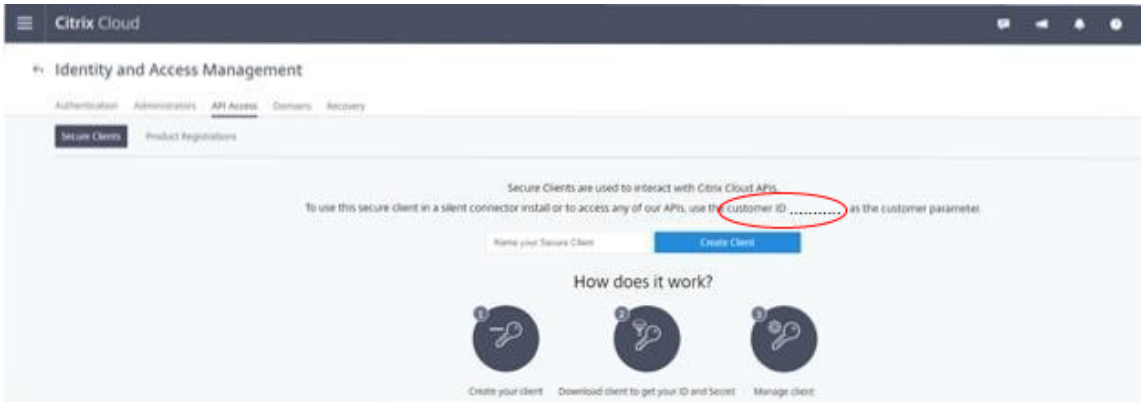


2. ハンバーガーメニューをクリックして、ドロップダウンメニューから ［**ID** およびアクセス管理］を選択します。



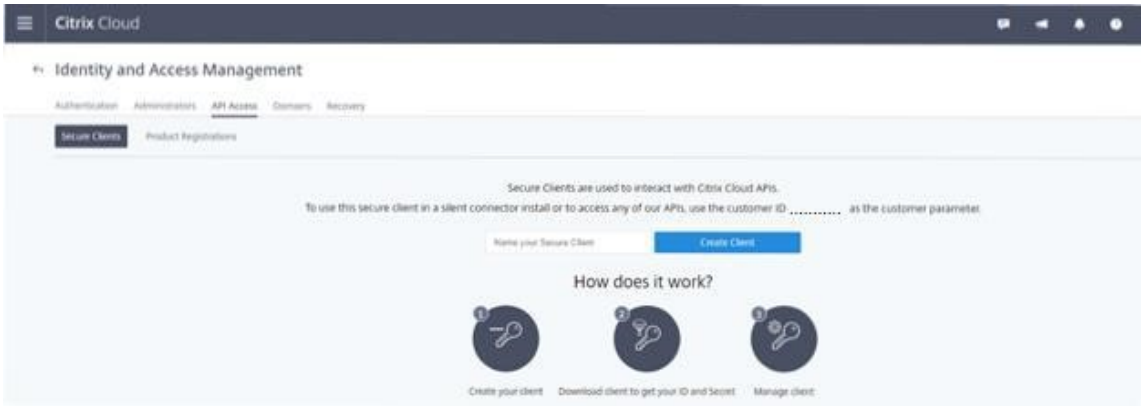


3. 顧客 **ID** は ［**ID** およびアクセス管理］ページで確認できます。

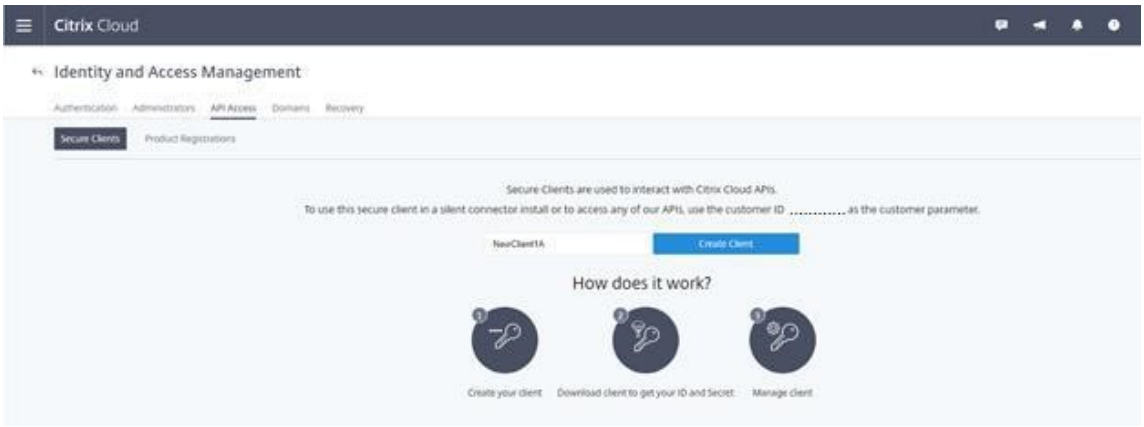


クライアント **ID** と秘密キーを取得するには:

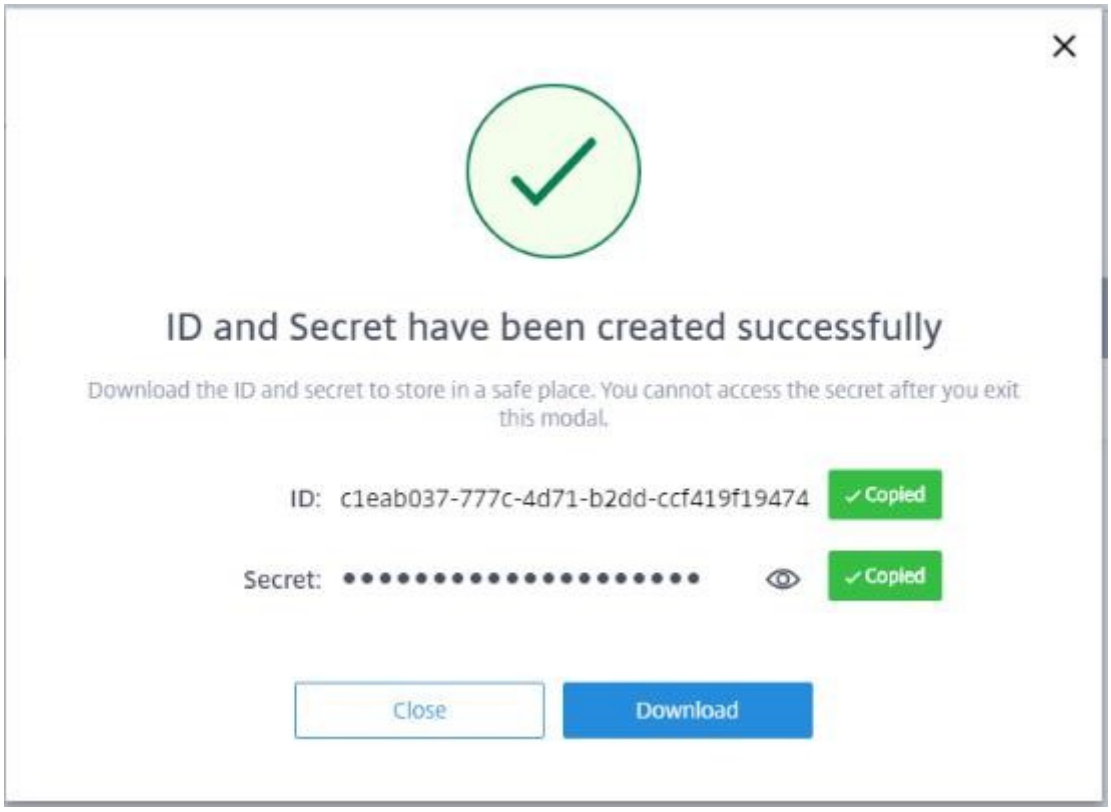
1. ［**ID** およびアクセス管理］ページで ［**API** アクセス］タブをクリックします。



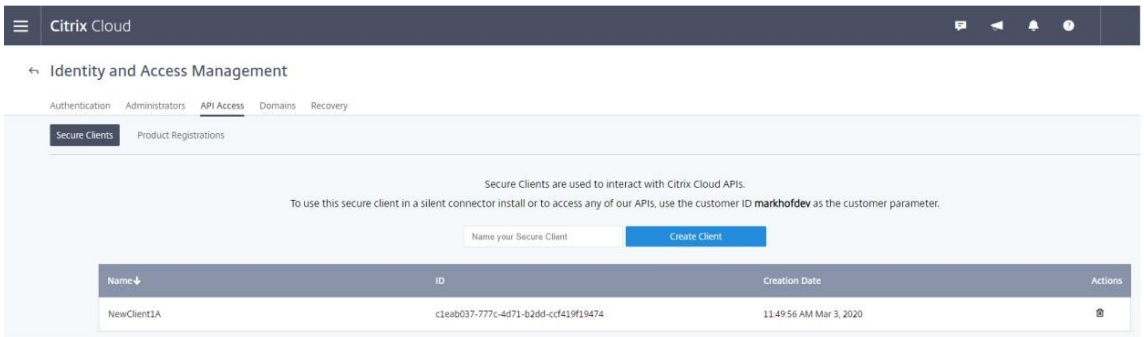
2. ボックスに名前を入力します。この名前は、複数のクライアント ID と秘密キーを区別するために使用されます。［クライアントの作成］をクリックして、クライアント ID と秘密キーを作成します。



3. クライアント ID と秘密キーが正常に作成されると、次のダイアログボックスが表示されます。両方の値を安全な場所にコピーするか、この情報を含む.csv ファイルをダウンロードしてください。.csv ファイルを使用して CustomerInfo.yml ファイルを作成できます。



4. クライアント ID と秘密キーが正常に作成されます。



これらの値を安全な場所に配置し、ツールやクラウド Rest API へのアクセスが必要な信頼できる企業メンバーのみと共有します。クライアント ID と秘密キーに有効期限はありません。これらが危険にさらされた場合には、[ゴミ箱] アイコンを使用してすぐに削除し、新しいものを作成します。

> 注:
>
> 秘密キーは、紛失したり忘れたりすると取得できません。新しいクライアント ID と秘密キーを作成する必要があります。

顧客情報ファイルの作成

CustomerInfo.yml ファイルを使用すると、各コマンドレットの実行時に、顧客情報パラメーターを指定する必要がなくなります。すべての顧客情報は、コマンドレットパラメーターを使用して上書きできます。

New-CvadAcCustomerInfoFileコマンドレットを使用することで CustomerInfo.yml ファイルを作成します。

> 重要:
>
> CustomerInfo.yml ファイルを手動で編集しないでください。これを行うと、不注意によるフォーマットエラーが発生する可能性があります。

New-CvadAcCustomerInfoFileには、以下の必須パラメーターがあります。

- CustomerId —顧客の ID。
- ClientId —Citrix Cloud で作成された、顧客のクライアント ID。
- Secret —Citrix Cloud で作成された、顧客のシークレット。

```
New-CvadAcCustomerInfoFile -CustomerId markhof123 -ClientId 6813EEA6
-46CC-4F8A-BC71-539F2DAC5984 -Secret TwBLaaaaaaaaaaaaaaaaw==
```

ダウンロードした security.csv ファイルを指すSecurityCsvFileSpecパラメーターを使用して CustomerInfo.yml を作成することもできます。CustomerId も指定する必要があります。

```
New-CvadAcCustomerInfoFile -SecurityCsvFileSpec C:\Users\my_user_name
\downloads/security.csv -CustomerId markhof123
```

Set-CvadAcCustomerInfoFileコマンドレットを使用して CustomerInfo.yml ファイルを更新します。このコマンドレットではクライアント ID のみが変更されます。

```
Set-CvadAcCustomerInfoFile -ClientId C80487EE-7113-49F8-85DD-2CFE30CC398E
```

以下は、CustomerInfo.yml ファイルの例です。

```
# Created/Updated on 2020/01/29 16:46:47
CustomerId:  'markhof123'
ClientId:  '6713FEA6-46CC-4F8A-BC71-539F2DDK5384'
Secret:  'TwBLaaabbbaaaaaaaaaw=='
Environment: Production
AltRootUrl:  ''
StopOnError: False
AlternateFolder:  ''
Locale:  'en-us'
Editor:  'C:\Program Files\Notepad++\notepad++.exe'
Confirm: True
DisplayLog: True
```


ゾーンマッピングファイルの作成

オンプレミスゾーンは、クラウドのリソースの場所に相当します。他のサイトコンポーネントとは異なり、オンプレミスゾーンをクラウドに自動的にインポートすることはできません。代わりに、ZoneMapping.yml ファイルを使用して、手動でマップする必要があります。ゾーン名が既存のリソースの場所の名前と関連付けられていない場合、インポートエラーが発生することがあります。

ゾーンが 1 つしかないオンプレミスサイトとリソースの場所が 1 つしかないクラウドサイトの場合、自動構成ツールは正しい関連付けを行うため、ZoneMapping.yml ファイルを手動で管理する必要はありません。

複数のゾーンを持つオンプレミスサイトまたは複数のリソースの場所を持つクラウドサイトの場合、オンプレミスゾーンからクラウドのリソースの場所への正しいマッピングが反映されるように、ZoneMapping.yml ファイルを手動で更新する必要があります。これは、クラウドへのインポート操作を試行する前に実行する必要があります。

ZoneMapping.yml ファイルは、*%HOMEPATH%\Documents\Citrix\AutoConfig* にあります。.yml ファイルには、キーがゾーン名、値がリソースの場所の名前の辞書が定義されます。

例として、プライマリゾーン「Zone-1」とセカンダリゾーン「Zone-2」を持つオンプレミスの Citrix Virtual Apps and Desktops サイトが Citrix DaaS 環境に移行されると、2 つの新しく作成されたクラウドのリソースの場所は「Cloud-RL-1」および「Cloud-RL-2」になります。この例では、ZoneMapping.yml は次のように構成されます:

```
1               Zone-1: Cloud-RL-1
2
3               Zone-2: Cloud-RL-2
```

> 注:
>
> コロンとリソースの場所の名前との間にはスペースが必要です。ゾーンまたはリソースの場所の名前にスペースが使用されている場合は、名前を引用符で囲みます。

ホスト接続

ホスト接続とそれに関連するハイパーバイザーは、自動構成を使用してエクスポートおよびインポートできます。

ホスト接続にハイパーバイザーを追加するには、ハイパーバイザーのタイプに固有のセキュリティ情報が必要となります。セキュリティ上の配慮から、オンプレミスのサイトからこの情報をエクスポートすることはできません。自動構成でホスト接続とハイパーバイザーをクラウドサイトに正常にインポートできるように、この情報を手動で指定する必要があります。

エクスポート処理により、*%HOMEPATH%\Documents\Citrix\AutoConfig* に CvadAcSecurity.yml ファイルが作成されます。このファイルには、特定の種類のハイパーバイザーに必要な各セキュリティアイテムのプレースホルダーが含まれています。クラウドサイトにインポートする前に、CvadAcSecurity.yml ファイルを更新する必要があります。管理者の更新は複数のエクスポートにわたって保持され、必要に応じて新しいセキュリティプレースホルダーが追加されます。セキュリティアイテムは削除されません。詳しくは、「cvadacSecurity.yml ファイルを手動で更新してください」を参照してください。


```
HostConn1:
ConnectionType: XenServer
UserName: root
PasswordKey: rootPassword
HostCon2:
ConnectionType: AWS
ApiKey: 78AB6083-EF60-4D26-B2L5-BZ35X00DA5CH
SecretKey: TwBLaaaaaaaaaaaaaaaaw==
Region: East
```

ハイパーバイザーごとのセキュリティ情報　以下に、ハイパーバイザーの種類ごとに必要なセキュリティ情報を示します。

- XenServer、Hyper-V、VMware
  - ユーザー名
  - クリアテキストパスワード
- Microsoft Azure
  - サブスクリプション ID
  - アプリケーション ID
  - アプリケーションシークレット
- Amazon Web Services
  - サービスアカウント ID
  - アプリケーションシークレット
  - リージョン

セキュリティに関する特別な注意事項　セキュリティ情報はすべてクリアテキストで入力されます。クリアテキストが推奨されない場合は、ホスト接続および関連するハイパーバイザーは、［管理］**>**［完全な構成］インターフェイスを使用して手動で作成できます。ホスト接続およびハイパーバイザー名は、ホスト接続を使用するマシンカタログが正常にインポートされるように、オンプレミスのホスト接続およびハイパーバイザー名と正確に一致する必要があります。

サイトのアクティブ化

オンプレミスサイトとクラウドサイトの両方の Delivery Controller は、仲介するデスクトップやアプリケーション、再起動するマシンなどのリソースを制御します。共通のリソースセットが 2 つ以上のサイトによって制御されている場合に問題が発生します。このような状況は、オンプレミスサイトからクラウドサイトに移行するときに発生する可能性があります。オンプレミスとクラウドの Delivery Controller の両方でリソースの同じセットを管理するこ

とは可能です。このような二重管理をすると、リソースを利用できず管理できなくなることにつながる可能性があり、診断が困難になることがあります。

サイトのアクティブ化により、アクティブなサイトを制御する場所を制御できます。

サイトのアクティブ化は、デリバリーグループメンテナンスモードを使用して管理します。サイトが非アクティブの場合、デリバリーグループはメンテナンスモードになります。メンテナンスモードは、アクティブなサイトのデリバリーグループでは解除されます。

サイトのアクティブ化によって、VDA 登録またはマシンカタログが影響を受けたり管理されることはありません。

- `Set-CvadAcSiteActiveStateCloud`
- `Set-CvadAcSiteActiveStateOnPrem`

すべてのコマンドレットで、`IncludeByName`および`ExcludeByName` フィルタリングがサポートされています。このパラメーターを使用すると、メンテナンスモードを変更できるデリバリーグループを選択できます。デリバリーグループは、必要に応じて選択的に変更できます。

制御のインポートとクラウドへの転送

以下は、オンプレミスサイトからクラウドサイトに制御をインポートして転送する方法の概要です。

1. オンプレミスサイトをクラウドにエクスポートおよびインポートします。どのインポートコマンドレットにも `-SiteActive`パラメーターがないことを確認してください。オンプレミスサイトはアクティブで、クラウドサイトは非アクティブです。デフォルトでは、クラウドサイトのデリバリーグループはメンテナンスモードになっています。
2. クラウドのコンテンツと構成を確認します。
3. 営業時間外は、オンプレミスサイトを非アクティブに設定します。 `-SiteActive`パラメーターが存在しない必要があります。すべてのオンプレミスサイトのデリバリーグループはメンテナンスモードになっています。
    - `Set-CvadAcSiteActiveStateOnPrem`
4. クラウドサイトをアクティブに設定します。 `-SiteActive`パラメーターが存在する必要があります。クラウドサイトのデリバリーグループはメンテナンスモードになっていません。
    - `Set-CvadAcSiteActiveStateCloud -SiteActive`
5. クラウドサイトがアクティブであり、オンプレミスサイトが非アクティブであることを確認します。

制御をオンプレミスサイトに戻す

クラウドサイトからオンプレミスサイトに制御を転送するには:

1. 営業時間外は、クラウドサイトを非アクティブに設定します。すべてのクラウドサイトのデリバリーグループはメンテナンスモードになっています。

- `Set-CvadAcSiteActiveStateCloud`

2. オンプレミスサイトをアクティブに設定します。オンプレミスサイトのデリバリーグループはメンテナンスモードになっていません。

   - `Set-CvadAcSiteActiveStateOnPrem -SiteActive`

サイトのアクティブ化に関する追加情報

- 電源が管理されているマシンがなく再起動スケジュールがない場合（これは通常、ホスト接続もないことを意味します）、すべてのクラウドのデリバリーグループをアクティブ状態でインポートできます。インポート後に、`Merge-CvadAcToSite`/`Import-CvadAcToSite`に`-SiteActive`を追加、または`Set-CvadAcSiteActiveStateCloud -SiteActive`を実行します。
- マシンの電源が管理されている場合、または再起動スケジュールがある場合は、別のプロセスが必要です。たとえば、この状況でオンプレミスからクラウドに切り替える場合は、`Set-CvadAcSiteActiveStateOnPrem`を使用してオンプレミスサイトを非アクティブに設定します。次に、`Set-CvadAcSiteActiveStateCloud -SiteActive`を使用して、クラウドサイトをアクティブに設定します。
- `Set-CvadAcSiteActiveStateCloud`および`Set-CvadAcSiteActiveStateOnPrem`コマンドレットは、逆のプロセスを実行する場合にも使用します。たとえば、`-SiteActive`パラメーターなしで`Set-CvadAcSiteActiveStateCloud`を実行してから、`-SiteActive`パラメーター付きで`Set-CvadAcSiteActiveStateOnPrem`を実行します。

Machine Creation Services でプロビジョニングされたカタログの移行について

> 注:
>
> この機能は、バージョン 3.0 以降でのみ使用できます。自動構成内で`Get-CvadAcStatus`を使用してバージョンを確認してください。

Machine Creation Services（MCS）カタログでは、次の 2 種類のカタログが作成されます:

- マシンに加えられた変更が失われたか無効になった場合（通常は、アプリケーションが公開されているサーバー OS）- これは、プール型 VDI またはマルチセッションのユースケースです
- マシンに加えられた変更が再起動後も保持される場合（通常は、専用ユーザーがいるクライアント OS）- これは、静的 VDI のユースケースです

カタログの種類は、Citrix Studio でカタログノードにおいて、カタログの「ユーザーデータ:」値で確認できます。

> 注:
>
> 自動構成を使用して MCS をクラウドからバックアップすることはできません。

プール型 **VDI** またはマルチセッションのカタログ

「ユーザーデータ：破棄」となっているカタログは、プール型 VDI のカタログであり、メインイメージと構成のみを移行できます。これらのカタログ内の仮想マシンは移行されません。これは、仮想マシンのライフサイクルがインポート元のサイトによって維持されているためです。つまり、マシンの電源がオンになるたびに、その状態が変化する可能性があります。これにより、仮想マシンのインポートデータがすぐに同期されなくなるのでインポートが不可能になります。

ツールを使用してこれらのカタログを移行すると、カタログメタデータが作成され、メインイメージの作成が開始されますが、マシンはインポートされません。

このプロセスは、メインイメージのサイズによっては作成に時間がかかる場合があるため、ツール内のインポートコマンドは、MCS カタログの作成を開始するだけであり、その終了まで待ちません。インポートが完了したら、クラウド環境で［完全な構成］管理インターフェイスを使用して、カタログ作成の進行状況をモニターします。

メインイメージが作成されたら、マシンをプロビジョニングできます。オンプレミスでの使用によって容量が消費されるので、容量について考慮する必要があります。

そのカタログを使用する他のすべてのオブジェクト（デリバリーグループ、アプリケーション、ポリシーなど）をインポートでき、メインイメージの作成を待つ必要はありません。カタログの作成が完了したら、インポートしたカタログにマシンを追加できます。その後、ユーザーがそれらのリソースを起動できます。

> 注:
>
> ツール内で使用できるのと同じコマンドを使用して、カタログや他のすべてのオブジェクトを移行します。

静的 **VDI** のカタログ

> 注:
>
> この操作ではデータベースに保存されている低レベルの詳細がインポートされるので、このプロセスは、データベースにアクセスできるマシンから実行する必要があります。

静的 VDI のカタログでは、メインイメージ、構成、およびすべての仮想マシンが移行されます。プール型 VDI のユースケースとは異なり、イメージを作成する必要はありません。

VDA をクラウドに登録するには、VDA でコネクタが参照されている必要があります。

再起動スケジュール、電源管理、およびその他の項目がクラウドによって制御されるように、クラウドサイトをアクティブにするには、「サイトのアクティブ化」セクションを参照してください。

移行の完了後に、オンプレミスサイトからこのカタログを削除する必要がある場合は、VM と AD アカウントの保持を選択する必要があります。そうしないと、それらは削除され、クラウドサイトは削除された VM を参照したままになります。

移行後に孤立したリソースを検出するために **MCS** タグを更新する

オンプレミス構成からクラウドサイトに移行した後、またはクラウド構成から別のクラウドサイトに移行した後、永続的な VM の場合は孤立したリソースが正しく検出できるように MCS サイト ID タグを更新する必要があります。これを行うには、PowerShell コマンド`Set-ProvResourceTags`を使用します。現在、この機能は Azure に適用されます。

詳細な手順は次のとおりです:

1. PowerShell コマンド`Set-ProvResourceTags`を使用して、新しい Citrix サイトから MCS サイト ID タグを更新します。例:

   ```
   Set-ProvResourceTags -ProvisioningSchemeUid xxxxx  [-VMName <
       String>] [-VMBatchSize XX] [-ResourceType XX]
   <!--NeedCopy-->
   ```

   または

   ```
   Set-ProvResourceTags -ProvisioningSchemeName xxxxx  [-VMName <
       String>] [-VMBatchSize XX] [-ResourceType XX]
   <!--NeedCopy-->
   ```

パラメーターの詳細は次のとおりです:

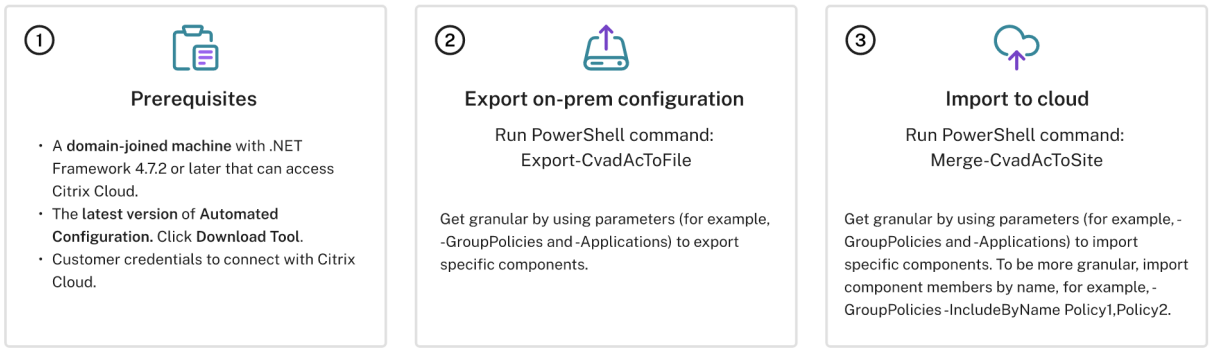
- `ProvisioningSchemeUid`または`ProvisioningSchemeName`は必須パラメーターです。
- `VMName`はオプションのパラメーターです。`VMName`が指定されていない場合、このマシンカタログのすべての VM のタグが更新されます。
- `VMBatchSize`は、すべての VM をバッチに分割するためのオプションのパラメーターです。`VMBatchSize`が指定されていない場合は、デフォルト値（10）が適用されます。範囲は 1〜60 です。
- `ResourceType`は、次のいずれかになります:
  - `MachineCatalog`: マシンカタログリソースのタグを更新します。
  - `VirtualMachine`: VM 関連リソースのタグを更新します。
  - `All`:（デフォルトの ResourceType）: マシンカタログと VM 関連リソースの両方のタグを更新します。

オンプレミスからクラウドへの移行

May 17, 2024

自動構成を使用すると、オンプレミス構成のクラウドサイトへの移行を自動化できます。

次の画像は、構成をクラウドに移行するために自動構成でできることの概要です。



構成を移行するための前提条件

Citrix Virtual Apps and Desktops から構成をエクスポートする場合は、次のものが必要です:

- Citrix Virtual Apps and Desktops：現在のリリースとその直前のリリース、または Citrix Virtual Apps and Desktops、XenApp と XenDesktop LTSR：すべてのバージョン
- .NET Framework 4.7.2 以降および Citrix PowerShell SDK を備えたドメイン参加済みマシン。これは Delivery Controller に自動的にインストールされます（オンプレミス Delivery Controller 以外のマシンで実行するには、適切な PowerShell スナップインがインストールされるように、Citrix Studio がインストールされている必要があります。Studio のインストーラーは、Citrix Virtual Apps and Desktops のインストールメディアに格納されています）。

Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）に構成をインポートする場合は、次のものが必要です:

- Citrix Cloud にアクセスできるマシン。これは、Delivery Controller やドメイン参加済みマシンである必要はありません。
- プロビジョニングされた Citrix DaaS。
- コネクタがインストールされた、オンプレミスセットアップと同じドメインにドメイン参加済みのアクティブなリソースの場所。
- Citrix Cloud にアクセスするサイトへの接続が許可され、利用可能であること。詳しくは、「システムおよび接続要件」を参照してください。

> 注:
>
> 自動構成は、Cloud Connector システムにインストールできません。

Citrix Virtual Apps and Desktops オンプレミス構成のエクスポート

> 重要:
>
> - 顧客 ID、クライアント ID、および秘密キー情報を含む CustomerInfo.yml ファイルが必要です。顧客

ID、クライアント ID、および秘密キーの取得方法について詳しくは、「顧客 ID、クライアント ID、および秘密キーの生成」を参照してください。この情報を CustomerInfo.yml ファイルに追加する方法については、「顧客情報ファイルの作成」を参照してください。
- ZoneMapping.yml ファイルには、オンプレミスゾーンをクラウド内のリソースの場所にマップする情報が含まれている必要があります。ゾーンのマッピング方法について詳しくは、「ゾーンマッピングファイルの作成」を参照してください。
- ホスト接続がある場合、対応する情報を CvadAcSecurity.yml ファイルに入力する必要があります。

1. 自動構成をインストールします。
2. 自動構成アイコンをダブルクリックします。PowerShell ウィンドウが表示されます。
3. 次のコマンドを実行して、すべてのコンポーネントをエクスポートします。オンプレミス構成は、エクスポートしてもまったく変更されません。

   ```
   Export-CvadAcToFile
   ```

コマンドレットを初めて実行すると、.yml 構成ファイルとログを含むエクスポートフォルダーが作成されます。このフォルダーは *%HOMEPATH%\Documents\Citrix\AutoConfig* にあります。連続してエクスポートするたびに、サブフォルダーが作成されます。親フォルダー*%HOMEPATH%\Documents\Citrix\AutoConfig* には、常に最新のエクスポートでエクスポートされたファイルが含まれます。

注:

自動構成が Delivery Controller にインストールされていない場合は、ツールを使用する前に PowerShell で「`import-module Citrix.AutoConfig.Commands`」を実行してください。自動構成アイコンを使用して自動構成を開く場合、この作業は必要ありません。

エラーや例外が発生した場合は、ログファイルの **Fixups** セクションを参照してください。

Citrix DaaS への構成のインポート

重要:

- 顧客 ID、クライアント ID、および秘密キー情報を含む CustomerInfo.yml ファイルが必要です。顧客 ID、クライアント ID、および秘密キーの取得方法について詳しくは、「顧客 ID、クライアント ID、および秘密キーの生成」を参照してください。この情報を CustomerInfo.yml ファイルに追加する方法については、「顧客情報ファイルの作成」を参照してください。
- ZoneMapping.yml ファイルには、オンプレミスゾーンをクラウド内のリソースの場所にマップする情報が含まれている必要があります。ゾーンのマッピング方法について詳しくは、「ゾーンマッピングファイルの作成」を参照してください。
- ホスト接続がある場合、対応する情報を CvadAcSecurity.yml ファイルに入力する必要があります。
- オンプレミスの展開をクラウドに移行する場合は、Citrix 設定を含むドメインと OU GPO がクラウドに移行されていることを確認してください。Citrix Web Studio は GPMC をサポートしていないため、ドメインおよび OU GPO は Web Studio に表示されません。Citrix ポリシーエンジンは、ドメインおよ

> び OU 内の VDA およびユーザーにドメインおよび OU GPO を適用します。VDA にログインすると、ユーザーはドメインおよび OU GPO のポリシーがセッションに適用されていることを確認できます。ただし、管理者はこれらのポリシーと設定を確認できないため、混乱が発生する可能性があります。

インポートの実行

1. 自動構成アイコンをダブルクリックします。PowerShell ウィンドウが表示されます。
2. 次のコマンドを実行して、すべてのコンポーネントをインポートします。

   ```
   Merge-CvadAcToSite
   ```

最新の状態により、想定される状態を確認します。さまざまなインポートオプションにより、インポート結果が同一であるか、オンプレミスサイトのサブセットであるかを制御します。

コマンドレットを実行すると、.yml 構成ファイルとログを含むエクスポートフォルダーが作成されます。このフォルダーは *%HOMEPATH%\Documents\Citrix\AutoConfig* にあります。

エラーや例外が発生した場合は、ログファイルの **Fixups** セクションを参照してください。

> 注:
>
> 自動構成が Delivery Controller にインストールされていない場合は、ツールを使用する前に PowerShell で「`import-module Citrix.AutoConfig.Commands`」を実行してください。自動構成アイコンを使用して自動構成を開く場合、この作業は必要ありません。

元の Citrix DaaS 構成に戻す方法については、「Citrix DaaS 構成のバックアップ」を参照してください。

インポート操作の詳細

インポートプロセスは、更新を正確に実行し、必要な更新のみを実行し、すべての更新が正しく行われたことを確認するように設計されています。すべてのインポート操作で実行される手順は次のとおりです。

1. エクスポートされた.yml ファイルを読み取ります（予想される状態）。
2. クラウドを読み取ります（現在の状態）。
3. インポート前のクラウドの状態を.yml ファイルにバックアップします（必要に応じてバックアップ前の状態を復元できます）。
4. 予想される状態と現在の状態の違いを評価します。これにより、どの更新を行うかが決まります。
5. 更新します。
6. クラウドを読み直します（新しい現在の状態）。
7. インポート後のクラウドの状態を.yml ファイルにバックアップします（必要に応じてバックアップ後の状態を復元できます）。
8. 新しい現在の状態を予想された状態と比較します。
9. 比較の結果を報告します。

詳細な移行

> 重要:
>
> コンポーネントの移行順序について詳しくは、「コンポーネントの移行順序」を参照してください。

コンポーネントのみ、またはコンポーネント名のみを選択的に移行できます。

- サポートされているコンポーネントパラメーターとしては、`MachineCatalogs`や `Tags`などがあります。
- サポートされているコンポーネント名パラメーターとしては、`IncludeByName`や`ExcludeByName`などがあります。

パラメーターとその使用方法について詳しくは、「詳細な移行のパラメーター」を参照してください。

サイトのアクティブ化

サイトのアクティブ化により、どのサイトがアクティブであるかを制御することや、リソースを制御することができます。詳しくは、「サイトのアクティブ化」を参照してください。

複数のサイトを 1 つのサイトにマージする

March 31, 2024

自動構成でのマルチサイトサポートは、複数のオンプレミスサイトを単一のクラウドサイトにマージする方法を提供します。

マルチサイトサポートは、オンプレミスサイトごとにコンポーネント名に一意のプレフィックスとサフィックスを追加し、複数のオンプレミスサイトが単一のクラウドサイトにマージされた後の名前の一意性を保証します。

プレフィックスとサフィックスは、オンプレミスサイトごとに次の各コンポーネントに割り当てることができます。

- `AdminScope`
- `AdminRole`
- `ApplicationAdmin`
- `ApplicationFolder`
- `ApplicationGroup`
- `ApplicationUser`
- `DeliveryGroup`
- `GroupPolicy`
- `HostConnection`
- `MachineCatalog`

- StoreFront
- Tag

アプリケーションフォルダーは、プレフィックス、サフィックス、およびルート変更をサポートしています。ルート変更により、アプリケーションの既存のフォルダー構造にトップレベルのフォルダーが追加されます。

プレフィックスとサフィックスの規則

1. プレフィックスとサフィックスには、次の特殊文字を含めることができません: \ , / ; : # . * ? = < > | ( )"' { } [ ]
2. プレフィックスとサフィックスでは、末尾にスペースを入れられますが先頭には入れられません。
3. プレフィックスとサフィックスでは、末尾にスペースを入れるために二重引用符で囲む必要があります。
4. プレフィックスとサフィックスは、インポート時、マージ時、および追加時に適用されます。ソースの.yml ファイルが変更されることはありません。
5. プレフィックスとサフィックスの処理では、依存するコンポーネントがある場合にそのコンポーネントの名前に自動的にプレフィックスまたはサフィックスを付けます。たとえば、マシンカタログ名のプレフィックスが「East」になっている場合、それらのカタログ名を参照するデリバリーグループもプレフィックスが「East」になっています。
6. コンポーネント名に既にプレフィックスまたはサフィックスが付いている場合、プレフィックスまたはサフィックスは追加されません。コンポーネント名に、まったく同じプレフィックスまたはサフィックスを二重に含めることはできません。
7. プレフィックスとサフィックスは、個別に使用することも、組み合わせて使用することもできます。
8. コンポーネントでプレフィックスまたはサフィックスを使用するかどうかはオプションです。

> 注:
>
> 完全な構成インターフェイスでは、コンポーネントがアルファベット順に表示されます。

サイトでグループ化

プレフィックスを使用して、単一のサイトのコンポーネントを視覚的にグループ化します。各サイトは、異なるサイトグループをアルファベット順にしてプレフィックスを付けた独自のグループでリストされます。

名前でグループ化

サフィックスを使用して、複数のサイトから似た名前のコンポーネントを視覚的にグループ化します。異なるサイトからの似た名前のコンポーネントは、視覚的に交互に並びます。

SitePrefixes.yml ファイル

サイトのプレフィックス管理は、1 つまたは複数のオンプレミスサイトのサイトプレフィックスおよびサフィックスのマッピング情報を含む SiteMerging.yml ファイルから始めます。SiteMerging.yml ファイルは手動で管理するか、「複数のオンプレミスサイトのマージのコマンドレット」セクションにリストされている利用可能なコマンドレットを使用して管理できます。

エクスポート、インポート、マージ、および追加

オンプレミスサイトをエクスポートするまで、マージを開始することはできません。オンプレミスサイトをエクスポートするには、「オンプレミスからクラウドへの移行」を参照してください。

中央エクスポートターゲットフォルダー

このセクションで説明する方法では、複数のサイトエクスポートを中央のファイル共有場所に配置します。SiteMerging.yml ファイル、CustomerInfo.yml ファイル、およびすべてのエクスポートファイルは、そのファイル共有場所に存在するため、オンプレミスサイトから独立した 1 つの場所からインポートを実行できます。

クラウドアクセス操作は、オンプレミスサイトまたは Active Directory を参照しないため、どこからでもクラウドアクセス操作を実行できます。

直接ファイル共有

エクスポート、インポート、マージ、および新規/追加操作では、デフォルトフォルダー（*%HOMEPATH%\Documents\Citrix\AutoConfig*）以外のフォルダーをターゲットまたはソースにするためのパラメーターを提供します。次の例では、管理者が既にアクセス権限を持っている`\\share.central.net`にある中央ファイル共有を使用し、必要に応じて資格情報を入力しています。

エクスポートのターゲットをサイト固有のフォルダーにするには、`-TargetFolder`パラメーターを使用します:

East DDC から:

```
mkdir \\share.central.net\AutoConfig\SiteEast

Export-CvadAcToFile -TargetFolder \\share.central.net\AutoConfig\
SiteEast
```

West DDC から:

```
mkdir \\share.central.net\AutoConfig\SiteWest

Export-CvadAcToFile -TargetFolder \\share.central.net\AutoConfig\
SiteWest
```


エクスポートが完了したら、CustomerInfo.yml ファイルと SiteMerging.yml ファイルを作成して\\share.central.net\AutoConfigに配置します。

> 注:
>
> この直接ファイル共有参照方式を使用する場合は、SitePrefixes.yml を作成するときにSiteRootFolderパラメーターを使用しないでください。

直接ファイル共有からインポート、マージ、または追加するには、クラウドアクセス操作を実行するマシンを決定する必要があります。次のオプションがあります。

- ツールが既にインストールされているオンプレミス DDC のうちの 1 つ。
- ファイル共有をホストしているマシン。
- 別のマシン。

自動構成は、クラウドにアクセスするマシンにインストールする必要があります。オンプレミスの PowerShell SDK、DDC、Active Directory のいずれも使用されないため、クラウドアクセスの実行要件はエクスポート要件よりも単純です。

East DDC をクラウドにマージするには:

```
Merge-CvadAcToSite -SiteName East -SourceFolder \\share.central.
net\AutoConfig\SiteEast -CustomerInfoFileSpec \\share.central.net\
AutoConfig\CustomerInfo.yml
```

West DDC をクラウドにマージするには:

```
Merge-CvadAcToSite -SiteName West -SourceFolder \\share.central.
net\AutoConfig\SiteWest -CustomerInfoFileSpec \\share.central.net\
AutoConfig\CustomerInfo.yml
```

以下は、前の例で使用したサンプルの SitePrefixes.yml ファイルです。

```
1     East:
2       SiteRootFolder: "" # Important: leave this empty
3       AdminScopePrefix: "East_"
4       AdminRolePrefix: "East_"
5       ApplicationAdminPrefix: "East_"
6       ApplicationFolderPrefix: "" # Note that a new parent root folder
           is used instead
7       ApplicationFolderRoot: "East"
8       ApplicationGroupPrefix: "East_"
9       ApplicationUserPrefix: "East_"
10      DeliveryGroupPrefix: "East_"
11      GroupPolicyPrefix: "East_"
12      HostConnectionPrefix: "East_"
13      MachineCatalogPrefix: "East_"
14      StoreFrontPrefix: "East_"
15      TagPrefix: "East_"
16      AdminScopeSuffix: "_east"
```



```
17        AdminRoleSuffix: "_east"
18        ApplicationAdminSuffix: "_east"
19        ApplicationFolderSuffix: "_east"
20        ApplicationGroupSuffix: "_east"
21        ApplicationUserSuffix: "_east"
22        DeliveryGroupSuffix: "_east"
23        GroupPolicySuffix: "_east"
24        HostConnectionSuffix: "_east"
25        MachineCatalogSuffix: "_east"
26        StoreFrontSuffix: "_east"
27        TagSuffix: "_east"
28      West:
29        SiteRootFolder: "" # Important: leave this empty
30        AdminScopePrefix: "Western "
31        AdminRolePrefix: "Western "
32        ApplicationAdminPrefix: "Western "
33        ApplicationFolderPrefix: "" # Note that a new parent root folder
              is used instead
34        ApplicationFolderRoot: "Western"
35        ApplicationGroupPrefix: "Western "
36        ApplicationUserPrefix: "Western "
37        DeliveryGroupPrefix: "Western "
38        GroupPolicyPrefix: "Western "
39        HostConnectionPrefix: "Western "
40        MachineCatalogPrefix: "Western "
41        StoreFrontPrefix: "Western "
42        TagPrefix: "Western "
43        AdminScopeSuffix: ""
44        AdminRoleSuffix: ""
45        ApplicationAdminSuffix: ""
46        ApplicationFolderSuffix: ""
47        ApplicationGroupSuffix: ""
48        ApplicationUserSuffix: ""
49        DeliveryGroupSuffix: ""
50        GroupPolicySuffix: ""
51        HostConnectionSuffix: ""
52        MachineCatalogSuffix: ""
53        StoreFrontSuffix: ""
54        TagSuffix: ""
```

SiteMerging.yml を使用したファイル共有参照

この方式では、サイトのプレフィックスセットの`SiteRootFolder`メンバーが使用されます。この方式は、直接ファイル共有方式よりも複雑ですが、エクスポート、インポート、マージ、または追加するときに、間違ったフォルダーをターゲットにしてしまう可能性が少なくなります。

まず、SiteMerging.yml ファイルの各サイトに`SiteRootFolder`を設定します。共有の場所でこれを行う必要があります。

```
New-CvadAcSiteMergingInfo -SiteName East -SiteRootFolder \\share.
```



```
central.net\AutoConfig\SiteEast -SitePrefixesFolder \\share.central.
net\AutoConfig

New-CvadAcSiteMergingInfo -SiteName West -SiteRootFolder SiteWest -
SitePrefixesFolder \\share.central.net\AutoConfig
```

この例では、East は完全修飾フォルダー仕様であり、West は相対フォルダー仕様です。

SiteMerging.yml ファイルを使用して、エクスポートのターゲットをサイト固有のフォルダーにするには:

East DDC から:

```
mkdir \\share.central.net\AutoConfig\SiteEast

Export-CvadAcToFile -SiteName East -CustomerInfoFileSpec \\share.
central.net\AutoConfig\CustomerInfo.yml
```

West DDC から:

```
mkdir \\share.central.net\AutoConfig\SiteWest

Export-CvadAcToFile -SiteName West -CustomerInfoFileSpec \\share.
central.net\AutoConfig\CustomerInfo.yml
```

エクスポートコマンドレットは、CustomerInfo.yml フォルダーの場所を使用して SiteMerging.yml ファイルを検索します。East の場合、`SiteRootFolder`は完全修飾されています。そのまま使用します。West の場合、`SiteRootFolder`は完全修飾されていません。これを CustomerInfo.yml フォルダーの場所と組み合わせて、West の完全修飾フォルダーの場所を取得します。

East DDC をクラウドにマージするには:

```
Merge-CvadAcToSite -SiteName East -CustomerInfoFileSpec \\share.
central.net\AutoConfig\CustomerInfo.yml
```

West DDC をクラウドにマージするには:

```
Merge-CvadAcToSite -SiteName West -CustomerInfoFileSpec \\share.
central.net\AutoConfig\CustomerInfo.yml
```

以下は、前の例で使用したサンプルの SitePrefixes.yml ファイルです。

```
1       East:
2       SiteRootFolder: "\\\\share.central.net\\AutoConfig\\SiteEast"
3       AdminScopePrefix: "East_"
4       AdminRolePrefix: "East_"
5       ApplicationAdminPrefix: "East_"
6       ApplicationFolderPrefix: "" # Note that a new parent root folder
           is used instead
7       ApplicationFolderRoot: "East"
8       ApplicationGroupPrefix: "East_"
9       ApplicationUserPrefix: "East_"
10      DeliveryGroupPrefix: "East_"
11      GroupPolicyPrefix: "East_"
```



```
12        HostConnectionPrefix: "East_"
13        MachineCatalogPrefix: "East_"
14        StoreFrontPrefix: "East_"
15        TagPrefix: "East_"
16        AdminScopeSuffix: "_east"
17        AdminRoleSuffix: "_east"
18        ApplicationAdminSuffix: "_east"
19        ApplicationFolderSuffix: "_east"
20        ApplicationGroupSuffix: "_east"
21        ApplicationUserSuffix: "_east"
22        DeliveryGroupSuffix: "_east"
23        GroupPolicySuffix: "_east"
24        HostConnectionSuffix: "_east"
25        MachineCatalogSuffix: "_east"
26        StoreFrontSuffix: "_east"
27        TagSuffix: "_east"
28      West:
29        SiteRootFolder: "\\\\share.central.net\\AutoConfig\\SiteWest"
30        AdminScopePrefix: "Western "
31        AdminRolePrefix: "Western "
32        ApplicationAdminPrefix: "Western "
33        ApplicationFolderPrefix: "" # Note that a new parent root folder
              is used instead
34        ApplicationFolderRoot: "Western"
35        ApplicationGroupPrefix: "Western "
36        ApplicationUserPrefix: "Western "
37        DeliveryGroupPrefix: "Western "
38        GroupPolicyPrefix: "Western "
39        HostConnectionPrefix: "Western "
40        MachineCatalogPrefix: "Western "
41        StoreFrontPrefix: "Western "
42        TagPrefix: "Western "
43        AdminScopeSuffix: ""
44        AdminRoleSuffix: ""
45        ApplicationAdminSuffix: ""
46        ApplicationFolderSuffix: ""
47        ApplicationGroupSuffix: ""
48        ApplicationUserSuffix: ""
49        DeliveryGroupSuffix: ""
50        GroupPolicySuffix: ""
51        HostConnectionSuffix: ""
52        MachineCatalogSuffix: ""
53        StoreFrontSuffix: ""
54        TagSuffix: ""
```

中央ファイル共有方式が使用されておらず、インポート、マージ、または追加が個々の DDC から行われる場合は、クラウドに移行される各 DDC で SiteMerging.yml ファイルを作成して複製します。デフォルトの場所は*%HOMEPATH%\Documents\Citrix\AutoConfig* です。正しいサイトプレフィックスを選択するには、`-SiteName`パラメーターを指定する必要があります。

サイトのマージ

Citrix では、クラウド操作を段階的に実行し、次のクラウド操作を実行する前に各結果を完全に確認することをお勧めします。たとえば、3 つのサイトを 1 つのクラウドサイトにマージする場合:

1. 適切な`SiteName`値を使用して、初期サイトをクラウドにマージします。
2. [完全な構成] 管理インターフェイスでの結果の確認
3. 結果が正しくない場合は、問題とその原因を判別して修正してから、マージを再実行します。必要に応じて、クラウドコンポーネントを削除し、選択したコンポーネントとメンバーに対して`Remove-CvadAcFromSite`を使用して最初から開始します。結果が正しい場合は、続行します。
4. 最初のマージが正しい場合は、2 番目のサイトを単一のクラウドサイトにマージします。
5. 手順 2 と 3 を繰り返します。
6. 2 番目のマージが正しい場合は、3 番目のサイトを単一のクラウドサイトにマージします。
7. 手順 2 と 3 を繰り返します。
8. ユーザーの観点からリソースを確認し、ビューが望ましい状態になっていることを確認します。

サイトプレフィックスを使用したコンポーネントの削除

`Remove-CvadAcFromSite`コマンドレットの `-IncludeByName`パラメーターのプレフィックスを使用して、単一サイトコンポーネントを選択して削除できます。次の例では、West DDC デリバリーグループが正しくありません。West サイトのみのデリバリーグループを削除するには:

```
Remove-CvadAcFromSite -DeliveryGroups -IncludeByName “Western *”
```

すべての West コンポーネントを削除するには、次のコマンドレットを順番に実行します。

```
Remove-CvadAcFromSite -GroupPolicies -IncludeByName “Western *”
Remove-CvadAcFromSite -Applications -IncludeByName “Western *”
Remove-CvadAcFromSite - ApplicationGroups -IncludeByName “Western *”

Remove-CvadAcFromSite -DeliveryGroups -IncludeByName “Western *”
Remove-CvadAcFromSite -MachineCatalogs -IncludeByName “Western *”
Remove-CvadAcFromSite -HostConnections -IncludeByName “Western *”
Remove-CvadAcFromSite -Tags -IncludeByName “Western *”
```

East コンポーネントのグループポリシーを削除するには、次のサフィックスを使用します:

```
Remove-CvadAcFromSite -GroupPolicies -IncludeByName “*_east”
```


クラウドからクラウドへの移行

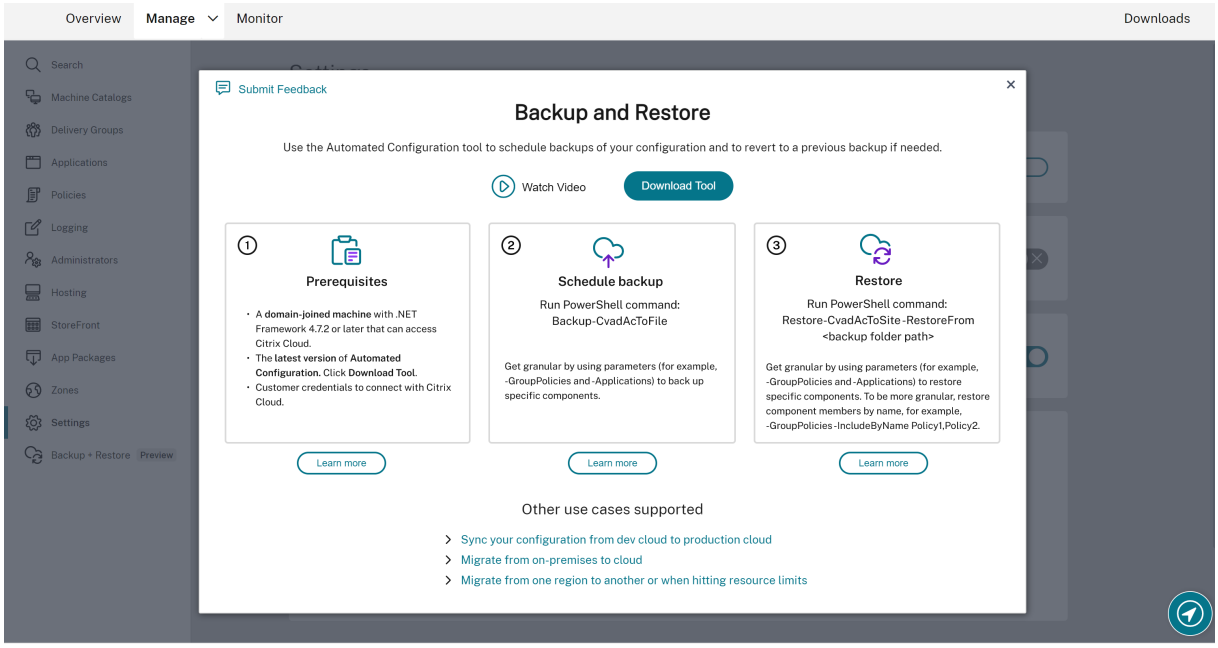
April 18, 2024

自動構成を使用すると、クラウド構成を別のクラウドサイトに移動したり、独自のクラウドサイトを復元したりすることができます。

自動構成を使用すると、多くのユースケースを解決できます:

- テストまたはステージから実稼働環境へのサイトの同期
- 構成のバックアップと復元
- リソース制限に達する
- あるリージョンから別のリージョンへの移行

自動構成についてと、それを使用して構成をクラウドからクラウドに移行する方法については、Citrix Cloud 上の［完全な構成］でバックアップと復元ノードを参照してください。



構成を移行するための前提条件

構成をバックアップおよび復元するには、次のことが必要です:

- Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）がプロビジョニングされていること。
- アクティブなリソースの場所にコネクタがインストールされていること。
- Citrix Cloud にアクセスするサイトへの接続が許可され、利用可能であること。詳しくは、「システムおよび接続要件」を参照してください。

> 注:
>
> 自動構成を使用して MCS をクラウドからバックアップすることはできません。

Citrix DaaS 構成のバックアップ

> 重要:
>
> - 顧客 ID、クライアント ID、および秘密キー情報を含む CustomerInfo.yml ファイルが必要です。顧客 ID、クライアント ID、および秘密キーの取得方法について詳しくは、「顧客 ID、クライアント ID、および秘密キーの生成」を参照してください。この情報を CustomerInfo.yml ファイルに追加する方法については、「顧客情報ファイルの作成」を参照してください。
> - バックアップコマンドを実行する場合、CustomerInfo.yml には、バックアップの取得元となるソースサイトのお客様の詳細が含まれている必要があります。
> - 復元コマンドを実行する場合、CustomerInfo.yml には、構成を復元する先のサイトのお客様の詳細が含まれている必要があります。
> - ZoneMapping.yml ファイルには、クラウド内のリソースの場所をマップする情報が含まれている必要があります。ゾーンのマッピング方法について詳しくは、「ゾーンマッピングファイルの作成」を参照してください。
> - ホスト接続がある場合、対応する情報を CvadAcSecurity.yml ファイルに入力する必要があります。

1. 自動構成をインストールします。

   > 注:
   >
   > クラウドからクラウドへの移行の場合、自動構成は、管理者が直接アクセスできるインターネットにアクセス可能なマシンにインストールできます。

2. 自動構成アイコンをダブルクリックします。PowerShell ウィンドウが表示されます。
3. 次のコマンドを実行して、バックアップを実行します。

   ```
   Backup-CvadAcToFile
   ```

コマンドレットを初めて実行すると、.yml 構成ファイルとログを含むエクスポートフォルダーが作成されます。このフォルダーは *%HOMEPATH%\Documents\Citrix\AutoConfig* にあります。

エラーや例外が発生した場合は、ログファイルの **Fixups** セクションを参照してください。

Citrix DaaS への構成の復元

1. 自動構成アイコンをダブルクリックします。PowerShell ウィンドウが表示されます。
2. 次のコマンドを実行して、復元を実行します。

   ```
   Restore-CvadAcToSite -RestoreFolder <folder path of the backup files>
   ```


最新の状態により、想定される状態を確認します。

コマンドレットを実行すると、.yml 構成ファイルとログを含むエクスポートフォルダーが作成されます。このフォルダーは *%HOMEPATH%\Documents\Citrix\AutoConfig* にあります。

エラーや例外が発生した場合は、ログファイルの **Fixups** セクションを参照してください。

バックアップと復元のプロセスは、クラウドサイト構成の意図しない変更や破損からユーザーを保護します。自動構成は変更が行われるたびにバックアップを作成しますが、このバックアップは変更前のクラウドサイト構成の状態を反映します。自分自身を保護するには、クラウドサイトの構成を定期的にバックアップし、安全な場所に保存する必要があります。望ましくない変更または破損が発生した場合は、バックアップを使用すれば、詳細または完全なサイト構成レベルで変更または破損を修正できます。

詳細な移行

> 重要:
>
> コンポーネントの移行順序について詳しくは、「コンポーネントの移行順序」を参照してください。

コンポーネント全体の復元

1 つのコンポーネントを復元するには、1 つまたは複数のコンポーネントパラメーターを選択する必要があります。

デリバリーグループ全体とマシンカタログコンポーネントを復元するには、次の例に従います:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\
AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

コンポーネントメンバーの復元

1 つまたは複数のコンポーネントメンバーを復元するには、`IncludeByName`機能を使用します。`Restore`コマンドレットは、選択した単一のコンポーネントおよび包含の一覧とともに、`RestoreFolder`パラメーターを指定して実行します。

バックアップから 2 つのグループポリシーを復元するには、次の例に従います:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\
AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
-GroupPolicies -IncludeByName Policy1,Policy2
-DeliveryGroups -MachineCatalogs
```


クラウドサイト構成全体の復元

完全なクラウドサイト構成を復元するということは、復元するすべてのコンポーネントを選択することを意味します。

クラウドサイトの構成全体を復元するには、次の例に従います:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\
AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

サイトのアクティブ化

サイトのアクティブ化により、どのサイトがアクティブであるかを制御することや、リソースを制御することができます。詳しくは、「サイトのアクティブ化」を参照してください。

自動構成ツールコマンドレット

March 31, 2024

このページには、ツールでサポートされているすべてのコマンドレットとパラメーターが一覧で示されています。

すべてのコマンドレットは、次のいずれかのタイプのパラメーターを取ります。

- 文字列
- 文字列のリスト
- ブール：`$true`または`$false`
- SwitchParameter：このパラメーターがある場合は`$true`を意味し、ない場合は`$false`を意味します。

> 注:
>
> SwitchParameter は、true か false かを選択するための推奨される方法ですが、従来の問題が原因で、このツールではブールが引き続き使用されます。

以下の表に、すべてのコマンドレットをまとめます。各コマンドレットでサポートされているパラメーターについては、個々のセクションを参照してください。

カテゴリ	コマンドレット	説明
オンプレミスからクラウドへの移行	`Export-CvadAcToFile`	オンプレミスファイルを YAML ファイルにエクスポートします。`Import-CvadAcToSite` `Merge-CvadAcToSite`

カテゴリ	コマンドレット	説明
		New-CvadAcToSite Sync-CvadAcToSite 詳細な移行 コンポーネントの場合は、上記のコマンドでパラメーターを使用します。例: MachineCatalogs、Tags。コンポーネント名の場合は、上記のコマンドでパラメーターを使用します。例: IncludeByName、ExcludeByName。
クラウドからクラウドへのコマンドレット	Backup-CvadAcToFile	クラウドサイトからすべての構成をバックアップします。
		Restore-CvadAcToSite Remove-CvadAcFromSite 詳細な移行 コンポーネントの場合は、上記のコマンドでパラメーターを使用します。例: MachineCatalogs、Tags。コンポーネント名の場合は、上記のコマンドでパラメーターを使用します。例: IncludeByName、ExcludeByName。
その他の基本的なコマンドレット	Compare-CvadAcToSite	オンプレミスの.yml ファイルとクラウド構成を比較します。
前提条件関連のコマンドレット	New-CvadAcCustomerInfoFile	顧客情報ファイルを作成します。
		Set-CvadAcCustomerInfoFile
コマンドレットのサポートとトラブルシューティング	New-CvadAcZipInfoForSupport	すべてのログファイルと.yml ファイルを 1 つの zip ファイルに圧縮して、サポートを受けるために Citrix に送信してください。 Get-CvadAcStatus

カテゴリ	コマンドレット	説明
		Test-CvadAcConnectionWithSite
		Find-CvadAcConnector
		Get-CvadAcCustomerSites
		New-CvadAcTemplateToFile
		Show-CvadAcDocument
		Find-CvadAcInFile
サイトアクティブ化コマンドレット	Set-CvadAcSiteActiveStateOnPrem	オンプレミスサイトの状態をアクティブまたは非アクティブに設定します。
		Set-CvadAcSiteActiveStateCloud
複数のオンプレミスサイトコマンドレットのマージ	New-CvadAcSiteMergingInfo	サイトマージのプレフィックス/サフィックス情報セットを作成します。
		Set-CvadAcSiteMergingInfo
		Remove-CvadAcSiteMergingInfo

パラメーターとその使用方法について詳しくは、「詳細な移行のパラメーター」を参照してください。

基本的なコマンドレット

オンプレミスからクラウドへのコマンドレット

- Export-CvadAcToFile - オンプレミスファイルを YAML ファイルにエクスポートします。

  オンプレミスセットアップから構成をエクスポートします。これは、自動構成のデフォルトのエクスポート操作です。オンプレミスサイトの構成は変更されません。エクスポートされたファイルは、一意の名前の **Export** サブフォルダーにある*%HOMEPATH%\Documents\Citrix\AutoConfig* ディレクトリに配置され

ます。*%HOMEPATH%\Documents\Citrix\AutoConfig* フォルダーには常に、最も新しくエクスポートされたオンプレミスサイトの構成があります。

パラメーター:

名前	説明	必須?	種類
コンポーネントによる移行	「コンポーネントによる移行」を参照してください		SwitchParameter
オブジェクト名によるフィルタリング	「オブジェクト名によるフィルタリング」を参照してください		文字列のリスト
`TargetFolder`	エクスポート先フォルダーを指定します。		文字列
`Locale`	エクスポート可能な、人間が判読できるテキストの言語を指定します。		文字列
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter
`AdminAddress`	エクスポートが Delivery Controller で実行されていないときの、Delivery Controller の DNS または IP アドレスを指定します。		文字列
`CheckUserAndMachines`	ユーザーとマシンが Active Directory にあるかどうかを確認します。Active Directory にないユーザーとマシンは、インポートに失敗することがあります。		`$true` または `$false`
`ZipResults`	複数の YAML ファイルを圧縮して単一の zip ファイルにバックアップします。このファイルは、バックアップされた YAML ファイルと同じフォルダーにあり、フォルダーと同じ名前になります。		SwitchParameter

戻り値:

- 「コマンドレットの戻り値」を参照してください

データをクラウドにインポートする方法は 3 つあります。特定のコマンドレットを実行すると、クラウドサイトでの操作の 3 つの組み合わせのいずれかになります:

- 追加、更新、および削除
- 追加と更新のみ
- 追加のみ

コマンドレット	追加	アップデート	削除
インポート	X	X	X
マージ	X	X	

コマンドレット	追加	アップデート	削除
変更後	X		

- `Import-CvadAcToSite` - YAML ファイルをクラウドにインポートします。作成、更新、削除の操作をサポートします。

  すべてのオンプレミスのファイルをクラウドにインポートします。このコマンドにより、クラウドの終了状態がオンプレミスの状態と同じになります。このオプションにより、クラウドに存在する変更がすべて削除されます。インポートされたサイト構成ファイルのソースは、*%HOMEPATH%\Documents\Citrix\AutoConfig* にあります。注意して使用してください。

  パラメーター:

名前	説明	必須?	種類
コンポーネントによる移行	「コンポーネントによる移行」を参照してください。		SwitchParameter
オブジェクト名によるフィルタリング	「オブジェクト名によるフィルタリング」を参照してください。		文字列のリスト
クラウドアクセスパラメーター	「クラウドアクセスパラメーター」を参照してください。		SwitchParameter
`SourceFolder`	*%HOMEPATH%\Documents\Citrix\AutoConfig* の代替ルートフォルダーを特定します。		文字列
`Locale`	エクスポート可能な、人間が判読できるテキストの言語を指定します。		文字列
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。`$false`に設定すると、ログの表示が抑制されます。		`$true` または `$false`
`Merge`	`$true`に設定すると、クラウドサイトにコンポーネントを追加するのみになります。コンポーネントは削除されません。コンポーネントを削除するには`$false`に設定します。		`$true` または `$false`
`AddOnly`	`$true`に設定すると、新しいコンポーネントのみが追加され、既存のコンポーネントは更新または削除されません。`$false`に設定すると、更新と削除が可能になります。このパラメーターが`$true`のとき、`Merge`は無視されます。		`$true` または `$false`

名前	説明	必須?	種類
MergePolicies	ポリシー設定とフィルターをマージします。マージは、インポートされるポリシーがクラウドの Desktop Delivery Controller に既に存在する場合にのみ発生します。ポリシーをマージした結果、クラウドの Desktop Delivery Controller ポリシーには、既に存在していた設定とフィルター、およびインポートされた新しい設定とフィルターが含まれます。設定とフィルターの競合が発生した場合はインポートされた値が優先されることに注意してください。		SwitchParameter
OnErrorAction	「OnErrorAction パラメーター」を参照してください。		文字列

戻り値:

- 「コマンドレットの戻り値」を参照してください

- Merge-CvadAcToSite - YAML ファイルをクラウドにインポートします。作成および更新の操作をサポートします。

  オンプレミスのファイルをクラウドにマージしますが、クラウド内またはオンプレミスサイト内のコンポーネントは削除しません。これにより、クラウドで既に行われた変更が維持されます。Citrix Cloud に同じ名前のコンポーネントが存在する場合、このコマンドによりそのコンポーネントを変更できます。これは、自動構成のデフォルトのインポート操作です。マージされたサイト構成ファイルのソースは、*%HOMEPATH%\Documents\Citrix\AutoConfig* にあります。

  パラメーター:

名前	説明	必須?	種類
コンポーネントによる移行	「コンポーネントによる移行」を参照してください。		SwitchParameter
オブジェクト名によるフィルタリング	「オブジェクト名によるフィルタリング」を参照してください。		文字列のリスト
クラウドアクセスパラメーター	「クラウドアクセスパラメーター」を参照してください。		SwitchParameter
SourceFolder	*%HOMEPATH%\Documents\Citrix\AutoConfig* の代替ルートフォルダーを特定します。		文字列
Locale	エクスポート可能な、人間が判読できるテキストの言語を指定します。		文字列
Quiet	コンソールへのログ記録を抑制します。		SwitchParameter

名前	説明	必須?	種類
DisplayLog	コマンドレットの完了時にログファイルを表示します。$falseに設定すると、ログの表示が抑制されます。		$true または $false
Merge	$trueに設定すると、クラウドサイトにコンポーネントを追加するのみになります。コンポーネントは削除されません。コンポーネントを削除するには$falseに設定します。		$true または $false
AddOnly	$trueに設定すると、新しいコンポーネントのみが追加され、既存のコンポーネントは更新または削除されません。$falseに設定すると、更新と削除が可能になります。このパラメーターが$trueのとき、Mergeは無視されます。		$true または $false
MergePolicies	ポリシー設定とフィルターをマージします。マージは、インポートされるポリシーがクラウドの Desktop Delivery Controller に既に存在する場合にのみ発生します。ポリシーをマージした結果、クラウドの Desktop Delivery Controller ポリシーには、既に存在していた設定とフィルター、およびインポートされた新しい設定とフィルターが含まれます。設定とフィルターの競合が発生した場合はインポートされた値が優先されることに注意してください。		SwitchParameter
OnErrorAction	「OnErrorAction パラメーター」を参照してください。		文字列

戻り値:

- 「コマンドレットの戻り値」を参照してください

- New-CvadAcToSite - YAML ファイルをクラウドにインポートします。作成および更新の操作をサポートします。

  オンプレミスのサイト構成をクラウドにインポートしますが、新しいコンポーネントのみを追加します。既存のクラウドサイトコンポーネントは更新も削除もされません。このコマンドは、既存のクラウドサイトコンポーネントを未変更のままにする必要がある場合に使用します。

  パラメーター:

名前	説明	必須?	種類
コンポーネントによる移行	「コンポーネントによる移行」を参照してください。		SwitchParameter

名前	説明	必須?	種類
オブジェクト名によるフィルタリング	「オブジェクト名によるフィルタリング」を参照してください。		文字列のリスト
クラウドアクセスパラメーター	「クラウドアクセスパラメーター」を参照してください。		SwitchParameter
SourceFolder	*%HOMEPATH%\Documents\Citrix\AutoConfig* の代替ルートフォルダーを特定します。		文字列
Locale	エクスポート可能な、人間が判読できるテキストの言語を指定します。		文字列
Quiet	コンソールへのログ記録を抑制します。		SwitchParameter
DisplayLog	コマンドレットの完了時にログファイルを表示します。$false に設定すると、ログの表示が抑制されます。		$true または $false
OnErrorAction	「OnErrorAction パラメーター」を参照してください。		文字列

戻り値:

- 「コマンドレットの戻り値」を参照してください

- Sync-CvadAcToSite - エクスポートとインポートを 1 つの手順で実行します。

  Sync は、エクスポートとインポートの両方を一度に実行します。SourceTargetFolderパラメーターを使用してエクスポート/インポート先フォルダーを指定します。

  パラメーター:

名前	説明	必須?	種類
コンポーネントによる移行	「コンポーネントによる移行」を参照してください		SwitchParameter
オブジェクト名によるフィルタリング	「オブジェクト名によるフィルタリング」を参照してください		文字列のリスト
クラウドアクセスパラメーター	「クラウドアクセスパラメーター」を参照してください		SwitchParameter
SourceTargetFolder	エクスポート/インポート先フォルダーを指定します。		文字列
Locale	エクスポート可能な、人間が判読できるテキストの言語を指定します。		文字列
AdminAddress	エクスポートが Delivery Controller で実行されていないときの、Delivery Controller の DNS または IP アドレスを指定します。		文字列

名前	説明	必須?	種類
Quiet	コンソールへのログ記録を抑制します。		SwitchParameter
DisplayLog	コマンドレットの完了時にログファイルを表示します。$falseに設定すると、ログの表示が抑制されます。		$true または $false
Merge	$trueに設定すると、クラウドサイトにコンポーネントを追加するのみになります。コンポーネントは削除されません。コンポーネントを削除するには$falseに設定します。		$true または $false
AddOnly	$trueに設定すると、新しいコンポーネントのみが追加され、既存のコンポーネントは更新または削除されません。$falseに設定すると、更新と削除が可能になります。このパラメーターが$trueのとき、Mergeは無視されます。		$true または $false
MergePolicies	ポリシー設定とフィルターをマージします。マージは、インポートされるポリシーがクラウドの Desktop Delivery Controller に既に存在する場合にのみ発生します。ポリシーをマージした結果、クラウドの Desktop Delivery Controller ポリシーには、既に存在していた設定とフィルター、およびインポートされた新しい設定とフィルターが含まれます。設定とフィルターの競合が発生した場合はインポートされた値が優先されることに注意してください。		SwitchParameter

戻り値:

- 「コマンドレットの戻り値」を参照してください

クラウドからクラウドへのコマンドレット

- Backup-CvadAcToFile - クラウドサイトからすべての構成をバックアップします。

  クラウド構成を.yml ファイルにエクスポートします。このバックアップをバックアップと復元のプロセスで使用して、失われたコンポーネントを復元できます。

  パラメーター:

名前	説明	必須?	種類
コンポーネントによる移行	「コンポーネントによる移行」を参照してください		SwitchParameter
クラウドアクセスパラメーター	「クラウドアクセスパラメーター」を参照してください		SwitchParameter
TargetFolder	エクスポート先フォルダーを指定します。		文字列
Locale	エクスポート可能な、人間が判読できるテキストの言語を指定します。		文字列
Quiet	コンソールへのログ記録を抑制します。		SwitchParameter
DisplayLog	コマンドレットの完了時にログファイルを表示します。$falseに設定すると、ログの表示が抑制されます。		$true または $false
ZipResults	複数の YAML ファイルを圧縮して単一の zip ファイルにバックアップします。このファイルは、バックアップされた YAML ファイルと同じフォルダーにあり、フォルダーと同じ名前になります。		SwitchParameter

戻り値:

- 「コマンドレットの戻り値」を参照してください

- Restore-CvadAcToSite - バックアップ YAML ファイルをクラウドサイトに復元します。このクラウドサイトは、ソースクラウドサイトと同じでも異なっていてもかまいません。

  クラウドサイトを以前の構成に復元します。インポートされるファイルは、-RestoreFolderパラメーターを使用して指定されたフォルダーから供給されます。このパラメーターでは、クラウドサイトに復元する.yml ファイルを含むフォルダーを指定します。これは、完全修飾フォルダー仕様である必要があります。このコマンドレットは、以前の構成に戻す場合、またはクラウドサイトのバックアップと復元を実行する場合に使用できます。このコマンドでは、クラウドサイトを追加、削除、および更新できます。

  パラメーター:

名前	説明	必須?	種類
コンポーネントによる移行	「コンポーネントによる移行」を参照してください。		SwitchParameter
オブジェクト名によるフィルタリング	「オブジェクト名によるフィルタリング」を参照してください。		文字列のリスト
クラウドアクセスパラメーター	「クラウドアクセスパラメーター」を参照してください。		SwitchParameter
RestoreFolder	クラウドサイトに復元する.yml ファイルを含むフォルダーを特定します。これは、完全修飾フォルダー仕様である必要があります。		文字列

名前	説明	必須?	種類
Locale	エクスポート可能な、人間が判読できるテキストの言語を指定します。		文字列
Quiet	コンソールへのログ記録を抑制します。		SwitchParameter
DisplayLog	コマンドレットの完了時にログファイルを表示します。$falseに設定すると、ログの表示が抑制されます。		$true または $false
Merge	$trueに設定すると、クラウドサイトにコンポーネントを追加するのみになります。コンポーネントは削除されません。コンポーネントを削除するには$falseに設定します。		$true または $false
AddOnly	$trueに設定すると、新しいコンポーネントのみが追加され、既存のコンポーネントは更新または削除されません。$falseに設定すると、更新と削除が可能になります。このパラメーターが$trueのとき、Mergeは無視されます。		$true または $false
MergePolicies	ポリシー設定とフィルターをマージします。マージは、インポートされるポリシーがクラウドの Desktop Delivery Controller に既に存在する場合にのみ発生します。ポリシーをマージした結果、クラウドの Desktop Delivery Controller ポリシーには、既に存在していた設定とフィルター、およびインポートされた新しい設定とフィルターが含まれます。設定とフィルターの競合が発生した場合はインポートされた値が優先されることに注意してください。		SwitchParameter
OnErrorAction	「OnErrorAction パラメーター」を参照してください。		文字列

戻り値:

- 「コマンドレットの戻り値」を参照してください

- Remove-CvadAcFromSite -クラウドからコンポーネントメンバーを削除します。

  サイト全体をリセットしたり、メンバーアイテムをコンポーネントから削除したりできます（たとえば、カタログリストからマシンカタログを削除するなど）。これは、IncludeByNameパラメーターと組み合わせて、特定のメンバーを選択的に削除する場合に使用できます。

  パラメーター:

名前	説明	必須?	種類
コンポーネントによる移行	「コンポーネントによる移行」を参照してください		SwitchParameter
オブジェクト名によるフィルタリング	「オブジェクト名によるフィルタリング」を参照してください		文字列のリスト
クラウドアクセスパラメーター	「クラウドアクセスパラメーター」を参照してください		SwitchParameter
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。`$false`に設定すると、ログの表示が抑制されます。		`$true` または `$false`

戻り値:

- 「コマンドレットの戻り値」を参照してください

その他の基本的なコマンドレット

- `Compare-CvadAcToSite` - オンプレミスの.yml ファイルをクラウド構成と比較し、`Import`、`Merge`、または`Restore`コマンドレットによって行われた変更のレポートを生成します。

  パラメーター:

名前	説明	必須?	種類
コンポーネントによる移行	「コンポーネントによる移行」を参照してください。		SwitchParameter
オブジェクト名によるフィルタリング	「オブジェクト名によるフィルタリング」を参照してください。		文字列のリスト
クラウドアクセスパラメーター	「クラウドアクセスパラメーター」を参照してください。		SwitchParameter
`SourceFolder`	*%HOMEPATH%\Documents\Citrix\AutoConfig* の代替ルートフォルダーを特定します。		文字列
`Locale`	エクスポート可能な、人間が判読できるテキストの言語を指定します。		文字列
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。`$false`に設定すると、ログの表示が抑制されます。		`$true` または `$false`

名前	説明	必須?	種類
Merge	$trueに設定すると、クラウドサイトにコンポーネントを追加するのみになります。コンポーネントは削除されません。コンポーネントを削除するには$falseに設定します。		$true または $false
AddOnly	$trueに設定すると、新しいコンポーネントのみが追加され、既存のコンポーネントは更新または削除されません。$falseに設定すると、更新と削除が可能になります。このパラメーターが$trueのとき、Mergeは無視されます。		$true または $false
OnErrorAction	「OnErrorAction パラメーター」を参照してください。		文字列

戻り値:

- 「コマンドレットの戻り値」を参照してください

詳細な移行のパラメーター

コンポーネントによる移行

以下のコンポーネントは、これらのコンポーネントをサポートしているコマンドレットで指定できます。コンポーネントのパラメーターが指定されていない場合、Allオプションが自動的に選択されます。エラーを回避するために、次の順序でコンポーネントを移行することをお勧めします:

- All
- Tags
- AdminRoles
- AdminScopes
- HostConnections
- MachineCatalogs
- StoreFronts
- DeliveryGroups
- ApplicationGroups
- ApplicationFolders
- Applications
- GroupPolicies
- UserZonePreference

オブジェクト名によるフィルタリング

コンポーネント名による移行　IncludeByNameおよびExcludeByNameパラメーターでは、コンポーネントメンバーを名前でコマンドレットに含めたり、コマンドレットから除外したりできます。サポートされるコマンドレットで一度に選択できるコンポーネント（たとえば、デリバリーグループなど）は 1 つのみです。コンポーネントメンバーが両方の領域にある場合、除外を使用すると、他のパラメーターはすべて上書きされ、除外されたコンポーネントとメンバーの名前を示すログ修復リストにエントリが作成されます。

IncludeByNameおよびExcludeByNameは、コンポーネントメンバー名のリストを取得します。すべての名前に 1 文字以上のワイルドカードを含めることができます。次の 2 種類のワイルドカードがサポートされています。メンバー名に特殊文字が含まれている場合は、コンポーネントメンバー名のリストを一重引用符で囲む必要があります。

- * 任意の数の文字に一致
- ? 1 文字に一致

IncludeByNameおよびExcludeByNameにより、メンバーのリストを含むファイルを取得することもできます。そこには各メンバーが明示されているか、ワイルドカードが含まれています。ファイルの各行には、メンバーを 1 つ含めることができます。先頭または末尾のスペースはメンバー名から削除されます。ファイル名は先頭に @ を付け、一重引用符で囲む必要があります（@ が再解釈されないようにするための PowerShell の要件）。メンバー名が混在するのに加え、複数のファイルをリストできます。

名前がDgSite1で始まるデリバリーグループとHome2を含むデリバリーグループすべてをマージする例を次に示します:

```
Merge-CvadAcToSite -DeliveryGroups -IncludeByName DgSite1*,*Home2*
```

デリバリーグループ名で　ByDeliveryGroupNameは、アプリケーションとアプリケーショングループのデリバリーグループ名でフィルタリングします。このパラメーターは、常にデリバリーグループの関連付けに基づいて含めるメンバーを識別する包含の一覧です。

ByDeliveryGroupNameは、デリバリーグループ名の一覧を取得します。すべての名前に 1 文字以上のワイルドカードを含めることができます。次の 2 種類のワイルドカードがサポートされています。

- * は任意の数の文字に一致
- ? は 1 文字に一致

次の例では、EastDgで始まるすべてのデリバリーグループ名を参照するすべてのアプリケーションをマージします:

```
Merge-CvadAcToSite -Applications -ByDeliveryGroupName EastDg*
```

無効を除外　ExcludeDisabledは、無効になっているすべてのアプリケーションとアプリケーショングループをインポート操作から除外します。ExcludeDisabledはデフォルトでは**false**になっています。これは、

有効の状態に関係なく、すべてのアプリケーションとアプリケーショングループがインポートされることを意味します。

マシン名で　ByMachineNameは、マシンカタログおよびデリバリーグループのマシン名でフィルタリングします。このパラメーターは常に、マシン名の関連付けに基づいて、含めるメンバーを識別する包含のリストです。

ByMachineNameは、任意の名前に 1 つまたは複数のワイルドカードを含めることができるマシン名のリストを取ります。次の 2 種類のワイルドカードがサポートされています。

- * は任意の数の文字に一致
- ? は 1 文字に一致

ByMachineNameをエクスポートまたはインポートして使用し、マシン名フィルターを使用してもマシンカタログまたはデリバリーグループにマシンがない場合、マシンカタログまたはデリバリーグループはエクスポートまたはインポートから除外されます。

> 注:
>
> インポートタイプのコマンドレットのByMachineNameを使用すると、MergeMachinesが$trueに設定されます。

マシンのマージ　MergeMachinesは、$trueに設定すると、マシンカタログまたはデリバリーグループにマシンのみを追加するようインポート操作を指示します。マシンは削除されないため、段階的な追加操作が可能です。

MergeMachinesはデフォルトで false になっており、これはマシンがマシンカタログまたはデリバリーグループの.yml ファイルに存在しない場合に削除されることを意味します。ByMachineNameが使用されているが、MergeMachinesを false に設定しても上書きできない場合に、MergeMachinesは$trueに設定されます。

前提条件関連のコマンドレット

- New-CvadAcCustomerInfoFile - 顧客情報ファイルを作成します。デフォルトでは、顧客情報ファイルは*%HOMEPATH%\Documents\Citrix\AutoConfig* にあります。

  パラメーター:

名前	説明	必須?	種類
CustomerId	顧客の ID。	x	文字列

名前	説明	必須?	種類
ClientId	Citrix Cloud で作成された、顧客のクライアント ID。このパラメーターを使用するときは、CustomerId と Secret を指定する必要があります。	条件付き	文字列
Secret	Citrix Cloud で作成される、顧客の秘密キー。このパラメーターを使用するときは、CustomerId と ClientId を指定する必要があります。	条件付き	文字列
Environment	Production 環境、ProductionGov 環境、または ProductionJP 環境。		列挙
LogFileName	ログファイルのプレフィックスを CitrixLog から別のプレフィックスに変更します。		文字列
AltRootUrl	シトリックスの指示の下でのみ使用してください。		文字列
StopOnError	最初のエラーで操作を停止します。		$true または $false
TargetFolder	*%HOMEPATH%\Documents\Citrix\AutoConfig* ではなく、ルートフォルダーとして指定したフォルダーを使用します。		文字列
Locale	ツールが実行されているシステムから取得したロケールではなく、指定したロケールを使用します。		文字列
Editor	各コマンドレットの完了時に、指定したエディターを使用してログを表示します。Notepad.exe がデフォルトのエディターです。このパラメーターには、エディターのフルパス指定を含める必要があり、エディターは唯一のパラメーターとしてログファイルの指定を受け取る必要があります。		文字列
SecurityCsvFileSpec	Citrix Identity and Access Management からダウンロードされた SecurityClient.csv ファイルを示す、完全修飾ファイルの指定です。このパラメーターを使用するときは、CustomerId を指定する必要があります。		文字列

戻り値:

- 「コマンドレットの戻り値」を参照してください

- `Set-CvadAcCustomerInfoFile` - 既存の顧客情報ファイルを更新します。コマンドレットで指定されたパラメーターのみが変更されます。CustomerInfo.yml ファイル内の指定されていないパラメーター値はすべて変更されません。

  パラメーター:

名前	説明	必須?	種類
`CustomerId`	顧客の ID。		文字列
`ClientId`	Citrix Cloud で作成された、顧客のクライアント ID。		文字列
`Secret`	Citrix Cloud で作成される、顧客の秘密キー。		文字列
`Environment`	Production 環境、ProductionGov 環境、または ProductionJP 環境。		列挙
`LogFileName`	ログファイルのプレフィックスを CitrixLog から別のプレフィックスに変更します。		文字列
`StopOnError`	最初のエラーで操作を停止します。		`$true` または `$false`
`TargetFolder`	*%HOMEPATH%\Documents\Citrix\AutoConfig* ではなく、ルートフォルダーとして指定したフォルダーを使用します。		文字列
`Locale`	ツールが実行されているシステムから取得したロケールではなく、指定したロケールを使用します。		文字列
`Editor`	各コマンドレットの完了時に、指定したエディターを使用してログを表示します。Notepad.exe がデフォルトのエディターです。このパラメーターには、エディターのフルパス指定を含める必要があり、エディターは唯一のパラメーターとしてログファイルの指定を受け取る必要があります。		文字列
`SecurityCsvFileSpec`	Citrix Identity and Access Management からダウンロードされた SecurityClient.csv ファイルを示す、完全修飾ファイルの指定です。このパラメーターを使用するときは、CustomerId を指定する必要があります。		文字列

  戻り値:

  - 「コマンドレットの戻り値」を参照してください

前提条件関連のパラメーター

クラウドアクセスパラメーターに加えて、次のパラメーターを前提条件関連のコマンドレットで使用できます:

- `Environment` - Production 環境または ProductionGov 環境。
- `LogFileName` - ログファイルのプレフィックスを CitrixLog から別のプレフィックスに変更します。
- `StopOnError` - 最初のエラーで操作を停止します。
- `AlternateRootFolder` - *%HOMEPATH%\Documents\Citrix\AutoConfig* ではなく、ルートフォルダーとして指定したフォルダーを使用します。
- `Locale` - ツールが実行されているシステムから取得したロケールではなく、指定したロケールを使用します。
- `Editor` - 各コマンドレットの完了時に、指定したエディターを使用してログを表示します。Notepad.exe がデフォルトのエディターです。このパラメーターには、エディターのフルパス指定を含める必要があり、エディターは唯一のパラメーターとしてログファイルの指定を受け取る必要があります。

コマンドレットのサポートとトラブルシューティング

- `New-CvadAcZipInfoForSupport` - すべてのログファイルと.yml ファイルを 1 つの zip ファイルに圧縮します。Citrix のサポートを受ける際はこのファイルを送信してください。顧客の機密情報（CustomerInfo.yml および CvadAcSecurity.yml）はこの zip に含まれません。Icon.yml ファイルもそのサイズが理由で除外されます。zip ファイルは、*%HOMEPATH%\Documents\Citrix\AutoConfig* に置かれ、日付とタイムスタンプに基づいて *CvadAcSupport_yyyy_mm_dd_hh_mm_ss.zip* という名前になります。この zip ファイルはバックアップとしても機能します。

  パラメーター:

名前	説明	必須?	種類
`TargetFolder`	zip ファイルを作成して保存するためのターゲットフォルダーを指定します。		文字列
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter

  戻り値:

  - コマンドプロンプトに zip ファイルの zip ファイル名前とその場所が表示されます。

- `Get-CvadAcStatus` - 接続をテストし、すべての前提条件が満たされていることを確認するために使用します。バージョン番号、クラウドとの接続、コネクタのステータスなど、ツールに関する情報を返します。

  パラメーター:

名前	説明	必須?	種類
クラウドアクセスパラメーター	「クラウドアクセスパラメーター」を参照してください		SwitchParameter
SiteId	接続するサイトを特定します。		文字列
AdminAddress	管理者のアクセスレベルを確認するために使用される、オンプレミスの Delivery Controller の DNS または IP アドレスです。これは、ツールが Delivery Controller で実行されていない場合に必要です。		文字列

戻り値:

- 各アイテムの結果を表示します。

- Test-CvadAcConnectionWithSite -クラウドサイトとの接続をテストし、通信接続が機能していることを確認します。このコマンドレットは、クラウドアクセスパラメーターまたは CustomerInfo.yml ファイルを使用して、顧客の接続情報を指定します。

  パラメーター:

名前	説明	必須?	種類
クラウドアクセスパラメーター	「クラウドアクセスパラメーター」を参照してください		SwitchParameter
Quiet	コンソールへのログ記録を抑制します。		SwitchParameter

戻り値:

- テスト結果はコマンドラインに表示されます。

- Find-CvadAcConnector - 既存のコネクタを検索し、コネクタの実行状態を判別します。このコマンドレットは、CustomerInfo.yml ファイルまたは顧客 ID パラメーターの情報を使用して、顧客のコネクタを検索します。

  パラメーター:

名前	説明	必須?	種類
CustomerInfoFileSpec	デフォルトの場所と名前を上書きするための、顧客情報ファイルを示すファイルの指定です。CustomerIdパラメーターが指定されている場合、このパラメーターは無視されます。		文字列

名前	説明	必須?	種類
CustomerId	顧客の ID。このパラメーターは、CustomerInfo.yml ファイル内の同じ値を上書きします。		文字列

戻り値:

- 結果はコマンドラインに表示されます。

- Get-CvadAcCustomerSites - すべての顧客サイトのリストを返します。このコマンドレットは、クラウドアクセスパラメーターまたは CustomerInfo.yml ファイルを使用して、顧客の接続情報を指定します。

  パラメーター:

  - 「クラウドアクセスパラメーター」を参照してください

  戻り値:

  - 見つかった顧客サイト ID のリストを表示します。

- New-CvadAcTemplateToFile –選択されたコンポーネントのテンプレートファイルを作成し、インポートファイルを手動で作成できるようにします。

  パラメーター:

名前	説明	必須?	種類
コンポーネントによる移行	「コンポーネントによる移行」を参照してください		SwitchParameter
TargetFolder	エクスポート先フォルダーを指定します。		文字列

戻り値:

- 「コマンドレットの戻り値」を参照してください

- Show-CvadAcDocument - このドキュメントをデフォルトのブラウザーで表示します。

  パラメーター:

  - ありません。

  戻り値:

  - この Web ページをデフォルトの Web ブラウザーに表示します。

- `Find-CvadAcInFile` - ファイル内検索でコンポーネントの YAML ファイルを検索し、ワイルドカードを含む可能性がある名前に一致するメンバーを見つけます。結果は、見つかったメンバーのレポートです。ファイル内検索では、一度に 1 つのコンポーネントしか検索できません。ファイル内検索では、現在のフォルダー内とすべてのサブフォルダー内で、すべての YAML ファイルが検索されます。`FindSourceFolder`を使用して、検索するファイルの数を制限します。

  パラメーター:

名前	説明	必須?	種類
コンポーネントによる移行	「コンポーネントによる移行」を参照してください。注: `-All`値は無効です。		SwitchParameter
`IncludeByName`	サイトのアクティブ状態をアクティブに設定するときに含めるデリバリーグループの名前を指定するリスト。名前では「*」および「?」ワイルドカードがサポートされています。		文字列のリスト
`Unique`	見つかった一意のメンバーのみを報告します。		SwitchParameter
`IncludeYaml`	メンバー固有の YAML を含めます。		SwitchParameter
`FindSourceFolder`	フォルダー検索ではここで検索が開始されます。		文字列
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。`$false`に設定すると、ログの表示が抑制されます。		SwitchParameter
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter

  戻り値:

  - 指定されたコンポーネントについて、見つかったメンバーを含むレポートを作成します。

サイトアクティブ化コマンドレット

サイトのアクティブ化とこれらのコマンドレットの使用方法について詳しくは、「サイトのアクティブ化」を参照してください。

- `Set-CvadAcSiteActiveStateOnPrem` - オンプレミスサイトの状態をアクティブまたは非アクティブに設定します。

  パラメーター:

名前	説明	必須?	種類
クラウドアクセスパラメーター	「クラウドアクセスパラメーター」を参照してください		SwitchParameter
SiteActive	存在する場合、オンプレミスサイトをアクティブに設定し、すべてのデリバリーグループからメンテナンスモードを解除します。このパラメーターが存在しない場合、すべてのデリバリーグループにメンテナンスモードが設定されます。		SwitchParameter
IncludeByName	サイトのアクティブ状態をアクティブに設定するときに含めるデリバリーグループの名前を指定するリスト。名前では「*」および「?」ワイルドカードがサポートされています。		文字列のリスト
ExcludeByName	サイトのアクティブ状態をアクティブに設定するときに除外するデリバリーグループの名前を指定するリスト。名前では「*」および「?」ワイルドカードがサポートされています。		文字列のリスト
Quiet	コンソールへのログ記録を抑制します。		SwitchParameter
DisplayLog	コマンドレットの完了時にログファイルを表示します。$falseに設定すると、ログの表示が抑制されます。		$true or $false

戻り値:

- 「コマンドレットの戻り値」を参照してください

- Set-CvadAcSiteActiveStateCloud - クラウドサイトの状態をアクティブまたは非アクティブに設定します。

  パラメーター:

名前	説明	必須?	種類
クラウドアクセスパラメーター	「クラウドアクセスパラメーター」を参照してください		SwitchParameter
SiteActive	存在する場合、クラウドサイトをアクティブに設定し、すべてのデリバリーグループからメンテナンスモードを解除します。このパラメーターが存在しない場合、すべてのデリバリーグループにメンテナンスモードが設定されます。		SwitchParameter

名前	説明	必須?	種類
IncludeByName	サイトのアクティブ状態をアクティブに設定するときに含めるデリバリーグループの名前を指定するリスト。名前では「*」および「?」ワイルドカードがサポートされています。		文字列のリスト
ExcludeByName	サイトのアクティブ状態をアクティブに設定するときに除外するデリバリーグループの名前を指定するリスト。名前では「*」および「?」ワイルドカードがサポートされています。		文字列のリスト
Quiet	コンソールへのログ記録を抑制します。		SwitchParameter
DisplayLog	コマンドレットの完了時にログファイルを表示します。$falseに設定すると、ログの表示が抑制されます。		$true or $false

戻り値:

- 「コマンドレットの戻り値」を参照してください

複数のオンプレミスサイトコマンドレットのマージ

サイトのマージとこれらのコマンドレットの使用方法について詳しくは、「複数のサイトを 1 つのサイトにマージする」を参照してください。

- New-CvadAcSiteMergingInfo - サイトマージのプレフィックス/サフィックス情報セットを作成します。始めからすべてのプレフィックスまたはサフィックス情報を把握している必要はありません。プレフィックスやサフィックスは、Set-CvadAcSiteMergingInfoを使用するか、SiteMerging.yml ファイルを手動で編集することで更新できます。
  パラメーター:

名前	説明	必須?	種類
SiteName	特定サイトのプレフィックス/サフィックスのセットを識別するために使用する名前。実際のサイトの名前と一致させることはできますが、一致させる必要はありません。	x	文字列
サイトマージパラメーター	「サイトマージパラメーター」を参照してください		SwitchParameter

名前	説明	必須?	種類
Quiet	コンソールへのログ記録を抑制します。		SwitchParameter

戻り値:

- なし

- Set-CvadAcSiteMergingInfo - サイトマージの既存のプレフィックス/サフィックス情報セットを更新します。

  パラメーター:

名前	説明	必須?	種類
SiteName	特定サイトのプレフィックス/サフィックスのセットを識別するために使用する名前。実際のサイトの名前と一致させることはできますが、一致させる必要はありません。	x	文字列
サイトマージパラメーター	「サイトマージパラメーター」を参照してください		SwitchParameter
Quiet	コンソールへのログ記録を抑制します。		SwitchParameter

  戻り値:

  - なし

- Remove-CvadAcSiteMergingInfo - サイトマージの既存のプレフィックス/サフィックス情報セットを削除します。

  パラメーター:

  - SiteName -サイトのプレフィックスとサフィックスのセットを特定します。これは文字列であり、必須です。

  戻り値:

  - なし

サイトマージパラメーター

次のパラメーターは、サイトマージコマンドレットを実行するときに使用できます。リストされているすべてのパラメーターは文字列です。

- SiteName - 特定サイトのプレフィックス/サフィックスのセットを識別するために使用する名前。実際のサイトの名前と一致させることはできますが、一致させる必要はありません。SiteName は必須パラメーターです。
- AdminScopedPrefix - 管理者スコープに適用するプレフィックス。
- ApplicationPrefix - アプリケーションに適用するプレフィックス。
- ApplicationFolderPrefix - アプリケーションフォルダーに適用するプレフィックス。ApplicationFolderPrefixはApplicationFolderRootと組み合わせることができます。
- ApplicationFolderRoot - アプリケーションフォルダーへの新しいルートフォルダー。これにより、追加のフォルダー階層が作成されます。ApplicationFolderRootはApplicationFolderPrefixと組み合わせることができます。
- ApplicationGroupPrefix - アプリケーショングループのプレフィックス。
- ApplicationUserPrefix - ユーザーに表示されるアプリケーション名に適用するプレフィックス。
- ApplicationAdminPrefix - 管理者に表示されるアプリケーション名に適用するプレフィックス。
- DeliveryGroupPrefix - デリバリーグループに適用するプレフィックス。
- GroupPolicyPrefix - ポリシー名に適用するプレフィックス。
- HostConnectionPrefix - ホスト接続に適用するプレフィックス。
- MachineCatalogPrefix - マシンカタログに適用するプレフィックス。
- StoreFrontPrefix - StoreFront 名に適用するプレフィックス。
- TagPrefix - タグに適用するプレフィックス。
- AdminScopedSuffix - 管理者スコープに適用するサフィックス。
- ApplicationSuffix - アプリケーションに適用するサフィックス。
- ApplicationFolderSuffix - アプリケーションフォルダーに適用するサフィックス。ApplicationFolderSuffixはApplicationFolderRootと組み合わせることができます。
- ApplicationGroupSuffix - アプリケーショングループのサフィックス。
- ApplicationUserSuffix - ユーザーに表示されるアプリケーション名に適用するサフィックス。
- ApplicationAdminSuffix - 管理者に表示されるアプリケーション名に適用するサフィックス。
- DeliveryGroupSuffix - デリバリーグループに適用するサフィックス。
- GroupPolicySuffix - ポリシー名に適用するサフィックス。
- HostConnectionSuffix - ホスト接続に適用するサフィックス。
- MachineCatalogSuffix - マシンカタログに適用するサフィックス。
- StoreFrontSuffix - StoreFront 名に適用するサフィックス。
- TagSuffix - タグに適用するサフィックス。
- SiteRootFolder - エクスポートおよびインポートに使用する完全修飾フォルダー名。これは、ローカルフォルダーまたはファイル共有に適用できます。

一般的なパラメーター

クラウドアクセスパラメーター

クラウドにアクセスするすべてのコマンドレットで、以下の追加パラメーターがサポートされています。

> 注:
>
> CustomerId、ClientId、および Secret は、CustomerInfo.yml ファイル内に設定するか、次のパラメーターを使用してコマンドレットで指定できます。両方で指定されている場合は、コマンドレットパラメーターが優先されます。

- `CustomerId` –Rest API で使用される顧客 ID で、すべての Rest API へのアクセスで必要となります。顧客 ID は Citrix Cloud に保存されています。
- `ClientId` –Citrix Cloud の「ID およびアクセス管理」Web サイトで作成されたクライアント ID です。これは、すべての Rest API の認証で必要なベアラートークンを取得するのに必要です。
- `Secret` –Citrix Cloud の「ID およびアクセス管理」Web サイトで作成された秘密キーです。これは、すべての Rest API の認証で必要なベアラートークンを取得するのに必要です。
- `CustomerInfoFileSpec` –デフォルトの場所と名前を上書きするための、顧客情報ファイルを示すファイルの指定です。

移行モードパラメーター

クラウドサイト構成を変更するコマンドレット（`Import`、`Restore`、`Merge`、`New`、および`Sync`）では、柔軟性を高める以下の追加パラメーターがサポートされています。

- `CheckMode` –インポート操作を実行しますが、変更は行いません。インポート実行前に、想定されるすべての変更が報告されます。このコマンドを使用して、インポートを実行前にテストできます。
- `BackupFirst` –クラウド構成を変更する前に、クラウドコンテンツを.yml ファイルにバックアップします。これはデフォルトで有効になっています。
- `Confirm` –true の場合、クラウドサイト構成を変更してよいか確認するプロンプトが表示されます`Remove`コマンドレットでは、その破壊的な性質のためにプロンプトが表示されます。自動スクリプト内で実行する場合など、プロンプトが不要な場合には false に設定します。`Confirm`のデフォルトは true です。
- `SecurityFileFolder` –これは、認証制御下にあるローカルフォルダーまたはネットワーク共有フォルダーを指している可能性がある、CustomerInfo.yml ファイルを含む完全修飾フォルダーです。このツールは資格情報の入力を求めません。ツールを実行する前に、制御されたリソースへのアクセス権限を取得する必要があります。
- `SiteName` - インポート時に使用するサイトマージのプレフィックスとサフィックスのセットを指定します。
- `SiteActive` - インポートされたサイトがアクティブか非アクティブかを指定します。デフォルトではこのパラメーターは`$false`に設定されており、これはインポートされたサイトが非アクティブであることを意味します。

ログ表示パラメーター

Export、Import、Sync、Restore、Backup、Compare、およびRemoveコマンドレットは、操作が完了するとログファイルを表示します。-DisplayLogパラメーターを$falseに設定することにより、表示を抑制できます。デフォルトでは、Notepad.exe を使用してログファイルが表示されます。CustomerInfo.yml ファイルに別のエディターを指定することもできます。

```
Editor: C:\Program Files\Notepad++\notepad++.exe
```

コマンドレットの戻り値

ActionResult

すべてのコマンドレットで以下の値が戻されます。

```
public class ActionResult
{

    public bool                             Overall_Success;
    public Dictionary<string, string>   Individual_Success;
    public object                           CustomResult;
 }
```

Overall_Successは、選択したすべてのコンポーネントでのコマンドレットの全体的な成功を示す 1 つのブール値を返します：true は成功を示し、false は失敗を示します。

Individual_Successは、主要コンポーネントごとに 1 つまたは 3 つの値を返します。コンポーネントの結果は、Success、Failure、Skipped のいずれかです。Skipped は、コマンドレットがコンポーネントを実行対象に選択しなかったことを示します。

CustomResultはコマンドレットに固有です。

CustomResult

Import、Merge、Restore、Sync、Compare、Compare File、およびRemoveは、EvaluationResultData の単一インスタンスに以下のカスタム結果情報を返します。

> 注:
>
> コマンドレットExportおよびTemplateはカスタム結果を返しません。

```
public class EvaluationResultData
{

    public Dictionary<string, Dictionary<string,
       ActionResultValues >> EvaluationResults;
```



```
5                       public int                  Added;
6                       public int                  Updated;
7                       public int                  Deleted;
8                       public int                  NoChange;
9                       public int                  TotalChanged;
10                      public EvaluationResults     OverallResult;
11                      public string               CloudBackupFolder;
12                      public string               SourceBackupFolder;
13                   }
14
15                  Where:
16                  public enum ActionResultValues
17                 {
18
19                      Add,
20                      Update,
21                      Delete,
22                      Identical,
23                      DoNothing
24                   }
25
26                  public enum EvaluationResults
27                  {
28
29                      Success,
30                      Failure,
31                      Skipped
32                   }
```

EvaluationResultsは、選択したコンポーネントごとに 1 つのエントリを持つリストを表示します。キーはコンポーネント名で、値は各コンポーネントメンバーのリストとそのコンポーネントメンバーに実行される操作です。操作はActionResultValuesの値のいずれかにできます。

Added、Updated、Deleted、およびNoChangeでは、追加、更新、削除、または操作が実行されなかったコンポーネントメンバーの合計数がその順序で示されます。

TotalChangedは、Added、Updated、Deletedの合計です。

OverallResultは、コマンドレットの結果を示す 1 つのブール値です。true はすべてのコンポーネントの全体的な成功を示し、false は 1 つ以上のコンポーネントの処理が失敗したことを示します。

CloudBackupFolderは、コマンドレットがクラウド変更操作を実行する前の、クラウドサイト構成バックアップのフルパスのファイル指定です。

SourceBackupFolderは、コマンドレットの完了後に作成されたソースファイルバックアップのフルパスのファイル指定です。デフォルトでは、これらのファイルは *%HOMEPATH%\Documents\Citrix\AutoConfig* にあります。

PowerShell ヘルプ

コマンドレットごとに、PowerShell ヘルプが提供されます。各コマンドレットのすべてのパラメーターが、コマンドレットの簡単な説明とともに文書化されています。コマンドレットのヘルプにアクセスするには、コマンドレットの前に「`Get-Help`」と入力します。

```
Get-Help Import-CvadAcToSite
```

自動構成のトラブルシューティングと追加情報

March 31, 2024

> 重要:
>
> 自動構成および対応するソリューションで発生することが多いエラーメッセージについては、ナレッジセンターの記事 CTX277730でトラブルシューティングに関する *FAQ* を参照してください。

自動構成ツールのエラー

自動構成ツールの操作で、エラーが発生することがあります。この問題が発生した場合、マシンカタログ、デリバリーグループ、グループポリシーなどのコンポーネントを処理するときにエラーが発生する可能性があります。`OnErrorAction`および継続パラメーターを使用すると、処理中にエラーをキャッチし、それを解決し、中断した場所を確認できます。

デフォルトの`OnErrorAction`値は`StopCompEnd`です。エラーが発生すると、ツールは現在のコンポーネントの処理を終了します。追加のコンポーネントは処理されず、エラーはダウンストリームの依存コンポーネントには適用されません。エラーを解決したら、継続パラメーターを適用してコマンドレットを再実行できます。

OnErrorAction パラメーター

移行コマンドの`OnErrorAction`パラメーター値を定義することで、コンポーネントの処理時に検出されたエラーに対するツールの応答方法を制御できます。

次の表に、パラメーター値とその説明を示します:

値	説明
`Continue`	可能な限り多くのコンポーネントの処理を試みます。
`Pause`	処理の最後に一時停止し、続行または停止を求めるメッセージを表示します。

値	説明
StopCompEnd	可能な限り多くのコンポーネントの処理を試みます。コンポーネント終了後に停止します。（デフォルト）
StopImmediately	エラーが見つかると処理を停止します。

移行コマンドレット

OnErrorActionパラメーターは、次の移行コマンドに適用できます:

- Compare-CvadAcToSite
- Import-CvadAcToSite
- Merge-CvadAcToSite
- New-CvadAcToSite
- Restore-CvadAcToSite

例: `Merge-CvadAcToSite -OnErrorAction StopImmediately`

再開パラメーター

これらのパラメーターにより、エラーが原因で操作が一時停止または停止した後にツールを再開する方法を定義します。

再開パラメーターを、以下のいずれかのOnErrorActionパラメーター値を含む移行コマンドレットに適用できます:

- Pause
- StopCompEnd
- StopImmediately

次の表に、パラメーター値とその説明を示します:

値	説明
-AllRemaining	開始コンポーネントが必要です。処理は開始コンポーネントから開始され、残りのコンポーネントがすべて処理されます。複数のコンポーネントが処理されます。
-Resume	CurrentComponent.txtのコンポーネントを開始点として使用します。残りはすべて true に設定されます。複数のコンポーネントが処理されます。

値	説明
-Repeat	CurrentComponent.txtのコンポーネントを開始点として使用します。残りはすべて false に設定されます。処理されるコンポーネントは 1 つだけです。

最後に処理されるコンポーネントは、AutoConfig フォルダーのCurrentComponent.txtファイルに保存されます。このファイルを編集することはお勧めしません。
-Resumeまたは-Repeatを指定していてCurrentComponent.txtが存在しないまたは無効な場合、処理が停止し、コンポーネントを選択するように求められます。

CustomerInfo.yml ファイルでの **OnErrorAction** の設定

CustomerInfo.ymlファイル内のOnErrorAction値を設定することもできます。次のコマンドレットを使用して値を設定します:

- 新しいファイルの場合: `New-CvadAcCustomerInfoFile -OnErrorAction Continue | Pause | StopCompEnd | StopImmediately`
- 既存のファイルの場合: `Set-CvadAcCustomerInfoFile -OnErrorAction Continue | Pause | StopCompEnd | StopImmediately`

ログ

コマンドレットを実行すると、ログファイルが作成され、メインの履歴ログファイルにエントリが作成されます。操作ログファイルはすべて、バックアップフォルダーに配置されます。ログファイル名はすべてCitrixLogで始まり、自動構成操作とコマンドレットの実行日およびタイムスタンプを示します。ログは自動削除されません。

メインの履歴ログは、*%HOMEPATH%\Documents\Citrix\AutoConfig*の **History.Log** という名前のファイルに格納されています。各コマンドレットを実行すると、実行の日付、操作、結果、バックアップ、およびログファイルの場所を含むメインのログエントリが作成されます。

New-CvadAcZipInfoForSupportコマンドレットを使用してログを収集し、サポートを受けるためにシトリックスに送信することもできます。このコマンドレットでは、すべてのログファイルと.yml ファイルが 1 つの zip ファイルに圧縮されます。顧客の機密情報（CustomerInfo.yml および CvadAcSecurity.yml）はこの zip に含まれません。Icon.yml ファイルもそのサイズが理由で除外されます。zip ファイルは、*%HOMEPATH%\Documents\Citrix\AutoConfig* に置かれ、日付とタイムスタンプに基づいて *CvadAcSupport_yyyy_mm_dd_hh_mm_ss.zip* という名前になります。この zip ファイルはバックアップとしても機能します。

各ログファイルには以下が含まれます:

- 操作名と、チェックモードが有効かどうか
- 開始日時と終了日時
- 各コンポーネントの操作と成功/失敗の通知に関する複数のエントリ
- 作成されたオブジェクト数を含む、実行された操作アクションの概要
- 推奨される修正プログラム（ある場合）
- バックアップフォルダーの場所（ある場合）
- メインのログの場所
- 継続時間

診断ファイル

診断ファイルは、問題の判別と解決に役立ちます。操作の実行時に、以下のファイルが作成されます。これらは、*%HOMEPATH%\Documents\Citrix\AutoConfig* の下の操作固有のサブフォルダーに格納されています。問題解決サポートに情報を提供する際には、これらのファイルを含めます。

エクスポート

`PoshSdk_yyyy_mm_dd_hh_mm_ss.ps1`

このファイルには、サイト構成をファイルにエクスポートするために行われた、Broker PowerShell SDK のすべての呼び出しがカウントされます。

インポート、マージ、復元、同期、バックアップ、比較

`Transaction_yyyy_mm_dd_hh_mm_ss.txt`

このファイルには、各 Rest API 呼び出しとそれに関連する情報が記載されています。

`RestApiContent_yyyy_mm_dd_hh_mm_ss.txt`

このファイルには`Add`、`Update`、および`Delete`の Rest API コンテンツがすべて含まれます。

依存関係に起因する問題

依存関係がないため、インポートとマージが失敗することがあります。一般的な問題には次のようなものがあります:

1. グループポリシーにデリバリーグループフィルターがありません。通常の原因は、インポートされていないデリバリーグループです。
2. アプリケーションがインポートまたはマージに失敗します。通常の原因は、インポートされていないデリバリーグループまたはアプリケーショングループがないことです。

3. アプリケーショングループに RestrictTo タグがありません。通常の原因は、インポートされていないタグです。
4. ホスト接続が失敗します。通常の原因は、CvadAcSecurity.yml ファイルにセキュリティ情報がないことです。
5. マシンカタログが失敗します。通常の原因は、インポートされなかったホスト接続です。
6. マシンカタログおよびデリバリーグループにないマシン。通常の原因は、Active Directory で見つからなかったマシンです。
7. デリバリーグループにないユーザー。通常の原因は、Active Directory で見つからなかったユーザーです。

推奨事項

- 一度に複数の自動構成インスタンスを実行しないでください。複数インスタンスを同時に実行すると、クラウドサイトで想定外の結果となる場合があります。これが発生したら、自動構成の 1 つのインスタンスを再実行して、サイトを想定した状態にします。
- 自動構成の実行中は、［管理］タブの［完全な構成］での作業またはデータ変更は行わないでください。
- マージ、インポート、または復元の結果を［完全な構成］で常に視覚的に検証して、クラウドサイトが想定どおりとなるようにしてください。

フォルダー

デフォルトのフォルダールートの場所

自動構成ツールのすべての操作は、ルートフォルダーまたはその内部のサブフォルダーで行われます。ルートフォルダーは *%HOMEPATH%\Documents\Citrix\AutoConfig* にあります。

エクスポート

エクスポートされたファイルはすべて、使いやすさとエクスポートの履歴を提供する 2 つのフォルダーに配置されます。エクスポートは常にルートフォルダーに配置されます。コピーは、エクスポート日時の **Export** という名前のサブフォルダーに配置されます。

ルートフォルダーには常に、エクスポートされた最新のオンプレミスサイト構成が含まれています。各 **Export** サブフォルダーには、示された日時に行われたエクスポートが含まれ、エクスポートの履歴が保持されます。**Export** サブフォルダーを使用して、クラウドサイトを構成できます。自動構成では、既存のエクスポートサブフォルダーは削除または変更されません。

Import/Merge/Sync/Compare

`Import`、`Merge`、および`Compare`操作の操作元は常に、ルートフォルダーにあるファイルです。各操作によって、ルートフォルダー内のファイルがコピーされるサブフォルダーが作成され、クラウドサイトのソースファイル変

更履歴が提供されます。

復元

Restore操作では、既存のサブフォルダーを使用してクラウドサイトを構成します。ソースフォルダーは、必須の-RestoreFolderパラメーターで指定されます。他のコマンドとは異なり、Restore操作では既存のサブフォルダーが使用されるため、新しいサブフォルダーは作成されません。復元フォルダーはルートフォルダーでも構いませんが、-RestoreFolderパラメーターで指定する必要があります。

バックアップ

自動構成は、クラウドサイト構成を初期化、更新、およびバックアップします。長期間使用すると、クラウドサイトのさまざまな設定が変更される可能性があります。自動構成では、長期間の使用を容易にし、変更履歴を保持するために、保存スキームを使用して変更履歴を保存し、以前の状態を復元する方法を提供しています。

クラウドサイト構成のバックアップは常に、バックアップのデータと時刻の **Backup** という名前のサブフォルダーに作成されます。自動構成では、既存のエクスポートサブフォルダーは削除または変更されません。

バックアップを使用して、特定のコンポーネントや構成全体を復元できます。デリバリーグループおよびマシンカタログコンポーネント全体を復元するには、次のコマンドレットを使用します:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\
AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss -DeliveryGroups -MachineCatalogs
```

> 注:
>
> 上記のコマンドレットのバックアップファイル情報は、独自のバックアップに基づいています。

クラウドサイト構成全体を復元するには、次のコマンドレットを使用します:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\
AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

> 注:
>
> 上記のコマンドレットのバックアップファイル情報は、独自のバックアップに基づいています。

デフォルトのルートフォルダーの変更

Export、Import、Merge、Sync、およびCompareの各操作では、 -AlternateFolderパラメーターを使用してデフォルトのルートフォルダーを変更できます。操作ごとのサブフォルダーの作成と管理は、前述の手順と同じです。

サブフォルダーにコピーされるファイル

拡張子が「.yml」のファイルはすべて、以下を除き、操作サブフォルダーにコピーされます:

- CustomerInfo.yml
- ZoneMapping.yml
- CvadAcSecurity.yml

自動フェイルセーフクラウドサイトバックアップ

構成を変更する操作を行う前に、現在のクラウドサイト構成のバックアップが作成されます。これには`Import`、`Merge`、`Sync`、および`Restore`パラメーターが含まれます。バックアップは常に、操作サブフォルダーの下のサブフォルダーに格納されます。

`Restore`の場合、バックアップフォルダーは、`-RestoreFolder`パラメーターで指定されたフォルダーのサブフォルダーです。

自動化

自動構成ツールのコマンドレットは、コマンドレット完了時のプロンプトとログ結果の表示を抑制することにより、管理者の介入なしに自動スクリプトで実行できます。また、CustomerInfo.yml ファイルを使用することにより、パラメーターを設定して同じ処理を行うこともできます。

プロンプトの表示を抑制するには、クラウド変更コマンドレットに次のパラメーターを追加します。

```
-Confirm $false
```

コマンドレット完了時のログの表示を抑制するには、コマンドレットに以下のパラメーターを追加します。

```
-DisplayLog $false
```

次のパラメーターをコマンドレットに追加して、PowerShell コマンドウィンドウへのログ記録を抑制します。

```
-Quiet
```

別の方法として、CustomerInfo.yml ファイルに以下のパラメーターを挿入することもできます。

```
Confirm: False
DisplayLog: False
```

Delivery Controller 以外の **PC** からのエクスポート

自動構成ツールは、複数の Citrix PowerShell SDK を使用してオンプレミスサイト構成をファイルにエクスポートします。これらの SDK は Delivery Controller に自動的にインストールされるため、追加の操作を行わずに Delivery Controller 上でツールを実行できます。Delivery Controller 以外のマシンで実行する場合は、ツールに

必要な一連の Citrix PowerShell SDK をインストールする必要があります。この一連の SDK は Citrix Studio の一部で、Citrix Virtual Apps and Desktops インストールメディアからインストールできます。

> 注:
>
> 自動構成は、Cloud Connector では実行できません。

Citrix Cloud Government と **Japan** コントロールプレーンへの移行

Citrix Cloud Government 環境と Japan コントロールプレーン環境では、さまざまなアクセスポイントを使用して、アクセストークンの認証と割り当てを行います。この独自の要件は、クラウドにアクセスするすべての自動構成ツールに適用されます。これらの環境で自動構成を使用するには、次の手順を実行します。

1. *%HOMEPATH%\Documents\Citrix\AutoConfig* フォルダーにある CustomerInfo.yml を編集します。
2. 接続する環境に応じて、次のいずれかの行を CustomerInfo.yml に追加します（または、既に存在する場合は変更します）。

   ```
   Environment: 'ProductionGov'
   ```

   または

   ```
   Environment: 'ProductionJP'
   ```

自動構成をこれらの環境で使用できるようになりました。

Citrix Cloud のデータ収集

Citrix Cloud が収集する情報については、「Citrix Cloud サービスの顧客コンテンツとログの処理」を参照してください。

そのほかの情報の入手先

ディスカッション フォーラム

自動構成に関する Citrix Discussions のフォーラムにアクセスしてください。

ビデオ

YouTube で、「Citrix Virtual Apps and Desktops の自動構成ツールの内容」をご覧ください。

トレーニング

Cloud Learning Center には、この記事で説明するタスクなど、サービス展開を構築する手順についてのビデオガイドがあります。Citrix Virtual Apps and Desktops の Citrix Cloud への移行のラーニングパスを参照してください。

Image Portability Service の使用によるリソースの場所間でのワークロードの移行

May 17, 2024

Image Portability Service は、すべてのプラットフォームにおいてイメージを簡単に管理できるようにします。Citrix Virtual Apps and Desktops の REST API を使用して、Citrix Virtual Apps and Desktops サイト内のリソースの管理を自動化できます。

Image Portability ワークフローは、Citrix Cloud を使用して 2 つのリソースの場所間でイメージを移行しようとすると、開始されます。イメージをエクスポートした後、Image Portability Service は、ターゲットのハイパーバイザーまたはパブリッククラウドで実行するためのイメージの転送、準備を支援をします。最終的に、Citrix Provisioning または Machine Creation Services は、ターゲット環境でイメージをプロビジョニングします。

コンポーネント

Image Portability Service のコンポーネントは以下のようなものがあります:

- Citrix Cloud サービス
- Citrix Credential Wallet
- Citrix Connector Appliance
- Compositing Engine VM
- PowerShell のサンプルスクリプト

Citrix Cloud サービス

Citrix Cloud Services API は、Image Portability Service と通信する REST API サービスです。REST API サービスを使用すると、Image Portability ジョブを作成および監視できます。たとえば、API 呼び出しを行って、ディスクのエクスポートなどの Image Portability ジョブを開始してから、呼び出しを行ってそのジョブのステータスを取得します。

Citrix Credential Wallet

Citrix Credentials Wallet サービスは、システムの資格情報を安全に管理し、Image Portability Service がアセットと通信できるようにします。たとえば、vSphere から SMB 共有にディスクをエクスポートする場合、Image

Portability Service は、ディスクの書き込みのために、SMB 共有への接続を開くための資格情報を必要とします。資格情報が Credential Wallet に保存されている場合、Image Portability Service はそれらの資格情報を取得して使用できます。

このサービスにより、資格情報を完全に管理することができます。Cloud Services API はアクセスポイントとして機能し、資格情報を作成、更新、および削除する機能を提供します。

Compositing Engine

Compositing Engine は、Image Portability Service の主力製品です。Compositing Engine（CE）は、Image Portability のエクスポートまたは準備ジョブの開始時に作成される単一の VM です。この VM は、ジョブが実行されているのと同じ環境で作成されます。たとえば、vSphere からディスクをエクスポートする場合、CE は vSphere サーバー上に作成されます。同様に、Azure、AWS、または Google Cloud で準備ジョブを実行すると、CE はそれぞれ Azure、AWS、または Google Cloud で作成されます。CE はディスクを自身にマウントしてから、必要な操作をディスクに対して実行します。準備またはエクスポートジョブが完了すると、CE VM とそのすべてのコンポーネントが削除されます。

Connector Appliance

IPS リソースを管理するためにプロバイダーソフトウェアを実行している Connector Appliance は、ご使用の環境（オンプレミスと、Azure、AWS、または Google Cloud サブスクリプション）で実行され、個々のジョブのコントローラーとして機能します。クラウドサービスからジョブの指示を受け取り、Compositing Engine VM を作成および管理します。Connector Appliance VM は、クラウドサービスとご使用の環境との間の安全な単一の通信ポイントとして機能します。各リソースの場所（オンプレミス、Azure、AWS、または Google Cloud）に 1 つまたは複数の Connector Appliance を展開します。Connector Appliance は、セキュリティのために各リソースの場所に展開されます。Connector Appliance と Compositing Engine を同じ場所に配置することで、すべてのコンポーネントと通信がリソースの場所内に保持されるため、展開のセキュリティ体制が大幅に向上します。

PowerShell モジュール

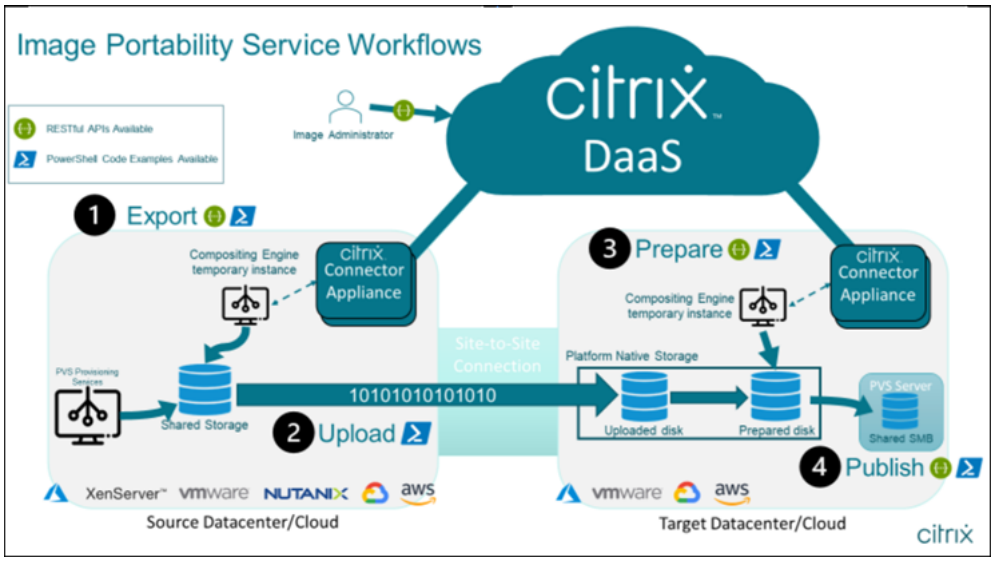
スクリプト内で使用する PowerShell モジュールのコレクションを提供しており、これを開始時に使用することで独自のカスタムの自動処理を開発できます。提供されているモジュールはそのままでサポートされますが、ご使用の環境で必要に応じて変更できます。

PowerShell 自動化では、提供された構成パラメーターを使用して Citrix Cloud API サービスへの REST 呼び出しを構成し、ジョブを開始してから、ジョブの進行に合わせて定期的に更新できます。

独自の自動化ソリューションを開発する場合は、好みのプログラミング言語を使用してクラウドサービスを直接呼び出すことができます。Image Portability Service のREST エンドポイントと PowerShell モジュールの構成と使用について詳しくは、API ポータルを参照してください。

ワークフロー

Image Portability Service は、マルチフェーズワークフローを使用して、パブリッククラウドサブスクリプションのオンプレミスのリソースの場所から、マスターカタログイメージを準備します。このサービスは、オンプレミスのハイパーバイザープラットフォームからイメージをエクスポートし、パブリッククラウドサブスクリプションにアップロードします（提供されている PowerShell アップロードユーティリティを使用すると、これを自動化できます）。次に、Image Portability は、パブリッククラウドプラットフォームと互換性があるようにイメージを準備します。最終的に、イメージが公開され、クラウドのリソースの場所に新しいマシンカタログとして展開できるようになります。



これらの高レベルのワークフローは、イメージのソースおよびターゲットのプロビジョニング構成（Machine Creation または Citrix Provisioning）に基づいています。選択したワークフローによって、必要な Image Portability のジョブステップが決まります。

次の表を参照して、サポートされている各 IPS ワークフローに必要なジョブを把握してください。

ワークフロー（ソースからターゲット）	エクスポート	アップロード	準備	公開
MCS から MCS へ	Y	Y	Y	N
PVS から MCS へ *	N	Y	Y	N
PVS から PVS へ	-	Y	Y	Y
MCS から PVS へ	Y	Y	Y	Y

* 元のイメージは Citrix Provisioning vDisk で、ソースのプラットフォームハイパーバイザーから直接をエクスポートする必要がないと仮定しています。

要件

Image Portability を開始するには、次の要件を満たしている必要があります。

Citrix マシンカタログイメージ

IPS では、以下のいずれかの検証済み構成のイメージを使用する必要があります:

- Windows Server 2016、2019、2022H2
- Windows 10 または 11
- Machine Creation Services または Citrix Provisioning を使用してプロビジョニングされている
- Citrix Virtual Delivery Agent:
  - 1912 および 2203 LTSR の最新の 2 つの累積更新プログラム
  - 最も新しい 2 つの最新リリース
- Azure でコンソールアクセスが有効になっているリモートデスクトップサービス

Image Portability Service は、以下のハイパーバイザーとクラウドプラットフォームをサポートします:

ソースプラットフォーム:

- VMware vSphere 7.0 および 8.0
- XenServer 8/Citrix Hypervisor 8.2
- Nutanix AHV（Prism Element のみ）
- Microsoft Azure
- Google Cloud Platform

ターゲットプラットフォーム:

- VMware vSphere 8.0
- XenServer 8/Citrix Hypervisor 8.2
- Nutanix AHV（Prism Element のみ）
- Microsoft Azure
- AWS
- Google Cloud Platform

Citrix Connector Appliance

Image Portability を使用する予定の各リソースの場所に、Citrix Connector Appliance をインストールして構成する必要があります。たとえば、Image Portability を使用して、イメージを vSphere から Azure、AWS、Google Cloud に移行する場合は、少なくとも 4 つの Citrix Connector Appliance が必要です:

詳しい手順については、「Connector Appliance の展開」を参照してください。

SMB（Windows）ファイル共有

エクスポートジョブの出力を保存するには、Windows **SMB** ファイル共有が必要です。この共有は、Image Portability Service を使用しているリソースの場所に作成された Compositing Engine VM にアクセスできる必要があります。共有に使用できる空き容量が、イメージのファイルシステムの構成済みサイズの 2 倍以上であることを確認してください。

PowerShell スクリプトを実行するためのマシン

PowerShell スクリプトを実行するマシンには、以下のものがあります:

- PowerShell バージョン 5.1。
- SMB ファイル共有への高速ネットワーク接続。ファイル共有をホストしているのと同じマシンにすることができます。
- Image Portability 機能を使用する予定のパブリッククラウドプラットフォームへの高速ネットワーク接続。たとえば、Azure、AWS、または Google Cloud です。

  PowerShell ギャラリーから Image Portability モジュールをダウンロードして構成する方法について詳しくは、「PowerShell 用のマシンの準備」セクションを参照してください。

Citrix Cloud 顧客 ID

Citrix DaaS のサブスクリプションが有効であることを確認してください。

続行するには、Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）にアクセスする必要があります。アクセス権がない場合は、Citrix の担当者にお問い合わせください。

Image Portability で使用する API クライアントを作成および構成する手順については、「API Getting Started」のドキュメントを参照してください。

Azure に必要な権限と構成

Image Portability Service が Azure リソースで動作するためには、特定の Azure 機能へのアクセス権限を Image Portability Service が使用する Azure サービスプリンシパルに付与する必要があります。詳細な一覧については、「Microsoft Azure に必要な権限」を参照してください。

関連付けられたリソースのサービスプリンシパルに、**Contributor**（投稿者）の役割を割り当てることができます。または、必要な最小限のアクセス権限を割り当てるには、必要な権限を使用してカスタム役割を作成し、それを適切なリソースにスコープ設定したサービスプリンシパルに割り当てます。

「Azure サービスプリンシパルのセキュリティロールの構成」と「カスタム役割の作成」については、Azure のドキュメントを参照してください。

Google Cloud に必要な権限と構成

Image Portability Service が Google Cloud プロジェクトで動作するためには、特定の機能へのアクセス権限を Image Portability Service が使用する Google Cloud サービスプリンシパルに付与する必要があります。

詳細な一覧については、「Google Cloud に必要な権限」を参照してください。

これらの権限は、次の役割を使用して割り当てることができます：

- Cloud Build エディター
- コンピューティング管理者
- ストレージ管理者
- サービスアカウントユーザー

サービスアカウントの権限の構成について詳しくは、Google Cloud のドキュメントを参照してください。

Amazon Web Services に必要な権限と構成

Amazon Web Services（AWS）アカウントで Image Portability Service のワークフローを実行するには、それぞれの Identity and Access Management（IAM）ID で適切な権限が必要です。

詳細な一覧については、「AWS に必要な権限」を参照してください。

Image Portability Service のセットアップ

Image Portability Service をセットアップするには、以下を実行します：

- Connector Appliance を展開する
- PowerShell 用のマシンを準備する
- Credential Wallet に資格情報を追加する

Connector Appliance を展開する

Image Portability では、Image Portability ジョブを作成するために Citrix Connector Appliance が必要です。Connector Appliance は、オンプレミスおよびパブリッククラウド環境との安全な通信をサポートします。Connector Appliance は、Image Portability Service と通信して、ジョブのステータスと全体的なサービス稼働状況を報告します。

ご使用の環境で Connector Appliance を展開および構成するには、「クラウドサービス用の Connector Appliance」の手順に従います。

展開を計画するときは、アプライアンスに必要なハードウェア構成とネットワークポートアクセスに注意してください。

アプライアンスを展開して登録すると、Image Portability を有効にするために必要なコンポーネントが自動的にインストールされます。

PowerShell 用のマシンを準備する

Image Portability の起動と実行をサポートするために、サービスを使用し、カスタマイズおよび使用できる PowerShell モジュールを作成しました。

次のセクションでは、PowerShell スクリプトを実行するためのマシンを準備する方法について説明します。これらのスクリプトはほんの一例です。ニーズに合わせて変更または拡張してください。

> 注:
>
> 初期インストール後、**Update-Module** を使用して PowerShell モジュールを更新します。

PowerShell の要件　PowerShell スクリプトを使用するには、次のものが必要です:

- Image Portability ジョブを駆動する PowerShell スクリプトを実行するための Windows マシン。このマシンでは、以下が必要です:
  - PowerShell の最新バージョン。
  - オンプレミスの SMB ファイル共有への 10Gbs 以上のネットワーク接続、およびパブリッククラウド（Azure、AWS、または Google Cloud など）への高速接続がある。
  - ファイル共有をホストしているのと同じマシンにすることが可能である。
  - 最新の Microsoft パッチを適用した Windows10、Windows Server 2019、または Windows Server 2022 を実行しているマシンである。
  - Microsoft PowerShell ギャラリーに接続して、必要な PowerShell ライブラリをダウンロードできる。

Windows のバージョンによっては、TLS 1.0 または 1.1 のサポートを無効にする必要がある場合があります。詳しくは、Microsoft PowerShell ギャラリー TLS サポートのドキュメントを参照してください。

デフォルトでは、PowerShell はプロキシサーバーを介して自動的に認証されません。Microsoft およびプロキシベンダーのベストプラクティスに従い、PowerShell セッションがプロキシサーバーを使用するように構成されていることを確認してください。

サービス終了したバージョンまたは古いバージョンの PowerShellGet に関連する PowerShell スクリプトを実行する際にエラーが表示される場合は、次のように最新バージョンをインストールする必要があります:

```
Install-Module -Name PowerShellGet -Force -Scope CurrentUser -
    AllowClobber
<!--NeedCopy-->
```

ライブラリとモジュールのインストール　Image Portability Service は、Microsoft PowerShell ギャラリーのライブラリを使用して、移植操作を促進します。

> 重要:
>
> 初期インストール後、**Update-Module** を使用して新しいバージョンをインストールします。

1. 次の PowerShell コマンドを実行して、最新のモジュールをダウンロードします:

   ```
   Install-Module -Name "Citrix.Workloads.Portability","Citrix.Image.
       Uploader" -Scope CurrentUser
   <!--NeedCopy-->
   ```

   - PATH 環境変数を変更するには:

     Y と **Enter** キーを押して受け入れます。

   - NuGet プロバイダーをインストールするには:

     Y と **Enter** キーを押して受け入れます。

   - 信頼できないリポジトリについて通知された場合:

     A（すべてはい）と **Enter** キーを押して続行します。

2. 次のコマンドを実行して、必要なすべてのモジュールがダウンロードされたことを確認します:

   ```
   Get-InstalledModule -Name Citrix.*
   <!--NeedCopy-->
   ```

   このコマンドは、次のような出力を返します:

名前	リポジトリ	説明
Citrix.Image.Uploader	PSGallery	VHD（x）を Azure Storage Account、AWS、または GCP にアップロードし、VHD（x）に関する情報を取得するコマンド
Citrix.Workloads.Portability	PSGallery	Citrix Image Portability Service のイメージジョブ用のスタンドアロンコマンドレット

モジュールの最新バージョンへの更新　次のコマンドを実行して、スクリプトを最新バージョンに更新します。

```
Update-Module -Name "Citrix.Workloads.Portability","Citrix.Image.
    Uploader" -Force
<!--NeedCopy-->
```

Citrix Virtual Apps and Desktops Remote PowerShell SDK のインストール　Image Portability Service では、Citrix Cloud 内で移植ジョブを作成および管理するために、Citrix Virtual Apps and Desktops Remote PowerShell SDK が必要です。

Remote PowerShell SDKをダウンロードして、マシンにインストールします。

プラットフォーム固有のサードパーティコンポーネントのインストール　Image Portability Service の PowerShell モジュールは、サードパーティの依存関係をインストールしません。したがって、対象とするプラットフォームのみにインストールを制限できます。次のいずれかのプラットフォームを使用している場合は、プラットフォームの依存関係のインストールに関する手順に従ってください：

VMware　VMware 環境と通信する Image Portability ジョブを作成している場合は、次のコマンドを実行して、必要な VMware PowerShell モジュールをインストールします。

```
Install-Module -Name VMWare.PowerCLI -Scope CurrentUser -AllowClobber -
    Force -SkipPublisherCheck
<!--NeedCopy-->
```

Amazon Web Services　AWS で Image Portability ジョブを作成する場合は、AWS コマンドラインインターフェイスをダウンロードしてインストールしてから、次のコマンドを実行して、必要な AWS PowerShell モジュールをインストールします：

```
Install-Module -Name AWS.Tools.Installer
Install-AWSToolsModule AWS.Tools.EC2,AWS.Tools.S3
<!--NeedCopy-->
```


Azure　Azure で Image Portability ジョブを作成する場合は、Azure コマンドラインユーティリティをダウンロードしてインストールしてから、次のコマンドを実行して、必要な Azure PowerShell モジュールをインストールします:

```
Install-Module -Name Az.Accounts -Scope CurrentUser -AllowClobber -
    Force
Install-Module -Name Az.Compute -Scope CurrentUser -AllowClobber -Force
<!--NeedCopy-->
```

Google Cloud　Google Cloud で Image Portability ジョブを作成している場合は、Google Cloud SDKをダウンロードしてマシンにインストールします。

スクリプトとモジュールのアンイストール　次のコマンドを実行して、Image Portability ソフトウェアで使用されているモジュールをアンインストールします。

> 注:
>
> IPS モジュールをアンインストールするときに、サードパーティのスクリプトとコンポーネントが自動的に削除されることはありません。

モジュールをアンインストールするには:

```
Get-InstalledModule -Name "Citrix.Workloads.Portability","Citrix.Images
    .Uploader" | Uninstall-Module
<!--NeedCopy-->
```

Credential Wallet に資格情報を追加する

エンドツーエンドの自動化のシナリオでは、Citrix Cloud、パブリッククラウド、およびオンプレミスリソースと対話なしに認証できるように、Image Portability Service を構成できます。また、Image Portability Service は、API がオンプレミスおよびパブリッククラウドのリソースで直接認証しているときは、常に Citrix Credential Wallet に保存されている資格情報を使用します。エクスポート、準備、および公開のジョブを実行するには、このセクションで説明しているように資格情報を設定する必要があります。

ジョブを実行する場合、Image Portability Service には、制御可能なリソースへのアクセスが必要です。たとえば、Image Portability Service が vSphere サーバーから SMB 共有にディスクをエクスポートする場合、Image Portability Service には両方のシステムへのログインアクセスが必要です。このアカウント情報を保護するために、Image Portability Service は Citrix Credential Wallet サービスを使用します。このサービスは、資格情報をユーザー定義の名前を付けて Wallet に保存します。ジョブを実行する場合は、使用する資格情報の名前を指定します。また、これらの資格情報はいつでもウォレットから更新または削除できます。

多くの場合、以下のプラットフォームの資格情報が保存されます:

- Microsoft Azure

- AWS
- Google Cloud
- SMB 共有
- VMware vSphere
- Nutanix AHV
- XenServer

資格情報を管理する方法については、「Image Portability Service APIs」と、Developer API ポータルの「Credentials Management」を参照してください。

Image Portability Service の使用

オンプレミスのリソースの場所のイメージをパブリッククラウドサブスクリプションに配置するには、Citrix Cloud 内に Image Portability ジョブを作成する必要があります。スクリプトまたはプログラム内でサービスに直接 API 呼び出しを行うジョブを作成するか、API 呼び出しを自動化するために開発したサンプルの PowerShell モジュールを使用して、ジョブを作成できます。REST API と PowerShell モジュールを使用して IPS ジョブを作成する方法については、Image Portability Service の Developer API ポータル を参照してください。

Citrix Provisioning を使用してマシンカタログを公開する

Image Portability Service（IPS）は、Azure、AWS、Google Cloud、Nutanix, vSphere、および XenServer で Machine Creation Services（MCS）とともに、または Azure、Google Cloud、vSphere、および XenServer で Citrix Provisioning（PVS）とともに使用されます。このガイドで説明されている PowerShell および REST ソリューションをご使用のプラットフォームツール、プラットフォームの API、または Citrix DaaS SDK と組み合わせることで、準備されたオンプレミスイメージに基づいてマシンカタログを作成する、シームレスで自動化されたエンドツーエンドのワークフローを作成できます。選択したクラウドプラットフォームによっては、IPS 準備ジョブの完了とカタログの作成または PVS ターゲットへの割り当ての間に、中間ステップが必要な場合があります。

AWS　AWS での IPS 準備ジョブは、ボリュームを生成します。Machine Creation Services では、カタログの作成中に Amazon マシンイメージ（AMI）が必要です。移行したイメージから AMI を生成するには、最初に生成したボリュームからイメージのスナップショットを作成し、次にそのスナップショットに基づいて AMI を作成する必要があります。これは、AWS コマンドラインインターフェイス（CLI）で実行できます：

```
> aws ec2 create-snapshot --volume-id <VolumeId>
> aws ec2 register-image --name <AmiName> --architecture 'x86_64' --
    root-device-name '/dev/sda1 --boot-mode uefi --ena-support --
    virtualization-type 'hvm' --block-device-mappings 'DeviceName=/dev/
    sda1,Ebs={
 SnapshotId=<SnapshotID> }
 '
<!--NeedCopy-->
```


<VolumeId>は、IPS 準備ジョブからの出力です。生成された AMI は、MCS マスターイメージとして使用できます。

ワークフローのこの部分を自動化するための PowerShell サンプルスクリプトは、New-IpsAwsImage.ps1という名前のスクリプトとして Citrix.Workloads.Portability モジュールで提供されます。

Azure　Azure では、IPS は MCS マスターイメージとして直接使用できる管理対象ディスクを生成します。生成されたイメージを PVS ターゲットに割り当てるために、IPS は、管理対象ディスクを PVS ストアの VHD(x) ファイルにコピーするための「publish」オペレーションを提供します。

Google Cloud　Google Cloud 上の IPS 準備ジョブはディスクを生成します。MCS には Google Cloud インスタンステンプレートが必要です。ディスクから MCS のインスタンステンプレートを作成するプロセスについては、「マスター仮想マシンインスタンスと永続ディスクを準備する」で詳しく説明しています。

Google Cloud 上の PVS ターゲットでは、IPS は、管理対象ディスクを PVS ストアの VHD(x) ファイルにコピーするための「publish」オペレーションを提供します。

VDA 構成を自動化する

オンプレミスで作成された Citrix 管理のイメージを準備する場合、イメージ内で VDA を再構成して、イメージが準備されているターゲット環境をサポートできます。Image Portability Service は、ワークフローの準備フェーズで、臨機応変に VDA 構成の変更を適用できます。次の構成パラメーターは、移行されたイメージ内で VDA がどのように動作するかを定義します：**InstallMisa**、**XdReconfigure**、および **InstallMcsio**。IPS ジョブの作成時にこれらのパラメーターを定義するには、「Image Portability Service の PowerShell の例」を参照してください。

構成

- **InstallMisa** を**true**に構成し、MCS でイメージをプロビジョニングするために必要な VDA コンポーネントを Image Portability Service がインストールできるようにします。
- **InstallMisa** を**true**に、または **InstallMcsio** を**true**に構成するためには、**CloudProvisioningType** をMcsに構成する必要があります。
- **InstallPvs** を、イメージが展開されている PVS サーバーのバージョンに設定します。**InstallPvs** が設定されている場合、Image Portability Service（IPS）は、準備ジョブ中に、指定されたバージョンの PVS ターゲットデバイスソフトウェアをイメージに自動インストールします。IPS は、最新の 2 つの長期サービスリリース（LTSR）と最新リリース（CR）に対して、最新の 2 つのビルド（ベース リリースまたは累積更新プログラム）をサポートします。

InstallMisa と **InstallMcsio** の両方について、次の点に注意してください：

- これらの機能をサポートしているのは、VDA の最近の LTSR および CR リリースのみです。

- インストールされた VDA に必要なコンポーネントが既に存在する場合、パラメーターが構成されていても、変更は行われません。
- サポートされているバージョンの VDA の場合、必要な VDA コンポーネントが存在しない場合でも、Image Portability は必要なコンポーネントの適切なバージョンをインストールします。
- サポートされていないバージョンの VDA の場合、再構成は失敗し、必要な VDA コンポーネントが存在しない場合はメッセージがログに記録されます。VDA の再構成が完了しなくても、準備ジョブは完了します。

XdReconfigure には、次のいずれかの値が必要です：`controllers`または`site_guid`。それぞれの値を使用した構成パラメーターの例を以下に示します：

controllers を使用：

```
XdReconfigure = @(
    [pscustomobject]@{

        ParameterName = 'controllers'
        ParameterValue = 'comma-separated-list-of-your-cloud-connectors
           -fqdns'
     }

)
<!--NeedCopy-->
```

ここで、**ParameterValue** は、VDA を指定する新しい DDC（Desktop Delivery Controller）の FQDN（完全修飾ドメイン名）のリストです。複数の DDC をコンマ区切り形式で指定できます。

site_guid を使用：

```
XdReconfigure = @(
    [pscustomobject]@{

        ParameterName = 'site_guid'
        ParameterValue = 'active-directory-site-guid'
     }

)
<!--NeedCopy-->
```

XdReconfigure は、**/reconfigure** インストールスイッチを使用すると、VDA コマンドラインインストーラー実行時に、サポートされる値を受け入れます（例：**XenDesktopVdaSetup.exe /reconfigure**）。サポートされる値には、**wem_agent_port**、**wem_cached_data_sync_port**、**wem_cloud_connectors**、または **wem_server** などがあります。VDA 再構成コマンドラインオプションの完全なリストについては、Citrix DaaS VDA のドキュメントを参照してください。

InstallMcsio を`true`に構成すると、イメージに自動的に MCSIO がインストールされます。イメージへの MCSIO の自動インストールを無効にするには、**InstallMcsio** を`false`に構成します。

> 注:
>
> コマンドの実行中に-DryRunを使用して、構成と Connector Appliance のネットワーク設定を検証できます。

リファレンス

このセクションでは、ニーズに基づいたテクニカルリファレンス情報を詳しく説明します。

Image Portability Service に必要な権限

このセクションでは、サポートされているオンプレミスおよびクラウドプラットフォームのそれぞれで、Image Portability Service に必要とされる権限について詳しく説明します。

Connector Appliance に必要な権限　Image Portability Service でイメージを準備するには、Connector Appliance が次の URL にアクセスできる必要があります:

```
api-ap-s.cloud.com
api-eu.cloud.com
api-us.cloud.com
credentialwallet.citrixworkspaceapi.net
graph.microsoft.com
login.microsoftonline.com
management.azure.com
*.blob.storage.azure.net
<!--NeedCopy-->
```

VMware vCenter に必要な権限　VMware 環境で IPS エクスポートディスクジョブを実行するには、次の vCenter 権限が必要です。これらの権限は、vCenter 管理パネルの ［アクセス制御］セクションの ［役割］にあります。

```
- Cryptographic operations
    - Direct Access

- Datastore
    - Allocate space
    - Browse datastore
    - Low level file operations
    - Remove file

- Folder
    - Create folder
    - Delete folder

- Network
```



```
    -  Assign network

-  Resource
    -  Assign virtual machine to resource pool

-  Virtual machine
    -  Change Configuration
        -  Add existing disk
        -  Add new disk
        -  Remove disk

    -  Edit Inventory
        -  Create from existing
        -  Create new
        -  Remove

    -  Interaction
        -  Power off
        -  Power on
<!--NeedCopy-->
```

Microsoft Azure に必要な権限　Image Portability は、Azure サービスアカウントに次の権限があることを必要とします。

Compositing Engine で使用するリソースグループが指定されている場合（REST 要求の *resourceGroup* プロパティで、または Citrix.Workloads.Portability PowerShell コマンドを使用する場合は*-AzureVmResourceGroup* パラメーターで）、リソースグループのスコープで次の権限が必要です。

```
Microsoft.Compute/disks/beginGetAccess/action
Microsoft.Compute/disks/endGetAccess/action
Microsoft.Compute/disks/delete
Microsoft.Compute/disks/read
Microsoft.Compute/disks/write
Microsoft.Compute/virtualMachines/delete
Microsoft.Compute/virtualMachines/powerOff/action
Microsoft.Compute/virtualMachines/read
Microsoft.Compute/virtualMachines/write
Microsoft.Network/networkInterfaces/delete
Microsoft.Network/networkInterfaces/join/action
Microsoft.Network/networkInterfaces/read
Microsoft.Network/networkInterfaces/write
Microsoft.Network/networkSecurityGroups/delete
Microsoft.Network/networkSecurityGroups/join/action
Microsoft.Network/networkSecurityGroups/read
Microsoft.Network/networkSecurityGroups/write
Microsoft.Resources/deployments/operationStatuses/read
Microsoft.Resources/deployments/read
Microsoft.Resources/deployments/write
Microsoft.Resources/subscriptions/resourcegroups/read
<!--NeedCopy-->
```


Compositing Engine で使用するリソースグループが指定されていない場合、サブスクリプションのスコープで次の権限が必要です。

```
Microsoft.Compute/disks/beginGetAccess/action
Microsoft.Compute/disks/endGetAccess/action
Microsoft.Compute/disks/read
Microsoft.Compute/disks/write
Microsoft.Compute/virtualMachines/powerOff/action
Microsoft.Compute/virtualMachines/read
Microsoft.Compute/virtualMachines/write
Microsoft.Network/networkInterfaces/join/action
Microsoft.Network/networkInterfaces/read
Microsoft.Network/networkInterfaces/write
Microsoft.Network/networkSecurityGroups/join/action
Microsoft.Network/networkSecurityGroups/read
Microsoft.Network/networkSecurityGroups/write
Microsoft.Resources/deployments/operationStatuses/read
Microsoft.Resources/deployments/read
Microsoft.Resources/deployments/write
Microsoft.Resources/subscriptions/resourceGroups/delete
Microsoft.Resources/subscriptions/resourceGroups/write
Microsoft.Authorization/roleAssignments/read
Microsoft.Authorization/roleDefinitions/read
<!--NeedCopy-->
```

次の権限は、指定されたターゲットリソースグループ（つまり、REST 要求の *targetDiskResourceGroupName* プロパティ、または PowerShell を使用する場合は*-TargetResourceGroup* パラメーターで指定されたリソースグループ）のスコープで必要です。

```
Microsoft.Compute/disks/beginGetAccess/action
Microsoft.Compute/disks/delete
Microsoft.Compute/disks/read
Microsoft.Compute/disks/write
Microsoft.Compute/snapshots/delete
Microsoft.Compute/snapshots/read
Microsoft.Compute/snapshots/write
<!--NeedCopy-->
```

次の権限は、指定された仮想ネットワークリソースグループ（つまり、REST 要求の *virtualNetworkResourceGroupName* プロパティ、または PowerShell を使用する場合は*-AzureVirtualNetworkResourceGroupName* パラメーターで指定されたリソースグループ）のスコープで必要です。

```
Microsoft.Network/virtualNetworks/read
Microsoft.Network/virtualNetworks/subnets/join/action
<!--NeedCopy-->
```

> 重要:
>
> 「prepare」および「prepareAndPublish」ジョブの`ceVmSku`オプションは、作成されたターゲットディスクに適した Azure VM の種類を制御します。出力イメージからプロビジョニングする予定の仮想マシンと同じ

> ファミリーおよびバージョンの ceVmSku を選択する必要があります。`Standard_D2S_v3`のデフォルト値は、すべての Dv3 ファミリーマシンでの実行に適しています。一時ディスクを含まないマシン SKU の指定はサポートされていません。

Google Cloud に必要な権限　Image Portability は、Google Cloud サービスアカウントに次の権限があることを必要とします:

```
cloudbuild.builds.create
cloudbuild.builds.get
cloudbuild.builds.list
compute.disks.create
compute.disks.delete
compute.disks.get
compute.disks.list
compute.disks.setLabels
compute.disks.use
compute.globalOperations.get
compute.images.create
compute.images.delete
compute.images.get
compute.images.list
compute.images.setLabels
compute.images.useReadOnly
compute.instances.create
compute.instances.delete
compute.instances.get
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setServiceAccount
compute.instances.setTags
compute.instances.stop
compute.instances.updateDisplayDevice
compute.networks.get
compute.subnetworks.use
compute.subnetworks.useExternalIp
compute.zoneOperations.get
compute.zones.list
iam.serviceAccounts.actAs
iam.serviceAccounts.get
iam.serviceAccounts.list
resourcemanager.projects.get
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
<!--NeedCopy-->
```


AWS に必要な権限　Image Portability では、次の構成の JSON ポリシードキュメントを Identity and Access Management (IAM) ユーザーにアタッチする必要があります:

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ebs:StartSnapshot",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ec2:CreateTags",
                "ec2:CreateImage",
                "ec2:DeleteSnapshot",
                "ec2:DeleteVolume",
                "ec2:DeregisterImage",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:RebootInstances",
                "ec2:RegisterImage",
                "ec2:RunInstances",
                "ec2:TerminateInstances",
            ],
            "Effect": "Allow",
            "Resource": "*"
         }

    ]
 }

<!--NeedCopy-->
```

> 注:
>
> 必要に応じて、リソースのスコープをさらに縮小することができます。

Nutanix AHV の必要な権限　Image Portability を利用するには、Nutanix AHV 構成のクラスタ管理者である必要があります。

XenServer での必要な権限　Image Portability を使用するには、XenServer ホストが含まれるプールに対して少なくとも「VM 管理者」役割を持っている必要があります。

ネットワーク　Image Portability Service（IPS）は、Compositing Engine（CE）と呼ばれるワーカー VM を作成して、イメージ操作を実行します。関連付けられたリソースの場所/ゾーン内のすべての Connector Appliance が、CE と HTTPS 経由で通信できる必要があります。
Connector Appliance（CA）と CE の間のすべての通信は、CE と CA の間で双方向 HTTPS 通信が行われる vSphere のケースの 1 つの例外を除いて、CA によって開始されます。

クラウド環境（Azure、AWS、Google Cloud）では、CE はプライベート IP アドレスを使用して作成されます。したがって、CE は CA と同じ仮想ネットワーク上か CA から到達可能な仮想ネットワーク上に存在する必要があります。

さらに、サーバーメッセージブロック共有上のファイルが関係するジョブ（エクスポートジョブなど）の場合、CE はサーバーメッセージブロック共有への接続が可能なネットワーク上に存在する必要があります。

サポートされている各プラットフォームで CE に使用するネットワークを指定する方法について詳しくは、Image Portability Service API のドキュメントを参照してください。

「prepare」ジョブの場合、イメージに含まれるオペレーティングシステムが起動され（CE 上）、特殊化やその他のタスクが実行されます。コントロールサーバーに通信する管理エージェントまたはセキュリティエージェントがイメージに含まれている場合、これらのプロセスが準備プロセスに干渉する可能性があります。

ドメインの参加解除オプションが指定されている場合、ネットワーク接続が結果に影響を与える可能性があります。Compositing Engine VM がネットワーク経由で Active Directory ドメインコントローラーにアクセスできる場合、参加解除によりコンピューターアカウントがドメインから削除されます。これにより、イメージが抽出された元の VM のドメインメンバーシップが損なわれます。

したがって、操作のために提供されるネットワークを他のネットワークリソースから分離することをお勧めします。これは、サブネットの分離またはファイアウォール規則によって実行できます。詳しくは、「ネットワークの分離」を参照してください。

一部のオンプレミスのハイパーバイザー環境では、ハイパーバイザーが TLS サーバー証明書を使用して構成される可能性があります。この証明書は、CA の信頼されたルート証明機関のセットによって信頼されていないか、サーバーのホスト名と一致しません。このような状況に対して、問題を回避するために使用できるジョブ要求を **IPS** は提供します。詳しくは、「TLS 証明書」を参照してください。

ネットワークプロキシ　CA とインターネット間のネットワークトラフィックが TLS イントロスペクションを実行するプロキシを通過する場合、プロキシのルート認証局（つまり、プロキシが生成する TLS 証明書に署名するために使用する証明書）を CA のルート認証局のセットに追加する必要があることがあります。詳しくは、「Connector Appliance を Citrix Cloud に登録する」を参照してください。

ネットワークの分離

- Azure

  Azure では、操作で使用される Azure サービスプリンシパルが必要な Azure の権限を持っている場合、CE はデフォルトで NIC に接続されたネットワークセキュリティグループ（NSG）を使用して作成されます[1]。

- Microsoft.Network/networkSecurityGroups/join/action
- Microsoft.Network/networkSecurityGroups/read
- Microsoft.Network/networkSecurityGroups/write

  または、明示的なリソースグループが使用されていない場合は、サブスクリプションのスコープで次の権限が付与されます：

  * Microsoft.Network/networkSecurityGroups/delete
  * Microsoft.Network/networkSecurityGroups/join/action
  * Microsoft.Network/networkSecurityGroups/read
  * Microsoft.Network/networkSecurityGroups/write

この NSG は、以下を除く、CE を出入りするすべてのトラフィックをブロックするように構成されています：

- SMB（ポート 445）送信
- HTTPS（ポート 443）受信
- 内部 Azure サービスに必要なもの

NSG の使用は、ジョブ要求の *networkIsolation* プロパティを *true* に設定することで強制的に有効になります。このケースでは、操作において使用されるサービスプリンシパルに必要なアクセス許可がない場合、ジョブは失敗します。NSG の使用は、*networkIsolation* プロパティを *false* に設定することで無効にできます。

- AWS

AWS で CE のネットワーク分離を実現するには、すべての不要なトラフィックをブロックするネットワークセキュリティグループを作成してから、ジョブ要求において、セキュリティグループ ID のリストを値として取得する *securityGroupIds* 要求パラメーターを使用してセキュリティグループを CE インスタンスに割り当てます。

- Google Cloud

Google Cloud では、CE のネットワーク分離を実現するために、不要なトラフィックをすべてブロックするファイアウォール規則を作成し、ネットワークタグを介してそれらの規則を CE に適用できます。IPS はネットワークタグ *compositing-engine* を使用して CE を作成し、タグのリストを値として取得する *networkTags* ジョブ要求パラメーターを使用して、他のネットワークタグをその CE に割り当てることができます。

TLS 証明書　ハイパーバイザーのサーバー証明書が、CA によって信頼されていない機関によって署名されている場合、問題を解決するために使用できる代替手段が 2 つあります。

1. 証明書の検証で使用する追加のルート証明機関を、ジョブ要求で指定します。この証明書は、ハイパーバイザーのサーバー証明書の署名に使用されるルート証明機関である必要があります。
2. ハイパーバイザーのサーバー証明書の SHA-1 フィンガープリントを、ジョブ要求で指定します。このケースでの証明書の検証は、ハイパーバイザーから返された証明書の SHA-1 フィンガープリントが、ジョブ要求で提供されたものと一致することを確認することになります。CE とハイパーバイザーの間に TLS インターセプトプロキシがある場合、この方法は機能しない可能性があります。

上記のジョブ要求パラメーターは、プラットフォームごとに以下のようになります:

- vSphere
    1. vCenterSslCaCertificate
    2. vCenterSslFingerprint
- Nutanix
    1. prismSslCaCertificate
    2. prismSslFingerprint
- XenServer
    1. xenSslCaCertificate
    2. xenSslFingerprint

詳しくは、「Image Portability Service API のドキュメント」を参照してください。

証明書の検証エラーは、ハイパーバイザーサーバーのホスト名とその証明書内のホスト名が一致しない場合にも発生する可能性があります。このケースでは、ジョブ要求で以下のパラメーターを *true* に設定することで、ホスト名の一致を無効にできます:

- vSphere
    - vCenterSslNoCheckHostname
- Nutanix
    - prismSslNoCheckHostname
- XenServer
    - xenSslNoCheckHostname

関連ドキュメント

- Image Portability Service API のドキュメント
- クラウドサービス用の Connector Appliance
- Google Cloud のドキュメント
- Google Cloud サービスアカウント
- Microsoft Azure アプリの登録と認証

1. If 明示的なリソースグループが操作に使用されている場合、リソースグループのスコープで次の権限が付与されます:

印刷

April 22, 2022

環境でのプリンター管理には、以下の複数の段階があります。

1. 印刷の概念を理解します。
2. 印刷アーキテクチャを計画します。これには、業務上のニーズや既存の印刷インフラストラクチャについての分析と、ユーザーやアプリケーションが現状でどのように印刷を行っているか、および理想的な印刷管理モデルは何かについての評価が含まれます。
3. プリンタープロビジョニングの方法を選択し、印刷設計を展開するためのポリシーを作成して印刷環境を構成します。新しい従業員またはサーバーが追加されたときにポリシーを更新します。
4. 新しい印刷環境を実務環境に展開する前に、その環境をテストします。
5. プリンタードライバーを管理し、印刷のパフォーマンスを最適化して Citrix の印刷環境を維持します。
6. 発生する問題をトラブルシューティングします。

まず「印刷」で、Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）環境での印刷に関する全情報を確認してください。この記事を読み終えたら、次の作業に進むことができます:

- 印刷構成の例
- ベストプラクティス
- 印刷に関するポリシーと設定
- プリンターのプロビジョニング
- 印刷環境の保守

プリントサーバーに **Universal Print Server** をインストールする

1. 各プリントサーバーに Microsoft Virtual C++ Runtime 2017、32 ビットおよび 64 ビットがインストールされていることを確認します。
2. Citrix Universal Print Server の ダウンロードページにアクセスし、［ファイルのダウンロード］をクリックします。
3. 各プリントサーバー上で、次のいずれかのコマンドを実行します。
    - 32 ビットオペレーティングシステムの場合：**UpsServer_x86.msi**
    - 64 ビットオペレーティングシステムの場合：**UpsServer_x64.msi**

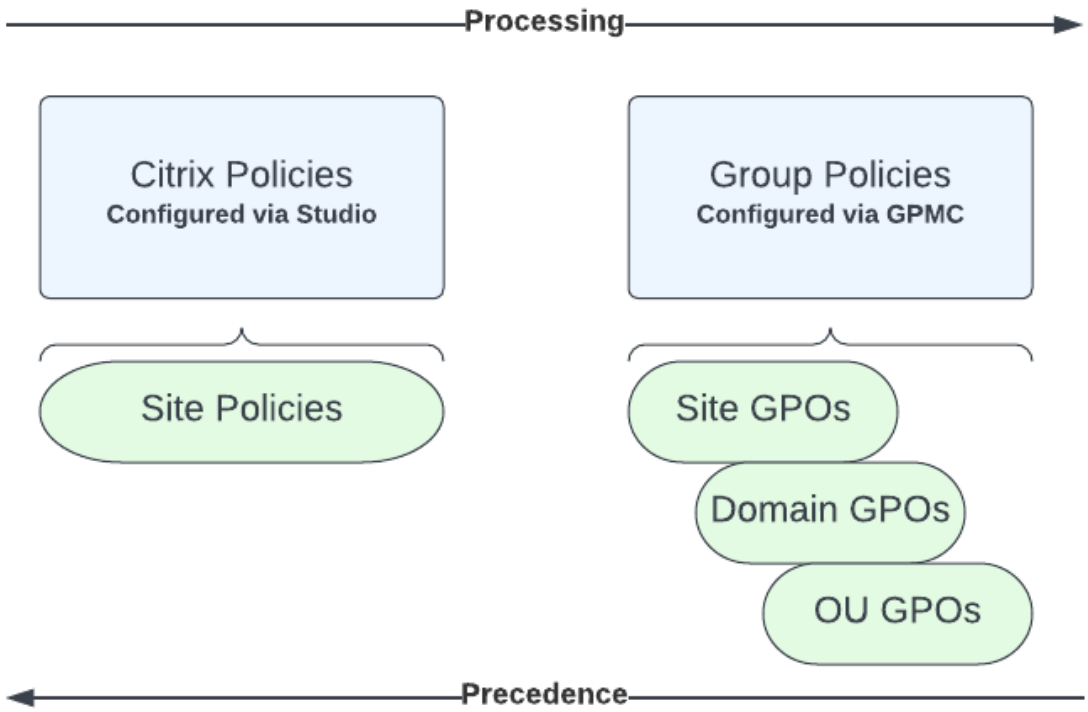
Universal Print Server をインストールしたら、「プリンターのプロビジョニング」の説明に従ってこのコンポーネントを構成します。

ポリシー

April 10, 2023

ポリシーは構成可能な設定項目をグループ化したもので、特定のユーザー、デバイス、または接続の種類に対して特定のセッション、帯域幅、およびセキュリティ構成が適用されるように制御する目的で使用します。

ポリシー設定項目は、VDA またはユーザーに適用できます。Web Studio または Active Directory グループポリシーオブジェクト（GPO）で設定項目を編集できます。ポリシーのフィルター（オブジェクトの割り当て）を指定できます。ポリシーをフィルターに明示的に割り当てない場合、その設定項目はすべてのユーザーセッションに適用されます。



ポリシーは、ネットワークのさまざまなレベルに割り当てることができます。組織単位の GPO レベルに割り当てられたポリシーは、そのネットワークで最も優先されます。ドメイン GPO レベルのポリシーは、サイトグループポリシーオブジェクトレベルのポリシーよりも優先されます。サイトグループポリシーオブジェクトレベルは、Microsoft や Citrix のローカルポリシーレベルの競合ポリシーよりも優先されます。

すべての Citrix サイトポリシーは、Web Studio コンソールで作成および管理され、サイト構成データベースに保存されます。グループポリシーは、Microsoft グループポリシー管理コンソール（GPMC）を使用して作成および管理され、Active Directory に格納されます。Microsoft ローカルポリシーは Windows 上で作成され、レジストリ内に格納されます。

Web Studio のモデル作成ウィザードを使用すると、複数のテンプレートやポリシーの設定項目とその構成内容を比較してポリシーの競合や重複を避けることができます。

複数のポリシーの設定内容は、ポリシーの優先度や条件に基づいて統合されます。優先度のより高いポリシーの設定で［無効］または［禁止］が選択されている場合、優先度の低いポリシーで［有効］または［許可］が選択されていても、その設定内容は無視されます。未構成の設定項目は無視され、優先度の低いポリシーでの設定を上書きすることはありません。

Web Studio ポリシーと Active Directory のグループポリシーの設定内容が競合する場合、優先されるポリシーは状況により異なります。

すべてのポリシーは、以下の順番で処理されます。

1. Citrix Workspace アプリから、エンドユーザーはドメイン資格情報を使用して VDA にログオンします。
2. Citrix ポリシーはエンドユーザーおよび VDA のために処理されます
3. ポリシーは次の順序で適用されます:

    a) ローカルポリシー
    b) サイトポリシー
    c) ドメインポリシー
    d) OU（組織単位）ポリシー

> 注:
>
> - ポリシーが上記 4 つのレベルに存在するとは限りません。ほとんどのユーザーは、サイトポリシーのみを使用します。ローカルポリシーでは、ユーザーが VDA にログオンしてポリシーを編集する必要があります。そのため、これらのポリシーはほとんど使用されません。
> - 1 つの GPO に Windows ポリシーと Citrix ポリシーを混在させることはできません。

Citrix ポリシーについて詳しくは、以下を参照してください:

- ポリシーの使用
- ポリシーテンプレート
- ポリシーの作成
- 優先度、モデル作成、比較およびトラブルシューティングのポリシー
- デフォルトのポリシー設定
- ポリシー設定リファレンス

    > 注:
    >
    > Citrix DaaS のポリシー設定リファレンスは、Citrix Virtual Apps and Desktops のポリシー設定と

> 同じです。そのため、Citrix DaaS については、Citrix Virtual Apps and Desktops ドキュメントの「ポリシー設定リファレンス」セクションも参照できます。

ポリシーの使用

May 25, 2023

ユーザーのアクセスやセッション環境を制御するには、Citrix ポリシーを構成します。Citrix ポリシーを使用して、接続、セキュリティ、および帯域幅の設定を効率的に制御できます。ポリシーは、特定のグループのユーザー、デバイス、または接続の種類を対象に適用できます。1 つのポリシーに複数の設定を選択して構成できます。

Citrix ポリシーを構成するツール

- Studio - Studio を使用して作成したポリシーはサイトデータベースに保存され、次のいずれかの場合に更新プログラムが VDA にプッシュされます:
  - その VDA が Controller に登録された場合
  - ユーザーがセッションを開始した場合
- グループポリシー管理コンソール -ネットワーク環境で Active Directory が使用されており、グループポリシーの管理権限が付与されている場合は、グループポリシー管理コンソール（GPMC）を使用してサイトのポリシーを作成、編集できます。このコンソールでは、必要な設定とフィルターを使用してグループポリシーオブジェクト（GPO）を構成できます。これらのポリシーは、Studio で構成されたポリシーよりも優先されます。詳しくは、CTX238166を参照してください。

ポリシーの処理順序と優先順位

グループポリシーの設定は、以下の順で処理されます。

1. Citrix DaaS サイトのグループポリシーオブジェクト（サイトデータベースに保存されます）
2. ドメインレベルの GPO
3. 組織単位

ただし、2 つのグループポリシーオブジェクトで同じポリシーに異なる設定が適用されている場合は、最後に処理されたポリシー設定によって、以前に処理された設定が上書きされます。つまり、この構成では、ポリシーの設定が以下の順番で優先されることになります:

1. 組織単位
2. ドメインレベルの GPO
3. Citrix DaaS サイトのグループポリシーオブジェクト（サイトデータベースに保存されます）

複数のポリシーを適用する場合は、競合する設定項目が正しく処理されるように優先順位を設定できます。詳しくは、「優先度、モデル作成、比較およびトラブルシューティングのポリシー」を参照してください。

Citrix ポリシーの設定工程

ポリシーを設定する工程は次のとおりです。

1. ポリシーを作成します。
2. ポリシー設定を構成します。
3. ポリシーをマシンやユーザーオブジェクトに割り当てます。
4. ポリシーの優先度を設定します。
5. Citrix グループポリシーモデル作成ウィザードを実行して、ポリシーの効果を確認します。

   > 注:
   >
   > ［ポリシー］>［モデル作成］タブに移動して ［操作］ペインの ［モデル作成ウィザードの起動］をクリックすると、Citrix グループポリシーモデル作成ウィザードが開きます。［モデル作成］タブは、Citrix Cloud でホストされている Web Studio で（顧客の要求ごとに）使用できます。

Citrix ポリシーと設定の使用

ポリシーやテンプレートの設定項目が機能に基づいて分類されています。たとえば、［Profile Management］セクションには、Profile Management のポリシー設定が含まれています。

- 「コンピューター設定」（マシンに適用される設定項目）は仮想デスクトップの動作を制御し、仮想デスクトップの起動時に適用されます。これらの設定項目は、仮想デスクトップにアクティブなユーザーセッションがない場合でも適用されます。
- ユーザー設定によりユーザーエクスペリエンスを制御します。ユーザー設定項目は、ユーザーが接続または再接続するたびに適用されます。

ポリシー、設定項目、およびテンプレートを管理するには、Web Studio のナビゲーションペインで ［ポリシー］を選択します。

- ［ポリシー］タブには、すべての既存のポリシーが表示されます。ポリシーを選択すると、下のタブが表示されます:
  - 概要 - 名前、優先度、有効/無効ステータス、および説明の一覧
  - 設定 - 構成されたすべての設定項目の一覧
  - 割り当て先 - デリバリーグループの一覧割り当ての設定を編集または削除できます。セッションを実行しているデスクトップのデリバリーグループメンバーシップに基づいてポリシーを適用します。詳しくは、「ポリシーの作成」を参照してください。

- ［テンプレート］タブには、組み込みおよびカスタムのテンプレートが表示されます。テンプレートを選択すると、下のタブが表示されます：
  - 説明（テンプレートを使用する理由）
  - 設定（構成された設定項目の一覧）。詳しくは、「ポリシーテンプレート」を参照してください。
  - ［比較］タブでは、複数のポリシーやポリシーテンプレートの設定項目を比較することができます。環境に適した設定項目が構成されているかどうかを確認するときに、この機能を使用できます。詳しくは、「優先度、モデル作成、比較およびトラブルシューティングのポリシー」を参照してください。
  - ［モデル作成］タブでは、特定の接続シナリオでの Citrix ポリシーの効果をシミュレートできます。詳しくは、「優先度、モデル作成、比較およびトラブルシューティングのポリシー」を参照してください。

  ポリシーやテンプレートの設定項目を検索するには、以下の手順に従います：

  1. ポリシーまたはテンプレートを選択します。
  2. ［ポリシーの編集］タブ、または ［テンプレートの編集］タブを選択します。
  3. ［設定項目の選択］ページで、設定項目の名前を入力します。

  以下を選択して、検索を絞り込むことができます：

  - カテゴリ（帯域幅など）
  - ［選択項目のみを表示する］チェックボックス
  - 選択したポリシーに追加された設定項目のみを検索します。

- ポリシーの設定項目を検索するには、以下の手順に従います：

  1. ポリシーを選択します。
  2. ［設定］タブを選択し、設定項目の名前を入力します。

いったんポリシーを作成したら、それは使用されるテンプレートとは無関係です。新しいポリシーの ［説明］フィールドを使って、使用されるソーステンプレートを追跡できます。

ポリシーテンプレート

November 18, 2022

テンプレートは、事前定義された開始ポイントからポリシーを作成するためのソースです。組み込み Citrix テンプレートは、特定の環境またはネットワーク状況に対して最適化され、次のように使用できます。

- サイト間で共有する自分のポリシーおよびテンプレートを作成するためのソース。
- 結果を引用できるため、展開環境間で結果をより簡単に比較するためのリファレンス。例：”…when using Citrix template x or y…”
- Citrix サポートまたは信頼するサードパーティとポリシーを通信するための手段。テンプレートをインポートまたはエクスポートすることで実行できます。

組み込みの **Citrix** テンプレート

使用できるポリシーテンプレートは以下のとおりです。

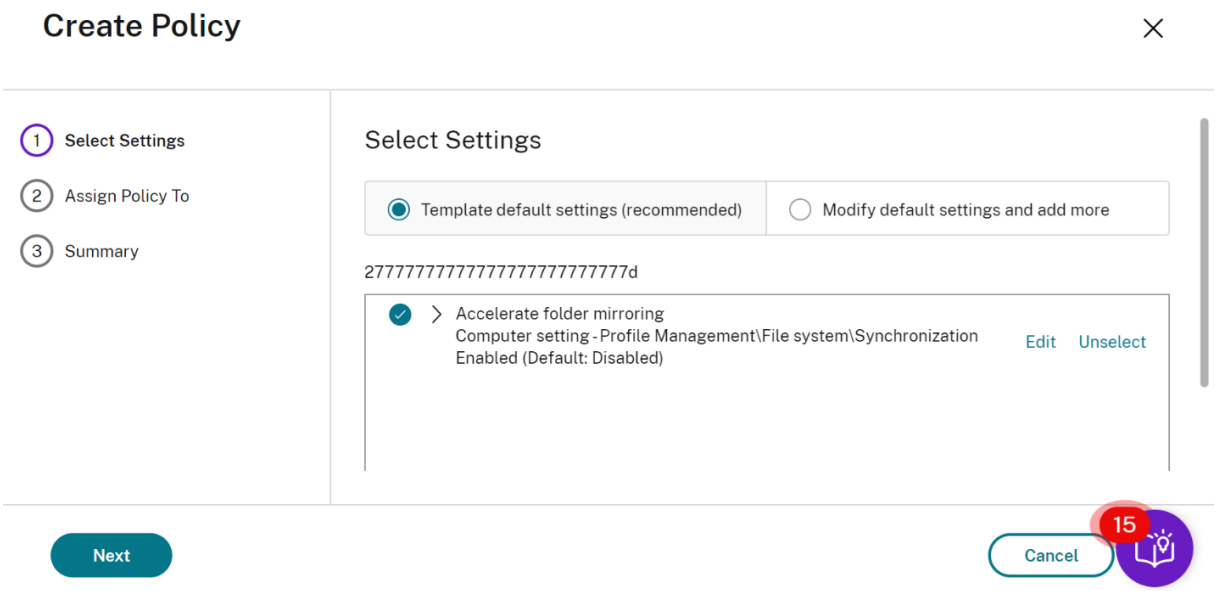
- 最高品位ユーザーエクスペリエンス。このテンプレートは、デフォルトの設定を適用してユーザーエクスペリエンスを最大化します。このテンプレートは、複数のポリシーが優先順に処理されるシナリオで使用します。
- 高サーバースケーラビリティ。サーバーリソースの浪費を避けるには、このテンプレートを適用します。このテンプレートはユーザーエクスペリエンスとサーバーのスケーラビリティの均衡をとります。単一のサーバー上でホストできるユーザー数を増やしつつ、良質のユーザーエクスペリエンスを提供します。このテンプレートは、グラフィックの圧縮にビデオコーデックを使用せず、サーバー側のマルチメディアレンダリングを防ぎます。
- 高サーバースケーラビリティ **-** レガシ **OS**。この高サーバースケーラビリティテンプレートは、Windows Server 2008 R2 または Windows 7 以前が動作する VDA にのみ適用されます。このテンプレートは、これらのオペレーティングシステムでより効率的に機能する従来のグラフィックモードに依存します。
- **NetScaler SD-WAN** に最適化。これは、NetScaler SD-WAN が展開されたブランチオフィスユーザーに適用して Citrix Virtual Desktops の配信を最適化するテンプレートです。（NetScaler SD-WAN は、CloudBridge の新しい名前です）。
- **WAN** の最適化。このテンプレートは、共有 WAN、または低帯域幅接続のリモートの場所を使用する、ブランチオフィスのタスクワーカー向けです。ワーカーは、シンプルなグラフィックのユーザーインターフェイスと、マルチメディアコンテンツがほとんどないアプリケーションにアクセスします。このテンプレートでは、ビデオ再生エクスペリエンスと一部のサーバースケーラビリティが帯域幅の効率性を最適化するため犠牲にされます。
- **WAN** の最適化 **-** レガシ **OS**。このテンプレートは、Windows Server 2008 R2 または Windows 7 以前が動作する VDA にのみ適用されます。このテンプレートは、これらのオペレーティングシステムでより効率的に機能する従来のグラフィックモードに依存します。
- セキュリティと制御。許容率が低い環境でのこのテンプレートの使用にはリスクがあります。Citrix DaaS ではデフォルトで有効な機能が最小化することになります。このテンプレートには、以下へのアクセスを無効にする設定が含まれています：

  - 印刷
  - クリップボード
  - 周辺機器
  - ドライブマッピング
  - ポートリダイレクト
  - ユーザーデバイス上の Flash アクセラレーション

  このテンプレートを適用すると、より多くの帯域幅が消費され、サーバーごとのユーザー密度が減ります。

組み込み Citrix テンプレートはそのデフォルトの設定のままで使用することをお勧めしますが、その設定には特定の推奨値はありません。たとえば、WAN の最適化テンプレートにはセッション全体の最大帯域幅があります。この場

合、テンプレートにより設定が公開され、これによって管理者はこの設定がそのシナリオに適用されようとしていることを理解します。



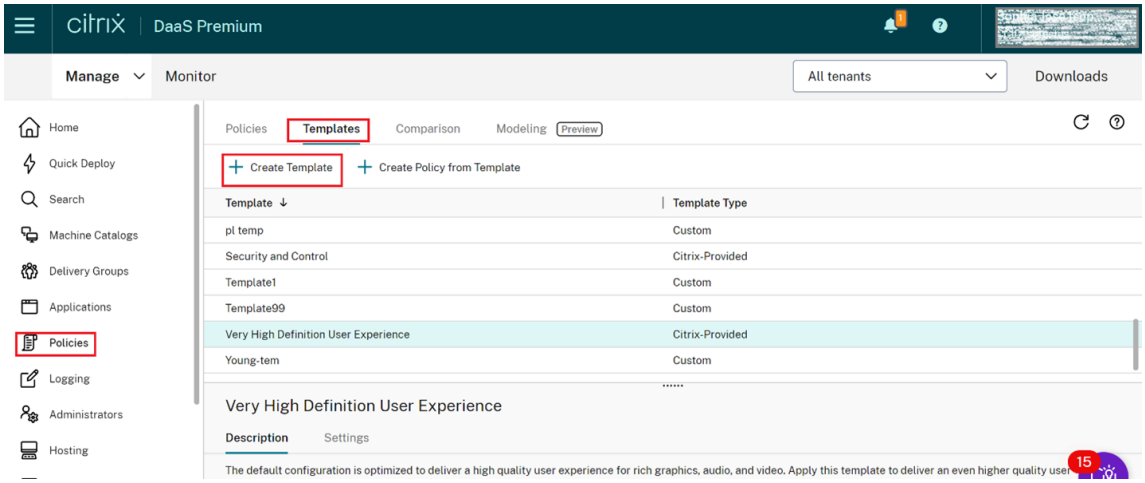
XenApp および XenDesktop 7.6 FP3 より前の環境（ポリシー管理と VDA）を使用しているとします。また、高いサーバースケーラビリティと WAN テンプレートの最適化が必須です。この場合、これらのテンプレートを適用する場合は、従来のバージョンの OS を使用します。

> 注:
>
> Citrix が組み込みテンプレートを開発およびアップデートします。これらのテンプレートを変更したり削除したりすることはできません。

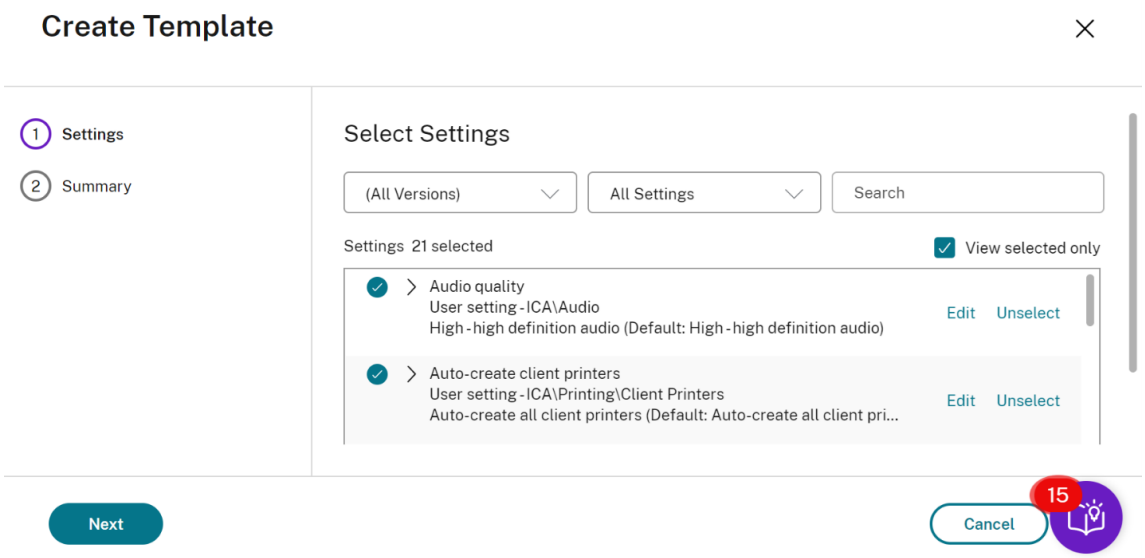
Web Studio 使ったテンプレートの作成と管理

テンプレートをベースにしたテンプレートを作成するには:

1. Web Studio のナビゲーションペインで ［ポリシー］を選択します。



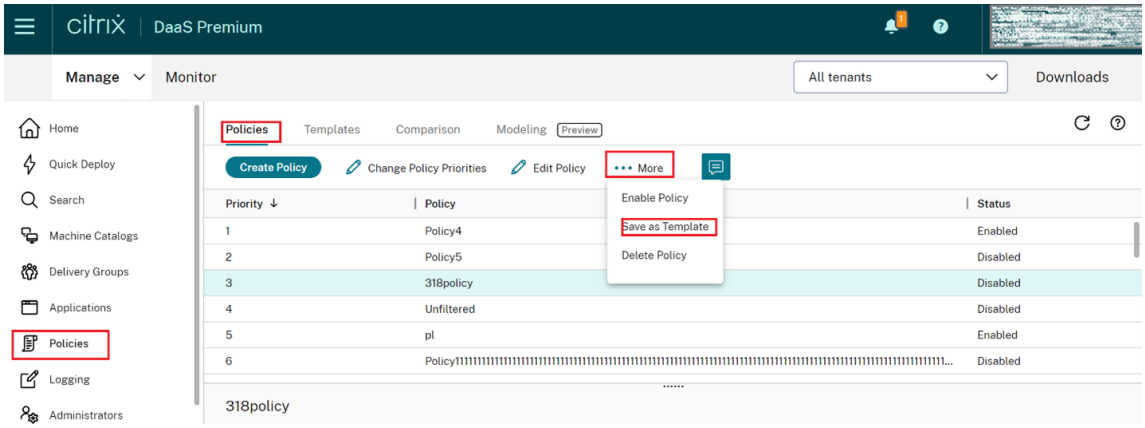
2. ［テンプレート］タブを選択し、作成元のテンプレートを選択します。
3. ［テンプレートの作成］タブを選択します。［設定項目の選択］画面が表示されます。



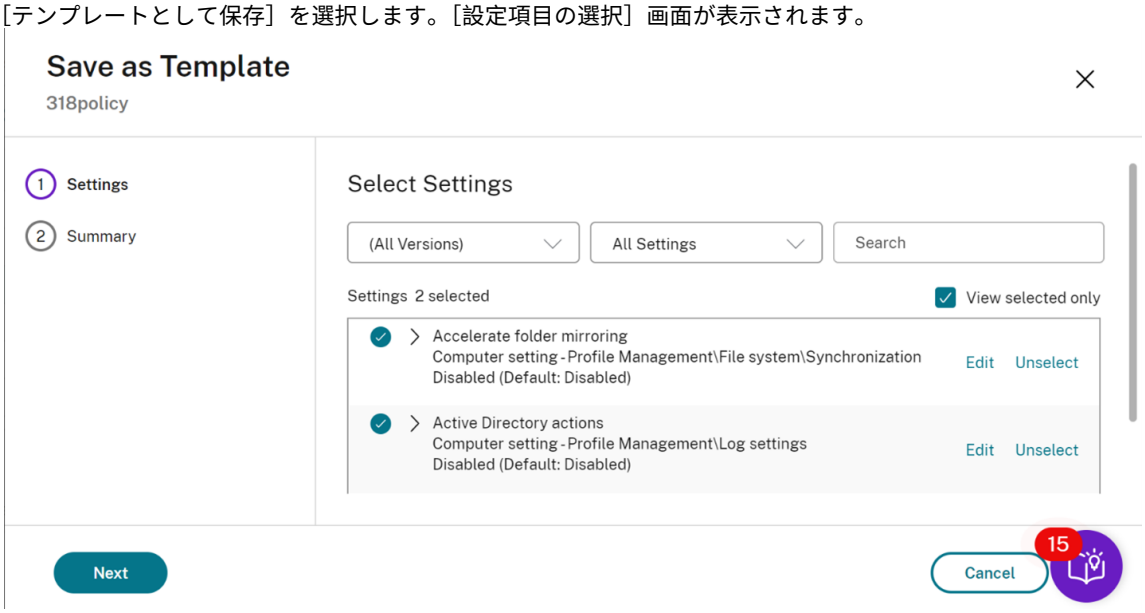
4. テンプレートのポリシー設定を選択して構成します。
5. ［次へ］をクリックします。［概要］画面が開きます。
6. テンプレートの名前を入力します。
7. ［完了］をクリックします。新しいテンプレートが［テンプレート］タブに表示されます。

ポリシーをベースにテンプレートを作成するには：

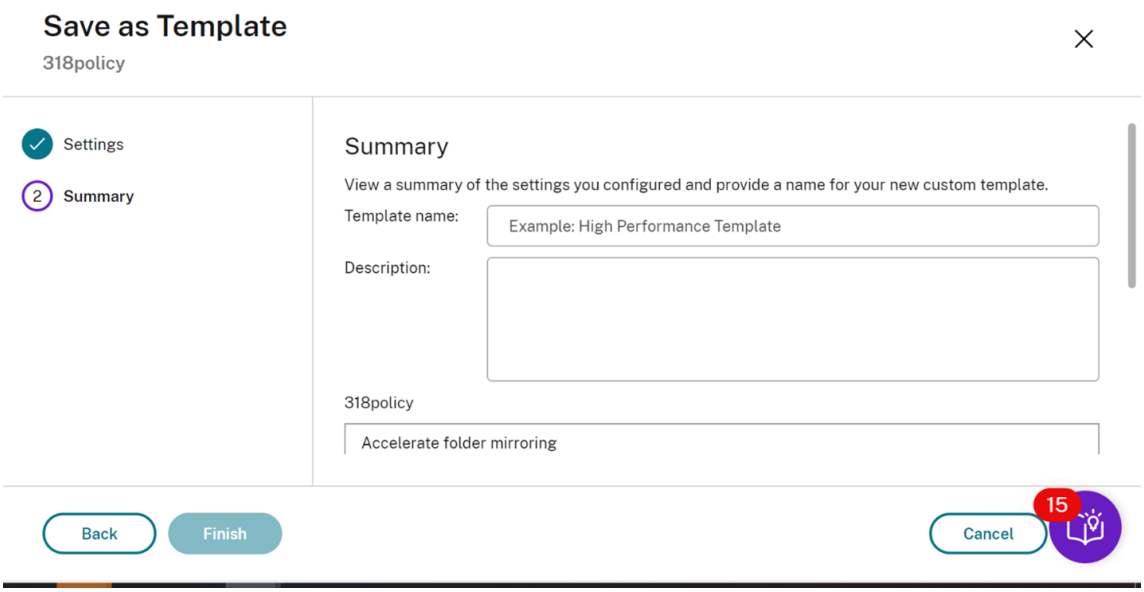
1. Web Studio のナビゲーションペインで ［ポリシー］を選択します。
2. ［ポリシー］タブを選択し、作成元のポリシーを選択します。



3. [詳細] タブをクリックします。
4. [テンプレートとして保存] を選択します。[設定項目の選択] 画面が表示されます。



5. テンプレートに含める新しいポリシー設定を追加して構成します。
6. [次へ] をクリックします。[概要] 画面が開きます。



7. 新しいテンプレートの名前と説明を入力し、［完了］をクリックします。

ポリシーの作成

October 30, 2023

ポリシーを作成する前に、そのポリシーが適用される可能性があるユーザーまたはデバイスのグループを決定します。ユーザーの担当業務、接続の種類、ユーザーデバイス、または作業場所に応じたポリシーを作成できます。

グループに適用するポリシーを作成済みの場合は、別のポリシーを作成するのではなく、そのポリシーを編集することを検討してください。ポリシーを編集した後、適切な設定を構成します。特定の設定内容を変更するため、または特定のユーザーを適用対象から除外するためだけにポリシーを作成することは避けてください。

既存のポリシーテンプレートを基にポリシーを作成し、必要に応じて設定項目をカスタマイズできます。テンプレートを使用せずに作成し、必要なすべての設定を追加することもできます。

Citrix Studio では、新しいポリシーを作成すると、［ポリシーの有効化］チェックボックスが明示的にオンになっていない限り［無効］に設定されます。

ポリシーの作成時および設定の構成時に、システムによって設定の種類を表示するオプションが提供されます。表示できる設定の種類は以下のとおりです。

- すべての設定 - すべての VDA バージョンのすべての設定を表示します
- 現在の設定のみ - 現在の VDA バージョンのみの設定を表示します
- 従来の設定のみ - 廃止された VDA バージョンのみの設定を表示します

設定の構成中に設定を表示するには、以下の手順に従います。

1. DaaS Premium にログインします。
2. 左側のナビゲーションで、［ポリシー］をクリックします。
3. ［ポリシー］タブで、［ポリシーの作成］をクリックします。
4. ［設定の選択］テーブルで、［設定］の横にあるドロップダウンをクリックします。
5. ドロップダウンから次のオプションのいずれかを選択します。
   - すべての設定 - すべての VDA バージョンのすべての設定を表示します
   - 現在の設定のみ - 現在の VDA バージョンのみの設定を表示します
   - 従来の設定のみ - 廃止された VDA バージョンのみの設定を表示します
6. ［設定］テーブルには、前の手順に基づいて使用可能な設定がリストされます。

ポリシー設定

ポリシーを設定するには、適用するポリシー設定を選択して値を構成します。デフォルトでは、ポリシーに追加されている設定項目はありません。設定を適用するには、ポリシーに追加する必要があります。

ポリシーを作成または編集するための設定を構成する際にすべてのデリバリーグループが無効になっていると、システムによって「このフィルター内のどの要素も有効ではありません」という警告通知サインが表示されます。少なくとも 1 つのデリバリーグループが有効になっている場合、システムによる警告サインは表示されません。

ポリシーの作成中に警告を表示するには、以下の手順に従います。

1. DaaS Premium にログインします。
2. 左側のナビゲーションで、［ポリシー］をクリックします。
3. ［ポリシー］タブで、［ポリシーの作成］をクリックします。
4. ［設定項目の選択］テーブルで任意の設定を選択し、［次へ］をクリックします。
5. ［ポリシーの割り当て先］テーブルで、ドロップダウンからフィルタを選択します。
6. ［有効にする］チェックボックスの選択を解除し、［保存］をクリックします。

> 注:
>
> フィルターによっては ［有効にする］チェックボックスの選択を解除できない場合があります。
> ［フィルター］テーブルでは、フィルターによる警告が表示されます。

ポリシーの編集中に警告を表示するには、以下の手順に従います。

1. DaaS Premium にログインします。
2. 左側のナビゲーションで、［ポリシー］をクリックします。
3. ［ポリシー］タブで、リストされているポリシーのいずれかを選択し、［ポリシーの編集］をクリックします。
4. ［ポリシーの編集］ページで、左側のナビゲーションにある ［ポリシーに割り当てる］をクリックします。

5. ［フィルター］テーブルで、必要なフィルターを選択または ［編集］をクリックします。

   - フィルターに ［編集］ボタンがない場合は、フィルタを選択します。
   - フィルターに編集 ボタンがある場合は、［編集］をクリックします。

6. ［有効にする］オプションの選択を解除し、［保存］をクリックします。

> 注:
>
> フィルターによっては ［有効にする］チェックボックスの選択を解除できない場合があります。［フィルター］テーブルでは、フィルターによる警告が表示されます。

ポリシーのいくつかの設定では、次のオプションを指定します。

