Citrix Virtual Apps and Desktops Standard for Azure

Machine translated content

Disclaimer

Contents

Citrix Virtual Apps and Desktops Standard for Azure

July 16, 2021

はじめに

Citrix Virtual Apps and Desktops Standard for Azure は、Microsoft Azure から Windows アプリケーションとデスクトップを配信する最も簡単で最速の方法です。このサービスは、クラウドベースの管理、プロビジョニング、および仮想アプリやデスクトップを任意のデバイスに配信するための管理された機能を提供します。

このソリューションには次のものが含まれます。

- Citrix がホストする Azure 仮想デスクトップ、およびアプリケーションをマルチセッションマシンから配信するためのクラウドベースの管理とプロビジョニング。
- Citrix Workspace アプリを使用して、幅広いデバイスからの高品位ユーザーエクスペリエンス。
- Citrix が最新の Citrix Virtual Delivery Agent（VDA）がインストールされた Windows および Linux のシングルセッションイメージおよびマルチセッションイメージとともに、イメージの作成と管理ワークフローを簡素化します。
- Citrix Gateway サービスのグローバルプレゼンスポイントを使用して、あらゆるデバイスからのリモートアクセスを保護します。
- 高度な監視機能とヘルプデスク管理機能。
- Azure のコンピューティング、ストレージ、および仮想デスクトップを提供するためのネットワークを含む、管理対象 Azure taaS。

Citrix リモート PC アクセス機能を使用すると、ユーザーはオフィスにある既存の物理マシンをリモートで使用できます。ユーザーは、Citrix HDX を使用して社内 PC セッションを提供することで、最高のユーザーエクスペリエンスを実現できます。

他の Citrix Virtual Apps and Desktops 製品に精通している場合は、Citrix Virtual Apps and Desktops Standard for Azure により、仮想アプリケーションとデスクトップの展開が簡素化されます。Citrix は、これらのワークロードをホストするためのインフラストラクチャを管理できます。

Citrix Virtual Apps およびデスクトップ標準は、Citrix Cloud サービスです。Citrix Cloud は、Citrix Cloud サービスをホストおよび管理するプラットフォームです。Citrix Cloud の詳細情報。

コンポーネント、データフロー、およびセキュリティに関する考慮事項については、セキュリティの技術概要を参照してください。この記事では、お客様と Citrix 責任についても説明します。

Citrix Virtual Apps and Desktops Standard for Azure は、以前は Citrix Managed Desktops という名前でした。以前の名前は、しばらくの間、さまざまな場所に引き続き表示される場合があります。

ユーザーがデスクトップとアプリにアクセスする方法

ユーザー（サブスクライバーと呼ばれることもあります）は、Citrix HTML5 クライアントを使用して、ブラウザを介してデスクトップやアプリケーションに直接アクセスします。ユーザーは、管理者によって提供される Citrix Workspace URL を参照します。Citrix Workspace プラットフォームは、デジタルリソースを列挙してユーザーに配信します。ユーザーは、ワークスペースからデスクトップまたはアプリケーションを起動します。

デスクトップとアプリケーションを配信するマシンのカタログ（またはリモート PC アクセス用の物理マシンを含むカタログ）を構成すると、サービスに Workspace URL が表示されます。次に、その URL に移動してデスクトップやアプリを起動するようにユーザーに通知します。

Citrix Workspace に移動してデスクトップやアプリにアクセスする代わりに、ユーザーは Citrix Workspace アプリをデバイスにインストールできます。エンドポイントデバイスのオペレーティングシステムに適したアプリをダウンロードします。https://www.citrix.com/downloads/workspace-app/。

概念と用語

このセクションでは、管理者がこのサービスで使用するいくつかの項目と用語を紹介します。

- カタログ
- リソースの場所
- 画像
- Azure サブスクリプション
- ネットワーク接続
- ドメイン参加と非ドメイン参加

カタログ

カタログはマシンのグループです。

- サービスによってユーザーに配信されるデスクトップとアプリは、仮想マシン (VM) 上に存在します。これらの仮想マシンはカタログに作成 (プロビジョニング) されます。

  デスクトップを展開すると、カタログ内のマシンは選択したユーザーと共有されます。アプリケーションを公開すると、マルチセッションマシンは、選択したユーザーと共有されるアプリケーションをホストします。

- リモート PC アクセスの場合、カタログには既存のシングルセッション物理マシンが含まれています。一般的な展開には、オフィスにあるマシンが含まれます。これらのマシンへのユーザーアクセスを制御するには、構成済みのユーザー割り当て方法および選択したユーザーを使用します。

他の Citrix Virtual Apps and Desktops 製品に精通している場合は、このサービスのカタログは、マシンカタログとデリバリーグループの組み合わせに似ています。

詳しくは、次のトピックを参照してください:

- 公開デスクトップとアプリのカタログを作成する。

- リモート PC アクセス用のカタログを作成する。
- カタログの管理。
- ユーザーと認証。

リソースの場所

カタログのマシンは、リソースの場所にあります。リソースの場所には、2 つ以上のCloud Connectorも含まれます。

- デスクトップまたはアプリを公開すると、最初のカタログを作成するときに、Citrix によってリソースの場所と Cloud Connector が自動的に作成されます。
- リモート PC アクセスの場合、管理者はカタログを作成する前に、リソースの場所と Cloud Connector を作成します。

公開デスクトップおよびアプリケーションのカタログをさらに作成すると、Azure サブスクリプション、リージョン、およびドメインによって、Citrix が別のリソースの場所を作成するかどうかが決まります。これらの基準が既存のカタログと一致する場合、Citrix はそのリソースの場所を再利用しようとします。

詳しくは、次のトピックを参照してください:

- カタログの作成時にリソースの場所情報を指定する。
- リソースの場所の操作。

画像

公開デスクトップとアプリケーションのカタログを作成すると、マシンを作成するためのテンプレートとしてマシンイメージが（他の設定とともに）使用されます。

- このサービスは、Citrix プリペアドイメージをいくつか提供します。
  - Windows 10 Enterprise（単一セッション）
  - Windows 10 エンタープライズ仮想デスクトップ (マルチセッション)
  - オフィス 365 ProPlus と Windows 10 エンタープライズ仮想デスクトップ (マルチセッション)
  - Windows Server 2012 R2
  - Windows Server 2016
  - Windows Server 2019
  - Linux

  Citrix 用意された各イメージには、Citrix VDA とトラブルシューティングツールがインストールされています。VDA は、ユーザーのマシンとサービスを管理する Citrix Cloud インフラストラクチャとの間の通信メカニズムです。

  新しい VDA バージョンがリリースされると、使用可能な準備済みイメージが更新されます。
- Azure から独自のイメージをインポートして使用することもできます。イメージを使用してカタログを作成する前に、イメージに VDA（およびその他のソフトウェア）をインストールする必要があります。

多くの場合、「VDA」という用語は、アプリやデスクトップを配信するマシンと、そのマシンにインストールされているソフトウェアコンポーネントを指します。

詳しくは、「画像」を参照してください。

Azure サブスクリプション

デスクトップとアプリケーションを配信するためのカタログを作成し、Citrix Managed Azure サブスクリプションまたは独自の（顧客管理）Azure サブスクリプションのいずれかでイメージをビルド/インポートできます。

Citrix Virtual Apps and Desktops Standard for Azure サービスのみを注文する場合は、独自の Azure サブスクリプションをインポート（追加）して使用する必要があります。Citrix Azure 消費基金も注文すると、Citrix Managed Azure サブスクリプションを受け取ります。カタログの作成時または新しいイメージの構築時に、Citrix Managed Azure サブスクリプションまたはインポートした Azure サブスクリプションのいずれかを使用できます。

詳しくは、次のトピックを参照してください:

- 展開シナリオはこのサービスで Azure サブスクリプションを使用する方法を説明します。
- Azure サブスクリプションでは、Citrix Managed Azure とカスタマー管理 Azure サブスクリプションの違いについて説明します。この記事では、サブスクリプションを表示、追加、および削除する方法についても説明します。
- セキュリティの技術概要 では、Citrix Managed Azure およびカスタマー管理 Azure サブスクリプションとの責任の違いについて説明します。

ネットワーク接続

Citrix Managed Azure サブスクリプションを使用してカタログを作成する場合、ユーザーが公開デスクトップとアプリケーションから企業のオンプレミスネットワーク上の場所とリソースにアクセスできるかどうか、および方法を指定します。選択肢は、接続なし、Azure VNet ピアリング、および Citrix SD-WAN です。

独自の Azure サブスクリプションを使用する場合、接続を作成する必要はありません。Azure サブスクリプションをサービスにインポート (追加) するだけで済みます。

詳しくは、「ネットワーク接続」を参照してください。

ドメイン参加と非ドメイン参加

マシン（VDA）がドメインに参加しているかドメインに参加していないかによって、いくつかのサービス操作と機能が異なります。ドメインメンバーシップは、利用可能な展開シナリオにも影響します。

- ドメイン参加マシンと非ドメイン参加マシンは、ユーザーのワークスペースで使用可能なユーザー認証方法のいずれかをサポートします。

- ドメインに参加しているマシンとドメインに参加していないマシンから、デスクトップ、アプリケーション、またはその両方を公開できます。リモート PC アクセスカタログ内のマシンは、ドメインに参加している必要があります。

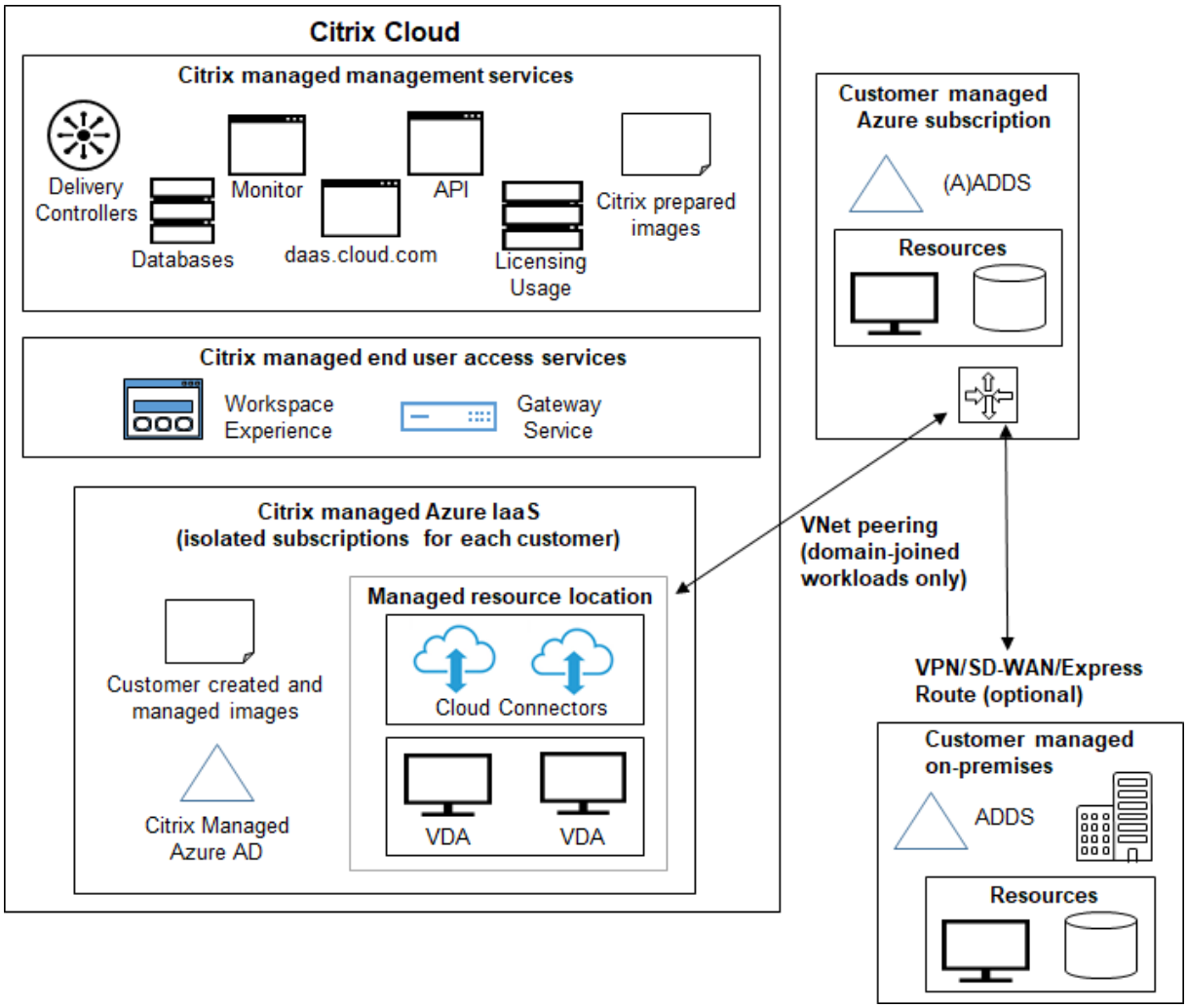
次の表に、デスクトップおよびアプリケーションを配信する際の、ドメインに参加していないマシンとドメインに参加しているマシンの違いをいくつか示します。

ドメインに参加していない	ドメインに参加しました
Active Directory はマシンには使用されません。マシンは AD ドメインに参加していません。	Active Directory はマシンに使用されます。マシンは AD ドメインに参加しています。
Active Directory グループポリシーをマシン（VDA）に適用することはできません。(カタログの作成に使用するイメージにローカル GPO を適用できます)。	VDA は、カタログ作成時に指定した AD OU のグループポリシーを継承します。
ユーザーはシングルサインオンを使用してサインインします。	ユーザーが Active Directory 以外の認証方法を使用してワークスペースにサインインすると、デスクトップまたはアプリの起動時にサインインを求められます。
オンプレミスネットワークに接続する必要はありません。	(Citrix Managed Azure サブスクリプションを使用する場合）Microsoft Azure VNet または Citrix SD-WAN を使用して、オンプレミスネットワークにアクセスするための接続が必要です。
VDA のプロビジョニングには、Citrix Managed Azure サブスクリプションを使用する必要があります。(VDA のプロビジョニングに独自の Azure サブスクリプションを使用することはできません。ただし、ユーザーは独自の Azure AD から接続できます。)	Citrix Managed Azure サブスクリプションと独自の Azure サブスクリプションを使用できます。
踏み台マシンまたは直接 RDP を使用してトラブルシューティングを行うことはできません。	踏み台マシンまたは直接 RDP を使用してトラブルシューティングできます。
Citrix Profile Management を使用できません。(推奨: 永続カタログを使用してください。)	Citrix Profile Management または FSLogix を使用できます。

展開シナリオ

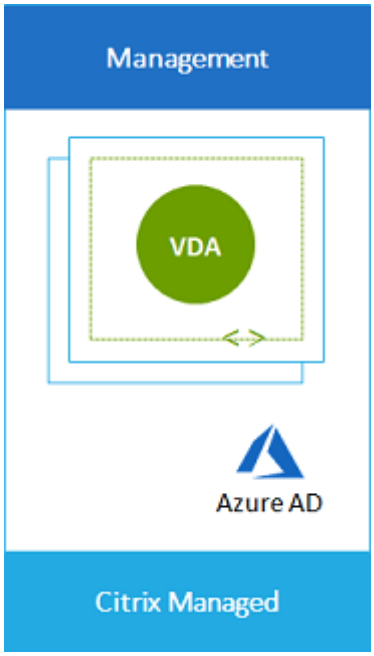
公開デスクトップとアプリケーションの展開シナリオは、Citrix Managed Azure サブスクリプションを使用しているか独自の顧客管理 Azure サブスクリプションを使用しているかによって異なります。

Citrix マネージド **Azure** サブスクリプションでのデプロイ

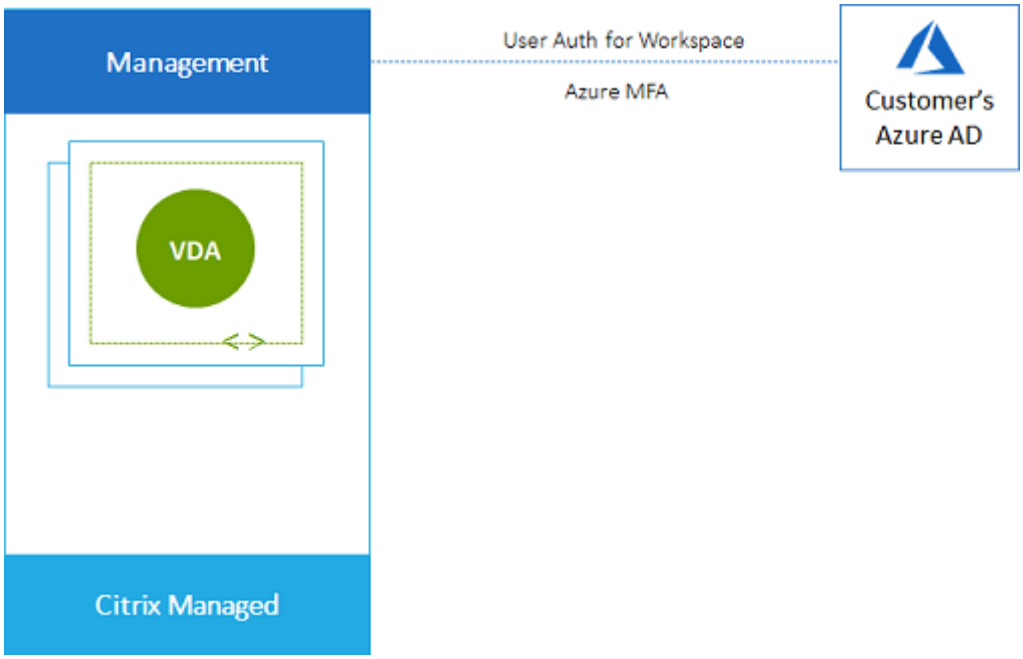


Citrix Virtual Apps およびデスクトップ標準では、接続とユーザー認証に関するいくつかの展開シナリオがサポートされています。

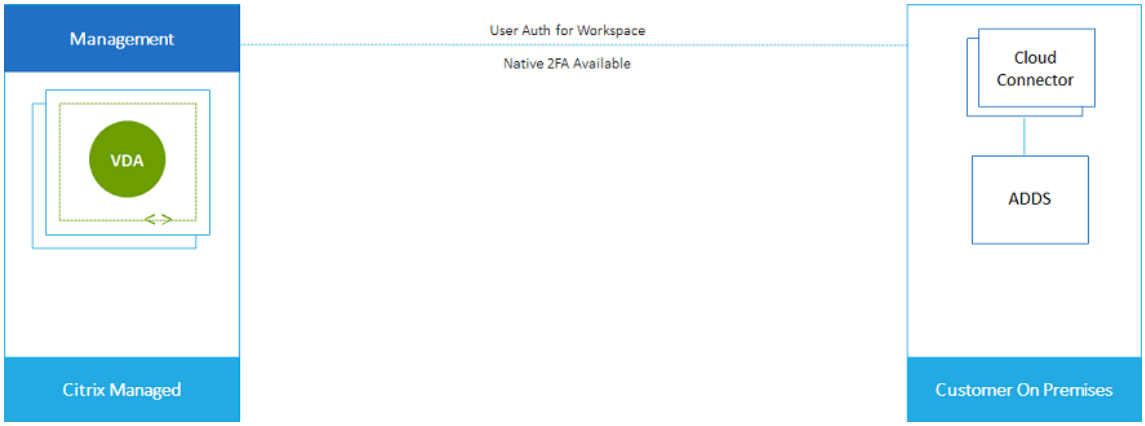
- 管理対象 **Azure AD**：これは、ドメインに参加していない VDA を使用した最も単純な展開です。コンセプトの証明におすすめです。管理対象 Azure AD（Citrix が管理する）を使用してユーザーを管理します。ユーザーは、オンプレミスネットワークのリソースにアクセスする必要はありません。



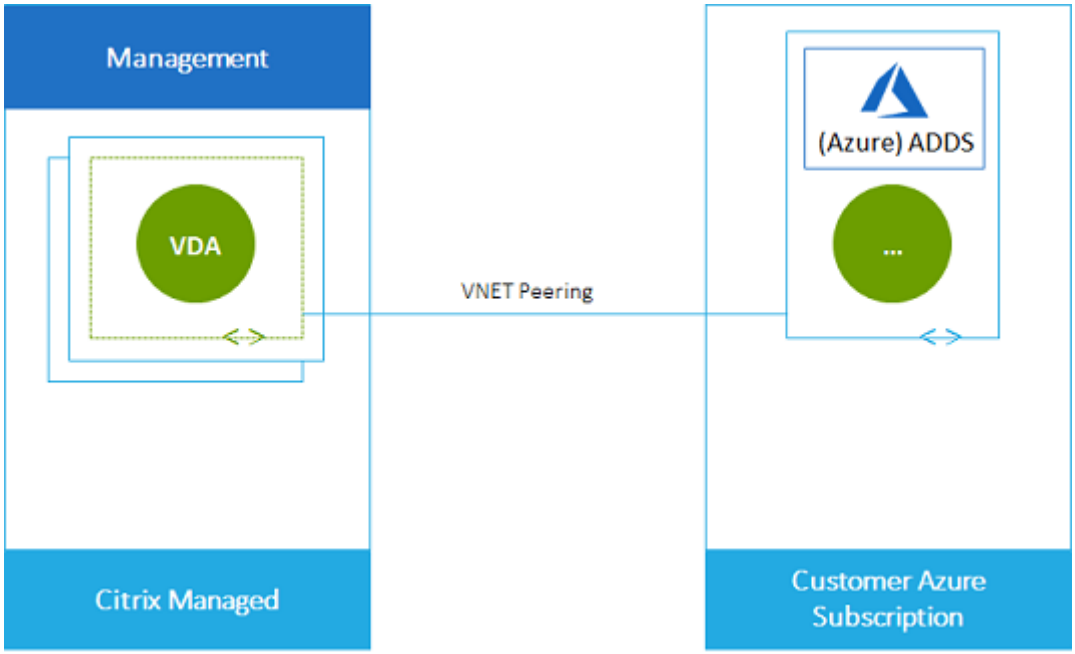
- お客様の **Azure Active Directory**：この展開には、ドメインに参加していない VDA が含まれています。エンドユーザー認証には、独自の Active Directory または Azure Active Directory (AAD) を使用します。このシナリオでは、ユーザーはオンプレミスネットワーク上のリソースにアクセスする必要はありません。



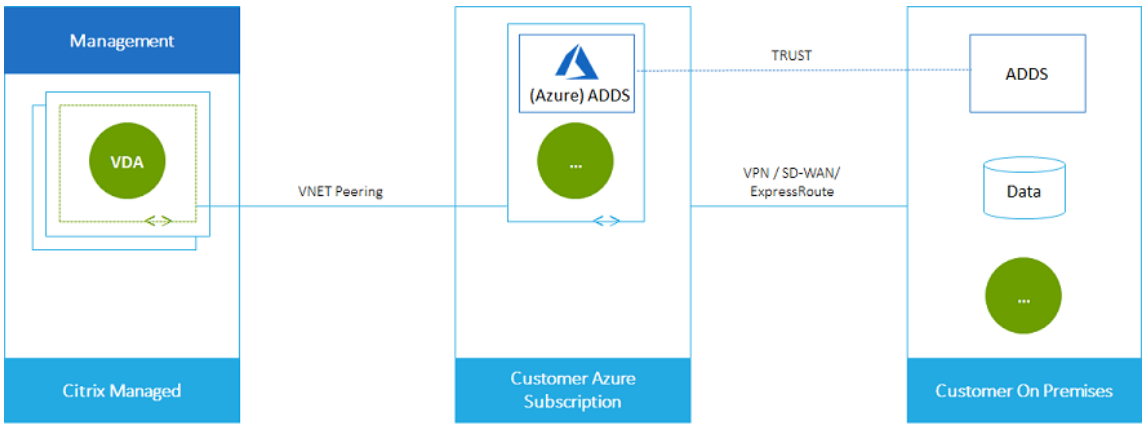
- オンプレミスアクセスを持つお客様の **Azure Active Directory**：この展開には、ドメインに参加していない VDA が含まれます。エンドユーザー認証には、独自の AD または AAD を使用します。このシナリオでは、オンプレミスネットワークに Citrix Cloud Connector をインストールすると、そのネットワーク内のリソースにアクセスできます。



- お客様の **Azure Active Directory** ドメインサービスおよび **VNet** ピアリング**:** AD または AAD が独自の Azure VNet および Azure サブスクリプションに存在する場合は、Microsoft Azure VNet ピアリング機能をネットワーク接続に使用し、エンドユーザー認証に Azure Active Directory ドメインサービス (AADDS) を使用できます。VDA はドメインに参加しています。

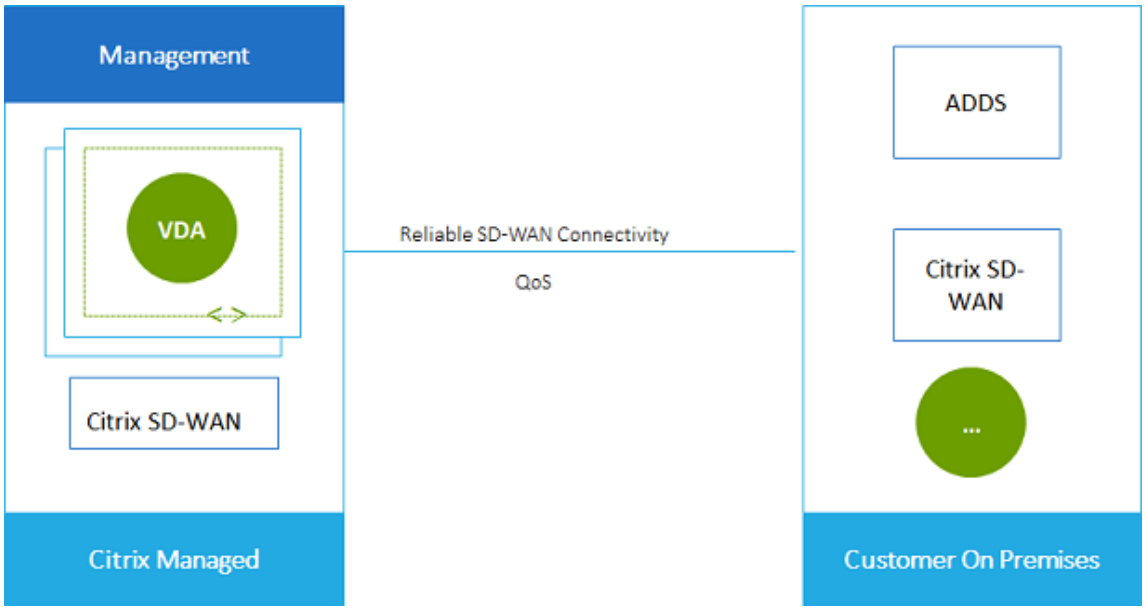


ユーザーがオンプレミスネットワークに保存されているデータにアクセスできるようにするには、Azure サブスクリプションからオンプレミスの場所への VPN 接続を使用できます。Azure VNet ピアリングはネットワーク接続に使用されます。オンプレミスの場所にある Active Directory ドメインサービスは、エンドユーザー認証に使用されます。

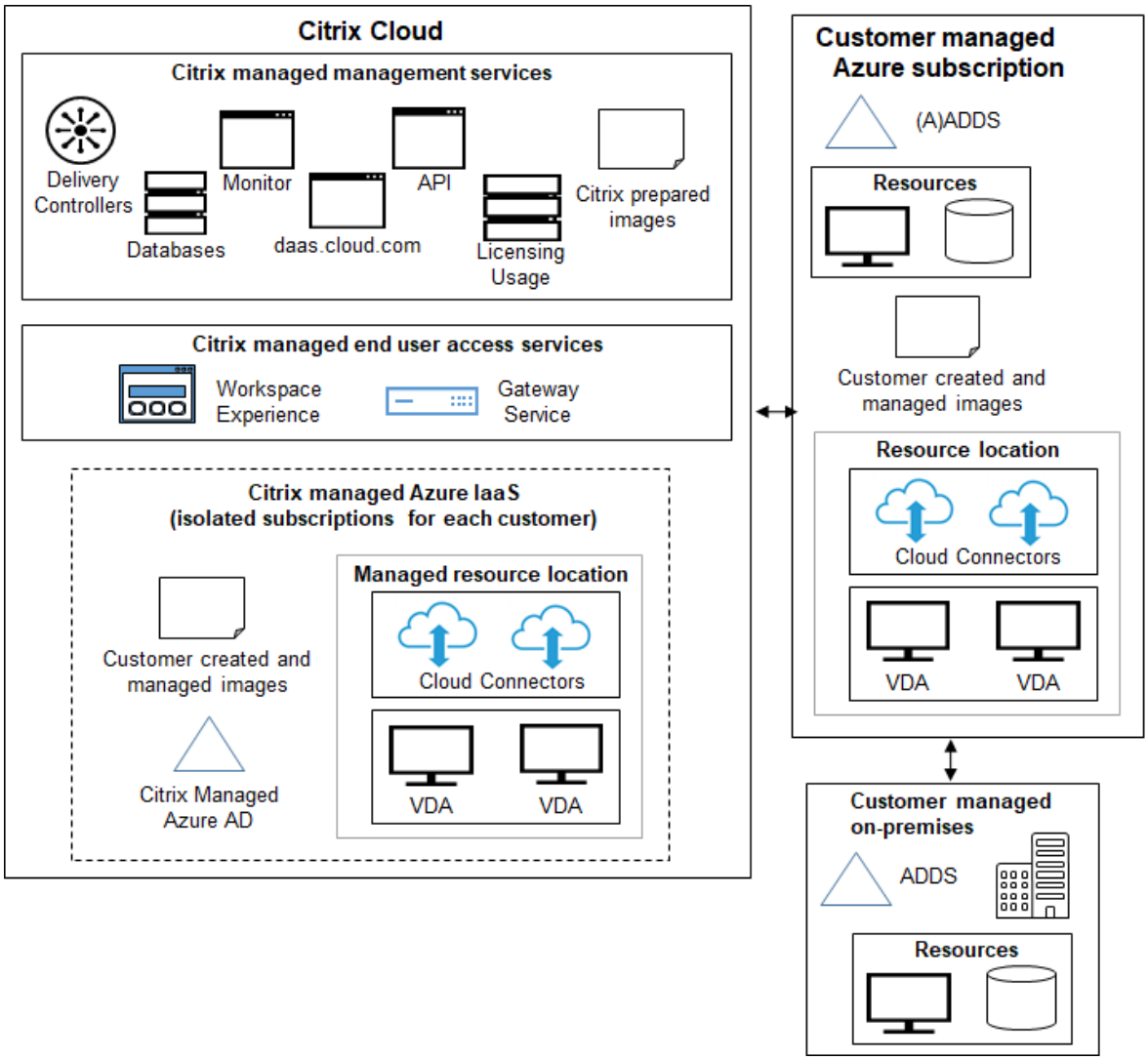


- お客様の **Active Directory** と **SD-WAN:** オンプレミスまたはクラウド SD-WAN ネットワークからファイルやその他のアイテムへのアクセスをユーザーに提供できます。

  Citrix SD-WAN は、Citrix Virtual Apps およびデスクトップ標準で必要とされるすべてのネットワーク接続を最適化します。HDX テクノロジーと連携して、Citrix SD-WAN は、ICA およびアウトオブバンド Citrix Virtual Apps およびデスクトップ標準トラフィックにサービス品質と接続の信頼性を提供します。



カスタマー管理の **Azure** サブスクリプションでのデプロイ



前の図のデプロイでは、カスタマー管理の Azure サブスクリプションを使用しています。ただし、Citrix Managed Azure サブスクリプションは、点線のアウトラインで示されているように、他のカタログおよびイメージのオプションとして残ります。

管理インターフェイス

Citrix Virtual Apps and Desktops Standard for Azure には、クイックデプロイと Web Studio 2 つの管理インターフェイスがあります。

- 合理化された Quick Deploy インターフェイスにより、カタログをすばやく作成し、ユーザーへのデスクトップとアプリケーションの配信を開始できます。(したがって、クイックデプロイという名前です。) これは、サービスを開始するときのデフォルトのインターフェイスです。このインターフェイスには、[管理] **> [**クイック展開] を選択してアクセスすることもできます。この製品ドキュメントセットの手順では、クイック展開を使用していることを前提としています。

- Web Studio インターフェイスは、展開をカスタマイズするためのより多くの機能と構成オプションを提供します。たとえば、Citrix ポリシーを作成および管理できます。クイック展開で作成したカタログは Web Studio に自動的に表示されます。そのため、クイック展開を使用してカタログを作成し、Web Studio を使用して Web Studio でのみ使用可能な機能を使用してカタログを管理できます。クイック展開から Web Studio に移動するには、[管理**] > [Web Studio**] を選択します。

Web Studio でカタログを変更した後は、Web Studio を使用してそのカタログを管理し続ける必要があります。クイック展開インターフェイスでは、そのカタログを管理できなくなります。ただし、クイック展開を使用して、そのカタログに関連付けられていないイメージやネットワーク接続に加えて、新しいカタログを作成および管理できます。)

同様に、クイック展開でカタログを作成すると、関連するデリバリーグループが Web Studio に自動的に作成されます。Web Studio から、そのデリバリーグループを編集して、ユーザー、マシン、アプリケーション、セッションに影響する設定を有効化、無効化、および変更できます。これらの設定の多くは、クイック展開からアクセスできません。ただし、Web Studio でそのデリバリーグループを変更すると、クイック展開インターフェイスで関連するカタログを管理できなくなります。

Web Studio では、Azure ホストへの接続を作成し、カタログとデリバリーグループの作成を含む、独自のカタログ作成プロセスも提供します。このプロセスは、独自の Azure サブスクリプションを使用する場合にのみサポートされます。クイック展開でカタログを作成する方がはるかに簡単です。

カタログまたはイメージの作成時に Citrix Managed Azure サブスクリプションを使用する場合は、クイックデプロイを使用する必要があります。その後、クイック展開または Web Studio でカタログを管理できます。

Web Studio は、Azure 以外のハイパーバイザーおよびクラウドサービスホストに関連するプロセスをサポートしています。これらは、Citrix Virtual Apps and Desktops Standard for Azure のお客様では使用できません。

Web Studio からクイック展開に戻るには (Web Studio で新規アイテムを作成したり、変更していないアイテムを管理するには)、[管理**] > [**クイック展開] の順にクリックします。

Web Studio を使用して構成できる内容の詳細については、以下を参照してください。

- マシンカタログの管理 （Web Studio はカタログをマシンカタログと呼びます）
- デリバリーグループの管理
- ポリシー

詳細情報

技術的な詳細については、以下を参照してください:

- Citrix Tech Zone リファレンスアーキテクチャ
- Citrix Tech Zone 技術概要

準備が整ったら、導入。

新機能

July 16, 2021

Citrix の目標は、新機能と製品アップデートが利用可能になったときに、サービスをお客様に提供することです。新しいリリースでは、より便利な機能をご利用いただけます。今すぐ更新してください。お客様管理者には、このプロセスは透過的です。

Citrix 準備イメージの更新

Citrix 提供イメージには、現在の Citrix Virtual Delivery Agent（VDA）がインストールされています。通常、新しい VDA バージョンは毎年数回リリースされ、使用可能な Citrix 準備イメージは自動的に最新の VDA で更新されます。VDA の最新バージョンの新機能および拡張機能の詳細については、以下を参照してください。

- Windows VDA
- Linux VDA

2021 年 6 月

- クイック展開と Web Studio の 2 つの管理インターフェイスサポート。

2021 年 5 月

- このサービスは、サービス継続性のプレビューをサポートします。
- Citrix 提供イメージには、Ubuntu シングルセッションとマルチセッションバージョンが含まれるようになりました。
- Citrix Managed Azure サブスクリプションを使用してCloud Connector をリソースの場所に追加する場合、Cloud Connector マシンのパフォーマンスタイプを指定できます。
- カタログを作成する場合、マシンパフォーマンスの選択肢に、選択したイメージの生成タイプ (gen1 または gen2) に一致するオプションが含まれます。カタログのマシンがその世代タイプをサポートしている場合は、別の世代タイプのイメージを使用してカタログを更新できます。

2021 年 1 月

- 消費コミットメント使用量を表示するプレビューサポートです。

2020 年 10 月

- 監視シャドウ機能を使用して、ユーザーの仮想マシンまたはセッションを表示または操作できます。

- リモート PC アクセスのプロダクションサポート。
- カタログ作成オプションをAzure 仮想デスクトップ適格ライセンスまたは Azure ハイブリッド特典を使用するように拡張しました。
- マシンでの再起動アクションが失敗した場合は、強制再起動アクションを使用できます。

2020 年 9 月

- 画像に関する詳細が再編成され、拡張されている。たとえば、準備またはインポートした画像に関するメモを追加および編集できるようになりました。指定された IP アドレスのみにアクセスを制限することもできます。
- Azure 仮想ネットワークゲートウェイを使用するAzure VNet ピア接続を作成場合、仮想ネットワークゲートウェイルート伝播を有効にすることもできます。
- 製品名が Citrix Managed Desktops から Citrix Virtual Apps and Desktops Standard for Azure に変更されました。

2020 年 8 月

- リモート PC アクセスのサポートをプレビューします。
- Citrix が準備した Windows Server 2019 イメージが利用可能になりました。

2020 年 7 月

- Cloud Connector をリソースの場所に追加するときに、カスタマー管理の Azure サブスクリプションを使用して、Cloud Connector マシンのパフォーマンスタイプと Azure リソースグループを指定できます。詳しくは、「リソースの場所の操作」を参照してください。
- カタログを作成するときに、マシン命名スキームを指定できます。「カスタム作成を使用してカタログを作成する」を参照してください。

2020 年 6 月

- CSP 環境では、SD-WAN 接続はテナントごとに作成されます。CSP 管理者が SD-WAN 接続オプションを使用できるようにするには、テナントに SD-WAN Orchestrator サービス資格が必要です。詳しくは、「顧客によるリソースのフィルタリング (マルチテナント展開)」を参照してください。
- カスタマー管理の Azure サブスクリプションを使用する場合のLinux VDAの運用サポート。
- サブスクリプションあたりの VDA上限数は 1,200 になりました。

2020 年 5 月

- Citrix Managed Azure サブスクリプションあたりの制限を超えるマシンが必要な場合に別の Citrix マネージド Azure サブスクリプションを追加することが可能です。
- DNS サーバーに関する追加情報。

2020 年 3 月

- SD-WAN 接続のプロダクションサポート。

2020 年 2 月

- Citrix ライセンスの使用状況に関する情報を表示するには、Citrix Managed Desktops サービスのライセンスとアクティブな使用状況の監視のガイダンスに従います。
- Red Hat Enterprise Linux または Ubuntu マシンを含むカタログのサポートをプレビューします。この機能は、顧客管理の Azure サブスクリプションを使用する場合にのみ有効で、Citrix Linux VDA を含むインポートされたイメージが必要です。
- これで、すべてのマルチセッションマシンに対して、垂直または水平負荷分散を構成できます。(以前は、すべてのマシンが水平負荷分散を使用していました)。このグローバル選択は、展開内のすべてのカタログに適用されます。「負荷分散」を参照してください。
- グローバル管理者でない場合、Azure サブスクリプションを追加できるようになりました。
- Citrix 準備イメージが、Office 365 ProPlus と Windows 10 エンタープライズ仮想デスクトップ（マルチセッション）で利用可能になりました。

2020 年 1 月

- VNet ピア接続でカスタムルートのサポートを追加します。
- ポートとルール情報を強化するためのセキュリティ記事が更新されました。

2019 年 11 月

- SD-WAN 接続のサポートをプレビューします。

2019 年 10 月

- サポートされるオペレーティングシステムで、次のエントリを追加しました。
  - Windows 7（最新の累積更新プログラムの VDA 7.15 のみをサポートします)。
  - Windows Server 2019。
- Windows Server 2012 R2 Citrix 準備イメージ が利用可能になりました。
- リソースの場所設定情報を追加しました。詳しくは、「リソースの場所の操作」と「カタログ作成時のリソースの場所設定」を参照してください。

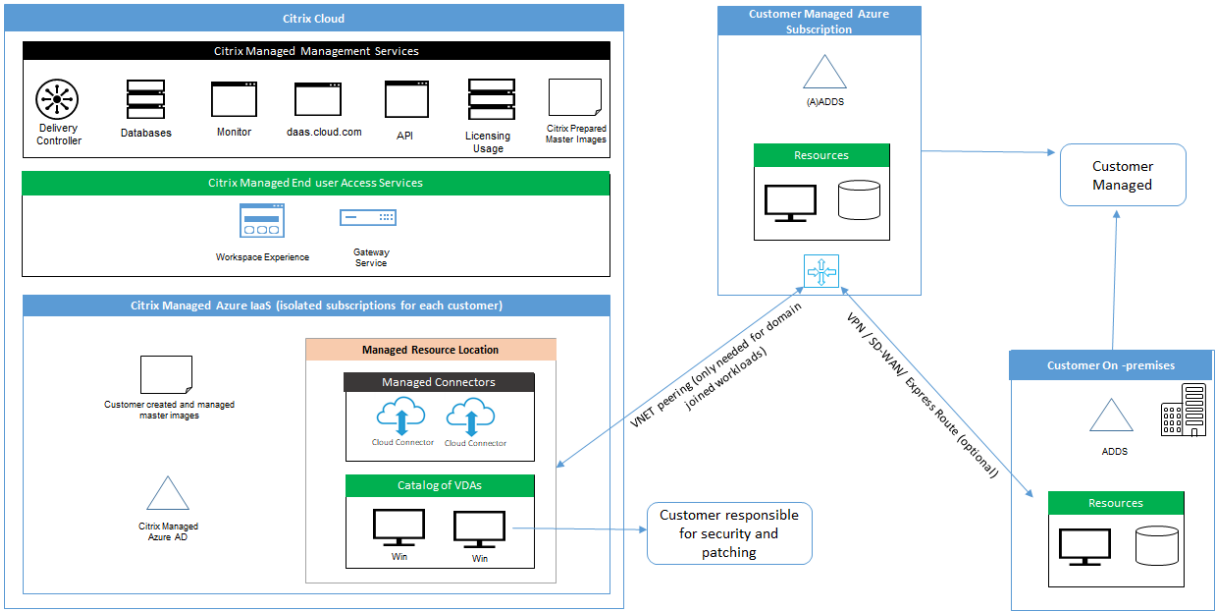
2019 年 9 月

- デフォルトでは、マシンは Citrix Managed Azure サブスクリプションで作成されます。これで、独自のカスタマー管理の Azure サブスクリプションでカタログとイメージを作成することもできます。

セキュリティの技術概要

July 16, 2021

次の図は、Citrix Virtual Apps and Desktops Standard for Azure のコンポーネントを示しています。この例では、VNet ピア接続を使用します。



Citrix Virtual Apps and Desktops Standard for Azure では、デスクトップとアプリケーションを配信するお客様の仮想配信エージェント（VDA）と Citrix Cloud Connector が、Citrix が管理する Azure サブスクリプションおよびテナントに展開されます。

Citrix クラウドベースのコンプライアンス

2021 年 1 月時点で、さまざまな Citrix Virtual Apps and Desktops サービスエディションおよび Workspace Premium Plus での Citrix Managed Azure Capacity の使用は、Citrix SOC 2（タイプ 1 または 2）、ISO 27001、HIPAA、またはその他のクラウドコンプライアンスの要件に対して評価されていません。Citrix Cloud の認定について詳しくは、「Citrix Trust Center」を参照してください。また、頻繁に更新を確認してください。

