Citrix DaaS for Azure

Machine translated content

Disclaimer

Contents

Citrix DaaS Standard for Azure

September 9, 2022

はじめに

Citrix DaaS Standard for Azure（旧称 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。Citrix DaaS for Azure は、仮想アプリケーションとデスクトップを任意のデバイスに配信するためのクラウドベースの管理、プロビジョニング、および管理容量を提供します。

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 DaaS 製品に精通している場合は、Citrix DaaS for Azure を使用すると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 DaaS for Azure 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 について詳しく知る。

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、「技術的なセキュリティの概要」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。

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、Citrix DaaS for Azure 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 Citrix DaaS for Azure で使用する項目と用語の一部を紹介します。

- 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。

- Citrix DaaS for Azure 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 DaaS 製品に精通している場合、Citrix DaaS のカタログは、マシンカタログとデリバリーグループを組み合わせたものと似ています。

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します。
- リモート PC アクセス用のカタログを作成します。
- カタログを管理します。
- ユーザーと認証。

リソースの場所

カタログのマシンは、リソースの場所に存在します。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:

- カタログを作成するときに、リソースの場所情報を指定します。
- リソースの場所アクション。

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。

- Citrix DaaS for Azure には、Citrix 提供イメージがいくつか用意されています:
  - Windows 10 Enterprise（シングルセッション）
  - Windows 10 Enterprise Virtual Desktop（マルチセッション）
  - Office 365 ProPlus を使用する Windows 10 Enterprise Virtual Desktop（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、Citrix DaaS for Azure 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、「イメージ」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。

Azure 用の Citrix DaaS 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:

- 展開シナリオでは、Azure サブスクリプションを Citrix DaaS for Azure で使用する方法を示します。
- Azure サブスクリプションでは 、Citrix Managed Azure サブスクリプションとカスタマー管理の 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。
- 「テクニカルセキュリティの概要」 では、Citrix Managed Azure サブスクリプションと顧客管理の Azure サブスクリプション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。

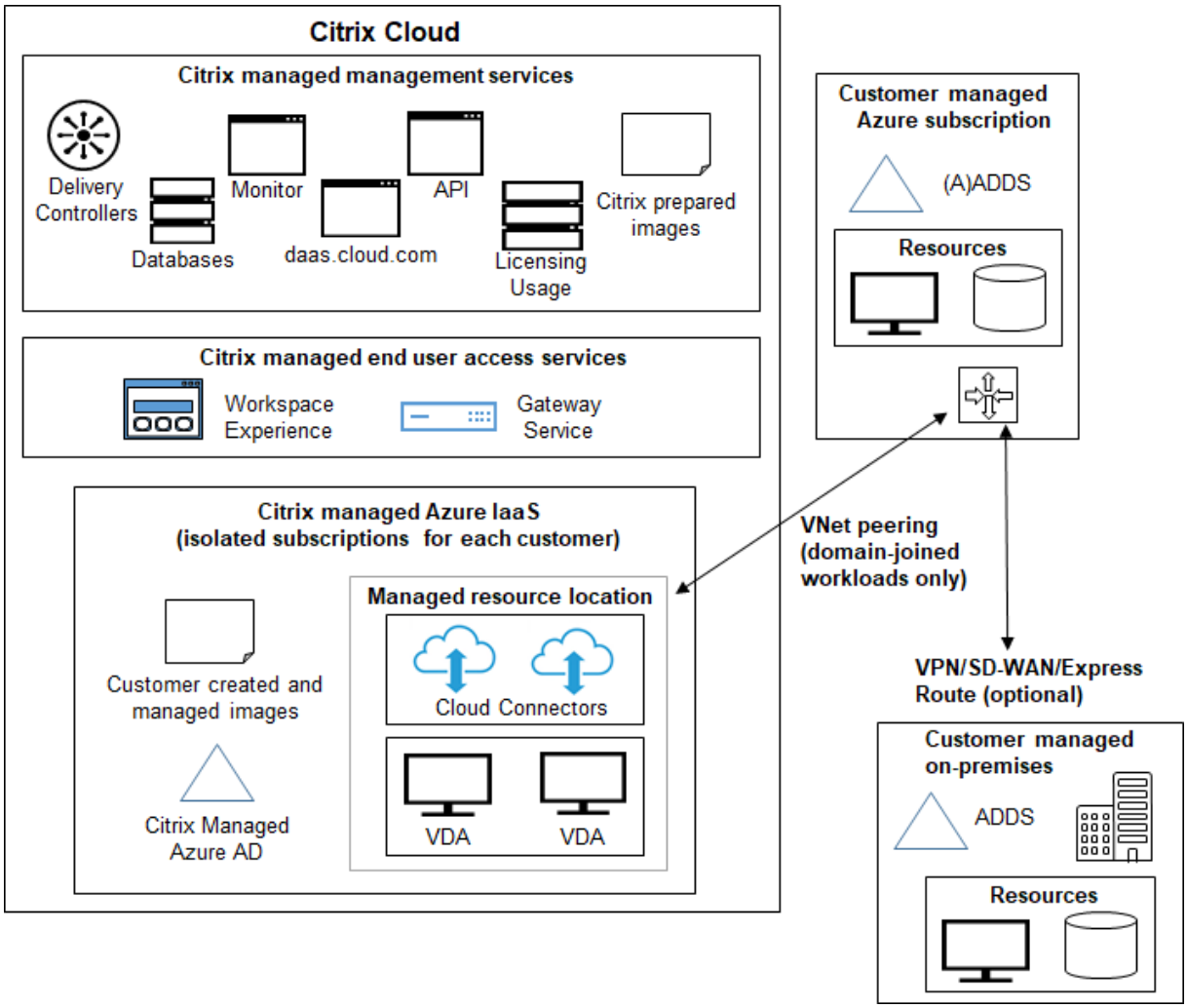
次の表に、デスクトップおよびアプリケーションを配信する際の、ドメインに参加していないマシンとドメインに参加しているマシンの違いをいくつか示します。

ドメイン非参加	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 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)。	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。 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

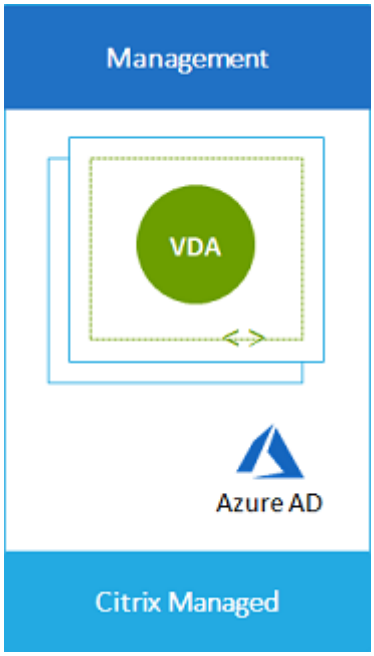
公開デスクトップとアプリケーションの展開シナリオは、Citrix Managed Azure サブスクリプションを使用しているか独自の顧客管理 Azure サブスクリプションを使用しているかによって異なります。

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

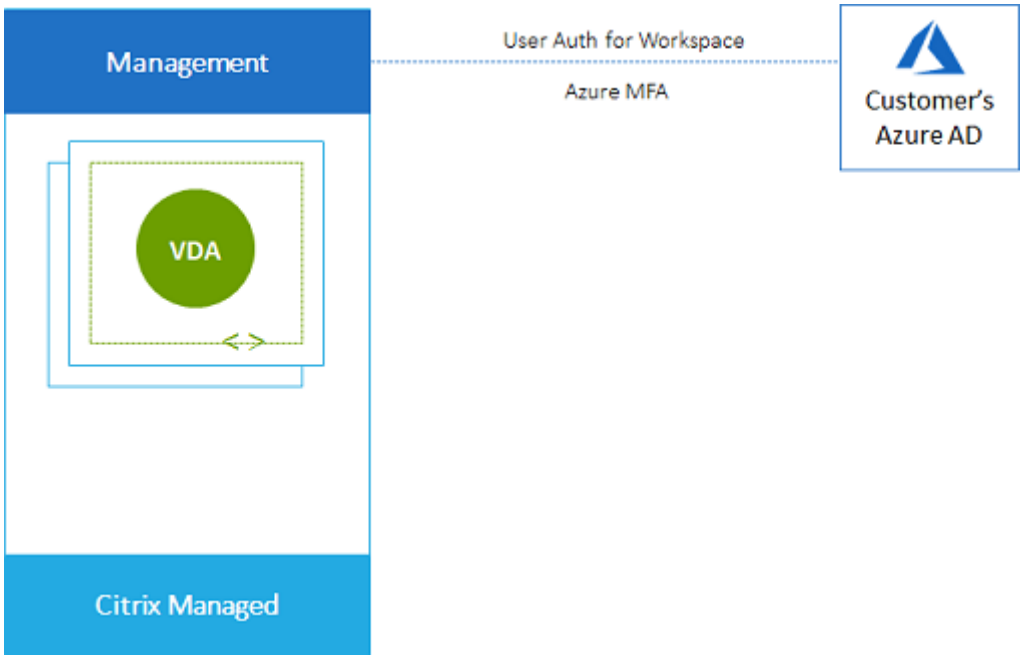


Citrix DaaS for Azure は、接続とユーザー認証のためのいくつかの展開シナリオをサポートしています。

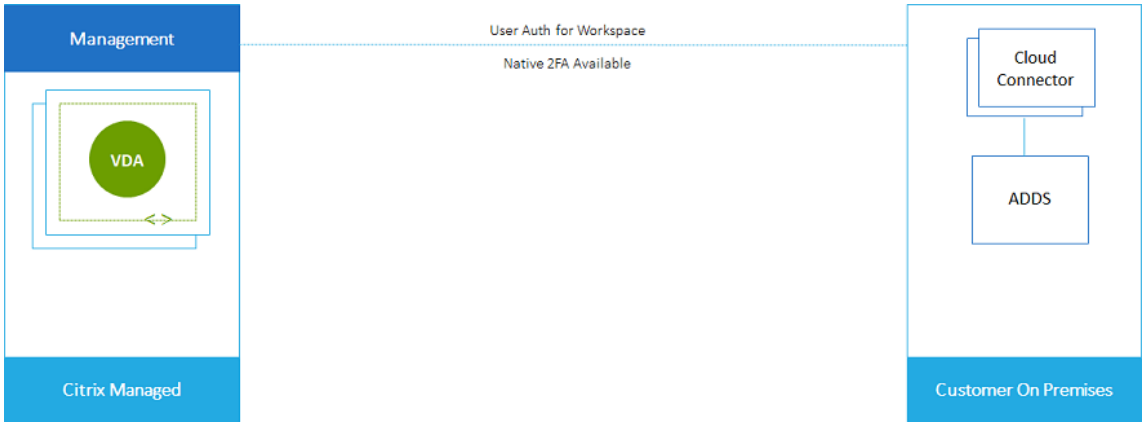
- 管理対象 **Azure AD**：これは、ドメインに参加していない VDA を使用した最も単純な展開です。コンセプトの証明におすすめです。管理対象 Azure AD（Citrix が管理する）を使用してユーザーを管理します。ユーザーは、オンプレミスネットワークのリソースにアクセスする必要はありません。



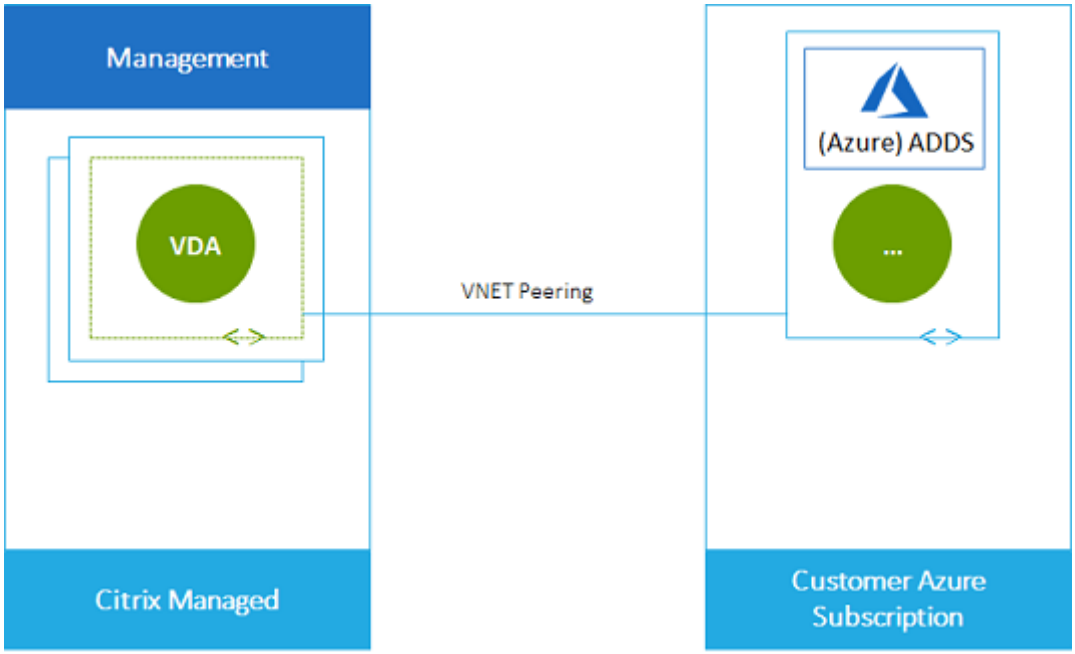
- お客様の **Azure Active Directory**：この展開には、ドメインに参加していない VDA が含まれています。エンドユーザー認証には、独自の Active Directory または Azure Active Directory (AAD) を使用します。このシナリオでは、ユーザーはオンプレミスネットワーク上のリソースにアクセスする必要はありません。



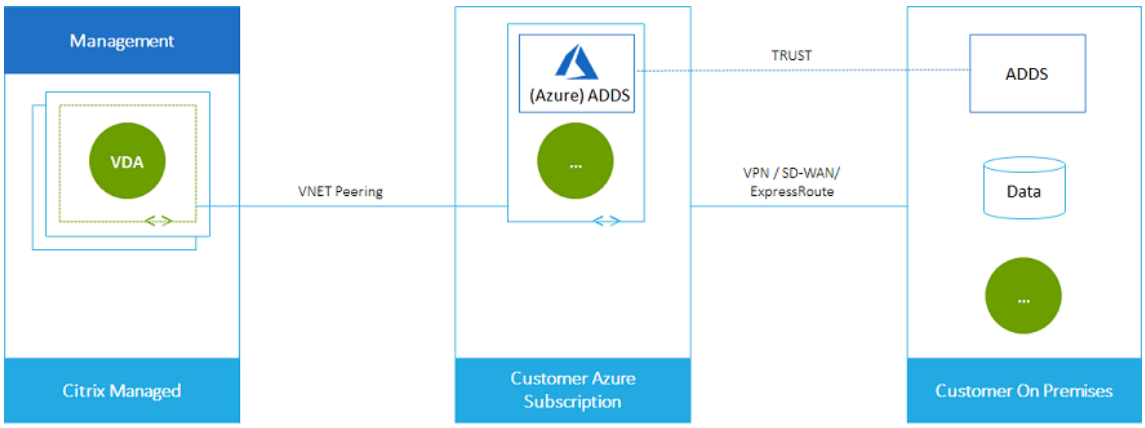
- オンプレミスアクセスを持つお客様の **Azure Active Directory**：この展開には、ドメインに参加していない VDA が含まれます。エンドユーザー認証には、独自の AD または AAD を使用します。このシナリオでは、オンプレミスネットワークに Citrix Cloud Connector をインストールすると、そのネットワーク内のリソースにアクセスできます。



- 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。

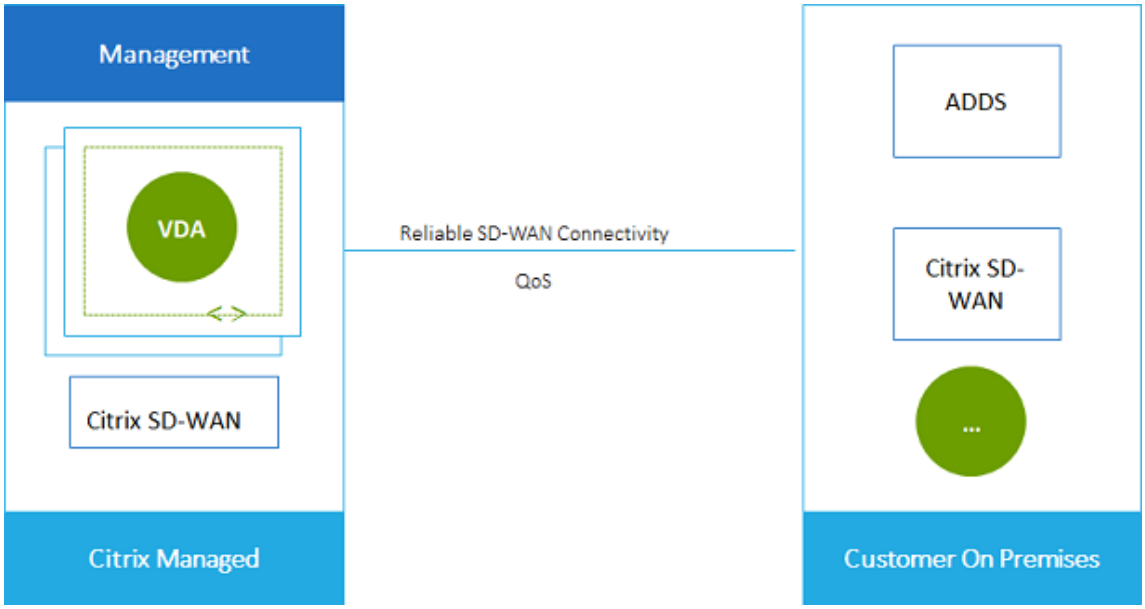


ユーザーがオンプレミスネットワークに保存されているデータにアクセスできるようにするには、Azure サブスクリプションからオンプレミスの場所への VPN 接続を使用できます。Azure VNet ピアリングはネットワーク接続に使用されます。オンプレミスの場所にある Active Directory ドメインサービスは、エンドユーザー認証に使用されます。

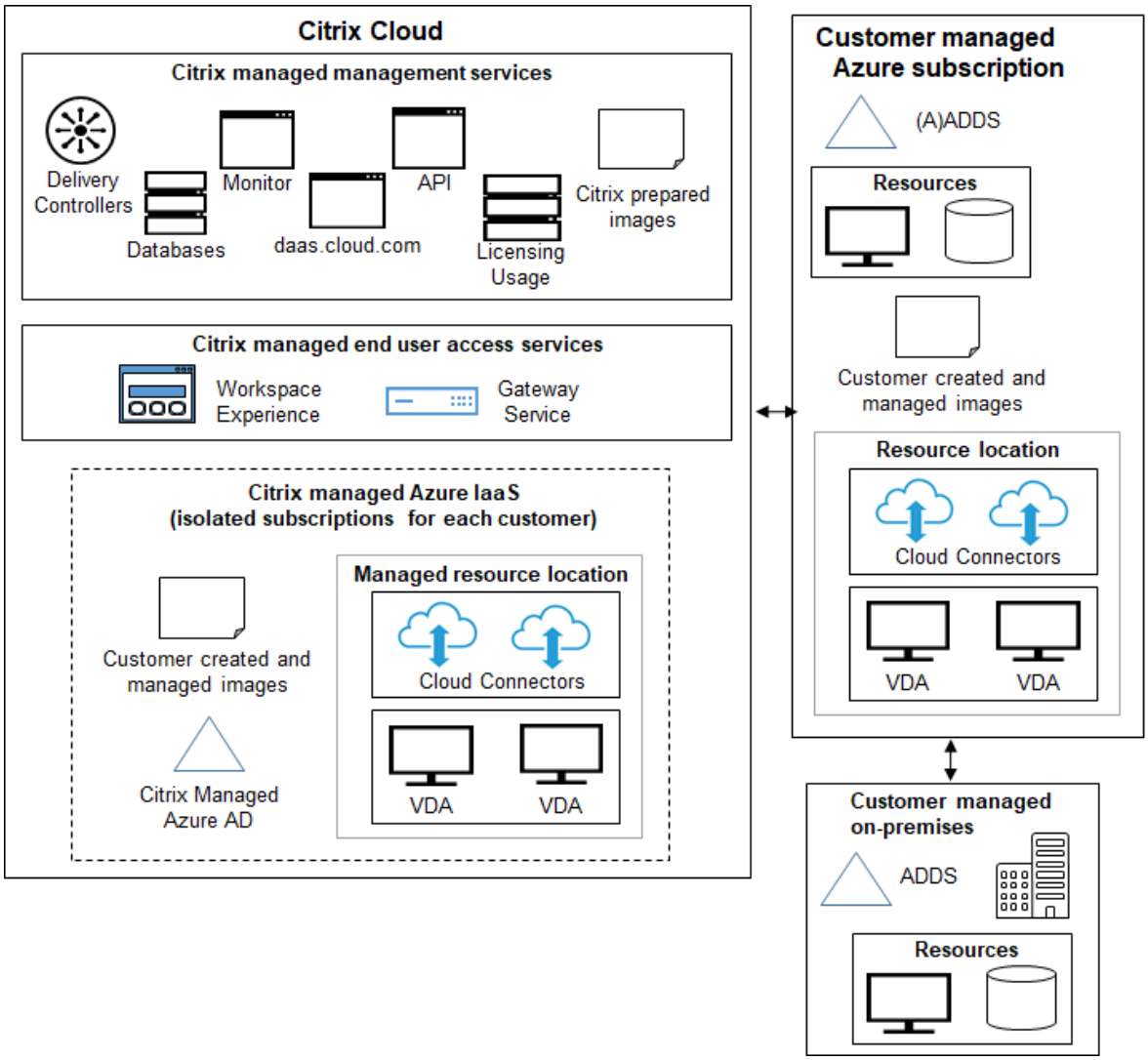


- お客様の **Active Directory** と **SD-WAN:** オンプレミスまたはクラウド SD-WAN ネットワークからファイルやその他のアイテムへのアクセスをユーザーに提供できます。

  Citrix SD-WAN は、Citrix DaaS for Azure に必要なすべてのネットワーク接続を最適化します。Citrix SD-WAN は、HDX テクノロジと連携して、ICA と、アウトオブバンドの Citrix DaaS for Azure トラフィックに、QoS（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 DaaS for Azure には、クイック展開と完全構成という 2 つのグラフィカル管理インターフェイスがあります。

- **Quick Deploy** を使用すると、カタログをすばやく作成して、デスクトップとアプリケーションのユーザーへの配信を開始できます。(そのため、「クイック展開」という名前になっています。) これは、Citrix DaaS for Azure を起動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] **> [Azure**

Quick Deploy] 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。

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。

- **Full Configuration** には、展開を調整および管理するための高度な機能と設定オプションが用意されています。簡易展開で作成したカタログは、自動的に [完全構成] に表示されます。簡易展開から完全構成に移動するには、[管理**] > [**完全構成] を選択します。

  簡易展開でカタログを作成すると、関連付けられたデリバリーグループとホスト接続が [完全構成] で自動的に作成されます。

  フル構成では、Azure ホストへの接続の作成、カタログとデリバリーグループの作成など、独自のカタログ作成プロセスも提供しています。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。

  完全構成は、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ます。Citrix DaaS for Azure の顧客は使用できません。

クイック展開インターフェイスで作成されたカタログの管理

［クイック展開］インターフェイスでカタログを作成した後は、引き続きそのインターフェイスでそのカタログを管理できます。詳しくは、「カタログの管理」を参照してください。［完全な構成］インターフェイスを使用することもできます。

［クイック展開］でカタログを作成すると、そのカタログ（およびバックグラウンドで自動的に作成されるデリバリーグループとホスト接続）に`Citrix managed object`のスコープが割り当てられます。スコープは、オブジェクトをグループ化するために、委任管理で使用されます。

`Citrix managed object`スコープを使用するカタログ、デリバリーグループ、接続は、［完全な構成］インターフェイスでの特定の操作では禁止されています。（［完全な構成］でこれらの操作を許可すると、［クイック展開］と［完全な構成］の両方をサポートするシステムの機能に悪影響を与えることがあるため、これらの操作は無効です。）［完全な構成］インターフェイスでは：

- カタログ：ほとんどのカタログ管理操作は使用できません。カタログは削除できません。
- デリバリーグループ：ほとんどのデリバリーグループ管理操作を使用できます。デリバリーグループは削除できません。
- 接続：ほとんどの接続管理操作は使用できません。接続は削除できません。`Citrix managed object`スコープの接続に基づく接続を作成することはできません。

独自の Azure サブスクリプション（［クイック展開］に追加したもの）を使用して［クイック展開］でカタログを作成し、カタログ（とそのデリバリーグループおよび接続）をすべて［完全な構成］で管理する場合は、カタログを変換できます。

- カタログを変換すると、その管理は［完全な構成］インターフェイスのみに制限されます。カタログが変換されると、［クイック展開］インターフェイスを使用してそのカタログを管理することはできなくなります。
- カタログが変換された後、以前は［完全な構成］で使用できなかった操作を選択できるようになります。(`Citrix managed object`スコープは、変換されたカタログ、デリバリーグループ、ホスト接続から削除されます。)
- カタログを変換するには:

  Citrix DaaS for **Azure** の **[管理] > [Azure** クイック展開] ダッシュボードで、カタログのエントリ内の任意の場所をクリックします。［詳細］タブの［詳細設定］で、［カタログを変換］を選択します。確認のメッセージが表示されたら、変換を確定します。
- Citrix Managed Azure サブスクリプションを使用して、［クイック展開］で作成されたカタログを変換することはできません。

変換されたカタログを完全構成で管理する方法については、以下を参照してください。

- マシンカタログの管理 （フル構成はカタログをマシンカタログとして参照します）
- デリバリーグループの管理

追加情報

技術的な詳しくは、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

デプロイの自動化について詳しくは、「管理対象デスクトップのパブリック API プレビュー」を参照してください。

準備ができたら、始めましょう。

新機能

December 28, 2023

シトリックスは、Citrix DaaS for Azure をご使用のお客様に、新機能と製品の更新をいち早くお届けするよう取り組んでいます。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 提供イメージの更新

Citrix 提供イメージには、最新の 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 提供イメージは自動的に最新の VDA に更新されます。VDA の最新バージョンの新機能および拡張機能の詳しくは、以下を参照してください。

- Windows VDA
- Linux VDA

2022 年 **8** 月

- この機能は一般公開されています。Azure Active Directory に参加しているマシンのカタログを作成できるようになりました。「カタログの作成」を参照してください。

2022 年 **5** 月

- これで、Azure Active Directory に参加しているマシンのカタログを作成できます。この機能はプレビュー段階です。「カタログの作成」を参照してください。
- Citrix Service Provider は、Citrix DaaS for Azure サービスを顧客から削除できるようになりました。「サービスの削除」を参照してください。

2022 年 **4** 月

- Citrix Hypervisor、Microsoft SCVMM、VMware vSphere、PrismCentral、および Nutanix AHV のホスト接続の作成が可能になりました。そのため、Azure に加えてオンプレミスのハイパーバイザーを使用できるようになりました。
- 製品名が Citrix Virtual Apps and Desktops Standard for Azure から Citrix DaaS for Azure に変更されました。すべての Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）オファリングのブランド変更について詳しくは、Citrix DaaS の「新機能 」を参照してください。名称変更について詳しくは、ブログでの発表を参照してください。

2022 年 **1** 月

- カタログを作成すると、マシンを標準の SSD ストレージに保存できるようになりました。以前は、標準ディスク (HDD) とプレミアム SSD のみがサポートされていました。
- VDA ワークロードをホストするための新しいリージョン（ブラジル南部、インド中部、日本東部、米国中南部、英国南部）のサポート。

- Citrix Managed Azure および BYO Azure でホストされている永続デスクトップで、スナップショットと復元を使用できるようになりました。「VDA のスナップショットと復元」を参照してください。
- ホストされている VDA からのすべてのアウトバウンドトラフィックの静的パブリック IP アドレスを使用できるようになりました。IP アドレスを取得するように Azure NAT ゲートウェイを構成できます。パブリック静的 IP アドレスの作成を参照してください。
- Azure VPN はテクニカルプレビューで利用できます。Azure VPN を使用すると、Citrix マネージド Azure をオンプレミスのデータセンターに直接接続できます。Azure VPN テクニカルプレビューを参照してください。
- Citrix 提供イメージでは、新しい Linux イメージを使用できます。

2021 年 11 月

- 営業による承認に加えて、自動承認による 7 日間のトライアルが利用可能になりました。
- Citrix サービスプロバイダーは、サービスの［管理］**>**［**Azure Quick Deploy**］ダッシュボードまたは **Citrix Cloud** コンソールからユーザーを管理できるようになりました。詳しくは、「顧客 ID プロバイダーへのパートナーアクセス」を参照してください。

2021 年 10 月

- ［クイック展開］で作成されたカタログの管理に関する新しい情報。

2021 年 9 月

- API コンテンツのプレビューが利用可能です。
- Windows Server 2022 のサポート（最低 VDA 2106 が必要）。

2021 年 7 月

- Web Studio 管理インターフェイスが［完全な構成］に名称変更。

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をサポートします。

2021 年 5 月

- このサービスは、サービス継続性プレビューをサポートしています。
- Citrix 提供イメージに、Ubuntu のシングルセッションとマルチセッションの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ときに、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、マシンのパフォーマンスの選択肢には、選択したイメージの世代タイプ（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でカタログを更新できます。

2022 年 4 月

- 製品名が Citrix Virtual Apps and Desktops Standard for Azure から Citrix DaaS for Azure に変更されました。

2021 年 1 月

- 消費コミットメントの使用状況を表示するためのプレビューサポート。

2020 年 10 月

- シャドウの監視機能を使用して、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 アクセスの実稼働サポート。
- Azure Virtual Desktop の適格ライセンスまたは Azure Hybrid Benefit を使用するためのカタログ作成オプションの機能強化。
- マシンでの再起動操作が失敗した場合は、強制再起動操作を使用できます。

2020 年 9 月

- イメージの詳細情報が再編成および拡張されています。たとえば、準備またはインポートしたイメージ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 ピアリング接続を作成するときに、仮想ネットワークゲートウェイのルート伝達も有効にできるようになりました。
- 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 アクセスのプレビューサポート。
- Citrix 提供の 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、顧客が管理する 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、「リソースの場所アクション」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たカタログの作成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。
- 顧客が管理する Azure サブスクリプションを使用する場合のLinux VDAの実稼働サポート。
- サブスクリプションあたりの VDA の制限数が 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は、別の Citrix Managed Azure サブスクリプションを追加できます 。
- DNS サーバーに関する追加情報。

2020 年 3 月

- SD-WAN 接続の実稼働サポート。

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 DaaS Standard for Azure のライセンスと使用状況の監視」のガイダンスに従ってください。
- 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、顧客が管理する 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に、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 提供イメージが、Office 365 ProPlus を使用する Windows 10 Enterprise Virtual Desktop（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 接続のプレビューサポート。

2019 年 10 月

- 「サポートされているオペレーティングシステム」に、次のエントリが追加されました。
  - 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 のCitrix 提供イメージが利用可能になりました。
- リソースの場所設定に関する情報を追加しました。詳しくは、「リソースの場所のアクション」および「カタログ作成時のリソースの場所の設定」を参照してください。

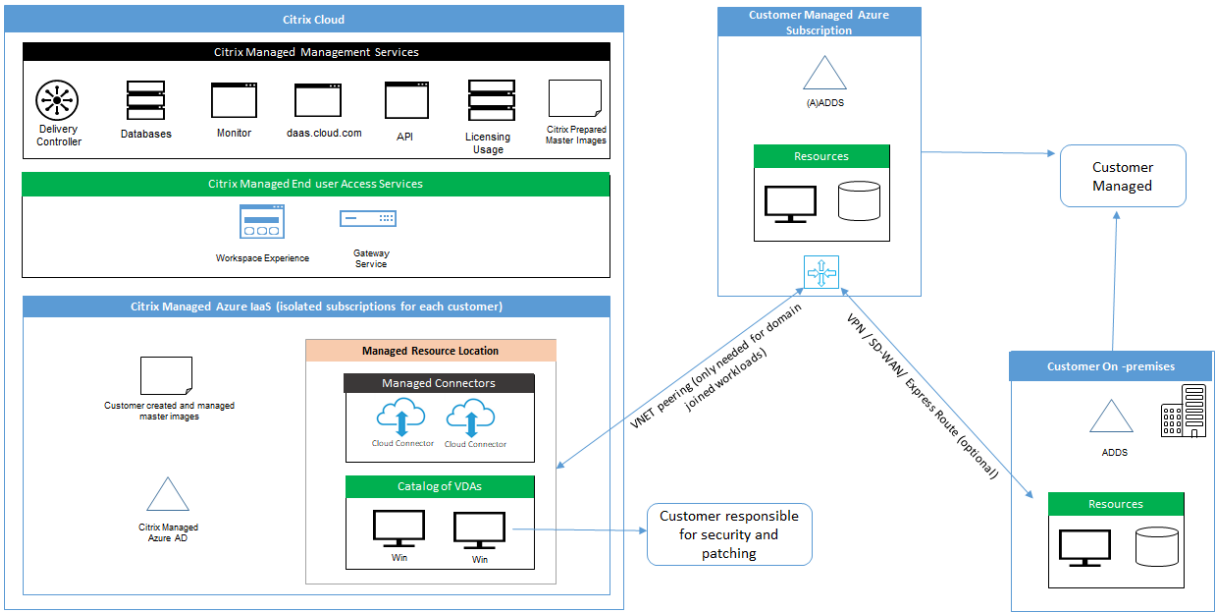
2019 年 9 月

- 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、顧客が管理する独自の 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

May 20, 2022

次の図に、Citrix DaaS Standard for Azure（旧称 Citrix Virtual Apps and Desktops Standard for Azure）展開に含まれるコンポーネントを示します。この例では、VNet ピアリング接続を使用しています。