```
- Allowed or Prohibited allows or prevents the action controlled by the setting. Sometimes users are allowed or prevented from managing the setting's action in a session. For example, if the menu animation setting is set to Allowed, users can control menu animations in their client environment
- Enabled or Disabled turns the setting on or off. If you disable a setting, it is not enabled in lower-ranked policies.
```

また、一部の設定は、それに依存する設定の効果を制御します。たとえば、［クライアントドライブのリダイレクト］設定により、クライアントデバイス側のドライブへのアクセスが制御されます。この設定と ［クライアントネットワークドライブ］設定の両方がポリシーに追加され、ユーザーのネットワークドライブへのアクセスが許可されている必要があります。この場合、［クライアントドライブのリダイレクト］設定で［禁止］を選択すると、［クライアントネットワークドライブ］設定で［許可］を選択しても、ユーザーがネットワークドライブにアクセスできなくなります。

通常、マシンの動作を制御するポリシー設定に対する変更内容は、仮想デスクトップが再起動したときまたはユーザーがログオンしたときに適用されます。また、ユーザーの機能を制御する設定項目は、そのユーザーの次回ログオン時に適用されます。

一部の設定項目では、ポリシーに追加するときに値を入力または選択します。［デフォルト値を使用する］チェックボックスをオンにすると、設定の構成を制限できます。この選択によって設定の構成が無効になり、ポリシーが適用されると、設定項目のデフォルト値しか使用できなくなります。［デフォルト値を使用する］をオンにする前に入力した値は無視されます。

ベストプラクティス:

- ポリシーの適用先として、個々のユーザーアカウントではなくグループアカウントを使用します。ポリシーの対象ユーザーを個々に追加したり削除したりするよりも、そのユーザーがグループアカウントに属しているかどうかで管理した方が効率的です。
- 使用しないポリシーは無効にしておきます。ポリシーに設定を追加しない場合でも、そのポリシーにより不要な処理が行われます。

ポリシーの割り当て

ポリシーを作成するときに、特定のユーザーとマシンオブジェクトにポリシーを割り当てます。そのポリシーは、特定の基準または規則に従って接続に適用されます。通常、1 つのポリシーに複数の割り当てを指定して、複数の条件を組み合わせることができます。割り当てを指定しない場合、そのポリシーはすべての接続に適用されます。

割り当てを指定しない場合、または指定しても無効にしている場合、そのポリシーはすべての接続に適用されます。

> 注:
>
> ポリシーの割り当ては、ポリシーフィルターとも呼ばれます。詳しくは、次のトピックを参照してください:
>
> - ポリシーフィルターの作成、変更、または削除
> - フィルターはどのように適用されますか?

次の表は、使用可能な割り当ての一覧です。

割り当て名	ポリシーの適用対象
アクセス制御	セッションに接続するときのアクセス制御条件。接続の種類 - 接続が NetScaler Gateway 経由かどうかを指定します。*NetScaler Gateway* ファーム名 - NetScaler Gateway 仮想サーバーの名前を指定します。アクセス条件 - 使用するエンドポイント解析ポリシーまたはセッションポリシーの名前を入力します。
Citrix SD-WAN	ユーザーセッションで Citrix SD-WAN が使用されているかどうか。注: ポリシーに追加できる Citrix SD-WAN 割り当ては 1 つのみです。
クライアント IP アドレス	セッションに接続するクライアントデバイスの IP アドレス。IPv4 の場合は 12.0.0.0、12.0.0.*、12.0.0.1-12.0.0.70、12.0.0.1/24 など。IPv6 の場合は、2001:0db8:3c4d:0015:0:0:abcd:ef12、2001:0db8:3c4d:0015::/54 など。
クライアント名	ユーザーデバイスの名前。完全一致の場合、ClientABCName。ワイルドカード文字を使用する場合、Client*Name。
デリバリーグループ	所属するデリバリーグループ。
デリバリー グループの種類	実行されるデスクトップまたはアプリケーションの種類。プライベートデスクトップ、共有デスクトップ、プライベートアプリケーション、または共有アプリケーションから選択します。
組織単位（OU）	組織単位。

割り当て名	ポリシーの適用対象
タグ	マシンのタグ。注：このポリシーをすべてのタグ付きマシンに適用します。アプリケーションタグは含まれていません。
ユーザーまたはグループ	ユーザー名またはグループ名。

ユーザーがログオンするときに、その接続の条件に一致するすべてのポリシーが検出されます。検出されたポリシーは優先度順に処理されます。このとき、ポリシー間で重複している設定がある場合は、最も優先度の高いポリシーの内容が適用されます。たとえば、優先度の高いポリシーの設定で［無効］が選択されている場合、優先度の低いポリシーの同じ設定で［有効］が選択されていても、その設定には［無効］が適用されます。構成されていないポリシー設定は無視されます。

> 重要：
>
> グループポリシー管理コンソールを使って Active Directory ポリシーと Citrix ポリシーの両方を構成する場合、割り当ておよび設定が意図したとおりに適用されない場合があります。詳しくは、CTX127461を参照してください。

「Unfiltered」という名前のポリシーはデフォルトで提供されています。

- Web Studio を使用して Citrix ポリシーを管理する場合は、Unfiltered ポリシーに追加する設定がそのサイトのすべてのサーバー、仮想デスクトップ、および接続に適用されます。
- このサイトと接続は、ポリシーを含むグループポリシーオブジェクト（GPO）のスコープ内にある必要があります。たとえば、営業部署の組織単位に大阪支社のすべての営業メンバーを含んでいる Sales-OSK という GPO がある場合に、いくつかのユーザーポリシー設定を追加した Unfiltered ポリシーを Sales-OSK に設定します。ここで大阪支社の営業部長がサイトにログオンすると、Unfiltered ポリシーのすべての設定が自動的にセッションに適用されます。この構成は、ユーザーが Sales-OSK GPO のメンバーであるためです。

割り当ての［モード］によっても、そのポリシーの適用先が異なります。割り当てのモードとして［許可］（デフォルト）が設定されている場合、その割り当て条件にマッチした接続にのみポリシーが適用されます。割り当てのモードとして［拒否］が設定されている場合、その割り当て条件にマッチしない接続にのみポリシーが適用されます。以下の例では、複数の割り当てを追加した Citrix ポリシーで、割り当てのモードがどのように適用されるかについて説明します。

- 例：同じ種類の割り当てでモードが異なる場合 - ポリシーに同じ種類の割り当てを 2 つ追加し、一方を［許可］にしてもう一方を［拒否］にした場合、［拒否］を設定した割り当てが優先されます。例：

  Policy 1 に以下の割り当てを追加します：

  - Assignment A は営業部署のグループアカウントに適用されます。［許可］を設定します。
  - Assignment B は営業部長のアカウントに適用されます。［拒否］を設定します。

ここで営業部長がログオンした場合、営業部長が営業部署のグループアカウントに属していても、Assignment B が［拒否］モードなのでこの Policy 1 は適用されません。

- 例：異なる種類の割り当てでモードが同じ場合 - ポリシーに異なる種類の複数の割り当てを追加し、すべての割り当てに［許可］を設定した場合、すべての種類の割り当てに一致しないとポリシーは適用されません。例：

  Policy 2 に以下の割り当てを追加します：

  - Assignment C は営業部署のグループアカウントに適用される［ユーザーまたはグループ］割り当てです。［許可］を設定します。
  - Assignment D は 10.8.169.*（企業ネットワーク）を指定するクライアント IP アドレス割り当てです。［許可］を設定します。

  ここで営業部長が社内のオフィスからログオンした場合、上記 2 つの割り当てに合致するので、この Policy 2 が適用されます。

  Policy 3 に以下の割り当てを追加します：

  - Assignment E は営業部署のグループアカウントに適用される［ユーザーまたはグループ］割り当てです。［許可］を設定します。
  - Assignment F は特定の NetScaler Gateway 接続に適用される［アクセス制御］割り当てです。［許可］を設定します。

  ここで営業部長が社内のオフィスからログオンした場合、Assignment F の要件を満たさないので、この Policy 3 は適用されません。

ポリシーセット（**Technical Preview**）

May 17, 2024

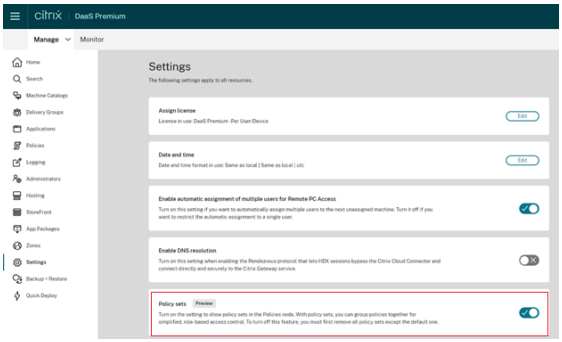
ポリシーセットとは、Citrix DaaS のオブジェクトであり、簡素化された役割ベースのアクセスと容易な管理を可能にするポリシーを集約したものです。ポリシーセットを作成して、管理者チームと会社の論理的な部門をミラーリングできます。たとえば、地理的地域、事業単位、または特定のユースケースごとにポリシー セットを作成できます。ポリシーセットが作成されると、スコープとデリバリーグループが割り当てられるため、権限のある管理者のみが関連するユーザーとマシンに適用されるポリシーを管理できます。

メリット

- 分散された管理者チームに対応した役割ベースのアクセス制御
- 合併、買収、統合の簡素化
- 障害ドメインの限定
- ポリシーのマルチテナントのサポート

ポリシーセットの有効化

Citrix DaaS の ［管理］タブから ［設定］に移動し、［ポリシーセット］設定をオンにします。



> 注:
>
> ポリシーセットを作成する前に、ポリシーセットを有効にする必要があります。

機能比較

ポリシーセットの適用前	ポリシーセットの適用後
サイト全体のポリシー、設定、フィルター、およびポリシーの優先順位は、Citrix Studio 内の 1 か所で構成されます。	ポリシー、設定、フィルター、およびポリシーの優先順位は、ポリシーセットごとに個別に構成されます。
1 つのポリシーを管理する場合は、すべてのポリシーを管理する必要があります。	すべての管理権限を実行できる管理者は、特定のポリシーセットを個別に管理する権限を下位レベルの管理者に委任できます。
大規模な分散環境のポリシーは複雑になり、管理が困難になります。	大規模な分散環境のポリシーは分割して簡単に管理できます。

ポリシーセットはどのように機能しますか?

一般的な概要

- ポリシーセットはデリバリーグループに割り当てられます
- ポリシーセットには 1 つまたは複数のスコープがあります
- ポリシーセットが割り当てられていないデリバリーグループは、デフォルトのポリシーセットを受け取ります
- 1 つのデリバリーグループにはポリシーセットを 1 つだけ割り当てることができます
- 複数のデリバリーグループが同じポリシーセットを使用できます
- ポリシーセットがデリバリー グループに割り当てられている場合でも、ポリシーはそれぞれのフィルターを維持します

詳しくは、「フィルターはどのように適用されますか?」を参照してください。ポリシーセットに関するポリシー割り当てまたはポリシーフィルターの動作に変更はありません。つまり、ポリシーの場合と同じように機能します。

デフォルトポリシーセット

- ポリシーセット設定がオンになっている場合、既存のポリシーはすべてデフォルトのポリシーセット内でグループ化されます。
- 管理者チームがポリシーセットを作成してデリバリーグループに割り当てない限り、すべてのデリバリーグループはデフォルトのポリシーセットを受け取ります。
- デリバリーグループに別のポリシーセットが割り当てられると、デフォルトのポリシーセットからポリシーを取得できなくなります。

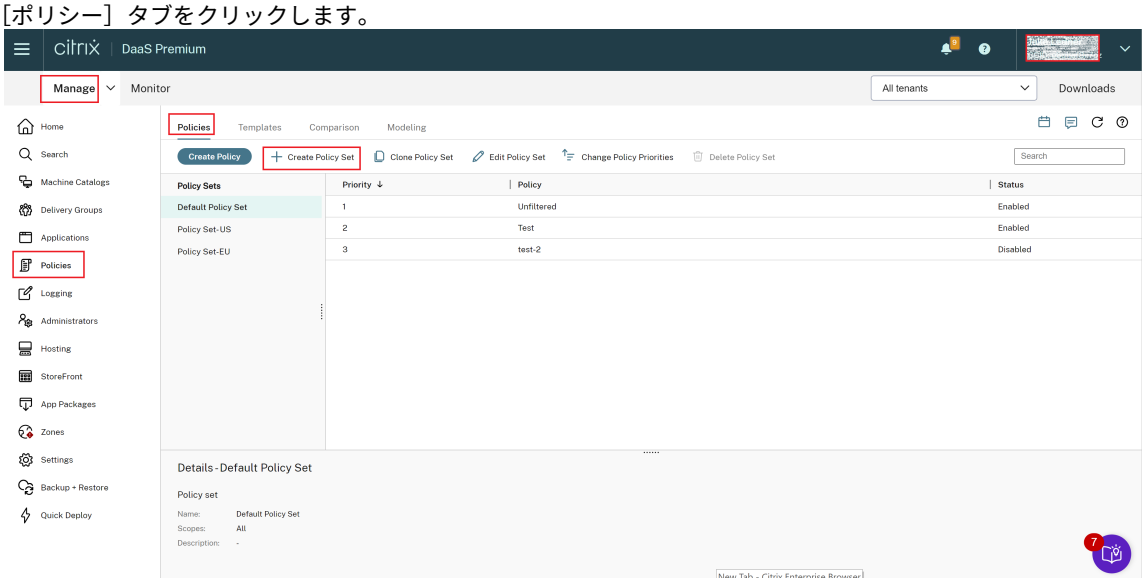
ポリシーセットの作成

ポリシーセットは、次の 2 つの方法で作成できます:

- ポリシーセットの作成 - この操作により、空のポリシーセットが作成されます。
- ポリシーセットの複製 - この操作により、既存のポリシーセットに基づいてポリシーセットが作成されます。

ポリシーセットの作成

1. Citrix DaaS の構成ページで、［管理］タブをクリックします。
2. ［ポリシー］タブをクリックします。



3. ［ポリシーセットの作成］を選択します。［はじめに］タブが表示されます。
4. ［次へ］をクリックするか、［名前と説明］タブをクリックします。
5. ポリシーセットの名前と説明を入力します。
6. ［次へ］をクリックするか、［割り当て］タブをクリックします。

7. ポリシーセットを割り当てるデリバリーグループを 1 つまたは複数選択します。
8. ［次へ］をクリックするか、［スコープ］タブをクリックします。
9. ポリシーセットのスコープを選択します。
10. ［**Create**］をクリックします。ポリシーセットは、定義された割り当てとスコープを使用して作成されます。

ポリシーセットの複製

1. Citrix DaaS の構成ページで、［管理］タブをクリックします。
2. ［ポリシー］タブをクリックします。
3. ［ポリシーセットの複製］を選択します。
4. ポリシーセットの名前を変更します。
5. ポリシーセットの割り当てを変更または作成し、［次へ］をクリックします。
6. 複製されたポリシーセットに含めるポリシーを選択または選択解除します。
7. ポリシーのスコープを変更します。
8. ［**Create**］をクリックします。ポリシーセットが作成されます。

ポリシーセットの編集

1. Citrix DaaS の構成ページで、［管理］タブをクリックします。
2. ［ポリシー］タブをクリックします。
3. ［ポリシーセットの編集］を選択します。
4. ポリシーセットの名前を変更し、［次へ］をクリックします。
5. ポリシーセットの割り当てを変更または作成し、［次へ］をクリックします。
6. ポリシーのスコープを変更します。
7. ［**Create**］をクリックします。

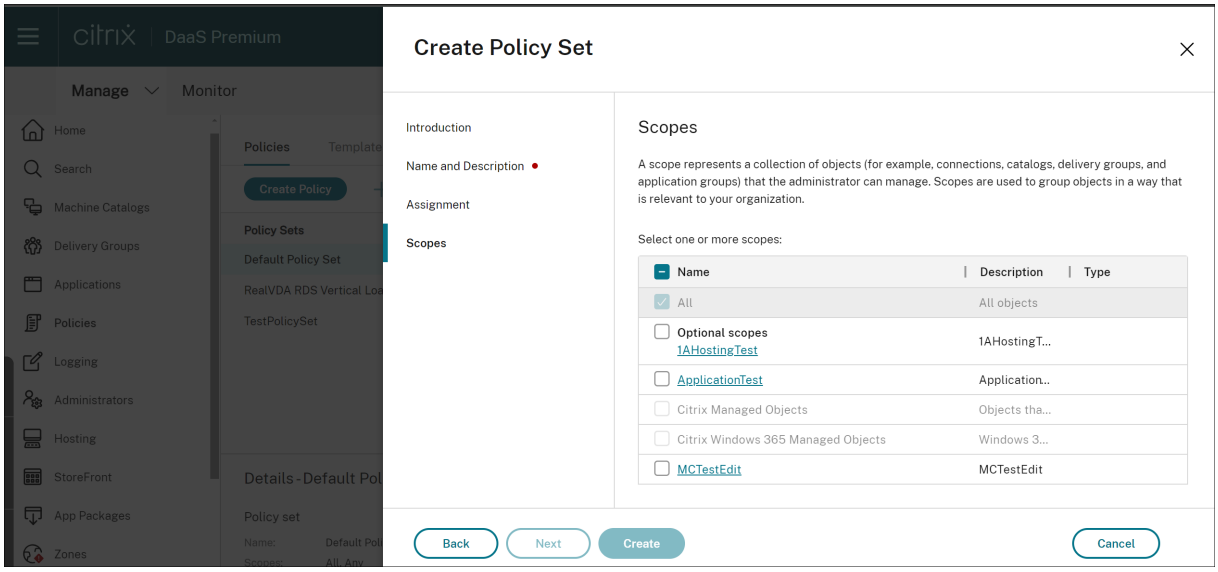
ポリシーセットの割り当て

ポリシーセットはデリバリーグループに割り当てられます。ポリシーセットの作成または編集時に割り当てを構成できます。また、デリバリーグループの作成または編集時に割り当てを構成することもできます。

ポリシーセットのスコープ

管理者は、権限のある管理者のみが表示または編集できるようにポリシーセットのスコープを定義できます。ポリシーセットの作成または編集時にスコープを構成できます。

ポリシーセットの導入により、API を使用して Citrix ポリシーを作成および管理することもできます。詳しくは、「How to create a policy set in Citrix DaaS」を参照してください。



優先度、モデル作成、比較およびトラブルシューティングのポリシー

June 9, 2023

ポリシーを使用して、以下に基づいてユーザーのニーズを満たすように環境をカスタマイズできます:

- 担当業務
- 作業場所
- 接続の種類

たとえば、セキュリティの改善を目的として、機密データを日常的に取り扱うユーザーグループのアクセスに、一定の制限を適用したい場合があります。

また、この場合、ユーザーがローカルのクライアントドライブ上に機密データファイルを保存することを禁止するポリシーを作成できます。ユーザーグループ内のユーザーがローカルドライブにアクセスする必要がある場合は、別のポリシーを作成できます。同じユーザーに複数のポリシーが適用される場合は、それらのポリシーをランク付けして、適用される設定内容を制御できます。多くのポリシーを使用する場合は、次のことを決定する必要があります:

- ポリシーに優先順位を付ける方法
- 例外を作成する方法
- ポリシーが競合する場合に効果的なポリシーを表示する方法

ポリシーの優先度

複数のポリシーで設定内容が競合することを防ぐために、ポリシーに優先度を設定できます。接続の割り当てと一致するポリシーの識別は、ユーザーがシステムにサインオンしたときに行われます。識別されたポリシーとそれに関連

する設定は、優先度順に並べ替えられます。最も優先度の高いポリシーの内容が適用されます。

Web Studio では、ポリシーの優先順位番号を設定できます。デフォルトでは、新しいポリシーに最低の優先度が設定されます。複数のポリシー設定で競合が生じると、優先度の高いポリシーによって優先度の低いポリシーが上書きされます。優先順位番号が 1 のポリシーが最も優先度の高いポリシーです。ポリシー設定は、以下に従ってマージされます:

- ポリシーの優先度
- ポリシーのフィルターで指定されている条件

ポリシーに優先順位を付けるには、次の手順を実行します:

1. 左ペインで ［ポリシー］を選択します。
2. ［ポリシー］タブで、操作バーの ［ポリシーの優先度の変更］を選択します。［ポリシーの優先度の変更］ページが開きます。
3. 優先度一覧で、次の方法を使用してポリシーの優先度を変更します:
    - ポリシーを目的の位置にドラッグします。
    - 位置を 1 つずつ上または下に移動するには、それぞれ上方向アイコンまたは下方向アイコンをクリックします。
    - 一覧の最上部または最下部に移動するには、それぞれ上部矢印アイコンまたは下部矢印アイコンをクリックします。
    - 優先度の番号を変更するには、［編集］アイコンをクリックし、必要に応じた番号を入力し、［保存］をクリックします。
4. ［保存］をクリックします。

例外

ポリシーを作成し、フィルターを使用してユーザー、ユーザーデバイス、またはマシンのグループにそのポリシーを割り当てるとき、いくつかのポリシー設定をグループの中の一部のメンバーに適用したくない場合は、以下の方法で例外を設定します。

- 例外処理を適用するグループメンバー用に新しいポリシーを作成して、ほかのポリシーより高い優先度を設定します。
- ポリシーに追加する割り当てのモードとして ［拒否］を選択します。

割り当てのモードとして ［拒否］を選択すると、その条件にマッチしない接続にのみポリシーが適用されます。たとえば、ポリシーには次の割り当てが含まれます:

- *Assignment A* は、［クライアントの IP アドレス］割り当てで「`208.77.88.*`」を指定します。［許可］を設定します。
- *Assignment B* は、ユーザー割り当てで特定のユーザーアカウントを指定します。［拒否］を設定します。

このポリシーは、*Assignment A* で指定した範囲の IP アドレスでサイトにサインオンするすべてのユーザーに適用されます。ただし、*Assignment B* で指定したユーザーアカウントでサイトにサインオンするユーザーには、このポリシーは適用されません。

> 注:
>
> ［ポリシーの割り当て］の手順で、有効化チェックボックスの選択をオフにすると、ポリシーの割り当ては無効になります。ポリシーの割り当てだけを無効にする場合は、割り当てないのと同じことになり、そのポリシーがサイト内のすべてのオブジェクトに適用されます。

接続に適用されるポリシーの確認

複数のポリシーが適用されるために、意図した設定が接続に反映されないことがあります。作成したポリシーよりも優先度の高いポリシーがあると、意図した設定内容が上書きされてしまいます。管理者は、ポリシーの結果セットを算出でき、接続のために最終的にポリシー設定をどのようにマージするかを決定できます。

以下の方法で、ポリシーの結果セットを算出できます:

- **Citrix** グループポリシーモデル作成ウィザードを使用して、接続シナリオをシミュレートし、Citrix ポリシーがどのように適用されるかを確認する。次のような接続シナリオの条件を指定できます:
  - ユーザー
  - Citrix ポリシーの割り当ての証拠値
- ［グループポリシーの結果］を使用して、特定のユーザーや Virtual Delivery Agent（VDA）に適用される Citrix ポリシーのレポートを作成します。

Web Studio を使用して作成したサイトポリシー設定は、グループポリシー管理コンソールで **Citrix** グループポリシーモデル作成ウィザードを実行する場合、ポリシーの結果セットに含まれません。ポリシーの作成にグループポリシー管理コンソールのみを使用している場合を除き、最も包括的なポリシーの結果セットを確実に取得するためには、**Web Studio** から **Citrix** グループポリシーモデル作成ウィザードを起動することをお勧めします。

ポリシーのモデル作成ウィザードの使用

ポリシーのモデル作成は、計画およびテストのために、フィルターを使用してポリシーを有効にするシミュレーションを行うのに役立ちます。フィルターを使用して有効にしたポリシーのみがモデル化されます。無効にしたポリシーは適用されず、フィルターなしで有効にしたポリシーは常に適用されます。

ポリシーのモデル作成ウィザードを開くには、次の手順を実行します:

1. ［完全な構成］で、［ポリシー］を選択します。
2. ［モデル作成］タブを選択します。
3. 操作バーの ［ポリシーのモデル作成］を選択します。
4. ［はじめに］ページで ［次へ］をクリックします。

5. ユーザーまたはコンピューターを選択します。コンテナまたは特定のユーザーまたはコンピューターを参照できます。［次へ］をクリックします。
6. フィルター値を選択します。オプションで、デリバリーグループ、タグ、クライアント **IP** アドレスなどの追加の詳細を入力することで、シミュレーションをより詳細にすることができます。［次へ］をクリックします。
7. 選択した内容の概要を確認し、［実行］をクリックします。

［実行］をクリックすると、モデル作成の結果のレポートが生成されます。このレポートを表示している間、次のことができます:

- ドロップダウン メニューで ［すべての設定］、［コンピューター設定］、または ［ユーザー設定］を表示するかどうかを選択します。
- 検索バーを使用して、特定の設定を探します。
- 特定の設定をクリックして、その設定の詳細を表示します。たとえば、すべてのユーザー設定が特定のポリシーに適用されなかった場合、［詳細］ペインに設定が適用されなかった理由が表示されます。
- ［エクスポート］をクリックして、モデル作成結果を JSON 形式、HTML 形式、またはその両方でエクスポートします。

ポリシーのモデル作成を実行すると、より多くのオプションを利用できるようになります。次の操作を実行できます:

- モデル作成レポートの表示：このオプションにより、上と同じモデル作成レポートが開き、再度表示したり、エクスポートしたりできます。
- ポリシーのモデル作成の再実行：これにより、以前に選択した同じ一連の基準を使用してポリシーのモデル作成を再実行し、新しいモデル作成の結果を生成できます。これは、一部のポリシーが変更され、それらの変更が現在のモデルにどのように影響するかを確認したい場合に役立ちます。
- モデル作成レポートの削除：これにより、現在のモデル作成レポートが削除されます。

ポリシーおよびテンプレートの比較

Studio では、1 つのポリシーまたはテンプレートの設定を、複数のポリシーまたはテンプレートの設定と比較することができます。たとえば、ベストプラクティスのコンプライアンス状態を維持できる値に設定されているかどうかを確認する場合、ポリシーやテンプレートの各設定項目の設定値を、デフォルトの値と比較することもできます。

1. **Web Studio** のナビゲーションペインで ［ポリシー］を選択します。
2. ［比較］タブをクリックし、［選択］をクリックします。
3. 比較するポリシーまたはテンプレートのチェックボックスをオンにします。［設定項目のデフォルト値と比較する］チェックボックスをオンにすると、各設定項目のデフォルト値が比較結果に追加されます。
4. ［比較］をクリックすると、構成された設定項目とその設定値が一覧表示されます。
5. すべての設定項目を表示するには、［すべての設定項目を表示］を選択します。元の表示に戻るには、［共通の設定項目を表示］を選択します。

ポリシーのトラブルシューティング

複数のポリシーで、適用先として同じ割り当て（ユーザーアカウントやクライアントの IP アドレスなど）を指定することも可能です。このシナリオでは、ポリシーの設定が別のポリシーの設定と競合すると、ポリシーが意図したとおりに適用されない可能性があります。**Citrix** グループポリシーモデル作成ウィザードを実行すると、ユーザー接続に適用されるポリシーが見つからないことがあります。このようなシナリオでは、ポリシーの評価基準に合致する条件でアプリケーションおよびデスクトップに接続するユーザーには、ポリシー設定が適用されません。この状況は、次の場合に発生します：

- 割り当て条件に合致するポリシーがない場合。
- 割り当て条件に合致したポリシーに設定項目が追加されていない場合。
- 割り当て条件に合致したポリシーが無効になっている場合。

指定した条件の接続にポリシーが適用されるようにするには、以下の内容を確認します。

- そのポリシーが有効になっている。
- そのポリシーに追加した設定項目の内容が適切である。

> 注：
>
> ダブルホップシナリオの 2 つ目のホップでは、シングルセッション OS VDA をマルチセッション OS VDA に接続することを検討してください。この場合、Citrix ポリシーは、ユーザーデバイスであるかのように、シングルセッション OS VDA に作用します。たとえば、ポリシーがユーザーデバイスにイメージをキャッシュするように設定されているとします。この例では、ダブルホップ環境における 2 つ目のホップに対してキャッシュされたイメージは、シングルセッション OS VDA マシンでキャッシュされます。

Director

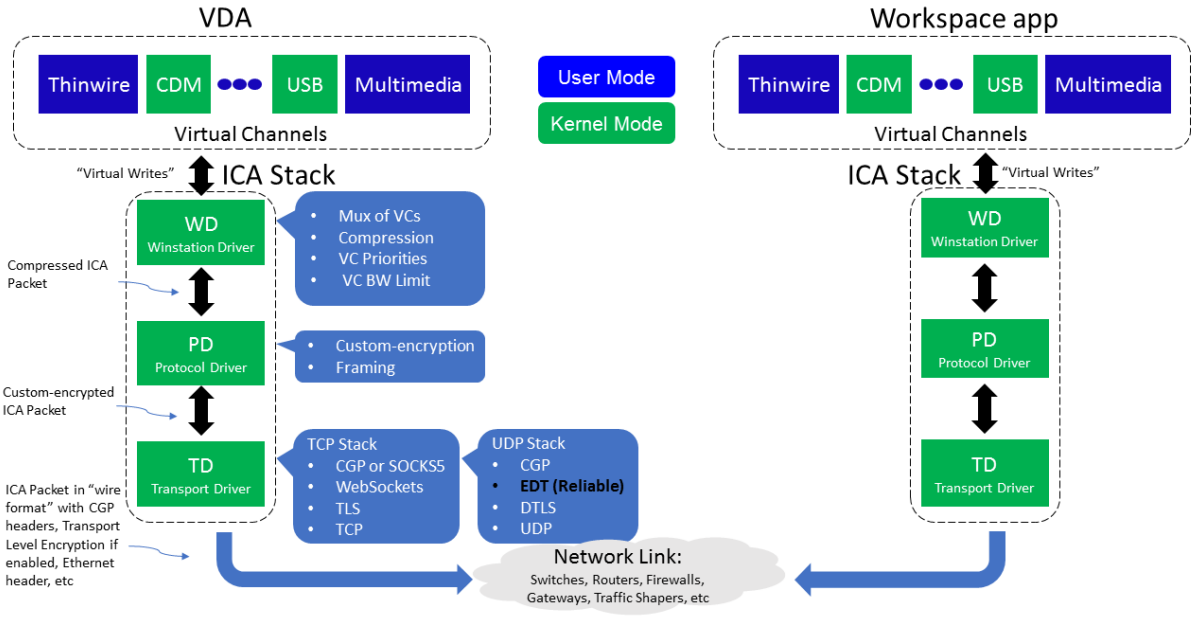
管理者以外の管理者は Director を使用して、ユーザーセッションに適用されるポリシーを表示できます。

HDX の概要

April 18, 2024

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

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

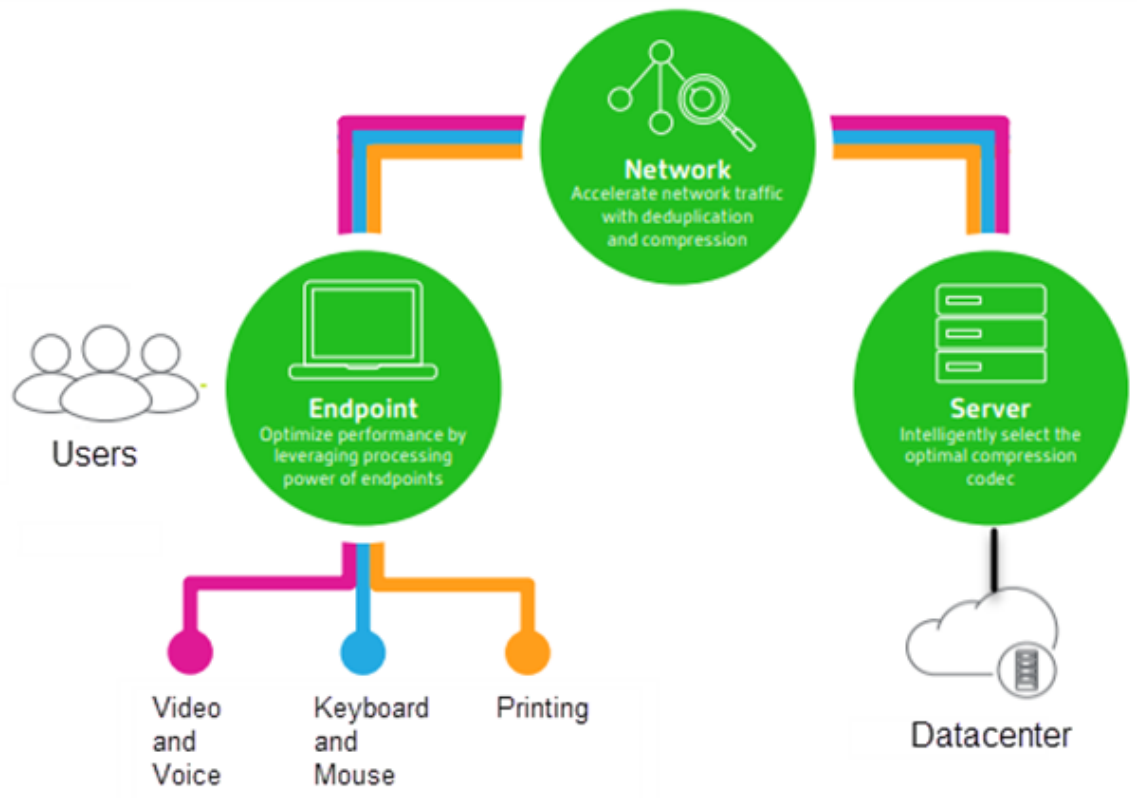


HDX は、次の 3 つの技術原則に基づいて設計されています:

- インテリジェントリダイレクト
- 連続文字圧縮
- データ重複排除

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

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



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

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

デバイスで

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

ネットワークで

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

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

データセンターでは

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

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

HDX Insight

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

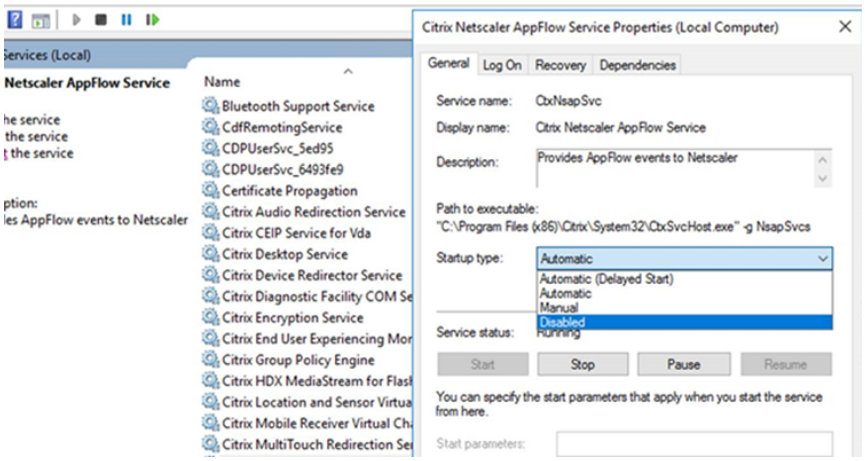
NetScaler で HDX Insight 仮想チャネルを使用して必要なすべてのデータポイントを非圧縮形式で移動できるようにすることができます。この機能を無効にした場合、NetScaler デバイスは、さまざまな仮想チャネルに分散した ICA トラフィックを暗号化解除して解凍します。単一の仮想チャネルを使用すると、複雑さが軽減され、スケーラビリティが向上し、コスト効率が向上します。

最小要件:

- Citrix Virtual Apps and Desktops 7 バージョン 1808
- XenApp および XenDesktop 7.17
- NetScaler バージョン 12.0 ビルド 57.x
- Windows 向け Citrix Workspace アプリ 1808
- Citrix Receiver for Windows 4.10
- Mac 向け Citrix Workspace アプリ 1808
- Citrix Receiver for Mac 12.8

HDX Insight 仮想チャネルを有効または無効にする

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



仮想デスクトップからの **HDX** 機能の体験

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

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

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

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

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

- HDX は、クライアントプラットフォーム、アプリケーション、およびネットワーク帯域幅に基づいて最適な配信方法を自動的に選択し、状況の変化に応じて自動調整します。
- HDX は、2D および 3D のグラフィックおよびビデオのパフォーマンスを最適化します。
- HDX は、インターネットやイントラネット上のマルチメディアコンテンツなどをホストサーバーを介さず直接ユーザーデバイス上にストリーム配信します。このクライアント側でのコンテンツ取得に必要な条件が満た

されない場合、メディア配信はサーバー側でのコンテンツ取得とマルチメディアリダイレクトにフォールバックします。通常、マルチメディアリダイレクト機能に関するポリシーを変更する必要はありません。

- マルチメディアリダイレクトが利用できない場合、HDX は仮想デスクトップにサーバー側でレンダリングしたビデオコンテンツを提供します。http://www.microsoft.com/silverlight/iis-smooth-streaming/demo/などのサイトにアクセスして、高品位ビデオを含む Web サイト上のビデオをご覧ください。

ヒント:

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

クライアントの自動再接続とセッション画面の保持

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

クライアントの自動再接続:

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

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

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

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

クライアントの自動再接続のデフォルト設定:

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

詳しくは、「クライアントの自動再接続のポリシー設定」を参照してください。

セッション画面の保持:

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

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

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

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

セッション画面の保持のデフォルト設定

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

詳しくは、「セッション画面の保持のポリシー設定」を参照してください。

NetScaler とクライアントの自動再接続およびセッション画面の保持:

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

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

HDX アダプティブスループット

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

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

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

この機能には以下の要件があります:

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

ユーザーデバイスに送信されるイメージ品質の改善

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

- 表示品質。ユーザーデバイス上に表示されるイメージの表示品質として、[低]、[中]、[高]、[常に無損失]、または［操作時は低品質］を指定します。デフォルトは［中］です。メディアのデフォルト設定による実際のビデオ品質は、利用可能な帯域幅によって異なります。
- ターゲットフレーム数仮想デスクトップからユーザーデバイスに送信されるイメージの 1 秒あたりの最大フレーム数（fps）を指定します。デフォルトは 30fps です。CPU が低速なデバイスでは、小さい値を指定した方がユーザーエクスペリエンスが向上する場合があります。サポートされている 1 秒あたりの最大フレームレートは 60 です。
- 表示メモリの制限。セッションのビデオバッファーの最大サイズをキロバイト単位で指定します。デフォルトは 65536KB です。高い色数および解像度を使用するセッションでは、大きい値を指定します。必要なメモリの量は算出できます。

ビデオ会議パフォーマンスの改善

いくつかの一般的なビデオ会議アプリケーションは、マルチメディアリダイレクトを介する Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）からの配信に最適化されています（「HDX RealTime Optimization Pack」などを参照）。最適化されていないアプリケーションでは、HDX Web カメラビデオ圧縮を使用すると、セッションで

のビデオ会議で Web カメラの帯域幅使用効率および遅延に対する耐性が向上します。この機能では、Web カメラのトラフィックが専用のマルチメディア仮想チャネルでストリーム配信されます。この機能では、HDX Plug-n-Play USB リダイレクトサポートのアイソクロナス転送に比べて帯域幅消費が少なく、WAN 接続に適しています。

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

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

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

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

ネットワークトラフィックの優先度

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

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

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

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

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

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

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

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

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

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

リモート言語バーを表示または非表示にする

言語バーには、アプリケーションセッションでの優先される入力言語が表示されます。この機能が有効（デフォルト）になっている場合、Windows 向け Citrix Workspace アプリの ［詳細設定］ > ［言語バー］から言語バーを表示または非表示にできます。VDA 側でレジストリ設定を使用すると、言語バー機能のクライアント制御を無効にできます。この機能を無効にした場合、クライアントの UI 設定が有効にならず、ユーザーごとの現在の設定によって言語バーの状態が決まります。詳しくは、「ユーザーエクスペリエンスの向上」を参照してください。

VDA から言語バー機能のクライアント制御を無効にするには:

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

Unicode キーボードマッピング

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

Unicode キーボードレイアウトマッピングを有効または無効にする

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

KEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

値の名前：EnableKlMap

種類：DWORD

値：1

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

Unicode キーボードレイアウトマッピング互換モードを有効にする

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

HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

値の名前：DisableWindowHook

種類：DWORD

値：1

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

Citrix ICA 仮想チャネル

March 5, 2024

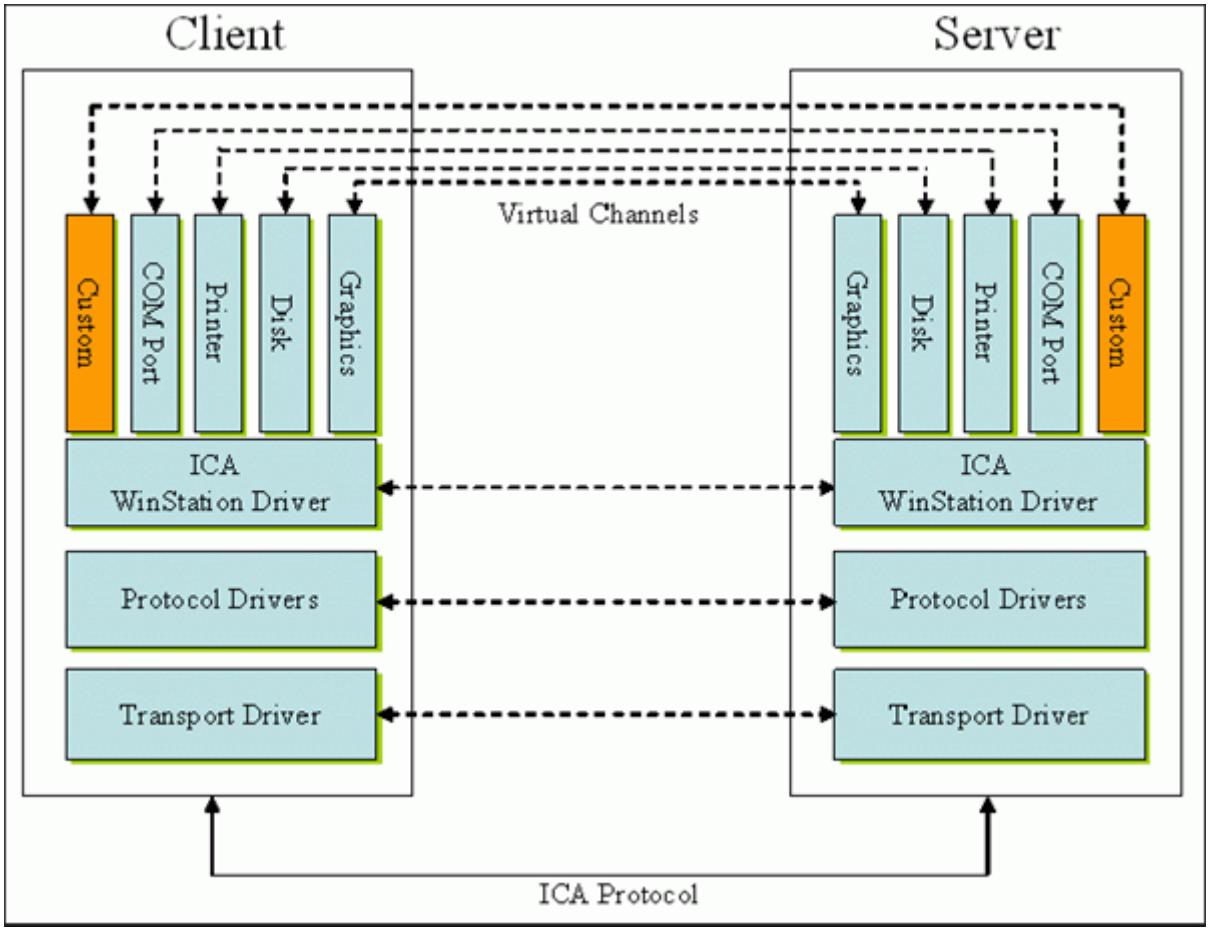
> 警告:
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix では一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

ICA 仮想チャネルとは何か

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

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

Citrix DaaS および Citrix Workspace アプリとともに、追加機能を提供する新しい仮想チャネルが随時リリースされます。



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

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

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

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

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

または

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

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

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

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

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

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

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

64 ビット環境との互換性

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

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

汎用 **USB** 仮想チャネル

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

- ctxusbm.sys
- ctxusbr.sys

ICA 仮想チャネルの動作

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

以下は、シェルによって読み込まれる仮想チャネルモジュールの例です：

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

以下の例のように、カーネルモードで読み込まれる場合もあります：

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

サーバー側のグラフィック仮想チャネル

XenApp 7.0 および XenDesktop7.0 以降では、`ctxgfx.exe`はワークステーションとターミナルサーバーの両方でセッションごとにグラフィック仮想チャネルをホストします。`Ctxgfx`は、対応するドライバー（RDSH の場合は`Icardd.dll`、ワークステーションの場合は`vdod.dll`と`vidd.dll`）と通信するプラットフォーム固有のモジュールをホストします。

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

Windows サービスでの専用チャネルのホスト

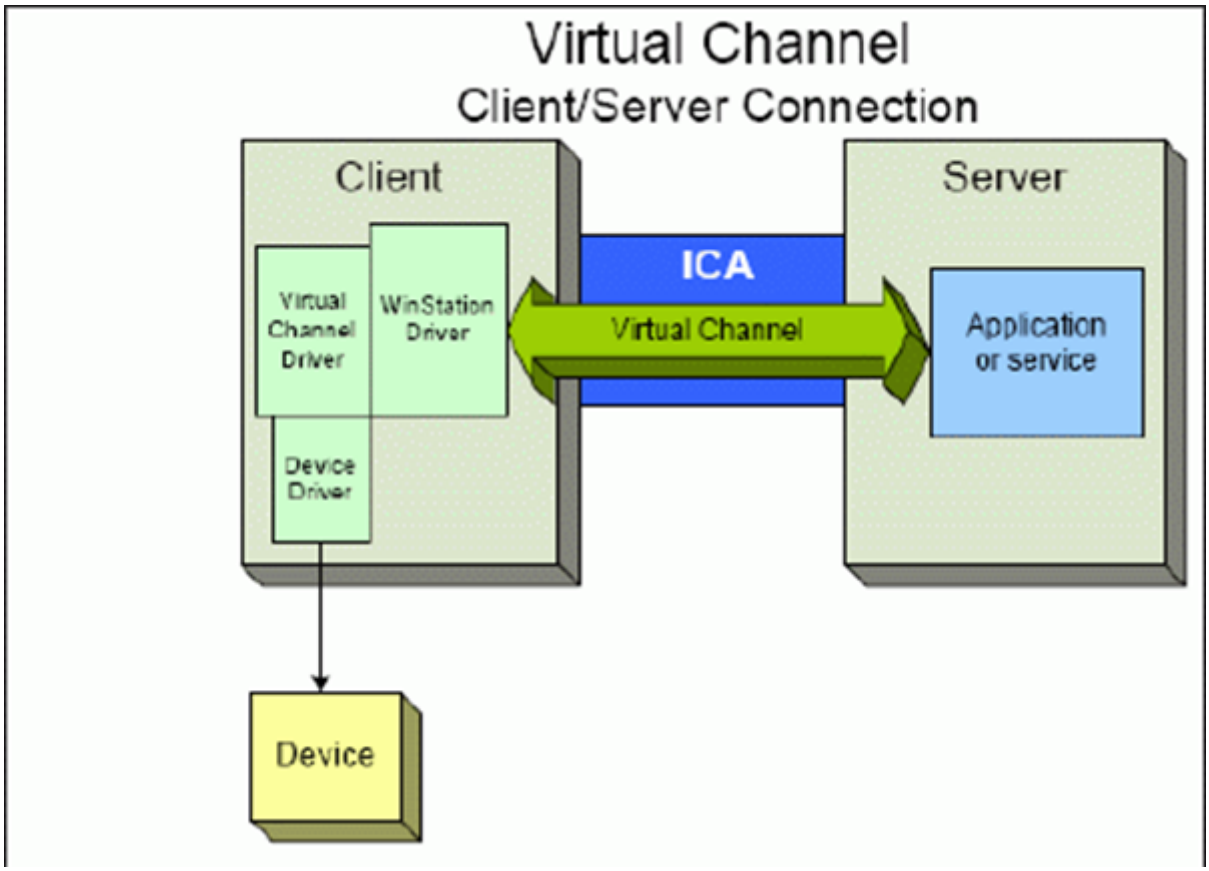
Citrix DaaS サーバーでは、さまざまなチャネルが Windows サービスとしてホストされています。これによって、サーバー上のシングルセッションおよびマルチセッションで複数のアプリケーションの 1 対多の運用が可能になります。以下はこうしたサービスの例です：

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

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

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

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



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

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

- サーバー側アプリケーションにクライアントへの送信データがある場合は、そのデータが直ちにクライアントに送信されます。クライアントがこのデータを受け取ると、WinStation ドライバーが ICA ストリームから仮想チャネルデータを逆多重化し、それを直ちにクライアント仮想ドライバーに渡します。
- クライアント仮想ドライバーにサーバーへの送信データがある場合は、WinStation ドライバーが次回ポーリングを行ったときにそのデータが送信されます。サーバーがこのデータを受信すると、そのデータは仮想チャネルアプリケーションが読み込むまでキューに保持されます。サーバーがデータを受け取ったことは、サーバーの仮想チャネルアプリケーションに通知されません。

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

仮想チャネル **SDK** を使って独自の仮想チャネルを作成する

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

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

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

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

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

詳しくは、『Client Object API Specification Programmer’s Guide』を参照してください。

仮想チャネルのパススルー機能

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

以下の機能は、シングルホップ構成でもマルチホップ構成でも同様に動作します:

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

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

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

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

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

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

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

以下の標準的な仮想チャネルおよびその機能がサポートされています：

- Client
- クライアント側 COM ポートのマッピング
- クライアントドライブマッピング

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

セキュリティと **ICA** 仮想チャネル

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

ベストプラクティス

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

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

仮想チャネルの名前付け：

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

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

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

ダブルホップのサポート：

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

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

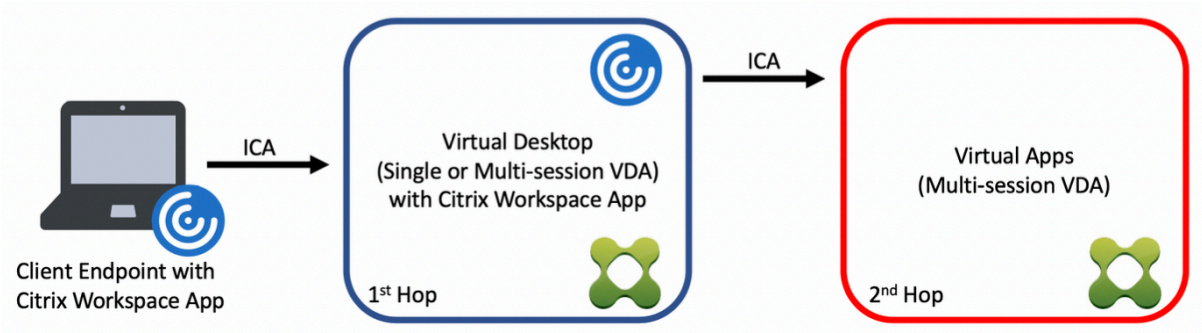
関連項目

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

Citrix DaaS でのダブルホップ

May 17, 2024

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



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

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

システム要件

すべての Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）エディションは、ダブルホップをサポートしています。

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

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

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

ダブルホップでの **HDX** の展開に関する考慮事項

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

グラフィック

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

遅延

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

マルチメディア

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

USB デバイスリダイレクト

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

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

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

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

サポートの例外

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

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

HDX 接続

May 17, 2024

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

HDX は、次の 3 つの技術原則に基づいて設計されています：

- インテリジェントリダイレクト
- 連続文字圧縮
- データ重複排除

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

HDX オファリング内では、独自の専用トランスポートプロトコルを介して接続し、セッションを確立するときに最大転送ユニットを利用し、Citrix SD-WAN との接続を最適化できます。

アダプティブトランスポート

May 17, 2024

アダプティブトランスポートは、Citrix Virtual Apps and Desktops のメカニズムであり、優先トランスポートプロトコルを使用して HDX セッションの接続を確立し、優先プロトコルによる接続が利用できない場合に TCP へのフォールバックを提供します。

次のトランスポートプロトコルがサポートされています:

- Enlightened Data Transport（EDT）
- 伝送制御プロトコル（TCP）

構成

アダプティブトランスポートはデフォルトで有効になっています。アダプティブトランスポートを次のモードで動作するように構成できます:

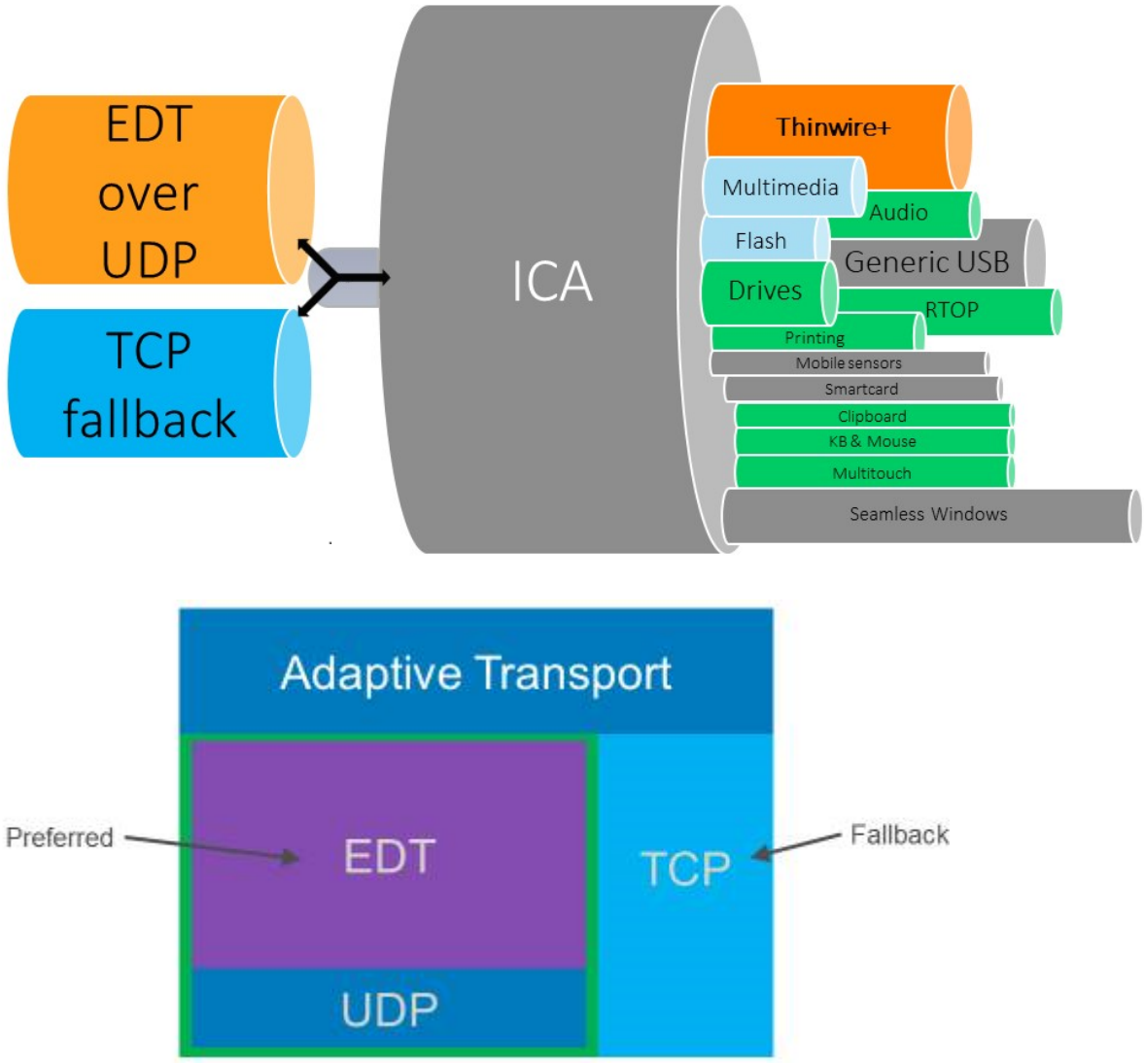
- 優先:（デフォルト）クライアントは優先プロトコルで接続を試み、優先プロトコルで接続できない場合は TCP にフォールバックします。
- 診断モード:クライアントは、優先プロトコルを使用してのみ接続を試行します。[Fall back to TCP] は無効です。
- オフ:クライアントは TCP を使用してのみ接続を試行します。

機能

アダプティブトランスポートが`Preferred`に設定されている場合、クライアントは優先プロトコルと TCP の両方を並行してセッションに接続しようとします。これにより、優先プロトコルで接続できず、クライアントが TCP の使用にフォールバックする必要がある場合に、接続時間を最適化できます。TCP を使用して接続が確立された場合、クライアントは 5 分ごとにバックグラウンドで優先プロトコルを使用して接続を試行します。

アダプティブトランスポートが`Diagnostic mode`に設定されている場合、クライアントは優先プロトコルのみを使用してセッションに接続します。クライアントが優先プロトコルを使用して接続を確立できない場合、TCP の使用にフォールバックせず、接続は失敗します。

アダプティブトランスポートが`Off`に設定されている場合、アダプティブトランスポート は無効になり、クライアントは TCP のみを使用してセッションに接続します。



システム要件

アダプティブトランスポートと EDT を使用するための要件は次のとおりです:

- コントロールプレーン
  - Citrix DaaS（旧称：Citrix Virtual Apps and Desktops サービス）
  - Citrix Virtual Apps and Desktops：現在サポートされているバージョン
- Virtual Delivery Agent
  - Windows：現在サポートされているバージョン（2402 以降を推奨）
  - Linux：現在サポートされているバージョン（2402 以降を推奨）
- Citrix Workspace アプリ

  - Windows：現在サポートされているバージョン（2402 以降を推奨）
  - Linux：現在サポートされているバージョン（2402 以降を推奨）
  - Mac：現在サポートされているバージョン（2402 以降を推奨）
  - iOS：Apple App Store で入手可能な最新バージョン
  - Android：Google Play で利用可能な最新バージョン

- Citrix NetScaler Gateway
  - 14.1.12.30 以降（推奨）
  - 13.1.17.42 以降（13.1-52.19 以降を推奨）

> 注：
>
> Linux VDA の詳細については、Linux Virtual Delivery Agentのドキュメントを参照してください。

ネットワークの要件

次のセクションは、アダプティブトランスポートで EDT を使用するためのネットワーク要件です：

セッションホスト

セッションホストに Windows Defender ファイアウォールなどのファイアウォールがある場合は、内部接続に対して次の受信トラフィックを許可する必要があります。

説明	接続元	プロトコル	ポート
内部接続 - セッション画面の保持が有効	クライアント	UDP	2598
内部接続 - セッション画面の保持が無効			1494
内部接続 - HDX Direct または VDA SSL			443

> 注：
>
> VDA インストーラーは、適切な受信規則を Windows Defender ファイアウォールに追加します。別のファイアウォールを使用する場合は、上記の規則を追加する必要があります。

内部ネットワーク

次の表は、ネットワークで EDT を使用するために必要なファイアウォール規則を示しています：

説明	プロトコル	接続元	接続先	接続先ポート
直接内部接続 - セッションの信頼性が有効	UDP	クライアント側ネットワーク	VDA ネットワーク	2598
直接内部接続 - セッションの信頼性が有効				1494
直接内部接続 - HDX Direct または SSL VDA				443
NetScaler Gateway		NetScaler SNIP		2598
NetScaler Gateway - VDA SSL				443

> 注:
>
> Citrix Gateway サービスを使用している場合は、**Rendezvous** が EDT をトランスポートプロトコルとして使用できるようにする必要があります。システムおよびネットワークの要件については、Rendezvousのドキュメントを参照してください。

クライアント側ネットワーク

次の表は、クライアントデバイスの接続要件を示しています:

説明	プロトコル	接続元	接続先	接続先ポート
内部接続 - セッション画面の保持が有効	UDP	クライアント IP	VDA ネットワーク	2598
内部接続 - セッション画面の保持が無効				1494
内部接続 - HDX Direct または SSL VDA				443
外部接続 - NetScaler Gateway			NetScaler Gateway パブリック IP アドレス	443

説明	プロトコル	接続元	接続先	接続先ポート
外部接続 - Citrix Gateway サービス			Citrix Gateway サービス	443

> 注:
>
> Citrix Gateway サービスを使用している場合、クライアントはhttps://*.*.nssvc.netにアクセスできる必要があります。https://*.*.nssvc.netを使用してすべてのサブドメインを許可できない場合、代わりにhttps://*.c.nssvc.netおよびhttps://*.g.nssvc.netを使用します。詳しくは、Knowledge CenterのCTX270584を参照してください。

Enlightened Data Transport

May 17, 2024

Enlightened Data Transport（EDT）は、ユーザーデータグラムプロトコル（UDP）上に構築された Citrix 独自のトランスポートプロトコルです。サーバーのスケーラビリティを維持しながら、要求の厳しい長距離接続で優れたユーザーエクスペリエンスを提供します。EDT は、信頼性の低いネットワーク上のすべての ICA 仮想チャネルのデータスループットを向上させ、より優れた、より一貫性のあるユーザーエクスペリエンスを提供します。

アダプティブトランスポートが有効になっている場合、EDT が優先プロトコルになります。

知っておくべきこと

- NetScaler Gateway および Citrix Gateway サービスで **MTU Discovery** と EDT を使用するには、セッション画面の保持を有効にする必要があります。
- パケットの断片化により、パフォーマンスが低下したり、場合によってはセッションの起動に失敗したりすることがあります。これを防ぐには、EDT MTU をネットワークに適した値に調整する必要があります。EDT MTU Discovery を使用するか、「How to configure MSS when using EDT on networks with non-standard MTU」の説明に従って手動の回避策を使用できます。
- NetScaler Gateway で EDT の使用を有効にする方法の詳細については、「Enlightened Data Transport をサポートするように NetScaler Gateway を構成する」を参照してください。

EDT MTU Discovery

MTU Discovery により、セッション確立時に EDT が最大伝送単位（MTU）を自動的に決定できるようにします。これにより、パフォーマンスの低下やセッションの確立失敗となる可能性のある、EDT パケットのフラグメンテーショ

ンが防止されます。

MTU Discovery はデフォルトで有効になっています。無効にする必要がある場合、詳細は「レジストリで管理される HDX 機能」を参照してください。

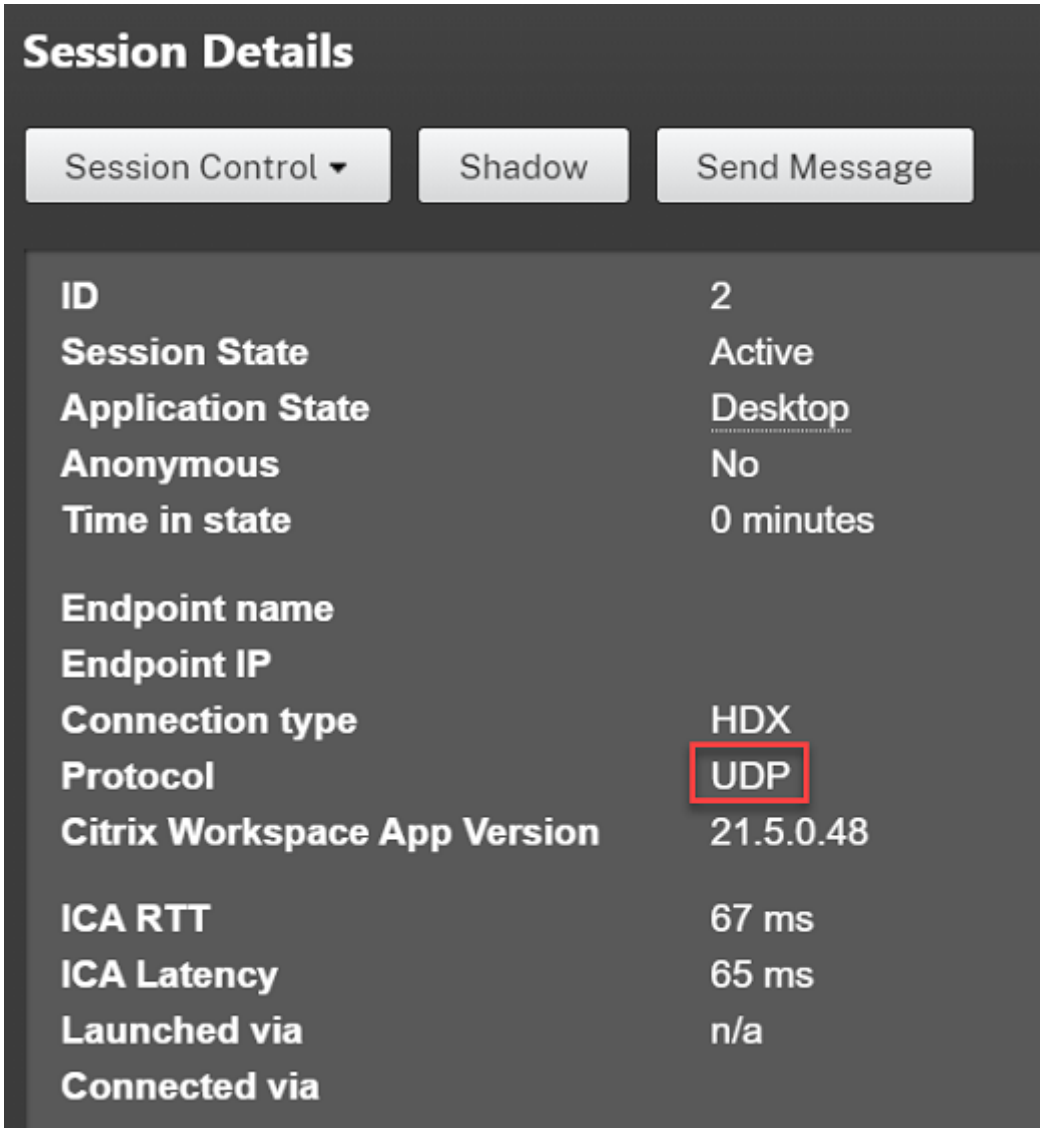
> 注:
>
> - MTU Discovery が機能するには、［セッション画面の保持］を有効にする必要があります。
> - マルチストリーム ICA を使用した MTU Discovery は、VDA バージョン 2209 以降で利用できます。

トラブルシューティング

May 17, 2024

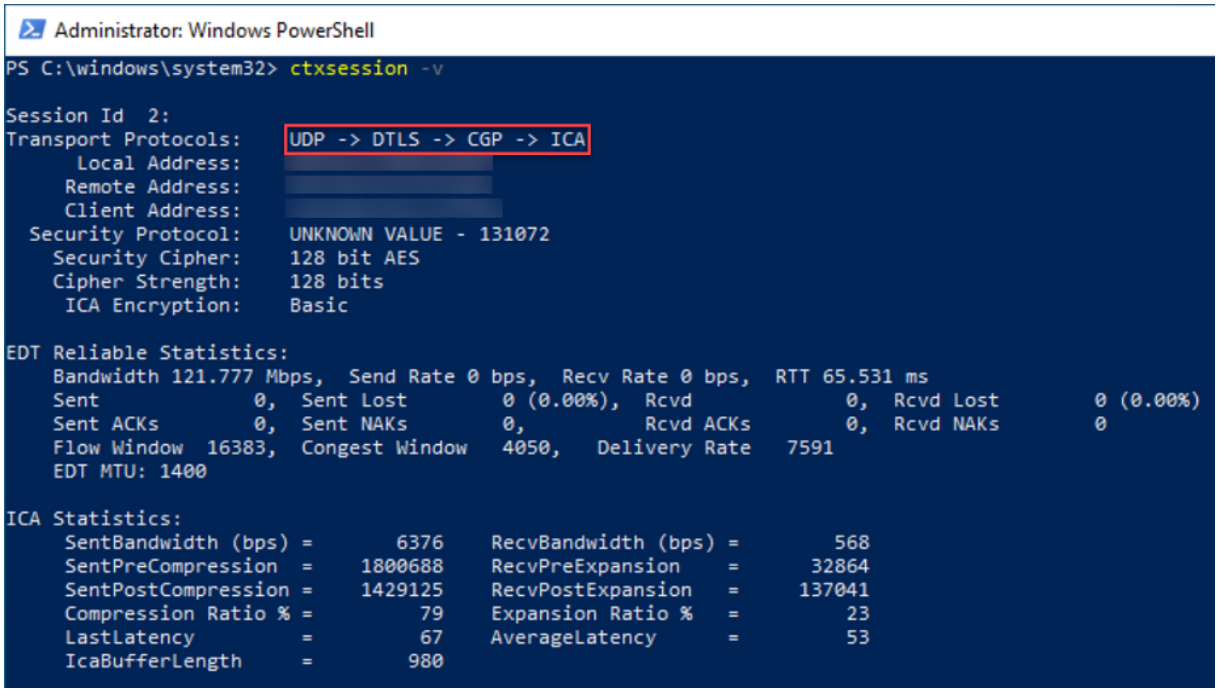
EDT がセッションのトランスポートプロトコルとして使用されていることを確認するために、VDA で Director または`CtxSession.exe`コマンドラインユーティリティを使用できます。

Director でセッションを検索し、［詳細］を選択します。［接続の種類］がHDXで ［プロトコル］がUDPの場合、セッションのトランスポートプロトコルとして EDT が使用されています。



CtxSession.exe ユーティリティを使用するには、セッション内でコマンドプロンプトまたは PowerShell を起動し、`ctxsession.exe`を実行します。詳細な統計を表示するには、`ctxsession.exe -v`を実行します。EDT が使用されている場合、トランスポートプロトコルは次のいずれかを示します:

- **UDP > ICA**（セッション画面の保持が無効）
- **UDP > CGP > ICA**（セッション画面の保持が有効）
- **UDP > DTLS > CGP > ICA**（ICA は DTLS で暗号化されたエンドツーエンド）



EDT でセッションが接続に失敗した場合

アダプティブトランスポートと **EDT** のトラブルシューティングを行うには、次のことをお勧めします:

1. システム要件、ネットワーク要件、既知の問題、および知っておくべきことを確認し、すべての項目に対応していることを確認します。
2. Studio または GPO に Citrix ポリシーがあり、目的の **HDX** アダプティブトランスポート設定を上書きしていないかどうかを確認します。
3. 目的の HDX アダプティブトランスポート設定を上書きする設定がクライアントにあるかどうかを確認します。上書きする設定とは、GPO 設定、オプションの Workspace アプリ管理テンプレートを使用して構成された設定、またはレジストリやクライアントの構成ファイルで手動で構成された **HDXoverUDP** 設定などです。
4. マルチセッション VDA マシンでは、UDP リスナーがアクティブであることを確認してください。VDA マシンでコマンドプロンプトを開き、`netstat -a -p udp`を実行します。詳しくは、「How to Confirm HDX Enlightened Data Transport Protocol」を参照してください。
5. ネットワークファイアウォールと VDA マシンで実行されているファイアウォールの両方で適切なファイアウォール規則が構成されているかどうかを確認します。
6. NetScaler Gateway または Citrix Gateway サービスをバイパスして内部で直接セッションを開始し、使用中のプロトコルを確認します。セッションで EDT を使用する場合、VDA は NetScaler Gateway または Citrix Gateway サービスを介した外部接続に EDT を使用するよう準備しています。
7. EDT が直接の内部接続では機能し、NetScaler Gateway または Citrix Gateway サービスを経由するセッションでは機能しない場合は、次の手順を実行します:

- セッション画面の保持が有効になっていることを確認します。
- NetScaler Gateway を使用する場合は、「Enlightened Data Transport および HDX Insight をサポートするように NetScaler Gateway を構成する」に記載されている必須構成に準拠していることを確認してください。

8. Citrix Gateway サービスを使用している場合は、Rendezvous が有効になっていて動作していることを確認します。
9. ユーザーの接続に非標準の MTU が必要かどうかを確認します。有効 MTU が 1500 バイト未満の接続は、EDT パケットの断片化を引き起こし、パフォーマンスに影響を与えたり、セッションの起動に失敗したりすることがあります。この問題は、VPN、一部の Wi-Fi アクセスポイント、および 4G や 5G などのモバイルネットワークを使用している場合によく発生します。MTU Discovery が有効になっているか、または「標準以外の MTU を持つネットワークで EDT を使用する場合に MSS を構成する方法」で説明されているようにカスタム MTU を設定していることを確認します。

既知の問題

- 非対称ネットワークパスにより、MTU Discovery が、NetScaler Gateway または Citrix Gateway サービスを介さない接続に失敗することがあります。この問題に対処するには、VDA バージョン 2103 以降にアップグレードします。[CVADHELP-16654]
- NetScaler Gateway を使用している場合、非対称ネットワークパスが原因で MTU Discovery が失敗することがあります。これは、Gateway で EDT パケットのヘッダーの Don’t Fragment（DF）ビットが伝播されないことが原因です。この問題の修正は、ファームウェアリリース 13.1 ビルド 17.42 以降で利用できます。修正プログラムを有効にする方法について詳しくは、NetScaler Gatewayのドキュメントを参照してください。[CGOP-18438]
- DS-Lite ネットワークを介して接続するユーザーの場合、MTU Discovery が失敗することがあります。一部のモデムでは、パケット処理が有効になっていると DF ビットを正しく処理できず、MTU Discovery が断片化を検出できなくなります。この状況では、次のオプションを使用できます:
  - ユーザーのモデムでパケット処理を無効にします。
  - **MTU Discovery** を無効にして、「How to configure MSS when using EDT on networks with non-standard MTU」の説明に従ってハードコードされた MTU を使用します。
  - アダプティブトランスポートを無効にして、セッションに TCP の使用を強制します。ユーザーのサブセットのみが影響を受ける場合は、他のユーザーが引き続き EDT を使用できるように、クライアント側でそれを無効にすることを検討してください。

Rendezvous プロトコル

June 9, 2023

Citrix Gateway サービスを使用する場合、Rendezvous プロトコルにより、VDA が Citrix Cloud Connector をバイパスして、Citrix Cloud コントロールプレーンに直接かつ安全に接続できます。

考慮すべきトラフィックには 2 つのタイプがあります:

1. VDA 登録とセッション仲介のための制御用トラフィック。
2. HDX セッショントラフィック。

利用可能な Rendezvous には次の 2 つのバージョンがあります:

- バージョン 1（V1）: HDX セッショントラフィックの場合のみ、Citrix Cloud Connector のバイパスをサポートします。
- バージョン 2 (V2): 制御用トラフィックと HDX セッショントラフィックの両方で、Citrix Cloud Connector のバイパスをサポートします。

各 Rendezvous バージョンのシステム要件、考慮事項、構成について詳しくは、それぞれのドキュメントを確認してください。

Rendezvous V1 のドキュメント

Rendezvous V2 のドキュメント

Rendezvous V1

April 28, 2023

Citrix Gateway サービスを使用する場合、Rendezvous プロトコルにより、VDA が Citrix Cloud Connector をバイパスして、Citrix Cloud コントロールプレーンに直接かつ安全に接続できます。

要件

- Citrix Workspace と Citrix Gateway サービスを使用して環境にアクセスします。
- コントロールプレーン: Citrix DaaS（Citrix Cloud）。
- VDA: バージョン 1912 以降。
  - バージョン 2012 は、EDT Rendezvous に必要な最小バージョンです。
  - バージョン 2012 は、不透明なプロキシサポート（PAC ファイルのサポートなし）に必要な最小バージョンです。
  - バージョン 2103 は、PAC ファイルを使用したプロキシ構成に必要な最小バージョンです。
- Citrix ポリシーで Rendezvous プロトコルを有効にします。詳しくは、「Rendezvous プロトコルポリシー設定」を参照してください。

- VDA は、すべてのサブドメインを含むhttps://*.nssvc.netにアクセスできる必要があります。この方法ですべてのサブドメインを許可リストに登録できない場合、代わりにhttps://*.c.nssvc.netおよびhttps://*.g.nssvc.netを使用します。詳しくは、Citrix Cloud のドキュメント（Citrix DaaS 内）の「インターネット接続の要件」セクションおよび Knowledge Center の記事CTX270584を参照してください。
- VDA は、TCP Rendezvous および EDT Rendezvous のそれぞれについて、TCP 443 および UDP 443 で前述のアドレスに接続できる必要があります。
- Cloud Connector は、セッションを仲介する場合、VDA の FQDN を取得する必要があります。このタスクを完了するには、次の 2 つの方法があります:
  - サイトの **DNS** 解決を有効にします。［完全な構成］**>**［設定］に移動し、［**DNS** 解決を有効にする］設定をオンにします。または、Citrix Virtual Apps and Desktops Remote PowerShell SDK を使用して、コマンドSet-BrokerSite -DnsResolutionEnabled $trueを実行します。Citrix Virtual Apps and Desktops Remote PowerShell SDK について詳しくは、「SDK および API」を参照してください。
  - **VDA** の **PTR** レコードを含む **DNS** 逆引き参照ゾーン。このオプションを選択した場合は、常に PTR レコードの登録を試行するように VDA を構成することをお勧めします。これを行うには、グループポリシーエディターまたはグループポリシーオブジェクトを使用して、［コンピューターの構成］**>**［管理用テンプレート］**>**［ネットワーク］**>**［**DNS** クライアント］に移動し、［**PTR** レコードを登録する］を［有効］および［登録］に設定します。接続の DNS サフィックスがドメインの DNS サフィックスと一致しない場合は、マシンが PTR レコードを正常に登録できるように、［接続固有の **DNS** サフィックス］設定も構成する必要があります。

> 注:
>
> DNS 解決オプションを使用する場合、Cloud Connector で VDA マシンの完全修飾ドメイン名（FQDN）を解決できなければなりません。内部ユーザーが VDA マシンに直接接続する場合、クライアントデバイスも VDA マシンの FQDN を解決できる必要があります。
>
> DNS 逆引き参照ゾーンを使用する場合、PTR レコードの FQDN は VDA マシンの FQDN と一致する必要があります。PTR レコードに別の FQDN が含まれている場合、Rendezvous 接続は失敗します。たとえば、マシンの FQDN がvda01.domain.netの場合、PTR レコードにはvda01.domain.netが含まれている必要があります。vda01.sub.domain.netなどの別の FQDN だと機能しません。

プロキシ構成

VDA は、プロキシを介した Rendezvous 接続の確立をサポートしています。

プロキシに関する考慮事項

Rendezvous でプロキシを使用する場合は、次の点を考慮してください:

- 透過プロキシ、非透過 HTTP プロキシ、および SOCKS5 プロキシがサポートされています。
- パケットの暗号化解除と検査はサポートされていません。VDA と Gateway サービスの間の ICA トラフィックが傍受、暗号化解除、または検査されないように、例外を構成します。例外を構成しないと、接続が切断されます。
- HTTP プロキシは、Negotiate および Kerberos プロトコル、または NT LAN Manager（NTLM）認証プロトコルを使用して、マシンベースの認証をサポートします。

  プロキシサーバーに接続するとき、Negotiate 認証スキームによって Kerberos プロトコルが自動的に選択されます。Kerberos がサポートされていない場合、Negotiate は NTLM 認証にフォールバックします。

  > 注:
  >
  > Kerberos を使用するには、プロキシサーバーのサービスプリンシパル名（SPN）を作成し、それをプロキシの Active Directory アカウントに関連付ける必要があります。VDA は、セッションの確立時に`HTTP/<proxyURL>`形式の SPN を生成します。この場合、プロキシ URL は **Rendezvous** プロキシのポリシー設定から取得されます。SPN を作成しない場合、認証は NTLM にフォールバックします。どちらの場合も、VDA マシンの ID が認証に使用されます。

- SOCKS5 プロキシによる認証は、現在サポートされていません。SOCKS5 プロキシを使用する場合、要件で指定されている Gateway サービスアドレス宛てのトラフィックが認証をバイパスできるように、例外を構成する必要があります。
- EDT を介したデータ転送をサポートしているのは、SOCKS5 プロキシのみです。HTTP プロキシの場合、ICA のトランスポートプロトコルとして TCP を使用します。

透過プロキシ

ネットワークで透過プロキシを使用している場合、VDA で追加の構成は必要ありません。

非透過プロキシ

ネットワークで非透過プロキシを使用している場合は、Rendezvous プロキシの構成の設定を行います。この設定が有効になっている場合、VDA が使用するプロキシを認識できるように、HTTP または SOCKS5 プロキシアドレスを指定するか、PAC ファイルへのパスを入力します。例:

- プロキシアドレス: `http://<URL or IP>:<port>`または`socks5://<URL or IP>:<port>`
- PAC ファイル: `http://<URL or IP>/<path>/<filename>.pac`

PAC ファイルを使用してプロキシを構成する場合は、Windows HTTP サービスに必要な構文を使用してプロキシを定義します：`PROXY [<scheme>=]<URL or IP>:<port>`。例：`PROXY socks5=<URL or IP>:<port>`。

Rendezvous の検証

すべての要件を満たしている場合は、次の手順に従って、Rendezvous が使用されているかを検証します：

1. HDX セッション内で PowerShell またはコマンドプロンプトを起動します。
2. `ctxsession.exe -v`を実行します。
3. 使用中のトランスポートプロトコルは、接続の種類を示しています：
    - TCP Rendezvous：**TCP > SSL > CGP > ICA**
    - EDT Rendezvous：**UDP > DTLS > CGP > ICA**
    - Cloud Connector を介したプロキシ：**TCP > CGP > ICA**

そのほかの考慮事項

Windows の暗号の組み合わせの順序

カスタムの暗号の組み合わせの順序については、VDA でサポートされている暗号の組み合わせが含まれていることを次のリストから確認してください：

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

カスタムの暗号の組み合わせの順序にこれらの暗号の組み合わせが含まれていない場合、Rendezvous 接続は失敗します。

Zscaler Private Access

Zscaler Private Access（ZPA）を使用している場合は、Gateway サービスのバイパス設定を構成して、遅延の増加とそれに伴うパフォーマンスへの影響を回避することをお勧めします。これを行うには、要件で指定されている Gateway サービスアドレスのアプリケーションセグメントを定義し、それらを常にバイパスするように設定する必要があります。ZPA をバイパスするようにアプリケーションセグメントを構成する方法については、Zscaler のマニュアルを参照してください。

Rendezvous V2

May 17, 2024

Citrix Gateway サービスを使用する場合、Rendezvous プロトコルにより、VDA が Citrix Cloud Connector をバイパスして、Citrix Cloud コントロールプレーンに直接かつ安全に接続できます。

Rendezvous V2 は、標準のドメイン参加マシン、ハイブリッド Azure AD 参加マシン、Azure AD 参加マシン、非ドメイン参加マシンでサポートされています。

> 注:
>
> 現時点では、_Azure AD 参加済み _ マシン、および _ ドメイン非参加 _ マシンでのみ、コネクタを使用しない展開が可能です。標準の AD ドメイン参加済みマシンおよびハイブリッド Azure AD 参加マシンでも、VDA 登録とセッション仲介には Cloud Connector が必要です。ただし、Rendezvous V2 を使用するための DNS 要件はありません。
>
> オンプレミス AD ドメインへの接続、オンプレミスハイパーバイザーへの MCS プロビジョニングなど、VDA 通信に関連しないほかの機能についての Cloud Connector の要件に変更はありません。

要件

Rendezvous V2 を使用するための要件は次のとおりです:

- Citrix Workspace と Citrix Gateway サービスを使用した環境へのアクセス
- コントロールプレーン: Citrix DaaS
- VDA バージョン 2203
- Citrix ポリシーで Rendezvous プロトコルを有効にします。詳しくは、「Rendezvous プロトコルポリシー設定」を参照してください。
- VDA でセッションの信頼性を有効にする必要があります。
- VDA マシンは、以下にアクセスできる必要があります:
  - TCP 443での`https://*.xendesktop.net`。この方法ですべてのサブドメインを許可できない場合は、`https://<customer_ID>.xendesktop.net`を使用できます。<customer_ID> は、Citrix Cloud 管理者ポータルに表示される Citrix Cloud 顧客 ID です。
  - Gateway サービスとの制御接続用の、TCP 443での`https://*.*.nssvc.net`。
  - TCP および EDT を介した HDX セッションには、それぞれTCP 443およびUDP 443での`https://*.*.nssvc.net`。

> 注:
>
> `https://*.*.nssvc.net`を使用してすべてのサブドメインを許可できない場合、代わりに`https://*.c.nssvc.net`および`https://*.g.nssvc.net`を使用します。詳しくは、Knowledge Center のCTX270584を参照してください。

プロキシ構成

VDA は、Rendezvous を使用する場合、制御用トラフィックと HDX セッショントラフィックの両方のプロキシを介した接続をサポートします。どちらのタイプのトラフィックも要件と考慮事項が異なるため、慎重に確認してください。

制御用トラフィックプロキシの考慮事項

- HTTP プロキシのみがサポートされています。
- パケットの暗号化解除と検査はサポートされていません。VDA と Citrix Cloud コントロールプレーンの間の制御用トラフィックが傍受、暗号化解除、または検査されないように、例外を構成します。信頼済みの証明書が見つからない場合は、失敗します。
- プロキシ認証はサポートされていません。

HDX トラフィックプロキシの考慮事項

- HTTP および SOCKS5 プロキシがサポートされています。
- EDT は、SOCKS5 プロキシでのみ使用できます。
- デフォルトでは、HDX トラフィックは制御用トラフィック対して定義されたプロキシを使用します。HDX トラフィックに別のプロキシを使用する必要がある場合、別の HTTP プロキシ、SOCKS5 プロキシを問わず、Rendezvous プロキシの構成ポリシー設定を使用します。
- パケットの暗号化解除と検査はサポートされていません。VDA と Citrix Cloud コントロールプレーンの間の HDX トラフィックが傍受、暗号化解除、または検査されないように、例外を構成します。信頼済みの証明書が見つからない場合は、失敗します。
- マシンベースの認証は、HTTP プロキシでのみ、かつ VDA マシンが AD ドメインに参加している場合にサポートされます。Negotiate/Kerberos、または NTLM 認証を使用できます。

  > 注:
  >
  > Kerberos を使用するには、プロキシサーバーのサービスプリンシパル名（SPN）を作成し、それをプロキシの Active Directory アカウントに関連付けます。VDA は、セッションの確立時にHTTP/<proxyURL>形式の SPN を生成します。この場合、プロキシ URL はRendezvous プロキシの構成ポリシー設定から取得されます。SPN を作成しない場合、認証は NTLM にフォールバックします。どち

> らの場合も、VDA マシンの ID が認証に使用されます。

- SOCKS5 プロキシによる認証は、現在サポートされていません。SOCKS5 プロキシを使用する場合、要件で指定されている Gateway サービスアドレス宛てのトラフィックが認証をバイパスできるように、例外を構成します。
- EDT を介したデータ転送をサポートしているのは、SOCKS5 プロキシのみです。HTTP プロキシの場合、ICA のトランスポートプロトコルとして TCP を使用します。

透過プロキシ

ネットワークで透過プロキシを使用している場合、VDA で追加の構成は必要ありません。

非透過プロキシ

ネットワークで非透過プロキシを使用している場合は、VDA のインストール中にプロキシを指定して、制御用トラフィックが Citrix Cloud コントロールプレーンに到達できるようにします。インストールと構成を始める前に、制御用トラフィックプロキシの考慮事項を確認してください。

VDA インストールウィザードで、［追加コンポーネント］ページの ［**Rendezvous** プロキシの構成］を選択します。このオプションを使用すると、後ほどインストールウィザードにて ［**Rendezvous** プロキシの構成］ページを使用できるようになります。ここで、使用するプロキシを VDA が認識できるようにプロキシアドレスまたは PAC ファイルのパスを入力します。例:

- プロキシアドレス: `http://<URL or IP>:<port>`
- PAC ファイル: `http://<URL or IP>/<path/<filename>.pac`

HDX トラフィックプロキシの考慮事項に記載されているように、HDX トラフィックは、VDA のインストール中に定義されたプロキシをデフォルトで使用します。HDX トラフィックに別のプロキシを使用する必要がある場合、別の HTTP プロキシ、SOCKS5 プロキシを問わず、Rendezvous プロキシの構成ポリシー設定を使用します。この設定が有効になっている場合、HTTP または SOCKS5 プロキシアドレスを指定します。また、PAC ファイルのパスを入力して、使用するプロキシを VDA が認識できるようにすることもできます。例:

- プロキシアドレス: `http://<URL or IP>:<port>` または `socks5://<URL or IP>:<port>`
- PAC ファイル: `http://<URL or IP>/<path/<filename>.pac`

PAC ファイルを使用してプロキシを構成する場合は、Windows HTTP サービスに必要な構文を使用してプロキシを定義します: `PROXY [<scheme>=]<URL or IP>:<port>`。例: `PROXY socks5=<URL or IP>:<port>`.

Rendezvous の構成方法

以下は、ご使用の環境で Rendezvous を構成するための手順です:

1. すべての要件が満たされているか確認してください。
2. ご使用の環境で非透過 HTTP プロキシを使用する必要がある場合は、VDA のインストール中に構成してください。詳しくは、「プロキシ構成」セクションを参照してください。
3. インストールが完了したら、VDA マシンを再起動します。
4. Citrix ポリシーを作成するか、既存のポリシーを編集します:
    - **Rendezvous** プロトコル設定を ［許可］に設定します。
    - HDX トラフィックに対して HTTP プロキシまたは SOCKS5 プロキシを構成する必要がある場合は、［**Rendezvous** プロキシの構成］設定を構成します。
    - Citrix ポリシーフィルターが正しく設定されていることを確認します。このポリシーは、Rendezvous を有効にする必要があるマシンに適用されます。
5. 別のポリシーを上書きしないように、Citrix ポリシーの優先度が正しいことを確認してください。

> 注:
>
> VDA バージョン 2308 以前を使用している場合は、デフォルトで V1 が使用されます。使用するバージョンを構成する方法については、「レジストリで管理される HDX 機能」を参照してください。

Rendezvous の検証

すべての要件を満たし、構成が完了したら、次の手順に従って、Rendezvous が使用されているかどうかを検証します:

1. 仮想デスクトップ内で、コマンドプロンプトまたは PowerShell を開きます。
2. `ctxsession.exe -v`を実行します。
3. 表示されるトランスポートプロトコルは、接続の種類を示しています:
    - TCP Rendezvous：TCP > SSL > CGP > ICA
    - EDT Rendezvous：UDP > DTLS > CGP > ICA
    - Rendezvous ではない：TCP > CGP > ICA
4. 報告された Rendezvous のバージョンが、使用中のバージョンです。

そのほかの考慮事項

Windows の暗号の組み合わせの順序

VDA マシンで暗号の組み合わせの順序が変更されている場合は、VDA でサポートされている暗号の組み合わせを追加してください:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

カスタムの暗号の組み合わせの順序にこれらの暗号の組み合わせが含まれていない場合、Rendezvous 接続は失敗します。

Zscaler Private Access

Zscaler Private Access（ZPA）を使用している場合は、Gateway サービスのバイパス設定を構成して、遅延の増加とそれに伴うパフォーマンスへの影響を回避することをお勧めします。これを行うには、要件で指定されている Gateway サービスアドレスのアプリケーションセグメントを定義し、それらを常にバイパスするように設定する必要があります。ZPA をバイパスするようにアプリケーションセグメントを構成する方法については、Zscaler のマニュアルを参照してください。

既知の問題

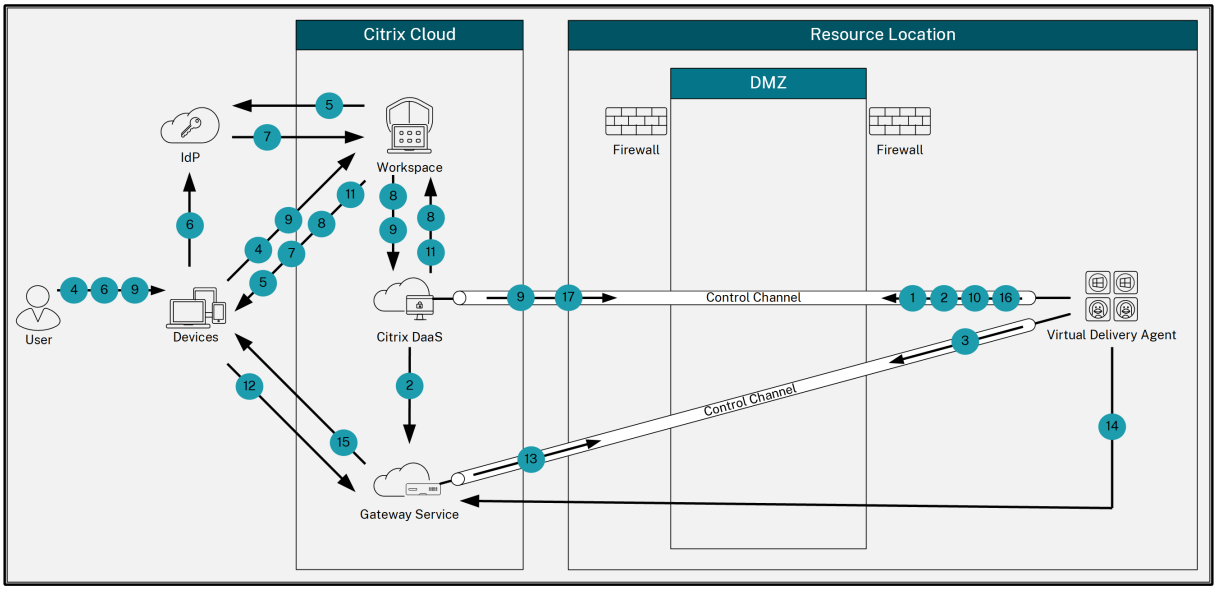
VDA 2203 インストーラーでプロキシアドレスに対してスラッシュ（/）を入力できない

回避策として、VDA のインストール後にレジストリでプロキシを構成できます:

```
Key: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent
Value type: String
Value name: ProxySettings
Value data: Proxy address or path to pac file. For example:
    Proxy address: http://squidk.test.local:3128
    Pac file: http://file.test.com/config/proxy.pac
```

Rendezvous トラフィックフロー

次の図は、Rendezvous のトラフィックフローに関する一連の手順を示しています。



1. VDA は、Citrix Cloud との WebSocket 接続を確立し、登録します。
2. VDA は Citrix Gateway サービスに登録し、専用のトークンを取得します。
3. VDA は、Gateway サービスとの永続的な制御接続を確立します。
4. ユーザーは Citrix Workspace に移動します。
5. Workspace は認証構成を評価し、認証のためにユーザーを適切な ID プロバイダーにリダイレクトします。
6. ユーザーは自分の資格情報を入力します。
7. ユーザーの資格情報が正常に検証された後、ユーザーは Workspace にリダイレクトされます。
8. Workspace はユーザーのリソースをカウントして表示します。
9. ユーザーは、Workspace からデスクトップまたはアプリケーションを選択します。Workspace は要求を Citrix DaaS に送信し、Citrix DaaS は接続を仲介し、VDA にセッションの準備を指示します。
10. VDA は、Rendezvous 機能とその ID で応答します。
11. Citrix DaaS は起動チケットを生成し、Workspace 経由でユーザーデバイスに送信します。
12. ユーザーのエンドポイントは Gateway サービスに接続し、接続するリソースを認証および識別するための起動チケットを提供します。
13. Gateway サービスは、接続情報を VDA に送信します。
14. VDA は、Gateway サービスへの直接接続を確立します。
15. Gateway サービスは、エンドポイントと VDA 間の接続を完了します。
16. VDA は、セッションのライセンスを検証します。
17. Citrix DaaS は、適用するポリシーを VDA に送信します。

HDX Direct（Technical Preview）

June 12, 2024

Citrix が提供するリソースにアクセスする場合、HDX Direct を使用すると、内部および外部の両方のクライアントデバイスはセッションホストとのセキュアな直接接続を確立できます（直接通信が可能な場合）。

> 重要：
>
> HDX Direct は現在、Technical Preview 段階にあります。この機能はサポートなしで提供されているため、運用環境での使用はまだ推奨されていません。フィードバックを送信したり、問題を報告したりする場合は、このフォームを使用してください。

システム要件

HDX Direct を使用するためのシステム要件は次のとおりです：

- コントロールプレーン
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2402 以降
- Virtual Delivery Agent（VDA）
  - Windows：バージョン 2402 以降
- Workspace アプリ
  - Windows：バージョン 2402 以降
- アクセス層
  - Citrix Workspace（Citrix Gateway Service 使用）
  - Citrix Workspace（NetScaler Gateway 使用）
- その他
  - 外部直接接続に対してアダプティブトランスポートを有効にする必要がある

ネットワークの要件

HDX Direct を使用するためのネットワーク要件は次のとおりです：

セッションホスト

セッションホストに Windows Defender ファイアウォールなどのファイアウォールがある場合は、内部接続に対して次の受信トラフィックを許可する必要があります。

説明	接続元	プロトコル	ポート
内部直接接続	クライアント	TCP	443
内部直接接続	クライアント	UDP	443

> 注:
>
> VDA インストーラーは、適切な受信規則を Windows Defender ファイアウォールに追加します。別のファイアウォールを使用する場合は、上記の規則を追加する必要があります。

クライアント側ネットワーク

次の表に、内部ユーザーと外部ユーザーのクライアントネットワークを示します。

内部ユーザー

説明	プロトコル	接続元	送信元ポート	接続先	接続先ポート
内部直接接続	TCP	クライアント側ネットワーク	1024～65535	VDA ネットワーク	443
内部直接接続	UDP	クライアント側ネットワーク	1024～65535	VDA ネットワーク	443

外部ユーザー

説明	プロトコル	接続元	送信元ポート	接続先	接続先ポート
STUN（外部ユーザーのみ）	UDP	クライアント側ネットワーク	1024～65535	インターネット（下記の注を参照）	3478、19302
外部ユーザー接続	UDP	クライアント側ネットワーク	1024～65535	データセンターのパブリック IP アドレス	1024～65535

データセンターネットワーク

次の表に、内部ユーザーと外部ユーザーのデータセンターネットワークを示します。

内部ユーザー

説明	プロトコル	接続元	送信元ポート	接続先	接続先ポート
内部直接接続	TCP	クライアント側ネットワーク	1024～65535	VDA ネットワーク	443
内部直接接続	UDP	クライアント側ネットワーク	1024～65535	VDA ネットワーク	443

外部ユーザー

説明	プロトコル	接続元	送信元ポート	接続先	接続先ポート
STUN（外部ユーザーのみ）	UDP	VDA ネットワーク	1024～65535	インターネット（下記の注を参照）	3478、19302
外部ユーザー接続	UDP	DMZ/内部ネットワーク	1024～65535	VDA ネットワーク	55000～55250
外部ユーザー接続	UDP	VDA ネットワーク	55000～55250	クライアントのパブリック IP	1024～65535

> 注:
>
> VDA と Workspace アプリは両方とも、STUN 要求を以下のサーバーにこの順序で送信しようとします:
>
> - stunserver.stunprotocol.org:3478
> - employees.org:3478
> - stun.l.google.com:19302
>
> [**HDX Direct** のポート範囲] ポリシー設定を使用して外部ユーザー接続のデフォルトのポート範囲を変更する場合、カスタムポート範囲が対応するファイアウォール規則を満たしている必要があります。

構成

デフォルトでは、HDX Direct は無効になっています。この機能を構成するには、Citrix ポリシーの [**HDX Direct**] 設定を使用します。

- **HDX Direct**: 機能を有効または無効にします。
- **HDX Direct** モード: **HDX Direct** を内部クライアントのみで使用可能にするか、内部クライアントと外部クライアントの両方で使用可能にするかを設定します。
- **HDX Direct** のポート範囲: VDA が外部クライアントからの接続に使用するポート範囲を定義します。

注意事項

HDX Direct を使用するための注意事項は次のとおりです:

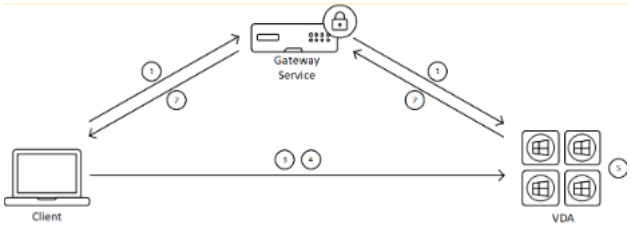
- HDX Direct を外部ユーザーが使用できるようにするには、トランスポートプロトコルとして EDT（UDP）を使用する必要があります。このため、［アダプティブトランスポート］を有効にする必要があります。
- **HDX Insight** を使用している場合は、**HDX Direct** を使用すると、セッションが NetScaler Gateway の仲介によるアクセス対象にされなくなるため、HDX Insight のデータ収集が妨げられることに注意してください。
- Virtual Apps and Desktops に非永続マシンを使用する場合、各マシンが独自の証明書を生成できるように、**HDX Direct** をマスター/テンプレートイメージ内ではなくセッションホスト上で有効にすることをお勧めします。
- HDX Direct での独自の証明書の使用は現在サポートされていません。

機能

HDX Direct を使用すると、直接通信が利用できる場合、クライアントはセッションホストへの直接接続を確立できます。HDX Direct で直接接続を行うと、自己署名証明書により、ネットワークレベルの暗号化（TLS/DTLS）で直接接続が保護されます。

内部ユーザー

次の図は、内部ユーザーの HDX Direct 接続プロセスの概要を示しています。

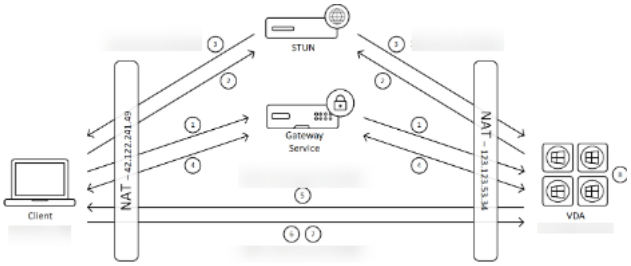


1. クライアントは、Gateway Service を通じて HDX セッションを確立しようとします。
2. 接続が成功すると、VDA は、VDA マシンの FQDN、その IP アドレスの一覧、および VDA マシンの証明書を HDX 接続経由でクライアントに送信します。
3. クライアントは IP アドレスをプローブして、VDA に直接アクセスできるかどうかを確認します。
4. クライアントは共有 IP アドレスのいずれかを使用して VDA に直接接続できる場合、手順（2）で交換した証明書と一致する証明書を使用して、（D）TLS で保護された、VDA との直接接続を確立しようとします。
5. 直接接続が正常に確立されると、セッションが新しい接続に転送されるので、Gateway Service への接続は終了します。

> 注:
>
> 上記の手順 2 で接続が確立されると、セッションがアクティブになります。後続の手順を実行しても、仮想アプリケーションまたはデスクトップを使用しようとする場合に遅延や妨害が生じることはありません。後続の手順のいずれかが失敗した場合でも、Gateway を介した接続はユーザーのセッションを中断することなく維持されます。

外部ユーザー

次の図は、外部ユーザーの HDX Direct 接続プロセスの概要を示しています:



1. クライアントは、Gateway Service を通じて HDX セッションを確立しようとします。
2. 接続が成功すると、クライアントと VDA の両方がパブリックな IP アドレスとポートを検出するための STUN 要求を送信します。
3. STUN サーバーは、対応するパブリックな IP アドレスとポートを使用してクライアントと VDA に応答します。
4. HDX 接続を通じて、クライアントと VDA はパブリックな IP アドレスと UDP ポートを交換し、VDA は証明書をクライアントに送信します。
5. VDA は、クライアントのパブリックな IP アドレスと UDP ポートに UDP パケットを送信します。クライアントは、UDP パケットを VDA のパブリックな IP アドレスと UDP ポートに送信します。
6. クライアントは VDA からメッセージを受信すると、セキュリティで保護された接続の要求で応答します。
7. DTLS ハンドシェイク中に、クライアントは証明書が手順（4）で交換された証明書と一致するかどうかを検証します。検証後、クライアントは承認トークンを送信します。これで、セキュリティで保護された直接接続が確立されました。
8. 直接接続が正常に確立されると、セッションが新しい接続に転送されるので、Gateway Service への接続は終了します。

> 注:
>
> 上記の手順 2 で接続が確立されると、セッションがアクティブになります。後続の手順を実行しても、仮想アプリケーションまたはデスクトップを使用しようとする場合に遅延や妨害が生じることはありません。後続の手順のいずれかが失敗した場合でも、Gateway を介した接続はユーザーのセッションを中断することなく維持されます。

証明書管理

セッションホスト

VDA マシン上の次の 2 つのサービスは証明書の作成と管理を処理します。どちらのサービスもマシンの起動時に自動的に実行されるように設定されています:

- Citrix ClxMtp サービス: CA 証明書キーを生成・ローテーションします。
- Citrix Certificate Manager サービス: 自己署名のルート CA 証明書とマシン証明書を生成・管理します。

次の手順は、証明書管理プロセスを示しています:

1. サービスは、マシンの起動時に開始されます。
2. キーがまだ作成されていない場合、`Citrix ClxMtp Service`によってキーが作成されます。
3. Citrix Certificate Manager サービスは、**HDX Direct** が有効になっているかどうかを確認します。有効になっていない場合、サービスは自動的に停止します。
4. **HDX Direct** が有効になっている場合、Citrix Certificate Manager サービスは、自己署名のルート CA 証明書が存在するかどうかをチェックします。存在しない場合は、自己署名のルート証明書が作成されます。
5. ルート CA 証明書が使用できるようになると、Citrix Certificate Manager サービスは、自己署名のマシン証明書が存在するかを確認します。存在しない場合は、サービスはキーを生成し、マシンの FQDN を使用して新しい証明書を作成します。
6. Citrix Certificate Manager サービスによって作成された既存のマシン証明書があり、サブジェクト名がマシンの FQDN と一致しない場合、新しい証明書が生成されます。

> 注:
>
> Citrix Certificate Manager サービスは、2048 ビットキーを利用する RSA 証明書を生成します。

クライアントデバイス

セキュリティで保護された **HDX Direct** 接続の確立を成功させるには、クライアントはセッションの保護に使用される証明書を信頼できる必要があります。そのため、クライアントは ICA ファイル（Workspace によって提供される）を使用してセッションの CA 証明書を受信します。したがって、CA 証明書をクライアントデバイスの証明書ストアに配布する必要はありません。

NAT の互換性

June 12, 2024

外部ユーザーのデバイスとセッションホスト間の直接接続を確立するために、HDX Direct は STUN と NAT トラバーサルのホールパンチングを利用して、クライアントデバイスとセッションホストの間でパブリックな IP アドレス

とポートのマッピングを交換できるようにします。これは、VoIP、統合コミュニケーション、P2P ソリューションの仕組みと似ています。

ファイアウォールおよびその他のネットワークコンポーネントが HDX セッションおよび STUN 要求の UDP トラフィックを許可するように構成されている限り、外部ユーザー向けの HDX Direct は機能することが期待できます。ただし、ユーザーネットワークの NAT タイプとセッションホストネットワークの NAT タイプに互換性がない場合に HDX Direct が失敗する場合もあります。

検証

クライアントの NAT タイプとセッションホストの NAT タイプを検証するには、STUNTMAN の STUN クライアントユーティリティを使用します:

1. ターゲットプラットフォームに適切なパッケージを stunprotocol.org からダウンロードし、内容を抽出します。
2. コマンドウィンドウを開き、内容が抽出されたディレクトリに移動します。
3. 次のコマンドを実行します:
   ```
   .\stunclient.exe stunserver.stunprotocol.org --mode behavior
   ```
4. 出力をメモします。

バインドテストと動作テストが成功した場合、**binding test** と **behavior test** の両方によって成功が報告され、NAT の動作が指定されます:

テストが失敗した場合、**binding test** と **behavior test** の両方によって失敗が報告されます。

次の表を参照すると、外部ユーザー向けの HDX Direct が動作することを期待できるかどうかを、クライアントテストとセッションホストテストの両方の結果に基づいて判断することができます:

クライアントデバイス	セッションホスト	機能しますか?
エンドポイントに依存しないマッピング	エンドポイントに依存しないマッピング	はい
エンドポイントに依存しないマッピング	エンドポイントに依存したマッピング	はい
エンドポイントに依存したマッピング	エンドポイントに依存しないマッピング	はい

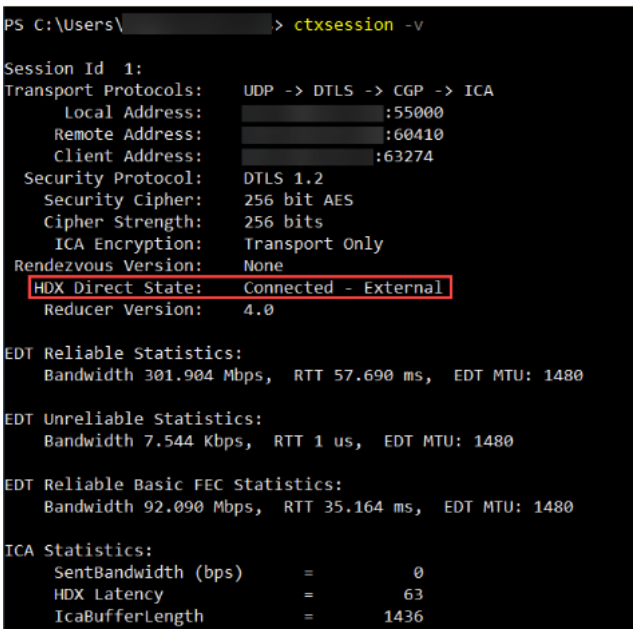
クライアントデバイス	セッションホスト	機能しますか?
エンドポイントに依存したマッピング	エンドポイントに依存したマッピング	いいえ
アドレスとポートに依存したマッピング	任意の NAT タイプ	いいえ
任意の NAT タイプ	アドレスとポートに依存したマッピング	いいえ
失敗	任意の NAT タイプ	いいえ
任意の NAT タイプ	失敗	いいえ
失敗	失敗	いいえ

トラブルシューティング

January 25, 2024

HDX Direct が直接接続の確立に成功したことを確認するには、VDA マシンで`CtxSession.exe`ユーティリティを使用します。

`CtxSession.exe`ユーティリティを使用するには、セッション内でコマンドプロンプトまたは PowerShell を起動し、`ctxsession.exe -v`を実行します。**HDX Direct** 接続の確立が成功した場合、［**HDX Direct Status**］が`Connected`と表示されます。



HDX Direct 接続の確立が成功したか失敗したかを確認する別の方法としては、セッションホストのイベントログを確認するという方法もあります。詳しくは、「イベントログ」セクションを参照してください。

> 注:
>
> セッションホストで使用できる IP アドレスの数と環境によっては、HDX Direct 接続が確立されるまでに最大 5 分かかる場合があります。

HDX Direct が直接接続を確立できない場合

HDX Direct が直接接続を確立できない場合は、次の手順を確認してください:

1. 使用している VDA のバージョンと Workspace アプリのバージョンがシステム要件に応じた機能をサポートしていることを確認します。
2. HDX Direct を有効にするポリシーが VDA に適用されていること、およびこの機能を無効にする優先度の高いポリシーが他にないことを確認します。
3. 必要な HDX Direct モードを設定するポリシーが VDA に適用されていること、および構成を上書きする優先度の高いポリシーが他にないことを確認します。
4. Citrix ClxMtp サービスがセッションホストで実行されていることを確認します。
5. Citrix Certificate Manager サービスがセッションホストで実行されていることを確認します。実行されていない場合は、手動で開始してください。HDX Direct を無効にすると、このサービスは自動的に停止します。
6. セッションホストに自己署名のルート CA 証明書があるかどうかを確認します:
    a) 発行先:`CA-<hostname>`(例:CA-FTLW11-001)
    b) 発行者:`CA-<hostname>`(例:CA-FTLW11-001)
    c) 発行者の詳細:Citrix Systems, Inc.(組織名)
7. セッションホストに自己署名のサーバー証明書があるかどうかを確認します:
    a) 発行先:`<host FQDN>`(例:FTLW11-001.ctxlab.net)
    b) 発行者:`CA-<hostname>`(例:CA-FTLW11-001)
    c) 発行者の詳細:Citrix Systems, Inc.(組織名)
8. 証明書が見つからない場合は、Citrix 技術サポートにお問い合わせください。
9. 証明書が存在する場合:
    a) セッションホストで実行されている Citrix Certificate Manager サービスを停止します。
    b) 自己署名のルート CA 証明書と自己署名のサーバー証明書を両方とも削除します。
    c) セッションホストで Citrix Certificate Manager サービスを開始します。本サービスは開始されると新しい証明書を作成します。
10. 内部ユーザーの場合:
    a) セッションホストのファイアウォールが、HDX over EDT および HDX over TCP の TCP 443 または UDP 443 での受信トラフィックをブロックしていないことを確認します。

b) ネットワークファイアウォールが、クライアントのネットワークとセッションホストのネットワーク間の UDP 443 および TCP 443 のトラフィックをブロックしていないことを確認します。

11. 外部ユーザーの場合:

a) クライアントの NAT タイプとセッションホストの NAT タイプを確認し、これらのの NAT タイプの組み合わせが正常に機能することを確認します。詳しくは、「NAT の互換性」セクションを参照してください。

b) クライアントまたはセッションホストのいずれかで NAT のテストが失敗した場合:

i. ファイアウォールがシステムで実行されている場合は、UDP 3478 の送信トラフィックをブロックしていないことを確認します。

ii. ネットワークファイアウォールが UDP 3478 の送信トラフィックをブロックしていないことを確認します。

iii. ファイアウォールが STUN サーバーの応答をブロックしていないことを確認します。

c) ネットワークファイアウォールに、必要なトラフィックをすべて許可する適切な規則が構成されていることを確認します。詳しくは、「ネットワーク要件」セクションを参照してください。

d) [HDX Direct のポート範囲] ポリシー設定を使用してデフォルトのポート範囲を変更する場合は、カスタムポート範囲に対してファイアウォール規則が設定されていることを確認します。

イベントログ

VDA マシンのイベントログに記録されるイベントは、次のとおりです:

ログ	ID	接続元	レベル	説明
[アプリケーションとサービスログ] > [Citrix-HostCore-HDX Direct/Operational]	1	HDX Direct	情報	内部ユーザー <username> の HDX Direct 接続が確立されました。
[アプリケーションとサービスログ] > [Citrix-HostCore-HDX Direct/Operational]	2	HDX Direct	情報	外部ユーザー <username> の HDX Direct 接続が確立されました。

ログ	ID	接続元	レベル	説明
[アプリケーションとサービスログ] > [Citrix-HostCore-HDX Direct/Operational]	3	HDX Direct	情報	ユーザー<username>のHDX Direct 接続に失敗しました。

既知の問題

HDX Direct が既に有効になっているマシンで VDA のインプレースアップグレードを実行すると、**HDX Direct** が動作しなくなる場合があります。
この問題を解決するには、次の手順を実行します:

1. セッションホストで実行されている Citrix Certificate Manager サービスを停止します。
2. 自己署名のルート CA 証明書と自己署名のサーバー証明書を削除します。
3. レジストリを開きます。
4. `HKLM\Software\Citrix\HDX-Direct`キーを削除します。
5. `HKLM\SYSTEM\CurrentControlSet\Control\TerminalServer\Wds\icawd`に 移動します。
6. **SSLEnabled** 値を`0`に設定します。
7. **SSLThumbprint** 値の内容を削除します。
8. **Citrix Certificate Manager** サービスを開始します。

Secure HDX（Technical Preview）

June 12, 2024

Secure HDX は、トラフィックパス内のネットワーク要素が HDX トラフィックを検査できないようにするアプリケーションレベルの暗号化（ALE）ソリューションです。これは、AES-256-GCM 暗号化を使用して、Citrix Workspace アプリ（クライアント）と VDA（セッションホスト）間のアプリケーションレベルで真のエンドツーエンド暗号化（E2EE）を提供することで実現します。

> 重要:
>
> Secure HDX は現在、Technical Preview 段階にあります。この機能はサポートなしで提供されているため、運用環境での使用はまだ推奨されていません。フィードバックを送信したり、問題を報告したりする場合は、このフォームを使用してください。

システム要件

Secure HDX を使用するためのシステム要件は次のとおりです。

- コントロールプレーン
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2402 以降
- Virtual Delivery Agent（VDA）
  - Windows：バージョン 2402 以降
- Workspace アプリ
  - Windows：バージョン 2402 以降
- アクセス層
  - Citrix Workspace
  - Citrix StoreFront 2402 以降

構成

デフォルトでは、Secure HDX は無効になっています。この機能は、Citrix ポリシーの Secure HDX 設定を使用して構成できます：

Secure HDX：機能をすべてのセッションに対して有効にするか、直接接続に対してのみ有効にするか、無効にするかを定義します。

注意事項

Secure HDX を使用するための注意事項は次のとおりです：

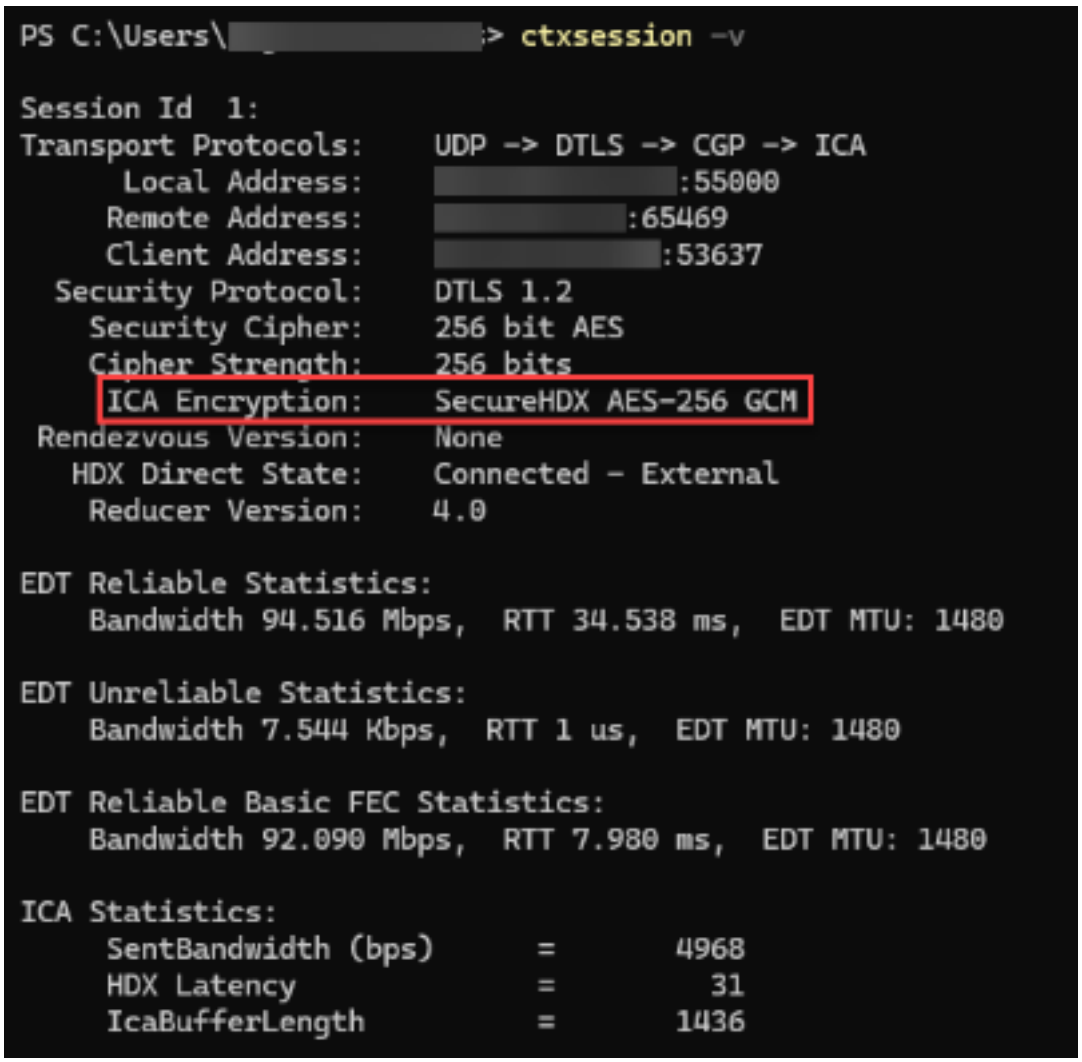
- ユーザーが、機能をサポートしていないクライアントを使用して、Secure HDX が有効になっているセッションホストに接続しようとすると、接続は拒否されます。
- HDX Insight を使用する場合、NetScaler は暗号化された HDX トラフィックを検査できないため、Secure HDX を使用すると HDX Insight データの収集が妨げられることに注意してください。HDX Insight を使用する必要がある場合は、直接接続に対してのみ Secure HDX を有効にするように設定できます。
- サービス継続性は現在、Secure HDX ではサポートされていません。Citrix Cloud 環境でサービス継続性を有効にしている場合、クラウドサービスが停止すると、Secure HDX が有効になっているセッションホストに接続できなくなる可能性があります。

- SmartControl を使用する場合、Secure HDX を使用すると、NetScaler が暗号化された HDX トラフィックを検査できないため、SmartControl が機能しなくなることに注意してください。SmartControl を使用する必要がある場合は、直接接続に対してのみ Secure HDX を有効にするように設定できます。
- Secure HDX が有効になっている場合、マルチストリーム ICA はサポートされません。
- HDX トラフィックの検査に依存するサードパーティソリューションを使用している場合、HDX トラフィックは暗号化されているため、Secure HDX を有効にするとそれらのソリューションは機能しなくなります。

トラブルシューティング

Secure HDX がアクティブであることを確認するには、VDA マシンで `ctxsession.exe`ユーティリティを使用できます。

`CtxSession.exe`ユーティリティを使用するには、セッション内でコマンドプロンプトまたは PowerShell を開き、`ctxsession.exe -v`を実行します。Secure HDX が使用されている場合、ICA 暗号化には`SecureHDX AES-256 GCM`が表示されます。



セッションで **Secure HDX** が有効にならない場合

- 使用中の VDA のバージョンがシステム要件に応じた機能をサポートしていることを確認します。
- Secure HDX を有効にするポリシーが VDA に適用されていること、およびこの機能を無効にする優先度の高いポリシーが他にないことを確認します。
- クライアントデバイスが NetScaler Gateway または Gateway Service 経由で接続している場合は、Secure HDX が「直接接続のみ」に設定されていないことを確認してください。
- Secure HDX を構成したときにセッションホストが既に実行されていた場合は、変更を有効にするためにマシンを再起動します。

仮想チャネルの許可リスト

May 17, 2024

仮想チャネル許可リストは、環境内で許可される Citrix 以外の仮想チャネルを制御できる機能です。デフォルトでは、仮想チャネル許可リスト機能が有効になっています。その結果、Citrix 仮想チャネルのみが Citrix Virtual Apps and Desktops セッションで開けるようになっています。自社製、サードパーティ製を問わず、カスタム仮想チャネルを使用する必要がある場合は、これらを許可リストに明示的に追加する必要があります。

構成

仮想チャネル許可リストがデフォルトで有効になっています。この機能は、Citrix ポリシーの次の設定を使用して構成できます:

- 仮想チャネル許可リスト：機能を有効または無効にし、仮想チャネルをリストに追加します。
- 仮想チャネルの許可リストのログ調整：仮想チャネル許可リストのイベント ログの調整期間を設定します。
- 仮想チャネル許可リストのログ：仮想チャネル許可リストのログレベルを設定します。

許可リストへの仮想チャネルの追加

仮想チャネルを許可リストに追加するには、次の情報が必要です:

1. コードで定義されている仮想チャネル名。最大 7 文字の長さにすることができます。例：`CTXCVC1`。
2. VDA マシンで仮想チャネルを開くプロセスのパス。例：`C:\Program Files\Application\run.exe`。

必要な情報を取得したら、仮想チャネルの許可リストポリシー設定を使用して、仮想チャネルを許可リストに追加する必要があります。仮想チャネルをリストに追加するには、仮想チャネル名のあとにコンマを入力してから、その仮想チャネルにアクセスするプロセスへのパスを入力します。プロセスが複数ある場合は、各プロセスをコンマで区切って追加できます。

単一プロセスの場合

前の例を使用して、以下のエントリをリストに追加します:

```
CTXCVC1,C:\Program Files\Application\run.exe
```

複数プロセスの場合

複数のプロセスがある場合は、以下のエントリをリストに追加します:

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application
\run2.exe
```

ワイルドカード文字の使用

ワイルドカードの使用（*）がサポートされています。アプリケーションのバージョンに基づいてディレクトリまたは実行可能ファイルの名前が変更された場合、またはサードパーティコンポーネントがユーザーのプロファイルにインストールされている場合は、ワイルドカードを使用できます。

ワイルドカードは次のシナリオで使用できます:

- 完全なディレクトリ名を置き換える場合。
  例: `C:\Program Files\Application\*\run1.exe`
- ディレクトリ名の一部を置き換える場合。
  例: `C:\Program Files\Application\v*\run1.exe`
- 実行可能ファイルの名前を置き換える場合。
  例: `C:\Program Files\Application\v1.2\*.exe`
- 実行可能ファイルの名前の一部を置き換える場合。
  例: `C:\Program Files\Application\v1.2\run*.exe`

次の制限事項が適用されます:

- ワイルドカードは、単一のディレクトリを置き換えるためにのみ使用できます。たとえば、実行可能ファイルが`C:\Program Files\Application\v1.2\run1.exe`にある場合、以下のようになります
  - 使用可能: `C:\Program Files\Application\*\run1.exe`
  - 使用不可: `C:\Program Files\*\run1.exe`

- エントリにはファイル拡張子が含まれている必要があります。
  - 使用可能: `C:\Program Files\Application\v1.2\*.exe`
  - 使用不可: `C:\Program Files\Application\v1.2\*`
- すべてのパスはローカルである必要があります。

> 注:
>
> - ネットワークパスの使用は許可されていません。
> - ワイルドカードのサポートは、Citrix Virtual Apps and Desktops 2206 から利用できます。
> - ワイルドカードのサポートは、Citrix Virtual Apps and Desktops 2203 LTSR の CU2 から利用できます。

システム環境変数の使用

システム環境変数を使用すると、許可リスト内の信頼できるプロセスの定義を簡素化できます。`%programfiles%`、`%programfiles(x86)%`、`%systemdrive%`、`%systemroot%`などの通常の変数を使用できます。

システムレベルで定義されている限り、カスタム環境変数を使用することもできます。

次の例は、通常の環境変数を示しています:

- `%programfiles%\Application\v1.2\run.exe`
- `%programfiles%\Application\*\run.exe`
- `%programfiles(x86)%\Application\v1.*\run.exe`

次の例は、カスタムのシステム環境変数を示しています:

- カスタム変数名: `app`
- カスタム変数値: `%programfiles%\Application\`
- 許可リストのエントリ: `CTXCVC1,%app%\run.exe`

> 注:
>
> ユーザー環境変数はサポートされていません。
>
> 環境変数のサポートは、Citrix Virtual Apps and Desktops バージョン 2209 から利用できます。

仮想チャネル名とプロセスの取得

仮想チャネルの名前と VDA マシンで仮想チャネルを開くプロセスを取得する最も簡単な方法は、仮想チャネルを提供した開発者またはサードパーティベンダーから情報を取得することです。

別の方法としては、機能のログを適用し、次の手順に従うことで情報を取得することもできます:

1. カスタム仮想チャネルのクライアントコンポーネントとサーバーコンポーネントを配置したら、仮想アプリケーションまたは仮想デスクトップを起動します。
2. VDA マシンのシステムイベントログにて、開こうとしたカスタム仮想チャネルの名前とプロセスを探します。利用可能なイベントについて詳しくは、「イベントログ」を参照してください。
3. セッションからログアウトします。
4. 仮想チャネル許可リストポリシー設定に、識別された仮想チャネルとプロセスに関するエントリを追加します。
5. マシンを再起動してください。
6. VDA が登録されたら、仮想アプリケーションまたは仮想デスクトップを実行して、カスタム仮想チャネルが正常に開くことを確認します。

Citrix 仮想チャネルに関する考慮事項

組み込みの Citrix 仮想チャネルはすべて信頼されており、追加の構成なしで開くことができます。ただし、次の 2 つの機能は、外部の依存関係のために許可リストに明示的なエントリを必要とします:

- マルチメディアリダイレクト
- HDX RealTime Optimization Pack for Skype for Business

マルチメディアリダイレクト

Windows Media Player 以外のメディアプレーヤーをシステムメディアプレーヤーとして使用する場合は、信頼できるプロセスとして許可リストに追加する必要があります。次の情報は、許可リストのエントリに必要です:

- 仮想チャネル名: `CTXMM`
- プロセス: VDA マシンで使用されているメディアプレーヤーのパス。例: `C:\Program Files (x86)\Windows Media Player\wmplayer.exe`。
- 許可リストのエントリ: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

HDX RealTime Optimization Pack for Skype for Business

次の情報は、許可リストのエントリに必要です:

- 仮想チャネル名: `CTXRMEP`
- プロセス: VDA マシン内の Skype for Business 実行可能ファイルのパス。Skype for Business のバージョンや、カスタムインストールパスの使用の有無によって異なる場合があります。例: `C:\Program Files\Microsoft Office\root\Office16\lync.exe`.
- 許可リストのエントリ: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

トラブルシューティング

May 17, 2024

カスタム仮想チャネルが開かない場合は、次の手順を確認してください：

1. 正しい VDA バージョンを使用していることを確認します。
2. 仮想チャネル許可リストでポリシーがカスタム仮想チャネルを含む VDA に適用されていること、およびこの構成を上書きする優先度の高い他のポリシーがないことを確認します。
3. VDA のイベントログを確認し、報告された仮想チャネル名が許可リストで定義されているものと一致していることを確認します。

    a) 複数のプロセスがある場合は、「許可リストへの仮想チャネルの追加」の説明に従って、これらが適切に定義されていることを確認してください。
    b) 定義されたプロセスパスでワイルドカードを使用している場合は、「ワイルドカード文字の使用」のガイドラインに従っていることを確認してください。
    c) 定義されたプロセス パスで環境変数を使用している場合は、「システム環境変数の使用」のガイドラインに従っていることを確認してください。

イベントログ

VDA マシンのイベントログに記録されるイベントは、次のとおりです。

シングルセッション **VDA**

次のイベントは、シングルセッション VDA マシンのイベントログに記録されます：

ログ名	Id	接続元	レベル	説明
System	2001	`Picadd`	情報	カスタム仮想チャネル<`vcName`>がプロセス< `processName`>によって開かれました

ログ名	Id	接続元	レベル	説明
System	2002	Picadd	警告	カスタム仮想チャネル<vcName>をプロセス<processName>で開くことはできません
System	2003	Picadd	情報	<username>がカスタム仮想チャネル<vcName>を開きました
System	2004	Picadd	警告	<username>がカスタム仮想チャネル<vcName>を開こうとしました
System	2005	Picadd	エラー	ポリシー<pathInPolicy>で指定されたパスは、プロセスパスに解決できません
System	2007	Picadd	情報	読み込まれたプロセスパスは<processPath>です
System	2008	Picadd	エラー	VC ポリシー パスに環境変数<varName>が見つかりません

マルチセッション **VDA**

次のイベントは、マルチセッション VDA マシンのイベントログに記録されます:

ログ名	Id	接続元	レベル	説明
System	13	Rpm	情報	カスタム仮想チャネル<vcName>がプロセス<processName>によって開かれました
System	14	Rpm	警告	カスタム仮想チャネル<vcName>をプロセス<processName>で開くことはできません
System	15	Rpm	情報	<username>がカスタム仮想チャネル<vcName>を開きました
System	16	Rpm	警告	<username>がカスタム仮想チャネル<vcName>を開こうとしました
System	17	Rpm	エラー	ポリシー<pathInPolicy>で指定されたパスは、プロセスパスに解決できません
System	18	Rpm	情報	読み込まれたプロセスパスは<processPath>です
System	19	Rpm	エラー	VC ポリシー パスに環境変数<varName>が見つかりません

既知のサードパーティ仮想チャネル

May 17, 2024

以下は、カスタム Citrix 仮想チャネルを使用する既知のサードパーティソリューションです。このリストには、カスタム Citrix 仮想チャネルを使用するすべてのソリューションが含まれているわけではありません。

- Cerner
- ControlUp
- Cisco WebEx Teams
- Cisco WebEx Meetings 仮想デスクトップソフトウェア
- deviceTrust
- Epic Warp Drive
- Epic Slingshot
- Imprivata OneSign
- Midmark IQPath クライアント拡張機能
- Nuance PowerMic クライアント拡張機能
- Nuance Dragon Medical Network Edition 360 vSync
- Zoom Meetings for VDI
- Ultima IA-Connect

関連する仮想チャネルを許可リストに追加することについて詳細を取得するには、ソリューションのベンダーに連絡してください。または、「仮想チャネル名とプロセスの取得」に記載されている手順に従ってください。

デバイス

August 29, 2023

HDX は、どんな場所にあるどんなデバイスでも高品位なユーザーエクスペリエンスを提供します。「デバイス」セクションの記事では、以下のデバイスについて説明します。

- クライアントドライブマッピング
- 一般的な USB デバイス
- モバイルおよびタッチスクリーンデバイス
- シリアルデバイス
- 特殊キーボード
- TWAIN デバイス
- Web カメラ
- WIA デバイス

最適化された **USB** デバイスと一般的な **USB** デバイス

最適化された USB デバイスとは、Citrix Workspace アプリが特定のサポートを提供しているデバイスです。たとえば、HDX マルチメディア仮想チャネルを使用して Web カメラをリダイレクトする機能などのサポートです。一般的なデバイスとは、Citrix Workspace アプリで特定のサポートがない USB デバイスのことです。

一般的な USB のリダイレクト機能では、一般モードに設定されていなければ、最適化された仮想チャネルをサポートする USB デバイスをデフォルトではリダイレクトできません。

一般的に、USB デバイスは一般モードよりも最適化モードで優れたパフォーマンスを発揮します。ただし、USB デバイスが最適化モードでの機能を完全に備えていない場合があります。そのデバイスの機能を完全に利用するには、一般モードに切り替える必要がある場合もあります。

USB 大容量記憶装置デバイスでは、Citrix ポリシーによって制御されるクライアントドライブマッピングまたは一般的な USB のリダイレクト機能のどちらか、またはその両方を使用できます。主な違いは次のとおりです。

一般的な USB のリダイレクト機能とクライアントドライブマッピングのポリシーの両方が有効な場合、セッション開始前または後に挿入された大容量記憶装置デバイスがクライアント側ドライブのマッピングによりリダイレクトされます。

これらの条件が満たされると、大容量記憶装置は一般的な USB のリダイレクト機能を使用してリダイレクトされます。

- 一般的な USB のリダイレクト機能とクライアントドライブマッピングのポリシーの両方が有効になっています。
- デバイスが自動リダイレクトに構成されています。
- 大容量記憶装置がセッションの開始前または後に挿入されます。

詳しくは、http://support.citrix.com/article/CTX123015を参照してください。

機能	クライアントドライブマッピング	汎用 USB リダイレクト
デフォルトで有効	はい	いいえ
読み取り専用アクセスの構成が可能	はい	いいえ
デバイスアクセスが暗号化される	はい（仮想セッションでデバイスにアクセスする前に暗号化のロックを解除した場合）。	Citrix Virtual Desktops のみ

クライアントドライブマッピング（**CDM**）

October 30, 2023

クライアントドライブマッピングは、クライアントエンドポイントのストレージドライブを Citrix HDX セッション内で利用できるようにすることで、ファイルやフォルダーをクライアントからセッションホストに、またはその逆方向に転送できるようになります。この機能はデフォルトで読み取り権限と書き込み権限の両方で有効になっています。マップされたクライアント側デバイス上でのフォルダーおよびファイルの追加や変更を禁止するには、[クライアント側ドライブへの読み取り専用アクセス] 設定を有効にします。この設定項目をポリシーに追加するときは、[クライアントドライブのリダイレクト] 設定も追加されており、[許可] が選択されていることを確認してください。

セキュリティ上の予防措置として、デフォルトでは、エンドポイントドライブは実行権限なしでマップされます。マップされたクライアントドライブから実行可能ファイルをユーザーが直接実行できるようにするには、セッションホストの **ExecuteFromMappedDrive** レジストリ値を編集します。詳しくは、「レジストリを介して管理される機能」にある「マップされたクライアントドライブ」を参照してください。

要件

CDM を使用するための要件は以下のとおりです。

Citrix コントロールプレーン

- Citrix Virtual Apps and Desktops 1912 以降
- Citrix DaaS

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - Windows Server 2016 以降
  - Linux：Linux Virtual Delivery Agent の「システム要件」を参照してください。
- VDA
  - Windows：Citrix Virtual Apps and Desktops 1912 以降
  - Linux：Linux Virtual Delivery Agent のドキュメントを参照してください。

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - Linux：Linux のシステム要件については、Workspace アプリを参照してください。

関連ポリシー

CDM の設定については、「ポリシー設定リファレンス」セクションを参照してください。

ダブルホップのシナリオ

CDM はダブルホップのシナリオでサポートされます。デフォルトでは、クライアントエンドポイントのドライブは 2 番目のホップセッションにマップされ、最初のホップのドライブは使用できません。ただし、これは、クライアントエンドポイントのドライブでなく最初のホップのドライブが 2 番目のホップのセッションにマップされるように設定することもできます。

この機能を構成するには、次のレジストリ値を編集します。

- キー:HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced
- 値の名前: NativeDriveMapping
- 値の種類: REG_SZ
- 値のデータ:
  - True - 最初のホップセッションのドライブを 2 番目のホップセッションにマッピングします。
  - False - クライアント エンドポイントのドライブを 2 番目のホップセッションにマッピングします。

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

一般的な **USB** デバイス

April 18, 2024

HDX テクノロジは、一般的な USB デバイスのほとんどに最適化されたサポートを提供します。これらのデバイスには、以下のものが含まれます:

- モニター
- マウス
- キーボード
- ボイスオーバー IP 電話
- ヘッドセット
- Web カメラ

- スキャナー
- カメラ
- プリンター
- ドライブ
- スマートカードリーダー
- 描画用タブレット
- 署名パッド

最適化されたサポートにより、パフォーマンスが良くなることでユーザーエクスペリエンスが向上し、WAN 経由の帯域幅効率が改善されます。最適化されたサポートは通常、遅延が多い環境やセキュリティが厳しい環境で最善のオプションです。

HDX テクノロジは、特殊デバイスに次のような最適化されたサポートがないとき、または不適切なときに汎用 **USB** リダイレクトを提供します。一般的な USB のリダイレクトの設定について詳しくは、「Citrix の一般的な USB のリダイレクト機能」を参照してください。

USB デバイスおよび Windows 向け Citrix Workspace アプリについて詳しくは、「複合 USB デバイスのリダイレクト機能の構成」および「USB サポートの構成」を参照してください。

モバイルおよびタッチスクリーンクライアントデバイスのサポート

February 19, 2024

Citrix Virtual Apps and Desktops を使用すると、ユーザーはモバイルデバイスやタッチスクリーンクライアントデバイスから公開アプリケーションやデスクトップにアクセスできます。

要件

Citrix コントロールプレーン

- Citrix Virtual Apps and Desktops 7.15 以降
- Citrix DaaS

セッションホスト

- オペレーティングシステム
  - Windows 10 1903 以降
  - Windows Server 2016 以降
- VDA

  - Windows：バージョン 7.15 以降

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
- Windows 向け Citrix Workspace アプリバージョン 1808 以降

Windows Continuum を使用したタッチスクリーンデバイス用タブレットモード

Continuum は、クライアントデバイスの使用方法に対応する Windows 10 の機能です。VDA がタッチ対応クライアントのキーボードまたはマウスの存在を検出すると、クライアントをデスクトップモードにします。キーボードまたはマウスが存在しない場合、VDA はクライアントをタブレット/モバイルモードにします。この検出は、セッションの接続時と再接続時に行われます。また、セッション中にキーボードまたはマウスが接続または切断されたときにも行われます。

この機能はデフォルトで有効にされています。この機能を無効にするには、ポリシー設定で ［タブレットモードの切り替え］ を構成します。

上記のタッチスクリーンデバイスの要件に加えて、Windows Continuum では次の要件があります：

XenServer

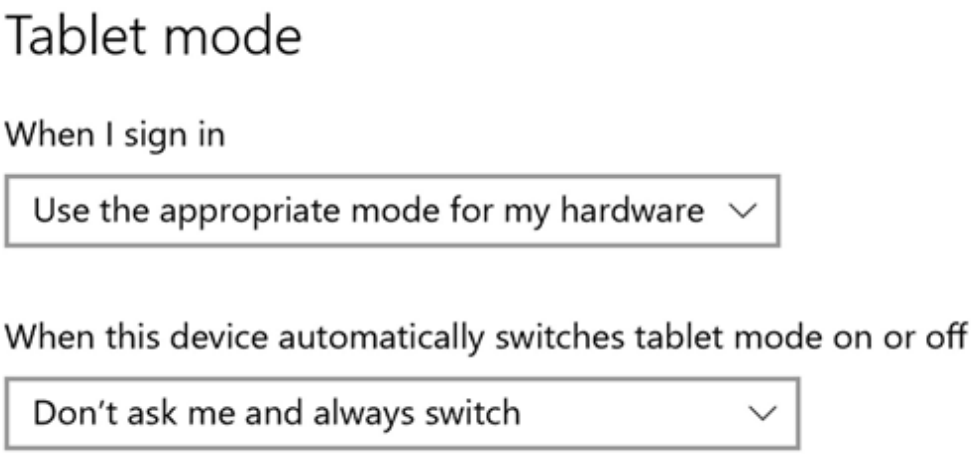
- Citrix Hypervisor 8.2 以降
- ノートブック/タブレットの切り替えを許可するには、XenServer CLI コマンドを実行します：
  xe vm-param-set uuid=<VM_UUID> platform:acpi_laptop_slate=1

> 重要：
>
> メタデータ設定を変更した後で既存のマシンカタログの基本イメージを更新しても、以前にプロビジョニングされた VM には影響しません。XenServer VM の基本イメージを変更した後、カタログを作成し、基本イメージを選択し、新しい MCS（Machine Creation Services）マシンをプロビジョニングします。

セッションホスト

- オペレーティングシステム
  - Windows 10 1903 以降
  - Windows 11
- VDA

- Windows：バージョン 7.16 以降
- オペレーティング システム構成の現在の制限により、ユーザーは最初の **ICA** セッションを開始して **VDA** を再起動した後、ドロップダウンメニューから次のオプションを設定する必要があります：
  - ［設定］**>**［システム］**>**［タブレットモード］
    - ハードウェアに適切なモードを使用する
    - 確認なしで常に切り替える



タブレットモードでは、タッチスクリーンにより適した以下のユーザーインターフェイスが提供されます：

- やや大きめのボタン
- スタート画面や開始したアプリケーションを全画面で開く
- タスクバーに戻るボタンを表示
- タスクバーからアイコンを削除

File Explorer にアクセスできます。

Windows 10 は、この更新された BIOS を基にターゲット仮想マシンに GPIO ドライバーをロードします。これは、

仮想マシン内でタブレットモードとデスクトップモードを切り替えるのに使用されます。

HTML5 向け Citrix Workspace アプリは、Windows Continuum 機能をサポートしていません。

デスクトップモードでは、PC とキーボードとマウスを使用するのと同じ方法で対話する従来のユーザーインターフェイスが提供されます。

Microsoft Surface Pro および **Surface Book** のペン

Windows Ink を使用するアプリケーションで標準のペン機能をサポートします。サポートされるペン機能には、ポインティング、消去、筆圧、Bluetooth 信号、オペレーティングシステムのファームウェアやペンモデルによって異なるその他の機能が含まれます。たとえば、筆圧は最大 4096 レベルまで可能です。この機能はデフォルトで有効になっています。

ペン機能のサポートの要件は次のとおりです:

Citrix コントロールプレーン

- Citrix Virtual Apps and Desktops 1903 以降
- Citrix DaaS

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - Windows Server 2016 以降
  - Windows 11
- VDA
  - Windows: バージョン 1903 以降

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
- Windows 向け Citrix Workspace アプリバージョン 1902 以降

Windows Ink とペン機能のデモを見るには、以下の画像をクリックしてください:

この機能を無効または有効にするには、レジストリを介して管理される機能の一覧にある「Microsoft Surface Pro および Surface Book のペン」を参照してください。

既知の問題

ペン機能のサポートに関する既知の問題は次のとおりです:

- Windows Server 2k22 の OS の制限により、2k22 サーバーまたはデスクトップに接続している場合、ユーザーは［コントロールパネル］でペンのショートカットを設定したり、ペン/Ink の設定に調整を加えたりすることができません。
- OS の制限のため、ペン機能に対応した Windows 11 クライアントでペンのショートカットが機能しません。

シリアルポート

April 22, 2022

ほとんどの新しい PC には、シリアル（COM）ポートは内蔵されていません。シリアルポートは USB コンバーターを使用して簡単に追加できます。シリアルポートに適したアプリケーションには、センサー、コントローラー、旧式のチェックリーダー、パッドなどがあります。一部の USB 仮想 COM ポートデバイスでは、Windows 提供のドライバー（usbser.sys）の代わりにベンダー固有のドライバーが使用されます。これらのドライバーを使用すると、USB デバイスの仮想 COM ポートを別の USB ソケットに接続しても変更されないように強制することができます。これは、［デバイスマネージャー］**>**［ポート（**COM** & **LPT**）］**>**［プロパティ］から、またはデバイスを制御するアプリケーションから設定できます。

クライアント側 COM ポートのマッピングを使用すると、ユーザーのエンドポイント上の COM ポートに接続されているデバイスを仮想セッション中に使用できるようになります。これらのマッピングは他のネットワークマッピングと同様に使用できます。

各 COM ポートには、オペレーティングシステムのドライバーによって COM1 や COM2 などのシンボリックリンク名が割り当てられます。アプリケーションはそのリンクを使用してポートにアクセスします。

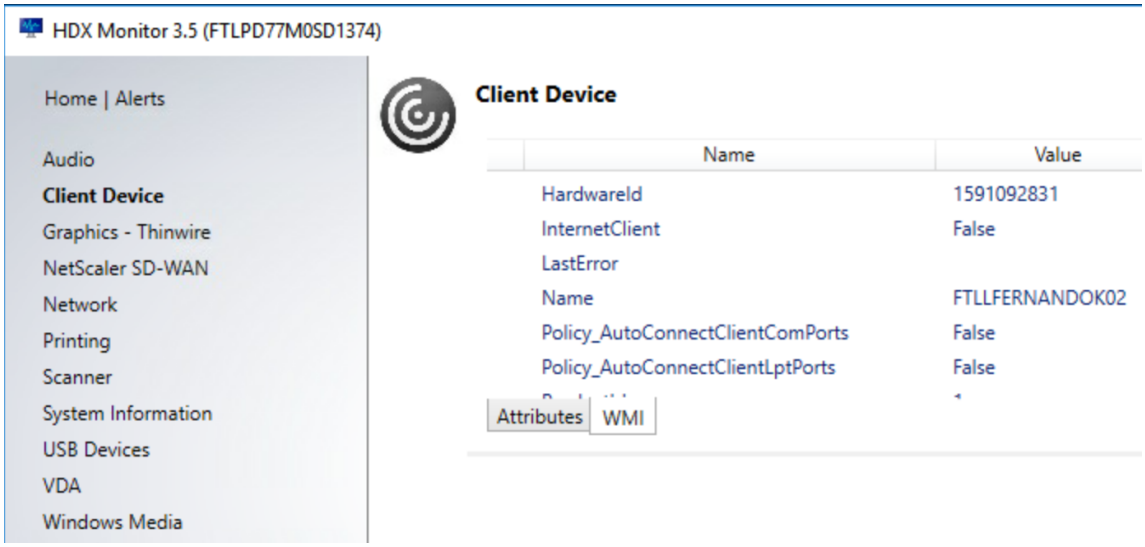
> 重要:
>
> デバイスは USB を直接使用してエンドポイントに接続できるため、汎用 USB リダイレクトを使用してデバイスをリダイレクトすることはできません。一部の USB デバイスは仮想 COM ポートとして機能し、アプリケーションは物理シリアルポートと同じ方法でそのポートにアクセスできます。オペレーティングシステムは、COM ポートを抽象化して、ファイル共有のように扱うことができます。仮想 COM でよく使用されるプロトコルは CDC ACM と MCT の 2 つです。RS-485 ポート経由で接続すると、アプリケーションがまったく機能しないことがあります。RS-485 を COM ポートとして使用するには、RS-485-to-RS232 コンバーターを入手してください。
> 重要:
>
> 一部のアプリケーションは、デバイス（たとえば、署名パッド）がクライアントワークステーションの COM1 または COM2 に接続されている場合に限り、そのデバイスを一貫して認識します。

クライアント **COM** ポートをサーバーの **COM** ポートにマップする

クライアントの COM ポートを Citrix セッションにマップするには、次の 3 つの方法があります。

- ［管理］コンソールのポリシー。ポリシーについて詳しくは、「ポートリダイレクトのポリシー設定」を参照してください。
- VDA コマンドプロンプト。
- リモートデスクトップ（ターミナルサービス）構成ツール。

1. ［クライアント **COM** ポートリダイレクト］と ［クライアント **COM** ポートを自動接続する］の Studio ポリシーを有効にします。適用すると、一部の情報が HDX Monitor で利用可能になります。



2. ［クライアント **COM** ポートを自動接続する］でポートのマッピングに失敗した場合は、そのポートを手動でマップするか、またはログオンスクリプトを使用します。VDA にログオンし、コマンドプロンプトウィンドウで次のように入力します:

   NET USE COMX: \\CLIENT\COMZ:

   または

   NET USE COMX: \\CLIENT\CLIENTPORT:COMZ:

   < X > は VDA 上の COM ポートの番号です（マッピングに使用できるのはポート 1～9 です）。**< Z >** は、マップするクライアント COM ポートの番号です。

   その操作が成功したことを確認するには、VDA コマンドプロンプトで **NET USE** と入力します。マップされているドライブ、LPT ポート、およびマップされている COM ポートの一覧が表示されます。

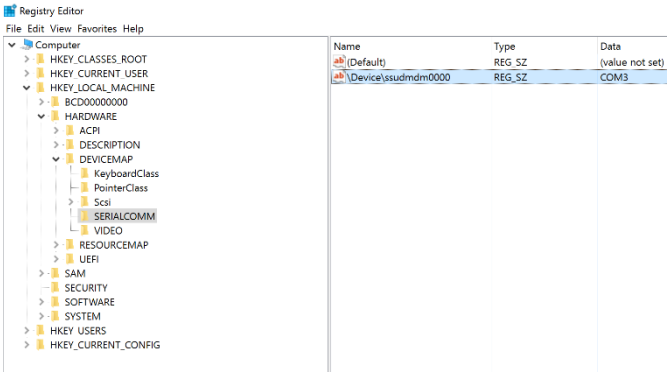
3. その COM ポートを仮想デスクトップやアプリケーションで使用するには、ユーザーデバイスアプリケーションをインストールし、マップされている COM ポート名を指すようにします。たとえば、クライアントの COM1 をサーバーの COM3 にマップしている場合は、COM ポートデバイスアプリケーションを VDA にインストールし、セッション中に COM3 を指すようにします。この方法でマップした COM ポートは、ユーザーデバイスの COM ポートと同じように使用できます。

> 重要:
>
> COM ポートマッピングは TAPI 対応ではありません。Windows テレフォニーアプリケーションプログラミン

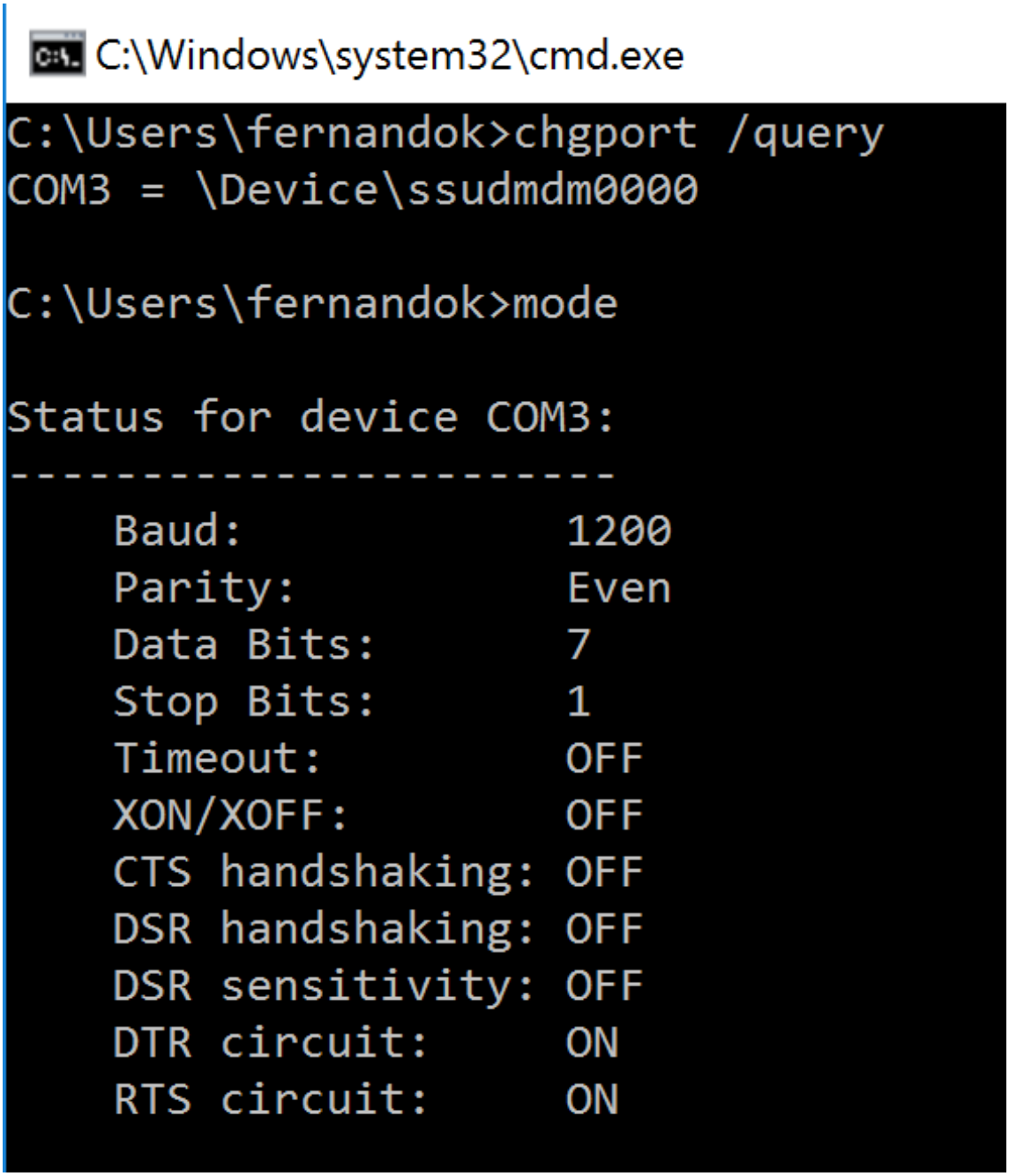
> グインターフェイス（TAPI）デバイスをクライアント COM ポートにマップすることはできません。TAPI は、アプリケーションがデータ、ファックス、および音声通話のテレフォニー機能を制御するための標準的な方法を定義します。TAPI は、ダイヤル、応答、通話終了などのシグナリングを管理します。また、保留、転送、会議通話などの付加的サービスも管理します。

トラブルシューティング

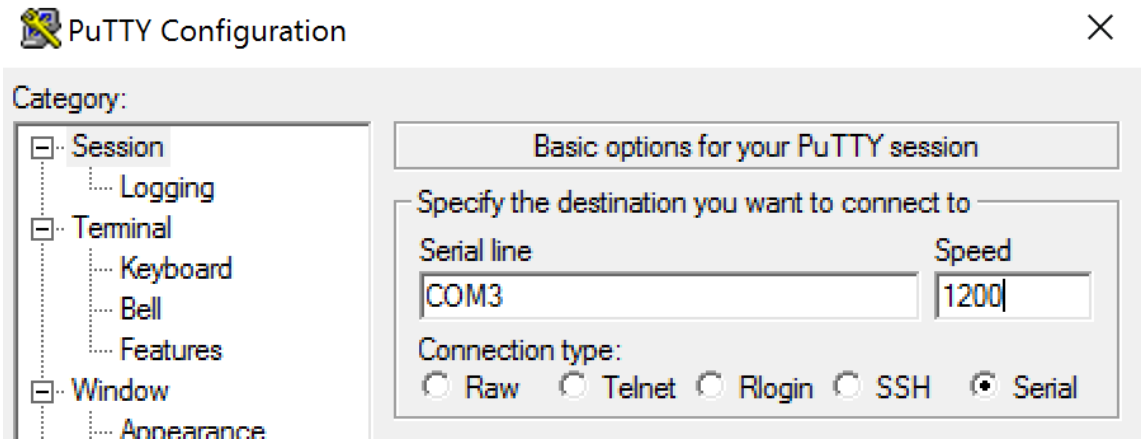
1. Citrix をバイパスしてエンドポイントからデバイスに直接アクセスできることを確認します。ポートが VDA にマップされていない間は、Citrix セッションに接続していません。デバイスに付属しているトラブルシューティングの指示に従って、まずデバイスがローカルに動作することを確認します。
   デバイスがシリアル COM ポートに接続されている場合は、次のハイブにレジストリキーが作成されています:



   この情報は、コマンドプロンプトで **chgport /query** を実行して確認することもできます。



デバイスのトラブルシューティングの手順を利用できない場合は、PuTTY セッションを開いてみます。［セッション］を選択し、［シリアル回線］で COM ポートを指定します。



ローカルのコマンドウィンドウで **MODE** コマンドを実行すると、その出力に、使用中の COM ポート、および PuTTY セッションで必要なボーレート/パリティ/データビット/ストップビットの情報が表示されます。PuTTY 接続に成功した場合は、**Enter** キーを押すとデバイスからのフィードバックが表示されます。入力した文字が画面上で繰り返されるか、または応答が返されます。この手順が正常に行われない場合、仮想セッションからデバイスにアクセスすることはできません。

2. ローカル COM ポートを VDA にマップし（ポリシーまたは **NET USE COM< X >: \\CLIENT\COM< Z >** を使用）、今回は VDA PuTTY から、前と同じ PuTTY 手順を繰り返します。PuTTY が「**Unable to open connection to COM1. Unable to open serial port**」というエラーで失敗する場合は、別のデバイスが COM1 を使用している可能性があります。

3. **chgport /query** を実行します。VDA 上の Windows の組み込みシリアルドライバーによって、VDA の COM1 ポートに\Device\Serial0 が自動的に割り当てられている場合は、次のようにします：
   A. VDA でコマンドウィンドウを開いて、次のコマンドを入力します：**NET USE**

   B. VDA の既存のマッピング（たとえば、COM1）を削除します。

   NET USE COM1 /DELETE

   C. そのデバイスを VDA にマップします。

   NET USE COM1: \\CLIENT\COM3:

   D. VDA 上のアプリケーションが COM3 を指すようにします。

   最後に、ローカル COM ポート（COM3 など）を VDA の別の COM ポート（COM1 以外の COM3 など）にマップしてみます。アプリケーションがそのポートを指すようにします：
   NET USE COM3: \\CLIENT\COM3

4. この時点でポートがマップされていることを確認できた場合、PuTTY は動作していますがデータは渡されていないため、競合状態である可能性があります。ポートがマップされる前にアプリケーションがそのポートに接続して開き、ロックしているためにマップできない可能性があります。次のいずれかを試してみます。

   - 同じサーバーで公開されている別のアプリケーションを開きます。ポートがマップされるまで数秒待ってから、そのポートを使用しようとする実際のアプリケーションを開きます。

- サービスの［管理］>［完全な構成］インターフェイスではなく、Active Directory のグループポリシーエディターから、COM ポートリダイレクトポリシーを有効にします。有効にするポリシーは、［クライアント **COM** ポートリダイレクト］と ［クライアント **COM** ポートを自動接続する］です。この方法で適用されるポリシーは、［管理］コンソールポリシーより前に処理され、COM ポートがマップされることが保証される可能性があります。Citrix ポリシーは VDA にプッシュされ、次の場所に格納されています。
  `HKLN\SOFTWARE\Policies\Citrix \<user session ID\>`
- このログオンスクリプトをユーザーに対して使用するか、またはアプリケーションを公開する代わりに使用して、VDA の任意のマッピングを削除した後に仮想 COM ポートを再マッピングしてから、そのアプリケーションを起動する.bat スクリプトを公開します。

@echo off
NET USE COM1 /delete
NET USE COM2 /delete
NET USE COM1: \\CLIENT\COM1:
NET USE COM2: \\CLIENT\COM2:
MODE COM1: BAUD=1200（など必要な値なら何でも）
MODE COM2: BAUD=9600 PARITY=N Data=8 Stop=1（など必要な値なら何でも）
START C:\Program Files\< ソフトウェアのパス >\\< ソフトウェアの.exe ファイル > ソフトウェアの.exe ファイル > ソフトウェアのパス >

5. 最後の手段としては、Sysinternals の Process Monitor があります。VDA でこのツールを実行するときは、COM3、picaser.sys、CdmRedirector など（特に、<your_app>.exe）のオブジェクトを検索してフィルタリングします。「アクセスが拒否されました」などのエラーが表示されることがあります。

特殊キーボード

April 18, 2024

Bloomberg キーボード

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

Citrix Virtual Apps and Desktops では、Bloomberg モデル 4 Starboard キーボード（およびそれ以前のモデル

3）がサポートされています。このキーボードを使用すると、金融分野の顧客は、キーボードの特殊機能を使用して金融市場データにアクセスし、取引を迅速に実行できます。

このキーボードは KVM スイッチボックスと互換性があり、次の 2 つのモードで動作します。

- PC（USB ケーブル 1 本、KVM なし）
- KVM モード（USB ケーブル 2 本、1 本は KVM 経由）

> 重要：
>
> Bloomberg キーボードは 1 つのセッションのみで使用することをお勧めします。複数の同時セッション（1 つのクライアントからのマルチセッション）でこのキーボードを使用することはお勧めしません。

Bloomberg キーボードモデル 4 は、1 つの物理シェル内に次の 4 つの USB デバイスを備える、USB 複合デバイスです。

- キーボード。
- 指紋リーダー。
- 音量を増減するためのキーおよびスピーカーとマイクをミュートするためのキーが付いているオーディオデバイス。このデバイスには、オンボードスピーカー、マイク、およびマイクとヘッドセット用のジャックが備わっています。
- これらのすべてのデバイスをシステムに接続するための USB ハブ。

要件：

- Windows 向け Citrix Workspace アプリが接続するセッションで、USB デバイスがサポートされている必要があります。
- Bloomberg キーボードモデル 3 および 4 は、Windows 向け Citrix Workspace アプリ 1808 以降および Citrix Receiver for Windows 4.8 以降でサポートされています。
- モデル 4 の KVM モード（USB ケーブル 2 本、1 本は KVM 経由）を使用するには、Windows 向け Citrix Workspace アプリ 1808 以降または Citrix Receiver for Windows 4.12 以降が必要です。

Windows 向け Citrix Workspace アプリでの Bloomberg キーボードの構成について詳しくは、「Bloomberg キーボードの構成」を参照してください。

Bloogberg キーボードのサポートを有効にするには、レジストリを介して管理される機能の一覧にある「Bloomberg キーボード」を参照してください。

サポートを確認する：

Bloomberg キーボードのサポートが Citrix Workspace アプリで有効になっているかどうかを確認するには、Desktop Viewer で Bloomberg キーボードのデバイスが正しく報告されているかどうかを確認します。

デスクトップの場合：

Desktop Viewer を開きます。Bloomberg キーボードのサポートが有効になっている場合は、Desktop Viewer で USB アイコンの下に次の 3 つのデバイスが表示されています：

- Bloomberg Fingerprint Scanner
- Bloomberg Keyboard Features
- Bloomberg LP Keyboard 2013

シームレスアプリケーションのみの場合:

Citrix Workspace アプリの通知領域アイコンから ［コネクションセンター］ メニューを開きます。Bloomberg キーボードのサポートが有効になっている場合は、［デバイス］ メニューに 3 つのデバイスが表示されています。

各デバイスに付いているチェックマークは、そのデバイスがそのセッションでリモートであることを示しています。

TWAIN デバイス

April 22, 2022

要件

- スキャナーは TWAIN 準拠である必要があります。
- ローカルデバイスに TWAIN ドライバーをインストールします。サーバー上には TWAIN ドライバーは必要ありません。
- スキャナーをローカルに接続します（USB 経由など）。
- スキャナーが Windows Image Acquisition サービスではなくローカルの TWAIN ドライバーを使用していることを確認します。
- テストに使用するユーザーアカウントに、ICA セッション内の帯域幅を制限しているポリシー（たとえば、クライアント USB デバイスリダイレクトの最大帯域幅）が適用されていないことを確認します。

ポリシー設定について詳しくは、「TWAIN デバイスのポリシー設定」を参照してください。

Web カメラ

August 18, 2022

高品位 Web カメラストリーミング

Web カメラは、仮想セッション内で実行されているビデオ会議アプリケーションで使用できます。サーバーのアプリケーションは、サポートされている形式の種類に基づいて Web カメラの形式と解像度を選択します。セッションが開始されると、クライアントは Web カメラ情報をサーバーに送信します。ビデオ会議アプリケーションから Web カ

メラを選択します。Web カメラとアプリケーションがどちらも高品位レンダリングをサポートする場合、アプリケーションは高品位解像度を使用します。1920x1080 までの Web カメラ解像度がサポートされています。

この機能を使用するには、Citrix Receiver for Windows の最小バージョン 4.10 が必要です。HDX Web カメラリダイレクトをサポートする Citrix Workspace アプリプラットフォームの一覧については、「Citrix Workspace アプリの機能マトリックス」を参照してください。

高品位 Web カメラでのストリーミングについて詳しくは、「HDX ビデオ会議と Web カメラビデオ圧縮」を参照してください。

レジストリキーを使用してこの機能を無効または有効にすることで、特定の解像度を設定することができます。詳しくは、レジストリを介して管理される機能の一覧にある「高品位 Web カメラストリーミングと高品位 Web カメラ解像度」を参照してください。

WIA デバイス

April 22, 2022

要件

- スキャナーは WIA 準拠である必要があります。
- ローカルデバイスに WIA ドライバーをインストールします。サーバー上には TWAIN ドライバーは必要ありません。
- スキャナーをローカルに接続します（USB 経由など）。
- スキャナーが TWAIN ドライバーではなくローカルの Windows Image Acquisition サービスを使用していることを確認します。
- テストに使用するユーザーアカウントに、ICA セッション内の帯域幅を制限しているポリシー（たとえば、クライアント USB デバイスリダイレクトの最大帯域幅）が適用されていないことを確認します。

Windows Image Acquisition アプリケーションの許可リスト

許可リストにより、VDA 上のどのアプリケーションに Windows Image Acquisition スキャナーのリダイレクトへのアクセスを許可するかを制御できます。レジストリエディターでは、Windows Image Acquisition を含む各 VDA の許可リスト設定からの入力を使用します。デフォルトでは、Windows Image Acquisition にアクセスできるアプリケーションはありません。

VDA 上のアプリケーションの Windows Image Acquisition を調整するには、レジストリで管理される機能の一覧にある「Windows Image Acquisition アプリケーションの許可リスト」の設定を参照してください。

ポリシー設定について詳しくは、「WIA デバイスのポリシー設定」を参照してください。

グラフィック

April 22, 2022

Citrix HDX グラフィックは広範囲な一連のグラフィックアクセラレーションと、Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）からのリッチグラフィックアプリケーションの配信を最適化するエンコード技術を備えています。このグラフィック技術は、グラフィックを多用する仮想アプリケーションをリモートで使用する際に、物理デスクトップを使う場合と同じ操作性を提供します。

グラフィックにはハードウェアまたはソフトウェアレンダリングが使用できます。ソフトウェアレンダリングには、ソフトウェアラスタライザーと呼ばれるサードパーティのライブラリが必要です。たとえば、Windows には DirectX ベースのグラフィックのための WARP ラスタライザーが含まれています。他のソフトウェアレンダラーを使うことも可能です。ハードウェアレンダリング（ハードウェアアクセラレーション）にはグラフィックプロセッサ（GPU）が必要です。

HDX グラフィックは、一般的なユースケースのほとんどの場合に最適化された、デフォルトのエンコーディング構成を備えています。Citrix ポリシーを使用すると、IT 管理者は異なる要件を満たすさまざまなグラフィック関連の設定を構成し、望ましいユーザーエクスペリエンスを実現することもできます。

Thinwire

Thinwire とは、Citrix DaaS で使用される、Citrix のデフォルトのディスプレイリモートテクノロジです。

ディスプレイリモートテクノロジを使用すると、あるマシンで生成されたグラフィックが、通常はネットワークを経由して、別のマシンに転送され、表示されます。グラフィックは、ユーザー入力（たとえば、キー入力やマウス操作）の結果として生成されます。

HDX 3D Pro

Citrix DaaS の HDX 3D Pro 機能を使用すると、ハードウェアアクセラレーションにグラフィック処理装置（GPU）を使用して最高の性能を発揮するデスクトップとアプリケーションを配信できます。たとえば、OpenGL や DirectX を使用する 3D プロフェッショナルグラフィックアプリケーションでこの機能を使用します。標準 VDA では、DirectX の GPU アクセラレーションのみがサポートされます。

Windows シングルセッション OS のための GPU アクセラレーション

HDX 3D Pro を使用することで、グラフィックアプリケーションを仮想デスクトップ上で提供したりシングルセッションOS マシン上のアプリケーションとして配信したりできます。HDX 3D Pro は、物理コンピューター（デスクトップ、ブレード、およびラックワークステーションなど）と、XenServer、vSphere、および Hyper-V（パススルーのみ）ハイパーバイザーが提供する GPU パススルーおよび GPU 仮想化技術をサポートします。

GPU パススルー機能を使用すると、グラフィック処理ハードウェアに排他的にアクセスする仮想マシンを作成できます。ハイパーバイザーに複数の GPU を装着して、各仮想マシンに GPU を 1 つずつ割り当てることができます。

GPU 仮想化を使用すると、複数の仮想マシンで単一の物理 GPU によるグラフィック処理能力に直接アクセスできるようになります。

Windows マルチセッション OS のための GPU アクセラレーション

HDX 3D Pro 機能により、Windows マルチセッション OS のセッションで実行しているグラフィック処理アプリケーションで、サーバー上の GPU（Graphics Processing Unit）リソースを使用できるようになります。OpenGL、DirectX、Direct3D、および Windows Presentation Foundation（WPF）の処理をサーバーの GPU に移すことで、グラフィック処理によりサーバーの CPU 速度が低下することを回避できます。また、ワークロードが CPU と GPU で分担されるため、サーバーでより多くのグラフィック処理が可能になります。

Framehawk

> 重要:
>
> Citrix Virtual Apps and Desktops 7 1903 以降、Framehawk はサポートされなくなりました。代わりに、アダプティブトランスポートが有効なThinwireを使用します。

Framehawk は、ブロードバンドワイヤレス接続（Wi-Fi および 4G/LTE セルラーネットワーク）でのモバイルワーカー向けディスプレイリモートテクノロジです。Framehawk はスペクトル干渉や多重伝搬による課題を克服し、仮想アプリおよびデスクトップのユーザーに、滑らかで対話的なユーザーエクスペリエンスを提供します。

テキストベースのセッションウォーターマーク

テキストベースのセッションウォーターマークは、データ盗難を防止し、追跡できるようにするために役立ちます。この情報は追跡可能であり、セッションデスクトップに表示されることで、データを盗むために写真やスクリーンキャプチャを使用する場合の抑止力になります。テキストのレイヤーであるウォーターマークは自分で指定できます。ウォーターマークは元のドキュメントのコンテンツを変更することなく、セッション画面全体に表示されます。テキストベースのセッションウォーターマークには、VDA サポートが必要です。

関連情報

- HDX 3D Pro
- Windows シングルセッション OS のための GPU アクセラレーション
- Windows マルチセッション OS のための GPU アクセラレーション
- Thinwire
- テキストベースのセッションウォーターマーク

HDX 3D Pro

January 25, 2024

Citrix Virtual Apps and Desktops の HDX 3D Pro 機能を使用すると、グラフィック処理装置（GPU）によるハードウェアアクセラレーションで最高の性能を発揮するデスクトップとアプリケーションを配信できます。たとえば、

OpenGL や DirectX を使用する 3D プロフェッショナルグラフィックアプリケーションでこの機能を使用します。標準 VDA では、DirectX の GPU アクセラレーションのみがサポートされます。

HDX 3D Pro のポリシー設定については、「3D 画像ワークロードの最適化」を参照してください。

サポート対象の Citrix Workspace アプリすべてで、3D グラフィックを使用できます。複雑な 3D ワークロード、高解像度モニター、マルチモニター構成、および高フレームレートアプリケーションで最高のパフォーマンスを得るには、Windows 向け Citrix Workspace アプリおよび Linux 向け Citrix Workspace アプリを最新バージョンにすることをお勧めします。サポート対象の Citrix Workspace アプリのバージョンについて詳しくは、「Citrix Workspace アプリのライフサイクルマイルストーン」を参照してください。

これらの 3D グラフィック処理アプリケーションとして次のものがあります:

- コンピューター支援設計（CAD）、コンピューター支援製造（CAM）、およびコンピューター支援エンジニアリング（CAE）アプリケーション
- 地理情報システム（GIS）ソフトウェア
- 医療画像処理のための画像保存通信システム（PACS）
- 最新バージョンの OpenGL、DirectX、NVIDIA CUDA、OpenCL、および WebGL を使用するアプリケーション
- 並列計算に NVIDIA Compute Unified Device Architecture（CUDA）GPU を使用する計算集約型の非グラフィックアプリケーション

HDX 3D Pro では、さまざまな帯域幅において最適なユーザーエクスペリエンスが提供されます。

- WAN 接続の場合：帯域幅が 1.5Mbps の WAN 接続でもインタラクティブなユーザーエクスペリエンスが提供されます。
- LAN 接続の場合：LAN 接続ではローカルデスクトップに匹敵するユーザーエクスペリエンスが提供されます。

  ユーザーが使用する複雑で高価なワークステーションをよりシンプルなユーザーデバイスに置き換えて、グラフィック処理をユーザー側から中央管理が可能なデータセンター内に移管できます。

HDX 3D Pro により、Windows シングルセッションOS マシンと Windows マルチセッション OS マシンでの GPU アクセラレーションが提供されます。詳しくは、「Windows シングルセッション OS のための GPU アクセラレーション」および「Windows マルチセッション OS のための GPU アクセラレーション」を参照してください。

HDX 3D Pro は、次のハイパーバイザーが提供する GPU パススルーや GPU 仮想化、およびベアメタルと互換性があります:

- XenServer
  - NVIDIA GRID、AMD および Intel GVT-d による GPU パススルー
  - NVIDIA GRID、AMD および Intel GVT-g による GPU 仮想化
  - ハードウェア互換性については、「Hypervisor ハードウェア互換性リスト」を参照してください。

HDX Monitor を使用すると、HDX 仮想テクノロジの操作と構成を検証して、HDX の問題を診断して解決できます。このツールの詳細およびダウンロード方法については、https://taas.citrix.com/hdx/download/を参照してください。

Windows マルチセッション OS のための GPU アクセラレーション

January 25, 2024

HDX 3D Pro 機能により、Windows マルチセッション OS のセッションで実行しているグラフィック処理アプリケーションで、サーバー上の GPU（Graphics Processing Unit）リソースを使用できるようになります。OpenGL、DirectX、Direct3D、および Windows Presentation Foundation（WPF）の処理をサーバーの GPU に移すことで、グラフィック処理によりサーバーの CPU 速度が低下することを回避できます。また、ワークロードが CPU と GPU で分担されるため、サーバーでより多くのグラフィック処理が可能になります。

Windows Server はマルチユーザーオペレーティングシステムなので、GPU 仮想化（vGPU）を行わなくても、Citrix Virtual Apps がアクセスする GPU を複数のユーザーで共有できます。

このトピックの説明にはレジストリの編集が含まれています。レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windows の再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix では一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

GPU 共有

GPU 共有により、リモートデスクトップセッションで動作する OpenGL アプリケーションおよび DirectX アプリケーションで GPU ハードウェアによるレンダリング処理が可能になります。GPU 共有には、以下の特徴があります:

- ベアメタルまたは仮想マシン上で使用でき、アプリケーションのスケーラビリティとパフォーマンスが向上します。
- 複数の同時接続セッションで GPU リソースを共有できます（ほとんどのユーザーは専用 GPU のレンダリングパフォーマンスを必要としません）。
- 特別な設定は必要ありません。

GPU は、ハイパーバイザーと GPU ベンダーの要件に従って、完全パススルーモードまたは仮想 GPU（vGPU）モードのいずれかで、Windows Server 仮想マシンに割り当てることができます。物理 Windows Server マシンでのベアメタル展開もサポートされています。

GPU 共有は、特定のグラフィックカードに依存するものではありません。

- 仮想マシンの場合は、使用中のハイパーバイザーと互換性のあるグラフィックカードを選択します。XenServer のハードウェア互換性リストについては、「Hypervisor ハードウェア互換性リスト」を参照してください。
- ベアメタルを実行するときは、オペレーティングシステムで単一のディスプレイアダプターを有効にすることをお勧めします。複数の GPU がハードウェアに取り付けられている場合は、デバイスマネージャーを使用して 1 つだけ残して無効にします。

GPU 共有でのスケーラビリティは、以下の要素により異なります。

- 実行するアプリケーション
- 消費されるビデオ RAM の量
- グラフィックカードの処理能力

一部のアプリケーションでは、ビデオ RAM の不足をより効果的に処理できます。ハードウェアが過負荷になると、グラフィックカードドライバーが不安定になるか、クラッシュが発生する可能性があります。このような問題を避けるには、同時接続ユーザーの数を制限してください。

GPU アクセラレーションが正しく動作しているかどうかを確認するには、GPU-Z などのサードパーティ製ツールを使用できます。このツールは、http://www.techpowerup.com/gpuz/で提供されています。

- NVIDIA GPU の高パフォーマンスビデオエンコーダーと Intel Iris Pro グラフィックプロセッサへのアクセス。ポリシー設定（デフォルトで有効）によりこの機能を制御し、H.264 エンコーディングのハードウェアエンコーディングを許可します（利用可能な場合）。該当するハードウェアが利用可能でない場合、VDA はソフトウェアビデオコーデックを使用して、CPU ベースのエンコーディングにフォールバックします。詳しくは、「グラフィックのポリシー設定」を参照してください。

DirectX、**Direct3D**、および **WPF** レンダリング

DirectX、Direct3D、および WPF レンダリングは、DDI（Display Driver Interface）Version 9ex、10、または 11 をサポートする GPU が搭載されたサーバーでのみ使用可能です。

- Windows Server 2008 R2 では、DirectX および Direct3D で単一 GPU を使用するために特別な設定は不要です。
- Windows Server 2012 以降の RD Session Host サーバー上のリモートデスクトップサービス（RDS）セッションでは、デフォルトのアダプターとして Microsoft 基本レンダリングドライバーが使用されます。Windows Server 2012 以降での RDS セッションで GPU を使用するには、グループポリシーの ［ローカルコンピューターポリシー］>［コンピューターの構成］>［管理用テンプレート］>［**Windows** コンポーネント］>［リモートデスクトップサービス］>［リモートデスクトップセッションホスト］>［リモートセッション環境］で ［すべてのリモートデスクトップサービスセッションにハードウェアの既定のグラフィックスアダプターを使用する］を有効にします。
- WPF アプリケーションでのレンダリングにサーバーの GPU を使用するようにするには、Windows マルチセッション OS セッションを実行するサーバー上でレジストリキーを設定します。レジストリの設定について詳しくは、レジストリを介して管理される機能の一覧にある「Windows Presentation Foundation（WPF）のレンダリング」を参照してください。

CUDA または **OpenCL** アプリケーション用の **GPU** アクセラレーション機能

ユーザーセッションで実行中の CUDA および OpenCL アプリケーションの GPU アクセラレーションは、デフォルトで無効です。

CUDA アクセラレーション POC 機能を使用するには、レジストリ設定を有効にします。詳しくは、レジストリを介して管理される機能の一覧にある「CUDA または OpenCL アプリケーション用の GPU アクセラレーション機能」を参照してください。

Windows シングルセッション OS のための GPU アクセラレーション

January 25, 2024

HDX 3D Pro を使用することで、グラフィックアプリケーションを仮想デスクトップ上で提供したりシングルセッションOS マシン上のアプリケーションとして配信したりできます。HDX 3D Pro は、物理ホストコンピューター（デスクトップ、ブレード、ラックワークステーションなど）と、XenServer、vSphere、Nutanix および Hyper-V（パススルーのみ）ハイパーバイザーが提供する GPU パススルーおよび GPU 仮想化技術をサポートします。

HDX 3D Pro の機能は以下のとおりです：

- WAN およびワイヤレス接続でのパフォーマンスを最適化する Adaptive H.264 ベースまたは H.265 ベースの深圧縮。HDX 3D Pro のデフォルトでは、CPU ベースの全画面 H.264 圧縮が使用されます。H.264 によるハードウェアエンコーディングは、NVENC をサポートする NVIDIA、Intel、AMD カードで使用されます。H.265 によるハードウェアエンコーディングは、NVENC をサポートする NVIDIA カードで使用されます。
- 特殊なユースケースのための無損失圧縮オプション。HDX 3D Pro では CPU ベースの無損失コーデックも提供され、医療用画像処理などピクセル単位での精密なグラフィックが求められるアプリケーションがサポートされます。真の無損失圧縮はネットワークおよび処理リソースに対する負荷が非常に高いため、特殊なユースケースでのみ使用することをお勧めします。

  無損失圧縮を使用すると、以下のように動作します。

  - 表示しているフレームに非可逆圧縮が適用されているのか無損失圧縮が適用されているのかを示すインジケーター（システムトレイアイコン）がユーザーの通知領域に表示されます。このアイコンは、ポリシーの ［表示品質］設定で ［操作時は低品質］が選択されている場合に便利です。送信されたフレームが無損失の場合、このインジケーターが緑色になります。
  - ユーザーは、無損失スイッチを使ってセッション内でいつでも［常に無損失］モードを有効にできます。セッション内で［無損失］を選択または選択解除するには、アイコンを右クリックして ［完全に無損失に切り替える］をクリックするか、ショートカット Alt+Shift+1 を使用します。

    無損失圧縮の場合：HDX 3D Pro では、ポリシーで指定されているコーデックに関係なく、無損失コーデックが使用されます。

    非可逆圧縮の場合：HDX 3D Pro では、デフォルトのコーデックまたはポリシーで指定されているコーデックが使用されます。

    無損失スイッチの設定は保持されず、次回のセッションではリセットされます。すべてのセッションで無損失コーデックが使用されるようにするには、ポリシーの ［表示品質］設定で ［常に無損失］を選択

します。

- デフォルトのショートカットである ALT+SHIFT+1 を無効にし、セッション内で無損失を選択または選択解除できます。HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\LLIndicator で新しいレジストリ設定を構成します。
  - 値の名前：HKEY_LOCAL_MACHINE_HotKey、種類：String
  - ショートカットの組み合わせを構成する形式は、C=0 | 1, A=0 | 1, S=0 | 1, W=0 | 1, K=val です。キーはコンマ「,」で区切る必要があります。キーの順番は関係ありません。
  - A、C、S、W、および K はキーです。ここで、C=Control、A=ALT、S=SHIFT、W=Win、および K=a が有効なキーです。K に対して使用できる値は、0～9、a～z、およびすべての仮想キーコードです。
  - 例：
    - F10 には、以下を設定します：K=0x79
    - Ctrl + F10 には、以下を設定します：C=1, K=0x79
    - Alt + A には、以下を設定します：A=1, K=a または A=1, K=A または K=A, A=1
    - Ctrl + Alt + 5 には、以下を設定します：C=1, A=1, K=5 または A=1, K=5, C=1
    - Ctrl + Shift + F5 には、以下を設定します：A=1, S=1, K=0x74

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

- 複数および高解像度モニターのサポート。シングルセッション OS マシンの場合、HDX 3D Pro では最大で 4 つのモニターが構成されたユーザーデバイスがサポートされます。ユーザーはそれらのモニターを自由に配置でき、解像度や向きが異なるモニターを組み合わせて使用できます。モニターの数は、ホストコンピューターの GPU、ユーザーデバイス、および使用できる帯域幅による制限を受けます。HDX 3D Pro では、ホストコンピューター上の GPU でサポートされるすべてのモニター解像度がサポートされます。
- 動的解像度仮想デスクトップまたはアプリケーションのウィンドウのサイズを任意に変更できます。注：解像度は、VDA のセッションウィンドウのサイズを変更することでのみ変更できます。VDA セッション内での解像度の変更（[コントロールパネル] > [デスクトップのカスタマイズ] > [ディスプレイ] > [画面の解像度] で変更）はサポートされていません。
- NVIDIA vGPU アーキテクチャのサポート。HDX 3D Pro は、NVIDIA vGPU カードをサポートしています。GPU パススルーと GPU 共有については「NVIDIA vGPU」を参照してください。NVIDIA vGPU を使用すると、複数の仮想マシンで単一の物理 GPU に同時に直接アクセスできます。このとき、仮想化されていないオペレーティングシステムで動作するものと同じ NVIDIA グラフィックドライバーが使用されます。
- Virtual Direct Graphics Acceleration（vDGA）を使った VMware vSphere および VMware ESX のサポート - RDS および VDI の両方のワークロードで、vDGA を使用する HDX 3D Pro がサポートされます。
- NVIDIA vGPU および AMD MxGPU を使用する VMware vSphere/ESX のサポート。

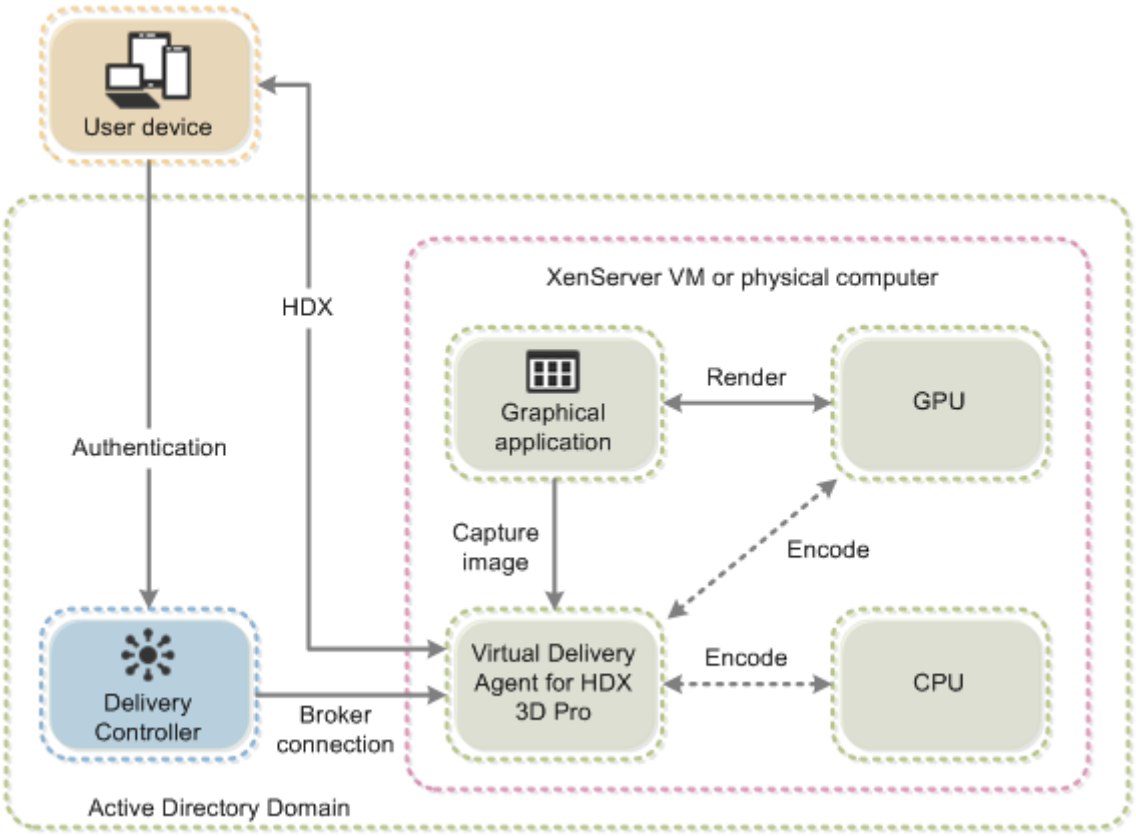
- Windows Server 2016 の Discrete Device Assignment を使用した Microsoft HyperV のサポート。
- Intel Xeon Processor E3 ファミリによるデータセンターグラフィックのサポート。HDX 3D Pro では、サポートされる Intel プロセッサファミリで、マルチモニター（最大 3 つ）、コンソールのブランキング、カスタム解像度、および高いフレームレートがサポートされます。詳しくは、「http://www.citrix.com/intel」および「http://www.intel.com/content/www/us/en/servers/data-center-graphics.html」を参照してください。
- AMD FirePro S シリーズのサーバーカードでの AMD RapidFire のサポート。HDX 3D Pro では、マルチモニター（最大 6 つ）、コンソールのブランキング、カスタム解像度、および高いフレームレートがサポートされます。注：HDX 3D Pro による AMD MxGPU（GPU 仮想化）のサポートで対応しているのは、VMware vSphere の vGPU のみです。GPU パススルーに対応しているのは、XenServer と Hyper-V です。詳しくは、「AMD 仮想化ソリューション」を参照してください。
- NVIDIA GPU の高パフォーマンスビデオエンコーダー、AMD GPU、Intel Iris Pro グラフィックプロセッサへのアクセス。この機能はポリシー設定（デフォルトで有効）によって制御されます。この機能により H.264 エンコーディングのハードウェアエンコーディングが許可されます（利用可能な場合）。該当するハードウェアが利用可能でない場合、VDA はソフトウェアビデオコーデックを使用して、CPU ベースのエンコーディングにフォールバックします。詳しくは、「グラフィックのポリシー設定」を参照してください。

以下の図を参照してください：

- ユーザーが Citrix Workspace アプリにログオンして仮想アプリケーションまたはデスクトップにアクセスすると、Controller でユーザーが認証されます。Controller は VDA for HDX 3D Pro にアクセスし、グラフィカルアプリケーションをホストしているコンピューターへの接続を仲介します。

VDA for HDX 3D Pro はホスト上の適切なハードウェアを使って、デスクトップ全体またはグラフィックアプリケーションだけのビューを圧縮します。

- デスクトップまたはアプリケーションのビューおよびそれに対するユーザーの応答は、ホストコンピューターとユーザーデバイス間で転送されます。この転送は、Citrix Workspace アプリと VDA for HDX 3D Pro の間の直接 HDX 接続を介して行われます。



HDX 3D Pro のユーザーエクスペリエンスの最適化

マルチモニター環境で HDX 3D Pro を使用するには、ユーザーデバイスに接続されているモニター数以上のモニターがホストコンピューター側に構成されている必要があります。ホストコンピューター側で構成されているモニターは、物理モニターまたは仮想モニターのどちらでも構いません。

ユーザーがグラフィックアプリケーションの仮想デスクトップまたはアプリケーションに接続している間は、ホストコンピューターにモニター（物理または仮想のいずれも）を接続しないでください。これを行うと、ユーザーのセッションが不安定になることがあります。

グラフィックアプリケーションセッションを実行しているときにデスクトップの解像度を変更しないようにユーザーに通知してください。アプリケーションセッションを閉じた後、［Citrix Workspace アプリ - Desktop Viewer 基本設定］ダイアログボックスで Desktop Viewer ウィンドウの解像度を変更できます。

ブランチオフィスなど、帯域幅が制限された接続を複数のユーザーで共有している場合、ポリシーの ［セッション全体の最大帯域幅］設定を使用して、各ユーザーが使用できる帯域幅を制限することをお勧めします。この設定により、ユーザーがログオンしたりログオフしたりするときに、使用可能な帯域幅が大きく変動しなくなります。HDX 3D Pro では使用可能なすべての帯域幅が使用されるため、ユーザーのセッション中に使用可能な帯域幅が大きく増減するとパフォーマンスが低下します。

たとえば、60Mbps の接続を 20 人のユーザーで共有する場合、各ユーザーが使用できる帯域幅は、同時接続ユーザ

ーの数に応じて 3Mbps～60Mbps の間で変動します。この場合におけるユーザーエクスペリエンスを最適化するには、各ユーザーがピーク時に必要とする帯域幅を調べて、常時この値でユーザーを制限します。

ユーザーが 3D マウスを使用する場合は、汎用 USB リダイレクト仮想チャネルの優先度を 0 にすることをお勧めします。仮想チャネルの優先度を変更する方法については、Knowledge Center のCTX128190を参照してください。

Thinwire

May 25, 2023

はじめに

Thinwire は Citrix HDX テクノロジの一部で、Citrix Virtual Apps and Desktops で使用される、Citrix のデフォルトのディスプレイリモートテクノロジです。

ディスプレイリモートテクノロジを使用すると、あるマシンで生成されたグラフィックが、通常はネットワークを経由して、別のマシンに転送され、表示されます。

正常なディスプレイリモートソリューションでは、ローカル PC と同様の、高度にインタラクティブなユーザーエクスペリエンスが提供されます。Thinwire では、幅広く複合的、効果的な画像解析および圧縮技術の使用により、これを実現しています。Thinwire ではサーバーのスケーラビリティが最大化され、消費する帯域幅は他のディスプレイリモートテクノロジより少なくできます。

このようなバランスの良さから、Thinwire は大部分の一般的なビジネスユースケースに合致しており、Citrix Virtual Apps and Desktops のデフォルトのディスプレイリモートテクノロジとして使用されています。

HDX 3D Pro

デフォルト設定では、Thinwire は 3D または高度にインタラクティブなグラフィックを提供し、グラフィック処理装置（GPU）を使用できます（存在する場合）。ただし、GPU を使用するシナリオでは、Citrix ポリシーの ［**3D** グラフィックの負荷の最適化］または ［表示品質］**>** ［操作時は低品質］ポリシーを使用して、HDX 3D Pro モードを有効にすることをお勧めします。これらのポリシーは、GPU が存在する場合、ハードウェアアクセラレーションを使用して、Thinwire がビデオコーデック（H.264 または H.265）で画面全体をエンコードできるよう構成します。これにより、3D Pro グラフィックは、より滑らかなエクスペリエンスを実現できます。詳しくは、「H.264 の［操作時は低品質］」、「HDX 3D Pro」および「Windows シングルセッション OS のための GPU アクセラレーション」を参照してください。

要件

Thinwire は、Windows Server 2012 R2、Windows Server 2016、Windows Server 2019、および Windows 10 など、最新のオペレーティングシステムに最適化されています。Windows Server 2008 R2 には、従来のグラフィックモードをお勧めします。ビルトインのCitrix ポリシーテンプレートである「高サーバースケーラビリティ - レガシ OS」と「WAN の最適化 - レガシ OS」を使用して、これらのユースケースに推奨されるポリシー設定の組み合わせを提供します。

> 注:
>
> このリリースでは、従来のグラフィックモードはサポートされていません。これは、XenApp 7.15 LTSR、XenDesktop 7.15 LTSR、および以前の VDA リリースを使用している場合の後方互換性のためにのみ含まれています。

- Thinwire の動作を制御する ［圧縮にビデオコーデックを使用する］ポリシー設定は、Citrix Virtual Apps and Desktops 7 1808 以降と XenApp および XenDesktop 7.6 FP3 以降の VDA バージョンで利用できます。Citrix Virtual Apps and Desktops 7 1808 以降と XenApp および XenDesktop 7.9 以降の VDA バージョンでは、［選択された場合ビデオコーデックを使用する］オプションがデフォルト設定になっています。
- Thinwire はすべての Citrix Workspace アプリでサポートされています。ただし、8 ビットまたは 16 ビットグラフィックで帯域幅の使用量が少なくなるなど、Thinwire の機能は Citrix Workspace アプリによってサポートの有無が異なることがあります。こうした機能のサポートは、Citrix Workspace アプリによって自動的にネゴシエートされます。
- Thinwire は、マルチモニターおよび高解像度のシナリオで、より多くのサーバーリソース（CPU、メモリ）を使用します。Thinwire が使用するリソース量は調整可能ですが、帯域幅の使用状況がその結果増大することがあります。
- 低帯域幅または高遅延のシナリオでは、8 または 16 ビットグラフィックを有効にして対話操作性を改善することを検討できます。表示品質は、特に 8 ビットの色数で影響を受けることがあります。

エンコーディング方法

Thinwire は、ポリシーとクライアントの機能に応じて、2 つの異なるエンコーディングモードで動作できます。

- 全画面 H.264 または H.265 による Thinwire
- 選択的な H.264 または H.265 による Thinwire

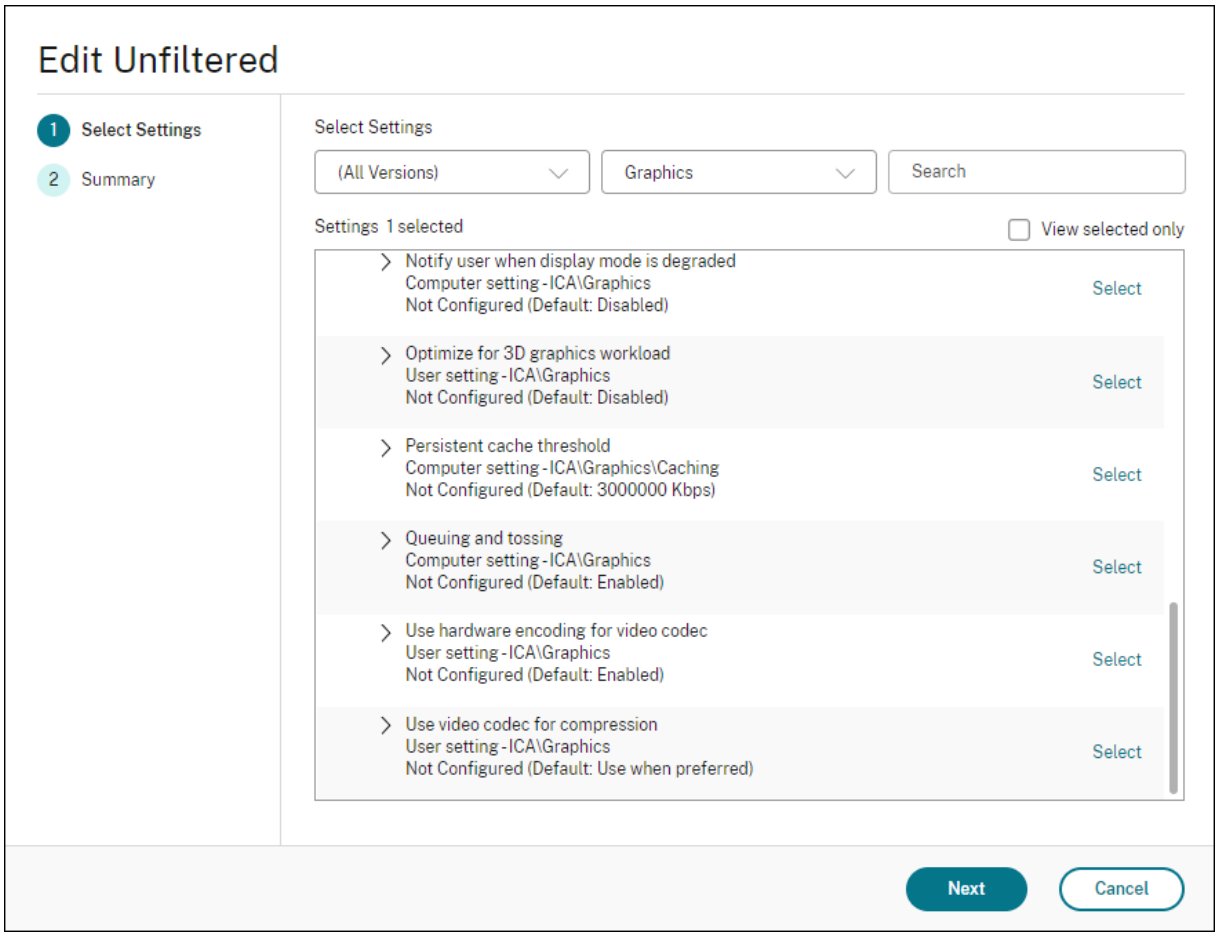
従来の GDI リモート処理では、Thinwire ビットマップエンコーダーではなく XPDM リモート処理ドライバーが使用されます。

構成

Thinwire はデフォルトのディスプレイリモートテクノロジです。

次のグラフィックポリシー設定はデフォルトを設定し、さまざまなユースケースに代替選択肢を提供します。

- 圧縮にビデオコーデックを使用する
  - 選択された場合ビデオコーデックを使用するこれがデフォルトの設定です。追加の構成は必要ありません。この設定をデフォルトとして保持することにより、すべての Citrix 接続で Thinwire が選択され、デスクトップの一般的なワークロードで、スケーラビリティ、帯域幅、および優れた画質の点で、確実に最適化されます。これは、機能的に ［領域をアクティブに変更］と同等です。
- このポリシー設定の他のオプションは、さまざまなユースケースで他のテクノロジと組み合わせて Thinwire を使用し続けます。例:
  - ［領域をアクティブに変更］。Thinwire の状況に応じたディスプレイテクノロジは、動画（ビデオ、3D インモーション）を識別し、画像が動く画面の部分でのみ H.264 または H.265 を使用します。
  - ［画面全体に使用］。特に 3D グラフィックを多用する事例で、Thinwire を全画面 H.264 または H.265 を使用して配信し、ユーザーエクスペリエンスと帯域幅を最適化します。H.264 4:2:0（［視覚的無損失］ポリシーが無効）の場合、最終イメージは完全に無損失ではなく、特定のシナリオには適さないことがあります。このような場合は、代わりにH.264 の［操作時は低品質］ を使用することを検討してください。



次の視覚表示ポリシー設定など、いくつかの他のポリシー設定は、ディスプレイリモートテクノロジのパフォーマンスを微調整するために使用できます。Thinwire はこれらすべてをサポートします。

- 簡素なグラフィックに対する優先的色の解像度

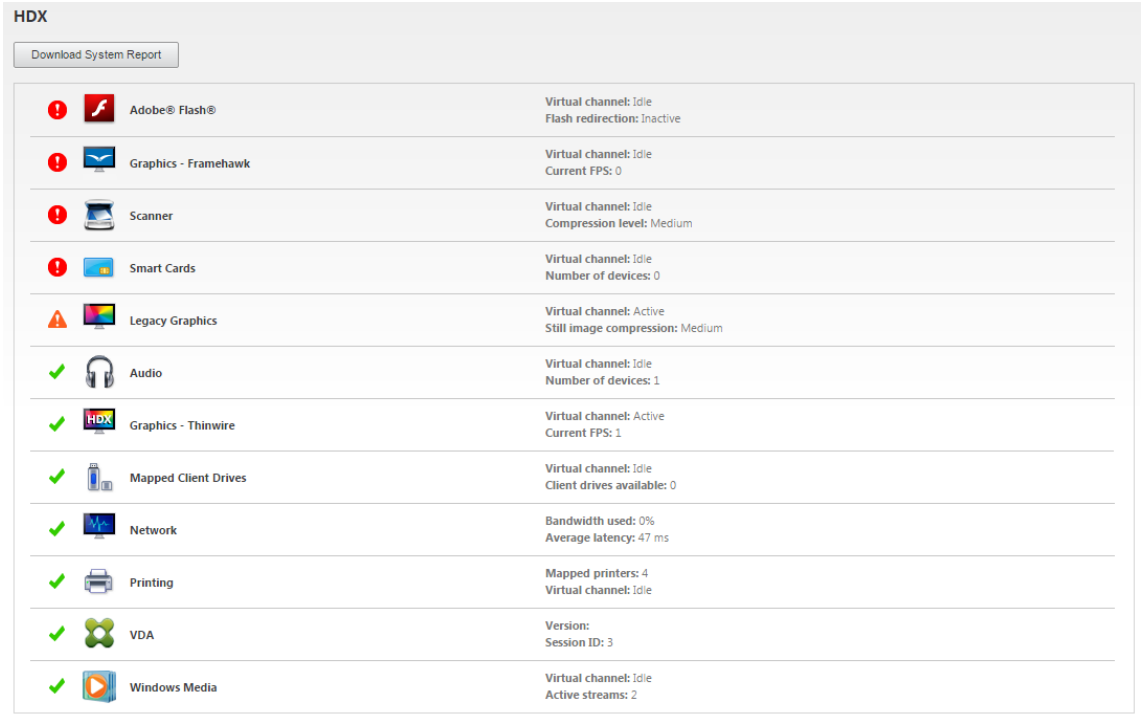
- ターゲットフレーム数
- 表示品質

さまざまなビジネスユースケースに対して Citrix で推奨されるポリシー設定の組み合わせを取得するには、組み込みのCitrix ポリシーテンプレートを使用します。「高サーバースケーラビリティ」および「最高品位ユーザーエクスペリエンス」テンプレートはどちらも、組織の優先順位やユーザーの予期に最も適したポリシー設定との組み合わせで Thinwire を使用します。

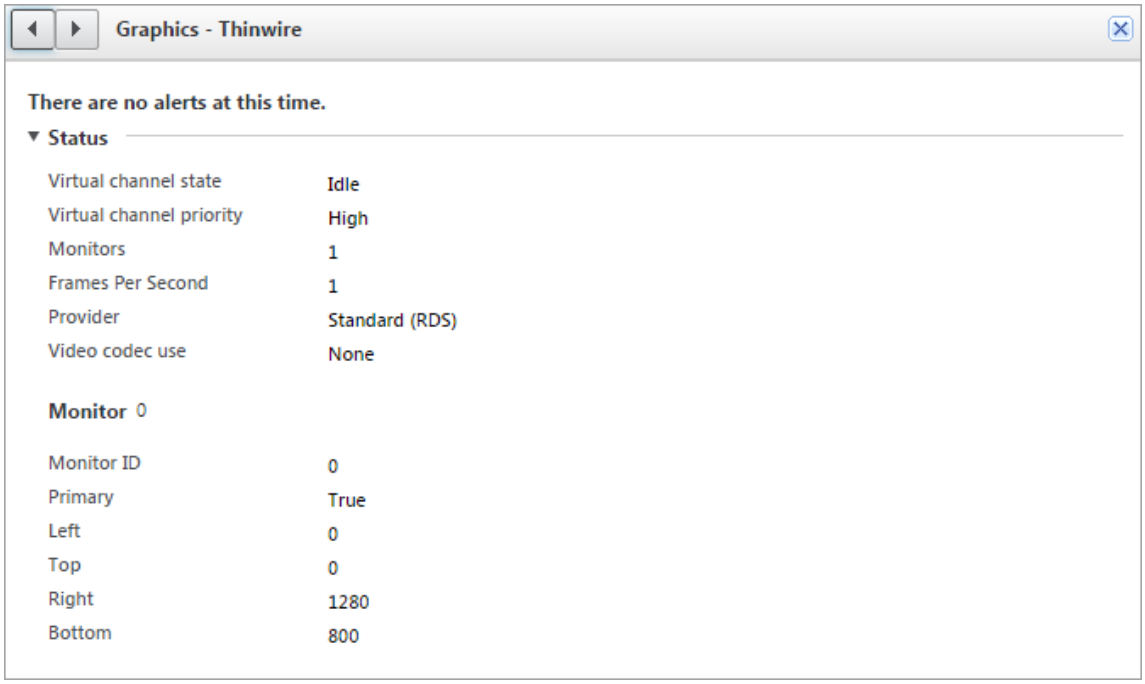
Thinwire のモニター

Citrix Director から Thinwire の利用状況とパフォーマンスをモニターすることができます。HDX 仮想チャネル詳細ビューには、あらゆるセッションで、Thinwire のトラブルシューティングやモニターに役立つ情報が表示されます。Thinwire 関連の測定基準を表示するには:

1. Director で、ユーザー、マシン、またはエンドポイントを検索し、アクティブなセッションを開いて ［詳細］をクリックします。または、［フィルター］**>** ［セッション］**>** ［すべてのセッション］を選択し、アクティブなセッションを開いて ［詳細］をクリックすることもできます。
2. ［**HDX**］パネルまで下にスクロールします。



3. ［グラフィック **- Thinwire**］を選択します。



無損失圧縮コーデック（**MDRLE**）

通常のデスクトップセッションでは、画面の大半が単純なグラフィックまたはテキスト領域です。Thinwire はこれらの領域の範囲を決定し、2DRLE コーデックを使用して無損失エンコーディングの領域を選択します。Citrix Workspace アプリのクライアント側では、これらの要素は、セッション表示時に Citrix Workspace アプリ側の 2DRLE デコーダーを使用してデコードされます。

XenApp および XenDesktop 7.17 では、より高い圧縮率の MDRLE コーデックが追加されており、通常のデスクトップセッションでは 2DRLE コーデックよりも少ない帯域幅しか消費しません。この新しいコーデックは、サーバーの拡張性には影響を与えることはありません。

消費帯域幅が抑えられるため、通常、（特に共有リンクまたは制約付きリンクで）セッションのインタラクティブ性が向上するとともに、コストを削減できます。たとえば、MDRLE コーデック使用時の予想される帯域幅消費量は、Office などの一般的なワークロードの場合、XenApp および XenDesktop 7.15 LTSR と比較して約 10～15%少なくなります。

MDRLE コーデックには構成は不要です。Citrix Workspace アプリで MDRLE デコードがサポートされている場合、VDA では、VDA の MDRLE エンコードと Citrix Workspace アプリの MDRLE デコードが使用されます。Citrix Workspace アプリで MDRLE デコードがサポートされていない場合、VDA では、自動的に 2DRLE エンコードにフォールバックされます。

MDRLE の要件:

- Citrix Virtual Apps and Desktops: VDA バージョン 7 1808 以降
- XenApp および XenDesktop: VDA バージョン 7.17 以降
- Windows 向け Citrix Workspace アプリ: バージョン 1808 以降

- Citrix Receiver for Windows バージョン 4.11 以降

プログレッシブモード

Citrix Virtual Apps and Desktops 1808 では、プログレッシブモードが導入され、デフォルトで有効になっています。制約のあるネットワーク環境（デフォルト：帯域幅 <2Mbps、または遅延 >200 ミリ秒）では、Thinwire が圧縮するテキストや静止画の量が増えて、画面アクティビティの対話操作性が改善されます。画面アクティビティが停止すると、大幅に圧縮されたテキストや画像は、その後徐々に、ランダムなブロック単位でシャープになります。このような方法で圧縮およびシャープ化して総合的な対話操作性を改善しながら、キャッシュ使用を低減し帯域幅の使用を増やしていきます。

Citrix Virtual Apps and Desktops 1906 の場合、プログレッシブモードはデフォルトで無効になっています。現在は、別のアプローチを使用しています。静止画の画質は、現在、ネットワーク状況に基づいて ［表示品質］設定ごとに事前定義された最小値および最大値の間で変化します。明示的なシャープ化の手順が存在しないため、Thinwire は、プログレッシブモードの利点をほぼすべて提供しながら画像配信を最適化し、キャッシュ効率を維持します。

プログレッシブモードの動作を変更する

プログレッシブモードの状態は、レジストリキーを使用して変更できます。詳しくは、レジストリを介して管理される機能の一覧にある「プログレッシブモード」を参照してください。

H.264 の［操作時は低品質］

［操作時は低品質］は、対話操作性のために画像配信や最終イメージの品質を最適化する Thinwire の特別な構成です。［表示品質］ポリシーを ［操作時は低品質］に設定することで有効にできます。

［操作時は低品質］の設定は画面のアクティビティ中に H.264（または H.265）を使用して画面を圧縮し、アクティビティが停止すると完全な無損失へシャープ化します。可能な限り最高のフレーム数を維持するために、使用可能なリソースの H.264（または H.265）画質に適応します。シャープ化の手順は、手順の開始後にユーザーが画面のアクティビティを開始した場合でも対応できるように、徐々に行われます。たとえば、モデルを選択してから、それを回転させる場合などです。

H.264 の ［操作時は低品質］では、ハードウェアアクセラレーションのような全画面 H.264 または H.265 のすべての利点を利用できますが、最終的な、無損失画面は保証されていません。これは、完全に無損失な最終イメージが必要な 3D タイプのワークロードにとって重要なポイントです。たとえば、医療画像を操作する場合です。また、H.264 の ［操作時は低品質］は全画面 H.264 4:4:4 よりも少ないリソースを使用します。その結果、［操作時は低品質］を使用すると通常、視覚的無損失 H.264 4:4:4 よりもフレーム数が多くなります。

> 注:
>
> ［表示品質］ポリシーに加えて ［圧縮にビデオコーデックを使用する］ポリシーを ［可能であれば使用］（デフォルト）または ［領域をアクティブに変更］に設定します。［圧縮にビデオコーデックを使用する］ポリシーを

> ［ビデオコーデックを使用しない］に設定して H.264 以外の［操作時は低品質］に戻すことができます。これによって動画は H.264（または H.265）の代わりに JPEG でエンコードされます。

テキストベースのセッションウォーターマーク

March 30, 2022

テキストベースのセッションウォーターマークは、データ盗難を防止し、追跡できるようにするために役立ちます。この情報は追跡可能であり、セッションデスクトップに表示されることで、データを盗むために写真やスクリーンキャプチャを使用する場合の抑止力になります。テキストのレイヤーであるウォーターマークは自分で指定できます。ウォーターマークは元のドキュメントのコンテンツを変更することなく、セッション画面全体に表示されます。テキストベースのセッションウォーターマークには、VDA サポートが必要です。

> 重要:
>
> テキストベースのセッションウォーターマーキングは、セキュリティ機能ではありません。このソリューションは、データ盗難を完全に防止するものではありませんが、ある程度の抑止力とトレーサビリティを提供します。この機能の使用時の完全な情報トレーサビリティが保証されるわけではありませんが、この機能を他のセキュリティソリューションと適切に組み合わせることをお勧めします。

セッションウォーターマークはテキストであり、ユーザーに配信されるセッションに適用されます。セッションウォーターマークによって、データ盗難を追跡するための情報が伝えられます。最も重要なデータは、画面イメージが撮影された現在のセッションのログオンユーザーの ID です。データ漏洩をより効果的に追跡するには、サーバーまたはクライアントのインターネットプロトコルアドレスや接続時間などのその他の情報を含めます。

ユーザーエクスペリエンスを調整するには、［セッションウォーターマーク］ポリシー設定を使用して、画面上の配置とウォーターマークの外観を構成します。

要件:

Virtual Delivery Agent:

マルチセッション OS 7.17
シングルセッション OS 7.17

制限事項:

- セッションウォーターマークは、ローカルアプリケーションアクセス、Windows Media リダイレクト、MediaStream、Web ブラウザーコンテンツリダイレクト、および HTML5 ビデオリダイレクトが使用されるセッションではサポートされていません。セッションウォーターマークを使用するには、これらの機能が無効になっていることを確認してください。
- 全画面ハードウェアアクセラレーションモード（全画面 H.264 または H.265 エンコーディング）でセッションが実行されている場合は、セッションウォーターマークはサポートされておらず、表示されません。

- これらの HDX ポリシーを設定すると、ウォーターマーク設定が有効にならず、ウォーターマークがセッション画面に表示されません。

［ビデオコーデックにハードウェアエンコーディングを使用します］を ［有効］
［圧縮にビデオコーデックを使用する］を ［画面全体に使用］

- これらの HDX ポリシーを設定すると、動作が不確定となり、ウォーターマークが表示されないことがあります。

  ［ビデオコーデックにハードウェアエンコーディングを使用します］を ［有効］
  ［圧縮にビデオコーデックを使用する］を ［画面全体に使用］

  ウォーターマークが表示されるようにするには、［ビデオコーデックにハードウェアエンコーディングを使用します］を ［無効］に設定するか、または ［圧縮にビデオコーデックを使用する］を ［領域をアクティブに変更］か ［ビデオコーデックを使用しない］に設定します。

- セッションウォーターマークは、Thinwire グラフィックモードのみをサポートします。
- ［Session Recording］を使用する場合、録画されたセッションにウォーターマークは含まれません。
- Windows リモートアシスタンスを使用している場合、ウォーターマークは表示されません。
- ユーザーが **Print Screen** キーを押して画面をキャプチャした場合、VDA 側でキャプチャされる画面にウォーターマークは含まれません。キャプチャされたイメージがコピーされるのを防ぐために対策を講じることをお勧めします。

マルチメディア

April 22, 2022

HDX 技術スタックは、マルチメディアアプリケーションの配信を次の 2 つの相補的なアプローチでサポートします。

- サーバー側でレンダリングするマルチメディア配信
- クライアント側でレンダリングするマルチメディアリダイレクト

これにより、良好なユーザーエクスペリエンスを保ちながら、サーバースケーラビリティを向上させ、ユーザーごとのコストを削減するあらゆる種類のマルチメディアフォーマットを配信できます。

サーバー側でレンダリングするマルチメディア配信で、オーディオとビデオコンテンツは、アプリケーションによって Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）サーバー上でデコードおよびレンダリングされます。コンテンツは圧縮され、ICA プロトコルでユーザーデバイス上の Citrix Workspace アプリに配信されます。この方法は、さまざまなアプリケーションとメディア形式に対して、最大レートの互換性を提供します。ビデオ処理は数値計算であるため、サーバー側でレンダリングされたマルチメディア配信はオンボードのハードウェアアクセラレーションの利点を大幅に活かすことがきます。たとえば、DirectX Video Acceleration（DXVA）のサポートは、

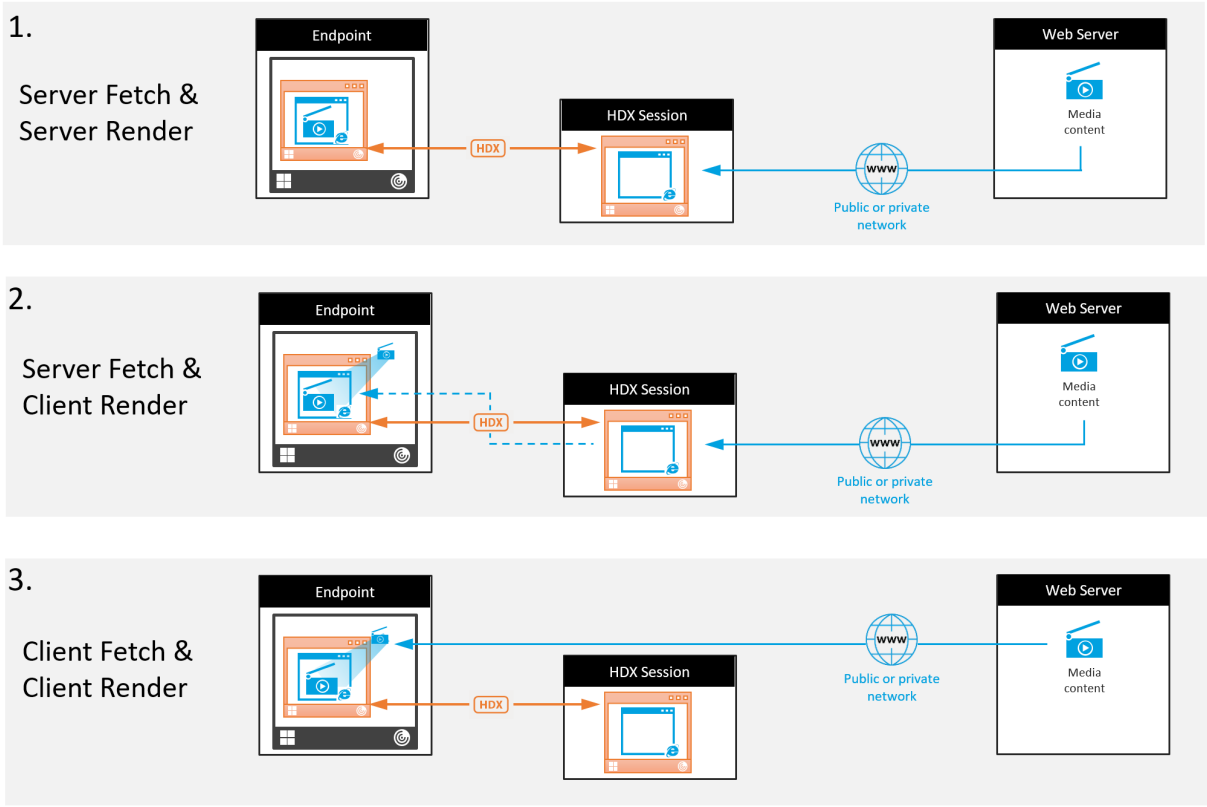
H.264 デコーディングを別のハードウェアで実行することで、CPU をオフロードします。Intel Quick Sync、AMD RapidFire、NVIDIA NVENC の機能により、ハードウェアアクセラレーション用の H.264 エンコーディングが利用できるようになりました。

ほとんどのサーバーにビデオ圧縮用のハードウェアアクセラレーションがないため、すべてのビデオ処理をサーバーの CPU で実行する場合は、サーバースケーラビリティに悪影響を及ぼします。多くのマルチメディア形式をユーザーデバイスにリダイレクトしてローカル側でレンダリングするようにすれば、高サーバースケーラビリティを維持できます。

- Windows Media リダイレクトは、一般的に Windows Media Player に関連した、さまざまな種類のメディア形式に対してサーバーをオフロードします。
- HTML5 ビデオが普及し、Citrix はこのタイプのコンテンツに対してリダイレクトテクノロジを導入しました。HTML5、HLS、DASH、または WebRTC を使用している Web サイトについては、Web ブラウザーコンテンツのリダイレクトをお勧めします。
- 一般的なアドレス帳リダイレクト機能である、ホストからクライアントへのリダイレクトとローカルアプリアクセスを、マルチメディアコンテンツに応用できます。

これらの機能を含めて、リダイレクトを構成しない場合は、HDX はサーバー側でのレンダリングを実行します。
リダイレクトを構成する場合、HDX はサーバー側でフェッチし、クライアント側でレンダリング、またはクライアント側でフェッチし、クライアント側でレンダリングのいずれかを実行します。これらの方法が失敗した場合、HDX は必要に応じてサーバー側でのレンダリングにフォールバックし、フォールバック防止ポリシーの対象になります。

サンプルシナリオ



シナリオ **1.**（サーバー側でフェッチし、サーバー側でレンダリング）**:**

1. サーバーはメディアファイルをソースからフェッチし、デコードし、コンテンツをオーディオデバイスまたはディスプレイデバイスに対して再生します。
2. サーバーは再生されたイメージまたはサウンドをディスプレイデバイスまたはオーディオデバイスからそれぞれ抽出します。
3. オプションとしてサーバーが抽出されたファイルを圧縮し、クライアントに送信します。

このアプローチでは、（抽出されたイメージやサウンドが効率的に圧縮されていない場合は）高 CPU コストと高帯域幅コストを負担することになり、サーバースケーラビリティは低くなります。

Thinwire とオーディオの仮想チャネルがこのアプローチを処理します。このアプローチの利点により、クライアントのハードウェアとソフトウェアの要件が削減されます。このアプローチでは、デコーディングはサーバーで実行され、より多くの種類のデバイスとフォーマットに対応します。

シナリオ **2.**（サーバー側でフェッチし、クライアント側でレンダリング）**:**

このアプローチは、オーディオまたはディスプレイデバイスに対してデコードおよび再生される前に、メディアコンテンツをインターセプトできることを前提としています。圧縮されたオーディオ/ビデオコンテンツは、クライアントに送信され、ローカルでデコードおよび再生されます。このアプローチの利点により、クライアントデバイスにオフロードされ、サーバーの CPU サイクルが節約されます。

ただし、このアプローチでは、クライアントにハードウェアとソフトウェアの要件が一部追加されます。クライアントは、受信する可能性のあるそれぞれのフォーマットをデコードできる必要があります。

シナリオ **3.**（クライアント側でフェッチし、クライアント側でレンダリング）**:**

このアプローチは、ソースからフェッチされる前に、メディアコンテンツの URL をインターセプトできることを前提としています。URL は、メディアコンテンツがローカルでフェッチ、デコード、および再生されたクライアントに送信されます。このアプローチは概念的に単純です。この利点により、制御コマンドのみがサーバーから送信されるため、サーバーの CPU サイクルと帯域幅の両方が節約されます。ただし、メディアコンテンツは、クライアントに常にアクセスできるわけではありません。

フレームワークとプラットフォーム**:**

シングルセッションオペレーティングシステム（Windows、Mac OS X、および Linux）は、マルチメディアアプリケーションのよりすばやい開発を可能にする、マルチメディアフレームワークを提供します。次の表に、より一般的なマルチメディアフレームワークの一部を示します。各フレームワークはメディア処理を複数の段階に分割して、パイプラインベースのアーキテクチャを使用します。

フレームワーク	プラットフォーム
DirectShow	Windows（98 以降）
Media Foundation	Windows（Vista 以降）
Gstreamer	Linux
Quicktime	Mac OS X

メディアリダイレクト機能によるダブルホップのサポート

	オーディオリダイレクト	いいえ
	ブラウザーコンテンツリダイレクト	いいえ
	HDX Web カメラリダイレクト	はい
	HTML5 ビデオリダイレクト	はい
	Windows Media リダイレクト	はい

オーディオ機能

September 30, 2022

ポリシーに以下の Citrix 設定項目を追加して、HDX のオーディオ機能を最適化できます。これらの設定項目の使用方法、およびほかのポリシー設定項目との依存関係について詳しくは、「オーディオのポリシー設定」、「帯域幅のポリシー設定」、「マルチストリーム接続のポリシー設定」を参照してください。

> 重要:
>
> TCP ではなくユーザーデータグラムプロトコル（UDP）を使用してオーディオを配信することをお勧めします。UDP を使用したオーディオをサポートしているのは、Windows Virtual Delivery Agent（VDA）のみです。
>
> DTLS を使用した UDP オーディオ暗号化は、Citrix Gateway と Citrix Workspace アプリ間でのみ有効です。このため、TCP トランスポートを使用した方が望ましい場合もあります。TCP では、VDA と Citrix Workspace アプリ間の、エンドツーエンドの TLS 暗号化がサポートされます。

音質

一般的に、音質を高くするほど、オーディオデータの転送に必要な帯域幅が大きくなり、サーバーの CPU にも負担がかかります。オーディオデータを圧縮すると、セッションのパフォーマンスと音質とのバランスを考慮しながら、ユーザーの操作感を最適化できます。これを行うには、サウンドファイルに適用する圧縮レベルを制御するには、Citrix ポリシーを使用します。

デフォルトでは、TCP トランスポート使用時の ［音質］ポリシー設定は［高 - 高品位オーディオ］に設定されています。UDP トランスポート使用時（推奨）は［中 - スピーチに最適化］に設定されています。高品位オーディオ設定では HiFi ステレオオーディオが提供されますが、ほかの品質設定よりも多くの帯域幅が消費されます。最適化されていないボイスチャットアプリケーションやビデオチャットアプリケーション（ソフトフォンなど）では、この音質を使用しないでください。リアルタイム通信に適していないオーディオパスに遅延が発生する可能性があるためです。選択されたトランスポートプロトコルに関係なく、リアルタイムオーディオには「スピーチに最適化」ポリシー設定をお勧めします。

衛星、ダイヤルアップ接続など帯域幅が制限されている場合、音質を ［低］に設定することで、帯域幅の消費を最小限に抑えることができます。この状況では、低帯域幅接続のユーザーに対して別のポリシーを作成し、高帯域幅接続のユーザーに影響しないようにします。

設定について詳しくは、「オーディオのポリシー設定」を参照してください。ユーザーデバイス側の［クライアント側オーディオ設定］が有効になっていることを確認してください。

オーディオの再生と録音の帯域幅ガイドライン:

- 高品質（デフォルト）
  - ビットレート: 再生では約 100kbps（最小 75、最大 175 kbps）、マイクキャプチャでは約 70kbps

  - チャンネル数：再生用 2（ステレオ）、マイクキャプチャ用 1（モノラル）
  - 周波数：44100Hz
  - ビット深度：16 ビット

- 中品質（VoIP 用に推奨）
  - ビットレート：再生では約 16kbps（最小 20、最大 40kbps）、マイクキャプチャでは約 16kbps
  - チャンネル数：再生とキャプチャの両方で 1（モノラル）
  - 周波数：16000Hz（ワイドバンド）
  - ビット深度：16 ビット

- 低品質
  - ビットレート：再生では約 11kbps（最小 10、最大 25kbps）、マイクキャプチャでは約 11kbps
  - チャンネル数：再生とキャプチャの両方で 1（モノラル）
  - 周波数：8000Hz（狭帯域）
  - ビット深度：16 ビット

クライアントオーディオリダイレクト

サーバー上で実行しているアプリケーションからユーザーデバイス上のスピーカーまたはサウンドデバイスでオーディオが再生されるようにするには、［クライアントオーディオリダイレクト］設定を ［許可］のままにしておきます。これがデフォルトの設定です。

クライアントオーディオマッピングを使用すると、サーバーとネットワークに大きな負荷がかかります。ただし、［クライアントオーディオリダイレクト］設定で［禁止］を選択すると、すべての HDX オーディオ機能が無効になります。

設定について詳しくは、「オーディオのポリシー設定」を参照してください。ユーザーデバイス側の［クライアント側オーディオ設定］が有効になっていることを確認してください。

クライアントマイクリダイレクト

ユーザーデバイス上のマイクなどのサウンド入力デバイスを使って録音できるようにするには、［クライアントマイクリダイレクト］設定をデフォルトのまま（[許可]）にします。

セキュリティ上の理由から、ユーザーデバイスとの信頼関係が設定されていないサーバーがマイクを使用しようとすると、警告メッセージが表示されます。ユーザーは、マイクを使用する前にアクセスを許可するか拒否するかを選択できます。この警告は、ユーザーが Citrix Workspace アプリ側で無効にできます。

設定について詳しくは、「オーディオのポリシー設定」を参照してください。ユーザーデバイス側の［クライアント側オーディオ設定］が有効になっていることを確認してください。

オーディオプラグアンドプレイ

ポリシーの［オーディオプラグアンドプレイ］設定では、録音やサウンド再生のための複数のオーディオデバイスの使用を許可または禁止します。この設定項目は、デフォルトで［有効］になっています。［オーディオプラグアンドプレイ］の機能を使用すると、ユーザーのセッションが開始されるまでプラグを差し込んだ状態にしなくても、オーディオデバイスを認識できます。

この設定項目は、Windows マルチセッション OS マシンのみに適用されます。

設定について詳しくは、「オーディオのポリシー設定」を参照してください。

オーディオリダイレクトの最大帯域幅（**Kbps**）とオーディオリダイレクトの最大帯域幅（**%**）

ポリシーの［オーディオリダイレクトの最大帯域幅（Kbps）］設定では、クライアント側デバイスによるオーディオの再生や録音で使用可能な最大帯域幅を、キロビット/秒（Kbps）単位で指定します。

ポリシーの［オーディオリダイレクトの最大帯域幅（%）］設定では、クライアント側デバイスによるオーディオの再生や録音で使用可能な最大帯域幅を、セッション全体に対する割合で指定します。

これらの設定には、デフォルトで 0 が指定されており、帯域幅に制限はありません。両方の設定を構成した場合、より高い制限（より小さい値）の設定が適用されます。

設定について詳しくは、「帯域幅のポリシー設定」を参照してください。ユーザーデバイス側の［クライアント側オーディオ設定］が有効になっていることを確認してください。

UDP でのオーディオリアルタイムトランスポートとオーディオ **UDP** ポートの範囲

ポリシーの［UDP でのオーディオリアルタイムトランスポート］設定は、デフォルトで［有効］が選択されています（インストール時に選択した場合）。これにより、サーバーの UDP ポートが開き、［UDP でのオーディオリアルタイムトランスポート］設定が有効な接続でそのポートが使用されます。ネットワークで輻輳やパケット損失が生じる場合、最適なユーザーエクスペリエンスを提供するために、オーディオの UDP/RTP を構成することをお勧めします。ソフトフォンアプリケーションなどのリアルタイムオーディオでは、EDT より UDP オーディオが優先されます。UDP は再送のないパケット損失が認められており、パケット損失が頻繁な場合でも接続に遅延が発生しません。

> 重要：
>
> Citrix Gateway がパス上にない場合、UDP で転送されるオーディオデータは暗号化されません。Citrix Gateway が Citrix Virtual Apps and Desktops のリソースにアクセスするよう構成されている場合、エンドポイントデバイスと Citrix Gateway 間のオーディオトラフィックは DTLS プロトコルで保護されます。

ポリシーの［オーディオ UDP ポートの範囲］設定では、Windows VDA でユーザーデバイスとのオーディオパケットデータの送受信に使用されるポート番号の範囲を指定します。

デフォルトでは、16500～16509 の範囲が指定されています。

［UDP でのオーディオリアルタイムトランスポート］について詳しくは、「オーディオポリシーの設定」を参照してください。［オーディオ UDP ポートの範囲］について詳しくは、「マルチストリーム接続のポリシー設定」を参照してください。ユーザーデバイス側の［クライアント側オーディオ設定］が有効になっていることを確認してください。

UDP を使用したオーディオには、Windows VDA が必要です。Linux VDA でサポートされているポリシーについては、「ポリシーサポート一覧」を参照してください。

ユーザーデバイス側のオーディオ設定ポリシー

1. 「グループポリシーオブジェクトテンプレート管理用テンプレートの構成」の手順に従って、グループポリシーテンプレートをロードします。
2. グループポリシーエディターで、［管理用テンプレート］**>** ［**Citrix Components**］**>** ［**Citrix Workspace**］**>** ［ユーザーエクスペリエンス］の順に開きます。
3. ［**Client audio settings**］を開き、［未構成］、［有効］、または［無効］をクリックします。
   - 未構成。デフォルトでは、オーディオリダイレクトは高品質オーディオ、または以前に構成したカスタムのオーディオ設定で有効になります。
   - 有効。オーディオリダイレクトは、選択したオプションで有効になります。
   - 無効。オーディオリダイレクトは無効化されます。
4. ［有効］をクリックした場合は、音質を選択します。UDP オーディオでは、［中］（デフォルト）を使用してください。
5. UDP オーディオでは、［**Enable Real-Time Transport**］チェックボックスをオンにして、ローカルの Windows ファイアウォールを通過するための着信ポートの範囲を指定します。
6. Citrix Gateway で UDP オーディオを使用するには、［ゲートウェイ経由でのリアルタイムトランスポートを許可する］チェックボックスをオンにします。Citrix Gateway で DTLS を構成します。詳しくは、こちらの記事を参照してください。