Citrix 責任

ドメインに参加していないカタログ用の **Citrix Cloud Connector**

Citrix Virtual Apps and Desktops Standard for Azure では、各リソースの場所に少なくとも 2 つの Cloud Connector がデプロイされます。一部のカタログは、同じ顧客の他のカタログと同じリージョンにある場合、リソースの場所を共有することがあります。

Citrix は、ドメインに参加していないカタログ Cloud Connectors に対する次のセキュリティ操作を担当します。

- オペレーティングシステムの更新とセキュリティパッチの適用
- ウイルス対策ソフトウェアのインストールとメンテナンス
- Cloud Connector ソフトウェアアップデートの適用

お客様は Cloud Connector にアクセスできません。したがって、ドメインに参加していないカタログ Cloud Connectors のパフォーマンスについては、Citrix が全面的に責任を負います。

Azure サブスクリプションと **Azure Active Directory**

Citrix は、お客様用に作成された Azure サブスクリプションと Azure Active Directory（AAD）のセキュリティを担当します。Citrix ではテナントの分離が保証されるため、各顧客には独自の Azure サブスクリプションと AAD が割り当てられ、異なるテナント間のクロストークが防止されます。また、Citrix は、AAD へのアクセスを、Citrix Virtual Apps and Desktops Standard for Azure サービスおよび Citrix 運用担当者のみに制限します。Citrix による各顧客の Azure サブスクリプションへのアクセスは監査されます。

ドメインに参加していないカタログをご利用のお客様は、Citrix Workspace での認証手段として、Citrix が管理する AAD を使用できます。これらのお客様のために、Citrix は Citrix が管理する AAD に限定された権限ユーザーアカウントを作成します。ただし、顧客のユーザーも管理者も、Citrix が管理する AAD 上でアクションを実行することはできません。これらのお客様が代わりに独自の AAD を使用することを選択した場合、そのセキュリティについて完全に責任を負います。

仮想ネットワークとインフラストラクチャ

お客様の Citrix Managed Azure サブスクリプション内で、Citrix はリソースの場所を分離するための仮想ネットワークを作成します。これらのネットワーク内で、Citrix は、ストレージアカウント、キーボールト、およびその他の Azure リソースに加えて、VDA、Cloud Connector、およびイメージビルダーマシン用の仮想マシンを作成します。Citrix は、Microsoft と協力して、仮想ネットワークファイアウォールを含む仮想ネットワークのセキュリティを担当します。

Citrix は、デフォルトの Azure ファイアウォールポリシー（ネットワークセキュリティグループ）が、VNet ピアリングおよび SD-WAN 接続のネットワークインターフェイスへのアクセスを制限するように構成されていることを確認します。通常、これは VDA および Cloud Connector への着信トラフィックを制御します。詳しくは、次のページを参照してください：

- Azure VNet ピア接続用のファイアウォールポリシー
- SD-WAN 接続のファイアウォールポリシー

お客様は、このデフォルトのファイアウォールポリシーを変更することはできませんが、Citrix が作成した VDA マシンに追加のファイアウォールルールを展開できます。たとえば、発信トラフィックを部分的に制限できます。Citrix が作成した VDA マシンに、仮想プライベートネットワーククライアントまたはファイアウォールルールをバイパスできるその他のソフトウェアをインストールするお客様は、発生する可能性のあるセキュリティリスクに対して責任を負うものとします。

Citrix Virtual Apps and Desktop Standard for Azure のイメージビルダーを使用して新しいマシンイメージを作成およびカスタマイズする場合、Citrix が管理する VNet でポート 3389-3390 が一時的に開かれ、新しいマシンイメージを含むマシンに RDP してカスタマイズできます。

Azure VNet ピア接続を使用する場合の **Citrix** スの責任

Citrix Virtual Apps and Desktops Standard for Azure の VDA がオンプレミスのドメインコントローラ、ファイル共有、またはその他のイントラネットリソースに接続するために、Citrix Virtual Apps および Desktops Standard for Azure は、接続オプションとして VNet ピアリングワークフローを提供します。お客様の Citrix が管理する仮想ネットワークは、顧客管理の Azure 仮想ネットワークとピアリングされます。カスタマーマネージド仮想ネットワークは、Azure ExpressRoute や IPsec トンネルなど、お客様が選択したクラウドからオンプレミスの接続ソリューションを使用して、お客様のオンプレミスリソースとの接続を有効にできます。

VNet ピアリングに対するシトリックスの責任は、Citrix とカスタマー管理の VNet 間のピアリング関係を確立するためのワークフローおよび関連する Azure リソース構成のサポートに限定されます。

Azure VNet ピア接続用のファイアウォールポリシー

Citrix は、VNet ピア接続を使用する受信トラフィックと送信トラフィックに対して、次のポートを開閉します。

ドメインに参加していないマシンを持つ **Citrix** が管理する **VNet**

- インバウンドルール
  - VDA から Cloud Connector、および Cloud Connector から VDA へのポート 80、443、1494、および 2598 の受信を許可します。
  - 監視シャドウ機能で使用される IP 範囲から VDA へのポート 49152～65535 での受信を許可します。「Citrix テクノロジで使用される通信ポート」を参照してください。
  - その他すべてのインバウンドを拒否します。これには、VDA から VDA への VNet 内トラフィック、および VDA から Cloud Connector への VNet トラフィックが含まれます。
- アウトバウンドルール
  - すべてのトラフィックアウトバウンドを許可します。

Citrix が管理するドメインに参加したマシンを持つ **VNet**

- インバウンドルール:
  - VDA から Cloud Connector、および Cloud Connector から VDA へのポート 80、443、1494、および 2598 の受信を許可します。
  - 監視シャドウ機能で使用される IP 範囲から VDA へのポート 49152～65535 での受信を許可します。「Citrix テクノロジで使用される通信ポート」を参照してください。
  - その他すべてのインバウンドを拒否します。これには、VDA から VDA への VNet 内トラフィック、および VDA から Cloud Connector への VNet トラフィックが含まれます。

- アウトバウンドルール
  - すべてのトラフィックアウトバウンドを許可します。

ドメインに参加したマシンを使用したカスタマーマネージド **VNet**

- VNet を正しく構成するかどうかは、お客様次第です。これには、ドメイン参加のために次のポートを開くことが含まれます。
- インバウンドルール:
  - 内部起動のために、クライアント IP から 443、1494、2598 のインバウンドを許可します。
  - Citrix VNet（お客様が指定した IP 範囲）からの 53、88、123、135-139、389、445、636 での受信を許可します。
  - プロキシ構成で開かれたポートでのインバウンドを許可します。
  - 顧客が作成したその他のルール。
- アウトバウンドルール:
  - 443、1494、2598 の Citrix VNet（お客様が指定した IP 範囲）への内部起動を許可します。
  - 顧客が作成したその他のルール。

SD-WAN 接続を使用する場合の **Citrix** の責任範囲

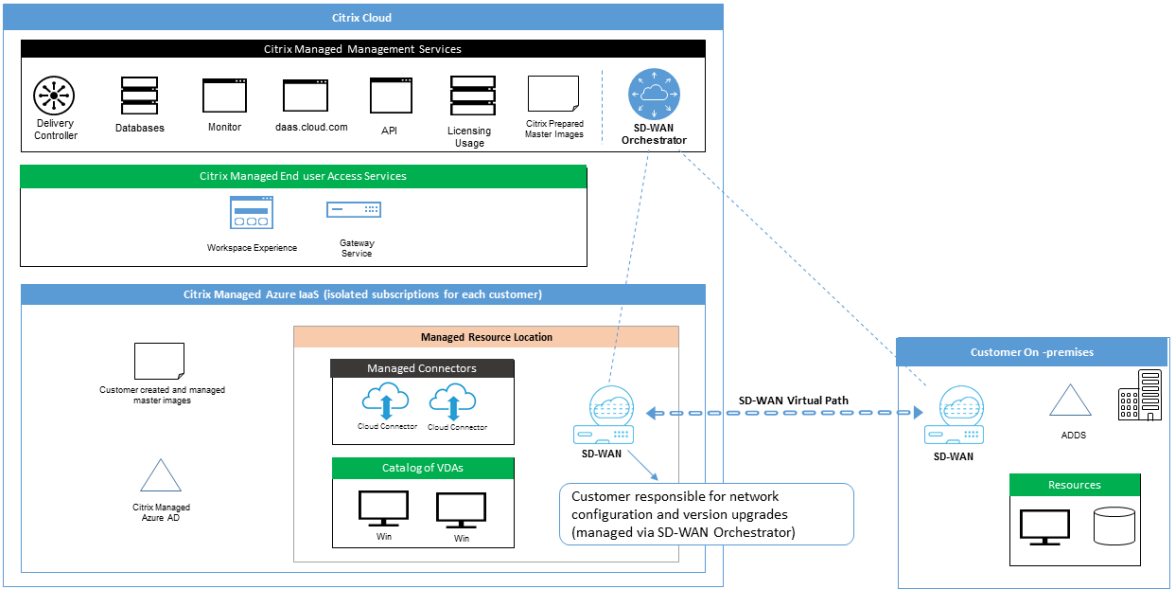
シトリックスは、仮想 Citrix SD-WAN インスタンスを展開する完全に自動化された方法をサポートし、Citrix Virtual Apps and Desktops Standard for Azure およびオンプレミスリソース間の接続を可能にします。Citrix SD-WAN 接続には、VNet ピアリングと比較して次のような多くの利点があります。

VDA-データセンターおよび VDA 間ブランチ（ICA）接続の高い信頼性とセキュリティ。

- 高度な QoS 機能と VoIP 最適化により、オフィスワーカーにとって最高のエンドユーザーエクスペリエンス。
- Citrix HDX ネットワークトラフィックやその他のアプリケーションの使用状況を検査、優先順位付け、レポートする機能が組み込まれています。

Citrix では、Citrix SD-WAN ネットワークを管理するために SD-WAN Orchestrator を使用して Citrix Virtual Apps and Desktops Standard for Azure の Citrix SD-WAN 接続を利用する必要があります。

次の図は、SD-WAN 接続を使用した Citrix Virtual Apps and Desktops Standard for Azure に追加されたコンポーネントを示しています。



Citrix Virtual Apps and Desktops Standard for Azure の Citrix SD-WAN 展開は、Citrix SD-WAN の標準の Azure 展開構成に似ています。詳しくは、「Azure に Citrix SD-WAN スタンダードエディションインスタンスをデプロイする」を参照してください。高可用性構成では、Azure ロードバランサーを備えた SD-WAN インスタンスのアクティブ/スタンバイペアが、VDA と Cloud Connector を含むサブネットとインターネットの間のゲートウェイとしてデプロイされます。非 HA 構成では、1 つの SD-WAN インスタンスのみがゲートウェイとしてデプロイされます。仮想 SD-WAN アプライアンスのネットワークインターフェイスには、2 つのサブネットに分割された個別の小さなアドレス範囲からアドレスが割り当てられます。

SD-WAN 接続を構成する場合、Citrix は上記の管理対象デスクトップのネットワーク構成にいくつかの変更を加えます。特に、インターネット宛先へのトラフィックを含む VNet からのすべての発信トラフィックは、クラウド SD-WAN インスタンスを介してルーティングされます。SD-WAN インスタンスは、Citrix が管理する VNet の DNS サーバーとしても構成されています。

仮想 SD-WAN インスタンスへの管理アクセスには、管理者ログインとパスワードが必要です。SD-WAN の各インスタンスには、SD-WAN Orchestrator UI、仮想アプライアンス管理 UI、および CLI によるリモートログインおよびトラブルシューティングに SD-WAN 管理者が使用できる、一意のランダムセキュアパスワードが割り当てられます。

他のテナント固有のリソースと同様に、特定のカスタマー VNet にデプロイされた仮想 SD-WAN インスタンスは、他のすべての VNet から完全に隔離されます。

お客様が Citrix SD-WAN 接続を有効にすると、Citrix Virtual Apps and Desktops Standard for Azure で使用される仮想 SD-WAN インスタンスの初期展開を自動化し、基盤となる Azure リソース（仮想マシン、ロードバランサなど）を維持し、安全で効率的なすぐに利用できます。仮想 SD-WAN インスタンスの初期設定のデフォルト設定で、SD-WAN Orchestrator による継続的なメンテナンスとトラブルシューティングを有効にします。また、SD-WAN ネットワーク構成の自動検証、既知のセキュリティリスクの確認、SD-WAN Orchestrator による対応する警告の表示など、合理的な対策を講じています。

SD-WAN 接続のファイアウォールポリシー

Citrix は、Azure ファイアウォールポリシー（ネットワークセキュリティグループ）とパブリック IP アドレスの割り当てを使用して、仮想 SD-WAN アプライアンスのネットワークインターフェイスへのアクセスを制限します。

- WAN と管理インターフェイスだけがパブリック IP アドレスを割り当てられ、インターネットへのアウトバウンド接続が許可されます。
- Citrix が管理する VNet のゲートウェイとして機能する LAN インターフェイスは、同じ VNet 上の仮想マシンとのネットワークトラフィックの交換のみ許可されます。
- WAN インターフェイスは、着信トラフィックを UDP ポート 4980（仮想パス接続のために Citrix SD-WAN によって使用される）に制限し、VNet へのアウトバウンドトラフィックを拒否します。
- 管理ポートは、ポート 443（HTTPS）および 22（SSH）へのインバウンドトラフィックを許可します。
- HA インターフェイスは、相互に制御トラフィックを交換することだけが許可されます。

インフラストラクチャへのアクセス

Citrix は、お客様の Citrix 管理インフラストラクチャ（Cloud Connector）にアクセスして、ログの収集（Windows イベントビューアを含む）やサービスの再起動などの特定の管理タスクを実行することがあります。Citrix は、これらのタスクを安全かつ安全に実行し、お客様への影響を最小限に抑える責任があります。Citrix は、ログファイルを安全かつ安全に取得、移送、および処理することを保証する責任もあります。カスタマー VDA にはこの方法ではアクセスできません。

ドメインに参加していないカタログのバックアップ

Citrix は、ドメインに参加していないカタログのバックアップを実行する責任を負いません。

マシンイメージのバックアップ

シトリックスは、Citrix Virtual Apps and Desktops Standard for Azure にアップロードされたすべてのマシンイメージ（イメージビルダーで作成されたイメージを含む）のバックアップを担当します。Citrix はこれらのイメージにローカル冗長ストレージを使用します。

ドメインに参加していないカタログの踏み台

Citrix 運用担当者は、必要に応じて、お客様が問題を認識する前に、お客様の問題を診断および修復するために、お客様の Citrix が管理する Azure サブスクリプションにアクセスするための踏み台を作成できます。Citrix は、踏み台の作成に顧客の同意を必要としません。Citrix が要塞を作成すると、Citrix は要塞に対して強力なランダムに生成されたパスワードを作成し、Citrix NAT IP アドレスへの RDP アクセスを制限します。要塞が不要になった場合、Citrix はそれを破棄し、パスワードは無効になります。踏み台（およびそれに付随する RDP アクセスルール）は、操作が完了すると、廃棄されます。Citrix は、踏み台を持つお客様のドメインに参加していない Cloud Connectors にのみアクセスできます。Citrix には、ドメインに参加していない VDA またはドメインに参加している Cloud Connector および VDA にログインするためのパスワードがありません。

トラブルシューティングツールを使用する場合のファイアウォールポリシー

お客様がトラブルシューティングのために踏み台マシンの作成を要求すると、Citrix が管理する VNet に次のセキュリティグループが変更されます。

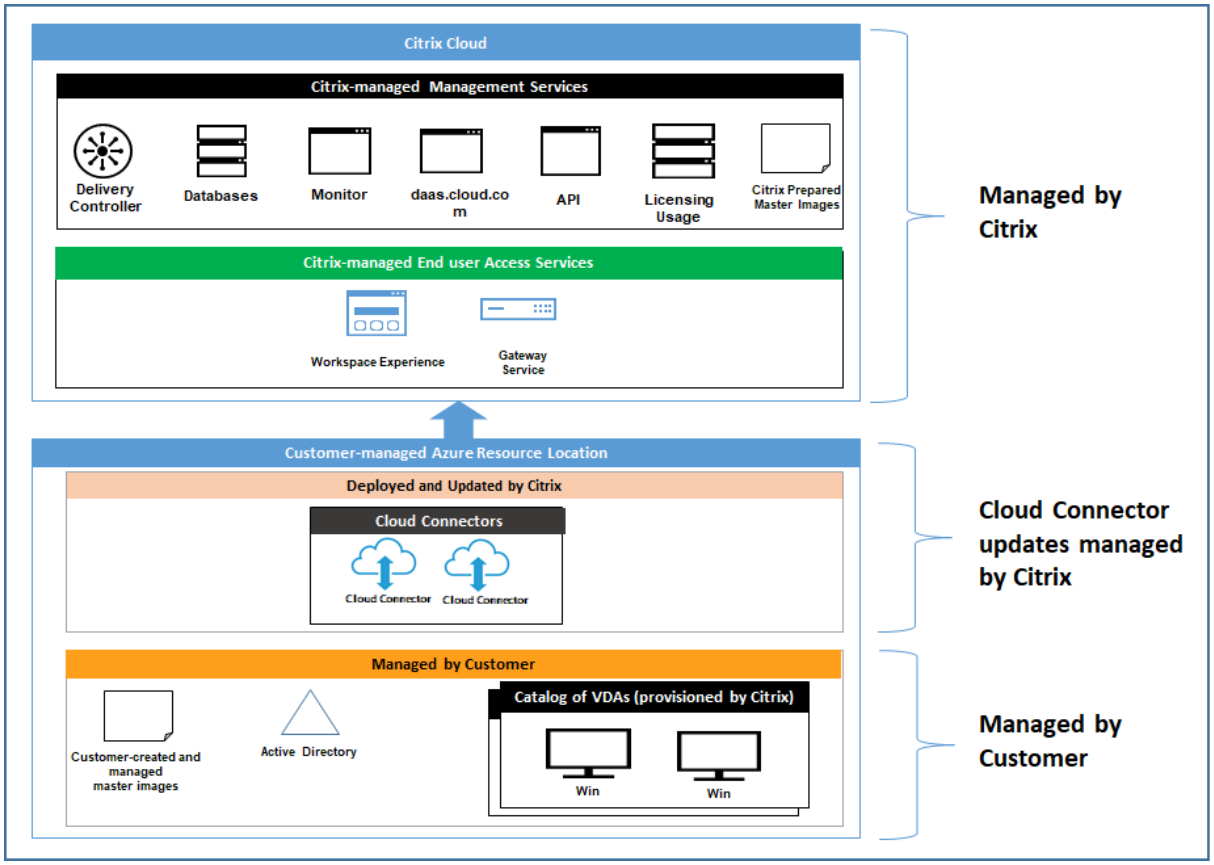
- お客様が指定した IP 範囲から踏み台への 3389 インバウンドを一時的に許可します。
- 要塞 IP アドレスから VNet（VDA および Cloud Connector）の任意のアドレスへの 3389 の受信を一時的に許可します。
- Cloud Connector、VDA、およびその他の VDA 間の RDP アクセスを引き続きブロックします。

お客様がトラブルシューティングのために RDP アクセスを有効にすると、Citrix が管理する VNet に次のセキュリティグループが変更されます。

- ユーザーが指定した IP 範囲から VNet（VDA および Cloud Connector）の任意のアドレスへの 3389 の受信を一時的に許可します。
- Cloud Connector、VDA、およびその他の VDA 間の RDP アクセスを引き続きブロックします。

カスタマー管理サブスクリプション

カスタマー管理サブスクリプションの場合、Citrix は Azure リソースのデプロイ時に上記の責任に従います。デプロイ後は、お客様が Azure サブスクリプションの所有者であるため、上記のすべてがお客様の責任に該当します。



お客様の責任

VDA とマシンイメージ

お客様は、VDA マシンにインストールされているソフトウェアのすべての側面について責任を負います。これには以下が含まれます。

- オペレーティングシステムの更新とセキュリティパッチ
- ウイルス対策とマルウェア対策
- VDA ソフトウェアアップデートとセキュリティパッチ
- 追加のソフトウェアファイアウォールルール（特にアウトバウンドトラフィック）
- Citrix のセキュリティに関する考慮事項とベストプラクティスに従ってください

Citrix は、出発点として用意されたイメージを提供します。このイメージは、概念実証やデモンストレーションの目的で、または独自のマシンイメージを構築するためのベースとして使用できます。Citrix は、この準備されたイメージのセキュリティを保証しません。Citrix は、準備されたイメージのオペレーティングシステムと VDA ソフトウェアを最新の状態に保ち、これらのイメージで Windows Defender を有効にします。

VNet ピアリングを使用する際のお客様の責任

お客様は、ドメインに参加したマシンを使用したカスタマーマネージド VNetで指定されたすべてのポートを開く必要があります。

VNet ピアリングを構成する場合、お客様は、独自の仮想ネットワークのセキュリティと、オンプレミスリソースへの接続について責任を負います。お客様は、Citrix が管理するピアリング仮想ネットワークからの着信トラフィックのセキュリティについても責任を負います。Citrix は、Citrix が管理する仮想ネットワークからお客様のオンプレミスリソースへのトラフィックをブロックするアクションは実行しません。

お客様には、着信トラフィックを制限するための以下のオプションがあります。

- Citrix が管理する仮想ネットワークに、お客様のオンプレミスネットワークまたは顧客管理の接続仮想ネットワーク内の他の場所で使用されていない IP ブロックを指定します。これは VNet ピアリングに必要です。
- Azure ネットワークセキュリティグループとファイアウォールをお客様の仮想ネットワークとオンプレミスネットワークに追加して、Citrix 管理の IP ブロックからのトラフィックをブロックまたは制限します。
- お客様の仮想ネットワークとオンプレミスネットワークに、侵入防御システム、ソフトウェアファイアウォール、行動分析エンジンなどの対策を Citrix が管理する IP ブロックをターゲットに展開します。

SD-WAN 接続を使用する場合のお客様の責任

SD-WAN 接続が構成されている場合、お客様は、Citrix Virtual Apps and Desktops Standard for Azure で使用する仮想 SD-WAN インスタンスをネットワーク要件に従って構成できます。ただし、Citrix 管理対象 VNet での SD-WAN の正しい動作を保証するために必要ないくつかの要素を除きます。お客様の責任には以下が含まれます。

- DNS およびインターネットトラフィックブレークアウトのルールを含む、ルーティングルールとファイアウォールルールの設計と構成。

- SD-WAN ネットワーク設定のメンテナンス。
- ネットワークの動作ステータスのモニタリング。
- Citrix SD-WAN ソフトウェアアップデートまたはセキュリティ修正プログラムをタイムリーに展開顧客ネットワーク上の Citrix SD-WAN のすべてのインスタンスは、同じバージョンの SD-WAN ソフトウェアを実行する必要があるため、Azure SD-WAN インスタンスの Citrix Virtual Apps and Desktops Standard for Azure SD-WAN インスタンスへの更新されたソフトウェアバージョンの展開は、ネットワークのメンテナンススケジュールと制約に従って顧客によって管理する必要があります。

SD-WAN ルーティングとファイアウォールルールの不適切な構成、または SD-WAN 管理パスワードの管理ミスにより、Citrix Virtual Apps and Desktops Standard for Azure の仮想リソースと、Citrix SD-WAN 仮想パスを介して到達可能なオンプレミスのリソースの両方にセキュリティリスクが発生する可能性があります。もう 1 つのセキュリティリスクは、Citrix SD-WAN ソフトウェアを最新のパッチリリースに更新しないことによるものです。SD-WAN Orchestrator およびその他の Citrix Cloud サービスはこのようなリスクに対処する手段を提供しますが、最終的には仮想 SD-WAN インスタンスが適切に構成されていることを確認する責任があります。

プロキシ

お客様は、VDA からのアウトバウンドトラフィックにプロキシを使用するかどうかを選択できます。プロキシを使用する場合、お客様は以下について責任を負います。

- VDA マシンイメージのプロキシ設定、または VDA がドメインに参加している場合は、Active Directory グループポリシーを使用してプロキシ設定を構成します。
- プロキシのメンテナンスとセキュリティ。

プロキシは、Citrix Cloud Connector または他の Citrix が管理するインフラストラクチャで使用することはできません。

カタログの復元力

Citrix は、回復力のレベルが異なる 3 種類のカタログを提供しています。

- 静的：各ユーザーは単一の VDA に割り当てられます。このカタログタイプは高可用性を提供しません。ユーザーの VDA がダウンした場合は、回復するために新しい VDA に配置する必要があります。Azure は、シングルインスタンス仮想マシンに 99.5% SLA を提供します。ユーザーは引き続きユーザープロファイルをバックアップできますが、VDA に対するカスタマイズ（プログラムのインストールや Windows の構成など）は失われます。
- ランダム：各ユーザーは起動時にサーバー VDA にランダムに割り当てられます。このカタログタイプは、冗長性によって高可用性を実現します。VDA がダウンしても、ユーザーのプロフィールが別の場所にあるため、情報は失われません。
- **Windows 10** のマルチセッション：このカタログタイプはランダムタイプと同じ方法で動作しますが、サーバー VDA の代わりに Windows 10 ワークステーション VDA を使用します。

ドメインに参加しているカタログのバックアップ

お客様が VNet ピアリングでドメインに参加しているカタログを使用する場合、お客様はユーザープロファイルをバックアップする責任があります。オンプレミスのファイル共有を構成し、Active Directory または VDA にポリシーを設定して、これらのファイル共有からユーザープロファイルをプルすることをお勧めします。お客様は、これらのファイル共有のバックアップと可用性について責任を負います。

障害回復

Azure のデータ損失が発生した場合、Citrix は Citrix が管理する Azure サブスクリプション内のリソースをできるだけ多くリカバリします。Citrix は、Cloud Connector と VDA の回復を試みます。Citrix がこれらのアイテムのリカバリに失敗した場合、お客様は新しいカタログを作成する責任があります。Citrix では、マシンイメージがバックアップされ、ユーザーがユーザープロファイルをバックアップし、カタログを再構築できるものと見なします。

Azure リージョン全体が失われた場合、お客様は、新しいリージョンで顧客管理仮想ネットワークを再構築し、Citrix Virtual Apps and Desktops Standard for Azure 内で新しい VNet ピアリングまたは新しい SD-WAN インスタンスを作成する責任があります。

Citrix とお客様共通の責任

ドメインに参加しているカタログ用の **Citrix Cloud Connector**

Citrix Virtual Apps and Desktops Standard for Azure では、各リソースの場所に少なくとも 2 つの Cloud Connector がデプロイされます。一部のカタログは、同じ顧客の他のカタログと同じリージョン、VNet ピアリング、およびドメインに存在する場合、リソースの場所を共有することがあります。Citrix は、イメージの次のデフォルトのセキュリティ設定に対して、お客様のドメインに参加している Cloud Connector を構成します。

- オペレーティングシステムの更新とセキュリティパッチ
- アンチウイルスソフトウェア
- Cloud Connector のソフトウェアアップデート

お客様は、通常 Cloud Connector にアクセスできません。ただし、カタログのトラブルシューティング手順を使用してドメイン資格情報を使用してログインすることで、アクセスを取得できます。踏み台からログインする際に行われた変更については、お客様が責任を負うものとします。

お客様は、Active Directory グループポリシーを使用して、ドメインに参加している Cloud Connector を制御することもできます。お客様は、Cloud Connector に適用されるグループポリシーが安全かつ賢明であることを保証する責任があります。たとえば、お客様がグループポリシーを使用してオペレーティングシステムの更新を無効にすることを選択した場合、お客様は Cloud Connector でオペレーティングシステムの更新を実行する責任があります。お客様は、グループポリシーを使用して、別のウイルス対策ソフトウェアをインストールするなど、Cloud Connector のデフォルトよりも厳格なセキュリティを適用することもできます。一般的に、Citrix では、Citrix が使用するデフォルトを問題なく適用できるため、ポリシーなしで Cloud ConnectCitrix s を独自の Active Directory ory 組織単位に配置することをお勧めします。

トラブルシューティング

Citrix Virtual Apps と Desktops Standard for Azure でカタログで問題が発生した場合、トラブルシューティングには 2 つのオプションがあります。踏み台の使用と RDP アクセスの有効化です。どちらのオプションでも、お客様にセキュリティリスクがもたらされます。お客様は、これらのオプションを使用する前に、このリスクを引き受けることに理解し、同意する必要があります。

Citrix は、トラブルシューティング操作を実行するために必要なポートを開閉し、これらの操作中にアクセスできるマシンを制限する責任があります。

踏み台または RDP アクセスのいずれかで、操作を実行するアクティブユーザーは、アクセスされているマシンのセキュリティを担当します。お客様が RDP 経由で VDA または Cloud Connector にアクセスし、誤ってウイルスに感染した場合、その責任はお客様の責任となります。Citrix サポート担当者がこれらのマシンにアクセスする場合、安全に操作を実行するのは担当者の責任です。展開内の踏み台または他のマシンにアクセスするユーザーによって公開された脆弱性に対する責任（たとえば、許可リストに IP 範囲を追加するお客様の責任、IP 範囲を正しく実装する Citrix の責任）については、このドキュメントの他の部分で説明します。

どちらのシナリオでも Citrix RDP トラフィックを許可するファイアウォールの例外を正しく作成する必要があります。シトリックスは、お客様が要塞を処分した後、または Citrix VCitrix Virtual Apps and Desktops Standard for Azure を介した RDP アクセスを終了した後で、これらの例外を取り消す責任もあります。

バスティオンズ

Citrix は、お客様の Citrix が管理するサブスクリプション内で、お客様の Citrix が管理する仮想ネットワークに踏み台を作成して、プロアクティブに（お客様への通知なし）、またはお客様が提起した問題に対応して、問題の診断と修復を行うことができます。踏み台は、お客様が RDP を介してアクセスし、RDP を介して VDA および（ドメイン参加カタログの場合）Cloud Connector にアクセスして、ログの収集、サービスの再起動、その他の管理タスクの実行に使用できるマシンです。デフォルトでは、踏み台を作成すると、外部ファイアウォールルールが開き、お客様が指定した範囲の IP アドレスから踏み台マシンへの RDP トラフィックを許可します。また、内部ファイアウォールルールを開き、RDP を介して Cloud Connector と VDA へのアクセスを許可します。これらのルールを開くと、大きなセキュリティリスクが生じます。

お客様は、ローカルの Windows アカウントに使用する強力なパスワードを提供する責任があります。お客様は、踏み台への RDP アクセスを許可する外部 IP アドレス範囲を提供する責任もあります。お客様が IP 範囲を提供しない（誰でも RDP アクセスを許可する）を選択した場合は、悪質な IP アドレスによって試みられるアクセスについてお客様が責任を負うものとします。

トラブルシューティングの完了後、踏み台を削除する責任もお客様にあります。要塞ホストは追加の攻撃面を公開するため、Citrix はマシンの電源投入後 8 時間後に自動的にシャットダウンします。ただし、Citrix は踏み台を自動的に削除することはありません。お客様が踏み台を長期間使用することを選択した場合、その踏み台をパッチ適用および更新する責任があります。踏み台を削除する前に、数日間だけ踏み台の使用をお勧めします。お客様が最新の踏み台が必要な場合は、現在の踏み台を削除してから新しい踏み台を作成できます。これにより、最新のセキュリティパッチを使用して新しいマシンをプロビジョニングできます。

RDP アクセス

ドメインに参加しているカタログでは、お客様の VNet ピアリングが機能している場合、ピアリングされた VNet から Citrix が管理する VNet への RDP アクセスを有効にできます。お客様がこのオプションを使用する場合、お客様は VNet ピアリングを介して VDA と Cloud Connector にアクセスする責任があります。送信元 IP アドレスの範囲を指定することで、お客様の内部ネットワーク内であっても RDP アクセスをさらに制限できます。お客様は、ドメイン資格情報を使用してこれらのマシンにログインする必要があります。お客様が Citrix サポートと協力して問題を解決している場合、お客様はこれらの認証情報をサポート担当者と共有する必要がある場合があります。問題が解決した後、お客様は RDP アクセスを無効にする責任があります。お客様のピアリングまたはオンプレミスネットワークから RDP アクセスをオープンに保つと、セキュリティリスクが生じます。

ドメイン資格情報

お客様がドメインに参加したカタログの使用を選択した場合、お客様は、Citrix Virtual Apps and Desktops Standard for Azure に対して、マシンをドメインに参加するための権限を持つドメインアカウント（ユーザー名とパスワード）を提供する責任があります。ドメインの資格情報を提供する場合、お客様は、次のセキュリティ原則を遵守する責任があります。

- 監査可能：アカウントが使用される対象を簡単に監査できるように、Citrix Virtual Apps and Desktops Standard for Azure 専用にアカウントを作成する必要があります。
- スコープ付き**:** このアカウントでは、マシンをドメインに参加させるためのアクセス許可のみが必要です。完全なドメイン管理者であってはなりません。
- セキュア**:** 強力なパスワードをアカウントに配置する必要があります。

Citrix は、お客様の Citrix が管理する Azure サブスクリプション内の Azure Key Vault にこのドメインアカウントの安全なストレージを担当します。アカウントは、操作でドメインアカウントのパスワードが必要な場合にのみ取得されます。

詳細情報

関連情報については、以下を参照してください。

- セキュリティで保護された Citrix Cloud プラットフォームの展開ガイド：Citrix Cloud プラットフォームのセキュリティ情報。
- セキュリティの技術概要：Citrix Virtual Apps and Desktops サービスのセキュリティ情報
- サードパーティ通知

サービスを購読する

July 16, 2021

はじめに

Citrix または Azure Marketplace を通じて、Citrix Virtual Apps and Desktops Standard for Azure サービスへのサブスクライブ（および Citrix Azure 消費基金の注文）を行うことができます。このサービスは Citrix スを通じて評価できます。

現在、Citrix Virtual Apps Essentials または Citrix Virtual Desktops Essentials をサブスクライブしている場合は、Citrix Virtual Apps and Desktops Standard for Azure をアップグレードできます。

包括的な注文には、次の 2 つの部分があります。

- **Citrix Virtual Apps and Desktops Standard for Azure**：独自の（顧客管理の）Azure サブスクリプションを使用できます。
- **Citrix Azure** 消費基金：さらに、独自の Azure サブスクリプションに加えて、Citrix Managed Azure サブスクリプションを使用することもできます。Citrix Managed Azure サブスクリプションを使用すると、次の利点があります。
  - 複数の企業からの請求ではなく、Citrix からの単一の請求。
  - Azure サブスクリプション機能の違い。
  - Citrix によるプレミアムレベルの Microsoft サポート。

Citrix Azure 消費基金は必要ありません。ただし、お持ちでない場合は、独自の Azure サブスクリプションのみの使用に制限され、その他の機能特典は受けられません。

注文プロセスは、Citrix または Azure Marketplace のどちらを使用して注文するかによって、若干異なります。

- Citrix 経由で注文すると、Citrix Virtual Apps and Desktops Standard for Azure サービスと Citrix Azure 消費基金を同時に注文できます。
- Azure Marketplace 経由で注文する場合は、まず Citrix Virtual Apps and Desktops Standard for Azure サービスを注文します。次に、Citrix Azure 消費基金を注文します。

  サービスのみを注文する場合は、後で Azure Marketplace または Citrix アカウント担当者を通じて、Citrix Azure 消費基金を注文できます。

サービスおよび消費基金の注文先に関係なく、Citrix はオンボーディングヘルプを提供します。また、サービスが実行され、正しく構成されていることを確認します。

注文サマリー

注文手順の概要:

1. Citrix Cloud アカウントを取得する。

   Citrix Cloud アカウントをすでにお持ちで、現在 Citrix Virtual Apps and Desktops サービスをサブスクライブしている場合は、「現在 Citrix Virtual Apps およびデスクトップサービスを購読している場合」を参照してください。

2. サービスと consumption fund をAzure Marketplace から注文するか、Citrix から注文してください。

トライアル

試用版が付与されると、Citrix Managed Azure サブスクリプションを使用してカタログ、イメージ、およびその他のタスクを作成できます。試用版から、有料サービスサブスクリプションに変換できます。

その時点で Citrix が管理するリソースがある場合は、消費を購入するか、Citrix が管理するリソースを削除する必要があります。消費を購入しないと、それらのリソースは自動的に削除され、ユーザーに影響を与える可能性があります。

Citrix Cloud アカウントを取得する

Citrix Cloud アカウントにサインアップしてトライアルをリクエストするには、https://onboarding.cloud.comに進みます。そのプロセスの詳細については、「Citrix Cloud へのサインアップ」を参照してください。アカウントには、Citrix Cloud コンソールの右上隅に常に表示される組織 ID（OrgID）があります。

次のステップ: サービスをCitrix からまたはAzure Marketplace から注文します。

現在 **Citrix Virtual Apps** およびデスクトップサービスを購読している場合

Citrix Cloud アカウントでは、一度に 1 つの Citrix Virtual Apps およびデスクトップサービス（または 1 つのエディション）のみをサブスクライブできます。たとえば、Citrix Virtual Apps and Desktops Premium エディションまたはこのサービスをサブスクライブできますが、両方を購読することはできません。いくつかの互換性の例を以下に示します。

現在 Citrix Virtual Apps and Desktops サービスをサブスクライブし、このサービスをサブスクライブする場合は、次のいずれかを行う必要があります。

- 別の Citrix Cloud アカウント（OrgID）を使用してこのサービスを購読します。
- 現在サブスクライブ中のサービスを使用停止にしてから、このサービスを購入する。使用停止の指示については、CTX239027を参照してください。

サービス互換性の例

現在 Workspace Premium Plus を購読している場合、同じ OrgID を使用して注文することはできません。

- Citrix Virtual Apps and Desktops Standard for Azure
- Citrix Virtual Apps Essentials または Citrix Virtual Desktops Essentials
- Citrix Azure 消費基金

現在、Citrix Virtual Apps and Desktops Standard for Azure（またはその旧名、Citrix 管理デスクトップ）をサブスクライブしている場合、同じ OrgID を使用して次の注文を行うことはできません。

- ワークスペースプレミアムプラス
- Citrix Virtual Apps およびデスクトップアドバンストまたは Citrix Virtual Apps およびデスクトッププレミアム

- Citrix Virtual Apps または Citrix Virtual Desktops
- Citrix Virtual Apps Essentials または Citrix Virtual Desktops Essentials

Citrix から注文する

このサービス（消費基金を含む）は、Citrix Cloud または Citrix アカウント担当者を通じて注文できます。

Citrix Cloud を通じて：

1. Citrix Cloudにサインインします。**Azure** の **Virtual Apps and Desktops** サービスタイルで [トライアルをリクエスト] をクリックします。要求された情報を入力します。タイル上のテキストが [トライアルリクエスト済み] に変わります。
2. Citrix から連絡があります。サービスが使用可能になると、サービスタイルのテキストが [管理**]** に変わります。
3. Citrix Cloudにサインインします。[**Azure** の **Virtual Apps and Desktops**] タイルで、[管理] をクリックします。サービスに初めてアクセスすると、[ようこそ] ページに移動します。

Citrix から月間サブスクリプションをキャンセルする

毎月のサブスクリプションは、毎月の初めに自動的に更新されます。サービスダッシュボードを使用して、Citrix から注文した月間サブスクリプションをキャンセルできます。

(サービスダッシュボードを使用して、Citrix スを介して注文した他のサブスクリプションの種類や Azure Marketplace で注文した注文をキャンセルすることはできません)。

月間サブスクリプションをキャンセルするには、次の操作を行います。

1. Citrix Cloudにサインインします。
2. 左上のメニューで、[マイサービス**] > [Azure** の **Virtual Apps and Desktops**] の順に選択します。
3. **[**管理**]** ダッシュボードで、右側の **[**全般**]** を展開します。
4. **[**サブスクリプションのキャンセル**]** をクリックします。
5. カタログ、イメージ、接続など、アクティブなリソースが一覧表示されます。このページには、キャンセル時に Citrix が実行するアクションの概要が掲載されています。また、実行しなければならないアクションがあれば、その旨を通知します。サービスをキャンセルする理由を明記してください。必要に応じて、より多くのフィードバックを提供します。完了したら、[サブスクリプションのキャンセル] をクリックします。
6. キャンセルの条件を理解していることを確認してください。

サービスダッシュボードのバナーは、キャンセルリクエストの受信を示します。

誤ってサブスクリプションをキャンセルした場合は、月末までに Citrix 営業担当者または Citrix パートナーに連絡して、サービスを再度アクティベートしてください。

Azure マーケットプレイスで注文する

まず Citrix Virtual Apps and Desktops Standard for Azure サービスを注文し、Citrix Azure 消費基金を注文します。

以前にサービスを購入しない限り、消費基金を注文することはできません。サービスと消費基金を 1 つの順序で組み合わせることはできません。

このサービスは、Azure クラウドソリューションプロバイダーポータルでは提供されません。プライオリティサポートのお客様、または優先サポートに興味がある場合は、Citrix アカウント担当者にお問い合わせください。

要件:

- Citrix Cloud アカウントからの OrgID。
  - Citrix Cloud アカウントを持っていても OrgID がわからない場合は、Citrix Cloud コンソールの右上隅を確認します。または、アカウントの作成時に受け取ったメールをご覧ください。
  - Citrix Cloud アカウントをお持ちでない場合は、Citrix Cloud アカウントを取得するのガイダンスに従ってください。
- Azure アカウントと、そのアカウントの少なくとも 1 つの Azure サブスクリプション。

Azure マーケットプレイスでサービスを注文する

1. Azure アカウントの認証情報を使用してAzure Marketplaceにサインインします。
2. **Citrix Virtual Apps and Desktops Standard for Azure** を検索し、に移動します。
3. [今すぐ入手] をクリックします。
4. [もう一つ] メッセージで、チェックボックスをオンにし、[続行] をクリックします。
5. タブには、製品、プラン、価格、使用状況に関する情報が含まれています。準備ができたら、プランを選択し (複数のプランがある場合)、[**Setup + Subscribe**] をクリックします。
6. [基本] タブで、次の操作を行います。
   - サブスクリプション: 選択したプランを示します。
   - 名前: サブスクリプション注文の名前を入力します。
   - [プラン] セクションには、月次および複数年 (年間) の条件に基づいて、選択したプランの価格が表示されます。

     プラン期間 (月間または年間) を変更するには、[プランの変更] を選択します。目的の用語を選択し、[プランの変更] をクリックします。
7. [レビュー + 購読] タブで、次の操作を行います。
   - Azure 基本プロファイルについて以前に入力した連絡先の詳細を確認します。住所、電話番号、またはその両方を変更できます。
   - [購読] をクリックします。

8. [サブスクリプションの進行中] ページで、[アカウントを今すぐ設定] をクリックします。(ボタンが無効になっている場合は、しばらくお待ちください。)Citrix スのアクティベーションページが表示されます。
9. アクティベーションページで、次の操作を行います。
    - [サインイン] リンクを使用して、Citrix Cloud にサインインします。正常にサインインすると、[組織 **ID**] フィールドに自動的に入力されます。
    - **Quantity**: ユーザー数を入力します。(最初の注文は 25 以上でなければなりません。) 見積価格が表示されます。
    - 利用規約に同意し、[注文の有効化] をクリックします。