Citrix DaaS for Azure を使用すると、デスクトップとアプリを提供する顧客の Virtual Delivery Agent（VDA）と Citrix Cloud Connector が、Citrix 管理の Azure サブスクリプションとテナントに展開されます。

> 注:
>
> この記事では、Citrix Managed Azure サブスクリプションを使用して Citrix DaaS for Azure を展開する顧客のセキュリティ要件の概要を説明します。セキュリティ情報を含む、顧客管理の Azure サブスクリプションを使用した Citrix DaaS for Azure の展開のアーキテクチャの概要については、「リファレンスアーキテクチャ:Virtual Apps and Desktops サービス-Azure」を参照してください。

Citrix クラウドベースのコンプライアンス

2021 年 1 月時点で、さまざまなエディションの Citrix DaaS 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。

シトリックスの責任

ドメイン非参加カタログ用の **Citrix Cloud Connector**

Citrix DaaS for Azure は、各リソースの場所に少なくとも 2 つの Cloud Connector を展開します。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できます。

シトリックスは、ドメイン非参加カタログの Cloud Connector に対する以下のセキュリティ操作に責任があります:

- 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
- アンチウイルスプログラムのインストールと保守
- Cloud Connector ソフトウェア更新プログラムの適用

顧客には Cloud Connector へのアクセス権限はありません。そのため、シトリックスは、ドメイン非参加カタログ Cloud Connector のパフォーマンスに全責任を負います。

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

シトリックスは、顧客向けに作成された Azure サブスクリプションと Azure Active Directory（AAD）のセキュリティに責任があります。シトリックスはテナント分離を保証しているため、各顧客は自身の Azure サブスクリプションと AAD を持ち、異なるテナント間の混線は防止されます。また、Citrix は、AAD へのアクセスを Citrix DaaS for Azure と Citrix 運用担当者のみに制限しています。シトリックスによる各顧客の Azure サブスクリプションへのアクセスは監査されます。

ドメイン非参加カタログを使用している顧客は、Citrix Workspace の認証手段として Citrix 管理の AAD を使用できます。これらの顧客のために、シトリックスは Citrix 管理の AAD で制限付き特権の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 管理の AAD に対して操作を行うことはできません。これらの顧客が代わりに独自の 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は顧客が全責任を負います。

仮想ネットワークとインフラストラクチャ

顧客の Citrix Managed Azure サブスクリプション内で、シトリックス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。シトリックスは、これらのネットワーク内で、ストレージアカウント、Key Vault、およびその他の Azure リソースに加え、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。シトリックスは、Microsoft と提携し、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に対する責任を負います。

シトリックスは、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保証します。通常、これは VDA と Cloud Connector への受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 ピアリング接続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

顧客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、シトリックスが作成した VDA マシンに追加のファイアウォール規則を展開することはできます。たとえば、送信トラフィックを部分的に制限できます。シトリックスが作成した 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規則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顧客は、発生する可能性のあるセキュリティリスクに責任を負います。

Citrix DaaS for Azure で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、ポート 3389～3390 が Citrix 管理の VNet で一時的に開かれるため、顧客は新しいマシンイメージを含むマシンに RDP（リモートデスクトッププロトコル）を使用することができ、そのマシンをカスタマイズできます。

Azure VNet ピアリング接続を使用する場合のシトリックスの責任

Citrix DaaS for Azure の VDA がオンプレミスのドメインコントローラー、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 DaaS 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。顧客の Citrix 管理の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 ピアリング接続のファイアウォールポリシー　シトリックスは、VNet ピアリング接続を使用する受信および送信トラフィック用に、以下のポートを開いたり閉じたりします。

ドメイン非参加マシンを使用した **Citrix** 管理の **VNet**

- 受信規則
  - VDA から Cloud Connector へ、および Cloud Connector から VDA への受信には、ポート 80、443、1494、および 2598 を許可します。
  - モニターシャドウイング機能で使用される IP 範囲から VDA への受信には、ポート 49152～65535 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。
  - 他のすべての受信を拒否します。これには、VDA から VDA への、および VDA から Cloud Connector への VNet 内トラフィックが含まれます。
- 送信規則
  - すべての送信トラフィックが許可されます。

ドメイン参加済みマシンがある **Citrix** 管理の **VNet**

- 受信規則:
  - VDA から Cloud Connector へ、および Cloud Connector から VDA への受信には、ポート 80、443、1494、および 2598 を許可します。
  - モニターシャドウイング機能で使用される IP 範囲から VDA への受信には、ポート 49152～65535 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。

  - 他のすべての受信を拒否します。これには、VDA から VDA への、および VDA から Cloud Connector への VNet 内トラフィックが含まれます。

- 送信規則
  - すべての送信トラフィックが許可されます。

ドメイン参加済みマシンがある顧客管理の **VNet**

- VNet を正しく構成することは顧客の責任です。この責任には、ドメイン参加のために以下のポートを開くことが含まれます。
- 受信規則:
  - 内部起動のために、クライアント IP からの 443、1494、2598 での受信を許可します。
  - Citrix VNet（顧客が指定した IP 範囲）からの 53、88、123、135～139、389、445、636 での受信を許可します。
  - プロキシ構成で開いたポートでの受信を許可します。
  - 顧客が作成したその他の規則。
- 送信規則:
  - 内部起動のために、Citrix VNet（顧客が指定した IP 範囲）への 443、1494、2598 での送信を許可します。
  - 顧客が作成したその他の規則。

SD-WAN 接続を使用する場合のシトリックスの責任

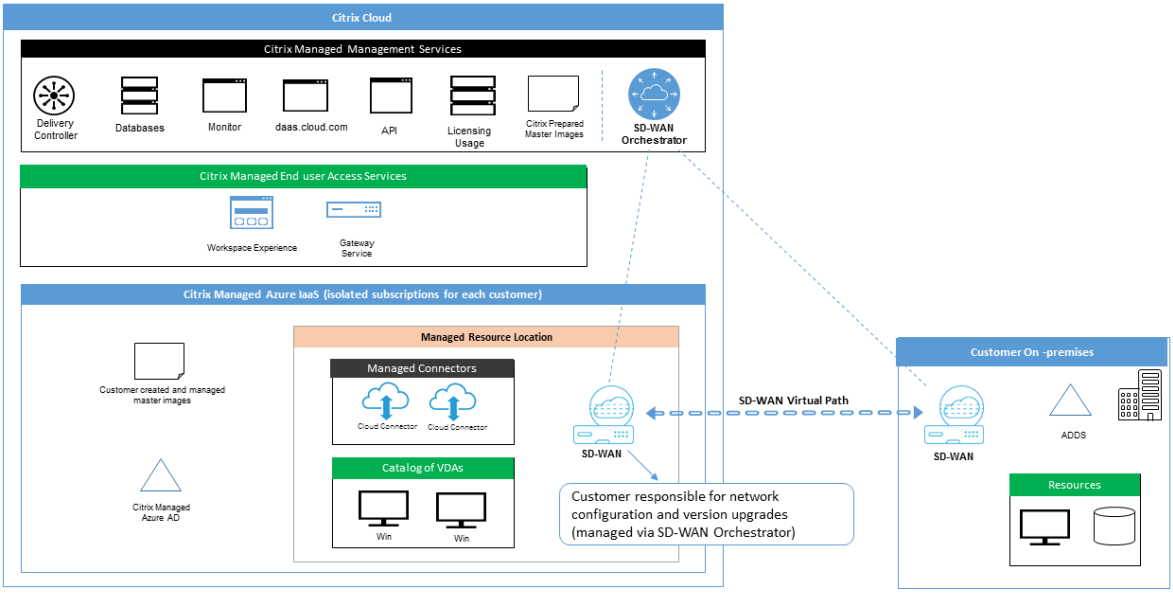
Citrix は、仮想 Citrix SD-WAN インスタンスを完全に自動で展開する方法をサポートしており、これにより Citrix DaaS for Azure とオンプレミスリソースとの間の接続が可能です。Citrix SD-WAN 接続には、VNet ピアリングと比較して次のような多くの利点があります。

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（サービス品質）機能と VoIP（ボイスオーバー IP）最適化機能を備えた、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と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、およびレポートする組み込み機能。

Citrix は、Citrix DaaS for Azure で SD-WAN 接続を利用する顧客が、SD-WAN Orchestrator を使用して Citrix SD-WAN ネットワークを管理することを求めます。

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



Citrix DaaS 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、「Citrix SD-WAN Standard Edition インスタンスの Azure への展開」を参照してください。高可用性構成では、Azure Load Balancer を使用した SD-WAN インスタンスのアクティブ/スタンバイペアは、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展開されます。高可用性ではない構成では、単一の SD-WAN インスタンスのみがゲートウェイとして展開されます。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、シトリックス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 管理の VNet の DNS サーバーとしても構成されます。

仮想 SD-WAN インスタンスへの管理アクセスには、管理者の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 管理者が、SD-WAN Orchestrator UI、仮想アプライアンス管理 UI、および CLI を介してリモートログインしたりトラブルシューティングしたりするための、ランダムで安全な一意の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、特定の顧客の VNet に展開された仮想 SD-WAN インスタンスは、他のすべての VNet から完全に分離されます。

顧客が Citrix SD-WAN 接続を有効にする場合、Citrix は、Citrix DaaS 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、ロードバランサーなど）を保守し、仮想 SD-WAN インスタンスの初期構成について安全で効率的な追加設定不要のデフォルト設定を提供し、SD-WAN Orchestrator を使用した継続的な保守とトラブルシューティングを可能にします。また、シトリックスは合理的な対策を講じて、SD-WAN ネットワーク構成の自動検証を実行し、既知のセキュリティリスクをチェックし、SD-WAN

Orchestrator を使用して対応する通知を表示します。

SD-WAN 接続のファイアウォールポリシー　シトリックスは、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 および管理インターフェイスのみにパブリック IP アドレスが割り当てられ、インターネットへの送信接続を許可します。
- Citrix 管理の 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みネットワークトラフィックを交換できます。
- WAN インターフェイスは、（仮想パス接続のために Citrix SD-WAN によって使用される）UDP ポート 4980 への受信トラフィックを制限し、VNet への送信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）への受信トラフィックを許可します。
- HA（高可用性）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のみが許可されます。

インフラストラクチャへのアクセス

シトリックスは、顧客の Citrix 管理インフラストラクチャ（Cloud Connector）にアクセスして、顧客に通知せずに、ログの収集（Windows イベントビューアーなど）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。シトリックスは、これらのタスクを安全かつ確実に実行し、顧客への影響を最小限に抑える責任があります。また、シトリックスは、ログファイルが安全かつ確実に取得、転送、および処理されるようにする責任があります。この方法では、顧客の VDA にアクセスすることはできません。

ドメイン非参加カタログのバックアップ

シトリックスは、ドメイン非参加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、イメージビルダーで作成されたイメージなど、Citrix DaaS for Azure にアップロードされたすべてのマシンイメージをバックアップする責任があります。シトリックスは、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。

ドメイン非参加カタログのバックアップのための踏み台マシン

シトリックスの運用担当者は、必要に応じて、顧客の Citrix 管理の Azure サブスクリプションにアクセスして、顧客の問題を診断および修復するための踏み台マシンを作成できます。これは、顧客が問題に気付く前に行われる可能性があります。シトリックスは、踏み台マシンを作成するために顧客の同意を必要としません。シトリックスが踏み台マシンを作成する場合、シトリックスは踏み台マシンに対してランダムに生成される強力な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。踏み台マシンが不要になると、シトリックス踏み台マシンを処分し、パスワードは無効になります。踏み台マシン（およびそれに付随する RDP アクセス規則）は、操作が完了すると破棄されます。シトリックスは、踏み台マシンを使用して、顧客のドメイン非参加の Cloud Connector にのみアクセスできます。シトリックスには、ドメイン非参加 VDA またはドメイン参加済み Cloud Connector と 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

顧客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場合、Citrix 管理の VNet に対して以下のセキュリティグループの変更が行われます：

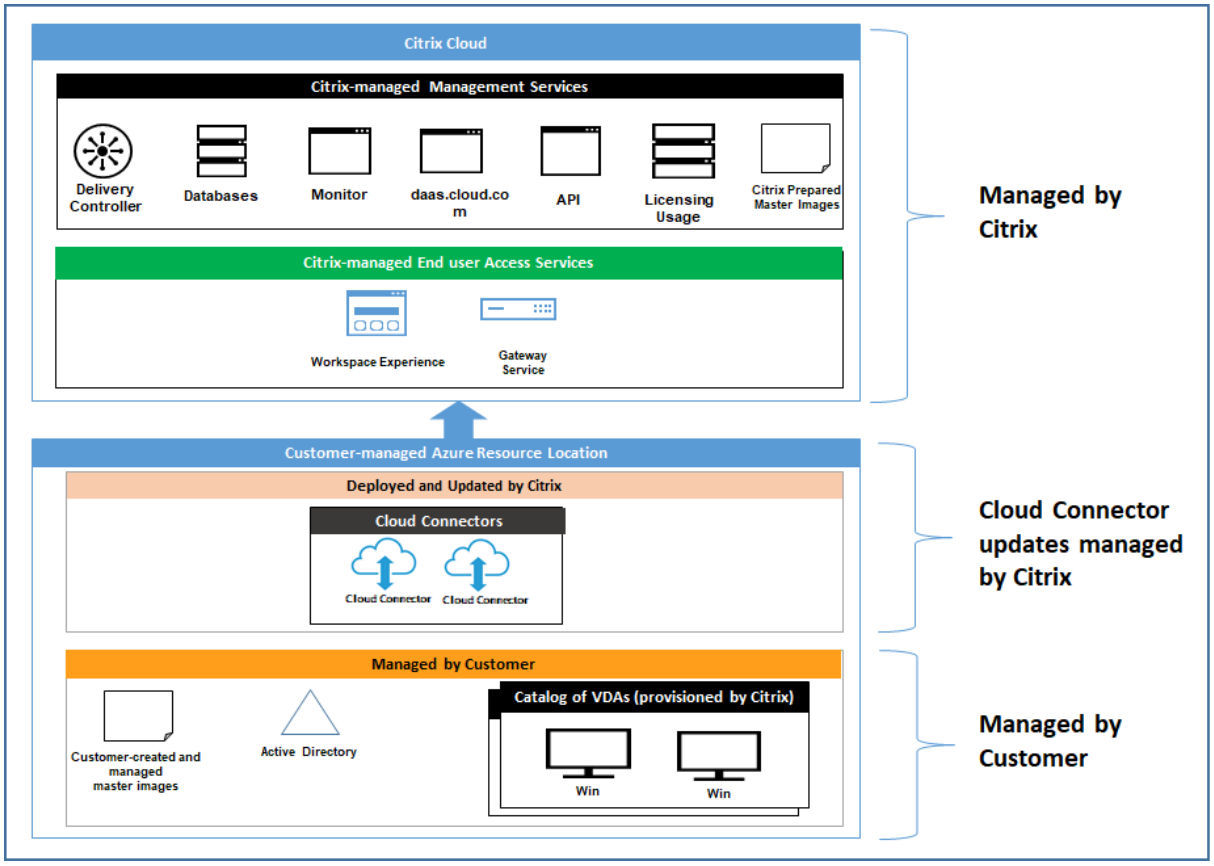
- 顧客指定の IP 範囲から踏み台マシンへの受信に、一時的にポート 3389 を許可します。
- 踏み台マシンの IP アドレスから VNet（VDA および Cloud Connector）内の任意のアドレスへの受信に、一時的にポート 3389 を許可します。
- Cloud Connector、VDA、およびその他の VDA の間の RDP アクセスを引き続き禁止します。

顧客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場合、Citrix 管理の VNet に対して以下のセキュリティグループの変更が行われます：

- 顧客指定の IP 範囲から VNet（VDA および Cloud Connector）内の任意のアドレスへの受信に、一時的にポート 3389 を許可します。
- Cloud Connector、VDA、およびその他の VDA の間の RDP アクセスを引き続き禁止します。

顧客管理のサブスクリプション

顧客管理のサブスクリプションの場合、シトリックスは、Azure リソースの展開時に上記の責任を順守します。展開後、顧客は Azure サブスクリプションの所有者であるため、上記のすべては顧客の責任になります。



顧客の責任

VDA とマシンイメージ

顧客は、以下のような、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:

- オペレーティングシステムの更新プログラム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 ソフトウェアの更新プログラム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規則（特に送信トラフィック）
- Citrix の「セキュリティに関する考慮事項およびベストプラクティス」に従ってください。

シトリックスは、出発点として意図的に準備されたイメージを提供します。顧客は、このイメージを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。シトリックスは、この Citrix 提供イメージのセキュリティを保証しません。シトリックスは、Citrix 提供イメージ上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つようにし、これらのイメージ上で Windows Defender を有効にします。

VNet ピアリングを使用する場合の顧客の責任

お客様は、「ドメイン参加済みマシンがある顧客管理の VNet」で指定されているすべてのポートを開く必要があります。

VNet ピアリングが構成されている場合、顧客は、自身の仮想ネットワークとオンプレミスリソースへの接続のセキュリティに責任があります。また、顧客は、Citrix 管理のピア仮想ネットワークからの受信トラフィックのセキュリティに責任があります。シトリックスは、Citrix 管理の仮想ネットワークから顧客のオンプレミスリソースへのトラフィックを禁止するための操作を実行しません。

顧客には、受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 管理の仮想ネットワークに、顧客のオンプレミスネットワークまたは顧客管理の接続済み仮想ネットワーク内の他の場所で使用されていない IP ブロックを与える。これは VNet ピアリングに必要です。
- 顧客の仮想ネットワークとオンプレミスネットワークに 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追加して、Citrix 管理の IP ブロックからのトラフィックを禁止または制限する。
- Citrix 管理の IP ブロックを対象として、侵入防止システム、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措置を、顧客の仮想ネットワークとオンプレミスネットワークに展開する。

SD-WAN 接続を使用する場合の顧客の責任

SD-WAN 接続が構成されている場合、顧客は、Citrix DaaS for Azure で使用される仮想 SD-WAN インスタンスをネットワーク要件に従って極めて柔軟に構成できます。ただし例外として、Citrix 管理の VNet で SD-WAN を確実に正しく動作させるために必要ないくつかの要素があります。顧客の責任には以下のようなものがあります:

- DNS とインターネットトラフィックブレークアウトの規則など、ルーティングとファイアウォールの規則の設計と構成。
- SD-WAN ネットワーク構成の保守。
- ネットワークの運用ステータスの監視。
- Citrix SD-WAN ソフトウェアの更新またはセキュリティの修正のタイムリーな展開。顧客のネットワーク上の Citrix SD-WAN のすべてのインスタンスで、同じバージョンの SD-WAN ソフトウェアを使う必要があるため、更新したバージョンのソフトウェアを Citrix DaaS for Azure の SD-WAN インスタンスに展開し、顧客のネットワーク保守スケジュールと制約に従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規則の不適切な構成、または SD-WAN 管理パスワードの誤った管理により、Citrix DaaS 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リソースの両方に、セキュリティリスクが生じる可能性があります。また、Citrix SD-WAN ソフトウェアを最新の利用可能なパッチリリースに更新しないことにより、セキュリティリスクが生じる可能性もあります。SD-WAN Orchestrator とその他の Citrix Cloud サービスはこうしたリスクに対処するための手段を提供しますが、顧客は仮想 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最終的な責任があります。

プロキシ

顧客は、VDA からの送信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、顧客は以下の責任を負います:

- VDA マシンイメージでプロキシ設定を構成してあるか、VDA がドメイン参加済みである場合は、Active Directory グループポリシーを使用します。
- プロキシの保守とセキュリティ。

Citrix Cloud Connector またはその他の Citrix 管理のインフラストラクチャでプロキシを使用することは許可されていません。

カタログの回復性

シトリックスは、回復性のレベルが異なる 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、回復するには新しい VDA に配置される必要があります。Azure は、シングルインスタンス VM に 99.5% の SLA を提供します。顧客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 に対して行われたカスタマイズ（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、冗長性により高可用性を提供します。VDA がダウンしても、ユーザーのプロファイルが他の場所にあるため、情報が失われることはありません。
- **Windows 10** 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ように動作しますが、サーバー VDA の代わりに Windows10 ワークステーション VDA を使用します。

ドメイン参加済みカタログのバックアップ

顧客が VNet ピアリングでドメイン参加済みカタログを使用している場合、顧客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取得することをお勧めします。顧客は、これらのファイル共有のバックアップと可用性に責任があります。

障害回復

Azure データが失われた場合、シトリックスは Citrix 管理の Azure サブスクリプション内のリソースを可能な限り多く回復します。シトリックスは、Cloud Connector と VDA の回復を試みます。シトリックスがこれらのアイテムの回復に失敗した場合、顧客には新しいカタログを作成する責任があります。シトリックスは、マシンイメージがバックアップされており、顧客がユーザープロファイルをバックアップして、カタログを再構築できることを前提としています。

Azure リージョン全体が失われた場合、顧客は、顧客管理の仮想ネットワークを新しいリージョンで再構築し、Citrix DaaS for Azure 内に新しい 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。

シトリックスと顧客が共有する責任

ドメイン参加済みカタログ用の **Citrix Cloud Connector**

Citrix DaaS for Azure は、各リソースの場所に少なくとも 2 つの Cloud Connector を展開します。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、ドメインにある場合、リソースの場所を共有することができます。シトリックスは、顧客のドメイン参加済み Cloud Connector を、イメージ上で次のようなセキュリティデフォルト設定に構成します:

- オペレーティングシステムの更新プログラムとセキュリティパッチ
- アンチウイルスプログラム
- Cloud Connector ソフトウェア更新プログラム

顧客には通常、Cloud Connector へのアクセス権限はありません。ただし、カタログのトラブルシューティング手順に従い、ドメインの資格情報を使用してログインすることで、アクセス権限を取得できます。踏み台マシンからログインするときに行った変更については、顧客の責任となります。

顧客は、Active Directory グループポリシーにより、ドメイン参加済み Cloud Connector を制御することもできます。顧客は、Cloud Connector に適用されるグループポリシーが安全で適切であることを確認する責任があります。たとえば、顧客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、顧客には 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。また、顧客は、グループポリシーを使用して、別のアンチウイルスプログラムをインストールするなど、Cloud Connector のデフォルト設定よりも厳格なセキュリティを適用できます。通常、顧客には、ポリシーを使用せず、自身の Active Directory の組織単位に Cloud Connector を配置することをお勧めします。これにより、シトリックスが使用するデフォルト設定を問題なく適用できるようになります。

トラブルシューティング

Citrix DaaS for Azure の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のために次の 2 つのオプションがあります: 踏み台マシンの使用、RDP アクセスの有効化。どちらのオプションも、顧客にセキュリティリスクをもたらします。顧客は、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を理解し、同意する必要があります。

シトリックスは、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。

踏み台マシンまたは RDP アクセスのいずれかを使用して操作を実行するアクティブユーザーは、アクセスするマシンのセキュリティに責任を負います。顧客が RDP 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、顧客の責任となります。シトリックスの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ことはそれらのサポート担当者の責任です。環境内の踏み台マシンや他のマシンにアクセスする人物によって生じる脆弱性に対する責任（リストを許可するために IP 範囲を追加する顧客の責任、IP 範囲を正しく実装するシトリックスの責任など）については、本ドキュメントの他の場所に説明があります。

どちらのシナリオでも、シトリックスはファイアウォールの例外を正しく作成して、RDP トラフィックを許可することに責任があります。シトリックスには、顧客が踏み台マシンを処分した後、または Citrix DaaS for Azure を介した RDP アクセスを終了した後、これらの例外を取り消す責任もあります。

踏み台マシン　シトリックスは、顧客の Citrix 管理サブスクリプション内で顧客の Citrix 管理仮想ネットワークに踏み台マシンを作成し、事前に（顧客への通知なしに）、または顧客が引き起こした問題に対応して、問題を診断および修復することができます。踏み台マシンは、顧客が RDP でアクセスし、RDP で VDA と（ドメイン参加済みカタログの場合は）Cloud Connector にアクセスして、ログの収集、サービスの再起動、またはその他の管理タスクを実行するために使用できるマシンです。デフォルトでは、踏み台マシンを作成すると外部のファイアウォール規則が開き、顧客が指定した範囲の IP アドレスからの踏み台マシンへの RDP トラフィックが許可されます。また、内部のファイアウォール規則が開き、Cloud Connector と VDA への RDP アクセスを許可します。これらの規則が開くと、大きなセキュリティリスクが生じます。

顧客は、ローカルの Windows アカウントで使用するパスワードを強力なものにする責任があります。顧客は、踏み台マシンへの RDP アクセスを可能にする外部 IP アドレス範囲を指定する責任もあります。顧客が IP 範囲を指定しないことを選択した場合（誰でも RDP アクセスできるようにした場合）、悪意のある IP アドレスからのアクセスに対しては顧客が責任を負います。

顧客は、トラブルシューティングが完了した後、踏み台マシンを削除する責任もあります。踏み台マシンホストはさらに攻撃対象領域をさらすため、シトリックスは電源を入れてから 8 時間後にマシンを自動的にシャットダウンします。ただし、シトリックスが踏み台マシンを自動的に削除することはありません。顧客が期間を延長して踏み台マシンを使用することを選択した場合、顧客にはそれにパッチを適用して更新していく責任があります。踏み台マシンは数日間だけ使用したのち削除することをお勧めします。顧客が最新の踏み台マシンを希望する場合は、現在の踏み台マシンを削除してから新しい踏み台マシンを作成できます。これにより、最新のセキュリティパッチが適用された新しいマシンがプロビジョニングされます。

RDP アクセス　ドメイン参加済みカタログの場合、顧客の VNet ピアリングが機能していれば、顧客はピアリングされた VNet から Citrix 管理の VNet への RDP アクセスを有効にできます。顧客がこのオプションを使用する場合、顧客は VNet ピアリングを介して VDA および 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できるため、顧客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。顧客は、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。顧客がシトリックスのサポート担当者と協力して問題を解決している場合、顧客はこれらの資格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、顧客は RDP アクセスを無効にする責任があります。顧客のピアネットワークまたはオンプレミスネットワークから RDP アクセスを開いたままにしておくと、セキュリティリスクが発生します。

ドメイン資格情報

顧客がドメイン参加済みカタログを使用することを選択した場合、顧客は、マシンをドメインに参加させるためのアクセス権限があるドメインアカウント（ユーザー名とパスワード）を Citrix DaaS for Azure に提供する責任があります。ドメイン資格情報を提供する場合、顧客は次のセキュリティ原則を順守する責任があります：

- 監査可能：アカウントを Citrix DaaS for Azure 用として作成し、アカウントの使用目的を容易に監査できるようにする必要があります。
- スコープ：アカウントには、マシンをドメインに参加させるためのアクセス権限のみが必要です。完全なドメイン管理者にするべきではありません。
- 安全：アカウントには強力なパスワードを設定する必要があります。

シトリックスには、顧客の Citrix 管理の Azure サブスクリプション内で、Azure Key Vault にこのドメインアカウントを安全に保存する責任があります。このアカウントは、ドメインアカウントのパスワードが操作に必要な場合にのみ取得します。

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 DaaS のセキュリティ情報
- サードパーティ通知

Citrix Daas for Azure にサブスクライブする

December 22, 2022

はじめに

Citrix または Azure Marketplace を通じて、Citrix DaaS Standard for Azure（旧称 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 Consumption Fund の注文）を行うことができます。Citrix 経由で Citrix DaaS for Azure を評価できます。

現在、Citrix Virtual Apps Essentials または Citrix Virtual Desktops Essentials にサブスクライブしている場合は、Citrix DaaS Standard for Azure に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 DaaS 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相違点。
  - 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 から購入する場合は、Citrix DaaS Standard for Azure と Citrix Azure Consumption Fund を同時に購入できます。
- Azure Marketplace から購入するときは、最初に Citrix DaaS Standard for Azure を購入します。次に、Citrix Azure 消費基金を注文します。

  Citrix DaaS for Azure のみを購入する場合は、Azure Marketplace または Citrix アカウント担当者を通じて、後から Citrix Azure Consumption Fund を購入できます。

Citrix DaaS Standard for Azure の注文先や消費基金に関係なく、Citrix はオンボーディングのヘルプを提供します。また、Citrix DaaS Standard for Azure が実行され、正しく構成されていることも確認します。

注文サマリー

注文手順の概要:

1. Citrix Cloud アカウントを取得します。

   Citrix Cloud アカウントをすでに持っていて、現在 Citrix DaaS にサブスクライブしている場合は、「現在 Citrix DaaS にサブスクライブしている場合」を参照してください。

2. Citrix DaaS Standard for Azure および消費基金を Azure Marketplace で注文するか、Citrix 経由で注文します。

トライアル

Citrix DaaS Standard for Azure では、次の 2 種類のトライアルを提供しています。

- 販売承認：販売承認済みのトライアルでは、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。トライアル版では、有料サービスサブスクリプションに変換して、Citrix Managed Azure 消費基金を注文できます。消費量を購入しない場合、Citrix Managed

Azure サブスクリプションを使用して作成した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。

- 自動承認**:** 自動承認されたトライアルでは、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、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。トライアル版から、有料サブスクリプションに変換できます。詳しくは、「自動承認されたサービストライアル」を参照してください。

トライアルの詳しくは、「Citrix Cloud サービストライアル」を参照してください。

自動承認されたサービストライアル

- 自動承認された Citrix DaaS Standard for Azure のトライアルは、7 暦日使用可能です。
- 自動承認されたトライアル期間中は、Azure 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。カタログには、デスクトップまたはアプリケーションを配信するマシンが含まれます。
- Citrix で準備されたイメージ、Azure からインポートしたイメージ、または Citrix DaaS Standard for Azure で構築したイメージを使用してカタログを作成できます。
- ユーザーは、Citrix Workspace がサポートするアイデンティティプロバイダーで構成する必要があります。
- トライアル展開では、最大 25 人のユーザーをカタログに割り当てることができます。1 人のユーザーを複数のカタログに割り当てることはできますが、トライアル展開では合計 25 人の一意の名前付きユーザーが許可されます。
- Microsoft Azure ユーザーアカウントと、そのアカウントに少なくとも 1 つの Azure サブスクリプションが必要です。トライアル版では、お客様が所有する (自社所有の) Azure サブスクリプションのユースケースのみがサポートされます。

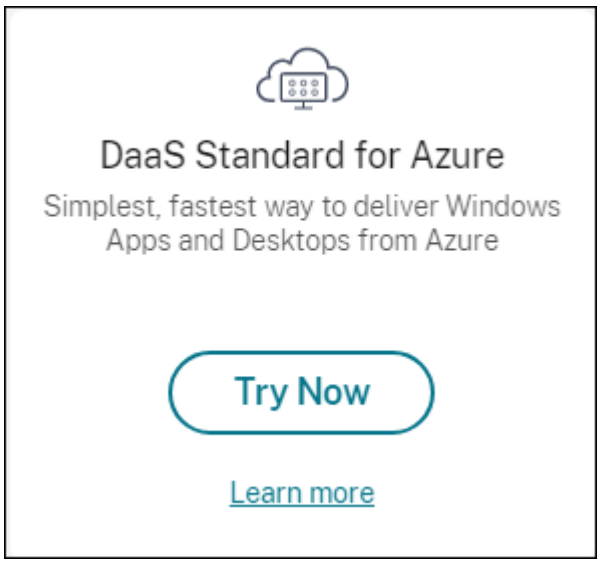
自動承認されたサービストライアルのリクエストと使用

1. Citrix Cloud アカウントにサインアップします（まだ持っていない場合）。

   a) Citrix Cloudを参照します。
   b) [サインアップ] を選択して無料でお試しください。
   c) 画面上のガイダンスに従います。

   しばらくすると、Citrix Cloud アカウントに関するメールが届きます。メールに記載されているサインインリンクを選択します。

2. 試用版をリクエストしてください。Citrix Cloud コンソールで、［**DaaS Standard for Azure**］タイルの［今すぐ試す］を選択します。



サービストライアルの有効化および準備が完了すると、メールが届きます (通常、トライアルをリクエストしてから約 2 時間後)。

3. Citrix Cloudにサインインします。
4. [**DaaS Standard for Azure**] タイルで [管理] をクリックします。
5. トライアル環境をセットアップして構成します。セットアップ中は、次の操作を行います。
   a) Azure サブスクリプションをサービスに追加します。
   b) Citrix Cloud コンソールから ID プロバイダーを接続します。
   c) カタログを作成します。
   d) ID プロバイダからカタログにユーザーを追加します。
   e) Citrix Workspace URL をユーザーに通知します。

グラフィカルインターフェイスは、セットアッププロセスをガイドします。詳しくは、次の製品ドキュメントを参照してください。

- 製品とその用語について知りましょう。
- セットアップの概要と詳細を確認します。

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。このプロセスの詳しくは、「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: Citrix または Azure Marketplace を通じて Citrix DaaS Standard for Azure を注文します。

現在 **Citrix DaaS** にサブスクライブしている場合

Citrix Cloud アカウントでは、Citrix OrgID ごとに一度に 1 つのエディションの Citrix DaaS にのみサブスクライブできます。

Citrix DaaS Standard for Azure から次のエディションのいずれかにアップグレードできます:

- Citrix DaaS Advanced エディション
- Citrix DaaS Premium エディション。

詳しくは、Citrix 担当者にお問い合わせください。

現在、Advanced または Premium 以外の Citrix DaaS エディション（Citrix Virtual Apps Essentials、Citrix Virtual Desktops Essentials など）にサブスクライブしていて、Citrix DaaS Standard for Azure に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、Citrix DaaS Standard for Azure にサブスクライブする。詳しくは、「Citrix DaaS Standard for Azure へのアップグレード」を参照してください。
- 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、Citrix DaaS Standard for Azure 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。

Citrix Managed Azure サブスクリプションを使用するには、Citrix Azure 消費基金を以下のいずれかのサービスエディションで購入します。