エンドポイントデバイスで上記の変更を行う制御権を持っていない場合、管理者として StoreFront の default.ica 属性を使用して UDP オーディオを有効にします。たとえば、自分のデバイスや家庭のコンピューターを持ち込む場合などです。

1. StoreFront マシンで、メモ帳などのエディターを使用して C:\inetpub\wwwroot\Citrix\< ストア名 >\App_Data\default.ica を開きます。ストア名 >
2. ［アプリケーション］セクションで以下の項目を入力します。

   ; リアルタイム転送を有効にします

   EnableRtpAudio=true

   ; ゲートウェイを介したリアルタイム転送を有効にします

   EnableUDPThroughGateway=true

   ;Audio quality を「Medium」に設定します

AudioBandwidthLimit=1

;UDP ポートの範囲を表します

RtpAudioLowestPort=16500

RtpAudioHighestPort=16509

ユーザーデータグラムプロトコル（UDP）オーディオは、default.ica の編集で有効になっている場合、そのストアを使用するすべてのユーザーに対して有効化されます。

マルチメディア会議でのエコーの解消

オーディオまたはビデオ会議にユーザーが参加したときに、音声にエコーがかかって聞こえることがあります。通常、この問題はスピーカーとマイクが近すぎる場合に発生します。このため、オーディオまたはビデオ会議ではヘッドセットを使用することをお勧めします。

HDX には、会議中のエコーを最小限に抑えるためのエコーキャンセル機能が用意されており、デフォルトで有効になっています。エコーキャンセル機能の効果は、スピーカーとマイクとの距離により異なります。デバイスが互いに近すぎたり遠すぎたりしないように注意してください。

エコーキャンセル機能を無効にするには、レジストリ設定を変更します。詳しくは、レジストリを介して管理される機能の一覧にある「マルチメディア会議でのエコーの解消」を参照してください。

ソフトフォン

ソフトフォンは、電話インターフェイスとして動作するソフトウェアです。コンピューターや他のスマートデバイスからインターネット経由で電話するには、ソフトフォンを使用します。ソフトフォンを使うことにより、画面を使って電話番号をダイヤルしたり、他の電話関連の機能を実行したりできます。

Citrix Virtual Apps and Desktops は、ソフトフォンの配信に対するいくつかの代替手段をサポートします。

- 制御モード。ホストされたソフトフォンが物理的な電話セットを制御します。このモードでは、Citrix Virtual Apps and Desktops サーバーを通過するオーディオトラフィックはありません。
- **HDX RealTime** に最適化されたソフトフォンのサポート（推奨）。このメディアエンジンはユーザーデバイス上で実行され、ボイスオーバー IP トラフィックがピアツーピアで流れます。たとえば、以下を参照してください：
  - Microsoft Teams の HDX 最適化
  - Microsoft Skype for Business の配信を最適化するHDX RealTime Optimization Pack
  - Cisco Jabber Softphone for VDI（旧称 VXME）
  - Cisco Webex Meetings for VDI
  - Avaya VDI Equinox（旧称 VDI Communicator）
  - Zoom VDI プラグイン

  - Genesys PureEngage Cloud
  - Nuance Dragon PowerMic ディクテーションデバイス

- ローカルアプリケーションアクセス。Citrix Virtual Apps and Desktops および Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）の機能により、ソフトフォンなどのアプリケーションは、Windows ユーザーのデバイス上ではローカルで実行されますが、その仮想/公開デスクトップとはシームレスに統合されています。これにより、ユーザーデバイスへのすべてのオーディオ処理の負荷が軽減されます。詳しくは、「ローカルアプリアクセスと URL リダイレクト」を参照してください。
- **HDX RealTime** の汎用ソフトフォンのサポート。ICA を介したボイスオーバー IP。

汎用ソフトフォンのサポート

汎用ソフトフォンのサポートにより、データセンターの XenApp または XenDesktop 上に、未変更のソフトフォンをホストすることができます。オーディオトラフィックは、Citrix ICA プロトコルを介して（UDP/RTP を優先的に使用して）、Citrix Workspace アプリを実行しているユーザーデバイスに送信されます。

汎用ソフトフォンのサポートは、HDX RealTime の機能です。ソフトフォンの配信に対するこのアプローチは、以下の場合に特に有効です。

- ソフトフォンの配信に最適なソリューションがなく、ローカルアプリケーションアクセスが可能な Windows デバイス上にユーザーがいない。
- ソフトフォンの最適化された配信に必要とされるメディアエンジンが、ユーザーデバイスにインストールされていないか、ユーザーデバイス上で実行しているオペレーティングシステムのバージョンで利用できない。このシナリオでは、汎用 HDX RealTime が価値のあるフォールバックソリューションを提供します。

Citrix Virtual Apps and Desktops を使用したソフトフォンの配信には、考慮事項が 2 つあります：

- ソフトフォンアプリケーションがどのように仮想/公開デスクトップに配信されるか。
- ユーザーのヘッドセット、マイクロフォン、およびスピーカー、または USB 電話セット間でオーディオがどのように配信されるか。

Citrix Virtual Apps and Desktops には、汎用ソフトフォンの配信をサポートする多くのテクノロジが含まれています：

- リアルタイムオーディオの高速エンコードと帯域幅の効率性のための、スピーチに最適化されたコーデック。
- 遅延の少ないオーディオスタック。
- ネットワーク遅延が変動する場合、オーディオをスムーズにするサーバー側のジッターバッファー。
- QoS のパケットのタグ付け（DSCP および WMM）
  - RTP パケットの DSCP タグ付け（レイヤー 3）
  - WiFi の WMM タグ付け

Windows、Linux、Chrome、および Mac 向けの Citrix Workspace アプリの各バージョンは、ボイスオーバー IP にも対応しています。Windows 向け Citrix Workspace アプリは以下の機能を提供します：

- クライアント側のジッターバッファー - ネットワーク遅延が変動する場合でもオーディオを確実にスムーズにします。
- エコーキャンセル - ヘッドセットを使用しないユーザー向けに、マイクとスピーカの距離を調整します。
- オーディオプラグアンドプレイ - オーディオデバイスは、セッション開始前にプラグインする必要はありません。いつでもプラグインできます。
- オーディオデバイスルーティング - ユーザーはヘッドセットの音声通信以外に、スピーカーに着信音を直接送信できます。
- マルチストリーム ICA - ネットワーク上で柔軟なサービス品質ベースのルーティングを有効にします。
- ICA は、4 つの TCP と 2 つの UDP ストリームをサポートします。UDP ストリームの 1 つは、RTP 上でリアルタイムオーディオをサポートします。

Citrix Workspace アプリの機能の概要については、『Citrix Receiver Feature Matrix』を参照してください。

システム構成の推奨事項

クライアントのハードウェアとソフトウェア：音質の最適化のために、最新バージョンの Citrix Workspace アプリとアコースティックエコーキャンセル（AEC）付きの高品質なヘッドセットをお勧めします。
Windows、Linux、および Mac 向けの Citrix Workspace アプリの各バージョンは、ボイスオーバー IP に対応しています。また、Dell Wyse は ThinOS（WTOS）のボイスオーバー IP サポートを提供します。

CPU 検討事項：VDA 上の CPU 使用率を監視して、それぞれの仮想マシンに 2 つの仮想 CPU を割り当てる必要があるかどうかを決定します。
リアルタイムの音声およびビデオはデータ量が多いです。2 つの仮想 CPU を構成すると、スレッドの切り替え遅延を減らすことができます。そのため、Citrix Virtual Desktops VDI 環境で 2 つの vCPU を構成することをお勧めします。

物理 CPU はセッションを超えて共有できるため、2 つの仮想 CPU を持つことは、必ずしも物理 CPU の数を倍にすることではありません。

セッション画面の保持機能に使われる Citrix Gateway Protocol（CGP）により、CPU の消費も増加します。高品質のネットワーク接続では、この機能を無効にして、VDA の CPU 消費を削減することができます。前述のいずれの手順も、強力なサーバーでは必要ないかもしれません。

UDP オーディオ：UDP によるオーディオは、ネットワークの輻輳やパケット損失に対する強力な耐性を提供します。利用できるのであれば、TCP から代えることをお勧めします。

LAN/WAN の設定：ネットワークの適切な設定は、リアルタイムオーディオの高い品質には極めて重要です。
通常、過度のブロードキャストパケットはジッターを発生させる場合があるため、仮想 LAN（VLAN）を構成する必要があります。IPv6 が有効なデバイスでは、大量のブロードキャストパケットが発生する場合があります。IPv6 のサポートが不要な場合は、それらのデバイスで IPv6 を無効にできます。QoS（サービス品質）をサポートするように構成してください。

WAN 接続使用時の設定：LAN および WAN 接続を経由したボイスチャットを使用できます。
WAN 接続では、音質は接続の遅延、パケット損失、およびジッターにより異なります。WAN 接続を経由してソフトフォンを配信する場合、データセンターとリモートオフィス間には NetScaler SD-WAN を使用することをお勧めし

ます。これにより、高いサービス品質が維持されます。NetScaler SD-WAN は、UDP を含むマルチストリーム ICA をサポートします。また、単一の TCP ストリームの場合は、さまざまな ICA 仮想チャネルの優先度を識別し、優先度の高いリアルタイムの音声データを優先的に扱うことができます。

HDX 構成を検証するには、Director またはHDX Monitorを使用してください。

リモートユーザーの接続：Citrix Gateway は DTLS をサポートし、UDP/RTP トラフィックをネイティブに（TCP でカプセル化せずに）送信します。

ポート 443 を介した UDP トラフィックに対してファイアウォールを双方向に開きます。

コーデックの選択と帯域幅の消費：
ユーザーデバイスとデータセンターの VDA 間には、中品質オーディオとも呼ばれる、スピーチに最適化されたコーデック設定を使用することをお勧めします。VDA プラットフォームと IP-PBX 間では、ソフトフォンは構成またはネゴシエートされたコーデックを使用します。例：

- G711 の音質は高いものの、通話で 1 秒あたり 80～100 キロビットの帯域幅（ネットワークのレイヤー 2 のオーバーヘッドにより異なる）が必要になります。
- G729 の音質は高く、通話で 1 秒あたり 30～40 キロビットの低帯域幅（ネットワークのレイヤー 2 のオーバーヘッドにより異なる）が必要になります。

ソフトフォンアプリケーションの仮想デスクトップへの配信

XenDesktop 仮想デスクトップにソフトフォンを配信するには、次の 2 つの方法があります。

- アプリケーションは、仮想デスクトップイメージにインストールできます。
- アプリケーションは、Microsoft App-V を使用して、仮想デスクトップにストリーム配信できます。このアプローチでは、仮想デスクトップイメージに手が加えられないため、管理上の利点があります。仮想デスクトップにストリーム配信された後、アプリケーションはその環境で、通常の方法でインストールされたかのように実行されます。すべてのアプリケーションが App-V 互換であるわけではありません。

ユーザーデバイスとのオーディオの配信

汎用 HDX RealTime は、ユーザーデバイスとのオーディオの配信を次の 2 つの方法でサポートします。

- **Citrix** オーディオ仮想チャネル。オーディオ転送専用に設計されているため、通常は Citrix オーディオ仮想チャネルをお勧めします。
- 汎用 **USB** リダイレクト。ユーザーデバイスが Citrix Virtual Apps and Desktops サーバーへの LAN または LAN のような接続上にある場合は、ボタンまたはディスプレイ（またはその両方）といったヒューマンインターフェイスデバイス（HID）を持つオーディオデバイスをサポートします。

Citrix オーディオ仮想チャネル

双方向の Citrix オーディオ仮想チャネル（CTXCAM）は、ネットワーク上でオーディオを効率的に配信することができます。汎用 HDX RealTime は、ユーザーのヘッドセットまたはマイクからオーディオを取り出して圧縮します。その後、ICA 経由で仮想デスクトップ上のソフトフォンアプリケーションに送信します。同様に、ソフトフォンのオーディオ出力も圧縮され、ユーザーのヘッドセットまたはスピーカーに向けて反対方向に送信されます。この圧縮は、

ソフトフォン自体で使われる圧縮（G.729、G.711 など）とは関係ありません。スピーチに最適化されたコーデック（中品質）で行われます。その特性はボイスオーバー IP に最適です。高速エンコード機能を備え、ピーク時でもおよそ 1 秒間に 56 キロビット（それぞれの方向で 28Kbps ずつ）しかネットワーク帯域幅を消費しません。このコーデックはデフォルトのオーディオコーデックではないため、サービスの［管理］コンソールで明示的に選択する必要があります。デフォルトは、HD オーディオコーデック（高品質）です。このコーデックは HiFi ステレオ録音には最適ですが、スピーチに最適化されたコーデックと比較してエンコードが遅くなります。

汎用 ***USB*** リダイレクト

Citrix 汎用 USB リダイレクトテクノロジ（CTXGUSB 仮想チャネル）は、複合デバイス（オーディオプラス HID）とアイソクロナス USB デバイスを含む、USB デバイスのリモート処理に一般的な手段を提供します。このアプローチは LAN 接続のユーザーに制限されます。USB プロトコルはネットワークの遅延に影響を受けやすく、相当量のネットワーク帯域幅を必要とするためです。ソフトフォンによっては、アイソクロナス USB リダイレクトが有効です。このリダイレクトは、優れた音声品質と低遅延を実現します。ただし、オーディオトラフィックに最適化されているため、Citrix オーディオ仮想チャネルが優先されます。主な例外は、ボタンが付いたオーディオデバイスを使う場合です。たとえば、データセンターに LAN 接続されているユーザーデバイスに取り付けられた USB 電話などです。この場合は、汎用 USB リダイレクトが、信号をソフトフォンに送ることで機能を制御する電話セットまたはヘッドセットのボタンをサポートします。デバイス上でローカルに動作するボタンでは問題ありません。

制限事項

クライアントにオーディオデバイスをインストールし、オーディオリダイレクトを有効にして、RDS セッションを開始すると、オーディオファイルがオーディオを再生できないことがあります。回避策として、レジストリキーを RDS マシンに追加し、マシンを再起動します。詳しくは、レジストリを介して管理される機能の一覧にある「オーディオ制限」を参照してください。

ブラウザーコンテンツのリダイレクト

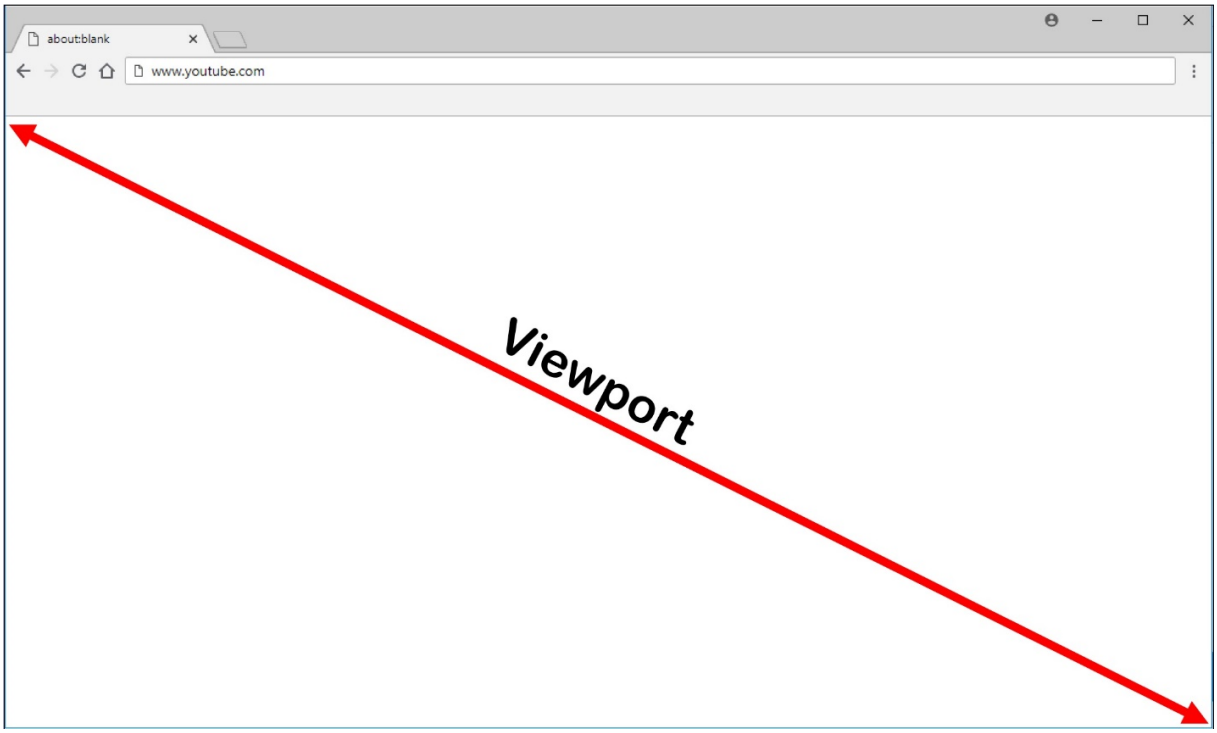
June 30, 2022

ブラウザーコンテンツリダイレクトのために、VDA 側の許可リストに登録された Web ページのレンダリングができません。この機能は、Citrix Workspace アプリを使用してクライアント側の対応するレンダリングエンジンをインスタンス化し、URL から HTTP および HTTPS コンテンツを取得します。

> 注:
>
> 禁止リストを使用することで、Web ページを VDA 側にリダイレクトする（クライアント側ではリダイレクトされない）ように指定できます。

このオーバーレイ Web レイアウトエンジンは、VDA 上ではなくエンドポイントデバイス上で実行され、エンドポイントの CPU、GPU、RAM、およびネットワークを使用します。

ブラウザーのビューポートだけがリダイレクトされます。ビューポートは、コンテンツが表示されるブラウザー内の長方形の領域です。ビューポートには、アドレスバー、お気に入りツールバー、ステータスバーなどは含まれません。これらの項目はユーザーインターフェイス内にあり、リダイレクト時も VDA のブラウザーで実行されます。



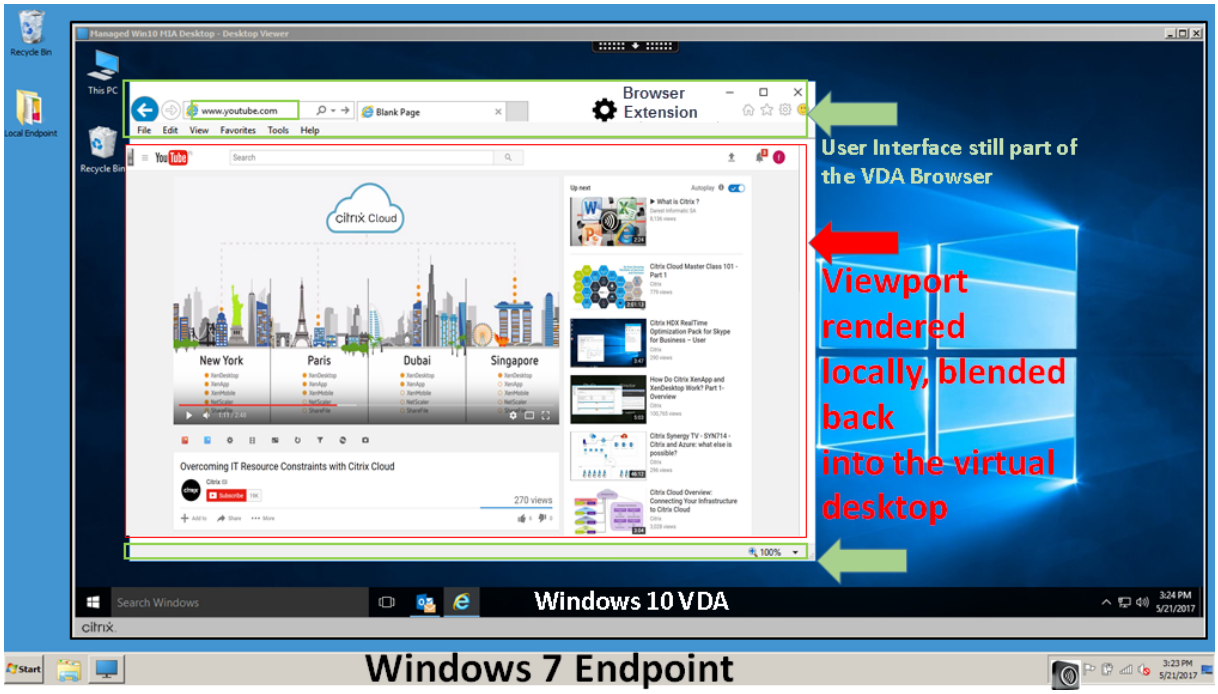
1. ［管理］>［完全な構成］インターフェイスでポリシーを構成し、許可リストまたは禁止リストからのリダイレクト用 URL が書かれたアクセス制御リストを指定します。ユーザーがナビゲートしている URL が許可リストと一致することや禁止リストと一致しないことを、VDA 上のブラウザーで検出するために、ブラウザーの拡張機能によって比較が実行されます。Internet Explorer 11 向けの Web ブラウザー拡張機能はインストールメディアに含まれており、自動的にインストールされます。Chrome 向けのブラウザー拡張機能は Chrome ウェブストアで提供されており、グループポリシーと ADMX ファイルを使用して展開できます。Chrome の拡張機能は、ユーザーごとにインストールします。拡張機能を追加または削除する場合に、ゴールデンイメージを更新する必要はありません。
2. 許可リスト内に一致するものがあり（例: `https://www.mycompany.com/`）、禁止リスト内の URL と一致するもの（例: `https://www.mycompany.com/engineering`）がない場合、仮想チャネル（CTXCSB）は、リダイレクトが必要であることを Citrix Workspace アプリに指示し、URL をリレーします。Citrix Workspace アプリは、ローカルレンダリングエンジンをインスタンス化し、Web サイトを表示します。
3. Citrix Workspace アプリは、Web サイトを仮想デスクトップブラウザーのコンテンツ領域にシームレスにブレンドします。

ロゴの色は、Chrome 拡張機能のステータスを指定します。それは、以下の 3 つの色のいずれかです:

- 緑: アクティブで接続されています。
- グレー: 現在のタブではアクティブではないかアイドル状態です。

- 赤：壊れているか動作していません。

拡張機能メニューの ［オプション］を使用して、ログをデバッグできます。



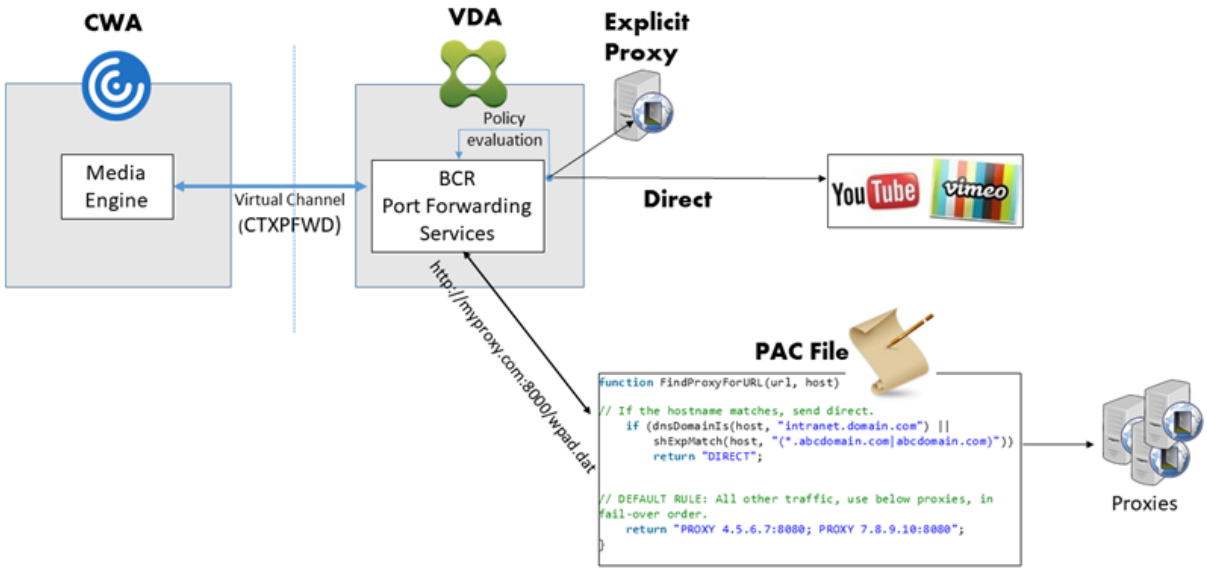
Citrix Workspace アプリがコンテンツをどのようにフェッチするかのシナリオを次に示します：

- サーバーフェッチとサーバーレンダリング：サイトを許可リストに登録していないか、リダイレクトに失敗したため、リダイレクトはありません。VDA 上での Web ページのレンダリングに戻り、Thinwire を使用してグラフィックスを遠隔操作します。ポリシーを使用してフォールバックの動作を制御します。VDA での CPU、RAM、および帯域幅の消費量が多い
- サーバーフェッチとクライアントレンダリング：Citrix Workspace アプリは仮想チャネル（CTXPFWD）を使用して、Web サーバーから VDA を通じてコンテンツに接続し、フェッチします。このオプションは、クライアントにインターネットアクセスがない場合（シンクライアントなど）に便利です。VDA では CPU と RAM の消費量は少なくなりますが、ICA 仮想チャネルでは帯域幅が消費されます。

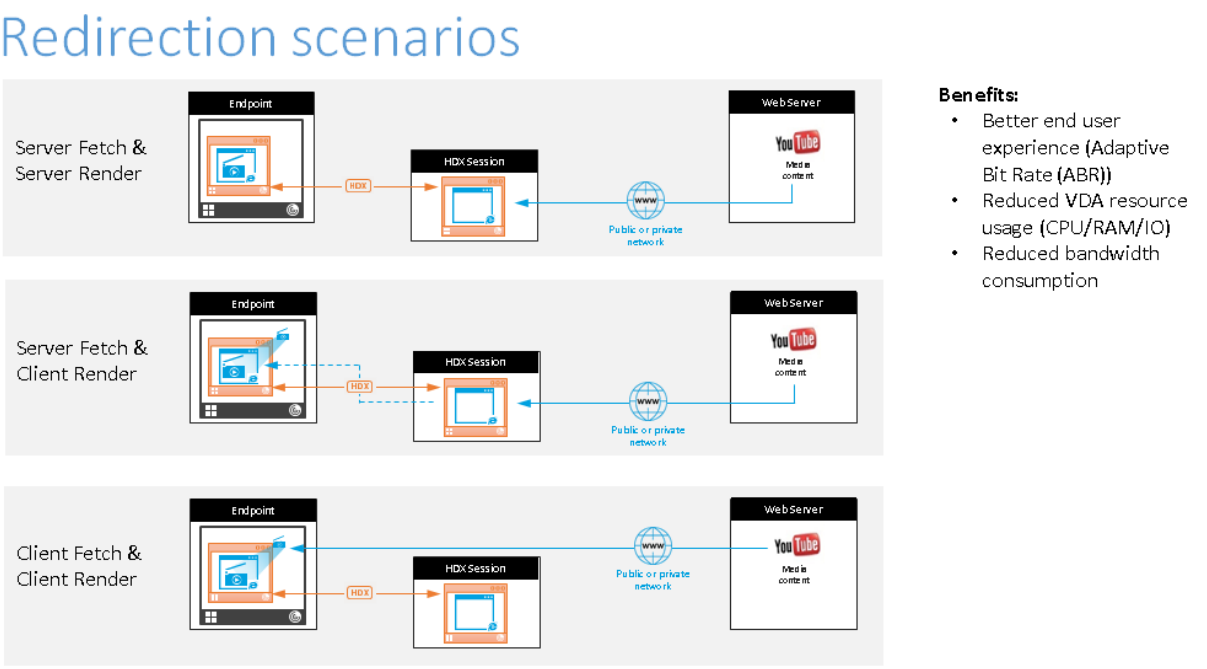
  このシナリオには 3 つの動作モードがあります。プロキシという用語は、VDA がインターネットアクセスのためにアクセスするプロキシデバイスを意味します。

  選択可能なポリシーオプション：

  - Explicit Proxy - データセンターに単一の明示的なプロキシがある場合。
  - Direct or Transparent - プロキシがない場合、または透過プロキシを使用している場合。
  - PAC files - PAC ファイルに依存して、指定された URL のフェッチに VDA のブラウザーが適切なプロキシサーバーを自動で選択できる場合。



- クライアントフェッチとクライアントレンダリング：Citrix Workspace アプリは Web サーバーに直接接続するため、インターネットにアクセスする必要があります。このシナリオでは、XenApp および XenDesktop サイトからネットワーク、CPU、および RAM の使用量をすべてオフロードします。



フォールバックのメカニズム：

クライアントのリダイレクトが失敗することがあります。たとえば、クライアントマシンでインターネットに直接アクセスできない場合、エラー応答が VDA に返される可能性があります。このような場合、VDA 上のブラウザーは、

サーバー上のページをリロードしてレンダリングできます。

既存の［**Windows** メディアフォールバック防止ポリシー］を使用することで、ビデオ要素のサーバーレンダリングを抑制できます。このポリシーを、［クライアントにあるすべてのコンテンツのみを再生］または［クライアント上のクライアントがアクセスできるコンテンツのみを再生］に設定します。これらの設定は、クライアントのリダイレクトが失敗した場合に、サーバー上でのビデオ要素の再生を禁止します。このポリシーは、Web ブラウザーコンテンツリダイレクトが有効になっており、［アクセス制御リスト］ポリシーにフォールバックする URL がある場合にのみ有効です。URL を禁止リストポリシーで指定することはできません。

システム要件：

Windows エンドポイント：

- Windows 10 または 11
- Windows 向け Citrix Workspace アプリ 1809 以降

> 注：
>
> ブラウザーコンテンツのリダイレクトは、Windows 向け Citrix Workspace アプリの最新リリースでのみサポートされています。Citrix Workspace アプリの LTSR リリース、1912 および 2203.1 ではサポートされていません。

Linux エンドポイント：

- Linux 向け Citrix Workspace アプリ 1808 以降
- Citrix Receiver for Linux 13.9 以降
- シンクライアント端末には WebKitGTK+ が必要です。

Citrix Virtual Apps and Desktops 7 1808、XenApp および XenDesktop 7.15 CU5、7.18、7.17、7.16：

- VDA オペレーティングシステム：Windows 10（バージョン 1607 以降）、Windows Server 2012 R2、Windows Server 2016
- VDA 上のブラウザー：
  - Google Chrome v66 以降（ユーザーエンドポイント上の Windows 向け Citrix Workspace アプリ 1809、Citrix Virtual Apps and Desktops 7 1808 VDA、Web ブラウザーコンテンツリダイレクト拡張機能が必要）
  - 次のオプションを構成した Internet Explorer 11：
    - ［インターネット オプション］>［詳細設定］**>**［セキュリティ］の下にある［拡張保護モードを有効にする］をオフにします。
    - ［インターネット オプション］**>**［詳細設定］**>**［ブラウズ］の下にある［サードパーティ製のブラウザー拡張を有効にする］をオンにします。

トラブルシューティング

トラブルシューティングについて詳しくは、Knowledge Center のhttps://support.citrix.com/article/CTX230052を参照してください。

Chrome 向けの **Web** ブラウザーコンテンツリダイレクト拡張機能

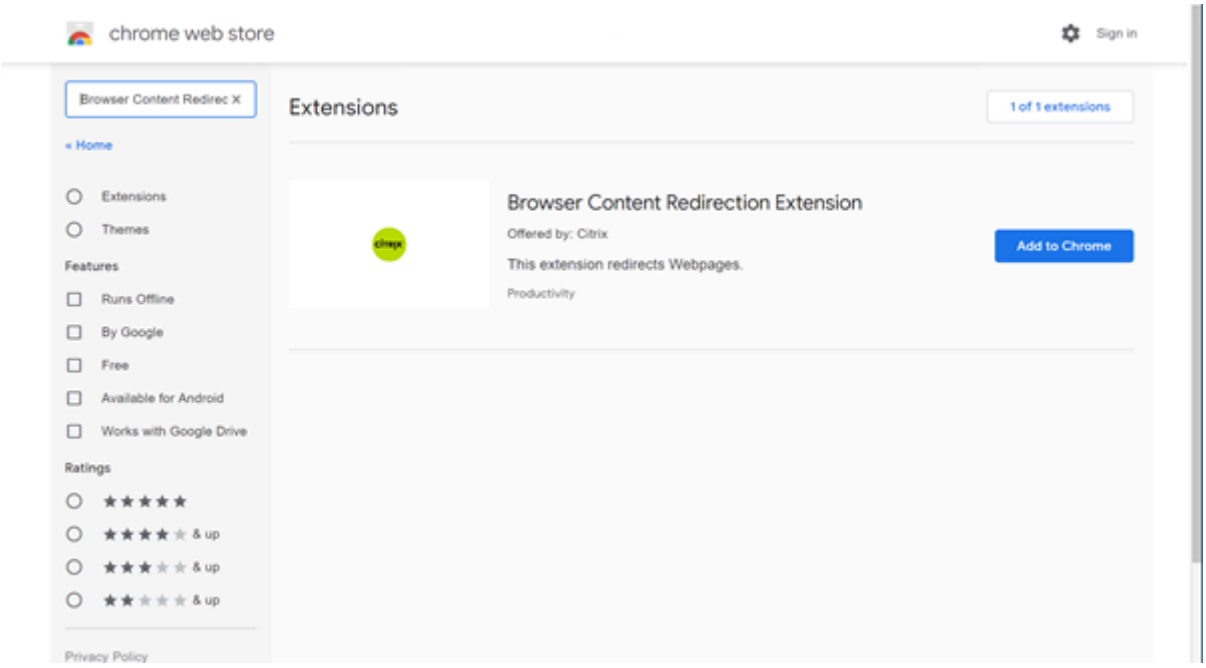
Chrome で Web ブラウザーコンテンツリダイレクトを使用するには、Chrome ウェブストアから Browser Content Redirection Extension を追加します。Citrix Virtual Apps and Desktops 環境で、[**Chrome** に追加] をクリックします。

この拡張機能は VDA にのみ必要であり、ユーザーのクライアントマシンには不要です。

システム要件

- Chrome v66 以上
- Browser Content Redirection Extension
- Citrix Virtual Apps and Desktops 7 1808 以降
- Windows 向け Citrix Workspace アプリ 1809 以降

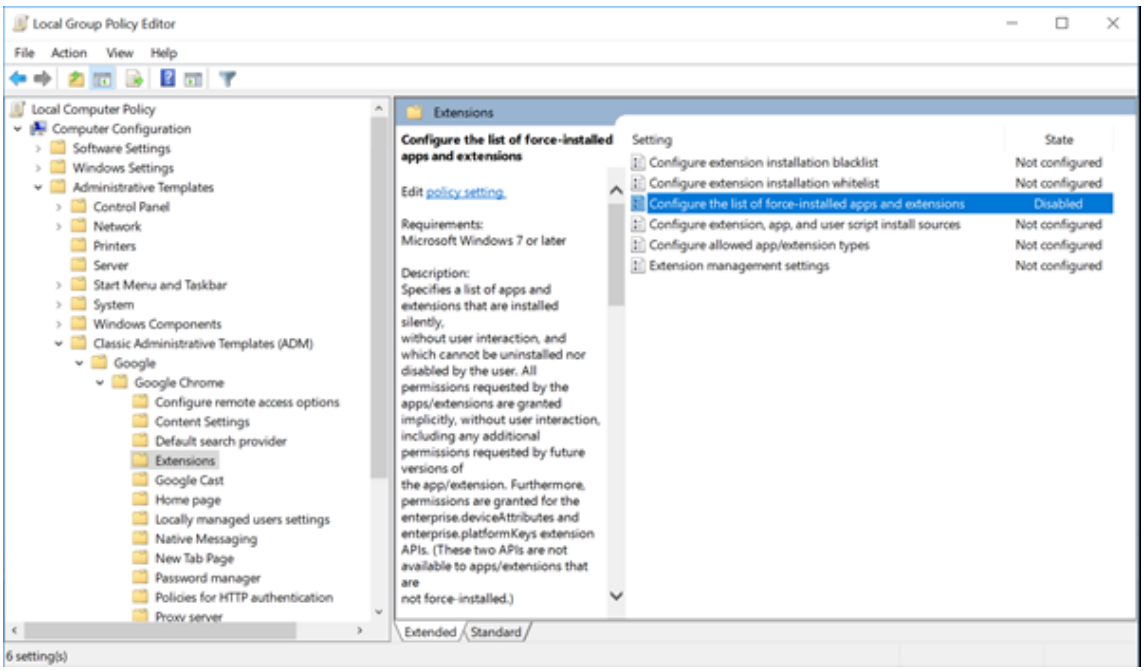
> 注:
>
> ブラウザーコンテンツのリダイレクトは、Windows 向け Citrix Workspace アプリの最新リリースでのみサポートされています。Citrix Workspace アプリの LTSR リリース、1912 および 2203.1 ではサポートされていません。



この方法は、ユーザーごとに行います。組織内の大規模なユーザーグループにこの拡張機能を展開するには、グループポリシーを使用して展開します。

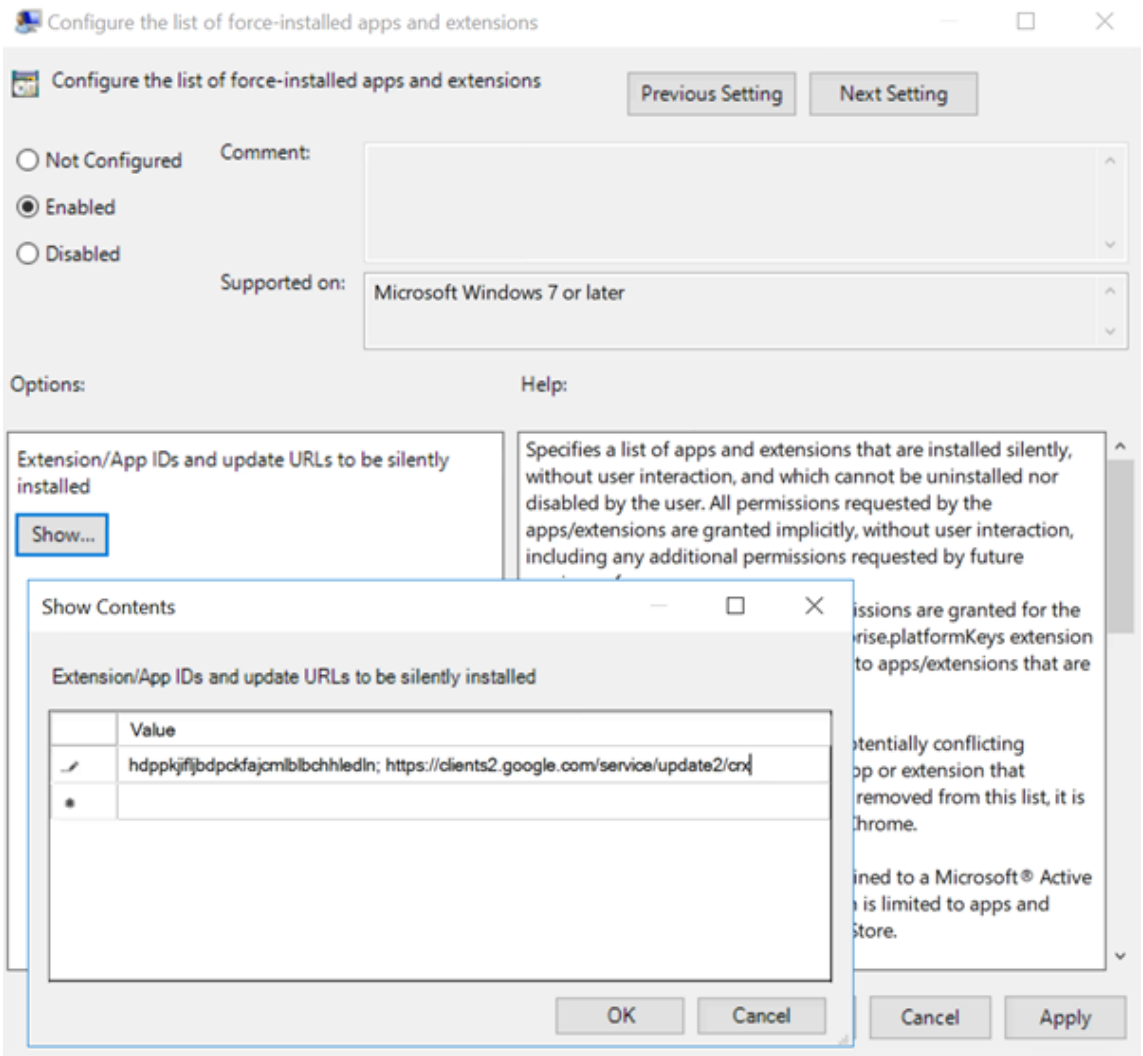
グループポリシーを使用して拡張機能を展開する

1. 現在の環境に Google Chrome ADMX ファイルをインポートします。ポリシーテンプレートをダウンロードしてグループポリシーエディターにインストールし、構成を行う方法については、管理対象パソコンに Chrome ブラウザーのポリシーを設定するを参照してください。
2. グループポリシー管理コンソールを開き、［ユーザーの構成］**>**［管理用テンプレート］**>**［従来の管理用テンプレート（**ADM**）］**>**［**Google**］**>**［**Google Chrome**］**>**［拡張機能］の順に選択します。［強制インストールするアプリと拡張機能のリストを設定します］設定を有効にします。



3. ［表示］をクリックして、拡張機能 ID に対応する文字列と、Browser Content Redirection Extension の更新用 URL を次のように指定します。

```
hdppkjifljbdpckfajcmlblbchhledln; https://clients2.google.com/service/update2/crx
```

4. 設定を適用し、**gpudate** が更新されると、ユーザーへこの拡張機能が自動で配信されます。ユーザーのセッションで Chrome ブラウザーを起動すると、この拡張機能が既に適用されています。ユーザーがこの機能を削除することはできません。

   拡張機能の更新は、設定で指定した更新用 URL を通じて、ユーザーのマシンに自動でインストールされます。

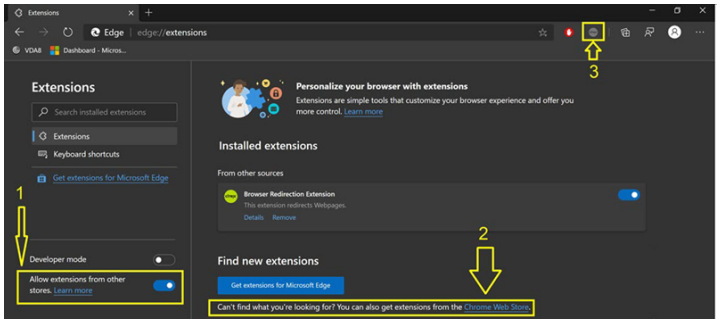
   [強制インストールするアプリと拡張機能のリストを設定します] 設定を [無効] に設定すると、この拡張機能はすべてのユーザーの Chrome から削除されます。

Chromium 版 **Edge** 向けの **Web** ブラウザーコンテンツリダイレクト拡張機能

Edge にブラウザーコンテンツリダイレクト拡張機能をインストールするため、Edge ブラウザーのバージョン **83.0.478.37** 以降がインストールされていることを確認してください。

1. メニューで [拡張機能] オプションをクリックし、[他のストアからの拡張機能を許可します。] をオンにします。

2. **Chrome** ウェブストアリンクをクリックすると、拡張機能が右上のバーに表示されます。
   Microsoft Edge の拡張機能について詳しくは、「拡張機能」を参照してください。



ブラウザーコンテンツリダイレクトと **DPI**

ユーザーのマシン上で Web ブラウザーコンテンツのリダイレクトの DPI（スケール）を 100% を超えて設定して使用すると、リダイレクトされたブラウザーコンテンツ画面が正しく表示されません。この問題を回避するため、ブラウザーコンテンツリダイレクトを使用するときに DPI を設定しないでください。この問題を回避するもう 1 つの方法は、ユーザーのマシン上でレジストリキーを作成して、Chrome で Web ブラウザーコンテンツのリダイレクトの GPU アクセラレーションを無効にすることです。詳しくは、レジストリを介して管理される機能の一覧にある「ブラウザーコンテンツリダイレクトと DPI」を参照してください。

user-agent 要求ヘッダー

user-agent ヘッダーは、Web ブラウザーコンテンツリダイレクトから送信された HTTP 要求を識別するのに役立ちます。この設定は、プロキシ規則とファイアウォール規則を構成するときに役立ちます。たとえば、サーバーが Web ブラウザーコンテンツリダイレクトから送信された要求を禁止する場合、user-agent ヘッダーを含む規則を作成して、特定の要件をバイパスできます。

Windows デバイスでのみ、user-agent 要求ヘッダーがサポートされています。

デフォルトでは、user-agent 要求ヘッダー文字列は無効になっています。クライアント側でレンダリングされたコンテンツの user-agent ヘッダーを有効にするには、レジストリエディターを使用します。詳しくは、レジストリを介して管理される機能の一覧にある「user-agent 要求ヘッダー」を参照してください。

HDX ビデオ会議と **Web** カメラビデオ圧縮

March 30, 2022

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

Web カメラは、HDX Web カメラビデオ圧縮または HDX プラグアンドプレイ汎用 USB リダイレクトにより、仮想セッション内で実行されるアプリケーションで使用できます。各モードの切り替えは、[**Citrix Workspace** アプリ] **>** [基本設定] **>** [デバイス] で行えます。可能であれば常に、HDX Web カメラビデオ圧縮を使用することをお勧めします。HDX 汎用 USB リダイレクトは、HDX ビデオ圧縮に関するアプリケーション互換性の問題がある場合、または Web カメラの高度なネイティブ機能が必要な場合にのみお勧めします。パフォーマンスを向上させるためには、Virtual Delivery Agent に少なくとも 2 つの仮想 CPU を用意することをお勧めします。

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

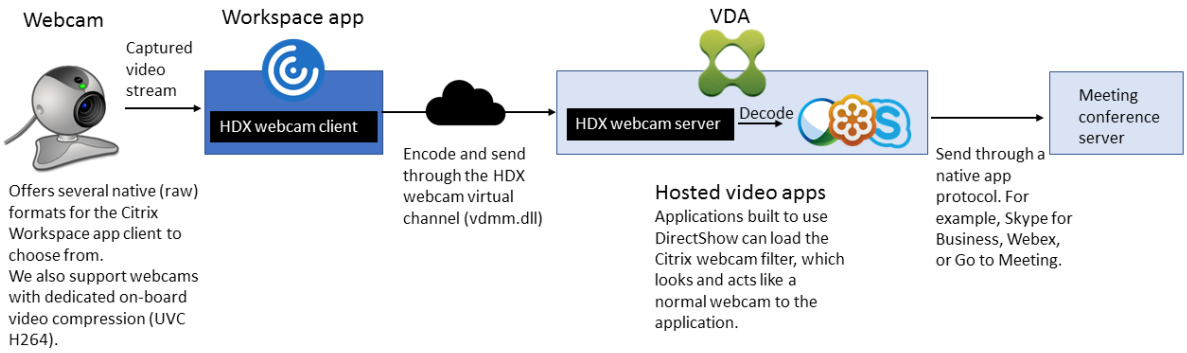
HDX Web カメラビデオ圧縮

HDX Web カメラビデオ圧縮は、最適化 Web カメラモードとも呼ばれます。このタイプの Web カメラビデオ圧縮では、仮想セッションで実行されているビデオ会議アプリケーションに H.264 ビデオを直接送信します。VDA リソースを最適化するため、HDX Web カメラ圧縮では Web カメラビデオをエンコード、トランスコード、およびデコードしません。この機能はデフォルトで有効になっています。

サーバーからビデオ会議アプリへの直接ビデオストリーミングを無効にするには、VDA でレジストリキーを 0 に設定します。詳しくは、レジストリを介して管理される機能の一覧にある「Web カメラビデオ圧縮」を参照してください。

ストリーミングビデオリソースのデフォルト機能を無効にすると、HDX Web カメラビデオ圧縮では、クライアントオペレーティングシステムに含まれるマルチメディアフレームワークテクノロジにより、キャプチャデバイスのビデオをインターセプトし、トランスコードおよび圧縮します。各キャプチャデバイスの製造元から、OS カーネルのストリーミングアーキテクチャに組み込まれるドライバーが提供されています。

クライアントは、Web カメラとの通信を処理します。その後、サーバーで適切に表示できるビデオのみを、サーバーに送信します。サーバーが Web カメラと直接やり取りをするわけではありませんが、統合によりデスクトップでも同様のエクスペリエンスが得られます。Citrix Workspace アプリがビデオを圧縮するため、帯域幅が節約され、WAN シナリオでの回復性の向上します。



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

- マルチメディア会議
- Windows Media リダイレクト

Web カメラでハードウェアエンコード機能がサポートされる場合、HDX Web カメラビデオ圧縮ではデフォルトでそのハードウェアエンコードが使用されます。ハードウェアエンコード機能は、ソフトウェアエンコードより多くの帯域幅を消費する場合があります。ソフトウェア圧縮が使用されるようにするには、クライアントのレジストリキーを編集します。詳しくは、レジストリを介して管理される機能の一覧にある「Web カメラソフトウェア圧縮」を参照してください。

HDX Web カメラビデオ圧縮の要件

HDX Web カメラのビデオ圧縮は、次のバージョンの Citrix Workspace アプリをサポートします:

プラットフォーム	プロセッサ
Windows 向け Citrix Workspace アプリ	Windows 向け Citrix Workspace アプリは、XenApp および XenDesktop 7.17 以降上の 32 ビットおよび 64 ビットアプリの Web カメラビデオ圧縮をサポートします。以前のバージョンでは、Windows 向け Citrix Workspace アプリは 32 ビットアプリのみをサポートしていました。
Mac 向け Citrix Workspace アプリ	Mac 向け Citrix Workspace アプリ 2006 は、XenApp および XenDesktop 7.17 以降上の 64 ビットアプリの Web カメラビデオ圧縮をサポートします。以前のバージョンでは、Mac 向け Citrix Workspace アプリは 32 ビットアプリのみをサポートしていました。
Linux 向け Citrix Workspace アプリ	Linux 向け Citrix Workspace アプリは、仮想デスクトップの 32 ビットアプリのみをサポートします。

プラットフォーム	プロセッサ
Chrome 向け Citrix Workspace アプリ	一部の ARM Chromebook は H.264 エンコーディングをサポートしていないため、最適化された HDX Web カメラビデオ圧縮を使用できるのは 32 ビットアプリのみです。

メディアファンデーション形式のビデオアプリケーションは、Windows 8.x 以降および Windows Server 2012 R2 以降での HDX Web カメラビデオ圧縮をサポートします。詳しくは、Knowledge Center の記事CTX132764を参照してください。

そのほかのユーザーデバイス要件:

- サウンド再生のためのハードウェア
- DirectShow 対応の Web カメラ（Web カメラのデフォルト設定を使用してください）。Web カメラ側のハードウェアエンコーディング機能を使用すると、クライアント側の CPU 使用率が軽減されます。
- HDX Web カメラを使用する場合、可能であれば、Web カメラの製造元から入手した Web カメラドライバーをクライアントにインストールしてください。サーバーにデバイスドライバーをインストールする必要はありません。

Web カメラが異なれば、フレームレートや、明るさとコントラストのレベルも異なります。Web カメラのコントラストを調整すると、アップストリームトラフィックを大幅に減らすことができます。Citrix 製品では、初期の機能検証に次の Web カメラを使用します:

- Microsoft LifeCam VX モデル（2000、3000、5000、7000）
- Creative Live! Cam Optia Pro
- Logitech QuickCam Messenger
- Logitech C600、C920
- HP Deluxe Webcam

最適なビデオフレームレートを調整するには、クライアントでレジストリキーを編集します。詳しくは、レジストリを介して管理される機能の一覧にある「Web カメラビデオ圧縮フレームレート」を参照してください。

高品位 **Web** カメラストリーミング

サーバーのビデオ会議アプリケーションは、サポートされている形式の種類に基づいて Web カメラの形式と解像度を選択します。セッションが開始されると、クライアントは Web カメラ情報をサーバーに送信します。アプリケーションから Web カメラを選択します。Web カメラとビデオ会議アプリケーションが高品位レンダリングをサポートする場合、アプリケーションは高品位解像度を使用します。1920x1080 までの Web カメラ解像度がサポートされています。

この機能を使用するには、Windows 向け Citrix Workspace アプリバージョン 1808 以降、または Citrix Receiver for Windows バージョン 4.10 以降が必要です。

レジストリキーを使用してこの機能を無効または有効にすることができます。詳しくは、レジストリを介して管理される機能の一覧にある「高品位 Web カメラストリーミング」を参照してください。

メディアの種類のネゴシエーションが失敗した場合、HDX はデフォルトの解像度である 352x288 CIF に戻ります。クライアントのレジストリキーを使用して、デフォルトの解像度を設定することができます。カメラが指定された解像度をサポートしていることを確認してください。詳しくは、レジストリを介して管理される機能の一覧にある「高品位 Web カメラの解像度」を参照してください。

HDX Web カメラのビデオ圧縮は、プラグアンドプレイの汎用 USB リダイレクトと比較して、使用する帯域幅が大幅に少なく、WAN 接続で適切に動作します。帯域幅を調整するには、クライアントでレジストリキーを設定します。詳しくは、レジストリを介して管理される機能の一覧にある「高品位 Web カメラの帯域幅」を参照してください。

1 秒あたりのビット数で値を入力します。帯域幅を指定しない場合、ビデオ会議アプリケーションはデフォルトで 350000bps を使用します。

HDX プラグアンドプレイ汎用 **USB** リダイレクト

HDX プラグアンドプレイ汎用 USB リダイレクト（アイソクロナス）は、汎用 Web カメラモードとも呼ばれます。HDX プラグアンドプレイ汎用 USB リダイレクトの利点は、シンクライアントやエンドポイントにドライバーをインストールする必要がないことです。USB スタックは仮想化されており、ローカルクライアントに接続した周辺機器はすべてリモート VM へ送信されます。リモートデスクトップは、ネイティブ接続の場合と同じように動作します。Windows デスクトップがハードウェアとのやり取りをすべて処理し、プラグアンドプレイロジックにより適切なドライバーが検出されます。ドライバーがサーバー上に存在し、ICA に対応する場合、ほとんどの Web カメラを使用できます。汎用 Web カメラモードでは、USB プロトコルにより未圧縮のビデオをネットワーク上で送信するため、はるかに多くの帯域幅（大量の Mbps）が使用されます。

HTML5 マルチメディアリダイレクション

June 12, 2024

HTML5 マルチメディアリダイレクションは、HDX MediaStream のマルチメディアリダイレクト機能を拡張し、HTML5 のオーディオとビデオを含むようにしたものです。マルチメディアコンテンツのオンライン配信の拡大、特にモバイルデバイスへの拡大により、ブラウザー業界はオーディオやビデオを再生するより効率的な方法を開発してきました。

Flash が標準となりましたが、Flash はプラグインが必要で、すべてのデバイスで稼働するわけではなく、また、モバイルデバイスでは大量のバッテリーを消費します。YouTube、NetFlix.com などの企業や Mozilla、Google、Microsoft のブラウザーの新バージョンは HTML5 に移行しており、これが新しい標準になっています。

HTML5 ベースのマルチメディアには、専用プラグインを超える以下のような多数の利点があります：

- 企業非依存型の標準（W3C）

- 簡素化されたデジタル著作権管理（DRM）ワークフロー
- プラグインが原因のセキュリティの問題がないことによる優れたパフォーマンス

HTTP プログレッシブダウンロード

HTTP プログレッシブダウンロードは、HTML5 をサポートする、HTTP ベースの疑似ストリーミング方式です。プログレッシブダウンロードでは、（単一品質でエンコードされた）1 つのファイルが HTTP Web サーバーからダウンロードされている間に、ブラウザーがそれを再生します。ビデオは受け取られるとドライブに保存され、ドライブから再生されます。ビデオを再度視聴する場合、ブラウザーがキャッシュからビデオをロードします。

プログレッシブダウンロードの例については、「HTML5 ビデオリダイレクションのテストページ」を参照してください。Web ページ内のビデオエレメントを調べ、以下のような HTML5 ビデオタグ内のソース（MP4 コンテナフォーマット）を探すには、使用するブラウザーの開発者ツールを使用します。

HTML5 と Flash の比較

機能	HTML5	Flash
専用のプレーヤーが必要	いいえ	はい
モバイルデバイスで実行	はい	一部
異なるプラットフォームでの実行速度	High	Slow
iOS でサポート	はい	いいえ
リソース使用率	比較的少ない	比較的多い
より高速なロード	はい	いいえ

要件

MP4 フォーマットでのプログレッシブダウンロードのリダイレクトのみがサポートされます。WebM、および DASH/HLS などのアダプティブビットレートストリーミングのテクノロジはサポートされません。

以下がサポートされており、ポリシーを使用してこれらを制御します。詳しくは、「マルチメディアのポリシー設定」を参照してください。

- サーバー側でレンダリング
- サーバー側でフェッチし、クライアント側でレンダリング
- クライアント側でフェッチしレンダリング

Citrix Workspace アプリおよび Citrix Receiver の最小バージョン:

- Windows 向け Citrix Workspace アプリ 1808
- Citrix Receiver for Windows 4.5
- Linux 向け Citrix Workspace アプリ 1808
- Citrix Receiver for Linux 13.5

VDA ブラウザーの最小バージョン	Windows OS のバージョン/ビルド/SP
Internet Explorer 11.0	Windows 10 x86（1607 RS1）および x64（1607 RS1。Windows Server 2016 RTM 14393（1607）。Windows Server 2012 R2
Firefox 47。Firefox 証明書ストアに証明書を手動で追加するか、Windows の信頼された機関からの証明書ストアで証明書を探すように Firefox を構成します。詳しくは、https://wiki.mozilla.org/CA:AddRootToFirefoxを参照してください:	Windows 10 x86（1607 RS1）および x64（1607 RS1。Windows Server 2016 RTM 14393（1607）。Windows Server 2012 R2
Chrome 51	Windows 10 x86（1607 RS1）および x64（1607 RS1。Windows Server 2016 RTM 14393（1607）。Windows Server 2012 R2

HTML5 ビデオリダイレクションソリューションのコンポーネント

- **HdxVideo.js** - Web サイト上のビデオコマンドを傍受する JavaScript フック。HdxVideo.js は、セキュア WebSocket（SSL/TLS）を使用して WebSocketService と通信します。
- **WebSocket SSL** 証明書
  - CA（ルート）の場合：**Citrix XenApp/XenDesktop HDX In-Product CA**（C = US、S = Florida、L = Fort Lauderdale、O = Citrix Systems, Inc.、OU = XenApp/XenDesktop Engineering、CN = Citrix XenApp/XenDesktop HDX In-Product CA）
    場所：［証明書 - ローカルコンピューター］>［信頼されたルート証明機関］>［証明書］
  - エンドエンティティ（リーフ）の場合：**Citrix XenApp/XenDesktop HDX Service**（C = US、S = Florida、L = Fort Lauderdale、O = Citrix Systems, Inc.、OU = XenApp/XenDesktop Engineering、CN = Citrix XenApp/XenDesktop HDX Service）
    場所：［証明書 - ローカルコンピューター］>［個人］>［証明書］
- **WebSocketService.exe** - ローカルシステムで稼働し、SSL の終了とユーザーセッションマッピングを実行します。127.0.0.1 ポート 9001 でリッスンする TLS Secure WebSocket です。
- **WebSocketAgent.exe** - ユーザーセッションで稼働し、WebSocketService コマンドの指示に従ってビデオをレンダリングします。

HTML5 ビデオリダイレクションを有効にするには

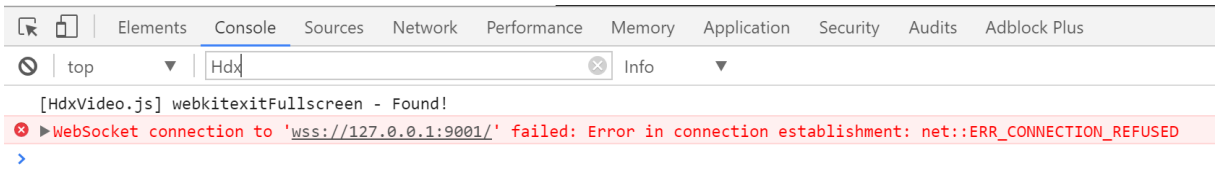
このリリースでは、この機能は管理対象 Web ページでのみ利用できます。HTML5 マルチメディアコンテンツが利用可能な Web ページに HdxVideo.js JavaScript（Citrix Virtual Apps and Desktops のインストールメディアに含まれています）を追加する必要があります。たとえば、社内研修サイトのビデオなどです。

youtube.com のようにアダプティブビットレート技術（HTTP ライブストリーミング（HLS）、Dynamic Adaptive Streaming over HTTP（DASH）など）をベースにした Web サイトは、サポートされていません。

詳しくは、「マルチメディアのポリシー設定」を参照してください。

トラブルシューティングのヒント

Web ページで HdxVideo.js を実行しようとすると、エラーが発生する場合があります。JavaScript が読み込みに失敗した場合、HTML5 リダイレクションメカニズムはエラーになります。使用するブラウザーの開発者ツールウィンドウでコンソールを調べて、HdxVideo.js に関連するエラーがないことを確認してください。例：



Microsoft Teams の最適化

June 12, 2024

> 注：
>
> 新しい Microsoft Teams 2.1 が VDA で一般提供されるようになりました。この Microsoft Teams のバージョンは、WebRTC（VDI 1.0）を使用した Citrix Microsoft Teams の最適化と互換性があります。
>
> Citrix Virtual Apps and Desktops 2402 以降を使用している場合、`msedgewebview2.exe`レジストリエントリはデフォルトで許可リストに登録されているため、手動で構成する必要はありません。
>
> 公開アプリは、新しい Microsoft Teams でサポートされるようになりました。
>
> Citrix Virtual Apps and Desktops 2311 以前を使用している場合、新しい Microsoft Teams が Citrix 仮想チャネルにアクセスできるようにするために、VDA で新しいレジストリ構成設定が必要です。Microsoft Teams 2.1 の最適化を有効にするには、VDA で次のレジストリキーを構成します：
>
> 場所：`HKLM\SOFTWARE\WOW6432Node\Citrix\WebSocketService`
>
> キー（REG_Multi_SZ）：`ProcessWhitelist`

> 値: `msedgewebview2.exe`
>
> 詳しくは、Microsoftのドキュメントを参照してください。

Citrix では Citrix Virtual Apps and Desktops および Citrix Workspace アプリを通じてデスクトップベースの Microsoft Teams の最適化を提供します。必要なコンポーネントはデフォルトで Citrix Workspace アプリと Virtual Delivery Agent（VDA）に付属しています。

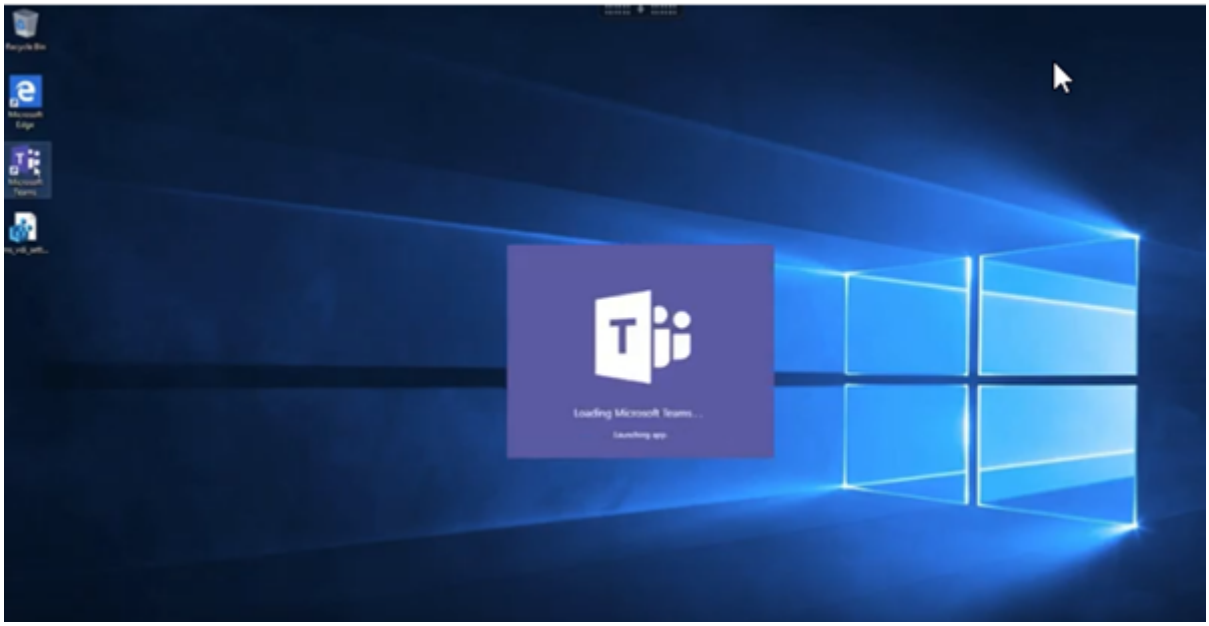
Microsoft Teams の最適化には、Microsoft Teams のホストアプリとのインターフェイスとしてコマンドを受信する、VDA 側の HDX サービスと API が含まれます。これらのコンポーネントにより Citrix Workspace アプリ側のメディアエンジンにつながる制御用の仮想チャネル（CTXMTOP）が開かれます。エンドポイントではマルチメディアがローカルでデコーディングおよび提供され、Citrix Workspace アプリのウィンドウはホストされている Microsoft Teams アプリに渡されます。

認証とシグナリングは他の Microsoft Teams サービス（チャットやコラボレーションなど）と同様に、Microsoft Teams のホストアプリでネイティブに行われます。これらのアプリはオーディオやビデオのリダイレクトによる影響を受けません。

CTXMTOPはコマンドであり、制御用の仮想チャネルです。つまり、Citrix Workspace アプリと VDA の間でメディアは交換されません。

クライアント側で取得またはクライアント側でレンダリングのみを利用できます。

このデモ動画をご覧いただければ、Microsoft Teams が Citrix の仮想環境でどのように機能するのかがおわかりいただけると思います。



Microsoft Teams のインストール

Citrix と Microsoft は、利用可能な最新バージョンの Microsoft Teams を使用し、最新の状態に保つことを推奨します。
リリース日が、現在のバージョンより 90 日を超えて古い Microsoft Teams デスクトップアプリのバージョンは、サポートされていません。
サポートされていない Microsoft Teams デスクトップアプリのバージョンでは、ユーザーをブロックするページが表示され、アプリの更新が要求されます。

利用可能な最新バージョンについては、「Teams アプリの更新履歴（デスクトップと Mac）」を参照してください。

Microsoft Teams のマシン全体のインストールガイドラインに従うことをお勧めします。また、AppDataに Microsoft Teams をインストールする.exe インストーラーの使用は避けてください。代わりに、コマンドラインでALLUSER=1フラグを使用してC:\Program Files (x86)\Microsoft\Teamsにインストールします。

```
msiexec /i <path_to_msi> /l*v <install_logfile_name> ALLUSER=1
ALLUSERS=1
```

この例では、ALLUSERS=1パラメーターも使用しています。このパラメーターを設定すると、Microsoft Teams のマシン全体のインストーラーが、［コントロールパネル］の［プログラムと機能］に表示されます。また、Windows の設定の ［アプリと機能］にも表示されます。これはそのコンピューターの全ユーザーが対象です。管理者の資格情報があれば、すべてのユーザーが Microsoft Teams をアンインストールできます。

ALLUSERS=1とALLUSER=1の違いを理解することが重要です。ALLUSERS=1パラメーターは、非 VDI 環境と VDI 環境で使用できます。マシンごとのインストールを指定するには、VDI 環境でのみALLUSER=1パラメーターを使用します。

ALLUSER=1モードでは、Microsoft Teams アプリケーションのバージョンが新しくなるたびに自動更新されることはありません。Windows Server または Windows 10 のランダム/プールカタログからホストされた共有アプリまたは共有デスクトップなど、非永続環境ではこのモードをお勧めします。詳しくは、「MSI を使用して Microsoft Teams をインストールする」（VDI インストールセクション）を参照してください。

Windows 10 専用の永続 VDI 環境をサポートします。Microsoft Teams アプリケーションを自動更新し、ユーザーごとにAppdata/Localに Microsoft Teams をインストールするこの場合、.exeインストーラーを使用するか、ALLUSER=1を設定せずに MSI を使用します。

> 注:
>
> ゴールデンイメージで Microsoft Teams をインストールする前に、VDA をインストールすることをお勧めします。このインストール順序は、ALLUSER=1フラグを有効にするために必要です。VDA をインストールする前に仮想マシンに Microsoft Teams がインストールされている場合は、Microsoft Teams をアンインストールして再インストールします。

リモート **PC** アクセス向け

VDA のインストール後に Microsoft Teams バージョン 1.4.00.22472 以降をインストールすることをお勧めします。そうしない場合は、Microsoft Teams で想定どおりに VDA が検出されるように、サインアウトしてから再度サインインする必要があります。バージョン 1.4.00.22472 以降には、VDA 検出のために Microsoft Teams の起動時およびサインイン時に実行される、拡張されたロジックが含まれています。これらのバージョンには、アクティブなセッションタイプの識別（HDX、RDP、またはクライアントマシンへのローカル接続）も含まれています。ローカル接続の場合、以前のバージョンの Microsoft Teams は、特定の機能または UI 要素の検出と無効化に失敗する可能性があります。たとえば、ブレークアウトルームでの、会議用やチャット用、または会議のリアクション用のウィンドウの表示などです。

> 重要:
>
> ローカルセッションから HDX セッションにローミングし、Microsoft Teams を開いてバックグラウンドで実行している場合は、Microsoft Teams を終了して再起動し、HDX で正しく最適化する必要があります。
> 逆に、最適化された HDX セッションを介してリモートで Microsoft Teams を使用する場合は、HDX セッションを切断し、デバイスのローカルで同じ Windows セッションに再接続します。オフィスから作業する場合は、Microsoft Teams を再起動して、リモート PC の状態（HDX またはローカル）を正しく検出できるようにする必要があります。Microsoft Teams は、アプリの起動時にのみ VDI モードを評価でき、バックグラウンドで既に実行されている間は評価できないためです。再起動しないと、Microsoft Teams はポップアウトウィンドウ、ブレークアウトルーム、会議のリアクションなどの機能の読み込みに失敗する可能性があります。

App Layering の場合

Citrix App Layering を使用して VDA と Microsoft Teams を異なるレイヤーで管理する場合、コマンドラインからALLUSER=1フラグを使用して Microsoft Teams をインストールする前に、Windows VDA で新しいレジストリキーを作成する必要があります。詳しくは、「マルチメディア」の「*Citrix App Layering* による *Microsoft Teams* の最適化」セクションを参照してください。

Profile Management の推奨事項

Windows Server 環境およびプールされた VDI Windows 10 環境では、マシン全体のインストーラーを使用することをお勧めします。

コマンドラインで **ALLUSER=1** フラグを MSI に渡すと、Microsoft Teams アプリはC:\Program Files（x86）（約 300MB）にインストールされます。このアプリはログにAppData\Local\Microsoft\TeamsMeetingAddinを、ユーザー独自の構成、ユーザーインターフェイスの要素のキャッシュなどにAppData\Roaming\Microsoft\Teams（約 600～700MB）を使用します。

> 重要:
>
> **ALLUSER=1** フラグを渡さない場合、MSI は Teams.exe インストーラーとsetup.jsonをC:\

> Program Files (x86)\Teams Installerに配置します。レジストリキー（TeamsMachine-Installer）が次の場所に追加されます：HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run
>
> 後続のユーザーログオンは、代わりに **AppData** の最終インストールをトリガーします。

マシン全体のインストーラー

以下は、Windows Server 2016 64 ビット仮想マシンに、Microsoft Teams のマシン全体のインストーラーをインストールすることによって作成されるフォルダー、デスクトップショートカット、およびレジストリの例です：

フォルダー：

- C:\Program Files (x86)\Microsoft\Teams
- C:\Users\<username>\AppData\Roaming\Microsoft\Teams

デスクトップのショートカット：

C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe

レジストリ：

- HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- 値の名前：Teams
- 種類：REG_SZ
- 値：C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe

> 注：
>
> レジストリの場所は、基盤となるオペレーティングシステムとビットによって異なります。

推奨事項

- Microsoft Teams のレジストリキーを削除して、自動起動を無効にすることをお勧めします。そうすることで、多数のログオンが同時に行われる場合（たとえば、就業日の開始時刻）に、VM の CPU 使用量が急上昇するのを防ぎます。
- 仮想デスクトップに GPU または vGPU がない場合は、Microsoft Teams の［設定］で［**GPU** ハードウェアアクセラレーションを無効にする］を選択し、パフォーマンスを改善します。この設定（"disableGpu":**true**）はdesktop-config.jsonの%Appdata%\Microsoft\Teamsに格納されています。ログオンスクリプトを使用してファイルを編集し、値を **true** に設定できます。
- Citrix Workspace Environment Management（WEM）を使用している場合は、［**CPU** スパイク保護］を有効にして、Microsoft Teams のプロセッサ消費を管理します。

ユーザーごとのインストーラー

.exeインストーラーを使用する場合は、インストールプロセスが異なります。すべてのファイルは AppData に配置されます。

フォルダー:

- C:\Users\<username>\AppData\Local\Microsoft\Teams
- C:\Users\<username>\AppData\Local\Microsoft\TeamsPresenceAddin
- C:\Users\<username>\AppData\Local\Microsoft\TeamsMeetingAddin
- C:\Users\<username>\AppData\Local\SquirrelTemp
- C:\Users\<username>\AppData\Roaming\Microsoft\Teams

デスクトップのショートカット:

```
C:\Users\<username>\AppData\Local\Microsoft\Teams\Update.exe --
processStart "Teams.exe"
```

レジストリ:

```
HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

ベストプラクティス

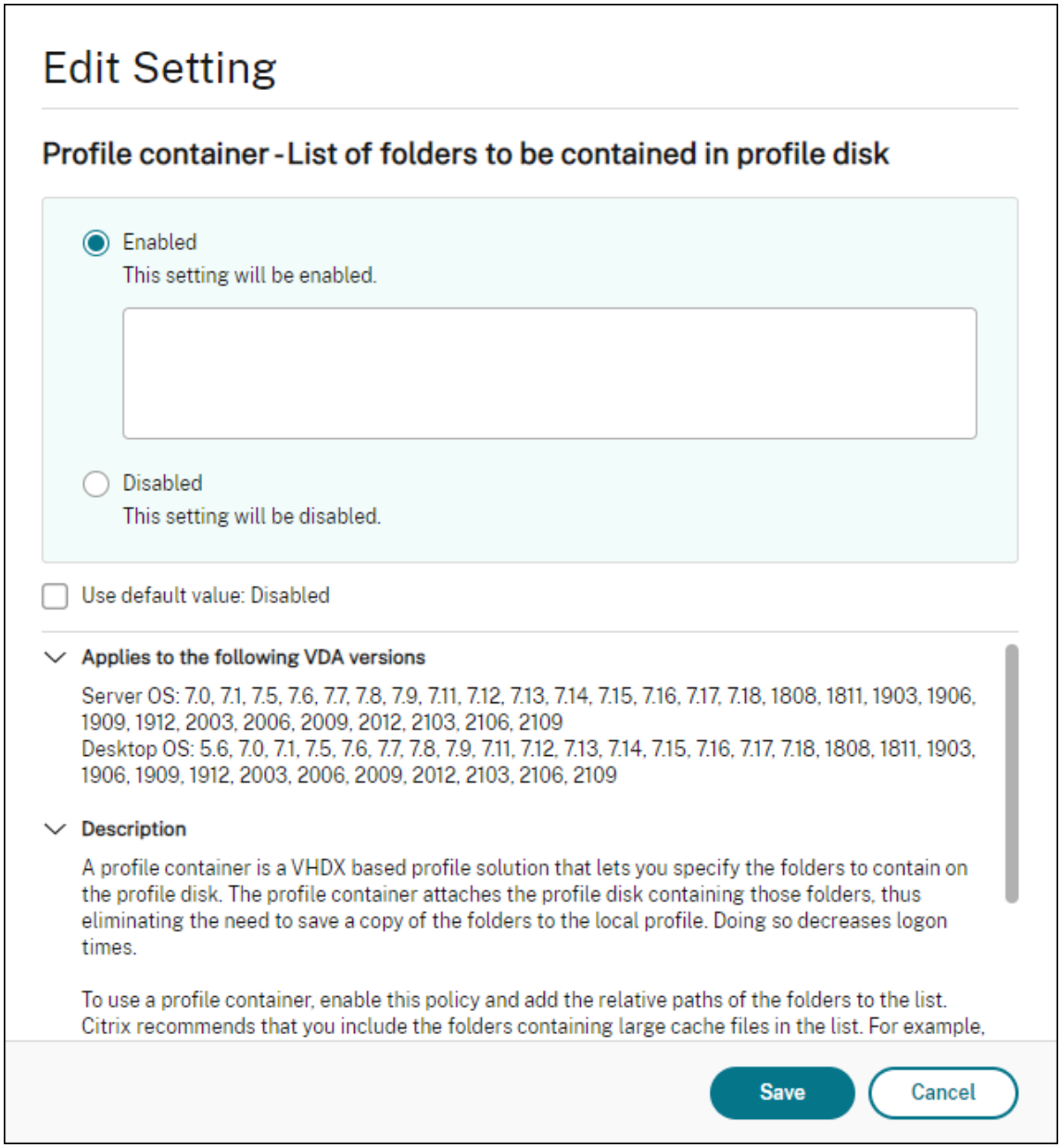
ベストプラクティスの推奨事項は、ユースケースのシナリオに基づいています。
非永続的な設定で Microsoft Teams を使用するには、Microsoft Teams ランタイムのデータ同期を効率的に実行するために、プロファイルキャッシュマネージャーが必要です。プロファイルキャッシュマネージャーを使用すると、適切なユーザー固有の情報がユーザーセッション中にキャッシュされます。たとえば、ユーザー固有の情報には、ユーザーデータ、プロファイル、設定が含まれます。次の 2 つのフォルダー内のデータを同期してください:

- C:\Users\<username>\AppData\Local\Microsoft\IdentityCache
- C:\Users\<username>\AppData\Roaming\Microsoft\Teams

非永続的な設定用の、**Microsoft Teams** でキャッシュしたコンテンツ除外一覧　Microsoftのドキュメントで説明されているように、ファイルとディレクトリを Microsoft Teams のキャッシュフォルダーから除外します。この操作は、ユーザーのキャッシュサイズを減らして、非永続的な設定をさらに最適化するのに役立ちます。

ユースケース: シングルセッションシナリオ　このシナリオでは、エンドユーザーは、一度に 1 つの場所で Microsoft Teams を使用します。2 つの Windows セッションで同時に Microsoft Teams を実行する必要はありません。共通の仮想デスクトップ展開では、各ユーザーが 1 つのデスクトップに割り当てられ、Microsoft Teams は 1 つのアプリケーションとして仮想デスクトップに展開されます。
Citrix Profile コンテナを有効にして、ユーザーごとのインストーラーに表示されるユーザーごとのディレクトリをコンテナにリダイレクトすることをお勧めします。

1. Microsoft Teams のマシン全体のインストーラー（**ALLUSER=1**）をゴールデンイメージで展開します。
2. Citrix Profile Management を有効にし、適切な権限でユーザープロファイルストアを設定します。
3. 次の Profile Management ポリシー設定を有効にします：［ファイルシステム］**>**［同期］**>**［プロファイルコンテナ **-** プロファイルディスクに含まれるフォルダー一覧］。



この構成にユーザーごとのすべてのディレクトリをリストします。Citrix Workspace Environment Management（WEM）サービスを使用して、これらの設定を構成することもできます。

4. 設定を適切なデリバリーグループに適用します。
5. ログインして展開を検証します。

システム要件

推奨の最小バージョン **- Delivery Controller**（**DDC**）**1906.2**

以前のバージョンを使用している場合は、「Microsoft Teams の最適化を有効にする」を参照してください:

以下のオペレーティングシステムがサポートされています:

- Windows Server 2022、2019、2016、2012 R2 の Standard およびデータセンターエディション、および Server Core オプション付き

最小バージョン **- Virtual Delivery Agent**（**VDA**）**1906.2**

以下のオペレーティングシステムがサポートされています:

- Windows 11。
- Windows 10 64 ビット版、バージョン 1607 以降。VM Hosted App は、Windows 向け Citrix Workspace アプリ 2109.1 以降でサポートされます。
- Windows Server 2022、2019、2016、2012 R2（Standard およびデータセンターエディション）。

要件:

- BCR_x64.msi - Microsoft Teams の最適化コードが格納された MSI ファイルです。自動的に GUI で起動します。VDA のインストールにコマンドラインインターフェイスを使用する場合は、このファイルを除外しないでください。

推奨バージョン **- Windows** 向け **Citrix Workspace** アプリの最新 **CR** および最小バージョン **- Windows** 向け **Citrix Workspace** アプリ **1907**

- Windows 11。
- Windows 10（Embedded エディションを含む 32 ビットおよび 64 ビットエディション）（Windows 7 のサポートはバージョン 2006 で終了しました）（Windows 8.1 のサポートはバージョン 2204.1 で終了しました）。
- Windows 10 IoT Enterprise 2016 LTSB（v1607）および 2019 LTSC（v1809）。
- サポートされているプロセッサ（CPU）アーキテクチャ：x86 および x64（ARM はサポートされていません）。
- エンドポイントの要件：2.2～2.4GHz 程度のデュアル CPU を搭載し、ピアツーピアのビデオ会議通話で 720p HD の解像度に対応していること。
- デュアルまたはクアッドコア CPU、低い基本速度（約 1.5GHz）で Intel Turbo Boost または AMD Turbo Core を搭載し、少なくとも 2.4GHz までブーストできる。
- 検証済みの HP シンクライアント：t630/t640、t730/t740、mt44/mt45。
- 検証済みの Dell シンクライアント：5070、5470 モバイル TC、AIO。
- 検証済みの 10ZiG シンクライアント：4510 および 5810q。

- 検証済みエンドポイントの全一覧については、「シンクライアント」を参照してください。
- Citrix Workspace アプリでは、少なくとも 600MB のディスクスペースと 1GB の RAM が必要です。
- Microsoft .NET Framework の最小要件はバージョン 4.8 です。システムに.NET Framework が導入されていない場合は、Citrix Workspace アプリにより自動的にダウンロードとインストールが行われます。

管理者は Teams 最適化ポリシーを変更することにより、最適化モードで開始する Microsoft Teams を有効にするか無効にするかを選択できます。Citrix Workspace アプリで最適化モードで開始するユーザーは、Microsoft Teams を無効にできません。

最小バージョン **- Linux** 向け **Citrix Workspace** アプリ **2006**

ソフトウェア:

- `GStreamer` 1.0 以降または Cairo 2
- libc++-9.0 以降
- `libgdk` 3.22 以降
- OpenSSL 1.1.1d
- x64 Linux ディストリビューション

ハードウェア:

- 1.8GHz 以上のデュアル CPU を搭載し、ピアツーピアのビデオ会議通話で 720p HD の解像度に対応している
- デュアルまたはクアッドコア CPU、基本速度 1.8GHz で、2.9GHz 以上の高速 Intel Turbo Boost を搭載している

検証済みエンドポイントの全一覧については、「シンクライアント」を参照してください。

詳しくは、「Citrix Workspace アプリをインストールする前提条件」を参照してください。

`/opt/Citrix/ICAClient/config/module.ini`ファイル内の **VDWEBRTC** フィールドの値をオフに更新して、Microsoft Teams の最適化機能を無効にすることができます。デフォルトでは VDWEBRTC がオンになっています。更新が完了したら、セッションを再開します。(ルート権限が必要です)。

最小バージョン **- Mac** 向け **Citrix Workspace** アプリ **2012**

以下のオペレーティングシステムがサポートされています:

- macOS Catalina(10.15)。
- macOS Big Sur 11.0.1 以降。
- macOS Monterey。

サポートされる機能:

- オーディオ

- ビデオ
- 画面共有の最適化（受信および送信）

> 注:
>
> Citrix Viewer アプリでは、画面共有を機能させるために macOS の［セキュリティとプライバシー］の環境設定にアクセスする必要があります。この環境設定を行うには、アップルメニュー **>** ［システム環境設定］ **>** ［セキュリティとプライバシー］ **>** ［プライバシー］タブ **>** ［画面収録］の順に進み、［**Citrix Viewer**］を選択します。

Microsoft Teams の最適化は、Citrix Workspace アプリ 2012 以降および macOS 10.15 とデフォルトで機能します。

Microsoft Teams の最適化を無効にする場合は、ターミナルで次のコマンドを実行し、Citrix Workspace アプリを再起動します:

```
defaults write com.citrix.receiver.nomas mtopEnabled -bool NO
```

最小バージョン- 最新バージョンの **Chrome OS** で実行されている **Chrome OS** 向け **Citrix Workspace** アプリ

ハードウェア:

- Intel i3、クアッドコア 2.4GHz と同等またはそれ以上のパフォーマンスを発揮するプロセッサー。

サポートされる機能:

- オーディオ
- ビデオ
- 画面共有の最適化（受信および送信）- デフォルトで無効有効にする方法については、これらの設定を参照してください。

単一サーバーのスケーラビリティ

このセクションでは、単一の物理ホストでサポートできるユーザーまたは仮想マシン（VM）の数を見積もる際の推奨事項等を説明します。これは一般的に、Citrix Virtual Apps and Desktops の単一サーバーのスケーラビリティ（Single Server Scalability：SSS）と呼ばれます。Citrix Virtual Apps（CVA）またはセッション仮想化の文脈では、一般的にユーザー密度とも呼ばれます。これは、主要なハイパーバイザーを実行している単一のハードウェアで実行可能なユーザーまたは VM の数を調べることを意味します。

> 注:
>
> このセクションには、SSS を見積もるためのガイダンスがあります。このガイダンスは高レベルの説明であり、必ずしも特定の状況や環境に固有のことではないことに注意してください。Citrix Virtual Apps and Desktops の SSS を深く理解する唯一の方法は、Login VSI などのスケーラビリティまたは負荷テストツールを使用することです。ここに記載されているガイダンスと簡単な規則を用いて、すばやく SSS のみを見積もる

> ことをお勧めします。ただし、ハードウェアを購入したり、財務上の決定を行う前に、Login VSI または負荷テストツールを使用して結果を検証することをお勧めします。

ハードウェア（テスト対象のシステム）

- Dell PowerEdge R740
- Intel Xeon（Gold）6126 @ 2.60GHz（最大 Turbo 3.70GHz）、ソケットあたり 12 コア、Hyperthreading が有効なデュアルソケット
- 382GB の RAM
- ローカル SSD RAID 0 ストレージ（11 ディスク）6 TB

ソフトウェア

Citrix Virtual Apps and Desktops 2106
VMware ESXi 6.7 を実行している Windows 2019（TSVDA）の単一の仮想マシン（40 個の論理プロセッサ）

用語

- ナレッジワーカーのワークロード：Acrobat Reader、Freemind/Java、Photo viewer、Edge、および Excel、Outlook、PowerPoint、Word などの MS Office アプリ。
- 基準：サーバーのスケーラビリティのテストは、ナレッジワーカーのワークロード（Microsoft Teams なし）で実行されます。
- Microsoft Teams ワークロード：ナレッジワーカーの一般的なワークロード + Microsoft Teams。

Microsoft Teams のストレステスト方法

- Microsoft Teams は HDX で最適化されています。したがって、すべてのマルチメディア処理は、エンドポイントまたはクライアントにオフロードされ、測定の一部にはなりません。
- ワークロードが開始する前に、すべての Microsoft Teams プロセスが停止または強制終了されます。
- Microsoft Teams が開きます（コールドスタート）。
- Microsoft Teams がプライマリウィンドウを読み込んでフォーカスを取得するのにかかる時間を測定します。
- キーボードショートカットを使用して、チャットウィンドウに切り替えます。
- キーボードショートカットを使用して、カレンダーウィンドウに切り替えます。
- キーボードショートカットを使用して、特定のユーザーにチャットメッセージを送信します。
- キーボードショートカットを使用して、Microsoft Teams ウィンドウに切り替えます。

結果

- 基準（137 ユーザー）と比較した場合、Microsoft Teams ワークロード（81 ユーザー）によるスケーラビリティへの影響は 40% です。
- サーバー容量を 40% 以下（CPU 内）の範囲で増やすと、基準ワークロードと同じユーザー数を復元します。
- 基準と比較した場合、Microsoft Teams ワークロードでは 20% の追加メモリが必要です。
- 1 ユーザーあたりのストレージサイズを 512～1024MB の範囲で増やします。
- IOPS 書き込みは 50% 以下の範囲で増加、IOPS 読み取りは 100% 以下の範囲で増加。Microsoft Teams は、ストレージが遅い環境に大きな影響を与える可能性があります。

機能マトリックスとバージョンのサポート

機能	Microsoft Teams（最小バージョン）	VDA（最小バージョン）	Windows 向け Citrix Workspace アプリ CR（最小バージョン）	Mac 向け Citrix Workspace アプリ（最小バージョン）	Linux 向け Citrix Workspace アプリ（最小バージョン）	Chrome OS 向け Citrix Workspace アプリ
オーディオ/ビデオ (P2P および会議)	最新バージョンから 90 日を引いたバージョン	1906	1907	2009	2004	2105.5
画面共有	最新バージョンから 90 日を引いたバージョン	1906	1907	2012	2006	2105.5
i. 赤い枠線を画面に表示	最新バージョンから 90 日を引いたバージョン	1906	2002	2012	2006	いいえ
ii. キャプチャを Desktop Viewer に制限	最新バージョンから 90 日を引いたバージョン	1906	2009.5	2012	2006	いいえ
iii. マルチモニター	最新バージョンから 90 日を引いたバージョン	1912 CU6 以降	2106 (1)	2106	2106	いいえ

機能	Microsoft Teams（最小バージョン）	VDA（最小バージョン）	Windows 向け Citrix Workspace アプリ CR（最小バージョン）	Mac 向け Citrix Workspace アプリ（最小バージョン）	Linux 向け Citrix Workspace アプリ（最小バージョン）	Chrome OS 向け Citrix Workspace アプリ
DTMF	最新バージョンから 90 日を引いたバージョン	-	2102	2101	2101	2111.1
プロキシサーバーのサポート	最新バージョンから 90 日を引いたバージョン	-	2012 (2)	2104 (3)	2101 (3)	2305
アプリの共有	最新バージョンから 90 日を引いたバージョン	2109	2109.1	2203.1	2209	いいえ
ライブキャプション	最新バージョンから 90 日を引いたバージョン	-（4）	2109.1	2109	2109	2303
動的緊急通報（Dynamic e911）	最新バージョンから 90 日を引いたバージョン	-	2112.1	2112	2112	2112
制御を渡す	最新バージョンから 90 日を引いたバージョン	-	2112.1	2203.1	いいえ	いいえ
制御を要求	最新バージョンから 90 日を引いたバージョン	-	2112.1	2203.1	2203	2303
マルチウィンドウ	1.5.00.11865	2112、1912 CU6（5）	2112.1	2203.1	2203	2303

機能	Microsoft Teams（最小バージョン）	VDA（最小バージョン）	Windows 向け Citrix Workspace アプリ CR（最小バージョン）	Mac 向け Citrix Workspace アプリ（最小バージョン）	Linux 向け Citrix Workspace アプリ（最小バージョン）	Chrome OS 向け Citrix Workspace アプリ
会議のトランスクリプト	最新バージョンから 90 日を引いたバージョン	2112.1、1912 CU6 以降	2112	2203.1	2203	2303
背景のぼかし	最新バージョンから 90 日を引いたバージョン	2112、1912 CU6 以降	2207	2301	2212	2303

1. CD ビューアはフルスクリーンモードでのみ使用できます。SHIFT+F2 はサポートされていません。
2. Negotiate/Kerberos、NTLM、Basic、およびダイジェスト。Pacファイルもサポートされています。
3. 匿名のみ。
4. VDA が 2112 以降の場合、ライブキャプションは、Mac 向け Citrix Workspace アプリではバージョン 2203.1、Linux 向けでは 2203、Windows 向けでは 2112 の場合にのみ機能します。これは、Microsoft Teams がシングルウィンドウ UI モードまたはマルチウィンドウモードの場合で、ライブキャプションの動作が異なるためです。
5. マルチウィンドウは 2112 VDA で導入されましたが、VDA 1912 LTSR CU6 リリースにバックポートされました。

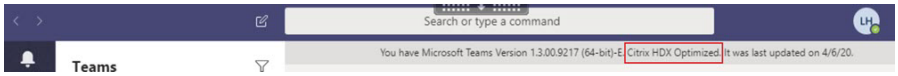
> 注:
>
> 「**Windows** 向け **Citrix Workspace** アプリ **1912 CU6** 以降」に記載されているすべての機能は、Windows 向け Citrix Workspace アプリ 2203.1 LTSR CU1 に適用されます。

Microsoft Teams の最適化を有効にする

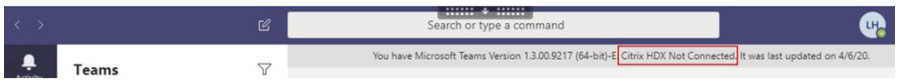
Microsoft Teams の最適化を有効にするには、「Microsoft Teams リダイレクト」で説明されている［管理］コンソールのポリシーを使用します。このポリシーは、デフォルトでは有効になっています。HDX はこのポリシーが有効になっていることと、Citrix Workspace アプリのバージョンが最低限必要とされるバージョン以上であることを確認します。ポリシーが有効で Citrix Workspace アプリがサポート対象のバージョンである場合は、VDA で **HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream\MSTeamsRedirSupport** の値が **1** に自動的に設定されます。Microsoft Teams はこのレジストリキーを VDI モードで読み取ってロードします。

> 注:
>
> ［管理］コンソール（Studio）で使用可能なポリシーがない古いバージョンのコントローラー（たとえばバージョン 7.15）でバージョン 1906.2 以降の VDA を使用している場合、その VDA では引き続き最適化が有効になっています。Microsoft Teams の HDX 最適化は、VDA ではデフォルトで有効になっています。

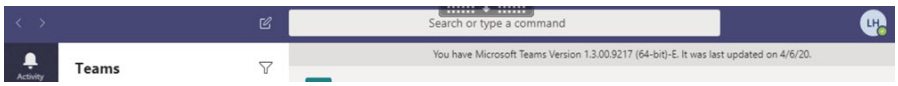
［バージョン情報］をクリックすると、**Citrix HDX Optimized** と表示されます:



Citrix HDX Not Connected と表示される場合は、Citrix API は Microsoft Teams に読み込まれています。API の読み込みは、リダイレクトへの最初の手順です。しかし、スタックの後半部分にエラーがあります。このエラーは、VDA サービスまたは Citrix Workspace アプリで発生する可能性があります。



凡例が表示されない場合、Microsoft Teams が Citrix API の読み込みに失敗しています。通知領域のアイコンを右クリックして Microsoft Teams を終了し、再起動します。［管理］コンソールのポリシーが ［禁止］に設定されていないこと、および Citrix Workspace アプリのバージョンがサポートされていることを確認します。



> 重要：セッションは再接続されます
>
> - 接続が変更されたときに、HDX で最適化されたセッションを取得するには、Microsoft Teams の再起動が必要な場合があります。たとえば、サポートされていないエンドポイント（iOS 用、Android 用、または古いバージョンの Windows/Linux/Mac 用の Workspace アプリ）から、サポートされているエンドポイント（Windows/Linux/Mac/ChromeOS/HTML5 用の Workspace アプリ）にローミングしている場合、またはその逆の場合。
> - VDA で Microsoft Teams の.exe インストーラーを使用してアプリをインストールした場合も、Microsoft Teams の再起動が必要です。永続する VDI 展開には、.exe インストーラーをお勧めします。この場合、Microsoft Teams は、HDX セッションが切断された状態のときに自動更新できます。そのため、HDX セッションに再接続するユーザーは、Microsoft Teams が最適化された状態で実行されていないことに気付きます。
> - ローカルセッションから HDX セッションにローミングする場合、HDX で最適化するには Microsoft Teams を再起動する必要があります。この操作は、リモート PC アクセスのシナリオで必要です。

ネットワークの要件

Microsoft Teams は、会議またはマルチパーティ通話で Microsoft 365 のメディアプロセッササーバーに依存します。また、次のシナリオで Microsoft Teams は Microsoft 365 トランスポートリレーに依存します:

- ピアツーピア通話の 2 つのピアが直接接続できない。
- 参加者がメディアプロセッサに直接接続できない。

そのため、ピアと Microsoft 365 クラウドの間のネットワークの状態が通話のパフォーマンスを左右します。ネットワーク計画に関するガイドラインについて詳しくは、Microsoft 365 ネットワーク接続の原則を参照してください。

環境を評価し、クラウド全体のオーディオおよびビデオ環境に影響を与える可能性のあるリスクと要件を特定することをお勧めします。
Skype for Business ネットワーク評価ツールを使用して、ネットワークが Microsoft Teams に対応できるかどうかをテストします。サポート情報については、「サポート」を参照してください。

リアルタイムプロトコル（**RTP**）トラフィックに関する主要なネットワーク推奨事項の要約

- 可能な限りブランチオフィスから直接 Microsoft 365 ネットワークに接続します。
- ブランチオフィスで十分な帯域幅を計画して提供します。
- 各ブランチオフィスのネットワークの接続性と品質について確認してください。
- ブランチオフィスで次のいずれかを使用する必要がある場合は、（Citrix Workspace アプリの HdxRtcEngine.exe で処理される）RTP/UDP のトラフィックが妨げられないことを確認してください。
  - プロキシサーバーのバイパス
  - ネットワークの SSL インターセプト
  - ディープパケットインスペクションデバイス
  - VPN ヘアピン（可能な場合は分割トンネリングを使用）

> 重要：**VPN** 分割トンネリング構成
>
> HdxRtcEngine.exe トラフィックは VPN トンネルから迂回させ、ユーザーのローカルインターネット接続を使用してサービスに直接接続できるようにする必要があります。これを実現する方法は、使用する VPN 製品とマシンプラットフォームによって異なりますが、ほとんどの VPN ソリューションでは、簡単にポリシーを設定してこのロジックを適用できます。VPN プラットフォーム固有の分割トンネルガイダンスについて詳しくは、この Microsoft の記事を参照してください。

Workspace アプリ（HdxRtcEngine.exe）の WebRTC メディアエンジンは、クライアントにオフロードされるマルチメディアストリームの Secure Real-time Transport Protocol（SRTP）を使用します。SRTP は、RTP に機密性と認証を提供します。この機能では、対称キー（DTLS とネゴシエート）を使用してメディアを暗号化し、AES 暗号化を使用してメッセージを制御します。

ポジティブなユーザーエクスペリエンスのために、次の測定基準をお勧めします：

メトリック	エンドポイントから Microsoft 365
遅延（片道）	50 ミリ秒未満

メトリック	エンドポイントから Microsoft 365
遅延（RTT）	100 ミリ秒未満
パケット損失	15 秒間隔で 1% 未満
パケット到着間ジッター	15 秒間隔で 30 ミリ秒未満

詳しくは、「Microsoft Teams 用に組織のネットワークを準備する」を参照してください。

帯域幅の要件に関して、Microsoft Teams 用の最適化では、オーディオ（OPUS/G.722/PCM G711）およびビデオ（H264）用にさまざまなコーデックを使用できます。

ピアは、セッション記述プロトコル（SDP）のオファー/アンサーを使用して、通話の確立プロセス中にこれらのコーデックをネゴシエートします。
Citrix のユーザーごとの最低推奨要件は次のとおりです:

種類	帯域幅	コーデック
オーディオ（片道）	約 90kbps	G.722
オーディオ（片道）	約 60kbps	Opus*
ビデオ（片道）	約 700kbps	H264 360p @ 30 fps 16:9
画面共有	約 300kbps	H264 1080p @ 15 fps

Opus と H264 は、ピアツーピアおよび電話会議に推奨されるコーデックです。

> 重要:
>
> パフォーマンスに関しては、クライアントマシンでの CPU 使用率のために、エンコードにはデコードよりもコストがかかります。Linux および Windows 用の Citrix Workspace アプリで最大エンコーディング解像度をハードコーディングできます。「エンコーダーのパフォーマンス見積もりツール」と「Microsoft Teams の最適化」を参照してください。

プロキシサーバー

プロキシの場所に応じて、次のことを考慮してください:

- VDA でのプロキシ構成:

  VDA で明示的なプロキシサーバーを構成し、プロキシ経由でローカルホストに接続をルーティングすると、リダイレクトは失敗します。プロキシを正しく構成するには、［インターネットオプション］**>**［接続］**>**［**LAN** の設定］**>**［プロキシサーバー］で ［ローカルアドレスにはプロキシサーバーを使用しない］を選択し、`127.0.0.1:9002`がバイパスされるようにする必要があります。

PAC ファイルを使用する場合、PAC ファイルの VDA プロキシ構成スクリプトは`wss://127.0.0.1:9002`に対して **DIRECT** を返す必要があります。そうでない場合、最適化は失敗します。このスクリプトが **DIRECT** を返すようにするには、`shExpMatch(url, "wss://127.0.0.1:9002/*")`を使用します。

- Citrix Workspace アプリでのプロキシ構成:

  ブランチオフィスがプロキシを介してインターネットにアクセスするように構成されている場合、以下のバージョンはプロキシサーバーをサポートします:

  - Windows 向け Citrix Workspace アプリバージョン 2012（Negotiate または Kerberos、NTLM、Basic、および Digest。Pacファイルもサポートされています）
  - Windows 向け Citrix Workspace アプリバージョン 1912 CU5(Negotiate または Kerberos、NTLM、Basic、および Digest。Pacファイルもサポートされています）
  - Linux バージョン 2101 向け Citrix Workspace アプリ（匿名認証）
  - Mac バージョン 2104 向け Citrix Workspace アプリ（匿名認証）

クライアントデバイスで以前のバージョンの Citrix Workspace アプリを使用している場合、プロキシ構成を読み取ることができません。これらのデバイスは、トラフィックを Microsoft 365 TURN サーバーに直接送信します。

> 重要:
>
> - クライアントデバイスが DNS サーバーに接続して DNS 解決を実行できることを確認します。クライアントデバイスは、次の Microsoft Teams Relay サーバーの FQDN を解決できる必要があります:
>
>   ```
>   - worldaz.relay.teams.microsoft.com
>   - inaz.relay.teams.microsoft.com
>   - uaeaz.relay.teams.microsoft.com
>   - euaz.relay.teams.microsoft.com
>   - usaz.relay.teams.microsoft.com
>   - turn.dod.teams.microsoft.us
>   - turn.gov.teams.microsoft.us
>   ```
>
> DNS 要求が失敗した場合、外部ユーザーとの P2P 呼び出しおよび会議通話のメディア確立は失敗します。
>
> - 会議サーバーの場所は、最初の参加者の仮想デスクトップの場所（クライアントではない）に基づいて選択されます。

通話の確立とメディアフローパス

可能な場合、Citrix Workspace アプリの HDX WebRTC メディアエンジン（HdxRtcEngine.exe）は、ピアツーピア通話で、ユーザーデータグラムプロトコル（UDP）上で、直接ネットワーク Secure Real-time Transport Protocol（SRTP）接続を確立しようとします。高 UDP ポートがブロックされている場合、メディアエンジンは TCP/TLS 443 にフォールバックします。

HDX メディアエンジンは、ICE、Session Traversal Utilities for NAT（STUN）、Traversal Using Relays around NAT（TURN）をサポートして、候補の検出と接続の確立を行います。このサポートは、エンドポイントで DNS 解決を実行できる必要があることを意味します。

2 つのピア間、またはピアと会議サーバー間に直接パスがなく、ユーザーがマルチパーティ通話または会議に参加しているとします。HdxRtcEngine.exe は、Microsoft 365 の Microsoft Teams トランスポートリレーサーバーを使用して、会議がホストされているほかのピアまたはメディアプロセッサに到達します。クライアントマシンには、3 つの Microsoft 365 サブネット IP アドレス範囲と 4 つの UDP ポート（または、UDP がブロックされている場合のフォールバックとしての TCP/TLS 443）にアクセスする権限が必要です。詳しくは、「通話のセットアップ」のアーキテクチャの図と「Office 365 の URL と IP アドレスの範囲 ID 11」を参照してください。

ID	カテゴリ	アドレス	ターゲットポート
11	最適化が必要	13.107.64.0/18, 52.112.0.0/14, 52.120.0.0/14	**UDP**：3478、3479、3480、3481、**TCP**：443（フォールバック）

これらの範囲には、Azure Load Balancer によって前処理されたトランスポートリレーとメディアプロセッサの両方が含まれます。
Microsoft Teams トランスポートリレーは、STUN および TURN 機能を提供しますが、ICE エンドポイントではありません。また、Microsoft Teams トランスポートリレーはメディアや TLS を終了せず、トランスコード処理も実行しません。ほかのピアまたはメディアプロセッサにトラフィックを転送するときに、TCP（HdxRtcEngine.exe が TCP を使用している場合）を UDP に中継できます。

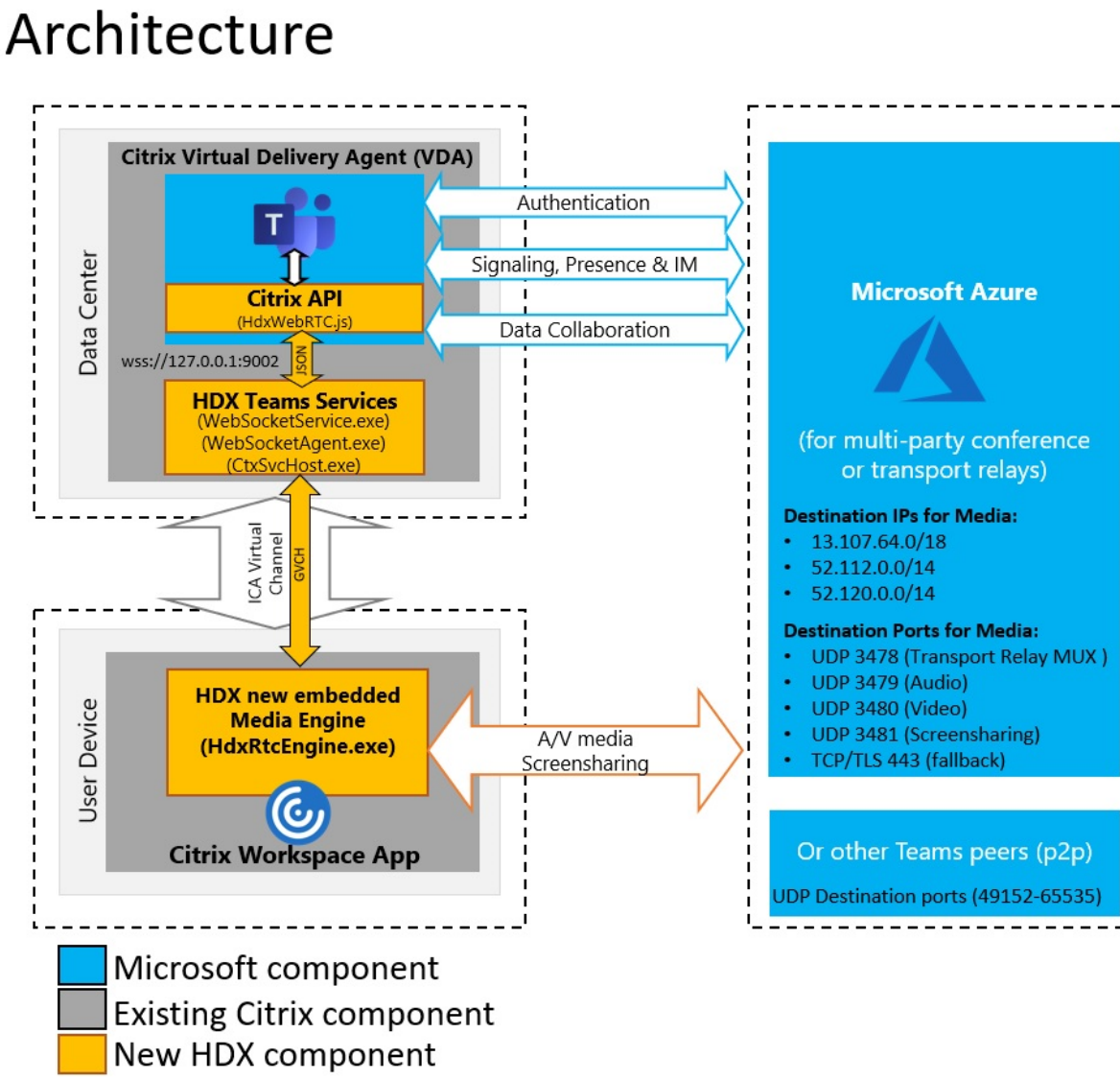
Workspace アプリの WebRTC メディアエンジンは、Microsoft 365 クラウド内の最も近い Microsoft Teams トランスポートリレーと通信します。メディアエンジンは、エニーキャスト IP とポート 3478～3481 UDP（ワークロードごとに異なる UDP ポート、多重化によって発生する場合あり）またはフォールバックに 443 TCP/TLS を使用します。通話品質は、基盤となるネットワークプロトコルによって異なります。UDP は常に TCP よりも推奨されるため、ブランチオフィスの UDP トラフィックに対応するようネットワークを設計することをお勧めします。

Microsoft Teams が最適化モードで読み込まれ、HdxRtcEngine.exe がエンドポイントで実行されている場合、ICE の失敗により、通話のセットアップエラーが発生するか、オーディオ/ビデオが一方通行になります。通話を完了できない場合、またはメディアストリームが全二重でない場合は、最初にエンドポイントの **Wireshark** トレースを確認してください。ICE 候補の収集プロセスについて詳しくは、「サポート」セクションの「ログの収集」を参照してください。

> 注:
>
> エンドポイントにインターネットアクセスがない場合でも、エンドポイントの両方が同じ LAN 上にあれば、ユーザーはピアツーピア通話ができる可能性があります。会議は失敗します。この場合、通話のセットアップが始まる前に 30 秒のタイムアウトがあります。

通話のセットアップ

このアーキテクチャ図は、通知フローシーケンスの視覚的なリファレンスとして使用します。対応する手順が図に示されています。



アーキテクチャ

1. Microsoft Teams を起動します。
2. Microsoft Teams が O365 に認証します。テナントポリシーが Microsoft Teams クライアントにプッシュダウンされ、関連する TURN およびシグナリングチャネル情報がアプリに中継されます。
3. Microsoft Teams は VDA で実行されていることを検出し、Citrix JavaScript API への API 呼び出しを行います。
4. Microsoft Teams 内の Citrix JavaScript は、VDA 上で実行されている WebSocketService.exe へのセキュアな WebSocket 接続を開き、ユーザーセッション内で実行される WebSocketAgent.exe を起動します。

5. WebSocketAgent.exe は、Citrix HDX Microsoft Teams リダイレクトサービス（CtxSvcHost.exe）を呼び出すことによって、汎用仮想チャネルをインスタンス化します。
6. Citrix Workspace アプリの wfica32.exe（HDX エンジン）は、Microsoft Teams の最適化に使用される新しい WebRTC エンジンである HdxRtcEngine.exe という新しいプロセスを生成します。
7. Citrix メディアエンジンと Teams.exe は、双方向仮想チャネルパスを持ち、マルチメディア要求の処理を開始できます。

   ––ユーザー呼び出し――

8. ピア **A** が 呼び出し ボタンをクリックします。Teams.exe は Microsoft 365 の Microsoft Teams サービスと通信し、ピア **B** とのエンドツーエンドのシグナリングパスを確立します。Microsoft Teams は、サポートされている一連の呼び出しパラメーター（コーデック、解像度など、セッション記述プロトコル（SDP）サービスとして知られています）を HdxRtcEngine に要求します。これらの呼び出しパラメーターは、Microsoft 365 の Microsoft Teams サービスへのシグナリングパスを使用して、そこからほかのピアに中継されます。
9. SDP オファーまたは応答（シングルパスネゴシエーション）はシグナリングチャネル経由で実行され、ICE 接続チェック（STUN バインド要求を使用した NAT およびファイアウォールトラバーサル）が完了します。次に、Secure Real-time Transport Protocol（SRTP）メディアは、HdxRtcEngine とほかのピア（または会議の場合は Microsoft 365 会議サーバー）の間で直接やり取りされます。

Microsoft 電話システム

電話システムは、Microsoft Teams を使用して Microsoft 365 クラウドで通話制御および PBX を有効にする Microsoft のテクノロジです。Microsoft Teams の最適化は、Microsoft 365 通話プランまたはダイレクトルーティングを使用する電話システムをサポートします。ダイレクトルーティングを使用すると、オンプレミスのソフトウェアを追加しなくても、サポートされている独自のセッションボーダーコントローラーを Microsoft 電話システムに直接接続できます。
通話キュー、転送、自動転送、保留、ミュート、および通話の再開がサポートされています。

DTMF

デュアルトーンマルチ周波数（DTMF）機能は、次のバージョン以降の Citrix Workspace アプリでサポートされています：

- Windows 向け Citrix Workspace アプリバージョン 2102
- Windows 向け Citrix Workspace アプリ LTSR 1912 CU5（Windows 10 OS のみ）
- Linux 向け Citrix Workspace アプリバージョン 2101
- Mac 向け Citrix Workspace アプリバージョン 2101
- Chrome OS 向け Citrix Workspace アプリバージョン 2111.1

動的緊急通報（**Dynamic e911**）のサポート

バージョン 2112 以降、Citrix Workspace アプリは動的な緊急通報をサポートしています。Microsoft 通話プラン、Operator Connect、ダイレクトルーティングで使用すると、以下を実行できます：

- 緊急電話の構成とルーティング
- セキュリティ担当者への通知。

通知は、VDA で実行されている Microsoft Teams クライアントではなく、エンドポイントで実行されている Citrix Workspace アプリの現在の場所に基づいて送信されます。

Ray Baum 法では、緊急車両を派遣可能な 911 発信者の位置情報を、適切な公衆安全応答ポイント（PSAP）に送信する必要があります。以下のバージョンの Citrix Workspace アプリで使用する場合、HDX を使用した Microsoft Teams 最適化は Ray Baum 法に準拠しています：

- Windows 向け Citrix Workspace アプリバージョン 2112.1 以降
- Linux 向け Citrix Workspace アプリバージョン 2112 以降
- Mac 向け Citrix Workspace アプリバージョン 2112 以降
- Chrome OS 向け Citrix Workspace アプリバージョン 2112 以降

動的緊急通報を有効にするには、管理者は Microsoft Teams 管理センターを使用し、以下を構成して、ネットワークまたは緊急事態発生位置マップを作成する必要があります：

- ネットワーク設定
- 位置情報サービス（Location Information Service：LIS）

動的緊急通報について詳しくは、Microsoft 社のドキュメントを参照してください。

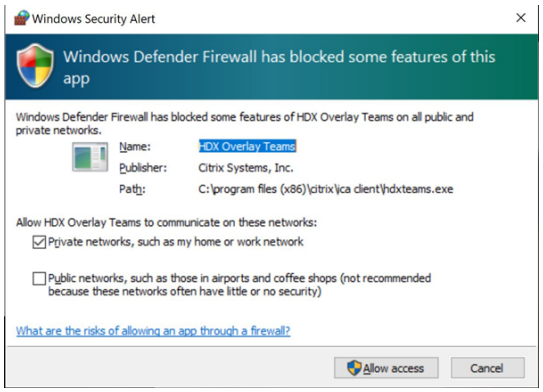
Citrix Workspace アプリが Microsoft Teams に送信する派遣可能位置情報は次のとおりです：

- イーサネット/スイッチ接続にリンク層検出プロトコル（Link Layer Discovery Protocol：LLDP）を使用するシャーシ ID/ポート ID イーサネット/スイッチ（LLDP）は、以下でサポートされています：
  - Windows バージョン 8.1 および 10
  - macOS（LLDP 対応ソフトウェアが必要です）LLDP 対応ソフトウェアをダウンロードするには、`www.microsoft.com`にアクセスして、LLDP 対応ソフトウェアを検索してください。
  - Linux（LLDP ライブラリが、シンクライアントのオペレーティングシステム（OS）ディストリビューションに含まれている必要があります）。
- WLAN BBSID および Citrix Workspace アプリがインストールされているエンドポイントの {IPv4-IPv6; サブネット; MAC アドレス}。
  - サブネットおよび WiFi ベースの場所情報は、Windows、Linux、および Mac 用の Workspace アプリでサポートされています。
- 緯度と経度（Citrix Workspace アプリがインストールされている OS レベルにおいてユーザー権限が付与されている場合）。

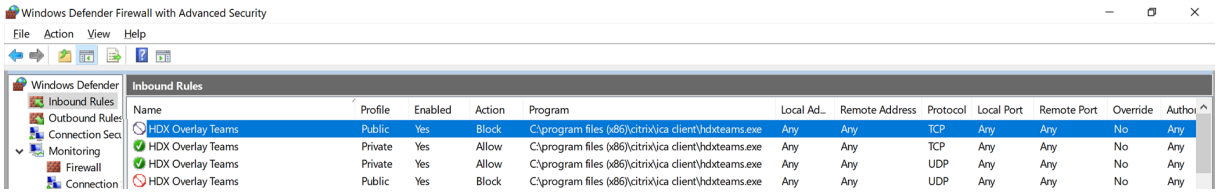
- すべての Workspace アプリプラットフォームでサポートされています。ただし、Linux 向け Citrix Workspace の場合、シンクライアントの OS ディストリビューションに`libgps`ライブラリを含める必要があります（sudo apt-get install libgps23 gpsd lldpd）。

ファイアウォールについての考慮事項

ユーザーが初めて Microsoft Teams クライアントを使用して最適化された呼び出しを開始すると、**Windows** ファイアウォール設定の警告が表示されることがあります。この警告は、HdxTeams.exe または HdxRtcEngine.exe（HDX Overlay Microsoft Teams）の通信を許可するようユーザーに求めます。



以下の 4 つのエントリが ［セキュリティが強化された **Windows Defender** ファイアウォール］コンソールの ［受信規則］に追加されます。必要に応じて、より制限的な規則を適用できます。

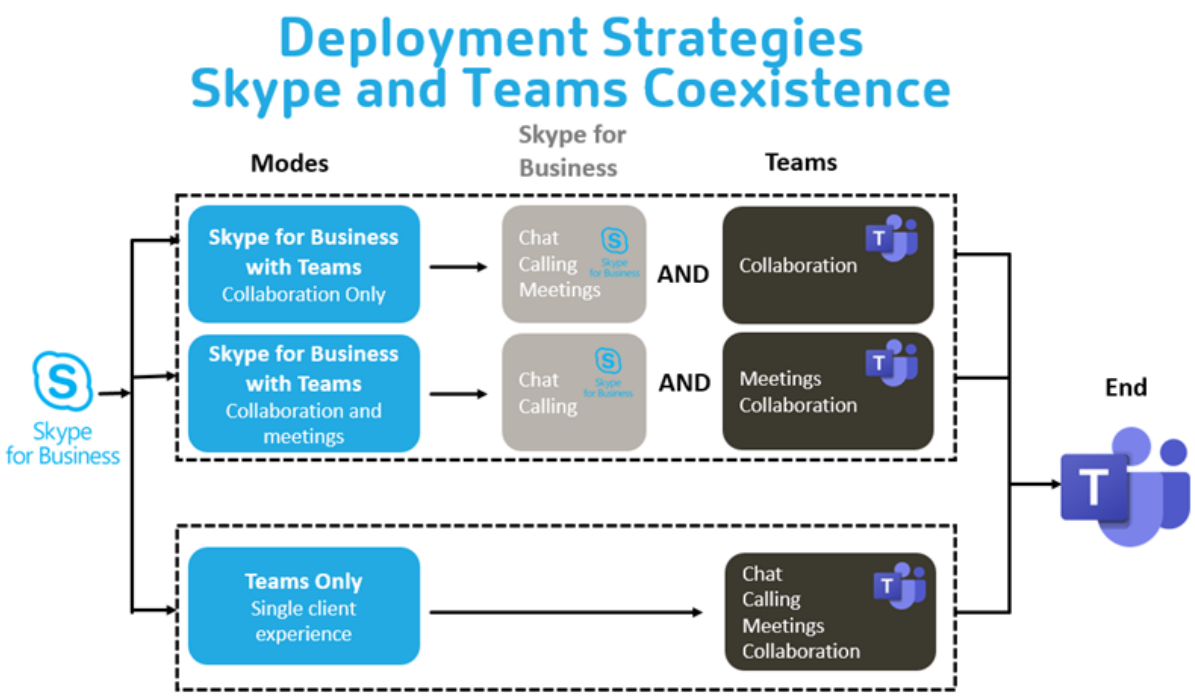


Microsoft Teams と **Skype for Business** の共存

Microsoft Teams と Skype for Business を、機能が重複する 2 つの個別のソリューションとして並べて展開できます。
詳しくは、「Microsoft Teams と Skype for Business の共存と相互運用性の理解」を参照してください。

Microsoft Teams マルチメディアエンジン用の Citrix RealTime Optimization Pack および HDX 最適化は、環境で設定された構成を尊重します。例としては、アイランドモードや Skype for Business と Microsoft Teams のコラボレーションがあります。また、Skype for Business と Microsoft Teams のコラボレーションと会議もあります。

周辺機器アクセス権限は、一度に 1 つのアプリケーションにのみ付与されます。たとえば、通話中に RealTime Media Engine が Web カメラにアクセスすると、通話の間、イメージデバイスがロックされます。デバイスがリリースされると、Microsoft Teams で使用できるようになります。



Citrix SD-WAN：**Microsoft Teams** 向けに最適化されたネットワーク接続

オーディオとビデオの最適な品質には、Microsoft 365 クラウドへのネットワーク接続で低遅延、低ジッター、低パケット損失が必要です。Citrix Workspace アプリユーザーによるブランチオフィスからデータセンターへの Microsoft Teams 音声ビデオ RTP トラフィックのバックホールで追加の遅延が発生することがあります。また、WAN リンクで輻輳が発生することがあります。Citrix SD-WAN は Microsoft 365 ネットワーク接続の原則に従って、Microsoft Teams の接続を最適化します。Citrix SD-WAN は、Microsoft REST ベースの Microsoft 365 IP アドレスと Web サービス、および近接 DNS を使用します。この用途は、Microsoft Teams のトラフィックを識別、分類、誘導するためのものです。

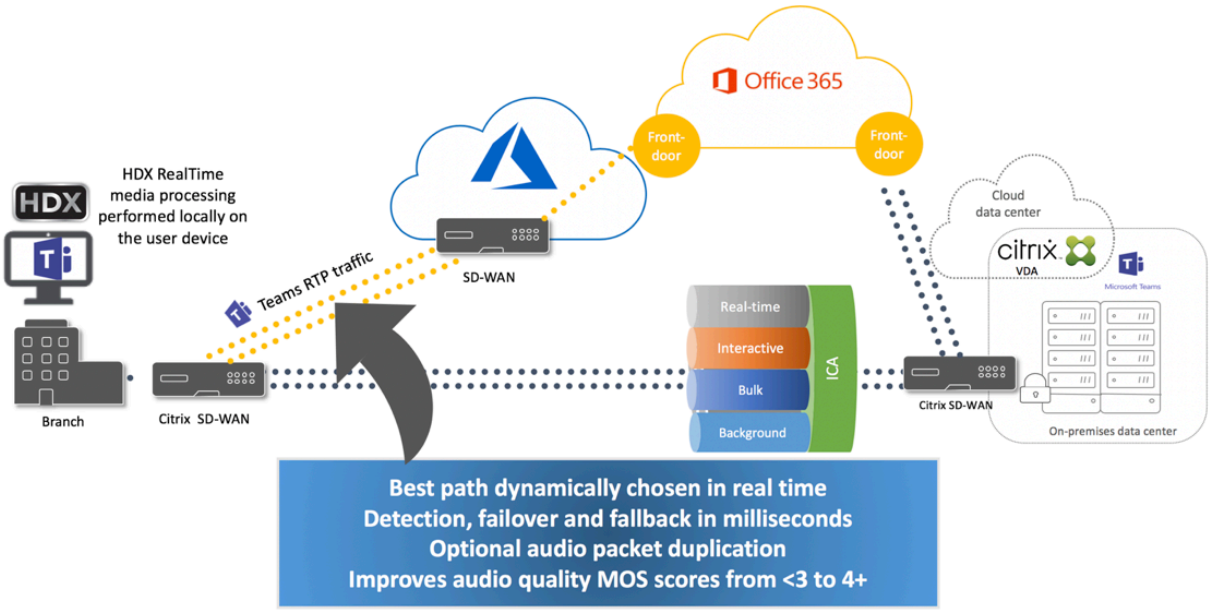
多くの地域のビジネス用ブロードバンドインターネット接続は、断続的なパケット損失、過度のジッター期間、停止に悩まされています。

Citrix SD-WAN は、ネットワークの状態がさまざまに異なる場合、または低下している場合、Microsoft Teams のオーディオ/ビデオ品質を保持する 2 つのソリューションを提供します。

- Microsoft Azure を使用している場合、Azure VNET で導入された Citrix SD-WAN 仮想アプライアンス（VPX）は、高度な接続の最適化を提供します。これらの最適化には、シームレスなリンクフェールオーバーとオーディオパケットトレースが含まれます。
- Citrix SD-WAN のお客様は Citrix Cloud Direct サービスを介して Microsoft 365 に接続できます。このサービスは、すべてのインターネットのトラフィックに信頼できる安全な配信を提供します。

ブランチオフィスのインターネット接続の品質が問題にならない場合は、遅延を最小限に抑えるのに十分な可能性があります。Microsoft Teams のトラフィックを、Citrix SD-WAN ブランチアプライアンスから一番近い Microsoft

365 フロントドアに直接誘導して、遅延を最小限に抑えます。詳しくは、「Citrix SD-WAN Office 365 の最適化」を参照してください。



マルチウィンドウ会議とチャット

Windows の Microsoft Teams では、複数の会議またはチャットウィンドウを使用できます。ポップアウト機能について詳しくは、Microsoft 365 サイトのMicrosoft Teams のチャットおよび会議でのポップアウトウィンドウに関する記事を参照してください。

> 注:
>
> この機能は、Windows 2112.1、Mac 2203、Linux 2203、および ChromeOS 2303 向けの Citrix Workspace アプリでサポートされています。この場合 VDA 2112 以降が必要であり、1912 CU6 以降の LTSR、VDA 2112 にバックポートされました。

背景のぼかしと効果

Windows 向け、Mac 向け、Linux 向けおよび ChromeOS/HTML5 向け Citrix Workspace アプリで、HDX を使用した Microsoft Teams の最適化における背景のぼかしと効果がサポートされます。

背景をぼかしたり、デフォルト画像に置き換えたりして、会話中にシルエット（体と顔）に集中できるようにすることで、集中力が乱されることを回避できます。この機能は、P2P 通話または電話会議で使用できます。

> 注:
>
> この機能は、Microsoft Teams の UI/ボタンと統合されています。マルチウィンドウのサポートは、VDA を 2112 以降に更新するときに必要な前提条件です。詳しくは、「マルチウィンドウ会議とチャット」を参照して

> ください。

背景のぼかしと効果に関する Microsoft Teams UI コントロールを利用するには、次の最小バージョンが必要です:

- Windows 向け Citrix Workspace アプリ 2207
- Mac 向け Citrix Workspace アプリ 2301
- Linux 向け Citrix Workspace アプリ 2212
- ChromeOS 向け Citrix Workspace アプリ 2303

制限事項:

- クライアントで背景画像を Microsoft Teams のデフォルト画像に置き換えるときは、デバイスをインターネットに接続する必要があります。
- 管理者およびユーザーが定義した背景画像の置き換えは Microsoft Teams の UI ではサポートされていません。カスタムの背景画像は、画像がクライアントにも保存されている限り、構成設定を使用して設定できます。

カスタムの背景画像の設定

次のレジストリキーは、Microsoft Teams UI を使用して機能を制御する予定がない場合、または管理者がデフォルトの動作を上書きしたい場合にのみ必要です。たとえば、エンドポイントの性能が十分ではないため、背景のぼかしを無効にするなど。

Windows の場合　カスタムの背景画像を設定するには、管理者またはエンドユーザーがクライアントまたはエンドポイントで次のレジストリキーを構成する必要があります:

場所: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`

- 名前: VideoBackgroundEffect
- 種類: DWORD
- 値: 0（無効）、1（有効）、2（背景画像の置換）

値を 1 に設定すると、背景がぼやけます。この値は、エンドユーザーまたは管理者が設定できます。

値を 2 に設定するには、**VideoBackgroundImage** キーも存在する必要があります。この値を設定できるのは管理者だけです。次のキーは、背景画像を置き換えたい場合にのみ必要であり、ぼかしには必要ありません:

- 名前: VideoBackgroundImage
- 種類: REG_SZ
- 値: my_image_name.jpeg

ビデオの背景画像は`C:\Program Files (x86)\Citrix\ICA Client`ディレクトリに格納されている必要があります。

このレジストリ構成によって、Microsoft Teams UI セレクターを使用せずに、Citrix Workspace アプリ 2206 で背景のぼかしまたは画像の置換を有効にすることもできます。つまり、環境または VDA がマルチウィンドウをサポートしていない場合でも、Citrix Workspace アプリ 2206 以降で HKEY_CURRENT_USER レジストリによる回避策を適用して同様の結果を得ることができます。ただし、ユーザーは HDX セッションまたは Microsoft Teams 通話中に機能を制御することはできません。

レジストリキーの変更は、HDX セッションが接続されたときにのみ有効になります。

Mac の場合　ユーザーがダウンロードした画像の場所：*/Users/username/Downloads/any_image.png*

次のコマンドを実行して、カスタム画像をデフォルトの画像として設定します：

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundEffect -int 2

defaults write com.citrix.HdxRtcEngine VideoBackgroundImage -string "
/Users/username/Downloads/any_image.png"
```

Linux の場合　ユーザーがダウンロードした画像の場所：*/home/username/Downloads/any_image.jpg*

ファイル*/var/.config/citrix/hdx_rtc_engine/config.json* を作成して、次の構成キーを JSON 形式で追加します。例：

```
{


"VideoBackgroundEffect":2,

"VideoBackgroundImage":"/home/username/Downloads/any_image.jpg"

 }

<!--NeedCopy-->
```

HTML5 の場合　HTML5 の場合、背景のぼかしのみがサポートされます。カスタムイメージの置換はサポートされていません。

背景をぼかすには、次の手順を実行します：

1. **HTML5Client** フォルダーの **configuration.js** ファイルに移動します。
2. **backgroundEffects** 属性を追加し、この属性を **true** に設定します。例：

```
'features' : {

    'msTeamsOptimization' :
    {

        'backgroundEffects' : true
```



```
7         }
8
9     }
10
11  <!--NeedCopy-->
```

3. 変更を保存します。

クライアントの **CPU** 消費に関する考慮事項

ぼかし機能による CPU への影響はわずかですが、消費量の増加が予想されます。たとえば、最大 2.8GHz のターボブーストを利用した 4 コア、1.5GHz の Intel® Pentium® Silver チップを搭載したシンクライアントでは、背景のぼかしによって CPU 使用率が約 2% 上昇します。平均 CPU 使用率は 20% 未満です。

Microsoft Teams のギャラリービューとアクティブスピーカー

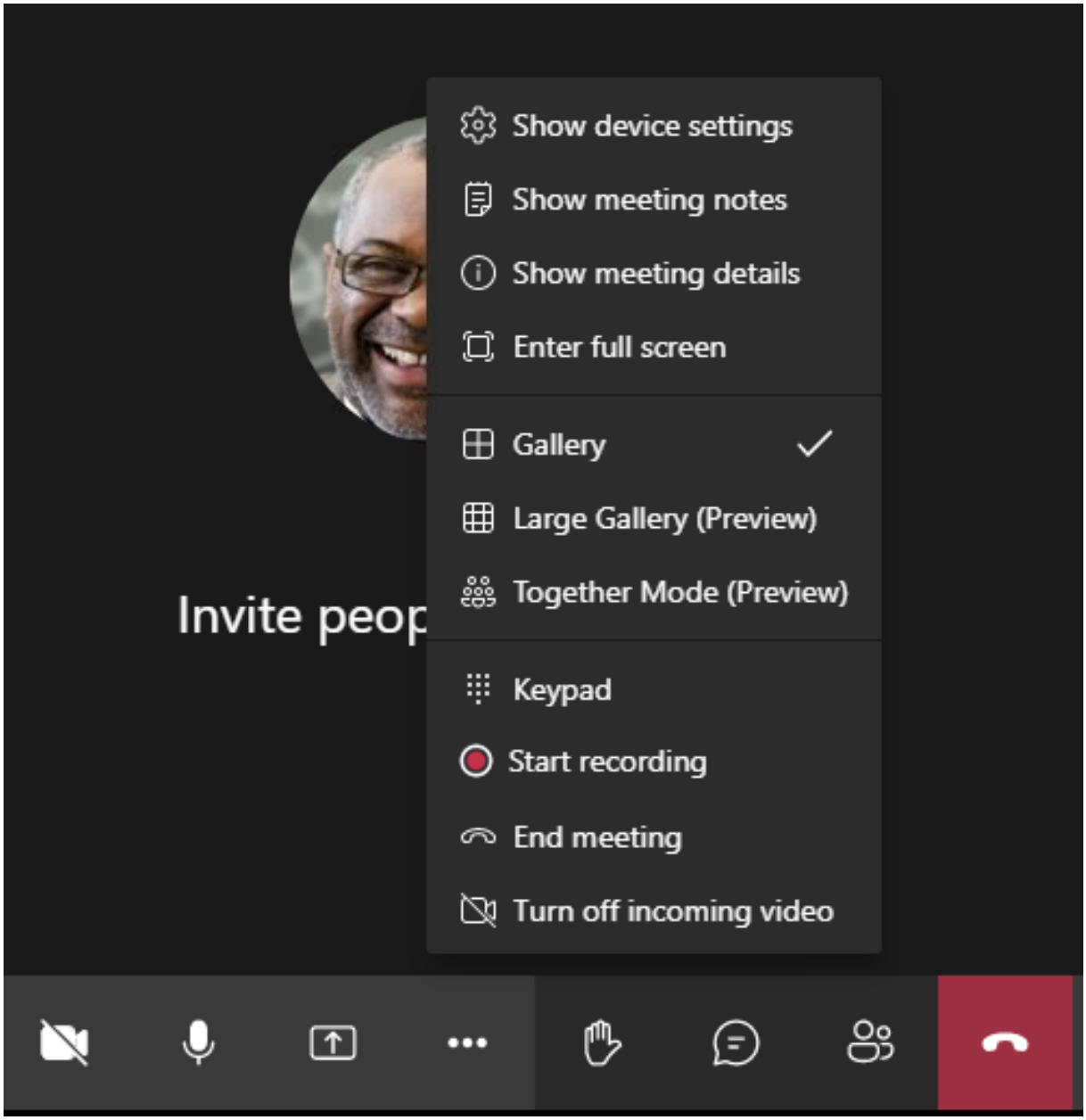
Microsoft Teams は、[ギャラリー]、[大きいギャラリー]、および［集合モード］のレイアウトをサポートしています。

Microsoft Teams は、4 人の参加者のビデオストリームによる 2x2 グリッドを表示します（ギャラリーと呼ばれます）。この場合、Microsoft Teams はデコードのために 4 つのビデオストリームをクライアントデバイスに送信します。ビデオを共有している参加者が 4 人を超える場合、最新の 4 人のうち最もアクティブなスピーカーのみが画面に表示されます。

Microsoft Teams は、最大 7x7 のグリッドを表示する大きなギャラリービューも提供します。その結果、Microsoft Teams 会議サーバーは単一のビデオフィードを合成し、それをデコードのためにクライアントデバイスに送信するため、CPU 消費量を抑えられます。この単一のマス目形式のフィードには、ユーザーのセルフプレビュービデオも含まれることがあります。

最後に、Microsoft Teams は、新しい会議エクスペリエンスの一部である集合モードをサポートしています。Microsoft Teams は、AI セグメンテーションテクノロジを使用して参加者を共有の背景にデジタルで配置し、すべての参加者を同じホールの客席に表示します。

ユーザーは、省略記号メニューで［ギャラリー]、[大きいギャラリー]、または［集合モード］のレイアウトを選択することにより、会議中にこれらのモードを制御できます。



ビデオのアスペクト比の制限のサポート（Windows 向け Citrix Workspace アプリ 2102、Linux 向け Citrix Workspace アプリ 2106、MAC 向け Citrix Workspace アプリ 2106 以降）:

- ［**Fill to frame**］オプションは、［Gallery］ビューまたは［Large Gallery］ビューで使用できます。このオプションにより、サブウィンドウに収まるようにビデオサイズがトリミングされます。一方、［**Fit to frame**］を使用すると、ビデオの側面に黒いバー（レターボックス）が表示され、トリミングが行われません。

次の表に、［ギャラリー］と［大きいギャラリー］のレイアウトの比較を示します:

	［ギャラリー］ビュー 2x2（デフォルト）	［大きいギャラリー］ビュー
レイアウト/グリッド	4 人の参加者がいるビデオストリームでは 2x2 のグリッドが表示されます。直近の最もアクティブなスピーカー 4 人のみが画面に表示され、他の参加者はグリッドに表示されません。	49 人の参加者がいるビデオストリームでは 7x7 のグリッドが表示されます。
ミキシング技法	メディアルーターは、各参加者からすべてのユーザーに個々のストリームを転送します。	中央会議サーバーは、すべてのオーディオまたはビデオをミキシングおよびトランスコードして、参加者ごとに調整した複合レイアウトを作成します。この操作により、さらに遅延が発生します。
アクティブなスピーカー	新しいアクティブなスピーカーは、グリッド内で最もアクティブでないスピーカーに取って代わります。	アクティブか非アクティブかに関係なく、すべての参加者が表示されます。
エンドポイントでのエンコード	サイマルキャストが有効な場合、1 つまたは複数のビデオストリームがエンドポイントでエンコードされる可能性があります。サイマルキャストのサポートについて詳しくは、「サイマルキャスト」を参照してください。	サイマルキャストが有効な場合、1 つまたは複数のビデオストリームがエンドポイントでエンコードされる可能性があります。サイマルキャストのサポートについて詳しくは、「サイマルキャスト」を参照してください。
エンドポイントでのデコード	各参加者は、最大 4 つの個別のメディアストリームを取得します。これにより、HdxRtcEngine.exe によるエンドポイントでの CPU 消費量が増加します（デコードおよびレンダリングのため）。	各参加者は、オーディオとビデオのストリームを 1 つだけ取得します。この設定により、エンドポイントでの CPU 消費量が減少します。
最大解像度	720p。4 人の参加者がビデオを共有している場合、最大解像度はビデオフィードあたり 360p です。参加者 4 人未満でビデオを共有している場合は、ビデオフィードあたりの解像度が高くなる可能性があります。	複合レイアウトまたはミキシングの場合は 720p です。複合レイアウトでは、参加者ごとに高品質のビデオストリームは必要ありません。この条件のため、各送信者が解像度やアップロードのビットレートを下げます。

	［ギャラリー］ビュー 2x2（デフォルト）	［大きいギャラリー］ビュー
「低速ユーザー」の問題	送信者は、各モダリティ（オーディオ、ビデオ、および画面共有）の品質を、参加者間で最も低い共通ネットワーク品質に変更します。このマルチメディアストリームは、その後、他のすべての参加者に転送されます。その結果、ネットワーク状態が悪い参加者が、その通話に参加している他のすべての人の品質に影響を与えます。	最も低品質な共通ネットワークのシナリオには左右されません。会議サーバーは、個々の参加者のネットワーク状態に基づいてさまざまな品質を提供します。
セルフプレビュー	自分自身を小さなサムネイルでリアルタイムで表示します。	自分自身をサムネイルで表示し、残りのビデオフィードとは区別しません。その結果、メインのビデオレイアウトに自分が含まれ、多少の遅延がさらに発生する場合があります。

Microsoft Teams の画面共有

Microsoft Teams は、H264 のようなビデオコーデックで共有されているデスクトップを効果的にエンコードし高画質ストリームを作成する、ビデオベースの画面共有（VBSS）に依存しています。HDX 最適化により、受信画面共有はビデオストリームとして扱われます。

Windows、Linux、または Mac 向けの Citrix Workspace アプリ 2109 以降および ChromeOS 向け Citrix Workspace アプリ 2303 以降のユーザーは画面とビデオカメラを同時に共有できます。

以前のバージョンでは、ビデオ通話の最中にほかのピアがデスクトップの共有を開始すると、元のカメラのビデオフィードが一時停止されます。代わりに、画面共有ビデオフィードが表示されます。その後、このピアは手動でカメラ共有を再開する必要があります。

> **PowerPoint Live** に関するメモ
>
> PowerPoint Live のコンテンツを共有している場合、この制限はありません。その場合でも、他のピアは Web カメラとコンテンツを確認し、前後に移動して他のスライドを確認できます。このシナリオでは、スライドは VDA でレンダリングされています。PowerPoint Live スライドデッキにアクセスするには、［Share tray］ボタンをクリックして提案された PowerPoint スライドの 1 つを選択するか、［Browse］をクリックしてコンピューターまたは OneDrive で PowerPoint ファイルを検索します。

発信画面共有も最適化され Citrix Workspace アプリにオフロードされます。この場合、メディアエンジンは、周りに赤い境界線が描画された Citrix Desktop Viewer（CDViewer.exe）ウィンドウのみをキャプチャして送信します。Desktop Viewer と重複するローカルアプリケーションはキャプチャされません。

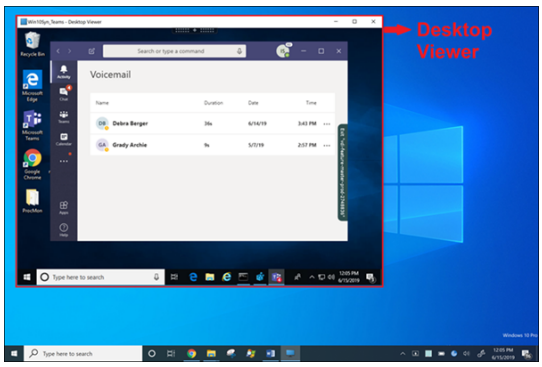
> 注
>
> Mac 向け Citrix Workspace アプリでの特定の権限を設定して、画面共有を有効にします。詳しくは、「システム要件」を参照してください。

マルチモニター

Desktop Viewer（CDViewer.exe）が全画面モードでマルチモニターセットアップ全体にまたがる場合、Citrix Workspace アプリ 2106 以降（Windows/Linux/Mac）では、共有するモニターをスクリーンピッカーで選択できます。

既知の制限事項:

- Desktop Viewer が無効になっている場合、または Desktop Lock が使用されている場合は、マルチモニターは Microsoft Teams のスクリーンピッカーで選択できません。Desktop Viewer は、`.ICA`ファイルテンプレートと`StoreFront web.config`のいずれかを編集したことで、無効になっている可能性があります。SHIFT+F2 ホットキーはマルチモニターの画面共有と互換性がありません。
- Workspace アプリの 2106 より前のバージョンでは、プライマリモニターのみが共有されます。仮想デスクトップ上のアプリケーションを、通話中のほかのピアのプライマリモニターにドラッグして表示します。
- 仮想モニターレイアウト機能（単一の物理モニターの論理パーティション）を使用して Citrix Workspace アプリを構成した場合は、マルチモニター画面共有が機能しないことがあります。この場合、すべての仮想モニターが 1 つの合成画像として共有されます。
- 古いバージョンの Windows 向け Citrix Workspace アプリ（1907 から 2008）では、クライアントマシンで実行されているローカルアプリケーションも共有されます。この共有は、ローカルアプリが Desktop Viewer の上に重なっている場合にのみ可能です。この動作は、2009.6 以降、および 1912 CU5 以降で削除されました。
- 画面共有中にウィンドウモードから全画面に変更すると、画面共有が停止します。画面共有を機能させるには、停止して再度共有する必要があります。



シームレスアプリケーションからの画面共有:

Microsoft Teams をスタンドアロンのシームレスアプリケーションとして公開している場合、画面共有は、物理エンドポイントのローカルデスクトップをキャプチャします。Citrix Workspace アプリのバージョンは 1909 以降である必要があります。

アプリの共有

Windows 2112.1 および VDA 2112 向け Citrix Workspace アプリ以降、Microsoft Teams はアプリ共有をサポートしています。

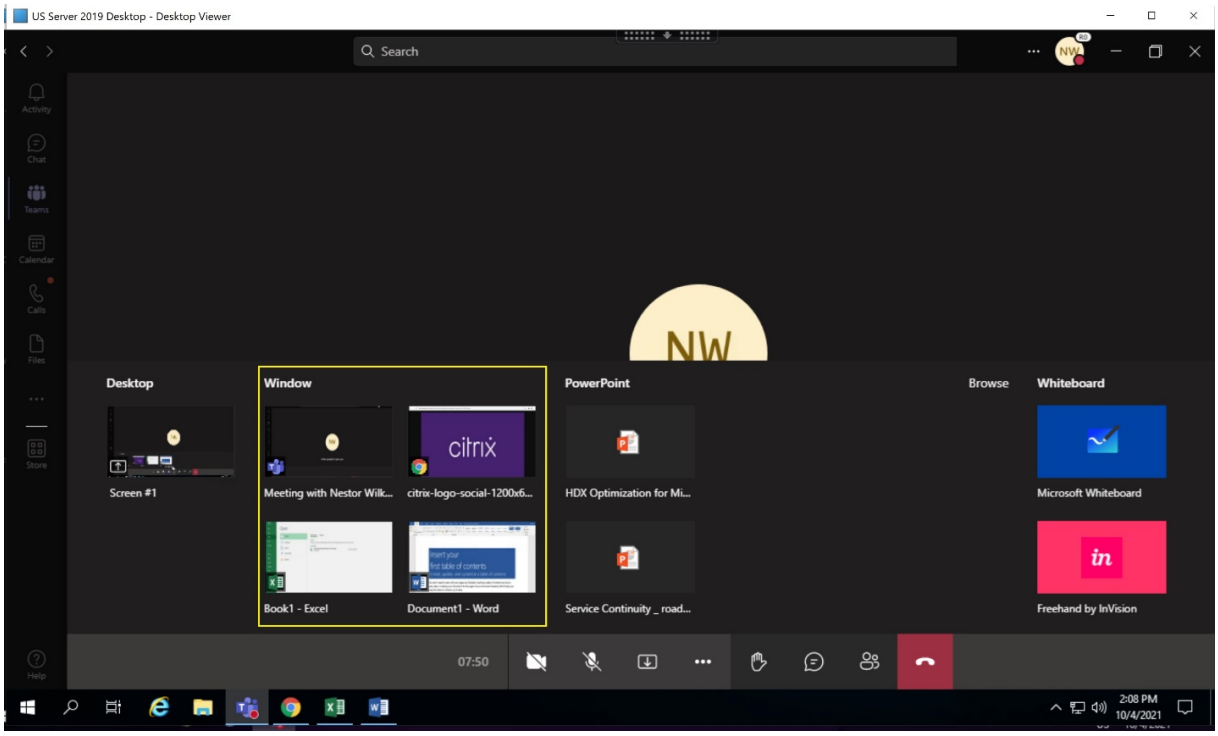
Citrix Workspace アプリの Windows 向け 2109、Mac 向け 2203、Linux 向け 2209、および VDA 向け 2109 以降では、Microsoft Teams が仮想セッションで実行されている特定のアプリの画面共有をサポートしています。特定のアプリを共有するには:

1. リモートセッション内の Microsoft Teams アプリに移動します。
2. Microsoft Teams UI の ［コンテンツの共有］をクリックします。
3. 会議で共有するアプリを選択します。選択したアプリの周りに赤い枠線が表示され、通話中の同僚は共有アプリを確認できます。

別のアプリを共有するには、もう一度 ［コンテンツの共有］をクリックして、新しいアプリを選択します。

アプリの共有を無効にする場合は、`HKLM\SOFTWARE\Citrix\Graphics`の VDA に次のレジストリキーを作成します:
名前: `UseWsProvider`
種類: `DWORD`
値: 0

> 注:
>
> - Microsoft によって更新プログラムがロールアウトされたら、ドキュメントのアップデートおよび発表内容について、CTX253754を確認することができます。
> - アプリを最小化すると、Microsoft Teams は共有アプリの最後のイメージを表示します。ウィンドウを最大化すると、画面共有を再開できます。
> - 画面共有は、ウィンドウの VDA 側のキャプチャに依存します。その後、コンテンツは最大速度で Citrix Workspace アプリに中継されます。最大速度は毎秒 30 フレームです。Citrix Workspace アプリは、コンテンツをピアまたは会議サーバーに転送します。



特定のアプリの画面共有に関する既知の制限:

- アプリを画面共有しているときは、マウスポインターは表示されません。
- アプリを共有しているときにアプリを最小化すると、アプリアイコンのみがスクリーンピッカーに表示されます。アプリのサムネイルはスクリーンピッカーでプレビューされません。そのコンテンツを共有することはできず、アプリを最大化するまで赤い枠線は表示されません。
- LAA アプリは、VDA の最適化された Microsoft Teams のデスクトップアプリと共有できるアプリの一覧を表示します。ただし、一覧からアプリを選択すると、想定した結果にならない場合があります。

App Protection との互換性

特定のアプリの画面共有は、HDX 最適化の Microsoft Teams のアプリ保護機能と互換性があります。App Protection が有効になっているデリバリーグループからアプリまたはデスクトップを起動した場合は、特定のアプリを画面共有できます。

Microsoft Teams UI で ［コンテンツの共有］をクリックすると、画面選択メニューから ［デスクトップ］オプションが削除されます。開いているアプリを共有するために選択できるオプションは ［ウィンドウ］だけです。

> 注:
>
> App Protection が有効になっているデリバリーグループからアプリまたはデスクトップを起動すると、着信ビデオや画面共有を表示できません。

Microsoft Teams での制御の付与と要求　この機能は、Citrix Workspace アプリの以下のバージョンでサポートされています（VDA バージョンまたはオペレーティングシステム、シングルセッションまたはマルチセッションへの依存はありません）:

- Windows 向け Citrix Workspace アプリバージョン 2112.1 以降
- Mac 向け Citrix Workspace アプリバージョン 2203.1 以降
- Linux 向け Citrix Workspace アプリバージョン 2203 以降
- ChromeOS 向け Citrix Workspace アプリバージョン 2303 以降

参加者が画面を共有しているときに、Microsoft Teams の通話中に制御を要求できます。制御できるようになると、共有画面に対して選択、編集、またはその他のキーボードとマウスのアクティビティを実行できます。

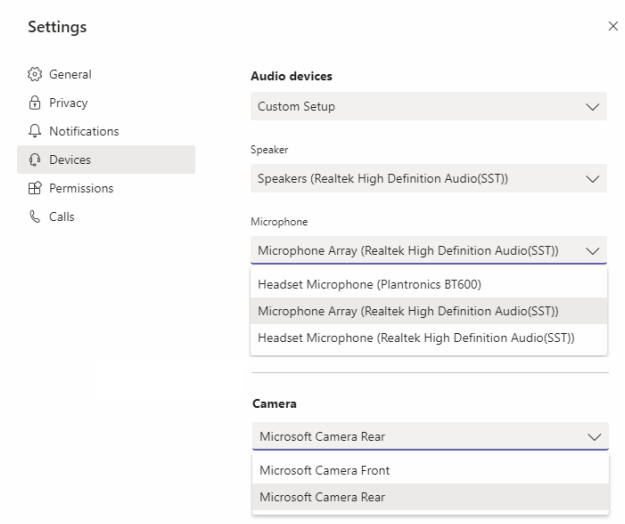
画面が共有されているときに制御を取得するには、Microsoft Teams UI の ［制御を要求］ボタンをクリックします。画面を共有している会議参加者は、要求を許可または拒否できます。

制御中は、共有画面に対して選択、編集、その他の変更を実行できます。これらの操作には、キーボードとマウスの両方を使用できます。入力が完了したら、［制御を要求］をクリックします。

> 制限事項:
>
> - ユーザーが単一のアプリを共有している場合（アプリ共有）、制御の付与および要求は実行できません。デスクトップまたはモニター全体を共有する必要があります。
> - コントロールバーを特定の場所に固定する機能は使用できません。

Microsoft Teams の周辺機器

Microsoft Teams の最適化がアクティブな場合、Citrix Workspace アプリは周辺機器に（ヘッドセット、マイク、カメラ、スピーカーなど）にアクセスします。その後、周辺機器は Microsoft Teams UI に正しく表示されます（[設定] **>** ［デバイス］）。



Microsoft Teams はデバイスに直接アクセスしません。メディアの取得、キャプチャ、処理には、代わりに Workspace アプリの WebRTC メディアエンジンが使用されます。Microsoft Teams では、ユーザーが選択できるデバイスが一覧表示されます。

Microsoft Teams がアクティブなときに挿入される周辺機器は、デフォルトでは選択されていません。Microsoft Teams UI の ［設定］ > ［デバイス］画面で、周辺機器を手動で選択する必要があります。周辺機器が選択されると、Microsoft Teams は周辺機器の情報をキャッシュします。これにより、同じエンドポイントからセッションに再接続すると、周辺機器が自動的に選択されます。

推奨事項:

- エコーキャンセル機能が組み込まれたMicrosoft Teams 認定ヘッドセット。マイクとスピーカーが別のデバイスにある複数周辺機器セットアップでは、エコーが発生することがあります。これは、マイクが Web カメラに内蔵されており、スピーカーがモニターに搭載されている場合などです。外部スピーカーを使用する場合は、マイクからできるだけ離して配置してください。また、マイクに音を反響させる可能性のある表面からも離して配置してください。
- Microsoft Teams 認定のカメラ。ただし、Skype for Business 認定の周辺機器は Microsoft Teams と互換性があります。
- Citrix Workspace アプリのメディアエンジンは、オンボード H.264 エンコーディング-UVC 1.1 および 1.5 を実行する Web カメラで CPU オフロードを利用できません。

> 注:
>
> Windows 向け Workspace アプリ 2009.6 では、24 ビットのオーディオ形式または 96kHz を超える周波数のオーディオ形式の周辺機器を取得できるようになりました。
>
> HdxTeams.exe（Windows 2009 以前の Citrix Workspace アプリ内）は、次の特定のオーディオデバイス形式（チャネル、ビット深度、およびサンプルレート）のみをサポートします:
>
> - 再生デバイス：最大 2 チャネル、16 ビット、最大 96,000Hz の周波数
> - 録音デバイス：最大 4 チャネル、16 ビット、最大 96,000Hz の周波数
>
> 1 つのスピーカーまたはマイクが通常の設定と一致しない場合でも、Microsoft Teams のデバイス列挙は失敗し、［設定］**>**［デバイス］になしが表示されます。
> **HdxTeams.exe** の
> **Webrpc** ログはこのような情報を表示します:
>
> ```
> Mar 27 20:58:22.885 webrtcapi.WebRTCEngine Info: init. initializing
> ...
> Mar 27 20:58:23.190 webrtcapi.WebRTCEngine Error: init. couldn't
> create audio module!
> ```
>
> 回避策として、特定のデバイスを無効にするか、以下を実行します:
>
> 1. サウンドコントロールパネル（mmsys.cpl）を開きます。
> 2. 再生デバイスまたは録音デバイスを選択します。
> 3. ［プロパティ］**>**［詳細設定］に移動し、サポートされているモードに設定を変更します。

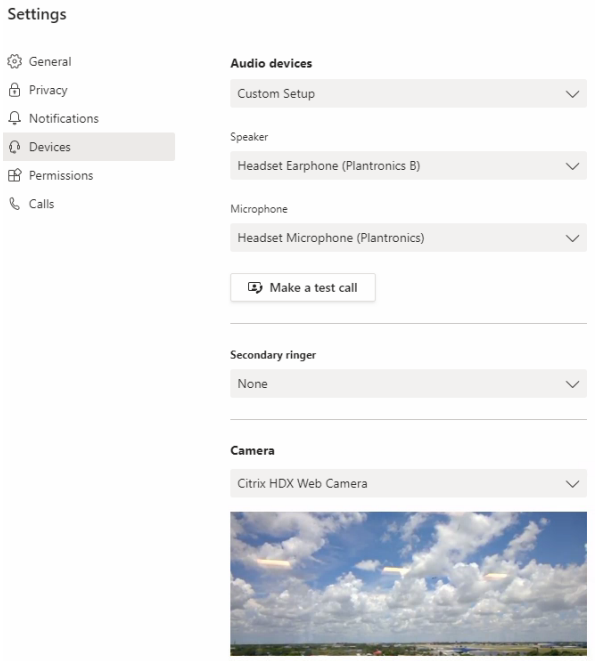
フォールバックモード

最適化された VDI モードで Microsoft Teams が読み込めない場合（Teams/About/Version で「Citrix HDX 未接続」）、VDA では従来の HDX テクノロジにフォールバックされます。従来の HDX テクノロジとしては、Web カメラリダイレクトやクライアントのオーディオとマイクのリダイレクトなどが挙げられます。Microsoft Teams の最適化をサポートしていない Workspace アプリのバージョンまたはプラットフォーム OS を使用している場合は、フォールバックレジストリキーが適用されません。
フォールバックモードでは、周辺機器が VDA にマップされます。周辺機器は、Microsoft Teams アプリには仮想デスクトップにローカルで接続されているように表示されます。

VDA でレジストリキーを設定することで、フォールバックメカニズムを細かく制御できるようになりました。詳しくは、レジストリを介して管理される機能の一覧にある「Microsoft Teams フォールバックモード」を参照してください。

この機能を使用するには、Microsoft Teams バージョン 1.3.0.13565 以降が必要です。

Microsoft Teams アプリの ［設定］**>**［デバイス］タブで表示されるカメラ名の違いで、最適化モードか非最適化モードかを判断できます。Microsoft Teams が非最適化モードで読み込まれた場合、従来の HDX テクノロジが起動します。以下の画像のように、Web カメラ名の冒頭には **Citrix HDX** が表示されます。スピーカーとマイクのデバイス名は、最適化モードと比べてわずかに異なる（または省略される）場合があります。



従来の HDX テクノロジを使用する場合、Microsoft Teams はオーディオ、ビデオ、および画面共有処理をエンドポイントの Citrix Workspace アプリ WebRTC メディアエンジンにオフロードしません。代わりに、HDX テクノロジでサーバー側でのレンダリングが使用されます。ビデオをオンにすると、VDA の CPU 消費量が高くなることが予想されます。リアルタイムのオーディオパフォーマンスは最適ではない場合があります。

既知の制限事項

Citrix の制限

Citrix Workspace アプリでの制限:

- HID ボタン - 応答と通話終了はサポートされていません。音量の増減はサポートされています。
- Microsoft Teams の管理センターの QoS（サービス品質）設定は、VDI ユーザーには適用されません。
- Citrix Workspace アプリの App Protection アドオン機能は、発信画面共有を妨げ、受信画面共有およびビデオを禁止します。
- VDA で Snipping Tool を使用している場合、ユーザーは Microsoft Teams コンテンツのスクリーンショットを撮ることができません。ただし、Snipping Tool をクライアント側で使用した場合は、コンテンツをキャプチャできます。

VDA での制限:

- Citrix Workspace アプリの高 DPI 設定を ［はい］にすると、リダイレクトされたビデオウィンドウがずれて表示されます。この制限は、モニターの DPI スケールファクターが 100% を超えて設定されている場合に発生します。

Citrix Workspace アプリと VDA での制限:

- 最適化された通話の音量は、VDA ではなくクライアントマシンの音量バーでのみ制御できます。

サイマルキャスト

サイマルキャストのサポートは、Windows および Mac での最適化された Microsoft Teams ビデオ会議通話に対して有効になっています。Linux の場合は、シンクライアントのベンダーに確認してください。
サイマルキャストでは、すべての発信者に最適な通話エクスペリエンスを提供できる適切な解像度に適応しているため、さまざまなエンドポイントでのビデオ会議通話の品質とエクスペリエンスが向上します。

この向上したエクスペリエンスにより、各ユーザーは、エンドポイントの機能、ネットワークの状態などのいくつかの要因に応じて、複数のビデオ ストリームを異なる解像度（720p、360p など）で配信できます。次に、受信側のエンドポイントは、可能な範囲で最高品質の解像度を要求します。これにより、すべてのユーザーに最適なビデオ体験を提供できます。

> 注:
>
> この機能は、Microsoft Teams からの更新のロールアウト後にのみ使用できます。ETA については、https://www.microsoft.com/にアクセスし、Microsoft 365 ロードマップを検索してください。Microsoft によって更新プログラムがロールアウトされたら、ドキュメントのアップデートおよび発表内容について、CTX253754を確認することができます。

Microsoft の制限

- 3x3 ギャラリービューはサポートされていません。Microsoft Teams の依存関係 - 3x3 グリッドの実装予定については、Microsoft にお問い合わせください。
- Skype for Business との相互運用性は音声通話に限定され、ビデオのモダリティはありません。
- 受信および発信ビデオストリームの最大解像度は 720p です。Microsoft Teams の依存関係 - 1080p の実装予定については、Microsoft にお問い合わせください。
- PSTN 通話の呼び出し音はサポートされていません。
- ダイレクトルーティングのメディアバイパスはサポートされていません。
- ブロードキャストおよびライブイベントのプロデューサーの役割とプレゼンターの役割はサポートされていません。参加者の役割はサポートされていますが、最適化されていません（代わりに VDA でレンダリングされます）。
- Microsoft Teams のズームインおよびズームアウト機能はサポートされていません。
- 場所ベースのルーティング（LBR）およびメディアバイパスはサポートされていません。
- 通話の結合はサポートされていません（このオプションはユーザーインターフェイスに表示されません）。

Citrix と Microsoft の制限

- 画面共有を行うと ［システムオーディオを含める］オプションを使用できません。
- サイマルキャストは ChromeOS ではサポートされていません。

EOL 予定の Microsoft Teams シングルウィンドウ

2024 年 1 月 31 日、Microsoft は VDI で Microsoft Teams 最適化を使用した場合のシングルウィンドウ UI に対するサポートを終了し、マルチウィンドウ エクスペリエンスのみをサポートします。Microsoft は、この機能廃止について M365 管理センターで 2023 年 9 月 8 日（投稿 ID：MC674419）に発表しました。
マルチウィンドウ機能について公開された詳細情報については、Tech Community の記事「New Meeting and Calling Experience in Microsoft Teams」を参照してください。

引き続きビデオと画面共有が最適化されたモードで Microsoft Teams を使用するには、VDA および Citrix Workspace アプリをサポートされているバージョンにアップグレードする必要があります。マルチウィンドウをサポートするためにインフラストラクチャとエンドポイントをアップグレードしない場合は、音声通話のみを確立できます。最適化されたビデオおよび画面共有機能は使用できなくなります。

次の表は、Citrix VDI 上の Microsoft Teams で最適化された通話を引き続き使用するために必要な VDA および Citrix Workspace アプリの最小バージョン、LTSR バージョン、および推奨バージョンを示しています：

コンポーネント	最小バージョン	LTSR でサポートされているバージョン	推奨バージョン
Microsoft Teams	1.5.00.11865	該当なし	最新バージョン

コンポーネント	最小バージョン	LTSR でサポートされているバージョン	推奨バージョン
VDA	1912 CU6 LTSR、2203 LTSR、2112 CR	1912 CU7 以降、2203 CU2 以降	2308 CR 以降
Windows 向け Citrix Workspace アプリ	2205 CR	2203 CU2 以降	2309 CR 以降
Mac 向け Citrix Workspace アプリ	2209 CR	該当なし	2308 CR 以降
Linux 向け Citrix Workspace アプリ	2209 CR	該当なし	2308 CR 以降
ChromeOS または HTML5 向け Citrix Workspace アプリ	2303 CR	該当なし	2309 CR 以降

WebRTC による **SDP** 形式（**Plan B**）の廃止に関する情報

Citrix は、将来のリリースで WebRTC による現在の SDP 形式（Plan B）のサポートを廃止する予定です。最適化された Microsoft Teams 機能をサポートするには、WebRTC で Unified Plan を使用する必要があります。

影響を受ける製品

Citrix Workspace アプリケーションの今後のリリースのいずれかでは、Citrix Workspace アプリの次期リリースのエンドポイントと Citrix Workspace アプリ 2108 以前のバージョンのエンドポイント間の通話はサポートされなくなります。互換性がなくなる通話には、1912 LTSR Citrix Workspace アプリ クライアント (CWA) が含まれます。次の Citrix Workspace アプリクライアントが影響を受けます：

- Windows 向け Citrix Workspace アプリ
- Linux 向け Citrix Workspace アプリ
- Mac 向け Citrix Workspace アプリ
- Chrome 向け Citrix Workspace アプリ

Plan B を置き換える

2109 よりも古いバージョンの Citrix Workspace アプリを実行している場合は、サポートされているバージョン（可能であれば最新の CR リリース）にアップグレードする必要があります。そうしないと、将来のリリースまたは新しいエンドポイントで通話が接続できません。連携パートナーが Citrix Workspace をアップグレードしていない場合、将来のリリースと連携通信パートナー間の通話も失敗する可能性があります。

Citrix Workspace アプリバージョン 2108 のサポート期限は 2023 年 3 月に終了しているため、新しいバージョンにアップグレードする必要があります。詳しくは、Workspace アプリで Citrix Workspace アプリのバージョンサポートの詳細を参照してください。

Plan B の廃止について詳しくは、WebRTCのドキュメントを参照してください。

追加情報

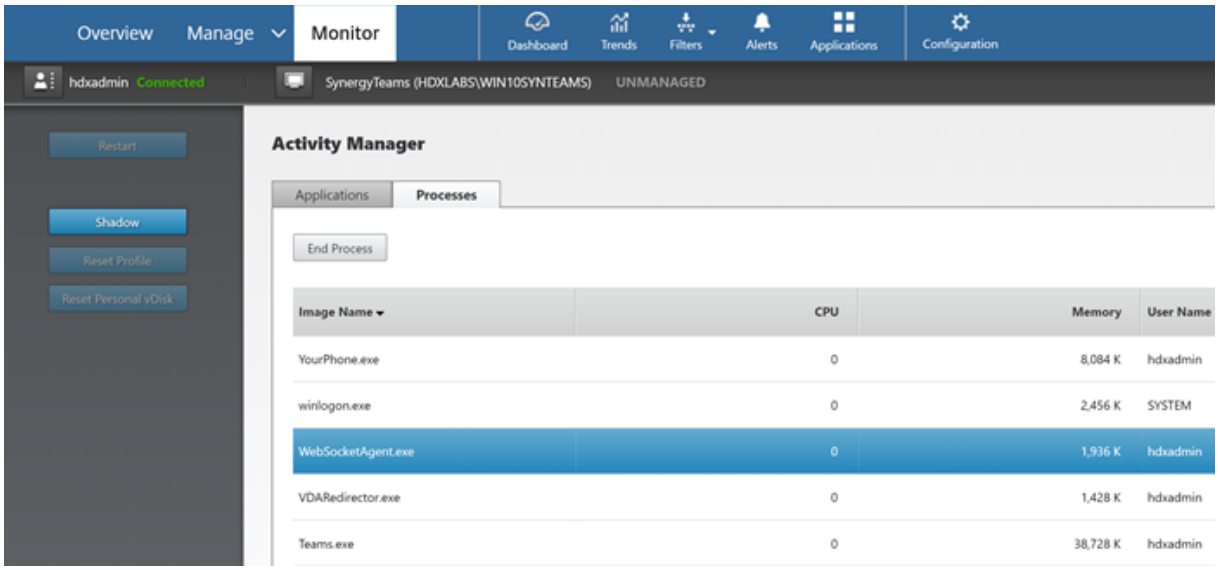
- Microsoft Teams の監視、トラブルシューティング、およびサポート
- Microsoft Teams デスクトップアプリの仮想マシンへの展開
- MSI を使用した Microsoft Teams のインストール（VDI インストールセクション）
- シンクライアント
- Skype for Business ネットワーク評価ツール
- Microsoft Teams と Skype for Business の共存と相互運用性の理解

Microsoft Teams の監視、トラブルシューティング、およびサポート

April 18, 2024

Teams の監視

このセクションでは、HDX による Microsoft Teams の最適化を監視するためのガイドラインを提供します。最適化モードで実行していて、`HdxRtcEngine.exe`がクライアントマシンで実行されている場合、`WebSocketAgent.exe`と呼ばれる VDA のプロセスがセッションで実行されています。Director で ［アクティビティマネージャー］を使用してアプリケーションを表示します。



VDA バージョン 1912 以降では、Citrix HDX Monitor（最小バージョン 3.11）を使用してアクティブな Teams 通話を監視できます。Citrix Virtual Apps and Desktops 製品の ISO には、フォルダー`layout\image-full\Support\HDX Monitor`に最新の`hdxmonitor.msi`が含まれます。

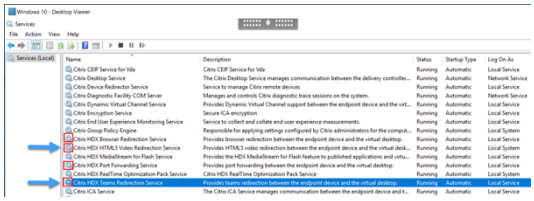
詳しくは、Knowledge Center のCTX253754の「*Monitoring*」を参照してください。

トラブルシューティング

このセクションでは、Microsoft Teams の最適化を実施する際に想定される問題に対処するためのヒントを提供します。詳しくは、CTX253754を参照してください。

Virtual Delivery Agent の状態

BCR_x64.msi. により 4 つのサービスがインストールされています。そのうちの 2 つが、VDA での Microsoft Teams のリダイレクトを担当します。

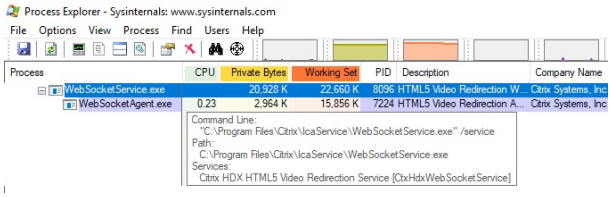


- **Citrix HDX Teams** リダイレクトサービスは Microsoft Teams が使用する仮想チャネルを確立します。このサービスは CtxSvcHost.exe に依存します。
- **Citrix HDX HTML 5** ビデオリダイレクトサービスは WebSocketService.exe として実行され、127.0.0.1 の TCP ポート 9002 をリッスンします。WebSocketService.exe には主に 2 つの機能があります。

  i. Microsoft Teams アプリのコンポーネントとして組み込まれている vdiCitrixPeerConnection.js から **WebSocket** のセキュリティを確保する **TLS** ターミネーションに対して、安全な WebSocket 接続が渡されます。この接続はプロセスモニターで追跡可能です。証明書について詳しくは、「Controller と VDA の間の通信」の「TLS および HTML5 ビデオリダイレクション、およびブラウザーコンテンツリダイレクト」を参照してください。

  一部のウイルス対策ソフトウェアおよびデスクトップセキュリティソフトウェアは、`WebSocketService.exe`およびその証明書の適切な動作を妨げます。Citrix HDX HTML5 ビデオリダイレクトサービスは、`services.msc`コンソールで動作している可能性がありますが、localhost `127.0.0.1:9002` TCP ソケットが netstat で表示されるようにリスニングモードになることはありません。サービスを再起動しようとすると、サービスがハングします（「停止しています…」）。`WebSocketService.exe`プロセスで適切な除外を適用するようにしてください。

ii. ユーザーセッションのマッピング。Microsoft Teams アプリケーションが起動すると、WebSocketService.exe は VDA のユーザーセッションで WebSocketAgent.exe プロセスを起動します。WebSocketService.exe は LocalSystem アカウントの動作として、セッション 0 で実行されます。



netstat を使用して、WebSocketService.exe サービスが VDA でアクティブなリッスン状態であるかどうかを確認できます。

管理者特権でのコマンドプロンプトウィンドウから`netstat -anob -p tcp`を実行します:

```
 TCP    127.0.0.1:9001         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
 TCP    127.0.0.1:9002         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
```

接続が成功すると、状態が ESTABLISHED に変わります:

```
 TCP    127.0.0.1:9002         127.0.0.1:58069        ESTABLISHED     8096
[WebSocketService.exe]
 TCP    127.0.0.1:58069        127.0.0.1:9002         ESTABLISHED     748
[Teams.exe]
```

> 重要:
>
> WebSocketService.exe は 127.0.0.1:9001 と 127.0.0.1:9002 の 2 つの TCP ソケットでリッスンします。ポート 9001 はブラウザーコンテンツのリダイレクトと HTML5 ビデオのリダイレクトに、ポート 9002 は Microsoft Teams のリダイレクトにそれぞれ使用されます。VDA の Windows OS に、Teams.exe と WebSocketService.exe の間の直接通信を妨げる可能性があるプロキシ構成がないことを確認してください。Internet Explorer 11（[インターネットオプション] > [接続] > [**LAN** の設定] > [プロキシサーバー]）で明示的なプロキシを構成すると、接続は割り当てられたプロキシサーバーを経由する場合があります。手動および明示的なプロキシ設定を使用する場合、[ローカルアドレスにはプロキシサーバーを使用しない] がオンになっていることを確認します。

サービスの場所と説明

サービス	Windows Server OS の実行可能ファイルへのパス	ログオン名	説明
Citrix HTML5 ビデオリダイレクトサービス	“C:\Program Files (x86)\Citrix\System32\WebSocketService.exe” /service	ローカルシステムアカウント	仮想デスクトップとエンドポイントデバイス間でメディアのリダイレクトを実行する場合に必要な、複数の HDX マルチメディアサービスの初期のフレームワークを提供します。
Citrix HDX ブラウザーリダイレクトサービス	“C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe” -g BrowserRedirSvcs	使用アカウント（ローカル	エンドポイントデバイスと仮想デスクトップ間で Web ブラウザーコンテンツのリダイレクトを実行します。
Citrix ポート フォワーディングサービス	“C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe” -g PortFwdSvcs	使用アカウント（ローカル	エンドポイントデバイスと仮想デスクトップ間で Web ブラウザーコンテンツのリダイレクトのポートフォワーディングを実行します。
Citrix HDX Teams リダイレクトサービス	“C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe” -g TeamsSvcs	ローカルシステムアカウント	エンドポイントデバイスと仮想デスクトップ間で Microsoft Teams のリダイレクトを実行します。

Citrix Workspace アプリ

Windows 向け Citrix Workspace アプリは、ユーザーのエンドポイント上で HdxTeams.exe という名前の新しいサービスをインスタンス化します。これは、Microsoft Teams が VDA で起動し、ユーザーがセルフプレビューで周辺機器の呼び出しやアクセスを試みたときに行われます。このサービスが表示されない場合は、次の点を確認してください：

1. Windows 向け Workspace アプリのバージョン 1905 以上がインストールされていることを確認します。Workspace アプリのインストールパスに HdxTeams.exe と webrpc.dll バイナリがあるかを確認します
2. 手順 1 の確認ができたら、次の手順を実行して HdxTeams.exe が起動するかを確認してください。
   a) VDA で Microsoft Teams を終了します。
   b) VDA で services.msc を起動します。
   c) Citrix HDX Teams リダイレクトサービスを停止します。
   d) ICA セッションを切断します。

e) ICA セッションを接続します。
f) Citrix HDX チームリダイレクトサービスを起動します。
g) Citrix HDX HTML5 ビデオリダイレクトサービスを再起動します。
h) VDA で Microsoft Teams を起動します。

3. これでもクライアントエンドポイントで HdxTeams.exe が起動しない場合は、次の手順を実行してください:

a) VDA を再起動します。
b) クライアントエンドポイントを再起動します。

サポート

Citrix と Microsoft は Citrix Virtual Apps and Desktops での Microsoft Teams の提供について、Microsoft Teams の最適化を通じて共同でサポートしています。この共同サポートは両社の緊密な協力関係により実現したものです。サポート契約の有効期間にこのソリューションで問題が発生した場合は、原因と考えられるコードの担当ベンダーのサポートチケットを開いてください。つまり Teams の場合は Microsoft の、最適化コンポーネントの場合は Citrix のサポートチケットを開きます。

Citrix または Microsoft はチケットを受け取り、問題を優先順位付けし、必要に応じてエスカレーションします。管理者が各社のサポートチームに連絡する必要はありません。

問題がある場合は、Teams UI の ［**Help**］**>** ［**Report a Problem**］にアクセスすることをお勧めします。VDA 側のログは Citrix と Microsoft の間で自動的に共有されるため、技術的な問題をより迅速に解決できます。

ログの収集

HDX メディアエンジンのログは、VDA ではなくユーザーのマシンにあります。問題が発生した場合は、必ずサポートケースにログを添付してください。

Windows ログ:

Windows ログは、%TEMP%**HDXTeams** フォルダー（AppData/Local/Temp/HDXTeams または AppData/Local/Temp/HdxRtcEngine）内にあります。「webrpc_Day_Month_timestamp_Year.txt」という名称の.txt ファイルを探します。Citrix Workspace アプリ 2009.5 以降など、新しいバージョンの Citrix Workspace アプリを使用している場合は、ログを AppData\Local\Temp\HdxRtcEngine に保存します。

各セッションは、ログ用に個別のフォルダーを作成します。

Mac ログ:

1. VDWEBRTC ログ - 仮想チャネルの実行を記録します。

   場所: /Users/<User Name>/Library/Logs/Citrix Workspace/CitrixViewer_<Y_M_D_H_M_S>.txt

2. HdxRtcEngine ログ - HdxRtcEngine でのプロセスの実行を記録します。

   場所: $TMPDIR/hdxrtcengine/<W_M_D_H_M_S_Y>/hdxrtcengine.log

   HdxRtcEngine ログは、デフォルトで有効になっています。

3. WebRTC ログ - WebRTC ライブラリのラップアップの実行を記録する最も重要なログです。

   場 所: /Users/<USERNAME>/Library/Logs/HdxRtcEngine/<W_M_D_H_M_S_Y>/webrpc.log

Linux ログ:

Linux ログは、/tmp/webrpc/<current date>/ and /tmp/hdxrtcengine/<current date>/フォルダーにあります。
WebRTC ログ: /tmp/webrpc/<current date>/webrtc.log
カーネルログ: /var/log/syslog

ICE/STUN/TURN/ログ:

通話を確立する場合、次の 4 つの ICE フェーズが必要です:

- 候補の収集
- 候補の交換
- 接続性チェック（STUN バインド要求）
- 候補のプロモーション

HdxRtcEngine.exe のログでは、以下のエントリが関連の対話型接続確立（ICE）エントリです。通知のセットアップを成功させるには、次のエントリが必要です。収集のフェーズについては、次のサンプルスニペットを参照してください:

```
RPCStubs Info: -> device id = \?\display#int3470#4&1835d135&0&uid13424
    #{
 65e8773d-8f56-11d0-a3b9-00a0c9223196 }
 {
 bf89b5a5-61f7-4127-a279-e187013d7caf }
  label = Microsoft Camera Front groupId =

webrtcapi.RTCPeerConnection Info: createOffer. audio = 1 video = 1
webrtcapi.RTCPeerConnection Info: setLocalDescription.
>>> begin:sdp
[…]

webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
    HaveLocalOffer

webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state =
    Gathering

[…]
>>> begin:sdp
```



```
candidate:840548147 1 udp 2122194687 10.108.124.215 56927 typ host
    generation 0 ufrag oVk6 network-id 1
<<< end:sdp
[…]
>>> begin:sdp
candidate:1938109490 1 udp 24911871 52.114.xxx.xxx 52786 typ relay
    raddr 73.205.xxx.x rport 25651 generation 0 ufrag dDML network-id 1
    network-cost 10
<<< end:sdp
[…]
>>> begin:sdp
candidate:4271145120 1 udp 1685987071 66.xxx.xxx.xxx 55839 typ srflx
    raddr 10.108.124.215 rport 55839 generation 0 ufrag uAVH network-id
    1
<<< end:sdp
[…]

webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state =
    Complete webrtcapi.RTCPeerConnection Info: setRemoteDescription.
>>> begin:sdp
[…]

webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
    HaveRemotelOffer

<!--NeedCopy-->
```

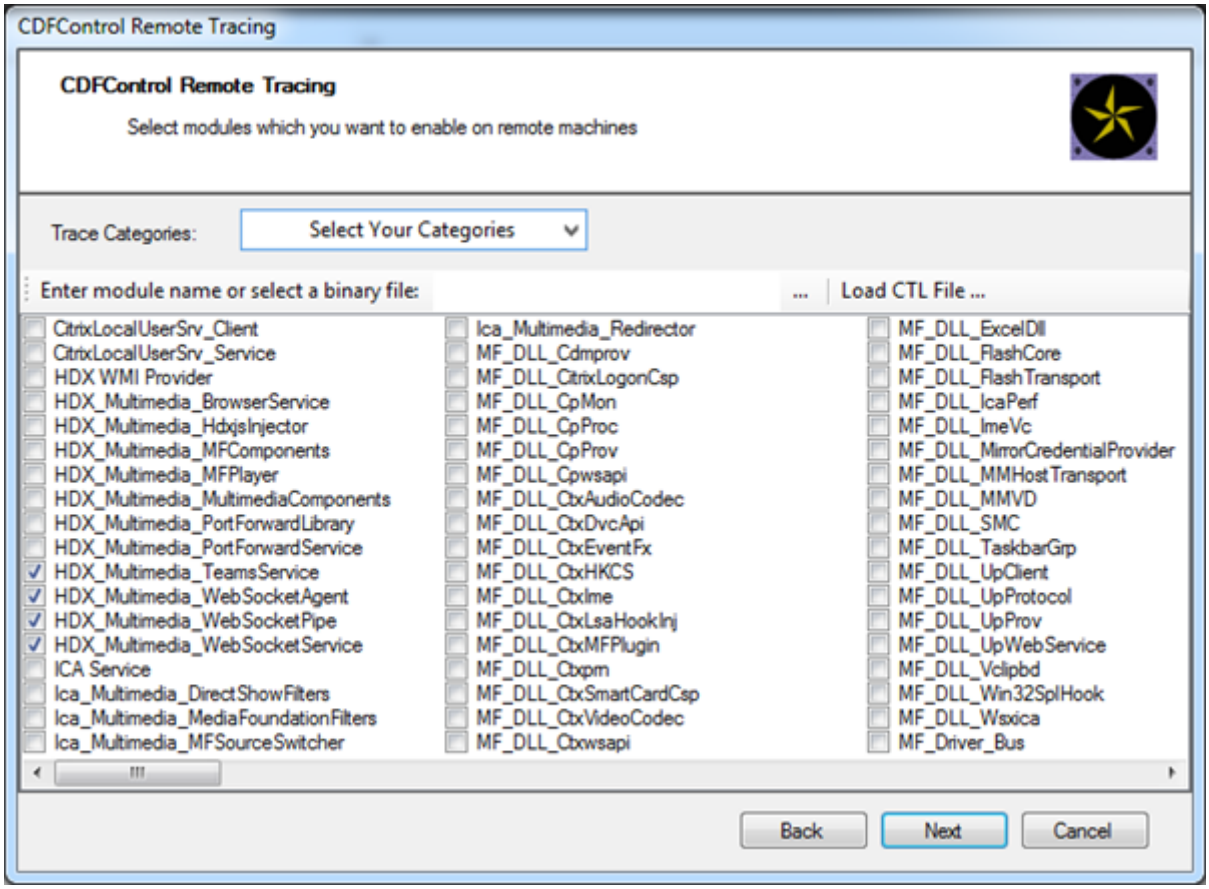
複数の ICE 候補がある場合、優先順位は次のとおりです:

1. host
2. peer reflexive
3. server reflexive
4. transport relay

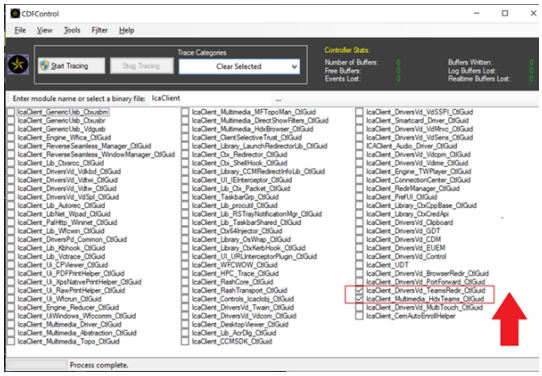
問題が発生し、一貫して再現できる場合は、Teams で［**Help**］**>**［**Report a problem**］にアクセスすることをお勧めします。Microsoft でケースを開いた場合の技術的な問題を解決するために、Citrix と Microsoft の間でログが共有されます。
Citrix サポートに連絡する前に CDF トレースをキャプチャすることもお勧めします。詳しくは、Knowledge Center の「CDFcontrol」を参照してください。

CDF トレースを収集する際の推奨事項については、Knowledge Center の「Recommendations for Collecting the CDF Traces」を参照してください。

VDA 側の **CDF** トレース **-** 次の **CDF** トレースプロバイダーを有効にします:



Workspace アプリ側の **CDF** トレース **-** 次の **CDF** トレースプロバイダーを有効にします:



- IcaClient_DriversVd_TeamsRedir（オプション）
- IcaClient_Multimedia_HdxTeams （Citrix Workspace アプリ 2012 以降が必要です）

Windows Media リダイレクト

March 30, 2022

Windows Media リダイレクトは、サーバーでのユーザーへのオーディオとビデオのストリーム配信方法を制御および最適化します。サーバーではなくクライアントデバイスでメディアランタイムファイルを再生することで、Windows Media リダイレクトはマルチメディアファイルの再生に必要な帯域幅を減少させます。Windows Media リダイレクトは、仮想 Windows デスクトップで実行中の Windows Media Player および互換プレーヤーのパフォーマンスを向上させます。

Windows メディアのクライアント側でのコンテンツ取得の要件が満たされない場合、メディア配信は自動的にサーバー側での取得を使用します。その方法はユーザーにとって透過的です。Citrix Scout を使用して、HostMMTransport.dll から Citrix Diagnosis Facility（CDF）トレースを実行すると、その使用方法を決定できます。詳しくは、「Citrix Scout」を参照してください。

Windows Media リダイレクトは、ホストサーバーでのメディアパイプラインをインターセプトし、ネイティブの圧縮フォーマットでメディアデータをキャプチャし、コンテンツをクライアントデバイスにリダイレクトします。クライアントデバイスはパイプラインを再作成し、ホストサーバーから受信したメディアデータの展開およびレンダリングを行います。Windows Media リダイレクトは Windows オペレーティングシステムを実行中のクライアントデバイスで正しく動作します。これらのデバイスは、ホストサーバーに存在したパイプラインを再構築するために必要なマルチメディアフレームワークを備えています。Linux クライアントは、メディアパイプラインを再構築するために、同様のオープンソースメディアフレームワークを使用します。

[**Windows Media** リダイレクト］ポリシー設定で、この機能を制御します。デフォルトは ［許可］です。この設定は、通常、セッション内で再生されるオーディオおよびビデオの品質が向上して、クライアントデバイス上のファイルを再生しているときの品質に近くなります。まれに、Windows Media リダイレクトによるメディアの再生品質が、基本的な ICA 圧縮および通常のオーディオ機能での品質よりも悪い場合があります。その場合は、［**Windows Media** リダイレクト］設定をポリシーに追加し、その値を ［禁止］にすることで、機能を無効にできます。

ポリシーの設定について詳しくは、「マルチメディアのポリシー設定」を参照してください。

制限事項:

セッション内でリモート音声およびビデオ拡張機能（RAVE）を有効にして Windows Media Player を使用しているときに、画面表示が黒くなることがあります。この黒い画面は、ビデオコンテンツを右クリックし、［プレイビューを常に手前に表示］を選択すると表示されることがあります。

一般コンテンツリダイレクト

April 22, 2022

コンテンツのリダイレクト機能では、ユーザーが特定の種類のコンテンツにアクセスするときに、公開アプリケーションを使うのか、ユーザーデバイス上のアプリケーションを使うのかを制御できます。

クライアントフォルダーのリダイレクト

クライアントフォルダーのリダイレクトは、クライアント側のファイルがホスト側のセッションのへアクセスする方法を変更します。

- サーバー上でクライアント側ドライブのマッピングのみを有効にすると、クライアントの側の全ボリュームが UNC（Universal Naming Convention）リンクとしてセッションに自動的にマップされます。
- 管理者がサーバー上でクライアントフォルダーのリダイレクトを有効にして、ユーザーがそれを Windows デスクトップデバイス上で構成すると、ユーザーが指定したローカルボリュームの一部がリダイレクトされます。

ホストからクライアントへのリダイレクト

一般的ではないユースケースでの、ホストからクライアントへのリダイレクト機能の使用を検討します。通常は、ほかのコンテンツリダイレクト機能を使用することをお勧めします。この種類のリダイレクト機能は、マルチセッション OS VDA でのみサポートされ、シングルセッション OS VDA ではサポートされません。

ローカルアプリアクセスと URL リダイレクト

ローカルアプリアクセスを有効にすると、ローカルにインストールされている Windows アプリケーションが仮想デスクトップ環境にシームレスに統合されます。コンピューター間で切り替えるはありません。

HDX テクノロジは、特殊デバイスに次のような最適化されたサポートがないとき、または不適切なときに汎用 **USB** リダイレクトを提供します。

クライアントフォルダーのリダイレクト

March 30, 2022

クライアントフォルダーのリダイレクトは、クライアント側のファイルがホスト側のセッションのへアクセスする方法を変更します。サーバー上でクライアント側ドライブのマッピングのみを有効にすると、クライアントの側の全ボリュームが UNC（Universal Naming Convention）リンクとしてセッションに自動的にマップされます。管理者がサーバー上でクライアントフォルダーのリダイレクトを有効にして、ユーザーがそれをユーザーデバイス上で構成すると、ユーザーが指定したローカルボリュームの一部がリダイレクトされます。

セッション内でユーザー指定のフォルダーのみが UNC リンクとして表示されます。つまり、ユーザーデバイス上のファイルシステム全体が表示されるわけではありません。レジストリで UNC リンクを無効にすると、クライアントフォルダーはマップされたドライブとしてセッション内で表示されます。

クライアントフォルダーのリダイレクトは Windows シングルセッションOS マシンでのみサポートされます。

外部 USB ドライブに対するクライアントフォルダーのリダイレクトは、デバイスを解除して再接続しても保存されません。

サーバー側でクライアントフォルダーのリダイレクトを有効にします。次に、クライアントデバイス上でリダイレクト対象フォルダーを指定します。クライアントフォルダーオプションの指定に使用するアプリケーションは、このリリースで提供される Citrix Workspace アプリに含まれています。

要件:

サーバーの場合:

- Windows Server 2019、Standard、および Datacenter エディション。
- Windows Server 2016、Standard、および Datacenter エディション。
- Windows Server 2012 R2、Standard、および Datacenter エディション。

クライアントの場合:

- Windows 10 32 ビット版および 64 ビット版（バージョン 1607 以降）
- Windows 8.1 32 ビット版および 64 ビット版（Embedded エディションを含む）
- Windows 7 32 ビット版および 64 ビット版（Embedded エディションを含む）

サーバーでクライアントフォルダーのリダイレクトを有効にするには、レジストリを介して管理される機能の一覧にある「クライアントフォルダーのリダイレクト」を参照してください。

ユーザーデバイスで、リダイレクトするフォルダーを指定します:

1. 最新バージョンの Citrix Workspace アプリがインストールされていることを確認します。
2. Citrix Workspace アプリのインストール先ディレクトリで、CtxCFRUI.exe を実行します。
3. [カスタム] ラジオボタンをクリックし、フォルダーを追加、編集、または削除します。
4. セッションを切断してから再接続すると、変更が適用されます。

コンテンツの双方向リダイレクトの構成

February 9, 2024

コンテンツの双方向リダイレクトを使用すると、構成に応じてクライアントからサーバーへ、およびサーバーからクライアントへリダイレクトするように URL を構成できます。このポリシー設定は、廃止された次の 3 つの設定を置き換えます:

- コンテンツの双方向リダイレクトを許可する
- VDA へのリダイレクトを許可する URL
- クライアントへのリダイレクトを許可する URL

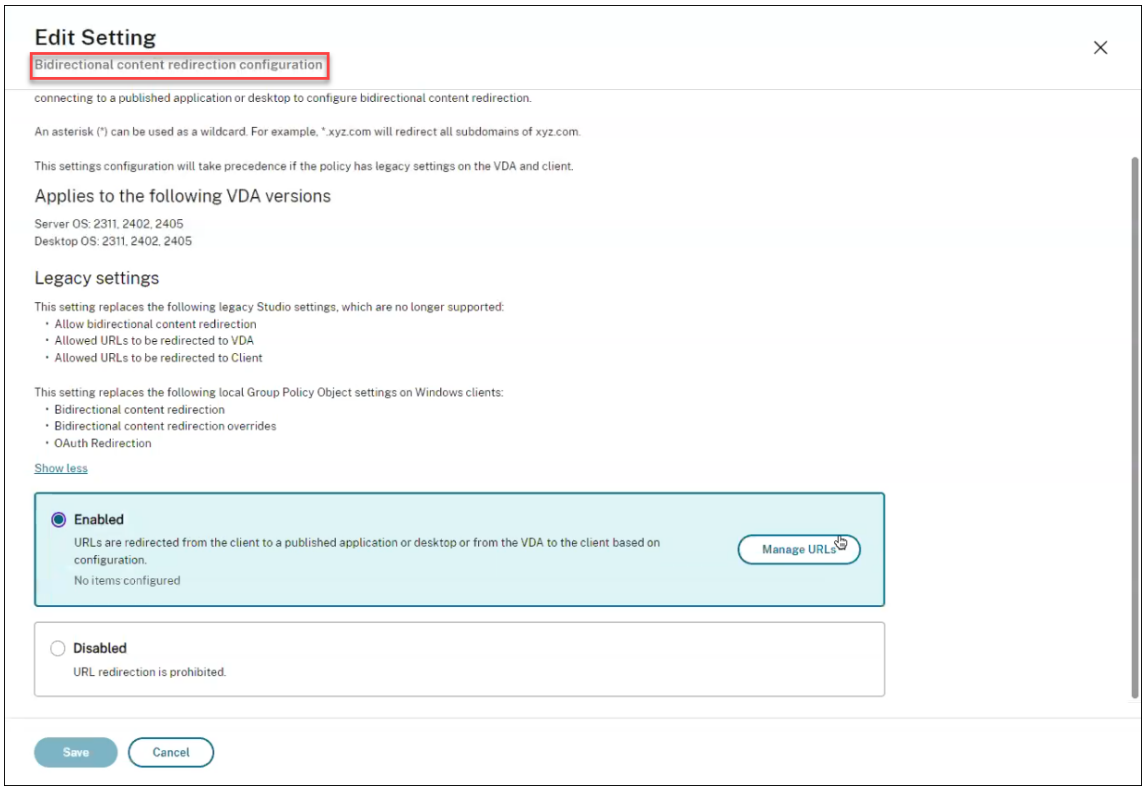
また、Windows クライアント上の次の 3 つのローカル GPO 設定も置き換えられます:

- コンテンツの双方向リダイレクト
- コンテンツの双方向リダイレクトでの上書き
- OAuth リダイレクト

この設定が構成されている場合、Studio およびクライアントの従来の設定よりも優先されます。コンテンツの双方向リダイレクトポリシーを構成するには、次の手順を実行します:

1. Citrix DaaS の構成ページで、[管理] タブをクリックします。
2. [ポリシー] タブをクリックします。

3. ［ポリシーの作成］をクリックします。［ポリシーの作成］ブレードが開きます。
4. ［検索］フィールドで`Bidirectional content redirection configuration`を検索し、チェックボックスをオンにして ［編集］をクリックします。
5. ［設定の変更］ブレードで、このポリシーを ［有効］に設定し、［**URL** を管理する］をクリックします。



6. ［**URL** を管理する］ブレードの ［**VDA** からクライアントへのリダイレクト］で、以下を指定します:

   - **URL**（必須）: クライアントで開くために VDA からリダイレクトする URL を追加します。OAuth リダイレクトの場合、セッションをホストにリダイレクトするようにクライアントで認証スキームとパターンを設定します。
   - パターン（オプション）: ホストからクライアントへの URL リダイレクトを介してクライアントにリダイレクトされると OAuth 認証フローが開始されたかのように追跡され、フローが完了すると（結果のスキームまたは開かれたリダイレクト URL パターンによって検出）、結果の URL がフローを開始したホスト VDA にリダイレクトされる URL 正規表現です。
   - スキーム（オプション）: スキームが指定されている場合、終了 URL は「`scheme://<something>`」の形式である必要があります。スキームが指定されていない場合（空の場合）、元の結果の URL パターンが正規表現キャプチャグループを介してパターンから抽出されます（パターンで指定されている必要があります）。元の URL は`citrix-oauth-redir://`リダイレクト URL を使用するように書き換えられます。フローが完了すると、元のリダイレクト URL がホスト（VDA）に再度リダイレクトされます。この場合、OAuth 認証サーバーは`citrix-oauth-redir://byIndex/1 (2, 3, ... N)`リダイレクト URL を許可するように設定する必要があります。

> 注:
>
> パターンとスキームはどちらもオプションですが、パターンが指定されている場合は、スキームも指定する必要があります。

7. ［**URL** を管理する］ブレードの ［クライアントから **VDA** へのリダイレクト］で、以下を指定します:
   - 種類: デスクトップまたはアプリケーションを選択します。
   - 名前: 種類に名前を付けます。
   - **URL**: ソースにリダイレクトする URL を指定します。複数の URL を追加し、不要な URL を削除できます。
8. ［保存］をクリックします。［設定の変更］ブレードには、構成されている項目の数が表示されます。
9. ［保存］をクリックします。［ポリシーの作成］ブレードには、構成されている現在の値が表示されます。［次へ］をクリックします。
10. ［ポリシーの割り当て先］の手順で、［次へ］をクリックします。
11. ［概要］の手順で、［ポリシーの有効化］チェックボックスを選択し、［ポリシー名］フィールドに名前を入力します。
12. ［完了］をクリックします。新しいポリシーが表示されます。
13. 作成された新しいポリシーを選択して、構成された設定を確認します。

従来の設定については、「ホストからクライアントへのリダイレクト」および「コンテンツの双方向リダイレクト」を参照してください。

ホストからクライアントへのリダイレクト

February 9, 2024

> 注:
>
> この記事では、従来のホストからクライアントへのリダイレクト設定について説明します。最新の設定については、「コンテンツの双方向リダイレクトの構成」を参照してください。新しいポリシー設定は従来の設定より優先されます。予期しない動作を避けるために、新しいポリシー設定のみを使用し、従来の設定は削除することをお勧めします。

ホストからクライアントへのリダイレクトにより、Citrix セッションで実行中のアプリケーションにハイパーリンクとして埋め込まれている URL を、ユーザーエンドポイントデバイスにある対応するアプリケーションを使用して開くことができます。ホストからクライアントへのリダイレクトの一般的なユースケースは次のとおりです:

- Citrix サーバーにソースへのインターネットまたはネットワークアクセスがない場合の Web サイトのリダイレクト。
- Citrix セッション内で Web ブラウザーを実行している場合の Web サイトのリダイレクトは、セキュリティ、パフォーマンス、互換性、またはスケーラビリティの観点から望ましくありません。
- URL を開くために必要なアプリケーションが Citrix サーバーにインストールされていない場合の特定の URL タイプのリダイレクト。

ホストからクライアントへのリダイレクトは、Web ページでアクセスする URL、または Citrix セッションで実行されている Web ブラウザーのアドレスバーに入力する URL を対象としていません。Web ブラウザーでの URL のリダイレクトについては、「双方向の URL のリダイレクト」または「Web ブラウザーコンテンツのリダイレクト」を参照してください。

システム要件

- マルチセッション OS VDA
- サポートされているクライアント:
  - Windows 向け Citrix Workspace アプリ
  - Mac 向け Citrix Workspace アプリ
  - Linux 向け Citrix Workspace アプリ
  - HTML5 向け Citrix Workspace アプリ
  - Chrome 向け Citrix Workspace アプリ

クライアントデバイスには、URL タイプのリダイレクトを処理するためのアプリケーションがインストールおよび構成されている必要があります。

構成

「ホストからクライアントへのリダイレクト」の Citrix ポリシーを使用して、この機能を有効にします。ホストからクライアントへのリダイレクトはデフォルトで無効になっています。ホストからクライアントへのリダイレクトポリシーを有効にすると、Citrix Launcher アプリケーションが Windows サーバーに登録され、URL をインターセプトしてクライアントデバイスに送信できるようになります。

次に、必要な URL タイプのデフォルトアプリケーションとして Citrix Launcher を使用するように、Windows グループポリシーを構成する必要があります。Citrix サーバー VDA で、ServerFTAdefaultPolicy.xml ファイルを作成し、次の XML コードを挿入します。

```
<?xml version="1.0" encoding="UTF-8"?>

<DefaultAssociations>

<Association Identifier="http" ProgId="ServerFTAHTML" ApplicationName="
    ServerFTA" />
```



```
6
7  <Association Identifier="https" ProgId="ServerFTAHTML" ApplicationName=
       "ServerFTA" />
8
9  </DefaultAssociations>
10 <!--NeedCopy-->
```

グループポリシー管理コンソールから、[コンピューターの構成] **>** [管理用テンプレート] **>** [**Windows** コンポーネント] **>** [エクスプローラー] **>** [既定の関連付け構成ファイルの設定] の順に移動し、ServerFTAdefaultPolicy.xml ファイルを保存します。

> 注:
>
> Citrix サーバーにグループポリシー設定がない場合、URL を開くためのアプリケーションを選択するよう求める Windows プロンプトが表示されます。

デフォルトでは、次の URL タイプのリダイレクトをサポートしています:

- HTTP
- HTTPS
- RTSP
- RTSPU
- PNM
- MMS

リダイレクト用の一覧に追加の標準 URL タイプまたはカスタム URL タイプを含めるには、前に参照した ServerFTAdefaultPolicy.xml ファイルに新しい **Association Identifier**（関連付け識別子）行を作成します。例:

```
<Association Identifier="ftp"ProgId="ServerFTAHTML"ApplicationName="
ServerFTA"/>

<Association Identifier="mailto"ProgId="ServerFTAHTML"ApplicationName
="ServerFTA"/>

<Association Identifier="customtype1"ProgId="ServerFTAHTML"ApplicationName
="ServerFTA"/>

<Association Identifier="customtype2"ProgId="ServerFTAHTML"ApplicationName
="ServerFTA"/>
```

一覧に URL タイプを追加するには、クライアントの構成も必要です。Windows クライアントで次のレジストリキーと値を作成します。

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

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

- キー：HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA
- 値の名前：ExtraURLProtocols
- 値の種類：REG_SZ
- 値のデータ：必要な URL タイプをセミコロンで区切って指定します。URL の権限部分の前にすべてを含めます。例：
  `ftp://;mailto:;customtype1://;custometype2://`

Windows クライアントに対してのみ URL タイプを追加できます。上記のレジストリ設定がないクライアントは、Citrix セッションへ戻るリダイレクトを拒否します。クライアントには、指定された URL タイプを処理するようにアプリケーションがインストールおよび構成されている必要があります。

デフォルトのリダイレクト一覧から URL タイプを削除するには、サーバー VDA で次のレジストリキーと値を作成します。

- キー：HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- 値の名前：DisableServerFTA
- 値の種類：DWORD
- 値のデータ：1
- 値の名前：NoRedirectClasses
- 値の種類：REG_MULTI_SZ
- 値のデータ：値の組み合わせを指定します：`http`、`https`、`rtsp`、`rtspu`、`pnm`、または`mms`。1 つの行に 1 つの値を入力してください。例：

```
http
https
rtsp
```

特定の Web サイトのセットについてホストからクライアントへのリダイレクト機能を有効にするには、サーバー VDA でレジストリキーと値を作成します。

- キー：HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- 値の名前：ValidSites
- 値の種類：REG_MULTI_SZ
- 値のデータ：FQDN（完全修飾ドメイン名：Fully-Qualified Domain Name）の組み合わせを指定します。1 つの行に 1 つの FQDN を入力してください。プロトコル（`http://`または`https://`）を使用せずに、FQDN のみを含めます。FQDN には、左端にのみワイルドカード文字としてアスタリスク（*）を含めることができます。このワイルドカードは単一レベルのドメインと照合されます。これは RFC 6125 の規則に準拠しています。例：

`www.exmaple.com`

`*.example.com`

> 注:
>
> **ValidSites** キーを **DisableServerFTA** キーおよび **NoRedirectClasses** キーと組み合わせて使用することはできません。

サーバー **VDA** のデフォルトの **Web** ブラウザー構成

このセクションで参照されているようにホストからクライアントへのリダイレクトを有効にすると、サーバー VDA の以前のデフォルトの Web ブラウザー構成が置き換えられます。Web URL がリダイレクトされない場合、Citrix Launcher は URL を`command_backup`レジストリキーで構成された Web ブラウザーに渡します。キーはデフォルトで Internet Explorer を指定しますが、これを変更して別の Web ブラウザーへのパスを含めることができます。詳しくは、レジストリを介して管理される機能の一覧にある「サーバー VDA のデフォルトの Web ブラウザー構成」を参照してください。

コンテンツの双方向リダイレクト

April 18, 2024

> 注:
>
> この記事では、従来のコンテンツの双方向リダイレクト設定について説明します。最新のポリシー設定については、「コンテンツの双方向リダイレクトの構成」を参照してください。新しいポリシー設定は従来の設定より優先されます。予期しない動作を避けるために、新しいポリシー設定のみを使用し、従来の設定は削除することをお勧めします。

コンテンツの双方向リダイレクトにより、Web ブラウザーの HTTP または HTTPS の URL、あるいはアプリケーションに埋め込まれた URL を、Citrix VDA セッションとクライアントエンドポイントの間で双方向に転送できます。Citrix セッションで実行されているブラウザーに入力された URL は、クライアントのデフォルトのブラウザーを使用して開くことができます。逆に、クライアントで実行されているブラウザーに入力された URL は、公開アプリケーションまたはデスクトップのいずれかを使用して、Citrix セッションで開くことができます。コンテンツの双方向リダイレクトの一般的なユースケースは次のとおりです:

- 起動ブラウザーがソースへのネットワークアクセス権を持っていない場合の Web URL のリダイレクト。
- ブラウザーの互換性とセキュリティ上の理由からの Web URL のリダイレクト。
- Citrix セッションまたはクライアントで Web ブラウザーを実行する必要がない場合の、アプリケーションに埋め込まれた Web URL のリダイレクト。

システム要件

- シングルセッションまたはマルチセッションの OS VDA
- Windows 向け Citrix Workspace アプリ

ブラウザー:

- Citrix Browser Redirection Extension を備えた Google Chrome（Google Chrome ウェブストアで入手可能）
- Citrix Browser Redirection Extension を備えた Microsoft Edge（Chromium）（Google Chrome ウェブストアで入手可能）

構成

リダイレクトを機能させるには、VDA とクライアントの両方で Citrix ポリシーを使用して、コンテンツの双方向リダイレクトを有効にする必要があります。コンテンツの双方向リダイレクトはデフォルトで有効になっています。

VDA の構成については、「ICA ポリシー」設定の「コンテンツの双方向リダイレクト」を参照してください。

クライアントの構成については、Windows 向け Citrix Workspace アプリのドキュメントの「コンテンツの双方向リダイレクト」を参照してください。

ブラウザー拡張機能は、示されているコマンドを使用して登録する必要があります。使用中のブラウザーに基づいて、VDA およびクライアントで、必要に応じてコマンドを実行します。

ブラウザー拡張機能を VDA に登録するには、コマンドプロンプトを開きます。次に、次の例に示すように、必要なブラウザーオプションを指定して`%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe`を実行します:

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regIE
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regChrome
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regEdge
```

使用可能なすべてのブラウザーで拡張機能を登録するには、次のコマンドを実行します:

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regall
```

ブラウザー拡張機能の登録を解除するには、次の例のように`/unreg<browser>`オプションを使用します:

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /unregIE
```

クライアントにブラウザー拡張機能を登録するには、コマンドプロンプトを開き、示されている例と同じオプションを指定して`%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe`を実行します。

> 注:
>
> 登録コマンドを使用すると、Chrome および Edge ブラウザーは、最初の起動時に Citrix Browser Redirec-

> tion Extension を有効にするようにユーザーに促します。ブラウザー拡張機能は、Google Chrome ウェブストアから手動でインストールすることもできます。

Citrix VDA からクライアントへのワイルドカードリダイレクト

コンテンツの双方向リダイレクトでは、リダイレクトされる URL を定義するときにワイルドカードを使用できます。コンテンツの双方向リダイレクトを構成するには、「構成」手順を参照してください。

Citrix Studio で、［クライアントへのリダイレクトを許可する **URL**］にワイルドカード URL を設定します。アスタリスク（*）はワイルドカード文字です。

> 注:
>
> - クライアントポリシーで、［クライアントへのリダイレクトを許可する **URL**］を設定しないでください。リダイレクトの無限ループを回避するために、サイトが ［クライアントへのリダイレクトを許可する **URL**］を設定していることを確認してください。
> - 最上位ドメインはサポートされていません。たとえば、`https://www.citrix.*`または`http://www.citrix.co*`はリダイレクトされません。

VDA からクライアントへのカスタムプロトコルリダイレクト

コンテンツの双方向リダイレクトは、Citrix VDA からクライアントへのカスタムプロトコルのリダイレクトをサポートします。HTTP または HTTPS 以外のプロトコルがサポートされています。コンテンツの双方向リダイレクトを構成するには、「構成」手順を参照してください。

Citrix Studio で、［クライアントへのリダイレクトを許可する **URL**］にカスタムプロトコルを設定します。

> 注:
>
> - クライアントには、プロトコルを処理するためのアプリケーションが登録されている必要があります。登録されていない場合、URL はクライアントにリダイレクトされ、起動に失敗します。
> - Chrome および Edge ブラウザーで入力または起動するカスタムプロトコル URL はサポートされておらず、リダイレクトは機能しません。
> - 次のプロトコルはサポートされていません: `rtsp://`, `rtspu://`, `pnm://`, `mms://`。

そのほかの考慮事項

- ブラウザーの要件と構成は、リダイレクトを開始するブラウザーにのみ適用されます。リダイレクトが成功した後に URL が開く宛先ブラウザーは、サポートの対象とは見なされません。URL を VDA からクライアントにリダイレクトする場合、サポートされているブラウザー構成は VDA でのみ必要です。逆に、URL をクライアントから VDA にリダイレクトする場合、サポートされているブラウザー構成はクライアントでのみ必要です。リダイレクトされた URL は、方向に応じて、クライアントまたは VDA のいずれかの宛先マシン上で構成

されたデフォルトのブラウザーに渡されます。VDA とクライアントで同じブラウザーの種類を使用する必要はありません。

- リダイレクト規則がループした構成になっていないことを確認してください。たとえば、VDA ポリシーが`https://www.citrix.com`をリダイレクトするように設定され、クライアントポリシーが同じ URL をリダイレクトするように設定されていると、無限ループが発生します。
- HTTP/HTTPS プロトコル URL のみがサポートされています。URL の短縮はサポートされていません。
- クライアントから VDA にリダイレクトするには、Windows クライアントを管理者権限でインストールする必要があります。
- 宛先ブラウザーが既に開いている場合は、リダイレクトされた URL が新しいタブで開きます。それ以外の場合、URL は新しいブラウザーウィンドウで開きます。
- ローカルアプリアクセス（LAA）が有効になっている場合、コンテンツの双方向リダイレクトは機能しません。

ローカルアプリアクセスと **URL** リダイレクト

June 17, 2022

はじめに

ローカルアプリアクセスを有効にすると、ローカルにインストールされている Windows アプリケーションが仮想デスクトップ環境にシームレスに統合されます。ローカルアプリアクセスにより、以下の操作が可能になります。

- ラップトップや PC などの物理コンピューター上にローカルにインストールされたアプリケーションに仮想デスクトップからアクセスする。
- フレキシブルなアプリケーション配信ソリューションをユーザーに提供する。仮想化できないアプリケーションや IT 担当者が管理しないアプリケーションをユーザーのローカルにインストールして、仮想デスクトップ上にインストールされたアプリケーションのように使用できます。
- アプリケーションが仮想デスクトップから個別にホストされている場合、ダブルホップによる遅延を排除します。このために、ユーザーの Windows デバイス上で公開アプリケーションのショートカットを作成します。
- 次のようなアプリケーションを使用する。
  - GoToMeeting などのビデオ会議ソフトウェア。
  - 仮想化されていない特殊なアプリケーション。
  - ユーザーデバイスとサーバー間で大量のデータ転送が発生するアプリケーションや周辺機器。たとえば、DVD バーナーや TV チューナーなどです。

Citrix Virtual Apps and Desktops では、URL のリダイレクトにより、ホストされたデスクトップセッションからローカルアプリケーションアクセスアプリケーションを起動できます。URL リダイレクトでは、複数の URL アドレスでアプリケーションを起動できます。デスクトップセッションで、Web ブラウザー内に埋め込まれたリンクをクリ

ックすると、Web ブラウザーの URL 禁止リストに基づいてローカルの Web ブラウザーが起動します。禁止リストにない URL をクリックすると、その URL がデスクトップセッションで再度開きます。

URL リダイレクトはデスクトップセッションでのみ機能し、アプリケーションセッションでは機能しません。アプリケーションセッションで使用できるリダイレクト機能は、サーバー FTA（File Type Association：ファイルタイプの割り当て）リダイレクトの 1 つである「ホストからクライアントへのコンテンツのリダイレクト」のみです。この FTA では、HTTP、HTTPS、RTSP、MMS など、特定のプロトコルがクライアント側に転送されます。たとえば、HTTP の埋め込みリンクを開くときに、クライアント側のアプリケーションが使用されます。URL 禁止リストまたは許可リストのサポートはありません。

ローカルアプリケーションアクセスを有効にすると、ローカルで実行されるアプリケーション、ホストされるアプリケーション、またはデスクトップ上のショートカットからアクセスされた URL を、以下のいずれかの方法でリダイレクトできます。

- ユーザーのコンピューターから、ホストされているデスクトップへ
- Citrix Virtual Apps and Desktops サーバーからユーザーのコンピューターへ
- 起動された環境内で処理（リダイレクトなし）

特定の Web サイトでのリダイレクト方法を指定するには、Virtual Delivery Agent 上の URL 許可リストおよび URL 禁止リストを構成します。これらのリストでは、URL リダイレクトのポリシー設定を指定する複数行文字列値を設定します。詳しくは、「ローカルアプリアクセスのポリシー設定」を参照してください。

すべての URL を VDA 側の Web ブラウザーで開くこともできますが、以下の URL についてはエンドポイント上の Web ブラウザーで開くためのポリシーを構成できます。

- ジオ/ロケール情報—ユーザーの現在位置の情報に基づいて適切なページを自動的に表示する msn.com や news.google.com などの Web サイト。たとえば、イギリスにあるデータセンターで提供される VDA にインドのクライアントから接続する場合、in.msn.com が表示されるはずですが、代わりに、uk.msn.com が表示されます。
- マルチメディアコンテンツ—メディアリッチな Web サイト。クライアント側で処理されるように設定すると、ユーザーエクスペリエンスが向上し、狭帯域幅接続での使用帯域幅や処理能力が改善されます。この機能は、Silverlight などの他のメディアの種類のサイトをリダイレクトします。これにより、環境のセキュリティも向上します。つまり、管理者により許可された URL だけがクライアント側で処理され、ほかの URL はすべて VDA 側で処理されます。

URL リダイレクトに加えて、FTA リダイレクトも使用できます。FTA により、セッションで特定のファイルを開くときにローカルのアプリケーションが使用されます。ローカルアプリケーションでファイルを開くには、そのローカルアプリケーションがそのファイルにアクセスできる必要があります。つまり、ローカルアプリケーションで開くことができるのは、ネットワーク共有上またはクライアントドライブ上にあるファイル（クライアント側ドライブのマッピング機能）のみです。たとえば、PDF ファイルを開く場合、ローカルにインストールされている PDF リーダーでファイルが表示されます。ローカルアプリケーションはファイルに直接アクセスできるため、ファイルを開くときに ICA によるネットワーク転送は発生しません。

要件、考慮事項、および制限事項

ローカルアプリアクセスは、Windows マルチセッション OS 対応 VDA および Windows シングルセッション OS 対応 VDA でサポートされるオペレーティングシステムでサポートされています。ローカルアプリケーションアクセスには、バージョン 4.1 以降の Windows 向け Citrix Workspace アプリが必要です。次の Web ブラウザーがサポートされています:

- Edge: 最新バージョン
- Firefox: 最新バージョンおよび延長サポートリリース
- Chrome: 最新バージョン

ローカルアプリアクセスや URL リダイレクトを使用するときは、以下の考慮事項および制限事項について確認してください。

- ローカルアプリアクセスは全画面モード用に設計されています。このため、以下の制限事項があります。
  - ローカルアプリケーションアクセスをウィンドウ表示モードの仮想デスクトップで使用するなど、単一の仮想デスクトップをすべてのモニター上で表示しない場合、ユーザーエクスペリエンスに混乱が生じます。
  - マルチモニター環境で、アプリケーションの表示を 1 つのモニターで最大化すると、すべてのアプリケーションがそのモニター上に表示されます。このデフォルトの状態は、以降のアプリケーションが通常は他のモニターに表示される場合でも発生します。
  - この機能は、単一 VDA での使用を想定して設計されています。複数の同時接続 VDA を対象とするものではありません。
- 一部のアプリケーションでは、以下の予期されない問題が発生する場合があります。
  - ドライブ文字により、ユーザーが仮想デスクトップの C ドライブとローカルの C ドライブを混同する場合があります。
  - 仮想デスクトップで使用できるプリンターは、ローカルアプリケーションでは使用できません。
  - 管理者特権が必要なアプリケーションは、ローカルアプリケーションアクセスでは起動できません。
  - 単一インスタンスアプリケーション（Windows Media Player など）もほかのアプリケーションと同等に処理されます。
  - ローカルアプリケーションはローカルマシンの Windows テーマで表示されます。
  - 全画面アプリケーションはサポートされません。これらのアプリケーションには、PowerPoint のスライドショーやデスクトップ全体で表示されるフォトビューアーなど、全画面で開くアプリケーションが含まれます。
  - ローカルアプリケーションアクセスでは、VDA 上のローカルアプリケーションのプロパティ（デスクトップや［スタート］メニューのショートカットなど）が複製されます。ただし、ショートカットキーや読み取り専用属性などの他のプロパティはコピーされません。
  - 一部のアプリケーションで、各ウィンドウが正しい重なり順で表示されない場合があります。これにより、一部のウィンドウが非表示になることがあります。

  - マイコンピューター、ごみ箱、コントロールパネル、ネットワークドライブ、フォルダーなどのショートカットはサポートされません。
  - カスタムのファイルタイプ、関連付けられたプログラムのないファイル、ZIP ファイル、および隠しファイルはサポートされません。
  - ビット数の異なるローカルアプリケーションと VDA アプリケーションのタスクバーでのグループ化はサポートされません。つまり、32 ビットのローカルアプリケーションと 64 ビットの VDA アプリケーションは、タスクバーでグループ化されません。
  - アプリケーションは COM を使って起動できません。たとえば、Office アプリケーション内に埋め込まれている Office ドキュメントをクリックしても、プロセス起動が検出されないため、ローカルアプリケーション統合に失敗します。

- ユーザーが、仮想デスクトップセッション内から別の仮想デスクトップを起動するダブルホップシナリオはサポートされていません。
- 明示的な URL リダイレクトのみがサポートされます。つまり、Web ブラウザーのアドレスバーに表示される URL や、ブラウザー内ナビゲーションによる URL だけが正しくリダイレクトされます。
- URL リダイレクトはデスクトップセッションでのみ機能し、アプリケーションセッションでは機能しません。
- VDA セッションのローカルデスクトップフォルダーにユーザーがファイルを作成することはできません。
- ローカルアプリケーションの複数のインスタンスのタスクバーアイコンは、仮想デスクトップのタスクバー設定に基づいて表示されます。ただし、ローカルで実行されているアプリケーションのショートカットは、このアプリケーションの実行インスタンスのアイコンとはグループ化されません。また、ホストされているアプリケーションの実行インスタンスや、そのアプリケーションのピン留めアイコンともグループ化されません。タスクバー上のアイコンでは、ローカルで実行されているアプリケーションのウィンドウのみを閉じることができます。ローカルアプリケーションのショートカットをデスクトップタスクバーや［スタート］メニューに固定することもできますが、そのショートカットからアプリケーションを起動できなくなる場合があります。
- ポリシーの ［ローカルアプリアクセスを許可する］設定を ［有効］に設定した場合、ブラウザーコンテンツリダイレクトはサポートされません。

Windows 上での動作

ローカルアプリアクセスは、Windows 上で次のように動作します。

- Windows 8 および Windows Server 2012 のショートカットの動作
  - クライアント上にインストールされた Windows ストアアプリケーションは、ローカルアプリケーションアクセスのショートカットとして列挙されません。
  - イメージファイルとビデオファイルは、デフォルトで Windows ストアアプリケーションで開きます。ただし、ローカルアプリケーションアクセスでは、Windows ストアアプリケーションが列挙され、ショートカットがデスクトップアプリケーションで開かれます。
- Local Programs フォルダー
  - Windows 7 の場合、［スタート］メニューに Local Programs フォルダーが表示されます。

  - Windows 8 の場合、ユーザーがスタート画面のカテゴリとして ［すべてのアプリ］を選択した場合のみ、Local Programs フォルダーが表示されます。Local Programs フォルダーにすべてのサブフォルダーが表示されるわけではありません。

- アプリケーション用の Windows 8 グラフィック機能
  - デスクトップアプリケーションはデスクトップ領域に制限され、スタート画面および Windows 8 スタイルアプリケーションの背面に表示されます。
  - ローカルアプリアクセスは、マルチモニターモードでデスクトップアプリケーションのようには動作しません。マルチモニターモードでは、スタート画面とデスクトップは別のモニター上で表示されます。
- Windows 8 およびローカルアプリアクセスの URL リダイレクト
  - Windows 8 上の Internet Explorer ではアドオンを使用できないため、URL リダイレクトを有効にする場合はデスクトップ版の Internet Explorer を使用する必要があります。
  - Windows Server 2012 上の Internet Explorer では、デフォルトでアドオンが無効になっています。URL リダイレクトを実装するには、Internet Explorer の拡張構成を無効にしてください。標準ユーザーに対してアドオンが有効になるように、Internet Explorer のオプションを再設定して再起動します。

ローカルアプリアクセスと **URL** リダイレクトの構成

Citrix Workspace アプリでローカルアプリケーションアクセスと URL リダイレクトを使用するには:

- ローカルクライアントマシンに Citrix Workspace アプリをインストールします。Citrix Workspace アプリのインストール時に両方の機能を有効することも、グループポリシーエディターを使ってローカルアプリケーションアクセステンプレートを有効にすることも可能です。
- ポリシーの ［ローカルアプリアクセスを許可する］設定を ［有効］に設定します。URL リダイレクトの URL 許可リストおよび禁止リストのポリシー設定を構成することもできます。詳しくは、「ローカルアプリアクセスのポリシー設定」を参照してください。

ローカルアプリアクセスと **URL** リダイレクトの有効化

すべてのローカルアプリケーションのローカルアプリアクセスを有効にするには、次の手順を実行します:

1. ［管理］**>**［完全な構成］の左側ペインで ［ポリシー］を選択します。
2. 操作バーの ［ポリシーの作成］を選択します。
3. ［ポリシーの作成］ウィンドウで、検索ボックスに「ローカルアプリアクセスを許可する」と入力して、［選択］をクリックします。
4. ［設定の編集］ウィンドウで、［許可］を選択します。デフォルトでは、［ローカルアプリアクセスを許可する］ポリシーは禁止されます。この設定が許可されている場合、VDA により、公開アプリケーションおよびローカルアプリアクセスのショートカットを有効にするかをエンドユーザーが指定できます。(この設定が禁止されている場合、公開アプリケーションおよびローカルアプリケーションアクセスのショートカットのいずれも

VDA で機能しません。）このポリシー設定は、URL リダイレクトのポリシー設定だけではなく、マシン全体に適用されます。

5. ［ポリシーの作成］ウィンドウで、検索ボックスに「URL リダイレクトの許可リスト」と入力して、［選択］をクリックします。URL リダイレクトの許可リストは、リモートセッションのデフォルトの Web ブラウザーで開く URL を指定します。
6. ［設定の編集］ウィンドウで ［追加］をクリックして URL を追加し、［**OK**］を選択します。
7. ［ポリシーの作成］ウィンドウで、検索ボックスに「URL リダイレクトの禁止リスト」と入力して、［選択］をクリックします。URL リダイレクトの禁止リストは、エンドポイント上で実行されているデフォルトの Web ブラウザーにリダイレクトされる URL を指定します。
8. ［設定の編集］ウィンドウで ［追加］をクリックして URL を追加し、［**OK**］を選択します。
9. ［設定］ページで、［次へ］をクリックします。
10. ［ユーザーおよびマシン］ページでポリシーを該当のデリバリーグループに割り当てて、［次へ］をクリックします。
11. ［概要］ページで、設定を確認して ［完了］をクリックします。

Citrix Workspace アプリのインストール中、すべてのローカルアプリケーションで URL リダイレクトを有効にするには、以下の手順を実行します：

1. Citrix Workspace アプリのインストール時に、マシンのすべてのユーザーに対して URL リダイレクトを有効にします。これにより、URL リダイレクト機能で使用される Web ブラウザーアドオンも登録されます。
2. コマンドプロンプトで次のいずれかのオプションを付けて適切なコマンドを実行し、Citrix Workspace アプリをインストールします：
   - CitrixReceiver.exe の場合、/ALLOW_CLIENTHOSTEDAPPSURL=1を使用します。
   - CitrixReceiverWeb.exe の場合、/ALLOW_CLIENTHOSTEDAPPSURL=1を使用します。

グループポリシーエディターを使ってローカルアプリアクセステンプレートを有効にするには

> 注：
>
> - グループポリシーエディターを使用してローカルアプリアクセステンプレートを有効にする前に、receiver.admx/admlテンプレートファイルをローカルグループポリシーオブジェクト（GPO）に追加します。詳しくは、「はじめに」を参照して、「グループポリシーオブジェクト管理用テンプレート」を検索してください。
> - Windows 向け Citrix Workspace アプリのテンプレートファイルは、［管理用テンプレート］**>** ［**Citrix** コンポーネント］**>** ［**Citrix Workspace**］フォルダーのローカル GPO にあります（ユーザーがCitrixBase.admx/CitrixBse.admlを%systemroot%\policyDefinitions フォルダーに追加する場合のみ）。

グループポリシーエディターを使ってローカルアプリアクセステンプレートを有効にするには、以下の手順を実行します：

1. **gpedit.msc** を実行します。

2. [コンピューターの構成] > [管理用テンプレート] > [従来の管理用テンプレート（**ADM**）] > [**Citrix** コンポーネント] > [**Citrix Workspace**] > [ユーザーエクスペリエンス] の順に移動します。
3. [ローカルアプリケーションアクセス設定] を選択します。
4. [有効] を選択し、[**URL** のリダイレクトを許可します] チェックボックスをオンにします。URL リダイレクト機能を使用するには、この記事の「*Web* ブラウザーアドオンの登録」セクションに記載されているコマンドラインを使用して、Web ブラウザーアドオンを登録してください。

公開アプリケーションへのアクセスのみを提供する

レジストリエディターまたは PowerShell SDK を使用して、公開アプリケーションへのアクセスを管理できます。

レジストリの設定については、レジストリを介して管理される機能の一覧にある「公開アプリケーションのローカルアプリアクセス」を参照してください。

PowerShell SDK を使用するには:

1. Delivery Controller が実行されているマシンで PowerShell を開きます。
2. コマンド:`set-configsitemetadata -name "studio_clientHostedAppsEnabled "-value "true"`を実行します。

Citrix DaaS 展開で ［ローカルアプリアクセスアプリケーションの追加］にアクセスするには、Citrix Virtual Apps and Desktops Remote PowerShell SDK を使用します。詳しくは、「Citrix Virtual Apps and Desktops Remote PowerShell SDK」を参照してください。

1. インストーラーをダウンロードします:

   https://download.apps.cloud.com/CitrixPoshSdk.exe

2. 次のコマンドを実行します:

   a) `asnp citrix.*`
   b) `Get-XdAuthentication`

3. コマンド:`set-configsitemetadata -name “studio_clientHostedAppsEnabled” -value “true”`を実行します。

上記の手順を完了したら、以下の手順に従って続行します。

1. [管理] > [完全な構成] の左側ペインで ［アプリケーション］を選択します。
2. 中央上部のペインで空白の領域を右クリックし、メニューから ［ローカルアプリアクセスアプリケーションの追加］を選択します。また、[操作] ペインで ［ローカルアプリアクセスアプリケーションの追加］をクリックすることもできます。[操作] ペインで [ローカルアプリアクセスアプリケーションの追加] オプションを表示させるには、[更新] をクリックします。
3. ローカルアプリアクセスアプリケーションを公開します。

- ローカルアプリケーションアクセスウィザードが起動され、［はじめに］ページが表示されます。このページは、今後このウィザードが起動されたときに開かないように設定できます。
- ウィザードの指示に従って、［グループ］、［場所］、［識別］、［配信］、［概要］の各ページで操作を行います。各ページの操作を終えたら、［概要］ページに到達するまで ［次へ］をクリックします。
- ［グループ］ページで、アプリケーションが追加されるデリバリーグループを選択して ［次へ］をクリックします。
- ［場所］ページで、ユーザーのローカルマシン上にあるアプリケーションの実行可能ファイルのフルパスを入力し、アプリケーションが存在するフォルダーへのパスを入力します。Citrix ではシステム環境変数のパスを使用することをお勧めします（例：%ProgramFiles(x86)%\Internet Explorer\iexplore.exe）。
- ［識別］ページで、既定値をそのまま使用するか、必要な情報を入力して ［次へ］をクリックします。
- ［配信］ページで、このアプリケーションをユーザーに配信する方法を構成して ［次へ］をクリックします。選択したアプリケーションのアイコンを指定できます。このローカルアプリケーションのショートカットを仮想デスクトップの［スタート］メニューやデスクトップに追加するかどうかを指定することもできます。
- ［概要］ページで、設定を確認して ［完了］をクリックし、ローカルアプリケーションアクセスウィザードを閉じます。

Web ブラウザーアドオンの登録

> 注：
>
> URL リダイレクト機能に必要な Web ブラウザーアドオンは、コマンドラインでの Citrix Workspace アプリのインストール時に`/ALLOW_CLIENTHOSTEDAPPSURL=1`オプションを指定すると自動的に登録されます。

以下のコマンドを実行して、適切な Web ブラウザーにアドオンを登録したり登録解除したりできます。

- クライアントデバイスにアドオンを登録する場合：<*client-installation-folder*>\redirector.exe /reg<*browser*>
- クライアントデバイスのアドオンの登録を解除する場合：<*client-installation-folder*>\redirector.exe /unreg<*browser*>
- VDA にアドオンを登録する場合：<*VDAinstallation-folder*>\VDARedirector.exe /reg<*browser*>
- VDA のアドオンの登録を解除する場合：<*VDAinstallation-folder*>\VDARedirector.exe /unreg<*browser*>

ここで <*browser*> は、「Internet Explorer」、「Firefox」、「Chrome」、または「All」です。

たとえば、Citrix Workspace アプリを実行するデバイスに、Internet Explorer 用のアドオンを登録するには、次のコマンドを実行します。

C:\Program Files\Citrix\ICA Client\redirector.exe/regIE

また、Windows マルチセッション OS VDA が動作するサーバー上ですべてのアドオンを登録するには、次のコマンドを実行します。

C:\Program Files (x86)\Citrix\HDX\bin\VDARedirector.exe /regAll

さまざまな **Web** ブラウザーでの **URL** リダイレクト

- Internet Explorer では、入力された URL がデフォルトでリダイレクトされます。禁止リストに追加されていない URL が Web ブラウザーや Web サイトによりほかの URL にリダイレクトされた場合、最終的な URL はリダイレクトされません。禁止リストにあってもリダイレクトされません。

URL リダイレクトが正しく機能するためには、Web ブラウザーに表示されるメッセージに従ってアドオンを有効にする必要があります。インターネットオプションを使用するアドオンやメッセージで示されたアドオンが無効の場合、URL リダイレクトは正しく機能しません。

- Firefox アドオンでは、URL が常にリダイレクトされます。

Firefox では、アドオンのインストールを許可するかどうかを確認するメッセージが新しいタブに表示されます。URL リダイレクトが正しく機能するためには、アドオンのインストールを許可します。

- Chrome のアドオンでは、ユーザーがナビゲーションにより開いた最終的な URL（ユーザーが入力したものでない URL）は常にリダイレクトされます。

拡張機能が外部的にインストールされます。この拡張機能を無効にすると、Chrome で URL リダイレクトが動作しなくなります。シークレットモードで URL リダイレクトを使用するには、Web ブラウザーの設定でシークレットモードでの拡張機能の実行を許可する必要があります。

ログオフおよび切断時のローカルアプリケーションの動作の構成

> 注:
>
> 以下の手順どおりに設定を構成しなかった場合、ユーザーが仮想デスクトップからログオフまたは切断しても、デフォルトで、ローカルアプリケーションは実行したまま保持されます。仮想デスクトップに再接続すると、そのローカルアプリケーションが再統合されます（仮想デスクトップで使用可能な場合）。

ログオフおよび切断時のローカルアプリケーションの動作を構成するには、レジストリを介して管理される機能の一覧にある「ログオフおよび切断時のローカルアプリケーションの動作」を参照してください。

汎用 **USB** リダイレクトとクライアント側ドライブの考慮事項

April 18, 2024

HDX テクノロジは、一般的な USB デバイスのほとんどに最適化されたサポートを提供します。最適化されたサポートにより、パフォーマンスが良くなることでユーザーエクスペリエンスが向上し、WAN 経由の帯域幅効率が改善されます。最適化されたサポートは通常、遅延が多い環境やセキュリティが厳しい環境で最善のオプションです。

HDX テクノロジにより、特殊デバイスに次のような最適化されたサポートがないときや、不適切なときに汎用 **USB** リダイレクトを使用できます:

- USB デバイスに追加の高度な機能があり（追加ボタンがあるマウスや Web カメラなど）、それらの機能が最適化されたサポートに含まれていないとき。
- ユーザーが最適化されたサポートに含まれない機能を必要とするとき。
- USB デバイスが特殊なデバイス（テスト用機器、測定用機器、工業用コントローラーなど）であるとき。
- アプリケーションが USB デバイスとしてデバイスに直接アクセスする必要があるとき。
- USB デバイスで Windows ドライバーしか使用できないとき。たとえば、スマートカードリーダーには、Android 向け Citrix Workspace アプリで使用できるドライバーがないことがあります。
- 使用しているバージョンの Citrix Workspace アプリで、該当するタイプの USB デバイスに最適化されたサポートを利用できないとき。

汎用 USB リダイレクトでは、以下に注意してください。

- ユーザーデバイスにデバイスドライバーをインストールする必要はありません。
- USB クライアントドライバーは VDA マシン上にインストールされます。

> 重要:
>
> - 汎用 USB リダイレクトは、最適化されたサポートと併用できます。汎用 USB リダイレクトを有効にする場合は、Citrix の「USB デバイスのポリシー設定」で汎用 USB リダイレクトと最適化されたサポートの両方を構成します。
> - 一部の USB デバイスでは、クライアント USB デバイス最適化規則の Citrix ポリシー設定が、汎用 USB リダイレクト専用の設定となります。ここで説明したような、最適化されたサポートには該当しません。
> - Citrix ソフトウェアを使用して Azure 仮想マシンにセッションを仲介する場合、Citrix は Azure 仮想マシンへの USB リダイレクトに関するベストエフォートサポートを提供します。Citrix ソフトウェアの問題の修正をサポートしていますが、基盤となる Azure 仮想マシンはサポートしていません。
> - ディスク書き込み機能を備えた CD/DVD デバイスはリダイレクトできますが、そのデバイスの書き込み機能は使用できません。これは、セッションのバッファ制限によるものです。

USB デバイスのパフォーマンスに関する考慮事項

一部のタイプの USB デバイスで汎用 USB リダイレクトを使用する場合、ネットワークの遅延と帯域幅がユーザーエクスペリエンスと USB デバイスの操作に影響を与えます。たとえば、遅延が多く低帯域幅のリンクでタイミングが重要なデバイスが正しく動作しないことがあります。可能な場合は、代わりに最適化されたサポートを使用してください。

3D マウスなどの一部の USB デバイスは、高い帯域幅を使用できる必要があります（通常、これも高帯域幅を必要とする 3D アプリとともに使用）。帯域幅を増やすことができない場合には、帯域幅ポリシー設定を使用して他のコンポーネントの帯域幅使用状況を調整することで、問題を緩和できます。詳しくは、「帯域幅のポリシー設定」（クライアント USB デバイスリダイレクトの場合）および「マルチストリーム接続のポリシー設定」を参照してください。

USB デバイスのセキュリティに関する考慮事項

スマートカードリーダーやフィンガープリントリーダー、署名パッドなどの一部の USB デバイスは、もともとセキュリティを重視します。USB ストレージデバイスなどの他の USB デバイスは、機密扱いである可能性のあるデータの受け渡しに使用できます。

USB デバイスは、しばしばマルウェアの配信に使用されます。このような USB デバイスのリスクは、Citrix Workspace アプリと Citrix Virtual Apps and Desktops の構成により減らすことはできますが、すべて取り除くことはできません。こうした状況は、汎用 USB リダイレクトを使用しているか最適化されたサポートを使用しているかにかかわらず発生します。

> 重要:
>
> セキュリティを重視するデバイスやデータを扱う場合は、TLSまたは IPsec のどちらかを使用して、常に HDX 接続をセキュリティで保護してください。
>
> 必要な USB デバイスのサポートのみを有効にしてください。汎用 USB リダイレクトと最適化されたサポートの両方で、このニーズを満たしてください。
>
> USB デバイスの安全な使用についての以下のようなガイダンスをユーザーに提供してください。
>
> - 信頼できるソースから入手した USB デバイスのみを使用する。
> - USB デバイスを人がいないオープンな環境に置きっぱなしにしない（例: インターネットカフェに Flash ドライブを置きっぱなしにしない）。
> - また、複数のコンピューターで 1 つの USB デバイスを使用することのリスクを説明してください。

汎用 USB リダイレクトの互換性

汎用 USB リダイレクトは、USB 2.0 以前のデバイスでサポートされます。USB 3.0 デバイスを USB 2.0 または USB 3.0 ポートに接続した場合も、汎用 USB リダイレクトがサポートされます。汎用 USB リダイレクトは、USB3.0 に導入された超高速などの USB 機能はサポートしません。

汎用 USB リダイレクトは、次の Citrix Workspace アプリでサポートされます:

- Windows 向け Citrix Workspace アプリ。「アプリケーション配信の構成」を参照してください。
- Mac 向け Citrix Workspace アプリ。「Mac 向け Citrix Workspace アプリ」を参照してください。
- Linux 向け Citrix Workspace アプリ。「最適化」を参照してください。
- Chrome OS 向け Citrix Workspace アプリ。「Chrome 向け Citrix Workspace アプリ」を参照してください。

Citrix Workspace アプリのバージョンについては、『Citrix Workspace app feature matrix』を参照してください。

過去のバージョンの Citrix Workspace アプリを使用している場合は、Citrix Workspace アプリのドキュメントを参照して、汎用 USB リダイレクトがサポートされていることを確認してください。サポート対象の USB デバイスのタイプに関する制限事項については、Citrix Workspace アプリのドキュメントを参照してください。

汎用 USB リダイレクトはシングルセッション OS 対応 VDA のバージョン 7.6 以上のデスクトップセッションでサポートされます。

汎用 USB リダイレクトはマルチセッション OS 対応 VDA のバージョン 7.6 以上のデスクトップセッションでサポートされますが、以下の制限事項があります:

- VDA は Windows Server 2012 R2、Windows Server 2016、Windows Server 2019、Windows Server 2022 のいずれかで動作している必要があります。
- USB デバイスドライバーには、完全仮想化サポートなど、VDA OS（Windows 2012 R2）のリモートデスクトップセッションホスト（RDSH）との完全な互換性がある必要があります。

次のような一部のタイプの USB デバイスは、リダイレクトしても役に立たないため、汎用 USB リダイレクトをサポートしません。

- USB モデム。
- USB ネットワークアダプター。
- USB ハブ。USB ハブに接続した USB デバイスは、個別に扱われます。
- USB 仮想 COM ポート。汎用 USB リダイレクトではなく、COM ポートリダイレクトを使用します。

汎用 USB リダイレクトでテストされた USB デバイスについては、Citrix Ready Marketplaceを参照してください。一部の USB デバイスは、汎用 USB リダイレクトを使用すると正しく動作しません。

汎用 **USB** リダイレクトの設定

汎用 USB リダイレクトを使用する USB デバイスのタイプを制御し、個別に構成できます。

- Citrix ポリシー設定を使って VDA で設定します。詳しくは、「ポリシー設定リファレンス」の「クライアントドライブやデバイスのリダイレクト」、および「USB デバイスのポリシー設定」を参照してください。
- Citrix Workspace アプリで、Citrix Workspace アプリに依存するメカニズムを使用して設定します。たとえば、管理用テンプレートは、Windows 向け Citrix Workspace アプリを構成するレジストリ設定を制御できます。USB リダイレクトのデフォルトでは、特定のクラスの USB デバイスでのみ許可され、ほかのクラスのデバイスはリダイレクトされません。詳しくは、Windows 向け Citrix Workspace アプリのドキュメントの「構成」を参照してください。

別々に設定できることで柔軟性が提供されます。例:

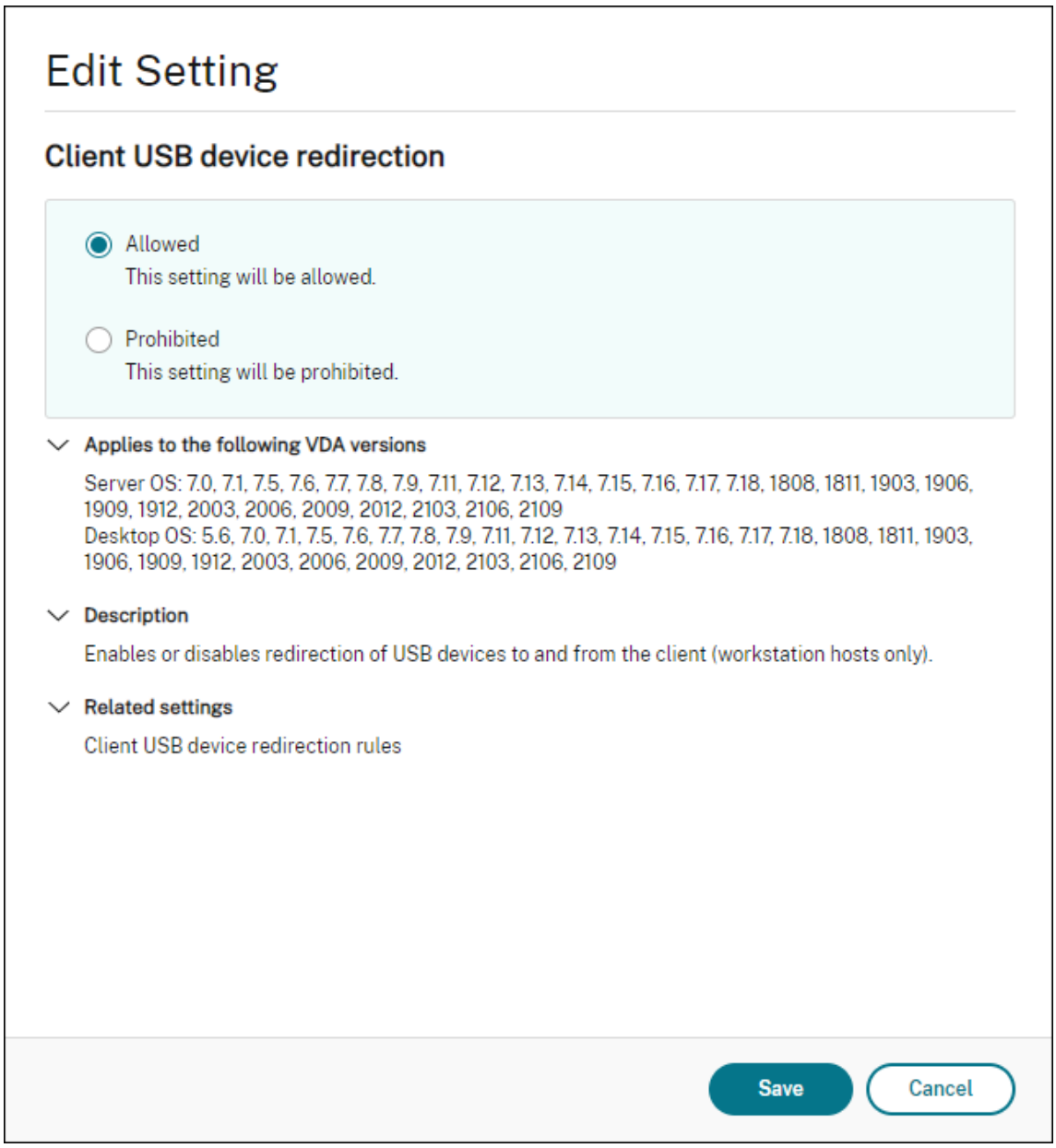
- 2 つの異なる組織または部門が Citrix Workspace アプリと VDA を担当している場合に、それぞれが別に制御を実行できます。この構成は、ある組織のユーザーが別の組織のアプリケーションにアクセスするときにも適用されます。
- Citrix ポリシー設定では、特定のユーザー、または（Citrix Gateway 経由ではなく）LAN 経由で接続しているユーザーのみに許可された USB デバイスを制御できます。

汎用 **USB** リダイレクトの有効化

汎用 USB リダイレクトを有効化して、ユーザーの手動リダイレクトを不要にするには、Citrix ポリシー設定と Citrix Workspace アプリの接続設定の両方を構成します。

Citrix ポリシー設定で、次の手順に従います：

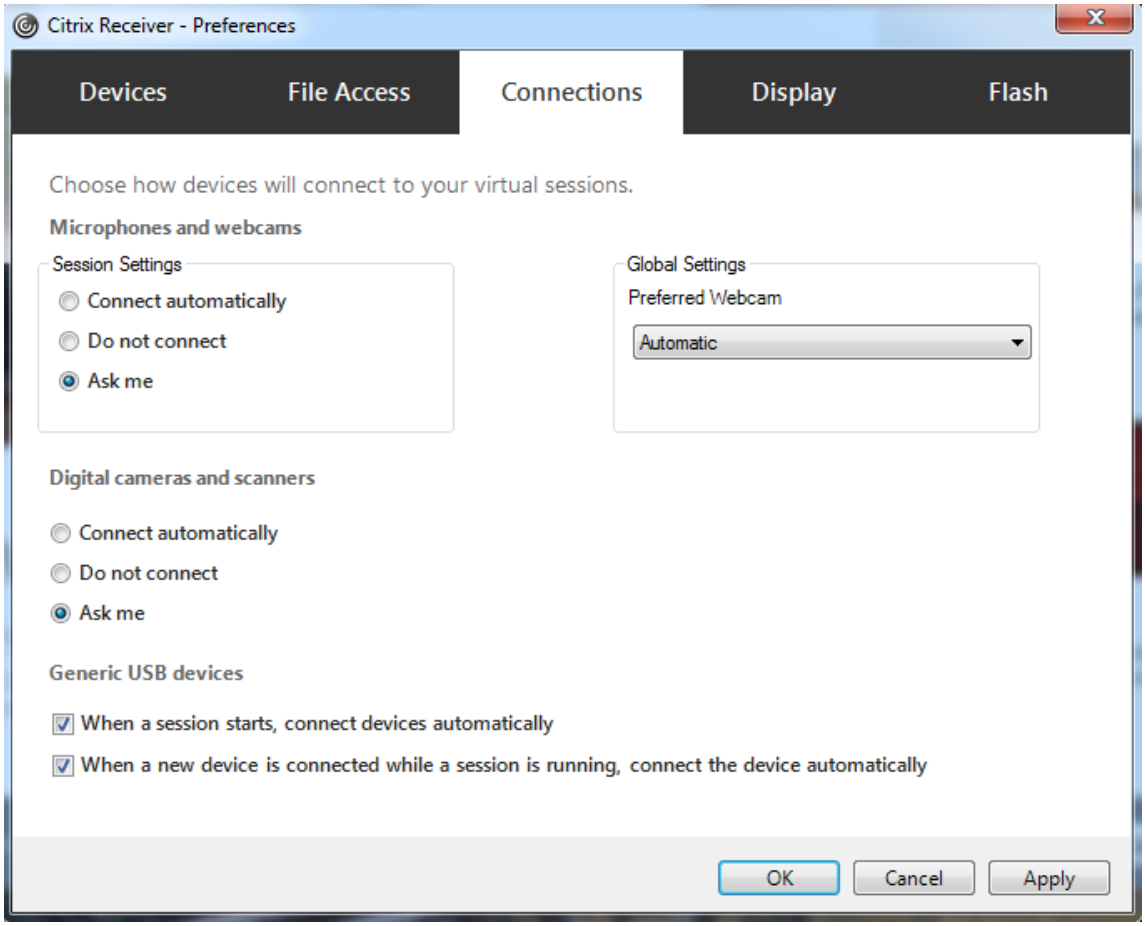
1. ポリシーに ［クライアント USB デバイスリダイレクト］ を追加して、値を ［許可］に設定します。



2. 必要な場合は、ポリシーに ［クライアント USB デバイスリダイレクト規則］ 設定を追加して USB ポリシー規則を指定し、リダイレクトする USB デバイスの一覧を変更します。

   Citrix Workspace アプリで、次の手順を実行します:

3. デバイスが手動リダイレクトなしで自動的に接続されるように設定します。この設定は、管理用テンプレートを使うか、Windows 向け Citrix Workspace アプリの［基本設定］>［接続］で実行できます。



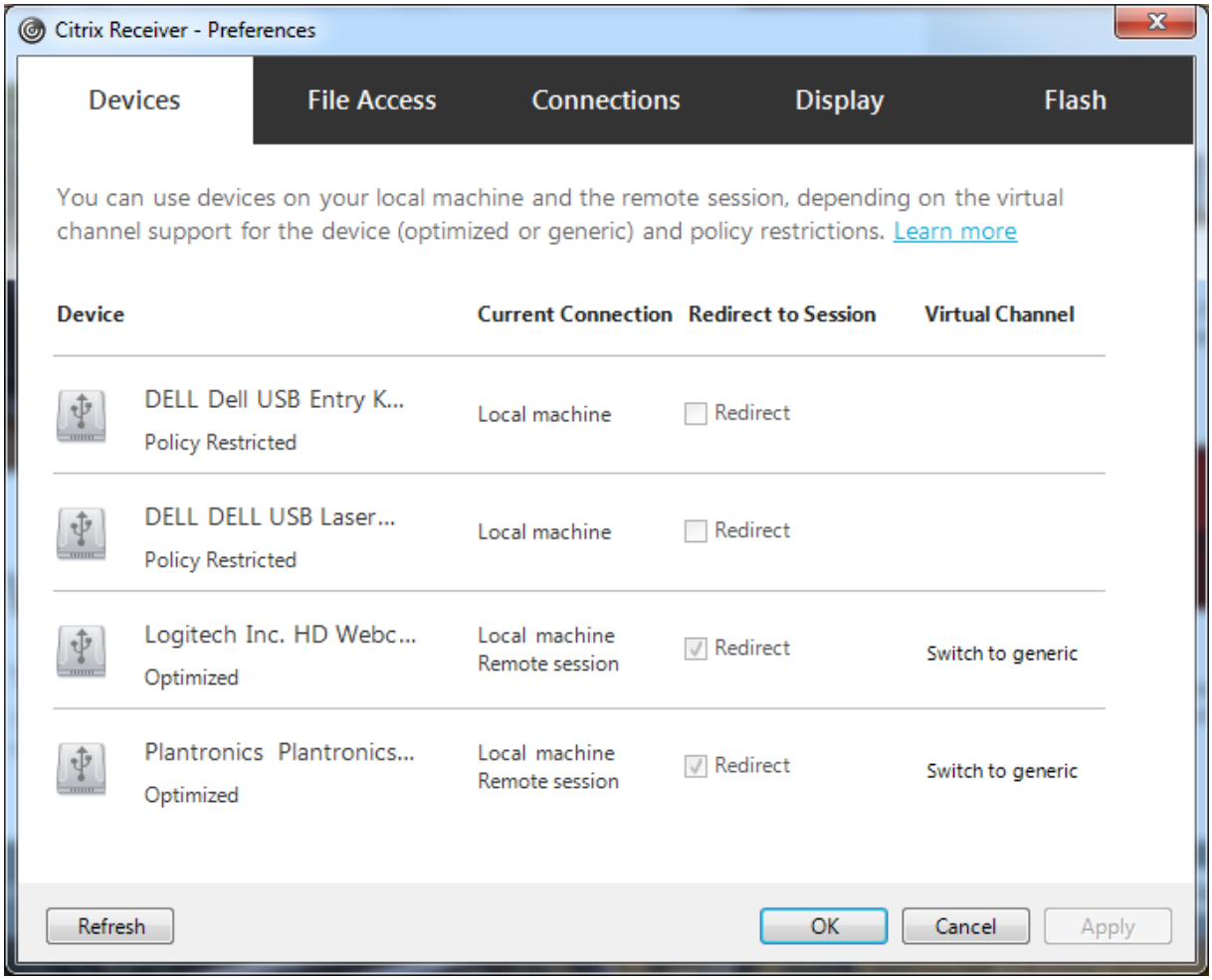
前の手順で VDA の USB ポリシー規則を指定した場合は、Citrix Workspace アプリにも同じポリシー規則を指定します。

シンクライアントでの USB サポートおよびその構成方法については、デバイスの製造元に問い合わせてください。

汎用 **USB** リダイレクトで使用できる **USB** デバイスタイプの設定

USB サポート機能が有効になっており、USB 関連のユーザー設定で USB デバイスに自動接続するように設定されている場合は、USB デバイスが自動的にリダイレクトされます。接続バーが表示されていない場合も、USB デバイスは自動的にリダイレクトされます。

ユーザーは、USB デバイスの一覧からデバイスを選択することによって、自動的にリダイレクトされないデバイスを明示的にリダイレクトすることができます。詳しくは、Windows 向け Citrix Workspace アプリのユーザーヘルプの「Desktop Viewer でのデバイスの表示」を参照してください。



最適化されたサポートではなく汎用 USB リダイレクトを使用するには、次のどちらかの手順を実行します。

- Citrix Workspace アプリで、汎用 USB リダイレクトを使う USB デバイスを手動で選択し、［基本設定］ダイアログボックスの［デバイス］タブで ［汎用に切り替え］をオンにします。
- USB デバイスタイプの自動リダイレクトを設定することで（たとえば AutoRedirectStorage=1）、汎用 USB リダイレクトを使う USB デバイスを自動選択して、USB ユーザー基本設定を自動接続 USB デバイスに設定します。詳しくは、「USB デバイスの自動リダイレクトの設定」を参照してください。

> 注:
>
> Web カメラと HDX マルチメディアリダイレクトの互換性がない場合は、Web カメラで使用する汎用 USB リダイレクトのみを設定します。

Citrix Workspace アプリおよび VDA のデバイス規則を定義して、USB デバイスを一覧に表示しないようにしたり、リダイレクトできないようにしたりできます。

汎用 USB リダイレクトでは、少なくとも USB デバイスクラスとサブクラスを知っておく必要があります。すべての USB デバイスが明確な USB デバイスクラスとサブクラスを持つわけではありません。例:

- ペンはマウスデバイスクラスを使用します。

- スマートカードリーダーはベンダー定義のクラスまたは HID デバイスクラスを使用できます。

より正確な制御のためには、ベンダー ID、製品 ID、およびリリース ID を知っておく必要があります。この情報はデバイスベンダーから入手できます。

> 重要:
>
> 悪意のある USB デバイスが、意図された使用状況にマッチしない USB デバイス特性を示すことがあります。デバイス規則は、この動作を防ぐことを目的としていません。

VDA と Citrix Workspace アプリ両方の USB デバイスリダイレクト規則を指定し、デフォルトの USB ポリシー規則よりも優先することで、汎用 USB リダイレクトを使用可能な USB デバイスを制御できます。

VDA の場合:

- グループポリシー規則を介して、マルチセッション OS マシン上の OS の管理者による上書き規則を編集します。グループポリシー管理コンソールは、インストールメディアにあります。
  - x64 の場合: DVD ルートの\os\lang\x64\Citrix Policy\ CitrixGroupPolicyManagement_x64.msi
  - x86 の場合: DVD ルートの\os\lang\x86\Citrix Policy\ CitrixGroupPolicyManagement_x86.msi

Windows 向け Citrix Workspace アプリの場合:

- ユーザーデバイス側のレジストリを編集します。インストールメディアに収録されている管理テンプレート（ADM ファイル。DVD のルート \os\lang\Support\Configuration\icaclient_usb.adm）により、Active Directory のグループポリシーを使用してユーザーデバイスを変更できます。

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

製品のデフォルトの規則は、HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\GenericUSB\DeviceRules に格納されています。このデフォルトの規則は変更しないでください。ただし、以下で説明しているように、製品のデフォルトの規則を参照して管理者による上書き規則を作成できます。管理者による上書き規則は、製品のデフォルトの規則よりも先に評価されます。

管理者による上書き規則は、HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\PortICA\GenericUSB\DeviceRules に格納されています。GPO ポリシー規則は、**{Allow: | Deny:}** の後にスペースで区切った一連の「*tag=value*」式の形式で設定します。

以下のタグがサポートされます。

タグ	説明
VID	デバイス記述子のベンダー ID
PID	デバイス記述子の製品 ID
REL	デバイス記述子のリリース ID
クラス	デバイス記述子またはインターフェイス記述子のクラス。使用可能な USB クラスコードについては、USB Web サイトhttp://www.usb.org/を参照してください
SubClass	デバイス記述子またはインターフェイス記述子のサブクラス
Prot	デバイス記述子またはインターフェイス記述子のプロトコル

ポリシー規則を作成する場合、以下の点に注意してください。

- 大文字と小文字は区別されません。
- 規則の末尾に、「#」で始まる任意のコメントを追加できます。区切り文字は不要で、コメントは無視されます。
- 空白行およびコメントのみの行は無視されます。
- 区切り文字にはスペースが使用されますが、番号または識別子の間には使用できません。たとえば、「Deny: Class = 08 SubClass=05」は有効ですが、「Deny: Class=0 Sub Class=05」は無効です。
- タグには等号（=）を使用する必要がありますたとえば、VID=1230 とします。
- 各規則を 1 行ずつ記述するか、同一行に記述する場合はセミコロンで区切られたリスト形式である必要があります。

> 注:
>
> ADM テンプレートを使用する場合は、規則を単一行に（セミコロン区切りのリストとして）作成する必要があります。

例:

- 次の例に、ベンダー ID と製品 ID に関する管理者定義の USB ポリシー規則を示します。

```
Allow: VID=046D PID=C626 # Allow Logitech SpaceNavigator 3D Mouse
 Deny: VID=046D # Deny all Logitech products
```

- 次の例に、クラス、サブクラス、およびプロトコルに関する管理者定義の USB ポリシー規則を示します。

```
Deny: Class=EF SubClass=01 Prot=01 # Deny MS Active Sync devices
Allow: Class=EF SubClass=01 # Allow Sync devices Allow: Class=EF
# Allow all USB-Miscellaneous devices
```


USB デバイスの装着と取り外し

ユーザーは、仮想セッションの開始前および開始後に USB デバイスを装着できます。

Windows 向け Citrix Workspace アプリでは、以下の点について考慮してください:

- セッションを開始した後で装着したデバイスは、Desktop Viewer の［USB］メニューに直ちに追加されます。
- USB デバイスが正しくリダイレクトされない場合、仮想セッションが開始されてからデバイスを装着することで問題が解決される場合があります。
- データの損失を避けるため、Windows で推奨される手順（［ハードウェアの安全な取り外し］アイコンの使用など）に従って USB デバイスを取り外してください。

USB マスストレージデバイスのセキュリティ制御

USB マスストレージデバイスでは最適化されたサポートが提供されます。このサポートは、Citrix Virtual Apps and Desktops のクライアント側ドライブのマッピング機能に含まれています。ユーザーのログオン時にユーザーデバイス上のドライブが自動的に仮想デスクトップのドライブ文字にマップされます。これらのドライブは、マップされたドライブ文字を持つ共有フォルダーとして表示されます。クライアント側ドライブのマッピングを構成するには、［クライアント側リムーバブルドライブ］設定を使用します。この設定は、ICA ポリシー設定の ［ファイルリダイレクトポリシー設定］ セクションにあります。

USB マスストレージデバイスでは、Client 側ドライブのマッピングまたは汎用 USB リダイレクトのどちらか、またはこの両方を使用できます。これらは Citrix ポリシーを使って制御されます。主な違いは次のとおりです。

機能	クライアントドライブマッピング	汎用 USB リダイレクト
デフォルトで有効	はい	いいえ
読み取り専用アクセスの構成が可能	はい	いいえ
デバイスアクセスが暗号化される	はい、デバイスにアクセスする前に暗号化のロックを解除した場合	はい
BitLocker To Go デバイス	いいえ	いいえ
セッション中にデバイスを安全に取り外せる	いいえ	はい（ユーザーがオペレーティングシステムで推奨される手順に従う場合）

汎用 USB リダイレクトとクライアント側ドライブのマッピングのポリシーの両方が有効な場合、セッション開始前または後に装着されたマスストレージデバイスがクライアント側ドライブのマッピングによりリダイレクトされます。汎用 USB リダイレクトとクライアント側ドライブのマッピングのポリシーの両方が有効で、自動リダイレクトが構成されている場合、セッション開始前または後に装着されたマスストレージデバイスが汎用 USB リダイレクトによりリダイレクトされます。詳しくは、Knowledge Center のCTX123015を参照してください。

> 注:
>
> USB リダイレクトはより低い帯域幅の接続（50Kbps など）でもサポートされます。ただし、大きなファイルはコピーできません。

管理

April 22, 2022

Citrix Virtual Apps and Desktops サービス環境は、シトリックスが Citrix Cloud のコアコンポーネントと機能をインストールおよびメンテナンスして管理しています。

お客様が管理する必要があるのは、アプリやデスクトップを配信するリソースの場所のマシン（VDA）です。また、これらのリソースの場所への接続、アプリ、デスクトップ、ユーザーを管理することもできます。

- **Autoscale**：プロアクティブにマシンの電源を管理するための、一貫した、高性能なソリューション。
- アプリケーション：アプリケーションはデリバリーグループで管理します。
- 仮想 **IP** および仮想ループバック： Microsoft 社の仮想 IP アドレス機能により、セッションごとに動的に割り当てられる一意の IP アドレスを公開アプリケーションで使用できます。Citrix の仮想ループバックを使用すると、ローカルホスト（デフォルトで 127.0.0.1）と通信するアプリケーションで、ローカルホストの範囲内（127.*）で固有の仮想ループバックアドレスが使用されるように構成できます。
- **VDA** 登録：アプリやデスクトップの配信に VDA を利用するには、Cloud Connector に VDA を登録（接続を確立）する必要があります。Cloud Connector のアドレスは、この記事で説明する複数の方法で指定できます。Cloud Connector を追加する場合、VDA には最新の情報が必要です。
- セッション：最高のユーザーエクスペリエンスを提供するためには、セッションアクティビティを保守することが重要です。中には、セッションの信頼性を最適化し、不便さやダウンタイム、生産性の損失を軽減できる機能もあります。
- 検索の使用：［完全な構成］管理インターフェイスでマシン、セッション、マシンカタログ、アプリケーション、デリバリーグループに関する情報を表示する場合、柔軟な検索機能を使用できます。
- **IPv4** または **IPv6** のサポート： Citrix Virtual Apps and Desktops では、IPv4 のみまたは IPv6 のみ（ピュア IPv4 またはピュア IPv6）の環境、および重複する IPv4 と IPv6 のネットワークを使用したデュアルスタック環境がサポートされます。ここでは、これらの展開について説明します。また、IPv4 または IPv6 の使用を制御する Citrix ポリシー設定についても説明します。
- **Profile Management**： VDA をインストールする場合は、Citrix Profile Management もインストールできます。このユーザープロファイルソリューションを使用する場合は、そのマニュアルを参照してください。

- **Citrix Insight Services**: Citrix Insight Services（CIS）は、計測を行って利用統計情報を収集し、ビジネス洞察を得るための、Citrix が提供するプラットフォームです。VDA をインストールすると、分析情報と診断情報が収集されます。
- ローカルホストキャッシュ：ローカルホストキャッシュ機能を使用すると、リソースの場所にある Cloud Connector が Citrix Cloud と通信できなくなった場合でも、接続仲介操作を続行できるようになります。スケール、サイズ、およびその他の構成に関する考慮事項も提供されます。
- 委任管理：委任管理により、組織内の役割に応じて管理者に必要となる、すべてのアクセス権限を構成できます。
- 構成ログ：構成ログにより、管理者は構成の変更や管理のアクティビティを追跡できます。
- イベントログ：Citrix Virtual Apps and Desktops 内のサービスは、発生するイベントをログに記録します。イベントログは、操作を監視およびトラブルシューティングするために使用できます。
- ライセンス：Citrix Cloud コンソールからこのサービスの Citrix ライセンスの使用状況を表示できます。
- マシンの負荷分散：マシンの負荷分散方法を制御できます。

アダプティブアクセス

June 30, 2022

今日の絶え間なく変化する世界では、アプリケーションのセキュリティはあらゆるビジネスにとって不可欠な要素となっています。コンテキストに基づいてセキュリティ上の決定を行いながら、アプリケーションへのアクセスを許可することで、関連リスクを軽減しながら、ユーザーがアクセスできるようにします。

アダプティブアクセス機能は、アプリケーションへのセキュアなアクセスを可能にする、包括的なゼロトラストアクセスのアプローチを提供します。アダプティブアクセスにより、管理者は、ユーザーによるアプリへのアクセスを、コンテキストに基づいて詳細なレベルで設定できます。「コンテキスト」という用語は、以下を指します：

- ユーザーとグループ（ユーザーとユーザーグループ）
- デバイス（デスクトップまたはモバイルデバイス）
- 場所（位置情報またはネットワークの場所）
- Device posture（デバイスの態勢チェック）
- リスク（ユーザーリスクスコア）

Device Posture

March 5, 2024

Citrix Device Posture サービスは、クラウドベースのソリューションであり、エンドデバイスが Citrix DaaS (Citrix Virtual Apps and Desktops ）または Citrix Secure Private Access のリソース（SaaS および Web アプリまたは TCP および UDP アプリ）にアクセスするために満たす必要がある特定の要件を、管理者が適用するのに役立ちます。ゼロトラストベースのアクセスを導入するためには、デバイスのセキュリティ態勢をチェックしてデバイスの信頼性を確立することが重要です。Device Posture サービスは、エンドデバイスのコンプライアンス（管理対象/BYOD、およびセキュリティ態勢）をチェックすることで、エンドユーザーがログインする前にネットワークにゼロトラストの原則を適用します。

詳しくは、「Device Posture」を参照してください。

アダプティブ認証サービス

March 31, 2024

Citrix Cloud のお客様は、Citrix Workspace を使用して、Citrix DaaS にアダプティブ認証を提供できます。アダプティブ認証は、Citrix Workspace にログインしている顧客とユーザーに高度な認証を可能にする Citrix Cloud サービスです。アダプティブ認証サービスは、Citrix が管理し Citrix Cloud がホストする ADC であり、次のようなすべての高度な認証機能を提供します:

- Active Directory、RADIUS、証明書、SAML 2.0、OAuth、OIDC、Google Captcha を使用した複数のサードパーティ ID プロバイダーなど、さまざまな認証方法を使用した多要素認証。
- 場所、デバイスステータス、ユーザーグループなどの要因に基づいて、ユーザー ID と認証レベルを確認します。
- DaaS（仮想化）および SPA（Web および SaaS アプリなどの非仮想化リソース）へのコンテキストアクセスまたはスマートアクセスを可能にします。
- ログインページのカスタマイズ

アダプティブ認証ついて詳しくは、「アダプティブ認証サービス」を参照してください。

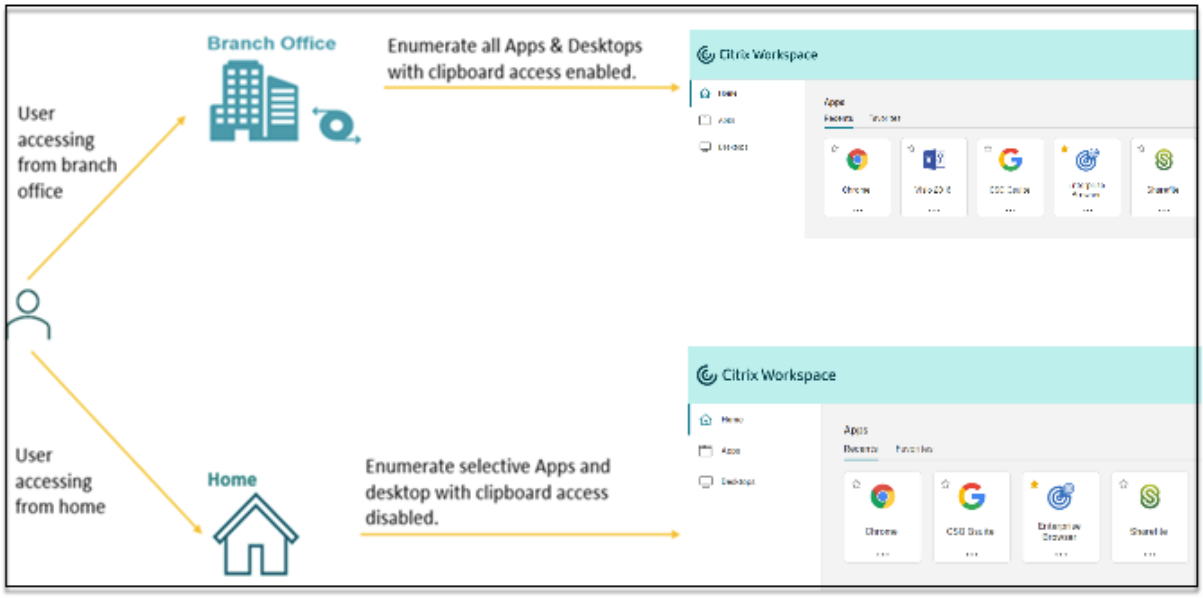
ユーザーのネットワークの場所に基づいたアダプティブアクセス

June 12, 2024

Citrix Workspace アダプティブアクセス機能は、高度なポリシーインフラストラクチャを使用して、ユーザーのネットワークの場所に基づいた Citrix DaaS へのアクセスを可能にします。場所は、IP アドレス範囲またはサブネットアドレスで定義されます。

管理者は、ユーザーのネットワークの場所に基づいて、仮想アプリおよび仮想デスクトップを列挙するかどうかのポリシーを定義できます。また、管理者は、ユーザーのネットワークの場所に基づいて、クリップボードアクセス、プ

リンター、クライアントドライブマッピングなどを有効または無効にすることで、ユーザー操作を制御できます。たとえば、自宅からリソースにアクセスするユーザーにはアプリケーションへのアクセスが制限され、ブランチオフィスからリソースにアクセスするユーザーにはフルアクセスが許可されるようにポリシーを設定できます。



管理者は、アプリケーションにアクセスするための以下のポリシーを実装できます:

- 企業の社屋またはブランチオフィスからのみ、機密性の高いアプリケーションをいくつか列挙する。
- 従業員が外部ネットワークからワークスペースにアクセスしている場合は、機密性の高いアプリケーションを列挙しない。
- ブランチオフィスからのプリンターアクセスを無効にする。
- ユーザーが企業ネットワークの外部にいる場合は、クリップボードアクセスとプリンターアクセスを無効にする。

使用権

アダプティブアクセス機能は、次のライセンスのいずれかを持つお客様にご利用いただけます。

- DaaS Premium/Premium Plus
- Secure Private Access Advanced

前提条件

- アダプティブアクセス機能が有効になっていることを確認します（[**Citrix Workspace**] > [アクセス] > [アダプティブアクセス]）。詳しくは、「アダプティブアクセス機能を有効にする」を参照してください。

  アダプティブアクセスが有効になっている場合、DaaS アクセスポリシーは、[**Citrix Gateway** を経由する接続] オプションを使用するように更新されます。

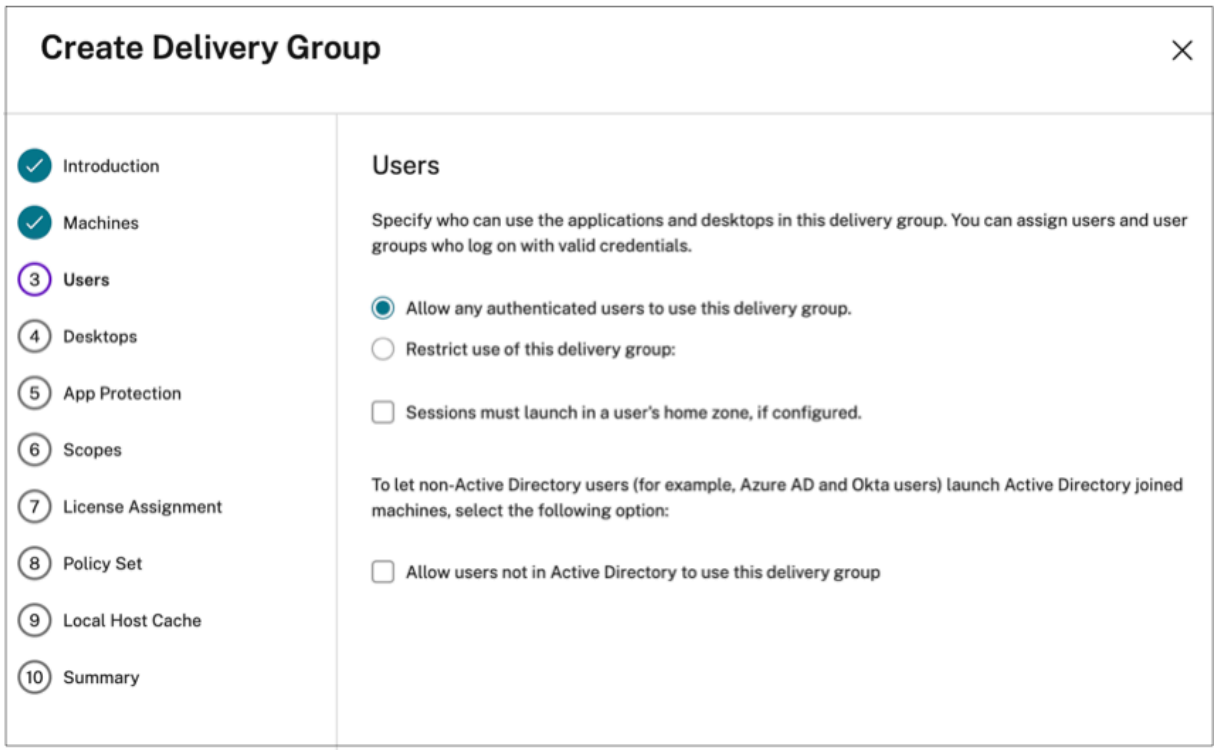
> 注:
>
> DaaS アクセスポリシーにスマートアクセスタグを追加するには、NetScaler Gateway が必要です。ただし、DaaS は Device Posture、アダプティブアクセス、およびアダプティブ認証サービスからのタグを消費するため、環境の NetScaler Gateway で構成する必要はありません。

- 場所のタグについての知識。詳しくは、「ネットワークの場所のタグ」を参照してください。

注意事項

次の項目は、場所に基づいてアプリケーションの列挙を制限する場合にのみ適用されます。アダプティブアクセスを使用して、ネットワークの場所に基づくクリップボードアクセス、プリンターリダイレクト、クライアントドライブマッピングを無効にするなどのユーザーコントロールを制限する場合は、これらのガイドラインは必要ありません。

- ネットワークの場所に基づいて Citrix DaaS を選択的に列挙する場合は、ワークスペースではなく Citrix Studio ポリシーを使用して、これらのデリバリーグループに対してユーザー管理を実行する必要があります。デリバリーグループを作成するときは、［ユーザー設定］で、［このデリバリーグループの使用を制限します］または ［任意の認証ユーザーによるこのデリバリーグループの使用を許可します］を選択します。これにより、［デリバリーグループ］下の ［アクセスポリシー］タブでアダプティブアクセスを構成できます。



- アダプティブアクセスが有効な場合は、直接ワークロード接続に変更されます。
  - ［場所のタグ］フィールドが ［**Citrix Cloud**］**>**［ネットワークの場所］**>**［ネットワークの場所を追加］**>**［場所のタグ］に表示されます。

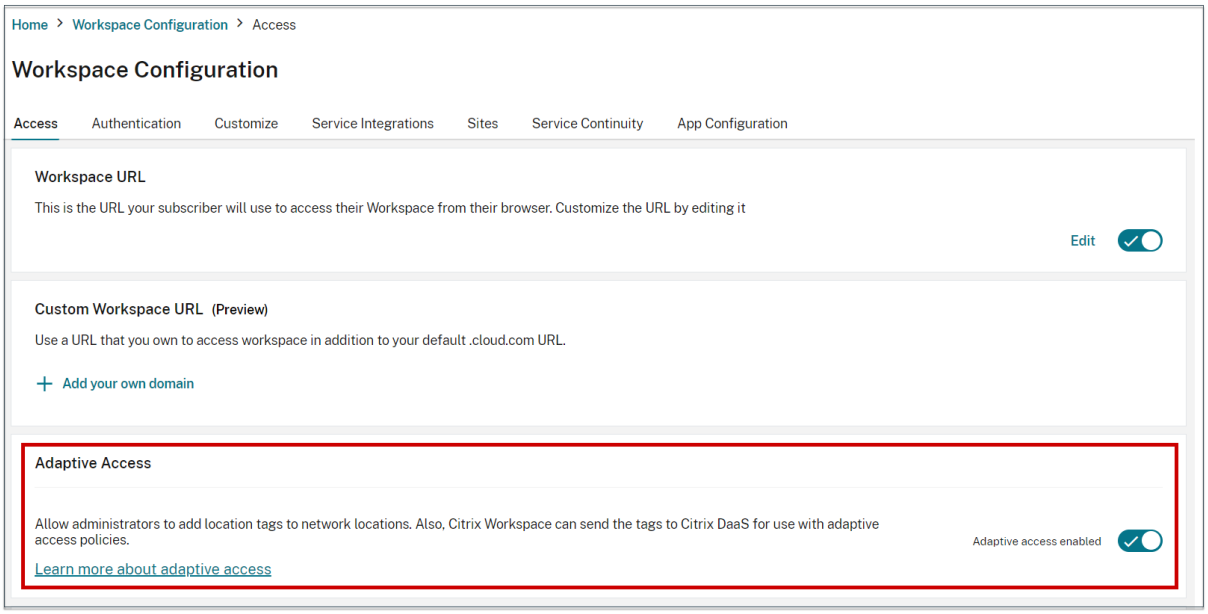
  - 既存の直接ワークロード接続ポリシーは正常に機能します。
  - 新しいポリシーは、ネットワークの場所サービス（タグを定義しない）とデリバリーグループで作成する必要があります。さらに、ネットワーク接続の種類は内部である必要があります。
  - タグを使用した直接ワークロード接続の新しいポリシーの場合は、ネットワークの場所サービスでタグを定義する必要があり、DaaS Studio のデリバリーグループまたはアクセスポリシーでも同じタグを定義する必要があります。さらに、ネットワーク接続の種類は内部である必要があります。場所のタグは、直接ワークロード接続には関係ありません。

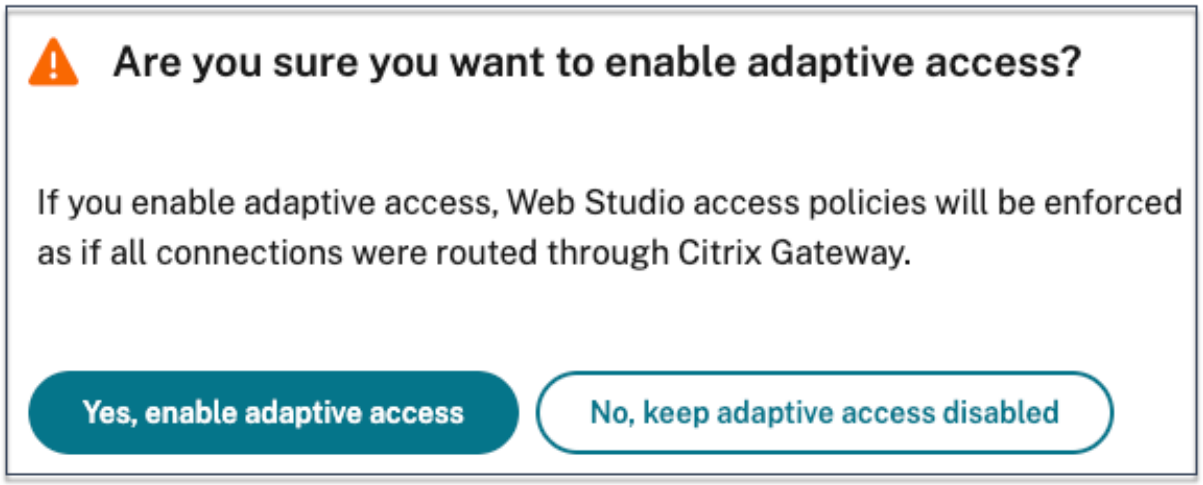
- Citrix DaaS 展開でのテストには、以下をお勧めします。

  - テストのデリバリーグループを特定するか、デリバリーグループを作成して、この機能を実装します。
  - ポリシーを作成するか、テストのデリバリーグループで使用できるポリシーを特定します。

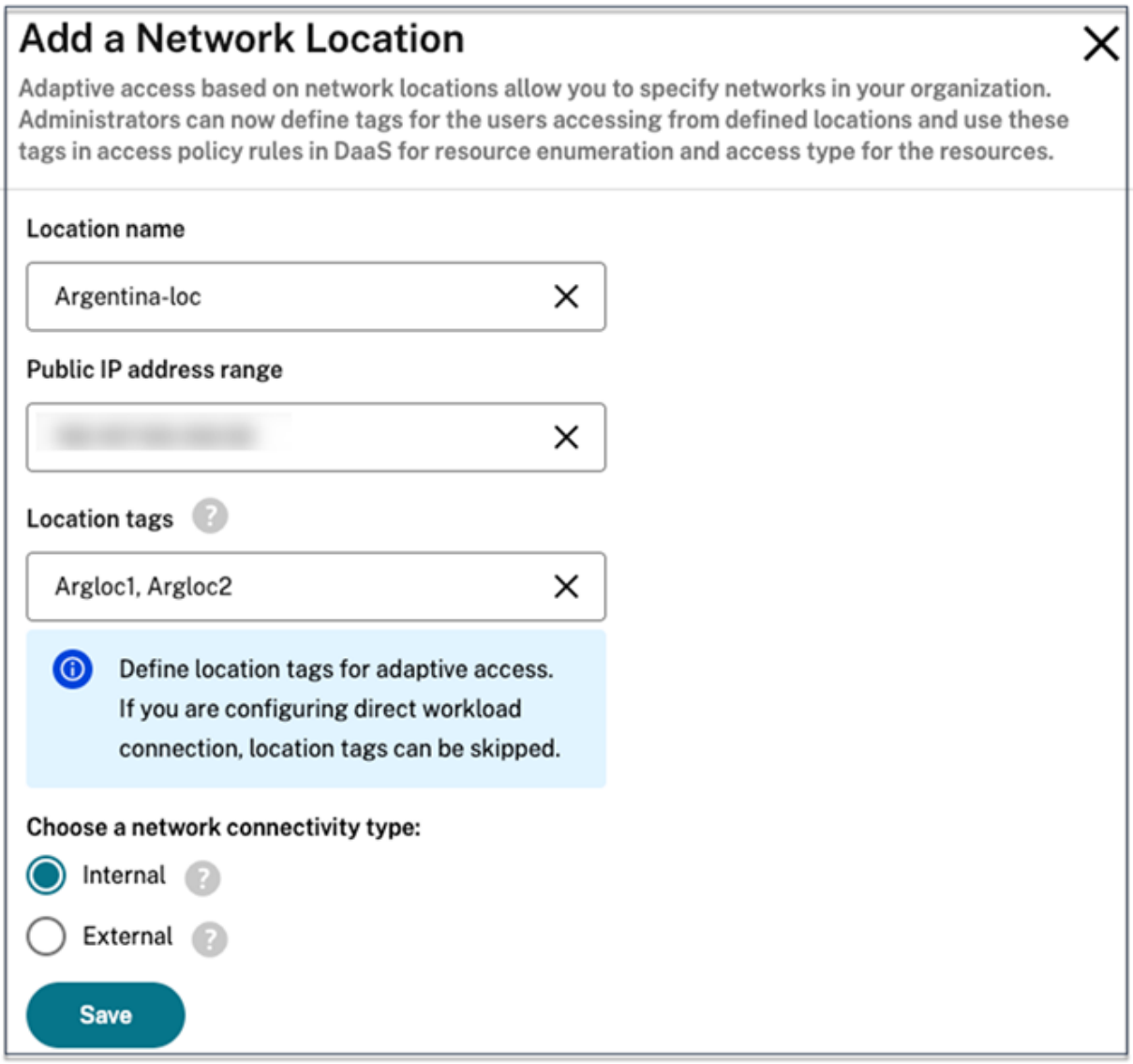
アダプティブアクセス機能を有効にする

1. Citrix Cloud にログオンします。
2. ハンバーガーメニューから ［ワークスペース構成］を選択します。
3. ［アダプティブアクセス］のトグルは、デフォルトではオフになっています。［アダプティブアクセス］のトグルをオンにします。
4. 確認メッセージで ［はい。アダプティブアクセスを有効にします］をクリックします。

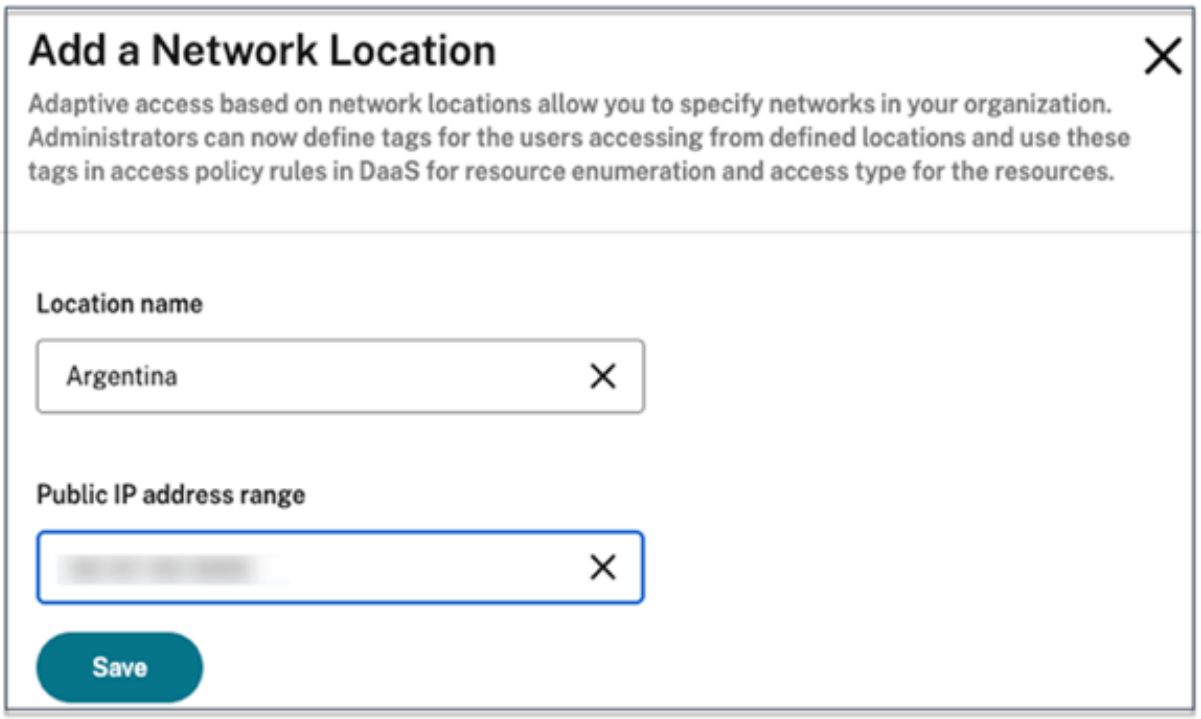




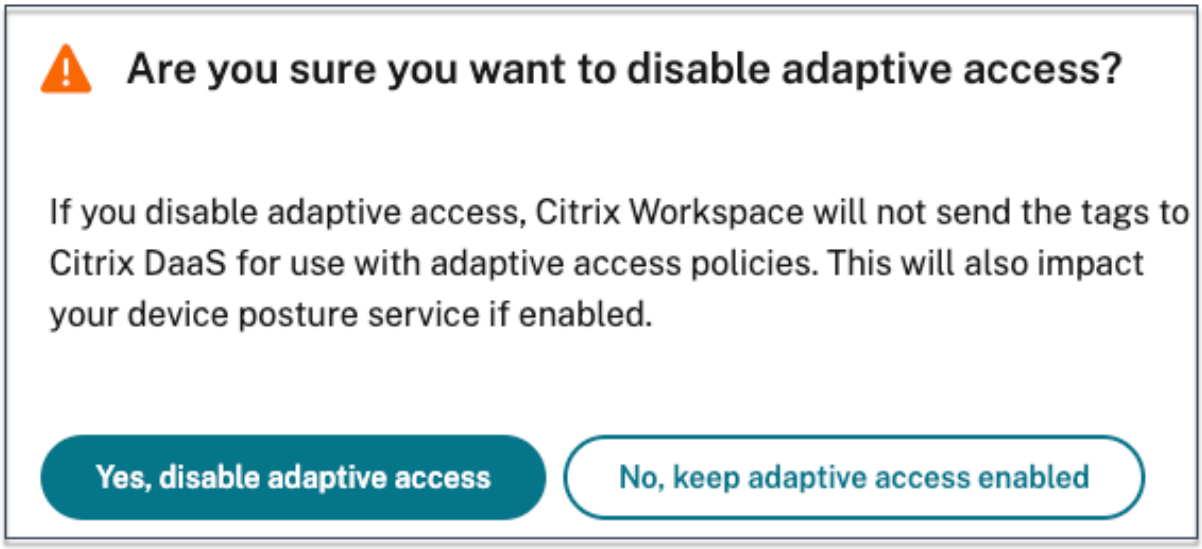
アダプティブアクセスが有効になっている場合、アダプティブアクセスの場所のタグを定義できます（[**Citrix Cloud**] **>** [ネットワークの場所] **>** [ネットワークの場所を追加] **>** [場所のタグ]）。



アダプティブアクセスが無効になっている場合は、ネットワークの場所を追加できません。この場合、場所のタグは適用できません。



> 重要:
>
> アダプティブアクセス機能を無効にしようとすると、次のメッセージが表示されます。この機能が無効になっている場合、Workspace はアダプティブアクセスのタグを DaaS に送信しないことに注意してください。



アダプティブアクセスを構成する

ネットワークの場所に基づいてアダプティブアクセスを設定するには、次の基本手順が必要です。

1. ネットワークの場所ポリシーを定義します

2. DaaS Studio でタグを定義します

構成の例として、2 種類のユーザー（**BranchOffice** ユーザーと **WorkFromHome** ユーザー）が選択され、次のユースケースを達成します。

- BranchOffice ユーザーは、すべてのアクセス権でアプリケーションにアクセスできる必要があります。
- WorkFromHome ユーザーはクリップボードにアクセスできない必要があります。

この構成例では、タグの例として **Home** と **Office** が使用されています。

ネットワークの場所ポリシーを構成する

1. Citrix Cloud にサインインします。
2. ハンバーガーメニューから ［ネットワークの場所］ を選択します。
   ［アダプティブアクセス］ トグルが有効になっていることを確認します。それ以外の場合は、直接ワークロード接続のユーザー インターフェイスが表示されます。
3. ［ネットワークの場所を追加］ をクリックします。

   - 場所の名前：ポリシーの適切な名前を入力します。

     例：BranchOffice または WorkFromHome

   - パブリック **IP** アドレスの範囲：ネットワークのパブリック IP アドレスの範囲を定義します。

     例：172.9.2.1-172.9.2.30

   - 場所のタグ：場所のタグを定義します。これには、自分の場所を表す名前を使用できます。これらのタグは、Citrix Studio でアダプティブアクセスポリシーを構成するために使用されます。詳しくは、「**Citrix Studio** でタグを定義する」を参照してください。

     例：*BranchOffice* または *WorkFromHome*

   - 接続の種類：アプリケーション起動の種類を定義します。

   内部 - アプリケーション起動でゲートウェイをバイパスします。
   外部 - アプリケーション起動には Citrix Gateway サービスまたは従来のゲートウェイを使用します。
4. ［**Save**］ をクリックします。

DaaS Studio でこれらのタグを使用して、アダプティブアクセスを有効にできるようになりました。

> 注：
>
> 場所のタグを定義する場合は、プレフィックス「LOCATION_TAG」を付けずに目的のタグ名のみを入力してください。例：「BranchOffice」。ただし、Citrix Studio でタグを定義する場合は、タグ名の前に「LOCATION_TAG」というプレフィックスを付ける必要があります。例：「LOCATION_TAG_BRANCHOFFICE」。

GUI を使用して **Citrix Studio** でタグを定義する

この例では、ユーザーのアプリケーションの列挙を制限するために、デリバリー グループでタグが定義されています。2 つのデリバリー グループが作成されます。

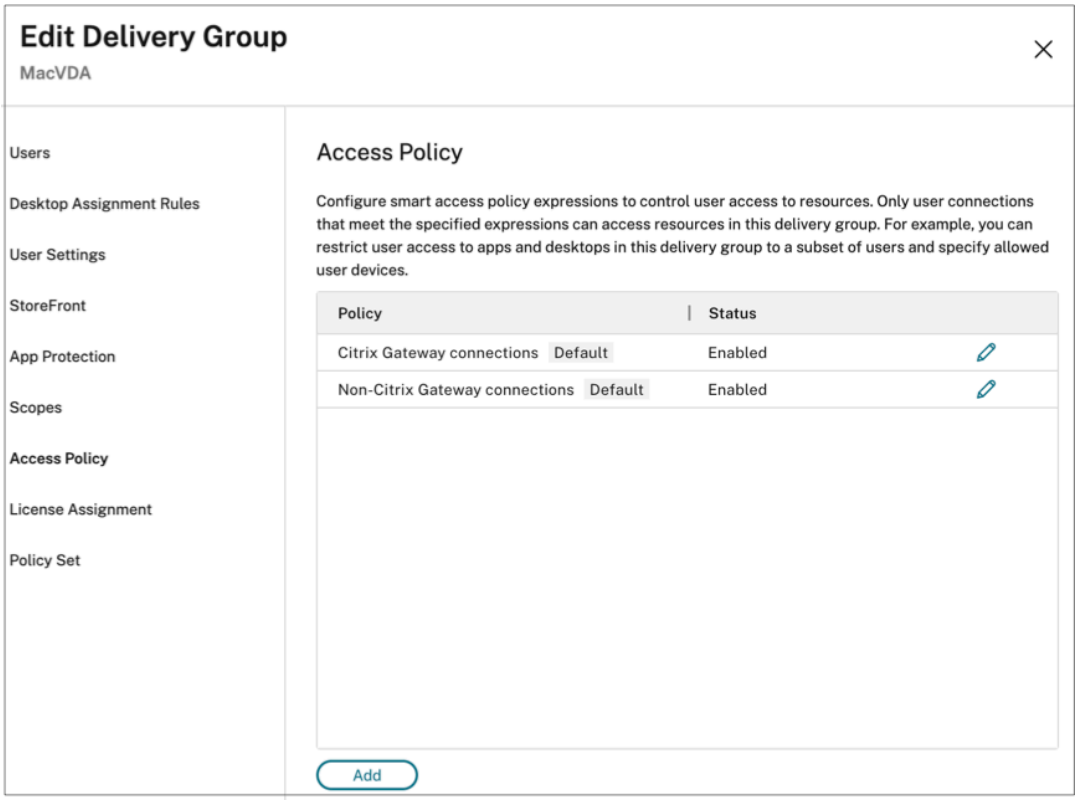
- アダプティブアクセスデリバリーグループ–**BranchOffice** の場所のユーザー用。これらのユーザーには、このデリバリーグループのすべてのアプリケーションが表示される必要があります。
- WFH デリバリーグループ–**WorkfromHome** の場所のユーザー用。これらのユーザーには、このデリバリーグループのアプリケーションが表示される必要があります。

1. Citrix Cloud にサインインします。
2. [**Citrix DaaS**] タイルで、[管理] をクリックします。
3. デリバリーグループを作成します。詳しくは、「デリバリーグループの作成」を参照してください。
4. 作成したデリバリーグループを選択し、[デリバリーグループの編集] をクリックします。
5. [アクセスポリシー] をクリックします。
6. Citrix Workspace プラットフォーム内でアダプティブアクセスを使用しているお客様は、次の手順を実行して、デリバリーグループのアクセスを内部ネットワークのみに制限してください:

   a) デリバリーグループを右クリックし、[編集] を選択します。

   b) 左ペインでアクセスポリシーを選択します。

   c) 編集アイコンをクリックして、デフォルトの Citrix Gateway 接続ポリシーを変更します。



d) ［ポリシーの編集］ページで、［次の条件に一致する接続］を選択し、［一部が一致］を選択して、条件を追加します。

WorkFromHome ユーザーの場合は、各 Delivery Controller で次の値を入力します。

ファーム：ワークスペース

フィルター：LOCATION_TAG_WORKFROMHOME

BranchOffice ユーザーの場合は、各 Delivery Controller で次の値を入力します。

フィルター：ワークスペース

値：LOCATION_TAG_BRANCHOFFICE

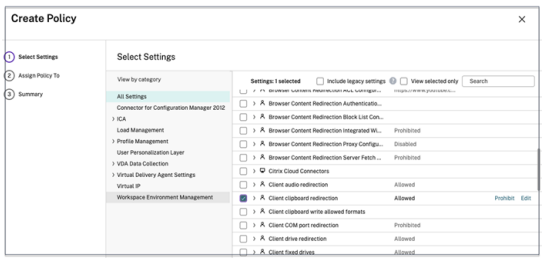
これらのタグを使用して、アプリケーションへのアクセスを制限できるようになりました。

> 注：
>
> 値フィールドには、ネットワークの場所ポリシーの作成時に定義した、プレフィックス「LOCATION_TAG」が付いた正しい場所のタグ名を入力してください。たとえば、場所のタグを「BranchOffice」と定義した場合は、値フィールドに「LOCATION_TAG_BRANCHOFFICE」と入力する必要があります。場所のタグの構成について詳しくは、「ネットワークの場所ポリシーを構成する」を参照してください。

アプリケーションのアクセスを制限する

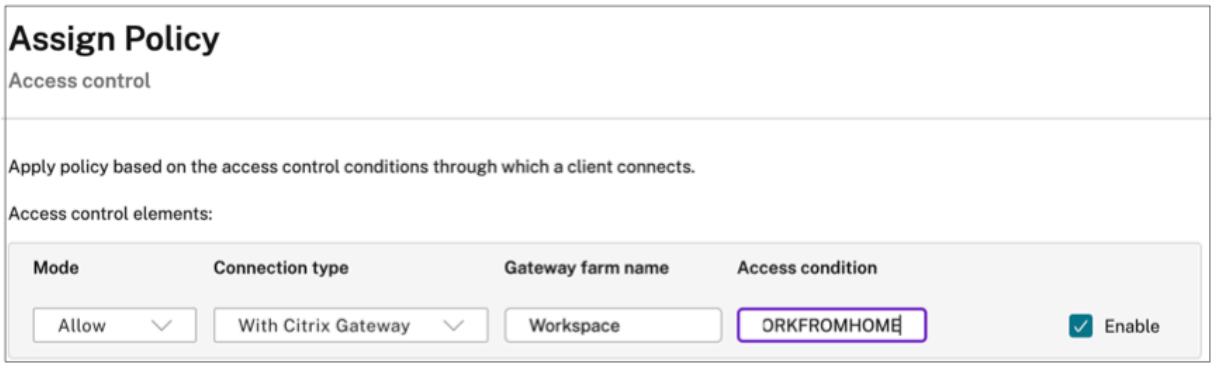
この例では、WorkFromHome の場所からのユーザーに対してクライアントクリップボードリダイレクトが無効になっています。

1. Citrix DaaS にサインインします。
2. ［ポリシー］に移動し、［ポリシーの作成］をクリックします。
3. ［クライアントクリップボードリダイレクト］を選択し、［禁止］をクリックします。
4. ［次へ］をクリックします。



1. ［ポリシーの割り当て］ページで、［アクセス制御］を選択します。
2. ポリシーに次の値を定義します：

   - モード：許可
   - 接続の種類：**Citrix Gateway** を使用する
   - Gateway ファーム名：ワークスペース
   - アクセス条件：**LOCATION_TAG_WORKFROMHOME**（すべて大文字）



1. ［次へ］をクリックします。
2. ポリシーの名前を入力し、ポリシーの説明を追加します。
3. ［完了］をクリックします。

場所 **WorkFromHome** からのユーザーは、起動されたリソースへのクリップボードアクセスを実行できません。

タグに基づいた **Session Recording** ポリシーの構成

Session Recordingにより、組織は仮想セッションでの画面上のユーザーアクティビティを録画できます。カスタム Session Recording ポリシー、イベント検出ポリシー、またはイベント応答ポリシーを作成するときに、ネットワークの場所のタグなどのタグを指定できます。例に関しては、「カスタム録画ポリシーの作成」を参照してください。

ネットワークの場所のタグ

ネットワークの場所サービスは次のタグを提供します。

- デフォルトのタグ：これらのタグは、ネットワークの場所サービスで定義されます。以下のデフォルトのタグが利用可能です。
  - **Location_internal**：ネットワーク接続の種類が内部に設定されている場合に、デフォルトで送信されるタグ。
  - **Location_external**：ネットワーク接続の種類が外部に設定されている場合に、デフォルトで送信されるタグ。
  - **Location_undefined**：ポリシーで定義されていないが、ネットワークの場所サービスを経由する IP アドレスで送信されるタグ。これらのユーザーの起動は、リソースグループで定義されているものと同じです。
- カスタムタグ：管理者はポリシーでカスタムタグ名を定義できます。例：office、home、branch

例：

デフォルトのタグ：LOCATION_INTERNAL、LOCATION_EXTERNAL、LOCATION_UNDEFINED

カスタムタグ：LOCATION_TAG_OFFICE、LOCATION_TAG_HOME

> 注:
>
> ネットワークの場所サービスのタグを定義するときは、次の点を確認してください:
>
> - デフォルトのタグは常にプレフィックス「LOCATION_<tag name>」で始まります。たとえば、LOCATION_INTERNAL。
> - カスタムタグは常にプレフィックス「LOCATION_TAG<tag name>」で始まります。たとえば、LOCATION_TAG_OFFICE。

既知の問題

アダプティブアクセス機能を有効にし、規則（タグと接続の種類）を設定した後でアダプティブアクセス機能を無効にしても、場所のタグと接続の種類の列は非表示になりますが、［ネットワークの場所］ページから場所は削除されません。ただし、これらの場所はバックエンドでは無効になっています。これは表示上の問題です。

アプリパッケージ

June 12, 2024

アプリケーションをユーザーに配信するためのパッケージテクノロジには、App-V、MSIX、MSIX アプリのアタッチ、FlexApp などがあります。ここでは、Citrix DaaS 環境でこれらのパッケージアプリケーションを展開および配信する方法について説明します:

- App-V アプリケーションの展開および配信
- MSIX および MSIX アプリのアタッチアプリケーションの展開と配信
- FlexApp アプリケーションの展開および配信

App-V アプリケーションの展開および配信

このセクションでは、次の情報について説明します:

- 概要。Citrix DaaS が App-V パッケージの配信および管理に使用する管理方法について説明します。
- 手順。これらのパッケージを展開および配信する手順を提供します。

概要

このセクションでは、Citrix DaaS が App-V パッケージの配信および管理に使用する管理方法について説明します。App-V パッケージアプリケーションの配信時に対話するコンポーネントと概念について詳しくは、

Microsoft のドキュメントを参照してください：https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-for-windows。

Citrix DaaS は、次の方法を使用して App-V パッケージを配信および管理します：

- デュアル管理。アプリケーションパッケージは、App-V サーバーで構成および管理されます。Citrix DaaS サーバーと App-V サーバーは連携して、パッケージを配信および管理します。

  この方法では、Citrix DaaS が、App-V サーバーの状態を示すスナップショットビューを定期的に更新する必要があります。これにより、ハードウェア、インフラストラクチャ、および管理にオーバーヘッドが生じます。Citrix DaaS と App-V サーバーは、特にユーザーの権限においては、同期されたままである必要があります。

  デュアル管理は、App-V と Citrix Cloud が緊密に連携している環境で最適に機能します：

  - **App-V** 管理サーバー。App-V パッケージと動的構成ファイルのライフサイクルを公開および管理します。
  - VDA マシンにインストールされた **Citrix Personalization** コンポーネント。アプリケーションの起動に必要な、適切な App-V 公開サーバーの登録を管理します。

  この方式によって、App-V 公開サーバーは適切なタイミングでユーザーに対して同期されます。公開サーバーは、ログオングループや接続グループの更新など、パッケージのライフサイクルにおけるさまざまな面を維持します。

- シングル管理。アプリケーションパッケージはネットワーク共有に保存されます。Citrix DaaS は、パッケージを個別に配信および管理します。

  この方式では、環境に App-V サーバーとデータベースインフラストラクチャが必要ないため、オーバーヘッドが削減されます。

  この方式では、App-V パッケージをネットワーク共有に保存し、そのメタデータをその場所から Citrix Cloud にアップロードします。VDA マシンにインストールされた Citrix Personalization コンポーネントは、次のようにアプリケーションを管理および配信します：

  - アプリケーションの起動時に、展開の構成ファイルとユーザー構成ファイルを処理します。
  - ホストマシン上のパッケージのライフサイクルに関するすべての面を管理します。

両方の管理方式を同時に使用することもできます。つまり、アプリケーションをデリバリーグループに追加する場合、App-V サーバーまたはネットワーク共有にある App-V パッケージからアプリケーションを追加できます。

> 注：
>
> 両方の管理方式を同時に使用しており、App-V パッケージで両方の場所に動的構成ファイルがある場合は、App-V サーバーのファイル（デュアル管理）が使用されます。

手順

App-V アプリケーションの配信をサポートするには、VDA マシンに Citrix Personalization コンポーネントをインストールする必要があります。詳しくは、「VDA マシンへの Citrix Personalization コンポーネントのインストール」を参照してください。

App-V パッケージアプリケーションをユーザーに配信するには、次の手順に従います:

1. アプリケーションパッケージをネットワーク共有に保存する。
2. アプリケーションパッケージを Citrix Cloud にアップロードする。
3. デリバリーグループにアプリケーションを追加する。
4. 相互依存する App-V パッケージの自動配信を有効にするには、分離グループを作成します。

Citrix DaaS がシングル管理方式で App-V 動的構成ファイルを認識し、適用できるようにするには、こちらのCitrix ブログを参照してください。

MSIX および MSIX アプリのアタッチアプリケーションの展開と配信

このセクションでは、次の情報について説明します:

- 概要。Citrix DaaS が MSIX および MSIX アプリのアタッチパッケージを配信および管理する方法について説明します。
- 手順。これらのパッケージを展開および配信する手順を提供します。

概要

Citrix DaaS は、VDA マシンにインストールされた Citrix Personalization コンポーネントを介して、MSIX および MSIX アプリのアタッチアプリケーションをユーザーに提供します。このコンポーネントは、ホストマシン上のパッケージのライフサイクルに関するすべての面を管理します。

MSIX および MSIX アプリのアタッチについて詳しくは、Microsoft のドキュメント（それぞれhttps://docs.microsoft.com/en-us/windows/msix/およびhttps://docs.microsoft.com/en-us/azure/virtual-desktop/what-is-app-attach）を参照してください。

手順

MSIX および MSIX アプリのアタッチパッケージの配信をサポートするには、VDA マシンに Citrix Personalization コンポーネントをインストールする必要があります。詳しくは、「VDA マシンへの Citrix Personalization コンポーネントのインストール」を参照してください。

MSIX および MSIX アプリのアタッチパッケージアプリケーションをユーザーに配信するには、次の手順に従います:

1. アプリケーションパッケージをネットワーク共有に保存する。
2. アプリケーションパッケージを Citrix Cloud にアップロードする。
3. デリバリーグループにアプリケーションを追加する。

FlexApp アプリケーションの展開および配信

このセクションでは、次の情報について説明します:

- 概要。Citrix DaaS が FlexApp パッケージを配信および管理する方法について説明します。
- 手順。これらのパッケージを展開および配信する手順を提供します。

概要

Citrix DaaS は、VDA マシンにインストールされた Citrix Personalization コンポーネントおよび FlexApp 配信エージェントを介して、FlexApp アプリケーションをユーザーに提供します。これら 2 つのコンポーネントは、ホストマシン上のパッケージのライフサイクルに関するすべての面を管理します。

手順

FlexApp アプリケーションの配信をサポートするには、VDA マシンに次のコンポーネントをインストールする必要があります:

- VDA マシンへの Citrix Personalization コンポーネントのインストール。詳しくは、「VDA マシンへの Citrix Personalization コンポーネントのインストール」を参照してください。
- VDA への FlexApp エージェントのインストール。詳しくは、「FlexApp エージェントのインストール」を参照してください。

FlexApp パッケージアプリケーションをユーザーに配信するには、次の手順を実行します:

1. アプリケーションパッケージをネットワーク共有に保存する。
2. アプリケーションパッケージを Citrix Cloud にアップロードする。
3. デリバリーグループにアプリケーションを追加する。

VDA マシンへの Citrix Personalization コンポーネントのインストール

Citrix Personalization コンポーネントは、App-V、MSIX、MSIX アプリのアタッチ、および FlexApp 形式のアプリケーションパッケージの公開プロセスを管理します。VDA をインストールする場合、このコンポーネントはデフォルトではインストールされません。VDA のインストール中またはインストール後にコンポーネントをインストールできます。

VDA のインストール中にコンポーネントをインストールするには、次のいずれかの方法を使用します:

- インストールウィザードで、［追加コンポーネント］ページに移動してから、［**Citrix Personalization for App-V - VDA**］チェックボックスをオンにします。
- コマンドラインインターフェイスの場合は、「**/includeadditional** “**Citrix Personalization for App-V –VDA**”」オプションを使用します。

VDA のインストール後にコンポーネントをインストールするには、次の手順に従います：

1. VDA マシンで、［コントロールパネル］**>**［プログラム］**>**［プログラムと機能］に移動し、［**Citrix Virtual Delivery Agent**］を右クリックして ［変更］を選択します。
2. ウィザードが表示されたら、［追加コンポーネント］ページに移動し、［**Citrix Personalization for App-V - VDA**］チェックボックスをオンにします。

> 注：
>
> Microsoft App-V デスクトップクライアントは、ユーザーデバイス上の App-V パッケージから仮想アプリケーションを実行するコンポーネントです。Windows 10（1607 以降）、Windows Server 2016、および Windows Server 2019 には、この App-V クライアントソフトウェアが既に組み込まれています。VDA マシンでオンにするだけで使用できます。詳しくは、こちらの Microsoft 社のドキュメントを参照してください：https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-enable-the-app-v-desktop-client。

アプリケーションパッケージをネットワーク共有に保存する

インフラストラクチャをセットアップした後、アプリケーションパッケージを生成し、それらを UNC または SMB ネットワーク共有などのネットワークの場所、または Azure ファイル共有に保存します。

詳細な手順は次のとおりです：

1. アプリケーションパッケージを生成します。詳しくは、Microsoft 社のドキュメントを参照してください。
2. アプリケーションパッケージをネットワークの場所に保存します：
   - **App-V** のシングル管理の場合：パッケージとそれに対応する動的構成ファイル（App-V）を UNC または SMB ネットワーク共有、または Azure ファイル共有に保存します。
   - **App-V** のデュアル管理の場合：UNC パスから App-V 管理サーバーにパッケージを公開します。（HTTP URL からの公開はサポートされていません。）
   - **MSIX** または **MSIX** アプリのアタッチの場合：パッケージを UNC または SMB ネットワーク共有、または Azure ファイル共有に保存します。
   - **FlexApp** の場合：パッケージを UNC または SMB ネットワーク共有、または Azure ファイル共有に保存します。
3. VDA にパッケージストレージパスの読み取り権限があることを確認してください：

- AD ドメインの UNC または SMB ネットワーク共有にパッケージを保存する場合は、VDA マシンにストレージパスへの読み取り権限を付与します。これを行うには、マシンの AD アカウントに共有への読み取り権限を明示的に付与するか、その権限を持つ AD グループにアカウントを含めることができます。
- パッケージを Azure ファイル共有に保存する場合は、最初にユーザーアカウントに Azure のストレージパスへの読み取り権限を付与します。次に、そのユーザーアカウントを使用してパッケージストレージパスにアクセスするように VDA マシンで実行される`ctxAppVService`を構成します。手順について詳しくは、以降のセクションを参照してください。

ユーザーログオンアカウントの変更

VDA は`ctxAppVService`を呼び出して、パッケージストレージパスにアクセスします。デフォルトでは、`ctxAppVService`はマシンのローカルシステムアカウントを使用してパッケージストレージパスにアクセスします。この種類のマシン認証は、AD ドメインで機能します。ただし、ユーザーアカウントベースの認証が必要となる AD と Azure AD との統合シナリオでは機能しません。

パッケージを Azure ファイル共有に保存する場合は、`ctxAppVService`のログオンアカウントをパッケージストレージパスへの読み取り権限があるユーザーアカウントに変更します。詳細な手順は次のとおりです:

1. [サービス] を起動し、**ctxAppVService** を右クリックして、[プロパティ] を選択します。
2. [ログオン] タブで、[このアカウント] を選択し、パッケージストレージパスへの読み取り権限があるユーザーアカウントを入力してから、ユーザーのパスワードを 2 回入力します。
3. [**OK**] をクリックします。

アプリケーションパッケージを **Citrix Cloud** にアップロードする

必要に応じてアプリケーションパッケージをネットワークの場所に保存した後、それらを Citrix Cloud にアップロードして配信します。必要に応じて、次のいずれかの方法を使用します:

- 一括アップロード
- 1 つずつアップロード

準備

Citrix DaaS は、VDA マシンを使用して、パッケージ検出用のネットワークの場所への接続をセットアップします。したがって、事前にデリバリーグループを作成し、グループ内の 1 つ以上の VDA が次の要件を満たしていることを確認してください:

- VDA バージョン:
  - App-V パッケージを検出する場合：2203 以降

  - MSIX および MSIX アプリのアタッチパッケージを検出する場合：2209 以降
  - FlexApp パッケージを検出する場合：2311 以降
- Citrix Personalization for App-V コンポーネント：インストール済み
- パッケージの場所での権限：読み取り（手順 2 のアプリケーションパッケージをネットワーク共有に保存するを参照してください。）
- 電源：オン
- 状態：登録済み

必須の役割

デフォルトでは、クラウド管理者またはすべての管理権限を実行できる管理者の役割がある場合は、アプリケーションパッケージを Citrix Cloud にアップロードできます。カスタム役割を作成して、アップロード操作を実行することもできます。次の表に、アプリパッケージの操作に必要な権限を示します。

アクション	必要な権限
パッケージの追加（1 つずつアップロード）	アプリケーション検出セッションの作成
ソースの追加（一括アップロード）	アプリケーション検出プロファイルの作成
パッケージの更新の確認	アプリケーション検出セッションの作成
ソースの削除	アプリケーション検出プロファイルの削除

アプリケーションパッケージの一括アップロード

ネットワークの場所にあるパッケージを Citrix Cloud にアップロードします。アップロードする前に、次のアイテムの準備ができていることを確認してください：

- 「準備」に記載されている要件を満たすデリバリーグループ
- ネットワークの場所のパス

パッケージを一括でアップロードするには、次の手順に従います：

1. ［管理］**>**［完全な構成］の左側ペインで ［アプリパッケージ］を選択します。
2. ［ソース］タブで、［追加］ボタンをクリックします。［ソースの追加］ページが表示されます。
3. ［名前］フィールドに、わかりやすいパッケージソースの名前を入力します。
4. ［デリバリーグループ］フィールドで、［デリバリーグループの選択］をクリックします。次に、「準備」に記載されている要件を満たすデリバリーグループを選択し、［**OK**］をクリックします。
5. ［場所の種類］フィールドで、パッケージの保存場所に基づいて ［**Microsoft App-V** サーバー］または ［ネットワーク共有］を選択し、それに対応する設定を構成します：

- ［**Microsoft App-V** サーバー］を選択した場合は、次の情報を入力します：
  - 管理サーバーの URL。例：`http://appv-server.example.com`
  - 管理サーバー管理者のログイン資格情報。
  - 公開サーバーの URL とポート番号。例：`http://appv-server.example.com:3330`
- ［ネットワーク共有］を選択した場合は、次の情報を指定します：
  - ネットワーク共有の UNC パスを入力します。例：`\\Package-Server\apps\`
  - アップロードするパッケージの種類を選択します。オプションには、App-V、MSIX、MSIX アプリのアタッチ、FlexApp があります。
  - サブフォルダーでパッケージを検索するかどうかを指定します。

6. ［ソースの追加］をクリックします。

   ［ソースの追加］ページが閉じ、新しく追加されたソースがソース一覧に表示されます。Citrix DaaS は、デリバリーグループの VDA を使用してパッケージを Citrix Cloud にアップロードします。アップロードが完了すると、［ステータス］フィールドに「インポート成功」と表示されます。対応するパッケージが ［パッケージ］タブに表示されます。

   > 注：
   >
   > ソースの場所でパッケージの更新を確認して Citrix Cloud にインポートするには、ソース一覧で場所を選択し、［パッケージの更新の確認］をクリックします。

アプリケーションパッケージを **1** つずつアップロード

ネットワーク共有から Citrix Cloud にアプリケーションパッケージをアップロードします。アップロードする前に、次のアイテムの準備ができていることを確認してください：

- 「準備」に記載されている要件を満たすデリバリーグループ
- ネットワークの場所のパス。

パッケージを Citrix Cloud にアップロードするには、次の手順に従います：

1. ［管理］**>**［完全な構成］の左側ペインで ［アプリパッケージ］を選択します。
2. ［パッケージ］タブで、［パッケージの追加］ボタンをクリックします。［パッケージの追加］ページが開きます。
3. ［デリバリーグループ］フィールドで、［デリバリーグループの選択］をクリックします。次に、「準備」に記載されている要件を満たすデリバリーグループを選択し、［**OK**］をクリックします。
4. ［パッケージの完全パス］フィールドに、必要に応じてパスを入力します：
   - 一度に複数のパッケージをアップロードするには、セミコロン（`;`）で区切って完全パスを入力します。例：`\\Package-Server\apps\office365.appv;\\Package-Server\apps\skype.msix;\\Package-Server\apps\slack.vhd`

- ネットワーク共有にあるすべてのパッケージをアップロードするには、ストレージパスを入力します。例：\package-Server\apps\

5. ［パッケージの追加］をクリックします。

   アプリケーションパッケージが ［パッケージ］タブに表示されます。

デリバリーグループへのアプリケーションの追加

アプリケーションパッケージが完全にアップロードされたら、必要に応じてそのアプリケーションを 1 つまたは複数のデリバリーグループに追加します。これらのデリバリーグループに関連付けられているユーザーは、アプリケーションにアクセスできるようになります。

> 注：
>
> - デリバリーグループを通じて、パッケージアプリケーションをシングルセッション VDA およびマルチセッション VDA に配信できます。
> - デフォルトでは、エンドユーザーは、シングルセッション（またはデスクトップと呼ばれる）VDA に関連付けられたデリバリーグループに割り当てられた、すべてのパッケージアプリケーションにアクセスできます。デスクトップ VDA 上のパッケージアプリケーションの表示を特定のユーザーまたはグループに制限するには、アプリケーションノードに移動し、［アプリケーションプロパティの編集］**>**［表示の制限］を選択して、変更を加えます。

パッケージ内の 1 つまたは複数のアプリケーションを複数のデリバリーグループに追加するには、次の手順に従います：

1. ［管理］**>**［完全な構成］の左側ペインで ［アプリパッケージ］を選択します。
2. ［パッケージ］タブで、必要に応じてパッケージを選択します。
3. 操作バーで、［アプリケーションをデリバリーグループに割り当てる］をクリックします。［アプリケーションをデリバリーグループに割り当てる］ページが表示されます。
4. 必要に応じてパッケージ内の 1 つまたは複数のアプリケーションを選択し、［次へ］をクリックします。
5. デリバリーグループ一覧で、アプリケーションを割り当てるグループを選択し、［次へ］をクリックします。

   > 注：
   >
   > - *MSIX* または *MSIX* アプリのアタッチパッケージを選択した場合、機能レベルが 2106 以降のデリバリーグループのみが一覧に表示されます。
   > - *FlexApp* パッケージを選択した場合、機能レベルが 2206 以降のデリバリーグループのみが一覧に表示されます。

6. ［完了］をクリックします。

さまざまなパッケージのアプリケーションを複数のデリバリーグループに追加するには、次の手順を実行します：

1. ［管理］**>**［完全な構成］の左側ペインで ［アプリケーション］を選択します。
2. ［アプリケーション］タブで、［アプリケーションの追加］を選択します。
3. ［グループ］ページで、必要に応じて 1 つまたは複数のデリバリーグループを選択します。
4. ［アプリケーション］ページで、次のように 1 つまたは複数のアプリケーションパッケージを選択します:

    a) ［追加］をクリックし、［アプリケーションパッケージ］を選択します。
    b) 必要なパッケージソースの種類（たとえば、App-V のシングル管理）を選択します。この種類のすべてのパッケージが表示されます。
    c) 必要に応じて 1 つまたは複数のパッケージを選択します。
    d) ［**OK**］、［次へ］をクリックします。
    e) 異なる種類のパッケージのアプリケーションをさらに追加するには、手順 a から d を繰り返します。

5. ［完了］をクリックします。

以下を実行する際に、パッケージアプリケーションをデリバリーグループに追加することもできます:

- デリバリーグループを作成する。詳しくは、「デリバリーグループの作成」を参照してください。
- 既存のデリバリーグループまたはアプリケーショングループを編集する。詳しくは、「アプリケーションの追加」を参照してください。

（オプション）App-V パッケージの分離グループの作成

分離グループを作成し、相互依存する App-V パッケージの自動配信を有効にできます。

> 注:
>
> 分離グループは、App-V のシングル管理方式でサポートされています。App-V のデュアル管理方式を使用している場合は、Microsoft App-V インフラストラクチャで接続グループを作成することで同じ目的を達成できます。詳しくは、こちらの Microsoft 社のドキュメントを参照してください: https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-connection-group-file。

分離グループについて

分離グループは、仮想環境を作成するために同じ Windows サンドボックスで実行する必要がある相互依存するアプリケーションパッケージのコレクションです。Citrix App-V 分離グループは、App-V 接続グループと似ていますが同じではありません。分離グループには、次の 2 種類のパッケージが含まれます:

- **Explicit**（明示的な）アプリケーションパッケージ。特定のライセンス要件があるアプリケーション。これらのアプリケーションをデリバリーグループに追加することで、これらのアプリケーションを特定の範囲のユーザーに制限できます。
- **Automatic**（自動）アプリケーションパッケージ。デリバリーグループに追加されているかどうかに関係なく、すべてのユーザーが常に使用できるアプリケーション。

たとえば、アプリケーションapp-aを実行するには JRE 1.7 が必要です。app-a（「*Explicit*」とマークされている）と JRE 1.7（「*Automatic*」とマークされている）を含む分離グループを作成できます。次に、app-aの App-V パッケージを 1 つまたは複数のデリバリーグループに追加します。ユーザーが app-a を実行すると、JRE 1.7 が自動的に app-a で展開されます。

ユーザーが分離グループで *Explicit* とマークされた App-V アプリケーションを起動すると、Citrix DaaS はデリバリーグループ内のアプリケーションへのユーザーのアクセス権限を確認します。ユーザーがそのアプリケーションにアクセスする権限を持っている場合、ユーザーは同じ分離グループ内のすべての *Automatic* アプリケーションパッケージを使用できます。

Automatic パッケージをデリバリーグループに追加する必要はありません。分離グループに別の *Explicit* アプリケーションパッケージがある場合、そのパッケージは、同じデリバリーグループにある場合にのみユーザーが使用できます。

分離されたグループについて詳しくは、こちらのCitrix ブログを参照してください。

App-V 分離グループの作成　分離グループを作成し、相互依存するアプリケーションパッケージを追加します。詳細な手順は次のとおりです：

1. ［分離グループ］タブで、［分離グループの追加］をクリックします。
2. 分離グループの名前と説明を入力します。Citrix Cloud のすべてのアプリケーションパッケージが ［使用可能なパッケージ］一覧に表示されます。
3. ［使用可能なパッケージ］一覧から、必要に応じたアプリケーションを選択し、右矢印をクリックします。選択したアプリケーションが ［分離グループ内のパッケージ］一覧に表示されます。
4. ［展開］フィールドで、そのアプリケーションに対して **Explicit**（明示的）または **Automatic**（自動）を選択します。
5. 手順 2～3 を繰り返して、さらにパッケージを追加します。
6. 一覧のパッケージの順序を変更するには、上矢印または下矢印をクリックします。
7. ［**Save**］をクリックします。

> 注：
>
> 分離グループの構成により、VDA 上に App-V 接続グループが作成されます。展開シナリオは複雑になる可能性があり、App-V クライアントは、1 つのアクティブな接続グループに同時に存在するパッケージをサポートします。同じデリバリーグループに追加された 2 つの異なる分離グループに、同じパッケージを追加しないことをお勧めします。

Autoscale

March 5, 2024

Autoscale は、プロアクティブにマシンの電源を管理するための、一貫した、高性能なソリューションを提供します。その目的は、コストとユーザーエクスペリエンスのバランスを取ることです。Autoscale により、Smart Scale テクノロジ（廃止）が ［管理］コンソールの電源管理ソリューションに組み込まれます。

Autoscale によって、デリバリーグループに登録されているすべてのシングルセッションおよびマルチセッション OS マシンの電源をプロアクティブに管理できます。

Autoscale 機能には、次が含まれます:

- スケジュールベースおよび負荷ベースの設定
- 動的セッションタイムアウト
- タグ付きマシンのオートスケール（クラウドバースト）
- マシンの動的なプロビジョニング
- ユーザーログオフ通知

サポートされる **VDA** ホストプラットフォーム

Autoscale は、Citrix DaaS がサポートするすべてのプラットフォームをサポートします。これには XenServer（旧称 Citrix Hypervisor）、Amazon Web Services、Google Cloud Platform、Microsoft Azure Resource Manager、VMware vSphere など、さまざまなインフラストラクチャプラットフォームが含まれます。サポート対象のプラットフォームの一覧については、Citrix DaaS の「システム要件」を参照してください。

サポートされるワークロード

Autoscale は、マルチセッション OS とシングルセッション OS の両方のデリバリーグループをサポートしています。考慮するユーザーインターフェイスは 3 種類です:

- マルチセッション OS のデリバリーグループ（旧 RDS デリバリーグループ）の Autoscale ユーザーインターフェイス
- シングルセッション OS のランダム（プールされた）デリバリーグループ（旧プールされた VDI デリバリーグループ）の Autoscale ユーザーインターフェイス
- シングルセッション OS の静的デリバリーグループ（旧静的 VDI デリバリーグループ）の Autoscale ユーザーインターフェイス

さまざまなデリバリーグループのユーザーインターフェイスについて詳しくは、「Autoscale ユーザーインターフェイス」を参照してください。

メリット

Autoscale 機能には次の長所があります:

- デリバリーグループ内のマシンの電源を管理するための、単一の一貫したメカニズムを提供します。
- 負荷ベース、スケジュールベース、またはその両方を組み合わせた電源管理によって、可用性とコストの管理を可能にします。
- コスト削減や処理能力の利用状況などのメトリックを監視し、通知を有効にするには、［監視］タブの［Director］を使用します。

ビデオツアー（2 分間）

次のビデオでは、Autoscale を簡単に紹介するクイックツアーを提供しています。

これは埋め込みビデオです。リンクをクリックしてビデオを見る

Autoscale の利用開始

October 30, 2023

Autoscale はデリバリーグループレベルで機能します。設定したスケジュールに基づいて、デリバリーグループ内のマシンの電源をプロアクティブに管理します。

Autoscale はすべての種類のデリバリーグループに適用されます：

- シングルセッションの静的 OS
- シングルセッションランダム OS
- マルチセッションランダム OS

この記事では、Autoscale 関連の基本的な概念について説明し、デリバリーグループの Autoscale を有効にして構成する方法について説明します。

基本的な概念

始める前に、以下の Autoscale の基本的な概念について説明します：

- スケジュール
- 処理能力バッファ
- 負荷インデックス

スケジュール

Autoscale は、設定したスケジュールに基づいて、デリバリーグループのマシンの電源をオンまたはオフにします。

スケジュールには、ピーク時とオフピーク時の動作が定義された、時間枠ごとのアクティブなマシンの数などの情報が含まれます。

スケジュール設定は、デリバリーグループの種類によって異なります。詳しくは、次のトピックを参照してください:

- マルチセッション OS のデリバリーグループ
- シングルセッション OS のランダムデリバリーグループ
- シングルセッション OS の静的デリバリーグループ

処理能力バッファ

処理能力バッファは、動的な負荷の増加を考慮し、現在の需要に応じて予備の処理能力を追加するために使用されます。次の 2 つのシナリオに注意する必要があります:

- マルチセッション OS のデリバリーグループの場合、処理能力バッファは、負荷インデックスを基準としたデリバリーグループの合計処理能力のパーセンテージで定義されます。
- シングルセッション OS のデリバリーグループの場合、処理能力バッファは、デリバリーグループ内のマシンの総数に対するパーセンテージで定義されます。

負荷インデックス

> 重要:
>
> 負荷インデックスは、マルチセッションのデリバリーグループにのみ適用されます。

負荷インデックスのメトリックで、マシンがユーザーのログオン要求を受け入れる可能性を判断します。負荷インデックスの値は、同時ログオン、セッション、CPU、ディスク、メモリの使用が構成された **Citrix** 負荷管理ポリシー設定で算出されます。

負荷インデックスの範囲は、0～10,000 です。デフォルトでは、マシンは 250 のセッションをホストしている時に負荷限界であると見なされます:

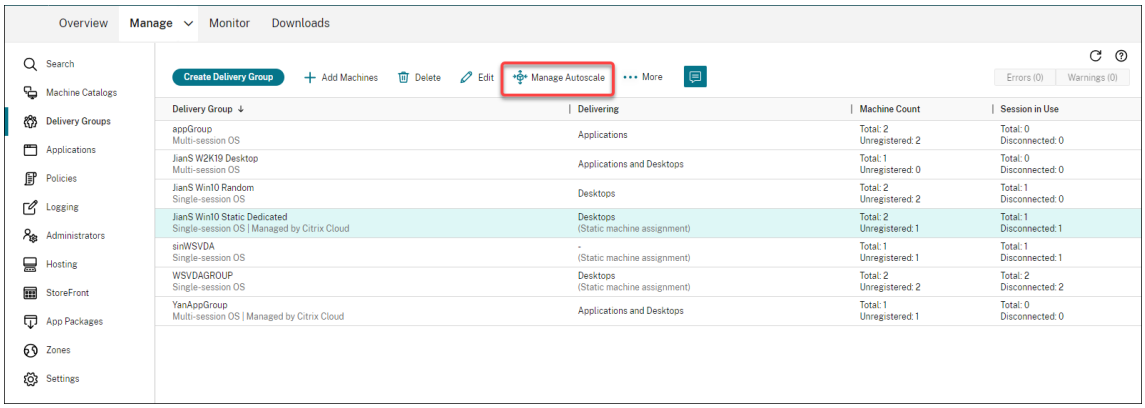
- 値が「0」であれば、マシンは負荷から解放されています。負荷インデックス値が「0」のマシンは基準の負荷状態です。
- 値が「10,000」であれば、これ以上セッションを実行できない、負荷が最大状態のマシンです。

デリバリーグループの **Autoscale** の有効化

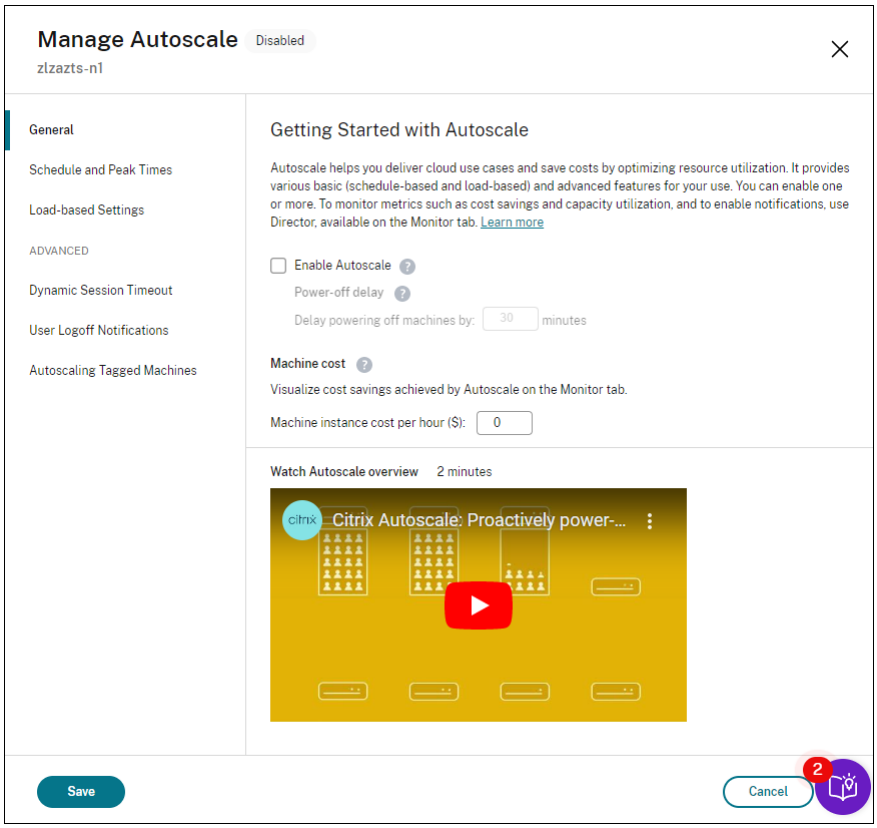
デリバリーグループを作成すると、デフォルトでは Autoscale が無効になります。[完全な構成] インターフェイスを使用してデリバリーグループの Autoscale を有効にして構成するには、次の手順に従います:

PowerShell コマンドを使用して、デリバリーグループの Autoscale を有効にして構成することもできます。詳しくは、「Broker PowerShell SDK コマンド」を参照してください。

1. ［管理］**>**［完全な構成］の左側ペインで ［デリバリーグループ］を選択します。
2. 管理するデリバリーグループを選択し、［**Autoscale** の管理］をクリックします。



3. ［**Autoscale** の管理］ページで ［**Autoscale** を有効にする］チェックボックスをオンにして Autoscale を有効にします。Autoscale を有効にすると、ページ上のオプションが有効になります。



4. 組織のニーズに合わせてデフォルト設定を変更するには、次のように設定します：
   - スケジュールの設定
   - より効率的に非アクティブなマシンの電源をオフにするには、動的セッションタイムアウトとユーザーログオフ通知を使用します。

- デリバリーグループ内のマシンのサブセットの電源管理を行う場合は、タグ付けされたマシンのAutoscaleを使用します。

Autoscale を無効にするには、[**Autoscale**] チェックボックスをオフにします。ページのオプションが灰色表示になり、選択したデリバリーグループに対して Autoscale が無効になっていることを示します。

> 重要:
>
> - Autoscale を無効にすると、Autoscale によって管理されているすべてのマシンは、無効になった時点の状態のままになります。
> - Autoscale を無効にした後、ドレイン状態にあるマシンはドレイン状態が解除されます。ドレイン状態について詳しくは、「ドレイン状態」を参照してください。

PowerShell スクリプトを使用して、グループのマシンを動的にプロビジョニングできます。詳しくは、「マシンの動的なプロビジョニング」を参照してください。

メトリックの監視

デリバリーグループの Autoscale を有効にすると、[監視] タブで Autoscale 管理対象マシンの以下のメトリックを監視できます。

- マシンの使用量
- 見積もり削減額
- マシンとセッションのアラート通知
- マシンの状態
- 負荷評価傾向

> 注:
>
> 最初にデリバリーグループの Autoscale を有効にすると、そのデリバリーグループの監視データを表示するのに数分かかることがあります。
> デリバリーグループの Autoscale が有効から無効になっても、監視データは引き続き利用できます。Autoscale は、5 分間隔で監視データを収集します。

メトリックについて詳しくは、「Autoscale 管理対象マシンの監視」を参照してください。

ヒント

Autoscale はデリバリーグループレベルで機能します。そのため、デリバリーグループごとに構成され、選択したデリバリーグループ内のマシンのみを電源管理します。

処理能力とマシン登録

Autoscale では、容量（処理能力）の決定時に、サイトに登録されているマシンのみを扱います。電源がオンになった未登録のマシンは、セッション要求を受け入れることができません。結果として、これらのマシンはデリバリーグループの総合的な処理能力に含まれません。

複数のマシンカタログにわたるスケーリング

一部のサイトでは、複数のマシンカタログが単一のデリバリーグループに関連付けられている場合があります。Autoscale は、スケジュールまたはセッション需要の要件を満たすために、各カタログからランダムにマシンの電源をオンにします。

たとえば、デリバリーグループに 2 つのマシンカタログがあるとします。カタログ A には電源がオンになった 3 台のマシンがあり、カタログ B には電源がオンになった 1 台のマシンがあります。Autoscale が追加のマシンの電源をオンにする必要がある場合は、カタログ A またはカタログ B のいずれかからマシンの電源をオンにします。

マシンのプロビジョニングとセッション需要

デリバリーグループに関連付けられているマシンカタログには、需要の増減に応じて電源をオンまたはオフするために十分な数のマシンが必要です。セッション需要がデリバリーグループ内の登録済みマシンの総数を超えても、Autoscale はすべての登録済みマシンの電源がオンになっていることを確認します。しかし、**Autoscale** が追加のマシンをプロビジョニングすることはありません。

このボトルネックを解消するために、PowerShell スクリプトを使用してマシンを作成し動的にそれらを削除できます。詳しくは、「マシンの動的プロビジョニング」を参照してください。

インスタンスサイズの考慮事項

パブリッククラウドでインスタンスのサイズを適切に設定することで、コストを最適化できます。ワークロードのパフォーマンスと処理能力に関する要件を満たす限り、小さいインスタンスをプロビジョニングすることをお勧めします。

小さいインスタンスは、大きいインスタンスよりも少ないユーザーセッションをホストします。そのため、最後のユーザーセッションがログオフされるまでの時間が短いので、Autoscale はマシンをいち早くドレイン状態にします。つまり、Autoscale は小さいインスタンスの電源をすぐにオフにするので、コストを削減できます。

ドレイン状態

Autoscale は、デリバリーグループ内の電源がオンになっているマシンの数を、構成されたプールサイズおよび処理能力バッファにまでスケールダウンしようとします。

この目標を達成するために、Autoscale は、セッションの数が最も少ない余分なマシンを「ドレイン状態」にし、すべてのセッションがログオフしたときにそれらの電源をオフにします。この動作は、セッション需要が減少し、スケジュールに必要なマシンの数が電源オンになったマシンよりも少なくなる場合に発生します。

Autoscale は、余分なマシンを 1 台ずつ「ドレイン状態」にします:

- 2 台以上のマシンに同数のアクティブなセッションがある場合、Autoscale は指定された電源オフの遅延期間中電源がオンになっているマシンをドレイン状態にします。

  これによって、最近電源がオンになった、セッション数が少ない可能性が高いマシンをドレイン状態にすることを回避します。

- 指定された電源オフの遅延期間中複数のマシンの電源がオンになっている場合、Autoscale はそれらのマシンを 1 台ずつランダムにドレイン状態にします。

ドレイン状態のマシンは、新しいセッションの開始をホストしなくなり、既存のセッションがログオフされるまで待機します。すべてのセッションがログオフされた場合にのみ、マシンはシャットダウンの候補になります。ただし、セッション起動時にすぐに使用できるマシンがない場合、Autoscale は、新しくマシンの電源をオンにするのではなく、ドレイン状態のマシンでセッションを起動することを優先します。

次のいずれかの条件が満たされると、マシンの状態がドレイン状態以外に変更されます:

- マシンの電源がオフになる。
- マシンが属するデリバリーグループの Autoscale が無効化される。
- Autoscale により、必要なスケジュールまたは負荷の需要の要件を満たすためにマシンが使用される。これは、スケジュール（スケジュールベースのスケール）または現在の需要（負荷ベースのスケール）で、この時点で電源がオンになっているマシンより多くのマシンが必要な場合に発生します。

> 重要:
>
> セッション起動用にすぐに使用できるマシンがない場合、Autoscale は、新しくマシンの電源をオンにするのではなく、ドレイン状態のマシンでセッションを起動することを優先します。セッション起動をホストするドレイン状態のマシンは、ドレイン状態を維持します。

どのマシンがドレイン状態にあるかを調べるには、PowerShell コマンドの`Get-BrokerMachine`を使用します。例: `Get-BrokerMachine -DrainingUntilShutdown $true`。または、［管理］コンソールを使用できます。「ドレイン状態のマシンの表示」を参照してください。

ドレイン状態のマシンの表示

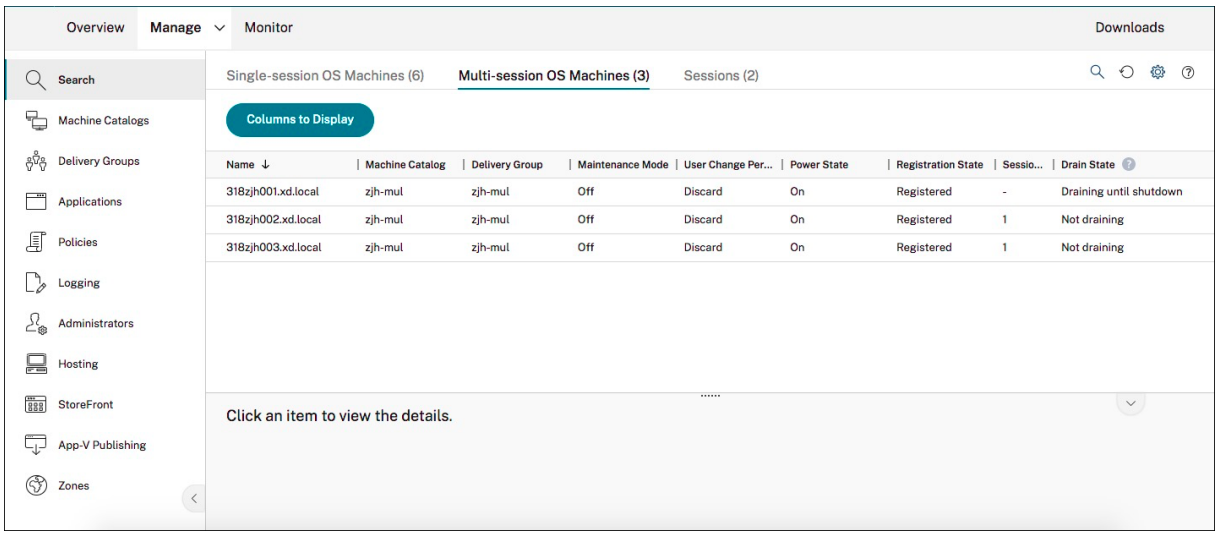
> 注:
>
> この機能は、マルチセッションマシンのみに適用されます。

［管理］**>**［完全な構成］では、ドレイン状態のマシンを表示して、まもなくシャットダウンされるマシンを確認できます。次の手順を実行します:

1. ［検索］ノードに移動し、［表示する列］をクリックします。
2. ［表示する列］ウィンドウで、［ドレイン状態］の横にあるチェックボックスをオンにします。
3. ［保存］をクリックして、［表示する列］ウィンドウを閉じます。

［ドレイン状態］列には、次の情報を表示できます：

- シャットダウンまでドレインを実行中。マシンがシャットダウンされるまでドレイン状態のときに表示されます。
- ドレインは実行されていません。マシンがまだドレイン状態でないときに表示されます。



追加情報

Autoscale について詳しくは、Tech Zone の「Citrix Autoscale」を参照してください。

スケジュールベースおよび負荷ベースの設定

October 30, 2023

Autoscale によるマシンの電源管理方法

Autoscale は、選択したスケジュールに基づいてマシンの電源をオンまたはオフにします。Autoscale では、特定の曜日を含む複数のスケジュールを設定し、その期間中利用可能なマシンの数を調整できます。特定の日の特定の時間に特定のユーザーグループがマシンリソースを消費すると予想される場合は、その間のエクスペリエンスを最適化できます。それらのマシンで実行中のセッションがあるかどうかにかかわらず、スケジュール中にマシンの電源がオンになることに注意してください。

> 注:
>
> Autoscale は、すべての電力管理マシンをサポートします。

これはデリバリーグループのタイムゾーンに基づいたスケジュールです。タイムゾーンを変更するには、デリバリーグループのユーザー設定を変更します。詳しくは、「デリバリーグループの管理」を参照してください。

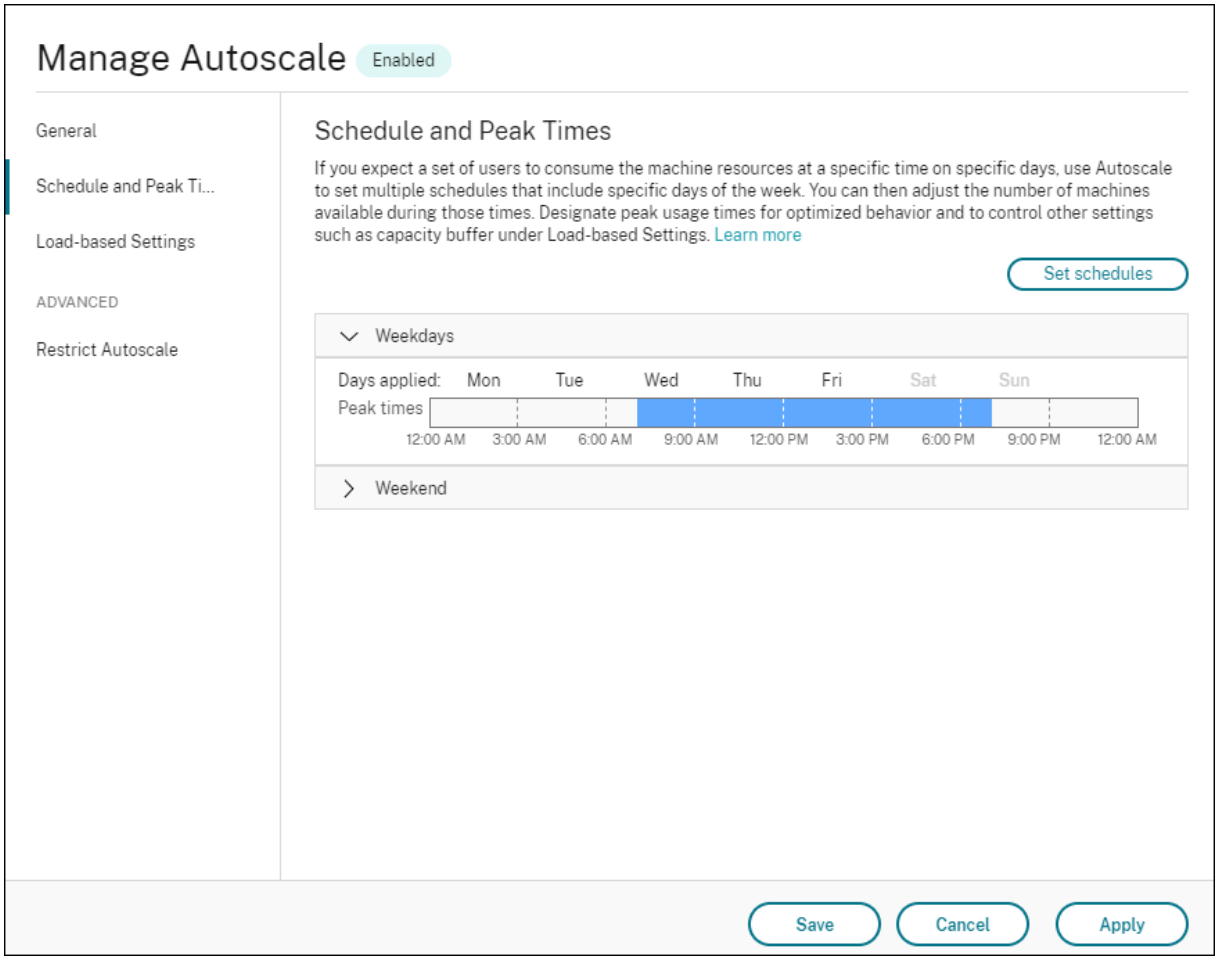
Autoscale には次の 2 種類のデフォルトのスケジュールがあります: 平日（月曜日から金曜日まで）と週末（土曜日と日曜日）。デフォルトでは、平日のスケジュールでは、ピーク時の午前 7 時から午後 6 時 30 分までの間、1 台のマシンの電源が投入され、オフピーク時には稼働しません。デフォルトの処理能力バッファは、ピーク時とオフピーク時には 10% に設定されます。デフォルトでは、週末のスケジュールでは、マシンの電源はオンになりません。

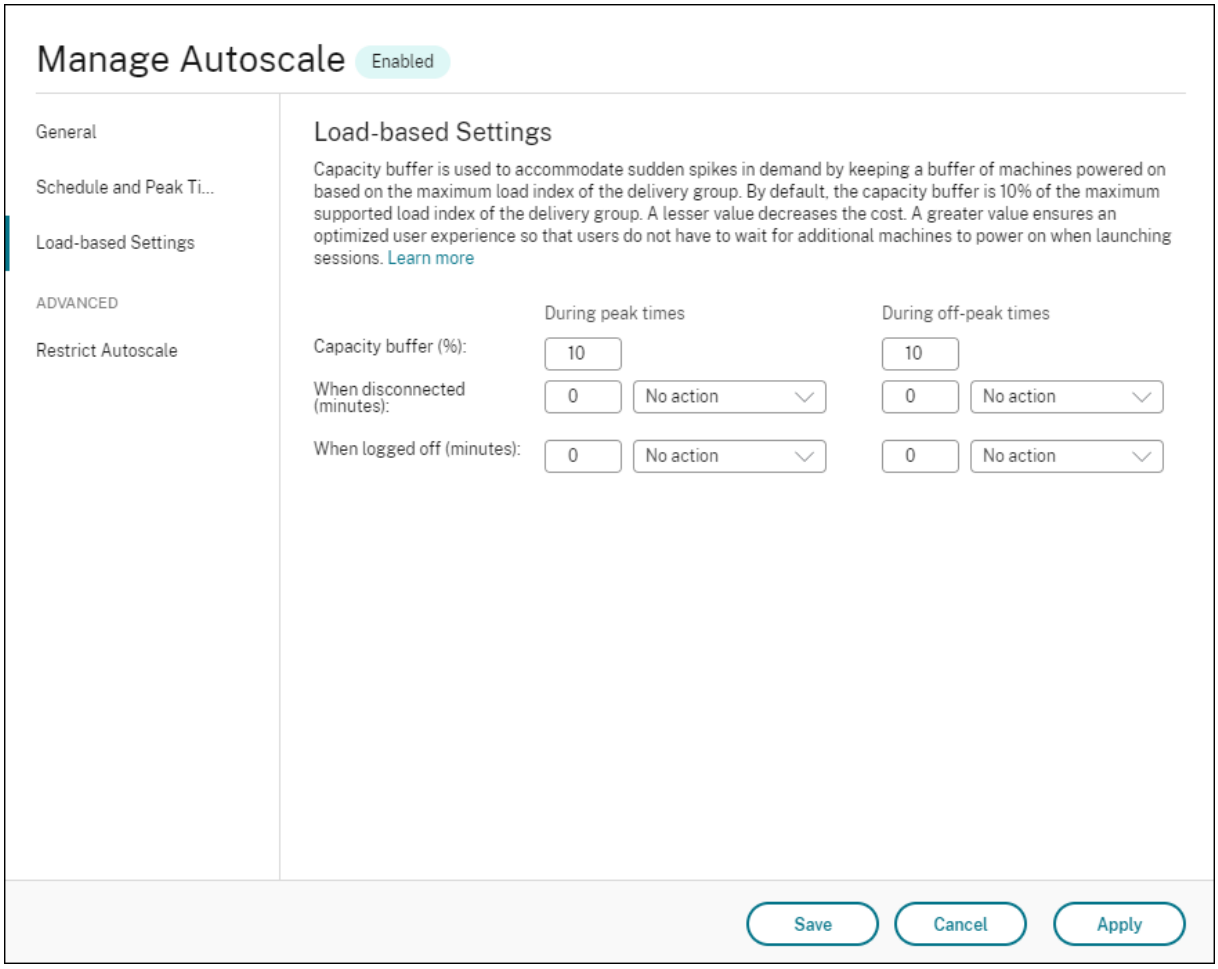
> 注:
>
> Autoscale は、サイトに登録されているマシンのみを、使用可能な処理能力の一部として計算します。「登録されている」とは、そのマシンが使用可能であるか、既に使用中であることを意味します。これによって、ユーザーセッションを実行できるマシンのみがデリバリーグループの処理能力として見なされるようになります。

ユーザーインターフェイス

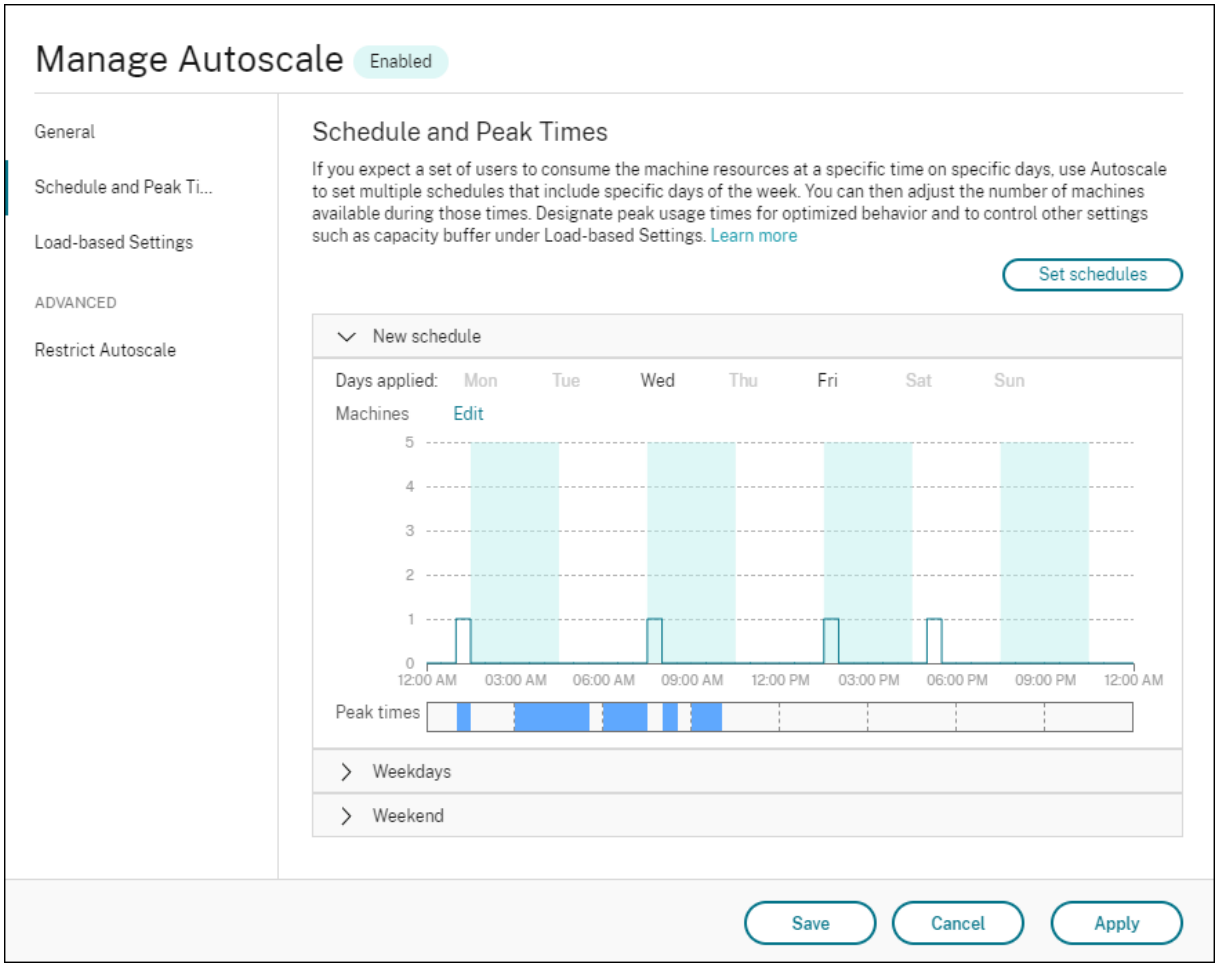
考慮するユーザーインターフェイスは 3 種類です。

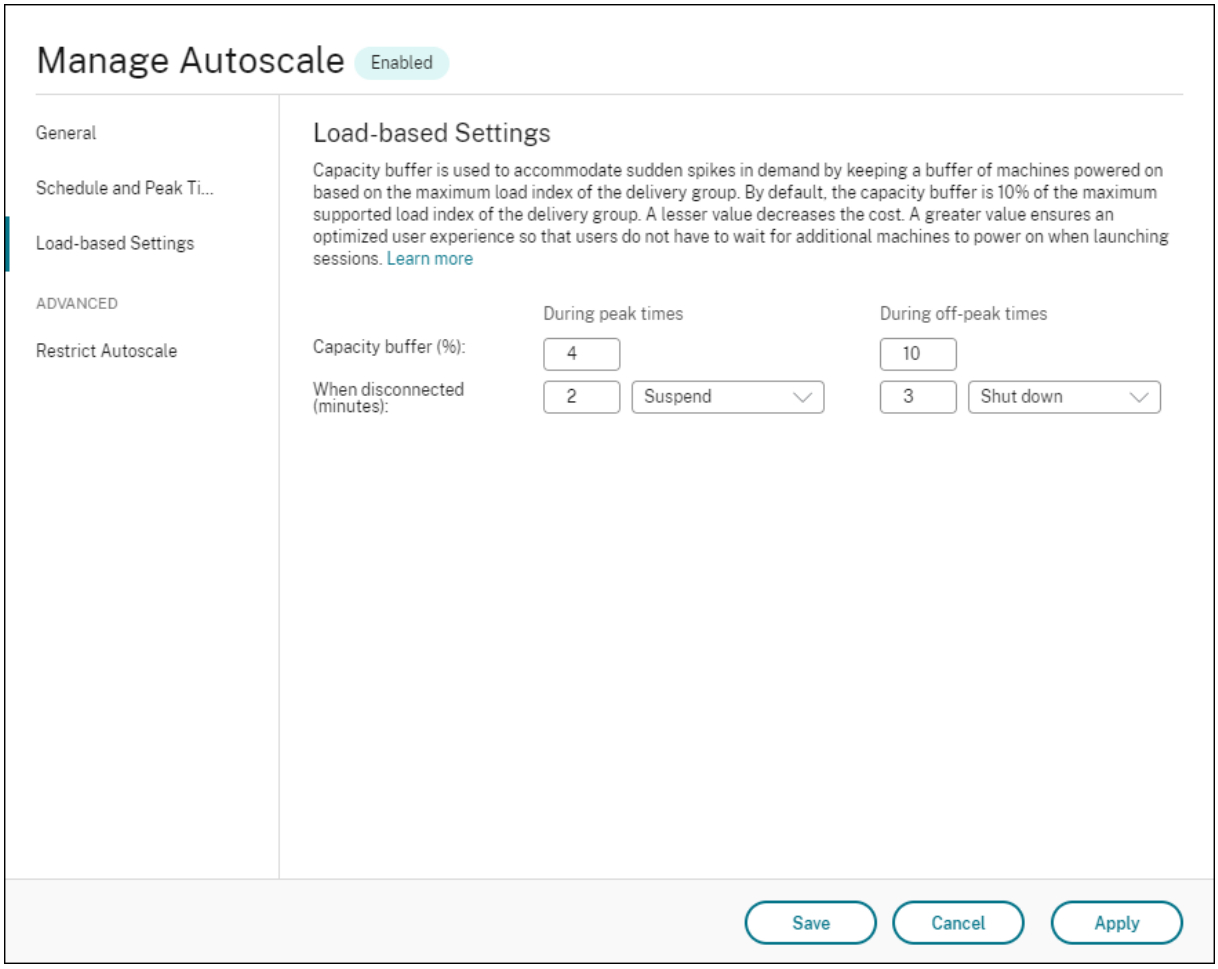
シングルセッション *OS* の静的デリバリーグループのユーザーインターフェイス:



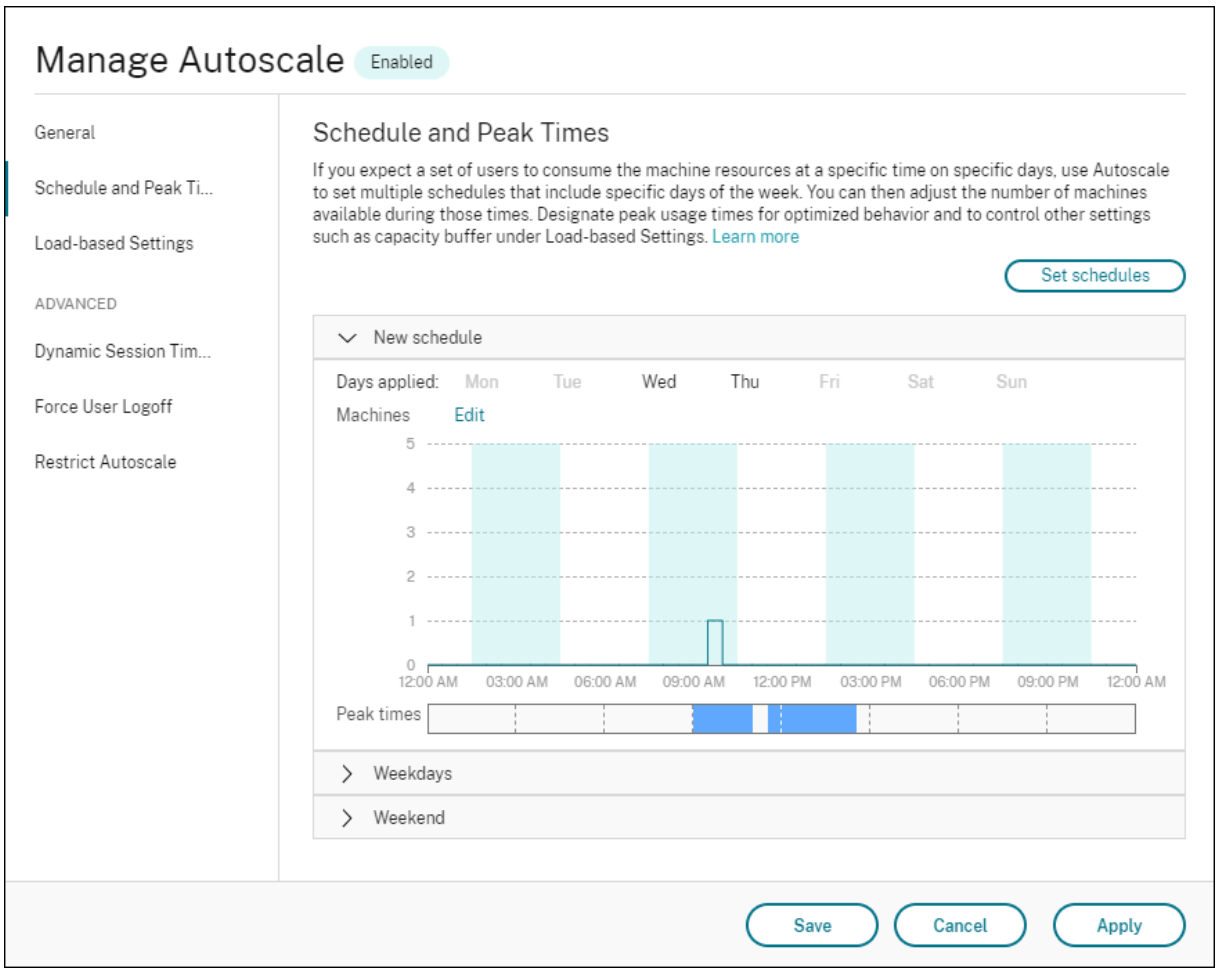


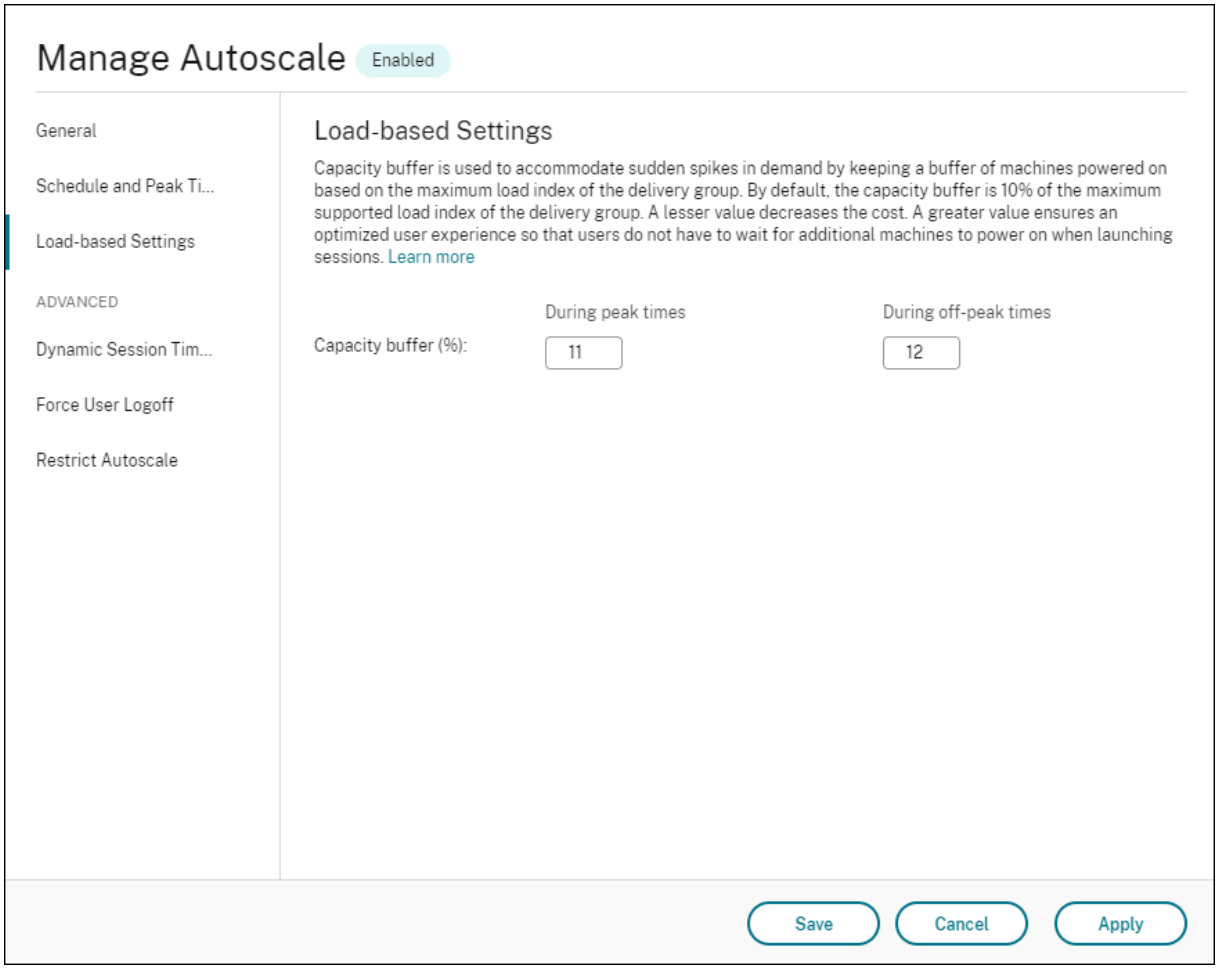
シングルセッション *OS* のランダムデリバリーグループの Autoscale ユーザーインターフェイス:





マルチセッション *OS* デリバリーグループの Autoscale ユーザーインターフェイス:





スケジュールベースの設定

Autoscale スケジュール。スケジュールを追加、編集、選択、削除できます。

適用する曜日。選択したスケジュールに適用した曜日を強調表示します。残りの曜日は灰色表示されます。

編集。1 時間ごとまたは 30 分ごとにマシンを割り当てることができます。数字またはパーセンテージでマシンを割り当てることができます。

> 注:
>
> - このオプションは、マルチセッション OS およびシングルセッション OS のランダムデリバリーグループの Autoscale ユーザーインターフェイスでのみ使用可能です。
> - ［編集］の横のヒストグラムは、異なる時間枠で実行中のマシンの数またはパーセンテージを表示します。
> - ［ピーク時］の上の ［編集］をクリックすると、時間枠ごとにマシンを割り当てることができます。［起動するマシン］ウィンドウのメニューで選択したオプションによって、マシンを数字またはパーセンテージで割り当てることができます。
> - マルチセッション OS のデリバリーグループの場合、実行するマシンの最小数を 1 日あたり 30 分単位で

> 個別に設定できます。シングルセッション OS のランダムデリバリーグループの場合、実行するマシンの最小数を 1 日あたり 60 分単位で個別に設定できます。

独自にスケジュールを定義するには、以下の手順を実行します:

1. [**Autoscale** の管理] ウィンドウの [スケジュールとピーク時] ページで、[スケジュールの設定] をクリックします。
2. [**Autoscale** スケジュールの編集] ウィンドウで、各スケジュールに適用する日付を選択します。必要に応じてスケジュールを削除することもできます。
3. [完了] をクリックしてスケジュールを保存し、[スケジュールとピーク時] ページに戻ります。
4. 該当するスケジュールを選択し、必要に応じて構成します。
5. [適用] をクリックして [**Autoscale** の管理] ウィンドウを終了するか、他のページで設定を構成します。

> 重要:
>
> - Autoscale では、同じ日を異なるスケジュールで上書きすることはできません。たとえば、schedule1 で月曜日を選択した後に schedule2 で月曜日を選択すると、schedule1 で自動的に月曜日が消去されます。
> - スケジュール名では大文字と小文字が区別されません。
> - スケジュール名は空白にしたり、スペースだけを含めたりすることはできません。
> - Autoscale では、文字間にスペースを入れることができます。
> - スケジュール名に次の文字は使用できません: \ / ; : # . * ? = < > | [ ] ( ) { } “ “。
> - Autoscale では、重複したスケジュール名は使用できません。スケジュールごとに異なる名前を入力してください。
> - Autoscale では、空のスケジュールはサポートしていません。つまり、選択した日のないスケジュールは保存されません。
>
> 注:
>
> 選択したスケジュールに含まれている日が強調表示され、含まれていない日は灰色表示になります。

負荷ベースの設定

ピーク時。選択したスケジュールに適用した曜日のピーク時間を定義できます。このためには、横棒グラフを右クリックします。ピーク時間を定義すると、残りの未定義の時間はデフォルトでオフピーク時間に設定されます。デフォルトでは、午前 7 時から午後 7 時の時間枠が選択したスケジュールの曜日のピーク時間として定義されます。

> 重要:
>
> - マルチセッション OS のデリバリーグループの場合、ピーク時の棒グラフが処理能力バッファに使用されます。
> - シングルセッション OS のデリバリーグループの場合、ピーク時の棒グラフが処理能力バッファに使用さ

> れ、ログオフや切断後にトリガーされるアクションを制御します。
> - マルチセッション OS とシングルセッション OS のデリバリーグループの両方について、スケジュールに含まれる日のピーク時間を 30 分の詳細レベルで定義できます。または、代わりに`New-BrokerPowerTimeScheme PowerShell`コマンドを使用できます。詳しくは、「Broker PowerShell SDK コマンド」を参照してください。

処理能力バッファ。電源がオンになっているマシンのバッファを維持できます。値が小さいほどコストが低くなります。値を大きくするとユーザーエクスペリエンスが確実に最適化されるため、セッションを起動する時に追加のマシンの電源がオンになるまで待機する必要がありません。デフォルトでは、処理能力バッファはピーク時およびオフピーク時の 10% です。処理能力バッファを 0（ゼロ）に設定した場合、セッションを起動する時に追加のマシンの電源がオンになるまで待機が必要な場合もあります。Autoscale では、ピーク時とオフピーク時で個別に処理能力バッファを指定できます。

その他の設定

> ヒント：
>
> - Broker PowerShell SDK を使用して、その他の設定を構成することを選択できます。詳しくは、「Broker PowerShell SDK コマンド」を参照してください。
> - 切断時およびログオフ時の設定に関連する SDK コマンドを理解するには、https://citrix.github.io/delivery-controller-sdk/Broker/about_Broker_PowerManagement/#power-policyを参照してください。

切断時。セッションが切断されてから一時停止またはシャットダウンされるまで、切断されロックされたマシンの電源をオンにしておく時間を指定できます。指定した切断時間が経過すると、構成したアクションに応じて、マシンは一時停止またはシャットダウンします。デフォルトでは、切断されたマシンにアクションは割り当てられていません。ピーク時とオフピーク時で個別にアクションを定義できます。このためには、下向き矢印をクリックして、メニューから次のいずれかのオプションを選択します：

- 何もしない。これを選択すると、セッション切断後のマシンの電源はオンのままになります。Autoscale は何もしません。
- 一時停止。これを選択すると、指定された切断時間が経過したときに Autoscale がマシンをシャットダウンせずに一時停止します。［一時停止］を選択すると、以下のオプションが使用できます。
  - 再接続がない場合（分）。一時停止したマシンは、切断されたユーザーが再接続すると引き続き使用できますが、新しいユーザーは使用できません。マシンを再び使用可能にしてすべてのワークロードを処理できるようにするには、マシンをシャットダウンします。Autoscale がマシンをシャットダウンするまでのタイムアウト時間を分単位で指定します。
- シャットダウン。これを選択すると、指定された切断時間が経過したときに Autoscale がマシンをシャットダウンします。

> 注:
>
> このオプションは、シングルセッション OS のランダムおよび静的デリバリーグループの Autoscale ユーザーインターフェイスでのみ使用可能です。

ログオフ時。セッションのログオフから一時停止またはシャットダウンされるまで、マシンの電源をオンにしておく時間を指定できます。指定したログオフ時間が経過すると、構成したアクションに応じて、マシンは一時停止またはシャットダウンします。デフォルトでは、ログオフしたマシンにアクションは割り当てられていません。ピーク時とオフピーク時で個別にアクションを定義できます。このためには、下向き矢印をクリックして、メニューから次のいずれかのオプションを選択します:

- 何もしない。これを選択すると、セッションログオフ後のマシンの電源はオンのままになります。Autoscale は何もしません。
- 一時停止。これを選択すると、指定されたログオフ時間が経過したときに Autoscale がマシンをシャットダウンせずに一時停止します。
- シャットダウン。これを選択すると、指定されたログオフ時間が経過したときに Autoscale がマシンをシャットダウンします。

> 注:
>
> このオプションは、シングルセッション OS の静的デリバリーグループの Autoscale ユーザーインターフェイスでのみ使用可能です。

セッションが切断された状態で異なる期間に移行するシングルセッション **OS** マシンの電源管理

> 重要:
>
> - この拡張機能は、セッションが切断されたシングルセッション OS マシンにのみ適用されます。ログオフされたセッションがあるシングルセッション OS マシンには適用されません。
> - この機能拡張を有効にするには、該当するデリバリーグループの Autoscale を有効にする必要があります。それ以外の場合、電源ポリシーの切断操作は、期間の移行時にトリガーされません。

以前のリリースでは、アクション（切断アクション =「一時停止」または「シャットダウン」）が必要な期間に移行するシングルセッション OS マシンの電源がオンのままになっていました。このシナリオは、操作（切断アクション =「何もしない」）が不要な期間（ピーク時またはオフピーク時）にマシンが切断された場合に発生しました。

このリリース以降では、指定した切断時間が経過すると、Autoscale はマシンを一時停止または電源をオフにします。これは、その期間に対して構成された切断アクションによって異なります。

たとえば、シングルセッション OS デリバリーグループに対して次の電源ポリシーを構成するとします:

- `PeakDisconnectAction`を「何もしない」に設定
- `OffPeakDisconnectAction`を「シャットダウン」に設定
- 「OffPeakDisconnectTimeout」を「10」に設定

> 注:
>
> 切断アクション電源ポリシーについて詳しくは、「https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policy」および「https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/」を参照してください。

以前のリリースでは、ピーク時にセッションが切断されたシングルセッション OS マシンは、ピークからオフピークに移行しても電源がオンのままでした。このリリース以降、`OffPeakDisconnectAction`および`OffPeakDisconnectTimeout`ポリシーのアクションは、期間移行時にシングルセッション OS マシンに適用されます。その結果、オフピークに移行してから 10 分後にマシンの電源がオフになります。

以前の動作に戻す（つまり、セッションが切断された状態でピークからオフピークまたはオフピークからピークに移行するマシンでは何も実行しない）場合は、次のいずれかの操作を行います:

- 「LegacyPeakTransitionDisconnectedBehaviour」レジストリ値を 1 に設定します（true: 以前の動作を有効にします）。デフォルトでは、値は 0 です（false、期間の移行時に電源ポリシーの切断アクションがトリガーされます）。
  - パス: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer
  - 値の名前: LegacyPeakTransitionDisconnectedBehaviour
  - 種類: REG_DWORD
  - 値のデータ: 0x00000001（1）
- `Set-BrokerServiceConfigurationData` PowerShell コマンドを使用して設定を構成します。例:
  - `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

期間移行時に電源ポリシーアクションを適用するには、マシンが次の条件を満たす必要があります:

- 切断されたセッションがある。
- 保留中の電源操作がない。
- 異なる期間に移行するシングルセッション OS のデリバリーグループに属している。
- 特定の期間（ピーク時またはオフピーク時）に切断し、電源操作が割り当てられている期間に移行するセッションがある。

処理能力バッファについて

処理能力バッファは、動的な負荷の増加を考慮し、現在の需要に応じて予備の処理能力を追加するために使用されます。次の 2 つのシナリオに注意する必要があります:

- マルチセッション OS のデリバリーグループの場合、処理能力バッファは、負荷インデックスを基準としたデリバリーグループの合計処理能力のパーセンテージで定義されます。負荷インデックスについて詳しくは、「負荷インデックス」を参照してください。
- シングルセッション OS のデリバリーグループの場合、処理能力バッファは、コンピューターの数を基準としたデリバリーグループの合計処理能力のパーセンテージで定義されます。

> 注:
>
> Autoscale をタグ付きマシンに制限するシナリオでは、処理能力バッファは、負荷インデックスを基準としたデリバリーグループ内のタグ付きマシンの合計処理能力のパーセンテージとして定義されます。

Autoscale では、ピーク時とオフピーク時で個別に処理能力バッファを指定できます。処理能力バッファフィールドの値を小さくすると、Autoscale がオンにする予備の処理能力が少なくなるため、コストが削減されます。値を大きくするとユーザーエクスペリエンスが確実に最適化されるため、セッションを起動する時に追加のマシンの電源がオンになるまで待機する必要がありません。デフォルトでは、処理能力バッファは 10% です。

> 重要:
>
> 処理能力バッファにより、予備の合計処理能力がデリバリーグループの合計処理能力の「X」パーセントを下回るレベルに低下すると、マシンの電源がオンになります。これによって、必要なパーセンテージの予備の処理能力が確保されます。

マルチセッション **OS** のデリバリーグループ

マシンの電源がオンになる状況

> 重要:
>
> スケジュールが選択されている場合、Autoscale はスケジュールで電源をオンにするよう構成されている、すべてのマシンの電源をオンにします。負荷に関係なく、このスケジュール中、指定された台数のマシンの電源をオンにしたままにします。

デリバリーグループ内の電源がオンになっているマシンの数が負荷インデックス基準で処理能力を確保するためのバッファに一致しなくなると、Autoscale は追加のマシンの電源をオンにします。たとえば、デリバリーグループに 20 台のマシンがあり、スケジュールベースのスケール、20% の処理能力バッファで 3 台のマシンの電源がオンになる予定とします。この場合、負荷がなくなると、最終的に 4 台のマシンの電源がオンになります。これは、バッファとして 4x10,000 の負荷インデックスが必要であり、少なくとも 4 台のマシンの電源をオンにする必要があるためです。こうした事態は、ピーク時、マシンの負荷が増加したとき、新しいセッションの起動時、新しいマシンをデリバリーグループに追加したときに発生する可能性があります。Autoscale は、次の基準を満たすマシンの電源のみをオンにします:

- マシンがメンテナンスモードではない。
- マシンが稼働しているハイパーバイザーがメンテナンスモードになっていない。

- 現在マシンの電源がオフになっている。
- マシンに保留中の電源操作がない。

マシンの電源がオフになる状況

> 重要:
>
> - スケジュールが選択されている場合、Autoscale はスケジュールに従ってマシンの電源をオフにします。
> - このスケジュール中、電源がオンになるよう構成されているマシンの電源はオフにしません。

デリバリーグループの電源がオンになっているマシンの数（処理能力バッファを含める）をサポートするのに十分な数のマシンがある場合、Autoscale は追加のマシンの電源をオフにします。こうした事態は、オフピーク時、マシンの負荷が減少したとき、セッションのログオフ時、そしてマシンをデリバリーグループから削除した時に発生する可能性があります。Autoscale は、次の基準を満たすマシンの電源のみをオフにします:

- マシンとそのマシンが稼働しているハイパーバイザーがメンテナンスモードになっていない。
- 現在マシンの電源がオンになっている。
- マシンが利用可能として登録されている、または起動後、登録を待機している。
- マシンにアクティブなセッションがない。
- マシンに保留中の電源操作がない。
- マシンが指定された電源オフの遅延条件を満たしている。これは、少なくとも「X」分間マシンの電源がオンになっていたことを意味します。「X」は対象のデリバリーグループで指定された電源オフの遅延です。

サンプルシナリオ

次のようなシナリオを想定します:

- デリバリーグループの構成。Autoscale が電源管理するデリバリーグループには 10 台のマシンが含まれています（M1～M10）。
- **Autoscale** の構成
  - 処理能力バッファは 10% に設定します。
  - 選択したスケジュールにマシンが含まれていません。

このシナリオは以下の順序で実行されます:

1. ユーザーはログオンしていません。
2. ユーザーセッションが増加します。
3. 追加のユーザーセッションが開始されます。

4. セッションの終了により、ユーザーセッションの負荷が減少します。
5. ユーザーセッションの負荷は、オンプレミスリソースによってのみ処理されるようになるまで減少し続けます。

上記のシナリオで Autoscale がどのように機能するかについては、以下を参照してください。

- ユーザー負荷なし（初期の状態）
  - 1 台のマシン（例：M1）の電源がオンになっています。マシンの電源がオンになっているのは、処理能力バッファが構成されているためです。この場合、10（マシン数）×10,000（負荷インデックス）×10%（構成された処理能力バッファ）=10,000 です。したがって、1 台のマシンの電源がオンになります。
  - 電源がオンになっているマシン（M1）の負荷インデックス値は基準の負荷（負荷インデックス = 0）です。
- 最初のユーザーがログオンする
  - セッションは、マシン M1 でホストされます。
  - 電源がオンになっているマシン M1 の負荷インデックスが増大し、M1 は基準の負荷を超えます。
  - 処理能力バッファが構成されているため、需要の増大に応じて Autoscale が追加のマシン（M2）の電源をオンにします。
  - マシン M2 の負荷インデックス値は基準の負荷になっています。
- ユーザーが負荷を増やす
  - マシン M1 と M2 の間でセッションの負荷が分散されます。その結果、電源がオンになっているマシン（M1 と M2）の負荷インデックスが増加します。
  - 予備の合計処理能力は、まだ負荷インデックス基準で 10,000 を超えています。
  - マシン M2 の負荷インデックス値は基準の負荷ではなくなります。
- 追加のユーザーセッションが開始される
  - マシン間（マシン M1 と M2）でセッションの負荷が分散されます。その結果、電源がオンになっているマシン（M1 と M2）の負荷インデックスがさらに増加します。
  - 予備の合計処理能力が負荷インデックス基準で 10,000 未満に低下すると、処理能力バッファが構成されているため、需要の増大に応じて Autoscale が追加のマシン（M3）の電源をオンにします。
  - マシン M3 の負荷インデックス値は基準の負荷になっています。
- さらに追加のユーザーセッションが開始される
  - マシン間（マシン M1 から M3 まで）でセッションの負荷が分散されます。その結果、電源がオンになっているマシン（M1 から M3 まで）の負荷インデックスが増加します。
  - 予備の合計処理能力は、負荷インデックス基準で 10,000 を超えています。
  - マシン M3 の負荷インデックス値は基準の負荷ではなくなります。
- セッションの終了によりユーザーセッションの負荷が減少する

  - ユーザーがセッションからログオフした後、またはアイドル状態のセッションがタイムアウトした後、マシン M1 から M3 までの解放された処理能力は、他のユーザーが開始したセッションのホストで再利用されます。
  - 予備の合計処理能力が負荷インデックス基準で 10,000 を超えるレベルに増加すると、Autoscale はいずれかのマシン（例：M3）をドレイン状態にします。その結果、他のユーザーによって開始されたセッションは、新しい変更がない限りはそのマシンに送信されなくなります。たとえば、エンドユーザーの負荷が再び増加したり、他のマシンの負荷が最小になったりした場合です。

- ユーザーセッションの負荷が減少し続ける
  - マシン M3 上のすべてのセッションが終了し、指定された電源オフの遅延でタイムアウトになると、Autoscale はマシン M3 の電源をオフにします。
  - さらにユーザーがセッションからログオフすると、電源がオンになったマシン（M1 と M2）の解放された処理能力は他のユーザーが開始したセッションのホストで再利用されます。
  - 予備の合計処理能力が負荷インデックス基準で 10,000 を超えるレベルに増加すると、Autoscale はいずれかのマシン（例：M2）をドレイン状態にします。その結果、他のユーザーによって開始されたセッションは、そのマシンに送信されなくなります。

- セッションがすべて終了するまで、ユーザーセッションの負荷は減少し続けます。
  - マシン M2 上のすべてのセッションが終了し、指定された電源オフの遅延でタイムアウトになると、Autoscale はマシン M2 の電源をオフにします。
  - 電源がオンになっているマシン（M1）の負荷インデックス値は基準の負荷になっています。処理能力バッファが構成されているため、Autoscale はマシン M1 をドレイン状態にしません。

> 注:
>
> マルチセッション OS のデリバリーグループの場合、ユーザーのセッションログオフ時にデスクトップへの変更はすべて失われます。ただし、ユーザー固有の設定が構成されている場合、ユーザープロファイル設定とともにローミングされます。

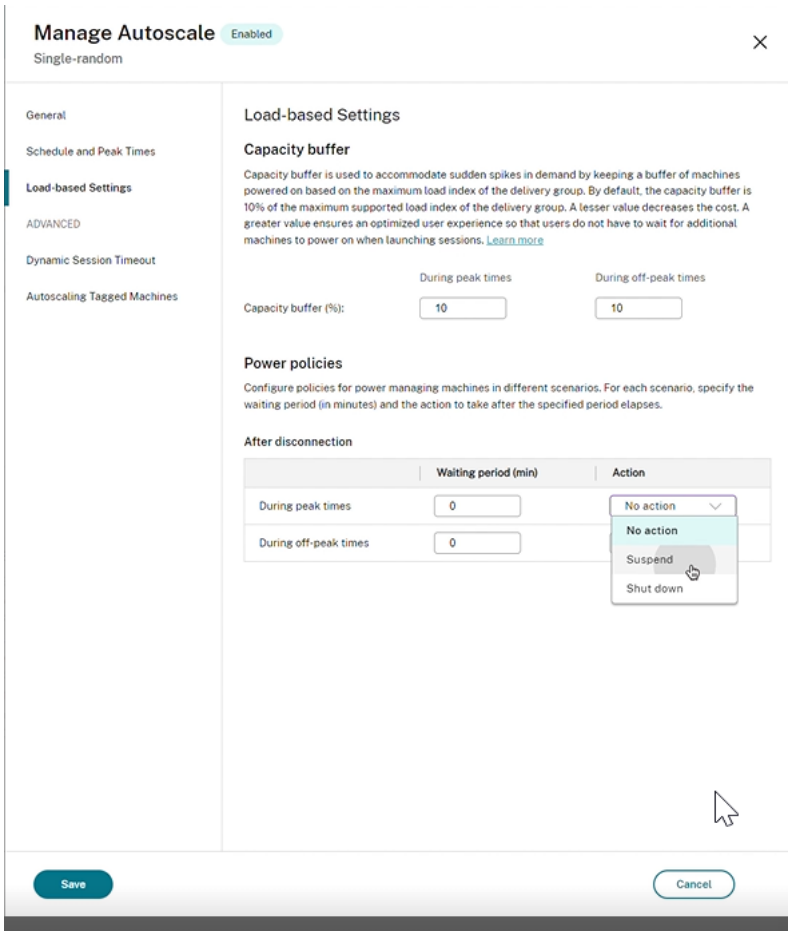
シングルセッション **OS** のランダムデリバリーグループ

処理能力バッファを使用すると、デリバリーグループ内のマシンの総数を基にして電源がオンになっているマシンのバッファを確保することで、需要の急増に対応できます。デフォルトでは、処理能力バッファは、デリバリーグループ内にあるマシンの総数の 10% です。

マシン数（処理能力バッファを含む）が現在電源がオンになっているマシンの総数を上回っている場合、需要に対応して追加のマシンの電源がオンになります。マシン数（処理能力バッファを含む）が現在電源がオンになっているマシンの総数を下回っている場合、構成されたアクションに従って余分なマシンはシャットダウンするか一時停止します。

電源ポリシー

さまざまなシナリオに合わせてマシンの電源管理ポリシーを構成します。シナリオごとに、待機時間（分単位）と、指定した時間の経過後に実行するアクションを指定できます。電源ポリシーは、シングルセッション OS のランダムデリバリーグループとシングルセッション OS の静的デリバリーグループに適用されます。

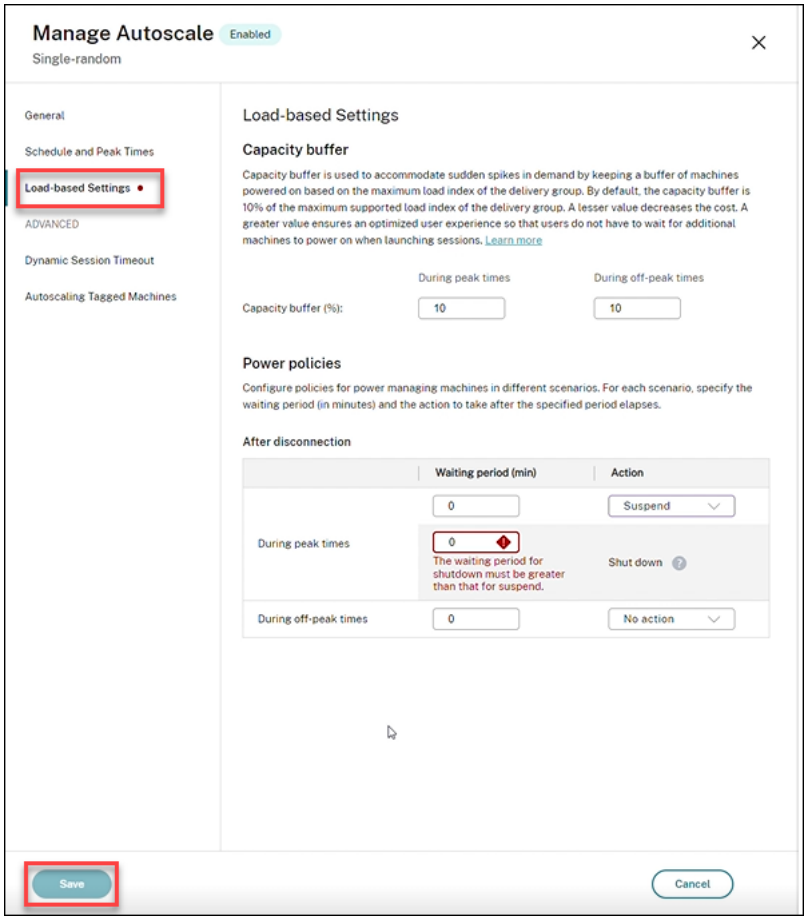


切断後は、以下の設定がピーク時とオフピーク時の両方に適用されます。

待ち時間を分単位で設定し、ドロップダウンから何もしない、一時停止、シャットダウンなどのアクションを設定できます。

- 一時停止アクションを選択した場合は、マシンをシャットダウンするまでの追加の待機時間を構成します。

> 注:
>
> - ピーク時およびオフピーク時においては、シャットダウンアクションの待機時間をサスペンドの待機時間より長くする必要があります。
> - 一時停止されたマシンには、切断されたユーザーのみが再接続することによりアクセスできます。一時停止されたマシンを新しいユーザーが使用できるようにするには、マシンをシャットダウンします。
> - 一時停止フィールドおよびシャットダウンフィールドの時間設定が正しく構成されていない場合、［保存］オプションは無効になり、ナビゲーション項目の横に設定エラーを示す赤い点も表示されます。



例

- 待機時間を 12 分に設定し、最初のアクションとして何もしないを選択した場合は、12 分が経過した後もマシンは引き続きパワーオンの状態になります。
- 待機時間を 15 分に設定して最初のアクションとして一時停止を選択し、2 番目の待機時間を 20 分に選択した場合、15 分が経過するとマシンは一時停止されます。2 番目の待機時間が終了すると、マシンはシャットダウンされます。
- 待機時間を 18 分に設定し、シャットダウンする最初のアクションを選択した場合、18 分が経過するとマシンがシャットダウンされます。

サンプルシナリオ

次のようなシナリオを想定します:

- デリバリーグループの構成。Autoscale が電源管理するデリバリーグループには 10 台のマシンが含まれています（M1～M10）。
- **Autoscale** の構成
  - 処理能力バッファは 10% に設定します。

  - 選択したスケジュールにマシンが含まれていません。

このシナリオは以下の順序で実行されます：

1. ユーザーはログオンしていません。
2. ユーザーセッションが増加します。
3. 追加のユーザーセッションが開始されます。
4. セッションの終了により、ユーザーセッションの負荷が減少します。
5. ユーザーセッションの負荷は、オンプレミスリソースによってのみ処理されるようになるまで減少し続けます。

上記のシナリオで Autoscale がどのように機能するかについては、以下を参照してください。

- ユーザー負荷なし（初期の状態）
  - 1 台のマシン（M1）の電源がオンになっています。マシンの電源がオンになっているのは、処理能力バッファが構成されているためです。この場合、10（マシン数）×10%（構成された処理能力バッファ）=1 です。したがって、1 台のマシンの電源がオンになります。
- 最初のユーザーがログオンする
  - デスクトップを使用するためにユーザーが初めてログオンしたときに、電源がオンになったマシンでホストされたデスクトッププールからデスクトップが割り当てられます。この場合、ユーザーにはマシン M1 からデスクトップが割り当てられます。
  - 処理能力バッファが構成されているため、需要の増大に応じて Autoscale が追加のマシン（M2）の電源をオンにします。
- 2 人目のユーザーがログオンする
  - ユーザーにはマシン M2 からデスクトップが割り当てられます。
  - 処理能力バッファが構成されているため、需要の増大に応じて Autoscale が追加のマシン（M3）の電源をオンにします。
- 3 人目のユーザーがログオンする
  - ユーザーにはマシン M3 からデスクトップが割り当てられます。
  - 処理能力バッファが構成されているため、需要の増大に応じて Autoscale が追加のマシン（M4）の電源をオンにします。
- ユーザーのログオフ
  - ユーザーがログオフした後、またはユーザーのデスクトップがタイムアウトした後、解放された処理能力（M3 など）をバッファとして利用できます。その結果、処理能力バッファが 10% で構成されているため Autoscale はマシン M4 の電源をオフにします。
- ユーザーがいなくなるまで、ユーザーのログオフは続きます。

  - さらにユーザーがログオフすると、Autoscale はマシンの電源（M2 または M3 など）をオフにします。
  - ユーザーが残っていなくても、Autoscale は予備の処理能力用に確保された最後の 1 台のマシン（M1 など）の電源はオフにしません。

> 注:
>
> シングルセッション OS のランダムデリバリーグループの場合、ユーザーのセッションログオフ時にデスクトップへの変更はすべて失われます。ただし、ユーザー固有の設定が構成されている場合、ユーザープロファイル設定とともにローミングされます。

シングルセッション **OS** の静的デリバリーグループ

処理能力バッファを使用すると、デリバリーグループ内の未割り当てのマシンの総数を基に電源がオンになっている未割り当てのマシンのバッファを確保することで、需要の急増に対応できます。デフォルトでは、処理能力バッファは、デリバリーグループ内にある未割り当てのマシンの総数の 10% です。

> 重要:
>
> デリバリーグループ内のすべてのマシンが割り当てられた後は、処理能力バッファがマシンの電源のオンオフに関与することはなくなります。

マシン数（処理能力バッファを含む）が現在電源がオンになっているマシンの総数を上回っている場合、需要に対応して未割り当てのマシンの電源が追加でオンになります。マシン数（処理能力バッファを含む）が現在電源がオンになっているマシンの総数を下回っている場合、構成されたアクションに従って余分なマシンは電源がオフになるか一時停止します。

シングルセッション OS の静的デリバリーグループの Autoscale:

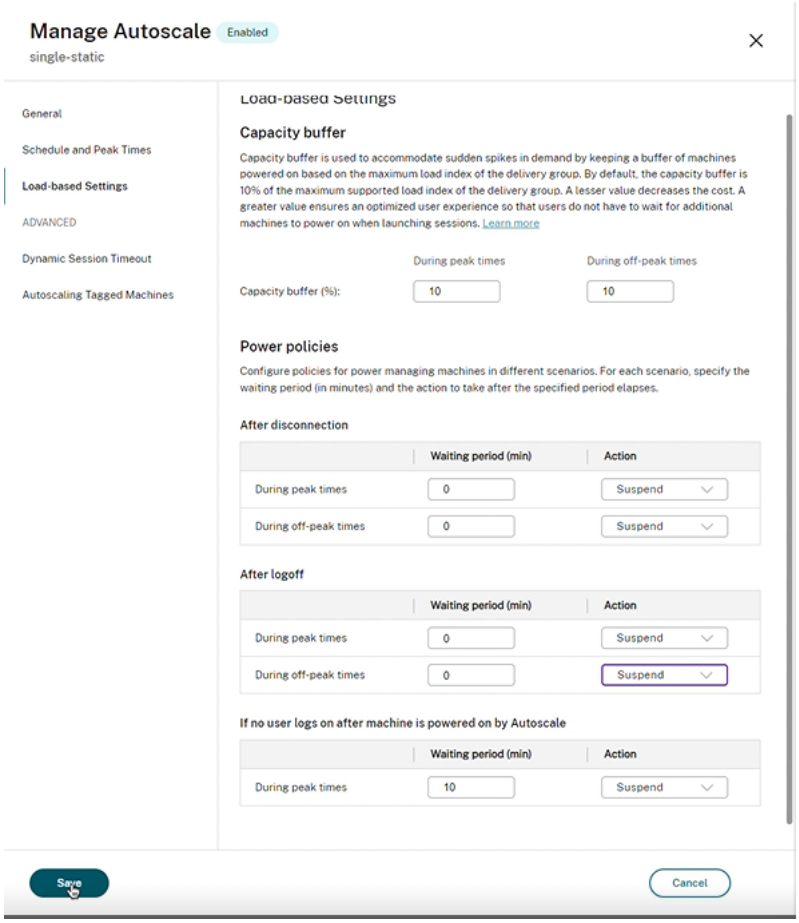
- 該当するシングルセッション OS のデリバリーグループの`AutomaticPowerOnForAssigned`プロパティが true に設定されているときにのみ、割り当てられたマシンの電源をピーク時にオンにし、オフピーク時にオフにします。
- `AutomaticPowerOnForAssignedDuringPeak`プロパティが true に設定されているデリバリーグループに所属するマシンの電源がピーク時にオフになっている場合、自動的にオンにします。

割り当てられたマシンで処理能力バッファがどのように機能するかを理解するには、次のことを考慮してください:

- 処理能力バッファは、デリバリーグループに未割り当てのマシンが 1 つまたは複数ある場合にのみ機能します。
- デリバリーグループ内に未割り当てのマシンがない（すべてのマシンが割り当てられている）場合、処理能力バッファがマシンの電源のオンオフに関与することはなくなります。
- `AutomaticPowerOnForAssignedDuringPeak`プロパティは割り当てられたマシンの電源がピーク時にオンになるかを決定します。true に設定されている場合、Autoscale はピーク時にマシンの電源をオンのままにします。Autoscale は、電源がオフの場合でも電源をオンにします。

電源ポリシー

さまざまなシナリオに合わせてマシンの電源管理ポリシーを構成します。シナリオごとに、待機時間（分単位）と、指定した時間の経過後に実行するアクションを指定できます。電源ポリシーは、シングルセッション OS のランダムデリバリーグループとシングルセッション OS の静的デリバリーグループに適用されます。



切断後およびログオフ後は、以下の設定がピーク時とオフピーク時の両方に適用されます。
待ち時間を分単位で設定し、ドロップダウンから何もしない、一時停止、シャットダウンなどのアクションを設定できます。

Autoscale によってマシンの電源がオンになった後、ユーザーがログオンしていない場合、以下の設定がピーク時に適用されます。待ち時間を分単位で設定し、ドロップダウンから何もしない、一時停止、シャットダウンなどのピーク時のアクションを設定できます。

サンプルシナリオ

次のようなシナリオを想定します：

- デリバリーグループの構成。Autoscale が電源管理するデリバリーグループには 10 台のマシンが含まれています（M1～M10）。

- **Autoscale** の構成
  - マシン M1 から M3 までが割り当てられ、マシン M4 から M10 までは未割り当てです。
  - 処理能力バッファはピーク時およびオフピーク時の 10% に設定します。
  - 選択されたスケジュールに従って、Autoscale は午前 9:00 から午後 6:00 までマシンの電源を管理します。

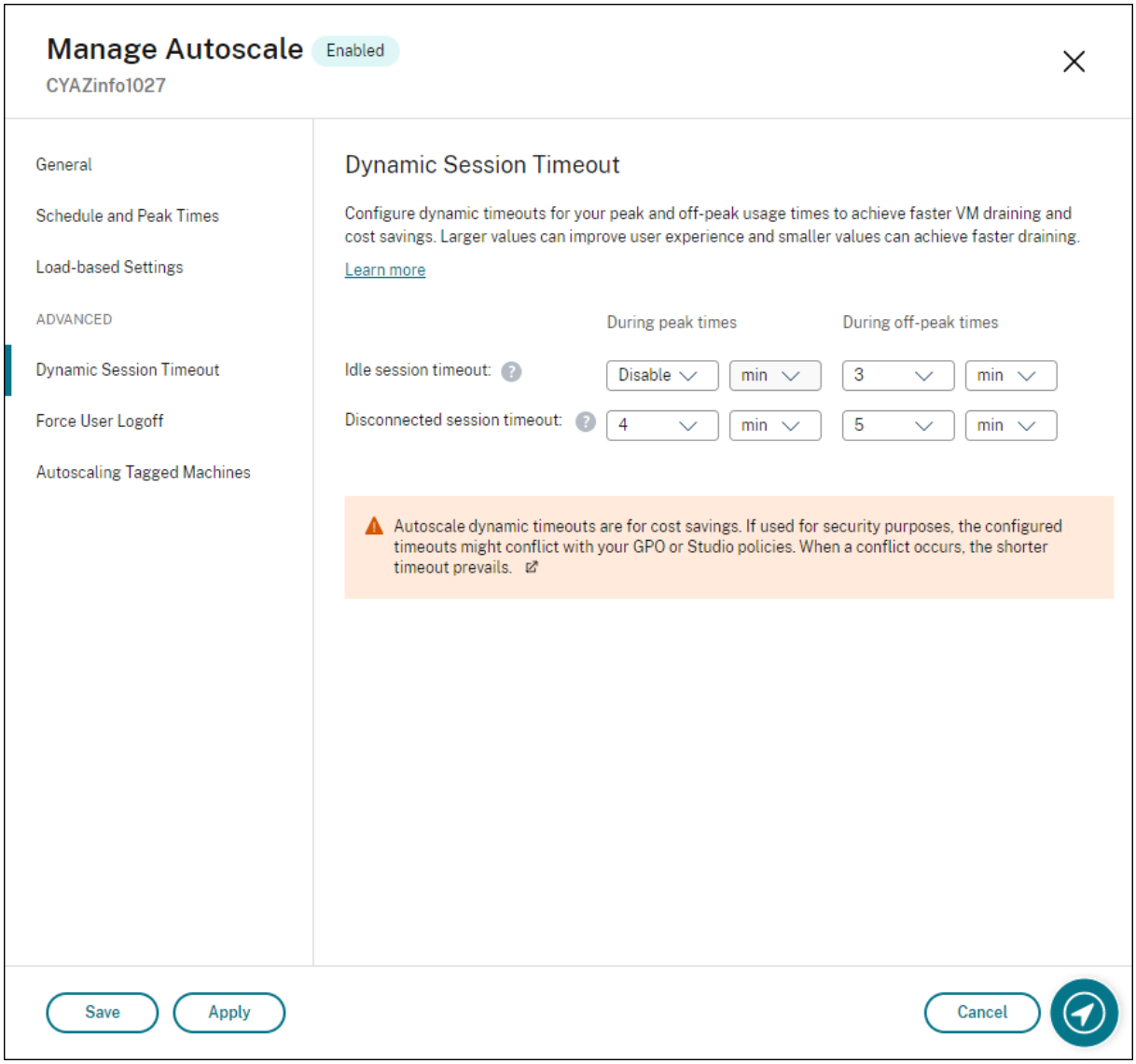
上記のシナリオで Autoscale がどのように機能するかについては、以下を参照してください。

- スケジュールの開始 - 午前 09:00
  - Autoscale は、マシン M1 から M3 までの電源をオンにします。
  - 処理能力バッファが構成されているため、Autoscale が追加のマシン（例：M4）の電源をオンにします。マシン M4 は未割り当てです。
- 最初のユーザーがログオンする
  - デスクトップを使用するためにユーザーが初めてログオンしたときに、電源がオンになった未割り当てのマシンでホストされたデスクトッププールからデスクトップが割り当てられます。この場合、ユーザーにはマシン M4 からデスクトップが割り当てられます。そのユーザーによる以降のログオンでは、最初の使用時に割り当てられたデスクトップに接続します。
  - 処理能力バッファが構成されているため、需要の増大に応じて Autoscale が追加のマシン（例：M5）の電源をオンにします。
- 2 人目のユーザーがログオンする
  - ユーザーには電源がオンになっている未割り当てのマシンからデスクトップが割り当てられます。この場合、ユーザーにはマシン M5 からデスクトップが割り当てられます。そのユーザーによる以降のログオンでは、最初の使用時に割り当てられたデスクトップに接続します。
  - 処理能力バッファが構成されているため、需要の増大に応じて Autoscale が追加のマシン（例：M6）の電源をオンにします。
- ユーザーのログオフ
  - ユーザーがデスクトップからログオフしたり、デスクトップがタイムアウトになると、Autoscale は午前 09:00 から午後 06:00 までマシン M1 から M5 までの電源をオンにしたままにします。これらのユーザーが次回ログオンすると、最初の使用時に割り当てられたものと同じデスクトップに接続されます。
  - 未割り当てのマシン M6 は、未割り当ての新規ユーザーにデスクトップを提供するため待機します。
- スケジュールの終了 - 午後 06:00
  - Autoscale は午後 06:00 にマシン M1 から M5 までの電源をオフにします。
  - 処理能力バッファが構成されているため、Autoscale は未割り当てのマシン M6 の電源をオンにしたままにします。このマシンは、未割り当ての新規ユーザーにデスクトップを提供するため待機しています。
  - このデリバリーグループ内では、マシン M6 から M10 までは未割り当てのマシンです。

動的セッションタイムアウト

June 26, 2023

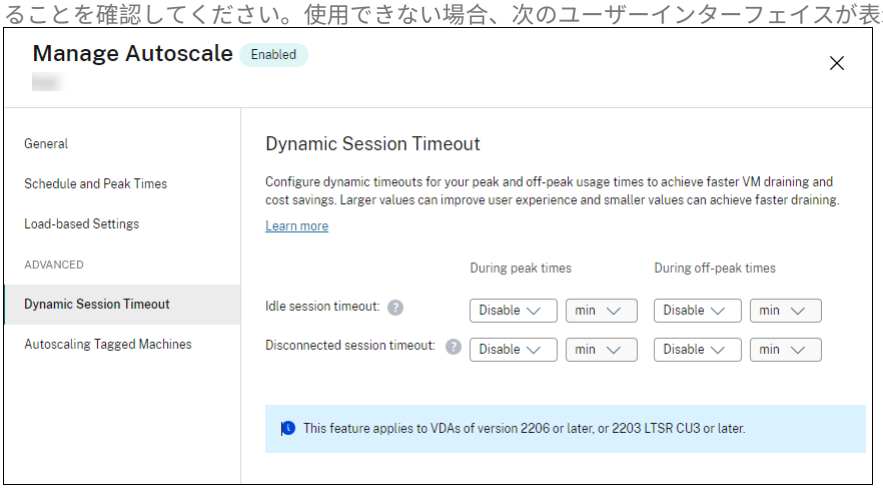
この機能を使用すると、ピーク時とオフピーク時に切断されるセッションとアイドル状態になるセッションのタイムアウトを構成して、マシンのドレインを高速化し、コストを削減できます。この機能は、シングルセッションおよびマルチセッションの OS マシンに適用されます。VDA は、10 分を超えてアイドル状態になっているセッションのアイドル時間を報告するため、動的セッションタイムアウトは、アイドル状態から 10 分以内はアイドル状態のセッションを切断できません。値が小さいほど、残留セッションが早く削除されるため、コストが削減されます。



注:

- この機能は、マルチセッション OS のデリバリーグループでサポートされています。

- シングルセッション OS デリバリーグループの場合、この機能は VDA のバージョン 2206 CR 以降、または 2203 LTSR CU3 以降に適用されます。これらの VDA が Citrix Cloud に最低 1 回は登録されていることを確認してください。使用できない場合、次のユーザーインターフェイスが表示されます:



（動的セッションタイムアウトが使用できません）

- Autoscale の動的タイムアウトは、コスト削減のためのオプションです。セキュリティ上の目的で使用すると、構成されたタイムアウトが GPO または［管理］コンソールのポリシーと競合することがあります。競合が発生すると、短いタイムアウトが優先されます。

アイドル状態セッションタイムアウト。ユーザーからの入力がない場合に、中断のないユーザー接続をどのくらい長く維持するのかを指定するタイマーを有効または無効にします。タイマーが時間切れになると、セッションは切断状態になり、［切断されたセッションタイムアウト］が適用されます。［切断されたセッションタイムアウト］が無効な場合、セッションはログオフしません。

重要:

- 10 分（600 秒）以下の値を指定すると、Autoscale は、関連するセッションが 10 分間アイドル状態になった後、それらのセッションを切断します。これは、VDA が報告するセッションアイドル時間に Autoscale が依存しているためです。VDA は、10 分を超えてアイドル状態になっているセッションについてのみアイドル時間を報告します。
- アイドルセッションがタイムアウトに達してから最後の 5 分以内にユーザーがそのセッションと通信した場合、アイドルセッションは切断状態のままになります。

切断されたセッションタイムアウト。切断されたデスクトップをロックしたままセッションがログオフするまでの時間を指定するタイマーを有効または無効にします。有効な場合、タイマーが時間切れになると、切断されたセッションはログオフします。

タグ付けされたマシンの **Autoscale**（クラウドバースト）

March 2, 2023

> 注:
>
> この機能は、以前は Autoscale の制限と呼ばれていました。

はじめに

Autoscale には、デリバリーグループ内のマシンのサブセットのみを電源管理できる柔軟性があります。この場合、1 つまたは複数のマシンにタグを適用し、タグ付きマシンのみを電源管理するように Autoscale を構成します。

この機能はクラウドの処理が増大した場合に有用であり、クラウドベースのリソースで追加の需要（バーストワークロード）が発生する前にオンプレミスのリソース（またはパブリッククラウドのリザーブドインスタンス）を使用してワークロードを処理できます。最初にオンプレミスのマシン（またはリザーブドインスタンス）をワークロードに対応させるには、タグ制限とゾーン優先度を使用する必要があります。

タグ制限は、Autoscale で電源管理されるマシンを指定します。ゾーン優先度では、ユーザーの起動要求を処理する優先ゾーンのマシンを指定します。詳しくは、「タグ」および「ゾーン優先度」を参照してください。

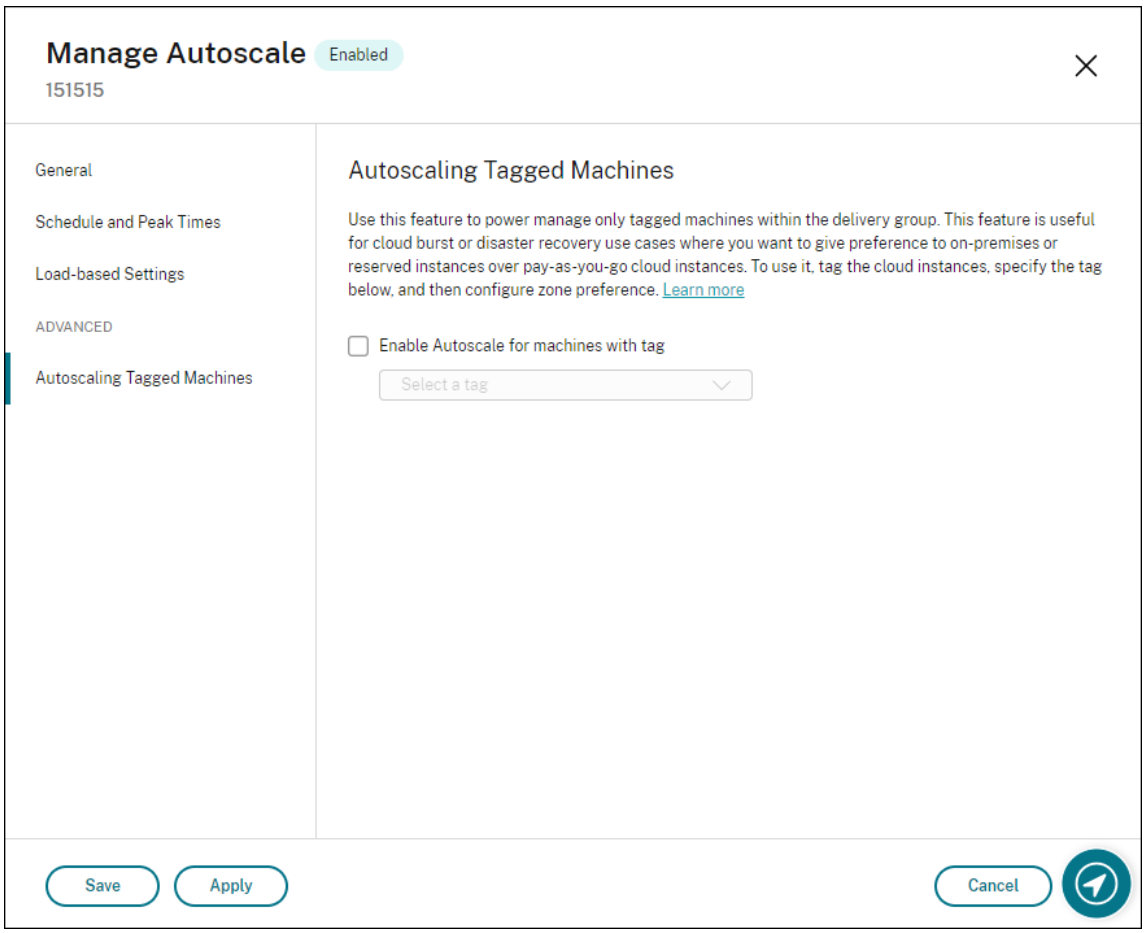
特定のタグ付きマシンをオートスケールするために、［管理］コンソールまたは PowerShell を使用できます。

［管理］コンソールを使用して特定のタグ付きマシンに **Autoscale** を使用する

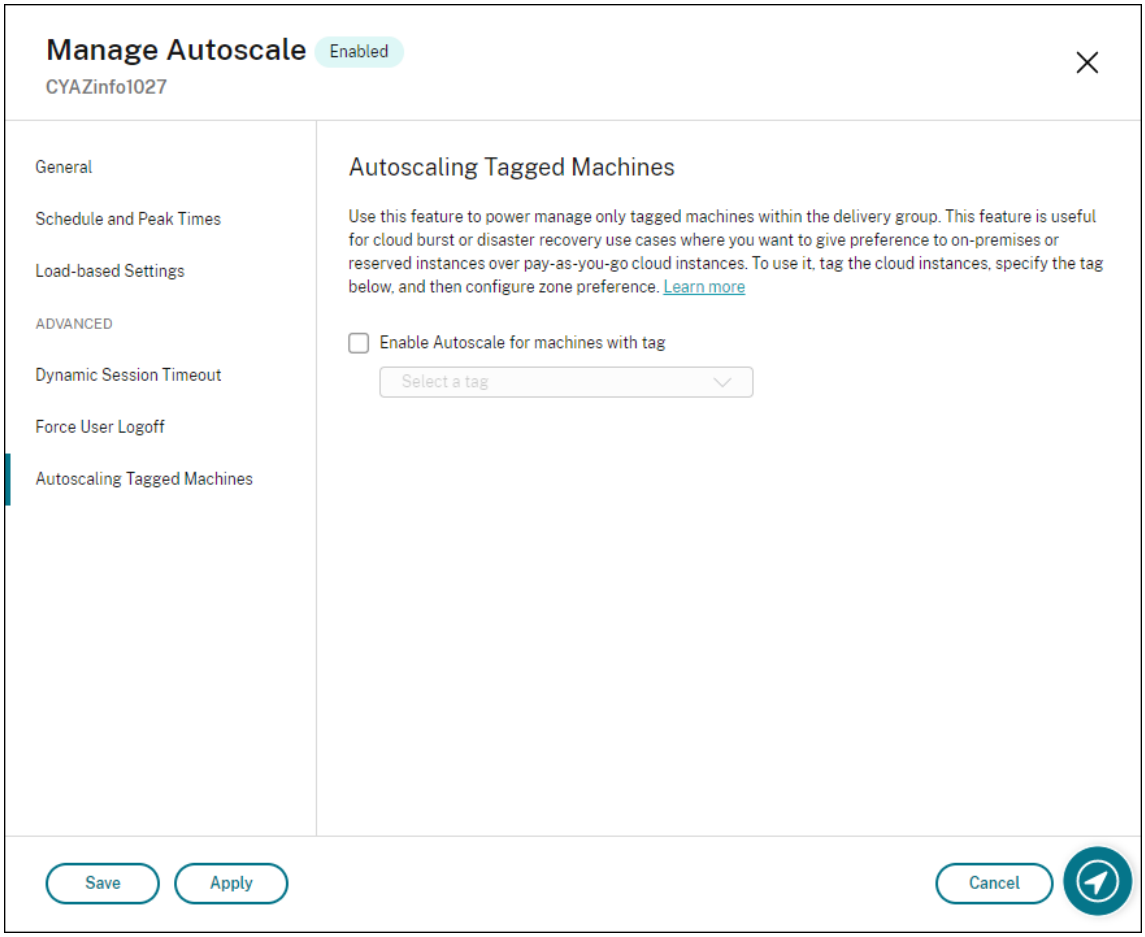
特定のタグ付きマシンに Autoscale を使用には、次の手順を実行します:

1. タグを作成し、そのタグをデリバリーグループ内の該当するマシンに適用します。詳しくは、「タグとタグ制約の管理」を参照してください。
2. デリバリーグループを選択し、**Autoscale** の管理ウィザードを開きます。
3. ［タグ付けされたマシンの **Autoscale**］ページで ［タグ付けされたマシンの **Autoscale** を有効にする］を選択し、一覧からタグを選択します。次に ［適用］をクリックして変更を保存します。

   シングルセッション OS の静的およびランダムのデリバリーグループのユーザーインターフェイス:



マルチセッション *OS* デリバリーグループのユーザーインターフェイス:



> 警告:
>
> - 特定のタグを持つマシンの Autoscale では、ヒストグラムが自動的に更新され、タグごとのマシンの数に反映される場合があります。［スケジュールとピーク時間］ページで、必要であれば手動で時間枠ごとにマシンを割り当てることができます。
> - タグ付きマシンで使用されているタグを削除することはできません。タグを削除するには、最初にタグ制限を削除する必要があります。

タグ制限を適用し、あとからデリバリーグループから削除することができます。これを行うには、［**Autoscale** の管理］**>**［タグ付けされたマシンの **Autoscale**］ページに移動してから、［タグ付けされたマシンの **Autoscale** を有効にする］をオフにします。

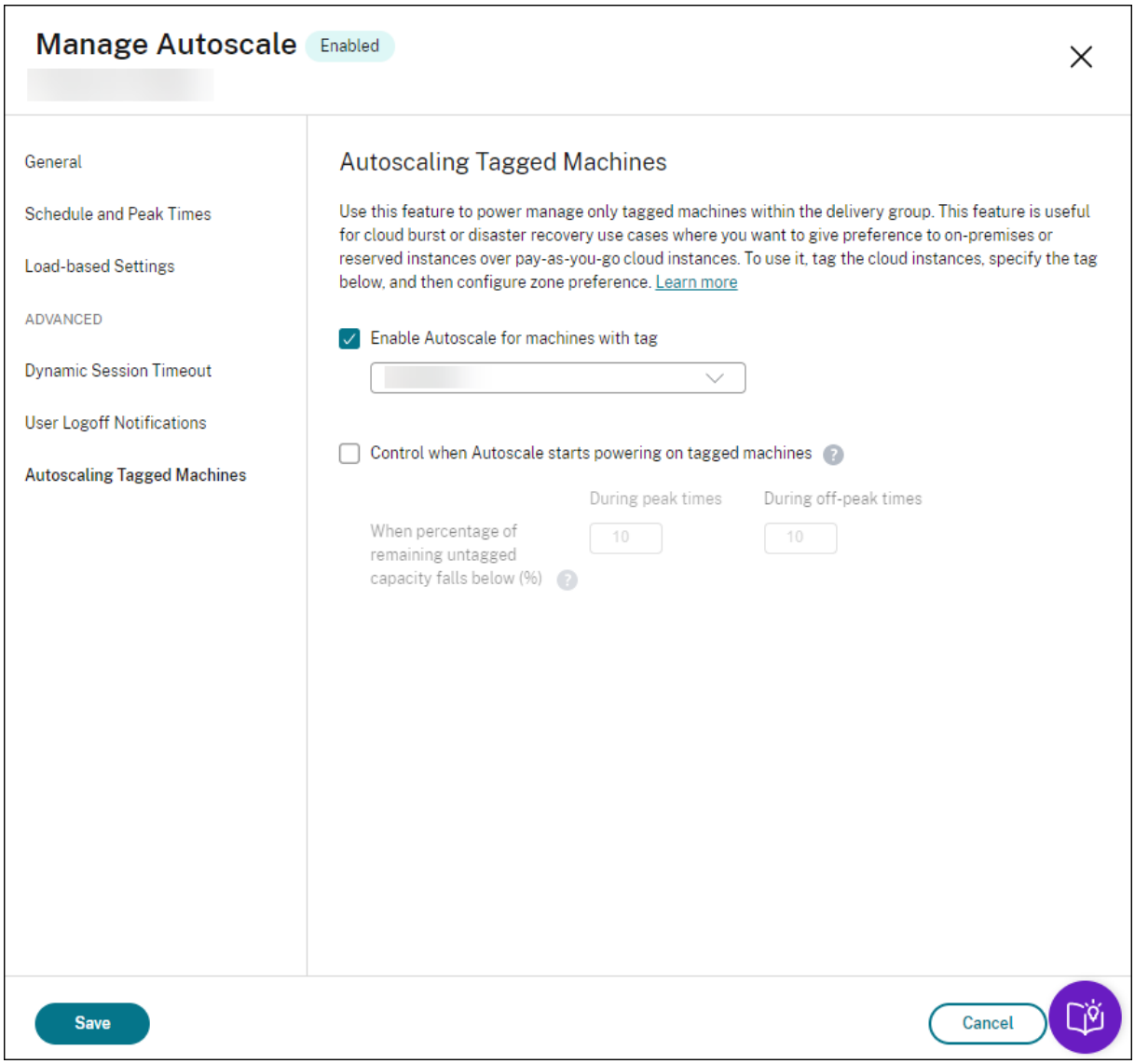
> 警告:
>
> - ［タグ付きマシンの **Autoscale** を有効にする］をオフにしないで該当マシンからタグを削除し、［**Autoscale** の管理］ウィザードを開くと、警告を受け取ることがあります。マシンからタグを削除すると Autoscale で指定したタグが無効になるため、Autoscale が管理するマシンがなくなる可能性があります。警告を解決するには、［タグ付けされたマシンの **Autoscale**］ページで無効なタグを削除し、［適用］をクリックして変更を保存します。

Autoscale がリソースを電源オンするタイミングを制御する

Autoscale は、タグ付けされていないマシンの使用状況に基づいて、タグ付けされたマシンの電源投入を開始するタイミングを制御することもできます。これにより、タグ付きまたはパブリッククラウドのワークロードの消費をさらに最適化できます。

このためには、次の手順を実行します:

1. ［タグ付けされたマシンの **Autoscale**］ページで、［**Autoscale** がタグ付けされたマシンの電源投入を開始するタイミングを制御する］を選択します。
2. ピーク時およびオフピーク時のタグなしマシン使用量のパーセンテージを入力し、［適用］をクリックします。使用できる値：0～100。



> ヒント：
>
> このパーセンテージは、Autoscale によるタグ付けされたマシンの電源投入を開始するタイミングを制御します。パーセンテージがしきい値を下回った場合（デフォルトは 10%）、Autoscale がタグ付けされたマシンの電源投入を開始します。パーセンテージがしきい値を超えると、Autoscale は電源オフモードになります。パーセンテージを入力するときは、次の 2 つのシナリオを考慮してください。
>
> - シングルセッション OS デリバリーグループの場合：この値は、アイドル状態にあるタグなしマシンの総数のパーセンテージで定義されます。例：タグなしのシングルセッション OS マシンが 10 台あるとします。セッションのないマシンが 1 台だけ残っている場合、Autoscale はタグ付けされたマシンの電源を投入し始めます。
> - マルチセッション OS のデリバリーグループの場合：この値は、負荷インデックスを基準とした使用可能なタグなしマシンの合計処理能力のパーセンテージで定義されます。例：タグなしのマルチセッション OS マシンが 10 台あるとします。負荷が 90% になると、Autoscale はタグ付けされたマシンの電源を投入し始めます。

PowerShell を使用して特定のタグ付きマシンを **Autoscale** する

PowerShell SDK を直接使用するには、次の手順を実行します：

1. タグを作成します。New-Brokertag PowerShell コマンドを使用してタグを作成します。
   - 例：`$managed = New-BrokerTag Managed`。この場合、タグの名前は「Managed」です。New-Brokertag PowerShell コマンドについて詳しくは、https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/New-BrokerTag/を参照してください。
2. タグをマシンに適用します。Get-Brokermachine PowerShell コマンドを使用して、Autoscale で電源管理するカタログのマシンにタグを適用します。
   - 例：`Get-BrokerMachine -CatalogName "cloud"| Add-BrokerTag $managed.Name`。この場合、カタログの名前は「cloud」です。
   - Get-Brokermachine PowerShell コマンドについて詳しくは、https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerMachine/を参照してください。

   > 注：
   >
   > タグの適用後、新しいマシンをカタログに追加できます。タグはこれらの新しいマシンに自動的に適用されません。

3. **Autoscale** で電源管理するデリバリーグループにタグ付きのマシンを追加します。Get-BrokerDesktopGroup PowerShell コマンドを使用して、対象のマシンが含まれるデリバリーグループにタグ制限を追加します（つまり、「X タグでマシンの起動を制限します」）。

- 例: `Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscaleTagUid $managed.Uid`。この場合、デリバリーグループの UID は 1 です。
- Get-BrokerDesktopGroup PowerShell コマンドについて詳しくは、https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/を参照してください。

タグ制限を適用し、あとからデリバリーグループから削除することができます。この場合、Get-BrokerDesktopGroup PowerShell コマンドを使用します。

例:`Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscaleTagU $null`。この場合、デリバリーグループの UID は 1 です。

> 注:
>
> タグなしのマシンは、ユーザーが電源をオフにすると自動的に再起動します。この動作により、ワークロードをより迅速に処理できるようになります。この動作は、`Set-BrokerDesktopGroup` の`AutomaticRestartForUntaggedMachines`プロパティを使用して、デスクトップごとのグループで有効または無効にできます。詳しくは、https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/を参照してください。

サンプルシナリオ

次のようなシナリオを想定します:

- マシンカタログの構成。2 つのマシンカタログ（C1 と C2）があります。
  - カタログ C1 には、オンプレミス展開でローカルにある 5 台のマシン（M1 から M5）が含まれています。
  - カタログ C2 には、クラウド展開でリモートにある 5 台のマシン（M6 から M10）が含まれています。
- タグ制限。「Cloud」という名前のタグが作成され、カタログ C2 のマシン M6 から M10 に適用されます。
- ゾーン構成。2 つのゾーン（Z1 および Z2）が作成されます。
  - カタログ C1 を含むゾーン Z1 は、オンプレミス展開に対応しています。
  - カタログ C2 を含むゾーン Z2 は、クラウド展開に対応しています。
- デリバリーグループの構成
  - このデリバリーグループには、10 台のマシン（M1 から M10）、カタログ C1 からの 5 台のマシン（M1 から M5）、およびカタログ C2 からの 5 台のマシン（M6 から M10）が含まれます。
  - マシン M1 から M5 は手動で電源をオンにされ、スケジュール全体を通してオンのままになります。
- **Autoscale** の構成
  - 処理能力バッファは 10% に設定します。

  - Autoscale はタグ「Cloud」が付いたマシンのみ電源を管理します。この場合、Autoscale はクラウドマシン M6 から M10 の電源を管理します。

- 公開アプリケーションまたはデスクトップの構成。ゾーン優先度が、たとえば公開デスクトップ用に構成されると、ユーザーの起動要求でゾーン Z1 がゾーン Z2 より優先されます。

  - ゾーン Z1 は、公開デスクトップの優先ゾーン（ホームゾーン）として構成されます。

このシナリオは以下の順序で実行されます：

1. ユーザーはログオンしていません。
2. ユーザーセッションが増加します。
3. ユーザーセッションは、すべてのオンプレミスマシンが消費されるまで増加します。
4. 追加のユーザーセッションが開始されます。
5. セッションの終了により、ユーザーセッションが減少します。
6. ユーザーセッションは、セッションの負荷がオンプレミスマシンによってのみ処理されるようになるまで減少し続けます。

上記のシナリオで Autoscale がどのように機能するかについては、以下を参照してください。

- ユーザー負荷なし（初期の状態）

  - オンプレミスマシン M1 から M5 まですべての電源がオンになっています。
  - クラウド内の 1 台のマシン（たとえば M6）の電源がオンになります。マシンの電源がオンになっているのは、処理能力バッファが構成されているためです。この場合、10（マシン数）×10,000（負荷インデックス）×10%（構成された処理能力バッファ）=10,000 です。したがって、1 台のマシンの電源がオンになります。
  - 電源がオンになっているすべてのマシン（M1 から M6）の負荷インデックス値は基準の負荷（負荷インデックス =0）になっています。

- ユーザーのログオン

  - セッションは構成されたゾーン優先度によってマシン M1 〰 M5 でホストされ、これらのオンプレミスマシン全体で負荷が分散されます。
  - 電源がオンになっているマシン（M1 から M5 まで）の負荷インデックスが増加します。
  - 電源がオンになっているマシン M6 の負荷インデックス値は基準の負荷になっています。

- ユーザーが負荷を増やし、すべてのオンプレミスのリソースを消費

  - セッションは構成されたゾーン優先度によってマシン M1 〰 M5 でホストされ、これらのオンプレミスマシン全体で負荷が分散されます。
  - 電源がオンになっているすべてのマシン（M1 から M5 まで）の負荷インデックスが 10,000 に達します。
  - 電源がオンになっているマシン M6 の負荷インデックス値は基準の負荷のままです。

- さらに 1 人のユーザーがログオン

  - ゾーン優先度がオーバーフローし、セッションはクラウドマシン M6 でホストされます。
  - 電源がオンになっているすべてのマシン（M1 から M5 まで）の負荷インデックスが 10,000 に達します。
  - 電源がオンになっているマシン M6 の負荷インデックス値が上昇し、基準の負荷を超えます。予備の合計処理能力が負荷インデックス基準で 10,000 未満に低下すると、処理能力バッファが構成されているため、需要の増大に応じて Autoscale が追加のマシン（M7）の電源をオンにします。マシン M7 の電源をオンにするまで時間がかかり、準備が整うまで遅延が生じる場合があります。

- さらにユーザーがログオン

  - セッションは、マシン M6 でホストされます。
  - 電源がオンになっているすべてのマシン（M1 から M5 まで）の負荷インデックスが 10,000 に達します。
  - 電源がオンになったマシン M6 の負荷インデックス値がさらに上昇しますが、予備の合計処理能力は、負荷インデックス基準で 10,000 を超えています。
  - 電源がオンになっているマシン M7 の負荷インデックス値は基準の負荷のままです。

- さらに多くのユーザーがログオン

  - マシン M7 の準備が整うと、セッションはマシン M6 および M7 でホストされるようになり、これらのマシン間で負荷が分散されます。
  - 電源がオンになっているすべてのマシン（M1 から M5 まで）の負荷インデックスが 10,000 に達します。
  - マシン M7 の負荷インデックス値は基準の負荷ではなくなります。
  - 電源がオンになっているマシン（M6 と M7）の負荷インデックスが増加します。
  - 予備の合計処理能力は、まだ負荷インデックス基準で 10,000 を超えています。

- セッションの終了によりユーザーセッションの負荷が減少する

  - ユーザーがセッションからログオフした後、またはアイドルセッションがタイムアウトした後、マシン M1 から M7 までの解放された処理能力は他のユーザーが開始したセッションのホストで再利用されます。
  - 予備の合計処理能力が負荷インデックス基準で 10,000 を超えるレベルに増加すると、Autoscale はいずれかのマシン（例：M6 〰 M7）をドレイン状態にします。その結果、他のユーザーによって開始されたセッションは、（ユーザー負荷が再度増大する、または他のクラウドマシンの負荷が最小になるなど）新しい変更が行われない限り、そのマシン（M7 など）に送信されなくなります。

- 1 つまたは複数のクラウドマシンが不要になるまで、ユーザーセッションの負荷はさらに減少します。

  - マシン M7 上のすべてのセッションが終了し、指定された電源オフの遅延でタイムアウトになると、Autoscale はマシン M7 の電源をオフにします。
  - 電源がオンになっているマシン（M1 から M5 まで）の負荷インデックスが 10,000 を下回るレベルに下降します。
  - 電源がオンになっているマシン（M6）の負荷インデックスが減少します。

- クラウドマシンが不要になるまで、ユーザーセッションの負荷はさらに減少します。
  - マシン M6 にユーザーセッションがない場合でも、Autoscale は予備の処理能力用に確保しているため電源をオフにしません。
  - 処理能力バッファが構成されているため、Autoscale は残されたクラウドマシン M6 の電源をオンにしたままにします。このマシンは、新規ユーザーにデスクトップを提供するため待機しています。
  - セッションは、オンプレミスマシンに利用できる処理能力がある限り、マシン M6 でホストされません。

マシンの動的プロビジョニング

November 28, 2022

Autoscale には、マシンを動的に作成および削除する機能が備えられています。PowerShell スクリプトを使用してこの機能を活用できます。このスクリプトで、現在の負荷条件に基づいて、デリバリーグループ内のマシンの数を動的にスケールアップまたはスケールダウンできます。

このスクリプトには、次の利点（およびその他）があります：

- ストレージコストの削減。コンピューティングコストを削減させる Autoscale とは異なり、スクリプトではマシンをプロビジョニングするためによりコスト効率の高いソリューションを実現します。
- 負荷の変化の効率的的な処理。このスクリプトで、現在のデリバリーグループの負荷に基づいてマシンの数を自動的にスケールアップまたはスケールダウンすることにより、負荷の変化を処理できます。

スクリプトのダウンロード

PowerShell スクリプトは次の場所にあります。https://github.com/citrix/Powershell-Scripts/tree/master/XAXD/AutoscaleMcs

スクリプトの機能の仕方

> 重要：
>
> - 1 つのマシンカタログを複数のデリバリーグループに指定して、スクリプトで管理することはできません。つまり、複数のデリバリーグループが同じマシンカタログを共有している場合、これらのデリバリーグループのいずれでもスクリプトは機能しません。
> - 同じデリバリーグループのスクリプトを複数の場所から同時に実行することはできません。

スクリプトはデリバリーグループレベルで機能します。負荷を（負荷インデックス基準で）測定し、マシンを作成するか削除するかを決定します。

このスクリプトによって作成されたマシンには一意のタグが付けられるので（`ScriptTag`パラメーターを使用）、後で識別できます。マシンの作成または削除は、以下に基づいて行われます：

- デリバリーグループの最大負荷率。Autoscale で余分な負荷に対処するためにマシンを作成する最大レベルを指定します。このしきい値を超えると、マシンがバッチで作成され、現在の負荷はしきい値以下にされます。
- デリバリーグループの最小負荷率。このスクリプトで作成され、アクティブなセッションのないマシンを削除する最小レベルを指定します。このしきい値を超えると、このスクリプトで作成され、アクティブなセッションのないマシンが削除されます。

このスクリプトはデリバリーグループ全体を監視し、トリガー条件が満たされたときにマシンを作成または削除することを目的としています。これはそれぞれの実行ごとに行われます。つまり、スクリプトが意図したとおりに機能するように、定期的にスクリプトを実行する必要があります。5 分以上の間隔でスクリプトを実行することをお勧めします。これにより、全体的な応答性が向上します。

スクリプトは、以下のパラメーターに依存して機能します：

パラメーター	種類	デフォルト値	説明
DeliveryGroupName	文字列	X	現在の負荷を判定するために監視するデリバリーグループの名前。名前をセミコロンで区切ったリストを作成できます。例：`Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName 'dg1;dg2;dg3' -XdProfileName profile`。
XdProfileName	文字列	X	リモートサーバーの認証に使用するプロファイルの名前。このパラメーターを使用したリモートサーバーの認証について詳しくは、「認証 API」を参照してください。
HighWatermark	整数	80	Autoscale で余分な負荷に対処するためにマシンを作成する（負荷インデックス基準での）最大負荷率。

パラメーター	種類	デフォルト値	説明
LowWatermark	整数	15	このスクリプトで作成され、アクティブなセッションのないマシンを削除する（負荷インデックス基準での）最小負荷率。
MachineCatalogName	文字列	X	マシンが作成されるマシンカタログの名前。
MaximumCreatedMachine	整数	-1	指定されたデリバリーグループで作成できるマシンの最大数。値が 0 以下の場合、スクリプトはこのパラメーターを処理しません。
ScriptTag	文字列	AutoscaledScripted	スクリプトで作成されたマシンに適用されるタグ。
EventLogSource	文字列	X	Windows イベントビューアーに表示されるソース名。

> 注:
>
> 「X」は、そのパラメーターにデフォルト値が指定されていないことを示します。

デフォルトでは、スクリプトを初めて実行するときには（`ScriptTag`パラメーター以外の）すべてのパラメーターが必要です。それ以降の実行では、`DeliveryGroupName`および`XdProfileName`パラメーターのみが必須です。必要に応じて、最小負荷率および最大負荷率を更新するよう選択できます。

スクリプトを初めて実行するときは、単一のデリバリーグループを指定する必要があることに注意してください。たとえば、スクリプトを初めて実行するときに次の PowerShell コマンドを使用して 2 つのデリバリーグループを指定すると、このスクリプトは機能しません:

- `Invoke-AutoscaleMachineCreations.ps1 -DeliveryGroupName 'dg1; dg2'-XdProfileName profile -LowWatermark 20 -HighWatermark 70 -MachineCatalogName 'cat1'\`

代わりに、最初に次のコマンドを使用して単一のデリバリーグループ（この例では dg1）を指定します:

- `Invoke-AutoscaleMachineCreations.ps1 -DeliveryGroupName 'dg1 '-XdProfileName profile -LowWatermark 20 -HighWatermark 70 -MachineCatalogName 'cat1'\`

次に、次のコマンドを使用して、2 番目のデリバリーグループ（この例では dg 2）にスクリプトを実行します:

- `Invoke-AutoscaleMachineCreations.ps1 -DeliveryGroupName 'dg1;dg2' -XdProfileName profile`

前提条件

スクリプトを実行するには、次の前提条件が満たされていることを確認してください:

- マシンが作成されている同じドメイン内にマシンが存在する。
- Remote PowerShell SDK がそのマシンにインストールされている。Remote PowerShell SDK について詳しくは、「SDK および API」を参照してください。
- その他の前提条件:
  - 監視対象とするデリバリーグループ
  - プロビジョニングスキーム (テンプレート) が関連付けられている Machine Creation Services (MCS) で作成されたマシンカタログ
  - プロビジョニングスキームに関連付けられている ID プール
  - スクリプトが Windows イベントログに情報を書き込めるように作成されるイベントログソース
  - リモートサーバーへの認証を可能にするセキュアクライアント

権限、推奨事項、および通知

スクリプトを実行するときは、以下に注意してください:

- `XdProfileName`パラメーターを使用してリモートサーバーを認証する場合は、Citrix Cloud コンソールで作成された API アクセスセキュアクライアントを使用して、認証プロファイルを定義する必要があります。詳しくは、「認証 API」を参照してください。
- Active Directory でマシンアカウントを作成および削除する権限が必要です。
- Windows タスクスケジューラを使用して PowerShell スクリプトを自動化することをお勧めします。詳しくは、「Windows タスクスケジューラを使用した自動化タスクの作成」を参照してください。
- スクリプトで Windows イベントログに情報（エラーやアクションなど）を書き込む場合は、最初に`New-EventLog`コマンドレットを使用してソース名を指定する必要があります。例: `New-EventLog -LogName Application -Source <sourceName>`。その後、Windows イベントビューアーの ［アプリケーション］ペインでイベントを表示できます。
- スクリプトの実行中にエラーが発生した場合は、スクリプトを手動で実行してからスクリプトチェックを実行し、問題のトラブルシューティングを行います。

認証 **API**

スクリプトを実行する前に、API アクセスセキュアクライアントを使用して認証プロファイルを定義する必要があります。スクリプトを実行するアカウントと同じアカウントを使用して、セキュアクライアントを作成する必要があり

ます。

セキュアクライアントには以下の権限が必要です:

- MCS を使用してマシンを作成および削除する。
- マシンカタログを編集する（マシンを追加および削除する）。
- デリバリーグループを編集する（マシンを追加および削除する）。

セキュリティクライアントを作成するときには、セキュリティクライアントが現在のアカウントから自動的に権限を継承するので、アカウントに上記の権限があることを確認してください。

セキュアクライアントを作成するには、次の手順を実行します:

1. Citrix Cloud にサインインし、［**ID** およびアクセス管理］**>**［**API** アクセス］に移動します。
2. セキュアクライアントの名前を入力し、［クライアントの作成］をクリックします。

リモートサーバーを認証するには、`Set-XDCredentials` PowerShell コマンドを使用します。例:

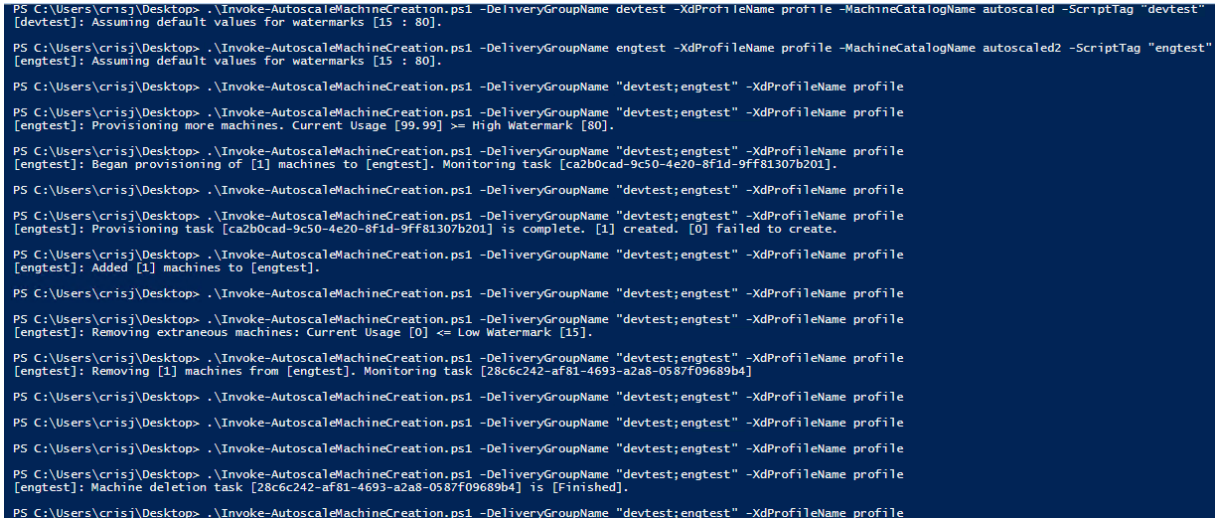
- `Set-XDCredentials -APIKey <key_id> -CustomerId <customer_id> -SecretKey <secret_key> -StoreAs <name specified by the XdProfileName parameter>`

Windows タスクスケジューラを使用した自動化タスクの作成

Windows タスクスケジューラを使用して PowerShell スクリプトを自動化できます。これにより、特定の間隔で、または特定の条件が満たされたときに、スクリプトが自動的に実行されます。このスクリプトを Windows タスクスケジューラで実行するには、必ず ［タスクの作成］**>**［設定］タブで ［新しいインスタンスを開始しない］を選択します。これにより、スクリプトが既に実行されている場合でも、Windows タスクスケジューラではスクリプトの新しいインスタンスを実行できなくなります。

スクリプト実行例

スクリプトの実行例については、下記を参照してください。スクリプトファイルは複数回呼び出されることに注意してください。この例では、負荷をシミュレートするために、1 つのセッションが起動され、終了します。



スクリプトのトラブルシューティングチェックリスト

スクリプトは、情報（エラーやアクションなど）を Windows イベントログに書き込みます。この情報は、スクリプトの実行時に発生する問題のトラブルシューティングに役立ちます。以下のトラブルシューティングチェックリストを念頭に置いておくと役立つでしょう：

- リモートサーバーと通信できない。選択できるアクション：
  - サーバーへの接続を確認します。
  - 使用する API キーが有効であることを確認します。
- マシンを作成できない。選択できるアクション：
  - スクリプトを実行しているユーザーアカウントに、ユーザーアカウントをドメインに作成するための十分な権限があることを確認します。
  - API キーを作成したユーザーに、MCS を使用してマシンをプロビジョニングするための十分な権限があることを確認します。
  - マシンカタログの有効性（つまり、そのイメージがまだ存在し、良好な状態であること）を確認します。
- マシンをマシンカタログまたはデリバリーグループに追加できない。選択できるアクション：
  - API キーを作成したユーザーが、マシンカタログおよびデリバリーグループとの間でマシンを追加および削除するための十分な権限を持っていることを確認します。

ユーザーログオフ通知（旧称ユーザー強制ログオフ）

June 9, 2023

> 重要:
>
> この機能は、デリバリーグループベースのマルチセッションアプリ用の Autoscale ユーザーインターフェイスでのみ使用可能です。

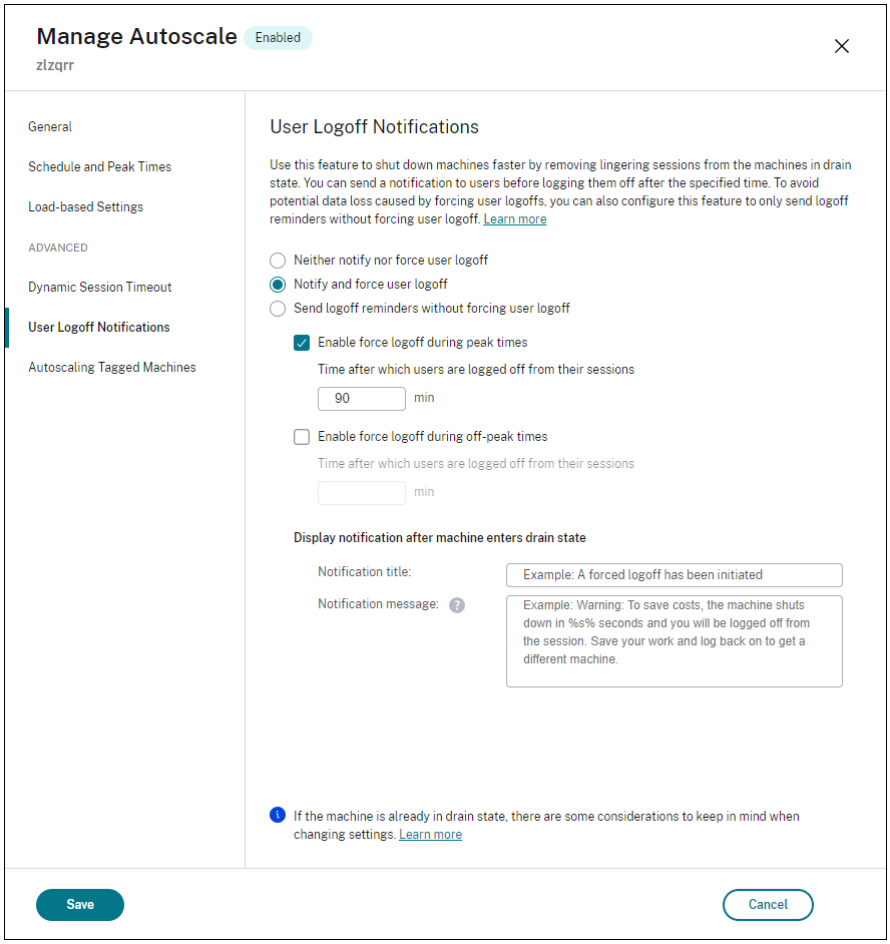
適切なコスト削減のために、Autoscale では、管理者が残留セッションからのログオフを強制することができます。この場合、管理者がカスタム通知をユーザーに送信でき、セッションが強制的にログオフされた後の猶予期間を設定できます。これは、ドレイン状態のマシンに対してのみ実行され、電源がオンになっているマシンすべてに対しては実行されません。ユーザーを強制ログオフすることで生じるデータ損失の可能性を避けるため、代わりに、ユーザーを強制ログオフせずにログオフリマインダーを送信するだけにすることもできます。

次のオプションがあります:

- ユーザーに通知して強制ログオフする
- ユーザーを強制的にログオフせずにログオフリマインダーを送信する
- ユーザーを強制的にログオフしない（通知なし）

ユーザーに通知して強制ログオフする

これを選択した場合、下記で指定する時間が経過すると、Autoscale はユーザーをセッションからログオフします。



ピーク時の強制ログオフを有効にする。これを選択した場合、ピーク時に指定された時間が経過すると、Autoscale はユーザーをセッションからログオフします。

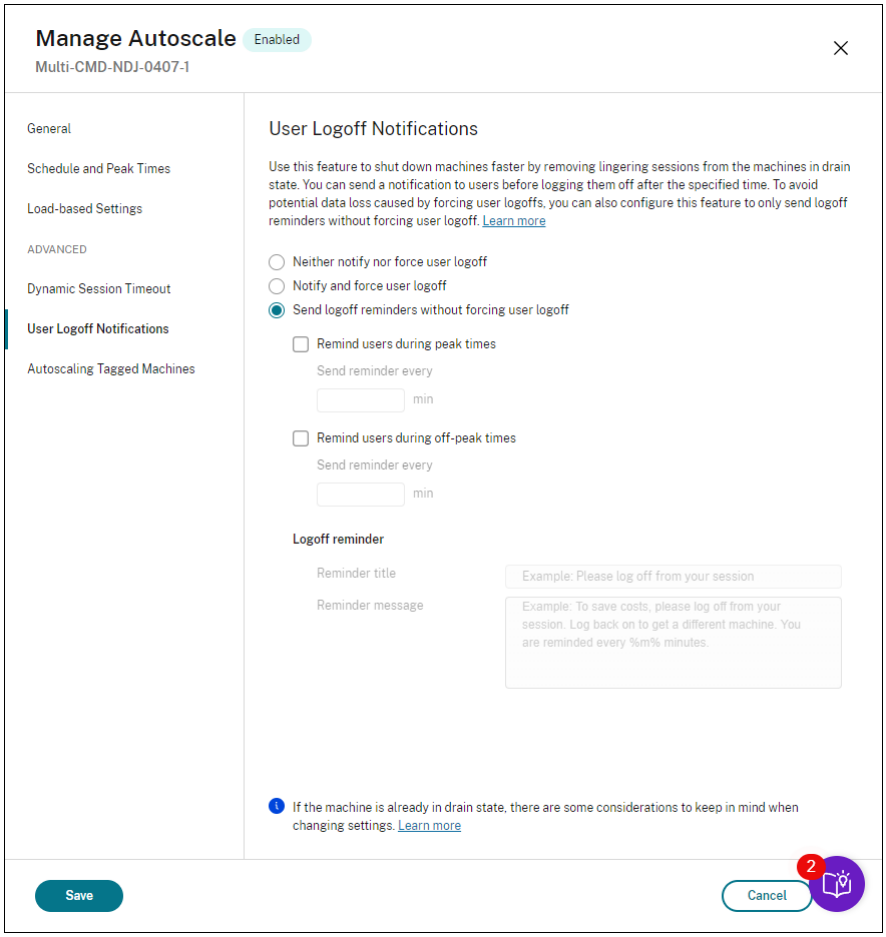
オフピーク時の強制ログオフを有効にする。これを選択した場合、オフピーク時に指定された時間が経過すると、Autoscale はユーザーをセッションからログオフします。

マシンがドレイン状態になった後に通知を表示する。ユーザーのマシンがドレイン状態になった後、ユーザーに通知を送信できます。

- 通知タイトル。ユーザーに送信する通知のタイトルを指定できます。例: `A forced logoff has been initiated.`
- 通知メッセージ。ユーザーに送信する通知の内容を指定できます。%s% または%m% を変数として使用して、メッセージで指定された時間を示すことができます。時間を秒単位で表すには、%s% を使用します。時間を分単位で表すには、%m% を使用します。例: `Warning: To save costs, the machine shuts down in %s% seconds and you will be logged off from the session. Save your work and log back on to get a different machine.`

ユーザーを強制的にログオフせずにログオフリマインダーを送信する

これを選択した場合、ユーザーは、マシンがドレイン状態になった後にマシンからログオフされる旨のリマインダーを受け取ります。このリマインダーは、下記で指定する間隔で送信されるように構成できます。



ピーク時にユーザーにリマインダーを送付する。これを選択した場合、ユーザーは、ピーク時にセッションからログオフされる旨のリマインダーを X 分ごとに受け取ります（X は指定した時間）。

オフピーク時にユーザーにリマインダーを送付する。これを選択した場合、ユーザーは、オフピーク時にセッションからログオフされる旨のリマインダーを X 分ごとに受け取ります（X は指定した時間）。

ログオフリマインダー。ユーザーのマシンがドレイン状態になった後、ユーザーにリマインダーを送信するように構成できます。

- リマインダーの件名。ユーザーに送信するリマインダーのタイトルを指定できます。例：`Please log off from your session`。
- リマインダーメッセージ。ユーザーに送信するメッセージを指定できます。例：`Please log off from your session and log back on to save costs`。

ユーザーを強制的にログオフしない（通知なし）

選択すると、Autoscale はユーザーにドレイン状態のマシンからのログオフを強制したり、別のマシンに手動で切り替えるように通知したりしません。

注意事項

マシンが既にドレイン状態にある場合は、設定を変更するときに次の点を考慮してください：

- ［ユーザーを強制的にログオフせずにログオフリマインダーを送信する］を ［ユーザーに通知して強制ログオフする］に変更すると、この新しい設定がすぐに有効になります。
- ［ユーザーに通知して強制ログオフする］を ［ユーザーを強制的にログオフせずにログオフリマインダーを送信する］に変更した場合、この新しい設定は、次にマシンがドレイン状態になるまで有効になりません。引き続き、ユーザーは強制的にログオフされます。

Autoscale 設定の有効性の分析

February 19, 2024

この機能を使用するには、［**DaaS**］**>** ［ホーム］**>** ［プレビュー機能］での ［**Autoscale** の分析情報］の切り替えを有効にしてください。［**Autoscale** の分析情報］を有効にしてから表示されるまでに約 15 分かかる場合があります。

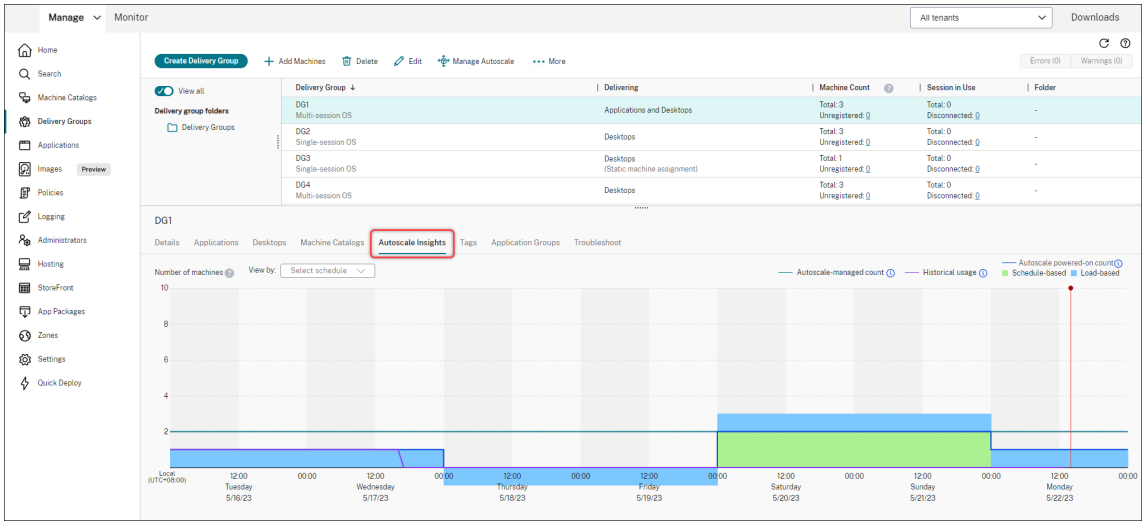
前週のマシンの使用状況に基づいて、Autoscale 設定の有効性を分析できます。分析を通じて、Autoscale 設定の有効性について次のような分析情報を得ることができます。

- 過剰なプロビジョニングによって生じる財務上の無駄を特定します。
- プロビジョニング不足によりユーザーエクスペリエンスが悪影響を受けているかどうかを判断します。
- プロビジョニングされた容量がマシンの使用状況と適切に調整されていることを確認してください。

この目標を達成するには、次の手順に従います。

1. Autoscale が有効なデリバリーグループを選択します。
2. 下部ペインで、［**Autoscale** の分析情報］タブをクリックします。

   次のグラフが表示され、前週のマシン利用状況データと、Autoscale 設定に基づいて電源がオンになるマシンの数との比較が示されます。



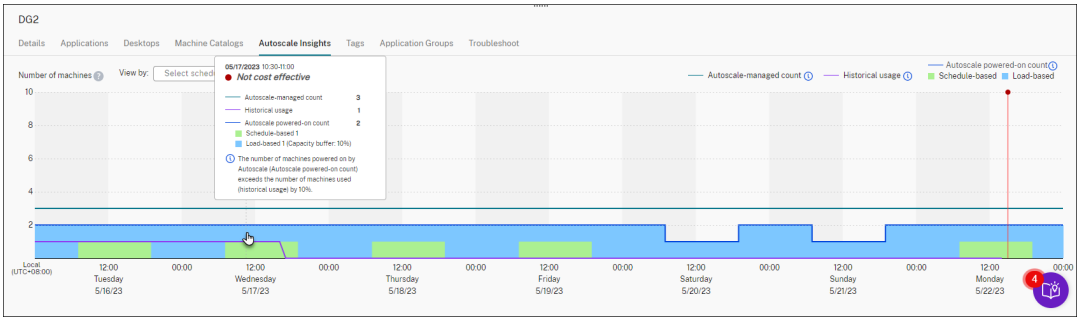
* 赤い縦線は現在時刻を示します。

次の表は、このグラフに表示されるメトリックに関する説明です。

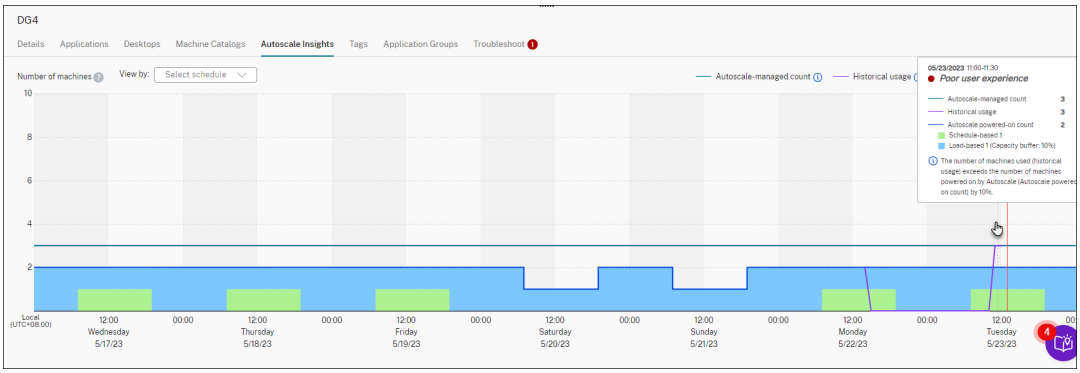
メトリック	説明
Autoscale で管理される数	Autoscale によって管理されるマシンの合計数。Autoscale 管理対象マシン数 = デリバリーグループ内のマシンの合計数–メンテナンスモードのマシン数–Autoscale 用にタグ付けされていないマシン（タグ制限が有効な場合）。
Autoscale による電源オン数	Autoscale によって電源がオンになっているマシンの合計数。Autoscale による電源オン数 = スケジュールベースのマシン数 + 負荷ベースのマシン数。
使用履歴	ユーザーに配信されたマシンの数。
スケジュールベース	Autoscale のスケジュールベースの設定に基づいて電源がオンになっているマシンの数（注：スケジュールベースの設定は、静的なシングルセッション OS タイプのデリバリーグループには適用されません）。
負荷ベース	Autoscale の負荷ベースの設定に基づいて電源がオンになっているマシンの数。

3. 特定の時間帯での Autoscale 設定の有効性を確認するには、グラフ上の該当の時間枠の上にマウスを置きます。情報ボックスが表示され、比較結果と詳細なマシン数が表示されます。

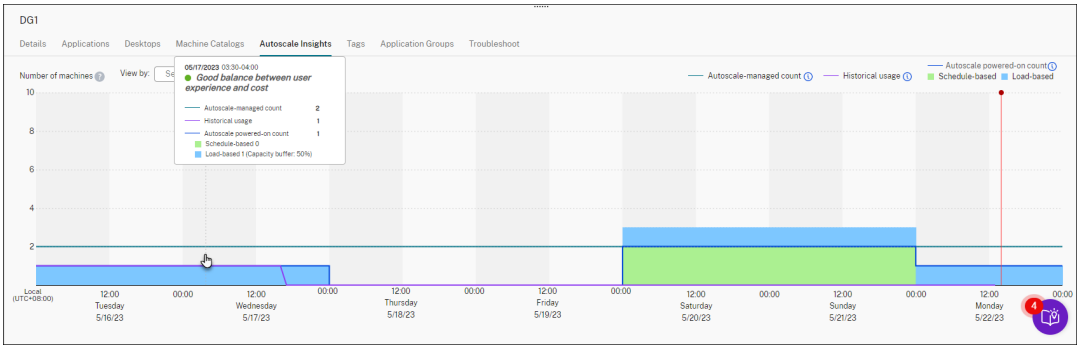
    - 費用対効果が低い。使用履歴は、Autoscale 設定（Autoscale によって電源がオンになった数）の 90% 未満です。その結果、無駄な容量が存在する可能性があります。



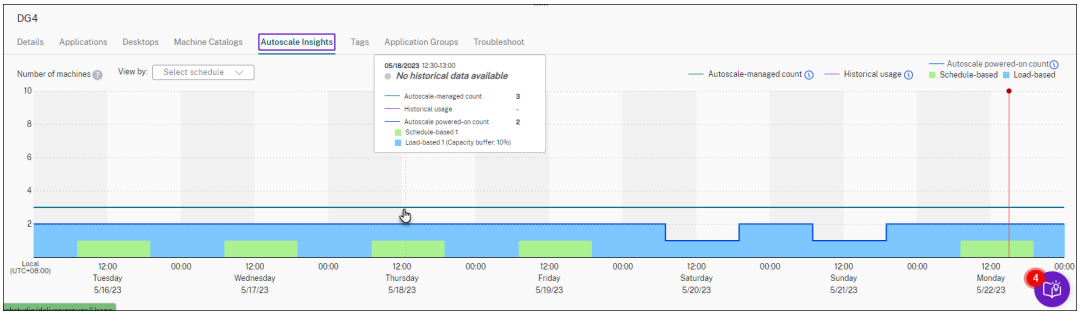
- ユーザーエクスペリエンスの質が低い。使用履歴は、Autoscale 設定（Autoscale によって電源がオンになった数）の 110% を超えています。その結果、マシンの電源がオンになるまでの待ち時間が長くなる可能性があります。



- ユーザーエクスペリエンスとコストのバランスが取れています。使用履歴と Autoscale 設定(Autoscale によって電源がオンになった数）の差は 10% 未満です。Autoscale 設定は、使用履歴に合わせて調整されます。



- 利用可能な履歴データはありません。利用可能な履歴データはありません。考えられる原因は、デリバリーグループに対して Autoscale が有効になってから 1 週間未満であることなどです。



4. Autoscale スケジュールに基づいて日付範囲を強調表示するには、［表示基準］フィールドからスケジュールを選択します。
5. 分析に基づいて Autoscale 設定を調整します。詳しくは、「スケジュールベースおよび負荷ベースの設定」を参照してください。

Broker PowerShell SDK コマンド

November 22, 2023

Broker PowerShell SDK を使用してデリバリーグループの Autoscale を構成できます。PowerShell コマンドを使用して Autoscale を構成するには、Remote PowerShell SDK バージョン 7.21.0.12 以降を使用する必要があります。Remote PowerShell SDK について詳しくは、「SDK および API」を参照してください。

Set-BrokerDesktopGroup

既存の BrokerDesktopGroup の有効化と無効化を切り替えるか、またはグループの設定を変更します。このコマンドレットについて詳しくは、https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/を参照してください。

例

PowerShell コマンドレットの使用方法について詳しくは、以下の例を参照してください:

Autoscale の有効化

- 「MyDesktop」という名前のデリバリーグループに対して Autoscale を有効にする場合、PowerShell コマンドSet-BrokerDesktopGroupを使用します。例:

```
- PS C:\> Set-BrokerDesktopGroup "MyDesktop"-AutoscalingEnabled
  $true
```

ピーク時とオフピーク時で個別に処理能力バッファを構成する

- 「MyDesktop」という名前のデリバリーグループに対して、ピーク時には処理能力バッファを 20% に、オフピーク時には 10% に設定する場合、PowerShell コマンド`Set-BrokerDesktopGroup`を使用します。例:

  ```
  PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakBufferSizePercent
  20 -OffPeakBufferSizePercent 10
  ```

切断時のタイムアウト設定の構成

- 「MyDesktop」という名前のデリバリーグループに対して切断時のタイムアウトの値を、ピーク時には 60 分に、オフピーク時には 30 分に設定する場合、PowerShell コマンド`Set-BrokerDesktopGroup`を使用します。例:

  ```
  PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakDisconnectTimeout
  60 -OffPeakDisconnectTimeout 30
  ```

ログオフ時のタイムアウト設定の構成

- 「MyDesktop」という名前のデリバリーグループに対してログオフ時のタイムアウトの値を、ピーク時には 60 分に、オフピーク時には 30 分に設定する場合、PowerShell コマンド`Set-BrokerDesktopGroup`を使用します。例:

  ```
  PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakLogOffTimeout
  60 -OffPeakLogOffTimeout 30
  ```

電源オフの遅延設定の構成

- 「MyDesktop」という名前のデリバリーグループに対して、電源オフの遅延を 15 分に設定する場合、PowerShell コマンド`Set-BrokerDesktopGroup`を使用します。例:

  ```
  PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PowerOffDelay 15
  ```

電源オフの遅延が有効にならない期間の構成

- 「MyDesktop」という名前のデリバリーグループに対して、電源オフの遅延を 30 分が経過してから有効に設定する場合、PowerShell コマンド`Set-BrokerDesktopGroup`を使用します。例:

  ```
  C:\PS> Set-BrokerDesktopGroup "MyDesktop"-SettlementPeriodBeforeAutoSh
  30。
  ```

マシンインスタンスコスト設定の構成

- 「MyDesktop」という名前のデリバリーグループに対して、1 時間あたりのマシンインスタンスコストを 0.2 ドルに設定する場合、PowerShell コマンド`Set-BrokerDesktopGroup`を使用します。例:

  ```
  PS C:\> Set-BrokerDesktopGroup "MyDesktop"-MachineCost 0.2
  ```


New-BrokerPowerTimeScheme

デリバリーグループ用に BrokerPowerTimeScheme を作成します。詳しくは、https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerPowerTimeScheme/を参照してください。

例

UID 値が 3 のデリバリーグループに対して、電源時間スキームを作成する場合、新しいスキームで週末、月曜日、火曜日を指定します。これらの曜日で、午前 8:00 から午後 6:30 の時間枠をピーク時間として定義します。ピーク時のプールサイズ（電源をオンにしたままにするマシンの数）は 20 で、オフピーク時は 5 です。PowerShell コマンドのSet-BrokerDesktopGroupを使用できます。例:

- `PS C:\> $ps48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37){ 5 } else { 20 } } )`
- `PS C:\> $pt48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37){ $false } else { $true } } )`
- `PS C:\> New-BrokerPowerTimeScheme -Name 'First Half Week'-DaysOfWeek Weekend,Monday,Tuesday -DesktopGroupUid 3 -PeakHalfHours $pt48 -PoolSize $ps48`

動的セッションタイムアウトのパラメーター

次の Broker PowerShell SDK コマンドレットは、動的セッションタイムアウト用に拡張され、複数の新しいパラメーターをサポートします:

- Get-BrokerDesktopGroup
- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup

これらのパラメーターには次が含まれます:

- **DisconnectPeakIdleSessionAfterSeconds** - ピーク時にアイドル状態のセッションが切断されるまでの時間を秒単位で表します。このプロパティのデフォルト値は 0 です。これは、関連する動作がピーク時に無効になっていることを示します。0 より大きい値は、ピーク時のデリバリーグループの動作のみを有効にします。
- **DisconnectOffPeakIdleSessionAfterSeconds** - オフピーク時にアイドル状態のセッションが切断されるまでの時間を秒単位で表します。このプロパティのデフォルト値は 0 です。これは、関連する動作がオフピーク時に無効になっていることを示します。0 より大きい値は、オフピーク時のデリバリーグループの関連する動作のみを有効にします。

- **LogoffPeakDisconnectedSessionAfterSeconds** - ピーク時に切断されたセッションが終了するまでの時間を秒単位で表します。このプロパティのデフォルト値は 0 です。これは、関連する動作がピーク時に無効になっていることを示します。0 より大きい値は、ピーク時のデリバリーグループの関連する動作のみを有効にします。
- **LogoffOffPeakDisconnectedSessionAfterSeconds** - オフピーク時に切断されたセッションが終了するまでの時間を秒単位で表します。このプロパティのデフォルト値は 0 です。これは、関連する動作がオフピーク時に無効になっていることを示します。0 より大きい値は、オフピーク時のデリバリーグループの関連する動作のみを有効にします。

例

「MyDesktop」という名前のデリバリーグループについて、ピーク時のアイドル状態セッションタイムアウトを 3,600 秒に設定するとします。PowerShell コマンド`Set-BrokerDesktopGroup`を使用します。例:

- `C:\PS> Set-BrokerDesktopGroup "MyDesktop"-DisconnectOffPeakIdleSessionAfte`
  `3600`

これにより、「MyDesktop」という名前のデスクトップグループで、オフピーク時に 1 時間を超えてアイドル状態になっているセッションが切断されます。

Cloud Health Check

December 12, 2022

> 注:
>
> Cloud Health Check は Citrix DaaS に統合されています。この機能は、［完全な構成］管理インターフェイスの［ヘルスチェックの実行］で使用できます。詳しくは、「VDA 登録とセッション起動の問題のトラブルシューティング」を参照してください。

Cloud Health Check では、サイトとそのコンポーネントの正常性と可用性を測定するチェックを実行できます。実行できるのは、Virtual Delivery Agent（VDA）、StoreFront サーバー、および Profile Management のヘルスチェックです。VDA のヘルスチェックは、一般的な VDA 登録およびセッションの起動の問題を引き起こす原因となるものを見つけ出します。

チェック中に問題が見つかった場合、Cloud Health Check は詳細なレポートと問題を修正するためのアクションを提供します。Cloud Health Check が開始される際は毎回、コンテンツ配信ネットワーク（CDN）上のスクリプトのバージョンが最新かどうかチェックされ、ローカルマシン上に最新のスクリプトが存在しない場合は自動でダウンロードされます。Cloud Health Check では、常に最新のローカルバージョンのスクリプトを選択してヘルスチェックを実行します。

> 注:
>
> Cloud Health Check は、実行するたびに更新されるわけではありません。

Citrix Cloud 環境では、ドメイン参加済みマシンから Cloud Health Check を起動して、1 つ以上の VDA または StoreFront サーバーでチェックを実行します。

> 注:
>
> Cloud Connector で Cloud Health Check をインストールまたは実行することはできません。

Cloud Health Check アプリケーションのログは`C:\ProgramData\Citrix\TelemetryService\CloudHealthCheck.log`に保存されます。このファイルは、トラブルシューティングに使用できます。

Cloud Health Check の概要を表示します。

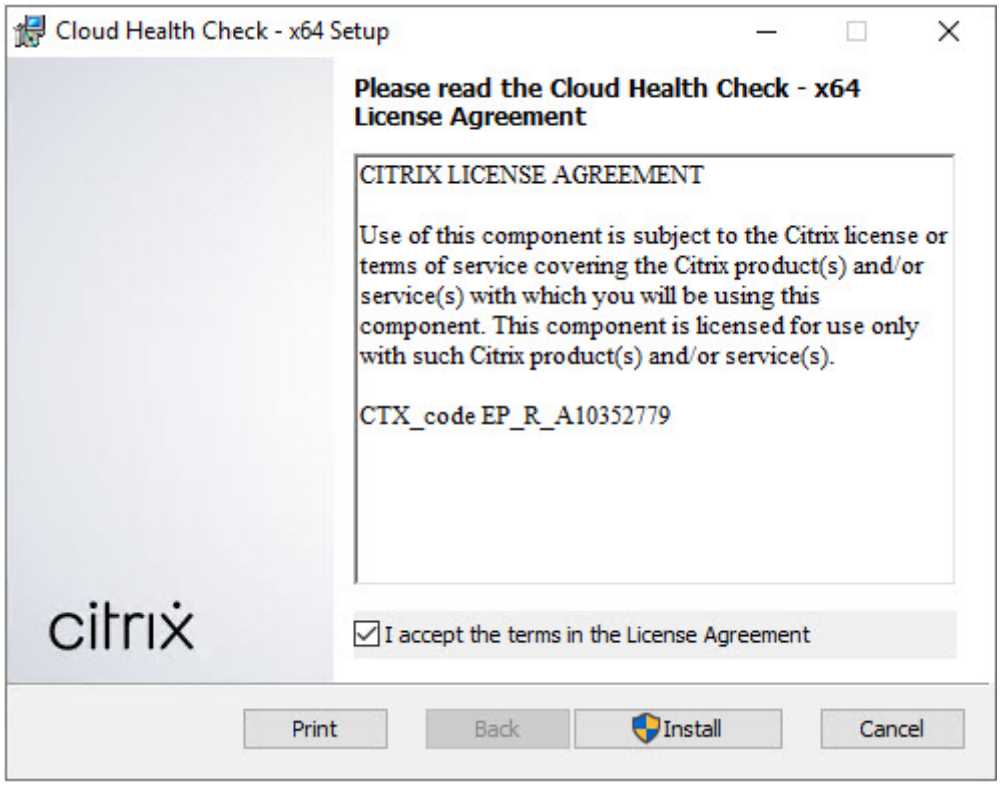
Cloud Health Check をいつ使用するかを表示します。

インストール

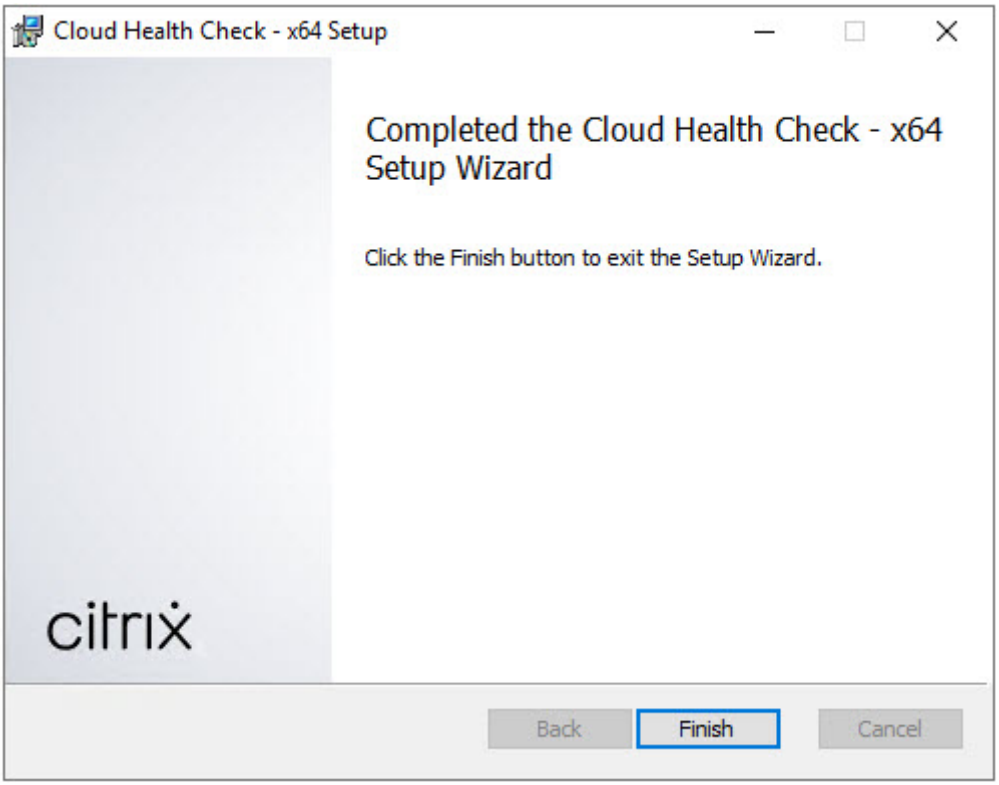
Cloud Health Check をインストールするための環境を準備するには、ドメイン参加済みの Windows マシンが必要です。

> 注:
>
> Cloud Connector で Cloud Health Check をインストールまたは実行することはできません。

1. ドメイン参加済みのマシンで、Cloud Health Check インストーラーをダウンロードします。
2. CloudHealthCheckInstaller_x64.msi をダブルクリックします。
3. ボックスをオンにして規約に同意します。
4. ［インストール］をクリックします。



5. インストールが完了したら、［完了］をクリックします。



権限と要件

アクセス許可:

- ヘルスチェックを実行するには、以下の条件を満たしている必要があります:
  - ドメインユーザーグループのメンバーである必要があります。
  - すべての権限を持つ管理者であるか、対象サイトに対する読み取り専用の権限と ［環境テストの実行］権限があるカスタムの役割が付与されている必要があります。
  - スクリプトを実行するには、スクリプトの実行ポリシーを`RemoteSigned`またはそれ以上に設定する必要があります。例: `Set-ExecutionPolicy RemoteSigned`。注: 他のスクリプト実行権限も同様に機能します。
- Cloud Health Check の起動時には ［管理者として実行］を使用してください。

ヘルスチェックを実行する VDA または StoreFront マシンは、すべて以下の要件を満たす必要があります:

- OS は 64 ビットである必要があります。
- Cloud Health Check がマシンと通信できる必要があります。
- ファイルとプリンターの共有は設定されている必要があります。
- PSRemoting と WinRM は有効になっている必要があります。PowerShell 3.0 以降が実行されている必要もあります。
- Windows Management Infrastructure（WMI）へのアクセスが有効になっている必要があります。

ヘルスチェックについて

ヘルスチェックデータは`C:\ProgramData\Citrix\TelemetryService\`の下のフォルダーに保存されます。

VDA のヘルスチェック

VDA への登録について、Cloud Health Check は以下をチェックします:

- VDA ソフトウェアのインストール状況
- VDA マシンドメインへの参加状況
- VDA の通信ポートの可用性
- VDA サービスの状態
- Windows ファイアウォールの構成
- Controller との通信
- Controller との時刻同期
- VDA の登録状態

VDA でのセッション開始について、Cloud Health Check は以下をチェックします:

- セッション開始時の通信ポートの可用性
- セッション開始時のサービスの状態
- セッション開始時の Windows ファイアウォールの構成
- VDA リモートデスクトップサービスのクライアントアクセスライセンス
- VDA のアプリケーション起動パス
- セッションの起動レジストリ設定
- Citrix ユニバーサルインジェクションドライバー（CTXUVI）のステータス

VDA の Profile Management では、Cloud Health Check は以下をチェックします:

- ハイパーバイザーの検出
- プロビジョニングの検出
- Citrix Virtual Apps and Desktops
- Personal vDisk の構成
- ユーザーストア
- Profile Management サービスの状態検出
- Winlogon.exe のフックテスト

Profile Management でチェックを実行するには、VDA に Profile Management をインストールして有効にする必要があります。Profile Management の構成チェックについて詳しくは、Knowledge Center のCTX132805を参照してください。

StoreFront ヘルスチェック

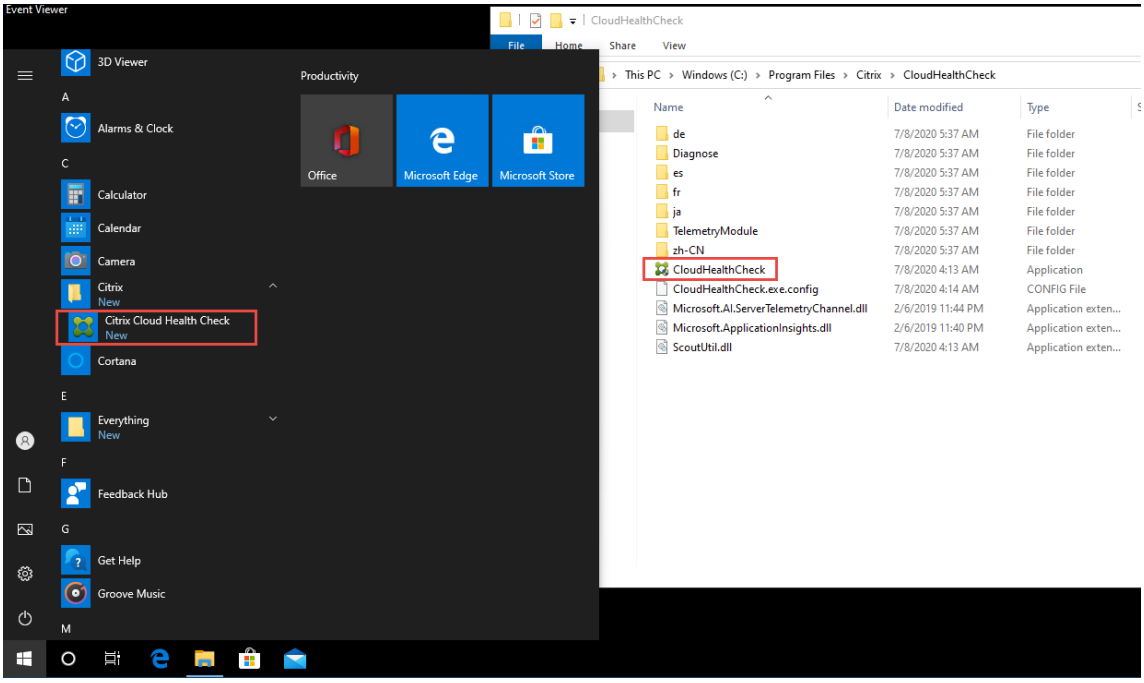
StoreFront チェックでは以下が確認されます:

- Citrix デフォルトドメインサービスが実行されている
- Citrix Credential Wallet サービスが実行されている
- StoreFront サーバーから Active Directory への接続にポート 88 が使用されている
- StoreFront サーバーから Active Directory への接続にポート 389 が使用されている
- StoreFront サーバーから Active Directory への接続にポート 464 が使用されている
- ベース URL の FQDN が有効である
- ベース URL からの正しい IP アドレスを取得できる
- IIS アプリケーションプールで.NET 4.0 を使用している
- 証明書がホスト URL の SSL ポートにバインドされている
- 証明書チェーンが完全である
- 証明書の有効期限が切れている
- 証明書の有効期限切れが 30 日以内である

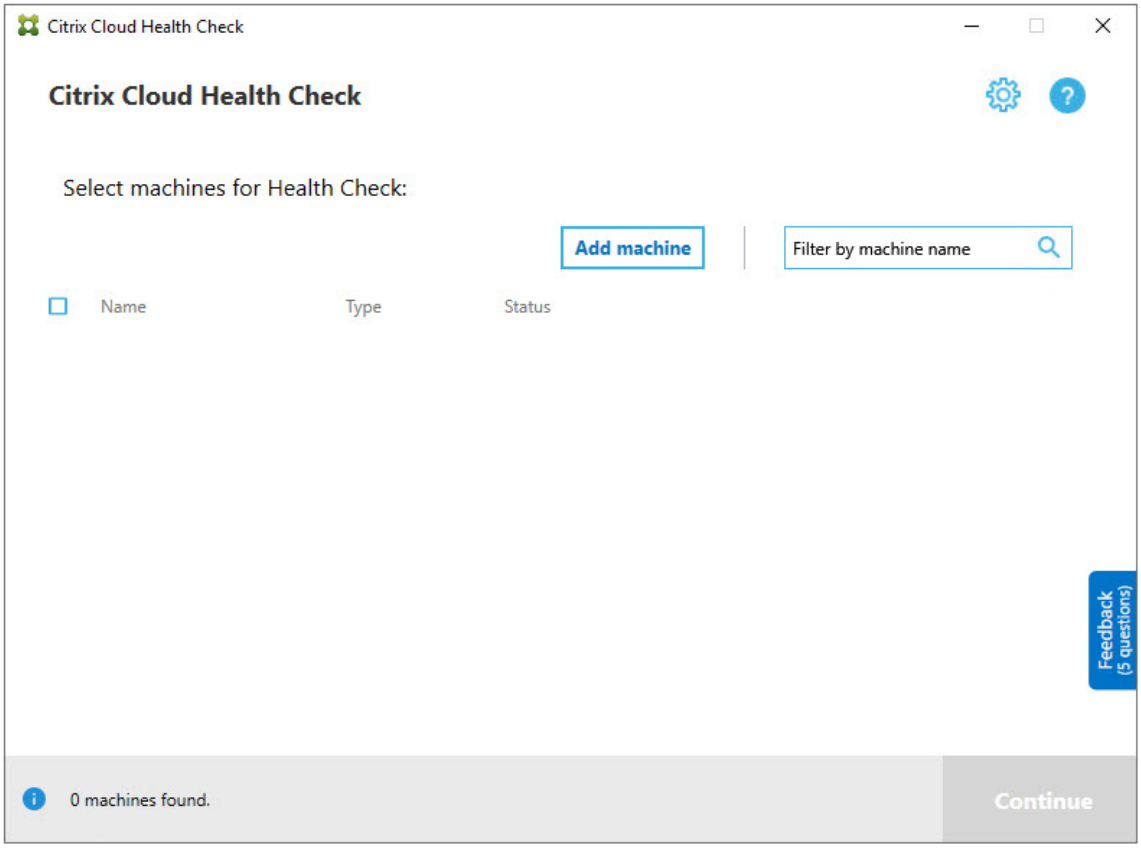
Cloud Health Check の実行

Citrix Cloud Health Check を実行するには次の手順に従います:

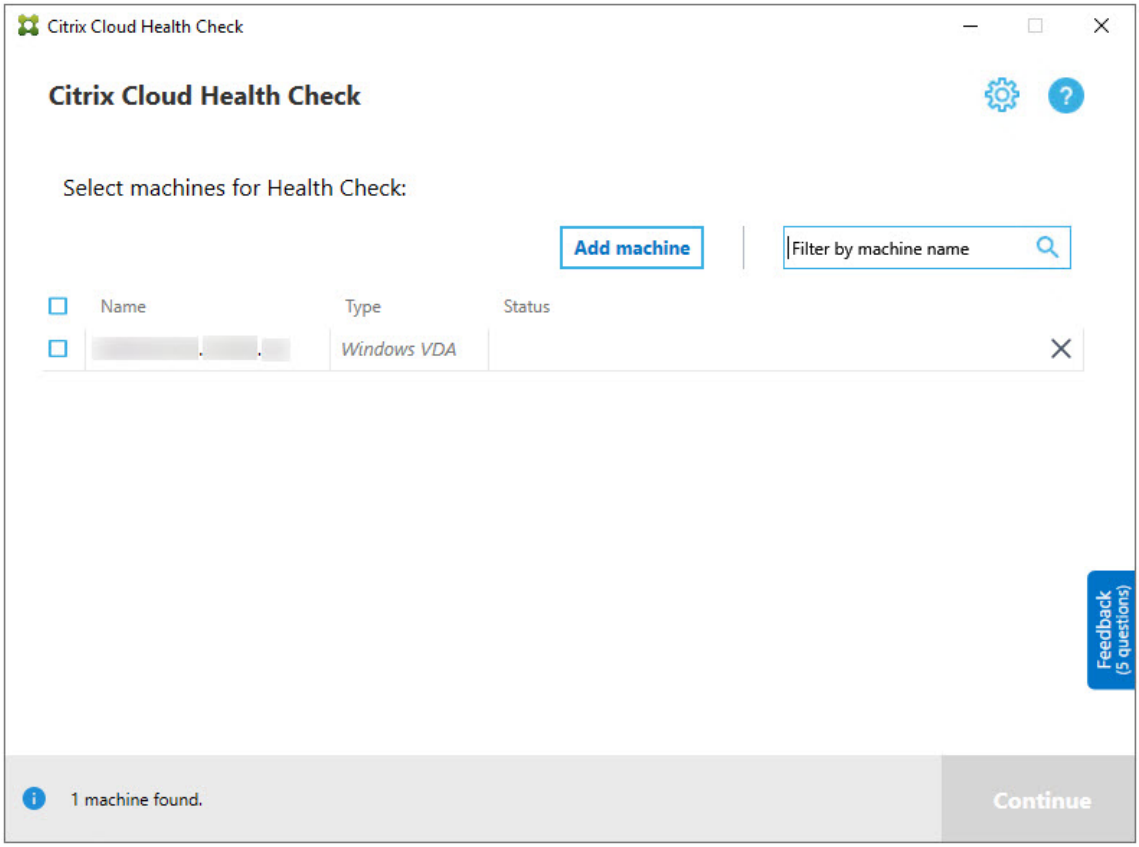
1. マシンの［スタート］メニューから［**Citrix**］**>**［**Citrix Cloud Health Check**］を選択するか、または、`C:\Program Files\Citrix\CloudHealthCheck`で`CloudHealthCheck.exe`を実行します。



2. Cloud Health Check のメイン画面で、［マシンの追加］をクリックします。



3. 追加するマシンの完全修飾ドメイン名を入力します。注：完全修飾ドメイン名の代わりに DNS エイリアスを入力しても有効に見える場合がありますが、ヘルスチェックは失敗する可能性があります。
4. ［続行］をクリックします。
5. 必要に応じて、他のマシンの追加を繰り返します。



6. 手動で追加したマシンを削除するには、行の右端にある ［**X**］をクリックして削除を確定します。手動で追加した他のマシンの削除を繰り返します。

Cloud Health Check は、削除されるまで、手動で追加されたマシンを覚えています。Cloud Health Check を閉じてから再び開くと、手動で追加したマシンはそのまま一覧の一番上に表示されています。

VDA マシンのインポート

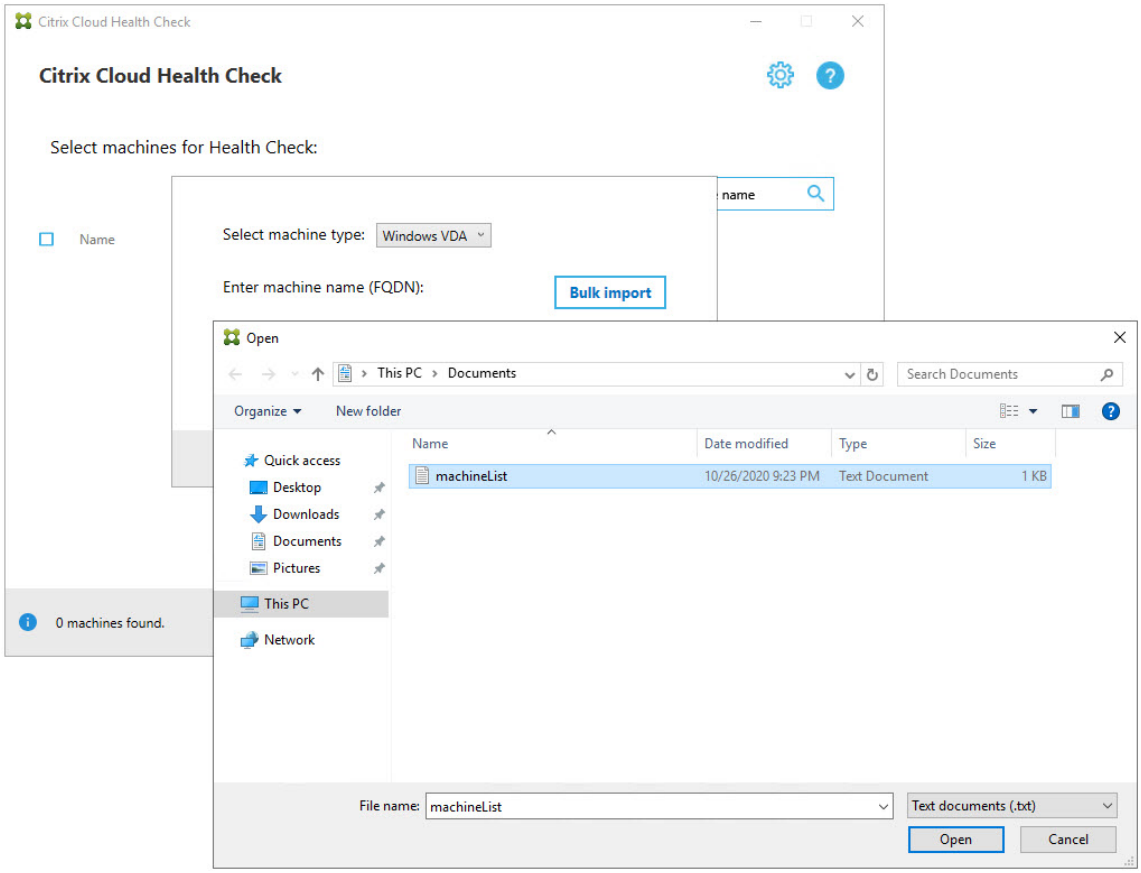
ヘルスチェックを実行するとき、VDA マシンを環境にインポートできます。

1. Connector で、以下の PowerShell コマンドを使用してマシンリストファイルを生成します。Connector では、Citrix 資格情報を入力し、ポップアップダイアログで顧客を選択する必要があります。

```
Get-BrokerMachine| foreach { $_.DnsName } | out-file C:\machineList.
txt
```

1. machineList.txt ファイルを、Cloud Health Check を起動するドメイン参加済みマシンにコピーします。
2. ［Cloud Health Check］ページで、［マシンの追加］をクリックします。
3. マシンの種類で［Windows VDA］を選択します。
4. ［**VDA** マシンのインポート］をクリックします。

5. machineList.txt ファイルを選択します。
6. ［開く］をクリックします。



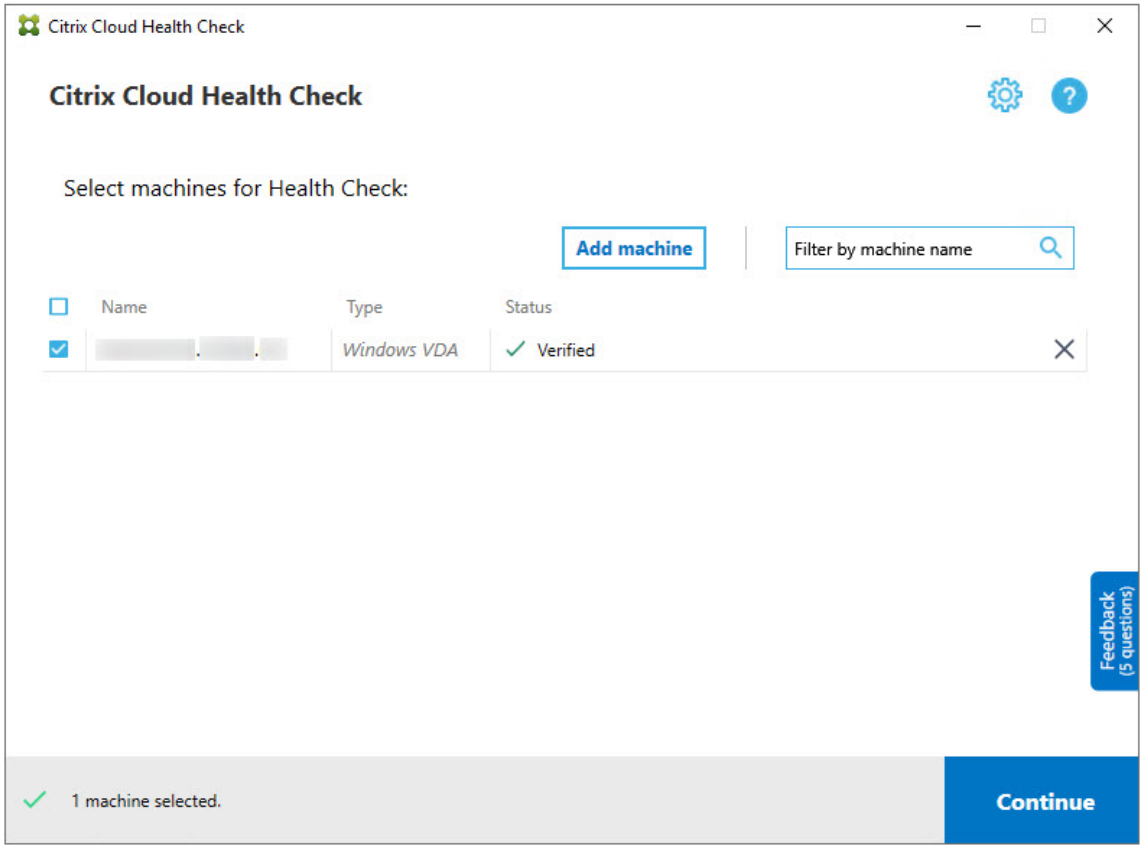
インポートされた VDA マシンは、［Cloud Health Check］ページに一覧表示されます。

7. ヘルスチェックを実行する各マシンの横にあるチェックボックスをオンにします。

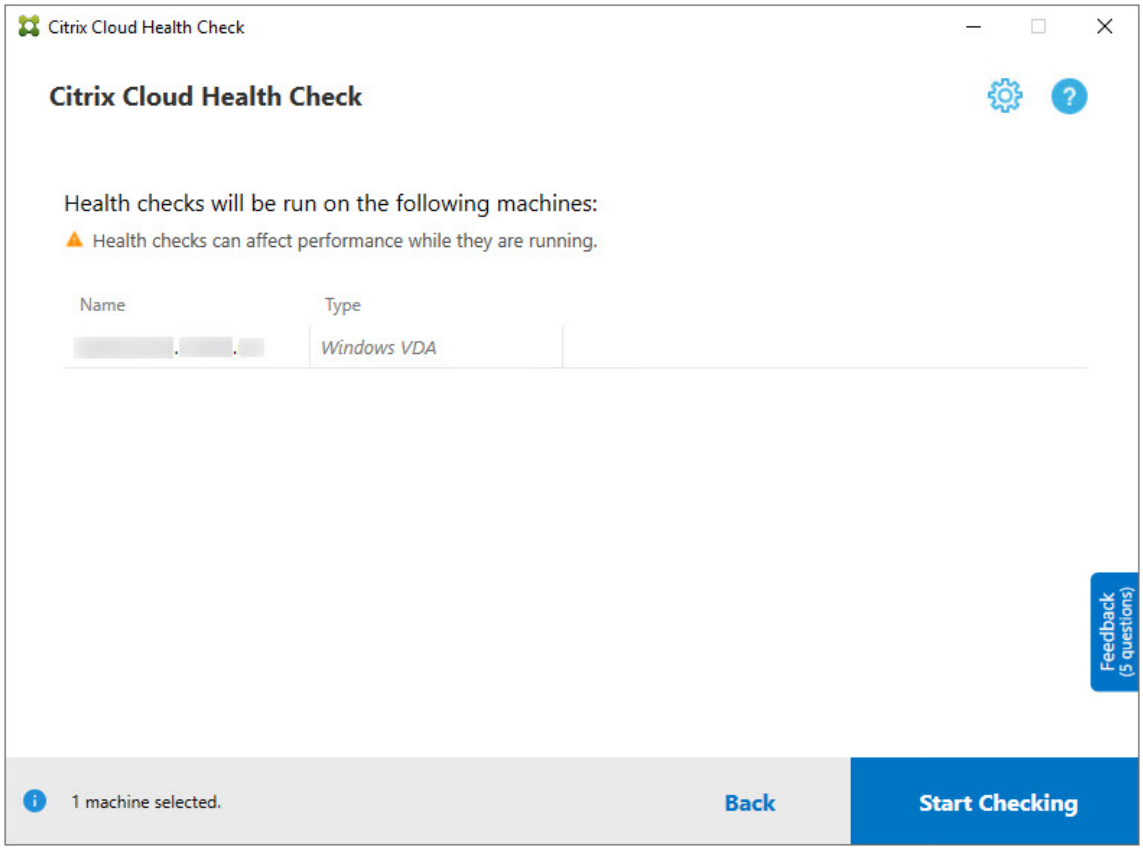
   選択した各マシン上で確認テストが自動で開始され、各マシンが確認テストに記載されている基準を満たしているか確認されます。確認テストで不合格になると、［状態］列にメッセージが表示され、該当するマシンのチェックボックスがオフになります。その後、次のことができます:

   - 問題を解決して該当するマシンのチェックボックスを再びオンにします。このようにすると、確認テストが再び行われます。
   - チェックボックスをオフのままにして、該当するマシンを収集対象から除外します。そのマシンのヘルスチェックは実行されません。

8. 確認テストが完了したら、［続行］をクリックします。

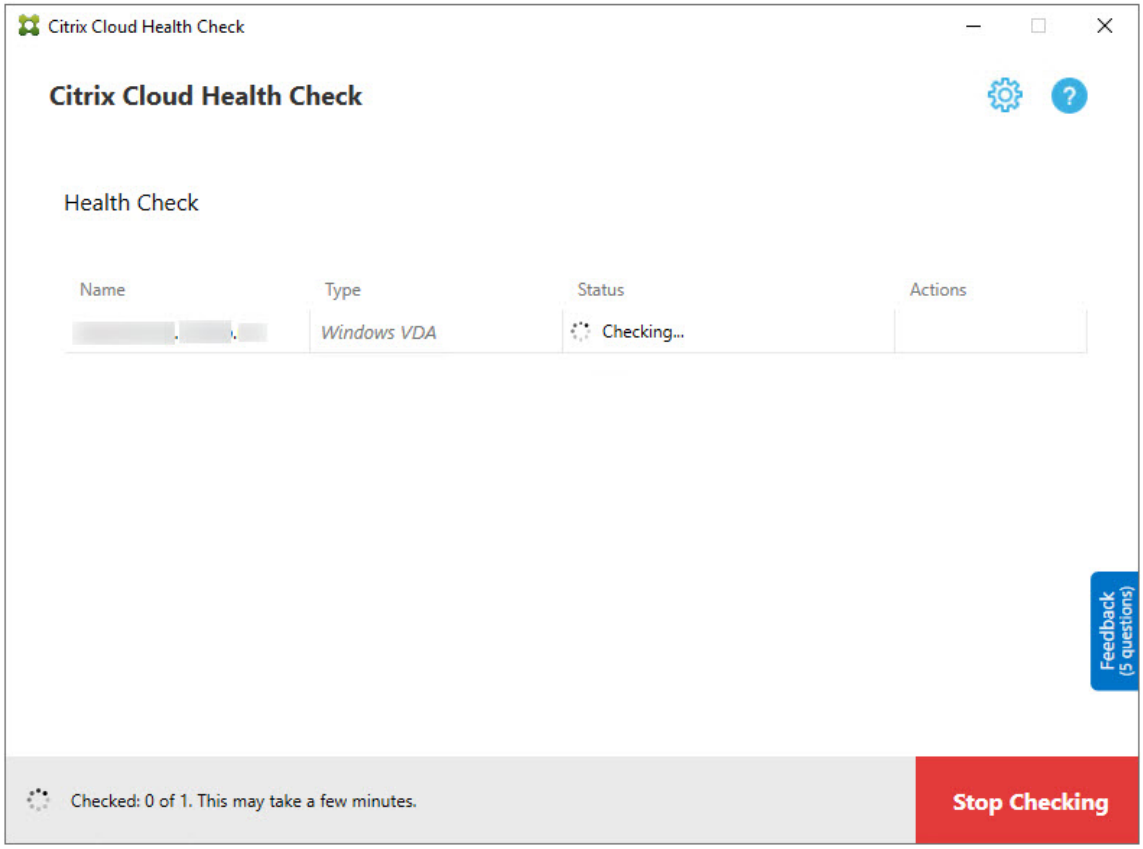


9. 選択したマシンのヘルスチェックを実行します。概要に、ヘルスチェックが実行されるマシン（選択し、確認テストに合格したマシン）が一覧表示されます。
10. ［チェックの開始］をクリックします。

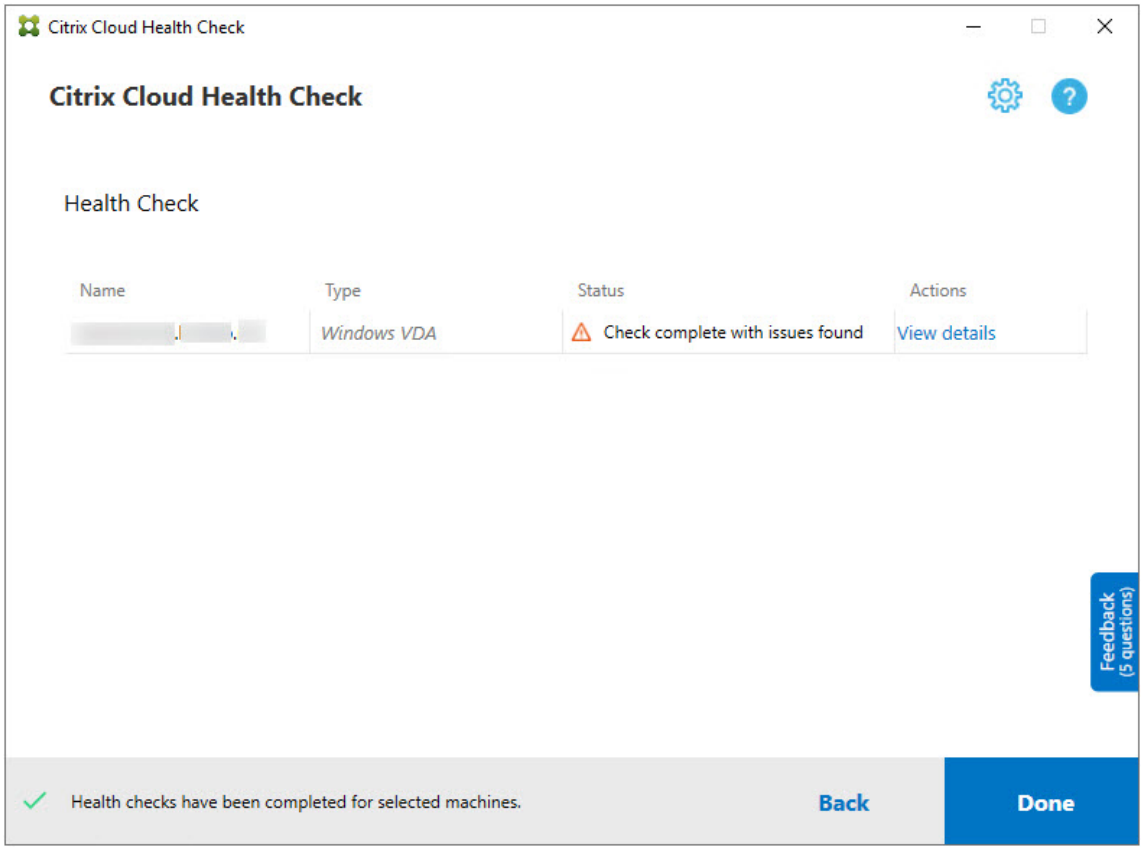


チェック中およびチェック後、［状態］列には、マシンの現在のチェック状態が表示されます。

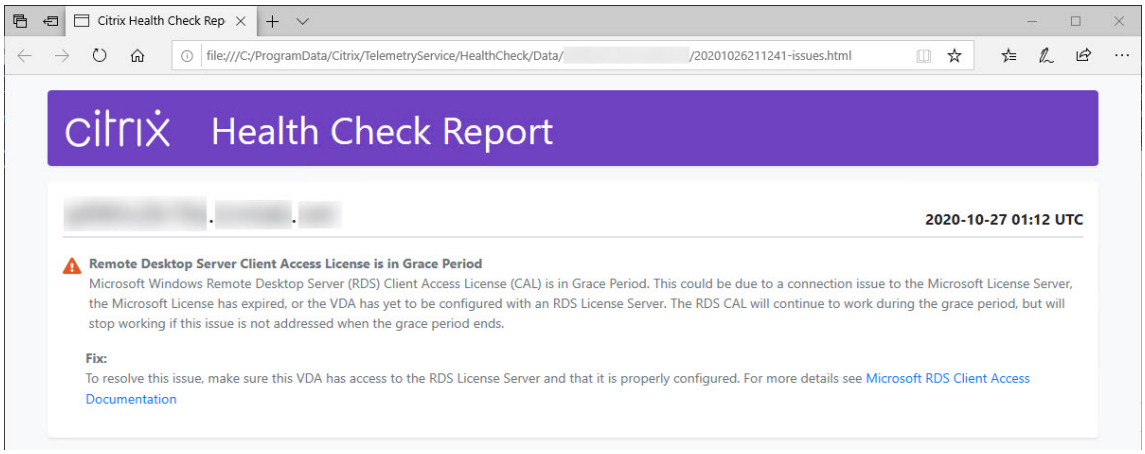
11. 進行中のチェックをすべて停止するには、ページの右下隅にある ［チェックの停止］をクリックします。ヘルスチェックの取り消しはチェック対象のマシン全台に適用されます。マシン単体を選んで取り消すことはできません。



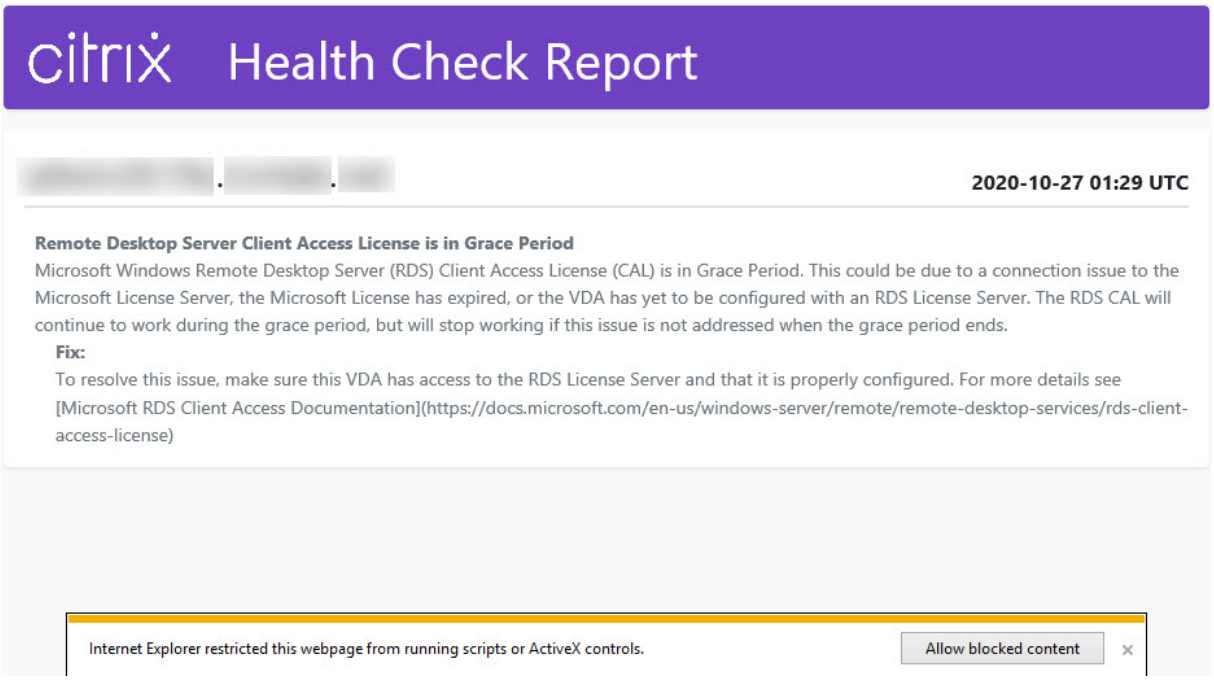
12. すべての選択したマシンでチェックが完了すると、右下隅にある［チェックの停止］が［完了］に変わります。



- チェックが失敗した場合は、［操作］列の ［再試行］をクリックできます。
- チェックが完了しても問題が見つからなかった場合は、［操作］列には何も表示されません。
- チェックで問題が見つかった場合は、［詳細の表示］で結果を確認できます。



Internet Explorer を使用してレポートを表示する場合、ハイパーリンクを表示するには、［ブロックされているコンテンツを許可］をクリックする必要があります。



選択したすべてのマシンでチェックが完了した後に ［戻る］をクリックすると、チェック結果が失われます。

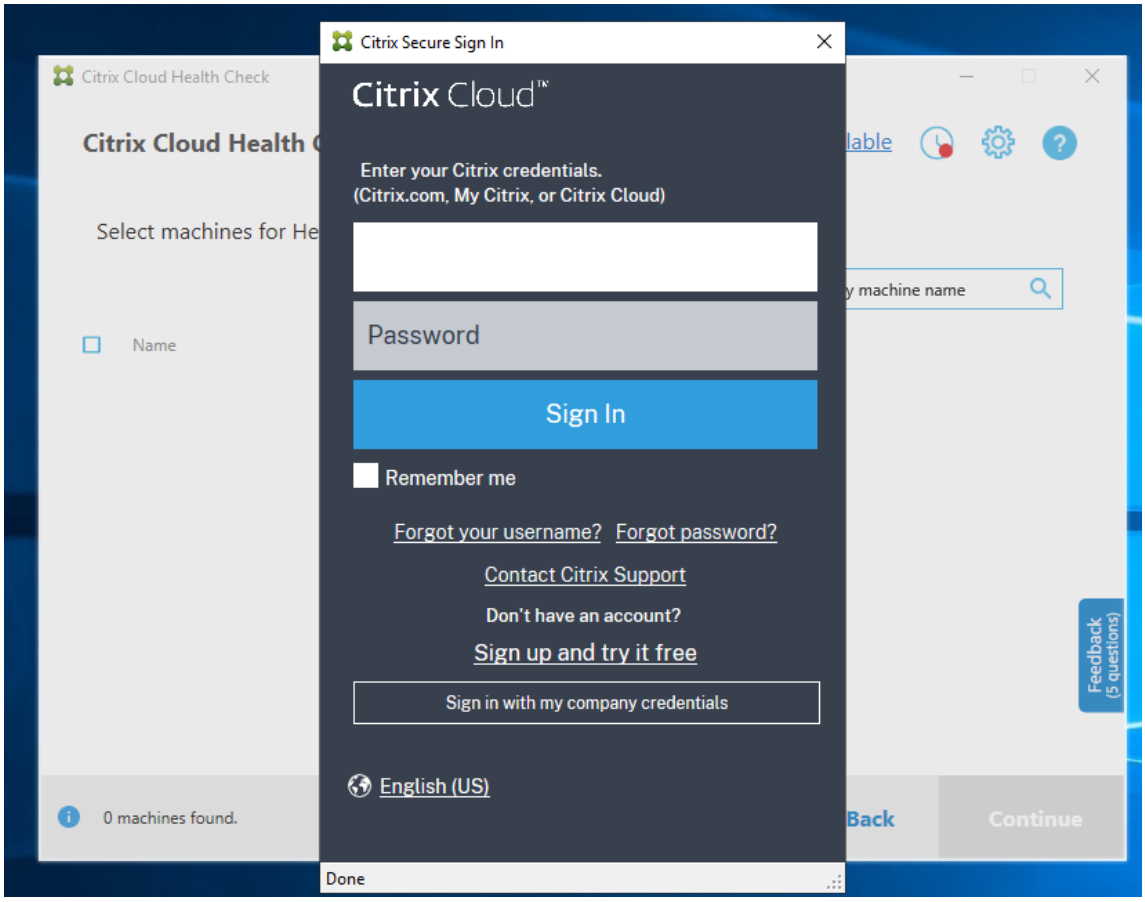
チェックが完了したら ［完了］をクリックして、Cloud Health Check のメイン画面に戻ります。

VDA マシンの取得

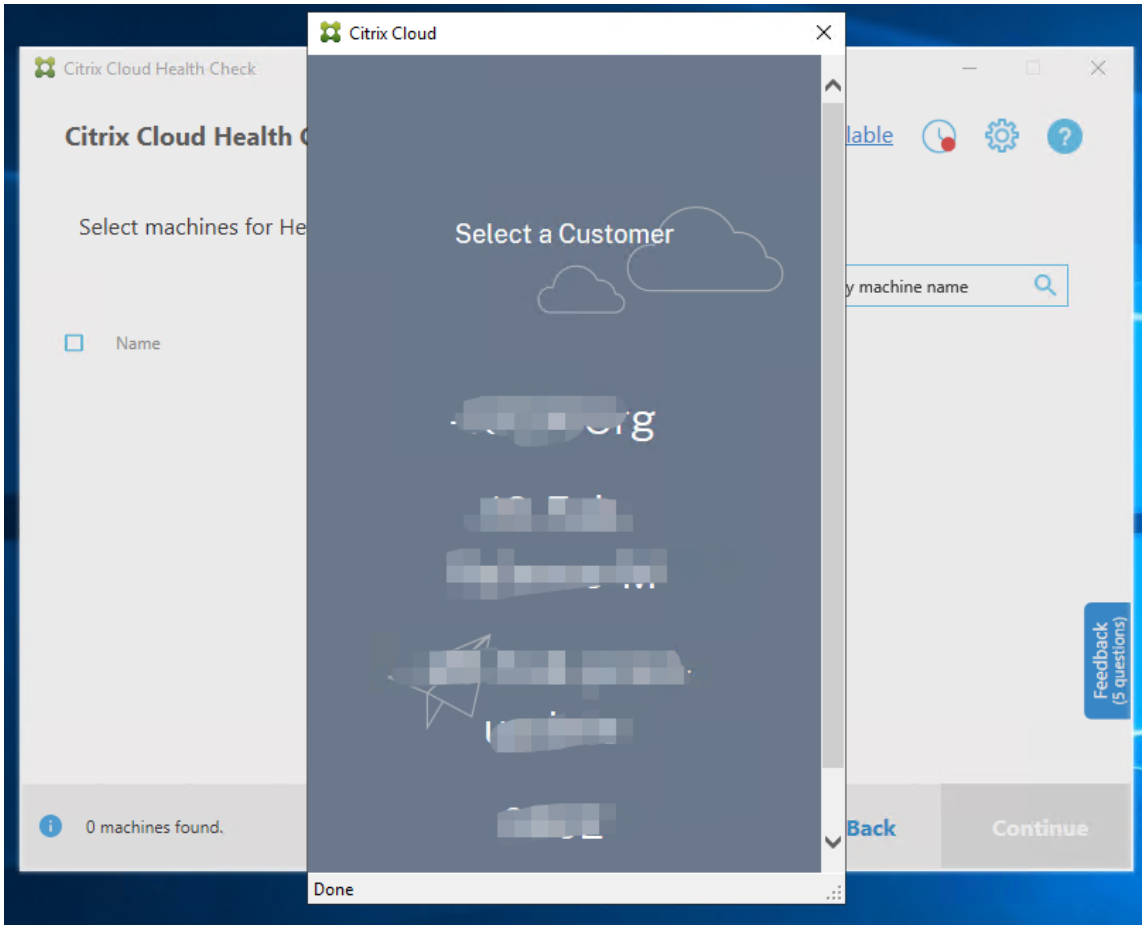
Cloud Health Check は、Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）展開から VDA を自動的に検出して取得できます。

VDA を取得するには:

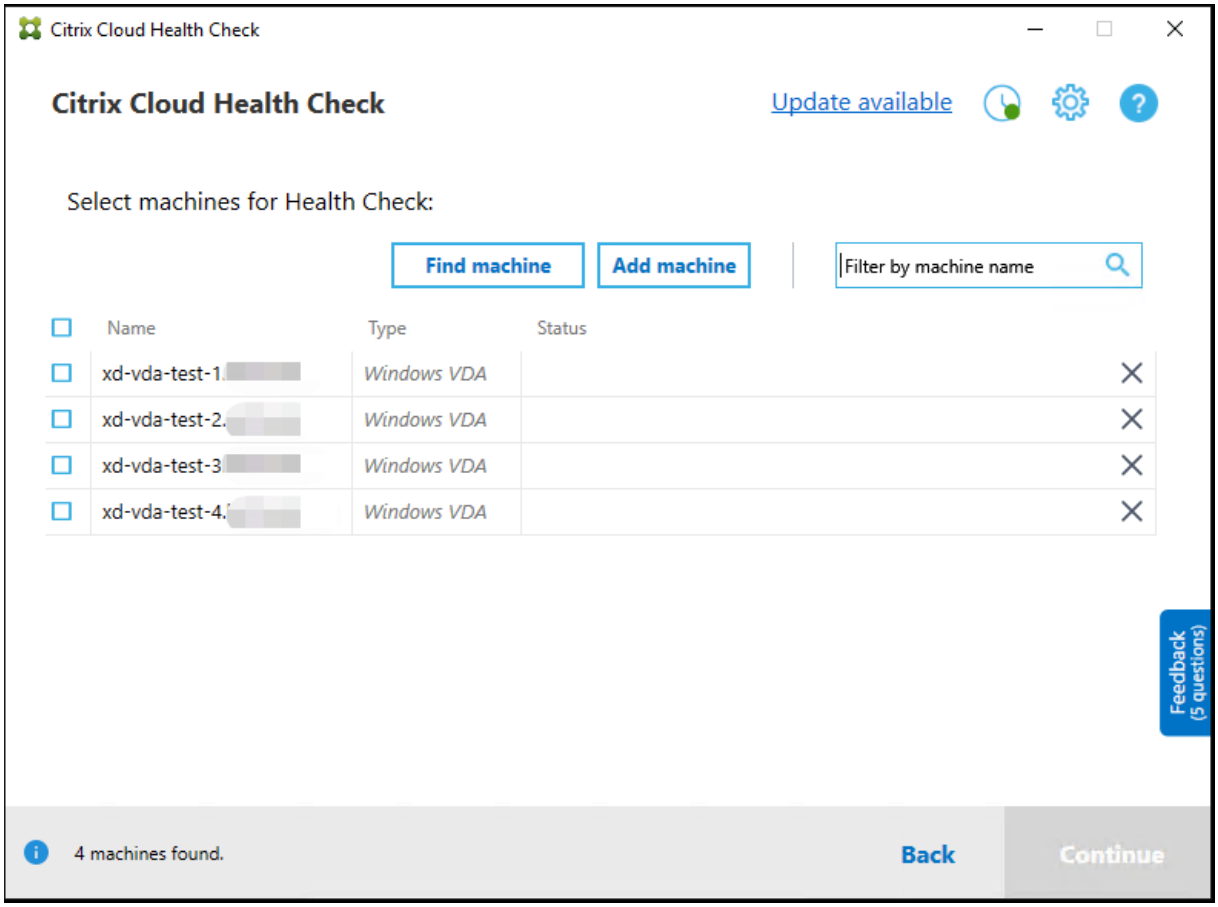
1. Cloud Health Check が実行されているマシンと同じドメインフォレストに参加している新しいマシンを準備します。
2. Cloud Health Check を開き、［マシンの検索］をクリックして Citrix Cloud にサインインします。



3. 取得するクラウドサイトを持つ顧客を選択します。

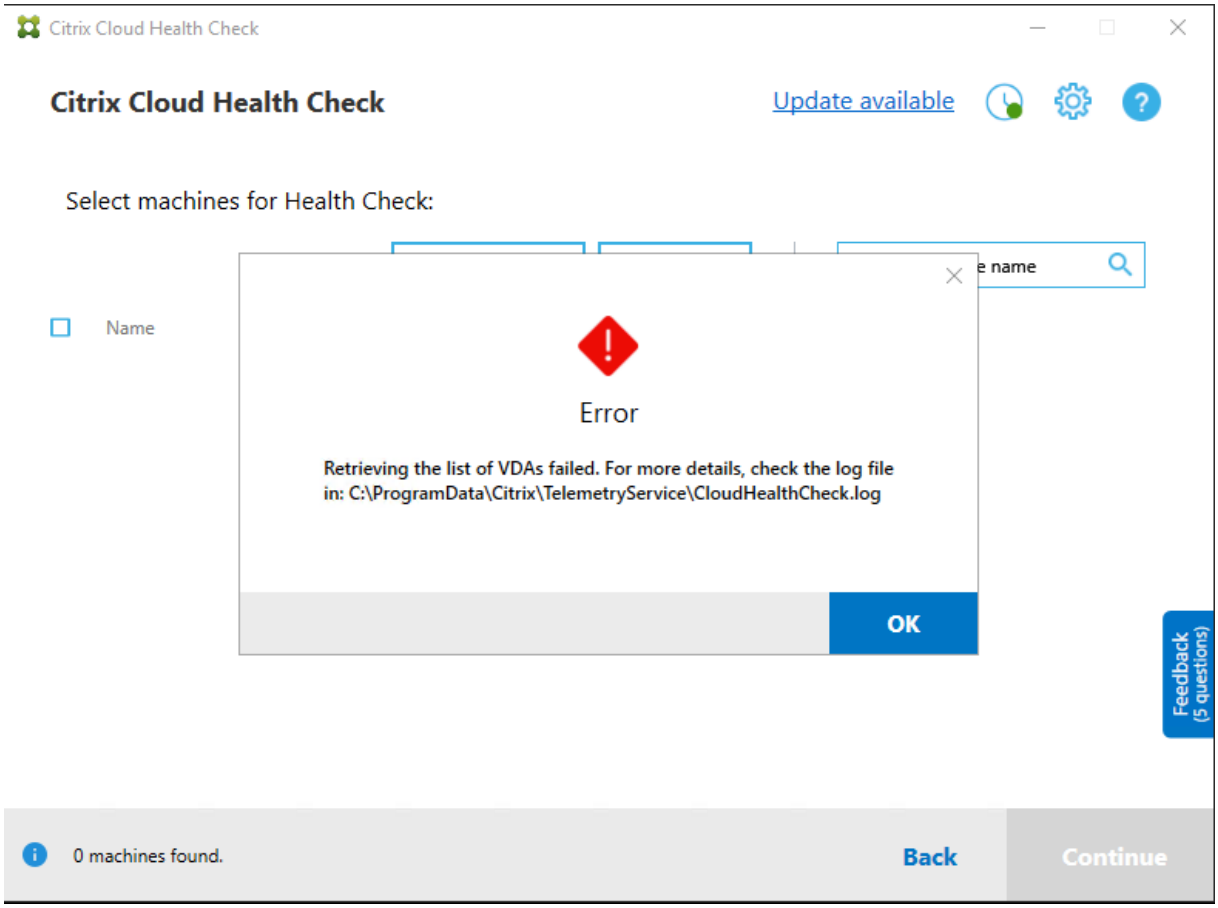


VDA リストが Cloud Health Check に表示されます。リストは、\ProgramData\Citrix\TelemetryService\ChcDiscovery\ChcDiscoveredMachineList.jsonにあるローカルファイルにも保存されます。



Cloud Health Check を再度開くと、マシンリストにローカルキャッシュが読み込まれます。利用環境で更新を行った場合は、［マシンの検索］をクリックしてマシンリストを更新する必要があります。

> 注:
>
> - Cloud Health Check は、Cloud Health Check が実行されているマシンと同じドメインフォレスト内のマシンのみを検出します。
> - Citrix Cloud のセッションは 1 時間で期限切れになります。1 時間後に最新の VDA リストを取得する場合は、［マシンの検索］を再度クリックする必要があります。
> - VDA リストの取得に失敗すると、エラーメッセージが表示されます。詳細は、`C:\ProgramData\Citrix\TelemetryService\CloudHealthCheck.log`で確認できます。



ヘルスチェックの結果

レポートを生成するヘルスチェックには、次の要素が含まれます:

- 結果レポートが生成された日時
- チェックされたマシンの完全修飾ドメイン名
- チェック対象マシンでチェックされた条件

コマンドラインで **Cloud Health Check** を実行する

Cloud Health Check をコマンドラインで実行して、顧客がヘルスチェックを実行できるようにすることができます。コマンドラインで Cloud Health Check を使用するには、Cloud Health Check が実行されているマシンの管理者である必要があります。

> 注:
>
> コマンドラインで Cloud Health Check を使用する場合、一度にチェックできるマシンは 1 つだけです。ターゲットマシンで同時に実行できる`CloudHealthCheck.exe`のインスタンスは 1 つだけです。複数の

> マシンをチェックする場合は、コマンドレットをコマンドレット/PowerShell スクリプトのループでラップして、マシンを 1 つずつチェックする必要があります。開いている Cloud Health Check の UI インスタンスもすべて閉じる必要があります。

コマンドレット

サポートされているコマンドラインコマンドレットは次のとおりです:

- `MachineFQDN` - このコマンドレットは必須です。これは、ターゲットマシンの完全修飾ドメイン名です。
- `MachineType` - このコマンドレットはオプションです。コマンドレットの値は、Windows VDA（デフォルト値）または StoreFront にすることができます。
- `ReportName` - このコマンドレットはオプションです。コマンドレットの値は、Windows で有効なファイル名である必要があります。デフォルトの値は`HealthCheckReport`です。
- `SkipAdminCheck` - このコマンドレットはオプションです。これを追加すると、管理者権限が必要なチェックをスキップできます。
- `UpdateScripts` - このコマンドレットはオプションです。これを追加すると、CDN サーバーからチェックスクリプトを更新できます。
- `DisableCeip` - このコマンドレットは、UI で CEIP が有効になっている場合はオプションであり、追加すると CEIP が無効になります。
- `Help` - パラメーターに関するヘルプ情報を表示します。

例:

```
HealthCheckCLI.exe -MachineFQDN machine.domain.local

HealthCheckCLI.exe -MachineFQDN machine.domain.local -ReportName
checkreport

HealthCheckCLI.exe -MachineFQDN machine.domain.local -SkipAdminCheck


HealthCheckCLI.exe -MachineFQDN machine.domain.local -UpdateScripts

HealthCheckCLI.exe -MachineFQDN machine1.domain.local,machine2.domain
.local,machine3.domain.local

HealthCheckCLI.exe -Help
```

> 注:
>
> パラメーター名では大文字と小文字は区別されません。

デフォルトでは、コンソール出力はコマンドラインコンソールウィンドウに表示されません。コマンドレットに「`|more`」を追加することで、出力を手動で表示できます。

例: `HealthCheckCLI.exe -MachineFQDN machine.domain.local|more`

コマンドラインのデフォルトを実行するには、管理者権限が必要です。-SkipAdminCheckのパラメーターを追加すると、管理者権限の必要性が上書きされます。

終了コード

終了コードは、コマンドライン内で Cloud Health Check のチェック結果を説明します。終了コードを取得するには、コマンドレットの前に「start /wait」を追加する必要があります。

例: `start /wait HealthCheckCLI.exe -MachineFQDN machine.domain.local`

終了コードは次のとおりです:

- 0 - 正常、チェックが完了して合格。
- 1 - 失敗、問題のある状態でチェックが完了。
- 2 - エラー、エラーがありチェックが未完了。

コマンドレット「echo %errorlevel%」で、最後に実行されたコマンドの終了コードを取得することもできます。

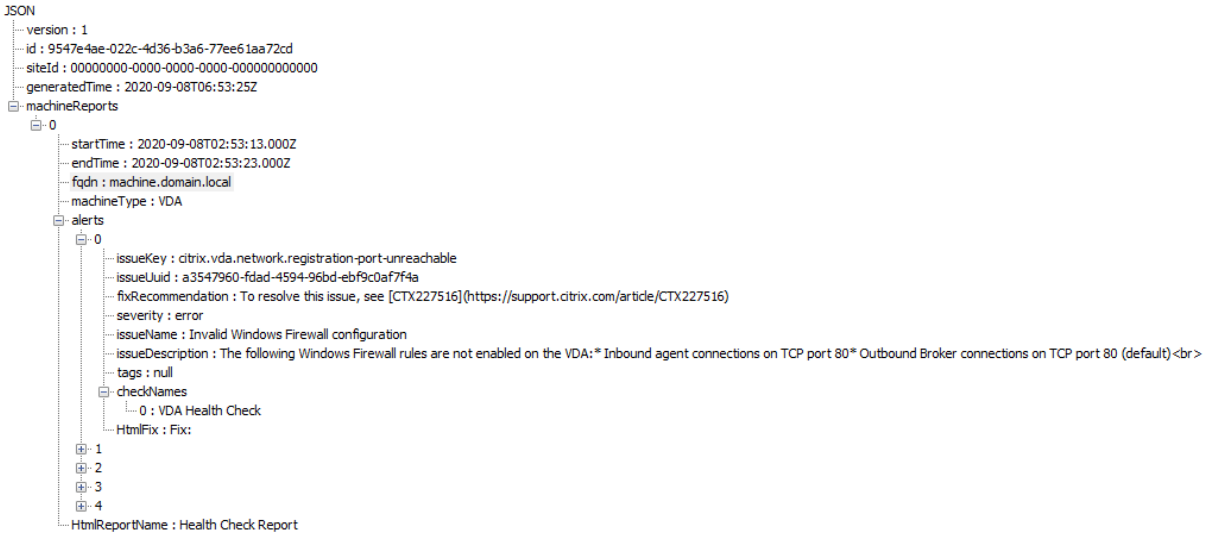
レポート

Cloud Health Check は、ターゲットマシンのHealthCheckDataFolderにそのマシンの名前が付けられたフォルダーを作成します。Cloud Health Check がインストールされているマシンに.html ファイルと.json ファイルが作成されます。ヘルスチェックレポートは%ProgramData%\Citrix\TelemetryService\HealthCheck\DataのHealthCheckDataFolderにあります。

レポートは、ターゲットマシンに問題が存在する場合にのみ作成されます。

> 注:
>
> 指定したレポート名が存在する場合、レポートファイルが上書きされます。

通知と基本情報は.json レポートに保存されます。

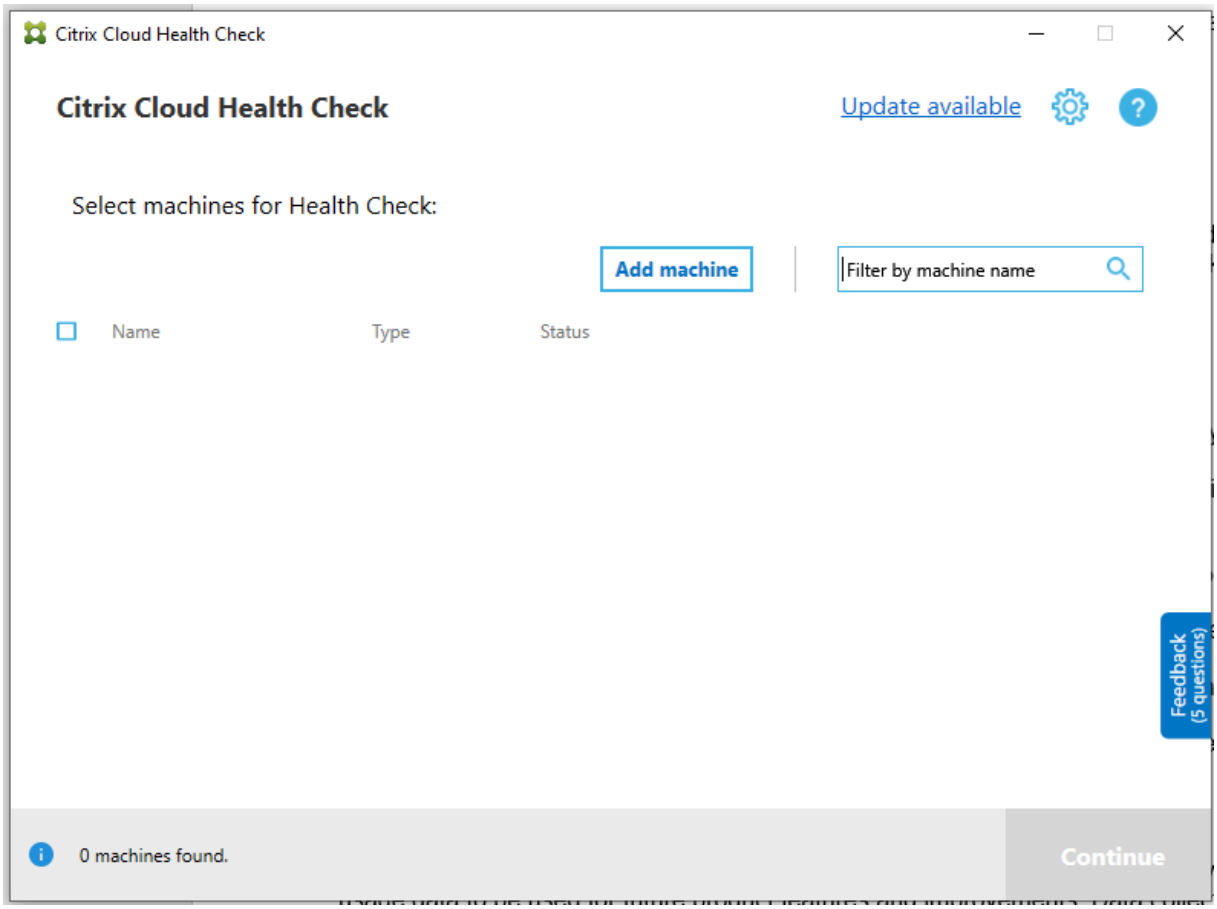


レポートコードは次のとおりです:

- **issueKey**: 問題のプレーンテキスト説明。
- **issueUuid**: 問題の一意の識別子文字列。
- **fixRecommendation**: 問題の修正に関する推奨事項。
- 重大度: 問題を修正する必要があるかどうかを示します。エラーは、コンポーネント (VDA または StoreFront) が誤動作している可能性を示しており、警告は、コンポーネントが機能していても潜在的な問題がある可能性を示しています。
- **issueName**: 問題のタイトル。
- **issueDescription**: 問題の詳細な説明。

Cloud Health Check の更新

Cloud Health Check に利用可能な新しいバージョンがある場合、[Cloud Health Check] ウィンドウの右上に [更新プログラムを利用できます] というリンクが表示されます。リンクをクリックしてシトリックスのダウンロードページに移動し、新しいバージョンを入手してください。

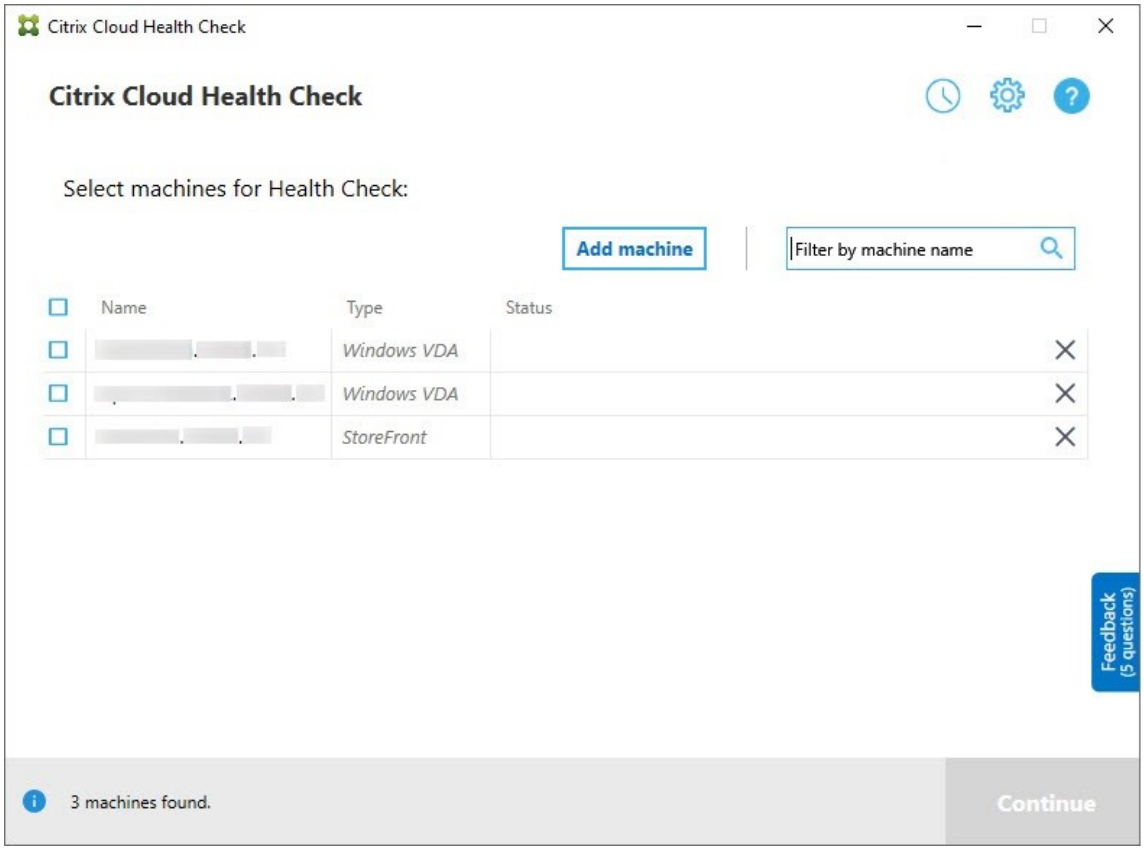


Cloud Health Check スケジューラ

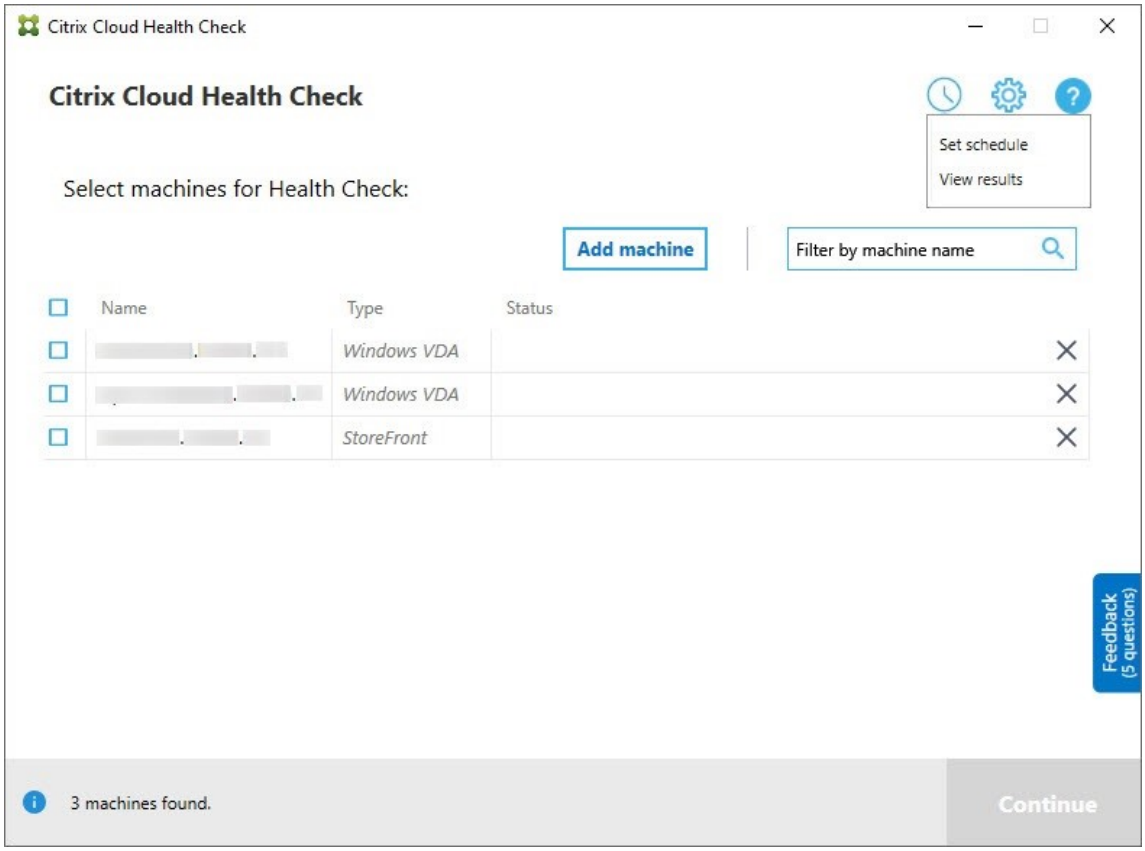
Cloud Health Check スケジューラを使用して、定期的なヘルスチェックを実行します。

スケジュールを設定する

1. Cloud Health Check のメインウィンドウで ［マシンの追加］をクリックして、定期的なチェックを実行するマシンを追加します。



2. 時計アイコンをクリックし、［スケジュールの設定］をクリックします。



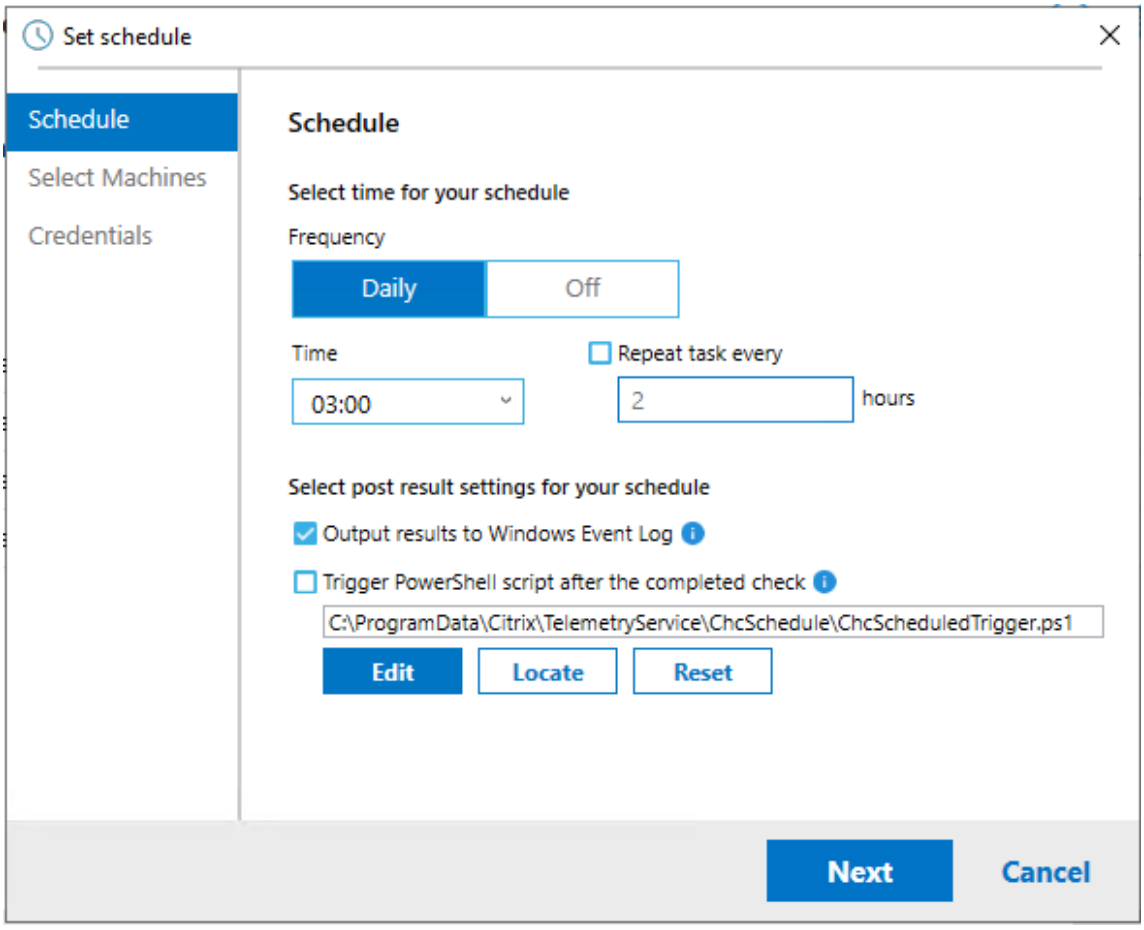
3. スケジュールの時間を選択し、［次へ］をクリックします。［タスクを繰り返す間隔］チェックボックスをオンにすると、タスクを繰り返すように設定できます。
4. 結果を Windows イベントログに出力するように選択します。結果を Windows イベントログに書き込むように、タスクを設定できます。
5. スケジュールされたチェックの終了後にカスタムの PowerShell スクリプトがトリガーされるように選択し、［次へ］をクリックします。

    - 必要に応じて、［編集］をクリックして、Windows PowerShell ISE のスクリプトコンテンツを編集します。
    - ［検索］をクリックしてファイルの場所を開き、別のエディターを使用してファイルを開いてスクリプトを編集します。
    - スクリプトを元の設定にリセットするには、［リセット］をクリックします。

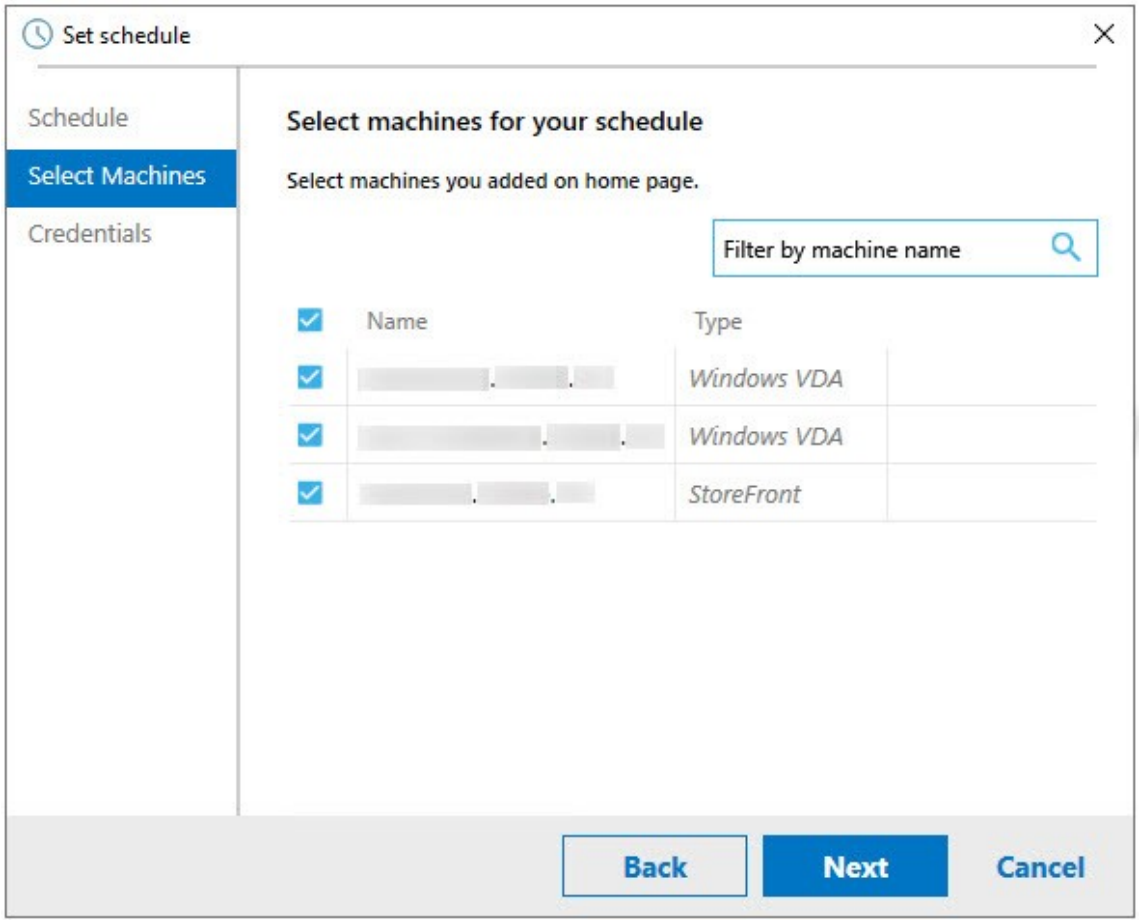
    > 注:
    >
    > – スクリプトのスクリプト名とパスを変更することはできません。
    > – ChcShceduledTrigger.ps1 スクリプトを使用して、スケジュールされたチェックレポートの準備ができたら電子メールを送信するなど、カスタムアクションを実装できます。スクリプトの最後に、次のコードを追加します。コードをカスタマイズして、正しいメールアカウ

> ントと SMTP サーバーアドレスを追加します。スケジュールされたタスクが実行されるアカウントの資格情報を使用して、メール通知が送信されます。

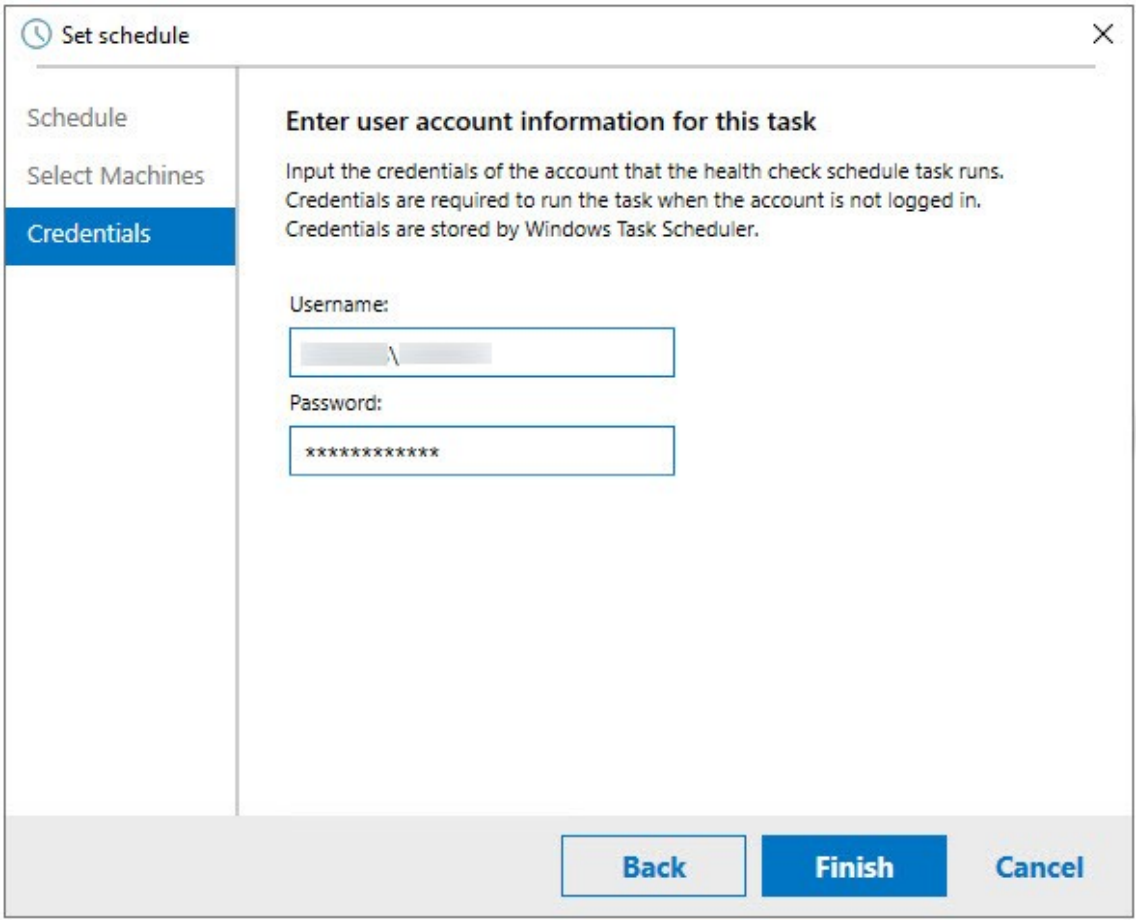
```
#Sending email example code:
$body = "CreatedTime: $($report.CreatedTime)"
$body = $body + "`nStatusCode: $($report.StatusCode)"
$body = $body + "`nMachineCount: $($report.MachineReports.Count)"
$from = "mock_email_accout"
$to = "mock_email_accout"
$smtpServer = "mock_smtp_server"

Send-MailMessage -Subject "Citrix Cloud Health Check Scheduler
    Report" -Body $body -From $from -To $to -SmtpServer $smtpServer
<!--NeedCopy-->
```



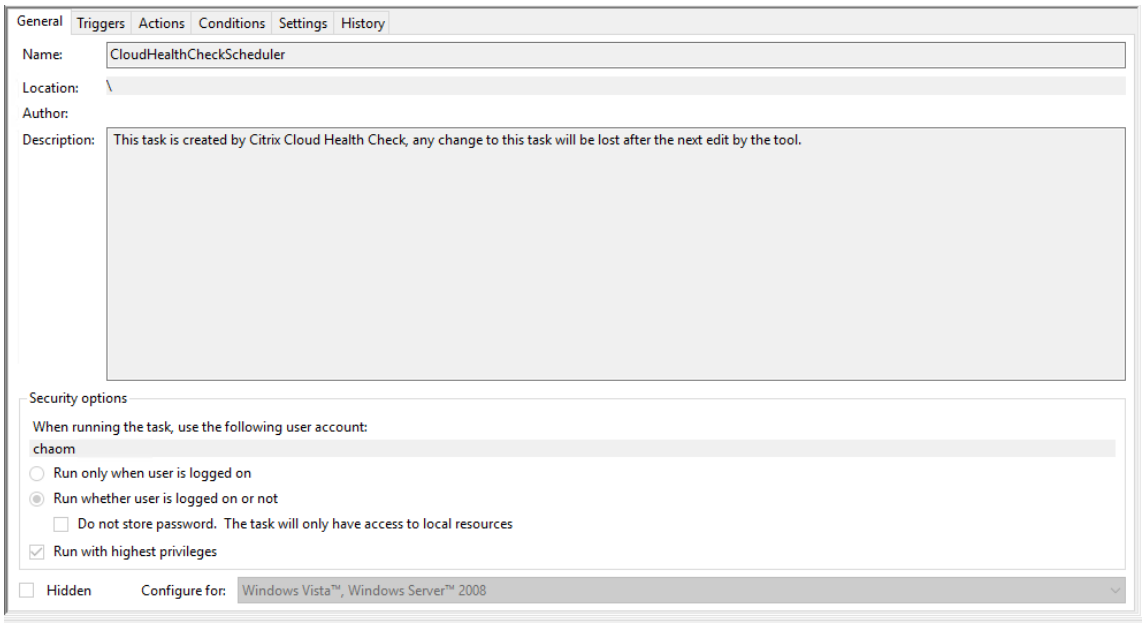
6. スケジュールに合ったマシンを選択し、［次へ］をクリックします。



7. タスクを実行するアカウントの資格情報を入力し、［完了］をクリックします。

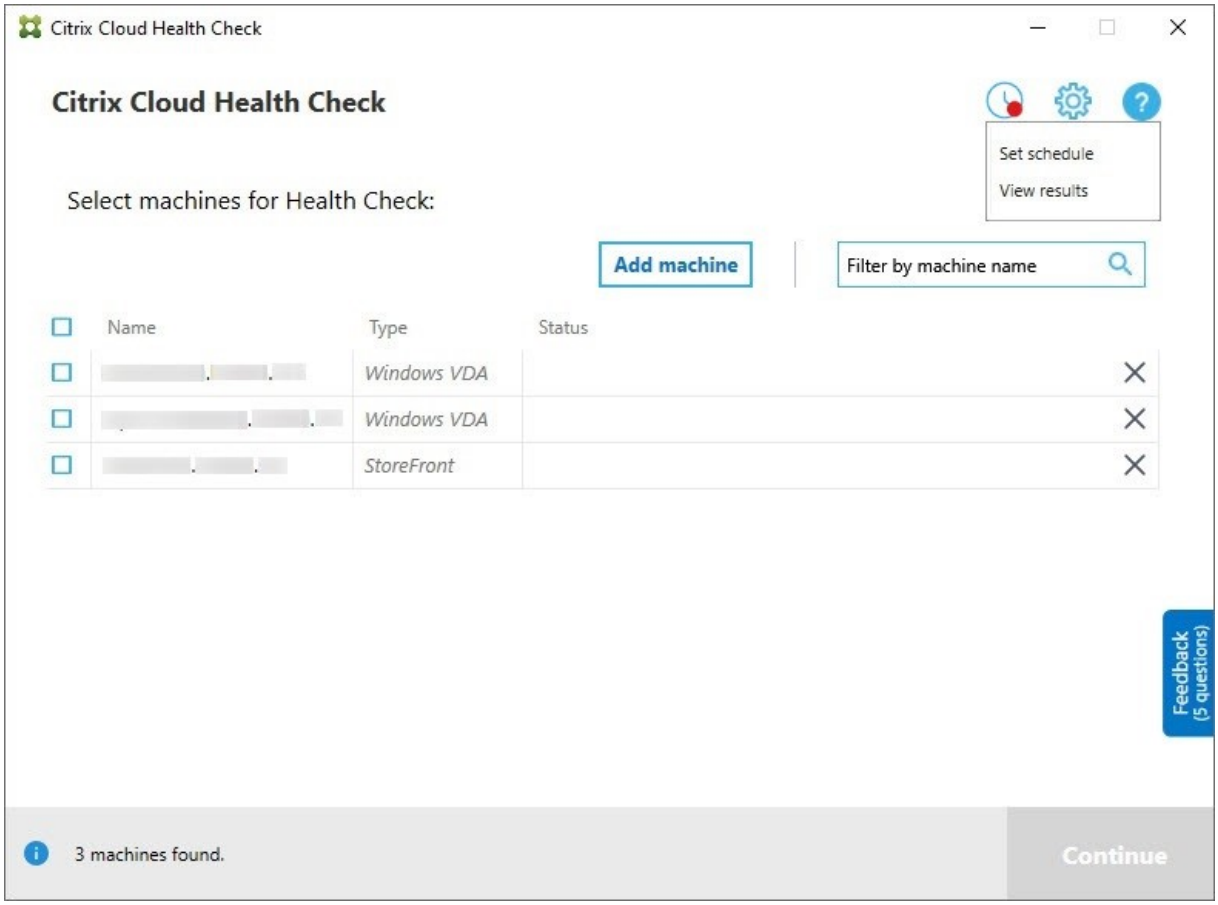


8. CloudHealthCheckScheduler タスクが、Windows タスクスケジューラで作成されます。

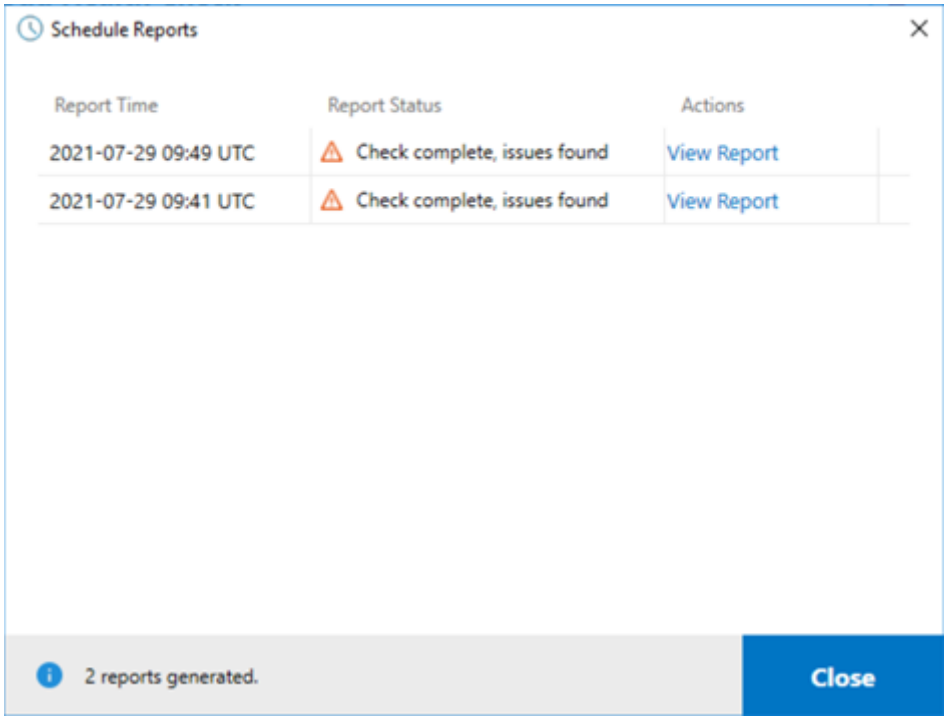


スケジュール結果を表示する

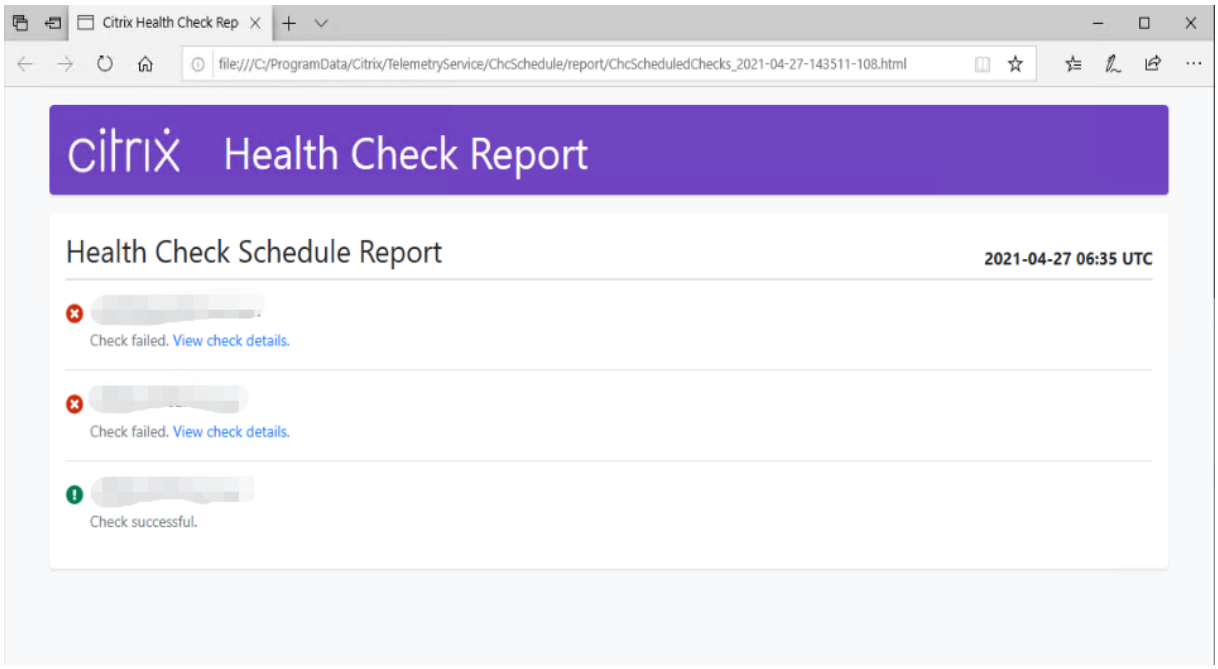
赤い点の付いた時計アイコンは、最後のチェックで問題が見つかったことを示します。結果を表示するには、時計アイコンをクリックし、［結果の表示］をクリックします。



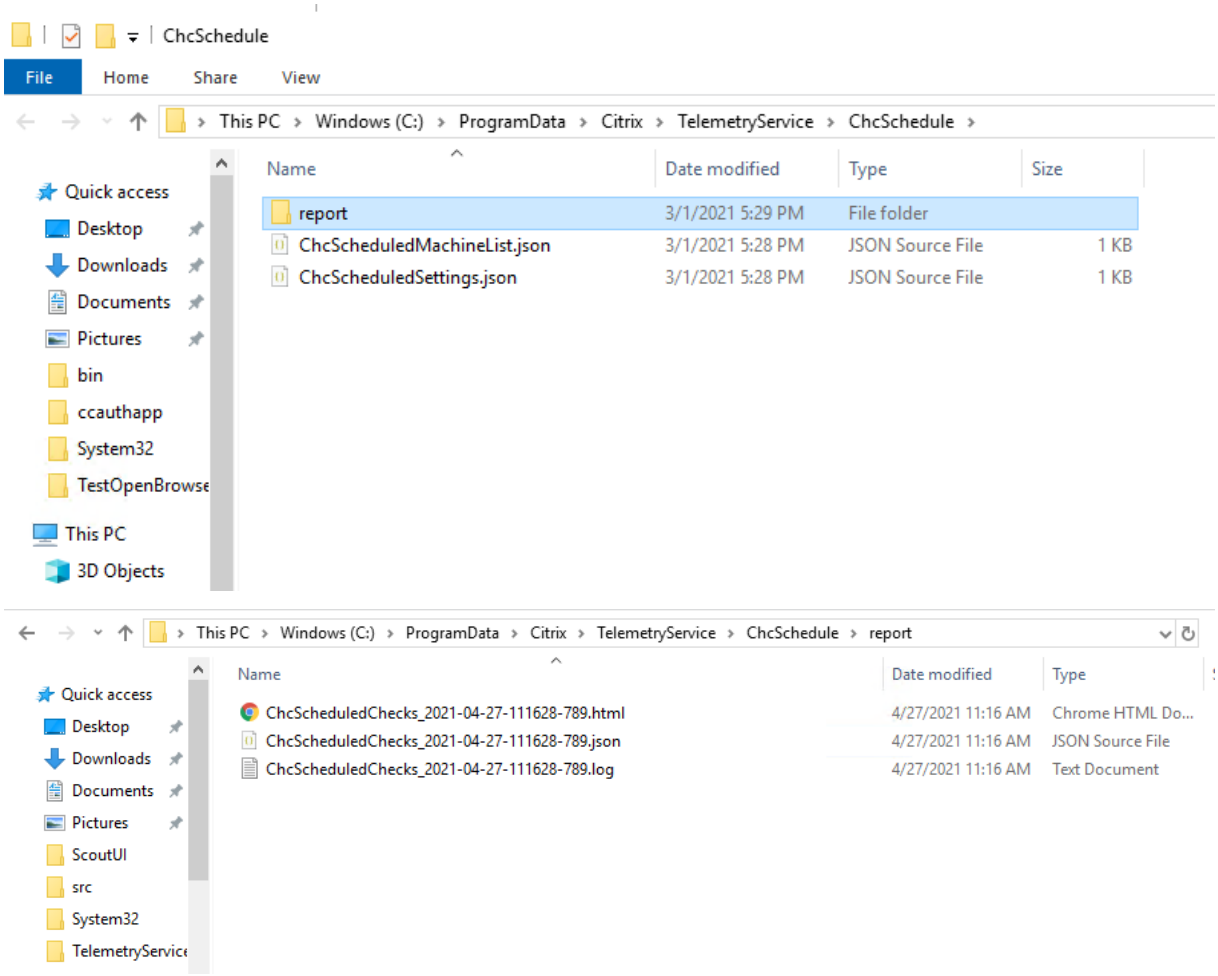
［スケジュールしたタスク実行レポート］ページには、スケジュールされたすべてのヘルスチェックタスクの結果が表示されます。［レポートの表示］をクリックして、各スケジュールのレポートを確認します。



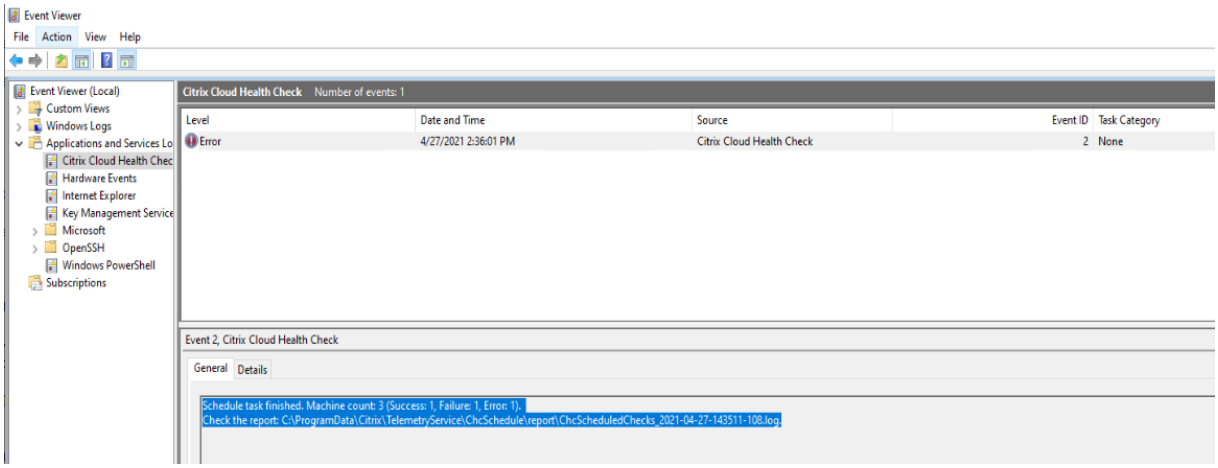
html レポートには、各スケジュールの全体的なレポートが一覧表示されます。レポートの例を以下に示します:



ヘルスチェックの結果はすべて、ChcSchedule というフォルダーに保存されます。Cloud Health Check は、各チェックの実行中に 3 つのファイルを作成します。最大 500 回分の反復ログが保持されます。

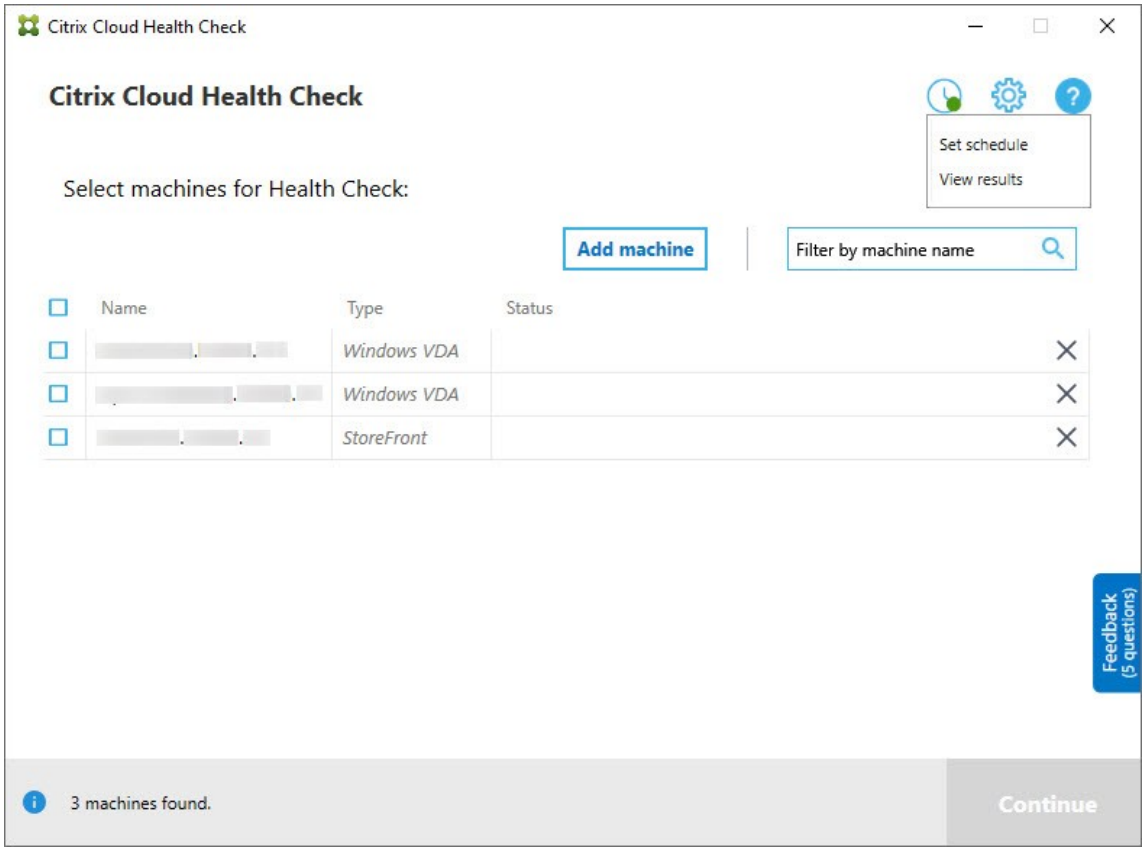


[結果を **Windows** イベントログに出力する] チェックボックスがオンになっている場合、チェック結果は Windows イベントログにも送信されます。

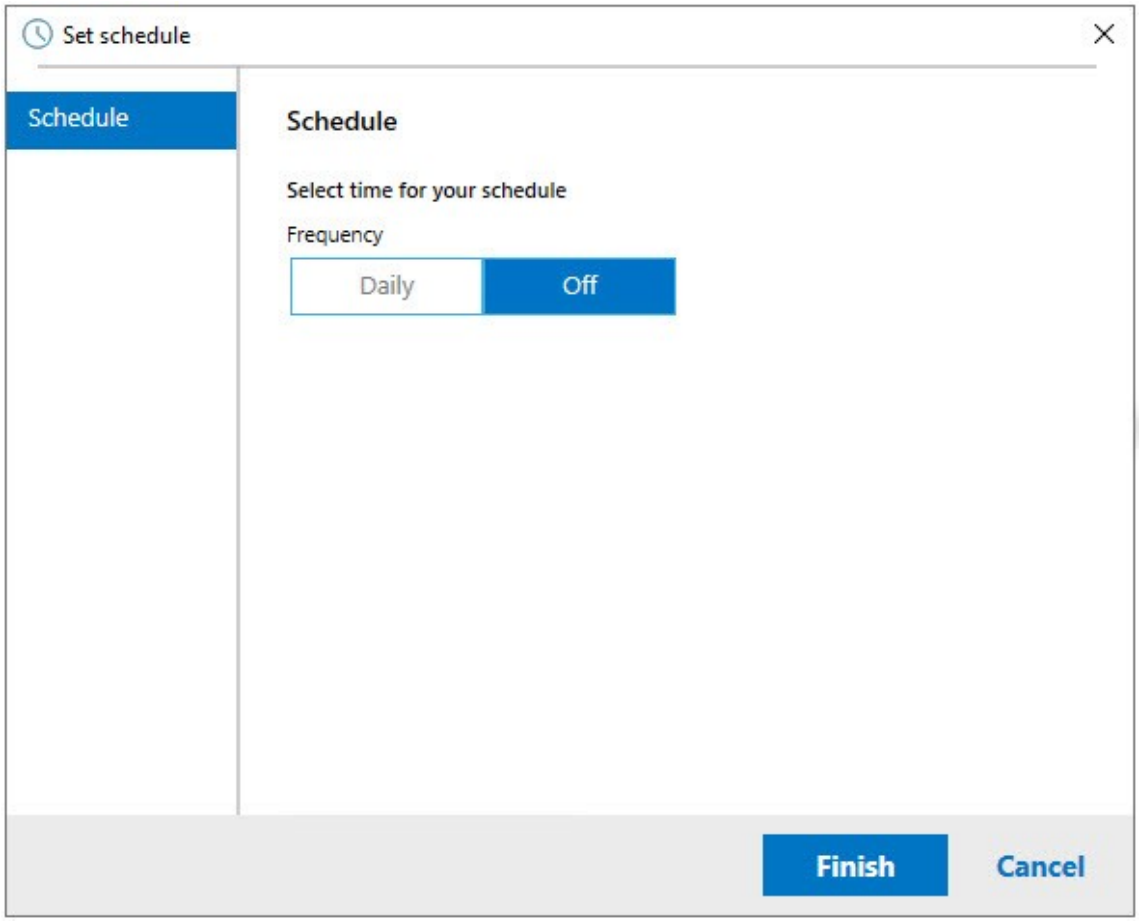


スケジュールを無効にする

1. 時計アイコンをクリックし、［スケジュールの設定］をクリックします。



2. ［オフ］をクリックし、［完了］をクリックしてスケジューラを無効にします。



追加情報

- 最初に VDA を、Cloud Health Check に追加またはインポートする必要があります。詳しくは、「VDA マシンのインポート」を参照してください。
- Cloud Health Check スケジューラは、ドメインに参加しているマシンで一度に 1 つのタスクのみをスケジュールできます。スケジュールを複数回設定すると、最新のものだけが有効になります。

確認テスト

ヘルスチェックの開始前に、指定した各マシンについて自動で確認テストが実行されます。これらのテストで、ヘルスチェックを実行する要件が満たされているか確認されます。あるマシンでテストが失敗した場合、Cloud Health Check には修正アクション案を含むメッセージが表示されます。

- **Cloud Health Check** はこのマシンに接続できません：次のことを確認してください：
  - マシンの電源がオンになっていること。
  - ネットワーク接続が正しく動作していること（これにはファイアウォールが正しく構成されていることを含みます。）

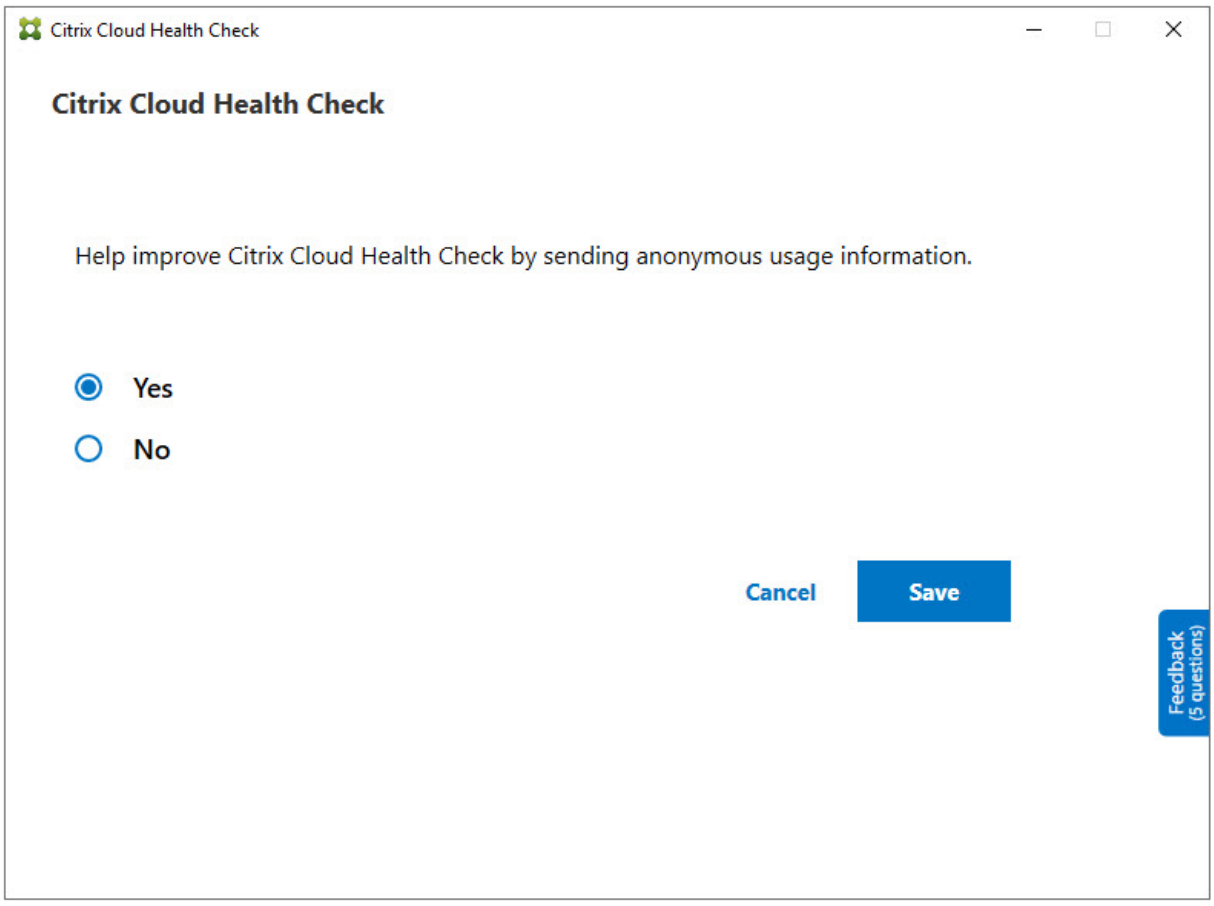
  - ファイルおよびプリンターの共有が設定されていること。手順については、Microsoft 社のドキュメントを参照してください。

- **PSRemoting** および **WinRM** を有効にする：PowerShell を管理者として実行し、Enable-PSRemoting コマンドレットを実行すると、PowerShell リモート処理と Win リモート管理を有効にできます。詳しくは、Microsoft のコマンドレットのヘルプを参照してください。
- **Cloud Health Check** には **PowerShell 3.0** 以降が必要です：マシンに PowerShell 3.0 以降をインストールして、PowerShell リモート処理を有効にします。
- **WMI** がマシン上で実行されていません：Windows Management Instrumentation（WMI）アクセスが有効になっていることを確認してください。
- **WMI** 接続がブロックされました：Windows ファイアウォールサービスで WMI を有効にします。

使用状況データ収集

Cloud Health Check を使用する場合、シトリックスは Google Analytics を使用して匿名の使用状況データを収集し、将来の製品機能や改善に役立てます。データ収集は、デフォルトで有効に設定されています。

使用状況データの収集とアップロードを変更するには、Cloud Health Check UI の ［設定］歯車をクリックします。次に、［はい］か ［いいえ］を選択して情報を送信するかどうかを選択できます。選択したら ［保存］をクリックします。



自動修正

自動修正により、Cloud Health Check は、設定を変更したりサービスを再起動したりすることで、特定の問題を自動的に検出して修正できます。

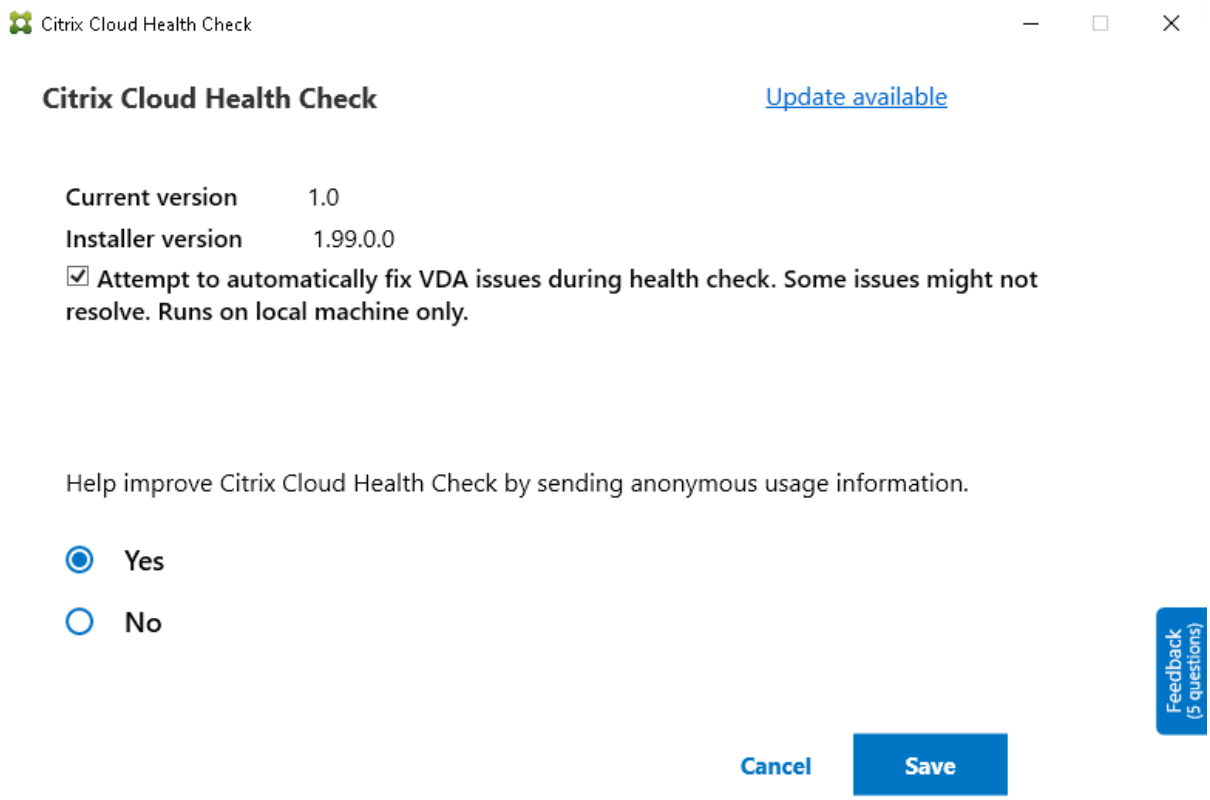
自動修正は、次の VDA 登録項目をチェックし、推奨される修正を行います:

- VDA マシンドメインへの参加状況
  - 修正:「修復」モデルを使用して接続セキュリティチャネルをテストし、修正します
- VDA サービスの状態
  - 修正: BrokerAgent サービスを再起動します
- Controller との通信
  - 修正: BrokerAgent サービスを再起動します
- Controller との時刻同期
  - 修正: W32tm コマンドを実行します

セッションの起動の場合、自動修正は次の項目をチェックし、推奨される修正を行います:

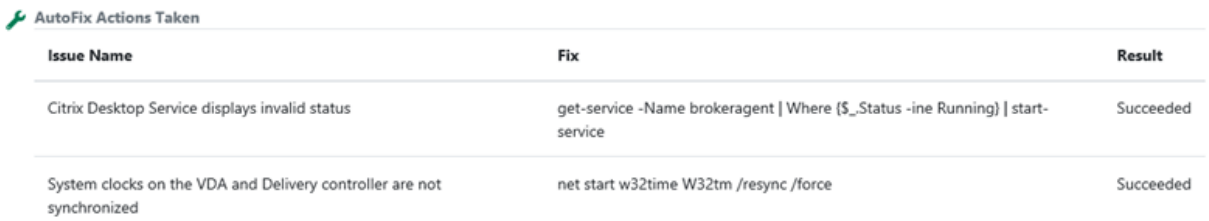
- セッション起動サービスの状態
  - 修正: BrokerAgent サービスを再起動します

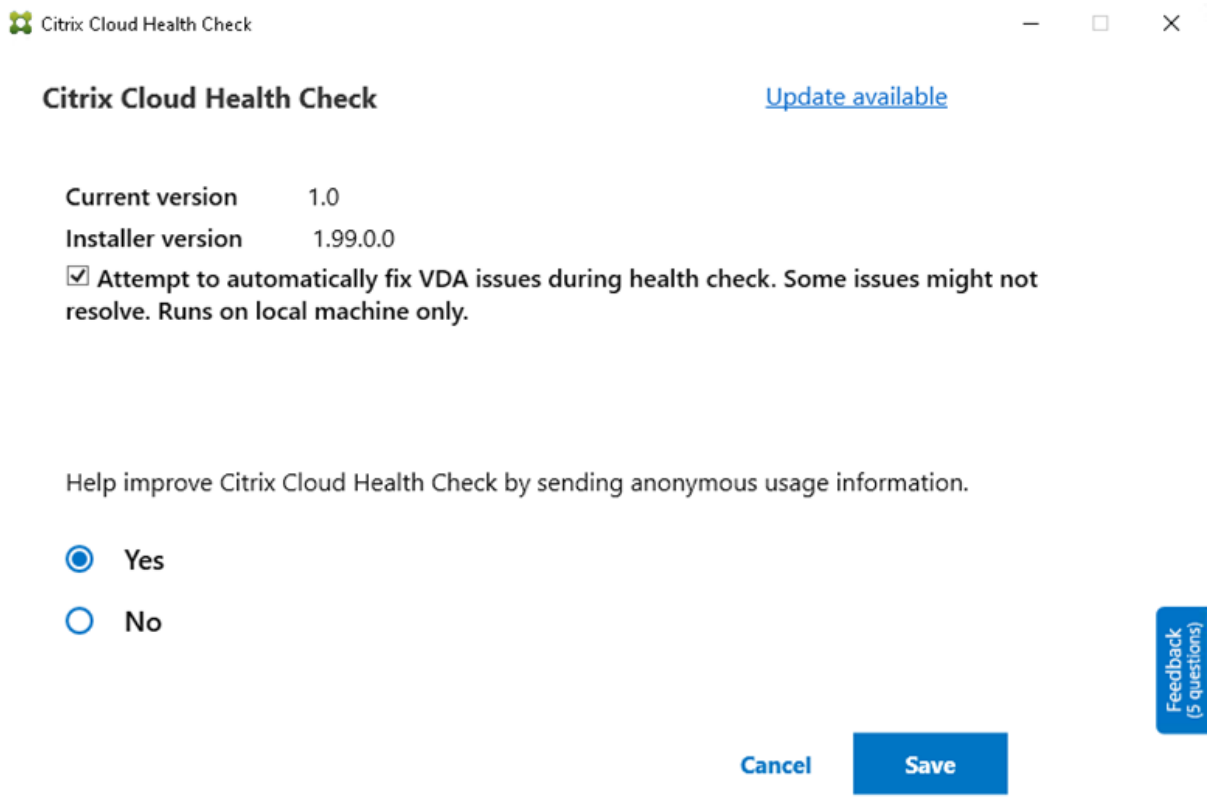
この機能はデフォルトで有効になっています。無効にするには、Cloud Health Check メインウィンドウの右上隅にある歯車のアイコンをクリックし、［ヘルスチェック時に **VDA** の問題の自動修正を試みる］をオフにします。



結果レポート

自動修正を実行した後、チェック結果レポートにすべての詳細を表示するセクションがあります:





トラブルシューティング

Cloud Health Check の実行に失敗したり、例外が発生したりした場合は、`C:\ProgramData\Citrix\TelemetryService\CloudHealthCheck.log`にある Cloud Health Check のログを確認します。

各ターゲットマシンの Cloud Health Check ログは、`C:\ProgramData\Citrix\TelemetryService\HealthCheck\Data\$TargetMachineFQDN\log.txt`にあります。

デバッグログを有効にする手順は、次の通りです:

`C:\Program Files\Citrix\CloudHealthCheck\CloudHealthCheck.exe.config` を編集して、`<add name="TraceLevelSwitch"value="3"/> to <add name="TraceLevelSwitch "value="4"/>`に更新し、ファイルを保存して Cloud Health Check をもう一度開きます。

フィードバック

Cloud Health Check に関するフィードバックをお送りいただける場合は、Citrix アンケートにご協力ください。

構成ログ

May 17, 2024

> 注:
>
> 構成ログレコードは、Citrix Cloud アカウントで選択した言語に関係なく、英語でのみ表示されます。このレコードに関連付けられている日付と時刻は、協定世界時（UTC）の MM/DD/YY 形式です。

構成ログは、Citrix Virtual Apps and Desktops および Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）展開の構成の変更と管理活動を Citrix Cloud のログデータベースに記録する機能です。このログは、以下の目的で使用できます:

- 構成変更の履歴を確認して問題の診断およびトラブルシューティングを行う。ログではブレッドクラムが示されます。
- 変更管理の補助および構成の追跡を行う。
- 管理アクティビティのレポートを生成する。

この Citrix DaaS では、構成ログは常に有効になっています。無効にはできません。

[完全な構成] 管理インターフェイスで、構成ログの内容を日付範囲またはフルテキスト検索でフィルタリングして表示できます。また、PowerShell を使用して CSV レポートを生成することもできます。このコンソールでは、ログの内容の編集や削除はできません。Remote PowerShell SDK を使用して、ログから定期的にデータを削除するスケジュールを設定します。

DaaS 構成ログの保持の更新

DaaS テナントのパフォーマンスを維持するため、2024 年 9 月 9 日より構成ログの保持期間が 180 日に設定されます。

2024 年 9 月 9 日時点で 180 日を超えたログは削除されます。単一の DaaS テナントに対する DaaS の制限が拡大し続ける中、この実装により、お客様に最高のパフォーマンスと復元性が保証されます。

ベストプラクティスとして、四半期ごとのエクスポートメカニズムを用意することをお勧めします。これは PowerShell を使用して実行できます。「レポートの生成」を参照してください。また、定期的なデータ削除をスケジュールすることをお勧めします。「定期的なデータ削除のスケジュール」を参照してください。

必要な権限（「委任管理」を参照）:

- Citrix Cloud のすべての管理権限を実行できる管理者、Citrix DaaS のクラウド管理者と読み取り専用管理者は、[管理] コンソールで構成ログを表示できます。
- すべての管理権限を実行できる管理者、およびクラウド管理者は、PowerShell を使用してログアクティビティの CSV レポートをダウンロードすることもできます。

ログの内容

次の操作はログに記録されます:

- ［管理］タブと ［監視］タブから開始される構成の変更と管理アクティビティ
- PowerShell スクリプト
- REST API 要求

> 注:
>
> Citrix Cloud プラットフォームの内部操作（データベースの設定や管理など）のログエントリは表示できません。

たとえば、以下の項目に対する操作（作成、編集、削除、割り当てなど）が構成ログに記録されます:

- マシンカタログ
- デリバリーグループ（電源管理設定の変更を含む）
- 管理者の役割とスコープ
- ホストのリソースおよび接続
- ［管理］コンソールを介した Citrix ポリシー

ログが記録される管理変更の例には次のものがあります:

- 仮想マシンまたはユーザーのデスクトップの電源管理
- ユーザーにメッセージを送信する機能の管理または監視

次の操作はログに記録されません。（顧客管理者はこれらの操作の多くを使用できません。）

- 仮想マシンのプール管理電源オンなどの自動操作。
- グループポリシー管理コンソール（GPMC）でのポリシー操作。これらの操作のログは Microsoft のツールを使って表示できます。
- レジストリによる変更、または［完全な構成］管理インターフェイス、［監視］、PowerShell 以外での変更。

構成ログの内容の表示

構成ログの内容を表示するには、次の手順に従います:

1. Citrix Cloudにサインインします。左上のメニューで、［マイサービス］**>** ［**DaaS**］を選択します。
2. ［管理］**>** ［完全な構成］の左側ペインで ［ログ］**>** ［イベント］を選択します。

デフォルトでは、中央ペインにログコンテンツが時系列順に（最新のエントリが最初に）表示されます。次の操作を実行できます:

- 列の見出しで表示を並べ替える。

- 日間隔またはカスタムの期間を指定したり、［検索］ボックスにテキストを入力したりして、表示をフィルター処理する。検索を使用した後で通常のログ表示に戻すには、［検索］ボックスの文字列をクリアします。
- 表の右上隅にある 表示する列アイコンを選択して、画面に表示する列を選択します。たとえば、管理者が DaaS にアクセスするために使用する IP アドレスを表示するには、アイコンをクリックしてクライアント **IP** 列を追加します。

表示特性：

- 管理および監視中に作成された高レベルの操作は、中央上部のペインに一覧表示されます。高レベル操作により、1 つまたは複数のサービスおよび PowerShell SDK 呼び出しが実行されます。これは、低レベル操作です。中央上部のペインで高レベル操作を選択すると、下部のペインに低レベル操作が表示されます。
- PowerShell で親の高レベル操作を指定せずに低レベル操作を作成すると、構成ログにより、代わりの高レベル操作が作成されます。
- 操作が完了する前に失敗すると、データベースでログ操作が完結しない場合があります。たとえば、開始レコードに対応する停止レコードがないなどです。このような場合、情報不足であることがログに示されます。時間の範囲を指定してログを表示する場合、未完結のログが表示される場合があります。たとえば、直近 5 日間のログを表示する場合、その 5 日間に開始時間のみが含まれ、終了時間が含まれていない場合も、その操作のログが表示されます。
- 注：Citrix Cloud プラットフォームの内部操作（データベースの設定や管理など）のログエントリは表示できません。

マシンカタログ操作に関連するタスクの表示

マシンカタログ操作に関連するタスクを表示するには、［管理］**>**［完全な構成］**>**［ログ］**>**［タスク］に移動します。［タスク］タブには、Machine Creation Services（MCS）または Provisioning Services（PVS）を介して作成されたカタログに関連するタスクのみが表示されます。具体的には、以下のマシンカタログ操作に関連するタスクが表示されます：

- カタログの作成
- カタログの複製
- マシンの追加
- マシンの削除
- カタログの更新（イメージまたはマシンの更新）
- マシン更新のロールバック

> ヒント：
>
> ［タスク］タブには、プロビジョニングスキームの変更（プロビジョニングスキームの作成または変更）に関連するタスクのみが表示されます。

タスクは以下の状態になります：

- 完了

- 未開始
- 実行中
- キャンセルされました
- 失敗
- 不明

実行中のタスクをキャンセルするには、タスクを選択してから ［キャンセル］をクリックします。キャンセルが完了するまでに少し時間がかかります。

ログに記録されたタスクには、次のようなものがあります：

- 特定のカタログのイメージの更新が完了
- 特定のカタログのイメージの更新中にエラーが発生
- 特定のカタログのイメージの更新をキャンセル
- 特定のカタログへの VM のプロビジョニング
- 特定のカタログからの VM の削除
- 特定のカタログを作成

デフォルトでは、ログに記録されたタスクが中央ペインで時系列順に（最新のエントリが最初に）表示されます。列の見出しで表示を並べ替えることができます。完了したタスクをクリアするには、［タスク］タブの ［完了したタスクのクリア］をクリックします。画面に表示する列を選択するには、表の右上隅にある表示する列アイコンを選択します。

API ログの表示

REST API ログを表示するには、［管理］**>** ［完全な構成］**>** ［ログ］**>** ［**API**］に移動します。［**API**］タブには、特定の期間中に行われた REST API 要求が表示されます。

次の考慮事項に注意してください：

- コンソールからサインアウトすると、REST API ログはクリアされます（Web ブラウザーウィンドウを更新した場合もクリアされます。）
- API 呼び出しが発生するコンソール操作については、対応する API 要求が ［**API**］タブに表示されます。
- 画面には、API 要求が時系列順に（最新のエントリが最初に）表示されます。表示される API 要求の最大数は 1,000 です。

PowerShell ログを表示する

その日に実行した UI 操作に対応する PowerShell コマンドを表示するには、［管理］**>** ［完全な構成］**>** ［ログ］**>** ［**PowerShell**］タブにアクセスします。

メタデータを構成ログに関連付ける

MetadataMapというname-valueペアをログレコードに関連付けることにより、構成ログにメタデータを添付できます。

> 注:
>
> - メタデータは高レベルの操作オブジェクトにのみ添付できます。
> - メタデータは、実行時に既存のレコードに関連付けられます。

メタデータを設定する

PowerShell コマンドSet-LogHighLevelOperationMetadataを実行して、ログレコードをMetadataMapに関連付けます。
Set-LogHighLevelOperationMetadataは次のパラメーターを使用します:

- **Id**: 高レベルの操作の ID。
- **InputObject**: メタデータを追加する高レベルの操作。これは、Idパラメーターの代わりの方法で、高レベルの操作オブジェクトまたはオブジェクトのリストが PowerShell コマンドに渡されます。
- **Name**: 追加されるメタデータのプロパティ名。プロパティは、指定された高レベルの操作に対して一意である必要があります。プロパティには次の文字を含めることはできません:
  ()\/;:#.*?=<>|[]"'
- **Value**: プロパティの値。
- **Map**: プロパティの（名前、値）ペアのディクショナリ。これは、-Nameおよび-Valueパラメーターを使用してメタデータを設定する代わりの方法です。

たとえば、ID 40 のすべての高レベルのログレコードにメタデータを添付するには、次の PowerShell コマンドを実行します:

```
Get-LogHighLevelOperation - Id 40 | Set-LogHighLevelOperationMetadata
 -Name A -Value B
```

ユーザーabc@example.comの高レベルのレコードにメタデータを添付するには、次の PowerShell コマンドを実行します:

```
Get-LogHighLevelOperation - User `abc@example.com` | Set-LogHighLevelOperationM
 -Name C -Value D
```

メタデータを使用して取得する

次の PowerShell コマンドを実行して、関連するメタデータを使用してログレコードを取得します:

- キーと値で検索:

  ```
  Get-LogHighLevelOperation -Metadata "Key:Value"
  ```


- 値と任意のキーで検索:

```
Get-LogHighLevelOperation -Metadata "*:Value"
```

- キーと任意の値で検索:

```
Get-LogHighLevelOperation -Metadata "Key:*"
```

メタデータを削除する

PowerShell コマンド`Remove-LogHighLevelOperationMetadata`を実行して、関連するメタデータを削除します。
`Remove-LogHighLevelOperationMetadata`は次のパラメーターを使用します:

- **Id**: 高レベルの操作の ID。
- **InputObject**: メタデータを追加する高レベルの操作。これは、`Id`'パラメーターの代わりの方法で、高レベルの操作オブジェクトまたはオブジェクトのリストが PowerShell コマンドに渡されます。
- **Name**: 削除するメタデータのプロパティ名。指定したオブジェクトのすべてのメタデータを削除するには、$null に設定します。
- **Map**: プロパティの（名前、値）ペアのディクショナリ。これは、ハッシュテーブル（@{ “name1” = “val1” ; “name2” = “val2” } で作成）または文字列ディクショナリ（new-object “System.Collections.Generic.Dictionary[String, String]” で作成）のいずれかです。名前がマップ内のキーと一致するプロパティは削除されます。

レポートの生成

構成ログデータを含む CSV レポートまたは HTML レポートを生成するには、Citrix Virtual Apps and Desktops Remote PowerShell SDK 内の ConfigLogging Service 用の PowerShell コマンドレットを使用します。詳しくは、次のページを参照してください:

- `Export-LogReportCsv`
- `Export-LogReportHtml`

定期的なデータ削除のスケジュール

Remote PowerShell SDK を使用して、構成ログデータベースでデータが維持される期間を指定します。（この機能は［完全な構成］管理インターフェイスでは利用できません）。Citrix DaaS では、フルアクセス権が必要です。

`Set-LogSite`コマンドレットの`-LoggingDBPurgeDurationDays`パラメーターは、構成ログデータベースから自動的に削除されるまでデータが維持される日数を指定します。

- デフォルトでは、このパラメーターの値は 0 です。値がゼロの場合、構成ログデータベースのデータは自動的に削除されません。

- ゼロ以外の値を設定すると、データベースは 120 分ごとに確認され保有期間より古いデータは削除されます。

`Get-LogSite`を使用して、パラメーターの現在値を表示します。

オンプレミス **Citrix Virtual Apps and Desktops** との相違点

オンプレミスの Virtual Apps and Desktops 製品の構成ログを使い慣れている場合は、Citrix Cloud バージョンにはいくつかの違いがあることに注意してください。Citrix Cloud の場合:

- 構成ログは常に有効になっています。無効にはできません。必須ログは使用できません。
- 構成ログデータベースは Citrix Cloud プラットフォームで管理されるため、構成ログデータベースの場所を変更することはできません。
- 構成ログの表示には、Citrix Cloud プラットフォーム内で実行される操作やアクティビティは含まれません。
- ログに記録された操作の CSV または HTML レポートを作成できるのは、PowerShell のみです。オンプレミス製品では、Citrix Studio または PowerShell からレポートを生成できます。
- 構成ログの内容は削除できません。

委任管理

March 31, 2024

概要

Citrix Cloud での委任管理により、組織内の役割に応じて管理者に必要となる、すべてのアクセス権限を構成できます。

デフォルトでは、管理者にはフルアクセス権があります。この設定により、Citrix Cloud 内の利用可能なすべての顧客管理機能および管理機能と、サブスクライブしているすべてのサービスにアクセスできます。管理者のアクセス権を調整するには:

- Citrix Cloud での管理者の一般的な管理権限についてカスタムアクセス権を構成します。
- サブスクライブしているサービスについてカスタムアクセス権を構成します。Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）では、新しい管理者を招待するときにカスタムアクセス権を構成できます。管理者のアクセス権は後で変更できます。

管理者一覧の表示とアクセス権限の定義については、「Citrix Cloud への管理者のアクセスを管理する」を参照してください。

この記事では、Citrix DaaS でカスタムアクセス権を構成する方法について説明します。

管理者、役割、およびスコープ

管理権限の委任機能では、カスタムアクセス権について次の 3 つの概念が使用されます：管理者、役割、およびスコープ。

- 管理者：管理者とは、Citrix Cloud サインイン（通常は電子メールアドレス）によって識別された人物を表します。各管理者には、1 つまたは複数の役割とスコープのペアが割り当てられます。
- 役割：役割とは管理ジョブの機能を表し、それぞれ権限が割り当てられています。これらの権限により、Citrix DaaS 固有の特定のタスクが許可されます。たとえば、デリバリーグループ管理者役割には、デリバリーグループの作成とデリバリーグループからのデスクトップの削除の権限、およびその他の関連する権限があります。管理者は複数の役割を持つことができます。管理者は、デリバリーグループ管理者であり、マシンカタログ管理者でもある可能性があります。

  Citrix DaaS には、いくつかの組み込みのカスタムアクセス権役割が用意されています。これらの組み込みの役割内の権限の変更や、これらの役割の削除はできません。

  必要に応じてカスタムアクセス権役割を作成して、より詳細な権限を委任することができます。カスタム役割を使用して、操作またはタスク単位で権限を割り当てることができます。カスタマイズされた役割は、管理者に割り当てられていない場合にのみ削除できます。

  管理者が持つ役割は変更できます。

  役割は、必ずスコープとペアになっています。

- スコープ：接続、マシンカタログ、デリバリーグループなど、その管理者が管理できるオブジェクトをグループ化したものです。スコープは、組織に関連する方法でオブジェクトをグループ化するために使用されます。オブジェクトは、複数のスコープに存在できます。

  次の組み込みのスコープには、すべてのオブジェクトが含まれています:「すべて」。Citrix Cloud 管理者とヘルプデスク管理者は、必ず「すべて」スコープとペアになっています。これらの管理者のそのスコープを変更することはできません。

  管理者をこのサービスに招待（追加）した場合、役割は必ずスコープ（デフォルトでは「すべて」スコープ）とペアになります。

  スコープの作成と削除は、［管理］**>**［完全な構成］インターフェイスで行います。役割/スコープのペアの割り当ては、Citrix Cloud コンソールで行います。

  フルアクセス権管理者については、スコープは表示されません。定義上は、これらの管理者は、顧客が管理する Citrix Cloud、およびサブスクライブしているサービスのオブジェクトすべてにアクセスできます。

組み込みの役割とスコープ

Citrix DaaS には、次の役割が組み込まれています。

- クラウド管理者： Citrix DaaS から開始できるすべてのタスクを実行できます。

  コンソールで ［管理］タブと ［監視］タブを表示できます。この役割は、必ず「すべて」スコープと結合されています。スコープは変更できません。

  この役割の名前を混同しないでください。カスタムアクセス権クラウド管理者は、Citrix Cloud レベルのタスクを実行できません（Citrix Cloud のタスクにはフルアクセス権が必要です）。

- 読み取り専用管理者：（全体的な情報のほかに）指定されたスコープ内のすべてのオブジェクトを表示できますが、変更はできません。たとえば、「大阪」というスコープを作成して読み取り専用管理者に割り当てると、グローバルオブジェクトと、［大阪］スコープのオブジェクト（大阪支社用のデリバリーグループなど）を表示できます。ただし、この管理者は「ニューヨーク」スコープのオブジェクトを表示できません。

  コンソールで ［管理］タブと ［監視］タブを表示できます。

- ヘルプデスク管理者：デリバリーグループを表示し、デリバリーグループに関連付けられているセッションとマシンを管理できます。監視対象のデリバリーグループについて、マシンカタログとホスト情報を表示できます。また、それらのデリバリーグループ内のマシンのセッションや電源を管理できます。

  コンソールで ［監視］タブを表示できます。［管理］タブは表示できません。この役割は、必ず「すべて」スコープと結合されています。スコープは変更できません。

- マシンカタログ管理者：マシンカタログの作成と管理や、マシンカタログへのマシンのプロビジョニングができます。基本イメージの管理やソフトウェアのインストールができますが、アプリケーションやデスクトップをユーザーに割り当てることはできません。

  コンソールで ［監視］タブと ［管理］タブを表示できます。［監視］タブは表示できません。スコープは変更できます。

- デリバリーグループ管理者：アプリケーション、デスクトップ、およびマシンを配信できます。関連セッションを管理することもできます。ポリシーや電源管理設定など、アプリケーションおよびデスクトップの構成を管理できます。

  コンソールで ［監視］タブと ［管理］タブを表示できます。スコープは変更できます。

  > 注：
  >
  > デリバリーグループ管理者としてデスクトップの表示名を変更するには、マシンの更新権限が必要です。この権限が必要になる理由は、表示名を変更するのにマシンのプロパティを更新する必要があるためです。

- ホスト管理者：ホスト接続およびその関連リソース設定を管理できます。マシン、アプリケーション、またはデスクトップをユーザーに配信することはできません。

  コンソールで ［管理］タブを表示できます。［監視］タブは表示できません。スコープは変更できます。

- セッション管理者：監視されているデリバリーグループを表示し、関連するセッションとマシンを管理できます。

  コンソールで ［監視］タブを表示できます。［管理］タブは表示できません。スコープは変更できません。

- 完全な管理者：すべてのタスクと操作を実行できます。完全な管理者は、常に ［すべて］のスコープ と結び付けられています。

  コンソールで ［管理］タブと ［監視］タブを表示できます。この役割は、常に ［すべて］のスコープ と結び付けられています。スコープは変更できません。

- 完全なモニター管理者：［監視］タブのすべてのビューとコマンドに対するフルアクセス権限があります。

  コンソールで ［監視］タブを表示できます。［管理］タブは表示できません。スコープは変更できません。

- プローブエージェント管理者：プローブエージェント API へのアクセス権限があります。

  コンソールで ［監視］タブと ［管理］タブを表示できます。［アプリケーション］ページへの読み取り専用アクセス権限がありますが、他のビューにはアクセスできません。

次の表は、Citrix DaaS 内の各カスタムアクセス権役割にどのコンソールタブが表示されるかと、役割をカスタムスコープとともに使用できるかどうかの一覧です。

カスタムアクセス権管理者役割	コンソールで ［管理］タブを表示できるか	コンソールで ［監視］タブを表示できるか	役割をカスタムスコープと共に使用できるか
クラウド管理者	はい	はい	いいえ
読み取り専用管理者	はい	はい	はい
ヘルプデスク管理者	いいえ	はい	いいえ
マシンカタログ管理者	はい	はい	はい
デリバリーグループ管理者	はい	はい	はい
ホスト管理者	はい	いいえ	はい
セッション管理者	いいえ	はい	いいえ
すべての管理権限を実行できる管理者	はい	はい	いいえ
完全なモニター管理者	いいえ	はい	いいえ
Probe Agent 管理者	はい	はい	いいえ

> 注：
>
> クラウド管理者およびヘルプデスク管理者以外のカスタムアクセス権管理者の役割は、Citrix Virtual Apps and Desktops Standard for Azures、Virtual Apps Essentials、Virtual Desktops Essentials で利用できません。

役割に関連付けられた権限を表示するには：

1. Citrix Cloudにサインインします。左上のメニューで、［マイサービス］**>** ［**DaaS**］を選択します。

2. ［管理］**>**［完全な構成］の左側ペインで ［管理者］を選択します。
3. ［役割］タブを選択します。
4. 中央上部のペインで役割を選択します。下部のペインの ［役割定義］タブに、カテゴリと権限が一覧表示されます。カテゴリを選択すると、特定の権限が表示されます。［管理者］タブには、選択した役割が割り当てられている管理者が一覧表示されます。

   既知の問題：すべての管理権限を実行できる管理者のエントリに、フルアクセス権 Citrix DaaS 管理者の正しい権限セットが表示されません。

必要な管理者の数

一般的に、管理者数およびその権限の細分性は、環境の規模と複雑度に応じて異なります。

- 小規模または検証用の展開サイトでは、1 人または少数の管理者ですべてを管理します。カスタムアクセス権を持つ委任管理者は存在しません。この場合、各管理者はフルアクセス権を持ち、必ず「すべて」スコープを持ちます。
- より多くのマシン、アプリケーション、およびデスクトップがあるサイトでは、委任管理者の配置が必要になります。何人かの管理者に、より専門的な管理責任（役割）を付与できます。たとえば、2 人にフルアクセス権を付与し、残りをヘルプデスク管理者にします。さらに、特定部門のマシンカタログなど、オブジェクトの特定グループ（スコープ）の管理を 1 人の管理者に任せることもできます。この場合は、新しいスコープを作成し、適切なカスタムアクセス権役割とスコープを持つ管理者を作成します。

管理者の管理の概要

Citrix DaaS に管理者を設定する手順は、次のとおりです：

1. 管理者に付与する役割が、（Citrix Cloud のすべてのサブスクライブされたサービスを含む）すべての管理権限を実行できる管理者の役割または組み込みの役割以外である場合、カスタムの役割を作成します。
2. 管理者に「すべて」以外のスコープを設定する場合（また、目的の役割に別のスコープが許可されており、そのスコープがまだ作成されていない場合）は、スコープを作成します。
3. Citrix Cloud から管理者を招待します。新しい管理者にデフォルトのフルアクセス権以外の権限を付与する場合は、カスタムアクセス権役割/スコープのペアを指定します。

後で管理者のアクセス権（役割とスコープ）を変更する場合は、「カスタムアクセス権の構成」を参照してください。

管理者を追加する

管理者を追加（招待）するには、「Citrix Cloud アカウントに管理者を追加する」の手順に従ってください。ここでは、その情報の一部を繰り返します。

> 重要:
>
> 「カスタム」と「カスタムアクセス権」を混同して使用しないでください。
>
> - 管理者を作成し、Citrix Cloud コンソールで Citrix DaaS の役割を割り当てる場合、「カスタムアクセス権」という用語には、組み込みの役割とサービスの ［管理］ **>** ［完全な構成］ インターフェイスで作成された追加のカスタム役割が含まれます。
> - サービスの ［管理］ **>** ［完全な構成］ インターフェイスにおける「カスタム」は、組み込みの役割から区別するための呼称です。

管理者を追加するための一般的なワークフローは次のとおりです:

1. Citrix Cloudにサインインし、左上のメニューで ［**ID** およびアクセス管理］ を選択します。
2. ［**ID** およびアクセス管理］ ページで ［管理者］ を選択します。［管理者］ タブには、そのアカウントに対する現在のすべての管理者が一覧表示されます。
3. ［管理者］ タブで、ID の種類を選択し、管理者のメールアドレスを入力して、［招待］ をクリックします。
   - 管理者にフルアクセスを許可する場合は、［フルアクセス］ を選択します。このようにして、管理者は Citrix Cloud とサブスクライブされたすべてのサービスで、すべての顧客管理者機能にアクセスできます。
   - 管理者に制限付きアクセスを許可する場合は、［カスタムアクセス］ を選択します。次に、カスタムアクセス権役割とスコープのペアを選択できます。このようにして、管理者には Citrix Cloud にサインインするときに意図した権限が付与されます。
4. ［招待を送信する］ をクリックします。管理者がオンボードを完了した後、Citrix Cloud はメールアドレスに招待状を送信し、管理者をリストに追加します。

メールを受信した管理者は、［サインイン］ リンクをクリックして招待を承諾します。

Citrix Cloud 管理者の追加について詳しくは、「Citrix Cloud 管理者を管理する」を参照してください。

または、［管理］ **>** ［完全な構成］ **>** ［管理者］ **>** ［管理者］ の順に移動し、［管理者の追加］ をクリックします。［**ID** およびアクセス管理］ **>** ［管理者］ に直接移動します。これは、新しいブラウザータブで開きます。そこで管理者を追加し終えたら、タブを閉じてコンソールに戻り、ほかの構成タスクに移ります。

役割の作成と管理

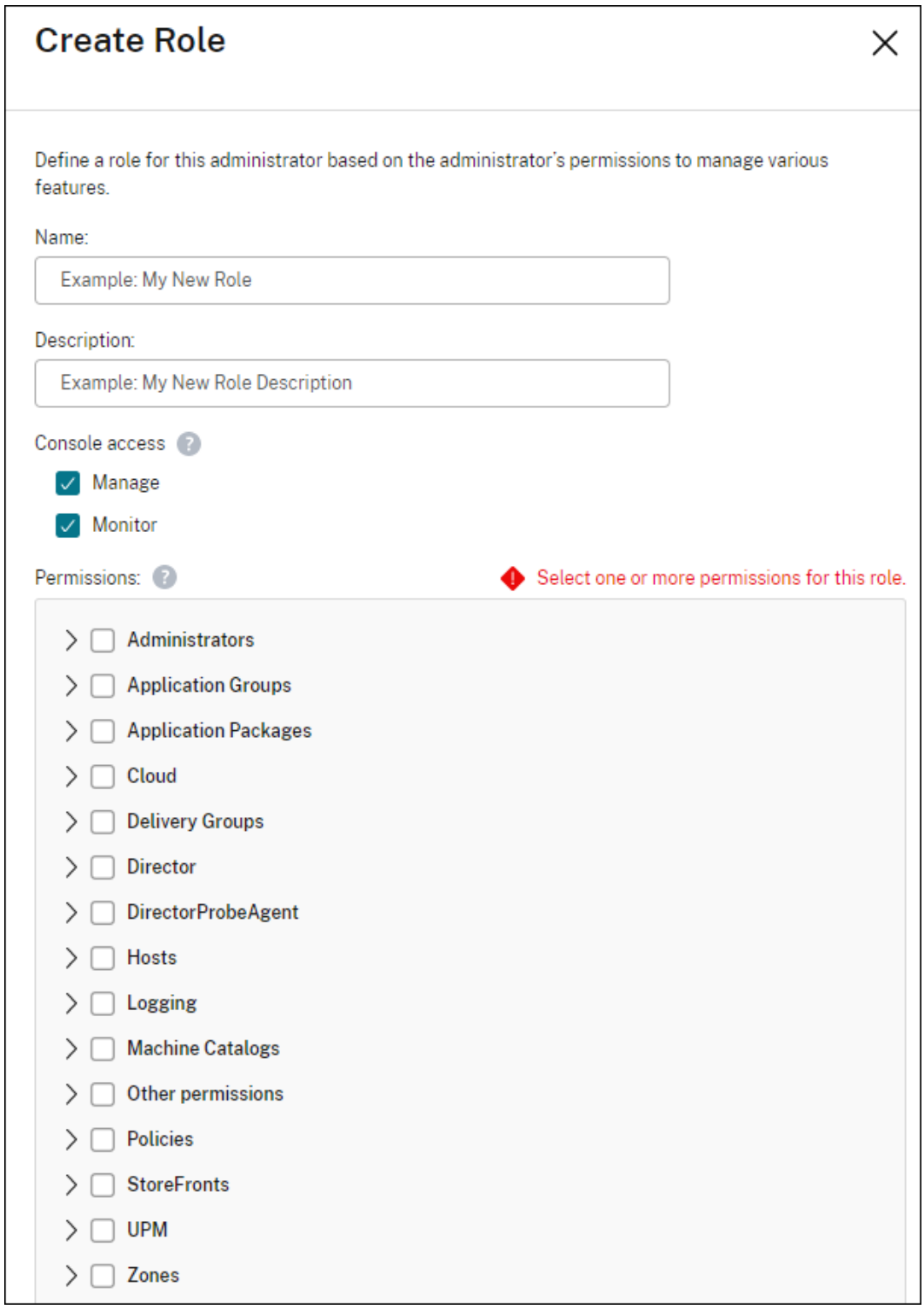
管理者が役割を作成または編集する場合、自身が持っている権限のみを有効にできます。これにより、管理者は現在よりも多くの権限を持つ役割を作成して自身に割り当てる（または既に割り当てられた役割を編集する）ことができなくなります。

カスタム役割には、Unicode 文字で 64 文字以下の名前を付けることができます。名前には、次の文字は使用できません: バックスラッシュ、スラッシュ、セミコロン、コロン、番号記号、コンマ、アスタリスク、疑問符、等号、小なり記号、大なり記号、パイプ、角かっこ、丸かっこ、二重引用符、およびアポストロフィ。

役割の説明には、256 文字までの Unicode 文字を入力できます。

1. まだCitrix Cloudにサインインしていない場合は、サインインします。左上のメニューで、［マイサービス］**>** ［**DaaS**］を選択します。
2. ［管理］**>** ［完全な構成］の左側ペインで ［管理者］を選択します。
3. ［役割］タブを選択します。
4. 完了するタスク用の手順を実行します：

    - 役割の詳細を表示する：中央ペインでその役割を選択します。中央ペインの下部に、その役割のオブジェクトの種類および許可される権限が表示されます。ここで ［管理者］タブをクリックすると、その役割が割り当てられている管理者が表示されます。
    - カスタム役割を作成する：操作バーで ［役割の作成］を選択します。次のように設定を構成します：
        - 名前と説明を入力します。
        - コンソールアクセス権を構成します。管理者に表示されるコンソールを指定します。コンソールを選択せずに続行することもできます。その場合、役割を持つ管理者は ［管理］と ［監視］にはアクセスできませんが、SDK と API を使用してオブジェクトにアクセスしたり、オブジェクトを表示または管理したりできます。
        - この役割に割り当てるオブジェクトの種類と権限を選択します。オブジェクトの種類にフルアクセス権限を付与するには、そのチェックボックスをオンにします。より細かくアクセス権限を付与するには、［オブジェクトの種類］を広げて［種類］内の ［管理］で ［読み取り専用］または個々のオブジェクトを選択します。



- 役割をコピーする：中央ペインで役割を選択し、操作バーの ［役割のコピー］を選択します。必要に応じて、役割の名前、説明、および権限を変更します。完了したら、［保存］を選択します。
- カスタム役割を編集する：中央ペインで役割を選択し、操作バーの ［役割の編集］を選択します。必要

に応じて、役割の名前、説明、および権限を変更します。組み込みの役割を編集することはできません。完了したら、［保存］を選択します。

- カスタム役割を削除する：中央ペインで役割を選択し、操作バーの ［役割の削除］を選択します。確認のメッセージが表示されたら、［削除］をクリックします。組み込みの役割を削除することはできません。管理者に割り当てられたカスタム役割は削除できません。

スコープの作成と管理

デフォルトでは、すべての役割に、関連オブジェクトの［すべて］スコープが設定されています。たとえば、デリバリーグループ管理者は、すべてのデリバリーグループを管理できます。一部の管理者役割では、その管理者役割が関連オブジェクトの一部にアクセスできるようにスコープを作成できます。たとえば、すべてのカタログではなく特定の種類のマシンを含むカタログのみに、マシンカタログ管理者がアクセスできるようにすることができます。

- フルアクセス権管理者またはカスタムアクセス権クラウド管理者は、読み取り専用管理者、マシンカタログ管理者、デリバリーグループ管理者、およびホスト管理者の役割のスコープを作成できます。
- スコープをフルアクセス権管理者用に作成することや、クラウド管理者またはヘルプデスク管理者用に作成することはできません。これらの管理者には、必ず［すべて］スコープが設定されます。

スコープの作成と管理のルール：

- スコープには、Unicode 文字で 64 文字以下の名前を付けることができます。名前には、次の文字は使用できません：バックスラッシュ、スラッシュ、セミコロン、コロン、番号記号、コンマ、アスタリスク、疑問符、等号、小なり記号、大なり記号、パイプ、角かっこ、丸かっこ、二重引用符、およびアポストロフィ。
- スコープの説明には、256 文字までの Unicode 文字を入力できます。
- スコープをコピーまたは編集するときにオブジェクトをスコープから削除すると、管理者がそのオブジェクトにアクセスできなくなる可能性があることに注意してください。編集するスコープにいくつかの役割が関連付けられている場合は、編集により役割/スコープのペアが使用できなくならないかどうかを確認してください。

スコープを作成し管理するには：

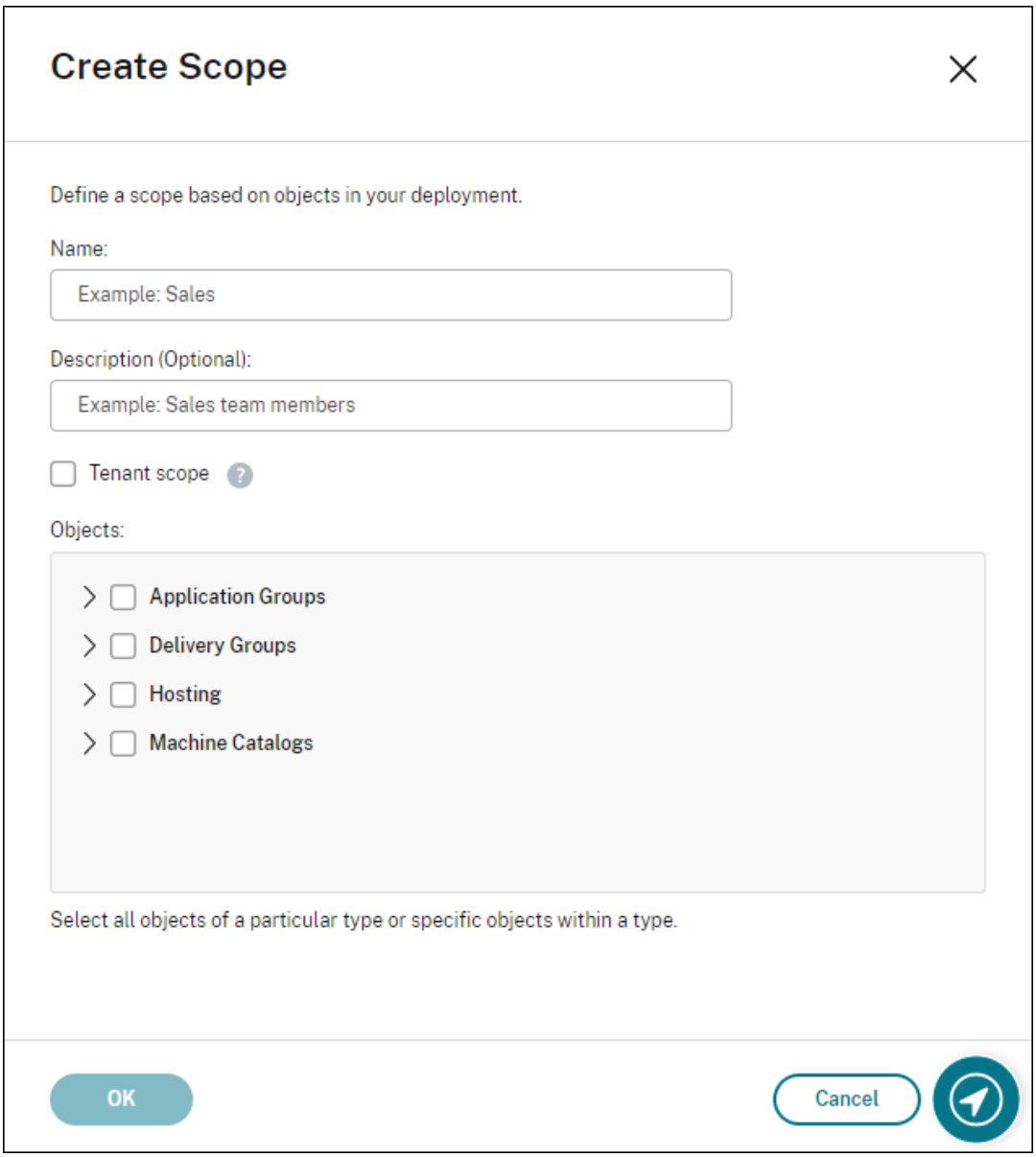
1. Citrix Cloudにサインインします。左上のメニューで、［マイサービス］**>**［**DaaS**］を選択します。
2. ［管理］**>**［完全な構成］の左側ペインで ［管理者］を選択します。
3. ［スコープ］タブを選択します。
4. 完了するタスク用の手順を実行します：
   - スコープの詳細を表示する：スコープを選択します。ペインの下部には、そのスコープを持つオブジェクトと管理者が一覧表示されます。
   - スコープを作成する：操作バーの ［スコープの作成］を選択します。名前と説明を入力します。オブジェクトは、デリバリーグループやマシンカタログなど、種類別に一覧表示されます。

- オブジェクトの種類のチェックボックスをオンにすると、その種類のすべてのオブジェクト（たとえば、すべてのデリバリーグループ）がスコープに追加されます。
- 特定の種類の個々のオブジェクトを追加するには、その種類を展開してから、そのオブジェクトのチェックボックス（たとえば、特定のデリバリーグループ）をオンにします。

  > 注：
  >
  > アプリケーショングループ、デリバリーグループ、またはマシンカタログは、DaaS での管理に合わせたフォルダー構造で表示されます。フォルダーを選択してそのすべてのオブジェクトを選択したり、フォルダーを展開して特定のオブジェクトを選択したりできます。

- テナント顧客を作成するには、［テナントスコープ］チェックボックスをオンにします。選択した場合、スコープに入力した名前はテナント名です。テナントスコープについて詳しくは、［テナント管理］を参照してください。

完了したら、［**OK**］を選択します。



- スコープのコピー：中央ペインでスコープを選択し、操作バーの ［スコープのコピー］を選択します。名前と説明を変更します。必要に応じて、オブジェクトの種類とオブジェクトを変更します。完了したら、［保存］を選択します。
- スコープの編集：中央ペインでスコープを選択し、操作バーの ［スコープの編集］を選択します。必要に応じて、名前、説明、オブジェクトの種類、およびオブジェクトを変更します。完了したら、［保存］を選択します。
- スコープの削除：中央ペインでスコープを選択し、操作バーの ［スコープの削除］を選択します。確認のメッセージが表示されたら、［削除］をクリックします。

  スコープが役割に割り当てられている場合、そのスコープは削除できません。これを行おうとすると、権限がないことを示すエラーメッセージが表示されます。実際に、このスコープを使用する役割/スコー

プのペアが管理者に割り当てられているので、このエラーが発生します。まず、その役割/スコープのペアの割り当てを、それを使用するすべての管理者から削除します。次に、［管理］コンソールのスコープを削除します。

スコープを作成すると、Citrix Cloud コンソール内の ［カスタムアクセス］ボックスの一覧に表示されます。その後、役割を管理者に割り当てるときに選択できます。

たとえば、CAD という名前のスコープを作成し、CAD アプリケーションに適したマシンを含むカタログを選択するとします。Citrix Cloud コンソールに戻り、役割の ［スコープを編集］を選択すると、使用可能なスコープの一覧に、以前に作成した CAD スコープが表示されます。

クラウド管理者とヘルプデスク管理者には必ず「すべて」スコープが設定されているため、「CAD」スコープは適用されません。

テナント管理

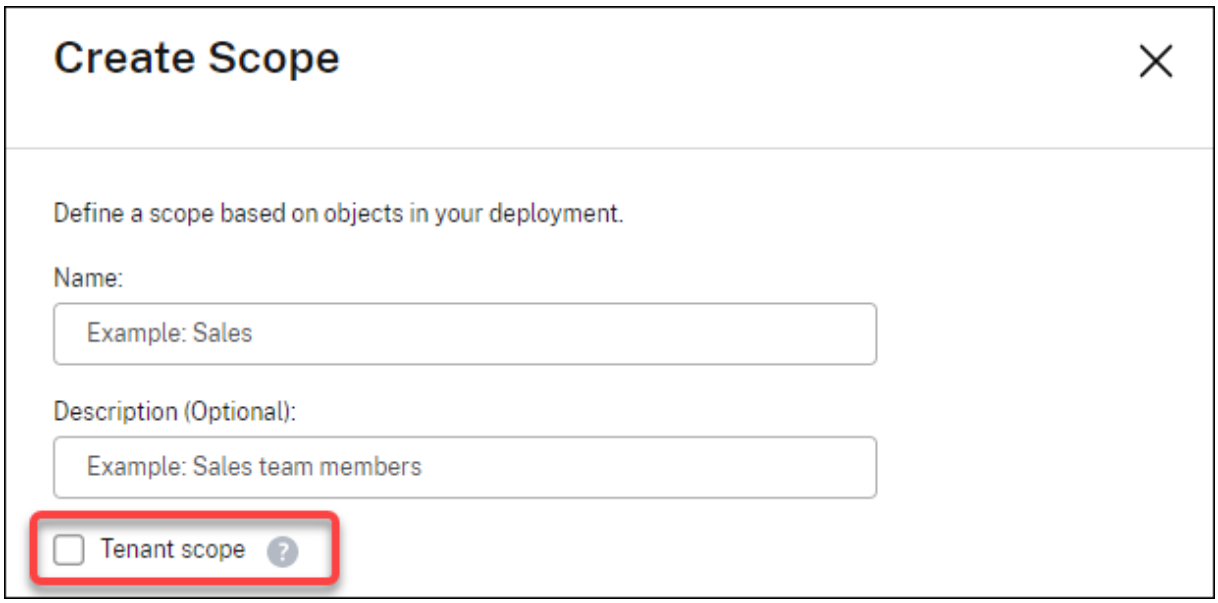
［完全な構成］管理インターフェイスを使用すると、単一の Citrix DaaS の下に相互排他的なテナントを作成できます。構成パーティションは、［管理者］**>**［スコープ］でテナントスコープを作成し、マシンカタログやデリバリーグループなど、関連する構成オブジェクトをそれらのテナントと関連付けることで作成できます。これにより、テナントへのアクセス権を持つ管理者は、テナントに関連付けられているオブジェクトのみを管理できます。

この機能は、たとえば、組織が以下のような場合に役立ちます:

- さまざまなビジネスサイロ（独立した部門または個別の IT 管理チーム）がある、または
- 複数のオンプレミスサイトがあり、単一の Citrix DaaS インスタンスで同じセットアップを維持したいと考えている。

このインターフェイスでは、テナント顧客を名前でフィルタリングできます。デフォルトでは、このインターフェイスにはすべてのテナント顧客に関する情報が表示されます。特定のテナントに関する情報を表示するには、右上隅の一覧からそのテナントを選択します。

テナント顧客の作成　テナント顧客を作成するには、スコープ作成時に ［テナントスコープ］をオンにします。このオプションを選択することにより、異なるビジネスユニット間で Citrix DaaS インスタンスを共有するシナリオにおいて、オブジェクトに適用される一意のスコープタイプを作成します。これらの各ビジネスユニットは、他のビジネスユニットから独立しています。テナントスコープを作成した後は、スコープタイプを変更することはできません。



［スコープ］タブには、すべてのスコープアイテムが表示されます。通常のスコープとテナントスコープの唯一の違いは、［タイプ］列にあります。空白の列フィールドは、通常のスコープを意味します。必要に応じて、［タイプ］列をクリックしてスコープアイテムを並べ替えることができます。

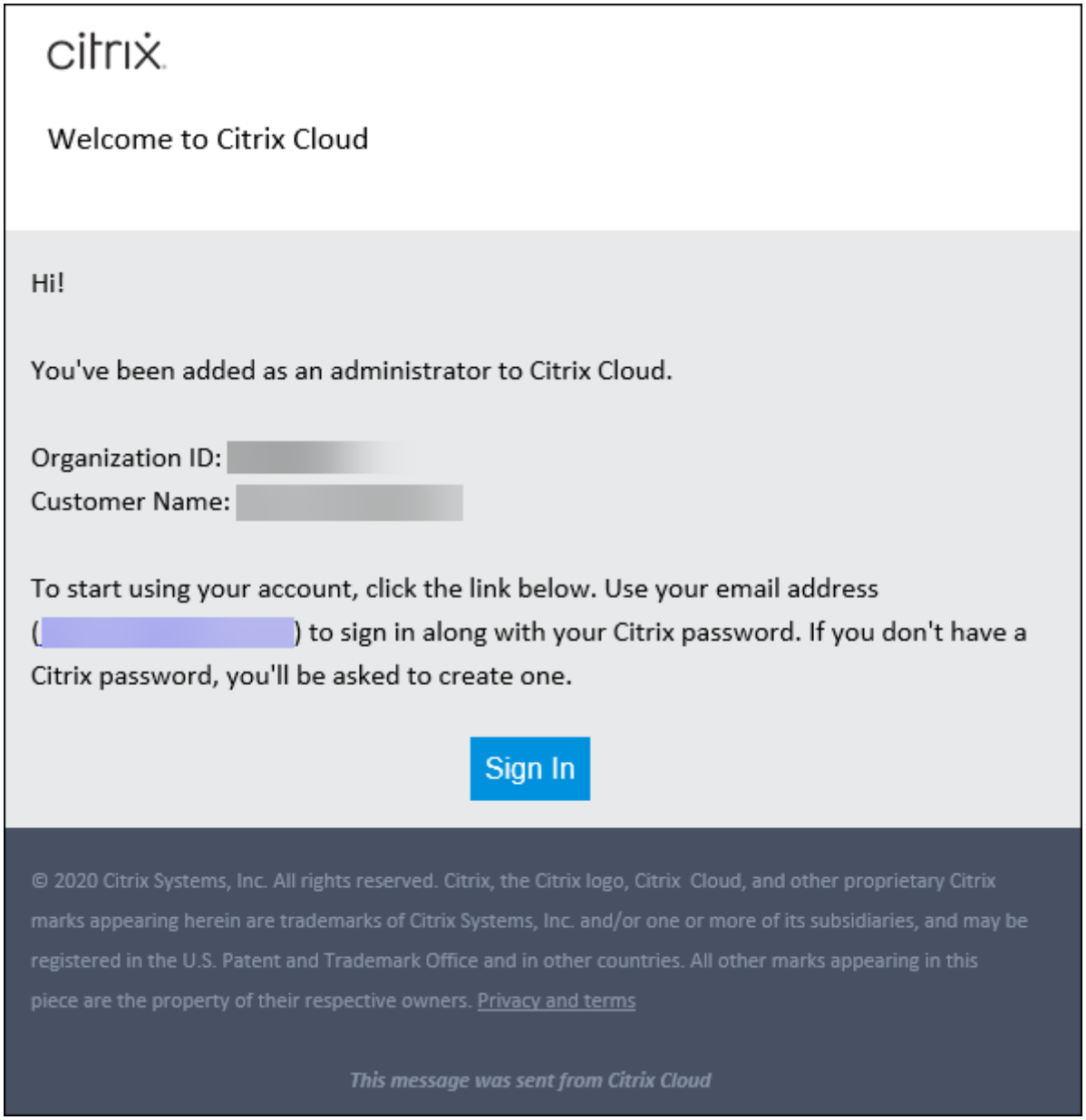
スコープに接続されているリソース（オブジェクト）を表示するには、左側ペインで ［管理者］を選択します。［スコープ］タブでスコープを選択し、操作バーの ［スコープの編集］を選択します。

> ヒント：
>
> テナントプロパティはスコープレベルで割り当てられます。マシンカタログ、デリバリーグループ、アプリケーション、および接続は、該当するスコープからテナントプロパティを継承します。

テナントスコープを使用する場合は、次の考慮事項に注意してください：

- テナントプロパティは、次の順序で割り当てられます：ホスト **>** マシンカタログ **>** デリバリーグループ **>** アプリケーション。下位レベルのオブジェクトは、上位レベルのオブジェクトに依存してテナントプロパティを継承します。たとえば、デリバリーグループを選択するときは、関連するホストとマシンのカタログを選択する必要があります。選択しないと、デリバリーグループはテナントプロパティを継承できません。
- テナントスコープを作成した後、オブジェクトを変更してテナントの割り当てを編集できます。テナントの割り当てが変更された場合でも、同じテナントまたはそれらのテナントのサブセットに割り当てる必要があるという制約があります。ただし、テナントの割り当てが変更されても、下位レベルのオブジェクトは再評価されません。テナントの割り当てを変更するときは、オブジェクトが適切に制限されていることを確認してください。たとえば、TenantAとTenantBのマシンカタログが使用できる場合、TenantAのデリバリーグループとTenantBのデリバリーグループを作成できます（TenantAとTenantBは両方ともそのマシンカタログに関連付けられています）。次に、TenantAのみに関連付けられるようにマシンカタログを変更できます。その結果、TenantBに関連付けられているデリバリーグループは無効になります。

管理者のカスタムアクセス権の構成　テナントスコープを作成したら、それぞれの管理者のカスタムアクセス権を構成します。詳しくは、「管理者のカスタムアクセス権の構成」を参照してください。Citrix Cloud は、指定したこれらの顧客管理者に招待状を送信し、管理者を一覧に追加します。メールを受信した管理者は、［サインイン］をクリックして招待を承諾します。［完全な構成］管理インターフェイスにログオンすると、割り当てられた役割とスコープのペアに含まれるリソースが表示されます。



テナントへのアクセス権を持つ管理者は、テナントに関連付けられているオブジェクト（マシンカタログ、デリバリーグループなど）のみを管理できます。

管理者のカスタムアクセス権の構成

この機能を使用すると、既存の管理者または招待した管理者のアクセス権限を、組織での役割に合わせて定義できます。

アクセス権限に加えた変更が有効になるまで 5 分かかります。[完全な構成] 管理インターフェイスからログアウトして再度ログオンすると、変更がすぐに有効になります。変更が有効になった後も管理者が再接続せずに管理インターフェイスを引き続き使用するシナリオでは、アクセス権限がなくなったアイテムにアクセスしようとすると警告が表示されます。

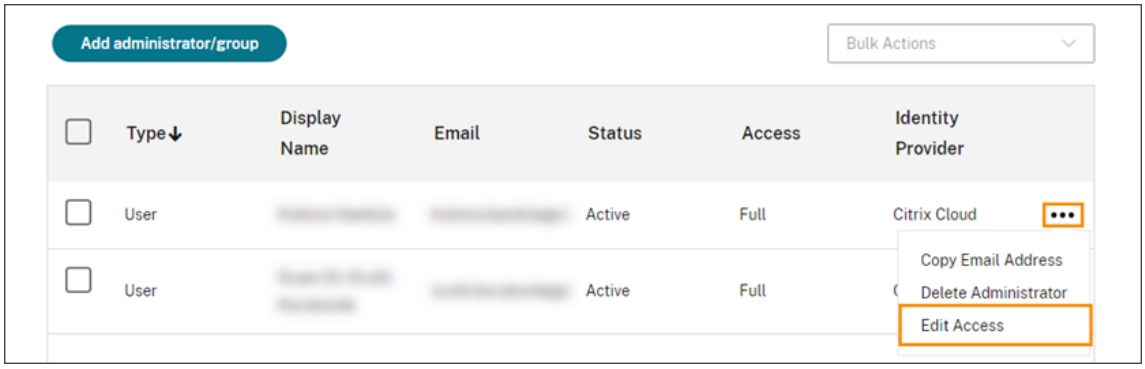
デフォルトでは、管理者を招待すると、それらの管理者にフルアクセス権が与えられます。フルアクセス権があると、管理者は、サブスクライブしているすべてのサービス、および Citrix Cloud 操作（管理者を追加で招待するなど）を管理できます。Citrix Cloud 環境には、フルアクセス権を持つ管理者が少なくとも 1 人必要です。

管理者を招待するときに、カスタムアクセス権を付与することもできます。カスタムアクセス権により、管理者は指定したサービスと操作のみを管理できます。

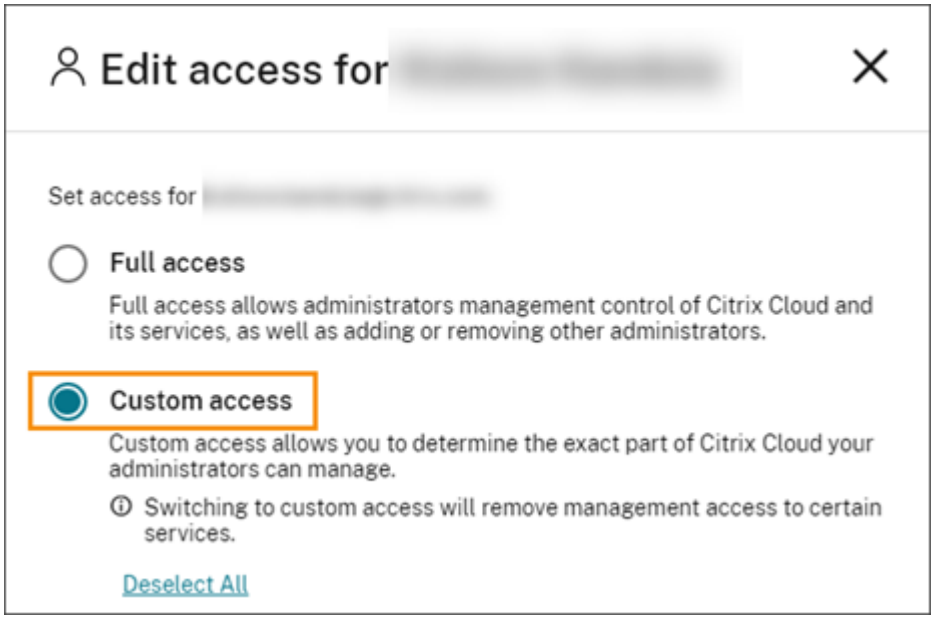
Citrix DaaS で役割またはスコープを作成した場合、Citrix DaaS のカスタムアクセス権一覧に表示され、選択できます。管理者の役割を選択すると、必要に応じてスコープを変更して、組織内の管理者の役割に反映できます。

管理者のカスタムアクセス権を構成するには:

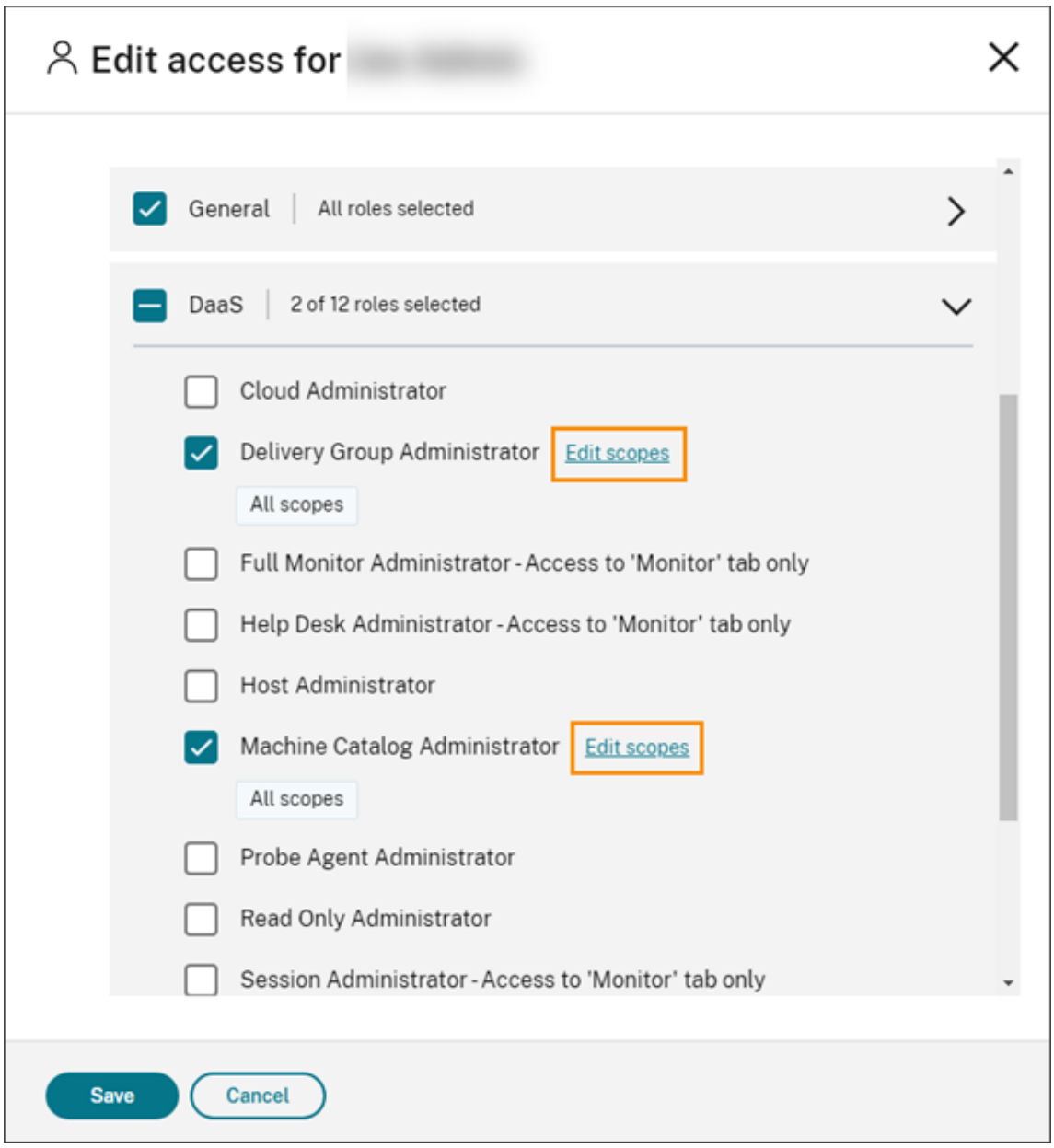
1. Citrix Cloudにサインインします。左上のメニューで [**ID** およびアクセス管理] > [管理者] を選択します。
2. 管理対象の管理者を見つけ、省略記号メニューを選択し、[アクセスの編集] を選択します。



3. [カスタムアクセス] を選択します。

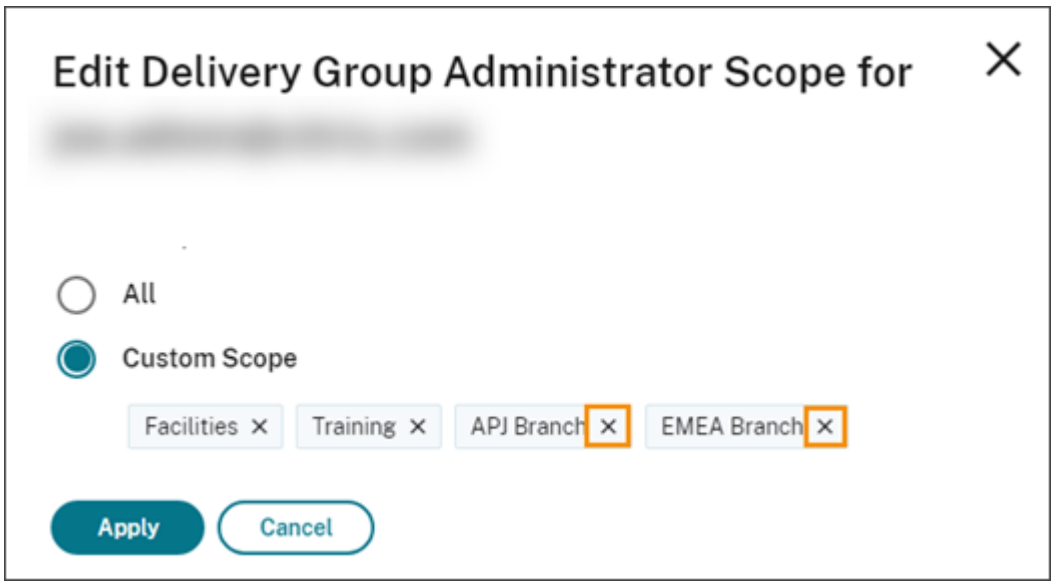


4. **DaaS** の下で、1 つまたは複数の役割の横にあるチェックマークを選択または選択解除します。割り当てられた役割に関連付けられているスコープを変更するには、［スコープの編集］を選択します。

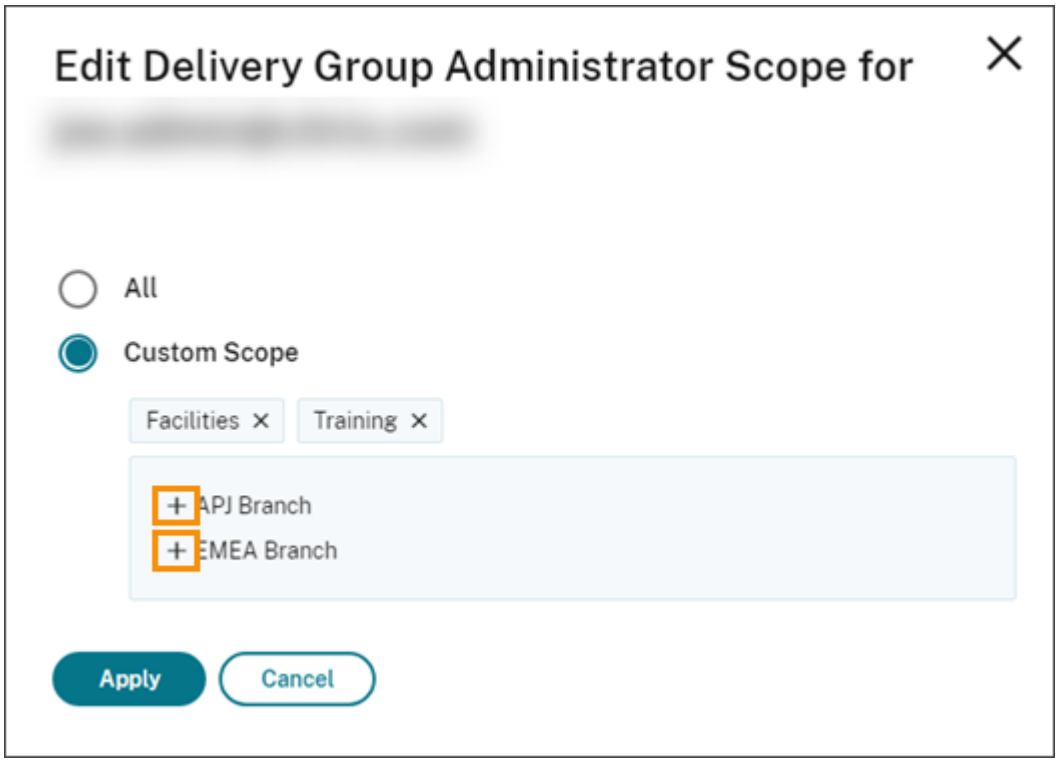


デフォルトでは、［すべてのスコープ］ラベルで示されているように、選択された各役割ですべてのスコープが選択されています。

5. 選択した役割でスコープを指定するには、［カスタムスコープ］を選択し、適切なスコープを追加または削除します。デフォルトでは、すべてのカスタムスコープが役割に追加されます。スコープを削除するには、スコープの［X］アイコンをクリックします。



削除され、役割に追加できるスコープは、既に追加されているスコープの下の一覧に表示されます。役割にスコープを追加するには、スコープのプラスアイコン（+）を選択します。



6. スコープの選択が完了したら、［適用］を選択します。
7. ［保存］を選択して、選択した管理者の役割を保存します。

オンプレミス **Citrix Virtual Apps and Desktops** との相違点

オンプレミスの Citrix Virtual Apps and Desktops 製品の委任管理機能を使い慣れている場合は、Citrix DaaS といくつかの違いがあることに注意してください。

Citrix Cloud の場合:

- 管理者は、Active Directory アカウントではなく、Citrix Cloud ログインによって識別されます。Active Directory の個人（グループではない）の役割/スコープのペアを作成できます。
- 管理者の作成、構成、削除は、Citrix DaaS ではなく Citrix Cloud コンソールで行います。
- 管理者への役割/スコープのペアの割り当ては、Citrix DaaS ではなく Citrix Cloud コンソールで行います。
- レポートは利用できません。サービスの［管理］**>**［完全な構成］インターフェイスでは、管理者、役割、およびスコープ情報を表示できます。
- カスタムアクセス権クラウド管理者は、オンプレミスバージョンでのすべての管理権限を実行できる管理者に似ています。どちらも、使用している Citrix Virtual Apps and Desktops バージョンでの、管理と監視のすべての権限があります。

  ただし、Citrix DaaS では、すべての管理権限を実行できる管理者という名前の役割はありません。Citrix Cloud での「フルアクセス」を、オンプレミスの Citrix Virtual Apps and Desktops での「すべての管理権限を実行できる管理者」と同等と見なさないでください。Citrix Cloud での「フルアクセス」とは、プラットフォームレベルのドメイン、ライブラリ、通知、およびリソースの場所に加え、サブスクライブしているすべてのサービスに及びます。

以前の **Citrix DaaS** リリースとの相違点

拡張カスタムアクセス権機能のリリース（2018 年 9 月）の前は、次の 2 つのカスタムアクセス権管理者役割がありました：すべての管理権限を実行できる管理者、およびヘルプデスク管理者。環境で委任管理（プラットフォームの設定）が有効になっている場合、それらの役割は自動的にマップされます。

- カスタムアクセス権を持つ **Virtual Apps and Desktops**（または **XenApp** および **XenDesktop**）サービス：すべての管理権限を実行できる管理者 として以前に構成されていた管理者は、カスタムアクセス権クラウド管理者になりました。
- カスタムアクセス権を持つ **Virtual Apps and Desktops**（または **XenApp** および **XenDesktop**）サービス：ヘルプデスク管理者 として以前に構成されていた管理者は、カスタムアクセス権ヘルプデスク管理者になりました。

追加情報

サービスの［監視］コンソールで使用される管理者、役割、スコープについて詳しくは、「委任管理と監視」を参照してください。

［完全な構成］インターフェイスのホームページ

October 30, 2023

サブスクリプションを最大限に活用するために役立つ情報と、Citrix DaaS 展開およびワークロードの概要を提供します。このページは次の内容で構成されています：

- サービス概要
- サービス正常性アラート
- 推奨事項
- 新機能
- プレビュー機能
- 開始

ホームページにアクセスするには、次の手順を実行します：

1. Citrix Cloudにサインインします。
2. ［**DaaS**］タイルで、［管理］をクリックします。
3. ［管理］**>**［完全な構成］を選択します。ホームページが表示されます。

サービス概要

Citrix DaaS 展開とワークロードの概要を提供します：

- リソース。展開されたリソースの数をカテゴリ別に表示します。

リソース	カテゴリ別に数を表示する方法
マシン	［マシン］をクリックし、状態を選択してから、ドーナツグラフにカーソルを合わせて詳細を確認します。使用可能なオプション：［可用性の状態］（使用可能、使用中、オフ、または使用不可）、［登録状態］（登録済みおよび未登録）、および ［メンテナンス状態］（保守モードおよび保守モードではない）。可用性の状態別にマシン数を表示する場合、状態をクリックして、対応するマシンの詳細を表示できます。
アプリケーション	［アプリケーション］をクリックし、ドーナツグラフにカーソルを合わせて詳細を確認します。
デリバリーグループ	［デリバリーグループ］をクリックし、ドーナツグラフにカーソルを合わせて詳細を確認します。

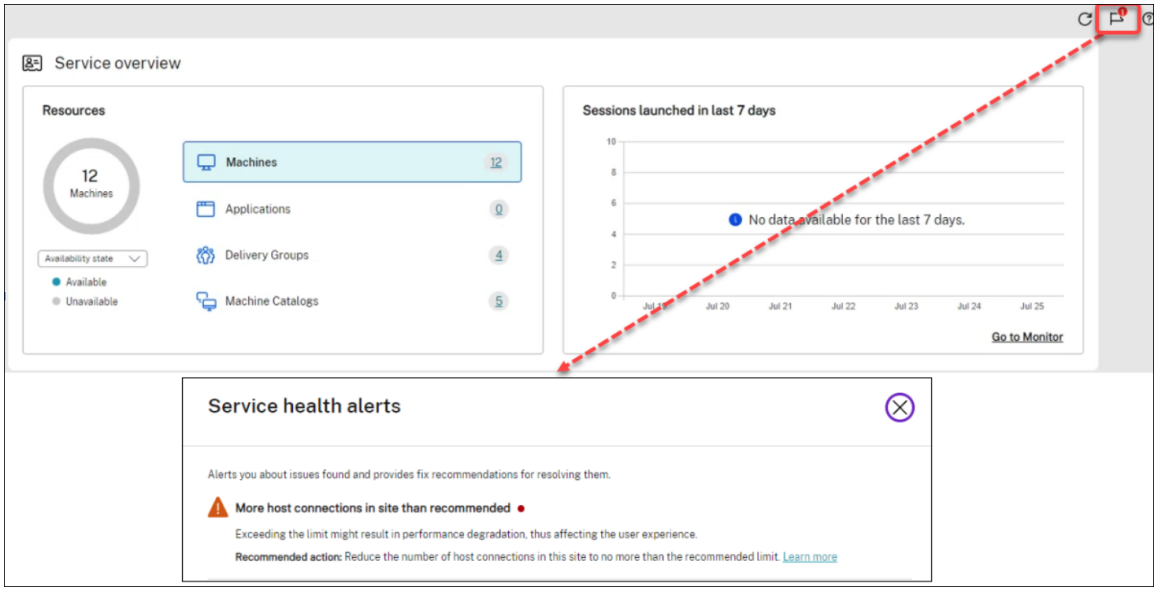
リソース	カテゴリ別に数を表示する方法
マシンカタログ	［マシンカタログ］をクリックし、ドーナツグラフにカーソルを合わせて詳細を確認します。

- 過去 **7** 日間に起動されたセッション過去 7 日間のそれぞれの日に起動されたデスクトップセッションとアプリセッションの数を表示します。詳細にドリルダウンするには、［監視に移動］をクリックします。

サービス正常性アラート

見つかった問題について警告し、解決するための修正推奨事項を提供します。アラートは、警告記号とエラー記号とともに表示されます。

> 注:
>
> 診断は 1 時間ごとに更新されます。
>
> アラートの例:



推奨事項

Workspace Environment ManagementやAutoscaleなど、サブスクリプションで使用できる機能をお勧めします。レコメンドに対して好きか嫌いかのフィードバックを残すことで、当社へお知らせください。

> 注:
>
> 推奨事項に対して低評価アイコンを選択した場合、その推奨事項は表示されなくなります。すべてのレコメン

> ドまたはお勧めウィジェットを嫌いにした場合、お勧めウィジェットは表示されなくなります。

新機能

ビジネスの必要性に応じて選択できる、最新の Citrix DaaS 機能の一覧を表示します。これらの機能を使用すると、サブスクリプションを最大限に活用できます。新機能の完全な一覧については、「新機能」を参照してください。

プレビュー機能

現在プレビュー段階の機能を表示します。フルアクセス権を持つ Citrix Cloud 管理者は、Citrix に連絡することなく、プレビュー機能をオンまたはオフにすることができます。変更が有効になるまでに最大 15 分かかります。

プレビュー機能は、実稼働環境以外での使用をお勧めします。プレビュー機能で見つかった問題は、Citrix テクニカルサポートではサポートされません。

開始

アプリとデスクトップの初期セットアップの手順を示します。

セットアップ手順は次のとおりです:

1. リソースの場所の作成

   リソースの場所とは、ユーザーに配信するアプリケーションとデスクトップがある場所を指します。この手順では、リソースの場所を DaaS に追加し、そこに Cloud Connector をインストールできます。Cloud Connector は、Citrix Cloud とリソースの場所の間ですべての通信を認証および暗号化するチャネルとして機能します。

2. ホスト接続を作成する

   ホストは、リソースの場所で使用されているハイパーバイザーまたはクラウドサービスです。この手順では、DaaS がホスト上の仮想マシンと通信するために使用する情報を指定できます。詳細情報には、リソースの場所、ホストの種類、アクセス資格情報、使用するストレージ方法、およびホスト上の仮想マシンが使用できるネットワークが含まれます。

3. マスターイメージの準備

   マスターイメージには、オペレーティングシステム、必要なすべてのアプリケーション、および Virtual Delivery Agent（VDA）が含まれます。VDA は、VM とユーザーデバイス間の接続を確立して維持します。

4. マシンカタログの作成

   マシンカタログは、ユーザーに割り当てる同一のシングルセッション OS VM またはマルチセッション OS VM のコレクションです。この手順では、プロビジョニングテクノロジ、マスターイメージ、および VM のサイズを指定して、マシンカタログを作成できます。

5. ユーザーを割り当てる

   デリバリーグループは、いくつかのマシンカタログから選択したマシンをグループ化したものです。この手順では、デリバリーグループを作成して、どのチーム、部署、またはユーザーの種類がどのマシンを使用できるかを指定できます。

6. ワークスペースの構成

   ［ワークスペース構成］**>**［アクセス］からワークスペース URL をユーザーと共有します。

ライセンス

March 30, 2022

この記事では、Microsoft ライセンスと Citrix ライセンスのタスクとリソースについて説明します。

Windows Server ワークロード用の **Microsoft RDS** ライセンスサーバーの構成

ここでの情報は、Windows Server ワークロードを配信する場合に適用されます。

このサービスは、Windows 2019 などの Windows Server ワークロードを配信するとき、Windows Server リモートセッション機能にアクセスします。これには通常、リモートデスクトップサービスクライアントアクセスライセンス（RDS CAL）が必要です。VDA は、RDS CAL の要求のために RDS ライセンスサーバーに接続できる必要があります。

ライセンスサーバーをインストールしてアクティブ化してください。詳しくは、Microsoft 社のドキュメント「リモートデスクトップサービスライセンスサーバーをアクティブ化する」を参照してください。概念実証環境では、Microsoft から提供される猶予期間を利用できます。

この方法により、このサービスでライセンスサーバーの設定を適用できます。イメージの RDS コンソールでは、ライセンスサーバーおよび接続ユーザー数モードを構成できます。また、Microsoft のグループポリシー設定を使用して、ライセンスサーバーを構成することもできます。詳しくは、Microsoft 社のドキュメント「クライアントアクセスライセンス（CAL）を使用して RDS 展開をライセンスする」を参照してください。

Microsoft グループポリシー設定を使用して RDS ライセンスサーバーを構成するには:

1. 使用可能な VM に、リモートデスクトップサービスのライセンスサーバーをインストールします。この VM は常に使用可能なものである必要があります。また、Citrix サービスのワークロードが常にこのライセンスサーバーに到達できる必要があります。
2. Microsoft のグループポリシーを使用して、ライセンスサーバーアドレスと単一ユーザーライセンスモードを指定します。　詳しくは、Microsoft 社のドキュメント「リモートデスクトップサービスライセンスサーバーをアクティブ化する」を参照してください。

Windows 10 ワークロードには、適切な Windows 10 ライセンスのアクティブ化が必要です。Microsoft のドキュメントに従って、Windows 10 ワークロードをアクティブ化することをお勧めします。

Citrix ライセンスの使用状況

ライセンスの使用状況に関する情報については、以下を参照してください:

- クラウドサービスのライセンスおよびアクティブな使用状況の監視
- Citrix DaaS のライセンスとアクティブな使用状況の監視

マルチタイプのライセンス

August 18, 2023

マルチタイプのライセンスでは、単一の Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）環境にあるさまざまなライセンス使用権を使用できます。この記事は、Citrix ライセンス使用権が複数ある場合に適用されます。Citrix の使用権は、以下の組み合わせです:

- 製品。ここでは DaaS についてのケースであるため、常に Citrix DaaS
- サービスエディション（例: Advanced、Advanced Plus、Premium、または Premium Plus）
- ライセンスモデル（例: ユーザー/デバイスまたは同時使用）

使用権の混在に関する規則

サービスエディションを混在させる場合の規則は次のとおりです:

- DaaS Advanced と Advanced Plus の混在のみが許可されます
- DaaS Premium と Premium Plus の混在のみが許可されます
- DaaS Standard は他のエディションと混在できません

前述のサービスエディション規則に従っている場合は、ライセンスモデルを混在させることができます。

サイトおよびデリバリーグループレベルでの使用権

ライセンス使用権は、次の 2 つのレベルで構成および使用できます:

- サイト（Citrix DaaS 製品の展開）
- デリバリーグループ

サイトまたはデリバリーグループの使用権をまだ構成していない場合は、次のデフォルトの動作に注意してください:

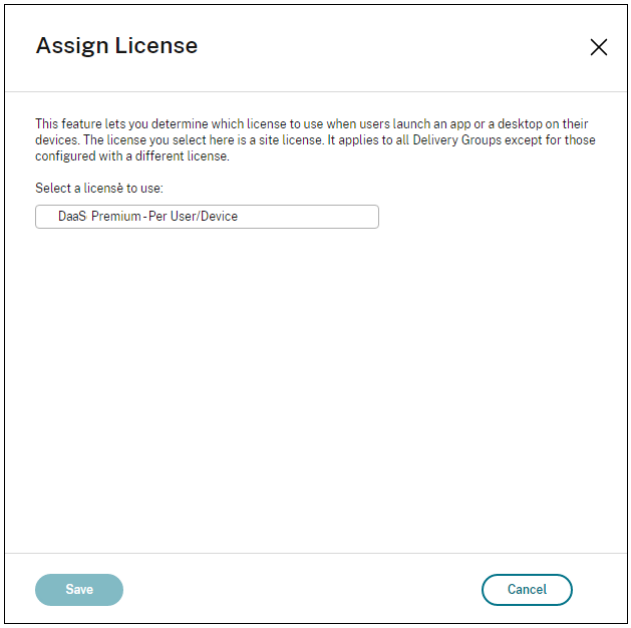
- 同時に注文された複数の使用権をお持ちの場合、利用可能な中で最も機能の高いものがサイト全体の使用権として選択されます。それ以外の場合、後で明示的に変更しない限り、最初に表示されたものがサイト全体のデフォルトの使用権になります。
- デリバリーグループの使用権が構成されていない場合、サイトの使用権が使用されます。

> 注:
>
> サイトまたはデリバリーグループの使用権の構成は、Citrix Cloud で表示されるライセンス使用状況画面で、ライセンス消費がどのようにカウントされるかに影響します。

サイトレベルの使用権の表示および更新

サイト全体で使用するライセンス使用権を指定するには、[完全な構成] > [設定] > [ライセンスの割り当て] に移動して [編集] をクリックします。[ライセンスの割り当て] ブレードが表示されます。[完全な構成] ページにアクセスする方法については、Citrix DaaSのドキュメントを参照してください。

[ライセンスの割り当て] ブレードで、サイトで使用するライセンスを選択します。選択したライセンスは、別のライセンスで構成されているデリバリーグループを除き、サイト上のすべてのデリバリーグループに適用されます。



選択できるライセンスは次のとおりです:

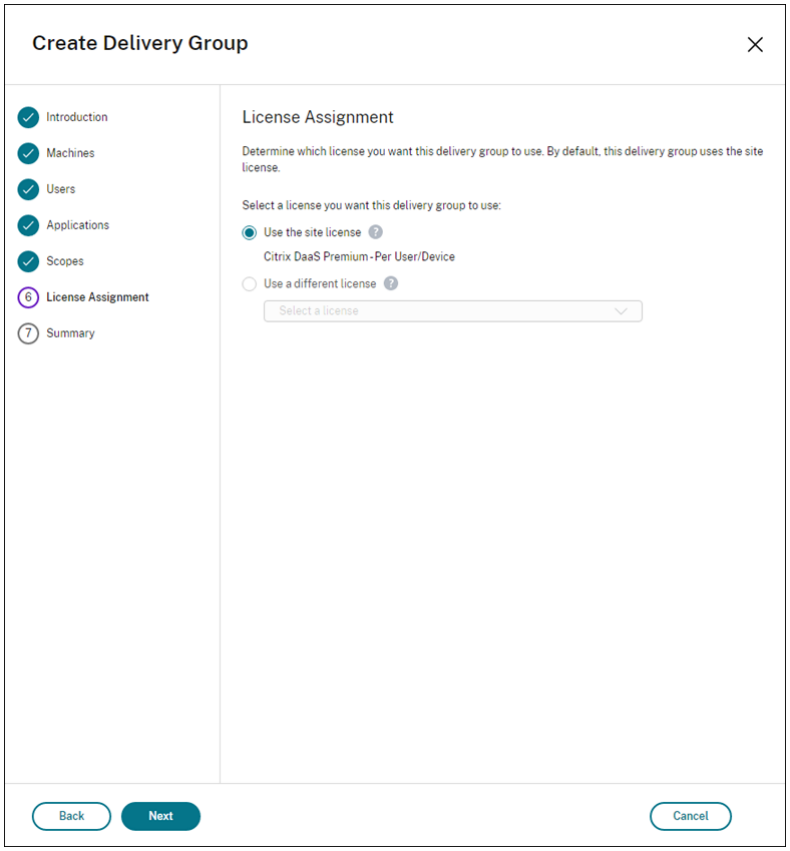
- Citrix DaaS Premium –ユーザー/デバイスごと
- Citrix DaaS Premium –同時使用
- Citrix DaaS Premium for Google Cloud - ユーザー/デバイスごと
- Citrix DaaS Premium for Google Cloud - 同時使用

- Citrix DaaS Advanced –ユーザー/デバイスごと
- Citrix DaaS Advanced –同時使用
- Citrix DaaS Advanced Plus –ユーザー/デバイスごと
- Citrix DaaS Advanced Plus –同時使用
- Citrix DaaS Standard for Azure –ユーザー/デバイスごと
- Citrix DaaS Standard for Azure –同時使用
- Citrix DaaS Standard for Google Cloud - ユーザー/デバイスごと
- Citrix DaaS Standard for Google Cloud –同時使用

有効期限が切れたライセンスがある場合は、Citrix の営業担当者に連絡してライセンスを更新するか、新しいライセンスを購入してください。

デリバリーグループレベルの使用権の表示および更新

デリバリーグループを作成または編集するときに、デリバリーグループが使用するライセンスを指定できます。［ライセンスの割り当て］ページで、オプションを選択します。



オプション:

- サイトライセンスを使用する。サイトライセンスは、別のライセンスで構成されているデリバリーグループを除き、すべてのデリバリーグループに適用されます。このオプションの下に表示されるライセンスは、使用中

のサイトライセンスです。サイトライセンスを構成するには、［管理］**>**［完全な構成］に移動し、［設定］ノードを選択して、［ライセンスの割り当て］を編集します。

- 別のライセンスを使用する。このオプションを使用すると、サイトライセンスとは異なるライセンスを使用するようにこのデリバリーグループを構成できます。ライセンス使用権は、製品コード、エディション、およびライセンスモデルを組み合わせたものです。デリバリーグループは、サイトと同じライセンスエディション（Standard、Premium、または Advanced）を使用する必要があります。ライセンスが構成されている場合、デリバリーグループは選択されたライセンスのみを消費します。選択されたライセンスが完全に消費されたり無効になったりしても、デリバリーグループはサイトライセンスにフォールバックしません。

デフォルトでは、デリバリーグループでサイトのライセンスが使用されます。

デリバリーグループのライセンスの有効期限が切れて有効でなくなった場合、別のライセンスを使用します。

> 注:
>
> 別のライセンスを使用するように後からデリバリーグループを構成すると、現在のライセンスを使用している接続ユーザーは、デスクトップとアプリケーションに一時的にアクセスできなくなる可能性があります。

使用権の混在の例

たとえば、顧客 A が最初に Advanced Edition を購入し、後で Advanced Plus Edition を購入したとします。この場合、顧客 A は Advanced Edition のみのサイト全体で使用されるライセンスを持ったままです。Citrix は、顧客 A がサイトレベルで最初に設定した内容を変更しません。ライセンスエディションをサイトレベルで Advanced Plus に変更するのは、顧客 A の責任です。

同様に、顧客 A は、デリバリーグループのライセンスエディションを Advanced Plus に更新することもできます。この設定が構成されていない場合、デリバリーグループはサイトレベルで設定されたライセンスエディションを継承します。

顧客 A の管理者は、次の方法でライセンスエディションを更新できます:

- サイトレベルのライセンスエディションの更新 - ［管理］**>**［完全な構成］に移動し、［設定］ノードを選択して、［ライセンスの割り当て］を編集します。
- デリバリーグループレベルのライセンスエディションの更新 - ［管理］**>**［完全な構成］に移動し、［デリバリーグループ］ノードを選択します。ターゲットデリバリーグループを編集して変更を加えます。

PowerShell コマンドを使用してデリバリーグループを更新する

デリバリーグループを更新するための PowerShell コマンドは以下のとおりです:

```
1 Set-BrokerDesktopGroup -Name <DGName> -ProductCode <Name of the product
      code> -LicenseModel <The type of license model>
2 <!--NeedCopy-->
```


お使いの環境の詳細に応じて、前述のコマンドを更新してください。

たとえば、次を参照してください:

- `Set-BrokerDesktopGroup -Name DG1 -ProductCode VADS -LicenseModel CONCURRENT`
- `Set-BrokerDesktopGroup -Name DG1 -ProductCode $null -LicenseModel $null`（デリバリーグループレベルの構成をサイトレベルの構成セットに設定します）
- `Set-BrokerSite -CloudSiteLicense VADS:ADVANCED:USERDEVICE`

ライセンスモデルと製品コードがデリバリーグループレベルで設定されていないとします。このシナリオでは、サイトレベルで設定されたこれら 2 つのプロパティがデリバリーグループに使用されます。

Citrix DaaS Remote PowerShell SDK について詳しくは、「SDK および API」のドキュメントを参照してください。

追加情報

- ライセンス
- デリバリーグループの作成
- デリバリーグループの管理

マシンの負荷分散

December 5, 2023

> 注:
>
> この機能は、すべてのカタログ（シングルセッション OS カタログまたはマルチセッション OS カタログ）に適用されます。垂直負荷分散は、マルチセッション OS マシンにのみ適用されます。

負荷分散はサイトレベルとデリバリーグループレベルで構成できます。垂直と水平の 2 つのオプションがあります。デフォルトでは、水平負荷分散が有効になっています。

サイトレベルでの負荷分散設定

- 垂直負荷分散。最大負荷に達していない最も負荷の高いマシンに受信のユーザーセッションを割り当てます。これにより、既存のマシンが飽和状態になった後、新しいマシンに移ります。ユーザーが既存のマシンから切断すると、マシンの容量が解放されます。次に、受信の負荷がこれらのマシンに割り当てられます。垂直負荷分散により、ユーザーエクスペリエンスは低下しますが、コストを削減できます（セッションが電源オンのマシンの処理能力を最大化）。

例：それぞれ 10 セッション用に構成された 2 つのマシンがあります。最初のマシンは、最初の 10 個の同時セッションを処理します。2 つ目のマシンは、11 番目のセッションを処理します。

> ヒント：
>
> マシンがホストできるセッションの最大数を指定するには、最大セッション数ポリシー設定を使用します。

または、PowerShell を使用して、サイト全体で垂直負荷分散を有効または無効にすることができます。`Set-BrokerSite`コマンドレットの`UseVerticalScalingForRdsLaunches`設定を使用します。`Get-BrokerSite`を使用して、`UseVerticalScalingForRdsLaunches`設定の値を表示します。詳しくは、コマンドレットのヘルプを参照してください。

- 水平負荷分散。受信ユーザーセッションを、最も負荷が少なく電源がオンになっている使用可能なマシンに割り当てます。水平負荷分散によりユーザーエクスペリエンスは向上しますが、コストが増加します（より多くのマシンで電源オンの状態が保持されるため）。デフォルトでは、水平負荷分散が有効になっています。

  例：それぞれ 10 セッション用に構成された 2 つのマシンがあります。最初のマシンは 5 つの同時セッションを処理します。2 つ目のマシンも 5 つのセッションを処理します。

この機能を構成するには、［管理］**>**［完全な構成］の左側ペインで ［設定］を選択します。［マルチセッションカタログの負荷分散］でオプションを選択します。

デリバリーグループレベルでの負荷分散設定

デリバリーグループレベルで負荷分散を構成すると、サイトレベルから継承した負荷分散設定を上書きできます。デリバリーグループレベルで垂直負荷分散を選択すると、各マシンの使用率を最大化できます。これはパブリッククラウドのコスト削減に役立ちます。この構成は、新しいデリバリーグループの作成時または既存のデリバリーグループの編集時に実行できます。

水平負荷分散。セッションは、電源がオンになっているマシン間で分散されます。たとえば、2 台のマシンがそれぞれ 10 セッション用に構成されている場合、1 台目のマシンが 5 つ、2 台目のマシンが 5 つの同時セッションを処理します。

垂直負荷分散。セッションは電源オンのマシンの容量を最大化し、マシンコストを節約します。たとえば、2 台のマシンがそれぞれ 10 セッション用に構成されている場合、最初のマシンが最初の 10 個の同時セッションを処理します。2 つ目のマシンは、11 番目のセッションを処理します。

ローカルホストキャッシュ

June 12, 2024

> ヒント：
>
> ［完全な構成］>［ホーム］では、サービス正常性アラート機能により、ローカルホストキャッシュとゾーンが正しく構成されていることを確認するための予防的なアラートが表示されます。これにより、停止が発生した場合でも、ローカルホストキャッシュが機能するためユーザーは影響を受けません。アラートには 2 つのレベルがあります。ホーム（フラグアイコン）に表示されるサイト全体のアラートと、各ゾーンの［トラブルシューティング］タブに表示されるゾーン関連のアラートです。詳しくは、「ゾーン」を参照してください。

ローカルホストキャッシュ（LHC）を使用すると、Cloud Connector が Citrix Cloud と通信できなくなった場合でも、Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）環境での接続仲介操作を続行できるようになります。ローカルホストキャッシュは、ネットワーク接続の切断時間が 60 秒に達すると作動します。

ローカルホストキャッシュがあれば、接続済みのユーザーは、停止状態が発生した場合も途切れることなく作業を続行できます。再接続時および新規接続時の接続遅延は最小限に抑えられます。

> 重要：
>
> オンプレミスの StoreFront 環境を使用している場合は、VDA が登録されている（または登録できる）すべての Cloud Connector を、Delivery Controller として StoreFront に追加する必要があります。StoreFront に追加されていない Cloud Connector は停止モードに移行できないため、ユーザーの起動に失敗することがあります。
>
> オンプレミスの StoreFront を使用しない展開の場合は、Citrix Workspace プラットフォームのサービス継続性機能を使用して、ユーザーが停止中にリソースに接続できるようにします。詳しくは、「サービス継続性」を参照してください。

データコンテンツ

ローカルホストキャッシュには、メインデータベースの情報の一部として次の情報が格納されます：

- サイトから公開されたリソースに対する権限が割り当てられているユーザーおよびグループの ID。
- サイトの公開リソースを現在使用しているか、最近使用したユーザーの ID。
- サイトで構成されている VDA マシン（リモート PC アクセスマシンを含む）の ID。
- 公開リソースへの接続で頻繁に使用されている Citrix Workspace アプリクライアントマシンの ID（名前と IP アドレス）

また、メインデータベースが利用できなくなったときに確立され、現在アクティブな接続に関する情報も格納されています：

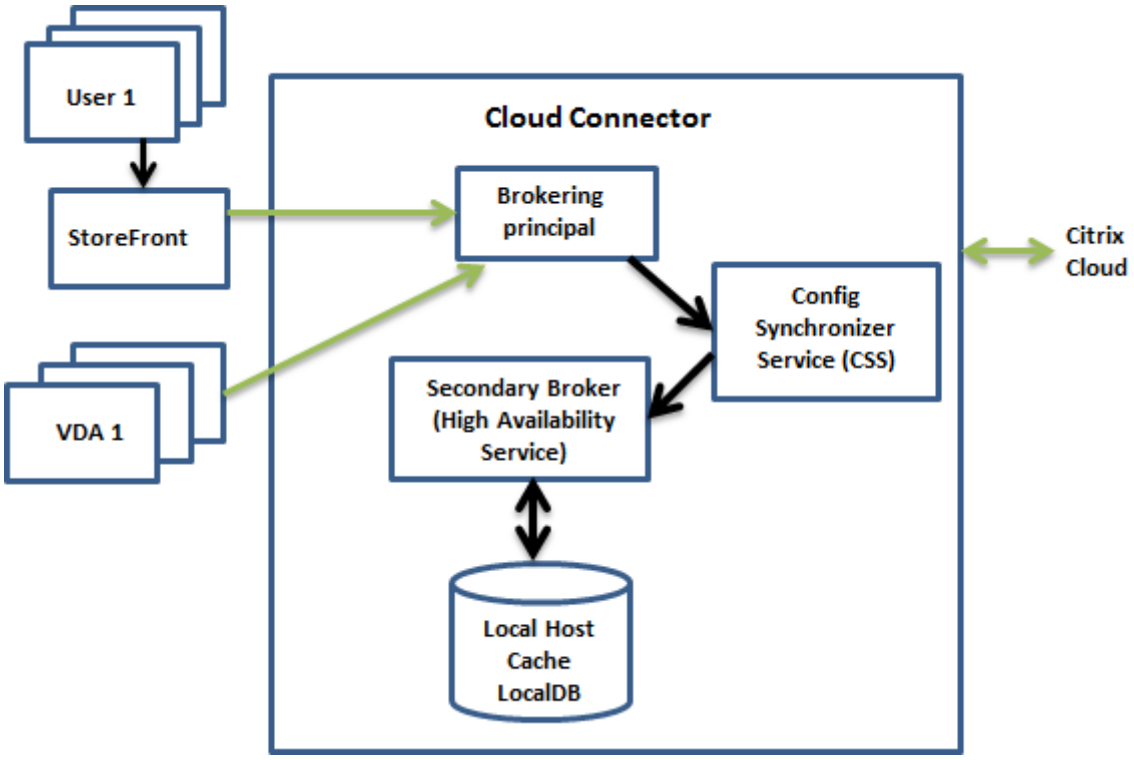
- Citrix Workspace アプリで実行されたクライアントマシンエンドポイント分析の結果
- サイトに関連するインフラストラクチャマシン（Citrix Gateway や StoreFront サーバーなど）の ID
- ユーザーによる最近のアクティビティの日時とタイプ

機能

ローカルホストキャッシュが Citrix Cloud とどのように相互作用するかを表示します。

これは埋め込みビデオです。リンクをクリックしてビデオを見る

通常の操作中



- Cloud Connector 上のプリンシパルブローカー(Citrix Remote Broker Provider Service)は、StoreFront からの接続要求を受け取ります。プリンシパルブローカーは、Citrix Cloud と通信して、Cloud Connector に登録済みの VDA にユーザーを接続します。
- Citrix Config Synchronizer Service（CSS）は、Citrix Cloud のブローカーを 5 分おきにチェックして、構成に変更がないか確認します。こうした変更には、管理者によるもの（デリバリーグループのプロパティの変更など）とシステム操作（マシン割り当てなど）があります。
- 前回のチェック以降に構成が変更された場合、CSS は、Cloud Connector のセカンダリブローカーに情報を同期（コピー）します（セカンダリブローカーは、上記の図で示されているように High Availability Service または HA ブローカーとも呼ばれます)。

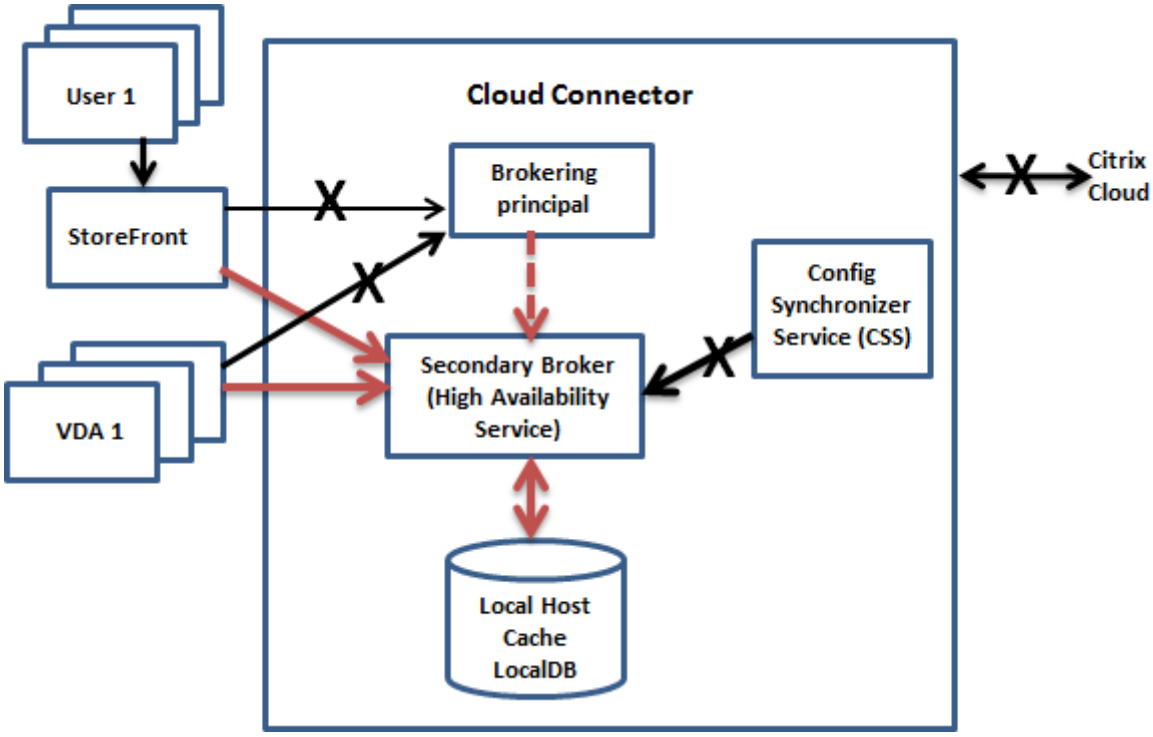
  前回のチェック以降に変更された項目だけでなく、すべての構成データがコピーされます。CSS は、Cloud Connector 上の Microsoft SQL Server Express LocalDB データベースに構成データをインポートします。このデータベースはローカルホストキャッシュデータベースとして参照されます。CSS は、ローカルホストキ

ャッシュデータベースの情報が Citrix Cloud のサイトデータベースの情報と一致することを確認します。ローカルホストキャッシュデータベースは、同期が発生するたびに再作成されます。

Cloud Connector をインストールする場合、（ローカルホストキャッシュデータベースで使用するために）自動で Microsoft SQL Server Express LocalDB がインストールされますローカルホストキャッシュデータベースを Cloud Connector 間で共有することはできません。ローカルホストキャッシュデータベースのバックアップを作成する必要はありません。構成の変更が検出されるたびに再作成されます。

- 前回のチェック以降に変更が発生行われていない場合、構成データはコピーされません。

停止状態中



停止が開始された場合：

- セカンダリブローカーは、接続要求のリッスンと処理を開始します。
- 停止状態の開始時には、セカンダリブローカーに最新の VDA 登録データはありませんが、VDA との通信が始まると登録処理がトリガーされます。その処理中、セカンダリブローカーは、その VDA に関する現在のセッション情報も取得します。
- セカンダリブローカーが接続を処理する間も、プリンシパルブローカーは引き続き Citrix Cloud への接続を監視します。接続が回復すると、プリンシパルブローカーはセカンダリブローカーに接続情報のリスニングを停止するように指示して、仲介操作を再開します。VDA がプリンシパルブローカーと次に通信するときに、登録処理がトリガーされます。セカンダリブローカーは、前回の停止状態以降に残っている VDA 登録をすべて削除します。CSS は、Citrix Cloud で構成が変更されたことを検出すると、情報の同期を再開します。

同期中に停止状態が開始されるという可能性の低い事象では、その時点のインポートは破棄され、最新の既知の構成が使用されます。

イベントログに、同期および停止状態が発生した時刻が記録されます。

停止モードでの操作に時間制限は適用されませんが、

意図的に停止を引き起こすこともできます。これを行う理由と方法について詳しくは、「停止状態の強制」を参照してください。

リソースの場所に **Cloud Connector** が複数存在する場合

CSS は、他のタスクの合間に、リソースの場所内にあるすべての Cloud Connector に関する情報を定期的にセカンダリブローカーに提供しますリソースの場所で他の Cloud Connector を実行している各セカンダリブローカーは、この情報からすべてのピアセカンダリブローカーを把握します。

セカンダリブローカーは独立したチャネルで相互に通信します。これらのセカンダリブローカーは、実行しているマシンの FQDN 名のアルファベット順の一覧を使用して、停止状態が発生したときにどのセカンダリブローカーがゾーン内の仲介操作を担当するかを決定（選出）します。停止状態中、すべての VDA が、選出されたセカンダリブローカーに再登録します。選出されていないゾーン内のセカンダリブローカーは、受信接続と VDA 登録要求を能動的に拒否します。

> 重要:
>
> リソースの場所内の Connector は、`http://<FQDN_OF_PEER_CONNECTOR>:80/Citrix/CdsController/ISecondaryBrokerElection`で相互に接続できる必要があります。Connector がこのアドレスで通信できない場合、複数のブローカーが選出され、ローカルホストキャッシュイベント中に断続的な起動エラーが発生する可能性があります。

停止状態中に、選出されたセカンダリブローカーに障害が発生した場合、別のセカンダリブローカーが選出されて処理を引き継ぎ、VDA は新しく選出されたセカンダリブローカーに登録されます。

停止状態中に Cloud Connector を再起動した場合:

- この Cloud Connector がブローカーに選出されていない場合は、再起動しても影響はありません。
- この Cloud Connector をブローカーに選出している場合は、別 Cloud Connector が選出されて VDA はそちらに登録されます。再起動した Cloud Connector の電源がオンになると、この Cloud Connector が自動的に仲介処理を引き継ぐため、VDA はこちらの Connector にもう一度登録されます。このシナリオでは、登録中にパフォーマンスに影響が生じることがあります。

イベントログには、選出に関する情報が含まれます。

停止状態中にできなくなること、およびその他の相違点

停止モードでの操作に時間制限は適用されませんが、リソースの場所から Citrix Cloud の接続が失われた場合は、可能な限り迅速にリソースの場所の接続を復元することをお勧めします。

停止状態中:

- ローカルホストキャッシュイベント中、完全な構成インターフェイスに一時的にアクセスできない場合があります。完全な構成インターフェイスにアクセスできる場合、HA モードで動作しているリソースの場所にある VDA は、完全な構成インターフェイスでは未登録として表示されます。これらの VDA には、ローカルホストキャッシュで引き続きアクセスできます。
- Remote PowerShell SDK へのアクセスが制限されます。
  - 次のことを最初に行う必要があります:
    * レジストリキー`EnableCssTestMode`を値 1 で追加します: `New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTestMode -PropertyType DWORD -Value 1`
    * SDK プロキシがコマンドレット呼び出しをリダイレクトしようとしないようにするため、SDK 認証を`OnPrem`に設定します: `$XDSDKAuth="OnPrem"`
    * ポート 89 を使用します: `Get-BrokerMachine -AdminAddress localhost:89 | Select MachineName, ContollerDNSName, DesktopGroupName, RegistrationState`
  - これらのコマンドを実行すると、次のものを使用できるようになります:
    * すべての`Get-Broker*`コマンドレット。
- 停止状態中は、監視データが Citrix Cloud に送信されなくなります。このため、［監視］機能には、停止状態中のアクティビティは表示されません。
- ハイパーバイザー資格情報をホストサービスから取得できません。すべてのマシンの電力状態が不明で、電源操作を発行できません。ただし、電源が入っているホスト上の VM を接続要求のために使用することができます。
- 割り当てられたマシンは、通常の操作中に割り当てが発生した場合のみ使用できます。停止状態中は新しい割り当てはできません。
- リモート PC アクセスマシンの自動登録と構成はできません。ただし、通常の操作中に登録、構成されたマシンは使用できます。
- サーバーでホストされるアプリケーションとデスクトップのユーザーは、リソースが異なるゾーンにある場合、構成されている最大セッション数よりも多くのセッションを使用できる場合があります。
- 各ゾーンは、LHC イベント中に個別に動作します。停止状態中は、ゾーン間での起動（あるゾーンのブローカーから別のゾーンの VDA へ）はサポートされません。StoreFront の詳細なヘルス チェック機能を使用して、LHC イベント中に起動要求を適切なゾーンにルーティングします。
- デリバリーグループ内の VDA に対してスケジュールされた再起動が開始される前にサイトデータベースの停止が発生した場合、停止が終了すると再起動が開始されます。このシナリオは意図しない結果につながる可能性があります。詳しくは、「データベースの停止によるスケジュールされた再起動の遅延」を参照してください。
- ［ゾーン優先度］を構成できません。構成されていても、環境設定はセッション起動では考慮されません。

- タグを使用してリソースの場所を指定するタグ制限機能は、セッション起動ではサポートされていません。このタグ制限が構成されていて、StoreFront ストアの ［詳細なヘルスチェック］ オプションが有効になっている場合、セッションが断続的に起動に失敗することがあります。

StoreFront の要件

オンプレミスの StoreFront 環境を使用している場合は、VDA が登録されている（または登録できる）すべての Cloud Connector を、Delivery Controller として StoreFront に追加する必要があります。StoreFront に追加されていない Cloud Connector は停止モードに移行できないため、ユーザーの起動に失敗することがあります。

リソースの可用性

停止状態中のリソースの可用性（アプリとデスクトップ）を確保するには、次の 2 つの方法があります：

- 展開内のすべてのリソースの場所にリソースを公開します。
- StoreFront 1912 CU4 またはそれ以降を使用している場合は、リソースを少なくとも 1 つのリソースの場所に公開し、すべての StoreFront サーバーで詳細なヘルスチェックをオンにします。StoreFront 2308 より前のバージョンでは、詳細なヘルスチェックはデフォルトでオフになっており、管理者が有効にする必要があります。StoreFront バージョン 2308 およびそれ以降では、この機能はデフォルトで有効になっています。詳細なヘルスチェックを有効にする方法の詳細と手順については、「詳細なヘルス チェック」を参照してください。

アプリケーションとデスクトップのサポート

LHC は次の種類の VDA と配信モデルをサポートしています：

VDA の種類	配信モデル	LHC イベント中の VDA の可用性
マルチセッション OS	アプリケーションとデスクトップ	常に利用できます。
シングルセッション OS 静的（割り当て済み）	デスクトップ	常に利用できます。
電源管理されたシングルセッション OS ランダム（プール）	デスクトップ	デフォルトでは利用できません。プールされたデリバリーグループ内の電源管理された VDA に対する、すべてのセッション起動の試みは、デフォルトで失敗します。

> 注：
>
> プールされたデリバリーグループ内の電源管理されたデスクトップ VDA へのアクセスを有効にしても、通常の操作中に構成された`ShutdownDesktopsAfterUse`プロパティの機能結果には影響しません。LHC 中

照してください。
重要：電源管理された、シングルセッションのプールされたマシンへのアクセスを有効にすると、以前のユーザーセッションからのデータと変更が後続のセッションに残る可能性

> にこれらのデスクトップへのアクセスが有効になっている場合、LHC イベントの完了後、VDA は自動的に再起動しません。プールされたデリバリーグループ内の電源管理されたデスクトップ VDA は、再起動するまで以前のセッションのデータを保持できます。VDA の再起動は、ユーザーが LHC 以外の操作中に VDA からログオフしたとき、または管理者が VDA を再起動したときに発生することがあります。

完全な構成を使用し、電源管理されたシングルセッション **OS** のプールされた **VDA** に対して **LHC** を有効にします

完全な構成を使用すると、デリバリーグループごとに、これらのマシンを LHC イベント中に新しい接続で利用できるようにすることができます:

- デリバリーグループの作成中にこの機能を有効にするには、「デリバリーグループの作成」を参照してください。
- 既存のデリバリーグループでこの機能を有効にするには、「デリバリーグループの管理」を参照してください

> 注:
>
> この設定は、電源管理された VDA を配信するプールされたデスクトップデリバリーグループに対する、完全な構成でのみ使用できます。

PowerShell を使用し、電源管理されたシングルセッション **OS** のプールされた **VDA** に対して **LHC** を有効にします

特定のデリバリーグループ内の VDA に対して LHC を有効にするには、次の手順を実行します:

1. 次のコマンドを実行して、サイトレベルでこの機能を有効にします:

   ```
   Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
   ```

2. デリバリーグループ名を指定してこのコマンドを実行し、デリバリーグループの LHC を有効にします:

   ```
   Set-BrokerDesktopGroup -Name "name"-ReuseMachinesWithoutShutdownInOutage
    $true
   ```

電源管理された VDA を含む新しく作成されたプールされたデリバリーグループで、デフォルトの LHC の可用性を変更するには、次のコマンドを実行します:

```
Set-BrokerSite -DefaultReuseMachinesWithoutShutdownInOutage $true
```

ローカルホストキャッシュが動作していることを確認する

ローカルホストキャッシュが正しく構成されていることを確認する方法を以下の動画で説明します。

これは埋め込みビデオです。リンクをクリックしてビデオを見る

ローカルホストキャッシュが適切に設定され動作していることを確認するには:

- StoreFront を使用している場合は、ローカルの StoreFront が、このリソースの場所内のすべての Cloud Connector をポイントしていることを確認します。
- 同期のインポートが正常に完了していることを確認します。イベントログをチェックします。
- 各 Cloud Connector にローカルホストキャッシュデータベースが作成されていることを確認します。これにより、必要に応じて High Availability Service が処理を引き継げるようになります。
  - Cloud Connector サーバーで`c:\Windows\ServiceProfiles\NetworkService`を参照します。
  - `HaDatabaseName.mdf`および`HaDatabaseName_log.ldf`が作成されたことを確認します。
- リソースの場所にあるすべての Cloud Connector を強制的に停止します。ローカルホストキャッシュが動作することを確認したら、すべての Cloud Connector を通常モードに戻します。これには約 15 分かかります。

イベントログ

イベントログに、同期および停止状態が発生した時刻が示されます。イベントビューアーのログでは、停止状態モードは *HA* モードと見なされます。

Config Synchronizer Service

通常の操作中、ローカルホストキャッシュブローカーを使用して CSS が構成データをローカルホストキャッシュデータベースにインポートすると次のイベントが発生することがあります。

- 503: Citrix Config Sync Service が更新された構成を受信しました。このイベントは、Citrix Cloud から更新済みの構成を受信するたびに発生します。このイベントは、同期プロセスが開始されたことを表します。
- 504: Citrix Config Sync Service が更新された構成をインポートしました。構成のインポートが正常に完了しました。
- 505: Citrix Config Sync Service がインポートに失敗しました。構成のインポートが正常に完了しませんでした。過去に正常にインポートされた構成がある場合、停止状態の発生時にはその構成が使用されます。ただし、この構成は現在の構成よりも古いものです。使用可能な過去の構成がない場合、停止状態中、サービスはセッション仲介に参加できません。この場合は、「トラブルシューティング」セクションを確認の上、Citrix サポートにお問い合わせください。
- 507: システムが停止状態であり、ローカルホストキャッシュブローカーが使用中であるため、Citrix Config Sync Service によりインポートが中止されました。サービスは新しい構成を受け取りましたが、停止状態が発生したためインポートは中止されました。これは正常な動作です。
- 510: プライマリ構成サービスから構成サービス構成データを受信していません。
- 517: プライマリブローカーとの通信に問題がありました。
- 518: セカンダリブローカー（High Availability Service）が実行されていないため、Config Sync スクリプトが中止されました。

高可用性サービス

このサービスは、ローカルホストキャッシュブローカーとも呼ばれます。

- 3502：停止状態が発生しローカルホストキャッシュブローカーが仲介操作を実行しています。
- 3503：停止状態が解消され、通常の操作が再開しました。
- 3504：どのローカルホストキャッシュブローカーが選出されたかと、選出に関わった他のローカルホストキャッシュブローカーを示します。
- 3507：ローカルホストキャッシュの更新された状態情報を 2 分ごとに提供します。この情報は、選択されたブローカーでローカルホストキャッシュモードがアクティブであることを示すものです。停止時間、VDA 登録、セッション情報など、停止の概要も含まれます。
- 3508：選択されたブローカー上でローカルホストキャッシュがアクティブではなくなり、通常の操作が復元されたことを通知します。停止時間、ローカルホストキャッシュ（LHC）イベント中に登録されたマシンの数、LHC イベント中に成功した起動の数など、停止の概要も含まれます。
- 3509：選択されていないブローカー上でローカルホストキャッシュがアクティブであることを通知します。2 分ごとの停止時間と選択されているブローカーも通知します。
- 3510：選択されていないブローカー上でローカルホストキャッシュがアクティブでなくなったことを通知します。停止時間と選択されているブローカーも通知します。

Remote Broker Provider

このサービスは、Citrix Cloud と VDA および Cloud Connector 間のプロキシとして機能します。

- 3001：Cloud Connector が HA モードに移行する必要があるかどうかを確認します。このイベントは、Cloud Connector のヘルスチェックが 1 回失敗した後に発生します。60 秒後に追加のヘルスチェックが失敗した場合、Cloud Connector は HA モードに移行します。
- 3002：Cloud Connector が HA モードに移行できないことを通知します。HA モードに移行できない理由はイベント情報に含まれます。
- 3003：Cloud Connector がさまざまな HA モード状態に移行していることを通知します。この図は、HA モードの開始と終了の状態を示しています。イベントでは以下の詳細が提供されます：
  - Cloud Connector の移行前の状態。
  - Cloud Connector の移行後の状態。
  - 前の状態の継続期間。

> 注：
>
> Cloud Connector で、3001 イベントが頻繁に表示されることがあります。これらのイベントはネットワークの状態によって発生する可能性があり、心配する必要はありません。

停止状態の強制

停止状態は意図的に発生させることもできます。

- ネットワークが稼動と停止を繰り返している場合。ネットワークの問題が解決するまで強制的に停止状態にすることにより、通常モードと停止状態モードの移行が繰り返され、VDA 登録ストームが頻繁に発生するのを防げます。
- 障害回復プランをテストするには:
- ローカルホストキャッシュが正常に動作することを確認する場合。

Cloud Connector は強制停止中に更新できますが、予期しない問題が発生する可能性があります。強制停止モードの間隔を避けるために、Cloud Connector の更新のスケジュールを設定することをお勧めします。

強制的に停止状態にするには、各 Cloud Connector サーバーのレジストリを編集します。`HKLM\Software\Citrix\DesktopServer\LHC`で`OutageModeForced`を作成し、`REG_DWORD`を`1`に設定します。この設定により、ローカルホストキャッシュブローカーは Citrix Cloud への接続状態に関係なく停止状態モードに入ります。値を`0`に設定すると、ローカルホストキャッシュブローカーの停止状態モードは終了します。

イベントを確認するには、`C:\ProgramData\Citrix\workspaceCloud\Logs\Plugins\HighAvailabilityService`の`Current_HighAvailabilityService`ログファイルを監視します。

トラブルシューティング

ローカルホストキャッシュデータベースへの同期インポートが失敗し 505 イベントがポストされた場合には、次のトラブルシューティングツールが役立ちます。

CDF トレーシング: ConfigSyncServer モジュールおよび BrokerLHC モジュール向けのオプションが用意されています。これらのオプションと他のブローカーモジュールを組み合わせることで、問題を特定できます。

レポート: 同期インポートが失敗した場合は、レポートを生成できます。このレポートの最後に、エラーの原因となったオブジェクトが記載されています。このレポート機能は同期速度に影響するため、Citrix では使用しないときは無効にしておくことをお勧めします。

CSS トレースレポートを有効化および作成するには、次のコマンドを入力します:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -PropertyType DWORD -Value 1
```

HTML レポートは`C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\CitrixBrokerConfigSyncReport.html`に格納されます。

レポートが生成されたら、次のコマンドを入力してレポート機能を無効にします:

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -Value 0
```


ローカルホストキャッシュ用の **PowerShell** コマンド

PowerShell コマンドを使用して、Cloud Connector 上のローカルホストキャッシュを管理できます。

PowerShell モジュールは、Cloud Connector 上の次の場所にあります。

```
C:\Program Files\Citrix\Broker\Service\ControlScripts
```

> 重要:
>
> このモジュールは Cloud Connector 上でのみ実行します。

PowerShell モジュールのインポート　PowerShell モジュールをインポートするには、Cloud Connector で次のコマンドを実行します。

```
cd C:\Program Files\Citrix\Broker\Service\ControlScripts Import-Module .\HighAvailabilityServiceControl.psm1
```

LHC を管理するための **PowerShell** コマンド　以下のコマンドレットは、Cloud Connector で LHC モードをアクティブ化して管理するのに役立ちます。

コマンドレット	機能
`Enable-LhcForcedOutageMode`	ブローカーを LHC モードにします。`Enable-LhcForcedOutageMode`が正しく機能するには、ローカルホストキャッシュのデータベースファイルが ConfigSync Service によって正常に作成されている必要があります。このコマンドレットは、LHC が実行されていた Cloud Connector でのみ、LHC を強制的にアクティブ化します。LHC をアクティブにするには、リソースの場所内のすべての Cloud Connector でこのコマンドレットを実行する必要があります。
`Disable-LhcForcedOutageMode`	ブローカーの LHC モードを解除します。このコマンドレットは、実行された Cloud Connector 上でのみ LHC モードを無効にします。`Disable-LhcForcedOutageMode`をリソースの場所内のすべての Cloud Connector で実行する必要があります。

コマンドレット	機能
`Set-LhcConfigSyncIntervalOverride`	Citrix Config Synchronizer Service（CSS）が Citrix DaaS サイト内に構成変更がないかをチェックする間隔を設定します。この時間間隔の範囲は 60 秒（1 分）～ 3600 秒（1 時間）です。この設定は、LHC が実行されていた Cloud Connector にのみ適用されます。Cloud Connector 全体で一貫した設定になるよう、各 Cloud Connector でこのコマンドレットを実行することを検討してください。たとえば、次のようになります: `Set-LhcConfigSyncIntervalOverride -Seconds 1200`
`Clear-LhcConfigSyncIntervalOverride`	Citrix Config Synchronizer Service（CSS）が Citrix DaaS サイト内に構成変更がないかをチェックする間隔をデフォルト値の 300 秒（5 分）に設定します。この設定は、LHC が実行されていた Cloud Connector にのみ適用されます。Cloud Connector 全体で一貫した設定になるよう、各 Cloud Connector でこのコマンドレットを実行することを検討してください。
`Enable-LhcHighAvailabilitySDK`	LHC が実行されていた Cloud Connector 内で、すべての`Get-Broker*`コマンドレットへのアクセスを有効にします。
`Disable-LhcHighAvailabilitySDK`	LHC が実行されていた Cloud Connector 内で、Broker PowerShell コマンドレットへのアクセスを無効にします。

> 注:
>
> - Cloud Connector で`Get-Broker*`コマンドレットを実行する場合は、ポート 89 を使用します。例:
>
>   ```
>   - Get-BrokerMachine -AdminAddress localhost:89
>   ```
>
> - LHC モードではない Cloud Connector の LHC ブローカーは、構成情報のみを保持しています。
> - LHC モード中、選択された Cloud Connector の LHC ブローカーは次の情報を保持しています。
>   - リソースの状態
>   - セッションの詳細
>   - VDA 登録
>   - 構成情報

追加情報

以下については、「ローカルホストキャッシュのスケールおよびサイズの考慮事項」を参照してください:

- テスト方法と結果
- RAM サイズの考慮事項
- CPU コアとソケットの構成に関する考慮事項
- ストレージの考慮事項

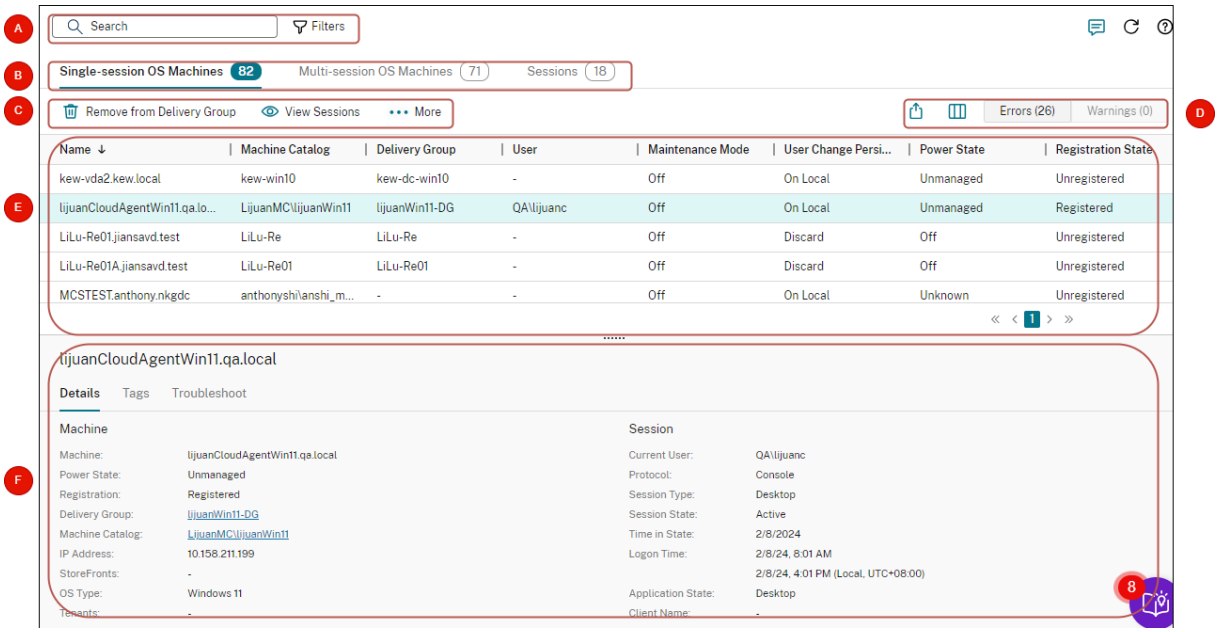
検索を使用してマシンとセッションを監視および管理

June 12, 2024

この記事では、［完全な構成］>［検索］を使用してマシンとセッションを監視および管理する方法について説明します。

このノードについて

検索ノードは、マシンとユーザーセッションをまとめて監視および管理するための場所を提供します。



ラベル	エリア	説明
A	検索バー	クイック検索と、複雑な検索条件を定義できるフィルターベースの検索を提供します。詳しくは、「インスタンスの検索」を参照してください。
B	種類のタブ	マシンを種類別に一覧表示するか、すべてのセッションを表示するタブを表示します。インスタンス数はタブ名に表示されます。
C	インスタンスレベルの操作	選択したインスタンス（マシンまたはセッション）で実行できる操作が表示されます。詳しくは、マシンの操作および セッションの操作を参照してください。
D	一覧レベルの操作	現在の一覧に対して実行できる操作を表示します エクスポートアイコン：メイン ビューに表示されているインスタンスの一覧を CSV ファイルにエクスポートします。
E	メインビュー	表示する列のアイコン：一覧のメインインスタンスとそのプロパティを表示します。表示する列アイコンを選択して、メインビューをカスタマイズできます。使用可能な列について詳しくは、マシンの列およびセッションの列を参照してください。 エラーラベル：このラベルを有効にすると、エラーのある未登録のマシンのみがメインビューに表示されます。問題の詳細を表示するには、［詳細］ペインの［トラブルシューティング］タブに移動します。 警告ラベル：このラベルを有効にすると、警告のある未登録のマシンのみがメインビューに表示されます。問題の詳細を表示するには、［詳細］ペインの［トラブルシューティング］タブに移動します。
F	詳細ペイン	選択したインスタンス（マシンまたはセッション）の詳細 選択したマシンに適用されるタグ 選択したマシンのエラーまたは警告の詳細（問題、考えられる原因、推奨される解決策など）

インスタンスの検索

検索機能を使用して、特定のマシンカタログを見つけます：

- フィルターを使用して検索する
- クイック検索のために現在のフィルターセットを保存する

- 検索バーにフィルターフィールドを固定する
- クイック検索ボックスを使用して検索する
- 高度な検索を行うためのヒント

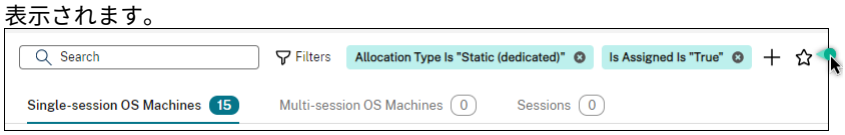
フィルターを使用して検索する

たとえば、静的でユーザーに割り当てられているすべてのシングルセッション OS マシンを見つけるには、次の手順を実行します:

1. [シングルセッション **OS** マシン] タブで、フィルターアイコンをクリックします。フィルターパネルが表示されます。
2. 必要なフィルター基準を追加します。

3. すべてのフィルター基準に一致する結果が検索で返されるようにする場合は、[すべて一致] (AND 演算子) を選択します。いずれかのフィルター基準に一致する結果が検索で返されるようにする場合は、[一部が一致] (OR 演算子) を選択します。
4. [適用] をクリックします。

   フィルター後の一覧には、静的かつユーザーに割り当てられているすべてのシングルセッション OS マシンが表示されます。

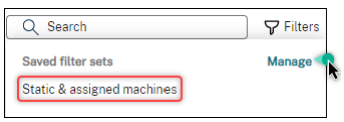


クイック検索のために現在のフィルターセットを保存する

たとえば、静的でユーザーに割り当てられているシングルセッション OS マシンのフィルターセットを以降の検索のために保存するには、次の手順を実行します:

1. フィルターベースの検索を実行した後、上の図に示された検索バーの星のアイコンをクリックします。
2. 表示されたページで、このフィルターセットの名前を入力します (例: 静的で割り当てられたマシン)。
3. [**Save**] をクリックします。

   保存されたフィルターセットは、検索ボックスをクリックすると検索履歴一覧に表示されます。

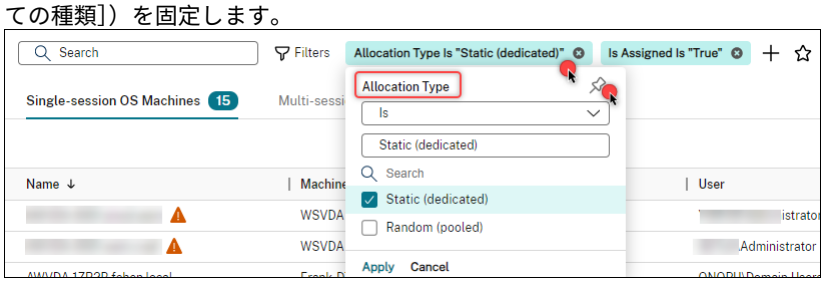


> 注:
>
> フィルターセットはユーザーアカウントごとに保存されます。保存済みのフィルターセットを管理するには、［管理］を選択します。

検索バーにフィルターフィールドを固定する

頻繁に使用するフィルターフィールドを検索バーに固定して、簡単にアクセスできるようにします。たとえば、フィルターベースの検索を実行した後、検索バーに［割り当ての種類］を固定するとします。以下の手順を実行します:

1. 検索バーで「フィルターの設定」** をクリックします。
2. 表示されたパネルで、固定アイコンをクリックして、検索バーのフィルターフィールド（この例では ［割り当ての種類］）を固定します。



クイック検索ボックスを使用して検索する

クイック検索ボックスは、名前関連のプロパティまたは保存されたフィルターセットに基づいてインスタンスを検索する便利な方法を提供します。詳細な手順は次のとおりです:

1. 検索ボックスをクリックします。最近の検索と保存されたフィルターセットがドロップダウンリストに表示されます。以前の検索またはフィルターセットをクリックすると、簡単に検索できます。
2. 新しい検索を開始するには、次のオプションから名前の全部または一部を入力します:

   - マシン名または DNS 名
   - マシンカタログ名
   - デリバリーグループ名
   - セッションユーザー名
   - セッションのクライアント名
   - ハイパーバイザーによって使用される、セッションをホストする仮想マシンのフレンドリ名
   - ホストサーバー名

高度な検索を行うためのヒント

検索機能を使用するときは、次のヒントを考慮してください:

- ［検索］ノードで、任意の列を選択してアイテムを並べ替えます。
- 検索と並べ替えができる画面に追加の特性を表示するには、［表示する列］を選択するか、任意の列をクリックして ［表示する列］を選択します。［表示する列］ウィンドウで、表示するアイテムの横にあるチェックボックスをオンにし、［保存］を選択して終了します。

  > 注:
  >
  > パフォーマンスを低下させる列には、［パフォーマンスの低下］ラベルが付きます。

- マシンに接続しているユーザーデバイスを検索するには、［クライアント（**IP**）］および ［次のもの］を指定してデバイスの IP アドレスを入力します。
- アクティブなセッションを検索するには、［セッション状態］、［次のもの］、［接続済み］を指定します。
- デリバリーグループ内のすべてのマシンを一覧表示するには、左側ペインで ［デリバリーグループ］を選択します。グループを選択し、操作バーまたはコンテキストメニューから ［マシンの表示］を選択します。

並べ替え操作を実行するときは、次の考慮事項に留意してください:

- アイテムの数が 5,000 を超えない限り、任意の列をクリックしてその中のアイテムを並べ替えることができます。数が 5,000 を超える場合は、（現在のタブに応じて）名前または現在のユーザーでのみ並べ替えることができます。並べ替えを有効にするには、フィルターを使用してアイテムの数を 5,000 以下に減らします。
- アイテム数が 500 を超え 5,000 を超えない場合:
  - 並べ替えのパフォーマンスを向上させるために、すべてのデータをローカルにキャッシュします。［シングル セッション **OS** マシン］タブと ［マルチセッション **OS** マシン］タブでは、列（［名前］列を除く任意の列）を最初にクリックして並べ替えたときにデータがキャッシュされます。［セッション］タブでは、列（［現在のユーザー］列を除く任意の列）を最初にクリックして並べ替えたときにデータがキャッシュされます。その結果、並べ替えの完了に時間がかかります。パフォーマンスを向上させるには、名前または現在のユーザーで並べ替えるか、フィルターを使用してアイテムの数を減らします。
  - 表の下にある次のメッセージは、データがキャッシュされていることを示しています。最終更新: <the time when you refreshed the table>。この場合、並べ替え操作は以前に読み込まれたアイテムに基づいて行われます。これらのアイテムは最新ではない可能性があります。最新にするには、更新アイコンをクリックします。

表示する列のカスタマイズ

パーソナライズされたメイン ビューを作成して、日常の操作に重要なプロパティとステータスを表示します。詳細な手順は次のとおりです:

1. 検索ノードで、必要に応じて ［マルチセッション **OS** マシン］、［シングルセッション **OS** マシン］、または ［セッション］タブを選択します。

2. 操作バーの 表示する列アイコンをクリックし、列を選択します。

   使用可能な列とその説明について詳しくは、「マシン列」および「セッション列」を参照してください。

列の選択中、［パフォーマンスの低下］ラベルの付いた列が表示されることがあります。これらの列を選択すると、コンソールのパフォーマンスが低下する可能性があります。次の考慮事項に留意してください:

- カスタマイズの完了後、テーブルが更新され、選択した列が表示されます。このような列が存在すると、テーブルを更新するときに遅延が発生する可能性があります。
- ブラウザーを更新するか、コンソールからサインアウトしてサインインすると、これらの列を保持するかどうかを尋ねるメッセージが表示されます。それらを保持することを選択した場合、コンソールのパフォーマンスを最適化するために、テーブルの更新間隔が 1 分以下にならないように制限されます。より頻繁に更新するには、パフォーマンスを低下させる列を削除します。

マシンとセッションの管理

検索ノードの操作を使用して、マシンやセッションの問題のトラブルシューティングを行ったり、ユーザー要求を処理したりできます。

ヒント

さまざまなレベルでマシンを管理できます:

- 個別のマシンレベルの場合。検索ノードを使用してターゲットマシンを見つけ、操作を実行します。
- マシンカタログレベルの場合。カタログのマスターイメージの変更、カタログからのマシンの削除、カタログへのマシンの追加など。詳しくは、「マシンカタログの管理」を参照してください。
- デリバリーグループレベルの場合。グループ内のマシンのメンテナンスモードのオンまたはオフなど。詳しくは、「デリバリーグループの管理」を参照してください。

個別のセッションレベルに加えて、デリバリーグループのセッションの事前起動や残留の構成など、デリバリーグループレベルでセッションを管理することもできます。詳しくは、「デリバリーグループの管理」を参照してください。

マシンまたはセッション上で操作を実行する

個別のインスタンスレベルでマシンまたはセッションを管理するには、次の手順を実行します:

1. 検索ノードで、［マルチセッション **OS** マシン］、［シングルセッション **OS** マシン］、または ［セッション］タブを選択します。
2. 必要に応じて 1 つまたは複数のインスタンスを選択します。

3. 操作バーまたは右クリックメニューから、インスタンスまたはユーザー要求で発生した問題に基づいて操作を選択します。

   使用可能な操作とその説明について詳しくは、「マシンの操作」および「セッションの操作」を参照してください。

> 注:
>
> 2 つ以上のインスタンスを選択した場合、それらすべてに適用される操作のみが使用可能になります。

マシンまたはセッションのデータを **CSV** ファイルにエクスポート

タブに表示されているインスタンス（マシンまたはセッション）の一覧（最大 30,000 項目）を CSV ファイルにエクスポートします。詳細な手順は次のとおりです:

1. 検索ノードで、必要に応じて［マルチセッション **OS** マシン］、［シングルセッション **OS** マシン］、または［セッション］タブを選択します。
2. 右上隅にあるエクスポートアイコンをクリックします。
3. ダイアログボックスが表示されたら、［続行］をクリックします。

   エクスポートが完了するまでに数分かかる場合があります。このファイルは、ブラウザーのデフォルトのダウンロードフォルダーにあります。

> 注:
>
> 検索ノードの各タブでは、エクスポートの進行中に別のエクスポートを実行することはできません。

マシンの操作と列

June 12, 2024

この記事では、参照用にマシンの操作と列を記載します。

操作

マシン上で実行できる操作とその説明を表示します。

アクション	説明	適用先
ヘルスチェックの実行	登録済みの Windows VDA バージョン 2019 以降でのみ使用できます。マシン上でヘルスチェックを実行します。確認する内容について詳しくは、「ヘルスチェックについて」を参照してください。	シングルセッションとマルチセッション
デリバリー グループから削除	デリバリーグループからのマシンを削除します。	シングルセッションとマルチセッション
デリバリーグループに追加	マシンをデリバリーグループに追加します。	シングルセッションとマルチセッション
セッションの表示	マシン上で実行中のセッションを表示します	シングルセッションとマルチセッション
タグの管理	マシンのタグを追加および管理します。タグの一般的な使用例について詳しくは、「タグ」を参照してください。	シングルセッションとマルチセッション
メンテナンスモードをオンにする	パッチを適用する前、またはトラブルシューティングの際には、マシンをメンテナンスモードにします。このモードでは、そのマシンに新たに接続できなくなります。ユーザーはそのマシンの既存のセッションに接続できますが、そのマシンの新しいセッションを開始することはできなくなります。	シングルセッションとマルチセッション
メンテナンスモードをオフにする	マシンのメンテナンスモードをオフにします。	シングルセッションとマルチセッション
VDA のアップグレード	マシンの VDA をアップグレードします。	特定の要件を満たすシングルセッションまたはマルチセッション OS マシン：詳細情報。
ログオフ	マシンを強制的にログオフします	シングルセッションとマルチセッション
削除	VM をハイパーバイザーまたはクラウドサービス上にそのまま残して、マシンカタログから VM を削除します。	シングルセッションとマルチセッション
ユーザーの変更	マシンを特定のユーザーに割り当てます。	シングルセッションの静的マシン。

アクション	説明	適用先
開始	マシンを起動します。	シングルセッションとマルチセッション
シャットダウン	マシンをシャットダウンします。	シングルセッションとマルチセッション
再起動	マシンを再起動します	シングルセッションとマルチセッション
一時停止	マシンを休止状態または一時停止状態にします。マシンを一時停止すると、DaaS はマシンのメモリ内容をファイルに保存し、マシンをシャットダウンします。	シングルセッション OS マシン
再開	一時停止したマシンを再開します。一時停止したマシンを再開すると、DaaS はマシンを起動し、以前の状態に復元します。	シングルセッション OS マシン
強制再起動	マシンを強制的に再起動します。	シングルセッション OS マシン
強制シャットダウン	マシンを強制的にシャットダウンします。	シングルセッション OS マシン

列

すべてのマシン列とその説明を種類別に表示します:

- マシン
- マシンの詳細
- アプリケーション
- ホスト
- 接続
- 登録
- セッションの詳細
- セッション

マシン

マシン カテゴリの列。

列	説明	適用先
名前	マシンの DNS ホスト名です。	シングルセッションとマルチセッション
マシンカタログ	マシンが属するカタログの名前。	シングルセッションとマルチセッション
デリバリーグループ	マシンが属するデリバリーグループの名前。	シングルセッションとマルチセッション
ユーザー表示名	マシンに関連付けられているユーザーのフルネーム（通常は `Firstname Lastname`の形式）。関連付けられたユーザーは、共有マシンの現在のユーザーと、専用マシンの割り当てられたユーザーです。	シングルセッションとマルチセッション
ユーザー	マシンに関連付けられているユーザーのユーザー名（「ドメイン\ユーザー」の形式）。関連付けられたユーザーは、共有マシンの現在のユーザーと、専用マシンの割り当てられたユーザーです。	シングルセッションとマルチセッション
ユーザープリンシパル名	マシンに関連付けられているユーザーのユーザープリンシパル名（「ユーザー @ ドメイン」の形式）。関連付けられたユーザーは、共有マシンの現在のユーザーと、専用マシンの割り当てられたユーザーです。	シングルセッションとマルチセッション
デスクトップの表示名	セッションの起動に最初に使用されたマシンの公開名。これは、Citrix Workspace アプリまたは StoreFront に表示される名前です。注：デスクトップの表示を変更するには、［マシンの更新］の権限が必要です。表示名の変更にはマシンプロパティの更新が含まれるためです。	シングルセッションのみ
デスクトップ状態	マシンの未処理のデスクトップ状態の一覧。設定可能な値：不明、CPU、ICA 遅延、および UPM ログオン時間。	シングルセッションとマルチセッション

列	説明	適用先
割り当ての種類	マシンの割り当ての種類：無期限。ユーザーに無期限で割り当てられる場合。ランダム。ランダムに割り当てられる場合。	シングルセッションとマルチセッション
メンテナンスモード	マシンがメンテナンス モードであるかどうかを示します。	シングルセッションとマルチセッション
Windows 接続設定	Windows によって報告されたログオンモード。 設定可能な値：ログオン有効、ドレイン中、再起動するまでドレイン中、およびログオン無効。	マルチセッションのみ
割り当て済み	専用デスクトップがユーザーまたはクライアントに割り当てられているかどうかを示します（名前/アドレス）。ユーザーは明示的に割り当てることも、初回使用時割り当てで割り当てることができます。	シングルセッションとマルチセッション
物理的	マシンが物理的かどうかを示します。`True`はマシンが物理的であることを示し、DaaS によって電源管理されていないことを意味します。`False`はそうでないことを示します。	シングルセッションとマルチセッション
プロビジョニングの種類	マシンがプロビジョニングされた方法。設定可能な値： 手動：PVS または MCS を使用してプロビジョニングされていません。 PVS：PVS を使用したプロビジョニング（物理マシン、ブート デバイス、仮想マシン） MCS：MCS を使用したプロビジョニング（VM のみ）	シングルセッションとマルチセッション
スケジュールされた再起動	マシンのスケジュールされた再起動操作の状態。設定可能な値： なし：再起動はスケジュールされていません。 保留中：再起動を待機中ですが、使用できます。 ドレイン中：再起動を待機しているため、新しいセッションには使用できませんが配置されて既存の接続の再接続は引き続き許可されます。 進行中：スケジュールされた再起動が進行中です。 ドレイン中：スケジュールされた再起動が進行中です。マシンは再起動を待機しています。	シングルセッションとマルチセッション
ゾーン	マシンが配置されているゾーンの名前。	シングルセッションとマルチセッション

列	説明	適用先
状態	マシンに関連付けられたデスクトップの全体的な状態。セッション状態、登録状態、電源状態などのさまざまな特定の状態から派生します。 想定できる状態：オフ、未登録、使用可能、切断、使用中、および準備中。	シングルセッションとマルチセッション
タグ	マシンに関連付けられたタグの一覧。	シングルセッションとマルチセッション
VDA のアップグレード	VDA パッケージのアップグレード操作のマシンの状態。 設定可能な値：MissingUpgradeType、UpgradeScheduled、UpgradeAvailable、UpToDate、および Unknown。	シングルセッションとマルチセッション
一時停止が可能	マシンが電源操作（一時停止および再開）をサポートしているかどうかを示します。	シングルセッションとマルチセッション
負荷インデックス	現在の負荷インデックス。詳しくは、詳細情報を参照してください。	マルチセッションのみ
ドレイン状態	マシンがドレイン中であり、マシン上のすべてのセッションが終了した後にシャットダウンするかどうかを示します。True は、電源管理されたマルチセッションマシンの場合にのみ表示されます。 注：マシンがメンテナンスモードの場合、マシンはシャットダウンしません。メンテナンスモードをオフにした後にのみシャットダウンします。	マルチセッションのみ

マシンの詳細

マシンの詳細カテゴリの列。

列	説明	適用先
エージェントのバージョン	マシン上にインストールされた Virtual Desktop Agent（VDA）のバージョンです。	シングルセッションとマルチセッション
IP アドレス	マシンの IP アドレス。	シングルセッションとマルチセッション
割り当て済み	専用デスクトップがユーザーまたはクライアントに割り当てられているかどうかを示します（名前/アドレス）。ユーザーは明示的に割り当てることも、初回使用時割り当てで割り当てることができます。	シングルセッションとマルチセッション
OS の種類	マシンで実行されているオペレーティングシステムの種類です。	シングルセッションのみ

アプリケーション

アプリケーションカテゴリの列。

列	説明	適用先
使用中のアプリケーション	マシン上で使用中のアプリケーションの一覧（ブラウザー名として表示）。	シングルセッションとマルチセッション
公開アプリケーション	マシンで公開されたアプリケーションの一覧（ブラウザー名として表示）。	シングルセッションとマルチセッション

接続

接続カテゴリの列。

列	説明	適用先
クライアント（IP）	マシンに接続されているクライアントの IP アドレス。	シングルセッションのみ
クライアント	マシンに接続されているクライアントのホスト名。	シングルセッションのみ

列	説明	適用先
プラグインのバージョン	接続されたクライアント上の Citrix Workspace アプリのバージョン。	シングルセッションのみ
接続経由	受信接続のホスト名（通常はゲートウェイ、ルーター、またはクライアント）。	シングルセッションのみ
接続経由（IP アドレス）	受信接続の IP アドレス（通常はゲートウェイ、ルーター、またはクライアント）。	シングルセッションのみ
接続の種類	セッションに使用されるプロトコル。設定可能な値：HDX、RDP、およびコンソール。注：XenDesktop 5 VDA 上のコンソールセッションの場合、フィールドは空白のままです。	シングルセッションのみ
前回の接続時間（UTC）	最後に検出された接続試行が失敗または成功した時間。	シングルセッションとマルチセッション
直前の接続ユーザー	最後にマシンへの接続を試みたユーザーの SAM 名（「ドメイン\ユーザー」の形式）。SAM 名が使用できない場合は、SID が使用されます。	シングルセッションとマルチセッション
SecureICA アクティブ	SecureICA が現在のセッションでアクティブであるかどうかを示します。マルチセッションマシンの場合は常に null。	シングルセッションとマルチセッション

ホスト

ホストカテゴリの列。

列	説明	適用先
VM	これは、ハイパーバイザーによって使用されセッションを実行する、ホストされているマシンのフレンドリ名です。マシンの DNS 名や AD 名と必ずしも一致するとは限りません。	シングルセッションとマルチセッション
ホストサーバー名	管理対象のマシンをホストするハイパーバイザーの DNS 名です。	シングルセッションとマルチセッション

列	説明	適用先
接続	セッションをホストするマシンに割り当てられたホスト接続の名前。	シングルセッションとマルチセッション
更新保留中	ホストされているマシンの VM イメージが古いため、マシンの次回の再起動時に新しいイメージに更新される予定であるかどうかを示します。	シングルセッションとマルチセッション
ユーザー変更の保持	ユーザーの変更がどのように処理されるか、変更が永続的であるかどうかを示します: ローカル上：永続的。ユーザーによる変更はローカルに保存されます。 なし：非永続的。ユーザーによる変更は破棄されます。	シングルセッションとマルチセッション
保留中の電源操作	マシンに対して保留中の電源操作があるかどうかを示します。	シングルセッションとマルチセッション
電源状態	マシンの電源状態。設定可能な値: 非管理、不明、使用不可、オフ、オン、一時停止、投入中、シャットダウン中、一時停止中、および再開中。	シングルセッションとマルチセッション
使用後にシャットダウン	電源管理されたシングルセッションのマシンにのみ適用されます。マシンが不良状態であり、マシン上のすべてのセッションが終了した後にシャットダウンするかどうかを示します。 注：マシンがメンテナンスモードの場合、シャットダウンされません。メンテナンスモードを解除した後にのみシャットダウンします。	シングルセッションのみ

登録

登録カテゴリの列。

列	説明	適用先
前回の登録エラー	マシンがブローカーで最後に登録解除された理由。	シングルセッションとマルチセッション

列	説明	適用先
	設定可能な値は次のとおりです：エージェントのシャットダウン、エージェント一時停止、エージェント要求、非互換バージョン、エージェント アドレス解決の失敗、エージェントとの通信不可、エージェントの Active Directory OU が正しくない、登録要求が空、登録機能がない、エージェントバージョンがない、登録機能に整合性がない、機能のライセンスがない、サポートされていない資格情報セキュリティ バージョン、無効な登録要求、シングル/マルチ セッションの不一致、カタログに対して機能レベルが低すぎる、デスクトップ グループに対して機能レベルが低すぎる、電源オフ、デスクトップが再起動した、デスクトップが削除された、デスクトップが削除された、送信設定エラー、セッション監査エラー、セッション準備エラー、接続の損失、設定作成エラー、不明なエラー、および ブローカー登録制限に到達した。	
前回の登録エラー時刻（UTC）	マシンが最後に登録解除された時間。	シングルセッションとマルチセッション
登録状態	マシンの登録状態。設定可能な値：未登録、初期化中、登録済み、および エージェントエラー。	シングルセッションとマルチセッション
障害の状態	マシンの現在の障害の状態に関する概要。設定可能な値： なし：障害はありません。マシンは正常です。 起動に失敗：マシンの最後の電源投入操作が失敗しました。 起動時にスタック：マシンの電源を入れた後、起動に失敗しました。 未登録。マシンが予想期間内に登録できなかったか、登録が拒否されました。 最大容量：マシンは最大容量時に報告します。	シングルセッションとマルチセッション

セッションの詳細

セッションの詳細カテゴリの列。

列	説明	適用先
起動経由	現在のブローカーセッションの起動に使用される StoreFront サーバーのホスト名。マルチセッションマシンの場合は常に null。	シングルセッションとマルチセッション
起動経由（IP アドレス）	現在のブローカーセッションの起動に使用される StoreFront サーバーの IP アドレス。マルチセッションマシンの場合は常に null。	シングルセッションとマルチセッション
セッション変更時間（UTC）	現在のセッションの状態が最後に変更された時間。	シングルセッションのみ
SmartAccess フィルター	現在のセッションの Smart Access タグ。マルチセッションマシンの場合は常に null。	シングルセッションとマルチセッション

セッション

セッションのカテゴリの列。

列	説明	適用先
セッション状態	現在のセッションの状態。設定可能な値：そのほか、セッション準備中、接続済み、アクティブ、切断済み、再接続中、非仲介セッション、および不明。	シングルセッションのみ
現在のユーザー	現在のセッションのユーザーの名前(「ドメイン\ユーザー」の形式)。	シングルセッションのみ
開始日時（UTC）	現在のセッションの開始時間。	シングルセッションのみ
セッション数	マシン上のセッションの数。	マルチセッションのみ

セッションの操作と列

June 12, 2024

この記事では、参照用にマシンの操作と列を記載します。

操作

セッションで実行できる操作とその説明を表示します。

アクション	説明	次のセッションに適用
ログオフ	ユーザーをセッションからログオフします。	シングルセッション OS マシンまたはマルチセッション OS マシン
メッセージの送信	セッションのユーザーにメッセージを送信します。	シングルセッション OS マシンまたはマルチセッション OS マシン
マシンの表示	セッションのホストマシンを表示します。	シングルセッション OS マシンまたはマルチセッション OS マシン
切断	セッションを切断します。セッションが切断状態になると、セッションおよびアプリケーションは終了しませんが、DaaS とユーザーデバイス間の通信が切断されます。	シングルセッション OS マシンまたはマルチセッション OS マシン
マシンをシャットダウンします	セッションに関連付けられたマシンをシャットダウンします。	シングルセッション OS マシン
マシンを再起動します	セッションに関連付けられたマシンを再起動します。	シングルセッション OS マシン

列

セッション列とその説明を表示します。

列	説明
現在のユーザー	ユーザーの名前。ユーザーのユーザープリンシパル名 (UPN)。
名前	セッションをホストしているマシンの DNS ホスト名。
デリバリーグループ	セッションのホストマシンを含むデリバリーグループの名前。

列	説明
マシンカタログ	セッションのホストマシンを含むマシンカタログの名前。
エージェントのバージョン	セッションをホストしているマシン上にインストールされた Virtual Desktop Agent（VDA）のバージョン。
使用中のアプリケーション	セッションで使用されているアプリケーションの一覧。管理名で識別されます。
自律的仲介	これが仲介なしに直接接続によって確立された HDX セッションであるかどうか。
仲介時間（UTC）	セッションが仲介された時間。
仲介ユーザー名	仲介ユーザーの名前。
クライアント（IP）	セッションに接続されているクライアントの IP アドレス。
クライアント	セッションに接続されているクライアントのホスト名。
プラグインのバージョン	セッションに接続されたクライアントで実行されている Citrix Workspace アプリのバージョン。
接続経由	受信接続のホスト名（通常はゲートウェイ、ルーター、またはクライアント）。
接続経由（IP アドレス）	受信接続の IP アドレス（通常はゲートウェイ、ルーター、またはクライアント）。
割り当ての種類	セッションが共有か専用か。
非表示	セッションをユーザーに対して非表示にして、再接続されないようにするかどうか。
VM	ハイパーバイザーによって使用される、セッションをホストする仮想マシンのフレンドリ名です。マシンの DNS 名や AD 名と必ずしも一致するとは限りません。
ホストサーバー名	セッションの管理対象のマシンをホストするハイパーバイザーの DNS 名。
接続	セッションをホストするマシンに割り当てられたホスト接続の名前。
更新保留中	ホストされているマシンの VM イメージが古く、マシンの次回の再起動時に新しいイメージに更新される予定であるかどうか。
メンテナンスモード	セッションをホストしているマシンがメンテナンスモードであるかどうか。
IP アドレス	セッションをホストしているマシンの IP アドレス。

列	説明
物理的	セッションをホストしているマシンが物理かどうか。`True`はマシンが物理であることを示し、DaaS によって電源管理されていないことを意味します。`False`はそれ以外を示します。
起動経由	セッションの起動に使用される StoreFront サーバーのホスト名。セッションがワークスペース経由で起動された場合は空白です。
起動経由（IP アドレス）	セッションの起動に使用される StoreFront サーバーの IP アドレス。セッションがワークスペース経由で起動された場合は空白です。
OS の種類	セッションをホストしているオペレーティングシステムの ID 文字列。
ユーザー変更の保持	ユーザーの変更がどのように処理されるか、変更が永続的であるかどうかを示します： ローカル上：永続的。ユーザーによる変更はローカルに保存されます。 破棄：非永続的。ユーザーによる変更は破棄されます。
接続の種類	HDX、RDP、コンソールなど、セッションに使用されるプロトコル。注： XenDesktop 5 VDA 上のコンソールセッションの場合、フィールドは空白です。
プロビジョニングの種類	セッションをホストしているマシンがプロビジョニングされた方法： 手動：PVS または MCS を使用してプロビジョニングされていません。 PVS：PVS によるプロビジョニング（物理マシン、ブレード、仮想マシン）。 MCS：MCS によるプロビジョニング（VM のみ）。
SecureICA アクティブ	SecureICA がセッションでアクティブであるかどうか。
セッション状態	セッションの状態。設定可能な値：接続済み、アクティブ、または切断済み。L7 より前の機能レベルのマシン上のセッションでは、セッション準備中、再接続中、非仲介セッション、そのほか、不明など、他の状態が発生する可能性があります。
セッション変更時間	セッションが最新の状態に変更された時間。
アプリケーションの状態	セッション内のアプリケーションの状態。設定可能な値：ログオン前、事前起動、アクティブ、デスクトップ、残留、および NoApps。
セッションサポート	セッションをホストしているマシンが複数のセッションをサポートするか、単一のセッションをサポートするか。

列	説明
ゾーン	セッションをホストしているマシンが配置されているゾーンの名前。
SmartAccess フィルター	セッションの Smart Access タグ。
開始日時（UTC）	セッションが開始された日時。
状態	マシンの状態の概要。設定可能な値：未登録、切断済み、または使用中。
この状態での経過時間（UTC）	セッションが現在の状態になってからの時間。
Delivery Controller	セッションのホストマシンが登録しているコントローラーの DNS ホスト名。
ユーザー表示名	ユーザーのフルネーム。
デスクトップの表示名	セッションの起動に最初に使用されたマシンの公開名。これは、Citrix Workspace アプリまたは StoreFront に表示される名前です。アプリケーションセッションの場合、アプリケーションがその後終了した場合でも、セッション内で最初に起動されたアプリケーションの名前になります。後でリソースの名前が変更または削除されても、名前は変更されません。

セキュリティキーの管理

April 10, 2023

> 注:
>
> - この機能は、StoreFront 1912 LTSR CU2 以降とともに使用する必要があります。
> - Secure XML 機能は、Citrix ADC および Citrix Gateway リリース 12.1 以降でのみサポートされます。

この機能を使用すると、承認された StoreFront マシンおよび Citrix Gateway マシンのみが Citrix Delivery Controller と通信できるようになります。この機能を有効にすると、キーが含まれていないすべての要求がブロックされます。この機能を使用して、内部ネットワークの攻撃から保護するセキュリティ層を追加します。

この機能を使用するための一般的なワークフローは次のとおりです:

1. [完全な構成] インターフェイスでセキュリティキー設定を表示します。(Remote PowerShell SDK を使用)
2. 展開の設定を構成します。([完全な構成] インターフェイスまたは Remote PowerShell SDK を使用します)。

3. StoreFront で設定を構成します（PowerShell を使用します）。
4. Citrix ADC で設定を構成します。

[完全な構成] インターフェイスでのセキュリティキー設定の表示

デフォルトでは、セキュリティキーの設定は［完全な構成］インターフェイスで非表示になっています。それらをインターフェイスに表示するには、Remote PowerShell SDK を使用します。Remote PowerShell SDK について詳しくは、「SDK および API」を参照してください。

詳細な手順は次のとおりです:

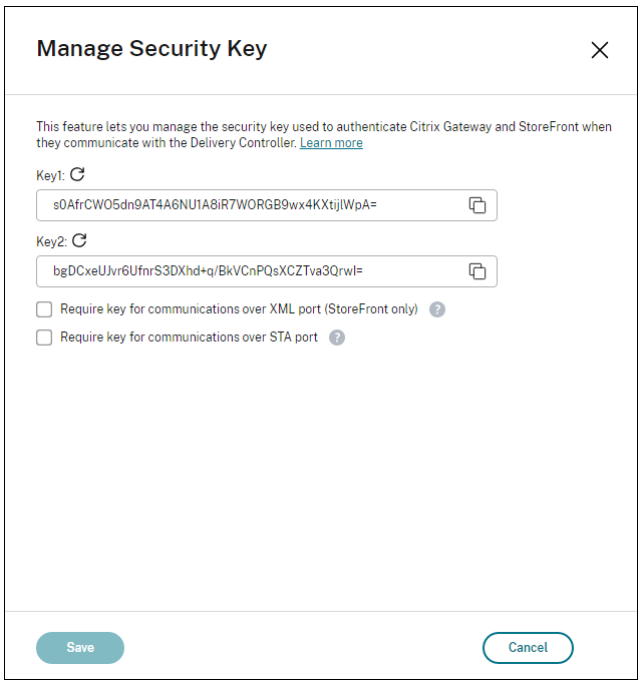
1. Remote PowerShell SDK を実行します。
2. コマンドウィンドウで、次のコマンドを実行します:
   - `Add-PSSnapIn Citrix*`。このコマンドは、Citrix スナップインを追加します。
   - `Set-ConfigSiteMetadata -Name "Citrix_DesktopStudio_SecurityKeyManageme "-Value "True"`

展開の設定を構成する

［完全な構成］または PowerShell を使用して、展開の設定を構成できます。

完全な構成インターフェイスの使用

この機能を有効にした後、［完全な構成］**>**［設定］**>**［セキュリティキーの管理］に移動し、［編集］をクリックします。［セキュリティキーの管理］ブレードが開きます。［保存］をクリックして変更を適用し、ブレードを終了します。



> 重要:
>
> - 2 つのキーを使用できます。XML ポートと STA ポートを介した通信に、同じキーまたは異なるキーを使用できます。一度に 1 つのキーのみを使用することをお勧めします。未使用のキーは、キーの交換にのみ使用されます。
> - 既に使用中のキーを更新するために［更新］アイコンをクリックしないでください。クリックした場合、サービスが中断されます。

更新アイコンをクリックしてキーを生成します。

XML ポート経由の通信にキーが必須とする（**StoreFront** のみ）。選択されている場合、XML ポート経由での通信を認証するためにキーを必要とするかを示します。StoreFront は、このポートを介して Citrix Cloud と通信します。XML ポートの変更について詳しくは、Knowledge Center のCTX127945を参照してください。

STA ポート経由の通信にキーが必須とする。選択されている場合、STA ポート経由での通信を認証するためにキーを必要とするかを示します。Citrix Gateway および StoreFront は、このポートを介して Citrix Cloud と通信します。STA ポートの変更について詳しくは、Knowledge Center のCTX101988を参照してください。

変更を適用後、［閉じる］をクリックして ［セキュリティキーの管理］ブレードを終了します。

Remote PowerShell SDK を使用する

以下は、［完全な構成］インターフェイスでの操作と同じ PowerShell での手順です。

1. Remote PowerShell SDK を実行します。
2. コマンドウィンドウで、次のコマンドを実行します:

- `Add-PSSnapIn Citrix*`

3. 次のコマンドを実行してキーを生成し、Key1 を設定します:

   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey1 <the key you generated>`

4. 次のコマンドを実行してキーを生成し、Key2 を設定します:

   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey2 <the key you generated>`

5. 次のコマンドのいずれかまたは両方を実行して、通信の認証でキーを使用できるようにします:

   - XML ポート経由での通信を認証するには、次を実行します:
     - `Set-BrokerSite -RequireXmlServiceKeyForNFuse $true`
   - STA ポート経由での通信を認証するには、次を実行します:
     - `Set-BrokerSite -RequireXmlServiceKeyForSta $true`

ガイダンスと構文について詳しくは、PowerShell コマンドのヘルプを参照してください。

StoreFront での設定の構成

展開の設定が完了したら、PowerShell を使って StoreFront で関連する設定を構成する必要があります。

StoreFront サーバーで、次の PowerShell コマンドを実行します:

- XML ポート経由での通信のキーを構成するには、`Get-STFStoreServie`および `Set-STFStoreService`コマンドを使用します。例:
  - `PS C:\> Set-STFStoreFarm $farm -Farmtype XenDesktop -Port 80 -TransportType HTTP -Servers <domain name1, domain name2> -XMLValidationEnabled $true -XMLValidationSecret <the key you generated in Studio>`
- STA ポート経由での通信のキーを設定するには、`New-STFSecureTicketAuthority`コマンドを使用します。例:
  - `PS C:\> $sta = New-STFSecureTicketAuthority -StaUrl <STA URL> -StaValidationEnabled $true -StavalidationSecret <the key you generated in Studio>`

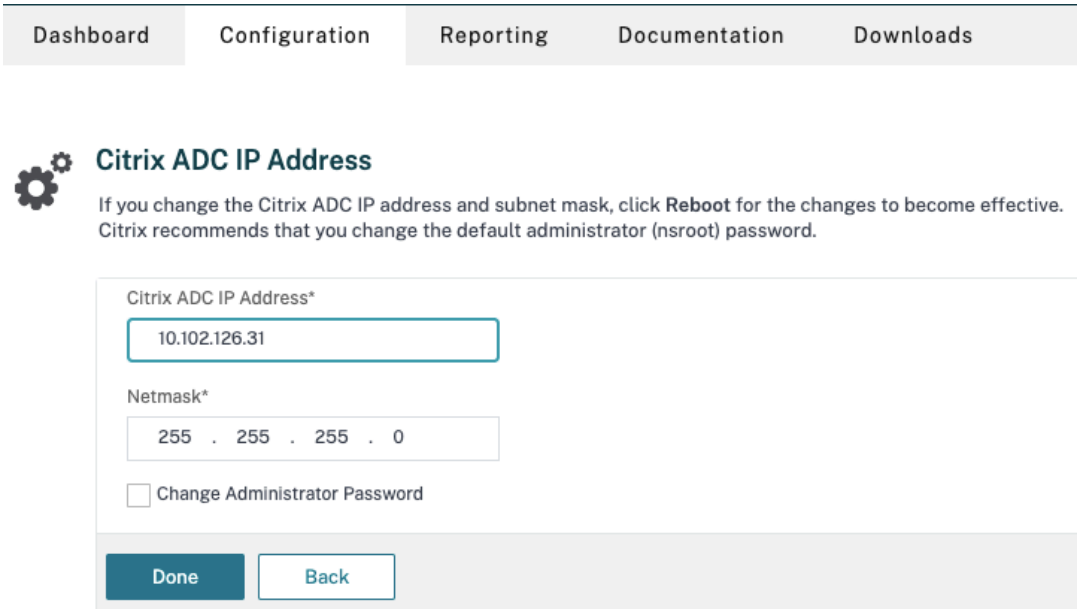
ガイダンスと構文について詳しくは、PowerShell コマンドのヘルプを参照してください。

Citrix ADC での設定の構成

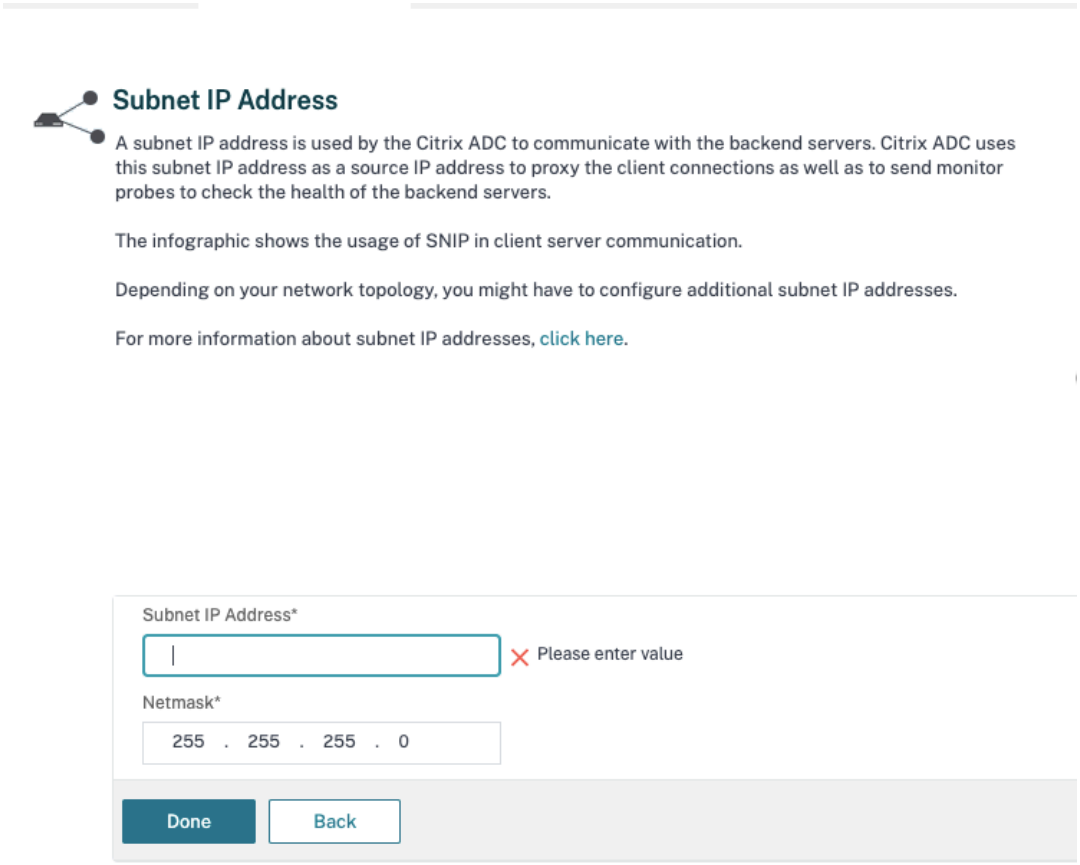
> 注:
>
> ゲートウェイとして Citrix ADC を使用しない限り、Citrix ADC でこの機能を構成する必要はありません。Citrix ADC を使用する場合は、以下の手順に従ってください。

1. 以下の前提条件の構成が既に設定されていることを確認してください:

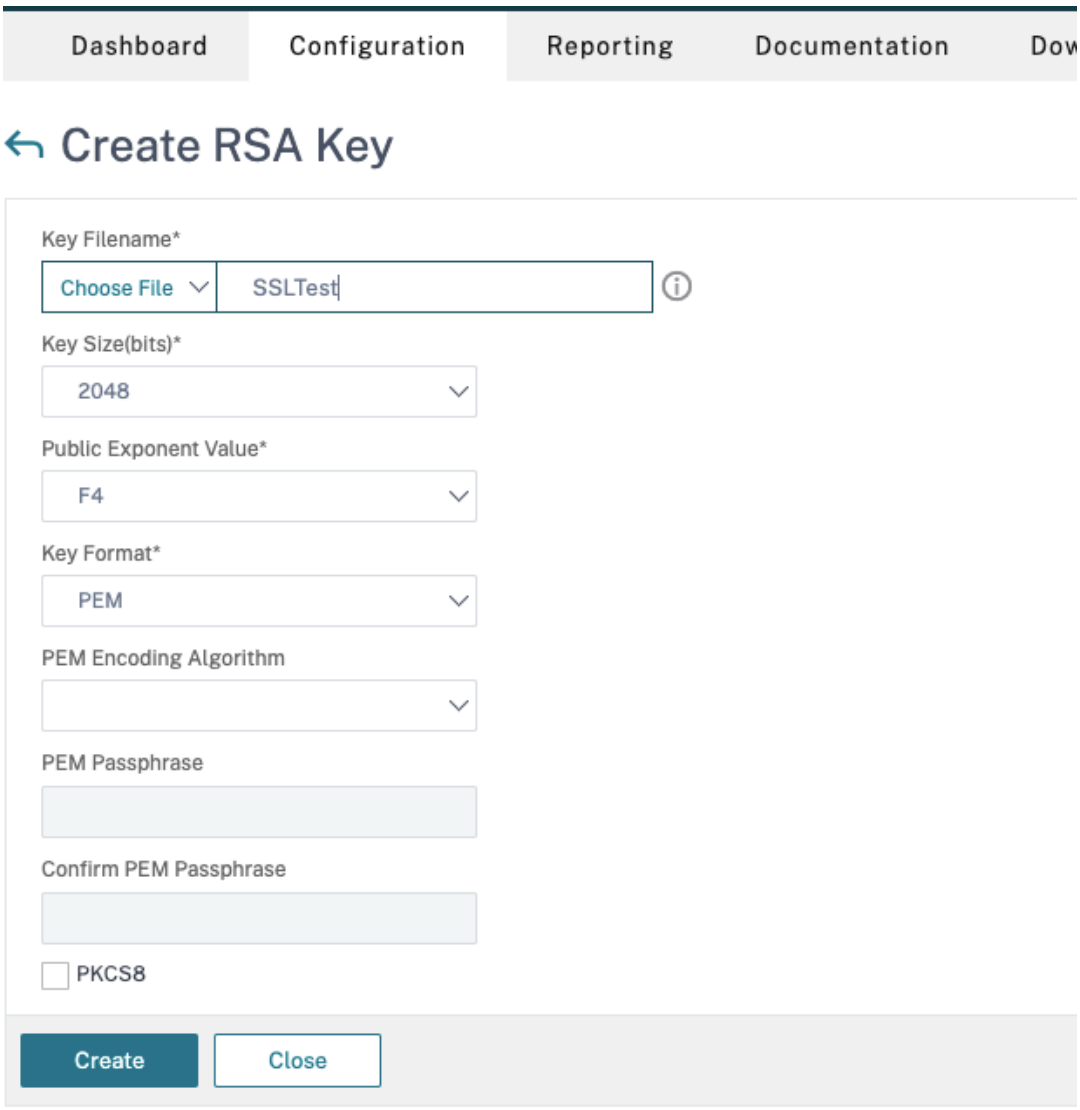
   - 以下の Citrix ADC 関連の IP アドレスが構成されている。
     - Citrix ADC コンソールにアクセスするための Citrix ADC 管理 IP（NSIP）アドレス。詳しくは、「NSIP アドレスの構成」を参照してください。



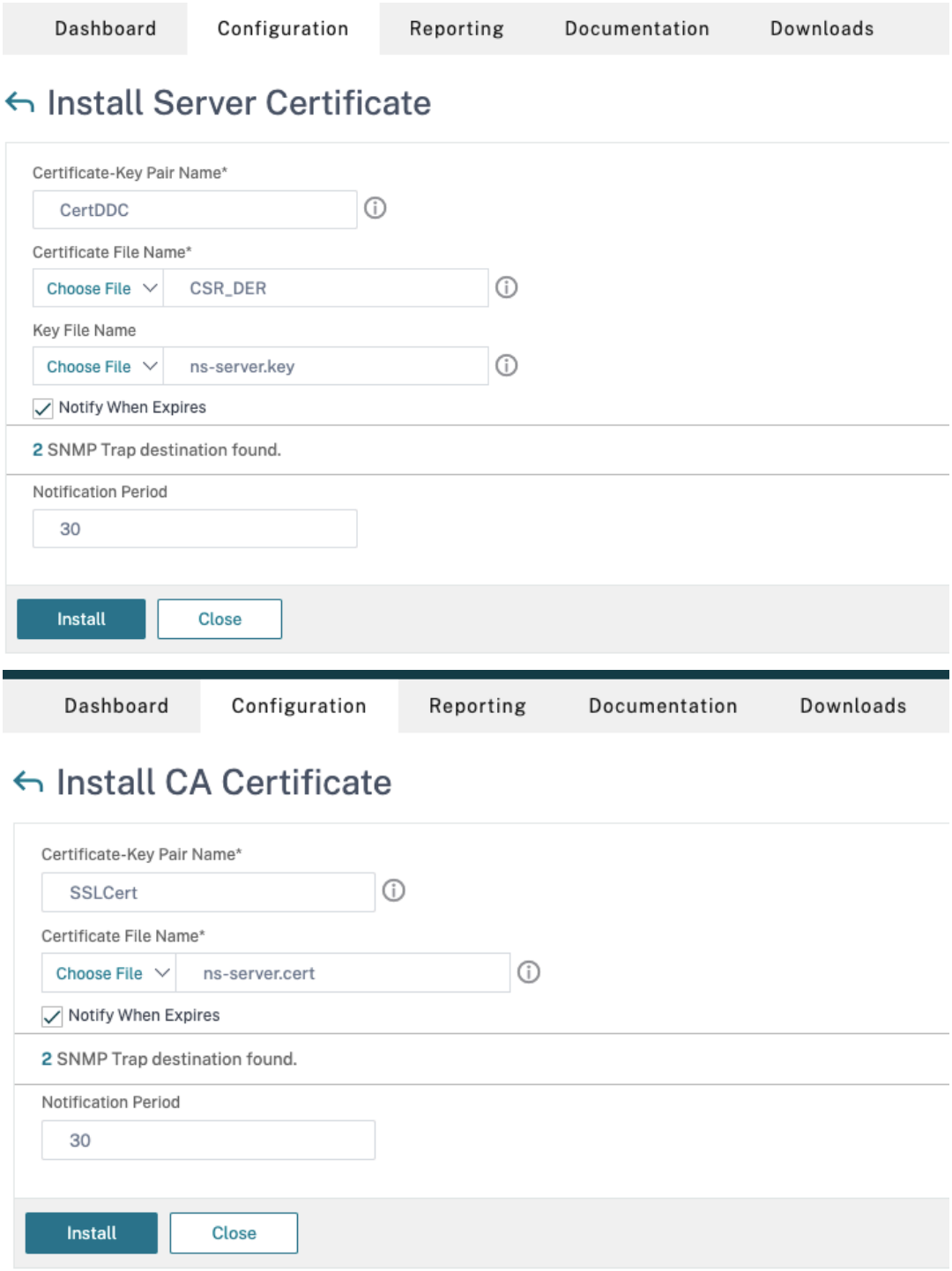
     - Citrix ADC アプライアンスとバックエンドサーバー間の通信を有効にするためのサブネット IP（SNIP）アドレス。詳しくは、「サブネット IP アドレスの構成」を参照してください。
     - ADC アプライアンスにログインしてセッションを起動するための Citrix Gateway 仮想 IP アドレスとロードバランサー仮想 IP アドレス。詳しくは、「仮想サーバーの作成」を参照してください。



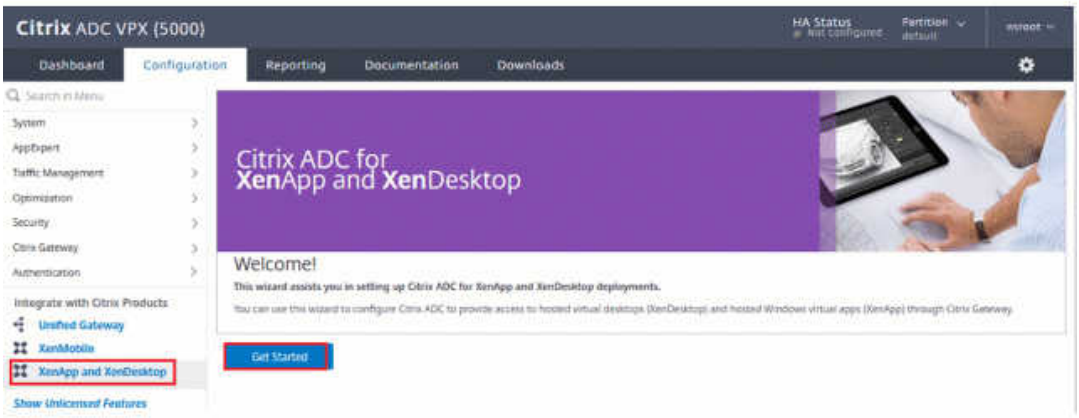
- Citrix ADC アプライアンスで必要なモードと機能が有効である。
  - モードを有効にするには、Citrix ADC GUI で［**System**］>［**Settings**］>［**Configure Mode**］の順に移動します。
  - 機能を有効にするには、Citrix ADC GUI で ［**System**］>［**Settings**］>［**Configure Basic Features**］の順に移動します。
- 証明書関連の構成が完了している。
  - 証明書署名要求（CSR：Certificate Signing Request）が作成されていること。詳しくは、「証明書の作成」を参照してください。



- サーバー証明書と CA 証明書およびルート証明書がインストールされていること。詳しくは、「インストール、リンク、および更新」を参照してください。

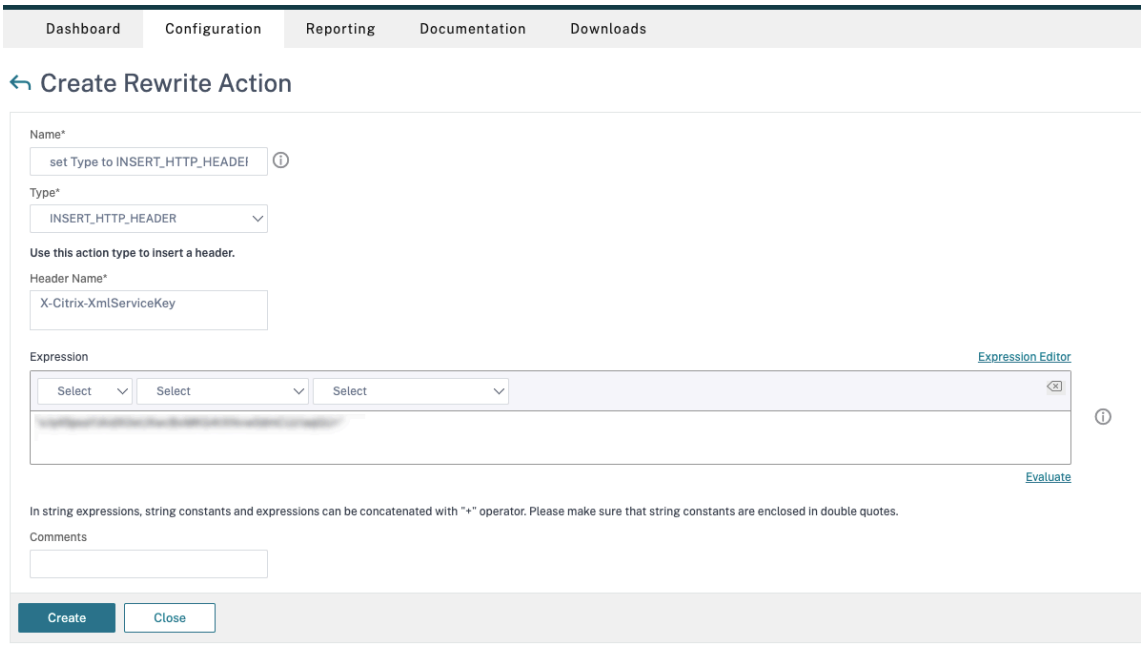


- Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）用の Citrix Gateway が作成されました。[**Test STA Connectivity**] ボタンをクリックして接続をテストし、仮想サーバーがオンラインであることを確認します。詳しくは、「Citrix Virtual Apps and Desktops 用の Citrix ADC のセットアップ」を参照してください。

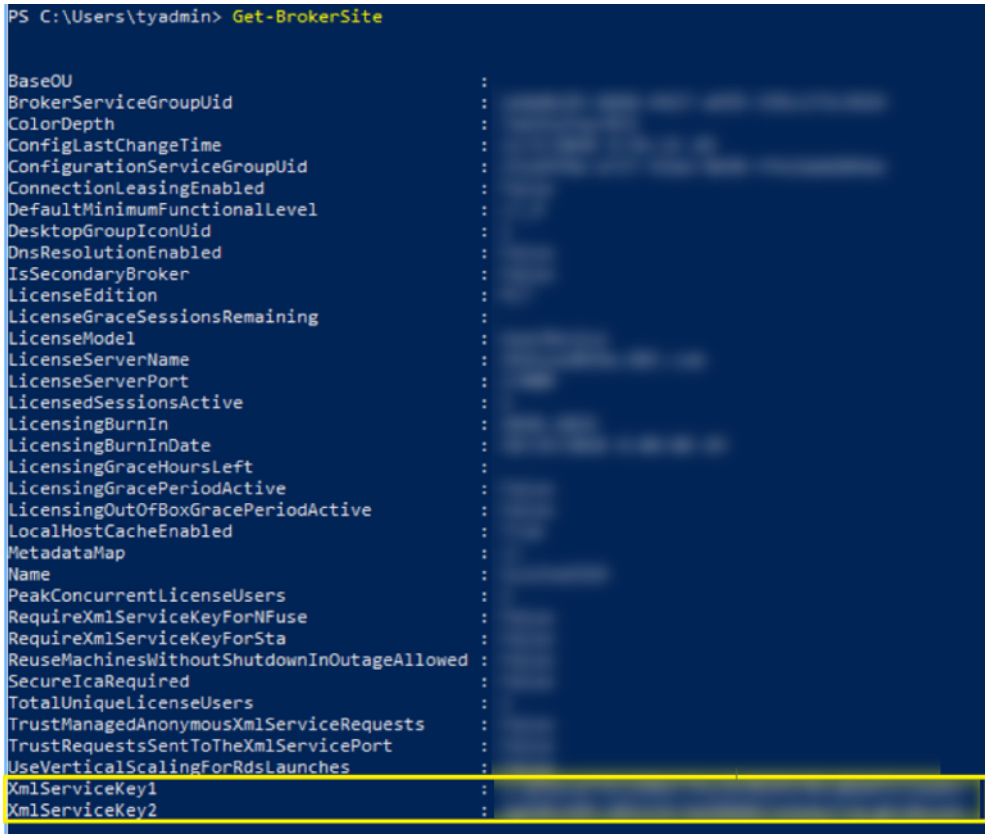


2. 書き換えアクションを追加します。詳しくは、「書き換えアクションの構成」を参照してください。

   a) [**AppExpert**] > [**Rewrite**] > [**Actions**] の順に移動します。
   b) [**Add**] をクリックして、新しい書き換えアクションを追加します。アクションに「set Type to INSERT_HTTP_HEADER」という名前を付けることができます。



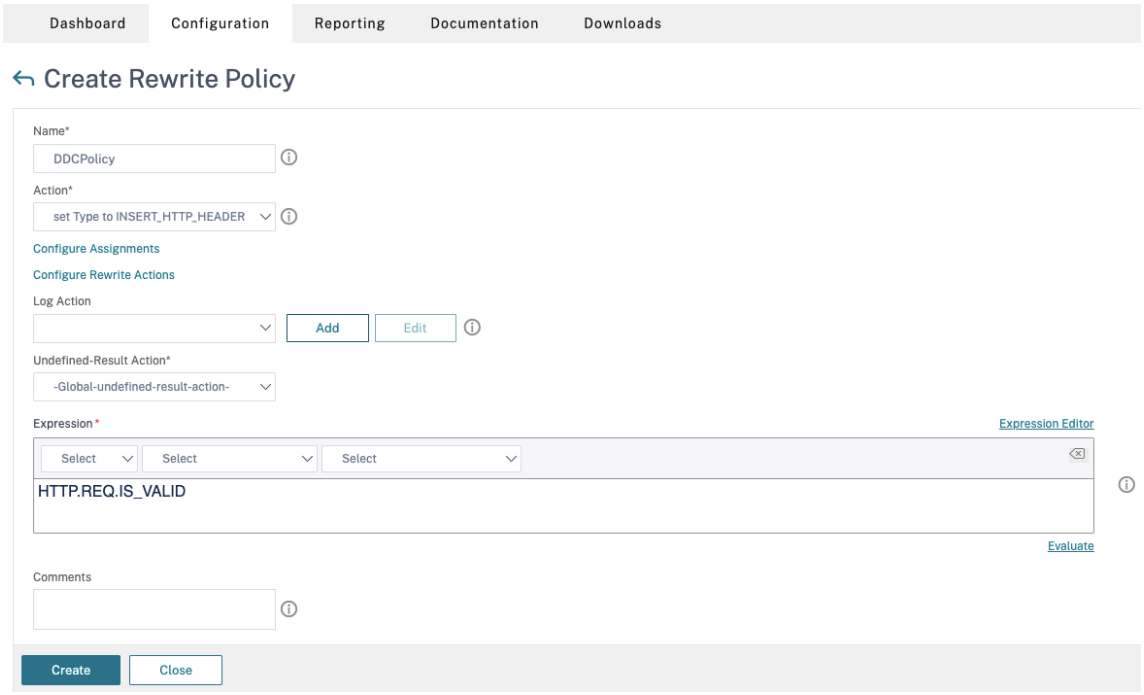
   a) [**Type**] で、[**INSERT_HTTP_HEADER**] を選択します。
   b) [**Header Name**] に「X-Citrix-XmlServiceKey」と入力します。
   c) [**Expression**]に、引用符付きで「<XmlServiceKey1 value>」を追加します。XmlServiceKey1 の値は、Desktop Delivery Controller の構成からコピーできます。



3. 書き換えポリシーを追加します。詳しくは、「書き換えポリシーの構成」を参照してください。

   a) [**AppExpert**] > [**Rewrite**] > [**Policies**] の順に移動します。

   b) [**Add**] をクリックして、新しいポリシーを追加します。



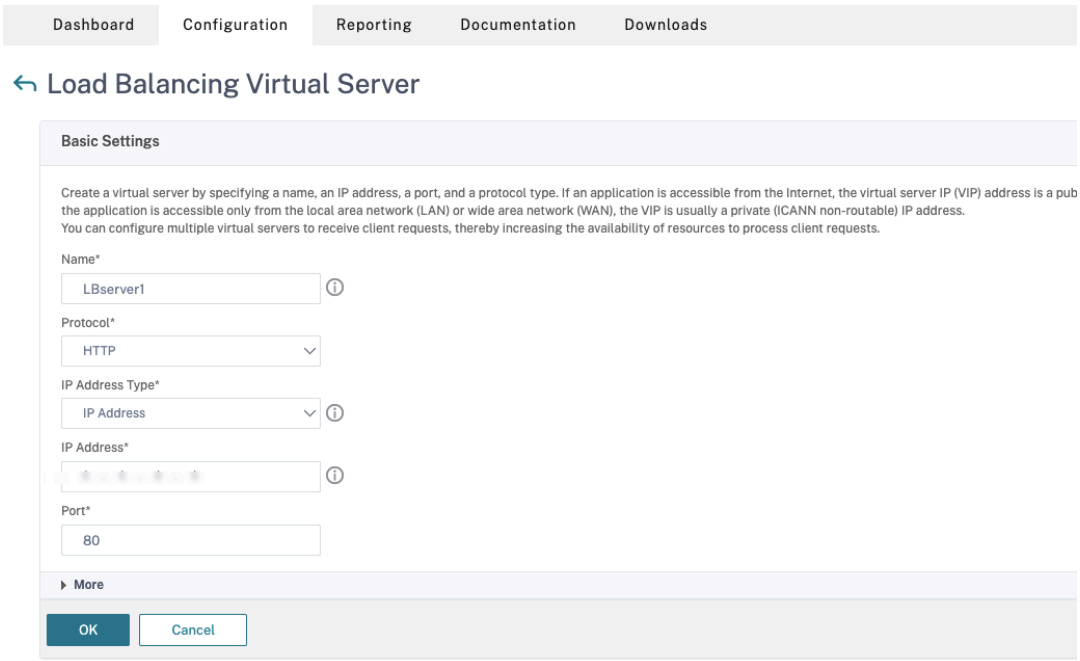
a) [**Action**] で、前の手順で作成したアクションを選択します。
b) [**Expression**] に、「HTTP.REQ.IS_VALID」を追加します。
c) [**OK**] をクリックします。

4. 負荷分散を設定します。STA サーバーごとに 1 つの負荷分散仮想サーバーを構成する必要があります。そうしない場合、セッションの起動が失敗します。

   詳しくは、「基本的な負荷分散の設定」を参照してください。

   a) 負荷分散仮想サーバーを作成します。

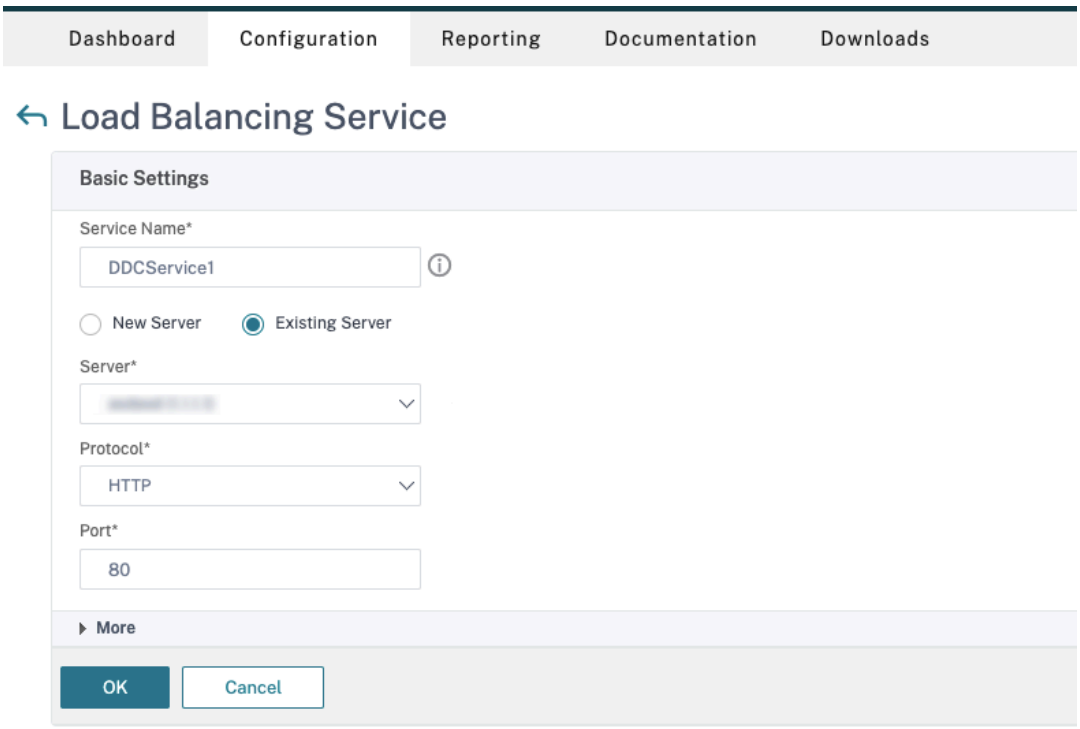
   - [**Traffic Management**] > [**Load Balancing**] > [**Servers**] の順に移動します。
   - [**Virtual Servers**] ページで [**Add**] をクリックします。



   - [**Protocol**] で、[**HTTP**] を選択します。
   - 負荷分散仮想 IP アドレスを追加し、[**Port**] で [**80**] を選択します。
   - [**OK**] をクリックします。

   b) 負荷分散サービスを作成します。

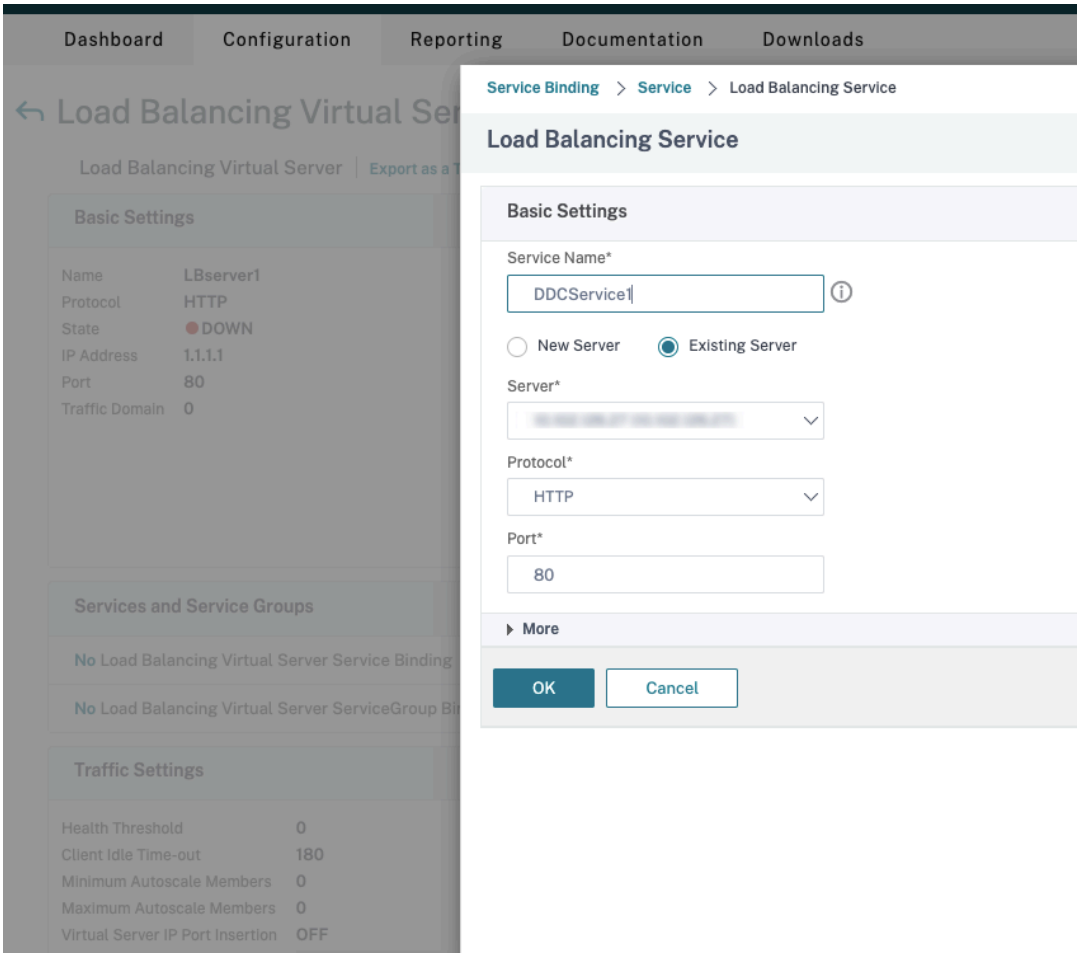
   - [**Traffic Management**] > [**Load Balancing**] > [**Services**] の順に移動します。



- [**Existing Server**] で、前の手順で作成した仮想サーバーを選択します。
- [**Protocol**] で [**HTTP**] を選択し、[**Port**] で [**80**] を選択します。
- [**OK**] をクリックし、[**Done**] をクリックします。

c) サービスを仮想サーバーにバインドします。

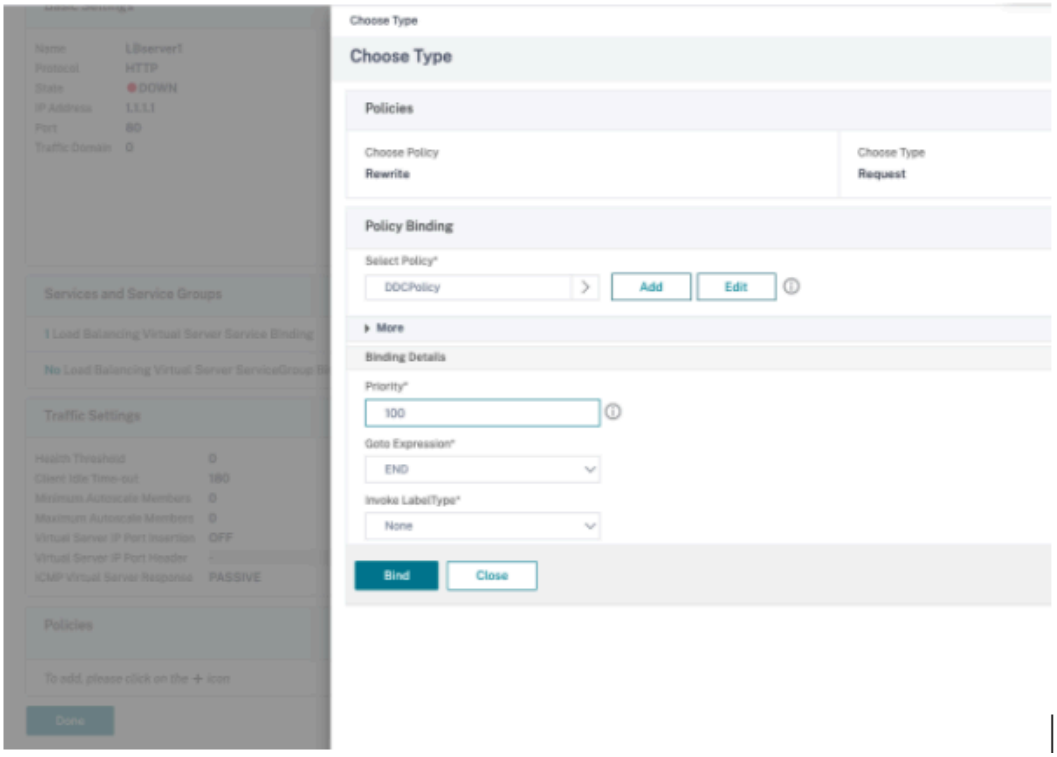
- 以前に作成した仮想サーバーを選択し、[**Edit**] をクリックします。
- [**Services and Service Groups**] の [**No Load Balancing Virtual Server Service Binding**] をクリックします。



- [**Service Binding**] で、前に作成した Citrix DaaS を選択します。
- [**Bind**] をクリックします。

d) 以前に作成した書き換えポリシーを仮想サーバーにバインドします。

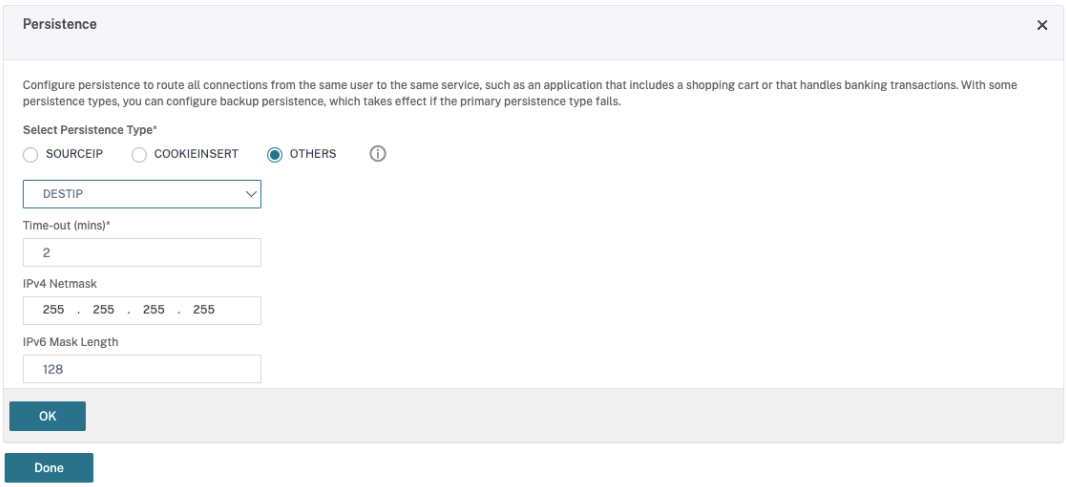
- 以前に作成した仮想サーバーを選択し、[**Edit**] をクリックします。
- [**Advanced Settings**] で [**Policies**] をクリックし、[**Policies**] セクションで [**+**] をクリックします。



- [**Choose Policy**] で [**Rewrite**] を選択し、[**Choose Type**] で [**Request**] を選択します。
- [続行] をクリックします。
- [**Select Policy**] で、前に作成した書き換えポリシーを選択します。
- [**Bind**] をクリックします。
- [完了] をクリックします。

e) 必要に応じて、仮想サーバーの永続性を設定します。

- 以前に作成した仮想サーバーを選択し、[**Edit**] をクリックします。
- [**Advanced Settings**] で、[**Persistence**] をクリックします。



- 永続性タイプを [**Others**] にします。

- 仮想サーバーによって選択されたサービスの IP アドレス（宛先 IP アドレス）に基づいて、永続セッションを作成するには、[**DESTIP**] を選択します。
- [**IPv4 Netmask**] で、DDC と同じネットワークマスクを追加します。
- [**OK**] をクリックします。

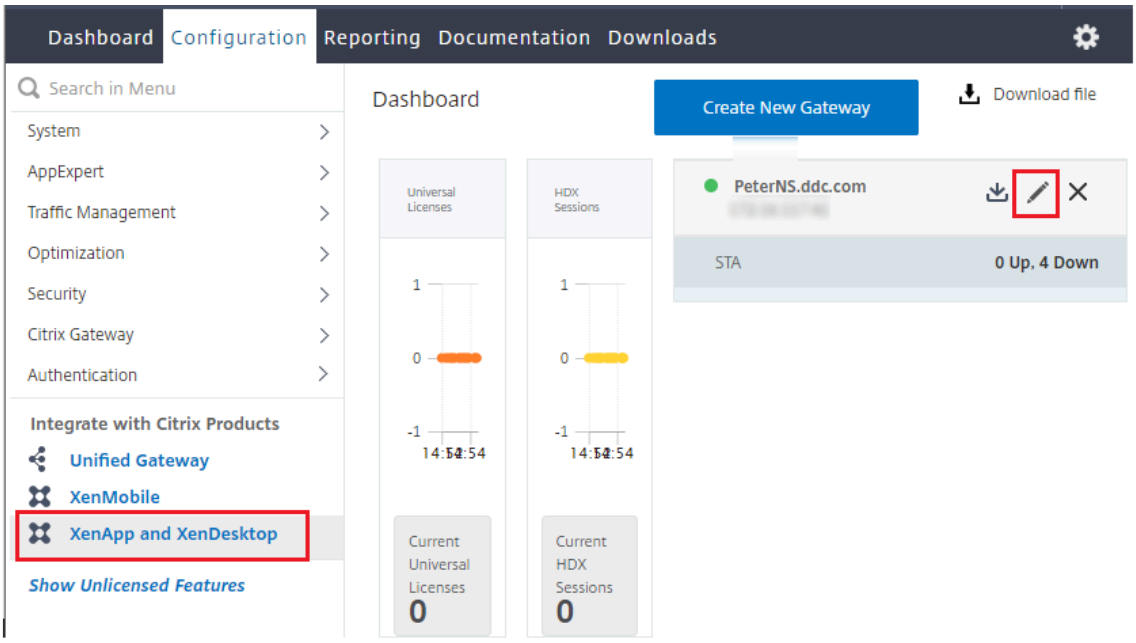
f) 他の仮想サーバーについても、これらの手順を繰り返します。

Citrix ADC アプライアンスが既に **Citrix DaaS** により構成されている場合の構成の変更

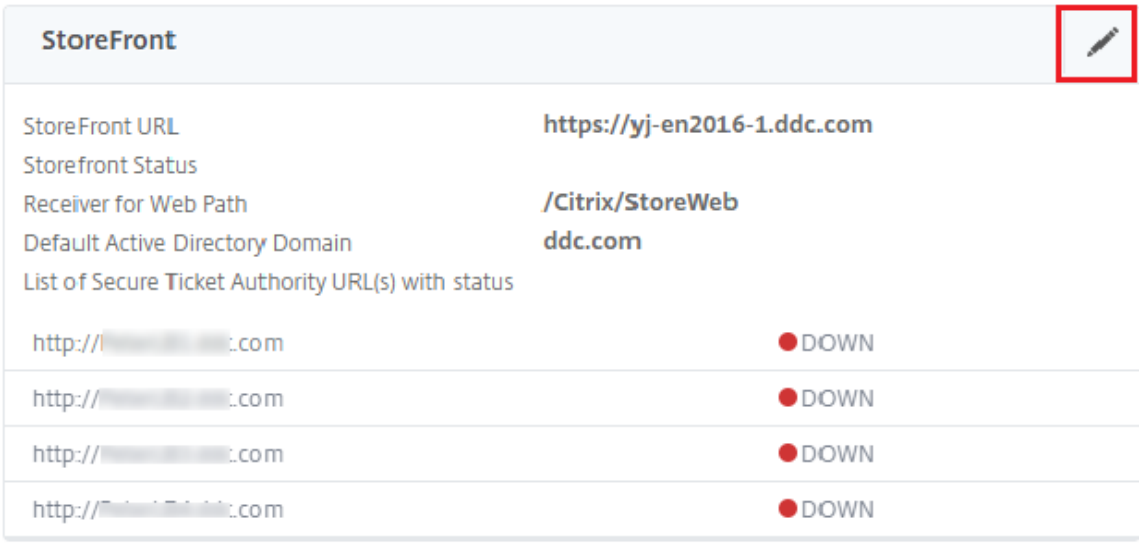
Citrix DaaS を使用して Citrix ADC アプライアンスを既に構成している場合、Secure XML 機能を使用するには、次の構成変更を行う必要があります。

- セッションを起動する前に、ゲートウェイの **Security Ticket Authority URL** を変更して、負荷分散仮想サーバーの FQDN（完全修飾ドメイン名）を使用します。
- `TrustRequestsSentToTheXmlServicePort`パラメーターが False に設定されていることを確認してください。デフォルトでは、`TrustRequestsSentToTheXmlServicePort`パラメーターは False に設定されています。ただし、顧客が Citrix DaaS 用に Citrix ADC を既に構成している場合は、`TrustRequestsSentToTheXmlServicePort`が True に設定されています。

1. Citrix ADC GUI で、[**Configuration**] > [**Integrate with Citrix Products**] の順に移動し、[**XenApp and XenDesktop**] をクリックします。
2. ゲートウェイインスタンスを選択し、編集アイコンをクリックします。

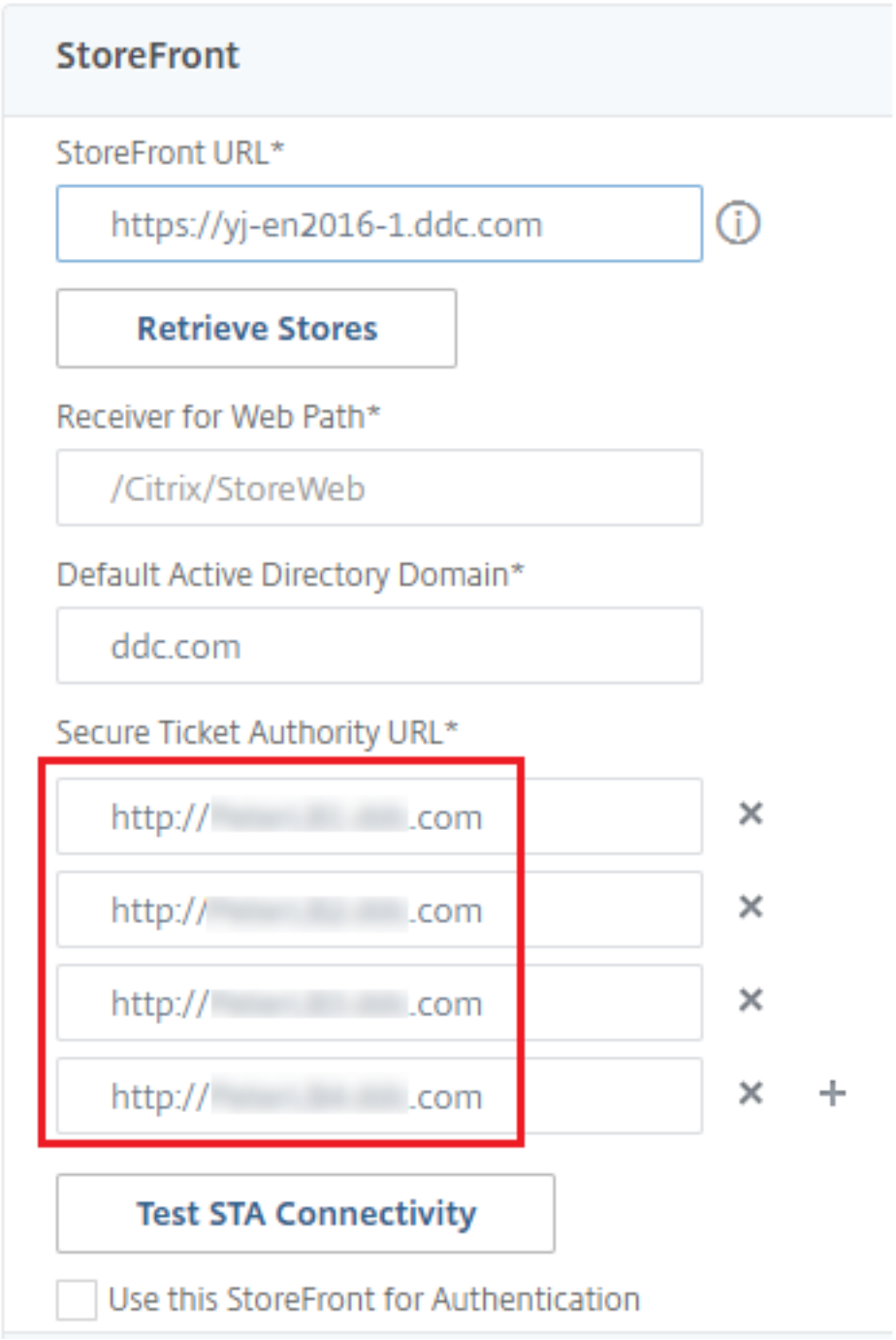


3. StoreFront ペインで、編集アイコンをクリックします。



4. [**Secure Ticket Authority URL**] を追加します。

   - Secure XML 機能が有効になっている場合、STA URL は負荷分散サービスの URL である必要があります。
   - Secure XML 機能が無効になっている場合、STA URL は STA の URL（DDC のアドレス）である必要があり、DDC の TrustRequestsSentToTheXmlServicePort パラメーターは True に設定されている必要があります。



セッションの復元性設定

March 31, 2024

最高のユーザーエクスペリエンスを提供するためには、日々のセッションアクティビティを保守することが重要です。

ネットワークの信頼性が低い、通信速度が一定していない、ワイヤレスデバイスの伝送距離が制限されているなどの理由でネットワーク接続が失われると、ユーザーの労働意欲が損なわれます。ワークステーション間をすばやく移動でき、ログオンするたびに同じアプリケーションのセットにアクセスできることは、病院の医療スタッフなど多くのモバイルワーカーにとっての優先事項です。

この記事で説明する機能では、セッションの信頼性が最適化され、利便性が向上し、ダウンタイムの増加や生産性の低下を防ぐことができます。また、モバイルユーザーがデバイス間をすばやく移動できるようになります。

セッション画面の保持

セッション画面の保持機能は、ICA セッションをアクティブのまま保持し、ネットワークの接続が切断されても、セッションの画面を表示したままにできます。ユーザーは、接続が回復するまでセッション画面を見ることができます。

この機能は、ワイヤレス接続を使用するモバイルユーザーにとって特に有用です。たとえば、ワイヤレス接続でのセッション中にトンネルや障害物などの影響で接続に障害が生じた場合、通常はセッションが切断され、セッションの画面が表示されなくなります。この場合、切断セッションに再接続されるまで、そのセッションでは何もできません。セッション画面の保持機能を有効にすると、データを損失することなくセッションがアクティブのまま保持されます。ネットワークが中断されると、セッション画面が停止し、カーソルの形が砂時計に変わるため、ユーザーにもネットワークが切断されていることがわかります。このとき、セッションウィンドウが閉じたりエラーメッセージが表示されたりする代わりに画面表示が保持され、バックグラウンドで再接続が試行されます。ネットワーク接続が回復すると、自動的にセッションでの作業を再開できるようになります。また、セッションに再接続するときに再認証用のログオン画面が表示されないため、ユーザーは即座に作業を再開できます。

Citrix Workspace アプリのユーザーは、Controller 側の設定を上書きできません。

セッション画面の保持機能と共に、TLS（Transport Layer Security）を使用できます。TLS は、ユーザーデバイスと Citrix Gateway 間で送信されるデータのみを暗号化します。

セッション画面の保持機能は、以下のポリシー設定で構成します。

- ［セッション画面の保持］ポリシー設定により、セッション画面の保持を許可または禁止します。
- ［セッション画面の保持のタイムアウト］ポリシー設定には、デフォルトで 180 秒（3 分）が設定されています。この時間を長く設定することもできますが、この機能の本来の目的は、ネットワークから切断されたユーザーを再認証することなくセッションに再接続することにあるので注意が必要です。必要以上に長い時間を設定すると、接続の再開を待ちきれないユーザーが席を離れてしまい、その間に不正なユーザーがセッションにアクセスしてしまう危険性があります。
- セッション画面の保持機能が有効な受信接続ではポート 2598 が使用されます。このポート番号はポリシーの［セッション画面の保持のポート番号］設定で変更できます。
- 切断したセッションに再接続するユーザーを再認証する場合は、クライアントの自動再接続機能を使用します。［クライアントの自動再接続時の認証］ポリシー設定を構成して、中断されたセッションにユーザーが再接続するときに再認証を要求することができます。

セッション画面の保持機能とクライアントの自動再接続機能を一緒に使用する場合は、次のように処理されます。まず、ネットワークが切断されると、セッション画面の保持機能により、セッションがアクティブのままサーバー上に

保持されます。［セッション画面の保持のタイムアウト］設定で指定した時間が経過すると、サーバー上のセッションが終了または切断されます。この後で［クライアントの自動再接続］の各ポリシー設定が有効になり、切断セッションへの再接続が行われます。

クライアントの自動再接続

クライアント自動再接続機能では、ネットワークの問題などによって切断されたセッションを Citrix Workspace アプリが検出して、そのセッションに自動的に再接続します。この機能がサーバーで有効になっていると、ユーザーは作業を続けるために手動で再接続する必要がありません。

アプリケーションセッションでは、Citrix Workspace アプリは、接続に成功するかユーザーがキャンセルするまで再接続を繰り返し試行します。

デスクトップセッションでは、Citrix Workspace アプリは、指定された時間の間に、再接続に成功するかユーザーが再接続キャンセルするまで再接続を繰り返し試みます。デフォルトでは、この時間は 5 分です。この時間を変更するには、ユーザーデバイスで以下のレジストリを編集します:

```
HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds; DWORD;<seconds>
```

`seconds`には、セッションの再接続の試行をやめるまでの時間を秒数で指定します。

クライアント自動再接続機能は、以下のポリシー設定で構成します。

- クライアントの自動再接続：接続が中断した場合の Citrix Workspace アプリによる自動再接続を有効または無効にします。
- クライアントの自動再接続時の認証：自動再接続時にユーザーの認証を要求するかどうかを指定します。
- クライアントの自動再接続のログ：再接続イベントのイベントログへの記録を有効または無効にします。ログ機能は、デフォルトで無効になっています。この機能を有効にすると、サーバーのシステムログに自動再接続の成功および失敗イベントが記録されます。各サーバーは自身のシステムログに、再接続イベントに関する情報を記録します。サイトは、すべてのサーバーの再接続イベントを記録した統合ログを提供しません。

クライアントの自動再接続機能には、暗号化されたユーザー資格情報に基づく再認証メカニズムが使用されています。ユーザーが最初にログオンしたときに、サーバーにより暗号化されたユーザー資格情報がメモリに格納され、その暗号キーを含んだ Cookie が Citrix Workspace アプリに送信されます。Citrix Workspace アプリは、再接続時にこのキーをサーバーへ送信します。サーバーは復号化した資格情報を Windows のログオンプロセスに送信して認証を求めます。Cookie の有効期限が切れた場合、ユーザーは資格情報を再入力する必要があります。

［クライアントの自動再接続時の認証］設定を有効にした場合、Cookie は使用されません。その代わりに、Citrix Workspace アプリの切断セッションへの自動再接続時に、ユーザーの資格情報を入力するためのダイアログボックスが開きます。

ユーザーの資格情報とセッションのセキュリティを最大限に保護するために、クライアントとサイトの間のすべての通信で暗号化機能を使用してください。

Windows 向け Citrix Workspace アプリで自動再接続機能を無効にするには、icaclient.adm ファイルを編集します。詳しくは、該当するバージョンの Windows 向け Citrix Workspace アプリのドキュメントを参照してください。

接続の設定も、クライアントの自動再接続機能に影響します。

- 前述のように、クライアントの自動再接続はポリシー設定のデフォルトによりサイト全体で有効になっています。ユーザーの再認証も不要です。ただし、サーバーで ICA TCP 接続が切断されたときにセッションをリセットするように設定すると、自動再接続は実行されません。クライアントの自動再接続は、エラーの発生またはタイムアウトによりサーバーがセッションを切断した場合にのみ実行されます。ここでの ICA TCP 接続とは、実際のネットワーク接続ではなく、TCP/IP ネットワーク上のセッションで使用されるサーバーの仮想ポートを指します。
- サーバー上の ICA TCP 接続では、デフォルトでエラーやタイムアウトが発生した接続のセッションを切断するように設定されています。切断されたセッションはそのままシステムメモリに残るので、ユーザーは同じサーバーに自動的に再接続して、そのセッションでの作業を続行できます。
- エラーが生じたりタイムアウトしたりした接続のセッションについてはリセット、つまりログオフされるように構成できます。セッションがリセットされた場合、再接続しようとすると、新しいセッションが開始されます。切断前の作業状態からセッションが復元されるのではなく、アプリケーションが再起動されます。
- セッションがリセットされるようにサーバーが構成されている場合、クライアントの自動再接続によりセッションが作成されます。この場合、ユーザーが自分の資格情報を入力して、サーバーにログオンし直す必要があります。
- 外部からの侵入などによって Citrix Workspace アプリまたはプラグインから正しくない認証情報が提供された場合、またはセッションの切断が検出されてから自動再接続までの時間が長すぎた場合は、自動再接続に失敗することがあります。

ICA Keep-Alive

ICA Keep-Alive 機能を有効にすると、ネットワークの問題により切断されたセッションにユーザーが再接続できなくなることを防ぐことができます。この機能が有効な場合、セッションのアイドル状態（たとえばクロックデータの更新、マウス操作、画面更新などがない状態）が検出されたときに、リモートデスクトップサービスによりセッションが切断されることを防ぐことができます。サーバーは、定期的に Keep-Alive パケットを送信して、セッションがアクティブかどうかを検出します。セッションがアクティブでないことが検出されると、サーバーにより「切断」状態として認識されます。

> 重要:
>
> ICA Keep-Alive は、セッション画面の保持機能を使用しない環境でのみ正しく動作します。セッション画面の保持機能では、ICA Keep-Alive とは異なるメカニズムで切断セッションが管理されます。セッション画面の保持機能を使用しない環境でのみ、ICA Keep-Alive を有効にしてください。

ここでの Keep-Alive 機能の設定は、Windows のグループポリシーによる同様の設定よりも優先されます。

ICA Keep-Alive 機能は、以下のポリシー設定で構成します。

- **ICA Keep-Alive** タイムアウト： ICA Keep-Alive メッセージの送信間隔を 1〜3600 秒の範囲で指定します。ただし、ネットワークの問題によるセッションの切断が少なく、アイドル状態のセッションをネットワーク監視ソフトウェアで自動的に閉じるように設定している環境では、このオプションを構成しないでください。

  デフォルト値は 60 秒で、サーバーからユーザーデバイスに ICA Keep-Alive パケットが 60 秒おきに送信されます。クライアントが 60 秒以内に応答しない場合、そのセッションは「切断」状態（タイムアウト）と認識されます。

- **ICA Keep-Alive**： ICA Keep-Alive メッセージを送信するかどうかを指定します。

ワークスペースコントロール

ワークスペースコントロール機能を有効にすると、ユーザーがセッションの途中でデバイスを切り替えても、新しいデバイス上でそのデスクトップやアプリケーションでの作業を継続できます。これにより、ユーザーは自分のデスクトップや作業中のアプリケーションにどこからでもシームレスにアクセスできるようになります。たとえば、病院内の複数のワークステーション間を移動しながら、常に同じアプリケーションセットにアクセスしなければならない医療従事者をサポートするために、この機能を利用できます。ワークスペースコントロールを構成すると、ユーザーは複数のアプリケーションを一度に切断して、その後で別のクライアントデバイスからそれらのアプリケーションに再接続できます。

ワークスペースコントロールを有効にすると、ユーザーの操作は以下のようになります。

- ログオン：デフォルトでは、ユーザーが移動先でログオンすると、実行されていたすべてのデスクトップおよびアプリケーションに自動的に再接続されます。デスクトップやアプリケーションを手作業で起動する必要はありません。ワークスペースコントロールにより、ユーザーは切断されたデスクトップまたはアプリケーションを開くことができ、別のクライアントデバイス上でデスクトップまたはアプリケーションがアクティブな場合でも開くことができます。ユーザーがデスクトップやアプリケーションとの接続を切断しても、サーバー上のセッションは終了しません。管理者は、ユーザーが切断したものだけが再接続されるように構成することもできます。これにより、移動先のクライアントデバイスを使ってユーザーが再ログオンしたときに、前のクライアントデバイスでアクティブなデスクトップやアプリケーションには再接続されず、切断されているものだけが再接続されます。
- 再接続：サーバーに再ログオンしたユーザーは、［再接続］をクリックすることで自分のデスクトップやアプリケーションに一度に再接続できます。デフォルトでは、切断されているデスクトップやアプリケーションと、ほかのクライアントデバイスでアクティブなデスクトップやアプリケーションが再接続されます。管理者は、切断されているデスクトップやアプリケーションだけが再接続されるように構成することもできます。
- ログオフ：ユーザーが StoreFront 経由でデスクトップやアプリケーションにアクセスする場合に、［ログオフ］コマンドにより StoreFront およびすべてのアクティブセッションからログオフするのか、StoreFront だけからログオフするのかを管理者が構成できます。
- 切断：ユーザーは、実行中のすべてのデスクトップやアプリケーションを一度に切断できます。個々に切断する必要はありません。

Citrix StoreFront 接続または Citrix Workspace アプリを介してデスクトップやアプリケーションにアクセスするユーザーは、ワークスペースコントロールを利用できます。デフォルトでは、ワークスペースコントロールは仮想デ

スクトップセッションでは無効になっていますが、ホストされたアプリケーションでは有効になっています。公開デスクトップ上で公開アプリケーションを実行する場合、デフォルトではこれらのセッションは共有されません。

ユーザーが別のクライアントデバイスに移動すると、ポリシー、クライアント側ドライブのマッピング、およびプリンターの設定が適切に変更されます。ポリシーとクライアントドライブマッピングは、ユーザーがセッションにログオンするクライアントデバイスの条件に基づいて適用されます。たとえば、医療従事者が緊急治療室のクライアントデバイスからログオフして、レントゲン室のワークステーションにログオンして自分のワークスペースに再接続した場合は、レントゲン室でのセッションに適したポリシー、プリンターマッピング、およびクライアント側ドライブのマッピング設定がセッションの開始時に有効になります。

管理者は、ユーザーが場所を移動したときに使用可能になるプリンターをカスタマイズできます。また、ローカルプリンターでの印刷の可否やリモート接続時に使用される帯域幅などの印刷環境を制御することもできます。

ワークスペースコントロール機能を有効にして構成する方法については、StoreFront のドキュメントを参照してください。

セッションローミング

> 注:
>
> 次の情報は、PowerShell を使用したセッションローミングの構成について説明されたものです。代わりに、[完全な構成] 管理インターフェイスを使用することもできます。詳しくは、「デリバリーグループの管理」を参照してください。

デフォルトでは、ユーザーのクライアントデバイス間でセッションローミングが行われます。ユーザーがセッションを開始した後に別のデバイスに移動した場合、同じセッションが使用され、両方のデバイスで同時にアプリケーションを使用することができます。複数のデバイスでアプリケーションを表示できます。デバイスや、現在のセッションが存在するかどうかに関係なく、アプリケーションが引き継がれます。たいていの場合、アプリケーションに割り当てられたプリンターやそのほかのリソースも引き継がれます。

このデフォルト動作には多数のメリットがありますが、すべてのケースで理想的であるわけではありません。PowerShell SDK を使用して、セッションローミングを無効にすることができます。

例 1: 医療専門家が、2 つのデバイスを使用しています。デスクトップ PC では保険用紙に入力し、タブレットでは患者情報を確認します。

- セッションローミングが有効な場合、両方のアプリケーションが両方のデバイスに表示されます（どちらかのデバイスで起動されたアプリケーションが、使用しているすべてのデバイスに表示されます)。これが、セキュリティ要件に準拠しない場合があります。
- セッションローミングを無効にすると、患者レコードはデスクトップ PC には表示されず、保険用紙はタブレットには表示されません。

例 2: 生産管理者が、自分のオフィスにある PC でアプリケーションを起動します。デバイスの名前と場所に基づいて、このセッションで使用できるプリンターやそのほかのリソースが決定されます。その日のうちに、生産管理者は隣の建物のオフィスに移動し、プリンターを使用する必要があるミーティングに出席します。

- セッションローミングが有効な場合、生産管理者は会議室の近くにあるプリンターを使用できない可能性があります。ミーティングより前に自分のオフィス内でアプリケーションを起動したため、オフィスの近くにあるプリンターやそのほかのリソースへの割り当てが行われているためです。
- セッションローミングが無効な場合、(同じ資格情報を使用して) 別のマシンにログオンすると、新たなセッションが開始され、近くにあるプリンターやリソースを使用できます。

セッションローミングを構成する

セッションローミングを構成するには、「SessionReconnection」プロパティを含む以下の資格ポリシー規則コマンドレットを使用します。オプションで、「LeasingBehavior」プロパティを指定することもできます。

デスクトップセッションの場合:

```
Set-BrokerEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection
 <value> -LeasingBehavior Allowed|Disallowed
```

アプリケーションセッションの場合:

```
Set-BrokerAppEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection
 <value> -LeasingBehavior Allowed|Disallowed
```

ここでは、`value`には次のいずれかを指定できます:

- **Always**: クライアントデバイスに関係なく、セッションが接続中でも、切断中でも、セッションローミングが常に実行されます。これがデフォルト値です。
- **DisconnectedOnly**: 既に切断されているセッションのみに再接続します。それ以外のセッションについては、新規セッションを開始します (最初に切断するか、ワークスペースコントロールを使用して明示的にローミングすることによって、クライアントデバイス間のセッションローミングを実行することができます)。別のクライアントデバイスからのアクティブな接続済みセッションは、使用されません。代わりに、新規セッションが開始されます。
- **SameEndpointOnly**: ユーザーが使用する各クライアントデバイスに対し、一意のセッションが割り当てられます。ローミングは、完全に無効になります。ユーザーは、セッションで過去に使用されたものと同じデバイスのみに再接続できます。

「LeasingBehavior」プロパティについては、後述の説明を参照してください。

ほかの設定の影響:

セッションローミングの無効化は、デリバリーグループにおけるアプリケーションのプロパティのアプリケーション制限「1 ユーザーあたり 1 インスタンスのみ許可する」の影響を受けます。

- セッションローミングを無効にする場合、このアプリケーション制限も無効にします。
- このアプリケーション制限を有効にする場合、新規デバイスでの新規セッションを許可する 2 つの値は、どちらも設定しないでください。

ログオン間隔

デスクトップ VDA がインストールされている仮想マシンが、ログオンプロセスが完了する前に終了する場合は、プロセスにより多くの時間を割り当てることができます。7.6 以降のバージョンのデフォルトは 180 秒です（7.0〜7.5 は 90 秒です）。

マシン上（またはマシンカタログで使用されるマスターイメージ上）で、以下のレジストリキーを設定します：

キー：`HKLM\SOFTWARE\Citrix\PortICA`

- 値：`AutoLogonTimeout`
- 種類：`DWORD`
- 十進法時間（秒）を 0〜3600 の範囲で指定します。

マスターイメージを変更する場合は、新しいイメージをカタログにロールアウトします。詳しくは、「マスターイメージの変更」を参照してください。

この設定は、シングルセッションデスクトップ（ワークステーション）VDA を搭載した仮想マシンにのみ適用されます。マルチセッションサーバー VDA を搭載したマシンのログオンタイムアウトは、マイクロソフトにより制御されます。

タグ

November 22, 2023

はじめに

タグは、マシン、アプリケーション、デスクトップ、デリバリーグループ、アプリケーショングループ、ポリシーなどのアイテムを識別する文字列です。タグを作成してアイテムに追加すると、以下のように、特定の操作を指定されたタグのあるアイテムのみに適用するように調整できます。

- ［完全な構成］管理インターフェイスの［検索］画面を調整します。

  たとえば、テスターに最適化されているアプリケーションのみを表示するには、「テスト」という名前のタグを作成し、それらのアプリケーションに追加（適用）します。これで、検索結果を「テスト」タグでフィルタリングできます。

- 選択したデリバリーグループ内のマシンのサブセットだけを対象にして、アプリケーショングループまたは特定のデスクトップからアプリケーションを公開する。この機能は、タグによる制限と呼ばれます。

  タグによる制限で、複数の公開タスクに既存のマシンを使用できるので、追加のマシンを展開、管理するコストを節約できます。タグ制限は、デリバリーグループのマシンをさらに分割（またはパーティション化）する

ものと考えることができます。その機能は、7.x より前のリリースの XenApp ワーカーグループに類似していますが、同一ではありません。

タグ制限のあるアプリケーショングループやデスクトップを使用すると、デリバリーグループ内のマシンのサブセットを分離してトラブルシューティングするときに便利です。

タグ制約の使用の詳細と例については、この記事の後半で説明します。

- デリバリーグループ内のマシンのサブセットの定期再起動をスケジューリングする。

  マシンでタグによる制限を使用すると、新しい PowerShell コマンドレットを使用して、デリバリーグループ内のマシンのサブセットに対して複数の再起動スケジュールを構成できます。例と詳細については、「デリバリーグループの管理」を参照してください。

- デリバリーグループ、デリバリーグループの種類、指定されたタグを持つ（または持たない）OU（組織単位）への Citrix ポリシーの適用（割り当て）を調整する。

  たとえば、より強力なワークステーションにのみ Citrix ポリシーを適用するには、それらのマシンに「ハイパワー」という名前のタグを追加します。その後、ポリシーの作成ウィザードの ［ポリシーの割り当て］ページでこのタグを選択し、［有効化］チェックボックスをオンにします。デリバリーグループにタグを追加し、そのデリバリーグループに Citrix ポリシーを適用することもできます。詳しくは、「ポリシーの作成」を参照してください。

タグは次のものに適用できます：

- マシン
- アプリケーション
- マシンカタログ
- デリバリーグループ
- アプリケーショングループ

［完全な構成］管理インターフェイスで次のものを作成または編集するとき、タグ制約を構成できます：

- 共有デリバリーグループのデスクトップ
- アプリケーショングループ

デスクトップまたはアプリケーショングループのタグによる制限

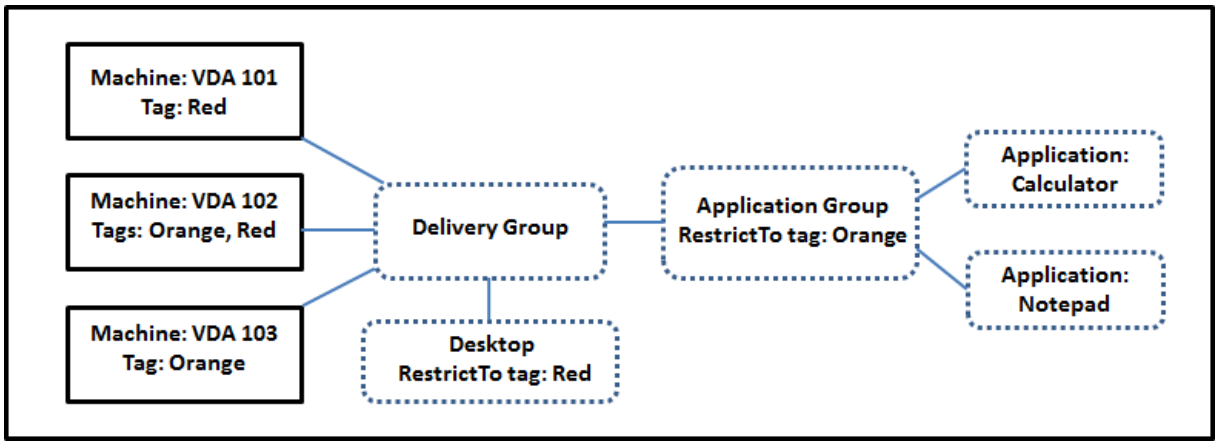
タグによる制限には、いくつかの手順があります：

- タグを作成し、マシンに追加（適用）します。
- タグ制約を持つグループを作成または編集します（言い換えると、タグ *x* を持つマシンに起動を制約します）。

タグによる制限は、コントローラーのマシン選択プロセスを拡張します。コントローラーは、関連するデリバリーグループから、アクセスポリシー、構成されたユーザーの一覧、ゾーン優先度、起動対応度、およびタグ制約（存在する場合）に従うマシンを選択します。アプリケーションの場合、コントローラーは優先度順に他のデリバリーグループにフォールバックし、関係する各デリバリーグループに同じマシン選択規則を適用します。

例 **1**：単純なレイアウト

この例では、あるデスクトップおよびアプリケーションの起動に関係するマシンを、タグを使用して制限する、単純なレイアウトを紹介します。1 つの共有デリバリーグループ、1 つの公開デスクトップ、および 2 つのアプリケーションで構成された 1 つのアプリケーショングループがあります。



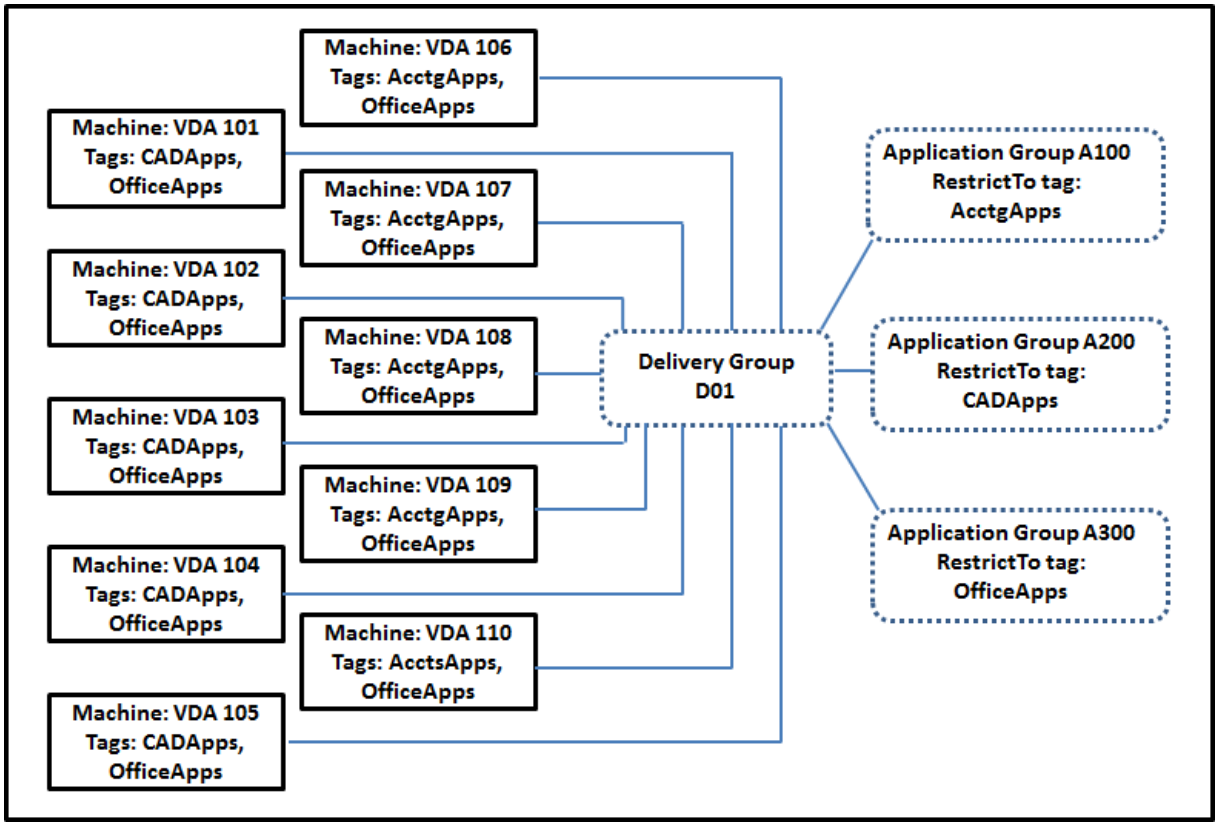
- 3 台のマシン（VDA 101～103）それぞれにタグが追加されています。
- デリバリーグループのデスクトップは、「Red」という名前のタグ制約付きで作成されました。そのため、このデスクトップは、「Red」タグが付いたそのデリバリーグループ内のマシン（VDA 101 および 102）でのみ起動できます。
- アプリケーショングループは、「Orange」タグ制約付きで作成されました。そのため、各アプリケーション（CalculatorおよびNotepad）は、「Orange」タグが付いたそのデリバリーグループ内のマシン（VDA 102 および 103）でのみ起動できます。

マシン VDA 102 は両方のタグ（RedおよびOrange）を持っているため、アプリケーションとデスクトップの起動に関与できます。

例 **2**：複雑なレイアウト

この例には、タグによる制限を使用して作成された複数のアプリケーショングループが含まれます。これにより、デリバリーグループのみを使用する場合に必要な数より少ないマシンでより多くのアプリケーションを提供できます

タグを作成、適用し、この例のタグによる制限を構成するための手順については、「例 2 を構成する方法」に示しています。



この例では、10 台のマシン（VDA 101～110）、1 つのデリバリーグループ（D01）、および 3 つのアプリケーショングループ（A100、A200、A300）を使用します。各アプリケーショングループの作成時に、各マシンにタグを適用し、タグによる制限を指定することにより、以下のことが可能です：

- グループ内の会計ユーザーは、5 台のマシン（VDA 101～105）上で、必要なアプリにアクセスできます。
- グループ内の CAD デザイナーは、5 台のマシン（VDA 106～110）上で、必要なアプリにアクセスできます。
- Office アプリケーションを必要とするグループのユーザーは、10 台のマシン（VDA 101～110）上で、Office アプリにアクセスできます。

使用されるマシンは 10 台のみで、デリバリーグループは 1 つだけです。1 台のマシンは 1 つのデリバリーグループにのみ属することができるので、デリバリーグループのみを使用する場合は（アプリケーショングループ不使用時）、2 倍のマシンが必要になります。

タグとタグによる制限の管理

タグの作成、追加（適用）、編集、適用済みのアイテムからの削除は、［完全な構成］管理インターフェイスの ［タグの管理］操作を使用して行います。

（例外：ポリシー割り当てに使用するタグは、［タグの管理］操作を使用して作成、編集、削除します。ただし、ポリシーの作成時にタグを適用し（割り当て）ます。詳しくは、「ポリシーの作成」を参照してください）。

タグによる制限は、デリバリーグループでデスクトップを作成または編集するとき、およびアプリケーショングループを作成および編集するときに構成されます。

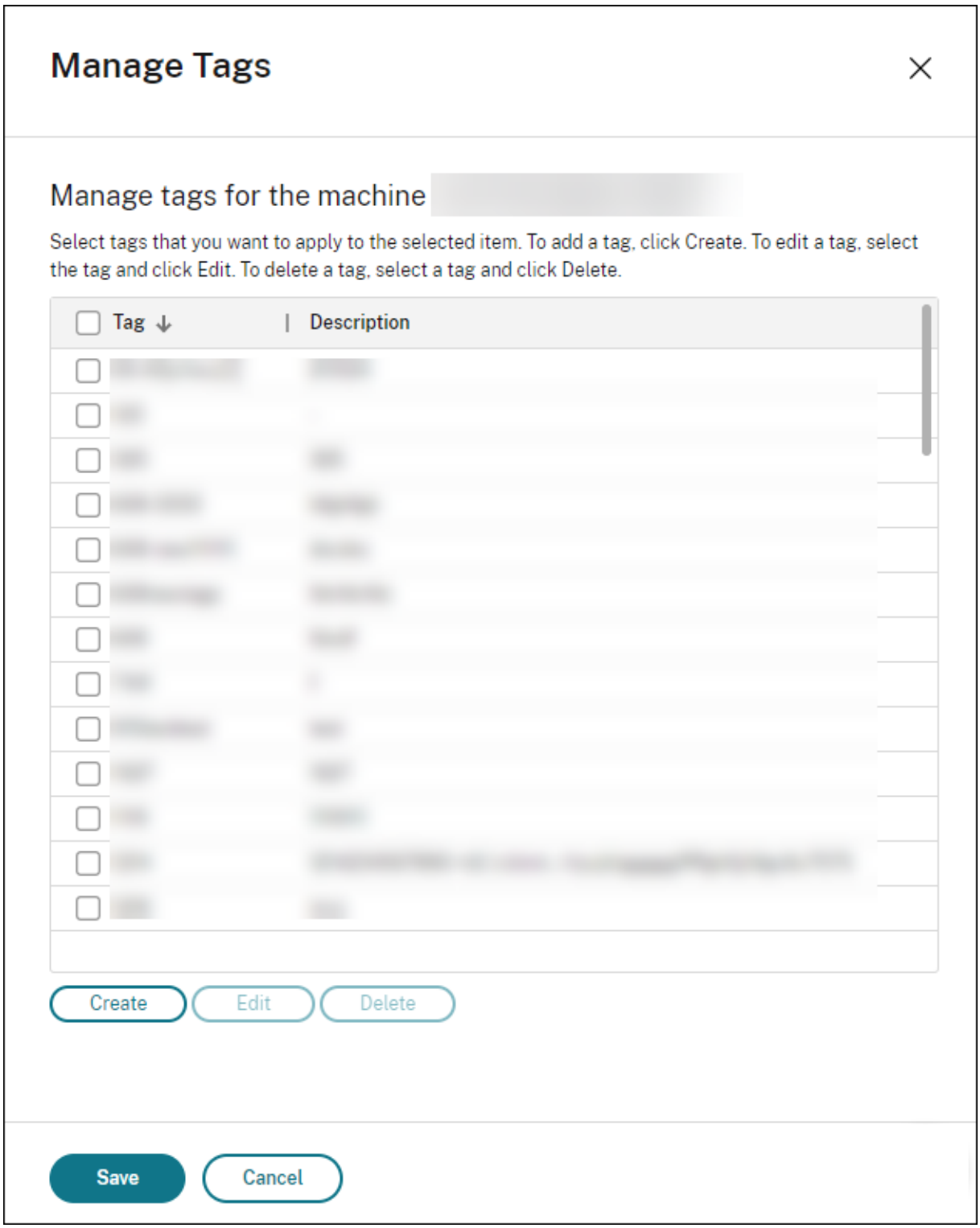
［タグの管理］機能の使用

［管理］**>**［完全な構成］で、タグを適用するアイテムを選択します。アイテムは次のとおりです：

- 1 つまたは複数のマシン
- 1 つまたは複数のアプリケーション
- デスクトップ、デリバリーグループ、またはアプリケーショングループ
- マシンカタログ

次に、操作バーの ［タグの管理］を選択します。［タグの管理］ダイアログボックスに、選択したアイテムのタグだけでなく、すべての既存のタグが表示されます。

- オンになっているチェックボックスは、選択したアイテムにタグが既に追加されていることを表します。（下の画面キャプチャで、選択されたマシンには「Tag1」という名前のタグが適用されています）。
- 複数の項目を選択する場合、ハイフンを含むチェックボックスは、一部の項目（すべての項目ではない）にそのタグが追加されていることを表します。



［タグの管理］ダイアログボックスでは、以下の操作を実行できます。「タグを使用する場合の注意事項」を確認してください。

- タグを作成するには:

［作成］を選択します。名前と説明を入力します。タグの名前は一意でなければならず、大文字と小文字は区別されません。次に ［保存］を選択します。

タグを作成しても、選択しているアイテムに自動的に適用されることはありません。チェックボックスを使用してタグを適用します。

- **1** つまたは複数のタグを追加（適用）するには：

  タグ名の隣にあるチェックボックスをオンにします。ハイフンを含むチェックボックスは、一部のアイテム（すべてのアイテムではない）にそのタグが追加されていることを表します。複数のアイテムを選択し、タグのチェックボックスにハイフンが含まれている場合に、ハイフンをチェックマークに変更すると、選択したすべてのマシンに影響します。

  マシンにタグを追加しようとしていて、そのタグがアプリケーショングループの制約として使用されている場合、この操作により、それらのマシンが起動対象になることがあるという警告が表示されます。それが意図どおりであれば続行します。

- **1** つまたは複数のタグを削除するには：

  タグ名の隣にあるチェックボックスをオフにします。ハイフンを含むチェックボックスは、一部のアイテム（すべてのアイテムではない）にそのタグが追加されていることを表します。複数のアイテムを選択し、タグのチェックボックスにハイフンが含まれている場合、チェックボックスをオフにすると、選択したすべてのマシンからタグが削除されます。

  マシンからタグ制約を削除しようとすると、その操作が起動対象のマシンに影響を与える可能性があるという警告が表示されます。それが意図どおりであれば続行します。

- タグを編集するには：

  タグを選択してから、［編集］を選択します。新しい名前、説明、またはその両方を入力します。同時に編集できるタグは 1 つのみです。

- **1** つまたは複数のタグを削除するには：

  タグを選択してから、［削除］を選択します。［タグの削除］ダイアログボックスに、選択したタグを現在使用しているアイテムの数が表示されます（「2 台のマシン」など）。アイテムを選択すると、詳細情報（たとえば、タグが適用されている 2 台のマシンの名前）が表示されます。タグを削除するかどうかを確認します。

  制約として使用されているタグを削除することはできません。最初にアプリケーショングループを編集してから、タグによる制限を削除するか、異なるタグを選択します。

［タグの管理］ダイアログボックスでの操作が完了したら、［保存］を選択します。

マシンにタグが適用されているかを確認するには、左側ペインで ［デリバリーグループ］を選択します。デリバリーグループを選択して、操作バーの ［マシンの表示］を選択します。マシンを選択し、［詳細］ペインで ［タグ］タブを選択します。

タグによる制限の管理

タグによる制限の構成は複数の手順があるプロセスです。まずタグを作成し、それをマシンに追加/適用します。次に、アプリケーショングループまたはデスクトップに制限を追加します。

- タグの作成と適用:

  上記の ［タグの管理］操作により、タグを作成してマシンに追加（適用）します。タグを追加したマシンには、タグ制約の影響が生じます。

- アプリケーショングループにタグによる制限を追加するには:

  アプリケーショングループを作成または編集します。［デリバリーグループ］ページで、［タグでマシンの起動を制限します］をオンにし、一覧からタグを選択します。

- アプリケーショングループのタグによる制限を変更または削除するには:

  グループを編集します。［デリバリーグループ］ページで、異なるタグを一覧から選択するか、［タグでマシンの起動を制限します］をオフにしてタグによる制限を完全に削除します。

- デスクトップにタグによる制限を追加するには:

  デリバリーグループを作成または編集します。［デスクトップ］ページで ［追加］または ［編集］を選択します。［デスクトップの追加］ダイアログボックスで、［タグでマシンの起動を制限します］をオンにし、ドロップダウンからタグを選択します。

- デリバリーグループのタグによる制限を変更または削除するには:

  グループを編集します。［デスクトップ］ページで、［編集］を選択します。ダイアログボックスで、異なるタグを一覧から選択するか、［タグでマシンの起動を制限します:］をオフにしてタグ制約を完全に削除します。

タグを使用する場合の注意事項

アイテムに適用されたタグは、さまざまな目的に使用できます。タグの追加や削除が意図しない結果になる可能性があることに注意してください。［完全な構成］管理インターフェイスの検索を使用する場合、タグを使用してマシンの表示を並べ替えできます。アプリケーショングループまたはデスクトップを構成するときに、制限として同じタグを使用できます。この操作により、タグが付いている指定されたデリバリーグループのマシンだけに起動対象が制限されます。

タグがデスクトップまたはアプリケーショングループのタグ制約として構成されている場合にマシンにタグを追加しようとすると、それらのマシンでその他のアプリケーションやデスクトップの起動が可能になることがあるという警告が表示されます。それが意図どおりであれば続行します。そうでない場合は、操作を取り消します。

たとえば、「Red」というタグ制約を持つアプリケーショングループを作成するとします。後から、そのアプリケーショングループによって使用される同じデリバリーグループに、他のマシンをいくつか追加します。それらのマシンに「Red」というタグを追加しようとすると、おおむね次のようなメッセージが表示されます:「タグ「Red」は、次のアプリケーショングループ上の制約として使用されています。このタグを追加すると、選択されたマシンからこのア

プリケーショングループのアプリケーションが起動可能になる可能性があります。」次に、それらの追加マシンへのそのタグの追加を確認またはキャンセルできます。

同様に、アプリケーショングループで起動を制限するためにタグが使用されている場合、グループを編集してタグ制約を削除するまで、このタグを削除できないという警告が表示されます（このタグの削除を許可されている場合、アプリケーショングループに関連付けられたデリバリーグループ内のすべてのマシンでアプリケーションの起動を許可することになる可能性があります）。デスクトップ起動の制約としてタグが使用されている場合も、タグの削除は同様に不可能です。アプリケーショングループまたはデリバリーグループ内のデスクトップを編集してタグによる制限を削除すれば、タグを削除できます。

すべてのマシンが同一セットのアプリケーションを持つとは限りません。1 人のユーザーが、それぞれ異なるタグによる制限を持ち、デリバリーグループのマシン構成が異なるか重なり合っている複数のアプリケーショングループに属する場合があります。次の表に、対象マシンがどのように決まるかを示します。

アプリケーションの追加先	選択したデリバリーグループ内で起動対象となるマシン
タグによる制限を持たない 1 つのアプリケーショングループ	すべてのマシン。
タグによる制限 A を持つ 1 つのアプリケーショングループ	タグ A が適用されているマシン。
2 つのアプリケーショングループ。タグによる制限 A を持つグループとタグによる制限 B を持つグループ	タグ A とタグ B を持っているマシン。存在しない場合、タグ A またはタグ B を持っているマシン。
2 つのアプリケーショングループ。タグによる制限 A を持つグループとタグによる制限を持たないグループ	タグ A を持つマシン。存在しない場合、すべてのマシン。

マシン再起動スケジュールでタグによる制限を使用している場合、タグ適用またはタグによる制限に影響する変更はすべて、次回のマシン再起動サイクルに影響を与えます。変更の実行中に進行している再起動サイクルには影響しません

例 **2** を構成する方法

次の手順は、タグを作成、適用し、前述の 2 番目の例で示したアプリケーショングループのためにタグ制約を構成する方法を示しています。

VDA とアプリケーションはマシンに既にインストール済み、デリバリーグループは作成済みです。

マシンにタグを作成し、適用します:

1. ［管理］**>**［完全な構成］の左側ペインで ［デリバリーグループ］を選択します。デリバリーグループD01を選択して、操作バーの ［マシンの表示］を選択します。
2. マシン VDA 101～105 を選択して、操作バーで ［タグの管理］を選択します。
3. ［タグの管理］ダイアログボックスで ［作成］を選択します。「CADApps」という名前のタグを作成します。［**OK**］を選択します。

4. ［作成］を再度選択して、OfficeAppsという名前のタグを作成します。［**OK**］を選択します。
5. ［タグの管理］ダイアログボックスで、各タグ名（CADAppsおよびOfficeApps）の隣にあるチェックボックスをオンにして、新しく作成したタグを選択したマシンに追加（適用）します。次に、ダイアログボックスを閉じます。
6. デリバリーグループD01を選択します。操作バーの ［マシンの表示］を選択します。
7. マシン VDA 106～110 を選択して、操作バーで ［タグの管理］を選択します。
8. ［タグの管理］ダイアログボックスで ［作成］を選択します。「AcctgApps」という名前のタグを作成します。［**OK**］を選択します。
9. 各タグ名の隣にあるチェックボックスをオンにして、選択したマシンに新しく作成したAcctgAppsタグとOfficeAppsタグを適用します。次に、ダイアログボックスを閉じます。

タグによる制限を持つアプリケーショングループを作成します。

1. ［管理］**>**［完全な構成］の左側ペインで ［アプリケーション］を選択します。
2. 操作バーの ［アプリケーショングループの作成］を選択します。ウィザードが起動します。
3. ［デリバリーグループ］ページでデリバリーグループD01を選択します。［タグでマシンの起動を制限します］をオンにし、一覧からAcctgAppsタグを選択します。
4. 会計ユーザーと会計アプリケーションを指定して、ウィザードを完了します（アプリケーションを追加するときに ［[スタート］メニューから］を選択すると、AcctgAppsタグが適用されているマシン上にあるアプリケーションが検索されます）。［概要］ページで、グループにA100という名前を付けます。
5. 前の手順を繰り返してアプリケーショングループA200を作成し、CADAppsタグを持っているマシンと、適切なユーザーおよびアプリケーションを指定します。
6. 手順を繰り返してアプリケーショングループA300を作成し、OfficeAppsタグを持っているマシンと、適切なユーザーおよびアプリケーションを指定します。

マシンカタログへのタグの適用

［管理］**>**［完全な構成］または PowerShell を使用して、マシンカタログにタグを適用できます。

- 管理インターフェイスの使用については、「タグの管理」で説明しています。カタログ表示では、タグが適用されているかどうかは示されません。
- PowerShell の使用については、「PowerShell を使用してタグをカタログに適用する」を参照してください。

カタログでタグを使用する例を次に示します：

- デリバリーグループには複数のカタログのマシンがありますが、操作（再起動スケジュールなど）を特定のカタログ内のマシンのみに適用する必要があります。該当するカタログにタグを適用することで、これが可能になります。

PowerShell を使用してタグをカタログに適用する

次の PowerShell コマンドレットを使用できます：

- `Add-BrokerTag`や`Remove-BrokerTag`などのコマンドレットにカタログオブジェクトを渡すことができます。
- `Get-BrokerTagUsage`で、タグを含むカタログの数が表示されます。
- `Get-BrokerCatalog`には`Tags`というプロパティがあります。

たとえば、次のコマンドレットにより、事前に作成された`fy2018`という名前のタグが`acctg`という名前のカタログに追加されます：`Get-BrokerCatalog -Name acctg | Add-BrokerTag fy2018`。

ガイダンスと構文について詳しくは、PowerShell コマンドレットのヘルプを参照してください。

自動タグ（プレビュー）

自動タグ付けにより、管理者はカスタムルールに基づいて、さまざまな DaaS オブジェクトのタグを自動的に設定したり削除したりできます。この機能拡張により、環境の最適化のために定期的に実行されるさまざまなスクリプトを保持する必要がなくなります。

使用例

自動タグ付けを使用すると、コストの削減、インフラストラクチャの最適化、消費の促進など、ビジネスの推進要因に関連する規則を実装できます。以下にユースケースの一部を示します。

- 未使用の **VDI** を解放する - 使用されていない期間が事前に構成された日数を超えている専用ワークロードを、使用可能なプールにリリースします。
- 余分なアプリを削除する - 使用されていない期間が事前に構成された日数を超えているアプリケーションを特定して、余分なアプリケーションを削減します。
- **X** 未満の機能レベルを持つ **DG** - 特定の機能レベル未満のデリバリーグループを見つけます。
- 非アクティブなユーザー - ログオンしていない期間が事前に構成された日数を超えているユーザーのリソースを解放します。

PowerShell コマンド

PowerShell コマンドを使用して自動タグを作成できます。自動タグの規則が作成されると、600 秒の頻度で評価されます。詳しくは、「New-BrokerAutoTagRule」を参照してください。

例　`New-BrokerAutoTagRule`は、`Get-BrokerMachine`コマンドレットと同じオブジェクトタイプとフィルターパラメーターを使用します。詳しくは、「GetBrokerMachine」を参照してください。

1. 30 日以上使用されていない専用 VDI に ID 123 のタグを付けます。

    a) 未使用の VDI にタグ付けするためのタグ（例：**unused-VDI**）を定義します。

    - タグ名：unused-VDI

- タグ ID： 123

b) 未使用のマシンにタグを付ける自動タグ付け規則を作成します。規則のパラメーターを定義します。

- 名前：規則の汎用名。
- オブジェクトの種類：マシン。
- 規則テキスト：静的な割り当て済みのマシンで、最終接続時から 30 日を超えているか、その値がない。
- タグ UID： 関連付けようとするタグ ID、123。

```
New-BrokerAutoTagRule -Name 'UnusedVdi' -ObjectType 'Machine' -RuleText "-AllocationType Static -IsAssigned $true -Filter { SummaryState -ne `"InUse`" -and ( LastConnectionTime -lt '-30' -or LastConnectionTime -eq `$null )} " -TagUid 123
```

c) **unused-VDI** タグが付いているマシンを確認し、リリースします。

2. X 未満の機能レベルでデリバリーグループにタグを付ける場合（**L7_20** をしきい値機能レベルとして使用）：

```
New-BrokerAutoTagRule -Name 'LowFL'-ObjectType 'DesktopGroup'-RuleText "-Filter { MinimumFunctionalLevel -lt 'L7_20' } "-TagUid 123
```

3. フォルダーを使用せずに公開された、ユーザーに表示されるアプリにタグを付ける場合：