サービスがプロビジョニングされると、Citrix から電子メールが送信されます。プロビジョニングには時間がかかる場合があります。翌日までにメールが届かない場合は、シトリックスサポートまでお問い合わせください。

Citrix からメールを受信したら、サービスの使用を開始できます。注意: サービスのみでは、独自の Azure サブスクリプションのみを使用できます。

Citrix Virtual Apps and Desktops Standard for Azure リソースを削除しないでください。そのリソースを削除すると、サブスクリプションがキャンセルされます。

Azure マーケットプレイスで消費基金を注文する

1. Azure アカウントの認証情報を使用してAzure Marketplaceにサインインします。
2. **Citrix Azure** 消費基金を検索し、移動します。
3. [今すぐ入手] をクリックします。
4. [設定 **+** 購読] をクリックします。
5. [購読] ページで、次の操作を行います。
    - [名前] に、「マイマネージドデスクトップ」など、わかりやすい名前を入力します。サービスサブスクリプションを変更する場合は、後でこの名前を使用できます。
    - サポートしたいユーザの数を 25 ～100000 の範囲で指定します。
    - メールアドレスと電話番号を入力します。

    完了したら、[購読] をクリックします。
6. [サブスクリプションの進行状況] ページで、[パブリッシャーのサイトで **SaaS** アカウントを構成する] ボタンがアクティブになったら (青)、それをクリックします。Citrix の注文アクティベーションページに自動的に誘導されます。
7. シトリックス注文のアクティブ化ページで、Citrix Cloud OrgID を入力します。前に入力した電子メールアドレスが表示されます。必要に応じて変更することができます。完了したら、[注文を有効にする] をクリックします。

8. 消費基金注文の履行には時間がかかりません。シトリックスが注文を通知されると、Citrix Virtual Apps and Desktops Standard サービスコンソールにバナーが表示され、Citrix Managed Azure サブスクリプションが準備中であることを示します。

   管理ダッシュボードの右側にある [クラウドサブスクリプション] パネルには、サブスクリプションの使用準備が整った時期が表示されます。

Azure マーケットプレイスを通じてユーザーシートを増減する

ユーザーシートを増やす必要がある場合は、必要な数の追加シートに対して新しい Azure Marketplace 注文を作成します。

座席数を減らすには、Azure Marketplace でサービスをキャンセルし、希望する座席数を注文します。

Azure Marketplace を通じてサービスまたは消費ファンドをキャンセルする

Azure Marketplace を通じてサービスまたは消費ファンドをキャンセルするには、次の手順を実行します。

1. Azure Marketplaceにサインインします。
2. **SaaS** を検索します。
3. キャンセルするリソースを選択します。
4. リソースの省略記号メニューで、[削除] を選択します。
5. 確認ボックスの [はい] をクリックして、返金ポリシーを知っていて、リソースをキャンセルすることを確認します。

> 重要:
>
> Citrix Managed Azure サブスクリプションで作成されたカタログやイメージなど、Citrix が管理するリソースを使用している場合は、Citrix Azure 消費基金をキャンセルしないでください。

注文が承認され、処理されたとき

試用版またはサービスが承認されると、Citrix Cloud のホームページにはいくつかのタイルが表示されます。

- Azure の Virtual Apps and Desktops
- Virtual Apps and Desktops
- Gateway

Azure の Virtual Apps and Desktops は、ユーザーが使用するためにアクティブ化される唯一のサービスです。

サービスを開始するには、Citrix Cloudにサインインします。次のいずれかの方法を使用して、サービスにアクセスします。

- [**Azure** の **Virtual Apps and Desktops**] タイルで、[管理] をクリックします。
- 左上のメニューで、[マイサービス] **> [Azure** の **Virtual Apps and Desktops**] の順に選択します。

セットアップガイダンスについては、はじめにを参照してください。

このサービスにアップグレードする

現在、Citrix Virtual Apps Essentials サービスまたは Citrix Virtual Desktops Essentials サービスをサブスクライブしている場合は、次のタスクを実行して、Citrix Virtual Apps and Desktops Standard for Azure にアップグレードします。

1. https://onboarding.cloud.com/で Citrix Virtual Apps and Desktops Standard for Azure で使用する新しい組織 ID（OrgID）を作成します。（この記事の前で説明したように、同じ OrgID を使用して複数の Citrix Virtual Apps およびデスクトップサービスをサブスクライブすることはできません）。
2. Citrix セールスに連絡して、新しい OrgID を使用して、Citrix Virtual Apps and Desktops Standard for Azure および Citrix Azure 消費基金を購入してください。消費基金を注文する必要はありませんが、それがなければ、サービスのすべての機能にアクセスすることはできません。）
3. Citrix Cloudにサインインします。左上のメニューで、[マイサービス] **> [Azure** の **Virtual Apps and Desktops**] の順に選択します。
4. サービスにAzure サブスクリプションを少なくとも 1 つ追加する。
5. サービスにAzure サブスクリプションから 1 つ以上のイメージをインポートする。
6. Azure サブスクリプションからインポートしたイメージを使用して、カタログを作成。
7. 作成したカタログにユーザーの追加。
8. Citrix Virtual Apps Essentials または Citrix Virtual Desktops Essentials で使用したのと同じワークスペース URL を保持する場合は、次の手順を実行します。
   a) Essentials サービスで使用する OrgID を使用して Citrix Cloud にサインインします。左上のメニューで [ワークスペース構成] を選択します。何か違うものにワークスペース URL を変更する。
   b) Citrix Virtual Apps and Desktops Standard for Azure サービスで使用する OrgID を使用して、Citrix Cloud にサインインします。左上のメニューで [ワークスペース構成] を選択します。以前は Essentials サービスに使用していたものにワークスペース URL を変更する。
9. Azure にサインインし、Essentials サービスで使用したすべてのリソースを削除します。ガイダンスについては、Virtual Apps Essentials のキャンセルを参照してください。（手順は Citrix Virtual Desktops Essentials と同じです）
10. Azure で Azure Marketplace リソースを削除して、Essentials サービスを停止します。

はじめに

July 16, 2021

この記事では、Citrix Virtual Apps and Desktops Standard for Azure サービスを使用してデスクトップとアプリケーションを配信するためのセットアップタスクの概要を示します。実際に実行する前に、各手順を見直して、何を期待するかを理解することをお勧めします。

リモート PC アクセスのセットアップタスクについては、リモート PC アクセスを参照してください。

セットアップタスクサマリー

この記事の次のセクションでは、セットアップタスクについて説明します。

1. セットアップの準備。
2. 次のいずれかのガイダンスに従って、デプロイをセットアップします。
   - 概念実証のクイック展開
   - 本番環境での展開
3. ワークスペース URL をユーザーに提供します。

準備

- カタログ、イメージ、ネットワーク接続、または Azure サブスクリプションについて詳しくない場合は、導入として概念と用語情報を確認してください。
- 「セキュリティの概要」を読んで、お客様（お客様）と Citrix が責任を負う内容について理解してください。
- このサービスに使用できる Citrix Cloud アカウントをまだお持ちでない場合は、1 つ取得し、サービスにサインアップする。
- 「システム要件」を確認してください。
- セットアップ手順 (概念実証または実稼働) を確認します。

概念実証のクイック展開のセットアップ

この手順には、Citrix Managed Azure サブスクリプションが必要です。

1. 簡易作成を使用してカタログを作成します。
2. 管理対象の Azure AD にユーザーを追加する。
3. ユーザーをカタログに追加する。
4. Workspace URL をユーザーに通知。

実稼働環境を設定する

1. ユーザー認証に独自のアクティブディレクトリまたは Azure Active Directory を使用している場合は、Citrix Cloud でそのメソッドを接続して設定する。
2. ドメインに参加しているマシンを使用している場合は、有効な DNS サーバーエントリがあることを確認.
3. （Citrix Managed Azure サブスクリプションではなく）独自の Azure サブスクリプションを使用している場合は、Azure サブスクリプションをインポートする。
4. イメージを作成またはインポートする。Citrix 準備イメージの 1 つをカタログ内で使用できますが、これらは主に概念実証の展開を対象としています。
5. Citrix Managed Azure サブスクリプションを使用して、ユーザーがネットワーク内のアイテム（ファイルサーバーなど）にアクセスできるようにするには、Azure VNet ピアリングまたはCitrix SD-WAN接続を設定します。
6. カスタム作成を使用してカタログを作成する。

7. マルチセッションマシンのカタログを作成する場合は、必要に応じてアプリをカタログに追加。
8. Citrix Managed Azure AD を使用してユーザーを認証している場合は、ユーザーをディレクトリに追加する。
9. カタログにユーザーを追加する。
10. Workspace URL をユーザーに通知。

展開を設定したら、[監視] ダッシュボードを使用して、デスクトップの使用状況、セッション、マシンの数を表示します。

システム要件

すべてのデプロイで、次のようになります。

- **Citrix Cloud**: このサービスは Citrix Cloud を介して提供され、オンボーディングプロセスを完了するには Citrix Cloud アカウントが必要です。詳しくは、「Citrix Cloud アカウントを取得する」を参照してください。
- **Windows** ライセンス**:** Windows Server ワークロードまたは Windows 10 用の Azure 仮想デスクトップライセンスのいずれかを実行するために、リモートデスクトップサービスに対して適切なライセンスが付与されていることを確認します。

Citrix Managed Azure サブスクリプションを使用している場合は、次の手順を実行します。

- **Azure VNet** ピアリングを使用する場合の **Azure** サブスクリプション **(**オプション**):** Azure VNet ピア接続を使用して独自の Azure ネットワーク内のリソース (AD やその他のファイル共有など) にアクセスする場合は、Azure サブスクリプションが必要です。
- **Azure Active Directory** への **VDA** の参加（オプション）: Active Directory グループポリシーを使用して VDA をドメインに参加するには、Active Directory でそのアクションを実行する権限を持つ管理者である必要があります。詳しくは、「お客様の責任」を参照してください。

社内オンプレミスネットワークへの接続を構成するには、追加の要件があります。

- 任意の接続 (Azure VNet ピアリングまたは SD-WAN): すべての接続の要件。
- Azure VNet ピアリング接続: VNet ピアリングの要件と準備。
- SD-WAN 接続: SD-WAN 接続要件と準備。

カタログの作成時に独自の Azure イメージを使用する場合は、このサービスにインポートする前にこれらの画像は特定の要件を満たしている必要があります。

追加情報:

- インターネット接続要件: システムおよび接続要件。
- サービス展開におけるリソース制限: 制限。

サポートされるオペレーティングシステム

Citrix マネージド Azure サブスクリプションを使用する場合:

- Windows 7（VDA は最新の累積更新プログラムでは 7.15 LTSR である必要があります）

- Windows 10 シングルセッション
- Windows 10 マルチセッション
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Red Hat Enterprise Linux と Ubuntu

カスタマー管理の Azure サブスクリプションを使用する場合:

- Windows 7（VDA は最新の累積更新プログラムでは 7.15 LTSR である必要があります）
- Windows 10 エンタープライズシングルセッション
- Windows 10 エンタープライズ仮想デスクトップマルチセッション
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Red Hat Enterprise Linux と Ubuntu

ワークスペース **URL**

カタログを作成してユーザーを割り当てた後、デスクトップおよびアプリケーションの検索先 (Workspace URL) をユーザーに通知します。ワークスペース URL は、すべてのカタログとユーザーで同じです。

[管理] ダッシュボードから、右側の [ユーザーアクセスと認証] を展開して URL を表示します。

Citrix Cloud のワークスペース URL の最初の部分を変更できます。手順については、「ワークスペース URL をカスタマイズする」を参照してください。

支援が必要な場合

トラブルシューティング 記事を見直してください。

それでもサービスに問題がある場合は、ヘルプとサポートの利用の手順に従ってチケットを開きます。

カタログを作成

July 16, 2021

公開デスクトップとアプリケーションで使用する場合、カタログは同一の仮想マシンのグループです。デスクトップを展開すると、カタログ内のマシンは選択したユーザーと共有されます。アプリケーションを公開すると、マルチセッションマシンは、選択したユーザーと共有されるアプリケーションをホストします。

> 注:
>
> リモート PC アクセスカタログの作成については、リモート PC アクセスを参照してください。

マシンの種類

カタログには、次のいずれかのタイプのマシンを含めることができます。

- 静的**:** カタログには、シングルセッションの静的マシン (個人用デスクトップ、専用デスクトップ、または永続デスクトップとも呼ばれます) が含まれます。静的とは、ユーザーがデスクトップを起動したときに、そのデスクトップがそのユーザーに「属する」ことを意味します。ユーザーがデスクトップに加えた変更は、ログオフ時に保持されます。後で、そのユーザーが Citrix Workspace に戻ってデスクトップを起動すると、同じデスクトップになります。
- ランダム**:** カタログには、シングルセッションのランダムマシン (非永続デスクトップとも呼ばれます) が含まれています。ランダムとは、ユーザーがデスクトップを起動したときに、そのユーザーがそのデスクトップに加えた変更がログオフ後に破棄されることを意味します。後でそのユーザーが Citrix Workspace に戻ってデスクトップを起動すると、同じデスクトップである場合とそうでない場合があります。
- マルチセッション**:** カタログには、アプリとデスクトップを備えたマシンが含まれています。複数のユーザーがこれらの各マシンに同時にアクセスできます。ユーザーは、ワークスペースからデスクトップまたはアプリを起動できます。アプリセッションは共有できます。アプリとデスクトップの間では、セッション共有は許可されていません。
  - マルチセッションカタログを作成するときは、作業負荷 (データ入力など)、標準 (オフィスアプリなど)、重い (エンジニアリングなど)、またはカスタムを選択します。各オプションは、マシンごとの特定のマシンとセッション数を表し、カタログがサポートするセッションの総数を示します。
  - カスタム作業負荷を選択した場合は、CPU、RAM、およびストレージの使用可能な組み合わせから選択します。マシンあたりのマシン数およびセッション数を入力します。これにより、カタログがサポートするセッションの総数が得られます。

デスクトップを展開する場合、静的およびランダムマシンタイプは「デスクトップタイプ」と呼ばれることがあります。

カタログの作成方法

カタログを作成して構成するには、いくつかの方法があります。

- クイック作成は、開始する最速の方法です。最小限の情報を提供し、サービスは残りの処理を行います。クイック作成カタログは、テスト環境や概念実証に最適です。
- カスタム作成では、クイック作成よりも多くの構成を選択できます。クイック作成カタログよりも本番環境に適しています。
- リモート **PC** アクセスカタログには、ユーザーがリモートでアクセスする既存のマシン（通常は物理）が含まれています。これらのカタログの詳細と手順については、リモート PC アクセスを参照してください。

クイック作成とカスタム作成の比較を次に示します。

クイック作成	カスタム作成
提供する情報が少なくなります。	提供する詳細情報。
一部の機能の選択肢が少なくなります。	一部の機能の選択肢が増えます。
Citrix が管理する Azure Active Directory ユーザー認証。	Citrix が管理する Azure Active Directory、またはアクティブディレクトリ/Azure Active Directory のいずれかを選択できます。
オンプレミスネットワークへの接続がありません。	選択肢: オンプレミスネットワーク、Azure VNet ピアリング、および SD-WAN への接続なし。
Citrix が準備した Windows 10 イメージを使用します。そのイメージには、現在のデスクトップ VDA が含まれています。	選択肢は次のとおりです。Citrix が準備したイメージ、Azure からインポートしたイメージ、または Citrix のプリペアドイメージまたはインポートしたイメージからサービスに構築したイメージ。
各デスクトップには、Azure 標準ディスク (HDD) ストレージがあります。	複数のストレージオプションを使用できます。
静的デスクトップのみ。	静的、ランダム、またはマルチセッションデスクトップ。
電源管理スケジュールは、作成時に設定できません。セッションが終了すると、デスクトップをホストしているマシンの電源がオフになります。この設定は後で変更できます。)	電源管理スケジュールは、作成中に構成できます。
Citrix Managed Azure サブスクリプションを使用する必要があります。	Citrix Managed Azure または独自の Azure サブスクリプションを使用できます。

詳しくは、次のページを参照してください:

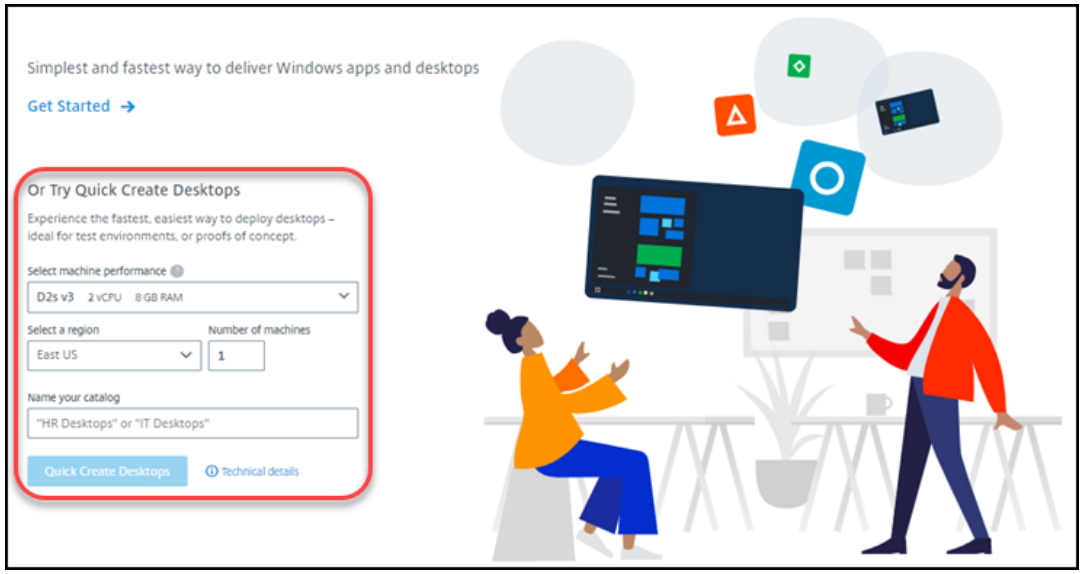
- 簡易作成を使用してカタログを作成します
- カスタム作成を使用してカタログを作成する

簡易作成を使用してカタログを作成します

このカタログ作成方法では、常に Citrix Managed Azure サブスクリプションが使用されます。

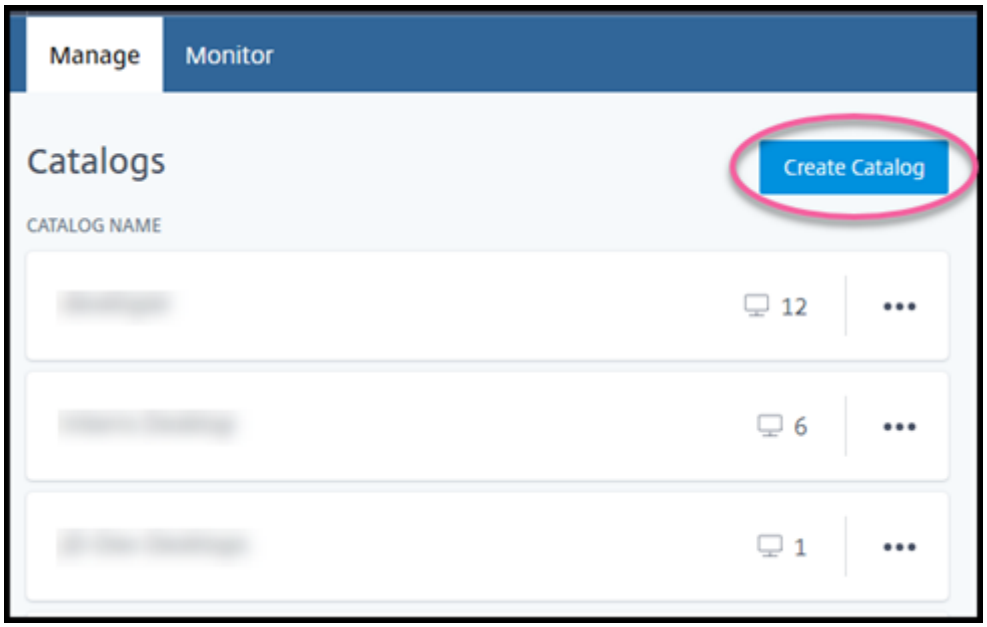
1. Citrix Cloudにサインインします。
2. 左上のメニューで、[マイサービス] **> [Virtual Apps and Desktops** 標準] の順に選択します。
3. カタログがまだ作成されていない場合は、[ようこそ] ページに移動します。次のいずれかを選択します。

- このページでカタログを構成します。手順 6 ～10 に進みます。

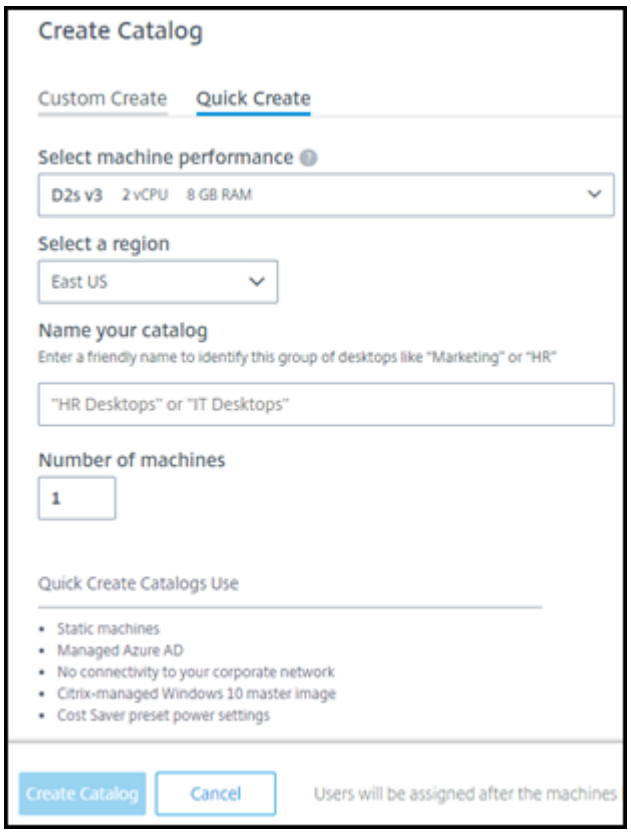


- [開始] をクリックします。管理ダッシュボードに移動します。［カタログの作成］をクリックします。

4. カタログがすでに作成されている (別のカタログを作成している場合)、[管理] ダッシュボードに移動します。［カタログの作成］をクリックします。



5. ページの上部にある [クイック作成] (Quick Create) をクリックします (まだ選択されていない場合)。



- マシンのパフォーマンス**:** マシンタイプを選択します。各選択肢には、CPU、RAM、およびストレージのユニークな組み合わせがあります。高性能マシンの場合、月額コストが高くなります。
- リージョン**:** マシンを作成するリージョンを選択します。ユーザーに近いリージョンを選択できます。
- 名前**:** カタログの名前を入力します。このフィールドは必須で、デフォルト値はありません。
- マシン数**:** 必要なマシンの数を入力します。

6. 完了したら、[カタログを作成] をクリックします。[ようこそ] ページから最初のカタログを作成する場合は、[デスクトップのクイック作成] をクリックします。)

管理ダッシュボードに自動的に表示されます。カタログの作成中に、カタログの名前がカタログのリストに追加され、作成の進行状況が示されます。

また、このサービスはリソースの場所を自動的に作成し、2 つの Cloud Connector を追加します。

次の手順:

- Citrix Managed Azure AD をユーザー認証に使用している場合は、カタログの作成中にユーザーをディレクトリに追加することができます。
- どのユーザー認証方法を使用するかにかかわらず、カタログの作成後、ユーザーをカタログに追加します。

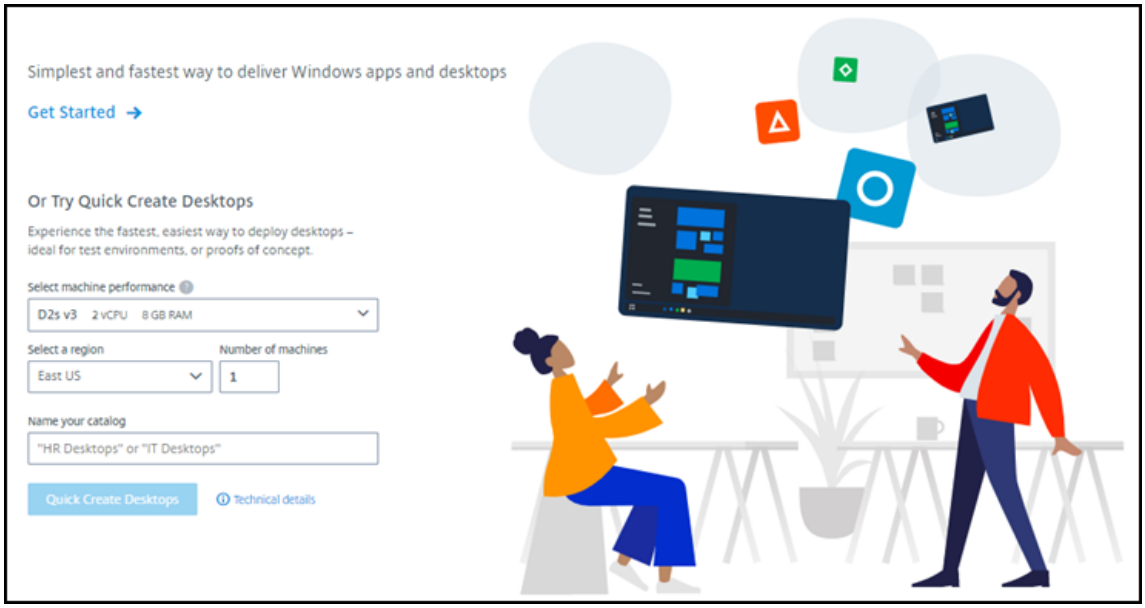
カスタム作成を使用してカタログを作成する

Citrix Managed Azure サブスクリプションを使用していて、カタログを作成する前に、オンプレミスのネットワークリソースへの接続を使用する予定の場合、そのネットワーク接続を作成します。ユーザーがオンプレミスリソースまたは他のネットワークリソースにアクセスできるようにするには、その場所の Active Directory 情報も必要です。

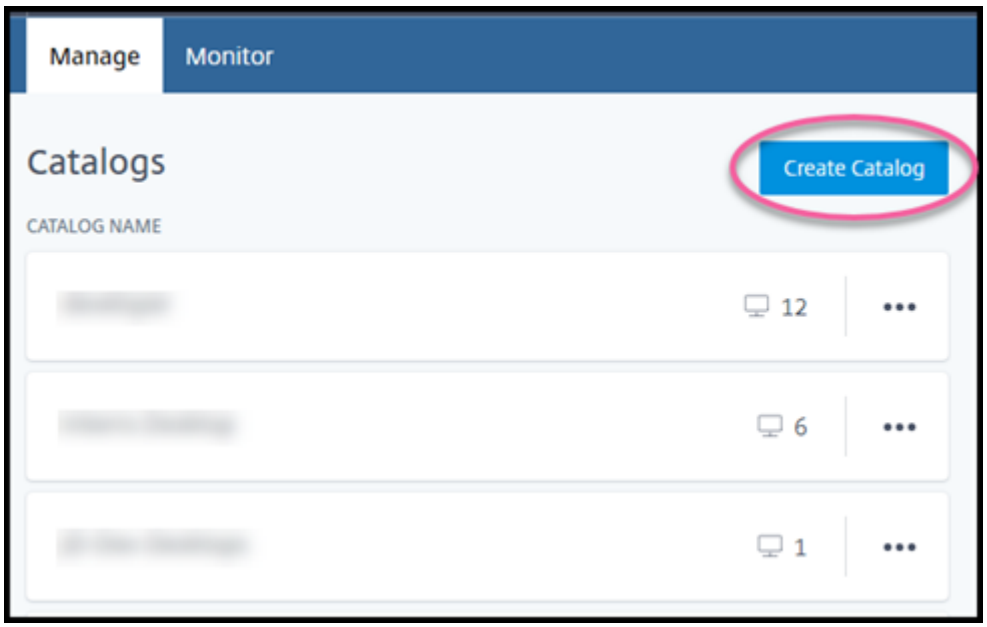
Citrix Managed Azure サブスクリプションがない場合は、カタログを作成する前に、サービスに自分の Azure サブスクリプションの少なくとも 1 つをインポート (追加)する必要があります。

カタログを作成するには、次の手順に従います。

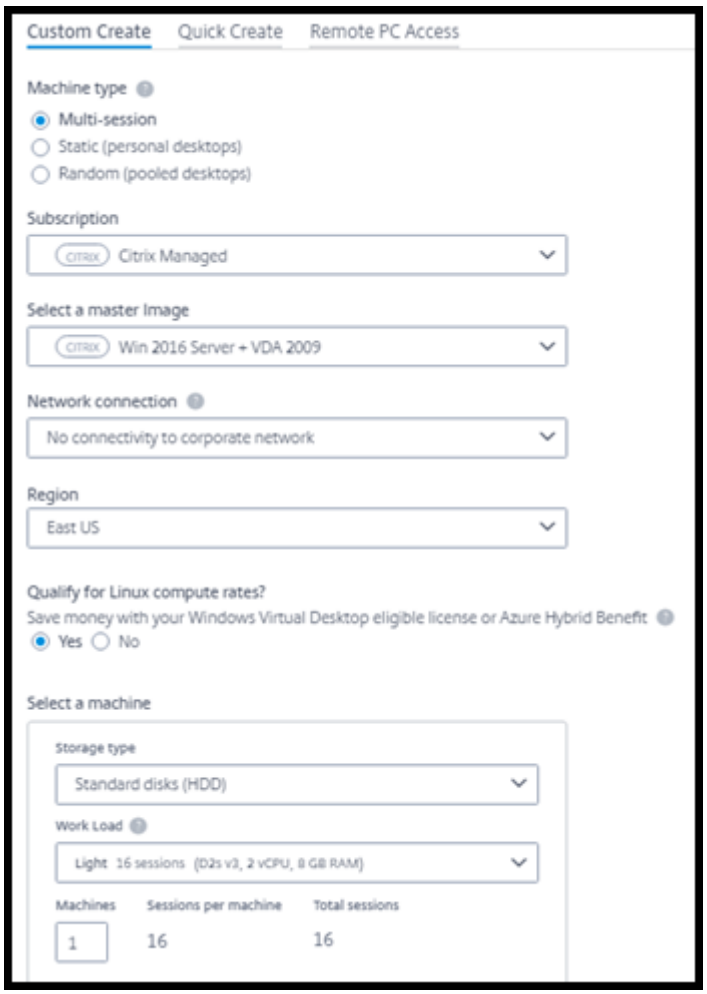
1. Citrix Cloudにサインインします。
2. 左上のメニューで、[マイサービス] **> [Virtual Apps and Desktops** 標準] の順に選択します。
3. カタログがまだ作成されていない場合は、[ようこそ] ページに移動します。[開始] をクリックします。イントロダクションページの最後に、[管理] ダッシュボードに移動します。[カタログの作成] をクリックします。



カタログがすでに作成されている場合は、[管理] ダッシュボードに移動します。[カタログの作成] をクリックします。



4. ページの上部にある [カスタム作成] (Custom Create) が選択されていない場合は、[カスタム作成] を選択します。



5. 次のフィールドに入力します。(一部のフィールドは、特定のマシンタイプでのみ有効です。フィールドの順序は異なる場合があります。)

   - マシンの種類。マシンタイプを選択します。詳しくは、「マシンの種類」を参照してください。
   - サブスクリプション。Azure サブスクリプションを選択します。詳しくは、「Azure サブスクリプション」を参照してください。
   - マスターイメージ**:** オペレーティングシステムイメージを選択します。詳しくは、「画像」を参照してください。
   - ネットワーク接続**:** ネットワーク内のリソースへのアクセスに使用する接続を選択します。詳しくは、「ネットワーク接続」を参照してください。

     Citrix Managed Azure サブスクリプションの場合、次の選択肢があります。

     - 接続なし：ユーザーはオンプレミスの企業ネットワーク上の場所やリソースにアクセスできません。
     - 接続： VNet ピアリングや SD-WAN 接続などの接続を選択します。

     顧客管理の Azure サブスクリプションの場合、適切なリソースグループ、仮想ネットワーク、サブネットを選択します。
   - [リージョン**]:** ([****** ネットワーク接続**]** で **[**接続なし ******] を選択した場合にのみ使用可能) デスクトップを作成するリージョンを選択します。ユーザーに近いリージョンを選択できます。

     [ネットワーク接続] で接続名を選択した場合、カタログはそのネットワークのリージョンを使用します。
   - **Linux** コンピューティングレートの対象になりますか (Windows イメージを選択した場合にのみ使用できます)。対象となるライセンスまたは Azure ハイブリッド特典を使用すると、コストを節約できます。

     Azure 仮想デスクトップの特典**:** 対象の Windows 10 または Windows 7 ユーザーライセンスについて:

     - Microsoft 365 E3/ES
     - Microsoft 365 A3/AS/Student Use Benefits
     - Microsoft 365 F3
     - Microsoft 365 Business Premium
     - Windows 10 Enterprise E3/E5
     - Windows 10 Education A3/A5
     - Windows 10 VDA per user

     Windows Server ワークロードのソフトウェアアシュアランスを搭載した RDS CAL のユーザーまたはデバイスライセンスごと。

     Azure ハイブリッドの利点**:** アクティブなソフトウェアアシュアランス、または同等の適格なサブスクリプションライセンスを持つ Windows Server ライセンス。https://azure.microsoft.com/en-us/pricing/hybrid-benefit/を参照してください。

- マシン**:**
  - ストレージタイプ。HDD か SSD か
  - マシンのパフォーマンス（****** 静的またはランダムマシンタイプの場合 ** ）、またはワークロード（マルチセッションマシンタイプの場合）。選択肢には、選択したイメージの生成タイプ (gen1 または gen2) に一致するオプションのみが含まれます。

    カスタム作業負荷を選択する場合は、[マシンパフォーマンス] フィールドにマシンあたりのマシンとセッション数を入力します。
  - マシン。このカタログに何台のマシンが必要ですか。
- マシンの命名スキーム**:**、マシンの命名スキームを参照してください。
- 名前**:** カタログの名前を入力します。この名前は [管理] ダッシュボードに表示されます。
- 電源スケジュール**:** デフォルトでは、[後でこれを構成します] チェックボックスがオンになっています。詳しくは、「電源管理スケジュール」を参照してください。
- ローカルの **Active Directory** ドメインに参加します。([ネットワーク接続] で Azure VNet ピア接続名を選択した場合にのみ使用できます)。[はい] または [いいえ] を選択します。「はい」を選択した場合は、次のように入力します。
  - ドメインの FQDN (例:Contoso.com)。
  - 組織単位: デフォルトの OU (コンピュータ) を使用するには、このフィールドを空のままにします。
  - サービスアカウント名: 名前 @domain または domain\ name の形式のドメイン管理者またはエンタープライズ管理者である必要があります。
  - サービスアカウント名のパスワード。
- 詳細設定**:**「カタログ作成時のリソースの場所設定」を参照してください。

6. 完了したら、[カタログを作成] をクリックします。

カタログの作成時期は、管理ダッシュボードに表示されます。また、このサービスはリソースの場所を自動的に作成し、2 つの Cloud Connector を追加します。

次の手順:

- まだ実行していない場合は、認証方法を構成することでユーザーが Citrix Workspace で認証できるようにします。
- カタログの作成後、ユーザーをカタログに追加します。
- マルチセッションカタログを作成した場合、アプリケーションを追加 （ユーザーを追加する前または後に）。

カタログ作成時のリソースの場所設定

カタログを作成するときに、オプションで複数のリソースの場所設定を構成できます。

カタログ作成ダイアログで [詳細設定] をクリックすると、サービスはリソースの場所情報を取得します。

- カタログ用に選択されたドメインおよびネットワーク接続のリソースの場所がすでにある場合は、作成中のカタログで使用するために保存できます。

  そのリソースの場所に Cloud Connector が 1 つしかない場合は、別のクラウドコネクタが自動的にインストールされます。追加する Cloud Connector の詳細設定を指定することもできます。

- カタログ用に選択されたドメインおよびネットワーク接続にリソースの場所が設定されていない場合は、リソースの場所を構成するように求められます。

詳細設定を構成します。

- (リソースの場所がすでに設定されている場合にのみ必要です)。リソースの場所の名前。
- 外部接続タイプ：Citrix Gateway サービス経由または社内ネットワーク内からの接続タイプ。
- Cloud Connector の設定:
  - (顧客管理の Azure サブスクリプションを使用している場合にのみ使用可能) マシンのパフォーマンス。この選択は、リソースの場所の Cloud Connector に使用されます。
  - (顧客管理の Azure サブスクリプションを使用している場合にのみ使用可能) Azure リソースグループ。この選択は、リソースの場所の Cloud Connector に使用されます。デフォルトは、リソースの場所で最後に使用されたリソースグループです (該当する場合)。
  - 組織単位 (OU) デフォルトは、リソースの場所で最後に使用された OU です (該当する場合)。

詳細設定が完了したら、[保存] をクリックして、カタログ作成ダイアログに戻ります。

カタログを作成した後、いくつかのリソースロケーションアクションが使用可能になります。詳しくは、「リソースの場所の操作」を参照してください。

マシンの命名スキーム

カタログの作成時にマシン命名規則を指定するには、[マシン命名スキームの指定] を選択します。1〜4 個のワイルドカード（ハッシュマーク）を使用して、名前の連続した数字または文字が表示される場所を示します。規則

- 命名規則には、少なくとも 1 つのワイルドカードを含める必要があります。ただし、4 つ以上のワイルドカードを含めることはできません。すべてのワイルドカードは、一緒にする必要があります。
- ワイルドカードを含む名前全体は、2 〜15 文字にする必要があります。
- 名前には、空白（スペース)、スラッシュ、バックスラッシュ、コロン、アスタリスク、山括弧、パイプ、カンマ、チルダ、感嘆符、アットマーク、ドル記号、パーセント記号、キャレット、括弧、またはアンダースコアを含めることはできません。
- 名前の先頭をピリオドで始めることはできません。
- 名前には数字だけを含めることはできません。
- 名前の末尾に次の文字を使用しないでください。`-GATEWAY`、`-GW`、`-TAC`。

連続する値が数字 (0-9) と文字 (A-Z) のどちらであるかを示します。

たとえば、`PC-Sales-####` (**0-9** が選択されている) という命名スキームは、`PC-Sales-01`、`PC-Sales-02`、`PC-Sales-03`などの名前のコンピュータアカウントになります。

成長のための十分な余地を残してください。

- たとえば、2 つのワイルドカードと 13 文字 (MachineSales-####など) の命名規則では、最大文字数 (15) が使用されます。
- カタログに 99 台のマシンが含まれると、次のマシンの作成は失敗します。サービスは 3 桁 (100) のマシンを作成しようとしますが、16 文字の名前が作成されます。最大値は 15 です。
- したがって、この例では、短い名前（PC-Sales-####など）を使用すると、99 台のマシンを超えてスケーリングできます。

マシン命名スキームを指定しない場合、サービスはデフォルトの命名スキームを使用します DAS %%%%%-**-######。

- %%%%% = リソースの場所のプレフィックスに一致する 5 つのランダムな英数字
- ** = カタログの英数字 2 文字
- ###### = 3 桁です。

関連情報

- ドメインに参加しているマシンとドメインに参加していないマシン。
- リモート PC アクセスカタログ。
- プロキシサーバーを使用するネットワーク内にカタログを作成する。
- カタログ情報を表示する。

リモート **PC** アクセス

July 16, 2021

はじめに

Citrix リモート PC アクセスを使用すると、ユーザーはオフィスにある物理 Windows または Linux マシンをリモートで使用できます。ユーザーは、Citrix HDX を使用して社内 PC セッションを提供することで、最高のユーザーエクスペリエンスを実現できます。

リモート PC アクセスは、ドメインに参加しているマシンをサポートします。

仮想デスクトップおよびアプリケーションの配信との違い

仮想デスクトップとアプリケーションの提供に慣れている場合は、リモート PC アクセス機能にはいくつかの違いがあります。

- リモート PC アクセスカタログには、通常、既存の物理マシンが含まれています。したがって、リモート PC アクセスを使用するために、イメージを準備したり、マシンをプロビジョニングしたりする必要はありません。デスクトップとアプリケーションの配信は、通常、仮想マシン (VM) を使用し、イメージは VM をプロビジョニングするためのテンプレートとして使用されます。
- リモート PC アクセスのランダムプールカタログ内のマシンの電源がオフになると、イメージの元の状態にリセットされません。
- リモート PC アクセスの静的ユーザー割り当てカタログでは、ユーザーがログインした後（マシンまたは RDP を介して）割り当てが実行されます。デスクトップおよびアプリを配信する場合、マシンが使用可能であればユーザーに割り当てられます。

インストールと構成の概要

タスクを開始する前に、このセクションを確認してください。

1. 以下の点に注意してください：
   a)「要件と考慮事項」を確認してください。
   b) 準備タスクを完了します。
2. Citrix Cloud から：
   a) Citrix Cloud アカウントを設定し、Citrix Virtual Apps and Desktops Standard for Azure サービスを購読する。
   b) Active Directory リソースにアクセスできるリソースの場所を設定します。リソースの場所に少なくとも 2 つの Cloud Connector をインストールします。Cloud Connector は Citrix Cloud と通信します。

      リソースの場所を作成し、その場所に Cloud Connector をインストールするのガイダンスに従ってください。この情報には、システム要件、準備、および手順が含まれます。
   c) Active Directory を Citrix Cloud に接続する。
3. ユーザーがリモートでアクセスする各マシンでCitrix Virtual Delivery Agent（VDA）をインストールする。VDA は、リソースの場所にある Cloud Connector を介して Citrix Cloud と通信します。
4. Citrix Virtual Apps and Desktops Standard for Azure から：
   a) リモート PC アクセスカタログを作成する。この手順では、リソースの場所を指定し、ユーザー割り当て方法を選択します。
   b) カタログに登録者 (ユーザー) を追加する、必要であれば。カタログが静的自動割り当てまたはランダムプールされたユーザー割り当て方法のいずれかを使用している場合は、カタログにユーザーを追加します。静的事前割り当て済みカタログにユーザーを追加する必要はありません。
5. Workspace の URL をユーザーに送信。ワークスペースから、ユーザーはオフィス内のマシンにログオンできます。

要件および考慮事項

このセクションのマシンへの参照は、ユーザーがリモートでアクセスするマシンを指します。

全般:

- マシンは、シングルセッションの Windows 10 または Linux（Red Hat Enterprise Linux および Ubuntu）オペレーティングシステムを実行している必要があります。
- マシンは Active Directory ドメインサービスドメインに参加している必要があります。
- Citrix Virtual Apps およびデスクトップでのリモート PC アクセスの使用に慣れている場合、このサービスでは Wake-on-LAN 機能を使用できません。

ネットワーク:

- マシンにはアクティブなネットワーク接続が必要です。信頼性と帯域幅を高めるには、有線接続をお勧めします。
- Wi-Fi を使用している場合:
  - 電源設定でワイヤレスアダプターの電源を入れたままにするようにします。
  - ユーザーがサインインする前にワイヤレスネットワークに自動的に接続できるように、ワイヤレスアダプターとネットワークプロファイルを構成します。そうしないと、ユーザーがログオンするまで VDA は登録されません。ユーザーがログオンするまで、マシンはリモートアクセスに使用できません。
  - Wi-Fi ネットワークから Cloud Connector に到達できることを確認します。