- Citrix DaaS Standard for Azure
- Citrix DaaS Advanced
- Citrix DaaS Advanced Plus
- Citrix DaaS Premium

Citrix から購入する

Citrix DaaS Standard for Azure（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 から:

1. Citrix Cloudにサインインします。[**DaaS Standard for Azure**] タイルの [今すぐ試す] 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。Citrix DaaS Standard for Azure が使用可能になると、タイル上のテキストが [管理] に変わります。
3. Citrix Cloudにサインインします。[**DaaS Standard for Azure**] タイルで、[管理] をクリックします。Citrix DaaS Standard for Azure に初めてアクセスすると、クイック展開のようこそページが表示されます。

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。Citrix DaaS Standard for Azure ダッシュボードを使用して、Citrix を通じて注文した毎月のサブスクリプションをキャンセルできます。

(Citrix DaaS Standard for Azure ダッシュボードを使用して、Citrix を通じて注文した他の種類のサブスクリプション、または Azure Marketplace からの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] **>** [**DaaS Standard for Azure**] を選択します。
3. [管理] **> [Azure Quick Deploy**] ダッシュボードで、右側の [一般] 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。

Citrix DaaS Standard for Azure ダッシュボードのバナーに、キャンセルリクエストの受領が表示されます。

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、Citrix DaaS Standard for Azure を再アクティブ化してください。

Azure Marketplace から購入する

まず Citrix DaaS Standard for Azure を注文し、次に Citrix Azure Consumption Fund を注文します。

以前に Citrix DaaS Standard for Azure を購入していない限り、消費基金を注文することはできません。Citrix DaaS Standard for Azure と消費基金を 1 つの注文で組み合わせることはできません。

Citrix DaaS Standard for Azure 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ていません。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、そのアカウント内の少なくとも 1 つの Azure サブスクリプション。

Azure Marketplace で **Citrix DaaS Standard for Azure** を注文する

1. Azure アカウントの資格情報を使用して、Azure Marketplaceにサインインします。
2. 「**Citrix DaaS Standard for Azure**」を検索して移動します。
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. [**Basics**] タブで:
   - 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:
   - [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、Citrix サポートまでお問い合わせください。

Citrix からメールを受信すると、Citrix DaaS Standard for Azure の使用を開始できます。注意: Citrix DaaS Standard for Azure の場合のみ、独自の Azure サブスクリプションのみを使用できます。

Azure 内の Citrix DaaS Standard for Azure リソースを削除しないでください。Azure のサービス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 アカウントの資格情報を使用して、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. Citrix 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。購入したことが Citrix に通知されると、Citrix DaaS for Azure 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が示されます。

   [管理**] > [Azure Quick Deploy**] 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、そのサブスクリプションが使用可能にな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。

保有しているシート数を減らすには、Azure Marketplace で Citrix DaaS Standard for Azure をキャンセルしてから、希望する数のシートを注文します。

Azure Marketplace を通じて **Citrix DaaS Standrad for Azure** または消費基金をキャンセルする

Azure Marketplace を通じて Citrix DaaS Standard for Azure または 消費基金をキャンセルするには、次の手順を実行します:

1. Azure マーケットプレイスにサインインします。

2. **DaaS** を検索してください。
3. [新規] **>** [表示] を選択します。
4. キャンセルするリソースを選択します。
5. リソースの省略記号メニューで、[削除] を選択します。
6. 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。

- Citrix DaaS for Azure
- Citrix DaaS
- Gateway

Citrix DaaS for Azure は、アクティブ化される唯一のサービスです。

Citrix DaaS Standard for Azure を使い始めるには、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、Citrix DaaS Standard for Azure にアクセスします。

- ［**DaaS Standard for Azure**］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］**>** ［**DaaS Standard for Azure**］を選択します。

セットアップのガイダンスについては、「はじめに」を参照してください。

Citrix DaaS Standard for Azure へのアップグレード

現在、Citrix Virtual Apps Essentials または Citrix Virtual Desktops Essentials サービスにサブスクライブしている場合は、次のタスクを完了して Citrix DaaS Standard for Azure にアップグレードします。

1. https://onboarding.cloud.com/で Citrix DaaS Standard for Azure で使用する新しい組織 ID（OrgID）を作成します。（この記事で前述したように、同じ OrgID を使用して複数の Citrix DaaS エディションにサブスクライブすることはできません）。
2. 新しい OrgID を使用して、Citrix DaaS Standard for Azure および Citrix Azure Consumption Fund を購入するには、Citrix 営業担当者にお問い合わせください。（消費基金を注文する必要はありませんが、この基金がなければ、Citrix DaaS Standard for Azure 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］**>** ［**DaaS Standard for Azure**］を選択します。

4. Azure サブスクリプションの 1 つ以上を Citrix DaaS Standard for Azure に追加します。
5. Azure サブスクリプションから 1 つ以上のイメージを Citrix DaaS Standard for Azure にインポートします。
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、カタログを作成します。
7. 作成したカタログにユーザーを追加します 。
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。ワークスペース URL を別のものに変更します 。
    b) Citrix DaaS Standard for Azure 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。ワークスペース URL を、以前 Essentials サービスで使用していたものに変更します 。

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。

開始

September 9, 2022

この記事では、Citrix DaaS Standard for Azure（旧称 Citrix Virtual Apps and Desktops Standard or 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確認し、何をするのかを把握しておく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。

> 重要:
>
> Citrix Cloud およびサブスクライブしている Citrix サービスに関する重要な情報を確実に取得するには、すべてのメール通知を受信できることを確認してください。たとえば、Citrix は、Azure の消費量（使用量）の詳細を記載した情報通知メールを毎月送信します。
>
> Citrix Cloud コンソールの右上隅で、顧客名と OrgID フィールドの右側にあるメニューを展開します。［アカウント設定］を選択します。［マイプロファイル］タブで、［メール通知］セクションのすべてのエントリを選択します。

セットアップタスクの概要

この記事の以下のセクションで、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をします 。
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
   - 実稼働環境での展開
3. ワークスペースの 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慣れていない場合は、概要の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 の責任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、アカウントを取得してサービスにサインアップします。
- システム要件を確認してください。
- 設定手順 ([概念実証または実稼働](#set-up-a-production-deployment)) 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 Azure AD にユーザーを追加します。
3. カタログにユーザーを追加します。
4. ワークスペース URL をユーザーに通知します。

実稼働環境のセットアップ

1. ユーザーの認証に自身の Active Directory または Azure Active Directory を使用する場合は、接続して Citrix Cloud でその方法を設定します。
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します。
3. （Citrix Managed Azure サブスクリプションの代わりに）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します。
4. イメージを作成またはインポートします。Citrix 提供イメージの 1 つをカタログでそのまま使用できますが、これらは主に概念実証の展開を目的としています。
5. Citrix Managed Azure サブスクリプションを使用していて、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場合は、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します。
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、必要に応じてカタログにアプリを追加します。
8. Citrix Managed Azure AD を使用してユーザーを認証している場合は、ディレクトリにユーザーを追加します。
9. カタログにユーザーを追加します。
10. ワークスペース URL をユーザーに通知します。

展開をセットアップした後、Citrix DaaS for Azure の ［監視］ダッシュボードを使用して、デスクトップ使用量、セッション、およびマシンを確認します。

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 アカウントの取得」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 の Azure Virtual Desktop ライセンスのいずれかをリモートデスクトップサービスが実行するための適切なライセンスがあ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、「顧客の責任」を参照してください。

企業の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 接続の要件と準備。

カタログを作成するときに自身の Azure イメージを使用する場合は、Citrix DaaS for Azure にインポートする前に、これらのイメージが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: システムと接続要件。
- 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
- Windows Server 2022（最低でも VDA 2106 が必要）
- Red Hat Enterprise Linux および 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 Enterprise シングルセッション
- Windows 10 Enterprise Virtual Desktop マルチセッション
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022（最低でも VDA 2106 が必要）
- Red Hat Enterprise Linux および 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ら、デスクトップとアプリがある場所のワークスペース 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] > [Azure Quick Deploy] 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 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」の記事を確認してください。

引き続きサービスで問題が発生する場合は、「ヘルプとサポートの利用」の手順に従ってチケットを作成してください。

カタログの作成

October 7, 2022

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すると、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。その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: このカタログには、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: このカタログには、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間での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に、作業負荷を選択します: 低（データエントリなど）、中（オフィスアプリなど）、高（エンジニアリングなど）、またはカスタム。各オプションは、特定のマシン数とマシンあたりのセッション数を表します。それにより、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。
  - カスタムの作業負荷を選択する場合は、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。

- 簡易作成は、最速で開始できる方法です。最小限の情報を指定するだけで、その他の処理は Citrix DaaS for Azure が行います。簡易作成カタログは、テスト環境や概念実証に最適です。
- カスタム作成は、簡易作成より多くの構成項目を選択できます。簡易作成カタログよりも実稼働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。

簡易作成とカスタム作成の比較を次に示します：

簡易作成	カスタム作成
指定する情報が少ない。	指定する情報が多い。
一部の機能の選択肢が少ない。	一部の機能の選択肢が多い。
Citrix 管理の Azure Active Directory ユーザー認証。	選択肢：Citrix 管理の Azure Active Directory、または Active Directory か Azure Active Directory。
オンプレミスネットワークに接続しない	選択肢：オンプレミスネットワークに接続しない、Azure VNet ピアリングに接続しない、および SD-WAN に接続しない。
Citrix 提供の Windows 10 イメージを使用する。このイメージには、現在のデスクトップ VDA が含まれる。	選択肢：Citrix 提供イメージ、Azure からインポートしたイメージ、または Citrix 提供イメージかインポートしたイメージから Citrix DaaS for Azure に組み込んだイメージ。
各デスクトップには、Azure 標準ディスク（HDD）ストレージがある。	複数のストレージオプションを利用できる。
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のデスクトップ。
作成中に電源管理スケジュールを構成できない。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る。（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：

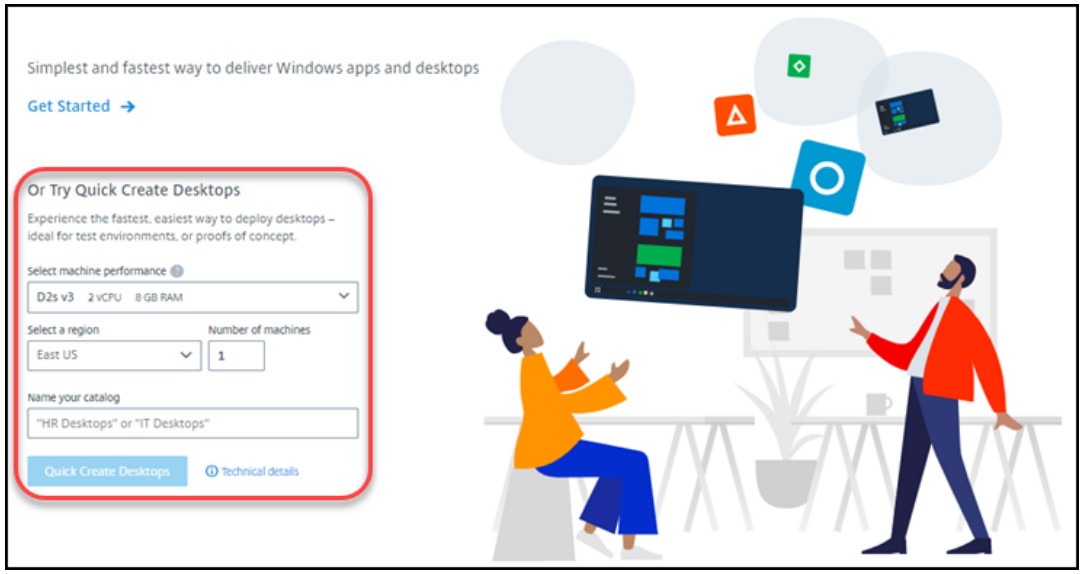
- 簡易作成を使用してカタログを作成します
- カスタム作成を使用してカタログを作成

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。

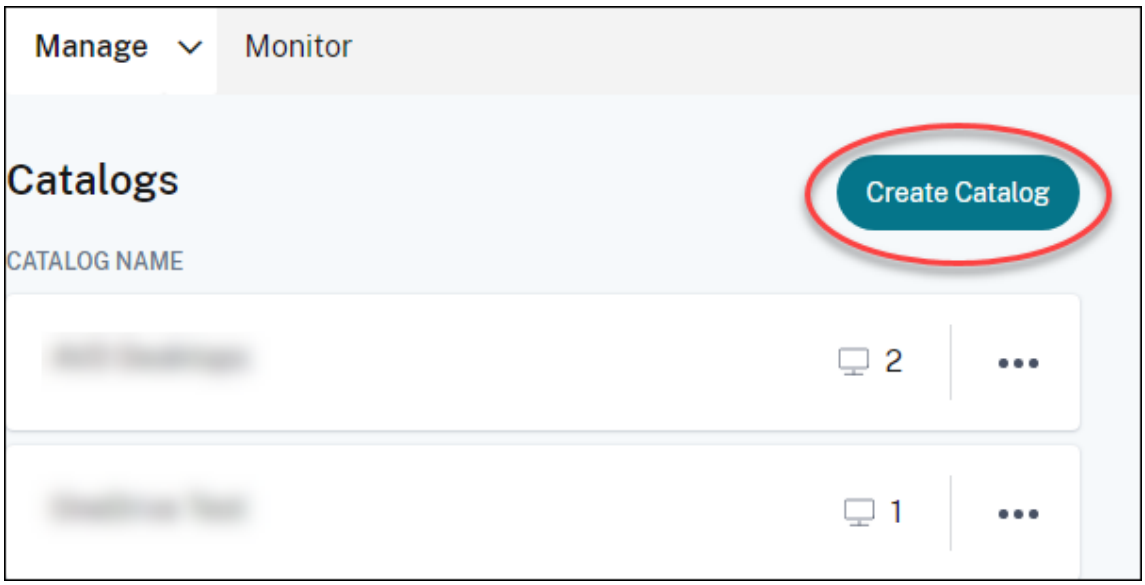
1. Citrix Cloudにサインインします。
2. 左上のメニューで、［マイサービス］**>**［**DaaS Standard for Azure**］を選択します。
3. カタログがまだ作成されていない場合は、クイック展開の [ようこそ] ページが表示されます。次のいずれかを選択します:

   - このページでカタログを構成します。引き続き、手順 6～10 を実行します。

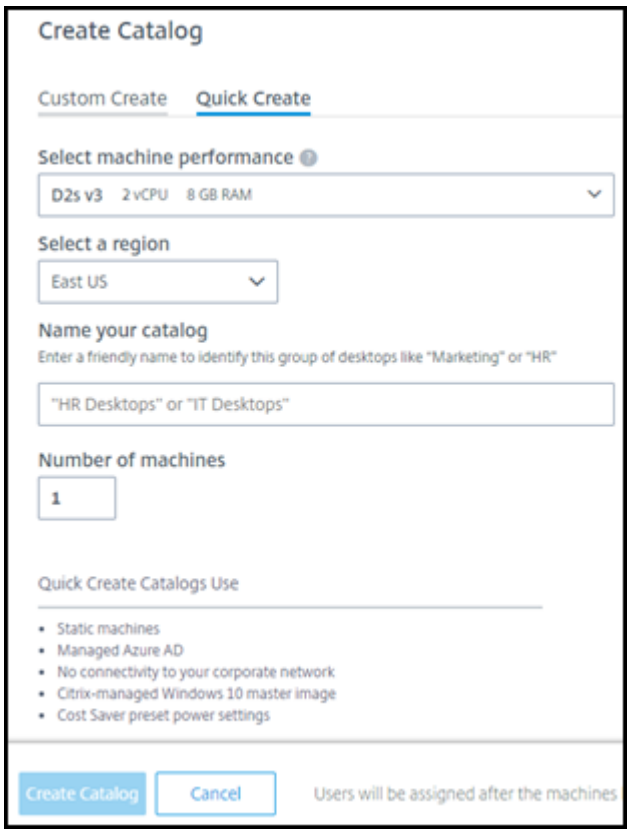
   

   - [始める] をクリックします。[管理**] > [Azure** クイックデプロイ] ダッシュボードが表示されます。［カタログの作成］をクリックします。

4. カタログが既に作成されている (そして別のカタログを作成している) 場合は、[管理**] > [Azure Quick Deploy**] ダッシュボードが表示されます。［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)。



- マシンパフォーマンス：マシンの種類を選択します。それぞれの選択肢には、CPU、RAM、およびストレージの独自の組み合わせがあります。高性能のマシンは月額費用が高くなります。
- 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あり、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。(クイック展開の [ようこそ] ページから最初のカタログを作成する場合は、[デスクトップの簡易作成] をクリックします)。

[管理] **> [Azure** クイックデプロイ] ダッシュボードに自動的に移動します。カタログの作成中に、カタログの名前がカタログ一覧に追加され、作成の進行状況が表示されます。

Citrix DaaS for Azure はまた、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。

次にやること:

- ユーザー認証に Citrix Managed Azure AD を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できます 。
- 使用するユーザー認証方法に関係なく、カタログの作成後にユーザーをカタログに追加します。

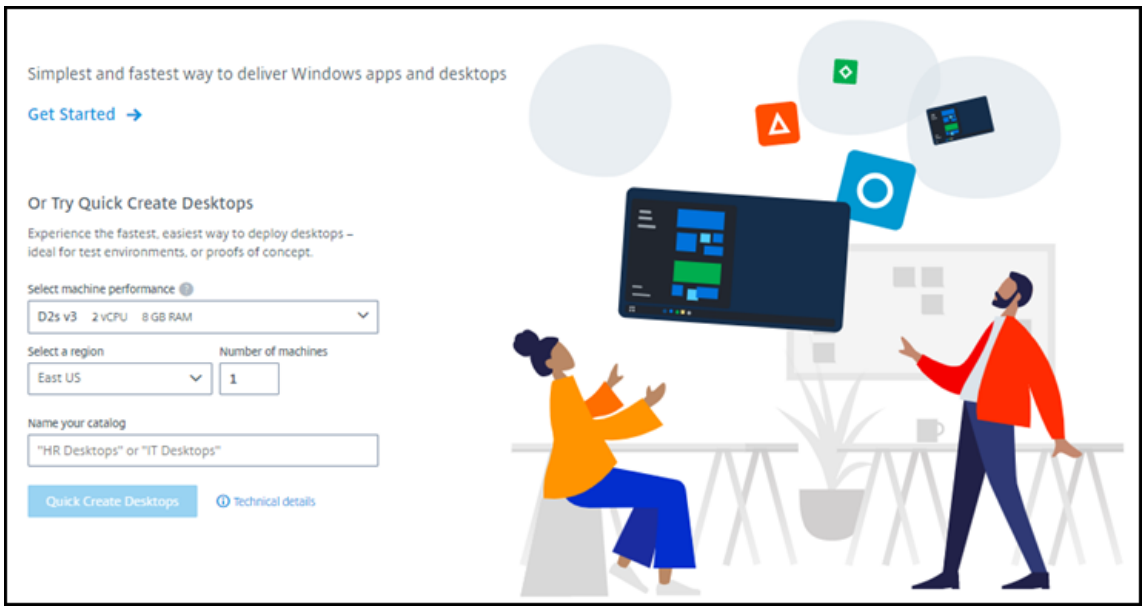
カスタム作成を使用してカタログを作成

Citrix Managed Azure サブスクリプションを使用していて、オンプレミスネットワークのリソースへの接続を使用する予定の場合は、カタログを作成する前に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またはその他のネットワークの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。

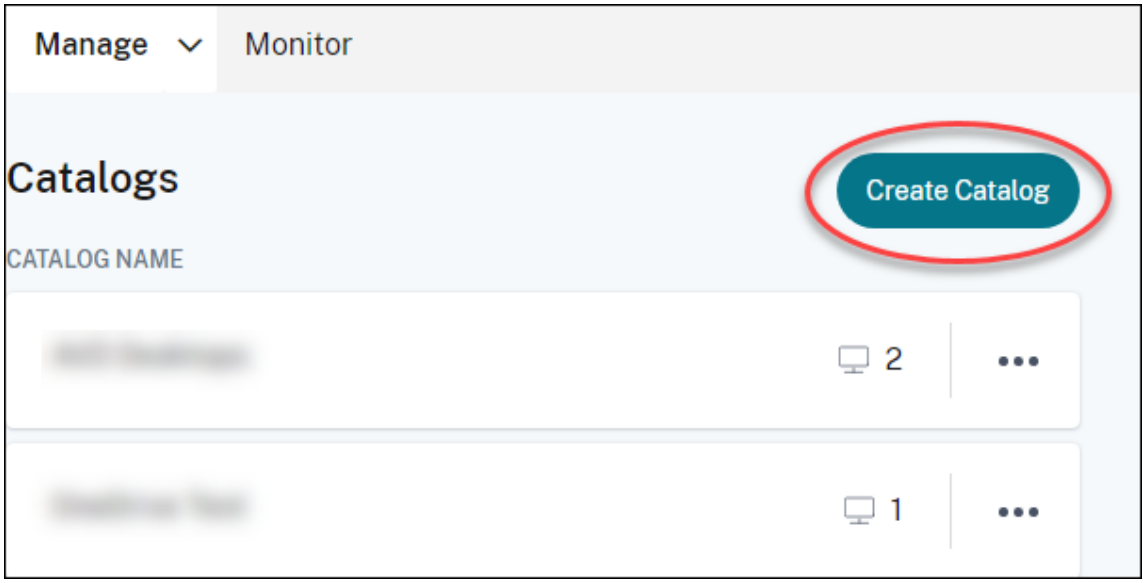
Citrix Managed Azure サブスクリプションがない場合は、カタログを作成する前に、少なくとも 1 つの独自の Azure サブスクリプションを Citrix DaaS for Azure にインポート（追加）する必要があります。

カタログを作成するには:

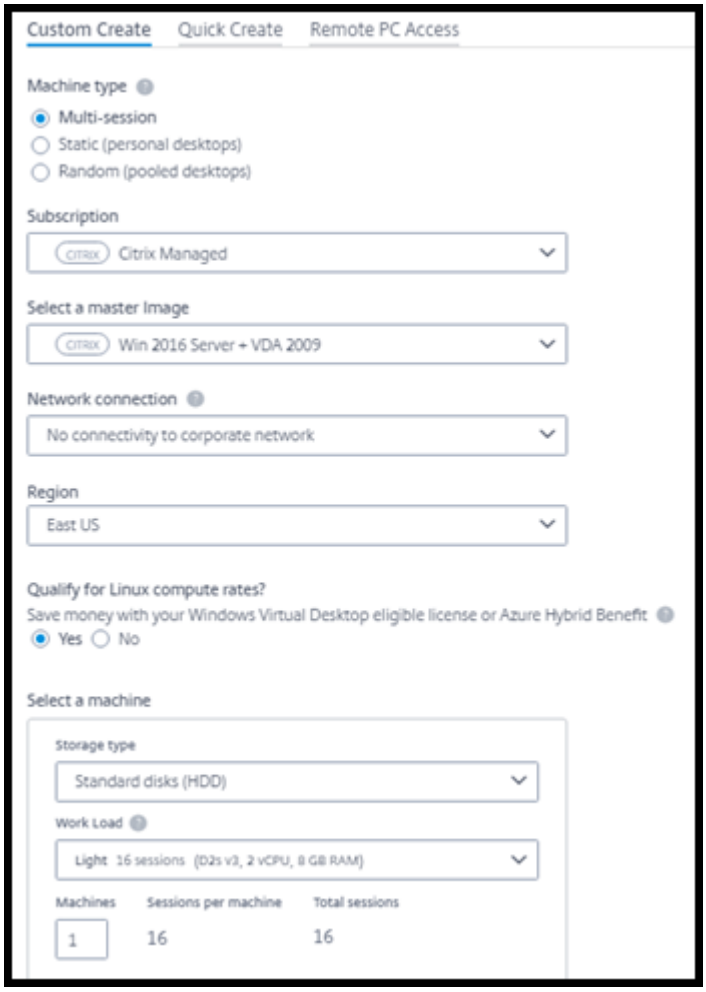
1. Citrix Cloudにサインインします。
2. 左上のメニューで、［マイサービス］**>** ［**DaaS Standard for Azure**］を選択します。
3. カタログがまだ作成されていない場合は、クイック展開の [ようこそ] ページが表示されます。[始める] をクリックします。紹介ページの最後には、[管理] **> [Azure Quick Deploy**] ダッシュボードが表示されます。［カタログの作成］をクリックします。



カタログがすでに作成されている場合は、[管理] **>** [**Azure** クイック展開] 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. まだ選択されていない場合は、ページ上部の [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、特定のマシンの種類に対してのみ有効です。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。マシンの種類を選択します。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、「イメージ」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。

- [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
  - ユーザーごとに Windows 10 VDA

  Windows Server ワークロード用の Software Assurance が付いた RDS CAL のユーザーごとまたはデバイスごとのライセンス。

  Azure Hybrid 特典：アクティブな Software Assurance が付いた Windows Server ライセンス、またはそれと同等の適格なサブスクリプションライセンス。https://azure.microsoft.com/en-us/pricing/hybrid-benefit/を参照してください。

- マシン:

  - ストレージの種類。標準ディスク (HDD)、標準 SSD、またはプレミアム SSD。
  - マシンパフォーマンス（マシンの種類が ［静的］または ［ランダム］の場合)、または ［ワークロード］（マシンの種類がマルチセッションの場合)。選択肢には、選択したイメージの世代の種類（gen1 または gen2）に一致するオプションのみが含まれます。

    カスタムの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数とマシンあたりのセッション数を入力します。
  - マシン。このカタログに必要なマシンの数。

- マシン命名スキーム**:**「マシン命名スキーム」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、「電力管理スケジュール」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。

[管理] > [Azure Quick Deploy] ダッシュボードは、カタログがいつ作成される Citrix DaaS for Azure はまた、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。

次にやること:

- ユーザーが Citrix Workspace に認証するための認証方法の構成をまだ行っていない場合は、構成します。
- カタログが作成されたら、カタログにユーザーを追加します。
- マルチセッションカタログを作成した場合は、(ユーザーを追加する前または後に) アプリケーションを追加します。

Azure AD ドメイン参加マシンのカタログの作成

カスタム作成を使用して、Azure Active Directory に参加しているマシンのカタログを作成できます。

要件

展開には Citrix Cloud Connector が含まれている必要があります。Machine Creation Services は、カタログの作成時に提供された Azure AD ドメインに関する情報に基づいて Cloud Connector をデプロイします。

この種類のカタログは、静的マシンまたはランダムマシンのプロビジョニングにのみ使用できます。マルチセッションマシンのプロビジョニングは、現時点ではサポートされていません。

カタログを作成する前に、マスターイメージを Azure AD に参加させないでください。Citrix MCS が、カタログの作成時にマスターイメージを Azure AD に参加させます。

VDA バージョン 2203 またはそれ以降を使用してください。

Azure Portal で、Virtual Machine User Login の IAM 役割をカタログ内の仮想マシンに割り当てます。これはいくつかの方法で行うことができます:

- 最も安全な方法:静的マシンを作成する場合は、マシンに割り当てられたユーザーに役割を割り当てます。
- 代替方法:カタログへのアクセス権を持つすべてのユーザーに、仮想マシンを含むリソースグループの役割を割り当てます。
- 最も安全性が低い方法:カタログへのアクセス権を持つすべてのユーザーに、サブスクリプションの役割を割り当てます。

カタログ内のマシンに対して、参加する Azure AD を使用するように Workspace 認証を設定します。手順については、「Citrix Cloud でのユーザー認証の構成」を参照してください。

要件、既知の問題、および考慮事項について詳しくは、「Azure Active Directory 参加済みおよび非ドメイン参加済み VDA の構成」で、純粋な Azure AD 参加の場合の VDA 構成に関する情報を参照してください。

カタログを作成するには

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］**>**［**DaaS Standard for Azure**］を選択します。
3. ［管理］**>**［**Azure** クイック展開］の順に選択します。
4. 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。［はじめに］を選択します。紹介ページの最後で、[管理**] > [Azure Quick Deploy**] ダッシュボードに移動します。［カタログの作成］を選択します。カタログがすでに作成されている場合は、［管理］**>**［**Azure** クイック展開］ダッシュボードに移動します。［カタログの作成］を選択します。
5. まだ選択されていない場合は、ページ上部の ［カスタム作成］を選択します。
6. 次のフィールドに入力します。

    - マシンの種類。［静的（個人用デスクトップ）］または［ランダム（プールされたデスクトップ）］を選択します。
    - サブスクリプション。リンクする Azure サブスクリプションを選択します。
    - マスターイメージ。カタログ内のマシンに使用するオペレーティングシステムのイメージを選択します。
    - ネットワーク接続。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。
    - ドメイン構成。ドメインの種類として ［**Azure Active Directory**］を選択します。Workspace 認証でこの Azure AD を使用するように設定するよう促す警告が表示されることがあります。

7. ウィザードの残りの部分を完了してカタログを作成します。

カタログ作成時のリソースの場所の設定

カタログを作成するときに、オプションでいくつかのリソースの場所の設定を構成できます。

クイック展開のカタログ作成ダイアログボックス ［詳細設定］をクリックすると、Citrix DaaS for Azure はリソースの場所の情報を取得します。

- カタログ用に選択したドメインとネットワーク接続のリソースの場所が既にある場合は、作成するカタログで使用するためにそのリソースの場所を保存できます。

  そのリソースの場所に Cloud Connector が 1 つしかない場合は、別の Cloud Connector が自動的にインストールされます。オプションで、追加する Cloud Connector の詳細設定を指定できます。

- カタログ用に選択したドメインとネットワーク接続にリソースの場所を設定していない場合は、リソースの場所を構成するように求められます。

詳細設定の構成：

- （リソースの場所が既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。
- 外部接続の種類：Citrix Gateway サービスを使用、または企業ネットワーク内から。
- Cloud Connector 設定：

- （顧客が管理する Azure サブスクリプションを使用する場合にのみ使用できます）マシンパフォーマンス。この選択肢は、リソースの場所にある Cloud Connector に使用されます。
- （顧客が管理する Azure サブスクリプションを使用する場合にのみ使用できます）Azure リソースグループ。この選択肢は、リソースの場所にある Cloud Connector に使用されます。デフォルトは、その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、その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 [クイック展開カタログ作成] ダイアログに戻ります。

カタログを作成した後、リソースの場所のいくつかの操作を使用できます。詳しくは、「リソースの場所アクション」を参照してください。

マシンの名前付けスキーム

クイック展開を使用してカタログを作成するときにマシンの命名規則を指定するには、[マシン命名規則の指定] を選択します。1〜4 個のワイルドカード（ハッシュ記号）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

- 名前付けスキームには、少なくとも 1 個のワイルドカードを含める必要がありますが、4 個を超えてはいけません。すべてのワイルドカードは一緒に使用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 文字である必要があります。
- 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、山かっこ、パイプ、コンマ、チルダ、感嘆符、記号、ドル記号、パーセント記号、キャレット、丸括弧、中括弧、または下線を含めることはできません。
- 名前をピリオドで始めることはできません。
- 名前を数字だけにす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`、および`-TAC`。

連続する値を数字（0〜9）にするか、文字（A〜Z）にするかを指定します。

たとえば、名前付けスキームとして「`PC-Sales-##`」を指定して「**0**〜**9**」を指定すると、コンピューターアカウントの名前が`PC-Sales-01`、`PC-Sales-02`、`PC-Sales-03`などになります。

増加の余地を十分に持たせてください。

- たとえば、2 つのワイルドカードとその他 13 文字（たとえば、`MachineSales-##`）を使用する名前付けスキームでは、最大文字数（15 文字）を使用します。
- そのため、カタログに 99 台のマシンが含まれていると、その次のマシン作成は失敗します。サービスは、3 桁（100）を使ってマシンを作成しようとしますが、それは 16 文字の名前を作成することになるからです。最大文字数は 15 文字です。
- そのため、この例では、もっと短い名前（たとえば、`PC-Sales-##`）を使用することで、99 台を超えるマシンをスケーリングできるようになります。

マシンの名前付けスキームを指定していない場合、Citrix DaaS for Azure はデフォルトの名前付けスキームDAS%%%%%−**−###を使用します。

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

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にカタログを作成します。
- カタログ情報を表示します。

リモート **PC** アクセス

September 9, 2022

はじめに

> 注:
>
> この記事では、Citrix DaaS for Azure（旧称 Citrix Virtual Apps and Desktops Standard for Azure サービス）でクイック展開管理インターフェイスを使用する場合に、リモート PC アクセスを構成する方法について説明します。完全構成管理インターフェイスを使用するときにリモート PC アクセスを構成する方法については、「リモート PC アクセス」を参照してください。

Citrix リモート PC アクセスにより、ユーザーはオフィスにある物理的な 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

仮想デスクトップおよびアプリの提供に慣れている方は、リモート PC アクセス機能には以下のような違いがあります:

- 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。そのため、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。デスクトップおよびアプリの提供では通常、仮想マシン（VM）が使用され、VM をプロビジョニングするためのテンプレートとしてイメージが使用されます。
- リモート PC アクセスで、ランダムにプールされたカタログ内のマシンが電源オフになっても、イメージの元の状態にリセットされることはありません。
- リモート PC アクセスの静的ユーザー割り当てカタログの場合、割り当ては、ユーザーが（マシンまたは RDP で）ログインした後に行われます。デスクトップとアプリを提供するときにマシンが使用可能であれば、ユーザーが割り当てられます。

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) 準備作業を完了してください。
2. Citrix Cloud で：
   a) Citrix Cloud アカウントを設定し、Citrix DaaS Standard for Azure サービスにサブスクライブします。
   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。