```
New-BrokerAutoTagRule -Name 'NoFolder'-ObjectType 'Application'-RuleText "-Enabled $true -Filter { ClientFolder -eq $null )} "-TagUid 123
```

追加情報

ブログ記事：How to Assign Desktops to Specific Servers。

タイムゾーンの設定

March 5, 2024

必要に応じて、管理コンソールの日付と時刻の形式をカスタマイズします。

> 注：
>
> この設定は各ユーザーアカウントに固有です。

1. ［完全な構成］ **>** ［設定］ **>** ［日時］ に移動します。

2. ［編集］をクリックして次の設定を構成します：

   - 時間形式：
     - 12 時間制（例：09:00 PM）または 24 時間制（例：21:00）で時刻を表示することを選択します。

     > 注：
     >
     > 形式をブラウザのタイムゾーンに合わせる場合は、「ローカルと同じ」オプションを選択します。

   - 日付の形式：
     - 環境設定に合わせて日付形式を構成します。例：yyyy/MM/dd。

     > 注：
     >
     > 形式をブラウザのタイムゾーンに合わせる場合は、「ローカルと同じ」オプションを選択します。

   - タイムゾーン：
     - **UTC**：ユーザーインターフェイス全体で、日付と時刻を UTC で表示します。マウスオーバーすると、現在のタイムゾーンのローカルの日付と時刻が表示されます。
     - ローカルタイムゾーン：ユーザーインターフェイス全体で、日付と時刻をローカルタイムゾーンで表示します。マウスオーバーすると日付と時刻が UTC 形式で表示されます。

VDA 登録とセッション起動の問題のトラブルシューティング

March 30, 2022

Citrix では、VDA の状態を測定できるヘルスチェック機能を提供しています。この機能を使用すると、［完全な構成］管理インターフェイスを介して、VDA 登録とセッション起動に関する一般的な問題の考えられる原因を特定できます。

サイトとその他のコンポーネントの状態と可用性を測定するためのスタンドアロンツールであるCloud Health Checkとは異なり、この機能は、［完全な構成］管理インターフェイスの ［ヘルスチェックの実行］アクションとして使用できます。

［ヘルスチェックの実行］アクションは、次のチェックを除いて、Cloud Health Checkと同じチェックを実行できます：

- VDA 登録の場合：
  - VDA の通信ポートの可用性
- VDA でのセッション起動の場合：
  - セッション開始時の通信ポートの可用性
  - VDA のアプリケーション起動パス

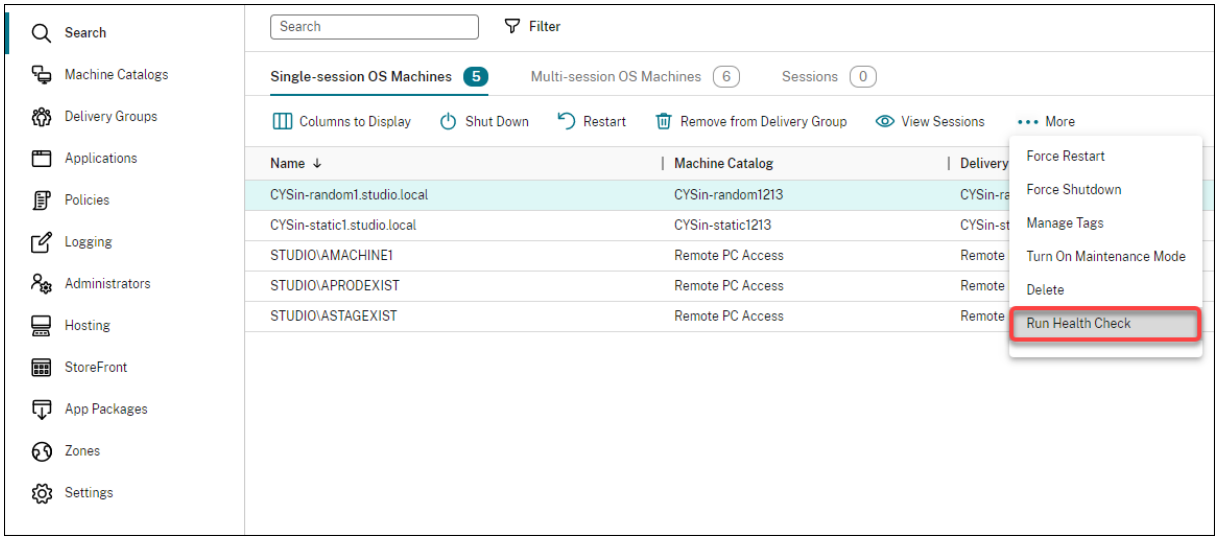
前提条件

この機能を使用する前に、次の前提条件を満たしていることを確認してください:

- Windows VDA
- VDA バージョン 2109 以降
- VDA が登録されている

VDA のヘルスチェックの実行

1. [完全な構成] 管理インターフェイスで、[検索] ノードに移動します。
2. 1 台または複数のマシンを選択し、操作バーの [ヘルスチェックの実行] を選択します。



> 注:
>
> 現在、ヘルスチェックは登録済みの VDA に対してのみ実行できます。[ヘルスチェックの実行] アクションは、未登録の VDA では使用できません。

[ヘルスチェックの実行] を選択すると、ヘルスチェックの進行状況を示すウィンドウが表示されます。ヘルスチェックが完了するまで待ちます。または、[キャンセル] をクリックしてチェックをキャンセルします。必要に応じて、ウィンドウを移動できます。

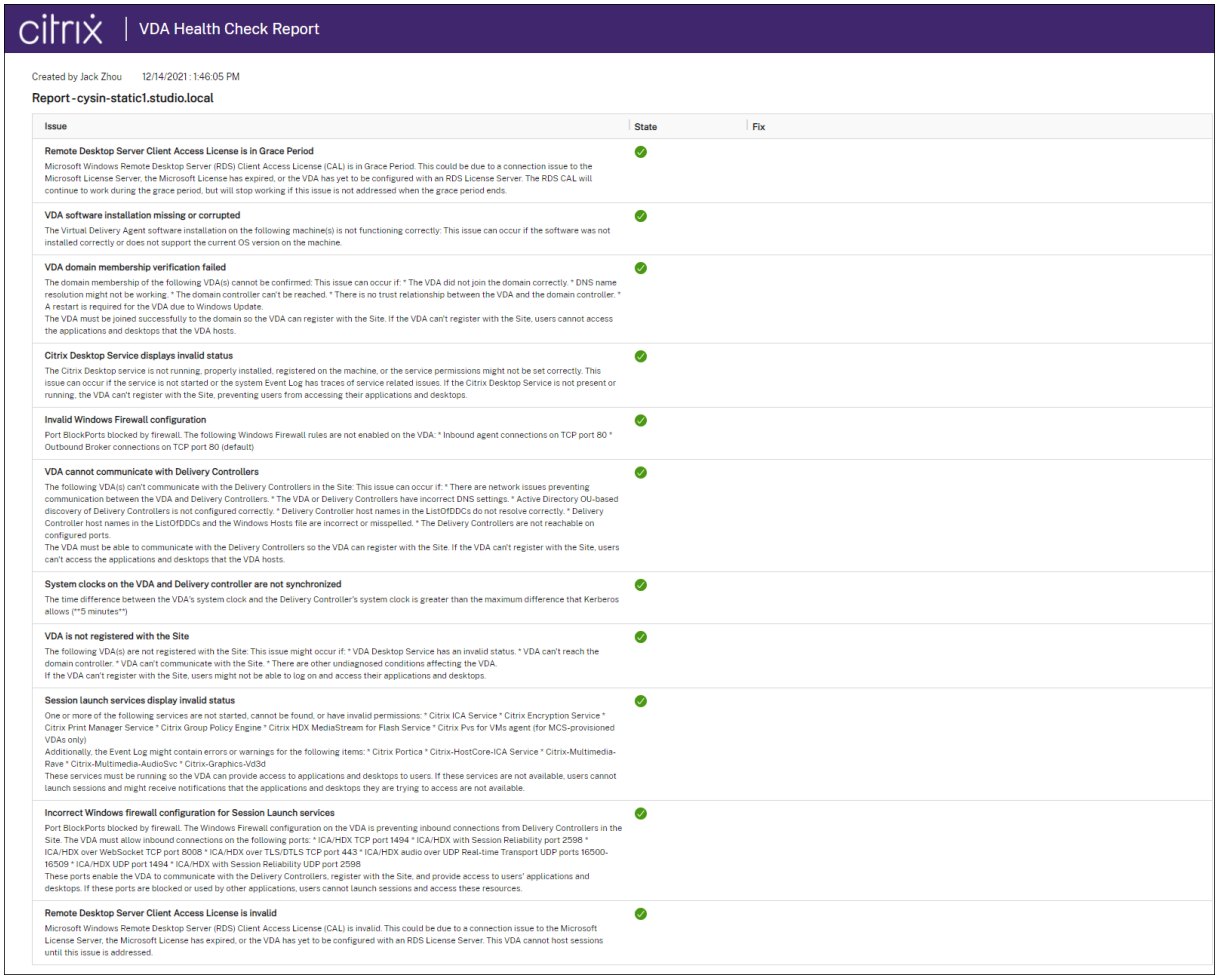
> 注:
>
> 「ヘルスチェックが進行中」のウィンドウが既に存在するシナリオでは、既存のヘルスチェックが完了するまで

> 追加のヘルスチェックは実行できません。

ヘルスチェックが完了すると、［レポートの表示］と ［閉じる］の 2 つのボタンが表示されます。ヘルスチェックの結果を表示するには、［レポートの表示］をクリックします。

ヘルスチェックレポートが新しいブラウザータブで開きます。レポートには、次の要素が含まれています:

- 結果レポートが生成された日時
- ヘルスチェックを実行した人
- 対象マシンで実行されたチェック
- 見つかった問題と修正の推奨事項



ヘルスチェックは個別と一括で実行できます。

> 注:
>
> ヘルスチェックを一括で実行する場合、選択できるマシンの数は 10 台以下です。それを超える場合、［ヘルスチェックの実行］アクションは使用できません。

ユーザーアクセス

April 26, 2023

Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）の展開におけるアプリケーションとデスクトップへのアクセスを提供する主なコンポーネントは 2 つあります:

- **Citrix Workspace** プラットフォーム: Citrix Workspace プラットフォームは、組織内の個人の役割に関連する情報、アプリ、およびその他のコンテンツへの安全なアクセスを提供できる完全なデジタルソリューションです。ユーザーは、利用可能なサービスをサブスクライブし、場所とデバイスを選ばずにアクセスできます。Citrix Workspace プラットフォームを使用して、ユーザーがコラボレーション、意思決定の改善、作業への完全な集中に必要とする最も重要な詳細を整理および自動化できます。

  Citrix Workspace は展開する手間がかからず、Citrix により常に最新状態に保たれます。Citrix Workspace プラットフォームは、新規および既存の顧客、プレビュー用途、および概念実証用途に適しています。

- オンプレミス **StoreFront**: 既存の StoreFront を使用して、Citrix Cloud 内のアプリケーションとデスクトップを集約することもできます。このユースケースでは、2 要素認証のサポートなどセキュリティが強化されており、ユーザーはクラウドサービスにパスワードを入力できません。また、ドメイン名と URL をカスタマイズすることもできます。この展開タイプは、StoreFront を展開済みのすべての Citrix Virtual Apps and Desktops ユーザーに適しています。

  「ローカルホストキャッシュと StoreFront」も参照してください。

ユーザーが組織のファイアウォールの外側から接続する場合、Citrix Cloud で Citrix Gateway（旧称 NetScaler Gateway）技術を使用して接続を SSL で保護できます。Citrix Gateway や Citrix VPX 仮想アプライアンスは非武装地帯（DMZ）に配置する SSL VPN アプライアンスであり、企業ファイアウォールを介した安全な単一アクセスポイントを提供します。

Citrix Workspace の使用

ワークスペースへのアクセスは`https://<customername>.cloud.com`を介して行われます。必要に応じて、ワークスペース URL の一部（`<customername>`）をカスタマイズすることができます。その後、使用するリソースの場所ごとに接続を構成すると、エンドユーザーが自分のワークスペースのリソースにアクセスできるようになります。エンドユーザーは、最新バージョンの Citrix Workspace アプリを使用して自分のワークスペースにアクセスします。

Citrix Workspace アプリの使用について詳しくは、次を参照してください:

- ワークスペースの構成: アクセスとカスタマイズを構成する場合。
- セキュアなワークスペース: 認証を構成する場合。
- ワークスペース環境の管理: エンドユーザーが自分のワークスペースにアクセスする方法、およびその表示内容を知りたい場合。

Citrix Workspace を介してエンドユーザーにリモートアクセスを提供する場合、Citrix Gateway サービスか、独自の Citrix Gateway を使用できます。

- Citrix Gateway サービスを使用するには:

  1. [**Citrix Cloud**] > [リソースの場所] で、使用するリソースの場所として [**Gateway**] を選択します。
  2. [**Gateway Service**] を選択し、[保存] をクリックします。
  3. [**Citrix Cloud**] > [ワークスペース構成] > [サービス統合] で、Gateway サービスを見つけて省略記号メニューから [有効にする] を選択します。

- 独自の Citrix Gateway を使用するには:

  1. Citrix Gateway を ICA プロキシとして設定します（認証ポリシーやセッションポリシーは不要です）。
  2. Citrix Gateway を使用するようにリソースの場所を設定します:

     a) [**Citrix Cloud**] > [リソースの場所] で、使用するリソースの場所として [**Gateway**] を選択します。

     b) [従来のゲートウェイ] を選択し、外部 FQDN を入力します。プロトコルは追加しないでください。ポートはオプションです。Citrix Workspace では、リモートアクセスと内部アクセスの組み合わせはサポートされません。

  3. Citrix Cloud Connector を、Secure Ticket Authority（STA）サーバーとして Citrix Gateway にバインドします。詳しくは、CTX232640を参照してください。

     > 注:
     >
     > Citrix Gateway で STA サーバーとして使用できるのは、Citrix Cloud Connector マシンのみです。Connector Appliance など、他のコネクタを STA サーバーとして使用することはサポートされていません。

Citrix Gateway サービスと Citrix Gateway について詳しくは、「Citrix Gateway」を参照してください。

オンプレミス **StoreFront** の使用

オンプレミス StoreFront の構成方法については、StoreFront のドキュメントを参照してください。

既存の StoreFront を使用するメリットの 1 つは、Citrix Cloud Connector によりユーザーパスワードが暗号化されることです。資格情報は、ランダムに生成されるワンタイムキーを使用して AES-256 で Cloud Connector によ

り暗号化されます。このキーは Citrix Workspace アプリに直接返され、クラウドに送信されることはありません。Citrix Workspace アプリは返されたキーをセッションの開始時に VDA に提供して、資格情報の暗号化を解除して Windows へのシングルサインオンを実現します。

- 転送には、HTTP とポート 80 を選択します。StoreFront マシンは、指定した FQDN（完全修飾ドメイン名）から Cloud Connector に直接アクセスできる必要があります。Cloud Connector は、クラウド NFuse/STA の URL に到達できる必要があります（`https://<customername\>.xendesktop.net/Scripts/wpnbr.dll`および`ctxsta.dll`）。
- 高可用性を確保するには、Cloud Connector を Delivery Controller として追加します。

最新バージョンの StoreFront を使用してください。

外部アクセス

Citrix Gateway およびオンプレミス StoreFront を介した外部アクセスを提供するには：

- 通常と同様に、認証ポリシーおよびセッションポリシーを使用して Citrix Gateway を設定します。詳しくは、Citrix Gateway のドキュメントを参照してください。
- オンプレミス StoreFront ストアの Delivery Controller を、Citrix Cloud Connector にポイントします。Cloud Connector を、STA サーバーとして Citrix Gateway にバインドします。
- Citrix Gateway には、StoreFront と同じ STA URL を使用する必要があります。既存の Citrix Virtual Apps and Desktops 環境の STA を使用するようゲートウェイを設定していない場合は、Cloud Connector を STA として使用できます。

内部アクセス

オンプレミス StoreFront を介した内部アクセスを提供するには、オンプレミス StoreFront ストアの Delivery Controller を、Citrix Cloud Connector にポイントします。

外部アクセスと内部アクセス

Citrix Gateway およびオンプレミス StoreFront を介した外部および内部アクセスを提供するには：

- 通常と同様に、認証ポリシーおよびセッションポリシーを使用して Citrix Gateway を設定します。詳しくは、Citrix Gateway のドキュメントを参照してください。
- Cloud Connector を、STA サーバーとして Citrix Gateway にバインドします。
- オンプレミス StoreFront ストアの Delivery Controller を、Cloud Connector にポイントします。

ローカルホストキャッシュと **StoreFront**

ローカルホストキャッシュを使用すると、Cloud Connector が Citrix Cloud と通信できなくなった場合でも、Citrix DaaS 環境での接続仲介操作を続行できるようになります。

ローカルホストキャッシュは、顧客が展開したオンプレミス StoreFront が含まれるリソースの場所でのみ動作します。Citrix Workspace でのローカルホストキャッシュの使用はサポートされていません。

各リソースの場所には、顧客が展開するオンプレミスの StoreFront が必要です。リソースの場所に、このリソースの場所内のすべての Cloud Connector をポイントするローカルの StoreFront が含まれていることを確認します。

詳しくは、「ローカルホストキャッシュ」を参照してください。

仮想 **IP** と仮想ループバック

March 30, 2022

> 重要:
>
> Windows 10 Enterprise マルチセッションでは、リモートデスクトップ IP 仮想化（仮想 IP）がサポートされていないため、Windows 10 Enterprise マルチセッションでは、仮想 IP も仮想ループバックもサポートしていません。

仮想 IP および仮想ループバック機能は、Windows Server 2016 マシンでサポートされています。これらの機能は、Windows デスクトップ OS マシンでは使用できません。

Microsoft 社の仮想 IP アドレス機能により、セッションごとに動的に割り当てられる固有の IP アドレスを公開アプリケーションで使用できます。Citrix の仮想ループバック機能を使用すると、ローカルホスト（デフォルトで 127.0.0.1）と通信するアプリケーションで、ローカルホストの範囲内（127.*）で固有の仮想ループバックアドレスが使用されるように構成できます。

CRM（Customer Relationship Management）や CTI（Computer Telephony Integration）などの特定のアプリケーションでは、アドレス割り当て、ライセンス付与、識別、またはそのほかの目的で IP アドレスが使用されるため、セッションに固有の IP アドレスまたはループバックアドレスが必要です。また、一部のアプリケーションでは静的なポートにバインドされるため、マルチユーザー環境でそのアプリケーションの追加インスタンスを起動しようとすると、そのポートが使用済みなので起動に失敗します。これらのアプリケーションが Citrix Virtual Apps 環境で正しく動作するためには、クライアントデバイスごとに異なる IP アドレスが使用される必要があります。

仮想 IP と仮想ループバックは、それぞれ独立した機能です。これらの機能のいずれかまたは両方を使用できます。

使用する機能に応じて、管理者は以下の操作を行います。

- Microsoft 社の仮想 IP 機能を使用するには、Windows サーバー上で仮想 IP を有効にして構成します。（Citrix ポリシーの設定は必要ありません。）

- Citrix の仮想ループバック機能を使用するには、Citrix ポリシーで 2 つの設定項目を構成します。

仮想 **IP**

Windows サーバー上で仮想 IP 機能を有効にすると、セッション内で動作する各アプリケーションで固有のアドレスが使用されるように構成できます。ユーザーは、Citrix Virtual Apps 上にあるこれらのアプリケーションを、ほかの公開アプリケーションと同じように使用することができます。以下のいずれかの動作をするプロセスでは、仮想 IP アドレスを設定します。

- ハードコードされた（固定された）TCP ポート番号を使用する。
- Windows ソケットを使用し、固有の IP アドレスまたは固定された TCP ポート番号を使用する。

アプリケーションで仮想 IP アドレスが必要かどうかを判断するには、次の手順に従います。

1. Microsoft 社の Web サイトから、TCPView ツールを入手します。このツールを使用すると、特定の IP アドレスおよびポートを使用しているすべてのアプリケーションを一覧表示できます。
2. TCPView の［Options］メニューで、［Resolve Addresses］を無効にします。これにより、一覧にホスト名ではなくアドレスが表示されるようになります。
3. 対象となるアプリケーションを起動して、使用されている IP アドレスとポート、およびそれらのポートを開いているプロセスの名前を TCPView で確認します。
4. サーバーの IP アドレス 0.0.0.0 または 127.0.0.1 を使用するプロセスを構成します。
5. そのアプリケーションの追加インスタンスを起動して、別のポート上で同じ IP アドレスが使用されないことを確認します。

Microsoft リモートデスクトップ（**RD**）の **IP** 仮想化のしくみ

- 仮想 IP アドレスを使用するには、Windows サーバー上でこの機能を有効にする必要があります。

  たとえば、Windows Server 2016 環境でサーバーマネージャーを使用し、［リモートデスクトップサービス］**>**［**RD** セッションホストの構成］の順に展開して RD IP 仮想化機能を有効にします。次に、IP アドレスを DHCP（Dynamic Host Configuration Protocol：動的ホスト構成プロトコル）サーバーによりセッションごとまたはプログラムごとに動的に割り当てるように設定を行います。手順については、Microsoft 社のドキュメントを参照してください。

- この機能を有効にすると、セッション起動時にサーバーは、DHCP サーバーから動的に割り当てられた IP アドレスを要求します。

- RD IP 仮想化機能によって、セッションごとまたはプログラムごとに、リモートデスクトップ接続に IP アドレスが割り当てられます。複数のプログラムに IP アドレスを割り当てる場合、これらのプログラム間でセッションごとの IP アドレスが共有されます。

- アドレスがセッションに割り当てられた後、以下の呼び出しが行われるたびに、セッションはシステムのプライマリ IP アドレスではなく仮想アドレスを使用します：`bind`、`closesocket`、`connect`、

`WSAConnect`、`WSAAccept`、`getpeername`、`getsockname`、`sendto`、`WSASendTo`、`WSASocketW`、`gethostbyaddr`、`getnameinfo`、`getaddrinfo`。

リモートデスクトップセッションのホスト環境で Microsoft の IP 仮想化機能を使用すると、アプリケーションと Winsock コールとの間に「フィルター」コンポーネントを挿入することで、アプリケーションと特定の IP アドレスがバインドされます。IP アドレスがバインドされると、アプリケーションはそのアドレスだけで要求を待ち受けるようになります。アプリケーションの TCP リスナーまたは UDP リスナーは自動的に仮想 IP アドレス（または仮想ループバックアドレス）にバインドされ、アプリケーションからの接続はその仮想アドレスから開かれます。

Windows ポリシーにより制御される`GetAddrInfo()`など、アドレスを返すファンクションでローカルホスト IP アドレスが要求されると、返された IP アドレスがそのセッションの仮想 IP アドレスに変換されます。このようなファンクションでローカルサーバーの IP アドレスを取得しようとするアプリケーションには、セッション固有の仮想 IP アドレスだけが渡されます。このようにしてアプリケーションに渡された IP アドレスは、後続のソケットコール（bind や connect など）で使用されます。Windows ポリシーについて詳しくは、RDS IP Virtualization in Windows Serverを参照してください。

アプリケーションでは、アドレス 0.0.0.0 で、リスナー用のポートのバインドが必要になる場合があります。このようなアプリケーションで静的なポート番号が使用されると、競合が発生するため、複数のインスタンスを起動できなくなります。仮想 IP アドレス機能では、0.0.0.0 へのファンクションコールが特定の仮想 IP アドレスに変換されます。これにより、セッションごとに異なるアドレス上のポートが使用されるため、同じポート番号を使用する複数のアプリケーションを実行できるようになります。このファンクションコールは、仮想 IP アドレス機能が有効な ICA セッションでのみ変換されます。たとえば、すべてのインターフェイス（0.0.0.0）と特定のポート（9000 など）にバインドするアプリケーションの 2 つのインスタンスが、それぞれ異なるセッションで実行される場合、VIPAddress1:9000 と VIPAddress2:9000 にバインドされるため、競合が起きません。

仮想ループバック

Citrix ポリシーで仮想 IP ループバック機能を有効にすると、各セッションで通信に独自のループバックアドレスが使用されるようになります。アプリケーションが Winsock 呼び出しでローカルホストのアドレス（デフォルトで 127.0.0.1）を使用する場合、仮想ループバック機能により、127.0.0.1 が 127.X.X.X（X.X.X はセッション ID に 1 を足したものです）に置き換えられます。たとえば、セッション ID が 7 の場合は 127.0.0.8 になります。セッション ID が 4 オクテットを超える場合（つまり 255 を超える場合）は、127.0.1.0 のように次のオクテットに繰り上げられます。また、最大値は 127.255.255.255 です。

以下のいずれかの動作をするプロセスでは、仮想ループバックを設定します。

- Windows ソケットのループバック（localhost）アドレス 127.0.0.1 を使用する。
- ハードコードされた（固定された）TCP ポート番号を使用する。

プロセス間通信でループバックアドレスを使用するアプリケーションでは、仮想ループバックアドレスポリシー設定を使用します。追加の構成は必要ありません。仮想ループバックは仮想 IP に依存しないため、Windows サーバーの構成は不要です。

- 仮想 IP ループバックサポートこのポリシー設定を有効にすると、各セッション固有の仮想ループバックアドレスが使用されるようになります。このチェックボックスは、デフォルトでオフになっています。この機能は、［仮想 IP ループバックプログラム一覧］ポリシー設定で指定したアプリケーションにのみ適用されます。
- 仮想 IP ループバックプログラム一覧このポリシー設定では、仮想 IP ループバック機能を使用するアプリケーションを指定します。この設定は、［仮想 IP ループバックサポート］ポリシー設定が有効になっている場合のみ適用されます。

関連機能

次のレジストリ設定により、仮想ループバックが仮想 IP よりも優先されるようになります（優先ループバック機能）。ただし、以下の点に注意してください。

- 仮想 IP アドレスと仮想ループバックの両方の機能を有効にする場合にのみ、優先ループバック機能を使用してください。そうしないと、意図しない結果が生じる可能性があります。
- レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、シトリックスでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

アプリケーションのホストサーバー上で、regedit を実行します。

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP
- 値の名前：PreferLoopback、種類：REG_DWORD、値のデータ：1
- 値の名前：PreferLoopbackProcesses、種類：REG_MULTI_SZ、データ：< プロセスの一覧 > プロセスの一覧 >

ゾーン

May 17, 2024

はじめに

Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）展開が WAN で接続された広範な場所に分散している場合、ネットワークの遅延と信頼性による問題が発生することがあります。ゾーンを使用することにより、離れた場所にいるユーザーは、WAN の大規模セグメントを経由する接続がなくてもリソースに接続できるようになります。Citrix DaaS 環境では、各リソースの場所はゾーンと見なされます。

ゾーンは、あらゆる規模の展開で有用です。ゾーンを使用して、アプリケーションおよびデスクトップとユーザーの距離を縮めることにより、パフォーマンスを改善することができます。ゾーンは、障害回復、地理的に離れたデータセンター、ブランチオフィス、クラウド、またはクラウドのアベイラビリティゾーンに使用できます。

この記事を通じ、ローカルという用語は対象となるゾーンを指します。たとえば、「VDA はローカル Cloud Connector に登録されます」という場合、VDA は VDA が存在するゾーンの Cloud Connector に登録されることを意味します。

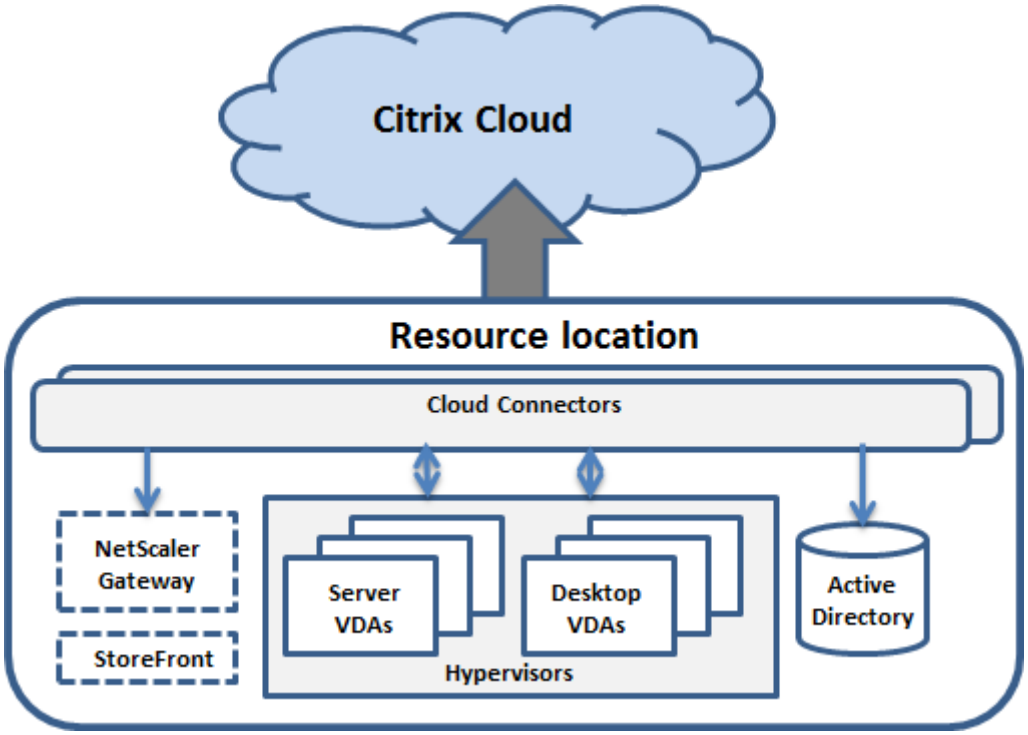
オンプレミスの **Citrix Virtual Apps and Desktops** 環境のゾーンとの違い

Citrix DaaS 環境のゾーンは、オンプレミスの Citrix Virtual Apps and Desktops 環境のものと似ていますが、同一ではありません。

- Citrix DaaS のゾーンは、リソースの場所を作成して Cloud Connector を追加すると自動的に作成されます。オンプレミス展開とは異なり、Citrix DaaS 環境によってゾーンがプライマリまたはサテライトに分類されることはありません。
- XenApp 6.5 以前のバージョンでは、ゾーンにはデータコレクターが含まれていました。Citrix DaaS は、ゾーンにデータコレクターを使用しません。また、フェールオーバーおよび優先ゾーンの機能も異なります。

ゾーンのコンテンツ

ゾーンは、リソースの場所に相当します。リソースの場所を作成して Cloud Connector をインストールすると、ゾーンが自動的に作成されます。お客様のニーズと環境に応じて、各ゾーンにはさまざまなリソースを含めることができます。



各ゾーンには、少なくとも 1 つの Cloud Connector が必要であり、冗長性を確保するには Cloud Connector を 2 つ以上インストールすることが推奨されます。

ゾーンには、マシンカタログ、ハイパーバイザー、ホスト接続、ユーザー、アプリケーションを配置することができます。また、Citrix Gateway サーバーおよび StoreFront サーバーを配置することもできます。ローカルホストキャッシュ機能を使用するには、ゾーンに StoreFront サーバーを配置する必要があります。

ゾーンは、Citrix Workspace および Citrix Gateway サービスでサポートされています。

ゾーンにアイテムを配置すると、これらのアイテムおよびこれらに関連する他のオブジェクトと Citrix DaaS との通信方法に影響します。

- ハイパーバイザーコネクションをサテライトゾーンに配置すると、このコネクションの管理対象であるすべてのハイパーバイザーも同じサテライトゾーン内に存在するものとみなされます。
- マシンカタログをゾーンに配置すると合、このカタログ内のすべての VDA も同じサテライトゾーンにあるとみなされます。
- ゾーンには Citrix Gateway インスタンスも追加できます。リソースの場所の作成時に、Citrix Gateway を追加するオプションを使用できます。Citrix Gateway をゾーンに関連付けると、そのゾーンの VDA への接続時に優先して使用されるようになります。
- ゾーンの Citrix Gateway を、ほかのゾーンまたは外部からそのゾーンへのユーザー接続に使用するのが理想的です。ゾーン内の接続にも使用できます。
- リソースの場所をさらに作成して Cloud Connector をインストールすると（追加のゾーンが自動作成されます）、ゾーン間でリソースを移動できるようになります。この柔軟性により、近くに配置することで最適に動作するアイテムを分離してしまう可能性があります。たとえば、カタログを、カタログ内のマシンを作成する接続（ホスト）とは異なるゾーンに移動すると、パフォーマンスに影響する可能性があります。そのため、アイテムをゾーン間で移動する前に、意図しない影響が出る可能性を考慮してください。カタログと、カタログで使用されるホスト接続は、同じゾーン内に保持します。

あるゾーンと Citrix Cloud 間の接続に障害が生じた場合でも、ローカルホストキャッシュ機能により、そのゾーン内の Cloud Connector は同ゾーン内の VDA への接続を仲介し続けることができます（ゾーンには StoreFront をインストールしておく必要があります）。この機能により、たとえばオフィスを社内ネットワークに接続する WAN リンクで障害が発生しても、作業者はローカル StoreFront サイトを使用してローカルリソースにアクセスできます。詳しくは、「ローカルホストキャッシュ」を参照してください。

VDA の登録先

以下のゾーン登録機能を使用するには、VDA のバージョンが 7.7 以上である必要があります:

- ゾーン内の VDA は、ローカル Cloud Connector に登録されます。
  - この Cloud Connector が Citrix Cloud と通信できる限り、通常の操作が行われます。
  - この Cloud Connector が動作していても Citrix Cloud と通信できない場合、ゾーンにローカル StoreFront があれば、Connector はローカルホストキャッシュ停止状態モードになります。
  - Cloud Connector に障害が発生した場合、このゾーン内の VDA は別のローカル Cloud Connector への登録を試みます。あるゾーンの VDA が、別のゾーンの Cloud Connector に登録しようとすることはありません。

- Citrix Cloud 管理コンソールを使用してゾーンの Cloud Connector を追加または削除した場合、自動更新が有効になっていれば、このゾーンの VDA には利用可能なローカル Cloud Connector の最新の一覧が提供されるため、各 VDA は登録し接続を受け入れられる Cloud Connector を把握できます。
- ［完全な構成］管理インターフェイスを使用してマシンカタログを別のゾーンに移動すると、そのカタログの VDA は、カタログの移動先のゾーンにある Cloud Controller に再登録されます。カタログを移動する際には、関連するホスト接続も同じゾーンに移動してください。
- 停止状態（ゾーン内の Cloud Connector が Citrix Cloud と通信できない状態）では、そのゾーンに登録済みのマシンに関連付けられているリソースのみを利用できます。

ゾーン優先度

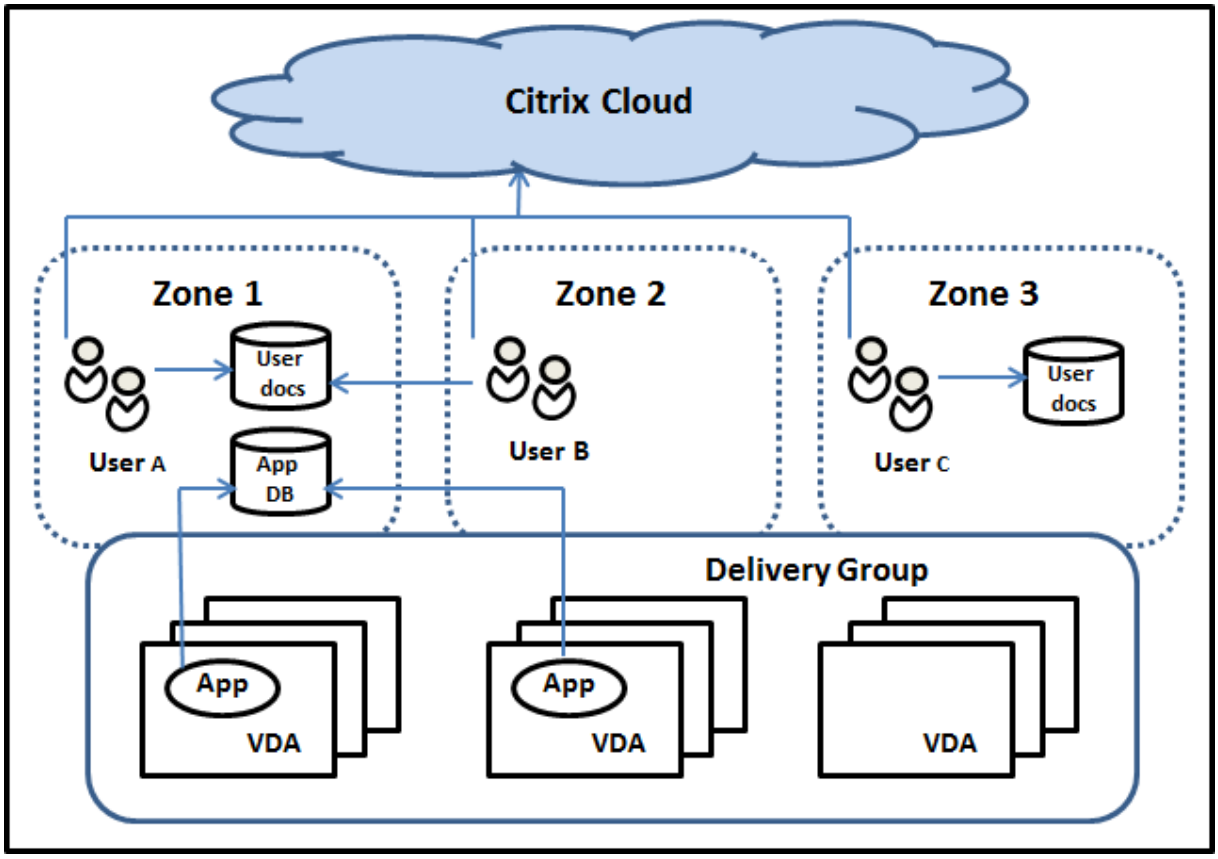
複数のゾーンがあるサイトでは、管理者は、アプリケーションやデスクトップの起動にどの VDA が使用されるかを、ゾーンの優先度機能によってより柔軟に制御できます。

ゾーンの優先度のしくみ

ゾーンの優先度には以下の 3 つの形式があります。以下によっては、特定のゾーンに VDA を使用するのが好ましい場合があります。

- アプリケーションのデータの保存先。これを「アプリケーションホーム」と呼びます。
- プロファイルやホームシェアなどの、ユーザーのホームデータの場所。これを「ユーザーホーム」と呼びます。
- （Citrix Workspace アプリが実行されている）ユーザーの現在位置。これを「ユーザーの場所」と呼びます。ユーザーの場所には、バージョン 3.7 以降の StoreFront およびバージョン 11.0-65.x 以降の Citrix Gateway（旧称 NetScaler Gateway）が必要です。

次の図は、マルチゾーン構成の例を示しています。



この例では、VDA は 3 つのゾーンに分散されていますが、属しているデリバリーグループは同じです。そのため、Citrix DaaS ブローカーはユーザーの起動依頼にどの VDA を使用するかを選択できる場合があります。この例は、ユーザーがそれぞれ異なる場所で Citrix Workspace アプリのエンドポイントを実行できることを示しています。ユーザー A は、ゾーン 1 の Citrix Workspace アプリでデバイスを使用しています。ユーザー B は、ゾーン 2 のデバイスを使用しています。同様に、ユーザーのドキュメントも異なる場所に保管できます。ユーザー A と B は、ゾーン 1 にある共有を使用します。ユーザー C はゾーン 3 の共有を使用します。また、公開アプリケーションの 1 つは、ゾーン 1 にあるデータベースを使用しています。

ユーザーまたはアプリケーションにホームゾーンを構成して、ユーザーまたはアプリケーションをゾーンと関連付けることができます。このようにすると、ブローカーはこれらの関連付けを使用して、セッションを開始するゾーンを選択できます（リソースが利用可能な場合）。以下を実行します：

- ユーザーをゾーンに追加して、ユーザーのホームゾーンを構成します。
- アプリケーションのプロパティを編集して、アプリケーションのホームゾーンを構成します。

ユーザーまたはアプリケーションに構成できるホームゾーンは 1 回あたり 1 つのみです（ユーザーについては、複数のゾーンメンバーシップがある場合は例外となることがあります。「そのほかの考慮事項」セクションを参照してください。ただし、その場合においても、ブローカーが使うホームゾーンは 1 つのみです）。

ユーザーおよびアプリケーションのゾーン優先度を構成できますが、ブローカーは起動する優先ゾーンを 1 つだけ選択します。優先ゾーンの選択におけるデフォルトの優先順位は、アプリケーションホーム、ユーザーホーム、ユーザーの場所の順になります。ユーザーがアプリケーションを起動すると、優先ゾーンは次のように選択されます：

- アプリケーションに構成済みのゾーンの関連付け（アプリケーションホーム）がある場合、優先ゾーンはそのアプリケーションのホームゾーンとなります。
- アプリケーションには構成済みのゾーンの関連付けがなく、ユーザーには構成されたゾーン（ユーザーホーム）がある場合、優先ゾーンはそのユーザーのホームゾーンとなります。
- アプリケーションにもユーザーにもゾーンの関連付けが構成されていない場合、優先ゾーンはユーザーが Citrix Workspace アプリインスタンスを実行しているゾーン（ユーザーの場所）となります。このゾーンが定義されていない場合は、VDA およびゾーンのランダム選択が使用されます。負荷分散は、優先ゾーン内のすべての VDA に適用されます。優先ゾーンがない場合、負荷分散はデリバリーグループ内のすべての VDA に適用されます。

ゾーン優先度の調整

ユーザーまたはアプリケーションのホームゾーンを構成（または削除）することで、ゾーン優先度を使用する（または使用しない）方法をさらに制限できます。

- ユーザーのホームゾーンの使用必須：デリバリーグループで、「セッションをユーザーのホームゾーンで開始し（ユーザーのホームゾーンがある場合）、ホームゾーンでリソースが利用可能でない場合には別のゾーンにフェールオーバーしない」ように指定できます。この制限は、ゾーン間での大きなプロファイルやデータファイルのコピーを禁止する必要がある場合に有用です。つまり、他のゾーンでセッションを開始するのではなく、他のゾーンではセッションが開始されないようにします。
- アプリケーションのホームゾーンの使用必須：同様に、アプリケーションのホームゾーンを構成する際に、「アプリケーションをそのゾーンでのみ起動し、アプリケーションのホームゾーンでリソースが利用可能でない場合には他のゾーンにフェールオーバーしない」ように指定できます。
- アプリケーションのホームゾーンなし、構成済みのユーザーホームゾーンは無視：アプリケーションのホームゾーンを指定しない場合は、「アプリケーションを起動するときに構成済みのユーザーゾーンを考慮しない」ように指定することもできます。たとえば、ユーザーに他のホームゾーンがある場合でも、ユーザーのマシンの近くにある VDA で特定のアプリケーションが実行されるようにするには、ユーザーの場所ゾーン優先度を使用します。

優先ゾーンによるセッション使用への影響

ユーザーがアプリケーションやデスクトップを起動すると、ブローカーは既存のセッションよりも優先ゾーンを使用しようとします。

アプリケーションまたはデスクトップを起動しているユーザーに、起動中のリソースに最適なセッション（アプリケーションのセッション共有を使用できるセッション、または起動中のリソースを既に実行しているセッションなど）があるにもかかわらず、セッションがユーザーまたはアプリケーションの優先ゾーン以外のゾーンの VDA に存在する場合、新しいセッションが作成されることがあります。このアクションにより、セッションは、ユーザーのセッション要件に対して優先度の低いゾーンに再接続される前に、正しいゾーンで開始されます（そのゾーンに使用可能な容量がある場合）。

操作できなくなる孤立セッションが発生しないようにするため、優先ではないゾーンにあっても、再接続は既存の切断されたセッションにのみ許可されます。

セッション開始の望ましさの順は、以下のとおりです。

1. 優先ゾーンにある既存セッションに再接続する。
2. 非優先ゾーンにある既存の切断済みセッションに再接続する。
3. 優先ゾーンで新しいセッションを開始する。
4. 非優先ゾーンにある接続中の既存セッションに再接続する。
5. 非優先ゾーンで新しいセッションを開始する。

ゾーン優先度に関するそのほかの考慮事項

- ユーザーグループ（セキュリティグループなど）のホームゾーンを構成する場合、（直接または間接メンバーシップによる）そのグループのユーザーは、指定されたゾーンに関連付けられます。ただし、ユーザーは複数のセキュリティグループのメンバーになることができるため、別のグループのメンバーシップで他のホームゾーンが構成されている可能性があります。そのような場合は、そのユーザーのホームゾーンの特定があいまいになる可能性があります。

  ユーザーに、グループメンバーシップで取得されなかった構成済みのホームゾーンがある場合、そのゾーンがゾーン優先度に使用されます。グループメンバーシップで取得されたゾーンの関連付けはすべて無視されます。

  ユーザーに、グループメンバーシップのみで取得された複数の異なるゾーンの関連付けがある場合、ブローカーはそれらのゾーンの中からランダムに選択します。ブローカーがゾーンを選択すると、そのゾーンはユーザーのグループメンバーシップが変更されるまで、後続のセッションの開始に使用されます。

- ユーザーの場所ゾーン優先度には、デバイス接続で経由されている Citrix Gateway により、エンドポイントデバイス上の Citrix Workspace アプリが検出される必要があります。Citrix は、特定のゾーンに IP アドレスの範囲を関連付けるように構成される必要があります。検出されたゾーンの ID は、StoreFront を介して Citrix DaaS に渡す必要があります。

「Zone Preference Internals」はゾーンのオンプレミスでの使用方法に関するブログ記事ですが、関連する技術的な詳細についても説明しています。

ゾーンの管理権限

すべての管理権限を実行できる管理者が、サポートされるゾーン管理タスクをすべて実行できます。アイテムをゾーン間で移動する場合、ゾーン関連の権限（ゾーン読み取り権限を除く）は必要ありません。ただし、移動するアイテムの編集権限が必要になります。たとえば、マシンカタログをゾーン間で移動するには、そのカタログの編集権限が必要です。

Citrix Provisioning を使用する場合： Citrix Provisioning コンソールではゾーンが認識されないため、特定のゾーンに配置するマシンカタログを作成する場合は ［管理］**>**［完全な構成］インターフェイスを使用することをお

勧めします。カタログを作成した後、Citrix Provisioning コンソールを使用して、そのカタログのマシンをプロビジョニングできます。

ゾーンの作成

Citrix Cloud でリソースの場所を作成し Cloud Connector を追加すると、Citrix DaaS により名前付きのゾーンが自動的に作成されます。オプションとして、後で説明を追加できます。

リソースの場所を複数作成し、各ゾーンが自動的に作成されると、ゾーン間でリソースを移動できるようになります。

リソースの場所とゾーンは、定期的に（通常はおよそ 5 分ごとに）同期されます。このため、Citrix Cloud でリソースの場所の名前を変更した場合、その変更内容は 5 分以内に関連付けられたゾーンに反映されます。

ゾーンの説明を追加または変更する

ゾーンの名前は変更できませんが、ゾーンの説明を追加または変更することはできます。

1. ［管理］**>**［完全な構成］の左側ペインで ［ゾーン］を選択します。
2. 中央ペインでゾーンを選択し、操作バーで ［ゾーンの編集］を選択します。
3. ゾーンの説明を追加するか変更します。
4. ［**OK**］または ［適用］を選択します。

ゾーン間でリソースを移動する

1. ［管理］**>**［完全な構成］の左側ペインで ［ゾーン］を選択します。
2. 中央ペインでゾーンを選択し、1 つまたは複数のアイテムを選択します。
3. アイテムを移動先ゾーンにドラッグするか、または操作バーで ［アイテムを移動］を選択してから移動先ゾーンを指定します。（Cloud Connector を選択することはできますが、それを実際に別のゾーンに移動することはできません）。

選択したアイテムが確認メッセージで一覧表示され、それらすべてのアイテムを移動してよいか確認されます。

注：マシンカタログでハイパーバイザーまたはクラウドサービスへのホスト接続を使用している場合、そのカタログと接続が同じゾーン内にあることを確認してください。同じゾーンに含まれていない場合、パフォーマンスが低下する可能性があります。どちらかのアイテムを移動したら、もう 1 つのアイテムも移動してください。

ゾーンの削除

ゾーンは削除できません。ただし、リソースの場所を削除することはできます（Cloud Connector の削除後）。リソースの場所を削除すると、ゾーンも自動的に削除されます。

- ゾーンにアイテム（カタログ、接続、アプリケーション、ユーザーなど）が含まれていない場合、ゾーンは次回のゾーンとリソースの場所間の同期時に削除されます。同期は 5 分間隔で発生します。
- ゾーンにアイテムが含まれている場合は、すべてのアイテムを削除するとゾーンは自動的に削除されます。

ユーザーのホームゾーンの追加

ユーザーにホームゾーンを構成することは、ゾーンへのユーザーの追加とも言います。

1. ［管理］**>**［完全な構成］の左側ペインで ［ゾーン］を選択します。
2. 中央ペインでゾーンを選択し、操作バーで ［ゾーンへのユーザーの追加］を選択します。
3. ［ゾーンへのユーザーの追加］ダイアログボックスで、［追加］を選択してから、ゾーンに追加するユーザーおよびユーザーグループを選択します。既にホームゾーンがあるユーザーを指定すると、2 つの選択肢を提供するメッセージが表示されます。［はい］を選択すると、指定したユーザーのうち、ホームゾーンのないユーザーのみが追加されます。［いいえ］を選択すると、ユーザー選択ダイアログに戻ります。
4. ［**OK**］を選択します。

構成済みのホームゾーンがあるユーザーについては、ユーザーのホームゾーンからのセッション開始のみ要求できます。

1. デリバリーグループを作成または編集します。
2. ［ユーザー］ページで、［セッションはユーザーのホームゾーンで開始（構成済みの場合）］チェックボックスを選択します。

そのデリバリーグループ内のユーザーによって開始されたすべてのセッションは、そのユーザーのホームゾーンから開始される必要があります。そのデリバリーグループ内のユーザーに構成済みのホームゾーンがない場合、この設定は有効になりません。

ユーザーのホームゾーンの削除

この手順は、ゾーンからのユーザーの削除とも言います。

1. ［管理］**>**［完全な構成］の左側ペインで ［ゾーン］を選択します。
2. 中央ペインでゾーンを選択し、操作バーで ［ゾーンのユーザーの削除］を選択します。
3. ［ゾーンへのユーザーの追加］ダイアログボックスで、［削除］を選択して、ゾーンから削除するユーザーおよびグループを選択します。この操作では、ユーザーはゾーンからのみ削除されます。削除されたユーザーは、属するデリバリーグループには残ったままになります。
4. 確認のメッセージが表示されたら、削除を確定します。

アプリケーションのホームゾーンの管理

アプリケーションにホームゾーンを構成することは、ゾーンへのアプリケーションの追加とも言います。デフォルトで、マルチゾーン環境では、アプリケーションにはホームゾーンがありません。

アプリケーションのホームゾーンは、アプリケーションのプロパティで指定されます。アプリケーションのプロパティは、アプリケーションをグループに追加するとき、またはその後に構成できます。

- デリバリーグループの作成時または既存のグループへのアプリケーションの追加時に、ウィザードの ［アプリケーション］ページで ［プロパティ］を選択します。
- アプリケーションの追加後にアプリケーションのプロパティを変更するには、左側ペインで ［ゾーン］を選択します。アプリケーションを選択し、操作バーで ［プロパティ］を選択します。

アプリケーションのプロパティまたは設定の ［ゾーン］ページで以下の操作を行います:

- アプリケーションにホームゾーンを追加する場合は、
  - ［選択したゾーンを決定に使用］をクリックしてから、ゾーンを選択します。
  - アプリケーションを選択したゾーンからのみ起動する（他のゾーンからは起動しないようにする）には、ゾーン選択の下にあるチェックボックスを選択します。
- アプリケーションにホームゾーンを設定しない場合は、
  - ［ホームゾーンを構成しない］ラジオボタンを選択します。
  - このアプリケーションを起動するときに、ブローカーによって構成済みのユーザーのゾーンが考慮されないようにするには、ラジオボタンの下にあるチェックボックスを選択します。この場合、アプリケーションのホームゾーンおよびユーザーのホームゾーンが、このアプリケーションを起動する場所の決定に使用されることはありません。

ゾーンの指定が含まれるそのほかの操作

ゾーンが複数ある場合、ホスト接続を追加するとき、またはカタログを作成するときに特定のゾーンを指定できます。ゾーンは、選択リストにアルファベット順で一覧表示されます。デフォルトでは、アルファベット順で先頭の名前が選択されています。

トラブルシューティング

［完全な構成］は、ローカルホストキャッシュとゾーンが正しく構成されていることを確認するための予防的なアラートを提供するため、停止による影響がユーザーに生じる前に問題を解決できます。この機能は、基幹業務のワークロードへの継続的なユーザーアクセスを維持するのに役立ちます。

問題のあるゾーンそれぞれに対して ［トラブルシューティング］タブが表示されます。

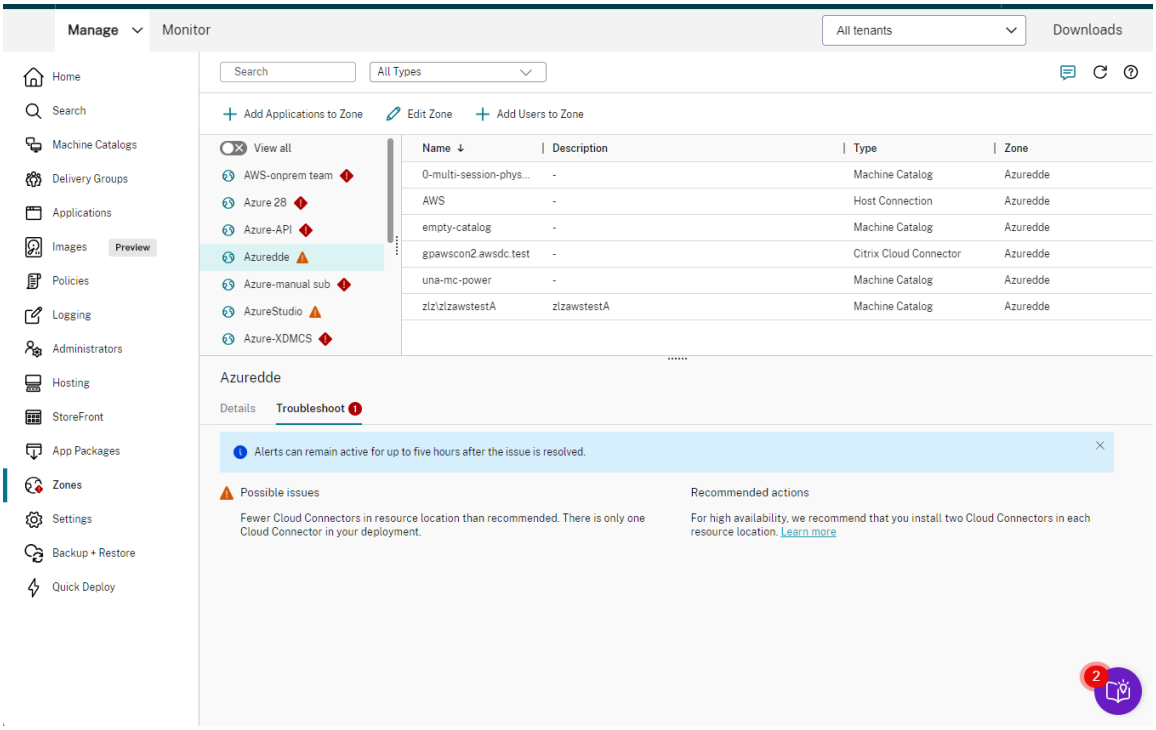
ゾーン関連の問題を確認するには、以下の手順に従います。

1. ［完全な構成］**>** ［ゾーン］に移動し、警告アイコンのあるゾーンをクリックします。
2. 下部ペインの ［トラブルシューティング］タブに移動し、そこで表示される情報を読みます。

注:

診断は 1 時間ごとに更新されます。

トラブルシューティング情報の例:



次の表に、ゾーン関連の警告とエラーの完全なリストを示します。

重要度	考えられる問題	推奨される操作
警告	リソースの場所に複数のドメインが含まれています。リソースの場所に複数のドメインがある場合、信頼関係が適切に構成されていないと、VDA の登録に時間がかかることがあります。また、VDA は高可用性モードでの登録に失敗する可能性があります。	このリソースの場所においてドメイン間の信頼関係が正しく構成されていることを確認します。Citrix Cloud Connector の技術詳細を参照してください。
警告	リソースの場所に推奨される数よりも多くのホスト接続があります。上限値を超えると、パフォーマンスが低下し、ユーザーエクスペリエンスに影響を与える可能性があります。	このリソースの場所におけるホスト接続数を推奨上限値以下に減らします。「上限」を参照してください。

重要度	考えられる問題	推奨される操作
警告	論理 CPU プロセッサが推奨される数より少ない。高可用性モードではパフォーマンスが低下する可能性があります。	各 Cloud Connector が論理 CPU プロセッサの最小要件を満たしていることを確認してください。「ローカルホストキャッシュ」を参照してください。
警告	リソースの場所にある Cloud Connector が推奨される数よりも少ない。この展開には Cloud Connector が 1 つしかありません。	可用性を高めるため、リソースの場所ごとに Cloud Connector を 2 つインストールすることをお勧めします。Citrix Cloud Connector の技術詳細を参照してください。
警告	少なくとも 1 つの Cloud Connector に、推奨される RAM より少ない RAM があります。高可用性モードではパフォーマンスが低下する可能性があります。	各 Cloud Connector が RAM の最小要件を満たしていることを確認してください。「Cloud Connector のサイズおよびスケールの考慮事項」を参照してください。
エラー	リソースの場所に推奨される数よりも多くの VDA があります。高可用性モードでは、ローカルホストキャッシュで登録できる VDA は 10000 個のみです。それ以上の VDA による登録の試行は失敗します。	このリソースの場所にある VDA の数を推奨上限以下に減らします。「上限」を参照してください。
エラー	ゾーン内の Cloud Connector に到達できません。ゾーン内のどの Cloud Connector にも到達できません。ローカルホストキャッシュまたはサービス継続性が展開用に構成されていない限り、このリソースの場所にある VDA は使用できない可能性があります。	ゾーン内の Cloud Connector の接続を確認し、レジストリをチェックして、レジストリによって LHC モードが強制されているかどうかを確認します。レジストリが LHC を強制していない場合は、Cloud Connector 接続チェックユーティリティを実行することを検討してください。問題が解決しない場合は、サポートチケットを開いてください。

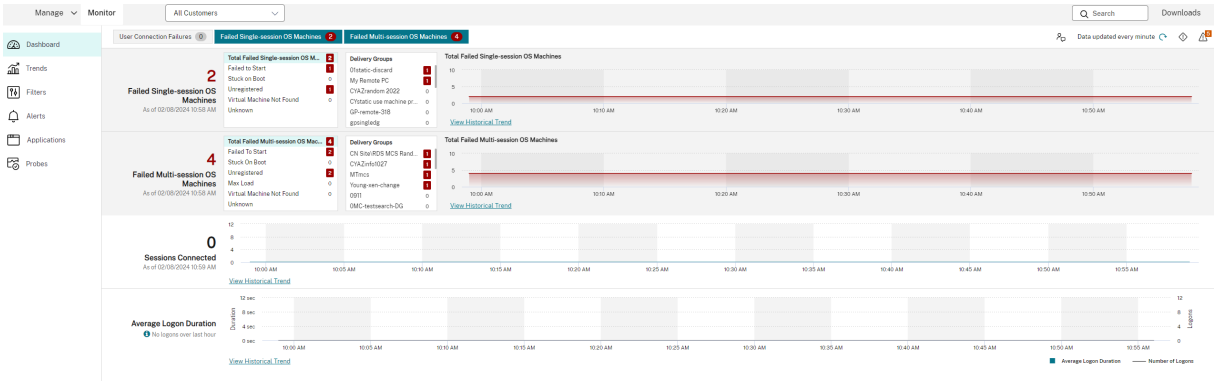
監視

February 19, 2024

管理者およびヘルプデスクのスタッフは、監視およびトラブルシューティングコンソールである ［監視］から Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）を監視できます。［監視］タブで表示されるダッシュボードでは、監視、トラブルシューティング、利用者をサポートするタスクを実行できます。

> 注:
>
> ［監視］は、Director コンソールとして使用でき、Citrix Virtual Apps and Desktops の最新リリースおよびLTSR環境で、監視およびトラブルシューティング機能を提供します。

［監視］にアクセスするには、Citrix Cloudにサインインします。左上のメニューで、［マイサービス］**>** ［**DaaS**］を選択します。［監視］をクリックします。



> 注:
>
> Citrix Monitor の表示に推奨される最適な画面解像度は 1440 × 1024 です。

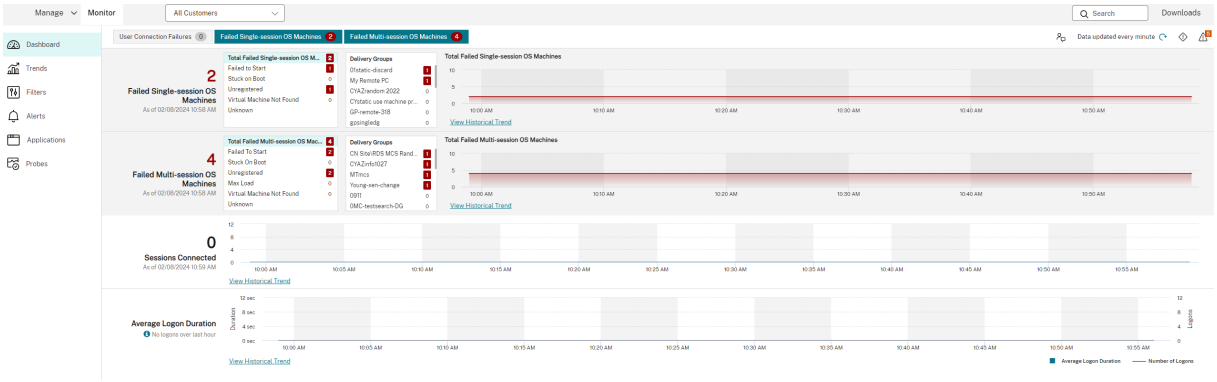
［監視］は以下の機能を提供します:

- Broker Agent からのリアルタイムデータ。Analytics および Performance Manager の機能が統合されたコンソールを使用します。
- Analytics には、ヘルスおよびキャパシティのチェック機能と履歴傾向が含まれており、Citrix DaaS 環境のネットワークによるボトルネックを検出できます。
- 監視データベースに格納される履歴データ。構成ログデータベースへのアクセスで使用されます。
- Citrix DaaS 環境の仮想アプリケーションやデスクトップを使用するエンドユーザーのユーザーエクスペリエンスを視覚化できます。
- ［監視］では、Citrix DaaS のリアルタイムおよび履歴ヘルス監視を提供するトラブルシューティングダッシュボードが使用されます。この機能により、リアルタイムで問題を確認して、エンドユーザーがどのような問題に直面しているのかを判断できるようになります。

サイト分析

March 31, 2024

［監視］ダッシュボードでは、サイトの正常性や使用状況を一元的に監視できます。



現在エラーがなく、かつ直近の 60 分間にエラーが発生していない場合、パネルは閉じたままになります。エラーが発生している場合はそのエラーを示すパネルが自動的に開きます。

パネル	説明
ユーザー接続エラー	過去 60 分間の接続エラーが表示されます。エラー総数の横にあるカテゴリをクリックして、各種のエラーのメトリックを確認します。隣接したテーブルでは、その数が各デリバリーグループに基づいてさらに分類されています。接続エラーには、アプリケーション制限に達したことによって発生したエラーも含まれます。アプリケーション制限について詳しくは、「アプリケーション」を参照してください。
失敗したシングルセッションOS マシンまたは失敗したマルチセッション OS マシン	過去 60 分間の総エラー数がデリバリーグループごとに分類されます。エラーの種類として、起動の失敗、起動時のスタック、および未登録があります。マルチセッション OS マシンの場合は、最大負荷に達しているマシンも含まれます。
接続セッション	すべてのデリバリーグループでの過去 60 分間の接続セッションが表示されます。
平均ログオン時間	過去 60 分間のログオン処理に関するデータが表示されます。左側にある大きなサイズの数値は、全体的な平均ログオン処理時間を示します。この平均には、XenDesktop 7.0 より前のバージョンの VDA へのログオンデータは含まれません。詳しくは、「ユーザーログオンの問題の診断」を参照してください。

> 注:
>
> 使用しているホストの種類が特定のメトリックをサポートしていない場合、その特定のメトリックにアイコンは表示されません。たとえば、System Center Virtual Machine Manager（SCVMM）ホスト、AWS および CloudStack のヘルス情報は表示されません。

これらのオプション（前のセクションで説明）を使用して、問題のトラブルシューティングを続けます:

- ユーザーマシンの電源の制御
- マシンへの接続の無効化

セッションの監視

セッションが切断されても、セッションはアクティブのままで、アプリケーションは引き続き実行されます。ただし、ユーザーデバイスはサーバーと通信していません。

操作	説明
ユーザーが接続しているマシンまたはセッションを表示する	［アクティビティマネージャー］および［ユーザーの詳細］ビューで、ユーザーが接続しているマシンまたはセッションを表示します。また、そのユーザーがアクセスしているすべてマシンおよびセッションの一覧を表示します。セッションの一覧にアクセスするには、そのユーザーのビューのタイトルバーにあるセッション切り替え用のアイコンをクリックします。詳しくは、「セッションの復元」を参照してください。
すべてのデリバリーグループで接続されたセッションの総数を表示する	ダッシュボードの ［接続セッション］ペインには、すべてのデリバリーグループで過去 60 分間に接続されたセッションの合計数が表示されます。次に、大きい合計数をクリックすると、［フィルター］ビューが開きます。ここでは、デリバリーグループごとのセッションデータや、すべてのデリバリーグループでの特定期間の使用状況を視覚的に確認できます。

操作	説明
アイドル状態のセッションを終了する	［セッションフィルター］ビューにすべてのアクティブなセッションの関連データが表示されます。セッションに関連付けられているユーザー、デリバリーグループ、セッション状態、しきい値の時間を超えたアイドル時間に基づいてフィルターできます。フィルターされた一覧で、ログオフまたは切断するセッションを選択します。詳しくは、「アプリケーションのトラブルシューティング」を参照してください。
長期間のデータを表示する	［傾向］ビューで、［セッション］タブを選択して、より具体的な使用状況データにドリルダウンします。長期間にわたって接続されたセッションと切断されたセッションのデータをドリルダウンできます。過去 60 分より前のセッションの合計を表示できます。この情報を表示するには、［履歴傾向の表示］をクリックします。

> 注:
>
> ユーザーデバイスが Virtual Delivery Agent 7 より前のバージョンの VDA、または Linux VDA などの古い VDA で実行されている場合、［監視］はセッションに関する完全な情報を表示できません。代わりに、利用できる情報がないというメッセージが表示されます。

デスクトップ割り当て規則の制限:

［管理］コンソールでは、さまざまなユーザーまたはユーザーグループの複数のデスクトップ割り当て規則（DAR）をデリバリーグループ内の 1 つの VDA に割り当てることができます。StoreFront は、ログインしたユーザーの DAR に従って、割り当てられたデスクトップを対応する表示名で表示します。ただし、Monitor では DAR はサポートされておらず、ログインしているユーザーに関係なく、デリバリーグループ名を使用して割り当て済みのデスクトップが表示されます。このため、Monitor で特定のデスクトップをマシンにマッピングすることはできません。

StoreFront に表示されている割り当て済みデスクトップを、Monitor に表示されているデリバリーグループ名にマッピングできます。マッピングには、次の PowerShell コマンドを使用します:

```
Get-BrokerDesktopGroup | Where-Object {
  $_.Uid -eq (Get-BrokerAssignmentPolicyRule | Where-Object {
  $_.PublishedName -eq "<Name on StoreFront>"  }
 ).DesktopGroupUid  }
  | Select-Object -Property Name, Uid
<!--NeedCopy-->
```

ブログで説明されている手順で、Remote PowerShell SDK を使用して前述の PowerShell コマンドを実行します。

アクティビティマネージャーで実行中のアプリケーションを非表示にする

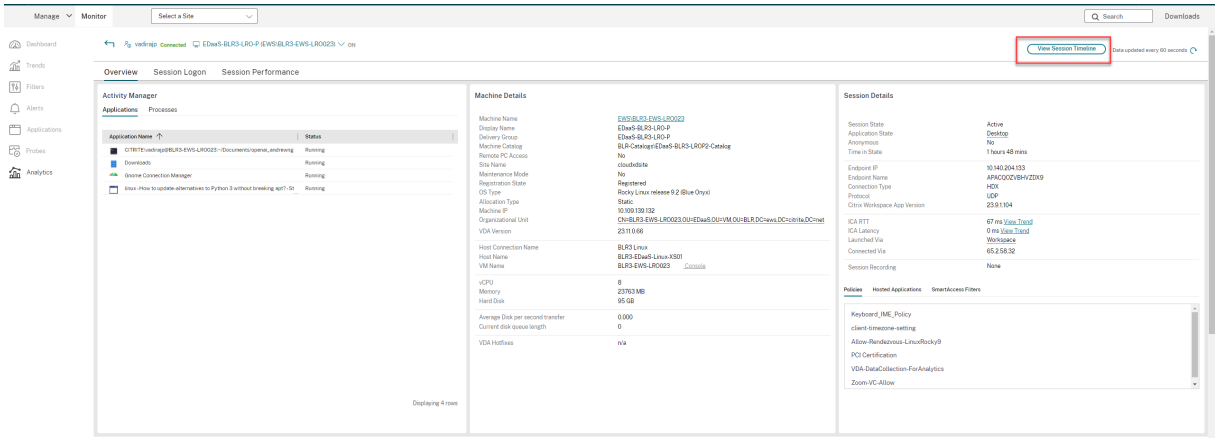
アクティビティマネージャーのデフォルトでは、そのユーザーのセッションで実行されているすべてのアプリケーションが一覧表示されます。アクティビティマネージャー機能へのアクセス権限があるすべての管理者は、この情報を表示できます。この権限を持つ管理者の役割は、すべての管理権限を実行できる管理者、デリバリーグループ管理者、およびヘルプデスク管理者です。

ユーザーのプライバシーと、ユーザーが使用しているアプリケーションを保護するために、［アプリケーション］タブでアプリケーションの一覧を非表示にできます。このためには、VDA で HKEY_LOCAL_MACHINE\Software\Citrix\Director\TaskManagerDataDisplayed のレジストリキーを編集します。デフォルトでは 1 に設定されています。値を 0 に変更すると、VDA から情報が収集されなくなるため、アクティビティマネージャーに情報が表示されなくなります。

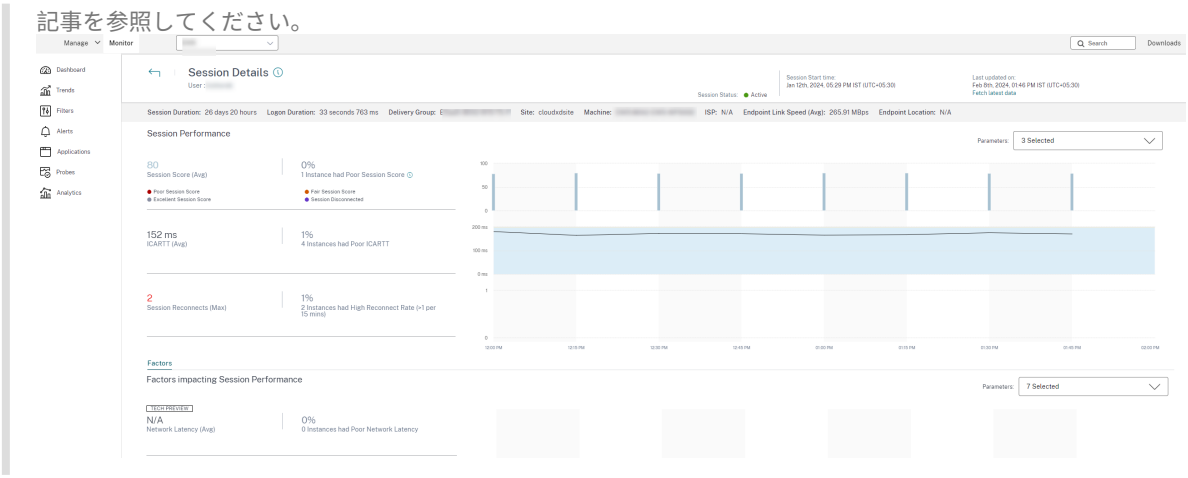
> 警告:
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix は一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

Citrix Analytics for Performance - Session Details へのアクセス

［監視］から Citrix Analytics for Performance の［Session Details］ページにアクセスできます。アクティビティマネージャーの［セッション詳細］セクションで［セッションタイムラインの表示］をクリックすると、［監視］内で Citrix Analytics for Performance の［Session Details］ページが開きます。



> 注:
>
> この機能を使用するには、有効な Citrix Analytics for Performance の使用権が必要です。
>
> ［Session Details］は、Citrix Analytics for Performance の［Excellent］、［Fair］、または［Poor］に分類されたセッションで使用できます。セッションが分類されない理由について詳しくは、「分類されていない」の

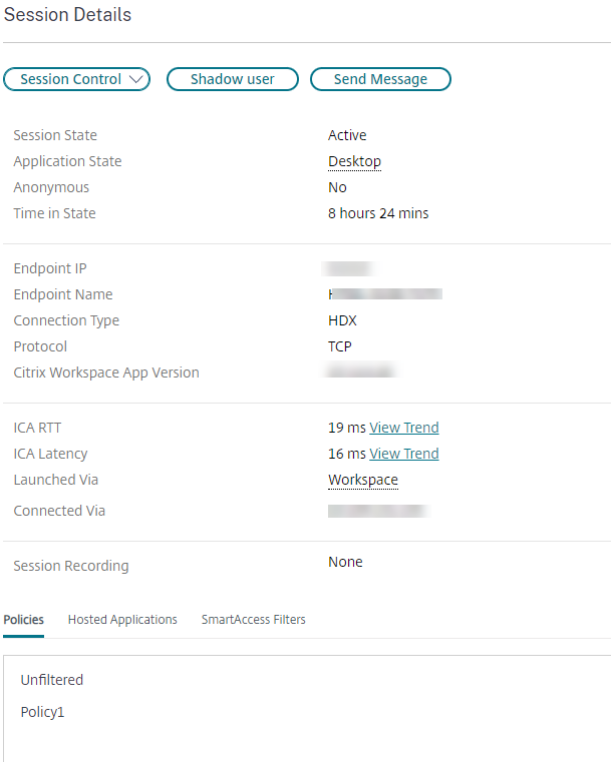


過去 3 日間のセッションのセッションエクスペリエンスの傾向を確認できます。この傾向のビューには、セッションエクスペリエンスの要因も含まれます。この情報は、ヘルプデスク管理者がセッションエクスペリエンス関連の問題のトラブルシューティング中に使用するライブデータ（[監視] で利用可能）を補足します。

[Session Details] ページについて詳しくは、「セッション詳細」を参照してください。

セッショントランスポートプロトコル

[セッション詳細] パネルで、現在のセッションの HDX 接続タイプに使用されているトランスポートプロトコルを表示します。この情報はバージョン 7.13 以降の VDA で起動するセッションで利用できます。



［セッション詳細］ペインの ［セッション制御］ドロップダウンメニューを使用して、セッションをログオフまたは切断します。

- **HDX** 接続の種類の場合、
  - EDT が HDX 接続に使用されている場合、プロトコルは **UDP** と表示されます。
  - TCP が HDX 接続に使用されている場合、プロトコルは **TCP** と表示されます。
- **RDP** 接続の種類の場合、プロトコルは「該当なし」と表示されます。

アダプティブトランスポートが構成されている場合、セッショントランスポートプロトコルは、ネットワーク条件に応じて、EDT（UDP 上）と TCP を動的に切り替えます。HDX セッションを EDT で確立できない場合は、TCP プロトコルにフォールバックします。

アダプティブトランスポート構成について詳しくは、「アダプティブトランスポート」を参照してください。

レポートのエクスポート

傾向データをエクスポートして、通常使用レポートおよび能力管理レポートを生成できます。エクスポートでは、PDF、Excel、および CSV レポート形式がサポートされます。PDF と Excel 形式のレポートには、傾向がグラフとテーブルとして表示されます。CSV 形式のレポートには、ビューの生成やアーカイブに使用できる表形式のデータが含まれています。

レポートをエクスポートするには、次の手順に従います。

1. ［傾向］タブに移動します。
2. フィルターの基準と期間を設定し、［適用］をクリックします。傾向グラフとテーブルにデータが入力されます。
3. ［エクスポート］をクリックして、レポートの名前と形式を入力します。

［監視］は、選択したフィルター基準に基づいてレポートを生成します。フィルター基準を変更した場合は、［適用］をクリックしてから ［エクスポート］をクリックします。

> 注:
>
> 大量のデータをエクスポートすると、監視サーバー、Delivery Controller および SQL サーバーのメモリと CPU の消費が著しく増加します。サポートされる同時エクスポート処理の数とエクスポートできるデータの量は、エクスポートのパフォーマンスを最適にするため、デフォルトの上限に設定されています。

サポートされるエクスポート上限

エクスポートされる PDF と Excel のレポートは、選択されたフィルター基準によるグラフィカルなチャートが含まれています。ただし、すべてのレポート形式の表形式のデータは、行の数またはテーブルのレコード数のデフォルト値を超えた値は切り捨てられています。サポートされるデフォルトのレコード数は、レポート形式に基づいて定義されます。

VHD 形式	サポートされるデフォルトのレコード数
PDF	500
Excel	100,000
CSV	100,000（[セッション］タブで 10,000,000）

Error Handling

エクスポート処理中に発生する可能性があるエラー：

- **Director** のタイムアウト：このエラーは、Director サーバーでの、または Monitor Service によるネットワーク問題や高いリソース使用率によって発生することがあります。
- 監視のタイムアウト：このエラーは、Monitor Service による、または SQL サーバーでのネットワーク問題や高いリソース使用率によって発生する可能性があります。
- 同時エクスポートまたはプレビュー処理上限：特定の期間にエクスポートまたはプレビューを実行できるインスタンスは 1 つだけです。同時エクスポートまたはプレビュー処理上限エラーが発生した場合は、次の処理を後で実行してください。

Hotfix の監視

特定のマシンの VDA（物理または仮想）にインストールされている Hotfix を確認するには、［マシンの詳細］ビューを選択します。

ユーザーマシンの電源状態の制御

監視で選択したマシンの電源の状態を制御するには、［電源制御］オプションを使用します。これらのオプションはシングルセッション OS マシンに対して実行できますが、マルチセッション OS マシンに対しては使用できないことがあります。

> 注：
>
> この機能は、物理マシンまたはリモート PC アクセスを使用しているマシンに対しては使用できません。

コマンド	機能
再起動	仮想マシン上のすべてのプロセスを停止して、通常の再起動処理（ソフト再起動）を実行します。たとえば、起動に失敗したマシンを再起動するときにこのコマンドを使用します。
強制再起動	通常のシャットダウン処理を行わずに強制的に仮想マシンを再起動します。これは、物理サーバーの電源プラグを抜いてから電源を入れるのと同等の操作です。
シャットダウン	仮想マシンの正常な（ソフト）シャットダウンを実行します。実行中のプロセスはすべて個別に停止されます。
強制シャットダウン	通常のシャットダウン処理を行わずに強制的に仮想マシンをシャットダウンします。物理サーバーの電源プラグを抜くのと同等の操作です。実行中のプロセスを正しく停止できない場合があるため、この方法で仮想マシンをシャットダウンするとデータが失われる可能性があります。
一時停止	仮想マシンを一時停止して、そのときの状態をデフォルトのストレージリポジトリ上にファイルとして保存します。この方法で仮想マシンを一時停止してからそのホストサーバーをシャットダウンし、ホストサーバーを再起動してから仮想マシンを元の実行状態に戻すことができます。
再開	一時停止状態の仮想マシンを再開して、元の実行状態に戻します。
起動	シャットダウン状態の仮想マシンを起動します（「コールドスタート」とも呼ばれます）。

電源制御操作に失敗した場合、アラート上にマウスポインターを置くと問題の詳細情報がポップアップメッセージとして表示されます。

マシンへの接続の無効化

メンテナンスモードでは、管理者がイメージの保守作業を行っている間、一時的にユーザーが接続できなくなります。

マシンをメンテナンスモードにすると、メンテナンスモードを解除するまでそのマシンへの接続が禁止されます。そのマシンにユーザーがログオンしている場合は、すべてのユーザーがログオフした後でメンテナンスモードに切り替わります。ユーザーのログオフを促すために、マシンのシャットダウンを通知するメッセージをユーザーに送信できます。電源制御機能を使って強制的にマシンをシャットダウンできます。

1. ［ユーザーの詳細］ビューなどからマシンを選択するか、［フィルター］ビューでマシンのグループを選択します。
2. ［メンテナンスモード］を選択し、オプションをオンにします。

メンテナンスモードの割り当て済みデスクトップにユーザーが接続を試みると、デスクトップを使用できないことを示すメッセージが表示されます。管理者がメンテナンスモードを解除するまで、新しい接続は許可されません。

アプリケーション分析

［アプリケーション］タブには、アプリケーションのパフォーマンスを効率的に分析および管理するのに役立つアプリケーションごとの分析結果が、単一の統合ビューで表示されます。サイトに公開されているすべてのアプリケーションの正常性および使用状況に関する情報について貴重な分析情報を得ることができます。次のようなメトリックが表示されます：

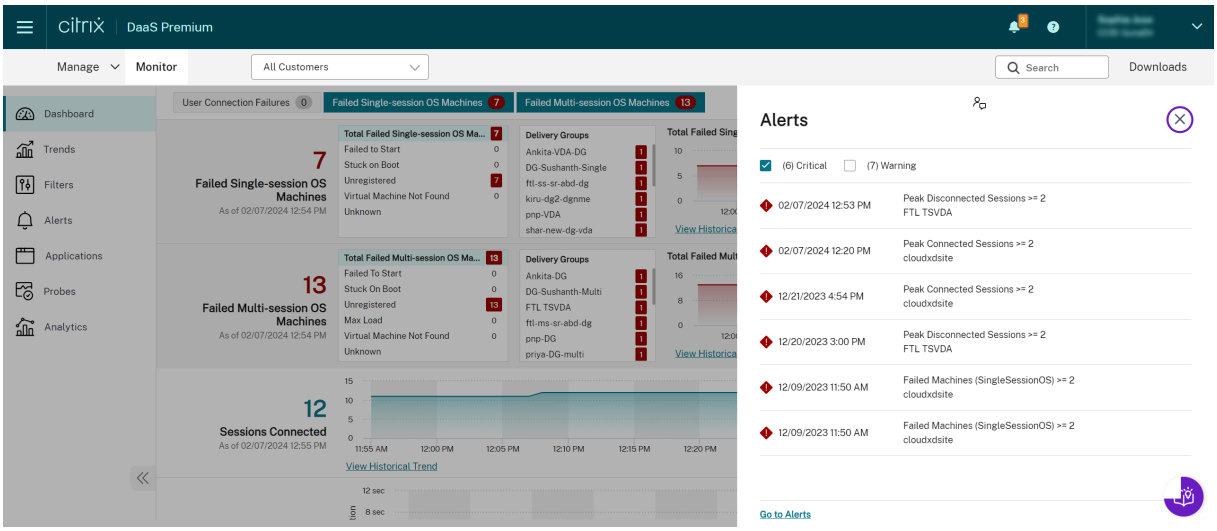
- プローブの結果
- アプリケーションごとのインスタンス数
- 公開アプリケーションに関連する障害およびエラー

詳しくは、「アプリケーションのトラブルシューティング」の「アプリケーションの分析」セクションを参照してください。

アラートおよび通知

February 19, 2024

アラートは、ダッシュボードの監視およびそのほかの概要ビューに、警告および重大アラートシンボルと共に表示されます。アラートは、1 分ごとに自動的に更新されます。オンデマンドで更新することもできます。

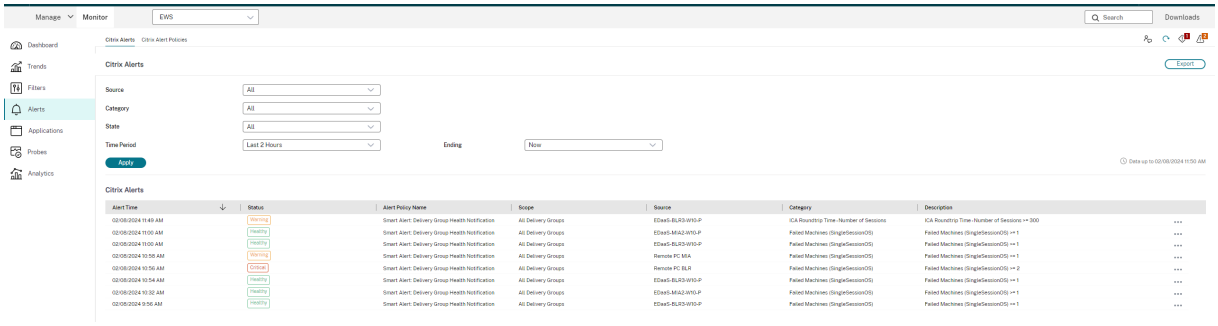


警告アラート（黄色の三角形）は、条件の警告しきい値以上になっていることを示します。

重大アラート（赤の円）は、条件の重大しきい値以上になっていることを示します。

サイドバーでアラートを選択して下部にある ［アラートに移動］リンクをクリックするか、［監視］ページの上部にある ［アラート］を選択すると、アラートに関するさらに詳細な情報を表示できます。

［アラート］ビューで、アラートをフィルターおよびエクスポートできます。たとえば、先月特定のデリバリーグループで失敗したマルチセッション OS マシンや、特定のユーザーに対するすべてのアラートを特定することができます。詳しくは、「レポートのエクスポート」を参照してください。



Citrix アラート

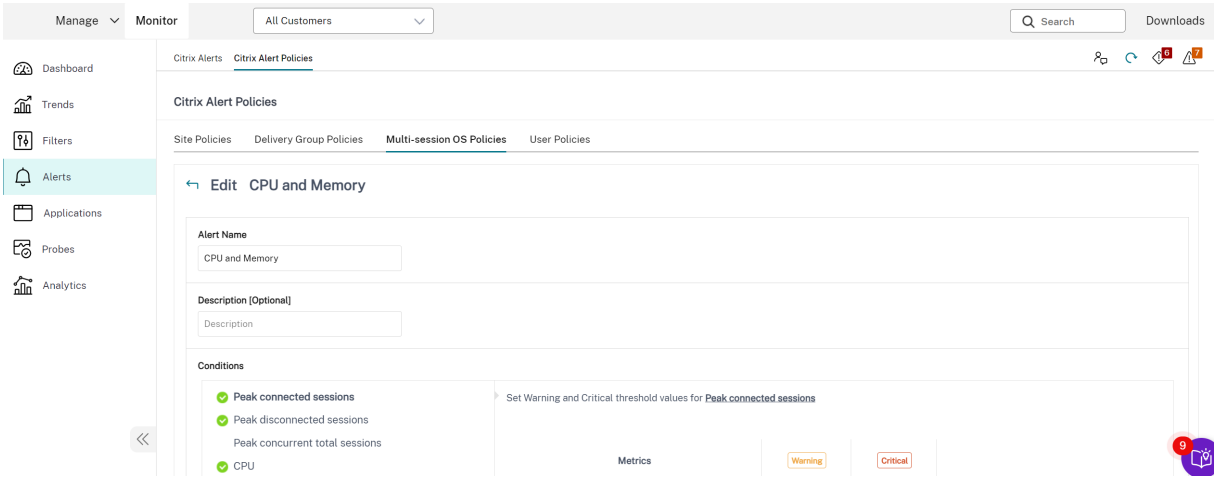
Citrix アラートは、Citrix コンポーネントで発生するアラートです。Citrix アラートは、［監視］内で ［アラート］> [**Citrix** アラートポリシー］の順に選択して構成できます。この構成では、設定したしきい値を超過した場合のアラートに関して、ユーザーおよびグループにメール送信する通知を設定できます。Citrix アラートのセットアップについて詳しくは、「アラートポリシーの作成」を参照してください。

スマートアラートポリシー

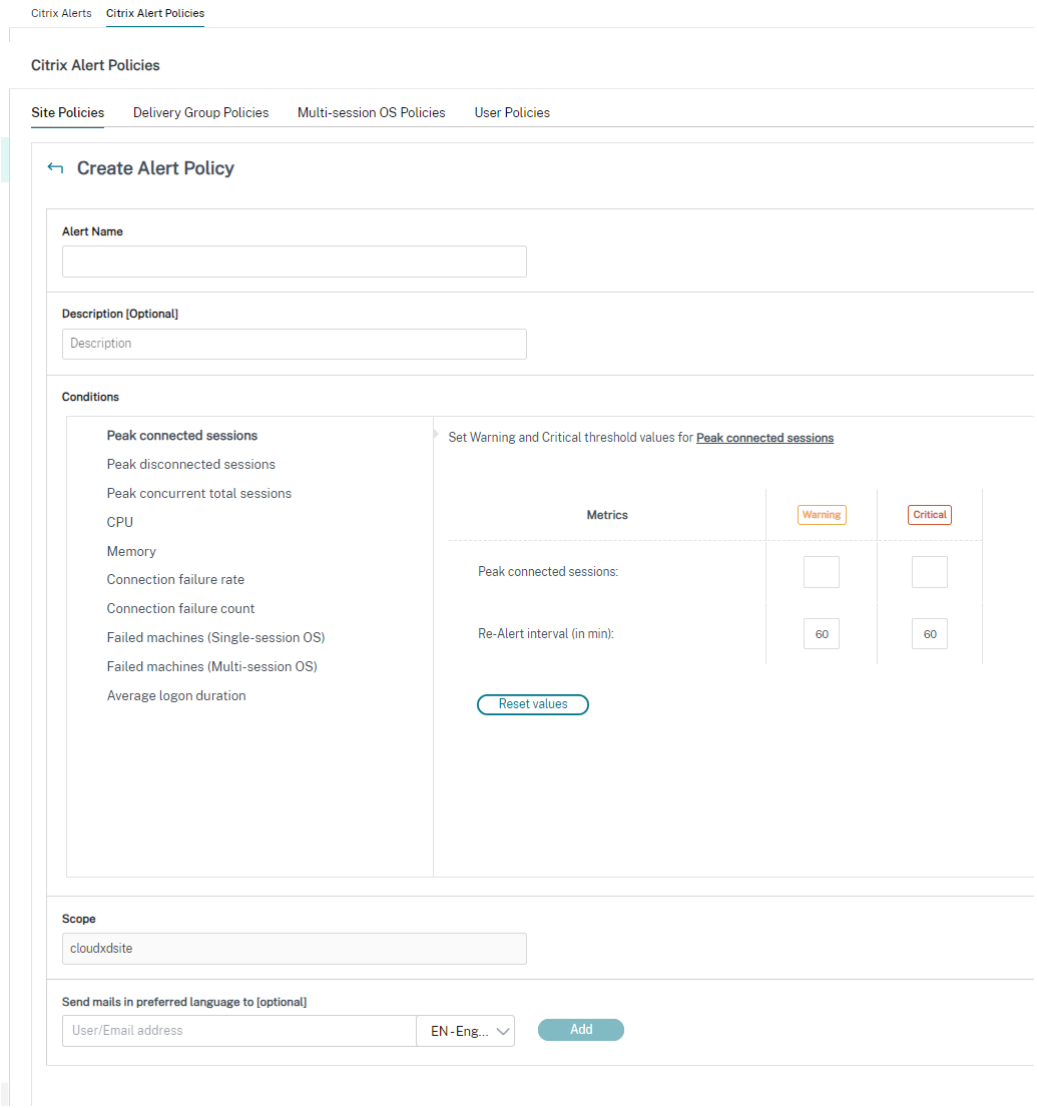
定義済みのしきい値を持つ組み込みアラートポリシーのセットは、デリバリーグループおよびマルチセッション OS VDA スコープで使用できます。［アラート］> [**Citrix** アラートポリシー］で、組み込みアラートポリシーのしきい値パラメーターを変更できます。
これらのポリシーは、少なくとも 1 つのアラートターゲット（サイト内に定義されているデリバリーグループまたはマルチセッション OS VDA）が存在する場合に作成されます。さらに、これらの組み込みアラートは、新しいデリバリーグループまたはマルチセッション OS VDA に自動的に追加されます。

対応するアラートルールが監視データベースに存在しない場合にのみ、組み込みアラートポリシーが作成されます。

組み込みアラートポリシーのしきい値については、「アラートポリシーの条件」を参照してください。



アラートポリシーの作成



特定のセッション数基準のセットを満たした場合にアラートを生成するなどの目的で、新しいアラートポリシーを作成するには、以下の手順に従います:

1. [アラート] > [**Citrix** アラートポリシー] の順に選択し、[マルチセッション OS ポリシー] などを選択します。
2. [作成] をクリックします。
3. ポリシーの名前と説明を入力し、アラートをトリガーするために満たす必要がある条件を設定します。たとえば、最大接続済みセッション数、最大切断セッション数、および最大同時セッション数に対して、警告とする数および重大とする数を指定します。警告値を重大値よりも大きくすることはできません。詳しくは、「アラートポリシーの条件」を参照してください。
4. 再アラート間隔を設定します。アラートの条件が引き続き満たされている場合、アラートはこの間隔で再トリガーされます。アラートポリシーで設定されている場合は、メール通知が生成されます。クリアされたアラートの場合、再アラート間隔でメール通知が生成されることはありません。

5. スコープを設定します。たとえば、特定のデリバリーグループに対して設定します。
6. お知らせ設定で、アラートがトリガーされたときのメール通知の送信先を指定します。メール通知は SendGrid で送信されます。メールアドレスdonotreplynotifications@citrix.comがメール設定で許可リストに登録されていることを確認してください。
7. [保存] をクリックします。

スコープに 20 件以上のデリバリーグループが定義されているポリシーを作成すると、構成が完了するまでにおよそ 30 秒かかる場合があります。完了するまで、スピナーアイコンが表示されます。

最大 20 の一意のデリバリーグループに対して、50 以上のポリシー（合計で 1000 デリバリーグループターゲット）を作成すると、応答時間が遅くなることがあります（5 秒以上）。

アクティブなセッションがあるマシンをデリバリーグループから別のデリバリーグループに移動すると、マシンパラメーターで定義されたデリバリーグループアラートが誤って発信されることがあります。

> 注:
> アラートポリシーを削除した後、ポリシーによって生成されたアラート通知が停止するまでに最大 30 分かかる場合があります。

アラートポリシーの条件

アラートカテゴリ、アラートを緩和するための推奨アクション、および定義されている場合は組み込みポリシーの条件を以下に示します。組み込みアラートポリシーは、60 分のアラートおよび再アラートの間隔で定義されています。

最大切断セッション数

- [監視] のセッション傾向ビューで、最大接続済みセッション数をチェックします。
- セッションの負荷に対応するのに十分な処理能力があることを確認します。
- 必要に応じ、マシンを追加します。

最大切断セッション数

- [監視] のセッション傾向ビューで、最大切断セッション数をチェックします。
- セッションの負荷に対応するのに十分な処理能力があることを確認します。
- 必要に応じ、マシンを追加します。
- 必要に応じ、切断されたセッションからログオフします。

合計最大同時セッション数

- [監視] のセッション傾向ビューで、最大同時セッション数をチェックします。

- セッションの負荷に対応するのに十分な処理能力があることを確認します。
- 必要に応じ、マシンを追加します。
- 必要に応じ、切断されたセッションからログオフします。

CPU

CPU 使用率は、プロセスも含めた VDA の全体的な CPU の消費を示します。関連 VDA の ［マシンの詳細］ページで個別のプロセスによる CPU 使用率に関する情報を表示できます。

- ［マシンの詳細］**>**［履歴使用率の表示］**>**［上位 **10** 位のプロセス］に移動して、CPU を消費しているプロセスを確認します。プロセス監視ポリシーが有効になっていることを確認して、プロセスレベルのリソース使用統計の収集を開始します。
- 必要に応じてプロセスを終了します。
- プロセスを終了すると、保存されていないデータは失われます。
- すべてが想定どおりに機能している場合は、将来的に CPU リソースを追加します。

  > 注:
  >
  > ポリシー設定 ［リソースの監視を有効にします］はデフォルトで有効で、VDA がインストールされているマシンの CPU とメモリパフォーマンスカウンターを監視できます。このポリシー設定が無効にされると、CPU とメモリの条件に関するアラートはトリガーされません。詳しくは、「監視のポリシー設定」を参照してください。

  スマートポリシーの条件:

  - スコープ: デリバリーグループ、マルチセッション OS スコープ
  - しきい値: 警告 - 80%、重大 - 90%

メモリ

メモリ使用率は、プロセスも含めた VDA の全体的なメモリの消費を示します。関連 VDA の ［マシンの詳細］ページで個別のプロセスによるメモリ使用率に関する情報を表示できます。

- ［マシンの詳細］**>**［履歴使用率の表示］**>**［上位 **10** 位のプロセス］に移動して、メモリを消費しているプロセスを確認します。プロセス監視ポリシーが有効になっていることを確認して、プロセスレベルのリソース使用統計の収集を開始します。
- 必要に応じてプロセスを終了します。
- プロセスを終了すると、保存されていないデータは失われます。
- すべてが想定どおりに機能している場合は、将来的にメモリを追加します。

> 注:
>
> ポリシー設定 ［リソースの監視を有効にします］はデフォルトで有効で、VDA がインストールされているマシンの CPU とメモリパフォーマンスカウンターを監視できます。このポリシー設定が無効にされると、CPU とメモリの条件に関するアラートはトリガーされません。詳しくは、「監視のポリシー設定」を参照してください。

スマートポリシーの条件:

- スコープ: デリバリーグループ、マルチセッション OS スコープ
- しきい値: 警告 - 80%、重大 - 90%

接続エラー率

過去 1 時間の接続エラーの率。

- 接続の合計試行回数に対する合計エラー数の割合に基づいて計算されます。
- ［監視］の接続エラーの傾向ビューで、構成ログから記録されたイベントをチェックします。
- アプリケーションまたはデスクトップにアクセスできるかどうかを確認します。

接続エラー数

過去 1 時間の接続エラー数。

- ［監視］の接続エラーの傾向ビューで、構成ログから記録されたイベントをチェックします。
- アプリケーションまたはデスクトップにアクセスできるかどうかを確認します。

ICA 往復時間（平均）

平均 ICA 往復時間

- Citrix ADM で ICA RTT のブレークダウンをチェックして、原因を特定します。詳しくは、Citrix ADMのドキュメントを参照してください。
- Citrix ADM が利用可能でない場合は、［監視］の［ユーザーの詳細］ビューで ICA RTT および遅延をチェックして、これがネットワークの問題か、それともアプリケーションやデスクトップの問題かを特定します。

ICA 往復時間（セッション数）

ICA 往復時間を超過しているセッションの数。

- Citrix ADM で、ICA RTT が高いセッションの数をチェックします。詳しくは、Citrix ADMのドキュメントを参照してください。

- Citrix ADM を利用できない場合は、ネットワークチームと協力して原因を特定してください。

  スマートポリシーの条件:

  - スコープ: デリバリーグループ、マルチセッション OS スコープ
  - しきい値: 警告 - 5 つ以上のセッションで 300ms、重大 - 10 以上のセッションで 400ms

ICA 往復時間（セッションの**%**）

平均 ICA 往復時間を超過しているセッションの割合。

- Citrix ADM で、ICA RTT が高いセッションの数をチェックします。詳しくは、Citrix ADMのドキュメントを参照してください。
- Citrix ADM を利用できない場合は、ネットワークチームと協力して原因を特定してください。

ICA RTT（ユーザー）

特定のユーザーによって開始されたセッションに適用された ICA 往復時間。1 つ以上のセッションで ICA RTT がしきい値よりも高い場合は、アラートがトリガーされます。

障害が発生したマシン（シングルセッション **OS**）

失敗したシングルセッション OS マシンの数。[監視] ダッシュボードビューおよび [フィルター] ビューに表示されるように、エラーはさまざまな理由で発生します。

- Citrix Scout 診断を実行して、原因を特定します。詳しくは、「ユーザーの問題のトラブルシューティング」を参照してください。

  スマートポリシーの条件:

  - スコープ: デリバリーグループスコープ
  - しきい値: 警告 - 1、重大 - 2

障害が発生したマシン（マルチセッション **OS**）

失敗したマルチセッション OS マシンの数。[監視] ダッシュボードビューおよび [フィルター] ビューに表示されるように、エラーはさまざまな理由で発生します。

- Citrix Scout 診断を実行して、原因を特定します。

  スマートポリシーの条件:

  - スコープ: デリバリーグループ、マルチセッション OS スコープ
  - しきい値: 警告 - 1、重大 - 2

障害が発生したマシン（**%**）

障害が発生したマシンの数に基づいて計算された、デリバリーグループ内の障害が発生したシングルセッションおよびマルチセッション OS マシンの割合。アラートの条件を設定する際、アラートのしきい値をデリバリーグループ内の障害が発生したマシンの割合で構成できます。この条件は 30 秒ごとに計算されます。
Director の［ダッシュボード］ビューおよび［フィルター］ビューに表示されるように、失敗はさまざまな理由で発生することがあります。Citrix Scout 診断を実行して、原因を特定します。詳しくは、「ユーザーの問題のトラブルシューティング」を参照してください。

平均ログオン時間

過去 1 時間に行われたログオンの平均ログオン処理時間。

- ［監視］ダッシュボードをチェックし、ログオン処理時間に関する最新のメトリックを取得します。短時間のうちに多数のユーザーがログインするとログオン処理時間が長引くことがあります。
- 原因を絞り込むため、ログオンのベースラインおよび内訳をチェックします。詳しくは、「ユーザーログオンの問題の診断」を参照してください。

  スマートポリシーの条件：

  - スコープ：デリバリーグループ、マルチセッション OS スコープ
  - しきい値：警告 - 45 秒、重大 - 60 秒

ログオン処理時間（ユーザー）

過去 1 時間に行われた指定されたユーザーのログオンに関するログオン処理時間。

負荷評価基準インデックス

過去 5 分間の負荷評価基準インデックスの値。

- ［監視］で、ピーク負荷（最大負荷）に達している可能性があるマルチセッション OS マシンをチェックします。ダッシュボード（失敗）および負荷評価基準インデックス傾向レポートを表示します。

  スマートポリシーの条件：

  - スコープ：デリバリーグループ、マルチセッション OS スコープ
  - しきい値：警告 - 80%、重大 - 90%

ハイパーバイザーアラートの監視

［監視］では、ハイパーバイザーの正常性を監視するアラートが表示されます。Citrix Hypervisor と VMware vSphere のアラートは、ハイパーバイザーのパラメーターと状態を監視するのに役立ちます。ハイパーバイザーへの接続状態も監視され、クラスターまたはホストのプールが再起動された場合、または使用できなくなった場合にアラートが出されます。

ハイパーバイザーアラートを受信するには、［管理］タブでホスト接続が作成されている必要があります。詳しくは、「接続およびリソース」を参照してください。ハイパーバイザーアラートではこれらの接続のみが監視されます。次の表に、ハイパーバイザーアラートのさまざまなパラメーターと状態を示します。

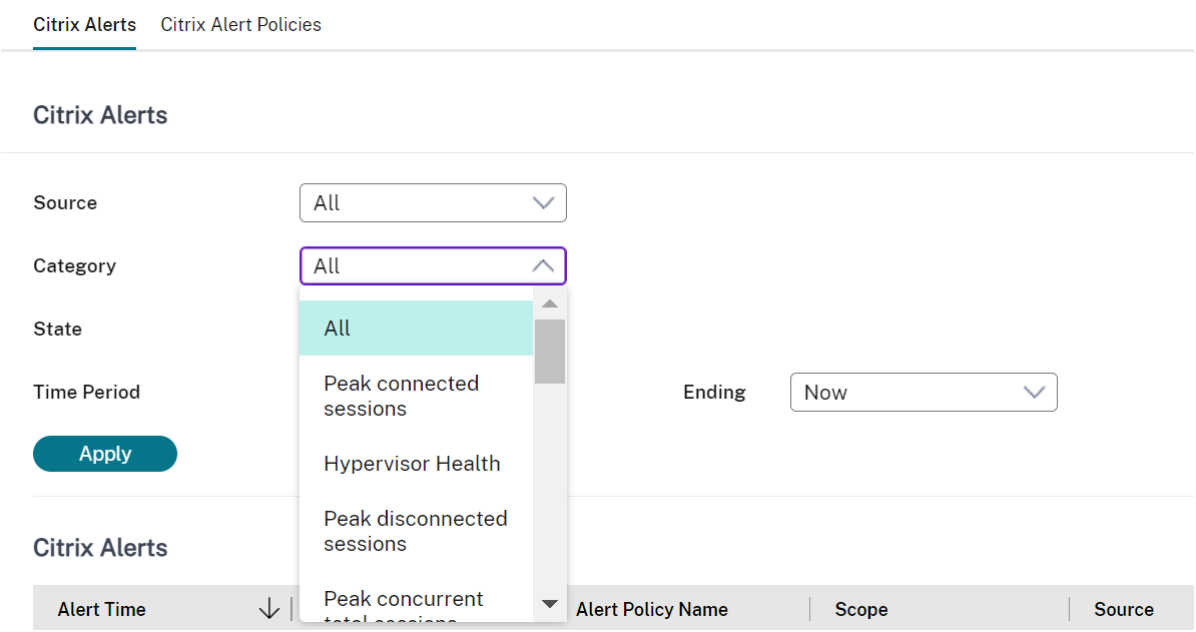
通知	サポートされるハイパーバイザー	トリガー元	条件	構成
CPU 使用率	Citrix Hypervisor、VMware vSphere	ハイパーバイザー	CPU 使用率アラートしきい値に達しているか、超過している	アラートしきい値は、ハイパーバイザーで設定する必要があります。
メモリ使用率	Citrix Hypervisor、VMware vSphere	ハイパーバイザー	メモリ使用率アラートしきい値に達しているか、超過している	アラートしきい値は、ハイパーバイザーで設定する必要があります。
ネットワーク使用状況	Citrix Hypervisor、VMware vSphere	ハイパーバイザー	ネットワーク使用率アラートしきい値に達しているか、超過している	アラートしきい値は、ハイパーバイザーで設定する必要があります。
ディスク使用率	VMware vSphere	ハイパーバイザー	ディスク使用率アラートしきい値に達しているか、超過している	アラートしきい値は、ハイパーバイザーで設定する必要があります。
ホスト接続や電源の状態	VMware vSphere	ハイパーバイザー	ハイパーバイザーホストが再起動されたか、または利用できない	アラートは VMware vSphere にあらかじめ組み込まれています。追加の構成は必要ありません。

通知	サポートされるハイパーバイザー	トリガー元	条件	構成
使用不可のハイパーバイザー接続	Citrix Hypervisor、VMware vSphere	Delivery Controller	ハイパーバイザー（プールまたはクラスター）への接続が失われるか、電源がオフになるか、再起動されます。このアラートは、接続が利用できない間、1 時間ごとに生成されます。	アラートは Delivery Controller にあらかじめ組み込まれています。追加の構成は必要ありません。

> 注:
>
> アラートの構成について詳しくは、「Citrix XenCenter アラート」を参照するか、VMware vCenter アラートのドキュメントを確認してください。

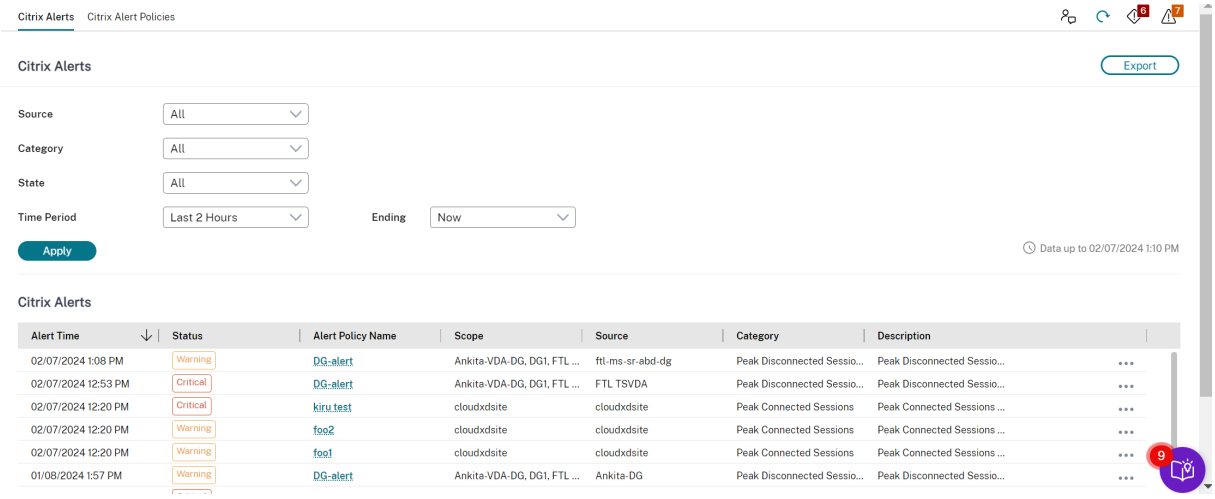
メール通知設定は、［**Citrix** アラートポリシー］**>**［サイトポリシー］**>**［ハイパーバイザーの正常性］から設定できます。Hypervisor のアラートポリシーのしきい値条件は、［監視］からではなくハイパーバイザーからのみ設定、編集、無効化、または削除できます。ただし、メール設定の変更とアラートの解除は［監視］で行うことができます。

> 重要:
>
> - 2 日以上経過したハイパーバイザー通知は、すべて自動的に破棄されます。
> - アラートは Hypervisor により取得され、［監視］に表示されます。ただし、Hypervisor のアラートのライフサイクルや状態に対する変更は、［監視］には反映されません。
> - 正常状態のアラートや Hypervisor コンソールで破棄または無効化したアラートであっても、［監視］には表示され続けるため、Director で明示的に破棄する必要があります。
> - アラートを［監視］で破棄しても、Hypervisor コンソールで自動的に破棄されることはありません。



ハイパーバイザーアラートのみをフィルタリングできるように、「ハイパーバイザーの正常性」という新しいアラートカテゴリが追加されました。これらのアラートは、しきい値に達するか超過すると表示されます。ハイパーバイザーのアラートには次のものがあります:

- 重大—ハイパーバイザーアラームポリシーの重大しきい値に達したか超過した
- 警告—ハイパーバイザーアラームポリシーの警告しきい値に達したか超過した
- 解除—アラートはアクティブなアラートとして表示されなくなる

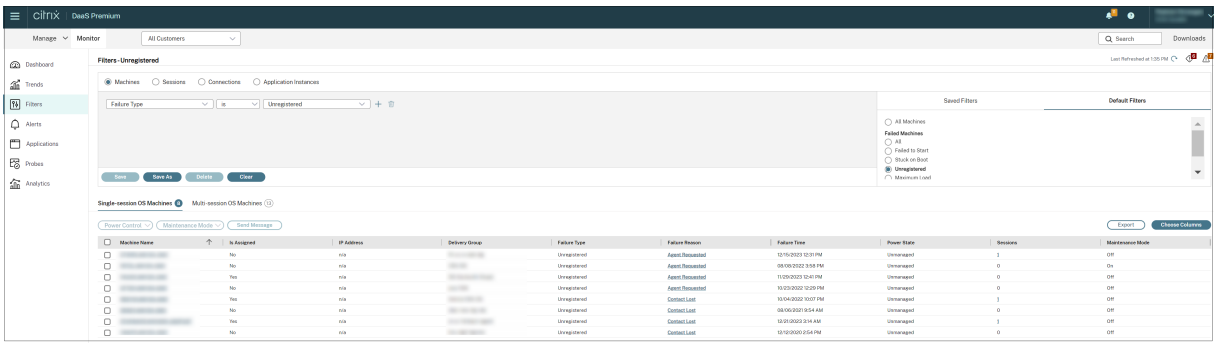


トラブルシューティングのためのデータのフィルター処理

August 18, 2023

［ダッシュボード］で数値をクリックしたり ［フィルター］タブから事前定義のデフォルトのフィルターを選択したりすると、［フィルター］ビューが開きます。ここには、選択したマシンまたはエラーの種類に関するデータが表示されます。

すべてのデリバリーグループのマシン、接続、セッション、アプリケーションインスタンスのカスタムフィルタービューを作成して、後でアクセスしやすいように保存できます。事前定義のフィルターを編集して、［保存済み］フィルターとして保存できます。



1. 以下のビューを選択します。

    - マシン。シングルセッションOS マシンまたはマルチセッション OS マシンを選択します。これらのタブには構成されたマシンの数が表示されます。また、［マルチセッション OS マシン］タブには負荷評価基準インデックスが表示され、その測定値上にマウスポインターを置くと各パフォーマンスカウンターの測定値やセッション数がツールチップとして表示されます。
    - セッション。［セッション］ビューでセッション数を表示することもできます。アイドル時間の測定値から、しきい値時間を超えてアイドル状態にあるセッションを特定できます。［**Associated User**］をクリックすると、ユーザーのアクティビティマネージャーが開きます。エンドポイントの名前をクリックすると、エンドポイントのアクティビティマネージャーが開きます。各場合に［詳細の表示］をクリックすると、［ユーザーの詳細］ページまたは ［エンドポイント詳細］ページが開きます。詳しくは、［ユーザーの詳細］を参照してください。
    - 接続。直近の 60 分、24 時間、または 7 日間の接続が表示されます。
    - アプリケーションインスタンス。このビューは、マルチセッションおよびシングルセッション OS VDA 上におけるすべてのアプリケーションインスタンスのプロパティを表示します。セッションのアイドル時間測定機能は、マルチセッション OS 対応 VDA のアプリケーションインスタンスに利用できます。

2. ［保存済み］または［デフォルト］のフィルターの一覧からフィルターを選択します。
3. ドロップダウンリストを使用して、さらにフィルター基準を選択します。
4. 必要に応じて追加の列を選択して、より詳細な情報を表示します。
5. フィルターに名前を付けて保存します。
6. 後でフィルターを開くには、［フィルター］ビューで［表示］（マシン、セッション、接続、またはアプリケーションインスタンス）を選択し、［保存済み］フィルターを選択します。

7. データを CSV 形式のファイルにエクスポートするには、［エクスポート］をクリックします。最大 100,000 レコードのデータをエクスポートできます。
8. ［マシン］ビューまたは ［接続］ビューでは、必要に応じ一覧でマシンを選択して電源制御操作を実行できます。［セッション］ビューでは、セッション制御を実行したりメッセージを送信したりできます。
9. ［マシン］ビューおよび ［接続］ビューで障害が発生したマシンまたは接続の ［エラーの理由］をクリックすると、障害の詳細な説明と、障害をトラブルシューティングするために推奨される操作が表示されます。マシンおよび接続でエラーが発生した場合のエラーの理由と推奨される解決手順は、『Citrix Director Failure Reasons Troubleshooting Guide』に記載されています。
10. ［マシン］ビューでマシン名のリンクをクリックすると、対応する ［マシンの詳細］ページが開きます。マシンの詳細を表示するこのページでは、電源制御が提供され、CPU、メモリ、ディスクの監視、および GPU の監視グラフが表示されます。また、［履歴使用率の表示］をクリックすると、マシンのリソース使用傾向が表示されます。詳しくは、「マシンのトラブルシューティング」を参照してください。
11. ［アプリケーションインスタンス］ビューでは、しきい値時間を超えた ［アイドル時間］に基づいてソートまたはフィルターできます。終了させるアイドル状態のアプリケーションインスタンスを選択します。ログオフまたはアプリケーションインスタンスを切断すると同一セッション内のすべてのアクティブなアプリケーションインスタンスが終了します。詳しくは、「アプリケーションのトラブルシューティング」を参照してください。アプリケーションインスタンスのフィルターページと、セッションのフィルターページにあるアイドル時間の測定値は、VDA のバージョンが 7.13 以降である場合に使用可能です。

> 注:
>
> ［管理］コンソールでは、さまざまなユーザーまたはユーザーグループの複数のデスクトップ割り当て規則（DAR）をデリバリーグループ内の 1 つの VDA に割り当てることができます。StoreFront は、ログインしたユーザーの DAR に従って、割り当てられたデスクトップを対応する表示名で表示します。ただし、［監視］では DAR はサポートされておらず、ログインしているユーザーに関係なく、デリバリーグループ名を使用して割り当て済みのデスクトップが表示されます。このため、［監視］で特定のデスクトップをマシンにマッピングすることはできません。StoreFront に表示されている割り当て済みデスクトップを［監視］に表示されているデリバリーグループ名にマッピングするには、次の PowerShell コマンドを使用します。ブログで説明されている手順で、Remote PowerShell SDK を使用して PowerShell コマンドを実行します。