デバイスと周辺機器:

- 次のデバイスはサポートされていません。
  - KVM スイッチ、またはセッションを切断する可能性のあるそのほかのコンポーネント。
  - ハイブリッド PC（オールインワンおよび NVIDIA Optimus ノートブックおよび PC を含む）。
- キーボードとマウスを直接本製品に接続します。電源を切ったり接続を切断したりできるモニターなどのコンポーネントに接続すると、これらの周辺機器が使用できなくなることがあります。キーボードやマウスをモニターなどのデバイス経由で接続する必要がある場合は、それらのコンポーネントの電源をオフにしないでください。
- ラップトップおよび Surface Pro デバイスの場合：ラップトップがバッテリで動作するのではなく、電源に接続されていることを確認します。ラップトップの電源オプションを、デスクトップマシンのオプションに合わせて構成します。次に例を示します:
  - 休止機能を無効にする。
  - スリープ機能を無効にする。
  - カバーを閉じた場合の動作を ［何もしない］ に設定する。
  - [電源ボタンを押す] アクションを [シャットダウン] に設定します。
  - ビデオカードおよび NIC の省電力設定を無効にする。

  ドッキングステーションを使用する場合は、ラップトップをドッキング解除して再ドッキングできます。ラップトップをアンドックすると、VDA は Wi-Fi 経由で Cloud Connector に再登録されます。ただし、ラップ

トップを再ドッキングすると、ワイヤレスアダプタを取り外さない限り、VDA は有線接続を使用するように切り替えません。有線接続が確立されると、組み込まれた機能がワイヤレスアダプターを切断するデバイスもあります。その他のデバイスでは、ワイヤレスアダプタを取り外すには、カスタムソリューションまたはサードパーティ製のユーティリティが必要です。前述の Wi-Fi に関する考慮事項を確認してください。

リモート PC アクセスデバイスのドッキングとドッキング解除を有効にするには、次の手順を実行します。

- [スタート] **>** [設定] **>** [システム] **>** [電源とスリープ] で、[スリープ] を [しない
- [デバイスマネージャ] **>** [ネットワークアダプタ] **>** [イーサネットアダプタ] で、[電源管理] に移動し、[コンピュータの電源を切って電力を節約できるようにする] をオフにします。[このデバイスでコンピュータのスリープ解除を許可する] が選択されていることを確認します。

Linux VDA:

- Linux VDA は、非 3D モードの物理マシンでのみ使用します。NVIDIA のドライバーの制限により、HDX 3D モードが有効になっている場合、PC のローカル画面はブラックアウトせず、画面にはセッションのアクティビティが表示されます。この画面の表示は、セキュリティ上のリスクです。
- Linux マシンを使用するカタログでは、静的事前割り当てのユーザー割り当て方法を使用する必要があります。Linux マシンのカタログでは、静的な自動割り当てまたはランダムプールされた割り当てメソッドは使用できません。

ワークスペースに関する考慮事項:

- 同じ社内 PC にアクセスする複数のユーザーには、Citrix Workspace で同じアイコンが表示されます。ユーザーが Citrix Workspace にサインインすると、そのマシンが別のユーザーによってすでに使用されている場合、そのマシンは使用不可と表示されます。

準備

- マシンに VDA をインストールする方法を決定します。いくつかの方法を使用できます。
  - 各マシンに VDA を手動でインストールします。
  - グループポリシー、スクリプトを使うを使用して VDA インストールをプッシュします。
  - Microsoft システムセンター構成マネージャ（SCCM）などの電子ソフトウェア配布（ESD）ツールを使用して、VDA のインストールをプッシュします。詳しくは、「SCCM を使用した VDA のインストール」を参照してください。
- ユーザー割り当てメソッドについて参照し、を使用する方法を決定してください。リモート PC アクセスカタログを作成するときに、この方法を指定します。
- マシン（実際にはマシンにインストールする VDA）が Citrix Cloud に登録する方法を決定します。Citrix Cloud でセッションブローカーとの通信を確立するには、VDA を登録する必要があります。

  VDA は、リソースの場所にある Cloud Connector を介して登録します。VDA をインストールするとき、または後で Cloud Connector アドレスを指定できます。

VDA の最初の（初期）登録では、ポリシーベースの GPO または LGPO をお勧めします。初回登録後、自動更新 Citrix。自動更新はデフォルトで有効になっています。VDA 登録の詳細。

VDA をインストールする

ユーザーがリモートでアクセスする各物理マシンに VDA をダウンロードしてインストールします。

VDA をダウンロードする

- Windows VDA をダウンロードするには:
  1. Citrix Cloud アカウントの認証情報を使用して、Citrix Virtual Apps and Desktops サービスダウンロードページを参照します。
  2. 最新の VDA をダウンロードします。インストールパッケージには 2 種類あります。。VDA タイトルの年と月の値は異なります。
- リモート PC アクセス用の Linux VDA をダウンロードするには、Linux VDA に関するドキュメントのガイダンスに従ってください。

Windows VDA インストールパッケージの種類

Citrix ダウンロードサイトには、リモート PC アクセスマシンで使用できる 2 つの Windows VDA インストールパッケージタイプが用意されています。

- シングルセッションコア VDA インストーラ(リリースは **yymm**):`VDAWorkstationCoreSetup_release.exe`

  シングルセッションコア VDA インストーラは、リモート PC アクセス専用にカスタマイズされています。軽量で、ネットワーク経由ですべてのマシンに（他の VDA インストーラよりも）簡単に展開できます。Citrix Profile Management、マシンアイデンティティサービス、ユーザーパーソナライズ層など、これらの展開では通常必要ないコンポーネントは含まれません。

  ただし、Citrix Profile Management がインストールされていない場合、パフォーマンス向け Citrix Analytics のディスプレイおよび一部のモニターの詳細は表示されません。これらの制限の詳細については、ブログ記事リモート PC アクセスマシンの監視とトラブルシューティングを参照してください。

  完全な分析と監視の表示が必要な場合は、シングルセッションフル VDA インストーラーを使用します。

- シングルセッションフル VDA インストーラ（リリースは **yymm**）: `VDAWorkstationSetup_release.exe`

  シングルセッションフル VDA インストーラは、シングルセッションコア VDA インストーラよりも大きなパッケージですが、必要なコンポーネントのみをインストールするようにカスタマイズできます。たとえば、Profile Management をサポートするコンポーネントをインストールできます。

リモート **PC** アクセス用の **Windows VDA** を対話形式でインストールする

1. ダウンロードした VDA インストールファイルをダブルクリックします。
2. [環境] ページで、[リモート **PC** アクセスを有効にする] を選択し、[次へ] をクリックします。
3. [**Delivery Controller**] ページで、次のいずれかを選択します。
   - Cloud Connectors のアドレスがわかっている場合は、[手動で行う] を選択します。Cloud Connector の FQDN を入力し、[追加] をクリックします。リソースの場所にある他の Cloud Connector についても同じ手順を繰り返します。
   - AD 構造で Cloud Connector をインストールした場所がわかっている場合は、[**Active Directory** から場所を選択] を選択し、その場所に移動します。他の Cloud Connector についても同じ手順を繰り返します。
   - Citrix グループポリシーで Cloud Connector アドレスを指定する場合は、[後で実行する（詳細設定）] を選択し、プロンプトが表示されたら、その選択を確認します。

   完了したら、[次へ] をクリックします。
4. シングルセッションフル VDA インストーラーを使用している場合は、[追加コンポーネント] ページで、Profile Management など、インストールするコンポーネントを選択します。（このページは、シングルセッションコア VDA インストーラを使用している場合は表示されません）。
5. [機能] ページで、[次へ] をクリックします。
6. [ファイアウォール] ページで、[自動] を選択します (まだ表示されていない場合)。[次へ] をクリックします。
7. [概要] ページで [インストール] をクリックします。
8. [診断] ページで、[接続] をクリックします。チェックボックスがオンになっていることを確認します。求められたら、Citrix アカウント資格情報を入力します。認証情報が検証されたら、[次へ] をクリックします。
9. [完了] ページで、[完了] をクリックします。

インストールの詳細については、VDA のインストールを参照してください。

コマンドラインを使用してリモート **PC** アクセス用の **Windows VDA** をインストールする

- シングルセッションコア VDA インストーラーを使用している場合は、`VDAWorkstationCoreSetup.exe`を実行し、`/quiet`、`/enable_hdx_ports`および`/enable_hdx_udp_ports`オプションを含めます。Cloud Connector アドレスを指定するには、`/controllers` オプションを使用します。

  たとえば、次のコマンドは、シングルセッションコア VDA をインストールします。Citrix Workspace アプリとその他の非コアサービスはインストールされません。2 つの Cloud Connector の FQDN が指定され、Windows ファイアウォールサービスのポートが自動的に開きます。管理者が再起動を処理します。

  ```
  VDAWorkstationCoreSetup .exe /quiet /controllers "Connector-East.domain
  .com" "Connector-East2.domain.com"  /enable_hdx_ports /noreboot
  ```


- シングルセッションフル VDA インストーラを使用し、Profile Management（またはその他のオプションの追加コンポーネント）を含める場合：VDAWorkstationSetup.exeを実行し、/remotepcおよび/includeadditionalオプションを含めます。この/remotepcオプションを使用すると、ほとんどの追加コンポーネントのインストールが防止されます。この/includeadditionalオプションは、インストールする追加コンポーネントを正確に指定します。

  たとえば、次のコマンドは、Profile Management を除くすべてのオプションの追加コンポーネントをインストールできないようにします。

  ```
  VDAWorkstationSetup.exe /quiet /remotepc /includeadditional "Citrix User Profile Manager","Citrix User Profile Manager WMI Plugin" /controllers "connector.domain.com" "connector2.domain.com" /enable_hdx_ports /noresume /noreboot
  ```

詳しくは、「VDA のインストールで使用するコマンドラインオプション」を参照してください。

Linux VDA をインストールする

Linux VDA を対話的にインストールするか、コマンドラインを使用する場合Linux ドキュメントのガイダンスに従ってください。

リモート PC アクセスカタログを作成する

カタログを正常に作成するには、少なくとも 2 つの Cloud Connector を含むリソースの場所が存在する必要があります。

> 重要：
>
> マシンは、一度に 1 つのカタログにしか属せません。カタログに追加するマシンを指定する場合、この制限は適用されません。ただし、制限を無視すると、後で問題が発生する可能性があります。

1. Citrix Cloudにサインインします。
2. 左上のメニューで、[マイサービス] **> [Azure** の **Virtual Apps and Desktops**] の順に選択します。
3. まだカタログを作成していない場合は、[ようこそ] ページの [はじめに] をクリックします。カタログを作成した場合は、[管理] ダッシュボードの [カタログの作成] をクリックします。
4. [リモート **PC** アクセス] タブで、ユーザーをマシンに割り当てる方法を選択。
5. カタログの名前を入力し、作成したリソースの場所を選択します。
6. マシンの追加。
7. [カタログの作成] をクリックします。
8. [リモート **PC** アクセスカタログの作成中] ページで、[完了] をクリックします。

9. 新しいカタログのエントリが [管理] ダッシュボードに表示されます。

   カタログが正常に作成されたら、利用者（ユーザー）をカタログに追加するへのリンクの 1 つをクリックします。この手順は、カタログが静的自動割り当てまたはランダムプール未割り当てのユーザー割り当て方法を使用する場合に適用されます。

カタログを作成し、必要に応じて、ユーザを追加した後、ユーザーにワークスペース URL を送信する。

ユーザー割り当て方法

カタログの作成時に選択するユーザー割り当て方法は、ユーザーがマシンに割り当てられる方法を示します。

- 静的自動割り当て：ユーザー割り当ては、マシンに VDA をインストールした後、ユーザーがマシン（対面や RDP など Citrix を使用していない）にログオンしたときに実行されます。後で他のユーザーが（Citrix を使用していない）そのマシンにログオンすると、そのユーザーも割り当てられます。一度に 1 人のユーザーしかマシンを使用できません。これは、コンピュータを共有するオフィスワーカーまたはシフトワーカーの一般的な設定です。

  この方法は、Windows マシンでサポートされています。Linux マシンでは使用できません。

- 静的事前割り当て**:** ユーザーはマシンに事前割り当てられます。（これは通常、マシンとユーザーのマッピングを含む CSV ファイルをアップロードして設定します）。VDA のインストール後に割り当てを確立するためにユーザーログオンは必要ありません。また、カタログの作成後にユーザをカタログに割り当てる必要もありません。これはオフィスワーカーに最適です。

  このメソッドは Windows および Linux マシンでサポートされています。

- ランダムプール未割り当て**:** ユーザーは使用可能なマシンにランダムに割り当てられます。一度に 1 人のユーザーしかマシンを使用できません。これは、学校のコンピューティングラボに最適です。

  この方法は、Windows マシンでサポートされています。Linux マシンでは使用できません。

マシンをカタログに追加する方法

注意：各マシンには VDA がインストールされている必要があります。

カタログを作成または編集するときに、マシンをカタログに追加するには、次の 3 つの方法があります。

- マシンアカウントを 1 つずつ選択する。
- OU を選択。
- CSV ファイルを使用して一括追加する。CSV ファイルに使用できるテンプレートを使用できます。

マシン名を追加する

このメソッドは、マシンアカウントを 1 つずつ追加します。

1. ドメインを選択します。

2. マシンアカウントを検索します。
3. [追加] をクリックします。
4. この手順を繰り返して、さらにマシンを追加します。
5. マシンの追加が完了したら、[完了] をクリックします。

OU を追加

この方法では、マシンアカウントが常駐する組織単位に従ってマシンアカウントを追加します。
OU を選択するときは、より細かい精度を得るために、下位レベルの OU を選択します。その粒度が必要ない場合は、上位レベルの OU を選択できます。

たとえば、`Bank`/`Officers`/`Tellers`の場合は、粒度を上げるには`Tellers`を選択します。それ以外の場合は、要件に基づいて`Officers`または`Bank`を選択できます。

リモート PC アクセスカタログに割り当てた後に OU を移動または削除すると、VDA の関連付けに影響し、今後の割り当てで問題が発生します。AD 変更プランでカタログの OU 割り当ての更新が反映されていることを確認します。

OU を追加するには、次の手順を実行します。

1. ドメインを選択します。
2. 追加するマシンアカウントを含む OU を選択します。
3. チェックボックスで、選択内容に含まれるサブフォルダを含めるかどうかを指定します。
4. OU の選択が完了したら、[完了] をクリックします。

一括で追加する

1. [**CSV** テンプレートのダウンロード] をクリックします。
2. テンプレートで、マシンアカウント情報 (最大 100 エントリ) を追加します。CSV ファイルには、各マシンに割り当てられたユーザーの名前を含めることもできます。
3. ファイルを保存します。
4. ファイルを [一括でマシンを追加] ページにドラッグするか、ファイルを参照します。
5. ファイルの内容のプレビューが表示されます。目的のファイルではない場合は、別のファイルを作成し、ドラッグまたはブラウズすることができます。
6. 完了したら、[完了] をクリックします。

リモート **PC** アクセスカタログを管理する

リモート PC アクセスカタログの構成情報を表示または変更するには、管理ダッシュボードからカタログを選択します (エントリの任意の場所をクリックします)。

- [詳細] タブでは、マシンを追加または削除できます。
- [サブスクライバ] タブでは、ユーザーを追加または削除できます。

- [マシン] タブでは、次の操作を実行できます。
  - マシンの追加と削除: **[**マシンの追加と削除] ボタン。
  - ユーザー割り当ての変更: 割り当てのゴミ箱のアイコンを削除する、省略記号メニューでマシン割り当てを編集する。
  - どのマシンが登録されているかを確認し、マシンをメンテナンスモードまたはメンテナンスモードから外します。

Azure サブスクリプション

July 16, 2021

はじめに

Citrix Virtual Apps and Desktops Standard for Azure は、Citrix Managed Azure サブスクリプションと独自の顧客管理 Azure サブスクリプションの両方をサポートします。

- 独自の Azure サブスクリプションを使用するには、まずそれらのサブスクリプションを 1 つまたは複数サービスにインポート (追加) します。この操作により、サービスが Azure サブスクリプションにアクセスできるようになります。
- Citrix Managed Azure サブスクリプションを使用するには、サブスクリプション構成は必要ありません。ただし、Citrix Managed Azure サブスクリプションを利用できるようにするには、Citrix Azure 消費基金（Citrix Virtual Apps and Desktops Standard for Azure に加えて）を注文している必要があります。

カタログを作成するとき、またはイメージをビルドするときに、利用可能な Azure サブスクリプションの中から選択します。

一部のサービス機能は、マシンが Citrix Managed Azure サブスクリプションであるか、または独自の Azure サブスクリプションにあるかによって異なります。

Citrix 管理対象 Azure	独自の Azure サブスクリプション
ドメインに参加しているマシンまたはドメインに参加していないマシンをサポートします。	ドメインに参加しているマシンのみをサポートします。
クイック作成およびカスタム作成カタログをサポートします。	カスタム作成カタログのみをサポートします。
カタログおよびイメージの作成時に、常に使用可能 (デフォルトのサブスクリプション選択)。	カタログを作成する前に、Azure サブスクリプションをサービスに追加する必要があります。
ユーザー認証では、Citrix 管理対象 Azure Active Directory または独自の Active Directory をサポートしています。	独自のアクティブディレクトリと Azure Active Directory を接続できます。

Citrix 管理対象 Azure	独自の Azure サブスクリプション
ネットワーク接続オプションには、[接続なし] が含まれます。	ネットワーク接続オプションには、独自の仮想ネットワークのみが含まれます。
Azure VNet ピアリングを使用してリソースに接続する場合は、サービスで VNet ピア接続を作成する必要があります。	既存の仮想ネットワークを選択します。
Azure からイメージをインポートするときは、イメージの URI を指定します。	イメージをインポートするときは、Azure サブスクリプションで VHD を選択するか、ストレージを参照できます。
お客様の Azure サブスクリプションで踏み台マシンを作成して、マシンのトラブルシューティングを行うことができます。	サブスクリプション内のマシンにすでにアクセスできるため、踏み台マシンを作成する必要はありません。

サブスクリプションの表示

サブスクリプションの詳細を表示するには、サービスの [管理] ダッシュボードから、右側の [クラウドサブスクリプション] を展開します。次に、サブスクリプションのエントリをクリックします。

- 詳細ページには、マシンの数に加えて、サブスクリプション内のカタログとイメージの数と名前が表示されます。
- [リソースの場所] ページには、サブスクリプションが使用されているリソースの場所が一覧表示されます。

顧客管理の **Azure** サブスクリプションを追加する

カスタマー管理 Azure サブスクリプションを使用するには、そのサブスクリプションを使用するカタログまたはイメージを作成する前に、Citrix Virtual Apps and Desktops Standard for Azure に追加する必要があります。Azure サブスクリプションを追加する場合は、次の 2 つのオプションがあります。

- ディレクトリのグローバル管理者で、サブスクリプションのコントリビューター権限を持っている場合**:** Azure アカウントに対して認証するだけです。
- グローバル管理者ではなく、サブスクリプションのコントリビューター権限を持っている場合**:** サブスクリプションをサービスに追加する前に、Azure Azure AD で Azure アプリを作成し、そのアプリをサブスクリプションのコントリビューターとして追加します。そのサブスクリプションをサービスに追加すると、関連するアプリ情報が提供されます。

グローバル管理者の場合は、カスタマー管理の **Azure** サブスクリプションを追加する

このタスクには、ディレクトリに対するグローバル管理者権限と、サブスクリプションに対するコントリビュータ権限が必要です。

1. サービスの ［管理］ダッシュボードで、右側の ［サブスクリプション］ を展開します。
2. [**Azure** サブスクリプションの追加］ をクリックします。
3. [サブスクリプションの追加] ページで、[**Azure** サブスクリプションの追加] をクリックします。
4. ユーザーに代わって、サービスが Azure サブスクリプションにアクセスできるようにするボタンを選択します。
5. **[Azure** アカウントの認証**]** をクリックします。Azure サインインページに移動します。
6. Azure 認証情報を入力します。
7. 自動的にサービスに戻ります。**[**サブスクリプションの追加**]** ページには、検出された Azure サブスクリプションが一覧表示されます。必要に応じて、検索ボックスを使用してリストをフィルタリングします。1 つ以上のサブスクリプションを選択します。完了したら、[サブスクリプションの追加] をクリックします。
8. 選択したサブスクリプションを追加することを確認します。

[サブスクリプション] を展開すると、選択した Azure サブスクリプションが一覧表示されます。追加したサブスクリプションは、カタログまたはイメージの作成時に選択できます。

グローバル管理者でない場合に、顧客管理の **Azure** サブスクリプションを追加する

グローバル管理者でない場合の Azure サブスクリプションの追加は、次の 2 つの部分からなるプロセスです。

- サービスにサブスクリプションを追加する前に、Azure AD でアプリを作成し、そのアプリをサブスクリプションのコントリビューターとして追加します。。
- サブスクリプションをサービスに追加、Azure で作成したアプリに関する情報を使用します。

Azure AD でアプリを作成し、コントリビューターとして追加する

1. Azure AD に新しいアプリケーションを登録します。
   a) ブラウザから、https://portal.azure.comに移動します。
   b) 左上のメニューで、[**Azure Active Directory**] を選択します。
   c) [管理] リストで、[アプリの登録] をクリックします。
   d) [**+** 新規登録] をクリックします。
   e) [アプリケーションの登録] ページで、次の情報を入力します。
      - 名前**:** 接続名を入力します。
      - アプリケーションの種類**:Web** アプリケーション**/ API** を選択します。
      - リダイレクト **URI:** 空白のまま
   f) ［作成］ をクリックします。
2. アプリケーションのシークレットアクセスキーを作成し、ロールの割り当てを追加します。
   a) 前の手順から、[アプリの登録] を選択して詳細を表示します。

b) アプリケーション **ID** とディレクトリ ID** を書き留めます。これは、後でサブスクリプションをサービスに追加するときに使用します。

c) [管理] で、[証明書とシークレット] を選択します。

d) [クライアントシークレット] ページで、[**+** 新しいクライアントシークレット] を選択します。

e) [クライアントシークレットの追加] ページで、説明を入力し、有効期限を選択します。次に、［追加］をクリックします。

f) クライアントの秘密の値を書き留めます。これは、後でサブスクリプションをサービスに追加するときに使用します。

g) サービスにリンク (追加) する Azure サブスクリプションを選択し、[アクセスコントロール **(IAM)**] をクリックします。

h) [役割の割り当ての追加] ボックスで、[追加] をクリックします。

i) [役割の割り当ての追加] タブで、次の項目を選択します。

- 役割**:** コントリビューター
- アクセス権を割り当てる**:** Azure AD ユーザー、グループ、またはサービスプリンシパル
- 選択**:** 前に作成した Azure アプリケーションの名前。

j)［保存］をクリックします。

サブスクリプションをサービスに追加する

Azure AD で作成したアプリケーションのアプリケーション ID、ディレクトリ ID、およびクライアントシークレットの値が必要になります。

1. サービスの ［管理］ダッシュボードで、右側の ［サブスクリプション］を展開します。
2. [**Azure** サブスクリプションの追加］をクリックします。
3. [サブスクリプションの追加] ページで、[**Azure** サブスクリプションの追加] をクリックします。
4. [サブスクリプションのコントリビューターロールを持つ **Azure** アプリケーションがある] を選択します。
5. Azure で作成したアプリケーションのテナント ID (ディレクトリ ID)、クライアント ID (アプリケーション ID)、およびクライアントシークレットを入力します。
6. [サブスクリプションを選択] をクリックし、目的のサブスクリプションを選択します。

後で、サービスダッシュボードのサブスクリプションの [詳細] ページから、省略記号メニューからクライアントシークレットを更新するか、Azure アプリを置き換えることができます。

サービスが追加された後に Azure サブスクリプションにアクセスできない場合、いくつかのカタログ電源管理および個々のマシンアクションは許可されません。メッセージには、サブスクリプションを再度追加するオプションが表示されます。サブスクリプションが Azure アプリを使用して最初に追加された場合は、Azure アプリを置き換えることができます。

Citrix 管理対象 **Azure** サブスクリプションを追加する

Citrix Managed Azure サブスクリプションは、制限に示されているマシンの数をサポートします。（ここでは、「マシン」は Citrix VDA がインストールされている仮想マシンを指します。これらのマシンは、アプリとデスクトップをユーザーに配信します。Cloud Connectors など、リソースの場所に他のマシンは含まれません。）

Citrix Managed Azure サブスクリプションがすぐに制限に達する可能性があり、十分な Citrix ライセンスがある場合は、別の Citrix Managed Azure サブスクリプションをリクエストできます。制限値に近づくと、ダッシュボードに通知が表示されます。

Citrix Managed Azure サブスクリプションを使用するすべてのカタログのマシンの総数が、制限に示されている値を超える場合は、カタログを作成（またはカタログにマシンを追加する）ことはできません。

たとえば、Citrix Managed Azure サブスクリプションあたり 1,000 台のマシンが仮想的に制限されているとします。

- 同じ Citrix Managed Azure サブスクリプションの 2 つのカタログ（`Cat1` および `Cat2`）があるとします。`Cat1`には現在 500 台のマシンが含まれており、`Cat2`には 250 台あります。
- 将来の容量ニーズに対応するために、200 台のマシンを`Cat2`に追加します。Citrix Managed Azure サブスクリプションでは、950 台のマシン（`Cat 1`で 500、`Cat 2`で 450）がサポートされるようになりました。ダッシュボードには、サブスクリプションが制限に近づいたことが示されます。
- さらに 75 台のマシンが必要な場合は、そのサブスクリプションを使用して 75 台のマシンでカタログを作成することはできません（または、既存のカタログに 75 台のマシンを追加する）。これは、サブスクリプションの制限を超過します。代わりに、別の Citrix Managed Azure サブスクリプションをリクエストします。その後、そのサブスクリプションを使用してカタログを作成できます。

Citrix Managed Azure サブスクリプションが複数ある場合:

- これらのサブスクリプション間で共有されるものはありません。
- 各サブスクリプションには一意の名前があります。
- Citrix Managed Azure サブスクリプション（および追加した顧客管理 Azure サブスクリプション）は、次の場合に選択できます。
  - カタログの作成
  - イメージをビルドまたはインポートする。
  - VNet ピアリングまたは SD-WAN 接続の作成

要件:

- 別の Citrix Managed Azure サブスクリプションの追加を保証するのに十分な Citrix ライセンスが必要です。前述の仮説の例を使用して、Citrix 管理サブスクリプションを通じて少なくとも 1,500 台のマシンを展開する見込みで 2,000 の Citrix ライセンスがある場合は、別の Citrix Managed Azure サブスクリプションを追加できます。

Citrix Managed Azure サブスクリプションを追加するには:

1. Citrix 担当者に連絡して、別の Citrix Managed Azure サブスクリプションをリクエストしてください。続行できる場合は通知されます。
2. サービスの ［管理］ダッシュボードで、右側の ［サブスクリプション］を展開します。
3. [**Azure** サブスクリプションの追加］をクリックします。
4. ［サブスクリプションの追加］ページで、[**Citrix Managed Azure** サブスクリプションの追加］をクリックします。
5. **Citrix** 管理サブスクリプションの追加］ページで、ページの下部にある［サブスクリプションの追加］をクリックします。

Citrix Managed Azure サブスクリプションの作成中にエラーが発生したことが通知された場合は、Citrix サポートにお問い合わせください。

Azure サブスクリプションを削除する

Azure サブスクリプションを削除するには、まず、それを使用するすべてのカタログとイメージを削除する必要があります。

Citrix Managed Azure サブスクリプションを 1 つ以上持っている場合、それらのサブスクリプションをすべて削除することはできません。少なくとも 1 つは残っていなければなりません。

1. サービスの ［管理］ダッシュボードで、右側の ［サブスクリプション］を展開します。
2. サブスクリプションのエントリをクリックします。
3. [詳細] タブで、[サブスクリプションの削除] をクリックします。
4. **[Azure** アカウントの認証**]** をクリックします。Azure サインインページに移動します。
5. Azure 認証情報を入力します。
6. 自動的にサービスに戻ります。チェックボックスで削除を確認し、[はい、サブスクリプションを削除] をクリックします。

ネットワーク接続

July 16, 2021

はじめに

この記事では、Citrix Managed Azure サブスクリプションを使用する場合のいくつかの展開シナリオの詳細について説明します。

カタログを作成するときに、Azure デスクトップとアプリケーションの Citrix Virtual Apps and Desktops Standard for Azure デスクトップからユーザーが企業のオンプレミスネットワーク上の場所とリソースにアクセスするかどうか、および方法を指定します。

Citrix Managed Azure サブスクリプションを使用する場合、次の選択肢があります。

- 接続なし
- Azure VNet ピアリング
- SD-WAN

独自のカスタマー管理の Azure サブスクリプションのいずれかを使用する場合、サービスへの接続を作成する必要はありません。Azure サブスクリプションをサービスに追加するするだけです。

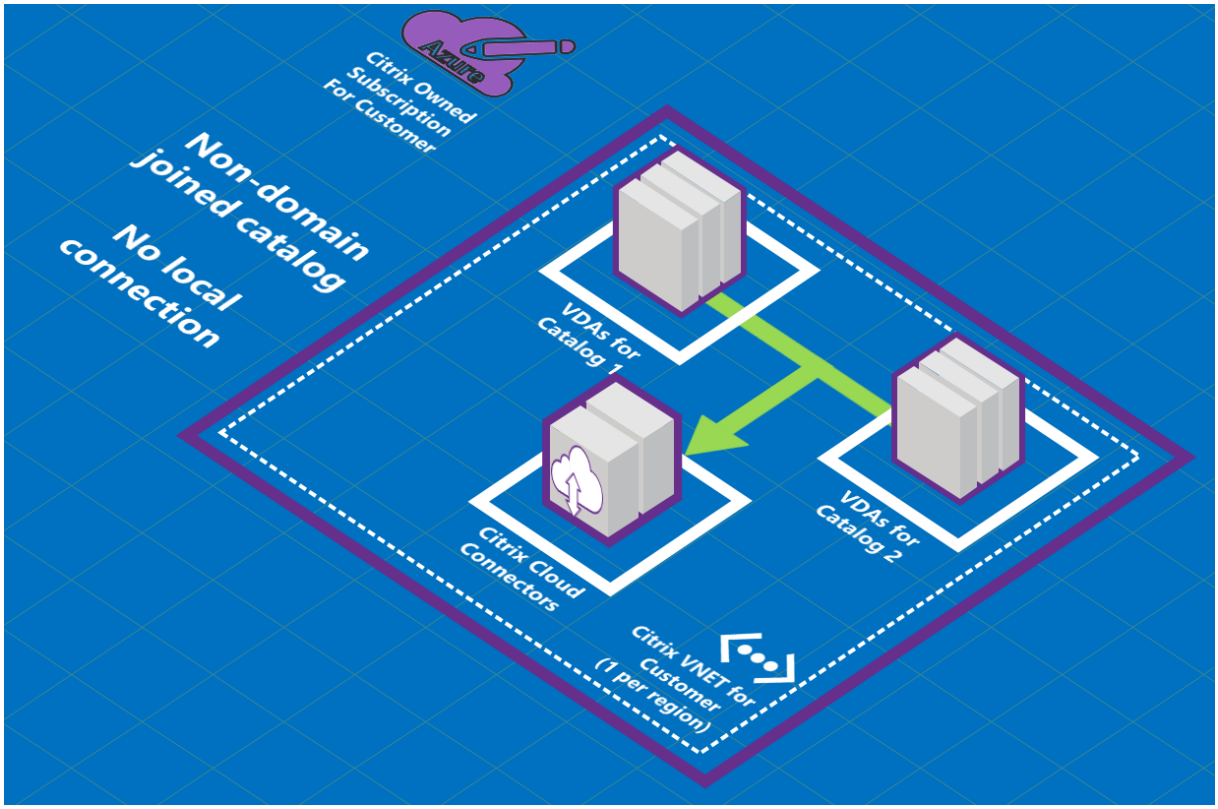
カタログの作成後は、カタログの接続タイプを変更することはできません。

すべてのネットワーク接続の要件

- 接続を作成するときは、有効な DNS サーバーエントリが必要です。
- セキュア DNS またはサードパーティ DNS プロバイダーを使用する場合は、許可リストの DNS プロバイダーの IP アドレスに、サービスによって使用するために割り当てられているアドレス範囲を追加する必要があります。このアドレス範囲は、接続の作成時に指定されます。
- 接続を使用するすべてのサービスリソース (ドメインに参加しているマシン) は、時刻の同期を確実にするために、ネットワークタイムプロトコル (NTP) サーバーに到達できる必要があります。

接続なし

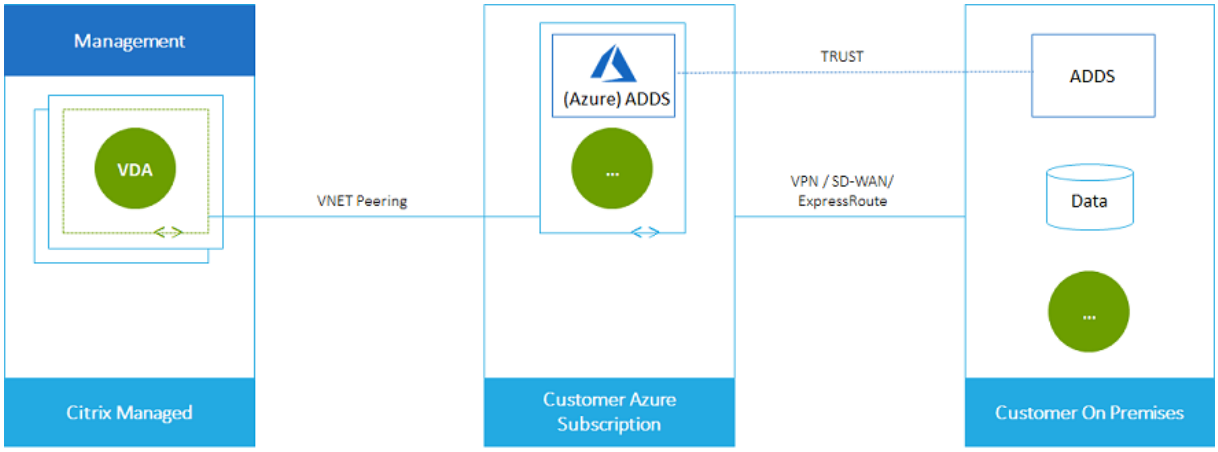
カタログが接続なしで構成されている場合、ユーザーはオンプレミスまたは他のネットワークのリソースにアクセスできません。クイック作成を使用してカタログを作成する場合は、これが唯一の選択肢です。



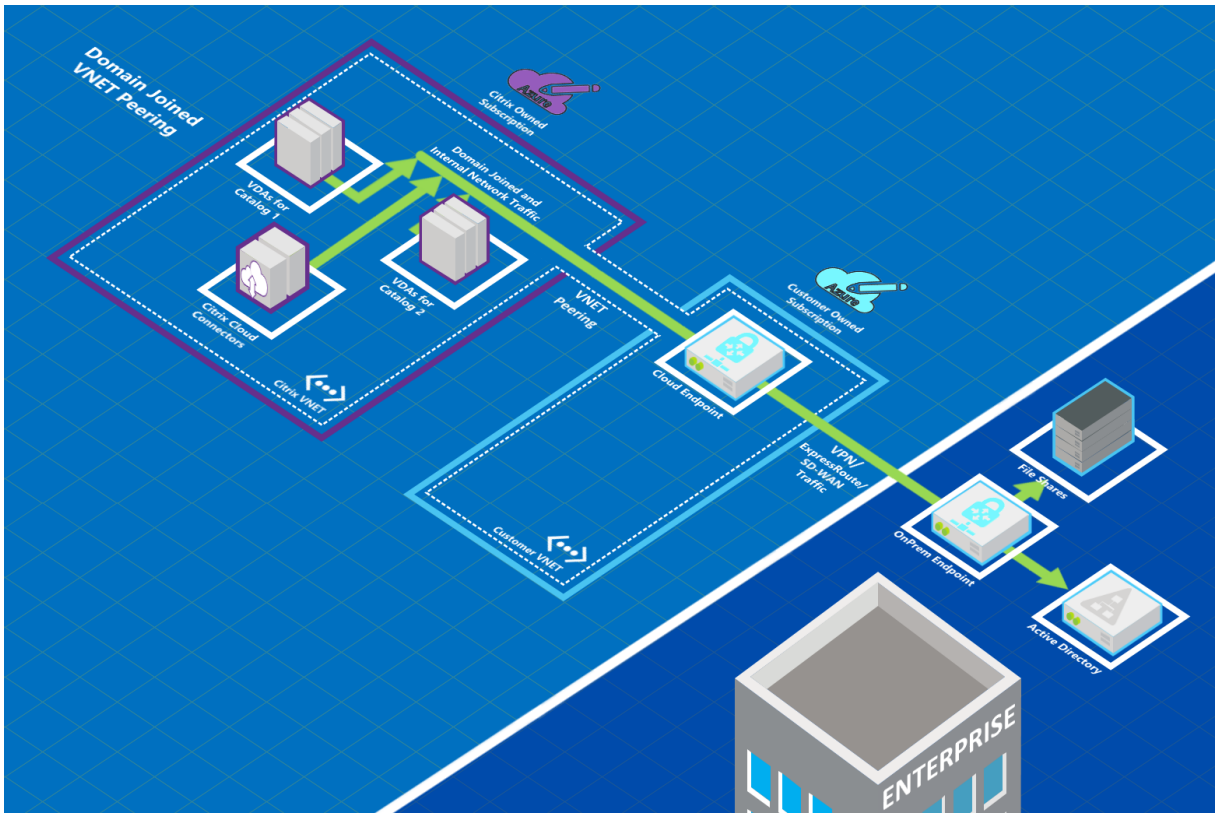
Azure VNET ピアリング接続について

仮想ネットワークピアリングは、2 つの Azure 仮想ネットワーク（VNet）をシームレスに接続します。お客様と Citrix Virtual Apps and Desktops Standard for Azure。また、ピアリングにより、ユーザーはオンプレミスネットワークからファイルやその他のアイテムにアクセスできるようになります。

次の図に示すように、Citrix Managed Azure サブスクリプションから会社の Azure サブスクリプション内の VNet への Azure VNet ピアリングを使用して接続を作成します。



VNet ピアリングの別の図を次に示します。



ユーザーは、カタログの作成時にローカルドメインに参加することで、オンプレミスのネットワークリソース (ファ

イルサーバーなど) にアクセスできます。(つまり、ファイル共有やその他の必要なリソースが存在する AD ドメインに参加します)。Azure サブスクリプションは、これらのリソースに接続します (グラフィックでは、VPN または Azure ExpressRoute を使用して)。カタログを作成するときは、ドメイン、OU、およびアカウントの認証情報を指定します。

> 重要:
>
> - このサービスで VNet ピアリングを使用する前に、VNet ピアリングについて学習します。
> - VNet ピア接続を使用するカタログを作成する前に、VNet ピア接続を作成します。

Azure VNet ピアリングカスタムルート

カスタムルートまたはユーザー定義のルートは、VNet ピアリング、オンプレミスネットワーク、およびインターネット内の仮想マシン間のトラフィックを転送するための Azure のデフォルトのシステムルートを上書きします。Citrix Virtual Apps and Desktops Standard リソースがアクセスすることが想定されているが、VNet ピアリングを介して直接接続されていないネットワークがある場合は、カスタムルートを使用できます。たとえば、ネットワークアプライアンスを経由してインターネットまたはオンプレミスのネットワークサブネットへのトラフィックを強制するカスタムルートを作成できます。

カスタムルートを使用するには、次の手順に従います。

- Citrix Virtual Apps and Desktops Standard 環境に、既存の Azure 仮想ネットワークゲートウェイまたは Citrix SD-WAN などのネットワークアプライアンスが必要です。
- カスタムルートを追加するときは、エンドツーエンドの接続性を確保するために、Citrix Virtual Apps and Desktops Standard の宛先 VNet 情報で会社のルートテーブルを更新する必要があります。
- カスタムルートは、Citrix Virtual Apps と Desktops Standard に入力された順序で表示されます。この表示順序は、Azure がルートを選択する順序には影響しません。

カスタムルートを使用する前に、カスタムルート、ネクストホップタイプの使用、および Azure がアウトバウンドトラフィックのルートを選択する方法について、Microsoft の記事仮想ネットワークトラフィックルーティングを参照してください。

カスタムルートは、Azure VNet ピア接続を作成するとき、または Citrix Virtual Apps およびデスクトップ標準環境の既存のピア接続を作成するときに追加できます。VNet ピアリングでカスタムルートを使用する準備ができたら、この記事の次のセクションを参照してください。

- 新しい Azure VNet ピアリングを使用したカスタムルートの場合: Azure VNet ピアリング接続を作成する
- 既存の Azure VNet ピアリングを持つカスタムルートの場合: 既存の Azure VNet ピア接続のカスタムルートを管理する

Azure VNet ピアリングの要件と準備

- Azure Resource Manager サブスクリプション所有者の資格情報。これは Azure Active Directory アカウントである必要があります。このサービスは、live.com や外部 Azure AD アカウント (別のテナント) など、他のアカウントタイプをサポートしていません。

- Azure サブスクリプション、リソースグループ、および仮想ネットワーク (VNet)。
- Citrix Managed Azure サブスクリプションの VDA がネットワークの場所と通信できるように、Azure ネットワークルートを設定します。
- VNet から指定された IP 範囲まで Azure ネットワークセキュリティグループを開きます。
- **Active Directory**: ドメインに参加しているシナリオでは、ピアリングされた VNet で何らかの形式の Active Directory サービスを実行することをお勧めします。これは、Azure VNet ピアリングテクノロジーの低レイテンシー特性を利用します。

  たとえば、構成には、Azure Active Directory ドメインサービス (AADDS)、VNet 内のドメインコントローラー仮想マシン、またはオンプレミスの Active Directory への Azure AD 接続などがあります。

  AADDS を有効にした後は、管理対象ドメインを削除せずに管理対象ドメインを別の VNet に移動することはできません。したがって、管理対象ドメインを有効にするには、正しい VNet を選択することが重要です。先に進む前に、Microsoft の記事Azure AD ドメインサービスのネットワークに関する考慮事項を確認してください。

- **VNet IP** 範囲**:** 接続を作成するときは、ネットワークリソースと Azure VNet の間で一意な、使用可能な CIDR アドレス空間 (IP アドレスとネットワークプレフィックス) を提供する必要があります。これは、Citrix Virtual Apps およびデスクトップ標準のピアリングされた VNet 内の仮想マシンに割り当てられる IP 範囲です。

  Azure ネットワークとオンプレミスネットワークで使用するアドレスと重複しない IP 範囲を指定してください。

  - たとえば、Azure VNet のアドレス空間が 10.0.0.0 /16 の場合、Citrix Virtual Apps およびデスクトップ標準で 192.168.0.0 /24 などの VNet ピア接続を作成します。
  - この例では、IP 範囲が 10.0.0.0 /24 のピア接続を作成すると、アドレス範囲が重複していると見なされます。