      「リソースの場所の作成とその場所への Cloud Connector のインストール」のガイダンスに従います。このガイダンスには、システム要件、準備、および手順が記載されています。
   c) Active Directory を Citrix Cloud に接続します。
3. ユーザーがリモートでアクセスする各マシンに、Citrix Virtual Delivery Agent（VDA）をインストールします。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 DaaS for Azure クイック展開管理インターフェイスから次の操作を行います：
   a) リモート PC アクセスカタログを作成します。この手順では、リソースの場所の場所を指定し、ユーザーの割り当て方法を選択します。
   b) 必要があれば、利用者（ユーザー）をカタログに追加します。ユーザー割り当て方法のうち、静的自動割り当てまたはランダムプールのいずれかの方法をカタログで使用している場合は、カタログにユーザーを追加します。静的事前割り当てのカタログにユーザーを追加する必要はありません。
5. ワークスペース URL をユーザーに送信します。ユーザーは自分のワークスペースから、オフィスの自分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 Domain Services ドメインに参加している必要があります。
- Citrix Virtual Apps and Desktops でリモート PC アクセスを使用することに慣れている方は、Citrix DaaS for Azure では Wake-on-LAN 機能が使用できないことに注意してください。

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は、マシンを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）。
  - デュアルブートマシン。
- キーボードとマウスをマシンに直接接続します。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。
- ノートブックと Surface Pro デバイスの場合：ノートブックがバッテリーで動作しているのではなく、電源に接続されていることを確認します。デスクトップマシンのオプションに合わせて、ノートブックの電源オプションを構成します。例:
  - 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している場合、ノートブックをドッキング解除して再接続できます。ドッキング解除すると、VDA は Wi-Fi 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ーを切断するまで、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。それ以外のデバイスでは、ワイヤレスアダプターを切断するためのカスタムソリューションか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。

デバイスのリモート PC アクセスでドッキングとドッキング解除を有効にするには:

- ［スタート］**>**［設定］**>**［システム］**>**［電源とスリープ］で、［スリープ］を ［なし］に設定します。
- ［デバイスマネージャー］**>**［ネットワークアダプター］**>**［イーサネットアダプター］で ［電源管理］に移動し、［電力の節約のために、コンピューターでこのデバイスの電源をオフにできるようにする］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、PC のローカル画面はブラックアウトされず、HDX 3D モードが有効になっている場合はセッション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 マシンのカタログは、静的に事前に割り当てられたユーザー割り当て方法を使用する必要があります。Linux マシンを含むカタログでは、静的自動割り当てまたはランダムプールの割り当て方法を使用できません。

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、そのマシンは他のユーザーによって既に使用されている場合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。いくつかの方法が使用可能です:
  - 各マシンに VDA を手動でインストールします。
  - スクリプトを使用し、グループポリシーを使用して VDA のインストールをプッシュします。
  - Microsoft System Center Configuration Manager（SCCM）などの電子ソフトウェア配信（ESD: Electronic Software Distribution）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。
- ユーザー割り当て方法について学習し、使用する方法を決定します。リモート PC アクセスカタログを作成するときに方法を指定します。

- マシン（実際にはマシンにインストールする VDA）を Citrix Cloud に登録する方法を決定します。VDA は、Citrix Cloud のセッションブローカーとの通信を確立するために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）登録には、ポリシーベースの GPO（グループポリシーオブジェクト）または LGPO を使用することをお勧めします。初期登録後は、デフォルトで有効になっている自動更新を使用することをお勧めします。VDA 登録についてはさらに詳しい説明があります。

VDA のインストール

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 のダウンロード

- Windows VDA をダウンロードするには:

  1. Citrix Cloud アカウントの資格情報を使用して、Citrix DaaS ダウンロードページにアクセスします。
  2. 最新の VDA をダウンロードします。2 種類のインストールパッケージを使用できます。VDA タイトルの年と月の値は、場合によって異なります。

- 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 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では、リモート PC アクセスマシンに使用できる 2 種類の Windows VDA インストールパッケージを提供しています:

- シングルセッションコア VDA インストーラー(*release* は *yymm* です):`VDAWorkstationCoreSetup_release.exe`

  シングルセッションコア VDA インストーラーは、リモート PC アクセス用に特別に調整されています。ネットワークを介してすべてのマシンに（他の VDA インストーラーよりも）軽量で簡単に展開できます。Citrix Profile Management、Machine Identity Service、ユーザー個人設定レイヤーなど、こうした展開では通常必要とされないコンポーネントは含まれていません。

  ただし、Citrix Profile Management がインストールされていない場合、Citrix Analytics for Performance 画面と一部のモニターの詳細は使用できません。これらの制限について詳しくは、ブログ投稿記事の「Monitor and troubleshoot Remote PC Access machines」を参照してください。

  完全な分析と監視を表示する必要がある場合は、シングルセッションの完全版 VDA インストーラーを使用してください。

- シングルセッション完全版 VDA インストーラー(*release* は *yymm* です):`VDAWorkstationSetup_release.exe`

  シングルセッション完全版 VDA インストーラーは、シングルセッションコア VDA インストーラー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調整できます。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 **Windows VDA** の対話式インストール

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 Connector のアドレスがわかっている場合は、[手動で指定する] を選択します。Cloud Connector の FQDN（完全修飾ドメイン名）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、同じ作業を繰り返します。
   - Active Directory（AD）構造のどこに Cloud Connector をインストールしたかがわかっている場合は、[**Active Directory** から場所を選択する] を選択して、その場所に移動します。他の Cloud Connector についても、同じ作業を繰り返します。
   - 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（上級）] 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完全版 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（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、このページは表示されません）。
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（まだ選択されていない場合）。[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。資格情報が確認されたら、[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。

フルインストールについて詳しくは、「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たリモート **PC** アクセス用 **Windows VDA** のインストール

- 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:`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放されます。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完全版 VDA インストーラーを使用していて、Profile Management（またはその他のオプションのコンポーネント）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。/remotepcオプションを使用すると、ほとんどのオプションコンポーネントをインストールできなくなります。/includeadditionalオプションは、インストールするコンポーネントを正確に指定します。