```
Get-BrokerDesktopGroup | Where-Object {
  $\_.Uid -eq (Get-BrokerAssignmentPolicyRule | Where-Object {
  $\_.PublishedName -eq "<Name on StoreFront>"  }
 ).DesktopGroupUid  }
  | Select-Object -Property Name, Uid
<!--NeedCopy-->
```


サイト全体の履歴傾向の監視

January 25, 2024

［傾向］ビューでは、次のパラメーターについて各サイトの履歴傾向情報が表示されます：

- セッション
- 接続エラー
- マシンエラー
- ログオン処理のパフォーマンス
- 負荷評価
- 容量管理
- マシンの使用量
- リソース使用

この情報を表示するには、［傾向］メニューをクリックします。

ズームインドリルダウン機能により、（グラフ内のデータポイントをクリックして）ある期間について着目し、その傾向に関連する詳細情報を表示させて、傾向チャートを参照できます。これにより、表示中の傾向により誰が、または何が影響を受けているかについてより詳細に把握できます。

各グラフのデフォルトの表示範囲を変更するには、［期間］フィルターを変更して適用します。

> 注：
>
> - 期間を［先月］（現時点まで）以下に設定すると、セッション、エラー、ログオンパフォーマンスの傾向情報をグラフや表として表示できます。期間に、終了日が設定可能な［先月］、または［昨年］を選択すると、傾向情報はグラフとして表示できますが、テーブルとしては表示できません。
> - Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）で保存される履歴データは、90 日間分のみです。このため、［監視］の 1 年間の傾向とレポートには過去 90 日分のデータが表示されます。

利用できる傾向

セッションの傾向の表示：［セッション］タブから、同時接続セッション数に関するより詳細な情報を表示するデリバリーグループと期間を選択します。

［セッションの自動再接続］列はセッション内で自動的に再接続を行う回数を表します。自動再接続は、［セッション画面の保持］ポリシーまたは［クライアントの自動再接続］ポリシーが機能している場合に有効になります。エンドポイントでネットワークの接続が中断された場合は、次のポリシーが有効になります：

- セッション画面の保持ポリシーが有効になり、デフォルトで 3 分間の持続時間に Citrix Receiver または Citrix Workspace アプリが VDA への接続を試みます。

- クライアントの自動再接続ポリシーが有効になり、3〜5 分間の持続時間にクライアントが VDA への接続を試みます。

どちらの場合も再接続の情報は記録され、ユーザーが確認できるようになっています。この情報が Director UI に表示されるまでには、再接続が施行されてから最大 5 分ほどかかることがあります。

自動再接続の情報は中断が発生したネットワーク接続の確認やトラブルシューティングに役立つだけでなく、シームレスなネットワークの分析にも活用できます。再接続数はデリバリーグループを指定したり、フィルターで特定の期間に絞り込んだりしたうえで表示することができます。

ドリルダウンではセッション画面の保持やクライアントの自動再接続、タイムスタンプ、エンドポイントの IP、Workspace アプリがインストールされているマシンのエンドポイント名などの詳しい情報を確認できます。

デフォルトでは、ログはイベントが起きたタイムスタンプに従って降順で並び替えられます。この機能は、Windows 向け Citrix Workspace アプリ、Mac 向け Citrix Workspace アプリ、Citrix Receiver for Windows、および Citrix Receiver for Mac で使用できます。この機能を使用するには、VDA 1906 以降が必要です。

セッションの再接続について詳しくは、「セッション」を参照してください。ポリシーについて詳しくは、「クライアントの自動再接続のポリシー設定」および「セッション画面の保持のポリシー設定」を参照してください。

次の理由により、自動再接続データがモニターに表示されない場合があります:

- Workspace アプリから VDA に自動再接続データが送信されていない。
- VDA から監視サービスにデータが送信されていない。

> 注:
>
> 特定の Citrix Gateway ポリシーが設定されていると、クライアント IP アドレスが正しく取得できないことがあります。

接続エラーの傾向の表示:［エラー］タブで、サイト全体のユーザー接続エラーの詳細情報を含むグラフを表示する接続、マシンの種類、エラーの種類、デリバリーグループ、および期間を選択します。

マシン障害の傾向の表示:［失敗したシングルセッションOS マシン］タブまたは［失敗したマルチセッション OS マシン］タブで、サイト全体のマシンエラーの詳細情報を含むグラフを表示するエラーの種類、デリバリーグループ、および期間を選択します。

ログオンパフォーマンスの傾向の表示:［ログオンパフォーマンス］タブで、サイト全体のログオン処理時間と、ログオン数がパフォーマンスに影響しているかについての詳細情報を含むグラフを表示するデリバリーグループと期間を選択します。このビューには、仲介処理時間や仮想マシンの起動時間などのログオンフェーズにおける平均時間も表示されます。
このデータはユーザーのログオンに関するものであり、切断セッションへの再接続は含まれません。
グラフの下のテーブルに、ユーザーセッションごとのログオン時間が表示されます。表示する列を選択し、いずれかの列を基準にレポートを並べ替えることができます。
詳しくは、「ユーザーログオンの問題の診断」を参照してください。

負荷評価の傾向の表示：［負荷評価基準インデックス］タブで、マルチセッション OS マシン間で分散された負荷に関する情報を表示します。このグラフでは、対象のデリバリーグループ、デリバリーグループのマルチセッション OS マシン、マルチセッション OS マシン、および期間を指定できます（マルチセッション OS マシンは、デリバリーグループのマルチセッション OS マシンが選択されている場合のみ指定可能）。負荷評価インデックスは、合計 CPU、メモリ、ディスク、またはセッションの割合として表示され、最新の間隔における接続ユーザー数と比較されます。

ホストされたアプリケーションの使用量の表示：［容量管理］の［ホストされたアプリケーションの使用量］タブでデリバリーグループと期間を選択すると、最大同時使用量を示すグラフと、アプリケーションごとの使用量を示す表が表示されます。［アプリケーションごとの使用量］の表では、特定のアプリケーションについての詳細や、そのアプリケーションを使用しているユーザー、および使用していたユーザーの情報を表示できます。

シングルセッション **OS** およびマルチセッション **OS** の使用状況の表示：［傾向］ビューでは、サイト別およびデリバリーグループ別のシングルセッション OS の使用状況が表示されます。［サイト］を選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、ユーザーごとの使用状況が表示されます。
［傾向］ビューでは、サイト別、デリバリーグループ別、およびマシン別のマルチセッション OS の使用状況も表示されます。［サイト］を選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、マシンごとおよびユーザーごとの使用状況が表示されます。マシンを選択すると、ユーザーごとの使用状況が表示されます。

仮想マシン使用量の確認：［マシン使用量］タブで［シングルセッションOS マシン］または［マルチセッション OS マシン］を選択して、仮想マシンの使用状況をリアルタイムで表示させることができます。このページでは、選択したデリバリーグループおよび期間に電源がオンになっている、Autoscale 対応マルチセッションおよびシングルセッションOS マシンの総数を表示します。選択したデリバリーグループで Autoscale を有効にすることで達成される見積もり削減額も表示できます。これは、マシンあたりのコストを使用してパーセンテージで算出されます。

Autoscale 対応マシンの使用状況の傾向は、マシンの実際の使用状況を示しているため、サイトの処理能力ニーズを迅速に評価することができます。

- シングルセッション OS の可用性 - シングルセッション OS マシン（VDI）の現在の状態をサイト全体または特定のデリバリーグループについて可用性に基づいて表示します。
- マルチセッション OS の可用性 - マルチセッション OS マシンの現在の状態をサイト全体または特定のデリバリーグループについて可用性に基づいて表示します。

> 注：
>
> チャートの下のグリッドに、デリバリーグループベースでリアルタイムのマシンの使用量データを表示します。このデータには、Autoscale 対応かどうかにかかわらず、すべてのマシンの可用性が含まれています。グリッドの使用可能なカウンター列に表示されるマシンの数には、メンテナンスモードのマシンが含まれます。

監視データの統合は、選択した期間によって異なります。

- 期間が 1 日および 1 週間の監視データは時間単位で統合されます。
- 期間が 1 か月の監視データは日にち単位で統合されます。

マシンの状態は統合時に読み取られ、その期間中の変更は考慮されません。統合期間については、「Monitor API のドキュメント」を参照してください。

Autoscale 対応マシンの監視について詳しくは、「Autoscale」を参照してください。

リソース使用の表示：［リソース使用］タブで［シングルセッションOS マシン］または［マルチセッション OS マシン］を選択して、各 VDI マシンの CPU とメモリ使用量、および IOPS とディスク遅延に関する履歴傾向を取得し、容量の計画に役立てることができます。
この機能を使用するには、VDA のバージョン **7.11** 以降が必要です。
平均 CPU、平均メモリ、平均 IOPS、ディスク遅延、および最大同時セッション数を表示するグラフです。マシンにドリルダウンして、CPU を消費している上位 10 のプロセスに関するデータとチャートを表示できます。デリバリーグループ別および期間別でフィルターできます。過去 2 時間、24 時間、7 日間、月、年の CPU、メモリ使用量、最大同時セッション数のグラフを入手できます。平均 IOPS とディスク遅延は、過去 24 時間、月、年のグラフが入手可能です。

> 注：
>
> - データを収集して［マシン使用率の履歴］ページの［上位 10 位のプロセス］表に表示するには、監視ポリシーの［プロセスの監視を有効にします］設定を［許可］に設定する必要があります。このポリシーはデフォルトでは禁止されています。デフォルトではすべてのリソース使用データが収集されます。これは、ポリシーの［リソース監視の有効化］設定で無効にできます。グラフの下のテーブルは、マシンごとのリソース使用状況データを示しています。
> - 平均 IOPS は、1 日の平均値を示します。最大 IOPS は、選択した期間の IOPS の平均において最も高い IOPS が算出されます。（IOPS の平均は、選択した期間に VDA で収集された IOPS の 1 時間当たりの平均です）。
> - マシンのドリルダウンで、平均 CPU または平均メモリ使用率が 1% を超えるプロセスが一覧表示されます（一覧に含まれるプロセスが 10 個未満になることがあります）。

アプリケーション障害の表示：［アプリケーション障害］タブで、VDA 上の公開アプリケーションに関連した障害が表示されます。

この機能を使用するには、VDA のバージョン **7.15** 以降が必要です。Windows Vista 以降が動作するシングルセッション OS 対応 VDA、および Windows Server 2008 以降が動作するマルチセッション OS 対応 VDA がサポートされます。
詳しくは、「アプリケーション障害履歴の監視」を参照してください。

デフォルトでは、マルチセッション OS VDA からのアプリケーション障害のみが表示されます。監視ポリシーを使って、アプリケーション障害の監視の設定ができます。詳しくは、「監視のポリシー設定」を参照してください。

カスタム レポートの作成：［カスタムレポート］タブには、監視データベースのリアルタイムデータおよび履歴データを含むカスタムレポートを表形式で生成するためのユーザーインターフェイスがあります。

以前に保存されたカスタムレポートクエリの一覧で、［実行してダウンロード］をクリックするとそのレポートを CSV 形式でエクスポートでき、［**OData** のコピー］をクリックすると該当する OData クエリをコピーして共有でき、［編集］をクリックするとクエリを編集できます。
マシン、接続、セッション、またはアプリケーションインスタンスに基づいて、カスタムレポートクエリを作成できます。フィールド（たとえばマシン、デリバリーグループ、または期間）に基づいてフィルター条件を指定します。カ

スタムレポートで必要な追加の列を指定します。プレビューには、レポートデータのサンプルが表示されます。カスタムレポートクエリを保存すると、保存済みクエリのリストに追加されます。

コピーした OData クエリに基づいて、カスタムレポートクエリを作成できます。それには、OData Query オプションを選択し、コピーした OData クエリを貼り付けます。結果として得られたクエリを、後で実行するために保存できます。

> 注:
>
> OData クエリを使用して生成したレポートのプレビューとエクスポートでは、列名はローカライズされず、英語で表示されます。

また、重要なイベントやアクションの発生は、フラグアイコンで示されます。フラグをクリックすると、発生したイベントまたはアクションが表示されます。

> 注:
>
> - バージョン 7 より前の VDA に対しては、HDX 接続のログオンデータは収集されません。以前のバージョンの VDA については、チャートデータが 0 として表示されます。
> - ［管理］コンソールで削除されたデリバリーグループは、関連データがクリーンアップされるまで［傾向］フィルターで選択できます。削除されたデリバリーグループを選択すると、保存まで使用可能なデータのグラフが表示されます。ただし、テーブルにはデータは表示されません。
> - デリバリーグループ間でアクティブなセッションがあるマシンを移動すると、移動後のデリバリーグループの ［リソース使用率］および［負荷評価基準インデックス］テーブルで両方のデリバリーグループの統合されたメトリックが表示されます。

Autoscale 管理対象マシンの監視

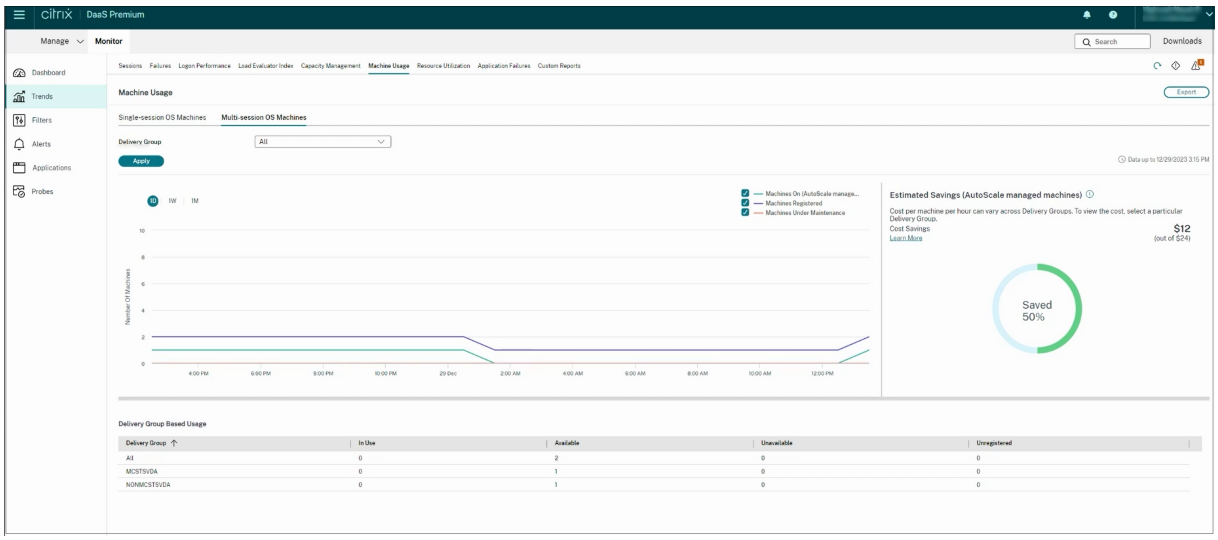
March 30, 2022

Autoscale は、デリバリーグループに登録されているすべてのマルチセッションおよびシングルセッションOS マシンの電源をプロアクティブに管理できる電源管理機能です。Autoscale は、［管理］タブで選択したデリバリーグループで構成できます。詳しくは、「Autoscale」を参照してください。
［監視］タブで Autoscale 対応マシンの主要メトリックを監視できます。

マシンの使用量

［監視］>［傾向］>［マシンの使用量］ページでは、選択したデリバリーグループおよび期間に電源がオンになっている、Autoscale 対応マルチセッションおよびシングルセッションOS マシンの総数を表示します。このメトリックは、デリバリーグループ内のマシンの実際の使用量を示します。

［シングルセッション **OS** マシン］または ［マルチセッション **OS** マシン］タブで、デリバリーグループと期間を選択します。

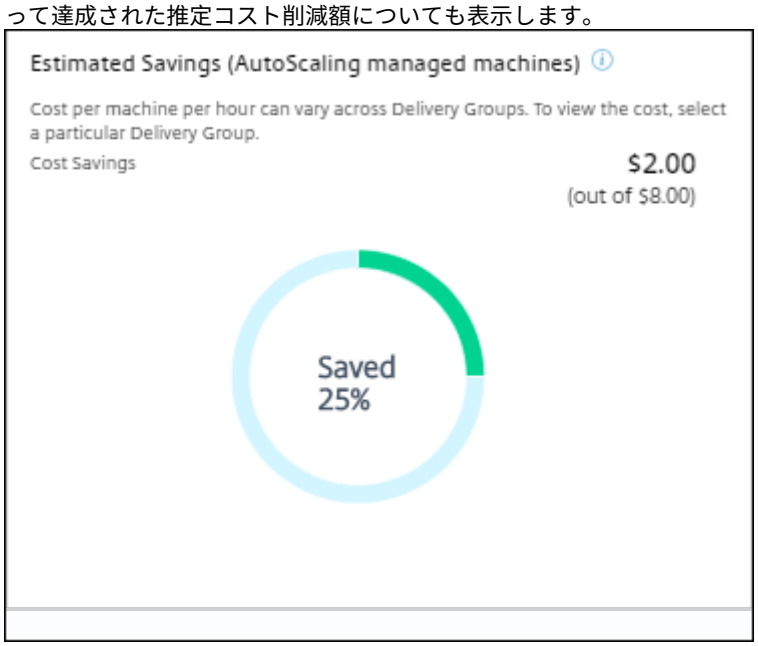


このチャートは、以下のメトリックを表示しています:

- 有効になっているマシン - 電源がオンになっている Autoscale 対応マシンの数
- 登録されたマシン - 登録されたマルチセッションまたはシングルセッション OS マシンの数
- メンテナンス中のマシン - メンテナンスモードがオンになっているマルチセッションまたはシングルセッションOS マシンの数

見積もり削減額

［監視］>［傾向］>［マシン使用量］ページでは、選択したデリバリーグループで Autoscale を有効にすることによって達成された推定コスト削減額についても表示します。



見積もり削減額は、［管理］>［デリバリーグループの編集］>［**Autoscale**］で構成された 1 時間あたりのマシンごとの削減額（米ドル）をパーセンテージで算出します。マシンごとの削減額の構成について詳しくは、「Autoscale」を参照してください。

すべてのデリバリーグループを選択すると、すべてのデリバリーグループに関する見積もり削減額の平均値が表示されます。
見積もり削減額は、管理者が既存のインフラストラクチャを統合し、削減額と使用率を最大化するための処理能力を計画する時に役立ちます。

マシンとセッションのアラート通知

［監視］ダッシュボードには、ドリルダウン可能なアラート通知が表示されます。アラートの詳細は ［監視］>［アラート］ページに表示されます。

- デリバリーグループでアラートポリシーを作成するには、［監視］>［アラート］>［**Citrix** アラートポリシー］>［デリバリーグループポリシー］に移動します。
- ここでは、以下の警告および限界しきい値を設定できます：
  - 失敗したマシン（シングルセッション OS）と失敗したマシンマルチセッション OS）、
  - デリバリーグループでの最大接続セッション数、最大切断セッション数、合計最大同時セッション数。
- デリバリーグループ内の対応するメトリックがしきい値に達すると、アラートが生成されます。

アラートポリシーの条件と新しいアラートポリシーの作成について詳しくは、「アラートおよび通知」を参照してください。

マシンの状態

- ［監視］>［フィルター］>［マシン］では、すべてのマシンの電源状態を表形式で表示します。特定のデリバリーグループで絞り込むことができます。
- ［監視］>［フィルター］>［セッション］はマシン名ごとにフィルターを表示し、関連付けられたセッションおよびリアルタイムの状態を確認できます。
- ［監視］>［傾向］>［セッション］でデリバリーグループと期間を選択して、セッションの傾向と関連するメトリックを表示します。

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

負荷評価傾向

［監視］>［傾向］>［負荷評価基準インデックス］ページで、マルチセッション OS マシン間で分散された負荷に関する詳細な情報をグラフに表示します。このグラフでは、対象のデリバリーグループ、デリバリーグループのマルチセッション OS マシン、マルチセッション OS マシン、および期間を指定できます（マルチセッション OS マシンは、

デリバリーグループのマルチセッション OS マシンが選択されている場合のみ指定可能)。負荷評価基準インデックスは、合計 CPU、メモリ、ディスク、またはセッションのパーセンテージとして表示され、最後の間隔での接続ユーザー数と比較されます。

展開のトラブルシューティング

March 31, 2024

ヘルプデスク管理者は、問題を報告しているユーザーを検索できます。そして、そのユーザーに関連付けられたセッションまたはアプリケーションの詳細を表示します。

同様に、問題が報告されたマシンやエンドポイントも検索できます。関連するメトリックを監視し、適切な対処法を実行することで、問題を迅速に解決できます。

実行できるアクションは次のとおりです:

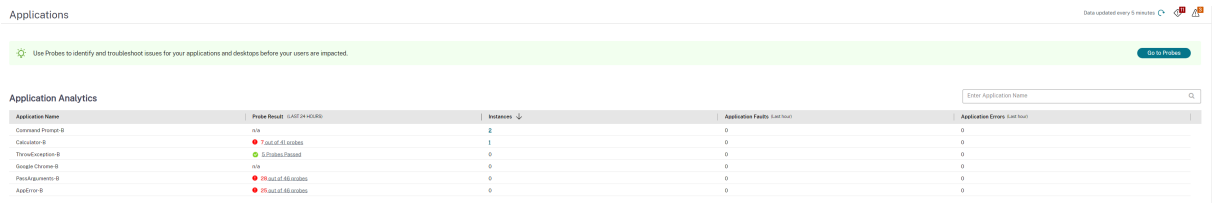
- 応答しないアプリケーションまたはプロセスの終了
- ユーザーのマシンでの操作のシャドウ
- 応答しないセッションのログオフ
- マシンの再起動
- マシンをメンテナンスモードにすること
- ユーザープロファイルのリセット

アプリケーションのトラブルシューティング

July 25, 2023

アプリケーション分析

［アプリケーション］ビューには、アプリケーションのパフォーマンスを効率的に分析および管理するのに役立つ、単一の統合ビューにアプリケーションベースの分析が表示されます。サイトに公開されているすべてのアプリケーションの正常性および使用状況に関する情報について貴重な分析情報を得ることができます。デフォルトのビューは、よく実行されているアプリケーションを識別するのに役立ちます。
この機能を使用するには、VDA のバージョン 7.15 以降が必要です。



[プローブの結果] 列には、過去 24 時間に実行されたアプリケーションプロービングの結果が表示されます。[傾向] > [プローブの結果] ページで詳細を表示するには、プローブの結果のリンクをクリックします。アプリケーションプローブを構成する方法について詳しくは、「アプリケーションおよびデスクトッププロービング」を参照してください。

[インスタンス] 列には、アプリケーションの使用状況が表示されます。現在実行中のアプリケーションインスタンス（接続インスタンスと切断インスタンスの両方）の数を示します。詳細なトラブルシューティングを行うには、[インスタンス] フィールドをクリックして、対応する [アプリケーションインスタンス] フィルターページを表示します。ここでは、ログオフまたは切断するアプリケーションインスタンスを選択できます。

> 注:
>
> カスタムスコープ管理者の場合、[監視] はアプリケーショングループに作成されたアプリケーションインスタンスを表示しません。すべてのアプリケーションインスタンスを表示するには、すべての管理権限を実行できる管理者である必要があります。詳しくは、Knowledge Center のCTX256001を参照してください。

[アプリケーション障害] 列と [アプリケーションエラー] 列を使用して、サイト内の公開アプリケーションの正常性をモニターします。これらの列には、過去 1 時間以内に対応するアプリケーションを起動している間に発生した障害とエラーの合計数が表示されます。[アプリケーション障害] または [アプリケーションエラー] フィールドをクリックすると、選択したアプリケーションに対応する [傾向] > [アプリケーション障害] ページに障害の詳細が表示されます。

アプリケーション障害ポリシーの設定では、障害やエラーの可用性と表示を管理します。ポリシーとその変更方法について詳しくは、「監視のポリシー設定」の「アプリケーション障害の監視ポリシー」を参照してください。

リアルタイムアプリケーション監視

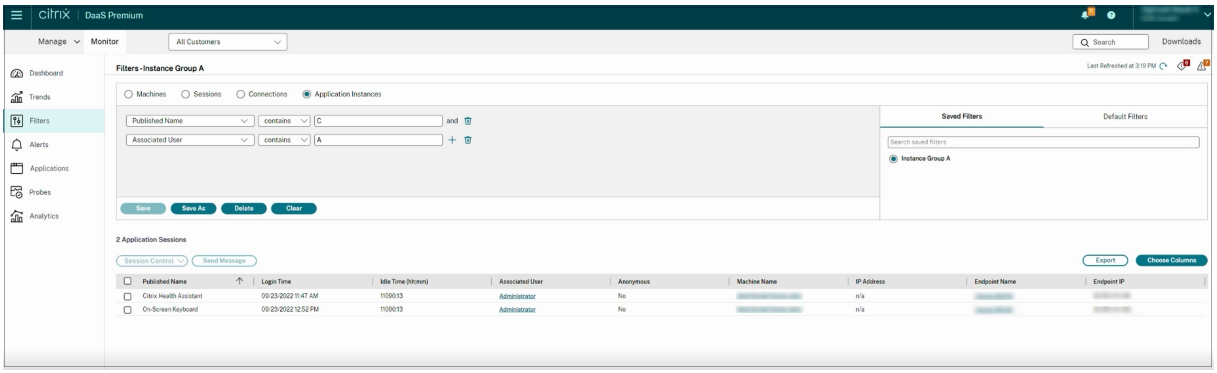
アイドル状態の時間の指標を使用して、特定の時間制限を超えてアイドル状態であるインスタンスを識別することで、アプリケーションとセッションをトラブルシューティングできます。

アプリケーションベースのトラブルシューティングの一般的な用途は、ヘルスケアのセクターです。このセクターでは、従業員間でアプリケーションライセンスが共有されています。このため、Citrix Virtual Apps and Desktops の環境の削除、パフォーマンスの低いサーバーの再構成、アプリケーションの保守およびアップグレードを行うには、アイドル状態のセッションとアプリケーションインスタンスを終了する必要があります。

[アプリケーションインスタンス] フィルターページには、マルチセッション OS 上とシングルセッション OS 上にある VDA のすべてのアプリケーションインスタンスが表示されます。関連付けられたアイドル時間の測定値は、10 分間以上アイドル状態になっているマルチセッション OS 対応 VDA のアプリケーションインスタンスについて表示されます。

> 注:
>
> アプリケーションインスタンスのメトリックは、すべてのライセンスエディションのサイトで確認できます。

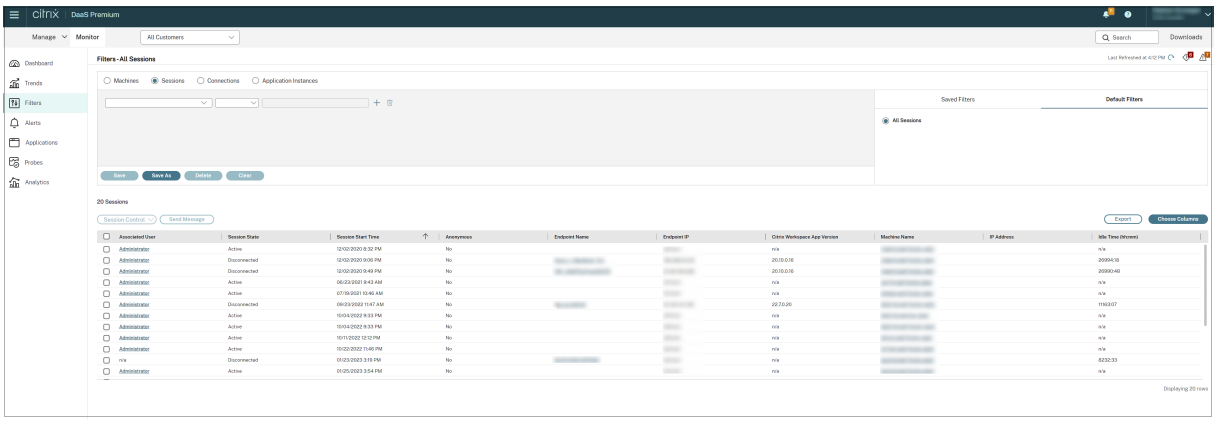
一定時間以上アイドル状態になっているアプリケーションインスタンスを識別して、必要に応じてログオフするか接続を切断するためにこの情報を使用します。これを行うには、[フィルター] > [アプリケーション インスタンス] の順に選択し、保存済みのフィルターを選択するか [すべてのアプリケーションインスタンス] を選択し、独自のフィルターを作成します。



フィルターの例は次のようになります。[フィルター基準] 条件として [公開名] (アプリケーションの公開名) と [アイドル時間] を選択します。次に [アイドル時間] に [次のもの以上] を設定して特定の時間制限を指定、再利用のためのフィルターを保存します。フィルター後の一覧から、アプリケーションインスタンスを選択します。メッセージを送信するオプションを選択するか、[セッション制御] ドロップダウンリストから [ログオフ] または [切断] を選択してインスタンスを終了します。

> 注:
>
> ログオフするかアプリケーションインスタンスを切断すると、現在のセッションがログオフされるか切断されるため、同じセッションに属するすべてのアプリケーションインスタンスが終了します。

[セッション] フィルターページでセッション状態とセッションのアイドル時間の指標を使用してアイドル状態のセッションを識別できます。[アイドル時間] 列で並べ替えるか、特定の時間制限を超えてアイドル状態であるセッションを識別するフィルターを定義します。アイドル時間は、10 分間以上アイドル状態であるマルチセッション OS 対応 VDA 上のセッションに対して表示されます。



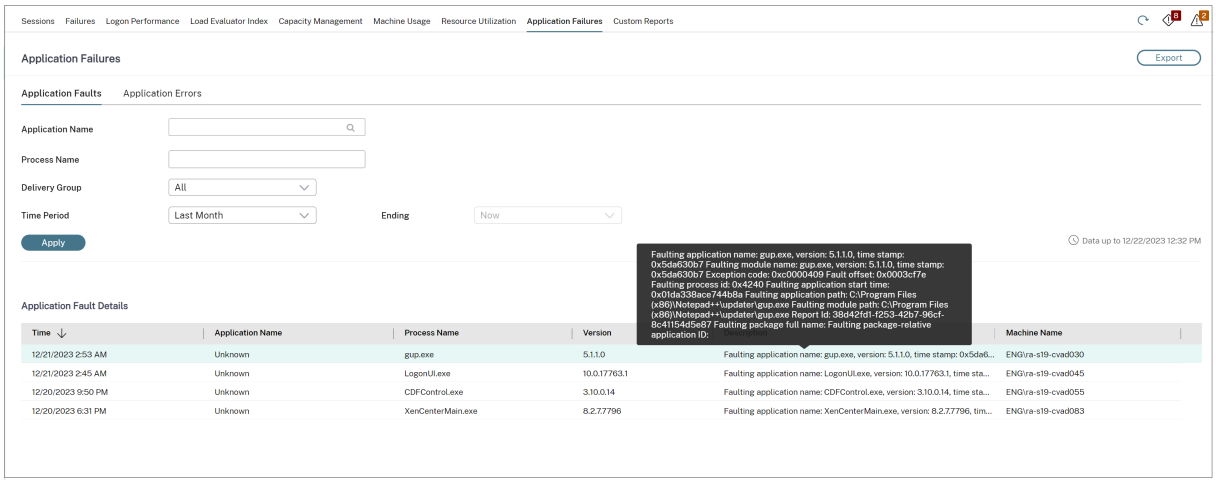
セッションまたはアプリケーションインスタンスが次のいずれかの場合、［アイドル時間］には ［なし］と表示されます。

- アイドル状態の時間が 10 分未満の場合
- シングルセッション OS 対応 VDA 上で起動されている場合
- バージョン 7.12 以前を実行する VDA 上で起動されている場合

アプリケーション障害履歴の監視

［傾向］>［アプリケーション障害］タブに、VDA 上の公開アプリケーションに関連する障害が表示されます。

アプリケーション障害の傾向の可用性について詳しくは、「データの粒度と保持」を参照してください。ソースに「アプリケーションエラー」がある場合は、イベントビューアーに記録されているアプリケーション障害が監視されます。［エクスポート］をクリックすると、CSV、Excel、または PDF フォーマットのレポートが生成されます。



障害はその重要度によって ［アプリケーション障害］または ［アプリケーションエラー］として表示されます。［アプリケーション障害］タブには、機能またはデータの損失に関連した障害が表示されます。［アプリケーションエラー］には、即座に関連しない問題が示されます。これは、将来問題が発生する可能性がある状況を意味しています。

障害は、公開アプリケーション名、プロセス名またはデリバリーグループ、および期間によってフィルターできます。表には、障害またはエラーコードと簡単な説明が表示されます。詳細な障害の説明はツールチップとして表示されます。

> 注:
>
> 対応するアプリケーション名を取得できない場合、公開アプリケーション名は「不明」として表示されます。これは、通常、アプリケーションの起動がデスクトップセッションで失敗した場合、または依存している実行ファイルが原因で処理できない例外により失敗した場合に発生します。

デフォルトでは、マルチセッション OS VDA でホストされたアプリケーションの障害のみが監視されています。監視グループポリシーでは次のような監視設定が変更できます：アプリケーション障害の監視の有効化、シングルセッシ

ョン OS 対応 VDA 上のアプリケーション障害の監視の有効化、および障害の監視から除外されるアプリケーションの一覧の設定。詳しくは、「監視のポリシー設定」の「アプリケーション障害の監視ポリシー」を参照してください。

［傾向］>［アプリケーションプローブの結果］ページには、そのサイトで過去 24 時間および 7 日間に実行されたアプリケーションプロービングの結果が表示されます。アプリケーションプローブを構成する方法について詳しくは、「アプリケーションプロービング」を参照してください。

アプリケーションプロービング

January 18, 2023

アプリケーションプロービングでは、サイトに公開されている Citrix Virtual Apps の状態チェックプロセスが自動化されます。アプリケーションプロービングの結果は、Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）の ［監視］タブで参照できます。Citrix Probe Agent は、Citrix Cloud Japan および Citrix Cloud Government コントロールプレーンでホストされるサイトをサポートするようになりました。

プローブエージェントが実行されるエンドポイントマシンは、Citrix Receiver for Windows バージョン 4.8 以降または Windows 向け Citrix Workspace アプリ（旧称 Citrix Receiver for Windows）バージョン 1808 以降がインストールされたマシンのみであることを確認してください。統合 Windows プラットフォーム（UWP）向けの Workspace アプリはサポートされていません。

要件:

- プローブエージェントが実行されるエンドポイントマシンは、Citrix Receiver for Windows バージョン 4.8 以降または Windows 向け Citrix Workspace アプリ（旧称 Citrix Receiver for Windows）バージョン 1906 以降がインストールされたマシンのみです。統合 Windows プラットフォーム（UWP）向けの Workspace アプリはサポートされていません。
- Citrix Probe Agent は、Citrix WorkSpace でサポートされているデフォルトのフォームベース認証をサポートしています。Citrix Probe Agent は、シングルサインオン（SSO）や多要素認証（MFA）などの他の認証方法をサポートしていません。同様に、Citrix Probe Agent は、Citrix Gateway や Citrix ADC のようなプロキシサーバーやロードバランサーが展開されていない場合にのみ機能します。
- Probe Agent をインストールするエンドポイントマシンに、Microsoft .NET Framework バージョン 4.7.2 以降がインストールされていることを確認します。
- Citrix Cloud Japan コントロールプレーンでプロービングエージェントを使用するには、パスのレジストリ値を「\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region」を 2 に設定します。Citrix Cloud Government コントロールプレーンでプロービングエージェントを使用するには、パスのレジストリ値を「\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\regi
を 3 に設定します。

アプリケーションプロービングを実行するために必要なユーザーアカウント/権限:

- 各エンドポイントマシンで調査するための固有の Workspace ユーザー。Workspace ユーザーは管理者である必要はありません。プローブは管理者以外も実行できます。
- エンドポイントマシンに Citrix Probe Agent をインストールおよび設定するための Windows 管理者権限を持つユーザーアカウント
- 次の権限を持つ完全な管理者ユーザーアカウント。アプリケーションプロービングに既存のユーザーアカウントを再利用すると、ユーザーのアクティブなセッションがログオフされることがあります。
  - デリバリーグループの権限:
    - Read-only
  - Director の権限:
    - プローブ構成の作成\編集\削除
    - 構成ページの表示
    - 傾向ページの表示

アプリケーションプロービングの構成

アプリケーションプローブを、複数の地域にわたってオフピーク時に実行するように構成します。包括的なプローブの結果は、アプリケーション、ホストマシン、または接続に関連する問題を、ユーザーが経験する前にトラブルシューティングするのに役立ちます。

Citrix Probe Agent バージョン 2103 は、サイトアグリゲーションをサポートしています。アプリケーションとデスクトップは、集約されたサイトから列挙して起動できます。プローブエージェントを構成するときは、[**Workspace**（**StoreFront**）のサイトアグリゲーションが有効になっています:］オプションを選択して、集約されたサイトからのアプリケーションとデスクトップの列挙を有効にします。次のサイトの組み合わせがサポートされています:

- 1 つの StoreFront URL を持つ複数のオンプレミスサイト。
- StoreFront または Workspace URL のいずれかを持つオンプレミスおよびクラウドサイト。
- 1 つの Workspace URL を持つ複数のクラウドサイト。

> 注:
>
> 1 つのサイトにのみアクセスできるプローブを構成するには、個別の管理者またはユーザーを作成する必要があります。

手順 **1**: **Citrix Probe Agent** をインストールして構成する

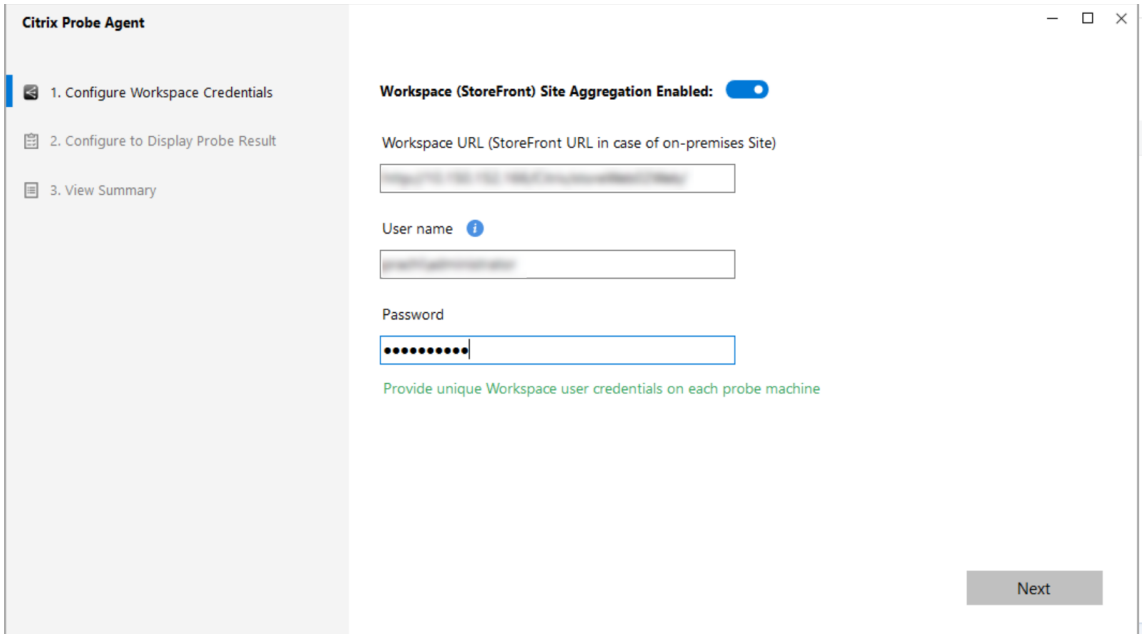
Citrix Probe Agent は、Citrix Workspace を介したユーザーの実際のアプリケーション起動をシミュレートする Windows 実行可能ファイルです。［監視］で構成したアプリケーション起動をテストし、結果を［監視］に報告します。

1. アプリケーションプロービングを実行するエンドポイントマシンを特定します。

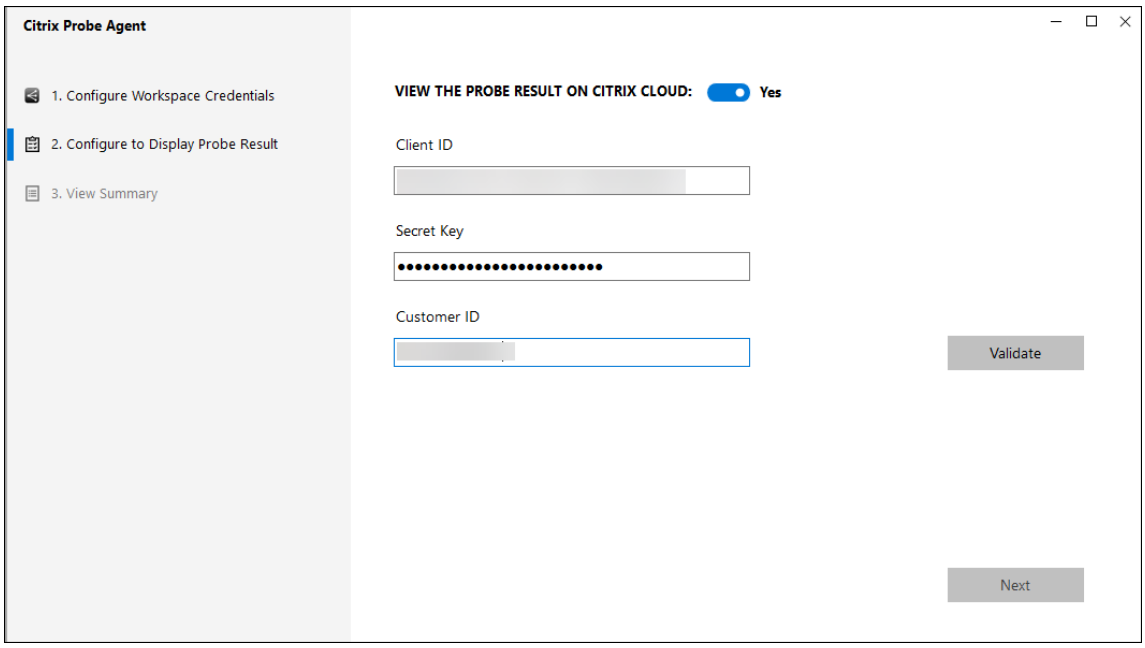
2. 管理者権限を持つユーザーは、Citrix Probe Agent をエンドポイントマシンにインストールして設定することができます。次の場所にある Citrix Probe Agent 実行可能ファイルをダウンロードします: https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html

3. エージェントを起動し、Citrix Workspace の資格情報を構成します。各エンドポイントマシンで固有の Workspace ユーザーを構成します。資格情報は暗号化され、安全に保管されます。

   > 注:
   >
   > - ネットワーク外からプローブされるサイトにアクセスするには、**Workspace URL** フィールドに Citrix Gateway のログイン URL を入力します。Citrix Gateway は、対応するサイトの Workspace URL に要求を自動的にルーティングします。
   > - ユーザー名フィールドのドメイン名として NetBIOS を使用します。例: NetBIOS/ユーザー名。
   > - アプリのプローブでは、ワークスペース認証 (AD のみ) を使用した Citrix Content Collaboration サービスがサポートされています。



4. [プローブ結果の表示構成] タブで、Citrix DaaS にアクセスするための資格情報を入力します。Citrix Cloud コンソールの [API アクセス] ページで、顧客名または顧客 ID、クライアント ID、秘密キーを確認できます。



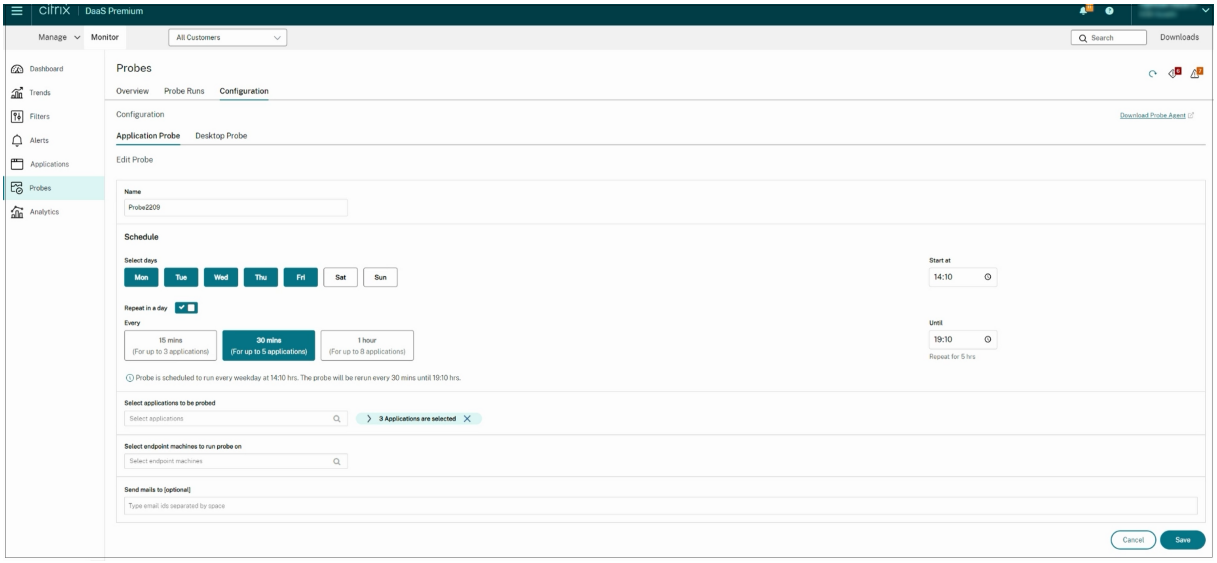
手順 **2**:［監視］タブでアプリケーションプロービングを設定する

1. Citrix DaaS で ［構成］>［プローブの構成］>［アプリケーションプローブ］に移動して、［プローブの作成］を選択します:
2. ［プローブの作成］ページで、プローブの名前を入力します。
3. スケジュールを選択します:

    a) プローブを実行する曜日を選択します。
    b) プローブを実行する開始時刻を入力します。
    c) また、［**1** 日での繰り返し］オプションを選択できます。終了時間と、プローブを 1 日の間に繰り返す間隔を入力します。たとえば、以下の構成にすると、毎週月曜日、水曜日、木曜日、日曜日の 12 時 8 分から 16 時 34 分まで、30 分ごとにアプリケーションプローブを実行できます。

4. この間隔に応じて、推奨されるプローブ対象アプリケーションの数を選択します。
5. プローブを実行する必要があるエンドポイントマシンを選択します。
6. プローブのエラー結果が送信されるメールアドレスを入力し、［保存］をクリックします。

この構成では、アプリケーションセッションは毎週月曜日、水曜日、木曜日、日曜日の 16 時 8 分まで、12 時 8 分、12 時 38 分、13 時 8 分などの時間に起動します。



> 注:
>
> - ［アラート］ > ［メール サーバー構成］でメールサーバーを構成してください。
> - ［監視］タブで構成後、エージェントは次の 1 時間から構成されたプローブを実行します。
> - ［**1** 日での繰り返し］オプションが導入される前にセットアップされたプローブは、スケジュールされた時間に引き続き実行されます。［**1** 日での繰り返し］オプションは、デフォルトで無効になっています。

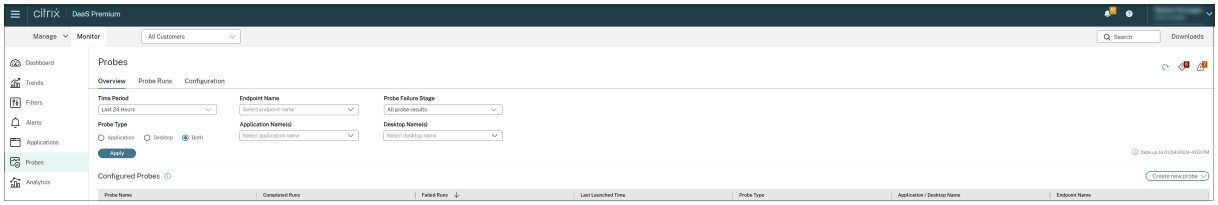
手順 **3**: プローブの実行

エージェントは、1 時間ごとに［監視］からフェッチするプローブ構成に従ってアプリケーションプロービングを実行します。Workspace を使用して、選択したアプリケーションを連続して起動します。エージェントは、監視データベースを介して［監視］に結果を報告します。エラーは、以下の 5 つの特定の段階で報告されます:

- **Workspace** の到達可能性 - 構成された Workspace URL に到達できません。
- **Workspace** の認証 - 構成された Workspace の資格情報が無効です。
- **Workspace** の列挙 - Workspace で列挙されるアプリケーションの一覧には、調査対象のアプリケーションが含まれていません。
- **ICA** のダウンロード - ICA ファイルは使用できません。
- アプリケーションの起動 - アプリケーションを起動できませんでした。

手順 **4**: プローブの結果を表示する

最新のプローブ結果は、Citrix DaaS の ［アプリケーション］ページで確認できます。



さらにトラブルシューティングするには、プローブの結果のリンクをクリックして、［傾向］>［アプリケーションプローブの結果］ページで詳細を表示します。

統合されたプローブの結果データは、このページの過去 24 時間または過去 7 日間の期間に使用できます。プローブが失敗した段階がわかります。特定のアプリケーション、プローブ障害段階、またはエンドポイントマシンの表をフィルタリングできます。

デスクトッププロービング

February 10, 2023

デスクトッププロービングでは、サイトに公開されている Citrix Virtual Desktops の状態チェックプロセスが自動化されます。デスクトッププロービングの結果は［監視］で確認できます。Citrix Probe Agent は、Citrix Cloud Japan および Citrix Cloud Government コントロールプレーンでホストされるサイトをサポートするようになりました。

［監視］の［構成］ページで、プローブするデスクトップ、プローブを実行するエンドポイントマシン、およびプローブ時間を設定します。エージェントは、選択したデスクトップの起動を Workspace を使用してテストし、その結果を［監視］に報告します。プローブの結果は［監視］の UI に表示されます。［アプリケーション］ページにアプリケーションの過去 24 時間のデータが表示され、［傾向］**>**［プローブの結果］**>**［デスクトッププローブの結果］ページにプローブの履歴データが表示されます。

ここでは、プローブ障害がどの段階（Workspace の到達可能性、Workspace の認証、Workspace の列挙、ICA ダウンロード、またはデスクトップの起動）で発生したかを確認できます。障害レポートは、設定されているメールアドレスに送信されます。

デスクトッププローブは、複数の地域にわたってオフピーク時に実行するようにスケジュールできます。包括的なプローブの結果は、デスクトップ、ホストマシン、または接続に関連する問題が生じてユーザーに影響が出る前に、予防的にトラブルシューティングするのに役立ちます。

この機能には、Probe Agent 1903 以降が必要です。

要件:

- プローブエージェントが実行されるエンドポイントマシンは、Citrix Receiver for Windows バージョン 4.8 以降または Windows 向け Citrix Workspace アプリ（旧称 Citrix Receiver for Windows）バージョン 1906 以降がインストールされたマシンのみです。統合 Windows プラットフォーム（UWP）向けの Workspace アプリはサポートされていません。

- Citrix Probe Agent は、StoreFront および Citrix WorkSpace でサポートされているデフォルトのフォームベース認証をサポートしています。Citrix Probe Agent は、シングルサインオン（SSO）や多要素認証（MFA）などの他の認証方法をサポートしていません。同様に、Citrix Probe Agent は、Citrix Gateway や Citrix ADC のようなプロキシサーバーやロードバランサーが展開されていない場合にのみ機能します。
- Probe Agent をインストールするエンドポイントマシンに、Microsoft .NET Framework バージョン 4.7.2 以降がインストールされていることを確認します。
- Citrix Cloud Japan コントロールプレーンでプロービングエージェントを使用するには、パスのレジストリ値を「\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region」を 2 に設定します。Citrix Cloud Government コントロールプレーンでプロービングエージェントを使用するには、パスのレジストリ値を「\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\regi
を 3 に設定します。

デスクトッププロービングを実行するために必要なユーザーアカウントまたは権限：

- 各エンドポイントマシンで調査するための固有の Workspace ユーザー。Workspace ユーザーは管理者である必要はありません。プローブは管理者以外も実行できます。
- エンドポイントマシンに Citrix Probe Agent をインストールおよび設定するための Windows 管理者権限を持つユーザーアカウント
- 次の権限を持つ完全な管理者ユーザーアカウントまたはカスタムロール。デスクトッププロービングに通常のユーザーアカウントを再利用すると、ユーザーがアクティブなセッションからログオフされることがあります。
  - デリバリーグループの権限：
    - Read-only
  - 権限の監視：
    - アラートメールサーバー構成の作成、編集、削除 - メールサーバーがまだ構成されていない場合
    - プローブ構成の作成、編集、削除
    - 構成ページの表示
    - 傾向ページの表示

デスクトッププロービングの設定

デスクトッププローブは、複数の地域にわたってオフピーク時に実行するようにスケジュールできます。包括的なプローブの結果は、デスクトップ、ホストマシン、または接続に関連する問題が生じてユーザーに影響が出る前にトラブルシューティングするのに役立ちます。

Citrix Probe Agent バージョン 2103 は、サイトアグリゲーションをサポートしています。アプリケーションとデスクトップは、集約されたサイトから列挙して起動できます。プローブエージェントを構成するときは、[**Workspace（StoreFront）のサイトアグリゲーションが有効になっています：**] オプションを選択して、集約されたサイトからのアプリケーションとデスクトップの列挙を有効にします。次のサイトの組み合わせがサポートされています：

- 1 つの StoreFront URL を持つ複数のオンプレミスサイト。

- StoreFront または Workspace URL のいずれかを持つオンプレミスおよびクラウドサイト。
- 1 つの Workspace URL を持つ複数のクラウドサイト。

> 注:
>
> 1 つのサイトにのみアクセスできるプローブを構成するには、個別の管理者またはユーザーを作成する必要があります。

手順 **1**：**Citrix Probe Agent** をインストールして構成する

Citrix Probe Agent は、Workspace を介したユーザーの実際のデスクトップ起動をシミュレートする Windows 実行可能ファイルです。［監視］で構成したデスクトップの起動をテストし、結果を［監視］に報告します。

1. デスクトッププロービングを実行するエンドポイントマシンを特定します。
2. 管理者権限を持つユーザーは、Citrix Probe Agent をエンドポイントマシンにインストールして設定することができます。次の場所にある Citrix Probe Agent 実行可能ファイルをダウンロードします: https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html
3. エージェントを起動し、Workspace Receiver for Web の認証情報を構成します。各エンドポイントマシンで固有の Workspace ユーザーを構成します。資格情報は暗号化され、安全に保管されます。

   > 注:
   >
   > - ネットワーク外からプローブされるサイトにアクセスするには、Workspace URL フィールドに Citrix Gateway のログインページ URL を入力します。Citrix Gateway は、対応するサイトの Workspace URL に要求を自動的にルーティングします。この機能は、Citrix Gateway バージョン 12.1 以降で使用できます。
   > - ユーザー名フィールドのドメイン名として NetBIOS を使用します。例：NetBIOS/ユーザー名。
   > - デスクトップのプローブでは、ワークスペース認証（AD のみ）を使用した Citrix Content Collaboration サービスがサポートされています。
   > - 構成済みの一意の StoreFront ユーザーに対して対話型ログオンを有効にする必要があります。

4. ［プローブ結果の表示構成］タブで、［監視］の資格情報を入力します。Citrix Cloud コンソールの［API アクセス］ページで、顧客名または顧客 ID、クライアント ID、秘密キーを確認できます。

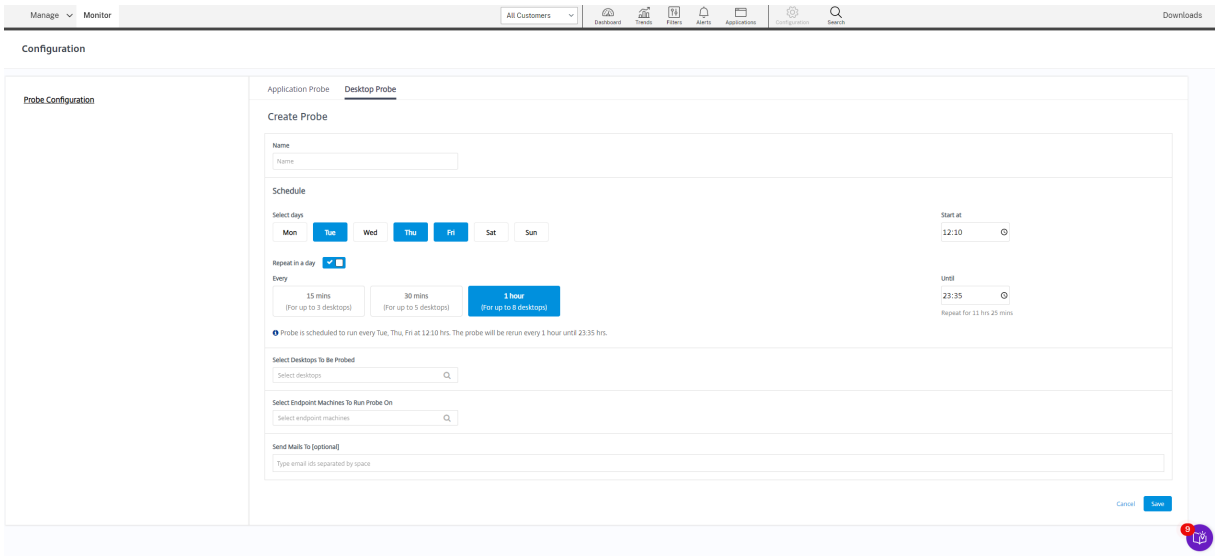
手順 **2**：［監視］でデスクトッププロービングを設定する

1. Citrix DaaS で ［構成］>［プローブの構成］ >［アプリケーションプローブ］に移動して、［プローブの作成］を選択します。
2. ［プローブの作成］ページで、プローブの名前を入力します。
3. スケジュールを選択します:

a) プローブを実行する曜日を選択します。
b) プローブを実行する開始時刻を入力します。
c) また、［**1** 日での繰り返し］オプションを選択できます。終了時間と、プローブを 1 日の間に繰り返す間隔を入力します。たとえば、以下の構成にすると、毎週火曜日、木曜日、金曜日の 12 時 10 分から 23 時 35 分まで、1 時間ごとにデスクトッププローブを実行できます。

4. この間隔に応じて、推奨されるプローブ対象デスクトップの数を選択します。
5. プローブを実行する必要があるエンドポイントマシンを選択します。
6. プローブのエラー結果が送信されるメールアドレスを入力し、［保存］をクリックします。

この構成では、デスクトップセッションは毎週火曜日、木曜日、金曜日の 23 時 10 分まで、12 時 10 分、13 時 10 分、14 時 10 分などの時間に起動します。



> 注:
>
> - ［アラート］ > ［メール サーバー構成］でメールサーバーを構成してください。
> - デスクトッププローブの構成が完了すると、エージェントは次の 1 時間から構成されたプローブを実行します。
> - ［**1** 日での繰り返し］オプションが導入される前にセットアップされたプローブは、スケジュールされた時間に引き続き実行されます。［**1** 日での繰り返し］オプションは、デフォルトで無効になっています。

手順 **3**: プローブの実行

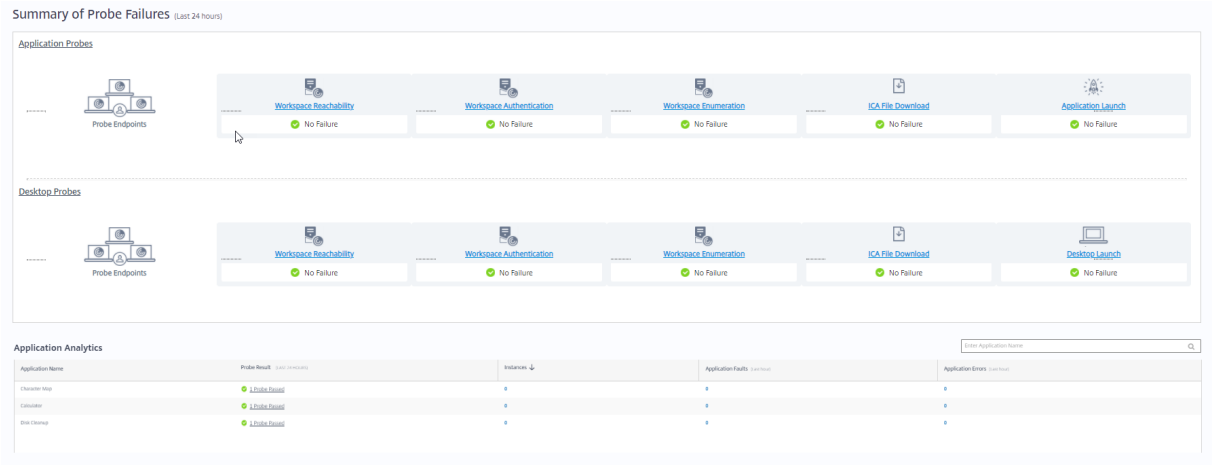
エージェントは、［監視］から定期的にフェッチするプローブ構成に従ってデスクトッププロービングを実行します。Workspace を使用して、選択したデスクトップを連続して起動します。エージェントは、監視データベースを介して［監視］に結果を報告します。エラーは、以下の 5 つの特定の段階で報告されます:

- **Workspace** の到達可能性 - 構成された Workspace URL に到達できません。
- **Workspace** の認証 - 構成された Workspace の資格情報が無効です。

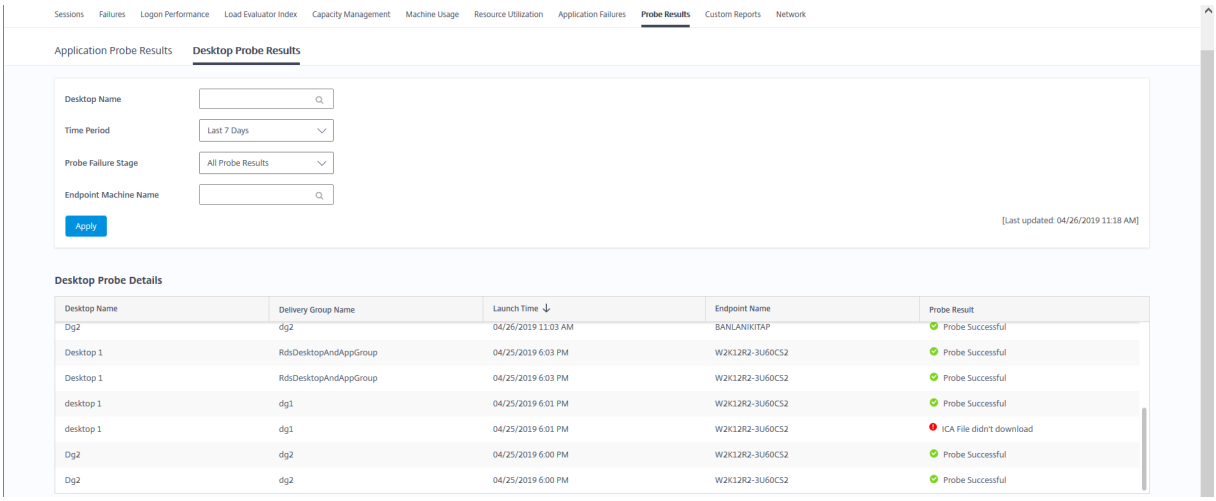
- **Workspace** の列挙 - Workspace で列挙されるデスクトップの一覧には、調査対象のデスクトップが含まれていません。
- **ICA** のダウンロード - ICA ファイルは使用できません。
- デスクトップ起動 - デスクトップを起動できません。

手順 **4**：プローブの結果を表示する

最新のプローブ結果は、［デスクトップ］ページで確認できます。



さらにトラブルシューティングするには、プローブの結果のリンクをクリックして、［傾向］ > ［プローブの結果］ > ［デスクトッププローブの結果］ページで詳細を表示します。



統合されたプローブの結果データは、このページの過去 24 時間または過去 7 日間の期間に使用できます。プローブが失敗した段階がわかります。この表をフィルタリングして、特定のデスクトップ、プローブの障害が発生した段階、またはエンドポイントマシンを確認することができます。

マシンのトラブルシューティング

May 17, 2024

> 注:
>
> **Citrix Health Assistant** は、未登録の VDA の構成に関する問題をトラブルシューティングするためのツールです。このツールは、いくつかのヘルスチェックを自動化して、セッションの起動やタイムゾーンリダイレクトの構成での VDA の登録の失敗や問題の根本原因を特定します。Knowledge Center の記事「Citrix Health Assistant - VDA の登録とセッションの起動のトラブルシューティング」には、**Citrix Health Assistant** ツールのダウンロード方法と使用方法が記載されています。

[監視] タブの [フィルター] **>** [マシン] ビューには、そのサイトに構成されているマシンが表示されます。また、[マルチセッション OS マシン] タブには負荷評価基準インデックスが表示され、その測定値上にマウスポインターを置くと各パフォーマンスカウンターの測定値やセッション数がツールチップとして表示されます。

登録に失敗したマシンの [失敗の理由] 列をクリックすると、失敗の詳細な説明とその失敗をトラブルシューティングするための推奨手順が表示されます。マシンおよび接続でエラーが発生した場合のエラーの理由と推奨される解決手順は、『Citrix Director Failure Reasons Troubleshooting Guide』に記載されています。

マシン名のリンクをクリックし、[マシンの詳細] ページに移動します。

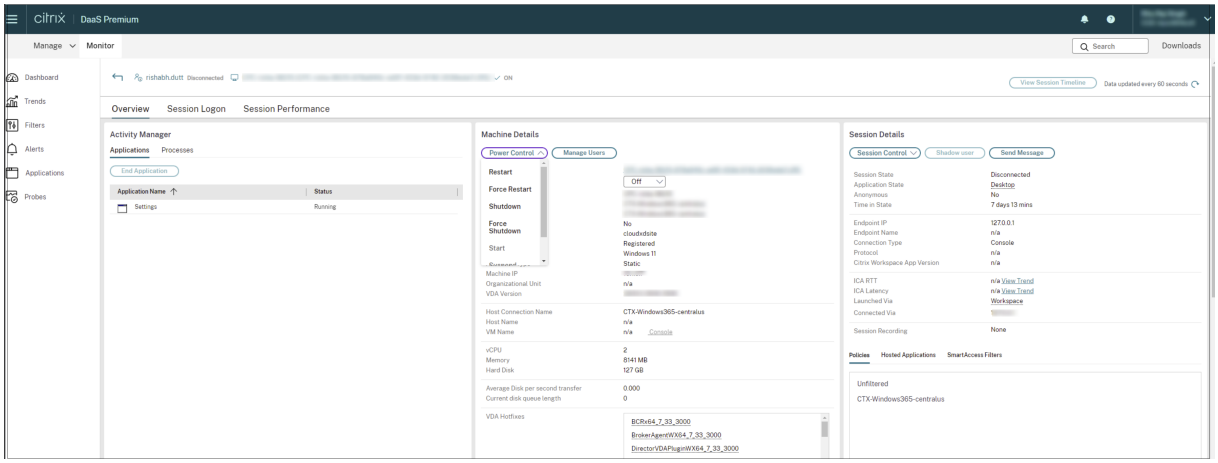
[マシンの詳細] ページには、マシンの詳細、インフラストラクチャの詳細、およびマシンに適用済みの HotFix の詳細の一覧が表示されます。

HDX Plus for Windows 365 クラウド **PC** および **Azure Virtual Desktop** のサポート:

> 注:
>
> HDX Plus for Windows 365 クラウド PC の場合、[再起動] および [強制再起動] の電源制御オプションのみが使用可能です。Azure Virtual Desktop（AVD）では、すべての電源制御オプションが利用可能です。

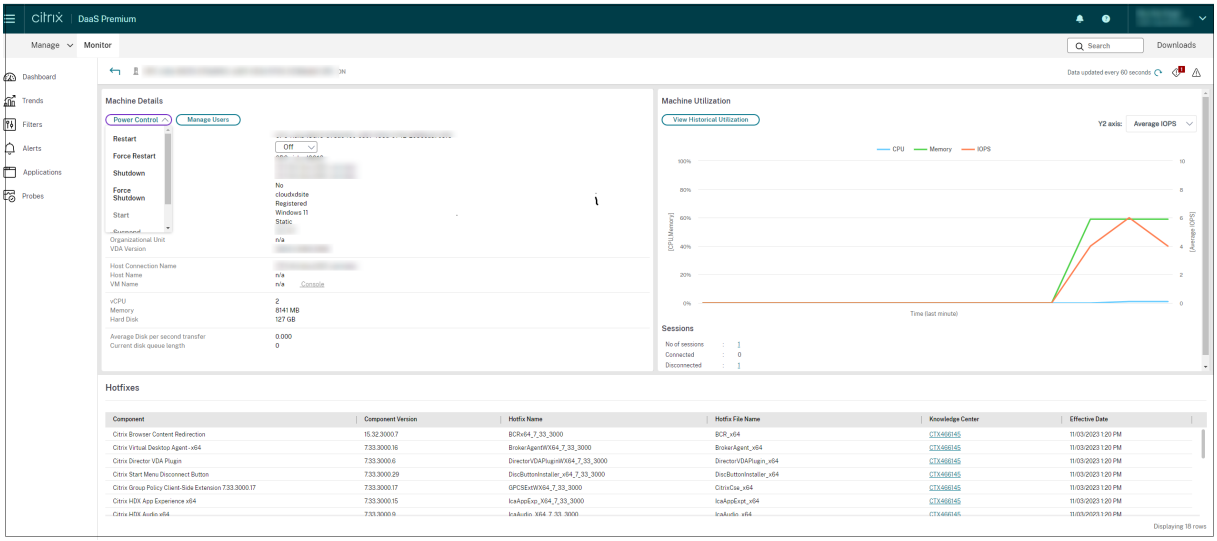
次のいずれかの方法を使用して、利用可能な電源制御オプションを表示できます:

[フィルター] > [セッション] > [詳細の表示] > [マシンの詳細] > [電源制御] ドロップダウンリストの順にクリックし、オプションを選択して、マシンに必要な電源制御オプションを割り当てます。



または、

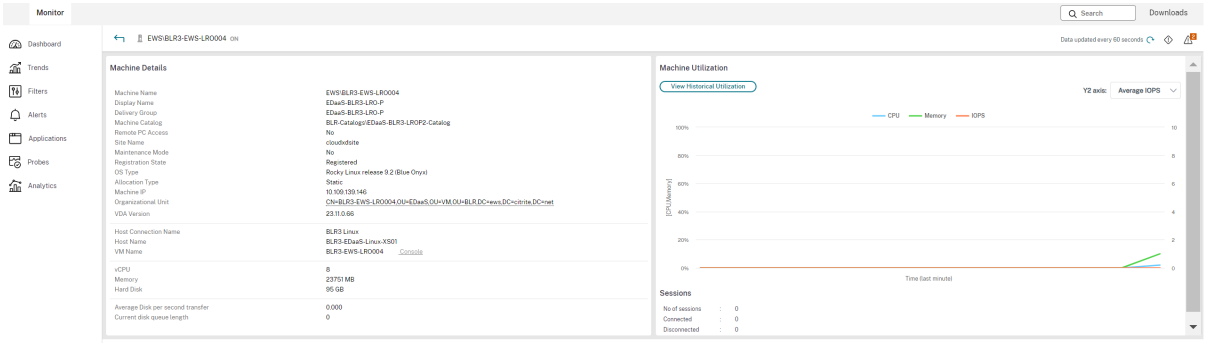
[フィルター] > [マシン] > [マシンの詳細] > [電源制御] ドロップダウンリストの順にクリックし、オプションを選択して、マシンに必要な電源制御オプションを割り当てます。



マシンごとのリアルタイムのリソース使用状況

[マシン稼働] パネルには、CPU とメモリのリアルタイムの使用状況を示すグラフが表示されます。VDA のバージョン 7.14 以降がインストールされているサイトでは、ディスクと GPU の監視グラフも表示されます。

重要なパフォーマンス測定値としてディスク監視グラフ、平均 IOPS、ディスク遅延があり、VDA ディスク関連の問題をモニターし解決する上で役立ちます。[平均 IOPS] グラフには、ディスクの読み取りおよび書き込みの平均回数が表示されます。[ディスク遅延] を選択すると、データが要求されてディスクから返されるまでの時間をミリ秒単位で示すグラフが表示されます。



GPU 使用率

[**GPU** 使用率] を選択すると GPU、GPU メモリ、およびエンコーダーとデコーダーの使用率がパーセント値として表示され、マルチセッションおよびシングルセッション OS の VDA での GPU に関連した問題を解決できます。

サポートされる **GPU** バージョン:

- ディスプレイ ドライバー バージョン 369.17 以降を実行する NVIDIA Tesla M60 GPU。詳しくは、NVIDIA vGPU Softwareを参照してください。
- AMD Radeon Instinct MI25 GPU および AMD EPYC 7V12（Rome）CPU。詳しくは、AMD ドライバーとサポートを参照してください。

ドライバー:

適切なドライバーまたは拡張機能が VDA にインストールされている必要があります。

- NVIDIA GPU の場合、GRID ドライバーを手動で、または拡張機能によってインストールします。詳しくは、NVIDIA vGPU Softwareを参照してください。
  - NVIDIA の場合、GRID ドライバーのみがサポートされていることに注意してください。CUDA ドライバーは NVadsA10 v5 シリーズでは動作せず、サポートされていません。
  - Azure ベースのマシンに拡張機能によって Nvidia Grid GPU ドライバーをインストールするプロセスのサンプルについては、「NVIDIA GRID ドライバー」を参照してください。NVIDIA GPU ドライバー拡張機能 - Azure Windows 仮想マシン - Azure 仮想マシン。
  - Nvidia Grid GPU ドライバーを手動でインストールするプロセスのサンプルについては、「Windows を実行している N シリーズ VM に NVIDIA GPU ドライバーをインストールする」を参照してください。
- AMD GPU の場合、AMD グラフィックドライバーを手動で、または拡張機能によってインストールします。詳しくは、AMD ドライバーとサポートを参照してください。
  - Azure ベースのマシンに拡張機能によって AMD GPU ドライバーをインストールするプロセスのサンプルについては、「Windows 用の AMD GPU ドライバー拡張機能」を参照してください。
  - Azure マシンに AMD GPU ドライバーを手動でインストールするプロセスのサンプルについては、「Windows を実行している N シリーズ VM に AMD GPU ドライバーをインストールする」を参照してください。

使用上の注意:

- GPU 使用率グラフは、64 ビット Windows を実行している VDA でのみ使用できます。
- AMD GPU 使用率グラフは、Citrix Virtual Apps and Desktops 7 2212 以降を実行している VDA でのみ使用できます。
- VDA で GPU アクセラレーションを使用するには、HDX 3D Pro を有効にする必要があります。詳しくは、「Windows シングルセッション OS のための GPU アクセラレーション」および「Windows マルチセッション OS のための GPU アクセラレーション」を参照してください。
- VDA が 1 つ以上の GPU にアクセスしている場合、［GPU 使用率］グラフには個々の GPU から収集された GPU 測定値の平均が表示されます。GPU 測定値は、個々のプロセスではなく VDA 全体について収集されます。
- AMD の場合、エンコーダーとデコーダーの使用は個別にはサポートされていません。GPU を使用するエンコーディング/デコーディングのワークロードは、GPU 使用率で一般的な 3D 負荷として報告されます。
- インストール中に NVIDIA WMI をインストールするようにしてください。このウィンドウは、手動インストール中にのみ使用できます。
- ドライバーがインストールされているが、Director が GPU を検出しない場合
  - タスクマネージャーを確認してください。ドライバーが正しくインストールされていれば、GPU がタスク マネージャーに表示されます。
  - マシンが登録されていることを確認してください。マシンがオンラインとして検出されるまでに時間がかかる場合があります。
- Director で GPU の使用率にアクティビティが表示されない場合は、実行中のワークロードが GPU を使用していることを確認してください。グラフィックワークロードは、［Settings］>［System］>［Display］>［Graphics Settings］で基本設定を設定するアプリを選択して、有効にできます。必ず高パフォーマンスを有効にしてください。場合によっては、他の設定に基づいて Windows がシステムのデフォルトまたは省電力に設定されている場合、デフォルト設定でグラフィックワークロードに CPU を使用することがあります。
- データは毎分更新され、**GPU** 使用率を選択してから 1 分以内にデータの視覚化が開始されます。

マシンごとの過去のリソース使用状況

［マシン稼働］パネルの ［履歴使用率の表示］をクリックすると、選択したマシンでのリソースの使用履歴を確認できます。
使用率グラフには、CPU、メモリ、最大同時セッション数、平均 IOPS、ディスク遅延などの重要なパフォーマンス測定が表示されます。

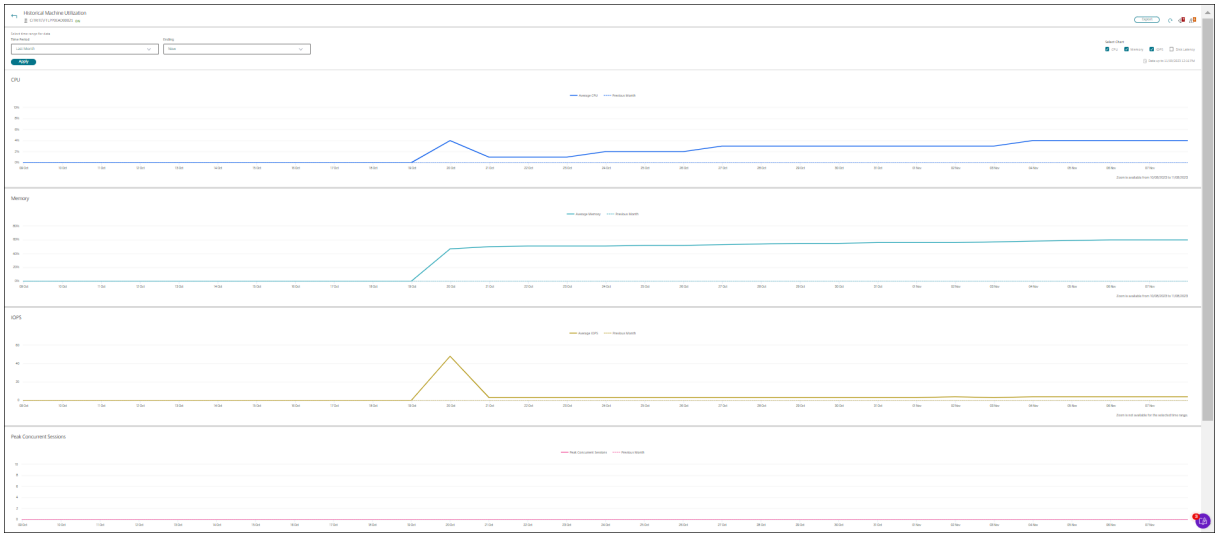
> 注:
>
> データを収集して［マシン使用率の履歴］ページの［上位 10 位のプロセス］表に表示するには、監視ポリシーの ［プロセスの監視を有効にします］設定を［許可］に設定する必要があります。この設定はデフォルトでは［禁止］に設定されています。

デフォルトでは、CPU とメモリの使用率、平均 IOPS、ディスク遅延に関するデータが収集されます。この収集は、［リソースの監視を有効にします］ポリシー設定で無効にできます。

1. ［マシンの詳細］ビューの ［マシン稼働］パネルから、［履歴使用率の表示］を選択します。
2. ［マシン使用率の履歴］ページで、［期間］で、使用率を表示する期間を過去 2 時間、過去 24 時間、過去 7 日間、過去 30 日間、または過去 1 年から選択します。

   > 注:
   >
   > 現在、平均 IOPS とディスク遅延のデータについては、過去 24 時間、過去 30 日間、過去 1 年についてのみ表示できます。カスタムの終了時刻は使用できません。

3. ［適用］をクリックして、目的のグラフを選択します。
4. グラフの他のセクションにマウスを合わせると、選択した期間の詳細が表示されます。



たとえば、［過去 **2** 時間］を選択すると、基準の期間は選択した時間範囲の 2 時間前になります。過去 2 時間と基準期間の CPU、メモリ、およびセッションの傾向を表示します。［過去 **1** か月］を選択すると、基準期間は過去 1 か月間になります。これを選択すると、先月から基準日時までの平均 IOPS およびディスク遅延が表示されます。

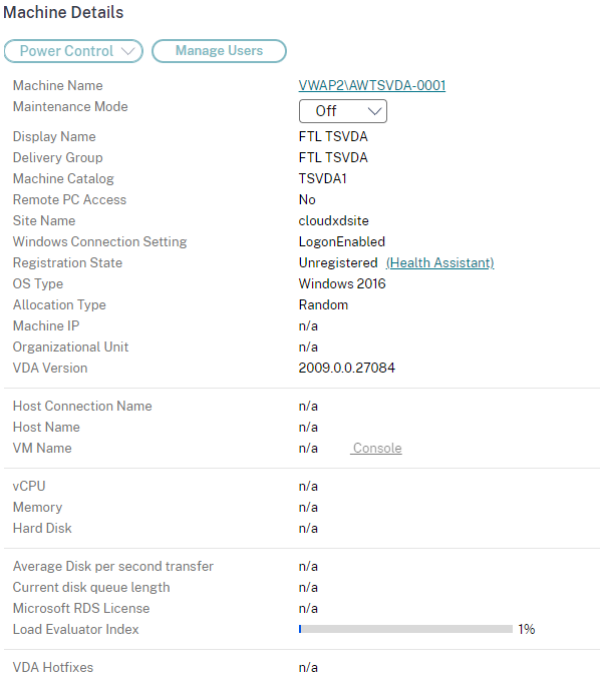
1. 選択した期間のリソース使用状況データをエクスポートするには、［エクスポート］をクリックします。詳しくは、「展開環境の監視」の「レポートのエクスポート」セクションを参照してください。
2. グラフの下には、CPU とメモリの使用率が上位 10 位のプロセスを示すテーブルが表示されます。選択した時間範囲のアプリケーション名、ユーザー名、セッション ID、平均 CPU、ピーク時の CPU、平均メモリ、ピーク時のメモリが表示される列から任意の列を選択してソートできます。［平均 IOPS］列と［ディスク遅延］列は並び替えできません。

   > 注:
   >
   > - システムプロセスのセッション ID は「0000」と表示されます。
   > - Citrix Cloud Japan または Citrix Cloud Government プレーンに属するサイトに 5,000 台を超えるマシンが含まれる場合、プロセスデータは最大 2,000 台のマシンについてのみ使用できます。これらのマシンではプロセス監視ポリシーを有効にする必要があります。

3. 特定プロセスのリソース消費に関する履歴傾向を表示するには、上位 10 位のプロセスから任意のプロセスを選択してドリルダウンします。

マシンコンソールへのアクセス

XenServer Version 7.3 以降でホストされているシングルセッション OS マシンおよびマルチセッション OS マシンのコンソールに、［監視］から直接アクセスできます。このため、XenServer がホストする VDA での問題を解決するために XenCenter を使用する必要はありません。この機能を使用するには、マシンをホストする XenServer がバージョン 7.3 以降で、［監視］からアクセスできる必要があります。



マシンのトラブルシューティングを行うには、対応する［マシンの詳細］パネルで ［コンソール］リンクをクリックします。提供したホスト資格情報が認証されると、Web ベースの VNC クライアントである noVNC を使用して、別のタブでマシンコンソールが開きます。これで、キーボードとマウスでコンソールにアクセスできるようになりました。

> 注:
>
> - この機能は、Internet Explorer 11 ではサポートされていません。
> - マシンコンソール上のマウスポインターの位置がずれている場合は、CTX230727で、問題を解決する手順を参照してください。
> - 新しいタブでコンソールアクセスを起動し、Web ブラウザー設定でポップアップが許可されていることを確認します。
> - セキュリティ上の理由から、Web ブラウザーに SSL 証明書をインストールすることを Citrix ではお勧めします。

最近電源操作を行ったマシンを検査する

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

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

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

次の方法を使用して、マシンの電源操作状態を表示できます:

［フィルター］ -> ［マシン］タブ。この場合、デフォルトでは、電源動作時間列と電源操作の結果列が表示されます。表示する列を選択することもできます。

［コストの最適化］タブ。この場合、デフォルトのフィルターは、［電源操作のトリガー］が ［*Autoscale*］に設定され、［電源操作の結果］が ［失敗］に設定されます。

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

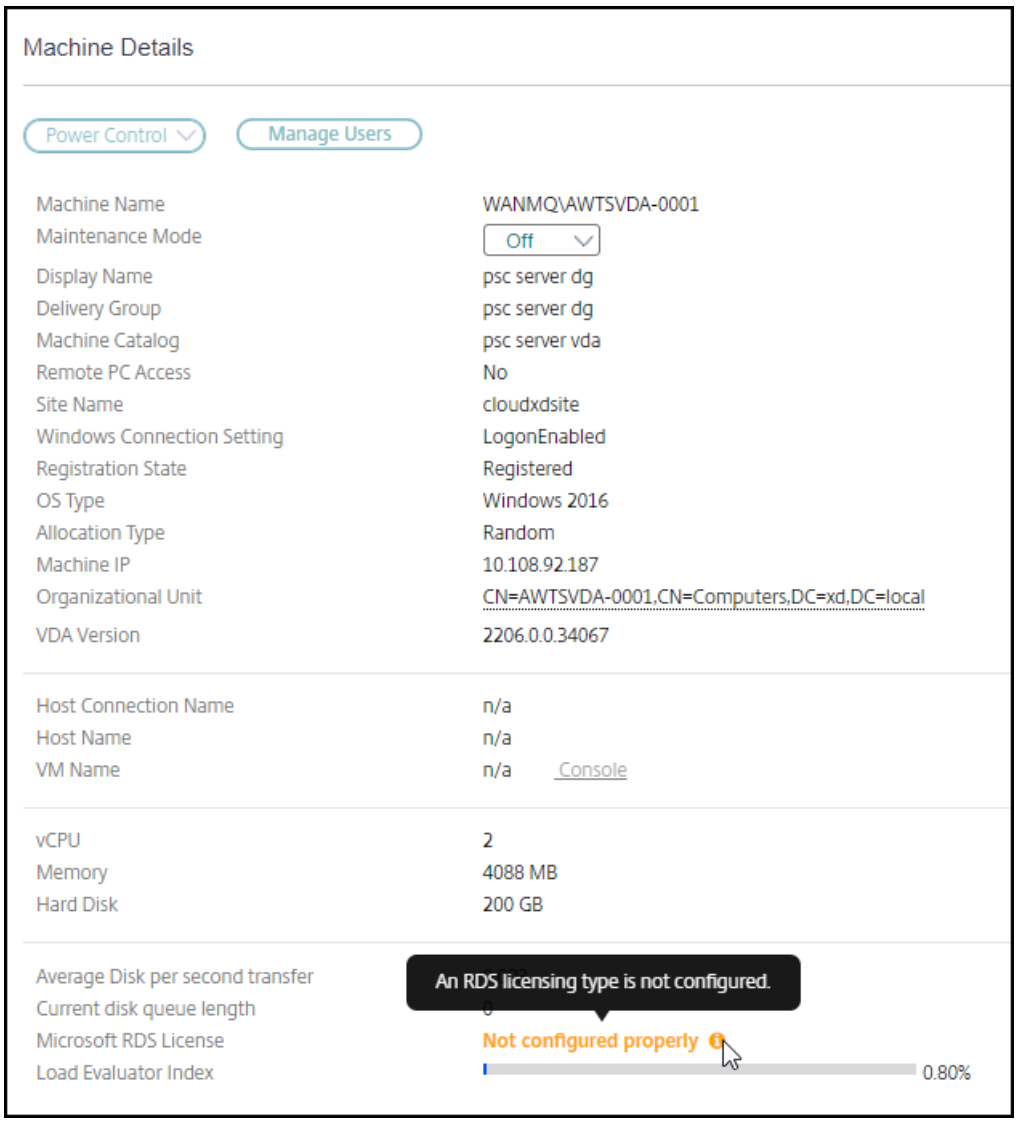
電源操作状態を表示するために、次のフィルターが追加されています:

フィルター	説明
電源操作の結果	電源操作の結果を表示します。使用可能なフィルター値は成功と失敗です。
電源操作のトリガー	誰が、または何が電源操作をトリガーしたかを表示します。使用可能なフィルター値は次のとおりです • Autoscale - この値は、以下によって電源操作がトリガーされたときに表示されます • 管理者が仮想マシンをシャットダウンして、仮想マシンの OS ディスクを初期状態に戻すとき • 設定されたポリシーに基づいて仮想マシンがシャットダウンまたは一時停止されたとき • プールサイズまたはバッファサイズの構成に基づいて仮想マシンが使用可能になったとき • 管理者 - この値は、電源操作が管理者によってトリガーされたときに表示されます。考えられる例としては、管理者が VM の電源オフ、電源オン、一時停止、再開、または再起動を要求した場合です。 • ユーザー - この値は、ユーザーによって電源操作がトリガーされたときに表示されます。例としては、ユーザーが仮想マシンをリセット、オンにしたとき、または仮想マシン上での作業を再開する場合があります。

フィルター	説明
	• そのほか - この値は、電源操作がスケジュールされた、または不明な理由によってトリガーされた場合に表示されます。
最後の電源操作	電源オン、電源オフ、シャットダウン、再起動、リセット、再開など、マシンで発生した電源操作を正確に表示します。
電源動作時間	電源操作が完了した時刻。可能なフィルター値は、過去 1 分間、過去 5 分間、過去 30 分間、過去 1 時間、今日、過去 24 時間、および昨日です。
電源操作の失敗の理由	失敗した理由が表示されます。可能なフィルター値は、ハイパーバイザーがエラーを報告した、ハイパーバイザーのレート制限を超えました、不明なエラー、およびなし、です。成功した操作がある場合は、「なし」と表示されます。

Microsoft RDS ライセンスの正常性

マルチセッション OS マシンの ［マシンの詳細］ページと ［ユーザーの詳細］ページの［マシンの詳細］パネルに、Microsoft RDS（Remote Desktop Services）のライセンスの状態を表示できます。



次のいずれかのメッセージが表示されます：

- ライセンスを使用できます
- 正しく構成されていません（警告）
- ライセンスエラー（エラー）
- 非互換 VDA バージョン（エラー）

> 注：
>
> 有効なライセンスのある猶予期間中のマシンの RDS ライセンス正常性の状態には、［ライセンスを使用できます］のメッセージが緑色で表示されます。有効期限が切れる前にライセンスを更新してください。

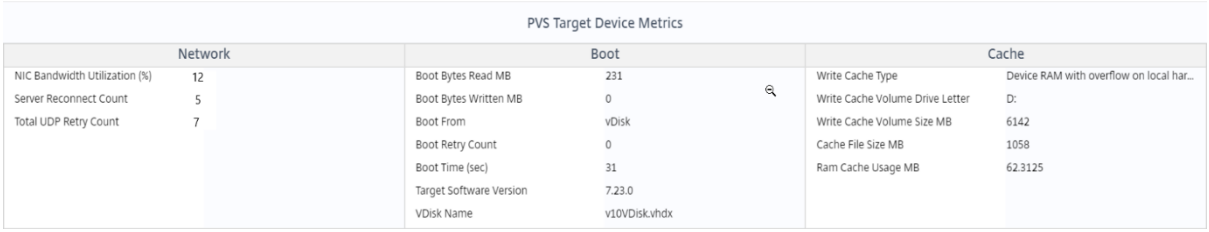
警告メッセージとエラーメッセージの場合、情報アイコンの上にカーソルを置くと、次の表に示す詳細情報が表示されます。

メッセージの種類	［監視］内のメッセージ
エラー	VDA バージョン 7.16 以降で使用可能
エラー	新しい RDS 接続は許可されていません。
エラー	RDS ライセンスの猶予期間が終わりました。
エラー	ライセンスサーバーが、クライアントアクセスライセンス（接続デバイス数）の種類で必要な OS レベル用に構成されていません。
エラー	構成されたライセンスサーバーは、クライアントアクセスライセンス（接続デバイス数）の RDS ホスト OS レベルと互換性がありません。
警告	パーソナルターミナルサーバーは Citrix Virtual Apps and Desktops 展開で有効な RDS ライセンスの種類ではありません。
警告	管理用リモートデスクトップは Citrix Virtual Apps and Desktops 展開で有効な RDS ライセンスの種類ではありません。
警告	RDS ライセンスの種類は構成されていません。
警告	RDS クライアントアクセスライセンス（接続ユーザー数）の種類では、ドメインコントローラーまたはライセンスサーバーに接続できません。
警告	ライセンスの種類がクライアントアクセス（接続デバイス数）の場合、必要な OS レベルのライセンスサーバーに接続できないため、クライアントデバイスライセンスを確認できません。

> 注:
>
> この機能は、Microsoft RDS CAL（クライアントアクセスライセンス）にのみ適用されます。

PVS ターゲットデバイスメトリック

［監視］の ［マシンの詳細］ページでシングルセッション OS マシンおよびマルチセッション OS マシンの PVS ターゲットデバイスの状態を表示できます。このパネルでは ［ネットワーク］、［起動］、［キャッシュ］のさまざまなメトリックを表示できます。これらのメトリックは、PVS ターゲットデバイスを監視およびトラブルシューティングして、PVS ターゲットデバイスが稼働していることを確認するのに役立ちます。



ネットワーク：

- ネットワーク帯域幅使用率：すべての NIC での平均帯域幅使用率
- サーバーの再接続回数：ネットワークの問題、サーバーの再配分またはシャットダウンによって、および Citrix Provisioning Stream Service の再起動によってサーバーが再接続した回数。
- 合計 UDP 再試行回数：Provisioning ターゲットデバイスが UDP を使用して Provisioning サーバーに再接続を試行した回数。このメトリックは、Citrix Provisioning Stream Service でネットワークに問題があるかどうか（スイッチ構成が間違っている場合など）を把握するのに役立ちます。

起動：

- 起動 - 読み取りバイト数（MB）：起動中に読み取られたバイト数。
- 起動 - 書き込みバイト数（MB）：起動中に書き込まれたバイト数。
- 起動元：起動メディア（vDisk、ローカルディスクなど）。
- 起動 - 再試行回数：マシンを起動するための再試行回数。
- 起動時間：マシンの起動にかかった時間（秒単位）。デフォルトでは、再試行間隔は 5 秒です。この遅延が 2 桁になると、起動時間が大幅に増加します。この問題を解決するには、Provisioning の構成を確認してください。
- ターゲットのソフトウェアバージョン：Provisioning ターゲットデバイスのソフトウェアのバージョン。
- vDisk 名：Provisioning ターゲットデバイスを起動する vDisk。

キャッシュ：

- 書き込みキャッシュの種類：vDisk は異なる種類のキャッシュに設定できます。詳しくは、Knowledge Center のCTX119469を参照してください。
- 書き込みキャッシュのボリュームドライブ文字：ドライブを使用する書き込みキャッシュのドライブ文字。
- 書き込みキャッシュのボリュームサイズ（MB）：書き込みキャッシュで構成されたボリュームサイズの合計。
- キャッシュファイルサイズ（MB）：現在のキャッシュファイルサイズ（ハードディスクへのオーバーフローありでデバイス RAM にキャッシュする）。
- RAM キャッシュ使用量（MB）：現在の RAM キャッシュサイズ（ハードディスクへのオーバーフローありでデバイス RAM にキャッシュする）。ディスクへのオーバーフローは、必要な場合にのみ使用します。このメトリックは、RAM キャッシュの適切なサイズを設定または最適化する場合に役立ちます。

詳しくは、「ターゲットデバイスでのステータストレイの使用方法」を参照してください。

Provisioning ターゲットデバイスのメトリックは、以下でのみ使用できます:

- マシンのプロビジョニング。
- Provisioning ターゲットデバイスバージョン 7.19 以降。
- VDA バージョン 2003 以降。

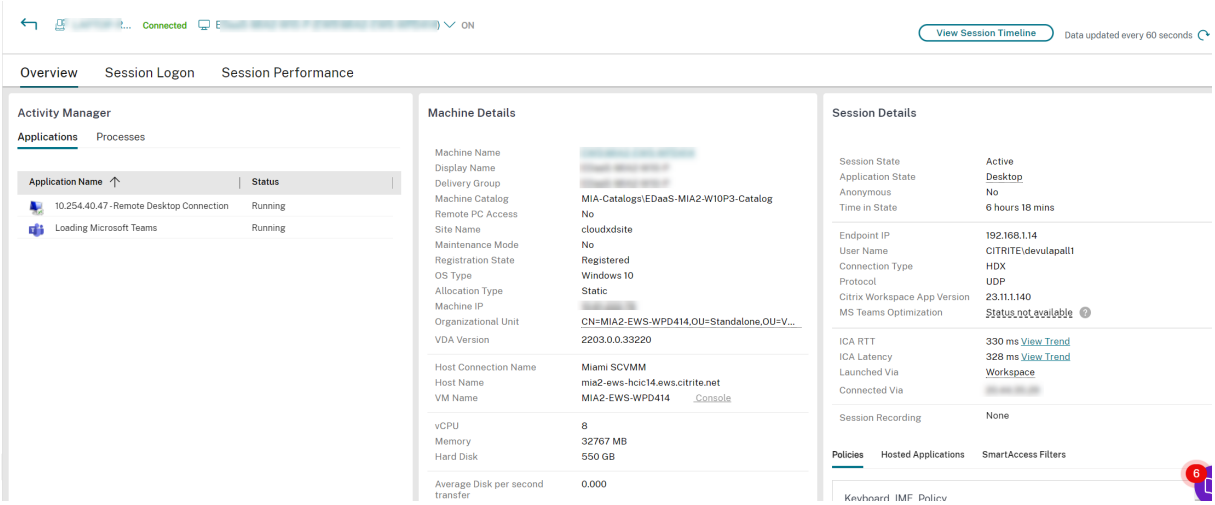
> 注:
>
> サーバーの再接続回数および UDP 再試行回数のメトリックは Provisioning ターゲットバージョン 1912 CU2 以降でのみ利用できます。

ユーザーの問題のトラブルシューティング

May 17, 2024

[監視] の [アクティビティマネージャー] ページにある [ヘルプデスク] ビューを使って、ユーザーまたはエンドポイントに関する情報を確認します。

ユーザーのアクティビティマネージャーから [詳細を表示] をクリックすると、[ユーザーの詳細] ページが開きます。エンドポイントのアクティビティ マネージャーから [詳細を表示] をクリックすると、[**Endpoint Details**] ページが開きます。



ユーザーが複数のセッションを開始した場合は、セッションセレクタが表示されます。

詳細を表示したいセッションを選択します。

- セッション、ユーザーのサインインエクスペリエンス、セッションの開始、接続、およびアプリケーションに関する詳細を確認できます。
- ユーザーのマシンをシャドウすることができます。
- 次の表に示す方法で問題のトラブルシューティングを行い、必要な場合は問題を担当の管理者に報告する。

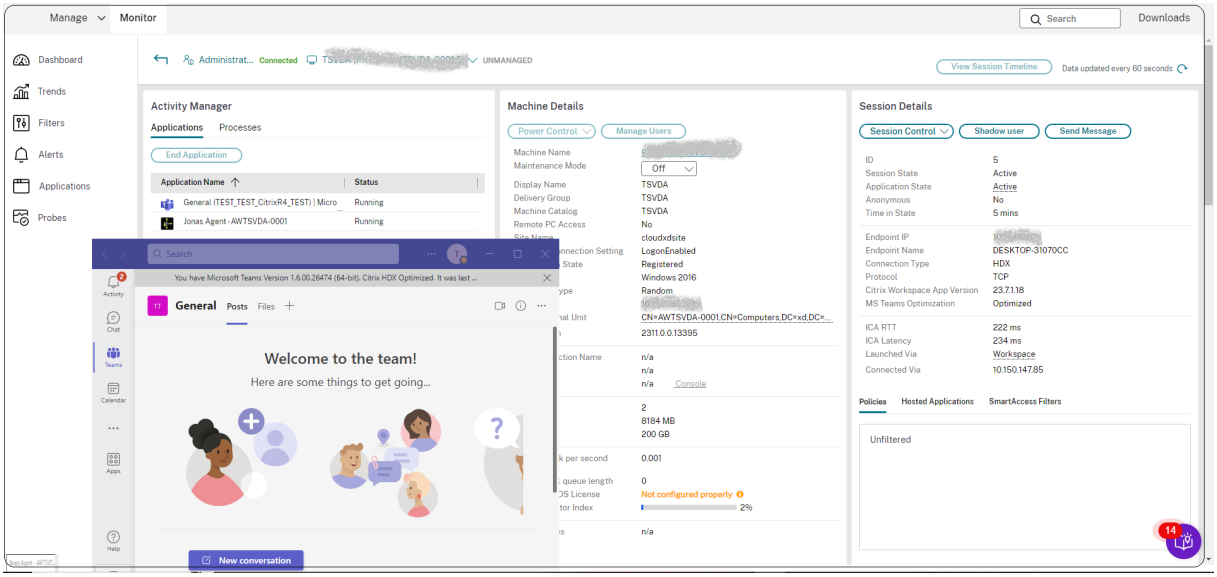
Microsoft Teams の最適化の状態

Citrix Monitor は、［ユーザーの詳細］ページ > ［セッションの詳細］パネル > ［**MS Teams** の最適化］フィールドで、HDX セッションの Microsoft Teams の最適化の状態を表示します。Microsoft Teams の最適化は、クリアな音声やビデオなどのユーザーエクスペリエンスを向上させるために重要です。Microsoft Teams の最適化の状態を可視化することは、チケットの解決に必要な時間を短縮するのに役立ち、管理者がトラブルシューティング中に重要なメトリックを特定するのに役立ちます。

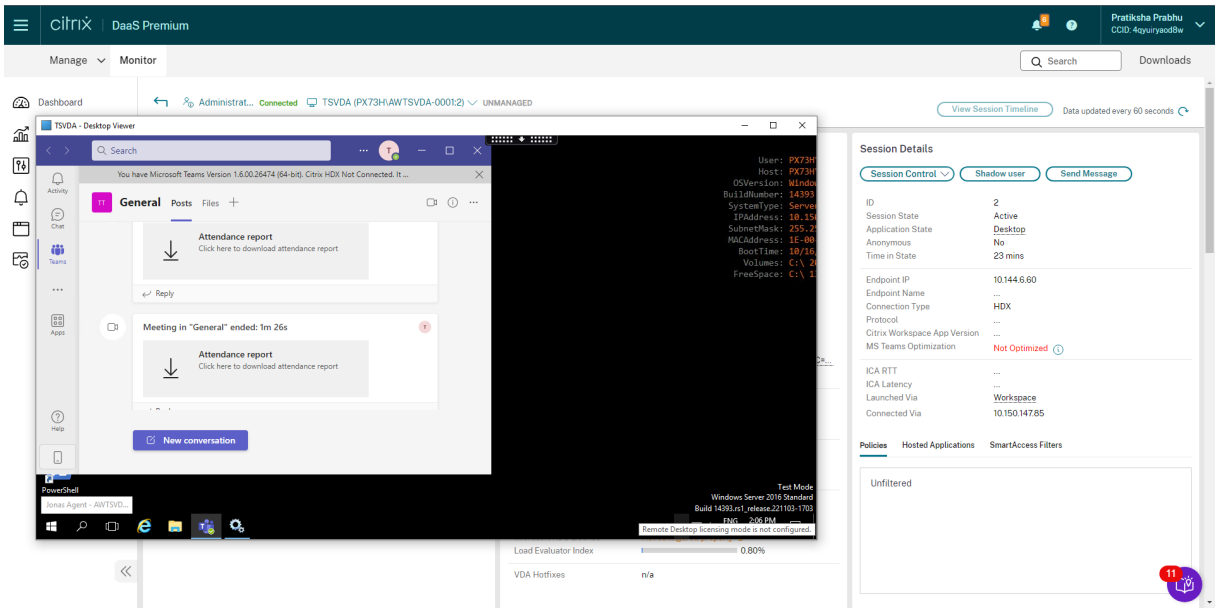
> 注:
>
> Citrix Monitor は、Microsoft Teams バージョン 2.1 以前をサポートします。

前提条件:

- サポートされている Citrix Workspace アプリのバージョンは、「Microsoft Teams の最適化」に記載されています。
- Microsoft Teams は、公開アプリとして、または公開デスクトップ内で実行されます。
- Citrix HDX HTML5 ビデオリダイレクトサービスなどの重要なサービスが実行されています。



Microsoft Teams が最適化されていない場合、ヒントには、Microsoft Teams を最適化するためのヒントを含む HDX の外部トラブルシューティングライブ記事へのリンクが表示されます。「HDX 最適化のトラブルシューティング」。



トラブルシューティングのヒント

ユーザーの問題	提案
ログオンに時間がかかる。断続的もしくは繰り返し失敗する	ユーザーログオンの問題の診断

ユーザーの問題	提案
セッションの開始に時間がかかる。断続的もしくは繰り返し失敗する	セッション起動の問題の診断
セッションの確立に関係するコンポーネントを特定する	［セッショントポロジ］ビューの分析
セッションの応答が遅い、または応答しない	セッションのパフォーマンスの問題を診断する
アプリケーションが遅い、または応答しない	アプリケーション障害の解決
接続に失敗した	デスクトップ接続の復元
セッションが遅いまたは応答しない	セッションの復元
ビデオが遅いまたは画質が悪い	HDX チャネルシステムレポートの実行

> 注:
>
> ［ユーザーの詳細］ビューの［マシンの詳細］パネルで、マシンがメンテナンスモードになっていないことを確認してください。

セッションパフォーマンス

［セッションパフォーマンス］タブでは、ユーザーセッション内の問題を特定する際にリアルタイムで指標を相関させる機能をはじめ、トラブルシューティングのワークフローが強化されています。［セッションのトポロジ］パネルは、接続された HDX セッションのセッション内パスを視覚的に表現します。［パフォーマンスメトリック］パネルは、ICARTT、ICA 遅延、フレーム数/秒、利用可能な出力帯域幅、消費された出力帯域幅などのセッションメトリックの傾向を提供し、これらの指標が時間の経過とともにどのように実行されたかを把握するのに役立てることができます。詳しくは、「セッションパフォーマンスの問題を診断する」を参照してください。

検索のヒント

ユーザー名の検索は、構成されているすべての Active Directory を横断して行われます。

［検索］フィールドにマルチユーザーマシンの名前を入力すると、そのマシンの［マシンの詳細］ページが開きます。

［検索］フィールドにエンドポイントの名前を入力すると、そのエンドポイントに接続している認証が不要なユーザー（匿名ユーザー）セッションおよび認証が必要なセッションを検索できます。この一覧により、匿名ユーザーセッションのトラブルシューティングを行うことができます。匿名ユーザーセッションのトラブルシューティングを行うには、エンドポイント名が重複していないことが重要です。

検索結果には、現在マシンを使用していないユーザーや、マシンに割り当てられていないユーザーも含まれます。

- 検索では大文字と小文字は区別されません。
- 検索語の一部を入力すると、一致する候補が一覧で表示されます。

- 2 つの部分で構成された名前の何文字かをスペースで区切って入力すると、両方の文字列と一致する項目が検索されます。2 つの部分で構成された名前の例には、ユーザー名、姓と名、または表示名があります。たとえば、「jo rob」と入力すると、「John Robertson」や「Robert, Jones」などが検索されます。

ホームページに戻るには、［監視］タブをクリックします。

セッション起動の問題の診断

February 19, 2024

［監視］には「ユーザーログオンの問題の診断」セクションに記載されているログオンプロセスのフェーズだけでなく、セッション開始時の実行時間も表示されます。この時間は ［ユーザーの詳細］ページの［Workspace アプリのセッション開始時間］と、［エンドポイント詳細］ページの［VDA のセッション開始時間］に分かれます。この 2 つの時間にはフェーズの情報も含まれていて、各フェーズの実行時間も確認できます。このデータはセッションの開始時間が長い場合に問題を把握し、トラブルシューティングを行うのに役立ちます。また、セッションの開始プロセスを構成する各フェーズの実行時間の情報は、それぞれのフェーズに関連する問題のトラブルシューティングに有効です。たとえばドライブマッピングの時間が長い場合は、有効なすべてのドライブが GPO に正しくマップされているかを確認するか、スクリプトを確認するという対処ができます。

前提条件

セッションの開始時間を表示するには、以下の条件を満たしている必要があります:

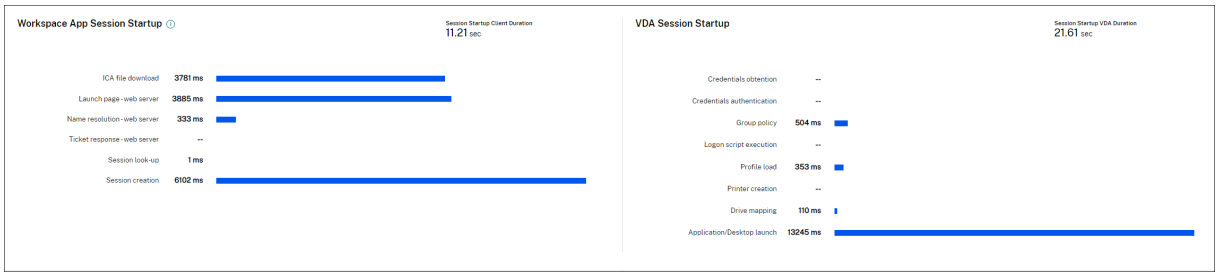
- VDA のバージョン 1903 以降。
- EUEM（End User Experience Monitoring：エンドユーザー状況監視）サービスが VDA で実行されている。

制限事項

［監視］でセッションの開始時間を表示する場合は、以下の制限が適用されます:

- セッションの開始時間は HDX セッションでのみ確認できます。
- iOS および Android OS から開始したセッションについては、セッション開始時の VDA の実行時間のみ確認できます。
- IFDCD は、Web ブラウザーからの起動時に Workspace アプリが検出された場合にのみ使用できます。
- macOS から開始したセッションで IFDCD を使用するには、Workspace アプリのバージョン 1902 以降が必要です。
- Windows OS から開始したセッションで IFDCD を使用するには、Workspace アプリのバージョン 1902 以降が必要です。それ以前のバージョンで IFDCD を表示するには、Workspace アプリが検出された状態で Web ブラウザーからアプリを起動する必要があります。

> 注:
>
> - 条件が整っているにもかかわらずセッションの開始時間を表示するのに問題がある場合は、CTX130320の記事を参考にして監視サーバーのログと VDA のログを確認してください。
>   共有セッション（複数のアプリケーションが同一セッションで起動された状態）では、Workspace アプリの開始メトリックには最新の接続または最新のアプリケーション起動についての情報が表示されます。
> - VDA セッションの開始では、再接続時には適用されないメトリックがあります。その場合はメッセージが表示されます。



Workspace アプリでのセッションの開始フェーズ

セッション開始時のクライアントの実行時間（**SSCD**）

このメトリックの値が高い場合は、開始時間が長くなる要因がクライアント側にあることを示しています。問題の根本的な原因を特定するには、後に続くメトリックを調査します。SSCD は、要求が発生した瞬間に可能な限り近いタイミング（マウスのクリック）を起点とし、クライアントデバイスと VDA をつなぐ ICA 接続が確立されたタイミングを終点とします。共有セッションの場合は、サーバーとの接続を新たに確立するときのセットアップコストがそれほど生じないため、この時間は大幅に短くなります。次のレベルではいくつかの詳しいメトリックを利用できます。

ICA ファイルのダウンロード実行時間（**IFDCD**）

IFDCD はクライアントがサーバーから ICA ファイルをダウンロードするのにかかった時間です。このプロセスの全容は、以下のとおりです:

1. ユーザーが Workspace アプリでリソース（アプリケーションまたはデスクトップ）をクリックします。
2. Citrix Gateway が構成されている場合は、それを介してユーザーの要求が StoreFront に送信されます。要求は StoreFront から Delivery Controller に送信されます。
3. Delivery Controller は要求を処理できるマシンを探し、そのマシンの情報などの詳細を StoreFront に送信します。また、StoreFront は Secure Ticket Authority にワンタイムチケットを要求し、これを受信します。
4. StoreFront は ICA ファイルを生成し、Citrix Gateway（構成されている場合）を介してユーザーに送信します。

IFDCD はこのプロセス（手順 1〜4）が完了するまでにかかる時間を表します。クライアントが ICA ファイルを受信すると、IFDCD のカウントが停止します。

LPWD は、このプロセスにおける StoreFront のコンポーネントです。

IFDCD の値が高い（ただし LPWD の値は普通である）場合、サーバー側の開始処理は正常ですが、クライアントデバイスと StoreFront との間の通信に問題があったことを示しています。これは 2 台のマシンをつなぐネットワーク上の問題によるものです。これがわかれば、最初にネットワークの潜在的な問題に対処することができます。

ページ開始時の **Web** サーバーの実行時間（**LPWD**）

これは StoreFront の起動ページ（launch.aspx）の処理にかかる時間を表します。LPWD の値が高い場合、StoreFront にボトルネックがある可能性があります。

考えられる原因は次のとおりです：

- StoreFront の高負荷 Internet Information Services（IIS：インターネットインフォメーションサービス）のログ、監視ツール、タスクマネージャー、パフォーマンスモニターなどを確認して速度低下の原因を特定します。
- StoreFront で Delivery Controller などの他のコンポーネントとの通信に問題が生じています。StoreFront と Delivery Controller との間のネットワーク接続が遅くなっていないか、または停止や過負荷の状態になっている Delivery Controller がないかを確認してください。

名前解決時の **Web** サーバーの実行時間（**NRWD**）

これは Delivery Controller が公開アプリケーションまたは公開デスクトップの名前を VDA マシンの IP アドレスに解決するのにかかる時間を表します。

このメトリックの値が高い場合、Delivery Controller が公開アプリケーションの名前を IP アドレスに解決するのに時間がかかっていることを示しています。考えられる原因は次のとおりです：

- クライアントの問題
- Delivery Controller の問題（過負荷など）や、クライアントと Delivery Controller をつなぐネットワークリンクの問題

チケット応答時の **Web** サーバーの実行時間（**TRWD**）

これはチケットが必要な場合に、Secure Ticket Authority（STA）サーバーまたは Delivery Controller からチケットを取得するのにかかる時間を表します。この時間が長い場合は、STA サーバーまたは Delivery Controller が過負荷になっていることを示しています。

セッション検索時のクライアントの実行時間（**SLCD**）

これは要求された公開アプリケーションをホストするためにすべてのセッションを照会するのにかかる時間を表します。この照会処理は既存のセッションでアプリケーションの起動要求を処理できるかどうかを判断するために、クライアント上で実行されます。新規セッションか共有セッションかによって異なる手法が使用されます。

セッション作成時のクライアントの実行時間（**SCCD**）

これはセッションの作成にかかった時間です。具体的には wfica32.exe ファイルが実行されてから接続が確立されるまでの時間を表しています。

VDA セッションの開始フェーズ

セッション開始時の **VDA** の実行時間（**SSVD**）

この時間は VDA が開始処理の全体を実行するのに要する時間を含めた、サーバー側の接続開始時の高レベルメトリックを表します。このメトリックの値が高い場合は、セッション開始までの時間が長くなる要因が VDA 側にあることを示しています。VDA が開始処理全体の実行にかかった時間は、この値に含まれます。

アカウント情報取得時の **VDA** の実行時間（**COVD**）

VDA がユーザーの資格情報を取得するのにかかった時間を表します。

この時間はユーザーが資格情報を適宜入力しなければいくらでも増加する可能性があるため、VDA の開始時間には含まれません。この時間が意味を持つと考えられるのは、ログイン操作が必要かつサーバー側で資格情報の入力を求めるダイアログボックスが表示される場合（またはログイン前に法律上の注意点が表示される場合）に限られます。

アカウント情報認証時の **VDA** の実行時間（**CAVD**）

これは VDA が認証プロバイダーを照会してユーザーの資格情報を認証するのにかかる時間を表します。認証プロバイダーは Kerberos、Active Directory、Security Support Provider Interface（SSPI）のいずれかになります。

グループポリシーの **VDA** の実行時間（**GPVD**）

これはログオン中にグループポリシーオブジェクトを適用するのにかかる時間を表します。

ログインスクリプト実行時の **VDA** の実行時間（**LSVD**）

これは VDA がユーザーのログインスクリプトを実行するのにかかる時間を表します。

ユーザーまたはグループのログインスクリプトの実行を非同期にできます。アプリケーション互換性スクリプトを最適化するか、代わりに環境変数を使用します。

プロファイルロード時の **VDA** の実行時間（**PLVD**）

これは VDA がユーザーのプロファイルを読み込むのにかかる時間を表します。

この時間が長い場合は、ユーザープロファイルの設定を見直してください。移動プロファイルのサイズと保存場所によってはセッションの開始が遅くなります。ユーザーがターミナルサービスの移動プロファイルとホームフォルダーが有効になっているセッションにログオンすると、移動プロファイルの内容とホームフォルダーへのアクセスがログオン時にマップされるため、その分だけリソースが必要になります。場合によっては CPU 使用率が著しく高くなることもあります。この問題による影響を軽減するには、ターミナルサービスのホームフォルダーとリダイレクトされた個人用フォルダーを使用してください。通常 Citrix 環境でユーザープロファイルを管理する場合は、Citrix Profile Management を使用します。Citrix Profile Management を使用していてログオン時間が遅くなる場合は、アンチウイルスプログラムが Citrix Profile Management ツールをブロックしていないかを確認してください。

プリンター作成時の **VDA** の実行時間（**PCVD**）

これは VDA がユーザーのクライアントプリンターを同期的にマップするのにかかる時間を表します。プリンターの作成を非同期で実行するように設定している場合は、セッションの開始処理の完了に影響しないため、PCVD の値は記録されません。

プリンターのマッピングの時間が長くなるのは、多くの場合プリンターの自動作成ポリシーの設定に原因があります。ユーザーのクライアントデバイスにローカルで追加されたプリンターの台数と印刷設定は、セッションの開始時間に直接影響を及ぼす可能性があります。Citrix Virtual Apps and Desktops はセッションが開始されると、ローカルにマップされたすべてのプリンターをクライアントデバイス上に作成する必要があります。特にユーザーの設定で多数のローカルプリンターが存在する場合は、印刷ポリシーを設定しなおして、作成するプリンターの台数を削減します。これを行うには、Delivery Controller と Citrix Virtual Apps and Desktops でプリンターの自動作成ポリシーを編集します。

ドライブマッピング時の **VDA** の実行時間（**DMVD**）

これは VDA がユーザーのクライアントドライブ、デバイス、ポートをマップするのにかかる時間です。

ICA プロトコルを最適化し、セッション全体のパフォーマンスを向上させるには、基本ポリシーにオーディオや COM ポートマッピングなどの未使用の仮想チャネルを無効にする設定が指定されていることを確認してください。

アプリケーション/デスクトップ起動時の **VDA** の実行時間（**ALVD/DLVD**）

このフェーズは userinit と Shell の実行時間を合わせたものです。ユーザーが Windows マシンにログオンすると、Winlogon は userinit.exe を実行します。userinit.exe はログオンスクリプトを実行し、ネットワーク接続を再確立して、Windows ユーザーインターフェイスである Explorer.exe を起動します。userinit は、userinit.exe の開始から、仮想デスクトップまたはアプリケーションのユーザーインターフェイスの起動までの時間に相当します。Shell の実行時間は、ユーザーインターフェイスの初期化から、ユーザーにキーボードとマウスの制御が渡されるまでの時間に相当します。

セッション作成時の **VDA** の実行時間（**SCVD**）

この時間には VDA でのセッション作成時における各種の遅延時間が含まれます。

ユーザーログオンの問題の診断

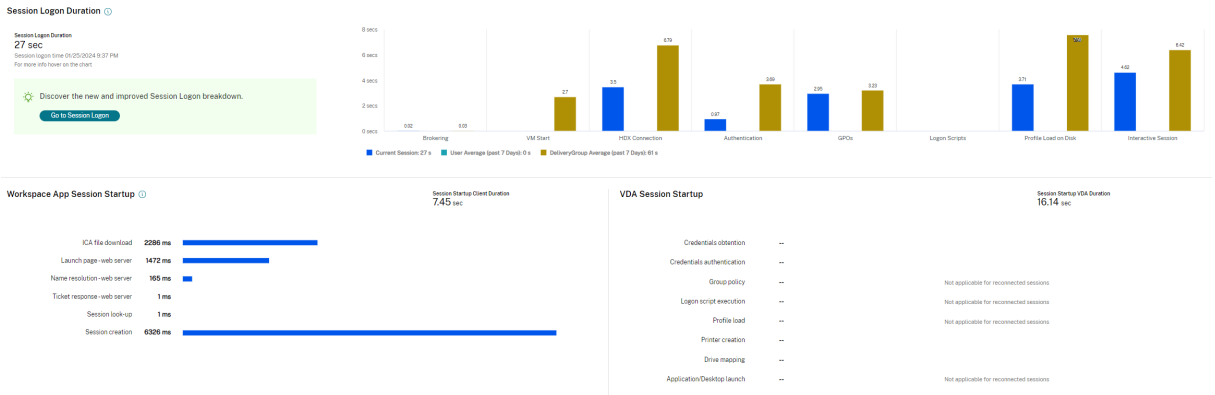
November 22, 2023

ユーザーログオンの問題のトラブルシューティングを行うには、ログオン処理時間データを使用します。

ログオン処理時間は、HDX を使用するデスクトップまたはアプリに初めて接続する場合のみ測定されます。このデータには、リモートデスクトッププロトコルを使用して接続しようとするユーザーや、切断されたセッションから再接続するユーザーは含まれません。具体的には、ユーザーが最初に HDX 以外のプロトコルを使用して接続してから、HDX を使用して再接続するときは、ログオン処理時間は測定されません。

[ユーザーの詳細] ビューでは、処理時間は、ログオン時刻表示の上にある数値と、ログオン処理のフェーズのグラフとして表示されます。

ユーザーが Citrix Virtual Apps and Desktops にログオンすると、Monitor Service により、ユーザーが Citrix Workspace アプリから接続した時点から、デスクトップが使用可能になった時点までのログオンプロセスの各フェーズが追跡されます。



左側の大きな数字は総ログオン時間であり、接続の確立および Delivery Controller からのデスクトップの取得にかかった時間と、仮想デスクトップの認証とログオンにかかった時間を合計して計算されます。処理時間の情報は秒単位（または秒の小数単位）まで表示されます。

前提条件

ログオン期間データとドリルダウンが表示されるようにするには、次の前提条件を満たす必要があります:

1. VDA に **Citrix User Profile Manager** と **Citrix User Profile Manager WMI Plugin** をインストールする。
2. Citrix Profile Management Service が実行されている。
3. XenApp および XenDesktop サイト 7.15 以前の場合、GPO 設定 ［従来の実行リストを処理しない］を無効にします。
4. 対話型セッションのドリルダウンでは、監査プロセスの追跡を有効にする必要があります。
5. GPO ドリルダウンの場合は、グループポリシーの操作ログのサイズを大きくします。

> 注:
>
> ログオン処理時間は、デフォルトの Windows シェル（explorer.exe）でのみサポートされ、カスタムシェルではサポートされません。

ユーザーログオンの問題のトラブルシューティング手順

1. ログオン状態のトラブルシューティングを行うには、［ユーザーの詳細］ビューの［ログオン処理時間］パネルを使用します。
    - ユーザーがログオン中の場合は、ここにログオンのプロセスが表示されます。
    - ユーザーがログオン済みの場合、ユーザーがそのセッションにログオンするときにかかった時間が［ログオン処理時間］パネルに表示されます。
2. ログオンプロセスの各フェーズを調査します。

ログオンプロセスのフェーズ

仲介

ユーザーに割り当てるデスクトップを決定するのに要した時間です。

仮想マシンの起動

マシンの起動を必要とするセッションの場合、これは仮想マシンの起動にかかった時間です。

HDX コネクション

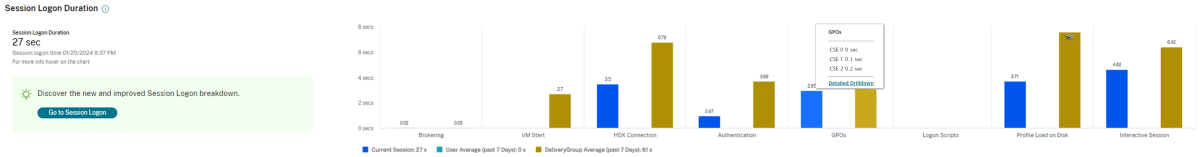
クライアントから仮想マシンへの HDX 接続の設定で必要な手順を実行するためにかかった時間です。

認証

リモートセッションへの認証を実行するのにかかった時間です。

GPO

仮想マシン上でグループポリシー設定が有効になっている場合に、ログオン中にグループポリシーオブジェクトの適用にかかった時間です。GPO バーにマウスカーソルを重ねると、CSE（クライアント側拡張機能）ごとに各ポリシーの適用にかかった時間の詳細がヒントとして表示されます。



［詳細なドリルダウン］をクリックすると、ポリシーの状態と対応する GPO 名を示すテーブルが表示されます。ドリルダウンの期間は CSE 処理時間のみを表し、合計 GPO 時間には加算されません。ドリルダウンテーブルは、詳細なトラブルシューティングやレポートで使用するためにコピーできます。各ポリシーの GPO 時間は、イベントビューアーのログから取得されます。操作ログに割り当てられているメモリ（デフォルトサイズは 4MB）によっては、このログは上書きされる可能性があります。操作ログのログサイズを増やす方法について詳しくは、Microsoft TechNet 記事の「https://docs.microsoft.com/en-us/previous-versions/tn-archive/dd277416(v=technet.10)」を参照してください。

ログオンスクリプト

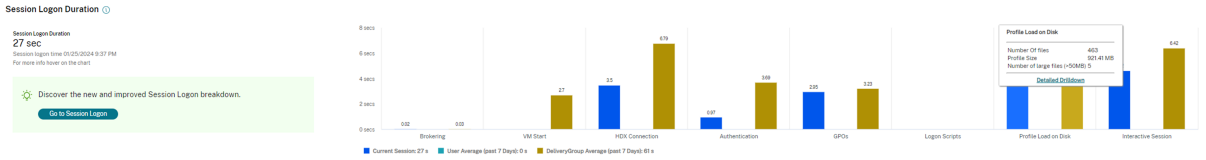
セッションでログオンスクリプトが構成されている場合、これはログオンスクリプトの実行にかかった時間です。

プロファイルのロード

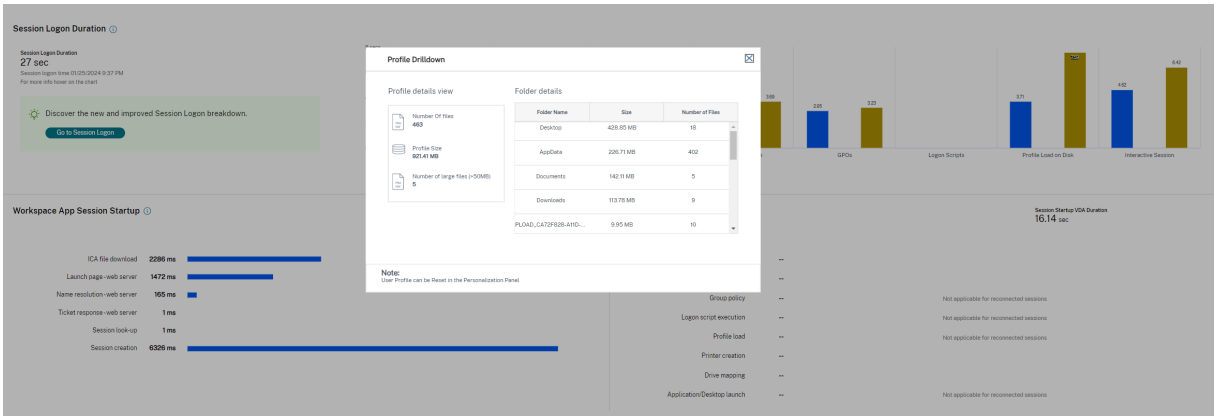
ユーザーまたは仮想マシンに対してプロファイル設定が構成されている場合、これはプロファイルのロードにかかった時間です。

Citrix Profile Management が構成されている場合、［プロファイルロード］バーに表示されるのは Citrix Profile Management がユーザープロファイルの処理に要する時間です。この情報は、管理者が処理に時間がかかる問題をトラブルシューティングするために役立ちます。Profile Management が構成されている場合、［プロファイルロード］バーには長くなった処理時間が表示されます。この処理時間の増加は機能を拡張した結果であり、パフォーマンスが低下したわけではありません。この機能拡張は、VDA 1903 以降で利用できます。

［プロファイルのロード］バーの上にカーソルを置くと、現在のセッションのユーザープロファイルの詳細を示すツールチップが表示されます。この追加情報は、高プロファイル負荷の問題のトラブルシューティングに役立ちます。



［詳細なドリルダウン］をクリックすると、プロファイルのルートフォルダー（C:/Users/username など）内の個別のフォルダー、そのサイズとファイル数（サブフォルダー内のファイルを含む）へと、さらにドリルダウンできます。



プロファイルドリルダウンは、VDA 1811 以降で利用できます。プロファイルドリルダウン情報を使用すると、長いプロファイルロード時間に関連する問題を解決できます。次の操作を実行できます：

- ユーザープロファイルをリセットする
- 大きな不要ファイルを削除してプロファイルを最適化する
- ファイル数を減らしてネットワーク負荷を軽減する
- プロファイルストリーム配信を使用する

デフォルトでは、すべてのフォルダ名が表示されます。フォルダ名を非表示にするには、次の手順に従って VDA マシンのレジストリ値を編集します：

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

1. VDA で、HKEY_LOCAL_MACHINE\Software\Citrix\Director に新しいレジストリ値 **ProfileFolderNameHidden** を追加します。\
2. 値を 1 に設定します。この値は、DWORD（32 ビット）値である必要があります。フォルダ名の表示が無効になりました。

3. フォルダ名を再度表示するには、値を 0 に設定します。

> 注:
>
> GPO または PowerShell を使用して、複数のマシンでレジストリ値の変更を適用できます。GPO を使用してレジストリの変更を展開する方法について詳しくは、ブログを参照してください。

追加情報

- プロファイルのドリルダウンでは、リダイレクトされたフォルダーは考慮されません。
- ルートフォルダー内の NTUser.dat ファイルは、エンドユーザーに表示されないことがあります。ただし、これらはプロファイルのドリルダウンに含まれ、ルートフォルダー内のファイルのリストに表示されます。
- AppData フォルダーには、プロファイルドリルダウンに含まれていない、いくつかの隠しファイルがあります。
- ファイル数およびプロファイルサイズに関するデータは、Windows の制限事項が原因で［個人設定］パネルのデータと一致しないことがあります。

対話型セッション

これは、ユーザープロファイルのロード後、キーボードやマウスの制御をユーザーに「渡す」までにかかった時間です。通常、ログオンプロセスのすべてのフェーズで最も長い時間であり、次のように計算されます：対話型セッションの処理時間 **=** デスクトップ準備完了イベントのタイムスタンプ（**VDA** の **EventId 1000**）**-** ユーザープロファイルロード完了イベントのタイムスタンプ（**VDA** の **EventId 2**）対話型セッションには、userinit 実行前、userinit、Shell の 3 つのサブフェーズがあります。対話型セッションにカーソルを合わせると、次のツールチップが表示されます：

- サブフェーズ
- 各サブフェーズの所要時間
- これらのサブフェーズ間の累積時間遅延合計

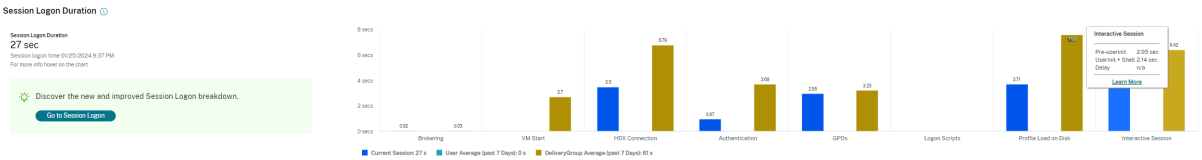
> 注:
>
> この機能は VDA バージョン 1811 以降で使用できます。7.18 より前のバージョンのサイトでセッションを開始してから 7.18 にアップグレードした場合、「サーバーエラーのためドリルダウンを使用できません。」というメッセージが表示されます。アップグレード後にセッションを起動した場合は、エラーメッセージは表示されません。

各サブフェーズの期間を表示するには、仮想マシン（VDA ）でプロセス追跡の監査を有効にします。プロセス追跡の監査が無効（デフォルト）の場合、表示されるのは userinit 実行前の時間と、Userinit と Shell の合計時間になります。以下の手順により、グループポリシーオブジェクト（GPO）を使用してプロセス追跡の監査を有効化できます：

1. GPO を作成し、GPO エディターで編集します。
2. ［コンピューターの構成］**>** ［**Windows** の設定］**>** ［セキュリティの設定］**>** ［ローカルポリシー］**>** ［監査ポリシー］の順に移動します。

3. 右側のペインで、［プロセス追跡の監査］をダブルクリックします。
4. ［成功］チェックボックスをオンにして、［OK］をクリックします。
5. この GPO を目的の VDA やグループに適用します。

プロセス追跡の監査の詳細とこの機能の有効化および無効化の切り替え方法については、Microsoft のドキュメントhttps://docs.microsoft.com/en-us/previous-versions/ms813609(v=msdn.10)を参照してください。



［ユーザーの詳細］ビューの［ログオン処理時間］パネル。

- 対話型セッション–**userinit** 実行前：対話型セッションの所要時間のうち、グループポリシーオブジェクトおよびスクリプトの適用にかかった時間です。このサブフェーズは、GPO とスクリプトを最適化することで短縮できます。
- 対話型セッション–**userinit**： Windows マシンにユーザーがログオンすると、Winlogon により userinit.exe が実行されます。Userinit.exe はログオンスクリプトを実行し、ネットワーク接続を再確立して、Windows ユーザーインターフェイスである Explorer.exe を起動します。この対話型セッションのサブフェーズは、userinit.exe の開始から、仮想デスクトップまたはアプリケーションのユーザーインターフェイスの起動までの時間に相当します。
- 対話型セッション–**Shell**：前のサブフェーズで、userinit により Windows ユーザーインターフェイスの初期化が開始されます。Shell サブフェーズは、ユーザーインターフェイスの初期化から、ユーザーにキーボードとマウスの制御が渡されるまでの時間に相当します。
- 遅延： **userinit** 実行前および **userinit** と **userinit** および **Shell** の各サブフェーズ間の累積遅延時間です。

総ログオン時間は、これらの各フェーズを厳密に合計したものではありません。たとえば、一部のフェーズは並行して発生するほか、フェーズによっては追加処理が発生してログオン処理時間が合計値よりも大きくなることがあります。総ログオン処理時間には、ICA ファイルのダウンロードとアプリケーションでの ICA ファイルの起動までの時間に相当する、ICA アイドル時間は含まれません。
アプリケーション起動時に ICA ファイルを自動的に開くようにするは、ICA ファイルをダウンロード時に自動で開くようにお使いの Web ブラウザーを構成します。詳しくは、CTX804493を参照してください。

> 注：
>
> ［ログオン処理時間］グラフには、ログオンフェーズが秒単位で表示されます。1 秒未満の時間値はすべて、秒未満の値として表示されます。1 秒を超える値は、0.5 秒単位に丸められます。グラフは、Y 軸の最高値を 200 秒として表示するように設計されています。200 秒を超える値はすべて、実際の値を棒グラフの上に添えて表示されます。

トラブルシューティングのヒント

グラフで異常な値または予期しない値を識別するには、現在のセッションの各フェーズで要した時間と、このユーザーの最近 7 日間の平均処理時間、およびこのデリバリーグループのすべてのユーザーの最近 7 日間の平均処理時間を比較します。

必要に応じて、担当管理者に報告します。たとえば、仮想マシンの起動に時間がかかり、ハイパーバイザーが問題の原因である可能性がある場合は、ハイパーバイザー管理者に問題を報告します。また、仲介処理に時間がかかる場合は、サイト管理者に Delivery Controller の負荷分散のチェックを依頼します。

以下の問題について調査します。

- （現在の）ログオンを示すバーが表示されていない。
- 現在のログオン処理時間とこのユーザーの平均処理時間が大きく食い違う。次の原因が考えられます：
  - 新しいアプリケーションがインストールされた。
  - オペレーティングシステムが更新された。
  - 構成が変更された。
  - ユーザーのプロファイルサイズが大きい。この場合、プロファイルロード時間が長くなります。
- ユーザーのログオン処理時間（現在値および平均値）とデリバリーグループの平均値が大きく食い違う。

必要な場合は、［再起動］をクリックしてユーザーに再ログオンしてもらい、仮想マシンの起動や仲介時に問題が発生するかどうかを確認します。

ユーザーのシャドウ

November 18, 2022

ユーザーのシャドウ機能を使用すると、ユーザーの仮想マシンまたはセッションを直接表示したり操作したりできます。Windows と Linux VDA の両方をシャドウできます。この機能を使用するには、そのマシンにユーザーが接続している必要があります。ユーザーが接続している場合、ユーザーのタイトルバーにそのマシン名が表示されます。

新しいタブでシャドウを開始し、Citrix Cloud URL からのポップアップを許可するように Web ブラウザーの設定を更新します。

［ユーザーの詳細］ビューからシャドウ機能にアクセスします。ユーザーセッションを選択し、［アクティビティマネージャー］ビューまたは［セッション詳細］パネルで、［シャドウ］をクリックします。

Linux VDA のシャドウ

シャドウは、RHEL7.3 または Ubuntu バージョン 16.04 Linux ディストリビューションを実行する Linux VDA バージョン 7.16 以降で使用できます。

> 注:
>
> - ［監視］は完全修飾ドメイン名を使用してターゲットの Linux VDA に接続します。［監視］クライアントが Linux VDA の完全修飾ドメイン名を解決できるようにしてください。
> - VDA には、python-websockify パッケージと x11vnc パッケージがインストールされている必要があります。
> - VDA への noVNC 接続は、WebSocket プロトコルを使用します。デフォルトでは、**ws://** WebSocket プロトコルが使用されます。セキュリティ上の理由からセキュリティ保護された **wss://** プロトコルを使用することをお勧めします。各監視クライアントおよび Linux VDA に SSL 証明書をインストールします。

VDA をシャドウ用に設定するには、「セッションのシャドウ」の手順に従います。

1. ［シャドウ］をクリックすると、シャドウ接続が初期化され、確認プロンプトがユーザーデバイスに表示されます。
2. ユーザーが ［はい］をクリックすると、マシンまたはセッションの共有が開始されます。
3. 管理者は、シャドウセッションのみを表示できます。

Windows VDA のシャドウ

Windows VDA セッションは、Windows リモートアシスタンスを使用してシャドウされます。VDA のインストール中にユーザーの Windows リモートアシスタンス機能を有効にします。詳しくは、「機能を有効または無効にする」セクションを参照してください。

1. ［シャドウ］をクリックするとシャドウ接続が初期化されます。これにより、.msrc インシデントファイルを開くか保存するかを確認するダイアログボックスが開きます。
2. デフォルトで選択されていない場合は、Remote Assistance Viewer でファイルを開きます。ユーザーデバイス側には、確認のメッセージが表示されます。
3. ユーザーが ［はい］をクリックすると、マシンまたはセッションの共有が開始されます。
4. ユーザーがマウスやキーボードの制御を許可すると、管理者がシャドウセッションを制御できるようになります。

シャドウのための **Microsoft Internet Explorer** ブラウザーの構成

Microsoft Internet Explorer ブラウザーでダウンロードした Microsoft リモートアシスタンスファイル（.msra）がリモートアシスタンスクライアントで自動的に開くように構成します。

これを行うには、グループポリシーエディターで［ファイルのダウンロード時に自動的にダイアログを表示］を有効にする必要があります。

［コンピューターの構成］>［管理用テンプレート］>［Windows コンポーネント］>［Internet Explorer］>［インターネットコントロールパネル］>［セキュリティページ］>［インターネットゾーン］>［ファイルのダウンロード時に自動的にダイアログを表示］

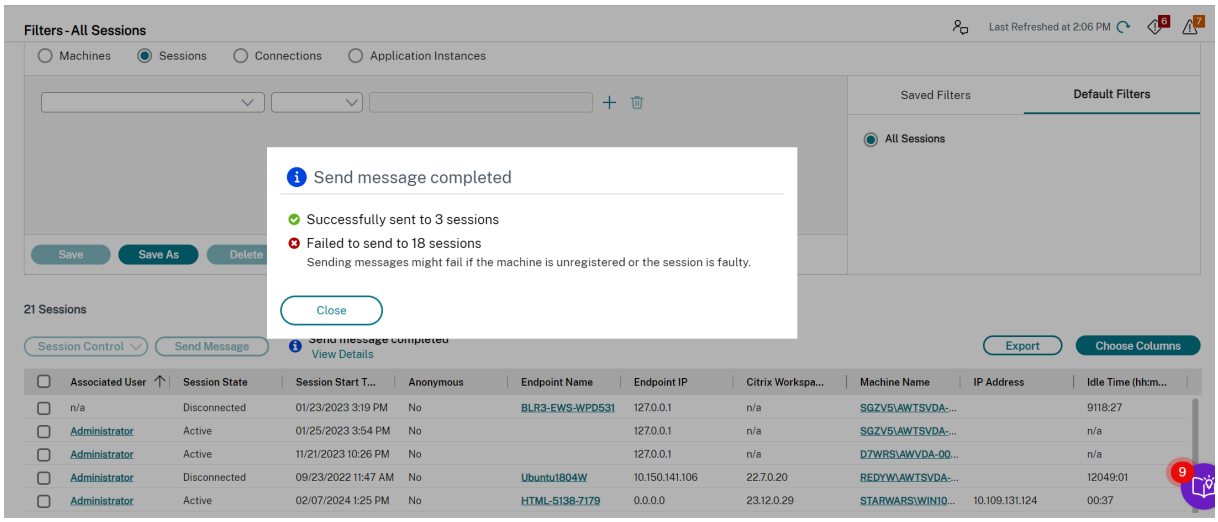
ユーザーへのメッセージの送信

January 25, 2024

［監視］では、マシンに接続しているユーザーにメッセージを送信できます。たとえば、突発的にデスクトップの保守、ログオフ、再起動、プロファイルのリセットなどが必要になった場合に、ユーザーに緊急のメッセージを送信できます。

ユーザーにメッセージを送信するには、次の手順を実行します:

1. ［監視］ > ［フィルター］ > ［マシン］ > ［すべてのマシン］と移動します。
2. メッセージの送信先のマシンを選択し、［メッセージの送信］をクリックします。
3. メッセージを入力して ［送信］をクリックします。



マシンが登録されていない場合、またはセッションに障害がある場合、メッセージの送信は失敗する可能性があります。

メッセージが正しく送信されると、確認メッセージが表示されます。マシンに接続しているユーザーにメッセージが表示されます。

メッセージの送信に問題が発生すると、エラーメッセージが表示されます。そのエラーメッセージに従って問題を解決してください。問題を解決したら、件名およびメッセージテキストを入力して再度 ［試行］をクリックします。

接続されているすべてのセッションに一括メッセージを送信する場合、操作の進行状況がパーセンテージで表示されます。操作が完了すると、送信に成功したメッセージの数と失敗したメッセージの数が表示されます。メッセージの

送信ステータスは、大規模なサイトを管理する場合に特に役立ちます。これは、メッセージを特定のユーザーに再送信する必要があるかどうかを理解するのに役立ちます。

アプリケーション障害の解決

February 10, 2023

［アクティビティマネージャー］ビューで ［アプリケーション］タブをクリックします。ここでは、このユーザーがアクセス権限をもつすべてのマシン上のすべてのアプリケーションとその状態を確認できます。これには、接続しているマシンのローカルアプリケーションおよびホストされるアプリケーションが含まれます。

一覧には、セッション内で起動されたアプリケーションのみが表示されます。

マルチセッション OS マシンおよびシングルセッション OS マシンでは、アプリケーションが切断セッションごとに一覧で表示されます。ユーザーが接続していない場合、アプリケーションは表示されません。

アクション	説明
応答していないアプリケーションを終了する	応答していないアプリケーションを選択し、［アプリケーションの終了］をクリックします。アプリケーションが終了したら、ユーザーに再度起動するように通知します。
応答していないプロセスを終了する	必要な権限がある場合は、［プロセス］タブをクリックします。アプリケーションに関連するプロセス、または CPU リソースやメモリを過度に消費しているプロセスを選択し、［プロセスの終了］をクリックします。プロセスを終了するための権限がない場合、プロセスを終了することはできません。
ユーザーのマシンを再起動する	シングルセッション OS マシンでは、選択したセッションで ［再起動］をクリックします。または、［マシンの詳細］ビューで電源制御を使ってマシンを再起動またはシャットダウンします。アプリケーションの状態を再確認するには、ユーザーに再度ログオンするように通知します。マルチセッション OS マシンでは、［再起動］オプションを使用できません。代わりに、ユーザーをログオフして、再度ログオンさせます。
マシンをメンテナンスモードにする	パッチまたはそのほかの更新などによりマシンのイメージをメンテナンスする必要がある場合は、マシンをメンテナンスモードにします。［マシンの詳細］ビューで ［詳細］をクリックして、メンテナンスモードのオプションをオンにします。担当の管理者に報告します。

実行中のアプリケーションを非表示にする

アクティビティマネージャーのデフォルトでは、そのユーザーのセッションで実行されているすべてのアプリケーションが一覧表示されます。この情報を表示するには、アクティビティマネージャー機能へのアクセス権限が必要です。この権限を持つ管理者の役割は、すべての管理権限を実行できる管理者、デリバリーグループ管理者、およびヘルプデスク管理者です。

ユーザーのプライバシーと、ユーザーが使用しているアプリケーションを保護するために、［アプリケーション］タブでアプリケーションの一覧を非表示にできます。このためには、VDA で HKEY_LOCAL_MACHINE\Software\Citrix\Director\TaskManagerDataDisplayed のレジストリキーを編集します。デフォルトでは 1 に設定されています。値を 0 に変更すると、VDA から情報が収集されなくなるため、アクティビティマネージャーに情報が表示されなくなります。

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

デスクトップ接続の復元

April 22, 2022

［監視］ビューでは、タイトルバーにそのユーザーの接続状態が表示されます。

デスクトップ接続に問題が発生するとその原因が表示されるため、トラブルシューティング方法を判別することができます。

アクション	説明
マシンがメンテナンスモードでないことを確認する	［ユーザーの詳細］ページで、メンテナンスモードがオフであることを確認します。
ユーザーのマシンを再起動する	マシンを選択して ［再起動］をクリックします。ユーザーのマシンが CPU リソースを過度に消費しているためにマシンが応答しないまたは接続できない場合は、このオプションを使用します。

セッションの復元

April 22, 2022

セッションが切断状態になると、セッションおよびアプリケーションは終了しませんが、サーバーとユーザーデバイス間の通信が切断されます。

[ユーザーの詳細] ビューの [セッション詳細] パネルで、セッション障害のトラブルシューティングを行います。現在のセッションがセッション ID で示され、詳細を確認できます。

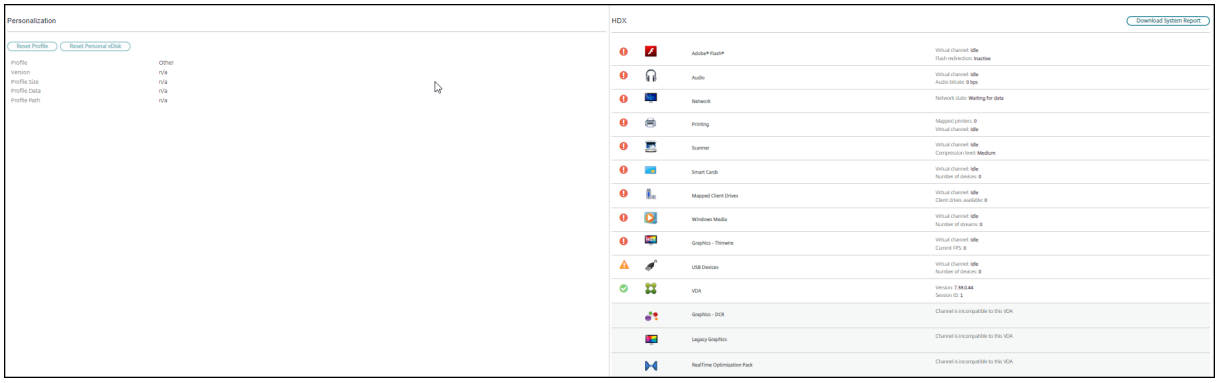
アクション	説明
応答していないアプリケーションまたはプロセスを終了する	[アプリケーション] タブをクリックします。応答していないアプリケーションを選択し、[アプリケーションの終了] をクリックします。同様に、応答していないプロセスを選択し、[プロセスの終了] をクリックします。また、メモリや CPU リソースを過度に消費しているプロセスを終了します。
Windows セッションを切断する	[セッション制御] をクリックし、[切断] を選択します。このオプションは、仲介されたマルチセッション OS マシンに対してのみ使用できます。仲介されていないセッションでは無効です。
セッションからユーザーをログオフする	[セッション制御] をクリックし、[ログオフ] を選択します。

セッション障害が解決されたことを確認するために、ユーザーに再度ログオンさせます。また、ユーザーをシャドウしてセッションをより詳しく監視することもできます。

HDX チャネルシステムレポートの実行

November 22, 2023

ユーザーのマシン上の HDX チャネルの状態を確認するには、[ユーザーの詳細] ビューの [HDX] パネルを使用します。このパネルは、HDX を使ってユーザーマシンに接続している場合にのみ操作できます。



情報を使用できないことを示すメッセージが表示された場合は、ページが更新されるまで 1 分待つか、[更新] ボタンをクリックしてください。HDX データはほかのデータより更新に時間がかかることがあります。

エラーまたは警告のアイコンをクリックすると、詳細が表示されます。

> ヒント:
>
> このダイアログボックスでは、タイトルバーの左隅にある矢印をクリックしてほかのチャネルの情報を表示することもできます。

HDX チャネルシステムレポートは、主に Citrix サポートチームによるトラブルシューティング時に使用されます。[HDX] パネルで、[システムレポートのダウンロード] をクリックしてください。

ユーザープロファイルのリセット

April 22, 2022

> 注意:
>
> プロファイルをリセットすると、そのユーザーのフォルダーやファイルは保存され、新しいプロファイルにコピーされます。ただし、多くのユーザープロファイルデータは削除されます。たとえば、レジストリはリセットされ、アプリケーション設定も削除される場合があります。

1. [監視] から、プロファイルをリセットするユーザーを検索し、このユーザーのセッションを選択します。
2. [プロファイルのリセット] をクリックします。
3. ユーザーに、すべてのセッションからログオフするように指示します。
4. ユーザーに再度ログオンするように指示します。ユーザープロファイルから保存されたフォルダーやファイルが新しいプロファイルにコピーされます。

   > 重要:
   >
   > 複数のプラットフォーム上（Windows 8 と Windows 7 など）にユーザーのプロファイルが存在する場合は、問題が発生したデスクトップまたはアプリケーションに最初にログオンするよう指示します。

> これにより、正しいプロファイルがリセットされます。Citrix ユーザープロファイルの場合、ユーザーのデスクトップが表示された時点でリセットされています。Microsoft の移動プロファイルの場合、フォルダーの復元処理に時間がかかる場合があります。この復元処理が完了するまで、ユーザーはログオンしていなければなりません。

これまでの手順では、Citrix Virtual Desktops（デスクトップ VDA）を使用している前提になっています。Citrix Virtual Desktops（サーバー VDA）を使用している場合は、プロファイルのリセットを実行するためにログオンする必要があります。ユーザーはいったんログオフしてから再度ログオンし、プロファイルのリセットを完了させる必要があります。

プロファイルが正しくリセットされない場合（ユーザーがそのマシンに再ログオンできなかったり一部のファイルが見つからなかったりする場合など）、管理者が手作業で元のプロファイルを復元する必要があります。

ユーザーのプロファイルのフォルダーやファイルが保存され、新しいプロファイルにコピーされます。これらのフォルダーは、以下の順番でコピーされます。

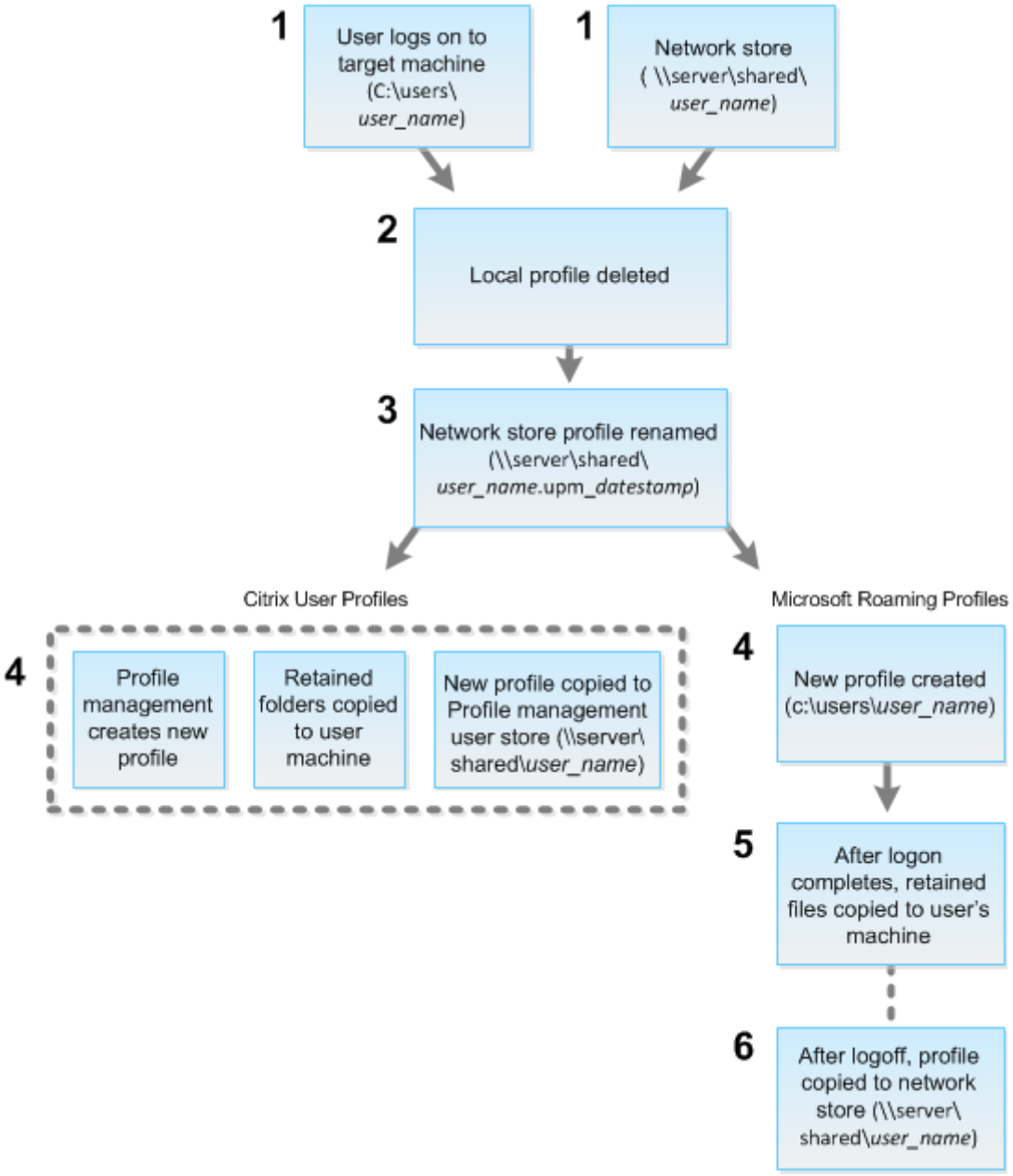
- デスクトップ
- Cookies
- お気に入り
- ドキュメント
- ピクチャ
- ミュージック
- ビデオ

> 注:
>
> Windows 8 以降では、プロファイルのリセット時にクッキーフォルダーはコピーされません。

リセットされたプロファイルはどのように処理されるか

いずれの Citrix ユーザープロファイルまたは Microsoft 移動プロファイルもリセットできます。ユーザーがログオフした後に管理者が［監視］または PowerShell SDK でリセットコマンドを選択すると、使用されているユーザープロファイルが識別され、［監視］により適切なリセットコマンドが発行されます。［監視］は Profile Management を介してプロファイルのサイズ、種類、およびログオン時間などに関する情報を取得します。

これは、ユーザーログオン後の、ユーザープロファイルがリセットされた場合の処理を説明した図です。



［監視］からのリセットコマンドにより、プロファイルの種類が指定されます。次に、Profile Management サービスによりその種類のプロファイルのリセットが試行され、適切なネットワーク共有（ユーザーストア）が検出されます。Profile Management がユーザーを処理したものの移動プロファイル用のコマンドを受け取ったという場合は、拒否されます（逆の場合も同様）。

1. ローカルプロファイルがある場合は削除されます。
2. ネットワークプロファイルの名前が変更されます。
3. 次の処理は、リセットされるプロファイルが Citrix ユーザープロファイルか Microsoft 移動プロファイルかにより異なります。

Citrix ユーザープロファイルの場合、Profile Management のインポート規則によって新しいプロファイルが作成され、フォルダーがネットワークプロファイルにコピーされ、ユーザーは通常どおりにログオンできます。リセットに移動プロファイルが使用される場合は、移動プロファイル内のすべてのレジストリ設定がリセットプロファイル内に保持されます。必要な場合は、テンプレートプロファイルが移動プロファイルよりも優先されるように Profile Management を構成することもできます。

Microsoft 移動プロファイルの場合、Windows によって新しいプロファイルが作成され、ユーザーがログオンするとフォルダーがユーザーデバイスにコピーされます。ユーザーが再度ログオフすると、新しいプロファイルがネットワークストアにコピーされます。

リセットに失敗したプロファイルを手動で復元するには

1. ユーザーに、すべてのセッションからログオフするように指示します。
2. ローカルプロファイルが存在する場合は削除します。
3. ネットワーク共有上のアーカイブフォルダーを検索します。アーカイブフォルダーには、名前に日時と upm_datestamp 拡張子が含まれます。
4. 現在のプロファイル名を削除します。つまり、upm_datestamp 拡張子のないものです。
5. 元のプロファイル名を使用して、アーカイブされたフォルダーの名前を変更します。つまり、日時の拡張子を削除します。プロファイルがリセット前の状態に戻りました。

セッションの録画

February 19, 2024

［監視］の ［ユーザーの詳細］と ［マシンの詳細］画面から、Session Recording 制御を使って、ICA セッションを録画することができます。この機能は **Platinum** ライセンスを持つユーザーが使用できます。

動的なセッション録画

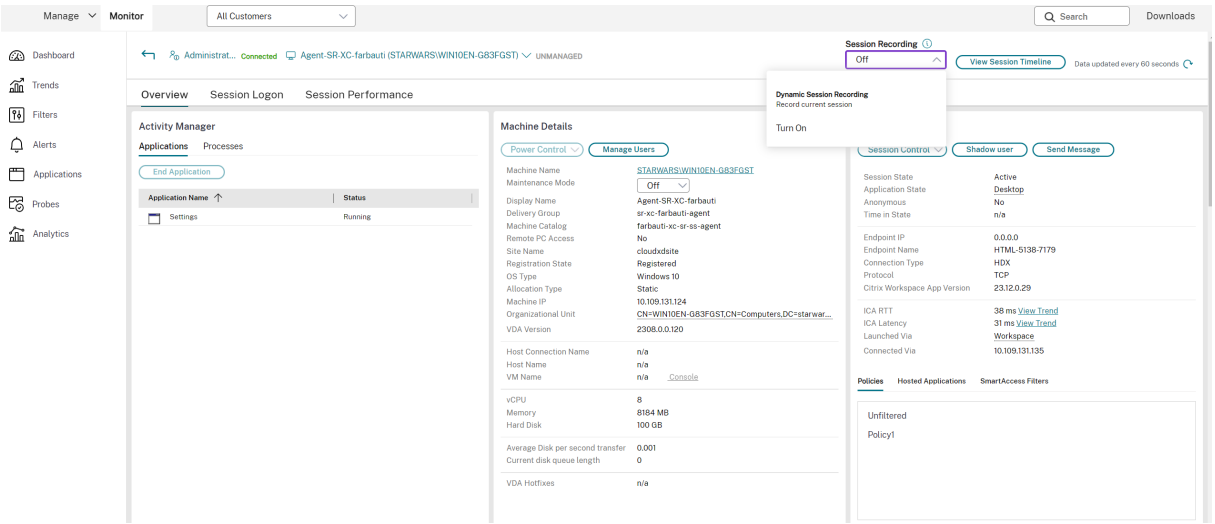
［ユーザーの詳細］画面から、Session Recording 制御を使って、現在アクティブなセッションを録画することができます。動的なセッション録画について詳しくは、「Session Recording サービス」の記事を参照してください。

［監視］での **Session Recording** 制御

［ユーザーの詳細］>［**Session Recording**］の次の操作で、現在のまたは以降のセッションを録画できます。

- 動的なセッション録画をオンにする - 現在のセッションが録画されます。
- オフにする - ユーザーのセッションの録画を無効にします。

［ポリシー］パネルには、アクティブな Session Recording ポリシーの名前が表示されます。



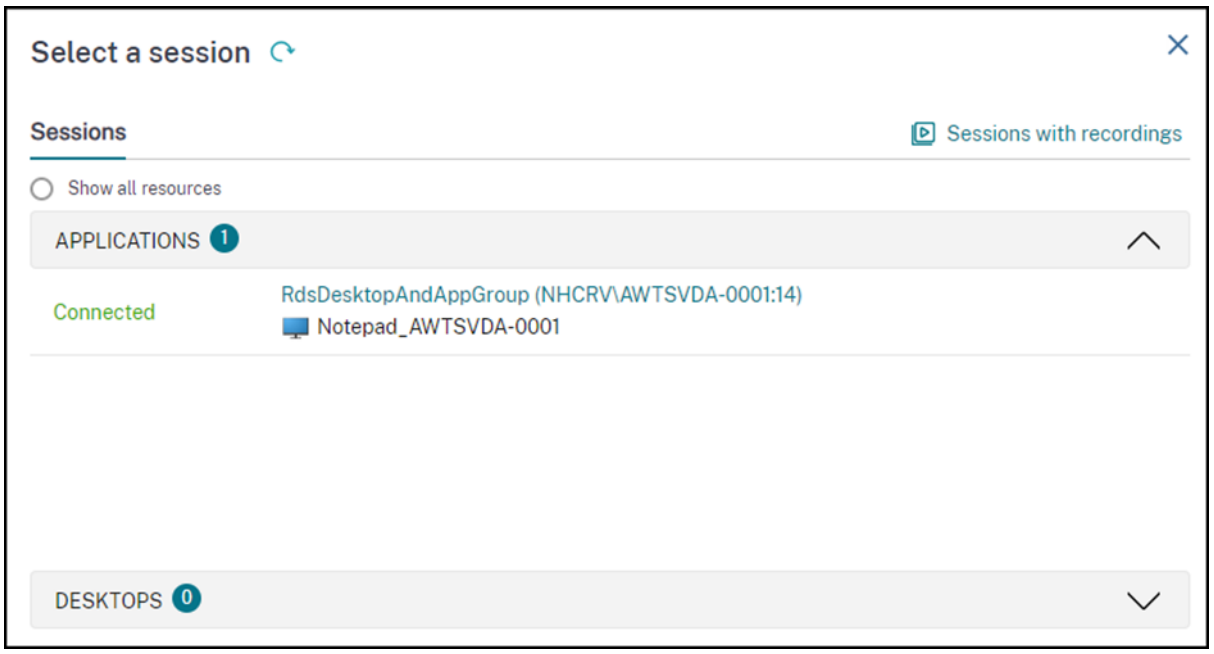
［マシンの詳細］パネルには、そのマシンの Session Recording ポリシーの状態が表示されます。

ライブセッションと録画されたセッションを再生する

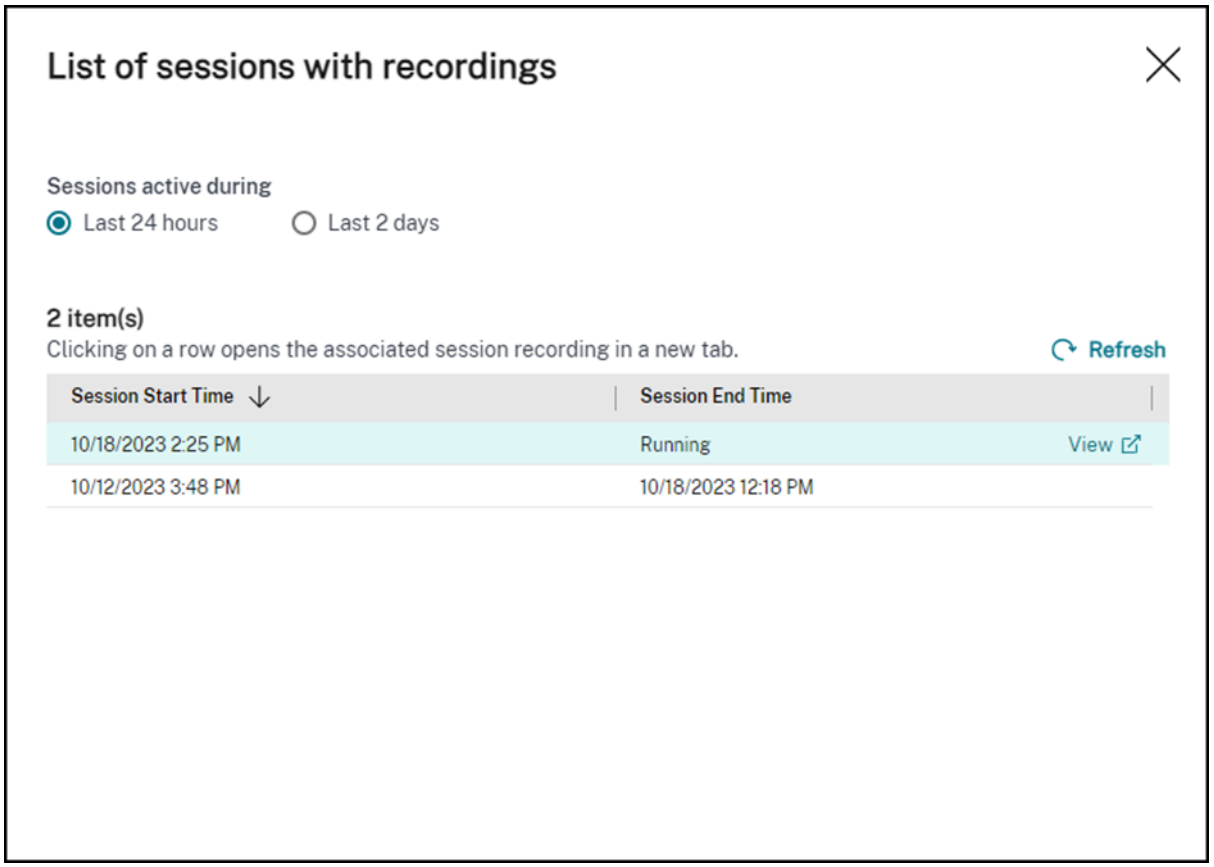
録画されたユーザーセッションやライブのユーザーセッションを再生することで、ユーザーが遭遇した問題を確認できます。監視コンソール内で録画およびセッション関連のメトリックに簡単にアクセスできるため、複数のセッション録画サーバー間で録画を検索したり、録画を表示するためのサードパーティアプリを探したりする必要がなくなります。これは、録画で検出された問題をパフォーマンスメトリックと関連付けるのに役立ちます。

この機能には、VDA および Session Recording サーバーのバージョン 2308 以降が必要です。

［監視］は、セッションの録画を集中リポジトリに保存します。セッションのセレクタモーダル > ［録画のあるセッション］リンクをクリックすると、そのユーザーに属する録画の一覧が表示されます。



過去 24 時間または過去 2 日間にアクティブだったセッションの録画を表示することを選択できます。現在アクティブなセッションのライブ録画には、［セッション終了時間］が ［実行中］としてマークされます。



［表示］リンクをクリックし、Citrix Session Recording 再生サーバーを使用して新しいタブで録画を再生します。

機能の互換性マトリックス

June 12, 2024

Citrix Monitor は、3 つの Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）エディションをサポートしています。**Premium**、**Citrix DaaS Advanced**、および **Citrix DaaS Advanced Plus** の 3 つです。次の表に、Citrix Monitor の特定の機能、VDA バージョン、依存コンポーネント、およびそれぞれのライセンスエディションを示します。

機能	依存関係 - 必要な最小バージョン	**Premium**	**Citrix DaaS Advanced**	**Citrix DaaS Advanced Plus**
AMD GPU で利用可能なリアルタイム GPU 使用率	64 ビット Windows を実行する VDA 7 2212	はい	はい	はい
Citrix Analytics for Performance- セッションの詳細へのアクセス	Citrix Analytics for Performance の使用権	はい	はい	はい
セッションの自動再接続	VDA 1906	はい	はい	はい
セッションの開始時間	VDA 1903	はい	はい	はい
デスクトッププロービング	Citrix Probe Agent 1903	はい	いいえ	いいえ
Citrix Profile Management のプロファイルのロード時間	VDA 1903	はい	はい	はい
プロファイルのドリルダウン	VDA 1811	はい	はい	はい
ハイパーバイザーアラートの監視	なし	はい	いいえ	いいえ
アプリケーションプロービング	Citrix Application Probe Agent 1811	はい	いいえ	いいえ
Microsoft RDS ライセンスの正常性	VDA 7.16	はい	はい	はい

機能	依存関係 - 必要な最小バージョン	Premium	Citrix DaaS Advanced	Citrix DaaS Advanced Plus
監視機能からのマシンコンソールへのアクセス	XenServer ハイパーバイザー 7.3	はい	はい	はい
フィルターデータのエクスポート	なし	はい	はい	はい
対話型セッションのドリルダウン	VDA 1808	はい	はい	はい
GPO のドリルダウン	VDA 1808	はい	はい	はい
OData API を使用したマシン履歴データの取得	なし	はい	はい	はい
スマートアラートポリシー	なし	はい	いいえ	いいえ
Health Assistant リンク	なし	はい	はい	はい
対話型セッションのドリルダウン	なし	はい	はい	はい
アプリケーション分析	VDA 7.15	はい	はい	はい
OData API V.4	なし	はい	はい	はい
Linux VDA ユーザーのシャドウ	VDA 7.16	はい	はい	はい
マシンコンソールへのアクセス	なし	はい	はい	はい
アプリケーション障害の監視	VDA 7.15	はい	はい	はい
アプリケーションを中心としたトラブルシューティング	VDA 7.13	はい	はい	はい
ディスクの監視	VDA 7.14	はい	はい	はい
GPU の監視	VDA 7.14	はい	はい	はい

機能	依存関係 - 必要な最小バージョン	Premium	Citrix DaaS Advanced	Citrix DaaS Advanced Plus
［セッション詳細］パネル上のトランスポートプロトコル	VDA 7.13	はい	はい	はい
ユーザーフレンドリな接続およびマシンの障害の説明	VDA 7.x	はい	はい	はい
履歴データの保持	VDA 7.x	はい	いいえ	いいえ
カスタムレポート	VDA 7.x	はい	いいえ	いいえ
リソース使用レポート	VDA 7.11	はい	はい	はい
CPU、メモリ、ICA RTT 条件に対応するアラート拡張	VDA 7.11	はい	いいえ	いいえ
エクスポートレポートの改善	VDA 7.x	はい	はい	はい
ログオン処理時間の内訳	VDA 7.x	はい	はい	はい
予見的な監視およびアラート	VDA 7.x	はい	いいえ	いいえ
ホストされたアプリケーションの使用量	VDA 7.x	はい	いいえ	いいえ
シングルセッション OS およびマルチセッション OS の使用	VDA 7.x	はい	いいえ	いいえ
Framehawk 仮想チャネルのサポート	VDA 7.6	はい	はい	はい

委任管理と監視

March 30, 2022

管理権限の委任機能では、管理者、役割、およびスコープという 3 つの概念が使用されます。管理者の権限は、その管理者の役割とそのスコープに基づいて定義されます。たとえば、管理者にヘルプデスク管理者の役割を割り当てて、その役割のスコープとして特定のサイトのエンドユーザーを指定できます。

付与されている管理権限により、その管理者に表示される監視のインターフェイスと実行可能なタスクが決定されます。権限により、次の内容が決定されます。

- その管理者がアクセスできる Director の表示内容。これを「ビュー」と呼びます。
- その管理者が表示したり操作したりできるデスクトップ、マシン、およびセッション。
- ユーザーセッションのシャドウやメンテナンスモードの有効化など、その管理者が実行できるコマンド。

監視では、管理者にカスタム定義された役割、または組み込みの役割を割り当てることができる委任管理者の役割がサポートされるようになりました。この役割は、使用可能な権限、つまり管理者がどのように監視を使用するかを決定します。それらの役割に適用可能なスコープを定義することもできます。スコープは、役割を適用できるオブジェクトを定義します。

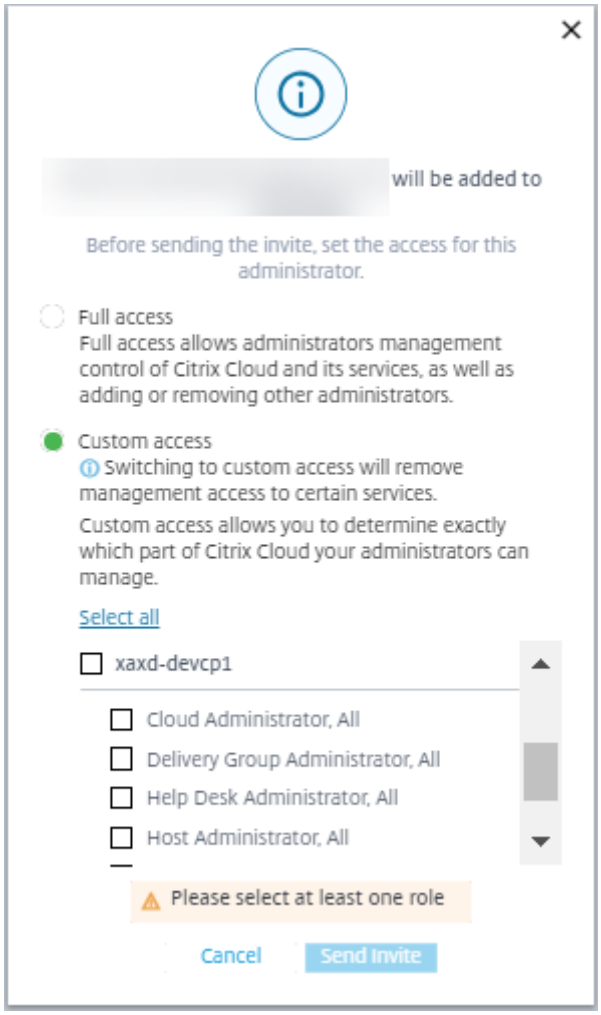
委任管理者の作成について詳しくは、「委任管理」を参照してください。

組み込みの役割および権限によって、管理者が ［監視］で実行できるタスクが決定されます:

管理者の役割	監視における権限
すべての管理権限を実行できる管理者	すべてのビューに制限なくアクセスして、ユーザーセッションのシャドウ、メンテナンスモードの有効化、傾向データのエクスポートなどすべてのコマンドを実行できます。
デリバリーグループ管理者	すべてのビューに制限なくアクセスして、ユーザーセッションのシャドウ、メンテナンスモードの有効化、傾向データのエクスポートなどすべてのコマンドを実行できます。
読み取り専用管理者	すべてのビューに制限なくアクセスして、一般的な情報と、指定されているスコープのすべてのオブジェクトを表示できます。HDX チャネルからレポートをダウンロードして、［傾向］ビューのエクスポートオプションを使って傾向データをエクスポートできます。そのほかのコマンドは実行できず、ビューで設定を変更することはできません。

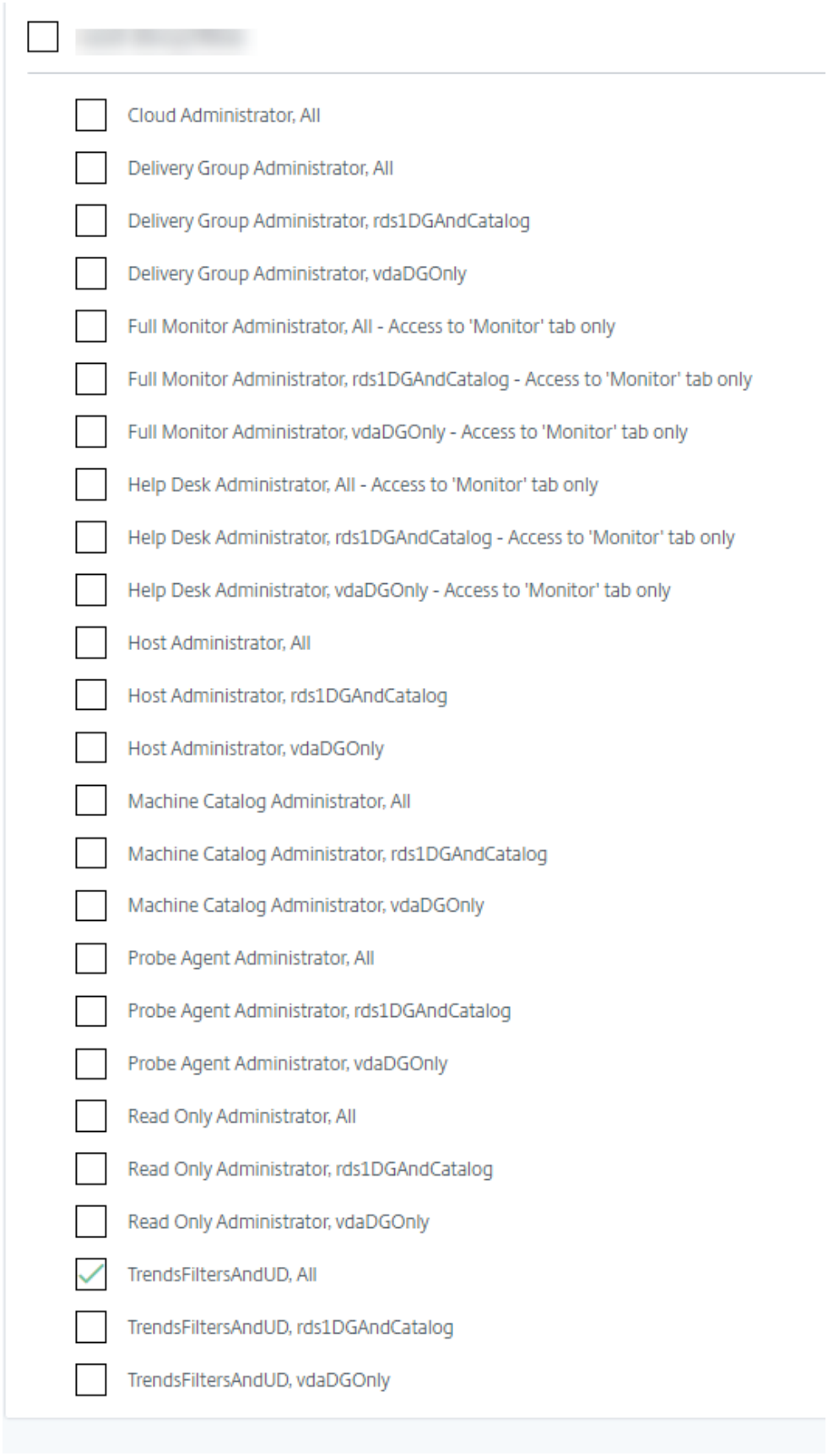
管理者の役割	監視における権限
ヘルプデスク管理者	［ヘルプデスク］および［ユーザーの詳細］ビューにのみアクセスでき、委任されたオブジェクトのみを表示できます。ユーザーセッションをシャドウしたり、そのユーザーに対してコマンドを実行したりできます。メンテナンスモードを有効にしたり解除したりできます。シングルセッション OS マシンの電源制御オプションを使用できます。［ダッシュボード］ビュー、［傾向］ビュー、［アラート］ビュー、および［フィルター］ビューにはアクセスできません。マルチセッション OS マシンの電源制御オプションは使用できません。
マシンカタログ管理者	［マシン詳細］ページ（マシンベースの検索）にのみアクセスできます。
ホスト管理者	アクセスなし。この管理者は、［監視］を使用したりデータを表示したりできません。
Probe Agent 管理者	［アプリケーション］ページへの読み取り専用アクセス。その他のページへはアクセスできません。エンドポイントマシン上で Citrix Probe Agent を実行するための役割です。
監視のすべての管理権限を実行できる管理者	［監視］タブのすべてのビューとコマンドに対するフルアクセス権限があります。
セッション管理者	［監視］タブの ［フィルター］ページでデリバリーグループを表示し、関連するセッションとマシンを管理できます。

役割（組み込みまたはカスタム）をユーザーに割り当てるには、Citrix Cloud メニューで ［**ID** およびアクセス管理］ > ［管理者］に移動します。管理者のアクセス権を追加または編集する場合、［カスタムアクセス］を選択して表示された役割から 1 つを選択できます。



カスタム役割とスコープは、［完全な構成］**>**［管理者］**>**［管理者］で定義できます。

組み込みの役割とカスタム役割は、カスタムスコープの一覧から選択できます。



データの粒度と保持

January 18, 2023

データ値の集計

Monitor Service は、ユーザーセッション使用状況、ユーザーログオンの処理性能の詳細、セッションの負荷分散の詳細、および接続とマシンのエラー情報を含む、さまざまなデータを収集します。データはカテゴリにより異なる方法で集計されます。OData Method API を使って示されたデータ値の集計を理解することは、データの解釈に不可欠です。例:

- 接続セッション（Connected Session）やマシンエラー（Machine Failure）は一定の期間の状態を示すため、その期間内の最大値として公開されます。
- ログオン期間（Logon Duration）は時間の長さを示す指標であるため、期間内の平均として公開されます。
- ログオン数（Logon Count）および接続障害（Connection Failure）は一定の期間に発生した数を示し、期間内の合計値として公開されます。

同時データ評価

重複しているセッションは同時発生していると考える必要があります。ただし、時間間隔が 1 分の場合、その 1 分内のすべてのセッションが（重複していても重複していなくても）同時と見なされます。この間隔のサイズは非常に小さいため、精度の計算に関連するパフォーマンス上のオーバーヘッドを考慮する必要はありません。2 つのセッションがその 1 時間内の別々の 1 分間に発生する場合、それらは重複しているとはみなされません。

サマリー表と生データの相関

データモデルでは、以下の 2 つの方法でメトリックが示されます:

- サマリーテーブルでは、分単位、時間単位、および日単位のメトリックを集計したものが示されます。
- 生データは、セッション、接続、アプリケーション、およびそのほかのオブジェクト内で記録された個々のイベントまたは現在の状態を示します。

データを API コール間またはそのデータモデル内で関連付けるときは、以下の概念および制限事項を考慮してください。

- 未完の間隔にはサマリーデータがありません。メトリックサマリーは長期間の履歴傾向を示すためのものであり、完結した間隔のサマリーテーブルに集計されます。データ収集の開始時（利用可能な最も古いデータ）や終了時の未完の間隔のサマリーデータはありません。1 日（間隔 =1440）の集計値の場合、最初と最後の未完の 1 日にはデータがないことを意味します。これらの未完の間隔に生データが存在しても、そのデータ

が集計されることはありません。各データ粒度の最初と最後の集計間隔は、各サマリーテーブルから最小と最大の SummaryDate を取得することで決定できます。SummaryDate 列は、間隔の開始時を示します。Granularity 列はその集計データの間隔の長さを示します。

- 時間による関連付け。前のセクションで説明したように、メトリックスは完結した間隔のサマリーテーブルに集計されます。これらの値は履歴傾向を知る目的で使用できますが、生イベントの方が集計された値よりも傾向分析に適切な状態を示している場合があります。集計値と生データとを時間ベースで比較する場合、未完の間隔や間隔の最初と最後にサマリーデータがないことを考慮する必要があります。
- 欠落イベントまたは潜在イベント集計期間で欠落または潜在しているイベントがあると、サマリーテーブルに集計されたメトリックが正確でない場合があります。Monitor Service では現在の状態の正確な維持が試行されますが、過去にさかのぼって欠落イベントや潜在イベントをサマリーテーブルに再集計することはありません。
- 接続の高可用性。接続の高可用性により、現在の接続のサマリーデータ数に差異が生じることがありますが、セッションインスタンスは生データ内で実行されています。
- データの保持期間。サマリーテーブルのデータは、生イベントデータとは異なるグルーミングスケジュールで保持されます。このため、サマリーテーブルまたは生テーブルのクリーンアップにより、データが消去されている場合があります。データの保有期間は、サマリーデータの粒度によっても異なる場合があります。低い粒度（分単位）のデータは、高い粒度（日単位）のデータよりも早くクリーンアップされます。特定の粒度のデータが消去されていても、より高い粒度のデータが存在している場合があります。API コールでは指定した粒度のデータのみが返されるため、データを取得できない場合でもその期間内のより高い粒度では取得できることがあります。
- タイムゾーン。格納されるメトリックのタイムスタンプでは UTC が使用されます。サマリーテーブルは 1 時間区切りのタイムゾーンごとに集計されます。1 時間区切りのタイムゾーンに属さない場合は、データの集計先に不整合が生じることがあります。

データの粒度と保持

［監視］で取得される集計データの粒度は、要求された時間（T）の関数です。以下の規則があります。

- 0 < T <= 30 日の場合は時間単位の粒度
- T > 31 日の場合は日単位の粒度

集計データから取得されないデータを要求すると、生のセッション（Session）および接続（Connection）情報から取得されます。このデータの量はすぐに大きくなるため、専用のスケジュールでクリーンアップされます。クリーンアップにより、意味のあるデータのみが長期間保持されます。これにより、レポートに必要な粒度を維持しながら良好なパフォーマンスが提供されます。

	設定名	対象データ	Premium の保持日数	Advanced の保持日数
1	GroomSessionsRetentionDays	1 より前の日付の後のセッションレコードと接続レコードの保有	90	31
2	GroomFailuresRetentionDays	MachineFailureLog レコードおよび ConnectionFailureLog レコード	90	31
3	GroomLoadIndexesRetentionDays	LoadIndex レコード	90	31
4	GroomDeletedRetentionDays	LifecycleState が「Deleted」である Machine エンティティ、Catalog エンティティ、DesktopGroup エンティティ、および Hypervisor エンティティ。関連する Session レコード、SessionDetail レコード、Summary レコード、Failure レコード、または LoadIndex レコードも削除されます。	90	31

	設定名	対象データ	Premium の保持日数	Advanced の保持日数
5	GroomSummariesRetentionDays	DesktopGroupSummary レコード、FailureLogSummary レコード、および LoadIndexSummary レコード。集計データ（日単位）	365	31
6	GroomMachineHotfixLogRetentionDays	Hotfix ログ Data および Controller マシンに適用された Hotfix	90	31
7	GroomHourlyRetentionDays	集計データ（時間単位）	32	31
8	GroomApplicationInstanceRetentionDays	アプリケーションインスタンスの履歴	90	該当なし
9	GroomNotificationLogRetentionDays	通知ログレコード	90	該当なし
10	GroomResourceUsageRawDataRetentionDays	ResourceUsage 生データ（生データ）	2	3
11	GroomResourceUsageHourDataRetentionDays	ResourceUsage 時間単位サマリーデータ（時間単位）	30	30
12	GroomResourceUsageDayDataRetentionDays	ResourceUsage 日単位サマリーデータ（日単位）	365	31
13	GroomProcessUsageRawDataRetentionDays	ProcessUsage 生データ（生データ）	1	1
14	GroomProcessUsageHourDataRetentionDays	ProcessUsage 時間単位データ（時間単位）	7	7
15	GroomProcessUsageDayDataRetentionDays	ProcessUsage 日単位データ（日単位）	30	30

	設定名	対象データ	Premium の保持日数	Advanced の保持日数
16	GroomSessionMetricsDataRetention	セッションメトリックデータ	1Days	1
17	GroomMachineMetricDataRetention	マシンメトリクデータ	3Days	3
18	GroomMachineMetricDaySummaryDataRetentionDays	マシンメトリクサマリーデータ	395	31
19	GroomApplicationErrorsRetention	アプリケーションエラーデータ	1Days	1
20	GroomApplicationFaultsRetention	アプリケーション障害データ	1Days	1

> 注意：
>
> Monitor Service データベースの値を変更することはできません。

データを長期間保持すると、テーブルのサイズについて以下の影響が発生します：

- 時間単位のデータ。時間単位のデータを 2 年などの長期間保持すると、1000 個のデリバリーグループがあるサイトではデータベースが以下の数式に基づいて増大します：

  「1000 個のデリバリーグループ ×24 時間/日 ×365 日/年 ×2 年＝ 17,520,000 行のデータ」集計テーブルのデータ量が多いため、パフォーマンスに大きな影響を及ぼします。ダッシュボードのデータがこのテーブルから取得されると、データベースサーバーに対する要求が高くなることがあります。データ量が過度に多いと、パフォーマンスが大きく低下することがあります。

- セッションとイベントのデータ。各セッションの開始時および接続/再接続時に収集されるデータです。大規模サイト（100,000 ユーザーなど）では、このデータの量が急速に増加します。たとえば、これらのテーブルでは 2 年間で 1TB 以上のデータが保持され、高性能なエンタープライズレベルのデータベースが必要になります。

セッション起動診断

March 31, 2024

> 注：
>
> セッション起動診断は現在プレビュー段階です。

セッション起動には、複数の Citrix コンポーネントが含まれます。セッション起動の失敗を診断するには、Citrix Monitor（つまり、Citrix Director サービス）を使用して、問題が発生した正確なコンポーネントとステージに原因を絞り込みます。問題を解決するために推奨される操作を実行します。Citrix Workspace アプリは、セッションの起動エラーの診断に使用できる 32 桁（8-4-4-4-12）のトランザクション ID を生成します。

> 注:
>
> この機能は、米国、南アジア太平洋、および EU リージョンのクラウド顧客のみが利用できます。日本および政府機関のリージョンではご利用いただけません。

前提条件

Citrix DaaS を使用している場合、オンボーディングは自動的に行われます。オンプレミスの StoreFront を使用しているクラウド顧客は、サポートされている StoreFront バージョンがオンボードされていることを確認する必要があります。

- Citrix Analytics for Performance を使用している場合は、オンプレミスの StoreFront をオンボードする手順について「データソース」を参照してください。
- Citrix Analytics for Performance を使用していない場合:
  1. `https://analytics.cloud.com/unified-datasources/perf/Citrix%20Virtual%20Apps%20and%20Desktops/site-details`に移動します。
  2. [**StoreFront** 展開に接続] をクリックし、詳細を開いて、構成ファイルをダウンロードします。詳しくは、「StoreFront を使用したオンプレミスサイトへのオンボード」を参照してください。

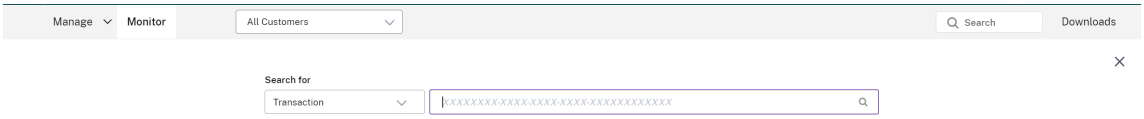
  > 注:
  >
  > クラウド管理者の役割がある管理者は、StoreFront 展開をオンボードすることが許可されますが、「監視のすべての管理権限を実行できる管理者」の役割がある管理者は、StoreFront 展開の表示のみが許可されます。

他のコンポーネントのサポートされている最小バージョンは次のとおりです:

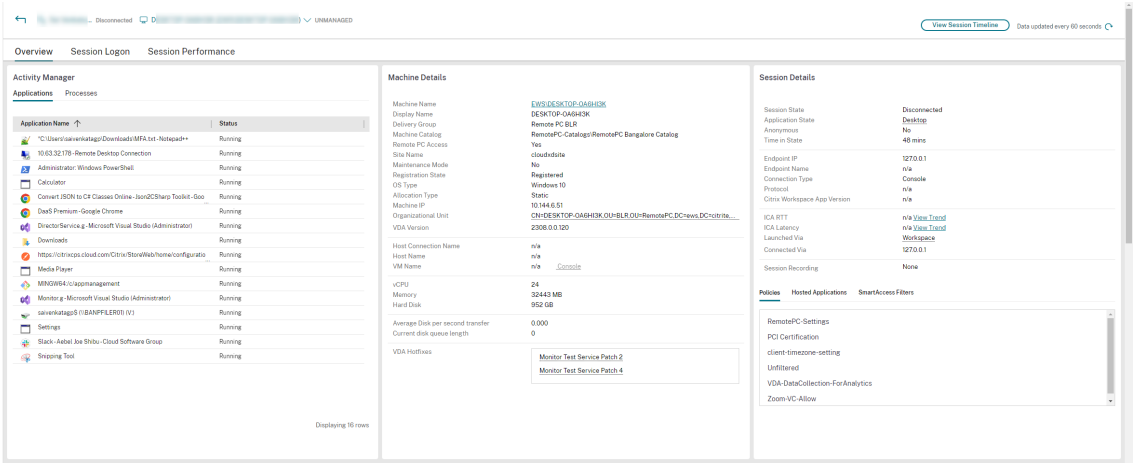
- Windows 向け Citrix Workspace アプリ 2109
- Mac 向け Citrix Workspace アプリ 2112
- Linux 向け Citrix Workspace アプリ 2112
- HTML5 向け Citrix Workspace アプリ 2110
- Chrome 向け Citrix Workspace アプリ 2110
- Android 向け Citrix Workspace アプリ 2110
- Citrix Virtual Apps and Desktops VDA バージョン 2112
- Citrix StoreFront 1912 LTSR CU4

セッションの起動エラーを診断する手順

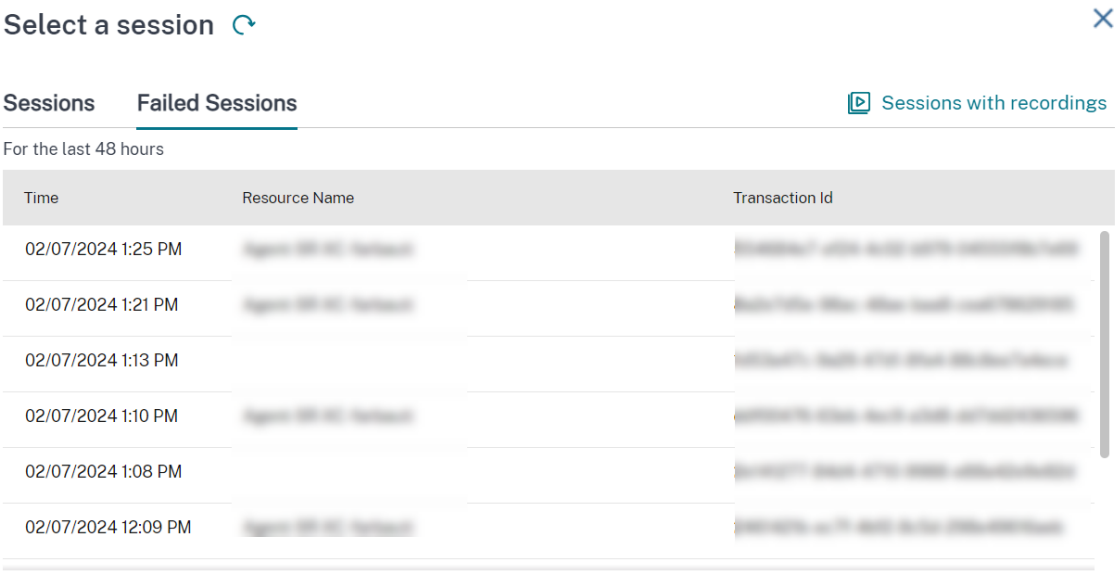
1. 失敗したセッション起動のトランザクション ID を Citrix Workspace アプリからコピーします。
2. Monitor UI で、32 桁のトランザクション ID を検索し、［詳細］をクリックします。



3. トランザクション ID が使用できない場合は、ユーザー名を使用して検索します。ユーザーのアクティビティマネージャーが表示されます。



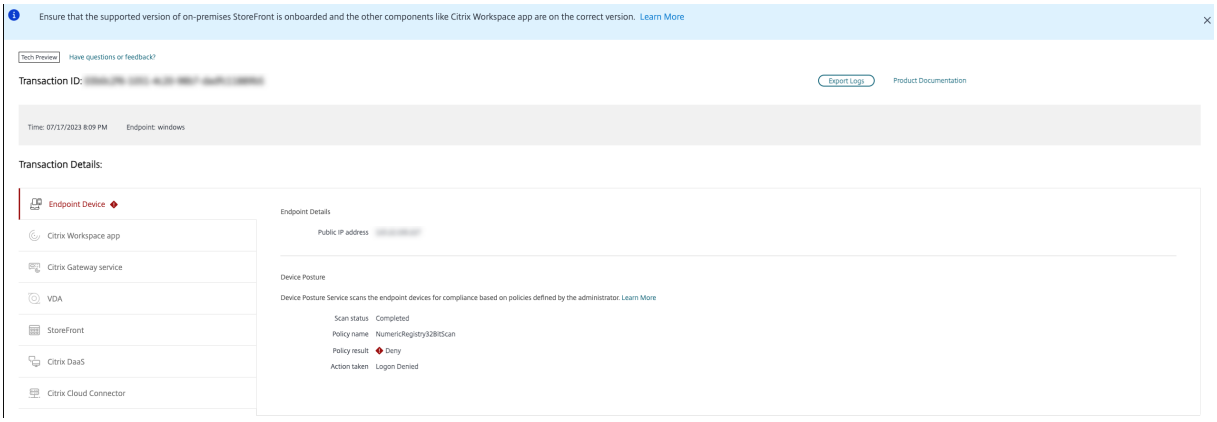
4. セッションセレクタをクリックします。［失敗したセッション］タブに移動します。過去 48 時間に失敗したセッションの一覧が表示されます。選択したセッションをクリックします。



5. Citrix Monitor は、ユーザー名、タイムスタンプ、障害が発生したアプリケーションまたはデスクトップな

ど、トランザクションに関する重要な情報を表示します。

6. ［トランザクションの詳細］パネルには、障害の発生を示すコンポーネントの一覧が含まれています。
7. コンポーネントの一覧で ［エンドポイントデバイス］をクリックして、Device Posture スキャンの状態を表示します。Device Posture サービスは、管理者が定義したポリシーに基づいて、エンドポイントデバイスのコンプライアンスをスキャンします。



スキャンの状態、ポリシー名、ポリシーの結果、および実行された操作が表示されます。Device Posture の記事で説明されているように、Device Posture サービスが DaaS で構成されていることを確認します。Device Posture によって記録されるエラーについては、「Device Posture のエラーログ」で説明されています。

1. 他のコンポーネント名をクリックして、［コンポーネントの詳細］と［最後に確認されたエラーの詳細］を確認します。
2. 障害の理由とエラーコードが表示されます。［エラーの詳細］リンクをクリックして、詳細な説明と推奨される操作を含む ［エラーコード］ セクションで特定のエラーコードを確認します。
3. ログをエクスポートして表示できます。ログファイルには、セッション起動の手順が時系列で一覧表示され、エラーが発生した正確なコンポーネントとそのステージが示されます。
4. コンポーネント間で複数の障害が発生した場合、［Transaction］ページには最後の既知の障害の詳細のみが表示されます。エクスポートされたログには、トランザクションに関連するすべての障害の詳細が含まれています。

> 注:
>
> クライアント側のエラーコードと診断情報は、Citrix StoreFront がオンボードされてデータを送信している場合にのみ使用できます。StoreFront のオンボードについて詳しくは、「前提条件」を参照してください。

Broker Agent

bka.prepare.session.failure.validation

- 説明：セッション準備要求の検証に失敗しました。

- 推奨される操作：操作を再試行してください。エラーが繰り返される場合は、コネクタが正常な状態にあることを確認してください。

bka.prepare.session.failure.rejected

- 説明：VDA が起動要求を受け入れられません。
- 推奨される操作：VDA で Citrix Delivery Agent サービスを再起動するか、VDA を再起動してください。

bka.hdx.prepare.failure.general

- 説明：HDX 準備エラー。
- 推奨される操作：VDA を再起動してください。

bka.hdx.validate.failure.ticket_not_found

- 説明：参照されたチケットまたは起動が起動キャッシュにありません。
- 推奨される操作：VDA がコネクタと通信できることを確認してください。

bka.ticketing.validate.failure.unlicensed

- 説明：起動用のライセンスを確認できません。
- 推奨される操作：Citrix サポートに連絡してください。

bka.ticketing.validate.failure.general

- 説明：チケット検証時の一般的なエラー。
- 推奨される操作：VDA のログを収集し、Citrix サポートに連絡してください。

bka.set.configuration.failure.policy

- 説明：ポリシーの設定中にエラーが発生しました。
- 推奨される操作：VDA で Citrix Delivery Agent サービスを再起動するか、VDA を再起動してください。

bka.set.configuration.failure

- 説明：構成の設定中にエラーが発生しました。
- 推奨される操作：VDA で Citrix Delivery Agent サービスを再起動するか、VDA を再起動してください。

ブローカー

brk.validate.credentials.failure.invalid

- 説明：何らかの問題が原因で、資格情報の検証に失敗しました。理由はメッセージパラメーターで表示できます。
- 推奨される操作：操作を再試行してください。エラーが繰り返される場合は、コネクタが正常な状態にあることを確認してください。

brk.resolve.machine.failure.general

- 説明：ワーカーの列挙または解決に失敗しました。理由はメッセージパラメーターで表示できます。
- 推奨される操作：このアプリケーションを起動できるマシンがブローカーに登録されていることを確認してください。使用可能なすべてのマシンが容量に達していないことを確認してください。

brk.license.check.failure.constraints

- 説明：ライセンスの制約により、セッションの起動に失敗しました。
- 推奨される操作：このタイプのアプリケーションまたはデスクトップで使用できるライセンスがあることを確認してください。

brk.resolve.machine.failure.timeout

- 説明：データベースへの接続中にブローカーがタイムアウトしました。
- 推奨される操作：サイトデータベースとの通信に問題があります。Citrix サポートに連絡してください。

brk.poweron.forlaunch.queued.failure.general

- 説明：電源操作をキューに入れることに失敗しました。
- 推奨される操作：サイトデータベースとの通信に問題があります。Citrix サポートに連絡してください。

brk.set.configuration.failure.general

- 説明：ターゲット VDA で構成を設定中に不特定のエラーが発生しました。
- 推奨される操作：VDA で Citrix Delivery Agent サービスを再起動するか、VDA を再起動してください。

brk.prepare.session.failure.host_unreachable

- 説明：VDA との通信に失敗しました。
- 推奨される操作：VDA で Citrix Delivery Agent サービスを再起動するか、VDA を再起動してください。

brk.prepare.session.failure.general

- 説明：VDA、UnsupportedClientType、または ConnectionRefused エラーでセッションを準備できませんでした。
- 推奨される操作：VDA で Citrix Delivery Agent サービスを再起動するか、VDA を再起動してください。

brk.validate.ticket.failure.license

- 説明：このセッションの有効なライセンスを取得できませんでした。
- 推奨される操作：サイトのサーバーヘルスの状態を確認し、すべてのコネクタと Citrix DDC が動作していることを確認してください。

brk.validate.ticket.failure.general

- 説明：無効なチケット発行呼び出し。
- 推奨される操作：Citrix サポートに連絡してください。

brk.reverse.prepare.failure.general

- 説明：セッション起動中の一般的なエラー。
- 推奨される操作：サイトのサーバーヘルスの状態を確認し、すべてのコネクタと Citrix DDC が動作していることを確認してください。

brk.reverse.prepare.failure.lease_revoked

- 説明：このセッションのリースは取り消されました。
- 推奨される操作：操作を再試行してください。エラーが繰り返される場合は、コネクタが正常な状態にあることを確認してください。

brk.reverse.prepare.failure.resource_unavailable

- 説明：リソースは既に使用されているか、一時的に使用できません。
- 推奨される操作：操作を再試行してください。エラーが繰り返される場合は、コネクタが正常な状態にあることを確認してください。

brk.reverse.prepare.failure.app_protection

- 説明：アプリ保護がありません。このセッションに必要です。
- 推奨される操作：この VDA でアプリ保護が有効になっていることを確認するか、アプリケーションからアプリ保護要件を削除してください。

HDX VDA Linux

VDA_LINUX_ERR_RECONNECT_PRE_LOGOFF

- 説明：ログオフ前の状態のセッションに再接続することが許可されていません。
- 推奨される操作：後で起動を再試行してください。これにより、セッションがログオフする時間ができます。

VDA_LINUX_ERR_RECONNECT_NO_SESSION

- 説明：終了していないセッションに再接続します。
- 推奨される操作：後で起動を再試行してください。それでも失敗する場合は、Citrix サポートに連絡してください。

VDA_LINUX_ERR_SAME_KEY

- 説明：接続の準備をしますが、同じセッションキーを持つ既存のセッションがあります。
- 推奨される操作：Citrix サポートに連絡してください。

VDA_LINUX_ERR_GET_FQDN

- 説明：この VDA の FQDN を取得できませんでした。
- 推奨される操作：VDA の DNS 構成が正しいことを確認してください。

VDA_LINUX_ERR_NO_CGP_LISTENER

- 説明：実行中の CGP リスナーがありません。
- 推奨される操作：［セッション画面の保持］ポリシーが有効になっていることを確認してください。CGP リスナーが VDA の予期されたポートでリッスンしていることを確認します（デフォルトのポートは 2598 で、［セッション画面の保持のポート番号］ポリシーを介して変更できます）。

VDA_LINUX_ERR_DTLS_CONNECT

- 説明: Gateway サービスへの DTLS 接続を確立できませんでした。
- 推奨される操作: Gateway サービス FQDN が VDA から到達可能であることを確認してください。パス/var/xdl/keystore/cacertsが VDA に存在することを確認します。/var/xdl/keystoreを削除し、/var/xdl/split_ca_bundle.shを実行して CA 証明書を再生成します。Gateway サービス FQDN（完全修飾ドメイン名）が VDA によって信頼されていることを確認します。

VDA_LINUX_ERR_ACCEPT_EDT_CONNECT

- 説明: クライアントからの EDT ハンドシェイクを受け入れることができませんでした。
- 推奨される操作: Citrix サポートに連絡してください。

VDA_LINUX_ERR_TCP_CONNECT

- 説明: Gateway サービスへの TCP 接続を確立できませんでした。
- 推奨される操作: Gateway サービス FQDN が VDA から到達可能であることを確認してください。

VDA_LINUX_ERR_TLS_CONNECT

- 説明: Gateway サービスへの TLS ハンドシェイクを確立できませんでした。
- 推奨される操作: パス/var/xdl/keystore/cacertsが VDA に存在することを確認してください。/var/xdl/keystoreを削除し、/var/xdl/split_ca_bundle.shを実行して CA 証明書を再生成します。Gateway サービス FQDN（完全修飾ドメイン名）が信頼されていることを確認します。

VDA_LINUX_ERR_RDVZ_HANDSHAKE

- 説明: Gateway サービスへのランデブーハンドシェイクを確立できませんでした。
- 推奨される操作: Citrix サポートに連絡してください。

VDA_LINUX_ERR_ACCEPT_ICA_CONNECT

- 説明: ICA 接続を受け入れることができませんでした。
- 推奨される操作: Citrix サポートに連絡してください。

VDA_LINUX_ERR_RECONNECT_TO_ANON_SESSION_NOT_ALLOWED

- 説明: 匿名セッションへの再接続が許可されていません。
- 推奨される操作: Citrix サポートに連絡してください。

VDA_LINUX_ERR_CONN_NOT_ALLOWED

- 説明：接続が許可されていません。
- 推奨される操作：結果コードが 3 の場合は、ライセンスの有効期限が切れていないことを確認してください。有効期限が切れていない場合は、後で起動を再試行してください。解決できない場合は、Citrix サポートに連絡してください。

VDA_LINUX_ERR_CONN_GENERAL

- 説明：接続の検証に失敗しました。
- 推奨される操作：Citrix サポートに連絡してください。

VDA_LINUX_ERR_USER_CANCELLED_LOGIN

- 説明：エンドユーザーがログオンをキャンセルしました。
- 推奨される操作：SSO が無効になっていて、エンドユーザーがログオンボックスの［キャンセル］ボタンをクリックした場合、このエラーが発生することがあります。それ以外の場合は、Citrix サポートに連絡してください。

VDA_LINUX_ERR_GET_TARGET

- 説明：ターゲットセッションの取得に失敗しました。
- 推奨される操作：Citrix サポートに連絡してください。

VDA_LINUX_ERR_START_LOGON_TIMERS

- 説明：ログオンタイマーの開始に失敗しました。
- 推奨される操作：Citrix サポートに連絡してください。

VDA_LINUX_ERR_SEND_CMD_TO_TARGET

- 説明：ターゲットセッションへのコマンドの送信に失敗しました。
- 推奨される操作：Citrix サポートに連絡してください。

VDA_LINUX_ERR_POST_RECONNECT_EVENT

- 説明：再接続イベントの投稿に失敗しました。
- 推奨される操作：Citrix サポートに連絡してください。

VDA_LINUX_ERR_RECONNECT_TIMEOUT

- 説明：ユーザーセッションタイムアウトに再接続します。
- 推奨される操作：Citrix サポートに連絡してください。

HDX VDA Windows

RENDEZVOUS_CONNECT_FAILED_TCP

- 説明：TCP を介したアウトバウンド Rendezvous トランスポート接続の試行に失敗しました。
- 推奨される操作：ネットワークの状態が悪いために、散発的なエラーが発生することがあります。これは予期されることです。これが頻繁に発生する場合は、VDA 構成を確認してから、Citrix サポートに連絡してください。

RENDEZVOUS_CONNECT_FAILED_EDT

- 説明：TCP を介したアウトバウンド Rendezvous トランスポート接続の試行に失敗しました。
- 推奨される操作：ネットワークの状態が悪いために、散発的なエラーが発生することがあります。これは予期されることです。これが頻繁に発生する場合は、VDA 構成を確認してから、Citrix サポートに連絡してください。

RENDEZVOUS_CONNECT_FAILED_PROXY

- 説明：プロキシ構成が無効なため、アウトバウンド Rendezvous トランスポート接続の試行に失敗しました。
- 推奨される操作：ランデブープロキシの設定を確認し、Citrix サポートに連絡してください。

RENDEZVOUS_CONNECT_FAILED_DTLS

- 説明：セキュアトランスポートハンドシェイクが失敗したため、アウトバウンド Rendezvous トランスポート接続の試行に失敗しました。
- 推奨される操作：ランデブー構成を確認し、暗号化構成を確認してください。Citrix サポートに連絡してください。

RENDEZVOUS_CONNECT_FAILED_TLS

- 説明：セキュアトランスポートハンドシェイクが失敗したため、アウトバウンド Rendezvous トランスポート接続の試行に失敗しました。
- 推奨される操作：ランデブー構成を確認し、暗号化構成を確認して、Citrix サポートに連絡してください。

RENDEZVOUS_CONNECT_FAILED_CGP

- 説明：CGP 構成に問題があるため、アウトバウンド Rendezvous トランスポート接続の試行に失敗しました。
- 推奨される操作：CGP（セッション画面の保持）が有効になっていて、CGP ポートがリッスンされていることを確認し、Citrix サポートに連絡してください。

CGP_SR_SUSPEND_RESUME_FAILED_TIMEOUT

- 説明：タイムアウトが原因でネットワークの中断が解決されませんでした。セッション画面の保持が接続を再開できませんでした。
- 推奨される操作：ネットワークの状態が悪いために、散発的なエラーが発生することがあります。これは予期されることです。

CGP_SR_SUSPEND_RESUME_FAILED

- 説明：予期しないエラーが原因でネットワークの中断が解決されませんでした。セッション画面の保持が接続を再開できませんでした。
- 推奨される操作：ネットワークの状態が悪いために、散発的なエラーが発生することがあります。これは予期されることです。

PREPARE_RECONNECT_REJECTED

- 説明：無効なセッションキーが原因で、VDA が受信 ICA 接続からの再接続要求を拒否しました。
- 推奨される操作：VDA の設定を確認し、Citrix サポートに連絡してください。

エラー：**PREPARE_REJECTED**

- 説明：無効なセッションキーが原因で、VDA が受信 ICA 接続からの接続要求を拒否しました。
- 推奨される操作：VDA の設定を確認し、Citrix サポートに連絡してください。

PREPARE_LISTENING_FAILED

- 説明：VDA が受信 ICA 接続のリスナーを開始できませんでした。
- 推奨される操作：ネットワーク構成を確認し、リスナーポートが他のアプリケーションで使用されていないことを確認し、Citrix サポートに連絡してください。

RENDEZVOUSCONNECTIONREQ_FAILED

- 説明：VDA は、アウトバウンド Rendezvous 接続を開始するように ICA スタックに通知できませんでした。
- 推奨される操作：ランデブー構成を確認し、ランデブープロキシ構成を確認し、CGP（セッション画面の保持）構成を確認し、Citrix サポートに連絡してください。

RENDEZVOUSCONNECTIONREQ_FAILED_PROXYCONFIG

- 説明：プロキシ構成エラーのため、VDA がアウトバウンド Rendezvous 接続の開始を ICA スタックに要求できませんでした。
- 推奨される操作：ランデブープロキシの設定を確認し、Citrix サポートに連絡してください。

ESTABLISH_SESSION_FAILED

- 説明：VDA は、受信 ICA 接続のセッションを作成できなかったか、既存のセッションに接続できませんでした。
- 推奨される操作：Citrix サポートに連絡してください。

ICA_ESTABLISH_FAILED

- 説明：ICA 接続の受け入れ、またはハンドシェイクが失敗しました。
- 推奨される操作：Citrix サポートに連絡してください。

VALIDATE_FAILED

- 説明：ブローカーが VDA からの受信 ICA 接続要求を検証できませんでした。
- 推奨される操作：Citrix サポートに連絡してください。

VALIDATE_TICKETING_FAILED

- 説明：チケット発行の問題が原因で、ブローカーは VDA からの受信 ICA 接続要求を検証できませんでした。
- 推奨される操作：Citrix サポートに連絡してください。

MCS

brk.poweron.forlaunch.execution.generalfailure

- 説明：一般的なエラー。
- 推奨される操作：Citrix サポートに連絡してください。

brk.poweron.forlaunch.execution.insufficientresourcefailure

- 説明：ハイパーバイザーのリソースが不足しているため、ハイパーバイザー操作を完了できません。
- 推奨される操作：ハイパーバイザーのリソースクォータを確認してください。解決策が見つからない場合は、Citrix サポートに連絡してください。

brk.poweron.forlaunch.execution.nosuchmanagedmachine

- 説明：マシン ID が存在しません。
- 推奨される操作：ハイパーバイザーでマシン ID を確認してください。解決策が見つからない場合は、Citrix サポートに連絡してください。

brk.poweron.forlaunch.execution.hypervisorconnectionfailure

- 説明：ハイパーバイザーへの接続を確立できません。ホストインフラストラクチャのアドレスが見つからなかったなど。
- 推奨される操作：ホストインフラストラクチャのアドレスが正しいことを確認してください。解決策が見つからない場合は、Citrix サポートに連絡してください。

brk.poweron.forlaunch.execution.invalidcredentialsfailure

- 説明：無効な資格情報。
- 推奨される操作：ハイパーバイザー接続の資格情報を確認してください。解決策が見つからない場合は、Citrix サポートに連絡してください。

brk.poweron.forlaunch.execution.authorizationfailure

- 説明：特権または資格情報が不十分です。
- 推奨される操作：ハイパーバイザー接続の資格情報に割り当てられた権限を確認してください。解決策が見つからない場合は、Citrix サポートに連絡してください。

brk.poweron.forlaunch.execution.sslcertauthfailure

- 説明：SSL 認証の問題により、接続を確立できません。
- 推奨される操作：ハイパーバイザーの接続証明書を確認してください。解決策が見つからない場合は、Citrix サポートに連絡してください。

brk.poweron.forlaunch.execution.ratelimitedfailure

- 説明：クラウド接続がレート制限を報告しています。
- 推奨される操作：ハイパーバイザーのレート制限によって要求がブロックされた場合は、後で接続を再試行してください。解決策が見つからない場合は、Citrix サポートに連絡してください。

brk.poweron.forlaunch.execution.connectorconnectionfailure

- 説明：クラウドコネクタにエラーがあります。接続の待機中にタイムアウトが発生するなど。タイムアウトに達すると、クラウドコネクタが切断されます。
- 推奨される操作：クラウドコネクタを再起動してください。それが失敗した場合は、Citrix サポートに連絡してください。

brk.poweron.forlaunch.execution.remotehclserverconnectionfailure

- 説明：HCL/remote プロキシプラグインへの接続設定時に、HCL/remote プロキシプラグインまたはエンドポイントにエラーが見つかりませんでした。
- 推奨される操作：コネクタを再起動してください。それが失敗した場合は、Citrix サポートに連絡してください。

brk.poweron.forlaunch.execution.expiredcredentialsfailure

- 説明：期限切れの資格情報が提供されました。
- 推奨される操作：ハイパーバイザー接続で使用されている期限切れの資格情報を更新してください。

brk.poweron.forlaunch.execution.mcsmachinemanagementcustomfailure

- 説明：マシン作成中のエラー。
- 推奨される操作：Citrix サポートに連絡してください。

brk.poweron.forlaunch.execution.detachdiskfailed

- 説明：仮想マシンで使用されているディスクの接続解除に失敗しました。
- 推奨される操作：Citrix サポートに連絡してください。

brk.poweron.forlaunch.execution.createclonefailed

- 説明：ハイパーバイザーでクローンディスクの作成に失敗しました。
- 推奨される操作：Citrix サポートに連絡してください。

brk.poweron.forlaunch.execution.provisionedvmnotfound

- 説明：プロビジョニングされた VM が見つかりませんでした。
- 推奨される操作：プロビジョニングされた VM をカタログから削除してください。それが失敗した場合は、Citrix サポートに連絡してください。

brk.poweron.forlaunch.execution.invalidvmstate

- 説明：VM の状態が無効なため、操作を続行できません。
- 推奨される操作：最初に VM を再起動して、操作を再試行してください。

brk.poweron.forlaunch.execution.insufficientresources

- 説明：操作中のリソースが不足しています。
- 推奨される操作：ハイパーバイザーが使用するリソースクォータを確認してください。

brk.poweron.forlaunch.execution.hypervisorinmaintenancemode

- 説明：ハイパーバイザーがメンテナンスモードであるため、操作を続行できません。
- 推奨される操作：ハイパーバイザーがメンテナンスモードになっているかどうかを確認してください。

brk.poweron.forlaunch.execution.delayed

- 説明：操作がキューに入れられています。
- 推奨される操作：プロセスが完了するのを待ってください。操作が失敗した場合は、Citrix サポートに連絡してください。

brk.poweron.forlaunch.execution.recreatevmfailed

- 説明：VM の再作成に失敗しました。
- 推奨される操作：Citrix サポートに連絡してください。

brk.poweron.forlaunch.execution.unknownvirtualmachine

- 説明：不明な仮想マシン。
- 推奨される操作：Citrix サポートに連絡してください。

brk.poweron.forlaunch.execution.ratelimitexceed

- 説明：クラウド接続がレート制限です。
- 推奨される操作：ハイパーバイザーのレート制限によって要求がブロックされた場合は、後で接続を再試行してください。

brk.poweron.forlaunch.execution.virtualdisknotyetonstorage

- 説明：仮想ディスクは保存されません。
- 推奨される操作：後で起動を再試行してください。それが失敗した場合は、Citrix サポートに連絡してください。

Profile Management

xendesktop.upm.userprofile.error.failure

- 説明：Citrix Profile Management はユーザープロファイルの処理に失敗しました。代わりに一時プロファイルを使用してください。
- 推奨される操作：このエラーによってログオンが失敗することはありません。Citrix Profile Management は、代わりに一時プロファイルを使用します。エラーのトラブルシューティングを行うには、Windows イベントログを確認してください。

xendesktop.upm.userprofile.error.timeout

- 説明：Citrix Profile Management は、指定された時間内にユーザープロファイルを処理できませんでした。
- 推奨される操作：このエラーによってログオンが失敗することはありません。Citrix Profile Management は、ユーザープロファイルの処理を続行します。エラーのトラブルシューティングを行うには、Citrix Profile Management ログを確認してください。

WEM エージェント

wem.agent.userpolicy.error.failure

- 説明：Workspace Environment Management（WEM）エージェントは、ユーザーのグループポリシーを処理できませんでした。ユーザーのログオンは続行されます。
- 推奨される操作：このエラーによってログオンが失敗することはありません。詳しくは、WEM 製品ドキュメントを参照し、WEM エージェントサービスログを確認してください。

wem.agent.userpolicy.error.timeout

- 説明：Workspace Environment Management（WEM）エージェントは、指定された時間内にユーザーのグループポリシーを処理できませんでした。ユーザーのログオンは続行されます。
- 推奨される操作：このエラーによってログオンが失敗することはありません。詳しくは、WEM 製品ドキュメントを参照し、WEM エージェントサービスログを確認してください。

Android の起動後

SessionManager.Launch.EngineLoadFailed

- 説明：ICA エンジンのロードまたは初期化に失敗しました。
- 推奨される操作：Citrix サポートに連絡してください。

SessionManager.Launch.ConnectionFailed

- 説明：接続する前にエンジンが終了しました。
- 推奨される操作：Citrix サポートに連絡してください。

SessionManager.Launch.LogonFailed

- 説明：ログインを完了せずにセッションが切断されました。
- 推奨される操作：Citrix サポートに連絡してください。

SessionManager.LeaseResolution.Failed

- 説明：リースの起動を試行できません。
- 推奨される操作：Citrix サポートに連絡してください。

SessionManager.clxmtp.SoftDeny

- 説明：エンジン CLXMTP ネゴシエーションが失敗しました（ソフト拒否）。
- 推奨される操作：Citrix サポートに連絡してください。

SessionManager.clxmtp.SoftDeny_Implicit

- 説明：エンジン CLXMTP 接続に失敗しました（暗黙的なソフト拒否）。
- 推奨される操作：Citrix サポートに連絡してください。

Transport.Connect.NoCGP_Fail

- 説明：接続に失敗しました（CGP が無効）。
- 推奨される操作：Citrix サポートに連絡してください。

Transport.Connect.FallbackFail

- 説明：接続に失敗しました。ICA フォールバックを試行しました。
- 推奨される操作：Citrix サポートに連絡してください。

Transport.Connect.Fail

- 説明：接続できません。
- 推奨される操作：Citrix サポートに連絡してください。

Android の起動前

CWA-ICADOWNLOAD_ERR_00001

- 説明：ICA 要求タイプの送信が正しくありません。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_00002

- 説明：ICA リクエストが無効です。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_00003

- 説明：ICA 要求のストアが null です。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_00004

- 説明：ICA 要求のストア URL が null です。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_00005

- 説明：ICA 要求のリソースパラメーターが null です。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_00006

- 説明：ICA 要求に提供されたリソースパラメーターは、有効なリソースタイプではありません。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_00007

- 説明：ICA 起動 URL の、ICA 要求で指定されたリソースパラメーターが null です。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_00008

- 説明：ICA 要求が Authentication Manager のパラメーターで null です。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_00009

- 説明：ICA 要求の本文が null です。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_000010

- 説明：ICA 要求の本文から HTTP エンティティを作成できませんでした。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_000011

- 説明：Authentication Manager 要求の作成の例外が原因で、ICA ファイルのダウンロードに失敗しました。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_000012

- 説明：Authentication Manager 要求の実行の例外が原因で、ICA ファイルのダウンロードに失敗しました。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_000013

- 説明：Authentication Manager 要求からの予期しない応答のため、ICA ファイルのダウンロードに失敗しました。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_000014

- 説明：Authentication Manager 応答から inputStream をコピーする際、ICA ファイルのダウンロードに失敗しました。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_000015

- 説明：Authentication Manager 応答からの inputStream を使用して、ICA ドキュメントを解析できませんでした。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_000016

- 説明：ダウンロードされた ICA ドキュメントが例外なしで null です。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_000017

- 説明：応答が失敗したため、ICA ファイルのダウンロードに失敗しました。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_000018

- 説明：リソースを利用できません。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_000019

- 説明：起動するリソースが存在しないか、有効になっていないか、ユーザーに表示されていません。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_000020

- 説明：もうアクティブなセッションがありません。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_000021

- 説明：要求されたアクティビティを実行するために必要なライセンスがサーバーにありません。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_000022

- 説明：使用可能なワークステーションがありません。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_000023

- 説明：ワークステーションに接続できません。サーバーが接続を拒否しました。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_000024

- 説明：ワークステーションがメンテナンス中であり、使用できません。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_000025

- 説明：ICA ファイルの`resourceerror`エラーのため、リソースを起動できません。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_000026

- 説明：ICA ファイルの`generalapplauncherror`エラーのため、リソースを起動できません。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_000027

- 説明：ICA ファイルの不明なエラーのため、リソースを起動できません。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_000028

- 説明：ICA ファイルの再起動エラーのため、リソースを起動できません。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_000029

- 説明：ICA ファイルの再開エラーのため、リソースを起動できません。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_000030

- 説明：ICA ファイルに未定義のエラーがあるため、リソースを起動できません。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_000031

- 説明：ICA ファイルをダウンロードできません。しかし、定義されたマップにエラーコードが見つかりません。
- 推奨される操作：Citrix サポートに連絡してください。

Linux の起動後

SessionManager.Launch.EngineLoadFailed

- 説明：ICA エンジンのロードに失敗しました。
- 推奨される操作：Citrix サポートに連絡してください。

SessionManager.Launch.Failed

- 説明：セッションの起動に失敗しました。
- 推奨される操作：Citrix サポートに連絡してください。

SessionManager.Launch.ConnectionFailed

- 説明：接続する前にエンジンが終了しました。
- 推奨される操作：起動の試行に関連する他のエラーを探してください。

SessionManager.Launch.LogonFailed

- 説明：ログインを完了せずにセッションが切断されました。
- 推奨される操作：このエラーはログインの失敗を示します（ユーザーが手動による資格情報の入力に失敗した場合など）。ユーザーのリモート VDA へのサインイン方法を調査します。

SessionManager.LeaseResolution.Failed

- 説明：リースの起動を試行できません。
- 推奨される操作：リースがクライアントマシンに同期されており、まだ有効であることを確認してください。ユーザーは、オンラインモードで Citrix Workspace にサインインして、リースの（再）同期をトリガーできます。Gateway または Cloud Connector コンポーネントが送信したエラーを探します。これらのエラーは、失敗の原因を示していることがあります。

Transport.Connect.NoCGP_Fail

- 説明：接続に失敗しました（CGP が無効）。
- 推奨される操作：クライアントが、TCP または EDT を介して、VDA に接続できない原因を調査してください。

Transport.Connect.FallbackFail

- 説明：接続に失敗しました。ICA フォールバックを試行しました。
- 推奨される操作：クライアントが、TCP または EDT を介して、Gateway、Connector、または VDA に接続できない原因を調査してください。

Transport.Connect.Fail

- 説明：Citrix Workspace アプリが、TCP、EDT、または UDP を介して、Gateway、Connector、または VDA に接続できませんでした。
- 推奨される操作：クライアントが、TCP、EDT、または UDP を介して、Gateway、Connector、または VDA に接続できない原因を調査してください。クライアントとホスト間のファイアウォールが、プロトコル（UDP/TCP）または必要なポートを許可していない可能性があります。

SessionManager.clxmtp.SoftDeny

- 説明：エンジン CLXMTP ネゴシエーションが失敗しました（ソフト拒否）。
- 推奨される操作：このエラーは、起動が必ず失敗することを示すものではありません。これは、エンジンが特定のネットワークパスを介して正常に動作できないことを示しています。Gateway または Cloud Connector コンポーネントが送信したエラーを探します。これらのエラーは、失敗の原因を示していることがあります。

SessionManager.clxmtp.SoftDeny_Implicit

- 説明：エンジン CLXMTP 接続に失敗しました（暗黙的なソフト拒否）。
- 推奨される操作：このエラーは、起動が必ず失敗することを示すものではありません。これは、エンジンが特定のネットワークパスを介して正常に動作できないことを示しています。クライアントが Connector または Gateway に接続できない原因を調査してください。ネットワークトポロジまたはファイアウォールの制限によりそのホストにアクセスできないことが予期されることがあります。

Linux の起動前

CWA-ICADOWNLOAD_ERR_00001

- 説明：Citrix Workspace アプリからの応答がないため、ストアに接続できません。
- 推奨される操作：Citrix Workspace または StoreFront がダウンしているかどうかを確認してください。また、インターネット接続を確認してください。

CWA-ICADOWNLOAD_ERR_00002

- 説明：ユーザーがセッションの起動をキャンセルしました。
- 推奨される操作：しばらくしてからセッションを再開してください。

CWA-ICADOWNLOAD_ERR_00003

- 説明：ストアに接続できません。サーバー証明書が有効であることを確認します。
- 推奨される操作：サーバー証明書がインストールされ、アクティブになっているかどうかを確認してください。

CWA-ICADOWNLOAD_ERR_00004

- 説明：起動するリソースが存在しないか、有効になっていないか、ユーザーに表示されていません。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_00005

- 説明：この要求にはワークステーションを使用できません。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_00006

- 説明：要求されたアクティビティを実行するために必要なライセンスがサーバーにありません。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_00007

- 説明：サーバーがワークステーションへの接続を拒否しました。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_00008

- 説明：要求されたワークステーションがメンテナンス中であり、使用できません。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_00009

- 説明：セッションの上限に達しました。
- 推奨される操作：管理者によって設定されたセッションの上限に達しました。セッションを再開してください。

CWA-ICADOWNLOAD_ERR_000010

- 説明：特定できない一般的なエラーです。
- 推奨される操作：Citrix サポートに連絡してください。

Mac の起動後

Desktop failed to start

- 説明：＜デスクトップ名＞デスクトップを起動できませんでした。Transaction ID - ＜トランザクション ID ＞。
- 推奨される操作：エラーの詳細を管理者に連絡してください。

Viewer failed to start

- 説明：ビューアーを起動できませんでした。Transaction ID - ＜トランザクション ID ＞。
- 推奨される操作：エラーの詳細を管理者に連絡してください。

Desktop failed to start

- 説明：＜デスクトップ名＞デスクトップは計画されたメンテナンスが行われています。Transaction ID - ＜トランザクション ID ＞。
- 推奨される操作：エラーの詳細を管理者に連絡してください。

Application failed to start

- 説明：＜アプリ名＞を起動できませんでした。
- 推奨される操作：エラーの詳細を管理者に連絡してください。

Application failed to start

- 説明：＜アプリ名＞を起動できませんでした。Transaction ID - ＜トランザクション ID ＞。
- 推奨される操作：エラーの詳細を管理者に連絡してください。

Desktop failed to start

- 説明：＜デスクトップ名＞デスクトップを起動できませんでした。
- 推奨される操作：エラーの詳細を管理者に連絡してください。

Desktop failed to start

- 説明：＜デスクトップ名＞デスクトップを起動できませんでした。Transaction ID - ＜トランザクション ID ＞。
- 推奨される操作：エラーの詳細を管理者に連絡してください。

Viewer failed to start

- 説明：ビューアーが＜アプリケーション名＞を開くことができませんでした。Transaction ID - ＜トランザクション ID ＞。
- 推奨される操作：エラーの詳細を管理者に連絡してください。

Viewer failed to start

- 説明：ビューアーがデスクトップ＜デスクトップ名＞を開くことができませんでした。Transaction ID - ＜トランザクション ID ＞。
- 推奨される操作：エラーの詳細を管理者に連絡してください。

Desktop failed to start

- 説明：＜デスクトップ名＞デスクトップは計画されたメンテナンスが行われています。
- 推奨される操作：エラーの詳細を管理者に連絡してください。

Desktop failed to start

- 説明：＜デスクトップ名＞デスクトップは計画されたメンテナンスが行われています。Transaction ID - ＜トランザクション ID ＞。
- 推奨される操作：エラーの詳細を管理者に連絡してください。

Unable to connect to the desktop

- 説明：＜デスクトップ名＞デスクトップにアクセスできません。Transaction ID - ＜トランザクション ID ＞。後で再試行してください。
- 推奨される操作：問題が解消されない場合は、管理者に連絡してください。

Mac の起動前

CWA-ICADOWNLOAD_ERR_00001

- 説明：ICA ファイルが無効です。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_00002

- 説明：起動要求がタイムアウトしました。
- 推奨される操作：インターネット接続を確認するか、Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_00003

- 説明：サーバーが応答しませんでした。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_00004

- 説明：起動するリソースが存在しないか、有効になっていないか、ユーザーに表示されていません。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_00005

- 説明：サーバーに到達できません。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_00006

- 説明：ビューアーの起動中にエラーが発生しました。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_00007

- 説明：Apple オープンイベントの起動に失敗しました。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_00008

- 説明：ビューアーパスに到達できません。
- 推奨される操作：Citrix サポートに連絡してください。

CWA-ICADOWNLOAD_ERR_00009

- 説明：ユーザーが認証をキャンセルしました。
- 推奨される操作：リソースを再起動するようにユーザーに依頼してください。

CWA-ICADOWNLOAD_ERR_000010

- 説明：ユーザーが LSI ウィンドウをキャンセルしました。
- 推奨される操作：リソースを再起動するようにユーザーに依頼してください。

CWA-ICADOWNLOAD_ERR_000011

- 説明：要求されたワークステーションがメンテナンス中であり、使用できません。
- 推奨される操作：メンテナンスが完了し、ワークステーションが使用可能になったら、ユーザーに試行を依頼してください。

CWA-ICADOWNLOAD_ERR_000012

- 説明：ユーザーのログイン資格情報を変更する必要があります。
- 推奨される操作：ログイン資格情報を変更するようにユーザーに依頼してください。

CWA-ICADOWNLOAD_ERR_000013

- 説明：リソースを接続しているセッションがアクティブではなくなりました。
- 推奨される操作：ユーザーに再試行するように依頼するか、Citrix テクニカルサポートに連絡してサポートを受けてください。

CWA-ICADOWNLOAD_ERR_000014

- 説明：ICA ファイルのダウンロードに失敗しました。
- 推奨される操作：Citrix サポートに連絡してください。

Windows の起動後

SessionManager.Launch.EngineLoadFailed

- 説明：リモートデスクトップまたはアプリケーションへの接続を確立するためのコアコンポーネントが、正しくロードまたは初期化できませんでした。エラーメッセージに追加の詳細が記載されている場合があります。
- 推奨される操作：Citrix Workspace アプリが予期したとおりに機能していません。サードパーティ（Citrix 以外）の仮想チャネル DLL または別のシステムコンポーネントが、この問題の原因である可能性があります。エラーの性質を判別するために、CDF トレースを収集して送信する必要がある場合があります。

SessionManager.Launch.ConnectionFailed

- 説明：このエラーは、起動の試行が失敗したことを示す一般的なエラーです。送信されたその他のエラーが原因を示していることがあります。
- 推奨される操作：起動の試行に関連する他のエラーを探してください。

SessionManager.Launch.LogonFailed

- 説明：このエラーは、リモートデスクトップまたはアプリケーションへの接続が確立されたことを示します。しかし、Windows（または他のオペレーティングシステム）のログインを完了せずに、セッションが切断されました。
- 推奨される操作：このエラーはいくつかのログインの失敗を示します（ユーザーが手動による資格情報の入力に失敗した場合など）。ユーザーのリモート VDA へのサインイン方法を調査します。

SessionManager.Launch.Cancelled

- 説明：Citrix エンジンの接続試行がキャンセルされました。ユーザーの操作が原因である可能性があります。
- 推奨される操作：このエラーは、接続が正常に確立されなかった原因を示していますが、正しい動作を示している可能性もあります。

SessionManager.LeaseResolution.Failed

- 説明：オフライン（リースベース）の起動が失敗したことを示します。このエラーは、リソースの有効で必須のリースがクライアントマシンで見つからなかったことが原因です。また、Gateway または Cloud Connector が起動要求を拒否したか、起動要求が何らかの理由で無効でした。
- 推奨される操作：リースがクライアントマシンに同期されており、まだ有効であることを確認してください。ユーザーは、オンラインモードで Citrix Workspace にサインインして、リースの（再）同期をトリガーできます。Gateway または Cloud Connector コンポーネントが送信したエラーを探します。これらのエラーは、失敗の原因を示していることがあります。

SessionManager.clxmtp.SoftDeny

- 説明：リースの起動が試行され、Connector または Gateway が、要求された起動を完了できないことをクライアントに通知しました。しかし、他の Connector または Gateway が起動に役立つ場合があります。
- 推奨される操作：このエラーは、起動が必ず失敗することを示すものではありません。これは、エンジンが特定のネットワークパスを介して正常に動作できないことを示しています。Gateway または Cloud Connector コンポーネントが送信したエラーを探します。これらのエラーは、失敗の原因を示していることがあります。

SessionManager.clxmtp.SoftDeny_Implicit

- 説明：リースの起動が試行されましたが、Connector または Gateway に到達できませんでした。しかし、他の Connector または Gateway が起動に役立つ場合があります。
- 推奨される操作：このエラーは、起動が必ず失敗することを示すものではありません。これは、エンジンが特定のネットワークパスを介して正常に動作できないことを示しています。クライアントが Connector または Gateway に接続できない原因を調査してください。ネットワークトポロジまたはファイアウォールの制限によりそのホストにアクセスできないことが予期されることがあります。

Transport.Connect.NoCGP_Fail

- 説明：Citrix Workspace アプリのコア（エンジン）コンポーネントが、ICA プロトコル（ポート 1494）を介して VDA ホストに接続できませんでした。このイベントが送信された場合、CGP プロトコルを介してゲートウェイまたは VDA に接続する試行は実行されなかったことになります。
- 推奨される操作：クライアントが、TCP または EDT を介して、VDA に接続できない原因を調査してください。

Transport.Connect.FallbackFail

- 説明：Citrix Workspace アプリのコア（エンジン）コンポーネントが、ICA プロトコル（ポート 1494）を介して VDA ホストに接続できませんでした。このエラーの後、Citrix Workspace アプリが、CGP プロトコル（ポート 2598）を介した Gateway または VDA への接続に失敗します。
- 推奨される操作：クライアントが、TCP または EDT を介して、Gateway、Connector、または VDA に接続できない原因を調査してください。

Transport.Connect.Fail

- 説明：Citrix Workspace アプリのコア（エンジン）コンポーネントが、CGP プロトコル（ポート 2598）を介して Gateway または VDA に接続できませんでした。このイベントが発生した場合、ICA プロトコルを介して VDA に接続する試行は実行されなかったことになります。
- 推奨される操作：クライアントが、TCP または EDT を介して、Gateway、Connector、または VDA に接続できない原因を調査してください。

Windows の起動前

CWA-ICADOWNLOAD_ERR_00001

- 説明：Citrix Workspace アプリからの応答がないため、ストアに接続できません。
- 推奨される操作：Citrix Workspace または StoreFront がダウンしているかどうかを確認してください。また、インターネット接続を確認してください。

CWA-ICADOWNLOAD_ERR_00002

- 説明：ユーザーがセッションの起動をキャンセルしました。
- 推奨される操作：しばらくしてからセッションを再開してください。

CWA-ICADOWNLOAD_ERR_00003

- 説明：ストアに接続できません。サーバー証明書が有効であることを確認します。
- 推奨される操作：エラーの詳細を IT 管理者に連絡してください。

CWA-ICADOWNLOAD_ERR_00004

- 説明：起動するリソースが存在しないか、有効になっていないか、ユーザーに表示されていません。
- 推奨される操作：エラーの詳細を IT 管理者に連絡してください。

CWA-ICADOWNLOAD_ERR_00005

- 説明：この要求にはワークステーションを使用できません。
- 推奨される操作：エラーの詳細を IT 管理者に連絡してください。

CWA-ICADOWNLOAD_ERR_00006

- 説明：要求されたアクティビティを実行するために必要なライセンスがサーバーにありません。
- 推奨される操作：エラーの詳細を IT 管理者に連絡してください。

CWA-ICADOWNLOAD_ERR_00007

- 説明：サーバーがワークステーションへの接続を拒否しました。
- 推奨される操作：エラーの詳細を IT 管理者に連絡してください。

CWA-ICADOWNLOAD_ERR_00008

- 説明：要求されたワークステーションがメンテナンス中であり、使用できません。
- 推奨される操作：エラーの詳細を IT 管理者に連絡してください。

CWA-ICADOWNLOAD_ERR_00009

- 説明：セッションの上限に達しました。
- 推奨される操作：管理者によって設定されたセッションの上限に達しました。セッションを再開してください。

CWA-ICADOWNLOAD_ERR_000010

- 説明：特定できない一般的なエラーです。
- 推奨される操作：エラーの詳細を IT 管理者に連絡してください。

ワークスペース

StoreLaunchIcaEndpoint.LaunchFailed

- 説明：起動中にエラーが発生しました。
- 推奨される操作：Citrix Virtual Apps and Desktops ログを確認してください。Citrix サポートに連絡してください。

StoreLaunchSessionEndpoint.BadRequest

- 説明：起動要求のパラメーターが無効または空でした。
- 推奨される操作：Citrix サポートに連絡してください。

StoreLaunchSessionEndpoint.FarmUnavailable

- 説明：起動に使用できるファームがありませんでした。
- 推奨される操作：Citrix Virtual Apps and Desktops ログを確認してください。

StoreLaunchSessionEndpoint.Error

- 説明：起動中に内部エラーが発生しました。
- 推奨される操作：Citrix サポートに連絡してください。

StoreGetIcaFileEndpoint.BadRequest

- 説明：要求で提供される起動チケットがありませんでした。
- 推奨される操作：Citrix サポートに連絡してください。

StoreGetIcaFileEndpoint.RetrieveIcaFileForTicketFailed

- 説明：ワークスペースが ICA ファイルを取得できませんでした。
- 推奨される操作：Citrix サポートに連絡してください。

StoreGetIcaFileEndpoint.Error

- 説明：ワークスペースが ICA ファイルを取得できませんでした。
- 推奨される操作：Citrix サポートに連絡してください。

WebProxyGetLaunchStatusEndPoint.DSAuthFailure

- 説明：認証に問題がありました。
- 推奨される操作：再認証を試行してください。Citrix サポートに連絡してください。

WebProxyGetLaunchStatusEndPoint.LaunchFailed

- 説明：アプリケーションの起動中に内部エラーが発生しました。
- 推奨される操作：Citrix サポートに連絡してください。

WebProxyGetLaunchStatusEndPoint.ResourceNotFound

- 説明：アプリケーションが見つからなかったことが原因で、起動に失敗しました。
- 推奨される操作：Citrix Virtual Apps and Desktops ログおよびアプリケーションの設定を確認してください。

WebProxyLaunchIcaEndpoint.DSAuthFailure

- 説明：認証に問題がありました。
- 推奨される操作：再認証を試行してください。Citrix サポートに連絡してください。

WebProxyLaunchIcaEndpoint.LaunchFailed

- 説明：アプリケーションの起動中に内部エラーが発生しました。
- 推奨される操作：Citrix サポートに連絡してください。

WebProxyLaunchIcaEndpoint.ResourceNotFound

- 説明：アプリケーションが見つからなかったことが原因で、起動に失敗しました。
- 推奨される操作：Citrix Virtual Apps and Desktops ログおよびアプリケーションの設定を確認してください。

WebProxySessionsLaunchIcaEndpoint.SessionNotFound

- 説明：ワークスペースが既存の HDX セッションに再接続できませんでした。セッションが終了することがあります。
- 推奨される操作：アプリケーションを再起動してください。

WebProxySessionsLaunchIcaEndpoint.DSAuthFailure

- 説明：認証に問題がありました。
- 推奨される操作：再認証を試行してください。Citrix サポートに連絡してください。

WebProxySessionsLaunchIcaEndpoint.ReconnectSessionFailed

- 説明：ワークスペースが既存の HDX セッションに再接続できませんでした。セッションが終了することがあります。
- 推奨される操作：Citrix サポートに連絡してください。

WebProxySessionsLaunchIcaEndpoint.Error

- 説明：セッションへの再接続中に内部エラーが発生しました。
- 推奨される操作：Citrix サポートに連絡してください。

WebProxySessionsGetLaunchStatusEndpoint.DSAuthFailure

- 説明：認証に問題がありました。
- 推奨される操作：再認証を試行してください。Citrix サポートに連絡してください。

WebProxySessionsGetLaunchStatusEndpoint.ReconnectSessionFailed

- 説明：ワークスペースが HDX セッションに再接続できませんでした。
- 推奨される操作：Citrix サポートに連絡してください。

WebProxySessionsGetLaunchStatusEndpoint.Error

- 説明：セッションへの再接続中に内部エラーが発生しました。
- 推奨される操作：Citrix サポートに連絡してください。

DetermineGateway.Error

- 説明：ワークスペースが、接続する Gateway を判別できませんでした。
- 推奨される操作：Gateway の構成を確認してください。Citrix サポートに連絡してください。

ConnectionRoutingProviderLaunch.Error

- 説明：ワークスペースが、接続する Gateway を判別できませんでした。
- 推奨される操作：Gateway の構成を確認してください。Citrix サポートに連絡してください。

BrokerGetAddressCall.AnonymousPrelaunchNotSupported

- 説明：ファームが匿名起動をサポートしていないことが原因で、ワークスペースがアプリケーションを起動できません。
- 推奨される操作：Citrix サポートに連絡してください。

BrokerGetAddressCall.LeasingError

- 説明：ワークスペースが Citrix Virtual Apps and Desktops ブローカーからエラーを受け取りました。
- 推奨される操作：Citrix Virtual Apps and Desktops ログを確認してください。Citrix サポートに連絡してください。

BrokerGetAddressCall.ServiceConnectionError

- 説明：ワークスペースが、ファーム内の Citrix Virtual Apps and Desktops ブローカーに接続できませんでした。
- 推奨される操作：Citrix Virtual Apps and Desktops ログを確認してください。Citrix サポートに連絡してください。

BrokerGetAddressCall.BrokerError

- 説明：ワークスペースが Citrix Virtual Apps and Desktops ブローカーからエラーを受け取りました。
- 推奨される操作：Citrix Virtual Apps and Desktops ログを確認してください。Citrix サポートに連絡してください。

BrokerGetAddressCall.LicensingError

- 説明：ライセンスエラーが原因で、ワークスペースがアプリケーションを起動できませんでした。
- 推奨される操作：Citrix Virtual Apps and Desktops ログを確認してください。Citrix サポートに連絡してください。

BrokerGetAddressCall.Error

- 説明：ワークスペースが Citrix Virtual Apps and Desktops ブローカーから VDA の詳細を取得できませんでした。
- 推奨される操作：Citrix Virtual Apps and Desktops ログを確認してください。Citrix サポートに連絡してください。

GetLaunchReference.NoAccessToken

- 説明：ワークスペースが VDA に正常に接続できません。
- 推奨される操作：Citrix Virtual Apps and Desktops ログを確認してください。Citrix サポートに連絡してください。

GetLaunchReference.BrokerError

- 説明：ワークスペースが VDA に正常に接続できません。
- 推奨される操作：Citrix Virtual Apps and Desktops ログを確認してください。Citrix サポートに連絡してください。

GetLaunchReference.Error

- 説明：ワークスペースが VDA に正常に接続できません。
- 推奨される操作：Citrix Virtual Apps and Desktops ログを確認してください。Citrix サポートに連絡してください。

GenerateIcaFile.InvalidIcaSetting

- 説明：HDX 接続の確立中に内部エラーが発生しました。
- 推奨される操作：Citrix サポートに連絡してください。

StoreIcaFileAndGetTicket.StoreIcaFileAndCreateTicketFailed

- 説明：HDX 接続の確立中に内部エラーが発生しました。
- 推奨される操作：Citrix サポートに連絡してください。

StoreIcaFileAndGetTicket.Error

- 説明：HDX 接続の確立中に内部エラーが発生しました。
- 推奨される操作：Citrix サポートに連絡してください。

GetFasVdaLogonTicket.Error

- 説明：HDX 接続の確立中に内部エラーが発生しました。
- 推奨される操作：Citrix サポートに連絡してください。

GenerateSTATicket.Error

- 説明：HDX 接続の確立中に内部エラーが発生しました。
- 推奨される操作：Citrix サポートに連絡してください。

GetVdaAddress.Error

- 説明：HDX 接続の確立中に内部エラーが発生しました。
- 推奨される操作：Citrix サポートに連絡してください。

GetTicket.NoAccessToken

- 説明：HDX 接続の確立中に内部エラーが発生しました。
- 推奨される操作：Citrix サポートに連絡してください。

GetTicket.BrokerError

- 説明：Citrix Virtual Apps and Desktops ブローカーは HDX セッションを起動できませんでした。
- 推奨される操作：エラーメッセージ内の ID を確認し、Citrix Virtual Apps and Desktops ログを確認してください。

GetTicket.ServiceConnectionError

- 説明：ワークスペースが Citrix Virtual Apps and Desktops ブローカーに接続できませんでした。
- 推奨される操作：Citrix サポートに連絡してください。

GetTicket.Error

- 説明：HDX 接続の確立中に内部エラーが発生しました。
- 推奨される操作：Citrix サポートに連絡してください。

GetNetscalerConfigurationByCustomer.Error

- 説明：HDX 接続の確立中に内部エラーが発生しました。
- 推奨される操作：Citrix サポートに連絡してください。

DiscoverMPSServerCapabilities.Error

- 説明：Citrix Virtual Apps and Desktops ブローカーへの要求で問題が発生しました。
- 推奨される操作：Citrix Virtual Apps and Desktops ログを確認してください。Citrix サポートに連絡してください。

GetResourceLocationNetScalerConfig.Error

- 説明：HDX 接続の確立中に内部エラーが発生しました。
- 推奨される操作：Citrix サポートに連絡してください。

GetCustomerResourceLocations.Error

- 説明：HDX 接続の確立中に内部エラーが発生しました。
- 推奨される操作：Citrix サポートに連絡してください。

GetResourceLocationFromResourceProvider.Error

- 説明：HDX 接続の確立中に内部エラーが発生しました。
- 推奨される操作：Citrix サポートに連絡してください。

GetNetScalerGatewayInfo.Error

- 説明：HDX 接続の確立中に内部エラーが発生しました。
- 推奨される操作：Citrix サポートに連絡してください。

GetCustomerEntitlements.Error

- 説明：HDX 接続の確立中に内部エラーが発生しました。
- 推奨される操作：Citrix サポートに連絡してください。

GetResourceLocationForServerFeed.Error

- 説明：HDX 接続の確立中に内部エラーが発生しました。
- 推奨される操作：Citrix サポートに連絡してください。

GetResourceInformation.Error

- 説明：HDX 接続の確立中に内部エラーが発生しました。
- 推奨される操作：Citrix サポートに連絡してください。

サービスとしての **Citrix Gateway**

CGS-ICASN_ERR_00001

- 説明：要求の解析エラーが原因で、アプリケーションの起動に失敗しました。
- 推奨される操作：Citrix サポートに連絡してください。

CGS-ICASN_ERR_00002

- 説明：認証チケットの検証に失敗しました。
- 推奨される操作：Citrix サポートに連絡してください。

CGS-ICASN_ERR_00003

- 説明：認証チケットの検証に失敗しました。
- 推奨される操作：Citrix サポートに連絡してください。

CGS-ICASN_ERR_00004

- 説明：認証チケットの検証に失敗しました。
- 推奨される操作：Citrix サポートに連絡してください。

CGS-ICASN_ERR_00005

- 説明：Connector への接続を確立できませんでした。
- 推奨される操作：コネクタの状態を確認してください。問題が解決されない場合は、Citrix サポートに連絡してください。

CGS_ICASN_ERR_00006

- 説明：Connector への接続要求がタイムアウトしました。
- 推奨される操作：コネクタの状態を確認してください。コネクタ/VDA と NGS 間でプロキシ設定がトラフィックをブロックしていないかどうかを確認してください。VDA と Connector 間の接続を確認してください。問題が解決されない場合は、Citrix サポートに連絡してください。

CGS_ICASN_ERR_00007

- 説明：Citrix Workspace アプリが接続を閉じました。
- 推奨される操作：クライアント側のネットワーク接続が安定していることを確認してください。問題が解決されない場合は、Citrix サポートに連絡してください。

CGS_ICASN_ERR_00008

- 説明：バックエンドが接続を閉じました。
- 推奨される操作：コネクタの状態を確認してください。Connector/VDA からパブリックネットワーク（NGS）へのネットワークの安定性を確認してください。問題が解決されない場合は、Citrix サポートに連絡してください。

CGS_ICASN_ERR_00009

- 説明：VDA から NGS への接続の確立（Rendezvous）に失敗しました。
- 推奨される操作：コネクタの状態を確認してください。VDA が NGS サービスに到達できる必要があります。VDA と Connector 間の接続を確認してください。問題が解決されない場合は、Citrix サポートに連絡してください。

CGS_ICASN_ERR_00010

- 説明：EDT から TCP へのフォールバック。EDT の前提条件を確認してください。
- 推奨される操作：Rendezvous を有効にし、VDA が UDP を介して NGS サービスに到達できる必要があります。問題が解決されない場合は、Citrix サポートに連絡してください。

CGS_ICASN_ERR_00011

- 説明：NGS 内部サービスにエラーが発生しました。
- 推奨される操作：Citrix サポートに連絡してください。

CGS_ICASN_ERR_00012

- 説明：NGS 内部サービスにエラーが発生しました。
- 推奨される操作：Citrix サポートに連絡してください。

CGS_ICASN_ERR_00013

- 説明：GCT 検証でエラーが発生しました。
- 推奨される操作：Citrix サポートに連絡してください。

CGS_ICASN_ERR_00014

- 説明：GCT 検証でエラーが発生しました。
- 推奨される操作：Citrix サポートに連絡してください。

CGS_ICASN_ERR_00015

- 説明：NGS 内部サービスにエラーが発生しました。
- 推奨される操作：Citrix サポートに連絡してください。

CGS_ICASN_ERR_00016

- 説明：NGS 内部サービスにエラーが発生しました。
- 推奨される操作：Citrix サポートに連絡してください。

CGS_ICASN_ERR_00017

- 説明：NGS 内部サービスにエラーが発生しました。
- 推奨される操作：Citrix サポートに連絡してください。

CGS_ICASN_ERR_00018

- 説明：認証チケットの検証に失敗しました。
- 推奨される操作：Citrix サポートに連絡してください。

CGS_ICASN_ERR_00019

- 説明：認証チケットの検証に失敗しました。
- 推奨される操作：Citrix サポートに連絡してください。

CGS_ICASN_ERR_00020

- 説明：CGS 内部ライセンスのエラー。
- 推奨される操作：Citrix サポートに連絡してください。

CGS_ICASN_ERR_00021

- 説明：機能フラグが無効になっていることが原因で、Rendezvous v2 がフォールバックします。
- 推奨される操作：Citrix サポートに連絡してください。

CGS_ICASN_ERR_00022

- 説明：NGS 内部サービスにエラーが発生しました。
- 推奨される操作：Citrix サポートに連絡してください。

CGS_ICASN_ERR_00023

- 説明：CLXMTP 交換のタイムアウト。
- 推奨される操作：コネクタが正常であり、NGS サービスに到達できることを確認してください。問題が解決されない場合は、Citrix サポートに連絡してください。

CGS_ICASN_ERR_00024

- 説明：CLXMTP VSR 検証でエラーが発生しました。
- 推奨される操作：Citrix サポートに連絡してください。

CGS_ICASN_ERR_00025

- 説明：CLXMTP VSR 検証でエラーが発生しました。
- 推奨される操作：Citrix サポートに連絡してください。

CGS_ICASN_ERR_00026

- 説明：Connector が CLXMTP で使用できません。
- 推奨される操作：コネクタがリソースの場所に対して正常な状態にあるかどうかを確認してください。問題が解決されない場合は、Citrix サポートに連絡してください。

CGS_ICASN_ERR_00027

- 説明：最大試行後、Connector への CLXMTP リダイレクトが失敗しました。
- 推奨される操作：コネクタがリソースの場所に対して正常な状態にあるかどうかを確認してください。`Citrix ClxMtp Service`サービスがすべてのコネクタで実行されていることを確認してください。Citrix サポートに連絡してください。

CGS_ICASN_ERR_00028

- 説明：Controller との通信に失敗しました。
- 推奨される操作：Citrix サポートに連絡してください。

成功：**CGS_ICASN_SUCCESS_00001**

- 説明：セッション起動要求を受信しました。
- 推奨される操作：該当なし

成功：**CGS_ICASN_SUCCESS_00002**

- 説明：セッション起動要求が完了しました。
- 推奨される操作：該当なし

XAXD プロキシ

XDPXY_INF_00001

- 説明：ブローカーが、受信接続の準備をするために VDA に要求を送信します。
- 推奨される操作：該当なし

XDPXY_INF_00002

- 説明：VDA が、ブローカーによる接続要求を確認します。
- 推奨される操作：該当なし

XDPXY_ERR_00001

- 説明：VDA との通信に失敗しました。
- 推奨される操作：Connector の状態を確認してください。詳しくは、「Citrix Cloud Connector」およびCTX224133を参照してください。
  - VDA で Citrix Delivery Agent サービスを再起動するか、VDA を再起動してください。
  - Connector と Broker 間に Web プロキシがある場合は、適切に構成されていることを確認してください。
  - 問題が解決されない場合は、Citrix サポートに連絡してください。

XDPXY_ERR_00002

- 説明：XaxdProxy が、VDA からの応答を待ってタイムアウトしました。
- 推奨される操作：Connector の状態を確認してください。詳しくは、「Citrix Cloud Connector」およびCTX224133を参照してください。
  - VDA で Citrix Delivery Agent サービスを再起動するか、VDA を再起動してください。
  - Connector と Broker 間に Web プロキシがある場合は、適切に構成されていることを確認してください。
  - 問題が解決されない場合は、Citrix サポートに連絡してください。

XDPXY_ERR_00003

- 説明：要求を実行しようとしたときに、WCF フォールトまたは例外が発生しました。
- 推奨される操作：Connector の状態を確認してください。詳しくは、「Citrix Cloud Connector」およびCTX224133を参照してください。
  - VDA で Citrix Delivery Agent サービスを再起動するか、VDA を再起動してください。
  - Connector と Broker 間に Web プロキシがある場合は、適切に構成されていることを確認してください。
  - 問題が解決されない場合は、Citrix サポートに連絡してください。

XDPXY_INF_00003

- 説明：受信 ICA または RDP 接続の検証要求が、スタックによって呼び出されます。
- 推奨される操作：該当なし

XDPXY_INF_00004

- 説明：受信 ICA または RDP 接続の検証が確立されます。
- 推奨される操作：該当なし

XDPXY_ERR_00001

- 説明：VDA プロキシとの通信に失敗しました。
- 推奨される操作：Connector の状態を確認してください。詳しくは、「Citrix Cloud Connector」およびCTX224133を参照してください。
  - VDA で Citrix Delivery Agent サービスを再起動するか、VDA を再起動してください。
  - Connector と Broker 間に Web プロキシがある場合は、適切に構成されていることを確認してください。

  - 問題が解決されない場合は、Citrix サポートに連絡してください。

XDPXY_ERR_00002

- 説明：XaxdProxy が、VDA プロキシからの応答を待ってタイムアウトしました。
- 推奨される操作：Connector の状態を確認してください。詳しくは、「Citrix Cloud Connector」およびCTX224133を参照してください。
  - VDA で Citrix Delivery Agent サービスを再起動するか、VDA を再起動してください。
  - Connector と Broker 間に Web プロキシがある場合は、適切に構成されていることを確認してください。
  - 問題が解決されない場合は、Citrix サポートに連絡してください。

XDPXY_ERR_00003

- 説明：要求を実行しようとしたときに、例外が発生しました。
- 推奨される操作：Connector の状態を確認してください。詳しくは、「Citrix Cloud Connector」およびCTX224133を参照してください。
  - VDA で Citrix Delivery Agent サービスを再起動するか、VDA を再起動してください。
  - Connector と Broker 間に Web プロキシがある場合は、適切に構成されていることを確認してください。
  - 問題が解決されない場合は、Citrix サポートに連絡してください。

XDPXY_INF_00005

- 説明：VDA に直接 HDX セッショントラフィックを要求します。
- 推奨される操作：該当なし

XDPXY_INF_00006

- 説明：VDA が、HDX セッショントラフィック用に、Citrix Cloud コントロールプレーンとの直接接続を確立します。
- 推奨される操作：該当なし

XDPXY_INF_00007

- 説明：クライアントは、リソースのオンプレミス StoreFront に接続要求を送信します。
- 推奨される操作：該当なし

XDPXY_INF_00008

- 説明：オンプレミスの StoreFront が、クライアントからのリソースの接続要求を受け入れます。
- 推奨される操作：該当なし

XDPXY_ERR_00004

- 説明：XaxdProxy が、接続試行時に HTTP エラーの応答を受け取りました。
- 推奨される操作：Connector の状態を確認してください。詳しくは、「Citrix Cloud Connector」およびCTX224133を参照してください。
  - Connector からパブリックネットワークへのネットワークの安定性を確認してください。
  - Connector と Broker 間に Web プロキシがある場合は、適切に構成されていることを確認してください。
  - 問題が解決されない場合は、Citrix サポートに連絡してください。

XDPXY_ERR_00006

- 説明：XML 要求の形式が無効です。
- 推奨される操作：Citrix サポートに連絡してください。

XDPXY_ERR_00007

- 説明：XML 要求の資格情報のヘッダーまたは形式、あるいはその両方が無効です。
- 推奨される操作：ログアウトし、再度ログインして、操作を再試行します。問題が解決しない場合は、Citrix サポートに連絡してください。

XDPXY_INF_00011

- 説明：サービス継続性の起動が、WSA を介してユーザーによって要求されます。
- 推奨される操作：該当なし

XDPXY_INF_00012

- 説明：サービス継続性の起動が、WSA を介してユーザーによって要求されます。
- 推奨される操作：該当なし

XDPXY_ERR_00004

- 説明：接続試行時に、XaxdProxy で HTTP エラーが発生しました。
- 推奨される操作：Connector の状態を確認してください。詳しくは、「Citrix Cloud Connector」およびCTX224133を参照してください。
  - Connector と Broker 間に Web プロキシがある場合は、適切に構成されていることを確認してください。
  - 問題が解決されない場合は、Citrix サポートに連絡してください。

XDPXY_ERR_00008

- 説明：XaxdProxy が応答の待機中にタイムアウトしたため、サービス継続性の起動に失敗しました。
- 推奨される操作：Connector の状態を確認してください。詳しくは、「Citrix Cloud Connector」およびCTX224133を参照してください。
  - Connector と Broker 間に Web プロキシがある場合は、適切に構成されていることを確認してください。
  - 問題が解決されない場合は、Citrix サポートに連絡してください。

XDPXY_ERR_00009

- 説明：リースがブロックされている、または取り消されている、あるいはその両方が原因で、サービス継続性の起動に失敗しました。
- 推奨される操作：エラーの詳細を Citrix Cloud 管理者に連絡してください。詳しくは、「サービス継続性」のドキュメントを参照してください。
  - 問題が解決されない場合は、Citrix サポートに連絡してください。

Citrix DaaS for Citrix Service Provider

February 9, 2024

この記事では、**Citrix Service Provider**（**CSP**）で Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）を Citrix Cloud のテナント顧客向けに設定する方法について説明します。Citrix パートナーが使用できる機能の概要については、「パートナー向けの Citrix Cloud」を参照してください。

要件

- Citrix Service Provider パートナーである。
- Citrix Cloud アカウントがある。
- Citrix DaaS のサブスクリプションがある。

制限事項と既知の問題

制限事項

- テナント名の変更がすべてのインターフェイスに適用されるまでに最大 24 時間かかります。
- テナントを作成する場合、メールアドレスは一意である必要があります。
- ［管理］**>**［完全な構成］では、スコープ（モニターに相当）によるフィルタリングは使用できません。スコープに接続されているリソースを表示するには、左側ペインで ［管理者］を選択します。［スコープ］タブでスコープを選択し、［操作］ペインの ［スコープの編集］を選択します。

既知の問題

- スコープがリソースに割り当てられた後、管理コンソールを使用してスコープの削除または割り当て解除を行うことができません。これらのタスクは、PowerShell を使用して実行できます。
- ［管理］**>**［完全な構成］では、スコープは適用されません。マシンカタログ、デリバリーグループ、およびアプリケーショングループを作成するときに、適切なスコープを選択する必要があります。
- 15 を超えるスコープが作成された場合（自動作成およびカスタム）、管理者の Citrix Cloud カスタムアクセス情報（[**ID** およびアクセス管理］**>**［管理者］）が正しく表示されません。回避策：スコープを 15 以下に制限します。

顧客の追加

1. Citrix Service Provider の資格情報で Citrix Cloud にサインインします。左上のメニューで ［顧客］を選択します。
2. 顧客ダッシュボードから、［招待または追加］を選択します。要求される情報を指定します。
3. 顧客が Citrix Cloud アカウントを持っていない場合、顧客を追加すると顧客アカウントが作成されます。顧客を追加すると、管理者はその顧客のアカウントのフルアクセス管理者として自動的に追加されます。
4. 顧客が Citrix Cloud アカウントを持っている場合：

    a) Citrix Cloud の URL が表示されるので、これをコピーして顧客に送信します。このプロセスについて詳しくは、「顧客を接続に招待する」を参照してください。
    b) 顧客は自分のアカウントへのフルアクセス管理者として、管理者を追加する必要があります。「Citrix Cloud アカウントに管理者を追加する」を参照する。

［管理］および ［監視］コンソールでは、後でさらに管理者を追加したり、管理者が表示できる顧客を制御したりできます。

Citrix DaaS を顧客に追加する

1. Citrix Service Provider の資格情報で Citrix Cloud にサインインします。左上のメニューで ［顧客］を選択します。
2. 顧客ダッシュボードから、顧客の省略記号メニューで ［サービスの追加］を選択します。
3. ［追加するサービスを選択する］で、［**Virtual Apps and Desktops**］を選択します。
4. 次に、［続行］を選択します。

この手順を完了すると、顧客が Citrix DaaS のサブスクリプションにオンボードされます。

オンボードが完了すると、自動的に Citrix DaaS に新しい顧客スコープが作成されます。スコープは、［管理］**>** ［完全な構成］画面に表示されます。このスコープはその顧客に固有です。スコープの名前を変更することはできますが、削除することはできません。

このスコープを使用して、他の管理者のアクセスを調整します。たとえば、10 人の顧客と 2 人の管理者がいるとします。一意のスコープを使用すると、1 人の管理者のアクセスを 3 人の顧客のみに制限できます。もう 1 人の管理者は、これら 3 人の顧客の 1 人と、他の 2 人の顧客にアクセスできます。詳しくは、「顧客への管理者アクセスの制御」を参照してください。

リソースの場所を設定する

リソースの場所には、顧客にアプリやデスクトップを提供するマシン、および Citrix Cloud Connector などのインフラストラクチャコンポーネントが保持されます。詳しくは、「Citrix Cloud への接続」を参照してください。

カタログとグループがアプリとデスクトップを配信するように設定する

> 注:
>
> テナント顧客の DaaS を管理するには、CSP 顧客のアカウントに切り替える必要があります。これを行うには、右上のメニューで顧客名をクリックし、［顧客を変更］をクリックします。

カタログは、同一の仮想マシンのグループです。カタログを作成すると、イメージがマシンを作成するためのテンプレートとして（他の設定とともに）使用されます。詳しくは、「マシンカタログの作成」を参照してください。

デリバリーグループは、いくつかのマシンカタログから選択したマシンをグループ化したものです。デリバリーグループでは、それらのマシンを使用できるユーザーと、そのユーザーに提供するアプリケーションまたはデスクトップを指定します。詳しくは、「デリバリーグループの作成」を参照してください。

アプリケーショングループを使用すると、アプリケーションのコレクションを管理できます。異なるデリバリーグループ間で共有されているアプリケーションや、デリバリーグループ内のユーザーのサブセットによって使用されるア

プリケーションのアプリケーショングループを作成できます。詳しくは、「アプリケーショングループの作成」を参照してください。

グループを構成するときは、次のことを確認してください:

- デリバリーグループのスコープは、マシンカタログのスコープのサブセットです。たとえば、カタログのスコープが A と B であると仮定します。デリバリーグループのスコープは、A または B か、A および B のいずれかです。
- アプリケーショングループのスコープは、デリバリーグループのスコープのサブセットです。たとえば、アプリケーショングループに関連付けられたデリバリーグループのスコープが A と B であるとします。アプリケーショングループのスコープは A または B か、A および B のいずれかです。

フェデレーションドメイン

フェデレーションドメインを使用すると、顧客ユーザーは、リソースの場所に関連付けられたドメインの資格情報を使用して、ワークスペースにサインインできます。これにより、顧客ユーザーがカスタムワークスペースの URL（customer.cloud.com など）を使用してアクセスできる専用のワークスペースを顧客に提供できます。リソースの場所は引き続き Citrix Cloud アカウント上にあります。顧客が Citrix Serivce Provider ワークスペースの URL（csppartner.cloud.com など）を使用してアクセスできる共有ワークスペースとともに、専用のワークスペースを提供できます。

顧客が専用のワークスペースにアクセスできるようにするには、管理する適切なドメインに顧客を追加します。ワークスペースの構成でワークスペースを構成した後、顧客のユーザーはワークスペースにサインインして、利用可能にしたアプリとデスクトップにアクセスできます。

ドメインへの顧客の追加

1. Citrix Service Provider の資格情報で Citrix Cloud にサインインします。左上のメニューで ［顧客］を選択します。
2. 顧客ダッシュボードから、左上のメニューにある ［**ID** およびアクセス管理］を選択します。
3. ［ドメイン］タブで、ドメインの省略記号メニューにある ［フェデレーションドメインの管理］を選択します。
4. ［フェデレーションドメインの管理］カードの ［利用可能な顧客］列で、ドメインに追加する顧客を選択します。顧客名の横にあるプラス記号を選択します。これで、選択した顧客が ［フェデレーション顧客］列に表示されるようになりました。繰り返し他の顧客を追加します。完了したら、［適用］を選択します。

ドメインからの顧客の削除

管理しているドメインから顧客を削除すると、顧客のユーザーはドメインの資格情報を使用してワークスペースにアクセスできなくなります。

1. Citrix Cloud メニューから、［**ID** およびアクセス管理］を選択し、次に ［ドメイン］を選択します。

2. 管理するドメインを見つけて、省略記号（…）ボタンを選択します。［フェデレーション ドメインの管理］を選択します。
3. フェデレーション顧客のリストから、削除する顧客を探すか検索して［X］ボタンを選択します。リスト内のすべての顧客をドメインから削除する場合は、［すべて削除］を選択します。選択した顧客が削除対象の顧客のリストに移動します。
4. ［適用］を選択します。
5. 選択した顧客を確認して ［顧客の削除］を選択します。

顧客への管理者アクセスの制御

Citrix DaaS を顧客に追加したときに作成された一意のスコープを使用して、顧客への管理者アクセスを制御できます。アクセスの設定は、管理者を追加するときまたは後からでも可能です。

Citrix DaaS で役割とスコープを使用してアクセスを制限する方法については、「委任管理」を参照してください。

アクセスが制限された管理者の追加

1. Citrix Service Provider の資格情報で Citrix Cloud にサインインします。左上のメニューで ［顧客］を選択します。
2. 顧客ダッシュボードから、左上のメニューにある ［**ID** およびアクセス管理］を選択します。
3. ［管理者］タブで、［追加する管理者の場所］を選択してから ［**Citrix ID**］を選択します。
4. 管理者として追加するユーザーのメールアドレスを入力して、［招待］を選択します。
5. 管理者に適切なアクセス権限を設定します。Citrix Cloud およびサブスクライブされたすべてのサービスの管理制御を管理者に行わせる場合以外は、［カスタムアクセス］を選択することをお勧めします。
6. ［カスタムアクセス］を選択した後、必要に応じて、Citrix DaaS の役割とスコープのペアを 1 つ以上選択します。顧客用に作成された一意のスコープを含むエントリのみを有効にしてください。
7. 役割とスコープのペアを選択したら、［招待を送信する］を選択します。

管理者が招待を受け入れると、管理者は割り当てられたアクセス権を持つようになります。

管理者の委任管理権限の編集

1. Citrix Service Provider の資格情報で Citrix Cloud にサインインします。左上のメニューで ［顧客］を選択します。
2. 顧客ダッシュボードから、左上のメニューにある ［**ID** およびアクセス管理］を選択します。
3. ［管理者］タブで、管理者の省略記号メニューから ［アクセスの編集］を選択します。
4. 必要に応じて、Citrix DaaS の役割とスコープのペアを選択して消去します。顧客用に作成された一意のスコープを含むエントリのみを有効にしてください。
5. ［**Save**］を選択します。

顧客管理者および割り当てられた役割とスコープの表示

1. Citrix Service Provider の資格情報で Citrix Cloud にサインインします。左上のメニューで ［顧客］を選択します。
2. 顧客ダッシュボードから、左上のメニューで ［マイサービス］**>** ［**DaaS**］を選択します。
3. Citrix DaaS で、［管理］**>** ［完全な構成］を選択します。
4. 左側ペインで ［管理者］を選択します。

情報は次の 3 つのタブで利用できます:

- ［管理者］タブには、作成された管理者およびその役割とスコープが一覧表示されます。
- ［役割］タブにはすべての役割が一覧表示されます。役割の詳細を表示するには、中央ペインでその役割を選択します。ペインの下部に、その役割のオブジェクトの種類および許可される権限が一覧表示されます。ここで［管理者］タブをクリックすると、その役割が割り当てられている管理者が表示されます。
- ［スコープ］タブには、Citrix パートナーの顧客用に生成されたスコープを含むすべてのスコープが一覧表示されます。

ワークスペースの構成

顧客には独自のワークスペースがあり、固有の`customer.cloud.com`の URL が設定されています。このワークスペースは、顧客のユーザーが公開されているアプリとデスクトップにアクセスする場所です。

ワークスペースの URL は 2 つの場所に表示されます:

- 顧客ダッシュボードから、左上のメニューにある ［ワークスペース構成］を選択します。
- Citrix DaaS の ［ようこそ］ページ（[概要］タブ）では、ページの下部に Workspace URL が表示されます。

ワークスペースへのアクセスと認証を変更できます。ワークスペースの外観と基本設定をカスタマイズすることも可能です。詳しくは、以下の記事を参照してください:

- ワークスペースの構成
- セキュアなワークスペース

顧客のサービスの監視

Citrix Service Provider 環境の ［監視］ダッシュボードは、基本的には Citrix Service Provider 以外の環境と同じです。詳しくは、「監視」を参照してください。

デフォルトでは、［監視］ダッシュボードにはすべての顧客に関する情報が表示されます。1 人の顧客に関する情報を表示するには、［顧客を選択します］を使用します。

顧客の監視画面を表示する機能は、管理者が設定したアクセス権によって制御されることに注意してください。アクセス権には、顧客の固有のスコープを含む役割とスコープのペアが含まれている必要があります。

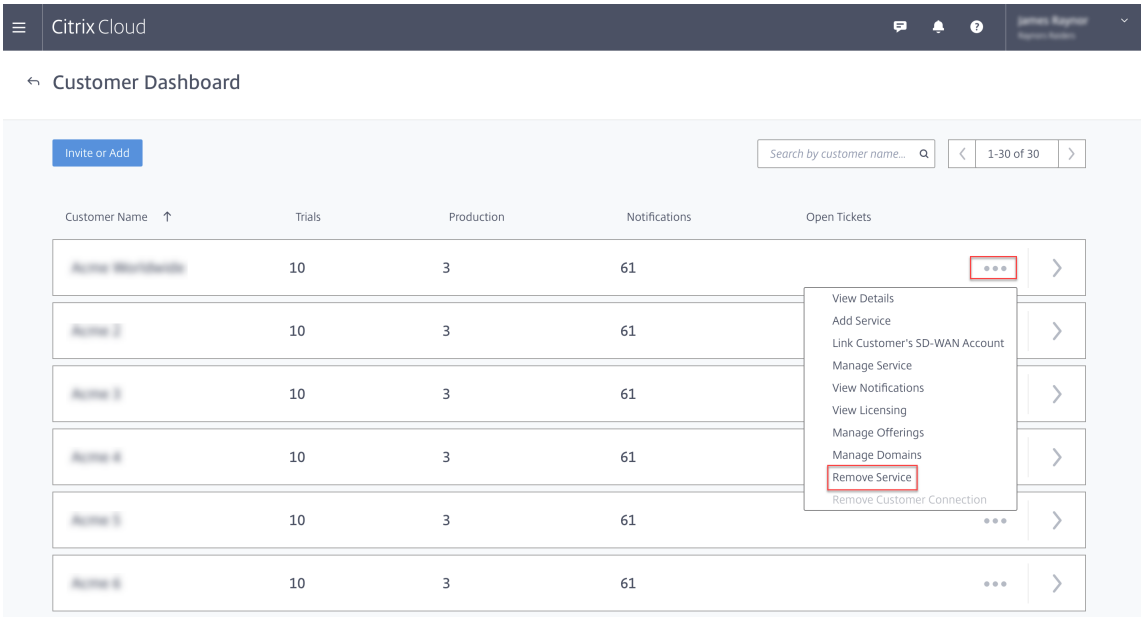
組み込みの役割を使用してアクセス権を構成する場合、組み込みの役割によって、管理者が ［管理］および ［監視］画面を表示できるかどうかを制御します。［監視］タブが表示されない役割と顧客スコープのペアのみを選択した場合、その管理者には、選択された顧客の ［監視］タブは表示されません。たとえば、管理者に読み取り専用管理者、**customerABC** アクセス権のみを付与する場合、その管理者には顧客 ABC の ［監視］タブは表示されません。これは、読み取り専用管理者は監視画面にアクセスできないためです。

サービスの削除

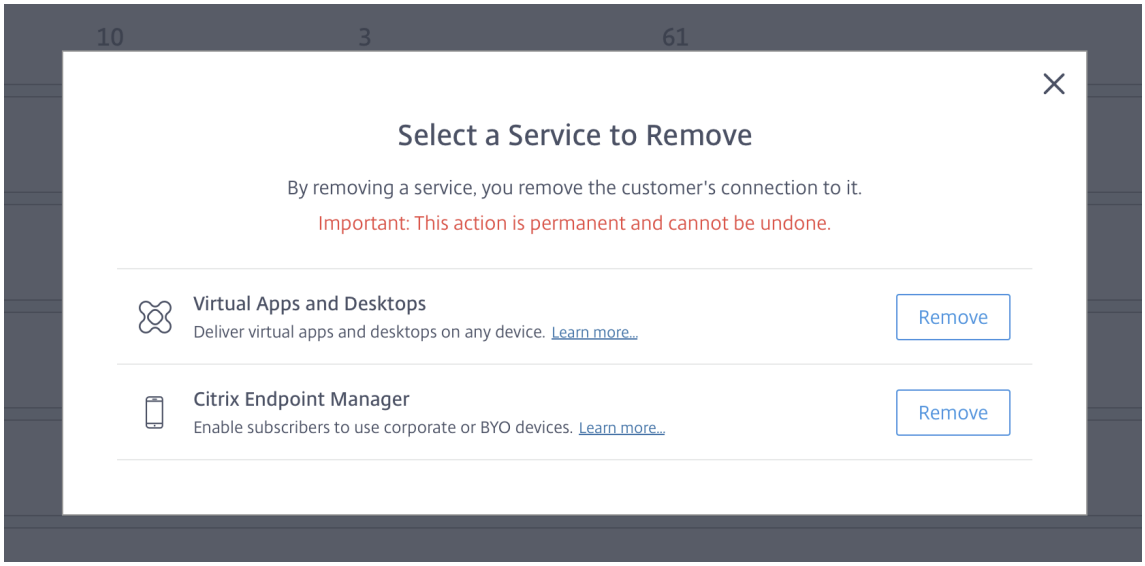
前提条件

- 顧客スコープが Citrix DaaS オブジェクトにリンクされていないことを確認してください。リンクされている場合、サービスを削除することはできません。スコープのリンクを解除するには、［**Citrix Studio**］**>**［管理者］**>**［スコープ］に移動して、スコープを編集します。
- 顧客スコープを把握して管理するには、「スコープの作成と管理」を参照してください。

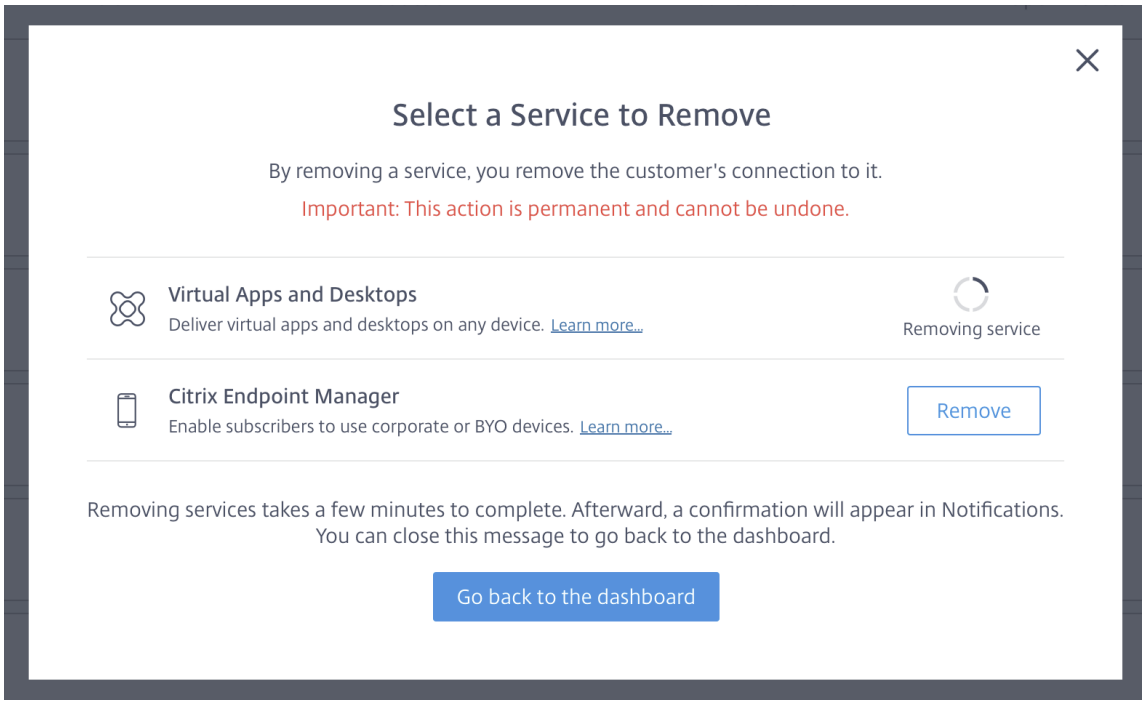
1. Citrix Service Provider の資格情報で Citrix Cloud にサインインします。
2. 顧客ダッシュボードで、サービスを削除する顧客の省略記号メニュー（…）をクリックし、［サービスの削除］を選択します。



［削除するサービス］ページが表示されます。



3. [削除] をクリックしてサービスを削除します。



Citrix Gateway サービス

November 14, 2022

Citrix Gateway は、Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）アプリケーションへの安全なアクセスをユーザーに提供します。

Citrix Gateway Service により、DMZ（Demilitarized Zone：非武装地帯）への Citrix Gateway の展開やファイアウォールの再構成の必要なく、これらのアプリケーションに安全にリモートでアクセスできます。Citrix Gateway の使用にかかるインフラストラクチャの全オーバーヘッドは、Citrix Cloud に移動します。

Citrix Gateway サービスについて詳しくは、製品ドキュメントを参照してください。このコンテンツには、Citrix Gateway サービスを有効にする方法と使用しているバージョンの既知の問題が含まれます。

Citrix ADC は、アプリケーション固有のトラフィックを分析し、Web アプリケーションのレイヤー 4～レイヤー 7（L4～L7）ネットワークトラフィックを、インテリジェントに分散、最適化、および保護するアプリケーションデリバリーコントローラーです。Citrix ADC VPX 仮想アプライアンスは、さまざまな仮想化およびクラウドプラットフォーム上でホストできます。詳しくは、「Citrix ADC VPX インスタンスを展開する」を参照してください。

SDK および API

December 19, 2023

Citrix DaaS Remote PowerShell SDK

Remote PowerShell SDK では、繰り返し行う複雑なタスクを自動化できます。この SDK のメカニズムにより、[管理] ユーザーインターフェイスを使用することなく、Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）環境を設定し管理できるようになります。

- コマンドレットの詳細については、「Citrix DaaS SDK」で説明しています。
- サポートされているモジュールは、「サポートと制限事項」に一覧で示されています。このセクションには、この SDK で無効なコマンドレットの一覧も示されています。
- Remote PowerShell SDK は、Citrix Web サイトからダウンロードできます。

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

この SDK と顧客管理の環境の SDK の違い

顧客管理者がインストールと管理を担当する Citrix Virtual Apps and Desktops 環境では、それらの管理者が、共通ドメイン構造内に VDA と Delivery Controller を含むサイトでコマンドレットとスクリプトを実行します。一方、Citrix DaaS では、VDA と Delivery Controller はそれぞれリソースの場所とコントロールプレーンに分けられています。このように分割されているため、元の Citrix Virtual Apps and Desktops PowerShell SDK は、Citrix DaaS 環境では使用できません。SDK が、リソースの場所とコントロールプレーンのセキュリティによる境界を越えられないからです。

この解決策となるのが、Citrix DaaS Remote PowerShell SDK です。リソースの場所で実行すると、Remote PowerShell SDK はローカルであるかのようにコントロールプレーンにアクセスします。これにより、単一の Citrix

Virtual Apps and Desktops サイトと同じ機能が提供されます。存在する通信レイヤーは最下層の不可視のものだけであり、単一のローカルサイトまたはクラウド環境で機能するように拡張されています。コマンドレットは同一であり、既存のスクリプトのほとんどは変更されていません。

`Get-XdAuthentication`コマンドレットでは、セキュリティで保護されたリソースの場所とコントロールプレーンとの境界を越えるための認証を行います。デフォルトでは、`Get-XdAuthentication`では CAS 資格情報の入力が求められます。また、このコマンドレットは PowerShell セッションごとに 1 回実行する必要があります。または、Citrix Cloud コンソールで API アクセス用セキュアクライアントを作成し、このクライアントを使用する認証プロファイルを定義することもできます。どちらの場合でも、セキュリティ情報は以降の PowerShell SDK 呼び出し用に保持されます。このコマンドレットが明示的に実行されない場合には、最初の PowerShell SDK コマンドレットによって呼び出されます。

前提条件

Citrix DaaS Remote PowerShell SDK を使用するには、次の URL をホワイトリストに登録します:

商用

- `https://accounts.cloud.com`
- `https://[service].citrixworkspacesapi.net/[customerid]`
- `https://[customerid].xendesktop.net:443`

日本

- `https://accounts.citrixcloud.jp`
- `https://[service].citrixworkspacesapi.jp/[customerid]`
- `https://[customerid].apps.citrixworkspacesapi.jp:443`

自治体

- `https://accounts.cloud.us`
- `https://[service].citrixworkspacesapi.us/[customerid]`
- `https://[customerid].xendesktop.us:443`

Remote PowerShell SDK をインストールして使用する

以下の要件および考慮事項があります:

> 注:
>
> Remote PowerShell SDK を Citrix Cloud Connector マシンにインストールしないでください。同じリソースの場所内のドメイン参加済みマシンにはインストールできます。

> Citrix は、Cloud Connector でのこの SDK のコマンドレットの実行をサポートしていません。これは、SDK の操作に Cloud Connector は関係しないためです。
>
> (Citrix DaaS 展開に加えて) Citrix Virtual Apps and Desktops 展開もある場合は、オンプレミスの Delivery Controller マシンに Remote PowerShell SDK をインストールしないでください。

- **Microsoft Edge WebView2** をインストールします。
- マシン上で PowerShell 3.0、4.0、5.0 のいずれかが使用できる必要があります。
- .NET Framework 4.8（またはそれ以降のサポートされているバージョン）がまだインストールされていない場合、SDK インストーラーによりダウンロードおよびインストールされます。
- マシンに Citrix Virtual Apps and Desktops SDK が既にインストールされている場合、(Windows プログラムや機能から）この SDK を削除してから Remote PowerShell SDK をインストールしてください。
- 自動化された環境の場合は、`-quiet`パラメーターを使用して、ユーザーの入力なしで SDK をインストールします。

Remote PowerShell SDK をインストールするには:

1. ダウンロードページから、Virtual Apps and Desktops Remote PowerShell SDK をダウンロードします。
2. SDK をインストールして実行します。

インストールログは%TEMP%\CitrixLogs\CitrixPoshSdkに作成されます。このログは、インストールの問題の解決に役立ちます。

この SDK は、そのリソースの場所内にあるドメイン参加済みコンピューターで実行します:

- PowerShell コマンドプロンプトを開きます。管理者として実行する必要はありません。
- (モジュールではなく）スナップインを使用する場合は、`Add-PSSnapin`（または`asnp`）コマンドレットを使用してスナップインを追加します。
- 認証を明示的に行うには、`Get-XdAuthentication`コマンドレットを使用します。また、最初の Remote PowerShell SDK コマンドを実行すると、`Get-XdAuthentication`と同じ認証が求められます。プロキシを使用している場合、`Get-XdAuthentication`コマンドレットを使用できるようにするには、プロキシに認証する必要があります。詳しくは、「Remote PowerShell SDK をプロキシで使用する」を参照してください。
- 認証プロンプトを省略するには、`Set-XdCredentials`コマンドレットを使用して、Citrix Cloud コンソールで作成したセキュアクライアントを使用するデフォルトの認証プロファイルを作成します。
- 引き続き PowerShell SDK コマンドレットまたは PowerShell SDK 自動スクリプトを実行します。例を参照してください。

Remote PowerShell SDK をアンインストールするには、プログラムの削除または変更を行う Windows 機能で、[**Citrix Virtual Apps and Desktops Remote PowerShell SDK**] を選択します。右クリックして [アンインストール] を選択します。ダイアログの手順を実行します。

Remote PowerShell SDK をプロキシで使用する　プロキシを使用している場合、`Get-xdAuthentication` コマンドレットが行う HTTP 要求がプロキシによってブロックされるため、このコマンドレットを使用できない場合

があります。

プロキシへの認証には 2 つの方法があります。ProxyUseDefaultパラメーター、またはProxyUsernameとProxyPasswordパラメーターのいずれかを使用できます。

- ProxyUseDefaultパラメーターは、デフォルトのプロキシ資格情報を使用したプロキシへの認証を有効にします。例:

```
1  Get-XdAuthentication -ProxyUseDefault
2  <!--NeedCopy-->
```

- ProxyUsernameおよびProxyPasswordパラメーターは、PowerShell セッション内でプロキシへの認証を有効にします。例:

```
1  $secureString = ConvertTo-SecureString -String "password" -
       AsPlainText -Force
2
3  Get-XdAuthentication -ProxyUsername user1 -ProxyPassword
       $secureString
4  <!--NeedCopy-->
```

アクティビティの例

一般的なアクティビティとしては、マシンカタログ、アプリケーション、ユーザーの設定が挙げられます。サンプルスクリプトを以下に示します。

```
1      $users = "xd.local\Domain Users"
2
3      $TSVDACatalogName = "TSVDA"
4
5      $TSVDADGName = "TSVDA"
6
7      $TSVDAMachineName = "xd\ds-tsvda2"
8
9      #Create TSVDA Catalog
10
11     $brokerUsers = New-BrokerUser -Name $users
12
13     $catalog = New-BrokerCatalog -Name $TSVDACatalogName -
           AllocationType "Random" -Description $TSVDACatalogName -
           PersistUserChanges "OnLocal" -ProvisioningType "Manual" -
           SessionSupport "MultiSession" -MachinesArePhysical $true
14
15     #Add TSVDA Machine to Catalog
16
17     $BrokeredMachine = New-BrokerMachine -MachineName $TSVDAMachineName
           -CatalogUid $catalog.uid
18
19     #Create new desktops & applications delivery group
20
```



```
21      $dg = New-BrokerDesktopGroup -Name $TSVDADGName -PublishedName
            $TSVDADGName -DesktopKind "Shared" -SessionSupport "MultiSession
            " -DeliveryType DesktopsAndApps -Description $TSVDADGName
22
23      #Create notepad application
24
25      New-BrokerApplication -ApplicationType HostedOnDesktop -Name "
            Notepad" -CommandLineExecutable "notepad.exe" -DesktopGroup $dg
26
27      #Assign users to desktops and applications
28
29      New-BrokerEntitlementPolicyRule -Name $TSVDADGName -DesktopGroupUid
             $dg.Uid -IncludedUsers $brokerUsers -description $TSVDADGName
30
31      New-BrokerAccessPolicyRule -Name $TSVDADGName -
            IncludedUserFilterEnabled $true -IncludedUsers $brokerUsers -
            DesktopGroupUid $dg.Uid -AllowedProtocols @("HDX","RDP")
32
33      New-BrokerAppEntitlementPolicyRule -Name $TSVDADGName -
            DesktopGroupUid $dg.Uid -IncludedUsers $brokerUsers -description
             $TSVDADGName
34
35      #Add machine to delivery group
36
37      Add-BrokerMachine -MachineName $TSVDAMachineName -DesktopGroup $dg
38  <!--NeedCopy-->
```

サポートと制限事項

Remote PowerShell SDK では、次のオペレーティングシステムがサポートされています:

- Windows 11
- Windows 10
- Windows 10 IoT Enterprise LTSC x32 2019
- Windows 10 IoT Enterprise LTSC x64 2019
- Windows 10 IoT Enterprise 21h1 x64
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

このリリースでサポートされている Citrix Virtual Apps and Desktops PowerShell モジュールは次のとおりです:

- ブローカー
- Active Directory（AD）ID
- マシンの作成
- 構成

- 構成ログ
- ホスト
- 委任管理
- 分析

コマンドレットについて詳しくは、「Citrix Virtual Apps and Desktops SDK」を参照してください。

認証のあと、リモートアクセスは 24 時間にわたり現在の PowerShell セッションで有効なままになります。この期限後は、資格情報の入力が必要になります。

Remote PowerShell SDK は、リソースの場所内にあるコンピューターで実行する必要があります。

Citrix Cloud のコントロールプレーンの整合性とセキュリティを維持するため、リモート操作では以下のコマンドレットは無効化されています。

Citrix.ADIdentity.Admin.V2:

- Copy-AcctIdentityPool
- Get-AcctDBConnection
- Get-AcctDBSchema
- Get-AcctDBVersionChangeScript
- Get-AcctInstalledDBVersion
- Remove-AcctServiceMetadata
- Reset-AcctServiceGroupMembership
- Set-AcctDBConnection
- Set-AcctServiceMetadata
- Set-AcctADAccountUserCert
- Test-AcctDBConnection

Citrix.Analytics.Admin.V1:

- Get-AnalyticsDBConnection
- Get-AnalyticsDBSchema
- Get-AnalyticsDBVersionChangeScript
- Get-AnalyticsInstalledDBVersion
- Import-AnalyticsDataDefinition
- Remove-AnalyticsServiceMetadata
- Reset-AnalyticsServiceGroupMembership
- Set-AnalyticsDBConnection
- Set-AnalyticsServiceMetadata
- Set-AnalyticsSite
- Set-AnalyticsDBConnection

Citrix.DelegatedAdmin.Admin.V1:

- Add-AdminRight
- Get-AdminDBConnection
- Get-AdminDBSchema
- Get-AdminDBVersionChangeScript
- Get-AdminInstalledDBVersion
- Import-AdminRoleConfiguration
- New-AdminAdministrator
- Remove-AdminAdministrator
- Remove-AdminAdministratorMetadata
- Remove-AdminRight
- Remove-AdminServiceMetadata
- Reset-AdminServiceGroupMembership
- Set-AdminAdministrator
- Set-AdminAdministratorMetadata
- Set-AdminDBConnection
- Set-AdminServiceMetadata
- Test-AdminDBConnection

Citrix.Broker.Admin.V2:

- Get-BrokerDBConnection
- Get-BrokerDBSchema
- Get-BrokerDBVersionChangeScript
- Get-BrokerInstalledDBVersion
- Get-BrokerLease
- Get-BrokerController
- New-BrokerMachineConfiguration
- Remove-BrokerControllerMetadata
- Remove-BrokerLease
- Remove-BrokerLeaseMetadata
- Remove-BrokerMachineConfigurationMetadata
- Remove-BrokerMachineConfiguration
- Remove-BrokerSiteMetadata
- Remove-BrokerUserFromApplication
- Reset-BrokerLicensingConnection
- Reset-BrokerServiceGroupMembership
- Set-BrokerControllerMetadata
- Set-BrokerDBConnection
- Set-BrokerLeaseMetadata
- Set-BrokerMachineConfiguration
- Set-BrokerMachineConfigurationMetadata

- Set-BrokerSiteMetadata
- Test-BrokerDBConnection
- Test-BrokerLicenseServer
- Update-BrokerBrokerLocalLeaseCache

Citrix.Configuration.Admin.V2:

- Export-ConfigFeatureTable
- Get-ConfigDBConnection
- Get-ConfigDBSchema
- Get-ConfigDBVersionChangeScript
- Get-ConfigInstalledDBVersion
- Get-ConfigServiceGroup
- Import-ConfigFeatureTable
- Register-ConfigServiceInstance
- Remove-ConfigRegisteredServiceInstanceMetadata
- Remove-ConfigServiceGroup
- Remove-ConfigServiceGroupMetadata
- Remove-ConfigServiceMetadata
- Remove-ConfigSiteMetadata
- Reset-ConfigServiceGroupMembership
- Set-ConfigDBConnection
- Set-ConfigRegisteredServiceInstance
- Set-ConfigRegisteredServiceInstanceMetadata
- Set-ConfigServiceGroupMetadata
- Set-ConfigServiceMetadata
- Set-ConfigSite
- Set-ConfigSiteMetadata
- Test-ConfigDBConnection
- Unregister-ConfigRegisteredServiceInstance

Citrix.Host.Admin.V2:

- Get-HypDBConnection
- Get-HypDBSchema
- Get-HypDBVersionChangeScript
- Get-HypInstalledDBVersion
- Remove-HypServiceMetadata
- Reset-HypServiceGroupMembership
- Set-HypDBConnection
- Set-HypServiceMetadata
- Test-HypDBConnection

Citrix.ConfigurationLogging.Admin.V1:

- Get-LogDBConnection
- Get-LogDBSchema
- Get-LogDBVersionChangeScript
- Get-LogInstalledDBVersion
- Remove-LogOperation
- Remove-LogServiceMetadata
- Remove-LogSiteMetadata
- Reset-LogDataStore
- Reset-LogServiceGroupMembership
- Set-LogDBConnection
- Set-LogServiceMetadata
- Set-LogSite
- Set-LogSiteMetadata
- Test-LogDBConnection

Citrix.MachineCreation.Admin.V2:

- Get-ProvDBConnection
- Get-ProvDBSchema
- Get-ProvDBVersionChangeScript
- Get-ProvInstalledDBVersion
- Get-ProvServiceConfigurationData
- Remove-ProvServiceConfigurationData
- Remove-ProvServiceMetadata
- Reset-ProvServiceGroupMembership
- Set-ProvDBConnection
- Set-ProvServiceMetadata
- Test-ProvDBConnection

Citrix.EnvTest.Admin.V1:

- Get-EnvTestDBConnection
- Get-EnvTestDBSchema
- Get-EnvTestDBVersionChangeScript
- Get-EnvTestInstalledDBVersion
- Remove-EnvTestServiceMetadata
- Reset-EnvTestServiceGroupMembership
- Set-EnvTestDBConnection
- Set-EnvTestServiceMetadata
- Test-EnvTestDBConnection

Citrix.Monitor.Admin.V1:

- Get-MonitorConfiguration
- Get-MonitorDBConnection
- Get-MonitorDBSchema
- Get-MonitorDBVersionChangeScript
- Get-MonitorDataStore
- Get-MonitorDataStore
- Get-MonitorInstalledDBVersion
- Remove-MonitorServiceMetadata
- Reset-MonitorDataStore
- Reset-MonitorServiceGroupMembership
- Set-MonitorConfiguration
- Set-MonitorDBConnection
- Set-MonitorServiceMetadata
- Test-MonitorDBConnection

Citrix.Storefront.Admin.V1:

- Build-SfCluster
- Get-SfClusters
- Get-SfDBConnection
- Get-SfDBSchema
- Get-SfDBVersionChangeScript
- Get-SfInstalledDBVersion

App-V パッケージおよびサーバー用の **Citrix DaaS** 検出モジュール

Citrix DaaS では、次のいずれかの方法を使用して、App-V パッケージに含まれるアプリケーションをエンドポイントに配信できます:

- シングル管理方式（ネットワーク共有からパッケージにアクセス）
- デュアル管理方式（Microsoft App-V 管理サーバーからパッケージにアクセス）

Citrix DaaS を使用して App-V パッケージおよび Microsoft App-V 管理サーバーと公開サーバーをアプリケーションライブラリに登録するプロセスは、オンプレミス展開を使用したパッケージ登録とは多少異なります。ただし、アプリケーションをユーザーに割り当て、それらをユーザーのエンドポイントで起動するプロセスはどちらでも同じです。

Citrix Cloud の Citrix DaaS 管理コンソールでは、リソースの場所にあるファイルを表示できません。また、インフラストラクチャ内の App-V パッケージまたは Microsoft App-V サーバーを直接検出することはできません。検出モジュールは、オンプレミスのインフラストラクチャ内の App-V パッケージ情報を検出し、そのパッケージ情報を

Citrix DaaS にアップロードする機能を提供します。パッケージ情報には、App-V パッケージ、Microsoft App-V サーバー、およびパッケージ内のアプリが含まれます。

この検出モジュールは、Virtual Apps and Desktops Remote PowerShell SDK を使用します。ネットワーク共有または Microsoft App-V 管理サーバーから、パッケージ情報を検出できます。検出モジュールは、リソースの場所にあるマシンで使用します。

検出モジュールを使用するための前提条件:

- マシン上で PowerShell 3.0 以降が使用できる必要があります。
- Citrix Virtual Apps and Desktops Remote PowerShell SDK がマシンにインストールされている必要があります。
- App-V パッケージが置かれたネットワーク共有へのアクセス権を有している必要があります。
- Citrix Cloud Connector がインストールされ、Microsoft App-V 管理サーバーがホストされているサーバーへのアクセス権を有している必要があります。

App-V パッケージを **Citrix Cloud** のアプリケーションライブラリに追加する

以下の手順は、ネットワーク共有から App-V パッケージを追加する場合（シングル管理方式）、および Microsoft App-V 管理サーバーからすべての公開 App-V パッケージを追加する場合（デュアル管理方式）に有効です。デュアル管理方式を使用する場合は、シングル管理方式を使用する場合と同様に、追加する App-V パッケージを管理する必要があります。

1. Citrix DaaS ダウンロードページ（https://www.citrix.com/downloads/citrix-cloud/product-software/xenapp-and-xendesktop-service.html）から検出モジュールをダウンロードします。使いやすいフォルダーに zip ファイル`Citrix.Cloud.AppLibrary.Admin.v1.psm1`を展開します。

   > 注:
   >
   > このファイルは、Citrix Virtual Apps and Desktops ISO の`Support\Tools\Scripts`でも提供されています。ローカルにコピーすることも、CD ドライブから直接参照することもできます。

2. Citrix Virtual Apps and Desktops Remote PowerShell SDK がマシンにインストールされているかを確認します。
3. 検出モジュールを含むフォルダーに移動します。PowerShell ウィンドウで、検出モジュールを含むフォルダーのフルパスを入力し、**Enter** キーを押します。
4. コマンド`Import-Module .\Citrix.Cloud.AppLibrary.Admin.v1.psm1`を使用して検出モジュールをインポートします。
5. 次のいずれかの方法を使用して、App-V パッケージを Citrix Cloud のアプリケーションライブラリに追加します。

   - ネットワーク共有から App-V パッケージを追加するには、次の PowerShell コマンドレットを実行します: `Import-AppVPackageToCloud`

例: `Import-AppVPackageToCloud -PackagePath \\AppVSrv\share\Notepad++.appv`

コマンドレットヘルプについては、`Get-Help Import-AppVPackageToCloud`と入力してください。

- Microsoft App-V 管理サーバーから App-V パッケージを追加するには、次の PowerShell コマンドレットを実行します: `Import-AppVPackagesFromManagementServerToCloud`

  例:`Import-AppVPackagesFromManagementServerToCloud -ManagementSrvFQDN AppVMngSrv.domain.local`

  コマンドレットヘルプについては,`Get-Help Import-AppVPackagesFromManagementServerTo`と入力してください。

  このコマンドは、公開されたすべての App-V パッケージを Microsoft App-V 管理サーバーから Citrix Cloud にインポートします。

  App-V パッケージを Citrix Cloud に追加したら、シングル管理方式と同様に管理する必要があります。

6. Citrix Cloud にサインインします。ターゲット顧客を選択します。スクリプトが正常に実行されると、App-V パッケージが Citrix Cloud のアプリケーションライブラリに追加されます。

High-level PowerShell 関数

このモジュールには、独自の PowerShell スクリプトから呼び出すことができる次の高レベル関数が含まれています:

- `Import-AppVPackageToCloud -PackagePath <Full UNC path to App-V package>`

  1 つの App-V パッケージからアプリケーションを公開するために必要なすべての情報を検出し、Citrix DaaS にアップロードします。

- `Import-AppVPackagesFromManagementServerToCloud -ManagementSrvFQDN <FQDN of a Microsoft App-V Management Server>`

  管理サーバーによって公開されたパッケージの UNC パスを検出し、その **Import-AppVPackageToCloud** を順番に呼び出します。

  この方法で検出されたパッケージは、シングル管理方式を使用して Citrix DaaS に読み込まれます。Citrix DaaS は、デュアル管理方式を使用してパッケージを配信することはできません。

- `Import-AppVDualAdminToCloud -ManagementSrvUrl <URL of a Microsoft App-V Management Server> -PublishingServerUrl <URL of a Microsoft App-V Publishing Server>`

Microsoft App-V 管理サーバーと公開サーバーを検出し、コンテンツをアプリケーションライブラリにインポートします。このコマンドレットは、Microsoft App-V 管理サーバーおよび関連情報を使用して管理されるすべてのパッケージをインポートします。サーバーは、PowerShell を使用して追加および削除できます。

このコマンドレットは、デュアル管理モードで App-V パッケージを追加します。Microsoft App-V 管理サーバー上で公開され、Active Directory グループが追加されている App-V パッケージのみがインポートされます。Microsoft App-V 管理サーバーに変更を加えた場合は、このコマンドレットを再実行して、アプリケーションライブラリを Microsoft App-V 管理サーバーと同期させます。

- `Remove-AppVServerFromCloud -ManagementSrvUrl <URL of a Microsoft App-V Management Server> -PublishingServerUrl <URL of a Microsoft App-V Publishing Server>`

  アプリケーションライブラリに追加された Microsoft App-V 管理サーバーと公開サーバーを削除します。

  このコマンドレットは、指定された Microsoft App-V 管理サーバーと公開サーバー、関連付けられているすべての App-V パッケージを削除します。

そのリソースの場所内にあるドメイン参加済みコンピューターで、App-V パッケージおよびサーバー用の検出モジュールを実行します。「Remote PowerShell SDK をインストールして使用する」のガイダンスに従って開始します。引き続き PowerShell コマンドレットまたはスクリプトを実行します。以下の例を参照してください。

アクティビティの例

Citrix DaaS App-V パッケージ検出モジュールをインポートします。

```
import-module "D:\Support\Tools\Scripts\Citrix.Cloud.AppLibrary.Admin.v1.psm1"
<!--NeedCopy-->
```

App-V パッケージのストアディレクトリをループし、各パッケージをアップロードします。

```
Get-ChildItem -Path "\FileServer.domain.net\App-V Packages" -Filter *.appv |
Foreach-Object{

    Import-AppVPackageToCloud -PackagePath $_.FullName
 }

<!--NeedCopy-->
```

Microsoft App-V 管理サーバーに登録されているパッケージを検出してアップロードします。

```
Import-AppVPackagesFromManagementServerToCloud -ManagementSrvFQDN AppVManagementServer.domain.net
<!--NeedCopy-->
```


Microsoft App-V 管理サーバーと公開サーバーを検出し、構成をアプリケーションライブラリに追加します。これにより、Microsoft App-V 管理サーバーが管理するすべてのパッケージもデュアル管理モードでインポートされます。

```
Import-AppVDualAdminCloud -ManagementSrvUrl http://AppVManagementServer.domain.net  - PublishingServerUrl http://AppVManagementServer.domain.net:8001
<!--NeedCopy-->
```

モジュールに含まれている PowerShell のヘルプドキュメントを読みます。

```
Get-Help Import-AppVPackageToCloud
<!--NeedCopy-->
```

制限事項

- Citrix Cloud の Citrix DaaS 管理コンソールから直接、リソースの場所のインフラストラクチャ上の App-V パッケージを検出できません。Citrix Cloud について詳しくは、Citrix Cloudのドキュメントを参照してください。
- Citrix Cloud の Citrix DaaS 管理コンソールに、Microsoft App-V 管理サーバーへのライブ接続がありません。Microsoft App-V 管理サーバーのパッケージおよびその他の構成を変更すると、`Import-AppVDualAdminCloud`を再実行するまで Citrix DaaS 管理コンソールには反映されません。

Monitor Service OData API

管理者は、監視機能で表示した履歴データを、Monitor Service の API を使って照会できます。API を使用して次のことを行います:

- 計画のために履歴傾向を分析する。
- 接続やマシンの障害に対する詳細なトラブルシューティングを実行する。
- ほかのツールおよびプロセスに情報をインポートする（Microsoft Excel の PowerPivot テーブルを使って別の方法でデータを表示するなど）。
- API で提供されるデータ上にカスタムユーザーインターフェイスを構築する。

詳しくは、「Monitor Service OData API」を参照してください。Monitor Service API にアクセスするには、「Access Monitor Service data using the OData v4 endpoint in Citrix Cloud」を参照してください。

Citrix DaaS API

Citrix DaaS API は、https://developer.cloud.com/citrixworkspace/citrix-daasで入手できます。

免責事項

このソフトウェアおよびサンプルコードは「現状のまま」提供され、いかなる種類の説明、保証、条件も付与されません。これらは、自己の責任において使用、変更、配布することができます。Citrix は、商品性、特定用途に対する適合性、資格、非侵害性に関するあらゆる保証を含む、明示、黙示、書面、口頭、法定によるいかなる保証も一切付与しません。前述の一般性を制限することなく、ユーザーは、(a) このソフトウェアおよびサンプルコードにはエラー、設計上の欠陥その他の問題が含まれている可能性があり、その結果データ損失または所有物の損傷が生じる可能性があること、(b) このソフトウェアおよびサンプルコードは完全には機能しない可能性があること、(c) Citrix は、通知なしで、もしくはユーザーに対して一切責任を負わず、このソフトウェアおよびサンプルコードの現行バージョンおよび/または将来のバージョンの提供を取り止める場合があることを承認、同意します。いかなる場合でも、このソフトウェア/コードは、生命維持関連または爆発物関連の作業を含む、ただしそれに限定されない、極度に危険な作業に使用すべきではありません。Citrix、その関連会社および代理店は、直接的、特別、付随的、懲罰的、間接的なあらゆる損害を含む、このソフトウェアまたはサンプルコードの使用により生じたあらゆる損害について、そのような損害の可能性について知らされていた場合でも、契約の不履行または責任に関するその他のあらゆる見解の不履行の下では、一切の責任を負いません。ユーザーは、ユーザーによるこのコードの使用、変更、配布により生じたいかなる申し立てに対しても、Citrix を免責し、Citrix を弁護することに同意します。