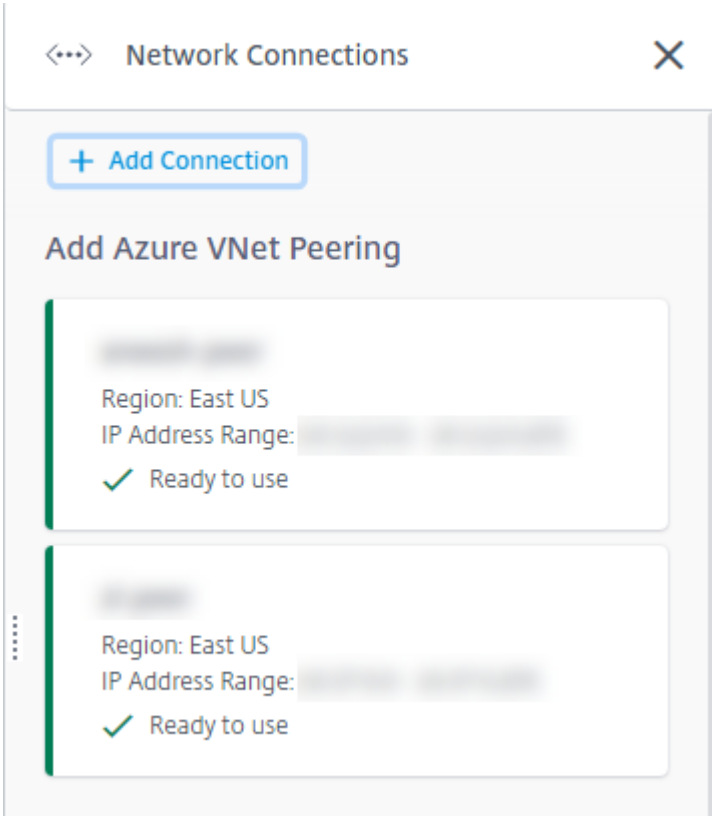
  アドレスが重複している場合、VNet ピア接続が正常に作成されない可能性があります。また、サイト管理タスクでは正しく動作しません。

VNet ピアリングの詳細については、次の Microsoft の記事を参照してください。

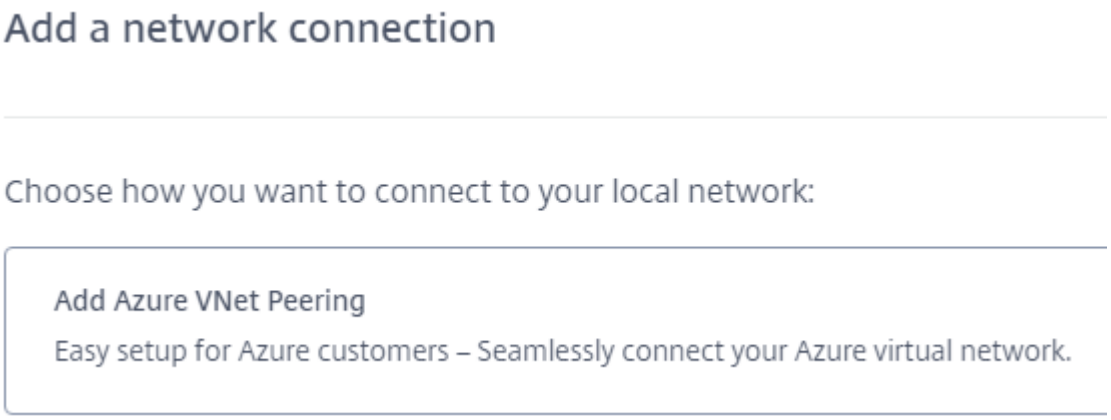
- 仮想ネットワークピアリング
- Azure VPN ゲートウェイ
- Azure ポータルでサイト間接続を作成する
- VPN ゲートウェイに関するよくある質問 (「オーバーラップ」を検索)

Azure VNet ピアリング接続を作成する

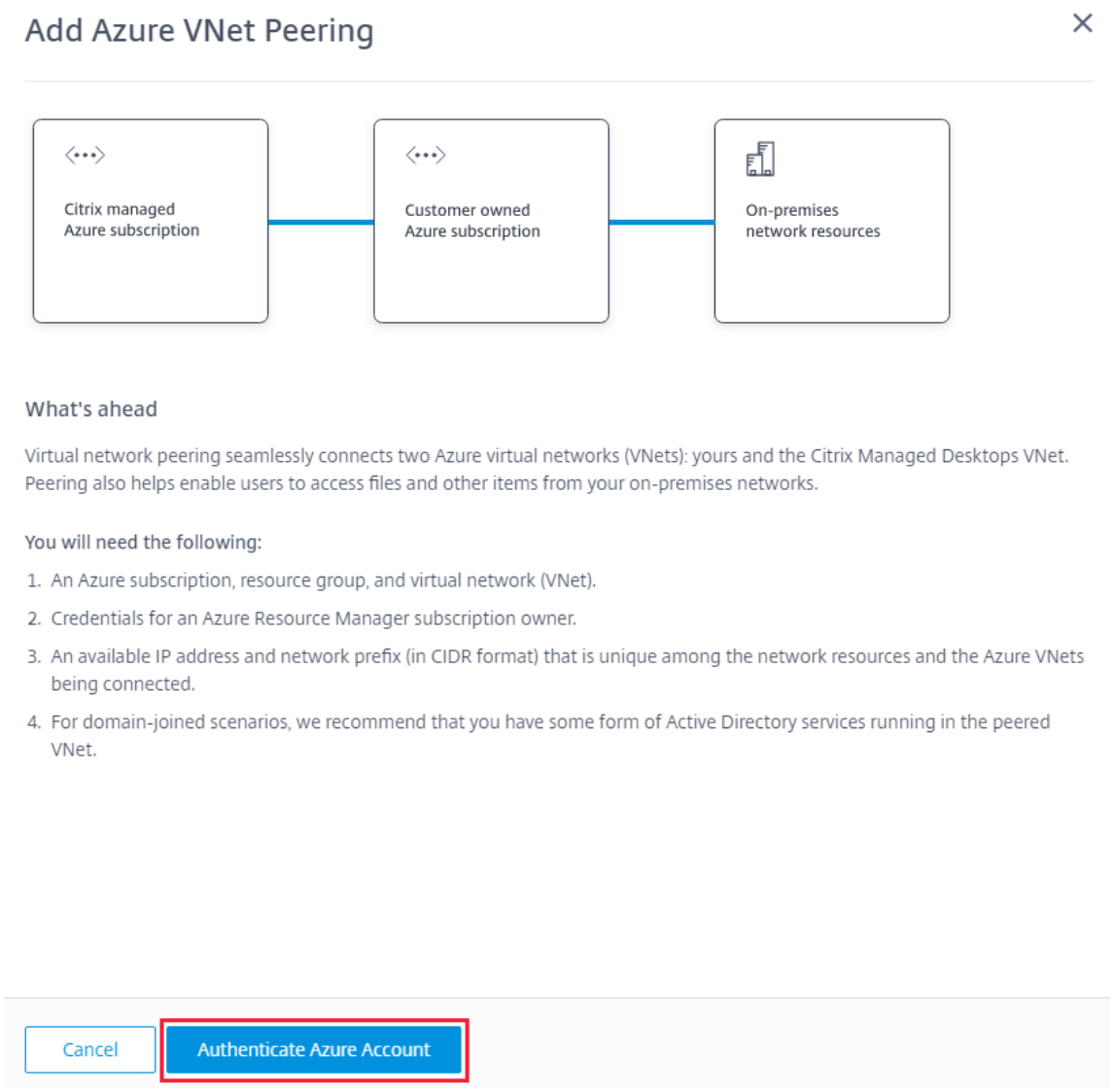
1. サービスの [管理] ダッシュボードから、右側の [ネットワーク接続] を展開します。接続をすでに設定している場合は、それらの接続が一覧表示されます。



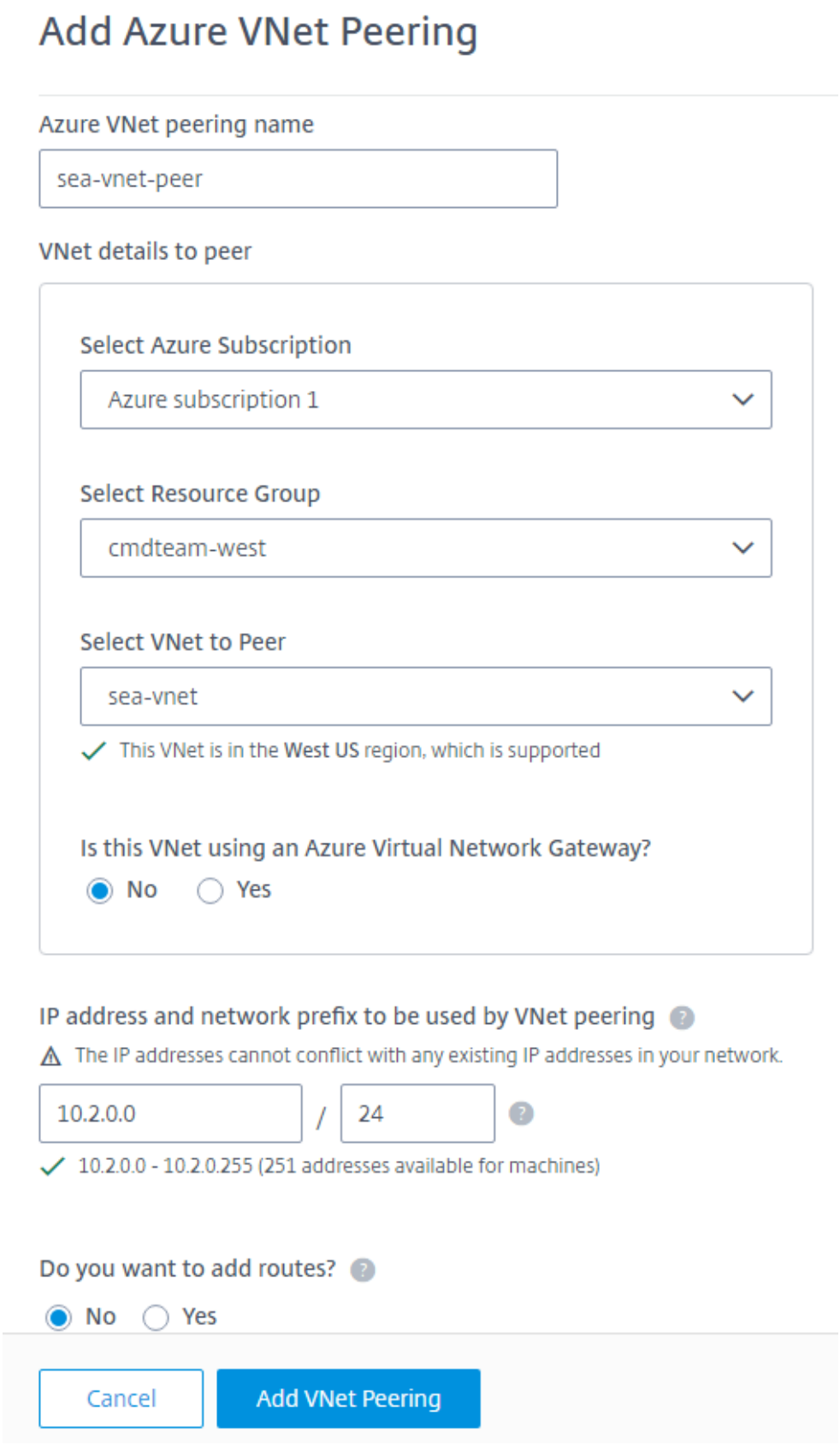
2. [接続の追加] をクリックします。
3. [**Azure VNet** ピアリングの追加] ボックスの任意の場所をクリックします。



4. **[Azure** アカウントの認証**]** をクリックします。



5. サービスによって Azure のサインインページが自動的に表示され、Azure サブスクリプションが認証されます。Azure に (グローバル管理者アカウントの認証情報を使用して) サインインし、条件に同意すると、[接続の作成の詳細] ダイアログに戻ります。



6. Azure VNet ピアの名前を入力します。
7. Azure サブスクリプション、リソースグループ、ピアへの VNet を選択します。
8. 選択した VNet が Azure 仮想ネットワークゲートウェイを使用するかどうかを指定します。詳細については、Microsoft の記事Azure VPN ゲートウェイを参照してください。
9. 前のステップ（選択した VNet が Azure 仮想ネットワークゲートウェイを使用）で「はい」と答えた場合は、仮想ネットワークゲートウェイルート伝播を有効にするかどうかを指定します。有効にすると、Azure はゲートウェイを経由するすべてのルートを自動的に学習 (追加) します。

   この設定は、後で接続の [詳細] ページで変更できます。ただし、これを変更すると、ルートパターンの変更や VDA トラフィックの中断が発生する可能性があります。また、後で無効にする場合は、VDA が使用するネットワークに手動でルートを追加する必要があります。
10. IP アドレスを入力し、ネットワークマスクを選択します。使用するアドレス範囲と、その範囲がサポートしているアドレスの数が表示されます。Azure ネットワークとオンプレミスネットワークで使用するアドレスが IP 範囲と重複しないようにします。

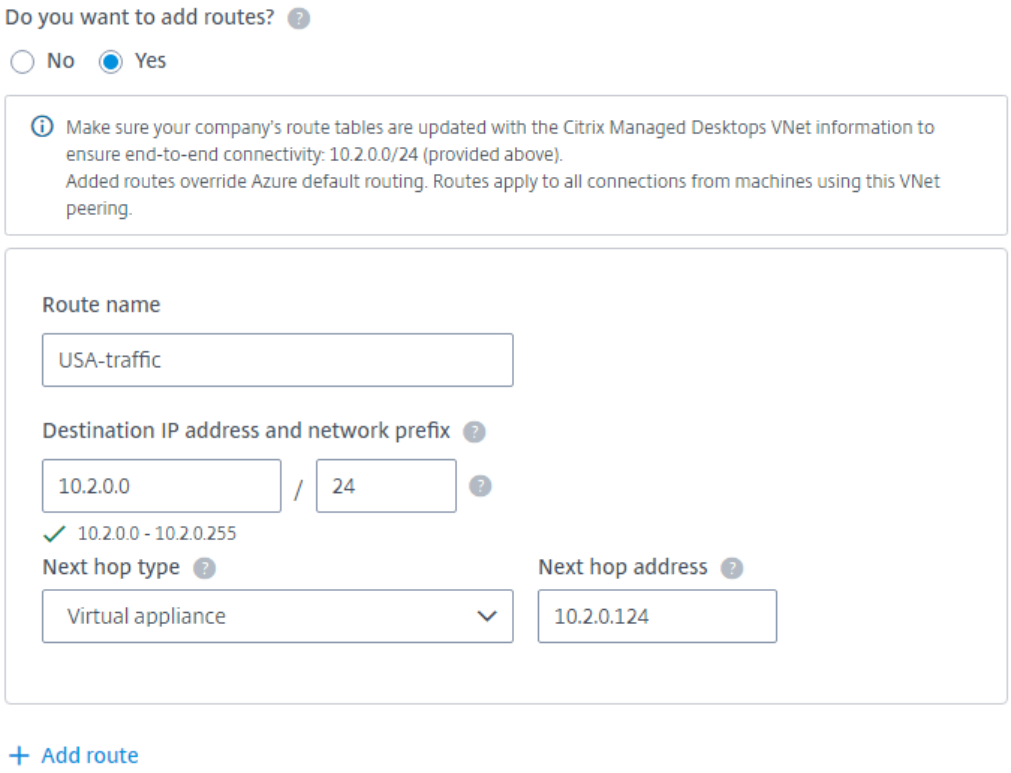
    - たとえば、Azure VNet のアドレス空間が 10.0.0.0/16 の場合、Citrix Virtual Apps およびデスクトップ標準で、192.168.0.0 /24 などの VNet ピア接続を作成します。
    - この例では、IP 範囲が 10.0.0.0 /24 の VNet ピアリング接続を作成することは、重複するアドレス範囲と見なされます。

    アドレスが重複している場合、VNet ピア接続が正常に作成されない可能性があります。また、サイト管理タスクでは正しく機能しません。
11. VNet ピア接続にカスタムルートを追加するかどうかを指定します。[はい] を選択した場合は、次の情報を入力します。

    a) カスタムルートのフレンドリ名を入力します。

    b) 宛先 IP アドレスとネットワークプレフィクスを入力します。ネットワークプレフィクスは 16 ～24 の間でなければなりません。

    c) トラフィックをルーティングする場所のネクストホップタイプを選択します。仮想アプライアンスを選択する場合は、アプライアンスの内部 IP アドレスを入力します。



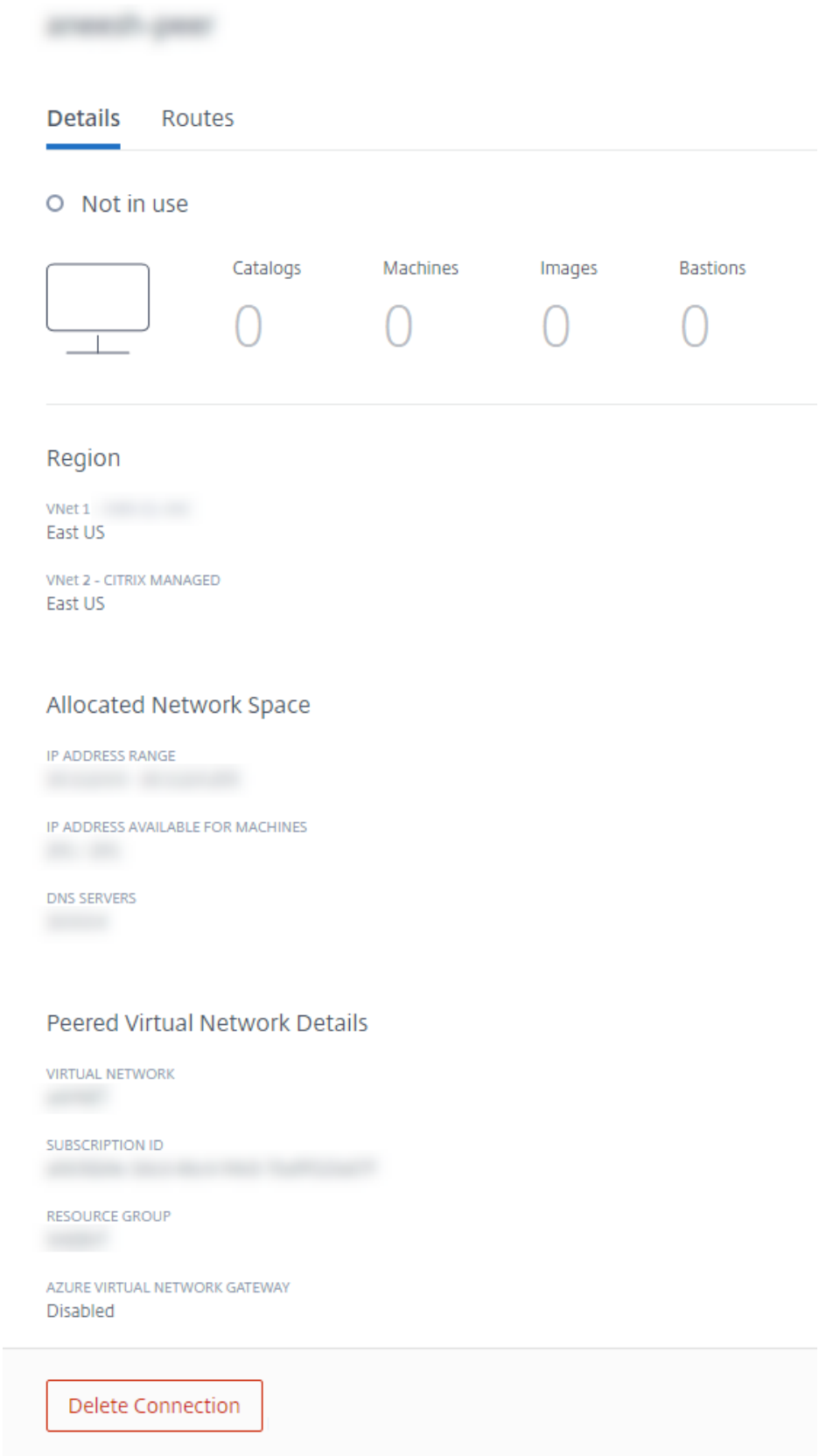
ネクストホップタイプの詳細については、Microsoft の記事仮想ネットワークトラフィックルーティングの「カスタムルート」を参照してください。

d) [ルートの追加] をクリックして、接続用の別のカスタムルートを作成します。

12. [**VNet** ピアリングを追加] をクリックします。

接続が作成されると、[管理] ダッシュボードの右側の [ネットワーク接続**] > [Azure VNet** ピア] の下に表示されます。カタログを作成すると、この接続が [使用可能なネットワーク接続] リストに含まれます。

Azure VNet ピア接続の詳細を表示する



1. サービスの [管理] ダッシュボードから、右側の [ネットワーク接続] を展開します。
2. 表示する Azure VNet ピアリング接続を選択します。

詳細には以下が含まれます。

- この接続を使用するカタログ、マシン、イメージ、および踏み台の数。
- リージョン、割り当てられたネットワーク領域、およびピア接続された VNet。
- VNet ピア接続用に現在構成されているルート。

既存の **Azure VNet** ピア接続のカスタムルートを管理する

既存の接続に新しいカスタムルートを追加したり、カスタムルートの無効化や削除など、既存のカスタムルートを変更したりできます。

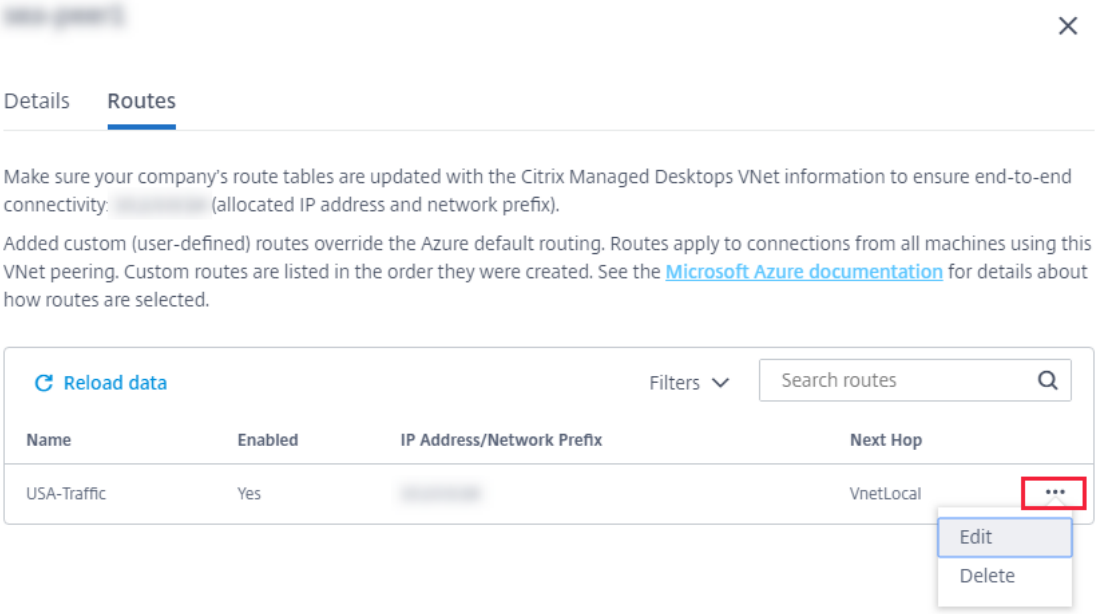
> 重要:
>
> カスタムルートを変更、無効化、または削除すると、接続のトラフィックフローが変更され、アクティブなユーザセッションが中断される可能性があります。

カスタムルートを追加するには、次の手順を実行します。

1. VNet ピア接続の詳細から、[ルート] を選択し、[ルートの追加] をクリックします。
2. フレンドリ名、宛先 IP アドレスとプレフィックス、および使用するネクストホップタイプを入力します。ネクストホップタイプとして **Virtual Appliance** を選択した場合は、アプライアンスの内部 IP アドレスを入力します。
3. カスタムルートを有効にするかどうかを指定します。デフォルトでは、カスタムルートは有効になっています。
4. [ルートの追加] をクリックします。

カスタムルートを変更または無効にするには、次の手順を実行します。

1. VNet ピア接続の詳細から、[ルート] を選択し、管理するカスタムルートを見つけます。
2. 省略記号メニューから、[編集] を選択します。



3. 必要に応じて、宛先 IP アドレスとプレフィックス、またはネクストホップタイプに対して必要な変更を加えます。
4. カスタムルートを有効または無効にするには、「このルートを有効にする?」で、[はい] または [いいえ] を選択します。
5. [保存] をクリックします。

カスタムルートを削除するには、次の手順を実行します。

1. VNet ピア接続の詳細から、[ルート] を選択し、管理するカスタムルートを見つけます。
2. 省略記号メニューから、[削除] を選択します。
3. [ルートを削除すると、アクティブなセッションが中断され、カスタムルートの削除による影響が認識されます。
4. [ルートを削除] をクリックします。

Azure VNet ピア接続を削除する

Azure VNet ピアを削除する前に、そのピアに関連付けられているカタログをすべて削除します。「カタログの削除」を参照してください。

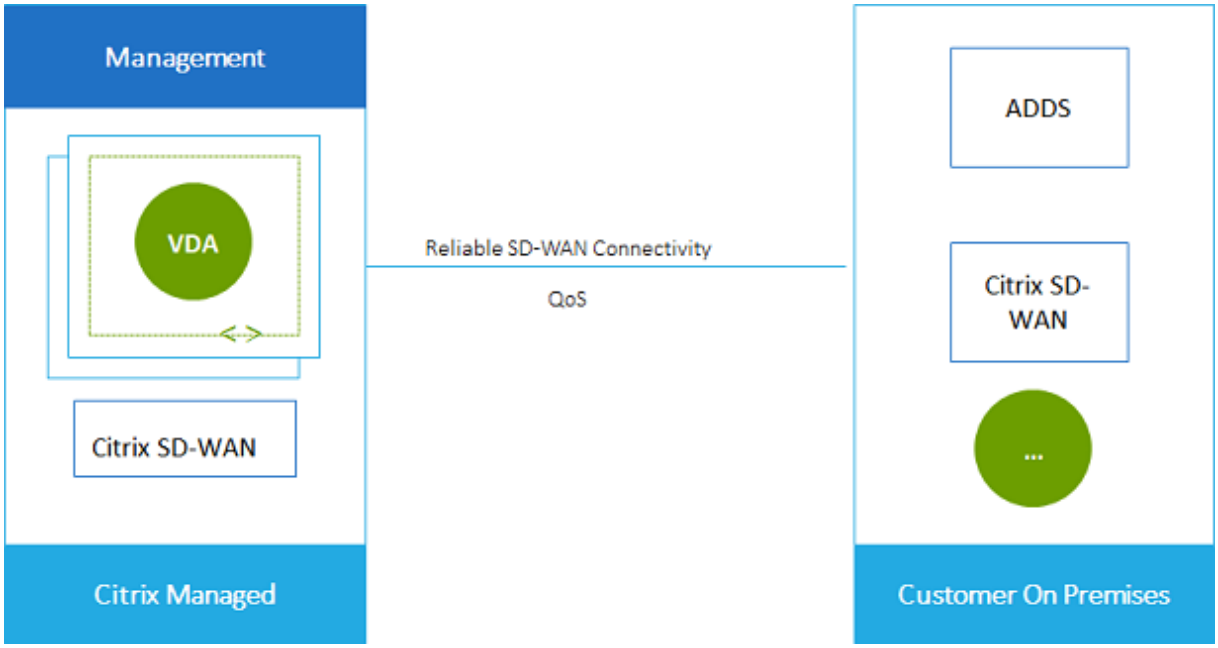
1. サービスの [管理] ダッシュボードから、右側の [ネットワーク接続] を展開します。
2. 削除する接続を選択します。
3. 接続の詳細から、[接続の削除] をクリックします。

SD-WAN 接続について

Citrix SD-WAN は、Citrix Virtual Apps and Desktops Standard for Azure で必要とされるすべてのネットワーク接続を最適化します。HDX テクノロジーと連携して、Citrix SD-WAN は、ICA およびアウトオブバンド Citrix Virtual Apps およびデスクトップ標準トラフィックにサービス品質と接続の信頼性を提供します。Citrix SD-WAN では、以下のネットワーク接続がサポートされています。

- ユーザーと仮想デスクトップ間のマルチストリーム ICA 接続
- 仮想デスクトップから Web サイト、SaaS アプリ、その他のクラウドプロパティへのインターネットアクセス
- 仮想デスクトップから Active Directory、ファイルサーバー、データベースサーバーなどのオンプレミスのリソースにアクセスする
- Workspace アプリのメディアエンジンから Microsoft Teams などのクラウドホスト型ユニファイドコミュニケーションサービスに RTP 経由で伝送されるリアルタイム/インタラクティブなトラフィック
- YouTube や Vimeo などのサイトからのクライアント側での動画の取得

次の図に示すように、Citrix Managed Azure サブスクリプションからサイトへの SD-WAN 接続を作成します。接続の作成時に、SD-WAN VPX アプライアンスは Citrix x 管理 Azure サブスクリプションに作成されます。SD-WAN の観点からは、その場所はブランチとして扱われます。



SD-WAN 接続要件と準備

- 次の要件が満たされない場合、SD-WAN ネットワーク接続オプションは使用できません。
  - Citrix Cloud のエンタイトルメント：Citrix Virtual Apps and Desktops Standard for Azure および SD-WAN Orchestrator。
  - インストールおよび構成済みの SD-WAN 展開。デプロイには、クラウドかオンプレミスかにかかわらず、マスターコントロールノード（MCN）が含まれ、SD-WAN Orchestrator で管理する必要がありま

す。

- VNet IP 範囲: 接続されているネットワークリソース間で一意の CIDR アドレス空間 (IP アドレスとネットワークプレフィックス) を提供します。これは、Citrix Virtual Apps and Desktops Standard VNet 内の仮想マシンに割り当てられる IP 範囲です。

  Cloud ネットワークとオンプレミスネットワークで使用するアドレスと重複しない IP 範囲を指定してください。

  - たとえば、ネットワークのアドレス空間が 10.0.0.0/16 の場合は、Citrix Virtual Apps およびデスクトップ標準で、192.168.0.0 /24 などの接続を作成します。
  - この例では、IP 範囲が 10.0.0.0 /24 の接続を作成すると、アドレス範囲が重複していると見なされます。

  アドレスが重複している場合、接続が正常に作成されない可能性があります。また、サイト管理タスクでは正しく動作しません。

- 接続設定プロセスには、ユーザー（サービス管理者）と SD-WAN Orchestrator 管理者が完了する必要があるタスクが含まれます。また、タスクを完了するには、SD-WAN Orchestrator 管理者から提供された情報が必要です。

  実際に接続を作成する前に、このドキュメントに記載されているガイダンスと SD-WAN のマニュアルの両方を確認することをお勧めします。

SD-WAN 接続を作成する

> 重要:
>
> SD-WAN の設定の詳細については、Citrix Virtual Apps and Desktops Standard for Azure の SD-WAN 構成を参照してください。

1. サービスの [管理] ダッシュボードから、右側の [ネットワーク接続] を展開します。
2. [接続の追加] をクリックします。
3. [ネットワーク接続の追加] ページで、[SD-WAN] ボックスの任意の場所をクリックします。
4. 次のページでは、何が先にあるのかをまとめます。読み終わったら、[**SD-WAN** の設定の開始] をクリックします。
5. [**SD-WAN** の設定] ページで、SD-WAN Orchestrator 管理者から提供された情報を入力します。
   - デプロイモード**:** [高可用性] を選択すると、2 つの VPX アプライアンスが作成されます (実稼働環境では推奨)。[スタンドアロン] を選択すると、1 つのアプライアンスが作成されます。この設定は後で変更できません。デプロイモードに変更するには、ブランチと関連するすべてのカタログを削除して再作成する必要があります。
   - 名前**:** SD-WAN サイトの名前を入力します。
   - スループットとオフィスの数**:** この情報は SD-WAN Orchestrator 管理者によって提供されます。

- リージョン**:** VPX アプライアンスが作成されるリージョン。
- **VDA** サブネットと **SD-WAN** サブネット：この情報は、SD-WAN Orchestrator 管理者によって提供されます。競合を回避する方法については、SD-WAN 接続要件と準備を参照してください。

6. 完了したら、[ブランチの作成] をクリックします。
7. 次のページでは、[管理] ダッシュボードで何を探すべきかをまとめます。読み終わったら、[それを手に入れる] をクリックします。
8. [管理] ダッシュボードの [ネットワーク接続] の下の新しい SD-WAN エントリに、設定プロセスの進行状況が表示されます。エントリがオレンジ色に変わり、「**SD-WAN** 管理者によるアクティベーションを待っています」というメッセージが表示されたら、**SD-WAN**Orchestrator 管理者に通知します。
9. SD-WAN Orchestrator の管理タスクについては、SD-WAN Orchestrator 製品ドキュメントを参照してください。
10. SD-WAN Orchestrator 管理者が終了すると、[ネットワーク接続] の SD-WAN エントリが緑色に変わり、[この接続を使用してカタログを作成できます**]** というメッセージが表示されます。

SD-WAN 接続の詳細を表示する

1. サービスの [管理] ダッシュボードから、右側の [ネットワーク接続] を展開します。
2. **SD-WAN** だけが選択されていない場合は、[SD-WAN] を選択します。
3. 表示する接続をクリックします。

ディスプレイには以下が含まれます。

- **[**詳細**]** タブ**:** 接続を構成するときに指定した情報。
- [ブランチ接続**]** タブ**:** 各ブランチおよび MCN の名前、クラウド接続、可用性、帯域幅層、ロール、場所。

SD-WAN 接続を削除する

SD-WAN 接続を削除する前に、SD-WAN 接続に関連付けられているすべてのカタログを削除します。「カタログの削除」を参照してください。

1. サービスの [管理] ダッシュボードから、右側の [ネットワーク接続] を展開します。
2. SD-WAN だけが選択されていない場合は、選択します。
3. 削除する接続をクリックし、詳細を展開します。
4. [詳細] タブで、[接続の削除] をクリックします。
5. 削除を確認します。

画像

July 16, 2021

デスクトップまたはアプリケーションを配信するためのカタログを作成すると、イメージが（他の設定とともに）マシンを作成するためのテンプレートとして使用されます。

Citrix 提供イメージ

Citrix Virtual Apps and Desktops Standard for Azure には、いくつかの Citrix が用意したイメージが用意されています。

- Windows 10 Enterprise（単一セッション）
- Windows 10 エンタープライズ仮想デスクトップ (マルチセッション)
- オフィス 365 ProPlus と Windows 10 エンタープライズ仮想デスクトップ (マルチセッション)
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Linux Ubuntu (シングルセッションとマルチセッション)

Citrix プリペアドイメージには、現在の Citrix Virtual Delivery Agent（VDA）とトラブルシューティングツールがインストールされています。VDA は、ユーザーのマシンとサービスを管理する Citrix Cloud インフラストラクチャとの間の通信メカニズムです。Citrix から提供された画像は、シトリックスとして表記されます。

Azure から独自のイメージをインポートして使用することもできます。

画像の使用方法

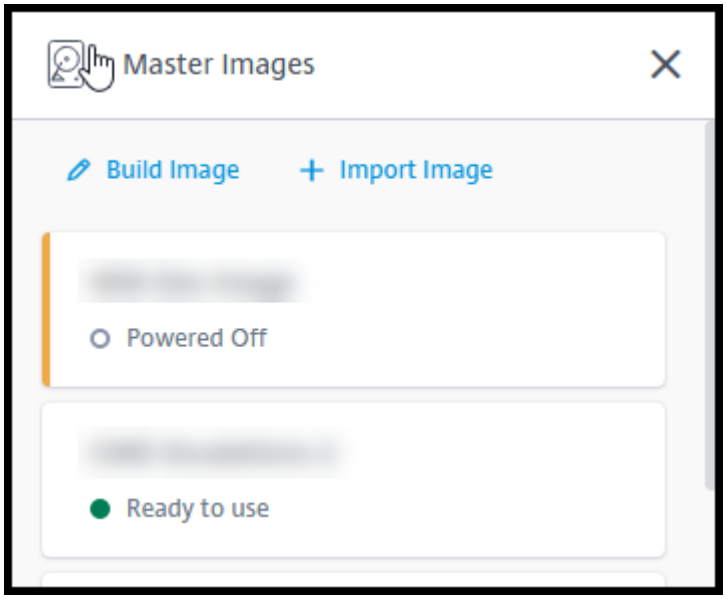
次の操作を実行できます:

- カタログを作成するときは、**Citrix** プリペアドイメージを使用します。この選択は、概念実証のデプロイにのみ推奨されます。
- **Citrix** プリペアドイメージを使用して、別のイメージを作成します。新しいイメージを作成した後、ユーザーが必要とするアプリケーションやその他のソフトウェアを追加して、イメージをカスタマイズします。その後、カタログを作成するときに、そのカスタマイズされたイメージを使用できます。
- **Azure** からイメージをインポートします。Azure からイメージをインポートした後、カタログの作成時にそのイメージを使用できます。または、そのイメージを使用して新しいイメージを作成し、アプリを追加してカスタマイズすることもできます。その後、カタログを作成するときに、そのカスタマイズされたイメージを使用できます。

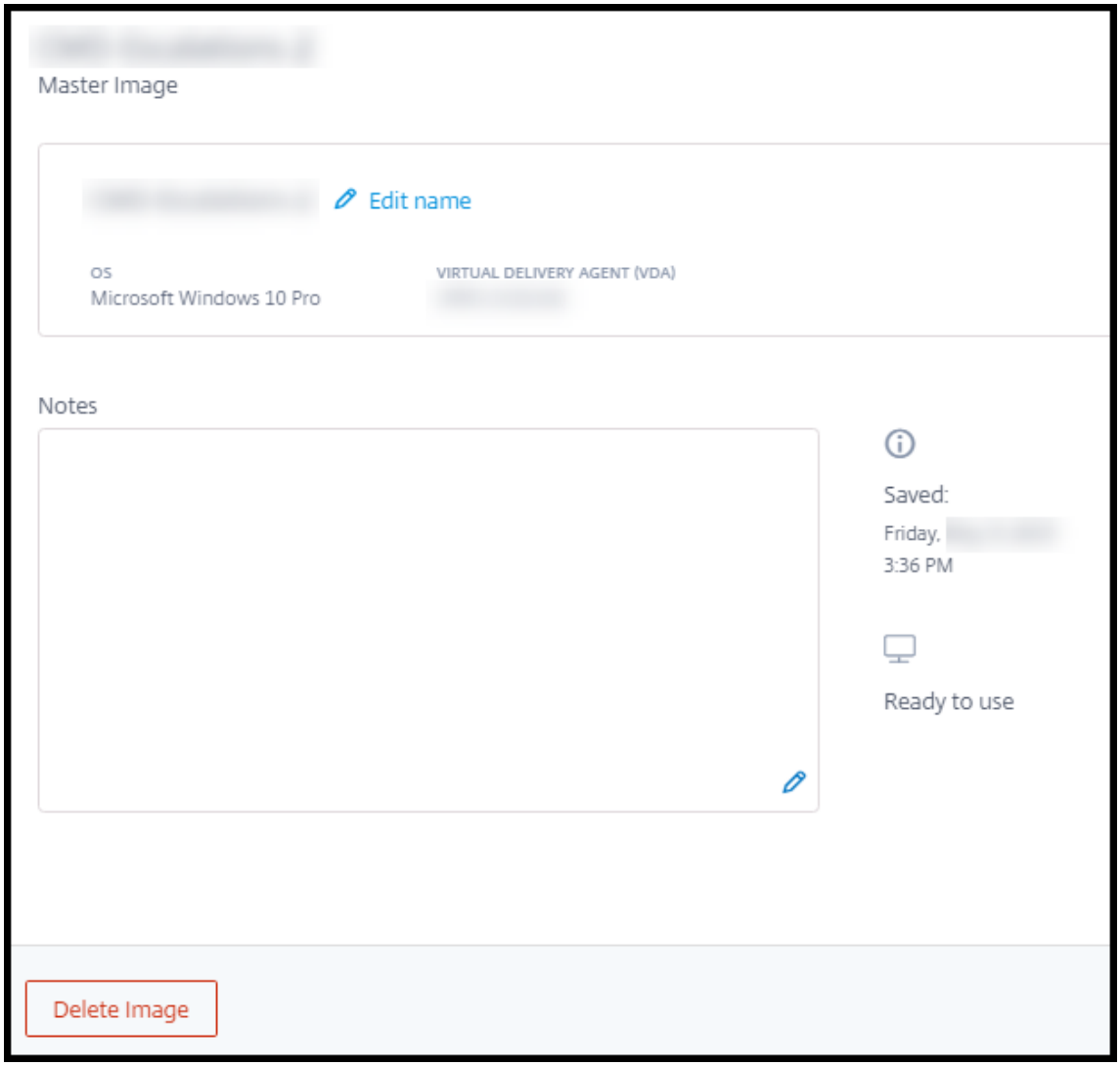
カタログを作成すると、サービスはイメージが有効なオペレーティングシステムを使用し、Citrix VDA とトラブルシューティングツールがインストールされていることを確認します（他のチェックとともに）。

画像情報の表示

1. サービスの [管理] ダッシュボードから、右側の [マスターイメージ] を展開します。画面には、Citrix が提供するイメージ、および作成およびインポートしたイメージがリストされます。



2. 画像をクリックすると、その詳細が表示されます。



詳細カードから、次のことができます。

- イメージの名前を変更 (編集) します。
- メモの追加と編集（シトリックス提供のイメージではなく、準備またはインポートした画像でのみ使用できます)。
- イメージを削除します。

新しいイメージを準備する

新しいイメージを準備するには、イメージの作成とカスタマイズが含まれます。イメージを作成すると、新しいイメージをロードするために新しい VM が作成されます。

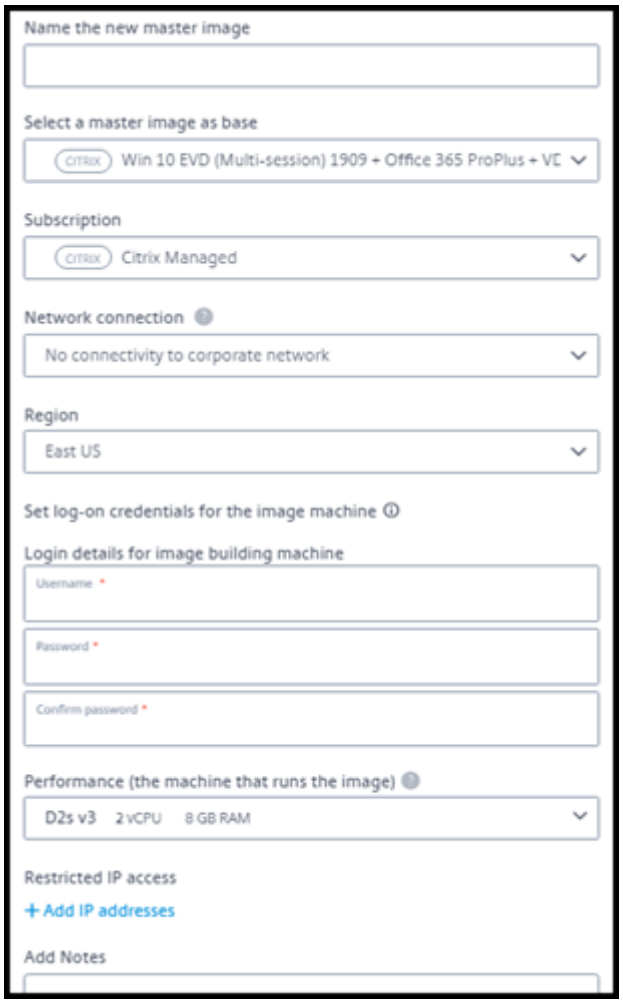
要件:

- マシンが必要とするパフォーマンス特性を知る。たとえば、CAD アプリケーションを実行する場合、他の Office アプリとは異なる CPU、RAM、およびストレージが必要になる場合があります。

- オンプレミスリソースへの接続を使用する場合は、イメージとカタログを作成する前にその接続を設定します。詳しくは、「ネットワーク接続」を参照してください。

イメージを作成するには、次の手順に従います。

1. サービスの [管理] ダッシュボードから、右側の [マスターイメージ] を展開します。
2. [イメージの作成] をクリックします。



3. 次のフィールドに値を入力します。
   - 名前**:** 新しいイメージの名前を入力します。
   - マスターイメージ**:** 既存のイメージを選択します。これは、新しいイメージの作成に使用されるベースイメージです。
   - サブスクリプション**:** Azure サブスクリプションを選択します。詳しくは、「Azure サブスクリプション」を参照してください。
   - ネットワーク接続**:**

  - Citrix Managed Azure サブスクリプションを使用している場合は、[接続なし] または [以前に作成した接続] を選択します。
  - 独自のカスタマー管理の Azure サブスクリプションを使用している場合は、リソースグループ、仮想ネットワーク、サブネットを選択します。次に、ドメインの詳細 (FQDN、OU、サービスアカウント名、資格情報) を追加します。

- リージョン**:** ([接続なし] の場合のみ使用可能) イメージを含むマシンを作成するリージョンを選択します。
- イメージマシンのログオン資格情報**:** 後で新しいイメージを含むマシンに (RDP) を接続するときに、これらの資格情報を使用して、アプリやその他のソフトウェアをインストールできるようにします。
- マシンのパフォーマンス**:** これは、イメージを実行するマシンの CPU、RAM、およびストレージ情報です。アプリの要件を満たすマシンのパフォーマンスを選択します。
- 制限付き **IP** アクセス**:** 特定のアドレスへのアクセスを制限する場合は、[**IP** アドレスの追加] を選択し、1 つ以上のアドレスを入力します。アドレスを追加したら、[完了] をクリックして [ビルドイメージ] カードに戻ります。
- メモ**:** オプションで 1024 文字までのノートを追加します。画像を作成したら、画像の詳細表示からメモを更新できます。
- ローカルドメイン参加**:** ローカル Active Directory ドメインに参加するかどうかを指定します。
  - [はい] を選択した場合は、Azure 情報 (FQDN、OU、サービスアカウント名、資格情報) を入力します。
  - [いいえ] を選択した場合は、ホストマシンの資格情報を入力します。

4. 完了したら、[イメージの構築] をクリックします。

イメージの構築には最大 30 分かかることがあります。管理ダッシュボードで、右側の [マスターイメージ] を展開して、現在の状態 ([ビルドイメージ] や [カスタマイズの準備完了] など) を確認します。

次の手順:新しいイメージに接続してカスタマイズする。

新しいイメージに接続してカスタマイズする

新しいイメージが作成されると、その名前がイメージリストに追加され、ステータスが [カスタマイズ可能] (または類似の文言) になります。そのイメージをカスタマイズするには、まず RDP ファイルをダウンロードします。そのファイルを使用してイメージに接続すると、アプリケーションやその他のソフトウェアをイメージに追加できます。

1. サービスの [管理] ダッシュボードから、右側の [マスターイメージ] を展開します。接続する画像をクリックします。
2. [**RDP** ファイルのダウンロード] をクリックします。RDP クライアントがダウンロードされます。

   イメージマシンの作成直後に RDP しないと、イメージマシンの電源が切れる場合があります。これにより、コストが節約されます。その場合は、[電源オン] をクリックします。

3. ダウンロードした RDP クライアントをダブルクリックします。新しいイメージを含むマシンのアドレスに自動的に接続しようとします。プロンプトが表示されたら、イメージの作成時に指定した認証情報を入力します。
4. マシンに接続したら、アプリを追加または削除し、更新プログラムをインストールして、その他のカスタマイズ作業を完了します。

   イメージを **Sysprep** しないでください。
5. 新しいイメージのカスタマイズが完了したら、[マスターイメージ] ボックスに戻り、[ビルドを終了] をクリックします。新しいイメージは自動的に検証テストを受けます。

後でカタログを作成すると、新しいイメージが選択可能なイメージのリストに含まれます。

管理ダッシュボードの右側に表示されるイメージは、各イメージを使用しているカタログとマシンの数を示します。

> 注:
>
> イメージを完成させた後は、編集できません。新しいイメージを作成し (前のイメージを開始点として使用して)、新しいイメージを更新する必要があります。

Azure からイメージをインポートする

ユーザーが必要とする Citrix VDA とアプリケーションを持つ Azure からイメージをインポートすると、それを使用してカタログを作成したり、既存のカタログ内のイメージを置き換えることができます。

インポートされたイメージの要件

> 注:
>
> このサービスは、Azure 第 2 世代 VM に関連付けられているディスクのインポートをサポートしていません。

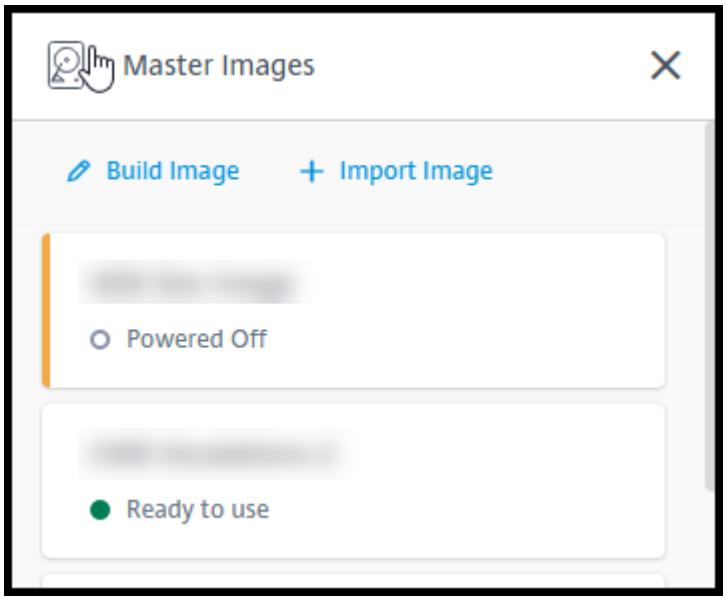
インポートされたイメージに対して検証 Citrix が実行されます。Citrix Virtual Apps and Desktops Standard にインポートするイメージを準備するときは、次の要件が満たされていることを確認してください。

- サポートされている **OS:** イメージは 対応している OS。Windows OS のバージョンを確認するには、`Get-WmiObject Win32_OperatingSystem`を実行します。
- サポートされている世代**:** 第 1 世代の VM のみがサポートされます。
- 一般化しない**:** イメージを一般化してはいけません。
- 構成済みの **Delivery Controller** がない: イメージに Citrix Delivery Controller が構成されていないことを確認します。次のレジストリキーがクリアされていることを確認します。
  - `HKLM:\SOFTWARE\Citrix\VirtualDesktopAgent\ListOfDDCs`
  - `HKLM:\SOFTWARE\Policies\Citrix\VirtualDesktopAgent\ListOfDDCs`
  - `HKLM:\SOFTWARE\Citrix\VirtualDesktopAgent\FarmGUID`
  - `HKLM:\SOFTWARE\Policies\Citrix\VirtualDesktopAgent\FarmGUID`
- **Personality.ini** ファイル**:**`personality.ini` ファイルはシステムドライブに存在する必要があります。

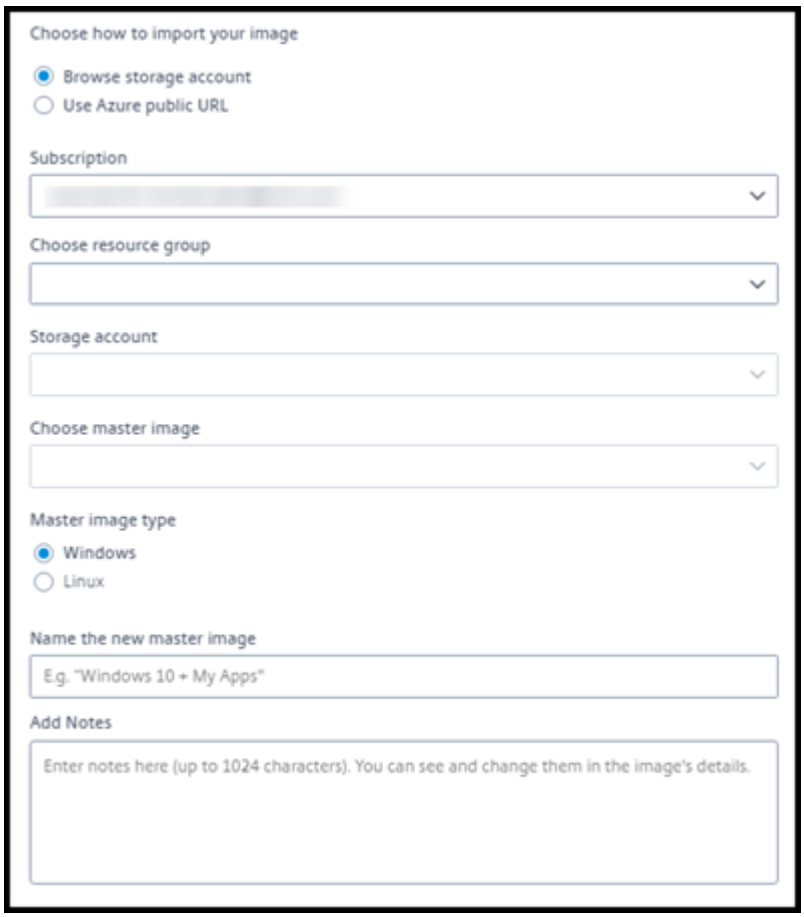
- 有効な **VDA**: イメージには、7.11 より新しい Citrix VDA がインストールされている必要があります。
  - Windows: 確認するには、`Get HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Citrix Virtual Desktop Agent`を使用します。インストールの手順については、「イメージに Windows VDA をインストールする」を参照してください。
  - Red Hat Enterprise Linux および Ubuntu: インストールガイダンスについては、製品ドキュメントを参照してください。
- **Azure** 仮想マシンエージェント**:** イメージをインポートする前に、Azure 仮想マシンエージェントがイメージにインストールされていることを確認してください。詳しくは、Microsoft 社のAzure 仮想マシンエージェントの概要を参照してください。

イメージをインポートする

1. サービスの [管理] ダッシュボードから、右側の [マスターイメージ] を展開します。



2. [イメージをインポート] をクリックします。



3. イメージのインポート方法を選択します。
   - 管理対象ディスクの場合は、エクスポート機能を使用して SAS URL を生成します。有効期限を 7200 秒以上に設定します。
   - ストレージアカウントの vHD の場合は、次のいずれかを選択します。
     - VHD ファイルの SAS URL を生成します。
     - ブロックストレージコンテナのアクセスレベルを BLOB またはコンテナに更新します。次に、ファイルの URL を取得します。
4. ストレージアカウントの参照] を選択した場合:
   a) サブスクリプション > リソースグループ > ストレージアカウント > イメージを順番に選択します。
   b) イメージに名前を付けます。
5. **Azure** パブリック **URL** を選択した場合:
   a) Azure 生成の VHD の URL を入力します。ガイダンスについては、Microsoft ドキュメントAzure から Windows VHD をダウンロードするへのリンクをクリックしてください。
   b) サブスクリプションを選択します。(Linux イメージは、カスタマー管理サブスクリプションを選択した場合にのみインポートできます)。
   c) イメージに名前を付けます。

6. 完了したら、[イメージのインポート] をクリックします。

新しいイメージでカタログを更新

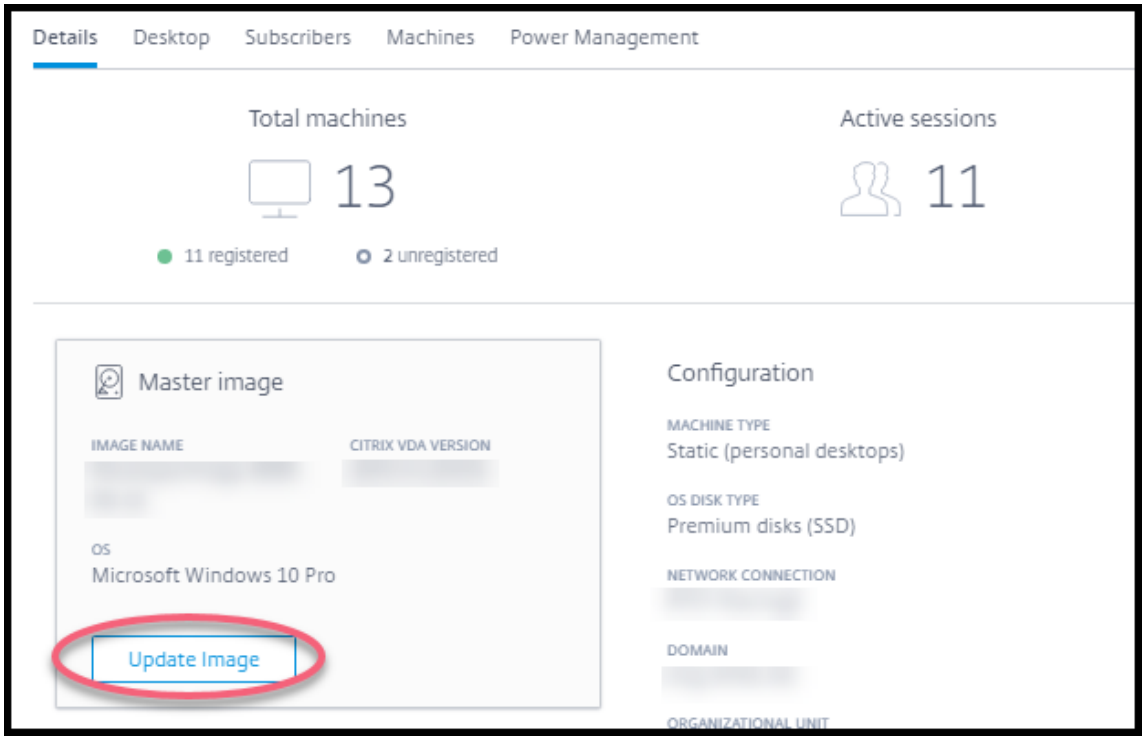
カタログの種類によって、カタログの更新時に更新されるマシンが決まります。

- ランダムカタログの場合、カタログに現在含まれているすべてのマシンが最新のイメージで更新されます。そのカタログにデスクトップを追加すると、それらのデスクトップは最新のイメージに基づきます。
- 静的カタログの場合、カタログ内のマシンは最新のイメージで更新されません。カタログ内のマシンは、作成元のイメージを引き続き使用します。ただし、そのカタログにマシンを追加すると、それらのマシンは最新のイメージに基づきます。

カタログのマシンが gen2 をサポートしている場合、gen1 イメージを持つマシンを含むカタログを gen2 イメージで更新できます。同様に、カタログのマシンが gen1 をサポートしている場合、gen2 マシンを含むカタログを gen1 イメージで更新できます。

カタログを新しいイメージで更新するには:

1. サービスの [管理] ダッシュボードから、カタログのエントリの任意の場所をクリックします。
2. [詳細] タブで、[イメージの更新] をクリックします。



3. イメージを選択します。
4. ランダムまたはマルチセッションカタログの場合: ログオフ間隔を選択します。サービスが初期イメージ処理を完了すると、サブスクライバは作業内容を保存してデスクトップからログオフする警告を受け取ります。ログオフ間隔は、ユーザがメッセージを受信してからセッションが自動的に終了するまでの時間を示します。

5. [イメージの更新] をクリックします。

イメージの削除

1. サービスの [管理] ダッシュボードから、右側の [マスターイメージ] を展開します。
2. 削除するイメージをクリックします。
3. カードの下部にある [イメージの削除] をクリックします。削除を確認します。

イメージに **Windows VDA** をインストールする

Citrix Virtual Apps およびデスクトップ標準にインポートする Windows イメージを準備する場合は、次の手順に従います。Linux VDA のインストールガイダンスについては、Linux VDA 製品ドキュメントを参照してください。

1. Azure 環境で、イメージ仮想マシンに接続します (まだ接続していない場合)。
2. Citrix Cloud ナビゲーションバーの［ダウンロード］リンクを使用して、VDA をダウンロードできます。または、ブラウザを使用して、Citrix Virtual Apps and Desktops サービスのダウンロードページに移動します。

   VDA を VM にダウンロードします。デスクトップ（シングルセッション）OS とサーバー（マルチセッション）OS には、別々の VDA ダウンロードパッケージがあります。
3. ダウンロードしたファイルをダブルクリックして、VDA インストーラーを起動します。インストールウィザードが起動します。
4. [環境] ページで、MCS を使用してイメージを作成するオプションを選択し、[次へ] をクリックします。
5. ［コアコンポーネント］ページで ［次へ］をクリックします。
6. ［**Delivery Controller**］ページで、［**Machine Creation Services** で自動的に指定する］を選択して ［次へ］をクリックします。
7. ［追加コンポーネント］、［機能］、［ファイアウォール］の各ページの設定については、シトリックスから別途指示がない限りデフォルトのままにします。各ページで ［次へ］をクリックします。
8. ［概要］ページで ［インストール］をクリックします。前提条件のインストールが始まります。再起動を求められたら、同意します。
9. VDA のインストールは自動的に再開されます。前提条件のインストールが完了すると、コンポーネントと機能がインストールされます。［**Call Home** ］ページで、デフォルト設定のままにしておきます（Citrix から指示がない限り）。接続したら、[次へ] をクリックします。
10. ［完了］をクリックします。マシンが自動的に再起動します。
11. 構成が正しいことを確認するには、VM にインストールした 1 つ以上のアプリケーションを起動します。
12. 仮想マシンをシャットダウンします。Sysprep は使用しないでください。

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

ユーザーと認証

July 16, 2021

ユーザー認証方法

ユーザーは、Citrix Workspace にログインしてデスクトップまたはアプリを起動するときに認証が必要です。

Citrix Virtual Apps and Desktops Standard for Azure では、次のユーザー認証方法がサポートされています。

- 管理対象 **Azure AD:** 管理対象 Azure AD は、Citrix が提供および管理する Azure Active Directory (AAD) です。独自の Active Directory 構造を提供する必要はありません。ユーザーをディレクトリに追加するだけです。
- アイデンティティプロバイダー： Citrix Cloud で利用可能な任意の認証方法を使用できます。

> 注:
>
> - リモート PC アクセス展開では、Active Directory のみが使用されます。詳しくは、「リモート PC アクセス」を参照してください。
> - Azure AD Domain Services を使用する場合：ワークスペースのログオン UPN（User Principal Name：ユーザープリンシパル名）には、Azure AD Domain Services の有効化時に指定したドメイン名を含める必要があります。作成したカスタムドメインをプライマリとして指定している場合でも、ログオンにカスタムドメインの UPN を使用することはできません。

ユーザ認証の設定には、次の手順が含まれます。

1. Citrix Cloud およびワークスペースの構成でユーザー認証方法を構成する。
2. ユーザー認証にマネージド Azure AD を使用している場合は、ユーザーをディレクトリに追加する。
3. カタログにユーザーを追加する。

Citrix Cloud でユーザー認証を構成する

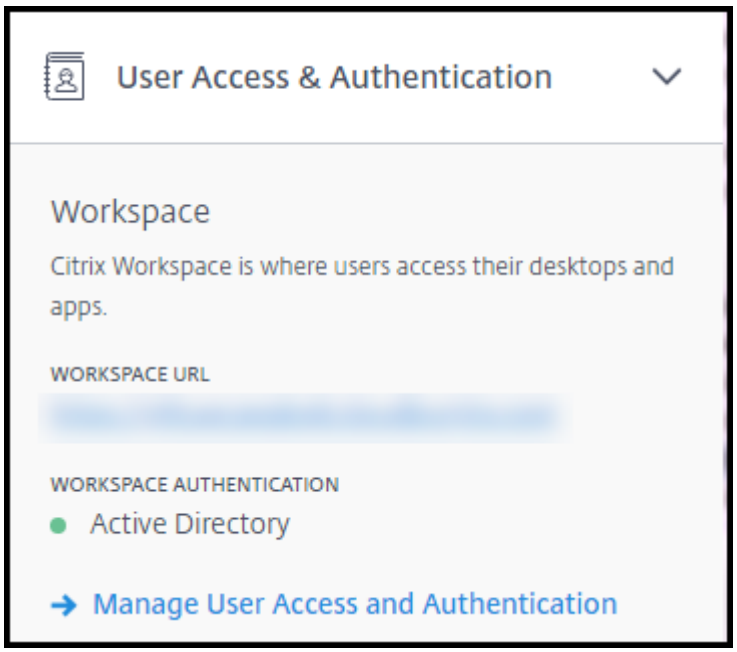
Citrix Cloud でユーザー認証を構成するには:

- 使用するユーザー認証方法に接続します。(Citrix Cloud では、認証方法から「接続」または「切断」します)。
- Citrix Cloud で、接続方法を使用するようにワークスペース認証を設定します。

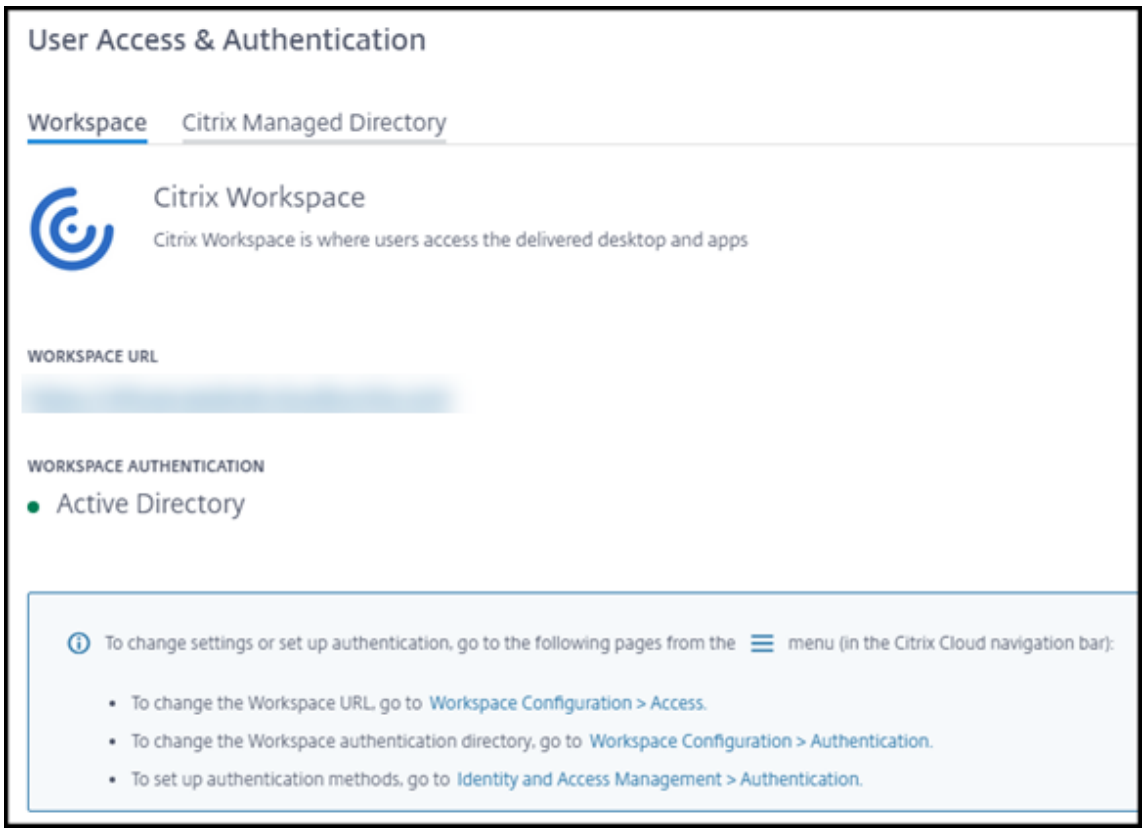
> 注:
>
> 管理対象の Azure AD 認証方法はデフォルトで設定されています。つまり、Citrix Cloud で自動的に接続され、ワークスペース認証はこのサービスで管理対象 Azure AD を使用するように自動的に設定されます。この方法を使用する場合（以前に別の方法を設定していない）場合は、管理対象 Azure AD でユーザーを追加および削除するに進みます。

認証方法を変更するには、次の手順に従います。

1. サービスの [管理] ダッシュボードから、右側の [ユーザーアクセスと認証] をクリックします。



2. [ユーザーアクセスと認証の管理] をクリックします。[ワークスペース] タブが選択されていない場合は、[ワークスペース] タブを選択します。(もう一方のタブは、現在構成されているユーザ認証方法を示します)。



3.「認証方法をセットアップするには」リンクに従います。このリンクをクリックすると、Citrix Cloud に移動

します。目的のメソッドの省略記号メニューで [接続] を選択します。

4. Citrix Cloud のまま、左上のメニューで［ワークスペースの構成］を選択します。[認証] タブで、必要な方法を選択します。

次の手順:

- マネージド Azure AD を使用している場合は、ユーザーをディレクトリに追加する。
- すべての認証方法について、ユーザーをカタログに追加。

管理対象 **Azure AD** でユーザーを追加および削除する

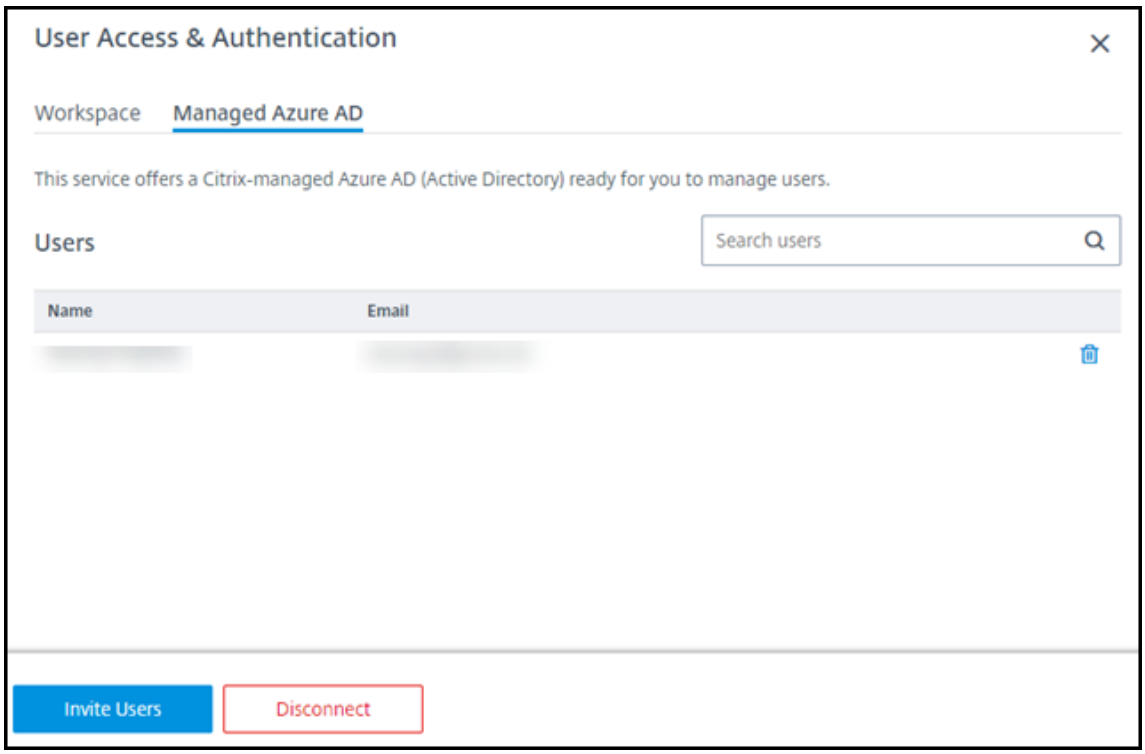
この手順は、Citrix Workspace へのユーザー認証に管理 Azure AD を使用している場合にのみ実行してください。

ユーザーの名前とメールアドレスを指定します。Citrix は、それぞれに招待状を電子メールで送信します。電子メールは、Citrix Managed Azure AD にユーザーを結合するリンクをクリックするようにユーザーに指示します。

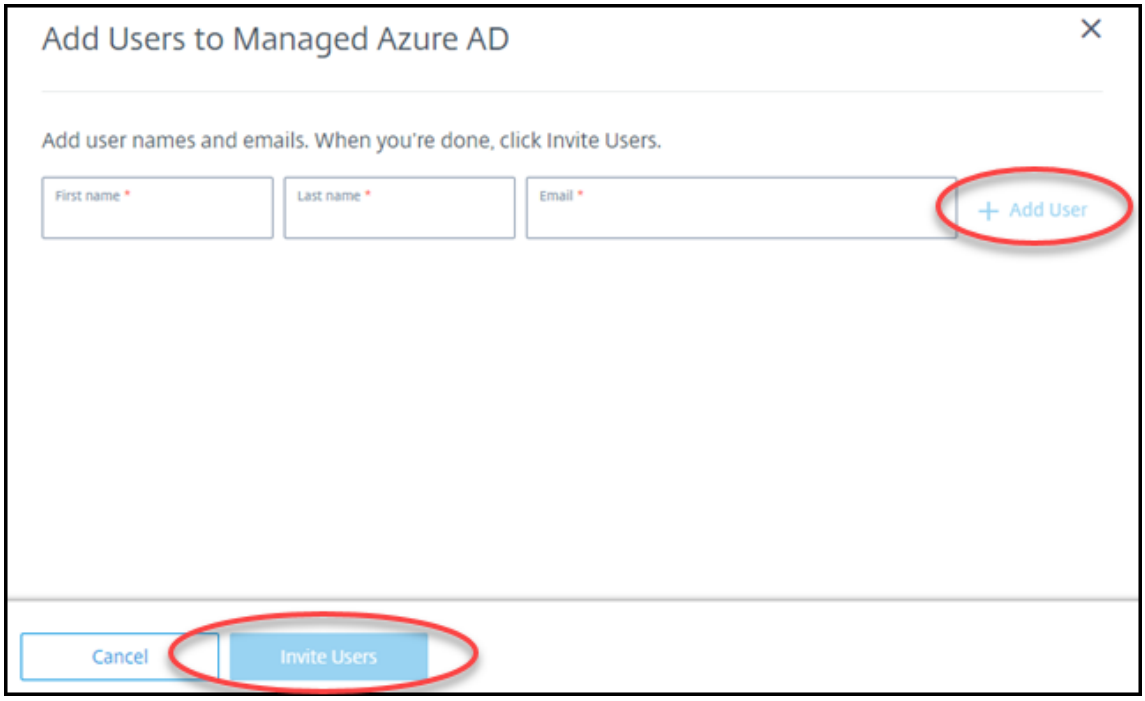
- ユーザーが指定した電子メールアドレスを持っている Microsoft アカウントをすでに持っている場合は、そのアカウントが使用されます。
- ユーザーが電子メールアドレスの Microsoft アカウントを持っていない場合、Microsoft はアカウントを作成します。

ユーザーを管理対象 Azure AD に追加して招待するには、次の手順に従います。

1. サービスの [管理] ダッシュボードから、右側の [ユーザーアクセスと認証] を展開します。[ユーザーアクセスと認証の管理] をクリックします。
2. [管理対象 **Azure AD**] タブをクリックします。
3. [ユーザーの招待] をクリックします。



4. ユーザーの名前とメールアドレスを入力し、[ユーザーの追加] をクリックします。



5. 前の手順を繰り返して、他のユーザーを追加します。
6. ユーザー情報の追加が完了したら、カードの下部にある [ユーザーを招待する] をクリックします。

Managed Azure AD からユーザーを削除するには、ディレクトリから削除するユーザーの名前の横にあるゴミ箱ア

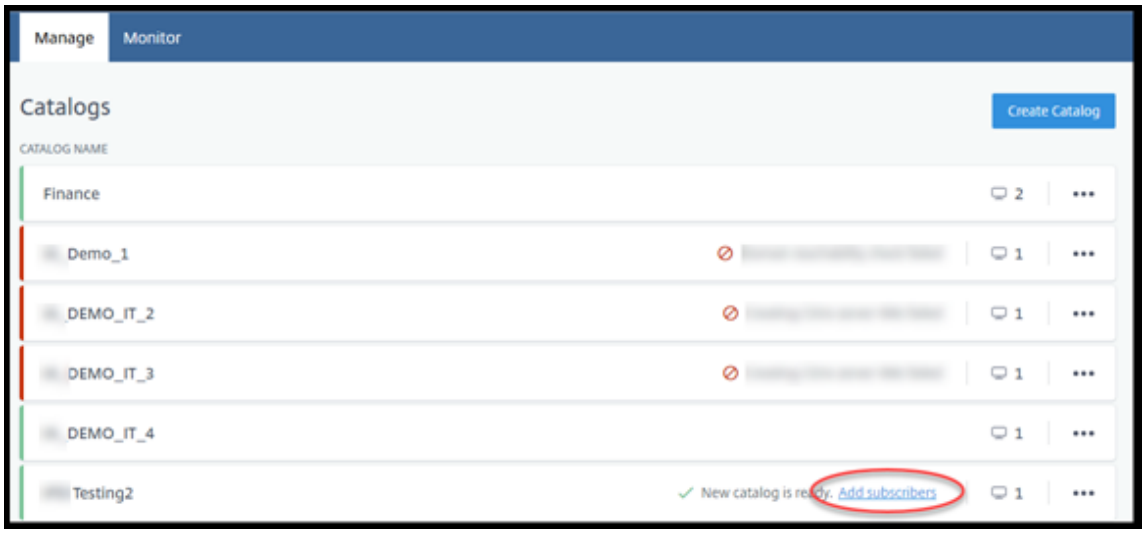
イコンをクリックします。削除を確認します。

次の手順：カタログにユーザーを追加する

カタログでユーザーを追加または削除する

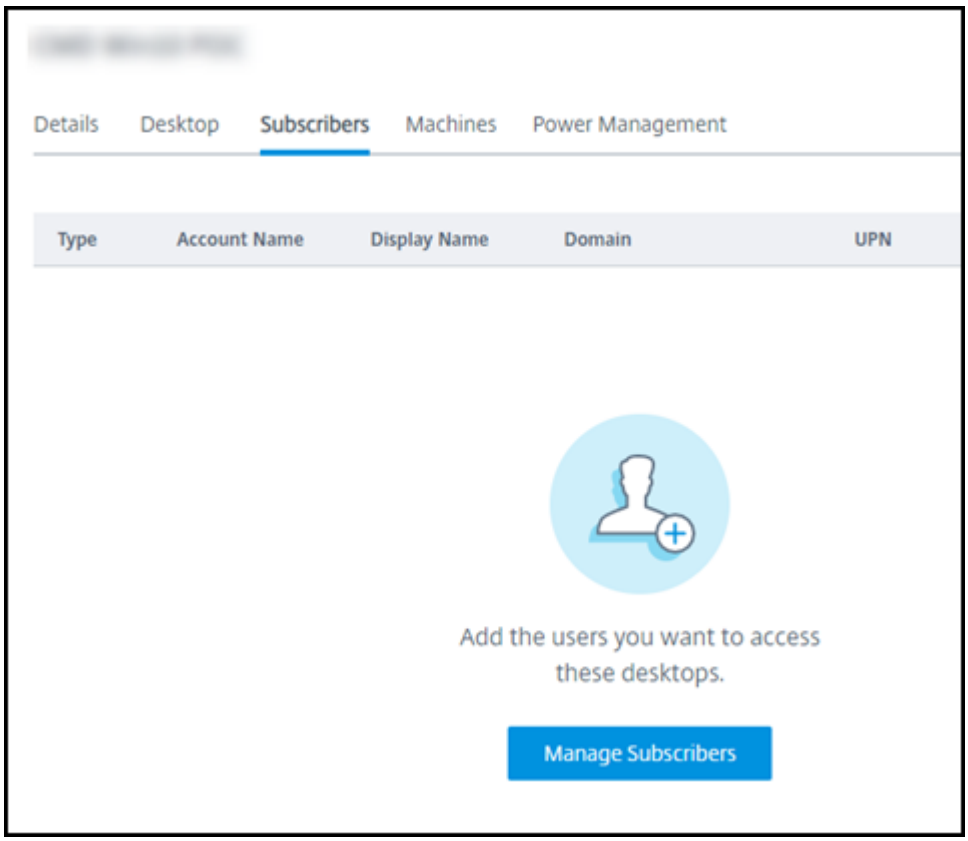
使用する認証方法に関係なく、この手順を実行します。

1. サービスの [管理] ダッシュボードで、カタログにユーザーを追加していない場合は、[登録者の追加] をクリックします。

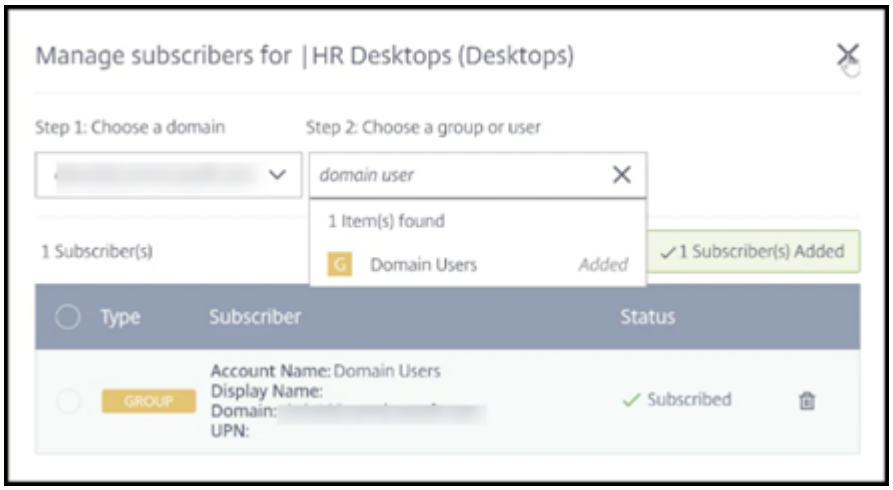


   すでにユーザーがあるカタログにユーザーを追加するには、カタログのエントリの任意の場所をクリックします。

2. [サブスクライバー] タブで、**[**** サブスクライバーの管理 **] をクリックします。



3. ドメインを選択します。マネージド Azure AD をユーザー認証に使用している場合、ドメインフィールドには 1 つのエントリしかありません。次に、ユーザーを選択します。



4. 必要に応じて、他のユーザーを選択します。完了したら、右上隅の [**X**] をクリックします。

カタログからユーザーを削除するには、手順 1 と 2 を実行します。手順 3 で、（ドメインとグループ/ユーザーを選択する代わりに）削除する名前の横にあるゴミ箱アイコンをクリックします。この操作は、ソース（管理対象 Azure AD、独自の AD または AAD など）からではなく、カタログからユーザーを削除します。

次の手順:

- マルチセッションマシンがあるカタログの場合、アプリケーションを追加（まだ存在していない場合）。
- すべてのカタログについて、ユーザーにCitrix Workspace URL を送信する。

詳細情報

Citrix Cloud での認証の詳細については、「ID およびアクセス管理」を参照してください。

カタログの管理

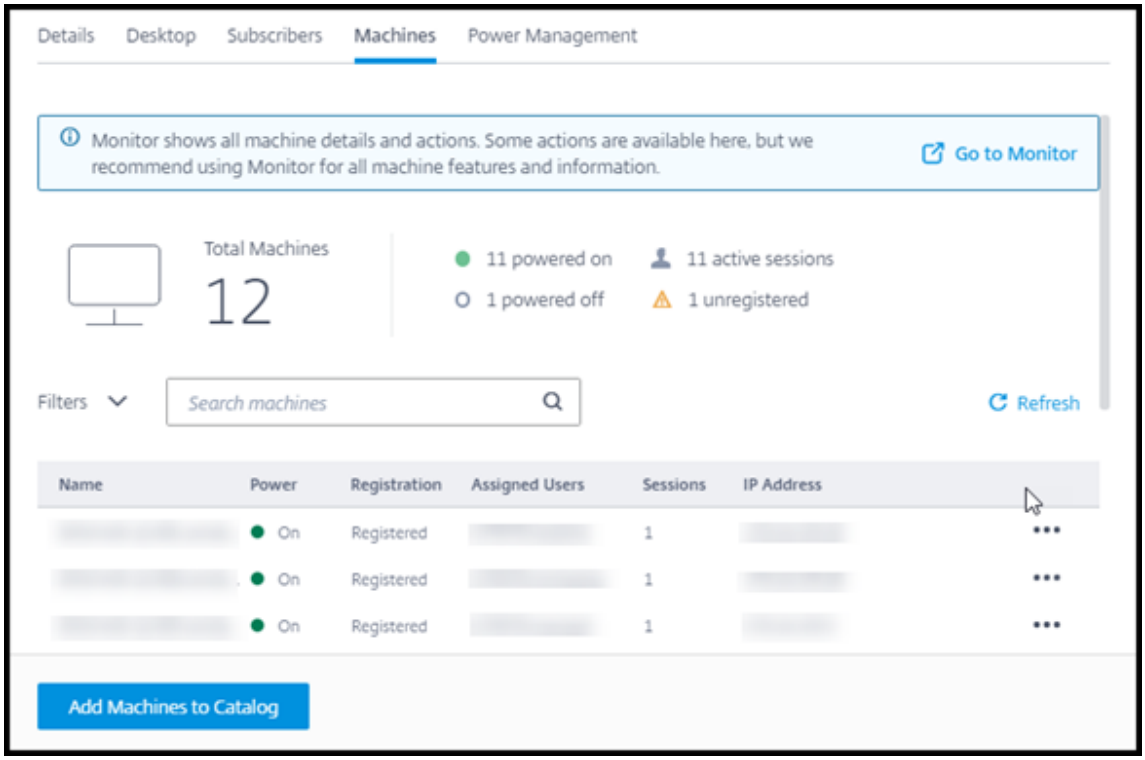
July 16, 2021

この記事では、カタログを管理するタスクについて説明します。

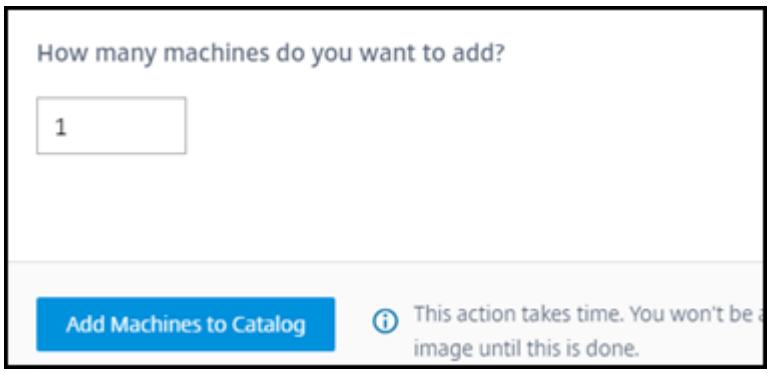
カタログへのマシンの追加

マシンをカタログに追加している間は、そのカタログに他の変更を加えることはできません。

1. サービスの [管理] ダッシュボードから、カタログのエントリの任意の場所をクリックします。
2. ［マシン］タブで、［マシンをカタログに追加］をクリックします。