  たとえば、次のコマンドにより、Profile Management を除くすべてのオプションの追加コンポーネントがインストールされなくなります。

  ```
  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 のインストール

Linux VDA を対話式でインストールする、またはコマンドラインを使用する方法については、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 アクセスカタログの作成

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している必要があります。

> 重要:
>
> マシンは同時に 1 つのカタログにしか属することはできません。カタログに追加するマシンを指定するときには、この制限は適用されません。しかし、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］**>**［**DaaS Standard for Azure**］を選択します。

3. カタログをまだ作成していない場合は、[クイック展開へようこそ] 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] > [Azure Quick Deploy**] 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します。
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. マシンを追加します。
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、いずれかのリンクをクリックして、カタログにユーザ（ユーザ）を追加します。ユーザー割り当て方法のうち、静的自動割り当てまたはランダムプール未割り当てのいずれかの方法をカタログで使用している場合は、この手順を適用します。

カタログを作成して（必要があれば）ユーザーを追加してから、ユーザーにワークスペース URL を送信します。

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、マシンへのユーザーの割り当て方法を指定します。

- 静的自動割り当て：ユーザー割り当ては、VDA がマシンにインストールされた後、ユーザーがマシンにログオンしたときに発生します（Citrix を使用しない場合、たとえば対面や RDP）。後で、他のユーザーが（Citrix を使用せずに）そのマシンにログオンすると、それらのユーザーも割り当てられます。同時に 1 人のユーザーのみがそのマシンを使用できます。これは、コンピューター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されています（これは通常、マシンとユーザーのマッピング情報を含む CSV ファイルをアップロードすることによって構成されます）。VDA のインストール後、ユーザーがログオンして割り当てる必要はありません。また、カタログの作成後にユーザー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。

  この方法は、Windows と Linux の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。同時に 1 人のユーザーのみがそのマシンを使用できます。これは学校のコンピューターラボに最適です。

  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。

カタログにマシンを追加する方法

注意事項：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場合、マシンをカタログに追加する方法は 3 つあります：

- マシンアカウントを 1 つずつ選択する。
- OU（組織単位）を選択する。
- CSV ファイルを使用して一括で追加する。この CSV ファイル用のテンプレートを使用できます。

マシン名の追加

この方法は、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. マシンの追加を繰り返します。
5. マシンの追加が終了したら、［完了］をクリックします。

OU の追加

この方法は、マシンアカウントが存在する組織単位（OU）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、より細分化するために下位レベルの OU を選択します。そうした細分性が必要ない場合は、上位レベルの OU を選択できます。

たとえば、`Bank`/`Officers`/`Tellers`の場合、より細分性を高めるために［`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。

OU がリモート PC アクセスカタログに割り当てられた後に OU を移動または削除すると、VDA の関連付けに影響し、今後の割り当てで問題が発生します。AD（Active Directory）の変更を計画するときは、カタログに対する OU の割り当てを更新することも考慮に入れてください。

OU を追加するには：

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. 選択に含まれるサブフォルダーを含めるかどうかをチェックボックスで指定します。
4. OU の選択が終了したら、［完了］をクリックします。

一括で追加

1. ［**CSV** テンプレートのダウンロード］をクリックします。

2. テンプレートに、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ている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. ［マシンを一括で追加］ページにファイルをドラッグするか、ファイルを参照します。
5. ファイル内容のプレビューが表示されます。それが目的のファイルでない場合は、別のファイルを作成してから、そのファイルをドラッグまたは参照できます。
6. 完了したら、［完了］をクリックします。

リモート **PC** アクセスカタログの管理

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**] > [Azure Quick Deploy**] 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、マシンを追加または削除できます。
- ［利用者］タブで、ユーザーを追加または削除できます。
- ［マシン］タブで、次のことができます:
  - マシンの追加または削除:［マシンの追加または削除］ボタン。
  - ユーザー割り当ての変更:［割り当ての削除］ゴミ箱アイコン、省略記号メニューの ［マシン割り当てを編集］。
  - 登録されているマシンを確認し、マシンを保守モードにするか、保守モードを解除します。

Azure サブスクリプション

December 28, 2023

はじめに

Citrix DaaS Standard for Azure（旧称 Citrix Virtual Apps and Desktops Standard for Azure サービス）は、Citrix Managed Azure サブスクリプションと、顧客が管理する独自の Azure サブスクリプションの両方をサポートしています。

- 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の 1 つ以上を Citrix DaaS for Azure にインポート (追加) します。この操作により、Citrix DaaS for Azure 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ために、サブスクリプションの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 DaaS Standard for Azure に加えて）Citrix Azure Consumption Fund 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 Managed Azure サブスクリプション	顧客自身の Azure サブスクリプション
ドメイン参加済みマシンまたはドメイン非参加マシンをサポート。	ドメイン参加済みマシンのみをサポート。
カタログの簡易作成およびカスタム作成をサポート。	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 Citrix DaaS for Azure に追加する必要があります。
ユーザー認証の場合、Citrix Managed Azure Active Directory または自身の Active Directory をサポート。	自身の Active Directory と Azure Active Directory を接続可能。
ネットワーク接続オプションに、[接続なし] などがある。	ネットワーク接続オプションに、自身の仮想ネットワークのみがある。
Azure VNet ピアリングを使用してリソースに接続する場合は、Citrix DaaS for Azure 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する。
Azure からイメージをインポートするときは、イメージの URI を指定する。	イメージをインポートするとき、Azure サブスクリプションで VHD を選択するか、ストレージを参照することができる。
顧客の Azure サブスクリプションに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る。	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、Citrix DaaS for **Azure** の **[管理] > [Azure** クイック展開] 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。

顧客が管理する **Azure** サブスクリプションを追加する

顧客が管理する 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、そのサブスクリプションを Citrix DaaS 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所有者権限を持っている場合**:** Azure アカウントで認証するだけです。
- グローバル管理者ではなく、サブスクリプションの所有者権限を持っている場合：サブスクリプションを **Citrix** DaaS for Azure に追加する前に、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 Citrix DaaS for Azure に追加すると、関連するアプリ情報が提供されます。

グローバル管理者である場合に、顧客が管理する **Azure** サブスクリプションを追加する

このタスクには、ディレクトリのグローバル管理者権限とサブスクリプションの所有者権限が必要です。

1. Citrix **DaaS for Azure** の **[**管理**] > [Azure** クイック展開] 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。
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 Citrix DaaS for Azure 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 の資格情報を入力します。
7. 自動的に Citrix DaaS for Azure 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一覧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、顧客が管理する **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。

- Citrix DaaS for Azure 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共同作成者として追加します。
- Azure で作成したアプリに関する情報を使用して、サブスクリプションを Citrix DaaS for Azure に追加します。

Azure AD でアプリを作成し、共同作成者として追加する

1. Azure AD に新しいアプリケーションを登録します:

a) Web ブラウザーから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。

- **Name**：接続名を入力します
- **Application type**：［**Web app / 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) 前述の手順で、［**App Registration**］を選択して詳細を表示します。

b)［**Application ID**］と ［**Directory ID**］をメモします。これは、後でサブスクリプションを Citrix DaaS for Azure に追加するときに使用します。

c)［**Manage**］にある ［**Certificates & secrets**］を選択します。

d)［**Client secrets**］ページで、［**+ New client secret**］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) クライアントシークレットの値をメモします。これは、後でサブスクリプションを Citrix DaaS for Azure に追加するときに使用します。

g) Citrix DaaS for Azure にリンク（追加）する Azure サブスクリプションを選択し、［**Access control (IAM)**］を選択します。

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。

- **Role**： Contributor（共同作成者）
- **Assign access to**： 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 **Citrix DaaS for Azure** 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. Citrix **DaaS for Azure** の **[管理] > [Azure** クイック展開] 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。

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。

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

追加後に Citrix DaaS for Azure が 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と個々のマシン操作が許可されません。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元々 Azure アプリを使用して追加されたものである場合は、Azure アプリを置き換えることができます。

Citrix Managed Azure サブスクリプションの追加

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、マシンとは Citrix VDA がインストールされている VM 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 Connector など、リソースの場所にある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まもなく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要求できます。ダッシュボードには、制限に近づいたときに通知が表示されます。

その 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、カタログの作成（またはカタログへのマシンの追加）はできません。

たとえば、Citrix Managed Azure サブスクリプションごとに 1,000 台のマシンという架空の制限があるとします。

- 同じ Citrix Managed Azure サブスクリプションを使用する 2 つのカタログ（`Cat1`と`Cat2`）があるとします。`Cat1`には現在 500 台のマシンがあり、`Cat2`には 250 台のマシンがあります。
- 将来の容量のニーズを考慮して、`Cat2`に 200 台のマシンを追加します。Citrix Managed Azure サブスクリプションは、現在、950 台のマシンをサポートしています（`Cat 1`で 500 台、`Cat 2`で 450 台）。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ているという通知が表示されます。
- さらに 75 台のマシンが必要な場合、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（または既存のカタログに 75 台のマシンを追加する）ことはできません。サブスクリプションの制限を超えてしまうためです。代わりに、別の Citrix Managed Azure サブスクリプションを要求します。次に、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。

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

- 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。
- 以下を実行する場合に、Citrix Managed Azure サブスクリプション（および追加した顧客管理の Azure サブスクリプション）の中から選択できます：
  - カタログの作成。
  - イメージの作成またはインポート。
  - 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を確実に追加できるようにするには、十分な Citrix ライセンスが必要です。前述の架空の例では、Citrix Managed Azure サブスクリプションを使用して少なくとも 1,500 台のマシンを展開することを見越し、2,000 個の Citrix ライセンスがある場合、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. シトリックスの担当者に連絡して、別の Citrix Managed Azure サブスクリプションを要求してください。続行できるようになれば、担当者がお知らせします。
2. Citrix **DaaS for Azure** の **[管理] > [Azure** クイック展開] 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。
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 つは残っている必要があります。

1. Citrix **DaaS for Azure** の **[管理] > [Azure** クイック展開] 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。
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 の資格情報を入力します。
6. 自動的に Citrix DaaS for Azure 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

May 19, 2023

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について詳しく説明します 。

カタログを作成するときに、ユーザーが Citrix Virtual Apps and Desktops Standard for Azure（旧称 Citrix Virtual Apps and Desktops Standard for Azure）のデスクトップとアプリから社内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、およびその方法を指定します。

Citrix Managed Azure サブスクリプションを使用する場合、選択肢は次のとおりです:

- 接続なし
- Azure VNet ピアリング
- SD-WAN

独自の顧客管理の Azure サブスクリプションのいずれかを使用する場合、Citrix DaaS for Azure 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 Citrix DaaS for DaaS に追加するだけです。

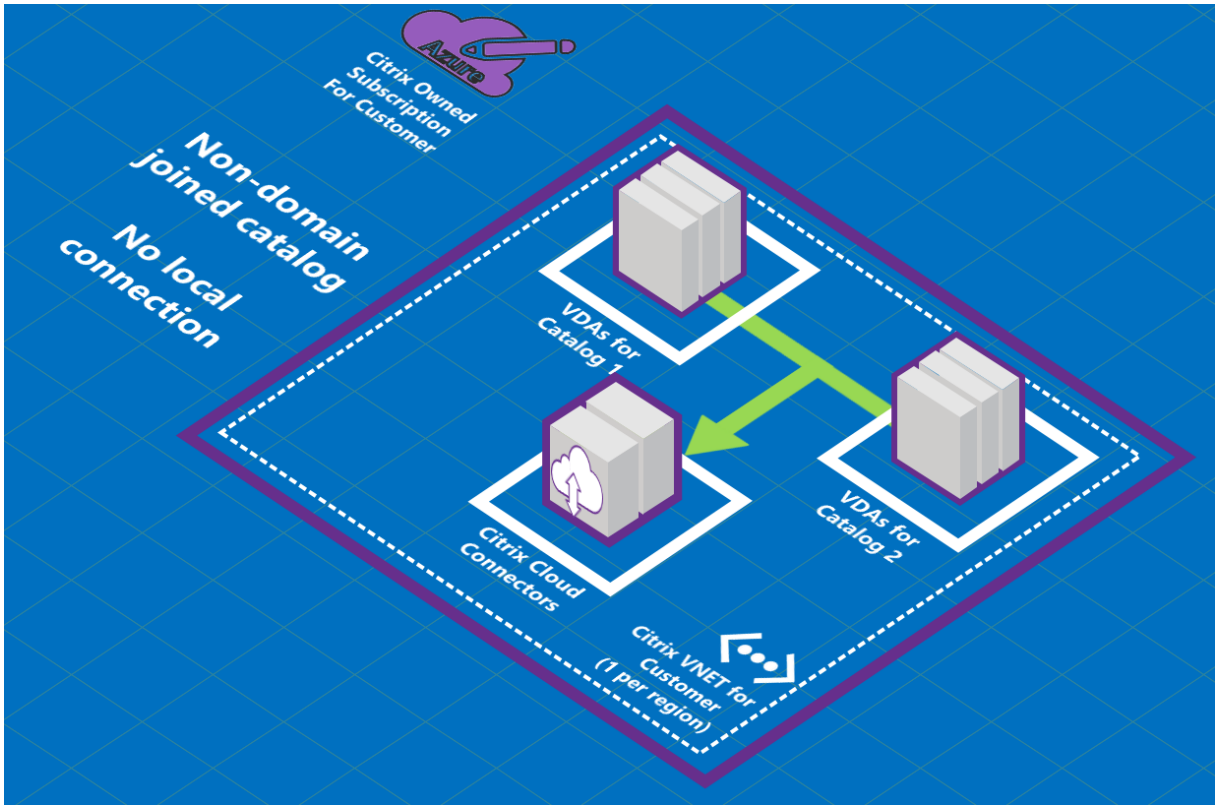
カタログの作成後にカタログの接続の種類を変更することはできません。

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。
- Secure DNS またはサードパーティの DNS プロバイダーを使用する場合は、Citrix DaaS for Azure で使用するために割り当てられたアドレス範囲を、許可リストにある DNS プロバイダーの IP アドレスに追加する必要があります。このアドレス範囲は、接続を作成するときに指定します。
- 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

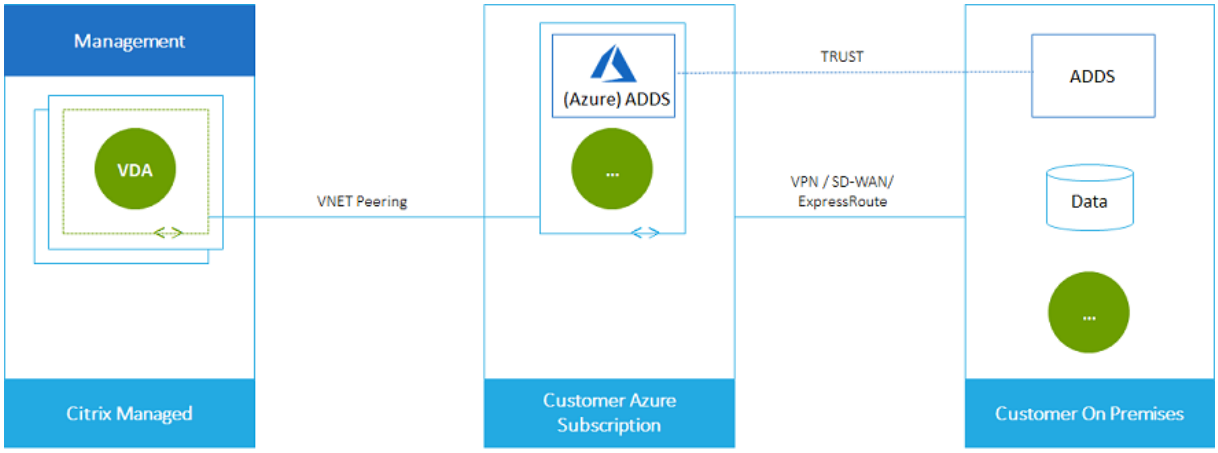
カタログが接続なしで構成されている場合、ユーザーはオンプレミスまたは他のネットワークのリソースにアクセスできません。クイック作成を使用してカタログを作成する場合は、これが唯一の選択肢です。



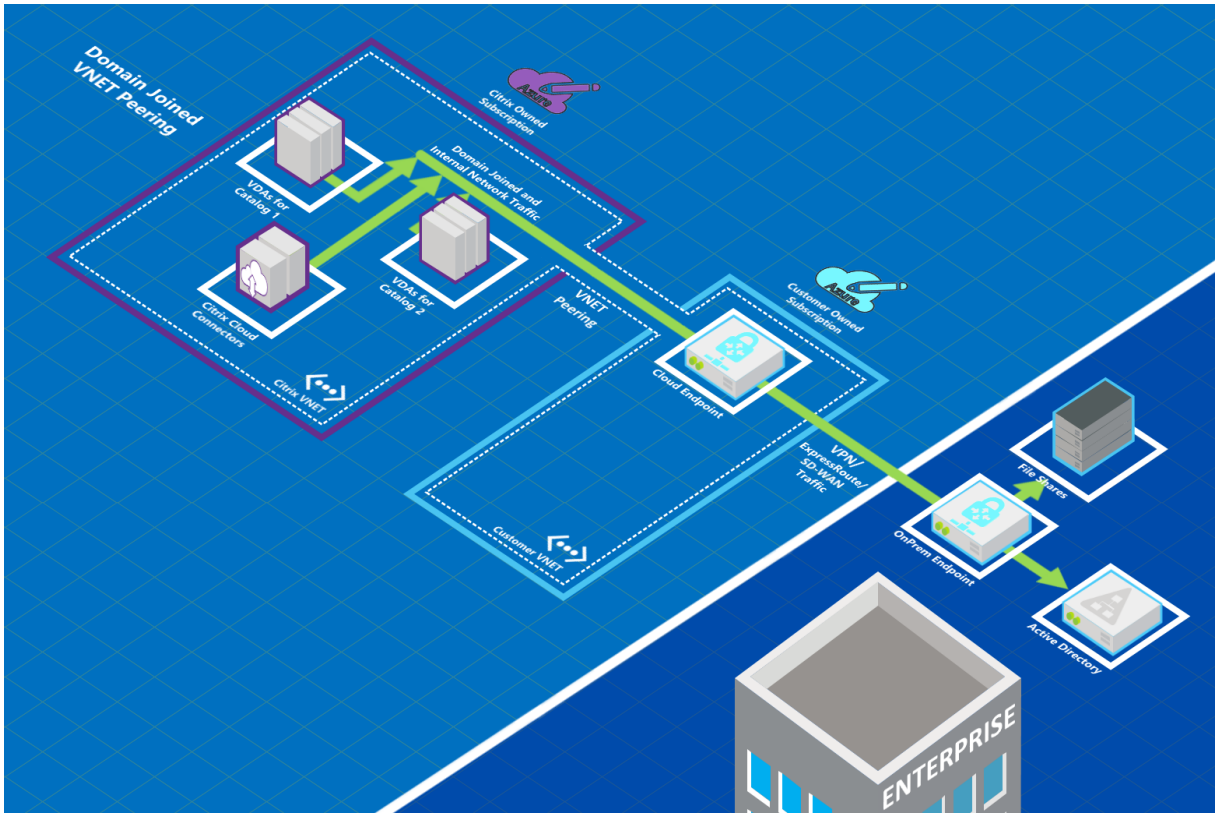
Azure VNet ピアリング接続について

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）：つまりユーザーのネットワークと Citrix DaaS for Azure VNet を、シームレスに接続します。ピアリングは、ユーザーが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するのにも役立ちます。

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:
>
> - Citrix DaaS for Azure で使用する前に、VNet ピアリングについて詳細を把握しておいてください。

> • VNet ピアリング接続を使用するカタログを作成する前に、VNet ピアリング接続を作成します。

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の仮想マシン間でトラフィックを転送するため、Azure のデフォルトのシステムルートよりも優先されます。Citrix DaaS for Azure のリソースがアクセスする予定だが VNet ピアリングで直接接続されていないという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、強制的にトラフィックをネットワークアプライアンス経由でインターネットまたはオンプレミスネットワークサブネットに転送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:

- Citrix DaaS for Azure 環境には、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を確保するために、Citrix DaaS for Azure の接続先 VNet 情報を使用して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、入力した順序で Citrix DaaS for Azure に表示されます。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、Microsoft 社の記事「仮想ネットワークトラフィックのルーティング」を確認して、カスタムルートの使用方法、次ホップの種類、および Azure が送信トラフィックのルートを選択する方法について把握しておいてください。

Azure VNet ピアリング接続を作成するとき、または Citrix DaaS for Azure 環境内の既存の接続に、カスタムルートを追加できます。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 ピアリングを持つカスタムルートの場合:Azure VNet ピアリング接続を作成します。
- 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

AzureVNet 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。Citrix DaaS for Azure は、live.com や外部の Azure AD アカウント（別のテナント内）など、他のアカウントの種類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、ネットワークリソースと接続中 Azure VNet との間で一意の使用可能な 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）を入力する必要があります。これは、Citrix DaaS for Azure のピアリングされた VNet 内の VM に割り当てられた IP 範囲です。

  Azure および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 範囲を指定していることを確認してください。

  - たとえば、Azure VNet のアドレス空間が 10.0.0.0 /16 の場合、Citrix DaaS for Azure で 192.168.0.0 /24 などの VNet ピアリング接続を作成します。
  - この例では、10.0.0.0 /24 の IP 範囲でピアリング接続を作成すると、アドレス範囲に重複すると見なされます。

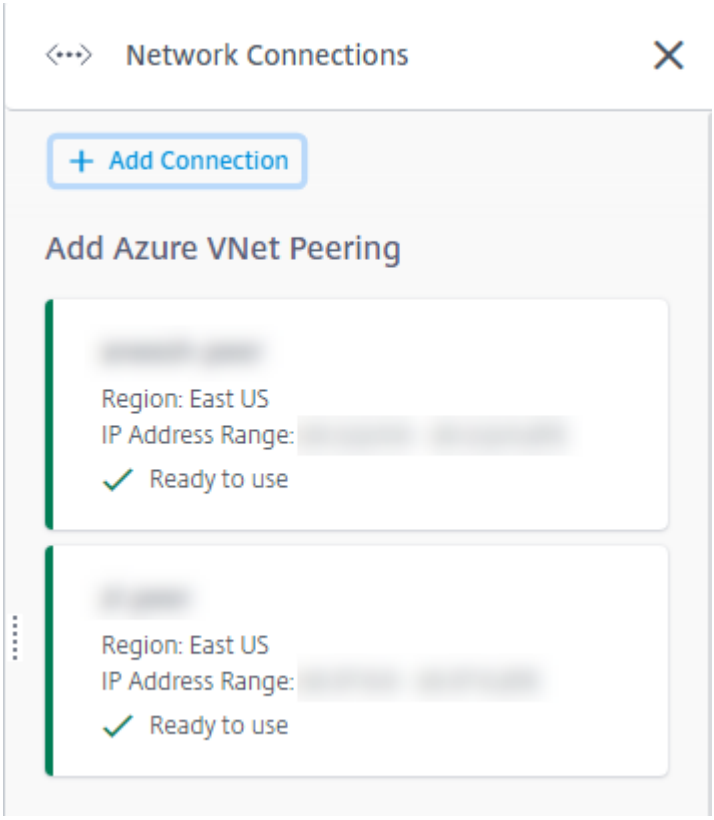
  アドレスが重複している場合、VNet ピア接続が正常に作成されない可能性があります。また、サイト管理タスクで接続が正しく機能しません。

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。

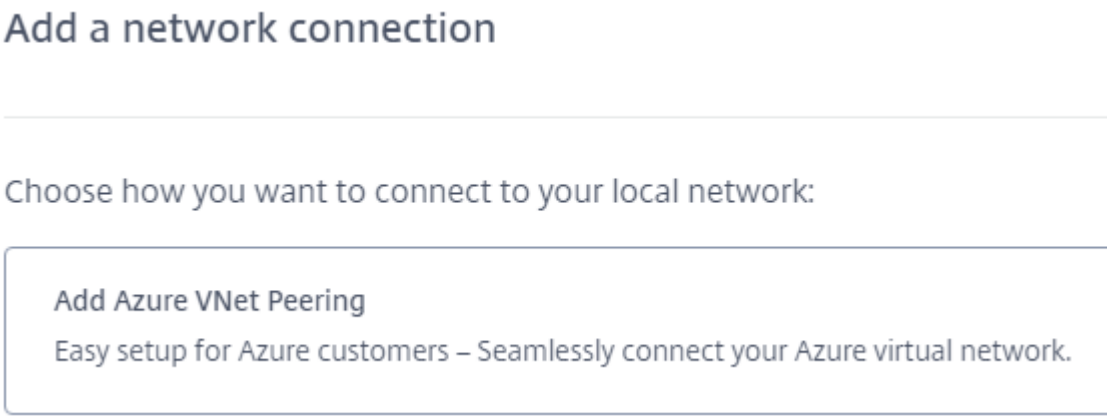
- 仮想ネットワークピアリング
- Azure VPN ゲートウェイ
- Azure ポータルでサイト間接続を作成する
- VPN ゲートウェイに関する FAQ (「オーバーラップ」を検索)

Azure VNet ピアリング接続の作成

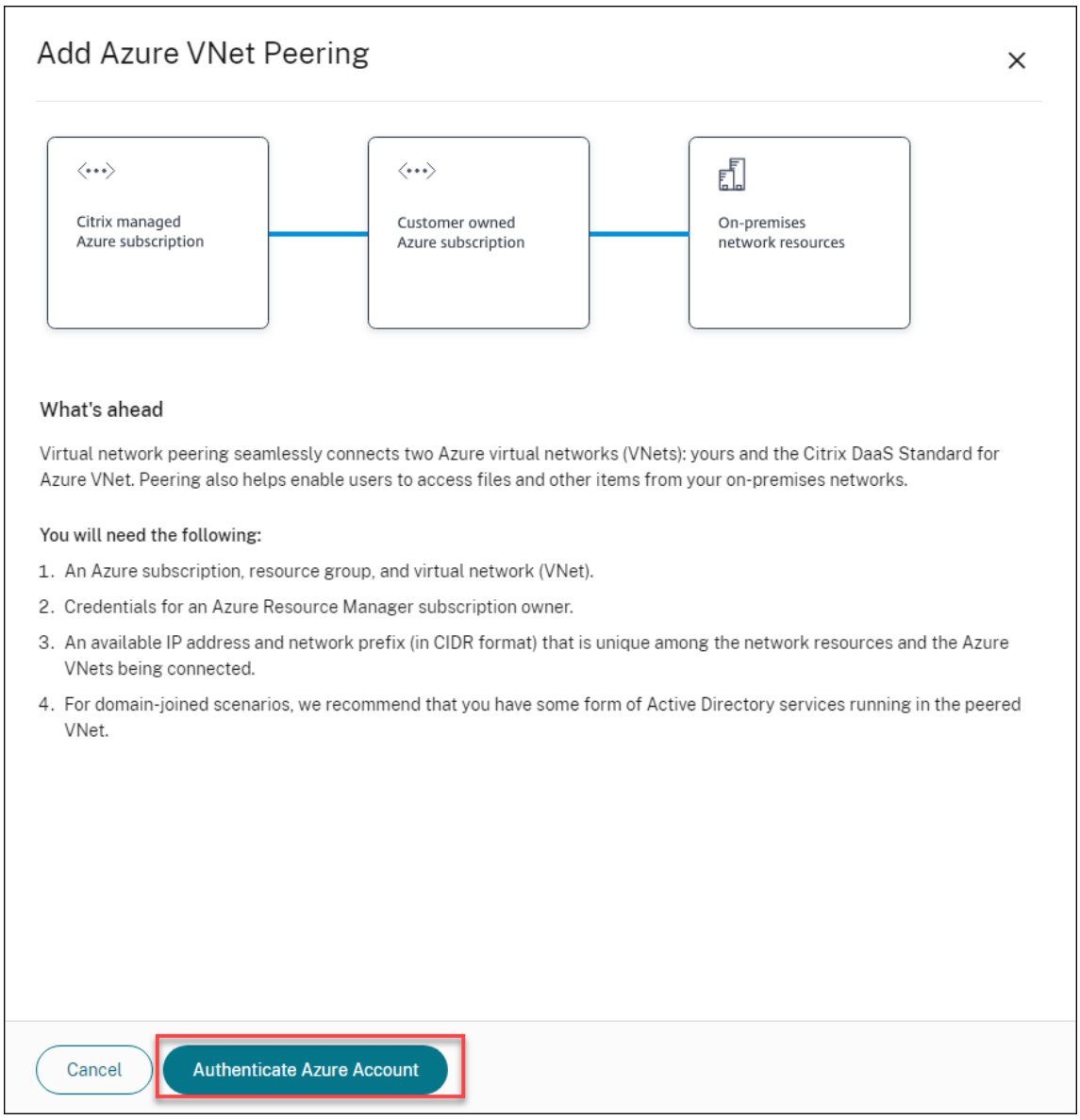
1. Citrix **DaaS for Azure** の **[管理] > [Azure** クイック展開] ダッシュボードから、右側の [ネットワーク接続] を展開します。すでに接続を設定している場合は、その接続が一覧表示されます。



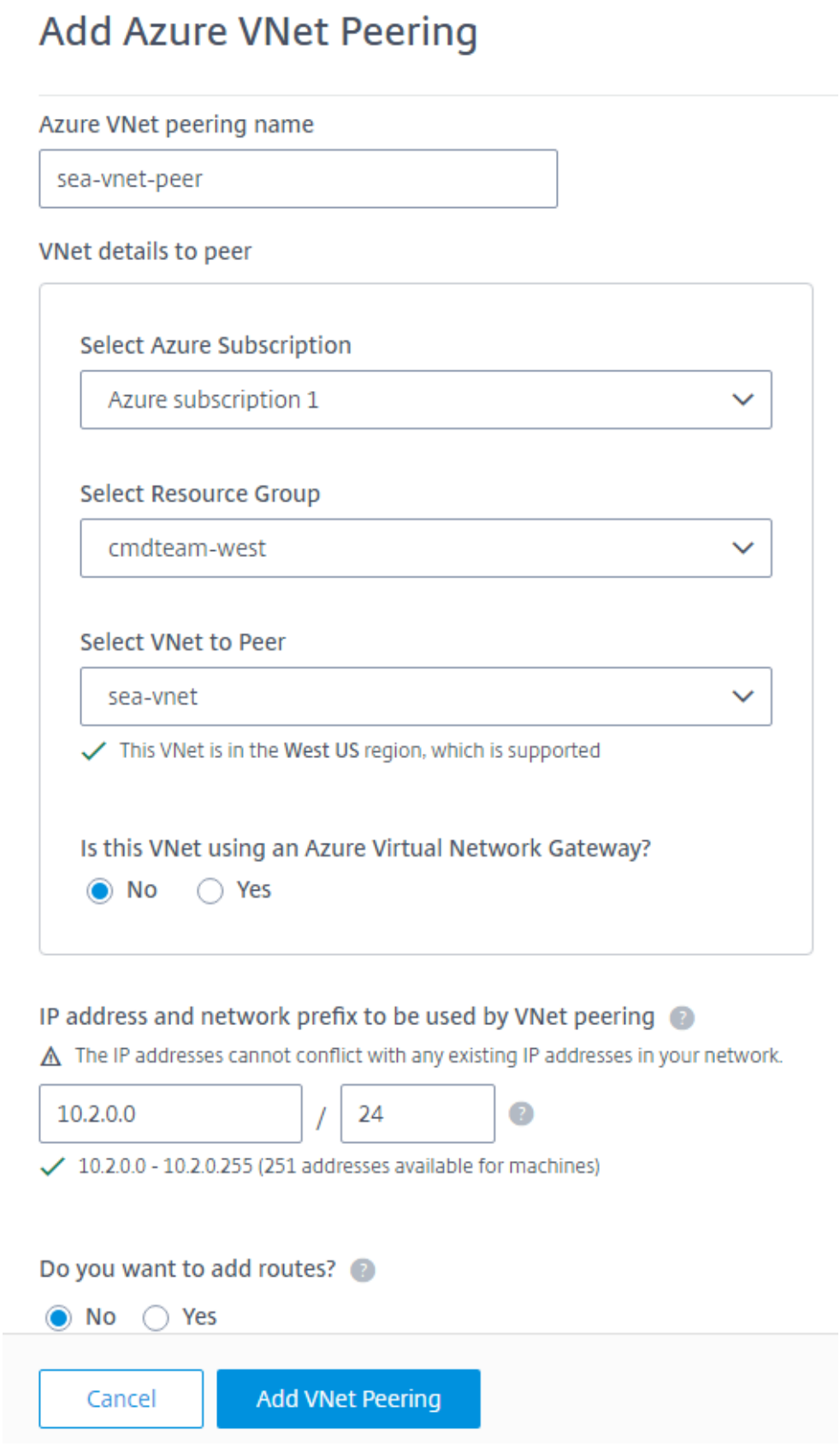
2. [接続の追加] をクリックします。
3. [**Azure VNet** ピアリングの追加] ボックスの任意の場所をクリックします。



4. **[Azure** アカウントの認証**]** をクリックします。



5. Citrix DaaS for Azure では、Azure サブスクリプションを認証するために Azure サインインページに自動的に移動します。グローバル管理者アカウントの資格情報を使用して Azure にサインインし、条件に同意すると、接続作成の詳細ダイアログボックスに戻ります。



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。詳しくは、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。

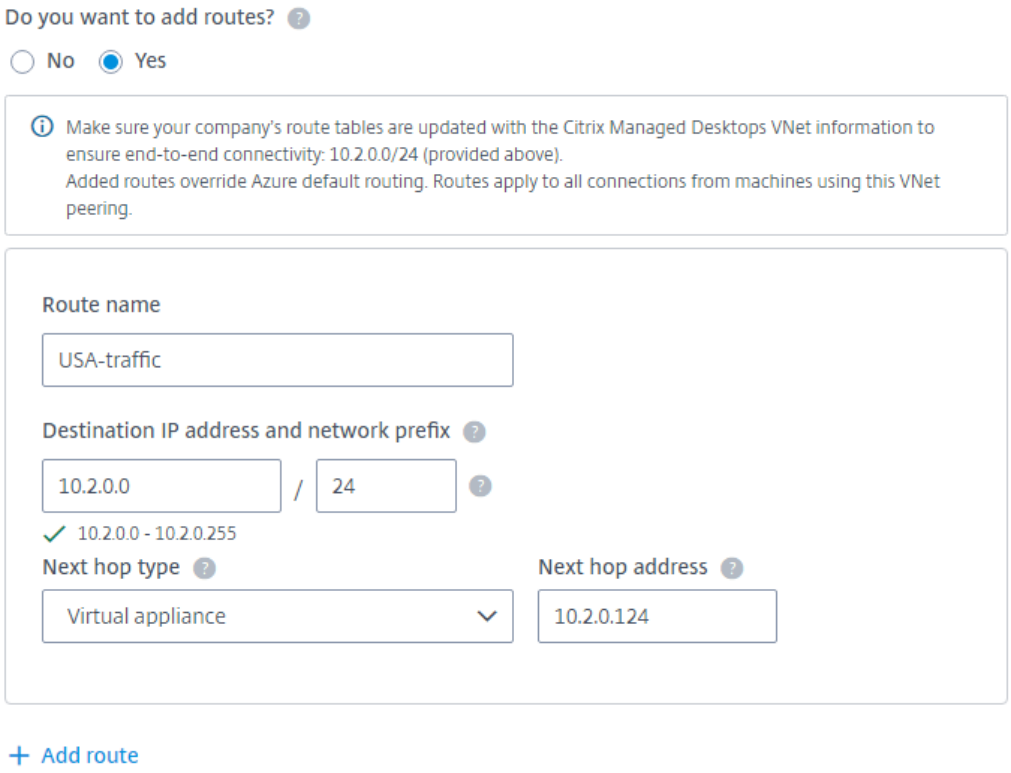
    - たとえば、Azure VNet のアドレス空間が 10.0.0.0/16 の場合、Citrix Virtual Apps and Desktops Standard で、192.168.0.0 /24 などの VNet ピア接続を作成します。
    - この例では、IP 範囲が 10.0.0.0 /24 の VNet ピアリング接続を作成することは、重複するアドレス範囲と見なされます。

    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。



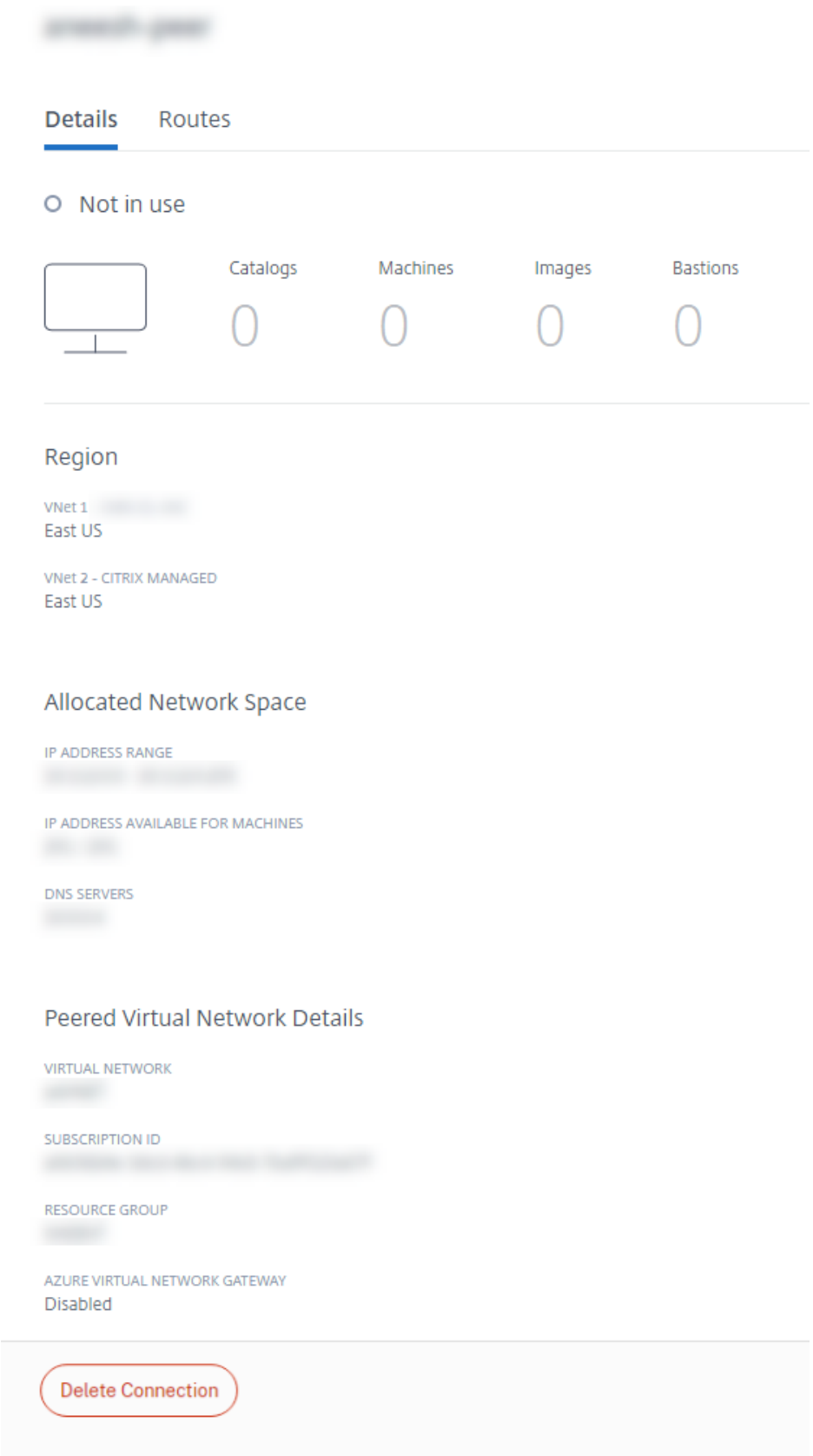
ネクストホップタイプの詳しくは、Microsoft の記事「仮想ネットワークトラフィックルーティング」の「カスタムルート」を参照してください。

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] **> [Azure** クイックデプロイ**]** ダッシュボードの右側にある **[**ネットワーク接続**] > [AzureVNet** ピア] の下に表示されます。カタログを作成すると、この接続は使用可能なネットワーク接続の一覧に表示されます。

Azure VNet ピア接続の詳細を表示する



1. Citrix **DaaS for Azure** の **[管理] > [Azure** クイック展開] 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。

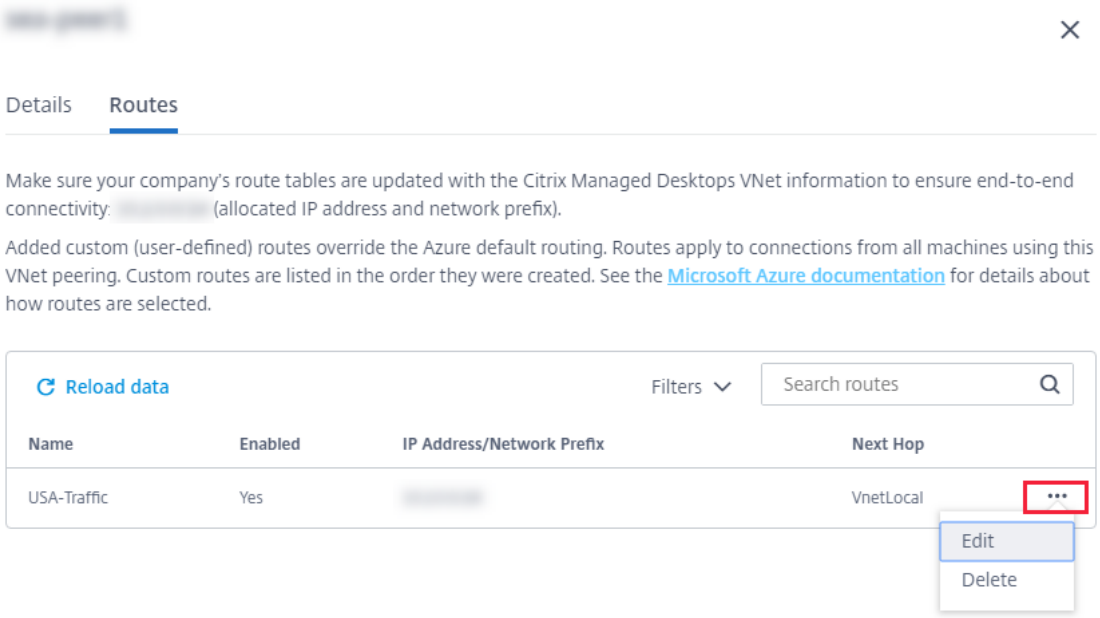
> 重要:
>
> カスタムルートを変更、無効化、または削除すると、接続のトラフィックフローが変更され、アクティブなユーザセッションが中断される可能性があります。

カスタムルートを追加するには:

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、ターゲット IP アドレスとプレフィックス、および使用する次ホップの種類を入力します。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（…）メニューの ［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:

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（…）メニューの ［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. Citrix **DaaS for Azure** の **[管理] > [Azure** クイック展開] 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。

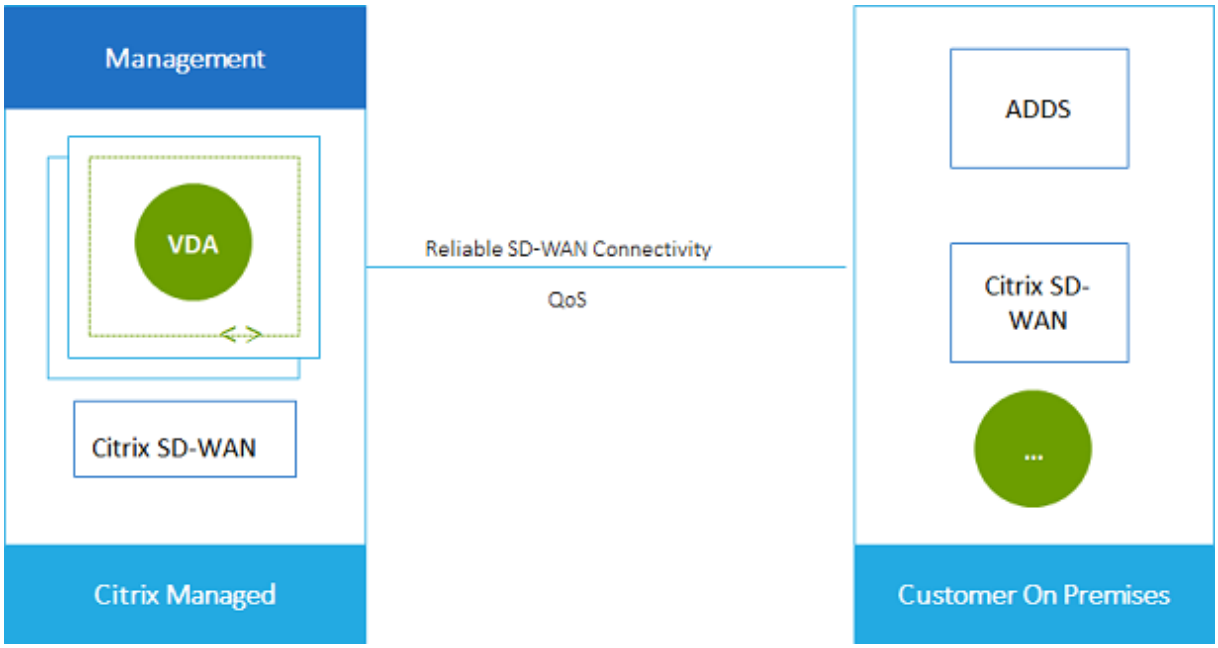
SD-WAN 接続について

> 重要:
>
> Citrix SD-WAN は廃止され、関連するすべてのコンテンツは将来のリリースでドキュメントから削除される予定です。Citrix のサービスに中断なくアクセスできるように、代替のネットワークソリューションに切り替えることをお勧めします。

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 and Desktops Standard 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 などのクラウドでホストされている総合コミュニケーションサービスへの、RTP で伝送されるリアルタイム/インタラクティブトラフィック
- 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 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 and Desktops Standard 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接続が正しく機能しません。

- 接続構成プロセスには、ユーザー（Citrix DaaS for Azure 管理者）と SD-WAN Orchestrator 管理者が完了する必要のあるタスクが含まれています。また、タスクを完了するには、SD-WAN Orchestrator 管理者から提供される情報が必要です。

  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 構成の詳しくは、「Citrix Virtual Apps and Desktops Standard for Azure 統合の SD-WAN 構成」を参照してください。

1. Citrix **DaaS for Azure** の **[**管理**] > [Azure** クイック展開] 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 接続の要件と準備 」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**] > [Azure Quick Deploy**] ダッシュボードで何を探すべきかをまとめています。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**] > [Azure Quick Deploy**] 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、構成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 の管理者タスクについては、SD-WAN Orchestrator の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 接続の詳細の表示

1. Citrix **DaaS for Azure** の **[**管理**] > [Azure** クイック展開] 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 が唯一の選択肢ではない場合は、［**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. Citrix **DaaS for Azure** の **[管理] > [Azure** クイック展開] 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 が唯一の選択肢ではない場合は、［SD-WAN］を選択します。
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。

Azure VPN テクニカルプレビュー

Azure VPN 機能はテクニカルプレビューで利用できます。

Azure VPN ゲートウェイ接続について

Azure VPN ゲートウェイ接続は、Citrix が管理する Azure VDA（デスクトップおよびアプリ）と、オンプレミスのネットワークや他のクラウド上の場所にあるリソースなどの会社のリソースとの間の通信リンクを提供します。これは、リモートブランチオフィスをセットアップして接続する場合と似ています。

セキュリティで保護された接続には、業界標準のプロトコルであるインターネットプロトコルセキュリティ (IPsec) とインターネットキーエクスチェンジ (IKE) が使用されます。

接続の作成プロセスでは、次の操作を行います。

- Citrix がゲートウェイと接続の作成に使用する情報を指定します。
- Citrix は、サイト間ルートベースの Azure VPN ゲートウェイを作成します。VPN ゲートウェイは、Citrix が管理する Azure サブスクリプションと VPN のホストデバイスとの間に直接インターネットプロトコルセキュリティ (IPsec) トンネルを形成します。
- Citrix が Azure VPN ゲートウェイと接続を作成したら、VPN の構成、ファイアウォールルール、およびルートテーブルを更新します。このプロセスでは、Citrix が提供するパブリック IP アドレスと、接続を作成するために指定した事前共有キー（PSK）を使用します。

接続の例を「Azure VPN ゲートウェイ接続を作成する」に示します。

この種類の接続を作成するのに、独自の Azure サブスクリプションは必要ありません。

オプションで、この接続タイプでカスタムルートを使用することもできます。

Azure VPN ゲートウェイのカスタムルート

カスタム (ユーザー定義) ルートは、ネットワーク内の仮想マシンとインターネット間のトラフィックを誘導するデフォルトのシステムルートよりも優先されます。Citrix Virtual Apps and Desktops Standard リソースがアクセスすると予想されるが、Azure VPN ゲートウェイ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、強制的にトラフィックをネットワークアプライアンス経由でインターネットまたはオンプレミスネットワークサブネットに転送するカスタムルートを作成できます。

接続にカスタムルートを追加すると、その接続を使用するすべてのマシンにカスタムルートが適用されます。

カスタムルートを使用するには:

- Citrix Virtual Apps and Desktops Standard 環境には、既存の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場合は、エンドツーエンドの接続を確保するために、会社のルートテーブルを宛先 VPN 情報で更新する必要があります。
- カスタムルートは、[接続] **>** [ルート] タブに入力された順に表示されます。この表示順序は、ルートの選択順序には影響しません。

カスタムルートを使用する前に、Microsoft 社の記事「仮想ネットワークトラフィックのルーティング」を確認して、カスタムルートの使用方法、次ホップの種類、および Azure が送信トラフィックのルートを選択する方法について把握しておいてください。

Azure VPN ゲートウェイ接続を作成するとき、またはサービス環境内の既存の接続にカスタムルートを追加できます。

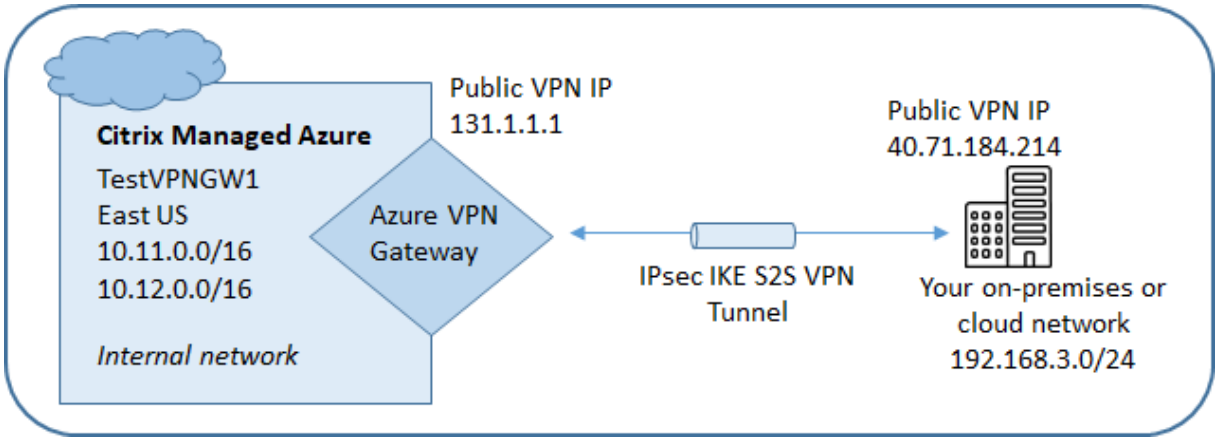
Azure VPN ゲートウェイの接続要件と準備

- Azure VPN ゲートウェイの詳しくは、Microsoft の記事「VPN ゲートウェイとは」を参照してください。
- すべてのネットワーク接続の要件を確認します。
- VPN が設定されている必要があります。仮想ネットワークは VPN ゲートウェイ経由でトラフィックを送受信できる必要があります。1 つの仮想ネットワークを複数の仮想ネットワークゲートウェイに関連付けることはできません。
- パブリック IP アドレスを持つ IPsec デバイスが必要です。検証済みの VPN デバイスについて詳しくは、Microsoft の記事「VPN デバイスについて」を参照してください。
- Azure VPN Gateway 接続を実際に開始する前に、「Azure VPN Gateway 接続の作成 」の手順を確認して、必要な情報を収集できるようにします。たとえば、ネットワーク内で許可されているアドレス、VDA とゲートウェイの IP 範囲、必要なスループットとパフォーマンスレベル、DNS サーバーアドレスなどが必要です。

Azure VPN ゲートウェイ接続を作成する

実際に開始する前に、必ずこの手順を確認してください。

次の図は、Azure VPN ゲートウェイ接続の構成例を示しています。通常、Citrix は図の左側でリソースを管理し、リソースは右側で管理します。次の手順では、図の例への参照を含む説明があります。



1. Citrix DaaS for Azure の ［管理］ダッシュボードから、右側にある ［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. [**Azure VPN** ゲートウェイ] ボックスの任意の場所をクリックします。
4. [**VPN** 接続の追加] ページの情報を確認し、[**VPN** 設定の開始] をクリックします。
5. [接続の追加**]** ページで、次の情報を入力します。

    - 名前**:** 接続の名前。(この図では、名前は TestVPNGW1 です)。