3. カタログに追加するマシンの数を入力します。



4. (カタログがドメインに参加している場合にのみ有効です)。サービスアカウントのユーザー名とパスワードを入力します。
5. [マシンをカタログに追加] をクリックします。

カタログのマシン数を減らすことはできません。ただし、電源管理のスケジュール設定を使用して、電源をオンにするマシンの数を制御できます。

マシンあたりのセッション数を変更する

マルチセッションマシンあたりのセッション数を変更すると、ユーザーのエクスペリエンスに影響を与える可能性があります。この値を大きくすると、同時セッションに割り当てられるコンピューティングリソースが削減されます。推奨事項: 使用状況データを観察して、ユーザーエクスペリエンスとコストの適切なバランスを判断します。

1. サービスの [管理] ダッシュボードから、マルチセッションマシンを含むカタログを選択します。
2. [詳細] タブで、[マシンごとのセッション] の横にある [編集] をクリックします。
3. マシンごとに新しいセッション数を入力します。
4. [セッション数の更新] をクリックします。
5. リクエストを確認します。

この変更は、現在のセッションには影響しません。セッションの最大数をマシンの現在アクティブなセッションよりも低い値に変更すると、新しい値はアクティブなセッションの通常の減少によって実装されます。

更新プロセスが開始する前に障害が発生した場合、カタログの [詳細] 表示には正しいセッション数が保持されます。更新プロセス中に障害が発生した場合、表示には必要なセッション数が表示されます。

カタログ内のマシンを管理する

> 注:
>
> [管理] ダッシュボードから使用できるアクションの多くは、[監視] ダッシュボードからも使用できます。

管理ダッシュボードからアクションを選択するには:

1. [管理] ダッシュボードから、カタログのエントリの任意の場所をクリックします。

2. [マシン] タブで、管理するマシンを見つけます。そのマシンの省略記号メニューで、目的のアクションを選択します。

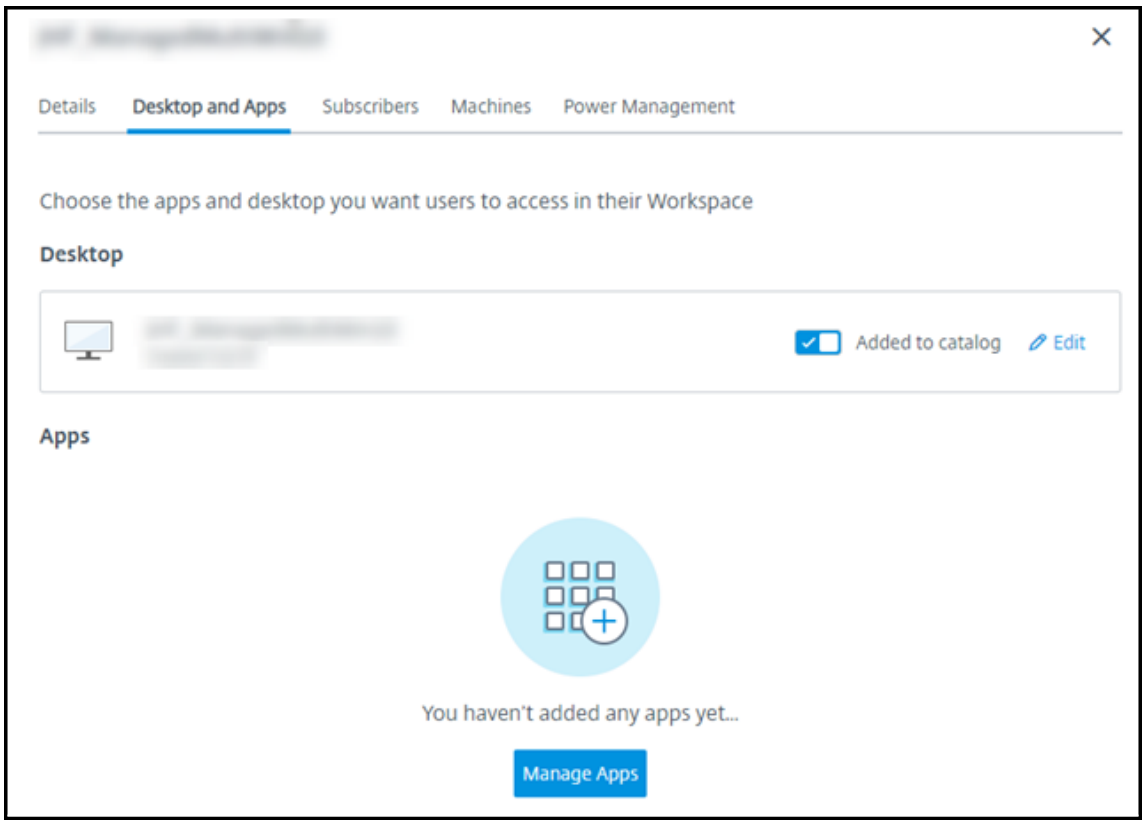
   - 再起動**:** 選択したマシンを再起動します。
   - 開始**:** 選択したマシンを起動します。この操作は、マシンの電源がオフになっている場合にのみ使用できます。
   - シャットダウン**:** 選択したマシンをシャットダウンします。この操作は、マシンの電源が入っている場合にのみ使用できます。
   - メンテナンスモードをオン**/**オフにする：選択したマシンのメンテナンスモードをオンにする（オフの場合）またはオフ（オンの場合）にします。

     デフォルトでは、マシンのメンテナンスモードはオフになっています。マシンのメンテナンスモードをオンにすると、そのマシンへの新しい接続が行われなくなります。ユーザーは、そのマシン上の既存のセッションに接続できますが、そのマシンで新しいセッションを開始することはできません。パッチを適用する前に、またはトラブルシューティングを行う前に、マシンをメンテナンスモードにすることができます。
   - 削除**:** 選択したマシンを削除します。この操作は、マシンのセッション数がゼロの場合にのみ使用できます。削除を確認します。

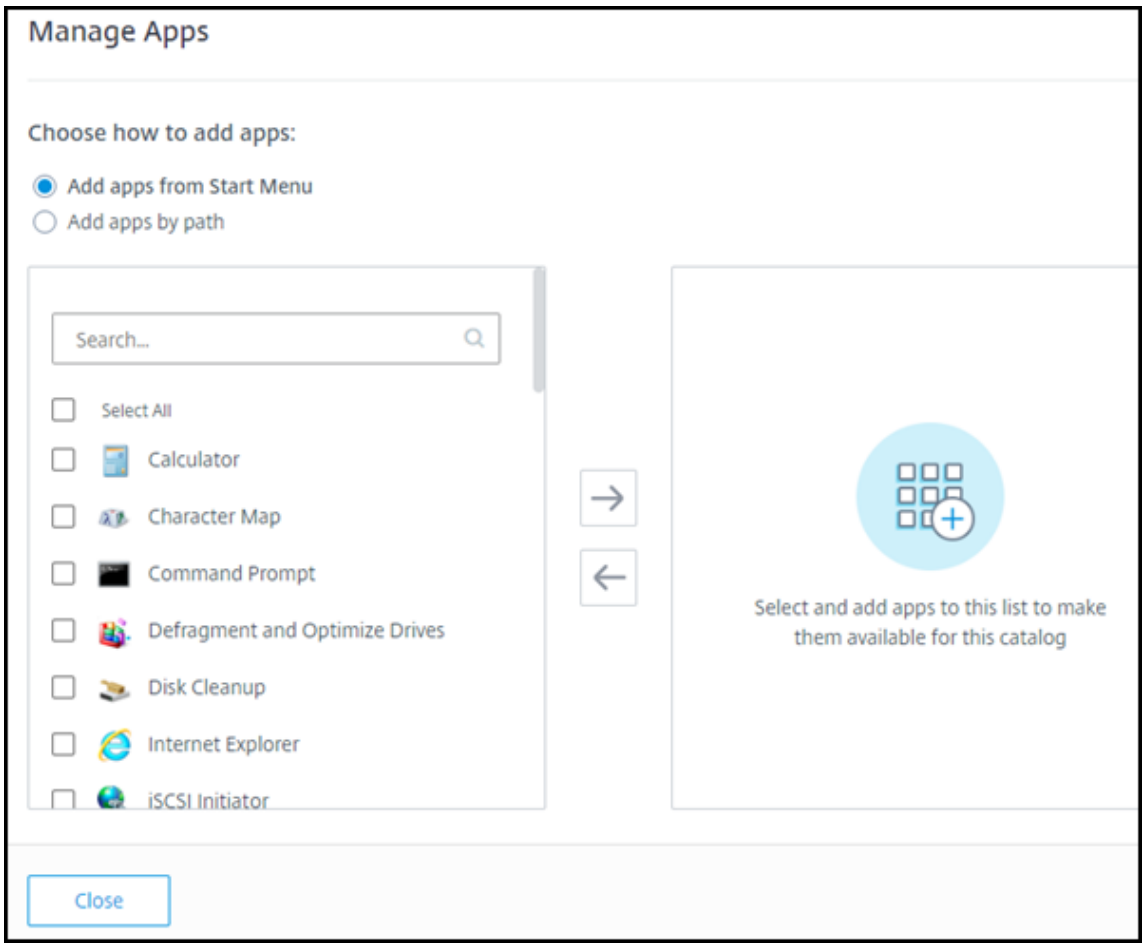
     マシンを削除すると、そのマシン上のすべてのデータが削除されます。
   - 強制再起動**:** 選択したマシンを強制的に再起動します。このアクションは、マシンの [再起動] 操作が失敗した場合にのみ選択します。

カタログへのアプリの追加

1. サービスの [管理] ダッシュボードから、カタログのエントリの任意の場所をクリックします。
2. [デスクトップとアプリ] タブで、[アプリの管理] をクリックします。

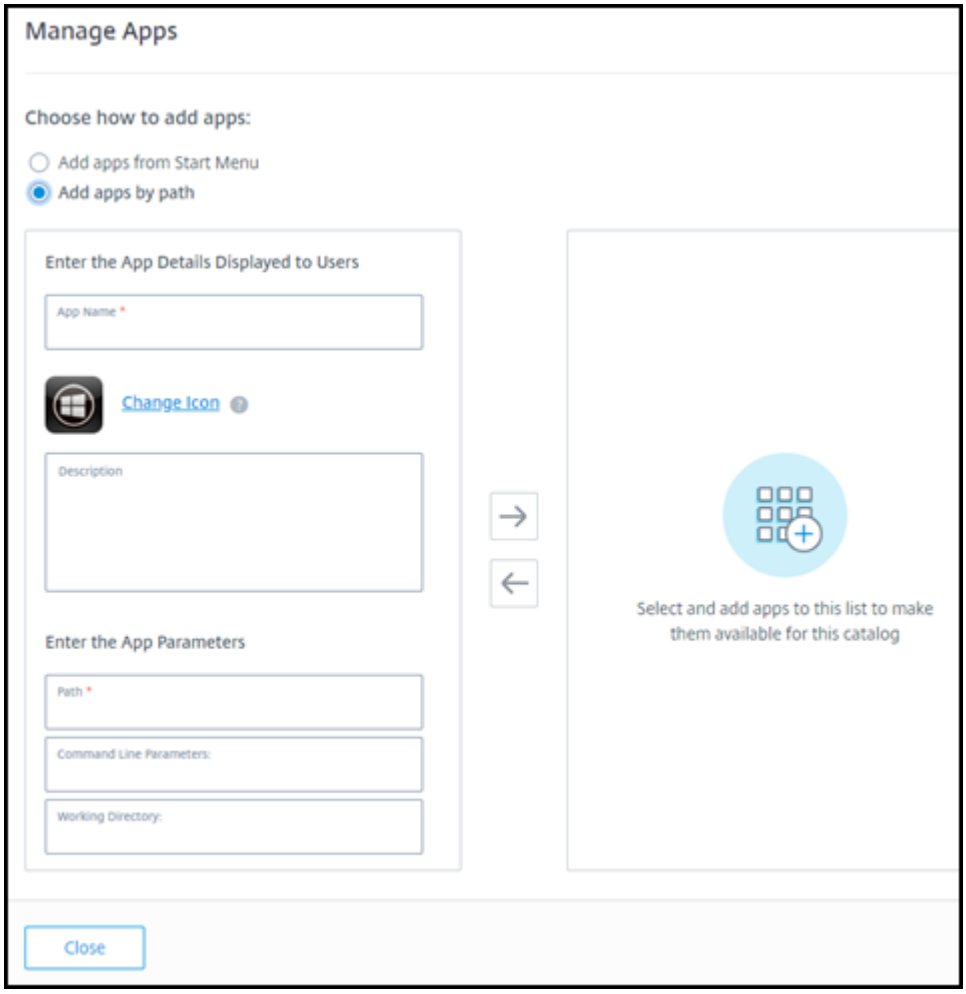


3. アプリケーションの追加方法を選択します。カタログ内のマシンの [スタート] メニュー、またはマシン上の別のパスから選択します。
4. [スタート] メニューからアプリを追加するには:



- 左側の列で利用可能なアプリを選択します。([検索] を使用して、アプリのリストをカスタマイズします。) 列の間にある右矢印をクリックします。選択したアプリが右側の列に移動します。
- 同様に、アプリを削除するには、右側の列でアプリを選択します。列の間にある左矢印をクリックします。
- [スタート] メニューに、同じ名前の同じアプリの複数のバージョンがある場合は、1 つのみ追加できます。そのアプリの別のバージョンを追加するには、そのバージョンを編集して名前を変更します。次に、そのバージョンのアプリを追加できます。

5. パス別にアプリを追加するには:



- アプリの名前を入力します。これは、Citrix Workspace でユーザーに表示される名前です。
- 表示されるアイコンは、Citrix Workspace でユーザーに表示されるアイコンです。別のアイコンを選択するには、[アイコンの変更] をクリックし、表示するアイコンに移動します。
- (オプション) アプリケーションの説明を入力します。
- アプリのパスを入力します。このフィールドは必須です。オプションで、コマンドラインパラメータと作業ディレクトリを追加します。コマンドラインパラメータの詳細については、公開アプリケーションにパラメーターを渡すを参照してください。

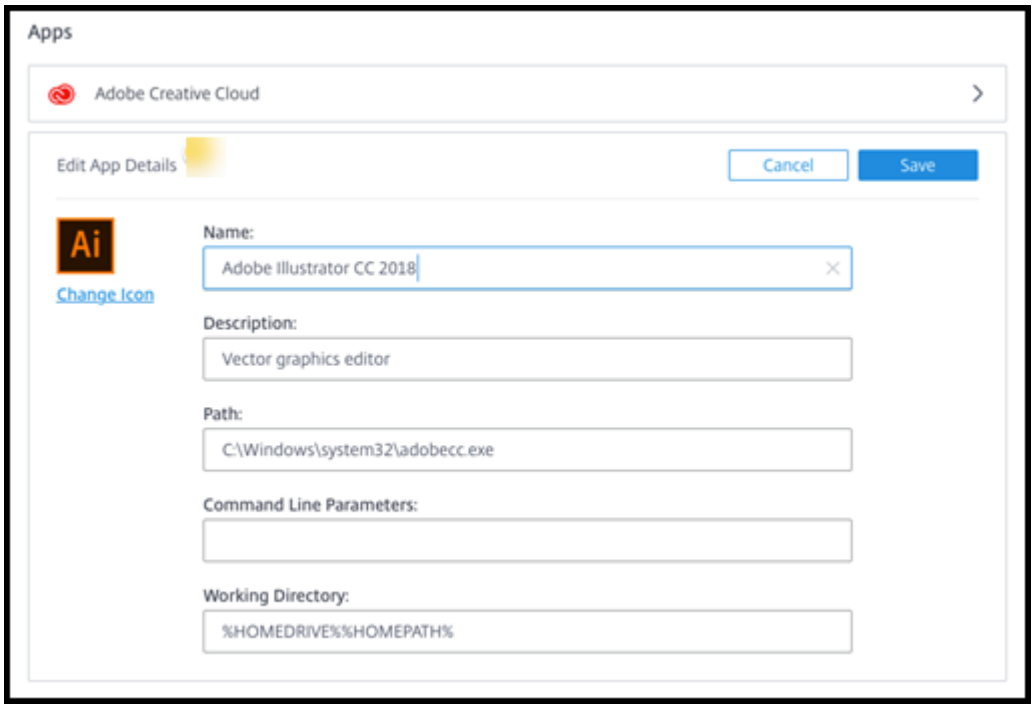
6. 完了したら、[閉じる] をクリックします。

次に何をすべきか (カタログの作成と配信のフローを完了している場合): ユーザーに Citrix Workspace の URL を送信、まだ行っていない場合。

Windows Server 2019 VDA では、構成中およびユーザーのワークスペースに一部のアプリケーションアイコンが正しく表示されないことがあります。回避策として、アプリが公開された後、アプリを編集 し、アイコンの変更機能を使用して、正しく表示される別のアイコンを割り当てます。

カタログ内のアプリの編集

1. サービスの [管理] ダッシュボードから、カタログのエントリの任意の場所をクリックします。
2. [デスクトップとアプリ] タブで、編集するアプリを含む行の任意の場所をクリックします。
3. 鉛筆アイコンをクリックします。



4. 次のいずれかのフィールドに変更を入力します。
   - 名前： Citrix Workspace でユーザーに表示される名前。
   - 説明
   - **Path:** 実行可能ファイルへのパス。
   - コマンドラインパラメータ**:** 詳細については、公開アプリケーションにパラメーターを渡すを参照してください。
   - 作業ディレクトリ
5. Citrix **Workspace** でユーザーに表示されるアイコンを変更するには、［変更］アイコンをクリックし、表示するアイコンに移動します。
6. 完了したら、[保存] をクリックします。

公開アプリケーションにパラメーターを渡す

公開アプリケーションをファイルタイプに関連付けると、パーセント記号と星記号 (二重引用符で囲む) がコマンドラインの最後に追加されます。これらの記号は、ユーザーデバイス側に渡されるパラメーターのプレースホルダーとして機能します。

- ファイルタイプに関連付けられている公開アプリケーションが起動しない場合は、記号が正しくコマンドラインに含まれていることを確認してください。デフォルトでは、ユーザーデバイスによって提供されるパラメーターは、シンボルが追加されたときに検証されます。

  ユーザーデバイスによって提供されるカスタマイズされたパラメータを使用する公開アプリケーションでは、コマンドライン検証をバイパスするために、シンボルがコマンドラインに追加されます。コマンドラインにこれらの記号が含まれていない場合は、手作業で追加できます。

- 実行可能ファイルのパスに、「C:\Program Files」のようなスペースを使ったフォルダー名が含まれている場合は、アプリケーションのコマンドラインを二重引用符で囲み、このスペースがコマンドラインに属していることを示します。パスの周りに二重引用符を追加し、パーセント記号と星記号の周りに別の二重引用符を追加します。パスの終了引用符と、パーセント記号と星記号の開始引用符の間にスペースを追加します。

  たとえば、公開アプリケーション Windows Media Player のコマンドラインは次のようになります: `“C:\Program Files\Windows Media Player\mplayer1.exe” “%*”`

カタログからアプリを削除する

カタログからアプリを削除しても、マシンからは削除されません。Citrix Workspace に表示されないようにするだけです。

1. サービスの [管理] ダッシュボードから、カタログのエントリの任意の場所をクリックします。
2. [デスクトップとアプリ] タブで、削除するアプリの横にあるごみ箱アイコンをクリックします。

カタログの削除

カタログを削除すると、カタログ内のすべてのマシンが完全に破棄されます。カタログの削除を元に戻すことはできません。

1. サービスの [管理] ダッシュボードから、カタログのエントリの任意の場所をクリックします。
2. [詳細] タブで、ウィンドウの下部にある [カタログの削除] をクリックします。
3. 確認のチェックボックスをオンにし、確認ボタンをクリックして、削除を確認します。

削除する必要のある残存の Active Directory マシンアカウントを特定するために、マシン名と Cloud Connector の名前のリストをダウンロードできます。

電源管理スケジュールの管理

電源管理のスケジュールは、カタログ内のすべてのマシンに影響します。スケジュールは次のものを提供します。

- 最適なユーザーエクスペリエンス: マシンは、必要なときに利用できます。
- セキュリティ: 指定した間隔の間アイドル状態のデスクトップセッションは切断され、ユーザーはワークスペースで新しいセッションを起動する必要があります。
- コスト管理と省電力: アイドル状態のデスクトップがあるマシンの電源がオフになります。スケジュールされた需要と実際の需要を満たすために、マシンの電源が投入されます。

電源スケジュールは、カスタムカタログの作成時に設定することも、後で行うこともできます。スケジュールが選択または構成されていない場合、セッションが終了するとマシンの電源がオフになります。

クイック作成を使用してカタログを作成するときに、電源スケジュールを選択または構成することはできません。デフォルトでは、簡易作成カタログでは、コスト節約プリセットスケジュールが使用されます。そのカタログについて、後で別のスケジュールを選択または構成できます。

スケジュール管理には以下が含まれます。

- スケジュールにどのような情報が含まれているかを知る
- スケジュールの作成

スケジュールの情報

次の図は、マルチセッションマシンを含むカタログのスケジュール設定を示しています。シングルセッション（ランダムまたは静的）マシンを含むカタログの設定は、若干異なります。

電源管理スケジュールには、次の情報が含まれています。

プリセットスケジュール

このサービスは、いくつかのプリセットスケジュールを提供しています。カスタムスケジュールを設定して保存することもできます。カスタムプリセットは削除できますが、Citrix が提供するプリセットは削除できません。

タイムゾーン

[マシンのパワーオン] 設定とともに使用し、選択したタイムゾーンに基づいて作業時間と時間外に作業時間を設定します。

この設定は、すべての種類のマシンに対して有効です。

マシンの電源投入**:** 作業時間と時間後

勤務時間を形成する曜日と開始停止時間。これは通常、マシンの電源をオンにする間隔を示します。これらの間隔外の時間は時間外とみなされます。複数のスケジュール設定により、勤務時間と営業時間外に別々の値を入力できます。他の設定も常に適用されます。

この設定は、すべての種類のマシンに対して有効です。

アイドル時にデスクトップセッションを切断する

セッションが切断される前に、デスクトップがアイドル状態（未使用）にできる期間。セッションが切断された後、ユーザーは Workspace に移動してデスクトップを再起動する必要があります。これはセキュリティ設定です。

この設定は、すべての種類のマシンに対して有効です。1 つの設定が常に適用されます。

アイドル状態のデスクトップの電源を切る

マシンの電源がオフになるまでの間、切断したままにできる期間。マシンの電源がオフになったら、ユーザーは Workspace に移動してデスクトップを再起動する必要があります。これは省電力設定です。

たとえば、デスクトップが 10 分間アイドル状態になった後に切断するとします。その後、マシンがさらに 15 分間切断されたままの場合は、マシンの電源を切ります。

トムがデスクトップの使用をやめ、1 時間のミーティングに出かけると、10 分後にデスクトップが切断されます。さらに 15 分後、マシンの電源がオフになります（合計 25 分）。

ユーザーから見ると、2 つのアイドル設定 (切断と電源オフ) は同じ効果を持ちます。トムがデスクトップから 12 分または 1 時間離れていれば、Workspace から再びデスクトップを起動する必要があります。2 つのタイマーの違いは、デスクトップを提供する仮想マシンの状態に影響します。

この設定は、シングルセッション（静的またはランダム）マシンで有効です。勤務時間および時間外の値を入力できます。

切断されたセッションをログオフする

セッションを閉じる前に、マシンを切断したままにできる期間。

この設定は、マルチセッションマシンで有効です。1 つの設定が常に適用されます。

電源オフ遅延

マシンの電源がオフになるまでの最小パワーオン時間（他の基準とともに）。この設定により、揮発性のセッション要求時にマシンが「フリップフロッピング」をオンまたはオフさせないようにします。

この設定はマルチセッションマシンで有効で、常に適用されます。

最小稼働マシン数

アイドル状態または切断されている期間に関係なく、電源をオンにしておく必要があるマシンの数はいくつですか。

この設定は、ランダムおよびマルチセッションマシンで有効です。勤務時間および時間外の値を入力できます。

キャパシティバッファ

キャパシティバッファは、マシンのバッファをパワーオンしたままにすることで、需要の急増に対応するのに役立ちます。バッファは、現在のセッション需要に対するパーセンテージで指定します。たとえば、アクティブなセッションが 100 個あり、処理能力バッファが 10%の場合、セッション 110 個分の処理能力が提供されます。需要の急増は、作業時間中に発生したり、カタログに新しいマシンを追加したりすることがあります。

値を小さくすると、コストが下がります。値を大きくすると、ユーザーエクスペリエンスの最適化が保証されます。セッションを起動するとき、ユーザーは追加のマシンの電源が入るのを待つ必要はありません。

カタログに必要な電源投入されたマシンの数 (容量バッファを含む) をサポートするのに十分な数を超えるマシンがある場合、追加のマシンの電源がオフになります。オフピーク時間、セッションログオフ、カタログ内のマシン数が少ないために電源オフが発生することがあります。マシンの電源を切る決定は、次の基準を満たす必要があります。

- マシンの電源はオンになっていて、メンテナンスモードではありません。
- マシンが利用可能として登録されているか、電源投入後に登録を待っている。
- マシンにはアクティブなセッションがありません。残りのセッションはすべて終了しました。（アイドルタイムアウト期間中はマシンがアイドル状態でした）。
- マシンの電源が少なくとも「X」分間オンされています。ここで、「X」はカタログに指定されている電源オフ遅延です。

  静的カタログでは、カタログ内のすべてのマシンが割り当てられた後、キャパシティバッファはマシンの電源をオンまたはオフにする役割を果たしません。

この設定は、すべての種類のマシンに対して有効です。勤務時間および時間外の値を入力できます。

電源管理スケジュールの作成

1. サービスの [管理] ダッシュボードから、カタログのエントリの任意の場所をクリックします。
2. [電源管理] タブで、あらかじめ設定されたスケジュール（上部のメニュー）のいずれかがニーズを満たしているかどうかを確認します。プリセットを選択して、使用する値を確認します。プリセットを使用する場合は、選択したままにします。

3. 任意のフィールド (日、時間、間隔など) の値を変更すると、プリセット選択は自動的にカスタムに変わります。アスタリスクは、カスタム設定が保存されていないことを示します。
4. カスタムスケジュールに必要な値を設定します。
5. 上部の [カスタム] をクリックし、[現在の設定を新しいプリセットとして保存] をクリックします。新しいプリセットの名前を入力し、チェックマークをクリックします。
6. 完了したら、[変更を保存] をクリックします。

後で、プリセットメニューの鉛筆アイコンまたはゴミ箱アイコンを使用して、カスタムプリセットを編集または削除できます。一般的なプリセットを編集または削除することはできません。

関連情報

- 新しいイメージでカタログを更新
- カタログ内のユーザーの追加と削除
- ドメイン参加と非ドメイン参加

モニター

July 16, 2021

モニターダッシュボードから、Citrix Virtual Apps and Desktops Standard for Azure 展開のデスクトップの使用状況、セッション、およびマシンを表示できます。また、セッションの制御、マシンの電源管理、実行中のアプリケーションの終了、実行中のプロセスの終了も可能です。

モニタダッシュボードにアクセスするには、次の手順に従います。

1. まだログインしていない場合は、Citrix Cloudにサインインします。左上のメニューで、[マイサービス] > **[Azure** の **Virtual Apps and Desktops**] の順に選択します。
2. サービスの [管理] ダッシュボードから、[監視] タブをクリックします。

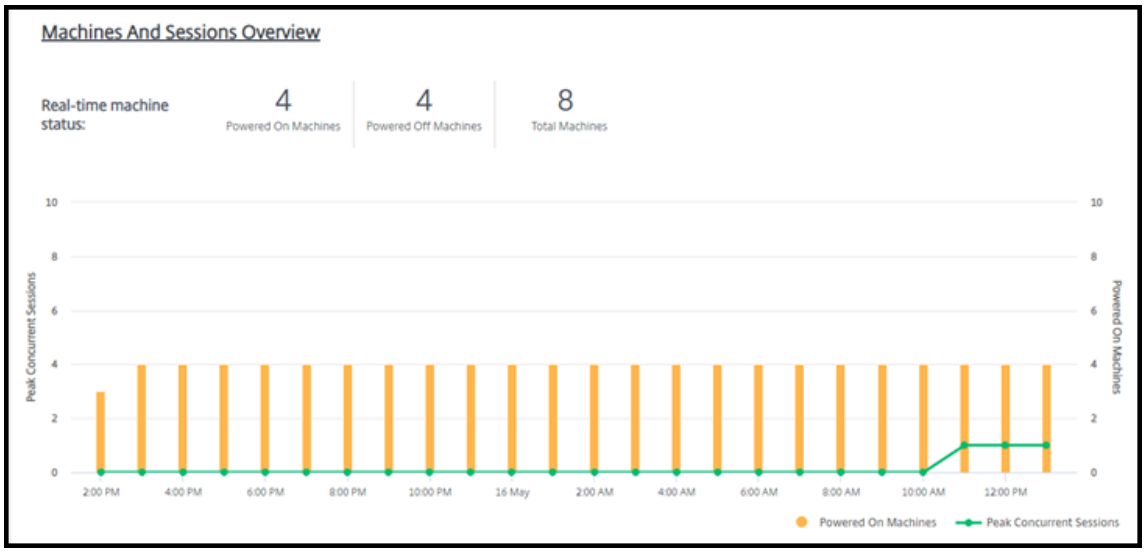
デスクトップの使用状況の監視

[監視] タブをクリックすると、[サービス使用状況] ページがデフォルトで表示されます。このページの表示は 5 分ごとに更新されます。

- マシンとセッションの概要：すべてのカタログ（デフォルト）または選択したカタログに関する情報を表示するように表示を調整できます。また、期間を、過去 1 日間、1 週間、1 か月間、または 3 か月間のいずれかに調整できます。

  ディスプレイの上部にある数には、マシンの総数と、電源が入っているマシンと電源がオフになっているマシンの数が表示されます。値の上にマウスポインターを置くと、単一セッションとマルチセッションの数が表示されます。

カウント下のグラフには、選択した期間中の通常のポイントでのパワーオン状態のマシンとピーク同時セッションの数が表示されます。グラフのポイントにカーソルを合わせると、そのポイントでのカウントが表示されます。



- 上位 **10:** 上位 10 のディスプレイをカスタマイズするには、過去 1 週間 (デフォルト)、月、または 3 か月の期間を選択します。また、シングルセッションマシン、マルチセッションマシン、またはアプリケーションに関連するアクティビティに関する情報のみを表示するようにディスプレイを調整することもできます。
  - アクティブユーザーの上位 **10:** 期間中にデスクトップを最も頻繁に起動したユーザーの一覧を表示します。行にカーソルを合わせると、合計起動数が表示されます。
  - アクティブなカタログの上位 **10:** 選択した期間内に最も長い期間を持つカタログを一覧表示します。期間は、そのカタログからのすべてのユーザーセッションの合計です。

デスクトップ使用状況レポート

先月のマシンの起動に関する情報を含むレポートをダウンロードするには、[アクティビティの起動] をクリックします。要求が処理中であることを示すメッセージが表示されます。レポートは、ローカルマシンのデフォルトのダウンロード場所に自動的にダウンロードされます。

フィルターと検索してマシンとセッションを監視する

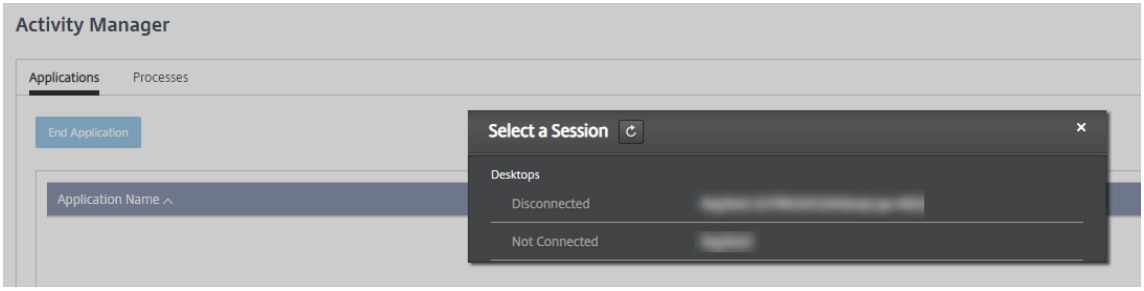
セッションとマシンの情報を監視しているときは、デフォルトですべてのマシンまたはセッションが表示されます。次の操作を実行できます:

- マシン、セッション、接続、またはアプリケーションによってディスプレイをフィルタリングします。
- 必要な条件を選択し、式を使用してフィルタを構築して、セッションまたはマシンの表示を絞り込みます。
- 作成したフィルタを保存して、再利用します。

ユーザーのアプリケーションを制御する

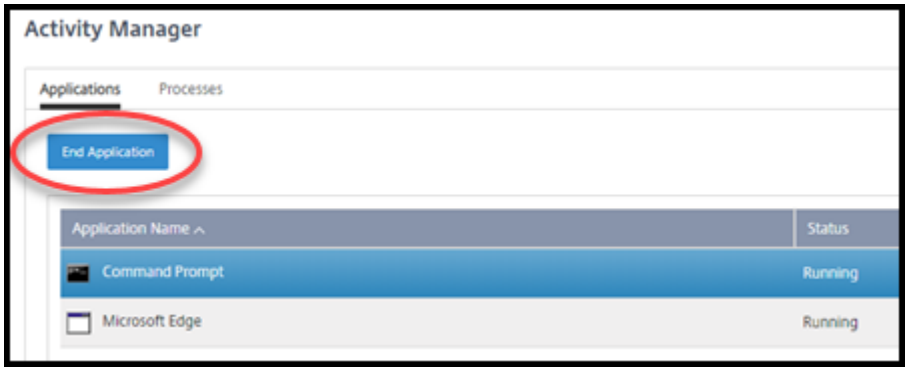
実行中のセッションまたはデスクトップが割り当てられているユーザーのアプリケーションとプロセスを表示および管理できます。

1. サービスの [監視] ダッシュボードから、[検索] をクリックし、ユーザー名 (またはユーザー名の先頭文字)、マシン、またはエンドポイントを入力します。検索結果から、探しているアイテムを選択します。検索せずに検索ボックスを折りたたむには、もう一度 [検索] をクリックします。)
2. セッションを選択します。



アクティビティマネージャには、ユーザーのセッションのアプリケーションとプロセスが一覧表示されます。

3. アプリケーションを終了するには、アクティビティマネージャの [アプリケーション] タブで、アプリケーションの行をクリックしてそのアプリケーションを選択し、[アプリケーションの終了] をクリックします。



4. プロセスを終了するには、アクティビティマネージャの [プロセス] タブで、プロセスの行をクリックしてそのプロセスを選択し、[プロセスの終了] をクリックします。
5. セッションの詳細を表示するには、右上の [詳細] をクリックします。アプリケーションとプロセスの表示に戻るには、右上にある [アクティビティマネージャ] をクリックします。
6. セッションを制御するには、セッションコントロール **>** ログオフまたはセッションコントロール **>** 切断をクリックします。

ユーザーのシャドウ

シャドウ機能を使用して、ユーザーの仮想マシンまたはセッションを直接表示または操作します。Windows と Linux の VDA をシャドウできます。この機能を使用するには、そのマシンにユーザーが接続している必要がありま

す。User タイトルバーに表示されているマシン名を確認して、これを確認します。

シャドウイングは新しいブラウザータブで起動します。ブラウザで Citrix Cloud URL からのポップアップが許可されていることを確認します。

シャドウイングは、ドメインに参加しているマシン上のユーザーに対してのみサポートされます。ドメインに参加していないマシンをシャドウするには、踏み台マシンをセットアップする必要があります。詳しくは、「踏み台マシンへのアクセス」を参照してください。

シャドウイングは、ドメインに参加しているマシンと同じ仮想ネットワーク上のマシンから開始し、ポート要件も満たす必要があります。

シャドウイングを有効にする

1. モニターダッシュボードから、[ユーザーの詳細] ビューに移動します。
2. ユーザーセッションを選択し、[アクティビティマネージャ] ビューまたは [セッションの詳細] パネルで [シャドウ] をクリックします。

シャドウ **Linux VDA**

シャドウは、RHEL7.3 または Ubuntu バージョン 16.04 Linux ディストリビューションを実行する Linux VDA バージョン 7.16 以降で使用できます。

モニターは FQDN を使用してターゲットの Linux VDA に接続します。[監視] クライアントが Linux VDA の完全修飾ドメイン名を解決できるようにしてください。

- VDA には、python-websockifyおよびx11vnc パッケージがインストールされている必要があります。
- VDA へのnoVNC接続では、WebSocket プロトコルが使用されます。デフォルトでは、ws://WebSocket プロトコルが使用されます。セキュリティ上の理由から、セキュリティで保護されたwss://プロトコルをお勧めします。各監視クライアントおよび Linux VDA に SSL 証明書をインストールします。

セッションシャドウイングの指示に従って、Linux VDA をシャドウイング用に構成します。

1. シャドウイングを有効にすると、シャドウ接続が初期化され、ユーザーデバイスに確認プロンプトが表示されます。
2. ユーザーが [はい] をクリックすると、マシンまたはセッションの共有が開始されます。
3. 管理者は、シャドウセッションのみを表示できます。

シャドウ **Windows VDA**

Windows VDA セッションは、Windows リモートアシスタンスを使用してシャドウされます。VDA のインストール時にこのUse Windows Remote Assistance機能を有効にします。

1. シャドウイングを有効にすると、シャドウ接続が初期化され、.msrc incident ファイルを開くか保存するかどうかを確認するダイアログボックスが表示されます。

2. デフォルトで選択されていない場合は、リモートアシスタンスビューアでインシデントファイルを開きます。ユーザーデバイス側には、確認のメッセージが表示されます。
3. ユーザーが ［はい］ をクリックすると、マシンまたはセッションの共有が開始されます。
4. ユーザーがマウスやキーボードの制御を許可すると、管理者がシャドウセッションを制御できるようになります。

セッションの監視と制御

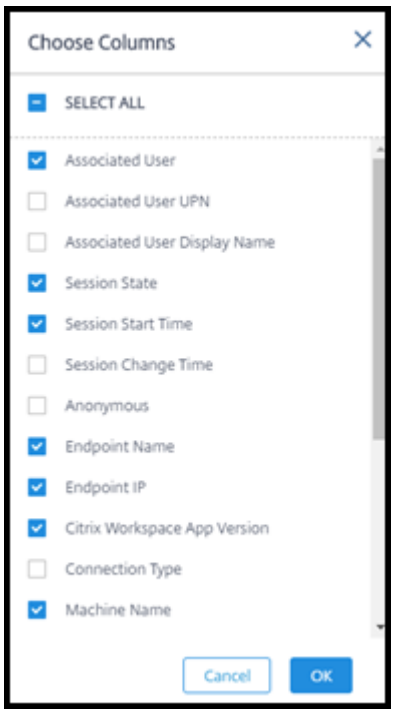
セッションの表示は毎分更新されます。

セッションの表示に加えて、1 つまたは複数のセッションを切断したり、セッションからユーザーをログオフしたりできます。

1. サービスの [監視] ダッシュボードから、[フィルタ] をクリックします。

2. [セッション] ビューを選択します。

3. 表示をカスタマイズするには、[列の選択] をクリックし、表示する項目のチェックボックスをオンにします。完了したら、「**OK**」をクリックします。セッションの表示は自動的に更新されます。



4. 制御する各セッションの左側にあるチェックボックスをクリックします。
5. セッションをログオフまたは切断するには、[セッションコントロール] **>** [ログオフ] または [セッションコントロール] **>** [切断] を選択します。

カタログの電源管理スケジュールでは、セッションの切断および切断されたセッションからのユーザーのログオフも制御できます。

上記の手順の代わりに、ユーザーを検索し、制御するセッションを選択し、セッションの詳細を表示することもできます。ログオフオプションと切断オプションも利用できます。

セッション情報レポート

セッション情報をダウンロードするには、セッション画面の [エクスポート] をクリックします。要求が処理中であることを示すメッセージが表示されます。レポートは、ローカルマシンのデフォルトのダウンロード場所に自動的にダウンロードされます。

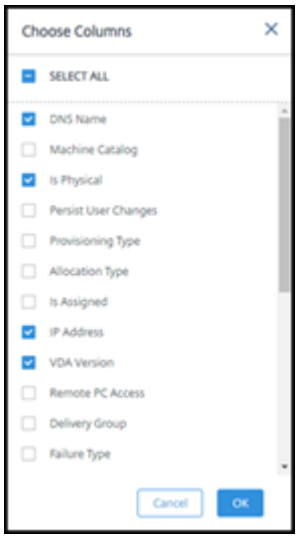
マシンの監視および電源管理

マシンの画面は、1 分ごとに更新されます。

1. サービスの [監視] ダッシュボードから、[フィルタ] をクリックします。
2. [マシン] ビューを選択します。

デフォルトでは、シングルセッションの OS マシンが一覧表示されます。または、マルチセッションマシンを表示することもできます。

3. 表示をカスタマイズするには、[列の選択] をクリックし、表示する項目のチェックボックスをオンにします。完了したら、「**OK**」をクリックします。マシンの表示は自動的に更新されます。



4. マシンの電源制御やメンテナンスモードへの切り替えには、制御する各マシンの左側にあるチェックボックスをオンにします。
5. 選択したマシンの電源制御を実行するには、[電源制御] をクリックし、アクションを選択します。

6. 選択したマシンをメンテナンスモードまたはメンテナンスモードに切り替えるには、メンテナンスモード **>** オン、またはメンテナンスモード **>** オフをクリックします。

検索機能を使用してマシンを検索して選択すると、マシンの詳細、使用率、過去 7 日間の使用率、および平均 IOPS が表示されます。

マシン情報レポート

セッション情報をダウンロードするには、マシン画面の [エクスポート] をクリックします。要求が処理中であることを示すメッセージが表示されます。レポートは、ローカルマシンのデフォルトのダウンロード場所に自動的にダウンロードされます。

アプリとデスクトップの正常性の確認

プロービングは、公開アプリとデスクトップの正常性をチェックするプロセスを自動化します。ヘルスチェックの結果は、**Monitor** ダッシュボードから入手できます。詳しくは、次のページを参照してください:

- アプリケーションプロービング
- デスクトッププロービング

Citrix サービスプロバイダ向け Citrix Virtual Apps and Desktops Standard for Azure

July 16, 2021

この記事では、Citrix サービスプロバイダー（CSP）が Citrix Cloud でテナント顧客向けの Citrix Virtual Apps and Desktops Standard for Azure サービスをセットアップする方法について説明します。

シトリックスパートナーが使用できる機能の概要については、「パートナー向けの Citrix Cloud」を参照してください。

要件

- Citrix Service Provider パートナーである。
- Citrix Cloud アカウントがある。
- Citrix Virtual Apps and Desktops Standard for Azure へのサブスクリプションがあること。

制限事項

- テナント名の変更は、すべてのインターフェイスに適用されるまで最大 24 時間かかる場合があります。
- テナントを作成する場合、電子メールアドレスは一意である必要があります。
- テナントによる管理フィルタリングは使用できません。テナントにアタッチされているリソースを表示するには、[アイテムの表示] でテナントを選択します。

- パートナーとテナントの顧客は、ドメインに参加したカタログを持つことができます。パートナーはドメインに参加していないカタログを持つことができますが、テナントの顧客はできません。

既知の問題

- テナントをリソースに割り当てた後は、それらのテナントを削除または割り当て解除することはできません。
- 管理コンソールでは、テナントユーザーの分離は強制されません。ユーザーは、適切なカタログおよびリソースにユーザーを追加する責任があります。
- Citrix Virtual Apps およびデスクトップ標準を顧客に追加した後、次の操作を行います。
  - 顧客から削除することはできません。
  - 顧客と Citrix Service Provider の間のリンクを削除することはできません。

顧客の追加

1. Citrix Service Provider の資格情報で Citrix Cloud にサインインします。左上のメニューにある［顧客］をクリックします。
2. カスタマーダッシュボードから、[招待] または [追加] をクリックします。要求される情報を指定します。

   顧客が Citrix Cloud アカウントを持っていない場合、顧客を追加すると顧客アカウントが作成されます。顧客を追加すると、管理者はその顧客のアカウントのフルアクセス管理者として自動的に追加されます。
3. 顧客が Citrix Cloud アカウントを持っている場合:
   a) Citrix Cloud の URL が表示されるので、これをコピーして顧客に送信します。このプロセスについて詳しくは、「顧客を接続に招待する」を参照してください。
   b) 顧客は自分のアカウントへのフルアクセス管理者として、管理者を追加する必要があります。「Citrix Cloud アカウントに管理者を追加する」を参照してください。

後で管理者を追加し、Citrix Virtual Apps and Desktops **Standard の管理および監視ダッシュボードで表示できる顧客を制御できます ** 。

Citrix Virtual Apps and Desktops Standard for Azure を顧客に追加する

1. Citrix Service Provider の資格情報で Citrix Cloud にサインインします。左上のメニューにある［顧客］をクリックします。
2. 「顧客」ダッシュボードで、顧客の省略記号メニューで「サービスの追加」を選択します。
3. ［追加するサービスの選択］で、［**Citrix Virtual Apps and Desktops Standard**］をクリックします。
4. ［続行］をクリックします。

この手順を完了すると、お客様は、Citrix Virtual Apps and Desktops Standard for Azure サブスクリプションにオンボーディングされます。

オンボーディングが完了すると、新しいテナントが Citrix Virtual Apps and Desktops Standard for Azure に自動的に作成されます。テナントは管理コンソールに表示されます。このテナントは、その顧客固有のものです。

顧客によるリソースのフィルタリング (マルチテナント展開)

Citrix Virtual Apps およびデスクトップ標準の管理ダッシュボードで、顧客ごとにリソースをフィルタリングできます。(デフォルトでは、すべてのリソースが表示されます)。カタログ、マシンイメージ、Azure サブスクリプションなどのリソースを操作する場合、特定の顧客ディスプレイを選択して、テナントのリソースを整理できます。

SD-WAN 接続は、テナントごとに作成されます。テナントには SD-WAN Orchestrator サービス資格が必要です。

- テナントの SD-WAN 接続を作成するには、SD-WAN 接続を作成するのガイダンスに従います。[ネットワーク接続の追加] ページで、テナントを選択します。[SD-WAN 接続タイプ] ボックスを選択できるのは、そのテナントに SD-WAN Orchestrator サービス資格がある場合のみです。
- 接続の作成を成功させるには、テナントにマスターコントロールノード (MCN) もインストールされている必要があります。ただし、SD-WAN 接続タイプを選択できるかどうかは SD-WAN オーケストレータサービス資格のみによって決定されます。

アプリケーションやデスクトップを配信するためのカタログの作成

カタログは、ユーザーのグループと、ユーザーがアクセスできる仮想マシンの集まりです。カタログを作成すると、マシンを作成するためのテンプレートとして（他の設定とともに）イメージが使用されます。詳しくは、「カタログを作成」を参照してください。

フェデレーションドメイン

フェデレーションドメインを使用すると、顧客ユーザーは、リソースの場所に関連付けられたドメインの資格情報を使用して、ワークスペースにサインインできます。リソースの場所は Citrix Cloud アカウントに残っている間、ユーザーがカスタムワークスペース URL（`customer.cloud.com`など）を介してアクセスできる専用のワークスペースを顧客に提供できます。

CSP ワークスペース URL (`csppartner.cloud.com`など) を使用して顧客がアクセスできる共有ワークスペースと一緒に専用のワークスペースを提供できます。カスタマーが専用のワークスペースにアクセスできるようにするには、管理する適切なドメインにユーザーを追加します。

ワークスペース構成でワークスペースを構成した後、顧客のユーザーはワークスペースにサインインして、利用可能にしたアプリとデスクトップにアクセスできます。

ドメインへの顧客の追加

1. Citrix Service Provider の資格情報で Citrix Cloud にサインインします。左上のメニューにある［顧客］をクリックします。

2. カスタマーダッシュボードから、左上のメニューで [**ID** とアクセス管理] を選択します。
3. ［ドメイン］タブで、ドメインの省略記号メニューにある ［フェデレーションドメインの管理］を選択します。
4. ［フェデレーションドメインの管理］カードの ［利用可能な顧客］列で、ドメインに追加する顧客を選択します。顧客名の横にあるプラス記号をクリックします。これで、選択した顧客が ［フェデレーション顧客］列に表示されるようになりました。繰り返し他の顧客を追加します。
5. 完了したら、［適用］をクリックします。

ドメインからの顧客の削除

管理しているドメインから顧客を削除すると、顧客のユーザーはドメインの資格情報を使用してワークスペースにアクセスできなくなります。

1. Citrix Cloud から、左上のメニューで［アイデンティティとアクセス管理］を選択します。
2. [ドメイン] タブで、管理するドメインの省略記号メニューから **[**フェデレーションドメインの管理] を選択します。
3. フェデレーション顧客のリストから、削除する顧客を検索または検索します。
   - [**X**] をクリックして、顧客を削除します。
   - リストされているすべての顧客をドメインから削除するには、[すべて削除] をクリックします。

   選択した顧客が [利用可能な顧客] のリストに移動します。
4. ［**Apply**］をクリックします。
5. 選択した顧客を確認し、[顧客の削除] をクリックします。

アクセスが制限された管理者の追加

1. Citrix Service Provider の資格情報で Citrix Cloud にサインインします。左上のメニューにある ［顧客］をクリックします。
2. カスタマーダッシュボードから、左上のメニューで [**ID** とアクセス管理] を選択します。
3. ［管理者］タブで、［追加する管理者の場所］を選択してから ［**Citrix ID**］を選択します。
4. 管理者として追加するユーザーのメールアドレスを入力して、［招待］をクリックします。
5. 管理者に適切なアクセス権限を設定します。Citrix Cloud およびサブスクライブされているすべてのサービスを管理者が管理できるようにする場合を除き、Citrix カスタムアクセス］を選択することをお勧めします。
6. 必要に応じて、Citrix Virtual Apps デスクトップ標準の役割とスコープのペアを 1 つ以上選択します。
7. 完了したら、[招待を送信] をクリックします。

管理者が招待を受け入れると、管理者は割り当てられたアクセス権を持つようになります。

管理者の委任管理権限の編集

1. Citrix Service Provider の資格情報で Citrix Cloud にサインインします。左上のメニューにある ［顧客］をクリックします。

2. カスタマーダッシュボードから、左上のメニューで [**ID** とアクセス管理] を選択します。
3. ［管理者］タブで、管理者の省略記号メニューから ［アクセスの編集］を選択します。
4. 必要に応じて、サービスのロールとスコープのペアを選択または選択解除します。顧客用に作成された一意のスコープを含むエントリのみを有効にしてください。
5. ［保存］をクリックします。

ワークスペースにアクセスして構成する

各テナントは、一意の`customer.cloud.com` URL を持つ独自のワークスペースを取得します。この URL は、顧客のユーザーが公開アプリおよびデスクトップにアクセスするための場所です。

- **Citrix Virtual Apps** およびデスクトップ標準から：［管理］ダッシュボードで、右側の［ユーザーアクセスと認証］を展開して URL を表示します。
- **Citrix Cloud** から：［カスタマー］ダッシュボードから、左上のメニューから［ワークスペース構成］を選択します。[アクセス] タブで URL を表示します。

ワークスペースへのアクセスと認証を変更できます。ワークスペースの外観と基本設定をカスタマイズすることも可能です。詳しくは、以下の記事を参照してください：

- ワークスペースの構成
- 安全なワークスペース

顧客のサービスの監視

CSP 環境での Citrix Virtual Apps およびデスクトップ標準モニターダッシュボードは、CSP 以外の環境と基本的に同じです。詳しくは、モニターを参照してください。

デフォルトでは、［監視］ダッシュボードにはすべての顧客に関する情報が表示されます。1 人の顧客に関する情報を表示するには、［顧客を選択します］を使用します。

顧客のモニターディスプレイを表示する機能は、管理者の構成されたアクセス権によって制御されることに注意してください。

トラブルシューティング

July 16, 2021

はじめに

リソースの場所には、デスクトップとアプリを配信するマシンが含まれます。これらのマシンはカタログ内に作成されるため、カタログはリソースの場所の一部と見なされます。各リソースの場所には Cloud Connector も含まれ

ます。Cloud Connector を使用すると、Citrix Cloud がリソースの場所と通信できるようになります。Citrix は Cloud Connector をインストールして更新します。

必要に応じて、Cloud Connector とリソースの場所の操作をいくつか開始できます。以下の情報も参照してください:

- リソースの場所の操作
- カタログ作成時のリソースの場所設定

このサービスには、デスクトップおよびアプリケーション（VDA）を配信するマシンとの構成および通信の問題を解決するのに役立つトラブルシューティングおよびサポートツールが用意されています。たとえば、カタログの作成に失敗したり、ユーザーがデスクトップやアプリを起動できない場合があります。

このトラブルシューティングには、踏み台マシンまたは直接 RDP を介して Citrix Managed Azure サブスクリプションにアクセスすることが含まれます。サブスクリプションにアクセスしたら、Citrix サポートツールを使用して問題を特定して解決できます。詳しくは、次のページを参照してください:

- 踏み台マシンまたは直接 RDP を使用した VDA のトラブルシューティング
- 踏み台マシンへのアクセス
- 直接 RDP アクセス

踏み台マシンまたは直接 **RDP** を使用した **VDA** のトラブルシューティング

サポート機能は、Citrix 問題のトラブルシューティング経験のあるユーザー向けです。以下が対象となります:

- Citrix サービスプロバイダー（CSP）および Citrix Virtual Apps およびデスクトップ製品に関する技術的な知識とトラブルシューティングの経験を持つその他。
- Citrix サポート担当者。

Citrix コンポーネントのトラブルシューティングに慣れていない、または慣れていない場合は、Citrix サポートにヘルプをリクエストできます。Citrix サポート担当者は、このセクションで説明するアクセス方法のいずれかを設定するよう求める場合があります。ただし、Citrix の担当者は、Citrix のツールとテクノロジーを使用して実際のトラブルシューティングを行います。

> 重要:
>
> これらのサポート機能は、ドメインに参加しているマシンでのみ有効です。カタログ内のマシンがドメインに参加していない場合は、Citrix サポートにトラブルシューティングのヘルプをリクエストするように指示されます。

アクセスメソッド

これらのアクセス方法は、Citrix Managed Azure サブスクリプションでのみ有効です。詳しくは、「Azure サブスクリプション」を参照してください。

2 つのサポート性アクセス方法が提供されています。

- お客様の専用 Citrix Managed Azure サブスクリプションの踏み台マシンを介してリソースにアクセスします。踏み台は、サブスクリプション内のマシンへのアクセスを許可する単一のエントリポイントです。指定された範囲の IP アドレスからのリモートトラフィックを許可することで、これらのリソースへのセキュアな接続を提供します。

  この方法のステップは次のとおりです。

  - 踏み台マシンを作成する
  - RDP エージェントをダウンロードする
  - 要塞マシンへの RDP
  - 踏み台マシンからサブスクリプション内の他の Citrix マシンに接続する

  踏み台マシンは短期間の使用を目的としています。この方法は、カタログまたはイメージマシンの作成に関する問題を対象としています。

- お客様の専用 Citrix Managed Azure サブスクリプションのマシンへの直接 RDP アクセス。RDP トラフィックを許可するには、ネットワークセキュリティグループにポート 3389 を定義する必要があります。

  この方法は、ユーザーがデスクトップを起動できないなど、作成以外のカタログの問題を対象としています。

注意：これら 2 つのアクセス方法の代わりに、Citrix サポートにヘルプを依頼してください。

踏み台マシンへのアクセス

1. サービスの [管理] ダッシュボードから、右側の [トラブルシューティングとサポート] を展開します。
2. ［トラブルシューティングオプションの表示］をクリックします。
3. [トラブルシューティング] ページで、最初の 2 つの問題のタイプのいずれかを選択し、[トラブルシューティングマシンを使用する] をクリックします。
4. [踏み台マシンを使用したトラブルシューティング] ページで、カタログを選択します。
   - 選択したカタログ内のマシンがドメインに参加していない場合は、Citrix サポートに連絡するように指示されます。
   - 選択したカタログのネットワーク接続への RDP アクセスで踏み台マシンがすでに作成されている場合は、手順 8 に進みます。
5. RDP アクセス範囲が表示されます。RDP アクセスをネットワーク接続で許可されている範囲よりも小さい範囲に制限する場合は、**[IP** アドレス範囲のコンピューターのみに **RDP** アクセスを制限する] チェックボックスをオンにし、目的の範囲を入力します。
6. 踏み台マシンに RDP するときのログインに使用するユーザー名とパスワードを入力します。パスワードの要件。

   ユーザ名に Unicode 文字を使用しないでください。
7. ［踏み台マシンを作成］をクリックします。

踏み台マシンが正常に作成されると、ページタイトルが **Bastion — *connection*** に変わります。

踏み台マシンの作成が失敗した場合 (または操作中に失敗した場合)、障害通知ページの下部にある [削除] をクリックします。踏み台マシンをもう一度作成してみてください。

RDP 範囲制限は、踏み台マシンの作成後に変更できます。［編集］をクリックします。新しい値を入力し、チェックマークをクリックして変更を保存します。([**X**] をクリックして、変更をキャンセルします。)

8. [**RDP** ファイルのダウンロード] をクリックします。
9. 要塞の作成時に指定した認証情報を使用して、要塞への RDP。(踏み台マシンのアドレスは、ダウンロードした RDP ファイルに埋め込まれています)。
10. 踏み台マシンからサブスクリプション内の他の Citrix マシンに接続します。その後、ログを収集して診断を実行できます。

踏み台マシンは、作成時にパワーオンされます。コストを節約するために、起動後にアイドル状態のままであれば、マシンの電源が自動的にオフになります。マシンは数時間後に自動的に削除されます。

ページの下部にあるボタンを使用して、踏み台マシンの電源管理または削除を行うことができます。踏み台マシンを削除する場合は、マシン上のアクティブなセッションが自動的に終了することを確認する必要があります。また、マシンに保存されたデータとファイルはすべて削除されます。

直接 **RDP** アクセス

1. サービスの [管理] ダッシュボードから、右側の [トラブルシューティングとサポート] を展開します。
2. ［トラブルシューティングオプションの表示］をクリックします。
3. [トラブルシューティング] ページで、[その他のカタログの問題] を選択します。
4. [**RDP** アクセスによるトラブルシューティング] ページで、カタログを選択します。

   選択したカタログのネットワーク接続に対して RDP がすでに有効になっている場合は、手順 7 に進みます。
5. RDP アクセス範囲が表示されます。RDP アクセスをネットワーク接続で許可されている範囲よりも小さい範囲に制限する場合は、**[IP** アドレス範囲のコンピューターのみに **RDP** アクセスを制限する] チェックボックスをオンにして、希望の範囲を入力します。
6. [**RDP** アクセスを有効にする**]** をクリックします。

   RDP アクセスが正常に有効になると、ページタイトルが **RDP** アクセス **—**接続に変わります。

   RDP アクセスが正常に有効になっていない場合は、障害通知ページの下部にある [**RDP** の有効化を再試行] をクリックします。
7. Active Directory 管理者の資格情報を使用してマシンに接続します。その後、ログを収集して診断を実行できます。

支援が必要な場合

それでも問題が解決しない場合は、ヘルプとサポートの利用の手順に従ってチケットを開きます。

制限

July 16, 2021

この記事では、Citrix Virtual Apps and Desktops Standard for Azure のリソースの制限について説明します。

構成の制限

リソース	上限
Active Directory ドメイン	25
カタログ	100
リソースの場所	25
サブスクリプションあたりの VDA	1,200

リソースの場所の制限

次の表は、各リソースの場所の制限です。要件がこれらの制限を超える場合は、より多くのリソースの場所をお勧めします。

リソース	上限
Active Directory ドメイン	1
シングルセッション VDA	5,000
マルチセッション VDA	500

プロビジョニングの制限

次の表に、単一の Citrix Cloud アカウントの推奨最大値を示します。

大規模な展開では、VDA が複数のサブスクリプションおよびネットワーク接続に分散されるハブアンドスポークモデルをお勧めします。

リソース	制限
カタログごとのマルチセッション VDA	500
カタログごとのシングルセッション VDA	1,200
Microsoft Azure サブスクリプションごとの VDA	1,200

使用制限

リソース	制限
フル管理者の同時監視	5
エンドユーザー（同時）	100,000
単一のユーザーに公開されたリソース	250
1 分あたりのセッション起動数	3,000

トライアル制限

次の表に、このサービスの試用期間中の制限を示します。

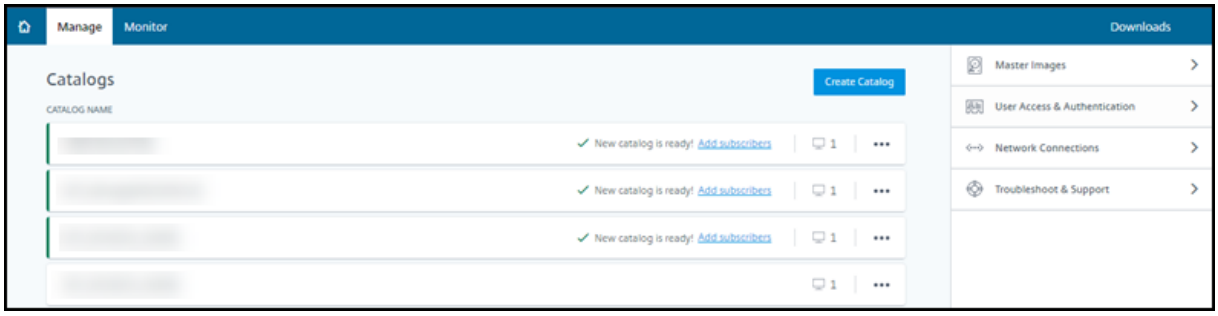
リソース	制限
カタログの最大数	3
最大ユーザー数	25
カタログあたりの VDA の最大数	3

参照

July 16, 2021

ダッシュボード

Citrix Virtual Apps and Desktops Standard for Azure サービスのほとんどの管理者アクティビティは、[**** 管理および監視 ****] ダッシュボードから入力できます。最初のカタログを作成した後、Citrix Cloud にサインインしてこのサービスを選択すると、管理ダッシュボードが自動的に起動します。



トライアルまたは購入のリクエストが承認され、完了した後で、ダッシュボードにアクセスできます。

ダッシュボードにアクセスするには:

1. Citrix Cloudにサインインします。
2. 左上のメニューで、[マイサービス] **> [Azure** の **Virtual Apps and Desktops**] の順に選択します。または、ディスプレイのメイン領域の [**Virtual Apps and Desktops** 標準] タイルで [管理] をクリックすることもできます。)
3. カタログがまだ作成されていない場合は、[ようこそ] ページの [はじめに] をクリックします。管理ダッシュボードに移動します。
4. カタログがすでに作成されている場合は、[管理] ダッシュボードに自動的に表示されます。
5. モニターダッシュボードにアクセスするには、[モニタ] タブをクリックします。

ダッシュボードからの製品内ガイダンスについては、右下隅にあるアイコンをクリックします。

[管理] ダッシュボードの [カタログ] タブ

サービスの [管理] ダッシュボードから、カタログのエントリの任意の場所をクリックします。次のタブには、カタログに関する情報が含まれています。

- 詳細**:** カタログの作成時 (または最新の編集) に指定された情報をリストします。また、カタログの作成に使用されたイメージに関する情報も含まれています。

  このタブでは、次の操作を実行できます。

  - カタログで使用されているイメージを変更する。
  - カタログを削除する。
  - カタログで使用されるリソースの場所の詳細を含むページにアクセスします。

- デスクトップ**:** シングルセッション (静的またはランダム) マシンを含むカタログでのみ使用できます。このタブから、カタログの名前と説明を変更できます。

- デスクトップとアプリ**:** [デスクトップとアプリ] タブは、マルチセッションマシンを含むカタログでのみ使用できます。このタブでは、次の操作を実行できます。

  - カタログのユーザーが Citrix Workspace でアクセスできるアプリケーションを追加、編集 、または削除。
  - カタログの名前と説明を変更します。

- サブスクライバ**:** タイプ (ユーザーまたはグループ)、アカウント名、表示名、Active Directory ドメインおよびユーザープリンシパル名など、すべてのユーザーを一覧表示します。

  このタブでは、カタログに対してユーザーを追加または削除することができます。

- マシン: カタログ内のマシンの総数と、メンテナンスモードがオンになっている登録マシン、未登録マシン、およびマシンの数が表示されます。

  カタログ内の各マシンについて、各マシンの名前、電源状態（オン/オフ）、登録状態（登録/未登録）、割り当てられたユーザー、セッション数（0/1）、メンテナンスモードのステータス（オンまたはオフを示すアイコン）が表示されます。

  このタブでは、次の操作を実行できます。

  - マシンを追加または削除する
  - マシンの起動、再起動、強制再起動、またはシャットダウン
  - マシンのメンテナンスモードをオンまたはオフにする

  詳しくは、「カタログの管理」を参照してください。マシンの操作の多くは、[モニタ] ダッシュボードからも使用できます。「マシンの監視および電源管理」を参照してください。

- 電源管理**:** カタログ内のマシンの電源をオンまたはオフにするタイミングを管理できます。スケジュールには、アイドル状態のマシンがいつ切断されるかが示されます。

  電源スケジュールは、カスタムカタログの作成時または後で作成するときに構成できます。スケジュールが明示的に設定されていない場合、セッションが終了するとマシンの電源がオフになります。

  クイック作成を使用してカタログを作成する場合、電源スケジュールを選択または構成することはできません。デフォルトでは、簡易作成カタログでは、コスト節約プリセットスケジュールが使用されます。ただし、そのカタログを後で編集してスケジュールを変更することはできます。

  詳しくは、「電源管理スケジュールの管理」を参照してください。

DNS サーバー

このセクションは、ドメインに参加しているマシンを含むすべてのデプロイに適用されます。ドメインに参加していないマシンのみを使用する場合は、このセクションを無視できます。

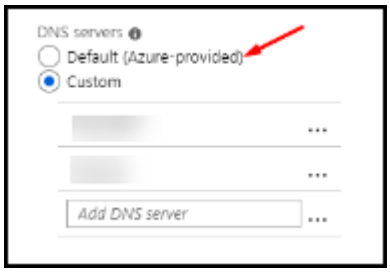
1. ドメイン参加カタログ（または Citrix Managed Azure サブスクリプションを使用している場合は、接続）を作成する前に、パブリックドメイン名とプライベートドメイン名を解決できる DNS サーバーエントリがあるかどうかを確認してください。

   サービスがカタログまたは接続を作成すると、少なくとも 1 つの有効な DNS サーバーエントリが検索されます。有効なエントリが見つからない場合、作成操作は失敗します。

確認する場所:

- 独自の Azure サブスクリプションを使用している場合は、Azure の **DNS** サーバーエントリを確認してください。
- Citrix Managed Azure サブスクリプションを使用して Azure VNet ピア接続を作成している場合は、ピアリングしている Azure **VNet** の **DNS** サーバーエントリを確認します。
- Citrix Managed Azure サブスクリプションを使用して SD-WAN 接続を作成している場合は、SD-WAN Orchestratorの DNS エントリを確認します。

2. Azure では、カスタム設定に少なくとも 1 つの有効なエントリが必要です。このサービスは、[デフォルト **(Azure** 提供**)**] 設定では使用できません。



   - デフォルト **(Azure** 提供**)** が有効になっている場合は、設定を [カスタム] に変更し、少なくとも 1 つの DNS サーバーエントリを追加します。
   - [カスタム] に DNS サーバーエントリが既にある場合は、このサービスで使用するエントリがパブリックドメインとプライベートドメインの IP 名を解決できることを確認します。
   - ドメイン名を解決できる DNS サーバーがない場合は、Azure が提供するこれらの機能を備えた DNS サーバーを追加することをお勧めします。

3. DNS サーバーエントリを変更した場合は、仮想ネットワークに接続されているすべてのマシンを再起動します。再起動すると、新しい DNS サーバー設定が割り当てられます。(仮想マシンは、再起動するまで現在の DNS 設定を使用します。)

DNS アドレスを後で変更する場合は、接続の作成後に次の操作を行います。

- 独自の Azure サブスクリプションを使用する場合、Azure でそれらを変更できます (前の手順で説明したように)。または、このサービスで変更することもできます。
- Citrix Managed Azure サブスクリプションを使用する場合、このサービスは Azure で行った DNS アドレスの変更を同期しません。ただし、このサービスの接続の DNS 設定を変更することはできます。

DNS サーバーのアドレスを変更すると、その接続を使用するカタログ内のマシンの接続の問題が発生する可能性があることに注意してください。

このサービスを通じて **DNS** サーバーを追加する

DNS サーバーアドレスを接続に追加する前に、DNS サーバーがパブリックドメイン名と内部ドメイン名を解決できることを確認してください。DNS サーバーを追加する前に、DNS サーバーへの接続をテストすることをお勧めします。

1. 接続の作成時に DNS サーバーアドレスを追加、変更、または削除するには、[接続タイプの追加] ページの [**DNS** サーバーの編集] をクリックします。または、DNS サーバーのアドレスが見つからなかったことを示すメッセージが表示された場合は、[**DNS** サーバーの追加] をクリックします。ステップ 3 に進みます。
2. 既存の接続の DNS サーバーアドレスを追加、変更、または削除するには
   a) サービスの [管理] ダッシュボードから、右側の [ネットワーク接続] を展開します。
   b) 編集する接続を選択します。
   c) [**DNS** サーバーの編集] をクリックします。
3. アドレスを追加、変更、または削除します。
   a) アドレスを追加するには、[**DNS** サーバーの追加] をクリックし、IP アドレスを入力します。
   b) 住所を変更するには、住所フィールド内をクリックし、番号を変更します。
   c) アドレスを削除するには、アドレスエントリの横にあるゴミ箱アイコンをクリックします。すべての DNS サーバーアドレスを削除することはできません。接続には少なくとも 1 つが必要です。
4. 完了したら、ページの下部にある [変更の確認] をクリックします。
5. その接続を使用するすべてのマシンを再起動します。再起動すると、新しい DNS サーバー設定が割り当てられます。(仮想マシンは、再起動するまで現在の DNS 設定を使用します。)

ポリシー

ドメインに参加していないマシンのグループポリシーの設定

1. イメージに使用されているマシンへの RDP。
2. Visual Studio 2017 がマシンにインストールされていることを確認します。
3. Citrix グループポリシー管理をインストールします。
   a) CTX220345を表示します。添付ファイルをダウンロードします。
   b) ダウンロードしたファイルをダブルクリックします。`Group Policy Templates 1912 > Group Policy Management`フォルダで、`CitrixGroupPolicyManagement_x64.msi` をダブルクリックします。
4. [ファイル名を指定して実行] コマンドを使用して、`gpedit.msc` を起動して、グループポリシーエディタを開きます。
5. `User Configuration Citrix Policies > Unfiltered`で、[ポリシーの編集] をクリックします。
6. 必要に応じてポリシー設定を有効にします。次に例を示します:
   - [設定] タブの [コンピュータの構成] または [ユーザーの構成] で作業する場合は、`Category > ICA / Printing`の [**PDF** ユニバーサルプリンタの自動作成] を選択し、`Enabled`に設定します。
   - ログインユーザーをデスクトップの管理者にする場合は、インタラクティブユーザーグループを組み込みの管理者グループに追加します。

7. 完了したら、画像を保存します。
8. 新しいイメージを使用して既存のカタログを更新するまたは新しいカタログを作成する。

ドメインに参加しているマシンのグループポリシーの設定

1. マシンに最低限の Visual Studio 2017 がインストールされていることを確認します。
2. グループポリシー管理機能がインストールされていることを確認します。
   - Windows マルチセッションマシンで、Windows ツールを使用して役割と機能 (役割と機能の追加など) を追加して、グループポリシー管理機能を追加します。
   - Windows シングルセッションマシンで、適切な OS のリモートサーバー管理ツールをインストールします。(このインストールにはドメイン管理者アカウントが必要です)。インストール後、グループポリシー管理コンソールは [スタート] メニューから使用できるようになります。
3. Citrixダウンロードページから Citrix グループポリシー管理パッケージをダウンロードしてインストールし、必要に応じてポリシー設定を構成します。ステップ 2 から最後まで、ドメインに参加していないマシンのグループポリシーの設定の手順に従います。

> 注:
>
> Citrix Studio コンソールはこのサービスでは利用できませんが、利用可能な機能については、ポリシー設定リファレンス記事を参照してください。

リソースの場所の操作

Citrix は、デスクトップとアプリケーションを公開するための最初のカタログを作成するときに、リソースの場所と 2 つの Cloud Connector を自動的に作成します。カタログの作成時に、リソースの場所に関連するいくつかの情報を指定できます。「カタログ作成時のリソースの場所設定」を参照してください。

リモート PC アクセスの場合は、リソースの場所と Cloud Connector を作成します。)

このセクションでは、リソースの場所の作成後に実行可能なアクションについて説明します。

1. サービスの ［管理］ダッシュボードで、右側の ［サブスクリプション］ を展開します。
2. サブスクリプションをクリックします。
   - [詳細] タブには、サブスクリプション内のカタログとイメージの数と名前が表示されます。また、デスクトップまたはアプリケーションを配信できるマシンの数も示します。この数には、イメージ、Cloud Connector、RDS ライセンスサーバーなど、他の目的で使用されるマシンは含まれません。
   - [リソースの場所] タブには、各リソースの場所が一覧表示されます。各リソースロケーションエントリには、リソースロケーション内の各 Cloud Connector のステータスとアドレスが含まれます。

リソースロケーションのエントリの省略記号メニューには、次の操作が含まれます。

ヘルスチェックの実行

[ヘルスチェックを実行] を選択すると、すぐに接続チェックが開始されます。チェックに失敗すると、Citrix Cloud と通信していないため、Cloud Connector の状態は不明になります。Cloud Connector を再起動したい場合があります。

コネクタの再起動

一度に 1 つの Cloud Connector を再起動することをお勧めします。再起動すると Cloud Connector がオフラインになり、ユーザーアクセスとマシンの接続が中断されます。

再起動する Cloud Connector のチェックボックスをオンにします。［再起動］をクリックします。

コネクタを追加

Cloud Connector の追加は、通常 20 分かかります。

次の情報を入力します。

- 追加する Cloud Connector の数はいくつですか。
- ドメインサービスアカウントの認証情報。Cloud Connector マシンをドメインに参加するために使用します。
- マシンのパフォーマンス。
- Azure リソースグループ。デフォルトは、リソースの場所で最後に使用されたリソースグループです。
- 組織単位 (OU) デフォルトは、リソースの場所で最後に使用された OU です。
- ネットワークでインターネット接続にプロキシサーバーが必要かどうか。**[**はい**]** を指定した場合は、プロキシサーバの FQDN または IP アドレス、およびポート番号を指定します。

完了したら、[コネクタを追加] をクリックします。

コネクタを削除

Cloud Connector が Citrix Cloud と通信できず、再起動しても問題が解決しない場合は、Citrix サポートはその Cloud Connector を削除することをお勧めします。

削除する Cloud Connector のチェックボックスをオンにします。次に、[削除] をクリックします。確認のメッセージが表示されたら、［削除］をクリックします。

利用可能な Cloud Connector を削除することもできます。ただし、その Cloud Connector を削除すると、リソースの場所で利用可能な Cloud Connector が 3 つ未満になる場合は、選択した Cloud Connector を削除することはできません。

[更新時刻**]** を選択します

Citrix は、Cloud Connector のソフトウェアアップデートを自動的に提供します。更新中、1 つの Cloud Connector がオフラインになり、更新され、他の Cloud Connector は引き続きサービスされます。最初の更新が完了すると、別

の Cloud Connector がオフラインになり、更新されます。このプロセスは、リソースの場所にあるすべての Cloud Connector が更新されるまで継続されます。更新を開始するのに最適な時期は、通常、通常の営業時間外です。

更新を開始する時刻を選択するか、更新が利用可能になったときに更新を開始するように指定します。完了したら、[保存] をクリックします。

名前の変更

リソースの場所の新しい名前を入力します。［保存］をクリックします。

接続性を構成する

ユーザーが Citrix Gateway サービスを介してデスクトップとアプリケーションにアクセスできるか、または企業ネットワーク内からのみアクセスできるかを指定します。

Profile Management

Profile Management は、ユーザーデバイスの場所に関係なく、ユーザーの仮想アプリケーションに個人設定が適用されるようにします。

Profile Management の構成は任意です。

Profile Management は、プロファイル最適化サービスで有効にできます。このサービスを利用することで、Windows でプロファイル設定を確実に管理できます。プロファイルを管理するとユーザーに単一のプロファイルのみが適用されるようになるため、一貫したユーザーエクスペリエンスを確保できます。ユーザープロファイルが自動的に集約および最適化されるため、管理と保存の手間が最小化されます。プロファイル最適化サービスにより、必要な管理、サポート、インフラストラクチャを最低限に抑えられます。また、プロファイルの最適化により、ユーザーはログオンとログオフのエクスペリエンスが向上します。

プロファイル最適化サービスを使用するには、すべての個人設定を保存するファイル共有が必要になります。ファイルサーバーは管理します。これらのファイルサーバーへのアクセスを許可するには、ネットワーク接続を設定することをお勧めします。ファイル共有は UNC パスとして指定する必要があります。このパスには、システム環境変数、Active Directory のユーザー属性、Profile Management の変数を含めることができます。UNC テキスト文字列の書式について詳しくは、「ユーザーストアへのパスの指定」を参照してください。

Profile Management を有効にする場合、ユーザープロファイルサイズの影響を最小限に抑えるようにフォルダーのリダイレクトを構成して、ユーザーのプロファイルをさらに最適化することを検討してください。フォルダーリダイレクトを適用することで、Profile Management ソリューションを強化できます。詳しくは、Microsoft Folder Redirection を参照してください。

Windows サーバーワークロード用の Microsoft RDS ライセンスサーバーを構成する

このサービスは、Windows 2016 などの Windows Server ワークロードを配信するとき、Windows Server リモートセッション機能にアクセスします。これには通常、リモートデスクトップサービスクライアントアクセスライセ

ンス（RDS CAL）が必要です。VDA は、RDS CAL の要求のために RDS ライセンスサーバーに接続できる必要があります。ライセンスサーバーをインストールしてアクティブ化してください。詳しくは、Microsoft 社のドキュメント「Activate the Remote Desktop Services License Server」を参照してください。概念実証環境では、Microsoft から提供される猶予期間を利用できます。

この方法により、このサービスでライセンスサーバーの設定を適用できます。イメージの RDS コンソールでは、ライセンスサーバーおよび接続ユーザー数モードを構成できます。また、Microsoft のグループポリシー設定を使用して、ライセンスサーバーを構成することもできます。詳しくは、Microsoft 社のドキュメント「License your RDS deployment with client access licenses (CALs)」を参照してください。

グループポリシー設定を使用して RDS ライセンスサーバーを構成するには

1. 使用可能な VM のいずれかに、リモートデスクトップサービスのライセンスサーバーをインストールします。この VM は常に使用可能なものである必要があります。また、Citrix サービスのワークロードが常にこのライセンスサーバーに到達できる必要があります。
2. Microsoft のグループポリシーを使用して、ライセンスサーバーのアドレスとユーザーごとのライセンスモードを指定します。　詳しくは、Microsoft 社のドキュメント「Specify the Remote Desktop Licensing Mode for an RD Session Host Server」を参照してください。

Windows 10 ワークロードには、適切な Windows 10 ライセンスのアクティブ化が必要です。Microsoft のドキュメントに従って、Windows 10 ワークロードをアクティブ化することをお勧めします。

消費コミットメントの使用状況

> 注:
>
> この機能はプレビュー中です。

管理ダッシュボードの [一般] カードの [消費] の値は、現在の暦月に使用された消費量を示します。この値には、月次および期間のコミットメントが含まれます。

[全般] をクリックすると、[通知] タブには次の情報が表示されます。

- その月（月間および期間）に使用された総消費量。
- 毎月の消費コミットメントのユニット数。
- 長期消費コミットメントの割合。

値および進行状況バーは、潜在的な使用量または実際の使用超過について警告できます。

実際のデータが表示されるまで 24 時間かかることがあります。使用状況と請求データは、暦月末から 72 時間後の最終データと見なされます。

使用方法の詳細については、「ライセンスとアクティブな使用状況を監視する」を参照してください。

オプションで、消費使用量（毎月、期間、または両方のコミットメント）が指定されたレベルに達したときに、管理ダッシュボードに表示される通知をリクエストできます。デフォルトでは、通知は無効になっています。

1. [通知] タブで、[通知プリファレンスの編集] をクリックします。

2. 通知を有効にするには、スライダーをクリックしてチェックマークが表示されます。
3. 値を入力します。必要に応じて、他の消費タイプについても繰り返します。
4. [保存] をクリックします。

通知を無効にするには、チェックマークが表示されなくなるようにスライダーをクリックし、[保存] をクリックします。

Citrix ライセンスの使用状況を監視する

Citrix ライセンスの使用状況に関する情報を表示するには、ライセンスとアクティブな使用状況を監視するのガイダンスに従います。次の項目を表示できます。

- ライセンスの概要
- 使用状況レポート
- 使用状況の傾向とライセンスアクティビティ
- ライセンス使用ユーザー

ライセンスをリリースすることもできます。

負荷分散

負荷分散は、単一セッションマシンではなく、マルチセッションマシンに適用されます。

> 重要:
>
> 負荷分散方法を変更すると、展開内のすべてのカタログに影響します。これには、サポート対象のホストタイプ（Studio や Quick Deploy など）の作成に使用されるインターフェイスに関係なく、クラウドベースおよびオンプレミスのホストタイプを使用して作成されたすべてのカタログが含まれます。
>
> 続行する前に、すべてのカタログに対して最大セッション制限が設定されていることを確認してください。
>
> - このサービスでは、その設定は各カタログの [詳細] タブにあります。
> - 他の Citrix Virtual Apps and Desktops サービスとエディションでは、負荷管理ポリシー設定を使用します。

負荷分散は、マシンの負荷を測定し、現在の条件下で受信ユーザーセッションに対して選択するマルチセッションマシンを決定します。この選択は、設定された負荷分散方式に基づいています。

負荷分散方式は、水平または垂直の 2 つのいずれかを設定できます。この方法は、サービス展開内のすべてのマルチセッションカタログ (したがって、すべてのマルチセッションマシン) に適用されます。

- **水平負荷分散:** 受信ユーザーセッションは、使用可能な最小負荷のパワーオン状態のマシンに割り当てられます。

  簡単な例：2 つのマシンがそれぞれ 10 セッション用に構成されています。最初のマシンは 5 つの同時セッションを処理します。2 台目のマシンは 5 台を処理します。

水平負荷分散は高いユーザーパフォーマンスを提供しますが、より多くのマシンの電源をオンにしてビジー状態を維持するにつれ、コストが増加する可能性があります。

このメソッドはデフォルトで有効になっています。

- 垂直負荷分散：着信ユーザーセッションは、負荷指数が最も高いパワーオン状態のマシンに割り当てられます。(サービスは、マルチセッションマシンごとに負荷インデックスを計算し、割り当てます。計算では、CPU、メモリ、同時実行性などの要素が考慮されます)。

  この方法は、新しいマシンに移行する前に既存のマシンを飽和させます。ユーザーが既存のマシンを切断して容量を解放すると、それらのマシンに新しく負荷が割り当てられます。

  簡単な例：2 つのマシンがそれぞれ 10 セッション用に構成されています。最初のマシンは、最初の 10 個の同時セッションを処理します。2 つ目のマシンは、11 番目のセッションを処理します。

  垂直負荷分散により、セッションは電源投入されたマシンの容量を最大化し、マシンコストを節約できます。

負荷分散方式を設定するには、次の手順を実行します。

1. サービスの [管理] ダッシュボードから、右側の [一般] を展開します。
2. [グローバル設定] で、[すべて表示] をクリックします。
3. [グローバル設定] ページの [マルチセッションカタログ負荷分散] で、負荷分散方式を選択します。
4. [確認] をクリックします。

プロキシサーバーを使用するネットワーク内にカタログを作成する

ネットワークでインターネット接続にプロキシサーバーが必要で、独自の Azure サブスクリプションを使用している場合は、この手順に従います。プロキシサーバーを必要とするネットワークで Citrix Managed Azure サブスクリプションを使用することはサポートされていません)。

1. Citrix Virtual Apps and Desktops Standard for Azure 管理コンソールから、必要な情報を入力して、ページの下部にある [カタログの作成] をクリックしてカタログ作成プロセスを開始します。
2. プロキシ要件のため、カタログの作成は失敗します。ただし、リソースの場所が作成されます。カタログの作成時にリソースの場所名を指定しない限り、そのリソースの場所の名前は「DAS」で始まります。Citrix Virtual Apps and Desktops Standard for Azure コンソールで、クラウドサブスクリプションを展開します。[リソースの場所] タブで、新しく作成されたリソースの場所に Cloud Connector があるかどうかを確認します。該当する場合は、削除してください。
3. Azure で、2 つの VM を作成します (「Cloud Connector のシステム要件」を参照)。これらのマシンをドメインに参加させます。
4. Citrix Cloud コンソールから、各仮想マシンでCloud Connector をインストールする。Cloud Connector が、以前に作成したリソースの場所と同じ場所にあることを確認します。次のガイダンスに従ってください。
   - Cloud Connector のプロキシとファイアウォールの構成
   - システムおよび接続要件

5. Citrix Virtual Apps and Desktops Standard for Azure 管理コンソールから、カタログ作成プロセスを繰り返します。カタログが作成されると、前の手順で作成した Cloud Connector のリソースの場所と Cloud Connector が使用されます。

支援が必要な場合

- 「トラブルシューティング」を確認してください。
- このサービスのサポートが必要な場合は、ヘルプとサポートの利用のガイダンスに従ってチケットを開いてください。

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States