    - **VPN IP** アドレス**:** 公開されている IP アドレス。

      この図では、住所は 40.71.184.214 です。
    - 許可されたネットワーク： Citrix サービスがネットワーク上でアクセスを許可されている 1 つ以上のアドレス範囲。通常、このアドレス範囲には、ファイルサーバーなど、ユーザーがアクセスする必要のあるリソースが含まれます。

      複数の範囲を追加するには、[**IP** アドレスを追加] をクリックして値を入力します。必要に応じて繰り返します。

      この図では、アドレス範囲は 192.168.3.0/24 です。
    - 事前共有キー**:** VPN の両端で認証に使用される値 (パスワードと同様)。この値を決めるのはあなたです。必ず値を書き留めておいてください。この情報は、後で接続情報を使用して VPN を設定するときに必要になります。
    - パフォーマンスとスループット**:** ユーザーがネットワーク上のリソースにアクセスするときに使用する帯域幅レベル。

      すべての選択肢がボーダーゲートウェイプロトコル (BGP) をサポートしているとは限りません。このような場合、[**BCP** 設定**]** フィールドは使用できません。
    - リージョン： この接続を使用するカタログを作成するときに、デスクトップおよびアプリ（VDA）を配信するマシンが Citrix によって展開される Azure リージョン。接続の作成後は、この選択を変更するこ

とはできません。後で別のリージョンを使うことにした場合は、目的のリージョンを指定する別の接続を作成するか使用する必要があります。

この図では、リージョンは EastUS です。

- アクティブ/アクティブ **(**高可用性**)** モード**:** 高可用性のために 2 つの VPN ゲートウェイが作成されるかどうか。このモードを有効にすると、一度に 1 つのゲートウェイだけがアクティブになります。アクティブ/アクティブ Azure VPN ゲートウェイについては、Microsoft ドキュメント「高可用性クロスプレミス接続」を参照してください。
- **BGP settings:** (選択した [パフォーマンスとスループット] が BGP をサポートする場合にのみ使用できます。) ボーダーゲートウェイプロトコル (BGP) を使用するかどうか。BGP については、Microsoft ドキュメント「Azure VPN ゲートウェイを使用した BGP について」を参照してください。BGP を有効にする場合は、次の情報を入力します。
  - 自律システム番号 **(ASN):** Azure 仮想ネットワークゲートウェイには、既定の ASN 65515 が割り当てられます。2 つのネットワークゲートウェイ間の BGP 対応接続では、それぞれの ASN が異なる必要があります。必要に応じて、ASN を今すぐ、またはゲートウェイの作成後に変更できます。
  - **BGP IP** ピアリング **IP** アドレス**:** Azure は 169.254.21 *x* から 169.254.22 *x* の範囲の BGP IP をサポートします。
- **VDA** サブネット: この接続を使用するカタログを作成するときに、Citrix VDA（デスクトップとアプリを配信するマシン）と Cloud Connector が存在するアドレス範囲。IP アドレスを入力してネットワークマスクを選択すると、アドレス範囲と、その範囲でサポートされるアドレスの数が表示されます。

  このアドレス範囲は Citrix 管理の Azure サブスクリプションでは維持されますが、ネットワークの拡張であるかのように機能します。
  - IP 範囲は、オンプレミスまたは他のクラウドネットワークで使用するアドレスと重複してはいけません。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、重複するアドレスは、サイト管理タスクでは正しく機能しません。
  - VDA サブネット範囲はゲートウェイサブネットアドレスと異なる必要があります。
  - この値は、接続の作成後は変更できません。別の値を使用するには、別の接続を作成します。

  この図では、VDA サブネットは 10.11.0.0/16 です。
- ゲートウェイサブネット**:** この接続を使用するカタログを作成するときに Azure VPN ゲートウェイが存在するアドレス範囲。
  - IP 範囲は、オンプレミスまたは他のクラウドネットワークで使用するアドレスと重複してはいけません。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、重複するアドレスは、サイト管理タスクでは正しく機能しません。
  - ゲートウェイサブネット範囲は、VDA サブネットアドレスと異なる必要があります。
  - この値は、接続の作成後は変更できません。別の値を使用するには、別の接続を作成します。

この図では、ゲートウェイサブネットは 10.12.0.9/16 です。

- – カスタムルートのフレンドリ名を入力します。
  - – 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。
  - – 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。ネクストホップタイプの詳しくは、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。

複数のルートを追加するには、[**Add route**] をクリックし、必要な情報を入力します。

- **DNS** サーバー**:** DNS サーバーのアドレスを入力し、優先するサーバーを指定します。DNS サーバーのエントリは後で変更できますが、変更すると、この接続を使用するカタログ内のマシンで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。

  3 つ以上の DNS サーバーアドレスを追加するには、**[**代替 **DNS** の追加] をクリックし、必要な情報を入力します。

6. [**VPN** 接続の作成] をクリックします。

Citrix が接続を作成すると、Citrix DaaS for Azure の ［管理］ダッシュボードの ［ネットワーク接続］**>** [**Azure VPN Gateway**] に一覧表示されます。接続カードにはパブリック IP アドレスが含まれています。（この図では、アドレスは 131.1.1.1 です）。

- このアドレス (および接続の作成時に指定した事前共有キー) を使用して VPN とファイアウォールを構成します。事前共有鍵を忘れた場合は、接続の [詳細] ページで変更できます。VPN ゲートウェイのエンドを設定するには、新しいキーが必要です。

  たとえば、構成した VDA およびゲートウェイサブネットの IP アドレス範囲について、ファイアウォールで例外を許可します。

- 会社のルートテーブルを Azure VPN Gateway 接続情報で更新し、エンドツーエンドの接続を確保します。

  この図では、192.168.3.0/24 から 10.11.0.0/16、10.12.0.9/16（VDA およびゲートウェイサブネット）に向かうトラフィックに新しいルートが必要です。

- カスタムルートを設定した場合は、カスタムルートにも適切な更新を行います。

接続の両端が正常に構成されると、[ネットワーク接続**] > [Azure VPN Gateway]** の接続のエントリに [使用準備完了] と表示されます。

Azure VPN ゲートウェイ接続を表示する

1. Citrix DaaS for Azure の ［管理］ダッシュボードから、右側にある ［ネットワーク接続］を展開します。

2. 表示する接続を選択します。

   ディスプレイ:

- ［詳細］タブには、この接続を使用するカタログ、マシン、イメージ、踏み台の数が表示されます。また、この接続に設定したほとんどの情報も含まれています。
- [ルート] タブには、接続のカスタムルート情報が表示されます。

Azure VPN ゲートウェイ接続のカスタムルートを管理する

既存の Azure VPN ゲートウェイ接続では、カスタムルートを追加、変更、無効化、および削除できます。

接続の作成時にカスタムルートを追加する方法については、「Azure VPN ゲートウェイ接続を作成する」を参照してください。

> 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化し、アクティブなユーザーセッションが中断される可能性があります。

1. Citrix DaaS for Azure の ［管理］ダッシュボードから、右側にある ［ネットワーク接続］を展開します。
2. 表示する接続を選択します。
   - カスタムルートを追加するには:
     a) 接続の [ルート**]** タブで、**[**** ルートの追加 ******] をクリックします。
     b) フレンドリ名、ターゲット IP アドレスとプレフィックス、および使用する次ホップの種類を入力します。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。
     c) 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。
     d) [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有効/無効にするには:
     a) 接続の [ルート] タブで、管理するカスタムルートを見つけます。
     b) 省略記号（…）メニューの ［編集］を選択します。
     c) 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を変更します。
     d) ルートを有効にするかどうかを指定します。
     e) [保存] をクリックします。
   - カスタムルートを削除するには:

a) 接続の [ルート] タブで、管理するカスタムルートを見つけます。

b) 省略記号（…）メニューの ［削除］を選択します。

c) 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。

d) [ルートを削除] をクリックします。

Azure VPN ゲートウェイ接続をリセットまたは削除する

> 重要:
>
> - 接続をリセットすると現在の接続が失われ、両端で接続を再確立する必要があります。リセットすると、アクティブなユーザセッションが中断されます。
> - 接続を削除する前に、その接続を使用しているカタログをすべて削除してください。「カタログの削除」を参照してください。

接続をリセットまたは削除するには:

1. Citrix DaaS for Azure の ［管理］ダッシュボードから、右側にある ［ネットワーク接続］を展開します。
2. リセットまたは削除する接続を選択します。
3. 接続の [詳細] タブで、次の操作を行います。
   - 接続をリセットするには、[接続のリセット] をクリックします。
   - 接続を削除するには、[接続の削除] をクリックします。
4. プロンプトが表示されたら、アクションを確定します。

パブリック静的 **IP** アドレスを作成する

接続上のすべてのマシン VDA で、インターネットへの単一の送信パブリック静的 IP アドレス（ゲートウェイ）を使用する場合は、NAT ゲートウェイを有効にします。NAT ゲートウェイは、ドメインに参加しているカタログまたはドメインに参加していないカタログへの接続に対して有効にできます。

接続で NAT ゲートウェイを有効にするには、次の手順を実行します。

1. Citrix **DaaS for Azure** の **[**管理**] > [Azure** クイック展開] 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. [ネットワーク接続] で、[**CITRIX** 管理] または [**AZURE VNET** ピアリング] で接続を選択します。
3. [接続の詳細] カードで、[**NAT** ゲートウェイを有効にする] をクリックします。
4. [NAT ゲートウェイの有効化] ページで、スライダを **[**はい**]** に移動し、アイドル時間を設定します。
5. [変更を確認] をクリックします。

NAT ゲートウェイを有効にすると、次のようになります。

- Azure はパブリック静的 IP アドレスをゲートウェイに自動的に割り当てます。(この住所は指定できません)。この接続を使用するすべてのカタログ内のすべての VDA は、そのアドレスをアウトバウンド接続に使用します。
- アイドルタイムアウト値を指定できます。この値は、NAT ゲートウェイ経由で開いているアウトバウンド接続が、接続が閉じられるまでにアイドル状態を維持できる時間 (分) を示します。
- ファイアウォールでパブリック静的 IP アドレスを許可する必要があります。

[接続の詳細] カードに戻って NAT ゲートウェイを有効または無効にし、タイムアウト値を変更できます。

画像

September 9, 2022

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 DaaS Standard for Azure（旧称 Citrix Virtual Apps and Desktops Standard for Azure）には、Citrix が提供するイメージがいくつか用意されています。

- Windows 10 Enterprise（シングルセッション）
- Windows 10 Enterprise Virtual Desktop（マルチセッション）
- Office 365 ProPlus を使用する Windows 10 Enterprise Virtual Desktop（マルチセッション）
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Linux Ubuntu（シングルセッションおよびマルチセッション）

シトリックス提供イメージには、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、Citrix DaaS for Azure 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

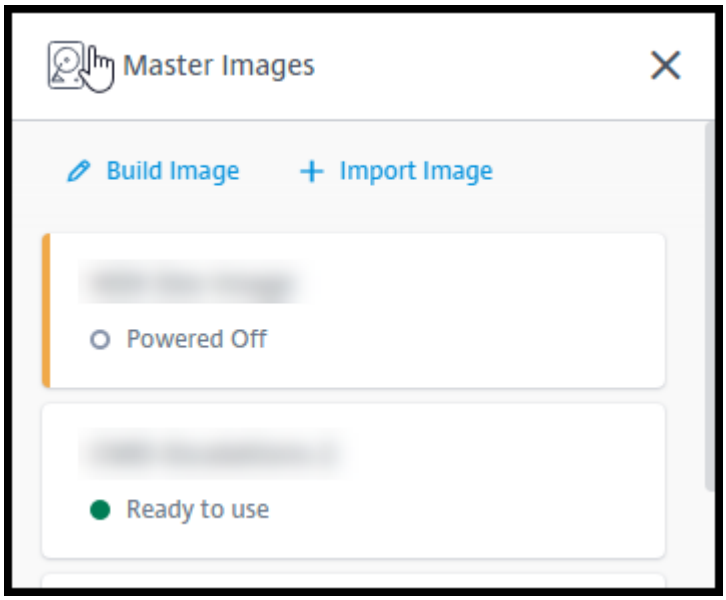
次の操作を実行できます:

- カタログ作成時に、シトリックス提供イメージを使用する。この選択肢は、概念実証の展開を行う場合にのみ推奨されます。
- シトリックス提供イメージを使用して、別のイメージを作成する。新しいイメージの作成後、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する。Azure からイメージをインポートした後、カタログを作成するときに、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。

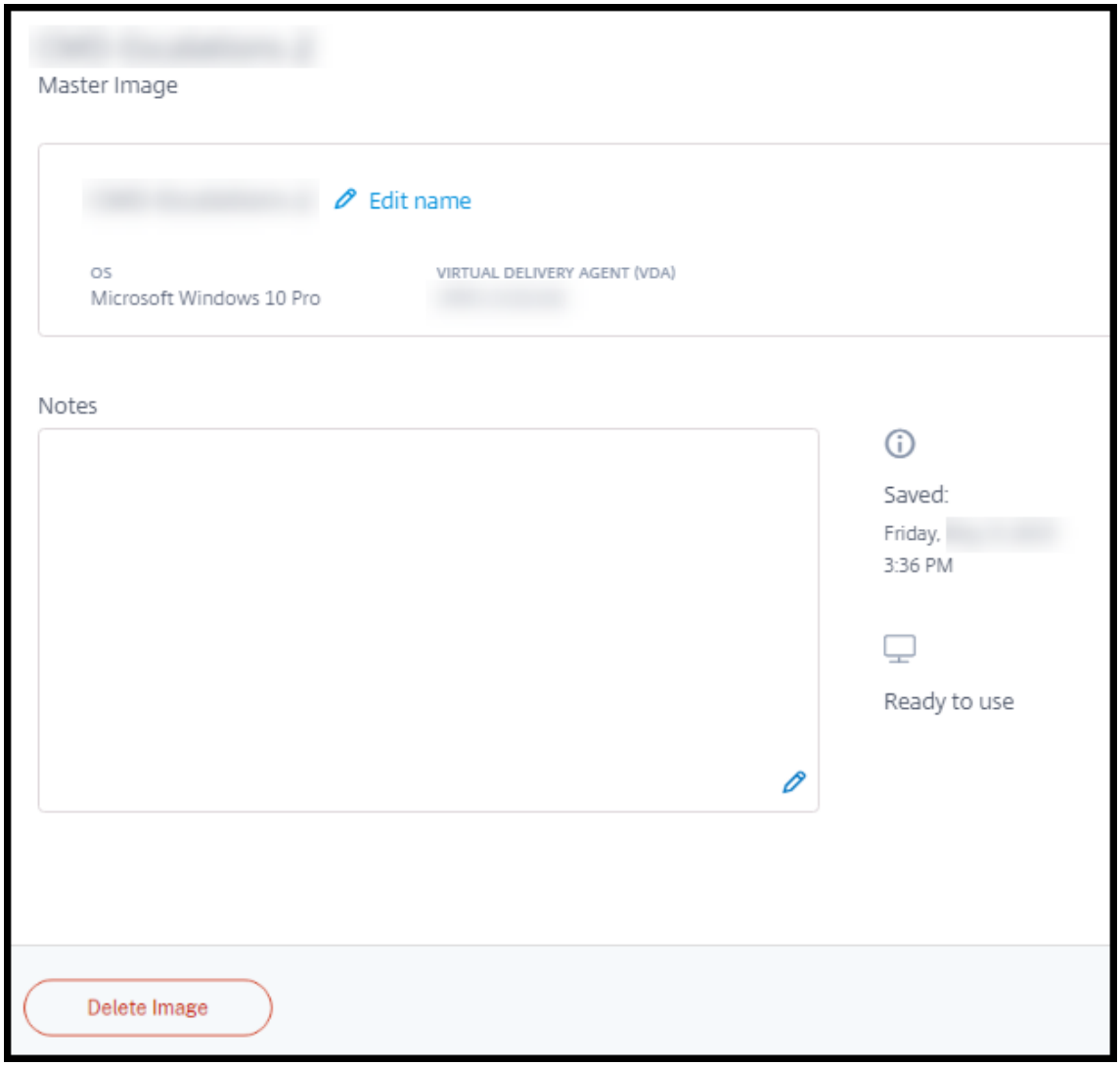
カタログを作成すると、Citrix DaaS for Azure は、イメージで有効なオペレーティングシステムが使用されていること、および Citrix VDA とトラブルシューティングツールがインストールされていることを（他のチェックとともに）確認します。

イメージ情報の表示

1. 管理**] > [Azure Quick Deploy**] ダッシュボードで、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。



この詳細カードで、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。

新しいイメージの準備

新しいイメージの準備には、イメージを作成してからそれをカスタマイズする作業が含まれます。イメージを作成すると、新しい VM が作成され、新しいイメージを読み込みます。

要件:

- マシンに必要なパフォーマンス特性を把握すること。たとえば、CAD アプリを実行するには、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。

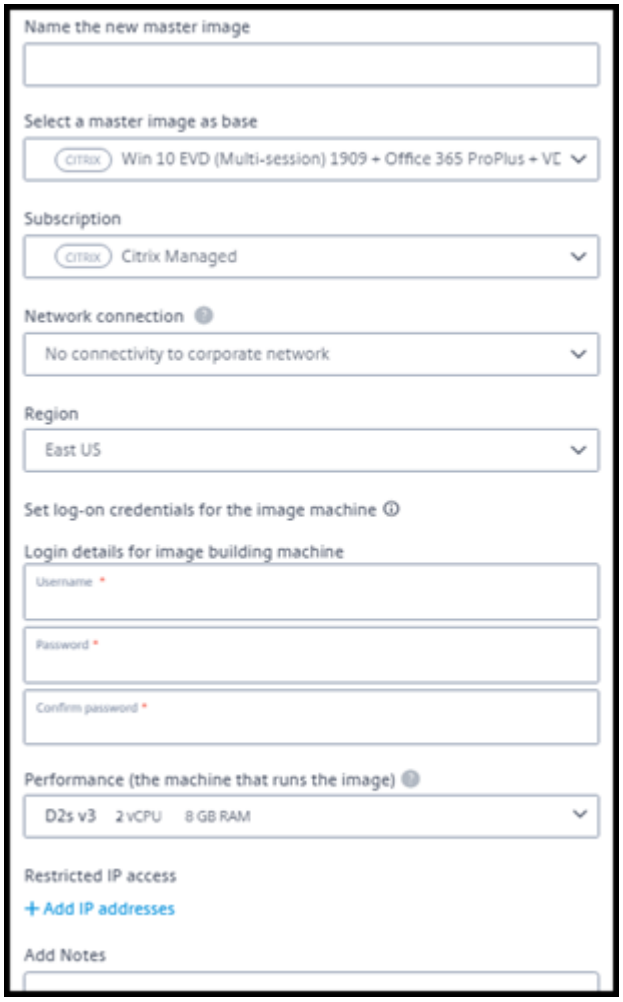
- オンプレミスリソースへの接続を行う予定の場合は、イメージとカタログを作成する前にその接続を設定すること。詳しくは、「ネットワーク接続」を参照してください。

シトリックス提供の Ubuntu イメージを使用して新しいイメージを作成すると、新しいイメージのルートパスワードが作成されます。このルートパスワードは変更できますが、変更できるのはイメージの作成およびカスタマイズを行うときのみです（イメージがカタログで使用された後に、ルートパスワードを変更することはできません）。

- イメージが作成されると、指定した管理者アカウント（イメージ作成マシンのログインの詳細）が`sudoers`グループに追加されます。
- 新しいイメージを含むマシンに RDP 接続した後、端末アプリケーションを起動し、「`sudo passwd root`」と入力します。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パスワードを入力します。確認後、ルートユーザーの新しいパスワードを入力するように求められます。

イメージを作成するには：

1. 管理**] > [Azure Quick Deploy**] ダッシュボードで、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、新しいイメージを作成するため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。
  - 独自の顧客管理の 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、および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、および資格情報を追加します。
- ドメイン構成：ドメインの種類として、Active Directory またはドメイン非参加を選択します。
  - Active Directory を選択した場合は、ドメインを選択または追加します。OU（オプション）、サービスアカウント名、およびパスワードを指定します。
  - ドメイ非ン参加を選択した場合、追加情報は必要ありません。
- リージョン：（[接続なし］の場合にのみ使用可能。）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接続（RDP）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、およびストレージの情報です。アプリの要件を満たすマシン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。イメージが作成されたら、イメージの詳細画面で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。

イメージの作成には最大 30 分かかることがあります。[管理**] > [Azure Quick Deploy**] 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 **[**カスタマイズ可能**]** など) を確認します。

次にやること：新しいイメージに接続してカスタマイズします。

新しいイメージへの接続とカスタマイズ

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. 管理**] > [Azure Quick Deploy**] ダッシュボードで、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。

   イメージマシンを作成した直後に RDP を実行しないと、イメージマシンの電源がオフになる場合があります。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資格情報を入力します。
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、選択可能なイメージの一覧にこの新しいイメージが表示されます。

[管理**] > [**クイック展開] 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

Citrix VDA とユーザーが必要とするアプリケーションを備えたイメージを Azure からインポートすると、そのイメージを使用してカタログを作成したり、既存のカタログのイメージを置き換えたりすることができます。

インポートされたイメージの要件

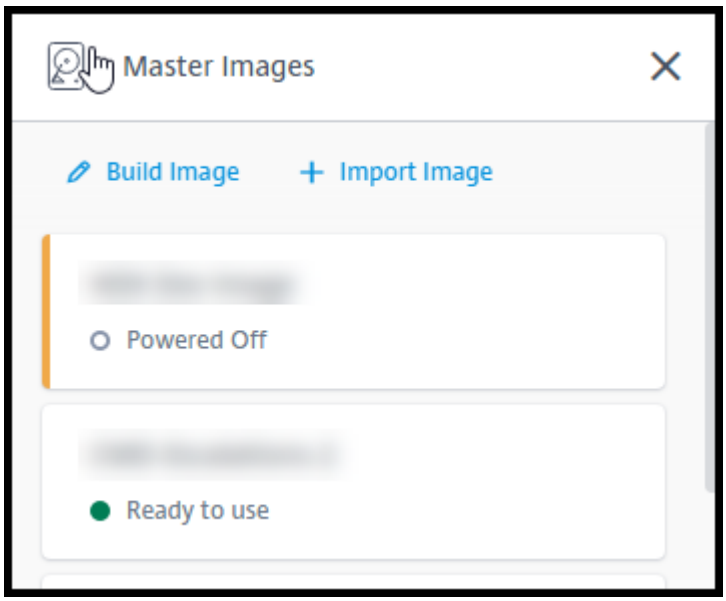
> 注:
>
> Citrix DaaS for Azure では、Azure 第 2 世代 VM に関連付けられているディスクのインポートをサポートしていません。

シトリックスは、インポートされたイメージに対して検証テストを実行します。Citrix DaaS for Azure 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。

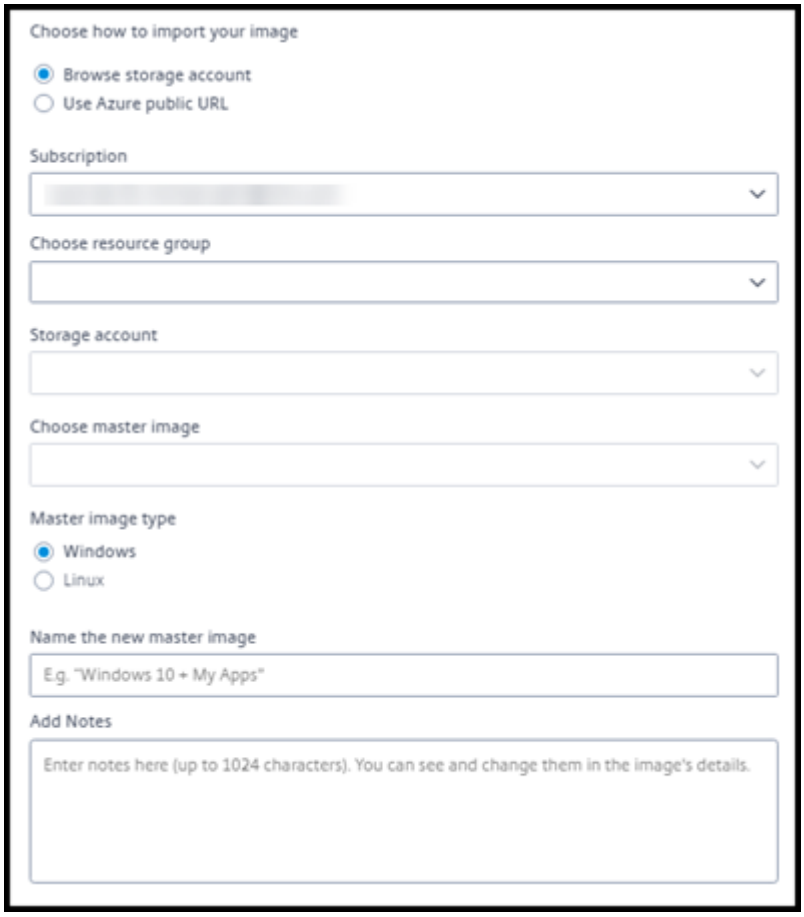
- サポートされるオペレーティングシステム：イメージはサポートされている OSである必要があります。Windows OS のバージョンを確認するには、「`Get-WmiObject Win32_OperatingSystem`」を実行します。
- サポートされる世代：第 1 世代の VM のみがサポートされています。
- 一般化しない イメージは一般化されてはいけません。
- 構成された **Delivery Controller** がない：イメージで Citrix Delivery Controller が構成されていないことを確認します。次のレジストリキーがないことを確認してください。
  - `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。インストール手順については、「イメージへの Windows VDA のインストール」を参照してください。
  - Red Hat Enterprise Linux および Ubuntu：インストール手順については、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 の記事「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. 管理] **> [Azure Quick Deploy**] ダッシュボードで、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 7,200

秒以上に設定してください。

- 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 を生成する。
  - 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する。その後、ファイルの URL を取得する。

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］の順に選択します。
   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) VHD の Azure 生成 URL を入力します。ガイダンスについては、Microsoft ドキュメントへのリンクをクリックしてください。Azure から Windows VHD をダウンロードします。
   b) サブスクリプションを選択します（Linux イメージは、顧客管理の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

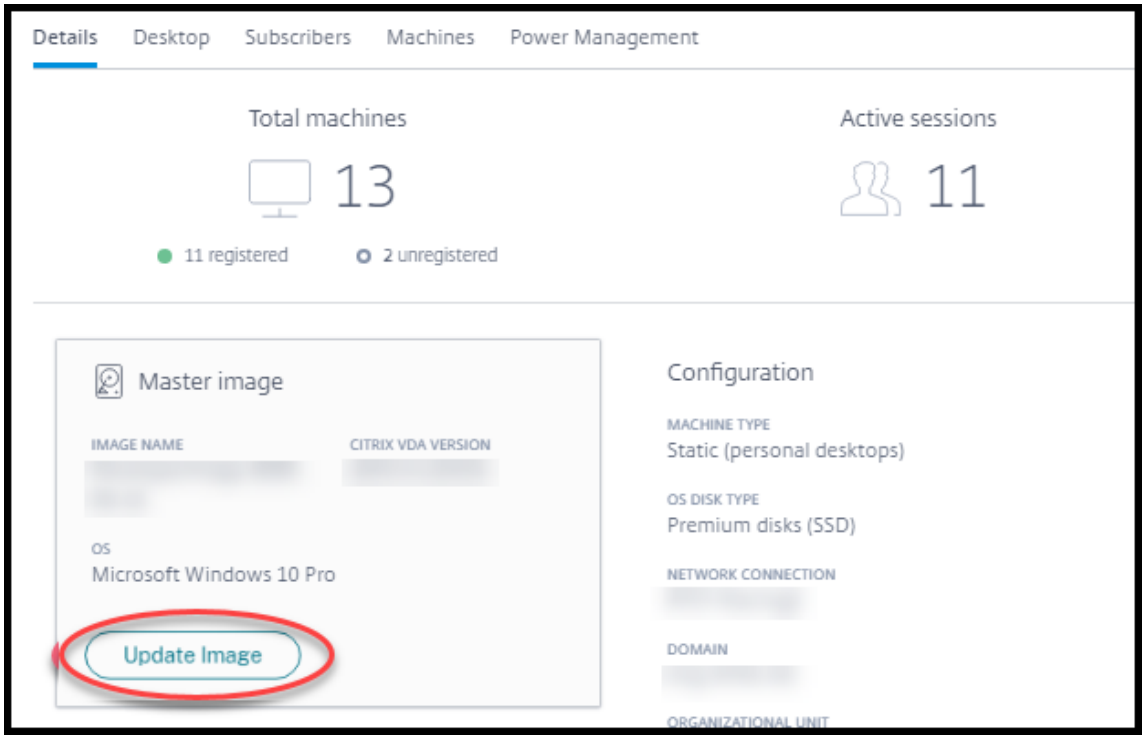
カタログの種類によって、カタログの更新時に更新されるマシンが決まります。

- ランダムカタログの場合、現在カタログにあるすべてのマシンが最新のイメージで更新されます。そのカタログにさら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、現在カタログにあるマシンは最新のイメージで更新されません。現在カタログにあるマシンは、作成元のイメージを引き続き使用します。ただし、そのカタログにさら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第 2 世代をサポートしている場合は、第 1 世代イメージのマシンを含むカタログを第 2 世代イメージで更新できます。同様に、カタログのマシンが第 1 世代をサポートしている場合は、第 2 世代マシンを含むカタログを第 1 世代イメージで更新できます。

新しいイメージでカタログを更新するには:

1. [管理**] > [Azure Quick Deploy**] ダッシュボードで、カタログのエントリ内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. ランダムカタログ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。Citrix DaaS for Azure が最初のイメージ処理を完了すると、利用者は、作業を保存してデスクトップからログオフするよう警告を受け取ります。ログオフ間隔は、利用者がメッセージを受け取っ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. 管理**] > [Azure Quick Deploy**] ダッシュボードで、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。

イメージへの **Windows VDA** のインストール

Citrix DaaS for Azure にインポートする予定の Windows イメージを準備するときは、次の手順に従います。Linux VDA インストールの手順については、Linux VDA の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 VM に接続します（まだ接続していない場合）。
2. Citrix Cloud のナビゲーションバーの ［ダウンロード］ リンクから、VDA をダウンロードできます。または、ブラウザーで Citrix DaaS for Azure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 用と、サーバー（マルチセッション）OS 用に、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、Citrix 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. 正常に構成されたことを確認するため、VM にインストールしたアプリケーションを 1 つまたは複数起動します。
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 のインストールについて詳しくは、「VDA のインストール」を参照してください。

ユーザーと認証

December 28, 2023

ユーザー認証方法

ユーザーは、デスクトップまたはアプリを起動するために Citrix Workspace にログインするとき、認証する必要があります。

Citrix DaaS 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、シトリックスが提供および管理する Azure Active Directory（AAD）です。お客様自身の 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。

- **ID** プロバイダー：Citrix Cloud で使用可能な任意の認証方法を使用できます。

> 注：
>
> - リモート PC アクセスの展開では、Active Directory のみを使用します。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。

ユーザー認証の設定には、次の手順があります：

1. Citrix Cloud および Workspace の構成で、ユーザー認証方法を構成します。
2. ユーザー認証に管理対象 Azure AD を使用している場合は、ディレクトリにユーザーを追加します。
3. カタログにユーザーを追加します。

Citrix Cloud でのユーザー認証の構成

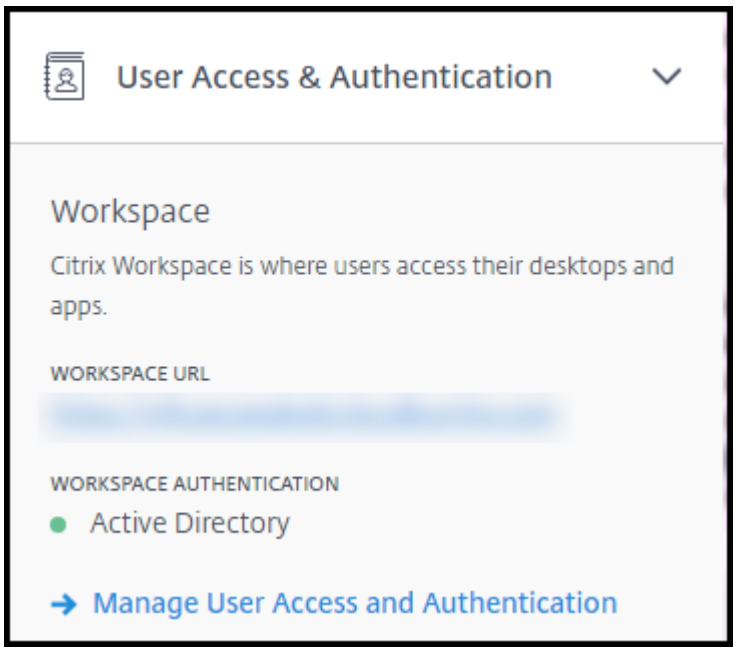
Citrix Cloud でユーザー認証を構成するには：

- 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、この接続方法を使用するように Workspace 認証を設定します。

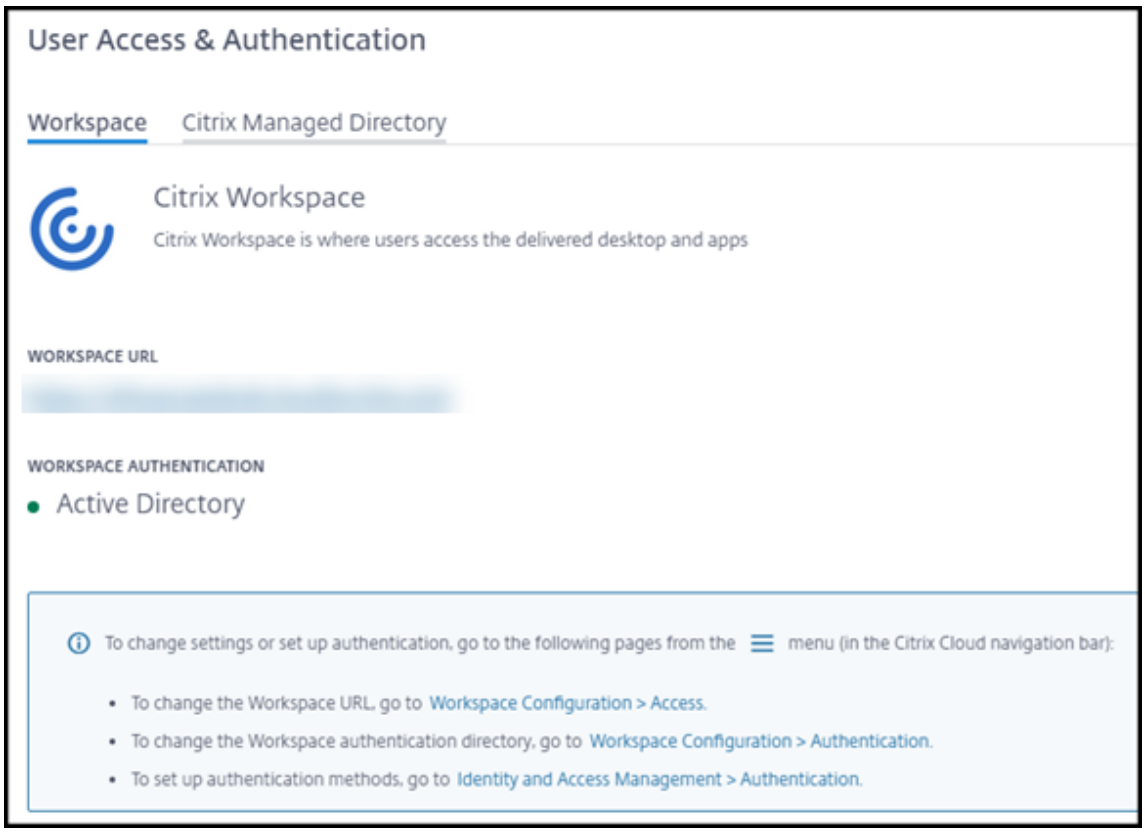
> 注：
>
> デフォルトでは、管理対象 Azure AD 認証方法が構成されています。つまり、Citrix Cloud に自動的に接続され、Citrix DaaS for Azure の管理対象 Azure AD を使用するように Workspace 認証が自動的に設定されます。この方法を使用する場合（および以前に別の方法を構成したことがない場合）は、「管理対象 Azure AD でのユーザーの追加と削除」に進みます。
> 管理対象 Azure AD が切断されると、Workspace の認証は Active Directory に切り替わります。別の認証方法を使用する場合は、以下の手順に従ってください。

認証方法を変更するには：

1. Citrix DaaS for **Azure** の［管理］**>**［**Azure** クイック展開］ダッシュボードで、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 1 つのタブは、現在構成されているユーザー認証方法を示します)。



3. [認証方法を設定するには] リンクをクリックすると、Citrix Cloud に移動します。選択する方法の省略記号メニューで [接続] を選択します。

4. 引き続き Citrix Cloud で、左上隅のメニューの ［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。

次にやること：

- 管理対象 Azure AD を使用している場合は、ディレクトリにユーザーを追加します。
- すべての認証方法で、カタログにユーザーを追加します。

管理対象 **Azure AD** でのユーザーの追加と削除

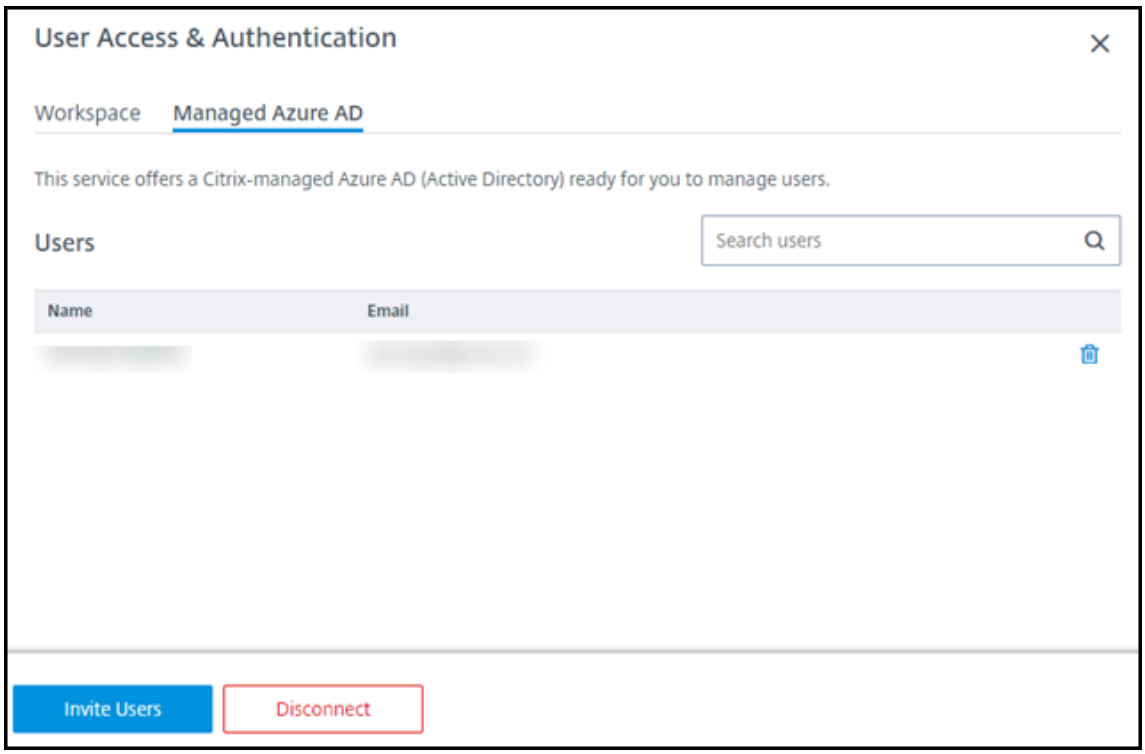
Citrix Workspace へのユーザー認証に管理対象 Azure AD を使用している場合にのみ、以下の手順に従ってください。

ユーザーの名前とメールアドレスを入力します。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。

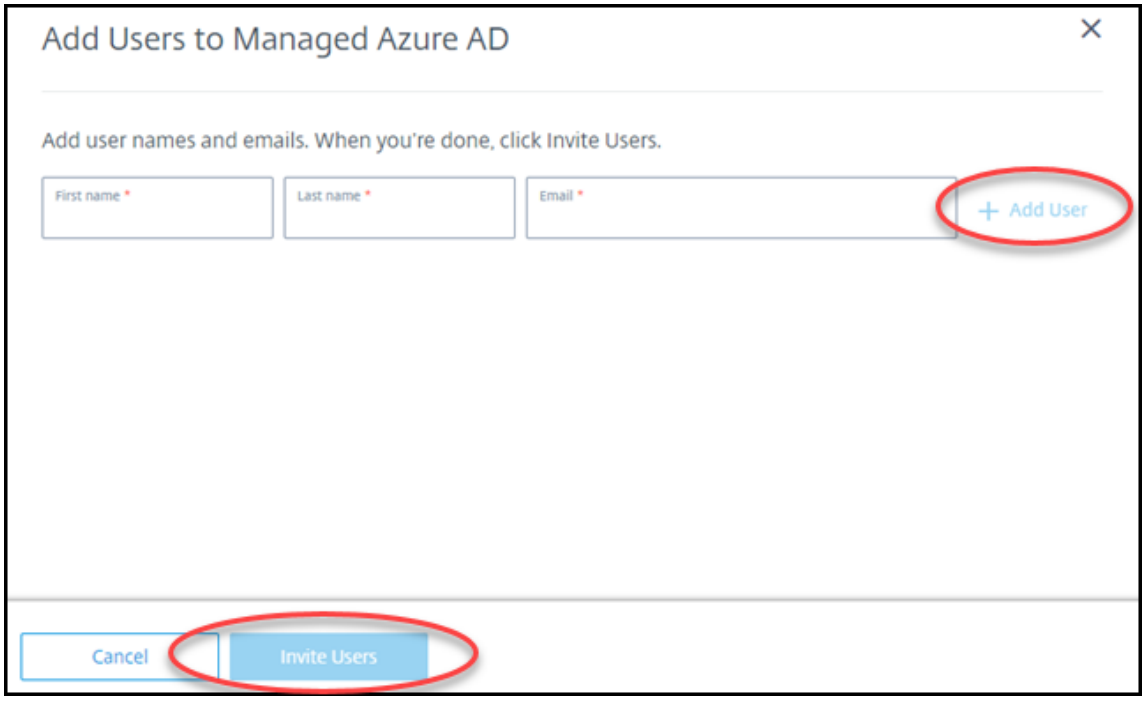
- ユーザーが指定した電子メールアドレスを持っている Microsoft アカウントをすでに持っている場合は、そのアカウントが使用されます。
- ユーザーがメールアドレスを使用した Microsoft アカウントを持っていない場合、Microsoft 社がアカウントを作成します。

ユーザーを管理対象 Azure AD に追加して招待するには：

1. Citrix **DaaS for Azure** の **[管理] > [Azure** クイック展開] 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

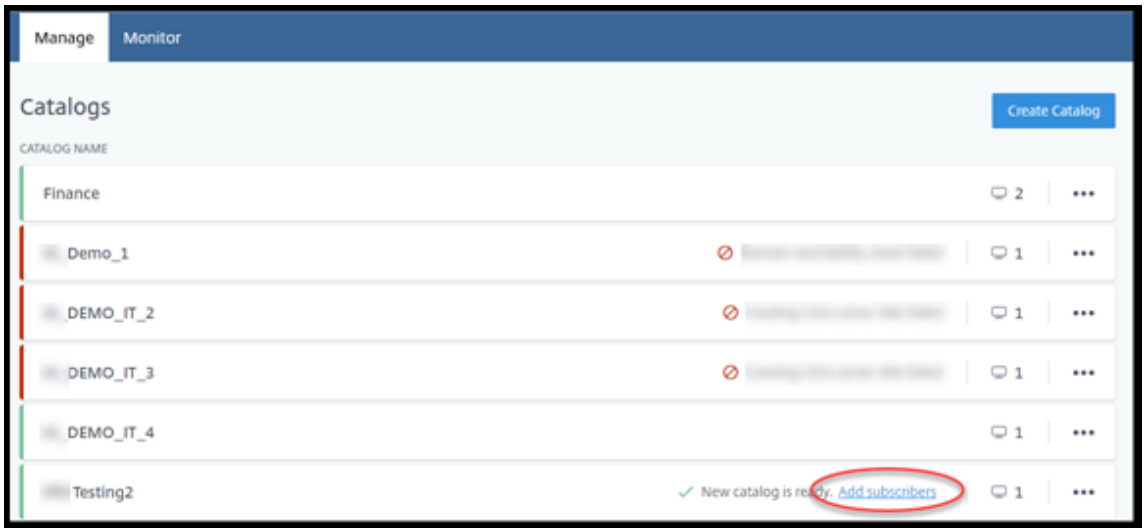
イコンをクリックします。削除を確認します。

次にやること：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

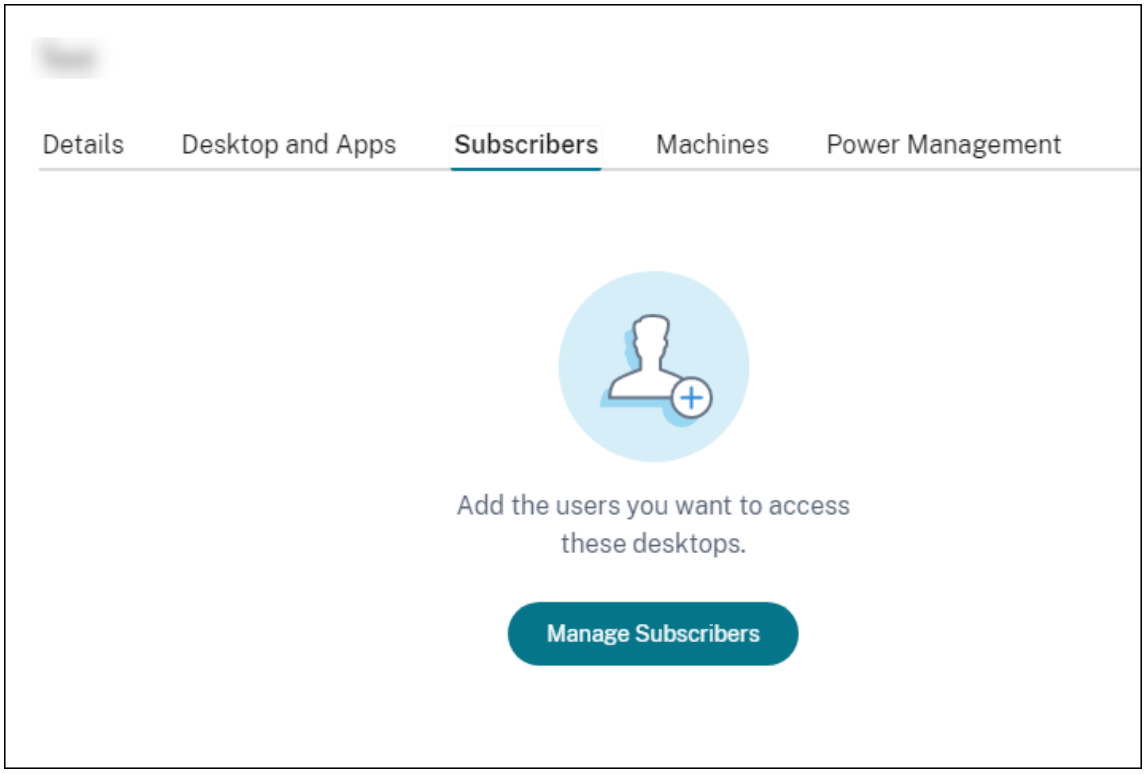
使用する認証方法に関係なく、以下の手順に従ってください。

1. Citrix DaaS for **Azure** の **[管理] > [Azure** クイック展開] 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、[サブスクライバーの追加] をクリックします。

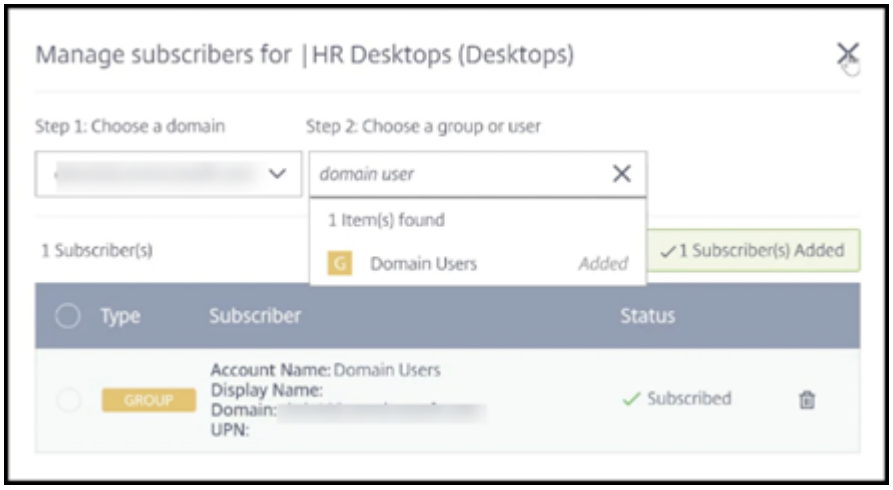


   すでにユーザーがあるカタログにユーザーを追加するには、カタログのエントリの任意の場所をクリックします。

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（ユーザー認証に管理対象 Azure AD を使用している場合、ドメインフィールドにはエントリが 1 つだけあります）。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。

次にやること：

- マルチセッションマシンを含むカタログの場合、まだ追加していない場合はアプリケーションを追加します。

- すべてのカタログについて、Citrix Workspace URL をユーザーに送信します 。

追加情報

Citrix Cloud での認証について詳しくは、「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

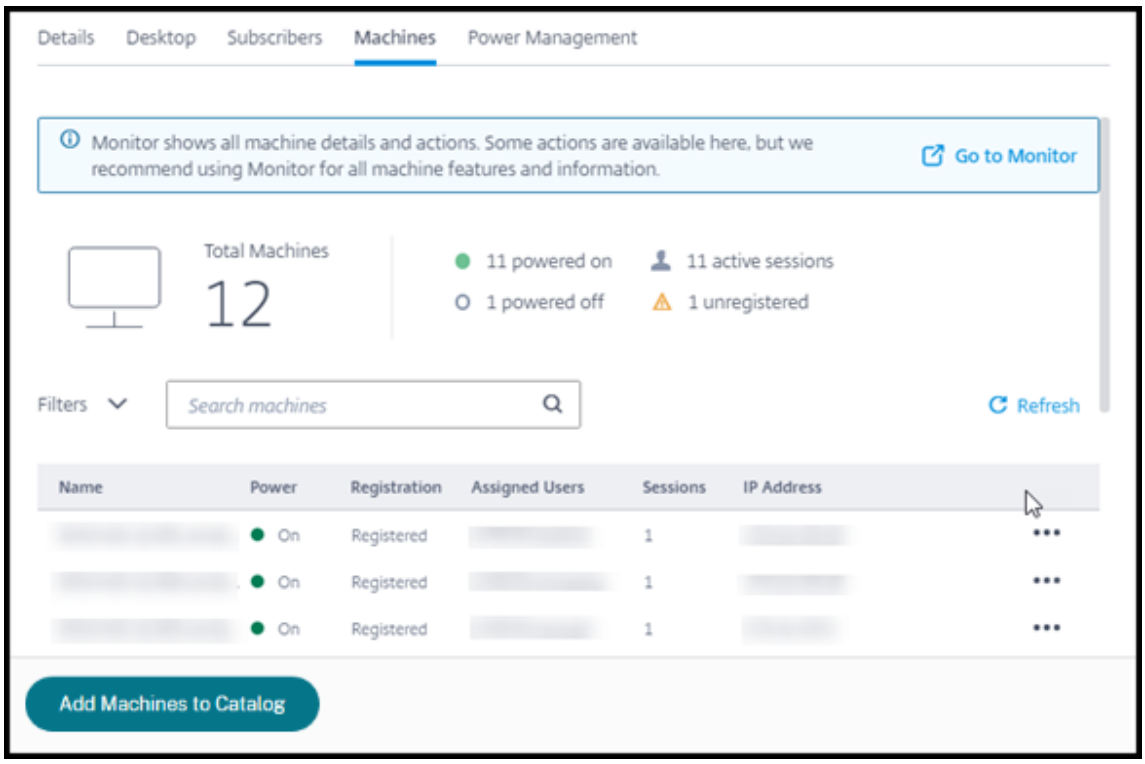
September 9, 2022

> 注:
>
> ここでは、簡易展開インターフェイスで作成されたカタログを管理するために使用できるタスクについて説明します。完全構成管理インターフェイスを使用したカタログ管理について詳しくは、「マシンカタログの管理」を参照してください。

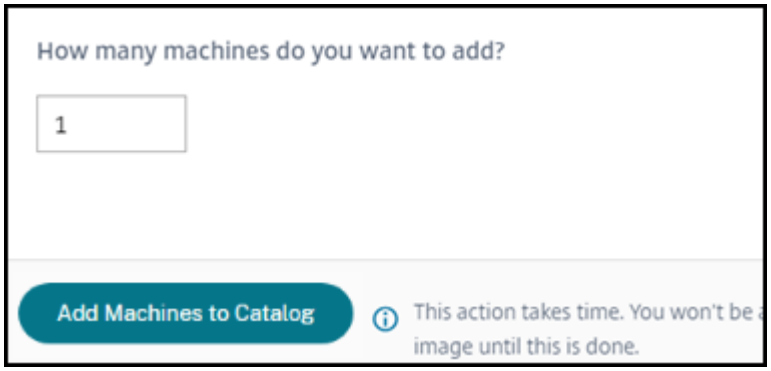
カタログへのマシンの追加

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. [管理] **> [Azure Quick Deploy**] ダッシュボードで、カタログのエントリ内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、電源管理スケジュール設定を使用して、電源がオンになっているマシンの数を制御したり ［マシン］タブから個別のマシンを削除したりできます。［マシン］タブからマシンを削除する方法については、「カタログ内のマシンの管理」を参照してください。

マシンあたりのセッション数の変更

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、ユーザーエクスペリエンスに影響を与えることがあります。この値を増やすと、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減少します。推奨事項:

利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. [管理**] > [Azure Quick Deploy**] 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. 要求を確認します。

この変更は、現在のセッションには影響しません。最大セッション数をマシンの現在アクティブなセッションの数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減少により実装されます。

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］画面には正しいセッション数が表示されます。更新プロセス中に障害が発生した場合、画面には求めたセッション数が示されます。

カタログ内のマシンの管理

> 注:
>
> **[**管理**] > [Azure** クイック展開**]** ダッシュボードから使用できるアクションの多くは、Citrix DaaS Standard for Azure（以前の Citrix Virtual Apps and Desktops Standard for Azure）の監視ダッシュボードからも使用できます。

管理**] > [Azure Quick Deploy**] ダッシュボードからアクションを選択するには:

1. [管理**] > [Azure Quick Deploy**] ダッシュボードで、カタログのエントリ内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。

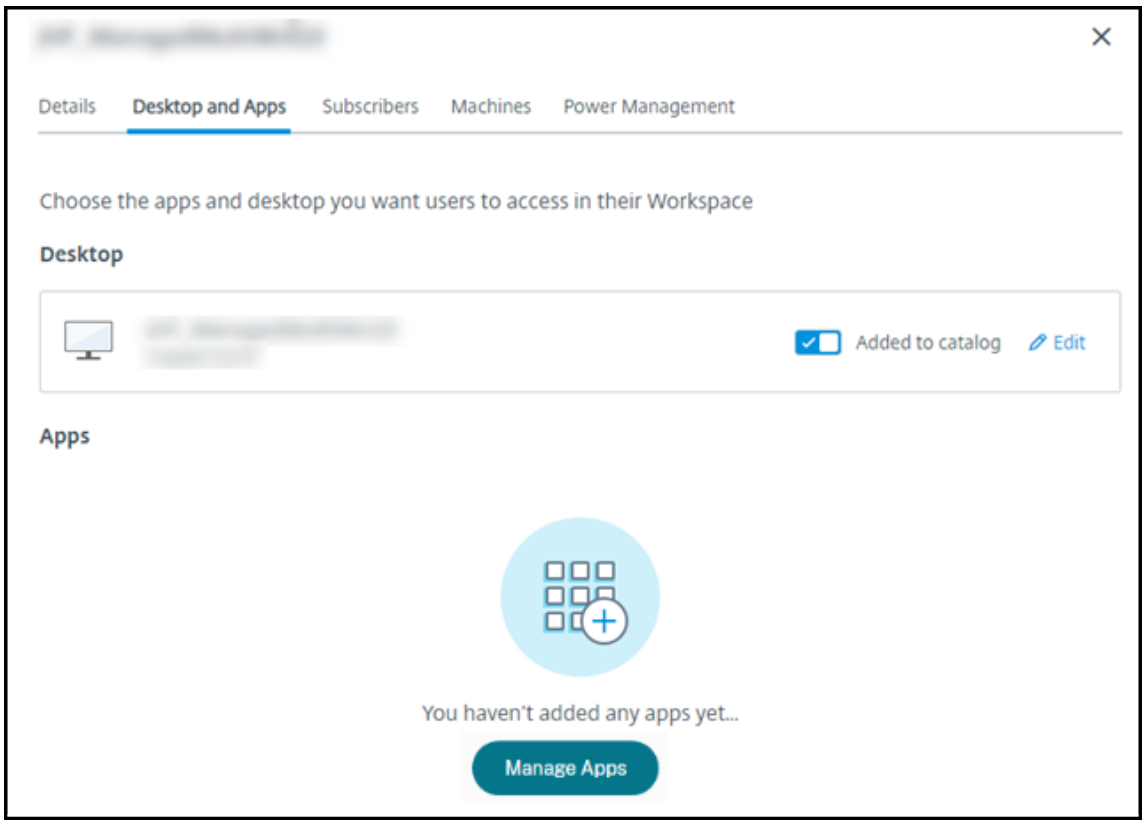
- 削除**:** 選択したマシンを削除します。この操作は、マシンのセッション数がゼロの場合にのみ使用できます。削除を確認します。

  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。

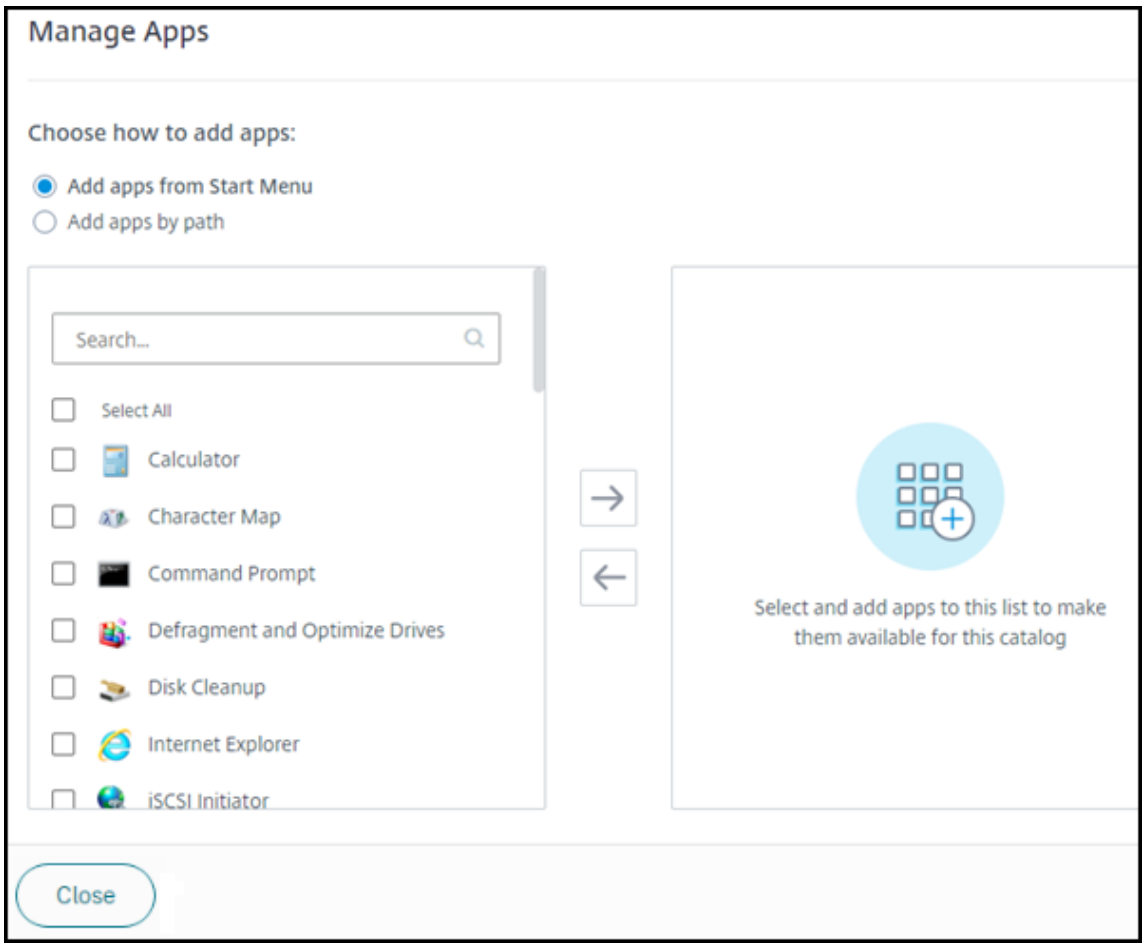
- 強制再起動**:** 選択したマシンを強制的に再起動します。このアクションは、マシンの [再起動] 操作が失敗した場合にのみ選択します。

カタログへのアプリの追加

1. [管理**] > [Azure Quick Deploy**] ダッシュボードで、カタログのエントリ内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。

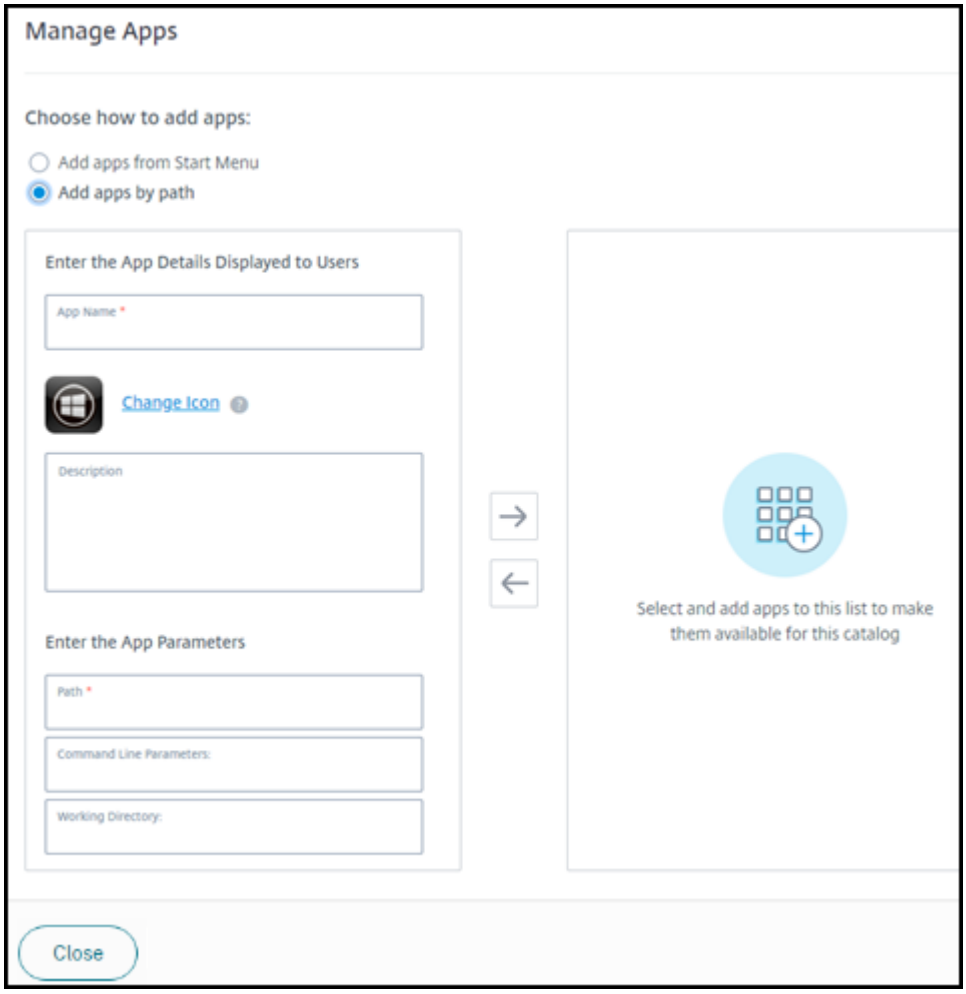


3. アプリを追加する方法を選択します：カタログ内のマシンの ［スタート］メニューから、またはマシン上の別のパスから。
4. ［スタート］メニューからアプリを追加するには：



- 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。そのあと、そのバージョンのアプリを追加できます。

5. パスにより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、ユーザーが Citrix Workspace で表示する名前です。
- 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。
- アプリへのパスを入力します。このフィールドは必須です。必要に応じて、コマンドラインパラメーター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ーの詳しくは、「公開アプリケーションへのパラメーターの受け渡し」を参照してください。

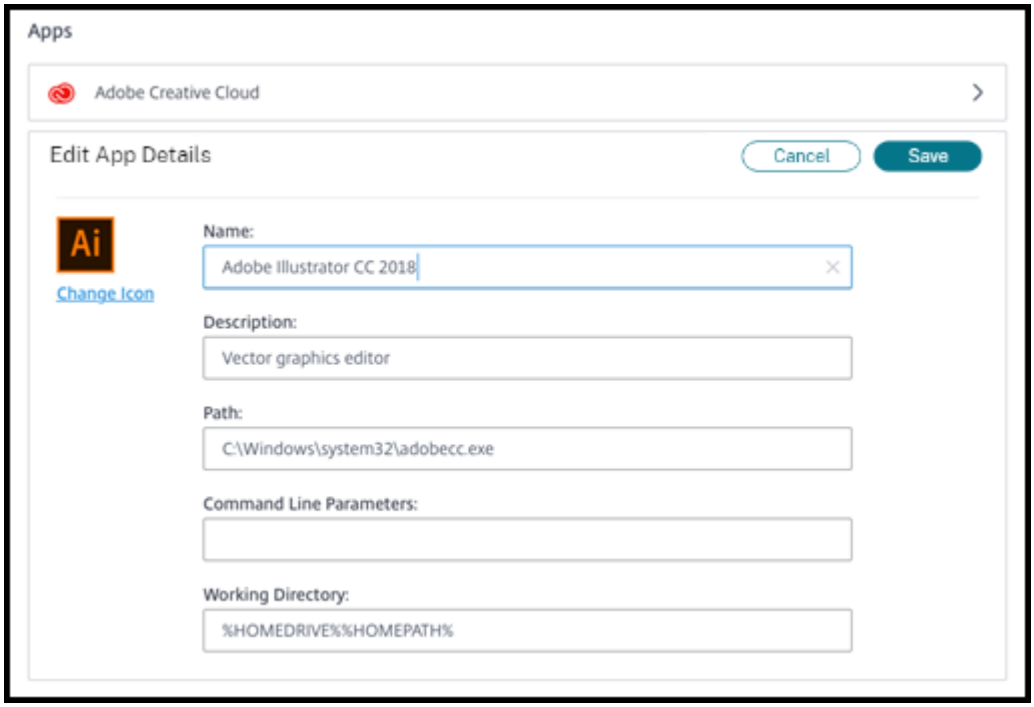
6. 完了したら、[閉じる] をクリックします。

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）: Citrix Workspace URL をユーザーに送信します（まだ送信していない場合）。

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場合があります。回避策として、アプリケーションの公開後に、アプリを編集して、正しく表示される別のアイコンを割り当てる ［アイコンの変更］機能を使用します。

カタログ内のアプリの編集

1. [管理] **> [Azure Quick Deploy**] ダッシュボードで、カタログのエントリ内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、編集するアプリが含まれている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内容を入力します:
   - 名前: ユーザーが Citrix Workspace で表示する名前。
   - 説明
   - パス: 実行可能ファイルへのパス。
   - コマンドラインパラメーター: 詳しくは、「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、コマンドライン（実行可能ファイルのパス）の末尾に（二重引用符で囲んだ）パーセント記号とアスタリスク記号が追加されます。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。記号が追加されている場合、デフォルトでは、ユーザーデバイスから渡されるパラメーターが検証されます。

  特殊なパラメーターを必要とする公開アプリケーションでは、コマンドラインに”%”（二重引用符で囲んだパーセント記号と 2 個のアスタリスク記号）が追加されています。これによりコマンドライン検証が無効になります。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。このとき、パスの末尾の二重引用符と、パーセント記号およびアスタリスク記号の前の二重引用符の間に、必ずスペースを 1 つ追加してください。

  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” “%*”
  ```

カタログからのアプリの削除

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 で表示されなくなるだけです。

1. [管理**] > [Azure Quick Deploy**] ダッシュボードで、カタログのエントリ内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。カタログの削除は元に戻すことができません。

1. [管理**] > [Azure Quick Deploy**] ダッシュボードで、カタログのエントリ内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。スケジュールは以下を提供します：

- 最適なユーザーエクスペリエンス：ユーザーは必要なときにマシンを使用できます。
- セキュリティ：指定した期間アイドル状態のままである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：デスクトップがアイドル状態のままであるマシンの電源はオフになります。マシンは、スケジュールされた実際の需要を満たすために電源がオンになります。

カスタムカタログを作成するとき、または後で作成するときに、電源スケジュールを構成できます。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。

簡易作成で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、クイック作成カタログは、コスト削減用プリセットスケジュールを使用します。後でそのカタログに対して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次のことが含まれています：

- スケジュールに含まれる情報を知ること
- スケジュールを作成すること

スケジュール内の情報

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、少し異なります。

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　Citrix DaaS for Azure には、いくつかのプリセットスケジュールが用意されています。カスタムスケジュールを構成して保存することもできます。カスタムプリセットを削除することはできますが、シトリックス提供のプリセットを削除することはできません。

タイムゾーン　電源がオンのマシンの設定とともにこれを使用することで、選択したタイムゾーンに基づいて営業時間と営業時間外を設定できます。

この設定は、すべてのマシンタイプで有効です。

電源オンのマシン：営業時間と営業時間外　営業時間を形成する曜日とその曜日の開始-終了時間。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、営業時間外と見なされます。いくつかのスケジュール設定では、営業時間と営業時間外に別々の値を入力できます。他の設定は常に適用されます。

この設定は、すべてのマシンタイプで有効です。

アイドル時のデスクトップセッションの切断　セッションが切断されるまで、デスクトップがアイドル状態（未使用）のままでいられる時間。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起動し直す必要があります。これはセキュリティ設定です。

この設定は、すべてのマシンタイプで有効です。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オフ　マシンの電源がオフになるまで、マシンが切断状態のままでいられる時間。マシンが電源オフになった後、ユーザーは Workspace に移動してデスクトップを起動し直す必要があります。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、デスクトップを切断するとします。次に、マシンがさらに 15 分間切断されたままだった場合は、マシンの電源をオフにします。

Tom さんがデスクトップを使用することをやめ、1 時間の会議に参加するため席を離れた場合、デスクトップは 10 分後に切断されます。さらに 15 分後、マシンの電源がオフになります（合計 25 分）。

ユーザーの立場から見ると、2 つのアイドル状態の設定（切断と電源オフ）は同じ効果があります。Tom さんがデスクトップから 12 分離れようと 1 時間離れようと、Workspace からデスクトップを起動し直す必要があります。この 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を与えます。

この設定は、シングルセッション（静的またはランダム）マシンに有効です。営業時間と営業時間外の値を入力できます。

切断されたセッションのログオフ　セッションが閉じるまで、マシンが切断状態のままでいられる時間。

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。

電源オフの遅延　マシンの電源がオフになる（および他の基準）まで、マシンの電源をオンにしておく必要がある最小時間。この設定により、セッション需要が不安定な期間にマシンが電源オンとオフを繰り返さないようにします。

この設定は、マルチセッションマシンで有効であり、常に適用されます。

実行中の最小マシン数　アイドル状態または切断状態の時間に関係なく、電源をオンのままにしておく必要があるマシンの数。

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。営業時間と営業時間外の値を入力できます。

処理能力バッファ　処理能力バッファは、バッファのマシンの電源をオンにしておくことで、需要の突然の急増に対応するのに役立ちます。このバッファは、現在のセッション需要のパーセンテージとして指定します。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、Citrix DaaS for Azure はセッション 110 個分の処理能力を提供します。需要の急増は、営業時間中、またはカタログへの新しいマシンの追加中に発生する可能性があります。

値が低いほど、コストが低くなります。値が高いほど、ユーザーエクスペリエンスの最適化に役立ちます。セッションを開始するとき、ユーザーは追加のマシンの電源がオンになるのを待つ必要はありません。

(処理能力バッファを含め）カタログに必要な電源オンのマシンの数をサポートするのに十分な数のマシンがある場合、追加のマシンの電源をオフにします。オフピーク時間だった、セッションがログオフした、またはカタログ内のマシンの数が少なかったことが原因で、電源オフが発生することがあります。マシンの電源をオフにする判断が下されるには、次の基準を満たす必要があります:

- マシンの電源がオンになっており、メンテナンスモードではない。
- マシンが使用可能なものとして登録されている、または電源をオンにした後で登録を待機している。
- マシンにアクティブなセッションがない。残りのセッションがすべて終了している（マシンがアイドルタイムアウト期間中アイドル状態だった)。
- 少なくとも「X」分間、マシンの電源がオンになっている（「X」はカタログで指定する電源オフの遅延時間)。

  静的カタログ内のすべてのマシンが割り当てられた後は、処理能力バッファがマシンの電源のオン/オフに関与することはなくなります。

この設定は、すべてのマシンタイプで有効です。営業時間と営業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. [管理**] > [Azure Quick Deploy**] ダッシュボードで、カタログのエントリ内の任意の場所をクリックします。
2. [電源管理] タブで、(上部のメニューにある）プリセットスケジュール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. いずれかのフィールド（日、時間、間隔など）の値を変更すると、プリセットの選択が自動的に ［カスタム］に変更されます。アスタリスク記号は、カスタム設定が保存されていないことを示します。
4. カスタムの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。共通プリセットを編集または削除することはできません。

VDA のスナップショットと復元

Citrix DaaS for Azure のスナップショットおよび復元機能は、デスクトップとアプリを配信する VDA での予期しないデータ損失やその他の障害から回復する方法を提供します。スナップショット操作では、マシンのスナップショットが作成され、保存されます。その後、リストアオペレーションでは、選択したスナップショットが使用されます。

- カタログ内のすべてのマシンに対して、日次および週次のスナップショットスケジュールを構成できます。このようなスナップショットを自動スナップショットと呼びます。カタログ内の各マシンのスナップショットが作成されます。デフォルトのスナップショットスケジュールはありません。
- カタログ内の 1 つの V をオンデマンドでバックアップできます。これを「手動スナップショット」と呼びます。マシンが属するカタログにスケジュールされたスナップショットがある場合でも、マシンの手動スナップショットを作成できます。ただし、単一マシンのスナップショットはスケジュールできません。

> 重要:
>
> Citrix DaaS for Azure のスナップショットおよび復元機能は、静的カタログ内のマシンおよびユーザーに割り当てられているマシンでのみサポートされます。

スナップショットスケジュール

注意：スナップショットスケジュールは、カタログ内のすべてのマシンに適用されます。

デフォルトでは、スナップショットスケジュールはありません。

スナップショットスケジュールを管理するには:

1. [管理] ダッシュボードで、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、[スナップショットのスケジュール] をクリックします。
3. [**Schedule Snapshots**] ページで、毎週または毎日の自動スナップショット、あるいはその両方のスケジュールを設定します。
    - 毎週のスナップショットを追加または変更するには、[毎週の自動スナップショット] のスライダーをチェックマークが表示されるまで動かします。曜日と開始時間を選択します。
    - 日次スナップショットを追加または変更するには、[毎日の自動スナップショット] のスライダーをチェックマークが表示されるまで動かします。開始時間を選択します。
    - 毎週のスナップショットを削除するには、[毎週の自動スナップショット] のスライダーを **X** が表示されるまで動かします。
    - 日次スナップショットを削除するには、[毎日の自動スナップショット] のスライダーを **X** が表示されるまで動かします。

4. 完了したら、ページの下部にある [保存] をクリックします。

手動スナップショット

手動スナップショットは、カタログ内の 1 台のマシンに対するものです。(1 台のマシンのスナップショットを撮るスケジュールは作成できません)。

1. [管理] ダッシュボードで、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、スナップショットを作成するマシンを探します。そのマシンの省略記号メニューで [スナップショット] を選択します。
3. [***VDA-name*** のスナップショット] ページで、[手動スナップショットの作成] をクリックします。
4. スナップショットの名前を指定します。推奨: 後で簡単に識別できる名前を選択します。
5. 要求を確認します。

スナップショットの表示と管理

1. [管理] ダッシュボードで、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、スナップショットを作成するマシンを探します。そのマシンの省略記号メニューで [スナップショット] を選択します。
3. ［***VDA-name*** のバックアップ］ページで、次の操作を行います。

    - マシンにスナップショットがない場合は、このマシンの手動スナップショットを作成するか、このマシンを含むカタログ内のすべてのマシンに対してスケジュールされたスナップショットを作成するように指示するメッセージが表示されます。
    - スナップショットを 1 つ選択して、マシンを復元できます。「復元」を参照してください。
    - スナップショットは削除できます。1 つまたは複数のスナップショットのチェックボックスをオンにし、テーブルヘッダーの [**Delete**] をクリックします。要求を確認します。

ヒント: カタログを削除すると、すべてのスナップショットが破棄されます。

復元

マシンは、そのマシンで使用可能な任意のスナップショットから復元できます。

リストア中は、マシンの電源がオフになります。スナップショットの復元中は、マシンの省略記号メニューのアクションは実行できません。

1. [管理] ダッシュボードで、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、スナップショットを作成するマシンを探します。そのマシンの省略記号メニューで [スナップショット] を選択します。
3. **[*VDA-name** のスナップショット**]** ページ * で、使用するスナップショットのチェックボックスをオンにします。

4. テーブルヘッダーの [復元] をクリックします。
5. リクエストを確定します。

［マシン］タブの［ステータス］列には、リストア操作の進行状況と結果が表示されます。

マシンがスナップショットの復元に失敗した場合は、再試行してください。

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

監視

May 19, 2023

［監視］ダッシュボードでは、Citrix DaaS Standard for Azure（旧称 Citrix Virtual Apps and Desktops 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、アプリケーション実行の終了、およびプロセス実行の終了も可能です。

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Citrix Cloudにサインインしていない場合は、サインインします。左上のメニューで、［マイサービス］**>** ［**DaaS Standard for Azure**］を選択します。
2. ［管理］ダッシュボードで、［監視］タブをクリックします。

デスクトップ使用状況の監視

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。期間をカスタマイズすることもできます (最終日、週、月)。

  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

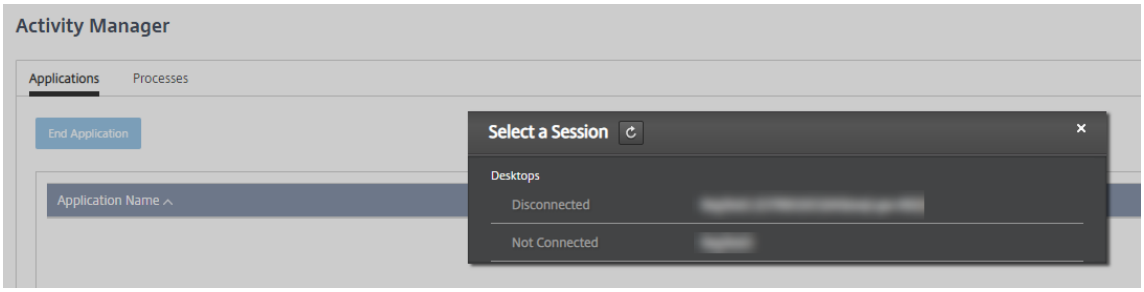
セッションとマシンの情報を監視しているときは、デフォルトですべてのマシンまたはセッションが表示されます。次の操作を実行できます:

- 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

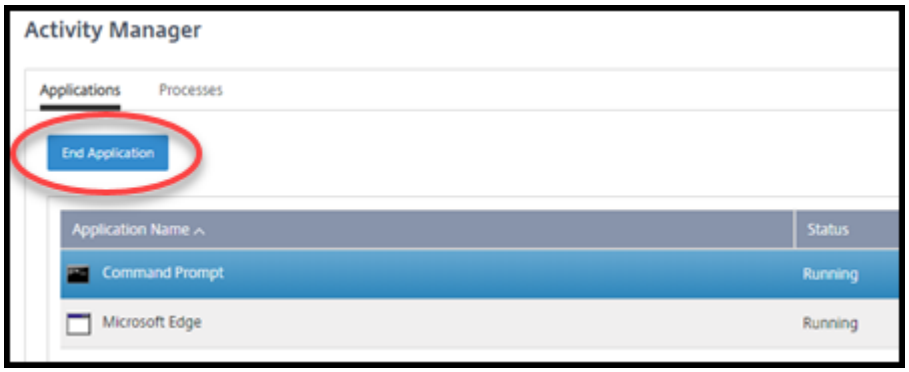
セッションを実行しているユーザーまたはデスクトップが割り当てられているユーザーのアプリケーションとプロセスを表示および管理できます。

1. [監視] ダッシュボードで ［検索］ をクリックし、ユーザー名（またはユーザー名の開始文字）、マシン、またはエンドポイントを入力します。検索結果の中から、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。

Citrix Managed Azure サブスクリプションでは、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。Citrix Managed Azure サブスクリプションでドメインに参加していないマシンをシャドウするには、要塞マシンを設定する必要があります。詳しくは、「踏み台マシンアクセス」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

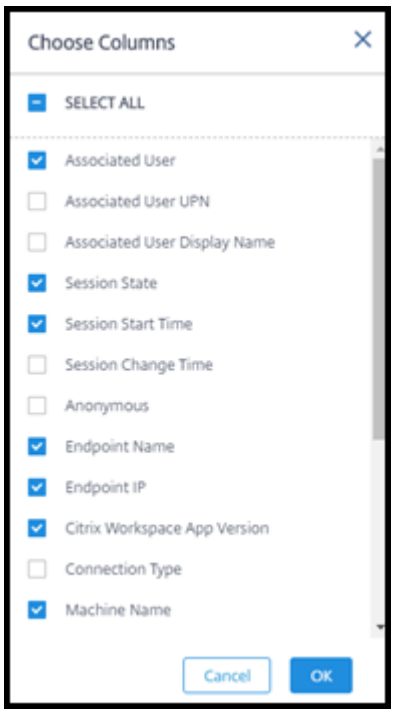
セッションの表示は毎分更新されます。

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. **[監視]** ダッシュボードから、**[フィルター]** タブをクリックします。

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。設定を完了したら、［**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。

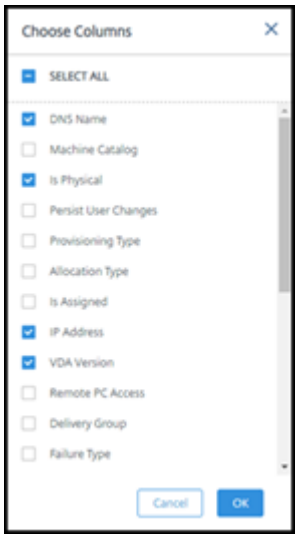
マシンの監視および電源管理

マシンの画面は、1 分ごとに更新されます。

1. **[**監視**]** ダッシュボードから、**[**フィルター**]** タブをクリックします。
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。設定を完了したら、[**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 DaaS for Azure for Citrix Service Providers

September 9, 2022

この記事では、Citrix Service Provider（CSP）で Citrix DaaS Standard for Azure（旧称 Citrix Virtual Apps and Desktops Standard for Azure サービス）を Citrix Cloud 内の顧客（テナント）向けに設定する方法について説明します。

Citrix 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 DaaS for Azure のサブスクリプションがある。

制限事項

- カスタマー名の変更がすべてのインターフェイスに適用されるまでに最大 24 時間かかる場合があります。
- 顧客を作成する際には、E メールアドレスは一意である必要があります。

既知の問題

- 顧客のユーザーがリソースに割り当てられた後は、そのユーザーを削除したり、割り当て解除したりすることはできません。
- 管理コンソールでは、お客様のユーザー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。

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」を参照する。

Citrix DaaS for Azure の ［管理］および ［監視］ダッシュボードでは、後でさらに管理者を追加したり、管理者が表示できる顧客を制御したりできます。

Citrix DaaS 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.［追加するサービスを選択する］で、［**Citrix DaaS Standard for Azure**］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、顧客が Citrix DaaS for Azure のサブスクリプションにオンボードされます。

オンボードが完了すると、自動的に Citrix DaaS for Azure に新しい顧客が作成されます。顧客は ［管理］**>**［クイック展開］に表示されます。

顧客別にリソースを絞り込む

Citrix DaaS for Azure の [管理**] > [Azure** クイック展開] ダッシュボードで、顧客別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 接続は顧客ごとに作成されます。お客様には SD-WAN Orchestrator サービス資格が必要です。

- 顧客の SD-WAN 接続を作成するには、SD-WAN 接続の作成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、顧客を選択します。[SD-WAN 接続タイプ] ボックスを選択できるのは、その顧客が SD-WAN Orchestrator サービス資格を持っている場合のみです。
- 接続を正常に作成するには、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、イメージが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）使用されます。詳しくは、「カタログを作成する」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。

Workspace Configuration を使用してワークスペースを構成すると、顧客のユーザーは各自のワークスペースにサインインして、使用可能にしたアプリや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. ［適用］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たすべてのサービスの管理制御を管理者に行わせる場合以外は、［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 DaaS for Azure 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。

カスタマー **ID** プロバイダへのパートナーのアクセス

ユーザーは、Citrix DaaS for Azure の **[**管理**] > [Azure** クイック展開] ダッシュボードまたは Citrix Cloud コンソールから管理できます。

ユーザーに非 AD アイデンティティプロバイダー（Citrix Managed Azure AD など）を使用する場合、その顧客のユーザーを管理するには、その顧客の Citrix Cloud Identity および Workspace 管理者である必要があります。顧客の管理者でない場合、その顧客のユーザーを追加または削除することはできません。

[管理] **> [Azure Quick Deploy]** ダッシュボードから顧客のユーザーを管理するには、[アイテムの表示] でパートナーまたは顧客を選択します。

- 例 **1**:［アイテムの表示］から顧客 A を選択します。ダッシュボードには顧客 A の品目だけが表示されるようになりました。カタログを選択すると、[購読者] タブには顧客 A のユーザのみが表示されます。顧客 A のユーザを追加または削除できます (その顧客の管理者である場合)。
- 例 **2:** [アイテムの表示] でパートナーエントリを選択します。ダッシュボードにはパートナーアイテムのみが表示されるようになりました。[サブスクライバー] タブには、パートナー用に作成されたユーザーのみが表示されます。顧客エントリは表示されません。そのパートナーのユーザーを追加または削除することはできますが (そのパートナーの管理者である場合)、この場所から顧客ユーザーを管理することはできません。

Citrix Cloud コンソールから顧客のユーザーを管理するには、サインイン後にプロンプトが表示されたら（または後で、Citrix Cloud コンソールの右上にある［顧客の変更］を使用して）顧客を選択します。ライブラリを使用してユーザーを管理する場合 、表示コンテキストには選択した顧客が反映されます。たとえば、顧客 A を選択した場合、ライブラリには顧客 A のオファリングのみが表示されます。

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、Citrix DaaS for Azure の役割とスコープのペアを選択またはクリアします。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

各顧客は、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 DaaS Standard for Azure** から：［管理］**>** ［**Azure** クイック展開］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
- セキュアなワークスペース

顧客のサービスの監視

CSP 環境では、Citrix Daas for Azure の ［監視］ダッシュボードは、基本的には CSP 以外の環境と同じです。詳しくは、「監視」を参照してください。

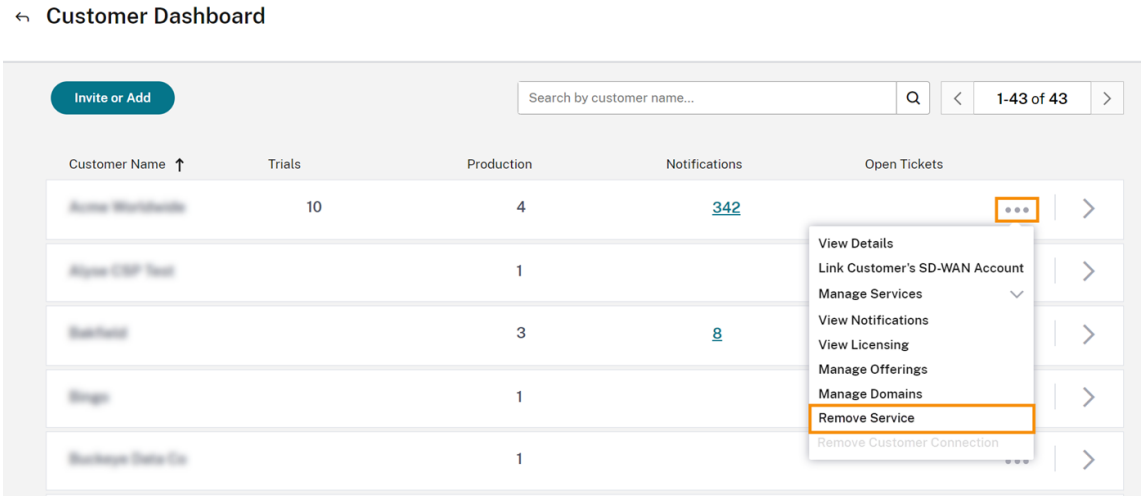
デフォルトでは、［監視］ダッシュボードにはすべての顧客に関する情報が表示されます。1 人の顧客に関する情報を表示するには、［顧客を選択します］を使用します。

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。

サービスの削除

開始する前に、顧客スコープが Citrix Daas Standard for Azure オブジェクトにリンクされていないことを確認してください。リンクされている場合、サービスを削除することはできません。スコープのリンクを解除するには、［**Citrix Studio**］**>** ［管理者］**>** ［スコープ］に移動して、スコープを編集します。スコープのリンク解除について詳しくは、「スコープの作成と管理」を参照してください。

1. Citrix Service Provider の資格情報で Citrix Cloud にサインインします。
2. 顧客ダッシュボードで、サービスを削除する顧客の省略記号メニュー（…）をクリックし、［サービスの削除］を選択します。



［削除するサービス］ページが表示されます。

3. ［削除］をクリックしてサービスを削除します。

トラブルシューティング

September 9, 2022

はじめに

リソースの場所には、デスクトップとアプリを提供するマシンが含まれています。これらのマシンはカタログで作成されるため、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 も含まれています。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。参照:

- 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の設定

Citrix DaaS for Azure には、デスクトップとアプリ（VDA）を提供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ツールとサポートツールがあります。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かったりすることがあります。

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 で 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後、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 サービスの問題のトラブルシューティングをした経験がある人を対象としています。以下が対象となります:

- Citrix DaaS 製品の技術的知識とトラブルシューティングの経験を持つ、Citrix Service Provider（CSP）など。
- 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、または自信がない場合は、Citrix サポートにサポートを依頼できます。Citrix サポート担当者から、このセクションで説明されているアクセス方法の 1 つを設定するように求められる場合があります。ただし、Citrix のツールと技術を使用した実際のトラブルシューティングは Citrix の担当者が行います。

> 重要:
>
> これらのサポート機能は、ドメイン参加済みマシンにのみ有効です。カタログ内のマシンがドメイン未参加の場合、Citrix サポートはトラブルシューティングのヘルプを要求するよう案内します。

アクセス方法

以下のアクセス方法は、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 つのサポートアクセス方法が提供されています。

- 顧客専用の Citrix Managed Azure サブスクリプション内の踏み台マシンを使用して、リソースにアクセスします。踏み台マシンは、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により、これらのリソースへの安全な接続を提供します。

  この方法の手順は次のとおりです:

  - 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
  - 踏み台マシンに RDP アクセスする
  - サブスクリプション内の踏み台マシンから他の 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連する問題を対象としています。

- 顧客専用の Citrix Managed Azure サブスクリプション内のマシンに直接 RDP アクセスします。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でポート 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。

注意事項：これら 2 つのアクセス方法以外の方法については、Citrix サポートにお問い合わせください。

踏み台マシンアクセス

1. Citrix **DaaS for Azure** の **[管理] > [Azure** クイック展開] 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 種類の問題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. [踏み台マシンを使ってトラブルシューティングを行う] ページで、カタログを選択します。
   - 選択したカタログのマシンがドメイン未参加の場合は、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既に作成されている場合は、手順 8 にスキップします。
5. RDP アクセス範囲が表示されます。ネットワーク接続で許可されている範囲よりも狭い範囲に RDP アクセスを制限する場合は、[**IP** アドレス範囲内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、目的の範囲を入力します。

6. 踏み台マシンに RDP アクセスするとき、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。

   ユーザー名に 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、ページタイトルが踏み台 **-** 接続に変わります。

   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）、失敗通知ページの下部にある ［削除］をクリックします。もう一度、踏み台マシンの作成を試行してください。

   踏み台マシンの作成後に、RDP 範囲の制限を変更できます。［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（変更をキャンセルするには、［**X**］をクリックします）。

8. ［**RDP** ファイルのダウンロード］をクリックします。
9. 踏み台マシンの作成時に指定した資格情報を使用して、踏み台マシンに RDP アクセスします（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. サブスクリプション内の踏み台マシンから他の 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、作成時に電源がオンになります。コストを節約するため、マシンが起動後にアイドル状態のままである場合、マシンの電源は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、踏み台マシンを電源管理または削除できます。踏み台マシンの削除を選択した場合は、マシン上のアクティブなセッションが自動的に終了になることを確認する必要があります。また、マシンに保存されていたデータやファイルはすべて削除されます。

直接 **RDP** アクセス

1. Citrix **DaaS for Azure** の **[管理] > [Azure** クイック展開] 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** アクセスを使ってトラブルシューティングを行う］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への RDP アクセスが既に有効になっている場合は、手順 7 にスキップします。

5. RDP アクセス範囲が表示されます。ネットワーク接続で許可されている範囲よりも狭い範囲に RDP アクセスを制限する場合は、［**IP** アドレス範囲内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、目的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、失敗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

引き続き問題が発生する場合は、「ヘルプとサポートの利用」の手順に従ってチケットを作成してください。

制限

May 19, 2023

この記事では、Citrix DaaS Standard for Azure（旧称 Citrix Virtual Apps and Desktops Standard for Azure サービス）の展開におけるリソースの制限を示します。

> 注:
>
> この制限は、Citrix が推奨するものです。

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	2,500

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	10,000
マルチセッション VDA	1,000

Citrix Cloud Connector はリソースロケーションに割り当てられ、ワークロードを Citrix DaaS for Azure にリンクします。Cloud Connector の制限とサイズとスケールの推奨事項については、「Cloud Connector のサイズとスケールの考慮事項」を参照してください。

プロビジョニング制限

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	上限
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	2,500

使用制限

リソース	上限
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、Citrix DaaS for Azure の試用期間中の制限を示します。

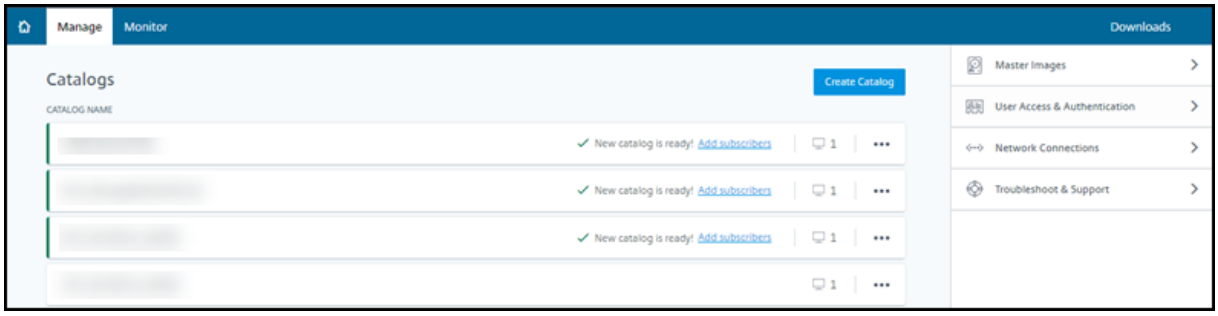
Azure サブスクリプション	リソース	上限
Citrix Managed Azure サブスクリプション	カタログの最大数	3
	最大ユーザー数	25
	カタログあたりの VDA の最大数	3
カスタマー管理の Azure サブスクリプション	カタログの最大数	10
	最大ユーザー数	25
	カタログあたりの VDA の最大数	10

リファレンス

September 9, 2022

ダッシュボード

Citrix DaaS Standard for Azure（旧称 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］ダッシュボードと ［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後、Citrix Cloud にサインインして Citrix DaaS for Azure 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］**>** ［**DaaS Standard for Azure**］を選択します。または、画面のメイン領域の ［**DaaS Standard for Azure**］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、［ようこそ］ページの ［開始］をクリックします。[管理**] > [Azure** クイックデプロイ] ダッシュボードが表示されます。
4. カタログが既に作成されている場合は、[管理**] > [Azure Quick Deploy**] ダッシュボードに自動的に移動します。
5. ［監視］ダッシュボードにアクセスするには、［監視］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を表示するには、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

[管理**] > [Azure Quick Deploy**] ダッシュボードで、カタログのエントリ内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表示されます:

- 詳細：カタログの作成時（または最新の編集時）に指定した情報を一覧表示します。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ます。

  このタブで、次のことができます:

  - カタログで使用されているイメージの変更。
  - カタログの削除。
  - カタログで使用されているリソースの場所の詳細が含まれる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。このタブで、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、次のことができます:

  - 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の追加、編集、または削除。
  - カタログの名前と説明の変更。

- 利用者：種類（ユーザーまたはグループ）、アカウント名、表示名、および Active Directory ドメインとユーザープリンシパル名を含むすべてのユーザーを一覧表示します。

  このタブで、カタログのユーザーを追加または削除できます。

- マシン：カタログ内のマシンの総数のほか、登録済みのマシン、未登録のマシン、およびメンテナンスモードがオンになっているマシンの数を表示します。

  カタログ内の各マシンについて、画面には各マシンの名前、電源状態（オン/オフ）、登録の状態（登録済み/未登録）、割り当て済みユーザー、セッション数（0/1）、およびメンテナンスモードの状態（オンまたはオフを示すアイコン）などが表示されます。

このタブで、次のことができます:

- マシンの追加または削除
- 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のオン/オフの切り替え

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、［監視］ダッシュボードからも使用できます。「マシンの監視と電源管理」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がオン/オフになるタイミングを管理できます。スケジュールは、アイドル状態のマシンがいつ切断されるかも示します。

  カスタムのカタログを作成するとき、または後で、電源スケジュールを構成できます。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、クイック作成カタログは、コスト削減用プリセットスケジュールを使用します。ただし、後でそのカタログを編集したりスケジュールを変更したりできます。

  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

このセクションの記述は、ドメイン参加済みマシンを含むすべての展開に適用されます。ドメイン非参加マシンのみを使用する場合は、このセクションを無視してかまいません。

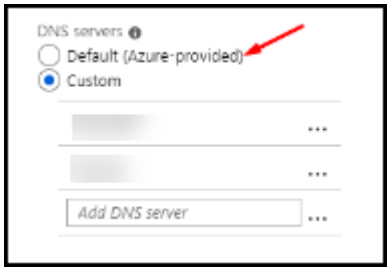
1. ドメイン参加済みカタログ（または、Citrix Managed Azure サブスクリプションを使用している場合は、接続）を作成する前に、パブリックドメイン名とプライベートドメイン名を解決できる DNS サーバーエントリがあるかどうかを確認してください。

   Citrix DaaS for Azure は、カタログまたは接続を作成するとき、少なくとも 1 つの有効な DNS サーバーエントリを探します。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:

   - 自身の 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］エントリを確認します。
   - Citrix Managed Azure サブスクリプションを使用していて、Azure VNet ピアリング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いて、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。Citrix DaaS for Azure は、［デフォルト **(Azure** で提供**)**］設定では使用できません。



- ［デフォルト **(Azure** で提供**)**］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］の下に DNS サーバーのエントリがすでにある場合は、Citrix DaaS for Azure 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てください。
- ドメイン名を解決できる DNS サーバーがない場合は、それらの機能を備えた Azure 提供の DNS サーバーを追加することを Citrix ではお勧めします。

3. DNS サーバーの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（VM は、再起動するまで現在の DNS 設定を使用し続けます）。

接続の作成後、後で DNS アドレスを変更する場合：

- 自身の Azure サブスクリプションを使用する場合は、（前の手順で説明したように）Azure で変更できます。または、Citrix DaaS for Azure 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、Citrix DaaS for Azure は、Azure で行った DNS アドレスの変更を同期しません。ただし、接続の DNS 設定は Citrix DaaS for Azure で変更できます。

DNS サーバー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に問題が生じる可能性があることに注意してください。

Citrix DaaS for Azure 経由で **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、その 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) 管理**] > [Azure Quick Deploy**] ダッシュボードで、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（VM は、再起動するまで現在の DNS 設定を使用し続けます）。

ポリシー

ドメイン未参加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に RDP で接続します。
2. Citrix グループポリシー管理をインストールします:

   a) CTX220345を参照します。添付ファイルをダウンロードしてください。
   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`フォルダーにある`CitrixGroupPolicyManagement_x64.msi`をダブルクリックしてください。

3. [ファイル名を指定して実行] `gpedit.msc`コマンドを使用してを起動すると、グループポリシーエディターが開きます。
4. `User Configuration Citrix Policies > Unfiltered`で、[ポリシーの編集] をクリックします。

   グループポリシー管理コンソールで障害が発生した場合は（CTX225742を参照）、Microsoft Visual C++ 2015 のランタイム（またはそのランタイムの以降のバージョン）をインストールします。

5. 必要に応じて、ポリシー設定を有効にします。例:

   - ［設定］タブの ［コンピューターの構成］または ［ユーザーの構成］で作業をする場合（構成するものに応じて選択）、`Category > ICA / Printing`で ［**PDF** ユニバーサルプリンターを自動作成する］を選択して［`Enabled`］に設定します。
   - ログインしたユーザーをデスクトップの管理者にする場合は、［対話型ユーザー］グループを組み込みの管理者グループに追加します。

6. 完了したら、イメージを保存します。
7. 新しいイメージを使用して、既存のカタログの更新または新しいカタログの作成を行います。

ドメイン参加済みマシンのグループポリシーの設定

1. 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には、役割と機能を追加するための Windows ツール（[役割と機能の追加］など）を使用して、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には、適切なオペレーティングシステム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、［スタート］メニューでグループポリシー管理コンソールを使用できます。
2. Citrix の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。「ドメインに参加していないマシンのグループポリシーを設定する、手順 2 から最後まで」の手順に従います。

> 注:
>
> Citrix Studio コンソールは Citrix DaaS for Azure では利用できませんが、利用可能な機能については、ポリシー設定の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

デスクトップとアプリを公開するための最初のカタログを作成すると、Citrix によりリソースの場所と 2 つの Cloud Connector が自動的に作成されます。カタログを作成するときに、その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の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、リソースの場所が作成された後に使用可能な操作について説明します。

1. 管理**] > [Azure Quick Deploy**] ダッシュボードで、右側の [クラウド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。各リソースの場所のエントリには、そのリソースの場所内の各 Cloud Connector の状態とアドレスが含まれます。

リソースの場所のエントリにある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

［ヘルスチェックの実行］を選択すると、接続チェックがすぐに開始されます。チェックに失敗した場合、その Cloud Connector は Citrix Cloud と通信していないため、状態は不明です。Cloud Connector を再起動することをお勧

めします。

Connector の再起動

Citrix では、一度に 1 つの Cloud Connector のみ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、完了するまでに 20 分かかります。

以下の情報を入力します:

- 追加する Cloud Connector の数。
- Cloud Connector マシンをドメインに参加させるために使用されるドメインサービスアカウントの資格情報。
- マシンパフォーマンス。
- Azure リソースグループ。デフォルトは、リソースの場所によって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。
- ネットワークにインターネット接続用の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、Citrix サポートはその Cloud Connector を削除することを推奨する場合があります。

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。

使用可能な Cloud Connector を削除することもできます。ただし、その Cloud Connector を削除することでリソースの場所で使用可能な Cloud Connector が 2 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。

更新時間の選択

Citrix は、Cloud Connector のソフトウェア更新プログラムを自動的に提供します。更新中、1 つの Cloud Connector がオフラインになって更新されますが、他の Cloud Connector はサービスを継続します。最初の更新

が完了すると、別の Cloud Connector がオフラインになって更新されます。このプロセスは、リソースの場所にあるすべての Cloud Connector が更新されるまで続きます。多くの場合、更新を開始するのに最適な時間は、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にアクセスできるのか、それとも企業ネットワーク内からのみアクセスできるのかを指定します。

Profile Management

Profile Managementを使用すると、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なります。

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、ログオンおよびログオフ時のユーザーエクスペリエンスも向上します。

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。そのファイルサーバーを管理します。これらのファイルサーバーへのアクセスを許可するように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 を有効にする場合は、ユーザーのプロファイルをさらに最適化するため、フォルダーリダイレクトを構成してユーザープロファイルのサイズの影響を最小限に抑えることも検討してください。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 フォルダーリダイレクト」を参照してください。

Windows Server ワークロード用の **Microsoft RDS** ライセンスサーバーの構成

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。Citrix VDA がインストールされている Windows マシンは、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「リモートデスクトップサービスライセンスサーバーをアクティブ化する」を参照してください。概念実証環境では、Microsoft 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「クライアントアクセスライセンス（CAL）を使用して RDS 展開をライセンスする」を参照してください。

グループポリシー設定を使用して RDS ライセンスサーバーを構成するには

1. 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アドレスと単一ユーザー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段階です。

[管理**] > [Azure Quick Deploy**] 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、月単位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。
- 月単位の消費コミットメントのユニット数。
- 期間の消費コミットメントのパーセンテージ。

値と進行状況バーにより、潜在的または実際の使用量の超過が通知されることがあります。

実際のデータが表示されるまでに 24 時間かかることがあります。使用状況と課金データは、カレンダー月の終わりから 72 時間後が最終と見なされます。

使用状況について詳しくは、「Citrix DaaS Standard for Azure のライセンスと使用状況の監視」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の監視

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 DaaS Standard for Azure のライセンスと使用状況の監視」のガイダンスに従ってください。以下を表示できます:

- 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

ライセンスを解放することもできます。

負荷分散

負荷分散は、シングル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、サポートされているホストの種類（クラウドベースおよびオンプレミス）を使用して作成したすべてのカタログが含まれます。カタログの作成に使用したインターフェイス（Studio や［クイック展開］など）は関係ありません。
>
> 続行する前に、すべてのカタログにセッションの上限が設定されていることを確認してください。
>
> - Citrix DaaS for Azure のクイック展開管理インターフェイスでは、この設定は各カタログの ［詳細］ タブにあります。
> - 他の Citrix DaaS 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。

負荷分散により、マシンの負荷が測定され、現在の条件下で受信ユーザーセッション用として選択されるマルチセッションマシンが決定されます。この選択は、構成済みの負荷分散方法に基づきます。

水平または垂直の 2 つの負荷分散方法のいずれかを構成できます。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（つまり、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を、最も負荷が少なく電源がオンになっている使用可能なマシンに割り当てます。

  簡単な例：それぞれ 10 セッション用に構成された 2 つのマシンがあるとします。最初のマシンは 5 つの同時セッションを処理します。2 つ目のマシンは他の 5 つのセッションを処理します。

  水平負荷分散によって高いユーザーパフォーマンスを実現できますが、より多くのマシンの電源をオンにして使用し続けるので、コストが増加する可能性があります。

  デフォルトでは、この方法が有効になっています。

- 垂直負荷分散：受信ユーザーセッションを、読み込みインデックスが最も高く電源がオンになっているマシンに割り当てます（Citrix DaaS for Azure は、すべてのマルチセッションマシンの読み込みインデックスを計算してから割り当てます。この計算では、CPU、メモリ、同時実行性などの要素が考慮されます）。

  この方法により、既存のマシンが飽和状態になった後、新しいマシンに移ります。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：それぞれ 10 セッション用に構成された 2 つのマシンがあるとします。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、セッションは電源オンのマシンの容量を最大化し、マシンコストを節約できます。

負荷分散方法を構成するには：

1. [管理] **> [Azure Quick Deploy**] ダッシュボードで、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

ネットワークにインターネット接続用のプロキシサーバーが必要であり、自身の Azure サブスクリプションを使用している場合は、以下の手順に従ってください（プロキシサーバーを必要とするネットワークでの Citrix Managed Azure サブスクリプションの使用はサポートされていません）。

1. **[**管理] **> [Azure Quick Deploy**] ダッシュボードから、必要な情報を入力し、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. プロキシ要件が原因で、カタログの作成は失敗します。ただし、リソースの場所は作成されます。カタログの作成時にリソースの場所の名前を指定した場合を除き、そのリソースの場所の名前は「DAS」で始まる名前になります。Citrix DaaS for Azure コンソールで、[**Cloud** 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。ある場合は、それらを削除します。

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）。そ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、各仮想マシンに Cloud Connector をインストールします 。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. **[管理] > [Azure Quick Deploy**] ダッシュボードから、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。
- Citrix DaaS for Azure についてさらに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サポートチケットを開いてください。